



# Red Hat Enterprise Linux 7

## コンテナ Identity Management サービスの使用

コンテナ Identity Management サービスの概要とインストール



# Red Hat Enterprise Linux 7 コンテナ Identity Management サービスの使用

---

コンテナ Identity Management サービスの概要とインストール

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

Copyright © 2023 | You need to change the HOLDER entity in the en-US/Using\_Containerized\_Identity\_Management\_Services.ent file |.

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

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

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

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

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

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

The OpenStack<sup>®</sup> 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

Red Hat Enterprise Linux 7 でのコンテナ Identity Management サービスについて学び、使い始めます。

## 目次

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>第1章 コンテナ IDENTITY MANAGEMENT サービスの概要</b> .....                 | <b>4</b>  |
| 1.1. IPA-SERVER および SSSD コンテナの概要                                  | 4         |
| 関連情報                                                              | 4         |
| 1.2. 利用可能なコンテナイメージ                                                | 4         |
| rhel7/ipa-server コンテナイメージ                                         | 4         |
| rhel7/sssdc コンテナイメージ                                              | 4         |
| 関連情報                                                              | 5         |
| 1.3. コンテナで IDENTITY MANAGEMENT を使用する利点と欠点                         | 5         |
| 利点                                                                | 5         |
| 短所                                                                | 5         |
| <b>パート I. IPA-SERVER CONTAINER (TECHNOLOGY PREVIEW) の使用</b> ..... | <b>6</b>  |
| <b>第2章 コンテナへの IDENTITY MANAGEMENT サーバーのデプロイ</b> .....             | <b>7</b>  |
| 2.1. 前提条件                                                         | 7         |
| 2.2. サーバーおよびレプリケートコンテナで利用可能な設定                                    | 7         |
| 利用可能                                                              | 7         |
| 利用不可                                                              | 7         |
| 2.3. コンテナへの IDENTITY MANAGEMENT サーバーのインストール基本的なインストール             | 8         |
| 作業を開始する前に                                                         | 8         |
| 手順                                                                | 8         |
| 2.4. コンテナへの IDENTITY MANAGEMENT サーバーのインストール外部 CA                  | 9         |
| 作業を開始する前に                                                         | 10        |
| 手順                                                                | 10        |
| 2.5. コンテナへの IDENTITY MANAGEMENT サーバーのインストールCA なし                  | 11        |
| 作業を開始する前に                                                         | 12        |
| 手順                                                                | 12        |
| 2.6. インストール後の次のステップ                                               | 13        |
| <b>第3章 コンテナへの IDENTITY MANAGEMENT レプリカのデプロイ</b> .....             | <b>14</b> |
| 3.1. 前提条件                                                         | 14        |
| 3.2. サーバーおよびレプリケートコンテナで利用可能な設定                                    | 14        |
| 利用可能                                                              | 14        |
| 利用不可                                                              | 14        |
| 3.3. コンテナへの IDENTITY MANAGEMENT レプリカのインストール基本的なインストール             | 15        |
| 作業を開始する前に                                                         | 15        |
| 手順                                                                | 15        |
| 3.4. コンテナへの IDENTITY MANAGEMENT レプリカのインストールCA なし                  | 17        |
| 作業を開始する前に                                                         | 17        |
| 手順                                                                | 17        |
| 3.5. インストール後の次のステップ                                               | 19        |
| <b>第4章 コンテナからホストシステムへのサーバーの移行</b> .....                           | <b>20</b> |
| 4.1. IDENTITY MANAGEMENT サーバーの、コンテナからホストシステムへの移行                  | 20        |
| 手順                                                                | 20        |
| <b>第5章 サーバーおよびレプリカコンテナのアンインストール</b> .....                         | <b>21</b> |
| 5.1. サーバーまたはレプリカコンテナのアンインストール                                     | 21        |
| 手順                                                                | 21        |
| 5.2. アンインストール後の次のステップ                                             | 21        |
| <b>パート II. SSSD コンテナの使用</b> .....                                 | <b>22</b> |

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>第6章 ATOMIC HOST で ID および認証サービスを提供するための SSSD コンテナの設定</b> ..... | <b>23</b> |
| 6.1. 前提条件                                                        | 23        |
| 6.2. 特権のある SSSD コンテナを使用した IDENTITY MANAGEMENT ドメインの登録            | 23        |
| 前提条件                                                             | 23        |
| 手順                                                               | 24        |
| 6.3. SSSD CONTAINER を使用した ACTIVE DIRECTORY ドメインのジョイン             | 25        |
| 手順                                                               | 25        |
| 関連情報                                                             | 26        |
| <b>第7章 異なる設定を含む SSSD コンテナのデプロイ</b> .....                         | <b>27</b> |
| 7.1. 前提条件                                                        | 27        |
| 7.2. SSSD コンテナを起動し、これをアイデンティティリソースにジョインさせる                       | 27        |
| 7.3. SSSD キャッシュをアプリケーションコンテナに渡す                                  | 27        |
| <b>第8章 HBAC ルールを使用した SSSD コンテナへのアクセスの付与および制限</b> .....           | <b>28</b> |
| <b>第9章 集中化された KERBEROS 認証情報キャッシュの作成と使用</b> .....                 | <b>29</b> |
| 9.1. 前提条件                                                        | 29        |
| 9.2. SSSD CONTAINER を使用した ACTIVE DIRECTORY ドメインのジョイン             | 29        |
| 手順                                                               | 29        |
| 関連情報                                                             | 30        |
| 9.3. コンテナで実行中の SSSD の認証                                          | 30        |
| 9.4. 異なるコンテナでの SSSD KERBEROS キャッシュの使用                            | 30        |
| <b>第10章 SSSD コンテナの更新</b> .....                                   | <b>32</b> |
| 手順                                                               | 32        |
| <b>第11章 SSSD コンテナのアンインストール</b> .....                             | <b>33</b> |
| 11.1. IDENTITY MANAGEMENT ドメインに登録された SSSD コンテナのアンインストール          | 33        |
| 手順                                                               | 33        |
| 11.2. ACTIVE DIRECTORY ドメインにジョインした SSSD コンテナのアンインストール            | 33        |
| 手順                                                               | 33        |
| <b>付録A コンテナで実行している IDM および SSSD のトラブルシューティングに関する情報の収集</b> .....  | <b>34</b> |
| A.1. ATOMIC HOST での SOSREPORT の作成                                | 34        |
| A.2. IDM および SSSD コンテナのバージョンの表示                                  | 34        |
| A.3. コンテナで実行している SSSD のデバッグログの作成                                 | 35        |
| A.4. IDM クライアントのインストールログの表示                                      | 35        |
| <b>付録B 改訂履歴</b> .....                                            | <b>37</b> |



## 第1章 コンテナ IDENTITY MANAGEMENT サービスの概要

以下のセクションでは、Red Hat Enterprise Linux におけるコンテナ Identity Management サービスの概要を説明します。



### 警告

`rhel7/ipa-server` コンテナはテクノロジープレビュー機能です。詳細は、Red Hat ナレッジベースの [Technology Preview Features Support Scope](#) を参照してください。

### 1.1. IPA-SERVER および SSSD コンテナの概要

コンテナで Identity Management または System Security Services Daemon (SSSD) を使用すると、ホストシステムからすべての Identity Management または SSSD プロセスが独立して実行されるようになります。これにより、これらのプロセスと競合せずに、ホストシステムが他のソフトウェアを実行できるようにします。



### 重要

`ipa-server` および `sssd` コンテナは、Red Hat Enterprise Linux Atomic Host システムで使用するよう設計されています。Atomic Host の詳細は、Atomic ドキュメントの [Getting Started with Atomic](#) を参照してください。

#### 関連情報

- [Overview of Containers in Red Hat Systems](#) では、コンテナの概要と仕組みについて説明しています。このガイドには、コンテナの使用に関するドキュメントへのリンクも含まれています。
- **Linux ドメイン Identity Management** の [Red Hat Identity Management の概要](#) では、Identity Management、Identity Management サーバー、Identity Management クライアントの概要を説明しています。
- [Atomic Host ドキュメント](#) では、一般的な Red Hat Enterprise Linux Atomic Host およびコンテナに関する情報を提供しています。

### 1.2. 利用可能なコンテナイメージ

#### `rhel7/ipa-server` コンテナイメージ

- Identity Management サーバーと関連サービスをコンテナで実行できます。
- Identity Management サーバーサービスを提供します。

#### `rhel7/sssd` コンテナイメージ

- コンテナで System Security Services Daemon (SSSD) を実行できます。

- Identity Management サーバーにシステムを登録するか、そのシステムを Active Directory ドメインに接続することで、ID および認証サービスを Atomic Host システムに提供します。
- その他のコンテナで実行中のアプリケーションに、ID および認証サービスを提供します。

#### 関連情報

- コンテナイメージについての詳細は、[Red Hat Container Catalog](#) を参照してください。

### 1.3. コンテナで IDENTITY MANAGEMENT を使用する利点と欠点

#### 利点

- Identity Management の設定およびデータはすべて、サブディレクトリーに分離して保持されます。
- Identity Management サーバーの移行は容易です。コンテナサブディレクトリーは、別のコンテナまたはホストシステムに移行できます。[4章 コンテナからホストシステムへのサーバーの移行](#) も併せて参照してください。

#### 短所

- Identity Management プロセスは Atomic で実行されます。たとえば、**docker** デーモンが終了する場合は、その下で実行されている Identity Management サーバーも終了します。ただし、複数のレプリカを維持すると、この欠点が発生します。
- SELinux の分離は、コンテナ内のコンポーネントには適用されません。ただし、コンポーネントはプロセス UID を使用して依然として分離されます。
  - SELinux はコンポーネント間で強制アクセス制御 (MAC) を適用することはありませんが、**sVirt** プロジェクトは MAC をコンテナ環境に適用します。これにより、コンテナ全体が他のコンテナから保護されます。
  - **ipa-server** コンテナは、Identity Management サーバー自体を実行するために必要なコンポーネントのみを実行します。コンテナは、SELinux の分離が欠落しているため、Identity Management を攻撃できるサードパーティーのコンポーネントを実行しません。
  - Atomic ドキュメントの [Secure Containers with SELinux](#) も参照してください。

## パート I. IPA-SERVER CONTAINER (TECHNOLOGY PREVIEW) の使用

このパートでは、Identity Management サーバーとレプリカをコンテナにデプロイする方法、サーバーをコンテナからホストシステムに移行する方法、最後にサーバーとレプリカコンテナをアンインストールする方法について説明します。

## 第2章 コンテナへの IDENTITY MANAGEMENT サーバーのデプロイ

本章では、新しいトポロジーを開始するための新しい Identity Management サーバーをインストールする方法を説明します。

開始する前に、「[前提条件](#)」と「[サーバーおよびレプリケートコンテナで利用可能な設定](#)」を読んでください。

以下のいずれかのインストール手順を選択します。どの認証局 (CA) 設定が状況に合っているかわからない場合は、[Linux ドメイン ID、認証、およびポリシーガイドの CA 設定の決定](#) を参照してください。

- [「コンテナへの Identity Management サーバーのインストール基本的なインストール」](#)
- [「コンテナへの Identity Management サーバーのインストール外部 CA」](#)
- [「コンテナへの Identity Management サーバーのインストールCA なし」](#)

終了後に、「[インストール後の次のステップ](#)」を読んでください。

### 2.1. 前提条件

- コンテナをインストールする前に Atomic Host システムをアップグレードします。[Red Hat Enterprise Linux Atomic Host 7 インストールおよび設定ガイドの アップグレードおよびダウングレード](#) を参照してください。

### 2.2. サーバーおよびレプリケートコンテナで利用可能な設定

利用可能

#### ドメインレベル1以降

コンテナには、ドメインレベル 0 は利用できません。[ドメインレベルの表示と引き上げ](#) も参照してください。

そのため、コンテナで実行しているサーバーは、Red Hat Enterprise Linux 7.3 以降に基づいて、Identity Management サーバーとのみレプリカ合意に加えることが可能です。

#### コンテナおよび非コンテナデプロイメントの組み合わせ

単一の Identity Management ドメイントポロジーには、コンテナベースおよび RPM ベースのサーバーの両方を追加できます。

利用不可

#### デプロイされたコンテナでのサーバーコンポーネントの変更

デプロイされたコンテナのランタイム変更は行わないでください。統合 DNS や Vault などのサーバーコンポーネントの変更または再インストールが必要な場合は、新しいレプリカを作成してください。

#### 異なる Linux ディストリビューション間でのアップグレード

`ipa-server` コンテナイメージを実行するプラットフォームは変更しないでください。たとえば、Red Hat Enterprise Linux で実行しているイメージを Fedora、Ubuntu、または CentOS に変更しないでください。同様に、Fedora、Ubuntu、または CentOS で実行しているイメージを Red Hat Enterprise Linux に変更しないでください。

Identity Management は、Red Hat Enterprise Linux の後続のバージョンへのアップグレードのみをサポートします。

## 実行中のコンテナを使用したシステムのダウングレード

`ipa-server` コンテナイメージを実行するシステムをダウングレードしないでください。

## Atomic Host 上のアップストリームコンテナ

Atomic Host で FreeIPA `ipa-server` イメージなどのアップストリームコンテナイメージはインストールしないでください。Red Hat Enterprise Linux で利用可能なコンテナイメージのみをインストールします。

## 単一の Atomic Host での複数コンテナ

単一の Atomic Host に `ipa-server` コンテナイメージのみをインストールします。

## 2.3. コンテナへの IDENTITY MANAGEMENT サーバーのインストール基本的なインストール

この手順では、統合 CA によるデフォルトの認証局 (CA) 設定で、コンテナ Identity Management サーバーをインストールする方法を説明します。

作業を開始する前に

- コンテナインストールは、`ipa-server-install` で使用している非コンテナインストールと同じデフォルト設定を使用することに注意してください。カスタム設定を指定するには、以下の手順で使用する `atomic install` コマンドに追加オプションを指定します。
  - `ipa-server` コンテナで利用できる Atomic オプション。完全な一覧は、コンテナヘルプページを参照してください。
  - `ipa-server-install` で利用できる Identity Management インストーラーオプションは、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management Server のインストールとアンインストール](#) で説明しています。

手順

1. `atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-server-install` コマンドを実行してインストールを開始します。

- コンテナには独自のホスト名が必要です。Atomic Host システムのホスト名とは異なるホスト名をコンテナに使用します。コンテナのホスト名は、DNS または `/etc/hosts` ファイルで解決できる必要があります。



### 注記

サーバーまたはレプリカコンテナをインストールしても、Atomic Host システム自体は Identity Management ドメインに登録されません。サーバーまたはレプリカに Atomic Host システムのホスト名を使用する場合は、後で Atomic Host システムを登録できなくなります。



### 重要

サーバーまたはレプリカコンテナをインストールするときは、`atomic install` で `--hostname` オプションを常に指定するようにしてください。この場合、`--hostname` は Identity Management インストーラーオプションではなく、Atomic オプションと見なされているため、`ipa-server-install` オプションの前に指定します。このインストールでは、`ipa-server-install` の後に指定した `--hostname` は無視されます。

- 統合 DNS でサーバーをインストールする場合は、**--ip-address** オプションを追加して、ネットワークから到達可能な Atomic Host のパブリック IP アドレスを指定します。**--ip-address** は複数回使用できます。



#### 警告

テスト目的のみでコンテナをインストールする場合を除き、**publish** オプションは常に使用してください。**publish** なしでは、Atomic Host システムにポートが公開されず、サーバーはコンテナ外から到達できなくなります。

2. **ipa-server-install** セットアップスクリプトが起動します。

```
The log file for this installation can be found in /var/log/ipaserver-install.log
```

```
=====
This program will set up the IPA Server.
[... output truncated ...]
```

このプロセスは、**ipa-server-install** ユーティリティを使用して非コンテナサーバーをインストールする場合と同じです。

#### 例2.1 インストールコマンドの例

**ipa-server** コンテナをインストールするためのコマンド構文:

```
$ atomic install [ --name <container_name> ] rhel7/ipa-server [ Atomic options ] [ ipa-server-install | ipa-replica-install ] [ ipa-server-install or ipa-replica-install options ]
```

**server-container** という名前のサーバーコンテナをインストールし、Identity Management サーバー設定のデフォルト値を使用するには、以下を実行します。

```
$ atomic install --name server-container rhel7/ipa-server publish --hostname server.example.com ipa-server-install --ip-address 2001:DB8::1111
```

カスタムのホスト名 (**--hostname**) と統合 DNS (**--setup-dns**) でサーバーをインストールするには、以下を実行します。

```
$ atomic install rhel7/ipa-server publish --hostname server.example.com ipa-server-install -setup-dns --ip-address 2001:DB8::1111
```

## 2.4. コンテナへの IDENTITY MANAGEMENT サーバーのインストール外部 CA

この手順では、外部 CA に属する統合 Identity Management 認証局 (CA) のでサーバーをインストールする方法を説明します。

コンテナ Identity Management サーバーおよび Atomic Host システムは、コンテナへの **バインドマウント** を使用してマウントされるファイルシステムの部分のみを共有します。そのため、外部ファイルに関連する操作は、このボリューム内から行われる必要があります。

**ipa-server** コンテナイメージは、`/var/lib/<container_name>/` ディレクトリーを使用して、Atomic Host ファイルシステムに永続的なファイルを保存します。永続ストレージボリュームは、コンテナ内の `/data/` ディレクトリーにマッピングします。

作業を開始する前に

- コンテナインストールは、**ipa-server-install** で使用している非コンテナインストールと同じデフォルト設定を使用することに注意してください。カスタム設定を指定するには、以下の手順で使用する **atomic install** コマンドに追加オプションを指定します。
  - **ipa-server** コンテナで利用できる Atomic オプション。完全な一覧は、コンテナヘルプページを参照してください。
  - **ipa-server-install** で使用できる Identity Management インストーラーオプションは、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management Server のインストールとアンインストール](#) で説明しています。

手順

1. **atomic install rhel7/ipa-server publish --hostname fully\_qualified\_domain\_name ipa-server-install --external-ca** コマンドを実行してインストールを開始します。

- コンテナには独自のホスト名が必要です。Atomic Host システムのホスト名とは異なるホスト名をコンテナに使用します。コンテナのホスト名は、DNS または `/etc/hosts` ファイルで解決できる必要があります。



#### 注記

サーバーまたはレプリカコンテナをインストールしても、Atomic Host システム自体は Identity Management ドメインに登録されません。サーバーまたはレプリカに Atomic Host システムのホスト名を使用する場合は、後で Atomic Host システムを登録できなくなります。



#### 重要

サーバーまたはレプリカコンテナをインストールするときは、**atomic install** で **--hostname** オプションを常に指定するようにしてください。この場合、**--hostname** は Identity Management インストーラーオプションではなく、Atomic オプションと見なされているため、**ipa-server-install** オプションの前に指定します。このインストールでは、**ipa-server-install** の後に指定した **--hostname** は無視されます。

- 統合 DNS でサーバーをインストールする場合は、**--ip-address** オプションを追加して、ネットワークから到達可能な Atomic Host のパブリック IP アドレスを指定します。**--ip-address** は複数回使用できます。

**警告**

テスト目的のみでコンテナをインストールする場合を除き、**publish** オプションは常に使用してください。**publish** なしでは、Atomic Host システムにポートが公開されず、サーバーはコンテナ外から到達できなくなります。

2. **ipa-server-install** セットアップスクリプトが起動します。

```
The log file for this installation can be found in /var/log/ipaserver-install.log
```

```
=====
```

```
This program will set up the IPA Server.
```

```
[... output truncated ...]
```

このプロセスは、**ipa-server-install** ユーティリティーを使用して非コンテナサーバーをインストールする場合と同じです。

3. コンテナのインストールスクリプトは、`/var/lib/<container_name>/root/ipa.csr` ファイルに証明書署名要求 (CSR) を生成します。外部 CA に CSR を送信します。発行した証明書および発行している CA の CA 証明書チェーンを取得します。  
詳細は、[Linux ドメイン ID、認証、およびポリシーガイドの 外部 CA を Root CA としてサーバーをインストールする手順](#) を参照してください。
4. 署名付き CA 証明書とルート CA 証明書を `/var/lib/<container_name>/` ディレクトリーにコピーします。

```
$ cp /root/{ipa,ca}.cert /var/lib/server-container/.
```

5. `--external-cert-file` オプションを指定して **atomic run** コマンドを実行し、証明書の場所を指定します。インストーラーによりコンテナ内の呼び出しが実行されるため、`/data/` ディレクトリーには相対的な場所を指定します。

```
$ atomic run rhel7/ipa-server ipa-server-install --external-cert-file /data/ipa.cert --external-cert-file /data/ca.cert
```

6. インストールを再開します。インストーラーは指定された証明書を使用して下位 CA を設定するようになりました。

## 2.5. コンテナへの IDENTITY MANAGEMENT サーバーのインストール CA なし

この手順では、統合 Identity Management 認証局 (CA) なしでサーバーをインストールする方法を説明します。

コンテナ Identity Management サーバーおよび Atomic Host システムは、コンテナへの **バインド** マウントを使用してマウントされるファイルシステムの部分のみを共有します。そのため、外部ファイルに関連する操作は、このボリューム内から行われる必要があります。

ipa-server コンテナイメージは、`/var/lib/<container_name>/` ディレクトリーを使用して、Atomic Host ファイルシステムに永続的なファイルを保存します。永続ストレージボリュームは、コンテナ内の `/data/` ディレクトリーにマッピングします。

作業を開始する前に

- コンテナインストールは、`ipa-server-install` で使用している非コンテナインストールと同じデフォルト設定を使用することに注意してください。カスタム設定を指定するには、以下の手順で使用する `atomic install` コマンドに追加オプションを指定します。
  - `ipa-server` コンテナで利用できる Atomic オプション。完全な一覧は、コンテナヘルプページを参照してください。
  - `ipa-server-install` で使用できる Identity Management インストーラーオプションは、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management Server のインストールとアンインストール](#) で説明しています。

手順

1. コンテナの永続ストレージディレクトリーを `/var/lib/<container_name>/` に手動で作成します。

```
$ mkdir -p /var/lib/ipa-server
```

2. 証明書チェーンを含むファイルをディレクトリーにコピーします。

```
$ cp /root/server-*.p12 /var/lib/ipa-server/.
```

必要なファイルに関する詳細は、Linux ドメイン ID、認証、およびポリシーガイドの [CA なしのインストール](#) を参照してください。

3. `atomic install` コマンドを使用し、サードパーティーの認証局から必要な証明書を指定します。

```
$ atomic install --name server-container rhel7/ipa-server publish \
  --hostname server.example.com \
  ipa-server-install \
  --dirsrv-cert-file=/data/server-dirsrv-cert.p12 \
  --dirsrv-pin=1234 \
  --http-cert-file=/data/server-http-cert.p12 \
  --http-pin=1234 \
  --pkinit-cert-file=/data/server-pkinit-cert.p12 \
  --pkinit-pin=1234
```

- コンテナには独自のホスト名が必要です。Atomic Host システムのホスト名とは異なるホスト名をコンテナに使用します。コンテナのホスト名は、DNS または `/etc/hosts` ファイルで解決できる必要があります。



#### 注記

サーバーまたはレプリカコンテナをインストールしても、Atomic Host システム自体は Identity Management ドメインに登録されません。サーバーまたはレプリカに Atomic Host システムのホスト名を使用する場合は、後で Atomic Host システムを登録できなくなります。



### 重要

サーバーまたはレプリカコンテナをインストールするときは、**atomic install** で **--hostname** オプションを常に指定するようにしてください。この場合、**--hostname** は Identity Management インストーラーオプションではなく、Atomic オプションと見なされているため、**ipa-server-install** オプションの前に指定します。このインストールでは、**ipa-server-install** の後に指定した **--hostname** は無視されます。

- 統合 DNS でサーバーをインストールする場合は、**--ip-address** オプションを追加して、ネットワークから到達可能な Atomic Host のパブリック IP アドレスを指定します。**--ip-address** は複数回使用できます。



### 警告

テスト目的のみでコンテナをインストールする場合を除き、**publish** オプションは常に使用してください。**publish** なしでは、Atomic Host システムにポートが公開されず、サーバーはコンテナ外から到達できなくなります。

4. **ipa-server-install** セットアップスクリプトが起動します。

```
The log file for this installation can be found in /var/log/ipaserver-install.log
=====
This program will set up the IPA Server.
[... output truncated ...]
```

このプロセスは、**ipa-server-install** ユーティリティを使用して非コンテナサーバーをインストールする場合と同じです。

## 2.6. インストール後の次のステップ

- コンテナを実行するには、**atomic run** コマンドを実行します。

```
$ atomic run rhel7/ipa-server
```

インストール時にコンテナの名前を指定した場合は、以下を実行します。

```
$ atomic run --name server-container rhel7/ipa-server
```

- **ipa-server** コンテナの実行は、ベアメタルまたは仮想マシンシステムでの標準的な Identity Management デプロイメントと同じ方法で機能します。たとえば、ドメインへのホストの登録やトポロジーの管理は、コマンドラインインターフェイス、Web UI、または RPM ベースの Identity Management システムと同じ方法で jsonrpc-API を使用して行えます。

## 第3章 コンテナへの IDENTITY MANAGEMENT レプリカのデプロイ

本章では、Identity Management レプリカをインストールする方法を説明します。たとえば、コンテナベースのレプリカを作成すると、既存のトポロジーでワークロードをコンテナベースのサーバーに徐々に転送する場合に便利です。

開始する前に、「[前提条件](#)」と「[サーバーおよびレプリケートコンテナで利用可能な設定](#)」を読んでください。

以下のいずれかのインストール手順を選択します。どの認証局 (CA) 設定が状況に合っているかわからない場合は、[Linux ドメイン ID、認証、およびポリシーガイドの CA 設定の決定](#) を参照してください。

- 「[コンテナへの Identity Management レプリカのインストール基本的なインストール](#)」
- 「[コンテナへの Identity Management レプリカのインストールCA なし](#)」

終了後に、「[インストール後の次のステップ](#)」を読んでください。

### 3.1. 前提条件

- コンテナをインストールする前に Atomic Host システムをアップグレードします。[Red Hat Enterprise Linux Atomic Host 7 インストールおよび設定ガイドの アップグレードおよびダウングレード](#) を参照してください。

### 3.2. サーバーおよびレプリケートコンテナで利用可能な設定

利用可能

#### ドメインレベル 1 以降

コンテナには、ドメインレベル 0 は利用できません。[ドメインレベルの表示と引き上げ](#) も参照してください。

そのため、コンテナで実行しているサーバーは、Red Hat Enterprise Linux 7.3 以降に基づいて、Identity Management サーバーとのみレプリカ合意に加えることが可能です。

#### コンテナおよび非コンテナデプロイメントの組み合わせ

単一の Identity Management ドメイントポロジーには、コンテナベースおよび RPM ベースのサーバーの両方を追加できます。

利用不可

#### デプロイされたコンテナでのサーバーコンポーネントの変更

デプロイされたコンテナのランタイム変更は行わないでください。統合 DNS や Vault などのサーバーコンポーネントの変更または再インストールが必要な場合は、新しいレプリカを作成してください。

#### 異なる Linux ディストリビューション間でのアップグレード

`ipa-server` コンテナイメージを実行するプラットフォームは変更しないでください。たとえば、Red Hat Enterprise Linux で実行しているイメージを Fedora、Ubuntu、または CentOS に変更しないでください。同様に、Fedora、Ubuntu、または CentOS で実行しているイメージを Red Hat Enterprise Linux に変更しないでください。

Identity Management は、Red Hat Enterprise Linux の後続のバージョンへのアップグレードのみをサポートします。

## 実行中のコンテナを使用したシステムのダウングレード

ipa-server コンテナイメージを実行するシステムをダウングレードしないでください。

## Atomic Host 上のアップストリームコンテナ

Atomic Host で FreeIPA ipa-server イメージなどのアップストリームコンテナイメージはインストールしないでください。Red Hat Enterprise Linux で利用可能なコンテナイメージのみをインストールします。

## 単一の Atomic Host での複数コンテナ

単一の Atomic Host に ipa-server コンテナイメージのみをインストールします。

## 3.3. コンテナへの IDENTITY MANAGEMENT レプリカのインストール基本的なインストール

この手順では、統合 CA によるデフォルトの認証局 (CA) 設定で、コンテナ Identity Management サーバーをインストールする方法を説明します。

### 作業を開始する前に

- コンテナインストールは、**ipa-replica-install** で使用している非コンテナインストールと同じデフォルト設定を使用することに注意してください。カスタム設定を指定するには、以下の手順で使用する **atomic install** コマンドに追加オプションを指定します。
  - ipa-server コンテナで利用できる Atomic オプション。完全な一覧は、コンテナヘルプページを参照してください。
  - ipa-replica-install で使用できる Identity Management インストーラーオプションは、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management のレプリカのインストールとアンインストール](#) で説明しています。
- インストール済みのサーバーが利用可能である必要があります。ベアメタルマシンまたは別の Atomic Host システムのいずれかになります。

### 手順

1. コンテナでマスターサーバーに対してレプリカをインストールするには、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management サーバーのインストールおよびアンインストール](#) で指定されているポートでマスターコンテナへの双方向通信を有効にします。
2. **atomic install rhel7/ipa-server publish --hostname fully\_qualified\_domain\_name ipa-replica-install** コマンドを使用してインストールを開始します。Identity Management のホスト名とドメイン名を指定するために **--server** および **--domain** オプションを含めます。
  - コンテナには独自のホスト名が必要です。Atomic Host システムのホスト名とは異なるホスト名をコンテナに使用します。コンテナのホスト名は、DNS または `/etc/hosts` ファイルで解決できる必要があります。



#### 注記

サーバーまたはレプリカコンテナをインストールしても、Atomic Host システム自体は Identity Management ドメインに登録されません。サーバーまたはレプリカに Atomic Host システムのホスト名を使用する場合は、後で Atomic Host システムを登録できなくなります。



## 重要

サーバーまたはレプリカコンテナをインストールするときは、**atomic install** で **--hostname** オプションを常に指定するようにしてください。この場合、**--hostname** は Identity Management インストーラーオプションではなく、Atomic オプションと見なされているため、**ipa-server-install** オプションの前に指定します。このインストールでは、**ipa-server-install** の後に指定した **--hostname** は無視されます。

- 統合 DNS でサーバーをインストールする場合は、**--ip-address** オプションを追加して、ネットワークから到達可能な Atomic Host のパブリック IP アドレスを指定します。**--ip-address** は複数回使用できます。
- [インタラクティブレプリカインストールモードにおける既知の問題](#) により、標準の **ipa-replica-install** オプションを追加して、以下のいずれかを指定します。
  - 特権ユーザーの認証情報 [例3.1「インストールコマンドの例」](#) を参照してください。
  - 一括登録のランダムパスワード。Linux ドメイン ID、認証、およびポリシーガイドの [無作為のパスワードを使用したレプリカのインストール](#) を参照してください。



## 警告

テスト目的のみでコンテナをインストールする場合を除き、**publish** オプションは常に使用してください。**publish** なしでは、Atomic Host システムにポートが公開されず、サーバーはコンテナ外から到達できなくなります。

### 例3.1インストールコマンドの例

ipa-server コンテナをインストールするためのコマンド構文:

```
$ atomic install [ --name <container_name> ] rhel7/ipa-server [ Atomic options ] [ ipa-server-install | ipa-replica-install ] [ ipa-server-install or ipa-replica-install options ]
```

管理者の認証情報を使用して **replica-container** という名前のレプリカコンテナをインストールするには、Identity Management レプリカ設定のデフォルト値を使用します。

```
$ atomic install --name replica-container rhel7/ipa-server publish \
  --hostname replica.example.com \
  ipa-replica-install \
  --server server.example.com \
  --domain example.com \
  --ip-address 2001:DB8::1111 \
  --principal admin \
  --admin-password <admin_password>
```

## 3.4. コンテナへの IDENTITY MANAGEMENT レプリカのインストール CA なし

この手順では、統合 Identity Management 認証局 (CA) なしでサーバーをインストールする方法を説明します。

コンテナ Identity Management サーバーおよび Atomic Host システムは、コンテナへの **バインドマウント** を使用してマウントされるファイルシステムの部分のみを共有します。そのため、外部ファイルに関連する操作は、このボリューム内から行われる必要があります。

`ipa-server` コンテナイメージは、`/var/lib/<container_name>/` ディレクトリーを使用して、Atomic Host ファイルシステムに永続的なファイルを保存します。永続ストレージボリュームは、コンテナ内の `/data/` ディレクトリーにマッピングします。

作業を開始する前に

- コンテナインストールは、`ipa-replica-install` で使用している非コンテナインストールと同じデフォルト設定を使用することに注意してください。カスタム設定を指定するには、以下の手順で使用する `atomic install` コマンドに追加オプションを指定します。
  - `ipa-server` コンテナで利用できる Atomic オプション。完全な一覧は、コンテナヘルプページを参照してください。
  - `ipa-replica-install` で使用できる Identity Management インストーラーオプションは、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management のレプリカのインストールとアンインストール](#) で説明しています。
- インストール済みのサーバーが利用可能である必要があります。ベアメタルマシンまたは別の Atomic Host システムのいずれかになります。

手順

1. コンテナでマスターサーバーに対してレプリカをインストールするには、Linux ドメイン ID、認証、およびポリシーガイドの [Identity Management サーバーのインストールおよびアンインストール](#) で指定されているポートでマスターコンテナへの双方向通信を有効にします。
2. コンテナの永続ストレージディレクトリーを `/var/lib/<container_name>/` に手動で作成します。

```
$ mkdir -p /var/lib/ipa-server
```

3. 証明書チェーンを含むファイルをディレクトリーにコピーします。

```
$ cp /root/server-*.p12 /var/lib/ipa-server/.
```

必要なファイルに関する詳細は、Linux ドメイン ID、認証、およびポリシーガイドの [CA なしのインストール](#) を参照してください。

4. `atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-replica-install` コマンドを使用して `--server` および `--domain` オプションを指定して、Identity Management サーバーのホスト名およびドメイン名を指定し、サードパーティーの認証局から必要な証明書を指定します。

```
$ atomic install --name replica-container rhel7/ipa-server publish \  
--hostname replica.example.com \  
ipa-replica-install \  

```

```

--server server.example.com \
--domain example.com \
--dirsrv-cert-file=/data/replica-dirsrv-cert.p12 \
--dirsrv-pin=1234 \
--http-cert-file=/data/replica-http-cert.p12 \
--http-pin=1234 \
--pkinit-cert-file=/data/replica-pkinit-cert.p12 \
--pkinit-pin=1234

```



### 注記

証明書へのパスには、永続ストレージボリュームがコンテナ内の `/data/` にマップするため `/data/` が含まれます。

- コンテナには独自のホスト名が必要です。Atomic Host システムのホスト名とは異なるホスト名をコンテナに使用します。コンテナのホスト名は、DNS または `/etc/hosts` ファイルで解決できる必要があります。



### 注記

サーバーまたはレプリカコンテナをインストールしても、Atomic Host システム自体は Identity Management ドメインに登録されません。サーバーまたはレプリカに Atomic Host システムのホスト名を使用する場合は、後で Atomic Host システムを登録できなくなります。



### 重要

サーバーまたはレプリカコンテナをインストールするときは、**atomic install** で **--hostname** オプションを常に指定するようにしてください。この場合、**--hostname** は Identity Management インストーラーオプションではなく、Atomic オプションと見なされているため、**ipa-server-install** オプションの前に指定します。このインストールでは、**ipa-server-install** の後に指定した **--hostname** は無視されます。

- 統合 DNS でサーバーをインストールする場合は、**--ip-address** オプションを追加して、ネットワークから到達可能な Atomic Host のパブリック IP アドレスを指定します。**--ip-address** は複数回使用できます。
- [インタラクティブレプリカインストールモードにおける既知の問題](#) により、標準の **ipa-replica-install** オプションを追加して、以下のいずれかを指定します。
  - 特権ユーザーの認証情報 [例3.1「インストールコマンドの例」](#) を参照してください。
  - 一括登録のランダムパスワード。Linux ドメイン ID、認証、およびポリシーガイドの [無作為のパスワードを使用したレプリカのインストール](#) を参照してください。



### 警告

テスト目的のみでコンテナをインストールする場合を除き、**publish** オプションは常に使用してください。**publish** なしでは、Atomic Host システムにポートが公開されず、サーバーはコンテナ外から到達できなくなります。

## 3.5. インストール後の次のステップ

- コンテナを実行するには、**atomic run** コマンドを実行します。

```
$ atomic run rhel7/ipa-server
```

インストール時にコンテナの名前を指定した場合は、以下を実行します。

```
$ atomic run --name replica-container rhel7/ipa-server
```

- **ipa-server** コンテナの実行は、ベアメタルまたは仮想マシンシステムでの標準的な Identity Management デプロイメントと同じ方法で機能します。たとえば、ドメインへのホストの登録やトポロジーの管理は、コマンドラインインターフェイス、Web UI、または RPM ベースの Identity Management システムと同じ方法で jsonrpc-API を使用して行えます。

## 第4章 コンテナからホストシステムへのサーバーの移行

本章では、最初にコンテナにインストールされたサーバーをベアメタルまたは仮想マシンシステムに移行する方法について説明します。以下のシナリオでは、Red Hat Enterprise Linux システムに移行します。

### 4.1. IDENTITY MANAGEMENT サーバーの、コンテナからホストシステムへの移行

この手順では、コンテナ化された Identity Management サーバーをホストシステムに移行する方法と、オプションでコンテナを切り離す方法について説明します。

#### 手順

1. ホストシステムをコンテナに対して Identity Management レプリカとして登録します。後で Identity Management サーバーでコンテナを停止する場合は、認証局 (CA) が設定されたレプリカを作成してください。  
[Identity Management のレプリカのインストールとアンインストール](#) を参照してください。
2. コンテナ内のサーバーから CA マスターのロールをホストシステムの新しいレプリカに移行します。  
[レプリカのマスター CA サーバーへのプロモート](#) を参照してください。
3. コンテナでサーバーを停止します。  
[5章サーバーおよびレプリカコンテナのアンインストール](#) を参照してください。

## 第5章 サーバーおよびレプリカコンテナのアンインストール

本章では、Identity Management サーバーまたはレプリカコンテナをアンインストールする方法を説明します。

### 5.1. サーバーまたはレプリカコンテナのアンインストール

この手順では、Identity Management サーバーまたはレプリカコンテナをアンインストールし、サーバーまたはレプリカがトポロジーから適切に削除されるようにする方法を説明します。

#### 手順

1. 既存のトポロジーに属するレプリカコンテナがそのトポロジーから適切に削除されるようにするには、登録したホストで **ipa server-del <container-host-name>** コマンドを実行します。**atomic uninstall** コマンドでは以下を行えないため、この手順は重要です。
  - 切断されていないドメインレベル1トポロジーや、最新の認証局 (CA)、鍵回復機関 (KRA)、または DNS サーバーが削除されないようにするためにチェックを実行します。
  - 既存のトポロジーからレプリカコンテナを削除します。
2. **atomic uninstall** コマンドを実行して、コンテナ名とイメージ名を追加します。

```
$ atomic uninstall --name <container_name> rhel7/ipa-server
```

### 5.2. アンインストール後の次のステップ

- コンテナのマウントされたデータディレクトリーのバックアップは、**/var/lib/<container\_name>.backup.<timestamp>** の下にあります。新しいコンテナを作成する必要がある場合は、バックアップにより、ボリュームに保存されている永続データを再利用できます。

## パート II. SSSD コンテナの使用

このパートでは、Atomic Host で **SSSD** コンテナをデプロイ、設定、更新、およびアンインストールする方法について説明します。さらに、このドキュメントでは、**SSSD** コンテナへのアクセスを許可または制限する方法と、一元化された Kerberos 認証情報キャッシュを作成および使用する方法について説明します。

## 第6章 ATOMIC HOST で ID および認証サービスを提供するための SSSD コンテナの設定

システム管理者は、コンテナで SSSD を使用して Atomic Host システムの外部 ID、認証、および承認サービスを提供できます。本章では、外部 ID ソース (Identity Management または Active Directory) からのユーザーが Atomic Host 自体で実行しているサービスを使用できるようにする **privileged** として、SSSD コンテナを実行する方法を説明します。

または、外部 ID ソース (Identity Management または Active Directory) からのユーザーが Atomic Host の他のコンテナで実行しているサービスを使用できるようにする、**unprivileged** として SSSD コンテナを実行することもできます。詳細は、[7章異なる設定を含む SSSD コンテナのデプロイ](#)を参照してください。

開始する前に、以下を参照してください。

- [「前提条件」](#)

Atomic Host を Identity Management サーバーに登録するには、以下を参照してください。

- [「特権のある SSSD コンテナを使用した Identity Management ドメインの登録」](#)

Atomic Host を Active Directory に登録するには、以下を参照してください。

- [「SSSD Container を使用した Active Directory ドメインのジョイン」](#)

### 6.1. 前提条件

- コンテナをインストールする前に Atomic Host システムをアップグレードします。[Red Hat Enterprise Linux Atomic Host 7 インストールおよび設定ガイドのアップグレードおよびダウングレード](#)を参照してください。

### 6.2. 特権のある SSSD コンテナを使用した IDENTITY MANAGEMENT ドメインの登録

この手順では、SSSD コンテナをインストールして、Identity Management サーバーに登録できるように設定する方法を説明します。インストール中に以下の手順を実行します。

- さまざまな設定およびデータがコンテナにコピーされます。
- Identity Management クライアントを設定するための `ipa-client-install` ユーティリティーが起動します。
- Identity Management ドメインへの登録に成功すると、設定およびデータは Atomic Host システムに再びコピーされます。

#### 前提条件

以下のいずれかが必要になります。

- Atomic Host システムのワンタイムクライアント登録のパスワードを Identity Management ドメインに行うための無作為なパスワード。このパスワードを生成するには、以下のように、Identity Management サーバー上の Identity Management ホストとして Atomic Host システムを追加します。

```
$ ipa host-add <atomic.example.com> --random
```

```
[... output truncated ...]
Random password: 4Re[>5]OB$3K($qYs:M&}B
[... output truncated ...]
```

詳細は、Linux ドメイン ID、認証、およびポリシーガイドの [クライアントのインストール](#) を参照してください。

- クライアント登録が許可された Identity Management ユーザーの認証情報。デフォルトでは、これは **admin** ユーザーです。

## 手順

1. **atomic install** コマンドを実行して **sssd** コンテナインストールを開始し、新しいホストの登録が可能な IdM ユーザーの無作為なパスワードまたは認証情報を指定します。多くの場合、これは **admin** ユーザーです。

```
# atomic install rhel7/sssd --password "4Re[>5]OB$3K($qYs:M&}B"
[... output truncated ...]
Service sssd.service configured to run SSSD container.
[... output truncated ...]
```

```
# atomic install rhel7/sssd -p admin -w <admin_password>
[... output truncated ...]
Service sssd.service configured to run SSSD container.
[... output truncated ...]
```

**atomic install rhel7/sssd** コマンドでは、標準の **ipa-client-install** オプションを指定できません。設定によっては、これらのオプションを指定して追加情報を入力する必要がある場合があります。たとえば、**ipa-client-install** がサーバーのホスト名およびドメイン名を判断できない場合は、**--server** および **--domain** オプションを指定します。

```
# atomic install rhel7/sssd --password "4Re[>5]OB$3K($qYs:M&}B" --server
<server.example.com> --domain <example.com>
```



### 注記

また、**atomic install** を実行する前に、**/etc/sss/ipa-client-install-options** ファイルに保存して、**ipa-client-install** にオプションを渡すことができます。たとえば、このファイルには以下が含まれます。

```
--password=4Re[>5]OB$3K($qYs:M&}B
--server=server.example.com
--domain=example.com
```

2. 以下のいずれかのコマンドを実行して、コンテナで SSSD を起動します。

```
# atomic run rhel7/sssd
```

```
# systemctl start sssd
```

3. 任意。コンテナが実行していることを確認します。

```
# docker ps
CONTAINER ID    IMAGE
5859b9366f0f  rhel7/sssds
```

4. 任意。Atomic Host の SSSD が Identity Management ドメインの ID を解決していることを確認します。
  - a. Identity Management ユーザーの Kerberos チケットを取得し、ssh ユーティリティーを使用して Atomic Host にログインします。

```
$ atomic run sssd kinit <idm_user>
$ ssh <idm_user>@<atomic.example.com>
```

- b. id ユーティリティーを使用し、所定のユーザーとしてログインしていることを確認します。

```
$ id
uid=1215800001(idm_user) gid=1215800001(idm_user) groups=1215800001(idm_user)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- c. hostname ユーティリティーを使用して、Atomic Host システムにログインしていることを確認します。

```
$ hostname
atomic.example.com
```

### 6.3. SSSD CONTAINER を使用した ACTIVE DIRECTORY ドメインのジョイン

この手順では、SSSD コンテナをインストールし、Atomic Host システムを Active Directory にジョインするように設定する方法を説明します。

#### 手順

1. 管理者など Active Directory ドメインにシステムを登録することができるユーザーのパスワードを、Atomic Host システムの `/etc/sssds/realm-join-password` ファイルに保存します。

```
# echo <password> > /etc/sssds/realm-join-password
```

`realm join` コマンドは、パスワードをコマンドラインパラメーターとして受け付けられないため、ファイルにパスワードを指定する必要があります。



#### 注記

デフォルト名 (`sssds`) の代わりに使用するために `atomic install` コマンドでカスタムコンテナイメージ名を後で指定する場合は、ファイルのパスにカスタム名を追加します (`/etc/sssds/<custom_container_name>/realm-join-password`)。

2. `atomic install` コマンドを実行して `sssds` コンテナインストールを開始し、参加するレルムを指定します。操作にデフォルトの管理者ユーザーアカウントを使用している場合は、以下を実行します。

```
# atomic install rhel7/sssdd realm join <ad.example.com>
```

```
docker run --rm=true --privileged --net=host -v /:/host -e NAME=sssdd -e IMAGE=rhel7/sssdd -
e HOST=/host rhel7/sssdd /bin/install.sh realm join ad.example.com
Initializing configuration context from host ...
Password for Administrator:
Copying new configuration to host ...
Service ssssdd.service configured to run SSSDD container.
```

別のユーザーアカウントを使用している場合は、**--user** オプションで指定します。

```
# atomic install rhel7/sssdd realm join --user <user_name> <ad.example.com>
```

- 以下のいずれかのコマンドを実行して、コンテナで SSSDD を起動します。

```
# atomic run rhel7/sssdd
```

```
# systemctl start ssssdd
```

- 任意。コンテナが実行していることを確認します。

```
# docker ps
CONTAINER ID    IMAGE
5859b9366f0f   rhel7/sssdd
```

- 任意。Atomic Host システムで、SSSD が Active Directory ドメインからアイデンティティを解決していることを確認します。

```
# id administrator@<ad.example.com>
uid=1397800500(administrator@ad.example.com) gid=1397800513(domain
users@ad.example.com)
```

## 関連情報

- realmd** ユーティリティーの詳細は、man ページの `realm(8)` または [Windows 統合ガイドの REALMD を使用した ACTIVE DIRECTORY ドメインへの接続](#) を参照してください。

## 第7章 異なる設定を含む SSSD コンテナのデプロイ

システム管理者は、Identity Management や Active Directory などの特定のアイデンティティプロバイダーを使用する、特権のない複数の SSSD コンテナをデプロイすることができます。これにより、他のアプリケーションコンテナが、優先の ID ソースのみを使用できます。

### 7.1. 前提条件

- SSSD コンテナが提供するサービスを他のコンテナから使用する場合は、クライアントコンテナの `rhel7` ベースイメージに `sssd-client` パッケージが含まれている必要があります。ただし、デフォルトの `rhel7` ベースイメージにはこのパッケージが含まれません。その他のコンテナから SSSD サービスを使用する必要がある場合は、デフォルトの `rhel7` ベースイメージに基づいてクライアントコンテナに独自のイメージを作成し、`sssd-client` を含めます。詳細は、[Creating Docker images](#) を参照してください。

### 7.2. SSSD コンテナを起動し、これをアイデンティティリソースにジョインさせる

SSSD コンテナを開始し、Active Directory などのアイデンティティリソースにジョインさせるには、以下を実行します。

1. `atomic install` コマンドを実行して、SSSD コンテナを起動します。以下に例を示します。

```
# atomic install --opt1='--dns=192.0.2.1 --dns-search=idm.example.com --
hostname=server.ad.example.com -e SSSD_CONTAINER_TYPE=application --
net=default' --name=ad_sssd rhel7/sssd realm join -v ad.example.com
```

前述の例は、`ad_sssd` という名前の SSSD アプリケーションコンテナを作成します。DNS サーバーの IP アドレス、検索ドメイン、ホスト名、および `realm join` コマンドを `atomic install` に渡し、コンテナで稼働している SSSD を Active Directory ドメインに自動的にジョインさせます。

この手順は、SSSD コンテナを提供する各アイデンティティプロバイダーに対して繰り返します。

2. コンテナを起動します。以下に例を示します。

```
# atomic run ad_sssd
```

### 7.3. SSSD キャッシュをアプリケーションコンテナに渡す

アプリケーションコンテナで SSSD キャッシュを使用するには、アプリケーションコンテナの起動時に関連のディレクトリーを `docker run` コマンドに渡します。

```
# docker run --rm --name=<container_name> -v=/var/lib/sssd_container/<sssd-container-
name>/client/etc/krb5.conf.d:/etc/krb5.conf.d -v=/var/lib/sssd_container/<sssd-container-
name>/client/var/lib/sss/pipes:/var/lib/sss/pipes/ <image_name>
```

これにより、SSSD コンテナのディレクトリーがアプリケーションコンテナ内の対応するディレクトリーにマッピングされます。

これでコンテナで実行中のアプリケーションは、`kinit` ユーティリティーや `mod_auth_gssapi` モジュールなどを使用して認証できるようになりました。

## 第8章 HBAC ルールを使用した SSSD コンテナへのアクセスの付与および制限

Identity Management ドメインでは、各 SSSD コンテナは、それぞれを異なるホストとして自身を示し、管理者は HBAC (ホストベースアクセス制御) ルールを設定して、個々のコンテナへのアクセスを許可または制限できます。

Identity Management で HBAC ルールを設定する詳細は、[Linux ドメイン ID、認証、およびポリシーガイドのホストベースのアクセス制御の設定](#) を参照してください。

## 第9章 集中化された KERBEROS 認証情報キャッシュの作成と使用

システム管理者は、Kerberos サーバーに対する認証を集中化して認証情報キャッシュを初期化できます。また、コンテナ内で実行中のアプリケーションが、キータブファイル、認証、または更新を別々に管理しなくても、この中央キャッシュを使用して認証を行うことができるようにすることもできます。

### 9.1. 前提条件

- SSSD コンテナが提供するサービスを他のコンテナから使用する場合は、クライアントコンテナの `rhel7` ベースイメージに **sssd-client** パッケージが含まれている必要があります。ただし、デフォルトの `rhel7` ベースイメージにはこのパッケージが含まれません。その他のコンテナから SSSD サービスを使用する必要がある場合は、デフォルトの `rhel7` ベースイメージに基づいてクライアントコンテナに独自のイメージを作成し、**sssd-client** を含めます。詳細は、[Creating Docker images](#) を参照してください。

### 9.2. SSSD CONTAINER を使用した ACTIVE DIRECTORY ドメインのジョイン

この手順では、SSSD コンテナをインストールし、Atomic Host システムを Active Directory にジョインするように設定する方法を説明します。

#### 手順

- 管理者など Active Directory ドメインにシステムを登録することができるユーザーのパスワードを、Atomic Host システムの `/etc/sss/realms-join-password` ファイルに保存します。

```
# echo <password> > /etc/sss/realms-join-password
```

**realm join** コマンドは、パスワードをコマンドラインパラメーターとして受け付けないため、ファイルにパスワードを指定する必要があります。



#### 注記

デフォルト名 (**sss**) の代わりに使用するために **atomic install** コマンドでカスタムコンテナイメージ名を後で指定する場合は、ファイルのパスにカスタム名を追加します (`/etc/sss/<custom_container_name>/realms-join-password`)。

- atomic install** コマンドを実行して **sss** コンテナインストールを開始し、参加するレルムを指定します。操作にデフォルトの管理者ユーザーアカウントを使用している場合は、以下を実行します。

```
# atomic install --opt1='--dns=<DNS_server_IP> --dns-search=<DNS_domain> --
hostname=<host_name> -e SSSD_CONTAINER_TYPE=application --net=default'
rhel7/sss realm join -v <ad.example.com>
docker run --rm=true --privileged --net=host -v /:/host -e NAME=sss -e IMAGE=rhel7/sss -
e HOST=/host rhel7/sss /bin/install.sh realm join -v ad.example.com
Initializing configuration context from host ...
* Resolving: _ldap._tcp.ad.example.com
* Performing LDAP DSE lookup on: 192.168.122.105
...
Service sss.service configured to run SSSD container.
```

別のユーザーアカウントを使用している場合は、**--user** オプションで指定します。

```
# atomic install rhel7/sss realm join --user <user_name> <ad.example.com>
```

- 以下のいずれかのコマンドを実行して、コンテナで SSSD を起動します。

```
# atomic run rhel7/sss
```

```
# systemctl start sssd
```

- 任意。コンテナが実行していることを確認します。

```
# docker ps
CONTAINER ID    IMAGE
5859b9366f0f   rhel7/sss
```

- 任意。Atomic Host システムで、SSSD が Active Directory ドメインからアイデンティティを解決していることを確認します。

```
# id administrator@<ad.example.com>
uid=1397800500(administrator@ad.example.com) gid=1397800513(domain
users@ad.example.com)
```

## 関連情報

- realmd** ユーティリティーの詳細は、man ページの `realm(8)` または **Windows 統合ガイド** の [REALMD を使用した ACTIVE DIRECTORY ドメインへの接続](#) を参照してください。

## 9.3. コンテナで実行中の SSSD の認証

コンテナ内で実行している SSSD を使用して Kerberos サーバーに対して認証するには、以下の手順に従います。

- kinit** オプションを **docker exec** コマンドに渡します。たとえば、**管理者ユーザー**として認証するには、以下を実行します。

```
# docker exec -i <container_name> kinit administrator
Password for administrator@<DOMAIN>:
```

- 必要に応じて、Kerberos 認証情報キャッシュが Kerberos Credential Manager (KCM) に保存されていることを確認します。

```
# docker exec -i <container_name> klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@<DOMAIN>

Valid starting Expires Service principal
08/11/17 11:51:06 08/11/17 21:51:06 krbtgt/<DOMAIN>@<DOMAIN>
renew until 08/18/17 11:51:03
```

## 9.4. 異なるコンテナでの SSSD KERBEROS キャッシュの使用

SSSD コンテナの Kerberos キャッシュを他のコンテナアプリケーションに利用できるようにするには、`/var/lib/sss/container/<sss-container-name>/client/etc/krb5.conf.d` および `/var/lib/sss/container/<sss-container-name>/client/lib/sss/pipes/` ディレクトリーをアプリケーションコンテナへのボリュームとして渡します。以下に例を示します。

```
# docker run --rm --name=<application_container> -v=/var/lib/sss/container/<sss-container-name>/client/etc/krb5.conf.d:/etc/krb5.conf.d/ -v=/var/lib/sss/container/<sss-container-name>/client/var/lib/sss/pipes/:/var/lib/sss/pipes/ docker-registry.engineering.redhat.com/idmqe/sss-client-test:2.0 klist
```

前の例は、コンテナで `klist` コマンドを実行し、SSSD コンテナで管理される Kerberos チケットを一覧表示します。



#### 注記

**kdestroy** ユーティリティーを使用してキャッシュから Kerberos チケットを削除すると、アプリケーションコンテナはチケットを使用しなくなります。

## 第10章 SSSD コンテナの更新

この手順では、新しいバージョンの `rhel7/sss` イメージがリリースされた場合に、SSSD (System Security Services Daemon) コンテナを更新する方法を説明します。

### 手順

1. SSSD サービスを停止します。

- a. SSSD がシステムコンテナとして実行されている場合は、以下を実行します。

```
# systemctl stop sssd
```

- b. SSSD がアプリケーションコンテナとして実行されている場合は、以下を実行します。

```
# atomic stop <container_name>
```

2. `docker rm` コマンドを使用してイメージを削除します。

```
# docker rm rhel7/sss
```

3. 最新の SSSD イメージをインストールします。

```
# atomic install rhel7/sss
```

4. SSSD サービスを起動します。

- a. SSSD がシステムコンテナとして実行している場合は、以下を実行します。

```
# systemctl start sssd
```

- b. SSSD がアプリケーションコンテナとして実行している場合は、`atomic start` コマンドを使用して各コンテナを起動します。

```
# atomic start <container_name>
```

## 第11章 SSSD コンテナのアンインストール

本章では、システムセキュリティーサービスデーモン (SSSD) コンテナをアンインストールする方法を説明します。

### 11.1. IDENTITY MANAGEMENT ドメインに登録された SSSD コンテナのアンインストール

この手順では、Atomic Host システムから System Security Services Daemon (SSSD) コンテナをアンインストールし、Identity Management ドメインから Atomic Host システムの登録を解除する方法を説明します。

#### 手順

1. **atomic uninstall** コマンドを実行して、イメージ名を追加します。

```
# atomic uninstall rhel7/sssdc
[... output truncated ...]
Unenrolling client from IPA server
[... output truncated ...]
Client uninstall complete
[... output truncated ...]
```

2. Identity Management サーバーで Atomic Host システムのホストエントリを削除します。たとえば、コマンドラインでは、以下ようになります。

```
$ ipa host-del <atomic.example.com>
```

3. Atomic Host 上の **sssdc** サービスが、現在では設定されていないコンテナを起動しないようにするには、サービスの **systemd** ユニットファイルを削除して、**systemd** プロセスを再ロードします。

```
# rm /etc/systemd/system/sssdc.service
# systemctl daemon-reload
```

### 11.2. ACTIVE DIRECTORY ドメインにジョインした SSSD コンテナのアンインストール

この手順では、Atomic Host システムから System Security Services Daemon (SSSD) コンテナをアンインストールし、Active Directory ドメインから Atomic Host システムの登録を解除する方法を説明します。

#### 手順

- **atomic uninstall** コマンドを実行して、イメージ名を追加し、残すレルムを指定します。操作にデフォルトの管理者ユーザーアカウントを使用している場合は、以下を実行します。

```
# atomic uninstall rhel7/sssdc realm leave <ad.example.com>
```

別のユーザーアカウントを使用している場合は、**--user** オプションで指定します。

```
# atomic uninstall rhel7/sssdc realm leave --user <user_name> <ad.example.com>
```

## 付録A コンテナで実行している IDM および SSSD のトラブルシューティングに関する情報の収集

この付録では、コンテナで実行している IdM および SSSD をトラブルシューティングし、Red Hat サポートチケットにアタッチ可能な重要な設定ファイルとログファイルを収集できるようにする手順を説明します。

### A.1. ATOMIC HOST での SOSREPORT の作成

このセクションでは、**rhel7/rhel-tools** コンテナをインストールして起動し、**sosreport** を作成する方法を説明します。

**rhel7/rhel-tools** コンテナは、このコンテナで実行中のプロセスを有効にする特権付きのセキュリティスイッチを使用します。

- ホストのすべてのセマフォおよび共有メモリーセグメントと対話する
- ホストのネットワークでポートおよび raw IP トラフィックをリッスンする
- ホストのすべてのプロセスと対話する

**rhel7/rhel-tools** は、ホストの分離なしで実行することに注意してください。このコンテナによるユーティリティーを使用することは、システム上で直接 **root** ユーザーとして実行するのと同様です。

#### 手順

1. **rhel7/rhel-tools** コンテナをインストールします。

```
# docker pull rhel7/rhel-tools
```

2. **rhel7/rhel-tools** コンテナを起動します。

```
# atomic run rhel7/rhel-tools
```

3. **sosreport** ユーティリティーを実行します。

```
# sosreport
```

このユーティリティーは、収集した情報のアーカイブを **/host/var/tmp/sos\_tal4k\_\*** ファイルに保存します。

4. **exit** を実行してコンテナを終了します。

```
# exit
```

5. **sosreport** アーカイブをサポートリクエストにアタッチします。

### A.2. IDM および SSSD コンテナのバージョンの表示

このセクションでは、インストールされている IdM と SSSD コンテナのバージョンを表示する方法を説明します。たとえば、この情報は、問題が新しいバージョンで修正された場合に、Red Hat Enterprise Linux リリースノートを検索するために使用します。

## 手順

- **rhel7/ipa-server** コンテナのバージョンを表示します。

```
# atomic images version rhel7/ipa-server
IMAGE NAME                VERSION  IMAGE ID
registry.access.redhat.com/rhel7/ipa-server:latest  4.6.5-29  9d500a8e4296
```

- **rhel7/sss** コンテナのバージョンを表示します。

```
# atomic images version rhel7/sss
IMAGE NAME                VERSION  IMAGE ID
registry.access.redhat.com/rhel7/sss:latest  7.7-12  19e5cab1c905
```

## A.3. コンテナで実行している SSSD のデバッグログの作成

このセクションでは、重要な SSSD 設定およびログファイルを使用してアーカイブを作成する方法を説明します。

### 手順

1. **sss** コンテナを停止します。

```
# docker stop sssd
```

2. SSSD のキャッシュおよびログディレクトリの内容を削除します。

```
# rm -rf /var/lib/sss/db/* /var/lib/sss/mc/* /var/log/sss/*
```

3. **/etc/sss/sss.conf** ファイルを編集し、**debug\_level** パラメーターを **9** に設定します。

```
[domain/dockerlab.local]
...
debug_level = 9

[nss]
debug_level = 9
```

4. **sss** コンテナを起動します。

```
docker start sssd
```

5. 関連する SSSD 設定およびログファイルが含まれる **/tmp/sss-debug.tar.gz** アーカイブを作成します。

```
# tar czvf /tmp/sss-debug.tar.gz /etc/sss/sss.conf /etc/nsswitch.conf /etc/krb5.conf
/etc/pam.d /etc/samba/smb.conf /var/log/secure /var/log/messages /var/log/sss
```

6. **/tmp/sss-debug.tar.gz** ファイルをサポートケースに添付します。

## A.4. IDM クライアントのインストールログの表示

このセクションでは、IdM クライアントのインストールログを表示する方法を説明します。ログファイルは、クライアントのインストールに失敗した場合の問題のデバッグに役立ちます。

## 手順

- IdM クライアントのインストールログを表示するには、次のコマンドを実行します。

```
# cat /var/log/sss/install/ipaclient-install.log
```

## 付録B 改訂履歴

以下の改訂番号は本ガイドに関するものであり、Red Hat Enterprise Linux のバージョン番号とは関係ありません。

| バージョン  | 日付と変更                                                                     | 作成者                    |
|--------|---------------------------------------------------------------------------|------------------------|
| 7.0-11 | 2019年10月15日:トラブルシューティング付録を追加。                                             | Marc Muehlfeld         |
| 7.0-10 | 2019年9月26日:HBACルールを使用したSSSDコンテナへのアクセスの付与および制限を追加。                         | Marc Muehlfeld         |
| 7.0-9  | 2019年8月23日:Atomic HostでIDおよび認証サービスを提供するためのSSSDコンテナの設定を更新。                 | Marc Muehlfeld         |
| 7.0-8  | 2018年4月5日:7.5 GA 公開用ドキュメントの準備。                                            | Lucie Maňásková        |
| 7.0-7  | 2018年3月19日:異なる設定を含むsssdコンテナのデプロイの更新                                       | Lucie Maňásková        |
| 7.0-6  | 2018年1月29日:若干の修正。                                                         | Aneta Šteflová Petrová |
| 7.0-5  | 2017年11月20日:SSSDコンテナを使用したIdentity Managementドメインへの登録を更新。                  | Aneta Šteflová Petrová |
| 7.0-4  | 2017年9月12日:ADドメインにジョインしているSSSDコンテナをアンインストールする手順を追加。                       | Aneta Šteflová Petrová |
| 7.0-3  | 2017年8月28日:より多くのユーザーストーリーと修正によりsssdコンテナの使用の一部を更新。                         | Aneta Šteflová Petrová |
| 7.0-2  | 2017年8月14日:利用可能なコンテナイメージとSSSDコンテナを使用したActive Directoryドメインのジョインのセクションを更新。 | Aneta Šteflová Petrová |
| 7.0-1  | 2017年7月18日:7.4 GA 公開用ドキュメントバージョン                                          | Aneta Šteflová Petrová |