

Impala配置LDAP身份认证

2018-07-17 | 0 评论 | 1,006 浏览

- [配置LDAP](#)
- [准备工作](#)
- [LDAP](#)
- [配置非SSL的LDAP](#)
- [配置proxy user](#)
- [core-site.xml](#)
- [可能出现的问题](#)
- [LDAP authentication specified, but without TLS. Passwords would go over the network in the clear](#)
- [解决办法](#)
- [User 'hue' is not authorized to delegate to 'cxy'. User delegation is disabled.](#)
- [问题描述](#)
- [解决办法](#)

配置LDAP

准备工作

安装OpenLDAP

LDAP

```
1 -enable_ldap_auth
2 -ldap_uri=ldap://cxy7.com:389
3 -ldap_bind_pattern=uid=#UID,ou=People,dc=cxy7,dc=com
```

注意ldap_bind_pattern和ldap_baseDN只能配置一个

启用 LDAP 身份验证 Impala (服务范围) [↗](#) 选中后, 启用对用户进行基于 LDAP 的身份验证。

enable_ldap_auth 已配置 LDAP 身份验证。但与 Impala daemon 通信时, Impala 客户端将不加密用户名和密码。将应用 Impala 客户端服务的 TLS/SSL 设置为 True, 以加密这些密码。显示 1 个类似的消息

LDAP URL Impala (服务范围) [↗](#) LDAP 服务器的 URL。URL 的前缀必须为 ldap:// 或 ldaps://。URL 可以随意指定一个自定义端口, 例如: ldaps://ldap_server.example.com:1636。请注意, 用户名和密码将以明文形式传输, 除非使用 ldaps:// URL 或打开“启用 LDAP TLS” (如果可用)。另请注意, 出于相同原因, 必须在客户端和此服务之间使用加密。

有关 LDAP URL 格式的详细信息, 请参见 RFC 2255 [↗](#)。可以输入以空格分隔的 URL 列表; 在此情况下, 将轮流尝试各个 URL, 直到有一个响应。

LDAP BaseDN Impala (服务范围) [↗](#) 此参数可用于对 OpenLDAP 等非 Active Directory 服务器进行身份验证。设置后, 此参数用于将用户名转换为 LDAP 可分辨名称(DN), 以便产生的 DN 类似于 uid=username,<this parameter>。例如, 如果该参数设置为 "ou=People,dc=cloudera,dc=com", 且传递进来的用户名为 "mike", 则产生的传递至 LDAP 服务器的身份验证类似于 "uid=mike,ou=People,dc=cloudera,dc=com"。此参数与 Active Directory 域相互排斥。

LDAP 模式 Impala (服务范围) [↗](#) 如已设置, 此参数允许从用户任意 mapping 到可分辨名称 (DN)。指定的字符串中必须包含名为 "#UID" 的占位符, 且该 #UID 由用户名替换。例如, 通过指定 "uid=#UID,ou=People,dc=cloudera,dc=com", 您可以模仿 LDAP BaseDN 的行为。当用户名 "mike" 传入时, 它将替换 #UID, 结果将变成 "uid=mike,ou=People,dc=cloudera,dc=com"。当需要对 DN 加强控制时, 应使用此选项。此参数与 LDAP 域和 LDAP BaseDN 相互排斥。

配置非SSL的LDAP

对于非SSL的LDAP, 还需要配置如下项

--ldap_passwords_in_clear_ok=true

Impala 命令行参数高级配置代码段 (安全网) Impala (服务范围) [↗](#) 仅限于高级用途。要添加(逐字逐句)到 Impala Daemon 命令行标志中的键/值对(每行一对)。适用于此服务中的所有角色。键名称应以连字符(-)开头。例如: -log_filename=foo.log

```
--ldap_passwords_in_clear_ok=true
```

配置proxy user

在Impala Dameon的启动参数中添加

--authorized_proxy_user_config=hue=*

core-site.xml

```
1 <property>
2 <name>hadoop.proxyuser.hue.hosts</name>
3 <value>*</value>
4 </property>
5 <property>
6 <name>hadoop.proxyuser.hue.groups</name>
7 <value>*</value>
8 </property>
```

Impala Daemon 命令行参数高级配置代码段 (安全网)

Impala Daemon Default Group

-authorized_proxy_user_config=hue=*

仅限于高级用途, 要添加(逐字逐句)到 Impala Daemon 命令行标志中的键/值对(每行一对), 键名称应以连字符(-)开头。例如:
-log_filename=foo.log

core-site.xml 的 Impala Daemon 高级配置代码段 (安全网)

Impala Daemon Default Group

以 XML 格式查看

仅限于高级用途, 将只被插入此角色的 core-site.xml 的字符串。

名称: hadoop.proxyuser.hue.hosts
值: *
说明: 说明
 最终

名称: hadoop.proxyuser.hue.groups
值: *
说明: 说明
 最终

可能出现的问题

LDAP authentication specified, but without TLS. Passwords would go over the network in the clear

| | | | |
|----------------|-------|--------|---|
| 晚上7点23:07.801分 | INFO | cc:125 | LDAP authenticat. without TLS. Pa ver the network : le TLS with -- ldap_tls or use : o override this : production enviro -ldap_passwords_ @ Status::Status() @ AuthManager::Ini @ InitAuth() @ InitCommonRuntime @ ain() @ @ 0x7f29 tart_main @) |
| 晚上7点23:07.801分 | FATAL | cc:211 | LDAP authenticat. without TLS. Pa ver the network : le TLS with -- ldap_tls or use : o override this : production enviro -ldap_passwords_ . Impalad exitin Wrote minidump to minidumps/impala 495e-a1a199ba-f2: |

解决办法

[配置ldap_passwords in clear ok](#)

User 'hue' is not authorized to delegate to 'cxy'. User delegation is disabled.

问题描述

User 'hue' is not authorized to delegate to 'cxy'. User delegation is disabled.

Bad status for request TOpenSessionReq(username='hue', password=None, client_protocol=6, configuration={'idle_session_timeout': '3600', 'impala.doas.user': 'u'cxy'}): TOpenSessionResp(status=TStatus(errorCode=None, errorMessage="User 'hue' is not authorized to delegate to 'cxy'. User delegation is disabled.\n", sqlState='HY000', infoMessages=None, statusCode=3),

sessionHandle=TSessionHandle(sessionId=THandleIdentifier(secret='\xf4\xcc\xcd\xbc\xf4\x05@M\xa3\t|\x16\xb6g\x16p guid='\x9a \xackX_H\$\xaa\xf3\xd9\x1e\xf08\xef\xfb')), configuration=None, serverProtocolVersion=5)

解决办法

[配置proxyuser](#)