Red Hat Ceph Storage 4

LDAP および ADを使用したオブジェクトゲートウェイガイド

LDAP および AD を使用してオブジェクトゲートウェイユーザーを認証するように Ceph Object Gateway を設定

Last Updated: 2023-02-19

Red Hat Ceph Storage 4 LDAP および ADを使用したオブジェクトゲートウェイガイド

LDAP および AD を使用してオブジェクトゲートウェイユーザーを認証するように Ceph Object Gateway を設定

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.

法律上の通知

概要

本ガイドでは、LDAP を使用して Ceph Object Gateway ユーザーを認証するように Directory Server または Active Directory および Ceph Object Gateway を設定する方法を説明します。 Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社の CTO、Chris Wright のメッセージを参照してください。

目次

第1章 前書き

Red Hat Ceph Storage は、Ceph Object Gateway ユーザーを認証するために、LDAP (Light-weight Directory Access Protocol) サーバーをサポートします。LDAP で使用するクラスターを設定するには、以下が必要です。

1. Ceph Object Gateway サーバーおよび Ceph Storage クラスター。
2. LDAP サーバー。
3. LDAPS の SSL 証明書。
4. Ceph Object Gateway を認証するための LDAP ユーザー。
5. S3 クライアントを認証するための LDAP ユーザーが 1 人以上いること。

第2章 LDAP および CEPH OBJECT GATEWAY の設定

Ceph Object Gateway ユーザーを認証するように Red Hat Directory Server を設定するには、以下の手順を実施します。

2.1. RED HAT DIRECTORY SERVER のインストール

コマンドラインで **hostname** を使用して、LDAP ホストの完全修飾ドメイン名 (FQDN) を取得します。次に、インストール前に、ホストの FQDN が DNS または **/etc/hosts** および **resolv.conf** で解決可能であることを確認してください。

Java Swing GUI Directory および管理コンソールを使用するには、グラフィカルユーザーインターフェース (GUI) を使用する Red Hat Enterprise Linux 7 サーバーに Red Hat Directory Server をインストールする必要があります。ただし、Red Hat Directory Server にはコマンドラインから排他的にサービスを提供できます。Red Hat Directory Server をインストールするには、Red Hat Directory Server 10 の『インストールガイド』を参照してください。

2.2. DIRECTORY SERVER ファイアウォールの設定

LDAP ホストで、LDAP クライアントが Directory Server にアクセスできるように、ファイアウォールが Directory Server のセキュアな (**636**) ポートにアクセスできることを確認します。デフォルトのセキュアでないポート (**389**) を閉じたままにしておきます。

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

2.3. SELINUX のラベルポート

SELinux が要求をブロックしないようにするには、SELinux のポートにラベルを付けます。詳細は、Red Hat Directory Server 10 の『**Administration Guide**』の「Changing Directory Server Port Numbers」を参照してください。

2.4. LDAPS の設定

Ceph Object Gateway は単純な ID およびパスワードを使用して LDAP サーバーとの認証を行うため、接続には LDAP の SSL 証明書が必要です。LDAP 用 Directory Server を設定するには、Red Hat Directory Server 10 の「**Administration Guide**」の「Configuring Secure Connections」の章を参照してください。

LDAP が動作したら、Ceph Object Gateway サーバーが Directory Server の証明書を信頼するように設定します。

1. LDAP サーバーの SSL 証明書に署名した認証局 (CA) の PEM 形式の証明書を抽出/ダウンロードします。
2. **/etc/openldap/ldap.conf** に **TLS_REQCERT** が設定されていないことを確認します。
3. **/etc/openldap/ldap.conf** に **TLS_CACERTDIR /etc/openldap/certs** 設定が含まれていることを確認します。
4. **certutil** コマンドを使用して、AD CA を **/etc/openldap/certs** のストアに追加します。たとえば、CA が「msad-frog-MSAD-FROG-CA」で、PEM 形式の CA ファイルが **ldap.pem** の場合は、以下のコマンドを使用します。

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

5. すべてのリモート LDAP サイトで SELinux を更新します。

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

注記

これは、SELinux が Permissive モードであっても、引き続き設定する必要があります。

6. **certs** データベースを誰でも読めるようにします。

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

root 以外のユーザーとして「ldapwhoami」を使用してサーバーに接続します。以下に例を示します。

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

-d 9 オプションは、SSL ネゴシエーションで何らかの問題が発生した場合にデバッグ情報を提供します。

2.5. ゲートウェイユーザーが存在するかどうかの確認

ゲートウェイユーザーを作成する前に、Ceph Object Gateway にユーザーがまだ存在していないことを確認してください。以下に例を示します。

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

このユーザー名は、このユーザー一覧には記載しないでください。

2.6. ゲートウェイユーザーの追加

Ceph Object Gateway の LDAP ユーザーを作成し、**binddn** を書き留めます。Ceph オブジェクトゲートウェイは **ceph** ユーザーを使用するため、**ceph** をユーザー名として使用することを検討してください。ユーザーに、ディレクトリーを検索するパーミッションが必要です。

ユーザーの作成が正常に機能することをテストします。ceph が People の下のユーザー ID で、example.com がドメインの場合は、ユーザーの検索を行うことができます。

Ceph Object Gateway は、**rgw_ldap_binddn** で指定したようにこのユーザーにバインドします。

ユーザーの作成が正常に機能することをテストします。**ceph** が **People** の下のユーザー ID で、**example.com** がドメインの場合は、ユーザーの検索を行うことができます。

```
# 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'
```

各ゲートウェイノードで、ユーザーのシークレットのファイルを作成します。たとえば、シークレットは **/etc/bindpass** という名前のファイルに保存されます。セキュリティー上の理由から、このファイルの所有者を **ceph** ユーザーおよびグループに変更し、グローバルに読み取りができないようにします。

Ceph クラスターの管理ノードで、Ceph 設定ファイルの **[global]** セクションに **rgw_ldap_secret** の設定を追加します。以下に例を示します。

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

最後に、更新された設定ファイルを各 Ceph ノードにコピーします。

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

2.7. LDAP を使用するようにゲートウェイを設定

Ceph クラスターの管理ノードで、Ceph 設定ファイルの **[global]** セクションに以下の設定を追加します。以下に例を示します。

```
[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
```

rgw_ldap_uri 設定の場合は、**<fqdn>** を LDAP サーバーの完全修飾ドメイン名に置き換えます。複数の LDAP サーバーがある場合には、各ドメインを指定します。

rgw_ldap_binddn 設定の場合は、**<binddn>** をバインドドメインに置き換えます。**users** および **accounts** の下に **example.com** のドメインおよび **ceph** ユーザーが使用されている場合には、以下のようになります。

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

rgw_ldap_searchdn 設定の場合は、**<searchdn>** を検索ドメインに置き換えます。**users** および **accounts** の下に **example.com** のドメインおよびユーザーがある場合は、以下のようになります。

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

更新された設定ファイルを各 Ceph ノードにコピーします。

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

最後に、Ceph Object Gateway を再起動します。次のいずれかでなければなりません。

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

2.8. カスタム検索フィルターの使用

rgw_ldap_searchfilter 設定を使用すると、ユーザーアクセスを制限するカスタム検索フィルターを作成できます。この設定は、Ceph 設定ファイル (**/etc/ceph/ceph.conf**) の **[global]** セクションに指定します。**rgw_ldap_searchfilter** 設定には、2 つの方法があります。

1. 部分フィルターの指定

   例

   ```
   "objectclass=inetorgperson"
   ```

   Ceph Object Gateway は、トークンのユーザー名および **rgw_ldap_dnattr** の値を使用して検索フィルターを生成します。構築されたフィルターは、**rgw_ldap_searchfilter** の値の一部フィルターと組み合わされます。たとえば、ユーザー名と設定により、最終的な検索フィルターが生成されます。

   例

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

   ユーザー **joe** は、LDAP ディレクトリーで見つかった場合にのみアクセスが許可され、**inetorgperson** のオブジェクトクラスがあり、有効なパスワードを指定します。

2. Complete フィルターの指定
   完全なフィルターには、認証の試行中にユーザー名に置き換えられる **USERNAME** トークンが含まれている必要があります。この場合、**rgw_ldap_dnattr** 設定は使用されません。たとえば、有効なユーザーを特定のグループに制限するには、以下のフィルターを使用します。

   例

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

第3章 AD および CEPH OBJECT GATEWAY の設定

Ceph Object Gateway ユーザーを認証するように Active Directory サーバーを設定するには、以下の手順を実施します。

3.1. MICROSOFT ACTIVE DIRECTORY の使用

Ceph Object Gateway の LDAP 認証は、Microsoft Active Directory を含む単純なバインド用に設定できる LDAP 準拠のディレクトリーサービスと互換性があります。Active Directory の使用は、Ceph オブジェクトゲートウェイが **rgw_ldap_binddn** 設定に設定されたユーザーとしてバインドし、LDAP を使用してセキュリティーを確保する RH Directory サーバーの使用と似ています。

Active Directory を設定するプロセスは基本的に LDAP および Ceph Object Gateway の設定 と同じですが、Windows 固有の使用方法がいくつかある可能性があります。

3.2. LDAPS の ACTIVE DIRECTORY の設定

Active Directory LDAP サーバーは、デフォルトで LDAP を使用するように設定されています。Windows Server 2012 以降では、Active Directory 証明書サービスを使用できます。Active Directory LDAP で使用する SSL 証明書を生成してインストールする手順は、MS TechNet の記事「LDAP over SSL (LDAPS) Certificate」を参照してください。

注記

ポート **636** が Active Directory ホストで開いていることを確認します。

3.3. ゲートウェイユーザーが存在するかどうかの確認

ゲートウェイユーザーを作成する前に、Ceph Object Gateway にユーザーがまだ存在していないことを確認してください。以下に例を示します。

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

このユーザー名は、このユーザー一覧には記載しないでください。

3.4. ゲートウェイユーザーの追加

Ceph Object Gateway の LDAP ユーザーを作成し、**binddn** を書き留めます。Ceph オブジェクトゲートウェイは **ceph** ユーザーを使用するため、**ceph** をユーザー名として使用することを検討してください。ユーザーに、ディレクトリーを検索するパーミッションが必要です。

ユーザーの作成が正常に機能することをテストします。ceph が People の下のユーザー ID で、example.com がドメインの場合は、ユーザーの検索を行うことができます。

Ceph Object Gateway は、**rgw_ldap_binddn** で指定したようにこのユーザーにバインドします。

ユーザーの作成が正常に機能することをテストします。**ceph** が **People** の下のユーザー ID で、**example.com** がドメインの場合は、ユーザーの検索を行うことができます。

```
# 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'
```

各ゲートウェイノードで、ユーザーのシークレットのファイルを作成します。たとえば、シークレットは **/etc/bindpass** という名前のファイルに保存されます。セキュリティー上の理由から、このファイルの所有者を **ceph** ユーザーおよびグループに変更し、グローバルに読み取りができないようにします。

Ceph クラスターの管理ノードで、Ceph 設定ファイルの **[global]** セクションに **rgw_ldap_secret** の設定を追加します。以下に例を示します。

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

最後に、更新された設定ファイルを各 Ceph ノードにコピーします。

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

3.5. ACTIVE DIRECTORY を使用するようにゲートウェイを設定

Ceph クラスターの管理ノードで、**rgw_ldap_secret** の設定後に Ceph 設定ファイルの **[global]** セクションに以下の設定を追加します。以下に例を示します。

```
[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
```

rgw_ldap_uri 設定の場合は、**<fqdn>** を LDAP サーバーの完全修飾ドメイン名に置き換えます。複数の LDAP サーバーがある場合には、各ドメインを指定します。

rgw_ldap_binddn 設定の場合は、**<binddn>** をバインドドメインに置き換えます。**users** および **accounts** の下に **example.com** のドメインおよび **ceph** ユーザーが使用されている場合には、以下のようになります。

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

rgw_ldap_searchdn 設定の場合は、**<searchdn>** を検索ドメインに置き換えます。**users** および **accounts** の下に **example.com** のドメインおよびユーザーがある場合は、以下のようになります。

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

更新された設定ファイルを各 Ceph ノードにコピーします。

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

最後に、Ceph Object Gateway を再起動します。次のいずれかでなければなりません。

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

第4章 設定のテスト

LDAP を使用してユーザーを認証するように Ceph Object Gateway を設定したら、設定をテストします。

4.1. S3 ユーザーの LDAP サーバーへの追加

LDAP サーバーの管理コンソールで S3 ユーザーを少なくとも 1 つ作成し、S3 クライアントが LDAP ユーザーの資格情報を使用できるようにします。認証情報を S3 クライアントに渡すときに使用するユーザー名およびシークレットを書き留めておきます。

4.2. LDAP トークンのエクスポート

LDAP で Ceph Object Gateway を実行する場合は、アクセストークンのみが必要です。ただし、アクセストークンは、アクセスキーとシークレットから作成されます。アクセスキーとシークレットキーを LDAP トークンとしてエクスポートします。

1. アクセスキーをエクスポートします。

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

2. シークレットをエクスポートします。

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

3. トークンをエクスポートします。LDAP の場合は、トークンタイプ (**ttype**) に **ldap** を使用します。

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

Active Directory の場合は、トークンタイプとして **ad** を使用します。

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

結果として、アクセストークンである base-64 でエンコードされた文字列になります。このアクセストークンを、アクセスキーの代わりに S3 クライアントに提供します。シークレットは不要になりました。

4. (任意) S3 クライアントが環境変数を使用している場合は、利便性を高めるために base-64 でエンコードされた文字列を環境変数 **RGW_ACCESS_KEY_ID** にエクスポートします。

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

4.3. S3 クライアントを使用した設定のテスト

Python Boto などの Ceph Object Gateway クライアントを選択します。**RGW_ACCESS_KEY_ID** 環境変数を使用するように設定します。base-64 でエンコードされた文字列をコピーし、アクセスキーとして指定できます。次に、Ceph クライアントを実行します。

注記

シークレットは不要になりました。