Red Hat Enterprise Linux 7

Using Containerized Identity Management Services

Overview and installation of containerized Identity Management services

Last Updated: 2022-01-28

Red Hat Enterprise Linux 7 Using Containerized Identity Management Services

Overview and installation of containerized Identity Management services

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

Legal Notice

Abstract

Learn about containerized Identity Management services in Red Hat Enterprise Linux 7, and start using them.

Table of Contents

CHAPTER 1. OVERVIEW OF THE CONTAINERIZED IDENTITY MANAGEMENT SERVICES

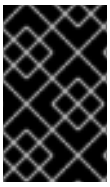
The following sections provide an overview of the containerized Identity Management services in Red Hat Enterprise Linux.

WARNING

The **rhel7/ipa-server** container is a Technology Preview feature. See Technology Preview Features Support Scope in the Red Hat Knowledgebase for details.

1.1. INTRODUCTION TO THE IPA-SERVER AND SSSD CONTAINERS

Using Identity Management or the System Security Services Daemon (SSSD) in a container ensures that all Identity Management or SSSD processes run in isolation from the host system. This enables the host system to run other software without conflicts with these processes.



IMPORTANT

The **ipa-server** and **sssd** containers are designed to be used on Red Hat Enterprise Linux Atomic Host systems. For details on Atomic Host, see Getting Started with Atomic in the Atomic documentation.

Additional Resources

- Overview of Containers in Red Hat Systems explains what containers are and how they work. The guide also includes links to documents for getting started with containers.
- Introduction to Red Hat Identity Management in the *Linux Domain Identity, Authentication, and Policy Guide* provides an overview of Identity Management, Identity Management servers, and Identity Management clients.
- Atomic Host documentation provides information about Red Hat Enterprise Linux Atomic Host and containers in general.

1.2. AVAILABLE CONTAINER IMAGES

The rhel7/ipa-server Container Image

- Enables you to run Identity Management servers and related services in a container.
- Provides Identity Management server services.

The rhel7/sssd Container Image

- Enables you to run the System Security Services Daemon (SSSD) in a container.
- Provides identity and authentication services to Atomic Host systems by enrolling the system to an Identity Management server or connecting it to an Active Directory domain.

- Provides identity and authentication services to applications running in other containers.

Additional Resources

- You can find more details about the container images in the Red Hat Container Catalog.

1.3. BENEFITS AND DRAWBACKS OF USING IDENTITY MANAGEMENT IN CONTAINERS

Benefits

- All Identity Management configuration and data are kept in isolation in a subdirectory.
- Migrating Identity Management servers is easier: the container subdirectory can be moved to another container or to the host system. See also Chapter 4, *Migrating a Server from a Container to a Host System*.

Drawbacks

- The Identity Management processes run under Atomic. For example, if the **docker** daemon terminates, the Identity Management server running under it also terminates. However, maintaining multiple replicas counters this drawback.
- SELinux separation is not applied to the components within a container. However, the components are still separated using process UIDs.
    - Note that although SELinux does not apply its mandatory access control (MAC) between the components, the **sVirt** project applies MAC to the container environment. This ensures that the container as a whole is protected from other containers.
    - The **ipa-server** container runs only the components required to run the Identity Management server itself. The container does not run any third-party components that can attack Identity Management due to the lack of SELinux isolation.
    - See also Secure Containers with SELinux in Atomic documentation.

PART I. USING THE IPA-SERVER CONTAINER (TECHNOLOGY PREVIEW)

This part covers how to deploy an Identity Management server and replica in a container, how to migrate a server from a container to a host system, and finally, how to uninstall server and replica containers.

CHAPTER 2. DEPLOYING AN IDENTITY MANAGEMENT SERVER IN A CONTAINER

This chapter describes how you can install a fresh Identity Management server to start a new topology.

Before you begin, read Section 2.1, "Prerequisites" and Section 2.2, "Available Configuration in Server and Replica Containers".

Choose one of the following installation procedures. If you are not sure which certificate authority (CA) configuration fits your situation, see Determining What CA Configuration to Use in the *Linux Domain Identity, Authentication, and Policy Guide*.

- Section 2.3, "Installing an Identity Management Server in a Container: Basic Installation"
- Section 2.4, "Installing an Identity Management Server in a Container: External CA"
- Section 2.5, "Installing an Identity Management Server in a Container: Without a CA"

After you are done, read Section 2.6, "Next Steps After Installation" .

2.1. PREREQUISITES

- Upgrade the Atomic Host system before installing the container. See Upgrading and Downgrading in the *Red Hat Enterprise Linux Atomic Host 7 Installation and Configuration Guide* .

2.2. AVAILABLE CONFIGURATION IN SERVER AND REPLICA CONTAINERS

What Is Available

Domain level 1 or higher

Domain level 0 is not available for containers. See also Displaying and Raising the Domain Level. As a consequence, servers running in containers can be joined in a replication agreement only with Identity Management servers based on Red Hat Enterprise Linux 7.3 or later.

Mixed container and non-container deployments

A single Identity Management domain topology can include both container-based and RPM-based servers.

What Is Not Available

Changing server components in a deployed container

Do not make runtime modifications of deployed containers. If you need to change or reinstall a server component, such as integrated DNS or Vault, create a new replica.

Upgrading between different Linux distributions

Do not change the platform on which an **ipa-server** container image runs. For example, do not change an image running on Red Hat Enterprise Linux to Fedora, Ubuntu, or CentOS. Similarly, do not change an image running on Fedora, Ubuntu, or CentOS to Red Hat Enterprise Linux. Identity Management supports only upgrades to later versions of Red Hat Enterprise Linux.

Downgrading the system with a running container

Do not downgrade the system on which an **ipa-server** container image runs.

Upstream containers on Atomic Host

Do not install upstream container images, such as the FreeIPA **ipa-server** image, on Atomic Host. Install only the container images available in Red Hat Enterprise Linux.

Multiple containers on a single Atomic Host

Install only one **ipa-server** container image on a single Atomic Host.

2.3. INSTALLING AN IDENTITY MANAGEMENT SERVER IN A CONTAINER: BASIC INSTALLATION

This procedure shows how to install a containerized Identity Management server in the default certificate authority (CA) configuration with an integrated CA.

Before You Start

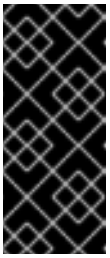
- Note that the container installation uses the same default configuration as a non-container installation using **ipa-server-install**. To specify custom configuration, add additional options to the **atomic install** command used in the procedure below:
  - Atomic options available for the **ipa-server** container. For a complete list, see the container help page.
  - Identity Management installer options accepted by **ipa-server-install**, described in Installing and Uninstalling an Identity Management Server in the *Linux Domain Identity, Authentication, and Policy Guide*.

Procedure

1. Use the **atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-server-install** command to start the installation.
   - The container requires its own host name. Use a different host name for the container than the host name of the Atomic Host system. The container's host name must be resolvable via DNS or the **/etc/hosts** file.

NOTE

Installing a server or replica container does not enroll the Atomic Host system itself to the Identity Management domain. If you use the Atomic Host system's host name for the server or replica, you will be unable to enroll the Atomic Host system later.



IMPORTANT

Always use the **--hostname** option with **atomic install** when installing the server or replica container. Because **--hostname** is considered an Atomic option in this case, not an Identity Management installer option, use it before the **ipa-server-install** option. The installation ignores **--hostname** when used after **ipa-server-install**.

   - If you are installing a server with integrated DNS, add also the **--ip-address** option to specify the public IP address of the Atomic Host that is reachable from the network. You can use **--ip-address** multiple times.

WARNING

Unless you want to install the container for testing purposes only, always use the **publish** option. Without **publish**, no ports will be published to the Atomic Host system, and the server will not be reachable from outside the container.

2. The **ipa-server-install** setup script starts:

```
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 ...]
```

The process is the same as when using the **ipa-server-install** utility to install a non-container server.

Example 2.1. Installation Command Examples

Command syntax for installing the **ipa-server** container:

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

To install a server container named **server-container** and use default values for the Identity Management server settings:

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

To install a server with a custom host name (**--hostname**) and integrated DNS (**--setup-dns**):

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

2.4. INSTALLING AN IDENTITY MANAGEMENT SERVER IN A CONTAINER: EXTERNAL CA

This procedure describes how to install a server with an integrated Identity Management certificate authority (CA) that is subordinate to an external CA.

A containerized Identity Management server and the Atomic Host system share only the parts of the file system that are mounted using a **bind** mount into the container. Therefore, operations related to external files must be performed from within this volume.

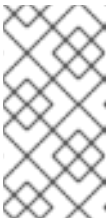
The **ipa-server** container image uses the **/var/lib/<container_name>/** directory to store persistent files on the Atomic Host file system. The persistent storage volume maps to the **/data/** directory inside the container.

Before You Start

- Note that the container installation uses the same default configuration as a non-container installation using **ipa-server-install**. To specify custom configuration, add additional options to the **atomic install** command used in the procedure below:
  - Atomic options available for the **ipa-server** container. For a complete list, see the container help page.
  - Identity Management installer options accepted by **ipa-server-install**, described in Installing and Uninstalling an Identity Management Server in the *Linux Domain Identity, Authentication, and Policy Guide*.

Procedure

1. Use the **atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-server-install --external-ca** command to start the installation.
   - The container requires its own host name. Use a different host name for the container than the host name of the Atomic Host system. The container's host name must be resolvable via DNS or the **/etc/hosts** file.



NOTE

Installing a server or replica container does not enroll the Atomic Host system itself to the Identity Management domain. If you use the Atomic Host system's host name for the server or replica, you will be unable to enroll the Atomic Host system later.

IMPORTANT

Always use the **--hostname** option with **atomic install** when installing the server or replica container. Because **--hostname** is considered an Atomic option in this case, not an Identity Management installer option, use it before the **ipa-server-install** option. The installation ignores **--hostname** when used after **ipa-server-install**.

   - If you are installing a server with integrated DNS, add also the **--ip-address** option to specify the public IP address of the Atomic Host that is reachable from the network. You can use **--ip-address** multiple times.

WARNING

Unless you want to install the container for testing purposes only, always use the **publish** option. Without **publish**, no ports will be published to the Atomic Host system, and the server will not be reachable from outside the container.

2. The **ipa-server-install** setup script starts:

```
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 ...]
```

   The process is the same as when using the **ipa-server-install** utility to install a non-container server.

3. The container installation script generates the certificate signing request (CSR) in the **/var/lib/<container_name>/root/ipa.csr** file. Submit the CSR to the external CA, and retrieve the issued certificate and the CA certificate chain for the issuing CA.
   See Installing a Server with an External CA as the Root CA in the *Linux Domain Identity, Authentication, and Policy Guide* for details.

4. Copy the signed CA certificate and the root CA certificate into the **/var/lib/<container_name>/** directory.

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

5. Use the **atomic run** command with the **--external-cert-file** option to specify the location of the certificates. Specify the location relative to the **/data/** directory because the installer performs the call from inside the container

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

6. The installation resumes. The installer now uses the supplied certificates to set up the subordinate CA.

2.5. INSTALLING AN IDENTITY MANAGEMENT SERVER IN A CONTAINER: WITHOUT A CA

This procedure describes how to install a server without an integrated Identity Management certificate authority (CA).

A containerized Identity Management server and the Atomic Host system share only the parts of the file system that are mounted using a **bind** mount into the container. Therefore, operations related to external files must be performed from within this volume.

The **ipa-server** container image uses the **/var/lib/<container_name>/** directory to store persistent files on the Atomic Host file system. The persistent storage volume maps to the **/data/** directory inside the container.

Before You Start

- Note that the container installation uses the same default configuration as a non-container installation using **ipa-server-install**. To specify custom configuration, add additional options to the **atomic install** command used in the procedure below:
  - Atomic options available for the **ipa-server** container. For a complete list, see the container help page.

- Identity Management installer options accepted by **ipa-server-install**, described in Installing and Uninstalling an Identity Management Server in the *Linux Domain Identity, Authentication, and Policy Guide*.

Procedure

1. Manually create the persistent storage directory for the container at **/var/lib/<container_name>/**:

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

2. Copy the files containing the certificate chain into the directory:

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

See Installing Without a CA in the *Linux Domain Identity, Authentication, and Policy Guide* for details on the required files.

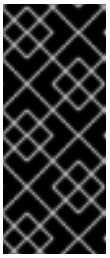
3. Use the **atomic install** command, and provide the required certificates from the third-party authority:

```
$ 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
```

- The container requires its own host name. Use a different host name for the container than the host name of the Atomic Host system. The container's host name must be resolvable via DNS or the **/etc/hosts** file.

NOTE

Installing a server or replica container does not enroll the Atomic Host system itself to the Identity Management domain. If you use the Atomic Host system's host name for the server or replica, you will be unable to enroll the Atomic Host system later.



IMPORTANT

Always use the **--hostname** option with **atomic install** when installing the server or replica container. Because **--hostname** is considered an Atomic option in this case, not an Identity Management installer option, use it before the **ipa-server-install** option. The installation ignores **--hostname** when used after **ipa-server-install**.

- If you are installing a server with integrated DNS, add also the **--ip-address** option to specify the public IP address of the Atomic Host that is reachable from the network. You can use **--ip-address** multiple times.

WARNING

Unless you want to install the container for testing purposes only, always use the **publish** option. Without **publish**, no ports will be published to the Atomic Host system, and the server will not be reachable from outside the container.

4. The **ipa-server-install** setup script starts:

```
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 ...]
```

The process is the same as when using the **ipa-server-install** utility to install a non-container server.

2.6. NEXT STEPS AFTER INSTALLATION

- To run the container, use the **atomic run** command:

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

If you specified a name for the container when you installed it:

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

- A running **ipa-server** container works in the same way as in a standard Identity Management deployment on bare-metal or virtual machine systems. For example, you can enroll hosts to the domain or manage the topology using the command-line interface, the web UI, or JSONRPC-API in the same way as RPM-based Identity Management systems.

CHAPTER 3. DEPLOYING AN IDENTITY MANAGEMENT REPLICA IN A CONTAINER

This chapter describes how you can install an Identity Management replica. For example, creating a container-based replica can be useful if you want to gradually transfer the workload in your existing topology to container-based servers.

Before you begin, read Section 3.1, "Prerequisites" and Section 3.2, "Available Configuration in Server and Replica Containers".

Choose one of the following installation procedures. If you are not sure which certificate authority (CA) configuration fits your situation, see Determining What CA Configuration to Use in the *Linux Domain Identity, Authentication, and Policy Guide*.

- Section 3.3, "Installing an Identity Management Replica in a Container: Basic Installation"
- Section 3.4, "Installing an Identity Management Replica in a Container: Without a CA"

After you are done, read Section 3.5, "Next Steps After Installation" .

3.1. PREREQUISITES

- Upgrade the Atomic Host system before installing the container. See Upgrading and Downgrading in the *Red Hat Enterprise Linux Atomic Host 7 Installation and Configuration Guide* .

3.2. AVAILABLE CONFIGURATION IN SERVER AND REPLICA CONTAINERS

What Is Available

Domain level 1 or higher

Domain level 0 is not available for containers. See also Displaying and Raising the Domain Level. As a consequence, servers running in containers can be joined in a replication agreement only with Identity Management servers based on Red Hat Enterprise Linux 7.3 or later.

Mixed container and non-container deployments

A single Identity Management domain topology can include both container-based and RPM-based servers.

What Is Not Available

Changing server components in a deployed container

Do not make runtime modifications of deployed containers. If you need to change or reinstall a server component, such as integrated DNS or Vault, create a new replica.

Upgrading between different Linux distributions

Do not change the platform on which an **ipa-server** container image runs. For example, do not change an image running on Red Hat Enterprise Linux to Fedora, Ubuntu, or CentOS. Similarly, do not change an image running on Fedora, Ubuntu, or CentOS to Red Hat Enterprise Linux. Identity Management supports only upgrades to later versions of Red Hat Enterprise Linux.

Downgrading the system with a running container

Do not downgrade the system on which an **ipa-server** container image runs.

Upstream containers on Atomic Host

Do not install upstream container images, such as the FreeIPA **ipa-server** image, on Atomic Host. Install only the container images available in Red Hat Enterprise Linux.

Multiple containers on a single Atomic Host

Install only one **ipa-server** container image on a single Atomic Host.

3.3. INSTALLING AN IDENTITY MANAGEMENT REPLICA IN A CONTAINER: BASIC INSTALLATION

This procedure shows how to install a containerized Identity Management server in the default certificate authority (CA) configuration with an integrated CA.

Before You Start

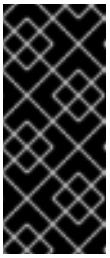
- Note that the container installation uses the same default configuration as a non-container installation using **ipa-replica-install**. To specify custom configuration, add additional options to the **atomic install** command used in the procedure below:
  - Atomic options available for the **ipa-server** container. For a complete list, see the container help page.
  - Identity Management installer options accepted by **ipa-replica-install**, described in Installing and Uninstalling Identity Management Replicas in the *Linux Domain Identity, Authentication, and Policy Guide*.
- You must have an installed server available: either on a bare metal machine, or on another Atomic Host system.

Procedure

1. If you want to install a replica against a master server in a container, enable two-way communication to the master container over the ports specified in Installing and Uninstalling an Identity Management Server in the *Linux Domain Identity, Authentication, and Policy Guide* .
2. Use the **atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-replica-install** command to start the installation. Include the **--server** and **--domain** options to specify the host name and domain name of your Identity Management server.
   - The container requires its own host name. Use a different host name for the container than the host name of the Atomic Host system. The container's host name must be resolvable via DNS or the **/etc/hosts** file.

NOTE

Installing a server or replica container does not enroll the Atomic Host system itself to the Identity Management domain. If you use the Atomic Host system's host name for the server or replica, you will be unable to enroll the Atomic Host system later.



IMPORTANT

Always use the **--hostname** option with **atomic install** when installing the server or replica container. Because **--hostname** is considered an Atomic option in this case, not an Identity Management installer option, use it before the **ipa-server-install** option. The installation ignores **--hostname** when used after **ipa-server-install**.

- If you are installing a server with integrated DNS, add also the **--ip-address** option to specify the public IP address of the Atomic Host that is reachable from the network. You can use **--ip-address** multiple times.
- Due to a known issue in the interactive replica installation mode , add standard **ipa-replica-install** options to specify one of the following:
  - A privileged user's credentials. See Example 3.1, "Installation Command Examples".
  - Random password for bulk enrollment. See Installing a Replica Using a Random Password in the *Linux Domain Identity, Authentication, and Policy Guide* .

WARNING

Unless you want to install the container for testing purposes only, always use the **publish** option. Without **publish**, no ports will be published to the Atomic Host system, and the server will not be reachable from outside the container.

Example 3.1. Installation Command Examples

Command syntax for installing the **ipa-server** container:

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

To install a replica container named **replica-container** using the administrator's credentials, while using default values for the Identity Management replica settings:

```
$ 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. INSTALLING AN IDENTITY MANAGEMENT REPLICA IN A CONTAINER: WITHOUT A CA

This procedure describes how to install a server without an integrated Identity Management certificate authority (CA).

A containerized Identity Management server and the Atomic Host system share only the parts of the file system that are mounted using a **bind** mount into the container. Therefore, operations related to external files must be performed from within this volume.

The **ipa-server** container image uses the **/var/lib/<container_name>/** directory to store persistent files on the Atomic Host file system. The persistent storage volume maps to the **/data/** directory inside the container.

Before You Start

- Note that the container installation uses the same default configuration as a non-container installation using **ipa-replica-install**. To specify custom configuration, add additional options to the **atomic install** command used in the procedure below:
  - Atomic options available for the **ipa-server** container. For a complete list, see the container help page.
  - Identity Management installer options accepted by **ipa-replica-install**, described in Installing and Uninstalling Identity Management Replicas in the *Linux Domain Identity, Authentication, and Policy Guide*.
- You must have an installed server available: either on a bare metal machine, or on another Atomic Host system.

Procedure

1. If you want to install a replica against a master server in a container, enable two-way communication to the master container over the ports specified in Installing and Uninstalling an Identity Management Server in the *Linux Domain Identity, Authentication, and Policy Guide* .
2. Manually create the persistent storage directory for the container at **/var/lib/<container_name>/**:

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

3. Copy the files containing the certificate chain into the directory:

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

   See Installing Without a CA in the *Linux Domain Identity, Authentication, and Policy Guide* for details on the required files.

4. Use the **atomic install rhel7/ipa-server publish --hostname fully_qualified_domain_name ipa-replica-install** command, include the **--server** and **--domain** options to specify the host name and domain name of your Identity Management server, and provide the required certificates from the third-party authority:

   ```
   $ 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
```

NOTE

The paths to the certificates include /**data**/ because the persistent storage volume maps to /**data**/ inside the container.

- The container requires its own host name. Use a different host name for the container than the host name of the Atomic Host system. The container's host name must be resolvable via DNS or the **/etc/hosts** file.

NOTE

Installing a server or replica container does not enroll the Atomic Host system itself to the Identity Management domain. If you use the Atomic Host system's host name for the server or replica, you will be unable to enroll the Atomic Host system later.

IMPORTANT

Always use the **--hostname** option with **atomic install** when installing the server or replica container. Because **--hostname** is considered an Atomic option in this case, not an Identity Management installer option, use it before the **ipa-server-install** option. The installation ignores **--hostname** when used after **ipa-server-install**.

- If you are installing a server with integrated DNS, add also the **--ip-address** option to specify the public IP address of the Atomic Host that is reachable from the network. You can use **--ip-address** multiple times.

- Due to a known issue in the interactive replica installation mode , add standard **ipa-replica-install** options to specify one of the following:

  - A privileged user's credentials. See Example 3.1, "Installation Command Examples".

  - Random password for bulk enrollment. See Installing a Replica Using a Random Password in the *Linux Domain Identity, Authentication, and Policy Guide* .

WARNING

Unless you want to install the container for testing purposes only, always use the **publish** option. Without **publish**, no ports will be published to the Atomic Host system, and the server will not be reachable from outside the container.

3.5. NEXT STEPS AFTER INSTALLATION

- To run the container, use the **atomic run** command:

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

If you specified a name for the container when you installed it:

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

- A running **ipa-server** container works in the same way as in a standard Identity Management deployment on bare-metal or virtual machine systems. For example, you can enroll hosts to the domain or manage the topology using the command-line interface, the web UI, or JSONRPC-API in the same way as RPM-based Identity Management systems.

CHAPTER 4. MIGRATING A SERVER FROM A CONTAINER TO A HOST SYSTEM

This chapter describes how you can migrate a server originally installed in a container to a bare-metal or a virtual machine system. In the following scenario, we migrate to a Red Hat Enterprise Linux system.

4.1. MIGRATING AN IDENTITY MANAGEMENT SERVER FROM A CONTAINER TO THE HOST SYSTEM

This procedure shows how to migrate a containerized Identity Management server to the host system and, optionally, decomission the container.

Procedure

1. Enroll the host system as an Identity Management replica against the container. If you want to decommission the container with the Identity Management server later, make sure you create the replica with a certificate authority (CA) configured.
   See Installing and Uninstalling Identity Management Replicas .

2. Migrate the CA master responsibilities from the server in the container to the new replica on the host system.
   See Promoting a Replica to a Master CA Server .

3. Decommission the server in the container.
   See Chapter 5, *Uninstalling Server and Replica Containers* .

CHAPTER 5. UNINSTALLING SERVER AND REPLICA CONTAINERS

This chapter describes how you can uninstall an Identity Management server or replica container.

5.1. UNINSTALLING A SERVER OR REPLICA CONTAINER

This procedure shows how to uninstall an Identity Management server or replica container and make sure the server or replica is properly removed from the topology.

Procedure

1. To ensure that a replica container belonging to an existing topology is properly removed from that topology, use the **ipa server-del <container-host-name>** command on any enrolled host. This step is necessary because the **atomic uninstall** command does not:

   - Perform checks to prevent disconnected domain level 1 topology or the removal of the last certificate authority (CA), key recovery authority (KRA), or DNS server
   - Remove the replica container from the existing topology

2. Use the **atomic uninstall** command, and include the container name and image name:

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

5.2. NEXT STEPS AFTER UNINSTALLING

- You can find a backup of the container's mounted data directory under **/var/lib/<container_name>.backup.<timestamp>**. If you need to create a new container, the backup enables you to reuse the persistent data stored in the volume.

PART II. USING THE SSSD CONTAINER

This part covers how to deploy, configure, update and uninstall the **SSSD** container on Atomic Host. In addition, this documentation explains how to grant or restrict access to **SSSD** containers and how to create and use a centralized Kerberos credential cache.

CHAPTER 6. CONFIGURING THE SSSD CONTAINER TO PROVIDE IDENTITY AND AUTHENTICATION SERVICES ON ATOMIC HOST

As a system administrator, you can use SSSD in a container to provide external identity, authentication, and authorization services for the Atomic Host system. This chapter describes how to run the SSSD container as **privileged**, which enables users from external identity sources (Identity Management or Active Directory) to leverage the services running on the Atomic host itself.

Alternatively, you can run the SSSD container as **unprivileged**, which enables users from external identity sources (Identity Management or Active Directory) to leverage the services running in other containers on the Atomic Host. This is covered in Chapter 7, *Deploying SSSD Containers With Different Configurations*.

Before you start, see:

- Section 6.1, "Prerequisites"

To enroll the Atomic Host to an Identity Management server, see:

- Section 6.2, "Enrolling to an Identity Management Domain Using a Privileged SSSD Container"

To enroll the Atomic Host to Active Directory, see:

- Section 6.3, "Joining an Active Directory Domain Using an SSSD Container"

6.1. PREREQUISITES

- Upgrade the Atomic Host system before installing the container. See Upgrading and Downgrading in the Red Hat Enterprise Linux Atomic Host 7 *Installation and Configuration Guide*.

6.2. ENROLLING TO AN IDENTITY MANAGEMENT DOMAIN USING A PRIVILEGED SSSD CONTAINER

This procedure describes how to install an SSSD container and configure it for enrollment against an Identity Management server. During the installation:

- Various configuration and data are copied into the container.
- The **ipa-client-install** utility for configuring an Identity Management client starts.
- After a successful enrollment into the Identity Management domain, the configuration and data are copied back to the Atomic Host system.

Prerequisites

You need one of the following:

- A random password for one-time client enrollment of the Atomic Host system to the Identity Management domain. To generate the password, add the Atomic Host system as an Identity Management host on the Identity Management server, for example:

```
$ ipa host-add <atomic.example.com> --random
[... output truncated ...]
```

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

For details, see Installing a Client in the *Linux Domain Identity, Authentication, and Policy Guide* .

- Credentials of an Identity Management user allowed to enroll clients. By default, this is the **admin** user.

Procedure

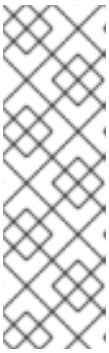
1. Start the **sssd** container installation by using the **atomic install** command, and provide the random password or credentials of an IdM user that is allowed to enroll new hosts. In most cases, this is the **admin** user.

```
# 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 ...]
```

The **atomic install rhel7/sssd** command accepts standard **ipa-client-install** options. Depending on your configuration, you might need to provide additional information using these options. For example, if **ipa-client-install** cannot determine the host name of your server and the domain name, use the **--server** and **--domain** options:

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



NOTE

You can also pass options to **ipa-client-install** by storing them to the **/etc/sssd/ipa-client-install-options** file on the Atomic Host before running **atomic install**. For example, the file can contain:

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

2. Start SSSD in the container by using one of the following commands:

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

```
# systemctl start sssd
```

3. *Optional.* Confirm that the container is running:

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

4. *Optional.* Confirm that SSSD on the Atomic Host resolves identities from the Identity Management domain.

   a. Obtain a Kerberos ticket for an Identity Management user, and log in to the Atomic Host by using the **ssh** utility.

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

   b. Use the **id** utility to verify that you are logged in as the intended user:

   ```
   $ 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. Use the **hostname** utility to verify that you are logged in to the Atomic Host system:

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

6.3. JOINING AN ACTIVE DIRECTORY DOMAIN USING AN SSSD CONTAINER

This procedure describes how to install an SSSD container and configure it to join the Atomic Host system to Active Directory.

Procedure

1. Save the password of a user allowed to enroll systems to the Active Directory domain, such as the Administrator, in the **/etc/sssd/realm-join-password** file on the Atomic Host system:

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

   Providing the password in the file is necessary because the **realm join** command does not accept the password as a command-line parameter.

   NOTE

   If you want to specify a custom container image name later with the **atomic install** command to use instead of the default name (**sssd**), add the custom name to the path of the file: **/etc/sssd/<custom_container_name>/realm-join-password**.

2. Start the **sssd** container installation by using the **atomic install** command, and specify the realm that you want to join. If you are using the default Administrator user account for the operation:

   ```
   # 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.
```

If you are using another user account, specify it with the **--user** option:

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

3. Start SSSD in the container by using one of the following commands:

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

```
# systemctl start sssd
```

4. *Optional.* Confirm that the container is running:

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

5. *Optional.* On the Atomic Host system, confirm that SSSD resolves identities from the Active Directory domain:

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

Additional Resources

- For details on the **realmd** utility, see Using realmd to Connect to an Active Directory Domain in the *Windows Integration Guide* or the realm(8) man page.

CHAPTER 7. DEPLOYING SSSD CONTAINERS WITH DIFFERENT CONFIGURATIONS

As a system administrator, you can deploy multiple unprivileged SSSD containers that each use a specific identity provider, such as Identity Management or Active Directory. This enables other application containers to use only their preferred identity source.

7.1. PREREQUISITES

- To use the services provided by the SSSD container from other containers, the client container's **rhel7** base image must include the **sssd-client** package. However, the default **rhel7** base image does not include this package.
  If you need to use the SSSD services from other containers, create your own image for the client container based on the default **rhel7** base image and include **sssd-client**. For details, see Creating Docker images.

7.2. STARTING THE SSSD CONTAINER AND JOINING IT TO AN IDENTITY RESOURCE

To start an SSSD container and join it to an identity resource, such as Active Directory:

1. Start the SSSD container by using the **atomic install** command. For example:

   ```
   # 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
   ```

   The previous example creates an SSSD application container named **ad_sssd**. Pass the DNS server IP address, search domain, host name, and **realm join** command to **atomic install** to automatically join SSSD running in the container to the Active Directory domain.

   Repeat this step for each identity provider for which you want to provide an SSSD container.

2. Start the container. For example:

   ```
   # atomic run ad_sssd
   ```

7.3. PASSING THE SSSD CACHE TO AN APPLICATION CONTAINER

To use the SSSD cache in an application container, pass the relevant directories to the **docker run** command when you start the application container:

```
# 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>
```

This maps the directories of the SSSD container to the corresponding directory inside the application container.

The application running in the container is now able to authenticate using, for example, the **kinit** utility or the **mod_auth_gssapi** module.

CHAPTER 8. GRANTING AND RESTRICTING ACCESS TO SSSD CONTAINERS USING HBAC RULES

For the Identity Management domain, each SSSD container represents itself as a different host, and administrators can set up host-based access control (HBAC) rules to allow or restrict access to individual containers separately.

For details about configuring HBAC rules in Identity Management, see Configuring Host-Based Access Control in the *Linux Domain Identity, Authentication, and Policy Guide*

CHAPTER 9. CREATING AND USING A CENTRALIZED KERBEROS CREDENTIAL CACHE

As a system administrator, you can centrally authenticate to a Kerberos server to initialize the credential cache. You can also ensure that applications running in containers are able to use this central cache to authenticate without requiring to manage keytab files, authentication, or renewal separately.

9.1. PREREQUISITES

- To use the services provided by the SSSD container from other containers, the client container's **rhel7** base image must include the **sssd-client** package. However, the default **rhel7** base image does not include this package.
  If you need to use the SSSD services from other containers, create your own image for the client container based on the default **rhel7** base image and include **sssd-client**. For details, see Creating Docker images.

9.2. JOINING AN ACTIVE DIRECTORY DOMAIN USING AN SSSD CONTAINER

This procedure describes how to install an SSSD container and configure it to join the Atomic Host system to Active Directory.

Procedure

1. Save the password of a user allowed to enroll systems to the Active Directory domain, such as the Administrator, in the **/etc/sssd/realm-join-password** file on the Atomic Host system:

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

   Providing the password in the file is necessary because the **realm join** command does not accept the password as a command-line parameter.

   NOTE

   If you want to specify a custom container image name later with the **atomic install** command to use instead of the default name (**sssd**), add the custom name to the path of the file: **/etc/sssd/<custom_container_name>/realm-join-password**.

2. Start the **sssd** container installation by using the **atomic install** command, and specify the realm that you want to join. If you are using the default Administrator user account for the operation:

   ```
   # 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.
   ```

If you are using another user account, specify it with the **--user** option:

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

3. Start SSSD in the container by using one of the following commands:

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

```
# systemctl start sssd
```

4. *Optional.* Confirm that the container is running:

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

5. *Optional.* On the Atomic Host system, confirm that SSSD resolves identities from the Active Directory domain:

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

Additional Resources

- For details on the **realmd** utility, see Using realmd to Connect to an Active Directory Domain in the *Windows Integration Guide* or the realm(8) man page.

9.3. AUTHENTICATING TO SSSD RUNNING IN A CONTAINER

To authenticate to a Kerberos server using SSSD that runs in a container:

1. Pass the **kinit** option to the **docker exec** command. For example, to authenticate as the *administrator* user:

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

2. Optionally, verify that your Kerberos credential cache is stored in the Kerberos Credential Manager (KCM):

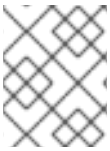
```
# docker exec -i <container_name> klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@<DOMAIN>

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. USING THE SSSD KERBEROS CACHE IN A DIFFERENT CONTAINER

To make a Kerberos cache from an SSSD container available to other container applications, pass the **/var/lib/sssd_container/<sssd-container-name>/client/etc/krb5.conf.d** and **/var/lib/sssd_container/<sssd-container-name>/client/var/lib/sss/pipes/** directories as volumes to the application container. For example:

```
# 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
```

The previous example executes the **klist** command in the container and lists the Kerberos tickets managed by the SSSD container.



NOTE

If you delete the Kerberos ticket from the cache using the **kdestroy** utility, the application containers can no longer use the ticket.

CHAPTER 10. UPDATING SSSD CONTAINERS

This procedure describes how you can update System Security Services Daemon (SSSD) containers if a new version of the **rhel7/sssd** image is released.

Procedure

1. Stop the SSSD service:
   a. If SSSD is running as a system container:

      ```
      # systemctl stop sssd
      ```

   b. If SSSD is running as an application container:

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

2. Use the **docker rm** command to remove the image:

   ```
   # docker rm rhel7/sssd
   ```

3. Install the latest SSSD image:

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

4. Start the SSSD service:
   a. If SSSD runs as a system container:

      ```
      # systemctl start sssd
      ```

   b. If SSSD runs as an application container, start each container using the **atomic start** command:

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

CHAPTER 11. UNINSTALLING SSSD CONTAINERS

This chapter describes how you can uninstall a System Security Services Daemon (SSSD) container.

11.1. UNINSTALLING AN SSSD CONTAINER ENROLLED IN AN IDENTITY MANAGEMENT DOMAIN

This procedure describes how to uninstall the System Security Services Daemon (SSSD) container from an Atomic Host system and unenroll the Atomic Host system from the Identity Management domain.

Procedure

1. Use the **atomic uninstall** command, and include the image name:

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

2. Remove the Atomic Host system's host entry on an Identity Management server. For example, from the command line:

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

3. To prevent the **sssd** service on the Atomic Host from attempting to start the container that is now unconfigured, remove the **systemd** unit file for the service and reload the **systemd** process:

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

11.2. UNINSTALLING AN SSSD CONTAINER JOINED TO AN ACTIVE DIRECTORY DOMAIN

This procedure describes how to uninstall the System Security Services Daemon (SSSD) container from an Atomic Host system and unenroll the Atomic Host system from the Active Directory domain.

Procedure

- Use the **atomic uninstall** command, include the image name, and specify the realm that you want to leave. If you are using the default Administrator user account for the operation:

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

  If you are using another user account, specify it with the **--user** option:

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

APPENDIX A. COLLECTING INFORMATION FOR TROUBLESHOOTING IDM AND SSSD RUNNING IN A CONTAINER

This appendix describes procedures that help you to troubleshoot IdM and SSSD running in a container, as well as collecting important configuration and log files that you can attach to Red Hat support tickets.

A.1. CREATING AN SOSREPORT ON ATOMIC HOST

This section describes how to install and start the **rhel7/rhel-tools** container, as well as creating an **sosreport**.

The **rhel7/rhel-tools** container uses privileged security switches that enables processes running in this container:

- To interact with all semaphores and shared memory segments on the host
- To listen to ports and raw IP traffic on the host's network
- Interact with all processes on the host

Note that **rhel7/rhel-tools** runs without any separation from the host. Using the utilities provided by this container is similar as running them as the **root** user directly on the system.

Procedure

1. Install the **rhel7/rhel-tools** container:

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

2. Start the **rhel7/rhel-tools** container:

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

3. Run the **sosreport** utility:

```
# sosreport
```

   The utility stores the archive of the collected information in the **/host/var/tmp/sos_tal4k_*** file.

4. Enter **exit** to leave the container.

```
# exit
```

5. Attach the **sosreport** archive to a support request.

A.2. DISPLAYING THE VERSIONS OF IDM AND SSSD CONTAINERS

This section describes how to display the version of installed IdM and SSSD containers. For example, use this information to search the Red Hat Enterprise Linux Release Notes if a problem has been fixed in a newer version.

Procedure

- Display the version of the **rhel7/ipa-server** container:

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

- Display the version of the **rhel7/sssd** container:

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

A.3. CREATING DEBUG LOGS FOR SSSD RUNNING IN A CONTAINER

This section describes how to create an archive with important SSSD configuration and log files.

Procedure

1. Stop the **sssd** container:

```
# docker stop sssd
```

2. Remove the contents of the SSSD cache and log directories:

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

3. Edit the **/etc/sssd/sssd.conf** file, and set the **debug_level** parameters to **9**:

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

[nss]
debug_level = 9
```

4. Start the **sssd** container:

```
docker start sssd
```

5. Create the **/tmp/sssd-debug.tar.gz** archive that contains the relevant SSSD configuration and log files:

```
# 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. Attach the **/tmp/sssd-debug.tar.gz** file to the support case.

A.4. DISPLAYING THE IDM CLIENT INSTALLATION LOG

This section describes how you display the IdM client installation log. The log files help you to debug the problem if the client installation fails.

Procedure

- To display the IdM client installation log:

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

APPENDIX B. REVISION HISTORY

The revision numbers below relate to the edition of this manual, not to version numbers of Red Hat Enterprise Linux.

Version	Date and change	Author
7.0-11	Oct 15 2019: Added troubleshooting appendix.	Marc Muehlfeld
7.0-10	Sep 26 2019: Added *Granting and Restricting Access to SSSD Containers Using HBAC Rules*.	Marc Muehlfeld
7.0-9	Aug 23 2019: Updated introduction of *Configuring the SSSD Container to Provide Identity and Authentication Services on Atomic Host*.	Marc Muehlfeld
7.0-8	Apr 05 2018: Preparing document for 7.5 GA publication.	Lucie Maňásková
7.0-7	Mar 19 2018: Updated *Deploying **sssd** containers with different configurations*.	Lucie Maňásková
7.0-6	Jan 29 2018: Minor fixes.	Aneta Šteflová Petrová
7.0-5	Nov 20 2017: Updated *Enrolling to an Identity Management Domain Using an SSSD Container*.	Aneta Šteflová Petrová
7.0-4	Sep 12 2017: Added a procedure for uninstalling an SSSD container joined to an AD domain.	Aneta Šteflová Petrová
7.0-3	Aug 28 2017: Updated part *Using the **sssd** container* with more user stories and fixes.	Aneta Šteflová Petrová
7.0-2	Aug 14 2017: Updated sections *Available Container Images* and *Joining an Active Directory Domain Using an SSSD Container*.	Aneta Šteflová Petrová
7.0-1	Jul 18 2017: Document version for 7.4 GA publication.	Aneta Šteflová Petrová