使用 LDAP

ONTAP 9

NetApp
April 24, 2024

目录

使用 LDAP

LDAP 概述

通过 LDAP （轻型目录访问协议）服务器，您可以集中维护用户信息。如果您将用户数据库存储在环境中的 LDAP 服务器上，则可以将存储系统配置为在现有 LDAP 数据库中查找用户信息。

- 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。
    - 在进行身份验证时、域密码应相同 `--bind-as-cifs-server` 设置为true。

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)

- 从ONTAP 9.11.1开始、您可以使用 "用于nsswitch身份验证的LDAP快速绑定。"
- 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。

对于追加信息，请参见 "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"。

LDAP 签名和签章概念

从 ONTAP 9 开始，您可以配置签名和签章，以便对 Active Directory （ AD ）服务器的查询启用 LDAP 会话安全性。您必须将Storage Virtual Machine (SVM)上的NFS服务器安全设置配置为与LDAP服务器上的安全设置相对应。

签名可使用密钥技术确认 LDAP 有效负载数据的完整性。密封功能对 LDAP 有效负载数据进行加密，以避免以明文形式传输敏感信息。"_LDAP 安全级别 _ " 选项指示 LDAP 流量是需要签名，签名和签章，还是两者都不需要。默认值为 `none`。测试

已使用在SVM上启用SMB流量的LDAP签名和签章 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

LDAPS 概念

您必须了解有关 ONTAP 如何确保 LDAP 通信安全的某些术语和概念。ONTAP 可以使用启动 TLS 或 LDAPS 在 Active Directory 集成的 LDAP 服务器或基于 UNIX 的 LDAP 服务器之间设置经过身份验证的会话。

术语

有关 ONTAP 如何使用 LDAPS 保护 LDAP 通信，您应了解一些特定术语。

- * LDAP *

（轻型目录访问协议）一种用于访问和管理信息目录的协议。LDAP 用作存储用户，组和网络组等对象的信息目录。LDAP 还提供目录服务，用于管理这些对象并满足 LDAP 客户端的 LDAP 请求。

- * ssl*

  （安全套接字层）一种专为通过 Internet 安全发送信息而开发的协议。ONTAP 9及更高版本支持SSL、但已弃用而改用TLS。

- * TLS *

  （传输层安全性）基于早期 SSL 规范的 IETF 标准跟踪协议。它是 SSL 的后继协议。ONTAP 9.5及更高版本支持TLS。

- * LDAPS （基于 SSL 或 TLS 的 LDAP ） *

  一种使用 TLS 或 SSL 保护 LDAP 客户端与 LDAP 服务器之间通信安全的协议。术语_LDAP over SSL_和_LDAP over TLS_有时可以互换使用。ONTAP 9.5及更高版本支持LAPS。

  - 在 ONTAP 9.2-9.8 中，只能在端口 636 上启用 LDAPS 。要执行此操作、请使用 `-use-ldaps-for-ad-ldap` 参数 `vserver cifs security modify` 命令：
  - 从 ONTAP 9.1.1 开始，可以在任何端口上启用 LDAPS ，但端口 636 仍为默认端口。为此、请设置 `-ldaps-enabled` 参数设置为 `true` 并指定所需的 `-port` 参数。有关详细信息，请参见 `vserver services name-service ldap client create` 手册页

  > NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。

- * 启动 TL*

  （也称为 *start_tls* ， *STARTTLS _* 和 *_Starttls* ）一种使用 TLS 协议提供安全通信的机制。

  ONTAP 使用 STARTTLS 保护 LDAP 通信，并使用默认 LDAP 端口（ 389 ）与 LDAP 服务器进行通信。必须将 LDAP 服务器配置为允许通过 LDAP 端口 389 进行连接；否则，从 SVM 到 LDAP 服务器的 LDAP TLS 连接将失败。

ONTAP 如何使用 LDAPS

ONTAP 支持 TLS 服务器身份验证，从而使 SVM LDAP 客户端能够在绑定操作期间确认 LDAP 服务器的身份。启用了 TLS 的 LDAP 客户端可以使用公共密钥加密的标准技术来检查服务器的证书和公有 ID 是否有效以及是否由客户端的可信 CA 列表中列出的证书颁发机构（ CA ）颁发。

LDAP 支持 STARTTLS 使用 TLS 对通信进行加密。StartTLS 以标准 LDAP 端口（ 389 ）上的纯文本连接开头，然后该连接升级到 TLS 。

ONTAP 支持以下功能：

- LDAPS 用于 Active Directory 集成的 LDAP 服务器和 SVM 之间的 SMB 相关流量
- LDAP 流量的 LDAPS ，用于名称映射和其他 UNIX 信息

  可以使用 Active Directory 集成的 LDAP 服务器或基于 UNIX 的 LDAP 服务器来存储 LDAP 名称映射的信息以及其他 UNIX 信息，例如用户，组和网络组。

- 自签名根 CA 证书

  使用 Active Directory 集成的 LDAP 时，在域中安装 Windows Server 证书服务时会生成自签名根证书。使用基于 UNIX 的 LDAP 服务器进行 LDAP 名称映射时，系统会使用适用于该 LDAP 应用程序的方法生成并保存自签名根证书。

默认情况下、LDIPS处于禁用状态。

启用 LDAP RFC2307bis 支持

如果您要使用 LDAP 并需要使用嵌套组成员资格的附加功能，则可以将 ONTAP 配置为启用 LDAP RFC2307bis 支持。

您需要的内容

您必须已为要使用的一个默认 LDAP 客户端模式创建一个副本。

关于此任务

在 LDAP 客户端模式中，组对象使用 memberUid 属性。此属性可以包含多个值，并列出属于该组的用户的名称。在启用了 RFC2307bis 的 LDAP 客户端模式中，组对象使用 uniqueMember 属性。此属性可以包含 LDAP 目录中另一个对象的完整可分辨名称（ DN ）。这样，您就可以使用嵌套组，因为组可以将其他组作为成员。

用户所属的组不应超过 256 个，包括嵌套组。ONTAP 会忽略超过 256 组限制的任何组。

默认情况下， RFC2307bis 支持处于禁用状态。

> 使用 MS-AD-BIS 模式创建 LDAP 客户端时， ONTAP 会自动启用 RFC2307bis 支持。

对于追加信息，请参见 "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 修改复制的 RFC2307 LDAP 客户端模式以启用 RFC2307bis 支持：

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. 修改模式以匹配 LDAP 服务器中支持的对象类：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. 修改模式以匹配 LDAP 服务器中支持的属性名称：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. 返回到管理权限级别：

```
set -privilege admin
```

LDAP 目录搜索的配置选项

您可以通过配置 ONTAP LDAP 客户端以最适合您的环境的方式连接到 LDAP 服务器来优化 LDAP 目录搜索，包括用户，组和网络组信息。您需要了解默认 LDAP 基础和范围搜索值何时足够，以及在自定义值更合适时需要指定哪些参数。

LDAP 客户端的用户，组和网络组信息搜索选项有助于避免 LDAP 查询失败，从而避免客户端无法访问存储系统。它们还有助于确保搜索尽可能高效，以避免客户端性能问题。

默认基础和范围搜索值

LDAP 基础是 LDAP 客户端用于执行 LDAP 查询的默认基础 DN 。所有搜索，包括用户，组和网络组搜索，均使用基础 DN 完成。如果 LDAP 目录相对较小且所有相关条目都位于同一 DN 中，则此选项适用。

如果未指定自定义基础DN、则默认值为 `root`。这意味着每个查询都会搜索整个目录。尽管这样可以最大限度地提高 LDAP 查询成功的机会，但它效率低下，并会显著降低大型 LDAP 目录的性能。

LDAP 基础范围是 LDAP 客户端用于执行 LDAP 查询的默认搜索范围。所有搜索，包括用户，组和网络组搜索，均使用基础范围完成。它将确定 LDAP 查询是仅搜索命名条目， DN 下一级的条目还是该 DN 下的整个子树。

如果未指定自定义基础范围、则默认值为 `subtree`。这意味着每个查询都会搜索 DN 下的整个子树。尽管这样可以最大限度地提高 LDAP 查询成功的机会，但它效率低下，并会显著降低大型 LDAP 目录的性能。

自定义基础和范围搜索值

您也可以为用户，组和网络组搜索指定单独的基准值和范围值。通过这种方式限制查询的搜索基础和范围可以显著提高性能，因为它会将搜索限制为 LDAP 目录的较小部分。

如果指定自定义基础值和范围值，则这些值将覆盖用户，组和网络组搜索的常规默认搜索基础和范围。用于指定自定义基础值和范围值的参数可在高级权限级别使用。

LDAP 客户端参数 …	指定自定义 …
`-base-dn`	所有 LDAP 搜索的基础 DN 如果需要，可以输入多个值（例如，如果在 ONTAP 9.5 及更高版本中启用了 LDAP 转介跟踪）。
`-base-scope`	所有 LDAP 搜索的基本范围
`-user-dn`	所有 LDAP 用户搜索的基础 DNS 此参数也适用于适用场景用户名映射搜索。
`-user-scope`	所有 LDAP 用户搜索的基本范围此参数也适用于适用场景用户名映射搜索。

`-group-dn`	所有 LDAP 组搜索的基础 DNS
`-group-scope`	所有 LDAP 组搜索的基础范围
`-netgroup-dn`	所有 LDAP 网络组搜索的基础 DNS
`-netgroup-scope`	所有 LDAP 网络组搜索的基本范围

多个自定义基础 DN 值

如果 LDAP 目录结构更复杂，则可能需要指定多个基础 DNS 来搜索 LDAP 目录的多个部分以查找某些信息。您可以为用户，组和网络组 DN 参数指定多个 DNS ，方法是使用分号（；）将其分隔开，并使用双引号（"）将整个 DN 搜索列表括起来。如果 DN 包含分号，则必须在 DN 中的分号前面添加一个转义字符（\）。

请注意，范围适用场景是为相应参数指定的整个 DNS 列表。例如，如果为用户范围指定了一个包含三个不同用户 DNS 和子树的列表，则 LDAP 用户搜索将在整个子树中搜索三个指定 DNS 中的每个 DNS 。

从 ONTAP 9.5 开始，您还可以指定 ldap_referral Chasing ，这样，如果主 LDAP 服务器未返回 LDAP 转介响应，则 ONTAP LDAP 客户端可以将查找请求转介给其他 LDAP 服务器。客户端使用该转介数据从转介数据中所述的服务器检索目标对象。要搜索转介 LDAP 服务器中的对象，可以在 LDAP 客户端配置中将转介对象的基础 DN 添加到基础 DN 中。但是、只有在启用转介跟踪(使用)后、才会查找转介对象 `-referral-enabled true` 选项)。

提高 LDAP 目录 netgroup-by-host 搜索的性能

如果 LDAP 环境配置为允许按主机搜索网络组，则可以将 ONTAP 配置为利用此功能并按主机执行网络组搜索。这样可以显著加快网络组搜索速度，并减少因网络组搜索期间出现延迟而可能导致的 NFS 客户端访问问题。

您需要的内容

LDAP目录必须包含 `netgroup.byhost` 映射。

DNS 服务器应同时包含 NFS 客户端的正向（A）和反向（PTR）查找记录。

在网络组中指定 IPv6 地址时，必须始终按照 RFC 5952 中的说明缩短和压缩每个地址。

关于此任务

NIS服务器将网络组信息存储在三个单独的映射中、这些映射称为 `netgroup`， `netgroup.byuser`，和 `netgroup.byhost`。的用途 `netgroup.byuser` 和 `netgroup.byhost` 映射用于加快网络组搜索速度。ONTAP 可以在 NIS 服务器上按主机执行网络组搜索，以缩短挂载响应时间。

默认情况下、LDAP目录不具有此类 `netgroup.byhost` 映射为NIS服务器。但是、借助第三方工具、可以导入NIS `netgroup.byhost` 映射到LDAP目录以启用按主机快速网络组搜索。如果您已将LDAP环境配置为允许按主机搜索网络组、则可以使用配置ONTAP LDAP客户端 `netgroup.byhost` 映射名称、DN和搜索范围、以加快按主机搜索网络组的速度。

通过更快地接收按主机搜索网络组的结果， ONTAP 可以在 NFS 客户端请求访问导出时更快地处理导出规则。这样可以减少因网络组搜索延迟问题而导致访问延迟的可能性。

步骤

1. 获取NIS的准确完整可分辨名称 `netgroup.byhost` 映射已导入到LDAP目录。

   映射 DN 可能因用于导入的第三方工具而异。为了获得最佳性能，应指定确切的映射 DN 。

2. 将权限级别设置为高级： `set -privilege advanced`

3. 在Storage Virtual Machine (SVM)的LDAP客户端配置中启用按主机搜索网络组： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`}启用或禁用对LDAP目录的按主机网络组搜索。默认值为 `false`。

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` 指定的可分辨名称 `netgroup.byhost` 映射到LDAP目录中。它会覆盖 netgroup-by-host 搜索的基础 DN 。如果不指定此参数，则 ONTAP 将改用基础 DN 。

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`}指定按主机搜索网络组的搜索范围。如果未指定此参数、则默认值为 `subtree`。

   如果LDAP客户端配置尚不存在、则可以在使用创建新的LDAP客户端配置时通过指定这些参数来启用按主机进行网络组搜索 `vserver services name-service ldap client create` 命令：

   > 从ONTAP 9.2开始、此字段为 `-ldap-servers` 替换字段 `-servers`。此新字段可以使用 LDAP 服务器的主机名或 IP 地址。

4. 返回到管理权限级别： `set -privilege admin`

示例

以下命令将修改名为"`ldap_corp`"的现有LDAP客户端配置、以使用启用netgroup-by主机搜索 `netgroup.byhost` 映射名为"`nisMapName="netgroup.byHost"、dc=corp、dc=ex例如、dc=com`"和默认搜索范围 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完成后

。 `netgroup.byhost` 和 `netgroup` 目录中的映射必须始终保持同步、以避免出现客户端访问问题。

相关信息

"IETF RFC 5952： IPv6 地址文本表示建议"

使用LDAP快速绑定进行nsswitch身份验证

从ONTAP 9.11.1开始、您可以利用ldap_fast bind_功能(也称为_concurrent bind_)来更快、更简单地处理客户端身份验证请求。要使用此功能、LDAP服务器必须支持快速绑定功能。

关于此任务

如果没有快速绑定、ONTAP 将使用LDAP简单绑定向LDAP服务器对管理员用户进行身份验证。使用此身份验证方法、ONTAP 会向LDAP服务器发送用户或组名称、接收存储的哈希密码、并将服务器哈希代码与本地通过用户密码生成的哈希密码进行比较。如果它们相同、则ONTAP 会授予登录权限。

借助快速绑定功能、ONTAP 仅通过安全连接向LDAP服务器发送用户凭据(用户名和密码)。然后、LDAP服务器会验证这些凭据并指示ONTAP 授予登录权限。

快速绑定的一个优势是、ONTAP 无需支持LDAP服务器支持的每个新哈希算法、因为密码哈希是由LDAP服务器执行的。

"了解如何使用快速绑定。"

您可以使用现有LDAP客户端配置进行LDAP快速绑定。但是、强烈建议为LDAP客户端配置TLS或LDAPS；否则、密码将通过线缆以纯文本形式发送。

要在ONTAP 环境中启用LDAP快速绑定、您必须满足以下要求：

- 必须在支持快速绑定的LDAP服务器上配置ONTAP 管理员用户。
- 必须在名称服务开关(nsswitch)数据库中为LDAP配置ONTAP SVM。
- 必须使用快速绑定为nsswitch身份验证配置ONTAP 管理员用户和组帐户。

步骤

1. 与LDAP管理员确认LDAP服务器支持LDAP快速绑定。
2. 确保已在LDAP服务器上配置ONTAP 管理员用户凭据。
3. 验证是否已为LDAP快速绑定正确配置管理或数据SVM。

   a. 要确认LDAP快速绑定服务器已在LDAP客户端配置中列出、请输入：

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

      "了解LDAP客户端配置。"

   b. 以确认此情况 `ldap` 是为nsswitch配置的源之一 `passwd` 数据库、输入：

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

   "了解nsswitch配置。"

4. 确保管理员用户正在使用nsswitch进行身份验证、并且已在其帐户中启用LDAP快速绑定身份验证。

   - 对于现有用户、输入 `security login modify` 并验证以下参数设置：

```
  -authentication-method nsswitch

-is-ldap-fastbind true
```

- 对于新的管理员用户、请参见 "启用LDAP或NIS帐户访问。"

显示LDAP统计信息

从 ONTAP 9.2 开始，您可以显示存储系统上 Storage Virtual Machine （SVM）的 LDAP 统计信息，以监控性能并诊断问题。

您需要的内容

- 您必须已在 SVM 上配置 LDAP 客户端。
- 您必须已确定可从中查看数据的 LDAP 对象。

步骤

1. 查看计数器对象的性能数据：

```
statistics show
```

示例

以下示例显示了对象的性能数据 `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance “vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1”

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```