Red Hat OpenStack Platform 17.0

OpenStack Identity と外部のユーザー管理サービスの統合

Active Directory または Red Hat Identity Management を外部認証バックエンドとして使用する方法

Last Updated: 2024-08-22

Red Hat OpenStack Platform 17.0 OpenStack Identity と外部のユーザー管理サービスの統合

Active Directory または Red Hat Identity Management を外部認証バックエンドとして使用する方法

OpenStack Team
rhos-docs@redhat.com

法律上の通知

概要

OpenStack Identity (keystone) サービスを Microsoft Active Directory Domain Service(AD DS)、Red Hat Identity Management(IdM)、および LDAP と統合します。

目次

多様性を受け入れるオープンソースの強化 3

第1章 OPENSTACK IDENTITY (KEYSTONE) と ACTIVE DIRECTORY の統合 4
1.1. ACTIVE DIRECTORY 認証情報の設定 4
1.2. ACTIVE DIRECTORY LDAPS 証明書のインストール 5
1.3. ドメイン固有の LDAP バックエンドを使用する DIRECTOR の設定 6
1.4. OPENSTACK IDENTITY ドメインへの管理ユーザーアクセス権の付与 8
1.5. RED HAT OPENSTACK PLATFORM プロジェクトへの外部グループアクセス権の付与 9
1.6. RED HAT OPENSTACK PLATFORM プロジェクトへの外部ユーザーアクセス権の付与 12
1.7. OPENSTACK IDENTITY ドメインおよびユーザーのリスト表示 14
1.8. 非管理者ユーザーの認証情報ファイルの作成 15
1.9. OPENSTACK IDENTITY と外部のユーザー管理サービスの統合のテスト 15
1.10. ACTIVE DIRECTORY との統合のトラブルシューティング 16

第2章 OPENSTACK IDENTITY (KEYSTONE) と RED HAT IDENTITY MANAGER (IDM) の統合 18
2.1. RED HAT IDENTITY MANAGER (IDM) との統合の計画 18
2.2. OPENSTACK 向けの IDENTITY MANAGEMENT (IDM) サーバーの推奨事項 20
2.3. ANSIBLE を使用した TLS-E の実装 21
2.4. TLS EVERYWHERE (TLS-E) による MEMCACHED トラフィックの暗号化 24
2.5. RED HAT IDENTITY MANAGER (IDM) サーバーの認証情報の設定 24
2.6. RED HAT IDENTITY MANAGER (IDM) LDAPS 証明書のインストール 25
2.7. ドメイン固有の LDAP バックエンドを使用する DIRECTOR の設定 26
2.8. OPENSTACK IDENTITY ドメインへの管理ユーザーアクセス権の付与 28
2.9. RED HAT OPENSTACK PLATFORM プロジェクトへの外部グループアクセス権の付与 29
2.10. RED HAT OPENSTACK PLATFORM プロジェクトへの外部ユーザーアクセス権の付与 31
2.11. OPENSTACK IDENTITY ドメインおよびユーザーのリスト表示 34
2.12. 非管理者ユーザーの認証情報ファイルの作成 34
2.13. OPENSTACK IDENTITY と外部のユーザー管理サービスの統合のテスト 35
2.14. RED HAT IDENTITY MANAGER (IDM) の統合に関するトラブルシューティング 36

多様性を受け入れるオープンソースの強化

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、Red Hat CTO である Chris Wright のメッセージ を参照してください。

第1章 OPENSTACK IDENTITY (KEYSTONE) と ACTIVE DIRECTORY の統合

OpenStack Identity (keystone) と Microsoft Active Directory Domain Service (AD DS) を統合することができます。Identity サービスは、特定の Active Directory Domain Services (AD DS) ユーザーを認証しますが、承認設定および重要なサービスアカウントは Identity サービスデータベースに保持されます。その結果、Identity サービスは、ユーザーアカウントの認証用に AD DS に読み取り専用でアクセスし、認証されたアカウントに割り当てられた権限の管理を継続します。

Identity サービスを AD DS と統合することで、AD DS ユーザーは Red Hat OpenStack Platform (RHOSP) に対して認証してリソースにアクセスできるようになります。Identity サービスや Image サービスなどの RHOSP サービスアカウントや承認管理は、Identity サービスのデータベースに残ります。パーミションとロールは、Identity サービスの管理ツールを使用して AD DS アカウントに割り当てられます。

OpenStack Identity と Active Directory を統合するプロセスには、以下の段階が含まれています。

1. Active Directory の認証情報を設定し、LDAPS 証明書をエクスポートする
2. OpenStack に LDAPS 証明書をインストールおよび設定する
3. 1 つまたは複数の LDAP バックエンドを使用するように director を設定する
4. Active Directory バックエンドにアクセスするようにコントローラーノードを設定する
5. OpenStack プロジェクトへの Active Directory ユーザーまたはグループのアクセスを設定する
6. ドメインおよびユーザーリストが正しく作成されていることを確認する
7. (オプション) 管理者以外のユーザーの認証情報ファイルを作成する

1.1. ACTIVE DIRECTORY 認証情報の設定

Active Directory Domain Service (AD DS) が OpenStack Identity と統合するように設定するには、Identity サービスが使用する LDAP アカウントを設定し、Red Hat OpenStack Platform ユーザーのユーザーグループを作成し、Red Hat OpenStack Platform のデプロイメントで使用する LDAPS 証明書の公開鍵をエクスポートします。

前提条件

- Active Directory ドメインサービスが設定済みで、稼働していること。
- Red Hat OpenStack Platform が設定済みで、稼働していること。
- DNS 名前解決が完全に機能しており、かつ全ホストが適切に登録されていること。
- AD DS 認証トラフィックが LDAPS で暗号化され、ポート 636 を使用していること。
- 推奨: 単一の障害点を避けるために、高可用性または負荷分散ソリューションを備えた AD DS を実装していること。

手順

Active Directory サーバーで以下の手順を実行します。

1. LDAP ルックアップアカウントを作成します。このアカウントは、Identity サービスが AD DS LDAP サービスにクエリーを実行するのに使用されます。

```
PS C:\> New-ADUser -SamAccountName svc-ldap -Name "svc-ldap" -GivenName LDAP -
Surname Lookups -UserPrincipalName svc-ldap@lab.local  -Enabled $false -
PasswordNeverExpires $true -Path 'OU=labUsers,DC=lab,DC=local'
```

2. このアカウントのパスワードを設定し、有効にします。AD ドメインのパスワードの複雑さの要件を満たすパスワードを指定するように要求されます。

```
PS C:\> Set-ADAccountPassword svc-ldap -PassThru | Enable-ADAccount
```

3. **grp-openstack** という名前の RHOSP ユーザーグループを作成します。OpenStack Identity でパーミッションを割り当てることができるのは、このグループのメンバーのみです。

```
PS C:\> NEW-ADGroup -name "grp-openstack" -groupscope Global -path
"OU=labUsers,DC=lab,DC=local"
```

4. プロジェクトグループを作成します。

```
PS C:\> NEW-ADGroup -name "grp-openstack-demo" -groupscope Global -path
"OU=labUsers,DC=lab,DC=local"
PS C:\> NEW-ADGroup -name "grp-openstack-admin" -groupscope Global -path
"OU=labUsers,DC=lab,DC=local"
```

5. **svc-ldap** ユーザーを **grp-openstack** グループに追加します。

```
PS C:\> ADD-ADGroupMember "grp-openstack" -members "svc-ldap"
```

6. AD Domain Controller から **Certificates MMC** を使用して、DER で暗号化された **x509** .cer ファイルとして LDAPS 証明書の (秘密鍵ではなく) 公開鍵 をエクスポートします。このファイルを RHOSP 管理者に送信します。

7. AD DS ドメインの NetBIOS 名の取得。

```
PS C:\> Get-ADDomain | select NetBIOSName
NetBIOSName
-----------
LAB
```

この値を RHOSP 管理者に送信します。

1.2. ACTIVE DIRECTORY LDAPS 証明書のインストール

OpenStack Identity (keystone) は、LDAPS クエリーを使用してユーザーアカウントを検証します。このトラフィックを暗号化するために、keystone は **keystone.conf** で定義されている証明書ファイルを使用します。LDAPS 証明書を設定するには、Active Directory から受け取った公開鍵を **.crt** 形式に変換し、その証明書を keystone が参照できる場所にコピーします。

注記

LDAP 認証に複数のドメインを使用する場合、**Unable to retrieve authorized projects** または **Peer's Certificate issuer is not recognized** など、さまざまなエラーが発生する可能性があります。これは、keystone が特定ドメインに誤った証明書を使用すると発生する可能性があります。回避策として、すべての LDAPS 公開鍵を単一の **.crt** バンドルにマージし、このファイルを使用するようにすべての keystone ドメインを設定します。

前提条件

- Active Directory の認証情報が設定されている。
- LDAPS 証明書が Active Directory からエクスポートされている。

手順

1. OpenStack Identity を実行中のノードに、LDAPS 公開鍵をコピーし、**.cer** から **.crt** に変換します。この例では、**addc.lab.local.cer** とうい名前の元の証明書ファイルを使用しています。

```
# openssl x509 -inform der -in addc.lab.local.cer -out addc.lab.local.crt
# cp addc.lab.local.crt /etc/pki/ca-trust/source/anchors
```

2. (オプション) **ldapsearch** などの診断のコマンドを実行する必要がある場合には、RHEL の証明書ストアに証明書を追加する必要もあります。
   a. **.cer** から **.pem** に変換します。この例では、**addc.lab.local.cer** とうい名前の元の証明書ファイルを使用しています。

```
# openssl x509 -inform der -in addc.lab.local.cer -out addc.lab.local.pem
```

   b. コントローラーノードに **.pem** をインストールします。たとえば、Red Hat Enterprise Linux の場合は以下を実行します。

```
# cp addc.lab.local.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust
```

1.3. ドメイン固有の LDAP バックエンドを使用する DIRECTOR の設定

director が 1 つ以上の LDAP バックエンドを使用するように設定するには、heat テンプレートで **KeystoneLDAPDomainEnable** フラグを **true** に設定し、各 LDAP バックエンドに関する情報が含まれる環境ファイルを設定します。次に、director は keystone ドメインごとに別の LDAP バックエンドを使用します。

注記

ドメイン設定ファイルのデフォルトのディレクトリーは **/etc/keystone/domains/** に設定されています。**keystone::domain_config_directory** hiera キーを使用して環境ファイル内に **ExtraConfig** パラメーターを追加して必要なパスを設定することによってオーバーライドすることができます。

手順

1. デプロイメントの heat テンプレートで、**KeystoneLDAPDomainEnable** フラグを **true** に設定します。これにより、**identity** 設定グループ内の keystone に **domain_specific_drivers_enabled** オプションが設定されます。

2. **tripleo-heat-templates** に **KeystoneLDAPBackendConfigs** パラメーターを設定して、LDAP バックエンド設定の仕様を追加します。その後、必要な LDAP オプションを指定できます。

3. **keystone_domain_specific_ldap_backend.yaml** 環境ファイルのコピーを作成します。

```
$ cp /usr/share/openstack-tripleo-heat-
templates/environments/services/keystone_domain_specific_ldap_backend.yaml
/home/stack/templates/
```

4. **/home/stack/templates/keystone_domain_specific_ldap_backend.yaml** 環境ファイルを編集して、デプロイメントに適した値を設定します。たとえば、以下のパラメーターは、**testdomain** という名前の keystone ドメイン向けの LDAP 設定を作成します。

```
parameter_defaults:
  KeystoneLDAPDomainEnable: true
  KeystoneLDAPBackendConfigs:
    testdomain:
      url: ldaps://192.0.2.250
      user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
      password: RedactedComplexPassword
      suffix: dc=director,dc=example,dc=com
      user_tree_dn: ou=Users,dc=director,dc=example,dc=com
      user_filter: "(memberOf=cn=OSuser,ou=Groups,dc=director,dc=example,dc=com)"
      user_objectclass: person
      user_id_attribute: cn
```

注記

keystone_domain_specific_ldap_backend.yaml 環境ファイルには、次の非推奨の書き込みパラメーターが含まれています。

- **user_allow_create**
- **user_allow_update**
- **user_allow_delete**

これらのパラメーターの値はデプロイメントに影響を与えないため、安全に削除できます。

5. (オプション) 環境ファイルにドメインをさらに追加します。以下に例を示します。

```
KeystoneLDAPBackendConfigs:
  domain1:
    url: ldaps://domain1.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
  domain2:
    url: ldaps://domain2.example.com
```

```
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
```

これにより、**domain1** と **domain2** という名前の 2 つのドメインが指定され、各ドメインには、異なる LDAP ドメインが独自の設定で適用されます。

1.4. OPENSTACK IDENTITY ドメインへの管理ユーザーアクセス権の付与

admin ユーザーが OpenStack Identity (keystone) ドメインにアクセスして **Domain** タブを表示するのを許可するには、ドメインと **admin** ユーザーの ID を取得した後、ドメインのユーザーに **admin** ロールを割り当てます。

注記

これにより、OpenStack admin アカウントには外部サービスドメインのパーミッションは付与されません。この場合には、**ドメイン** という用語は、OpenStack が使用する keystone ドメインのことを指しています。

手順

この手順では、**LAB** ドメインを使用。ドメイン名は、設定するドメインの実際の名前に置き換えます。

1. **LAB** ドメインの ID を取得します。

```
$ openstack domain show LAB
+---------+----------------------------------+
| Field   | Value                            |
+---------+----------------------------------+
| enabled | True                             |
| id      | 6800b0496429431ab1c4efbb3fe810d4 |
| name    | LAB                              |
+---------+----------------------------------+
```

2. **default** ドメインから **admin** ユーザーの ID を取得します。

```
$ openstack user list --domain default | grep admin
| 3d75388d351846c6a880e53b2508172a | admin      |
```

3. **admin** ロールの ID を取得します。

```
$ openstack role list
```

出力は、統合する外部サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+----------------------------------+-----------------+
| ID                               | Name            |
+----------------------------------+-----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin           |
| 034e4620ed3d45969dfe8992af001514 | member          |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin   |
```

```
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader          |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator   |
| ef3d3f510a474d6c860b4098ad658a29 | service         |
+----------------------------------+-----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 544d48aaffde48f1b3c31a52c35f01f9 | SwiftOperator |
| 6d005d783bf0436e882c55c62457d33d | ResellerAdmin |
| 785c70b150ee4c778fe4de088070b4cf | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
+----------------------------------+---------------+
```

4. ドメインおよび admin の ID を使用して、keystone **LAB** ドメインの **admin** ロールに **admin** ユーザーを追加するコマンドを構築します。

```
# openstack role add --domain 6800b0496429431ab1c4efbb3fe810d4 --user
3d75388d351846c6a880e53b2508172a 785c70b150ee4c778fe4de088070b4cf
```

1.5. RED HAT OPENSTACK PLATFORM プロジェクトへの外部グループアクセス権の付与

複数の認証されたユーザーが Red Hat OpenStack Platform (RHOSP) リソースにアクセスできるようにするには、外部ユーザー管理サービスから特定のグループを承認し、RHOSP プロジェクトへのアクセス権限を付与します。この場合、OpenStack 管理者は各ユーザーをプロジェクト内のロールに手動で割り当てる必要はありません。その結果、これらのグループのすべてのメンバーは、事前に決定したプロジェクトにアクセスできます。

前提条件

- 外部サービスの管理者が以下の手順を完了していることを確認してください。
  - **grp-openstack-admin** という名前のグループの作成。
  - **grp-openstack-demo** という名前のグループの作成。
  - 必要に応じて、RHOSP ユーザーをこれらのグループの 1 つに追加。
  - ユーザーを **grp-openstack** グループに追加。
- OpenStack Identity ドメインを作成します。この手順では、**LAB** ドメインを使用。
- RHOSP プロジェクトの作成や選択を行う。以下の手順では、**openstack project create --domain default --description "Demo Project" demo** コマンドで作成した **demo** という名前のプロジェクトを使用。

手順

1. OpenStack Identity ドメインからユーザーグループのリストを取得します。

```
# openstack group list --domain LAB
```

コマンド出力は、統合する外部のユーザー管理サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+------------------------------------------------------------------+--------------------+
| ID                                                               | Name               |
+------------------------------------------------------------------+--------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-
openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-
openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-
openstack-demo  |
+------------------------------------------------------------------+--------------------+
```

- Red Hat Identity Manager (IdM):

```
+------------------------------------------------------------------+--------------------+
| ID                                                               | Name               |
+------------------------------------------------------------------+--------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-
openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-
openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-
openstack-demo  |
+------------------------------------------------------------------+--------------------+
```

2. ロールのリストを取得します。

```
# openstack role list
```

コマンド出力は、統合する外部のユーザー管理サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+--------------+
| ID                               | Name         |
```

```
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. ユーザーグループを上記のロールの 1 つまたは複数に追加して、プロジェクトへのアクセス権を付与します。たとえば、**grp-openstack-demo** グループのユーザーを **demo** プロジェクトの一般ユーザーに指定するには、統合する外部サービスに応じて、グループを **member** または **_member_** ロールに追加する必要があります。

   - Active Directory Domain Service (AD DS):

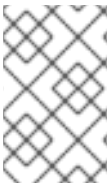
     ```
     # openstack role add --project demo --group
     d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8  member
     ```

   - Red Hat Identity Manager (IdM):

     ```
     $ openstack role add --project demo --group
     d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8
     _member_
     ```

結果

grp-openstack-demo のメンバーは、ユーザー名とパスワードを入力し、**Domain** フィールドに **LAB** を入力して Dashboard にログインすることができます。



注記

ユーザーに **Error: Unable to retrieve container list.** というエラーメッセージが表示され、コンテナーの管理が可能であることが想定されている場合には、**SwiftOperator** ロールに追加する必要があります。

関連情報

- 「Red Hat OpenStack Platform プロジェクトへの外部ユーザーアクセス権の付与」

1.6. RED HAT OPENSTACK PLATFORM プロジェクトへの外部ユーザーアクセス権の付与

grp-openstack グループからの特定認証ユーザーに OpenStack リソースへのアクセス権限を付与するには、これらのユーザーに Red Hat OpenStack Platform (RHOSP) プロジェクトへの直接アクセス権限を付与できます。グループにアクセス権を付与する代わりに、個々のユーザーにアクセス権を付与する場合は、このプロセスを使用します。

前提条件

- 外部サービスの管理者が以下の手順を完了していることを確認してください。
  - RHOSP ユーザーを **grp-openstack** グループに追加する。
  - OpenStack Identity ドメインを作成する。この手順では、**LAB** ドメインを使用。
- RHOSP プロジェクトの作成や選択を行う。以下の手順では、**openstack project create --domain default --description "Demo Project" demo** コマンドで作成した **demo** という名前のプロジェクトを使用。

手順

1. OpenStack Identity ドメインからユーザーのリストを取得します。

```
# openstack user list --domain LAB
 +----------------------------------------------------------------+----------------+
| ID                                                | Name           |
+----------------------------------------------------------------+----------------+
| 1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e | user1          |
| 12c062faddc5f8b065434d9ff6fce03eb9259537c93b411224588686e9a38bf1 | user2          |
| afaf48031eb54c3e44e4cb0353f5b612084033ff70f63c22873d181fdae2e73c | user3          |
| e47fc21dcf0d9716d2663766023e2d8dc15a6d9b01453854a898cabb2396826e | user4
|
+----------------------------------------------------------------+----------------+
```

2. ロールのリストを取得します。

```
# openstack role list
```

コマンド出力は、統合する外部のユーザー管理サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+----------------------------------+-----------------+
| ID                               | Name            |
+----------------------------------+-----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin           |
| 034e4620ed3d45969dfe8992af001514 | member          |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin   |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader          |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator   |
| ef3d3f510a474d6c860b4098ad658a29 | service         |
+----------------------------------+-----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. リスト表示されたロールの 1 つまたは複数にユーザーを追加して、RHOSP プロジェクトへのアクセス権を付与します。たとえば、**user1** を **demo** プロジェクトの一般ユーザーに指定するには、統合する外部サービスに応じて、ユーザーを **member** または **_member_** ロールに追加します。

   - Active Directory Domain Service (AD DS):

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e member
```

   - Red Hat Identity Manager (IdM):

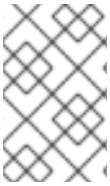
```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e _member_
```

4. **user1** を **demo** プロジェクトの管理ユーザーにするには、**admin** ロールに追加します。

```
# openstack role add --project demo --user
1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e admin
```

結果

user1 ユーザーは、外部ユーザー名とパスワードを入力し、**Domain** フィールドに **LAB** を入力して Dashboard にログインすることができます。



注記

ユーザーに **Error: Unable to retrieve container list.** というエラーメッセージが表示され、コンテナーの管理が可能であることが想定されている場合には、**SwiftOperator** ロールに追加する必要があります。

関連情報

- 「Red Hat OpenStack Platform プロジェクトへの外部グループアクセス権の付与」

1.7. OPENSTACK IDENTITY ドメインおよびユーザーのリスト表示

利用可能なエントリーを表示するには、**openstack domain list** コマンドを使用します。Identity サービスに複数のドメインを設定すると、Dashboard のログインページに新しい **Domain** フィールドが有効になります。ユーザーは、ログイン認証情報にマッチするドメインを入力する必要があります。

重要

統合が完了したら、**Default** ドメインまたは新たに作成する keystone ドメインに新規プロジェクトを作成するかどうかを決定する必要があります。ワークフローとユーザーアカウントの管理方法を検討する必要があります。可能な場合には、**Default** ドメインを内部ドメインとして使用し、サービスアカウントと **admin** プロジェクトを管理し、外部ユーザーを別のドメインに維持します。

この例では、外部アカウントは **LAB** ドメインを指定する必要があります。**admin** のような組み込みの keystone アカウントには、ドメインに **Default** を指定する必要があります。

手順

1. ドメインのリストを表示します。

```
# openstack domain list
+----------------------------------+---------+---------+-------------------------------------------------------
---------------+
| ID                               | Name    | Enabled | Description                                                  |
+----------------------------------+---------+---------+-------------------------------------------------------
---------------+
| 6800b0496429431ab1c4efbb3fe810d4 | LAB     | True    |
|
| default                          | Default | True    | Owns users and projects available on Identity API
v2. |
+----------------------------------+---------+---------+-------------------------------------------------------
---------------+
```

2. 特定のドメインのユーザーリストを表示します。このコマンド例では、**--domain LAB** を指定し、**grp-openstack** グループのメンバーである LAB ドメイン内のユーザーを返します。

```
# openstack user list --domain LAB
```

--domain Default を追加して、組み込みの keystone アカウントを表示することもできます。

```
# openstack user list --domain Default
```

1.8. 非管理者ユーザーの認証情報ファイルの作成

OpenStack Identity のユーザーおよびドメインを設定したら、管理者以外のユーザーの認証情報ファイルを作成する必要がある場合があります。

手順

- 非管理者ユーザー用の認証情報 (RC) ファイルを作成します。この例では、ファイルで **user1** ユーザーを使用しています。

```
$ cat overcloudrc-v3-user1
# Clear any old environment that may conflict.
for key in $( set | awk '{FS="="}  /^OS_/ {print $1}' ); do unset $key ; done
export OS_USERNAME=user1
export NOVA_VERSION=1.1
export OS_PROJECT_NAME=demo
export OS_PASSWORD=RedactedComplexPassword
export OS_NO_CACHE=True
export COMPUTE_API_VERSION=1.1
export no_proxy=,10.0.0.5,192.168.2.11
export OS_CLOUDNAME=overcloud
export OS_AUTH_URL=https://10.0.0.5:5000/v3
export OS_AUTH_TYPE=password
export PYTHONWARNINGS="ignore:Certificate has no, ignore:A true
SSLContext object is not available"
export OS_IDENTITY_API_VERSION=3
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=LAB
```

1.9. OPENSTACK IDENTITY と外部のユーザー管理サービスの統合のテスト

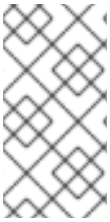
OpenStack Identity (keystone) と Active Directory Domain Service (AD DS) が正常に統合されていることをテストするには、Dashboard 機能へのユーザーアクセスをテストします。

前提条件

- Active Directory (AD) または Red Hat Identity Manager (IdM) などの外部のユーザー管理サービスとの統合

手順

1. 外部のユーザー管理サービスにテストユーザーを作成し、そのユーザーを **grp-openstack** グループに追加します。
2. Red Hat OpenStack Platform で、**demo** プロジェクトの **_member_** ロールにユーザーを追加します。
3. AD テストユーザーの認証情報を使用して Dashboard にログインします。
4. 各タブをクリックし、エラーメッセージなしに正常に表示されているかどうかを確認します。
5. Dashboard を使用してテストインスタンスをビルドします。



注記

これらの手順で問題が発生した場合は、**admin** アカウントを使用して Dashboard にログインし、そのユーザーとして後続の手順を実施します。テストが成功した場合、OpenStack が予想通りに機能していること、および OpenStack Identity と Active Directory との統合設定のどこかに問題が存在することを意味します。

関連情報

- 「Active Directory との統合のトラブルシューティング」

1.10. ACTIVE DIRECTORY との統合のトラブルシューティング

OpenStack Identity で Active Directory との統合を使用する際にエラーが発生する場合には、LDAP コネクションをテストするか、証明書トラスト設定をテストする必要がある場合があります。LDAPS ポートにアクセスできることを確認する必要がある場合もあります。

注記

エラーのタイプおよび場所に応じて、以下の手順の関連ステップのみを実行します。

手順

1. **ldapsearch** コマンドを使用して Active Directory Domain Controller に対してテストクエリーをリモートで実行して、LDAP 接続をテストします。クエリーが成功した場合には、ネットワーク接続が機能しており、AD DS サービスが稼働中であることを確認できます。以下の例では、テストクエリーはサーバー **addc.lab.local** のポート **636** に対して実行されます。

```
# ldapsearch -Z -x -H ldaps://addc.lab.local:636 -D "svc-ldap@lab.local" -W -b
"OU=labUsers,DC=lab,DC=local" -s sub "(cn=*)" cn
```

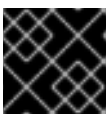
注記

- **ldapsearch** は、**openldap-clients** パッケージに含まれています。このパッケージは、**# dnf install openldap-clients** のコマンドを実行するとインストールすることができます。
- このコマンドを実行すると、ホストオペレーティングシステム内で必要な証明書が特定されるはずです。

2. **ldapsearch** コマンドのテストの際に **Peer's Certificate issuer is not recognized.** というエラーを受け取った場合には、**TLS_CACERTDIR** パスが正しく設定されていることを確認してください。以下に例を示します。

```
TLS_CACERTDIR /etc/openldap/certs
```

3. 一時的な回避策として、証明書の検証を無効にすることを検討してください。



重要

この設定は、永続的には使用しないでください。

/etc/openldap/ldap.conf で、**TLS_REQCERT** パラメーターを **allow** に設定します。

```
TLS_REQCERT allow
```

この値を設定した後に **ldapsearch** クエリーが機能した場合には、証明書トラストが正しく設定されているかどうかを確認する必要があります。

4. **nc** コマンドを使用して、LDAPS ポート **636** がリモートでアクセス可能であることを確認します。この例では、サーバー **addc.lab.local** に対してプローブを実行します。**ctrl-c** を押してプロンプトを終了します。

```
# nc -v addc.lab.local 636
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.200.10:636.
^C
```

接続を確立できなかった場合には、ファイアウォールの設定に問題がある可能性があります。

第2章 OPENSTACK IDENTITY (KEYSTONE) と RED HAT IDENTITY MANAGER (IDM) の統合

OpenStack Identity (keystone) と Red Hat Identity Manager (IdM) を統合する場合、OpenStack Identity は特定の Red Hat Identity Management (IdM) ユーザーを認証しますが、承認設定および重要なサービスアカウントは Identity サービスデータベースに保持されます。この手順を実行すると、Identity サービスは、IdM に読み取り専用でアクセスしてユーザーアカウントの認証を行う一方で、認証されたアカウントに割り当てる権限を引き続き管理するようになります。**novajoin** を使用して、ノードを IdM に登録することもできます。

注記

この統合用の設定ファイルは、Puppet によって管理されます。このため、次回 **openstack overcloud deploy** コマンドを実行すると、自分で追加したカスタム設定が上書きされる可能性があります。設定ファイルを手動で編集するのではなく、director を使用して LDAP 認証を設定できます。

IdM 統合を計画して設定する前に、以下の主要な項目を確認してください。

- **認証**: パスワードを使用して、ユーザーが本人であることを検証するプロセス。
- **承認**: 認証されたユーザーに対して、アクセスしようとしているシステムの適切なパーミッションが付与されていることを確認するプロセス。
- **ドメイン**: Identity サービス内で設定する追加のバックエンド。たとえば、Identity サービスは、外部の IdM 環境内のユーザーを認証するように設定することができます。このように設定されたユーザーの集合は、**ドメイン** として考えることができます。

OpenStack Identity と IdM を統合するプロセスには、以下の段階が含まれています。

1. novajoin を使用して、アンダークラウドおよびオーバークラウドを IdM に登録する
2. Ansible を使用して、アンダークラウドおよびオーバークラウドに TLS-e を実装する
3. IdM サーバーの認証情報を設定し、LDAPS 証明書をエクスポートする
4. OpenStack に LDAPS 証明書をインストールおよび設定する
5. 1 つまたは複数の LDAP バックエンドを使用するように director を設定する
6. IdM バックエンドにアクセスするようにコントローラーノードを設定する
7. OpenStack プロジェクトへの IdM ユーザーまたはグループのアクセスを設定する
8. ドメインおよびユーザーリストが正しく作成されていることを確認する
9. (オプション) 管理者以外のユーザーの認証情報ファイルを作成する

2.1. RED HAT IDENTITY MANAGER (IDM) との統合の計画

OpenStack Identity と Red Hat Identity Manager (IdM) の統合を計画する際には、両方のサービスが設定され稼動状態にあることを確認し、ユーザー管理、およびファイアウォール設定に対する統合の影響を確認してください。

前提条件

- Red Hat Identity Management が設定済みで、稼働していること。
- Red Hat OpenStack Platform が設定済みで、稼働していること。
- DNS 名前解決が完全に機能しており、かつ全ホストが適切に登録されていること。

アクセス権限およびロール

この統合により、IdM ユーザーが OpenStack に対して認証を実行して、リソースにアクセスできるようになります。OpenStack のサービスアカウント (keystone、glance など) および承認管理 (パーミッションとロール) は Identity サービスのデータベースに残ります。パーミションとロールは、Identity サービスの管理ツールを使用して IdM アカウントに割り当てられます。

高可用性のオプション

この設定により、単一の IdM サーバーの可用性に依存するようになるため、Identity サービスがその IdM サーバー に対して認証できない場合には、プロジェクトユーザーが影響を受けることになります。別の IdM サーバーが使用できなくなった場合に別の IdM サーバーにクエリーを実行するように keystone を設定したり、ロードバランサーを使用したりできます。この設定ではクライアントにフェイルオーバーが実装されているため、SSSD で IdM を使用する場合はロードバランサーを使用しないでください。

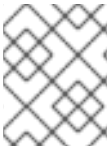
停止の要件

- IdM バックエンドを追加するには、Identity サービスを再起動する必要があります。
- ユーザーは、IdM でアカウントが作成されるまでは、Dashboard にアクセスできません。ダウンタイムを短縮するには、この変更の前に十分余裕をもって IdM アカウントのプレステージを行うことを検討してください。

ファイアウォールの設定

IdM と OpenStack 間の通信は、以下で設定されています。

- ユーザーの認証
- IdM によるコントローラーからの証明書失効リスト (CRL) の取得 (2 時間ごと)
- 有効期限が切れた時点で Certmonger による新しい証明書の要求



注記

最初の要求が失敗した場合に、certmonger の定期的なタスクで引き続き新しい証明書が要求されます。

ファイアウォールが IdM と OpenStack の間のトラフィックをフィルタリングしている場合には、以下のポートを介したアクセスを許可する必要があります。

ソース	送信先	タイプ	ポート
OpenStack コントローラーノード	Red Hat Identity Management	LDAPS	TCP 636

2.2. OPENSTACK 向けの IDENTITY MANAGEMENT (IDM) サーバーの推奨事項

Red Hat では IdM サーバーと OpenStack 環境の統合が円滑に進むように、以下の情報を提供しています。

IdM インストール用に Red Hat Enterprise Linux を準備する方法は、Identity Management のインストール を参照してください。

ipa-server-installコマンドを実行して、IdM をインストールおよび設定します。コマンドパラメーターを使用すると対話型プロンプトをスキップできます。IdM サーバーを Red Hat Open Stack Platform 環境と統合できるように、以下の推奨事項を使用してください。

表2.1 パラメーターの推奨事項

オプション	推奨事項
--admin-password	指定した値をメモしておいてください。Red Hat Open Stack Platform を IdM と連携するように設定するときに、このパスワードが必要になります。
--ip-address	指定した値をメモしておいてください。アンダークラウドノードとオーバークラウドノードには、この IP アドレスへのネットワークアクセスが必要です。
--setup-dns	このオプションを使用して、IdM サーバーに統合 DNS サービスをインストールします。アンダークラウドノードとオーバークラウドノードは、ドメイン名の解決に IdM サーバーを使用します。
--auto-forwarders	このオプションを使用して、**/etc/resolv.conf**のアドレスを DNS フォワーダーとして使用します。
--auto-reverse	このオプションを使用して、IdM サーバーの IP アドレスのリバースレコードとゾーンを解決します。リバースレコードもゾーンも解決できない場合には、IdM はリバースゾーンを作成します。こうすることで IdM のデプロイメントが簡素化されます。
--ntp-server, **--ntp-pool**	これらのオプションの両方またはいずれかを使用して、NTP ソースを設定できます。Id M サーバーと Open Stack 環境の両方で、時間が正しく同期されている必要があります。

Red Hat Open Stack Platform ノードとの通信を有効にするには、IdM に必要なファイアウォールポートを開く必要があります。詳細は、IdM に必要なポートの解放 を参照してください。

関連情報

- Identity Management の設定および管理
- Red Hat Identity Management のドキュメント

2.3. ANSIBLE を使用した TLS-E の実装

新しい **tripleo-ipa** メソッドを使用して、どこでも TLS (TLS-e) と呼ばれるオーバークラウドエンドポイントで SSL/TLS を有効にすることができます。必要な証明書の数が多いため、Red Hat OpenStack Platform は Red Hat Identity Management (IdM) と統合されています。**tripleo-ipa** を使用して TLS-e を設定する場合、IdM が認証局です。

前提条件

- stack ユーザーの作成など、アンダークラウドの設定手順がすべて完了していること。詳細は、director のインストールと使用方法 を参照してください。
- DNS サーバーの IP アドレスは、アンダークラウド上で IdM サーバーの IP アドレスに設定されます。以下のパラメーターのいずれかを **undercloud.conf** ファイルに設定する必要があります。
  - **DEFAULT/undercloud_nameservers**
  - **%SUBNET_SECTION%/dns_nameservers**

手順

次の手順で、Red Hat OpenStack Platform の新規インストール、または TLS-e で設定する既存のデプロイメントに TLS-e を実装します。事前にプロビジョニングされたノードに TLS-e を設定した Red Hat OpenStack Platform をデプロイする場合は、この方式を使用する必要があります。

注記

既存の環境に TLS-e を実装している場合は、**openstack undercloud install** や **openstack overcloud deploy** などのコマンドを実行する必要があります。これらの手順はべき等性を持ち、更新されたテンプレートおよび設定ファイルと一致するように既存のデプロイメント設定を調整するだけです。

1. **/etc/resolv.conf** ファイルを設定します。
   アンダークラウドの **/etc/resolv.conf** に、適切な検索ドメインおよびネームサーバーを設定します。たとえば、デプロイメントドメインが **example.com** で FreeIPA サーバーのドメインが **bigcorp.com** の場合、以下の行を /etc/resolv.conf に追加します。

```
search example.com bigcorp.com
nameserver $IDM_SERVER_IP_ADDR
```

2. 必要なソフトウェアをインストールします。

```
sudo dnf install -y python3-ipalib python3-ipaclient krb5-devel
```

3. ご自分の環境に固有の値で環境変数をエクスポートします。

```
export IPA_DOMAIN=bigcorp.com
export IPA_REALM=BIGCORP.COM
export IPA_ADMIN_USER=$IPA_USER (1)
export IPA_ADMIN_PASSWORD=$IPA_PASSWORD (2)
export IPA_SERVER_HOSTNAME=ipa.bigcorp.com
```

```
export UNDERCLOUD_FQDN=undercloud.example.com 3
export USER=stack
export CLOUD_DOMAIN=example.com
```

1 2 IdM のユーザー認証情報は、新しいホストおよびサービスを追加できる管理ユーザーでなければなりません。

3 **UNDERCLOUD_FQDN** パラメーターの値は、**/etc/hosts** の最初のホスト名から IP へのマッピングと一致します。

4. アンダークラウドで **undercloud-ipa-install.yaml** Ansible Playbook を実行します。

```
ansible-playbook \
--ssh-extra-args "-o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null" \
/usr/share/ansible/tripleo-playbooks/undercloud-ipa-install.yaml
```

5. undercloud.conf に以下のパラメーターを追加します。

```
undercloud_nameservers = $IDM_SERVER_IP_ADDR
overcloud_domain_name = example.com
```

6. [オプション] IPA レルムが IPA ドメインと一致しない場合は、**certmonger_krb_realm** パラメーターの値を設定します。

   a. **/home/stack/hiera_override.yaml** で **certmonger_krb_realm** の値を設定します。

   ```
   parameter_defaults:
     certmonger_krb_realm = EXAMPLE.COMPANY.COM
   ```

   b. **undercloud.conf** で **custom_env_files** パラメーターの値を **/home/stack/hiera_override.yaml** に設定します。

   ```
   custom_env_files = /home/stack/hiera_override.yaml
   ```

7. アンダークラウドをデプロイします。

```
openstack undercloud install
```

検証

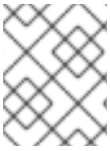
以下の手順を実施して、アンダークラウドが正しく登録されたことを確認します。

1. IdM のホストをリスト表示します。

```
$ kinit admin
$ ipa host-find
```

2. アンダークラウドに **/etc/novajoin/krb5.keytab** が存在することを確認します。

```
ls /etc/novajoin/krb5.keytab
```



注記

novajoin というディレクトリー名は、従来の方式に対応させる目的でのみ使用されています。

オーバークラウドでの TLS-e の設定

TLS everywhere (TLS-e) を設定したオーバークラウドをデプロイする場合、アンダークラウドおよびオーバークラウドの IP アドレスは自動的に IdM に登録されます。

1. オーバークラウドをデプロイする前に、以下のような内容で YAML ファイル **tls-parameters.yaml** を作成します。お使いの環境に固有の値を選択してください。

```
parameter_defaults:
    DnsSearchDomains: ["example.com"]
    CloudDomain: example.com
    CloudName: overcloud.example.com
    CloudNameInternal: overcloud.internalapi.example.com
    CloudNameStorage: overcloud.storage.example.com
    CloudNameStorageManagement: overcloud.storagemgmt.example.com
    CloudNameCtlplane: overcloud.ctlplane.example.com
    IdMServer: freeipa-0.redhat.local
    IdMDomain: redhat.local
    IdMInstallClientPackages: False

resource_registry:
      OS::TripleO::Services::IpaClient: /usr/share/openstack-tripleo-heat-
templates/deployment/ipa/ipaservices-baremetal-ansible.yaml
```

   - **OS::TripleO::Services::IpaClient** パラメーターに示す値は、**enable-internal-tls.yaml** ファイルのデフォルト設定を上書きします。**openstack overcloud deploy** コマンドで、**enable-internal-tls.yaml** の後に **tls-parameters.yaml** ファイルを指定するようにします。

   - TLS-e の実装に使用するパラメーターの詳細は、tripleo-ipa のパラメーター を参照してください。

2. オーバークラウドをデプロイする。デプロイメントコマンドに tls-parameters.yaml を追加する必要があります。

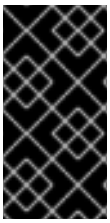
```
DEFAULT_TEMPLATES=/usr/share/openstack-tripleo-heat-templates/
CUSTOM_TEMPLATES=/home/stack/templates

openstack overcloud deploy \
-e ${DEFAULT_TEMPLATES}/environments/ssl/tls-everywhere-endpoints-dns.yaml \
-e ${DEFAULT_TEMPLATES}/environments/services/haproxy-public-tls-certmonger.yaml \
-e ${DEFAULT_TEMPLATES}/environments/ssl/enable-internal-tls.yaml \
-e ${CUSTOM_TEMPLATES}/tls-parameters.yaml \
...
```

3. keystone にエンドポイントリストのクエリーを行い、各エンドポイントが HTTPS を使用していることを確認します。

```
openstack endpoint list
```

2.4. TLS EVERYWHERE (TLS-E) による MEMCACHED トラフィックの暗号化



重要

この機能は、本リリースでは **テクノロジープレビュー** として提供しているため、Red Hat では全面的にはサポートしていません。これは、テスト用途にのみご利用いただく機能です。実稼働環境にはデプロイしないでください。テクノロジープレビュー機能についての詳細は、対象範囲の詳細 を参照してください。

memcached トラフィックを TLS-e で暗号化できるようになりました。この機能は、novajoin と tripleo-ipa の両方で機能します。

1. 以下の内容で **memcached.yaml** という名前の環境ファイルを作成し、memcached の TLS サポートを追加します。

```
parameter_defaults:
  MemcachedTLS: true
  MemcachedPort: 11212
```

2. オーバークラウドのデプロイプロセスに **memcached.yaml** 環境ファイルを追加します。

```
openstack overcloud deploy --templates \
-e /usr/share/openstack-tripleo-heat-templates/environments/ssl/enable-internal-tls.yaml \
-e /usr/share/openstack-tripleo-heat-templates/environments/ssl/tls-everywhere-endpoints-dns.yaml \
-e /usr/share/openstack-tripleo-heat-templates/environments/services/haproxy-public-tls-certmonger.yaml \
-e /home/stack/memcached.yaml
...
```

関連情報

- tripleo-ipa を使用した TLSe のデプロイに関する詳細は、Ansible を使用した TLS-e の実装 を参照してください。

2.5. RED HAT IDENTITY MANAGER (IDM) サーバーの認証情報の設定

Red Hat Identity Manager (IdM) が OpenStack Identity と統合するように設定するには、Identity サービスが使用する LDAP アカウントを設定して、Red Hat OpenStack ユーザーのユーザーグループを作成し、ルックアップアカウントのパスワードを設定します。

前提条件

- Red Hat Identity Manager (IdM) が設定済みで、稼働していること。
- Red Hat OpenStack Platform (RHOSP) が設定済みで、稼働していること。
- DNS 名前解決が完全に機能しており、かつ全ホストが適切に登録されていること。
- IdM 認証トラフィックが LDAPS で暗号化され、ポート 636 を使用していること。

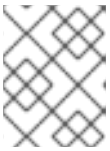
- 推奨: 単一の障害点を避けるために、高可用性または負荷分散ソリューションを備えた IdM を実装していること。

手順

IdM サーバーで以下の手順を実行します。

1. OpenStack Identity サービスで使用する LDAP ルックアップアカウントを作成して、IdM LDAP サービスにクエリーを実行します。

```
# kinit admin
# ipa user-add
First name: OpenStack
Last name: LDAP
User  [radministrator]: svc-ldap
```



注記

作成が完了したら、このアカウントのパスワード期限の設定を確認してください。

2. **grp-openstack** という名前の RHOSP ユーザーグループを作成します。OpenStack Identity でパーミッションを割り当てることができるのは、このグループのメンバーのみです。

```
# ipa group-add --desc="OpenStack Users" grp-openstack
```

3. **svc-ldap** アカウントのパスワードを設定して、**grp-openstack** グループに追加します。

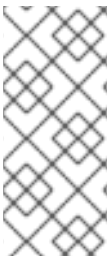
```
# ipa passwd svc-ldap
# ipa group-add-member --users=svc-ldap grp-openstack
```

4. **svc-ldap** ユーザーとしてログインし、プロンプトが表示されたらパスワードを変更します。

```
# kinit svc-ldap
```

2.6. RED HAT IDENTITY MANAGER (IDM) LDAPS 証明書のインストール

OpenStack Identity (keystone) は、LDAPS クエリーを使用してユーザーアカウントを検証します。このトラフィックを暗号化するために、keystone は **keystone.conf** で定義されている証明書ファイルを使用します。LDAPS 証明書をインストールするには、Red Hat Identity Manager (IdM) サーバーから keystone が参照できる場所に証明書をコピーし、それを **.crt** から **.pem** 形式に変換します。



注記

LDAP 認証に複数のドメインを使用する場合、**Unable to retrieve authorized projects** または **Peer's Certificate issuer is not recognized** など、さまざまなエラーが発生する可能性があります。これは、keystone が特定ドメインに誤った証明書を使用すると発生する可能性があります。回避策として、すべての LDAPS 公開鍵を単一の **.crt** バンドルにマージし、このファイルを使用するようにすべての keystone ドメインを設定します。

前提条件

- IdM サーバーの認証情報が設定されている。

手順

1. IdM の環境で、LDAPS 証明書を見つけます。このファイルの場所は、**/etc/openldap/ldap.conf** で確認することができます。

```
TLS_CACERT /etc/ipa/ca.crt
```

2. keystone サービスを実行しているコントローラーノードにファイルをコピーします。たとえば、**scp** コマンドは **ca.crt** ファイルを **node.lab.local** にコピーします。

```
# scp /etc/ipa/ca.crt root@node.lab.local:/root/
```

3. **ca.crt** ファイルを証明書のディレクトリーにコピーします。keystone サービスは、この場所を使用して証明書にアクセスします。

```
# cp ca.crt /etc/pki/ca-trust/source/anchors
```

4. (オプション) **ldapsearch** などの診断のコマンドを実行する必要がある場合には、RHEL の証明書ストアに証明書を追加する必要もあります。

   a. 3.コントローラーノードで **.crt** を **.pem** 形式に変換します。

```
# openssl x509 -in ca.crt -out ca.pem -outform PEM
```

   b. コントローラーノードに **.pem** をインストールします。たとえば、Red Hat Enterprise Linux の場合は以下を実行します。

```
# cp ca.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust
```

2.7. ドメイン固有の LDAP バックエンドを使用する DIRECTOR の設定

director が 1 つ以上の LDAP バックエンドを使用するように設定するには、heat テンプレートで **KeystoneLDAPDomainEnable** フラグを **true** に設定し、各 LDAP バックエンドに関する情報が含まれる環境ファイルを設定します。次に、director は keystone ドメインごとに別の LDAP バックエンドを使用します。

注記

ドメイン設定ファイルのデフォルトのディレクトリーは **/etc/keystone/domains/** に設定されています。**keystone::domain_config_directory** hiera キーを使用して環境ファイル内に **ExtraConfig** パラメーターを追加して必要なパスを設定することによってオーバーライドすることができます。

手順

1. デプロイメントの heat テンプレートで、**KeystoneLDAPDomainEnable** フラグを **true** に設定します。これにより、**identity** 設定グループ内の keystone に **domain_specific_drivers_enabled** オプションが設定されます。

2. **tripleo-heat-templates** に **KeystoneLDAPBackendConfigs** パラメーターを設定して、LDAP バックエンド設定の仕様を追加します。その後、必要な LDAP オプションを指定できます。

3. **keystone_domain_specific_ldap_backend.yaml** 環境ファイルのコピーを作成します。

```
$ cp /usr/share/openstack-tripleo-heat-
templates/environments/services/keystone_domain_specific_ldap_backend.yaml
/home/stack/templates/
```

4. **/home/stack/templates/keystone_domain_specific_ldap_backend.yaml** 環境ファイルを編集して、デプロイメントに適した値を設定します。たとえば、以下のパラメーターは、**testdomain** という名前の keystone ドメイン向けの LDAP 設定を作成します。

```
parameter_defaults:
  KeystoneLDAPDomainEnable: true
  KeystoneLDAPBackendConfigs:
    testdomain:
      url: ldaps://192.0.2.250
      user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
      password: RedactedComplexPassword
      suffix: dc=director,dc=example,dc=com
      user_tree_dn: ou=Users,dc=director,dc=example,dc=com
      user_filter: "(memberOf=cn=OSuser,ou=Groups,dc=director,dc=example,dc=com)"
      user_objectclass: person
      user_id_attribute: cn
```

注記

keystone_domain_specific_ldap_backend.yaml 環境ファイルには、次の非推奨の書き込みパラメーターが含まれています。

- **user_allow_create**
- **user_allow_update**
- **user_allow_delete**

これらのパラメーターの値はデプロイメントに影響を与えないため、安全に削除できます。

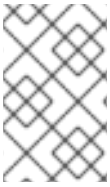
5. (オプション) 環境ファイルにドメインをさらに追加します。以下に例を示します。

```
KeystoneLDAPBackendConfigs:
  domain1:
    url: ldaps://domain1.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
  domain2:
    url: ldaps://domain2.example.com
    user: cn=openstack,ou=Users,dc=director,dc=example,dc=com
    password: RedactedComplexPassword
    ...
```

これにより、**domain1** と **domain2** という名前の 2 つのドメインが指定され、各ドメインには、異なる LDAP ドメインが独自の設定で適用されます。

2.8. OPENSTACK IDENTITY ドメインへの管理ユーザーアクセス権の付与

admin ユーザーが OpenStack Identity (keystone) ドメインにアクセスして **Domain** タブを表示するのを許可するには、ドメインと **admin** ユーザーの ID を取得した後、ドメインのユーザーに **admin** ロールを割り当てます。



注記

これにより、OpenStack admin アカウントには外部サービスドメインのパーミッションは付与されません。この場合には、**ドメイン** という用語は、OpenStack が使用する keystone ドメインのことを指しています。

手順

この手順では、**LAB** ドメインを使用。ドメイン名は、設定するドメインの実際の名前に置き換えます。

1. **LAB** ドメインの ID を取得します。

```
$ openstack domain show LAB
+---------+----------------------------------+
| Field   | Value                            |
+---------+----------------------------------+
| enabled | True                             |
| id      | 6800b0496429431ab1c4efbb3fe810d4 |
| name    | LAB                              |
+---------+----------------------------------+
```

2. **default** ドメインから **admin** ユーザーの ID を取得します。

```
$ openstack user list --domain default | grep admin
| 3d75388d351846c6a880e53b2508172a | admin      |
```

3. **admin** ロールの ID を取得します。

```
$ openstack role list
```

出力は、統合する外部サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+----------------------------------+-----------------+
| ID                               | Name            |
+----------------------------------+-----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin           |
| 034e4620ed3d45969dfe8992af001514 | member          |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin   |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader          |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator   |
| ef3d3f510a474d6c860b4098ad658a29 | service         |
+----------------------------------+-----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+--------------+
| ID                               | Name         |
+----------------------------------+--------------+
| 544d48aaffde48f1b3c31a52c35f01f9 | SwiftOperator |
| 6d005d783bf0436e882c55c62457d33d | ResellerAdmin |
| 785c70b150ee4c778fe4de088070b4cf | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
+----------------------------------+--------------+
```

4. ドメインおよび admin の ID を使用して、keystone **LAB** ドメインの **admin** ロールに **admin** ユーザーを追加するコマンドを構築します。

```
# openstack role add --domain 6800b0496429431ab1c4efbb3fe810d4 --user
3d75388d351846c6a880e53b2508172a 785c70b150ee4c778fe4de088070b4cf
```

2.9. RED HAT OPENSTACK PLATFORM プロジェクトへの外部グループアクセス権の付与

複数の認証されたユーザーが Red Hat OpenStack Platform (RHOSP) リソースにアクセスできるようにするには、外部ユーザー管理サービスから特定のグループを承認し、RHOSP プロジェクトへのアクセス権限を付与します。この場合、OpenStack 管理者は各ユーザーをプロジェクト内のロールに手動で割り当てる必要はありません。その結果、これらのグループのすべてのメンバーは、事前に決定したプロジェクトにアクセスできます。

前提条件

- 外部サービスの管理者が以下の手順を完了していることを確認してください。
  - **grp-openstack-admin** という名前のグループの作成。
  - **grp-openstack-demo** という名前のグループの作成。
  - 必要に応じて、RHOSP ユーザーをこれらのグループの 1 つに追加。
  - ユーザーを **grp-openstack** グループに追加。
- OpenStack Identity ドメインを作成します。この手順では、**LAB** ドメインを使用。
- RHOSP プロジェクトの作成や選択を行う。以下の手順では、**openstack project create --domain default --description "Demo Project" demo** コマンドで作成した **demo** という名前のプロジェクトを使用。

手順

1. OpenStack Identity ドメインからユーザーグループのリストを取得します。

```
# openstack group list --domain LAB
```

コマンド出力は、統合する外部のユーザー管理サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+------------------------------------------------------------------+--------------------+
| ID                                                               | Name               |
```

```
+------------------------------------------------------------------+--------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-
openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-
openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-
openstack-demo  |
+------------------------------------------------------------------+--------------------+
```

- Red Hat Identity Manager (IdM):

```
+------------------------------------------------------------------+--------------------+
| ID                                                               | Name               |
+------------------------------------------------------------------+--------------------+
| 185277be62ae17e498a69f98a59b66934fb1d6b7f745f14f5f68953a665b8851 | grp-
openstack       |
| a8d17f19f464c4548c18b97e4aa331820f9d3be52654aa8094e698a9182cbb88 | grp-
openstack-admin |
| d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8 | grp-
openstack-demo  |
+------------------------------------------------------------------+--------------------+
```

2. ロールのリストを取得します。

```
# openstack role list
```

コマンド出力は、統合する外部のユーザー管理サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+--------------+
| ID                               | Name         |
+----------------------------------+--------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin        |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_     |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+--------------+
```

3. ユーザーグループを上記のロールの 1 つまたは複数に追加して、プロジェクトへのアクセス権

を付与します。たとえば、**grp-openstack-demo** グループのユーザーを **demo** プロジェクトの一般ユーザーに指定するには、統合する外部サービスに応じて、グループを **member** または **_member_** ロールに追加する必要があります。

- Active Directory Domain Service (AD DS):

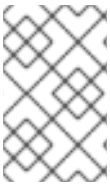
```
# openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8  member
```

- Red Hat Identity Manager (IdM):

```
$ openstack role add --project demo --group
d971bb3bd5e64a454cbd0cc7af4c0773e78d61b5f81321809f8323216938cae8
_member_
```

結果

grp-openstack-demo のメンバーは、ユーザー名とパスワードを入力し、**Domain** フィールドに **LAB** を入力して Dashboard にログインすることができます。



注記

ユーザーに **Error: Unable to retrieve container list.** というエラーメッセージが表示され、コンテナーの管理が可能であることが想定されている場合には、**SwiftOperator** ロールに追加する必要があります。

関連情報

- 「Red Hat OpenStack Platform プロジェクトへの外部ユーザーアクセス権の付与」

2.10. RED HAT OPENSTACK PLATFORM プロジェクトへの外部ユーザーアクセス権の付与

grp-openstack グループからの特定認証ユーザーに OpenStack リソースへのアクセス権限を付与するには、これらのユーザーに Red Hat OpenStack Platform (RHOSP) プロジェクトへの直接アクセス権限を付与できます。グループにアクセス権を付与する代わりに、個々のユーザーにアクセス権を付与する

場合は、このプロセスを使用します。

前提条件

- 外部サービスの管理者が以下の手順を完了していることを確認してください。
  - RHOSP ユーザーを **grp-openstack** グループに追加する。
  - OpenStack Identity ドメインを作成する。この手順では、**LAB** ドメインを使用。
- RHOSP プロジェクトの作成や選択を行う。以下の手順では、**openstack project create --domain default --description "Demo Project" demo** コマンドで作成した **demo** という名前のプロジェクトを使用。

手順

1. OpenStack Identity ドメインからユーザーのリストを取得します。

```
# openstack user list --domain LAB
 +------------------------------------------------------------------+----------------+
| ID                                                               | Name           |
+------------------------------------------------------------------+----------------+
| 1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e | user1          |
| 12c062faddc5f8b065434d9ff6fce03eb9259537c93b411224588686e9a38bf1 | user2          |
| afaf48031eb54c3e44e4cb0353f5b612084033ff70f63c22873d181fdae2e73c | user3          |
| e47fc21dcf0d9716d2663766023e2d8dc15a6d9b01453854a898cabb2396826e | user4
|
+------------------------------------------------------------------+----------------+
```

2. ロールのリストを取得します。

```
# openstack role list
```

コマンド出力は、統合する外部のユーザー管理サービスによって異なります。

- Active Directory Domain Service (AD DS):

```
+----------------------------------+----------------+
| ID                               | Name           |
+----------------------------------+----------------+
| 01d92614cd224a589bdf3b171afc5488 | admin          |
| 034e4620ed3d45969dfe8992af001514 | member         |
| 0aa377a807df4149b0a8c69b9560b106 | ResellerAdmin  |
| 9369f2bf754443f199c6d6b96479b1fa | heat_stack_user |
| cfea5760d9c948e7b362abc1d06e557f | reader         |
| d5cb454559e44b47aaa8821df4e11af1 | swiftoperator  |
| ef3d3f510a474d6c860b4098ad658a29 | service        |
+----------------------------------+----------------+
```

- Red Hat Identity Manager (IdM):

```
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 0969957bce5e4f678ca6cef00e1abf8a | ResellerAdmin |
```

```
| 1fcb3c9b50aa46ee8196aaaecc2b76b7 | admin         |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| d3570730eb4b4780a7fed97eba197e1b | SwiftOperator |
+----------------------------------+---------------+
```

3. リスト表示されたロールの 1 つまたは複数にユーザーを追加して、RHOSP プロジェクトへのアクセス権を付与します。たとえば、**user1** を **demo** プロジェクトの一般ユーザーに指定するには、統合する外部サービスに応じて、ユーザーを **member** または **_member_** ロールに追加します。

   - Active Directory Domain Service (AD DS):

     ```
     # openstack role add --project demo --user
     1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e member
     ```

   - Red Hat Identity Manager (IdM):

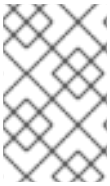
     ```
     # openstack role add --project demo --user
     1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e _member_
     ```

4. **user1** を **demo** プロジェクトの管理ユーザーにするには、**admin** ロールに追加します。

   ```
   # openstack role add --project demo --user
   1f24ec1f11aeb90520079c29f70afa060d22e2ce92b2eba7784c841ac418091e admin
   ```

結果

user1 ユーザーは、外部ユーザー名とパスワードを入力し、**Domain** フィールドに **LAB** を入力して Dashboard にログインすることができます。



注記

ユーザーに **Error: Unable to retrieve container list.** というエラーメッセージが表示され、コンテナーの管理が可能であることが想定されている場合には、**SwiftOperator** ロールに追加する必要があります。

関連情報

- 「Red Hat OpenStack Platform プロジェクトへの外部グループアクセス権の付与」

2.11. OPENSTACK IDENTITY ドメインおよびユーザーのリスト表示

利用可能なエントリーを表示するには、**openstack domain list** コマンドを使用します。Identity サービスに複数のドメインを設定すると、Dashboard のログインページに新しい **Domain** フィールドが有効になります。ユーザーは、ログイン認証情報にマッチするドメインを入力する必要があります。

重要

統合が完了したら、**Default** ドメインまたは新たに作成する keystone ドメインに新規プロジェクトを作成するかどうかを決定する必要があります。ワークフローとユーザーアカウントの管理方法を検討する必要があります。可能な場合には、**Default** ドメインを内部ドメインとして使用し、サービスアカウントと **admin** プロジェクトを管理し、外部ユーザーを別のドメインに維持します。

この例では、外部アカウントは **LAB** ドメインを指定する必要があります。**admin** のような組み込みの keystone アカウントには、ドメインに **Default** を指定する必要があります。

手順

1. ドメインのリストを表示します。

```
# openstack domain list
+----------------------------------+---------+---------+----------------------------------------------------------------
---------------+
| ID                               | Name    | Enabled | Description                                                    |
+----------------------------------+---------+---------+----------------------------------------------------------------
---------------+
| 6800b0496429431ab1c4efbb3fe810d4 | LAB     | True    |
|
| default                          | Default | True    | Owns users and projects available on Identity API
v2. |
+----------------------------------+---------+---------+----------------------------------------------------------------
---------------+
```

2. 特定のドメインのユーザーリストを表示します。このコマンド例では、**--domain LAB** を指定し、**grp-openstack** グループのメンバーである LAB ドメイン内のユーザーを返します。

```
# openstack user list --domain LAB
```

--domain Default を追加して、組み込みの keystone アカウントを表示することもできます。

```
# openstack user list --domain Default
```

2.12. 非管理者ユーザーの認証情報ファイルの作成

OpenStack Identity のユーザーおよびドメインを設定したら、管理者以外のユーザーの認証情報ファイルを作成する必要がある場合があります。

手順

- 非管理者ユーザー用の認証情報 (RC) ファイルを作成します。この例では、ファイルで **user1** ユーザーを使用しています。

```
$ cat overcloudrc-v3-user1
# Clear any old environment that may conflict.
for key in $( set | awk '{FS="="}  /^OS_/ {print $1}' ); do unset $key ; done
export OS_USERNAME=user1
export NOVA_VERSION=1.1
export OS_PROJECT_NAME=demo
export OS_PASSWORD=RedactedComplexPassword
export OS_NO_CACHE=True
export COMPUTE_API_VERSION=1.1
export no_proxy=,10.0.0.5,192.168.2.11
export OS_CLOUDNAME=overcloud
export OS_AUTH_URL=https://10.0.0.5:5000/v3
export OS_AUTH_TYPE=password
export PYTHONWARNINGS="ignore:Certificate has no, ignore:A true
SSLContext object is not available"
export OS_IDENTITY_API_VERSION=3
export OS_PROJECT_DOMAIN_NAME=Default
export OS_USER_DOMAIN_NAME=LAB
```

2.13. OPENSTACK IDENTITY と外部のユーザー管理サービスの統合のテスト

OpenStack Identity (keystone) と Active Directory Domain Service (AD DS) が正常に統合されていることをテストするには、Dashboard 機能へのユーザーアクセスをテストします。

前提条件

- Active Directory (AD) または Red Hat Identity Manager (IdM) などの外部のユーザー管理サービスとの統合

手順

1. 外部のユーザー管理サービスにテストユーザーを作成し、そのユーザーを **grp-openstack** グループに追加します。
2. Red Hat OpenStack Platform で、**demo** プロジェクトの **_member_** ロールにユーザーを追加します。
3. AD テストユーザーの認証情報を使用して Dashboard にログインします。
4. 各タブをクリックし、エラーメッセージなしに正常に表示されているかどうかを確認します。
5. Dashboard を使用してテストインスタンスをビルドします。

注記

これらの手順で問題が発生した場合は、**admin** アカウントを使用して Dashboard にログインし、そのユーザーとして後続の手順を実施します。テストが成功した場合、OpenStack が予想通りに機能していること、および OpenStack Identity と Active Directory との統合設定のどこかに問題が存在することを意味します。

関連情報

- 「Active Directory との統合のトラブルシューティング」

2.14. RED HAT IDENTITY MANAGER (IDM) の統合に関するトラブルシューティング

OpenStack Identity で Red Hat Identity Manager (IdM) との統合を使用する際にエラーが発生する場合には、LDAP コネクションをテストするか、証明書トラスト設定をテストする必要がある場合があります。LDAPS ポートにアクセスできることを確認する必要がある場合もあります。

注記

エラーのタイプおよび場所に応じて、以下の手順の関連ステップのみを実行します。

手順

1. **ldapsearch** コマンドを使用して IdM サーバーに対してテストクエリーをリモートで実行して、LDAP 接続をテストします。クエリーが成功した場合には、ネットワーク接続が機能しており、IdM サービスが稼働中であることを確認できます。以下の例では、テストクエリーはサーバー **idm.lab.local** のポート **636** に対して実行されます。

```
# ldapsearch -D "cn=directory manager" -H ldaps://idm.lab.local:636 -b "dc=lab,dc=local" -s sub "(objectclass=*)" -w RedactedComplexPassword
```

注記

ldapsearch は、**openldap-clients** パッケージに含まれています。このパッケージは、**# dnf install openldap-clients** のコマンドを実行するとインストールすることができます。

2. **nc** コマンドを使用して、LDAPS ポート **636** がリモートでアクセス可能であることを確認します。この例では、サーバー **idm.lab.local** に対してプローブを実行します。**ctrl-c** を押してプロンプトを終了します。

```
# nc -v idm.lab.local 636
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.200.10:636.
^C
```

接続を確立できなかった場合には、ファイアウォールの設定に問題がある可能性があります。