Red Hat Ceph Storage 2 Ceph Object Gateway with LDAP/AD Guide

Configuring Ceph Object Gateway to use LDAP and AD to authenticate object gateway users.

Red Hat Ceph Storage Documentation Team

Red Hat Ceph Storage 2 Ceph Object Gateway with LDAP/AD Guide

Configuring Ceph Object Gateway to use LDAP and AD to authenticate object gateway users.

Legal Notice

Abstract

This document describes how to configure Directory Server or Active Directory and the Ceph Object Gateway to use LDAP to authenticate Ceph Object Gateway users.

Table of Contents

PREFACE

Ceph v2.0 and beyond supports Light-weight Directory Access Protocol (LDAP) servers for authenticating Ceph Object Gateway users. Configuring a cluster for use with LDAP requires the following:

1. A Ceph Object Gateway server and Ceph Storage cluster.
2. An LDAP server.
3. An SSL certificate for LDAPS.
4. An LDAP user for authenticating the Ceph Object Gateway.
5. At least one LDAP user for authenticating S3 clients.

CHAPTER 1. CONFIGURING LDAP AND CEPH OBJECT GATEWAY

1.1. INSTALLING RED HAT DIRECTORY SERVER

Retrieve the LDAP host's fully qualified domain name (FQDN) using **hostname** on the command line. Then, ensure that the host FQDN is resolvable via DNS or in **/etc/hosts** and **resolv.conf** before installing.

Red Hat Directory Server should be installed on a RHEL 7 server with a graphical user interface (GUI) in order to use the Java Swing GUI Directory and Administration consoles. However,Red Hat Directory Server can still be serviced exclusively from the command line. To install Red Hat Directory Server, see the Red Hat Directory Server Quick Start for details.

1.2. CONFIGURING THE DIRECTORY SERVER FIREWALL

On the LDAP host, make sure that the firewall allows access to the Directory Server's secure (**636**) port, so that LDAP clients can access the Directory Server. Leave the default unsecure port (**389**) closed.

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

1.3. LABELING PORTS FOR SELINUX

To ensure SELinux doesn't block requests, label the ports for SELinux. See Labelling SSL Ports for details.

1.4. CONFIGURING LDAPS

The Ceph Object Gateway uses a simple ID and password to authenticate with the LDAP server, so the connection requires an SSL certificate for LDAPS. To configure Directory Server for LDAPs, see Secure Connections for details.

Once the LDAPs is working, configure the Ceph Object Gateway server(s) to trust the Directory Server's certificate.

For RHEL 7, perform the following steps:

1. Extract/Download a PEM-formatted certificate for the Certificate Authority (CA) that signed the LDAP server's SSL certificate.
2. Confirm that **/etc/openldap/ldap.conf** does not have **TLS_REQCERT** set.
3. Confirm that **/etc/openldap/ldap.conf** contains a **TLS_CACERTDIR /etc/openldap/certs** setting.
4. Use the **certutil** command to add the AD CA to the store at**/etc/openldap/certs.** For example, if the CA was named "msad-frog-MSAD-FROG-CA", and the PEM-formatted CA file is **ldap.pem**, you would run the following:

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

5. Make the **certs** database world-readable.

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

At this point you should be able to connect to the server using "ldapwhoami" as a non-root user. For example:

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

The **-d 9** option will provide debugging information in case something went wrong with the SSL negotiation.

For Ubuntu Xenial, perform the following steps:

1. Extract/Download a PEM-formatted certificate for the Certificate Authority (CA) that signed the LDAP server's SSL certificate. This step is identical to RHEL 7 above.
2. Confirm that **/etc/ldap/ldap.conf** does not have **TLS_REQCERT** set. This step is similar to RHEL 7, but note that the file path on Ubuntu is **/etc/ldap/ldap.conf**, not **/etc/openldap**.
3. Place the PEM-formatted CA cert at **/usr/local/share/ca-certificates/ldap-ca.crt** and ensure that its permissions are 0644 (world-readable).
4. Set **TLS_CACERT /usr/local/share/ca-certificates/ldap-ca.crt** in **/etc/ldap/ldap.conf**.

At this point you should be able to connect to the server using **ldapwhoami** as a non-root user. For example:

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

The **-d 9** option will provide debugging information in case something went wrong with the SSL negotiation.

1.5. CHECKING IF THE GATEWAY USER EXISTS

Before creating the gateway user, ensure that the Ceph Object Gateway doesn't already have the user. For example:

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

The user name should NOT be in this list of users.

1.6. ADDING A GATEWAY USER

On your LDAP node, create a user for the gateway in the Directory Server console. Since the Ceph object gateway uses the **ceph** user, consider using **ceph** as the username. The user needs to have permissions to search the directory.

Test to ensure that the user creation worked. Where **ceph** is the user ID under **People** and **example.com** is the domain, you can perform a search for the user.

```
# 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'
```

On each gateway node, create a file for the user's secret. For example, the secret may get stored in a file entitled **/etc/bindpass**. For security, change the owner of this file to the **ceph** user and group to ensure it is not globally readable.

On the administrative node for the Ceph cluster, add the **rgw_ldap_secret** setting in the **[global]** section of the Ceph configuration file. For example:

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

Finally, copy the updated configuration file to each Ceph node.

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

1.7. CONFIGURING THE GATEWAY TO USE LDAP

On the administrative node for the Ceph cluster, add the following settings in the **[global]** section of the Ceph configuration file. For example:

```
[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
```

For the **rgw_ldap_uri** setting, substitute **<fqdn>** with the fully qualified domain name of the LDAP server. If there is more than one LDAP server, specify each domain.

For the **rgw_ldap_binddn** setting, substitute **<binddn>** with the bind domain. With a domain of **example.com** and a **ceph** user under **users** and **accounts**, it should look something like this:

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

For the **rgw_ldap_searchdn** setting, substitute **<searchdn>** with the search domain. With a domain of **example.com** and users under **users** and **accounts**, it should look something like this:

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

Copy the updated configuration file to each Ceph node.

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

Finally, restart the Ceph Object Gateway. It should be one of:

-

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

1.8. USING A CUSTOM SEARCH FILTER

You can create a custom search filter to limit user access by using the **rgw_ldap_searchfilter** setting. Specify this setting under the **[global]** section of the Ceph configuration file (**/etc/ceph/ceph.conf**). There are two ways to use the **rgw_ldap_searchfilter** setting:

1. Specifying a Partial Filter

   Example

   ```
   "objectclass=inetorgperson"
   ```

   The Ceph Object Gateway will generate the search filter with the user name from the token and the value of **rgw_ldap_dnattr**. The constructed filter is then combined with the partial filter from the **rgw_ldap_searchfilter** value. For example, the user name and the settings generate the final search filter:

   Example

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

   User **joe** will only be granted access if he is found in the LDAP directory, he has an object class of **inetorgperson**, and he specifies a valid password.

2. Specifying a Complete Filter

   A complete filter must contain a **USERNAME** token which will be substituted with the user name during the authentication attempt. The **rgw_ldap_dnattr** setting is not used in this case. For example, to limit valid users to a specific group, use the following filter:

   Example

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

CHAPTER 2. CONFIGURING ACTIVE DIRECTORY AND CEPH OBJECT GATEWAY

2.1. USING MICROSOFT ACTIVE DIRECTORY

Ceph Object Gateway LDAP authentication is compatible with any LDAP-compliant directory service that can be configured for simple bind, including Microsoft Active Directory. Using Active Directory is similar to using RH Directory server in that the Ceph object gateway binds as the user configured in the **rgw_ldap_binddn** setting, and using LDAPs to ensure security.

The process for configuring Active Directory is essentially identical with Configuring LDAP and Ceph Object Gateway, but may have some Windows-specific usage.

2.2. CONFIGURING ACTIVE DIRECTORY FOR LDAPS

Active Directory LDAP servers are configured to use LDAPs by default. Windows Server 2012 and higher can use Active Directory Certificate Services. Instructions for generating and installing SSL certificates for use with Active Directory LDAP are available in the following MS TechNet article: LDAP over SSL (LDAPS) Certificate.

Note

Ensure that port **636** is open on the Active Directory host.

2.3. CHECK IF THE GATEWAY USER EXISTS

Before creating the gateway user, ensure that the Ceph Object Gateway doesn't already have the user. For example:

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

The user name should NOT be in this list of users.

2.4. ADDING A GATEWAY USER

Create an Active Directory user for the Ceph Object Gateway, and make a note of the **binddn**. The Ceph Object Gateway will bind to this user as specified in the **rgw_ldap_binddn**.

Like Add a Gateway User, test to ensure that the user creation worked. Where **ceph** is the user ID under **People** and **example.com** is the domain, you can perform a search for the user.

```
# 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'
```

On each gateway node, create a file for the user's secret. For example, the secret may get stored in a file entitled **/etc/bindpass**. For security, change the owner of this file to the **ceph** user and group to ensure it is not globally readable.

On the administrative node for the Ceph cluster, add the **rgw_ldap_secret** setting in the **[global]** section of the Ceph configuration file. For example:

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

Finally, copy the updated configuration file to each Ceph node.

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

2.5. CONFIGURING THE GATEWAY TO USE ACTIVE DIRECTORY

On the administrative node for the Ceph cluster, add the following settings in the **[global]** section of the Ceph configuration file after the **rgw_ldap_secret** setting. For example:

```
[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
```

For the **rgw_ldap_uri** setting, substitute **<fqdn>** with the fully qualified domain name of the LDAP server. If there is more than one LDAP server, specify each domain.

For the **rgw_ldap_binddn** setting, substitute **<binddn>** with the bind domain. With a domain of **example.com** and a **ceph** user under **users** and **accounts**, it should look something like this:

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

For the **rgw_ldap_searchdn** setting, substitute **<searchdn>** with the search domain. With a domain of **example.com** and users under **users** and **accounts**, it should look something like this:

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

Copy the updated configuration file to each Ceph node.

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

Finally, restart the Ceph Object Gateway. It should be one of:

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

CHAPTER 3. TESTING THE CONFIGURATION

3.1. ADDING AN S3 USER TO LDAP SERVER

In the administrative console on LDAP server, create at least one S3 user so that an S3 client can use the LDAP user credentials. Make a note of the user name and secret for use when passing the credentials to the S3 client.

3.2. EXPORT AN LDAP TOKEN

When running Ceph Object Gateway with LDAP, the access token is all that is required. However, the access token is created from the access key and secret. Export the access key and secret key as an LDAP token.

1. Export the access key.

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

2. Export the secret.

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

3. Export the token. For LDAP, use **ldap** as the token type (**ttype**).

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

   For Active Directory, use **ad** as the token type.

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

   The result is a base-64 encoded string, which is the access token. Provide this access token to S3 clients in lieu of the access key. The secret is no longer required.

4. (Optional) For added convenience, export the base-64 encoded string to the **RGW_ACCESS_KEY_ID** environment variable if the S3 client uses the environment variable.

```
# export
RGW_ACCESS_KEY_ID="ewogICAgIlJHV19UT0tFTiI6IHsKICAgICAgICAidmVyc2
lvbiI6IDEsCiAgICAgICAgInR5cGUiOiAibGRhcCIsCiAgICAgICAgImlkIjogImN
lcGgiLAogICAgICAgICJrZXkiOiAiODAwI0dvcmlsbGEiCiAgICB9Cn0K"
```

3.3. TEST THE CONFIGURATION WITH AN S3 CLIENT

Pick a Ceph Object Gateway client such as Python Boto. Configure it to use the **RGW_ACCESS_KEY_ID** environment variable. Alternatively, you may copy the base-64 encoded string and specify it as the access key. Then, run the Ceph client.

Note

The secret is no longer required.