



## 验证此配置是否能够无中断运行 ONTAP 9

NetApp  
September 12, 2024

This PDF was generated from <https://docs.netapp.com/zh-cn/ontap/smb-hyper-v-sql/health-monitoring-nondisruptive-operation-concept.html> on September 12, 2024. Always check docs.netapp.com for the latest.

# 目录

- 验证此配置是否能够无中断运行 ..... 1
  - 使用运行状况监控来确定无中断运行状态是否正常 ..... 1
  - 使用系统运行状况监控功能显示无中断运行状态 ..... 1
  - 验证持续可用的 SMB 共享配置 ..... 3
  - 验证 LIF 状态 ..... 5
  - 确定 SMB 会话是否持续可用 ..... 7

# 验证此配置是否能够无中断运行

## 使用运行状况监控来确定无中断运行状态是否正常

运行状况监控可提供有关整个集群中的系统运行状况的信息。运行状况监控器可通过 SMB 监控 Hyper-V 和 SQL Server 配置，以确保应用程序服务器无中断运行（NDO）。如果状态为 degraded，则可以查看有关问题的详细信息，包括可能发生原因和建议的恢复操作。

有多个运行状况监控器。ONTAP 可监控各个运行状况监控器的整体系统运行状况和运行状况。节点连接运行状况监控器包含 CIFS-NDO 子系统。监控器具有一组运行状况策略，可在某些物理条件可能导致中断时触发警报，如果存在中断情况，则会生成警报并提供有关更正操作的信息。对于基于 SMB 的 NDO 配置，将针对以下两种情况生成警报：

警报 ID	severity	条件
HaNotReadyCifsNdo_Alert	major	节点上聚合中某个卷托管的一个或多个文件已通过持续可用的 SMB 共享打开，并承诺在发生故障时会持久存在；但是，与配对节点的 HA 关系未配置或运行状况不佳。
NoStandbyLifCifsNdo_Alert	次要	Storage Virtual Machine （SVM）正在通过节点主动通过 SMB 提供数据，并且在持续可用的共享上持久打开了 SMB 文件；但是，其配对节点不会公开 SVM 的任何活动数据 LIF。

## 使用系统运行状况监控功能显示无中断运行状态

您可以使用 `system health` 用于显示有关集群的整体系统运行状况和CI-NDO子系统运行状况的信息、响应警报、配置未来警报以及显示有关如何配置运行状况监控的信息的命令。

### 步骤

1. 通过执行相应的操作来监控运行状况：

要显示的内容	输入命令 ...
系统的运行状况，反映单个运行状况监控器的整体状态	<code>system health status show</code>
有关 CIFS-NDO 子系统运行状况的信息	<code>system health subsystem show -subsystem CIFS-NDO -instance</code>

2. 显示有关如何通过执行相应操作配置 CIFS-NDO 警报监控的信息：

要显示的信息	输入命令 ...
CIFS-NDO 子系统运行状况监控器的配置和状态，例如受监控节点，初始化状态和状态	<b>system health config show -subsystem CIFS-NDO</b>
CIFS-NDO 警报，运行状况监控器可能会生成此警报	<b>system health alert definition show -subsystem CIFS-NDO</b>
CIFS-NDO 运行状况监控策略，用于确定何时发出警报	<b>system health policy definition show -monitor node-connect</b>



使用 `-instance` 用于显示详细信息的参数。

示例

以下输出显示了有关集群和 CIFS-NDO 子系统的整体运行状况的信息：

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
Number of Suppressed Alerts: 0
                Node: node2
    Subsystem Refresh Interval: 5m
```

以下输出显示了有关 CIFS-NDO 子系统运行状况监控器的配置和状态的详细信息：

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

## 验证持续可用的 **SMB** 共享配置

要支持无中断运行，必须将 Hyper-V 和 SQL Server SMB 共享配置为持续可用的共享。此外，您还必须检查某些其他共享设置。如果发生计划内或计划外中断事件，您应验证共享是否已正确配置，以便为应用程序服务器提供无缝无中断运行。

关于此任务

您必须验证以下两个共享参数是否设置正确：

- `-offline-files` 参数设置为任一 `manual` (默认值)或 `none`。

- 必须禁用符号链接。

要实现正确的无中断运行，必须设置以下共享属性：

- continuously-available
- oplocks

不能设置以下共享属性：

- homedirectory
- attributecache
- branchcache
- access-based-enumeration

#### 步骤

1. 验证脱机文件是否设置为 manual 或 disabled 并禁用符号链接：

```
vserver cifs shares show -vserver vserver_name
```

2. 验证 SMB 共享是否已配置为持续可用性：

```
vserver cifs shares properties show -vserver vserver_name
```

#### 示例

以下示例显示了 Storage Virtual Machine （SVM，以前称为 Vserver）vs1 上名为 share1 的共享的共享设置。脱机文件设置为 manual 和符号链接已禁用(在中使用连字符指定) Symlink Properties 字段输出)：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
      Vserver: vs1
      Share: share1
      CIFS Server NetBIOS Name: VS1
      Path: /data/share1
      Share Properties: oplocks
                      continuously-available
      Symlink Properties: -
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: -
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

以下示例显示了 SVM vs1 上名为 share1 的共享的共享属性：

```
cluster1::> vservers cifs share properties show -vservers vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1     oplocks
              continuously-available
```

## 验证 LIF 状态

即使您将采用 Hyper-V 和基于 SMB 的 SQL Server 配置的 Storage Virtual Machine (SVM) 配置为在集群中的每个节点上都具有 LIF，在日常操作期间，某些 LIF 也可能会移至另一节点上的端口。您必须验证 LIF 状态并采取任何必要的更正操作。

### 关于此任务

要提供无缝，无中断的操作支持，集群中的每个节点必须至少为 SVM 配置一个 LIF，并且所有 LIF 都必须与主端口关联。如果某些已配置的 LIF 当前未与其主端口关联，则必须修复任何端口问题，然后将 LIF 还原到其主端口。

### 步骤

1. 显示有关为 SVM 配置的 LIF 的信息：

```
network interface show -vservers vservers_name
```

在此示例中，"lif1" 不位于主端口上。

```
network interface show -vservers vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
vs1	lif1	up/up	10.0.0.128/24	node2	e0d
false	lif2	up/up	10.0.0.129/24	node2	e0d
true					

2. 如果某些 LIF 不在其主端口上，请执行以下步骤：

- a. 对于每个 LIF，确定 LIF 的主端口是什么：

```
network interface show -vservers vservers_name -lif lif_name -fields home-
node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

```
vserver lif  home-node  home-port
-----
vs1      lif1 node1      e0d
```

- b. 对于每个 LIF ，确定 LIF 的主端口是否已启动：

```
network port show -node node_name -port port -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

```
node      port link
-----
node1     e0d  up
```

+ 在此示例中、"lif1"应迁移回其主端口、 node1:e0d。

3. 如果应与这些IF关联的任何主端口网络接口不在中 up 请解决此问题、使这些接口正常运行。
4. 如果需要，请将 LIF 还原到其主端口：

```
network interface revert -vserver vs1 -lif lif1
```

```
network interface revert -vserver vs1 -lif lif1
```

5. 验证集群中的每个节点是否都具有适用于 SVM 的活动 LIF：

```
network interface show -vserver vs1
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	
true	lif2	up/up	10.0.0.129/24	node2	e0d	
true						



# 确定 SMB 会话是否持续可用

## 显示 SMB 会话信息

您可以显示有关已建立的 SMB 会话的信息，包括 SMB 连接和会话 ID 以及使用会话的工作站的 IP 地址。您可以显示有关会话的 SMB 协议版本和持续可用保护级别的信息，这有助于确定会话是否支持无中断操作。

### 关于此任务

您可以摘要形式显示 SVM 上所有会话的信息。但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息：

- 您可以使用可选 `-fields` 用于显示有关所选字段的输出的参数。  
  
您可以输入 `-fields ?` 以确定您可以使用哪些字段。
- 您可以使用 `-instance` 用于显示有关已建立SMB会话的详细信息的参数。
- 您可以使用 `-fields` 参数或 `-instance` 参数单独使用或与其他可选参数结合使用。

### 步骤

1. 执行以下操作之一：

要显示 <b>SMB</b> 会话信息的项	输入以下命令 ...
SVM 上的所有会话的摘要形式	<code>vserver cifs session show -vserver <i>vserver_name</i></code>
指定的连接 ID	<code>vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer</code>
指定的工作站 IP 地址	<code>vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i></code>
指定的 LIF IP 地址	<code>vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i></code>
在指定节点上	<code>`vserver cifs session show -vserver <i>vserver_name</i> -node {node_name</code>
<code>local}*`</code>	指定的 Windows 用户

要显示 <b>SMB</b> 会话信息的项	输入以下命令 ...
<b>vserver cifs session show -vserver vserver_name -windows-user user_name</b>  的格式 user_name 为 [domain]\user。	使用指定的身份验证机制
<b>vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism</b>  的值 -auth -mechanism 可以是以下选项之一：  <ul style="list-style-type: none"><li>• NTLMv1</li><li>• NTLMv2</li><li>• Kerberos</li><li>• Anonymous</li></ul>	使用指定的协议版本



要显示 <b>SMB</b> 会话信息的项	输入以下命令 ...
<pre> <b>vserver cifs</b> <b>session show</b> <b>-vserver</b> <b>vserver_name</b> <b>-continuously</b> <b>-available</b> <b>continuously_avail</b> <b>able_protection_le</b> <b>vel</b> </pre> <p>           的值 <code>-continuously</code>  <code>-available</code> 可以是以下选项之一：         </p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> <li>• Partial</li> </ul> <div>  <p>             持续可用状态为 Partial，这意味着会话至少包含一个打开的持续可用文件，但会话中的某些文件未使用持续可用保护打开。您可以使用 <code>vserver cifs session s file show</code> 命令、用于确定已建立会话中哪些文件未在持续可用的保护下打开。           </p> </div>	具有指定的 SMB 签名会话状态

## 示例

以下命令显示 SVM vs1 上从 IP 地址为 10.1.1.1 的工作站建立的会话的会话信息：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

以下命令显示 SVM vs1 上具有持续可用保护的会话的详细会话信息。此连接是使用域帐户建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

以下命令显示 SVM vs1 上使用 SMB 3.0 和 SMB 多通道的会话的会话信息。在此示例中，用户使用 LIF IP 地址从支持 SMB 3.0 的客户端连接到此共享；因此，身份验证机制默认为 NTLMv2。必须使用 Kerberos 身份验证进行连接，以获得持续可用的保护。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```

        Node: node1
        Vserver: vs1
        Session ID: 1
        **Connection IDs: 3151272607,31512726078,3151272609
        Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
        Workstation IP address: 10.1.1.3
        Authentication Mechanism: NTLMv2
        Windows User: DOMAIN\administrator
        UNIX User: pcuser
        Open Shares: 1
        Open Files: 0
        Open Other: 0
        Connected Time: 6m 22s
        Idle Time: 5m 42s
        Protocol Version: SMB3
        Continuously Available: No
        Is Session Signed: false
        User Authenticated as: domain-user
        NetBIOS Name: -
        SMB Encryption Status: Unencrypted
```

## 显示有关打开的 **SMB** 文件的信息

您可以显示有关打开的 SMB 文件的信息，包括 SMB 连接和会话 ID，托管卷，共享名称和共享路径。您还可以显示有关文件的持续可用保护级别的信息，这有助于确定打开的文件是否处于支持无中断操作的状态。

### 关于此任务

您可以显示有关已建立的 SMB 会话上打开的文件的信息。如果需要确定 SMB 会话中特定文件的 SMB 会话信息，则显示的信息非常有用。

例如、如果您有一个SMB会话、其中一些打开的文件已打开且具有持续可用的保护、而另一些文件未打开且具有持续可用的保护(的值 `-continuously-available` 字段输入 `vserver cifs session show` 命令输出为 `Partial`)、则可以使用此命令确定哪些文件不持续可用。

您可以使用以摘要形式显示Storage Virtual Machine (SVM)上已建立的SMB会话上的所有打开文件的信息 `vserver cifs session file show` 命令、而不带任何可选参数。

但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息。如果您只想查看一小部分打开文件的信息，这将非常有用。

- 您可以使用可选 `-fields` 用于显示所选字段的输出的参数。

您可以单独使用此参数，也可以与其他可选参数结合使用。

- 您可以使用 `-instance` 用于显示有关打开的SMB文件的详细信息的参数。

您可以单独使用此参数，也可以与其他可选参数结合使用。

## 步骤

1. 执行以下操作之一：

如果要显示打开的 <b>SMB</b> 文件 ...	输入以下命令 ...
以摘要形式显示在 SVM 上	<b>vserver cifs session file show -vserver vserver_name</b>
在指定节点上	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*`</code>	指定的文件 ID
<b>vserver cifs session file show -vserver vserver_name -file-id integer</b>	指定的 SMB 连接 ID
<b>vserver cifs session file show -vserver vserver_name -connection-id integer</b>	指定的 SMB 会话 ID
<b>vserver cifs session file show -vserver vserver_name -session-id integer</b>	在指定的托管聚合上
<b>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</b>	在指定卷上
<b>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</b>	指定的 SMB 共享上
<b>vserver cifs session file show -vserver vserver_name -share share_name</b>	指定的 SMB 路径上
<b>vserver cifs session file show -vserver vserver_name -path path</b>	具有指定级别的持续可用保护

如果要显示打开的 <b>SMB</b> 文件 ...	输入以下命令 ...
<pre><b>vserver cifs session file show</b> <b>-vserver vserver_name -continuously</b> <b>-available</b> <b>continuously_available_status</b></pre> <p>的值 <code>-continuously-available</code> 可以是以下选项之一：</p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <div>  <p>持续可用状态为 No，这意味着这些打开的文件无法从接管和恢复中无系统地恢复。它们也无法从高可用性关系中的合作伙伴之间的常规聚合重新定位中恢复。</p> </div>	具有指定的重新连接状态

您可以使用其他可选参数来细化输出结果。有关详细信息，请参见手册页。

## 示例

以下示例显示了有关 SVM vs1 上打开的文件的信息：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:    1
File      File      Open Hosting      Continuously
ID        Type      Mode Volume      Share      Available
-----
41        Regular    r      data      data      Yes
Path: \mytest.rtf
```

以下示例显示了有关 SVM vs1 上文件 ID 82 的已打开 SMB 文件的详细信息：



```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance
```

```
        Node: node1
        Vserver: vs1
        File ID: 82
    Connection ID: 104617
        Session ID: 1
        File Type: Regular
        Open Mode: rw
Aggregate Hosting File: aggr1
    Volume Hosting File: data1
        CIFS Share: data1
    Path from CIFS Share: windows\win8\test\test.txt
        Share Mode: rw
        Range Locks: 1
Continuously Available: Yes
        Reconnected: No
```

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。