Red Hat Enterprise Linux 7

コンテナー Identitty Management サービスの使用

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

Last Updated: 2021-01-26

Red Hat Enterprise Linux 7 コンテナー Identitty Management サービスの使用

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

Florian Delehaye
Red Hat Customer Content Services
fdelehay@redhat.com

Marc Muehlfeld
Red Hat Customer Content Services

Filip Hanzelka
Red Hat Customer Content Services

Lucie Maňásková
Red Hat Customer Content Services

Aneta Šteflová Petrová
Red Hat Customer Content Services

法律上の通知

概要

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

目次

パート I. はじめに

第1章 コンテナー IDENTITY MANAGEMENT サービスの概要

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

警告

rhel7/ipa-server コンテナー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 コンテナーの概要

コンテナーで 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なります。

重要

ipa-server および **sssd** コンテナーは、Red Hat Enterprise Linux Atomic Host システムで使用するように設計されています。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、コンテナー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、コンテナー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 およびコンテナー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ーイメージ

rhel7/ipa-server コンテナーイメージ

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

rhel7/sssd コンテナーイメージ

- コンテナーで 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。
- その他のコンテナー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

- コンテナー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. コンテナーで 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。コンテナーサブディレクトリーは、別のコンテナーまたはホストシステムに移行できます。または、*4章 コンテナーからホストシステムへのサーバーの移行*を参照してください。

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、コンテナー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 をコンテナー環境に適用します。これにより、コンテナー全体が他のコンテナーから保護されます。
  - **ipa-server** コンテナーは、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。コンテナーは、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 II. IPA-SERVER CONTAINER (TECHNOLOGY PREVIEW) の使用

第2章 コンテナーへの 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ーで利用可能な設定」 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。

- 「コンテナーへの Identity Management Server のインストール: 基本的なインストール」
- 「コンテナーへの Identity Management サーバーのインストール: 外部 CA」
- 「コンテナーへの 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

- コンテナー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ーで利用可能な設定

利用可能

ドメインレベル 1 以降

コンテナーには、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、コンテナー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。

コンテナーおよび非コンテナー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、コンテナーベースおよび 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ー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ー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 コンテナー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。

実行中のコンテナーを使用したシステムのダウングレード

ipa-server コンテナー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ー

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ー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ーイメージのみをインストールします。

単一の Atomic Host での複数コンテナー

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

2.3. コンテナーへの IDENTITY MANAGEMENT SERVER のインストール: 基本的なインストール

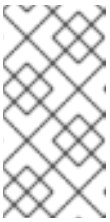
この手順では、統合 CA によるデフォルトの認証局 (CA) 設定で、コンテナー Identity Management サーバーをインストールする方法を説明します。

作業を開始する前に

- コンテナーインストールは、**ipa-server-install** で使用している非コンテナー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** コンテナーで利用できる Atomic オプション。完全な一覧は、コンテナー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。

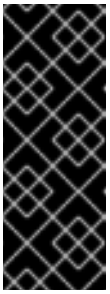
手順

1. **atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-server-install** コマンドを使用して、インストールを開始します。
   - コンテナー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ーに使用します。コンテナーのホスト名は、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ー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ーをインストールする場合は、**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。**ipa-server-install** の後に使用した場合には、インストールは **--hostname** を無視します。

- 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ー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ー外から到達できなくなります。

2. **ipa-server-install** 設定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コンテナー以外の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 コンテナー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ーをインストールし、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. コンテナーへの 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。

コンテナー Identity Management サーバーおよび Atomic Host システムは、コンテナーへの **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。

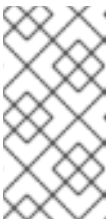
ipa-server コンテナーイメージは、**/var/lib/<container_name>/** ディレクトリーを使用して、Atomic Host ファイルシステムに永続的なファイルを保存します。永続ストレージボリュームは、コンテナー内の **/data/** ディレクトリーにマッピングします。

作業を開始する前に

- コンテナーインストールは、**ipa-server-install** で使用している非コンテナー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** コンテナーで利用できる Atomic オプション。完全な一覧は、コンテナー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** コマンドを使用して、インストールを開始します。
   - コンテナー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ーに使用します。コンテナーのホスト名は、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ー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ーをインストールする場合は、**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。**ipa-server-install** の後に使用した場合には、インストールは **--hostname** を無視します。

- 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ー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ー外から到達できなくなります。

2. **ipa-server-install** 設定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コンテナー以外のサーバーをインストールする場合と同じです。

3. コンテナー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. 署名済み 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}.crt /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ー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.crt --
external-cert-file /data/ca.crt
```

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. コンテナーへの 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。

コンテナー Identity Management サーバーおよび Atomic Host システムは、コンテナーへの **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 コンテナーイメージは、**/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、コンテナー内の **/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

- コンテナーインストールは、**ipa-server-install** で使用している非コンテナー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** コンテナーで利用できる Atomic オプション。完全な一覧は、コンテナー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. コンテナー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。

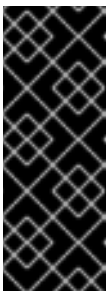
3. **atomic install** コマンドを使用し、サードパーティーの認証局から必要な証明書を指定します。

```
$ 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
```

- コンテナー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ーに使用します。コンテナーのホスト名は、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ー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ーをインストールする場合は、**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。**ipa-server-install** の後に使用した場合には、インストールは **--hostname** を無視します。

- 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ー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ー外から到達できなくなります。

4. **ipa-server-install** 設定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コンテナー以外の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

- コンテナーを実行するには、**atomic run** コマンドを使用します。

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

インストール時にコンテナー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 コンテナーの実行は、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ース、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 コンテナーへの 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、コンテナー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ー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ーで利用可能な設定」 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。

- 「コンテナーへの Identity Management レプリカのインストール：基本的なインストール」
- 「コンテナーに 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

- コンテナー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ーで利用可能な設定

利用可能

ドメインレベル 1 以降

コンテナーには、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、コンテナー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。

コンテナーおよび非コンテナー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、コンテナーベースおよび 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ー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ー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 コンテナー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。

実行中のコンテナーを使用したシステムのダウングレード

ipa-server コンテナー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ー

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ー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ーイメージのみをインストールします。

単一の Atomic Host での複数コンテナー

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

3.3. コンテナーへの IDENTITY MANAGEMENT レプリカのインストール：基本的なインストール

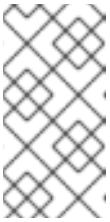
この手順では、統合 CA によるデフォルトの認証局 (CA) 設定で、コンテナー Identity Management サーバーをインストールする方法を説明します。

作業を開始する前に

- コンテナーインストールは、**ipa-replica-install** で使用している非コンテナー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** コンテナーで利用できる Atomic オプション。完全な一覧は、コンテナー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. コンテナー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ー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。
   - コンテナー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ーに使用します。コンテナーのホスト名は、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ー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ーをインストールする場合は、**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。**ipa-server-install** の後に使用した場合には、インストールは **--hostname** を無視します。

- 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ー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ー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 コンテナー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ー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. コンテナーに 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。

コンテナー Identity Management サーバーおよび Atomic Host システムは、コンテナーへの **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 コンテナーイメージは、**/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、コンテナー内の **/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

- コンテナーインストールは、**ipa-replica-install** で使用している非コンテナー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** コンテナーで利用できる Atomic オプション。完全な一覧は、コンテナー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. コンテナー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ーへの双方向通信を有効にします。
2. コンテナー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** コマンドに **--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および、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ー内の **/data/** にマップするため **/data/** が含まれます。

- コンテナー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ーに使用します。コンテナーのホスト名は、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ー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ーをインストールする場合は、**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。**ipa-server-install** の後に使用した場合には、インストールは **--hostname** を無視します。

- 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ー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ー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

- コンテナーを実行するには、**atomic run** コマンドを使用します。

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

インストール時にコンテナー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** コンテナーの実行は、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ース、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 コンテナーからホストシステムへのサーバーの移行

本章では、最初にコンテナー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、コンテナーからホストシステムへの移行

この手順では、コンテナー化された 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ー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ーに対して 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ーを停止する場合は、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. コンテナー内のサーバーから CA マスターの役割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. コンテナー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ー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ー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ー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ー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ー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ー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** コマンドが以下を行えないため、この手順は必須です。

   - 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ーを削除します。

2. **atomic uninstall** コマンドを実行して、コンテナー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

- コンテナー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>** にあります。新しいコンテナー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 III. SSSD コンテナーの使用

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 コンテナーの設定

システム管理者は、コンテナーで 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 ホスト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 コンテナー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 の他のコンテナーで実行しているサービスを使用できるようする、**unprivileged** として SSSD コンテナー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 コンテナーのデプロイ*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 コンテナーを使用した 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

- コンテナー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 コンテナーを使用した IDENTITY MANAGEMENT ドメインの登録

この手順では、SSSD コンテナー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ーにコピーされます。
- 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** コンテナー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 コマンドは、標準の **ipa-client-install** オプションを指定できます。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

atomic install の実行前に、Atomic Host の **/etc/sssd/ipa-client-install-options** ファイルに保存して、**ipa-client-install** にオプションを指定することもできます。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、コンテナーで SSSD を起動します。

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

```
# systemctl start sssd
```

3. **任意。**コンテナーが実行していることを確認します。

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

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

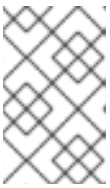
この手順では、SSSD コンテナーをインストールし、Atomic Host システムを Active Directory にジョインするように設定する方法を説明します。

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/sssd/realm-join-password** ファイルに保存します。

   ```
   # echo <password> > /etc/sssd/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

   atomic install でデフォルト名 (**sssd**) ではなく、カスタムのコンテナーイメージ名を指定する場合には、ファイルのパスにカスタム名を追加します (**/etc/sssd/<custom_container_name>/realm-join-password**)。

2. **atomic install** コマンドを実行して **sssd** コンテナー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/sssd realm join <ad.example.com>
docker run --rm=true --privileged --net=host -v /:/host -e NAME=sssd -e IMAGE=rhel7/sssd -
e HOST=/host rhel7/sssd /bin/install.sh realm join ad.example.com
Initializing configuration context from host ...
Password for Administrator:
Copying new configuration to host ...
Service sssd.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/sssd realm join --user <user_name> <ad.example.com>
```

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

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

```
# systemctl start sssd
```

4. **任意。**コンテナーが実行していることを確認します。

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

5. **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ー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 コンテナーのデプロイ

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ープロバイダーを使用する、特権のない複数の SSSD コンテナー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ーが、優先の ID ソースのみを使用できます。

7.1. 前提条件

- SSSD コンテナーが提供するサービスを他のコンテナーから使用する場合は、クライアントコンテナーの **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。
  その他のコンテナーから 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ー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 コンテナーを起動し、これをアイデンティティーリソースにジョインさせる

SSSD コンテナーを開始し、Active Directory などのアイデンティティー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** コマンドを使用して、SSSD コンテナーを起動します。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ーを作成します。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、コンテナーで稼働している SSSD を Active Directory ドメインに自動的に参加させます。

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

2. コンテナーを起動します。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ーに渡す

アプリケーションコンテナーで 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ー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 コンテナーのディレクトリーがアプリケーションコンテナー内の対応するディレクトリーにマッピングされます。

これでコンテナー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 コンテナーへのアクセスの付与および制限

Identity Management ドメインでは、各 SSSD コンテナーは、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、個々のコンテナー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、コンテナー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 コンテナーが提供するサービスを他のコンテナーから使用する場合は、クライアントコンテナーの **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。
  その他のコンテナーから 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ー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 コンテナーをインストールし、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/sssd/realm-join-password** ファイルに保存します。

   ```
   # echo <password> > /etc/sssd/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

   atomic install でデフォルト名 (**sssd**) ではなく、カスタムのコンテナーイメージ名を指定する場合には、ファイルのパスにカスタム名を追加します (**/etc/sssd/<custom_container_name>/realm-join-password**)。

2. **atomic install** コマンドを実行して sssd コンテナー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/sssd realm join -v <ad.example.com>
   docker run --rm=true --privileged --net=host -v /:/host -e NAME=sssd -e IMAGE=rhel7/sssd -
   e HOST=/host rhel7/sssd /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 sssd.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/sssd realm join --user <user_name> <ad.example.com>
```

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

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

```
# systemctl start sssd
```

4. **任意。**コンテナーが実行していることを確認します。

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

5. **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ー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. コンテナーで実行中の SSSD の認証

コンテナー内で実行している 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。

1. **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>:
```

2. 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. 異なるコンテナーでの SSSD KERBEROS キャッシュの使用

SSSD コンテナーから Kerberos キャッシュを他のコンテナーアプリケーションで利用できるようにするには、**/var/lib/sssd_container/<sssd-container-name>/client/etc/krb5.conf.d** と **/var/lib/sssd_container/<sssd-container-name>/client/var/lib/sss/pipes/** ディレクトリーをボリュームとしてアプリケーションコンテナーに指定します。以下に例を示します。

```
# docker run --rm --name=<application_container> -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/ docker-registry.engineering.redhat.com/idmqe/sssd-client-test:2.0 klist
```

前の例は、コンテナーで **klist** コマンドを実行し、SSSD コンテナーで管理される 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ーはチケットを使用しなくなります。

第10章 SSSD コンテナーの更新

この手順では、新しいバージョンの **rhel7/sssd** イメージがリリースされた場合に、SSSD (System Security Services Daemon) コンテナー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ー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ー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/sssd
   ```

3. 最新の SSSD イメージをインストールします。

   ```
   # atomic install rhel7/sssd
   ```

4. SSSD サービスを起動します。
   a. SSSD がシステムコンテナー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ー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ーを起動します。

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

第11章 SSSD コンテナー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) コンテナー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 コンテナー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) コンテナー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** コマンドを使用して、イメージ名を追加します。

```
# atomic uninstall rhel7/sssd
[... 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ーを削除します。たとえば、コマンドラインでは、以下のようになります。

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

3. Atomic Host 上の **sssd** サービスが、現在では設定されていないコンテナー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/sssd.service
# systemctl daemon-reload
```

11.2. ACTIVE DIRECTORY ドメインにジョインした SSSD コンテナー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) コンテナー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/sssd 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/sssd realm leave --user <user_name> <ad.example.com>
```

付録A コンテナーで実行している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、コンテナーで実行している 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

本セクションでは、**rhel7/rhel-tools** コンテナー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 コンテナーは、このコンテナー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ー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、ホストから分離せずに実行されることに注意してください。このコンテナー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等です。

手順

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

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

2. **rhel7/rhel-tools** コンテナーを起動します。

```
# 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** を入力してコンテナーを終了します。

```
# exit
```

5. サポートリクエストに **sosreport** アーカイブを添付します。

A.2. IDM および SSSD コンテナー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 コンテナー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** コンテナー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/sssd** コンテナーのバージョンを表示します。

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

A.3. コンテナーで実行している 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. **sssd** コンテナーを停止します。

```
# docker stop sssd
```

2. SSSD のキャッシュおよびログディレクトリーの内容を削除します。

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

3. **/etc/sssd/sssd.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. **sssd** コンテナーを起動します。

```
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/sssd-debug.tar.gz** アーカイブを作成します。

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

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

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/sssd/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 コンテナー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 コンテナーの設定**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 コンテナーのデプロイ**の更新	Lucie Maňásková
7.0-6	2018 年 1 月 29 日: マイナーな修正。	Aneta Šteflová Petrová
7.0-5	2017 年 11 月 20 日: **SSSD コンテナーを使用した 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 コンテナー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** コンテナー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ーイメージ**と**SSSD コンテナーを使用した 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