



Red Hat OpenStack Platform

9

ユーザーおよびアイデンティティ管理ガイド

ユーザーおよび認証メカニズムの管理

OpenStack Team

Red Hat OpenStack Platform 9 ユーザーおよびアイデンティティ管理ガイド

ユーザーおよび認証メカニズムの管理

OpenStack Team
rhos-docs@redhat.com

法律上の通知

Copyright © 2017 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

ユーザーおよびアイデンティティ管理ガイドでは、Red Hat OpenStack Platform 環境のユーザーロール、クォータ、プロジェクト、プロジェクトセキュリティ、Identity サービスの管理手順を説明します。

目次

前書き	3
第1章 ユーザーとロール管理	4
1.1. ユーザー管理	4
1.2. ロールの管理	5
1.3. クォータ管理	7
第2章 プロジェクト管理	11
2.1. プロジェクト管理	11
2.2. プロジェクトのセキュリティー管理	13
2.3. IDENTITY サービスの階層式マルチテナント	15
第3章 アイデンティティー管理	16
3.1. セキュアな LDAP 通信	16

前書き

クラウドの管理者は、プロジェクト、ユーザー、ロールを管理することができます。プロジェクトとは、ユーザーの割り当てが可能な、クラウド内の組織単位のこと、テナントまたはアカウントとしても知られています。ユーザーは、1つまたは複数のプロジェクトのメンバーにすることができ、ロールは、ユーザーが実行できるアクションを定義します。

各 OpenStack デプロイメントには、最低でもプロジェクト、ユーザー、ロールが1つずつあり、それらが連携している必要があります。クラウド管理者は、プロジェクトとユーザーの追加、更新、削除、1つまたは複数のプロジェクトへのユーザーの割り当てを行うことができます。プロジェクトとユーザーは、個別に管理することが可能です。

Keystone Identity サービスでユーザー認証を設定して、サービスおよびエンドポイントへのアクセスを制御することも可能です。Keystone では、トークンベースの認証が提供され、LDAP と Active Directory と統合することができるため、ユーザーとアイデンティティを外部で管理し、Keystone とユーザーデータを同期できます。

第1章 ユーザーとロール管理

1.1. ユーザー管理

クラウド管理者は、Dashboard でユーザーの追加、変更、削除ができます。ユーザーは、1 つまたは複数のプロジェクトに所属することができます。また、プロジェクトとユーザーは個別に管理することができます。

1.1.1. ユーザーの作成

Dashboard でユーザーを作成するには、以下の手順に従ってください。主要なプロジェクトとロールをユーザーに割り当てることができます。Dashboard で作成したユーザーは、デフォルトでは Keystone のユーザーとなっています。Active Directory ユーザーを統合するには、Red Hat OpenStack Platform の Identity サービスに含まれる LDAP プロバイダーを設定してください。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > ユーザー** を選択します。
2. **ユーザーの作成** をクリックします。
3. ユーザーのユーザー名、メールアドレス、仮のパスワードを入力します。
4. **主プロジェクト** のリストからプロジェクトを選択します。
5. **ロール** のリストからロールを選択します (デフォルトは `_member_` です)。
6. **ユーザーの作成** をクリックします。

1.1.2. ユーザーの編集

以下の手順に従って、主プロジェクトなど、ユーザーの詳細を更新します。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > ユーザー** を選択します。
2. ユーザーの **アクション** コラムで、**編集** をクリックします。
3. **ユーザーの更新** ウィンドウで、**ユーザー名**、**メール**、**主プロジェクト** を更新できます。
4. **ユーザーの更新** をクリックします。

1.1.3. ユーザーの有効化/無効化

以下の手順に従って、ユーザーを有効化または無効化します。1 度に 1 ユーザーしか無効化または有効化できません。無効化されたユーザーは Dashboard にはログインできず、OpenStack サービスへのアクセスもできません。また、無効化されたユーザーの主プロジェクトもアクティブに設定できません。アクションを元に戻せないユーザーの削除とは異なり、無効化されたユーザーをもう 1 度有効化することができます。また、ユーザーが無効な場合には、Dashboard のユーザーとプロジェクトのアクションを実行するには、ユーザーを有効化する必要があります。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > ユーザー** を選択します。

2. **アクション** コラムでドロップダウンリストをクリックし、**ユーザーの有効化** または **ユーザーの無効化** を選択すると、**有効** コラムの値が **True** または **False** に更新されます。

1.1.4. ユーザーの削除

管理者ユーザーが Dashboard を使用してユーザーを削除するには、以下の手順を実行します。このアクションは、ユーザーの無効化とは異なり、元に戻すことはできません。ユーザーを無効にした場合には、所属するプロジェクトのメンバー一覧から削除されます。ユーザーとプロジェクトのペアに関連付けられたロールはすべて失われます。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > ユーザー** を選択します。
2. 削除するユーザーを選択します。
3. **ユーザーの削除** をクリックします。**ユーザーの削除の確認** ウィンドウが表示されます。
4. **ユーザーの削除** をクリックしてアクションを確認します。

1.2. ロールの管理

OpenStack はロールベースアクセス制御 (RBAC) のメカニズムを使用して、リソースへのアクセスを管理します。ロールは、ユーザーが実行可能なアクションを定義します。デフォルトでは、テナントにアタッチされるメンバーロールと、管理者以外のユーザーが環境を管理できるようにする管理者ロールという事前定義済みのロールが 2 つあります。パーミッションには抽象レベルがあり、管理者が必要なロールを作成して適切にサービスを設定することができる点に注意してください。

1.2.1. ロールの表示

利用可能な事前定義済みのロールを一覧表示するには、以下のコマンドを使用します。

```
$ keystone role-list
+-----+-----+
|          id          |      name      |
+-----+-----+
| 71ccc37d41c8491c975ae72676db687f |      Member     |
| 149f50a1fe684bfa88dae76a48d26ef7 | ResellerAdmin  |
| 9fe2ff9ee4384b1894a90878d3e92bab |    _member_    |
| 6ecf391421604da985db2f141e46a7c8 |      admin     |
+-----+-----+
```

指定したロールの詳細を取得するには、以下のコマンドを実行します。

```
$ keystone role-get [ROLE]
```

例

```
$ keystone role-get admin
+-----+-----+
| Property |      Value      |
+-----+-----+
```

id	6ecf391421604da985db2f141e46a7c8
name	admin

1.2.2. ロールの作成および割り当て

クラウド管理者は、以下のコマンドー式を使用して Keystone クライアントでロールを作成、管理できます。各 OpenStack のデプロイメントには、最低でもプロジェクト、ユーザー、ロールが 1 つずつ必要で、それぞれ連携されている必要があります。ただし、ユーザーは複数のプロジェクトのメンバーになることができます。複数のプロジェクトにユーザーを割り当てるには、ロールを作成して、ユーザーとプロジェクトのペアにそのロールを割り当てます。Dashboard でユーザーを作成して、主プロジェクトとデフォルトのロールを割り当てることができる点に注意してください。



注記

ユーザー、ロール、プロジェクトの指定には名前または ID を使用することができます。

1. **new-role** という名前のロールを作成します。

```
$ keystone role-create --name [ROLE_NAME]
```

例

```
$ keystone role-create --name new-role
+-----+-----+
| Property | Value |
+-----+-----+
| id       | 61013e7aa4ba4e00a0a1ab4b14bc6b2a |
| name     | new-role |
+-----+-----+
```

2. ユーザーをプロジェクトに割り当てるには、ロールをユーザーとプロジェクトのペアに割り当てる必要があります。これには、ユーザー、ロール、プロジェクト名/ID を取得してください。

- a. ユーザーを一覧表示します。

```
$ keystone user-list
```

- b. ロールを一覧表示します。

```
$ keystone role-list
```

- c. プロジェクトを一覧表示します。

```
$ keystone tenant-list
```

3. ユーザーとプロジェクトのペアにロールを割り当てます。

```
$ keystone user-role-add --user [USER_NAME] --role [ROLE_NAME] --tenant [TENANT_NAME]
```

例

以下の例では、**new-role** ロールが **demo** と **demo** のペアに割り当てられます。

```
$ keystone user-role-add --user demo --role new-role --tenant demo
```

4. **demo** のロール割り当てを確認するには、以下のコマンドを実行します。

```
$ keystone user-role-list --user [USER_NAME] --tenant [TENANT_NAME]
```

例

```
$ keystone user-role-list --user demo --tenant demo
```

1.2.3. ロールの削除

1. ユーザーとプロジェクトのペアからロールを削除するには、以下のコマンドを使用します。ロールが削除されると、ユーザーとプロジェクトのペアの関連性も削除されます。

```
$ keystone user-role-remove --user [USER_NAME] --role [ROLE] --tenant [TENANT_NAME]
```

2. ロールが削除されていることを確認します。

```
$ keystone user-role-list --user [USER_NAME] --tenant [TENANT_NAME]
```

ロールが削除された場合、そのロールはコマンドの出力から省略されます。

1.3. クォータ管理

クラウド管理者は、プロジェクトのクォータを設定、管理できます。各プロジェクトには、リソースが割り当てられており、プロジェクトユーザーには、これらのリソースを消費するアクセス権が授与されています。これにより、それぞれのパーミッションやリソースを干渉することなく、複数のプロジェクトが単一のクラウドを使用できるようにします。リソースクォータセットは、新規テナントの作成時に事前設定されます。クォータには、テナントに割り当て可能な仮想 CPU、インスタンス、Floating IP の数量が含まれます。クォータは、テナント (またはプロジェクト) およびテナントとユーザーレベルの両方で強制できます。Dashboard を使用して新規/既存のテナントのコンピュートまたは Block Storage クォータを設定または変更できる点に注意してください。Dashboard でのプロジェクトクォータの設定および更新の手順については、「[2章 プロジェクト管理](#)」を参照してください。

1.3.1. ユーザーのコンピュートクォータの表示

ユーザーに現在設定されているクォータの値を一覧表示するには、以下のコマンドを実行します。

```
$ nova quota-show --user [USER] --tenant [TENANT]
```

例

```
$ nova quota-show --user demoUser --tenant demo
+-----+-----+
| Quota          | Limit |
+-----+-----+
| instances      | 10    |
| cores          | 20    |
| ram            | 51200 |
| floating_ips   | 5     |
| fixed_ips      | -1    |
| metadata_items | 128   |
| injected_files | 5     |
| injected_file_content_bytes | 10240 |
| injected_file_path_bytes  | 255   |
| key_pairs      | 100   |
| security_groups | 10    |
| security_group_rules | 20    |
| server_groups  | 10    |
| server_group_members | 10    |
+-----+-----+
```

1.3.2. ユーザーのコンピュータクォータの更新

特定のクォータ値を更新するには、以下のコマンドを実行します。

```
$ nova quota-update --user [USER] --[QUOTA_NAME] [QUOTA_VALUE] [TENANT]
$ nova quota-show --user [USER] --tenant [TENANT]
```

例

```
$ nova quota-update --user demoUser --floating-ips 10 demo
$ nova quota-show --user demoUser --tenant demo
+-----+-----+
| Quota          | Limit |
+-----+-----+
| instances      | 10    |
| cores          | 20    |
| ram            | 51200 |
| floating_ips   | 10    |
| ...            |       |
+-----+-----+
```

注記

quota-update コマンドのオプション一覧を表示するには、以下を実行します。

```
$ nova help quota-update
```

1.3.3. ユーザーのオブジェクトストレージクォータの設定

オブジェクトストレージクォータは、以下のカテゴリーに分類できます。

- ※ コンテナクォータ: 合計サイズ (バイト単位) または単一のコンテナで保存可能なオブジェクト数を制限します。
- ※ アカウントクォータ: Object Storage サービスでユーザーが利用可能な合計サイズ (バイト単位) を制限します。

コンテナクォータまたはアカウントクォータのいずれかを設定するには、Object Storage プロキシサーバーにおいて、**proxy-server.conf** ファイルの **[pipeline:main]** セクションに **container_quotas** または **account_quotas** (または両方) のパラメーターを追加する必要があります。

```
[pipeline:main]
pipeline = catch_errors [...] tempauth container-quotas \
account-quotas slo dlo proxy-logging proxy-server

[filter:account_quotas]
use = egg:swift#account_quotas

[filter:container_quotas]
use = egg:swift#container_quotas
```

オブジェクトストレージクォータの表示および更新には、以下のコマンドを使用します。プロジェクトに含まれるすべてのユーザーには、そのプロジェクトに指定されているクォータが表示されます。プロジェクトに設定されているオブジェクトストレージのクォータを更新するには、そのプロジェクトの ResellerAdmin のロールが必要です。

アカウントクォータを表示するには、以下のコマンドを実行します。

```
# swift stat

Account: AUTH_b36ed2d326034beba0a9dd1fb19b70f9
Containers: 0
Objects: 0
Bytes: 0
Meta Quota-Bytes: 214748364800
X-Timestamp: 1351050521.29419
Content-Type: text/plain; charset=utf-8
Accept-Ranges: bytes
```

クォータを更新するには、以下を実行します。

```
# swift post -m quota-bytes:<BYTES>
```

たとえば、アカウントに 5 GB のクォータを指定します。

```
# swift post -m quota-bytes:5368709120
```

クォータの確認をするには **swift stat** コマンドをもう 1 度実行します。

```
# swift stat
```

```
Account: AUTH_b36ed2d326034beba0a9dd1fb19b70f9
```

```
Containers: 0
```

```
Objects: 0
```

```
Bytes: 0
```

```
Meta Quota-Bytes: 5368709120
```

```
X-Timestamp: 1351541410.38328
```

```
Content-Type: text/plain; charset=utf-8
```

```
Accept-Ranges: bytes
```

第2章 プロジェクト管理

2.1. プロジェクト管理

クラウド管理者は、プロジェクト (テナント) を作成、管理することができます。テナントは、OpenStack ユーザーとリソースの割り当て数とプロジェクトのことです。テナントごとにクォータを設定することができます。これにより、プロジェクト間のパーミッションやリソースを干渉することなく、複数のプロジェクトが単一のクラウドを使用できるようになります。プロジェクトとテナントの用語はいずれも同じ意味で使用されます。ユーザーは、複数のプロジェクトに割り当てることができます。ユーザーとプロジェクトのペアごとに、ロールを 1 つ割り当てる必要があります。

2.1.1. プロジェクトの作成

プロジェクトの作成、プロジェクトへのメンバーの追加、プロジェクトのリソース制限の設定は、以下の手順を実行します。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > プロジェクト** を選択します。
2. **プロジェクトの作成** をクリックします。
3. **プロジェクト情報** タブでプロジェクトの名前と説明を入力します (**有効** のチェックボックスはデフォルトで選択されます)。
4. プロジェクトへのメンバーの追加は、**プロジェクトメンバー** タブの **すべてのユーザー** リストから行います。
5. **クォータ** タブで、プロジェクトのリソースの上限を指定します。
6. **プロジェクトの作成** をクリックします。

2.1.2. プロジェクトの編集

プロジェクトを編集して名前や説明を変更したり、プロジェクトを有効化または一時的に無効化したり、メンバーを更新したりすることができます。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > プロジェクト** を選択します。
2. プロジェクトの **アクション** コラムで、下向きの三角をクリックして **プロジェクトの編集** をクリックします。
3. **プロジェクトの編集** ウィンドウでプロジェクトを更新して名前や説明を変更したり、プロジェクトを有効化または一時的に無効化したりすることができます。
4. **プロジェクトメンバー** タブで、必要に応じてメンバーをプロジェクトに追加または削除します。
5. **保存** をクリックします。



注記

有効 のチェックボックスはデフォルトで選択されています。プロジェクトを一時的に無効にするには、**有効** のチェックボックスのチェックマークを外します。無効なプロジェクトを有効にするには、**有効** チェックボックスを選択します。

2.1.3. プロジェクトの削除

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > プロジェクト** を選択します。
2. 削除するプロジェクトを選択します。
3. **プロジェクトの削除** をクリックします。**プロジェクトの削除の確認** ウィンドウが表示されます。
4. **プロジェクトの削除** をクリックしてアクションを確認します。

プロジェクトが削除され、ユーザーとのペアリングの関連付けは解除されます。

2.1.4. プロジェクトクォータの更新

クォータとは、クラウドリソースを最適化するためにプロジェクトごとに設定可能な操作の制約のことです。クォータを設定して、通知なしにプロジェクトのリソースが使い果たされないようにします。クォータは、プロジェクトレベルとプロジェクトとユーザーレベルの両方で実行できます。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > プロジェクト** を選択します。
2. プロジェクトの **アクション** コラムで、下向きの三角をクリックして **クォータの変更** をクリックします。
3. **クォータ** タブで、必要に応じてプロジェクトクォータを変更します。
4. **保存** をクリックします。

2.1.5. 現在のプロジェクトの変更

ユーザーは、メンバーとなっているプロジェクトのみ、現在のプロジェクトとして設定することができます。また、**現在のプロジェクトに設定** オプションを有効にするには、ユーザーが複数のプロジェクトのメンバーである必要があります。現在のプロジェクトとして設定すると、現在のプロジェクトとして指定されたプロジェクトのオブジェクトに、Dashboard からアクセスできるようになります。無効にしたプロジェクトは、有効化しない限り、現在のプロジェクトとして設定できません。

1. Dashboard に管理ユーザーとしてログインして **アイデンティティ > プロジェクト** を選択します。
2. プロジェクトの **アクション** コラムで、下向きの三角をクリックして **現在のプロジェクトに設定** をクリックします。

3. または、管理者権限のないユーザーで、プロジェクトの **アクション** コラムの下向きの三角をクリックして **現在のプロジェクトに設定** をクリックすると、このコラムのデフォルトアクションになります。

2.2. プロジェクトのセキュリティー管理

セキュリティーグループとは、プロジェクトのインスタンスに割り当て可能な IP フィルターのルールセットで、インスタンスへのネットワークのアクセス権限を定義します。セキュリティーグループはプロジェクト別になっており、プロジェクトメンバーは自分のセキュリティーグループのデフォルトルールを編集して新規ルールセットを追加することができます。

プロジェクトにはすべて default セキュリティーグループが存在し、他にセキュリティーグループが定義されていないインスタンスに対して適用されます。このセキュリティーグループは、デフォルト値を変更しない限り、お使いのインスタンスへの受信トラフィックをすべて拒否し、送信トラフィックのみを許可します。

2.2.1. セキュリティーグループの作成

1. Dashboard で **プロジェクト > コンピュート > アクセスとセキュリティー** を選択します。
2. **セキュリティーグループ** タブで、**セキュリティーグループの作成** をクリックします。
3. セキュリティーグループに名前と説明を指定して、**セキュリティーグループの作成** をクリックします。

2.2.2. セキュリティーグループのルールの追加

デフォルトでは、新しいグループには、送信アクセスのルールのみが指定されます。他のアクセスを指定するには、新しいルールを追加する必要があります。

1. Dashboard で **プロジェクト > コンピュート > アクセスとセキュリティー** を選択します。
2. **セキュリティーグループ** タブで、編集するセキュリティーグループの **ルールの管理** をクリックします。
3. 新規ルールを追加するには、**ルールの追加** をクリックします。
4. ルールの値を指定して、**追加** をクリックします。

以下のルールのフィールドは必須です。

ルール

ルールタイプ。ルールテンプレート (例: **SSH**) を指定する場合には、そのフィールドは自動的に入力されます。

- ※ TCP: 一般的には、システム間のデータの交換や、エンドユーザーの通信に使用されます。
- ※ UDP: 一般的には、システム間のデータ交換に (特にアプリケーションレベルで) 使用されます。
- ※ ICMP: 一般的には、ルーターなどのネットワークデバイスがエラーや監視メッセージを送信するのに使用されます。

方向

受信 (インバウンド) または送信 (アウトバウンド)

開放するポート

TCP または UDP ルールでは、開放する **ポート** または **ポート範囲** (単一のポートまたはポートの範囲) を入力します。

- ※ ポート範囲では、**ポート番号 (下限)** と **ポート番号 (上限)** にポートの値を入力します。
- ※ 単一のポートの場合は **ポート** フィールドにポートの値を入力します。

タイプ

ICMP ルールのタイプ。 **-1:255** の範囲で指定する必要があります。

コード

ICMP ルールのコード。 **-1:255** の範囲で指定する必要があります。

接続相手

このルールが適用されるトラフィックの接続元

- ※ CIDR (Classless Inter-Domain Routing): 指定のブロック内の IP へのアクセスを制限する IP アドレスブロック。接続相手フィールドに CIDR を入力します。
- ※ セキュリティーグループ: グループ内のインスタンスが他のグループインスタンスにアクセスできるようにするソースのセキュリティーグループ

2.2.3. セキュリティーグループルールの削除

1. Dashboard で **プロジェクト > コンピュート > アクセスとセキュリティー** を選択します。
2. **セキュリティーグループ** タブで、セキュリティーグループの **ルールの管理** をクリックします。
3. セキュリティーグループルールを選択し、**イメージの削除** ボタンをクリックします。
4. 再度、**ルールの削除** をクリックします。



注記

削除の操作は元に戻すことはできません。

2.2.4. セキュリティーグループの削除

1. Dashboard で **プロジェクト > コンピュート > アクセスとセキュリティー** を選択します。
2. **セキュリティーグループ** タブで、グループを選択して、**セキュリティーグループの削除** をクリックします。
3. **セキュリティーグループの削除** をクリックします。

**注記**

削除の操作は元に戻すことはできません。

2.3. IDENTITY サービスの階層式マルチテナント

マルチテナンシーとは、ソフトウェアアプリケーションの単一インスタンスで複数の顧客にサービスを提供するアーキテクチャーのことです。クラウドコンピューティングでは、仮想化やリモートアクセスを活用する新サービスモデルが登場し、マルチテナンシーアーキテクチャーはより広い意味を持つようになりました。たとえば、Software-as-a-Service (SaaS) プロバイダーは、データベースのインスタンス 1 つでアプリケーションのインスタンス 1 つを実行し、複数の顧客が Web にアクセスできるようにします。このようなシナリオでは、各テナントのデータは分離されており、他のテナントには表示されません。

OpenStack Identity サービス (**keystone**) では、マルチテナンシーを使用してプロジェクトをネスト化します。ドメインは、ユーザー、グループ、プロジェクトのコレクションのことで、それぞれ 1 つのドメインにより所有されています。ユーザーは、他のドメインが所有するプロジェクトなど、プロジェクトのユーザーにロールを割り当てることで複数のプロジェクトに関連付けることができます。プロジェクトは、リソースのコンテナのことで、クォータや仮想マシンイメージへのアクセス権を定義します。

マルチテナンシーは、Red Hat OpenStack Platform 9 ではテクノロジープレビューとして提供されています。テクノロジープレビューとして提供されている機能のサポートスコープに関する詳しい情報は、<https://access.redhat.com/support/offerings/techpreview/> を参照してください。

第3章 アイデンティティ管理

3.1. セキュアな LDAP 通信

Identity サービス (Keystone) が LDAP サーバーに対して認証を行うか、LDAP サーバーから識別情報を取得するように設定した場合に、CA 証明書を使用して Identity サービスの LDAP 通信をセキュリティ保護することができます。

本項では、Active Directory から CA 証明書を取得する方法、CA 証明書ファイルを Privacy Enhanced Mail (PEM) ファイル形式に変換する方法、Identity サービスの LDAP 通信をセキュアに設定する 3 つの方法について説明します。それぞれの方法での手順は、CA トラストが設定された場所および方法に応じて実行するようにしてください。

3.1.1. Active Directory から CA 証明書を取得する方法

以下のコードは、Active Directory に対してクエリーを実行して CA 証明書を取得する方法の例を示しています。CA_NAME は証明書の名前に置き換え (mmc.exe で確認可能)、その他のパラメーターは実際の設定に応じて変更することができます。

```
CA_NAME="WIN2012DOM-WIN2012-CA"
AD_SUFFIX="dc=win2012dom,dc=com"
LDAPURL="ldap://win2012.win2012dom.com"
ADMIN_DN="cn=Administrator,cn=Users,$AD_SUFFIX"
ADMINPASSWORD="MyPassword"

CA_CERT_DN="cn=latexmath:[$CA_NAME,cn=certification
authorities,cn=public key
services,cn=services,cn=configuration,$]AD_SUFFIX"

TMP_CACERT=/tmp/cacert.`date +%Y%m%d%H%M%S`.$.pem

ldapsearch -xLLL -H
latexmath:[$LDAPURL -D `echo \"\$]ADMIN_DN\"` -W -s base -b`echo
\"$CA_CERT_DN\"` objectclass=* cACertificate
```

3.1.2. CA 証明書を PEM ファイル形式に変換する方法

/path/cacert.pem という名前のファイルを作成し、以下の例に示したように、Active Directory から CA 証明書を取得するための LDAP クエリーの内容をヘッダーとフッターの間に追加します。

```
-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIQD14hh1Yz7tPFLXCKKU0szANB... -----END
CERTIFICATE-----
```

トラブルシューティングを行う場合には、以下のクエリーを実行して LDAP が稼働しているかをチェックし、PEN 証明書ファイルが正しく作成されたことを確認してください。

```
LDAPTLS_CACERT=/path/cacert.pem ldapsearch -xLLL -ZZ -H $LDAPURL -s
base -b "" "objectclass=*" currenttime
```

このクエリーによって、以下のような結果が返されるはずです。

```
dn: currentTime:
20141022050611.0Z
```

CA 証明書が Web サーバーでホストされていた場合には、以下のコマンドを実行して CA 証明書を取得することができます。

例

```
✎ $HOST=redhat.com
```

```
✎ $PORT=443
```

```
# echo Q | openssl s_client -connect $HOST:$PORT | sed -n -e
'/BEGIN CERTIFICATE/,/END CERTIFICATE/ p'
```

3.1.3. Identity サービスのセキュアな LDAP 通信を設定する方法

3.1.3.1. 方法 1

CA 信頼が PEM ファイルを使用して LDAP レベルで設定されている場合は、この方法を使用してください。CA 証明書ファイルの場所は手動で指定します。以下の手順では、Identity サービスのみでなく、OpenLDAP ライブラリーを使用する全アプリケーションの LDAP 通信がセキュリティー保護されます。

1. CA 証明書チェーンが含まれているファイルを PEM 形式で **/etc/openldap/certs** ディレクトリーにコピーします。
2. **/etc/openldap/ldap.conf** を編集して以下のディレクティブを追加します。
[CA_FILE] は CA 証明書ファイルの場所と名前に置き換えます。

```
TLS_CACERT /etc/openldap/certs/[CA_FILE]
```

3. **openstack-keystone** サービスを再起動します。

```
# systemctl restart openstack-keystone.service
```

3.1.3.2. 方法 2

CA 信頼が Network Security Services (NSS) データベースを介して LDAP ライブラリーレベルで設定されている場合は、この方法を使用してください。**certutil** コマンドを使用して、OpenLDAP ライブラリーが使用する NSS 証明書データベースに CA 証明書をインポートして信頼します。以下の手順では、Identity サービスのみでなく、OpenLDAP ライブラリーを使用する全アプリケーションの LDAP 通信がセキュリティー保護されます。

1. 証明書をインポートして信頼します。[CA_FILE] は CA 証明書ファイルの場所と名前に置き換えます。

```
# certutil -d /etc/openldap/certs -A -n "My CA" -t CT,, -a -i
[CA_FILE]
```

2. CA 証明書が正しくインポートされていることを確認します。

■

```
# certutil -d /etc/openldap/certs -L
```

CA 証明書がリストされ、信頼の属性が **CT,,** に設定されます。

3. **openstack-keystone** サービスを再起動します。

```
# systemctl restart openstack-keystone.service
```

3.1.3.3. 方法 3

CA 信頼が PEM ファイルを使用して Keystone レベルで設定されている場合は、この方法を使用してください。Identity サービスと LDAP サーバー間の通信をセキュリティ保護する最後のメソッドは、Identity サービスに TLS を設定する方法です。

ただし、上記の 2 つのメソッドとは異なり、このメソッドでは、Identity サービスの LDAP 通信のみがセキュリティ保護され、OpenLDAP ライブラリーを使用する他のアプリケーションの LDAP 通信はセキュリティ保護されません。

以下の手順では、**openstack-config** コマンドを使用して **/etc/keystone/keystone.conf** ファイル内の値を編集します。

1. TLS を有効化します。

```
# openstack-config --set /etc/keystone/keystone.conf ldap use_tls
True
```

2. 証明書の場所を指定します。[CA_FILE] は CA 証明書ファイルの名前に置き換えます。

```
# openstack-config --set /etc/keystone/keystone.conf ldap
tls_cacertfile [CA_FILE]
```

3. LDAP サーバーから受信した TLS セッションに対して実行するクライアント証明書チェックを指定します。[CERT_BEHAVIOR] は以下にあげる動作のいずれか 1 つに置き換えてください。

demand

LDAP サーバーにより証明書が常に要求されます。証明書が提供されなかった場合、または提供された証明書が既存の認証局ファイルに対して検証できなかった場合には、セッションは終了します。

allow

LDAP サーバーにより証明書が常に要求されます。証明書が提供されなくてもセッションは通常どおりに続行されます。証明書が提供されたが、既存の認証局ファイルに対して検証できなかった場合には、その証明書は無視され、セッションは通常通りに続行します。

never

証明書は一切要求されません。

```
# openstack-config --set /etc/keystone/keystone.conf ldap
tls_req_cert [CERT_BEHAVIOR]
```

4. **openstack-keystone** サービスを再起動します。

```
# systemctl restart openstack-keystone.service
```