



# 在 **Active Directory** 域中设置 **SMB** 服务器 ONTAP 9

NetApp  
April 24, 2024

# 目录

- 在 Active Directory 域中设置 SMB 服务器 ..... 1
  - 配置时间服务 ..... 1
  - 用于在 NTP 服务器上管理对称身份验证的命令 ..... 1
  - 在 Active Directory 域中创建 SMB 服务器 ..... 2
  - 创建用于 SMB 身份验证的 keytab 文件 ..... 5

# 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	<code>cluster time-service ntp server create -server server_name</code>
使用对称身份验证配置 NTP 服务器	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>

要执行此操作 ...	使用此命令 ...
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。	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
配置共享 NTP 密钥	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>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</p> </div>
使用未知密钥 ID 配置 NTP 服务器	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
使用未在 NTP 服务器上配置的密钥 ID 配置服务器。	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>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。</p> </div>
禁用对称身份验证	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

## 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。

## 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。