在 SMB 服务器上配置通过 SMB 传输数据所需的 SMB 加密

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/smb-admin/configure-required-encryption-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目录

在 SMB 服务器上配置通过 SMB 传输数据所需的 SMB 加密

SMB加密概述

通过 SMB 进行数据传输的 SMB 加密是一种安全增强功能，您可以在 SMB 服务器上启用或禁用此功能。您还可以通过共享属性设置在共享基础上配置所需的 SMB 加密设置。

默认情况下、在Storage Virtual Machine (SVM)上创建SMB服务器时、SMB加密处于禁用状态。您必须启用 SMB 加密才能利用 SMB 加密提供的增强安全性。

要创建加密的 SMB 会话， SMB 客户端必须支持 SMB 加密。从 Windows Server 2012 和 Windows 8 开始的 Windows 客户端支持 SMB 加密。

SVM 上的 SMB 加密通过两种设置控制：

- 在SVM上启用此功能的SMB服务器安全选项
- 一种SMB共享属性、用于基于共享配置SMB加密设置

您可以决定是要求加密才能访问 SVM 上的所有数据，还是要求 SMB 加密才能仅访问选定共享中的数据。SVM 级别的设置将取代共享级别的设置。

有效的 SMB 加密配置取决于这两种设置的组合，下表对此进行了介绍：

已启用 **SMB** 服务器 **SMB** 加密	已启用共享加密数据设置	服务器端加密行为
true	false	已为 SVM 中的所有共享启用服务器级别加密。使用此配置时，整个 SMB 会话都会进行加密。
true	true	无论共享级别加密如何， SVM 中的所有共享都会启用服务器级别加密。使用此配置时，整个 SMB 会话都会进行加密。
false	true	已为特定共享启用共享级别加密。使用此配置时，会从树连接进行加密。
false	false	未启用加密。

不支持加密的SMB客户端无法连接到需要加密的SMB服务器或共享。

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。

SMB 加密对性能的影响

当 SMB 会话使用 SMB 加密时，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（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上的 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，新的加密负载下算法可以提高加密 SMB 流量的性能。如果启用了 SMB 加密，则默认情况下会启用 SMB 加密卸载。

增强的 SMB 加密性能需要 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 加密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。

SMB 服务器默认禁用 SMB 加密。您应仅在需要加密的 SMB 共享或 SMB 服务器上启用 SMB 加密。通过 SMB 加密， ONTAP 可以对请求进行解密，并对每个请求的响应进行加密。因此，只有在必要时才应启用 SMB 加密。

为传入的 SMB 流量启用或禁用所需的 SMB 加密

如果您希望为传入的 SMB 流量要求 SMB 加密，可以在 CIFS 服务器或共享级别启用它。默认情况下，不需要 SMB 加密。

关于此任务

您可以在 CIFS 服务器上启用 SMB 加密，该服务器会对 CIFS 服务器上的所有共享进行适用场景。如果您不希望 CIFS 服务器上的所有共享都需要 SMB 加密，或者您希望为基于共享的传入 SMB 流量启用所需的 SMB 加密，则可以在 CIFS 服务器上禁用所需的 SMB 加密。

在设置Storage Virtual Machine (SVM)灾难恢复关系时、您为选择的值 `-identity-preserve` 的选项 `snapmirror 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加密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加密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 SMB 加密，则必须在目标上手动启用 CIFS 服务器 SMB 加密。

步骤

1. 执行以下操作之一：

CIFS 服务器上传入的 **SMB** 流量所需的 **SMB** 加密	输入命令 **...**
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`

CIFS 服务器上传入的 SMB 流量所需的 SMB 加密	输入命令 ...
已禁用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. 验证是否已根据需要在CIFS服务器上启用或禁用所需的SMB加密： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 字段 `true` 如果需要、可在CIFS服务器和上启用SMB加密 `false` 如果已禁用。

示例

以下示例将为 SVM vs1 上的 CIFS 服务器的传入 SMB 流量启用所需的 SMB 加密：

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

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

确定客户端是否使用加密的 SMB 会话进行连接

您可以显示有关已连接 SMB 会话的信息，以确定客户端是否正在使用加密的 SMB 连接。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。

关于此任务

SMB 客户端会话可以具有以下三种加密级别之一：

- `unencrypted`

  SMB 会话未加密。未配置 Storage Virtual Machine （ SVM ）级别或共享级别的加密。

- `partially-encrypted`

  发生树连接时会启动加密。已配置共享级别加密。未启用 SVM 级别的加密。

- `encrypted`

  SMB 会话已完全加密。已启用 SVM 级别的加密。可能已启用，也可能未启用共享级别加密。SVM 级别的加密设置将取代共享级别的加密设置。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
具有指定 SVM 上会话的指定加密设置的会话	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定 SVM 上特定会话 ID 的加密设置	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

示例

以下命令显示会话 ID 为 2 的 SMB 会话的详细会话信息，包括加密设置：

```
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
```

监控 SMB 加密统计信息

您可以监控 SMB 加密统计信息，并确定哪些已建立的会话和共享连接已加密，哪些未加密。

关于此任务

- `statistics` 高级权限级别的命令提供了以下计数器、您可以使用这些计数器监控加密的SMB会话和共享连

接的数量：

计数器名称	说明
encrypted_sessions	提供加密的 SMB 3.0 会话的数量
encrypted_share_connections	提供发生树连接的加密共享的数量
rejected_unencrypted_sessions	提供因缺少客户端加密功能而拒绝的会话设置数量
rejected_unencrypted_shares	提供因缺少客户端加密功能而拒绝的共享映射的数量

这些计数器可用于以下统计信息对象：

- cifs 用于监控所有SMB 3.0会话的SMB加密。

  SMB 3.0统计信息包括在的输出中 cifs 对象。 如果要将加密会话数与会话总数进行比较、可以比较的输出 encrypted_sessions 计数器与的输出 established_sessions 计数器。

  如果要将加密共享连接数与共享连接总数进行比较、则可以比较的输出 encrypted_share_connections 计数器与的输出 connected_shares 计数器。

- rejected_unencrypted_sessions 提供尝试建立需要从不支持SMB加密的客户端加密的SMB会话的次数。
- rejected_unencrypted_shares 提供尝试连接到需要从不支持SMB加密的客户端加密的SMB共享的次数。

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。

3. 使用 statistics stop 命令停止收集样本数据。
4. 查看 SMB 加密统计信息：

要查看的信息	输入 ...
加密会话	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	已加密会话和已建立的会话
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	加密的共享连接
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
加密的共享连接和连接的共享	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒绝的未加密会话	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒绝未加密的共享连接
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

如果要仅显示单个节点的信息、请指定可选 `-node` 参数。

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 3.0 加密统计信息。

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 cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

以下命令将停止收集该样本的数据：

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

以下命令显示样本中节点的加密 SMB 会话和已建立的 SMB 会话：

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                Value
    ----------------------------  -----------------------
    established_sessions                      1
    encrypted_sessions                        1

2 entries were displayed
```

以下命令显示样本中节点拒绝的未加密 SMB 会话的数量：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

以下命令显示样本中节点的已连接 SMB 共享和加密 SMB 共享的数量：

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                      Value
    ----------------------------    ----------------------
    connected_shares                               2
    encrypted_share_connections                    1

2 entries were displayed.
```

以下命令显示样本中节点拒绝的未加密 SMB 共享连接的数量：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

相关信息

确定可用的统计信息对象和计数器

"性能监控和管理概述"

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。