



## 监控 **SMB** 活动 ONTAP 9

NetApp  
April 24, 2024

# 目录

- 监控 SMB 活动 ..... 1
  - 显示 SMB 会话信息 ..... 1
  - 显示有关打开的 SMB 文件的信息 ..... 4
  - 确定可用的统计信息对象和计数器 ..... 7
  - 显示统计信息 ..... 10

# 监控 SMB 活动

## 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 vserver_name</code>
指定的连接 ID	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
指定的工作站 IP 地址	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
指定的 LIF IP 地址	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
在指定节点上	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
local}`	指定的 Windows 用户

要显示 <b>SMB</b> 会话信息的项	输入以下命令 ...
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	使用指定的身份验证机制
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
使用指定的协议版本	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 持续可用的保护和 SMB 多通道仅适用于 SMB 3.0 及更高版本的会话。要查看其在所有符合条件的会话中的状态、应指定此参数并将值设置为 SMB3 或更高版本。  ====
具有指定级别的持续可用保护	<code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code>
Yes	Partial}`  [NOTE] ==== 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 sessions 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。  ====
具有指定的 SMB 签名会话状态	<code>`vserver cifs session show -vserver vserver_name -is-session-signed {true</code>

## 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
```

## 相关信息

[显示有关打开的 SMB 文件的信息](#)

# 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	<code>vserver cifs session file show -vserver vserver_name</code>
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
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	指定的 SMB 连接 ID
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	指定的 SMB 会话 ID
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	在指定的托管聚合上
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	在指定卷上
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	指定的 SMB 共享上
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	指定的 SMB 路径上
<code>vserver cifs session file show -vserver vserver_name -path path</code>	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 ...
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	<p>Yes}`</p> <p>[NOTE] ==== 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> <p>====</p>
具有指定的重新连接状态	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

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::> vsriver cifs session file show -vsriver 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
```

#### 相关信息

[显示 SMB 会话信息](#)

## 确定可用的统计信息对象和计数器

在获取有关 CIFS，SMB，审核和 BranchCache 哈希统计信息以及监控性能的信息之前，您必须了解哪些对象和计数器可用于获取数据。

#### 步骤

1. 将权限级别设置为高级：set -privilege advanced
2. 执行以下操作之一：

要确定的内容	输入 ...
哪些对象可用	statistics catalog object show
可用的特定对象	statistics catalog object show object object_name
哪些计数器可用	statistics catalog counter show object object_name

有关哪些对象和计数器可用的详细信息，请参见手册页。

3. 返回到管理权限级别：set -privilege admin

## 示例

以下命令显示与集群中的 CIFS 和 SMB 访问相关的选定统计信息对象的说明，如高级权限级别所示：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                    The CIFS object reports activity of the
                           Common Internet File System protocol
                           ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs             The Common Internet File System (CIFS)
                           protocol is an implementation of the
Server
                           ...

cluster1::*> statistics catalog object show -object smb1
    smb1                    These counters report activity from the
SMB                           revision of the protocol. For information
                           ...

cluster1::*> statistics catalog object show -object smb2
    smb2                    These counters report activity from the
                           SMB2/SMB3 revision of the protocol. For
                           ...

cluster1::*> statistics catalog object show -object hashd
    hashd                   The hashd object provides counters to
measure                        the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

以下命令显示有关的某些计数器的信息 `cifs` 对象、如高级权限级别所示：



此示例不会显示的所有可用计数器 `cifs` 对象；输出被截断。

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

相关信息

[显示统计信息](#)

# 显示统计信息

您可以显示各种统计信息，包括有关 CIFS 和 SMB ， 审核和 BranchCache 哈希的统计信息， 以监控性能并诊断问题。

## 开始之前

您必须已使用收集数据样本 `statistics start` 和 `statistics stop` 命令、 然后才能显示有关对象的信息。

## 步骤

- 1. 将权限级别设置为高级： `set -privilege advanced`
- 2. 执行以下操作之一：

要显示统计信息的对象	输入 ...
SMB 的所有版本	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x 和 SMB 3.0	<code>statistics show -object smb2</code>
节点的 CIFS 子系统	<code>statistics show -object nblade_cifs</code>
多协议审核	<code>statistics show -object audit_ng</code>
BranchCache 哈希服务	<code>statistics show -object hashd</code>
动态 DNS	<code>statistics show -object ddns_update</code>

有关详细信息，请参见每个命令的手册页。

- 3. 返回到管理权限级别： `set -privilege admin`

## 相关信息

[确定可用的统计信息对象和计数器](#)

[监控 SMB 签名会话统计信息](#)

[显示 BranchCache 统计信息](#)

[使用统计信息监控自动节点转介活动](#)

["Microsoft Hyper-V 和 SQL Server 的 SMB 配置"](#)

["性能监控设置"](#)

## 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。