使用 LDAP

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/nfs-config/using-ldap-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目录

使用 LDAP

LDAP 使用概述

如果在您的环境中使用 LDAP 提供名称服务，则需要与 LDAP 管理员一起确定要求和适当的存储系统配置，然后将 SVM 作为 LDAP 客户端启用。

从 ONTAP 9.10.1 开始，默认情况下， Active Directory 和名称服务 LDAP 连接均支持 LDAP 通道绑定。只有在启用了 Start-TLS 或 LDAPS 且会话安全设置为 sign 或 seal 的情况下， ONTAP 才会尝试使用 LDAP 连接进行通道绑定。要禁用或重新启用与名称服务器的LDAP通道绑定、请使用 `-try-channel-binding` 参数 `ldap client modify` 命令：

有关详细信息，请参见 "2020 年 Windows 的 LDAP 通道绑定和 LDAP 签名要求"。

- 在为 ONTAP 配置 LDAP 之前，您应验证站点部署是否符合 LDAP 服务器和客户端配置的最佳实践。具体而言，必须满足以下条件：
  - LDAP 服务器的域名必须与 LDAP 客户端上的条目匹配。
  - LDAP 服务器支持的 LDAP 用户密码哈希类型必须包括 ONTAP 支持的类型：
    - 加密（所有类型）和 SHA-1 （ SHA ， SSHA ）。
    - 从 ONTAP 9.8 开始， SHA-2 哈希（ SHA-256 ， SSH/384 ， SHA-512 ， SSHA-256 ， SSHA-384 和 SSHA-512 ）。
  - 如果 LDAP 服务器需要会话安全措施，则必须在 LDAP 客户端中配置这些措施。

    可以使用以下会话安全选项：
    - LDAP 签名（提供数据完整性检查）和 LDAP 签名和签章（提供数据完整性检查和加密）
    - START TLS
    - LDAPS （基于 TLS 或 SSL 的 LDAP ）
  - 要启用签名和签章的 LDAP 查询，必须配置以下服务：
    - LDAP 服务器必须支持 GSSAPI （ Kerberos ） SASL 机制。
    - LDAP 服务器必须在 DNS 服务器上设置 DNS A/AAAA 记录以及 PTR 记录。
    - Kerberos 服务器必须在 DNS 服务器上存在 SRV 记录。
  - 要启用启动 TLS 或 LDAPS ，应考虑以下几点。
    - NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。
    - 如果使用 LDAPS ，则必须在 ONTAP 9.5 及更高版本中为 TLS 或 SSL 启用 LDAP 服务器。ONTAP 9.09.4 不支持 SSL 。
    - 必须已在域中配置证书服务器。
  - 要启用 LDAP 转介跟踪（在 ONTAP 9.5 及更高版本中），必须满足以下条件：
    - 这两个域都应配置以下信任关系之一：
      - 双向

    - 单向，主站点信任转介域
    - 父 - 子
  - 必须配置 DNS 以解析所有转介的服务器名称。
  - 当 -bind-as-cifs-server 设置为 true 时，域密码应相同以进行身份验证。

> LDAP 转介跟踪不支持以下配置。
>
> - 对于所有 ONTAP 版本：
> - 管理 SVM 上的 LDAP 客户端
> - 对于 ONTAP 9.8 及更早版本（ 9.9.1 及更高版本支持这些功能）：
> - LDAP签名和签章(`-session-security` 选项)
> - 加密TLS连接(`-use-start-tls` 选项)
> - 通过LAPS端口636 (`-use-ldaps-for-ad-ldap` 选项)

- 在 SVM 上配置 LDAP 客户端时，必须输入 LDAP 模式。

  在大多数情况下，默认 ONTAP 模式之一是合适的。但是，如果环境中的 LDAP 模式与这些模式不同，则必须在创建 LDAP 客户端之前为 ONTAP 创建新的 LDAP 客户端模式。有关您的环境要求，请咨询 LDAP 管理员。

- 不支持使用 LDAP 进行主机名解析。

有关详细信息 ...

- "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"
- "在 SVM 上安装自签名根 CA 证书"

创建新的 LDAP 客户端模式

如果环境中的 LDAP 模式与 ONTAP 默认值不同，则必须在创建 LDAP 客户端配置之前为 ONTAP 创建新的 LDAP 客户端模式。

关于此任务

大多数 LDAP 服务器都可以使用 ONTAP 提供的默认模式：

- MS-AD-BIS （大多数 Windows 2012 及更高版本 AD 服务器的首选架构）
- AD-IDMU （ Windows 2008 ， Windows 2012 及更高版本的 AD 服务器）
- AD-SFU （ Windows 2003 及更早版本的 AD 服务器）
- RFC-2307 （ UNIX LDAP 服务器）

如果需要使用非默认 LDAP 模式，则必须在创建 LDAP 客户端配置之前创建该模式。在创建新模式之前，请咨询 LDAP 管理员。

无法修改 ONTAP 提供的默认 LDAP 模式。要创建新模式，请创建一个副本，然后相应地修改该副本。

步骤

1. 显示现有 LDAP 客户端模式模板以确定要复制的模板：

   ```
   vserver services name-service ldap client schema show
   ```

2. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

3. 为现有 LDAP 客户端模式创建副本：

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. 修改新架构并根据您的环境对其进行自定义：

   ```
   vserver services name-service ldap client schema modify
   ```

5. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

创建 LDAP 客户端配置

如果您希望ONTAP访问您环境中的外部LDAP或Active Directory服务、则需要先在存储系统上设置LDAP客户端。

您需要的内容

Active Directory域解析列表中前三个服务器之一必须已启动并提供数据。否则，此任务将失败。

> 有多个服务器、其中在任意时间点有两个以上的服务器停机。

步骤

1. 请咨询LDAP管理员以确定的适当配置值 `vserver services name-service ldap client create` 命令：

   a. 指定与 LDAP 服务器的基于域或基于地址的连接。

      - `-ad-domain` 和 `-servers` 选项不能同时使用。

        - 使用 `-ad-domain` 选项以在Active Directory域中启用LDAP服务器发现。

          - 您可以使用 `-restrict-discovery-to-site` 用于将LDAP服务器发现限制为指定域的CIFS默认站点的选项。如果使用此选项、则还需要使用指定CIFS默认站点 `-default-site`。

        - 您可以使用 `-preferred-ad-servers` 此选项可按IP地址在逗号分隔列表中指定一个或多个首选Active Directory服务器。创建客户端后、您可以使用修改此列表 `vserver services name-service ldap client modify` 命令：

        - 使用 `-servers` 可选择通过IP地址在逗号分隔列表中指定一个或多个LDAP服务器(Active Directory

或UNIX)。

> 。 `-servers` 选项在ONTAP 9.2中已弃用。从ONTAP 9.2开始、 `-ldap-servers` 字段将取代 `-servers` 字段。此字段可以使用LDAP服务器的主机名或IP地址。

b. 指定默认或自定义 LDAP 模式。

大多数 LDAP 服务器都可以使用 ONTAP 提供的默认只读模式。除非另有要求，否则最好使用这些默认模式。如果是，您可以通过复制默认模式（默认模式为只读）并修改副本来创建自己的模式。

默认模式：

- MS-AD-BIS

  此模式基于 RFC-2307bis ，是大多数标准 Windows 2012 及更高版本 LDAP 部署的首选 LDAP 模式。

- `AD-IDMU`

  此模式基于适用于 UNIX 的 Active Directory 身份管理，适用于大多数 Windows 2008 ， Windows 2012 及更高版本的 AD 服务器。

- `AD-SFU`

  此模式基于适用于 UNIX 的 Active Directory 服务，适用于大多数 Windows 2003 及更早版本的 AD 服务器。

- `RFC-2307`

  根据 RFC-2307 （使用 LDAP 作为网络信息服务的方法 _ ），此模式适用于大多数 UNIX AD 服务器。

c. 选择绑定值。

- `-min-bind-level {anonymous|simple|sasl}` 指定最低绑定身份验证级别。

  默认值为 **`anonymous`**。

- `-bind-dn` *`LDAP_DN`* 指定绑定用户。

  对于 Active Directory 服务器，您必须在帐户（域 \ 用户）或主体（ user@domain.com ）表单中指定用户。否则，您必须以可分辨名称（ CN=user ， DC=domain ， DC=com ）形式指定用户。

- `-bind-password` *`password`* 指定绑定密码。

d. 如果需要，选择会话安全选项。

如果 LDAP 服务器需要，您可以启用 LDAP 签名和签章或基于 TLS 的 LDAP 。

- `--session-security {none|sign|seal}`

  您可以启用签名 (`sign`、数据完整性)、签名和签章 (`seal``数据完整性和加密)、或者两者都不是 `none`，无签名或签章)。默认值为 `none`。

您还应设置 `-min-bind-level {sasl}`，除非您希望绑定身份验证回退到 **anonymous** 或 **simple** 签名和签章绑定失败时。

- `-use-start-tls {true|false}`

  如果设置为 **true** 如果LDAP服务器支持此功能、则LDAP客户端将使用加密TLS连接连接到该服务器。默认值为 **false**。要使用此选项，您必须安装 LDAP 服务器的自签名根 CA 证书。

> 如果Storage VM已将SMB服务器添加到域中、并且LDAP服务器是SMB服务器主域的域控制器之一、则可以修改 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

e. 选择端口，查询和基本值。

建议使用默认值，但您必须向 LDAP 管理员确认这些值适合您的环境。

- `-port port` 指定LDAP服务器端口。

  默认值为 `389`。

如果您计划使用 Start TLS 来保护 LDAP 连接，则必须使用默认端口 389 。启动 TLS 以 LDAP 默认端口 389 上的纯文本连接开头，然后该连接升级到 TLS 。如果更改此端口，则启动 TLS 将失败。

- `-query-timeout integer` 指定查询超时(以秒为单位)。

  允许的范围为 1 到 10 秒。默认值为 `3` 秒。

- `-base-dn LDAP_DN` 指定基础DN。

  如果需要，可以输入多个值（例如，如果启用了 LDAP 转介跟踪）。默认值为 `""` (root)。

- `-base-scope {base|onelevel|subtree}`指定基本搜索范围。

  默认值为 `subtree`。

- `-referral-enabled {true|false}`指定是否启用LDAP转介跟踪。

  从 ONTAP 9.5 开始，如果主 LDAP 服务器返回 LDAP 转介响应，指示转介的 LDAP 服务器上存在所需记录，则 ONTAP LDAP 客户端可以将查找请求转介给其他 LDAP 服务器。默认值为 **false**。

要搜索转介 LDAP 服务器中的记录，必须在 LDAP 客户端配置中将转介记录的基础 DN 添加到基础 DN 中。

2. 在Storage VM上创建LDAP客户端配置：

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

创建LDAP客户端配置时、必须提供Storage VM名称。

3. 验证是否已成功创建 LDAP 客户端配置：

```
vserver services name-service ldap client show -client-config
client_config_name
```

示例

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与适用于LDAP的Active Directory服务器配合使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与需要签名和签章的LDAP的Active Directory服务器配合使用、并且LDAP服务器发现仅限于指定域的特定站点：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与需要LDAP转介跟踪的LDAP Active Directory服务器配合使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

以下命令通过指定基础DN来修改Storage VM VS1的LDAP客户端配置ldap1：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

以下命令通过启用转介跟踪来修改Storage VM VS1的LDAP客户端配置ldap1：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

将 LDAP 客户端配置与 SVM 关联

要在SVM上启用LDAP、必须使用 `vserver services name-service ldap create` 命令将LDAP客户端配置与SVM关联。

您需要的内容

- LDAP 域必须已存在于网络中，并且必须可供 SVM 所在的集群访问。
- SVM 上必须存在 LDAP 客户端配置。

步骤

1. 在SVM上启用LDAP：

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > 从ONTAP 9.2开始、 `vserver services name-service ldap create` 命令会执行自动配置验证、并在ONTAP无法联系名称服务器时报告错误消息。

   以下命令将在 vs1" SVM 上启用 LDAP ，并将其配置为使用 "ldap1" LDAP 客户端配置：

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. 使用 vserver services name-service ldap check 命令验证名称服务器的状态。

   以下命令将验证 SVM vs1. 上的 LDAP 服务器。

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                |
   | Client Configuration Name: c1                               |
   | LDAP Status: up                                             |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                              |
   ```

   从 ONTAP 9.2 开始，可以使用 name service check 命令。

在名称服务切换表中验证 LDAP 源

您必须验证 SVM 的名称服务切换表中是否正确列出了名称服务的 LDAP 源。

步骤

1. 显示当前名称服务切换表内容：

   `vserver services name-service ns-switch show -vserver` *`svm_name`*

   以下命令显示 SVM My_SVM 的结果：

   ```
   ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                   Source
   Vserver         Database        Order
   --------------- ------------    ---------
   My_SVM          hosts           files,
                                   dns
   My_SVM          group           files,ldap
   My_SVM          passwd          files,ldap
   My_SVM          netgroup        files
   My_SVM          namemap         files
   5 entries were displayed.
   ```

   `namemap` 指定要搜索名称映射信息的源及其顺序。在纯 UNIX 环境中，不需要此条目。只有同时使用 UNIX 和 Windows 的混合环境才需要名称映射。

2. 更新 `ns-switch` 根据需要输入：

要更新 **ns-switch** 条目的项	输入命令 **...**
用户信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database passwd -sources ldap,files`
组信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database group -sources ldap,files`
网络组信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`

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。