# Contents


- Failoverclustering
  - Neues beim Failoverclustering
  - Grundlegende Informationen
    - Dateiserver mit horizontaler Skalierung für Anwendungsdaten
    - Cluster- und Poolquorum
    - Fehlerdomänenunterstützung
    - Vereinfachte SMB Multichannel- und Multi-NIC-Clusternetzwerke
    - VM-Lastenausgleich
    - VM-Lastenausgleich (Vertiefung)
    - Clustergruppen
    - Clusteraffinität
  - Planen
    - Hardwareanforderungen
    - Verwenden von freigegebenen Clustervolumes (CSVs)
    - Verwendung von Gast-VM-Clustern
  - Bereitstellen
    - Erstellen eines Failoverclusters
    - Bereitstellen eines Dateiservers mit zwei Knoten
    - Vorabbereitstellen eines Clusters in AD DS
      - Konfigurieren von Clusterkonten in Active Directory
    - Verwalten des Quorums und von Zeugen
    - Bereitstellen eines Cloudzeugen
    - Bereitstellen eines Dateifreigabezeugen
    - Paralleles Upgrade für Clusterbetriebssystem
    - Upgrade eines Failoverclusters auf derselben Hardware
  - Verwalten
    - Clusterfähiges Aktualisieren
      - Anforderungen und Best Practices
      - Erweiterte Optionen

Häufig gestellte Fragen
Plug-Ins
Integritätsdienst
Berichte
Fehler
Aktionen
Einstellungen
Clusterdomänenmigration
Problembehandlung mit der Windows-Fehlerberichterstattung
Problembehandlung bei einem Clusterproblem mit Ereignis-ID 1135
Problem beim Löschen eines Knotens
Entfernen eines Knotens aus aktiver Failoverclustermitgliedschaft
Anpassen des Baselinenetzwerk-Schwellenwerts für das Failover
Cluster System-Protokollereignisse
Änderungsverlauf für Failovercluster-Themen

# Failoverclustering in Windows Server

15.05.2020 • 3 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Ein Failovercluster ist eine Gruppe aus unabhängigen Computern, die miteinander interagieren, um die Verfügbarkeit und Skalierbarkeit von Clusterrollen (früher Clusteranwendungen und -dienste genannt) zu erhöhen. Die Clusterserver (sogenannte Knoten) sind durch physische Kabel und durch Software miteinander verbunden. Wenn auf einem oder mehreren der Clusterknoten ein Fehler auftritt, werden seine Aufgaben sofort von anderen Knoten übernommen. Dieser Vorgang wird als Failover bezeichnet. Zusätzlich werden die Clusterrollen proaktiv überwacht, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Funktionieren sie nicht, werden sie neu gestartet oder auf einen anderen Knoten verschoben.

Failovercluster stellen darüber hinaus Funktionen für freigegebene Clustervolumes (Cluster Shared Volume, CSV) mit einem konsistenten verteilten Namespace bereit, mit dem Clusterrollen von allen Knoten aus auf den freigegebenen Speicher zugreifen können. Das Failoverclusteringfeature sorgt dafür, dass die Unterbrechung auf Benutzerseite nur minimal ist.

Für Failoverclustering gibt es viele praktische Anwendungsfälle, einschließlich:

- Hoch verfügbarer oder fortlaufend verfügbarer Dateifreigabespeicher für Anwendungen wie Microsoft SQL Server und Hyper-V-basierte virtuelle Computer
- Hoch verfügbare Clusterrollen, die auf physischen Servern oder virtuellen Computern ausgeführt werden, die auf Servern mit Hyper-V installiert sind

| GRUNDLEGENDE INFORMATIONEN | PLANUNG | BEREITSTELLUNG |
|---|---|---|
| Neues beim Failoverclustering | Planen der Hardwareanforderungen und Speicheroptionen für Failoverclustering | Erstellen eines Failoverclusters |
| Dateiserver mit horizontaler Skalierung für Anwendungsdaten | Verwenden von freigegebenen Clustervolumes (CSVs) | Bereitstellen eines Dateiservers mit zwei Knoten |
| Cluster- und Poolquorum | Verwenden von virtuellen Gastcomputerclustern mit direkten Speicherplätzen | Vorabbereitstellen von Clustercomputerobjekten in Active Directory Domain Services |
| Fehlerdomänenunterstützung | | Konfigurieren von Clusterkonten in Active Directory |
| Vereinfachte SMB Multichannel- und Multi-NIC-Clusternetzwerke | | Verwalten des Quorums und von Zeugen |
| VM-Lastenausgleich | | Bereitstellen eines Cloudzeugen |
| Clustergruppen | | Bereitstellen eines Dateifreigabezeugen |
| Clusteraffinität | | Paralleles Upgrade für Clusterbetriebssystem |

| GRUNDLEGENDE INFORMATIONEN | PLANUNG | BEREITSTELLUNG |
| --- | --- | --- |
| | | Upgrade eines Failoverclusters auf derselben Hardware |
| | | Bereitstellen eines von Active Directory getrennten Clusters |

| VERWALTEN | TOOLS UND EINSTELLUNGEN | COMMUNITYRESSOURCEN |
| --- | --- | --- |
| Clusterfähiges Aktualisieren | PowerShell-Cmdlets für Failoverclustering | Forum für hohe Verfügbarkeit (Clustering) |
| Integritätsdienst | PowerShell-Cmdlets für das clusterfähige Aktualisieren | Teamblog zu Failoverclustering und Netzwerklastenausgleich |
| Clusterdomänenmigration | | |
| Problembehandlung mit der Windows-Fehlerberichterstattung | | |

# What's new in Failover Clustering (Neues beim Failoverclustering)

13.06.2020 • 22 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

In diesem Thema werden die neuen und geänderten Funktionen in Failoverclustering für Windows Server 2019 und Windows Server 2016 erläutert.

## Neuerungen in Windows Server 2019

- **Clustergruppen**

  Cluster Gruppen ermöglichen es Ihnen, die Anzahl der Server in einer einzelnen SDDC-Lösung (Software-Defined Datacenter) über die aktuellen Grenzwerte eines Clusters hinaus zu erhöhen. Dies wird erreicht, indem mehrere Cluster zu einem Cluster Satz gruppiert werden: eine lose gekoppelte Gruppierung mehrerer Failovercluster: COMPUTE, Speicher und hyperkonvergiert. Mit Cluster Sätzen können Sie virtuelle Online Computer (Live Migration) zwischen Clustern innerhalb des Cluster Satzes verschieben.

  Weitere Informationen finden Sie unter Cluster Sets.

- **Azure erkennende Cluster**

  Failovercluster erkennen nun automatisch, wenn Sie auf virtuellen Azure-IaaS-Computern ausgeführt werden, und optimieren die Konfiguration, um ein proaktives Failover und die Protokollierung von geplanten Azure-Wartungs Ereignissen bereitzustellen, um die höchste Verfügbarkeit zu erreichen Die Bereitstellung wird auch vereinfacht, da der Load Balancer mit dem dynamischen Netzwerknamen für den Cluster Namen nicht konfiguriert werden muss.

- **Domänenübergreifende Clustermigration**

  Failovercluster können nun dynamisch von einer Active Directory Domäne zu einer anderen migrieren, sodass die Domänen Konsolidierung vereinfacht wird und Cluster von Hardwarepartnern erstellt und später der Kunden Domäne hinzugefügt werden können.

- **USB-Zeugen**

  Sie können jetzt ein einfaches USB-Laufwerk, das mit einem Netzwerk Switch verbunden ist, als Zeuge zum Ermitteln des Quorums für einen Cluster verwenden. Dadurch wird der Datei frei gaben Zeuge erweitert, um beliebige SMB2-kompatible Geräte zu unterstützen.

- **Verbesserungen der Clusterinfrastruktur**

  Der CSV-Cache ist jetzt standardmäßig aktiviert, um die Leistung virtueller Computer zu steigern. MSDTC unterstützt jetzt freigegebene Clustervolumes, um die Bereitstellung von MSDTC-Arbeits Auslastungen auf direkte Speicherplätze wie SQL Server zu ermöglichen. Erweiterte Logik zum Erkennen von partitionierten Knoten mit Selbstreparatur, um Knoten an die Cluster Mitgliedschaft zurückzugeben. Erweiterte Cluster Netzwerk Routen Erkennung und Selbstreparatur.

- **Clusterfähiges Aktualisieren unterstützt „Direkte Speicherplätze"**

  Das Cluster fähige aktualisieren (Cluster fähiges aktualisieren) ist jetzt integriert und berücksichtigt direkte Speicherplätze, die Überprüfung und Sicherstellung, dass die Neusynchronisierung der Daten auf jedem

Knoten abgeschlossen ist. Das Cluster fähige aktualisieren prüft Updates auf einen intelligenten Neustart, wenn dies erforderlich ist. Dies ermöglicht das orchestrieren von Neustarts aller Server im Cluster für eine geplante Wartung.

- **Verbesserungen für Dateifreigabezeugen**

  Wir haben die Verwendung eines Dateifreigabe Zeugen in den folgenden Szenarien aktiviert:

  - Fehlender oder sehr schlechter Internet Zugriff aufgrund eines Remote Standorts, der die Verwendung eines cloudzeugen verhindert.
  - Fehlende freigegebene Laufwerke für einen Datenträger Zeugen. Dabei kann es sich um eine direkte Speicherplätze hyperkonvergierte Konfiguration, eine SQL Server Always on Verfügbarkeits Gruppen (AG) oder eine * Exchange-Daten Bank Verfügbarkeits Gruppe (DAG) handeln, von denen keine freigegebene Datenträger verwendet.
  - Fehlende Domänen Controller Verbindung, weil der Cluster hinter einer DMZ liegt.
  - Eine Arbeitsgruppe oder ein Domänen übergreifender Cluster, für die kein Active Directory Cluster Namen Objekt (CNO) vorhanden ist. Weitere Informationen zu diesen Verbesserungen finden Sie im folgenden Beitrag in Server & Management-Blogs: Failovercluster-Dateifreigabe Zeuge und DFS.

    Außerdem wird die Verwendung einer DFS-Namespaces-Freigabe explizit als Speicherort blockiert. Das Hinzufügen eines Dateifreigabe Zeugen zu einer DFS-Freigabe kann zu Stabilitätsproblemen für Ihren Cluster führen, und diese Konfiguration wurde nie unterstützt. Wir haben Logik hinzugefügt, um zu erkennen, ob eine Freigabe DFS-Namespaces verwendet. Wenn DFS-Namespaces erkannt werden, blockiert Failovercluster-Manager die Erstellung des Zeugen und zeigt eine Fehlermeldung an, die nicht unterstützt wird.

- **Clusterhärtung**

  Die interne Cluster Kommunikation über SMB (Server Message Block) für freigegebene Clustervolumes und direkte Speicherplätze nutzt nun Zertifikate, um die sicherste Plattform bereitzustellen. Dadurch können Failovercluster ohne Abhängigkeiten von NTLM funktionieren und Sicherheitsbaselines aktivieren.

- **Failovercluster verwendet keine NTLM-Authentifizierung mehr**

  Failovercluster verwenden nicht mehr die NTLM-Authentifizierung. Stattdessen wird die Kerberos-Authentifizierung und die Zertifikat basierte Authentifizierung exklusiv verwendet. Für den Benutzer oder die Bereitstellungs Tools sind keine Änderungen erforderlich, um diese Sicherheits Erweiterung nutzen zu können. Außerdem können Failovercluster in Umgebungen bereitgestellt werden, in denen NTLM deaktiviert wurde.

# Neues in Windows Server 2016

**Paralleles Upgrade für Clusterbetriebssystem**

Das parallele Upgrade des Cluster Betriebssystems ermöglicht einem Administrator, das Betriebssystem der Cluster Knoten von Windows Server 2012 R2 auf eine neuere Version zu aktualisieren, ohne die Hyper-V-oder die Dateiserver mit horizontaler Skalierung Arbeits Auslastungen zu beenden. Mit diesem Feature können die Downtimesanktionen laut Vereinbarungen zum Servicelevel (Service Level Agreements, SLA) vermieden werden.

### Welchen Nutzen bietet diese Änderung?

Zum Aktualisieren eines Hyper-V-oder Dateiserver mit horizontaler Skalierung Clusters von Windows Server 2012 R2 auf Windows Server 2016 sind keine Ausfallzeiten mehr erforderlich. Der Cluster funktioniert weiterhin auf Windows Server 2012 R2-Ebene, bis auf allen Knoten im Cluster Windows Server 2016 ausgeführt wird. Die Cluster Funktionsebene wird mithilfe des Windows PowerShell-Cmdlet auf Windows Server 2016 aktualisiert `Update-ClusterFunctionalLevel` .

> **WARNING**
> - Nachdem Sie die Cluster Funktionsebene aktualisiert haben, können Sie nicht mehr zu einer Windows Server 2012 R2-Cluster Funktionsebene zurückkehren.
> - Bis zum `Update-ClusterFunctionalLevel` Ausführen des Cmdlets kann der Prozess rückgängig gemacht werden, und Windows Server 2012 R2-Knoten können hinzugefügt werden, und Windows Server 2016-Knoten können entfernt werden.

### Worin bestehen die Unterschiede?

Ein Hyper-V-oder Dateiserver mit horizontaler Skalierung-Failovercluster kann jetzt problemlos ohne Ausfallzeiten aktualisiert werden, oder es muss ein neuer Cluster mit Knoten erstellt werden, auf denen das Betriebssystem Windows Server 2016 ausgeführt wird. Beim Migrieren von Clustern zu Windows Server 2012 R2 wurde der vorhandene Cluster offline geschaltet, und das neue Betriebssystem wird für jeden Knoten neu installiert, und der Cluster wird wieder online geschaltet. Der alte Prozess war mühsam und erforderte Ausfallzeiten. In Windows Server 2016 muss der Cluster jedoch zu keinem Zeitpunkt offline geschaltet werden.

Die Cluster Betriebssysteme für das Upgrade in Phasen lauten wie folgt für jeden Knoten in einem Cluster:

- Der Knoten wird angehalten und auf allen virtuellen Computern, auf denen er ausgeführt wird, entladen.
- Die virtuellen Computer (oder eine andere Cluster Arbeitsauslastung) werden zu einem anderen Knoten im Cluster migriert.
- Das vorhandene Betriebssystem wird entfernt, und es wird eine Neuinstallation des Betriebssystems Windows Server 2016 auf dem Knoten ausgeführt.
- Der Knoten, auf dem das Betriebssystem Windows Server 2016 ausgeführt wird, wird wieder zum Cluster hinzugefügt.
- An diesem Punkt wird der Cluster als im gemischten Modus ausgeführt, da auf den Cluster Knoten entweder Windows Server 2012 R2 oder Windows Server 2016 ausgeführt wird.
- Die Cluster Funktionsebene bleibt bei Windows Server 2012 R2. Auf dieser Funktionsebene sind neue Features in Windows Server 2016, die sich auf die Kompatibilität mit früheren Versionen des Betriebssystems auswirken, nicht verfügbar.
- Schließlich werden alle Knoten auf Windows Server 2016 aktualisiert.
- Die Cluster Funktionsebene wird dann mithilfe des Windows PowerShell-Cmdlets in Windows Server 2016 geändert `Update-ClusterFunctionalLevel` . An diesem Punkt können Sie die Features von Windows Server 2016 nutzen.

Weitere Informationen finden Sie unter Cluster Operating System Rolling Upgrade.

### Speicher Replikat

Das Speicher Replikat ist ein neues Feature, das Speicher agnostische, synchrone Replikation auf Blockebene zwischen Servern oder Clustern für die Notfall Wiederherstellung sowie das Strecken eines Failoverclusters Zwischenstand Orten ermöglicht. Die synchrone Replikation ermöglicht die Spiegelung von Daten an physischen Standorten mit ausfallsicheren Volumes, um auf Dateisystemebene sicherzustellen, dass kein Datenverlust auftritt. Die asynchrone Replikation ermöglicht die Standorterweiterung über regionale Bereiche hinaus mit der Möglichkeit von Datenverlusten.

### Welchen Nutzen bietet diese Änderung?

Mithilfe des Speicher Replikats können Sie folgende Aufgaben ausführen:

- Bereitstellen einer Notfallwiederherstellungslösung von einem einzigen Anbieter für geplante und ungeplante Ausfälle unternehmenskritischer Workloads.
- Verwenden des SMB3-Transportprotokolls mit bewährter Zuverlässigkeit, Skalierbarkeit und Leistung.

- Strecken von Windows-Failoverclustern über regionale Bereiche hinweg.
- Verwenden Sie Microsoft-Software End-to-End für Speicherung und Clustering, wie z. b. Hyper-V, Speicher Replikat, Speicherplätze, Cluster, Dateiserver mit horizontaler Skalierung, SMB3, Datendeduplizierung und Refs/NTFS.
- Aufgrund der folgenden Merkmale können Sie die Kosten und die Komplexität senken:
  - Hardwareagnostisches System, das keine spezifische Speicherkonfiguration wie DAS oder SAN benötigt.
  - Möglichkeit, allgemeine Speicher- und Netzwerktechnologien zu nutzen.
  - Problemlose grafische Verwaltung für einzelne Knoten und Cluster über den Failovercluster-Manager.
  - Umfangreiche Skriptoptionen über Windows PowerShell.
- Weniger Downtime sowie höhere Zuverlässigkeit und Produktivität dank Windows.
- Unterstützbarkeit, Leistungsmetriken und Diagnosefunktionen.

Weitere Informationen finden Sie unter Speicherreplikate in Windows Server 2016.

**Cloudzeuge**

Der Cloudzeuge ist ein neuer Failovercluster-Quorumzeugen-Typ in Windows Server 2016, der Microsoft Azure als Vermittlungspunkt nutzt. Der Cloudzeuge erhält wie jeder andere Quorumzeuge ein Votum und kann an der Quorumberechnung teilnehmen. Sie können den Cloudzeugen als Quorumzeugen konfigurieren, indem Sie den Assistenten zum Konfigurieren eines Clusterquorums verwenden.

### Welchen Nutzen bietet diese Änderung?

Die Verwendung des cloudzeugen als Failovercluster-Quorum Zeugen bietet die folgenden Vorteile:

- Nutzt Microsoft Azure und entfällt, dass ein drittes separates Daten Center benötigt wird.
- Verwendet den standardmäßigen öffentlich verfügbaren Microsoft Azure BLOB Storage der den zusätzlichen Wartungsaufwand von virtuellen Computern, die in einem Public Cloud gehostet werden, entfällt.
- Dasselbe Microsoft Azure Storage Konto kann für mehrere Cluster verwendet werden (eine BLOB-Datei pro Cluster; eindeutige Cluster-ID, die als BLOB-Dateiname verwendet wird).
- Bietet sehr niedrige Kosten für das Speicherkonto (sehr kleine Daten, die pro BLOB-Datei geschrieben werden, BLOB-Dateien werden nur einmal aktualisiert, wenn sich der Status der Cluster Knoten ändert).

Weitere Informationen finden Sie unter Bereitstellen eines cloudzeugen für einen Failovercluster.

### Worin bestehen die Unterschiede?

Dies ist eine neue Funktion in Windows Server 2016.

**Resilienz virtueller Computer**

**Computeresilienz** Windows Server 2016 umfasst höhere computeresilienz von virtuellen Computern, um Probleme bei der Cluster Kommunikation in Ihrem Computecluster wie folgt zu reduzieren:

- **Resilienzoptionen, die für virtuelle Computer verfügbar sind:** Nun können Sie die resilienzoptionen für virtuelle Computer konfigurieren, die das Verhalten der virtuellen Computer während vorübergehender Fehler definieren:
  - **Resilienzstufe:** Unterstützt Sie beim Definieren der Behandlung vorübergehender Fehler.
  - **Resilienzzeitraum:** Hilft Ihnen bei der Definition, wie lange alle virtuellen Computer isoliert

ausgeführt werden dürfen.

- **Quarantäne fehlerhafter Knoten:** Fehlerhafte Knoten werden unter Quarantäne gestellt und sind nicht mehr berechtigt, dem Cluster beizutreten. Dadurch wird verhindert, dass Knoten in anderen Knoten und dem gesamten Cluster negativ beeinflusst werden.

Weitere Informationen finden Sie unter Compute resilienzworkflow und Knoten Quarantäne Einstellungen, mit denen gesteuert wird, wie der Knoten isoliert oder isoliert wird. Weitere Informationen finden Sie unter computeressourcen für virtuelle Computer in Windows Server 2016.

**Speicherresilienz** In Windows Server 2016 sind virtuelle Computer stabiler für vorübergehende Speicher Ausfälle. Durch die verbesserte Resilienz virtueller Computer werden die Sitzungs Zustände der Mandanten-virtuellen Computer im Falle einer Speicher Unterbrechung beibehalten. Dies wird durch eine intelligente und schnelle Reaktion von virtuellen Computern auf Probleme mit der Speicherinfrastruktur erreicht.

Wenn ein virtueller Computer die Verbindung mit dem zugrunde liegenden Speicher trennt, hält er an und wartet auf die Wiederherstellung des Speichers. Bei angehaltenen Computern behält der virtuelle Computer den Kontext der Anwendungen bei, die darin ausgeführt werden. Wenn die Verbindung des virtuellen Computers mit dem Speicher wieder hergestellt wird, wird der virtuelle Computer wieder in den Status "wird ausgeführt" zurückversetzt. Folglich wird der Sitzungs Status des Mandanten Computers bei der Wiederherstellung beibehalten.

In Windows Server 2016 ist die Resilienz von Speicher für virtuelle Computer für Gast Cluster auch bekannt und optimiert.

### Diagnose Verbesserungen bei Failoverclustering

Zum Diagnostizieren von Problemen mit Failoverclustern umfasst Windows Server 2016 Folgendes:

- Mehrere Verbesserungen an Cluster Protokolldateien (z. b. Zeitzoneninformationen und diagnosticverbose-Protokoll), die das Beheben von Problemen mit dem Failoverclustering vereinfachen. Weitere Informationen finden Sie unter Windows Server 2016-Failovercluster-Problembehandlung bei Verbesserungen-Cluster Protokoll.

- Ein neuer dumptyp des **aktiven Speicher Abbilds**, das die meisten Speicherseiten filtert, die virtuellen Maschinen zugeordnet sind. Dadurch wird der Speicher. dmp wesentlich kleiner und leichter zu speichern oder zu kopieren. Weitere Informationen finden Sie unter Verbesserungen bei der Problembehandlung für Windows Server 2016-Failovercluster-aktives Dump

### Standortabhängige Failovercluster

Windows Server 2016 umfasst standortabhängige Failovercluster, die Gruppenknoten in gestreckten Clustern basierend auf dem physischen Standort (Standort) aktivieren. Cluster Site-Awareness erweitert wichtige Vorgänge während des Cluster Lebenszyklus, z. b. Failoververhalten, Platzierungs Richtlinien, Takt zwischen den Knoten und Quorum Verhalten. Weitere Informationen finden Sie unter Site-Aware Failover Clusters in Windows Server 2016.

### Arbeitsgruppencluster und Cluster mit mehreren Domänen

In Windows Server 2012 R2 und früheren Versionen kann ein Cluster nur zwischen Mitglieds Knoten erstellt werden, die mit derselben Domäne verknüpft sind. Windows Server 2016 beseitigt diese Hindernisse und führt die Möglichkeit zum Erstellen eines Failoverclusters ohne Active Directory-Abhängigkeiten ein. Sie können jetzt in den folgenden Konfigurationen Failovercluster erstellen:

- **Einzel Domänen Cluster.** Cluster mit allen Knoten, die mit derselben Domäne verknüpft sind.

- **Cluster mit mehreren Domänen.** Cluster mit Knoten, die Mitglieder von unterschiedlichen Domänen sind.

- **Arbeitsgruppen Cluster.** Cluster mit Knoten, die Mitglied Server/Arbeitsgruppe sind (nicht mit der Domäne verknüpft).

Weitere Informationen finden Sie unter Arbeitsgruppe und Cluster mit mehreren Domänen in Windows Server 2016 .

### Lastenausgleich für virtuelle Computer

Der Lastenausgleich für virtuelle Computer ist ein neues Feature in Failoverclustering, das den nahtlosen Lastenausgleich virtueller Maschinen über die Knoten in einem Cluster hinweg ermöglicht. Über belegte Knoten werden basierend auf dem Arbeitsspeicher der virtuellen Maschine und der CPU-Auslastung auf dem Knoten identifiziert. Virtuelle Computer werden dann (Live migriert) von einem übergeordneten Knoten zu Knoten mit verfügbarer Bandbreite (falls zutreffend) verschoben. Die Aggressivität des Ausgleichs kann optimiert werden, um eine optimale Leistung und Auslastung des Clusters sicherzustellen. Der Lastenausgleich ist in Windows Server 2016 Technical Preview standardmäßig aktiviert. Der Lastenausgleich ist jedoch deaktiviert, wenn die dynamische SCVMM-Optimierung aktiviert ist.

### Start Reihenfolge der virtuellen Maschine

Die Start Reihenfolge des virtuellen Computers ist ein neues Feature in Failoverclustering, das die Orchestrierung starten für virtuelle Computer (und alle Gruppen) in einem Cluster einführt. Virtuelle Computer können nun in Ebenen gruppiert werden, und es können Start Auftrags Abhängigkeiten zwischen unterschiedlichen Ebenen erstellt werden. Dadurch wird sichergestellt, dass die wichtigsten virtuellen Computer (z. b. Domänen Controller oder virtuelle Computer des-Hilfsprogramms) zuerst gestartet werden. Virtuelle Computer werden erst gestartet, wenn die virtuellen Maschinen, von denen Sie abhängig sind, ebenfalls gestartet werden.

### Vereinfachte SMB Multichannel-und Multi-NIC-Cluster Netzwerke

Failoverclusternetzwerke sind nicht mehr auf eine einzelne NIC pro Subnetz/Netzwerk beschränkt. Bei vereinfachten SMB Multichannel-und Multi-NIC-Cluster Netzwerken erfolgt die Netzwerkkonfiguration automatisch, und jede NIC im Subnetz kann für Cluster-und workloaddatenverkehr verwendet werden. Diese Erweiterung ermöglicht es Kunden, den Netzwerk Durchsatz für Hyper-V, SQL Server-Failoverclusterinstanz und andere SMB-Arbeits Auslastungen zu maximieren.

Weitere Informationen finden Sie unter vereinfachte SMB Multichannel-und Multi-NIC-Cluster Netzwerke.

## Weitere Informationen

- Speicher
- Neuerungen beim Speicher in Windows Server 2016

# Übersicht über Dateiserver mit horizontaler Skalierung für Anwendungsdaten

09.04.2020 • 18 minutes to read • Edit Online

Gilt für: Windows Server 2012 R2, Windows Server 2012

Der Dateiserver mit horizontaler Skalierung soll Dateifreigaben mit horizontaler Skalierung bereitstellen, die fortlaufend als dateibasierter Serveranwendungsspeicher verfügbar sind. Dateifreigaben mit horizontaler Skalierung ermöglichen das Freigeben eines Ordners von mehreren Knoten des gleichen Clusters. Der Schwerpunkt dieses Szenarios ist die Planung und Bereitstellung eines Dateiservers mit horizontaler Skalierung.

Sie können mithilfe einer der folgenden Methoden einen gruppierten Dateiserver bereitstellen und konfigurieren:

- **Dateiserver mit horizontaler Skalierung für Anwendungsdaten** Diese Cluster Dateiserver-Funktion wurde in Windows Server 2012 eingeführt und ermöglicht das Speichern von Server Anwendungsdaten, wie z. b. Dateien virtueller Hyper-V-Computer, auf Dateifreigaben und das Erreichen eines ähnlichen Maß an Zuverlässigkeit, Verfügbarkeit, Verwaltbarkeit und hoher Leistung, das Sie von einer Storage Area Network erwarten. Alle Dateifreigaben sind auf allen Knoten gleichzeitig online. Die dieser Art von gruppiertem Dateiserver zugeordneten Dateifreigaben werden als Dateifreigaben mit horizontaler Skalierung bezeichnet. Dies wird mitunter als Aktiv/Aktiv bezeichnet. Dies ist der empfohlene Dateiservertyp beim Bereitstellen von entweder Hyper-V über Server Message Block (SMB) oder Microsoft SQL Server über SMB.
- **Dateiserver zur allgemeinen Verwendung** Dies ist die Weiterführung des gruppierten Dateiservers, der seit der Einführung des Failoverclusterings in Windows Server unterstützt wird. Diese Art von gruppiertem Dateiserver (und damit alle dem gruppierten Dateiserver zugeordneten Dateifreigaben) ist jeweils auf einem Knoten online. Dies wird mitunter als Aktiv/Passiv oder zweifach aktiv bezeichnet. Die dieser Art von gruppiertem Dateiserver zugeordneten Dateifreigaben werden als gruppierte Dateifreigaben bezeichnet. Dies ist der empfohlenen Dateiservertyp bei der Bereitstellung von Information-Worker-Szenarien.

## Beschreibung des Szenarios

Mithilfe von Dateifreigaben mit horizontaler Skalierung können Sie denselben Ordner auf mehreren Knoten eines Clusters freigeben. Wenn Sie beispielsweise über einen Dateiserver Cluster mit vier Knoten verfügen, der Server Message Block (SMB) für horizontales Skalieren verwendet, kann ein Computer, auf dem Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird, auf Dateifreigaben von einem der vier Knoten zugreifen. Dies wird mit neuen Windows Server-Features für das Failoverclustering und Funktionen des Windows-Dateiserverprotokolls SMB 3.0 erreicht. Dateiserveradministratoren können Dateifreigaben mit horizontaler Skalierung und fortlaufend verfügbare Dateidienste für Serveranwendungen bereitstellen und auf höheren Bedarf reagieren, indem sie schnell weitere Server online schalten. All dies ist in einer Produktionsumgebung möglich und erfolgt für die Serveranwendung vollständig transparent.

Zu den wichtigsten Vorteilen des Dateiservers mit horizontaler Skalierung gehören folgende:

- **Aktiv/aktiv-Datei**Freigaben. Alle Cluster Knoten können SMB-Client Anforderungen akzeptieren und verarbeiten. Da auf den Inhalt der Dateifreigaben über alle Clusterknoten gleichzeitig zugegriffen werden kann, ermöglichen Cluster und Clients mit SMB 3.0 gemeinsam transparentes Failover auf alternative Clusterknoten bei geplanten Wartungsarbeiten und bei nicht geplanten Fehlern mit Dienstunterbrechung.
- **Erhöhung der Bandbreite**. Die maximale Freigabe Bandbreite entspricht der Gesamtbandbreite aller Dateiserver-Cluster Knoten. Im Gegensatz zu vorherigen Versionen von Windows Server wird die Gesamtbandbreite nicht mehr durch die Bandbreite eines einzelnen Clusterknotens begrenzt, sondern durch

die Möglichkeiten des unterstützenden Speichersystems. Sie können die Gesamtbandbreite erhöhen, indem Sie Knoten hinzufügen.

- **Chkdsk ohne Ausfallzeiten**. CHKDSK wurde in Windows Server 2012 erheblich verbessert, um die Zeit zu verkürzen, die ein Dateisystem für die Reparatur offline ist. Mit den freigegebenen Clustervolumes (Clustered Shared Volumes, CSVs) wird dies noch weiter verbessert, da die Offlinephase ganz entfällt. In einem CSV-Dateisystem (CSVFS) kann CHKDSK verwendet werden, ohne dass sich Auswirkungen auf Anwendungen mit geöffneten Handles im Dateisystem ergeben.
- **Cache für freigegebenen Clustervolumes**. Csvs in Windows Server 2012 bietet Unterstützung für einen Lesecache, der die Leistung in bestimmten Szenarien erheblich verbessern kann, z. b. in einer virtuellen Desktop Infrastruktur (VDI).
- **Einfachere Verwaltung**. Mit Dateiserver mit horizontaler Skalierung erstellen Sie die Dateiserver mit horizontaler Skalierung und fügen dann die erforderlichen csvs und Dateifreigaben hinzu. Es ist nicht mehr notwendig, mehrere Clusterdateiserver jeweils mit separaten Clusterdatenträgern zu erstellen und dann Platzierungsrichtlinien zu entwickeln, um Aktivität auf den einzelnen Clusterknoten sicherzustellen.
- **Automatischer Ausgleich von Dateiserver mit horizontaler Skalierung Clients**. In Windows Server 2012 R2 verbessert die automatische Neuverteilung die Skalierbarkeit und Verwaltbarkeit von Dateiservern mit horizontaler Skalierung. SMB-Clientverbindungen werden nach Dateifreigabe (und nicht nach Server) nachverfolgt. Clients werden dann an den Clusterknoten mit dem besten Zugriff auf das von der Dateifreigabe verwendete Volume umgeleitet. Dadurch wird die Effizienz gesteigert, da der Umleitungsdatenverkehr zwischen Dateiserverknoten verringert wird. Clients werden nach der Anfangsverbindung und bei einer Neukonfiguration des Clusterspeichers umgeleitet.

## Inhalt dieses Szenarios

Die folgenden Themen bieten hilfreiche Informationen, um einen Dateiserver mit horizontaler Skalierung bereitzustellen:

- Planen der Dateiserver mit horizontaler Skalierung
  - Schritt 1: Planen des Speichers in Dateiserver mit horizontaler Skalierung
  - Schritt 2: Planen des Netzwerks in Dateiserver mit horizontaler Skalierung
- Dateiserver mit horizontaler Skalierung bereitstellen
  - Schritt 1: Installieren der erforderlichen Komponenten für Dateiserver mit horizontaler Skalierung
  - Schritt 2: Konfigurieren von Dateiserver mit horizontaler Skalierung
  - Schritt 3: Konfigurieren von Hyper-V für die Verwendung von Dateiserver mit horizontaler Skalierung
  - Schritt 4: Konfigurieren von Microsoft SQL Server für die Verwendung Dateiserver mit horizontaler Skalierung

## Anwendungsbereiche eines Dateiservers mit horizontaler Skalierung

Sie sollten einen Dateiserver mit horizontaler Skalierung nicht verwenden, wenn die Arbeitsauslastung eine hohe Anzahl von Metadatenvorgängen generiert, beispielsweise Öffnen von Dateien, Schließen von Dateien, Erstellen neuer Dateien oder Umbenennen vorhandener Dateien. Ein typischer Information-Worker generiert zahlreiche Metadatenvorgänge. Sie sollten einen Dateiserver mit horizontaler Skalierung verwenden, wenn die damit verbundene Skalierbarkeit und Einfachheit für Sie von Interesse ist und Sie nur Technologien benötigen, die von einem Dateiserver mit horizontaler Skalierung unterstützt werden.

In der folgenden Tabelle sind die neuen Funktionen in SMB 3.0, die gängigen Windows-Dateisysteme, Datenverwaltungstechnologien für Dateiserver und übliche Arbeitsauslastungen aufgeführt. Sie können sehen, ob die Technologie mit horizontaler Skalierung unterstützt wird oder ein herkömmlicher gruppierter Dateiserver (auch bekannt als ein Dateiserver zur allgemeinen Verwendung) erforderlich ist.

| TECHNOLOGIEBEREICH | FEATURE | DATEISERVERCLUSTER ZUR ALLGEMEINEN VERWENDUNG | DATEISERVER MIT HORIZONTALER SKALIERUNG |
|---|---|---|---|
| SMB | Fortlaufende Verfügbarkeit von SMB | Ja | Ja |
| SMB | SMB Multichannel | Ja | Ja |
| SMB | SMB Direct | Ja | Ja |
| SMB | SMB-Verschlüsselung | Ja | Ja |
| SMB | SMB – Transparentes Failover | Ja (wenn kontinuierliche Verfügbarkeit aktiviert ist) | Ja |
| Dateisystem | NTFS | Ja | N/V |
| Dateisystem | Robustes Datei System (Refs) | Empfohlen mit direkte Speicherplätze | Empfohlen mit direkte Speicherplätze |
| Dateisystem | Dateisystem des freigegebenen Clustervolumes (CSV) | N/V | Ja |
| Dateiverwaltung | BranchCache | Ja | Nein |
| Dateiverwaltung | Datendeduplizierung (WindowsServer 2012) | Ja | Nein |
| Dateiverwaltung | Datendeduplizierung (Windows Server 2012 R2) | Ja | Ja (nur VDI) |
| Dateiverwaltung | DFS-Namespace (DFSN) – Stammserverstamm | Ja | Nein |
| Dateiverwaltung | DFS-Namespace (DFSN) – Zielserver für Ordner | Ja | Ja |
| Dateiverwaltung | DFS-Replikation (DFSR) | Ja | Nein |
| Dateiverwaltung | Ressourcen-Manager für Dateiserver (Bildschirme und Kontingente) | Ja | Nein |
| Dateiverwaltung | Dateiklassifizierungsinfrastruktur | Ja | Nein |
| Dateiverwaltung | Dynamische Zugriffssteuerung (anspruchsbasierter Zugriff) | Ja | Nein |
| Dateiverwaltung | Ordnerumleitung | Ja | Nicht empfohlen |
| Dateiverwaltung | Offlinedateien (clientseitiges Zwischenspeichern) | Ja | Nicht empfohlen |

| TECHNOLOGIEBEREICH | FEATURE | DATEISERVERCLUSTER ZUR ALLGEMEINEN VERWENDUNG | DATEISERVER MIT HORIZONTALER SKALIERUNG |
|---|---|---|---|
| Dateiverwaltung | Roamingbenutzerprofile | Ja | Nicht empfohlen |
| Dateiverwaltung | Basisverzeichnisse | Ja | Nicht empfohlen |
| Dateiverwaltung | Arbeitsordner | Ja | Nein |
| NFS | NFS-Server | Ja | Nein |
| Anwendungen | Hyper-V | Nicht empfohlen | Ja |
| Anwendungen | Microsoft SQL Server | Nicht empfohlen | Ja |

* Ordner Umleitung, Offlinedateien, Roamingbenutzerprofilen oder Basis Verzeichnisse generieren eine große Anzahl von Schreibvorgängen, die sofort auf den Datenträger geschrieben werden müssen (ohne Pufferung), wenn fortlaufend verfügbare Dateifreigaben verwendet werden, um die Leistung im Vergleich zu allgemeinen Dateifreigaben zu verringern Fortlaufend verfügbare Dateifreigaben sind zudem nicht mit dem Ressourcen-Manager für Dateiserver und PCs unter Windows XP kompatibel. Darüber hinaus wird Offlinedateien möglicherweise 3-6 Minuten lang nicht in den Offline Modus versetzt, nachdem ein Benutzer den Zugriff auf eine Freigabe verloren hat, was Benutzer stören kann, die noch nicht den Modus "immer offline" von Offlinedateien verwenden.

## Praktische Anwendungsfälle

Dateiserver mit horizontaler Skalierung eignen sich ideal für die Speicherung von Serveranwendungen. Es folgen einige Beispiele für Serveranwendungen, die ihre Daten in einer Dateifreigabe mit horizontaler Skalierung speichern können:

- Der IIS-Webserver (Internetinformationsdienste) kann Konfigurationen und Daten für Websites in einer Dateifreigabe mit horizontaler Skalierung speichern. Weitere Informationen finden Sie unter Freigegebene Konfiguration.
- Hyper-V kann Konfigurationen und aktive virtuelle Datenträger in einer Dateifreigabe mit horizontaler Skalierung speichern. Weitere Informationen finden Sie unter Bereitstellen von Hyper-V über SMB.
- SQL Server kann aktive Datenbankdateien in einer Dateifreigabe mit horizontaler Skalierung speichern. Weitere Informationen finden Sie unter Installieren von SQL Server mit SMB-Dateifreigabe als Speicheroption.
- Virtual Machine Manager (VMM) kann eine Bibliotheksfreigabe (mit Vorlagen für virtuelle Computer und zugehörigen Dateien) in einer Dateifreigabe mit horizontaler Skalierung speichern. Der Bibliothek Server selbst kann jedoch kein Dateiserver mit horizontaler Skalierung sein – er muss sich auf einem eigenständigen Server oder einem Failovercluster befinden, der die Dateiserver mit horizontaler Skalierung Cluster Rolle nicht verwendet.

Wenn Sie eine Dateifreigabe mit horizontaler Skalierung als Bibliotheksfreigabe verwenden, können Sie nur Technologien nutzen, die mit dem Dateiserver mit horizontaler Skalierung kompatibel sind. Beispielsweise können Sie DFS-Replikation nicht verwenden, um eine Bibliotheks Freigabe zu replizieren, die auf einer Dateifreigabe mit horizontaler Skalierung gehostet wird. Es ist auch wichtig, dass für den Dateiserver mit horizontaler Skalierung die neuesten Softwareupdates installiert sind.

Zum Verwenden einer Dateifreigabe mit horizontaler Skalierung fügen Sie zunächst einen Bibliotheksserver (wahrscheinlich einen virtuellen Computer) mit einer lokalen Freigabe bzw. ohne Freigaben hinzu. Wenn Sie dann eine Bibliotheks Freigabe hinzufügen, wählen Sie eine Dateifreigabe aus, die auf einem Dateiserver mit horizontaler Skalierung gehostet wird. Diese Freigabe muss von VMM verwaltet werden und ausschließlich für die

Verwendung durch den Bibliotheksserver erstellt worden sein. Stellen Sie außerdem sicher, dass auf dem Dateiserver mit horizontaler Skalierung die neuesten Updates installiert werden. Weitere Informationen zum Hinzufügen von VMM-Bibliothek Servern und Bibliotheks Freigaben finden Sie unter Hinzufügen von Profilen zur VMM-Bibliothek. Eine Liste der derzeit verfügbaren Hotfixes für Datei- und Speicherdienste finden Sie im Microsoft Knowledge Base-Artikel 2899011.

> **NOTE**
> Einige Benutzer, wie z. B. Information-Worker, haben Arbeitsauslastungen, die eine größere Auswirkung auf die Leistung haben. Vorgänge wie das Öffnen und Schließen von Dateien, das Erstellen neuer Dateien und das Umbenennen vorhandener Dateien haben Auswirkungen auf die Leistung, wenn sie durch mehrere Benutzer erfolgen. Wenn eine Dateifreigabe mit fortlaufender Verfügbarkeit aktiviert ist, bietet diese Datenintegrität, wirkt sich aber auch auf die allgemeine Leistung aus. Die fortlaufende Verfügbarkeit erfordert das Schreiben von Daten auf den Datenträger, damit bei einem Ausfall eines Clusterknotens in einem Dateiserver mit horizontaler Skalierung die Integrität gewährleistet ist. Daher muss ein Benutzer, der mehrere große Dateien auf einen Dateiserver kopiert, in einer fortlaufend verfügbaren Dateifreigabe mit einer erheblich langsameren Leistung rechnen.

## In diesem Szenario enthaltene Features

In der folgenden Tabelle werden die Features dieses Szenarios und die Art der bereitgestellten Unterstützung aufgeführt.

| FEATURE | AUF WELCHE WEISE DIESES SZENARIO UNTERSTÜTZT WIRD |
| --- | --- |
| Failoverclustering | Failovercluster haben in Windows Server 2012 die folgenden Features hinzugefügt, um einen Datei Server mit horizontaler Skalierung zu unterstützen: Name des verteilten Netzwerks, der Dateiserver mit horizontaler Skalierung Ressourcentyp, freigegebene Clustervolumes (CSV) 2 und die Dateiserver mit horizontaler Skalierung hoch Verfügbarkeits Rolle. Weitere Informationen zu diesen Features finden Sie unter What'es New in Failover Clustering in Windows Server 2012 [umgeleitet]. |
| Server Message Block | SMB 3,0 hat die folgenden Features in Windows Server 2012 hinzugefügt, um einen Datei Server mit horizontaler Skalierung zu unterstützen: SMB transparent Failover, SMB Multichannel und SMB Direct.<br><br>Weitere Informationen zu neuen und geänderten Funktionen für SMB in Windows Server 2012 R2 finden 'Sie unter Neues in SMB unter Windows Server. |

## Weitere Informationen

- Leitfaden zu Entwurfs Überlegungen für Software definierte Speicher
- Erhöhen der Server-, Speicher-und Netzwerkverfügbarkeit
- Bereitstellen von Hyper-V über SMB
- Bereitstellen schneller und effizienter Dateiserver für Serveranwendungen
- To scale out or not to scale out, that is the question (Blogbeitrag)
- Ordnerumleitung, Offlinedateien und Roamingbenutzerprofile

# Grundlegendes zum Cluster- und Poolquorum

09.04.2020 • 23 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Windows Server-Failoverclustering bietet hohe Verfügbarkeit für Arbeits Auslastungen. Diese Ressourcen werden als hoch verfügbar angesehen, wenn die Knoten, die Ressourcen hosten, hoch verfügbar sind. der Cluster erfordert jedoch in der Regel mehr als die Hälfte der Knoten, die ausgeführt werden müssen. Dies wird als vorhanden sein eines *Quorums*bezeichnet.

Das Quorum ist so konzipiert, dass *Split-Brain*- Szenarien vermieden werden, die auftreten können, wenn eine Partition im Netzwerk vorhanden ist und Teilmengen von Knoten nicht miteinander kommunizieren können. Dies kann dazu führen, dass beide Teilmengen der Knoten den Besitzer der Arbeitsauslastung haben und auf den gleichen Datenträger schreiben, was zu zahlreichen Problemen führen kann. Dies wird jedoch durch das Quorum Konzept des Failoverclustering verhindert, das zwingt, dass nur eine dieser Knotengruppen weiter ausgeführt wird, sodass nur eine dieser Gruppen online bleibt.

Das Quorum bestimmt die Anzahl von Fehlern, die der Cluster unterstützen kann, während er weiterhin online bleibt. Das Quorum ist so konzipiert, dass es das Szenario behandelt, wenn ein Problem mit der Kommunikation zwischen Teilmengen von Cluster Knoten vorliegt, sodass mehrere Server nicht versuchen, gleichzeitig eine Ressourcengruppe zu hosten und gleichzeitig auf denselben Datenträger zu schreiben. Durch dieses Konzept des Quorums erzwingt der Cluster, dass der Cluster Dienst in einer der Teilmengen von Knoten angehalten wird, um sicherzustellen, dass nur ein echter Besitzer einer bestimmten Ressourcengruppe vorhanden ist. Wenn die wieder beendeten Knoten erneut mit der Haupt Knotengruppe kommunizieren können, treten Sie automatisch dem Cluster bei und starten Ihren Cluster Dienst.

In Windows Server 2019 und Windows Server 2016 gibt es zwei Komponenten des Systems, die über eigene Quorum Mechanismen verfügen:

- **Cluster Quorum**: Dies wird auf Cluster Ebene betrieben (d. h., Sie können Knoten verlieren, und der Cluster bleibt in Betrieb).
- **Pool Quorum**: Dies funktioniert auf Poolebene, wenn direkte Speicherplätze aktiviert ist (d. h., Sie können Knoten und Laufwerke verlieren und den Pool in Betrieb behalten). Speicherpools wurden so entworfen, dass Sie in gruppierten und nicht gruppierten Szenarien verwendet werden, weshalb Sie über einen anderen Quorum Mechanismus verfügen.

## Übersicht über Cluster Quorum

Die folgende Tabelle enthält eine Übersicht über die Cluster Quorum Ergebnisse pro Szenario:

| SERVER KNOTEN | KANN EINEN SERVER KNOTEN FEHLER ÜBERSTEHEN. | KANN EINEN SERVER KNOTEN FEHLER ÜBERSTEHEN, EIN WEITERER | KANN ZWEI GLEICHZEITIGE SERVER KNOTEN AUSFÄLLE ÜBERSTEHEN |
|---|---|---|---|
| 2 | 50/50 | Nein | Nein |
| 2 + Zeuge | Ja | Nein | Nein |
| 3 | Ja | 50/50 | Nein |

| SERVER KNOTEN | KANN EINEN SERVER KNOTEN FEHLER ÜBERSTEHEN. | KANN EINEN SERVER KNOTEN FEHLER ÜBERSTEHEN, EIN WEITERER | KANN ZWEI GLEICHZEITIGE SERVER KNOTEN AUSFÄLLE ÜBERSTEHEN |
|---|---|---|---|
| 3 + Zeuge | Ja | Ja | Nein |
| 4 | Ja | Ja | 50/50 |
| 4 + Zeuge | Ja | Ja | Ja |
| 5 und höher | Ja | Ja | Ja |

**Cluster Quorum Empfehlungen**

- Wenn Sie über zwei Knoten verfügen, ist ein Zeuge **erforderlich**.
- Wenn Sie über drei oder vier Knoten verfügen, wird Zeuge **dringend empfohlen**.
- Wenn Sie über Internet Zugang verfügen, verwenden Sie einen **cloudzeugen** .
- Wenn Sie sich in einer IT-Umgebung mit anderen Computern und Dateifreigaben befinden, verwenden Sie einen Dateifreigabe Zeugen.

# Funktionsweise des Cluster Quorums

Wenn Knoten ausfallen oder eine Teilmenge der Knoten den Kontakt mit einer anderen Teilmenge verliert, müssen die übergeordneten Knoten sicherstellen, dass Sie den *Großteil* des Clusters darstellen, der Online bleibt. Wenn Sie dies nicht überprüfen können, werden Sie offline geschaltet.

Das Konzept der *Mehrheit* funktioniert jedoch nur ordnungsgemäß, wenn die Gesamtzahl der Knoten im Cluster ungerade ist (z. b. drei Knoten in einem Cluster mit fünf Knoten). Was ist also mit Clustern mit einer geraden Anzahl von Knoten (z. a. einem Cluster mit vier Knoten)?

Es gibt zwei Möglichkeiten, wie der Cluster die *Gesamtzahl der Stimmen* ungerade machen kann:

1. Zuerst können *Sie einen Zeugen* mit einer zusätzlichen Stimme hinzufügen. Hierfür ist ein Benutzer Setup erforderlich.
2. Oder Sie können einen Schritt *nach unten* durchlaufen, indem Sie die Stimme eines nicht glücklichen Knotens NULLS (erfolgt bei Bedarf automatisch).

Wenn die Überprüfung erfolgreich ist, ob die Knoten die *Mehrheit*sind, wird die Definition der *Mehrheit* so aktualisiert, dass Sie nur zu den übergeordneten Knoten gehört. Dadurch kann der Cluster einen Knoten verlieren, dann einen anderen Knoten usw. Dieses Konzept der *Gesamtzahl der Stimmen* , die sich nach aufeinander folgenden Fehlern anpasst, wird als ***dynamisches Quorum***bezeichnet.

**Dynamischer Zeuge**

Der dynamische Zeuge schaltet die Stimme des Zeugen um, um sicherzustellen, dass die *Gesamtzahl der Stimmen* ungerade ist. Wenn eine ungerade Anzahl von Stimmen vorliegt, hat der Zeuge keine Stimme. Wenn eine gerade Anzahl von Stimmen vorliegt, hat der Zeuge eine Stimme. Der dynamische Zeuge verringert das Risiko, dass der Cluster aufgrund eines Zeugen Fehlers ausfällt. Der Cluster entscheidet, ob die Zeugen Abstimmung basierend auf der Anzahl der Abstimmungs Knoten, die im Cluster verfügbar sind, verwendet werden soll.

Dynamisches Quorum funktioniert mit dynamischem Zeuge wie unten beschrieben.

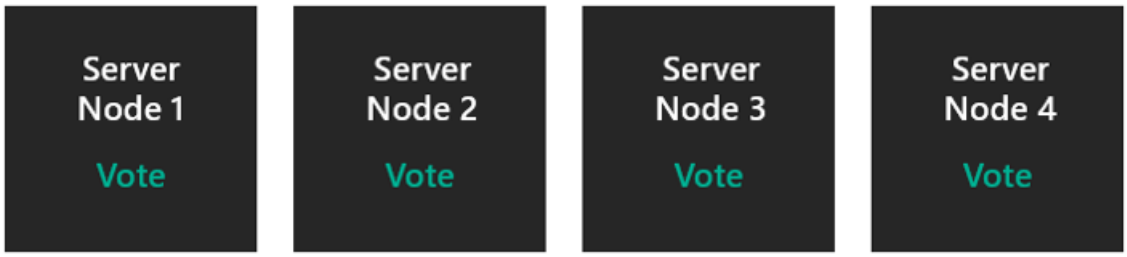
**Dynamisches Quorum Verhalten**

- Wenn Sie über eine **gerade** Anzahl von Knoten und keinen Zeugen verfügen, *erhält ein Knoten seine Stimme als nullt*. Beispielsweise erhalten nur drei der vier Knoten Stimmen, sodass die *Gesamtzahl der Stimmen* drei beträgt und zwei übergeordnete Knoten mit Stimmen als Mehrheit angesehen werden.

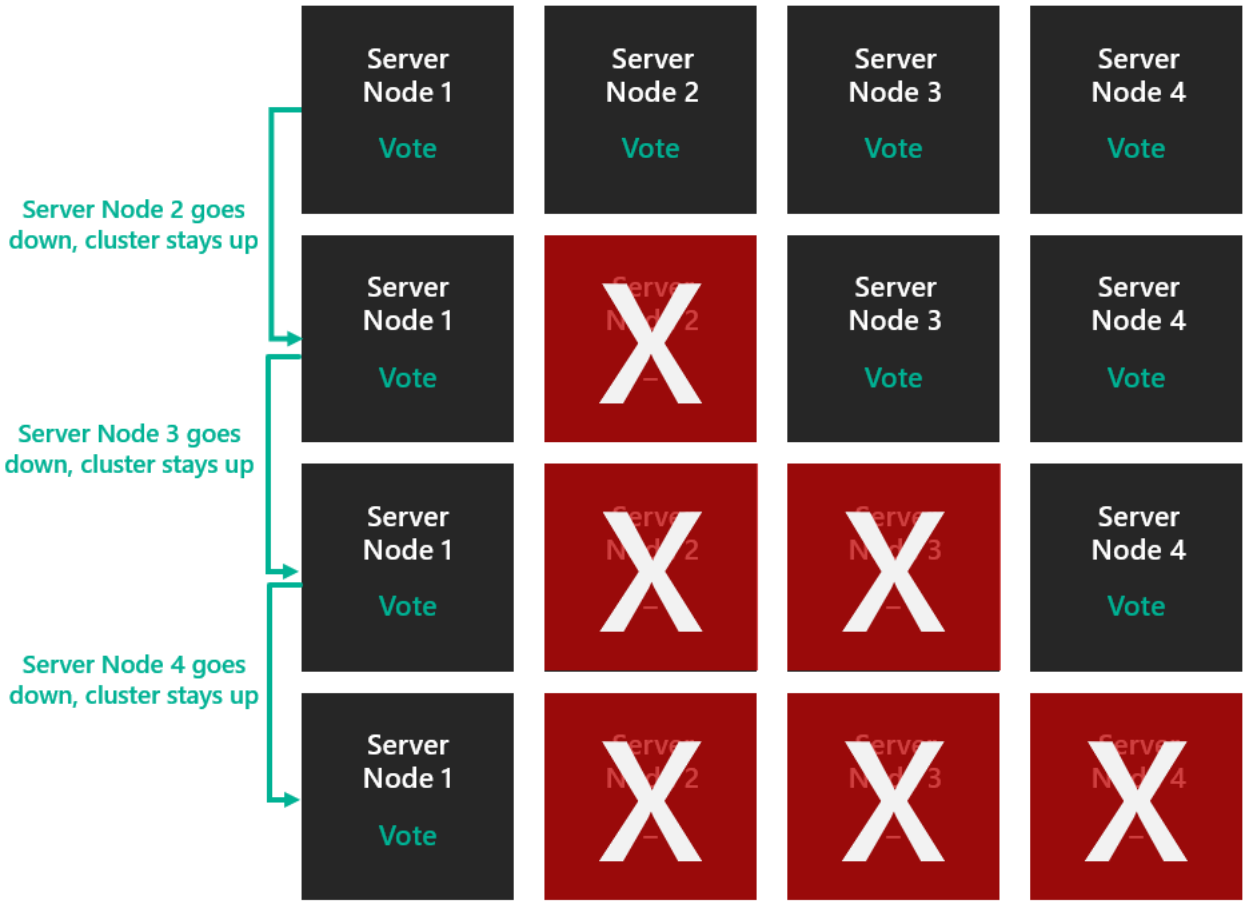
- Wenn Sie über eine **ungerade** Anzahl von Knoten und keinen Zeugen verfügen, *erhalten alle Stimmen*.
- Wenn Sie über eine **gerade** Anzahl von Knoten Plus Witness verfügen, *Stimmen der Zeuge*ab, sodass die Summe ungerade ist.
- Wenn Sie über eine **ungerade** Anzahl von Knoten Plus Witness verfügen, *stimmt der Zeuge nicht*.

Mithilfe des dynamischen Quorums kann einem Knoten eine Stimme dynamisch zugewiesen werden, um zu vermeiden, dass die Mehrheit der Stimmen verloren geht und der Cluster mit einem Knoten ausgeführt werden kann (auch als letzter als letzter bekannt). Nehmen wir als Beispiel einen Cluster mit vier Knoten. Angenommen, das Quorum erfordert 3 Stimmen.

In diesem Fall wäre der Cluster ausgefallen, wenn Sie zwei Knoten verloren haben.




Das dynamische Quorum verhindert jedoch, dass dies geschieht. Die *Gesamtanzahl der Stimmen* , die für das Quorum erforderlich sind, wird jetzt basierend auf der Anzahl der verfügbaren Knoten bestimmt. Mit dynamischem Quorum bleibt der Cluster auch dann in der Hand, wenn Sie drei Knoten verlieren.

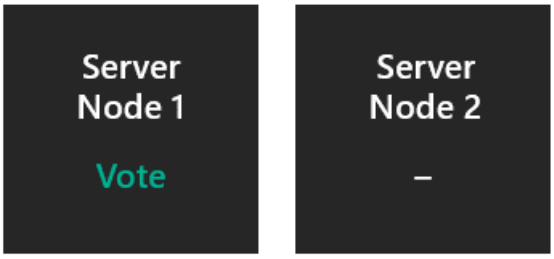



Das obige Szenario gilt für einen allgemeinen Cluster, für den direkte Speicherplätze nicht aktiviert ist. Wenn direkte Speicherplätze aktiviert ist, kann der Cluster jedoch nur zwei Knoten Ausfälle unterstützen. Dies wird im Abschnitt Pool Quorumausführlicher erläutert.

### Beispiele

**Zwei Knoten ohne Zeugen.**

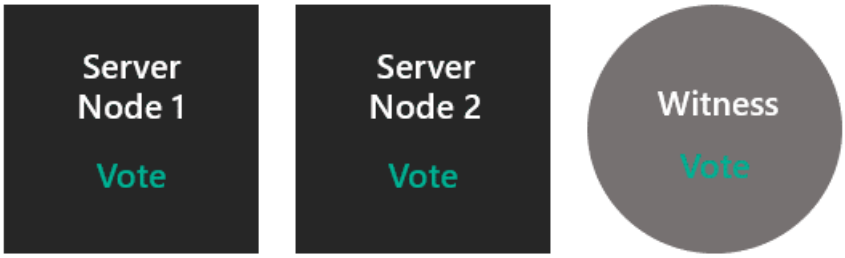
Die Stimme eines Knotens wird auf NULL gesetzt, sodass die *Mehrheit* der Stimme von insgesamt **1 Stimme**bestimmt wird. Wenn der Knoten ohne Abstimmung unerwartet ausfällt, verfügt der Survivor über 1/1, und der Cluster wird noch nicht angezeigt. Wenn der Abstimmungs Knoten unerwartet ausfällt, verfügt der Survivor über 0/1, und der Cluster wird herunterfährt. Wenn der Abstimmungs Knoten ordnungsgemäß heruntergefahren wird, wird die Stimme an den anderen Knoten übertragen, und der Cluster wird nicht mehr angezeigt. ***Aus diesem Grund ist es wichtig, einen Zeugen zu konfigurieren.***




- Kann einen Server Fehler überstehen: **50-prozentige Chance**.
- Kann einen Server Fehler überstehen, dann ein weiterer: **Nein**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Nein**.

**Zwei Knoten mit einem Zeugen.**

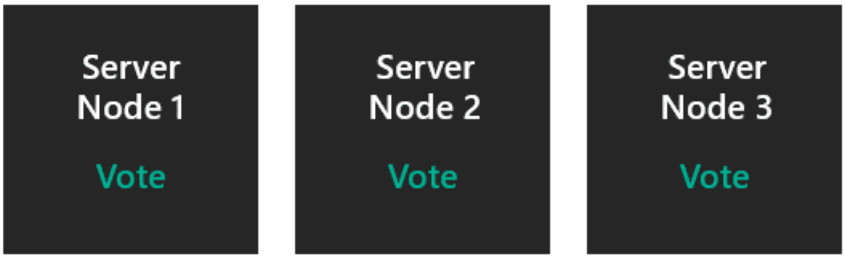
Beide Knoten Stimmen zusammen mit den Zeugen Stimmen, sodass die *Mehrzahl* aus insgesamt **3 Stimmen**ergibt. Wenn ein Knoten ausfällt, verfügt der Survivor über 2/3, und der Cluster wird noch nicht angezeigt.




- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann ein weiterer: **Nein**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Nein**.

**Drei Knoten ohne Zeugen.**

Alle Knoten Stimmen ab, sodass die *Mehrheit* von insgesamt **3 Stimmen**bestimmt wird. Wenn ein Knoten ausfällt, sind die Überlebenden 2/3, und der Cluster wird nicht mehr vorhanden sein. Der Cluster wird zu zwei Knoten ohne Zeugen – zu diesem Zeitpunkt befinden Sie sich in Szenario 1.

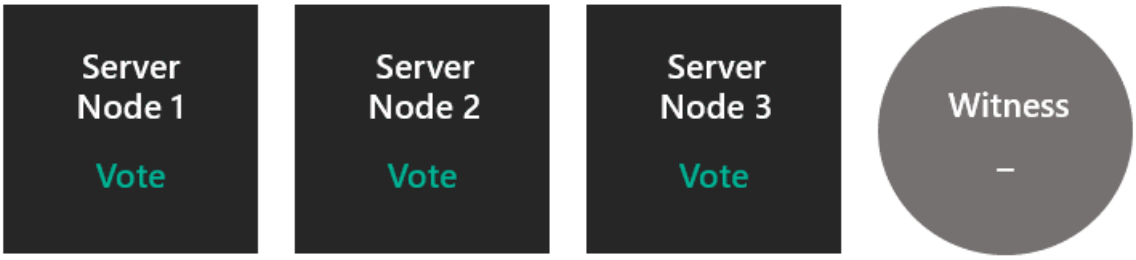



- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann ein weiterer Wert: **50 Prozent**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Nein**.

**Drei Knoten mit einem Zeugen.**

Alle Knoten Stimmen ab, sodass der Zeuge nicht anfänglich stimmt. Die *Mehrheit* wird aus insgesamt **3**

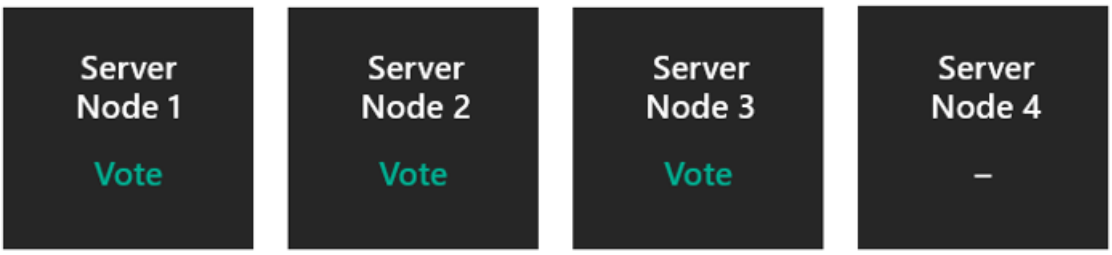
**Stimmen**ermittelt. Nach einem Fehler verfügt der Cluster über zwei Knoten mit einem Zeugen – der wieder zu Szenario 2 gehört. Nun stimmen die beiden Knoten und der Zeuge ab.




- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann einen weiteren: **Ja**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Nein**.

**Vier Knoten ohne Zeugen**

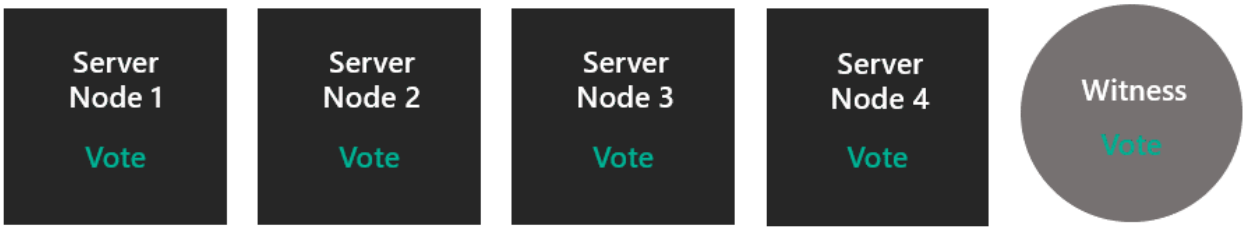
Die Stimme eines Knotens wird als nulloverwert festgelegt, sodass die *Mehrheit* aus insgesamt **3 Stimmen**ergibt. Nach einem Fehler wird der Cluster zu drei Knoten, und Sie sind in Szenario 3.




- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann einen weiteren: **Ja**.
- Kann zwei Serverausfälle gleichzeitig überstehen: **50 Prozent der Chance**.

**Vier Knoten mit einem Zeugen.**

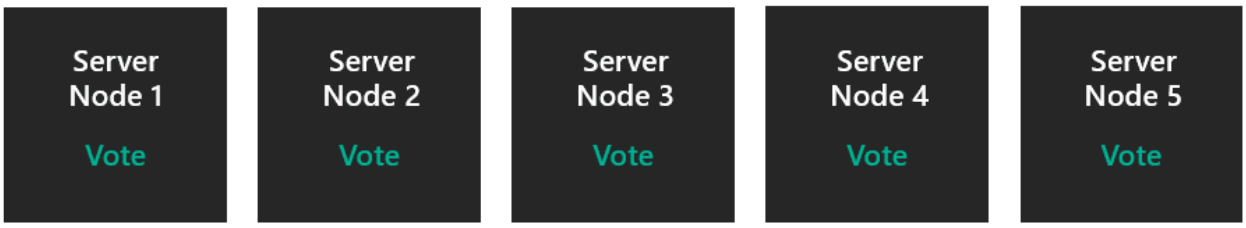
Alle Knoten Stimmen und der Zeuge Stimmen ab, sodass die *Mehrheit* von insgesamt **5 Stimmen**bestimmt wird. Nach einem Fehler sind Sie in Szenario 4. Nach zwei gleichzeitigen Fehlern überspringen Sie das Szenario 2.




- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann einen weiteren: **Ja**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Ja**.

**Fünf Knoten und darüber hinaus.**

Alle Knoten Stimmen oder nur eine Stimme ab, je nachdem, was das Gesamtergebnis ist. Direkte Speicherplätze können nicht mehr als zwei Knoten gleich sehen. an diesem Punkt ist daher kein Zeuge erforderlich oder nützlich.



- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann einen weiteren: **Ja**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Ja**.

Nachdem wir nun wissen, wie das Quorum funktioniert, betrachten wir die Typen von Quorum Zeugen.

**Quorum Zeugen Typen**

Failoverclustering unterstützt drei Arten von Quorum Zeugen:

- **Cloud Witness** : BLOB Storage in Azure, auf den alle Knoten des Clusters zugreifen. Sie verwaltet Clustering-Informationen in einer Datei "Witness. log", speichert jedoch keine Kopie der Cluster Datenbank.
- **Datei** frei gaben Zeuge – eine SMB-Dateifreigabe, die auf einem Dateiserver konfiguriert ist, auf dem Windows Server ausgeführt wird. Sie verwaltet Clustering-Informationen in einer Datei "Witness. log", speichert jedoch keine Kopie der Cluster Datenbank.
- Datenträger **Zeuge** : ein kleiner gruppierter Datenträger, der sich in der verfügbaren Speicher Gruppe des Clusters befindet. Dieser Datenträger ist hoch verfügbar und kann ein Failover zwischen Knoten durch finden. Sie enthält eine Kopie der Cluster Datenbank. ***Ein Datenträger Zeuge wird von direkte Speicherplätze nicht unterstützt***.

# Übersicht über das Pool Quorum

Wir haben soeben über das Cluster Quorum gesprochen, das auf Cluster Ebene funktioniert. Sehen wir uns nun das Pool Quorum an, das auf Poolebene funktioniert (d. h. Sie können Knoten und Laufwerke verlieren und den Pool in Betrieb nehmen). Speicherpools wurden so entworfen, dass Sie in gruppierten und nicht gruppierten Szenarien verwendet werden, weshalb Sie über einen anderen Quorum Mechanismus verfügen.

Die folgende Tabelle enthält eine Übersicht über die Ergebnisse des Pool Quorums pro Szenario:

| SERVER KNOTEN | KANN EINEN SERVER KNOTEN FEHLER ÜBERSTEHEN. | KANN EINEN SERVER KNOTEN FEHLER ÜBERSTEHEN, EIN WEITERER | KANN ZWEI GLEICHZEITIGE SERVER KNOTEN AUSFÄLLE ÜBERSTEHEN |
|---|---|---|---|
| 2 | Nein | Nein | Nein |
| 2 + Zeuge | Ja | Nein | Nein |
| 3 | Ja | Nein | Nein |
| 3 + Zeuge | Ja | Nein | Nein |
| 4 | Ja | Nein | Nein |
| 4 + Zeuge | Ja | Ja | Ja |
| 5 und höher | Ja | Ja | Ja |

# Funktionsweise des Pool Quorums

Wenn Laufwerke fehlschlagen oder eine Teilmenge der Laufwerke den Kontakt mit einer anderen Teilmenge verliert, müssen die überprüfenden Laufwerke sicherstellen, dass Sie den *Großteil* des Pools als online bleiben. Wenn Sie dies nicht überprüfen können, werden Sie offline geschaltet. Der Pool ist die Entität, die offline geschaltet wird oder online bleibt, je nachdem, ob Sie über genügend Datenträger für das Quorum verfügt (50% + 1). Der Besitzer der Pool Ressource (aktiver Cluster Knoten) kann + 1 sein.

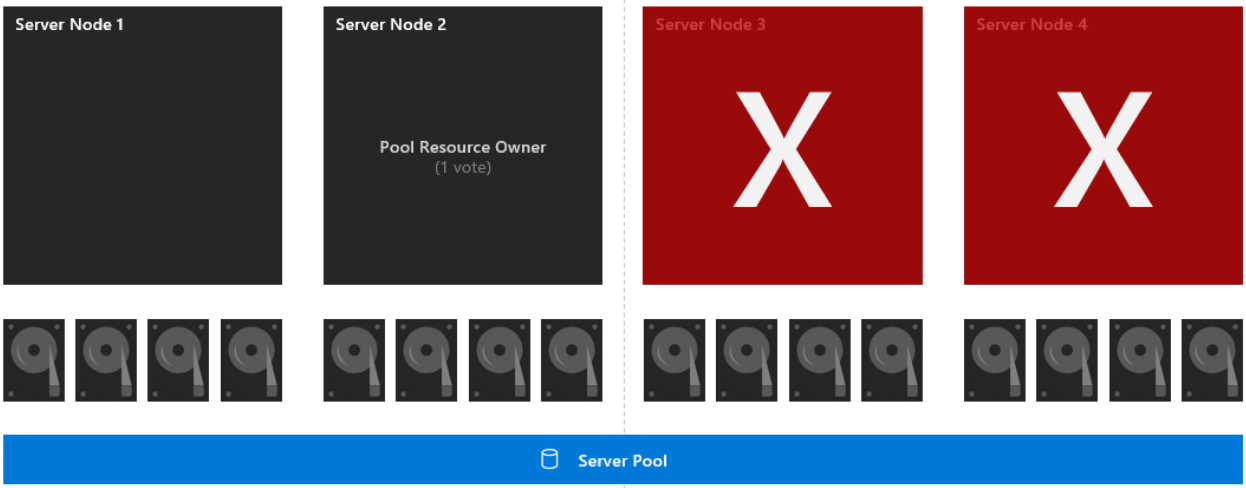
Das Pool Quorum funktioniert jedoch auf folgende Weise anders als das Cluster Quorum:

- der Pool verwendet einen Knoten im Cluster als Zeuge, um die Hälfte der Laufwerke zu überstehen (dieser Knoten ist der Besitzer der Pool Ressource).
- der Pool weist kein dynamisches Quorum auf.
- der Pool implementiert nicht seine eigene Version zum Entfernen einer Stimme.

### Beispiele

**Vier Knoten mit einem symmetrischen Layout.**

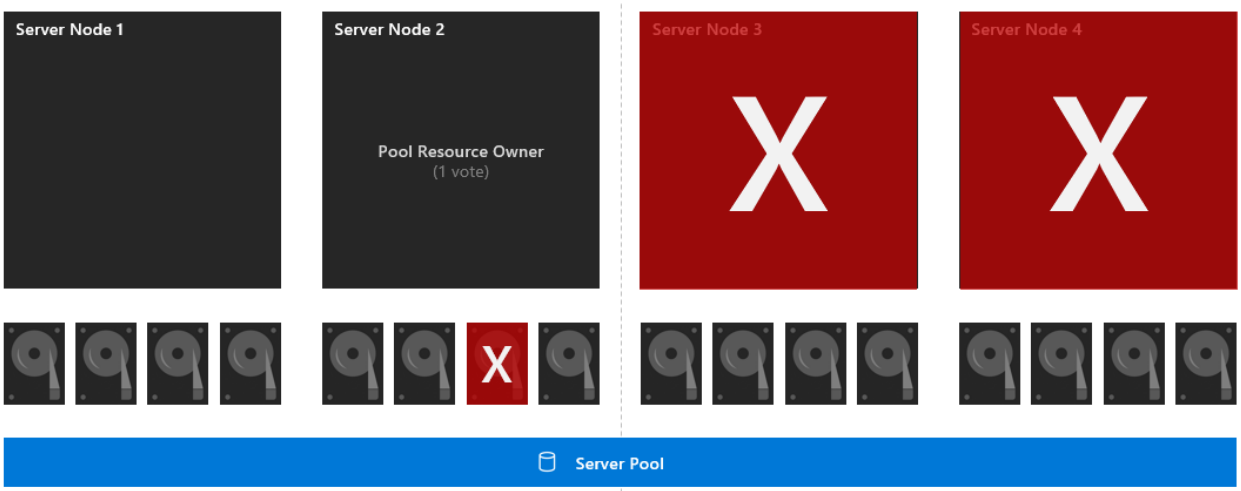
Jedes der 16 Laufwerke verfügt über eine Stimme, und Knoten zwei hat ebenfalls eine Stimme (da es sich um den Pool Ressourcen Besitzer handelt). Die *Mehrheit* wird von insgesamt **16 Stimmen** bestimmt. Wenn die Knoten drei und vier ausfallen, verfügt die verbleibende Teilmenge über 8 Laufwerke und den Pool Ressourcen Besitzer (9/16 Stimmen). Der Pool wird also nicht mehr angezeigt.




- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann einen weiteren: **Ja**.
- Kann zwei Server Fehler gleichzeitig überstehen: **Ja**.

**Vier Knoten mit einem symmetrischen Layout und Laufwerk Fehler.**

Alle 16 Laufwerke haben eine Stimme, und Knoten 2 verfügt auch über eine Stimme (da es sich um den Besitzer der Pool Ressource handelt). Die *Mehrheit* wird von insgesamt **16 Stimmen** bestimmt. Zuerst wird Laufwerk 7 heruntergefahren. Wenn die Knoten drei und vier ausfallen, verfügt die verbleibende Teilmenge über 7 Laufwerke und den Pool Ressourcen Besitzer (8/16 Stimmen). Der Pool hat also keine Mehrheit und ist nicht mehr vorhanden.

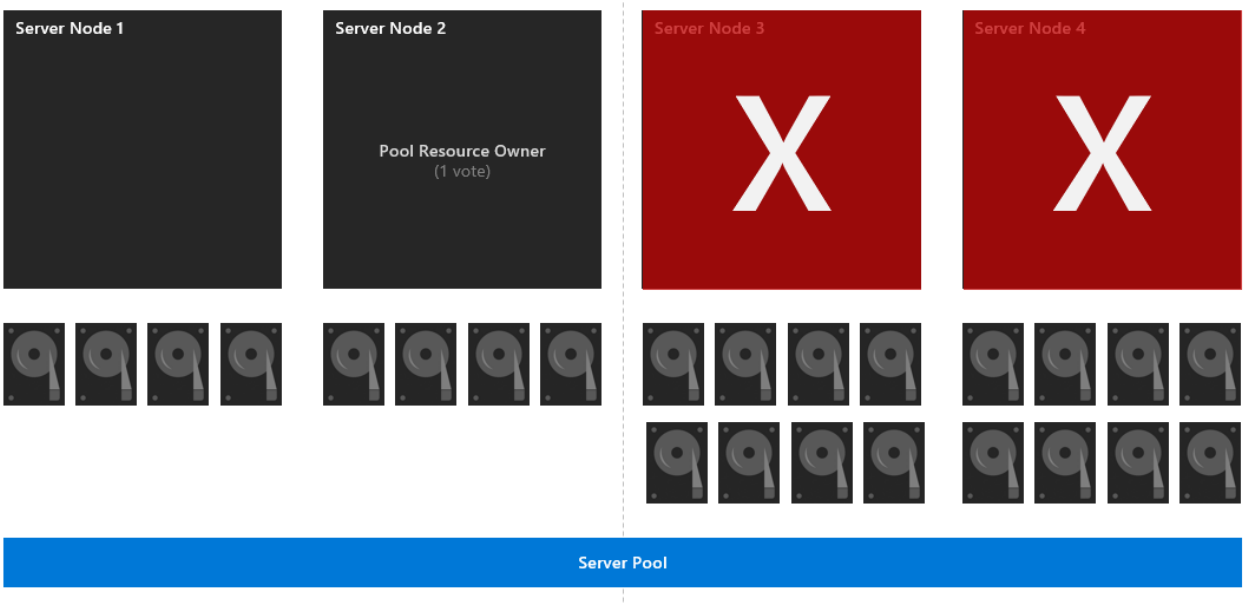



- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, dann ein weiterer: **Nein**.

- Kann zwei Server Fehler gleichzeitig überstehen: **Nein**.

**Vier Knoten mit einem nicht symmetrischen Layout.**

Jedes der 24 Laufwerke verfügt über eine Stimme, und Knoten zwei hat ebenfalls eine Stimme (da es sich um den Pool Ressourcen Besitzer handelt). Die *Mehrheit* wird von insgesamt **24 Stimmen** bestimmt. Wenn die Knoten drei und vier ausfallen, verfügt die verbleibende Teilmenge über 8 Laufwerke und den Pool Ressourcen Besitzer (9/24 Stimmen). Der Pool hat also keine Mehrheit und ist nicht mehr vorhanden.




- Kann einen Server Fehler überstehen: **Ja**.
- Kann einen Server Fehler überstehen, ein anderes: * * hängt von * * ab (kann nicht überleben, wenn beide Knoten drei und vier ausfallen, aber alle anderen Szenarien überstehen können.
- Kann zwei Server Fehler gleichzeitig überstehen: * * hängt von * * ab (kann nicht überleben, wenn beide Knoten drei und vier ausfallen, aber alle anderen Szenarien überstehen können.

**Empfehlungen für Pool Quorum**

- Stellen Sie sicher, dass jeder Knoten im Cluster symmetrisch ist (jeder Knoten verfügt über die gleiche Anzahl von Laufwerken).
- Aktivieren Sie drei-Wege-Spiegelung oder duale Parität, damit Sie Knoten Ausfälle tolerieren und die virtuellen Datenträger online halten können. Weitere Informationen finden Sie auf unserer Seite mit den Volumen Anleitungen .
- Wenn mehr als zwei Knoten heruntergefahren sind oder zwei Knoten und ein Datenträger auf einem anderen Knoten ausfällt, haben die Volumes möglicherweise keinen Zugriff auf alle drei Kopien Ihrer Daten und werden deshalb offline geschaltet und sind nicht verfügbar. Es wird empfohlen, die Server wieder zu nutzen oder die Datenträger schnell zu ersetzen, um die höchste Resilienz für alle Daten auf dem Volume sicherzustellen.

## Weitere Informationen

- Konfigurieren und Verwalten des Quorums
- Bereitstellen eines Cloudzeugen

# Fehlerdomänenunterstützung

09.04.2020 • 13 minutes to read • Edit Online

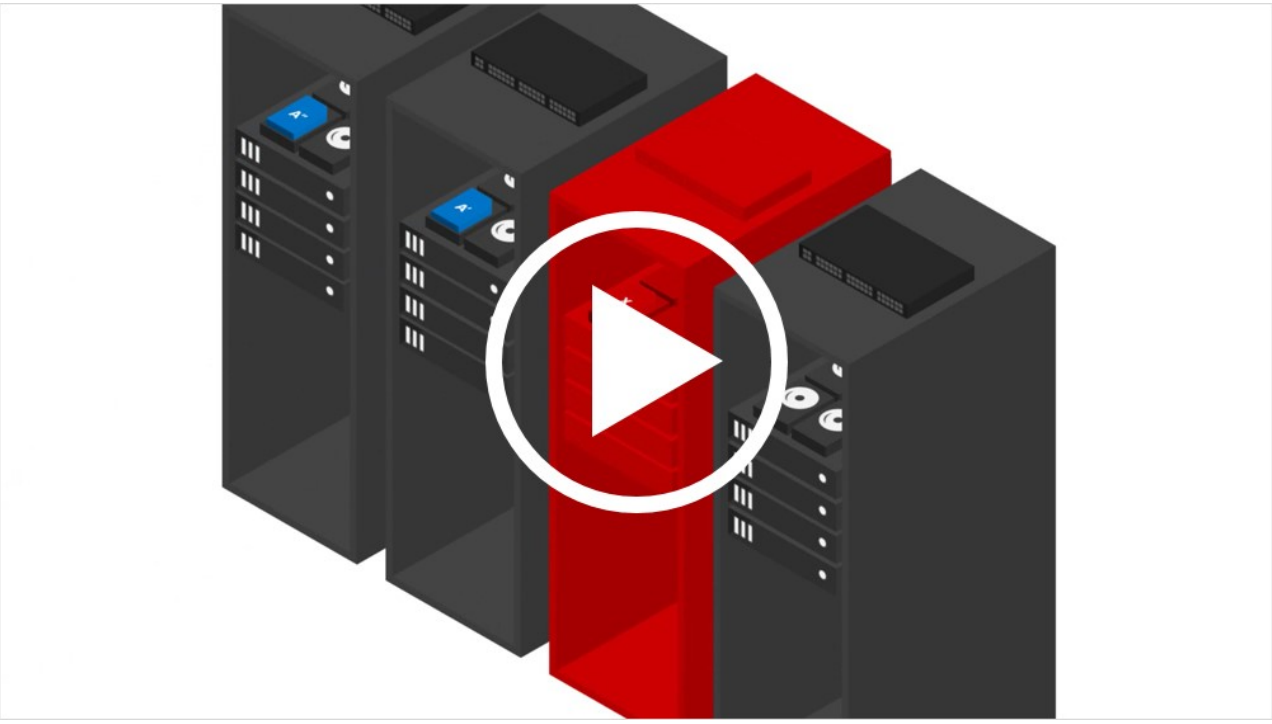
Gilt für: Windows Server 2019 und Windows Server 2016

Failoverclustering ermöglicht die Zusammenarbeit mehrerer Server, um hohe Verfügbarkeit zu bieten – oder anders ausgedrückt, um Knotenfehlertoleranz zu bieten. Die heutigen Unternehmen verlangen jedoch eine immer höhere Verfügbarkeit Ihrer Infrastruktur. Um cloudähnliche Betriebszeit zu erreichen, ist auch der Schutz bei sehr unwahrscheinlichen Vorfällen wie z.B. Gehäuse- und Rackausfällen oder Naturkatastrophen erforderlich. Aus diesem Grund haben Failoverclustering in Windows Server 2016 auch Gehäuse-, Rack-und Site Fehlertoleranz eingeführt.

## Fehlerdomänenunterstützung

Fehlerdomänen und Fehlertoleranz sind eng miteinander verwandte Konzepte. Eine Fehlerdomäne ist eine Reihe von Hardwarekomponenten, die einen gemeinsamen Single Point of Failure haben. Um ein bestimmtes Niveau an Fehlertoleranz zu erzielen, benötigen Sie mehrere Fehlerdomänen auf dieser Ebene. Beispielsweise setzt Rackfehlertoleranz voraus, dass Ihre Server und Daten auf mehrere Racks verteilt sind.

Dieses kurze Video bietet eine Übersicht über Fehler Domänen in Windows Server 2016:



**Fehler Domänen Bewusstsein in Windows Server 2019**

Fehler Domänen Bewusstsein ist in Windows Server 2019 verfügbar, aber standardmäßig deaktiviert und muss über die Windows-Registrierung aktiviert werden.

Um das Fehler Domänen Bewusstsein in Windows Server 2019 zu aktivieren, wechseln Sie zur Windows-Registrierung, und legen Sie (Get-Cluster) fest. Autozuzustandsite-Registrierungsschlüssel auf 1.

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

Um das Fehler Domänen Bewusstsein in Windows 2019 zu deaktivieren, navigieren Sie zur Windows-

Registrierung, und legen Sie (Get-Cluster) fest. Autozuzustandsite-Registrierungsschlüssel auf 0 (null).

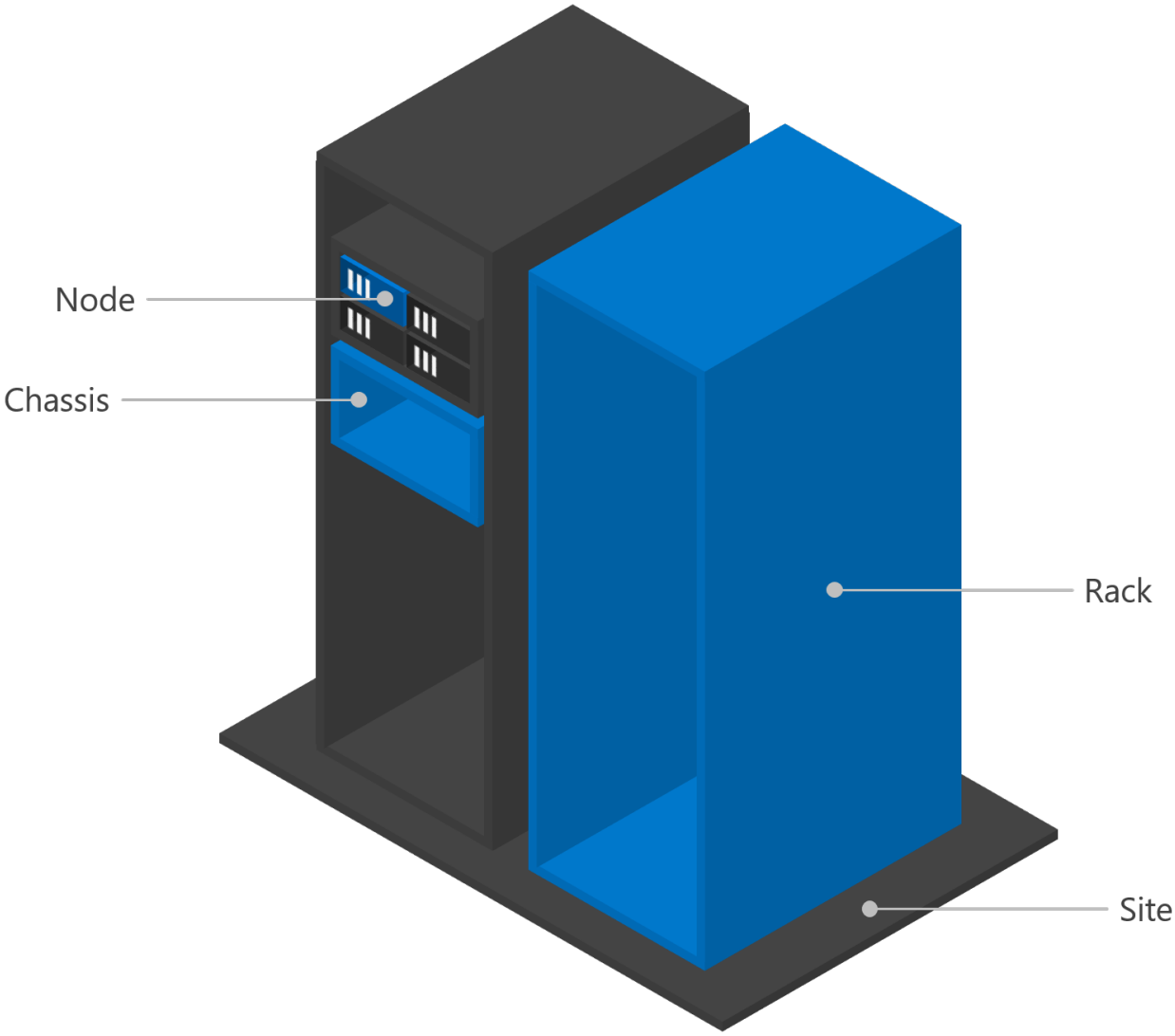
```
(Get-Cluster).AutoAssignNodeSite=0
```

## Vorteile

- **Speicherplätze, einschließlich direkte Speicherplätze, verwenden Fehler Domänen, um die Datensicherheit zu maximieren.**
  Die Resilienz in „Speicherplätze" ist konzeptionell wie verteiltes, softwaredefiniertes RAID. Mehrere Kopien aller Daten werden synchron beibehalten, und wenn bei einem Hardwareausfall eine Kopie verloren geht, werden andere zum Wiederherstellen der Resilienz erneut kopiert. Um die bestmögliche Resilienz zu erreichen, sollten Kopien in separaten Fehlerdomänen beibehalten werden.
- **Der Integritätsdienst verwendet Fehler Domänen, um hilfreichere Warnungen bereitzustellen.**
  Jeder Fehlerdomäne können Speicherortmetadaten zugeordnet werden, die automatisch in alle nachfolgenden Warnungen aufgenommen werden. Diese Deskriptoren können Vorgänge oder Wartungspersonal unterstützen und Fehler reduzieren, indem sie Hardware eindeutig machen.
- **Stretch Clustering verwendet Fehler Domänen für die Speicher Affinität.** Stretch-Clustering ermöglicht weit entfernten Servern, einem gemeinsamen Cluster beitreten. Für optimale Leistung sollten Anwendungen oder virtuelle Computer auf Servern ausgeführt werden, die sich in der Nähe derer befinden, die ihnen Speicherplatz bereitstellen. Fehler Domänen Bewusstsein ermöglicht diese Speicher Affinität.

## Ebenen der Fehlerdomänen

Es gibt vier kanonische Ebenen von Fehlerdomänen – Standort, Rack, Gehäuse und Knoten. Knoten werden automatisch erkannt; jede zusätzliche Ebene ist optional. Wenn Ihre Bereitstellung beispielsweise keine Blade Server enthält, ist die Gehäuseebene für Sie wahrscheinlich nicht sinnvoll.




## Verwendung

Sie können PowerShell oder XML-Markup zum Angeben von Fehler Domänen verwenden. Beide Ansätze sind äquivalent und bieten vollständige Funktionalität.

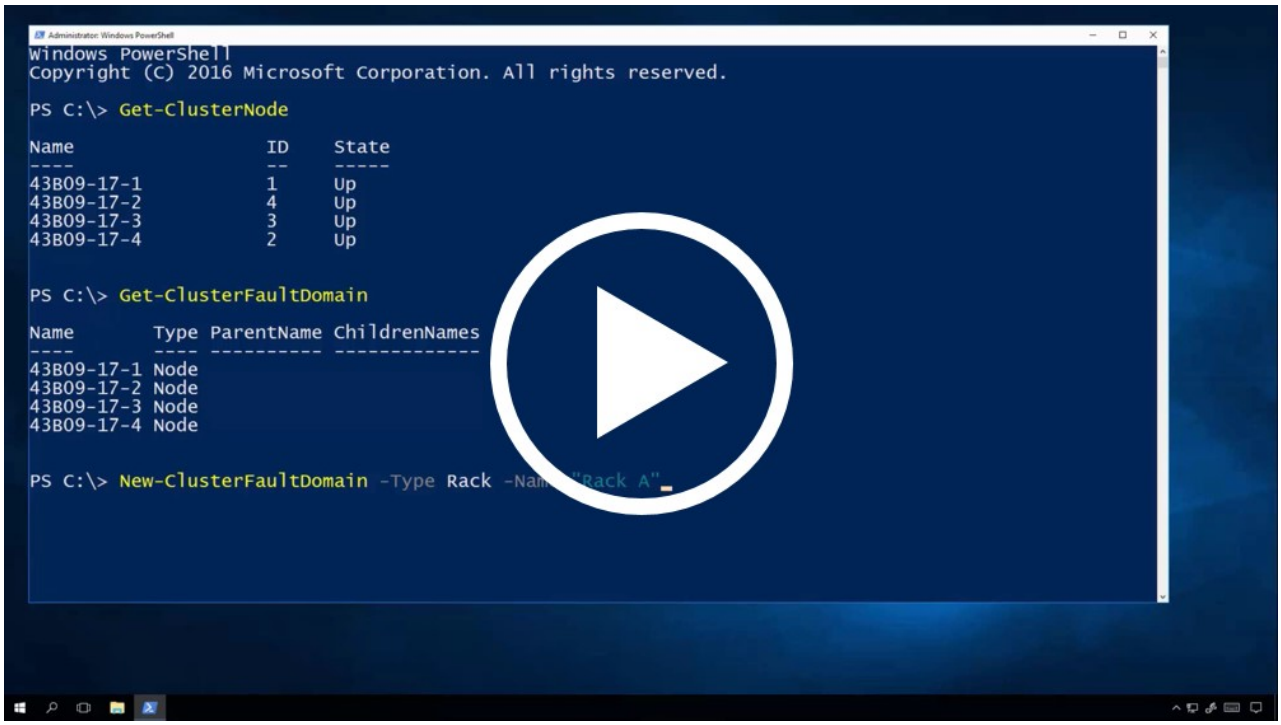
> **IMPORTANT**
>
> Geben Sie Fehlerdomänen wenn möglich an, bevor Sie „Direkte Speicherplätze" aktivieren. Dies ermöglicht die Vorbereitung von Pool, Ebenen und Einstellungen wie Resilienz und Anzahl der Spalten für Gehäuse- oder Rackfehlertoleranz durch automatische Konfiguration. Wenn Pool und Volumes erstellt sind, werden Daten nicht nachträglich in Reaktion auf Änderungen der Fehlerdomänentopologie verschoben. Um nach dem Aktivieren von „Direkte Speicherplätze" Knoten zwischen Gehäusen oder Racks zu verschieben, sollten Sie zuerst den Knoten sowie seine Laufwerke mit `Remove-ClusterNode -CleanUpDisks` aus dem Pool entfernen.

### Definieren von Fehler Domänen mit PowerShell

Windows Server 2016 führt die folgenden Cmdlets ein, um mit Fehler Domänen zu arbeiten:

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

Dieses kurze Video veranschaulicht die Verwendung dieser Cmdlets.




Verwenden Sie `Get-ClusterFaultDomain`, um die aktuelle Fehler Domänen Topologie anzuzeigen. Dadurch werden alle Knoten im Cluster sowie alle Gehäuse, Racks oder Standorte aufgelistet, die Sie erstellt haben. Sie können mit Parametern wie **-Type** oder **-Name** filtern, aber diese sind nicht erforderlich.

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

Verwenden Sie `New-ClusterFaultDomain`, um neue Chassis, Racks oder Standorte zu erstellen. Die Parameter "`-Type`" und "`-Name`" sind erforderlich. Die möglichen Werte für `-Type` sind `Chassis`, `Rack` und `Site`. Der `-Name` kann eine beliebige Zeichenfolge sein. (Bei `Node`-Typfehler Domänen muss der Name der tatsächliche Knoten Name sein, wie er automatisch festgelegt wird.)

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

> **IMPORTANT**
> Windows Server kann nicht sicherstellen, dass Fehler Domänen, die Sie erstellen, in der realen, physischen Welt übereinstimmen. (Dies mag offensichtlich klingen, aber es ist wichtig zu verstehen.) Wenn sich die Knoten in der physischen Welt alle in einem Rack befinden, wird durch das Erstellen von zwei `-Type Rack` Fehler Domänen in der Software nicht in der Praxis eine Gestell-Fehlertoleranz bereitgestellt. Sie sind dafür verantwortlich, sicherzustellen, dass die Topologie, die Sie mithilfe dieser Cmdlets erstellen, der tatsächlichen Anordnung der Hardware entspricht.

Verwenden Sie `Set-ClusterFaultDomain`, um eine Fehler Domäne in eine andere zu verschieben. Die Begriffe „übergeordnet" und „untergeordnet" werden häufig zur Beschreibung dieser geschachtelten Beziehung verwendet. Die Parameter "`-Name`" und "`-Parent`" sind erforderlich. Geben Sie in `-Name` den Namen der Fehler Domäne an, die verschoben wird. Geben Sie in `-Parent` den Namen des Ziels an. Um mehrere Fehlerdomänen gleichzeitig zu verschieben, listen Sie ihre Namen auf.

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

> **IMPORTANT**
> Bei der Verschiebung von Fehlerdomänen werden ihre untergeordneten Objekte mit ihnen verschoben. Wenn Rack A im obigen Beispiel server01.contoso.com übergeordnet ist, muss letztere nicht separat an den Standort Shanghai verschoben werden – sie ist schon durch das übergeordnete Element dort, wie in der realen Welt.

Die Beziehungen zwischen übergeordneten und untergeordneten Elementen können in der Ausgabe von `Get-ClusterFaultDomain` in den Spalten `ParentName` und `ChildrenNames` angezeigt werden.

Sie können auch `Set-ClusterFaultDomain` verwenden, um bestimmte andere Eigenschaften von Fehler Domänen zu ändern. Beispielsweise können Sie optionale `-Location` oder `-Description` Metadaten für jede Fehler Domäne bereitstellen. Wenn angegeben, werden diese Informationen in Hardwarewarnungen des Integritätsdiensts einbezogen. Sie können Fehler Domänen auch mit dem `-NewName` -Parameter umbenennen. Benennen Sie `Node` typfehlerdomänen nicht um.

```
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"
```

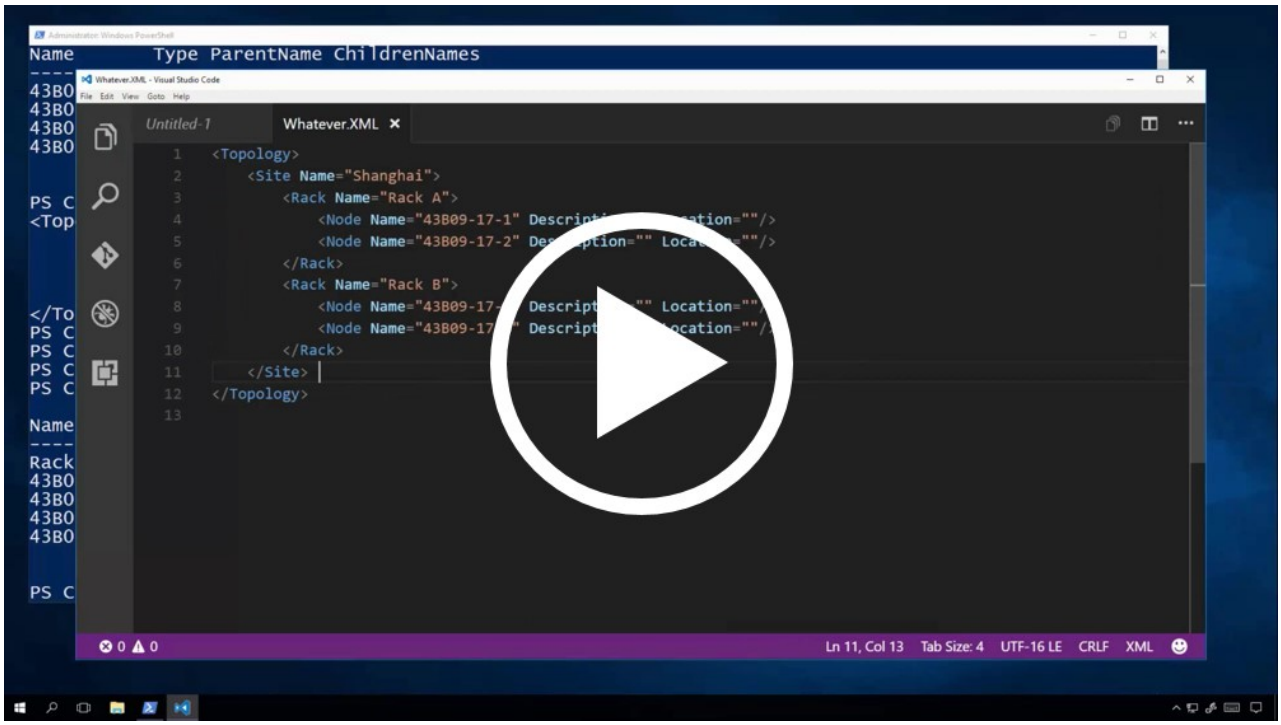
Verwenden Sie `Remove-ClusterFaultDomain`, um Chassis, Racks oder Standorte zu entfernen, die Sie erstellt haben. Der `-Name` -Parameter ist erforderlich. Eine Fehler Domäne, die untergeordnete Elemente enthält, kann nicht entfernt werden – entfernen Sie zunächst die untergeordneten Elemente, oder verschieben Sie Sie außerhalb der `Set-ClusterFaultDomain`. Wenn Sie eine Fehler Domäne außerhalb aller anderen Fehler Domänen verschieben möchten, legen Sie Ihre `-Parent` auf die leere Zeichenfolge ("") fest. Fehler Domänen von `Node` Typen können nicht entfernt werden. Um mehrere Fehlerdomänen gleichzeitig zu entfernen, listen Sie ihre Namen auf.

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

### Definieren von Fehlerdomänen mit XML-Markup

Fehlerdomänen können mithilfe einer XML-Syntax angegeben werden. Sie sollten Ihren bevorzugten Texteditor verwenden, z.B. Visual Studio Code ( *hier* kostenlos erhältlich) oder Editor, um ein XML-Dokument zu erstellen, das Sie speichern und wiederverwenden können.

Dieses kurze Video veranschaulicht die Verwendung von XML-Markup zur Angabe von Fehlerdomänen.




Führen Sie in PowerShell das folgende Cmdlet aus: `Get-ClusterFaultDomainXML`. Dadurch wird die aktuelle Fehlerdomänenspezifikation für den Cluster im XML-Format zurückgegeben. Dies spiegelt alle ermittelten `<Node>` wider, die beim Öffnen und schließen `<Topology>` Tags umschlossen sind.

Führen Sie Folgendes aus, um diese Ausgabe in einer Datei zu speichern.

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

Öffnen Sie die Datei, und fügen Sie `<Site>`, `<Rack>` und `<Chassis>` Tags hinzu, um anzugeben, wie diese Knoten Zwischenstand Orten, Racks und Chassis verteilt werden. Jedes Tag muss durch einen eindeutigen **Name** identifiziert werden. Für Knoten müssen Sie den Knotennamen als standardmäßig aufgefüllt beibehalten.

> **IMPORTANT**
>
> Während alle zusätzlichen Tags optional sind, muss die transitive Hierarchie Standort > Rack > Gehäuse > Knoten beibehalten und ordnungsgemäß geschlossen werden.
> Neben Name können auch Freiform- `Location="..."` und `Description="..."` Deskriptoren jedem Tag hinzugefügt werden.

**Beispiel: zwei Standorte, jeweils ein Rack**

```
<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>
```

**Beispiel: zwei Gehäuse, Blade Server**

```
<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>
```

Wenn Sie die neue Fehler Domänen Spezifikation festlegen möchten, speichern Sie Ihre XML-Datei, und führen Sie Folgendes in PowerShell aus.

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

Dieses Handbuch enthält nur zwei Beispiele, aber die `<Site>`-, `<Rack>`-, `<Chassis>`-und `<Node>`-Tags können gemischt und mit vielen zusätzlichen Möglichkeiten abgeglichen werden, um die physische Topologie Ihrer Bereitstellung widerzuspiegeln. Wir hoffen, dass diese Beispiele die Flexibilität dieser Tags und den Wert der Freiformpositionsdeskriptoren zu ihrer Unterscheidung veranschaulichen.

### Optional: Speicherort und Beschreibungs Metadaten

Sie können optionale **Speicherort** -oder **Beschreibungs** Metadaten für jede Fehler Domäne angeben. Wenn angegeben, werden diese Informationen in Hardwarewarnungen des Integritätsdiensts einbezogen. In diesem kurzen Video wird der Wert für das Hinzufügen solcher Deskriptoren veranschaulicht.

## Weitere Informationen

- Erste Schritte mit Windows Server 2019
- Beginnen Sie mit Windows Server 2016
- Übersicht über direkte Speicherplätze

# Vereinfachte SMB Multichannel- und Multi-NIC-Clusternetzwerke

02.12.2019 • 7 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Vereinfachtes SMB Multichannel und Multi-Nisches Cluster Netzwerke sind ein Feature, das die Verwendung mehrerer NICs im gleichen clusternetzwerksubnetz ermöglicht und SMB Multichannel automatisch aktiviert.

Vereinfachte SMB Multichannel-und Multi-NIC-Cluster Netzwerke bieten folgende Vorteile:

- Failoverclustering erkennt automatisch alle NICs auf Knoten, die denselben Switch/dasselbe Subnetz verwenden. es ist keine zusätzliche Konfiguration erforderlich.
- SMB Multichannel wird automatisch aktiviert.
- Netzwerke, die nur über IPv6-Verbindungs lokale (FE80) IP-Adress Ressourcen verfügen, werden in reinen Cluster Netzwerken (private Netzwerke) erkannt.
- Standardmäßig wird für jeden Netzwerknamen (Cap) des Cluster Zugriffs Punkts eine einzelne IP-Adress Ressource konfiguriert.
- Die Cluster Überprüfung gibt keine Warnmeldungen mehr aus, wenn mehrere NICs im selben Subnetz gefunden werden.

## Anforderungen

- Mehrere NICs pro Server mit demselben Switch/Subnetz.

## Nutzen von multinic-Cluster Netzwerken und vereinfachtem SMB Multichannel

In diesem Abschnitt wird beschrieben, wie Sie die neuen multinic-Cluster Netzwerke und die vereinfachten SMB Multichannel-Features nutzen können.

**Verwenden von mindestens zwei Netzwerken für Failoverclustering**

Obwohl es selten vorkommt, können Netzwerk Switches fehlschlagen. es wird immer noch empfohlen, mindestens zwei Netzwerke für das Failoverclustering zu verwenden. Alle gefundenen Netzwerke werden für Cluster Takte verwendet. Vermeiden Sie die Verwendung eines einzelnen Netzwerks für den Failovercluster, um eine Single Point of Failure zu vermeiden. Im Idealfall sollten mehrere physische Kommunikations Pfade zwischen den Knoten im Cluster und keine Single Point of Failure vorhanden sein.

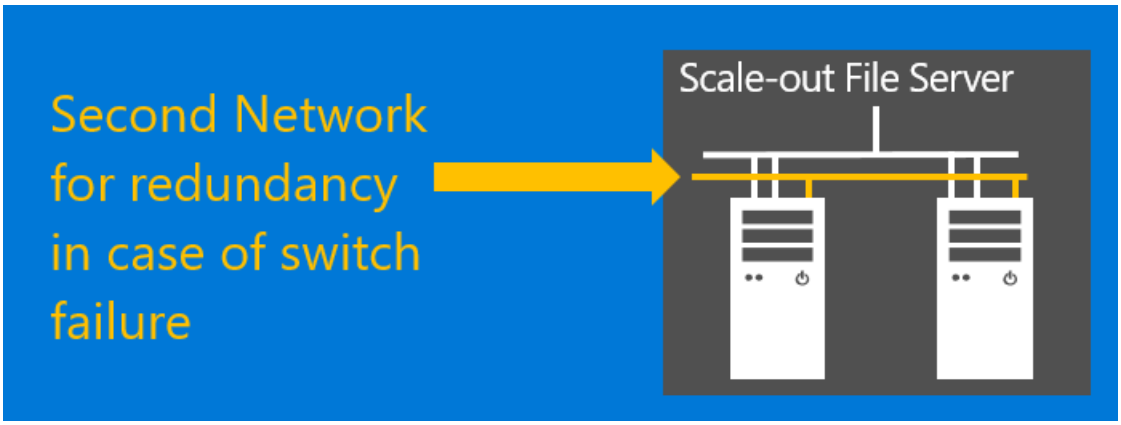


Abbildung 1: Verwenden von mindestens zwei Netzwerken für Failoverclustering

**Cluster übergreifende Verwendung mehrerer NICs**

Der größte Vorteil des vereinfachten SMB Multichannel wird erzielt, wenn mehrere NICs Cluster übergreifend in Speicher-und Speicher-Arbeits Auslastungs Clustern verwendet werden. Dadurch können Arbeits Auslastungs Cluster (Hyper-V, SQL Server-Failoverclusterinstanz, Speicher Replikat usw.) SMB Multichannel verwenden und eine effizientere Verwendung des Netzwerks erzielen. In einer konvergenten (auch disaggregierten) Cluster Konfiguration, in der ein Datei Server Cluster mit horizontaler Skalierung zum Speichern von Arbeits Auslastungs Daten für einen Hyper-V-oder SQL Server failoverclusterinstanzcluster verwendet wird, wird dieses Netzwerk häufig als "das Nord-Süd-Subnetz"/Netzwerk bezeichnet. Viele Kunden maximieren den Durchsatz dieses Netzwerks, indem Sie in RDMA-fähige NIC-Karten und-Switches investieren.

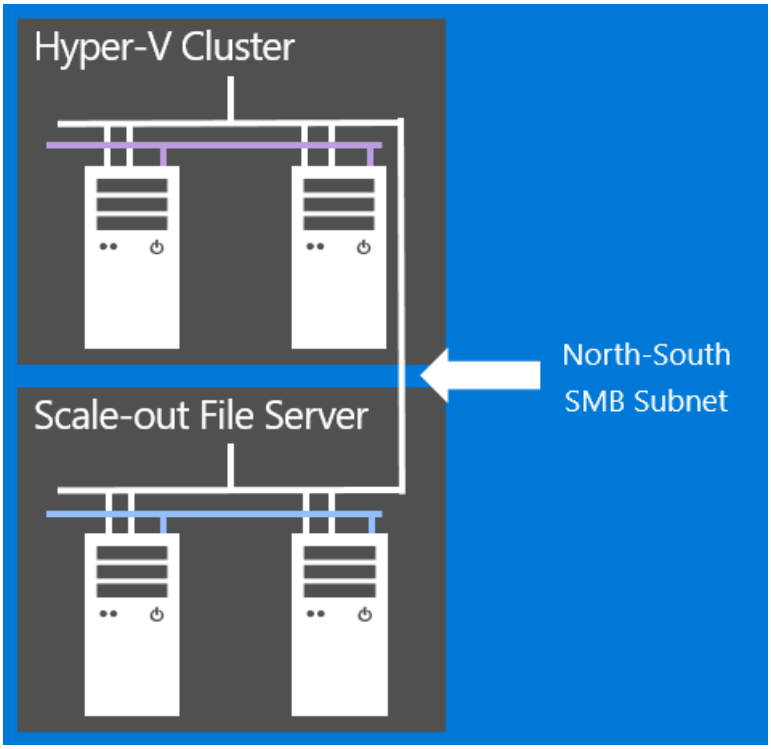



Abbildung 2: Verwenden Sie zum Erreichen des maximalen Netzwerk Durchsatzes mehrere NICs sowohl auf dem Datei Server Cluster mit horizontaler Skalierung als auch auf dem Hyper-V-oder SQL Server failoverclusterinstanzcluster, der das Subnetz Nord-Süd gemeinsam nutzt.

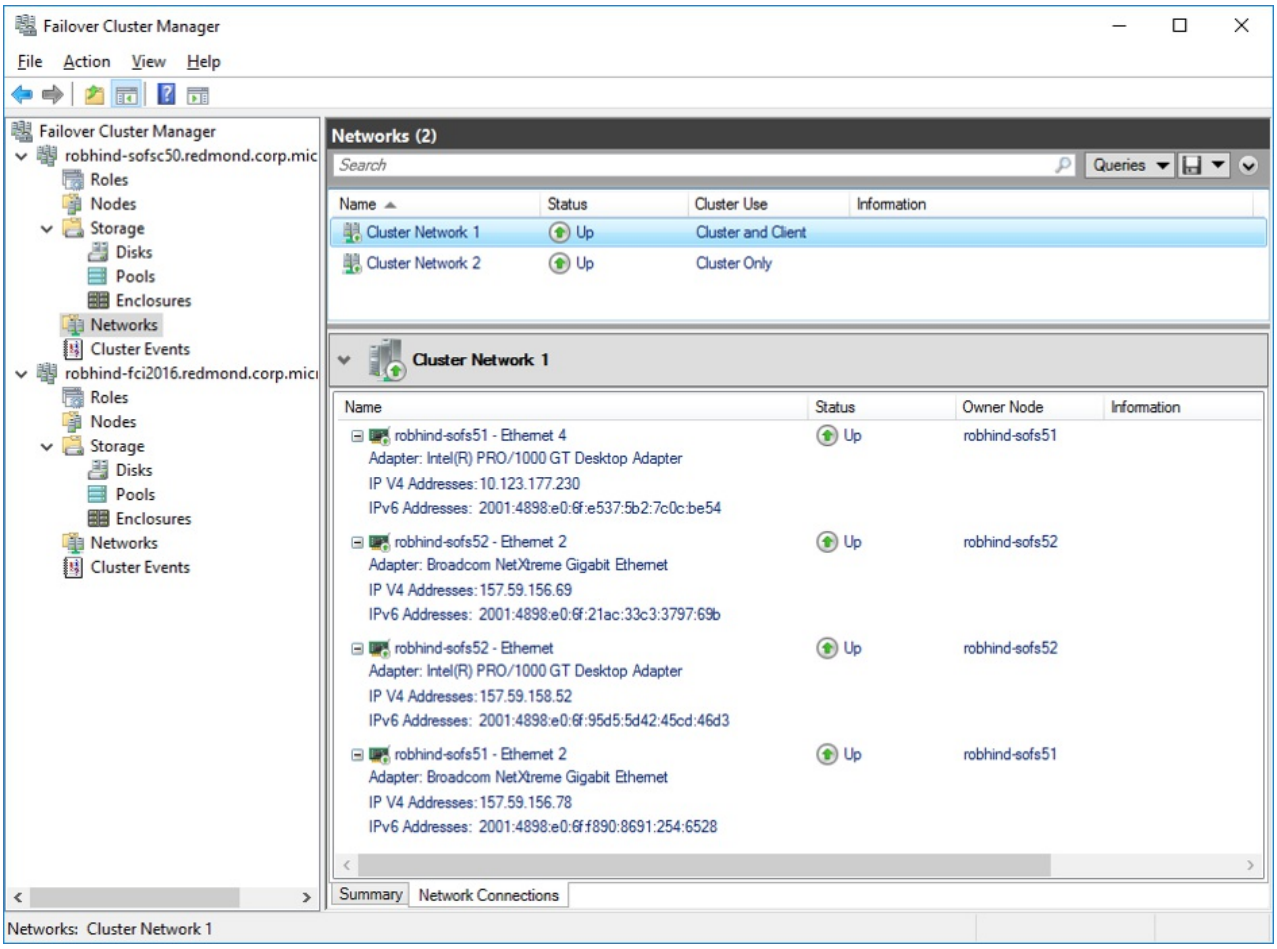



**Abbildung 3: zwei Cluster (Datei Server mit horizontaler Skalierung für Speicher, SQL Server FCI für die Arbeitsauslastung) verwenden beide mehrere NICs im gleichen Subnetz, um SMB Multichannel zu nutzen und einen besseren Netzwerk Durchsatz zu erzielen.**

## Automatische Erkennung von IPv6-Link-lokalen privaten Netzwerken

Wenn private Netzwerke (nur Cluster) mit mehreren Netzwerkkarten erkannt werden, erkennt der Cluster automatisch IPv6-Link Local (FE80)-IP-Adressen für jede NIC in jedem Subnetz. Dies spart Administratoren Zeit, da Sie IPv6-Verknüpfungs lokale (FE80) IP-Adress Ressourcen nicht mehr manuell konfigurieren müssen.

Wenn Sie mehr als ein privates Netzwerk (nur Cluster) verwenden, überprüfen Sie die IPv6-Routing Konfiguration, um sicherzustellen, dass das Routing nicht für Subnetze konfiguriert ist, da dadurch die Netzwerkleistung reduziert wird.

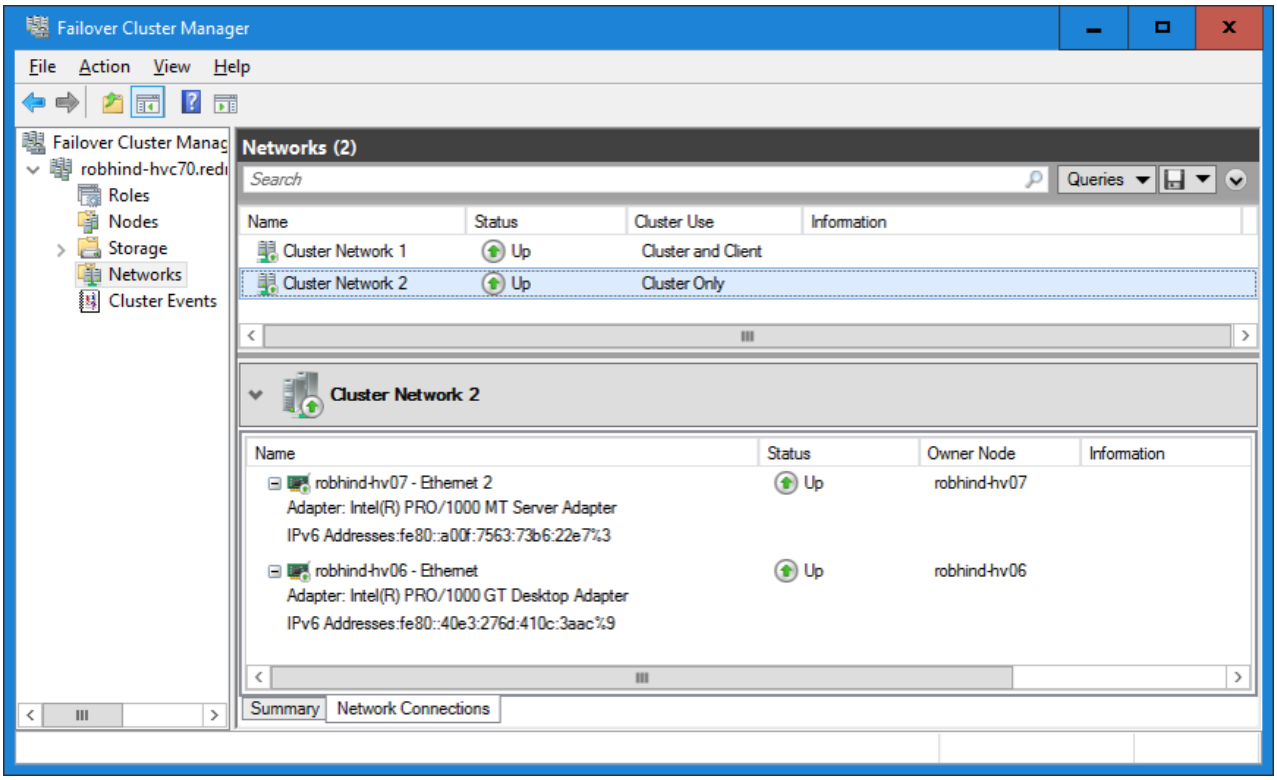



Abbildung 4: automatische IPv6-Link Local (FE80)-Adress Ressourcen Konfiguration

## Durchsatz und Fehlertoleranz

Mit Windows Server 2019 und Windows Server 2016 werden NIC-Funktionen automatisch erkannt, und es wird versucht, jede NIC in der schnellstmöglichen Konfiguration zu verwenden. NICs, die kombiniert werden, NICs mit RSS und NICs mit RDMA-Funktion können verwendet werden. In der folgenden Tabelle werden die Kompromisse bei der Verwendung dieser Technologien zusammengefasst. Maximaler Durchsatz wird erzielt, wenn mehrere RDMA-fähige NICs verwendet werden. Weitere Informationen finden Sie Untergrund lagen von SMB mutlichannel.

| | 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) | ▲▲ | ▲ | | ▲ |

Abbildung 5: Durchsatz und Fehlertoleranz für verschiedene NIC-conifigurationen

## Häufig gestellte Fragen

**Befinden sich alle NICs in einem Netzwerk mit mehreren Netzwerkkarten, die für Cluster-Herzschläge verwendet werden?**

Ja.

**Kann ein Netzwerk mit mehreren NIC nur für die Cluster Kommunikation verwendet werden? Oder kann Sie nur für die Kommunikation zwischen Client und Cluster verwendet werden?**

Beide Konfigurationen funktionieren. alle Cluster Netzwerk Rollen funktionieren in einem Netzwerk mit mehreren NIC.

**Wird SMB Multichannel auch für CSV-und Cluster Datenverkehr verwendet?**

Ja, standardmäßig werden für den gesamten Cluster-und CSV-Datenverkehr verfügbare multinic-Netzwerke verwendet. Administratoren können die PowerShell-Cmdlets für Failoverclustering oder Failovercluster-Manager-Benutzeroberfläche verwenden, um die Netzwerk Rolle zu ändern.

**Wie kann ich die SMB Multichannel-Einstellungen sehen?**
Verwenden Sie das Cmdlet **Get-smbserverconfiguration** , und suchen Sie nach dem Wert der enablemultichannel-Eigenschaft.

**Wird die allgemeine Cluster Eigenschaft "plumballcrosssubnettrotroutes" in einem Netzwerk mit mehreren NIC beachtet?**
Ja.

## Weitere Informationen

- Neues beim Failoverclustering unter Windows Server

# Übersicht über den Lastenausgleich virtueller Computer

02.12.2019 • 4 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Ein wichtiger Aspekt bei Private Cloud Bereitstellungen sind die Kapitalausgaben (CAPEX)) erforderlich, um in die Produktion zu wechseln. Es kommt häufig vor, dass Sie Redundanz zu Private Cloud bereit Stellungen hinzufügen, um eine unter Kapazität bei Spitzen Datenverkehr in der Produktion zu vermeiden. CAPEX). Der Bedarf an Redundanz wird durch unausgeglichene Private Clouds gesteuert, bei denen einige Knoten mehr Virtual Machines (VMs) und andere unterausgelastet sind (z. b. ein neu gestartetes Server).

**Übersicht über Quick Videos**
(6 Minuten)

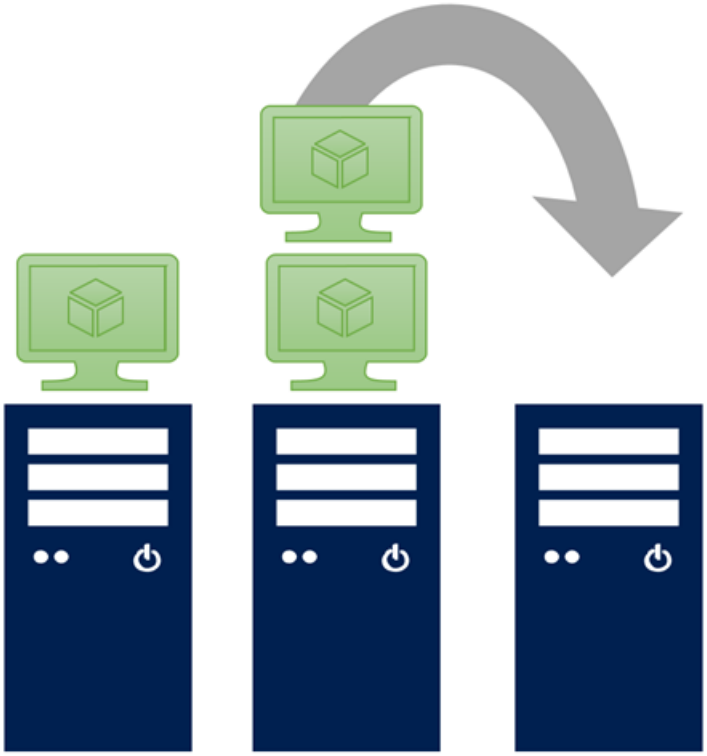
## Was ist der Lastenausgleich für virtuelle Computer?

Virtuelle Maschine Der Lastenausgleich ist ein in-Box-Feature in Windows Server 2019 und Windows Server 2016, mit dem Sie die Auslastung von Knoten in einem Failovercluster optimieren können. Es identifiziert Knoten, für die ein Commit ausgeführt wurde, und verteilt Sie erneut VMs von diesen Knoten zu Knoten, für die ein Commit ausgeführt wurde. Einige der wichtigsten Aspekte dieses Features lauten wie folgt:

- *Dabei handelt es sich um eine Lösung ohne Ausfallzeiten*: VMs werden in Knoten im Leerlauf migriert.
- *Nahtlose Integration in Ihre vorhandene Cluster Umgebung*: Fehler Richtlinien, wie z. b. antiaffinität, Fehler Domänen und mögliche Besitzer, werden berücksichtigt.
- *Heuristik für den Ausgleich*: Virtuelle Maschine Arbeitsspeicher Auslastung und CPU-Auslastung des Knotens.
- *Granulare Steuerung*: Standardmäßig aktiviert. Kann Bedarfs gesteuert oder in regelmäßigen Abständen aktiviert werden.
- *Schwellenwerte für Aggressivität*: Basierend auf den Merkmalen Ihrer Bereitstellung sind drei Schwellenwerte verfügbar.

## Das Feature in Aktion

**Dem Failovercluster wird ein neuer Knoten hinzugefügt.**



Wenn Sie dem Failovercluster neue Kapazität hinzufügen, wird der Virtuelle Maschine Der Lasten Ausgleichs Feature gleicht die Kapazität der vorhandenen Knoten automatisch mit dem neu hinzugefügten Knoten in der folgenden Reihenfolge ab:

1. Der Druck wird auf den vorhandenen Knoten im Failovercluster ausgewertet.
2. Alle Knoten, die den Schwellenwert überschreiten, werden identifiziert
3. Die Knoten mit dem höchsten Druck werden identifiziert, um die Priorität des Ausgleichs zu ermitteln.
4. VMs von einem Knoten, der den Schwellenwert überschreitet, zu einem neu hinzugefügten Knoten im Failovercluster werden Live migriert (ohne Zeitüberschreitung).

**Wiederkehrender Lastenausgleich**

Bei der Konfiguration des regelmäßigen Ausgleichs wird der Druck auf den Cluster Knoten alle 30 Minuten für den

Lastenausgleich ausgewertet. Alternativ kann der Druck bei Bedarf ausgewertet werden. Im folgenden finden Sie den Ablauf der Schritte:

1. Der Druck wird auf allen Knoten im Private Cloud ausgewertet.
2. Alle Knoten, die den Schwellenwert überschreiten, und die Untergrenze werden identifiziert
3. Die Knoten mit dem höchsten Druck werden identifiziert, um die Priorität des Ausgleichs zu ermitteln.
4. VMs von einem Knoten, der den Schwellenwert für den Knoten unter dem minimalen Schwellenwert überschreitet, werden Live migriert (ohne Zeitüberschreitung).

## Siehe auch

- Eingehender Einblick in den Lastenausgleich virtueller Computer
- Failoverclustering
- Übersicht über Hyper-V

# Eingehender Einblick in den Lastenausgleich virtueller Computer

02.12.2019 • 3 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Der Lastenausgleich des virtuellen Computers optimiert die Auslastung von Knoten in einem Failovercluster. In diesem Dokument wird beschrieben, wie Sie den VM-Lastenausgleich konfigurieren und steuern.

## Heuristik für den Ausgleich

Der Lastenausgleich des virtuellen Computers wertet die Auslastung eines Knotens basierend auf der folgenden Heuristik aus:

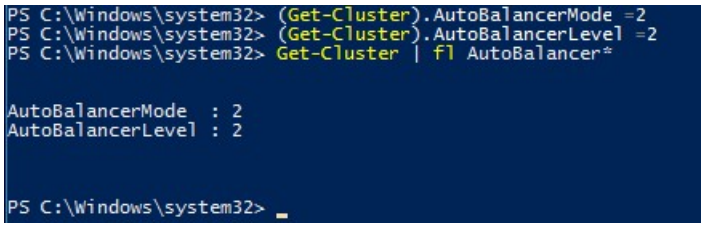
1. Aktueller **Speicher**Mangel: Der Arbeitsspeicher ist die häufigste Ressourcen Einschränkung auf einem Hyper-V-Host.
2. Die CPU- **Auslastung** des Knotens über ein 5-minütiges Fenster: Verhindert, dass ein Knoten im Cluster überlastet wird

## Steuern der Aggressivität des Ausgleichs

Die Aggressivität des Ausgleichs basierend auf der Arbeitsspeicher-und CPU-Heuristik kann mithilfe von über die allgemeine Cluster Eigenschaft "autobalancerlevel" konfiguriert werden. Führen Sie Folgendes in PowerShell aus, um die Aggressivität zu steuern:

```
(Get-Cluster).AutoBalancerLevel = <value>
```

| AUTOBALANCERLEVEL | AGGRESSI | VERHALTEN |
|---|---|---|
| 1 (Standard) | Niedrig | Verschieben, wenn Host mehr als 80% geladen ist |
| 2 | Mittel | Verschieben, wenn Host mehr als 70% geladen ist |
| 3 | Hoch | Durchschnittliche Knoten und verschieben, wenn der Host mehr als 5% oberhalb des Durchschnitts ist |



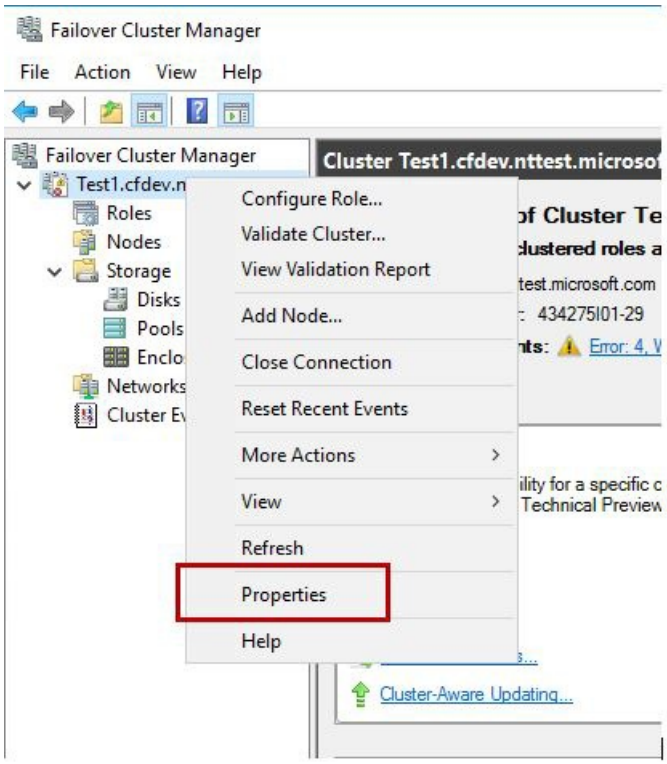

## Steuern des VM-Lasten Ausgleichs

Der VM-Lastenausgleich ist standardmäßig aktiviert, und wenn ein Lastenausgleich durchgeführt wird, kann die

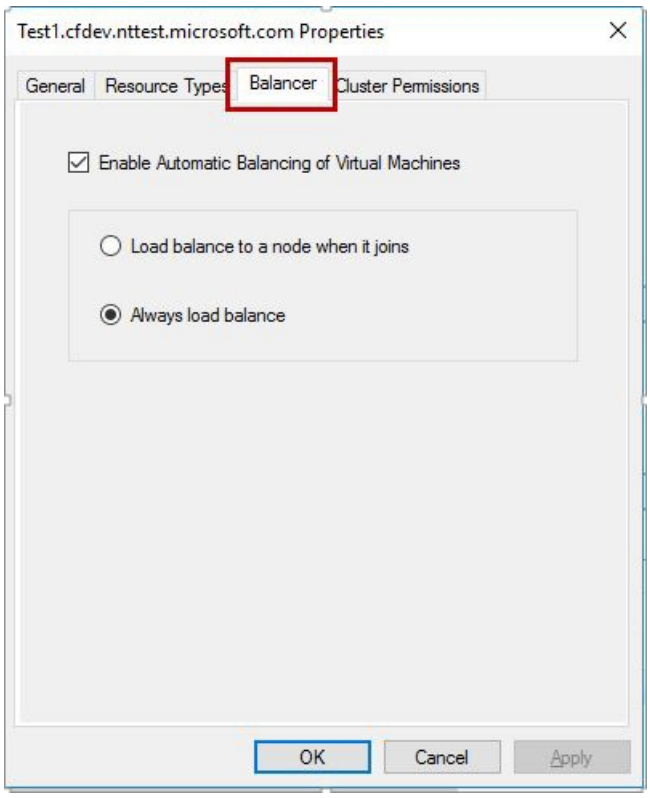
allgemeine Eigenschaft "autobalancermode" des Clusters konfiguriert werden. So steuern Sie, wann die Knoten Fairness den Cluster ausgleicht

**Verwenden von Failovercluster-Manager:**

1. Klicken Sie mit der rechten Maustaste auf den Cluster Namen, und wählen Sie die Option "Eigenschaften".




2. Wählen Sie den Bereich "Balancer" aus.




**Mithilfe von PowerShell:**

Führen Sie Folgendes aus:

```
(Get-Cluster).AutoBalancerMode = <value>
```

| AUTOBALANCERMODE | VERHALTEN |
| --- | --- |
| 0 | Disabled |
| 1 | Lastenausgleich bei Knoten Beitritt |
| 2 (Standard) | Lastenausgleich für den Knoten Beitritt und alle 30 Minuten |

## VM-Lastenausgleich im Vergleich zu Dynamische Optimierung System Center Virtual Machine Manager

Mit dem Feature "Knoten Fairness" werden in-Box-Funktionen bereitgestellt, die auf bereit Stellungen ohne System Center Virtual Machine Manager (SCVMM) ausgerichtet sind. Die dynamische SCVMM-Optimierung ist der empfohlene Mechanismus zum Ausgleichen der Auslastung virtueller Maschinen in Ihrem Cluster für SCVMM-bereit Stellungen. SCVMM deaktiviert den Lastenausgleich der Windows Server-VM automatisch, wenn die dynamische Optimierung aktiviert ist.

## Siehe auch

- Übersicht über den Lastenausgleich virtueller Computer
- Failoverclustering
- Übersicht über Hyper-V

# Clustergruppen

21.05.2020 • 44 minutes to read • Edit Online

Gilt für: Windows Server 2019

Cluster Sätze sind die neue Cloud-Technologie für horizontales Skalieren in der Windows Server 2019-Version, die die Anzahl der Cluster Knoten in einer einzelnen SDDC-Cloud (Software-Defined Data Center) in der Größe vergrößert. Bei einem Cluster Satz handelt es sich um eine lose gekoppelte Gruppierung mehrerer Failovercluster: COMPUTE-, Speicher-oder hyperkonvergierte Gruppierungen. Die Technologie von Cluster Sätzen ermöglicht die Flüssigkeit der virtuellen Maschine über Mitglieder Cluster innerhalb eines Cluster Satzes hinweg und einen vereinheitlichten Speicher Namespace über die Menge hinweg, um die Geschwindigkeit virtueller Computer zu unterstützen.

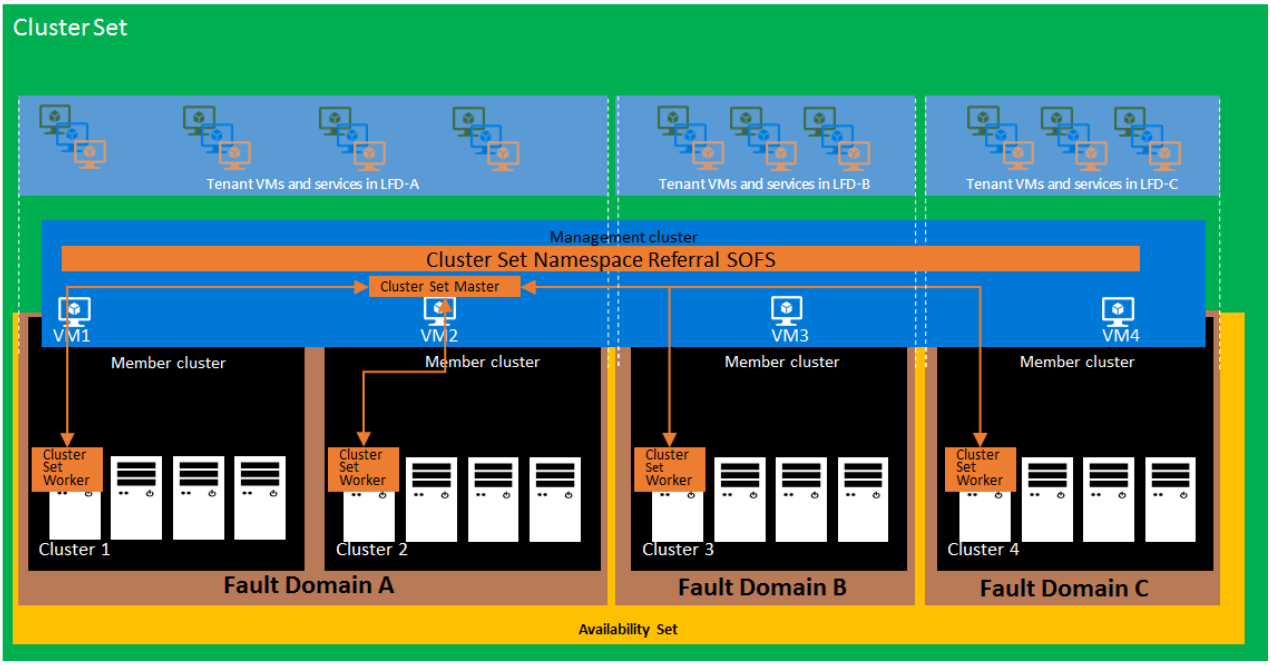
Bei der Beibehaltung der vorhandenen Failovercluster-Verwaltungsfunktionen auf Mitglieds Clustern bietet eine clusterset-Instanz zusätzlich wichtige Anwendungsfälle im Zusammenhang mit der Lebenszyklus Verwaltung für das Aggregat. Dieses Evaluierungs Handbuch für Windows Server 2019-Szenarien bietet Ihnen die erforderlichen Hintergrundinformationen sowie schrittweise Anleitungen zum Auswerten von Clustergruppen mithilfe von PowerShell.

## Einführung in die Technologie

Die Technologie von Cluster Sätzen wird so entwickelt, dass bestimmte Kundenanforderungen bei der Skalierung von Betriebs Software definierte Rechenzentrums Clouds (SDDC) erfüllt werden. Der Wert eines Cluster Sets kann wie folgt zusammengefasst werden:

- Erhöhen Sie die unterstützte SDDC-cloudskalierung für die Ausführung hoch verfügbarer virtueller Computer, indem Sie mehrere kleinere Cluster in einem einzelnen großen Fabric kombinieren, auch wenn die Softwarefehler Grenze auf einem einzelnen Cluster beibehalten wird.
- Verwalten des gesamten failoverclusterlebens Zyklus, einschließlich des Onboarding-und Außerbetriebnahme von Clustern, ohne Auswirkungen auf die Verfügbarkeit der Mandanten-VMS zu haben
- Einfaches Ändern der COMPUTE-zu-Speicher-Quote in der hyperkonvergierten I
- Profitieren Sie von Azure-ähnlichen Fehler Domänen und Verfügbarkeits Gruppen über Cluster hinweg bei der ersten Platzierung virtueller Maschinen und der nachfolgenden Migration virtueller Computer
- Kombinieren Sie verschiedene Generationen von CPU-Hardware mit dem gleichen Cluster Satz-Fabric, auch wenn Sie die einzelnen Fehler Domänen für maximale Effizienz einheitlich halten. Beachten Sie, dass die Empfehlung der gleichen Hardware immer noch in jedem einzelnen Cluster und dem gesamten Cluster Satz vorhanden ist.

Aus einer Ansicht auf hoher Ebene können Cluster Sätze aussehen.




Im folgenden finden Sie eine kurze Zusammenfassung der einzelnen Elemente in der obigen Abbildung:

### Verwaltungscluster

Bei einem Verwaltungs Cluster in einem Cluster Satz handelt es sich um einen Failovercluster, der die hoch verfügbare Verwaltungsebene des gesamten Cluster Satzes und des Unified Storage-Namespace (Cluster Satz Namespace) für den Verweis Dateiserver mit horizontaler Skalierung (sofs) hostet. Ein Verwaltungs Cluster ist logisch von Mitglieds Clustern entkoppelt, von denen die Arbeits Auslastungen virtueller Computer ausgeführt werden. Dadurch kann die Verwaltungsebene des Clusters anfällig für alle lokalisierten Cluster weiten Fehler sein, z. b. einen Stromausfall eines Mitglieds Clusters.

### Mitglieds Cluster

Bei einem Mitglieds Cluster in einem Cluster Satz handelt es sich in der Regel um einen herkömmlichen hyperkonvergenten Cluster mit virtuellen Maschinen und direkte Speicherplätze Workloads. Mehrere Mitglieds Cluster sind Teil einer einzelnen Cluster Satz Bereitstellung und bilden so das größere SDDC-Cloud-Fabric. Mitglieds Cluster unterscheiden sich in zwei wichtigen Aspekten von einem Verwaltungs Cluster: Mitglieds Cluster sind Teil der Fehler Domänen-und Verfügbarkeits Gruppen-Konstrukte, und Mitglieds Cluster sind ebenfalls zum Hosten virtueller Maschinen und direkte Speicherplätze Arbeits Auslastungen skaliert. Virtuelle Computer für Clustergruppen, die über Cluster Grenzen in einem Cluster Satz hinweg verschoben werden, dürfen aus diesem Grund nicht auf dem Verwaltungs Cluster gehostet werden.

### Cluster Satz-Namespace Verweis-sofs

Ein Cluster Satz-Namespace Verweis (Cluster Set Namespace) sofs ist eine Dateiserver mit horizontaler Skalierung, wobei jede SMB-Freigabe auf dem Cluster Satz Namespace sofs eine Verweis Freigabe – vom Typ "simplereferral" ist, die in Windows Server 2019 neu eingeführt wurde. Mit diesem Verweis können SMB-Clients (Server Message Block) auf die SMB-Ziel Freigabe zugreifen, die auf dem Mitglieds Cluster-sofs gehostet wird. Der clusterset-Namespace Verweis-sofs ist ein einfacher Verweis Mechanismus und ist daher nicht Teil des e/a-Pfads. Die SMB-Verweise werden auf den einzelnen Client Knoten ständig zwischengespeichert, und der Cluster legt Namespaces automatisch automatisch aktualisiert.

### Cluster Satz Master

In einem Cluster Satz ist die Kommunikation zwischen den Mitglieds Clustern lose gekoppelt und wird von einer neuen Cluster Ressource mit dem Namen "Cluster Satz Master" (CS-Master) koordiniert. Wie jede andere Cluster Ressource ist CS-Master hoch verfügbar und anfällig für Cluster Ausfälle einzelner Mitglieder und/oder Fehler des Verwaltungs Cluster Knotens. Über einen neuen Cluster Satz-WMI-Anbieter stellt CS-Master den Verwaltungs

Endpunkt für alle Interaktionen mit der Verwaltbarkeit von Clustergruppen bereit.

### Cluster Satz-Worker

In einer Cluster Satz Bereitstellung interagiert der CS-Master mit einer neuen Cluster Ressource auf den Mitglieds Clustern, die als "clusterset-Worker" (CS-Worker) bezeichnet werden. CS-Worker fungiert als einzige Verbindung auf dem Cluster, um die lokalen Cluster Interaktionen zu orchestrieren, die vom CS-Master angefordert werden. Beispiele für derartige Interaktionen sind z. b. die Platzierung virtueller Maschinen und die Ressourcen Inventur für lokale Cluster Ressourcen. Es gibt nur eine CS-Worker-Instanz für jeden Mitglieds Cluster in einem Cluster Satz.

### Fehlerdomäne

Eine Fehler Domäne ist die Gruppierung von Software-und Hardware Artefakten, die der Administrator beim Auftreten eines Fehlers möglicherweise fehlschlägt. Obwohl ein Administrator einen oder mehrere Cluster als Fehler Domäne bezeichnen könnte, könnte jeder Knoten in einer Fehler Domäne in einer Verfügbarkeits Gruppe teilnehmen. Cluster Sätze werden Überlegungen zur Identifizierung von Fehler Domänen an den Administrator weitergeleitet, der mit den Überlegungen zur Topologie von Rechenzentren gut vertraut ist – z. b. PDU, Netzwerk –, die Mitglied Cluster gemeinsam nutzen.

### Verfügbarkeitsgruppe

Eine Verfügbarkeits Gruppe unterstützt den Administrator dabei, die gewünschte Redundanz von gruppierten Arbeits Auslastungen für Fehler Domänen zu konfigurieren, indem Sie diese in einer Verfügbarkeits Gruppe organisieren und Workloads in dieser Verfügbarkeits Gruppe Nehmen wir an, wenn Sie eine Anwendung mit zwei Ebenen bereitstellen, empfehlen wir, dass Sie mindestens zwei virtuelle Computer in einer Verfügbarkeits Gruppe für jede Ebene konfigurieren, um sicherzustellen, dass bei Ausfall einer Fehler Domäne in dieser Verfügbarkeits Gruppe mindestens ein virtueller Computer auf jeder Ebene in einer anderen Fehler Domäne derselben Verfügbarkeits Gruppe gehostet wird.

## Gründe für die Verwendung von Cluster Sätzen

Cluster Sätze bieten den Vorteil der Skalierung, ohne die Resilienz zu beeinträchtigen.

Cluster Sätze ermöglichen das Clustering mehrerer Cluster, um ein großes Fabric zu erstellen, während jeder Cluster unabhängig von der Resilienz bleibt. Beispielsweise verfügen Sie über mehrere HCI-Cluster mit 4 Knoten, auf denen virtuelle Computer ausgeführt werden. Jeder Cluster bietet die erforderliche Resilienz für sich selbst. Wenn der Speicher oder der Arbeitsspeicher aufgefüllt wird, ist das zentrale hochskalieren der nächste Schritt. Beim zentralen hochskalieren gibt es einige Optionen und Überlegungen.

1. Fügen Sie dem aktuellen Cluster weiteren Speicherplatz hinzu. Mit direkte Speicherplätze kann dies schwierig sein, da genau dieselbe Modell-/firmwarelaufwerke nicht verfügbar sind. Die Überlegung der Neuerstellungs Zeiten muss ebenfalls berücksichtigt werden.
2. Fügen Sie weiteren Arbeitsspeicher hinzu. Was geschieht, wenn Sie den Arbeitsspeicher, der von den Computern verarbeitet werden kann, abgleichen? Was geschieht, wenn alle verfügbaren Speicher Slots voll sind?
3. Fügen Sie dem aktuellen Cluster zusätzliche Computeknoten mit Laufwerken hinzu. Dadurch wird die Option 1 benötigt.
4. Erwerben eines vollständigen neuen Clusters

An dieser Stelle bietet Cluster Sätze den Vorteil der Skalierung. Wenn ich meine Cluster zu einem Cluster Satz hinzufüge, kann ich Speicher oder Arbeitsspeicher nutzen, der in einem anderen Cluster möglicherweise ohne zusätzliche Käufe verfügbar ist. Aus Sicht der Resilienz bietet das Hinzufügen zusätzlicher Knoten zu einem direkte Speicherplätze keine weiteren Stimmen für das Quorum. Wie hiererwähnt, kann ein direkte Speicherplätze Cluster den Verlust von zwei Knoten überstehen, bevor er ausfällt. Wenn Sie über einen HCI-Cluster mit vier Knoten verfügen, wird der gesamte Cluster durch 3 Knoten herunterfahren. Wenn Sie über einen Cluster mit 8 Knoten verfügen, wird der gesamte Cluster durch 3 Knoten herunterfahren. Bei Cluster Sätzen mit zwei HCI-Clustern mit 4

Knoten in der Gruppe werden zwei Knoten in einem HCI heruntergeschaltet und ein Knoten im anderen HCI heruntergeschaltet. beide Cluster bleiben erhalten. Empfiehlt es sich, einen großen 16-Knoten-direkte Speicherplätze Cluster zu erstellen oder in vier Knoten mit vier Knoten zu unterbrechen und Cluster Sätze zu verwenden? Das vorhanden sein von vier Clustern mit vier Knoten und Cluster Sätzen bietet die gleiche Skalierbarkeit, aber eine bessere Resilienz darin, dass mehrere Computeknoten ausfallen können (unerwartet oder für Wartung) und die Produktion verbleibt.

## Überlegungen zum Bereitstellen von Cluster Sätzen

Berücksichtigen Sie bei der Überlegung, ob Cluster Sätze verwendet werden müssen, die folgenden Fragen:

- Müssen Sie über die aktuellen HCI-COMPUTE-und Speicher Skalierungs Limits hinausgehen?
- Sind alle Compute-und Speicheranforderungen nicht identisch?
- Werden virtuelle Computer zwischen Clustern Live migriert?
- Möchten Sie die Verfügbarkeits Gruppen von Azure-ähnlichen Computern und Fehler Domänen über mehrere Cluster hinweg angleichen?
- Müssen Sie sich die Zeit nehmen, sich alle Cluster anzusehen, um zu bestimmen, wo neue virtuelle Computer platziert werden müssen?

Wenn die Antwort "Ja" lautet, benötigen Sie Cluster Sätze.

Es gibt noch einige andere Punkte, die in Erwägung gezogen werden müssen, wenn ein größerer SDDC Ihre allgemeinen Rechenzentrums Strategien möglicherweise ändert. SQL Server ist ein gutes Beispiel. Erfordert das Verschieben von SQL Server virtuellen Maschinen zwischen Clustern die Lizenzierung von SQL für die Verwendung auf zusätzlichen Knoten?

## Dateiserver mit horizontaler Skalierung und Cluster Sätze

In Windows Server 2019 gibt es eine neue Datei Server Rolle mit horizontaler Skalierung namens Infrastructure Dateiserver mit horizontaler Skalierung (sofs).

Die folgenden Überlegungen gelten für eine Infrastruktur-sofs-Rolle:

1. In einem Failovercluster kann es höchstens eine Infrastruktur-sofs-Cluster Rolle geben. Die Infrastruktur-sofs-Rolle wird erstellt, indem der Switch-Parameter "**-Infrastructure**" für das Cmdlet " **Add-clusterscaleoutfileserverrole** " angegeben wird. Beispiel:

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

2. Jedes CSV-Volume, das im Failover erstellt wird, löst automatisch die Erstellung einer SMB-Freigabe mit einem automatisch generierten Namen auf Grundlage des CSV-Volumenamens aus. Ein Administrator kann SMB-Freigaben unter einer sofs-Rolle nicht direkt erstellen oder ändern, außer über CSV-Volume Create/Modify-Vorgänge.

3. In hyperkonvergierten Konfigurationen ermöglicht ein-Infrastruktur-sofs einem SMB-Client (Hyper-V-Host) die Kommunikation mit der garantierten kontinuierlichen Verfügbarkeit (ca) mit dem Infrastruktur-sofs-SMB-Server. Diese hyperkonvergierte SMB-Loopback Zertifizierungsstelle wird über virtuelle Computer erreicht, die auf Ihre vhdx-Dateien (Virtual Disk) zugreifen, bei denen die Identität des besitzenden virtuellen Computers zwischen dem Client und dem Server weitergeleitet wird. Diese Identitäts Weiterleitung ermöglicht die ACL-vhdx-Dateien genau wie bei standardmäßigen hyperkonvergierten Cluster Konfigurationen wie zuvor.

Nachdem ein Cluster Satz erstellt wurde, basiert der Cluster Satz-Namespace auf einem Infrastruktur-sofs auf jedem der Mitglieds Cluster und zusätzlich auf einem Infrastruktur-sofs im Verwaltungs Cluster.

Wenn einem Cluster Satz ein Mitglieds Cluster hinzugefügt wird, gibt der Administrator den Namen eines Infrastruktur-sofs in diesem Cluster an, sofern bereits ein Cluster vorhanden ist. Wenn die Infrastruktur-sofs nicht vorhanden ist, wird von diesem Vorgang eine neue Infrastruktur-sofs-Rolle auf dem neuen Mitglieds Cluster erstellt. Wenn eine Infrastruktur-sofs-Rolle bereits auf dem Mitglieds Cluster vorhanden ist, benennt der Add-Vorgang Sie nach Bedarf implizit in den angegebenen Namen um. Alle vorhandenen Singleton-SMB-Server oder nicht-Infrastruktur-sofs-Rollen auf den Mitglieds Clustern bleiben vom Cluster Satz nicht ausgelastet.

Zum Zeitpunkt der Erstellung des Cluster Satzes hat der Administrator die Möglichkeit, ein bereits vorhandenes AD-Computer Objekt als Namespace Stamm auf dem Verwaltungs Cluster zu verwenden. Bei der Erstellung von Cluster Satz-Vorgängen wird die Infrastruktur-sofs-Cluster Rolle auf dem Verwaltungs Cluster erstellt, oder die vorhandene Infrastruktur-sofs-Rolle wird wie zuvor für Mitglieder Cluster beschrieben umbenannt. Die Infrastruktur-sofs im Verwaltungs Cluster wird als Cluster Satz-Namespace Referenz (Cluster Set Namespace) sofs verwendet. Es bedeutet einfach, dass jede SMB-Freigabe im Cluster Satz Namespace sofs eine Verweis Freigabe – vom Typ "simplereferral" ist, die in Windows Server 2019 neu eingeführt wurde. Dieser Verweis ermöglicht SMB-Clients den Zugriff auf die SMB-Ziel Freigabe, die auf dem Mitglieds Cluster-sofs gehostet wird. Der clusterset-Namespace Verweis-sofs ist ein einfacher Verweis Mechanismus und ist daher nicht Teil des e/a-Pfads. Die SMB-Verweise werden auf den einzelnen Client Knoten ständig zwischengespeichert, und der Cluster legt Namespaces automatisch automatisch aktualisiert. diese Verweise werden bei Bedarf automatisch aktualisiert.

# Erstellen eines Cluster Satzes

**Voraussetzungen**

Wenn Sie einen Cluster Satz erstellen, werden die folgenden Voraussetzungen empfohlen:

1. Konfigurieren Sie einen Verwaltungs Client, auf dem Windows Server 2019 ausgeführt wird.
2. Installieren Sie die Failoverclustertools auf diesem Management Server.
3. Erstellen von Cluster Mitgliedern (mindestens zwei Cluster mit mindestens zwei freigegebenen Clustervolumes auf jedem Cluster)
4. Erstellen Sie einen Verwaltungs Cluster (physisch oder Gast), der die Mitglieder Cluster überschreitet. Mit diesem Ansatz wird sichergestellt, dass die Verwaltungsebene des Clusters weiterhin verfügbar ist, obwohl mögliche Mitglieder Cluster Fehler auftreten.

**Schritte**

1. Erstellen Sie einen neuen Cluster Satz aus drei Clustern, wie in den Voraussetzungen definiert. Das folgende Diagramm enthält ein Beispiel für zu erstellende Cluster. Der Name des Cluster Satzes in diesem Beispiel ist `csmaster`.

| CLUSTERNAME | DER SPÄTER ZU VERWENDENDE INFRASTRUKTUR-SOFS-NAME |
|---|---|
| Set-Cluster | sofs-clusterset |
| CLUSTER1 | Sofs-CLUSTER1 |
| CLUSTER2 | Sofs-CLUSTER2 |

2. Nachdem alle Cluster erstellt wurden, verwenden Sie den folgenden Befehl, um den Cluster Satz Master zu erstellen:

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

3. Verwenden Sie den unten aufgeführten Befehl, um dem Cluster Satz einen Cluster Server hinzuzufügen:

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

> **NOTE**
> Wenn Sie ein statisches IP-Adress Schema verwenden, müssen Sie *-staticaddress x. x. x. x* in den **New-clusterset** -Befehl einschließen.

4. Nachdem Sie den Cluster aus den Cluster Mitgliedern erstellt haben, können Sie die Knotengruppe und deren Eigenschaften auflisten. So zählen Sie alle Mitglieds Cluster im Cluster Satz auf:

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

5. So zählen Sie alle Mitglieds Cluster in der Clustergruppe einschließlich der Verwaltungs Cluster Knoten auf:

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

6. So Listen Sie alle Knoten aus den Mitglieds Clustern auf

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

7. So Listen Sie alle Ressourcengruppen im Cluster Satz auf:

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

8. Um zu überprüfen, ob beim Erstellen eines Cluster Satzes eine SMB-Freigabe (identifiziert als volume1 oder die Bezeichnung des CSV-Ordners) erstellt wurde, ist ScopeName der Infrastruktur Datei Server Name und der Pfad beide in der Infrastruktur-sofs für das CSV-Volume jedes Cluster Mitglieds:

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

9. Cluster Satz-Debugprotokolle können zur Überprüfung gesammelt werden. Sowohl der Cluster Satz als auch die Cluster-Debugprotokolle können für alle Mitglieder und den Verwaltungs Cluster erfasst werden:

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

10. Konfigurieren Sie die eingeschränkte Kerberos- Delegierung zwischen allen Mitgliedern der Clustergruppe.
11. Konfigurieren Sie den Authentifizierungstyp für die Live Migration der Cluster übergreifenden virtuellen Maschine auf jedem Knoten im Cluster Satz mit Kerberos.

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

12. Fügen Sie der lokalen Gruppe Administratoren auf jedem Knoten im Cluster Satz den Verwaltungs Cluster hinzu.

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

## Erstellen neuer virtueller Maschinen und hinzufügen zu Cluster Sätzen

Nachdem Sie den Cluster Satz erstellt haben, besteht der nächste Schritt im Erstellen neuer virtueller Maschinen. Normalerweise müssen Sie beim Erstellen virtueller Maschinen und beim Hinzufügen zu einem Cluster einige Überprüfungen an den Clustern durchführen, um festzustellen, ob die Anwendung am besten geeignet ist. Diese Überprüfungen können Folgendes umfassen:

- Wie viel Arbeitsspeicher ist auf den Cluster Knoten verfügbar?
- Wie viel Speicherplatz ist auf den Cluster Knoten verfügbar?
- Erfordert der virtuelle Computer bestimmte Speicheranforderungen (d. h. Ich möchte, dass meine SQL Server virtuellen Maschinen zu einem Cluster mit schnelleren Laufwerken wechseln, oder der virtuelle Computer der Infrastruktur ist nicht so kritisch und kann auf langsameren Laufwerken ausgeführt werden).

Nachdem Sie diese Fragen beantwortet haben, erstellen Sie den virtuellen Computer auf dem Cluster, den Sie benötigen. Einer der Vorteile von Cluster Sätzen besteht darin, dass Cluster Sätze diese Überprüfungen ausführen und den virtuellen Computer auf dem optimalen Knoten platzieren.

Mit den folgenden Befehlen wird der optimale Cluster identifiziert und der virtuelle Computer darauf bereitgestellt. Im folgenden Beispiel wird ein neuer virtueller Computer erstellt, der angibt, dass mindestens 4 Gigabyte Arbeitsspeicher für den virtuellen Computer verfügbar sind und dass er einen virtuellen Prozessor nutzen muss.

- Stellen Sie sicher, dass 4 GB für den virtuellen Computer verfügbar sind.
- Legen Sie den bei 1 verwendeten virtuellen Prozessor fest.
- Stellen Sie sicher, dass mindestens 10% CPU für den virtuellen Computer verfügbar ist.

```
# 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
```

Wenn der Vorgang abgeschlossen ist, erhalten Sie die Informationen zum virtuellen Computer und zum Speicherort des virtuellen Computers. Im obigen Beispiel würde Folgendes angezeigt werden:

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

Wenn Sie nicht genügend Arbeitsspeicher, CPU-Kapazität oder Speicherplatz zum Hinzufügen des virtuellen Computers haben, wird der folgende Fehler angezeigt:

```
Get-ClusterSetOptimalNodeForVM : A cluster node is not available for this operation.
```

Nachdem der virtuelle Computer erstellt wurde, wird er auf dem angegebenen Knoten im Hyper-V-Manager angezeigt. Verwenden Sie den folgenden Befehl, um den virtuellen Computer als Cluster Satz hinzuzufügen und ihn dem Cluster hinzuzufügen:

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

Wenn der Vorgang abgeschlossen ist, lautet die Ausgabe wie folgt:

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

Wenn Sie einen Cluster mit vorhandenen virtuellen Computern hinzugefügt haben, müssen die virtuellen Computer auch bei Cluster Sätzen registriert werden. Um alle diese virtuellen Computer gleichzeitig zu registrieren, muss der folgende Befehl verwendet werden:

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

Der Prozess ist jedoch noch nicht beendet, da der Pfad zum virtuellen Computer dem Cluster Satz-Namespace hinzugefügt werden muss.

Beispielsweise wird ein vorhandener Cluster hinzugefügt und verfügt über vorkonfigurierte virtuelle Computer, die sich auf dem lokalen freigegebenes Clustervolume (CSV) befinden. Der Pfad für die vhdx-Datei würde etwa wie folgt lauten: "c:\clusterstorage\volume1\myvm\virtual Hard disks\myvm.vhdx". Es muss eine Speicher Migration durchgeführt werden, da CSV-Pfade in einem Cluster mit einem einzelnen Mitglied erstellt werden und daher nicht für die virtuelle Maschine zugänglich sind, sobald Sie Live in Mitglieds Clustern migriert sind.

In diesem Beispiel wurde CLUSTER3 dem Cluster Satz mithilfe von Add-clustersetmember mit der Infrastruktur Dateiserver mit horizontaler Skalierung als sofs-CLUSTER3 hinzugefügt. Um die Konfiguration und den Speicher des virtuellen Computers zu verschieben, lautet der Befehl wie folgt:

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

Sobald der Vorgang abgeschlossen ist, erhalten Sie eine Warnung:

```
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.
```

Diese Warnung kann ignoriert werden, weil die Warnung "Es wurden keine Änderungen in der Speicherkonfiguration der Rolle für virtuelle Computer erkannt" angezeigt wird. Der Grund für die Warnung, weil der tatsächliche physische Speicherort nicht geändert wird. nur die Konfigurations Pfade.

Weitere Informationen zu "Move-vmstorage" finden Sie unter diesem Link.

Die Live Migration einer virtuellen Maschine zwischen unterschiedlichen Clustergruppen Clustern ist nicht mit der in der Vergangenheit identisch. In Szenarien, in denen es sich nicht um Cluster Sätze handelt, sind folgende Schritte erforderlich:

1. Entfernen Sie die Rolle für virtuelle Computer aus dem Cluster.
2. Live Migration der virtuellen Maschine zu einem Mitglieds Knoten eines anderen Clusters.

3. Fügen Sie den virtuellen Computer dem Cluster als neue Rolle für virtuelle Computer hinzu.

Bei Cluster Sätzen sind diese Schritte nicht erforderlich, und nur ein Befehl ist erforderlich. Legen Sie zunächst mithilfe des folgenden Befehls alle Netzwerke fest, die für die Migration verfügbar sein sollen:

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

Beispielsweise möchte ich einen virtuellen Computer für den Cluster Satz von CLUSTER1 auf Node2-CL3 auf CLUSTER3 verschieben. Der einzige Befehl lautet wie folgt:

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

Beachten Sie, dass dadurch nicht der Speicher oder die Konfigurationsdateien des virtuellen Computers verschoben werden. Dies ist nicht erforderlich, da der Pfad zum virtuellen Computer weiterhin \ \ SOFS-CLUSTER1\VOLUME1. Wenn ein virtueller Computer mit Cluster Sätzen registriert ist, muss der Pfad der Infrastruktur Datei Server Freigabe sein, und die Laufwerke und die virtuelle Maschine müssen sich nicht auf demselben Computer wie der virtuelle Computer befinden.

## Erstellen von Verfügbarkeits Gruppen

Wie in der Einführung beschrieben, können Azure-ähnliche Fehler Domänen und Verfügbarkeits Gruppen in einem Cluster Satz konfiguriert werden. Dies ist nützlich für die Platzierung von ersten virtuellen Computern und Migrationen zwischen Clustern.

Im folgenden Beispiel sind vier Cluster am Cluster Satz beteiligt. Innerhalb des Satzes wird eine logische Fehler Domäne mit zwei Clustern und einer Fehler Domäne erstellt, die mit den anderen beiden Clustern erstellt wurde. Diese beiden Fehler Domänen bestehen aus der Verfügbarkeits Gruppe.

Im folgenden Beispiel werden CLUSTER1 und CLUSTER2 in einer Fehler Domäne mit dem Namen **FD1** angezeigt, während CLUSTER3 und CLUSTER4 sich in einer Fehler Domäne mit dem Namen **FD2** befinden. Die Verfügbarkeits Gruppe wird **als csmaster-as** bezeichnet und besteht aus den beiden Fehler Domänen.

Um die Fehler Domänen zu erstellen, sind die folgenden Befehle:

```
New-ClusterSetFaultDomain -Name FD1 -FdType Logical -CimSession CSMASTER -MemberCluster CLUSTER1,CLUSTER2 -
Description "This is my first fault domain"

New-ClusterSetFaultDomain -Name FD2 -FdType Logical -CimSession CSMASTER -MemberCluster CLUSTER3,CLUSTER4 -
Description "This is my second fault domain"
```

Um sicherzustellen, dass Sie erfolgreich erstellt wurden, kann Get-clustersetfehlerdomain mit der angezeigten Ausgabe ausgeführt werden.

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

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

Nachdem die Fehler Domänen erstellt wurden, muss die Verfügbarkeits Gruppe erstellt werden.

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

Um zu überprüfen, ob er erstellt wurde, verwenden Sie Folgendes:

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

Wenn Sie neue virtuelle Maschinen erstellen, müssen Sie den Parameter "-availabilityset" im Rahmen der Ermittlung des optimalen Knotens verwenden. So sieht es in etwa wie folgt aus:

```
# Identify the optimal node to create a new virtual machine
$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)
```

Entfernen eines Clusters aus Cluster Sätzen aufgrund verschiedener Lebenszyklen. Es gibt Zeiten, in denen ein Cluster aus einem Cluster Satz entfernt werden muss. Als bewährte Vorgehensweise sollten alle virtuellen Computer mit Cluster Satz aus dem Cluster verschoben werden. Dies kann mithilfe der Befehle **Move-clustersetvm** und **Move-vmstorage** erreicht werden.

Wenn die virtuellen Computer jedoch nicht ebenfalls verschoben werden, führt Cluster Sätze eine Reihe von Aktionen aus, um dem Administrator ein intuitives Ergebnis zu bieten. Wenn der Cluster aus der Gruppe entfernt wird, werden alle verbleibenden virtuellen Computer Gruppen, die auf dem zu entfernenden Cluster gehostet werden, einfach zu hoch verfügbaren virtuellen Computern, die an diesen Cluster gebunden sind, vorausgesetzt, dass Sie Zugriff auf den Speicher haben. Cluster Sätze aktualisieren das Inventar auch automatisch wie folgt:

- Die Integrität des jetzt entfernten Clusters und der darauf laufenden virtuellen Maschinen werden nicht mehr nachverfolgt.
- Entfernt aus dem Cluster Satz Namespace und allen Verweisen auf Freigaben, die auf dem jetzt entfernten Cluster gehostet werden.

Beispielsweise wäre der Befehl zum Entfernen des CLUSTER1-Clusters aus Cluster Sätzen wie folgt:

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

## Häufig gestellte Fragen (FAQ)

**Frage:** Kann ich in meinem Cluster Satz nur hyperkonvergierte Cluster verwenden?
**Antwort:** Nein. Sie können direkte Speicherplätze mit herkömmlichen Clustern kombinieren.

**Frage:** Kann ich meinen Cluster Satz über System Center Virtual Machine Manager verwalten?
**Antwort:** System Center Virtual Machine Manager unterstützt derzeit keine Cluster Sätze.

**Frage:** Können Windows Server 2012 R2-oder 2016-Cluster gemeinsam im gleichen Cluster Satz vorhanden sein?
**Frage:** Kann ich Workloads von Windows Server 2012 R2-oder 2016-Clustern migrieren, indem diese Cluster einfach demselben Cluster Satz beitreten?
**Antwort:** Bei Cluster Sätzen handelt es sich um eine neue Technologie, die in Windows Server 2019 eingeführt wird und daher in früheren Versionen nicht vorhanden ist. Betriebssystem basierte Cluster auf Betriebssystemebene können keinem Cluster Satz beitreten. Die Technologie für parallele Upgrades des Cluster Betriebssystems sollte jedoch die Migrations Funktionalität bereitstellen, nach der Sie suchen, indem Sie diese

Cluster auf Windows Server 2019 aktualisieren.

**Frage:** Kann ich mit Cluster Sätzen Speicher oder COMPUTE (allein) Skalieren?
**Antwort:** Ja, durch einfaches Hinzufügen eines Speicherplatzes direkt oder eines herkömmlichen Hyper-V-Clusters. Bei Cluster Sätzen ist es eine einfache Änderung des Compute-zu-Speicher-Verhältnisses, auch in einem hyperkonvergenten Cluster Satz.

**Frage:** Was sind die Verwaltungs Tools für Cluster Sätze?
**Antwort:** PowerShell oder WMI in dieser Version.

**Frage:** Wie funktioniert die Cluster übergreifende Live Migration mit Prozessoren unterschiedlicher Generationen?
**Antwort:** Cluster Sätze können nicht um Prozessor Unterschiede umgehen und ersetzen, was Hyper-V derzeit unterstützt. Daher muss der Prozessor Kompatibilitätsmodus bei schnellen Migrationen verwendet werden. Die Empfehlung für Cluster Sätze besteht darin, die gleiche Prozessor Hardware in jedem einzelnen Cluster und den gesamten Cluster Satz für Live Migrationen zwischen Clustern zu verwenden.

**Frage:** Kann bei einem Cluster Fehler ein automatisches Failover für virtuelle Computer festgelegt werden?
**Antwort:** In dieser Version können virtuelle Computer für Clustergruppen nur manuell zwischen Clustern Live migriert werden. ein automatisches Failover ist jedoch nicht möglich.

**Frage:** Wie stellen wir sicher, dass der Speicher anfällig für Cluster Ausfälle ist?
**Antwort:** Verwenden Sie die Cluster-Cluster Speicher Replikat Lösung (SR) für Mitglieder Cluster, um die speicherresilienz bei Cluster Fehlern zu erkennen.

**Frage:** Ich verwende Speicher Replikat (SR) für die Replikation über Mitglieder Cluster. Ändern sich die UNC-Pfade für Cluster Satz-Namespace Speicher bei einem SR-Failover auf das Replikat Ziel direkte Speicherplätze Cluster?
**Antwort:** In dieser Version erfolgt eine solche Änderung des Cluster Satz-Namespace Verweises nicht bei einem SR-Failover. Bitte informieren Sie Microsoft, ob dieses Szenario für Sie von entscheidender Bedeutung ist und wie Sie es verwenden möchten.

**Frage:** Ist es möglich, bei einer Notfall Wiederherstellung ein Failover für virtuelle Computer auf Fehler Domänen durchzusetzen (z. h. die gesamte Fehler Domäne ist ausgefallen)?
**Antwort:** Nein, beachten Sie, dass das Cluster übergreifende Failover innerhalb einer logischen Fehler Domäne noch nicht unterstützt wird.

**Frage:** Kann ein Cluster Satz Cluster an mehreren Standorten (oder DNS-Domänen) umfassen?
**Antwort:** Hierbei handelt es sich um ein nicht getesteter Szenario, das nicht sofort für die Produktion vorgesehen ist. Bitte informieren Sie Microsoft, ob dieses Szenario für Sie von entscheidender Bedeutung ist und wie Sie es verwenden möchten.

**Frage:** Funktioniert der Cluster Satz mit IPv6?
**Antwort:** Sowohl IPv4 als auch IPv6 werden bei Cluster Sätzen wie bei Failoverclustern unterstützt.

**Frage:** Was sind die Active Directory Gesamtstruktur Anforderungen für Cluster Sätze?
**Antwort:** Alle Mitglieds Cluster müssen sich in derselben AD-Gesamtstruktur befinden.

**Frage:** Wie viele Cluster oder Knoten können Teil eines einzelnen Cluster Satzes sein?
**Antwort:** In Windows Server 2019 wurden Clustergruppen getestet und bis zu 64 Gesamtzahl der Cluster Knoten unterstützt. Die Architektur von Cluster Sätzen skaliert jedoch auf wesentlich größere Grenzwerte und ist nicht für eine Beschränkung hart codiert. Teilen Sie Microsoft mit, ob größere Skalierbarkeit für Sie von entscheidender Bedeutung ist und wie Sie die Verwendung planen.

**Frage:** Bilden alle direkte Speicherplätze Cluster in einem Cluster Satz einen einzelnen Speicherpool?
**Antwort:** Nein. Direkte Speicherplätze Technologie wird immer noch innerhalb eines einzelnen Clusters und nicht über Mitglieder Cluster in einem Cluster Satz hinweg betrieben.

**Frage:** Ist der Cluster Satz Namespace hoch verfügbar?
**Antwort:** Ja, der Cluster Satz-Namespace wird über einen fortlaufend verfügbaren verweisverweisnamespace

Server (ca) bereitgestellt, der auf dem Verwaltungs Cluster ausgeführt wird. Microsoft empfiehlt, dass Sie über eine ausreichende Anzahl von virtuellen Computern aus Mitglieds Clustern verfügen, damit Sie sich gegen lokalisierte Cluster weite Ausfälle anfällig machen. Um jedoch unvorhergesehene schwerwiegende Fehler zu berücksichtigen – z. b. alle virtuellen Computer im Verwaltungs Cluster gleichzeitig heruntergefahren werden – werden die Verweis Informationen zusätzlich in jedem Cluster Satz Knoten dauerhaft zwischengespeichert, auch bei Neustarts.

**Frage:** Verlangsamt der auf dem Cluster festgelegte Namespace basierte Speicherzugriff die Speicherleistung in einem Cluster Satz.
**Antwort:** Nein. Der clusterset-Namespace bietet einen Überlagerungs-Referenz Namespace in einem Cluster Satz – konzeptionell wie verteiltes Dateisystem Namespaces (DFSN). Und im Gegensatz zu DFSN werden alle clusterset-Namespace-Verweis Metadaten automatisch aufgefüllt und automatisch auf allen Knoten aktualisiert, ohne dass ein Administrator Eingriff ausgeführt wird, sodass der Speicherzugriffs Pfad fast keinen zusätzlichen Leistungs Aufwand erfordert.

**Frage:** Wie kann ich Cluster Satz Metadaten sichern?
**Antwort:** Diese Anleitung ist identisch mit der des Failoverclusters. Mit der System Status Sicherung wird auch der Cluster Status gesichert. Durch Windows Server-Sicherung können Sie eine Wiederherstellung der Cluster Datenbank eines Knotens durchführen (was nie benötigt wird, weil eine Reihe von Selbstkorrektur Logik vorhanden ist) oder eine autorisierende Wiederherstellung durchführen, um ein Rollback für die gesamte Cluster Datenbank über alle Knoten auszuführen. Im Fall von Cluster Sätzen empfiehlt Microsoft, eine solche autorisierende Wiederherstellung zunächst auf dem Mitglieds Cluster und dann auf den Verwaltungs Cluster durchgeführt werden.

# Clusteraffinität

02.05.2020 • 6 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Ein Failovercluster kann zahlreiche Rollen enthalten, die zwischen Knoten wechseln und ausgeführt werden können. Es gibt Zeiten, in denen bestimmte Rollen (z. b. virtuelle Computer, Ressourcengruppen usw.) nicht auf demselben Knoten ausgeführt werden dürfen. Dies kann auf den Ressourcenverbrauch, die Arbeitsspeicher Auslastung usw. zurückzuführen sein. Beispielsweise gibt es zwei virtuelle Computer, die Arbeitsspeicher und CPU-intensiv sind. wenn die beiden virtuellen Computer auf demselben Knoten ausgeführt werden, können sich auf einem oder beiden virtuellen Computern Probleme mit der Leistungs Beeinträchtigung ergeben. In diesem Artikel werden die Cluster-antiaffinitäts Stufen und deren Verwendung erläutert.

## Was ist Affinität und antiaffinität?

Die Affinität ist eine Regel, die Sie einrichten, die eine Beziehung zwischen zwei oder mehr Rollen (i, e, Virtual Machines, Ressourcengruppen usw.) herstellt, um sie zusammenzuhalten. Die antiaffinität ist identisch, wird jedoch verwendet, um zu versuchen, die angegebenen Rollen voneinander getrennt zu halten. Failovercluster verwenden die antiaffinität für Ihre Rollen. Genauer gesagt, ist der AntiAffinityClassNames -Parameter für die Rollen definiert, sodass Sie nicht auf demselben Knoten ausgeführt werden.

## AntiAffinityClassnames

Wenn Sie sich die Eigenschaften einer Gruppe ansehen, gibt es den Parameter AntiAffinityClassNames, der Standardwert ist leer. In den folgenden Beispielen sollten group1 und group2 von der Ausführung auf dem gleichen Knoten getrennt werden. Zum Anzeigen der-Eigenschaft lauten der PowerShell-Befehl und das-Ergebnis wie folgt:

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

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

Da "AntiAffinityClassNames" nicht als Standard definiert ist, können diese Rollen gleichzeitig ausgeführt werden. Das Ziel besteht darin, diese getrennt zu halten. Der Wert für "AntiAffinityClassNames" kann der gewünschte Wert sein. Sie müssen lediglich identisch sein. Das heißt, group1 und group2 sind Domänen Controller, die auf virtuellen Computern ausgeführt werden und am besten auf verschiedenen Knoten ausgeführt werden. Da es sich hierbei um Domänen Controller handelt, verwende ich DC als Klassenname. Um den Wert festzulegen, lauten der PowerShell-Befehl und die folgenden Ergebnisse:

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

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

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

Nachdem Sie festgelegt wurden, versucht das Failoverclustering, Sie zu trennen.

Der antiaffinityclassname-Parameter ist ein "Soft"-Block. Das heißt, es wird versucht, Sie zu trennen, aber wenn dies nicht möglich ist, können Sie es dennoch auf demselben Knoten ausführen. Beispielsweise werden die Gruppen auf einem Failovercluster mit zwei Knoten ausgeführt. Wenn ein Knoten für die Wartung Herunterfahren muss, bedeutet dies, dass beide Gruppen auf demselben Knoten ausgeführt werden. In diesem Fall wäre es in Ordnung, dies zu tun. Dies ist möglicherweise nicht die ideale, aber beide virtial Computer werden weiterhin in akzeptablen Leistungsbereichen ausgeführt.

## Ich benötige weitere

Wie bereits erwähnt, ist AntiAffinityClassNames ein weicher Block. Aber was ist, wenn eine harte Blockierung erforderlich ist? Die virtuellen Maschinen können nicht auf demselben Knoten ausgeführt werden. Andernfalls treten Leistungseinbußen auf und bewirken, dass einige Dienste möglicherweise ausfallen.

In diesen Fällen ist eine zusätzliche Cluster Eigenschaft von clusterenforcedantiaffinität vorhanden. Diese antiaffinitäts Ebene verhindert, dass alle gleichen AntiAffinityClassNames-Werte auf demselben Knoten ausgeführt werden.

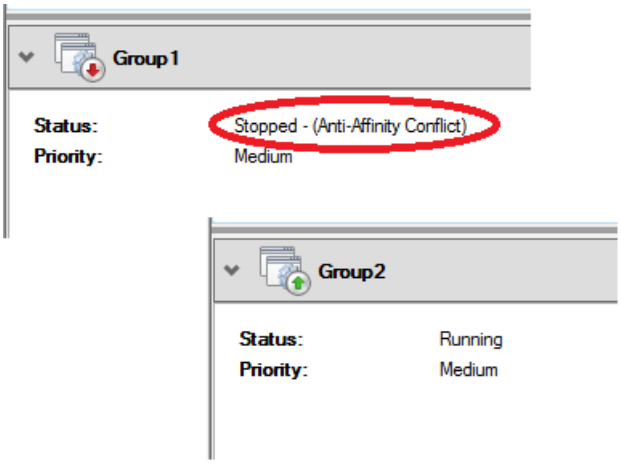
Zum Anzeigen der Eigenschaft und des Werts lautet der PowerShell-Befehl (und das Ergebnis) wie folgt:

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

Der Wert "0" bedeutet, dass er deaktiviert ist und nicht erzwungen werden soll. Der Wert "1" aktiviert dies und ist der feste Block. Zum Aktivieren dieser festen Blockierung lautet der Befehl (und das Ergebnis) wie folgt:

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

Wenn beide festgelegt sind, wird verhindert, dass die Gruppe online geschaltet wird. Wenn Sie sich auf demselben Knoten befinden, werden Sie in Failovercluster-Manager angezeigt.




In einer PowerShell-Auflistung der Gruppen würden Sie Folgendes sehen:

```
PS> Get-ClusterGroup

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

## Zusätzliche Kommentare

- Stellen Sie sicher, dass Sie die richtige antiaffinitäts Einstellung abhängig von den Anforderungen verwenden.
- Beachten Sie, dass in einem Szenario mit zwei Knoten und clusterenforcedantiaffinität, wenn ein Knoten instand ist, beide Gruppen nicht ausgeführt werden.
- Die Verwendung bevorzugter Besitzer für Gruppen kann mit der antiaffinität in einem Cluster mit drei oder mehr Knoten kombiniert werden.
- Die Einstellungen für "AntiAffinityClassNames" und "clusterenforcedantiaffinität" werden erst nach der Wiederverwendung der Ressourcen ausgeführt. Das heißt, Sie können diese festlegen, aber wenn beide Gruppen auf dem gleichen Knoten online sind, wenn Sie festgelegt sind, bleiben beide weiterhin online.

# Hardwareanforderungen und Speicheroptionen für Failoverclustering

09.04.2020 • 10 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Zum Erstellen eines Failoverclusters benötigen Sie die folgende Hardware. Die Unterstützung durch Microsoft setzt voraus, dass alle Hardware für die ausgeführte Version von Windows Server zertifiziert ist und die komplette Failoverclusterlösung alle Tests im Konfigurationsüberprüfungs-Assistenten besteht. Weitere Informationen zum Überprüfen eines Failoverclusters finden Sie unter Überprüfen der Hardware für einen Failovercluster.

- **Server**: Wir empfehlen, eine Reihe übereinstimmender PCs mit identischen oder ähnlichen Komponenten zu verwenden.
- **Netzwerkadapter und -kabel (für die Netzwerkkommunikation)** : Wenn Sie iSCSI verwenden, sollte jeder Netzwerkadapter entweder für die Netzwerkkommunikation oder für iSCSI zugewiesen werden, aber nicht für beides.

  Vermeiden Sie in der Netzwerkinfrastruktur, über die die Clusterknoten verbunden sind, die Verwendung von Komponenten, deren Ausfall einen Ausfall des Gesamtsystems zur Folge hätte. Sie können die Clusterknoten z. B. durch mehrere unterschiedliche Netzwerke verbinden. Alternativ können Sie Ihre Cluster Knoten mit einem Netzwerk verbinden, das mit kombinierten Netzwerkadaptern, redundanten Switches, redundanten Routern oder ähnlicher Hardware erstellt wird, die einzelne Fehlerquellen entfernt.

  > **NOTE**
  > Wenn Sie Clusterknoten nur mit einem Netzwerk verbinden, erfüllt das Netzwerk die Redundanzanforderung des Konfigurationsüberprüfungs-Assistenten. Der Bericht des Assistenten enthält aber eine Warnung, dass das Netzwerk keine einzelnen Fehlerpunkte enthalten sollte.

- **Gerätecontroller oder entsprechende Adapter für den Speicher**:
  - **Serial Attached SCSI oder Fibre Channel**: Wenn Sie Serial Attached SCSI oder Fibre Channel verwenden, sollten alle Elemente des Speicherstapels in allen Clusterservern identisch sein. Es ist erforderlich, dass die Multipfad-e/a-Software (MPIO) identisch ist und dass die DSM-Software (Device Specific Module) identisch ist. Es wird empfohlen, dass die Massenspeichergeräte-Controller – der Hostbus Adapter (HBA), HBA-Treiber und HBA-Firmware – identisch sind, die an den Cluster Speicher angefügt sind. Wenn Sie unterschiedliche HBAs verwenden, sollten Sie gemeinsam mit dem Speicheranbieter überprüfen, ob die unterstützten oder empfohlenen Konfigurationen eingehalten werden.
  - **iSCSI**: Wenn Sie iSCSI verwenden, sollte jeder Clusterserver über mindestens einen Netzwerkadapter oder HBA verfügen, der dem Clusterspeicher zugewiesen ist. Das für iSCSI verwendete Netzwerk sollte nicht für die Netzwerkkommunikation verwendet werden. Die zum Herstellen von Verbindungen mit dem iSCSI-Speicherziel verwendeten Netzwerkadapter müssen für alle Clusterserver identisch sein, und es empfiehlt sich, Gigabit Ethernet oder höher zu verwenden.
- **Speicher**: Sie müssen direkte Speicherplätze oder freigegebenen Speicher verwenden, der mit Windows Server 2012 R2 oder Windows Server 2012 kompatibel ist. Sie können freigegebenen Speicher verwenden, der angefügt ist, und Sie können auch SMB 3,0-Dateifreigaben als freigegebenen Speicher für Server verwenden, die Hyper-V ausführen und in einem Failovercluster konfiguriert sind. Weitere Informationen

finden Sie unter Bereitstellen von Hyper-V über SMB.

In den meisten Fällen sollte der angeschlossene Speicher mehrere separate, auf Hardwareebene konfigurierte Datenträger (logische Gerätenummern bzw. LUNs) enthalten. In einigen Clustern fungiert ein Datenträger als Datenträgerzeuge (siehe Beschreibung am Ende dieses Unterabschnitts). Andere Datenträger enthalten die erforderlichen Dateien für die Clusterrollen (früher bezeichnet als Clusterdienste oder -anwendungen). Die Speicheranforderungen beinhalten Folgendes:

- Um die systemeigene, im Failoverclustering enthaltene Datenträgerunterstützung verwenden zu können, müssen anstelle von dynamischen Datenträgern Basisdatenträger verwendet werden.
- Es wird empfohlen, die Partitionen mit NTFS zu formatieren. Wenn Sie freigegebene Clustervolumes (CSVs) verwenden, müssen diese jeweils über NTFS-Partitionen verfügen.

  > **NOTE**
  > Wenn Sie für Ihre Quorumkonfiguration über einen Datenträgerzeugen verfügen, können Sie den Datenträger entweder mit NTFS oder ReFS (Resilient File System) formatieren.

- Als Partitionsstil des Datenträgers können Sie entweder MBR (Master Boot Record) oder GPT (GUID-Partitionstabelle) verwenden.

  Ein Datenträger Zeuge ist ein Datenträger im Cluster Speicher, der eine Kopie der Cluster Konfigurations Datenbank enthalten soll. Ein Failovercluster besitzt nur dann einen Zeugendatenträger, wenn dies als Teil der Quorumkonfiguration angegeben ist. Weitere Informationen finden Sie Untergrund Legendes zu Quorum in direkte Speicherplätze.

## Hardwareanforderungen für Hyper-V

Wenn Sie einen Failovercluster erstellen, der virtuelle Clustercomputer einbezieht, müssen die Clusterserver die Hardwareanforderungen für die Hyper-V-Rolle unterstützen. Für Hyper-V ist ein 64-Bit-Prozessor erforderlich, der Folgendes einschließt:

- Hardwareunterstützte Virtualisierung. Diese ist für Prozessoren mit Virtualisierungsoption verfügbar, insbesondere für Prozessoren mit Intel VT (Intel Virtualization Technology)- oder AMD-V (AMD Virtualization)-Technologie.
- Von der Hardware erzwungene Datenausführungsverhinderung (DEP) muss verfügbar und aktiviert sein. Das heißt, Sie müssen Intel XD-Bit (Execute Disable Bit) oder AMD NX-Bit (No Execute Bit) aktivieren.

Weitere Informationen zur Hyper-v-Rolle finden Sie unter Hyper-v Overview (Übersicht über Hyper-v).

## Bereitstellen von SANs (Storage Area Networks) mit Failoverclustern

Befolgen Sie die folgenden Richtlinien, wenn Sie ein SAN mit einem Failovercluster bereitstellen:

- Überprüfen Sie **die Kompatibilität des Speichers**: Vergewissern Sie sich bei Herstellern und Anbietern, dass der Speicher einschließlich der für den Speicher verwendeten Treiber, Firmware und Software mit Failoverclustern in der Windows Server-Version kompatibel ist, die Sie ausführen.
- **Isolieren Sie Speichergeräte – ein Cluster pro Gerät**: Server aus unterschiedlichen Clustern dürfen keinen Zugriff auf die gleichen Speichergeräte haben. In den meisten Fällen muss eine LUN, die für eine Gruppe mit Clusterservern verwendet wird, durch LUN-Masking oder -Zonen von allen anderen Servern isoliert werden.
- **Verwenden Sie ggf. Multipfad-E/A-Software oder ein Netzwerkadapterteam**: In einem Speicherfabric mit hoher Verfügbarkeit können Sie Failovercluster mithilfe von Multipfad-E/A-Software oder

eines Netzwerkadapterteams (auch als Lastenausgleich und Failover oder LBFO bezeichnet) mit mehreren Hostbusadaptern bereitstellen. Auf diese Weise erhalten Sie den höchsten Grad an Redundanz und Verfügbarkeit. Für Windows Server 2012 R2 oder Windows Server 2012 muss die Multipfadlösung auf Microsoft Multipfad-e/a (MPIO) basieren. Die meisten Hardwarehersteller stellen ein gerätespezifisches MPIO-Modul (DSM) für die Hardware bereit, obwohl Windows Server mindestens ein DSM als Bestandteil des Betriebssystems enthält.

Weitere Informationen zu LBFO finden Sie unter NIC Teaming Overview in der technischen Bibliothek für Windows Server.

> **IMPORTANT**
>
> Bei Hostbusadaptern und der MPIO-Software muss möglicherweise genau auf die Version geachtet werden. Wenn Sie für Ihren Cluster eine Multipfadlösung implementieren, sollten Sie die richtigen Adapter sowie die Firm- und Software für die von Ihnen ausgeführte Version von Windows Server in enger Zusammenarbeit mit dem Hardwarehersteller auswählen.

- **Verwenden Sie die Verwendung von Speicherplätzen**: Wenn Sie planen, den mit Speicherplätzen konfigurierten SAS-Cluster Speicher (Serial Attached SCSI) bereitzustellen, finden Sie unter Bereitstellen von Cluster Speicherplätzen die Anforderungen.

## Weitere Informationen

- Failoverclustering
- Speicherplätze
- Verwenden von Gastclustering für hohe Verfügbarkeit

# Verwenden von freigegebenen Clustervolumes in einem Failovercluster

09.04.2020 • 38 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2

Mit freigegebenen Clustervolumes (Cluster Shared Volumes, CSVs) können mehrere Knoten in einem Failovercluster gleichzeitig über den Lese-/Schreibzugriff auf dieselbe LUN (Datenträger) verfügen, die als NTFS-Volume bereitgestellt wird. (In Windows Server 2012 R2 kann der Datenträger als NTFS oder robustes Datei System (Refs) bereitgestellt werden.) Bei CSV können Cluster Rollen schnell ein Failover von einem Knoten zu einem anderen Knoten ausführen, ohne dass eine Änderung des Laufwerks Besitzes erforderlich ist oder ein Volume getrennt und bereitgestellt wird. Freigegebene Clustervolumes vereinfachen auch die Verwaltung einer möglicherweise großen Anzahl von LUNs in einem Failovercluster.

CSV stellen ein allgemeines Cluster Dateisystem bereit, das über NTFS (oder Refs in Windows Server 2012 R2) geschichtet ist. CSV-Anwendungen umfassen Folgendes:

- VHD-Clusterdateien für virtuelle Hyper-V-Clustercomputer
- Dateifreigaben mit horizontaler Skalierung zum Speichern von Anwendungsdaten für die Clusterrolle „Dateiserver mit horizontaler Skalierung“. Beispiele für die Anwendungsdaten dieser Rolle umfassen Dateien von virtuellen Hyper-V-Computern und Microsoft SQL Server-Daten. (Beachten Sie, dass Refs für eine Dateiserver mit horizontaler Skalierung nicht unterstützt wird.) Weitere Informationen zu Dateiserver mit horizontaler Skalierung finden Sie unter Dateiserver mit horizontaler Skalierung für Anwendungsdaten.

> **NOTE**
> Csvs unterstützen die Microsoft SQL Server gruppierten Arbeits Auslastungen in SQL Server 2012 und früheren Versionen von SQL Server nicht.

In Windows Server 2012 wurde die CSV-Funktionalität erheblich verbessert. Abhängigkeiten von Active Directory-Domänendiensten wurden z. B. entfernt. Für die funktionalen Verbesserungen in **chkdsk**, für die Interoperabilität mit Antiviren- und Sicherungsanwendungen sowie für die Integration mit allgemeinen Speicherfeatures wie BitLocker-verschlüsselte Volumes und Speicherplätze wurde die entsprechende Unterstützung hinzugefügt. Eine Übersicht über die CSV-Funktionalität, die in Windows Server 2012 eingeführt wurde, finden Sie unter What es New in Failover Clustering in Windows Server 2012 [umgeleitet].

Windows Server 2012 R2 bietet zusätzliche Funktionen, wie z. b. den verteilten CSV-Besitz, eine erhöhte Resilienz durch die Verfügbarkeit des Server dienstanbietes, eine größere Flexibilität bei der Menge an physischem Speicher, die Sie dem CSV-Cache zuweisen können, eine bessere Diagnose und eine verbesserte Interoperabilität, die Unterstützung für Refs und Deduplizierung umfasst. Weitere Informationen finden Sie unter Neues beim Failoverclustering.

> **NOTE**
> Informationen zur Verwendung der Datendeduplizierung auf freigegebenen Clustervolumes für VDI-Szenarien (Virtual Desktop Infrastructure) finden Sie in den Blogbeiträgen Deploying Data Deduplication for VDI storage in Windows Server 2012 R2 und Extending Data Deduplication to new workloads in Windows Server 2012 R2(beide in englischer Sprache).

# Überprüfen der Anforderungen und Überlegungen zur Verwendung von CSV in einem Failovercluster

Bevor Sie freigegebene Clustervolumes (CSV) in einem Failovercluster verwenden, lesen Sie die Anforderungen und Überlegungen zum Netzwerk, Speicher und anderen Komponenten in diesem Abschnitt.

**Überlegungen zur Netzwerkkonfiguration**

Berücksichtigen Sie Folgendes, wenn Sie die Netzwerke konfigurieren, die freigegebene Clustervolumes unterstützen.

- **Mehrere Netzwerke und Netzwerkadapter**: Es wird empfohlen, dass mehrere Clusternetzwerke den CSV-Datenverkehr übernehmen oder Sie kombinierte Netzwerkadapter konfigurieren, um im Falle eines Netzwerkfehlers die entsprechende Fehlertoleranz bereitzustellen.

  Wenn die Clusterknoten mit Netzwerken verbunden sind, die vom Cluster nicht verwendet werden sollten, können Sie diese Netzwerke deaktivieren. Es wird z. B. empfohlen, dass Sie iSCSI-Netzwerke für Cluster deaktivieren, um CSV-Datenverkehr in diesen Netzwerken zu verhindern. Klicken Sie zum Deaktivieren eines Netzwerks in Failovercluster-Manager auf **Netzwerke**, wählen Sie das Netzwerk aus, wählen Sie die Aktion **Eigenschaften** aus, und wählen Sie dann **Netzwerkkommunikation für Cluster in diesem Netzwerk nicht zulassen**. Alternativ können Sie die **Role** -Eigenschaft des Netzwerks mithilfe des Windows PowerShell-Cmdlets Get-ClusterNetwork konfigurieren.

- **Netzwerkadaptereigenschaften** Stellen Sie in den Eigenschaften für alle Adapter, die für die Clusterkommunikation zuständig sind, sicher, dass die folgenden Einstellungen aktiviert sind:

  - **Client für Microsoft-Netzwerke** und **Datei- und Druckerfreigabe für Microsoft-Netzwerke**: Diese Einstellungen unterstützen SMB 3.0 (Server Message Block), mit dem standardmäßig der CSV-Datenverkehr zwischen den Knoten übertragen wird. Stellen Sie zum Aktivieren von SMB außerdem sicher, dass der Server- und der Arbeitsstationsdienst aktiv sind und diese auf den einzelnen Clusterknoten für den automatischen Start konfiguriert sind.

    > **NOTE**
    >
    > In Windows Server 2012 R2 gibt es mehrere Server Dienst Instanzen pro Failoverclusterknoten. Es gibt eine Standardinstanz, die den eingehenden Datenverkehr von SMB-Clients bearbeitet, die auf normale Dateifreigaben zugreifen. Dann gibt es noch eine zweite CSV-Instanz, die ausschließlich den CSV-Datenverkehr zwischen den Knoten bearbeitet. Wenn der Serverdienst auf einem Knoten Fehler aufweist, wechselt das CSV-Besitzrecht automatisch zu einem anderen Knoten.

    SMB 3.0 umfasst die Features SMB Multichannel und SMB Direct, sodass CSV-Datenverkehr über mehrere Netzwerke im Cluster gestreamt und Netzwerkadapter genutzt werden können, die Remotezugriff auf den direkten Speicher (Remote Direct Memory Access, RDMA) unterstützen. SMB Multichannel wird standardmäßig für den CSV-Datenverkehr verwendet. Weitere Informationen finden Sie unter Server Message Block – Übersicht

  - **Microsoft Failover Cluster Virtual Adapter Performance Filter**: Diese Einstellung verbessert die Möglichkeit von Knoten, eine E/A-Umleitung auszuführen, wenn diese erforderlich ist, um freigegebene Clustervolumes zu erreichen, z. B. wenn Verbindungsfehler einen Knoten daran hindern, eine direkte Verbindung zum CSV-Datenträger herzustellen. Weitere Informationen finden Sie weiter unten in diesem Thema unter Informationen zur e/a-Synchronisierung und e/a-Umleitung bei der CSV-Kommunikation .

- **Clusternetzwerkpriorisierung**: Im Allgemeinen wird empfohlen, dass Sie die für den Cluster konfigurierten Voreinstellungen für die Netzwerke nicht ändern.

- **IP-Subnetzkonfiguration**: Für Knoten in einem Netzwerk, in dem freigegebene Clustervolumes verwendet werden, ist keine bestimmte Subnetzkonfiguration erforderlich. Freigegebene Clustervolumes (CSV) können Cluster mit mehreren Subnetzen unterstützen.

- **Richtlinienbasierter QoS (Quality of Service)** : Es wird empfohlen, dass Sie für jeden Knoten eine QoS-Prioritätenrichtlinie und eine Richtlinie für die Mindestbandbreite für den Netzwerkverkehr konfigurieren, wenn Sie CSV verwenden. Weitere Informationen finden Sie unter Quality of Service (QoS).

- **Speichernetzwerk**: Empfehlungen zum Speichernetzwerk finden Sie in den Anleitungen Ihres Speicheranbieters. Weitere Überlegungen zum Speicher für CSV finden Sie unter Anforderungen an die Speicher-und Datenträger Konfiguration weiter unten in diesem Thema.

Eine Übersicht über die Hardware-, Netzwerk- und Speicheranforderungen für Failovercluster finden Sie unter Hardwareanforderungen und Speicheroptionen für das Failoverclustering.

**Informationen zur E/A-Synchronisierung und E/A-Umleitung bei der CSV-Kommunikation**

- E **/a-Synchronisierung**: CSV ermöglicht mehreren Knoten den gleichzeitigen Lese-/Schreibzugriff auf denselben freigegebenen Speicher. Wenn ein Knoten Datenträgereingaben/-ausgaben (E/A) für ein CSV-Volume ausführt, kommuniziert der Knoten direkt mit dem Speicher, z. B. über ein SAN (Storage Area Network). Zu jedem Zeitpunkt ist jedoch ein einzelner Knoten (als koordinatorknoten bezeichnet) "Besitzer" der physischen Datenträger Ressource, die der LUN zugeordnet ist. Der Koordinatorknoten für ein CSV-Volume wird im Failovercluster-Manager unter **Datenträger** als **Besitzerknoten** angezeigt. Sie wird auch in der Ausgabe des Windows PowerShell-Cmdlets Get-clustersharedvolume angezeigt.

  > **NOTE**
  > In Windows Server 2012 R2 ist der CSV-Besitz gleichmäßig auf die Failoverclusterknoten verteilt, basierend auf der Anzahl der CSV-Volumes, die für die einzelnen Knoten gehören. Zudem wird das Besitzrecht automatisch ausgeglichen, wenn z. B. folgende Bedingungen auftreten: CSV-Failover, ein Knoten wird dem Cluster erneut hinzugefügt, ein Knoten wird zum Cluster hinzugefügt, ein Clusterknoten wird neu gestartet, der Failovercluster wird nach dem Herunterfahren wieder gestartet.

  Wenn im Dateisystem auf einem CSV-Volume bestimmte kleinere Änderungen auftreten, müssen diese Metadaten nicht nur auf dem Koordinatorknoten, sondern auf den einzelnen physischen Knoten synchronisiert werden, die auf die LUN zugreifen. Wenn z. B. ein virtueller Computer auf einem CSV-Volume gestartet, erstellt, gelöscht oder migriert wird, müssen diese Informationen auf den einzelnen physischen Knoten synchronisiert werden, die auf den virtuellen Computer zugreifen. Diese Metadatenaktualisierungen werden in den Clusternetzwerken mithilfe von SMB 3.0 gleichzeitig ausgeführt. Für diese Vorgänge ist es nicht erforderlich, dass alle physischen Knoten mit dem freigegebenen Speicher kommunizieren.

- E/a- **Umleitung**: Speicher Verbindungsfehler und bestimmte Speichervorgänge können verhindern, dass ein bestimmter Knoten direkt mit dem Speicher kommuniziert. Um die Funktion aufrechtzuerhalten, während der Knoten nicht mit dem Speicher kommuniziert, leitet der Knoten die Datenträger-E/A über ein Clusternetzwerk an den Koordinatorknoten weiter, von dem der Datenträger derzeit bereitgestellt wird. Wenn auf dem aktuellen Koordinatorknoten ein Verbindungsfehler aufgetreten ist, werden alle E/A-Vorgänge des Datenträgers vorübergehend in eine Warteschlange gestellt, während ein neuer Knoten als Koordinatorknoten eingerichtet wird.

Der Server verwendet in Abhängigkeit von der Situation einen der folgenden E/A-Umleitungsmodi:

- **Dateisystemumleitung** Die Umleitung erfolgt pro Volume, wenn z. B. von einer Sicherungsanwendung CSV-Snapshots erstellt werden, sobald ein CSV-Volume manuell in den Modus „E/A-Umleitung“ versetzt wird.
- **Blockumleitung** Die Umleitung erfolgt auf Dateiblockebene, wenn z. B. die Speicherverbindung zu einem Volume unterbrochen wird. Die Blockumleitung erweist sich im Vergleich zur Dateisystemumleitung als wesentlich schneller.

In Windows Server 2012 R2 können Sie den Status eines CSV-Volumes auf Knoten Basis anzeigen. Sie können z. B. erkennen, ob die E/A-Vorgänge direkt oder umgeleitet erfolgen, oder ob das CSV-Volume möglicherweise nicht verfügbar ist. Wenn sich ein CSV-Volume im E/A-Umleitungsmodus befindet, wird auch der Grund hierfür angezeigt. Verwenden Sie das Windows PowerShell-Cmdlet **Get-ClusterSharedVolumeState**, um diese Informationen anzuzeigen.

> **NOTE**
>
> - In Windows Server 2012 führen CSV aufgrund von Verbesserungen beim CSV-Entwurf mehr Vorgänge im direkten e/a-Modus aus als in Windows Server 2008 R2.
> - Aufgrund der Integration von CSV mit SMB 3.0-Features wie SMB Multichannel und SMB Direct kann der umgeleitete E/A-Datenverkehr über mehrere Clusternetzwerke geleitet werden.
> - Sie sollten für Ihre Clusternetzwerke während der E/A-Umleitung eine mögliche Zunahme des Netzwerkdatenverkehrs zum Koordinatorknoten berücksichtigen.

**Anforderungen an die Speicher- und Datenträgerkonfiguration**

Der Speicher und die Datenträger müssen zur Verwendung von CSV die folgenden Anforderungen erfüllen:

- **Dateisystemformat**: In Windows Server 2012 R2 muss ein Datenträger oder ein Speicherplatz für ein CSV-Volume ein Basis Datenträger sein, der mit NTFS oder Refs partitioniert ist. In Windows Server 2012 muss ein Datenträger oder ein Speicherplatz für ein CSV-Volume ein Basis Datenträger sein, der mit NTFS partitioniert ist.

  Ein freigegebenes Clustervolume hat die folgenden zusätzlichen Anforderungen:

  - In Windows Server 2012 R2 können Sie keinen Datenträger für eine CSV-Datei verwenden, die mit FAT oder FAT32 formatiert ist.
  - In Windows Server 2012 können Sie keinen Datenträger für eine CSV-Datei verwenden, die mit FAT, FAT32 oder Refs formatiert ist.
  - Wenn Sie Speicherplatz für ein CSV verwenden möchten, können Sie einen einfachen oder einen Spiegelspeicherplatz konfigurieren. In Windows Server 2012 R2 können Sie auch einen Paritäts Speicherplatz konfigurieren. (In Windows Server 2012 werden Paritäts Speicherplätze von CSV nicht unterstützt.)
  - Ein CSV kann nicht als Quorumzeugendatenträger verwendet werden. Weitere Informationen zum Cluster Quorum finden Sie Untergrund Legendes zu Quorum in direkte Speicherplätze.
  - Nachdem Sie einen Datenträger als CSV hinzugefügt haben, wird es im CSVFS-Format (für das CSV-Dateisystem) festgelegt. Dadurch kann der CSV-Speicher vom Cluster und anderer Software vom NTFS- oder ReFS-Speicher unterschieden werden. Im Allgemeinen unterstützt CSVFS dieselbe Funktionalität wie NTFS oder ReFS. Bestimmte Features werden jedoch nicht unterstützt. In Windows Server 2012 R2 können Sie z. b. die Komprimierung für CSV nicht aktivieren. In Windows Server 2012 können Sie die Datendeduplizierung oder Komprimierung für CSV nicht aktivieren.
- **Ressourcentyp im Cluster**: Für ein CSV-Volume müssen Sie den Ressourcentyp „Physischer Datenträger" verwenden. Ein zum Clusterspeicher hinzugefügter Datenträger oder Speicherplatz wird standardmäßig auf diese Weise konfiguriert.

- **Auswahl von CSV- oder anderen Datenträgern im Clusterspeicher**: Berücksichtigen Sie bei der Auswahl eines oder mehrerer Datenträger für einen virtuellen Clustercomputer, wie die einzelnen Datenträger verwendet werden. Wenn ein Datenträger zum Speichern von Dateien verwendet wird, die von Hyper-V erstellt wurden, z. B. VHD-Dateien oder Konfigurationsdateien, können Sie zwischen den CSV-Datenträgern oder den anderen verfügbaren Datenträgern im Clusterspeicher wählen. Wenn ein Datenträger einem physischen Datenträger entspricht, der direkt an den virtuellen Computer angeschlossen ist (auch als Pass-Through-Datenträger bezeichnet), können Sie keinen CSV-Datenträger auswählen. Stattdessen müssen Sie aus den anderen verfügbaren Datenträgern im Clusterspeicher auswählen.

- **Pfadname zum Identifizieren von Datenträgern**: Datenträger werden in CSV über den Pfadnamen identifiziert. Jeder Pfad befindet sich auf dem Systemlaufwerk des Knotens als nummeriertes Volume unter dem **\ClusterStorage** -Ordner. Dieser Pfad ist beim Anzeigen auf jedem anderen Knoten im Cluster gleich. Die Volumes können bei Bedarf umbenannt werden.

Speicheranforderungen für CSV finden Sie in den Anleitungen Ihres Speicheranbieters. Weitere Überlegungen zur Speicherplanung für CSV finden Sie weiter unten in diesem Thema unter Planen der Verwendung von CSV in einem Failovercluster.

**Knotenanforderungen**

Die Knoten müssen zur Verwendung von CSV die folgenden Anforderungen erfüllen:

- **Laufwerkbuchstabe des Systemdatenträgers**. Der Laufwerkbuchstabe für den Systemdatenträger muss auf allen Knoten identisch sein.
- **Authentifizierungsprotokoll**. Das NTLM-Protokoll muss auf allen Knoten aktiviert werden. Dieses Verhalten ist standardmäßig aktiviert.

## Planen der Verwendung von CSV in einem Failovercluster

In diesem Abschnitt werden Planungsüberlegungen und Empfehlungen für die Verwendung von CSV in einem Failovercluster mit Windows Server 2012 R2 oder Windows Server 2012 aufgeführt.

> **IMPORTANT**
>
> Fragen Sie Ihren Speicheranbieter, um Empfehlungen zur Konfiguration Ihrer Speichereinheit für CSV zu erhalten. Wenn die Empfehlungen des Speicheranbieters von den Informationen in diesem Thema abweichen, richten Sie sich nach den Empfehlungen des Speicheranbieters.

**Anordnung von LUNs, Volumes und VHD-Dateien**

Um CSV optimal zur Bereitstellung von Speicher für virtuelle Clustercomputer zu nutzen, ist es hilfreich, die Anordnung der LUNs (Datenträger) beim Konfigurieren der physischen Server zu überprüfen. Wenn Sie die entsprechenden virtuellen Computer konfigurieren, versuchen Sie, die VHD-Dateien auf ähnliche Weise anzuordnen.

Betrachten Sie einen physischen Server, für den Sie die Datenträger und Dateien organisieren möchten, wie folgt:

- Systemdateien, einschließlich einer Auslagerungsdatei, auf einem physischen Datenträger
- Dateidateien auf einem anderen physischen Datenträger

Für einen ähnlichen virtuellen Clustercomputer sollten Sie die Volumes und Dateien auf ähnliche Weise anordnen:

- Systemdateien, einschließlich einer Auslagerungsdatei, in einer VHD-Datei auf einem CSV
- Datendateien in einer VHD-Datei auf einem anderen CSV

Wenn Sie einen weiteren virtuellen Computer hinzufügen, sollten Sie dieselbe Anordnung für die VHD-Dateien auf diesem virtuellen Computer beibehalten (falls möglich).

**Anzahl und Größe von LUNs und Volumes**

Wenn Sie die Speicherkonfiguration für einen Failovercluster planen, der CSV verwendet, berücksichtigen Sie die folgenden Empfehlungen:

- Wenden Sie sich an Ihren Speicheranbieter, um zu entscheiden, wie viele LUNs konfiguriert werden müssen. Ihr Speicheranbieter kann z. B. empfehlen, dass Sie jede LUN mit einer Partition konfigurieren, auf die ein CSV-Volume platziert wird.

- Es gibt keine Einschränkungen hinsichtlich der Anzahl der virtuellen Computer, die auf einem einzelnen

CSV-Volume unterstützt werden können. Sie sollten jedoch die Anzahl der virtuellen Computer, die für den Cluster geplant sind, und die Arbeitsauslastung (E/A-Vorgänge pro Sekunde) für die einzelnen virtuellen Computer berücksichtigen. Beachten Sie folgende Beispiele:

  - Eine Organisation stellt virtuelle Computer bereit, die eine virtuelle Desktopinfrastruktur (VDI) unterstützen, die eine relativ gemäßigte Arbeitsauslastung aufweist. Der Cluster verwendet leistungsstarken Speicher. Der Clusteradministrator entscheidet sich nach der Rückfrage beim Speicheranbieter dazu, eine relativ große Anzahl von virtuellen Computern auf den einzelnen CSV-Volumes zu platzieren.
  - Eine andere Organisation stellt eine große Anzahl von virtuellen Computern bereit, die eine stark beanspruchte Datenbankanwendung und somit eine stärkere Arbeitsauslastung unterstützen. Der Cluster verwendet weniger leistungsstarken Speicher. Der Clusteradministrator entscheidet sich nach der Rückfrage beim Speicheranbieter dazu, eine relativ kleine Anzahl von virtuellen Computern auf den einzelnen CSV-Volumes zu platzieren.

- Wenn Sie die Speicherkonfiguration für einen bestimmten virtuellen Computer planen, berücksichtigen Sie die Datenträgeranforderungen des Diensts, der Anwendung oder der Rolle, die vom virtuellen Computer unterstützt werden. Sie können Datenträgerkonflikte besser vermeiden, die zu schlechten Leistungen führen können, wenn Sie diese Anforderungen verstehen. Die Speicherkonfiguration für den virtuellen Computer sollte stark der Speicherkonfiguration ähneln, die Sie für einen physischen Server verwenden würden, der denselben Dienst, dieselbe Anwendung oder dieselbe Rolle ausführt. Weitere Informationen finden Sie weiter oben in diesem Thema unter Anordnung von LUNs, Volumes und VHD-Dateien .

  Sie können Datenträgerkonflikte auch dadurch reduzieren, dass Sie Speicher mit einer großen Anzahl von unabhängigen physischen Festplatten verwenden. Wählen Sie Ihre Speicherhardware entsprechend aus, und wenden Sie sich an den Anbieter, um die Leistung des Speichers zu optimieren.

- In Abhängigkeit von Ihrer Clusterarbeitsauslastung und dem entsprechenden Bedarf an E/A-Vorgängen können Sie erwägen, dass Sie nur einen Teil der virtuellen Computer für den Zugriff auf die einzelnen LUNs konfigurieren, während andere virtuelle Computer keine Verbindungen aufweisen und stattdessen zur Berechnung von Operationen vorgesehen sind.

# Hinzufügen von Datenträgern zum CSV auf einem Failovercluster

Das CSV-Feature ist für das Failoverclustering standardmäßig aktiviert. Wenn Sie einen Datenträger zum freigegebenen Clustervolume (CSV) hinzufügen möchten, müssen Sie einen Datenträger zur Gruppe **Verfügbarer Speicher** des Clusters hinzufügen (sofern er nicht bereits hinzugefügt wurde) und dann den Datenträger zum CSV auf dem Cluster hinzufügen. Sie können Failovercluster-Manager oder die Windows PowerShell-Cmdlets für Failovercluster verwenden, um diese Prozeduren auszuführen.

**Hinzufügen eines Datenträgers zum verfügbaren Speicher**

1. Erweitern Sie im Failovercluster-Manager in der Konsolenstruktur den Namen des Clusters, und erweitern Sie dann die Option **Speicher**.

2. Klicken Sie mit der rechten Maustaste auf Daten **Träger und dann**auf Datenträger **Hinzufügen** Es wird eine Liste mit den Datenträgern angezeigt, die zu einem Failovercluster hinzugefügt werden können.

3. Wählen Sie die Datenträger aus, die Sie hinzufügen möchten, und klicken Sie dann auf **OK**.

   Diese Datenträger werden jetzt zur Gruppe **Verfügbarer Speicher** zugeordnet.

**Äquivalente Windows PowerShell-Befehle (Hinzufügen eines Datenträgers zum verfügbaren Speicher)**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

Im folgenden Beispiel werden die Datenträger identifiziert, die zum Cluster hinzugefügt werden können, und diese

dann zur Gruppe **Verfügbarer Speicher** hinzugefügt.

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

**Hinzufügen eines Datenträgers im verfügbaren Speicher zum CSV**

1. Erweitern **Sie in** Failovercluster-Manager in der Konsolen Struktur den Namen des Clusters, erweitern Sie **Speicher**, und wählen Sie dann Datenträger aus.

2. Wählen Sie mindestens einen Datenträger aus, der dem **verfügbaren Speicher** zugewiesen ist, klicken Sie mit der rechten Maustaste auf die Auswahl, und wählen Sie dann **zu freigegebenen Clustervolumes**

   Die Datenträger werden jetzt im Cluster zur Gruppe **Freigegebene Clustervolumes** zugewiesen. Die Datenträger werden für die einzelnen Clusterknoten als nummerierte Volumes (Bereitstellungspunkte) unter dem Ordner „%SystemDisk%ClusterStorage“ zur Verfügung gestellt. Die Volumes werden im CSVFS-Dateisystem angezeigt.

> **NOTE**
> Sie können CSV-Volumes im Ordner „%SystemDisk%ClusterStorage“ umbenennen.

**Äquivalente Windows PowerShell-Befehle (Hinzufügen eines Datenträgers zu einem CSV)**

Die folgenden Windows PowerShell-Cmdlets führen dieselbe Funktion wie das vorherige Verfahren aus. Jedes Cmdlet sollte in einer eigenen Zeile eingegeben werden, obwohl sie hier aufgrund von Formateinschränkungen auf mehrere Zeilen umbrochen sein können.

Im folgenden Beispiel wird *Cluster Disk 1* in **Verfügbarer Speicher** zum CSV auf dem lokalen Cluster hinzugefügt.

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

## Aktivieren des CSV-Cache für Auslastungen mit intensiven Lesevorgängen (optional)

Der CSV-Cache ermöglicht das Zwischenspeichern von ungepufferten E/A-Vorgängen auf Blockebene, indem Systemspeicher (RAM) als Durchschreibcache zugewiesen wird. (Nicht gepufferte e/a-Vorgänge werden nicht vom Cache-Manager zwischengespeichert.) Dies kann die Leistung für Anwendungen wie Hyper-V verbessern, die nicht gepufferte e/a-Vorgänge für den Zugriff auf eine VHD durchführt. Der CSV-Cache kann die Leistung von Leseanforderungen verstärken, ohne Schreibanforderungen zwischenzuspeichern. Das Aktivieren des CSV-Cache ist auch für Dateiserverszenarien mit horizontaler Skalierung hilfreich.

> **NOTE**
> Es wird empfohlen, dass Sie den CSV-Cache für alle geclusterten Hyper-V- und Dateiserverbereitstellungen mit horizontaler Skalierung aktivieren.

In Windows Server 2012 ist der CSV-Cache standardmäßig deaktiviert. In Windows Server 2012 R2 und höher ist der CSV-Cache standardmäßig aktiviert. Sie müssen jedoch weiterhin die Größe des zu reservierenden Blockcache zuweisen.

In der folgenden Tabelle werden die beiden Konfigurationseinstellungen beschrieben, die den CSV-Cache steuern.

| WINDOWS SERVER 2012 R2 UND HÖHER | WINDOWS SERVER 2012 | BESCHREIBUNG |
|---|---|---|
| BlockCacheSize | SharedVolumeBlockCacheSizeInMB | Dies ist eine allgemeine Clustereigenschaft, mit der Sie festlegen können, wie viel Systemspeicher (in Megabytes) für den CSV-Cache auf den einzelnen Knoten im Cluster reserviert wird. Wenn Sie z. B. den Wert „512“ festlegen, werden 512 MB des Systemspeichers auf jedem Knoten reserviert. (In vielen Clustern ist 512 MB ein empfohlener Wert.) Die Standardeinstellung ist 0 (deaktiviert). |
| EnableBlockCache | CsvEnableBlockCache | Dies ist eine private Eigenschaft der physischen Datenträgerressource des Clusters. Mit dieser Eigenschaft können Sie den CSV-Cache auf einem einzelnen Datenträger aktivieren, der zum CSV hinzugefügt wird. In Windows Server 2012 ist die Standardeinstellung 0 (deaktiviert). Legen Sie den Wert 1 fest, um den CSV-Cache auf einem Datenträger zu aktivieren. In Windows Server 2012 R2 ist diese Einstellung standardmäßig aktiviert. |

Sie können den CSV-Cache über den Systemmonitor überwachen, indem Sie die Indikatoren unter **Cache für freigegebene Clustervolumes** hinzufügen.

**Konfigurieren des CSV-Caches**

1. Starten Sie Windows PowerShell als Administrator.
2. Geben Sie Folgendes ein, um einen Cache von *512* MB auf den einzelnen Knoten zu reservieren:
   - Für Windows Server 2012 R2 und höher:

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

   - Windows Server 2012:

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

3. Geben Sie in Windows Server 2012 folgendes ein, um den CSV-Cache auf einem CSV namens *Cluster Disk 1*zu aktivieren:

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

**NOTE**

- In Windows Server 2012 können Sie dem CSV-Cache nur 20% des gesamten physischen Arbeitsspeichers zuordnen. In Windows Server 2012 R2 und höher können Sie bis zu 80% zuordnen. Da Dateiserver mit horizontaler Skalierung in der Regel keine Speichereinschränkungen aufweisen, können Sie die Leistung erheblich steigern, indem Sie den zusätzlichen Arbeitsspeicher für den CSV-Cache verwenden.
- Um Ressourcenkonflikte zu vermeiden, sollten Sie jeden Knoten im Cluster neu starten, nachdem Sie den dem CSV-Cache zugeordneten Arbeitsspeicher geändert haben. In Windows Server 2012 R2 und höher ist ein Neustart nicht mehr erforderlich.
- Nachdem Sie den CSV-Cache auf einem einzelnen Datenträger aktiviert oder deaktiviert haben, müssen Sie die physische Datenträgerressource offline und anschließend wieder online schalten, damit die Einstellung wirksam wird. (In Windows Server 2012 R2 und höher ist der CSV-Cache standardmäßig aktiviert.)
- Weitere Informationen zum CSV-Cache, einschließlich Informationen zu Leistungsindikatoren, finden Sie im Blogbeitrag How to Enable CSV Cache(in englischer Sprache).

## Sichern von CSVs

Es gibt mehrere Methoden zum Sichern von Informationen, die in csvs in einem Failovercluster gespeichert werden. Sie können eine Microsoft-Sicherungsanwendung oder eine nicht von Microsoft stammende Anwendung verwenden. Im Allgemeinen erfordern freigegebene Clustervolumes (CSV) keine besonderen Sicherungsanforderungen. Lediglich der Clusterspeicher muss mit NTFS oder ReFS formatiert werden. Zudem unterbrechen CSV-Sicherungen keine anderen CSV-Speichervorgänge.

Bei der Auswahl einer Sicherungsanwendung und eines Sicherungszeitplans für CSV sollten Sie die folgenden Faktoren berücksichtigen:

- Die Sicherung eines CSV-Volumes auf Volumeebene kann von jedem Knoten ausgeführt werden, der über eine Verbindung zum CSV-Volume verfügt.
- Die Sicherungsanwendung kann Software- oder Hardwaremomentaufnahmen verwenden. In Abhängigkeit davon, ob sie von Ihrer Sicherungsanwendung unterstützt werden, können Sicherungen anwendungskonsistente und absturzkonsistente Momentaufnahmen des Volumeschattenkopie-Diensts (Volume Shadow Copy Service, VSS) verwenden.
- Wenn Sie ein freigegebenes Clustervolume sichern, das über mehrere aktive virtuelle Computer verfügt, sollten Sie im Allgemeinen eine auf dem Verwaltungsbetriebssystem basierende Sicherungsmethode auswählen. Es können mehrere virtuelle Computer gleichzeitig gesichert werden, wenn diese Option von Ihrer Sicherungsanwendung unterstützt wird.
- CSV unterstützt sicherungsanforderer, auf denen Windows Server 2012 R2 Backup, Windows Server 2012 Backup oder Windows Server 2008 R2 Backup ausgeführt wird. Die Windows Server-Sicherung bietet im Allgemeinen jedoch nur eine einfache Sicherungslösung, die möglicherweise nicht für Organisation mit großen Clustern geeignet ist. Die Windows Server-Sicherung unterstützt keine anwendungskonsistente Sicherung virtueller Computer auf freigegebenen Clustervolumes. Sie unterstützt ausschließlich die absturzkonsistente Sicherung auf Volumeebene. (Wenn Sie eine Absturz konsistente Sicherung wiederherstellen, befindet sich der virtuelle Computer im gleichen Zustand wie bei einem Absturz der virtuellen Maschine, die zu dem Zeitpunkt, zu dem die Sicherung erfolgte, abgestürzt ist.) Eine Sicherung eines virtuellen Computers auf einem CSV-Volume ist erfolgreich, es wird jedoch ein Fehler Ereignis protokolliert, das anzeigt, dass dies nicht unterstützt wird.
- Zum Sichern eines Failoverclusters sind möglicherweise Administratoranmeldeinformationen erforderlich.

**IMPORTANT**

Überprüfen Sie sorgfältig, welche Daten von der Sicherungsanwendung gesichert und wiederhergestellt werden, welche CSV-Features unterstützt werden und welche Ressourcenanforderungen für die Anwendung auf den einzelnen Clusterknoten erforderlich sind.

**WARNING**

Wenn Sie die Sicherungsdaten auf einem CSV-Volume wiederherstellen müssen, beachten Sie die Möglichkeiten und Einschränkungen der Sicherungsanwendung hinsichtlich der Verwaltung und Wiederherstellung anwendungskonsistenter Daten auf den verschiedenen Clusterknoten. Wenn das freigegebene Clustervolume z. B. bei einigen Anwendungen auf einem anderen Knoten als bei der Sicherung wiederherstellt wird, können Sie auf dem Knoten, auf dem die Wiederherstellung erfolgt, versehentlich wichtige Daten zum Anwendungsstatus überschreiben.

## Weitere Informationen

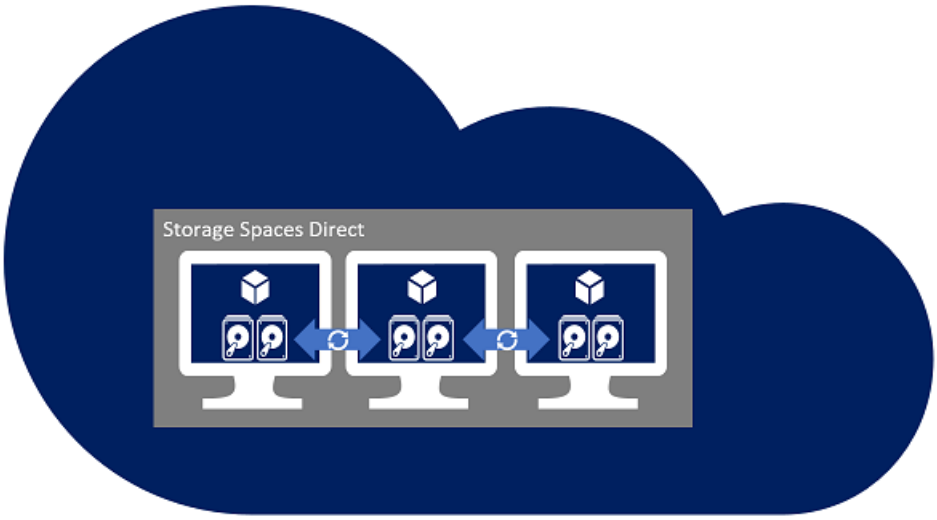
- Failoverclustering
- Bereitstellen von Cluster Speicherplätzen

# Verwenden von direkte Speicherplätze in Clustern virtueller Gastcomputer

21.05.2020 • 4 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Sie können direkte Speicherplätze in einem Cluster physischer Server oder in Gast Clustern für virtuelle Maschinen bereitstellen, wie in diesem Thema erläutert. Diese Art der Bereitstellung bietet virtuellen freigegebenen Speicher über eine Gruppe von virtuellen Computern, die auf einem privaten oder Public Cloud basieren, damit Anwendungslösungen mit hoher Verfügbarkeit verwendet werden können, um die Verfügbarkeit von Anwendungen zu erhöhen.




## Bereitstellen in Azure IaaS-VM-Gast Clustern

Azure-Vorlagen wurden veröffentlicht, um die Komplexität zu verringern, bewährte Methoden und die Geschwindigkeit Ihrer direkte Speicherplätze Bereitstellungen auf einem virtuellen Azure-IaaS-Computer zu konfigurieren. Dies ist die empfohlene Lösung für die Bereitstellung in Azure.

https://channel9.msdn.com/Series/Microsoft-Hybrid-Cloud-Best-Practices-for-IT-Pros/Step-by-Step-Deploy-Windows-Server-2016-Storage-Spaces-Direct-S2D-Cluster-in-Microsoft-Azure/player

## Anforderungen

Beim Bereitstellen von direkte Speicherplätze in einer virtualisierten Umgebung gelten die folgenden Überlegungen.

> **TIP**
> Azure-Vorlagen konfigurieren automatisch die folgenden Überlegungen für Sie und sind bei der Bereitstellung auf Azure-IaaS-VMS empfehlenswert.

- Mindestens 2 Knoten und maximal 3 Knoten
- zwei Knoten Bereitstellungen müssen einen Zeugen konfigurieren (cloudzeuge oder Dateifreigabe Zeuge)

- bei bereit Stellungen mit 3 Knoten kann ein Knoten Ausfall und der Verlust von mindestens einem Datenträger auf einem anderen Knoten toleriert werden. Wenn zwei Knoten heruntergefahren werden, werden die virtuellen Datenträger offline geschaltet, bis einer der Knoten zurückgibt.
- Konfigurieren der virtuellen Computer, die über Fehler Domänen hinweg bereitgestellt werden sollen
  - Azure – Verfügbarkeits Gruppe konfigurieren
  - Hyper-V – Konfigurieren von AntiAffinityClassNames auf den virtuellen Computern, um die VMs Knoten übergreifend zu trennen
  - VMware – konfigurieren Sie die antiaffinitäts Regel für VM-VM, indem Sie eine DRS-Regel vom Typ "separate Virtual Machines" erstellen, um die VMs zwischen ESX-Hosts zu trennen. Für Datenträger, die mit direkte Speicherplätze verwendet werden sollen, sollte der Adapter "paravirtual SCSI" (pvscsi) verwendet werden. Informationen zur pvscsi-Unterstützung mit Windows Server finden Sie unter https://kb.vmware.com/s/article/1010398 .
- Nutzen von geringer Latenz/Hochleistungsspeicher: verwaltete Azure Storage Premium-Datenträger sind erforderlich
- Bereitstellen eines flachen Speicher Entwurfs ohne konfigurierte cachinggeräte
- Mindestens zwei virtuelle Datenträger, die jedem virtuellen Computer angezeigt werden (VHD/vhdx/VMDK)

  Diese Zahl unterscheidet sich von Bare-Metal-bereit Stellungen, da die virtuellen Datenträger als Dateien implementiert werden können, die nicht anfällig für physische Fehler sind.
- Deaktivieren Sie die automatischen Laufwerk Ersetzungs Funktionen in der Integritätsdienst, indem Sie das folgende PowerShell-Cmdlet ausführen:

  ```
  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. Note that 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 backup and restore the data on the Storage Spaces Direct volumes.
- Host level virtual disk size change

  The virtual disks exposed through the virtual machine 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 virtual machines and adding them to the pool. It's highly recommended to use virtual disks of the same size and characteristics as the current virtual disks.

## See also

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

# Erstellen eines Failoverclusters

02.05.2020 • 25 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012

In diesem Thema wird gezeigt, wie ein Failovercluster mithilfe des Failovercluster-Manager-Snap-Ins oder mit Windows PowerShell erstellt wird. Das Thema behandelt eine typische Bereitstellung, bei der Computerobjekte für den Cluster und seine zugehörigen Clusterrollen in Active Directory-Domänendiensten (AD DS) erstellt werden. Wenn Sie einen direkte Speicherplätze Cluster bereitstellen, finden Sie weitere Informationen unter Bereitstellen direkte Speicherplätze.

Sie können auch einen Active Directory getrennten Cluster bereitstellen. Mit dieser Bereitstellungsmethode können Sie einen Failovercluster erstellen und benötigen dazu nicht die Berechtigungen zum Erstellen von Computerobjekten in AD DS. Außerdem müssen Sie nicht die Vorabbereitstellung von Computerobjekten in AD DS anfordern. Diese Option ist nur über Windows PowerShell verfügbar und wird nur für bestimmte Szenarien empfohlen. Weitere Informationen finden Sie unter Bereitstellen eines von Active Directory getrennten Clusters.

**Prüfliste: Erstellen eines Failoverclusters**

| STATUS | AUFGABE | REFERENZ |
|---|---|---|
| ☐ | Überprüfen der Voraussetzungen | Voraussetzungen |
| ☐ | Installieren Sie das Failoverclusteringfeature auf jedem Server, den Sie als Clusterknoten hinzufügen möchten. | Installieren des Failoverclusteringfeatures |
| ☐ | Ausführen des Clusterüberprüfungs-Assistenten zum Überprüfen der Konfiguration | Überprüfen der Konfiguration |
| ☐ | Ausführen des Clustererstellungs-Assistenten zum Erstellen des Failoverclusters | Erstellen des Failoverclusters |
| ☐ | Erstellen von Clusterrollen zum Hosten der Clusterarbeitsauslastung | Erstellen von Clusterrollen |

## Überprüfen der Voraussetzungen

Bevor Sie beginnen, überprüfen Sie die folgenden Voraussetzungen:

- Stellen Sie sicher, dass alle Server, die Sie als Clusterknoten hinzufügen möchten, dieselbe Version von Windows Server ausführen.
- Überprüfen Sie die Hardwareanforderungen, um sicherzustellen, dass Ihre Konfiguration unterstützt wird. Weitere Informationen finden Sie unter Hardwareanforderungen und Speicheroptionen für Failovercluster. Wenn Sie einen direkte Speicherplätze Cluster erstellen, finden Sie unter direkte Speicherplätze HardwareanforderungenWeitere Informationen.
- Um Cluster Speicher während der Cluster Erstellung hinzuzufügen, stellen Sie sicher, dass alle Server auf den Speicher zugreifen können. (Sie können Clusterspeicher auch nach der Erstellung des Clusters hinzufügen.)

- Stellen Sie sicher, dass alle Server, die Sie als Clusterknoten hinzufügen möchten, derselben Active Directory-Domäne angehören.
- (Optional) Erstellen Sie eine Organisationseinheit (OU), und verschieben Sie die Computerkonten für die Server, die Sie als Clusterknoten hinzufügen möchten, in die Organisationseinheit. Als bewährte Methode wird empfohlen, dass Sie Failovercluster in ihren eigenen Organisationseinheiten in AD DS bereitstellen. Auf diese Weise können Sie besser kontrollieren, welche Gruppenrichtlinieneinstellungen oder Sicherheitsvorlageneinstellungen die Clusterknoten beeinflussen. Das Isolieren der Cluster in eigenen Organisationseinheiten schützt zudem vor dem versehentlichen Löschen von Clustercomputerobjekten.

Überprüfen Sie zusätzlich die folgenden Kontoanforderungen:

- Stellen Sie sicher, dass das Konto, das Sie zum Erstellen des Clusters verwenden möchten, einem Domänenbenutzer entspricht, der auf allen Servern, die Sie als Clusterknoten hinzufügen möchten, über Administratorrechte verfügt.
- Stellen Sie sicher, dass eine der folgenden Aussagen zutrifft:
  - Der Benutzer, der die Cluster erstellt, verfügt für die Organisationseinheit oder den Container, in dem sich die Server befinden, die den Cluster bilden, über die Berechtigung **Computerobjekte erstellen**.
  - Wenn der Benutzer nicht über die Berechtigung **Computerobjekte erstellen** verfügt, bitten Sie einen Domänenadministrator, ein Clustercomputerobjekt für den Cluster vorab bereitzustellen. Weitere Informationen finden Sie unter Vorabbereitstellen von Clustercomputerobjekten in Active Directory-Domänendiensten.

> **NOTE**
> Diese Anforderung trifft nicht zu, wenn Sie einen Active Directory getrennten Cluster in Windows Server 2012 R2 erstellen möchten. Weitere Informationen finden Sie unter Bereitstellen eines von Active Directory getrennten Clusters.

## Installieren des Failoverclusteringfeatures

Sie müssen das Failoverclusteringfeature auf jedem Server installieren, den Sie als Failoverclusterknoten hinzufügen möchten.

**Installieren des Failoverclusteringfeatures**

1. Starten Sie den Server-Manager.
2. Wählen Sie im Menü **Verwalten** die Option **Rollen und Features hinzufügen** aus.
3. Wählen Sie **auf der Seite** Vorbereitung die Option **weiter** aus.
4. Wählen Sie auf der Seite **Installationstyp auswählen** die Option **rollenbasierte oder featurebasierte Installation** aus, und klicken Sie dann auf **weiter**.
5. Wählen Sie auf der Seite **Zielserver auswählen** den Server aus, auf dem Sie das Feature installieren möchten, und klicken Sie dann auf **weiter**.
6. Wählen Sie **Weiter** auf der Seite **Serverrollen auswählen** aus.
7. Aktivieren Sie auf der Seite **Features auswählen** das Kontrollkästchen **Failoverclustering**.
8. Wählen Sie zum Installieren der Failovercluster-Verwaltungs Tools **Features hinzufügen** aus, und klicken Sie dann auf **weiter**.
9. Wählen Sie auf der Seite **Installations Auswahl bestätigen** die Option **Installieren** aus.
   Ein Neustart des Servers ist für das Failoverclusteringfeature nicht erforderlich.
10. Wenn die Installation abgeschlossen ist, wählen Sie **Schließen** aus.

11. Wiederholen Sie diesen Vorgang auf jedem Server, den Sie als Failoverclusterknoten hinzufügen möchten.

> **NOTE**
>
> Es wird empfohlen, dass Sie nach der Installation des Failoverclusteringfeatures die neuesten Updates von Windows Update anwenden. Lesen Sie außerdem für einen Windows Server 2012-basierten Failovercluster die empfohlenen Hotfixes und Updates für Windows Server 2012-basierte Failovercluster Microsoft-Support Artikel, und installieren Sie alle Updates, die angewendet werden.

## Überprüfen der Konfiguration

Vor der Erstellung des Failovercluster wird dringend empfohlen, dass Sie die Konfiguration überprüfen, um sicherzustellen, dass die Hardware und die Hardwareeinstellungen mit dem Failoverclustering kompatibel sind. Microsoft unterstützt eine Clusterlösung nur, wenn die gesamte Konfiguration die Validierungstests besteht und die gesamte Hardware für die Version von Windows Server zertifiziert ist, die auf den Clusterknoten ausgeführt wird.

> **NOTE**
>
> Sie müssen mindestens zwei Knoten besitzen, um alle Tests ausführen zu können. Viele wichtige Speichertests können nicht ausgeführt werden, wenn nur ein Knoten verfügbar ist.

**Ausführen von Cluster Validierungstests**

1. Starten Sie den Failovercluster-Manager auf einem Computer, auf dem die Verwaltungstools für Failovercluster über die Remoteserver-Verwaltungstools installiert wurden, oder auf einem Server, auf dem Sie das Failoverclusteringfeature installiert haben. Um dies auf einem Server zu erreichen, starten Sie Server-Manager, und wählen Sie dann **im Menü Extras** die Option **Failovercluster-Manager** aus.

2. Klicken Sie im **Failovercluster-Manager** Bereich unter **Verwaltung** auf **Konfiguration** überprüfen.

3. Wählen Sie auf der Seite **Vorbereitung** die Option **Weiter**.

4. Geben Sie auf der Seite **Server oder Cluster auswählen** in das Feld **Name eingeben** den NetBIOS-Namen oder den voll qualifizierten Domänen Namen eines Servers ein, den Sie als Failoverclusterknoten hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**. Wiederholen Sie diesen Schritt für alle weiteren Server, die Sie hinzufügen möchten. Wenn Sie mehrere Server gleichzeitig hinzufügen möchten, trennen Sie die Namen durch ein Komma oder Semikolon. Geben Sie z. b. die Namen im `server1.contoso.com, server2.contoso.com` Format ein. Wenn Sie fertig sind, klicken Sie auf **Weiter**.

5. Wählen Sie auf der Seite **Test Optionen die Option alle Tests ausführen (empfohlen)** aus, und klicken Sie dann auf **weiter**.

6. Wählen Sie auf der Seite **Bestätigung** die Option **weiter** aus.

   Auf der Seite zur Ausführung der Überprüfung wird der Status der aktiven Tests angezeigt.

7. Führen Sie auf der Seite **Zusammenfassung** eine der folgenden Aktionen aus:

   - Wenn die Ergebnisse auf eine erfolgreiche Ausführung der Tests hinweisen und die Konfiguration für das Clustering geeignet ist und Sie den Cluster sofort erstellen möchten, stellen Sie sicher, dass das Kontrollkästchen **Cluster jetzt mit den überprüften Knoten erstellen** aktiviert ist, und klicken Sie dann auf **Fertig**stellen. Fahren Sie dann mit Schritt 4 des Verfahrens Erstellen des Failoverclusters fort.

   - Wenn die Ergebnisse darauf hindeuten, dass Warnungen oder Fehler aufgetreten sind, wählen Sie **Bericht anzeigen** aus, um die Details anzuzeigen und zu ermitteln, welche Probleme korrigiert werden müssen. Beachten Sie, dass eine Warnung für einen bestimmten Validierungstest darauf

hinweist, dass dieser Aspekt des Failoverclusters zwar unterstützt werden kann, er aber möglicherweise nicht den empfohlenen bewährten Methoden entspricht.

> **NOTE**
> Wenn Sie eine Warnung für den Test "Permanente Reservierung für Speicherplatz überprüfen" erhalten, finden Sie weitere Informationen im Blogbeitrag Windows Failover Cluster validation warning indicates your disks don't support the persistent reservations for Storage Spaces .

Weitere Informationen zu Hardwarevalidierungstests finden Sie unter Überprüfen der Hardware für einen Failovercluster.

## Erstellen des Failoverclusters

Stellen Sie zum Abschließen dieses Schritts sicher, dass das Benutzerkonto, mit dem Sie sich anmelden, den im Abschnitt Überprüfen der Voraussetzungen dieses Themas angegebenen Anforderungen entspricht.

1. Starten Sie den Server-Manager.
2. Wählen Sie **im Menü Extras** die Option **Failovercluster-Manager** aus.
3. Klicken Sie im **Failovercluster-Manager** Bereich unter **Verwaltung** auf **Cluster erstellen**.

   Der Clustererstellungs-Assistent wird geöffnet.
4. Wählen Sie auf der Seite **Vorbereitung** die Option **Weiter**.
5. Wenn die Seite **Server auswählen** angezeigt wird, geben Sie in das Feld **Name eingeben** den NetBIOS-Namen oder den voll qualifizierten Domänen Namen eines Servers ein, den Sie als Failoverclusterknoten hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**. Wiederholen Sie diesen Schritt für alle weiteren Server, die Sie hinzufügen möchten. Wenn Sie mehrere Server gleichzeitig hinzufügen möchten, trennen Sie die Namen durch ein Komma oder Semikolon. Geben Sie die Namen z. B. im Format *server1.contoso.com; server2.contoso.com* ein. Wenn Sie fertig sind, klicken Sie auf **Weiter**.

   > **NOTE**
   > Wenn Sie den Cluster sofort nach dem Ausführen der Überprüfung im Konfigurations Überprüfungsverfahren erstellt haben, wird die Seite **Server auswählen** nicht angezeigt. Die überprüften Knoten werden automatisch zum Clustererstellungs-Assistenten hinzugefügt, damit Sie diese nicht erneut eingeben müssen.
6. Wenn Sie die Validierung zuvor übersprungen haben, wird eine Seite mit einer **Validierungswarnung** angezeigt. Es wird dringend empfohlen, die Clustervalidierung auszuführen. Nur Cluster, die alle Validierungstests bestehen, werden von Microsoft unterstützt. Um die Validierungstests auszuführen, wählen Sie **Ja** aus, und klicken Sie dann auf **weiter**. Führen Sie den Konfigurationsüberprüfungs-Assistenten wie unter Überprüfen der Konfiguration beschrieben aus.
7. Gehen Sie auf der Seite **Zugriffspunkt für die Clusterverwaltung** wie folgt vor:

   a. Geben Sie in das Feld **Clustername** den Namen ein, über den Sie den Cluster verwalten möchten. Überprüfen Sie zuvor die folgenden Informationen:

      - Während der Clustererstellung wird dieser Name als Clustercomputerobjekt (auch als *Clusternamenobjekt* oder *CNO* bezeichnet) in AD DS registriert. Wenn Sie einen NetBIOS-Namen für den Cluster angeben, wird das Clustercomputerobjekt (CNO) am gleichen Speicherort erstellt, an dem sich die Computerobjekte für die Clusterknoten befinden. Hierbei kann es sich um den Standardcontainer des Computers oder um eine Organisationseinheit (OU) handeln.

- Wenn Sie einen anderen Speicherort für das CNO angeben möchten, können Sie den Distinguished Name einer Organisationseinheit im Feld **Clustername** eingeben. Zum Beispiel: *CN=ClusterName, OU=Clusters, DC=Contoso, DC=com*.
- Wenn ein Domänenadministrator das CNO in einer anderen Organisationseinheit vorab bereitgestellt hat, in der sich die Clusterknoten nicht befinden, geben Sie den Distinguished Name an, der vom Domänenadministrator bereitgestellt wird.

b. Wenn der Server nicht über einen für DHCP konfigurierten Netzwerkadapter verfügt, müssen Sie mindestens eine statische IP-Adresse für den Failovercluster konfigurieren. Aktivieren Sie das Kontrollkästchen neben den jeweiligen Netzwerkadaptern, die Sie für die Clusterverwaltung verwenden möchten. Wählen Sie das Feld **Adresse** neben einem ausgewählten Netzwerk aus, und geben Sie dann die IP-Adresse ein, die Sie dem Cluster zuweisen möchten. Diese IP-Adresse (oder Adressen) wird dem Clusternamen im Domain Name System zugeordnet.

> **NOTE**
>
> Wenn Sie Windows Server 2019 verwenden, haben Sie die Möglichkeit, einen verteilten Netzwerknamen für den Cluster zu verwenden. Ein verteilter Netzwerkname verwendet die IP-Adressen der Mitglieds Server, anstatt eine dedizierte IP-Adresse für den Cluster zu erfordern. Standardmäßig wird von Windows ein verteilter Netzwerkname verwendet, wenn erkannt wird, dass Sie den Cluster in Azure erstellen (sodass Sie keinen internen Lastenausgleich für den Cluster erstellen müssen) oder eine normale statische oder IP-Adresse, wenn Sie lokal ausgeführt werden. Weitere Informationen finden Sie unter Name des verteilten Netzwerks.

c. Wenn Sie fertig sind, klicken Sie auf **Weiter**.

8. Überprüfen Sie auf der Seite **Bestätigung** die Einstellungen. Das Kontrollkästchen **Der gesamte geeignete Speicher soll dem Cluster hinzugefügt werden** ist standardmäßig aktiviert. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie eine der folgenden Optionen ausführen möchten:

   - Sie möchten den Speicher später konfigurieren.
   - Sie planen die Erstellung von Clusterspeicherplätzen über den Failovercluster-Manager oder mithilfe von Windows PowerShell-Cmdlets für Failoverclustering und haben bisher keine Speicherplätze in den Datei- und Speicherdiensten erstellt. Weitere Informationen finden Sie unter Bereitstellen von Clusterspeicherplätzen.

9. Wählen Sie **weiter** aus, um den Failovercluster zu erstellen.

10. Bestätigen Sie auf der Seite **Zusammenfassung** die erfolgreiche Erstellung des Failoverclusters. Wenn Warnungen oder Fehler aufgetreten sind, zeigen Sie die Ausgabe der Zusammenfassung an, oder wählen Sie **Bericht anzeigen** aus, um den vollständigen Bericht anzuzeigen. Wählen Sie **Fertig stellen** aus.

11. Überprüfen Sie, ob der Clustername in der Navigationsstruktur unter **Failovercluster-Manager** aufgeführt ist, um die Erstellung des Clusters zu bestätigen. Sie können den Cluster Namen erweitern und dann unter **Knoten**, **Speicher** oder **Netzwerke** Elemente auswählen, um die zugeordneten Ressourcen anzuzeigen.

    Beachten Sie, dass es einen Moment dauern kann, bevor der Clustername im DNS erfolgreich repliziert wird. Wenn Sie nach der erfolgreichen DNS-Registrierung und-Replikation **alle Server** in Server-Manager ausgewählt haben, sollte der Cluster Name als Server mit dem **verwaltbarkeitsstatus Online**aufgeführt werden.

Nach der Erstellung des Clusters können Sie z. B. die Clusterquorumkonfiguration überprüfen und optional freigegebene Clustervolumes (CSV) erstellen. Weitere Informationen finden Sie Untergrund Legendes zu Quorums in direkte Speicherplätze und Verwenden von freigegebenen Clustervolumes in einem Failovercluster.

## Erstellen von Clusterrollen

Nachdem Sie den Failovercluster erstellt haben, können Sie Clusterrollen zum Hosten der Clusterarbeitsauslastung

erstellen.

> **NOTE**
> Für Clusterrollen, die einen Clientzugriffspunkt erfordern, wird ein virtuelles Computerobjekt (Virtual Computer Object, VCO) in AD DS erstellt. Standardmäßig werden alle virtuellen Computerobjekte für den Cluster in demselben Container oder in derselben Organisationseinheit wie das CNO erstellt. Beachten Sie, dass Sie das CNO nach der Erstellung eines Clusters in eine beliebige Organisationseinheit verschieben können.

So erstellen Sie eine Cluster Rolle:

1. Installieren Sie die Rolle oder das Feature, die bzw. das für eine Clusterrolle erforderlich ist, mit dem Server-Manager oder Windows PowerShell auf jeden Failoverclusterknoten. Wenn Sie z. B. einen Clusterdateiserver erstellen möchten, installieren Sie die Rolle "Dateiserver" auf allen Clusterknoten.

   In der folgenden Tabelle werden die Clusterrollen, die Sie im Assistenten für hohe Verfügbarkeit konfigurieren sowie die zugehörige Serverrolle oder das Feature angezeigt, die Sie als Voraussetzung installieren müssen.

| CLUSTERROLLE | VORAUSGESETZTE(S) ROLLE ODER FEATURE |
|---|---|
| Namespace Server | Namespaces (Teil der Datei Server Rolle) |
| DFS-Namespaceserver | DHCP-Serverrolle |
| Distributed Transaction Coordinator (DTC) | Keine |
| Dateiserver | Dateiserverrolle |
| Allgemeine Anwendung | Nicht verfügbar |
| Allgemeines Skript | Nicht verfügbar |
| Allgemeiner Dienst | Nicht verfügbar |
| Hyper-V-Replikatbroker | Hyper-V-Rolle |
| iSCSI Target Server | iSCSI-Zielserver (Teil der Dateiserverrolle) |
| iSNS-Server | iSNS-Serverdienstfeature |
| Message Queuing | Message Queuing-Dienstfeature |
| Anderer Server | Keine |
| Virtual Machine | Hyper-V-Rolle |
| WINS-Server | WINS-Server-Feature |

2. Erweitern Sie in Failovercluster-Manager den Cluster Namen, klicken Sie mit der rechten Maustaste auf **Rollen**, und wählen Sie dann **Rolle konfigurieren**aus.

3. Folgen Sie den Schritten im Assistenten für hohe Verfügbarkeit, um die Clusterrolle zu erstellen.

4. Stellen Sie im Bereich **Rollen** sicher, dass die Rolle den Status **Wird ausgeführt** aufweist, um die Erstellung

der Clusterrolle zu überprüfen. Im Bereich "Rollen" wird auch der Besitzerknoten angezeigt. Um das Failover zu testen, klicken Sie mit der rechten Maustaste auf die Rolle, zeigen Sie auf **verschieben**, und wählen Sie dann **Knoten auswählen**. Wählen Sie im Dialogfeld **Cluster Rolle verschieben** den gewünschten Cluster Knoten aus, und klicken Sie dann auf **OK**. Überprüfen Sie in der Spalte **Besitzerknoten**, ob der Besitzerknoten geändert wurde.

## Erstellen eines Failoverclusters mithilfe von Windows PowerShell

Die folgenden Windows PowerShell-Cmdlets führen dieselben Funktionen aus wie die vorherigen Prozeduren in diesem Thema. Geben Sie die einzelnen Cmdlets in einer einzelnen Zeile ein, auch wenn es den Anschein hat, dass aufgrund von Formatierungseinschränkungen Zeilenumbrüche vorhanden sind.

> **NOTE**
> Sie müssen Windows PowerShell verwenden, um einen Active Directory getrennten Cluster in Windows Server 2012 R2 zu erstellen. Weitere Informationen zur Syntax finden Sie unter Bereitstellen eines von Active Directory getrennten Clusters.

Im folgenden Beispiel wird das Failoverclusteringfeature installiert.

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

Im folgenden Beispiel werden alle Clustervalidierungstests auf den Computern *Server1* und *Server2* ausgeführt.

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

> **NOTE**
> Das **Test-Cluster-** Cmdlet gibt die Ergebnisse in eine Protokolldatei im aktuellen Arbeitsverzeichnis aus. Beispiel: c:\Users<username> \AppData\Local\Temp.

Im folgenden Beispiel wird ein Failovercluster namens *MyCluster* mit den Knoten *Server1* und *Server2* erstellt, die statische IP-Adresse *192.168.1.12* zugewiesen und der gesamte geeignete Speicher zum Failovercluster hinzugefügt.

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

Im folgenden Beispiel wird derselbe Failovercluster wie im vorherigen Beispiel erstellt, aber nicht der geeignete Speicher zum Failovercluster hinzugefügt.

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

Im folgenden Beispiel wird der Cluster *MyCluster* in der Organisationseinheit *Cluster* der Domäne *Contoso.com* erstellt.

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

Beispiele zum Hinzufügen von Clusterrollen finden Sie in Themen wie z. B. Add-ClusterFileServerRole und Add-ClusterGenericApplicationRole.

## Weitere Informationen

- Failoverclustering
- Bereitstellen eines Hyper-V-Clusters
- Dateiserver mit horizontaler Skalierung für Anwendungsdaten
- Bereitstellen eines von Active Directory getrennten Clusters
- Verwenden von Gastclustering für hohe Verfügbarkeit
- Clusterfähiges Aktualisieren
- New-Cluster
- Test-Cluster

# Bereitstellen eines Cluster Dateiservers mit zwei Knoten

09.04.2020 • 39 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

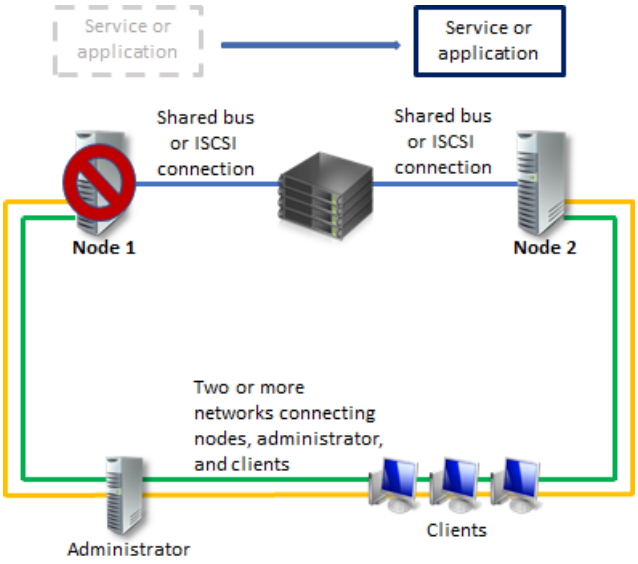
Ein Failovercluster besteht aus einer Gruppe von unabhängigen Computern, die miteinander interagieren und somit die Verfügbarkeit von Anwendungen und Diensten erhöhen. Die geclusterten Server ("Knoten") sind physisch über Kabel sowie durch Software verbunden. Wenn auf einem der Clusterknoten ein Fehler auftritt, werden seine Aufgaben sofort auf einen anderen Knoten übertragen. Dies wird als Failover bezeichnet. So ergeben sich für die Benutzer nur minimale Unterbrechungen des Betriebs.

In dieser Anleitung werden die Schritte zum Installieren und Konfigurieren eines allgemeinen Dateiserver-Failoverclusters mit zwei Knoten beschrieben. Wenn Sie die Konfiguration in dieser Anleitung erstellen, können Sie sich über Failovercluster informieren und sich mit der Snap-in-Schnittstelle für Failoverclusterverwaltung in Windows Server 2019 oder Windows Server 2016 vertraut machen.

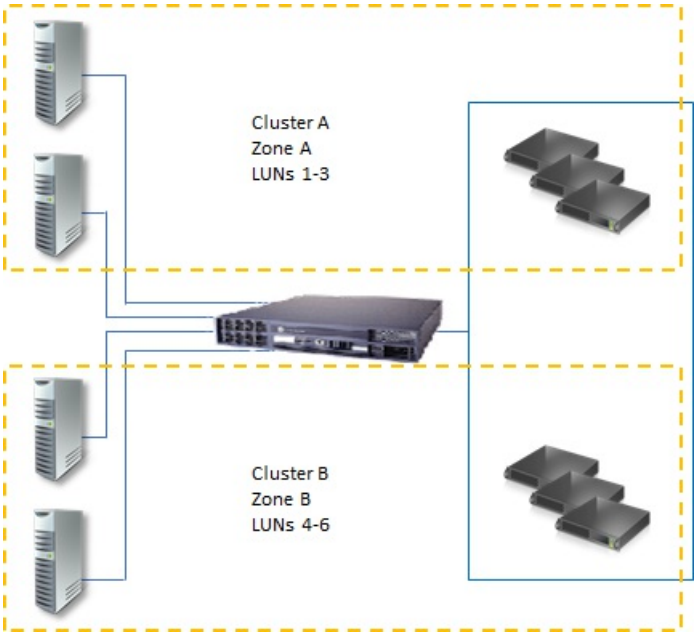
## Übersicht über einen Dateiservercluster mit zwei Knoten

Server in einem Failovercluster können in einer Vielzahl von Rollen eingesetzt werden, einschließlich der Rollen von Dateiserver, Hyper-V-Server oder Datenbankserver. Sie können Hochverfügbarkeit für eine Vielzahl anderer Dienste und Anwendungen bereitstellen. In dieser Anleitung wird die Konfiguration eines Dateiserverclusters mit zwei Knoten beschrieben.

Ein Failovercluster enthält normalerweise eine Speichereinheit, die mit allen Servern im Cluster physisch verbunden ist, obwohl auf jedes Volume im Speicher immer nur von je einem Server zugegriffen wird. Im folgenden Diagramm finden Sie einen Failovercluster mit zwei Knoten, der an mit einer Speichereinheit verbunden ist.




Die für die Knoten eines Clusters offen gelegten Speichervolumes oder logischen Gerätenummern (Logical Unit Numbers, LUNs) müssen für andere Server, einschließlich der Server in einem anderen Cluster, nicht offen gelegt werden. Dies wird im folgenden Diagramm veranschaulicht.




Beachten Sie, dass im Sinne einer optimalen Serververfügbarkeit bewährte Methoden der Serververwaltung zu befolgen, z. B. das sorgfältige Verwalten der physischen Umgebung der Server, das Testen von Softwareänderungen vor der vollständigen Implementierung und das gründliche Nachverfolgen von Softwareupdates und Konfigurationsänderungen auf allen geclusterten Servern.

Das folgende Szenario beschreibt, wie ein Dateiserver-Failovercluster konfiguriert werden kann. Die Dateien, die freigegeben werden sollen, befinden sich auf der Clusterspeichereinheit, und jeder Clusterserver kann als der Dateiserver fungieren, der diese freigibt.

## Freigegebene Ordner in einem Failovercluster

In der folgenden Liste werden die Konfigurationsfunktionen für freigegebene Ordner beschrieben, die in Failoverclustering integriert sind:

- Die Anzeige ist auf freigegebene Clusterordner beschränkt (keine Vermischung mit nicht gruppierten freigegebenen Ordnern): Wenn ein Benutzer freigegebene Ordner durch Angabe des Pfads eines gruppierten Dateiservers anzeigt, enthält die Anzeige nur die freigegebenen Ordner, die Teil der jeweiligen Dateiserver Rolle sind. Nicht gruppierte freigegebene Ordner werden ausgeschlossen, und es wird ein Teil von separaten Dateiserver Rollen verwendet, die sich auf einem Cluster Knoten befinden.

- Zugriffs basierte Enumeration: Sie können die Zugriffs basierte Enumeration verwenden, um einen angegebenen Ordner in der Benutzeransicht auszublenden. Anstatt den Ordner für den Benutzer anzuzeigen, ihn jedoch nicht darauf zugreifen zu lassen, können Sie den Ordner einfach ganz ausblenden. Sie können die Zugriffs basierte Enumeration für einen geclusterten freigegebenen Ordner auf die gleiche Weise wie für einen nicht gruppierten freigegebenen Ordner konfigurieren.

- Offline Zugriff: Sie können den Offline Zugriff (Caching) für einen geclusterten freigegebenen Ordner auf die gleiche Weise wie für einen nicht gruppierten freigegebenen Ordner konfigurieren.

- Geclusterte Datenträger werden immer als Teil des Clusters erkannt: unabhängig davon, ob Sie die Failoverclusterschnittstelle, Windows-Explorer oder das Freigabe-und Speicher Verwaltungs-Snap-in verwenden, erkennt Windows, ob ein Datenträger als im Cluster Speicher festgelegt wurde. Wenn ein solcher Datenträger bereits in der Failoverclusterverwaltung als Teil eines Cluster Dateiservers konfiguriert wurde, können Sie mithilfe einer der oben erwähnten Schnittstellen eine Freigabe auf dem Datenträger erstellen. Wenn der Datenträger nicht als Teil eines Clusterdateiservers konfiguriert wurde, ist es nicht möglich, versehentlich eine Freigabe darauf zu erstellen. Stattdessen gibt eine Fehlermeldung an, dass der Datenträger zuerst als Teil eines Clusterdateiservers konfiguriert werden muss, bevor er freigegeben werden kann.

- Integration von Services for Network File System: die Rolle "Datei Server" in Windows Server umfasst den optionalen Rollen Dienst "Dienste für NFS (Network File System)". Durch Installieren des Rollendiensts und Konfigurieren von freigegebenen Ordner mit Diensten für NFS können Sie einen Clusterdateiserver erstellen, der UNIX-basierte Clients unterstützt.

## Anforderungen für einen Failovercluster mit zwei Knoten

Damit ein Failovercluster in Windows Server 2016 oder Windows Server 2019 als offiziell unterstützte Lösung von Microsoft angesehen wird, muss die Lösung die folgenden Kriterien erfüllen.

- Alle Hardware- und Softwarekomponenten müssen die Qualifikationen für das entsprechende Logo erfüllen. Für Windows Server 2016 ist dies das Logo "Certified for Windows Server 2016". Für Windows Server 2019 ist dies das Logo "Certified for Windows Server 2019". Weitere Informationen dazu, welche Hardware-und Softwaresysteme zertifiziert wurden, finden Sie auf der Microsoft Windows Server-Katalog Website.
- Die vollständig konfigurierte Lösung (Server, Netzwerk und Speicher) muss alle Tests im Validierungs-Assistenten bestehen, der Teil des Failovercluster-Snap-Ins ist.

Für einen Failovercluster mit zwei Knoten ist Folgendes erforderlich:

- **Server:** Es wird empfohlen, übereinstimmende Computer mit denselben oder ähnlichen Komponenten zu verwenden. Auf den Servern für einen Failovercluster mit zwei Knoten muss die gleiche Version von Windows Server ausgeführt werden. Sie sollten auch die gleichen Software Updates (Patches) enthalten.
- **Netzwerkadapter und Kabel:** Die Netzwerkhardware muss wie andere Komponenten in der Failoverclusterlösung mit Windows Server 2016 oder Windows Server 2019 kompatibel sein. Wenn Sie iSCSI verwenden, müssen die Netzwerkadapter entweder für die Netzwerkkommunikation oder für iSCSI, nicht jedoch für beides dediziert sein. Vermeiden Sie in der Netzwerkinfrastruktur, über die die Clusterknoten verbunden sind, die Verwendung von Komponenten, deren Ausfall einen Ausfall des Gesamtsystems zur Folge hätte. Es gibt mehrere Methoden, dies zu erreichen. Sie können die Clusterknoten durch mehrere unterschiedliche Netzwerke verbinden. Zudem können Sie die Clusterknoten mit einem Netzwerk verbinden, das aus Netzwerkadapterteams, redundanten Switches, redundanten Routern oder ähnlicher Hardware besteht, die einzelne Fehlerpunkte beseitigt.

  > **NOTE**
  > Wenn die Cluster Knoten mit einem einzelnen Netzwerk verbunden sind, übergibt das Netzwerk die Redundanz Anforderung im Konfigurationsüberprüfungs-Assistenten. Der Bericht enthält jedoch eine Warnung, dass das Netzwerk keine Single Point of Failure haben sollte.

- **Geräte Controller oder geeignete Adapter für den Speicher:**
  - **Serielle angehängte SCSI-oder-Fibre Channel:** Wenn Sie Serial Attached SCSI oder Fibre Channel verwenden, sollten alle Komponenten des Speicher Stapels auf allen Cluster Servern identisch sein. Es ist erforderlich, dass die Multipfad-e/a (MPIO)-Software und DSM-Softwarekomponenten (Device Specific Module) identisch sind. Es wird empfohlen, identische Massenspeichergerätecontroller zu verwenden, d. h. Hostbusadapter (HBA), HBA-Treiber und HBA-Firmware. Wenn Sie unterschiedliche HBAs verwenden, sollten Sie gemeinsam mit dem Speicheranbieter überprüfen, ob die unterstützten oder empfohlenen Konfigurationen eingehalten werden.
  - **iSCSI:** Wenn Sie iSCSI verwenden, muss jeder Cluster Server über mindestens einen Netzwerkadapter oder Hostbus Adapter verfügen, der für den iSCSI-Speicher reserviert ist. Das Netzwerk, das Sie für iSCSI verwenden, kann nicht für die Netzwerkkommunikation verwendet werden. Die zum Herstellen von Verbindungen mit dem iSCSI-Speicherziel verwendeten Netzwerkadapter müssen für alle Clusterserver identisch sein, und es empfiehlt sich, Gigabit Ethernet oder höher zu verwenden.

- **Speicher:** Sie müssen freigegebenen Speicher verwenden, der für Windows Server 2016 oder Windows Server 2019 zertifiziert ist.

  Bei einem Failovercluster mit zwei Knoten sollte der Speicher mindestens zwei separate Volumes (LUNs) enthalten, wenn ein Zeugen Datenträger für das Quorum verwendet wird. Bei einem Zeugendatenträger handelt es sich um einen Datenträger im Clusterspeicher, auf dem eine Kopie der Clusterkonfigurationsdatenbank gespeichert ist. Bei diesem Beispiel für einen Cluster mit zwei Knoten ist die Quorum Konfiguration Knoten-und Datenträger Mehrheit. Knoten-und Datenträger Mehrheit bedeutet, dass die Knoten und der Zeugen Datenträger jeweils Kopien der Cluster Konfiguration enthalten, und der Cluster verfügt über ein Quorum, solange die Mehrheit (zwei von drei) dieser Kopien verfügbar ist. Das andere Volume (LUN) enthält die Dateien, die für die Benutzer freigegeben werden.

  Die Speicheranforderungen beinhalten Folgendes:

  - Um die systemeigene, im Failoverclustering enthaltene Datenträgerunterstützung verwenden zu können, müssen anstelle von dynamischen Datenträgern Basisdatenträger verwendet werden.
  - Die Formatierung als NTFS-Partitionen wird empfohlen (die Partition des Zeugendatenträgers muss NTFS-formatiert sein).
  - Als Partitionsstil des Datenträgers können Sie entweder MBR (Master Boot Record) oder GPT (GUID-Partitionstabelle) verwenden.
  - Der Speicher muss ordnungsgemäß auf bestimmte SCSI-Befehle Antworten. der Speicher muss dem Standard entsprechen, der als SCSI Primary Commands-3 (SPC-3) bezeichnet wird. Insbesondere muss der Speicher permanente Reservierungen unterstützen, wie im SPC-3-Standard angegeben.
  - Der für den Speicher verwendete Miniporttreiber muss mit dem StorPort-Speichertreiber von Microsoft kompatibel sein.

## Bereitstellen von SANs (Storage Area Networks) mit Failoverclustern

Beim Bereitstellen einer Storage Area Network (San) mit einem Failovercluster sollten die folgenden Richtlinien beachtet werden.

- **Bestätigen Sie die Zertifizierung des Speichers:** Bestätigen Sie mithilfe der Windows Server-Katalog Website, dass der Speicher des Anbieters, einschließlich der Treiber, Firmware und Software, für Windows Server 2016 oder Windows Server 2019 zertifiziert ist.

- **Isolieren Sie Speichergeräte, einen Cluster pro Gerät:** Server aus unterschiedlichen Clustern dürfen nicht auf dieselben Speichergeräte zugreifen können. In den meisten Fällen sollte eine LUN, die für einen Satz von Clusterservern verwendet wird, durch LUN-Maskierung oder -Zoneneinteilung von allen anderen Servern isoliert werden.

- **Verwenden Sie ggf. Multipfad-e/a-Software:** In einer hoch verfügbaren speicherfabric können Sie mithilfe von Multipfad-e/a-Software Failovercluster mit mehreren Hostbus Adaptern bereitstellen. Auf diese Weise erhalten Sie den höchsten Grad an Redundanz und Verfügbarkeit. Die Multipfadlösung muss auf Microsoft Multipfad-e/a (MPIO) basieren. Der Speicherhardware Hersteller kann ein Geräte spezifisches MPIO-Modul (DSM) für die Hardware bereitstellen, obwohl Windows Server 2016 und Windows Server 2019 mindestens eine DSMs als Teil des Betriebssystems enthalten.

## Anforderungen an die Netzwerkinfrastruktur und das Domänenkonto

Für einen Failovercluster mit zwei Knoten benötigen Sie die folgende Netzwerkinfrastruktur und ein Administratorkonto mit den folgenden Domänenberechtigungen:

- **Netzwerkeinstellungen und IP-Adressen:** Wenn Sie für ein Netzwerk identische Netzwerkadapter verwenden, verwenden Sie auch identische Kommunikationseinstellungen auf diesen Adaptern (z. b. Geschwindigkeit, Duplex Modus, Fluss Steuerung und Medientyp). Vergleichen Sie zudem die Einstellungen

zwischen dem Netzwerkadapter und dem Switch, zu dem eine Verbindung hergestellt wird, und stellen Sie sicher, dass die Einstellungen nicht miteinander in Konflikt stehen.

Wenn Sie über private Netzwerke verfügen, die nicht an die übrige Netzwerkinfrastruktur weitergeleitet werden, muss sichergestellt werden, dass jedes dieser privaten Netzwerke ein eindeutiges Subnetz verwendet. Dies ist auch dann erforderlich, wenn jeder Netzwerkadapter über eine eindeutige IP-Adresse verfügt. Wenn Sie beispielsweise in einer Zentrale mit einem physischen Netzwerk über einen Clusterknoten und in einer Filiale mit einem separaten physischen Netzwerk über einen weiteren Knoten verfügen, sollte 10.0.0.0/24 selbst dann nicht für beide Netzwerke angegeben werden, wenn Sie jedem Adapter eine eindeutige IP-Adresse zuweisen.

Weitere Informationen zu den Netzwerkadaptern finden Sie weiter oben in dieser Anleitung unter Hardwareanforderungen für einen Failovercluster mit zwei Knoten.

- **DNS:** Die Server im Cluster müssen für die Namensauflösung Domain Name System (DNS) verwenden. Das Protokoll für das dynamische DNS-Update kann verwendet werden.
- **Domänen Rolle:** Alle Server im Cluster müssen sich in derselben Active Directory Domäne befinden. Als bewährte Methode sollten alle geclusterten Server über dieselbe Domänenrolle verfügen (entweder Mitgliedsserver oder Domänencontroller). Die empfohlene Rolle ist Mitgliedsserver.
- **Domänen Controller:** Es wird empfohlen, dass die geclusterten Server Mitglied Server sind. Ist dies der Fall, benötigen Sie einen zusätzlichen Server, der in der Domäne, die den Failovercluster enthält, als Domänencontroller fungiert.
- **Clients:** Bei Bedarf können Sie einen oder mehrere vernetzte Clients mit dem Failovercluster verbinden, den Sie erstellen, und die Auswirkung auf einen Client beobachten, wenn Sie den Cluster Dateiserver von einem Cluster Knoten zum anderen verschieben oder einen Failover ausführen.
- **Konto zum Verwalten des Clusters:** Wenn Sie zum ersten Mal einen Cluster erstellen oder diesem Server hinzufügen, müssen Sie bei der Domäne mit einem Konto angemeldet sein, das über Administratorrechte und Berechtigungen für alle Server in diesem Cluster verfügt. Dabei muss es sich nicht unbedingt um ein Domänenadministratorenkonto handeln. Es kann auch ein Domänenbenutzerkonto verwendet werden, das der Gruppe Administratoren für die einzelnen Clusterserver angehört. Wenn es sich bei dem Konto nicht um ein Domänen-Admins-Konto handelt, muss dem Konto (oder der Gruppe, der das Konto angehört) außerdem die Berechtigung zum **Erstellen von Computer Objekten** und zum **Lesen aller Eigenschaften** in der Domänen Organisationseinheit (OE) erteilt werden, in der sich das Konto befindet.

## Schritte zum Installieren eines Dateiserverclusters mit zwei Knoten

Sie müssen die folgenden Schritte ausführen, um einen Dateiserver-Failovercluster mit zwei Knoten zu installieren.

Schritt 1: Verbinden der Cluster Server mit den Netzwerken und dem Speicher

Schritt 2: Installieren des Failoverclusterfeatures

Schritt 3: Überprüfen der Cluster Konfiguration

Schritt 4: Erstellen des Clusters

Wenn Sie die Clusterknoten bereits installiert haben und einen Dateiserver-Failovercluster konfigurieren möchten, finden Sie weiter unten in dieser Anleitung weitere Informationen unter Schritte zum Konfigurieren eines Dateiserverclusters mit zwei Knoten.

**Schritt 1: Verbinden der Cluster Server mit den Netzwerken und dem Speicher**

Vermeiden Sie in einem Failoverclusternetzwerk einzelne Fehlerpunkte. Es gibt mehrere Methoden, dies zu erreichen. Sie können die Clusterknoten durch mehrere unterschiedliche Netzwerke verbinden. Alternativ können

Sie die Clusterknoten mit einem Netzwerk verbinden, das aus kombinierten Netzwerkadaptern, redundanten Switches, redundanten Routern oder ähnlicher Hardware besteht, die einzelne Fehlerpunkte ausschließt (Wenn Sie ein Netzwerk für iSCSI verwenden, müssen Sie dieses Netzwerk zusätzlich zu den anderen Netzwerken einrichten).

Für einen Dateiservercluster mit zwei Knoten müssen Sie mindestens zwei Volumes (LUNs) verfügbar machen, wenn Sie die Server mit dem Clusterspeicher verbinden. Für gründliche Tests der Konfiguration können Sie bei Bedarf zusätzliche Volumes verfügbar machen. Die Clustervolumes dürfen nicht für Server verfügbar gemacht werden, die sich nicht im Cluster befinden.

**So verbinden Sie den Clusterserver mit den Netzwerken und dem Speicher**

1. Lesen Sie die Details zu Netzwerken unter Hardware Anforderungen für einen Failovercluster mit zwei Knoten und Netzwerkinfrastruktur-und Domänen Kontoanforderungen für einen Failovercluster mit zwei Knoten weiter oben in dieser Anleitung.

2. Verbinden und konfigurieren Sie die Netzwerke, die die Server im Cluster verwenden.

3. Wenn die Testkonfiguration Clients oder einen nicht geclusterten Domänencontroller umfasst, stellen Sie sicher, dass diese Computer über mindestens ein Netzwerk eine Verbindung mit den geclusterten Servern herstellen können.

4. Befolgen Sie die Anweisungen des Herstellers zum physischen Verbinden der Server mit dem Speicher.

5. Stellen Sie sicher, dass die Datenträger (LUNs), die Sie im Cluster verwenden möchten, für die zu gruppierenden Server (und zwar ausschließlich für diese Server) bereitgestellt wurden. Sie können Datenträger oder LUNs mit einer der folgenden Schnittstellen verfügbar machen:

   - Die Schnittstelle, die vom Hersteller des Speichers bereitgestellt wird

   - Wenn Sie iSCSI verwenden, eine entsprechende iSCSI-Schnittstelle

6. Wenn Sie Software erworben haben, mit der das Format oder die Funktion des Datenträgers gesteuert wird, befolgen Sie die Anweisungen des Herstellers, um zu erfahren, wie Sie diese Software mit Windows Server verwenden.

7. Klicken Sie auf einem der in den Cluster einzuschließenden Server nacheinander auf Start, Verwaltung, Computerverwaltung und Datenträgerverwaltung. (Wenn das Dialogfeld Benutzerkontensteuerung angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf Weiter.) Vergewissern Sie sich unter Datenträgerverwaltung, dass die Cluster Datenträger sichtbar sind.

8. Wenn Sie ein Speichervolume mit mehr als zwei Terabyte erstellen möchten und Sie zum Steuern des Datenträgerformats die Windows-Benutzeroberfläche verwenden, konvertieren Sie diesen Datenträger in den Partitionstyp GPT (GUID-Partitionstabelle). Sichern Sie hierzu alle Daten auf dem Datenträger, löschen Sie alle Volumes auf dem Datenträger, klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf den Datenträger (nicht jedoch auf eine Partition), und klicken Sie auf In GPT-Datenträger konvertieren. Für Volumes mit weniger als zwei Terabyte können Sie statt GPT den Partitionstyp MBR (Master Boot Record) verwenden.

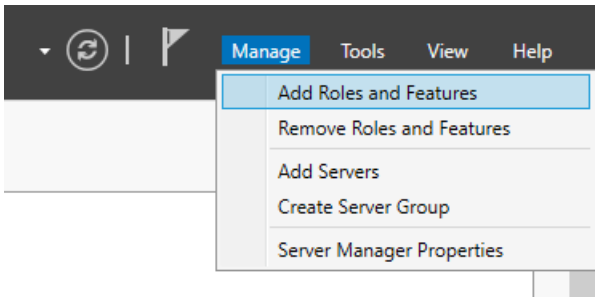
9. Überprüfen Sie das Format aller verfügbar gemachten Volumes bzw. LUNs. Es wird empfohlen, als Format NTFS zu verwenden (für den Zeugendatenträger muss NTFS verwendet werden).

### Schritt 2: Installieren der Dateiserver Rolle und des Failoverclusterfeatures

In diesem Schritt werden die Dateiserver Rolle und das Failoverclusterfeature installiert. Auf beiden Servern muss entweder Windows Server 2016 oder Windows Server 2019 ausgeführt werden.

**Verwenden von Server-Manager**

1. Öffnen Sie **Server-Manager** , und wählen Sie in der Dropdown-Dropdown- **Verwaltung Rollen und Features hinzufügen**.

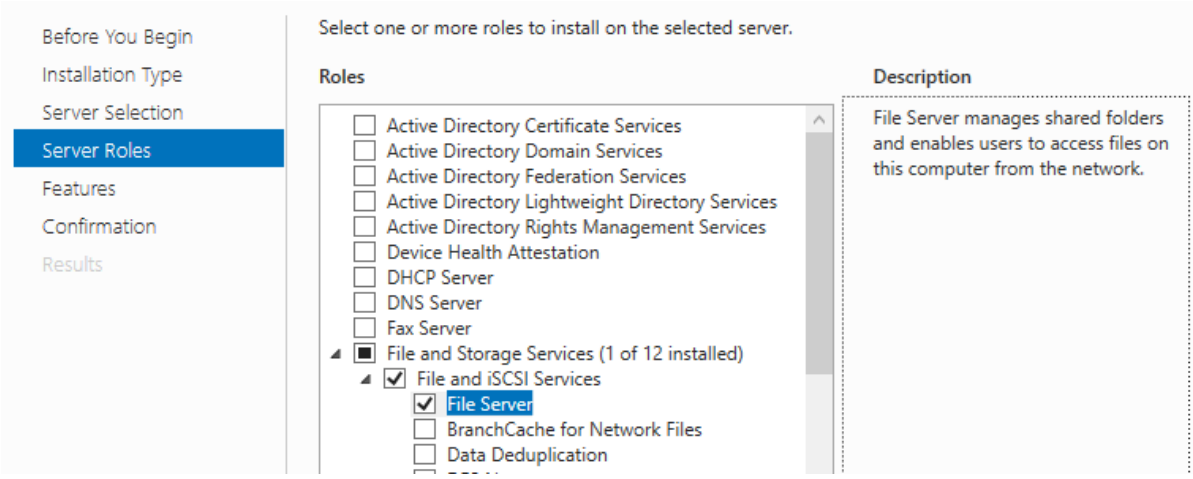



2. Wenn das Fenster **vor dem Beginn** geöffnet wird, wählen Sie **weiter** aus.

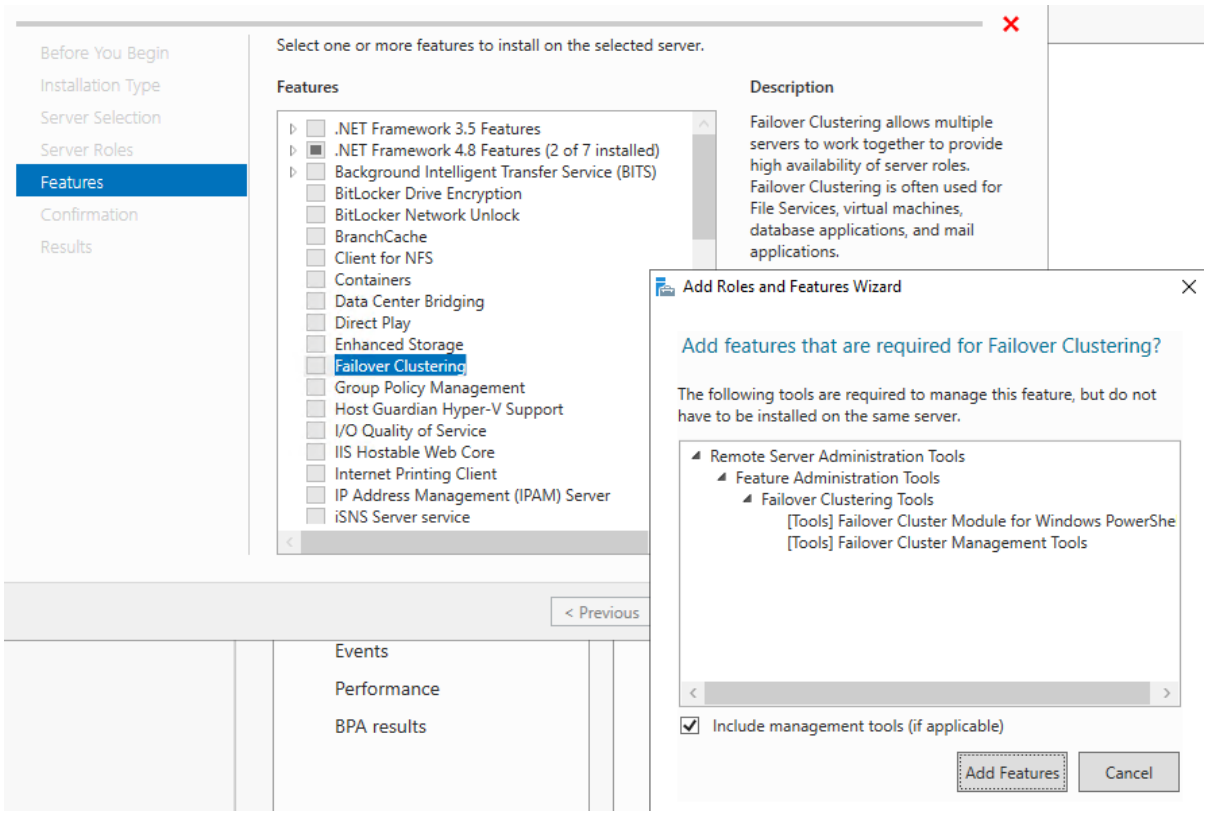
3. Wählen Sie für **Installationstyp** die Option **rollenbasierte oder featurebasierte Installation** und **dann weiter** aus.

4. Stellen Sie sicher, dass **Server aus dem Server Pool auswählen** ausgewählt ist, der Name des Computers hervorgehoben ist und **dann weiter**.

5. Öffnen Sie für die Server Rolle in der Liste der Rollen die **Dateidienste**, und wählen Sie dann **Datei Server** und **weiter** aus.




6. Wählen Sie für die Features in der Liste der Features **Failoverclustering** aus. Ein Popup Dialogfeld wird angezeigt, in dem die zu installierende Verwaltungs Tools aufgelistet sind. Behalten Sie alle ausgewählten Optionen bei, wählen Sie **Features hinzufügen** und **weiter** aus.




7. Wählen Sie auf der Seite Bestätigung die Option installieren aus.

8. Nachdem die Installation abgeschlossen ist, starten Sie den Computer neu.

9. Wiederholen Sie die Schritte auf dem zweiten Computer.

**Verwenden von PowerShell**

1. Öffnen Sie eine administrative PowerShell-Sitzung, indem Sie mit der rechten Maustaste auf die Schaltfläche Start klicken und dann **Windows PowerShell (admin)** auswählen.

2. Um die Datei Server Rolle zu installieren, führen Sie den folgenden Befehl aus:

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

3. Führen Sie den folgenden Befehl aus, um das Failoverclustering-Feature und seine Verwaltungs Tools zu installieren:

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

4. Sobald Sie abgeschlossen sind, können Sie mit den folgenden Befehlen überprüfen, ob Sie installiert sind:

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

5. Wenn Sie überprüft haben, starten Sie den Computer mit dem folgenden Befehl neu:

```
Restart-Computer
```

6. Wiederholen Sie die Schritte auf dem zweiten Server.

### Schritt 3: Überprüfen der Cluster Konfiguration

Es wird dringend empfohlen, vor dem Erstellen eines Clusters die Konfiguration zu überprüfen. Anhand der

Überprüfung können Sie sicherstellen, dass die Konfiguration der Server, Netzwerke und Speicher eine Reihe bestimmter Anforderungen für Failovercluster erfüllt.

**Verwenden von Failovercluster-Manager**

1. Wählen Sie in **Server-Manager** das Dropdown- **Tool** aus, und wählen Sie **Failovercluster-Manager** aus.
2. Wechseln Sie in **Failovercluster-Manager** zur mittleren Spalte unter **Verwaltung** , und klicken Sie auf **Konfiguration** überprüfen.
3. Wenn das Fenster **vor dem Beginn** geöffnet wird, wählen Sie **weiter** aus.
4. Fügen Sie im Fenster **Server oder Cluster auswählen** die Namen der beiden Computer hinzu, die die Knoten des Clusters sein werden. Wenn die Namen z. b. Node1 und Node2 lauten, geben Sie den Namen ein, und wählen Sie **Hinzufügen** aus. Sie können auch auf die Schaltfläche **Durchsuchen** klicken, um Active Directory nach den Namen zu suchen. Wenn beide unter **ausgewählte Server** aufgeführt sind, wählen Sie **weiter** aus.
5. Wählen Sie im Fenster **Test Optionen die Option alle Tests ausführen (empfohlen)** und **weiter** aus.
6. Auf der **Bestätigungs** Seite erhalten Sie die Liste aller Tests, die überprüft werden. Wählen Sie **weiter** aus, und die Tests werden gestartet.
7. Nach Abschluss des Vorgangs wird die Seite **Zusammenfassung** angezeigt, nachdem die Tests ausgeführt wurden. Um Hilfethemen anzuzeigen, die Ihnen bei der Interpretation der Ergebnisse helfen, klicken Sie auf **Weitere Informationen über Clustervalidierungstests**.
8. Klicken Sie auf der Seite Zusammenfassung auf Bericht anzeigen, und lesen Sie die Testergebnisse. Nehmen Sie erforderliche Änderungen an der Konfiguration vor, und führen Sie die Tests erneut aus. Informationen zum Anzeigen der Ergebnisse der Tests, nachdem Sie den Assistenten geschlossen haben, finden Sie unter *systemroot\cluster\reports\validation Report Date and Time. html*.
9. Um Hilfethemen zur Clustervalidierung nach dem Schließen des Assistenten anzuzeigen, klicken Sie in der Failovercluster-Verwaltung auf Hilfe, Hilfethemen und auf die Registerkarte Inhalt. Erweitern Sie den Inhalt für die Failoverclusterhilfe, und klicken Sie auf Überprüfen einer Failoverclusterkonfiguration.

**Verwenden von PowerShell**

1. Öffnen Sie eine administrative PowerShell-Sitzung, indem Sie mit der rechten Maustaste auf die Schaltfläche Start klicken und dann **Windows PowerShell (admin)** auswählen.
2. Führen Sie den folgenden Befehl aus, um die Computer (z. b. die Computernamen Node1 und Node2) für das Failoverclustering zu überprüfen:

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

3. Wenn Sie die Ergebnisse der Tests anzeigen möchten, nachdem Sie den Assistenten geschlossen haben, sehen Sie sich die angegebene Datei (in systemroot\cluster\reports)an, nehmen Sie dann alle erforderlichen Änderungen an der Konfiguration vor, und führen Sie die Tests erneut aus.

Weitere Informationen finden Sie unter Validieren einer Failoverclusterkonfiguration.

### Schritt 4: Erstellen des Clusters

Im folgenden wird ein Cluster aus den Computern und der Konfiguration erstellt, die Sie besitzen.

**Verwenden von Failovercluster-Manager**

1. Wählen Sie in **Server-Manager** das Dropdown- **Tool** aus, und wählen Sie **Failovercluster-Manager** aus.
2. Wechseln Sie in **Failovercluster-Manager** zur mittleren Spalte unter **Verwaltung** , und klicken Sie auf **Cluster erstellen**.

3. Wenn das Fenster **vor dem Beginn** geöffnet wird, wählen Sie **weiter** aus.

4. Fügen Sie im Fenster **Server auswählen** die Namen der beiden Computer hinzu, die die Knoten des Clusters sein werden. Wenn die Namen z. b. Node1 und Node2 lauten, geben Sie den Namen ein, und wählen Sie **Hinzufügen** aus. Sie können auch auf die Schaltfläche **Durchsuchen** klicken, um Active Directory nach den Namen zu suchen. Wenn beide unter **ausgewählte Server** aufgeführt sind, wählen Sie **weiter** aus.

5. Geben Sie im **Zugriffspunkt für die Verwaltung des Cluster** Fensters den Namen des Clusters ein, den Sie verwenden werden. Beachten Sie, dass dies nicht der Name ist, den Sie für die Verbindung mit den Dateifreigaben mit verwenden werden. Dies dient lediglich der Verwaltung des Clusters.

   > **NOTE**
   > Wenn Sie statische IP-Adressen verwenden, müssen Sie das zu verwendende Netzwerk auswählen und die IP-Adresse eingeben, die für den Cluster Namen verwendet werden soll. Wenn Sie DHCP für Ihre IP-Adressen verwenden, wird die IP-Adresse automatisch für Sie konfiguriert.

6. Wählen Sie **weiter** aus.

7. Überprüfen Sie auf der Seite **Bestätigung** , was Sie konfiguriert haben, und klicken Sie auf **weiter** , um den Cluster zu erstellen.

8. Auf der Seite **Zusammenfassung** erhalten Sie die Konfiguration, die Sie erstellt hat. Sie können Bericht anzeigen auswählen, um den Bericht der Erstellung anzuzeigen.

#### Verwenden von PowerShell

1. Öffnen Sie eine administrative PowerShell-Sitzung, indem Sie mit der rechten Maustaste auf die Schaltfläche Start klicken und dann **Windows PowerShell (admin)** auswählen.

2. Führen Sie den folgenden Befehl aus, um den Cluster zu erstellen, wenn Sie statische IP-Adressen verwenden. Die Computernamen sind z. b. Node1 und Node2, der Name des Clusters ist Cluster, und die IP-Adresse lautet 1.1.1.1.

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

3. Führen Sie den folgenden Befehl aus, um den Cluster zu erstellen, wenn Sie DHCP für IP-Adressen verwenden. Die Computernamen sind z. b. Node1 und Node2, und der Name des Clusters ist Cluster.

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

### Schritte zum Konfigurieren eines Dateiserver-Failoverclusters

Führen Sie die folgenden Schritte aus, um einen Dateiserver-Failovercluster zu konfigurieren.

1. Wählen Sie in **Server-Manager** das Dropdown- **Tool** aus, und wählen Sie **Failovercluster-Manager** aus.

2. Wenn Failovercluster-Manager geöffnet wird, sollte der Name des Clusters, den Sie erstellt haben, automatisch angezeigt werden. Wenn dies nicht der Fall ist, wechseln Sie in der mittleren Spalte unter **Verwaltung** , und wählen Sie **mit Cluster verbinden** aus. Geben Sie den Namen des Clusters ein, den Sie erstellt haben, und **OK**.

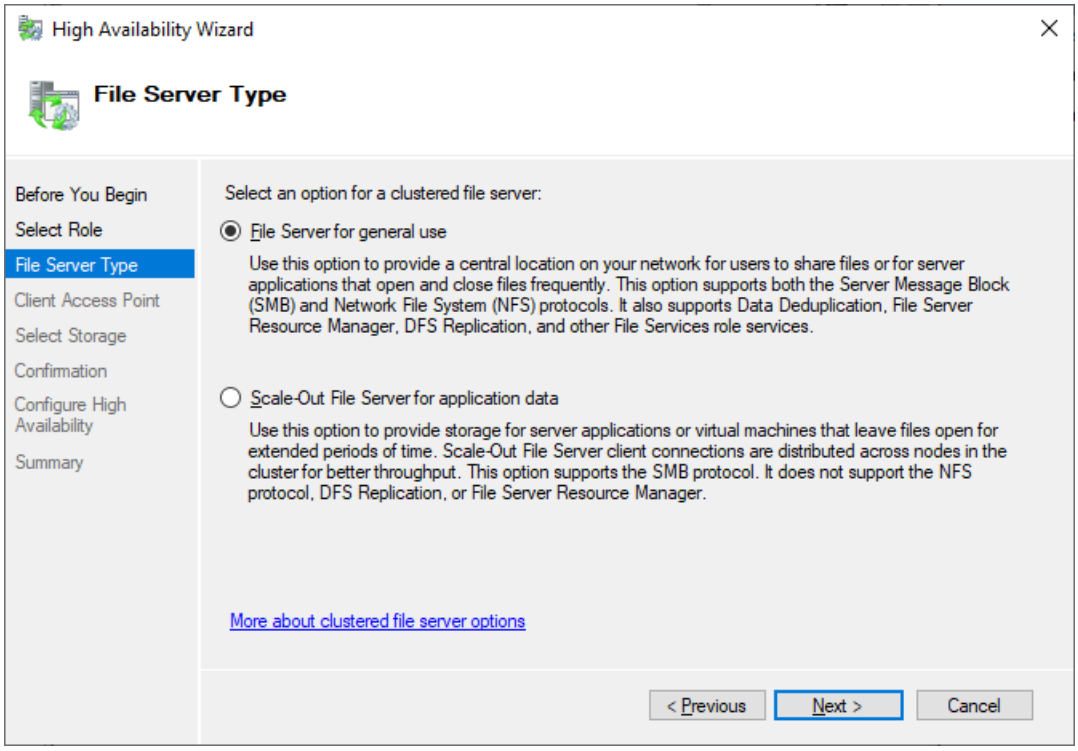
3. Klicken Sie in der Konsolen Struktur neben dem Cluster, den Sie erstellt haben, auf das Zeichen ">", um die darunter liegenden Elemente zu erweitern.

4. Klicken Sie mit der rechten Maustaste auf **Rollen** , und wählen Sie **Rolle konfigurieren**.

5. Wenn das Fenster **vor dem Beginn** geöffnet wird, wählen Sie **weiter** aus.

6. Wählen Sie in der Liste der Rollen **Datei Server** und **dann weiter** aus.

7. Wählen Sie für den Datei Servertyp die Option **Dateiserver zur allgemeinen Verwendung** und **dann weiter** aus.
   Informationen zu Dateiserver mit horizontaler Skalierung finden Sie unter Dateiserver mit horizontaler Skalierung Übersicht.




8. Geben Sie im Fenster **Client Zugriffspunkt** den Namen des Dateiservers ein, den Sie verwenden werden. Beachten Sie, dass dies nicht der Name des Clusters ist. Dies gilt für die Verbindung mit der Dateifreigabe. Wenn beispielsweise eine Verbindung mit \Server hergestellt werden soll, lautet der Name, der als "Server" verwendet wird.

   > **NOTE**
   > Wenn Sie statische IP-Adressen verwenden, müssen Sie das zu verwendende Netzwerk auswählen und die IP-Adresse eingeben, die für den Cluster Namen verwendet werden soll. Wenn Sie DHCP für Ihre IP-Adressen verwenden, wird die IP-Adresse automatisch für Sie konfiguriert.

9. Wählen Sie **weiter** aus.

10. Wählen Sie im Fenster **Speicher auswählen** das zusätzliche Laufwerk (nicht den Zeugen) aus, auf dem sich die Freigaben **befinden.**

11. Überprüfen Sie auf der Seite **Bestätigung** Ihre Konfiguration, und wählen Sie **weiter** aus.

12. Auf der Seite **Zusammenfassung** erhalten Sie die Konfiguration, die Sie erstellt hat. Sie können Bericht anzeigen auswählen, um den Bericht zur Erstellung der Dateiserver Rolle anzuzeigen.

13. Unter **Rollen** in der Konsolen Struktur sehen Sie, dass die neu erstellte Rolle als der von Ihnen erstellte Name aufgeführt wird. Wählen Sie unter dem Bereich **Aktionen** auf der rechten Seite die Option **Freigabe hinzufügen** aus.

14. Führen Sie den Freigabe-Assistenten aus, und geben Sie Folgendes ein:

    - Typ der Freigabe

- Speicherort/Pfad des freigegebenen Ordners
- Der Name der Freigabe, mit der Benutzer eine Verbindung herstellen.
- Zusätzliche Einstellungen wie z. b. Zugriffs basierte Aufzählung, Caching, Verschlüsselung usw.
- Berechtigungen auf Dateiebene, wenn Sie nicht die Standardwerte sind

15. Überprüfen Sie auf der Seite **Bestätigung** , was Sie konfiguriert haben, und wählen Sie **Erstellen** aus, um die Dateiserver Freigabe zu erstellen.

16. Wählen Sie auf der Seite **Ergebnisse** die Option schließen aus, wenn die Freigabe erstellt wurde. Wenn die Freigabe nicht erstellt werden konnte, erhalten Sie die Fehler.

17. Wählen Sie **Schließen** aus.

18. Wiederholen Sie diesen Vorgang für alle weiteren Freigaben.

# Vorabbereitstellen von Clustercomputerobjekten in Active Directory Domain Services

02.05.2020 • 16 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In diesem Thema wird gezeigt, wie Sie Clustercomputerobjekte in den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS) vorab bereitstellen. Sie können mit diesem Verfahren Benutzern oder Gruppen, die nicht über Berechtigungen zum Erstellen von Computerobjekten in AD DS verfügen, das Erstellen eines Failoverclusters ermöglichen.

Beim Erstellen eines Failoverclusters mit dem Clustererstellungs-Assistenten oder mit Windows PowerShell müssen Sie einen Namen für den Cluster angeben. Wenn Sie beim Erstellen des Clusters über ausreichende Berechtigungen verfügen, wird automatisch in AD DS ein Computerobjekt erstellt, das den gleichen Namen hat wie der Cluster. Dieses Objekt wird als *Clusternamenobjekt* oder CNO bezeichnet. Über das CNO werden automatisch virtuelle Computerobjekte (VCOs) erstellt, wenn Sie Clusterrollen konfigurieren, von denen Clientzugriffspunkte verwendet werden. Wenn Sie beispielsweise einen hoch verfügbaren Dateiserver mit einem Clientzugriffspunkt mit dem Namen *Dateiserver1*erstellen, wird vom CNO ein entsprechendes VCO in AD DS erstellt.

> **NOTE**
> Es gibt die Option, einen Active Directory getrennten Cluster zu erstellen, bei dem in AD DS keine CNO oder VCOs erstellt werden. Diese Möglichkeit ist für bestimmte Typen von Clusterbereitstellungen gedacht. Weitere Informationen finden Sie unter Bereitstellen eines von Active Directory getrennten Clusters.

Für die automatische Erstellung des CNOs benötigt der Benutzer, der den Failovercluster erstellt, die Berechtigung **Computerobjekte erstellen** für die Organisationseinheit (Organizational Unit, OU) oder den Container, in dem sich die Server befinden, aus denen der Cluster gebildet werden soll. Ein Benutzer mit entsprechenden Berechtigungen in AD DS (normalerweise ein Domänenadministrator) kann das CNO vorab in AD DS bereitstellen, damit ein Benutzer oder eine Gruppe ohne diese Berechtigung einen Cluster erstellen kann. Dadurch hat der Domänenadministrator außerdem mehr Kontrolle über die für den Cluster verwendete Benennungskonvention sowie darüber, in welcher Organisationseinheit die Clusterobjekte erstellt werden.

## Schritt 1: Vorabbereitstellen des CNOs in AD DS

Bevor Sie beginnen, sollten Sie sicherstellen, dass folgende Informationen vorhanden sind:

- Der Name, den Sie dem Cluster zuweisen möchten
- Der Name des Benutzerkontos oder der Gruppe, dem bzw. der Sie Rechte zum Erstellen des Clusters erteilen möchten.

Als bewährte Methode wird empfohlen, eine Organisationseinheit für die Clusterobjekte zu erstellen. Wenn bereits eine Organisationseinheit vorhanden ist, die Sie verwenden möchten, ist zum Ausführen dieses Schritts mindestens die Mitgliedschaft in der Gruppe **Konten-Operatoren** erforderlich. Wenn Sie eine Organisationseinheit für die Clusterobjekte erstellen, müssen Sie mindestens Mitglied der Gruppe **Domänen-Admins** oder einer entsprechenden Gruppe sein, um diesen Schritt auszuführen.

> **NOTE**
> Wenn Sie das CNO im Standardcontainer %%amp;quot;Computer%%amp;quot; anstatt in einer Organisationseinheit erstellen, müssen Sie Schritt 3 dieses Themas nicht ausführen. In diesem Szenario kann ein Clusteradministrator bis zu zehn VCOs ohne zusätzliche Konfiguration erstellen.

**CNO in AD DS vorab bereitstellen**

1. Öffnen Sie auf einem Computer, auf dem die AD DS-Tools aus den Remoteserver-Verwaltungstools installiert sind, oder auf einem Domänencontroller das Snap-In **Active Directory-Benutzer und -Computer**. Um dies auf einem Server zu erreichen, starten Sie Server-Manager, und wählen Sie dann **im Menü Extras** die Option **Active Directory Benutzer und Computer** aus.

2. Zum Erstellen einer Organisationseinheit für die Cluster Computer Objekte klicken Sie mit der rechten Maustaste auf den Domänen Namen oder eine vorhandene Organisationseinheit, zeigen Sie auf **neu**, und wählen Sie dann **Organisationseinheit** aus. Geben Sie im Feld **Name** den Namen der Organisationseinheit ein, und klicken Sie dann auf **OK**.

3. Klicken Sie in der Konsolen Struktur mit der rechten Maustaste auf die Organisationseinheit, in der Sie das CNO erstellen möchten, zeigen Sie auf **neu**, und wählen Sie dann **Computer** aus.

4. Geben Sie im Feld **Computer Name** den Namen ein, der für den Failovercluster verwendet werden soll, und klicken Sie dann auf **OK**.

   > **NOTE**
   > Diesen Clusternamen gibt der Benutzer, der den Cluster erstellt, auf der Seite **Zugriffspunkt für die Clusterverwaltung** im Clustererstellungs-Assistenten oder als Wert des *–Name* -Parameters für das Windows PowerShell-Cmdlet **New-Cluster** an.

5. Klicken Sie als bewährte Vorgehensweise mit der rechten Maustaste auf das gerade erstellte Computer Konto, wählen Sie **Eigenschaften** aus, und klicken Sie dann auf die Registerkarte **Objekt** . Aktivieren Sie auf der Registerkarte **Objekt** das Kontrollkästchen **Objekt vor zufälligem Löschen schützen** , und klicken Sie dann auf **OK**.

6. Klicken Sie mit der rechten Maustaste auf das gerade erstellte Computer Konto, und wählen Sie dann **Konto deaktivieren** aus. Wählen Sie zur Bestätigung **Ja** aus, und klicken Sie dann auf **OK**.

   > **NOTE**
   > Sie müssen das Konto deaktivieren, damit bei der Clustererstellung überprüft werden kann, ob das Konto zurzeit von einem vorhandenen Computer oder Cluster in der Domäne verwendet wird.

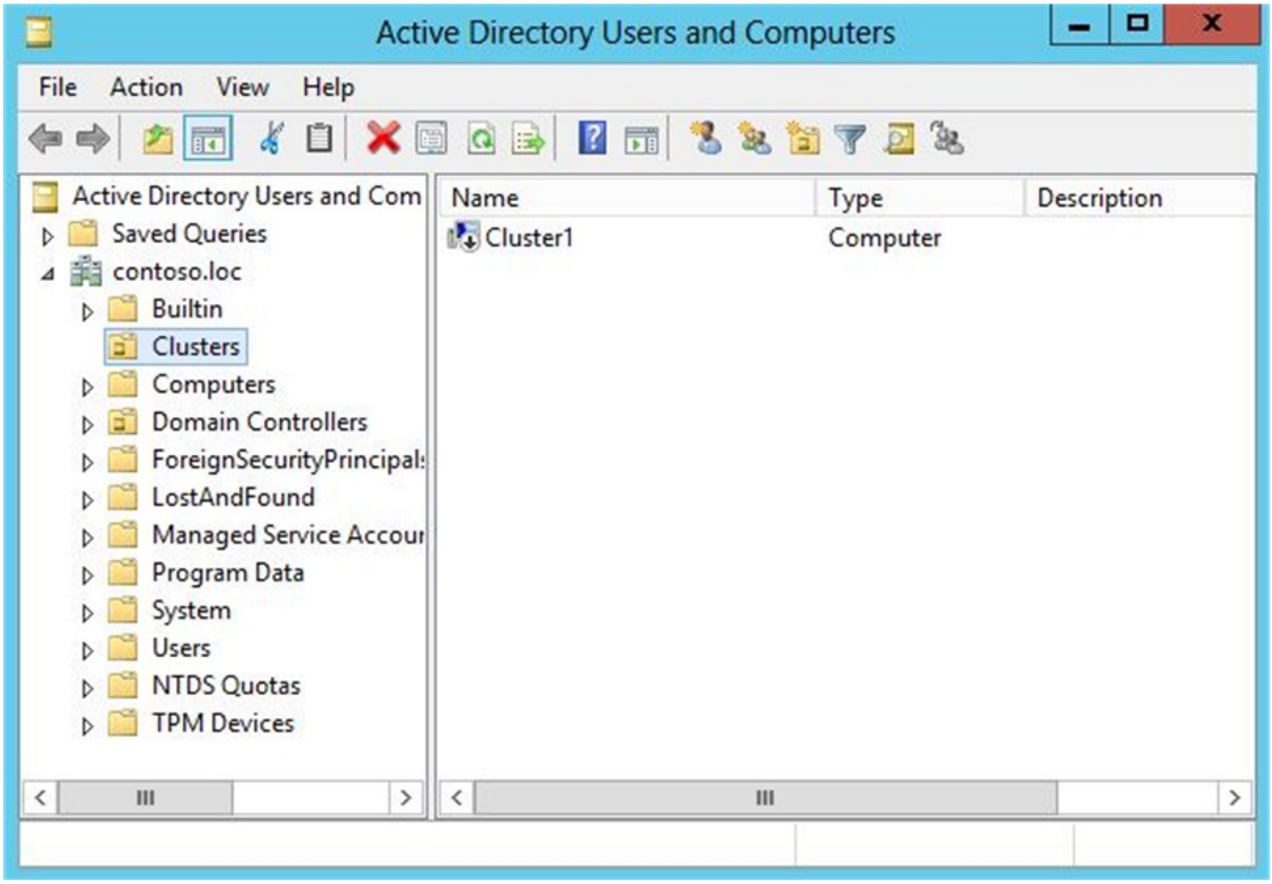



**Abbildung 1. Deaktiviertes CNO in der Organisationseinheit für Beispiel Cluster**

## Schritt 2: Erteilen der Benutzerberechtigungen zum Erstellen des Clusters

Sie müssen Berechtigungen konfigurieren, damit das Benutzerkonto, das zum Erstellen des Failoverclusters verwendet wird, über Vollzugriff auf das gerade erstellte CNO verfügt:

Sie müssen mindestens Mitglied der Gruppe **Konten-Operatoren** sein, um diesen Schritt ausführen zu können.

So erteilen Sie dem Benutzerberechtigungen zum Erstellen des Clusters:

1. Stellen Sie in %%amp;quot;Active Directory-Benutzer und -Computer%%amp;quot; sicher, dass im Menü **Ansicht** die Option **Erweiterte Features** ausgewählt ist.
2. Suchen Sie das CNO, klicken Sie mit der rechten Maustaste darauf, und wählen Sie dann **Eigenschaften**aus.
3. Wählen Sie auf der Registerkarte **Sicherheit** die Option **Hinzufügen** aus.
4. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppen auswählen** das Benutzerkonto oder die Gruppe an, dem bzw. der Sie Berechtigungen erteilen möchten, und klicken Sie dann auf **OK**.
5. Wählen Sie das gerade hinzugefügte Benutzerkonto bzw. die gerade hinzugefügte Gruppe aus, und aktivieren Sie dann neben **Vollzugriff** das Kontrollkästchen **Zulassen**.

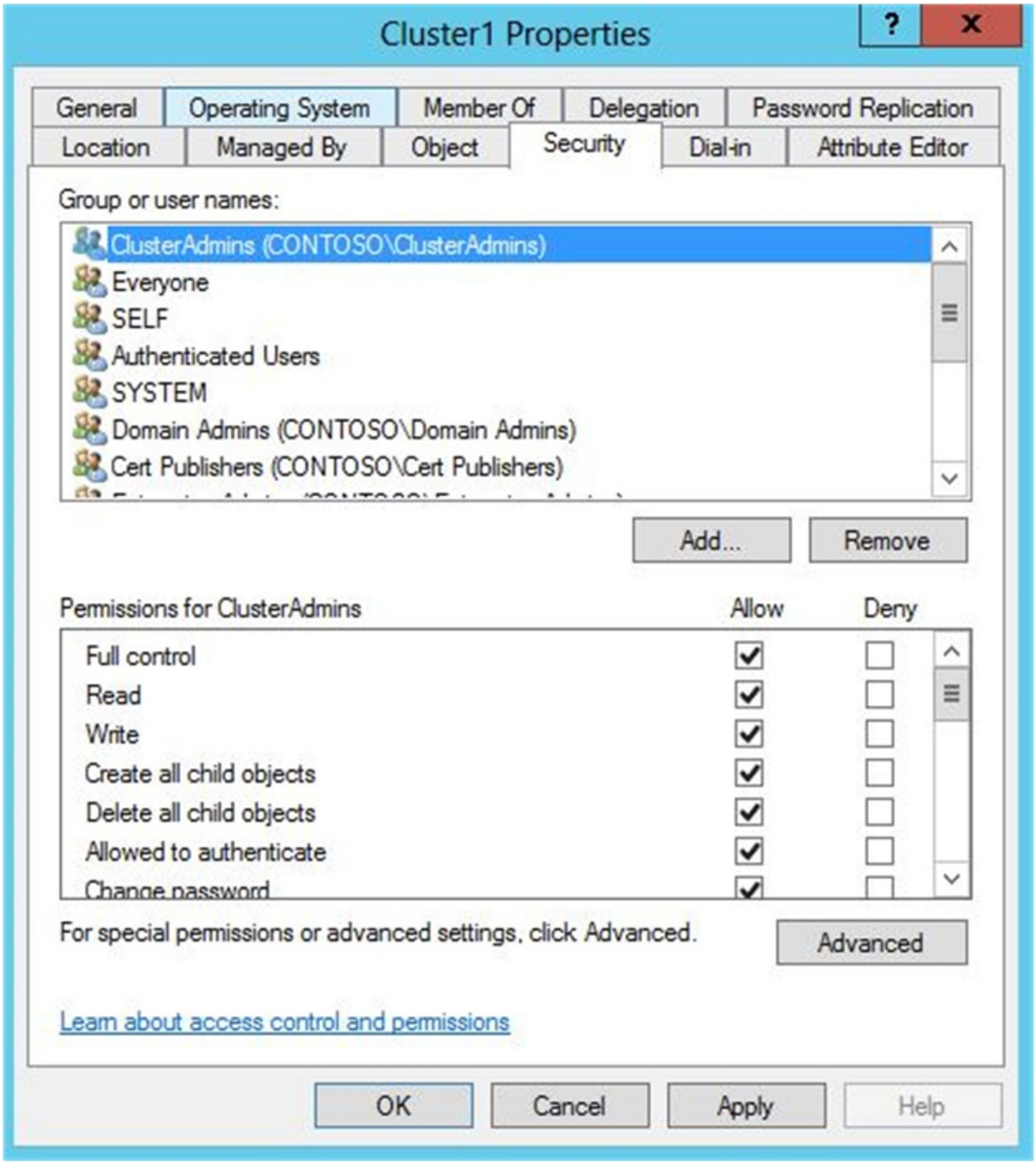



**Abbildung 2. Gewähren der vollständigen Kontrolle für den Benutzer oder die Gruppe, der den Cluster erstellt**

6. Klicken Sie auf **OK**.

Nach Abschluss dieses Schritts kann der Benutzer, dem Sie Berechtigungen erteilt haben, den Failovercluster erstellen. Wenn sich das CNO jedoch in einer Organisationseinheit befindet, kann der Benutzer erst dann Clusterrollen erstellen, für die ein Clientzugriffspunkt erforderlich ist, wenn Sie Schritt 3 abgeschlossen haben.

> **NOTE**
>
> Wenn sich das CNO im Standardcontainer %%amp;quot;Computer%%amp;quot; befindet, kann ein Clusteradministrator bis zu zehn VCOs ohne zusätzliche Konfiguration erstellen. Zum Hinzufügen von mehr als zehn VCOs müssen Sie explizit die Berechtigung **Computerobjekte erstellen** für das CNO für den Container %%amp;quot;Computer%%amp;quot; erteilen.

## Schritt 3: Erteilen der CNO-Berechtigungen für die Organisationseinheit oder Vorabbereitstellen von VCOs für

## Clusterrollen

Wenn Sie eine Clusterrolle mit einem Clientzugriffspunkt erstellen, wird vom Cluster ein VCO in der gleichen Organisationseinheit erstellt, in der sich das CNO befindet. Damit dies automatisch geschieht, muss das CNO über Berechtigungen zum Erstellen von Computerobjekten in der Organisationseinheit verfügen.

Wenn Sie das CNO vorab in AD DS bereitgestellt haben, können Sie eine der folgenden Aktionen ausführen, um VCOs zu erstellen:

- Option 1: Erteilen der CNO-Berechtigungen für die Organisationseinheit. Wenn Sie diese Option verwenden, können vom Cluster automatisch VCOs in AD DS erstellt werden. Daher kann ein Administrator für den Failovercluster Clusterrollen erstellen und muss Sie dazu nicht bitten, VCOs vorab in AD DS bereitstellen.

> **NOTE**
> Sie müssen mindestens Mitglied der Gruppe **Domänen-Admins** oder einer entsprechenden Gruppe sein, um die Schritte für diese Option ausführen zu können.

- Option 2: vorab Bereitstellen eines VCO für eine Cluster Rolle. Verwenden Sie diese Option, wenn aufgrund von Anforderungen in der Organisation Konten für Clusterrollen vorab bereitgestellt werden müssen. Beispielsweise kann es sein, dass Sie die Benennungskonvention steuern möchten, oder steuern möchten, welche Clusterrollen erstellt werden.

> **NOTE**
> Sie müssen mindestens Mitglied der Gruppe **Konten-Operatoren** oder einer entsprechenden Gruppe sein, um die Schritte für diese Option ausführen zu können.

**Erteilen der CNO-Berechtigungen für die Organisationseinheit**

1. Stellen Sie in %%amp;quot;Active Directory-Benutzer und -Computer%%amp;quot; sicher, dass im Menü **Ansicht** die Option **Erweiterte Features** ausgewählt ist.
2. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, in der Sie das CNO in Schritt 1: vorab Bereitstellen des CNO in AD DSerstellt haben, und wählen Sie dann **Eigenschaften**.
3. Wählen Sie auf der Registerkarte **Sicherheit** die Option **erweitert**aus.
4. Wählen Sie im Dialogfeld **Erweiterte Sicherheitseinstellungen** die Option **Hinzufügen**aus.
5. Klicken Sie neben **Prinzipal**auf **Prinzipal auswählen**.
6. Wählen Sie im Dialogfeld **Benutzer, Computer, Dienst Konto oder Gruppen auswählen** die **Objekttypen**aus, aktivieren Sie das Kontrollkästchen **Computer** , und klicken Sie dann auf **OK**.
7. Geben Sie unter **Geben Sie die zu ausgewäfenden Objektnamen**ein den Namen des CNO ein, wählen Sie **Namen überprüfen**aus, und klicken Sie dann auf **OK**. Wählen Sie als Antwort auf die Warnmeldung, die besagt, dass Sie im Begriff sind, ein deaktiviertes Objekt hinzuzufügen, **OK**aus.
8. Stellen Sie im Dialogfeld **Berechtigungseintrag** sicher, dass die Liste **Typ** auf **Zulassen** und die Liste **Anwenden auf** auf **Dieses und alle untergeordneten Objekte** festgelegt ist.
9. Aktivieren Sie unter **Berechtigungen** das Kontrollkästchen **Computerobjekte erstellen**.

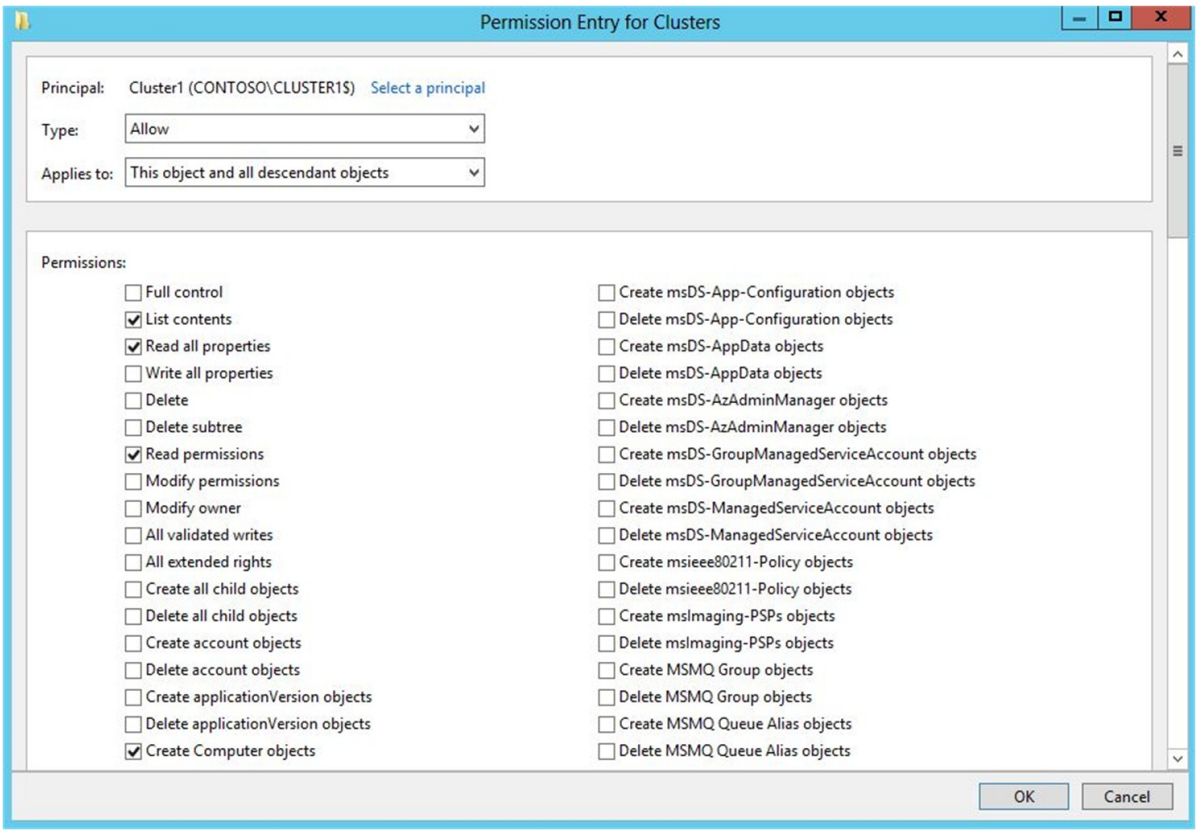



**Abbildung 3. Erteilen der Berechtigung zum Erstellen von Computer Objekten für das CNO**

10. Wählen Sie **OK** , bis Sie zum Active Directory Benutzer-und Computer-Snap-in zurückkehren.

Ein Administrator des Failoverclusters kann jetzt Clusterrollen mit Clientzugriffspunkten erstellen und die Ressourcen online schalten.

**Vorab Bereitstellen eines VCO für eine Cluster Rolle**

1. Stellen Sie, bevor Sie beginnen, sicher, dass Sie den Namen des Clusters und den Namen, den die Clusterrolle erhalten wird, kennen.
2. Stellen Sie in %%amp;quot;Active Directory-Benutzer und -Computer%%amp;quot; sicher, dass im Menü **Ansicht** die Option **Erweiterte Features** ausgewählt ist.
3. Klicken Sie unter Active Directory Benutzer und Computer mit der rechten Maustaste auf die Organisationseinheit, in der sich das CNO für den Cluster befindet, zeigen Sie auf **neu**, und wählen Sie dann **Computer**aus.
4. Geben Sie im Feld **Computer Name** den Namen ein, der für die Cluster Rolle verwendet werden soll, und klicken Sie dann auf **OK**.
5. Klicken Sie als bewährte Vorgehensweise mit der rechten Maustaste auf das gerade erstellte Computer Konto, wählen Sie **Eigenschaften**aus, und klicken Sie dann auf die Registerkarte **Objekt** . Aktivieren Sie auf der Registerkarte **Objekt** das Kontrollkästchen **Objekt vor zufälligem Löschen schützen** , und klicken Sie dann auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf das gerade erstellte Computer Konto, und wählen Sie dann **Eigenschaften**aus.
7. Wählen Sie auf der Registerkarte **Sicherheit** die Option **Hinzufügen** aus.
8. Wählen Sie im Dialogfeld **Benutzer, Computer, Dienst Konto oder Gruppen auswählen** die **Objekttypen**aus, aktivieren Sie das Kontrollkästchen **Computer** , und klicken Sie dann auf **OK**.
9. Geben Sie unter **Geben Sie die zu ausgewäfenden Objektnamen**ein den Namen des CNO ein, wählen Sie **Namen überprüfen**aus, und klicken Sie dann auf **OK**. Wenn Sie eine Warnmeldung erhalten, die besagt, dass Sie im Begriff sind, ein deaktiviertes Objekt hinzuzufügen, klicken Sie auf **OK**.
10. Stellen Sie sicher, dass das CNO ausgewählt ist, und aktivieren Sie dann neben **Vollzugriff** das

Kontrollkästchen **Zulassen**.

11. Klicken Sie auf **OK**.

Ein Administrator des Failoverclusters kann jetzt die Clusterrolle mit einem Clientzugriffspunkt erstellen, die dem vorab bereitgestellten VCO-Namen entspricht, und die Ressource online schalten.

## Weitere Informationen

- Failoverclustering
- Konfigurieren von Clusterkonten in Active Directory

# Konfigurieren von Clusterkonten in Active Directory

14.04.2020 • 42 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 und Windows Server 2008

Wenn Sie in Windows Server einen Failovercluster erstellen und geclusterte Dienste oder Anwendungen konfigurieren, erstellen die Failovercluster-Assistenten die erforderlichen Active Directory Computer Konten (auch Computer Objekte genannt) und stellen Ihnen bestimmte Berechtigungen zur Verfügung. Die Assistenten erstellen ein Computerkonto für den Cluster (dieses Konto wird auch als das Clusternamenobjekt oder CNO bezeichnet) und ein Computerkonto für die meisten Typen von geclusterten Diensten und Anwendungen, mit Ausnahme des virtuellen Hyper-V-Computers. Die Berechtigungen für diese Konten werden von den Failovercluster-Assistenten automatisch festgelegt. Wenn die Berechtigungen geändert wurden, müssen sie wieder zurückgesetzt werden, damit sie den Clusteranforderungen entsprechen. In dieser Anleitung werden diese Active Directory-Konten und -Berechtigungen beschrieben, Hintergrundinformationen dazu bereitgestellt, warum sie wichtig sind, und Schritte zum Konfigurieren und Verwalten der Konten beschrieben.

## Übersicht über Active Directory-Konten, die von einem Failovercluster benötigt werden

In diesem Abschnitt werden die Active Directory-Computerkonten (auch als Active Directory-Computerobjekte bezeichnet) beschrieben, die für einen Failovercluster wichtig sind. Dabei handelt es sich um die folgenden Konten:

- **Das Benutzerkonto, das zum Erstellen des Clusters verwendet wird.** Dies ist das Benutzerkonto, das verwendet wird, um den Clustererstellungs-Assistenten zu starten. Das Konto ist wichtig, da es die Grundlage bereitstellt, auf der ein Computerkonto für den Cluster erstellt wird.

- **Das Cluster Namen Konto.** (das Computer Konto des Clusters selbst, auch als Cluster Namen Objekt oder CNO bezeichnet). Dieses Konto wird automatisch vom Clustererstellungs-Assistenten erstellt und hat den gleichen Namen wie der Cluster. Das Clusternamenkonto ist sehr wichtig, da über dieses Konto andere Konten automatisch erstellt werden, wenn Sie neue Dienste und Anwendungen auf dem Cluster konfigurieren. Wenn das Clusternamenkonto gelöscht wird oder dem Konto Berechtigungen entzogen werden, können erst dann wieder andere für den Cluster erforderliche Konten erstellt werden, wenn das Clusternamenkonto wiederhergestellt bzw. die entsprechenden Berechtigungen wieder erteilt wurden.

  Wenn Sie beispielsweise einen Cluster mit dem Namen Cluster1 erstellen und dann versuchen, in dem Cluster einen Clusterdruckerserver mit dem Namen PrintServer1 zu konfigurieren, muss das Konto Cluster1 in Active Directory die erforderlichen Berechtigungen beibehalten, damit es verwendet werden kann, um ein Computerkonto mit dem Namen PrintServer1 zu erstellen.

  Das Clusternamenkonto wird im Standardcontainer für Computerkonten in Active Directory erstellt. Standardmäßig handelt es sich hierbei um den Container "Computer", aber der Domänen Administrator kann ihn an einen anderen Container oder eine Organisationseinheit (OU) umleiten.

- **Das Computer Konto (Computer Objekt) eines geclusterten Dienstanbieter oder einer geclusterten Anwendung.** Diese Konten werden automatisch vom Assistenten für hohe Verfügbarkeit im Rahmen der Erstellung der meisten Typen von geclusterten Diensten und Anwendungen erstellt, mit Ausnahme von virtuellen Hyper-V-Computern. Dem Cluster Namen Konto werden die erforderlichen Berechtigungen zum Steuern dieser Konten gewährt.

  Wenn Sie beispielsweise über einen Cluster mit dem Namen Cluster1 verfügen und dann einen

Clusterdateiserver mit dem Namen FileServer1 erstellen, erstellt der Assistent für hohe Verfügbarkeit ein Active Directory-Computerkonto mit dem Namen FileServer1. Der Assistent für hohe Verfügbarkeit erteilt dem Konto Cluster1 außerdem die erforderlichen Berechtigungen zum Steuern des FileServer1-Kontos.

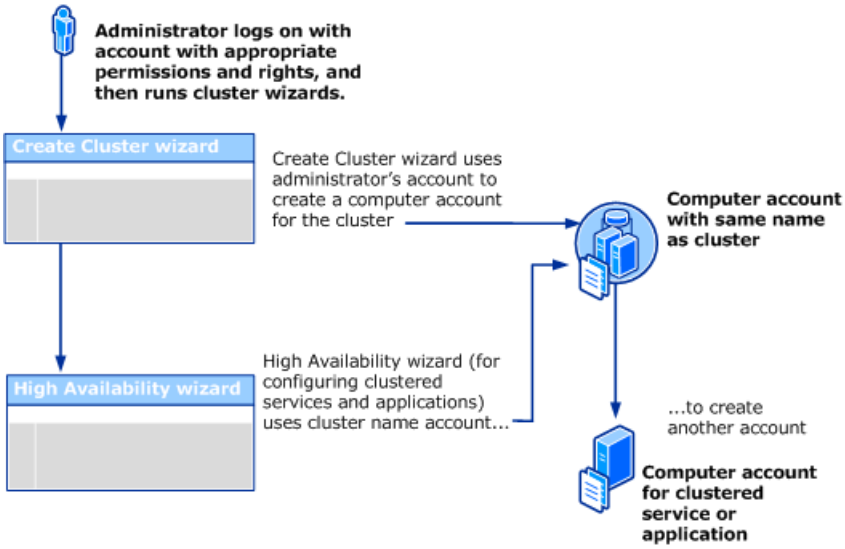
In der folgenden Tabelle werden die erforderlichen Berechtigungen für diese Konten beschrieben.

| KONTO | DETAILS ZU BERECHTIGUNGEN |
| --- | --- |
| Konto zum Erstellen des Clusters | Erfordert Administratorberechtigungen für die Server, die Clusterknoten werden. Benötigt außerdem die Berechtigung zum Erstellen von Computerobjektenund die Berechtigung zum Lesen aller Eigenschaftenin dem Container, der in der Domäne für Computerkonten verwendet wird. |
| Clusternamenkonto (Computerkonto des Clusters) | Wenn der Clustererstellungs-Assistent ausgeführt wird, erstellt er das Clusternamenkonto in dem Standardcontainer, der in der Domäne für Computerkonten verwendet wird. Standardmäßig kann das Clusternamenkonto (wie andere Computerkonten) bis zu zehn Computerkonten in der Domäne erstellen.<br><br>Wenn Sie das Clusternamenkonto (Clusternamenobjekt) erstellen, bevor Sie den Cluster erstellen, das Konto also vorab bereitstellen, müssen Sie diesem die Berechtigungen zum Erstellen von Computerobjektenund zum Lesen aller Eigenschaftenin dem Container erteilen, der in der Domäne für Computerkonten verwendet wird. Sie müssen das Konto außerdem deaktivieren und dem Konto **Vollzugriff** erteilen, das von dem Administrator verwendet wird, der den Cluster installiert. Weitere Informationen finden Sie weiter unten in dieser Anleitung unter Schritte für die Vorabbereitstellung des Clusternamenkontos. |
| Computerkonto eines geclusterten Diensts oder einer geclusterten Anwendung | Wenn der Assistent für hohe Verfügbarkeit ausgeführt wird (um einen neuen geclusterten Dienst oder eine neue Anwendung zu erstellen), wird in den meisten Fällen ein Computer Konto für den geclusterten Dienst oder die Anwendung in Active Directory erstellt. Dem Cluster Namen Konto werden die erforderlichen Berechtigungen zum Steuern dieses Kontos erteilt. Die Ausnahme ist ein geclusterter virtueller Hyper-V-Computer, für den kein Computer Konto erstellt wurde.<br><br>Wenn Sie das Computer Konto für einen geclusterten Dienst oder eine geclusterte Anwendung vorab bereitstellen, müssen Sie es mit den erforderlichen Berechtigungen konfigurieren. Weitere Informationen finden Sie weiter unten in dieser Anleitung unter Schritte für die Vorabbereitstellung eines Kontos für einen geclusterten Dienst oder eine geclusterte Anwendung. |

> **NOTE**
>
> In früheren Versionen von Windows Server gab es ein Konto für die Clusterdienst. Seit Windows Server 2008 wird der Clusterdienst jedoch automatisch in einem besonderen Kontext ausgeführt, der die spezifischen Berechtigungen und Berechtigungen bereitstellt, die für den Dienst erforderlich sind (ähnlich dem lokalen Systemkontext, jedoch mit eingeschränkten Berechtigungen). Andere Konten werden jedoch wie in dieser Anleitung beschrieben benötigt.

### Erstellen von Konten für die Failover-Clusterunterstützung mithilfe von Assistenten

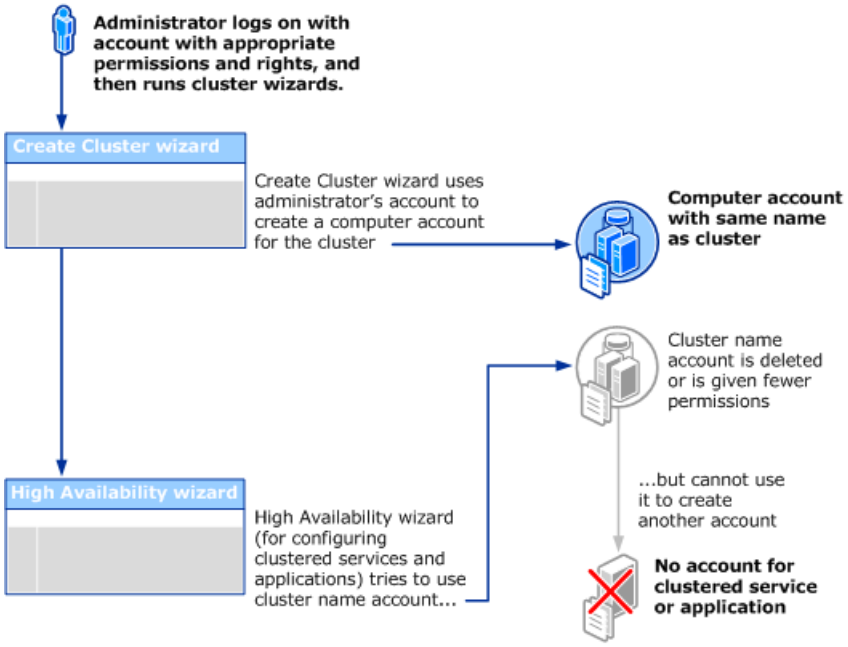
Im folgenden Diagramm werden die Verwendung und die Erstellung von Computerkonten (Active Directory-Objekte) veranschaulicht, die im vorherigen Unterabschnitt beschrieben werden. Diese Konten sind von Bedeutung, wenn ein Administrator den Clustererstellungs-Assistenten ausführt und anschließend den Assistenten für hohe Verfügbarkeit ausführt (um einen geclusterten Dienst oder eine geclusterte Anwendung zu konfigurieren).




Beachten Sie, dass im oben dargestellten Diagramm ein einzelner Administrator sowohl den Clustererstellungs-Assistenten als auch den Assistenten für hohe Verfügbarkeit ausführt. Dies können jedoch auch zwei verschiedene Administratoren sein, die zwei verschiedene Benutzerkonten verwenden, sofern beide Konten über ausreichende Berechtigungen verfügen. Die Berechtigungen werden weiter unten in dieser Anleitung unter Anforderungen für Failovercluster, Active Directory-Domänen und Konten ausführlicher beschrieben.

### Probleme, die sich durch Änderungen an den vom Cluster benötigten Konten ergeben können

Im folgenden Diagramm wird veranschaulicht, wie sich Probleme ergeben können, wenn das Clusternamenkonto (eines der für den Cluster erforderlichen Konten) geändert wird, nachdem es automatisch vom Clustererstellungs-Assistenten erstellt wurde.




Wenn die im Diagramm gezeigte Art von Problem auftritt, wird ein bestimmtes Ereignis (1193, 1194, 1206 oder 1207) in der Ereignisanzeige protokolliert. Weitere Informationen zu diesen Ereignissen finden Sie unter https://go.microsoft.com/fwlink/?LinkId=118271.

Beachten Sie, dass ein ähnliches Problem mit dem Erstellen eines Kontos für einen geclusterten Dienst oder eine geclusterte Anwendung auftreten kann, wenn das domänenweite Kontingent für das Erstellen von Computerobjekten (standardmäßig 10) erreicht wurde. Wenn dies der Fall ist, könnte es sinnvoll sein, sich an den Domänenadministrator zu wenden, damit dieser das Kontingent erhöht, obwohl dies eine domänenweite Einstellung ist und nur nach gründlicher Überlegung geändert werden sollte. Außerdem sollten Sie sich erst vergewissern, dass im vorstehenden Diagramm nicht Ihre Situation beschrieben wird. Weitere Informationen finden Sie weiter unten in dieser Anleitung unter Schritte zum Beheben von Problemen, die durch Änderungen an clusterbezogenen Active Directory-Konten verursacht wurden.

## Anforderungen für Failovercluster, Active Directory-Domänen und Konten

Wie in den vorausgehenden drei Abschnitten beschrieben, müssen bestimmte Anforderungen erfüllt sein, bevor geclusterte Dienste und Anwendungen auf einem Failovercluster erfolgreich konfiguriert werden können. Die grundlegendsten Anforderungen betreffen den Speicherort von Clusterknoten (innerhalb einer einzigen Domäne) und die Berechtigungsstufe des Kontos für die Person, die den Cluster installiert. Wenn diese Anforderungen erfüllt sind, können die anderen vom Cluster benötigten Konten von den Failovercluster-Assistenten automatisch erstellt werden. In der folgenden Liste werden Details zu diesen grundlegenden Anforderungen aufgeführt.

- **Knoten:** Alle Knoten müssen sich in der gleichen Active Directory Domäne befinden. (Die Domäne kann nicht auf Windows NT 4.0 basieren, das kein Active Directory einschließt.)
- **Konto der Person, die den Cluster installiert:** Die Person, die den Cluster installiert, muss ein Konto mit den folgenden Eigenschaften verwenden:
  - Das Konto muss ein Domänenkonto sein. Es muss kein Domänenadministratorkonto sein. Es kann ein Domänenbenutzerkonto sein, wenn es die anderen Anforderungen in dieser Liste erfüllt.
  - Das Konto muss über Administratorberechtigungen für die Server verfügen, die Clusterknoten werden sollen. Die einfachste Möglichkeit, diese Bedingung zu erfüllen, besteht darin, ein Domänenbenutzerkonto zu erstellen und dieses Konto anschließend der lokalen Gruppe Administratoren auf jedem Server hinzuzufügen, der ein Clusterknoten werden soll. Weitere Informationen finden Sie weiter unten in dieser Anleitung unter Schritte zum Konfigurieren des

Kontos für die Person, die den Cluster installiert.

- Dem Konto (oder der Gruppe, deren Mitglied das Konto ist) müssen die Berechtigungen zum Erstellen von Computerobjektenund zum Lesen aller Eigenschaftenin dem Container erteilt werden, der in der Domäne für Computerkonten verwendet wird. Weitere Informationen finden Sie weiter unten in dieser Anleitung unter Schritte zum Konfigurieren des Kontos für die Person, die den Cluster installiert.

- Wenn Ihre Organisation die vorab Bereitstellung des Cluster Namen Kontos (einem Computer Konto mit dem gleichen Namen wie der Cluster) auswählt, muss das Konto des vorab bereitgestellten Cluster namens dem Konto der Person, die den Cluster installiert, die Berechtigung "Vollzugriff" erteilen. Weitere wichtige Details zur Vorabbereitstellung des Clusternamenkontos finden Sie weiter unten in dieser Anleitung unter Schritte für die Vorabbereitstellung des Clusternamenkontos.

**Vorausplanung für Kennwortzurücksetzungen und andere Kontowartungsmaßnahmen**

Die Administratoren von Failoverclustern müssen möglicherweise manchmal das Kennwort des Clusternamenkontos zurücksetzen. Für diese Aktion ist eine spezielle Berechtigung erforderlich, die Berechtigung **Kennwort zurücksetzen**. Daher hat es sich bewährt, die Berechtigungen des Clusternamenkontos zu bearbeiten (mithilfe des Snap-Ins "Active Directory-Benutzer und -Computer"), um den Administratoren des Clusters die Berechtigung **Kennwort zurücksetzen** für das Clusternamenkonto zu erteilen. Weitere Informationen finden Sie weiter unten in dieser Anleitung unter Schritte zum Beheben von Kennwortproblemen mit dem Clusternamenkonto.

# Schritte zum Konfigurieren des Kontos für die Person, die den Cluster installiert

Das Konto der Person, die den Cluster installiert, ist wichtig, da es die Grundlage bereitstellt, auf der ein Computerkonto für den Cluster erstellt wird.

Die zum Ausführen des folgenden Verfahrens minimal erforderliche Gruppenmitgliedschaft ist davon abhängig, ob Sie das Domänenkonto erstellen und ihm die erforderlichen Berechtigungen in der Domäne zuweisen oder ob Sie das (von jemand anderem erstellte) Konto lediglich der lokalen Gruppe **Administratoren** auf den Servern hinzufügen, die Knoten im Failovercluster werden sollen. Wenn die erste, die Mitgliedschaft in **Konto Operatoren** oder einer entsprechenden Gruppe, mindestens erforderlich ist, um dieses Verfahren abzuschließen. Im zweiten Fall ist lediglich die Mitgliedschaft in der lokalen Gruppe **Administratoren** auf den Servern, die Knoten im Failovercluster werden sollen, oder eine gleichwertige Mitgliedschaft erforderlich. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter https://go.microsoft.com/fwlink/?LinkId=83477.

**So konfigurieren Sie das Konto für die Person, die den Cluster installiert**

1. Erstellen Sie ein Domänenkonto für die Person, die den Cluster installiert, oder rufen Sie es ab. Bei diesem Konto kann es sich um ein Domänen Benutzerkonto oder um ein **Konto Operator** Konto handeln. Wenn Sie ein Standardbenutzer Konto verwenden, müssen Sie diesem später in diesem Verfahren einige zusätzliche Berechtigungen einräumen.

2. Wenn das in Schritt 1 erstellte oder abgerufene Konto nicht automatisch in der lokalen Gruppe **Administratoren** auf den Computern in der Domäne enthalten ist, fügen Sie das Konto der lokalen Gruppe **Administratoren** auf den Servern hinzu, die als Knoten im Failovercluster verwendet werden sollen:

   a. Klicken Sie auf **Start**, klicken Sie auf **Verwaltung**, und klicken Sie dann auf **Server-Manager**.

   b. Erweitern Sie in der Konsolenstruktur nacheinander **Konfiguration**, **Lokale Benutzer und Gruppen** und **Gruppen**.

   c. Klicken Sie im mittleren Bereich mit der rechten Maustaste auf **Administratoren**, klicken Sie auf **Zur Gruppe hinzufügen** und dann auf **Hinzufügen**.

d. Geben **Sie unter Geben Sie die zu**erstellenden Objektnamen ein den Namen des Benutzerkontos ein, das in Schritt 1 erstellt oder abgerufen wurde. Wenn Sie dazu aufgefordert werden, geben Sie einen Kontonamen und ein Kennwort mit ausreichenden Berechtigungen für diese Aktion ein. Klicken Sie dann auf **OK**.

e. Wiederholen Sie diese Schritte für jeden Server, der ein Knoten im Failovercluster werden soll.

> **IMPORTANT**
>
> Diese Schritte müssen für alle Server wiederholt werden, die Knoten im Cluster werden sollen.

3. Wenn das in Schritt 1 erstellte oder abgerufene Konto ein Domänenadministratorkonto ist, überspringen Sie den Rest dieses Verfahrens. Erteilen Sie andernfalls dem Konto die Berechtigungen zum Erstellen von Computerobjektenund zum Lesen aller Eigenschaftenin dem Container, der in der Domäne für Computerkonten verwendet wird:

   a. Klicken Sie auf einem Domänencontroller auf **Start**, auf **Verwaltung** und dann auf **Active Directory-Benutzer und -Computer**. Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf **Weiter**.

   b. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Funktionen** ausgewählt ist.

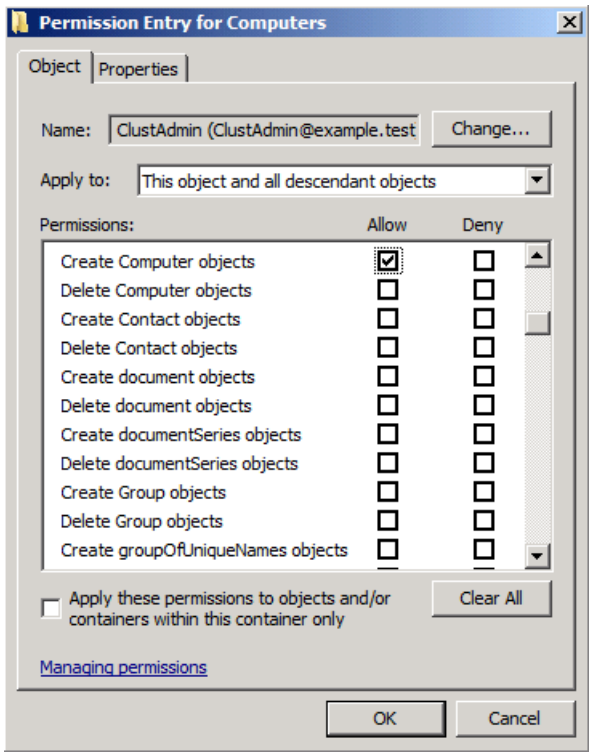
      Wenn **Erweiterte Funktionen** ausgewählt ist, wird die Registerkarte **Sicherheit** in den Eigenschaften der Konten (Objekte) in **Active Directory-Benutzer und -Computer** angezeigt.

   c. Klicken Sie mit der rechten Maustaste auf den Standardcontainer **Computer** oder den Standardcontainer, in dem Computerkonten in der Domäne erstellt werden, und klicken Sie dann auf **Eigenschaften**. **Computer** befinden sich unter **Active Directory Benutzer und Computer/** *Domäne-Knoten*/**Computers**.

   d. Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweitert**.

   e. Klicken Sie auf **Hinzufügen**, geben Sie den Namen des in Schritt 1 erstellten oder abgerufenen Kontos ein, und klicken Sie dann auf **OK**.

   f. Suchen Sie im Dialogfeld **Berechtigungs Eintrag für * * * Container* die Berechtigungen zum **Erstellen von Computer Objekten** und zum **Lesen aller Eigenschaften** , und stellen Sie sicher, dass das Kontrollkästchen **zulassen** für jeden Container aktiviert ist.




## Schritte für die Vorabbereitstellung des Clusternamenkontos

Es ist normalerweise einfacher, wenn Sie das Clusternamenkonto nicht vorab bereitstellen, sondern das Konto beim Ausführen des Clustererstellungs-Assistenten automatisch erstellen und konfigurieren lassen. Wenn es jedoch aufgrund der Anforderungen in Ihrer Organisation notwendig ist, das Clusternamenkonto vorab bereitzustellen, verwenden Sie das folgende Verfahren.

Sie müssen mindestens Mitglied der Gruppe **Domänen-Admins** oder einer entsprechenden Gruppe sein, um dieses Verfahren ausführen zu können. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter https://go.microsoft.com/fwlink/?LinkId=83477. Beachten Sie, dass Sie das gleiche Konto wie beim Erstellen des Clusters für dieses Verfahren verwenden können.

**So stellen Sie ein Clusternamenkonto vorab bereit**

1. Stellen Sie sicher, dass Sie den Namen, den der Cluster erhalten wird, und den Namen des Benutzerkontos, das von der Person verwendet wird, die den Cluster erstellt, kennen. (Beachten Sie, dass Sie dieses Konto verwenden können, um dieses Verfahren auszuführen.)

2. Klicken Sie auf einem Domänencontroller auf **Start**, auf **Verwaltung** und dann auf **Active Directory-Benutzer und -Computer**. Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf **Weiter**.

3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Computer** oder den Standardcontainer, in dem Computerkonten in der Domäne erstellt werden. **Computer** befinden sich unter **Active Directory Benutzer und Computer/***Domäne-Knoten***/Computers**.

4. Klicken Sie auf **Neu** und anschließend auf **Computer**.

5. Geben Sie den Namen, der für den Failovercluster verwendet wird, oder anders gesagt, den Clusternamen, der im Clustererstellungs-Assistenten angegeben wird, ein. Klicken Sie dann auf **OK**.

6. Klicken Sie mit der rechten Maustaste auf das Konto, das Sie gerade erstellt haben, und klicken Sie dann auf **Konto deaktivieren**. Wenn Sie zur Bestätigung Ihrer Auswahl aufgefordert werden, klicken Sie auf **Ja**.

   Das Konto muss deaktiviert werden, damit beim Ausführen des Clustererstellungs-Assistenten sichergestellt ist, dass das für den Cluster verwendete Konto nicht gerade von einem vorhandenen Computer oder Cluster in der Domäne verwendet wird.

7. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Funktionen** ausgewählt ist.

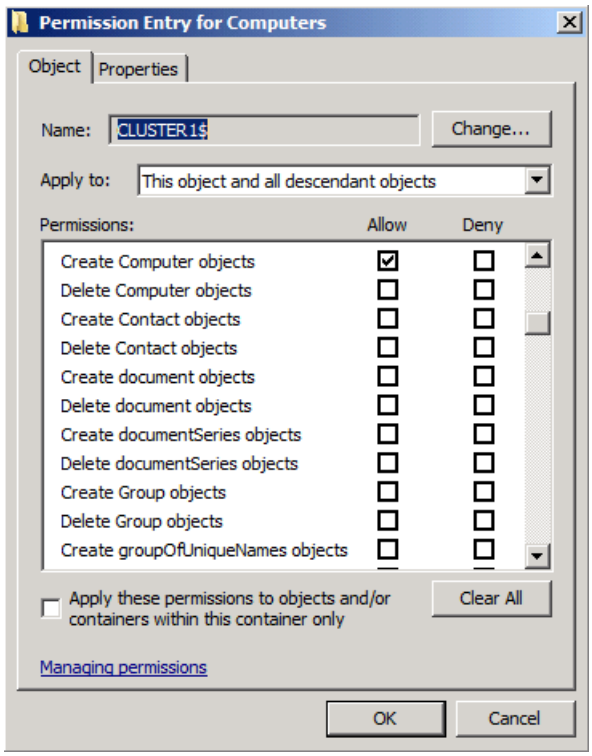
   Wenn **Erweiterte Funktionen** ausgewählt ist, wird die Registerkarte **Sicherheit** in den Eigenschaften der Konten (Objekte) in **Active Directory-Benutzer und -Computer** angezeigt.

8. Klicken Sie mit der rechten Maustaste auf den Ordner, auf den Sie in Schritt 3 geklickt haben, und klicken Sie dann auf **Eigenschaften**.

9. Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweitert**.

10. Klicken Sie auf **Hinzufügen** und dann auf **Objekttypen**, und stellen Sie sicher, dass **Computer** ausgewählt ist. Klicken Sie anschließend auf **OK**. Geben Sie anschließend unter **Geben Sie die zu verwendenden Objektnamen ein** den Namen des gerade erstellten Computerkontos ein, und klicken Sie dann auf **OK**. Wenn eine Nachricht angezeigt wird, die besagt, dass Sie im Begriff sind, ein deaktiviertes Objekt hinzuzufügen, klicken Sie auf **OK**.

11. Suchen Sie im Dialogfeld **Berechtigungs Eintrag** die Berechtigungen zum **Erstellen von Computer Objekten** und zum **Lesen aller Eigenschaften** , und stellen Sie sicher, dass das Kontrollkästchen **zulassen** für jede dieser Berechtigungen aktiviert ist.




12. Klicken Sie auf **OK**, bis Sie zum Snap-In **Active Directory-Benutzer und -Computer** zurückgekehrt sind.

13. Wenn Sie für dieses Verfahren dasselbe Konto verwenden, das zum Erstellen des Clusters verwendet werden soll, überspringen Sie die verbleibenden Schritte. Andernfalls müssen Sie Berechtigungen konfigurieren, damit das Benutzerkonto, das zum Erstellen des Clusters verwendet wird, über Vollzugriff auf das gerade erstellte Computerkonto verfügt:

    a. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Funktionen** ausgewählt ist.

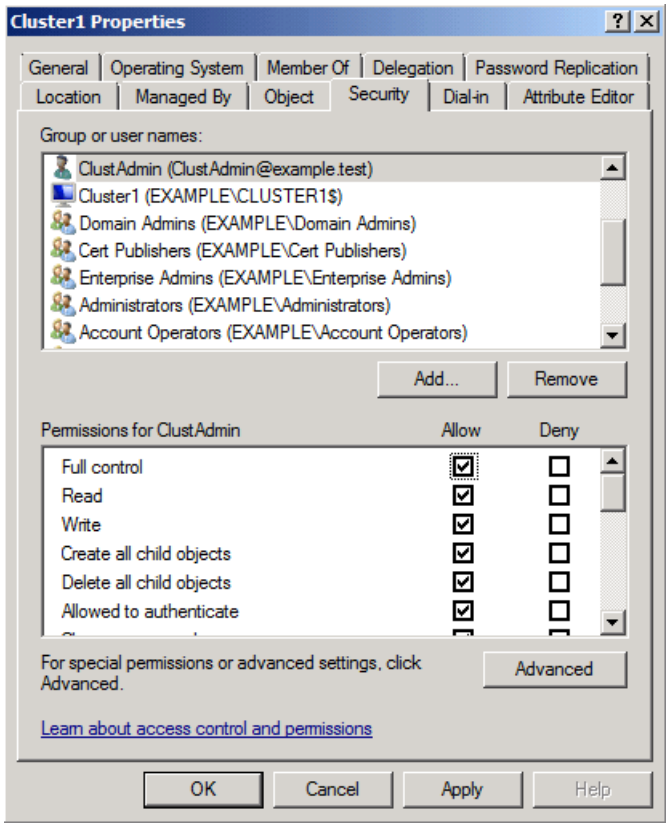
    b. Klicken Sie mit der rechten Maustaste auf das gerade erstellte Konto, und klicken Sie dann auf **Eigenschaften**.

    c. Klicken Sie auf der Registerkarte **Sicherheit** auf **Hinzufügen**. Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf **Weiter**.

    d. Geben Sie im Dialogfeld **Benutzer, Computer oder Gruppen auswählen** das Benutzerkonto an,

das zum Erstellen des Clusters verwendet werden soll. Klicken Sie dann auf **OK**.

e. Stellen Sie sicher, dass das gerade hinzugefügte Benutzerkonto ausgewählt ist, und aktivieren Sie dann neben **Vollzugriff** das Kontrollkästchen **Zulassen**.




## Schritte für die Vorabbereitstellung eines Kontos für einen geclusterten Dienst oder eine geclusterte Anwendung

Es ist normalerweise einfacher, wenn Sie das Computerkonto für einen geclusterten Dienst oder eine geclusterte Anwendung nicht vorab bereitstellen, sondern das Konto beim Ausführen des Assistenten für hohe Verfügbarkeit automatisch erstellen und konfigurieren lassen. Wenn es jedoch aufgrund der Anforderungen in Ihrer Organisation notwendig ist, Konten vorab bereitzustellen, verwenden Sie das folgende Verfahren.

Sie müssen mindestens Mitglied der Gruppe **Konten-Operatoren** oder einer entsprechenden Gruppe sein, um dieses Verfahren ausführen zu können. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter https://go.microsoft.com/fwlink/?LinkId=83477.

**So stellen Sie ein Konto für einen geclusterten Dienst oder eine geclusterte Anwendung vorab bereit**

1. Stellen Sie sicher, dass Sie den Namen des Clusters und den Namen, den der geclusterte Dienst oder die geclusterte Anwendung erhalten wird, kennen.

2. Klicken Sie auf einem Domänencontroller auf **Start**, auf **Verwaltung** und dann auf **Active Directory-Benutzer und -Computer**. Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf **Weiter**.

3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Computer** oder den Standardcontainer, in dem Computerkonten in der Domäne erstellt werden. **Computer** befinden sich unter **Active Directory Benutzer und Computer/***Domäne-Knoten***/Computers**.

4. Klicken Sie auf **Neu** und anschließend auf **Computer**.

5. Geben Sie den Namen ein, den Sie für den geclusterten Dienst oder die geclusterte Anwendung verwenden werden, und klicken Sie dann auf **OK**.

6. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Funktionen** ausgewählt ist.

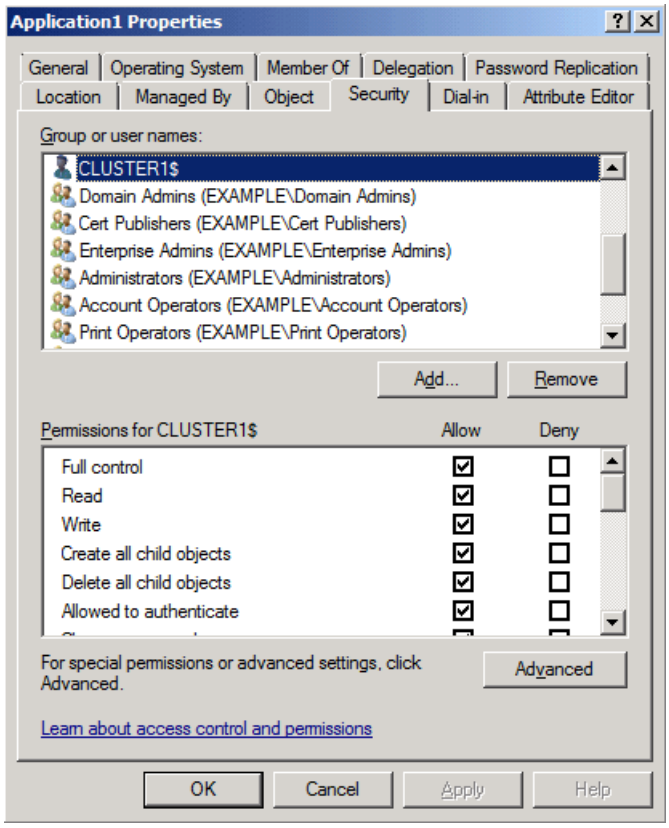
   Wenn **Erweiterte Funktionen** ausgewählt ist, wird die Registerkarte **Sicherheit** in den Eigenschaften der Konten (Objekte) in **Active Directory-Benutzer und -Computer** angezeigt.

7. Klicken Sie mit der rechten Maustaste auf das gerade erstellte Konto, und klicken Sie dann auf **Eigenschaften**.

8. Klicken Sie auf der Registerkarte **Sicherheit** auf **Hinzufügen**.

9. Klicken Sie auf **Objekttypen**, und stellen Sie sicher, dass **Computer** ausgewählt ist. Klicken Sie anschließend auf **OK**. Geben Sie dann unter **Geben Sie die zu verwendenden Objektnamen ein** das Clusternamenkonto ein, und klicken Sie anschließend auf **OK**. Wenn eine Nachricht angezeigt wird, die besagt, dass Sie im Begriff sind, ein deaktiviertes Objekt hinzuzufügen, klicken Sie auf **OK**.

10. Stellen Sie sicher, dass das Clusternamenkonto ausgewählt ist, und aktivieren Sie dann neben **Vollzugriff** das Kontrollkästchen **Zulassen**.




## Schritte zum Beheben von Problemen mit vom Cluster verwendeten Konten

Wenn Sie einen Failovercluster erstellen und geclusterte Dienste oder Anwendungen konfigurieren, erstellen die Failovercluster-Assistenten, wie weiter oben in dieser Anleitung beschrieben, die erforderlichen Active Directory-Konten und erteilen ihnen die passenden Berechtigungen. Wenn ein benötigtes Konto gelöscht wird oder notwendige Berechtigungen geändert werden, können sich Probleme ergeben. Die folgenden Unterabschnitte enthalten Schritte zum Beheben dieser Probleme.

- Schritte zur Problembehandlung von Kenn Wort Problemen mit dem Cluster Namen Konto
- Schritte zur Behebung von Problemen, die durch Änderungen an Cluster bezogenen Active Directory Konten verursacht wurden

### Schritte zum Beheben von Kennwortproblemen mit dem Clusternamenkonto

Verwenden Sie dieses Verfahren, wenn eine Ereignismeldung zu Computerobjekten oder der Clusteridentität

angezeigt wird, die den folgenden Text enthält. Beachten Sie, dass dieser Text in der Ereignismeldung steht, nicht am Anfang der Ereignismeldung:

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

Ereignismeldungen, die der vorstehenden Beschreibung entsprechen, geben an, dass das Kennwort für das Clusternamenkonto und das entsprechende von der Clustersoftware gespeicherte Kennwort nicht mehr übereinstimmen.

Informationen zum Sicherstellen, dass Clusteradministratoren die erforderlichen Berechtigungen haben, das folgende Verfahren ordnungsgemäß auszuführen, finden Sie weiter oben in dieser Anleitung unter Vorausplanung für Kennwortzurücksetzungen und andere Kontowartungsmaßnahmen.

Zum Ausführen dieses Verfahrens ist mindestens die Mitgliedschaft in der lokalen Gruppe **Administratoren** oder eine gleichwertige Berechtigung erforderlich. Außerdem muss Ihr Konto über die Berechtigung **Kennwort zurücksetzen** für das Clusternamenkonto verfügen (es sei denn, das Konto ist ein **Domänen-Admins**-Konto oder Ersteller-Besitzer des Clusternamenkontos). Das Konto, das von der Person verwendet wurde, die den Cluster installiert hat, kann für dieses Verfahren verwendet werden. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter https://go.microsoft.com/fwlink/?LinkId=83477.

#### So beheben Sie Kennwortprobleme mit dem Clusternamenkonto

1. Klicken Sie zum Öffnen des Failovercluster-Snap-Ins auf **Start**, auf **Verwaltung** und dann auf **Failover-Clusterverwaltung**. (Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf **weiter**.)

2. Wenn im Snap-In Failover-Clusterverwaltung der zu konfigurierende Cluster nicht angezeigt wird, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Failover-Clusterverwaltung**, klicken Sie auf **Cluster verwalten**, und wählen Sie den gewünschten Cluster aus, oder geben Sie diesen an.

3. Erweitern Sie im mittleren Bereich **Hauptressourcen des Clusters**.

4. Klicken Sie unter **Clustername** mit der rechten Maustaste auf das Element **Name**, zeigen Sie auf **Weitere Aktionen**, und klicken Sie dann auf **Active Directory-Objekt reparieren**.

### Schritte zum Beheben von Problemen, die durch Änderungen an clusterbezogenen Active Directory-Konten verursacht wurden

Wenn das Clusternamenkonto gelöscht wird oder dem Konto Berechtigungen entzogen werden, treten Probleme auf, wenn Sie einen neuen geclusterten Dienst oder eine neue geclusterte Anwendung konfigurieren. Sie können ein Problem, das möglicherweise auf diese Ursache zurückzuführen ist, beheben, indem Sie mithilfe des Snap-Ins "Active Directory-Benutzer und -Computer" das Clusternamenkonto und andere zugehörige Konten anzeigen bzw. ändern. Informationen zu den Ereignissen, die protokolliert werden, wenn diese Art von Problem auftritt (Ereignis 1193, 1194, 1206 oder 1207), finden Sie unter https://go.microsoft.com/fwlink/?LinkId=118271.

Sie müssen mindestens Mitglied der Gruppe **Domänen-Admins** oder einer entsprechenden Gruppe sein, um dieses Verfahren ausführen zu können. Ausführliche Informationen zur Verwendung der entsprechenden Konten und Gruppenmitgliedschaften finden Sie unter https://go.microsoft.com/fwlink/?LinkId=83477.

#### So beheben Sie Probleme, die durch Änderungen an clusterbezogenen Active Directory-Konten verursacht wurden

1. Klicken Sie auf einem Domänencontroller auf **Start**, auf **Verwaltung** und dann auf **Active Directory-Benutzer und -Computer**. Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die gewünschte Aktion angezeigt wird, und klicken Sie dann auf **Weiter**.

2. Erweitern Sie den Standardcontainer **Computer** bzw. den Ordner, in dem sich das Clusternamenkonto (das Computerkonto für den Cluster) befindet. **Computer** befinden sich unter **Active Directory Benutzer und Computer/***Domäne-Knoten***/Computers**.

3. Beachten Sie das Symbol für das Clusternamenkonto. Es darf keinen abwärts zeigenden Pfeil aufweisen, das

heißt, das Konto darf nicht deaktiviert sein. Wenn es als deaktiviert angezeigt wird, klicken Sie mit der rechten Maustaste darauf, und suchen Sie nach dem Befehl **Konto aktivieren**. Wenn Sie den Befehl sehen, klicken Sie darauf.

4. Stellen Sie sicher, dass im Menü **Ansicht** die Option **Erweiterte Funktionen** ausgewählt ist.

   Wenn **Erweiterte Funktionen** ausgewählt ist, wird die Registerkarte **Sicherheit** in den Eigenschaften der Konten (Objekte) in **Active Directory-Benutzer und -Computer** angezeigt.

5. Klicken Sie mit der rechten Maustaste auf den Standardcontainer **Computer** bzw. den Ordner, in dem sich das Clusternamenkonto befindet.

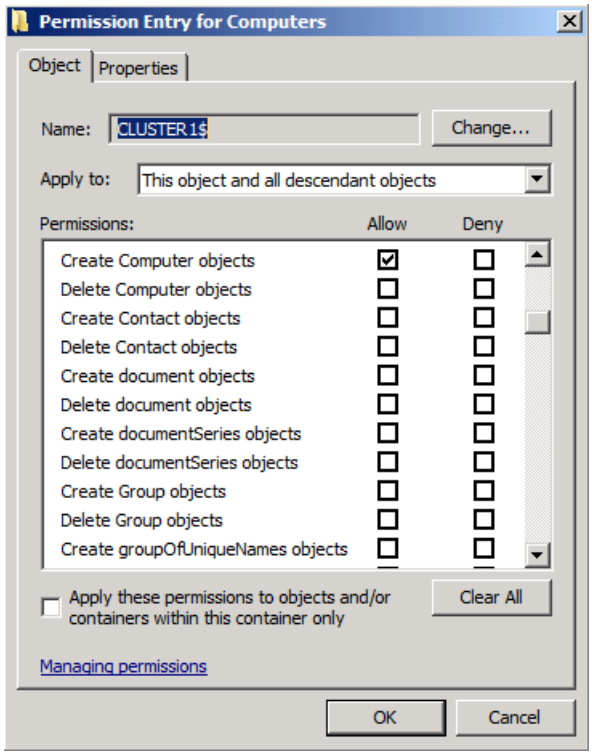
6. Klicken Sie auf **Eigenschaften**.

7. Klicken Sie auf der Registerkarte **Sicherheit** auf **Erweitert**.

8. Klicken Sie in der Liste der Konten mit Berechtigungen auf das Clusternamenkonto und dann auf **Bearbeiten**.

> **NOTE**
>
> Wenn das Clusternamenkonto nicht aufgeführt ist, klicken Sie auf **Hinzufügen**, und fügen Sie es der Liste hinzu.

9. Vergewissern Sie sich, dass für das Cluster Namen Konto (auch als Cluster Namen Objekt oder CNO bezeichnet) die Option **zulassen** für die Berechtigungen zum **Erstellen von Computer Objekten** und zum **Lesen aller Eigenschaften** ausgewählt ist.



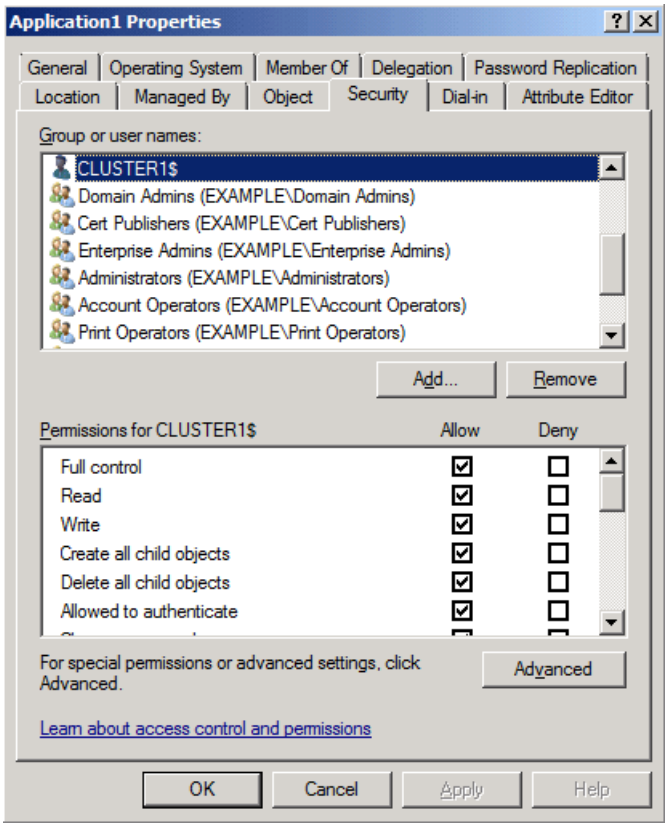

10. Klicken Sie auf **OK**, bis Sie zum Snap-In **Active Directory-Benutzer und -Computer** zurückgekehrt sind.

11. Überprüfen Sie die Domänenrichtlinien, die sich auf die Erstellung von Computerkonten (Objekten) beziehen (gegebenenfalls, indem Sie sich an einen Domänenadministrator wenden). Stellen Sie sicher, dass das Clusternamenkonto ein Computerkonto erstellen kann, immer wenn Sie einen geclusterten Dienst oder eine geclusterte Anwendung konfigurieren. Wenn der Domänenadministrator beispielsweise Einstellungen konfiguriert hat, die dazu führen, dass alle neuen Computerkonten in einem spezialisierten Container statt im Standardcontainer **Computer** erstellt werden, müssen Sie sicherstellen, dass diese Einstellungen es dem Clusternamenkonto ermöglichen, ebenfalls neue Computerkonten in diesem Container zu erstellen.

12. Erweitern Sie den Standardcontainer **Computer** oder den Container, in dem sich das Computerkonto für einen geclusterten Dienst oder eine geclusterte Anwendung befindet.

13. Klicken Sie mit der rechten Maustaste auf das Computerkonto für einen geclusterten Dienst oder eine geclusterte Anwendung, und klicken Sie dann auf **Eigenschaften**.

14. Vergewissern Sie sich, dass auf der Registerkarte **Sicherheit** das Clusternamenkonto unter den Konten aufgeführt wird, die über Berechtigungen verfügen, und wählen Sie es aus. Vergewissern Sie sich, dass das Clusternamenkonto über die Berechtigung **Vollzugriff** verfügt (das Kontrollkästchen **Zulassen** ist aktiviert). Wenn dies nicht der Fall ist, fügen Sie der Liste das Clusternamenkonto hinzu, und erteilen Sie dem Konto die Berechtigung **Vollzugriff**.




15. Wiederholen Sie die Schritte 13 und 14 für jeden geclusterten Dienst und jede geclusterte Anwendung, die im Cluster konfiguriert sind.

16. Überprüfen Sie, ob das domänenweite Kontingent für das Erstellen von Computerobjekten (standardmäßig 10) erreicht wurde (gegebenenfalls, indem Sie sich an einen Domänenadministrator wenden). Wenn alle vorstehenden Elemente in diesem Verfahren überprüft und korrigiert wurden und das Kontingent ausgeschöpft wurde, erwägen Sie, das Kontingent zu vergrößern. So ändern Sie das Kontingent

17. Öffnen Sie eine Eingabeaufforderung als Administrator, und führen Sie **ADSIEdit.msc** aus.

18. Klicken Sie mit der rechten Maustaste auf **ADSI-Editor**, klicken Sie auf **Verbinden mit** und dann auf **OK**. Der Knoten **Standardmäßiger Namenskontext** wird der Konsolenstruktur hinzugefügt.

19. Doppelklicken Sie auf **Standardmäßiger Namenskontext**, klicken Sie mit der rechten Maustaste auf das Domänenobjekt darunter, und klicken Sie dann auf **Eigenschaften**.

20. Führen Sie einen Bildlauf zu **ms-DS-MachineAccountQuota** durch und wählen Sie das Element aus. Klicken Sie auf **Bearbeiten**, ändern Sie den Wert, und klicken Sie dann auf **OK**.

# Konfigurieren und Verwalten des Quorums

02.05.2020 • 39 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Dieses Thema enthält Hintergrundinformationen und Schritte zum Konfigurieren und Verwalten des Quorums in einem Windows Server-Failovercluster.

## Grundlegendes zum Quorum

Das Quorum für einen Cluster wird über die Anzahl der Knoten mit Stimmen bestimmt, die Teil der aktiven Clustermitgliedschaft für diesen Cluster sein müssen, um ordnungsgemäß gestartet oder weiterhin ausgeführt werden zu können. Eine ausführlichere Erläuterung finden Sie im Dokument zum Grundlagen des Cluster-und Pool Quorums.

## Optionen für die Quorum Konfiguration

Das Quorum Modell in Windows Server ist flexibel. Wenn Sie die Quorum Konfiguration für Ihren Cluster ändern müssen, können Sie den Assistenten zum Konfigurieren des Cluster Quorums oder die Windows PowerShell-Cmdlets für Failovercluster verwenden. Schritte und Überlegungen zur Quorumkonfiguration finden Sie weiter unten in diesem Thema unter Konfigurieren des Clusterquorums.

In der folgenden Tabelle werden die drei Quorumkonfigurationsoptionen aufgelistet, die im Assistenten zum Konfigurieren des Clusterquorums verfügbar sind.

| OPTION | BESCHREIBUNG |
| --- | --- |
| „Typische Einstellungen verwenden“, und | Der Cluster weist automatisch jedem Knoten eine Stimme zu und verwaltet die Knotenstimmen dynamisch. Sofern es für Ihren Cluster angemessen ist und freigegebener Clusterspeicher zur Verfügung steht, wählt der Cluster einen Datenträgerzeugen aus. Diese Option wird für die meisten Situationen empfohlen, da die Clustersoftware automatisch eine Quorum- und Zeugenkonfiguration auswählt, die die höchste Verfügbarkeit für den Cluster bietet. |
| „Quorumzeugen hinzufügen oder ändern“ | Sie können eine Zeugenressource hinzufügen, ändern oder entfernen. Sie können einen Dateifreigabe- oder Datenträgerzeugen konfigurieren. Der Cluster weist automatisch jedem Knoten eine Stimme zu und verwaltet die Knotenstimmen dynamisch. |
| „Erweiterte Quorumkonfiguration und Zeugenauswahl“ | Wählen Sie diese Option nur aus, wenn für die Konfiguration des Quorums anwendungs- und standortspezifische Anforderungen gelten. Sie können den Quorumzeugen ändern, Knotenstimmen hinzufügen oder entfernen und auswählen, ob der Cluster die Knotenstimmen dynamisch verwalten soll. Standardmäßig werden zu allen Knoten Stimmen zugewiesen, und die Knotenstimmen werden dynamisch verwaltet. |

In Abhängigkeit von der gewählten Quorumkonfigurationsoption und Ihren spezifischen Einstellungen wird der Cluster in einem der folgenden Quorummodi konfiguriert:

| MODE | BESCHREIBUNG |
| --- | --- |
| Knotenmehrheit (kein Zeuge) | Nur Knoten haben Stimmen. Es wird kein Quorumzeuge konfiguriert. Das Clusterquorum entspricht der Mehrheit der abstimmenden Knoten in der aktiven Clustermitgliedschaft. |
| Keine Mehrheit mit Zeuge (Datenträger oder Dateifreigabe) | Knoten haben Stimmen. Zusätzlich hat ein Quorumzeuge eine Stimme. Das Clusterquorum entspricht der Mehrheit der abstimmenden Knoten in der aktiven Clustermitgliedschaft plus einer Zeugenstimme. Ein Quorumzeuge kann ein festgelegter Datenträgerzeuge oder ein Dateifreigabezeuge sein. |
| Keine Mehrheit (nur Datenträgerzeuge) | Knoten haben keine Stimmen. Nur ein Datenträgerzeuge hat eine Stimme.<br>Das Clusterquorum wird über den Status des Datenträgerzeugen bestimmt. Im Allgemeinen wird dieser Modus nicht empfohlen und er sollte nicht ausgewählt werden, da er für den Cluster einen einzelnen Fehlerpunkt erzeugt. |

In den folgenden Unterabschnitten erhalten Sie weitere Informationen zu erweiterten Quorum Konfigurationseinstellungen.

**„Zeugenkonfiguration"**

Im Allgemeinen sollten die abstimmenden Elemente im Cluster beim Konfigurieren eines Quorums eine ungerade Anzahl ergeben. Wenn der Cluster daher eine gerade Anzahl von abstimmenden Knoten enthält, sollten Sie einen Datenträgerzeugen oder einen Dateifreigabezeugen konfigurieren. Der Cluster ist in der Lage, einen zusätzlichen Knoten inaktiv zu halten. Zudem kann der Cluster durch das Hinzufügen einer Zeugenstimme die Ausführung fortsetzen, wenn die Hälfte der Clusterknoten gleichzeitig ausfällt oder deren Verbindung unterbrochen bzw. getrennt wird.

Ein Datenträgerzeuge wird in der Regel empfohlen, wenn der Datenträger für alle Knoten angezeigt wird. Ein Dateifreigabezeuge wird empfohlen, wenn Sie die Notfallwiederherstellung mit repliziertem Speicher für mehrere Standorte berücksichtigen müssen. Das Konfigurieren eines Datenträgerzeugen mit repliziertem Speicher ist nur möglich, wenn der Speicheranbieter den Lese-/Schreibzugriff auf den replizierten Speicher von allen Standorten aus unterstützt. ***Ein Datenträger Zeuge wird von direkte Speicherplätze nicht unterstützt***.

Die folgende Tabelle enthält zusätzliche Informationen und Überlegungen zu den Quorumzeugentypen.

| ZEUGENTYP | BESCHREIBUNG | ANFORDERUNGEN UND EMPFEHLUNGEN |
| --- | --- | --- |

| ZEUGENTYP | BESCHREIBUNG | ANFORDERUNGEN UND EMPFEHLUNGEN |
| --- | --- | --- |
| Datenträgerzeuge | • Dedizierte LUN, die eine Kopie der Clusterdatenbank speichert<br>• Besonders für Cluster mit freigegebenem (nicht repliziertem) Speicher geeignet | • Die Größe der LUN muss mindestens 512 MB betragen<br>• Muss für die Clusterverwendung dediziert sein und darf keiner Clusterrolle zugewiesen werden<br>• Muss in den Clusterspeicher einbezogen werden und die Speichervalidierungstests bestehen<br>• Darf kein Datenträger sein, der ein freigegebenes Clustervolume (CSV) ist<br>• Einfacher Datenträger mit einzelnem Volume<br>• Laufwerksbuchstabe ist nicht erforderlich<br>• Formatierung mit NTFS oder ReFS zulässig<br>• Kann für die Fehlertoleranz optional mit Hardware-RAID konfiguriert werden<br>• Sollte von Sicherungen und Antivirenscans ausgeschlossen werden<br>• Ein Datenträger Zeuge wird mit direkte Speicherplätze nicht unterstützt. |

| ZEUGENTYP | BESCHREIBUNG | ANFORDERUNGEN UND EMPFEHLUNGEN |
| --- | --- | --- |
| Dateifreigabezeuge | • SMB-Dateifreigabe, die auf einem Dateiserver konfiguriert ist, der Windows Server ausführt<br>• Speichert keine Kopie der Clusterdatenbank<br>• Verwaltet Clusterinformationen nur in der Datei "witness.log"<br>• Besonders für Cluster mit repliziertem Speicher für mehrere Standorte geeignet | • Es sind mindestens 5 MB freier Speicherplatz erforderlich<br>• Muss dem einzelnen Cluster zugeteilt und nicht zum Speichern von Benutzer- oder Anwendungsdaten verwendet werden<br>• Schreibberechtigungen müssen für das Computerobjekt für den Clusternamen aktiviert sein<br><br>Nachfolgend sind weitere Überlegungen zu einem Dateiserver aufgeführt, der den Dateifreigabezeugen hostet:<br>• Ein einzelner Dateiserver mit Dateifreigabezeugen kann für mehrere Cluster konfiguriert werden.<br>• Der Dateiserver muss sich an einem Standort befinden, der von der Clusterarbeitsauslastung getrennt ist. Dadurch haben alle Clusterstandorte bei einer Unterbrechung der Netzwerkkommunikation zwischen den Standorten dieselbe Chance, diesen Zwischenfall zu überstehen. Wenn sich der Dateiserver am gleichen Standort befindet, wird der Standort zum primären Standort. Dies ist dann der einzige Standort, der auf die Dateifreigabe zugreifen kann.<br>• Der Dateiserver kann auf einem virtuellen Computer ausgeführt werden, wenn der virtuelle Computer nicht auf demselben Cluster gehostet wird, der den Dateifreigabezeugen verwendet.<br>• Der Dateiserver kann auf einem separaten Failovercluster konfiguriert werden, um eine hohe Verfügbarkeit zu bieten. |
| Cloudzeuge | • Eine in Azure BLOB Storage gespeicherte Zeugen Datei<br>• Empfohlen, wenn alle Server im Cluster über eine zuverlässige Internet Verbindung verfügen. | Siehe bereitstellen eines cloudzeugen. |

**„Knotenvotumszuweisung“**

Als erweiterte Quorum Konfigurationsoption können Sie die Quorum Stimmen auf Knoten Basis zuweisen oder entfernen. Standardmäßig werden allen Knoten Stimmen zugewiesen. Unabhängig von der Stimmenzuweisung funktionieren alle Knoten im Cluster weiterhin. Zudem erhalten sie weiterhin Clusterdatenbankupdates und

können Anwendungen hosten.

Möglicherweise möchten Sie die Stimmen von Knoten in bestimmten Notfallwiederherstellungskonfigurationen entfernen. Bei einem Cluster mit mehreren Standorten könnten Sie z. B. Stimmen von den Knoten am Sicherungsstandort entfernen, damit sich diese Knoten nicht auf die Quorumberechnungen auswirken. Diese Konfiguration wird nur für standortübergreifende manuelle Failover empfohlen. Weitere Informationen finden Sie weiter unten in diesem Thema unter Quorumüberlegungen zu Notfallwiederherstellungskonfigurationen.

Die konfigurierte Stimme eines Knotens kann durch Überprüfen der allgemeinen **nodeweight** -Eigenschaft des Cluster Knotens mithilfe des Windows PowerShell-Cmdlets Get-clusternodeüberprüft werden. Der Wert 0 gibt an, dass für den Knoten keine Quorumstimme konfiguriert ist. Der Wert 1 gibt an, dass die Quorumstimme des Knotens zugewiesen wurde und sie vom Cluster verwaltet wird. Weitere Informationen zur Verwaltung von Knotenstimmen finden Sie unter Dynamische Quorumverwaltung in diesem Thema.

Die Stimmenzuweisung für alle Clusterknoten kann mithilfe des Validierungstests **Clusterquorum überprüfen** überprüft werden.

#### Weitere Überlegungen zur Zuweisung von Knoten Stimmen

- Die Knotenvotumszuweisung wird nicht empfohlen, um eine ungerade Anzahl von abstimmenden Knoten zu erzwingen. Stattdessen müssen Sie einen Datenträgerzeugen oder einen Dateifreigabezeugen konfigurieren. Weitere Informationen finden Sie weiter unten in diesem Thema unter Zeugen Konfiguration .
- Wenn die dynamische Quorumverwaltung aktiviert ist, können die Stimmen nur für Knoten dynamisch zugewiesen oder entfernt werden, die für die Zuweisung von Knotenstimmen konfiguriert sind. Weitere Informationen finden Sie weiter unten in diesem Thema unter Dynamische Quorumverwaltung.

### „Dynamische Quorumverwaltung“

In Windows Server 2012 können Sie als erweiterte Quorum Konfigurationsoption die dynamische Quorum Verwaltung nach Clustern aktivieren. Weitere Informationen zur Funktionsweise des dynamischen Quorums finden Sie in dieser Erklärung.

Bei der dynamischen Quorumverwaltung ist es außerdem für Cluster möglich, dass sie auf dem letzten verbleibenden Clusterknoten ausgeführt werden können. Durch die dynamische Anpassung der Anforderungen an die Quorummehrheit kann der Cluster das fortlaufende Herunterfahren von Knoten für einen einzelnen Knoten fortsetzen.

Die vom Cluster zugewiesene dynamische Stimme eines Knotens kann mit der allgemeinen **dynamicweight** -Eigenschaft des Cluster Knotens mithilfe des Windows PowerShell-Cmdlets Get-clusternode überprüft werden. Der Wert 0 gibt an, dass der Knoten keine Quorumstimme besitzt. Der Wert 1 gibt an, dass der Knoten eine Quorumstimme besitzt.

Die Stimmenzuweisung für alle Clusterknoten kann mithilfe des Validierungstests **Clusterquorum überprüfen** überprüft werden.

#### Weitere Überlegungen zur dynamischen Quorum Verwaltung

- Die dynamische Quorumverwaltung gestattet es dem Cluster nicht, dass die Mehrheit der abstimmenden Mitglieder gleichzeitig einen Fehler erhält. Damit die Ausführung fortgesetzt werden kann, muss der Cluster beim Herunterfahren eines Clusters oder bei einem Fehler immer über die Quorummehrheit verfügen.
- Falls Sie die Stimme eines Knotens explizit entfernt haben, kann sie vom Cluster nicht dynamisch hinzugefügt oder entfernt werden.
- Wenn direkte Speicherplätze aktiviert ist, kann der Cluster nur zwei Knoten Ausfälle unterstützen. Dies wird im Abschnitt Pool Quorum ausführlicher erläutert.

## „Allgemeine Empfehlungen zur Quorumkonfiguration“

Die Clustersoftware konfiguriert das Quorum für einen neuen Cluster auf Basis der Anzahl der konfigurierten

Knoten und der Verfügbarkeit von freigegebenen Speicher automatisch. Dies ist im Allgemeinen die am besten geeignete Quorumkonfiguration für diesen Cluster. Es ist jedoch eine gute Idee, die Quorumkonfiguration zu überprüfen, nachdem der Cluster erstellt wurde und bevor der Cluster in der Produktionsumgebung eingesetzt wird. Zum Anzeigen der detaillierten Konfiguration des Cluster Quorums können Sie den Konfigurationsüberprüfungs-Assistenten oder das Windows PowerShell-Cmdlet Test-Cluster verwenden, um den Test **Quorum Konfiguration** überprüfen auszuführen. In Failovercluster-Manager wird die grundlegende Quorum Konfiguration in den zusammenfassenden Informationen für den ausgewählten Cluster angezeigt. Sie können auch die Informationen zu den Quorum Ressourcen überprüfen, die beim Ausführen des Windows PowerShell-Cmdlets Get-Clusterquorum zurückgegeben werden.

Sie können den Test **Quorumkonfiguration überprüfen** jederzeit ausführen, um zu überprüfen, ob die Quorumkonfiguration für Ihren Cluster optimal geeignet ist. Die Testausgabe gibt die optimalen Einstellungen an. Zudem weist die darauf hin, ob eine Änderung an der Quorumkonfiguration empfohlen wird. Wenn eine Änderung empfohlen wird, können Sie die empfohlenen Einstellungen mithilfe des Assistenten zum Konfigurieren des Clusterquorums anwenden.

Ändern Sie die Quorumkonfiguration nicht nachdem der Cluster in der Produktionsumgebung eingesetzt wurde, sofern Sie nicht ermittelt haben, dass die Änderung für Ihren Cluster angemessen ist. In folgenden Situationen können Sie eine Änderung der Quorumkonfiguration erwägen:

- Hinzufügen oder Entfernen von Knoten
- Hinzufügen oder Entfernen von Speicher
- Bei langfristigen Knoten- oder Zeugenfehlern
- Wiederherstellung eines Clusters in einem Notfallwiederherstellungsszenario mit mehreren Standorten

Weitere Informationen zum Überprüfen eines Failoverclusters finden Sie unter Überprüfen der Hardware für einen Failovercluster.

## „Konfigurieren des Clusterquorums“

Sie können die Cluster Quorum Einstellungen mithilfe Failovercluster-Manager oder der Windows PowerShell-Cmdlets für Failovercluster konfigurieren.

> **IMPORTANT**
> In der Regel ist die Quorumkonfiguration am besten geeignet, die vom Assistenten zum Konfigurieren des Clusterquorums empfohlen wird. Es wird empfohlen, dass Sie die Quorumkonfiguration nur anpassen, wenn Sie ermittelt haben, dass die Änderung für den Cluster angemessen ist. Weitere Informationen finden Sie in diesem Thema unter Allgemeine Empfehlungen zur Quorumkonfiguration.

### Konfigurieren der Clusterquorumeinstellungen

Die erforderlichen Mindestberechtigungen zur Ausführung dieses Vorgangs ist die Mitgliedschaft in der lokalen Gruppe **Administratoren** auf den einzelnen Clusterservern oder eine gleichwertige Mitgliedschaft. Das verwendete Konto muss zudem ein Domänenbenutzerkonto sein.

> **NOTE**
> Sie können die Clusterquorumkonfiguration ändern, ohne den Cluster zu beenden oder die Clusterressourcen offline zu stellen.

### Ändern Sie die Quorum Konfiguration in einem Failovercluster, indem Sie Failovercluster-Manager

1. Wählen Sie im Failovercluster-Manager den zu ändernden Cluster aus, oder geben Sie ihn an.

2. Wählen Sie bei ausgewähltem Cluster unter **Aktionen** die Option **Weitere Aktionen** aus, und klicken Sie

dann auf **Cluster Quorum Einstellungen konfigurieren**. Der Assistent zum Konfigurieren des Clusterquorums wird angezeigt. Klicken Sie auf **Weiter**.

3. Wählen Sie auf der Seite **Quorumkonfigurationsoption auswählen** eine der drei verfügbaren Konfigurationsoptionen aus, und führen Sie dann die Schritte für diese Option aus. Bevor Sie die Quorumeinstellungen konfigurieren, können Sie Ihre Auswahl überprüfen. Weitere Informationen zu den Optionen finden Sie Untergrund Legendes zu Quorumsweiter oben in diesem Thema.

   - Um dem Cluster das automatische Zurücksetzen der Quorum Einstellungen zu ermöglichen, die für Ihre aktuelle Cluster Konfiguration optimal sind, wählen Sie **typische Einstellungen verwenden** aus, und schließen Sie dann den Assistenten ab.

   - Um den Quorum Zeugen hinzuzufügen oder zu ändern, wählen Sie **den Quorum Zeugen hinzufügen oder ändern**aus, und führen Sie dann die folgenden Schritte aus. Weitere Informationen und Überlegungen zum Konfigurieren eines Quorumzeugen finden Sie in diesem Thema unter Zeugenkonfiguration.

     a. Wählen Sie auf der Seite **Quorumzeugen auswählen** eine Option zum Konfigurieren eines Datenträgerzeugen oder eines Dateifreigabezeugen aus. Der Assistent zeigt die Zeugenauswahloptionen an, die für Ihren Cluster empfohlen werden.

     > **NOTE**
     > Sie können auch die Option **Keinen Quorumzeugen konfigurieren** auswählen und dann den Assistenten abschließen. Wenn Sie über eine gerade Anzahl von abstimmenden Knoten in Ihrem Cluster verfügen, ist dies möglicherweise nicht die empfohlene Konfiguration.

     b. Wenn Sie die Option zum Konfigurieren eines Datenträgerzeugen auswählen, wählen Sie auf der Seite **Speicherzeugen konfigurieren** das Speichervolume aus, das Sie als Datenträgerzeugen zuweisen möchten, und schließen Sie dann den Assistenten ab.

     c. Wenn Sie die Option zum Konfigurieren eines Dateifreigabezeugen auswählen, geben Sie auf der Seite **Dateifreigabezeugen konfigurieren** eine Dateifreigabe ein, oder navigieren Sie zu dieser Freigabe, die als Zeugenressource verwendet wird, und schließen Sie dann den Assistenten ab.

   - Um die Einstellungen für die Quorum Verwaltung zu konfigurieren und den Quorum Zeugen hinzuzufügen oder zu ändern, wählen Sie **Erweiterte Quorum Konfiguration und Zeugen Auswahl**aus, und führen Sie dann die folgenden Schritte aus. Weitere Informationen und Überlegungen zu den erweiterten Quorumkonfigurationseinstellungen finden Sie in diesem Thema unter Knotenvotumszuweisung und Dynamische Quorumverwaltung.

     a. Wählen Sie auf der Seite **Votierungskonfiguration auswählen** eine Option zum Zuweisen von Stimmen zu Knoten aus. Standardmäßig wird allen Knoten eine Stimme zugewiesen. In bestimmten Szenarien können Sie Stimmen jedoch nur zu einer Teilmenge von Knoten zuweisen.

     > **NOTE**
     > Sie können auch die Option **Keine Knoten** auswählen. Dies wird im Allgemeinen nicht empfohlen, da es den Knoten dadurch nicht gestattet ist, an der Quorumabstimmung teilzunehmen. Zudem erfordert sie die Konfiguration eines Datenträgerzeugen. Der Datenträgerzeuge wird für den Cluster zu einem einzelnen Fehlerpunkt.

     b. Auf der Seite **Quorumverwaltung konfigurieren** können Sie die Option **Die Zuordnung**

**von Knotenvoten kann vom Cluster dynamisch verwaltet werden** aktivieren oder deaktivieren. Durch die Auswahl dieser Option wird die Verfügbarkeit des Clusters im Allgemeinen erhöht. Die Option ist standardmäßig aktiviert, und es wird dringend empfohlen, diese Option nicht zu deaktivieren. Mithilfe dieser Option kann der Cluster in Fehlerszenarien weiterhin ausgeführt werden, die nicht möglich sind, wenn diese Option deaktiviert ist.

c. Wählen Sie auf der Seite **Quorumzeugen auswählen** eine Option zum Konfigurieren eines Datenträgerzeugen oder eines Dateifreigabezeugen aus. Der Assistent zeigt die Zeugenauswahloptionen an, die für Ihren Cluster empfohlen werden.

> **NOTE**
> Sie können auch die Option **Keinen Quorumzeugen konfigurieren** auswählen und dann den Assistenten abschließen. Wenn Sie über eine gerade Anzahl von abstimmenden Knoten in Ihrem Cluster verfügen, ist dies möglicherweise nicht die empfohlene Konfiguration.

d. Wenn Sie die Option zum Konfigurieren eines Datenträgerzeugen auswählen, wählen Sie auf der Seite **Speicherzeugen konfigurieren** das Speichervolume aus, das Sie als Datenträgerzeugen zuweisen möchten, und schließen Sie dann den Assistenten ab.

e. Wenn Sie die Option zum Konfigurieren eines Dateifreigabezeugen auswählen, geben Sie auf der Seite **Dateifreigabezeugen konfigurieren** eine Dateifreigabe ein, oder navigieren Sie zu dieser Freigabe, die als Zeugenressource verwendet wird, und schließen Sie dann den Assistenten ab.

4. Klicken Sie auf **Weiter**. Bestätigen Sie Ihre Auswahl auf der angezeigten Bestätigungsseite, und klicken Sie dann auf **weiter**.

Wenn Sie den Assistenten ausführen und die Seite **Zusammenfassung** angezeigt wird, klicken Sie auf **Bericht anzeigen**, wenn Sie einen Bericht über die vom Assistenten durchgeführten Aufgaben anzeigen möchten. Der neueste Bericht verbleibt im Ordner " *systemroot*\-**Cluster Berichte** " mit dem Namen " **quorenconfiguration.MHT**".

> **NOTE**
> Nachdem Sie das Clusterquorum konfiguriert haben, wird empfohlen, dass Sie den Test **Quorumkonfiguration überprüfen** ausführen, um die aktualisierten Quorumeinstellungen zu überprüfen.

### Gleichwertige Windows PowerShell-Befehle

In den folgenden Beispielen wird gezeigt, wie das Cmdlet Set-Clusterquorum und andere Windows PowerShell-Cmdlets zum Konfigurieren des Cluster Quorums verwendet werden.

Im folgenden Beispiel wird die Quorumkonfiguration für Cluster *CONTOSO-FC1* in eine Konfiguration mit einfacher Knotenmehrheit ohne Quorumzeugen geändert.

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

Im folgenden Beispiel wird die Quorumkonfiguration auf dem lokalen Cluster in eine Knotenmehrheit mit Zeugenkonfiguration geändert. Die Datenträgerressourcen namens *Cluster Disk 2* wird als Datenträgerzeuge konfiguriert.

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

Im folgenden Beispiel wird die Quorumkonfiguration auf dem lokalen Cluster in eine Knotenmehrheit mit Zeugenkonfiguration geändert. Die Dateifreigabe Ressource mit dem Namen * \ \"\deso-FS\-* Dateifreigabe" ist als Datei frei gaben Zeuge konfiguriert.

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

Im folgenden Beispiel wird die Quorumstimme von Knoten *ContosoFCNode1* auf dem lokalen Cluster entfernt.

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

Im folgenden Beispiel wird die Quorumstimme zum Knoten *ContosoFCNode1* auf dem lokalen Cluster hinzugefügt.

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

Im folgenden Beispiel wird die **DynamicQuorum**-Eigenschaft des Clusters *CONTOSO-FC1* aktiviert (wenn diese zuvor deaktiviert war):

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

# Wiederherstellen eines Clusters durch Starten ohne Quorum

Ein Cluster ohne ausreichende Anzahl von Quorumstimmen wird nicht gestartet. Als ersten Schritt sollten Sie immer die Clusterquorumkonfiguration bestätigen und untersuchen, warum der Cluster das Quorum verloren hat. Dies kann vorkommen, wenn Sie über nicht reagierende Knoten verfügen. Es kann auch auftreten, wenn der primäre Standort bei einem Cluster mit mehreren Standorten nicht erreichbar ist. Nachdem Sie die Hauptursache für den Clusterfehler ermittelt haben, können Sie die in diesem Abschnitt beschriebenen Wiederherstellungsschritte ausführen.

> **NOTE**
> - Wenn der Clusterdienst aufgrund eines verlorenen Quorums beendet wird, wird Ereignis-ID 1177 im Systemprotokoll angezeigt.
> - Die Ursache für ein verlorenes Clusterquorum muss immer ermittelt werden.
> - Bevorzugt sollte der Knoten oder Quorumzeuge in einen fehlerfreien Status (zum Cluster hinzugefügt) versetzt werden, anstatt den Cluster ohne Zeugen zu starten.

### Erzwungenes Starten von Clusterknoten

Nachdem Sie ermittelt haben, dass Ihr Cluster nicht wiederhergestellt werden kann, indem Sie die Knoten oder den Quorumzeugen in einen fehlerfreien Status versetzen, ist es erforderlich, den Start des Clusters zu erzwingen. Durch den erzwungenen Start des Clusters werden die Einstellungen Ihrer Clusterquorumkonfiguration außer Kraft gesetzt und der Cluster im Modus **ForceQuorum** gestartet.

Der erzwungene Start eines Clusters ohne Quorum ist möglicherweise besonders hilfreich für Cluster mit mehreren Standorten. Betrachten Sie ein Notfallwiederherstellungsszenario mit einem Cluster, der separat angeordnete primäre Standorte und Sicherungsstandorte, *SiteA* und *SiteB*, enthält. Wenn bei *SiteA* ein ernsthafter Notfall eintritt, könnte es sehr lange dauern, bis der Standort wieder online ist. Sie würden dann für *SiteB* sicherlich erzwingen wollen, dass dieser Standort online gestellt wird, auch wenn er kein Quorum besitzt.

Wenn ein Cluster im **ForceQuorum**-Modus gestartet wird und er ausreichend Quorumstimmen zurückgewonnen hat, verlässt der Cluster automatisch den erzwungenen Status und verhält sich normal. Daher ist es nicht

erforderlich, den Cluster erneut normal zu starten. Wenn der Cluster einen Knoten und dann das Quorum verliert, wird er offline gestellt, da er sich nicht mehr im erzwungenen Status befindet. Damit der Cluster wieder online geschaltet werden kann, wenn er nicht über ein Quorum verfügt, muss der Cluster ohne Quorum gestartet werden.

> **IMPORTANT**
>
> - Nachdem der Start eines Clusters erzwungen wurde, verfügt der Administrator über die vollständige Kontrolle über den Cluster.
> - Der Cluster verwendet die Clusterkonfiguration auf dem Knoten, auf dem der Start des Clusters erzwungen wurde und repliziert ihn auf alle anderen Knoten, die verfügbar sind.
> - Durch den erzwungenen Start des Clusters ohne Quorum werden alle Quorumkonfigurationseinstellungen ignoriert, während der Cluster im Modus **ForceQuorum** verbleibt. Dies umfasst bestimmte Knotenvotumszuweisungen und Einstellungen für die dynamische Quorumverwaltung.

**Verhindern des Quorums auf verbleibenden Clusterknoten**

Nachdem Sie den erzwungenen Start des Clusters auf einem Knoten ausgeführt haben, ist es erforderlich, alle verbleibenden Knoten im Cluster mit einer Einstellung zu starten, um das Quorum zu verhindern. Ein Knoten, der mit einer Einstellung gestartet wurde, die das Quorum verhindert, zeigt dem Clusterdienst an, dass die Zuordnung zu einem vorhandenen aktiven Cluster erfolgen soll, anstatt eine neue Clusterinstanz zu erzeugen. Dadurch wird verhindert, dass die verbleibenden Knoten einen unterteilten Cluster bilden, der zwei konkurrierende Instanzen enthält.

Dies ist erforderlich, wenn Sie Ihren Cluster in einigen Notfallwiederherstellungsszenarien mit mehreren Standorten wiederherstellen müssen, nachdem Sie den erzwungenen Start des Clusters an Ihrem Sicherungsstandort, *SiteB*, ausgeführt haben. Um den Cluster mit dem erzwungenen Start am Standort *SiteB* hinzuzufügen, müssen die Knoten am primären Standort, *SiteA*, mit verhindertem Quorum gestartet werden.

> **IMPORTANT**
>
> Nach dem erzwungenen Start eines Clusters auf einem Knoten wird empfohlen, dass Sie die verbleibenden Knoten immer mit verhindertem Quorum starten.

So stellen Sie den Cluster mit Failovercluster-Manager wieder her:

1. Wählen Sie im Failovercluster-Manager den wiederherzustellenden Cluster aus, oder geben Sie ihn an.
2. Wählen Sie bei ausgewähltem Cluster unter **Aktionen** die Option **Cluster Start erzwingen** aus.

   Der Failovercluster-Manager erzwingt den Start des Clusters auf allen erreichbaren Knoten. Der Cluster verwendet beim Starten die aktuelle Clusterkonfiguration.

> **NOTE**
>
> - Um den Start des Clusters auf einem bestimmten Knoten zu erzwingen, der eine Cluster Konfiguration enthält, die Sie verwenden möchten, müssen Sie die Windows PowerShell-Cmdlets oder entsprechende Befehlszeilen Tools verwenden, die nach diesem Verfahren dargestellt werden.
> - Wenn Sie den Failover-Manager verwenden, um die Verbindung zu einem Cluster mit erzwungenem Start herzustellen, und Sie die Aktion **Clusterdienst starten** verwenden, um einen Knoten zu starten, dann wird der Knoten automatisch mit der Einstellung gestartet, die das Quorum verhindert.

**Entsprechende Windows PowerShell-Befehle (Start-clusternode)**

Im folgenden Beispiel wird gezeigt, wie das **Start-ClusterNode**-Cmdlet verwendet wird, um den Start des Clusters auf dem Knoten *ContosoFCNode1* zu erzwingen.

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

Alternativ können Sie den folgenden Befehl lokal auf dem Knoten eingeben:

```
Net Start ClusSvc /FQ
```

Im folgenden Beispiel wird gezeigt, wie das **Start-ClusterNode**-Cmdlet verwendet wird, um den Clusterdienst mit dem auf Knoten *ContosoFCNode1* verhinderten Quorum zu starten.

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

Alternativ können Sie den folgenden Befehl lokal auf dem Knoten eingeben:

```
Net Start ClusSvc /PQ
```

# „Quorumüberlegungen zu Notfallwiederherstellungskonfigurationen“

In diesem Abschnitt werden die Merkmale und Quorumkonfigurationen für zwei Clusterkonfigurationen mit mehreren Standorten für Notfallwiederherstellungsbereitstellungen zusammengefasst. Die Anweisungen zur Quorumkonfiguration unterscheiden sich in Abhängigkeit davon, ob für Arbeitsauslastungen zwischen den Standorten ein automatisches oder manuelles Failover erforderlich ist. Ihre Konfiguration hängt normalerweise von den in Ihrer Organisation vorhandenen Vereinbarungen zum Servicelevel (SLAs) ab, um Clusterarbeitsauslastungen bei einem Fehler oder Notfall an einem Standort bereitzustellen und zu unterstützen.

### Automatisches Failover

In dieser Konfiguration besteht der Cluster aus zwei oder mehr Standorten, die Clusterrollen hosten können. Wenn an einem Standort ein Fehler auftritt, wird für die anderen Standorte ein automatisches Failover erwartet. Daher muss das Clusterquorum konfiguriert werden, damit ein beliebiger Standort einen vollständigen Standortfehler aushalten kann.

In der folgenden Tabelle sind die Überlegungen und Empfehlungen für diese Konfiguration zusammengefasst.

| ELEMENT | BESCHREIBUNG |
|---|---|
| Anzahl von Knotenstimmen pro Standort | Sollte gleich sein |
| „Knotenvotumszuweisung“ | Knotenstimmen sollten nicht entfernt werden, da alle Knoten gleich wichtig sind |
| „Dynamische Quorumverwaltung“ | Sollte aktiviert sein |
| „Zeugenkonfiguration“ | Es wird ein Dateifreigabezeuge empfohlen, der an einem Standort konfiguriert ist, der sich von Clusterstandorten unterscheidet |
| Arbeitsauslastungen | Arbeitsauslastungen können an einem beliebigen Standort konfiguriert werden |

#### Weitere Überlegungen zum automatischen Failover

- Das Konfigurieren eines Dateifreigabezeugen an einem separaten Standort ist erforderlich, damit jeder Standort die gleichen Überlebenschancen erhält. Weitere Informationen finden Sie in diesem Thema unter Zeugenkonfiguration.

### Manuelles Failover

In dieser Konfiguration besteht der Cluster aus einem primären Standort, *SiteA*, und einem Sicherungsstandort (Wiederherstellungsstandort), *SiteB*. Clusterrollen werden am Standort *SiteA* gehostet. Wenn auf allen Knoten in *SiteA* ein Fehler auftritt, beendet der Cluster aufgrund der Clusterquorumkonfiguration seine Funktion. In diesem Szenario muss der Administrator ein manuelles Failover für die Clusterdienste zum Standort *SiteB* durchführen und weitere Schritte zum Wiederherstellen des Clusters ausführen.

In der folgenden Tabelle sind die Überlegungen und Empfehlungen für diese Konfiguration zusammengefasst.

| ELEMENT | BESCHREIBUNG |
| --- | --- |
| Anzahl von Knotenstimmen pro Standort | • Knotenstimmen sollten nicht von Knoten am primären Standort, **SiteA**, entfernt werden.<br>• Knotenstimmen sollten von Knoten am Sicherungsstandort, **SiteB**, entfernt werden.<br>• Wenn am Standort **SiteA** ein langfristiger Ausfall eintritt, müssen die Stimmen zu Knoten am Standort **SiteB** zugewiesen werden, um im Rahmen der Wiederherstellung eine Quorummehrheit an diesem Standort zu aktivieren. |
| „Dynamische Quorumverwaltung“ | Sollte aktiviert sein |
| „Zeugenkonfiguration“ | • Konfigurieren eines Zeugen bei ungerader Anzahl der Knoten am Standort **SiteA**<br>• Wenn ein Zeuge erforderlich ist, konfigurieren Sie entweder einen Dateifreigabezeugen oder einen Datenträgerzeugen, auf den nur Knoten am Standort **SiteA** zugreifen können (gelegentlich als asymmetrischer Datenträgerzeuge bezeichnet). |
| Arbeitsauslastungen | Verwenden bevorzugter Besitzer, damit Arbeitsauslastungen auf Knoten von Standort **SiteA** erhalten bleiben |

#### Weitere Überlegungen zum manuellen Failover

- Nur die Knoten am Standort *SiteA* werden anfänglich mit Quorumstimmen konfiguriert. Dies ist erforderlich, um sicherzustellen, dass sich der Status der Knoten am Standort *SiteB* nicht auf das Clusterquorum auswirkt.
- Die Wiederherstellungsschritte können in Abhängigkeit davon abweichen, ob Standort *SiteA* einen temporären oder einen langfristigen Fehler aushält.

## Weitere Informationen

- Failoverclustering
- Windows PowerShell-Cmdlets für Failovercluster
- Grundlegendes zum Cluster-und Pool Quorum

# Bereitstellen eines Cloudzeugen für einen Failovercluster

09.04.2020 • 17 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Der cloudzeuge ist ein Failovercluster-Quorum Zeugen, der Microsoft Azure verwendet, um eine Stimme für das Cluster Quorum bereitzustellen. Dieses Thema enthält eine Übersicht über die Cloud-Zeugen Funktion, die unterstützten Szenarien sowie Anweisungen zum Konfigurieren eines cloudzeugen für einen Failovercluster.

## Cloud-Zeugen Übersicht

Abbildung 1 zeigt eine Konfiguration eines Failoverclusters mit mehreren Standorten mit Windows Server 2016. In dieser Beispielkonfiguration (Abbildung 1) gibt es zwei Knoten in zwei Rechenzentren (als Standorte bezeichnet). Beachten Sie, dass sich ein Cluster über mehr als 2 Rechenzentren erstrecken kann. Außerdem kann jedes Rechenzentrum mehr als zwei Knoten aufweisen. Durch eine typische Cluster Quorum Konfiguration in diesem Setup (automatisches Failover-SLA) erhält jeder Knoten eine Stimme. Der Quorum Zeuge erhält eine zusätzliche Stimme, damit der Cluster weiterhin ausgeführt werden kann, selbst wenn eines der Rechenzentren einen Stromausfall hat. Die Mathematik ist einfach: Es sind insgesamt 5 Stimmen vorhanden, und Sie benötigen 3 Stimmen, damit der Cluster weiterhin ausgeführt wird.

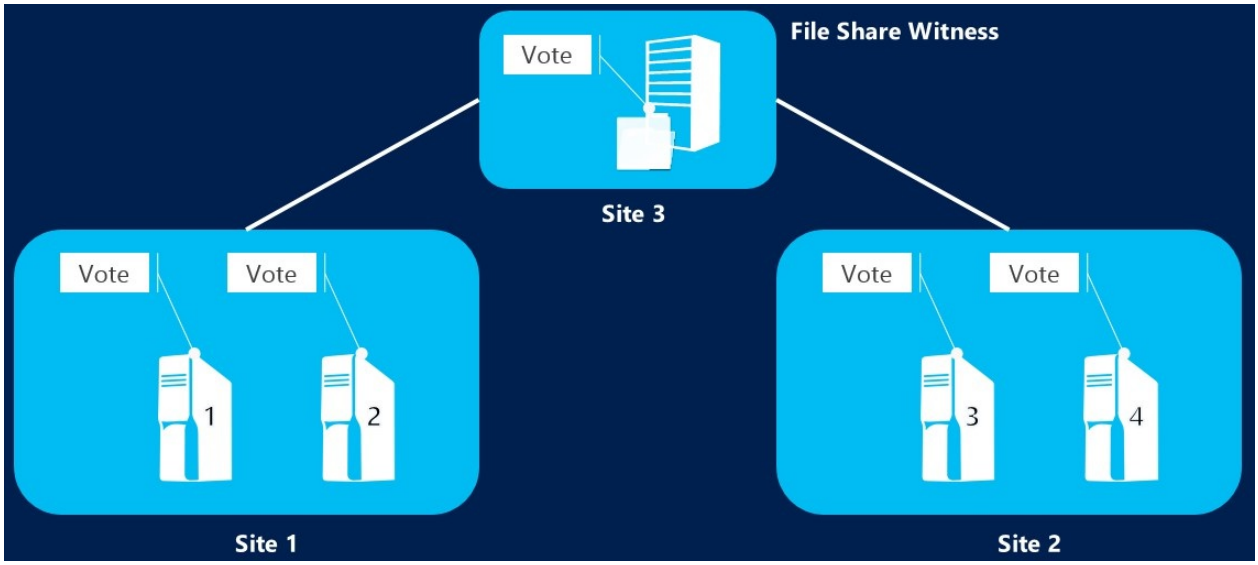



**Abbildung 1: Verwenden eines Dateifreigabe Zeugen als Quorum Zeugen**

Bei einem Stromausfall in einem Rechenzentrum wird empfohlen, den Quorum Zeugen an einem anderen Speicherort als den beiden Rechenzentren zu hosten, um dem Cluster in einem anderen Rechenzentrum die gleiche Chance zu geben. Dies bedeutet in der Regel, dass ein drittes separates Daten Center (Standort) zum Hosten eines Dateiservers erforderlich ist, der die Dateifreigabe unterstützt, die als Quorum Zeuge (Dateifreigabe Zeuge) verwendet wird.

Die meisten Organisationen verfügen über kein drittes separates Daten Center, das den Datei Server hostet, der den Dateifreigabe Zeugen unterstützt. Dies bedeutet, dass Unternehmen in erster Linie den Datei Server in einem der beiden Rechenzentren hosten, die durch Erweiterung dieses Rechenzentrum zum primären Daten Center machen. In einem Szenario, in dem ein Stromausfall im primären Daten Center auftritt, würde der Cluster ausfallen, da das andere Daten Center nur 2 Stimmen aufweisen würde, was unter dem Quorum der Mehrheit von 3 Stimmen liegt. Für Kunden, die über ein drittes separates Daten Center verfügen, um den Dateiserver zu

hosten, ist es ein zusätzlicher Aufwand, den hoch verfügbaren Dateiserver zu verwalten, der den Datei frei gaben Zeugen unterstützt. Das Hosting von virtuellen Computern in den Public Cloud, auf denen der Datei Server für den Dateifreigabe Zeugen im Gast Betriebssystem ausgeführt wird, ist ein erheblicher Aufwand in Bezug auf die Einrichtung & Wartung.

Der cloudzeuge ist ein neuer Failovercluster-Quorum Zeugen, der Microsoft Azure als Schiedsrichter Punkt nutzt (Abbildung 2). Es verwendet Azure BLOB Storage, um eine BLOB-Datei zu lesen und zu schreiben, die dann als Schlichtungs Punkt bei der Auflösung von Split Brain verwendet wird.

Diese Vorgehensweise hat bedeutende Vorteile:

1. Nutzt Microsoft Azure (kein drittes separates Rechenzentrum erforderlich).
2. Verwendet standardmäßig verfügbare Azure BLOB Storage (kein zusätzlicher Wartungsaufwand für in Public Cloud gehostete virtuelle Maschinen).
3. Dasselbe Azure Storage Konto kann für mehrere Cluster verwendet werden (eine BLOB-Datei pro Cluster; eindeutige Cluster-ID, die als BLOB-Dateiname verwendet wird).
4. Sehr niedriger $cost zum Speicherkonto (sehr kleine Daten, die pro BLOB-Datei geschrieben werden, BLOB-Dateien werden nur einmal aktualisiert, wenn sich der Status der Cluster Knoten ändert).
5. Integrierter cloudzeugen-Ressourcentyp.

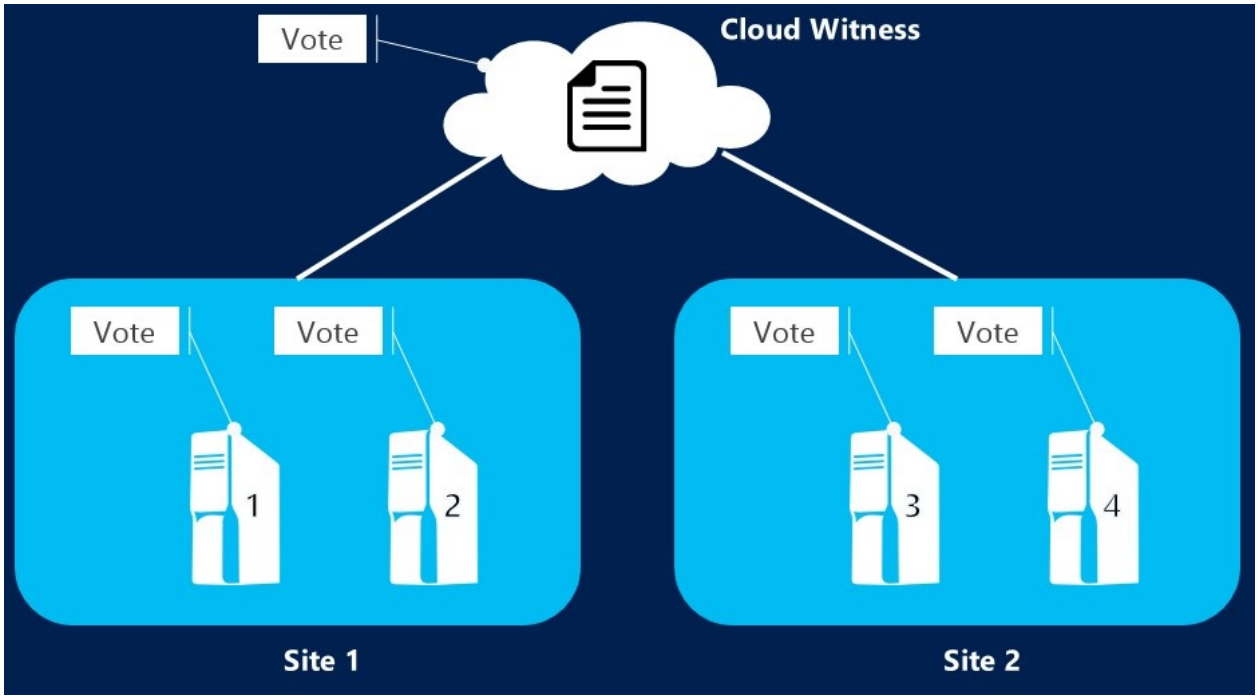



**Abbildung 2: Stretch-Cluster mit mehreren Standorten mit dem cloudzeugen als Quorum Zeugen**

Wie in Abbildung 2 dargestellt, gibt es keine dritte separate Site, die erforderlich ist. Der cloudzeuge erhält, wie jeder andere Quorum Zeuge, eine Stimme und kann an Quorum Berechnungen teilnehmen.

## Cloudzeuge: unterstützte Szenarien für einen einzelnen Zeugen Typen

Wenn Sie über eine failoverclusterbereitstellung verfügen, bei der alle Knoten das Internet erreichen können (durch Erweiterung von Azure), empfiehlt es sich, einen cloudzeugen als Quorum Zeugen Ressource zu konfigurieren.

Folgende Szenarien werden von einem cloudzeugen als Quorum Zeuge unterstützt:

- Die Notfall Wiederherstellung streckten Cluster mit mehreren Standorten (siehe Abbildung 2).
- Failovercluster ohne freigegebenen Speicher (SQL Always on usw.).
- Failovercluster, die in einem Gast Betriebssystem ausgeführt werden, das in Microsoft Azure Rolle für virtuelle

Computer (oder anderen Public Cloud) gehostet wird
- Failovercluster, die innerhalb des Gast Betriebssystems von Virtual Machines in privaten Clouds gehostet werden.
- Speicher Cluster mit oder ohne freigegebenen Speicher, z. b. Datei Server Cluster mit horizontaler Skalierung.
- Kleine Zweigstellen Cluster (auch Cluster mit zwei Knoten)

Ab Windows Server 2012 R2 empfiehlt es sich, immer einen Zeugen zu konfigurieren, da der Cluster die Zeugen Stimme automatisch verwaltet und die Knoten mit dynamischem Quorum Stimmen.

## Einrichten eines cloudzeugen für einen Cluster

Führen Sie die folgenden Schritte aus, um einen cloudzeugen als Quorum Zeugen für Ihren Cluster einzurichten:

1. Erstellen Sie ein Azure Storage Konto, das als cloudzeuge verwendet werden soll.
2. Konfigurieren Sie den cloudzeugen als Quorum Zeugen für Ihren Cluster.

## Erstellen Sie ein Azure Storage Konto, das als cloudzeuge verwendet werden soll.

In diesem Abschnitt wird beschrieben, wie Sie ein Speicherkonto erstellen und Endpunkt-URLs und Zugriffsschlüssel für dieses Konto anzeigen und kopieren.

Zum Konfigurieren des cloudzeugen müssen Sie über ein gültiges Azure Storage Konto verfügen, das zum Speichern der BLOB-Datei verwendet werden kann. Der cloudzeuge erstellt einen bekannten Container **MSFT-Cloud-Witness** unter dem Microsoft-Speicherkonto. Der cloudzeuge schreibt eine einzelne BLOB-Datei mit der entsprechenden eindeutigen Cluster-ID, die als Dateiname der BLOB-Datei in diesem **MSFT-Cloud-Witness-** Container verwendet wird. Dies bedeutet, dass Sie das gleiche Microsoft Azure Storage Konto verwenden können, um einen cloudzeugen für mehrere verschiedene Cluster zu konfigurieren.

Wenn Sie das gleiche Azure Storage Konto für die Konfiguration eines cloudzeugen für mehrere verschiedene Cluster verwenden, wird automatisch ein einzelner **MSFT-Cloud-Witness-** Container erstellt. Dieser Container enthält eine BLOB-Datei pro Cluster.

**So erstellen Sie ein Azure-Speicherkonto**

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie im Hubmenu Neu -> Daten und Speicher -> Speicherkonto.
3. Gehen Sie auf der Seite Speicherkonto erstellen folgendermaßen vor:
   a. Geben Sie einen Namen für Ihr Speicherkonto ein.
   Speicherkonto Namen müssen zwischen 3 und 24 Zeichen lang sein und dürfen nur Ziffern und Kleinbuchstaben enthalten. Der Name des Speicher Kontos muss auch innerhalb von Azure eindeutig sein.

   b. Wählen Sie unter **Kontoart** die Option **Allgemein** aus.
   Sie können kein BLOB Storage-Konto für einen cloudzeugen verwenden.

   c. Wählen Sie für **Leistung** die Option **Standard** aus.
   Azure Storage Premium kann nicht für einen cloudzeugen verwendet werden.

   d. Wählen Sie unter **Replikation** die Option **lokal redundanter Speicher (LRS)** aus.
   Failoverclustering verwendet die BLOB-Datei als Schiedsrichter Punkt. Dies erfordert einige Konsistenz Garantien beim Lesen der Daten. Daher müssen Sie für den **Replikationstyp** den **lokal redundanten Speicher** auswählen.

**Anzeigen und Kopieren von Speicherzugriffs Schlüsseln für Ihr Azure Storage Konto**

Wenn Sie ein Microsoft Azure Storage Konto erstellen, ist es zwei Zugriffs Schlüsseln zugeordnet, die

automatisch generiert werden: primärer Zugriffsschlüssel und sekundärer Zugriffsschlüssel. Verwenden Sie für die erstmalige Erstellung eines cloudzeugen den **primären Zugriffsschlüssel**. Es gibt keine Einschränkung hinsichtlich des Schlüssels, der für den cloudzeugen verwendet werden soll.

#### So können Sie Speicherzugriffs Schlüssel anzeigen und kopieren

Navigieren Sie im Azure-Portal zu Ihrem Speicherkonto, klicken Sie auf **alle Einstellungen** , und klicken Sie dann auf **Zugriffsschlüssel** , um Ihre Konto Zugriffsschlüssel anzuzeigen, zu kopieren und neu zu generieren. Das Blatt Zugriffsschlüssel enthält auch vorkonfigurierte Verbindungs Zeichenfolgen, die ihre primären und sekundären Schlüssel verwenden, die Sie zur Verwendung in Ihren Anwendungen kopieren können (siehe Abbildung 4).

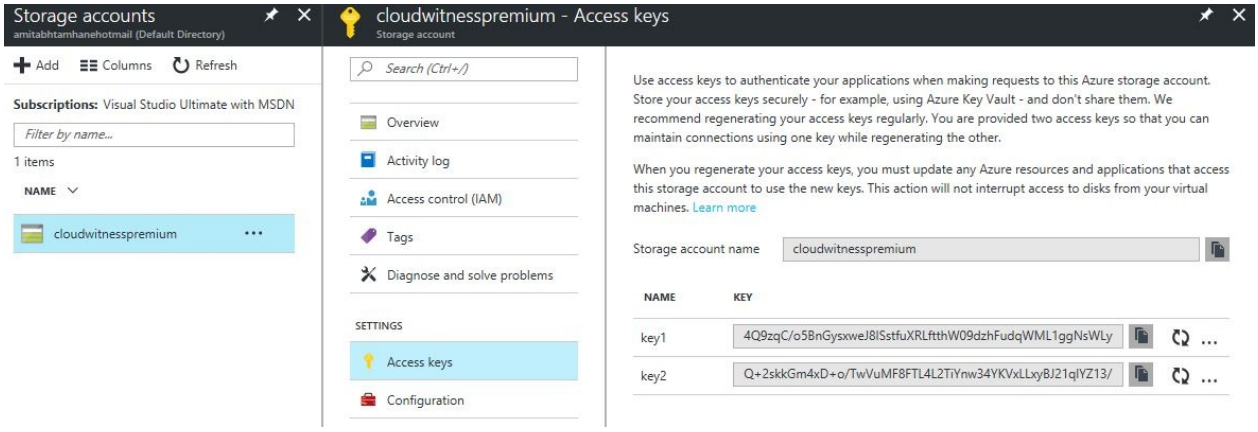



Abbildung 4: Speicherzugriffs Schlüssel

### Anzeigen und Kopieren von Endpunkt-URL-Links

Wenn Sie ein Speicherkonto erstellen, werden die folgenden URLs im folgenden Format generiert:

```
https://<Storage Account Name>.<Storage Type>.<Endpoint>
```

Der cloudzeuge verwendet immer **BLOB** als Speichertyp. Azure verwendet **. Core.Windows.net** als Endpunkt. Wenn Sie einen cloudzeugen konfigurieren, ist es möglich, ihn gemäß Ihrem Szenario mit einem anderen Endpunkt zu konfigurieren (z. b. Microsoft Azure Rechenzentrum in China einen anderen Endpunkt).

> **NOTE**
> Die Endpunkt-URL wird automatisch von der Cloud-Zeugen Ressource generiert, und für die URL ist kein zusätzlicher Konfigurationsschritt erforderlich.

#### So können Sie Endpunkt-URL-Links anzeigen und kopieren

Navigieren Sie im Azure-Portal zu Ihrem Speicherkonto, klicken Sie auf **alle Einstellungen** , und klicken Sie dann auf **Eigenschaften** , um Ihre Endpunkt-URLs anzuzeigen und zu kopieren (siehe Abbildung 5).

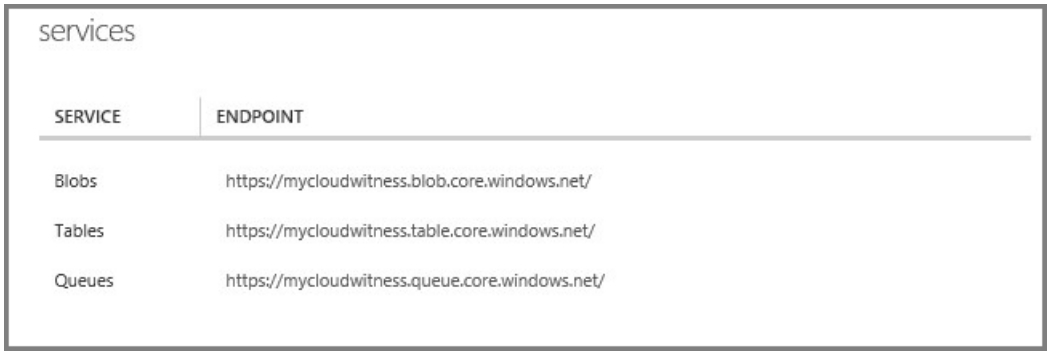



Abbildung 5: Verknüpfungen der Cloud-Zeugen Endpunkt-URL

Weitere Informationen zum Erstellen und Verwalten von Azure Storage Konten finden Sie unter Informationen zu Azure Storage Konten .

# Konfigurieren des cloudzeugen als Quorum Zeugen für Ihren Cluster

Die cloudzeugen Konfiguration ist innerhalb des vorhandenen Quorum Konfigurationsassistenten, der in die Failovercluster-Manager integriert ist, gut integriert.

**So konfigurieren Sie einen cloudzeugen als Quorum Zeugen**

1. Starten Sie Failovercluster-Manager.

2. Klicken Sie mit der rechten Maustaste auf den Cluster, > **Weitere Aktionen** -> **Konfigurieren der Cluster Quorum Einstellungen** (siehe Abbildung 6). Der Assistent zum Konfigurieren des Cluster Quorums wird gestartet.

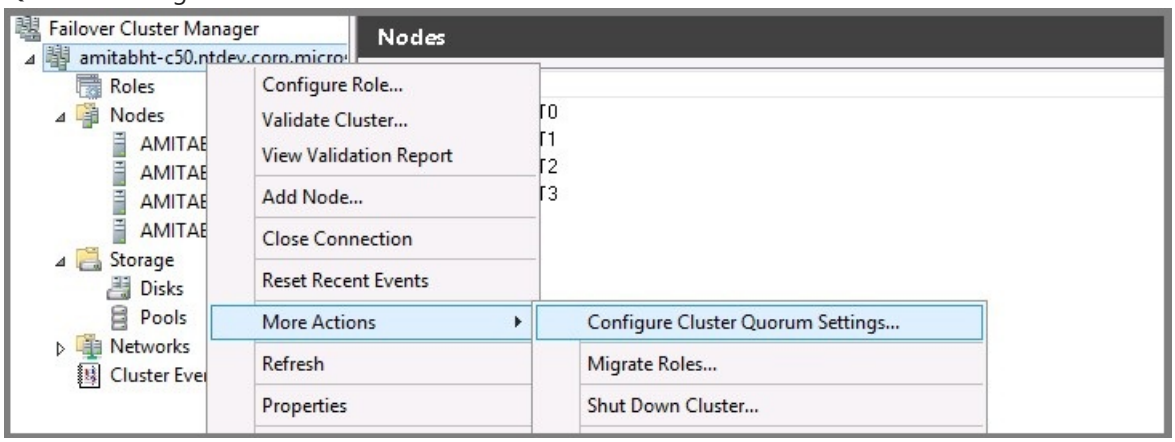



**Abbildung 6. Cluster Quorum Einstellungen**

3. Wählen Sie auf der Seite **Quorum Konfigurationen auswählen die Option Quorum Zeugen auswählen** (siehe Abbildung 7).

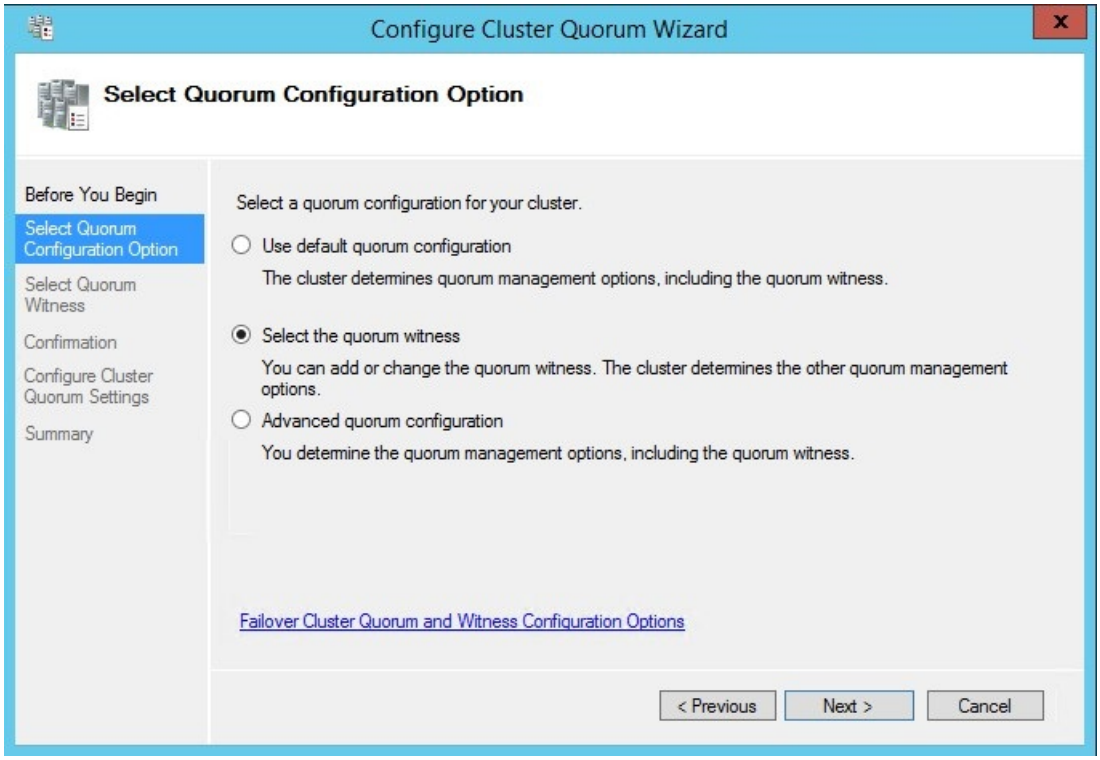



**Abbildung 7: Wählen Sie die Quorum Konfiguration aus.**

4. Wählen Sie auf der Seite **Quorum Zeugen auswählen** die Option **cloudzeuge konfigurieren** (siehe Abbildung 8).

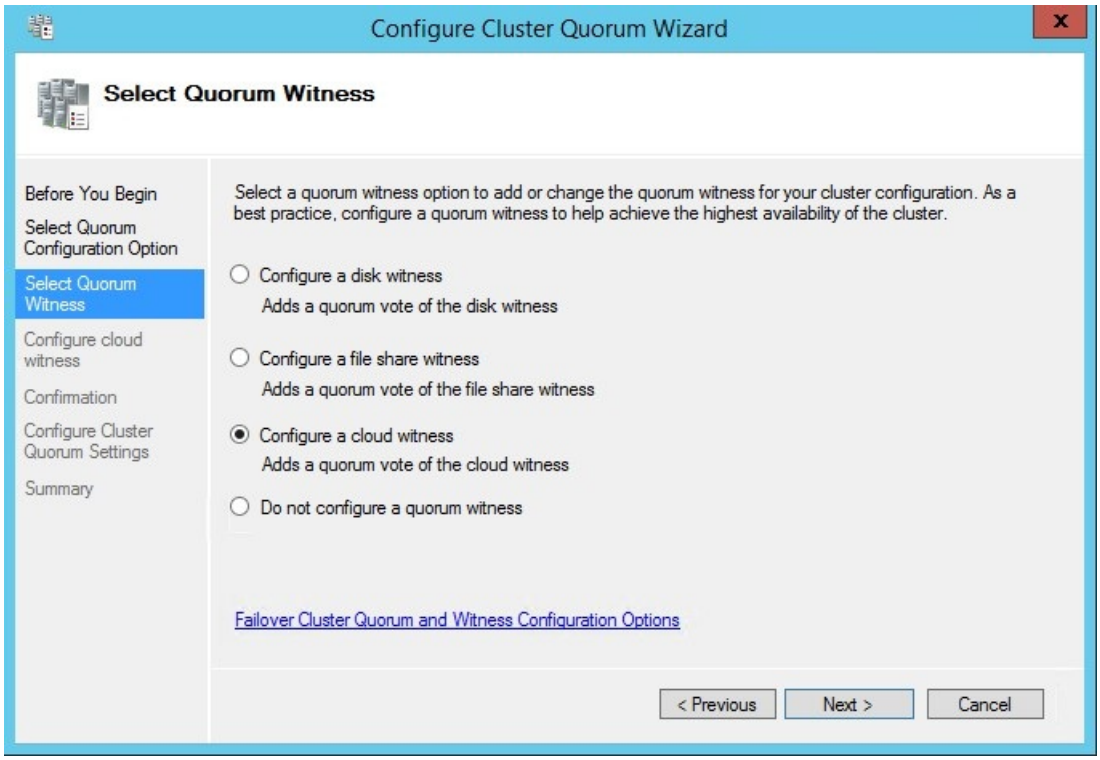



**Abbildung 8. Wählen Sie den Quorum Zeugen aus.**

5. Geben Sie auf der Seite **Cloud-Zeuge konfigurieren** die folgenden Informationen ein:

   a. (Erforderlicher Parameter) Azure Storage Kontoname.

   b. (Erforderlicher Parameter) Zugriffsschlüssel, der dem Speicherkonto entspricht.

      a. Wenn Sie zum ersten Mal erstellen, verwenden Sie den primären Zugriffsschlüssel (siehe Abbildung 5).

      b. Wenn Sie den primären Zugriffsschlüssel rotieren, verwenden Sie den sekundären Zugriffsschlüssel (siehe Abbildung 5).

   c. (Optionaler Parameter) Wenn Sie beabsichtigen, einen anderen Azure-Dienst Endpunkt (z. b. den Microsoft Azure-Dienst in China) zu verwenden, aktualisieren Sie den Endpunkt Servernamen.

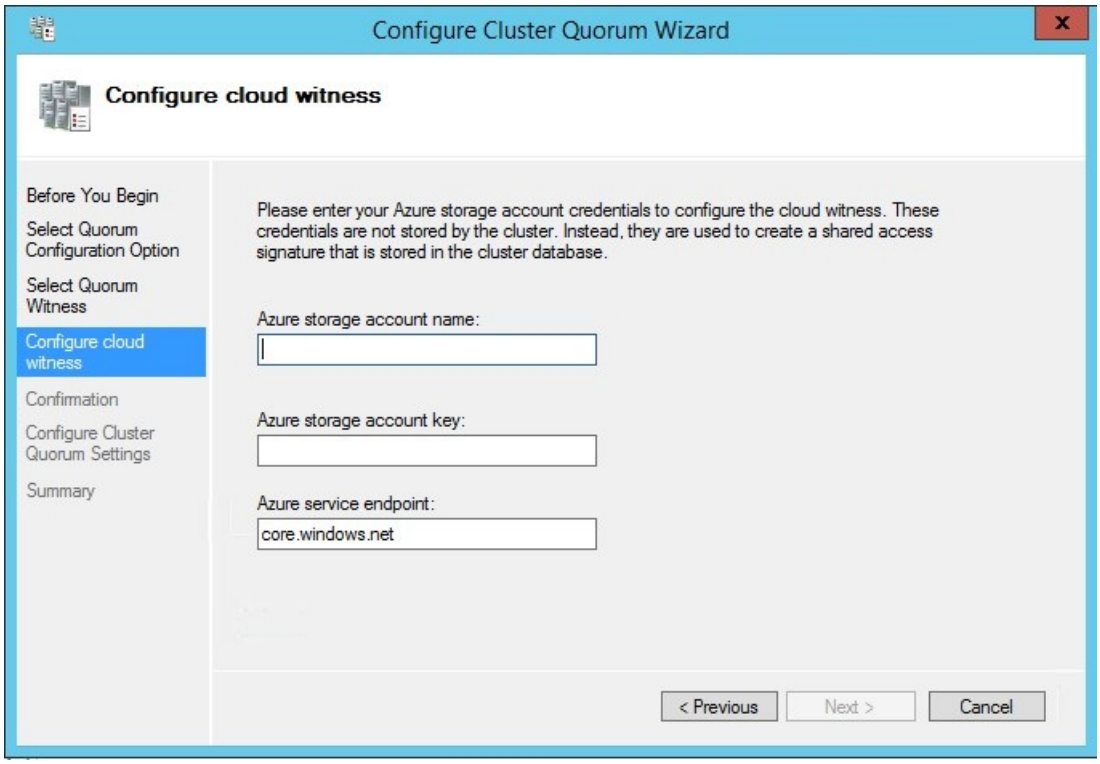



**Abbildung 9: Konfigurieren des cloudzeugen**

6. Nach erfolgreicher Konfiguration des cloudzeugen können Sie die neu erstellte Zeugen Ressource im Failovercluster-Manager-Snap-in anzeigen (siehe Abbildung 10).

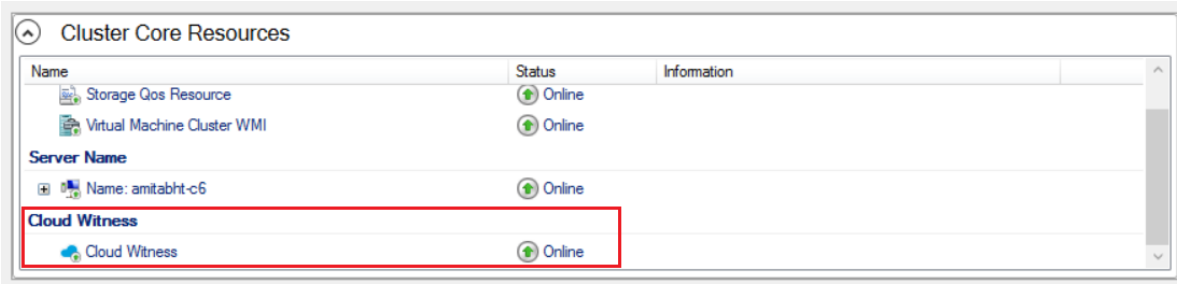



Abbildung 10: erfolgreiche Konfiguration des cloudzeugen

### Konfigurieren eines cloudzeugen mithilfe von PowerShell

Der vorhandene PowerShell-Befehl "Set-Clusterquorum" verfügt über neue zusätzliche Parameter, die dem cloudzeugen entsprechen.

Sie können den cloudzeugen mit dem `Set-ClusterQuorum` folgenden PowerShell-Befehl konfigurieren:

```
Set-ClusterQuorum -CloudWitness -AccountName <StorageAccountName> -AccessKey <StorageAccountAccessKey>
```

Für den Fall, dass Sie einen anderen Endpunkt (selten) verwenden müssen:

```
Set-ClusterQuorum -CloudWitness -AccountName <StorageAccountName> -AccessKey <StorageAccountAccessKey> -
Endpoint <servername>
```

### Überlegungen zu Azure Storage Konten mit dem cloudzeugen

Beachten Sie Folgendes, wenn Sie einen cloudzeugen als Quorum Zeugen für Ihren Failovercluster konfigurieren:

- Anstatt den Zugriffsschlüssel zu speichern, generiert und speichert der Failovercluster ein SAS-Token (Shared Access Security).
- Das generierte SAS-Token ist gültig, solange der Zugriffsschlüssel gültig ist. Wenn Sie den primären Zugriffsschlüssel rotieren, ist es wichtig, zuerst den cloudzeugen (auf allen Clustern, die dieses Speicherkonto verwenden) mit dem sekundären Zugriffsschlüssel zu aktualisieren, bevor Sie den primären Zugriffsschlüssel erneut generieren.
- Der cloudzeuge verwendet die HTTPS-Rest-Schnittstelle des Azure Storage Konto Diensts. Dies bedeutet, dass der HTTPS-Port auf allen Cluster Knoten geöffnet sein muss.

### Überlegungen zum Proxy mit dem cloudzeugen

Der cloudzeuge verwendet HTTPS (Standardport 443), um die Kommunikation mit dem Azure-BLOB-Dienst herzustellen. Stellen Sie sicher, dass der HTTPS-Port über den Netzwerk Proxy zugänglich ist

## Weitere Informationen

- Neues beim Failoverclustering unter Windows Server

# Bereitstellen eines Dateifreigabe Zeugen

09.04.2020 • 6 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ein Dateifreigabe Zeuge ist eine SMB-Freigabe, die der Failovercluster als Stimme im Cluster Quorum verwendet. Dieses Thema bietet einen Überblick über die Technologie und die neuen Funktionen in Windows Server 2019, einschließlich der Verwendung eines USB-Laufwerks, das mit einem Router als Datei frei gaben Zeuge verbunden ist.

Dateifreigabe Zeugen sind in folgenden Situationen nützlich:

- Ein cloudzeuge kann nicht verwendet werden, da nicht alle Server im Cluster über eine zuverlässige Internet Verbindung verfügen.
- Ein Datenträger Zeuge kann nicht verwendet werden, da keine freigegebenen Laufwerke für einen Datenträger Zeugen verwendet werden. Dabei kann es sich um einen direkte Speicherplätze Cluster, SQL Server Always on Verfügbarkeits Gruppen (AG), eine Exchange-Daten Bank Verfügbarkeits Gruppe (DAG) usw. handeln. Keiner dieser Cluster Typen verwendet freigegebene Datenträger.

## Anforderungen an den Dateifreigabe Zeugen

Sie können einen Dateifreigabe Zeugen auf einem in die Domäne eingebundenen Windows-Server hosten, oder auf Ihrem Cluster, auf dem Windows Server 2019 ausgeführt wird, auf allen Geräten, auf denen eine Dateifreigabe mit SMB 2 oder höher gehostet werden kann.

| DATEI SERVERTYP | UNTERSTÜTZTE CLUSTER |
| --- | --- |
| Alle Geräte mit einer SMB 2-Dateifreigabe | Windows Server 2019 |
| In die Domäne eingebundener Windows Server | Windows Server 2008 und höher |

Wenn auf dem Cluster Windows Server 2019 ausgeführt wird, gelten die folgenden Anforderungen:

- Eine SMB-Dateifreigabe *auf allen Geräten, die das SMB 2-Protokoll oder das spätere Protokoll verwenden*, einschließlich:
  - NAS-Geräte (Network-Attached Storage)
  - Windows-Computer, die einer Arbeitsgruppe hinzugefügt wurden
  - Router mit lokal verbundener USB-Speicher
- Ein lokales Konto auf dem Gerät zum Authentifizieren des Clusters
- Wenn Sie stattdessen Active Directory zum Authentifizieren des Clusters mit der Dateifreigabe verwenden, muss das Cluster Namen Objekt (CNO) über Schreibberechtigungen für die Freigabe verfügen, und der Server muss sich in derselben Active Directory Gesamtstruktur wie der Cluster befinden.
- Der freie Speicherplatz der Dateifreigabe beträgt 5 MB.

Wenn auf dem Cluster Windows Server 2016 oder eine frühere Version ausgeführt wird, gelten die folgenden Anforderungen:

- SMB-Dateifreigabe *auf einem Windows-Server, der mit derselben Active Directory Gesamtstruktur wie der Cluster* verknüpft ist
- Das Cluster Namen Objekt (CNO) muss über Schreibberechtigungen für die Freigabe verfügen.

- Der freie Speicherplatz der Dateifreigabe beträgt 5 MB.

Weitere Hinweise:

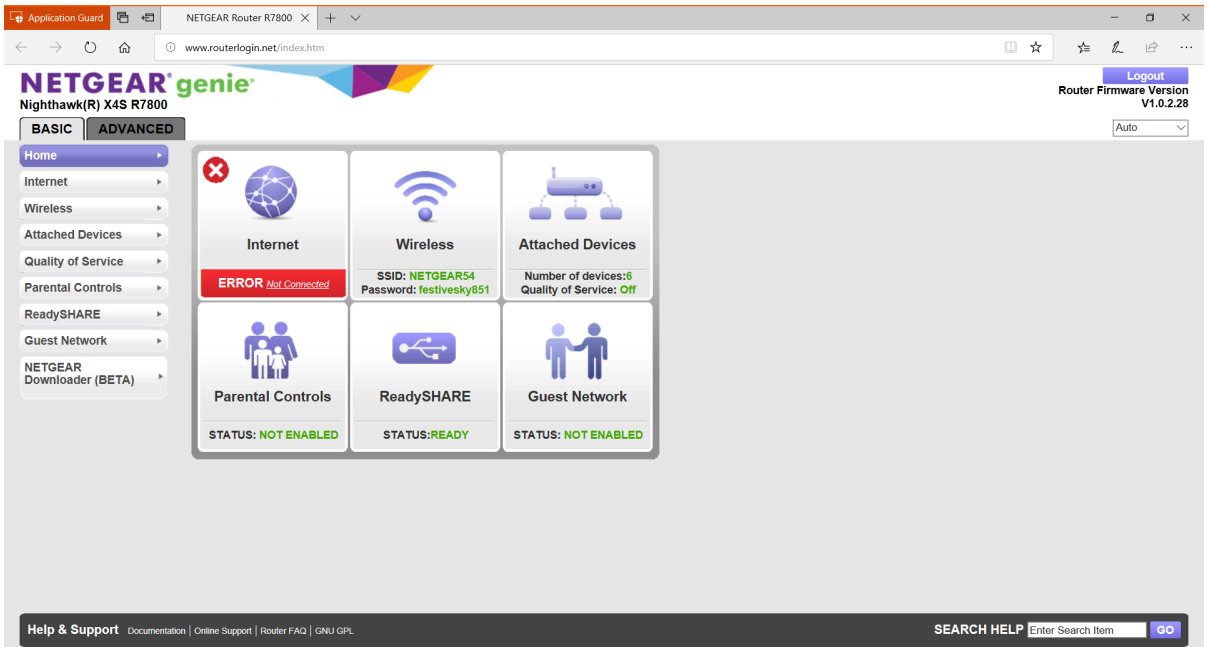
- Wenn Sie einen Dateifreigabe Zeugen verwenden möchten, der von anderen Geräten als einem in die Domäne eingebundenen Windows-Server gehostet wird, müssen Sie derzeit das PowerShell-Cmdlet **Set-Clusterquorum-Credential** verwenden, um den Zeugen festzulegen, wie weiter unten in diesem Thema beschrieben.
- Um Hochverfügbarkeit zu erreichen, können Sie einen Dateifreigabe Zeugen in einem separaten Failovercluster verwenden.
- Die Dateifreigabe kann von mehreren Clustern verwendet werden.
- Die Verwendung einer DFS-Freigabe (verteiltes Dateisystem) oder eines replizierten Speichers wird von keiner Version des Failoverclustering unterstützt. Diese können eine Split Brain-Situation verursachen, in der gruppierte Server unabhängig voneinander ausgeführt werden und zu einem Datenverlust führen können.

## Erstellen eines Dateifreigabe Zeugen auf einem Router mit einem USB-Gerät

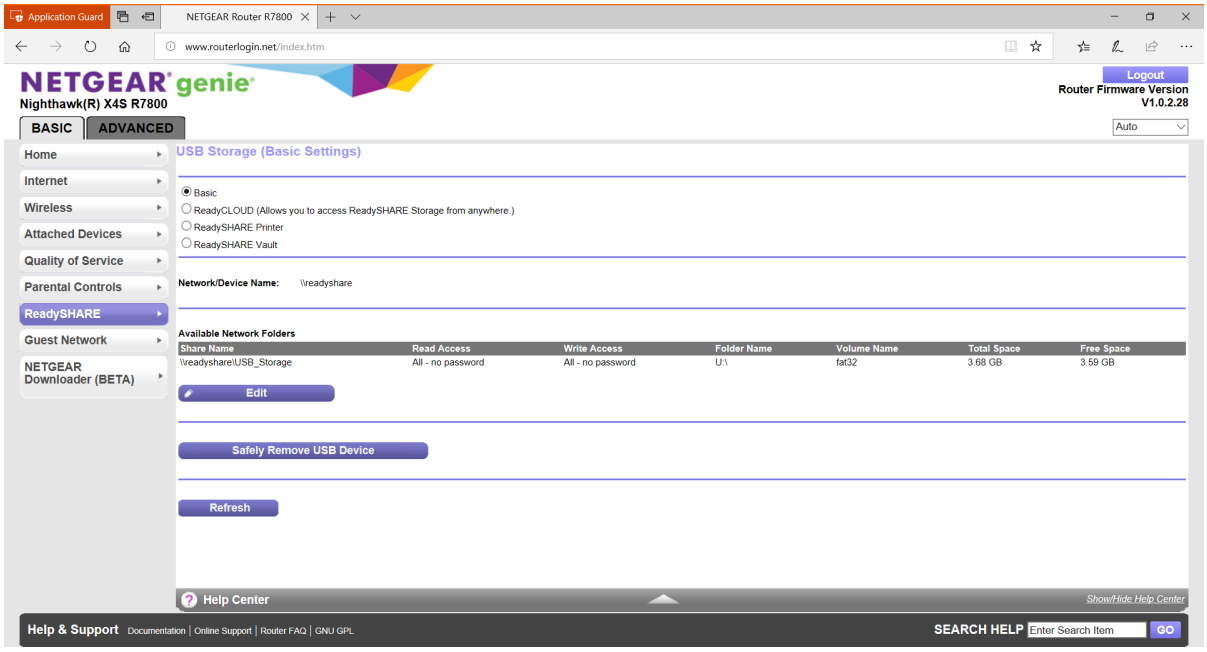
Bei der Microsoft Ignite 2018hatte DataOn Storage einen direkte Speicherplätze Cluster in seinem Kiosk Bereich. Dieser Cluster wurde mit einem Netgear Nighthawk X4S WiFi-Router über den USB-Anschluss als Datei frei gaben Zeuge verbunden, der diesem ähnelt.

Die Schritte zum Erstellen eines Dateifreigabe Zeugen mithilfe eines USB-Geräts auf diesem bestimmten Router sind unten aufgeführt. Beachten Sie, dass die Schritte auf anderen Routern und NAS-Geräten variieren und mit den vom Hersteller bereitgestellten Anweisungen durchgeführt werden sollten.

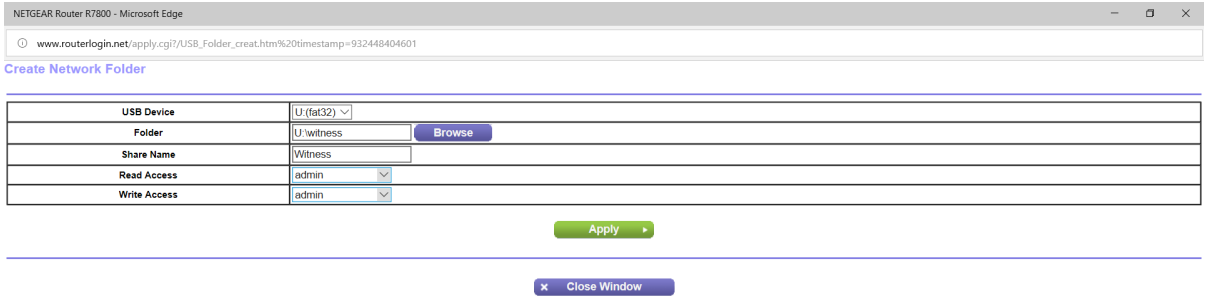
1. Melden Sie sich beim Router an, wenn das USB-Gerät angeschlossen ist.




2. Wählen Sie in der Liste der Optionen den Eintrag "Read-Share" aus. hier können Freigaben erstellt werden.




3. Für einen Dateifreigabe Zeugen ist nur eine einfache Freigabe erforderlich. Wenn Sie die Schaltfläche Bearbeiten auswählen, wird ein Dialogfeld angezeigt, in dem die Freigabe auf dem USB-Gerät erstellt werden kann.




4. Nachdem Sie die Schaltfläche anwenden ausgewählt haben, wird die Freigabe erstellt und kann in der Liste angezeigt werden.

Available Network Folders

| | Share Name | Read Access | Write Access | Folder Name | Volume Name | Total Space | Free Space |
|---|---|---|---|---|---|---|---|
| ○ | \\readyshare\USB_Storage | All - no password | All - no password | U:\ | fat32 | 3.68 GB | 3.59 GB |
| ○ | \\readyshare\Witness | admin | admin | U:\witness | fat32 | 3.68 GB | 3.59 GB |

+ Create Network Folder  Edit  × Delete

5. Nachdem die Freigabe erstellt wurde, wird die Erstellung des Datei frei gaben Zeugen für den Cluster mit PowerShell durchgeführt.

```
Set-ClusterQuorum -FileShareWitness \\readyshare\Witness -Credential (Get-Credential)
```

   Dadurch wird ein Dialogfeld angezeigt, in dem Sie das lokale Konto auf dem Gerät eingeben können.

Diese ähnlichen Schritte können auch auf anderen Routern mit USB-Funktionen, NAS-Geräten oder anderen Windows-Geräten ausgeführt werden.

# Paralleles Upgrade des Cluster Betriebssystems

09.04.2020 • 30 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Das parallele Upgrade des Cluster Betriebssystems ermöglicht einem Administrator, ein Upgrade des Betriebssystems der Cluster Knoten auszuführen, ohne die Hyper-V-oder Dateiserver mit horizontaler Skalierung Arbeits Auslastungen zu beenden. Mit diesem Feature können die Downtimesanktionen laut Vereinbarungen zum Servicelevel (Service Level Agreements, SLA) vermieden werden.

Das parallele Upgrade des Cluster Betriebssystems bietet die folgenden Vorteile:

- Failovercluster mit virtuellen Hyper-V-Computern und sofs-Workloads (Scale-Out File Server) können von Windows Server 2012 R2 (auf allen Knoten im Cluster ausgeführt) auf Windows Server 2016 (auf allen Cluster Knoten des Clusters ausgeführt) ohne Ausfallzeiten aktualisiert werden. Andere clusterworkloads, wie z. b. SQL Server, sind während der Zeit (in der Regel weniger als fünf Minuten) nicht verfügbar, um ein Failover auf Windows Server 2016 auszuführen.
- Es ist keine zusätzliche Hardware erforderlich. Sie können auch zusätzliche Cluster Knoten vorübergehend zu kleinen Clustern hinzufügen, um die Verfügbarkeit des Clusters während des parallelen Upgradevorgangs des Cluster Betriebssystems zu verbessern.
- Der Cluster muss nicht beendet oder neu gestartet werden.
- Ein neuer Cluster ist nicht erforderlich. Der vorhandene Cluster wird aktualisiert. Außerdem werden vorhandene in Active Directory gespeicherte Cluster Objekte verwendet.
- Der Upgradevorgang kann nur rückgängig gemacht werden, wenn der Kunde den "Point-of-No-Return"-Wert abweist, wenn auf allen Clusterknoten Windows Server 2016 ausgeführt wird und das PowerShell-Cmdlet "Update-clusterfunctionallevel" ausgeführt wird.
- Der Cluster unterstützt Patchen-und Wartungsvorgänge während der Ausführung im gemischten Betriebssystem Modus.
- Es unterstützt die Automatisierung über PowerShell und WMI.
- Die Eigenschaft **clusterfunctionallevel** der öffentlichen Cluster Eigenschaft gibt den Status des Clusters auf Windows Server 2016-Cluster Knoten an. Diese Eigenschaft kann mithilfe des PowerShell-Cmdlets von einem Windows Server 2016-Cluster Knoten, der zu einem Failovercluster gehört, abgefragt werden:

  ```
  Get-Cluster | Select ClusterFunctionalLevel
  ```

  Der Wert **8** gibt an, dass der Cluster auf der Windows Server 2012 R2-Funktionsebene ausgeführt wird. Der Wert **9** gibt an, dass der Cluster auf der Windows Server 2016-Funktionsebene ausgeführt wird.

In diesem Leitfaden werden die verschiedenen Phasen des parallelen Upgradevorgangs für Cluster Betriebssysteme, Installationsschritte, Featureeinschränkungen und häufig gestellte Fragen (FAQs) beschrieben. Sie gelten auch für die folgenden Szenarien für das parallele Upgrade des Cluster Betriebssystems in Windows Server 2016:

- Hyper-V-Cluster
- Dateiserver mit horizontaler Skalierung Cluster

Das folgende Szenario wird in Windows Server 2016 nicht unterstützt:

- Paralleles Upgrade des Cluster Betriebssystems von Gast Clustern unter Verwendung einer virtuellen Festplatte (vhdx-Datei) als frei gegebener Speicher

Das parallele Upgrade des Cluster Betriebssystems wird von System Center Virtual Machine Manager (SCVMM) 2016 vollständig unterstützt. Wenn Sie SCVMM 2016 verwenden, finden Sie unter Durchführen eines parallelen Upgrades eines Hyper-V-Host Clusters auf Windows Server 2016 in VMM eine Anleitung zum Aktualisieren der Cluster und zum Automatisieren der in diesem Dokument beschriebenen Schritte.

## Voraussetzungen

Führen Sie die folgenden Anforderungen aus, bevor Sie mit dem parallelen Upgrade des Cluster Betriebssystems beginnen:

- Beginnen Sie mit einem Failovercluster, auf dem Windows Server (halbjährlicher Kanal), Windows Server 2016 oder Windows Server 2012 R2 ausgeführt wird.
- Das Upgrade eines direkte Speicherplätze Clusters auf Windows Server 1709 wird nicht unterstützt.
- Wenn es sich bei der Cluster Arbeitsauslastung um virtuelle Hyper-V-Computer oder Dateiserver mit horizontaler Skalierung handelt, kann ein Upgrade ohne Ausfallzeiten erwartet werden.
- Stellen Sie sicher, dass die Hyper-V-Knoten über CPUs verfügen, die die Adressierungs Tabelle (slat) der zweiten Ebene mithilfe einer der folgenden Methoden unterstützen:
  -Überprüfen Sie, dass Sie slat-kompatibel sind? WP8 SDK Tip 01 Artikel, in dem zwei Methoden zum überprüfen beschrieben werden, ob eine CPU SLATS unterstützt
  -Laden Sie das Coreinfo v 3,31 -Tool herunter, um zu ermitteln, ob eine CPU slat unterstützt.

## Cluster Übergangszustände beim parallelen Upgrade des Cluster Betriebssystems

In diesem Abschnitt werden die verschiedenen Übergangszustände des Windows Server 2012 R2-Clusters beschrieben, der mit dem parallelen Upgrade des Cluster Betriebssystems auf Windows Server 2016 aktualisiert wird.

Damit die clusterworkloads während des parallelen Upgradevorgangs des Cluster Betriebssystems ausgeführt werden, funktioniert das Verschieben einer Cluster Arbeitsauslastung von einem Windows Server 2012 R2-Knoten auf einen Windows Server 2016-Knoten so, als ob auf beiden Knoten das Betriebssystem Windows Server 2012 R2 ausgeführt wird. Wenn dem Cluster Windows Server 2016-Knoten hinzugefügt werden, werden diese in einem Windows Server 2012 R2-Kompatibilitätsmodus ausgeführt. Im neuen konzeptionellen Cluster Modus mit dem Namen "gemischter Betriebssystem Modus" können Knoten unterschiedlicher Versionen im gleichen Cluster vorhanden sein (siehe Abbildung 1).

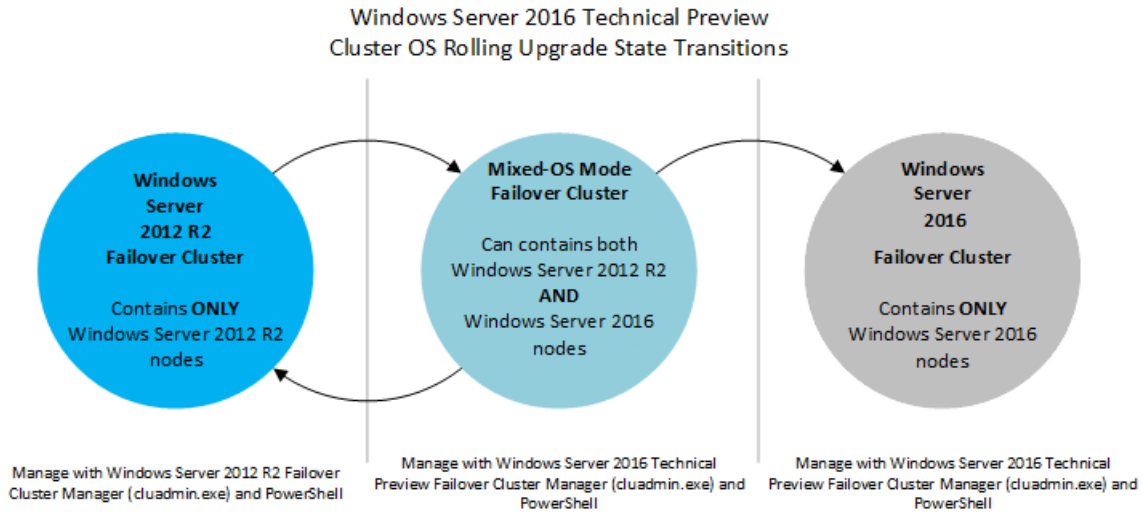



**Abbildung 1: Statusübergänge des Cluster Betriebssystems**

Ein Windows Server 2012 R2-Cluster wechselt in den Modus mit gemischtem Betriebssystem, wenn dem Cluster ein Windows Server 2016-Knoten hinzugefügt wird. Der Prozess ist vollständig umkehrbar. Windows Server 2016-Knoten können aus dem Cluster entfernt werden, und Windows Server 2012 R2-Knoten können dem Cluster in diesem Modus hinzugefügt werden. Der "Point of No Return" tritt auf, wenn das PowerShell-Cmdlet "Update-clusterfunctionallevel" auf dem Cluster ausgeführt wird. Damit dieses Cmdlet erfolgreich ausgeführt werden kann, müssen alle Knoten Windows Server 2016 sein, und alle Knoten müssen online sein.

## Übergangszustände eines Clusters mit vier Knoten beim Ausführen eines Upgrades für ein Betriebssystem

In diesem Abschnitt werden die vier verschiedenen Phasen eines Clusters mit frei gegebenem Speicher erläutert und beschrieben, dessen Knoten von Windows Server 2012 R2 auf Windows Server 2016 aktualisiert werden.

"Phase 1" ist der anfängliche Status. wir beginnen mit einem Windows Server 2012 R2-Cluster.

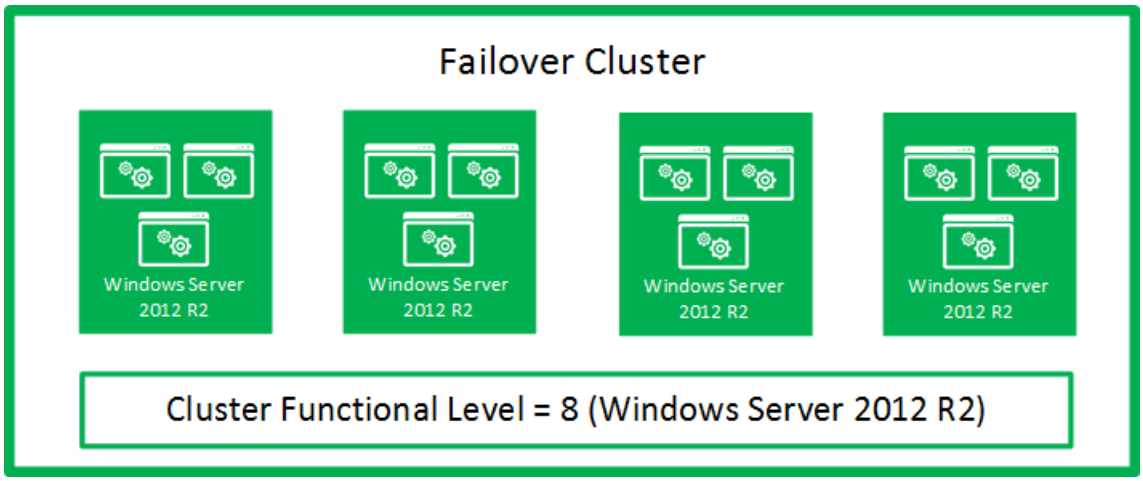



**Abbildung 2: Anfangs Status: Windows Server 2012 R2-Failovercluster (Phase 1)**

In "Phase 2" wurden zwei Knoten angehalten, entladen, entfernt, neu formatiert und mit Windows Server 2016 installiert.

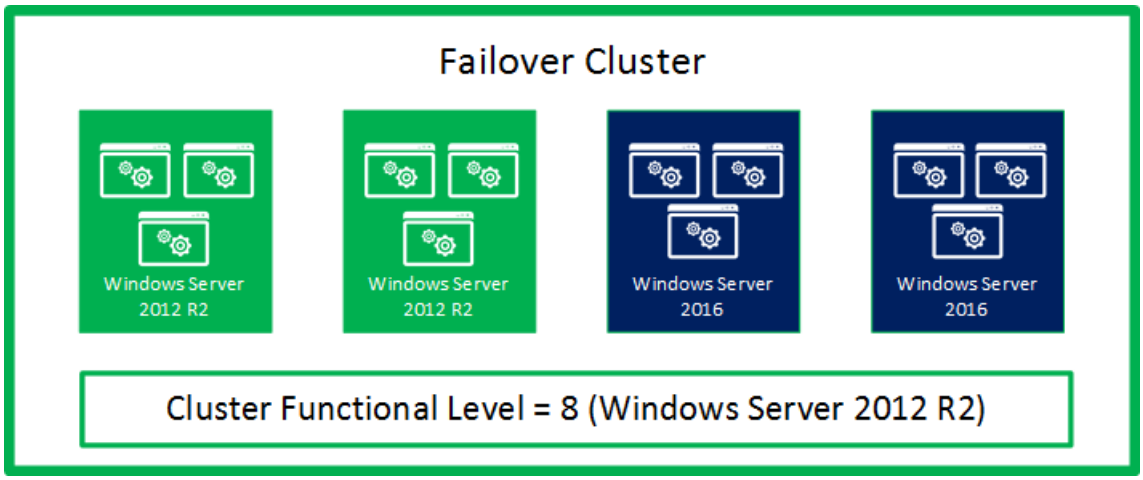



**Abbildung 3: Zwischenzustand: gemischter Betriebssystem Modus: Windows Server 2012 R2 und Windows Server 2016-Failovercluster (Phase 2)**

In "Phase 3" wurden alle Knoten im Cluster auf Windows Server 2016 aktualisiert, und der Cluster kann mit dem PowerShell-Cmdlet "Update-clusterfunctionallevel" aktualisiert werden.

> **NOTE**
> Zu diesem Zeitpunkt kann der Prozess vollständig rückgängig gemacht werden, und Windows Server 2012 R2-Knoten können diesem Cluster hinzugefügt werden.

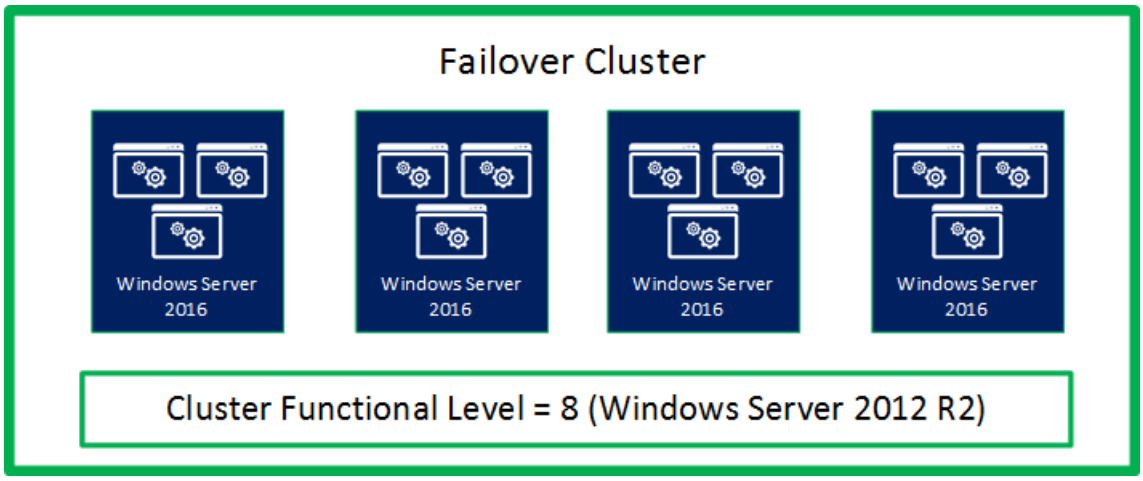



**Abbildung 4: zwischen Status: alle Knoten, die auf Windows Server 2016 aktualisiert wurden, bereit für Update-clusterfunctionallevel (Phase 3)**

Nachdem das Update-clusterfunctionallevelcmdlet ausgeführt wurde, wechselt der Cluster in "Phase 4", wo neue Windows Server 2016-Cluster Features verwendet werden können.

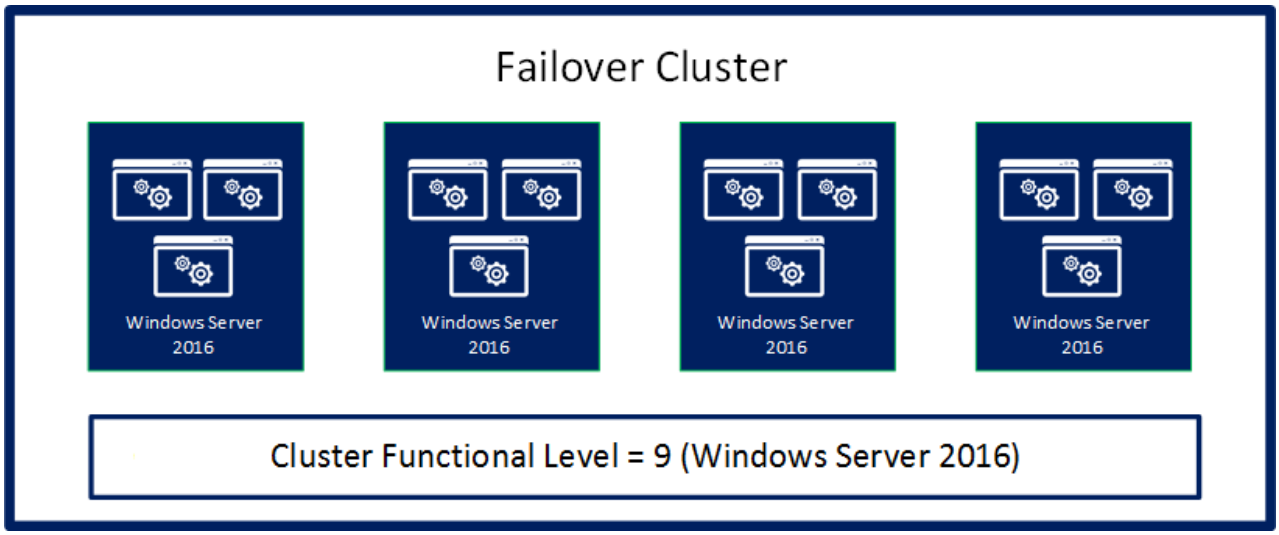



**Abbildung 5: Endzustand: Windows Server 2016-Failovercluster (Stufe 4)**

## Paralleles Upgrade des Cluster Betriebssystems

In diesem Abschnitt wird der Workflow für das parallele Upgrade des Cluster Betriebssystems beschrieben.

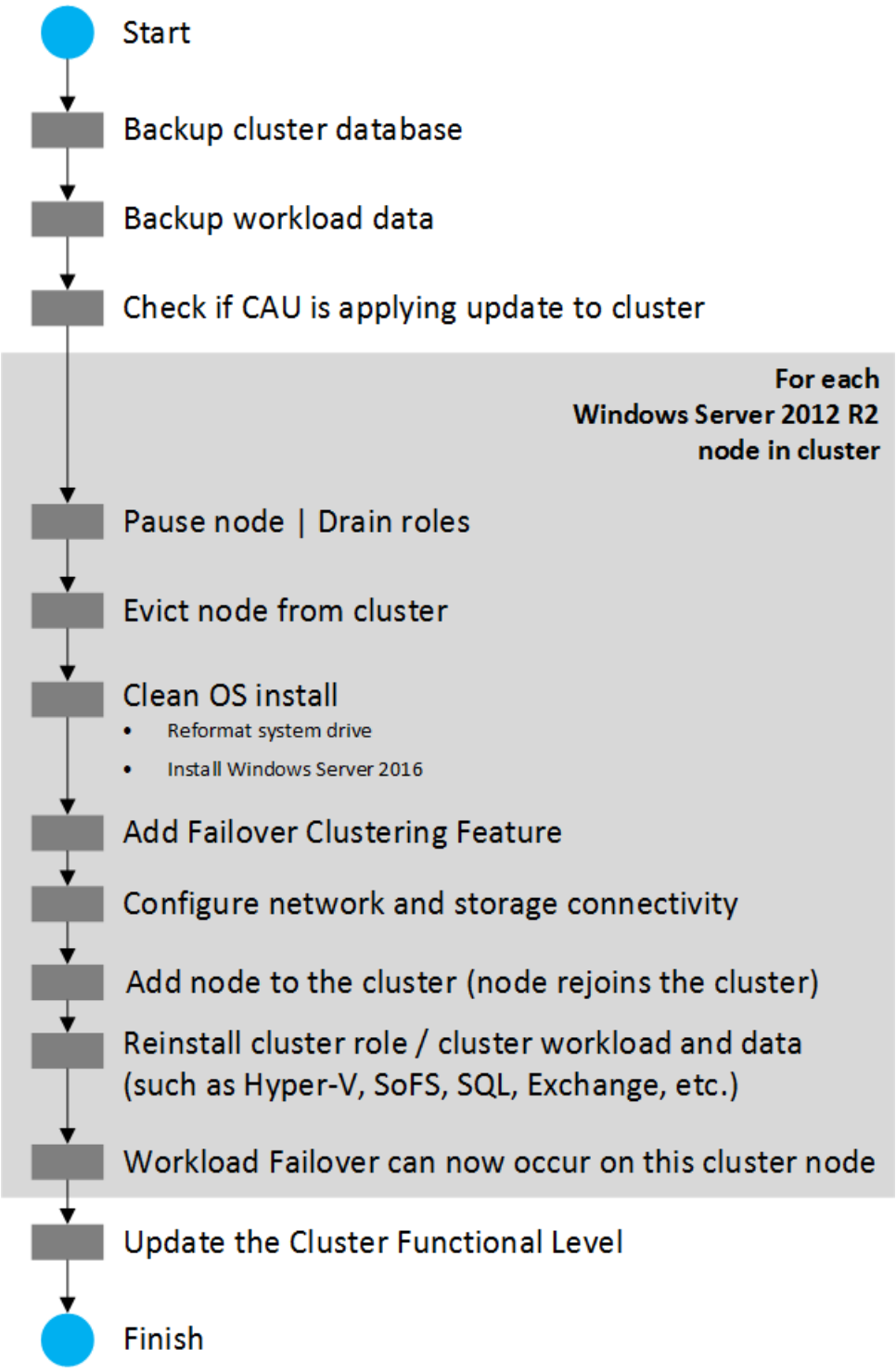



**Abbildung 6: Workflow für parallele Upgrades des Cluster Betriebssystems**

Das parallele Upgrade des Cluster Betriebssystems umfasst die folgenden Schritte:

1. Bereiten Sie den Cluster auf das Betriebssystem Upgrade wie folgt vor:

   a. Zum parallelen Upgrade des Cluster Betriebssystems muss jeweils ein Knoten aus dem Cluster entfernt werden. Überprüfen Sie, ob die Kapazität des Clusters ausreichend ist, um ha-SLAs beizubehalten, wenn einer der Cluster Knoten für ein Betriebssystem Upgrade aus dem Cluster entfernt wird. Dies bedeutet, dass Sie die Möglichkeit zum Failover von Arbeits Auslastungen auf einen anderen Knoten benötigen, wenn beim parallelen Upgrade des Cluster Betriebssystems ein Knoten aus dem Cluster entfernt wird? Verfügt der Cluster über die Kapazität zum Ausführen der erforderlichen Workloads, wenn ein Knoten für ein paralleles Upgrade des Cluster Betriebssystems aus dem Cluster entfernt wird?

   b. Überprüfen Sie für Hyper-v-Arbeits Auslastungen, ob alle Windows Server 2016 Hyper-V-Hosts über CPU-Unterstützung für die Adress Tabelle (slat) der zweiten Ebene verfügen Die Hyper-V-Rolle in

Windows Server 2016 kann nur von slat-fähigen Computern verwendet werden.

c. Überprüfen Sie, ob alle Arbeits Auslastungs Sicherungen abgeschlossen wurden, und sichern Sie den Cluster. Beendet Sicherungs Vorgänge beim Hinzufügen von Knoten zum Cluster.

d. Überprüfen Sie, ob alle Cluster Knoten online sind/Running/up mithilfe des Cmdlets `Get-ClusterNode` (siehe Abbildung 7).

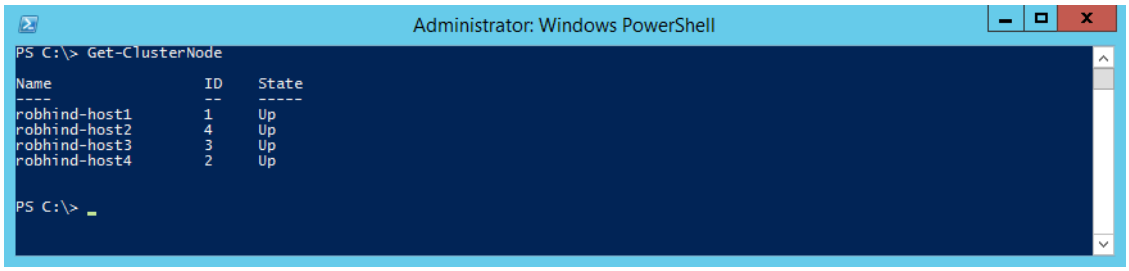



**Abbildung 7: Bestimmen des Knoten Status mithilfe des Get-clusternode-Cmdlets**

e. Wenn Sie Cluster fähige Updates (Cluster-Aware Updates, Cau) ausführen, überprüfen Sie, ob das **Cluster fähige aktualisieren** derzeit mithilfe der Benutzeroberfläche für Cluster fähiges aktualisieren oder mit dem Cmdlet " `Get-CauRun` " ausgeführt wird (siehe Abbildung 8). Verwenden Sie das Cmdlet " `Disable-CauClusterRole` " (siehe Abbildung 9), um zu verhindern, dass Knoten während des parallelen Upgradevorgangs des Cluster Betriebssystems angehalten und durch Cau entladen werden.

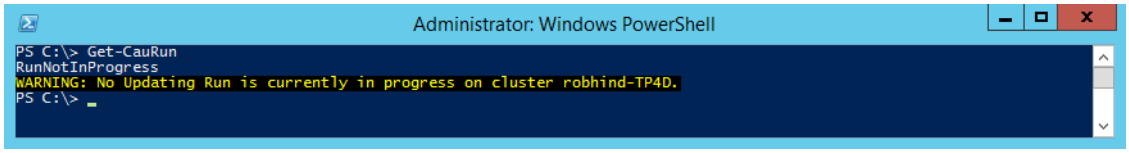



**Abbildung 8: Verwenden des `Get-CauRun` Cmdlets, um zu bestimmen, ob Cluster fähige Updates auf dem Cluster ausgeführt werden**

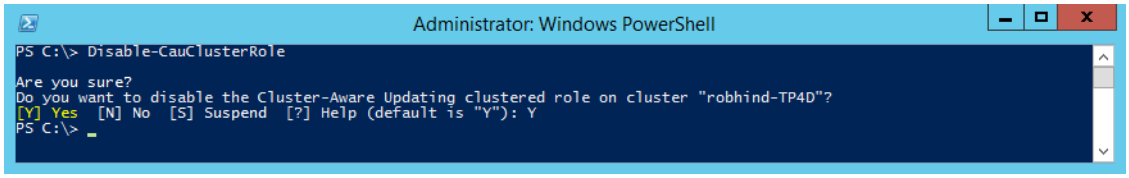



**Abbildung 9: Deaktivieren der Rolle "Cluster fähiges aktualisieren" mithilfe des `Disable-CauClusterRole` -Cmdlets**

2. Führen Sie für jeden Knoten im Cluster die folgenden Schritte aus:

a. Wählen Sie über die Benutzeroberfläche des Cluster-Managers einen Knoten aus, und verwenden Sie die **Pause Die Menüoption** zum Entfernen des Knotens (siehe Abbildung 10) oder Verwenden des `Suspend-ClusterNode` -Cmdlets (siehe Abbildung 11).

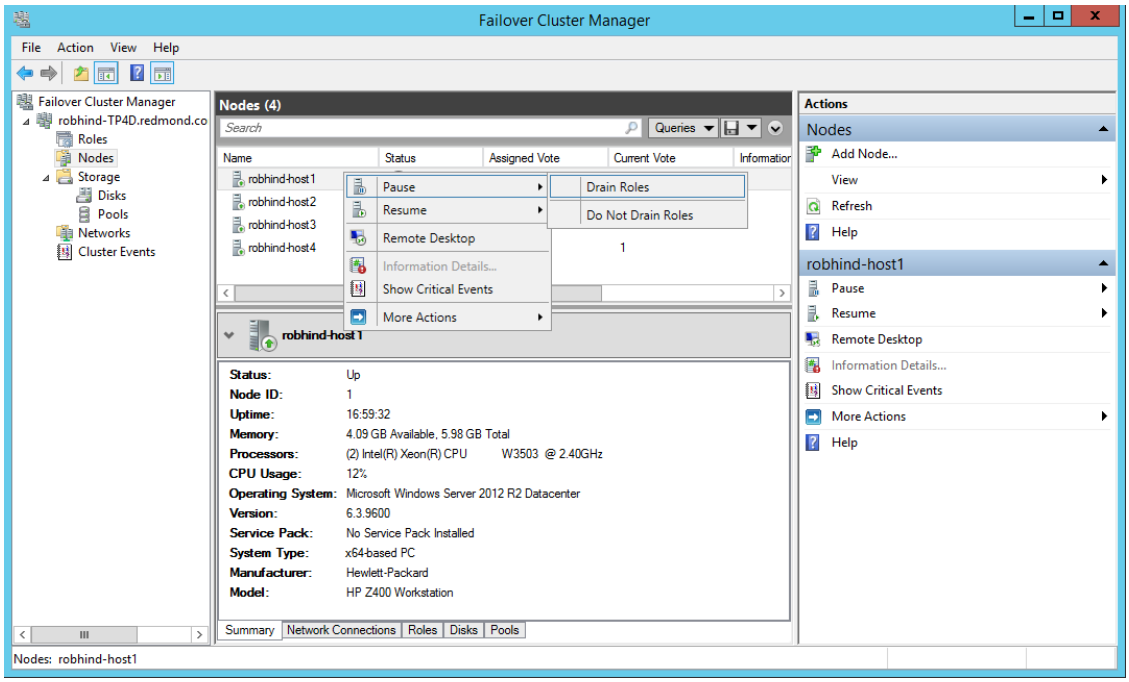



**Abbildung 10: Ableiten von Rollen von einem Knoten mithilfe von Failovercluster-Manager**

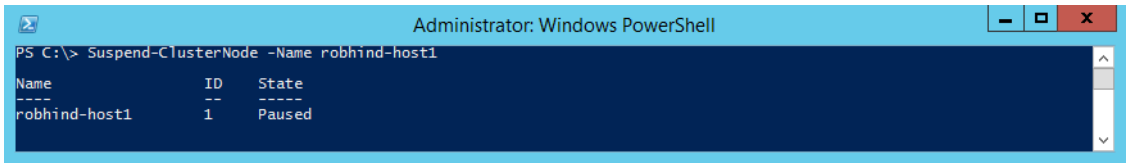



**Abbildung 11: Ableiten von Rollen von einem Knoten mithilfe des `Suspend-ClusterNode` -Cmdlets**

b. Entfernen Sie mithilfe der Benutzeroberfläche des Cluster-Managers den angehaltenen Knoten **aus dem Cluster** , oder verwenden Sie das Cmdlet " `Remove-ClusterNode` ".

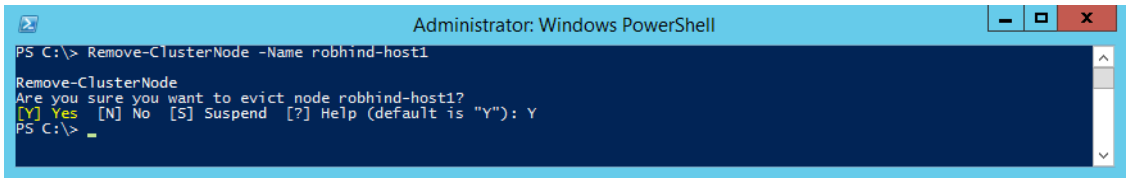



**Abbildung 12: Entfernen eines Knotens aus dem Cluster mithilfe `Remove-ClusterNode` Cmdlets**

c. Formatieren Sie das Systemlaufwerk neu, und führen Sie eine "Neuinstallation des Betriebssystems" von Windows Server 2016 auf dem Knoten mithilfe der Option **Benutzer definiert: nur Windows installieren (erweitert)** (siehe Abbildung 13) in der Datei "Setup. exe" aus. Wählen Sie die Option **Upgrade: Windows installieren und Dateien beibehalten, Einstellungen und Anwendungen** nicht aus, da das parallele Upgrade des Cluster Betriebssystems keine direkte Aktualisierung fördert.

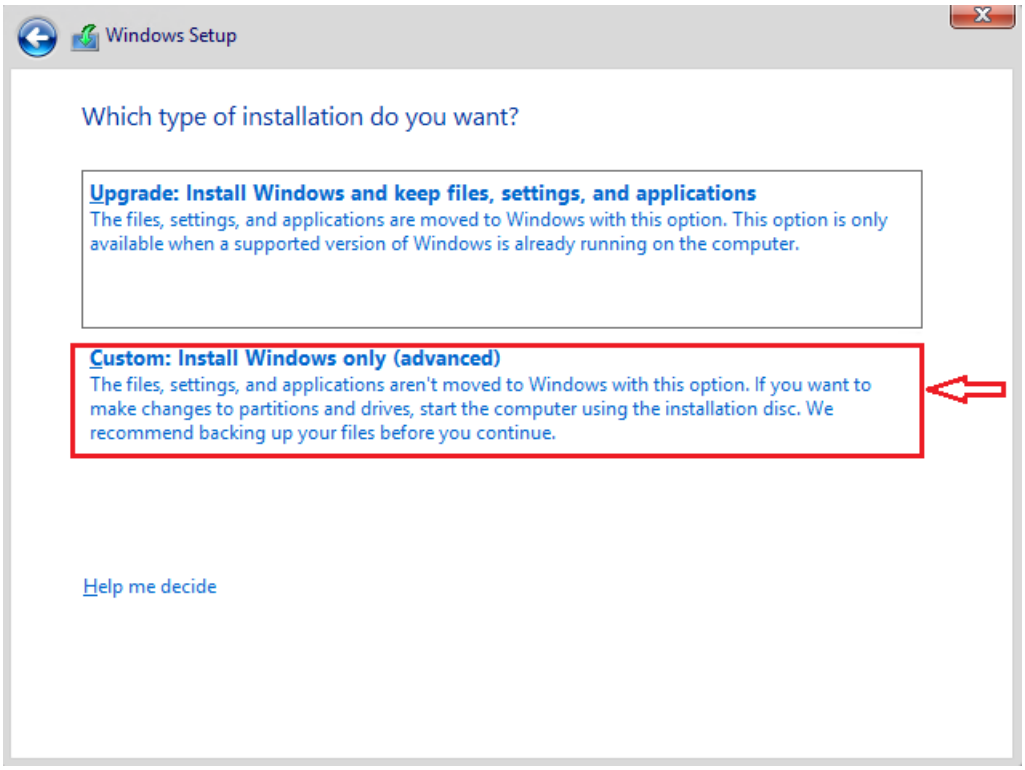



**Abbildung 13: verfügbare Installationsoptionen für Windows Server 2016**

d. Fügen Sie den Knoten der entsprechenden Active Directory Domäne hinzu.

e. Fügen Sie die entsprechenden Benutzer der Gruppe "Administratoren" hinzu.

f. Installieren Sie mit dem PowerShell-Cmdlet "Server-Manager UI" oder "Install-Windows Feature" alle benötigten Server Rollen, z. b. Hyper-V.

```
Install-WindowsFeature -Name Hyper-V
```

g. Installieren Sie das Failoverclustering-Feature mithilfe der Server-Manager-Benutzeroberfläche oder des PowerShell-Cmdlets install-Windows Feature.

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

h. Installieren Sie alle zusätzlichen Funktionen, die von ihren clusterworkloads benötigt werden.

i. Überprüfen Sie die Netzwerk-und Speicher Verbindungseinstellungen mithilfe der Failovercluster-Manager Benutzeroberfläche.

j. Wenn die Windows-Firewall verwendet wird, überprüfen Sie, ob die Firewalleinstellungen für den Cluster korrekt sind. Beispielsweise kann für Cluster fähiges aktualisieren (Cluster-Aware Update, Cau) Cluster eine Firewallkonfiguration erforderlich sein.

k. Verwenden Sie für Hyper-v-Workloads die Hyper-v-Manager-Benutzeroberfläche, um das Dialogfeld "Virtual Switch Manager" zu öffnen (siehe Abbildung 14).

   Überprüfen Sie, ob die Namen der verwendeten virtuellen Switches für alle Hyper-V-Host Knoten im Cluster identisch sind.

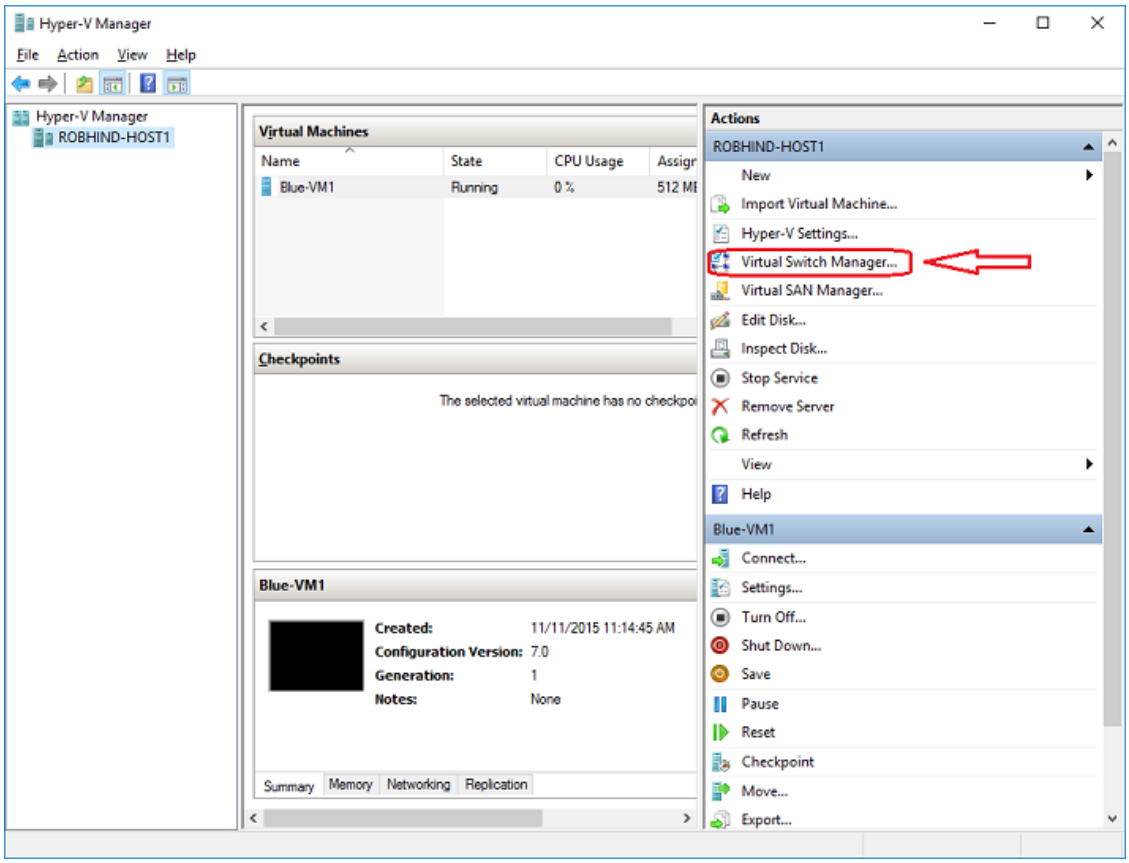



Abbildung 14: Manager für virtuelle Switches

l. Verwenden Sie auf einem Windows Server 2016-Knoten (verwenden Sie keinen Windows Server 2012 R2-Knoten) die Failovercluster-Manager (siehe Abbildung 15), um eine Verbindung mit dem Cluster herzustellen.

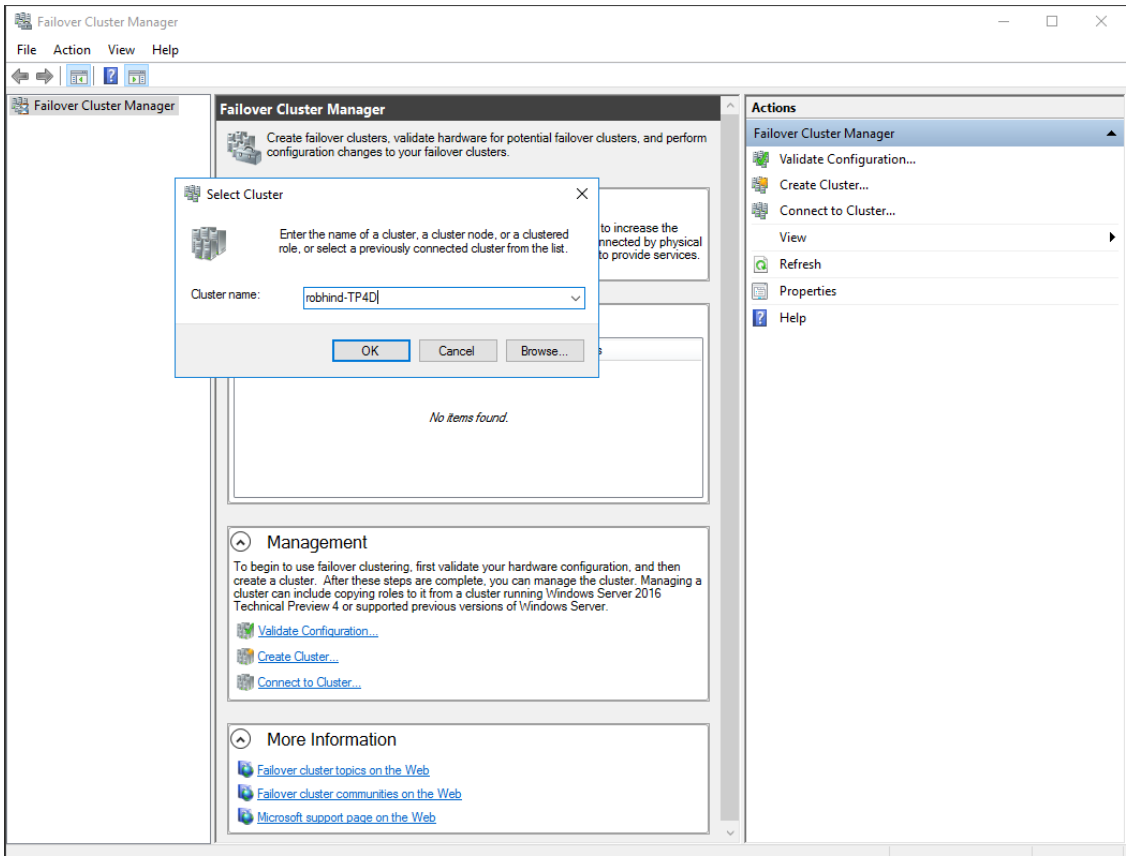



Abbildung 15: Hinzufügen eines Knotens zum Cluster mithilfe von Failovercluster-Manager

m. Verwenden Sie entweder die Failovercluster-Manager-Benutzeroberfläche oder das `Add-ClusterNode`

-Cmdlet (siehe Abbildung 16), um den Knoten zum Cluster hinzuzufügen.

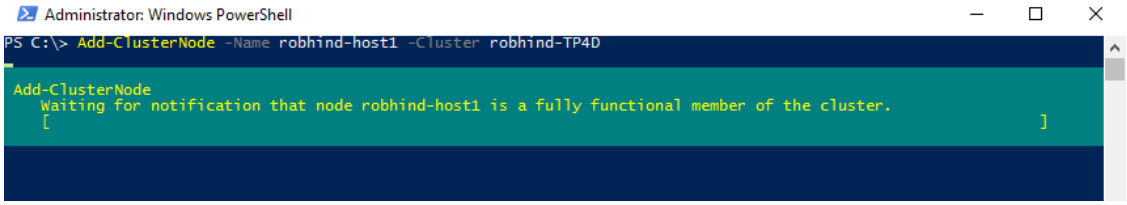



**Abbildung 16: Hinzufügen eines Knotens zum Cluster mithilfe `Add-ClusterNode` Cmdlets**

> **NOTE**
>
> Wenn der erste Windows Server 2016-Knoten dem Cluster Beitritt, wechselt der Cluster in den Modus "gemischter Betriebssystem", und die Hauptressourcen des Clusters werden auf den Knoten "Windows Server 2016" verschoben. Bei einem Cluster mit gemischtem Betriebssystem handelt es sich um einen voll funktionsfähigen Cluster, in dem die neuen Knoten in einem Kompatibilitätsmodus mit den alten Knoten ausgeführt werden. Der Modus "gemischter Betriebssystem" ist ein transitiver Modus für den Cluster. Es ist nicht als permanent gedacht, und die Kunden möchten innerhalb von vier Wochen alle Knoten Ihres Clusters aktualisieren.

n. Nachdem der Windows Server 2016-Knoten dem Cluster erfolgreich hinzugefügt wurde, können Sie (optional) einen Teil der Cluster Arbeitsauslastung auf den neu hinzugefügten Knoten verschieben, um die Arbeitsauslastung wie folgt auf den Cluster umzuverteilen:

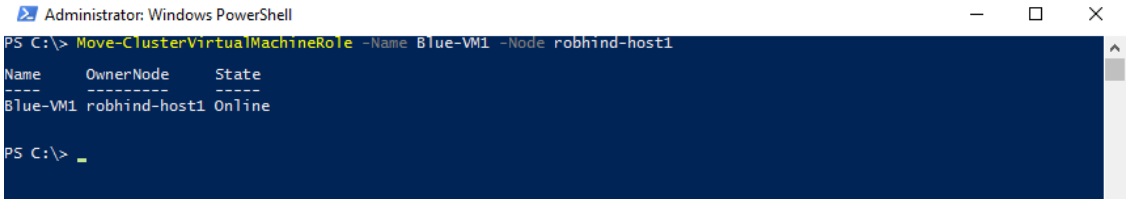



**Abbildung 17: Verschieben einer Cluster Arbeitsauslastung (Cluster-VM-Rolle) mithilfe `Move-ClusterVirtualMachineRole` Cmdlets**

a. Verwenden Sie **Livemigration** aus der Failovercluster-Manager für virtuelle Computer oder das `Move-ClusterVirtualMachineRole` -Cmdlet (siehe Abbildung 17), um eine Live Migration der virtuellen Computer durchzuführen.

```
Move-ClusterVirtualMachineRole -Name VM1 -Node robhind-host3
```

b. Verwenden Sie **Move** from the Failovercluster-Manager oder das `Move-ClusterGroup` -Cmdlet für andere clusterworkloads.

3. Gehen Sie wie folgt vor, wenn jeder Knoten auf Windows Server 2016 aktualisiert und wieder dem Cluster hinzugefügt wurde oder wenn verbleibende Windows Server 2012 R2-Knoten entfernt wurden:

> **IMPORTANT**
>
> - Nachdem Sie die Cluster Funktionsebene aktualisiert haben, können Sie nicht mehr zur Windows Server 2012 R2-Funktionsebene zurückkehren und Windows Server 2012 R2-Knoten können dem Cluster nicht mehr hinzugefügt werden.
> - Bis zum Ausführen des Cmdlets " `Update-ClusterFunctionalLevel` " ist der Prozess vollständig umkehrbar, und Windows Server 2012 R2-Knoten können diesem Cluster hinzugefügt werden, und Windows Server 2016-Knoten können entfernt werden.
> - Nachdem das Cmdlet " `Update-ClusterFunctionalLevel` " ausgeführt wurde, sind neue Features verfügbar.

a. Überprüfen Sie mithilfe der Failovercluster-Manager-Benutzeroberfläche oder des `Get-ClusterGroup` -Cmdlets, ob alle Cluster Rollen erwartungsgemäß auf dem Cluster ausgeführt werden. Im folgenden Beispiel wird der verfügbare Speicher nicht verwendet. stattdessen wird CSV verwendet. Daher zeigt der verfügbare Speicher einen **Offline** Status an (siehe Abbildung 18).

```
Administrator: Windows PowerShell
PS C:\> Get-ClusterGroup

Name               OwnerNode     State
----               ---------     -----
Available Storage  robhind-host2 Offline
Blue-VM1           robhind-host1 Online
Blue-VM2           robhind-host2 Online
Blue-VM3           robhind-host3 Online
Blue-VM4           robhind-host4 Online
Cluster Group      robhind-host1 Online

PS C:\>
```

**Abbildung 18: überprüfen, ob alle Clustergruppen (Cluster Rollen) mithilfe des `Get-ClusterGroup` -Cmdlets ausgeführt werden**

b. Überprüfen Sie, ob alle Cluster Knoten online sind und mit dem `Get-ClusterNode` -Cmdlet ausgeführt werden.

c. Führen Sie das `Update-ClusterFunctionalLevel` Cmdlet aus. es sollten keine Fehler zurückgegeben werden (siehe Abbildung 19).

```
Administrator: Windows PowerShell
PS C:\> Get-Cluster | Select ClusterFunctionalLevel

ClusterFunctionalLevel
----------------------
                     8

PS C:\> Update-ClusterFunctionalLevel

Updating the functional level for cluster robhind-TP4D.
Warning: You cannot undo this operation. Do you want to continue?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y

Name
----
robhind-TP4D

PS C:\> Get-Cluster | Select ClusterFunctionalLevel

ClusterFunctionalLevel
----------------------
                     9

PS C:\>
```

**Abbildung 19: Aktualisieren der Funktionsebene eines Clusters mithilfe von PowerShell**

d. Nachdem das Cmdlet " `Update-ClusterFunctionalLevel` " ausgeführt wurde, sind neue Features verfügbar.

4. Windows Server 2016-fortsetzen normaler Cluster Aktualisierungen und-Sicherungen:

a. Wenn Sie zuvor Cau ausgeführt haben, starten Sie es mithilfe der Cau-Benutzeroberfläche neu, oder verwenden Sie das Cmdlet " `Enable-CauClusterRole` " (siehe Abbildung 20).

```
Administrator: Windows PowerShell
PS C:\> Enable-CauClusterRole

Are you sure?
Do you want to enable the Cluster-Aware Updating clustered role on cluster "robhind-TP4D"?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\>
```

**Abbildung 20: Aktivieren der Rolle "Cluster fähige Updates" mithilfe des `Enable-CauClusterRole` -Cmdlets**

b. Fortsetzen von Sicherungs Vorgängen.

5. Aktivieren und verwenden Sie die Windows Server 2016-Features auf Hyper-V-Virtual Machines.

   a. Nachdem der Cluster auf die Funktionsebene von Windows Server 2016 aktualisiert wurde, verfügen viele Workloads wie Hyper-V-VMS über neue Funktionen. Eine Liste der neuen Hyper-V-Funktionen. siehe migrieren und Aktualisieren virtueller Computer

   b. Verwenden Sie auf jedem Hyper-v-Host Knoten im Cluster das Cmdlet " `Get-VMHostSupportedVersion` ", um die vom Host unterstützten Hyper-v-VM-Konfigurations Versionen anzuzeigen.

```
Administrator: Windows PowerShell (2)
PS C:\WINDOWS\system32> Get-VMHostSupportedVersion

Name                                                Version IsDefault
----                                                ------- ---------
Microsoft Windows 8.1/Server 2012 R2                5.0     False
Microsoft Windows 10/Server 2016 Technical Preview 3 6.2     False
Microsoft Windows Server 2016 Technical Preview 4   7.0     False
Microsoft Windows Server 2016 Technical Preview 5   7.1     True
Prerelease                                          254.0   False
Experimental                                        255.0   False
```

   **Abbildung 21: Anzeigen der vom Host unterstützten Hyper-V-VM-Konfigurations Versionen**

   c. Auf jedem Knoten des Hyper-v-Hosts im Cluster kann ein Upgrade für Hyper-v-VM-Konfigurations Versionen durchgeführt werden, indem ein kurzes Wartungsfenster für Benutzer geplant wird, um die virtuellen Computer zu sichern, zu deaktivieren und das Cmdlet " `Update-VMVersion` " ausgeführt wird (siehe Abbildung 22). Dadurch wird die Version des virtuellen Computers aktualisiert, und neue Hyper-v-Features werden aktiviert, sodass keine weiteren Updates von Hyper-v-Integrations Komponenten (IC) erforderlich sind. Dieses Cmdlet kann über den Hyper-V-Knoten ausgeführt werden, der als Host für den virtuellen Computer dient, oder mithilfe des `-ComputerName` -Parameters können Sie die VM-Version Remote aktualisieren. In diesem Beispiel aktualisieren wir die Konfigurations Version von VM1 von 5,0 auf 7,0, um von vielen neuen Hyper-V-Features zu profitieren, die dieser VM-Konfigurations Version zugeordnet sind, z. b. Produktions Prüfpunkte (Anwendungs konsistente Sicherungen) und binäre VM-Konfigurationsdatei.

```
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:\> _
```

   **Abbildung 22: Aktualisieren einer VM-Version mithilfe des PowerShell-Cmdlets "Update-VMVersion"**

6. Speicherpools können mithilfe des PowerShell-Cmdlets " Update-storagepool " aktualisiert werden. Dies ist ein Online Vorgang.

Obwohl wir auf Szenarien für die Private Cloud abzielen, insbesondere Hyper-V-und Datei Server Cluster mit horizontaler Skalierung, die ohne Ausfallzeiten aktualisiert werden können, kann der parallele Upgradeprozess des Cluster Betriebssystems für jede beliebige Cluster Rolle verwendet werden.

## Einschränkungen/Einschränkungen

- Diese Funktion funktioniert nur für Windows Server 2012 R2-und Windows Server 2016-Versionen. Diese Funktion kann keine Upgrades früherer Versionen von Windows Server wie Windows Server 2008, Windows Server 2008 R2 oder Windows Server 2012 auf Windows Server 2016 durchführen.
- Jeder Knoten von Windows Server 2016 sollte neu formatiert bzw. neu installiert werden. Der Installationstyp "direkt" oder "Upgrade" wird nicht empfohlen.
- Ein Windows Server 2016-Knoten muss zum Hinzufügen von Windows Server 2016-Knoten zum Cluster verwendet werden.
- Wenn Sie einen Cluster im gemischten Betriebssystem Modus verwalten, führen Sie die Verwaltungsaufgaben immer über einen komplexer Darstellung-Knoten aus, auf dem Windows Server 2016 ausgeführt wird. Windows Server 2012 R2-downlevelknoten können keine Benutzeroberflächen-oder Verwaltungs Tools für Windows Server 2016 verwenden.
- Wir empfehlen Kunden, den clusterupgradeprozess schnell durchzuführen, da einige Cluster Features nicht für den Modus mit gemischtem Betriebssystem optimiert sind.
- Vermeiden Sie das Erstellen oder Ändern der Größe von Speicher auf Windows Server 2016-Knoten, während der Cluster im Modus mit gemischtem Betriebssystem ausgeführt wird, da die Inkompatibilitäten bei einem Failover von einem Windows Server 2016-Knoten auf Windows Server 2012 R2-Knoten mit einer untergeordneten

## Häufig gestellte Fragen

**Wie lange kann der Failovercluster im gemischten Betriebssystem Modus ausgeführt werden?**
Wir empfehlen Kunden, das Upgrade innerhalb von vier Wochen abzuschließen. Es gibt viele Optimierungen in Windows Server 2016. Wir haben Hyper-V-und Datei Server Cluster mit horizontaler Skalierung ohne Ausfallzeiten in weniger als vier Stunden aktualisiert.

**Wird diese Funktion auf Windows Server 2012, Windows Server 2008 R2 oder Windows Server 2008 zurück portieren?**
Es ist nicht geplant, diese Funktion auf vorherige Versionen zurück zu portieren. Das parallele Upgrade des Cluster Betriebssystems ist unsere Vision für das Upgrade von Windows Server 2012 R2-Clustern auf Windows Server 2016 und höher.

**Muss für den Windows Server 2012 R2-Cluster alle Software Updates installiert sein, bevor der parallele Upgradeprozess des Cluster Betriebssystems gestartet wird?**
Ja, bevor Sie mit dem parallelen Upgrade des Cluster Betriebssystems beginnen, überprüfen Sie, ob alle Cluster Knoten mit den neuesten Software Updates aktualisiert wurden.

**Kann ich das `Update-ClusterFunctionalLevel` -Cmdlet ausführen, während Knoten deaktiviert oder angehalten werden?**
Nein. Alle Cluster Knoten müssen sich in der aktiven Mitgliedschaft befinden, damit das `Update-ClusterFunctionalLevel` -Cmdlet funktioniert.

**Funktioniert das parallele Upgrade des Cluster Betriebssystems für jede Cluster Arbeitsauslastung? Funktioniert es für SQL Server?**
Ja, das parallele Upgrade des Cluster Betriebssystems funktioniert für jede Cluster Arbeitsauslastung. Allerdings ist es für Hyper-V-und Datei Server Cluster mit horizontaler Skalierung nur zu Ausfallzeiten. Bei den meisten anderen Arbeits Auslastungen treten bei einem Failover einige Ausfallzeiten (in der Regel einige Minuten) auf, und ein Failover muss mindestens einmal während des parallelen Upgradevorgangs des Cluster Betriebssystems ausgeführt werden.

**Kann ich diesen Prozess mithilfe von PowerShell automatisieren?**
Ja, wir haben das parallele Upgrade für Cluster Betriebssysteme entworfen, um Sie mithilfe von PowerShell zu automatisieren.

**Kann ich bei einem großen Cluster mit zusätzlicher Arbeitsauslastung und Failoverkapazität mehrere Knoten gleichzeitig aktualisieren?**
Ja. Wenn ein Knoten aus dem Cluster entfernt wird, um das Betriebssystem zu aktualisieren, verfügt der Cluster über einen geringeren Knoten für das Failover und verfügt daher über eine reduzierte Failoverkapazität. Bei großen Clustern mit ausreichender Arbeitsauslastung und Failoverkapazität können mehrere Knoten gleichzeitig aktualisiert werden. Sie können dem Cluster vorübergehend Cluster Knoten hinzufügen, um beim parallelen Upgradeprozess des Cluster Betriebssystems eine verbesserte Arbeitsauslastung und Failoverkapazität bereitzustellen.

**Was geschieht, wenn ich nach dem erfolgreichen Ausführen `Update-ClusterFunctionalLevel` ein Problem in meinem Cluster entdeckt?**
Wenn Sie die Cluster Datenbank vor dem Ausführen von `Update-ClusterFunctionalLevel` mit einer Sicherung des System Status gesichert haben, können Sie eine autorisierende Wiederherstellung auf einem Windows Server 2012 R2-Cluster Knoten durchführen und die ursprüngliche Cluster Datenbank und-Konfiguration wiederherstellen.

**Kann ich für jeden Knoten ein direktes Upgrade verwenden, anstatt die Clean-OS-Installation durch Neuformatierung des System Laufwerks zu verwenden?**
Wir empfehlen nicht die Verwendung eines direkten Upgrades von Windows Server, aber wir wissen, dass es in einigen Fällen funktioniert, in denen Standardtreiber verwendet werden. Lesen Sie sorgfältig alle Warnmeldungen, die während der direkten Aktualisierung eines Cluster Knotens angezeigt werden.

**Wenn ich die Hyper-v-Replikation für eine Hyper-v-VM auf meinem Hyper-v-Cluster verwende, bleibt die Replikation während und nach dem parallelen Upgradeprozess des Cluster Betriebssystems erhalten?**
Ja, das Hyper-V-Replikat bleibt während und nach dem parallelen Upgrade des Cluster Betriebssystems intakt.

**Kann ich System Center 2016 Virtual Machine Manager (SCVMM) verwenden, um den parallelen Upgradeprozess für Cluster Betriebssysteme zu automatisieren?**
Ja, Sie können das parallele Upgradeverfahren für Cluster Betriebssysteme mithilfe von VMM in System Center 2016 automatisieren.

## Siehe auch

- Anmerkungen zu dieser Version: wichtige Probleme in Windows Server 2016
- Neuerungen in Windows Server 2016
- Neues beim Failoverclustering unter Windows Server

# Aktualisieren von Failoverclustern auf derselben Hardware

09.04.2020 • 10 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

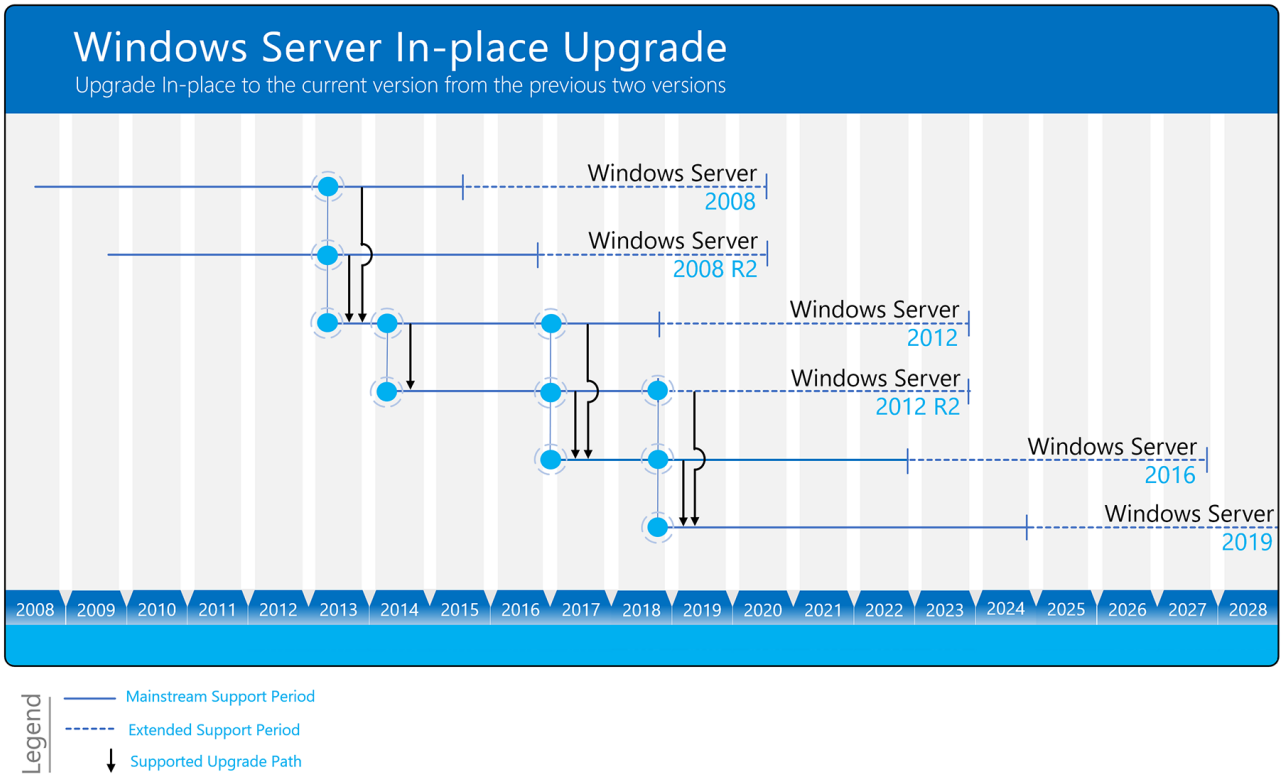
Ein Failovercluster besteht aus einer Gruppe von unabhängigen Computern, die miteinander interagieren und somit die Verfügbarkeit von Anwendungen und Diensten erhöhen. Die geclusterten Server ("Knoten") sind physisch über Kabel sowie durch Software verbunden. Wenn auf einem der Clusterknoten ein Fehler auftritt, werden seine Aufgaben sofort auf einen anderen Knoten übertragen. Dies wird als Failover bezeichnet. So ergeben sich für die Benutzer nur minimale Unterbrechungen des Betriebs.

In dieser Anleitung werden die Schritte zum Aktualisieren der Cluster Knoten auf Windows Server 2019 oder Windows Server 2016 von einer früheren Version mit derselben Hardware beschrieben.

## Übersicht

Das Upgrade des Betriebssystems auf einem vorhandenen Failovercluster wird nur unterstützt, wenn Sie von Windows Server 2016 zu Windows 2019 wechseln. Wenn auf dem Failovercluster eine frühere Version ausgeführt wird, wie z. b. Windows Server 2012 R2 und früher, können bei der Ausführung des Cluster Diensts keine Verbindungsknoten miteinander verknüpft werden. Wenn Sie dieselbe Hardware verwenden, können Sie Schritte ausführen, um Sie auf die neuere Version zu übernehmen.

Lesen Sie vor dem Upgrade des Failoverclusters den Windows Server-upgradeinhalt. Wenn Sie einen Windows-Server direkt aktualisieren, wechseln Sie von einer vorhandenen Betriebssystemversion zu einer neueren Version, während Sie auf derselben Hardware bleiben. Für Windows Server kann ein direktes Upgrade von mindestens einem ausgeführt werden, manchmal aber auch für zwei Versionen. Beispielsweise können Windows Server 2012 R2 und Windows Server 2016 direkt auf Windows Server 2019 aktualisiert werden. Beachten Sie auch, dass der Clustermigrations-Assistent verwendet werden kann, jedoch nur bis zu zwei Versionen wieder unterstützt werden. Die folgende Grafik zeigt die Upgradepfade für Windows Server. Nach unten zeigende Pfeile stellen den unterstützten Upgradepfad dar, der von früheren Versionen bis zu Windows Server 2019 wechselt.



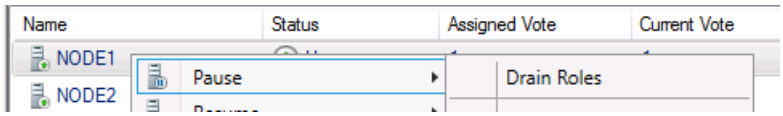

Die folgenden Schritte sind ein Beispiel für den Wechsel von einem Windows Server 2012-Failoverclusterserver zu Windows Server 2019 unter Verwendung derselben Hardware.

Stellen Sie vor dem Start eines Upgrades sicher, dass eine aktuelle Sicherung, einschließlich des Systemstatus, abgeschlossen ist. Stellen Sie außerdem sicher, dass alle Treiber und Firmware auf die zertifizierten Stufen des Betriebssystems aktualisiert wurden, das Sie verwenden werden. Diese beiden Notizen werden hier nicht behandelt.

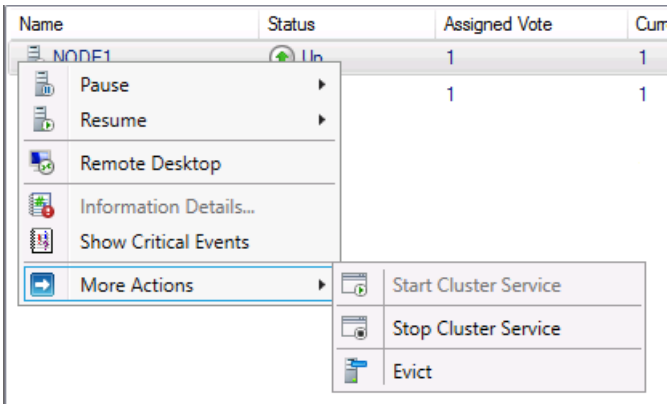
Im folgenden Beispiel ist der Name des Failoverclusters Cluster, und die Knoten Namen lauten Node1 und Node2.

## Schritt 1: Entfernen des ersten Knotens und Aktualisieren auf Windows Server 2016

1. Entfernen Sie in Failovercluster-Manager alle Ressourcen von Node1 zu Node2, indem Sie mit der rechten Maustaste auf den Knoten klicken und **Rollen**anhalten und **Entfernen auswählen.** Alternativ können Sie den PowerShell -Befehl Suspend-clusternodeverwenden.



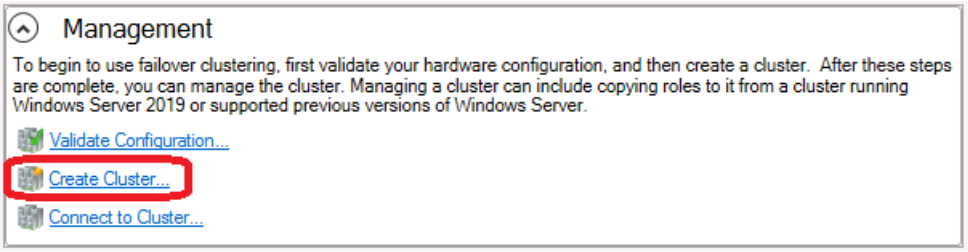

2. Entfernen Sie Node1 aus dem Cluster, indem Sie mit der rechten Maustaste auf den Knoten klicken **und Weitere Aktionen** auswählen und entfernen. Alternativ können Sie den PowerShell -Befehl Remove-clusternodeverwenden.



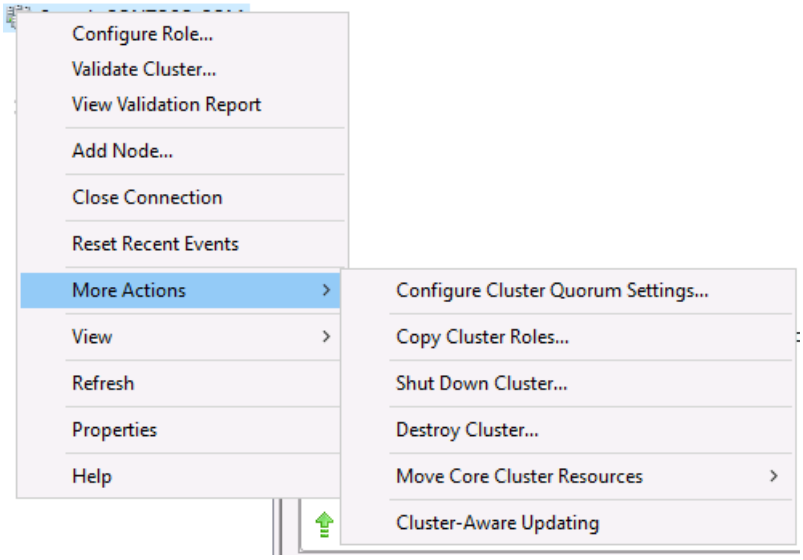

3. Trennen Sie als Vorsichtsmaßnahme Node1 vom verwendeten Speicher. In einigen Fällen genügt das Trennen der Speicher Kabel vom Computer. Wenden Sie sich bei Bedarf an Ihren Speicher Anbieter. Abhängig von Ihrem Speicher ist dies möglicherweise nicht erforderlich.

4. Erstellen Sie Node1 mit Windows Server 2016 neu. Stellen Sie sicher, dass Sie alle erforderlichen Rollen, Features, Treiber und Sicherheitsupdates hinzugefügt haben.

5. Erstellen Sie einen neuen Cluster mit dem Namen CLUSTER1 mit Node1. Öffnen Sie Failovercluster-Manager, und wählen Sie im Bereich **Verwaltung** die Option **Cluster erstellen** aus, und befolgen Sie die Anweisungen im Assistenten.




6. Nachdem der Cluster erstellt wurde, müssen die Rollen vom ursprünglichen Cluster zu diesem neuen Cluster migriert werden. Klicken Sie im neuen Cluster mit der rechten Maustaste auf den Cluster Namen (CLUSTER1), und wählen Sie **Weitere Aktionen** und **Cluster Rollen kopieren** aus. Befolgen Sie die Anweisungen im Assistenten, um die Rollen zu migrieren.




7. Nachdem alle Ressourcen migriert wurden, schalten Sie Node2 (ursprünglicher Cluster) ein, und trennen Sie den Speicher so, dass keine Störungen auftreten. Verbinden Sie den Speicher mit Node1. Sobald die Verbindung hergestellt ist, schalten Sie alle Ressourcen Online, und stellen Sie sicher, dass Sie wie folgt funktionieren.

## Schritt 2: Neuerstellen des zweiten Knotens in Windows Server 2019

Nachdem Sie überprüft haben, dass alles wie erforderlich funktioniert, kann Node2 auf Windows Server 2019 neu erstellt und dem Cluster hinzugefügt werden.

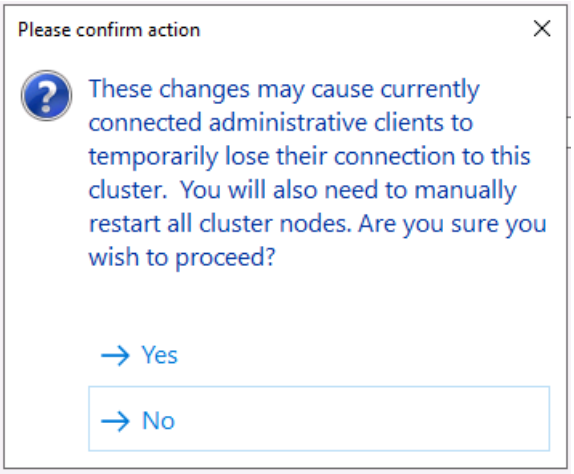
1. Führen Sie eine Neuinstallation von Windows Server 2019 auf Node2 aus. Stellen Sie sicher, dass Sie alle erforderlichen Rollen, Features, Treiber und Sicherheitsupdates hinzugefügt haben.

2. Nachdem der ursprüngliche Cluster (Cluster) nicht mehr vorhanden ist, können Sie den neuen Cluster Namen als CLUSTER1 belassen oder zum ursprünglichen Namen zurückkehren. Wenn Sie zum ursprünglichen Namen zurückkehren möchten, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf Node1 in Failovercluster-Manager klicken Sie mit der rechten Maustaste auf den Namen des Clusters (CLUSTER1), und wählen Sie **Eigenschaften**aus.

   b. Benennen Sie den Cluster auf der Registerkarte **Allgemein** in Cluster um.

   c. Wenn Sie "OK" oder "anwenden" auswählen, wird das folgende Dialogfeld angezeigt.




   d. Der Cluster Dienst wird beendet und muss erneut gestartet werden, damit die Umbenennung beendet wird.

3. Öffnen Sie auf Node1 Failovercluster-Manager. Klicken Sie mit der rechten Maustaste auf **Knoten** , und wählen Sie **Knoten hinzufügen** Durchlaufen Sie den Assistenten, indem Sie Node2 zum Cluster hinzufügen.

4. Fügen Sie den Speicher an Node2 an. Dies kann das erneute Verbinden der Speicher Kabel einschließen.

5. Entfernen Sie alle Ressourcen von Node1 zu Node2, indem Sie mit der rechten Maustaste auf den Knoten klicken und **Rollen**anhalten und **Entfernen auswählen.** Alternativ können Sie den PowerShell -Befehl Suspend-clusternodeverwenden. Stellen Sie sicher, dass alle Ressourcen online sind und wie Sie funktionieren.

## Schritt 3: Erneutes Erstellen des ersten Knotens in Windows Server 2019

1. Entfernen Sie Node1 aus dem Cluster, und trennen Sie die Verbindung zwischen dem Speicher und dem Knoten.

2. Erneutes Erstellen oder Aktualisieren von Node1 auf Windows Server 2019. Stellen Sie sicher, dass Sie alle erforderlichen Rollen, Features, Treiber und Sicherheitsupdates hinzugefügt haben.

3. Fügen Sie den Speicher erneut an, und fügen Sie Node1 wieder zum Cluster hinzu.

4. Verschieben Sie alle Ressourcen in Node1, und stellen Sie sicher, dass Sie online geschaltet werden und bei Bedarf funktionieren.

5. Die aktuelle Cluster Funktionsebene bleibt bei Windows 2016. Aktualisieren Sie die Funktionsebene mit dem PowerShell -Befehl Update-clusterfunctionallevelauf Windows 2019.

Sie führen jetzt mit einem voll funktionsfähigen Windows Server 2019-Failovercluster aus.

## Weitere Anmerkungen

- Wie bereits erläutert, ist die Trennung des Speichers möglicherweise nicht erforderlich. Wir möchten uns in unserer Dokumentation auf der Seite mit Vorsicht befinden. Wenden Sie sich an den Speicher Anbieter.
- Wenn als Ausgangspunkt Windows Server 2008-oder 2008 R2-Cluster verwendet wird, sind möglicherweise weitere Schritte erforderlich.
- Wenn auf dem Cluster virtuelle Computer ausgeführt werden, stellen Sie sicher, dass Sie die Ebene der virtuellen Maschine aktualisieren, sobald die Cluster Funktionsebene mit dem PowerShell -Befehl Update-VMVersionerreicht wurde.
- Beachten Sie Folgendes: Wenn Sie eine Anwendung wie SQL Server, Exchange Server usw. ausführen, wird die Anwendung nicht mit dem Assistenten zum Kopieren von Cluster Rollen migriert. Wenden Sie sich an den Hersteller der Anwendung, um die entsprechenden Migrations Schritte für die Anwendung auszuführen.

# Übersicht über die clusterfähige Aktualisierung.

09.04.2020 • 14 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Dieses Thema enthält eine Übersicht über die Cluster-bewusste Aktualisierung (Cau-), eine Funktion, die den Software Aktualisierungsprozess auf Cluster Servern unter Beibehaltung der Verfügbarkeit automatisiert.

> **NOTE**
>
> Wenn Sie direkte Speicherplätze Cluster aktualisieren, empfiehlt es sich, das Cluster fähige aktualisieren zu verwenden.

## Featurebeschreibung

Das Cluster fähige aktualisieren ist ein automatisiertes Feature, mit dem Sie Server in einem Failovercluster mit geringem oder ohne Verfügbarkeit während des Aktualisierungs Vorgangs aktualisieren können. Während einer Update Ausführung führt das Cluster fähige aktualisieren transparent die folgenden Aufgaben aus:

1. Versetzt jeden Knoten des Clusters in den Knoten Wartungsmodus.
2. Verschiebt die Cluster Rollen aus dem Knoten.
3. Installiert die Updates und alle abhängigen Updates.
4. Führt bei Bedarf einen Neustart durch.
5. Führt den Wartungsmodus des Knotens aus.
6. Stellt die Cluster Rollen auf dem Knoten wieder her.
7. Wechselt, um den nächsten Knoten zu aktualisieren.

Für viele Clusterrollen im Cluster löst der automatische Updateprozess ein geplantes Failover aus. Dadurch kann eine vorübergehende Dienstunterbrechung für angeschlossene Clients verursacht werden. Im Fall von fortlaufend verfügbaren Arbeits Auslastungen, z. b. Hyper-V mit Live Migration oder Dateiserver mit SMB transparent Failover, kann das Cluster fähige aktualisieren jedoch Cluster Aktualisierungen ohne Auswirkungen auf die Dienst Verfügbarkeit koordinieren.

## Praktische Anwendungsfälle

- Cau reduziert Dienst Ausfälle in geclusterten Diensten, verringert die Notwendigkeit von Problem Umgehungen für manuelles Aktualisieren und ermöglicht das Beenden--Ende des Cluster Aktualisierungsprozesses zuverlässiger für den Administrator. Wenn das Cau-Feature in Verbindung mit fortlaufend verfügbaren Cluster Arbeits Auslastungen verwendet wird, z. b. fortlaufend verfügbare Dateiserver (Dateiserver-Arbeitsauslastung mit SMB transparent Failover) oder Hyper-V, können die Cluster Aktualisierungen ohne Auswirkungen auf die Dienst Verfügbarkeit für Clients ausgeführt werden.

- CAU vereinfacht die unternehmensweite Übernahme von einheitlichen IT-Prozessen. Update Lauf Profile können für unterschiedliche Klassen von Failoverclustern erstellt und dann zentral auf einer Dateifreigabe verwaltet werden, um sicherzustellen, dass Aktualisierungen durch Cau-bereit Stellungen in der gesamten IT-Organisation einheitlich angewendet werden, auch wenn die Cluster über verschiedene Zeilen--Geschäfts oder Administratoren verwaltet werden.

- Mit CAU können Updateausführungen für regelmäßige tägliche, wöchentliche oder monatliche Intervalle zur Koordination von Clusteraktualisierungen mit anderen IT-Verwaltungsprozessen geplant werden.

- Cau stellt eine erweiterbare Architektur bereit, mit der die Cluster Software Inventur auf-bewusste Weise aktualisiert werden können. Dies kann von Verlegern verwendet werden, um die Installation von Software Updates zu koordinieren, die nicht auf Windows Update oder Microsoft Update veröffentlicht werden oder nicht von Microsoft zur Verfügung stehen, z. b. Updates für nicht-Microsoft-Gerätetreiber.
- Der Self--Aktualisierungs Modus für Cluster fähiges aktualisieren ermöglicht ein "Cluster in einem Box"-Gerät (eine Reihe von gruppierten physischen Computern, die in der Regel in einem Gehäuse verpackt sind,) sich selbst aktualisieren. Normalerweise werden solche Geräte in Filialen mit minimalem lokalem IT-Support zur Verwaltung von Clustern bereitgestellt. Der Self--Aktualisierungs Modus bietet in diesen Bereitstellungs Szenarien einen großen nutzen.

## Wichtige Funktionalität

Im folgenden finden Sie eine Beschreibung der wichtigen Funktionen für die Cluster fähige Aktualisierung:

- Eine Benutzeroberfläche (UI)-das Aktualisierungs Fenster für Cluster fähige Elemente und eine Reihe von Cmdlets, mit denen Sie die Updates in der Vorschau anzeigen, anwenden, überwachen und Berichte überwachen können.
- Eine End--, um die Automatisierung des Cluster-Aktualisierungs Vorgangs zu-(eine Update Ausführung), die von einem oder mehreren updatekoordinatorcomputern orchestriert wird.
- Ein Standard-Plug-in, das in den vorhandenen Windows Update-Agent (WUA-) und Windows Server Update Services (die WSUS-) Infrastruktur in Windows Server integriert ist, um wichtige Microsoft-Updates anzuwenden.
- Ein zweites Plug-in, das zum Anwenden von Microsoft-Hotfixes verwendet werden kann und das zum Anwenden von nicht-Microsoft-Updates angepasst werden kann
- Updateausführungsprofile, die Sie mit Einstellungen für Optionen zur Updateausführung konfigurieren, wie z. B. die maximale Anzahl an Versuchen, die eine Aktualisierung pro Knoten wiederholt wird. Updateausführungprofile ermöglichen eine schnelle Wiederverwendung derselben Einstellungen für verschiedene Updateausführungen und eine einfache Freigabe der Aktualisierungseinstellungen für andere Failovercluster.
- Eine erweiterbare Architektur, die neue Plug-in der Entwicklung unterstützt, um andere Knoten-Aktualisierungs Tools im Cluster zu koordinieren, z. b. benutzerdefinierte Software Installationsprogramme, BIOS-Aktualisierungs Tools und Netzwerkadapter-oder Hostbus Adapter (HBA-) Aktualisierungs Tools.

Beim Cluster fähigen aktualisieren kann der gesamte Cluster Aktualisierungs Vorgang in zwei Modi koordiniert werden:

- **Selbst-Aktualisierungs Modus** In diesem Modus wird die Cluster Rolle für Cluster fähiges aktualisieren als Arbeitsauslastung auf dem zu aktualisierenden Failovercluster konfiguriert, und es wird ein zugeordneter Aktualisierungs Zeitplan definiert. Der Cluster aktualisiert sich zu den geplanten Zeiten anhand eines standardmäßigen oder benutzerdefinierten Updateausführungsprofils selbst. Bei der Updateausführung startet der CAU-Updatekoordinatorprozess auf dem Knoten, der aktuell der Besitzer der Clusterrolle für CAU ist, und alle Clusterknoten werden nacheinander durch den Prozess aktualisiert. Von der CAU-Clusterrolle wird zum Aktualisieren des aktuellen Clusterknotens ein Failover zu einem anderen Clusterknoten ausgeführt, und ein neuer Updatekoordinatorprozess auf diesem Knoten übernimmt die Steuerung der Updateausführung. Im selbst-Aktualisierungs Modus kann das Cluster fähige aktualisieren den Failovercluster mithilfe eines vollständig automatisierten End--zum-Ende des Aktualisierungs Vorgangs aktualisieren. Ein Administrator kann auch Updates auf-Nachfrage in diesem Modus auslöst oder den Ansatz für die Remote-Aktualisierung verwenden, wenn gewünscht. Im selbst-Aktualisierungs Modus kann ein Administrator Zusammenfassungs Informationen zu einer laufenden

Update Ausführung erhalten, indem eine Verbindung mit dem Cluster hergestellt und das Windows PowerShell-Cmdlet **Get-caurun** ausgeführt wird.

- **Remote--Aktualisierungs Modus** Bei diesem Modus wird ein Remote Computer, der als Update Koordinator bezeichnet wird, mit den Cau-Tools konfiguriert. Der Updatekoordinator gehört nicht dem Cluster an, der im Rahmen der Updateausführung aktualisiert wird. Der-Administrator löst auf dem Remote Computer eine auf-Demand-Update ausführen mithilfe eines standardmäßigen oder benutzerdefinierten Update Lauf Profils aus. Der Aktualisierungs Modus für Remote-ist für die Überwachung des Echt Zeit-Zeitraums während der Update Ausführung und für Cluster, die auf Server Core-Installationen ausgeführt werden, hilfreich.

## Hardware- und Softwareanforderungen

Cau kann für alle Editionen von Windows Server, einschließlich Server Core-Installationen, verwendet werden. Ausführliche Informationen zu den Anforderungen finden Sie unter Anforderungen für das Cluster fähige aktualisieren und bewährte Methoden.

**Installieren des Cluster fähigen Updates**

Um Cau zu verwenden, installieren Sie das Failoverclustering-Feature in Windows Server, und erstellen Sie ein Failovercluster. Die Komponenten, die die CAU-Funktionalität unterstützen, werden automatisch auf jedem Clusterknoten installiert.

Zur Installation des Failoverclustering-Features können Sie die folgenden Tools verwenden:

- Assistent zum Hinzufügen von Rollen und Features im Server-Manager
- Install-Windows Feature Windows PowerShell-Cmdlet
- Befehlszeilentool %%amp;quot;Abbildverwaltung für die Bereitstellung%%amp;quot; (Deployment Image Servicing and Management, DISM)

Weitere Informationen finden Sie unter Installieren des Failoverclustering-Features.

Sie müssen auch die Failoverclustering-Tools installieren, die Teil der Remoteserver-Verwaltungstools sind und standardmäßig installiert werden, wenn Sie das Failoverclustering-Feature in Server-Manager installieren. Die Failoverclustering-Tools umfassen die Cluster fähige Aktualisierungs Benutzeroberfläche und PowerShell-Cmdlets.

Sie müssen die Failoverclusteringtools wie folgt installieren, um die verschiedenen CAU-Aktualisierungsmodi zu unterstützen:

- Installieren Sie die Failoverclustering-Tools auf den einzelnen Cluster Knoten, um das Cluster fähige aktualisieren im selbst-Aktualisierungs Modus zu verwenden.
- Installieren Sie die Failoverclustering-Tools auf einem Computer mit Netzwerk Konnektivität zum Failovercluster, um den Remote-Aktualisierungs Modus zu aktivieren.

> **NOTE**
> - Sie können die Failoverclustering-Tools unter Windows Server 2012 nicht verwenden, um das Cluster fähige Update auf einer neueren Version von Windows Server zu verwalten.
> - Die Installation der failoverclusteringtools auf den Cluster Knoten ist nicht erforderlich, um Cau nur im Remote-Aktualisierungs Modus zu verwenden. Bestimmte CAU-Features sind dann jedoch nicht verfügbar. Weitere Informationen finden Sie unter Requirements and Best Practices for Cluster-Aware Update.
> - Der Computer, auf dem die Cau-Tools installiert und die Updates koordiniert werden, kann nicht Mitglied des Failoverclusters sein, es sei denn, Sie verwenden Cau nur im Modus für die selbst-Aktualisierung.

**Aktivieren des selbst Aktualisierungs Modus**

Um den selbst Aktualisierungs Modus zu aktivieren, müssen Sie dem Failovercluster die Cluster Rolle für Cluster fähiges aktualisieren hinzufügen. Verwenden Sie hierzu eine der folgenden Methoden:

- Wählen Sie in Server-Manager **Tools** > **Cluster fähiges aktualisieren**aus, und wählen Sie dann im Fenster Cluster fähiges aktualisieren die **Option selbst Aktualisierungs Optionen für Cluster konfigurieren**aus.
- Führen Sie in einer PowerShell-Sitzung das Cmdlet Add-cauclusterrole aus.

Deinstallieren Sie zum Deinstallieren von Cau das Failoverclustering-Feature oder die failoverclusteringtools mithilfe von Server-Manager, dem Cmdlet " Uninstall-Windows Feature " oder dem Befehl "-Ausdruck"-Zeilen Tools.

**Weitere Anforderungen und Best Practices**

Sie können den Best Practices Analyzer für CAU ausführen, um die erfolgreiche Aktualisierung der Clusterknoten mit CAU sicherzustellen und weitere Informationen zum Konfigurieren der Failoverclusterumgebung für die Verwendung von CAU zu erhalten.

Ausführliche Informationen zu Anforderungen und bewährten Methoden für die Verwendung von Cau sowie Informationen zum Ausführen des Cau-Best Practices Analyzer finden Sie unter Anforderungen und Best Practices für Cluster-fähiges aktualisieren.

**Cluster fähiges aktualisieren wird gestartet**

**So starten Sie das Cluster fähige Aktualisieren von Server-Manager**

1. Starten Sie den Server-Manager.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie **im Menü Extras** auf **Cluster-fähiges aktualisieren**.
   - Wenn mindestens ein Cluster Knoten oder der Cluster zu Server-Manager hinzugefügt wird, klicken Sie auf der Seite **alle Server** mit der rechten-auf den Namen eines Knotens (oder den Namen des Clusters), und klicken Sie dann auf **Cluster aktualisieren**.

# Siehe auch

Die folgenden Links enthalten weitere Informationen zur Verwendung des Cluster fähigen Updates.

- [Anforderungen und bewährte Methoden für clusterfähiges Aktualisieren-
- Cluster-fähiges aktualisieren: häufig gestellte Fragen
- Erweiterte Optionen und Update Lauf Profile für Cau
- Funktionsweise von Cau-Plug-ins
- Cluster-fähiges Aktualisieren von Cmdlets in Windows PowerShell
- Cluster-fähiges Aktualisieren von Plug-als Referenz

# Anforderungen und Best Practices für clusterfähiges Aktualisieren

02.05.2020 • 40 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

In diesem Abschnitt werden die Anforderungen und Abhängigkeiten beschrieben, die zur Verwendung des Cluster fähigen Aktualisierens (Cluster-Aware Update , Cau) zum Anwenden von Updates auf einen Failovercluster unter Windows Server erforderlich sind

> **NOTE**
> Sie müssen möglicherweise unabhängig überprüfen, ob Ihre Cluster Umgebung für die Anwendung von Updates bereit ist,-Wenn Sie ein anderes Plug-in als **Microsoft. windowsupdatepluginverwenden**. Wenn Sie ein nicht--Microsoft-Plug--in verwenden, kontaktieren Sie den Herausgeber, um weitere Informationen zu erhalten. Weitere Informationen zu Plug--ins finden Sie unter Funktions-Weise von Plug-ins.

## Installieren des Failoverclustering-Features und der Failoverclusteringtools

Für das clusterfähige Aktualisieren ist die Installation des Failoverclustering-Features und der Failoverclusteringtools erforderlich. Die Failoverclustering-Tools umfassen die Cau-Tools ("clusterawareupdating. dll)", die Failoverclustering-Cmdlets und andere Komponenten, die für Cau-Vorgänge erforderlich sind. Schritte zum Installieren des Failoverclustering-Features finden Sie unter Installieren des Failoverclustering-Features und der Failoverclusteringtools.

Die genauen Installationsanforderungen für die failoverclusteringtools hängen davon ab, ob Updates von Cau als Cluster Rolle auf dem (Failovercluster-mithilfe des) selbst Aktualisierungs Modus oder eines Remote Computers koordiniert werden. Der selbst-Aktualisierungs Modus von Cau erfordert zusätzlich die Installation der Cluster Rolle für Cluster fähiges aktualisieren auf dem Failovercluster mithilfe der Cau-Tools.

In der folgenden Tabelle werden die Installationsanforderungen des Features für clusterfähiges Aktualisieren für die beiden Aktualisierungsmodi für clusterfähiges Aktualisieren zusammengefasst.

| INSTALLIERTE KOMPONENTE | SELBST-AKTUALISIERUNGS MODUS | REMOTE-AKTUALISIERUNGS MODUS |
|---|---|---|
| Failoverclustering-Feature | Auf allen Clusterknoten erforderlich | Auf allen Clusterknoten erforderlich |
| Failoverclusteringtools | Auf allen Clusterknoten erforderlich | -Erforderlich auf Remote-aktualisierbaren Computern<br>-Erforderlich auf allen Cluster Knoten zum Ausführen des Cmdlets " Save-caudebugtrace " |
| Clusterrolle für clusterfähiges Aktualisieren | Erforderlich | Nicht erforderlich |

## Anfordern eines Administratorkontos

Die folgenden Administratoranforderungen sind zur Verwendung der Features für clusterfähiges Aktualisieren erforderlich.

- Sie müssen ein Domänen Konto verwenden, das über lokale Administratorrechte (und) Berechtigungen für alle Cluster Knoten verfügt, um eine Vorschau oder Anwendung von Update Aktionen mithilfe der Benutzeroberfläche für die Benutzeroberfläche für Cluster fähiges aktualisieren oder der Cmdlets für das Cluster fähige aktualisieren zu verwenden. Wenn das Konto nicht auf jedem Knoten über ausreichende Berechtigungen verfügt, werden Sie im Fenster Cluster fähiges Aktualisieren aufgefordert, die erforderlichen Anmelde Informationen anzugeben, wenn Sie diese Aktionen ausführen. Wenn Sie die Cmdlets für das Cluster fähige aktualisieren verwenden möchten, können Sie die erforderlichen Anmelde Informationen als Cmdlet-Parameter angeben.
- Wenn Sie das Cluster fähige aktualisieren im-Remote Aktualisierungs Modus verwenden, wenn Sie mit einem Konto angemeldet sind, das nicht über lokale Administratorrechte und Berechtigungen auf den Cluster Knoten verfügt, müssen Sie die Tools für Cluster fähiges aktualisieren als Administrator ausführen, indem Sie ein lokales Administrator Konto auf dem Computer mit dem Update Koordinator oder ein Konto verwenden, das über das Benutzerrecht Identität **eines Clients annehmen nach der Authentifizierung** verfügt.
- Zum Ausführen des Best Practices Analyzer für Cluster fähiges aktualisieren müssen Sie ein Konto verwenden, das auf den Cluster Knoten über Administratorrechte und lokale Administratorrechte auf dem Computer, der zum Ausführen des Test-causetup- Cmdlets verwendet wird, oder zum Analysieren der Update Bereitschaft des Clusters mithilfe des Cluster fähigen Aktualisierungs Fensters verwendet wird. Weitere Informationen finden Sie unter Testen der Updatebereitschaft des Clusters.

## Überprüfen der Clusterkonfiguration

Nachfolgend sind allgemeine Anforderungen an einen Failovercluster zum Unterstützen von Updates mithilfe des clusterfähigen Aktualisierens aufgeführt. Weitere Konfigurationsanforderungen für die Remoteverwaltung auf den Knoten finden Sie weiter unten in diesem Thema unter Konfigurieren von Knoten für die Remoteverwaltung.

- Es müssen ausreichend Clusterknoten online sein, damit der Cluster das Quorum besitzt.
- Alle Clusterknoten müssen sich in derselben Active Directory-Domäne befinden.
- Der Clustername muss im Netzwerk mithilfe von DNS aufgelöst werden.
- Wenn das Cluster fähige aktualisieren im Remote-Aktualisierungs Modus verwendet wird, muss der Computer des Update Koordinators über eine Netzwerkverbindung mit den Failoverclusterknoten verfügen, und er muss sich in derselben Active Directory Domäne wie der Failovercluster befinden.
- Der Clusterdienst muss auf allen Clusterknoten ausgeführt werden. Dieser Dienst wird standardmäßig auf allen Clusterknoten installiert und für den automatischen Start konfiguriert.
- Stellen Sie sicher, dass-die Skripts-auf allen Cluster Knoten installiert sind oder dass Sie für alle Knoten verfügbar sind, z. b. auf einer hoch verfügbaren Netzwerkdatei Freigabe, um PowerShell-Skripts vor Update oder nach Update Skripts während einer Update-Update-Aktualisierung zu verwenden. Wenn Skripts auf einer Netzwerkdateifreigabe gespeichert werden, konfigurieren Sie den Ordner für die Gruppe "Alle" für die Berechtigung "Lesen".

## Konfigurieren der Knoten für die Remoteverwaltung

Zum Verwenden des Cluster fähigen Aktualisierens müssen alle Knoten des Clusters für die Remote Verwaltung konfiguriert sein. Standardmäßig müssen Sie zum Konfigurieren der Knoten für die Remote Verwaltung nur eine Firewallregel aktivieren, um automatische Neustarts zuzulassen.

In der folgenden Tabelle sind die Anforderungen an die gesamte Remote Verwaltung aufgeführt, wenn die Umgebung von den Standardeinstellungen abweicht.

Diese Anforderungen treten zusätzlich zu den Installationsanforderungen für Installieren des Failoverclustering-Features und der Failoverclusteringtools und zu den allgemeinen Anforderungen auf, die in vorherigen Abschnitten dieses Themas beschrieben werden.

| ANFORDERUNG | STANDARDSTATUS | SELBST-AKTUALISIERUNGS MODUS | REMOTE-AKTUALISIERUNGS MODUS |
|---|---|---|---|
| Aktivieren einer Firewallregel zum Zulassen automatischer Neustarts | Disabled | Auf allen Clusterknoten erforderlich, wenn eine Firewall verwendet wird | Auf allen Clusterknoten erforderlich, wenn eine Firewall verwendet wird |
| Aktivieren der Windows-Verwaltungsinstrumentation | Aktiviert | Auf allen Clusterknoten erforderlich | Auf allen Clusterknoten erforderlich |
| Aktivieren von Windows PowerShell 3.0 oder 4.0 und Windows PowerShell-Remoting | Aktiviert | Auf allen Clusterknoten erforderlich | Auf allen Clusterknoten muss Folgendes ausgeführt werden:<br>-Das Save-caudebugtrace -Cmdlet -PowerShell--Skripts vor-und nach dem Update während einer Update Lauf Zeit Aktualisierung -Tests der Update Bereitschaft des Clusters mithilfe des Cluster fähigen Aktualisierungs Fensters oder des Windows PowerShell-Cmdlets " -Test causetup " |
| Installieren von .NET Framework 4,6 oder 4,5 | Aktiviert | Auf allen Clusterknoten erforderlich | Auf allen Clusterknoten muss Folgendes ausgeführt werden:<br>-Das Save-caudebugtrace -Cmdlet -PowerShell--Skripts vor-und nach dem Update während einer Update Lauf Zeit Aktualisierung -Tests der Update Bereitschaft des Clusters mithilfe des Cluster fähigen Aktualisierungs Fensters oder des Windows PowerShell-Cmdlets " -Test causetup " |

**Aktivieren einer Firewallregel zum Zulassen automatischer Neustarts**

Um automatische Neustarts nach dem Anwenden (von Updates zuzulassen, wenn für die Installation eines Updates ein)Neustart erforderlich ist, muss auf jedem-Knoten, der folgenden Datenverkehr zulässt, eine

Firewallregel aktiviert werden, wenn die Windows-Firewall oder eine nicht-Microsoft-Firewall auf den Cluster Knoten verwendet wird:

- Protokoll: TCP
- Richtung: Eingehend
- Programm: wininit.exe
- Ports: Dynamische RPC-Ports
- Profil: Domäne

Wenn die Windows-Firewall auf den Clusterknoten verwendet wird, können Sie dazu die Regelgruppe **Remotecomputer herunterfahren** der Windows-Firewall auf den einzelnen Clusterknoten aktivieren. Wenn Sie das Fenster Cluster fähiges aktualisieren verwenden, um Updates anzuwenden und selbst-Aktualisierungs Optionen zu konfigurieren, wird die Regelgruppe **Remote herunter** fahren der Windows-Firewall auf jedem Cluster Knoten automatisch aktiviert.

> **NOTE**
> Die Regelgruppe **Remote Shutdown** der Windows-Firewall kann nicht aktiviert werden, wenn sie mit Gruppenrichtlinieneinstellungen in Konflikt steht, die für die Windows-Firewall konfiguriert sind.

Die Firewallregelgruppe **Remote Shutdown** wird auch durch Angeben des **– enablefirewallrules** -Parameters aktiviert, wenn die folgenden Cmdlets für Cluster fähiges aktualisieren ausgeführt werden: Add-cauclusterrole, Aufruf-caurunund setcauclusterrole.

Das folgende PowerShell-Beispiel zeigt eine zusätzliche Methode zum Aktivieren automatischer Neustarts auf einem Cluster Knoten.

```
Set-NetFirewallRule -Group "@firewallapi.dll,-36751" -Profile Domain -Enabled true
```

#### Windows-Verwaltungsinstrumentation aktivieren (WMI)

Alle Cluster Knoten müssen mit Windows-Verwaltungsinstrumentation (WMI)für die Remote Verwaltung konfiguriert werden. Diese Einstellung ist standardmäßig aktiviert.

Gehen Sie wie folgt vor, um die Remoteverwaltung manuell zu aktivieren:

1. Starten Sie in der Konsole "Dienste" den Dienst **Windows-Remoteverwaltung**, und legen Sie für den Starttyp **Automatisch** fest.
2. Führen Sie das -Cmdlet oder den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten aus:

   ```
   winrm quickconfig -q
   ```

Zur Unterstützung von WMI-Remoting muss die eingehende Firewallregel für ** (Windows-Remoteverwaltung http-in) ** auf jedem Knoten aktiviert sein, wenn die Windows-Firewall auf den Cluster Knoten verwendet wird. Diese Regel ist standardmäßig aktiviert.

#### Aktivieren von Windows PowerShell und Windows PowerShell-Remoting

PowerShell muss-installiert und aktiviert sein, damit Remote Befehle auf-allen Cluster Knoten ausgeführt werden können, um den selbst Aktualisierungs Modus und bestimmte Cau-Features im Remote Aktualisierungs Modus zu aktivieren. PowerShell ist standardmäßig installiert und für Remoting aktiviert.

Verwenden Sie eine der folgenden Methoden, um PowerShell-Remoting zu aktivieren:

- Führen Sie das -Cmdlet aus.
- Konfigurieren Sie eine-Gruppenrichtlinie Einstellung auf Domänen (Ebene für)Windows-Remoteverwaltung WinRM.

Weitere Informationen zum Aktivieren von PowerShell-Remoting finden Sie unter Informationen zu Remote Anforderungen.

**Installieren von .NET Framework 4,6 oder 4,5**

Um den selbst-Aktualisierungs Modus und bestimmte Features für Cluster fähiges-aktualisieren im Remote Aktualisierungs Modus zu aktivieren, muss .NET Framework 4,6 oder .NET Framework 4,5 (auf Windows Server 2012 R2) auf allen Cluster Knoten installiert sein. Standardmäßig ist .NET Framework installiert.

Verwenden Sie den folgenden Befehl, um .NET Framework 4,6 (oder 4,5) mithilfe von PowerShell zu installieren, wenn er nicht bereits installiert ist:

```
Install-WindowsFeature -Name NET-Framework-45-Core
```

# Empfehlungen zu bewährten Methoden für die Verwendung des Cluster fähigen Updates

**Empfehlungen zum Anwenden von Microsoft-Updates**

Wenn Sie mit der Verwendung von Cau zum Anwenden von Updates mit dem Standard-Plug--in für **Microsoft.windowsupdateplugin** in einem Cluster beginnen, sollten Sie keine anderen Methoden zum Installieren von Software Updates von Microsoft auf den Cluster Knoten mehr verwenden.

Caution

Das Kombinieren von Cau mit Methoden, die (einzelne Knoten automatisch nach einem) festgelegten Zeitplan aktualisieren, kann zu unvorhersehbaren Ergebnissen führen, einschließlich Dienstunterbrechungen und ungeplanter Ausfallzeiten.

Empfohlene Richtlinien:

- Um die besten Ergebnisse zu erzielen, empfiehlt es sich, dass Sie Einstellungen auf dem Clusterknoten für die automatische Aktualisierung deaktivieren, z. B. über die Einstellungen für automatische Updates in der Systemsteuerung oder über die Einstellungen, die mithilfe der Gruppenrichtlinie konfiguriert werden.

  Caution

  Die automatische Installation von Updates auf den Clusterknoten kann die Installation von Updates durch clusterfähiges Aktualisieren beeinträchtigen und somit beim clusterfähigen Aktualisieren zu Fehlern führen.

  Die folgenden Einstellungen für automatische Updates sind (sofern erforderlich) mit dem clusterfähigen Aktualisieren kompatibel, da der Administrator die zeitliche Abfolge der Updateinstallation steuern kann.

  - Einstellungen zur Benachrichtigung vor dem Herunterladen von Updates und zur Benachrichtigung vor der Installation
  - Einstellungen zum automatischen Herunterladen von Updates und zur Benachrichtigung vor der Installation

  Wenn die Option "Automatische Updates" Updates jedoch zur selben Zeit wie eine Updateausführung für clusterfähiges Aktualisieren herunterlädt, kann die Updateausführung möglicherweise länger dauern.

- Konfigurieren Sie kein Update System wie z. b (. Windows Server Update Services) WSUS, um (Updates

automatisch nach einem fest) gelegten Zeitplan auf Cluster Knoten anzuwenden.

- Alle Clusterknoten müssen einheitlich für die Verwendung derselben Updatequelle konfiguriert sein, z. B. WSUS-Server, Windows-Update oder Microsoft Update.
- Schließen Sie Clusterknoten von allen erforderlichen oder automatischen Updates aus, wenn Sie Softwareupdates mithilfe eines Konfigurationsverwaltungssystems auf Computer im Netzwerk anwenden. Beispiele für Konfigurations Verwaltungssysteme sind Microsoft Endpoint Configuration Manager und Microsoft System Center Virtual Machine Manager 2008.
- Wenn z. b. (von den WSUS-Servern) interne Software Verteilungs Server zum Speichern und Bereitstellen der Updates verwendet werden, stellen Sie sicher, dass die genehmigten Updates für die Cluster Knoten von diesen Servern korrekt identifiziert werden.

#### Anwenden von Microsoft-Updates in Filialszenarien

Wenn Sie in bestimmten Filialszenarien Microsoft-Updates über Microsoft Update oder Windows Update auf Clusterknoten herunterladen möchten, müssen Sie möglicherweise auf jedem Knoten Proxyeinstellungen für das lokale Systemkonto konfigurieren. Dies kann z. B. erforderlich sein, wenn die Filialcluster auf Microsoft Update oder Windows Update zugreifen, um Updates mithilfe eines lokalen Proxyservers herunterzuladen.

Konfigurieren Sie bei Bedarf die WinHTTP-Proxy Einstellungen auf den einzelnen Knoten, um einen lokalen Proxy Server anzugeben und (lokale Adress Ausnahmen (eine Umgehungs Liste für lokale)Adressen) zu konfigurieren. Dazu können Sie den folgenden Befehl an einer Eingabeaufforderung mit erhöhten Rechten auf den einzelnen Clusterknoten ausführen:

```
netsh winhttp set proxy <ProxyServerFQDN >:<port> "<local>"
```

Dabei ist <*proxyserverfqdn*> der voll qualifizierte Domänen Name für den Proxy Server und <*Port*> ist der Port, über den die Kommunikation stattfinden soll (normalerweise Port 443).

Geben Sie beispielsweise den folgenden Befehl ein, um die WinHTTP-Proxy Einstellungen für das lokale System Konto anzugeben, in dem der Proxy Server *MyProxy.contoso.com*mit Port 443 und lokale Adress Ausnahmen angegeben ist:

```
netsh winhttp set proxy MyProxy.CONTOSO.com:443 "<local>"
```

### Empfehlungen zur Verwendung von Microsoft.HotfixPlugin

- Es wird empfohlen, dass Sie Berechtigungen im Hotfixstammordner und in der Hotfixkonfigurationsdatei konfigurieren, um den Schreibzugriff nur auf lokale Administratoren auf den Computer zu beschränken, die zum Speichern dieser Dateien verwendet werden. Dadurch können Manipulationen an diesen Dateien durch nicht berechtigte Benutzer verhindert werden, die die Funktionalität des Failoverclusters beeinträchtigen könnten, wenn Hotfixes angewendet werden.
- Um die Datenintegrität für die Server Message Block (-SMB) -Verbindungen sicherzustellen, die für den Zugriff auf den hotfixstamm Ordner verwendet werden, sollten Sie die SMB-Verschlüsselung im freigegebenen SMB-Ordner konfigurieren, sofern dies möglich ist. **Microsoft.HotfixPlugin** erfordert, dass die SMB-Signatur oder SMB-Verschlüsselung konfiguriert ist, um die Datenintegrität für SMB-Verbindungen sicherzustellen.

  Weitere Informationen finden Sie unter Einschränken des Zugriffs auf den hotfixstamm Ordner und die hotfixkonfigurationsdatei.

### Weitere Empfehlungen

- Um Konflikte mit einer Updateausführung für clusterfähiges Aktualisieren zu vermeiden, die möglicherweise für den gleichen Zeitpunkt vorgesehen sind, planen Sie während der geplanten

Wartungszeitfenster keine Kennwortänderungen für Clusternamenobjekte und virtuelle Computerobjekte.

- Sie sollten die entsprechenden Berechtigungen für Skripts vor-und-nach dem Update festlegen, die in freigegebenen Netzwerk Ordnern gespeichert werden, um mögliche Manipulationen an diesen Dateien durch nicht autorisierte Benutzer zu verhindern.
- Zum Konfigurieren von Cau im-selbst Aktualisierungs Modus muss ein virtuelles (Computer Objekt) VCO für die Cluster Rolle für Cluster fähiges aktualisieren in Active Directory erstellt werden. Dieses Objekt kann durch das clusterfähige Aktualisieren automatisch zu dem Zeitpunkt erstellt werden, zu dem die Clusterrolle für clusterfähiges Aktualisieren hinzugefügt wird, wenn der Failovercluster über die entsprechenden Berechtigungen verfügt. Aufgrund der Sicherheitsrichtlinien in einigen Organisationen ist es möglicherweise erforderlich, das Objekt in Active Directory vorab bereitzustellen. Das entsprechende Verfahren hierfür finden Sie unter Schritte für die Vorabbereitstellung eines Kontos für eine Clusterrolle.
- Sie können Profile für die Updateausführung erstellen, um Updateausführungseinstellungen für verschiedene Failovercluster mit ähnlichen Aktualisierungsanforderungen in der IT-Organisation zu speichern und wiederzuverwenden. In Abhängigkeit vom Aktualisierungsmodus können Sie die Updateausführungsprofile zusätzlich auf einer Dateifreigabe speichern und verwalten, auf die alle Remotecomputer für den Updatekoordinator oder die Failovercluster zugreifen können. Weitere Informationen finden Sie unter Erweiterte Optionen und Update Lauf Profile für Cau.

## Testen der Updatebereitschaft des Clusters

Sie können Best Practices Analyzer (das BPA) -Modell für Cluster fähiges aktualisieren ausführen, um zu testen, ob ein Failovercluster und die Netzwerkumgebung vielen der Anforderungen entsprechen, damit Software Updates von Cau angewendet werden. Viele der Tests prüfen die Umgebung auf die Bereitschaft zur Anwendung von Microsoft-Updates mithilfe des Standard--Plug-ins, **Microsoft. windowsupdateplugin**.

> **NOTE**
> Möglicherweise müssen Sie unabhängig prüfen, ob Ihre Cluster Umgebung für die Anwendung von Software Updates bereit ist,-indem Sie ein anderes Plug-in als **Microsoft. windowsupdateplugin**verwenden. Wenn Sie ein nicht--Microsoft-Plug--in verwenden, z. b. ein von Ihrem Hardwarehersteller bereitgestelltes Plug-in, wenden Sie sich an den Herausgeber

Zum Ausführen des Best Practices Analyzer (BPA) haben Sie die folgenden beiden Möglichkeiten:

1. Wählen Sie in der Konsole für clusterfähiges Aktualisieren die Option **Vorbereitung auf das Clusterupdate analysieren** aus. Nachdem der BPA die Bereitschafts Tests abgeschlossen hat, wird ein Testbericht angezeigt. Wenn auf den Clusterknoten Probleme aufgetreten sind, werden die bestimmten Probleme und die betroffenen Knoten identifiziert, damit Sie entsprechende Korrekturmaßnahmen ergreifen können. Diese Tests können einige Minuten dauern.
2. Führen Sie das Test-CauSetup aus. Sie können das Cmdlet auf einem lokalen Computer oder einem Remote Computer ausführen, auf dem das Failoverclustering-Modul für Windows PowerShell (Teil der Failoverclustering-Tools) installiert ist. Sie können das Cmdlet auch auf einem Knoten des Failoverclusters ausführen.

**NOTE**

- Sie müssen ein Konto verwenden, das auf den Cluster Knoten über Administratorrechte und lokale Administratorrechte auf dem Computer, der zum Ausführen des **Test--causetup** -Cmdlets verwendet wird, oder zum Analysieren der Update Bereitschaft des Clusters mithilfe des Cluster fähigen Aktualisierungs Fensters verwendet wird. Zum Ausführen der Tests mithilfe des Cluster fähigen Aktualisierungs Fensters müssen Sie auf dem Computer mit den erforderlichen Anmelde Informationen angemeldet sein.
- Bei den Tests wird angenommen, dass die Tools für clusterfähiges Aktualisieren, die zum Anzeigen einer Updatevorschau oder zum Anwenden von Updates verwendet werden, auf demselben Computer und mit denselben Anmeldeinformationen ausgeführt werden, die zum Testen der Updatebereitschaft des Clusters verwendet werden.

**IMPORTANT**

Es wird dringend empfohlen, dass Sie die Cluster in den folgenden Situationen auf die Updatebereitschaft testen:

- Bevor Sie das clusterfähige Aktualisieren zum ersten Mal zum Anwenden von Softwareupdates verwenden können.
- Nachdem Sie einen Knoten zum Cluster hinzugefügt oder andere Hardwareänderungen am Cluster vorgenommen haben, die die Ausführung des Assistenten zum Überprüfen von Clustern erfordern.
- Nachdem Sie eine Update Quelle geändert haben, oder ändern Sie die Update (Einstellungen oder-Konfigurationen) , die sich auf die Anwendung von Updates auf den Knoten auswirken können.

### Tests für die Updatebereitschaft des Clusters

In der folgenden Tabelle sind die Tests für die Updatebereitschaft des Clusters, einige allgemeine Probleme sowie Schritte zur Behebung dieser Probleme aufgeführt.

| TEST | MÖGLICHE PROBLEME UND AUSWIRKUNGEN | LÖSUNGSSCHRITTE |
|---|---|---|
| Der Failovercluster muss verfügbar sein. | Der Failoverclustername kann nicht aufgelöst werden oder der Zugriff ist auf mindestens einen Clusterknoten nicht möglich. Der BPA kann die Clusterbereitschaftstests nicht ausführen. | -Überprüfen Sie die Schreibweise des Namens des Clusters, der während der BPA-Laufzeit angegeben wurde.<br>-Stellen Sie sicher, dass alle Knoten des Clusters online sind und ausgeführt werden.<br>-Überprüfen Sie, ob der Konfigurationsüberprüfungs-Assistent erfolgreich auf dem Failovercluster ausgeführt werden kann. |
| Die Failoverclusterknoten müssen über die Windows-Verwaltungsinstrumentation (WMI) für die Remoteverwaltung aktiviert sein. | Mindestens ein Failoverclusterknoten ist nicht mit Windows-Verwaltungsinstrumentation (WMI)für die Remote Verwaltung aktiviert. Die Clusterknoten können nicht über das clusterfähige Aktualisieren aktualisiert werden, wenn die Knoten nicht für die Remoteverwaltung konfiguriert sind. | Stellen Sie sicher, dass alle Failoverclusterknoten über die WMI für die Remoteverwaltung aktiviert wurden. Weitere Informationen finden Sie in diesem Thema unter Konfigurieren der Knoten für die Remoteverwaltung. |
| PowerShell-Remoting muss auf jedem Failoverclusterknoten aktiviert werden. | PowerShell ist nicht installiert oder nicht für das Remoting auf mindestens einem Failoverclusterknoten aktiviert. Cau kann nicht für den selbst-Aktualisierungs Modus konfiguriert werden oder bestimmte Features-im Remote Aktualisierungs Modus verwenden. | Stellen Sie sicher, dass PowerShell auf allen Cluster Knoten installiert und für das Remoting aktiviert ist.<br>Weitere Informationen finden Sie in diesem Thema unter Konfigurieren der Knoten für die Remoteverwaltung. |

| TEST | MÖGLICHE PROBLEME UND AUSWIRKUNGEN | LÖSUNGSSCHRITTE |
| --- | --- | --- |
| Failoverclusterversion | Mindestens ein Knoten im Failovercluster wird nicht unter Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt. Der Failovercluster kann nicht mithilfe des clusterfähigen Aktualisierens aktualisiert werden. | Vergewissern Sie sich, dass der während der BPA-Ausführung angegebene Failovercluster unter Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt wird.<br>Weitere Informationen finden Sie in diesem Thema unter Überprüfen der Clusterkonfiguration. |
| Die erforderlichen Versionen von .NET Framework und Windows PowerShell müssen auf allen Failoverclusterknoten installiert werden. | .NET Framework 4,6, 4,5 oder Windows PowerShell ist auf mindestens einem Cluster Knoten nicht installiert. Möglicherweise funktionieren einige Features für das clusterfähige Aktualisieren nicht. | Stellen Sie sicher, dass .NET Framework 4,6 oder 4,5 und Windows PowerShell auf allen Cluster Knoten installiert sind, sofern diese erforderlich sind.<br>Weitere Informationen finden Sie in diesem Thema unter Konfigurieren der Knoten für die Remoteverwaltung. |
| Der Clusterdienst muss auf allen Clusterknoten ausgeführt werden. | Der Clusterdienst wird auf mindestens einem Knoten nicht ausgeführt. Der Failovercluster kann nicht mithilfe des clusterfähigen Aktualisierens aktualisiert werden. | -Stellen Sie sicher, (dass die Clusterdienst) ClusSvc auf allen Knoten im Cluster gestartet wird und für den automatischen Start konfiguriert ist.<br>-Überprüfen Sie, ob der Konfigurationsüberprüfungs-Assistent erfolgreich auf dem Failovercluster ausgeführt werden kann.<br>Weitere Informationen finden Sie in diesem Thema unter Überprüfen der Clusterkonfiguration. |
| Automatische Updates dürfen nicht für die automatische Installation von Updates auf beliebigen Failoverclusterknoten konfiguriert werden. | Auf mindestens einem Failoverclusterknoten sind automatische Updates für die automatische Installation von Microsoft-Updates auf diesem Knoten konfiguriert. Die Kombination des clusterfähigen Aktualisierens mit anderen Aktualisierungsmethoden kann zu ungeplanter Downtime oder zu unvorhergesehenen Ergebnissen führen. | Wenn die Windows Update-Funktionalität auf mindestens einem Clusterknoten für automatische Updates konfiguriert ist, stellen Sie sicher, dass automatische Updates nicht für die automatische Installation von Updates konfiguriert sind.<br>Weitere Informationen finden Sie unter Empfehlungen zum Anwenden von Microsoft-Updates. |
| Die Failoverclusterknoten müssen dieselbe Updatequelle verwenden. | Mindestens ein Failoverclusterknoten ist für die Verwendung einer Updatequelle für Microsoft-Updates konfiguriert, die sich von den restlichen Knoten unterscheidet. Die Updates werden möglicherweise nicht einheitlich über das clusterfähige Aktualisieren auf die Clusterknoten angewendet. | Stellen Sie sicher, dass alle Clusterknoten für die Verwendung derselben Updatequelle konfiguriert sind, z. B. WSUS-Server, Windows-Update oder Microsoft Update.<br>Weitere Informationen finden Sie unter Empfehlungen zum Anwenden von Microsoft-Updates. |

| TEST | MÖGLICHE PROBLEME UND AUSWIRKUNGEN | LÖSUNGSSCHRITTE |
| --- | --- | --- |
| Eine Firewallregel, die das Remoteherunterfahren gestattet, muss auf jedem Knoten im Failovercluster aktiviert werden. | Mindestens ein Failoverclusterknoten verfügt nicht über eine aktivierte Firewallregel, die das Remoteherunterfahren gestattet, oder eine Gruppenrichtlinieneinstellung verhindert, dass diese Regel aktiviert wird. Eine Updateausführung, die Updates anwendet, die einen automatischen Neustart der Knoten erfordern, wurde möglicherweise nicht ordnungsgemäß beendet. | Wenn auf den Cluster Knoten die-Windows-Firewall oder eine nicht-Microsoft-Firewall verwendet wird, konfigurieren Sie eine Firewallregel, die das Remote Herunterfahren zulässt.<br>Weitere Informationen finden Sie in diesem Thema unter Aktivieren einer Firewallregel zum Zulassen automatischer Neustarts. |
| Die Proxyservereinstellung muss auf jedem Failoverclusterknoten auf einen lokalen Proxyserver festgelegt werden. | Mindestens ein Failoverclusterknoten weist eine fehlerhafte Proxyserverkonfiguration auf.<br>Wenn ein lokaler Proxyserver verwendet wird, muss die Proxyservereinstellung auf den einzelnen Knoten ordnungsgemäß konfiguriert werden, damit der Cluster auf Microsoft Update oder Windows Update zugreifen kann. | Stellen Sie sicher, dass die WinHTTP-Proxyeinstellungen auf allen Clusterknoten auf einem lokalen Proxyserver eingestellt sind, wenn dies erforderlich ist. Wenn in Ihrer Umgebung kein Proxyserver verwendet wird, kann diese Warnung ignoriert werden.<br>Weitere Informationen finden Sie in diesem Thema unter Anwenden von Updates in Filialszenarien. |
| Die Cluster Rolle für Cluster fähiges aktualisieren muss auf dem Failovercluster installiert werden,-um den selbst Aktualisierungs Modus zu aktivieren. | Die Clusterrolle für clusterfähiges Aktualisieren ist auf diesem Failovercluster nicht installiert. Diese Rolle ist für die selbst-Aktualisierung des Clusters erforderlich. | Wenn Sie Cau im selbst-Aktualisierungs Modus verwenden möchten, fügen Sie die Cluster Rolle für Cluster fähiges aktualisieren auf dem Failovercluster mit einer der folgenden Methoden hinzu:<br>-Führen Sie das PowerShell-Cmdlet Add-cauclusterrole aus.<br>-Wählen Sie im Fenster "Cluster fähiges aktualisieren" die Aktion " **selbst-Aktualisierungs Optionen für Cluster konfigurieren** " aus. |
| Die Cluster Rolle für Cluster fähiges aktualisieren muss auf dem Failovercluster aktiviert werden,-um den selbst Aktualisierungs Modus zu aktivieren. | Die Clusterrolle für clusterfähiges Aktualisieren ist deaktiviert. Die Cluster Rolle für Cluster fähiges aktualisieren ist z. b. nicht installiert oder wurde mithilfe des PowerShell-Cmdlets " cauclusterrole deaktivieren- " deaktiviert. Diese Rolle ist für die selbst-Aktualisierung des Clusters erforderlich. | Wenn Sie Cau im selbst-Aktualisierungs Modus verwenden möchten, aktivieren Sie die Cluster Rolle für Cluster fähiges aktualisieren auf diesem Failovercluster mit einer der folgenden Methoden:<br>-Führen Sie das PowerShell-Cmdlet enable-cauclusterrole aus.<br>-Wählen Sie im Fenster "Cluster fähiges aktualisieren" die Aktion " **selbst-Aktualisierungs Optionen für Cluster konfigurieren** " aus. |

| TEST | MÖGLICHE PROBLEME UND AUSWIRKUNGEN | LÖSUNGSSCHRITTE |
| --- | --- | --- |
| Das konfigurierte Cau--Plug--in für den selbst Aktualisierungs Modus muss auf allen Failoverclusterknoten registriert werden. | Die Cluster Rolle für Cluster fähiges aktualisieren auf einem oder mehreren Knoten dieses Failoverclusters kann nicht auf das Plug--in-Modul für Cluster fähiges aktualisieren-zugreifen, das in den selbst Aktualisierungs Optionen konfiguriert ist. Eine selbst-Aktualisierungs Ausführung kann fehlschlagen. | -Stellen Sie sicher, dass das konfigurierte Plug--in für Cluster fähiges aktualisieren auf allen Cluster Knoten installiert ist, indem Sie das Installationsverfahren für-das Produkt befolgen, das das Plug-in für Cluster fähiges<br>-Führen Sie das PowerShell-Cmdlet " -Register cauplugin "-aus, um das Plug-in auf den erforderlichen Cluster Knoten zu registrieren. |
| Alle Failoverclusterknoten müssen denselben Satz von registrierten Plug--ins für Cluster fähiges aktualisieren aufweisen. | Eine selbst-Aktualisierungs Ausführung kann fehlschlagen,-wenn das Plug-in, das für die Verwendung in einer Update Ausführung konfiguriert ist, in ein solches geändert wird, das nicht auf allen Cluster Knoten verfügbar ist. | -Stellen Sie sicher, dass das konfigurierte Plug--in für Cluster fähiges aktualisieren auf allen Cluster Knoten installiert ist, indem Sie das Installationsverfahren für-das Produkt befolgen, das das Plug-in für Cluster fähiges<br>-Führen Sie das PowerShell-Cmdlet " -Register cauplugin "-aus, um das Plug-in auf den erforderlichen Cluster Knoten zu registrieren. |
| Die konfigurierten Optionen für die Updateausführung müssen gültig sein. | Der selbst-Aktualisierungs Zeitplan und die Update Lauf Optionen, die für diesen Failovercluster konfiguriert sind, sind unvollständig oder ungültig. Eine selbst-Aktualisierungs Ausführung kann fehlschlagen. | Konfigurieren Sie einen gültigen-Zeitplan für die selbst Aktualisierung und einen Satz von Optionen für die Update Ausführung. Beispielsweise können Sie das PowerShell-Cmdlet " Set-cauclusterrole " verwenden, um die Cluster Rolle für Cluster fähiges aktualisieren zu konfigurieren. |
| Mindestens zwei Failoverclusterknoten müssen Besitzer der Clusterrolle für clusterfähiges Aktualisieren sein. | Eine im selbst-Aktualisierungs Modus gestartete Update Ausführung schlägt fehl, da die Cluster Rolle für Cluster fähiges aktualisieren keinen möglichen Besitzer Knoten besitzt, zu dem gewechselt werden kann. | Stellen Sie mithilfe der Failoverclustering-Tools sicher, dass alle Clusterknoten als mögliche Besitzer der Clusterrolle für clusterfähiges Aktualisieren konfiguriert sind. Dies ist die Standardkonfiguration. |
| Alle Failoverclusterknoten müssen auf die Windows PowerShell-Skripts zugreifen können. | Nicht alle möglichen Besitzer Knoten der Cluster Rolle für Cluster fähiges aktualisieren können auf die konfigurierten Windows PowerShell--Skripts-vor und nach dem Update zugreifen. Eine selbst-Aktualisierungs Ausführung schlägt fehl. | Stellen Sie sicher, dass alle möglichen Besitzer Knoten der Cluster Rolle für Cluster fähiges Aktualisieren über Berechtigungen für den Zugriff auf-die konfigurierten-PowerShell-Skripts vor und nach dem Update verfügen. |
| Alle Failoverclusterknoten müssen dieselben Windows PowerShell-Skripts verwenden. | Nicht alle möglichen Besitzer Knoten der Cluster Rolle für Cluster fähiges aktualisieren verwenden dieselbe Kopie der angegebenen Windows PowerShell-Skripts-vor und nach-dem Update. Eine selbst-Aktualisierungs Ausführung kann fehlschlagen oder ein unerwartetes Verhalten anzeigen. | Stellen Sie sicher, dass alle möglichen Besitzer Knoten der Cluster Rolle für Cluster fähiges aktualisieren dieselben PowerShell--Skripts-vor und nach dem Update verwenden. |

| TEST | MÖGLICHE PROBLEME UND AUSWIRKUNGEN | LÖSUNGSSCHRITTE |
| --- | --- | --- |
| Die Einstellung "WarnAfter", die für die Updateausführung angegeben wurde, muss niedriger sein als die Einstellung "StopAfter". | Die angegebenen Timeoutwerte der Updateausführung für clusterfähiges Aktualisieren sorgen dafür, dass der Warnungstimeout wirkungslos ist. Eine Updateausführung kann möglicherweise abgebrochen werden, bevor ein Warnereignisprotokoll generiert werden kann. | Konfigurieren Sie in den Optionen der Updateausführung einen Optionswert für **WarnAfter**, der niedriger als der Optionswert für **StopAfter** ist. |

## Weitere Informationen

- Übersicht über die clusterfähige Aktualisierung.

# Cluster fähiges aktualisieren erweiterter Optionen und Update Lauf profile

02.05.2020 • 17 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012.

In diesem Thema werden die Aktualisierungs Lauf Optionen beschrieben, die für das Update der Cluster fähigen Aktualisierung (Cluster-Aware Update , Cau) konfiguriert werden können. Diese erweiterten Optionen können konfiguriert werden, wenn Sie entweder die Benutzeroberfläche für Cluster fähiges aktualisieren oder die Windows PowerShell-Cmdlets für Cau verwenden, um Updates anzuwenden oder selbst Aktualisierungs Optionen zu konfigurieren.

Die meisten Konfigurationseinstellungen können als XML-Datei gespeichert werden; diese Datei wird als %%amp;quot;Profil für die Updateausführung%%amp;quot; bezeichnet und für weitere Updateausführungen wiederverwendet. Die von CAU bereitgestellten Standardwerte für die Updateausführungsoptionen können auch in zahlreichen Clusterumgebungen verwendet werden.

Informationen zu weiteren Optionen, die Sie für jede Updateausführung angeben können, sowie zu Profilen für die Updateausführung finden Sie in den folgenden Abschnitten in diesem Thema:

Optionen, die Sie beim Anfordern einer Update Laufzeit angeben, verwenden Optionen für die Update Lauf Profile, die in einem Profil für die Update Laufzeit festgelegt werden können.

Die folgende Tabelle enthält Optionen, die Sie in einem Profil für die CAU-Updateausführung festlegen können.

> **NOTE**
>
> Stellen Sie zum Festlegen der Option preupdatescript oder postupdatescript sicher, dass Windows PowerShell und .NET Framework 4,6 oder 4,5 installiert sind und dass PowerShell-Remoting auf jedem Knoten im Cluster aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren der Knoten für die Remote Verwaltung in Anforderungen und bewährte Methoden für das Cluster fähige aktualisieren.

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |
| **StopAfter** | Unbegrenzter Zeitraum | Die Zeit in Minuten, nach der die Updateausführung beendet wird, falls sie nicht abgeschlossen wurde. **Hinweis:** Wenn Sie ein PowerShell-Skript vor oder nach dem Update angeben, muss der gesamte Prozess zum Ausführen von Skripts und zum Ausführen von Updates innerhalb des **stopafter** -Zeitlimits vollständig ausgeführt werden. |
| **WarnAfter** | Standardmäßig; keine Warnung | Die Zeit in Minuten, nach der eine Warnung angezeigt wird, falls die Updateausführung (einschließlich eines ggf. konfigurierten Skripts vor oder nach dem Update) noch nicht abgeschlossen wurde. |

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |
| **MaxRetriesPerNode** | 3 | Die maximale Anzahl von Wiederholungen des Updateprozesses (einschließlich eines ggf. konfigurierten Skripts vor oder nach dem Update). Die maximale Anzahl ist 64. |
| **MaxFailedNodes** | Für die meisten Cluster eine ganze Zahl, die ca. ein Drittel der Anzahl der Clusterknoten beträgt | Maximale Anzahl von Knoten, an denen das Update fehlschlagen kann, entweder aufgrund von Knotenausfällen oder weil der Clusterdienst beendet wird. Tritt für einen weiteren Knoten ein Fehler auf, wird die Updateausführung beendet.<br>Der gültige Wertebereich ist 0 bis 1 weniger als die Anzahl von der Clusterknoten. |
| **RequireAllNodesOnline** | Keine | Gibt an, dass alle Knoten online und erreichbar sein müssen, bevor das Update gestartet wird. |
| **RebootTimeoutMinutes** | 15 | Die Zeit in Minuten, die bei CAU für den Neustart eines Knotens (sofern ein Neustart erforderlich ist) und das Starten aller Autostartdienst zulässig ist. Wenn der Neustart Vorgang nicht innerhalb dieses Zeitraums ausgeführt wird, wird die Update Ausführung für diesen Knoten als fehlgeschlagen markiert. |

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |
| **PreUpdateScript** | Keine | Der Pfad und der Dateiname für ein PowerShell-Skript, das auf jedem Knoten ausgeführt werden soll, bevor das Update gestartet und der Knoten in den Wartungsmodus versetzt wird. Die Dateinamenerweiterung muss **ps1** lauten, und die Gesamtlänge von Pfad und Dateiname darf nicht länger als 260 Zeichen sein. Es wird empfohlen, das Skript auf einem Datenträger im Clusterspeicher oder in einer hoch verfügbaren Dateifreigabe zu speichern, um sicherzustellen, dass alle Clusterknoten stets darauf zugreifen können. Wenn sich das Skript in einer Netzwerkdateifreigabe befindet, achten Sie darauf, die Dateifreigabe so zu konfigurieren, dass die Gruppe %%amp;quot;Jeder%%amp;quot; über die Leseberechtigung verfügt, und schränken Sie den Schreibzugriff ein, um eine Manipulationen an den Dateien durch nicht autorisierte Benutzer zu verhindern.<br>Vergewissern Sie sich bei Angabe eines Skripts vor dem Update, dass Einstellungen wie die Zeitlimits (beispielsweise **StopAfter**) so konfiguriert sind, dass das Skript erfolgreich ausgeführt werden kann. Diese Limits gelten für den gesamten Prozess (also sowohl für das Ausführen von Skripts als auch für das Installieren von Updates), nicht nur für das Installieren von Updates. |

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |
| **PostUpdateScript** | Keine | Der Pfad und der Dateiname für ein PowerShell-Skript, das nach Abschluss des Updates ausgeführt werden soll (nachdem der Knoten den Wartungsmodus verlassen hat). Die Dateinamenerweiterung muss **ps1** lauten, und die Gesamtlänge von Pfad und Dateiname darf nicht länger als 260 Zeichen sein. Es wird empfohlen, das Skript auf einem Datenträger im Clusterspeicher oder in einer hoch verfügbaren Dateifreigabe zu speichern, um sicherzustellen, dass alle Clusterknoten stets darauf zugreifen können. Wenn sich das Skript in einer Netzwerkdateifreigabe befindet, achten Sie darauf, die Dateifreigabe so zu konfigurieren, dass die Gruppe %%amp;quot;Jeder%%amp;quot; über die Leseberechtigung verfügt, und schränken Sie den Schreibzugriff ein, um eine Manipulationen an den Dateien durch nicht autorisierte Benutzer zu verhindern.<br>Vergewissern Sie sich bei Angabe eines Skripts nach dem Update, dass Einstellungen wie die Zeitlimits (beispielsweise **StopAfter**) so konfiguriert sind, dass das Skript erfolgreich ausgeführt werden kann. Diese Limits gelten für den gesamten Prozess (also sowohl für das Ausführen von Skripts als auch für das Installieren von Updates), nicht nur für das Installieren von Updates. |
| **ConfigurationName** | Diese Einstellung betrifft nur die Ausführung von Skripts.<br>Wenn Sie ein Skript vor dem Update oder ein Skript nach dem Update angeben, aber keinen **ConfigurationName**angeben, wird die standardmäßige Sitzungs Konfiguration für PowerShell (Microsoft. PowerShell) verwendet. | Gibt die PowerShell-Sitzungs Konfiguration an, die die Sitzung definiert, in der Skripts (angegeben durch **preupdatescript** und **postupdatescript**) ausgeführt werden, und die Befehle einschränken können, die ausgeführt werden können. |
| **CauPluginName** | **Microsoft.WindowsUpdatePlugin** | Plug-In, mit dem Sie das clusterfähige Aktualisieren konfigurieren, um eine Updatevorschau anzuzeigen oder eine Updateausführung vorzunehmen. Weitere Informationen finden Sie unter Funktionsweise von Plug-Ins für Cluster fähiges aktualisieren. |

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |
| **CauPluginArguments** | Keine | Ein Satz mit Paaren vom Typ *Name=Wert* (Argumenten) für das zu verwendende Update-Plug-In. Beispiel: **Domäne = Domäne. local**<br><br>Diese Paare vom Typ *Name=Wert* müssen für das in **CauPluginName** angegebene Plug-In verwertbar sein.<br><br>Zum Angeben eines Arguments mithilfe der Benutzeroberfläche für CAU geben Sie den *Namen*, ein, drücken die TAB-TASTE und geben dann den entsprechenden *Wert* ein. Drücken Sie erneut die TAB-TASTE, um das nächste Argument anzugeben. Jedes Paar aus *Name* und *Wert* wird automatisch durch ein Gleichheitszeichen getrennt. Mehrere Paare werden jeweils automatisch durch ein Semikolon getrennt.<br><br>Für das standardmäßige **Microsoft. windowsupdateplugin** -Plug-in sind keine Argumente erforderlich. Sie können jedoch ein optionales Argument angeben, z. B. zum Festlegen einer standardmäßigen Windows Update-Agent-Abfragezeichenfolge zum Filtern der Updates, die durch das Plug-In übernommen werden. Verwenden Sie *name*für einen Namen **QueryString**, und schließen Sie für einen *Wert*die gesamte Abfrage in Anführungszeichen ein.<br><br>Weitere Informationen finden Sie unter Funktionsweise von Plug-Ins für Cluster fähiges aktualisieren. |

## Optionen, die Sie beim Anfordern einer Update Laufzeit angeben

Die folgende Tabelle enthält Optionen, die Sie beim Anfordern einer Updateausführung angeben können und bei denen es sich nicht um Optionen eines Profils für die Updateausführung handelt Informationen zu den Optionen, die Sie in einem Profil für die Updateausführung festlegen können, finden Sie in der vorherigen Tabelle.

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |

| OPTION | STANDARDWERT | DETAILS |
| --- | --- | --- |
| **ClusterName** | Keine<br>**Hinweis:** Diese Option muss nur festgelegt werden, wenn die Benutzeroberfläche für Cluster fähiges aktualisieren nicht auf einem Failoverclusterknoten ausgeführt wird, oder wenn Sie auf einen Failovercluster verweisen möchten, der sich vom Standort der Cau-Benutzeroberfläche unterscheidet | Der NetBIOS-Name des Clusters, auf dem die Updateausführung erfolgen soll. |
| **Anmelde Informationen** | Aktuelle Kontoanmeldeinformationen | Die Administratoranmeldeinformationen für den Zielcluster, in dem die Updateausführung erfolgen soll. Möglicherweise verfügen Sie bereits über die erforderlichen Anmelde Informationen, wenn Sie die Cau-Benutzeroberfläche starten (oder eine PowerShell-Sitzung öffnen, wenn Sie die PowerShell-Cmdlets für Cau verwenden), von einem Konto, das über Administratorrechte und-Berechtigungen für den Cluster verfügt. |
| **NodeOrder** | Standardmäßig wird bei CAU mit dem Knoten begonnen, der die kleinste Anzahl von Clusterrollen besitzt. Danach folgen die Knoten mit der jeweils nächsthöheren Anzahl. | Die Namen der Clusterknoten in der Reihenfolge, in der sie aktualisiert werden sollten (sofern möglich). |

# Verwenden von Update Lauf Profilen

Jede Updateausführung kann einem bestimmten Profil für die Updateausführung zugeordnet werden. Das Standardprofil für die Profilerstellung wird im Ordner " *%windir%\Cluster* " gespeichert. Wenn Sie die Benutzeroberfläche für Cluster fähiges aktualisieren im Remote Aktualisierungs Modus verwenden, können Sie zum Zeitpunkt der Anwendung von Updates ein Profil für die Profilerstellung angeben, oder Sie können das Standardprofil für die Profilerstellung verwenden. Wenn Sie Cau im selbst Aktualisierungs Modus verwenden, können Sie die Einstellungen aus einem angegebenen Update Lauf Profil importieren, wenn Sie die selbst Aktualisierungs Optionen konfigurieren. In beiden Fällen können Sie bei Bedarf die angezeigten Werte für die Updateausführungsoptionen überschreiben. Die Updateausführungsoptionen können unter demselben oder einem anderen Dateinamen als Profil für die Updateausführung gespeichert werden. Wenn Sie das nächste Mal Updates übernehmen oder Selbstaktualisierungsoptionen konfigurieren, wählt CAU automatisch das zuvor ausgewählte Profil für die Updateausführung aus.

Sie können ein vorhandenes Update Testlauf-Profil ändern oder ein neues Profil erstellen, indem Sie auf der Cau-Benutzeroberfläche die Option **Update-Lauf Profil erstellen oder ändern** auswählen

Im folgenden finden Sie einige wichtige Hinweise zur Verwendung von Update Lauf Profilen:

- Bei einem Update Lauf Profil werden keine Cluster spezifischen Informationen, wie z. b. administrative Anmelde Informationen, gespeichert. Wenn Sie Cau im selbst Aktualisierungs Modus verwenden, speichert das Profil für die Update Ausführung auch keine Informationen zum selbst Aktualisierungs Zeitplan. Dies ermöglicht die Freigabe eines Profils für die Updateausführung in allen Failoverclustern in einer bestimmten Klasse.
- Wenn Sie selbst Aktualisierungs Optionen mithilfe eines Profils für die Update Laufzeit konfigurieren und das Profil später mit anderen Werten für die Update Lauf Optionen ändern, ändert sich die selbst Aktualisierungs

Konfiguration nicht automatisch. Sie müssen die Selbstaktualisierungsoptionen erneut konfigurieren, damit die neuen Einstellungen für die Updateausführung übernommen werden.

- Der Run profile Editor unterstützt leider keine Dateipfade, die Leerzeichen enthalten, z. b. " *c:\Programme*". Um dieses Problem zu umgehen, speichern Sie Ihre Pre-und Post-Update Skripts in einem Pfad, der keine Leerzeichen enthält, oder verwenden Sie PowerShell ausschließlich zum Verwalten von Lauf Profilen, indem Sie beim Ausführen von " **aufrufen-caurun**" die Anführungszeichen

**Gleichwertige Windows PowerShell-Befehle**

Sie können die Einstellungen aus einem Profil für die Update Ausführung importieren, wenn Sie das Cmdlet " **Aufruf-caurun**", " **Add-cauclusterrole**" oder " **Set-cauclusterrole** " ausführen.

Im folgenden Beispiel wird ein Scan und eine vollständige Updateausführung auf dem Cluster *CONTOSO-FC1* durchgeführt. Dazu werden die in *C:\Windows\Cluster\DefaultParameters.xml* festgelegten Updateausführungsoptionen verwendet. Für die übrigen Cmdlet-Parameter werden Standardwerte verwendet.

```
$MyRunProfile = Import-Clixml C:\Windows\Cluster\DefaultParameters.xml
Invoke-CauRun –ClusterName CONTOSO-FC1 @MyRunProfile
```

Durch die Verwendung eines Profils für die Updateausführung können Sie ein Failovercluster wiederholt mit einheitlichen Einstellungen für die Ausnahmenverwaltung, Zeitbindungen und weitere Betriebsparameter aktualisieren. Da diese Einstellungen in der Regel für eine Klasse von Failoverclustern spezifisch sind – z. b. "alle Microsoft SQL Server Cluster" oder "meine unternehmenskritischen Cluster" – können Sie jedes Profil für die Profilerstellung entsprechend der Klasse der Failovercluster benennen, mit der es verwendet wird. Außerdem sollten Sie das Profil für die Updateausführung in einer Dateifreigabe verwalten, die für alle Failovercluster einer bestimmten Klasse in Ihrer IT-Organisation zugänglich ist.

# Weitere Informationen

- Clusterfähiges Aktualisieren
- Cmdlets für clusterfähiges Aktualisieren in Windows PowerShell

# Clusterfähiges Aktualisieren: Häufig gestellte Fragen

09.04.2020 • 21 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Das Cluster fähige aktualisieren (Cau-) ist ein Feature, das Software Updates auf allen Servern in einem Failovercluster auf eine Art und Weise koordiniert, die sich nicht mehr auf die Dienst Verfügbarkeit auswirkt als ein Geplantes Failover eines Cluster Knotens. Bei einigen Anwendungen mit Features für die kontinuierliche Verfügbarkeit (z. b. Hyper-V mit Live Migration oder ein SMB 3. x-Dateiserver mit SMB transparent Failover), kann mit Cau die automatisierte Cluster Aktualisierung ohne Auswirkung auf die Dienst Verfügbarkeit koordiniert werden.

## Unterstützt Cau das Aktualisieren von direkte Speicherplätze Clustern?

Ja. Cau unterstützt das Aktualisieren von direkte Speicherplätze Clustern unabhängig vom Bereitstellungstyp: hyperkonvergiert oder konvergiert. Insbesondere wird durch die Orchestrierung von Cau sichergestellt, dass das Anhalten der einzelnen Cluster Knoten darauf wartet, dass der zugrunde liegende Cluster Speicherplatz fehlerfrei ist.

## Kann CAU für Windows Server 2008 R2 oder Windows 7 verwendet werden?

Nein. Cau koordiniert den Cluster Aktualisierungs Vorgang nur auf Computern, auf denen Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 10, Windows 8.1 oder Windows 8 ausgeführt wird. Auf dem zu Aktualisier Ende Failovercluster muss Windows Server 2016, Windows Server 2012 R2 oder Windows Server 2012 ausgeführt werden.

## Ist Cau auf bestimmte Cluster Anwendungen beschränkt?

Nein. CAU ist der Typ der Clusteranwendung unbekannt. Cau ist eine externe Cluster-Update Lösung, die oberhalb der Clustering-APIs und PowerShell-Cmdlets angeordnet ist. Daher kann mit Cau die Aktualisierung für eine beliebige geclusterte Anwendung koordiniert werden, die in einem Windows Server-Failovercluster konfiguriert ist.

> **NOTE**
>
> Derzeit werden die folgenden geclusterten Arbeits Auslastungen für Cau getestet und zertifiziert: SMB, Hyper-V, DFS-Replikation, DFS-Namespaces, iSCSI und NFS.

## Unterstützt CAU Updates von Microsoft Update und Windows Update?

Ja. Standardmäßig wird Cau mit einem Plug-in konfiguriert, das den Windows Update-Agent (WUA-APIs) Hilfsprogramm-APIs auf den Cluster Knoten verwendet. Die WUA-Infrastruktur kann so konfiguriert werden, dass Sie auf Microsoft Update und Windows Update verweist oder (WSUS-) als Quelle für Updates Windows Server Update Services.

## Unterstützt CAU WSUS-Updates?

Ja. Standardmäßig wird Cau mit einem Plug-in konfiguriert, das den Windows Update-Agent (WUA-APIs) Hilfsprogramm-APIs auf den Cluster Knoten verwendet. Die WUA-Infrastruktur kann so konfiguriert werden, dass Sie auf Microsoft Update und Windows Update oder auf eine lokale Windows Server Update Services (WSUS-) Server als Quelle für Updates verweist.

## Können von CAU Updates von Versionen mit eingeschränkter Verteilung angewendet werden?

Ja. Eingeschränkte Verteilungs Releases (LDR-) Updates, auch Hotfixes genannt, werden nicht über Microsoft Update oder Windows Update veröffentlicht, sodass Sie nicht vom Windows Update-Agent heruntergeladen werden können (WUA) Plug-, das standardmäßig von Cau verwendet wird.

Cau enthält jedoch eine zweite Plug-in, die Sie zum Anwenden von Hotfixupdates auswählen können. Diese Hotfix-Plug-in können auch angepasst werden, um nicht-Microsoft-Treiber, Firmware und BIOS-Updates anzuwenden.

## Kann ich CAU verwenden, um kumulative Updates anzuwenden?

Ja. Wenn es sich bei den kumulativen Updates um Updates von Versionen mit allgemeiner Verteilung oder LDR-Updates handelt, können sie von CAU angewendet werden.

## Kann ich Updates planen?

Ja. CAU unterstützt die folgenden Aktualisierungsmodi, bei denen Updates jeweils geplant werden können:

**Selbst-Aktualisierung** Ermöglicht dem Cluster, sich selbst gemäß einem definierten Profil und einem regulären Zeitplan (z. b. während eines monatlichen Wartungs Fensters) zu aktualisieren. Sie können auch eine selbst-Aktualisierung bei Bedarf jederzeit ausführen. Zum Aktivieren des selbst-Aktualisierungs Modus müssen Sie dem Cluster die Cluster Rolle für Cluster fähiges aktualisieren hinzufügen. Die Self-Update-Funktion von Cau wird wie jede andere gruppierte Arbeitsauslastung ausgeführt und kann problemlos mit den geplanten und ungeplanten Failover eines updatekoordinatorcomputers zusammenarbeiten.

**Remote-Aktualisierung** Hiermit können Sie jederzeit auf einem Computer mit Windows oder Windows Server eine Update Ausführung starten. Sie können eine Update Ausführung über das Cluster fähige Aktualisierungs Fenster oder mithilfe des PowerShell-Cmdlets **Aufruf-caurun** starten. Remote-Aktualisierung ist der Standard Aktualisierungs Modus für Cau. Mit der Aufgabenplanung können Sie das Cmdlet Invoke-CauRun nach einem gewünschten Zeitplan auf einem Remotecomputer ausführen, bei dem es sich nicht um einen der Clusterknoten handelt.

## Können Updates geplant werden, die während einer Sicherung angewendet werden sollen?

Ja. In diesem Zusammenhang werden von Cau keine Einschränkungen auferlegt. Das Durchführen von Software Updates auf einem Server (mit den zugehörigen potenziellen Neustarts) während der Ausführung einer Server Sicherung ist jedoch keine bewährte Vorgehensweise. Beachten Sie, dass von CAU nur Cluster-APIs verwendet werden, um Ressourcenfailover und -failbacks zu bestimmen. Daher ist CAU der Serversicherungsstatus nicht bekannt.

## Kann Cau mit Configuration Manager arbeiten?

Cau ist ein Tool, das Software Updates auf einem Cluster Knoten koordiniert und Configuration Manager auch Server Software Updates ausführt. Es ist wichtig, diese Tools so zu konfigurieren, dass Sie keine überlappende Abdeckung derselben Server in einer Daten Center Bereitstellung haben, einschließlich der Verwendung unterschiedlicher Windows Server Update Services Server. Dadurch wird sichergestellt, dass das Ziel für die Verwendung von Cau nicht versehentlich besiegt wird, da Configuration Manager-gesteuerte Aktualisierung keine

Cluster Informationen enthält.

## Benötige ich Administratoranmeldeinformationen, um CAU auszuführen?

Ja. Zum Ausführen der CAU-Tools sind Administratoranmeldeinformationen auf dem lokalen Server oder das Benutzerrecht **Annehmen der Clientidentität nach Authentifizierung** auf dem lokalen Server oder Clientcomputer erforderlich, auf dem CAU ausgeführt wird. Zum Koordinieren von Softwareupdates auf den Clusterknoten sind für CAU jedoch Clusteradministratoranmeldeinformationen auf allen Knoten erforderlich. Obwohl die Cau-Benutzeroberfläche ohne die Anmelde Informationen gestartet werden kann, werden Sie zur Eingabe der Anmelde Informationen für den Cluster Administrator aufgefordert, wenn eine Verbindung mit einer Cluster Instanz hergestellt wird, um eine Vorschau

## Kann ich ein Skript für Cau erstellen?

Ja. Cau verfügt über PowerShell-Cmdlets, die einen umfangreichen Satz von Skript Optionen bieten. Dies sind dieselben Cmdlets, die von der CAU-Benutzeroberfläche zum Ausführen von CAU-Aktionen aufgerufen werden.

## Was geschieht mit aktiven Cluster Rollen?

Cluster Rollen (früher als Anwendungs-und Dienst) bezeichnet, die auf einem Knoten aktiv sind, führen ein Failover auf andere Knoten aus, bevor die Software Aktualisierung beginnen kann. Diese Failover werden von CAU mithilfe des Wartungsmodus koordiniert, der den Knoten anhält und alle aktiven Clusterrollen auf ihm ausgleicht. Wenn die Softwareupdates abgeschlossen sind, wird der Knoten durch CAU fortgesetzt, und für die Clusterrollen wird ein Failback auf den aktualisierten Knoten ausgeführt. Dadurch wird sichergestellt, dass die Verteilung von Clusterrollen im Vergleich zu den Knoten bei den CAU-Aktualisierungsausführungen auf einem Cluster gleich bleibt.

## Wie werden Zielknoten für Cluster Rollen von Cau ausgewählt?

Von CAU werden Cluster-APIs verwendet, um die Failover zu koordinieren. Die Clustering-API-Implementierung wählt die Zielknoten aus, indem Sie sich auf interne Metriken und eine intelligente Platzierungs-Heuristik (wie Arbeits Auslastungs Ebenen) auf den Zielknoten.

## Führt der Cau-Lastenausgleich für die Cluster Rollen aus?

Cau führt keinen Lastenausgleich für die gruppierten Knoten durch, sondern versucht, die Verteilung der Cluster Rollen beizubehalten. Wenn das Update eines Clusterknotens durch CAU beendet wird, wird für die zuvor auf dem jeweiligen Knoten gehosteten Clusterrollen ein Failback ausgeführt. Von CAU werden Cluster-APIs verwendet, um für die Ressourcen ein Failback zum Anfang des angehaltenen Vorgangs auszuführen. Wenn keine ungeplanten Failover und bevorzugten Besitzereinstellungen vorhanden sind, bleibt die Verteilung der Clusterrollen daher unverändert.

## Wie wird von CAU die Reihenfolge der zu aktualisierenden Knoten ausgewählt?

Standardmäßig wird die Reihenfolge der zu aktualisierenden Knoten von CAU basierend auf dem Aktivitätsgrad ausgewählt. Die Knoten, auf denen die wenigsten Clusterrollen gehostet werden, werden zuerst aktualisiert. Ein Administrator kann jedoch eine bestimmte Reihenfolge für die Aktualisierung der Knoten angeben, indem er auf der Cau-Benutzeroberfläche einen Parameter für die Aktualisierungs Laufzeit oder mithilfe der PowerShell-Cmdlets angibt.

## Was geschieht, wenn ein Cluster Knoten offline ist?

Der Administrator, der die Aktualisierungsausführung initiiert, kann den zulässigen Schwellenwert für die Anzahl von Knoten angeben, die offline sein können. Daher kann eine Aktualisierungsausführung selbst dann auf einem Cluster fortgesetzt werden, wenn keiner der Clusterknoten online ist.

## Kann ich Cau verwenden, um nur einen einzelnen Knoten zu aktualisieren?

Nein. Cau ist ein Cluster-Tool für das Bereichs bezogene Update, sodass Sie nur zu Aktualisier Ende Cluster auswählen können. Wenn Sie einen einzelnen Knoten aktualisieren möchten, können Sie vorhandene Serveraktualisierungstools außerhalb von CAU verwenden.

## Können von Cau Updates gemeldet werden, die außerhalb von Cau initiiert wurden?

Nein. Von CAU können nur Aktualisierungsausführungen gemeldet werden, die innerhalb von CAU initiiert wurden. Wenn jedoch eine nachfolgende Cau-Aktualisierungs Laufzeit gestartet wird, werden Updates, die über nicht-Cau-Methoden installiert wurden, entsprechend berücksichtigt, um die zusätzlichen Updates zu bestimmen, die möglicherweise für die einzelnen Cluster Knoten gelten.

## Kann Cau meine individuellen Anforderungen an IT-Prozesse unterstützen?

Ja. CAU bietet die folgenden Dimensionen der Flexibilität, um den individuellen IT-Prozessanforderungen von Unternehmenskunden gerecht zu werden:

**Skripts** Bei einer Update-Lauf Zeit kann ein PowerShell-Skript vor-Update und ein PowerShell-Skript nach-Aktualisierung angegeben werden. Das Skript Pre-Update wird auf jedem Cluster Knoten ausgeführt, bevor der Knoten angehalten wird. Nachdem die Knoten Updates installiert wurden, wird das Skript nach-Aktualisierung auf jedem Cluster Knoten ausgeführt.

> **NOTE**
>
> .NET Framework 4,6 oder 4,5 und PowerShell müssen auf jedem Cluster Knoten installiert sein, auf dem Sie das Pre-Update ausführen und-Update Skripts ausführen möchten. Außerdem müssen Sie PowerShell-Remoting auf den Cluster Knoten aktivieren. Ausführliche Informationen zu den Systemanforderungen finden Sie unter Anforderungen und bewährte Methoden für das Cluster fähige aktualisieren.

**Erweiterte Aktualisierungs Lauf Optionen** Der Administrator kann zusätzlich einen umfangreichen Satz von erweiterten Optionen für die Aktualisierungs Laufzeit angeben, z. b. die maximale Anzahl von Wiederholungs versuchen für den Update Vorgang auf jedem Knoten. Diese Optionen können entweder über die Cau-Benutzeroberfläche oder über die PowerShell-Cmdlets für Cau angegeben werden. Diese benutzerdefinierten Einstellungen können in einem Profil für die Updateausführung gespeichert und bei späteren Updateausführungen wiederverwendet werden.

**Öffentliches Plug-in der Architektur** Cau enthält Features zum Registrieren, Aufheben der Registrierung und Auswählen von Plug-ins. Cau wird mit zwei Standard-Plug-ins ausgeliefert: eine koordiniert den Windows Update Agent (WUA-)-APIs auf jedem Cluster Knoten. die zweite Anwendung wendet Hotfixes an, die manuell in eine Dateifreigabe kopiert werden, auf die die Cluster Knoten zugreifen können. Wenn ein Unternehmen besondere Anforderungen hat, die mit diesen beiden Plug-ins nicht erfüllt werden können, kann das Unternehmen gemäß der öffentlichen API-Spezifikation ein neues Cau-Plug-in erstellen. Weitere Informationen finden Sie unter Referenz für Cluster-fähiges Aktualisieren von Plug-.

Informationen zum Konfigurieren und Anpassen von Plug-ins für Cluster fähiges aktualisieren, um unterschiedliche Aktualisierungs Szenarien zu unterstützen, finden Sie unter Funktionsweise von Plug-ins.

## Wie kann ich die CAU-Vorschau- und -Aktualisierungsergebnisse exportieren?

Cau bietet Exportoptionen über die Befehls--Zeilen Schnittstelle und über die Benutzeroberfläche.

**Optionen für Befehls-Zeilen Schnittstelle:**

- Vorschau Ergebnisse mit dem PowerShell-Cmdlet- **Aufruf-causcan | ConvertTo-XML**. Ausgabe: XML
- Melden Sie Ergebnisse mit dem PowerShell-Cmdlet **-Aufruf-caurun | ConvertTo-XML**. Ausgabe: XML
- Berichts Ergebnisse mithilfe des PowerShell-Cmdlets **Get-caureport | Exportieren Sie-caureport**. Ausgabe: HTML, CSV

**Benutzeroberflächen Optionen:**

- Kopieren Sie die Berichtsergebnisse aus dem Bildschirm **Vorschau der Updates anzeigen**. Ausgabe: CSV
- Kopieren Sie die Berichtsergebnisse aus dem Bildschirm **Bericht generieren**. Ausgabe: CSV
- Exportieren Sie die Berichtsergebnisse aus dem Bildschirm **Bericht generieren**. Ausgabe: HTML

## Wie installiere ich CAU?

Eine CAU-Installation ist nahtlos in das Feature "Failoverclustering" integriert. CAU wird wie folgt installiert:

- Wenn das Failoverclustering auf einem Cluster Knoten installiert ist, wird das Cau-Windows-Verwaltungsinstrumentation (WMI-)-Anbieter automatisch installiert.
- Wenn das Feature Failoverclustering-Tools auf einem Server oder Client Computer installiert ist, werden die Benutzeroberfläche für das Cluster fähige aktualisieren und die PowerShell-Cmdlets automatisch installiert.

## Muss für Cau Komponenten auf den Cluster Knoten ausgeführt werden, die aktualisiert werden?

Für Cau muss kein Dienst auf den Cluster Knoten ausgeführt werden. Für Cau muss jedoch eine Softwarekomponente (der WMI-Anbieter) auf den Cluster Knoten installiert sein. Diese Komponente wird mit dem Feature Failoverclustering installiert.

Zum Aktivieren des selbst-Aktualisierungs Modus muss die Cluster Rolle für Cluster fähiges aktualisieren ebenfalls dem Cluster hinzugefügt werden.

## Worin besteht der Unterschied zwischen der Verwendung von Cau und VMM?

- System Center Virtual Machine Manager (VMM-) ist darauf ausgerichtet, nur Hyper-V-Cluster zu aktualisieren, während mit Cau beliebige Typen unterstützter Failovercluster, einschließlich Hyper-v-Cluster, aktualisiert werden können.
- VMM erfordert zusätzliche Lizenzen, während Cau für alle Windows Server lizenziert ist. Die CAU-Features, -Tools und -Benutzeroberfläche werden mit Failoverclusteringkomponenten installiert.
- Wenn Sie bereits eine System Center-Lizenz besitzen, können Sie VMM weiterhin verwenden, um Hyper-V-Cluster zu aktualisieren, da es eine integrierte Verwaltungs-und Software Aktualisierungs Funktion bietet.

- Cau wird nur auf Clustern unterstützt, auf denen Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 ausgeführt werden. VMM unterstützt auch Hyper-V-Cluster auf Computern, auf denen Windows Server 2008 R2 und Windows Server 2008 ausgeführt werden.

## Kann ich die Remote-Aktualisierung auf einem Cluster verwenden, der für die selbst-Aktualisierung konfiguriert ist?

Ja. Ein Failovercluster in einer selbst-Aktualisierungs Konfiguration kann mithilfe von Remote-aktualisieren bei-Bedarf aktualisiert werden, so wie Sie eine Windows Update Überprüfung jederzeit auf dem Computer erzwingen können, auch wenn Windows Update für die automatische Installation von Updates konfiguriert ist. Sie müssen jedoch sicherstellen, dass gerade keine Aktualisierungsausführung erfolgt.

## Kann ich meine Clusteraktualisierungseinstellung für mehrere Cluster wiederverwenden?

Ja. Von CAU werden einige Aktualisierungsausführungsoptionen unterstützt, mit denen das Verhalten der Aktualisierungsausführung beim Aktualisieren des Clusters bestimmt wird. Diese Optionen können als Aktualisierungsausführungsprofil gespeichert und für beliebige Cluster wiederverwendet werden. Es wird empfohlen, Ihre Einstellungen für Failovercluster mit ähnlichen Aktualisierungsanforderungen zu speichern und wiederzuverwenden. Beispielsweise können Sie für alle Microsoft SQL Server Cluster, die Geschäfts-kritische Dienste unterstützen, das Profil "Geschäfts-kritische SQL Server Cluster Update-Profilerstellung" erstellen.

## Wo ist der Cau-Plug-in der Spezifikation?

- Cluster-fähiges Aktualisieren von Plug-als Referenz
- Plug-in für Cluster fähiges aktualisieren (Plug-in Beispiel

## Siehe auch

- [Clusterfähige Aktualisierung – Übersicht-

# Funktionsweise von Plug-Ins für Cluster fähiges aktualisieren

02.05.2020 • 41 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Beim Cluster fähigen aktualisieren (Cluster-Aware Update , Cau) werden Plug-ins verwendet, um die Installation von Updates auf Knoten in einem Failovercluster zu koordinieren. Dieses Thema enthält Informationen zur Verwendung der integrierten-Plug--ins für Cluster fähiges aktualisieren oder-anderer Plug-ins, die Sie für Cau installieren.

## Installieren eines Plug--ins

Ein anderes-Plug-in als die Standard--Plug-ins, die mit (Cau **Microsoft. windowsupdateplugin** und **Microsoft. hotfixplugin** ) installiert werden, müssen separat installiert werden. Wenn Cau im selbst-Aktualisierungs Modus verwendet wird, muss-das Plug-in auf allen Cluster Knoten installiert werden. Wenn das Cluster fähige aktualisieren im Remote-Aktualisierungs Modus verwendet wird-, muss das Plug-in auf dem Remote Computer für den Update Koordinator installiert sein. Bei einem-Plug-in, das Sie installieren, sind möglicherweise zusätzliche Installationsanforderungen auf den einzelnen Knoten erforderlich.

Befolgen Sie zum Installieren-eines Plug-ins die Anweisungen des Plug--in-Herausgebers. Wenn Sie ein Plug--in mit Cau manuell registrieren möchten, führen Sie das Register-cauplugin- Cmdlet auf-jedem Computer aus, auf dem das Plug-in installiert ist.

## Plug--in-und Plug--in-Argumente angeben

**Angeben eines Plug--ins für Cluster fähiges aktualisieren**

In der Benutzeroberfläche für Cluster fähiges aktualisieren wählen Sie-ein Plug-in-aus einer Dropdown Liste-der verfügbaren Plug-ins aus, wenn Sie mit Cau die folgenden Aktionen ausführen:

- Anwenden von Updates auf Cluster
- Updatevorschau für Cluster
- Konfigurieren von selbst-Aktualisierungs Optionen für Cluster

Standardmäßig wählt Cau den Plug--in **Microsoft. windowsupdateplugin**aus. Sie können jedoch ein beliebiges Plug--in angeben, das in Cau installiert und registriert ist.

> **TIP**
> Auf der Benutzeroberfläche für Cluster fähiges aktualisieren können Sie nur ein einzelnes-Plug-in für Cluster fähiges aktualisieren angeben, das für die Vorschauversion oder die Anwendung von Updates während einer Update Laufzeit verwendet werden soll. Mithilfe der PowerShell-Cmdlets für Cluster fähiges aktualisieren können Sie ein oder mehrere Plug--ins angeben. Wenn Sie mehrere Arten von Updates auf dem Cluster installieren müssen, ist es in der Regel effizienter, mehrere Plug--ins in einer Update Laufzeit anzugeben, anstatt für jedes Plug--in eine separate Update-Laufzeit zu verwenden. Dadurch sind z. B. meist weniger Knotenneustarts erforderlich.

Mithilfe der in der folgenden Tabelle aufgeführten PowerShell-Cmdlets für Cluster fähiges aktualisieren können Sie ein oder mehrere Plug--ins für eine Update-oder Scanvorgang angeben, indem Sie den **– caupluginname** -

Parameter übergeben. Sie können mehrere Plug--in-Namen angeben, indem Sie Sie durch Kommas trennen. - Wenn Sie mehrere Plug-ins angeben, können Sie auch steuern, wie-sich die Plug-ins während einer Update Ausführung gegenseitig beeinflussen, indem Sie die ** -Parameter runpluginsseridal**, ** -stoponpluginfailure**und – **separatereboots** angeben. Weitere Informationen zur Verwendung mehrerer Plug--ins finden Sie unter den Links, die für die Cmdlet-Dokumentation in der folgenden Tabelle bereitgestellt werden.

| CMDLET | BESCHREIBUNG |
| --- | --- |
| Add-CauClusterRole | Fügt die Cluster Rolle für Cluster fähiges aktualisieren hinzu, die-dem angegebenen Cluster die selbst Aktualisierungs Funktion bereitstellt. |
| Invoke-CauRun | Prüft Clusterknoten auf geeignete Updates und installiert diese Updates über eine Updateausführung auf dem angegebenen Cluster. |
| Invoke-CauScan | Prüft Clusterknoten auf geeignete Updates und gibt eine Liste des ersten Updatesatzes zurück, der auf jeden Knoten des angegebenen Clusters angewendet werden würde. |
| Set-CauClusterRole | Legt Konfigurationseigenschaften für die Clusterrolle für clusterfähiges Aktualisieren auf dem angegebenen Cluster fest. |

Wenn Sie mithilfe dieser Cmdlets keinen Plug--in-Parameter für Cluster fähiges aktualisieren angeben, ist der Standardwert-der Plug-in **Microsoft. windowsupdateplugin**.

### Cau-Plug--in-Argumente angeben

Wenn Sie die Optionen) für die Aktualisierungs Laufzeit konfigurieren, können Sie ein oder mehrere *Name=-Wert* -Paare (angeben-, die für das ausgewählte Plug-in verwendet werden sollen. Auf der Benutzeroberfläche für clusterfähiges Aktualisieren können Sie z. B. wie folgt mehrere Argumente angeben:

**Name1=value1; Name2=Value2; Name3=Wert3**

Diese *Name=-Wert* -Paare müssen für das von-Ihnen angegebene Plug-in sinnvoll sein. Für einige Plug--ins sind die Argumente optional.

Die Syntax der Plug--in-Argumente für Cau befolgt diese allgemeinen Regeln:

- Mehrere *Name=-Wert* -Paare werden durch Semikolons getrennt.
- Ein Wert, der Leerzeichen enthält, ist in Anführungszeichen eingeschlossen, z. b.: **Name1="value with spaces"**.
- Die genaue Syntax des *Werts* hängt vom Plug--in ab.

Zum Angeben von-Plug-in-Argumenten mithilfe der Cau-PowerShell-Cmdlets, die den Parameter – **caupluginparameters** unterstützen, übergeben Sie einen Parameter in der Form:

**-Caupluginarguments @ {Name1=value1; Name2=Value2; Name3=Wert3}**

Sie können auch eine vordefinierte PowerShell-Hash Tabelle verwenden. Um Plug--in-Argumente für mehr als ein-Plug-in anzugeben, übergeben Sie mehrere Hash Tabellen mit Argumenten, die durch Kommas getrennt sind. Übergeben Sie die-Plug-in-Argumente-in der Plug-in-Reihenfolge, die in **caupluginname**angegeben ist.

### Angeben Optionaler-Plug-in-Argumente

Die Plug--ins, die von (Cau **Microsoft. windowsupdateplugin** und **Microsoft. hotfixplugin** ) installiert werden, bieten zusätzliche Optionen, die Sie auswählen können. Diese werden auf der Benutzeroberfläche für

Cluster fähiges aktualisieren auf der Seite **zusätzliche Optionen** angezeigt, nachdem Sie die Optionen für-die Update Ausführung für das Plug-in konfiguriert haben. Wenn Sie die PowerShell-Cmdlets für Cluster fähiges aktualisieren verwenden, werden diese Optionen als optionale-Plug-in-Argumente konfiguriert. Weitere Informationen finden Sie weiter unten in diesem Thema unter Verwenden von Microsoft.WindowsUpdatePlugin und Verwenden von Microsoft.HotfixPlugin.

## Verwalten von-Plug-Ins mithilfe von Windows PowerShell-Cmdlets

| CMDLET | BESCHREIBUNG |
| --- | --- |
| Get-CauPlugin | Ruft Informationen zu einem oder mehreren Software Update-Plug--ins ab, die auf dem lokalen Computer registriert sind. |
| Register-CauPlugin | Registriert ein Plug--in für Cau-Software Updates auf dem lokalen Computer. |
| Unregister-CauPlugin | Entfernt ein Software Update--Plug-in aus der Liste-der Plug-ins, die von Cau verwendet werden können. **Hinweis:** Die Registrierung-der Plug-ins, die mit (Cau **Microsoft. windowsupdateplugin** und **Microsoft. hotfixplugin** ) installiert werden, kann nicht aufgehoben werden. |

## Verwenden von "Microsoft. windowsupdateplugin"

Das Standard--Plug-in für Cau, **Microsoft. windowsupdateplugin**, führt die folgenden Aktionen aus:

- Das Plug-In steht in Kontakt mit dem Windows Update-Agent auf den einzelnen Knoten des Failoverclusters, um Updates für die Microsoft-Produkte anzuwenden, die auf den einzelnen Knoten ausgeführt werden.
- Installiert Cluster Updates direkt von Windows Update oder Microsoft Update oder von einem-lokalen Windows Server Update Services (WSUS) -Server.
- Installiert nur die ausgewählten, allgemeinen () Updates der releasereleaseversion. Standardmäßig wendet das Plug--in nur wichtige Software Updates an. Es ist keine Konfiguration erforderlich. Die Standardkonfiguration lädt wichtige Updates von allgemeinen Vertriebsversionen auf die einzelnen Knoten herunter und installiert sie.

> **NOTE**
> Wenn Sie andere Updates als die wichtigen Software Updates anwenden möchten, die Standard (mäßig ausgewählt werden, z). b. Treiber Updates, können-Sie einen optionalen Plug-in-Parameter konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Abfragezeichenfolge für den Windows Update-Agent.

**Requirements (Anforderungen)**

- Der Failovercluster und der Remote Update (Coordinator-) Computer müssen die Anforderungen für Cau und die Konfiguration erfüllen, die für die Remote Verwaltung in den Anforderungen und bewährten Methoden für Cauerforderlich ist.
- Lesen Sie die Empfehlungen für die Anwendung von Microsoft-Updates, und nehmen Sie dann alle erforderlichen Änderungen an der Microsoft-Updatekonfiguration für die Failoverclusterknoten vor.
- Um optimale Ergebnisse zu erzielen, wird empfohlen, dass Sie das Cluster (fähige aktualisieren) (Cau Best Practices Analyzer BPA) ausführen, um sicherzustellen, dass die Cluster-und Update Umgebung ordnungsgemäß für die Anwendung von Updates über Cau Weitere Informationen finden Sie unter Testen der Updatebereitschaft für clusterfähiges Aktualisieren.

> **NOTE**
> Updates, die das Akzeptieren von Microsoft-Lizenzbedingungen oder andere Benutzerinteraktionen erfordern, werden ausgeschlossen und müssen manuell installiert werden.

### Weitere Optionen

Optional können Sie die folgenden Plug--in-Argumente angeben, um die vom Plug--in angewendeten Updates zu vergrößern oder einzuschränken:

- Um das Plug--in so zu konfigurieren, dass zusätzlich zu wichtigen Updates auf den einzelnen Knoten Empfohlene Updates angewendet werden, aktivieren Sie auf der Cau-Benutzeroberfläche auf der Seite **zusätzliche Optionen** das Kontrollkästchen **Empfohlene Updates auf die gleiche Weise wie wichtige Updates erhalten** .
  Alternativ können Sie das Plug--in-Argument **' includerecommendedupdates '=(true** ) konfigurieren.
- Um das Plug--in so zu konfigurieren, dass die Typen von DDR-Updates gefiltert werden, die auf die einzelnen Cluster Knoten angewendet werden, geben Sie eine Abfrage-Zeichenfolge für den Windows Update-Agent mit einem **QueryString** - Weitere Informationen finden Sie unter Konfigurieren der Abfragezeichenfolge für den Windows Update-Agent.

### Konfigurieren der Abfragezeichenfolge für den Windows Update-Agent

Sie können ein Plug--in-Argument für das Standard--Plug-in, **Microsoft. windowsupdateplugin**, konfigurieren, das (aus einer) Abfrage Zeichenfolge für den Windows Update-Agent WUA besteht. Diese Anweisung verwendet die WUA-API, um eine oder mehrere Gruppen von Microsoft-Updates zu ermitteln, die auf Basis bestimmter Auswahlkriterien auf die einzelnen Knoten angewendet werden. Sie können mehrere Kriterien mithilfe einer logischen UND- oder ODER-Operation kombinieren. Die WUA-Abfrage Zeichenfolge wird wie-folgt in einem Plug-in-Argument angegeben:

**QueryString="Kriterium1=value1 and/or Criterion2=Value2 and/or..."**

**Microsoft.WindowsUpdatePlugin** wählt z. B. wichtige Updates automatisch mithilfe des Standardarguments **QueryString** aus, das mit den Kriterien **IsInstalled**, **Type**, **IsHidden** und **IsAssigned** erzeugt wird:

**QueryString=="isinstemmt 0 und=Type ' Software ' and IsHidden=0 and isassigned=1"**

Wenn Sie ein **QueryString** -Argument angeben, wird es anstelle des standardmäßigen **QueryString** -Arguments verwendet, das für das-Plug-in konfiguriert ist.

#### Beispiel 1

So konfigurieren Sie **ein QueryString** -Argument, das ein bestimmtes Update installiert, gemäß ID *-f6ce46c1-971c 43f9-a2aa-783df125f003*:

**QueryString="UpdateId=' f6ce46c1-971c-43F 9-a2aa-783df125f 003 ' und isinstemstem0="**

> **NOTE**
> Das vorherige Beispiel gilt für die Anwendung von Updates mithilfe des Assistenten-zum Aktualisieren von Cluster fähigen Updates. -Wenn Sie ein bestimmtes Update durch Konfigurieren von selbst Aktualisierungs Optionen über die Benutzeroberfläche für Cluster fähiges aktualisieren oder mithilfe des PowerShell-Cmdlets " **Add-cauclusterrole** " oder " **Set-cauclusterrole**" installieren möchten, müssen Sie den UpdateId-Wert mit zwei einfachen-Anführungszeichen formatieren:
>
> **QueryString="UpdateId=" "f6ce46c1-971c-43F 9-a2aa-783df125-ID" "und isinstemstemter=0"**

#### Beispiel 2

So konfigurieren Sie ein **QueryString**-Argument, das ausschließlich Treiber installiert

**QueryString="isinstemmt=0 und=Typ" Driver "und IsHidden=0"**

Weitere Informationen zu Abfrage Zeichenfolgen für das Standard--Plug-in, **Microsoft. windowsupdateplugin**, (zu den Suchkriterien (z. b. **isinstemmt**)) und zur Syntax, die Sie in die Abfrage Zeichenfolgen einschließen können, finden Sie im Abschnitt zu den Suchkriterien in der Windows Update Agent-API-Referenz (WUA).

## Verwenden von "Microsoft.HotfixPlugin"

Mit dem-Plug-in " **Microsoft. hotfixplugin** " können Microsoft Limited Distribution Release (LDR) - (Updates, die auch als Hotfixes bezeichnet werden,) und früher als "QFEs" bezeichnet, die Sie unabhängig herunterladen, um bestimmte Microsoft-Software Probleme zu beheben. Das Plug-in installiert Updates aus einem Stamm Ordner auf einer SMB-Dateifreigabe und kann auch so angepasst werden,-dass Sie nicht von Microsoft stammenden Treiber, Firmware und BIOS-Updates anwenden.

> **NOTE**
> In Knowledge Base-Artikeln können Hotfixes manchmal von Microsoft heruntergeladen werden, Sie werden jedoch auch nach-Bedarf für Kunden bereitgestellt.

**Requirements (Anforderungen)**

- Der Failovercluster und der Remote Update (Coordinator-) Computer müssen die Anforderungen für Cau und die Konfiguration erfüllen, die für die Remote Verwaltung in den Anforderungen und bewährten Methoden für Cauerforderlich ist.
- Lesen Sie hierzu Empfehlungen zur Verwendung von Microsoft.HotfixPlugin.
- Um optimale Ergebnisse zu erzielen, empfiehlt es sich, das BPA () -Modell von Cau Best Practices Analyzer auszuführen, um sicherzustellen, dass die Cluster-und Update Umgebung ordnungsgemäß für die Anwendung von Updates mithilfe von Cau konfiguriert sind. Weitere Informationen finden Sie unter Testen der Updatebereitschaft für clusterfähiges Aktualisieren.
- Rufen Sie die Updates vom Verleger ab, kopieren Sie Sie, oder extrahieren Sie Sie in einen (SMB) -Datei (Freigabe) -hotfixstamm Ordner der Server Message Block-Dateifreigabe, der mindestens SMB 2,0 unterstützt und auf die von allen Cluster (Knoten und dem Remote-Update Koordinator--Computer)aus zugegriffen werden kann, wenn Cau im Remote Aktualisierungs Modus verwendet wird. Weitere Informationen finden Sie weiter unten in diesem Thema unter Konfigurieren einer Hotfixstammordnerstruktur.

  > **NOTE**
  > Standardmäßig werden von diesem-Plug-in nur Hotfixes mit den folgenden Dateinamen Erweiterungen installiert: MSU, MSI und MSP.

- Kopieren Sie (die Datei "defaulthotfixconfig. xml", die im Ordner " **%\SystemRoot% System32\WindowsPowerShell\\v 1.0\modules clusterawareupdating** " auf einem Computer, auf dem die Cau-Tools installiert) sind, in dem hotfixstamm Ordner, den Sie erstellt haben und in dem Sie die Hotfixes extrahiert haben, bereitgestellt werden. Kopieren Sie die Konfigurationsdatei z. b. in * \ \den\Ordner myfileserver Hotfixes\root*.

> **NOTE**
> Für die Installation der meisten von Microsoft bereitgestellten Hotfixes und anderer Updates kann die standardmäßige Hotfixkonfigurationsdatei ohne Änderungen verwendet werden. Sie können die Konfigurationsdatei als erweiterte Aufgabe anpassen, wenn dies in Ihrem Szenario erforderlich ist. Die Konfigurationsdatei kann benutzerdefinierte Regeln enthalten, z. B. zum Behandeln von Hotfixdateien mit spezieller Erweiterung oder zum Definieren eines Verhaltens für bestimmte Beendigungsbedingungen. Weitere Informationen finden Sie weiter unten in diesem Thema unter Anpassen der Hotfixkonfigurationsdatei.

**Konfiguration**

Konfigurieren Sie die folgenden Einstellungen. Weitere Informationen finden Sie über die Links zu weiter unten in diesem Thema folgenden Abschnitten.

- Der Pfad zum freigegebenen Hotfixstammordner, der die anzuwendenden Updates und die Hotfixkonfigurationsdatei enthält. Sie können diesen Pfad über die Benutzeroberfläche für Cluster fähiges aktualisieren eingeben oder den **Pfad "=<hotfixrootfolderpath">** PowerShell-Plug--in-Argument konfigurieren.

> **NOTE**
> Sie können den hotfixstamm Ordner als lokalen Ordner Pfad oder als UNC-Pfad der Form * \ \Servername\Freigabe\rootfoldername*angeben. Es kann-ein Domänen basierter oder eigenständiger DFS-Namespace Pfad verwendet werden. Die Plug--in-Features, mit denen die Zugriffsberechtigungen in der hotfixkonfigurationsdatei überprüft werden, sind jedoch nicht mit einem DFS-Namespace Pfad kompatibel. Wenn Sie also eine konfigurieren, müssen Sie die Überprüfung der Zugriffsberechtigungen über die Benutzeroberfläche für Cluster fähiges aktualisieren oder durch-Konfigurieren des Plug in-Arguments **disableaclchecks=' true '** deaktivieren.

- Einstellungen auf dem Server, der den hotfixstamm Ordner hostet, um die entsprechenden Berechtigungen für den Zugriff auf den Ordner zu überprüfen und die Integrität der Daten sicher (zustellen, auf die über)SMB-Signaturen oder SMB-Verschlüsselung im SMB-Ordner zugegriffen wird Weitere Informationen finden Sie unter Einschränken des Zugriffs auf den Hotfixstammordner.

**Weitere Optionen**

- Konfigurieren Sie optional das Plug--in, damit die SMB-Verschlüsselung beim Zugriff auf Daten von der hotfixdateifreigabe erzwungen wird. Wählen Sie auf der Benutzeroberfläche für Cluster fähiges aktualisieren auf der Seite **zusätzliche Optionen** die Option **SMB-Verschlüsselung beim Zugriff auf hotfixstamm Ordner** anfordern aus, oder konfigurieren Sie das PowerShell-Plug--in-Argument **="true"** .

> **IMPORTANT**
> Sie müssen auf dem SMB-Server zusätzliche Konfigurationsschritte ausführen, um die SMB-Datenintegrität mithilfe der SMB-Signatur oder SMB-Verschlüsselung zu ermöglichen. Weitere Informationen finden Sie unter Schritt 4 in Einschränken des Zugriffs auf den Hotfixstammordner. Wenn Sie die Option zum Erzwingen der Verwendung der SMB-Verschlüsselung auswählen und der Hotfixstammordner nicht für den Zugriff mit SMB-Verschlüsselung konfiguriert ist, tritt bei der Updateausführung ein Fehler auf.

- Deaktivieren Sie optional die Standardprüfungen auf ausreichende Berechtigungen für den Hotfixstammordner und die Hotfixkonfigurationsdatei. Wählen Sie auf der Benutzeroberfläche für Cluster fähiges aktualisieren die Option **Prüfung auf Administrator Zugriff auf hotfixstamm Ordner und Konfigurationsdatei deaktivieren aus**, oder konfigurieren Sie das Plug--in-Argument **disableaclchecks=' true '** .
- Konfigurieren Sie optional das **hotfixinstallertimeoutminutes= ** -Argument, um anzugeben, wie lange das-

Hotfix-Plug-in auf die Rückgabe des hotfixinstallations Prozesses wartet. (Der Standardwert ist 30 Minuten. ) Wenn Sie z. b. einen Timeout Zeitraum von zwei Stunden angeben möchten, legen Sie **=hotfixinstallertimeoutminutes 120**fest.

- Konfigurieren Sie optional das Plug--in-Argument **hotfixconfigfilename = ** , um einen Namen für die hotfixkonfigurationsdatei anzugeben, die sich im hotfixstamm Ordner befindet. Wenn der Name nicht angegeben wird, lautet der Standardname "DefaultHotfixConfig.xml".

### Konfigurieren einer Hotfixstammordnerstruktur

Damit das Hotfix--Plug-in funktioniert, müssen Hotfixes-in einer klar definierten Struktur in einem hotfixstamm Ordner ()der SMB-Dateifreigabe gespeichert werden, und Sie müssen das Hotfix-Plug--in mit dem Pfad zum hotfixstamm Ordner über die Benutzeroberfläche für Cluster fähiges aktualisieren oder über die PowerShell-Cmdlets für Cau konfigurieren. Dieser Pfad wird als- **hotfixrootfolderpath** -Argument an das Plug-in übermittelt. Gemäß Ihrer Aktualisierungsanforderungen können Sie für den Hotfixstammordner eine von vielen Strukturen auswählen, wie in den folgenden Beispielen gezeigt. Dateien oder Ordner, die der Struktur nicht entsprechen, werden ignoriert.

#### Beispiel 1: Ordnerstruktur, die zum Anwenden von Hotfixes auf alle Cluster Knoten verwendet wird

Um anzugeben, dass Hotfixes für alle Cluster Knoten gelten, kopieren Sie Sie in einen Ordner mit dem Namen **cauhotfix_all** unter dem hotfixstamm Ordner. In diesem Beispiel wird-das Plug-in-Argument **hotfixrootfolderpath** auf * \ \myfileserver\Hotfixes\root*festgelegt. Der Ordner **cauhotfix_all** enthält drei Updates mit den Erweiterungen MSU, MSI und MSP, die auf alle Cluster Knoten angewendet werden. Die Namen der Updatedateien dienen nur zur Veranschaulichung.

> **NOTE**
>
> In diesem und den folgenden Beispielen wird die Hotfixkonfigurationsdatei mit dem Standardnamen "DefaultHotfixConfig.xml" am erforderlichen Speicherort im Hotfixstammordner angezeigt.

```
\\MyFileServer\Hotfixes\Root\
   DefaultHotfixConfig.xml
   CAUHotfix_All\
      Update1.msu
      Update2.msi
      Update3.msp
      ...
```

#### Beispiel 2: Ordnerstruktur, die verwendet wird, um bestimmte Updates nur auf einen bestimmten Knoten anzuwenden

Um Hotfixes anzugeben, die nur auf einen bestimmten Knoten angewendet werden, verwenden Sie unter dem Hotfixstammordner einen Unterordner mit dem Namen dieses Knotens. Verwenden Sie den NetBIOS-Namen des Clusterknotens, z. B. *ContosoNode1*. Verschieben Sie dann die Updates, die nur für diesen Knoten gelten, in diesen Unterordner. Im folgenden Beispiel wird-das Plug-in-Argument **hotfixrootfolderpath** auf * \ \myfileserver\Hotfixes\root*festgelegt. Updates im **cauhotfix_all** -Ordner werden auf alle Cluster Knoten angewendet, und *_Node1 Specific_Update. msu* wird nur auf *ContosoNode1*angewendet.

```
\\MyFileServer\Hotfixes\Root\
   DefaultHotfixConfig.xml
   CAUHotfix_All\
      Update1.msu
      Update2.msi
      Update3.msp
      ...
   ContosoNode1\
      Node1_Specific_Update.msu
      ...
```

**Beispiel für eine drei-Ordner-Struktur, die zum Anwenden von anderen Updates als MSU-, MSI-und MSP-Dateien verwendet wird**

Das Plug-In **Microsoft.HotfixPlugin** wendet standardmäßig nur Updates mit den Erweiterungen MSU, MSI oder MSP an. Bestimmte Updates können jedoch andere Erweiterungen aufweisen und somit andere Installationsbefehle erfordern. Möglicherweise müssen Sie ein Firmwareupdate mit der Erweiterung EXE auf einen Knoten in einem Cluster anwenden. Sie können den hotfixstamm Ordner mit einem Unterordner konfigurieren, der angibt, dass ein-bestimmter, nicht standardmäßiger Updatetyp installiert werden muss. Sie müssen auch eine entsprechende Ordnerinstallationsregel konfigurieren, die den Installationsbefehl im `<FolderRules>` -Element in der XML-Datei der Hotfixkonfiguration angibt.

Im folgenden Beispiel wird-das Plug-in-Argument **hotfixrootfolderpath** auf * \ \myfileserver\Hotfixes\root*festgelegt. Es werden verschiedene Updates auf alle Clusterknoten angewendet. Zusätzlich wird das Firmwareupdate *SpecialHotfix1.exe* mithilfe von *FolderRule1* auf *ContosoNode1* angewendet. Weitere Informationen zum Konfigurieren von *FolderRule1* in der Hotfixkonfigurationsdatei finden Sie später in diesem Abschnitt unter Anpassen der Hotfixkonfigurationsdatei.

```
\\MyFileServer\Hotfixes\Root\
   DefaultHotfixConfig.xml
   CAUHotfix_All\
      Update1.msu
      Update2.msi
      Update3.msp
      ...

   ContosoNode1\
      FolderRule1\
          SpecialHotfix1.exe
      ...
```

### Anpassen der Hotfixkonfigurationsdatei

Die Hotfixkonfigurationsdatei steuert, wie bestimmte Hotfixtypen von **Microsoft.HotfixPlugin** in einem Failovercluster installiert werden. Das XML-Schema für die Konfigurationsdatei wird in der Datei "HotfixConfigSchema.xsd" definiert, die sich im folgenden Ordner auf einem Computer befindet, auf dem die Tools für clusterfähiges Aktualisieren installiert sind:

#### Ordner "%\systemroot\% System32\WindowsPowerShell\v\1.0 modules clusterawareupdating"

Kopieren Sie die Beispielkonfigurationsdatei "DefaultHotfixConfig.xml" aus diesem Speicherort in den Hotfixstammordner, und nehmen Sie die entsprechenden Änderungen für Ihr Szenario vor, um die Hotfixkonfigurationsdatei anzupassen:

> **IMPORTANT**
> Für die Anwendung der meisten von Microsoft bereitgestellten Hotfixes und anderer Updates kann die standardmäßige Hotfixkonfigurationsdatei ohne Änderungen verwendet werden. Die Anpassung der Hotfixkonfigurationsdatei zählt nur in fortgeschrittenen Verwendungsszenarios zu den erforderlichen Aufgaben.

Standardmäßig definiert die XML-Datei der Hotfixkonfiguration die Installationsregeln und Beendigungsbedingungen für die folgenden beiden Kategorien von Hotfixes:

- Hotfixdateien mit Erweiterungen, die vom-Plug-in standardmäßig (installiert werden können. msu-, MSI- und MSP-Dateien).

  Diese sind als `<ExtensionRules>` -Elemente im `<DefaultRules>` -Element definiert. Für jeden standardmäßig unterstützten Dateityp gibt es ein `<Extension>` -Element. Die allgemeine XML-Struktur sieht wie folgt aus:

```
<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>
```

Wenn Sie bestimmte Updatetypen auf alle Clusterknoten in der Umgebung anwenden müssen, können Sie weitere `<Extension>` -Elemente definieren.

- Hotfix oder andere Update Dateien, bei denen es sich nicht um MSI-, MSU-oder MSP-Dateien handelt,-z. b. nicht von Microsoft stammende Treiber, Firmware und BIOS-Updates.

  Jeder nicht-standardmäßige Dateityp wird als `<Folder>` -Element im `<FolderRules>` -Element konfiguriert. Das Namensattribut des `<Folder>` -Elements muss mit dem Namen eines Ordners im Hotfixstammordner übereinstimmen, der Updates vom entsprechenden Typ enthalten wird. Der Ordner kann sich im Ordner " **cauhotfix_all** " oder in einem-Knoten spezifischen Ordner befinden. Wenn *FolderRule1* z. B. im Hotfixstammordner konfiguriert ist, konfigurieren Sie das folgende Element in der XML-Datei, damit es eine Installationsvorlage und Beendigungsbedingungen für die Updates in diesem Ordner definiert:

```
<FolderRules>
      <Folder name="FolderRule1">
        <!-- Template and ExitConditions elements for installation of updates in FolderRule1 follow --
>
         ...
      </Folder>
      ...
</FolderRules>
```

In der folgenden Tabelle werden die `<Template>` -Attribute und mögliche `<ExitConditions>` -Unterelemente beschrieben.

| `<Template>`-ATTRIBUT | BESCHREIBUNG |
|---|---|
| `path` | Der vollständige Pfad zum Installationsprogramm für den Dateityp, der im `<Extension name>` -Attribut definiert ist.<br>Verwenden Sie `$update$`, um den Pfad zu einer Updatedatei in der Hotfix-Stammordnerstruktur anzugeben. |
| `parameters` | Eine Zeichenfolge erforderlicher und optionaler Parameter für das Programm, das in `path` angegeben ist.<br>Verwenden Sie `$update$`, um einen Parameter anzugeben, der dem Pfad zu einer Updatedatei in der Hotfix-Stammordnerstruktur entspricht. |

| `<EXITCONDITIONS>`-UNTERELEMENT | BESCHREIBUNG |
| --- | --- |
| `<Success>` | Definiert mindestens einen Beendigungscode, der auf die erfolgreiche Ausführung des angegebenen Updates hinweist. Dies ist ein erforderliches Unterelement. |
| `<Success_RebootRequired>` | Definiert optional mindestens einen Beendigungscode, der darauf hinweist, dass das Update erfolgreich ausgeführt wurde und der Knoten neu gestartet werden muss. **Hinweis:** Optional kann das `<Folder>` -Element das `alwaysReboot` -Attribut enthalten. Wenn dieses Attribut festgelegt ist, zeigt es an, dass wenn ein von dieser Regel installiertes Hotfix einen der Beendigungscodes zurückgibt, die in `<Success>` definiert sind, dieser als `<Success_RebootRequired>` -Beendigungsbedingung interpretiert wird. |
| `<Fail_RebootRequired>` | Definiert optional mindestens einen Beendigungscode, der darauf hinweist, dass das Update nicht erfolgreich ausgeführt wurde und der Knoten neu gestartet werden muss. |
| `<AlreadyInstalled>` | Definiert optional mindestens einen Beendigungscode, der darauf hinweist, dass das angegebene Update nicht angewendet wurde, da es bereits installiert ist. |
| `<NotApplicable>` | Definiert optional mindestens einen Beendigungscode, der darauf hinweist, dass das angegebene Update nicht angewendet wurde, da es nicht für den Clusterknoten gilt. |

**IMPORTANT**

Ein Beendigungscode, der in `<ExitConditions>` nicht explizit definiert ist, wird bei einem Fehler des Updates interpretiert und der Knoten wird nicht neu gestartet.

### Einschränken des Zugriffs auf den Hotfixstammordner

Sie müssen verschiedene Schritte ausführen, um den SMB-Dateiserver und die -Dateifreigabe so zu konfigurieren, dass sie den Schutz der Dateien im Hotfixstammordner nur für den Zugriff im Kontext von **Microsoft.HotfixPlugin** unterstützen. Diese Schritte aktivieren verschiedene Features, die dabei helfen, mögliche Manipulationen an den Hotfixdateien zu verhindern, die möglicherweise den Failovercluster gefährden können.

Dies sind die Hauptschritte:

1. Identifizieren Sie das Benutzerkonto, das für Update Ausführungen mithilfe des Plug--ins verwendet wird.
2. Konfigurieren dieses Benutzerkontos in den erforderlichen Gruppen auf einem SMB-Dateiserver
3. Konfigurieren der Berechtigungen für den Zugriff auf den Hotfixstammordner
4. Konfigurieren der Einstellungen für die SMB-Datenintegrität
5. Aktivieren der Windows-Firewall-Regel auf dem SMB-Server

#### Schritt 1: Identifizieren Sie das Benutzerkonto, das für Update Ausführungen verwendet wird, indem Sie das-Hotfix-Plug-in verwenden.

Das Konto, das in Cau zum Überprüfen der Sicherheitseinstellungen beim Ausführen einer Update Ausführung mithilfe von **Microsoft. hotfixplugin** verwendet wird, hängt davon ab,-ob das Cluster fähige-aktualisieren im Remote Aktualisierungs Modus oder im selbst Aktualisierungs Modus verwendet wird:

- **Remote-Aktualisierungs Modus** Das Konto, das über Administratorrechte für den Cluster verfügt, um die Vorschau anzuzeigen und Updates anzuwenden.
- **Selbst-Aktualisierungs Modus** Der Name des virtuellen Computer Objekts, das in Active Directory für die Cluster Rolle für Cluster fähiges aktualisieren konfiguriert ist. Dies ist entweder der Name eines vorab bereitgestellten virtuellen Computerobjekts in Active Directory für die Clusterrolle für clusterfähiges Aktualisieren oder der Name, der von der Clusterrolle für clusterfähiges Aktualisieren generiert wird. Wenn Sie den Namen abrufen möchten, wenn er von Cau generiert wurde, führen Sie das PowerShell-Cmdlet **get-cauclusterrole** Cau aus. In der Ausgabe ist **ResourceGroupName** der Name des generierten virtuellen Computerobjektkontos.

**Schritt 2: Konfigurieren dieses Benutzerkontos in den erforderlichen Gruppen auf einem SMB-Dateiserver**

> **IMPORTANT**
> Sie müssen das für die Updateausführungen verwendete Konto als lokales Administratorkonto auf dem SMB-Server hinzufügen. Wenn dies aufgrund der Sicherheitsrichtlinien in Ihrer Organisation nicht zulässig ist, konfigurieren Sie dieses Konto auf dem SMB-Server mit den erforderlichen Berechtigungen, indem Sie das folgende Verfahren durchführen.

**So konfigurieren Sie ein Benutzerkonto auf dem SMB-Server**

1. Fügen Sie das für Updateausführungen verwendete Konto zur Gruppe „Distributed COM-Benutzer" sowie zu einer der folgenden Gruppen hinzu: Hauptbenutzer, Servervorgang oder Druck-Operator.
2. Starten Sie die WMI-Verwaltungskonsole auf dem SMB-Server, um die erforderlichen WMI-Berechtigungen für das Konto zu aktivieren. Starten Sie PowerShell, und geben Sie dann den folgenden Befehl ein:

   ```
   wmimgmt.msc
   ```

3. Klicken Sie in der Konsolen Struktur-mit der rechten Maustaste auf **WMI- (Steuerung lokal)**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf **Sicherheit**, und erweitern Sie dann **Stamm**.
5. Klicken Sie auf **CIMV2** und dann auf **Sicherheit**.
6. Fügen Sie das für Updateausführungen verwendete Konto zur Liste **Gruppen- oder Benutzernamen** hinzu.
7. Erteilen Sie dem für Updateausführungen verwendeten Konto die Berechtigungen **Methoden ausführen** und **Remoteaktivierung**.

**Schritt 3: Konfigurieren der Berechtigungen für den Zugriff auf den Hotfixstammordner**

Wenn Sie versuchen, Updates anzuwenden, prüft das Hotfix-Plug--in standardmäßig die Konfiguration der NTFS-Dateisystem Berechtigungen für den Zugriff auf den hotfixstamm Ordner. Wenn die Ordner Zugriffsberechtigungen nicht ordnungsgemäß konfiguriert sind, kann eine Update Ausführung mit dem Hotfix-Plug--in fehlschlagen.

Wenn Sie die Standardkonfiguration des Hotfix-Plug--ins verwenden, stellen Sie sicher, dass die Berechtigungen für den Ordner Zugriff den folgenden Anforderungen entsprechen.

- Die Gruppe "Benutzer" verfügt über die Berechtigung "Lesen".
- Wenn das Plug--in Updates mit der Erweiterung ". exe" anwendet, verfügt die Gruppe "Benutzer" über die Berechtigung "ausführen".
- Nur bestimmte Sicherheits Prinzipale sind zulässig () , aber Sie müssen nicht über die Berechtigung Schreiben oder ändern verfügen. Die zulässigen Prinzipale sind die Gruppe der lokalen Administratoren,

SYSTEM, ERSTELLER-BESITZER und TrustedInstaller. Anderen Konten oder Gruppen ist es nicht gestattet, die Berechtigung "Schreiben" oder "Ändern" für den Hotfixstammordner zu verwenden.

Optional können Sie die obigen Prüfungen deaktivieren, die vom Plug--in standardmäßig durchgeführt werden. Dazu haben Sie zwei Möglichkeiten:

- Wenn Sie die PowerShell-Cmdlets für Cluster fähiges aktualisieren verwenden, konfigurieren Sie das **disableaclchecks=' true '** -Argument im **caupluginarguments** -Parameter für-das Hotfix-Plug-in.
- Wenn Sie die Benutzeroberfläche für clusterfähiges Aktualisieren verwenden, wählen Sie die Option **Prüfung auf Administratorzugriff auf Hotfixstammordner und Konfigurationsdatei deaktivieren** auf der Seite **Weitere Updateoptionen** aus, die zum Konfigurieren der Optionen von Updateausführungen verwendet wird.

Es wird jedoch in vielen Umgebungen als bewährte Methode empfohlen, dass Sie diese Prüfungen mithilfe der Standardkonfiguration erzwingen.

#### Schritt 4. Konfigurieren der Einstellungen für die SMB-Datenintegrität

Zum Überprüfen der Datenintegrität in den Verbindungen zwischen den Cluster Knoten und der SMB-Dateifreigabe erfordert das Hotfix-Plug--in, dass Sie die Einstellungen auf der SMB-Dateifreigabe für die SMB-Signatur oder SMB-Verschlüsselung aktivieren. Die SMB-Verschlüsselung, die in vielen Umgebungen eine höhere Sicherheit und bessere Leistung bietet, wird ab Windows Server 2012 unterstützt. Sie können eine oder beide Einstellungen wie folgt aktivieren:

- Informationen zum Aktivieren der SMB-Signatur finden Sie unter dem Verfahren in der Microsoft Knowledge Base in Artikel 887429 .
- Um die SMB-Verschlüsselung für den freigegebenen SMB-Ordner zu aktivieren, führen Sie das folgende PowerShell-Cmdlet auf dem SMB-Server aus:

  ```
  Set-SmbShare <ShareName> -EncryptData $true
  ```

  Dabei gibt <*ShareName*> den Namen des freigegebenen SMB-Ordners an.

Um optional die Verwendung der SMB-Verschlüsselung in den Verbindungen mit dem SMB-Server zu erzwingen, wählen Sie auf der Benutzeroberfläche für Cluster fähiges aktualisieren die Option **SMB-Verschlüsselung beim Zugriff auf hotfixstamm Ordner** anfordern aus, oder konfigurieren Sie das-Plug-in-Argument **="true"** , indem Sie die PowerShell-Cmdlets für Cau verwenden.

> **IMPORTANT**
> Wenn Sie die Option zum Erzwingen der Verwendung der SMB-Verschlüsselung auswählen und der Hotfixstammordner nicht für Verbindungen konfiguriert ist, die die SMB-Verschlüsselung verwenden, tritt bei der Updateausführung ein Fehler auf.

#### Schritt 5: Aktivieren der Windows-Firewall-Regel auf dem SMB-Server

Sie müssen die **Dateiserver- (Remoteverwaltungs--) SMB in** der Regel in der Windows-Firewall auf dem SMB-Dateiserver aktivieren. Dies ist in Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012 standardmäßig aktiviert.

## Weitere Informationen

- Übersicht über das Cluster fähige aktualisieren
- Windows PowerShell-Cmdlets für das clusterfähige Aktualisieren

- Referenz zu Plug-Ins für clusterfähiges Aktualisieren

# Integritätsdienst in Windows Server

08.03.2020 • 8 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Der Integritätsdienst ist ein neues Feature in Windows Server 2016, das die tägliche Überwachung und Betriebsbereitschaft für Cluster mit direkte Speicherplätze verbessert.

## Erforderliche Komponenten

Für „Direkte Speicherplätze" ist der Integritätsdienst standardmäßig aktiviert. Für seine Einrichtung und seinen Start sind keine weiteren Aktionen erforderlich. Weitere Informationen zu direkte Speicherplätze finden Sie unter direkte Speicherplätze in Windows Server 2016.

## Berichte

Siehe Integritätsdienst Berichte.

## Fehler

Siehe Integritätsdienst Fehler.

## Aktionen

Siehe Integritätsdienst Aktionen.

## Automatisierung

Im nächsten Abschnitt werden Workflows beschrieben, die vom Integritätsdienst im Lebenszyklus von Datenträgern automatisiert werden.

### Lebenszyklus von Datenträgern

Der Integritätsdienst automatisiert die meisten Phasen des Lebenszyklus physischer Datenträger. Angenommen, der Ausgangsstatus Ihrer Bereitstellung ist eine perfekte Integrität, was heißt, dass alle physischen Datenträger ordnungsgemäß funktionieren.

#### Deaktivierung

Physische Datenträger werden automatisch deaktiviert, wenn sie nicht mehr verwendet werden können, woraufhin ein entsprechender Fehler ausgelöst wird. Es gibt mehrere Fälle:

- Medienfehler: Der physische Datenträger ist definitiv ausgefallen oder beschädigt und muss ausgetauscht werden.
- Kommunikationsverlust: Der physische Datenträger hatte 15 Minuten lang keine Verbindung.
- Keine Reaktion: Der physische Datenträger hatte binnen einer Stunde dreimal oder öfter eine Latenz von 5,0 Sekunden zu verzeichnen.

> **NOTE**
> Wenn die Verbindung mit zahlreichen physischen Datenträgern gleichzeitig bzw. mit einem gesamten Knoten oder Speichergehäuse verloren geht, werden diese Datenträger vom Integritätsdienst *nicht* deaktiviert, weil sie wahrscheinlich nicht die Ursache sind.

Wenn der deaktivierte Datenträger als Cache für viele andere physische Datenträger fungiert hat, werden diese, sofern verfügbar, automatisch einem anderen Cachedatenträger neu zugewiesen. Es ist keine spezielle Benutzeraktion erforderlich.

**Wiederherstellen der Ausfallsicherheit**

Nachdem ein physischer Datenträger deaktiviert wurde, beginnt der Integritätsdienst sofort mit dem Kopieren seiner Daten auf die restlichen physischen Datenträger, um die vollständige Ausfallsicherheit wiederherzustellen. Sobald dies abgeschlossen ist, sind die Daten vollständig sicher und wieder fehlertolerant.

> **NOTE**
> Die sofortige Wiederherstellung erfordert ausreichend verfügbare Kapazität auf den verbleibenden physischen Datenträgern.

**Blinken der Leuchte**

Falls möglich, aktiviert der Integritätsdienst das Blinken der Leuchte auf dem deaktivierten physischen Datenträger oder an seinem Steckplatz. Dies wird dauerhaft fortgesetzt, bis der deaktivierte Datenträger ausgetauscht wird.

> **NOTE**
> Mitunter kann der Datenträger ggf. auf eine Weise ausfallen, die selbst das Funktionieren der Leuchte verhindert, z. B. beim Totalausfall des Stroms.

**Physischer Austausch**

Nach Möglichkeit sollten Sie den deaktivierten physischen Datenträger austauschen. In den meisten Fällen besteht dies aus einem Hot-Swap-Vorgang, d. h., das Ausschalten des Knotens oder des Speicher Gehäuses ist nicht erforderlich. In den Informationen zum Fehler finden Sie hilfreiche Angaben zu Stelle und Teil.

**Überprüfung**

Wenn der Ersetzungs Datenträger eingefügt wird, wird er anhand des Dokuments "Unterstützte Komponenten" überprüft (Weitere Informationen finden Sie im nächsten Abschnitt).

**Pooling**

Falls zulässig, wird der Austauschdatenträger automatisch dem Pool seines Vorgängers hinzugefügt, um den Betrieb aufzunehmen. Sobald der Fehler verschwunden ist, wird das System in seinen Ausgangszustand mit perfekter Integrität zurückgesetzt.

# Dokument zu unterstützten Komponenten

Der Integritätsdienst stellt einen Erzwingungs Mechanismus bereit, mit dem die von direkte Speicherplätze verwendeten Komponenten auf die von dem Administrator oder dem Lösungs Hersteller bereitgestellten Komponenten beschränkt werden. Diese kann verwendet werden, um eine versehentliche Nutzung nicht unterstützter Hardware durch Sie oder andere zu verhindern, sodass Garantie- und Supportvertragsbedingungen besser eingehalten werden. Diese Funktion ist zurzeit auf physische Festplattengeräte beschränkt, einschließlich SSDs, HDDs und nvme-Laufwerke. Das Dokument "Unterstützte Komponenten" kann für das Modell, den Hersteller (optional) und die Firmwareversion (optional) eingeschränkt werden.

## Verwendung

Im Dokument "Unterstützte Komponenten" wird eine XML-inspirierte Syntax verwendet. Es wird empfohlen, Ihren

bevorzugten Text-Editor, z. b. die kostenlose Visual Studio Code oder den Editor, zum Erstellen eines XML-Dokuments zu verwenden, das Sie speichern und wieder verwenden können.

**Strecken**

Das Dokument weist zwei unabhängige Abschnitte auf: `Disks` und `Cache`.

Wenn der `Disks` Abschnitt angegeben ist, können nur die aufgeführten Laufwerke (wie `Disk`) mit Pools verknüpft werden. Nicht aufgelistete Laufwerke werden daran gehindert, Pools beizutreten, was die Verwendung in der Produktion praktisch ausschließt. Wenn dieser Abschnitt leer bleibt, wird jedem Laufwerk das beitreten zu Pools gestattet.

Wenn der `Cache` Abschnitt angegeben wird, werden nur die aufgeführten Laufwerke (wie `CacheDisk`) für die Zwischenspeicherung verwendet. Wenn dieser Abschnitt leer bleibt, versucht direkte Speicherplätze, basierend auf Medientyp und Bustyp zu erraten. Die hier aufgeführten Laufwerke sollten auch unter `Disks` aufgeführt werden.

> **IMPORTANT**
>
> Das Dokument "Unterstützte Komponenten" gilt nicht rückwirkend für bereits in einem Pool zusammengefasste und verwendete Laufwerke.

**Beispiel**

```
<Components>

  <Disks>
    <Disk>
      <Manufacturer>Contoso</Manufacturer>
      <Model>XYZ9000</Model>
      <AllowedFirmware>
        <Version>2.0</Version>
        <Version>2.1</Version>
        <Version>2.2</Version>
      </AllowedFirmware>
      <TargetFirmware>
        <Version>2.1</Version>
        <BinaryPath>C:\ClusterStorage\path\to\image.bin</BinaryPath>
      </TargetFirmware>
    </Disk>
    <Disk>
      <Manufacturer>Fabrikam</Manufacturer>
      <Model>QRSTUV</Model>
    </Disk>
  </Disks>

  <Cache>
    <CacheDisk>
      <Manufacturer>Fabrikam</Manufacturer>
      <Model>QRSTUV</Model>
    </CacheDisk>
  </Cache>

</Components>
```

Fügen Sie zum Auflisten mehrerer Laufwerke einfach zusätzliche `<Disk>` oder `<CacheDisk>` Tags hinzu.

Um diese XML-Datei beim Bereitstellen von direkte Speicherplätze einzufügen, verwenden Sie den Parameter `-XML`:

```
$MyXML = Get-Content <Filepath> | Out-String
Enable-ClusterS2D -XML $MyXML
```

So können Sie das Dokument "Unterstützte Komponenten" nach der Bereitstellung direkte Speicherplätze festlegen oder ändern:

```
$MyXML = Get-Content <Filepath> | Out-String
Get-StorageSubSystem Cluster* | Set-StorageHealthSetting -Name "System.Storage.SupportedComponents.Document" -
Value $MyXML
```

> **NOTE**
> Die Eigenschaften „Model", „Manufacturer" und „FirmwareVersion" müssen exakt mit den Werten übereinstimmen, die Sie mit dem Cmdlet **Get-PhysicalDisk** abrufen. Je nach Implementierung des Herstellers weichen diese von Ihren Erwartungen ab. Anstatt „Contoso" kann der Hersteller (Manufacturer) „CONTOSO-LTD" heißen, oder dieser Eintrag ist leer, während das Modell „Contoso-XZY9000" ist.

Sie können dies mit dem folgenden PowerShell-Cmdlet überprüfen:

```
Get-PhysicalDisk | Select Model, Manufacturer, FirmwareVersion
```

## Einstellungen

Siehe Integritätsdienst Einstellungen.

## Siehe auch

- Integritätsdienst Berichte
- Integritätsdienst Fehler
- Integritätsdienst Aktionen
- Integritätsdienst Einstellungen
- Direkte Speicherplätze in Windows Server 2016

# Integritätsdienst Berichte

02.05.2020 • 8 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

## Was sind Berichte?

Der-Integritätsdienst reduziert den Aufwand, der erforderlich ist, um Informationen über die Leistung und die Kapazität Ihres direkte Speicherplätze Clusters zu erhalten. Ein neues Cmdlet bietet eine Liste mit wichtigen Metriken, die effizient gesammelt und dynamisch über Knoten aggregiert werden, mit integrierter Logik zum Erkennen der Cluster Mitgliedschaft. Alle Werte sind in Echtzeit und ausschließlich zeitpunktbezogen.

## Verwendung in PowerShell

Verwenden Sie dieses Cmdlet, um Metriken für den gesamten direkte Speicherplätze Cluster zu erhalten:

```
Get-StorageSubSystem Cluster* | Get-StorageHealthReport
```

Der optionale **count** -Parameter gibt an, wie viele Sätze von Werten in Intervallen von einer Sekunde zurückgegeben werden.

```
Get-StorageSubSystem Cluster* | Get-StorageHealthReport -Count <Count>
```

Sie können auch Metriken für ein bestimmtes Volume oder einen bestimmten Server erhalten:

```
Get-Volume -FileSystemLabel <Label> | Get-StorageHealthReport -Count <Count>

Get-StorageNode -Name <Name> | Get-StorageHealthReport -Count <Count>
```

## Verwendung in .net und C #

**Verbinden**

Um den Integritätsdienst abzufragen, müssen Sie eine **cimsession** mit dem Cluster einrichten. Zu diesem Zweck benötigen Sie einige Dinge, die nur in der Vollversion von .net verfügbar sind, was bedeutet, dass Sie dies nicht direkt über ein Web oder Mobile App durchführen können. Diese Codebeispiele verwenden C#, die einfachste Wahl für diese Datenzugriffs Schicht.

```
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;
}
```

Der angegebene Benutzername muss ein lokaler Administrator des Bereitstellungs Ziel Computers sein.

Es wird empfohlen, dass Sie das Kennwort **SecureString** direkt aus Benutzereingaben in Echtzeit erstellen, damit Ihr Kennwort niemals im Klartext in Klartext gespeichert wird. Dies trägt dazu bei, eine Vielzahl von Sicherheitsrisiken zu verringern. In der Praxis ist es jedoch üblich, diese wie oben beschrieben zu erstellen.

**Objekte ermitteln**

Nachdem die **cimsession** eingerichtet wurde, können Sie Windows-Verwaltungsinstrumentation (WMI) im Cluster Abfragen.

Bevor Sie Fehler oder Metriken erhalten können, müssen Sie Instanzen von mehreren relevanten Objekten erhalten. Zuerst das **MSFT_storagesubsystem** , das direkte Speicherplätze im Cluster darstellt. Mit diesem können Sie jede **_MSFT storagenode** -Instanz im Cluster und alle **MSFT_**-Volumes, die Datenvolumes, erhalten. Schließlich benötigen Sie auch **MSFT_storagehealth**, den Integritätsdienst selbst.

```
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();
}
```

Dabei handelt es sich um dieselben Objekte, die Sie in PowerShell mithilfe von Cmdlets wie " **Get-**

**storagesubsystem**", " **Get-storagenode**" und " **Get-Volume**" erhalten.

Sie können auf die gleichen Eigenschaften zugreifen, die unter Klassen der Speicher Verwaltungs-APIdokumentiert sind.

```
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());
}
```

Rufen Sie **GetReport** auf, um mit dem Streamen von Beispielen für eine vom Experten zusammengestellte Liste mit wichtigen Metriken zu beginnen, die effizient gesammelt und dynamisch über Knoten aggregiert werden, mit integrierter Logik zum Erkennen der Cluster Mitgliedschaft. Die Beispiele werden anschließend jede Sekunde empfangen. Alle Werte sind in Echtzeit und ausschließlich zeitpunktbezogen.

Metriken können für drei Bereiche gestreamt werden: Cluster, Knoten oder beliebiges Volume.

Die komplette Liste der Metriken, die in jedem Bereich in Windows Server 2016 verfügbar sind, ist unten dokumentiert.

### IObserver. OnNext ()

In diesem Beispielcode wird das Observer-Entwurfsmuster zum Implementieren eines Beobachters verwendet, dessen **OnNext ()** -Methode aufgerufen wird, wenn jedes neue metrikbeispiel erreicht wird. Die zugehörige **onabgeschlossene ()** -Methode wird beim Beenden des Streamings aufgerufen. Beispielsweise können Sie es verwenden, um das Streaming erneut zu initiieren, sodass es unbegrenzt fortgesetzt wird.

```
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
    }
}
```

### Streaming starten

Wenn der Observer definiert ist, können Sie mit dem Streaming beginnen.

Geben Sie die Ziel- **ciminstance** an, für die Sie die Metriken festlegen möchten. Dabei kann es sich um den Cluster, einen beliebigen Knoten oder ein beliebiges Volume handeln.

Der count-Parameter entspricht der Anzahl von Samplings, bevor das Streaming beendet wird.

```
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);
}
```

Natürlich können diese Metriken visualisiert, in einer Datenbank gespeichert oder in der gewünschten Weise verwendet werden.

**Eigenschaften von Berichten**

Jede Stichprobe von Metriken ist ein "Bericht", der viele "Datensätze" enthält, die einzelnen Metriken entsprechen.

Überprüfen Sie für das vollständige Schema die Klassen **_MSFT storagehealthreport** und **MSFT_healthrecord** in *storagewmi. MOF*.

Jede Metrik hat pro dieser Tabelle nur drei Eigenschaften.

| EIGENSCHAFT | BEISPIEL |
|---|---|
| Name | Iolatencyaverage |
| Wert | 0,00021 |
| Units | 3 |

Einheiten = {0, 1, 2, 3, 4}, wobei 0 = "Bytes", 1 = "bytespersecond", 2 = "count-persecond", 3 = "seconds" oder 4 = "Prozentsatz".

# Abdeckung

Im folgenden finden Sie die verfügbaren Metriken für jeden Bereich in Windows Server 2016.

**MSFT_StorageSubSystem**

| NAME | UNITS |
|---|---|
| CPUUsage | 4 |
| Capacityphysicalpooledavailable | 0 |
| Capacityphysicalpooledtotal | 0 |
| Capacityphysicaltotal | 0 |

| NAME | UNITS |
| --- | --- |
| Capacityphysicalunpooled | 0 |
| Capacityvolumesavailable | 0 |
| Capacityvolumestotal | 0 |
| Iolatencyaverage | 3 |
| Iolatencyread | 3 |
| Iolatencywrite | 3 |
| Iopsread | 2 |
| Iopstotal | 2 |
| Iopswrite | 2 |
| Iodurchputread | 1 |
| Iodurchlauf puttotal | 1 |
| Iothrough putwrite | 1 |
| Memoryavailable | 0 |
| MemoryTotal | 0 |

### MSFT_StorageNode

| NAME | UNITS |
| --- | --- |
| CPUUsage | 4 |
| Iolatencyaverage | 3 |
| Iolatencyread | 3 |
| Iolatencywrite | 3 |
| Iopsread | 2 |
| Iopstotal | 2 |
| Iopswrite | 2 |
| Iodurchputread | 1 |
| Iodurchlauf puttotal | 1 |

| NAME | UNITS |
| --- | --- |
| Iothrough putwrite | 1 |
| Memoryavailable | 0 |
| MemoryTotal | 0 |

**MSFT_Volume**

| NAME | UNITS |
| --- | --- |
| Verfügbare Kapazität | 0 |
| Capacitytotal | 0 |
| Iolatencyaverage | 3 |
| Iolatencyread | 3 |
| Iolatencywrite | 3 |
| Iopsread | 2 |
| Iopstotal | 2 |
| Iopswrite | 2 |
| Iodurchputread | 1 |
| Iodurchlauf puttotal | 1 |
| Iothrough putwrite | 1 |

# Weitere Informationen

- Der Integritätsdienst in Windows Server 2016

# Integritätsdienst Fehler

02.05.2020 • 24 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

## Was sind Fehler?

Der Integritätsdienst überwacht ständig ihren direkte Speicherplätze Cluster, um Probleme zu erkennen und "Fehler" zu generieren. Mit einem neuen Cmdlet werden alle aktuellen Fehler angezeigt, sodass Sie die Integrität Ihrer Bereitstellung problemlos überprüfen können, ohne dass Sie die einzelnen Entitäten oder Features nacheinander betrachten müssen. Fehler sind auf Präzision, leichte Verständlichkeit und Umsetzbarkeit ausgelegt.

Jeder Fehler enthält fünf wichtige Felder:

- severity
- Beschreibung des Problems
- Empfohlene nächste Schritte zum Beheben des Problems
- Identifizierende Informationen zur fehlerbehafteten Entität
- Die physische Stelle (falls zutreffend)

Es folgt ein Beispiel eines typischen Fehlers:

```
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**
> Die physische Stelle wird von der Konfiguration der Fehlerdomäne abgeleitet. Weitere Informationen zu Fehler Domänen finden Sie unter Fehler Domänen in Windows Server 2016. Wenn Sie diese Informationen nicht angeben, ist das Feld mit der Stelle weniger hilfreich, sodass z. B. nur die Steckplatznummer angezeigt wird.

## Analyse der Grundursache

Der Integritätsdienst kann die potenzielle Kausalität zwischen fehlerentitäten einschätzen, um Fehler zu identifizieren und zu kombinieren, die Folgen desselben zugrunde liegenden Problems sind. Durch erkennen von Kausalketten ergeben sich kürzere Berichte. Wenn ein Server z. b. herunterfährt, wird erwartet, dass er auch keine Konnektivität hat. Daher wird nur ein Fehler für die Grundursache ausgelöst, in diesem Fall der Server.

## Verwendung in PowerShell

Um aktuelle Fehler in PowerShell anzuzeigen, führen Sie dieses Cmdlet aus:

```
Get-StorageSubSystem Cluster* | Debug-StorageSubSystem
```

Dadurch werden alle Fehler zurückgegeben, die sich auf den gesamten direkte Speicherplätze Cluster auswirken. In den meisten Fällen beziehen sich diese Fehler auf die Hardware oder die Konfiguration. Wenn keine Fehler

vorliegen, gibt dieses Cmdlet nichts zurück.

> **NOTE**
> In einer nicht Produktionsumgebung können Sie mit dieser Funktion experimentieren, indem Sie Fehler selbst auslösen, z. b. durch Entfernen eines physischen Datenträgers oder Herunterfahren eines Knotens. Wenn der Fehler aufgetreten ist, fügen Sie den physischen Datenträger erneut ein, oder starten Sie den Knoten neu, und der Fehler wird wieder verschwindet.

Mithilfe der folgenden Cmdlets können Sie auch Fehler anzeigen, die sich nur auf bestimmte Volumes oder Dateifreigaben auswirken:

```
Get-Volume -FileSystemLabel <Label> | Debug-Volume

Get-FileShare -Name <Name> | Debug-FileShare
```

Dadurch werden alle Fehler zurückgegeben, die sich nur auf das jeweilige Volume oder die Dateifreigabe auswirken. In den meisten Fällen beziehen sich diese Fehler auf die Kapazitätsplanung, die datenresilienz oder Features wie Speicher Qualität oder Speicher Replikat.

## Verwendung in .net und C #

### Verbinden

Um den Integritätsdienst abzufragen, müssen Sie eine **cimsession** mit dem Cluster einrichten. Zu diesem Zweck benötigen Sie einige Dinge, die nur in der Vollversion von .net verfügbar sind, was bedeutet, dass Sie dies nicht direkt über ein Web oder Mobile App durchführen können. Diese Codebeispiele verwenden C#, die einfachste Wahl für diese Datenzugriffs Schicht.

```
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;
}
```

Der angegebene Benutzername muss ein lokaler Administrator des Bereitstellungs Ziel Computers sein.

Es wird empfohlen, dass Sie das Kennwort **SecureString** direkt aus Benutzereingaben in Echtzeit erstellen, damit Ihr Kennwort niemals im Klartext in Klartext gespeichert wird. Dies trägt dazu bei, eine Vielzahl von Sicherheitsrisiken zu verringern. In der Praxis ist es jedoch üblich, diese wie oben beschrieben zu erstellen.

### Objekte ermitteln

Nachdem die **cimsession** eingerichtet wurde, können Sie Windows-Verwaltungsinstrumentation (WMI) im Cluster Abfragen.

Bevor Sie Fehler oder Metriken erhalten können, müssen Sie Instanzen von mehreren relevanten Objekten erhalten. Zuerst das **MSFT_storagesubsystem** , das direkte Speicherplätze im Cluster darstellt. Mit diesem können Sie jede **_MSFT storagenode** -Instanz im Cluster und alle **MSFT_**-Volumes, die Datenvolumes, erhalten. Schließlich benötigen Sie auch **MSFT_storagehealth**, den Integritätsdienst selbst.

```
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();
}
```

Dabei handelt es sich um dieselben Objekte, die Sie in PowerShell mithilfe von Cmdlets wie " **Get-storagesubsystem**", " **Get-storagenode**" und " **Get-Volume**" erhalten.

Sie können auf die gleichen Eigenschaften zugreifen, die unter Klassen der Speicher Verwaltungs-APIdokumentiert sind.

```
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());
}
```

### Abfrage Fehler

Rufen Sie **Diagnose** auf, um alle aktuellen Fehler zu ermitteln, die auf die Ziel- **ciminstance bezogen**sind. Dies ist der Cluster oder ein beliebiges Volume.

Die komplette Liste der Fehler, die in jedem Bereich in Windows Server 2016 verfügbar sind, ist unten dokumentiert.

```
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-Klasse

Möglicherweise ist es sinnvoll, eine eigene Darstellung von Fehlern zu erstellen und beizubehalten. Diese **myfault** -Klasse speichert beispielsweise verschiedene wichtige Eigenschaften von Fehlern, einschließlich der **faultid**, die später verwendet werden kann, um Aktualisierungs-oder Entfernungs Benachrichtigungen zuzuordnen, oder um eine Deduplizierung durchzuführen, wenn derselbe Fehler mehrmals erkannt wird, aus einem beliebigen Grund.

```
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));
}
```

Die komplette Liste der Eigenschaften in den einzelnen Fehlern (**diagnoseresult**) ist unten dokumentiert.

### Fehlerereignisse

Wenn Fehler erstellt, entfernt oder aktualisiert werden, generiert der Integritätsdienst WMI-Ereignisse. Diese sind erforderlich, um den Anwendungs Status ohne häufige Abruf Vorgänge synchron zu halten, und können dabei helfen, wie z. b. das Festlegen von e-Mail-Benachrichtigungen. Um diese Ereignisse zu abonnieren, wird in diesem Beispielcode das Observer-Entwurfsmuster erneut verwendet.

Abonnieren Sie zuerst **MSFT_storagefaultevent** -Ereignisse.

```
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);
}
```

Implementieren Sie als nächstes einen Beobachter, dessen **OnNext ()** -Methode aufgerufen wird, wenn ein neues Ereignis generiert wird.

Jedes Ereignis enthält den **ChangeType** , der angibt, ob ein Fehler erstellt, entfernt oder aktualisiert wird, und die relevante **faultid**.

Außerdem enthalten Sie alle Eigenschaften des Fehlers selbst.

```
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
    }
}
```

### Grundlegendes zum Fault Lifecycle

Fehler sind nicht als "sichtbar" oder "aufgelöst" gekennzeichnet. Sie werden erstellt, wenn die Integritätsdienst ein Problem bemerkt, und Sie werden nur dann automatisch entfernt, wenn die Integritätsdienst das Problem nicht mehr beobachten kann. Im Allgemeinen zeigt dies, dass das Problem behoben wurde.

In einigen Fällen können jedoch Fehler von der Integritätsdienst (z. b. nach einem Failover oder aufgrund von zeitweiliger Konnektivität usw.) wiedererkannt werden. Aus diesem Grund ist es möglicherweise sinnvoll, eine eigene Darstellung von Fehlern beizubehalten, damit Sie problemlos deduplizieren können. Dies ist besonders wichtig, wenn Sie e-Mail-Benachrichtigungen oder eine gleichwertige senden.

**Eigenschaften von Fehlern**

Diese Tabelle enthält mehrere Schlüsseleigenschaften des Fault-Objekts. Überprüfen Sie für das vollständige Schema die Klasse " **_MSFT storagediagnoseresult** " in der Datei " *storagewmi. MOF*".

| EIGENSCHAFT | BEISPIEL |
|---|---|
| Faultid | {12345-12345-12345-12345-12345} |
| FaultType | Microsoft. Health. faultType. Volume. Capacity |
| `Reason` | "Auf dem Volume steht kein verfügbarer Speicherplatz mehr zur Verfügung." |
| Wahrnehmgrad | 5 |
| Faultingobjectdescription | XYZ9000 S.N. 123456789 |
| Faultingobjectlocation | Rack A06, ru 25, Slot 11 |
| Empfehlungs Aktionen | {"Erweitern Sie das Volume", "migrieren Sie Workloads zu anderen Volumes". |

**Faultid** Eindeutig innerhalb des Bereichs eines Clusters.

**Wahrnehmgrad** Wahrnehmvedschwere Grad = {4, 5, 6} = {"Information", "Warning" und "Error"}, oder äquivalente Farben wie blau, gelb und rot.

**Faultingobjectdescription** Teile Informationen für Hardware, in der Regel leer für Software Objekte.

**Faultingobjectlocation** Standortinformationen für Hardware, normalerweise leer für Software Objekte.

**Empfehlungs Aktionen** Liste der empfohlenen Aktionen, die unabhängig sind und in keiner bestimmten Reihenfolge sind. Heutzutage ist diese Liste häufig von der Länge 1.

# Eigenschaften von Fehlerereignissen

Diese Tabelle enthält mehrere Schlüsseleigenschaften des Fault-Ereignisses. Überprüfen Sie für das vollständige Schema die Klasse **MSFT_storagefaultevent** in *storagewmi. MOF*.

Beachten Sie den **ChangeType**, der angibt, ob ein Fehler erstellt, entfernt oder aktualisiert wird, und die **faultid**. Ein Ereignis enthält auch alle Eigenschaften des betroffenen Fehlers.

| EIGENSCHAFT | BEISPIEL |
|---|---|
| ChangeType | 0 |
| Faultid | {12345-12345-12345-12345-12345} |
| FaultType | Microsoft. Health. faultType. Volume. Capacity |

| EIGENSCHAFT | BEISPIEL |
| --- | --- |
| `Reason` | "Auf dem Volume steht kein verfügbarer Speicherplatz mehr zur Verfügung." |
| Wahrnehmgrad | 5 |
| Faultingobjectdescription | XYZ9000 S.N. 123456789 |
| Faultingobjectlocation | Rack A06, ru 25, Slot 11 |
| Empfehlungs Aktionen | {"Erweitern Sie das Volume", "migrieren Sie Workloads zu anderen Volumes". |

**ChangeType** ChangeType = {0, 1, 2} = {"Create", "Remove", "Update"}.

# Abdeckung

In Windows Server 2016 stellt die Integritätsdienst die folgende Fehlerabdeckung bereit:

### PhysicalDisk (8)

**FaultType: Microsoft. Health. faultType. PhysicalDisk. failedmedia**

- Schweregrad: Warnung
- Grund: *"Fehler bei der physischen Festplatte."*
- Empfehlungs Aktion: *"Ersetzen des physischen Datenträgers".*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. lostcommunication**

- Schweregrad: Warnung
- Ursache: *"die Verbindung mit dem physischen Datenträger ist verloren gegangen".*
- Empfehlungs Aktion: *"Überprüfen Sie, ob die physische Festplatte funktioniert und ordnungsgemäß verbunden ist."*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. nicht reagierend.**

- Schweregrad: Warnung
- Grund: *"der physische Datenträger stellt wiederkehrende nicht Reaktionsfähigkeit dar."*
- Empfehlungs Aktion: *"Ersetzen des physischen Datenträgers".*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. predictivefailure**

- Schweregrad: Warnung
- Ursache: *"ein Ausfall des physischen Datenträgers ist in Kürze geplant."*
- Empfehlungs Aktion: *"Ersetzen des physischen Datenträgers".*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. unsupportedhardware**

- Schweregrad: Warnung
- Ursache: *"der physische Datenträger wird unter Quarantäne gestellt, weil er von Ihrem Lösungsanbieter nicht unterstützt wird."*
- Empfehlungs Aktion: *"ersetzen Sie den physischen Datenträger durch unterstützte Hardware".*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. unsupportedfirmware**

- Schweregrad: Warnung
- Ursache: *"der physische Datenträger wird in Quarantäne gestellt, da seine Firmwareversion von Ihrem Lösungsanbieter nicht unterstützt wird."*
- Empfehlungs Aktion: *"Aktualisieren Sie die Firmware auf dem physischen Datenträger auf die Zielversion."*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. unerkenzedmetadata**

- Schweregrad: Warnung
- Grund: *"der physische Datenträger hat nicht erkannte Meta-Daten."*
- Empfehlungs Aktion: *"dieser Datenträger kann Daten aus einem unbekannten Speicherpool enthalten. Stellen Sie zunächst sicher, dass auf diesem Datenträger keine nützlichen Daten vorhanden sind, und setzen Sie dann den Datenträger zurück.*

**FaultType: Microsoft. Health. faultType. PhysicalDisk. failedfirmwareupdate**

- Schweregrad: Warnung
- Ursache: *"Fehler bei der Aktualisierung der Firmware auf dem physischen Datenträger."*
- Empfehlungs Aktion: *"versuchen Sie, eine andere Firmware-Binärdatei zu verwenden."*

### Virtueller Datenträger (2)

**FaultType: Microsoft. Health. faultType. virtualdisks. needsrepair**

- Schweregrad: Information
- Ursache: *"einige Daten auf diesem Volume sind nicht vollständig stabil. Der Zugriff ist weiterhin möglich. "*
- Empfehlungs Maßnahme: *"Wiederherstellen der Resilienz der Daten."*

**FaultType: Microsoft. Health. faultType. virtualdisks. getrennte**

- Schweregrad: Kritisch
- Grund: *"der Zugriff auf das Volume ist nicht möglich. Einige Daten können verloren gehen. "*
- Empfehlungs Aktion: *"Überprüfen Sie die physische und/oder Netzwerk Konnektivität aller Speichergeräte. Möglicherweise müssen Sie eine Wiederherstellung aus einer Sicherung durch erstellen. "*

### Pool Kapazität (1)

**FaultType: Microsoft. Health. faultType. storagepool. insuffizientreservecapacityfault**

- Schweregrad: Warnung
- Ursache: *"der Speicherpool verfügt nicht über die empfohlene Mindestreserve Kapazität. Dies kann die Fähigkeit zum Wiederherstellen von datenresilienz im Fall von Laufwerk Fehlern einschränken. "*
- Empfehlungs Aktion: *"zusätzliche Kapazität zum Speicherpool hinzufügen oder Kapazität freigeben. Die empfohlene Mindestreserve ist abhängig von der Bereitstellung, aber es sind ungefähr 2 Laufwerke ausgelastet. "*

### Volumekapazität (2)[1]

**FaultType: Microsoft. Health. faultType. Volume. Capacity**

- Schweregrad: Warnung
- Ursache: *"der verfügbare Speicherplatz auf dem Volume steht nicht mehr zur Verfügung."*
- Empfehlungs Aktion: *"erweitern Sie das Volume, oder migrieren Sie Arbeits Auslastungen zu anderen Volumes".*

**FaultType: Microsoft. Health. faultType. Volume. Capacity**

- Schweregrad: Kritisch
- Ursache: *"der verfügbare Speicherplatz auf dem Volume steht nicht mehr zur Verfügung."*
- Empfehlungs Aktion: *"erweitern Sie das Volume, oder migrieren Sie Arbeits Auslastungen zu anderen Volumes".*

### Server (3)

**FaultType: Microsoft. Health. faultType. Server. Down**

- Schweregrad: Kritisch
- Ursache: *"der Server kann nicht erreicht werden."*
- Empfehlungs Aktion: *"Server starten oder ersetzen"*

**FaultType: Microsoft. Health. faultType. Server. isoliert**

- Schweregrad: Kritisch
- Ursache: *"der Server ist aufgrund von Konnektivitätsproblemen vom Cluster isoliert".*
- Empfehlungs Aktion: *"Wenn die Isolation weiterhin besteht, überprüfen Sie die Netzwerk (e), oder migrieren Sie Arbeits Auslastungen zu anderen Knoten".*

**FaultType: Microsoft. Health. faultType. Server. Quarantäne**

- Schweregrad: Kritisch
- Ursache: *"der Server wird aufgrund von wiederkehrenden Fehlern durch den Cluster unter Quarantäne gestellt."*
- Empfehlungs Aktion: *"Server ersetzen oder Netzwerk reparieren".*

### Cluster (1)

**FaultType: Microsoft. Health. faultType. clusterquorüberwitness. Error**

- Schweregrad: Kritisch
- Ursache: *"der Cluster ist ein Server Fehler, der nicht mehr ausfällt."*
- Empfehlungs Aktion: *"Überprüfen Sie die Zeugen Ressource, und starten Sie Sie bei Bedarf neu. Starten oder ersetzen fehlerhafter Server. "*

### Netzwerk Adapter/-Schnittstelle (4)

**FaultType: Microsoft. Health. faultType. NetworkAdapter. getrennte**

- Schweregrad: Warnung
- Ursache: *"die Netzwerkschnittstelle wurde getrennt."*
- Empfehlungs Aktion: *"Verbindung mit dem Netzwerkkabel wiederherstellen".*

**FaultType: Microsoft. Health. faultType. NetworkInterface. Missing**

- Schweregrad: Warnung
- Grund: *"der Server" {Server} "verfügt über fehlende Netzwerkadapter (e), die mit dem Cluster Netzwerk" {Cluster Network} "verbunden sind.*
- Empfehlungs Aktion: *"Verbinden Sie den Server mit dem fehlenden Cluster Netzwerk".*

**FaultType: Microsoft. Health. faultType. NetworkAdapter. Hardware**

- Schweregrad: Warnung
- Ursache: *"bei der Netzwerkschnittstelle ist ein Hardwarefehler aufgetreten."*
- Empfehlungs Aktion: *"ersetzt den Netzwerkschnittstellen Adapter".*

**FaultType: Microsoft. Health. faultType. NetworkAdapter. deaktiviert**

- Schweregrad: Warnung
- Ursache: *"die Netzwerkschnittstelle" {Network Interface} "ist nicht aktiviert und wird nicht verwendet."*
- Empfehlungs Aktion: *"Netzwerkschnittstelle aktivieren".*

### Gehäuse (6)

**FaultType: Microsoft. Health. faultType. storageenclosure. lostcommunication**

- Schweregrad: Warnung
- Ursache: *"die Kommunikation mit dem Speicher Gehäuse ist verloren gegangen."*
- Empfehlungs Aktion: *"das Speicher Gehäuse wird gestartet oder ersetzt."*

**FaultType: Microsoft. Health. faultType. storageenclosure. fanerror**

- Schweregrad: Warnung
- Grund: *"der Lüfter an Position {Position} des Speicher Gehäuses ist fehlgeschlagen."*
- Empfehlungs Aktion: *"ersetzen Sie den Lüfter im Speicher Gehäuse."*

**FaultType: Microsoft. Health. faultType. storageenclosure. currentsensorerror**

- Schweregrad: Warnung
- Grund: *"Fehler beim aktuellen Sensor an Position {Position} des Speicher Gehäuses."*

- Empfehlungs Aktion: *"Ersetzen eines aktuellen Sensors im Speicher Gehäuse".*

**FaultType: Microsoft. Health. faultType. storageenclosure. voltagesensorerror**

- Schweregrad: Warnung
- Grund: *"der Spannungssensor an Position {Position} des Speicher Gehäuses ist fehlgeschlagen."*
- Empfehlungs Aktion: *"Ersetzen eines Spannungs Sensors im Speicher Gehäuse".*

**FaultType: Microsoft. Health. faultType. storageenclosure. iocontrollererror**

- Schweregrad: Warnung
- Ursache: "Fehler beim e/a- *Controller an Position {Position} des Speicher Gehäuses."*
- Empfehlungs Aktion: *"ersetzt einen IO-Controller im Speicher Gehäuse."*

**FaultType: Microsoft. Health. faultType. storageenclosure. temperaturesensorerror**

- Schweregrad: Warnung
- Grund: *"Fehler beim Temperatursensor an Position {Position} des Speicher Gehäuses."*
- Empfehlungs Aktion: *"Ersetzen eines Temperatursensors im Speicher Gehäuse".*

### Firmware-Rollout (3)

**FaultType: Microsoft. Health. faultType. fauldomain. failedmaintenancemode**

- Schweregrad: Warnung
- Ursache: *"der Fortschritt während der firmwarerollout kann zurzeit nicht fortgesetzt werden."*
- Empfehlungs Aktion: *"Überprüfen Sie, ob alle Speicherplätze fehlerfrei sind und derzeit keine Fehler Domäne im Wartungsmodus ist".*

**FaultType: Microsoft. Health. faultType. fauldomain. firmwareverifyversionfaile**

- Schweregrad: Warnung
- Grund: *"der firmwarerollout wurde aufgrund von unlesbaren oder unerwarteten Firmwareversion-Informationen nach dem Anwenden eines* Firmwareupdates abgebrochen"
- Empfehlungs Aktion: *"firmwarerollout neu starten, sobald das firmwareproblem behoben wurde".*

**FaultType: Microsoft. Health. faultType. fauldomain. deomanyfailedupdates**

- Schweregrad: Warnung
- Grund: *"der firmwarerollout wurde abgebrochen, weil zu viele physische* Datenträger fehlgeschlagen sind."
- Empfehlungs Aktion: *"firmwarerollout neu starten, sobald das firmwareproblem behoben wurde".*

### Speicher-QoS (3)[2]

**FaultType: Microsoft. Health. faultType. storqos. insuffizientdurchsatz**

- Schweregrad: Warnung
- Ursache: *"der Speicher Durchsatz reicht nicht aus, um Reserven zu erfüllen".*
- Empfehlungs Aktion: *"Speicher-QoS-Richtlinien neu konfigurieren".*

**FaultType: Microsoft. Health. faultType. storqos. lostcommunication**

- Schweregrad: Warnung
- Ursache: *"der Speicher-QoS-Richtlinien-Manager hat die Kommunikation mit dem Volume verloren."*
- Empfehlungs Aktion: *"Neustart der Knoten {Nodes}"*

**FaultType: Microsoft. Health. faultType. storqos. miskonfiguriredflow**

- Schweregrad: Warnung
- Ursache: *"mindestens ein speicherconsumer (in der Regel Virtual Machines) verwendet eine nicht vorhandene Richtlinie mit der ID {ID}".*
- Empfehlungs Aktion: *"alle fehlenden Speicher-QoS-Richtlinien neu erstellen".*

[1] gibt an, dass das Volume 80% vollständig (neben Schweregrad) oder 90% voll (Schweregrad) erreicht hat.
[2] gibt an, dass einige VHDs auf dem Volume nicht ihren minimalen IOPS-Aufwand für über 10% (neben Version),

30% (Hauptversion) oder 50% (kritisch) des parallelen 24-Stunden-Fensters erreicht haben.

> **NOTE**
> Die Integrität von Speichergehäusekomponenten wie Lüfter, Netzteile und Sensoren wird von SES (SCSI Enclosure Services) abgeleitet. Wenn Ihr Anbieter diese Informationen nicht bereitstellt, kann der Integritätsdienst sie nicht anzeigen.

## Weitere Informationen

- Der Integritätsdienst in Windows Server 2016

# Integritätsdienst Aktionen

09.04.2020 • 2 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Der Integritätsdienst ist ein neues Feature in Windows Server 2016, das die tägliche Überwachung und Betriebsbereitschaft für Cluster mit direkte Speicherplätze verbessert.

## Aktionen

Im nächsten Abschnitt werden Workflows beschrieben, die vom Integritätsdienst automatisiert werden. Um sicherzustellen, dass eine Aktivität tatsächlich autonom erfolgt, oder um ihren Fortschritt oder ihr Ergebnis nachzuverfolgen, generiert der Integritätsdienst „Aktionen". Im Gegensatz zu Protokollen verschwinden Aktionen, kurz nachdem sie erfolgt sind, und dienen hauptsächlich zum Gewinnen von Einblicken in laufende Aktivitäten, die sich auf die Leistung oder Kapazität auswirken können (z. B. Wiederherstellen der Ausfallsicherheit oder Neuverteilen von Daten).

### Verwendung

Mit einem neuen PowerShell-Cmdlet werden alle Aktionen angezeigt:

```
Get-StorageHealthAction
```

### Abdeckung

In Windows Server 2016 kann das Cmdlet **Get-storagehealthaction** die folgenden Informationen zurückgeben:

- Außerbetriebnahme misslungen, Verbindung verloren oder nicht reagierender physischer Datenträger
- Wechsel des Speicherpools, um physischen Austauschdatenträger zu verwenden
- Wiederherstellen der vollständigen Ausfallsicherheit für Daten
- Neuverteilen von Speicherpools

## Siehe auch

- Integritätsdienst in Windows Server 2016
- Entwicklerdokumentation, Beispielcode und API-Referenz auf MSDN

# Integritätsdienst Einstellungen

02.05.2020 • 2 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Der Integritätsdienst ist ein neues Feature in Windows Server 2016, das die tägliche Überwachung und Betriebsbereitschaft für Cluster mit direkte Speicherplätze verbessert.

Viele der Parameter, die das Verhalten der Integritätsdienst steuern, werden als Einstellungen verfügbar gemacht. Sie können diese ändern, um die Aggressivität von Fehlern oder Aktionen zu optimieren, bestimmte Verhalten ein-/ausschalten und vieles mehr.

Verwenden Sie das folgende PowerShell-Cmdlet, um Einstellungen festzulegen oder zu ändern.

## Verwendung

```
Get-StorageSubSystem Cluster* | Set-StorageHealthSetting -Name <SettingName> -Value <Value>
```

#### Beispiel

```
Get-StorageSubSystem Cluster* | Set-StorageHealthSetting -Name
"System.Storage.Volume.CapacityThreshold.Warning" -Value 70
```

## Allgemeine Einstellungen

Einige häufig geänderte Einstellungen sind im folgenden aufgeführt, zusammen mit ihren Standardwerten.

#### Schwellenwert für Volumenkapazität

```
"System.Storage.Volume.CapacityThreshold.Enabled"  = True
"System.Storage.Volume.CapacityThreshold.Warning"  = 80
"System.Storage.Volume.CapacityThreshold.Critical" = 90
```

#### Schwellenwert für Pool Reserve Kapazität

```
"System.Storage.StoragePool.CheckPoolReserveCapacity.Enabled" = True
```

#### Lebenszyklus physischer Datenträger

```
"System.Storage.PhysicalDisk.AutoPool.Enabled"                           = True
"System.Storage.PhysicalDisk.AutoRetire.OnLostCommunication.Enabled"     = True
"System.Storage.PhysicalDisk.AutoRetire.OnUnresponsive.Enabled"          = True
"System.Storage.PhysicalDisk.AutoRetire.DelayMs"                         = 900000 (i.e. 15 minutes)
"System.Storage.PhysicalDisk.Unresponsive.Reset.CountResetIntervalSeconds" = 360 (i.e. 60 minutes)
"System.Storage.PhysicalDisk.Unresponsive.Reset.CountAllowed"            = 3
```

#### Dokument zu unterstützten Komponenten

Weitere Informationen finden Sie im vorherigen Abschnitt.

#### Firmware-Rollout

```
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.SingleDrive.Enabled"       = True
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.RollOut.Enabled"           = True
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.RollOut.LongDelaySeconds"  = 604800 (i.e. 7 days)
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.RollOut.ShortDelaySeconds" = 86400 (i.e. 1 day)
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.RollOut.LongDelayCount"    = 1
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.RollOut.FailureTolerance"  = 3
```

**Plattform/ineszenz**

```
"Platform.Quiescence.MinDelaySeconds" = 120 (i.e. 2 minutes)
"Platform.Quiescence.MaxDelaySeconds" = 420 (i.e. 7 minutes)
```

**Metriken**

```
"System.Reports.ReportingPeriodSeconds" = 1
```

**Debuggen**

```
"System.LogLevel" = 4
```

# Weitere Informationen

- Der Integritätsdienst in Windows Server 2016
- Direkte Speicherplätze in Windows Server 2016

# Migration der failoverclusterdomäne

09.04.2020 • 10 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

Dieses Thema enthält eine Übersicht über das Verschieben von Windows Server-Failoverclustern von einer Domäne in eine andere.

## Gründe für die Migration zwischen Domänen

Es gibt mehrere Szenarios, in denen das Migrieren eines Clusters von einem doamin zu einem anderen notwendig ist.

- CompanyA wird zusammen mit CompanyB zusammengeführt und muss alle Cluster in die Domäne "CompanyA" verschieben.
- Cluster werden im Hauptrechenzentrum erstellt und an Remote Standorten ausgeliefert.
- Der Cluster wurde als Arbeitsgruppen Cluster erstellt und muss nun Teil einer Domäne sein.
- Der Cluster wurde als Domänen Cluster erstellt und muss nun Teil einer Arbeitsgruppe sein.
- Der Cluster wird in einen anderen Bereich des Unternehmens verschoben und ist eine andere Unterdomäne.

Microsoft bietet keine Unterstützung für Administratoren, die versuchen, Ressourcen von einer Domäne in eine andere zu verschieben, wenn der zugrunde liegende Anwendungs Vorgang nicht unterstützt wird. Beispielsweise bietet Microsoft keine Unterstützung für Administratoren, die versuchen, einen Microsoft Exchange-Server von einer Domäne in eine andere zu verschieben.

> **WARNING**
>
> Es wird empfohlen, dass Sie eine vollständige Sicherung des gesamten freigegebenen Speichers im Cluster durchführen, bevor Sie den Cluster verschieben.

## Windows Server 2016 und früher

In Windows Server 2016 und früher hatte die Clusterdienst nicht die Möglichkeit, von einer Domäne in eine andere zu wechseln. Dies war auf die zunehmende Abhängigkeit von Active Directory Domain Services und den erstellten virtuellen Namen zurückzuführen.

## Optionen

Um eine solche Verschiebung durchzuführen, gibt es zwei Optionen.

Die erste Option besteht darin, den Cluster zu zerstören und in der neuen Domäne neu zu erstellen.

# Previously, changing domains were destructive

Wie die Animation zeigt, ist diese Option mit den folgenden Schritten destruktiv:

1. Zerstören Sie den Cluster.
2. Ändern Sie die Domänen Mitgliedschaft der Knoten in die neue Domäne.
3. Erstellen Sie den Cluster neu in der aktualisierten Domäne. Dies würde dazu führen, dass alle Ressourcen neu erstellt werden müssen.

Die zweite Option ist weniger destruktiv, erfordert jedoch zusätzliche Hardware, da ein neuer Cluster in der neuen Domäne erstellt werden muss. Wenn sich der Cluster in der neuen Domäne befindet, führen Sie den Clustermigrations-Assistenten aus, um die Ressourcen zu migrieren. Beachten Sie, dass dadurch keine Daten migriert werden. Sie müssen ein anderes Tool zum Migrieren von Daten verwenden, z. b. den Speicher Migrationsdienst(nachdem die Cluster Unterstützung hinzugefügt wurde).

# Migration of resources is an option

Wie die Animation zeigt, ist diese Option nicht destruktiv, erfordert jedoch entweder eine andere Hardware oder einen Knoten aus dem vorhandenen Cluster, als entfernt wurde.

1. Erstellen Sie eine neue Domäne, während der alte Cluster weiterhin verfügbar ist.
2. Verwenden Sie den Clustermigrations-Assistenten , um alle Ressourcen in den neuen Cluster zu migrieren. Erinnerung: Dadurch werden keine Daten kopiert, daher muss Sie separat durchgeführt werden.
3. Entfernen oder zerstören Sie den alten Cluster.

Bei beiden Optionen muss auf dem neuen Cluster alle Cluster fähigen Anwendungen installiert sein, die Treiber sind auf dem neuesten Stand und möglicherweise Tests, um sicherzustellen, dass alles ordnungsgemäß ausgeführt wird. Dies ist ein zeitaufwändiger Prozess, wenn Daten ebenfalls verschoben werden müssen.

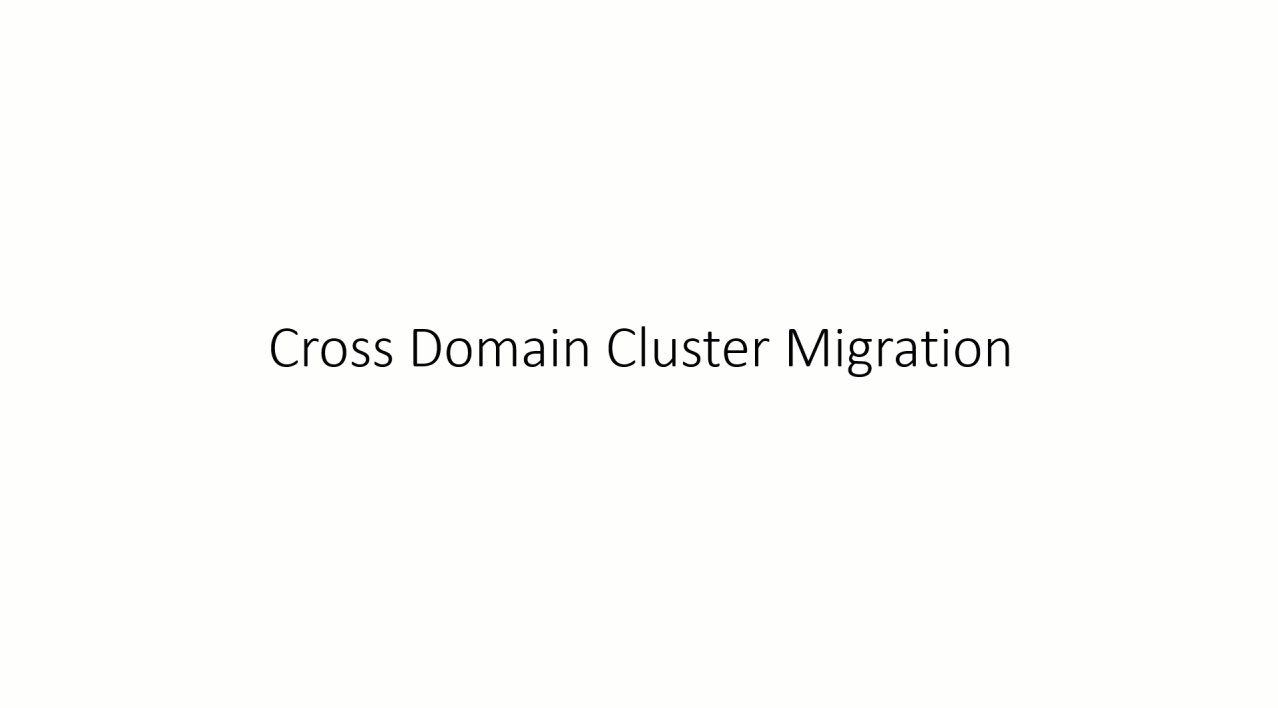
## Windows Server 2019

In Windows Server 2019 wurden Migrations Funktionen für Cluster übergreifende Domänen eingeführt. Nun können die oben aufgeführten Szenarien problemlos durchgeführt werden, und die Notwendigkeit der Neuerstellung ist nicht mehr erforderlich.

Das Verschieben eines Clusters aus einer Domäne ist ein geradliniger Prozess. Hierfür gibt es zwei neue PowerShell-Cmdlets.

**New-clusternameaccount** – erstellt ein Cluster Namen Konto in Active Directory **Remove-clusternameaccount** – entfernt die Cluster Namen Konten aus Active Directory

Um dies zu erreichen, müssen Sie den Cluster von einer Domäne in eine Arbeitsgruppe und zurück in die neue Domäne ändern. Es ist nicht erforderlich, einen Cluster zu zerstören, einen Cluster neu zu erstellen, Anwendungen zu installieren usw. Dies sieht beispielsweise wie folgt aus:




## Migrieren eines Clusters zu einer neuen Domäne

In den folgenden Schritten wird ein Cluster von der contoso.com-Domäne in die neue fabrikam.com-Domäne verschoben. Der Cluster Name ist *clusclus* und verfügt über eine Dateiserver Rolle namens *FS-clusclus*.

1. Erstellen Sie ein lokales Administrator Konto mit dem gleichen Namen und Kennwort auf allen Servern im Cluster. Dies ist möglicherweise erforderlich, um sich anzumelden, während die Server zwischen Domänen verschoben werden.

2. Melden Sie sich beim ersten Server mit einem Domänen Benutzer-oder Administrator Konto an, das über Active Directory Berechtigungen für das Cluster Namen Objekt (CNO), virtuelle Computer Objekte (VCO)

verfügt, Zugriff auf den Cluster hat, und öffnen Sie PowerShell.

3. Stellen Sie sicher, dass alle Cluster Netzwerk-namens Ressourcen offline sind, und führen Sie den folgenden Befehl aus. Mit diesem Befehl werden die Active Directory Objekte entfernt, die möglicherweise vom Cluster verwendet werden.

```
Remove-ClusterNameAccount -Cluster CLUSCLUS -DeleteComputerObjects
```

4. Verwenden Sie Active Directory-Benutzer und-Computer, um sicherzustellen, dass die diesem Cluster Namen zugeordneten CNO-und VCO-Computer Objekte entfernt wurden.

> **NOTE**
> Es empfiehlt sich, die Clusterdienst auf allen Servern im Cluster zu beenden und den Starttyp des Dienst auf "manuell" festzulegen, damit das Clusterdienst nicht startet, wenn die Server beim Ändern von Domänen neu gestartet werden.

```
Stop-Service -Name ClusSvc

Set-Service -Name ClusSvc -StartupType Manual
```

5. Ändern Sie die Domänen Mitgliedschaft der Server in eine Arbeitsgruppe, starten Sie die Server neu, fügen Sie die Server der neuen Domäne hinzu, und starten Sie erneut.

6. Wenn sich die Server in der neuen Domäne befinden, melden Sie sich bei einem Server mit einem Domänen Benutzer-oder Administrator Konto an, das über Active Directory Berechtigungen zum Erstellen von Objekten, Zugriff auf den Cluster und Öffnen von PowerShell verfügt. Starten Sie den Cluster Dienst, und legen Sie ihn wieder auf automatisch fest.

```
Start-Service -Name ClusSvc

Set-Service -Name ClusSvc -StartupType Automatic
```

7. Schalten Sie den Cluster Namen und alle anderen Cluster Netzwerk-namens Ressourcen in den Online Zustand.

```
Start-ClusterResource -Name "Cluster Name"

Start-ClusterResource -Name FS-CLUSCLUS
```

8. Ändern Sie den Cluster so, dass er Teil der neuen Domäne mit zugeordneten Active Directory-Objekten ist. Zu diesem Zweck ist der Befehl unten angegeben, und die Netzwerknamen Ressourcen müssen sich in einem Online Status befinden. Mit diesem Befehl werden die namens Objekte in Active Directory neu erstellt.

```
New-ClusterNameAccount -Name CLUSTERNAME -Domain NEWDOMAINNAME.com -UpgradeVCOs
```

   Hinweis: Wenn Sie keine zusätzlichen Gruppen mit Netzwerknamen haben (d. h. ein Hyper-V-Cluster mit nur virtuellen Computern), wird der Schalter-upgradevcos Parameter nicht benötigt.

9. Verwenden Sie Active Directory Benutzer und Computer, um die neue Domäne zu überprüfen und sicherzustellen, dass die zugeordneten Computer Objekte erstellt wurden. Wenn dies der Fall ist, schalten Sie die verbleibenden Ressourcen in den Gruppen online.

```
Start-ClusterGroup -Name "Cluster Group"

Start-ClusterGroup -Name FS-CLUSCLUS
```

## Bekannte Probleme

Wenn Sie die neue USB-Zeugen Funktion verwenden, können Sie den Cluster nicht der neuen Domäne hinzufügen. Der Grund dafür ist, dass der Dateifreigabezeuge Kerberos für die Authentifizierung verwenden muss. Ändern Sie den Zeugen in None, bevor Sie den Cluster der Domäne hinzufügen. Nachdem der Vorgang abgeschlossen ist, erstellen Sie den USB-Zeugen neu. Der folgende Fehler wird angezeigt:

```
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.
```

# Behandeln von Problemen mit einem Failovercluster mithilfe von Windows-Fehlerberichterstattung

09.04.2020 • 13 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016, Windows Server

Bei Windows-Fehlerberichterstattung (wer) handelt es sich um eine flexible ereignisbasierte Feedback Infrastruktur, mit der erweiterte Administratoren oder Support von Unterstützung von Windows Informationen zu den Hardware-und Softwareproblemen sammeln können, die von Windows erkannt werden können, die Informationen an Microsoft gemeldet werden und Benutzern alle verfügbaren Lösungen bereitgestellt werden. Diese Referenz enthält Beschreibungen und Syntax für alle windowserrorreporting-Cmdlets.

Die folgenden Informationen zur Problembehandlung sind hilfreich bei der Behebung erweiterter Probleme, die eskaliert wurden und möglicherweise erfordern, dass Daten für die Selektierung an Microsoft gesendet werden.

## Aktivieren von Ereignis Kanälen

Wenn Windows Server installiert ist, sind viele Ereignis Kanäle standardmäßig aktiviert. Doch manchmal möchten wir bei der Diagnose eines Problems einige dieser Ereignis Kanäle aktivieren, da dies bei der Selektierung und Diagnose von Systemproblemen hilfreich sein wird.

Sie können je nach Bedarf zusätzliche Ereignis Kanäle auf jedem Server Knoten in Ihrem Cluster aktivieren. Dieser Ansatz stellt jedoch zwei Probleme dar:

1. Beachten Sie, dass Sie die gleichen Ereignis Kanäle auf allen neuen Server Knoten aktivieren müssen, die Sie dem Cluster hinzufügen.
2. Bei der Diagnose kann es mühsam sein, bestimmte Ereignis Kanäle zu aktivieren, den Fehler zu reproduzieren und diesen Vorgang zu wiederholen, bis Sie die Ursache ermitteln.

Um diese Probleme zu vermeiden, können Sie Ereignis Kanäle beim Starten des Clusters aktivieren. Die Liste der aktivierten Ereignis Kanäle im Cluster kann mit der öffentlichen Eigenschaft " **enabledeventlogs**" konfiguriert werden. Standardmäßig sind die folgenden Ereignis Kanäle aktiviert:

```
PS C:\Windows\system32> (get-cluster).EnabledEventLogs
```

Dies ist ein Beispiel für die Ausgabe:

```
Microsoft-Windows-Hyper-V-VmSwitch-Diagnostic,4,0xFFFFFFFD
Microsoft-Windows-SMBDirect/Debug,4
Microsoft-Windows-SMBServer/Analytic
Microsoft-Windows-Kernel-LiveDump/Analytic
```

Die **enabledeventlogs** -Eigenschaft ist eine Multizeichenfolge, bei der jede Zeichenfolge das folgende Format hat: **Channel-Name, Protokollebene, Schlüsselwort Maske**. Das **Schlüsselwort Mask** kann ein hexadezimales Zeichen (Präfix 0x), oktal (Präfix 0) oder Dezimalzahl (ohne Präfix) sein. Um beispielsweise der Liste einen neuen Ereignis Kanal hinzuzufügen und sowohl **Protokoll-** als auch **Schlüsselwort Maske** zu konfigurieren, können Sie Folgendes ausführen:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,2,321"
```

Wenn Sie die **Protokollebene** festlegen, aber die **Schlüsselwort Maske** mit dem Standardwert behalten möchten, können Sie einen der folgenden Befehle verwenden:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,2"
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,2,"
```

Wenn Sie den Standardwert auf **Protokollebene** beibehalten möchten, aber die **Schlüsselwort Maske** festlegen, können Sie den folgenden Befehl ausführen:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,,0xf1"
```

Wenn Sie sowohl die **Protokollebene** als auch die **Schlüsselwort Maske** mit ihren Standardwerten belassen möchten, können Sie einen der folgenden Befehle ausführen:

```
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic"
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,"
(get-cluster).EnabledEventLogs += "Microsoft-Windows-WinINet/Analytic,,"
```

Diese Ereignis Kanäle werden auf jedem Cluster Knoten aktiviert, wenn der Cluster Dienst gestartet wird, oder wenn die **enabledeventlogs** -Eigenschaft geändert wird.

## Protokolle werden gesammelt.

Nachdem Sie Ereignis Kanäle aktiviert haben, können Sie die **dumplogquery** verwenden, um Protokolle zu erfassen. Die öffentliche Ressourcentyp Eigenschaft **dumplogquery** ist ein mutistring-Wert. Jede Zeichenfolge ist eine XPath-Abfrage, wie hier beschrieben.

Wenn Sie bei der Problembehandlung weitere Ereignis Kanäle erfassen müssen, können Sie die **dumplogquery** -Eigenschaft ändern, indem Sie zusätzliche Abfragen hinzufügen oder die Liste ändern.

Testen Sie hierzu zunächst die XPath-Abfrage mithilfe des PowerShell-Cmdlets Get-WinEvent :

```
get-WinEvent -FilterXML "<QueryList><Query><Select Path='Microsoft-Windows-GroupPolicy/Operational'>*
[System[TimeCreated[timediff(@SystemTime) &gt;= 600000]]]</Select></Query></QueryList>"
```

Fügen Sie anschließend die Abfrage an die **dumplogquery** -Eigenschaft der Ressource an:

```
(Get-ClusterResourceType -Name "Physical Disk".DumpLogQuery += "<QueryList><Query><Select Path='Microsoft-
Windows-GroupPolicy/Operational'>*[System[TimeCreated[timediff(@SystemTime) &gt;= 600000]]]</Select></Query>
</QueryList>"
```

Wenn Sie eine Liste der zu verwendenden Abfragen erhalten möchten, führen Sie Folgendes aus:

```
(Get-ClusterResourceType -Name "Physical Disk").DumpLogQuery
```

## Sammeln von Windows-Fehlerberichterstattung Berichten

Windows-Fehlerberichterstattung Berichte werden in **%ProgramData%\microsoft\windows\wer** gespeichert.

Im Ordner **wer** enthält der Ordner **reportsqueue** Berichte, die darauf warten, in Watson hochgeladen zu werden.

```
PS C:\Windows\system32> dir c:\ProgramData\Microsoft\Windows\WER\ReportQueue
```

Dies ist ein Beispiel für die Ausgabe:

```
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
```

Im Ordner **wer** enthält der Ordner **reportsarchive** Berichte, die bereits in Watson hochgeladen wurden. Die Daten in diesen Berichten werden gelöscht, aber die Datei " **Report. Wer** " bleibt erhalten.

```
PS C:\Windows\system32> dir C:\ProgramData\Microsoft\Windows\WER\ReportArchive
```

Dies ist ein Beispiel für die Ausgabe:

```
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-Fehlerberichterstattung bietet viele Einstellungen zur Anpassung der Problembericht Erstellungs Umgebung. Weitere Informationen finden Sie in der Windows-Fehlerberichterstattung- Dokumentation.

## Problembehandlung mithilfe von Windows-Fehlerberichterstattung Berichten

**Der physische Datenträger konnte nicht online geschaltet werden.**

Navigieren Sie zum Bericht "Wer-Bericht", um dieses Problem zu diagnostizieren:

```
PS C:\Windows\system32> dir
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\Critical_PhysicalDisk_b46b8883d892cfa8a26263afca228b17df8133
d_00000000_cab_08abc39c
```

Dies ist ein Beispiel für die Ausgabe:

```
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
```

Beginnen Sie als nächstes mit der Selektierung aus der Datei " **Report. Wer** " – Dadurch wird angezeigt, was nicht.

```
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
```

Da die Ressource nicht online geschaltet werden konnte, wurden keine Abbilder erfasst, aber der Windows-Fehlerberichterstattung Bericht hat Protokolle erfasst. Wenn Sie alle **evtx** -Dateien mithilfe von Microsoft Message Analyzer öffnen, werden alle gesammelten Informationen mithilfe der folgenden Abfragen über den systemchannel, den Anwendungs Kanal, Failovercluster-Diagnose Kanäle und einige andere generische Kanäle angezeigt.

```
PS C:\Windows\system32> (Get-ClusterResourceType -Name "Physical Disk").DumpLogQuery
```

Dies ist ein Beispiel für die Ausgabe:

```
<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>
```

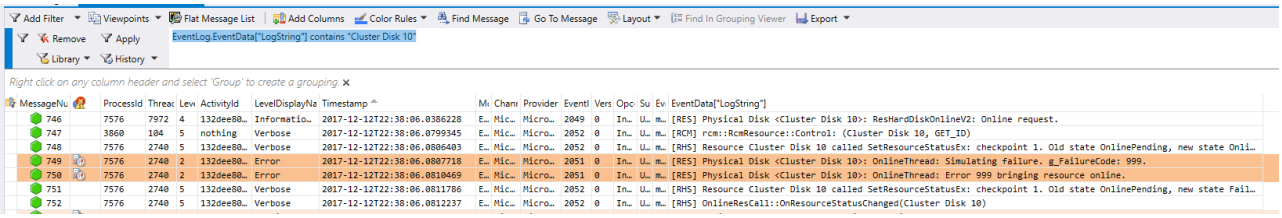
Message Analyzer ermöglicht Ihnen das erfassen, anzeigen und Analysieren des Protokollnachrichten Verkehrs. Außerdem können Sie Systemereignisse und andere Meldungen von Windows-Komponenten verfolgen und bewerten. Hier können Sie Microsoft Message Analyzerherunterladen. Wenn Sie die Protokolle in Message Analyzer laden, werden die folgenden Anbieter und Meldungen aus den Protokoll Kanälen angezeigt.

| MessageNu | ProcessId | Threac | Levi | 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 | | | | | | |

Sie können auch nach Anbietern gruppieren, um die folgende Ansicht anzuzeigen:

```
▷ 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
```

Um zu ermitteln, warum der Datenträger fehlgeschlagen ist, navigieren Sie zu den Ereignissen unter **Failoverclustering/Diagnose** und **Failoverclustering/diagnosticverbose**. Führen Sie dann die folgende Abfrage aus: **EventLog. EVENTDATA ["logstring"] enthält "Cluster Disk 10"** . Dadurch erhalten Sie die folgende Ausgabe:




### Timeout des physischen Datenträgers

Navigieren Sie zum Bericht, um dieses Problem zu diagnostizieren. Der Ordner enthält Protokolldateien und Dumpdateien für **RHS**, **ClusSvc. exe**und den Prozess, der den Dienst "**smphost**" hostet, wie unten dargestellt:

```
PS C:\Windows\system32> dir
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\Critical_PhysicalDisk_64acaf7e4590828ae8a3ac3c8b31da9a789586
d4_00000000_cab_1d94712e
```

Dies ist ein Beispiel für die Ausgabe:

```
 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
```

Beginnen Sie als nächstes mit der Selektierung aus der Datei " **Report. Wer** " – Hiermit wird angezeigt, welcher oder welche Ressource nicht mehr angezeigt wird.

```
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
```

Die Liste der Dienste und Prozesse, die in einem Dump gesammelt werden, wird durch die folgende Eigenschaft gesteuert: **PS c:\Windows\System32 > (Get-clusterresourcetype-Name "physischer Datenträger"). Dumpservicessmphost**

Um zu ermitteln, warum der Absturz aufgetreten ist, öffnen Sie die trag Dateien. Führen Sie dann die folgende Abfrage aus: **EventLog. EVENTDATA ["logstring"] enthält "Cluster** Datenträger 10", damit Sie die folgende Ausgabe erhalten:

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 | Leve | ActivityId | LevelDisplayNa | Timestamp | Mi | Chann | 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. |

Wir können dies mit dem Thread aus der Datei " **Memory. hdmp** " überprüfen:

```
# 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
```

# Problembehandlung bei einem Cluster Problem mit der Ereignis-ID 1135

03.06.2020 • 23 minutes to read • Edit Online

Dieser Artikel unterstützt Sie bei der Diagnose und Behebung der Ereignis-ID 1135, die während des Starts der Clusterdienst in der Failoverclustering-Umgebung protokolliert werden kann.

## Startseite

Die Ereignis-ID 1135 zeigt an, dass mindestens ein Cluster Knoten aus der aktiven failoverclustermitgliedschaft entfernt wurde. Möglicherweise werden die folgenden Symptome angezeigt:

- Cluster failover\knoten werden aus der aktiven failoverclustermitgliedschaft entfernt: Probleme mit Knoten, die aus der aktiven failoverclustermitgliedschaft entfernt werden
- Ereignis-ID 1069 Ereignis-ID 1069 – geclusterte Dienst-oder Anwendungs Verfügbarkeit
- Ereignis-ID 1177 für Quorum Verlust Ereignis-ID 1177 – Quorum und Konnektivität, die für das Quorum erforderlich sind
- Ereignis-ID 1006 für Clusterdienst angehalten: Ereignis-ID 1006 – Cluster Dienst Start

Eine Überprüfung und die Netzwerktests werden als einer der ersten Schritte zur Problembehandlung empfohlen, um sicherzustellen, dass keine Konfigurationsprobleme vorliegen, die eine Ursache für Probleme darstellen könnten.

**Überprüfen, ob die empfohlenen Hotfixes installiert sind**

Der Clusterdienst ist die wesentliche Softwarekomponente, die alle Aspekte des failoverclustervorgangs steuert und die Cluster Konfigurations Datenbank verwaltet. Wenn Sie die Ereignis-ID 1135 sehen, empfiehlt Microsoft Ihnen, die in den folgenden KB-Artikeln erwähnten Korrekturen zu installieren und alle Knoten des Clusters neu zu starten. Überprüfen Sie dann, ob das Problem erneut auftritt.

- Hotfix für Windows Server 2012 R2
- Hotfix für Windows Server 2012
- Hotfix für Windows Server 2008 R2

**Überprüfen Sie, ob der Cluster Dienst auf allen Knoten ausgeführt wird.**

Führen Sie den folgenden Befehl gemäß Ihrem Windows-Betriebssystem aus, um zu überprüfen, ob der Cluster Dienst kontinuierlich ausgeführt wird und verfügbar ist.

**Für Windows Server 2008 R2-Cluster**

Ausführen von cmd-Eingabeaufforderung mit erhöhten Rechten: `Cluster. exe-Knoten/stat`

**Für Windows Server 2012 \ und Windows Server 2012 R2-Cluster**

Ausführen des PS-Befehls: `Cluster Knoten/Status`

Wird der Cluster Dienst fortlaufend ausgeführt und ist auf allen Knoten verfügbar?

## Fehler bei der Lösung für den Cluster Dienst.

Wenn der Cluster Dienst ausfällt, beheben Sie die Problembehandlung in diesem Artikel: Windows Server 2008 und 2008R2-failoverclusterstartschalter.

# Mehrere Szenarien der Ereignis-ID 1135

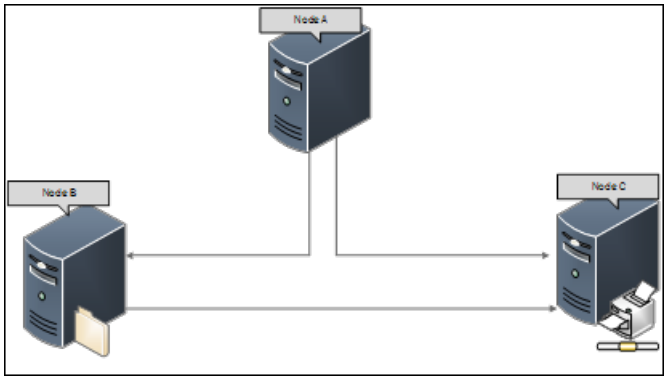
Wir möchten, dass Sie sich die System Ereignisprotokolle auf allen Knoten des Clusters genauer ansehen. Überprüfen Sie die Ereignis-ID 1135, die auf den Knoten angezeigt wird, und kopieren Sie alle Instanzen dieses Ereignisses. Dies erleichtert es Ihnen, Sie zu sehen und zu überprüfen.

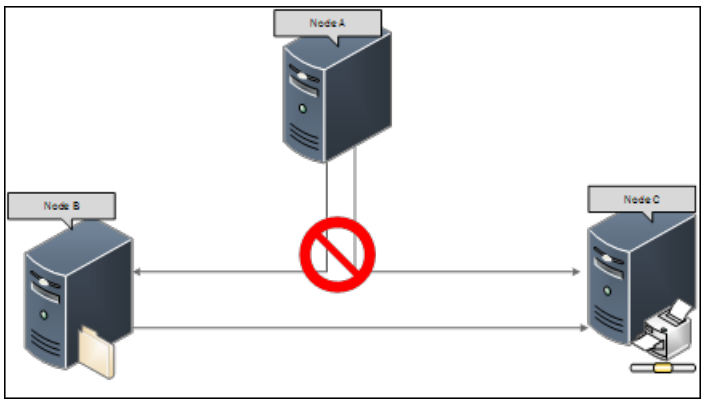
```
Event ID 1135
Cluster node ' **NODE A** ' was removed from the active failover cluster membership. The Cluster service on
this node may have stopped. This could also be due to the node having lost communication with other active
nodes in the failover cluster. Run the Validate a Configuration wizard 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.
```

Es gibt drei typische Szenarien:

### Szenario A

Sie sehen sich alle Ereignisse an, und alle Knoten im Cluster weisen darauf hin, dass die Kommunikation von Knoten A verloren gegangen ist.




Möglicherweise ist es möglich, dass beim Anzeigen der Systemprotokolle auf Knoten A Ereignisse für alle verbleibenden Knoten im Cluster angezeigt werden.

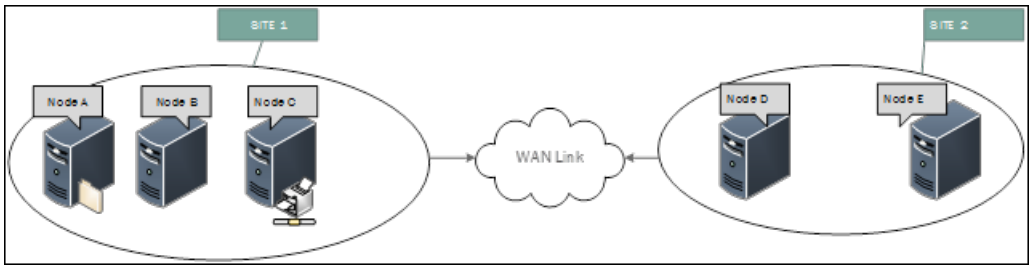
#### Lösung

Dies deutet darauf hin, dass zum Zeitpunkt des Problems entweder aufgrund einer Überlastung des Netzwerks oder andernfalls die Kommunikation mit dem Knoten A verloren gegangen ist.

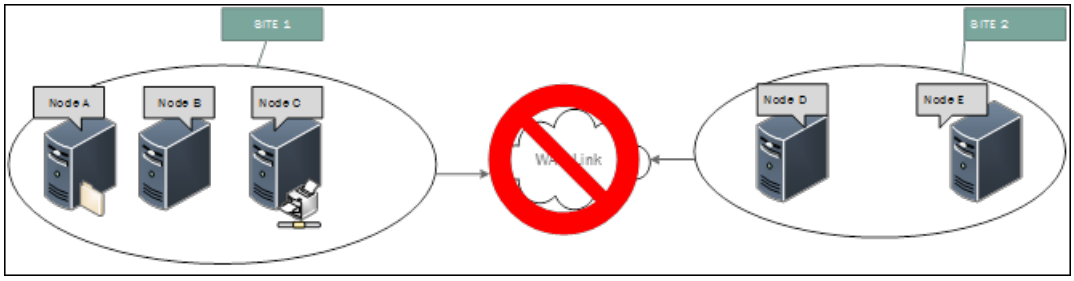
Sie sollten die Probleme mit der Netzwerkkonfiguration und der Kommunikation überprüfen und überprüfen. Denken Sie daran, nach Problemen im Zusammenhang mit Knoten A zu suchen.

### Szenario B

Sie sehen sich die Ereignisse auf den Knoten an, und wir sagen, dass Ihr Cluster auf zwei Standorte verteilt ist. Knoten a, Knoten B und Knoten C an Standort 1 und Knoten D & Knoten E an Standort 2.




Auf den Knoten A, B und C werden Sie feststellen, dass die protokollierten Ereignisse für die Konnektivität mit den Knoten D & E stehen. Wenn die Ereignisse auf Knoten D & E angezeigt werden, wird auf ähnliche Weise empfohlen, die Kommunikation mit A, B und C zu verlieren.



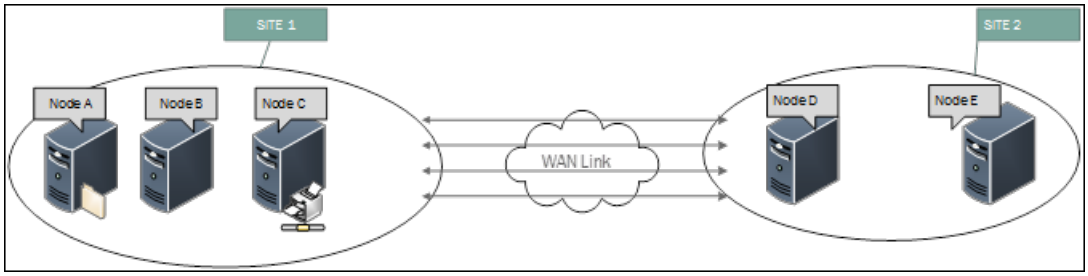

**Lösung**

Wenn eine ähnliche Aktivität angezeigt wird, weist dies darauf hin, dass ein Kommunikationsfehler aufgetreten ist, über den Link, der diese Standorte verbindet. Wir empfehlen Ihnen, die Verbindung über die Websites hinweg zu überprüfen. wenn es sich um eine WAN-Verbindung handelt, sollten Sie die Verbindung mit Ihrem ISP über die Konnektivität überprüfen.

### Szenario C

Sie sehen sich die Ereignisse auf den Knoten an, und Sie sehen, dass die Namen der Knoten nicht mit einem bestimmten Muster übereinstimmen. Nehmen wir an, dass Ihr Cluster auf zwei Standorte verteilt ist. Knoten a, Knoten B und Knoten C an Standort 1 und Knoten D & Knoten E an Standort 2.

- Auf Knoten A: Sie sehen Ereignisse für die Knoten B, D, E.
- Auf Knoten B: Sie sehen Ereignisse für die Knoten C, D, E.
- Auf Knoten C: werden Ereignisse für die Knoten A, B, E angezeigt.
- Auf Knoten D: Sie sehen Ereignisse für die Knoten A, C, E.
- Auf Knoten E: Es werden Ereignisse für die Knoten B, C, D angezeigt.
- Oder eine beliebige andere Kombination.




**Lösung**

Solche Ereignisse sind möglich, wenn die Netzwerk Kanäle zwischen den Knoten unterstrichen sind und die Cluster Kommunikations Nachrichten nicht rechtzeitig erreicht werden. Dadurch kann der Cluster die Kommunikation zwischen den Knoten verlieren, was dazu führt, dass Knoten aus der Cluster Mitgliedschaft entfernt werden.

## Überprüfen von Cluster Netzwerken

Es wird empfohlen, dass Sie die Cluster Netzwerke überprüfen, indem Sie die folgenden drei Optionen nacheinander überprüfen, um dieses Handbuch zur Problembehandlung fortzusetzen.

**Auf antivirenausschluss überprüfen**

Schließen Sie die folgenden Dateisystem Speicherorte von der Viren Überprüfung auf einem Server aus, auf dem Cluster Dienste ausgeführt werden:

- Der Pfad des Dateifreigabe Zeugen.
- Der *Ordner "%systemroot%\cluster* "

Konfigurieren Sie die Echt Zeit Scan Komponente in der Antivirussoftware, um die folgenden Verzeichnisse und Dateien auszuschließen:

- Standard Konfigurationsverzeichnis für virtuelle Maschinen (c:\ProgramData\Microsoft\Windows\Hyper-v)
- Konfigurations Verzeichnisse für benutzerdefinierte virtuelle Computer
- Standardverzeichnis für virtuelle Festplattenlaufwerke (c:\Users\Public\Documents\Hyper-v\virtuelle Festplatten)
- Benutzerdefinierte virtuelle Festplatten Laufwerks Verzeichnisse
- Benutzerdefinierte Replikations Datenverzeichnisse bei Verwendung des Hyper-V-Replikats
- Momentaufnahme Verzeichnisse
- MMS. exe

  > **NOTE**
  > Diese Datei muss möglicherweise als Prozess Ausschluss innerhalb der Antivirussoftware konfiguriert werden.)

- VMWP. exe

  > **NOTE**
  > Diese Datei muss möglicherweise als Prozess Ausschluss innerhalb der Antivirussoftware konfiguriert werden.

Wenn Sie Livemigration in Verbindung mit freigegebenen Clustervolumes verwenden, schließen Sie außerdem den CSV-Pfad *c:\ClusterStorage* und alle zugehörigen Unterverzeichnisse aus. Wenn Sie Failoverprobleme beheben oder allgemeine Probleme bei der Installation von Cluster Diensten und Antivirussoftware auftreten, deinstallieren Sie die Antivirussoftware vorübergehend, oder überprüfen Sie den Hersteller der Software, um zu ermitteln, ob die Antivirensoftware mit den Cluster Diensten Die Deaktivierung der Antivirussoftware ist in den meisten Fällen nicht ausreichend. Auch wenn Sie die Antivirussoftware deaktivieren, wird der Filtertreiber immer noch geladen, wenn Sie den Computer neu starten.

**Überprüfen der Netzwerk Port Konfiguration in der Firewall**

Der Clusterdienst steuert Server Cluster Vorgänge und verwaltet die Cluster Datenbank. Bei einem Cluster handelt es sich um eine Sammlung von unabhängigen Computern, die als einzelner Computer fungieren. Vorgesetzten, Programmierern und Benutzern wird der Cluster als einzelnes System angezeigt. Die Software verteilt Daten zwischen den Knoten des Clusters. Wenn ein Knoten ausfällt, stellen andere Knoten die Dienste und Daten bereit, die zuvor vom fehlenden Knoten bereitgestellt wurden. Wenn ein Knoten hinzugefügt oder repariert wird, werden von der Cluster Software einige Daten zu diesem Knoten migriert.

System Dienst Name: `ClusSvc`

| APPLICATION | PROTOCOL | PORTS |
| --- | --- | --- |
| Cluster Dienst | UDP | 3343 |
| Cluster Dienst | TCP | 3343 (dieser Port ist bei einem Knoten Verknüpfungs Vorgang erforderlich.) |
| RPC | TCP | 135 |
| Cluster Verwaltung | UDP | 137 |
| Kerberos | udp\tcp | 464 * |
| SMB | TCP | 445 |
| Nach dem Zufallsprinzip zugewiesene hohe UDP-Ports * * | UDP | Zufällige Portnummer zwischen 1024 und 65535<br>Zufällige Portnummer zwischen 49152 und 65535 * * * |
| | | |

> **NOTE**
> Außerdem sollten Sie für die erfolgreiche Überprüfung von Windows-Failoverclustern unter Windows Server 2008 und höher eingehenden und ausgehenden Datenverkehr für ICMP4, ICMP6 zulassen.

- Weitere Informationen finden Sie unter Erstellen eines Windows Server 2012-Failoverclusters schlägt fehl mit Fehler 0xc000005e.
- Weitere Informationen zum Anpassen dieser Ports finden Sie unter Dienst Übersicht und Netzwerk Port Anforderungen für Windows im Abschnitt "Verweise".

Dies ist der Bereich in Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows Server 2008 und Windows Vista.

Führen Sie außerdem den folgenden Befehl aus, um die Konfiguration des Netzwerk Ports in der Firewall zu überprüfen. Beispiel: Dieser Befehl hilft bei der Ermittlung von Port 3343 available\open, der für den Failovercluster verwendet wird:

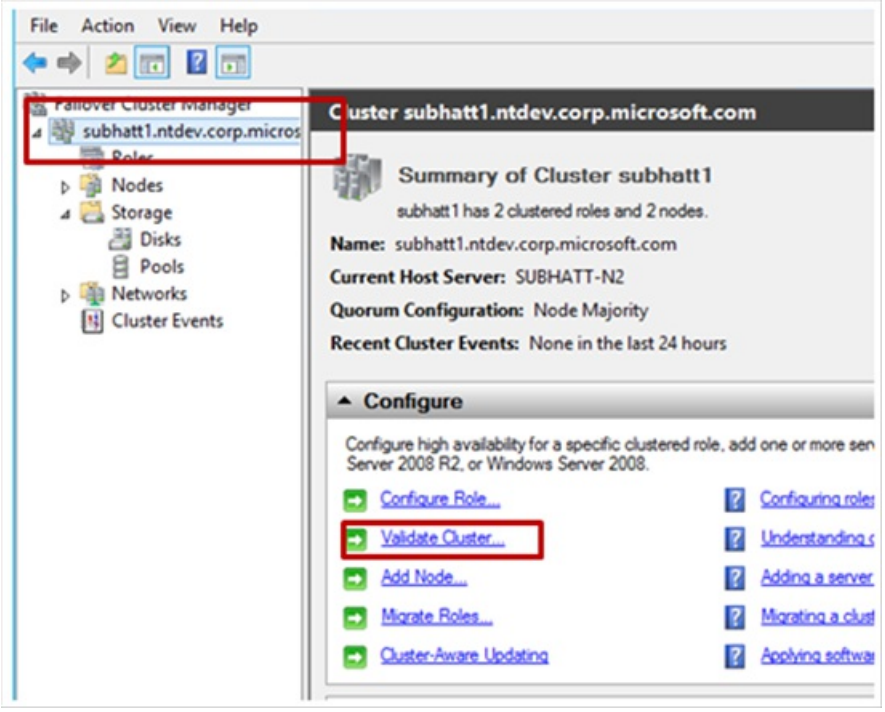
```
netsh advfirewall firewall show rule name="Failover Clusters (UDP-In)" verbose
```

### Ausführen des Cluster Validierungs Berichts für Fehler oder Warnungen

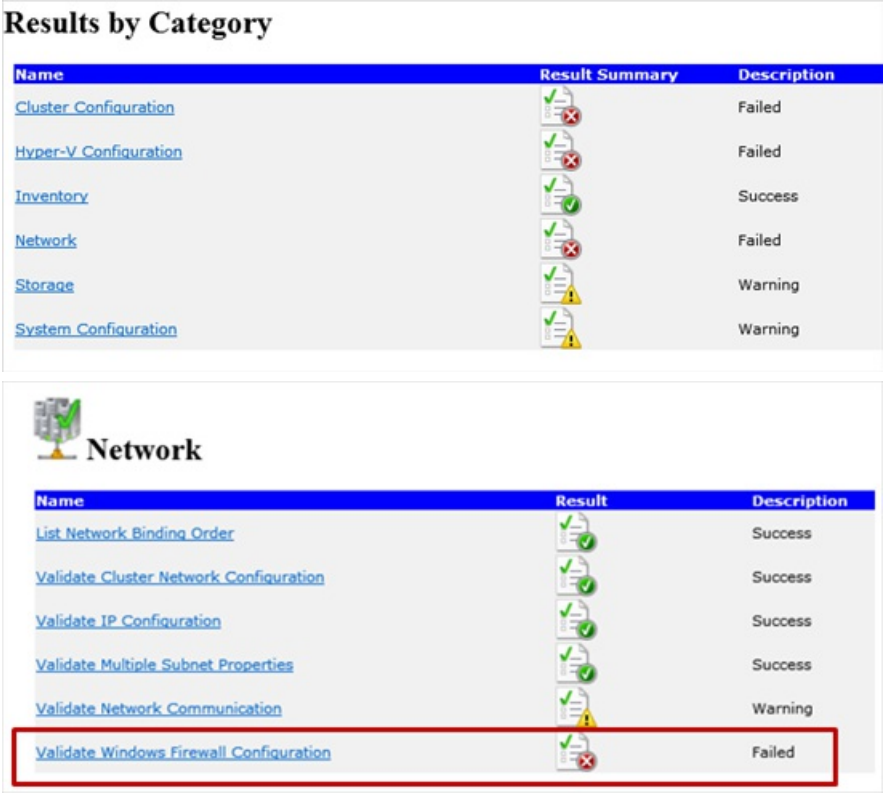
Das Cluster Überprüfungs Tool führt eine Reihe von Tests aus, um zu überprüfen, ob Ihre Hardware und Einstellungen mit dem Failoverclustering kompatibel sind.

Befolgen Sie diese Anweisungen:

1. Führen Sie den Cluster Validierungsbericht für Fehler oder Warnungen aus. Weitere Informationen finden Sie Untergrund Legendes zu Cluster Validierungs Tests: Netzwerk




2. Überprüfen Sie Warnungen und Fehler für Netzwerke. Weitere Informationen finden Sie Untergrund Legendes zu Cluster Validierungs Tests: Netzwerk.




**Überprüfen der Liste der Netzwerk Bindungs Reihenfolge**

Dieser Test listet die Reihenfolge auf, in der Netzwerke an die Adapter auf jedem Knoten gebunden werden.

Auf der Registerkarte Adapter und Bindungen werden die Verbindungen in der Reihenfolge aufgelistet, in der von Netzwerkdiensten auf die Verbindungen zugegriffen wird. Die Reihenfolge dieser Verbindungen gibt die Reihenfolge an, in der generische TCP/IP-Aufrufe/-Pakete an das Netzwerk gesendet werden.

Führen Sie die folgenden Schritte aus, um die Bindungs Reihenfolge der Netzwerkadapter zu ändern:

1. Klicken Sie im **Startmenü** auf **Ausführen**, geben Sie ncpa. cpl ein, und klicken Sie dann auf **OK**. Sie können die verfügbaren Verbindungen im **LAN-und Hochgeschwindigkeits-Internet** Abschnitt des Fensters **Netzwerkverbindungen** sehen.

2. Klicken Sie im Menü **erweitert** auf **Erweiterte Einstellungen**, und klicken Sie dann auf die Registerkarte **Adapter und Bindungen** .

3. Wählen Sie im Bereich **Verbindungen** die Verbindung aus, die Sie in der Liste nach oben verschieben möchten. Verwenden Sie die Pfeil Schaltflächen, um die Verbindung zu verschieben. Als allgemeine Regel gilt: die Karte, die mit dem Netzwerk kommuniziert (Domänen Konnektivität, Routing an andere Netzwerke usw.), sollte die erste gebundene Karte (oben auf der Liste) sein.

Cluster Knoten sind mehrfach vernetzte Systeme. Netzwerk Priorität wirkt sich auf den DNS-Client für ausgehende Netzwerk Konnektivität aus. Netzwerkadapter, die für die Client Kommunikation verwendet werden, sollten sich in der Bindungs Reihenfolge am Anfang befinden. Nicht weitergeleitete Netzwerke können mit niedrigerer Priorität platziert werden. In Windows Server 2012 und Windows Server2012 R2 der Cluster Netzwerktreiber (NetFT). Der sys-Adapter wird automatisch am unteren Rand der Liste der Bindungs Reihenfolge platziert.

#### Überprüfen Sie die Netzwerkkommunikation überprüfen

Dies kann auch dazu führen, dass die Latenz in Ihrem Netzwerk auftritt. Die Pakete können zwischen den Knoten nicht verloren gehen, Sie werden jedoch möglicherweise nicht schnell genug auf die Knoten übergegangen, bevor das Timeout abläuft.

Mit diesem Test wird überprüft, ob getestete Server mit akzeptabler Latenz in allen Netzwerken kommunizieren können.

Beispiel: unter Überprüfen der Netzwerkkommunikation werden möglicherweise folgende Meldungen zu Problemen mit der Netzwerk Latenz angezeigt.

```
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
```

Bei einem Cluster mit mehreren Standorten können Sie die Timeout Werte erhöhen. Weitere Informationen finden Sie unter Konfigurieren von Takt-und DNS-Einstellungen in einem Failovercluster mit mehreren StandOrten.

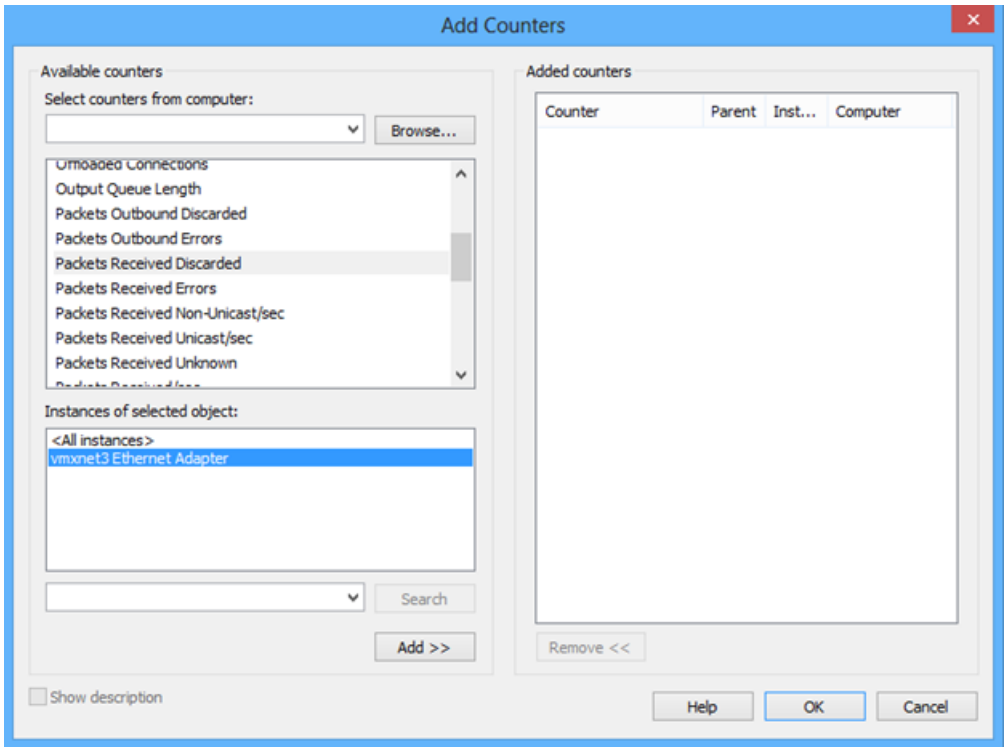
Wenden Sie sich an den ISP, um WAN-Verbindungsprobleme

Überprüfen Sie, ob die folgenden Probleme auftreten.

#### Zwischen Knoten verlorene Netzwerkpakete

1. Überprüfen von Paket Verlusten mithilfe der Leistung

   Wenn das Paket bei der Übertragung irgendwo zwischen den Knoten verloren geht, schlagen die Takte fehl. Wir können mühelos feststellen, ob es sich um ein Problem handelt. verwenden Sie hierzu den System Monitor, um den Leistungsindikatoren "Netzwerkschnittstelle\Empfangene Pakete erhalten" zu betrachten Wenn Sie diesen Leistungs Besatz hinzugefügt haben, sehen Sie sich die durchschnittlichen, minimalen und maximalen Zahlen an, und wenn es sich um einen Wert handelt, der größer als 0 (null) ist, muss der Empfangs Puffer für den Adapter angepasst werden.




Wenn Sie das Netzwerk Paket auf der VMware-Virtualisierungsplattform verloren haben, finden Sie weitere Informationen im Abschnitt "auf der VMware-Virtualisierungsplattform installierter Cluster

2. Aktualisieren der NIC-Treiber

   Dieses Problem kann aufgrund veralteter NIC-drivers\integration Components (IC) \vmtools oder fehlerhafter NIC-Adapter auftreten. Wenn zwischen den Knoten auf physischen Computern Netzwerkpakete verloren gehen, sollten Sie die Treiber Updates für den Netzwerkadapter durchführen. Alte oder veraltete Netzwerkkarten Treiber und/oder Firmware. Manchmal kann eine einfache Fehlkonfiguration der Netzwerkkarte oder des Schalters auch zu einem Verlust von Takten führen.

#### Cluster auf der VMware-Virtualisierungsplattform installiert

Überprüfen Sie die VMware-Adapter Probleme im Falle einer VMware-Umgebung.

Dieses Problem tritt möglicherweise auf, wenn die Pakete bei hohem Datenverkehrs aufkommen gelöscht werden. Stellen Sie sicher, dass keine Datenverkehrs Filterung stattfindet (z. b. mit einem e-Mail-Filter). Nachdem Sie diese Möglichkeit beseitigt haben, erhöhen Sie die Anzahl von Puffern im Gast Betriebssystem schrittweise, und überprüfen Sie, ob

Führen Sie die folgenden Schritte aus, um Burst Datenverkehr zu verringern:

1. Öffnen Sie das Testfeld mit der Windows-Taste + R.
2. Geben Sie devmgmt. msc ein, und drücken **Sie Eingabe**Taste.
3. Erweitern von **Netzwerkadaptern**
4. Klicken Sie mit der rechten Maustaste auf **vmxnet3, und klicken Sie**
5. Klicken Sie auf die Registerkarte **Erweitert**.
6. Klicken Sie auf **kleine RX-Puffer** , und erhöhen Sie den Wert. Der Standardwert ist 512, und der Höchstwert beträgt 8192.
7. Klicken Sie auf **RX-Ring #1** Größe, und erhöhen Sie den Wert. Der Standardwert ist 1024, und der Höchstwert beträgt 4096.

Überprüfen Sie die folgenden URLs, um Probleme bei VMware-Adaptern bei der VMware-Umgebung zu überprüfen

- Knoten werden aus der failoverclustermitgliedschaft in VMware ESX entfernt?

- Großer Paketverlust auf der Ebene des Gast Betriebssystems auf der VMXNET3-vNIC in ESXi

#### Netzwerk Überlastung bemerkt

Netzwerk Überlastung kann auch Probleme mit der Netzwerkverbindung verursachen.

Überprüfen Sie, ob Ihr Netzwerk gemäß MS und den Empfehlungen des Anbieters konfiguriert ist, siehe Konfigurieren von Windows-failoverclusternetzwerken

#### Überprüfen Sie die Netzwerkkonfiguration.

Wenn dies immer noch nicht funktioniert, überprüfen Sie, ob Sie ein partitioniertes Netzwerk in der Cluster-GUI oder NIC-Team Vorgang auf der Takt-NIC aktiviert haben.

Wenn Sie ein partitioniertes Netzwerk in der Cluster-GUI sehen, finden Sie weitere Informationen unter "partitionierte" Cluster Netzwerke , um das Problem zu beheben.

Wenn Sie NIC-Team Vorgang auf der Takt-NIC aktiviert haben, überprüfen Sie die Funktion "Team Vorgang Software" gemäß der Empfehlung des Hersteller Anbieters.

#### Aktualisieren der NIC-Treiber

Dieses Problem kann aufgrund veralteter NIC-Treiber oder fehlerhafter NIC-Adapter auftreten.

Wenn zwischen den Knoten auf physischen Computern Netzwerkpakete verloren gehen, lassen Sie den Treiber für den Netzwerkadapter aktualisieren. Alte oder veraltete Netzwerkkarten Treiber und/oder Firmware.

Manchmal kann eine einfache Fehlkonfiguration der Netzwerkkarte oder des Schalters auch zu einem Verlust von Takten führen.

#### Überprüfen Sie die Netzwerkkonfiguration.

Wenn dies immer noch nicht funktioniert, überprüfen Sie, ob Sie ein partitioniertes Netzwerk in der Cluster-GUI gesehen haben oder ob NIC-Team Vorgang auf der Takt-NIC aktiviert ist.

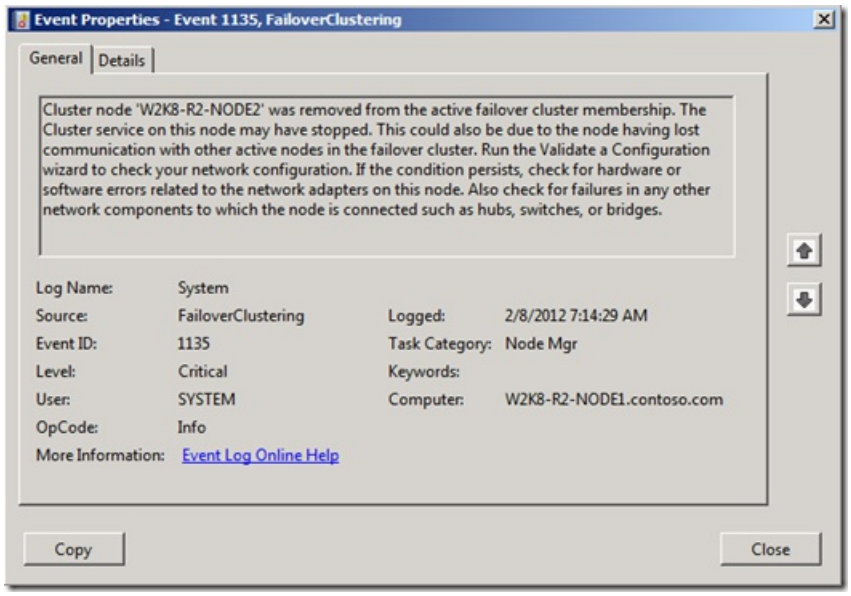
# Probleme mit Knoten, die aus der Mitgliedschaft des aktiven Failoverclusters entfernt wurden

03.06.2020 • 11 minutes to read • Edit Online

In diesem Artikel wird erläutert, wie Sie die Probleme beheben, bei denen Knoten zufällig aus der aktiven failoverclustermitgliedschaft entfernt werden.

## Symptome

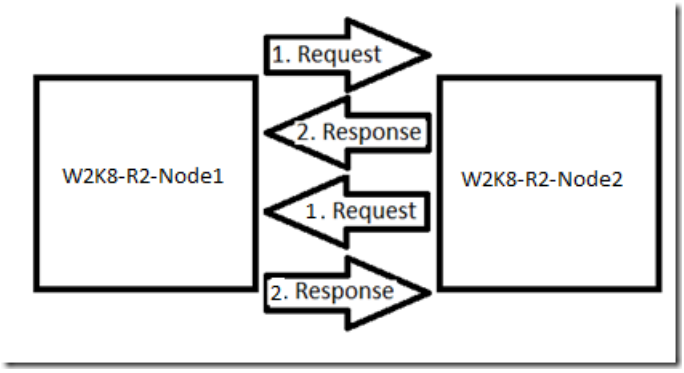
Wenn das Problem auftritt, sehen Sie, dass Ereignisse wie diese in Ihrem System Ereignisprotokoll protokolliert werden:




Dieses Ereignis wird auf allen Knoten im Cluster protokolliert, ausgenommen dem Knoten, der entfernt wurde. Der Grund für dieses Ereignis ist, dass einer der Knoten im Cluster den Knoten als "herunter" markiert hat. Anschließend werden alle anderen Knoten des Ereignisses benachrichtigt. Wenn die Knoten benachrichtigt werden, brechen Sie Ihre Takt Verbindungen mit dem untergeordneten Knoten ab und brechen Sie ab.

## Was hat bewirkt, dass der Knoten markiert ist

Alle Knoten in einem Windows 2008-oder 2008 R2-Failovercluster kommunizieren miteinander über die Netzwerke, die für die Netzwerkkommunikation im Netzwerk in diesem Netzwerk festgelegt sind. Die Knoten senden Takt Pakete über diese Netzwerke an alle anderen Knoten. Diese Pakete sollen von den anderen Knoten empfangen werden, und anschließend wird eine Antwort zurückgesendet. Jeder Knoten im Cluster weist seine eigenen Takte auf, die überwacht werden, um sicherzustellen, dass das Netzwerk aktiv ist und die anderen Knoten aktiv sind. Das folgende Beispiel sollte Ihnen helfen, dies zu verdeutlichen:




Wenn keines dieser Pakete zurückgegeben wird, wird der jeweilige Takt als fehlerhaft betrachtet. Beispielsweise sendet W2K8-R2-Node2 eine Anforderung und empfängt eine Antwort von W2K8-R2-Node1 an ein Takt Paket, damit das Netzwerk bestimmt wird und der Knoten aktiv ist. Wenn W2K8-R2-Node1 eine Anforderung an W2K8-R2-Node2 sendet und W2K8-R2-Node1 die Antwort nicht erhält, wird Sie als verlorener Takt angesehen, und W2K8-R2-Node1 verfolgt Sie nach. Diese verpasste Antwort kann W2K8-R2-Node1 das Netzwerk anzeigen, bis eine andere Takt Anforderung empfangen wird.

Standardmäßig sind für Cluster Knoten fünf Fehler in 5 Sekunden festgelegt, bevor die Verbindung markiert wird. Wenn W2K8-R2-Node1 die Antwort nicht fünfmal im Zeitraum empfängt, wird diese bestimmte Route als "W2K8-R2-Node2" betrachtet. Wenn andere Routen weiterhin als aktiv angesehen werden, bleibt W2K8-R2-Node2 als aktives Mitglied.

Wenn alle Routen für W2K8-R2-Node2 gekennzeichnet sind, werden Sie aus der aktiven failoverclustermitgliedschaft entfernt. das Ereignis 1135, das Sie im ersten Abschnitt sehen, wird protokolliert. Auf W2K8-R2-Node2 wird der Cluster Dienst beendet und dann neu gestartet, damit versucht wird, den Cluster erneut beizutreten.

Weitere Informationen zur Handhabung bestimmter Routen mit drei oder mehr Knoten finden Sie im Blog "partitionierte" Cluster Netzwerke , der von Jeff Hughes geschrieben wurde.

## Nachdem wir nun wissen, wie der Takt Prozess funktioniert, sind einige der bekannten Gründe für einen fehlerhaften Prozess zu erkennen.

1. Tatsächliche Netzwerkhardware Fehler. Wenn das Paket bei der Übertragung irgendwo zwischen den Knoten verloren geht, schlagen die Takte fehl. Dies wird durch eine Netzwerk Ablauf Verfolgung von beiden beteiligten Knoten offengelegt.

2. Das Profil für Ihre Netzwerkverbindungen kann möglicherweise erneut von Domäne zu öffentlich und wieder zurück in die Domäne überspringt werden. Während des Übergangs dieser Änderungen kann die Netzwerk-e/a blockiert werden. Sie können überprüfen, ob dies der Fall ist, indem Sie sich das Netzwerk Profil des Betriebs Protokolls ansehen. Sie finden dieses Protokoll durch Öffnen des Ereignisanzeige und navigieren zu: Anwendungs-und dienstprotokolle\microsoft\windows\networkprofile\operational. Sehen Sie sich die Ereignisse in diesem Protokoll auf dem Knoten an, der in der Ereignis-ID: 1135 erwähnt wurde, und überprüfen Sie, ob das Profil zu diesem Zeitpunkt geändert wurde. Wenn dies der Fall ist, lesen Sie den KB-Artikel Netzwerkadressen Profile von "Domäne" in "öffentlich" in Windows 7 oder in Windows Server 2008 R2.

3. Auf den Servern ist IPv6 aktiviert, aber die folgenden beiden Regeln sind für eingehende und ausgehende Daten in der Windows-Firewall deaktiviert:

   - Kern Netzwerk-Nachbar Ermittlungs Ankündigung
   - Kern Netzwerk-Nachbar Ermittlungs Anfrage

4. Die Antivirussoftware könnte diesen Prozess ebenfalls beeinträchtigen. Wenn Sie dies vermuten, testen Sie die Software, indem Sie Sie deaktivieren oder deinstallieren. Führen Sie dies auf eigene Gefahr aus, da Sie an

diesem Punkt nicht gegen Viren geschützt werden.

5. Dies kann auch dazu führen, dass die Latenz in Ihrem Netzwerk auftritt. Die Pakete können zwischen den Knoten nicht verloren gehen, Sie werden jedoch möglicherweise nicht schnell genug auf die Knoten übergegangen, bevor das Timeout abläuft.

6. IPv6 ist das Standardprotokoll, das von Failoverclustering für die Takte verwendet wird. Der Heartbeat selbst ist ein UDP-unicastnetzwerkpaket, das über Port 3343 kommuniziert. Wenn Switches, Firewalls oder Router nicht ordnungsgemäß konfiguriert sind, um diesen Datenverkehr durch zuzulassen, können Probleme wie diese auftreten.

7. Diese Probleme können auch durch IPSec-Sicherheitsrichtlinien aktualisiert werden. Das besondere Problem besteht darin, dass während der Aktualisierung der IPSec-Gruppenrichtlinie alle IPSec-Sicherheits Zuordnungen (SAS) von der Windows-Firewall mit erweiterter Sicherheit (wfas) abgebrochen werden. In diesem Fall wird die gesamte Netzwerk Konnektivität blockiert. Wenn beim Durchführen der Authentifizierung mit Active Directory Verzögerungen beim Durchführen der Sicherheits Zuordnungen auftreten, blockieren diese Verzögerungen (bei denen die gesamte Netzwerkkommunikation blockiert ist) auch die Durchführung von Cluster Takten und bewirken, dass die Cluster Integritäts Überwachung Knoten als instand erkennt, wenn Sie nicht innerhalb des Schwellenwerts von 5 Sekunden reagieren.

8. Alte oder veraltete Netzwerkkarten Treiber und/oder Firmware. Manchmal kann eine einfache Fehlkonfiguration der Netzwerkkarte oder des Schalters auch zu einem Verlust von Takten führen.

9. Bei modernen Netzwerkkarten und virtuellen Netzwerkkarten ist möglicherweise ein Paketverlust aufgetreten. Dies kann nachverfolgt werden, indem Sie den System Monitor öffnen und den Leistungsindikatoren "Netzwerkschnittstelle\Empfangene Pakete" hinzufügen. Dieser Wert ist kumulativ und wird nur erhöht, bis der Server neu gestartet wird. Eine große Anzahl von Paketen, die hier abgelegt werden, könnte ein Vorzeichen dafür sein, dass die Empfangs Puffer auf der Netzwerkkarte zu niedrig festgelegt sind oder der Server langsam funktioniert und den eingehenden Datenverkehr nicht verarbeiten kann. Jeder Netzwerkkarten Hersteller entscheidet, ob diese Einstellungen in den Eigenschaften der Netzwerkkarte verfügbar gemacht werden. Daher müssen Sie auf die Website des Herstellers verweisen, um zu erfahren, wie Sie diese Werte erhöhen und die empfohlenen Werte verwenden. Wenn Sie auf VMware ausführen, wird im folgenden Blog ausführlicher erläutert, wie Sie feststellen können, ob dies das Problem ist, und Sie werden auf den VMware-Artikel zu den zu ändernden Einstellungen verwiesen.

   Knoten, die aus der failoverclustermitgliedschaft in VMware ESX entfernt werden

Dies sind die häufigsten Gründe, aus denen diese Ereignisse protokolliert werden, aber es kann auch andere Gründe geben. Der Punkt dieses Blogs war, Ihnen einen Einblick in den Prozess zu vermitteln und außerdem Ideen dazu zu vermitteln, was Sie suchen sollten. Von einigen werden die folgenden Werte auf die maximalen Werte angehoben, um zu versuchen, dieses Problem zu verhindern.

| PARAMETER | STANDARD | RANGE |
|---|---|---|
| **SameSubnetDelay** | 1000 Millisekunden | 250-2000 Millisekunden |
| **CrossSubnetDelay** | 1000 Millisekunden | 250-4000 Millisekunden |
| **SameSubnetThreshold** | 5 | 3-10 |
| **CrossSubnetThreshold** | 5 | 3-10 |
| | | |

Wenn Sie diese Werte auf den maximalen Wert erhöhen, wird das Entfernen von Ereignis und Knoten möglicherweise entfernt, und das Problem wird lediglich maskiert. Das Problem kann nicht behoben werden. Das

beste daran ist, die Grundursache der Takt Ausfälle zu finden und diese festzulegen. Die einzige wirkliche Notwendigkeit, diese Werte zu erhöhen, liegt in einem Szenario mit mehreren Standorten, bei dem sich Knoten an unterschiedlichen Standorten befinden und die Netzwerk Latenz nicht umgangen werden kann.

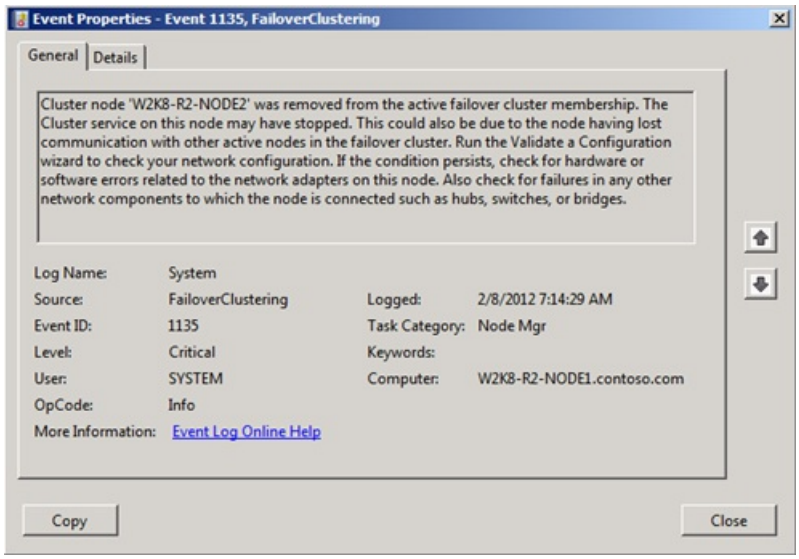
# Knoten, die aus der failoverclustermitgliedschaft in VMware ESX entfernt werden

29.05.2020 • 2 minutes to read • Edit Online

In diesem Artikel wird das Auffinden von Knoten, die aus der aktiven failoverclustermitgliedschaft entfernt werden, beim Hosten der Knoten in VMware ESX behandelt.

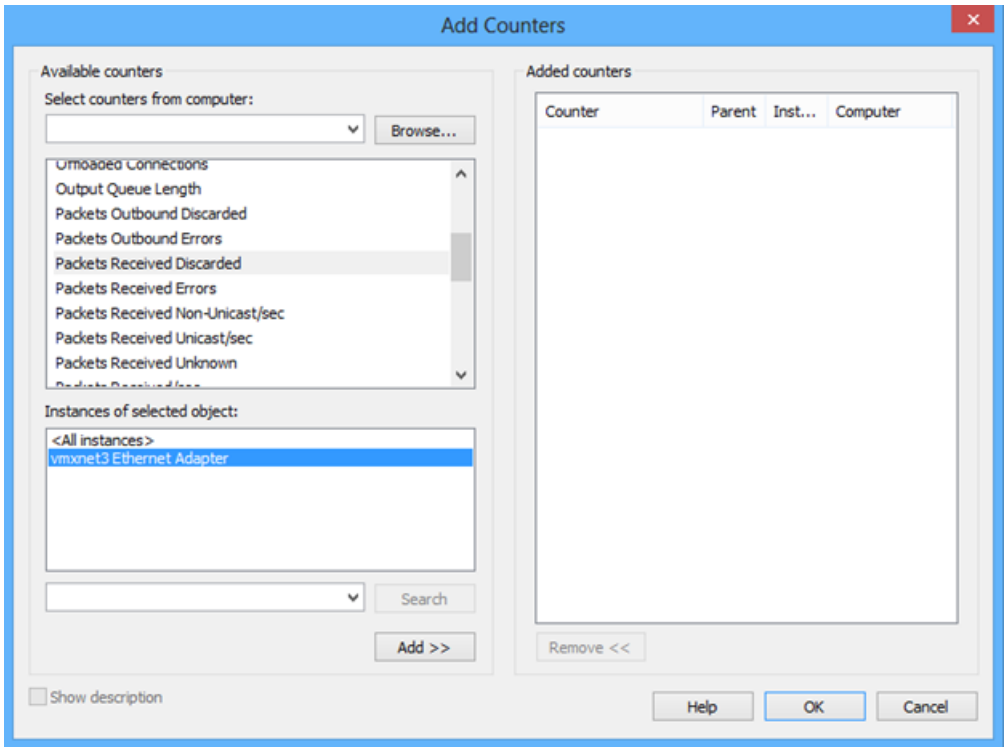
## Symptom

Wenn das Problem auftritt, wird im System Ereignisprotokoll des Ereignisanzeige Folgendes angezeigt:




## Lösung

Ein bestimmtes Problem besteht darin, dass die VMXNET3-Adapter eingehende Netzwerkpakete verwerfen, weil der eingehende Puffer zu niedrig eingestellt ist, um große Mengen an Datenverkehr zu verarbeiten. Wir können mühelos feststellen, ob es sich um ein Problem handelt. verwenden Sie hierzu den System Monitor, um den Leistungsindikatoren "Netzwerkschnittstelle\Empfangene Pakete erhalten" zu betrachten




Wenn Sie diesen Leistungs Besatz hinzugefügt haben, sehen Sie sich die durchschnittlichen, minimalen und maximalen Zahlen an, und wenn es sich um einen Wert handelt, der größer als 0 (null) ist, muss der Empfangs Puffer für den Adapter angepasst werden. Dieses Problem ist in der Knowledge Base von VMware dokumentiert: großer Paketverlust auf der Ebene des Gast Betriebssystems auf der VMXNET3-vNIC in ESXi 5. x/4. x.

# IaaS mit SQL Always On: Optimieren der Failovercluster-Netzwerkschwellenwerte

29.05.2020 • 8 minutes to read • Edit Online

In diesem Artikel werden Lösungen zum Anpassen des Schwellenwerts von failoverclusternetzwerken vorgestellt.

## Symptom

Wenn Sie Windows-Failoverclusterknoten in IaaS mit SQL Server AlwaysOn ausführen, wird empfohlen, die Cluster Einstellung in einen stärker gelockerten Überwachungs Status zu ändern. Standardmäßig sind die Cluster Einstellungen restriktiv und können zu nicht benötigten Ausfällen führen. Die Standardeinstellungen sind für hochoptimierte lokale Netzwerke konzipiert und berücksichtigen nicht die Möglichkeit der durch eine mehr Instanzen fähigen Umgebung, wie z. b. Windows Azure (IaaS), verursachten Latenz.

Das Windows Server-Failoverclustering überwacht ständig die Netzwerkverbindungen und die Integrität der Knoten in einem Windows-Cluster. Wenn ein Knoten über das Netzwerk nicht erreichbar ist, wird eine Wiederherstellungsaktion ausgeführt, um die Anwendungen und Dienste auf einem anderen Knoten im Cluster wieder online zu schalten. Die Latenz bei der Kommunikation zwischen Cluster Knoten kann zu folgendem Fehler führen:

> Fehler 1135 (System Ereignisprotokoll)

Der Cluster Knoten **Node1** wurde aus der aktiven failoverclustermitgliedschaft entfernt. Die Clusterdienst auf diesem Knoten wurde möglicherweise beendet. Dies kann auch darauf zurückzuführen sein, dass der Knoten die Kommunikation mit anderen aktiven Knoten im Failovercluster verloren hat. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit den Netzwerkadaptern auf diesem Knoten vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

Beispiel für Cluster. log:

```
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)
```

## Ursache

Zum Konfigurieren der konnektivitätsintegrität des Clusters werden zwei Einstellungen verwendet.

**Delay** – definiert die Häufigkeit, mit der Cluster Takte zwischen Knoten gesendet werden. Die Verzögerung ist die Anzahl der Sekunden, bevor der nächste Takt gesendet wird. Innerhalb desselben Clusters kann es unterschiedliche Verzögerungen zwischen Knoten im gleichen Subnetz und zwischen Knoten geben, die sich in unterschiedlichen Subnetzen befinden.

**Threshold** – definiert die Anzahl von Takten, die übersehen werden, bevor der Cluster eine Wiederherstellungs Aktion durchführt. Der Schwellenwert ist eine Anzahl von Takten. Innerhalb desselben Clusters können unterschiedliche Schwellenwerte zwischen Knoten im gleichen Subnetz und zwischen Knoten in unterschiedlichen Subnetzen vorhanden sein.

Standardmäßig legt Windows Server 2016 **samesubnetthreshold** auf 10 und **samesubnetdelay** auf 1000 ms fest. Wenn beispielsweise die Verbindungsüberwachung 10 Sekunden lang ausfällt, wird der failoverschwellen Wert erreicht, was dazu führt, dass der Knoten aus der Cluster Mitgliedschaft entfernt wurde. Dies führt dazu, dass die Ressourcen auf einen anderen verfügbaren Knoten im Cluster verschoben werden. Cluster Fehler werden gemeldet, einschließlich des Cluster Fehlers 1135 (oben).

# Lösung

Lockern Sie in einer IaaS-Umgebung die Konfigurationseinstellungen des Cluster Netzwerks.

### Schritte zum Überprüfen der aktuellen Konfiguration

Überprüfen Sie die aktuellen Cluster Netzwerk-Konfigurationseinstellungen, indem Sie den Befehl Get-Cluster verwenden:

```
C:\Windows\system32> get-cluster | fl *subnet*
```

Standard-, minimal-, höchst-und empfohlene Werte für jedes Support Betriebssystem

| | BETRIEBSSYSTEM | MIN | MAX | STANDARD | EMPFOHLEN |
|---|---|---|---|---|---|
| CrossSubnetThreshold | 2008 R2 | 3 | 20 | 5 | 20 |
| Crosssubnet-Schwellenwert | 2012 | 3 | 120 | 5 | 20 |
| Crosssubnet-Schwellenwert | 2012 R2 | 3 | 120 | 5 | 20 |
| Crosssubnet-Schwellenwert | 2016 | 3 | 120 | 20 | 20 |
| Samesubnet-Schwellenwert | 2008 R2 | 3 | 10 | 5 | 10 |
| Samesubnet-Schwellenwert | 2012 | 3 | 120 | 5 | 10 |
| Samesubnet-Schwellenwert | 2012 R2 | 3 | 120 | 5 | 10 |
| SameSubnetThreshold | 2016 | 3 | 120 | 10 | 10 |
| | | | | | |

Die Werte für Schwellenwert entsprechen den aktuellen Empfehlungen in Bezug auf den Umfang der Bereitstellung, wie im folgenden Artikel beschrieben:

Optimieren der Netzwerk Schwellenwerte für Failovercluster in Windows Server 2012 R2

Der **Schwellenwert** definiert die Anzahl der Takte, die übersehen werden, bevor der Cluster eine Wiederherstellungs Aktion durchführt. Der Schwellenwert ist eine Anzahl von Takten. Innerhalb desselben Clusters können unterschiedliche Schwellenwerte zwischen Knoten im gleichen Subnetz und zwischen Knoten vorhanden sein, die sich in unterschiedlichen Subnetzen befinden.

## Empfehlungen für die Umstellung auf die Einstellungen für mehr Instanzen fähige Umgebungen wie Azure (IaaS)

> **NOTE**
>
> Das Erhöhen der Resilienz ihrer Cluster Umgebung durch die Anpassung der Cluster Netzwerk-Konfigurationseinstellungen kann zu einer längeren Ausfallzeit führen. Weitere Informationen finden Sie unter Optimieren der Netzwerk Schwellenwerte für Failovercluster.

1. Ändern Sie die Einstellungen in den Einstellungen:

   > **NOTE**
   >
   > Das Ändern des Cluster Schwellenwerts wird sofort wirksam. Sie müssen den Cluster oder die Ressourcen nicht neu starten.

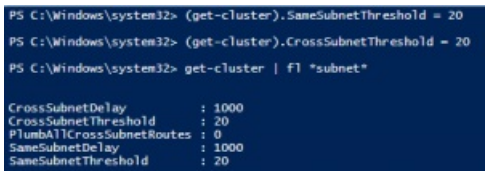
   Die folgenden Einstellungen werden sowohl für das gleiche Subnetz als auch für Regions übergreifende bereit Stellungen von AlwaysOn-Verfügbarkeits Gruppen empfohlen.

   ```
   C:\Windows\system32> (get-cluster).SameSubnetThreshold = 20
   ```

   ```
   C:\Windows\system32> (get-cluster).CrossSubnetThreshold = 20
   ```

2. Überprüfen Sie die Änderungen:

   ```
   C:\Windows\system32> get-cluster | fl *subnet*
   ```




## Referenzen

Weitere Informationen zum Optimieren der Netzwerk Konfigurationseinstellungen für Windows-Cluster finden Sie unter Optimieren der Netzwerk Schwellenwerte für Failovercluster.

Informationen zur Verwendung von "Cluster. exe" zum Optimieren der Netzwerk Konfigurationseinstellungen für Windows-Cluster finden Sie unter Konfigurieren von Cluster Netzwerken für einen Failovercluster.

# Failoverclustering-System Protokollereignisse

02.05.2020 • 133 minutes to read • Edit Online

Gilt für: Windows Server 2019, Windows Server 2016

In diesem Thema werden die Failoverclustering-Ereignisse aus dem Windows Server-System Protokoll (sichtbar in Ereignisanzeige) aufgelistet. Diese Ereignisse verwenden alle die Ereignis Quelle von **Failoverclustering** und können bei der Problembehandlung eines Clusters hilfreich sein.

## Kritische Ereignisse

### Ereignis 1000: UNEXPECTED_FATAL_ERROR

Unerwarteter schwerwiegender Fehler in Zeile %1 des Quell Moduls %2. Clusterdienst Fehlercode: %3.

### Ereignis 1001: ASSERTION_FAILURE

Fehler bei der Gültigkeits Überprüfung in Zeile "%1" des Quell Moduls "%2" Clusterdienst. "%3"

### Ereignis 1006: NM_EVENT_MEMBERSHIP_HALT

Clusterdienst wurde aufgrund unvollständiger Konnektivität mit anderen Cluster Knoten angehalten.

### Ereignis 1057: DM_DATABASE_CORRUPT_OR_MISSING

Die Cluster Datenbank konnte nicht geladen werden. Die Datei ist möglicherweise nicht vorhanden oder beschädigt. Es kann versucht werden, eine automatische Reparatur auszuführen.

### Ereignis 1070: NM_EVENT_BEGIN_JOIN_FAILED

Fehler beim Hinzufügen des Failoverclusters "%1" durch den Knoten aufgrund des Fehlercodes "%2".

### Ereignis 1073: CS_EVENT_INCONSISTENCY_HALT

Der Clusterdienst wurde angehalten, um eine Inkonsistenz innerhalb des Failoverclusters zu verhindern. Fehlercode: ' %1 '.

### Ereignis 1080: CS_DISKWRITE_FAILURE

Fehler beim Aktualisieren der Cluster Datenbank durch den Clusterdienst (Fehlercode "%1"). Mögliche Ursachen sind nicht genügend Speicherplatz oder eine Beschädigung des Dateisystems.

### Ereignis 1090: CS_EVENT_REG_OPERATION_FAILED

Der Clusterdienst kann nicht gestartet werden. Fehler beim Lesen von Konfigurationsdaten aus der Windows-Registrierung (Fehler: "%1"). Verwenden Sie das Failoverclusterverwaltungs-Snap-in, um sicherzustellen, dass dieser Computer Mitglied eines Clusters ist. Wenn Sie diesen Computer einem vorhandenen Cluster hinzufügen möchten, verwenden Sie den Assistenten zum Hinzufügen von Knoten. Wenn dieser Computer als Mitglied eines Clusters konfiguriert wurde, ist es auch erforderlich, die fehlenden Konfigurationsdaten wiederherzustellen, die für den Cluster Dienst erforderlich sind, um festzustellen, dass er ein Mitglied eines Clusters ist. Führen Sie eine System Status Wiederherstellung dieses Computers aus, um die Konfigurationsdaten wiederherzustellen.

### Ereignis 1092: NM_EVENT_MM_FORM_FAILED

Fehler beim Erstellen des Clusters "%1" mit dem Fehlercode "%2". Der Failovercluster ist nicht verfügbar.

### Ereignis 1093: NM_EVENT_NODE_NOT_MEMBER

Der Clusterdienst kann den Knoten "%1" nicht als Mitglied des Failoverclusters "%2" identifizieren. Wenn der Computername für diesen Knoten vor kurzem geändert wurde, sollten Sie den vorherigen Namen

wiederherstellen. Alternativ dazu können Sie den Knoten dem Failovercluster hinzufügen und ggf. Cluster Anwendungen neu installieren.

**Ereignis 1105: CS_EVENT_RPC_INIT_FAILED**

Der Clusterdienst konnte nicht gestartet werden, da die Schnittstelle (n) beim RPC-Dienst nicht registriert werden konnte. Fehlercode: ' %1 '.

**Ereignis 1135: EVENT_NODE_DOWN**

Der Cluster Knoten "%1" wurde aus der aktiven failoverclustermitgliedschaft entfernt. Die Clusterdienst auf diesem Knoten wurde möglicherweise beendet. Dies kann auch darauf zurückzuführen sein, dass der Knoten die Kommunikation mit anderen aktiven Knoten im Failovercluster verloren hat. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit den Netzwerkadaptern auf diesem Knoten vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

**Ereignis 1146: RCM_EVENT_RESMON_DIED**

Der RHS-Prozess (Cluster Ressourcenhosting-Subsystem) wurde beendet und wird neu gestartet. Dies ist in der Regel mit der Cluster Integritäts Erkennung und-Wiederherstellung einer Ressource verbunden. Bestimmen Sie anhand des System Ereignis Protokolls, welche Ressource und Ressourcen-DLL das Problem verursacht.

**Ereignis 1177: MM_EVENT_ARBITRATION_FAILED**

Der Clusterdienst wird heruntergefahren, weil das Quorum verloren gegangen ist. Dies kann auf den Verlust der Netzwerk Konnektivität zwischen einigen oder allen Knoten im Cluster oder einem Failover des Zeugen Datenträgers zurückzuführen sein.

Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

**Ereignis 1181: NETRES_RESOURCE_START_ERROR**

Die Cluster Ressource "%1" kann nicht online geschaltet werden, da der zugehörige Dienst nicht gestartet werden konnte. Der Dienst Rückgabecode ist "%2". Überprüfen Sie, ob dem Dienst weitere Ereignisse zugeordnet sind, und stellen Sie sicher, dass der Dienst richtig gestartet wird

**Ereignis 1247: CLUSTER_EVENT_INVALID_SERVICE_SID_TYPE**

Der Typ der Sicherheits-ID (SID) für den Cluster Dienst ist als "%1" konfiguriert, aber der erwartete SID-Typ ist "uneingeschränkt". Der Cluster Dienst ändert seine sid-typkonfiguration automatisch mit dem Dienststeuerungs-Manager (Service Control Manager, SCM) und wird neu gestartet, damit diese Änderung wirksam wird.

**Ereignis 1248: CLUSTER_EVENT_SERVICE_SID_MISSING**

Die mit dem Cluster Dienst verknüpfte Sicherheits-ID (SID) "%1" ist im Prozess Token nicht vorhanden. Der Cluster Dienst behebt dieses Problem automatisch und führt einen Neustart durch.

**Ereignis 1282: SM_EVENT_HANDSHAKE_TIMEOUT**

Der Sicherheits Hand Shake zwischen lokalen und Remote Endpunkten "%2" wurde in "%1" Sekunden nicht beendet, der Knoten beendet die Verbindung.

**Ereignis 1542: SERVICE_PRERESTORE_FAILED**

Die Wiederherstellungs Anforderung für die Cluster Konfigurationsdaten ist fehlgeschlagen. Diese Wiederherstellung ist während der Phase "vor der Wiederherstellung" nicht erfolgreich, was normalerweise darauf hinweist, dass einige Knoten, die den Cluster enthalten, zurzeit Stellen Sie sicher, dass der Cluster Dienst auf allen Knoten, die diesen Cluster umfassen, erfolgreich ausgeführt wird.

### Ereignis 1543: SERVICE_POSTRESTORE_FAILED

Fehler beim Wiederherstellungs Vorgang der Cluster Konfigurationsdaten. Bei dieser Wiederherstellung ist während der Phase "nach der Wiederherstellung" ein Fehler aufgetreten Es wird empfohlen, dass Sie die aktuelle Cluster Konfigurationsdatendatei (CLUSDB) durch "%1" ersetzen.

### Ereignis 1546: SERVICE_FORM_VERSION_INCOMPATIBLE

Der Knoten "%1" konnte keinen Failovercluster bilden. Dies liegt an einem oder mehreren Knoten, die inkompatible Versionen der Cluster Dienst Software ausführen. Wenn der Knoten "%1" oder ein anderer Knoten im Cluster vor kurzem aktualisiert wurde, überprüfen Sie, ob alle Knoten kompatible Versionen der Cluster Dienst Software ausführen.

### Ereignis 1547: SERVICE_CONNECT_VERSION_INCOMPATIBLE

Der Knoten "%1" hat versucht, einem Failovercluster beizutreten, konnte aber aufgrund von Inkompatibilität zwischen den Versionen der Cluster Dienst Software nicht ausgeführt werden. Wenn der Knoten "%1" oder ein anderer Knoten im Cluster vor kurzem aktualisiert wurde, überprüfen Sie, ob die geänderte Cluster Bereitstellung mit verschiedenen Versionen der Cluster Dienst Software unterstützt wird.

### Ereignis 1553: SERVICE_NO_NETWORK_CONNECTIVITY

Dieser Cluster Knoten verfügt über keine Netzwerk Konnektivität. Sie kann erst am Cluster teilnehmen, wenn die Verbindung wieder hergestellt wird. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

### Ereignis 1554: SERVICE_NETWORK_CONNECTIVITY_LOST

Dieser Cluster Knoten hat alle Netzwerkverbindungen verloren. Sie kann erst am Cluster teilnehmen, wenn die Verbindung wieder hergestellt wird. Der Cluster Dienst auf diesem Knoten wird beendet.

### Ereignis 1556: SERVICE_UNHANDLED_EXCEPTION_IN_WORKER_THREAD

Der Cluster Dienst hat ein unerwartetes Problem feststellen und wird heruntergefahren. Fehlercode: "%2".

### Ereignis 1561: SERVICE_NONSTORAGE_WITNESS_BETTER_TAG

Clusterdienst konnte nicht gestartet werden, da dieser Knoten festgestellt hat, dass er nicht über die neueste Kopie der Cluster Konfigurationsdaten verfügt. Die Änderungen am Cluster sind aufgetreten, während sich dieser Knoten nicht in der Mitgliedschaft befand und somit keine Konfigurationsdaten Aktualisierungen empfangen konnte.

#### Anleitungen

Versuchen Sie, den Cluster Dienst auf allen Knoten im Cluster zu starten, damit Knoten mit der neuesten Kopie der Cluster Konfigurationsdaten zuerst den Cluster bilden können. Dieser Knoten kann dann in den Cluster eingebunden werden und erhält automatisch die aktualisierten Cluster Konfigurationsdaten. Wenn keine Knoten mit der neuesten Kopie der Cluster Konfigurationsdaten verfügbar sind, führen Sie das Windows PowerShell-Cmdlet "Start-clusternode-f" aus. Mithilfe des ForceQuorum (FQ)-Parameters wird der Cluster Dienst gestartet, und die Kopie der Cluster Konfigurationsdaten dieses Knotens wird als autorisierend gekennzeichnet. Das Erzwingen des Quorums auf einem Knoten mit einer veralteten Kopie der Cluster Datenbank führt möglicherweise zu Änderungen an der Cluster Konfiguration, die aufgetreten sind, während der Knoten nicht an dem Cluster beteiligt war.

### Ereignis 1564: RES_FSW_ARBITRATEFAILURE

Die Dateifreigabe-Zeugen Ressource "%1" konnte die Dateifreigabe "%2" nicht überzeugen. Stellen Sie sicher, dass die Dateifreigabe "%2" vorhanden ist und dass der Cluster darauf zugreifen kann.

### Ereignis 1570: SERVICE_CONNECT_AUTHENTICATION_FAILURE

Der Knoten "%1" konnte beim beitreten zum Cluster keine Kommunikationssitzung einrichten. Dies war auf einen Authentifizierungsfehler zurückzuführen. Überprüfen Sie, ob die Knoten kompatible Versionen der Cluster Dienst

Software ausführen.

**Ereignis 1571: SERVICE_CONNECT_AUTHORIZAION_FAILURE**

Der Knoten "%1" konnte beim beitreten zum Cluster keine Kommunikationssitzung einrichten. Dies wurde aufgrund eines Autorisierungs Fehlers verursacht. Überprüfen Sie, ob die Knoten kompatible Versionen der Cluster Dienst Software ausführen.

**Ereignis 1572: SERVICE_NETFT_ROUTE_INITIAL_FAILURE**

Der Knoten "%1" konnte dem Cluster nicht beitreten, weil er keine Netzwerk Nachrichten zur Fehlererkennung mit anderen Cluster Knoten senden und empfangen konnte. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkeinstellungen sicherzustellen. Überprüfen Sie außerdem die Regeln der Windows-Firewall "Failovercluster".

**Ereignis 1574: DM_DATABASE_UNLOAD_FAILED**

Die failoverclusterdatenbank konnte nicht entladen werden. Wenn das Problem durch einen Neustart des Cluster Dienstanbieter nicht behoben werden kann, starten Sie den Computer neu.

**Ereignis 1575: DM_DATABASE_CORRUPT_OR_MISSING_FIXQUORUM**

Der Versuch, den Cluster Dienst zu erzwingen, ist fehlgeschlagen, da die Cluster Konfigurationsdaten auf diesem Knoten entweder nicht vorhanden oder beschädigt sind. Starten Sie zunächst den Cluster Dienst auf einem anderen Knoten, der über eine intakte und gültige Kopie der Cluster Konfigurationsdaten verfügt. Wiederholen Sie dann den Startvorgang auf diesem Knoten (der versucht, aktualisierte gültige Konfigurationsinformationen automatisch abzurufen). Wenn kein anderer Knoten verfügbar ist, verwenden Sie "Wbadmin. msc", um eine System Status Wiederherstellung dieses Knotens durchzuführen, um die Konfigurationsdaten wiederherzustellen.

**Ereignis 1593: DM_COULD_NOT_DISCARD_CHANGES**

Die failoverclusterdatenbank konnte nicht entladen werden, und möglicherweise falsche Änderungen im Arbeitsspeicher konnten nicht verworfen werden. Der Cluster Dienst versucht, die Datenbank zu reparieren, indem er von einem anderen Cluster Knoten abgerufen wird. Wenn der Cluster Dienst nicht online geschaltet wird, starten Sie den Cluster Dienst auf diesem Knoten neu. Wenn das Problem durch einen Neustart des Cluster Dienstanbieter nicht behoben werden kann, starten Sie den Computer neu. Wenn der Cluster Dienst nach einem Neustart nicht online geschaltet werden kann, stellen Sie die Cluster Datenbank aus der letzten Sicherung wieder her. Die aktuelle Datenbank wurde nach "%1" kopiert. Wenn keine Sicherungen verfügbar sind, kopieren Sie "%1" nach "%2", und versuchen Sie, den Cluster Dienst zu starten. Wenn der Cluster Dienst dann auf diesem Knoten online geschaltet wird, gehen möglicherweise einige Änderungen an der Cluster Konfiguration verloren, und der Cluster funktioniert möglicherweise nicht ordnungsgemäß. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Cluster Konfiguration zu überprüfen und sicherzustellen, dass die gehosteten Dienste und Anwendungen online und ordnungsgemäß funktionieren.

**Ereignis 1672: EVENT_NODE_QUARANTINED**

Der Cluster Knoten "%1" wurde unter Quarantäne gestellt. Im Knoten sind %2 aufeinanderfolgende Fehler innerhalb eines kurzen Zeitraums aufgetreten, der aus dem Cluster entfernt wurde, um weitere Unterbrechungen zu vermeiden. Der Knoten wird bis "%3" unter Quarantäne gestellt, und anschließend versucht der Knoten automatisch, den Cluster erneut beizutreten.

Informationen zu den Problemen auf diesem Knoten finden Sie in den System-und Anwendungs Ereignisprotokollen. Wenn das Problem behoben ist, kann die Quarantäne manuell gelöscht werden, damit der Knoten mit dem Windows PowerShell-Cmdlet "Start-clusternode – clearquarantäne" erneut verknüpft werden kann.

Knoten Name: %1

Anzahl der aufeinander folgenden Cluster Mitgliedschaften verliert: %2

Die Zeit Quarantäne wird automatisch gelöscht: %3

# Fehlerereignisse

**Ereignis 1024: CP_REG_CKPT_RESTORE_FAILED**

Der Registrierungs Prüf Punkt für die Cluster Ressource "%1" konnte nicht im Registrierungsschlüssel HKEY_LOCAL_MACHINE\"%2" wieder hergestellt werden. Die Ressource funktioniert möglicherweise nicht ordnungsgemäß. Stellen Sie sicher, dass keine anderen Prozesse über geöffnete Handles für Registrierungsschlüssel in dieser Registrierungs Unterstruktur verfügen.

**Ereignis 1034: RES_DISK_MISSING**

Die physische Datenträger Ressource "%1" des Clusters kann nicht online geschaltet werden, da der zugehörige Datenträger nicht gefunden wurde. Die erwartete Signatur des Datenträgers war "%2". Wenn der Datenträger ersetzt oder wieder hergestellt wurde, können Sie im Failovercluster-Manager-Snap-in die Reparatur Funktion (auf dem Blatt "Eigenschaften" für den Datenträger) verwenden, um den neuen oder wiederhergestellten Datenträger zu reparieren. Wenn der Datenträger nicht ersetzt wird, löschen Sie die zugehörige Datenträger Ressource.

**Ereignis 1035: RES_DISK_MOUNT_FAILED**

Beim Online schalten der Datenträger Ressource "%1" ist der Zugriff auf ein oder mehrere Volumes mit Fehler "%2" fehlgeschlagen. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Speicherkonfiguration zu überprüfen. Optional können Sie CHKDSK ausführen, um die Integrität aller Volumes auf diesem Datenträger zu überprüfen.

**Ereignis 1037: RES_DISK_FILESYSTEM_FAILED**

Das Dateisystem für eine oder mehrere Partitionen auf dem Datenträger für die Ressource "%1" ist möglicherweise beschädigt. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Speicherkonfiguration zu überprüfen. Optional können Sie CHKDSK ausführen, um die Integrität aller Volumes auf diesem Datenträger zu überprüfen.

**Ereignis 1038: RES_DISK_RESERVATION_LOST**

Der Besitz des Cluster Datenträgers "%1" wurde von diesem Knoten unerwartet verloren. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Speicherkonfiguration zu überprüfen.

**Ereignis 1039: RES_GENAPP_CREATE_FAILED**

Die generische Anwendung "%1" konnte bei dem Versuch, den Prozess zu erstellen, nicht online geschaltet werden (mit Fehler "%2"). Zu den möglichen Ursachen gehören: die Anwendung ist möglicherweise nicht auf diesem Knoten vorhanden, der Pfadname wurde möglicherweise falsch angegeben, der binäre Name wurde möglicherweise falsch angegeben.

**Ereignis 1040: RES_GENSVC_OPEN_FAILED**

Der generische Dienst "%1" konnte beim Versuch, den Dienst zu öffnen, nicht online geschaltet werden (mit Fehler "%2"). Zu den möglichen Ursachen gehören: der Dienst ist entweder nicht installiert, oder der angegebene Dienst Name ist ungültig.

**Ereignis 1041: RES_GENSVC_START_FAILED**

Der generische Dienst "%1" konnte beim Versuch, den Dienst zu starten, nicht online geschaltet werden (mit Fehler "%2"). Mögliche Ursache: die angegebenen Dienst Parameter sind möglicherweise ungültig.

**Ereignis 1042: RES_GENSVC_FAILED_AFTER_START**

Der generische Dienst "%1" ist mit Fehler "%2" fehlgeschlagen. Überprüfen Sie das Anwendungs Ereignisprotokoll.

**Ereignis 1044: RES_IPADDR_NBT_INTERFACE_CREATE_FAILED**

Fehler beim Erstellen einer neuen NetBIOS-Schnittstelle beim Online schalten der Ressource "%1" (Fehlercode "%2"). Möglicherweise wurde die maximale Anzahl von NetBIOS-Namen überschritten.

**Ereignis 1046: RES_IPADDR_INVALID_SUBNET**

Die Cluster-IP-Adress Ressource "%1" kann nicht online geschaltet werden, da der Wert für die Subnetzmaske ungültig ist. Überprüfen Sie die Eigenschaften der IP-Adress Ressource.

**Ereignis 1047: RES_IPADDR_INVALID_ADDRESS**

Die Cluster-IP-Adress Ressource "%1" kann nicht online geschaltet werden, da der Adress Wert ungültig ist. Überprüfen Sie die Eigenschaften der IP-Adress Ressource.

**Ereignis 1048: RES_IPADDR_INVALID_ADAPTER**

Die Cluster-IP-Adress Ressource "%1" konnte nicht online geschaltet werden. Die Konfigurationsdaten für den Netzwerkadapter, der der Cluster Netzwerkschnittstelle "%2" entspricht, konnten nicht ermittelt werden (Fehlercode: "%3"). Überprüfen Sie, ob die IP-Adress Ressource mit den richtigen Adress-und Netzwerk Eigenschaften konfiguriert ist.

**Ereignis 1049: RES_IPADDR_IN_USE**

Die Cluster-IP-Adress Ressource "%1" kann nicht online geschaltet werden, weil im Netzwerk eine doppelte IP-Adresse "%2" erkannt wurde. Stellen Sie sicher, dass alle IP-Adressen eindeutig sind.

**Ereignis 1050: RES_NETNAME_DUPLICATE**

Die Cluster Netzwerk-namens Ressource "%1" kann nicht online geschaltet werden, weil der Name "%2" mit diesem Cluster Knoten Namen übereinstimmt. Stellen Sie sicher, dass die Netzwerknamen eindeutig sind.

**Ereignis 1051: RES_NETNAME_NO_IP_ADDRESS**

Die Cluster Netzwerk-namens Ressource "%1" kann nicht online geschaltet werden. Stellen Sie sicher, dass die Netzwerkadapter für abhängige IP-Adress Ressourcen auf mindestens einen DNS-Server zugreifen können. Aktivieren Sie alternativ NetBIOS für abhängige IP-Adressen.

**Ereignis 1052: RES_NETNAME_CANT_ADD_NAME_STATUS**

Die Cluster Netzwerk-namens Ressource "%1" kann nicht online geschaltet werden, da der Name dem System nicht hinzugefügt werden konnte. Der zugehörige Fehlercode wird im Daten Abschnitt gespeichert.

**Ereignis 1053: RES_SMB_CANT_CREATE_SHARE**

Die Cluster Dateifreigabe "%1" kann nicht online geschaltet werden, da die Freigabe nicht erstellt werden konnte.

**Ereignis 1054: RES_SMB_SHARE_NOT_FOUND**

Fehler bei der Integritäts Überprüfung für die Dateifreigabe Ressource "%1". Fehler beim Abrufen von Informationen für Freigabe "%2" (mit Netzwerkname "%3"). Fehlercode: "%4". Stellen Sie sicher, dass die Freigabe vorhanden und zugänglich ist.

**Ereignis 1055: RES_SMB_SHARE_FAILED**

Fehler bei der Integritäts Überprüfung für die Dateifreigabe Ressource "%1". Beim Abrufen von Informationen für die Freigabe "%2" (mit dem Netzwerknamen "%3") wurde angegeben, dass die Freigabe nicht vorhanden ist (Fehlercode "%4"). Stellen Sie sicher, dass die Freigabe vorhanden und zugänglich ist.

**Ereignis 1069: RCM_RESOURCE_FAILURE**

Fehler bei der Cluster Ressource "%1" in der Cluster Rolle "%2".

**Ereignis 1069: RCM_RESOURCE_FAILURE_WITH_TYPENAME**

Fehler bei der Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2".

Basierend auf den Fehler Richtlinien für die Ressource und Rolle versucht der Cluster Dienst möglicherweise, die Ressource auf diesem Knoten online zu schalten oder die Gruppe auf einen anderen Knoten des Clusters zu verschieben und dann neu zu starten. Überprüfen Sie den Ressourcen-und Gruppenstatus mithilfe Failovercluster-Manager oder des Windows PowerShell-Cmdlets Get-Clusterresource.

**Ereignis 1069: RCM_RESOURCE_FAILURE_WITH_CAUSE**

Fehler bei der Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2". Fehlercode: "%5" ("%4").

Basierend auf den Fehler Richtlinien für die Ressource und Rolle versucht der Cluster Dienst möglicherweise, die Ressource auf diesem Knoten online zu schalten oder die Gruppe auf einen anderen Knoten des Clusters zu verschieben und dann neu zu starten. Überprüfen Sie den Ressourcen-und Gruppenstatus mithilfe Failovercluster-Manager oder des Windows PowerShell-Cmdlets Get-Clusterresource.

**Ereignis 1069: RCM_RESOURCE_FAILURE_WITH_ERROR_CODE**

Fehler bei der Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2". Fehlercode: "%4".

Basierend auf den Fehler Richtlinien für die Ressource und Rolle versucht der Cluster Dienst möglicherweise, die Ressource auf diesem Knoten online zu schalten oder die Gruppe auf einen anderen Knoten des Clusters zu verschieben und dann neu zu starten. Überprüfen Sie den Ressourcen-und Gruppenstatus mithilfe Failovercluster-Manager oder des Windows PowerShell-Cmdlets Get-Clusterresource.

**Ereignis 1069: RCM_RESOURCE_FAILURE_DUE_TO_VETO**

Fehler bei der Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2" aufgrund eines Versuchs, eine erforderliche Zustandsänderung in dieser Cluster Ressource zu blockieren.

**Ereignis 1077: RES_IPADDR_IPV4_ADDRESS_INTERFACE_FAILED**

Fehler bei der Integritäts Überprüfung für die IP-Schnittstelle "%1" (Adresse "%2") (Status ist "%3"). Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um sicherzustellen, dass der Netzwerkadapter ordnungsgemäß funktioniert.

**Ereignis 1078: RES_IPADDR_WINS_ADDRESS_FAILED**

Die Cluster-IP-Adress Ressource "%1" kann nicht online geschaltet werden, weil die WINS-Registrierung für die Schnittstelle "%2" mit Fehler "%3" fehlgeschlagen ist Stellen Sie sicher, dass ein gültiger, zugänglicher WINS-Server angegeben wurde.

**Ereignis 1121: CP_CRYPTO_CKPT_RESTORE_FAILED**

Verschlüsselte Einstellungen für die Cluster Ressource "%1" konnten nicht erfolgreich auf den Container Namen "%2" auf diesem Knoten angewendet werden.

**Ereignis 1127: TM_EVENT_CLUSTER_NETINTERFACE_FAILED**

Fehler bei der Cluster Netzwerkschnittstelle "%1" für Cluster Knoten "%2" im Netzwerk "%3". Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

**Ereignis 1129: TM_EVENT_CLUSTER_NETWORK_PARTITIONED**

Das Cluster Netzwerk "%1" ist partitioniert. Einige angefügte Failoverclusterknoten können nicht über das Netzwerk miteinander kommunizieren. Der Speicherort des Fehlers konnte vom Failovercluster nicht bestimmt werden. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

**Ereignis 1130: TM_EVENT_CLUSTER_NETWORK_DOWN**

Das Cluster Netzwerk "%1" ist nicht herunter. Keiner der verfügbaren Knoten kann mit diesem Netzwerk kommunizieren. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware-oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

**Ereignis 1137: RCM_DRAIN_MOVE_FAILED**

Das Verschieben der Cluster Rolle "%1" für den Ausgleich konnte nicht abgeschlossen werden. Fehler beim Vorgang. Fehlercode: %2.

**Ereignis 1138: RES_SMB_CANT_CREATE_DFS_ROOT**

Die Cluster Dateifreigabe-Ressource "%1" kann nicht online geschaltet werden. Fehler beim Erstellen des DFS-Namespace Stamms (Fehler: ' %3 '). Dies liegt möglicherweise daran, dass der DFS-Namespace-Dienst nicht gestartet oder der DFS-N-Stamm für die Freigabe "%2" nicht erstellt werden konnte.

**Ereignis 1141: RES_SMB_CANT_INIT_DFS_SVC**

Die Cluster Dateifreigabe-Ressource "%1" kann nicht online geschaltet werden. Fehler bei der erneuten Synchronisierung des DFS-Stamm Ziels "%2". Fehler: "%3".

**Ereignis 1142: RES_SMB_CANT_ONLINE_DFS_ROOT**

Die Cluster Dateifreigabe-Ressource "%1" für den DFS-Namespace kann aufgrund des Fehlers "%2" nicht online geschaltet werden.

**Ereignis 1182: NETRES_RESOURCE_STOP_ERROR**

Die Cluster Ressource "%1" kann nicht online geschaltet werden, da der zugeordnete Dienst bei einem versuchten Neustart einen Fehler verursacht hat. Der Fehlercode lautet "%2". Der Dienst erforderte einen Neustart, um Parameter zu aktualisieren. Der Dienst konnte jedoch nicht beendet und neu gestartet werden. Überprüfen Sie, ob dem Dienst weitere Ereignisse zugeordnet sind, und stellen Sie sicher, dass der Dienst ordnungsgemäß funktioniert.

**Ereignis 1183: RES_DISK_INVALID_MP_SOURCE_NOT_CLUSTERED**

Die Cluster Datenträger Ressource "%1" enthält einen ungültigen Einfügepunkt. Sowohl der Quell-als auch der Ziel Datenträger, die dem Bereitstellungs Punkt zugeordnet sind, müssen gruppierte Datenträger sein und müssen Mitglieder derselben Gruppe sein.
Der Einstellungspunkt "%2" für Volume "%3" verweist auf einen ungültigen Quell Datenträger. Stellen Sie sicher, dass es sich beim Quell Datenträger ebenfalls um einen gruppierten Datenträger und in derselben Gruppe wie der Ziel Datenträger handelt (der den Bereitstellungs Punkt

**Ereignis 1191: RES_NETNAME_DELETE_COMPUTER_ACCOUNT_FAILED_STATUS**

Die Cluster Netzwerk-namens Ressource "%1" konnte das zugehörige Computer Objekt in der Domäne "%2" nicht löschen. Fehlercode: ' %3 '.
Bitte lassen Sie einen Domänen Administrator das Computer Objekt manuell aus der Active Directory Domäne löschen.

**Ereignis 1192: RES_NETNAME_DELETE_COMPUTER_ACCOUNT_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte das zugehörige Computer Objekt in der Domäne "%2" aus folgendem Grund nicht löschen:
%3.

Bitte lassen Sie einen Domänen Administrator das Computer Objekt manuell aus der Active Directory Domäne löschen.

**Ereignis 1193: RES_NETNAME_ADD_COMPUTER_ACCOUNT_FAILED_STATUS**

Fehler beim Erstellen des zugeordneten Computer Objekts in der Domäne "%2" in der Cluster Netzwerknamen Ressource "%1" aus folgendem Grund: %3.

Der zugehörige Fehlercode lautet: %5

Wenden Sie sich an Ihren Domänen Administrator, um Folgendes sicherzustellen:

- Computer Objekte können von der Cluster Identität "%4" erstellt werden. Standardmäßig werden alle Computer

Objekte im Container "Computer" erstellt. Wenn dieser Speicherort geändert wurde, wenden Sie sich an den Domänen Administrator.

- Das Kontingent für Computer Objekte wurde nicht erreicht.
- Wenn ein Computer Objekt vorhanden ist, vergewissern Sie sich, dass die Cluster Identität "%4" für dieses Computer Objekt mit dem Tool Active Directory Benutzer und Computer über die Berechtigung "Vollzugriff" verfügt.

**Ereignis 1194: RES_NETNAME_ADD_COMPUTER_ACCOUNT_FAILED**

Fehler beim Erstellen des zugeordneten Computer Objekts in der Domäne "%2" in der Cluster Netzwerknamen Ressource "%1" während: %3.

Der Text für den zugeordneten Fehlercode lautet: %4

Wenden Sie sich an Ihren Domänen Administrator, um Folgendes sicherzustellen:

- Die Cluster Identität "%5" verfügt über Berechtigungen zum Erstellen von Computer Objekten. Standardmäßig werden alle Computer Objekte im gleichen Container wie die Cluster Identität "%5" erstellt.
- Das Kontingent für Computer Objekte wurde nicht erreicht.
- Wenn ein Computer Objekt vorhanden ist, überprüfen Sie, ob die Cluster Identität "%5" über die Berechtigung "Vollzugriff" für dieses Computer Objekt verfügt, indem Sie das Tool Active Directory Benutzer und Computer verwenden.

**Ereignis 1195: RES_NETNAME_DNS_REGISTRATION_FAILED_STATUS**

Fehler bei der Registrierung mindestens eines zugeordneten DNS-Namens für die Cluster Netzwerk-namens Ressource "%1". Fehlercode: "%2". Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit Zugriff auf mindestens einen DNS-Server konfiguriert sind.

**Ereignis 1196: RES_NETNAME_DNS_REGISTRATION_FAILED**

Fehler bei der Registrierung mindestens eines zugeordneten DNS-Namens für die Cluster Netzwerk-namens Ressource "%1" aus folgendem Grund:
%2.

Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit mindestens einem zugänglichen DNS-Server konfiguriert sind.

**Ereignis 1205: RCM_EVENT_GROUP_FAILED_ONLINE_OFFLINE**

Die Cluster Rolle "%1" konnte vom Clusterdienst nicht vollständig online oder offline geschaltet werden. Mindestens eine Ressource weist einen fehlerhaften Status auf. Dies hat möglicherweise Auswirkungen auf die Verfügbarkeit der Cluster Rolle.

**Ereignis 1206: RES_NETNAME_UPDATE_COMPUTER_ACCOUNT_FAILED_STATUS**

Das Computer Objekt, das der Cluster Netzwerk-namens Ressource "%1" zugeordnet ist, konnte in der Domäne "%2" nicht aktualisiert werden. Fehlercode: ' %3 '. Der Cluster Identität "%4" fehlen möglicherweise die erforderlichen Berechtigungen zum Aktualisieren des Objekts. Wenden Sie sich an Ihren Domänen Administrator, um sicherzustellen, dass die Cluster Identität Computer Objekte in der Domäne aktualisieren kann.

**Ereignis 1207: RES_NETNAME_UPDATE_COMPUTER_ACCOUNT_FAILED**

Das Computer Objekt, das der Cluster Netzwerk-namens Ressource "%1" zugeordnet ist, konnte in der Domäne "%2" nicht aktualisiert werden.
Vorgang "%3".

Der Text für den zugeordneten Fehlercode lautet: %4

Der Cluster Identität "%5" fehlen möglicherweise die erforderlichen Berechtigungen zum Aktualisieren des Objekts.

Wenden Sie sich an Ihren Domänen Administrator, um sicherzustellen, dass die Cluster Identität Computer Objekte in der Domäne aktualisieren kann.

**Ereignis 1208: RES_DISK_INVALID_MP_TARGET_NOT_CLUSTERED**

Die Cluster Datenträger Ressource "%1" enthält einen ungültigen Einfügepunkt. Sowohl der Quell-als auch der Ziel Datenträger, die dem Bereitstellungs Punkt zugeordnet sind, müssen gruppierte Datenträger sein und müssen Mitglieder derselben Gruppe sein.
Der Bereitstellungs Punkt "%2" für Volume "%3" verweist auf einen ungültigen Ziel Datenträger. Stellen Sie sicher, dass es sich bei dem Ziel Datenträger ebenfalls um einen gruppierten Datenträger und in derselben Gruppe wie der Quell Datenträger handelt

**Ereignis 1211: RES_NETNAME_NO_WRITEABLE_DC_STATUS**

Die Cluster Netzwerk-namens Ressource "%1" kann nicht online geschaltet werden. Es wurde versucht, einen beschreibbaren Domänen Controller (in Domäne %2) zu suchen, um ein Computer Objekt zu erstellen oder zu aktualisieren, das der Ressource zugeordnet ist. Fehlercode: ' %3 '. Stellen Sie sicher, dass für diesen Knoten innerhalb der konfigurierten Domäne ein Beschreib barer Domänen Controller verfügbar ist. Stellen Sie außerdem sicher, dass der DNS-Server ausgeführt wird, um den Namen des Domänen Controllers aufzulösen.

**Ereignis 1212: RES_NETNAME_NO_WRITEABLE_DC**

Die Cluster Netzwerk-namens Ressource "%1" kann nicht online geschaltet werden. Der Versuch, einen beschreibbaren Domänen Controller (in Domäne %2) zu suchen, um ein Computer Objekt zu erstellen oder zu aktualisieren, das der Ressource zugeordnet ist, konnte aus folgendem Grund nicht ausgeführt werden:
%3.

Fehlercode: "%4". Stellen Sie sicher, dass für diesen Knoten innerhalb der konfigurierten Domäne ein Beschreib barer Domänen Controller verfügbar ist. Stellen Sie außerdem sicher, dass der DNS-Server ausgeführt wird, um den Namen des Domänen Controllers aufzulösen.

**Ereignis 1213: RES_NETNAME_RENAME_RESTORE_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte das zugeordnete Computer Objekt auf dem Domänen Controller "%2" nicht vollständig umbenennen. Fehler beim Versuch, das Computer Objekt mit dem neuen Namen "%3" wieder in den ursprünglichen Namen "%4" umzubenennen. Fehlercode: ' %5 '. Dies wirkt sich möglicherweise auf die Client Konnektivität aus, bis der Netzwerkname und der zugehörige Computer Objektname konsistent sind. Bitten Sie den Domänen Administrator, das Computer Objekt manuell umzubenennen.

**Ereignis 1214: RES_NETNAME_CANT_ADD_NAME2**

Die Cluster-Netzwerknamen Ressource kann nicht bei NetBIOS registriert werden.

Netzwerk Name: "%3"
Fehlerursache: %2
Ressourcen Name: "%1"

Führen Sie nbtstat für den Netzwerknamen aus, um sicherzustellen, dass der Name nicht bereits bei NetBIOS registriert ist.

**Ereignis 1215: RES_NETNAME_NOT_REGISTERED_WITH_RDR**

Fehler bei der Integritäts Überprüfung für die Cluster Netzwerk-namens Ressource "%1". Der Netzwerkname "%2" ist nicht mehr auf diesem Knoten registriert. Fehlercode: ' %3 '. Überprüfen Sie Hardware-oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter. Sie können auch den Konfigurationsüberprüfungs-Assistenten ausführen, um die Netzwerkkonfiguration zu überprüfen.

**Ereignis 1218: RES_NETNAME_ONLINE_RENAME_RECOVERY_MISSING_ACCOUNT**

Die Cluster Netzwerk-namens Ressource "%1" konnte keinen namens Änderungs Vorgang ausführen (es wurde versucht, den ursprünglichen Namen "%3" in den Namen "%4" zu ändern). Das Computer Objekt konnte auf dem

Domänen Controller "%2" nicht gefunden werden (auf dem er erstellt wurde). Es wird versucht, das Computer Objekt neu zu erstellen, wenn die Ressource das nächste Mal online geschaltet wird. Wenden Sie sich außerdem an Ihren Domänen Administrator, um sicherzustellen, dass das Computer Objekt in der Domäne vorhanden ist.

**Ereignis 1219: RES_NETNAME_ONLINE_RENAME_DC_NOT_FOUND**

Die Cluster Netzwerk-namens Ressource "%1" konnte keinen namens Änderungs Vorgang ausführen. Der Domänen Controller "%2", auf dem das Computer Objekt "%3" umbenannt wurde, konnte nicht kontaktiert werden. Fehlercode: "%4". Stellen Sie sicher, dass auf einen beschreibbaren Domänen Controller zugegriffen werden kann, und prüfen Sie, ob Verbindungsprobleme

**Ereignis 1220: RES_NETNAME_ONLINE_RENAME_RECOVERY_FAILED**

Fehler beim Umbenennen des Computer Kontos für die Ressource "%1" von "%2" in "%3" mithilfe des Domänen Controllers "%4". Der zugehörige Fehlercode wird im Daten Abschnitt gespeichert.

Das Computer Konto für diese Ressource wurde gerade umbenannt und wurde nicht fertiggestellt. Dies wurde während des Online Vorgangs für diese Ressource erkannt. Um die Wiederherstellung durchzusetzen, muss das Computer Konto in den aktuellen Wert der Name-Eigenschaft umbenannt werden, d. h., der im Netzwerk angegebene Name.

Möglicherweise ist der Domänen Controller, auf dem der umbenannt wurde, nicht verfügbar. Wenn dies der Fall ist, warten Sie, bis der Domänen Controller wieder verfügbar ist. Dem Domänen Controller kann der Zugriff auf das Konto verweigert werden. versuchen Sie nach dem Auflösen des Zugriffs, den Namen erneut online zu schalten.

Wenn dies nicht möglich ist, deaktivieren Sie die Kerberos-Authentifizierung, und aktivieren Sie Sie erneut, und es wird versucht, das Computer Konto auf einem anderen Domänen Controller zu finden. Sie müssen die Name-Eigenschaft in "%2" ändern, damit das vorhandene Computer Konto verwendet werden soll.

**Ereignis 1223: RES_IPADDR_INVALID_NETWORK_ROLE**

Die Cluster-IP-Adress Ressource "%1" kann nicht online geschaltet werden, weil das Cluster Netzwerk "%2" nicht für den Client Zugriff konfiguriert ist. Verwenden Sie die Failovercluster-Manager-Snap-in, um die konfigurierten Eigenschaften des Cluster Netzwerks zu überprüfen.

**Ereignis 1226: RES_NETNAME_TCB_NOT_HELD**

Für die Netzwerknamen Ressource "%1" (mit dem zugeordneten Netzwerknamen "%2") ist die Kerberos-Authentifizierungs Unterstützung aktiviert. Fehler beim Hinzufügen der erforderlichen Anmelde Informationen zum LSA. der zugeordnete Fehlercode "%3" weist auf die für diesen Vorgang normalerweise erforderlichen Berechtigungen hin. Die erforderliche Berechtigung ist "Trusted Computing Base" und muss lokal auf jedem Knoten aktiviert sein, der den Cluster umfasst.

**Ereignis 1227: RES_NETNAME_LSA_ERROR**

Für die Netzwerknamen Ressource "%1" (mit dem zugeordneten Netzwerknamen "%2") ist die Kerberos-Authentifizierungs Unterstützung aktiviert. Fehler beim Hinzufügen der erforderlichen Anmelde Informationen zum LSA. der zugehörige Fehlercode ist "%3".

**Ereignis 1228: RES_NETNAME_CLONE_FAILURE**

Fehler bei der Cluster Netzwerknamen Ressource "%1" beim Aktivieren des Netzwerk namens auf diesem Knoten. Ursache für den Fehler:
"%2".

Fehlercode: ' %3 '.

Sie können die Netzwerknamen Ressource zum erneuten Versuch erneut offline und online schalten.

**Ereignis 1229: RES_NETNAME_NO_IPS_FOR_DNS**

Von der Cluster Netzwerk-namens Ressource "%1" konnten keine IP-Adressen identifiziert werden, die bei einem DNS-Server registriert werden. Stellen Sie sicher, dass mindestens ein Netzwerk für die Cluster Verwendung mit der Einstellung "Clients das Herstellen einer Verbindung über dieses Netzwerk gestatten" vorhanden ist und dass jeder Knoten über eine gültige IP-Adresse verfügt, die für die Netzwerke konfiguriert ist.

**Ereignis 1230: RCM_DEADLOCK_OR_CRASH_DETECTED**

Eine Komponente auf dem Server hat nicht rechtzeitig reagiert. Dies hat bewirkt, dass die Cluster Ressource "%1" (Ressourcentyp "%2", dll "%3") den Timeout Schwellenwert überschreitet. Im Rahmen der Cluster Integritäts Erkennung werden Wiederherstellungs Aktionen ausgeführt. Der Cluster versucht automatisch, eine automatische Wiederherstellung durch das Beenden und Neustarten des Ressourcenhosting-Subsystem (RHS)-Prozesses auszuführen, der diese Ressource ausgeführt hat. Überprüfen Sie, ob die zugrunde liegende Infrastruktur (z. b. Speicher, Netzwerk oder Dienste), die der Ressource zugeordnet ist, ordnungsgemäß funktioniert.

**Ereignis 1230: RCM_RESOURCE_CONTROL_DEADLOCK_DETECTED**

Eine Komponente auf dem Server hat nicht rechtzeitig reagiert. Dies hat bewirkt, dass die Cluster Ressource "%1" (Ressourcentyp "%2", dll "%3") bei der Verarbeitung des Steuerungs Codes "%4;" den Timeout Schwellenwert überschreitet. Im Rahmen der Cluster Integritäts Erkennung werden Wiederherstellungs Aktionen ausgeführt. Der Cluster versucht automatisch, eine automatische Wiederherstellung durch das Beenden und Neustarten des Ressourcenhosting-Subsystem (RHS)-Prozesses auszuführen, der diese Ressource ausgeführt hat. Überprüfen Sie, ob die zugrunde liegende Infrastruktur (z. b. Speicher, Netzwerk oder Dienste), die der Ressource zugeordnet ist, ordnungsgemäß funktioniert.

**Ereignis 1231: RES_NETNAME_LOGON_FAILURE**

Bei der Cluster Netzwerknamen Ressource "%1" ist ein Fehler bei der Anmeldung bei der Domäne aufgetreten. Ursache für den Fehler:
"%2".

Fehlercode: ' %3 '.

Stellen Sie sicher, dass für diesen Knoten innerhalb der konfigurierten Domäne ein Domänen Controller verfügbar ist.

**Ereignis 1232: RES_GENSCRIPT_TIMEOUT**

Der Einstiegspunkt "%2" in der generischen Skript Ressource "%1" hat die Ausführung nicht rechtzeitig beendet. Dies kann auf eine Endlosschleife oder andere Probleme zurückzuführen sein, die möglicherweise zu einem unendlichen warte Vorgang führen. Alternativ kann der angegebene ausstehende Timeout Wert für diese Ressource zu kurz sein. Überprüfen Sie den Skript Einstiegspunkt "%2", um sicherzustellen, dass alle möglichen unendlichen warte Vorgänge im Skriptcode korrigiert wurden. Dann sollten Sie ggf. den ausstehenden Timeout Wert erhöhen.

**Ereignis 1233: RES_GENSCRIPT_HANGMODE**

Generische Cluster Skript Ressource "%1": die Anforderung zum Ausführen des Vorgangs "%2" wird nicht verarbeitet. Dies liegt an einem zuvor fehlgeschlagenen Versuch, den Einstiegspunkt "%3" rechtzeitig auszuführen. Überprüfen Sie den Skriptcode für diesen Einstiegspunkt, um sicherzustellen, dass keine Endlosschleife oder andere Probleme vorhanden sind, die möglicherweise zu einem unendlichen warte Vorgang führen. Erhöhen Sie dann ggf. den Wert ausstehender Timeout Wert für Ressourcen.

**Ereignis 1234: CLUSTER_EVENT_ACCOUNT_MISSING_PRIVS**

Die Clusterdienst hat festgestellt, dass für das Dienst Konto mindestens eine der erforderlichen Berechtigungen fehlt. Die Liste der fehlenden Berechtigungen lautet: "%1" und wird dem Dienst Konto derzeit nicht gewährt. Verwenden Sie "SC. exe qprivs ClusSvc", um die Berechtigungen des Clusterdienst (ClusSvc) zu überprüfen. Überprüfen Sie außerdem, ob in Active Directory Domain Services Sicherheitsrichtlinien oder Gruppenrichtlinien vorhanden sind, die möglicherweise die Standard Berechtigungen geändert haben. Geben Sie den folgenden Befehl

ein, um dem Clusterdienst die erforderlichen Berechtigungen für die ordnungsgemäße Funktion zu erteilen:

```
sc.exe privs
clussvc
SeBackupPrivilege/SeRestorePrivilege/SeIncreaseQuotaPrivilege/SeIncreaseBasePriorityPrivilege/SeTcbPrivilege/Se
DebugPrivilege/SeSecurityPrivilege/SeAuditPrivilege/SeImpersonatePrivilege/SeChangeNotifyPrivilege/SeIncreaseWo
rkingSetPrivilege/SeManageVolumePrivilege/SeCreateSymbolicLinkPrivilege/SeLoadDriverPrivilege
```

### Ereignis 1242: RES_IPADDR_LEASE_EXPIRED

Die Lease der IP-Adresse "%2", die der Cluster-IP-Adress Ressource "%1" zugeordnet ist, ist abgelaufen oder läuft demnächst ab und kann zurzeit nicht erneuert werden. Stellen Sie sicher, dass der zugeordnete DHCP-Server zugänglich und ordnungsgemäß konfiguriert ist, um die Lease für diese IP-Adresse zu erneuern

### Ereignis 1245: RES_IPADDR_LEASE_RENEWAL_FAILED

Die Cluster-IP-Adress Ressource "%1" konnte die Lease für die IP-Adresse "%2" nicht erneuern. Stellen Sie sicher, dass der DHCP-Server zugänglich und ordnungsgemäß konfiguriert ist, um die Lease für diese IP-Adresse zu erneuern.

### Ereignis 1250: RCM_RESOURCE_EMBEDDED_FAILURE

Die Cluster Ressource "%1" in der Cluster Rolle "%2" hat eine Benachrichtigung über den kritischen Status erhalten. Für eine virtuelle Maschine gibt dies an, dass sich eine Anwendung oder ein Dienst innerhalb des virtuellen Computers in einem fehlerhaften Zustand befindet. Überprüfen Sie die Funktionalität des Dienstes oder der Anwendung, die auf dem virtuellen Computer überwacht wird.

### Ereignis 1254: RCM_GROUP_TERMINAL_FAILURE

Die Cluster Rolle "%1" hat den failoverschwellen Wert überschritten. Die konfigurierte Anzahl von failoverversuchen innerhalb des Failoverzeitraums, der ihm zugewiesen wurde, ist erschöpft und wird in einem fehlerhaften Zustand verbleiben. Es werden keine weiteren Versuche unternommen, die Rolle Online zu schalten oder ein Failover auf einen anderen Knoten im Cluster durchzuführen. Überprüfen Sie die Ereignisse, die dem Fehler zugeordnet sind. Nachdem die Probleme behoben wurden, die den Fehler verursacht haben, kann die Rolle manuell online geschaltet werden, oder der Cluster versucht, Sie nach dem Neustart Verzögerungs Zeitraum erneut online zu schalten.

### Ereignis 1255: RCM_RESOURCE_NETWORK_FAILURE

Die Cluster Ressource "%1" in der Cluster Rolle "%2" hat eine Benachrichtigung über den kritischen Status erhalten. Für eine virtuelle Maschine bedeutet dies, dass sich ein kritisches Netzwerk der virtuellen Maschine in einem fehlerhaften Zustand befindet. Überprüfen Sie die Netzwerk Konnektivität des virtuellen Computers und der virtuellen Netzwerke, für die der virtuelle Computer konfiguriert ist.

### Ereignis 1256: RES_NETNAME_DNS_REGISTRATION_FAILED_DYNAMIC_DNS_ZONE

Fehler bei der Registrierung von mindestens einem zugeordneten DNS-Namen durch die Cluster-Netzwerknamen Ressource, weil die entsprechende DNS-Zone keine dynamischen Updates akzeptiert.

Cluster Netzwerkname: "%1"
DNS-Zone: "%2"

#### Anleitungen

Stellen Sie sicher, dass das DNS als dynamische DNS-Zone konfiguriert ist. Wenn der DNS-Server keine dynamischen Updates akzeptiert, deaktivieren Sie in den Eigenschaften des Netzwerkadapters die Adressen dieser Verbindung in DNS registrieren.

### Ereignis 1257: RES_NETNAME_DNS_REGISTRATION_FAILED_SECURE_DNS_ZONE

Fehler bei der Registrierung von mindestens einem zugeordneten DNS-Namen durch die Cluster-Netzwerknamen Ressource, weil der Zugriff zum Aktualisieren der sicheren DNS-Zone verweigert wurde.

Cluster Netzwerkname: "%1"
DNS-Zone: "%2"

Stellen Sie sicher, dass dem Cluster Namen Objekt (CNO) Berechtigungen für die sichere DNS-Zone erteilt werden.

**Ereignis 1258: RES_NETNAME_DNS_REGISTRATION_FAILED_TIMEOUT**

Fehler bei der Registrierung eines oder mehrerer zugeordneter DNS-Namen durch die Cluster-Netzwerknamen Ressource, weil der DNS-Server nicht erreicht werden konnte.

Cluster Netzwerkname: "%1"
DNS-Zone: "%2"
DNS-Server: "%3"

Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit mindestens einem zugänglichen DNS-Server konfiguriert sind.

**Ereignis 1259: RES_NETNAME_DNS_REGISTRATION_FAILED_CLEANUP**

Fehler bei der Registrierung eines oder mehrerer zugeordneter DNS-Namen durch den Cluster-Netzwerknamen. der Cluster Dienst konnte die vorhandenen Datensätze, die dem Netzwerknamen entsprechen, nicht bereinigen.

Cluster Netzwerkname: "%1"
DNS-Zone: "%2"

Stellen Sie sicher, dass dem Cluster Namen Objekt (CNO) Berechtigungen für die sichere DNS-Zone erteilt werden.

**Ereignis 1260: RES_NETNAME_DNS_REGISTRATION_MODIFY_FAILED**

Die DNS-Registrierung konnte von der Cluster Netzwerk-namens Ressource nicht geändert werden.

Cluster Netzwerkname: "%1"
Fehlercode: "%2"

**Anleitungen**

Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit Zugriff auf mindestens einen DNS-Server konfiguriert sind.

**Ereignis 1261: RES_NETNAME_DNS_REGISTRATION_MODIFY_FAILED_STATUS**

Die DNS-Registrierung konnte von der Cluster Netzwerk-namens Ressource nicht geändert werden.

Cluster Netzwerkname: "%1"
Ursache: "%2"

**Anleitungen**

Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit Zugriff auf mindestens einen DNS-Server konfiguriert sind.

**Ereignis 1262: RES_NETNAME_DNS_REGISTRATION_PUBLISH_PTR_FAILED**

Die Cluster-Netzwerknamen Ressource konnte den PTR-Datensatz in der DNS-Reverse-Lookupzone nicht veröffentlichen.

Cluster Netzwerkname: "%1"
Fehler Code: "%2"

**Anleitungen**

Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit Zugriff auf

mindestens einen DNS-Server konfiguriert sind und dass die DNS-Reverse-Lookupzone vorhanden ist.

**Ereignis 1264: RES_NETNAME_DNS_REGISTRATION_PUBLISH_PTR_FAILED_STATUS**

Die Cluster-Netzwerknamen Ressource konnte den PTR-Datensatz in der DNS-Reverse-Lookupzone nicht veröffentlichen.

Cluster Netzwerkname: "%1"
Ursache: "%2"

**Anleitungen**

Stellen Sie sicher, dass die Netzwerkadapter, die abhängigen IP-Adress Ressourcen zugeordnet sind, mit Zugriff auf mindestens einen DNS-Server konfiguriert sind und dass die DNS-Reverse-Lookupzone vorhanden ist.

**Ereignis 1265: RES_TYPE_CONTROL_TIMED_OUT**

Timeout beim Cluster Ressourcentyp "%1" während der Verarbeitung des Steuerungs Codes "%2". Der Cluster versucht, automatisch eine Wiederherstellung durchführen, indem er den Ressourcenhosting-Subsystem (RHS)-Prozess beendet und neu startet, der den-Befehl verarbeitet hat.

**Ereignis 1289: NETFT_ADAPTER_NOT_FOUND**

Der Cluster Dienst konnte nicht auf den Netzwerkadapter ' %1 ' zugreifen. Stellen Sie sicher, dass andere Netzwerkadapter ordnungsgemäß funktionieren, und überprüfen Sie den Geräte-Manager auf Fehler im Zusammenhang mit Adapter "%1". Wenn die Konfiguration für den Adapter "%1" geändert wurde, ist es möglicherweise erforderlich, das Feature "Failoverclustering" auf diesem Computer erneut zu installieren.

**Ereignis 1360: RES_IPADDR_INVALID_NETWORK**

Die Cluster-IP-Adress Ressource "%1" konnte nicht online geschaltet werden. Stellen Sie sicher, dass die Netzwerk Eigenschaft ' %2 ' mit dem Cluster Netzwerknamen übereinstimmt oder die Address-Eigenschaft ' %3 ' mit einem der Subnetze in einem Cluster Netzwerk übereinstimmt. Wenn es sich um einen IPv6-Adresstyp handelt, stellen Sie sicher, dass das Cluster Netzwerk, das mit dieser Ressource übereinstimmt, mindestens ein IPv6-Präfix enthält, das kein Link-Local oder Tunnel

**Ereignis 1361: RES_IPADDR_MISSING_DEPENDANT**

Die IPv6-Tunnel Adress Ressource "%1" konnte nicht online geschaltet werden, da Sie nicht von einer IP-Adress Ressource (IPv4) abhängt. Es ist eine Abhängigkeit von mindestens einer IP-Adress Ressource (IPv4) erforderlich.

**Ereignis 1362: RES_IPADDR_MISSING_DATA**

Die Cluster-IP-Adress Ressource "%1" konnte nicht online geschaltet werden, weil die Eigenschaft "%2" nicht gelesen werden konnte. Stellen Sie sicher, dass die Ressource ordnungsgemäß konfiguriert ist.

**Ereignis 1363: RES_IPADDR_NO_ISATAP_SUPPORT**

Die IPv6-Tunnel Adress Ressource "%1" konnte nicht online geschaltet werden. Das mit der abhängigen IP-Adresse (IPv4)-Ressource "%3" verknüpfte Cluster Netzwerk "%2" unterstützt keine ISATAP-Tunnelung. Stellen Sie sicher, dass das Cluster Netzwerk ISATAP-Tunnelung unterstützt.

**Ereignis 1540: SERVICE_BACKUP_NOQUORUM**

Der Sicherungs Vorgang für die Cluster Konfigurationsdaten wurde abgebrochen, da das Quorum für den Cluster noch nicht erreicht wurde. Wiederholen Sie den Sicherungs Vorgang, nachdem der Cluster das Quorum erreicht hat.

**Ereignis 1554: SERVICE_RESTORE_INVALIDUSER**

Der Wiederherstellungs Vorgang für die Cluster Konfigurationsdaten ist fehlgeschlagen. Dies war auf unzureichende Berechtigungen zurückzuführen, die dem Benutzerkonto zugeordnet sind, das die Wiederherstellung durchführt. Stellen Sie sicher, dass das Benutzerkonto über lokale Administratorrechte verfügt.

**Ereignis 1557: SERVICE_WITNESS_ATTACH_FAILED**

Fehler beim Aktualisieren der Cluster Konfigurationsdaten für die Zeugen Ressource Clusterdienst. Stellen Sie sicher, dass die Zeugen Ressource online und zugänglich ist.

**Ereignis 1559: RES_WITNESS_NEW_NODE_CONFLICT**

Die der Dateifreigabe Zeugen-Ressource zugeordnete Dateifreigabe "%1" wird zurzeit von Server "%2" gehostet. Der Server "%2" wurde soeben als neuer Knoten innerhalb des Failoverclusters hinzugefügt. Das Hosting des Dateifreigabe Zeugen durch einen beliebigen Knoten, der denselben Cluster umfasst, wird nicht empfohlen. Wählen Sie einen Dateifreigabe Zeugen aus, der nicht von einem beliebigen Knoten im gleichen Cluster gehostet wird, und ändern Sie die Einstellungen der Dateifreigabe Zeugen-Ressource entsprechend.

**Ereignis 1560: RES_SMB_SHARE_CONFLICT**

Die Cluster Dateifreigabe-Ressource "%1" hat Konflikte im freigegebenen Ordner erkannt. Folglich sind einige dieser freigegebenen Ordner möglicherweise nicht zugänglich. Um diese Situation zu beheben, stellen Sie sicher, dass mehrere freigegebene Ordner nicht denselben Freigabe Namen aufweisen.

**Ereignis 1563: RES_FSW_ONLINEFAILURE**

Die Dateifreigabe-Zeugen Ressource "%1" konnte nicht online geschaltet werden. Stellen Sie sicher, dass die Dateifreigabe "%2" vorhanden ist und dass der Cluster darauf zugreifen kann.

**Ereignis 1566: RES_NETNAME_TIMEDOUT**

Die Cluster Netzwerk-namens Ressource "%1" kann nicht online geschaltet werden. Die Netzwerknamen Ressource wurde vom Ressourcen Host Subsystem beendet, weil ein Vorgang nicht in einem akzeptablen Zeitraum abgeschlossen wurde. Timeout des Vorgangs beim Ausführen von:
"%2"

**Ereignis 1567: SERVICE_FAILED_TO_CHANGE_LOG_SIZE**

Clusterdienst konnte die Größe des Ablauf Verfolgungs Protokolls nicht ändern. Überprüfen Sie die ClusterLogSize-Einstellung mit dem PowerShell | -Cmdlet "Get-Cluster Format-List *". Überprüfen Sie außerdem mit dem Leistungs Monitor-Snap-in die Sitzungs Einstellungen der Ereignis Ablauf Verfolgung für Failoverclustering.

**Ereignis 1567: RES_VIPADDR_ADDRESS_INTERFACE_FAILED**

Fehler bei der Integritäts Überprüfung für die IP-Schnittstelle "%1" (Adresse "%2") (Status ist "%3"). Überprüfen Sie Hardware-oder Softwarefehler im Zusammenhang mit den physischen oder virtuellen Netzwerkadaptern.

**Ereignis 1568: RES_CLOUD_WITNESS_CANT_COMMUNICATE_TO_AZURE**

Die cloudzeugen Ressource konnte Microsoft Azure Speicherdienste nicht erreichen.

Cluster Ressource: %1
Cluster Knoten: %2

**Anleitungen**

Dies kann auf die Netzwerkkommunikation zwischen dem Cluster Knoten und dem Microsoft Azure zu blockierenden Dienst zurückzuführen sein. Überprüfen Sie die Internet Konnektivität des Knotens mit Microsoft Azure. Stellen Sie eine Verbindung mit dem Microsoft Azure-Portal her, und überprüfen Sie, ob das Speicherkonto

**Ereignis 1569: SERVICE_USING_RESTRICTED_NETWORK**

Das Netzwerk "%1", das für die Verwendung des Failoverclusters deaktiviert wurde, war das einzige derzeit mögliche Netzwerk, das von Knoten "%2" für die Kommunikation mit anderen Knoten im Cluster verwendet werden kann. Dies kann Auswirkungen auf die Fähigkeit der Knoten haben, am Cluster teilzunehmen. Überprüfen Sie die Netzwerk Konnektivität von Knoten "%2", und aktivieren Sie mindestens ein Netzwerk für die Cluster Kommunikation. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen.

**Ereignis 1569: RES_CLOUD_WITNESS_TOKEN_EXPIRED**

Die Cloud-Zeugen Ressource konnte sich nicht bei Microsoft Azure Speicherdiensten authentifizieren. Beim

Kontaktieren des Microsoft Azure Speicher Kontos wurde ein Fehler vom Typ "Zugriff verweigert" zurückgegeben.

Cluster Ressource: %1

**Anleitungen**

Der Zugriffsschlüssel des Speicher Kontos ist möglicherweise nicht mehr gültig. Verwenden Sie den Assistenten zum Konfigurieren des Cluster Quorums in den Failovercluster-Manager oder dem Windows PowerShell-Cmdlet Set-Clusterquorum, um die Cloud-Zeugen Ressource mit dem aktualisierten Zugriffsschlüssel für das Speicherkonto zu konfigurieren.

### Ereignis 1573: SERVICE_FORM_WITNESS_FAILED

Knoten "%1" konnte keinen Cluster bilden. Der Grund war, dass auf den Zeugen nicht zugegriffen werden konnte. Stellen Sie sicher, dass die Zeugen Ressource online und verfügbar ist.

### Ereignis 1580: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_FAILED

Die Cluster Netzwerk-namens Ressource "%1" konnte den Namen "%2" für den Adapter "%4" in einer sicheren DNS-Zone nicht registrieren. Dies war auf einen vorhandenen Datensatz mit diesem Namen zurückzuführen, und die Cluster Identität verfügt nicht über ausreichende Berechtigungen zum Aktualisieren dieses Datensatzes. Fehlercode: ' %3 '. Wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob die Cluster Identität über Berechtigungen für den DNS-Datensatz "%2

### Ereignis 1580: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_FAILED

Die Cluster Netzwerk-namens Ressource "%1" konnte den Namen "%2" für den Adapter "%4" in einer sicheren DNS-Zone nicht registrieren. Dies war auf einen vorhandenen Datensatz mit diesem Namen zurückzuführen, und die Cluster Identität verfügt nicht über ausreichende Berechtigungen zum Aktualisieren dieses Datensatzes. Fehlercode: ' %3 '. Wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob die Cluster Identität über Berechtigungen für den DNS-Datensatz "%2

### Ereignis 1585: RES_FILESERVER_FSCHECK_SRVSVC_STOPPED

Fehler bei der Integritäts Überprüfung für die Cluster Dateiserver-Ressource "%1". Dies war darauf zurückzuführen, dass der Server Dienst nicht gestartet wurde. Verwenden Sie Server-Manager, um den Status des Server Dienstanbieter auf diesem Cluster Knoten zu bestätigen.

### Ereignis 1586: RES_FILESERVER_FSCHECK_SCOPED_NAME_NOT_REGISTERED

Fehler bei der Integritäts Überprüfung für die Cluster Dateiserver-Ressource "%1". Dies war darauf zurückzuführen, dass auf einige freigegebene Ordner zugegriffen werden konnte. Stellen Sie sicher, dass Clients auf die Ordner zugreifen können. Überprüfen Sie außerdem den Status des Server Dienstanbieter auf diesem Cluster Knoten mithilfe von Server-Manager, und suchen Sie nach anderen Ereignissen im Zusammenhang mit dem Server Dienst auf diesem Cluster Knoten. Möglicherweise muss die Netzwerknamen Ressource "%2" in dieser Cluster Rolle neu gestartet werden.

### Ereignis 1587: RES_FILESERVER_FSCHECK_FAILED

Fehler bei der Integritäts Überprüfung für die Cluster Dateiserver-Ressource "%1". Dies war darauf zurückzuführen, dass auf einige freigegebene Ordner zugegriffen werden konnte. Stellen Sie sicher, dass Clients auf die Ordner zugreifen können. Überprüfen Sie außerdem den Status des Server Dienstanbieter auf diesem Cluster Knoten mithilfe von Server-Manager, und suchen Sie nach anderen Ereignissen im Zusammenhang mit dem Server Dienst auf diesem Cluster Knoten.

### Ereignis 1588: RES_FILESERVER_SHARE_CANT_ADD

Die Cluster Dateiserver-Ressource "%1" kann nicht online geschaltet werden. Fehler beim Erstellen der dem Netzwerknamen "%3" zugeordneten Dateifreigabe "%2" durch die Ressource. Fehlercode: "%4". Überprüfen Sie, ob die Ordner vorhanden und zugänglich sind. Überprüfen Sie außerdem den Status des Server Dienstanbieter auf diesem Cluster Knoten mithilfe von Server-Manager, und suchen Sie nach anderen verwandten Ereignissen auf diesem Cluster Knoten. Möglicherweise muss die Netzwerknamen Ressource "%3" in dieser Cluster Rolle neu

gestartet werden.

**Ereignis 1600: CLUSAPI_CREATE_CANNOT_SET_AD_DACL**

Fehler beim Festlegen der Berechtigungen für das Cluster Computer Objekt "%1" Clusterdienst. Wenden Sie sich an den Netzwerkadministrator, um die Cluster Sicherheits Beschreibung des Computer Objekts in Active Directory zu überprüfen, sicherzustellen, dass die DACL nicht zu groß ist, und entfernen Sie ggf. unnötige zusätzliche ACE (s) für das Objekt.

**Ereignis 1603: RES_FILESERVER_CLONE_FAILED**

Der Datei Server konnte nicht gestartet werden, da die erwartete Abhängigkeit von der Ressource ' Network Name ' nicht gefunden wurde oder nicht ordnungsgemäß konfiguriert wurde. Fehler = 0x %2.

**Ereignis 1606: RES_DISK_CNO_CHECK_FAILED**

Die Cluster Datenträger Ressource "%1" enthält ein durch BitLocker geschütztes Volume "%2". für dieses Volume ist das Active Directory Cluster Namen Konto (auch als Cluster Namen Objekt oder CNO bezeichnet) keine BitLocker-Schutzvorrichtung für das Volume. Dies ist für mit BitLocker geschützte Volumes erforderlich. Um dies zu beheben, entfernen Sie zunächst den Datenträger aus dem Cluster. Fügen Sie als nächstes mit dem Befehlszeilen Tool "manage-bde. exe den Cluster Namen als adaccountorgroup-Schutzvorrichtung hinzu, und verwenden Sie\dabei das Format$ Domain Cluster Name für den Cluster Namen. Fügen Sie dann den Datenträger wieder zum Cluster hinzu. Weitere Informationen finden Sie in der Dokumentation zu "manage-bde. exe.

**Ereignis 1607: RES_DISK_CNO_UNLOCK_FAILED**

Die Cluster Datenträger Ressource "%1" konnte das durch BitLocker geschützte Volume "%2" nicht entsperren. Das Cluster Namen Objekt (CNO) ist nicht als gültige BitLocker-Schutzvorrichtung für dieses Volume festgelegt. Um dies zu beheben, entfernen Sie den Datenträger aus dem Cluster. Fügen Sie dann mit dem Befehlszeilen Tool "manage-bde. exe den Cluster Namen als adaccountorgroup-Schutzvorrichtung unter Verwendung des Formats Domain\Cluster Name$hinzu, und fügen Sie den Datenträger wieder zum Cluster hinzu. Weitere Informationen finden Sie in der Dokumentation zu "manage-bde. exe.

**Ereignis 1608: RES_FILESERVER_LEADER_FAILED**

Der Datei Server konnte nicht gestartet werden, da die erwartete Abhängigkeit von der Ressource ' Network Name ' nicht gefunden wurde oder nicht ordnungsgemäß konfiguriert wurde. Fehler = 0x %2.

**Ereignis 1609: RES_SODA_FILESERVER_LEADER_FAILED**

Scale Out Datei Server konnte nicht gestartet werden, da die erwartete Abhängigkeit von der Ressource ' verteilter Netzwerk Name ' nicht gefunden wurde oder nicht ordnungsgemäß konfiguriert wurde. Fehler = 0x %2.

**Ereignis 1632: CLUSAPI_CREATE_MISMATCHED_OU**

Fehler beim Erstellen des Clusters. Das Cluster Namen Objekt "%1" in der Active Directory-Organisationseinheit "%2" kann nicht erstellt werden. Das Objekt ist bereits in der Organisationseinheit "%3" vorhanden. Überprüfen Sie, ob der angegebene Distinguished Name-Pfad und das Cluster Namen Objekt korrekt sind. Wenn der Distinguished Name-Pfad nicht angegeben wird, wird das vorhandene Computer Objekt "%1" verwendet.

**Ereignis 1652: SERVICE_TCP_CONNECTION_FAILURE**

Cluster Knoten "%1" konnte dem Cluster nicht beitreten. Es konnte keine TCP-Verbindung mit den Knoten "%2" hergestellt werden. Überprüfen Sie die Netzwerk Konnektivität und die Konfiguration von Netzwerk Firewalls.

**Ereignis 1652: SERVICE_UDP_CONNECTION_FAILURE**

Cluster Knoten "%1" konnte dem Cluster nicht beitreten. Es konnte keine UDP-Verbindung mit den Knoten "%2" hergestellt werden. Überprüfen Sie die Netzwerk Konnektivität und die Konfiguration von Netzwerk Firewalls.

**Ereignis 1652: SERVICE_VIRTUAL_TCP_CONNECTION_FAILURE**

Cluster Knoten "%1" konnte dem Cluster nicht beitreten. Eine TCP-Verbindung, die den Microsoft-Failovercluster-Adapter verwendet, konnte nicht für Knoten "%2" eingerichtet werden. Überprüfen Sie die Netzwerk Konnektivität

und die Konfiguration von Netzwerk Firewalls.

**Ereignis 1653: SERVICE_NO_CONNECTIVITY**

Der Cluster Knoten "%1" konnte dem Cluster nicht beitreten, weil er nicht über das Netzwerk mit einem anderen Knoten im Cluster kommunizieren konnte. Überprüfen Sie die Netzwerk Konnektivität und die Konfiguration von Netzwerk Firewalls.

**Ereignis 1654: RES_VIPADDR_INVALID_ADAPTERNAME**

Fehler beim Online schalten der Cluster-IP-Adress Ressource "%1". Die Konfigurationsdaten für den Netzwerkadapter "%2" konnten nicht ermittelt werden (Fehlercode: "%3"). Überprüfen Sie, ob die IP-Adress Ressource mit den richtigen Adress-und Netzwerk Eigenschaften konfiguriert ist.

**Ereignis 1655: RES_VIPADDR_INVALID_VSID**

Fehler beim Online schalten der Cluster-IP-Adress Ressource "%1". Die Konfigurationsdaten für den Netzwerkadapter, die der virtuellen Subnetz-ID "%2" und der Routing Domänen-ID "%3" entsprechen, konnten nicht ermittelt werden (Fehlercode: "%4"). Überprüfen Sie, ob die IP-Adress Ressource mit den richtigen Adress-und Netzwerk Eigenschaften konfiguriert ist.

**Ereignis 1656: RES_VIPADDR_ADDRESS_CREATE_FAILED**

Fehler beim Hinzufügen der IP-Adresse "%2" für die nicht zusammenhängende IP-Adress Ressource "%1" (Fehlercode: "%3"). Überprüfen Sie Hardware-oder Softwarefehler im Zusammenhang mit den physischen oder virtuellen Netzwerkadaptern.

**Ereignis 1664: CLUSTER_UPGRADE_INCOMPLETE**

Fehler beim Upgrade der Funktionsebene des Clusters. Überprüfen Sie, ob alle Knoten des Clusters aktuell ausgeführt werden und die gleiche Version von Windows Server sind, und führen Sie dann das Windows PowerShell-Cmdlet Update-clusterfunctionallevel erneut aus.

**Ereignis 1676: EVENT_LOCAL_NODE_QUARANTINED**

Der lokale Cluster Knoten wurde von "%1" unter Quarantäne gestellt. Der Knoten wird bis "%2" unter Quarantäne gestellt, und anschließend versucht der Knoten automatisch, den Cluster erneut beizutreten.

Informationen zu den Problemen auf diesem Knoten finden Sie in den System-und Anwendungs Ereignisprotokollen. Wenn das Problem behoben ist, kann die Quarantäne manuell gelöscht werden, damit der Knoten mit dem Windows PowerShell-Cmdlet "Start-clusternode – clearquarantäne" erneut verknüpft werden kann.

Quarantinetype: von %1 unter Quarantäne gestellt
Die Zeit Quarantäne wird automatisch gelöscht: %2

**Ereignis 1677: EVENT_NODE_DRAIN_FAILED**

Fehler bei Knoten Ableitung auf Cluster Knoten %1.

Verweisen Sie auf die System-und Anwendungs Ereignisprotokolle und Cluster Protokolle des Knotens, um die Ursache für den Fehler bei der Ableitung zu ermitteln. Wenn das Problem behoben ist, können Sie den Ausgleichs Vorgang wiederholen.

**Ereignis 1683: RES_NETNAME_COMPUTER_ACCOUNT_NO_DC**

Der Cluster Dienst konnte keinen verfügbaren Domänen Controller in der Domäne erreichen. Dies kann Auswirkungen auf die Funktionalität haben, die von der Authentifizierung des Cluster Netzwerk namens abhängig ist.

DC-Server: %1

**Anleitungen**

Vergewissern Sie sich, dass auf die Domänen Controller im Netzwerk auf die Cluster Knoten zugegriffen werden kann.

### Ereignis 1684: RES_NETNAME_COMPUTER_OBJECT_VCO_NOT_FOUND

Die Cluster-Netzwerknamen Ressource konnte das zugehörige Computer Objekt in Active Directory nicht finden. Dies kann Auswirkungen auf die Funktionalität haben, die von der Authentifizierung des Cluster Netzwerk namens abhängig ist.

Netzwerk Name: %1
Organisationseinheit: %2

#### Anleitungen

Stellen Sie das Computer Objekt für den Netzwerknamen aus dem Active Directory Papierkorb wieder her. Alternativ dazu können Sie die Cluster-Netzwerknamen Ressource offline schalten und die Reparaturaktion ausführen, um das Computer Objekt in Active Directory neu zu erstellen.

### Ereignis 1685: RES_NETNAME_COMPUTER_OBJECT_CNO_NOT_FOUND

Die Cluster-Netzwerknamen Ressource konnte das zugehörige Computer Objekt in Active Directory nicht finden. Dies kann Auswirkungen auf die Funktionalität haben, die von der Authentifizierung des Cluster Netzwerk namens abhängig ist.

Netzwerk Name: %1
Organisationseinheit: %2

#### Anleitungen

Stellen Sie das Computer Objekt für den Netzwerknamen aus dem Active Directory Papierkorb wieder her.

### Ereignis 1686: RES_NETNAME_COMPUTER_OBJECT_VCO_DISABLED

Ressource des Cluster Netzwerk namens gefunden, dass das zugehörige Computer Objekt in Active Directory deaktiviert werden soll. Dies kann Auswirkungen auf die Funktionalität haben, die von der Authentifizierung des Cluster Netzwerk namens abhängig ist.

Netzwerk Name: %1
Organisationseinheit: %2

#### Anleitungen

Aktivieren Sie das Computer Objekt für den Netzwerknamen in Active Directory.

### Ereignis 1687: RES_NETNAME_COMPUTER_OBJECT_CNO_DISABLED

Ressource des Cluster Netzwerk namens gefunden, dass das zugehörige Computer Objekt in Active Directory deaktiviert werden soll. Dies kann Auswirkungen auf die Funktionalität haben, die von der Authentifizierung des Cluster Netzwerk namens abhängig ist.

Netzwerk Name: %1
Organisationseinheit: %2

#### Anleitungen

Aktivieren Sie das Computer Objekt für den Netzwerknamen in Active Directory. Alternativ dazu können Sie die Cluster-Netzwerknamen Ressource offline schalten und die Reparaturaktion ausführen, um das Computer Objekt in Active Directory zu aktivieren.

### Ereignis 1688: RES_NETNAME_COMPUTER_OBJECT_FAILED

Die Ressource "Cluster Netzwerkname" hat festgestellt, dass das zugeordnete Computer Objekt in Active Directory deaktiviert wurde und versucht, es zu aktivieren. Dies kann Auswirkungen auf die Funktionalität haben, die von der Authentifizierung des Cluster Netzwerk namens abhängig ist.

Netzwerk Name: %1
Organisationseinheit: %2

**Anleitungen**

Aktivieren Sie das Computer Objekt für den Netzwerknamen in Active Directory.

### Ereignis 4608: NODECLEANUP_GET_CLUSTERED_DISKS_FAILED

Clusterdienst konnte die Liste der gruppierten Datenträger nicht abrufen, während der Cluster zerstört wird. Fehlercode: ' %1 '. Wenn Sie auf diese Datenträger nicht zugreifen können, führen Sie das PowerShell-Cmdlet "Clear-clusterdiskreservation" aus.

### Ereignis 4611: NODECLEANUP_RELEASE_CLUSTERED_DISKS_FROM_PARTMGR_FAILED

Der gruppierte Datenträger mit der ID "%2" wurde vom Partitions-Manager nicht freigegeben, während der Cluster zerstört wurde. Fehlercode: ' %1 '. Durch Neustarten des Computers wird sichergestellt, dass der Datenträger vom Partitions-Manager freigegeben wird.

### Ereignis 4613: NODECLEANUP_CLEAR_CLUSDISK_DATABASE_FAILED

Der Cluster Dienst konnte einen gruppierten Datenträger mit der ID "%2" nicht ordnungsgemäß bereinigen, während der Cluster zerstört wurde. Fehlercode: ' %1 '. Möglicherweise ist der Zugriff auf diesen Datenträger erst möglich, wenn der Bereinigung erfolgreich abgeschlossen wurde. Löschen Sie für manuelles Cleanup den Wert ' attacheddisks ' des Schlüssels '\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services Clusdisk\Parameters ' in der Windows-Registrierung.

### Ereignis 4615: NODECLEANUP_DISABLE_CLUSTER_SERVICE_FAILED

Der Cluster Dienst wurde beendet und als Teil der Cluster Knoten Bereinigung als deaktiviert festgelegt.

### Ereignis 4616: NODECLEANUP_DISABLE_CLUSTER_SERVICE_TIMEOUT

Das Beenden des Cluster Dienstanbieter während der Bereinigung des Cluster Knotens wurde nicht innerhalb des erwarteten Zeitraums abgeschlossen. Starten Sie den Computer neu, um sicherzustellen, dass der Cluster Dienst nicht mehr ausgeführt wird.

### Ereignis 4618: NODECLEANUP_RESET_CLUSTER_REGISTRY_ENTRIES_FAILED

Fehler beim Zurücksetzen der Cluster Dienst-Registrierungseinträge während der Bereinigung des Cluster Knotens. Fehlercode: ' %1 '. Möglicherweise ist es nicht möglich, einen Cluster mit diesem Computer zu erstellen oder zu verknüpfen, bis die Bereinigung erfolgreich abgeschlossen wurde. Führen Sie für die manuelle Bereinigung das PowerShell-Cmdlet "Clear-clusternode" auf diesem Computer aus.

### Ereignis 4620: NODECLEANUP_UNLOAD_CLUSTER_HIVE_FAILED

Fehler beim Entladen der Cluster Dienst-Registrierungs Struktur während der Bereinigung des Cluster Knotens. Fehlercode: ' %1 '. Möglicherweise ist es nicht möglich, einen Cluster mit diesem Computer zu erstellen oder zu verknüpfen, bis die Bereinigung erfolgreich abgeschlossen wurde. Führen Sie für die manuelle Bereinigung das PowerShell-Cmdlet "Clear-clusternode" auf diesem Computer aus.

### Ereignis 4622: NODECLEANUP_ERRORS

Bei der Clusterdienst ist während des Knoten Bereinigungs Fehlers ein Fehler aufgetreten. Möglicherweise ist es nicht möglich, einen Cluster mit diesem Computer zu erstellen oder zu verknüpfen, bis die Bereinigung erfolgreich abgeschlossen wurde. Verwenden Sie für diesen Knoten das PowerShell-Cmdlet "Clear-clusternode".

### Ereignis 4624: NODECLEANUP_RESET_NLBSFLAGS_FAILED

Fehler beim Zurücksetzen des Registrierungs Werts für den IPSec-Sicherheits Zuordnungs Timeout während der Cluster Knoten Bereinigung. Fehlercode: ' %1 '. Führen Sie für die manuelle Bereinigung das PowerShell-Cmdlet "Clear-clusternode" auf diesem Computer aus. Alternativ können Sie das IPSec-Sicherheits Zuordnungs Timeout zurücksetzen, indem Sie den Wert "%2" und den Wert "%3" aus HKEY_LOCAL_MACHINE in der Windows-Registrierung löschen.

**Ereignis 4627: NODECLEANUP_DELETE_CLUSTER_TASKS_FAILED**

Fehler beim Löschen von gruppierten Tasks während der Knoten Bereinigung. Fehlercode: ' %1 '. Verwenden Sie Windows Taskplaner, um alle verbleibenden gruppierten Aufgaben zu löschen.

**Ereignis 4629: NODECLEANUP_DELETE_LOCAL_ACCOUNT_FAILED**

Während der Knoten Bereinigung wurde das lokale Benutzerkonto, das vom Cluster verwaltet wird, nicht gelöscht. Fehlercode: ' %1 '. Öffnen Sie lokale Benutzer und Gruppen (lusrmgr. msc), um das Konto zu löschen.

**Ereignis 4864: RES_VSSTASK_OPEN_FAILED**

Fehler beim Erstellen des Volumeschattenkopie-Dienst Tasks "%1". Fehlercode: "%2".

**Ereignis 4865: RES_VSSTASK_TERMINATE_TASK_FAILED**

Fehler beim Task "%1" des Volumeschattenkopie-Diensts. Fehlercode: "%2". Dies liegt daran, dass die zugeordnete Aufgabe nicht im Rahmen eines Offline Vorgangs beendet werden konnte. Sie müssen ihn ggf. manuell mit dem Taskplaner-Snap-in beendet.

**Ereignis 4866: RES_VSSTASK_DELETE_TASK_FAILED**

Fehler beim Task "%1" des Volumeschattenkopie-Diensts. Fehlercode: "%2". Dies liegt daran, dass die zugehörige Aufgabe nicht im Rahmen eines Offline Vorgangs gelöscht werden konnte. Sie müssen es unter Umständen manuell mithilfe des Taskplaner-Snap-Ins löschen.

**Ereignis 4867: RES_VSSTASK_ONLINE_FAILED**

Fehler beim Task "%1" des Volumeschattenkopie-Diensts. Fehlercode: "%2". Dies liegt daran, dass die zugehörige Aufgabe nicht als Teil eines Online Vorgangs hinzugefügt werden konnte. Verwenden Sie das Taskplaner-Snap-in, um sicherzustellen, dass ihre Aufgaben ordnungsgemäß konfiguriert sind

**Ereignis 4868: UNABLE_TO_START_AUTOLOGGER**

Clusterdienst Fehler beim Starten der Ablauf Verfolgungs Sitzung für das Cluster Protokoll. Fehlercode: "%2". Der Cluster funktioniert ordnungsgemäß, aber zusätzliche Protokollierungs Informationen fehlen. Verwenden Sie das Snap-in "System Monitor", um die Ereignis Kanaleinstellungen für "%1" zu überprüfen.

**Ereignis 4869: NETFT_WATCHDOG_PROCESS_HUNG**

Die Integritäts Überwachung im Benutzermodus hat festgestellt, dass das System nicht reagiert. Der virtuelle Adapter des Failoverclusters hat die Verbindung mit dem Prozess "%1" mit der Prozess-ID "%2" für "%3" Sekunden verloren. Verwenden Sie den System Monitor, um die Integrität des Systems zu evaluieren und zu bestimmen, welcher Prozess sich negativ auf das System auswirkt.

**Ereignis 4870: NETFT_WATCHDOG_PROCESS_TERMINATED**

Die Integritäts Überwachung im Benutzermodus hat festgestellt, dass das System nicht reagiert. Der virtuelle Adapter des Failoverclusters hat die Verbindung mit dem Prozess "%1" mit der Prozess-ID "%2" für "%3" Sekunden verloren. Wiederherstellungs Aktion wird durchgeführt.

**Ereignis 4871: NETFT_MINIPORT_INITIALIZATION_FAILURE**

Der Cluster Dienst konnte nicht gestartet werden. Dies war darauf zurückzuführen, dass der virtuelle Adapter des Failoverclusters den Mini Port-Adapter nicht initialisieren konnte. Fehlercode: ' %1 '. Vergewissern Sie sich, dass andere Netzwerkadapter ordnungsgemäß funktionieren, und überprüfen Sie den Geräte-Manager auf Fehler. Wenn die Konfiguration geändert wurde, muss ggf. die Failoverclustering-Funktion auf diesem Computer neu installiert werden.

**Ereignis 4872: NETFT_MISSING_DATALINK_ADDRESS**

Der virtuelle Adapter des Failoverclusters konnte keine eindeutige MAC-Adresse generieren. Entweder konnte kein physischer Ethernet-Adapter gefunden werden, von dem eine eindeutige Adresse generiert werden soll, oder die generierte Adresse steht in Konflikt mit einem anderen Adapter auf diesem Computer. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen.

**Ereignis 5122: DCM_EVENT_ROOT_CREATION_FAILED**

Fehler beim Erstellen des Stamm Verzeichnisses "%2" für freigegebene Clustervolumes Clusterdienst. Fehlermeldung: ' %1 '.

**Ereignis 5142: DCM_VOLUME_NO_ACCESS**

Auf Freigegebenes Clustervolume ' %1 ' (' %2 ') kann aufgrund des Fehlers ' %3 ' von diesem Cluster Knoten aus nicht mehr zugegriffen werden. Beheben Sie die Probleme dieser Knoten mit dem Speichergerät und der Netzwerk Konnektivität.

**Ereignis 5143: DCM_VETO_RESOURCE_MOVE_DUE_TO_CC**

Das Verschieben des Datenträgers ("%2") wird basierend auf dem aktuellen Status des Cache-Managers auf dem Knoten "%1" geprüft, um einen potenziellen Deadlock zu verhindern. "Cache Manager Dirty Pages theshold" ist "%3", und "Cache Manager Dirty Pages" ist "%4". Der Verschiebe Vorgang ist zulässig, wenn "geänderte Seiten des Cache-Managers" kleiner als 70% der "Cache-Manager-Änderungs Seiten theshold" ist oder wenn "Cache-Manager-Änderungs Seiten theshold" abzüglich "Cache-Manager-geänderte Seiten" größer als 128000 Seiten ist (etwa 500 MB, wenn eine Seitengröße 4096 Bytes beträgt). Der Cluster hat eine Ressourcen Verschiebung durchführen, um einen potenziellen Deadlock aufgrund von Cache-Manager-Drosselung gepufferten Schreibvorgängen zu verhindern, während freigegebene Clustervolumes auf diesem Datenträger angehalten werden

**Ereignis 5144: DCM_SNAPSHOT_DIFF_AREA_FAILURE**

Beim Hinzufügen des Datenträgers ("%1") zu freigegebenen Clustervolumes ist das Festlegen der expliziten momentaufnahmenvergleichs-Bereichs Zuordnung für Volume ("%2") mit Fehler "%3" fehlgeschlagen. Die einzige unterstützte Software Momentaufnahme-diff-Bereichs Zuordnung für freigegebene Clustervolumes ist selbst.

**Ereignis 5145: DCM_SNAPSHOT_DIFF_AREA_DELETE_FAILURE**

Von der Cluster Datenträger Ressource "%1" konnte eine Software Momentaufnahme nicht gelöscht werden. Der diff-Bereich auf Volume "%3" konnte nicht von Volume "%2" getrennt werden. Dies kann auf aktive Momentaufnahmen zurückzuführen sein. Für freigegebene Clustervolumes muss sich die Software Momentaufnahme auf demselben Datenträger befinden.

**Ereignis 5146: DCM_VETO_RESOURCE_MOVE_DUE_TO_DISMOUNT**

Das Verschieben der freigegebenes Clustervolume Ressource "%1" wurde aufgehoben, da eines der Volumes, die zur Ressource gehören, nicht bereitgestellt wurde. Wiederholen Sie die Aktion, nachdem der Vorgang zum Aufheben der Bereitstellung abgeschlossen ist.

**Ereignis 5147: DCM_VETO_RESOURCE_MOVE_DUE_TO_SNAPSHOT**

Das Verschieben der freigegebenes Clustervolume Ressource "%1" wurde aufgehoben, da eines der Volumes, die zur Ressource gehören, nicht bereitgestellt wurde. Wiederholen Sie die Aktion, nachdem der Vorgang zum Aufheben der Bereitstellung abgeschlossen ist.

**Ereignis 5148: DCM_VETO_RESOURCE_MOVE_DUE_TO_IO_MODE_CHANGE**

Der Verschiebe Vorgang der freigegebenes Clustervolume Ressource "%1" wurde aufgehoben, da ein Änderungs Vorgang für den IO-Modus (direkte e/a-Vorgänge an umgeleitete e/a oder umgekehrt) auf einem der Volumes, die zur Ressource gehören, ausgeführt wird. Wiederholen Sie die Aktion, nachdem der Vorgang abgeschlossen wurde.

**Ereignis 5150: DCM_SET_RESOURCE_IN_FAILED_STATE**

Fehler bei der physischen Datenträger Ressource "%1" für den Cluster. Der freigegebenes Clustervolume wurde mit folgendem Fehler in den Status "Fehler" versetzt: "%2"

**Ereignis 5200: CAM_CANNOT_CREATE_CNO_TOKEN**

Clusterdienst konnte kein Cluster Identitäts Token für freigegebene Clustervolumes erstellen. Fehlercode: ' %1 '. Stellen Sie sicher, dass auf den Domänen Controller zugegriffen werden kann, und überprüfen Sie Bis die Verbindung zum Domänen Controller wieder hergestellt ist, können einige Vorgänge auf diesem Knoten mit den

freigegebenen Clustervolumes fehlschlagen.

**Ereignis 5216: CSV_SW_SNAPSHOT_FAILED**

Fehler bei der Erstellung von Software Momentaufnahmen auf Freigegebenes Clustervolume "%1" ("%2") mit Fehler "%3". Die Ressource muss online sein, um die Momentaufnahme Erstellung zu unterstützen. Überprüfen Sie den Zustand der Ressource.

**Ereignis 5217: CSV_SW_SNAPSHOT_SET_FAILED**

Fehler beim Erstellen von Software Momentaufnahmen auf den freigegebenes Clustervolume ("%1") mit der Momentaufnahme Satz-ID "%2". Fehler: "%3". Überprüfen Sie den Status der CSV-Ressourcen und der Systemereignisse der Ressourcen Besitzer Knoten.

**Ereignis 5219: CSV_REGISTER_SNAPSHOT_PROV_WITH_VSS_FAILED**

Clusterdienst konnte den Momentaufnahme Anbieter für freigegebene Clustervolumes nicht mit dem volumeschattendienst (VSS) registrieren. Dies kann darauf zurückzuführen sein, dass der VSS-Dienst heruntergefahren wird oder dass ein Problem mit dem VSS-Dienst vorliegt, bei dem es nicht möglich ist, eingehende Anforderungen zu akzeptieren.
Fehler: %1

**Ereignis 5377: OPERATION_EXCEEDED_TIMEOUT**

Ein interner Clusterdienst Vorgang hat den definierten Schwellenwert von "%2" Sekunden überschritten. Die Clusterdienst wurde beendet, um wieder hergestellt zu werden. Der Dienststeuerungs-Manager startet den Clusterdienst neu, und der Knoten wird dem Cluster erneut hinzugefügt.

**Ereignis 5396: TWO_PARTITIONS_HAVE_QUORUM**

Die Clusterdienst auf diesem Knoten wird heruntergefahren, da erkannt wurde, dass andere Cluster Knoten vorhanden sind, die über ein Quorum verfügen. Dies tritt auf, wenn der Clusterdienst einen anderen Knoten erkennt, der mit dem Force-Quorum-Schalter (/FQ) gestartet wurde. Der Knoten, der mit dem Schalter Erzwingen des Quorums gestartet wurde, wird weiterhin ausgeführt. Überprüfen Sie mit Failovercluster-Manager, ob dieser Knoten beim Neustart des Cluster Dienstanbieter automatisch dem Cluster hinzugefügt wurde.

**Ereignis 5397: RLUA_ACCOUNT_FAILED**

Von der Cluster Ressource "%1" konnte das replizierte lokale Benutzerkonto "%2" auf diesem Knoten nicht erstellt oder geändert werden. Weitere Informationen finden Sie in den Cluster Protokollen.

**Ereignis 5398: NM_EVENT_CLUSTER_FAILED_TO_FORM**

Der Cluster konnte nicht gestartet werden. Die neueste Kopie der Cluster Konfigurationsdaten war innerhalb der Gruppe von Knoten, die versuchen, den Cluster zu starten, nicht verfügbar. Änderungen am Cluster sind aufgetreten, während die Gruppe der Knoten nicht Mitglied der Mitgliedschaft war und daher nicht in der Lage war, Konfigurationsdaten Aktualisierungen zu empfangen. .

Zum Starten des Clusters erforderliche Stimmen: %1
Verfügbare Stimmen: %2
Knoten mit Stimmen: %3

**Anleitungen**

Versuchen Sie, den Cluster Dienst auf allen Knoten im Cluster zu starten, damit Knoten mit der neuesten Kopie der Cluster Konfigurationsdaten zuerst den Cluster bilden können. Der Cluster kann gestartet werden, und die Knoten erhalten automatisch die aktualisierten Cluster Konfigurationsdaten. Wenn keine Knoten mit der neuesten Kopie der Cluster Konfigurationsdaten verfügbar sind, führen Sie das Windows PowerShell-Cmdlet "Start-clusternode-f" aus. Mithilfe des ForceQuorum (FQ)-Parameters wird der Cluster Dienst gestartet, und die Kopie der Cluster Konfigurationsdaten dieses Knotens wird als autorisierend gekennzeichnet. Das Erzwingen des Quorums auf einem Knoten mit einer veralteten Kopie der Cluster Datenbank führt möglicherweise zu Änderungen an der Cluster Konfiguration, die aufgetreten sind, während der Knoten nicht an dem Cluster beteiligt war.

# Warnungs Ereignisse

**Ereignis 1011: NM_NODE_EVICTED**

Der Cluster Knoten "%1" wurde aus dem Failovercluster entfernt.

**Ereignis 1045: RES_IPADDR_IPV4_ADDRESS_CREATE_FAILED**

Es wurde keine übereinstimmende Netzwerkschnittstelle für die IP-Adresse "%2" der Ressource "%1" gefunden (Rückgabecode war "%3"). Wenn sich Ihre Cluster Knoten in verschiedenen Subnetzen befinden, kann dies normal sein.

**Ereignis 1066: RES_DISK_CORRUPT_DISK**

Die Cluster Datenträger Ressource "%1" weist auf eine Beschädigung für Volume "%2" hin. Chkdsk wird ausgeführt, um Probleme zu beheben. Der Datenträger ist erst dann verfügbar, wenn Chkdsk abgeschlossen ist. Die CHKDSK-Ausgabe wird in der Datei "%3" protokolliert.
CHKDSK kann auch Informationen in das Anwendungs Ereignisprotokoll schreiben.

**Ereignis 1068: RES_SMB_SHARE_CANT_ADD**

Die Cluster Dateifreigabe-Ressource "%1" kann nicht online geschaltet werden. Fehler beim Erstellen der Dateifreigabe "%2" (für den Netzwerknamen "%3" festgelegt) aufgrund des Fehlers "%4". Dieser Vorgang wird automatisch wiederholt.

**Ereignis 1071: RCM_RESOURCE_ONLINE_BLOCKED_BY_LOCKED_MODE**

Der Vorgang für die Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2" konnte nicht abgeschlossen werden, da die Ressource oder einer ihrer Anbieter den gesperrten Status aufweist.

**Ereignis 1071: RCM_RESOURCE_OFFLINE_BLOCKED_BY_LOCKED_MODE**

Der Vorgang für die Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2" konnte nicht abgeschlossen werden, da die Ressource oder eine ihrer abhängigen Elemente den Status "gesperrt" aufweist.

**Ereignis 1094: SM_INVALID_SECURITY_LEVEL**

Die "SecurityLevel"-Eigenschaft des Clusters kann in diesem Cluster nicht geändert werden. Die Sicherheitsstufe des Clusters kann nicht geändert werden, da der Cluster derzeit für keinen Authentifizierungsmodus konfiguriert ist.

**Ereignis 1119: RES_NETNAME_DNS_REGISTRATION_MISSING**

Die Cluster Netzwerk-namens Ressource "%1" konnte den DNS-Namen "%2" für den Adapter "%4" aus folgendem Grund nicht registrieren:

"%3"

**Ereignis 1125: TM_EVENT_CLUSTER_NETINTERFACE_UNREACHABLE**

Die Cluster Netzwerkschnittstelle "%1" für Cluster Knoten "%2" im Netzwerk "%3" kann nicht von mindestens einem anderen Cluster Knoten, der mit dem Netzwerk verbunden ist, erreicht werden. Der Speicherort des Fehlers konnte vom Failovercluster nicht bestimmt werden. Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Wenn die Bedingung weiterhin besteht, prüfen Sie, ob Hardware- oder Softwarefehler im Zusammenhang mit dem Netzwerkadapter vorliegen. Überprüfen Sie auch, ob in anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler.

**Ereignis 1149: RES_NETNAME_CANT_DELETE_DNS_RECORDS**

Die der Cluster Ressource "%1" zugeordneten DNS-Host Einträge (A) und Zeiger (PTR)-Einträge wurden nicht aus dem zugeordneten DNS-Server der Ressource entfernt. Gegebenenfalls können Sie manuell gelöscht werden. Wenden Sie sich an Ihren DNS-Administrator, um Unterstützung bei diesem Aufwand

**Ereignis 1150: RES_NETNAME_DNS_PTR_RECORD_DELETE_FAILED**

Fehler beim Entfernen des DNS-Zeiger (PTR)-Datensatzes "%2" für den Host "%3", der der Cluster-Netzwerknamen Ressource "%1" zugeordnet ist. Fehler: "%4". Der Datensatz kann ggf. manuell gelöscht werden. Bitten Sie den DNS-Administrator um Unterstützung.

**Ereignis 1151: RES_NETNAME_DNS_A_RECORD_DELETE_FAILED**

Fehler beim Entfernen des DNS-Host (A)-Datensatzes "%2", der der Cluster-Netzwerknamen Ressource "%1" zugeordnet ist. Fehler: "%3". Der Datensatz kann ggf. manuell gelöscht werden. Bitten Sie den DNS-Administrator um Unterstützung.

**Ereignis 1155: RCM_EVENT_EXITED_QUEUING**

Die ausstehende Verschiebung für die Rolle "%1" wurde nicht abgeschlossen.

**Ereignis 1197: RES_NETNAME_DELETE_DISABLE_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte das zugehörige Computer Objekt "%2" beim Löschen von Ressourcen nicht löschen oder deaktivieren. Fehlercode: ' %3 '.
Überprüfen Sie, ob der Standort schreibgeschützt ist. Stellen Sie sicher, dass das Cluster Namen Objekt über die entsprechenden Berechtigungen für das Objekt "%2" in Active Directory verfügt.

**Ereignis 1198: RES_NETNAME_DELETE_VCO_GUID_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte das Computer Objekt mit der GUID "%2" nicht löschen. Fehlercode: ' %3 '.
Überprüfen Sie, ob der Standort schreibgeschützt ist. Stellen Sie sicher, dass das Cluster Namen Objekt über die entsprechenden Berechtigungen für das Objekt "%2" in Active Directory verfügt.

**Ereignis 1216: SERVICE_NETNAME_CHANGE_WARNING**

Fehler bei einem namens Änderungs Vorgang für die Cluster Core NetName-Ressource. Bei dem Versuch, den namens Änderungs Vorgang auf den ursprünglichen Namen zurückzusetzen, ist ebenfalls ein Fehler aufgetreten. Fehlercode: ' %1 '. Sie sind möglicherweise nicht in der Lage, den Cluster mithilfe des Cluster namens Remote zu verwalten, bis diese Situation manuell korrigiert wurde.

**Ereignis 1221: RES_NETNAME_RENAME_OUT_OF_SYNCH_WITH_COMPOBJ**

Die Cluster Netzwerk-namens Ressource "%1" weist den Namen "%2" auf, der nicht mit dem entsprechenden Computer Objektnamen "%3" übereinstimmt. Es ist wahrscheinlich, dass eine vorherige Namensänderung des Computer Objekts nicht auf allen Domänen Controllern in der Domäne repliziert wurde. Sie können die Netzwerknamen Ressource erst umbenennen, wenn die Namen konsistent werden. Wenn das Computer Objekt nicht vor kurzem geändert wurde, wenden Sie sich an Ihren Domänen Administrator, um das Computer Objekt umzubenennen und damit konsistent zu machen. Stellen Sie außerdem sicher, dass die Replikation über Domänen Controller hinweg erfolgreich abgeschlossen wurde.

**Ereignis 1222: RES_NETNAME_SET_PERMISSIONS_FAILED**

Das der Cluster Netzwerk-namens Ressource "%1" zugeordnete Computer Objekt konnte nicht aktualisiert werden.

Der Text für den zugeordneten Fehlercode lautet: %2

Der Cluster Identität "%3" fehlen möglicherweise die erforderlichen Berechtigungen zum Aktualisieren des Objekts. Wenden Sie sich an Ihren Domänen Administrator, um sicherzustellen, dass die Cluster Identität Computer Objekte in der Domäne aktualisieren kann.

**Ereignis 1240: RES_IPADDR_OBTAIN_LEASE_FAILED**

Die Cluster-IP-Adress Ressource "%1" konnte keine geleast-IP-Adresse abrufen.

**Ereignis 1243: RES_IPADDR_RELEASE_LEASE_FAILED**

Die Cluster-IP-Adress Ressource "%1" konnte die Lease für die IP-Adresse "%2" nicht freigeben.

**Ereignis 1251: RCM_GROUP_PREEMPTED**

Die Cluster Rolle "%2" wurde offline geschaltet. Diese Rolle wurde von der gruppierten Rolle "%1" mit höherer Priorität vorzeitig entfernt. Der Cluster Dienst versucht, die Cluster Rolle "%2" zu einem späteren Zeitpunkt online zu schalten, wenn Systemressourcen verfügbar sind.

**Ereignis 1544: SERVICE_VSS_ONABORT**

Der Sicherungs Vorgang für die Cluster Konfigurationsdaten wurde abgebrochen. Der VSS-Writer (Cluster Volumeschattenkopie-Dienst) hat eine Abbruch Anforderung empfangen.

**Ereignis 1548: SERVICE_CONNECT_VERSION_COMPATIBLE**

Knoten "%1" hat die Kommunikation mit dem Knoten "%2" hergestellt und erkannt, dass eine andere, aber kompatible Version des Betriebssystems ausgeführt wird. Es wird empfohlen, dass alle Knoten die gleiche Version des Betriebssystems ausführen. Nachdem alle Knoten aktualisiert wurden, führen Sie das Windows PowerShell-Cmdlet Update-clusterfunctionallevel aus, um das Upgrade des Clusters abzuschließen.

**Ereignis 1550: SERVICE_CONNECT_NOVERCHECK**

Knoten "%1" hat eine Kommunikationssitzung mit dem Knoten "%2" erstellt, ohne dass eine Versions Kompatibilitätsprüfung durchgeführt wurde, da die Versions Kompatibilitäts Überprüfung deaktiviert ist. Die Deaktivierung der Versions Kompatibilitäts Überprüfung wird nicht unterstützt.

**Ereignis 1551: SERVICE_FORM_NOVERCHECK**

Knoten "%1" hat einen Failovercluster ohne Versions Kompatibilitätsprüfung erstellt, da die Überprüfung der Versions Kompatibilität deaktiviert ist. Die Deaktivierung der Versions Kompatibilitäts Überprüfung wird nicht unterstützt.

**Ereignis 1555: SERVICE_NETFT_DISABLE_AUTOCONFIG_FAILED**

Fehler beim Versuch, IPv4 für den Netzwerkadapter "%1" zu verwenden. Dies war darauf zurückzuführen, dass die automatische IPv4-Konfiguration und DHCP nicht deaktiviert wurden. Dies wird möglicherweise erwartet, wenn der DHCP-Client Dienst bereits deaktiviert ist. Wenn diese Option aktiviert ist, wird IPv6 verwendet. andernfalls ist dieser Knoten möglicherweise nicht in der Lage, an einem Failovercluster teilzunehmen.

**Ereignis 1558: SERVICE_WITNESS_FAILOVER_ATTEMPT**

Der Cluster Dienst hat ein Problem mit der Zeugen Ressource festgestellt. Für die Zeugen Ressource wird ein Failover zu einem anderen Knoten im Cluster durchgeführt, wenn versucht wird, den Zugriff auf die Cluster Konfigurationsdaten wiederherzustellen.

**Ereignis 1562: RES_FSW_ALIVEFAILURE**

Die Dateifreigabe-Zeugen Ressource "%1" hat eine regelmäßige Integritäts Überprüfung für die Dateifreigabe "%2" nicht bestanden. Stellen Sie sicher, dass die Dateifreigabe "%2" vorhanden ist und dass der Cluster darauf zugreifen kann.

**Ereignis 1576: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_REFUSED**

Die Cluster Netzwerk-namens Ressource "%1" konnte den Namen "%2" für den Adapter "%4" in einer sicheren DNS-Zone nicht registrieren. Dies war auf einen vorhandenen Datensatz mit diesem Namen zurückzuführen, und die Cluster Identität verfügt nicht über ausreichende Berechtigungen zum Aktualisieren dieses Datensatzes. Fehlercode: ' %3 '. Wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob die Cluster Identität über Berechtigungen für den DNS-Datensatz "%2

**Ereignis 1576: RES_NETNAME_DNS_REGISTRATION_SECURE_ZONE_REFUSED**

Die Cluster Netzwerk-namens Ressource "%1" konnte den Namen "%2" für den Adapter "%4" in einer sicheren DNS-Zone nicht registrieren. Dies war auf einen vorhandenen Datensatz mit diesem Namen zurückzuführen, und die Cluster Identität verfügt nicht über ausreichende Berechtigungen zum Aktualisieren dieses Datensatzes. Fehlercode: ' %3 '. Wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob die Cluster Identität über Berechtigungen für den DNS-Datensatz "%2

**Ereignis 1577: RES_NETNAME_DNS_SERVER_COULD_NOT_BE_CONTACTED**

Fehler beim Registrieren des Namens "%2" für den Adapter "%4" durch die Cluster Netzwerk-namens Ressource "%1". Der DNS-Server konnte nicht kontaktiert werden. Fehlercode: "%3". Stellen Sie sicher, dass über diesen Cluster Knoten auf einen DNS-Server zugegriffen werden kann. Die DNS-Registrierung wird später erneut versucht.

**Ereignis 1577: RES_NETNAME_DNS_SERVER_COULD_NOT_BE_CONTACTED**

Fehler beim Registrieren des Namens "%2" für den Adapter "%4" durch die Cluster Netzwerk-namens Ressource "%1". Der DNS-Server konnte nicht kontaktiert werden. Fehlercode: "%3". Stellen Sie sicher, dass über diesen Cluster Knoten auf einen DNS-Server zugegriffen werden kann. Die DNS-Registrierung wird später erneut versucht.

**Ereignis 1578: RES_NETNAME_DNS_TEST_FOR_DYNAMIC_UPDATE_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte die dynamischen Updates für den Namen "%2" über den Adapter "%4" nicht registrieren. Der DNS-Server ist möglicherweise nicht für das akzeptieren dynamischer Updates konfiguriert. Fehlercode: ' %3 '. Wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob der DNS-Server verfügbar und für dynamische Updates konfiguriert ist.

Alternativ können Sie dynamische DNS-Updates deaktivieren, indem Sie die Einstellung "Adressen dieser Verbindung in DNS registrieren" in den erweiterten TCP/IP-Einstellungen für den Adapter "%4" auf der Registerkarte "DNS" deaktivieren.

**Ereignis 1578: RES_NETNAME_DNS_TEST_FOR_DYNAMIC_UPDATE_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte die dynamischen Updates für den Namen "%2" über den Adapter "%4" nicht registrieren. Der DNS-Server ist möglicherweise nicht für das akzeptieren dynamischer Updates konfiguriert. Fehlercode: ' %3 '. Wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob der DNS-Server verfügbar und für dynamische Updates konfiguriert ist.

Alternativ können Sie dynamische DNS-Updates deaktivieren, indem Sie die Einstellung "Adressen dieser Verbindung in DNS registrieren" in den erweiterten TCP/IP-Einstellungen für den Adapter "%4" auf der Registerkarte "DNS" deaktivieren.

**Ereignis 1579: RES_NETNAME_DNS_RECORD_UPDATE_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte den DNS-Datensatz für den Namen "%2" über den Adapter "%4" nicht aktualisieren. Fehlercode: ' %3 '. Stellen Sie sicher, dass auf einen DNS-Server von diesem Cluster Knoten aus zugegriffen werden kann, und wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob die Cluster Identität den DNS-Datensatz

**Ereignis 1579: RES_NETNAME_DNS_RECORD_UPDATE_FAILED**

Die Cluster Netzwerk-namens Ressource "%1" konnte den DNS-Datensatz für den Namen "%2" über den Adapter "%4" nicht aktualisieren. Fehlercode: ' %3 '. Stellen Sie sicher, dass auf einen DNS-Server von diesem Cluster Knoten aus zugegriffen werden kann, und wenden Sie sich an den DNS-Server Administrator, um zu überprüfen, ob die Cluster Identität den DNS-Datensatz

**Ereignis 1581: CLUSSVC_UNABLE_TO_MOVE_HIVE_TO_SAFE_FILE**

Die Wiederherstellungs Anforderung für die Cluster Konfigurationsdaten konnte keine Kopie der vorhandenen Cluster Konfigurationsdatendatei (CLUSDB) erstellen. Beim Versuch, die vorhandene Konfiguration beizubehalten, konnte der Wiederherstellungs Vorgang eine Kopie am Speicherort "%1" nicht erstellen. Dies wird möglicherweise erwartet, wenn die vorhandene Konfigurations Datendatei beschädigt ist. Der Wiederherstellungs Vorgang wurde fortgesetzt. es ist jedoch möglich, dass versucht wird, die vorhandene Cluster Konfiguration wiederherzustellen.

**Ereignis 1582: CLUSSVC_UNABLE_TO_MOVE_RESTORED_HIVE_TO_CURRENT**

Der Cluster Dienst konnte die wiederhergestellte Cluster Struktur bei "%1" nicht nach "%2" verschieben. Dadurch wird möglicherweise verhindert, dass der Wiederherstellungs Vorgang erfolgreich ausgeführt wird. Wenn die Cluster Konfiguration nicht ordnungsgemäß wieder hergestellt wurde, wiederholen Sie den Wiederherstellungs

Vorgang.

### Ereignis 1583: CLUSSVC_NETFT_DISABLE_CONNECTIONSECURITY_FAILED

Clusterdienst konnte die Internet Protokoll Sicherheit (IPSec) auf dem virtuellen failoverclusteradapter "%1" nicht deaktivieren. Dies kann sich negativ auf die Leistung der Cluster Kommunikation auswirken. Wenn dieses Problem weiterhin besteht, überprüfen Sie die Sicherheitsrichtlinien für lokale und Domänen Verbindungen, die auf IPSec und die Windows-Firewall angewendet werden. Überprüfen Sie außerdem, ob Ereignisse im Zusammenhang mit dem Basis Filtermodul-Dienst angezeigt werden.

### Ereignis 1584: SHARED_VOLUME_NOT_READY_FOR_SNAPSHOT

Eine Sicherungs Anwendung hat eine VSS-Momentaufnahme auf Freigegebenes Clustervolume "%1" ("%3") initiiert, ohne dass das Volume für die Momentaufnahme ordnungsgemäß vorbereitet wurde. Diese Momentaufnahme ist möglicherweise ungültig, und die Sicherung kann möglicherweise nicht für Wiederherstellungs Vorgänge verwendet werden. Wenden Sie sich an Ihren Anbieter für die Sicherungs Anwendung, um die Kompatibilität mit freigegebenen Clustervolumes

### Ereignis 1589: RES_NETNAME_DNS_RETURNING_IP_THAT_IS_NOT_PROVIDER

Die Cluster Netzwerk-namens Ressource "%1" hat mindestens eine IP-Adresse gefunden, die dem DNS-Namen "%2" zugeordnet ist, die keine abhängigen IP-Adress Ressourcen sind. Die gefundenen zusätzlichen Adressen waren "%3". Dies wirkt sich möglicherweise auf die Client Konnektivität aus, bis der Netzwerkname und die zugehörigen DNS-Einträge konsistent sind. Wenden Sie sich an den DNS-Server Administrator, um die dem Namen "%2" zugeordneten Datensätze zu überprüfen

### Ereignis 1604: RES_DISK_CHKDSK_SPOTFIX_NEEDED

Die Cluster Datenträger Ressource "%1" hat eine Beschädigung für Volume "%2" erkannt. Zum Beheben von Problemen ist "spotfix Chkdsk" erforderlich.

### Ereignis 1605: RES_DISK_SPOTFIX_PERFORMED

Die Cluster Datenträger Ressource "%1" hat die Ausführung von Chkdsk. exe/spotfix auf Volume "%2" abgeschlossen. Der Rückgabecode war "%4". Die Ausgabe von CHKDSK wurde in der Datei "%3" protokolliert. Überprüfen Sie das Anwendungs Ereignisprotokoll auf zusätzliche Informationen von Chkdsk.

### Ereignis 1671: RES_DISK_ONLINE_SET_ATTRIBUTES_COMPLETED_FAILURE

Die physische Datenträger Ressource des Clusters kann nicht online geschaltet werden.

Name der physischen Datenträger Ressource: %1
Fehler Code: %2
Verstrichene Zeit (Sekunden): %3

#### Anleitungen

Führen Sie den Konfigurationsüberprüfungs-Assistenten aus, um die Speicherkonfiguration zu überprüfen. Wenn der Fehlercode ERROR_CLUSTER_SHUTDOWN wurde, wurde der ausstehende Online Status von einem Administrator abgebrochen. Wenn es sich um ein repliziertes Volume handelt, könnte dies das Ergebnis eines Fehlers beim Festlegen der Datenträger Attribute sein. Überprüfen Sie die Speicher Replikations Ereignisse auf Weitere Informationen.

### Ereignis 1673: CLUSTER_NODE_ENTERED_ISOLATED_STATE

Der Cluster Knoten "%1" wurde in den isolierten Zustand versetzt.

### Ereignis 1675: EVENT_JOINING_NODE_QUARANTINED

Der Cluster Knoten "%1" wurde von "%2" unter Quarantäne gestellt und kann nicht dem Cluster beitreten. Der Knoten wird bis "%3" unter Quarantäne gestellt, und anschließend versucht der Knoten automatisch, den Cluster erneut beizutreten.

Informationen zu den Problemen auf diesem Knoten finden Sie in den System-und Anwendungs Ereignisprotokollen. Wenn das Problem behoben ist, kann die Quarantäne manuell gelöscht werden, damit der Knoten mit dem Windows PowerShell-Cmdlet "Start-clusternode – clearquarantäne" erneut verknüpft werden kann.

Knoten Name: %1
Quarantinetype: Quarantäne durch %2
Die Zeit Quarantäne wird automatisch gelöscht: %3

**Ereignis 1681: CLUSTER_GROUPS_UNMONITORED_ON_NODE**

Die virtuellen Maschinen auf dem Knoten "%1" haben einen nicht überwachten Zustand. Die Integrität der virtuellen Computer wird erneut überwacht, sobald der Knoten von einem isolierten Status zurückkehrt oder ein Failover durchführt, wenn der Knoten nicht zurückkehrt. Der virtuelle Computer wird nicht mehr überwacht: %2.

**Ereignis 1689: EVENT_DISABLE_AND_STOP_OTHER_SERVICE**

Der Cluster Dienst hat einen Dienst erkannt, der mit dem Failoverclustering nicht kompatibel ist. Der Dienst wurde deaktiviert, um mögliche Probleme mit dem Failovercluster zu vermeiden.

Dienst Name: "%1"

**Ereignis 4625: NODECLEANUP_RESET_NLBSFLAGS_PRESERVED**

Fehler beim Zurücksetzen des Registrierungs Werts für den IPSec-Sicherheits Zuordnungs Timeout während der Cluster Knoten Bereinigung. Dies liegt daran, dass das IPSec-Sicherheits Zuordnungs Timeout geändert wurde, nachdem dieser Computer als Mitglied eines Clusters konfiguriert wurde. Führen Sie für die manuelle Bereinigung das PowerShell-Cmdlet "Clear-clusternode" auf diesem Computer aus. Alternativ können Sie das IPSec-Sicherheits Zuordnungs Timeout zurücksetzen, indem Sie den Wert "%1" und den Wert "%2" aus HKEY_LOCAL_MACHINE in der Windows-Registrierung löschen.

**Ereignis 4873: NETFT_CLUSSVC_TERMINATE_BECAUSE_OF_WATCHDOG**

Der Cluster Dienst hat festgestellt, dass der virtuelle Adapter des Failoverclusters angehalten wurde. Dies wird erwartet, wenn die CPU-Auslastung auf diesem Knoten durchgeführt wird. Clusterdienst wird beendet und sollte nach Abschluss des Vorgangs automatisch neu gestartet werden. Überprüfen Sie, ob dem Dienst weitere Ereignisse zugeordnet sind, und stellen Sie sicher, dass der Cluster Dienst auf diesem Knoten neu gestartet wurde.

**Ereignis 5120: DCM_VOLUME_AUTO_PAUSE_AFTER_FAILURE**

Der freigegebenes Clustervolume "%1" ("%2") hat sich aufgrund von "%3" in einen angehaltenen Zustand versetzt. Alle e/a-Vorgänge werden vorübergehend in die Warteschlange eingereiht, bis ein Pfad zum Volume wieder hergestellt wird.

**Ereignis 5123: DCM_EVENT_ROOT_RENAME_SUCCESS**

Das Stammverzeichnis "%1" für freigegebene Clustervolumes ist bereits vorhanden. Das Verzeichnis "%1" wurde in "%2" umbenannt. Vergewissern Sie sich, dass Anwendungen, die auf Daten an diesem Speicherort zugreifen, bei Bedarf aktualisiert wurden.

**Ereignis 5124: DCM_UNSAFE_FILTERS_FOUND**

Freigegebenes Clustervolume "%1" ("%3") hat mindestens einen aktiven Filtertreiber auf diesem Geräte Stapel identifiziert, der die CSV-Vorgänge beeinträchtigen könnte. Der e/a-Zugriff wird über das Netzwerk über einen anderen Cluster Knoten an das Speichergerät umgeleitet. Dies kann zu einer Beeinträchtigung der Leistung führen. Wenden Sie sich an den Hersteller des Filter Treibers, um die Interoperabilität mit freigegebenen Clustervolumes

Aktive Filtertreiber gefunden:
%2

**Ereignis 5125: DCM_UNSAFE_VOLFILTER_FOUND**

Freigegebenes Clustervolume "%1" ("%3") hat mindestens einen aktiven Volumetreiber in diesem Geräte Stapel

identifiziert, der die CSV-Vorgänge beeinträchtigen könnte. Der e/a-Zugriff wird über das Netzwerk über einen anderen Cluster Knoten an das Speichergerät umgeleitet. Dies kann zu einer Beeinträchtigung der Leistung führen. Bitten Sie den volumetreiberhersteller, die Interoperabilität mit freigegebenen Clustervolumes zu überprüfen

Aktive Volumetreiber gefunden:
%2

**Ereignis 5126: DCM_EVENT_CANNOT_DISABLE_SHORT_NAMES**

Die physische Datenträger Ressource "%1" lässt keine Deaktivierung der Kurznamen Generierung zu. Dies kann zu Anwendungs Kompatibilitätsproblemen führen. Verwenden Sie "fsutil 8dot3name Set 2", um die Deaktivierung der Kurznamen Generierung zuzulassen und die Ressource dann offline/online zu schalten.

**Ereignis 5128: DCM_EVENT_CANNOT_DISABLE_SHORT_NAMES**

Die physische Datenträger Ressource "%1" lässt keine Deaktivierung der Kurznamen Generierung zu. Dies kann zu Anwendungs Kompatibilitätsproblemen führen. Verwenden Sie "fsutil 8dot3name Set 2", um die Deaktivierung der Kurznamen Generierung zuzulassen und die Ressource dann offline/online zu schalten.

**Ereignis 5133: DCM_CANNOT_RESTORE_DRIVE_LETTERS**

Der Cluster Datenträger "%1" wurde entfernt und in der Clustergruppe "verfügbarer Speicher" wieder abgelegt. Während dieses Vorgangs wurde der Versuch, den ursprünglichen Laufwerk Buchstaben wiederherzustellen, länger als erwartet benötigt, möglicherweise aufgrund der bereits verwendeten Laufwerksbuchstaben.

**Ereignis 5134: DCM_CANNOT_SET_ACL_ON_ROOT**

Clusterdienst Fehler beim Festlegen der Berechtigungen (ACL) für das Stammverzeichnis "%1" für freigegebene Clustervolumes. Fehler: "%2".

**Ereignis 5135: DCM_CANNOT_SET_ACL_ON_VOLUME_FOLDER**

Clusterdienst konnte die Berechtigungen für das freigegebenes Clustervolume Verzeichnis "%1" ("%2") nicht festlegen. Der Fehler lautet "%3".

**Ereignis 5136: DCM_CSV_INTO_REDIRECTED_MODE**

Der umgeleitete Zugriff freigegebenes Clustervolume "%1" ("%2") wurde aktiviert. Der Zugriff auf das Speichergerät wird über das Netzwerk von allen Cluster Knoten umgeleitet, die auf dieses Volume zugreifen. Dies kann zu einer Beeinträchtigung der Leistung führen. Deaktivieren Sie den umgeleiteten Zugriff für dieses Volume, um den normalen Betrieb wieder aufzunehmen.

**Ereignis 5149: DCM_CSV_BLOCK_CACHE_RESIZED**

Die Größe der Cache Größe wurde auf Grundlage des gefüllten Speichers in "%1" geändert. der Benutzer "setSize" ist zu hoch.

**Ereignis 5156: DCM_VOLUME_AUTO_PAUSE_AFTER_SNAPSHOT_FAILURE**

Der freigegebenes Clustervolume "%1" ("%2") hat sich aufgrund von "%3" in einen angehaltenen Zustand versetzt. Dieser Fehler wird angezeigt, wenn die Volsnap-Momentaufnahmen, die dem CSV-Volume zugrunde liegen, außerhalb einer Benutzer Anforderung gelöscht werden. Mögliche Ursachen dafür, dass die Momentaufnahmen gelöscht werden, sind nicht genügend Speicherplatz auf dem Volume, um die Momentaufnahmen zu vergrößern, oder e/a-Fehler beim Aktualisieren der Momentaufnahme Daten. Alle e/a-Vorgänge werden vorübergehend in die Warteschlange eingereiht, bis der Momentaufnahme Status mit Volsnap synchronisiert wird.

**Ereignis 5157: DCM_VOLUME_AUTO_PAUSE_AFTER_FAILURE_EXPECTED**

Der freigegebenes Clustervolume "%1" ("%2") hat sich aufgrund von "%3" in einen angehaltenen Zustand versetzt. Alle e/a-Vorgänge werden vorübergehend in die Warteschlange eingereiht, bis ein Pfad zum Volume wieder hergestellt wird. Dieser Fehler wird normalerweise durch einen Infrastruktur Fehler verursacht. Beispielsweise können Sie die Konnektivität mit dem Speicher oder dem Knoten verlieren, der das freigegebenes Clustervolume aus der aktiven Cluster Mitgliedschaft entfernt hat.

**Ereignis 5394: POOL_ONLINE_WARNINGS**

Beim Versuch, den Speicherpool online zu schalten, sind bei der Clusterdienst Speicherfehler aufgetreten. Führen Sie die Cluster Speicher Überprüfung aus, um das Problem zu beheben.

**Ereignis 5395: RCM_GROUP_AUTO_MOVE_STORAGE_POOL**

Die Gruppe wird vom Cluster für den Speicherpool "%1" verschoben, da der aktuelle Knoten "%3" nicht über eine optimale Konnektivität mit den physischen Datenträgern des Speicherpools verfügt.

# Informations Ereignisse

**Ereignis 1592: CLUSSVC_TCP_RECONNECT_CONNECTION_REESTABLISHED**

Der Cluster Knoten "%1" hat die Kommunikation mit dem Cluster Knoten "%2" verloren. Die Netzwerkkommunikation wurde wieder hergestellt. Dies kann darauf zurückzuführen sein, dass die Kommunikation vorübergehend durch eine Firewall oder ein Update der Verbindungs Sicherheitsrichtlinie blockiert wird. Wenn das Problem weiterhin besteht und die Netzwerkkommunikation nicht wieder hergestellt wird, wird der Cluster Dienst auf einem oder mehreren Knoten angehalten. Führen Sie in diesem Fall den Konfigurationsüberprüfungs-Assistenten aus, um die Netzwerkkonfiguration zu überprüfen. Überprüfen Sie außerdem auf Hardware-oder Softwarefehler im Zusammenhang mit den Netzwerkadaptern auf diesem Knoten, und überprüfen Sie, ob in allen anderen Netzwerkkomponenten, mit denen der Knoten verbunden ist, wie z. b. Hubs, Switches oder Bridges, auf Fehler

**Ereignis 1594: CLUSTER_FUNCTIONAL_LEVEL_UPGRADE_COMPLETE**

Clusterdienst erfolgreich ein Upgrade der Cluster Funktionsebene durchgeführt.

Funktionsebene: %1
Upgradeversion: %2

**Ereignis 1635: RCM_RESOURCE_FAILURE_INFO_WITH_TYPENAME**

Fehler bei der Cluster Ressource "%1" vom Typ "%3" in der Cluster Rolle "%2".

**Ereignis 1636: CLUSSVC_PASSWORD_CHANGED**

Der Clusterdienst hat das Kennwort des Kontos "%1" auf dem Knoten "%2" geändert.

**Ereignis 1680: CLUSTER_NODE_EXITED_ISOLATED_STATE**

Der Cluster Knoten ' %1 ' hat den isolierten Status beendet.

**Ereignis 1682: CLUSTER_GROUP_MOVED_NO_LONGER_UNMONITORED**

Für den virtuellen Computer "%2", der auf dem isolierten Knoten "%1" nicht überwacht wurde, wurde ein Failover auf einen anderen Knoten durchgeführt. Die Integrität des virtuellen Computers wird erneut überwacht.

**Ereignis 1682: CLUSTER_MULTIPLE_GROUPS_NO_LONGER_UNMONITORED**

Knoten "%1" wurde dem Cluster erneut hinzugefügt, und auf den folgenden virtuellen Computern, die auf diesem Knoten ausgeführt werden, wird erneut der Integritäts Status überwacht: %2.

**Ereignis 4621: NODECLEANUP_SUCCESS**

Dieser Knoten wurde erfolgreich aus dem Cluster entfernt.

**Ereignis 5121: DCM_VOLUME_NO_DIRECT_IO_DUE_TO_FAILURE**

Auf Freigegebenes Clustervolume ' %1 ' (' %2 ') kann von diesem Cluster Knoten aus nicht mehr direkt zugegriffen werden. Der e/a-Zugriff wird über das Netzwerk an den Knoten umgeleitet, der das Volume besitzt. Wenn dies zu einer Beeinträchtigung der Leistung führt, führen Sie eine Problembehandlung für die Verbindung dieses Knotens mit dem Speichergerät und e/a-Vorgänge in einen fehlerfreien Status aus, sobald die Verbindung mit dem Speichergerät wieder hergestellt wird.

**Ereignis 5218: CSV_OLD_SW_SNAPSHOT_DELETED**

Die physische Datenträger Ressource "%1" des Clusters löschte eine Software Momentaufnahme. Die Software Momentaufnahme auf Freigegebenes Clustervolume ' %2 ' wurde gelöscht, weil Sie älter als ' %3 ' Tag (e) war. Die Momentaufnahme-ID lautete "%4" und wurde aus dem Knoten "%5" auf "%6" erstellt. Es wird erwartet, dass Momentaufnahmen von einer Sicherungs Anwendung gelöscht werden, nachdem ein Sicherungsauftrag abgeschlossen wurde. Diese Momentaufnahme hat die Zeit überschritten, die für das vorhanden sein einer Momentaufnahme erwartet wird. Überprüfen Sie mit der Sicherungs Anwendung, ob Sicherungsaufträge erfolgreich abgeschlossen werden.

## Weitere Informationen

- Ausführliche Ereignis Informationen für Failoverclustering-Komponenten in Windows Server 2008

# Änderungsverlauf für Failovercluster-Themen

09.04.2020 • 3 minutes to read • Edit Online

> Gilt für: Windows Server 2019, Windows Server 2016

In diesem Thema werden neue und aktualisierte Themen in der Dokumentation zu Failoverclustering für Windows Server aufgeführt.

> Der Updateverlauf für Windows Server 2016 befindet sich unter Updateverlauf für Windows 10 und Windows Server 2016.

## 2020. Januar

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Cluster Ereignisse | Neu |

## 2019. März

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Clusteraffinität | Neu |

## Februar 2019

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Upgrade eines Failoverclusters auf derselben Hardware | Neu |
| Bereitstellen eines Dateiservers mit zwei Knoten | Neu |

## 2019. Januar

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Bereitstellen eines Dateifreigabezeugen | Neu |
| Clusterdomänenmigration | Neu |

## November 2018

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Konfigurieren von Clusterkonten in Active Directory | Migriert von der früheren Version der Bibliothek |

## Oktober 2018

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Neues beim Clustering | Updates für Windows Server 2019 |

## 2018. Juni

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Clustergruppen | Neues Thema |

## Mai 2018

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Konfigurieren und Verwalten des Quorums | Migriert von der vorherigen Versions Bibliothek. |

## April 2018

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Problembehandlung bei einem Failovercluster mit Windows-Fehlerberichterstattung | Neues Thema. |
| Dateiserver mit horizontaler Skalierung für Anwendungsdaten | Migriert von der vorherigen Versions Bibliothek. |
| Hardwareanforderungen | Migriert von der vorherigen Versions Bibliothek. |
| Verwenden von freigegebenen Clustervolumes (CSVs) | Migriert von der vorherigen Versions Bibliothek. |
| Erstellen eines Failoverclusters | Migriert von der vorherigen Versions Bibliothek. |
| Vorabbereitstellen eines Clusters in AD DS | Migriert von der vorherigen Versions Bibliothek. |
| Bereitstellen eines cloudzeugen für einen Failovercluster | Migriert von der vorherigen Versions Bibliothek. |

## Juni 2017

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Erweiterte Optionen für das Cluster fähige aktualisieren | Es wurden Informationen zur Verwendung von Pfad Profil Pfaden mit Leerzeichen hinzugefügt. |

## April 2017

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Übersicht über das Cluster fähige aktualisieren | Neues Thema. |

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Anforderungen und Best Practices für clusterfähiges Aktualisieren | Neues Thema. |
| Erweiterte Optionen für das Cluster fähige aktualisieren | Neues Thema. |
| FAQ zum Aktualisieren von Cluster fähigen Updates | Neues Thema. |
| Plug-Ins für Cluster fähiges aktualisieren | Neues Thema. |
| Bereitstellen eines cloudzeugen für einen Failovercluster | Der Typ des erforderlichen Speicher Kontos wurde erläutert (Sie können Azure Storage Premium-oder BLOB Storage-Konten nicht verwenden). |

## März 2017

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Bereitstellen eines cloudzeugen für einen Failovercluster | Aktualisierte Screenshots, um Änderungen an Microsoft Azure abzugleichen. |

## Februar 2017

| NEUES ODER GEÄNDERTES THEMA | BESCHREIBUNG |
| --- | --- |
| Paralleles Upgrade des Cluster Betriebssystems | Eine unnötige Vorsicht wurde entfernt, und es wurde ein Link hinzugefügt. |