Red Hat Ceph Storage 4

使用 LDAP 和 AD 指南的对象网关

将 Ceph 对象网关配置为使用 LDAP 和 AD 对对象网关用户进行身份验证。

Last Updated: 2021-08-26

Red Hat Ceph Storage 4 使用 LDAP 和 AD 指南的对象网关

将 Ceph 对象网关配置为使用 LDAP 和 AD 对对象网关用户进行身份验证。

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

本文档描述了如何配置目录服务器或 Active Directory，以及 Ceph 对象网关以使用 LDAP 验证 Ceph 对象网关用户。 红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。详情请查看 CTO Chris Wright 信息。

目录

第 1 章 前言

红帽 Ceph 存储支持轻量级目录访问协议(LDAP)服务器对 Ceph 对象网关用户进行身份验证。为 LDAP 配置集群需要以下内容：

1. Ceph 对象网关服务器和 Ceph 存储集群。
2. LDAP 服务器。
3. LDAPS 的 SSL 证书.
4. 用于对 Ceph 对象网关进行身份验证的 LDAP 用户.
5. 至少一个 LDAP 用户用于验证 S3 客户端。

第 2 章 配置 LDAP 和 CEPH 对象网关

执行以下步骤配置红帽目录服务器，以对 Ceph 对象网关用户进行身份验证。

2.1. 安装红帽目录服务器

在命令行中使用 **hostname** 检索 LDAP 主机的完全限定域名(FQDN)。然后，在安装前，通过 DNS 或 **/etc/hosts** 和 **resolv.conf** 解析主机 FQDN。

红帽目录服务器应安装在具有图形用户界面(GUI)的红帽企业 Linux 7 服务器上，以便使用 Java Swing GUI 目录和管理控制台。但是，红帽目录服务器仍可以单独从命令行提供服务。要安装红帽目录服务器，请参阅红帽目录服务器 10 的 _Installation Guide_。

2.2. 配置目录服务器防火墙

在 LDAP 主机上，确保防火墙允许访问目录服务器的安全(**636**)端口，以便 LDAP 客户端可以访问目录服务器。将默认非安全端口(**389**)保留关闭。

```
# firewall-cmd --zone=public --add-port=636/tcp
# firewall-cmd --zone=public --add-port=636/tcp --permanent
```

2.3. SELINUX 的标签端口

为确保 SELinux 不阻止请求，请标记 SELinux 的端口。详情请查看《*红帽目录服务器 10 管理指南》 中的更改目录服务器端口号* 一节。

2.4. 配置 LDAPS

Ceph 对象网关使用简单的 ID 和密码与 LDAP 服务器进行身份验证，因此连接需要 LDAP 的 SSL 证书。要为 LDAP *配置目录服务器，请参阅《红帽目录服务器 10 管理指南》 中的配置安全连接* 章节。

LDAP 运行后，配置 Ceph 对象网关服务器，以信任目录服务器的证书。

1. 为签署 LDAP 服务器的 SSL 证书的证书颁发机构(CA)提取/下载 PEM 格式的证书。
2. 确认 **/etc/openldap/ldap.conf** 没有设置 **TLS_REQCERT**。
3. 确认 **/etc/openldap/ldap.conf** 包含 **TLS_CACERTDIR /etc/openldap/certs** 设置。
4. 使用 **certutil** 命令将 AD CA 添加到位于 **/etc/openldap/certs.** 的存储中，例如，如果 CA 是 "msad-frog-MSAD-FROG-CA"，且 PEM 格式的 CA 文件为 **ldap.pem**，使用以下命令：

   ```
   # certutil -d /etc/openldap/certs -A -t "TC,," -n "msad-frog-MSAD-FROG-CA" -i
   /path/to/ldap.pem
   ```

5. 在所有远程 LDAP 站点更新 SELinux：

   ```
   # setsebool -P httpd_can_network_connect on
   ```

注意

即使 SELinux 处于 permissive 模式，这仍需要设置。

6. 使 **certs** 数据库为全局可读。

```
# chmod 644 /etc/openldap/certs/*
```

以非 root 用户身份使用"ldapwhoami"连接到服务器。例如：

```
$ ldapwhoami -H ldaps://rh-directory-server.example.com -d 9
```

当 SSL 协商出现问题时，**-d 9** 选项将提供调试信息。

2.5. 检查网关用户是否存在

在创建网关用户之前，请确保 Ceph 对象网关还没有 用户。例如：

```
# radosgw-admin metadata list user
```

用户名不应在此用户列表中。

2.6. 添加网关用户

为 Ceph 对象网关创建一个 LDAP 用户，并记下 **binddn**。由于 Ceph 对象网关使用 **ceph** 用户，请考虑使用 **ceph** 作为用户名。用户需要具有搜索目录的权限。

测试以确保用户创建有效。其中 ceph 是 People.com 下的用户 ID，而 example.com 是域，您可以对用户执行搜索。

Ceph 对象网关将绑定到 **rgw_ldap_binddn** 中指定的用户。

测试以确保用户创建有效。其中 **ceph** 是 **People** 下的用户 ID，**example.com** 是域，您可以对用户执行搜索。

```
# ldapsearch -x -D "uid=ceph,ou=People,dc=example,dc=com" -W -H ldaps://example.com -b
"ou=People,dc=example,dc=com" -s sub 'uid=ceph'
```

在每个网关节点上，为用户的机密创建一个文件。例如，secret 可能存储在具有 **/etc/bindpass** 的文件中。为安全起见，请将此文件的所有者更改为 **ceph** 用户和组，以确保其不可全局读取。

在 Ceph 集群的管理节点上，添加 Ceph 配置文件的 **[global]** 部分中的 **rgw_ldap_secret** 设置。例如：

```
[global]
...
rgw_ldap_secret = /etc/bindpass
```

最后，将更新的配置文件复制到每个 Ceph 节点。

```
# scp /etc/ceph/ceph.conf <node>:/etc/ceph
```

2.7. 将网关配置为使用 LDAP

在 Ceph 集群的管理节点上，将下列设置添加到 Ceph 配置文件的 **[global]** 部分中。例如：

```
[global]
```

```
rgw_ldap_uri = ldaps://<fqdn>:636
rgw_ldap_binddn = "<binddn>"
rgw_ldap_secret = "/etc/bindpass"
rgw_ldap_searchdn = "<seachdn>"
rgw_ldap_dnattr = "uid"
rgw_s3_auth_use_ldap = true
```

对于 **rgw_ldap_uri** 设置，将 **<fqdn>** 替换为 LDAP 服务器的完全限定域名。如果有多个 LDAP 服务器，请指定每个域。

对于 **rgw_ldap_binddn** 设置，将 **<binddn>** 替换为 bind 域。对于 **example.com** 域以及 **users** 和 **accounts** 下的 **ceph** 用户，它应当类似如下：

```
rgw_ldap_binddn = "uid=ceph,cn=users,cn=accounts,dc=example,dc=com"
```

对于 **rgw_ldap_searchdn** 设置，将 **<searchdn>** 替换为搜索域。对于 **example.com** 和 **users** 下的用户的域，它应该类似如下： **accounts**

```
rgw_ldap_searchdn = "cn=users,cn=accounts,dc=example,dc=com"
```

将更新的配置文件复制到每个 Ceph 节点。

```
scp /etc/ceph/ceph.conf <hostname>:/etc/ceph
```

最后，重新启动 Ceph 对象网关。它应该是：

```
# systemctl restart ceph-radosgw
# systemctl restart ceph-radosgw@rgw.`hostname -s`
```

2.8. 使用自定义搜索过滤器

您可以使用 **rgw_ldap_searchfilter** 设置创建自定义搜索过滤器来限制用户访问。在 Ceph 配置文件 (**/etc/ceph/ceph.conf**)的 **[global]** 部分下指定此设置。使用 **rgw_ldap_searchfilter** 设置的方法有两种：

1. 指定部分过滤器

   示例

   ```
   "objectclass=inetorgperson"
   ```

   Ceph 对象网关将生成搜索过滤器，其用户名为来自令牌，值为 **rgw_ldap_dnattr**。然后，构建的过滤器与 **rgw_ldap_searchfilter** 值中的部分过滤器合并。例如，用户名和设置会生成最终搜索过滤器：

   示例

   ```
   "(&(uid=joe)(objectclass=inetorgperson))"
   ```

   只有在 LDAP 目录中找到用户 **joe** 时，用户 **inetorgperson** 才会被授予访问权限，他的对象类为，并且指定了有效的密码。

2. 指定 Complete Filter

完整的过滤器必须包含 **USERNAME** 令牌，在身份验证尝试过程中，该令牌将被替换为用户名。在这种情况下不使用 **rgw_ldap_dnattr** 设置。例如，要将有效用户限制为特定组，请使用以下过滤器：

示例

```
"(&(uid=@USERNAME@)(memberOf=cn=ceph-users,ou=groups,dc=mycompany,dc=com))"
```

第 3 章 配置 AD 和 CEPH 对象网关

执行以下步骤，将 Active Directory 服务器配置为对 Ceph 对象网关用户进行身份验证。

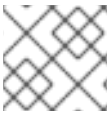
3.1. USING MICROSOFT ACTIVE DIRECTORY

Ceph 对象网关 LDAP 身份验证与任何兼容 LDAP 的目录服务兼容，可针对简单绑定（包括 Microsoft Active Directory）进行配置。使用 Active Directory 与使用 RH Directory 服务器类似，在 中，Ceph 对象网关作为 **rgw_ldap_binddn** 设置中配置的用户绑定，并使用 LDAP 来确保安全性。

配置 Active Directory 的过程基本上与 配置 LDAP 和 Ceph 对象网关 完全相同，但可能有一些特定于 Windows 的用法。

3.2. 为 LDAPS 配置 ACTIVE DIRECTORY

Active Directory LDAP 服务器默认配置为使用 LDAP。Windows Server 2012 及更高版本可以使用 Active Directory 证书服务。以下 MS TechNet 文章中提供了生成和安装与 Active Directory LDAP 一起使用的 SSL 证书的说明：LDAP over SSL(LDAPS)证书。



注意

确保 Active Directory 主机上打开了端口 **636**。

3.3. 检查网关用户是否存在

在创建网关用户之前，请确保 Ceph 对象网关还没有 用户。例如：

```
# radosgw-admin metadata list user
```

用户名不应在此用户列表中。

3.4. 添加网关用户

为 Ceph 对象网关创建一个 LDAP 用户，并记下 **binddn**。由于 Ceph 对象网关使用 **ceph** 用户，请考虑使用 **ceph** 作为用户名。用户需要具有搜索目录的权限。

测试以确保用户创建有效。其中 ceph 是 People.com 下的用户 ID，而 example.com 是域，您可以对用户执行搜索。

Ceph 对象网关将绑定到 **rgw_ldap_binddn** 中指定的用户。

测试以确保用户创建有效。其中 **ceph** 是 **People** 下的用户 ID，**example.com** 是域，您可以对用户执行搜索。

```
# ldapsearch -x -D "uid=ceph,ou=People,dc=example,dc=com" -W -H ldaps://example.com -b
"ou=People,dc=example,dc=com" -s sub 'uid=ceph'
```

在每个网关节点上，为用户的机密创建一个文件。例如，secret 可能存储在具有 **/etc/bindpass** 的文件中。为安全起见，请将此文件的所有者更改为 **ceph** 用户和组，以确保其不可全局读取。

在 Ceph 集群的管理节点上，添加 Ceph 配置文件的 **[global]** 部分中的 **rgw_ldap_secret** 设置。例如：

```
[global]
...
rgw_ldap_secret = /etc/bindpass
```

最后，将更新的配置文件复制到每个 Ceph 节点。

```
# scp /etc/ceph/ceph.conf <node>:/etc/ceph
```

3.5. 将网关配置为使用 ACTIVE DIRECTORY

在 Ceph 集群的管理节点上，在 **rgw_ldap_secret** 设置后将下列设置添加到 Ceph 配置文件的 **[global]** 部分中。例如：

```
[global]
rgw_ldap_secret = "/etc/bindpass"
...
rgw_ldap_uri = ldaps://<fqdn>:636
rgw_ldap_binddn = "<binddn>"
rgw_ldap_searchdn = "<seachdn>"
rgw_ldap_dnattr = "cn"
rgw_s3_auth_use_ldap = true
```

对于 **rgw_ldap_uri** 设置，将 **<fqdn>** 替换为 LDAP 服务器的完全限定域名。如果有多个 LDAP 服务器，请指定每个域。

对于 **rgw_ldap_binddn** 设置，将 **<binddn>** 替换为 bind 域。对于 **example.com** 域以及 **users** 和 **accounts** 下的 **ceph** 用户，它应当类似如下：

```
rgw_ldap_binddn = "uid=ceph,cn=users,cn=accounts,dc=example,dc=com"
```

对于 **rgw_ldap_searchdn** 设置，将 **<searchdn>** 替换为搜索域。对于 **example.com** 和 **users** 下的用户的域，它应该类似如下： **accounts**

```
rgw_ldap_searchdn = "cn=users,cn=accounts,dc=example,dc=com"
```

将更新的配置文件复制到每个 Ceph 节点。

```
scp /etc/ceph/ceph.conf <hostname>:/etc/ceph
```

最后，重新启动 Ceph 对象网关。它应该是：

```
# systemctl restart ceph-radosgw
# systemctl restart ceph-radosgw@rgw.`hostname -s`
```

第 4 章 测试配置

将 Ceph 对象网关配置为使用 LDAP 验证用户身份后，测试配置。

4.1. 将 S3 用户添加到 LDAP 服务器

在 LDAP 服务器上的管理控制台中，至少创建一个 S3 用户，以便 S3 客户端可以使用 LDAP 用户凭据。在将凭据传递给 S3 客户端时，记下要使用的用户名和机密。

4.2. 导出 LDAP 令牌

使用 LDAP 运行 Ceph 对象网关时，需要访问令牌。但是，访问令牌是从 access key 和 secret 创建的。将 access key 和 secret key 导出为 LDAP 令牌。

1. 导出 access key。

```
# export RGW_ACCESS_KEY_ID="<username>"
```

2. 导出该机密。

```
# export RGW_SECRET_ACCESS_KEY="<password>"
```

3. 导出令牌。对于 LDAP，使用 **ldap** 作为令牌类型(**ttype**)。

```
# radosgw-token --encode --ttype=ldap
```

对于 Active Directory，使用 **ad** 作为令牌类型。

```
# radosgw-token --encode --ttype=ad
```

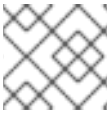
结果是一个 base-64 编码字符串，即访问令牌。将此访问令牌提供给 S3 客户端，以代替 access key。不再需要该 secret。

4. （可选）为方便起见，如果 S3 客户端使用 环境变量，请将 base-64 编码字符串导出到 **RGW_ACCESS_KEY_ID** 环境变量。

```
# export
RGW_ACCESS_KEY_ID="ewogICAgIlJHV19UT0tFTiI6IHsKICAgICAgICAidmVyc2lvbiI6IDEsCiAgICAgICAgInR5cGUiOiAibGRhcCIsCiAgICAgICAgImlkIjogImNlcGgiLAogICAgICAgICJrZXkiOiAiODAwI0dvcmlsbGEiCiAgICB9Cn0K"
```

4.3. 使用 S3 客户端测试配置

挑选 Ceph 对象网关客户端，如 Python Boto。将它配置为使用 **RGW_ACCESS_KEY_ID** 环境变量。或者，您可以复制 base-64 编码字符串，并将其指定为 access key。然后，运行 Ceph 客户端。



注意

不再需要该 secret。