配置对SVM的SMB访问

ONTAP 9

NetApp
April 24, 2024

目录

配置对SVM的SMB访问

配置对SVM的SMB访问

如果尚未为 SMB 客户端访问配置 SVM ，则必须创建并配置新的 SVM 或配置现有 SVM 。配置 SMB 包括打开 SVM 根卷访问，创建 SMB 服务器，创建 LIF ，启用主机名解析，配置名称服务，如果需要， 启用 Kerberos 安全性。

创建 SVM：

如果集群中还没有至少一个SVM来为SMB客户端提供数据访问、则必须创建一个SVM。

开始之前

- 从ONTAP 9.13.1开始、您可以为Storage VM设置最大容量。您还可以在SVM接近阈值容量级别时配置警报。有关详细信息，请参见 管理SVM容量。

步骤

1. 创建 SVM： `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - 对使用NTFS设置 `-rootvolume-security-style` 选项
   - 使用默认C.UTF-8 `-language` 选项
   - 。 `ipspace` 设置是可选的。
2. 验证新创建的 SVM 的配置和状态： `vserver show -vserver` *`vserver_name`*

   。 `Allowed Protocols` 字段必须包含CIFS。您可以稍后编辑此列表。

   。 `Vserver Operational State` 字段必须显示 `running` 状态。如果显示 `initializing` 状态、表示某些中间操作(如创建根卷)失败、您必须删除SVM并重新创建它。

示例

以下命令将在IP空间中创建用于数据访问的SVM `ipspaceA`：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

以下命令显示已创建根卷为1 GB的SVM、并且此SVM已自动启动并位于中 `running` 状态。根卷具有一个默认导出策略，该策略不包含任何规则，因此根卷在创建时不会导出。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
                Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                               IPspace Name: ipspaceA
```

> 从ONTAP 9.13.1开始、您可以设置自适应QoS策略组模板、以便为SVM中的卷应用吞吐量下限和上限限制。只有在创建SVM之后、才能应用此策略。要了解有关此过程的更多信息、请参见 设置自适应策略组模板。

验证是否已在SVM上启用SMB协议

要在SVM上配置和使用SMB、必须先验证协议是否已启用。

关于此任务

此操作通常在SVM设置期间完成、但如果您在设置期间未启用此协议、则可以稍后使用启用它 `vserver add-protocols` 命令：

> 创建 LIF 后，您不能在该 LIF 中添加或删除协议。

您还可以使用在SVM上禁用协议 `vserver remove-protocols` 命令：

步骤

1. 检查 SVM 当前已启用和禁用的协议： `vserver show -vserver vserver_name -protocols`

您也可以使用 `vserver show-protocols` 命令以查看集群中所有SVM上当前已启用的协议。

2. 如有必要，启用或禁用协议：
   - 启用SMB协议： `vserver add-protocols -vserver vserver_name -protocols cifs`
   - 禁用协议： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. 确认已启用和禁用的协议已正确更新： `vserver show -vserver vserver_name -protocols`

示例

以下命令显示 SVM vs1 上当前已启用和禁用（允许和不允许）的协议：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

以下命令可通过添加来允许通过SMB进行访问 `cifs` 到SVM VS1上已启用的协议列表：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

打开 SVM 根卷的导出策略

SVM根卷的默认导出策略必须包含一条规则、以允许所有客户端通过SMB进行公开访问。如果没有此规则、则会拒绝所有SMB客户端访问SVM及其卷。

关于此任务

创建新的 SVM 时，系统会自动为 SVM 的根卷创建默认导出策略（称为 default ）。您必须为默认导出策略创建一个或多个规则，客户端才能访问 SVM 上的数据。

您应验证是否已在默认导出策略中打开所有 SMB 访问，然后通过为单个卷或 qtree 创建自定义导出策略来限制对单个卷的访问。

步骤

1. 如果您使用的是现有 SVM ，请检查默认根卷导出策略： `vserver export-policy rule show`

   命令输出应类似于以下内容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: any
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

如果存在允许开放访问的规则，则此任务将完成。如果没有，请继续执行下一步。

2. 为 SVM 根卷创建导出规则： `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. 使用验证规则创建 `vserver export-policy rule show` 命令：

结果

现在、任何SMB客户端均可访问在SVM上创建的任何卷或qtree。

创建 LIF

LIF 是指与物理或逻辑端口关联的 IP 地址。如果组件出现故障，则 LIF 可以故障转移到或迁移到其他物理端口，从而继续与网络通信。

开始之前

- 底层物理或逻辑网络端口必须已配置为管理端口 `up` 状态。
- 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，则此子网必须已存在。

  子网包含属于同一第 3 层子网的 IP 地址池。它们是使用创建的 `network subnet create` 命令：

- 用于指定 LIF 处理的流量类型的机制已发生更改。对于 ONTAP 9.5 及更早版本， LIF 使用角色指定要处理的流量类型。从 ONTAP 9.6 开始， LIF 使用服务策略指定要处理的流量类型。

关于此任务

- 您可以在同一网络端口上创建 IPv4 和 IPv6 LIF 。
- 如果集群中有大量LIF、则可以使用验证集群上支持的LIF容量 `network interface capacity show` 命令以及每个节点上支持的LIF容量 `network interface capacity details show` 命令(在高级权限级别)。

- 从 ONTAP 9.7 开始，如果同一子网中已存在 SVM 的其他 LIF ，则无需指定 LIF 的主端口。ONTAP 会自动在与已在同一子网中配置的其他 LIF 位于同一广播域的指定主节点上选择一个随机端口。

步骤

1. 创建 LIF：

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol cifs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

* ONTAP 9.5 及更早版本 *
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

* ONTAP 9.6 及更高版本 *
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - 。 `-role` 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。
   - 。 `-data-protocol` 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。使用ONTAP 9.5及更早版本时、 `-data-protocol` 必须在创建LIF时指定参数、如果不销毁并重新创建数据LIF、则以后无法修改此参数。
   - `-home-node` 是LIF返回到的节点 `network interface revert` 命令将在LIF上运行。

     您还可以使用指定LIF是否应自动还原到主节点和主端口 `-auto-revert` 选项
   - `-home-port` 是LIF返回到的物理或逻辑端口 `network interface revert` 命令将在LIF上运行。
   - 您可以使用指定IP地址 `-address` 和 `-netmask` 选项、或者使用启用从子网分配 `-subnet_name` 选项
   - 使用子网提供 IP 地址和网络掩码时，如果使用网关定义了子网，则在使用该子网创建 LIF 时，系统会自动向 SVM 添加指向该网关的默认路由。
   - 如果您手动分配 IP 地址（而不使用子网），则在其他 IP 子网上存在客户端或域控制器时，可能需要配置指向网关的默认路由。。 `network route create` 手册页包含有关在SVM中创建静态路由的信息。
   - 。 `-firewall-policy` 选项中、使用相同的默认值 `data` 作为LIF角色。

     如果需要，您可以稍后创建和添加自定义防火墙策略。

> 从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 "为 LIF 配置防火墙策略"。

- `-auto-revert` 用于指定在启动、更改管理数据库状态或建立网络连接等情况下、数据LIF是否自动还原到其主节点。默认设置为 `false`，但您可以将其设置为 `false` 具体取决于您环境中的网络管理策略。

2. 验证是否已成功创建 LIF ：

```
network interface show
```

3. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

示例

以下命令将使用创建LIF并指定IP地址和网络掩码值 `-address` 和 `-netmask` 参数：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

以下命令将创建一个 LIF ，并从指定子网（名为 client1_sub ）分配 IP 地址和网络掩码值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

以下命令显示 cluster-1 中的所有 LIF 。数据 LIF datalif1 和 datalif3 配置了 IPv4 地址，而 datalif4 配置了 IPv6 地址：

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

以下命令显示如何创建分配给的NAS数据LIF `default-data-files` 服务策略：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

启用 DNS 以进行主机名解析

您可以使用 `vserver services name-service dns` 命令以在SVM上启用DNS、并将其配置为使用DNS进行主机名解析。主机名可使用外部 DNS 服务器进行解析。

开始之前

站点范围的 DNS 服务器必须可用于主机名查找。

您应配置多个 DNS 服务器，以避免单点故障。。 `vserver services name-service dns create` 如果仅输入一个DNS服务器名称、则命令会发出警告。

关于此任务

网络管理指南 _ 包含有关在 SVM 上配置动态 DNS 的信息。

步骤

1. 在 SVM 上启用 DNS： `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   以下命令将在 SVM vs1 上启用外部 DNS 服务器：

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > 从ONTAP 9.2开始、 `vserver services name-service dns create` 命令会执行自动配置验证、如果ONTAP无法联系到名称服务器、则会报告错误消息。

2. 使用显示DNS域配置 `vserver services name-service dns show` 命令：``

   以下命令显示集群中所有 SVM 的 DNS 配置：

   ```
   vserver services name-service dns show
                                                  Name
   Vserver           State     Domains              Servers
   ----------------- --------- -------------------- -------------
   cluster1          enabled   example.com          192.0.2.201,
                                                    192.0.2.202
   vs1.example.com   enabled   example.com          192.0.2.201,
                                                    192.0.2.202
   ```

   以下命令显示 SVM vs1 的详细 DNS 配置信息：

   ```
   vserver services name-service dns show -vserver vs1.example.com
                  Vserver: vs1.example.com
                  Domains: example.com
             Name Servers: 192.0.2.201, 192.0.2.202
       Enable/Disable DNS: enabled
           Timeout (secs): 2
         Maximum Attempts: 1
   ```

3. 使用验证名称服务器的状态 `vserver services name-service dns check` 命令：

   - `vserver services name-service dns check` 命令从ONTAP 9.2开始可用。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

在 Active Directory 域中设置 SMB 服务器

配置时间服务

在 Active Domain 控制器中创建 SMB 服务器之前，您必须确保集群时间和 SMB 服务器所属域的域控制器上的时间在五分钟内匹配。

关于此任务

您应将集群 NTP 服务配置为使用与 Active Directory 域相同的 NTP 服务器进行时间同步。

从 ONTAP 9.5 开始，您可以使用对称身份验证设置 NTP 服务器。

步骤

1. 使用配置时间服务 `cluster time-service ntp server create` 命令：
   - 要配置不采用对称身份验证的时间服务、请输入以下命令： `cluster time-service ntp server create -server server_ip_address`
   - 要使用对称身份验证配置时间服务、请输入以下命令： `cluster time-service ntp server create -server server_ip_address -key-id key_id` `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`
2. 使用验证是否已正确设置时间服务 `cluster time-service ntp server show` 命令：

```
cluster time-service ntp server show
```

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

用于在 **NTP** 服务器上管理对称身份验证的命令

从 ONTAP 9.5 开始，支持网络时间协议（ NTP ）版本 3 。NTPv3 包括使用 SHA-1 密钥的对称身份验证，可提高网络安全性。

要执行此操作 ...	使用此命令 ...
配置不使用对称身份验证的 NTP 服务器	`cluster time-service ntp server create -server server_name`
使用对称身份验证配置 NTP 服务器	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
为现有 NTP 服务器启用对称身份验证可以通过添加所需的密钥 ID 来修改现有 NTP 服务器以启用身份验证。	`cluster time-service ntp server modify -server server_name -key-id key_id`
配置共享 NTP 密钥	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共享密钥由 ID 引用。节点和 NTP 服务器上的 ID ，类型和值必须相同
使用未知密钥 ID 配置 NTP 服务器	`cluster time-service ntp server create -server server_name -key-id key_id`
使用未在 NTP 服务器上配置的密钥 ID 配置服务器。	`cluster time-service ntp server create -server server_name -key-id key_id` 密钥 ID ，类型和值必须与 NTP 服务器上配置的密钥 ID ，类型和值相同。
禁用对称身份验证	`cluster time-service ntp server modify -server server_name -authentication disabled`

在 **Active Directory** 域中创建 **SMB** 服务器

您可以使用 `vserver cifs create` 命令以在SVM上创建SMB服务器并指定其所属的Active Directory (AD)域。

开始之前

您用于提供数据的 SVM 和 LIF 必须已配置为允许 SMB 协议。LIF 必须能够连接到 SVM 上配置的 DNS 服务器以及要加入 SMB 服务器的域的 AD 域控制器。

任何有权在 SMB 服务器要加入的 AD 域中创建计算机帐户的用户都可以在 SVM 上创建 SMB 服务器。这可能包括来自其他域的用户。

从 ONTAP 9.7 开始，您的 AD 管理员可以为您提供 keytab 文件的 URI ，而不是为您提供特权 Windows 帐户的名称和密码。收到此URI后、请将其包含在中 `-keytab-uri` 参数 `vserver cifs` 命令

关于此任务

在 Active Directory 域中创建 SMB 服务器时：

- 指定域时，必须使用完全限定域名（ FQDN ）。
- 默认设置是将 SMB 服务器计算机帐户添加到 Active Directory CN=Computer 对象。
- 您可以选择使用将SMB服务器添加到其他组织单位(OU) `-ou` 选项
- 您也可以选择为 SMB 服务器添加一个或多个 NetBIOS 别名（最多 200 个）的逗号分隔列表。

  如果要将其他文件服务器中的数据整合到 SMB 服务器并希望 SMB 服务器响应原始服务器的名称，则为 SMB 服务器配置 NetBIOS 别名非常有用。

。 `vserver cifs` 手册页包含其他可选参数和命名要求。

> 从 ONTAP 9.1 开始，您可以启用 SMB 版本 2.0 以连接到域控制器（ DC ）。如果已在域控制器上禁用 SMB 1.0 ，则必须执行此操作。从 ONTAP 9.2 开始， SMB 2.0 默认处于启用状态。

从 ONTAP 9.8 开始，您可以指定对与域控制器的连接进行加密。当时、ONTAP需要对域控制器通信进行加密 `-encryption-required-for-dc-connection` 选项设置为 `true`；默认值为 `false`。如果设置了此选项，则只有 SMB3 协议将用于 ONONTAP DC 连接，因为只有 SMB3 才支持加密。。

"SMB管理" 包含有关 SMB 服务器配置选项的详细信息。

步骤

1. 验证集群上的SMB是否已获得许可： `system license show -package cifs`

   SMB许可证包含在中 "ONTAP One"。如果您没有ONTAP One、并且未安装许可证、请联系您的销售代表。

   如果 SMB 服务器仅用于身份验证，则不需要 CIFS 许可证。

2. 在AD域中创建SMB服务器： `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   加入域时，此命令可能需要几分钟才能完成。

   以下命令会在域 “example.com”: 中创建 SMB 服务器 " `sMB_server01` "

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

以下命令会在域 `mydomain.com`" 中创建 `SMB` 服务器 `sMB_server02`，并使用 keytab 文件对 ONTAP 管理员进行身份验证：

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. 使用验证SMB服务器配置 `vserver cifs show` 命令：

   在此示例中，命令输出显示已在 SVM vs1.example.com 上创建名为 `SMB_server01` 的 SMB 服务器，并加入 “example.com” 域。

```
cluster1::> vserver cifs show -vserver vs1

                                            Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. 如果需要、请启用与域控制器的加密通信(ONTAP 9.8及更高版本)： `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

示例

以下命令会在 SVM vs2.example.com 上的 “example.com” 域中创建一个名为 `sMB_server02` 的 SMB 服务器。计算机帐户在 "`OU=eng， OU=corp， DC=example， DC=com`" 容器中创建。SMB 服务器分配有 NetBIOS 别名。

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

以下命令允许来自其他域的用户（此处为受信任域的管理员）在 SVM vs3.example.com 上创建名为 `sMB_server03` 的 SMB 服务器。。 `-domain` 选项用于指定要在其中创建SMB服务器的主域的名称(在DNS配置中指定)。。 `username` 选项指定受信任域的管理员。

- 主域： example.com
- 受信任域： trust.lab.com
- 受信任域的用户名： Administrator1.

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

创建用于 **SMB** 身份验证的 **keytab** 文件

从 ONTAP 9.7 开始， ONTAP 支持使用 keytab 文件对 Active Directory （ AD ）服务器进行 SVM 身份验证。AD管理员生成一个keytab文件、并将其作为统一资源标识符(URI)提供给ONTAP管理员 `vserver cifs` 命令要求对AD域进行Kerberos身份验证。

AD管理员可以使用标准Windows Server创建keytab文件 `ktpass` 命令：此命令应在需要进行身份验证的主域上运行。。 `ktpass` 命令只能用于为主域用户生成keytab文件；不支持使用受信任域用户生成的密钥。

系统会为特定 ONTAP 管理员用户生成 keytab 文件。只要管理员用户的密码不更改，为特定加密类型和域生成的密钥就不会更改。因此，每当更改管理员用户的密码时，都需要一个新的 keytab 文件。

支持以下加密类型：

- ES256-SHA1

- DES-CBC-MD5

> ONTAP 不支持 DES-CBC-CRC 加密类型。

- RC4-HMAC

AES256 是最高的加密类型，如果在 ONTAP 系统上启用，则应使用此类型。

可以通过指定管理员密码或使用随机生成的密码来生成 keytab 文件。但是，在任何给定时间，只能使用一个密码选项，因为在 AD 服务器上需要管理员用户专用的专用密钥来解密 keytab 文件中的密钥。对特定管理员的私钥进行任何更改都会使 keytab 文件失效。

在工作组中设置 SMB 服务器

在工作组概述中设置 SMB 服务器

将 SMB 服务器设置为工作组的成员包括创建 SMB 服务器，然后创建本地用户和组。

当 Microsoft Active Directory 域基础架构不可用时，您可以在工作组中配置 SMB 服务器。

工作组模式下的 SMB 服务器仅支持 NTLM 身份验证，不支持 Kerberos 身份验证。

在工作组中创建 SMB 服务器

您可以使用 `vserver cifs create` 命令以在SVM上创建SMB服务器并指定其所属的工作组。

开始之前

您用于提供数据的 SVM 和 LIF 必须已配置为允许 SMB 协议。LIF 必须能够连接到 SVM 上配置的 DNS 服务器。

关于此任务

工作组模式下的 SMB 服务器不支持以下 SMB 功能：

- SMB3 见证协议
- SMB3 CA 共享
- 基于 SMB 的 SQL
- 文件夹重定向
- 漫游配置文件
- 组策略对象（GPO）
- 卷快照服务（VSS）

。 `vserver cifs` 手册页包含其他可选配置参数和命名要求。

步骤

1. 验证集群上的SMB是否已获得许可： `system license show -package cifs`

SMB许可证包含在中 "ONTAP One"。如果您没有ONTAP One、并且未安装许可证、请联系您的销售代表。

如果 SMB 服务器仅用于身份验证，则不需要 CIFS 许可证。

2. 在工作组中创建SMB服务器： `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   以下命令会在工作组 "`workgroup01` " 中创建 SMB 服务器 " `sMB_server01` "：

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. 使用验证SMB服务器配置 `vserver cifs show` 命令：

   在以下示例中，命令输出显示已在工作组 "`workgroup01` " 的 SVM vs1.example.com 上创建名为 `sMB_server01` 的 SMB 服务器：

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
   ```

完成后

对于工作组中的 CIFS 服务器，您必须在 SVM 上创建本地用户以及可选的本地组。

相关信息

"SMB管理"

创建本地用户帐户

您可以创建本地用户帐户，该帐户可用于授权通过 SMB 连接访问 SVM 中包含的数据。创建 SMB 会话时，您还可以使用本地用户帐户进行身份验证。

关于此任务

默认情况下，创建 SVM 时会启用本地用户功能。

创建本地用户帐户时，必须指定用户名，并且必须指定要与该帐户关联的 SVM 。

。 `vserver cifs users-and-groups local-user` 手册页包含有关可选参数和命名要求的详细信息。

步骤

1. 创建本地用户： `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   以下可选参数可能有用：

   - `-full-name`

     用户的全名。

   - `-description`

     本地用户的问题描述。

   - `-is-account-disabled {true|false}`

     指定用户帐户是启用还是禁用。如果未指定此参数，则默认为启用用户帐户。

   命令将提示输入本地用户的密码。

2. 输入本地用户的密码，然后确认该密码。
3. 验证是否已成功创建此用户： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将创建一个与 SVM vs1.example.com 关联的本地用户 " `SMB_server01\sue` " ，其全名为 " `Sue Chang` " ：

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- -------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator            Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

创建本地组

您可以创建本地组，用于授权通过 SMB 连接访问与 SVM 关联的数据。您还可以分配权限，以定义组成员的用户权限或功能。

关于此任务

创建 SVM 时，默认情况下会启用本地组功能。

创建本地组时，必须为该组指定一个名称，并且必须指定要与该组关联的 SVM 。您可以指定包含或不包含本地域名的组名称，也可以选择为本地组指定问题描述。您不能将本地组添加到其他本地组。

。 `vserver cifs users-and-groups local-group` 手册页包含有关可选参数和命名要求的详细信息。

步骤

1. 创建本地组： `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   以下可选参数可能很有用：

   - `-description`

     本地组的问题描述。

2. 验证是否已成功创建此组： `vserver cifs users-and-groups local-group show -vserver vserver_name`

示例

以下示例将创建一个与 SVM vs1 关联的本地组 `SMB_server01\engineering`：

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

完成后

您必须向新组添加成员。

管理本地组成员资格

您可以通过添加和删除本地或域用户，或者添加和删除域组来管理本地组成员资格。如果您希望根据对组的访问控制来控制对数据的访问，或者您希望用户拥有与该组关联的权限，则此功能非常有用。

关于此任务

如果您不再希望本地用户，域用户或域组具有基于组成员资格的访问权限，则可以从组中删除此成员。

向本地组添加成员时，必须牢记以下几点：

- 您不能将用户添加到特殊的 _Everyone 组。
- 您不能将本地组添加到其他本地组。
- 要将域用户或组添加到本地组， ONTAP 必须能够将此名称解析为 SID 。

从本地组中删除成员时，必须牢记以下几点：

- 您不能从特殊的 _Everyone _ 组中删除成员。
- 要从本地组中删除成员， ONTAP 必须能够将其名称解析为 SID 。

步骤

1. 向组添加成员或从组中删除成员。
   - 添加成员： `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     您可以指定要添加到指定本地组的本地用户，域用户或域组的逗号分隔列表。

   - 删除成员： `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     您可以指定要从指定本地组中删除的本地用户，域用户或域组的逗号分隔列表。

示例

以下示例将本地用户 `SMB_server01\sue` 添加到 SVM vs1.example.com 上的本地组 `SMB_server01\engineering`：

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

以下示例将从 SVM vs1.example.com 上的本地组 `Smb_server01\engineering` 中删除本地用户 `Smb_server01\sue` 和 `Smb_server01\james`：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

验证已启用的 SMB 版本

ONTAP 9 版本可确定默认情况下为与客户端和域控制器的连接启用的 SMB 版本。您应验证 SMB 服务器是否支持环境中所需的客户端和功能。

关于此任务

对于与客户端和域控制器的连接，应尽可能启用 SMB 2.0 及更高版本。出于安全原因，您应避免使用 SMB 1.0 ，如果您已确认环境中不需要 SMB 1.0 ，则应将其禁用。

在 ONTAP 9 中，默认情况下会为客户端连接启用 SMB 2.0 及更高版本，但默认启用的 SMB 1.0 版本取决于您的 ONTAP 版本。

- 从 ONTAP 9.1 P8 开始，可以在 SVM 上禁用 SMB 1.0 。
  - `-smb1-enabled` 选项 `vserver cifs options modify` 命令用于启用或禁用SMB 1.0。
- 从 ONTAP 9.3 开始，默认情况下会在新 SVM 上禁用此功能。

如果 SMB 服务器位于 Active Directory （ AD ）域中，则可以从 ONTAP 9.1 开始启用 SMB 2.0 以连接到域控制器（ DC ）。如果在 DC 上禁用了 SMB 1.0 ，则必须执行此操作。从 ONTAP 9.2 开始，默认情况下会为 DC 连接启用 SMB 2.0 。

> 条件 `-smb1-enabled-for-dc-connections` 设置为 `false` 同时 `-smb1-enabled` 设置为 `true`，ONTAP拒绝将SMB 1.0连接作为客户端，但继续接受入站SMB 1.0连接作为服务器。

"SMB管理" 包含有关支持的 SMB 版本和功能的详细信息。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 验证启用了哪些SMB版本：

   ```
   vserver cifs options show
   ```

   您可以向下滚动列表以查看为客户端连接启用的 SMB 版本，如果要在 AD 域中配置 SMB 服务器，则可以查看为 AD 域连接启用的 SMB 版本。

3. 根据需要为客户端连接启用或禁用 SMB 协议：

- 启用SMB版本：

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- 禁用SMB版本：

```
vserver cifs options modify -vserver vserver_name smb_version false
```

的可能值 `smb_version`：

  - `-smb1-enabled`
  - `-smb2-enabled`
  - `-smb3-enabled`
  - `-smb31-enabled`

以下命令将在SVM vs1.example.com上启用SMB 3.1：

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
-enabled true
```

1. 如果 SMB 服务器位于 Active Directory 域中，请根据需要为 DC 连接启用或禁用 SMB 协议：
   - 启用SMB版本：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for
-dc-connections true
```

   - 禁用SMB版本：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for
-dc-connections false
```

2. 返回到管理权限级别：

```
set -privilege admin
```

在 DNS 服务器上映射 SMB 服务器

您站点的 DNS 服务器必须具有一个条目，用于将 SMB 服务器名称和任何 NetBIOS 别名

指向数据 LIF 的 IP 地址，以便 Windows 用户可以将驱动器映射到 SMB 服务器名称。

开始之前

您必须对站点的 DNS 服务器具有管理访问权限。如果您没有管理访问权限，则必须要求 DNS 管理员执行此任务。

关于此任务

如果您对 SMB 服务器名称使用 NetBIOS 别名，则最好为每个别名创建 DNS 服务器入口点。

步骤

1. 登录到 DNS 服务器。
2. 创建正向（A - 地址记录）和反向（PTR - 指针记录）查找条目，将 SMB 服务器名称映射到数据 LIF 的 IP 地址。
3. 如果使用 NetBIOS 别名，请创建一个别名规范名称（CNAME 资源记录）查找条目，以便将每个别名映射到 SMB 服务器的数据 LIF 的 IP 地址。

结果

映射在网络中传播之后， Windows 用户可以将驱动器映射到 SMB 服务器名称或其 NetBIOS 别名。