



使用 **SMB** 签名增强网络安全性

ONTAP 9

NetApp
February 12, 2026

目录

使用 SMB 签名增强网络安全性	1
了解如何使用ONTAP SMB签名增强网络安全性	1
了解签名策略如何影响与ONTAP SMB服务器的通信	1
了解ONTAP SMB签名的性能影响	2
ONTAP SMB签名配置建议	3
了解适用于多个数据ONTAP的SMB签名配置	3
为传入的ONTAP流量配置SMB签名	4
确定ONTAP SMB会话是否已签名	5
监控ONTAP SMB签名会话统计信息	6

使用 SMB 签名增强网络安全性

了解如何使用 ONTAP SMB 签名增强网络安全性

SMB 签名有助于确保 SMB 服务器和客户端之间的网络流量不会受到影响；它可以通过防止重放攻击来实现这一点。默认情况下，当客户端请求 SMB 签名时，ONTAP 支持 SMB 签名。或者，存储管理员可以将 SMB 服务器配置为需要 SMB 签名。

了解签名策略如何影响与 ONTAP SMB 服务器的通信

除了 CIFS 服务器 SMB 签名安全设置之外，Windows 客户端上的两个 SMB 签名策略还控制客户端与 CIFS 服务器之间通信的数字签名。您可以配置满足业务要求的设置。

客户端 SMB 策略通过 Windows 本地安全策略设置进行控制，这些设置通过使用 Microsoft 管理控制台（MMC）或 Active Directory GPO 进行配置。有关客户端 SMB 签名和安全问题的详细信息，请参见 Microsoft Windows 文档。

下面介绍了 Microsoft 客户端上的两个 SMB 签名策略：

- Microsoft network client: Digitally sign communications (if server agrees)

此设置控制是否启用客户端的 SMB 签名功能。默认情况下，此选项处于启用状态。如果在客户端上禁用此设置，则客户端与 CIFS 服务器的通信取决于 CIFS 服务器上的 SMB 签名设置。

- Microsoft network client: Digitally sign communications (always)

此设置控制客户端是否需要 SMB 签名才能与服务器进行通信。默认情况下，此选项处于禁用状态。如果在客户端上禁用此设置、则 SMB 签名行为取决于的策略设置 Microsoft network client: Digitally sign communications (if server agrees) 和 CIFS 服务器上的设置。



如果您的环境包含配置为需要 SMB 签名的 Windows 客户端，则必须在 CIFS 服务器上启用 SMB 签名。否则，CIFS 服务器将无法为这些系统提供数据。

客户端和 CIFS 服务器 SMB 签名设置的有效结果取决于 SMB 会话是使用 SMB 1.0 还是 SMB 2.x 及更高版本。

下表总结了会话使用 SMB 1.0 时有有效的 SMB 签名行为：

客户端	不需要 ONTAP 签名	需要 ONTAP 签名
已禁用且不需要签名	未签名	已签名
已启用签名，但不需要签名	未签名	已签名
签名已禁用且为必填项	已签名	已签名
已启用且需要签名	已签名	已签名



如果在客户端上禁用了签名，但在 CIFS 服务器上需要签名，则较早的 Windows SMB 1 客户端和某些非 Windows SMB 1 客户端可能无法连接。

下表总结了会话使用 SMB 2.x 或 SMB 3.0 时有有效的 SMB 签名行为：



对于 SMB 2.x 和 SMB 3.0 客户端，SMB 签名始终处于启用状态。不能将其禁用。

客户端	不需要 ONTAP 签名	需要 ONTAP 签名
不需要签名	未签名	已签名
需要签名	已签名	已签名

下表总结了默认的 Microsoft 客户端和服务器的 SMB 签名行为：

协议	哈希算法	可以启用 / 禁用	可能需要 / 不需要	客户端默认值	服务器默认值	DC 默认值
SMB 1.0	MD5	是的。	是的。	已启用（不需要）	已禁用（不需要）	Required
SMB 2.x	HMAC SHA-256	否	是的。	不需要	不需要	Required
SMB 3.0	AES-CMAC	否	是的。	不需要	不需要	Required



Microsoft 不再建议使用 Digitally sign communications (if client agrees) 或 Digitally sign communications (if server agrees) 组策略设置。Microsoft 也不再建议使用 EnableSecuritySignature 注册表设置。这些选项仅影响 SMB 1 行为、可以替换为 Digitally sign communications (always) 组策略设置或 RequireSecuritySignature 注册表设置。您还可以从 Microsoft 博客中获取更多信息。<http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>[The 签名基础知识(涵盖 SMB1 和 SMB2)]

了解 ONTAP SMB 签名的性能影响

当 SMB 会话使用 SMB 签名时，与 Windows 客户端之间的所有 SMB 通信都会受到性能影响，从而影响客户端和服务器的（即运行包含 SMB 服务器的 SVM 的集群上的节点）。

性能影响显示为客户端和服务器的 CPU 利用率增加，但网络流量不会改变。

性能影响的程度取决于所运行的 ONTAP 9 版本。从 ONTAP 9.7 开始，新的非负载加密算法可以提高签名 SMB 流量的性能。如果启用了 SMB 签名，则默认情况下会启用 SMB 签名卸载。

要提高 SMB 签名性能，需要 AES-NI 卸载功能。请参见 Hardware Universe（HWU）以验证您的平台是否支持 AES-NI 卸载。

如果您能够使用SMB版本3.11、该版本支持更快的GCM算法、则性能也可能进一步提高。

根据您的网络，ONTAP 9 版本，SMB 版本和 SVM 实施情况，SMB 签名对性能的影响可能差别很大；您只能通过在网络环境中进行测试来验证它。

如果在服务器上启用了 SMB 签名，则大多数 Windows 客户端默认协商 SMB 签名。如果您需要为某些 Windows 客户端提供 SMB 保护，并且 SMB 签名导致性能问题，则可以在任何不需要防止重放攻击的 Windows 客户端上禁用 SMB 签名。有关在 Windows 客户端上禁用 SMB 签名的信息，请参见 Microsoft Windows 文档。

ONTAP SMB签名配置建议

您可以在 SMB 客户端和 CIFS 服务器之间配置 SMB 签名行为，以满足您的安全要求。在 CIFS 服务器上配置 SMB 签名时选择的设置取决于您的安全要求。

您可以在客户端或 CIFS 服务器上配置 SMB 签名。配置 SMB 签名时，请考虑以下建议：

条件	建议
您希望提高客户端与服务器之间通信的安全性	通过启用、在客户端上设置所需的SMB签名 Require Option (Sign always) 客户端上的安全设置。
您希望对特定 Storage Virtual Machine (SVM) 的所有 SMB 流量进行签名	通过将安全设置配置为需要 SMB 签名，在 CIFS 服务器上设置需要 SMB 签名。

有关配置 Windows 客户端安全设置的详细信息，请参见 Microsoft 文档。

了解适用于多个数据ONTAP的SMB签名配置

如果在 SMB 服务器上启用或禁用所需的 SMB 签名，则应了解 SVM 的多个数据 LIF 配置的准则。

配置 SMB 服务器时，可能会配置多个数据 LIF。如果是、则DNS服务器包含多个 A 记录CIFS服务器的条目、所有条目都使用相同的SMB服务器主机名、但每个条目都具有唯一的IP地址。例如、配置了两个数据生命周期的SMB服务器可能具有以下DNS A 记录条目：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

正常情况下，更改所需的 SMB 签名设置后，只有来自客户端的新连接才会受到 SMB 签名设置更改的影响。但是，此行为存在例外情况。在某些情况下，客户端已与共享建立连接，并且客户端会在更改此设置后创建与同一共享的新连接，同时保持原始连接。在这种情况下，新的和现有的 SMB 连接都采用新的 SMB 签名要求。

请考虑以下示例：

1. 客户端1使用路径连接到共享、而不需要SMB签名 o:\。

2. 存储管理员将 SMB 服务器配置修改为需要 SMB 签名。
3. 客户端1使用路径连接到具有所需SMB签名的同一共享 s:\ (同时使用路径保持连接 o:\) 。
4. 这样、在通过这两个访问数据时、将使用SMB签名 o:\ 和 s:\ 驱动器。

为传入的ONTAP流量配置SMB签名

您可以通过启用所需的 SMB 签名来强制实施客户端对 SMB 消息签名的要求。如果启用，则 ONTAP 仅在 SMB 消息具有有效签名时才接受这些消息。如果要允许 SMB 签名，但不需要它，可以禁用所需的 SMB 签名。

关于此任务

默认情况下，所需的 SMB 签名处于禁用状态。您可以随时启用或禁用所需的 SMB 签名。

在以下情况下，默认情况下不会禁用 SMB 签名：



1. 已启用所需的 SMB 签名，并且集群将还原到不支持 SMB 签名的 ONTAP 版本。
2. 集群随后升级到支持 SMB 签名的 ONTAP 版本。

在这些情况下，最初在受支持的 ONTAP 版本上配置的 SMB 签名配置将通过还原和后续升级保留。

在设置Storage Virtual Machine (SVM)灾难恢复关系时、是为选择的值 `-identity-preserve` 的选项 `snappmirror create` 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 `-identity-preserve` 选项 `true` (ID保留)、则SMB签名安全设置将复制到目标。

如果您设置了 `-identity-preserve` 选项 `false` (非ID保留)、则SMB签名安全设置不会复制到目标。在这种情况下，目标上的 CIFS 服务器安全设置将设置为默认值。如果已在源 SVM 上启用所需的 SMB 签名，则必须在目标 SVM 上手动启用所需的 SMB 签名。

步骤

1. 执行以下操作之一：

所需的 SMB 签名状态	输入命令 ...
enabled	<pre>vserver cifs security modify -vserver vserver_name -is-signing-required true</pre>
已禁用	<pre>vserver cifs security modify -vserver vserver_name -is-signing-required false</pre>

2. 通过确定中的值来验证是否已启用或禁用所需的SMB签名 Is Signing Required 字段设置为所需值：
`vserver cifs security show -vserver vserver_name -fields is-signing-required`

示例

以下示例将为 SVM vs1 启用所需的 SMB 签名：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----  -----
vs1      true
```



对加密设置所做的更改将对新连接生效。现有连接不受影响。

相关信息

- ["SnapMirror 创建"](#)

确定ONTAP SMB会话是否已签名

您可以显示有关 CIFS 服务器上已连接的 SMB 会话的信息。您可以使用此信息确定 SMB 会话是否已签名。这有助于确定 SMB 客户端会话是否使用所需的安全设置进行连接。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
指定 Storage Virtual Machine (SVM) 上的所有已签名会话	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>
SVM 上具有特定会话 ID 的已签名会话的详细信息	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>

示例

以下命令显示 SVM vs1 上已签名会话的会话信息。默认摘要输出不会显示 "Is Session Signed" 输出字段：

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

以下命令显示会话 ID 为 2 的 SMB 会话的详细会话信息，包括会话是否已签名：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
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: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

相关信息

[监控 SMB 签名会话统计信息](#)

监控ONTAP SMB签名会话统计信息

您可以监控 SMB 会话统计信息，并确定哪些已建立的会话已签名，哪些未签名。

关于此任务

。 `statistics` 命令可在高级权限级别提供 `signed_sessions` 可用于监控已签名SMB会话数的计数器。。
`signed_sessions` 计数器可用于以下统计信息对象：

- `cifs` 用于监控所有SMB会话的SMB签名。
- `smb1` 用于监控SMB 1.0会话的SMB签名。
- `smb2` 用于监控SMB 2.x和SMB 3.0会话的SMB签名。

SMB 3.0统计信息包括在的输出中 `smb2` 对象。

如果要已将签名会话数与会话总数进行比较、可以比较的输出 `signed_sessions` 计数器与的输出 `established_sessions` 计数器。

您必须先启动统计信息样本收集，然后才能查看生成的数据。如果不停止数据收集，您可以查看样本中的数据。停止数据收集可提供一个固定样本。如果不停止数据收集，则可以获取更新后的数据，以便与先前的查询进行比较。此比较可帮助您确定趋势。

步骤

1. 将权限级别设置为高级：`+ set -privilege advanced`
2. 开始数据收集：`+ statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

如果未指定 `-sample-id` 参数时、该命令将为您生成示例标识符、并将此示例定义为命令行界面会话的默认示例。的值 `-sample-id` 是文本字符串。如果您在同一命令行界面会话期间运行此命令、但未指定 `-sample-id` 参数、则此命令将覆盖先前的默认样本。

您也可以指定要收集统计信息的节点。如果未指定节点，则此示例将收集集群中所有节点的统计信息。

有关的详细信息 `statistics start`，请参见"[ONTAP 命令参考](#)"。

3. 使用 `statistics stop` 命令停止收集样本数据。

详细了解 `statistics stop` 在"[ONTAP 命令参考](#)"。

4. 查看 SMB 签名统计信息：

要查看的信息	输入 ...
已签名的会话	<code>`show -sample-id <i>sample_ID</i> -counter signed_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	已签名的会话和已建立的会话
<code>`show -sample-id <i>sample_ID</i> -counter signed_sessions</code>	<code>established_sessions</code>

如果要仅显示单个节点的信息、请指定可选 `-node` 参数。

有关的详细信息 `statistics show`，请参见"[ONTAP 命令参考](#)"。

5. 返回到管理权限级别：`+ set -privilege admin`

示例

以下示例显示了如何监控 Storage Virtual Machine (SVM) vs1 上的 SMB 2.x 和 SMB 3.0 签名统计信息。

以下命令将移至高级权限级别：

```
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
```

以下命令将开始收集新样本的数据：

```
cluster1::*> statistics start -object smb2 -sample-id smbSigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbSigning_sample
```

以下命令将停止收集样本的数据：

```
cluster1::*> statistics stop -sample-id smbSigning_sample
Statistics collection is being stopped for Sample-id: smbSigning_sample
```

以下命令按示例中的节点显示已签名的 SMB 会话和已建立的 SMB 会话：

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1
```

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

以下命令显示样本中 node2 的已签名 SMB 会话:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1
```

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

以下命令将移回管理权限级别:

```
cluster1::*> set -privilege admin
```

相关信息

- [确定 SMB 会话是否已签名](#)
- ["性能监控和管理概述"](#)

版权信息

版权所有 © 2026 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。