Red Hat Enterprise Linux 8

Installing Identity Management

Getting started using Identity Management

Last Updated: 2019-05-07

Red Hat Enterprise Linux 8 Installing Identity Management

Getting started using Identity Management

Legal Notice

Copyright © 2019 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Abstract

This documentation collection provides instructions on how to install Identity Management on Red Hat Enterprise Linux 8 (RHEL) and how to upgrade to it from RHEL 7.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages, make sure you are viewing the documentation in the Multi-page HTML format. Highlight the part of text that you want to comment on. Then, click the **Add Feedback** pop-up that appears below the highlighted text, and follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
  1. Go to the Bugzilla website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.

PART I. INSTALLING IDENTITY MANAGEMENT

CHAPTER 1. PREPARING THE SYSTEM FOR IDENTITY MANAGEMENT SERVER INSTALLATION

The following sections list the requirements to install an Identity Management server. Before the installation, make sure your system meets these requirements.

1.1. HARDWARE RECOMMENDATIONS

RAM is the most important hardware feature to size properly. Make sure your system has enough RAM available. Typical RAM requirements are:

- For 10,000 users and 100 groups: at least 3 GB of RAM and 1 GB swap space
- For 100,000 users and 50,000 groups: at least 16 GB of RAM and 4 GB of swap space

For larger deployments, it is more effective to increase the RAM than to increase disk space because much of the data is stored in cache.

NOTE

A basic user entry or a simple host entry with a certificate is approximately 5–10 kB in size.

1.2. CUSTOM CONFIGURATION REQUIREMENTS FOR IDENTITY MANAGEMENT

Install an Identity Management server on a clean system without any custom configuration for services such as DNS, Kerberos, Apache, or Directory Server.

The Identity Management server installation overwrites system files to set up the Identity Management domain. Identity Management backs up the original system files to **/var/lib/ipa/sysrestore/**. When an Identity Management server is uninstalled at the end of the lifecycle, these files are restored.

1.2.1. IPv6 requirements in Identity Management

The IdM system must have the IPv6 protocol enabled in the kernel. If IPv6 is disabled, then the CLDAP plug-in used by the IdM services fails to initialize.

NOTE

IPv6 does not have to be enabled on the network.

1.3. HOST NAME AND DNS REQUIREMENTS FOR IDENTITY MANAGEMENT

This section lists the host name and DNS requirements for server and replica systems. It also shows how to verify that the systems meet the requirements.

The requirements in this section apply to all Identity Management servers, those with integrated DNS and those without integrated DNS.

WARNING

DNS records are vital for nearly all Identity Management domain functions, including running LDAP directory services, Kerberos, and Active Directory integration. Be extremely cautious and ensure that:

- You have a tested and functional DNS service available
- The service is properly configured

This requirement applies to Identity Management servers with **and** without integrated DNS.

Verify the server host name

The host name must be a fully qualified domain name, such as **server.example.com**.
The fully qualified domain name must meet the following conditions:

- It is a valid DNS name, which means only numbers, alphabetic characters, and hyphens (-) are allowed. Other characters, such as underscores (_), in the host name cause DNS failures.
- It is all lower-case. No capital letters are allowed.
- It does not resolve to the loopback address. It must resolve to the system's public IP address, not to **127.0.0.1**.

To verify the host name, use the **hostname** utility on the system where you want to install:

```
# hostname
server.idm.example.com
```

The output of **hostname** must not be **localhost** or **localhost6**.

Verify the forward and reverse DNS configuration

1. Obtain the IP address of the server. The **ip addr show** command displays both the IPv4 and IPv6 addresses. In the following example, the relevant IPv6 address is **2001:DB8::1111** because its scope is global:

```
[root@server ~]# ip addr show
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
 link/ether 00:1a:4a:10:4e:33 brd ff:ff:ff:ff:ff:ff
 inet 192.0.2.1/24 brd 192.0.2.255 scope global dynamic eth0
  valid_lft 106694sec preferred_lft 106694sec
 inet6 2001:DB8::1111/32 scope global dynamic
   valid_lft 2591521sec preferred_lft 604321sec
 inet6 fe80::56ee:75ff:fe2b:def6/64 scope link
       valid_lft forever preferred_lft forever
...
```

1. Verify the forward DNS configuration using the **dig** utility.

   a. Run the command **dig +short *server.example.com* A**. The returned IPv4 address must match the IP address returned by **ip addr show**:

   ```
   [root@server ~]# dig +short server.example.com A
   192.0.2.1
   ```

   b. Run the command **dig +short *server.example.com* AAAA**. If it returns an address, it must match the IPv6 address returned by **ip addr show**:

   ```
   [root@server ~]# dig +short server.example.com AAAA
   2001:DB8::1111
   ```

   > NOTE
   >
   > If **dig** does not return any output for the AAAA record, it does not indicate incorrect configuration. No output only means that no IPv6 address is configured in DNS for the system. If you do not intend to use the IPv6 protocol in your network, you can proceed with the installation in this situation.

2. Verify the reverse DNS configuration (PTR records). Use the **dig** utility and add the IP address.
   If the commands below display a different host name or no host name, even though **dig +short *server_host_name*** in the previous step returned an IP address, it indicates that the reverse DNS configuration is incorrect.

   a. Run the command **dig +short -x *IPv4_address***. The output must display the server host name. For example:

   ```
   [root@server ~]# dig +short -x 192.0.2.1
   server.example.com
   ```

   b. If the command **dig +short -x *server.example.com* AAAA** in the previous step returned an IPv6 address, use **dig** to query the IPv6 address too. The output must display the server host name. For example:

   ```
   [root@server ~]# dig +short -x 2001:DB8::1111
   server.example.com
   ```

   > NOTE
   >
   > If **dig +short *server.example.com* AAAA** in the previous step did not display any IPv6 address, querying the AAAA record does not output anything. In this case, this is normal behavior and does not indicate incorrect configuration.

Verify the standards-compliance of DNS forwarders (required for integrated DNS only)

Ensure that all DNS forwarders you want to use with the Identity Management DNS server comply with the Extension Mechanisms for DNS (EDNS0) and DNS Security Extensions (DNSSEC) standards. To do this, inspect the output of the following command for each forwarder separately:

```
$ dig +dnssec @IP_address_of_the_DNS_forwarder . SOA
```

The expected output displayed by the command contains the following information:

- status: **NOERROR**
- flags: **ra**
- EDNS flags: **do**
- The **RRSIG** record must be present in the **ANSWER** section

If any of these items is missing from the output, inspect the documentation for your DNS forwarder and verify that EDNS0 and DNSSEC are supported and enabled. In the latest versions of the BIND server, the **dnssec-enable yes;** option must be set in the **/etc/named.conf** file.

Example of the expected output produced by **dig**:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48655
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

;; ANSWER SECTION:
. 31679 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2015100701 1800 900 604800 86400
. 31679 IN RRSIG SOA 8 0 86400 20151017170000 20151007160000 62530 . GNVz7SQs [...]
```

Verify the/etc/hosts file

IMPORTANT

Do not modify the **/etc/hosts** file manually. If **/etc/hosts** has been modified manually before, make sure its contents conform to the following rules.

The following is an example of a correctly configured **/etc/hosts** file:

- It properly lists the IPv4 and IPv6 localhost entries for the host.
- These entries are followed by the Identity Management server IP address and host name as the first entry.
- Note that the Identity Management server host name cannot be part of the **localhost** entry.

```
127.0.0.1 localhost.localdomain localhost
::1  localhost6.localdomain6 localhost6
192.0.2.1 server.example.com server
2001:DB8::1111 server.example.com server
```

1.4. PORT REQUIREMENTS FOR IDENTITY MANAGEMENT

Identity Management uses a number of ports to communicate with its services. These ports must be open and available for incoming connections to the Identity Management server for

Identity Management to work. They must not be currently used by another service or blocked by a firewall.

Table 1.1. Identity Management ports

Service	Ports	Protocol
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP and UDP
DNS	53	TCP and UDP (optional)
NTP	123	UDP (optional)

In addition, ports 8080, 8443, and 749 must be free as they are used internally. Do not open these ports and instead leave them blocked by a firewall.

Table 1.2. firewalld services

Service name	For details, see:
freeipa-ldap	**/usr/lib/firewalld/services/freeipa-ldap.xml**
freeipa-ldaps	**/usr/lib/firewalld/services/freeipa-ldaps.xml**
dns	**/usr/lib/firewalld/services/dns.xml**

Opening the required ports

1. Make sure the **firewalld** service is running.

   - To find out if **firewalld** is currently running:

     ```
     # systemctl status firewalld.service
     ```

   - To start **firewalld** and configure it to start automatically when the system boots:

     ```
     # systemctl start firewalld.service
     # systemctl enable firewalld.service
     ```

2. Open the required ports using the **firewall-cmd** utility. Choose one of the following options:

   a. Add the individual ports to the firewall by using the **firewall-cmd --add-port** command. For example, to open the ports in the default zone:

     ```
     # firewall-cmd --permanent --add-port=
     {80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp,123/udp}
     ```

b. Add the **firewalld** services to the firewall by using the **firewall-cmd --add-service** command. For example, to open the ports in the default zone:

```
# firewall-cmd --permanent --add-service={freeipa-ldap,freeipa-ldaps,dns}
```

For details on using **firewall-cmd** to open ports on a system, see the **firewall-cmd**(1) man page.

3. Reload the **firewall-cmd** configuration to ensure that the change takes place immediately:

```
# firewall-cmd --reload
```

Note that reloading **firewalld** on a system in production can cause DNS connection time outs. If required, to avoid the risk of time outs and to make the changes persistent on the running system, use the **--runtime-to-permanent** option of the **firewall-cmd** command, for example:

```
# firewall-cmd --runtime-to-permanent --add-port=
{80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp,123/udp}
```

4. **Optional.** To verify that the ports are available now, use the **nc**, **telnet**, or **nmap** utilities to connect to a port or run a port scan.

NOTE

Note that you also have to open network-based firewalls for both incoming and outgoing traffic.

1.5. INSTALLING PACKAGES REQUIRED FOR AN IDENTITY MANAGEMENT SERVER

In RHEL8, the packages necessary for installing an Identity Management (IdM) server are shipped as a module. The IdM server module stream is called the **DL1** stream, and you need to enable this stream before downloading packages from this stream. The following procedure shows how to download the packages necessary for setting up the Identity Management environment of your choice.

Prerequisites

- You have a newly installed RHEL system. You have not enabled an IdM module stream yet.

Procedure

1. Enable the **idm:DL1** stream:

```
# yum module enable idm:DL1
```

2. Switch to the RPMs delivered through the **idm:DL1** stream:

```
# yum distro-sync
```

3. Choose one of the following options, depending on your IdM requirements:

    - To download the packages necessary for installing an IdM server without an integrated DNS:

```
# yum module install idm:DL1/server
```

- To download the packages necessary for installing an IdM server with an integrated DNS:

```
# yum module install idm:DL1/dns
```

- To download the packages necessary for installing an IdM server that has a trust agreement with Active Directory:

```
# yum module install idm:DL1/adtrust
```

- To download the packages from multiple profiles, for example the **adtrust** and **dns** profiles:

```
# yum module install idm:DL1/{dns,adtrust}
```

- To download the packages necessary for installing an IdM client:

```
# yum module install idm:DL1/client
```

IMPORTANT

When switching to a new module stream once you have already enabled a different stream and downloaded packages from it, you need to first explicitly remove all the relevant installed content and disable the current module stream before enabling the new module stream. Trying to enable a new stream without disabling the current one results in an error. For details on how to proceed, see Switching module streams to install a different version of content.

WARNING

While it is possible to install packages from modules individually, be aware that if you install any package from a module that is not listed as "API" for that module, it is only going to be supported by Red Hat in the context of that module. For example, if you install **bind-dyndb-ldap** directly from the repository to use with your custom 389 Directory Server setup, any problems that you have will be ignored unless they occur for Identity Management, too.

CHAPTER 2. INSTALLING AN IDENTITY MANAGEMENT SERVER: WITH INTEGRATED DNS, WITH AN INTEGRATED CA

Installing a new Identity Management server with integrated DNS has the following advantages:

- You can automate much of the maintenance and DNS record management using native Identity Management tools. For example, DNS SRV records are automatically created during the setup, and later on are automatically updated.
- You can have a stable connection with the rest of the Internet by setting up global forwarders during the installation of the Identity Management server. Global forwarders are also useful for trusts with Active Directory.
- You can set up a DNS reverse zone to prevent emails from your domain to be considered spam by email servers outside of the Identity Management domain.

Installing Identity Management with integrated DNS has certain limitations:

- Identity Management DNS is not meant to be used as a general-purpose DNS server. Some of the advanced DNS functions are not supported.

This chapter describes how you can install a new Identity Management server with an integrated CA as the root CA.

> **NOTE**
>
> The default configuration for the **ipa-server-install** command is an integrated CA as the root CA. If no CA option, for example **--external-ca** or **--ca-less** is specified, the Identity Management server is installed with an integrated CA.

2.1. INTERACTIVE INSTALLATION

During the interactive installation using the **ipa-server-install** utility, you are asked to supply basic configuration of the system, for example the realm, the administrator’s password and the Directory Manager’s password.

The **ipa-server-install** installation script creates a log file at **/var/log/ipaserver-install.log**. If the installation fails, the log can help you identify the problem.

Procedure

1. Run the **ipa-server-install** utility.

   ```
   # ipa-server-install
   ```

2. The script prompts to configure an integrated DNS service. Enter **yes**.

   ```
   Do you want to configure integrated DNS (BIND)? [no]: yes
   ```

3. The script prompts for several required settings and offers recommended default values in brackets.

   - To accept a default value, press **Enter**.

- To provide a custom value, enter the required value.

  ```
  Server host name [server.example.com]:
  Please confirm the domain name [example.com]:
  Please provide a realm name [EXAMPLE.COM]:
  ```

  > **WARNING**
  >
  > Plan these names carefully. You will not be able to change them after the installation is complete.

4. Enter the passwords for the Directory Server superuser (**cn=Directory Manager**) and for the Identity Management administration system user account (**admin**).

   ```
   Directory Manager password:
   IPA admin password:
   ```

5. The script prompts for DNS forwarders.

   ```
   Do you want to configure DNS forwarders? [yes]:
   ```

   - To configure DNS forwarders, enter **yes**, and then follow the instructions on the command line. The installation process will add the forwarder IP addresses to the **/etc/named.conf** file on the installed Identity Management server.
     - For the forwarding policy default settings, see the **--forward-policy** description in the **ipa-dns-install**(1) man page.
   - If you do not want to use DNS forwarding, enter **no**.
     With no DNS forwarders, your environment will be isolated, and names from other DNS domains in your infrastructure will not be resolved.

6. The script prompts to check if any DNS reverse (PTR) records for the IP addresses associated with the server need to be configured.

   ```
   Do you want to search for missing reverse zones? [yes]:
   ```

   If you run the search and missing reverse zones are discovered, the script asks you whether to create the reverse zones along with the PTR records.

   ```
   Do you want to create reverse zone for IP 192.0.2.1 [yes]:
   Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
   Using reverse zone(s) 2.0.192.in-addr.arpa.
   ```

   > **NOTE**
   >
   > Using Identity Management to manage reverse zones is optional. You can use an external DNS service for this purpose instead.

7. Enter **yes** to confirm the server configuration.

   ```
   Continue to configure the system with these values? [no]: yes
   ```

8. The installation script now configures the server. Wait for the operation to complete.

9. After the installation script completes, add DNS delegation from the parent domain to the Identity Management DNS domain. For example, if the Identity Management DNS domain is **ipa.example.com**, add a name server (NS) record to the **example.com** parent domain.

   IMPORTANT

   Repeat this step each time after an Identity Management DNS server is installed.

2.2. NON-INTERACTIVE INSTALLATION

NOTE

The **ipa-server-install** installation script creates a log file at **/var/log/ipaserver-install.log**. If the installation fails, the log can help you identify the problem.

Procedure

1. Run the **ipa-server-install** utility with the options to supply all the required information. The minimum required options for non-interactive installation are:

   - **--realm** to provide the Kerberos realm name
   - **--ds-password** to provide the password for the Directory Manager (DM), the Directory Server super user
   - **--admin-password** to provide the password for **admin**, the Identity Management administrator
   - **--unattended** to let the installation process select default options for the host name and domain name

   To install a server with integrated DNS, add also these options:

   - **--setup-dns** to configure integrated DNS
   - **--forwarder** or **--no-forwarders**, depending on whether you want to configure DNS forwarders or not
   - **--auto-reverse** or **--no-reverse**, depending on whether you want to configure automatic detection of the reverse DNS zones that must be created in the Identity Management DNS or no reverse zone auto-detection

   For example:

   ```
   # ipa-server-install --realm EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended --setup-dns --forwarder 192.0.2.1 --no-reverse
   ```

2. After the installation script completes, add DNS delegation from the parent domain to the Identity Management DNS domain. For example, if the Identity Management DNS domain is **ipa.example.com**, add a name server (NS) record to the **example.com** parent domain.

   IMPORTANT

   Repeat this step each time after an Identity Management DNS server is installed.

Additional resources

- For a complete list of options accepted by **ipa-server-install**, run the **ipa-server-install --help** command.

CHAPTER 3. INSTALLING AN IDENTITY MANAGEMENT SERVER: WITH INTEGRATED DNS, WITH AN EXTERNAL CA

Installing a new Identity Management server with integrated DNS has the following advantages:

- You can automate much of the maintenance and DNS record management using native Identity Management tools. For example, DNS SRV records are automatically created during the setup, and later on are automatically updated.

- You can have a stable connection with the rest of the Internet by setting up global forwarders during the installation of the Identity Management server. Global forwarders are also useful for trusts with Active Directory.

- You can set up a DNS reverse zone to prevent emails from your domain to be considered spam by email servers outside of the Identity Management domain.

Installing Identity Management with integrated DNS has certain limitations:

- Identity Management DNS is not meant to be used as a general-purpose DNS server. Some of the advanced DNS functions are not supported.

This chapter describes how you can install a new Identity Management server with an external CA as the root CA.

3.1. INTERACTIVE INSTALLATION

During the interactive installation using the **ipa-server-install** utility, you are asked to supply basic configuration of the system, for example the realm, the administrator's password and the Directory Manager's password.

The **ipa-server-install** installation script creates a log file at **/var/log/ipaserver-install.log**. If the installation fails, the log can help you identify the problem.

This procedure describes how to install a server:

- with integrated DNS

- with an external certificate authority (CA) as the root CA

Prerequisites

- Decide on the type of the external CA you use (the **--external-ca-type** option). See the **ipa-server-install**(1) man page for details.

- Alternatively, decide on the **--external-ca-profile** option allowing an alternative Active Directory Certificate Services (AD CS) template to be specified. For example, to specify an AD CS installation-specific object identifier:

```
[root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-profile=1.3.6.1.4.1.311.21.8.8950086.10656446.2706058.12775672.480128.147.7130143.4405632:1
```

Procedure

1. Run the **ipa-server-install** utility with the **--external-ca** option.

   –

```
   # ipa-server-install --external-ca
   ```

   If you are using the Microsoft Certificate Services CA, use also the **--external-ca-type** option. For details, see the **ipa-server-install** (1) man page.

2. The script prompts to configure an integrated DNS service. Enter **yes** or **no**. In this procedure, we are installing a server with integrated DNS.

   ```
   Do you want to configure integrated DNS (BIND)? [no]: yes
   ```

   NOTE

   If you want to install a server without integrated DNS, the installation script will not prompt you for DNS configuration as described in the steps below. See Chapter 5, *Installing an Identity Management server: Without integrated DNS, with an integrated CA* for details on the steps for installing a server without DNS.

3. The script prompts for several required settings and offers recommended default values in brackets.

   - To accept a default value, press **Enter**.
   - To provide a custom value, enter the required value.

     ```
     Server host name [server.example.com]:
     Please confirm the domain name [example.com]:
     Please provide a realm name [EXAMPLE.COM]:
     ```

     WARNING

     Plan these names carefully. You will not be able to change them after the installation is complete.

4. Enter the passwords for the Directory Server superuser (**cn=Directory Manager**) and for the Identity Management administration system user account (**admin**).

   ```
   Directory Manager password:
   IPA admin password:
   ```

5. The script prompts for DNS forwarders.

   ```
   Do you want to configure DNS forwarders? [yes]:
   ```

   - To configure DNS forwarders, enter **yes**, and then follow the instructions on the command line. The installation process will add the forwarder IP addresses to the **/etc/named.conf** file on the installed Identity Management server.
     - For the forwarding policy default settings, see the **--forward-policy** description in the **ipa-dns-install**(1) man page.

ipa-dns-install(1) man page.

- If you do not want to use DNS forwarding, enter **no**.
  With no DNS forwarders, your environment will be isolated, and names from other DNS domains in your infrastructure will not be resolved.

6. The script prompts to check if any DNS reverse (PTR) records for the IP addresses associated with the server need to be configured.

   ```
   Do you want to search for missing reverse zones? [yes]:
   ```

   If you run the search and missing reverse zones are discovered, the script asks you whether to create the reverse zones along with the PTR records.

   ```
   Do you want to create reverse zone for IP 192.0.2.1 [yes]:
   Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
   Using reverse zone(s) 2.0.192.in-addr.arpa.
   ```

   NOTE

   Using Identity Management to manage reverse zones is optional. You can use an external DNS service for this purpose instead.

7. Enter **yes** to confirm the server configuration.

   ```
   Continue to configure the system with these values? [no]: yes
   ```

8. During the configuration of the Certificate System instance, the utility prints the location of the certificate signing request (CSR): **/root/ipa.csr**:

   ```
   ...

   Configuring certificate server (pki-tomcatd): Estimated time 3 minutes 30 seconds
     [1/8]: creating certificate server user
     [2/8]: configuring certificate server instance
   The next step is to get /root/ipa.csr signed by your CA and re-run /sbin/ipa-server-install as:
   /sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-file=/path/to/external_ca_certificate
   ```

   When this happens:

   a. Submit the CSR located in **/root/ipa.csr** to the external CA. The process differs depending on the service to be used as the external CA.

   b. Retrieve the issued certificate and the CA certificate chain for the issuing CA in a base 64-encoded blob (either a PEM file or a Base_64 certificate from a Windows CA). Again, the process differs for every certificate service. Usually, a download link on a web page or in the notification email allows the administrator to download all the required certificates.

      IMPORTANT

      Be sure to get the full certificate chain for the CA, not just the CA certificate.

c. Run **ipa-server-install** again, this time specifying the locations and names of the newly-issued CA certificate and the CA chain files. For example:

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-
file=/tmp/cacert.pem
```

9. The installation script now configures the server. Wait for the operation to complete.

> **NOTE**
>
> The **ipa-server-install --external-ca** command can sometimes fail with the following error:
>
> ```
> ipa         : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s
> CA -f /tmp/configuration_file' returned non-zero exit status 1
> Configuration of CA failed
> ```
>
> This failure occurs when the ***_proxy** environmental variables are set. For a solution of the problem, see Section 3.2, "Troubleshooting: External CA installation fails".

3.2. TROUBLESHOOTING: EXTERNAL CA INSTALLATION FAILS

The **ipa-server-install --external-ca** command fails with the following error:

```
ipa         : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f
/tmp/configuration_file' returned non-zero exit status 1
Configuration of CA failed
```

The **env|grep proxy** command displays variables such as the following:

```
# env|grep proxy
http_proxy=http://example.com:8080
ftp_proxy=http://example.com:8080
https_proxy=http://example.com:8080
```

What this means:
The ***_proxy** environmental variables are preventing the server from being installed.

To fix the problem:

1. Use the following shell script to unset the ***_proxy** environmental variables:

```
# for i in ftp http https; do unset ${i}_proxy; done
```

2. Run the **pkidestroy** utility to remove the unsuccessful CA subsystem installation:

```
# pkidestroy -s CA -i pki-tomcat; rm -rf /var/log/pki/pki-tomcat /etc/sysconfig/pki-
tomcat /etc/sysconfig/pki/tomcat/pki-tomcat /var/lib/pki/pki-tomcat /etc/pki/pki-tomcat
/root/ipa.csr
```

3. Remove the failed Identity Management server installation:

```
# ipa-server-install --uninstall
```

4. Retry running **ipa-server-install --external-ca**.

CHAPTER 4. INSTALLING AN IDENTITY MANAGEMENT SERVER: WITH INTEGRATED DNS, WITHOUT A CA

Installing a new Identity Management server with integrated DNS has the following advantages:

- You can automate much of the maintenance and DNS record management using native Identity Management tools. For example, DNS SRV records are automatically created during the setup, and later on are automatically updated.
- You can have a stable connection with the rest of the Internet by setting up global forwarders during the installation of the Identity Management server. Global forwarders are also useful for trusts with Active Directory.
- You can set up a DNS reverse zone to prevent emails from your domain to be considered spam by email servers outside of the Identity Management domain.

Installing Identity Management with integrated DNS has certain limitations:

- Identity Management DNS is not meant to be used as a general-purpose DNS server. Some of the advanced DNS functions are not supported.

This chapter describes how you can install a new Identity Management server without a certificate authority (CA).

4.1. CERTIFICATES REQUIRED TO INSTALL AN IDENTITY MANAGEMENT SERVER WITHOUT A CA

This section lists:

- the certificates required to install an Identity Management server without a certificate authority (CA)
- the command-line options used to provide these certificates to the **ipa-server-install** utility

IMPORTANT

You cannot install a server or replica using self-signed third-party server certificates because the imported certificate files must contain the full CA certificate chain of the CA that issued the LDAP and Apache server certificates.

The LDAP server certificate and private key

- **--dirsrv-cert-file** for the certificate and private key files for the LDAP server certificate
- **--dirsrv-pin** for the password to access the private key in the files specified in **--dirsrv-cert-file**

The Apache server certificate and private key

- **--http-cert-file** for the certificate and private key files for the Apache server certificate
- **--http-pin** for the password to access the private key in the files specified in **--http-cert-file**

The full CA certificate chain of the CA that issued the LDAP and Apache server certificates

- **--dirsrv-cert-file** and **--http-cert-file** for the certificate files with the full CA certificate chain or a part of it

The files provided using **--dirsrv-cert-file** and **--http-cert-file** must contain exactly one server certificate and exactly one private key. The contents of the files provided using **--dirsrv-cert-file** and **--http-cert-file** are often identical.

The certificate files to complete the full CA certificate chain (not needed in some environments)

- **--ca-cert-file** for the file or files containing the CA certificate of the CA that issued the LDAP, Apache Server, and Kerberos KDC certificates. Use this option if the CA certificate is not present in the certificate files provided by the other options.

The files provided using **--dirsrv-cert-file** and **--http-cert-file** combined with the file provided using **--ca-cert-file** must contain the full CA certificate chain of the CA that issued the LDAP and Apache server certificates.

The Kerberos key distribution center (KDC) PKINIT certificate and private key (optional)

- **--pkinit-cert-file** for the Kerberos KDC SSL certificate and private key
- **--pkinit-pin** for the password to access the Kerberos KDC private key in the files specified in **--pkinit-cert-file**
- **--no-pkinit** for disabling pkinit setup steps

If you do not provide the PKINIT certificate, **ipa-server-install** configures the IdM server with a local KDC with a self-signed certificate.

Additional resources

- For details on what the certificate file formats these options accept, see the **ipa-server-install**(1) man page.

4.2. INTERACTIVE INSTALLATION

During the interactive installation using the **ipa-server-install** utility, you are asked to supply basic configuration of the system, for example the realm, the administrator's password and the Directory Manager's password.

The **ipa-server-install** installation script creates a log file at **/var/log/ipaserver-install.log**. If the installation fails, the log can help you identify the problem.

Procedure

1. Run the **ipa-server-install** utility and provide all the required certificates. For example:

```
[root@server ~]# ipa-server-install \
    --http-cert-file /tmp/server.crt \
    --http-cert-file /tmp/server.key \
    --http-pin secret \
    --dirsrv-cert-file /tmp/server.crt \
--dirsrv-cert-file /tmp/server.key \
--dirsrv-pin secret \
--ca-cert-file ca.crt
```

See Section 4.1, “Certificates required to install an Identity Management server without a CA” for details on the provided certificates.

2. The script prompts to configure an integrated DNS service. Enter **yes** or **no**. In this procedure, we are installing a server with integrated DNS.

   ```
   Do you want to configure integrated DNS (BIND)? [no]: yes
   ```

   > **NOTE**
   >
   > If you want to install a server without integrated DNS, the installation script will not prompt you for DNS configuration as described in the steps below. See Chapter 5, *Installing an Identity Management server: Without integrated DNS, with an integrated CA* for details on the steps for installing a server without DNS.

3. The script prompts for several required settings and offers recommended default values in brackets.
   - To accept a default value, press **Enter**.
   - To provide a custom value, enter the required value.

     ```
     Server host name [server.example.com]:
     Please confirm the domain name [example.com]:
     Please provide a realm name [EXAMPLE.COM]:
     ```

     > **WARNING**
     >
     > Plan these names carefully. You will not be able to change them after the installation is complete.

4. Enter the passwords for the Directory Server superuser (**cn=Directory Manager**) and for the Identity Management administration system user account (**admin**).

   ```
   Directory Manager password:
   IPA admin password:
   ```

5. The script prompts for DNS forwarders.

   ```
   Do you want to configure DNS forwarders? [yes]:
   ```

   - To configure DNS forwarders, enter **yes**, and then follow the instructions on the command line. The installation process will add the forwarder IP addresses to the **/etc/named.conf** file on the installed Identity Management server.

    - For the forwarding policy default settings, see the **--forward-policy** description in the **ipa-dns-install**(1) man page.

  - If you do not want to use DNS forwarding, enter **no**.
    With no DNS forwarders, your environment will be isolated, and names from other DNS domains in your infrastructure will not be resolved.

6. The script prompts to check if any DNS reverse (PTR) records for the IP addresses associated with the server need to be configured.

   ```
   Do you want to search for missing reverse zones? [yes]:
   ```

   If you run the search and missing reverse zones are discovered, the script asks you whether to create the reverse zones along with the PTR records.

   ```
   Do you want to create reverse zone for IP 192.0.2.1 [yes]:
   Please specify the reverse zone name [2.0.192.in-addr.arpa.]:
   Using reverse zone(s) 2.0.192.in-addr.arpa.
   ```

   NOTE

   Using Identity Management to manage reverse zones is optional. You can use an external DNS service for this purpose instead.

7. Enter **yes** to confirm the server configuration.

   ```
   Continue to configure the system with these values? [no]: yes
   ```

8. The installation script now configures the server. Wait for the operation to complete.

9. After the installation script completes, add DNS delegation from the parent domain to the Identity Management DNS domain. For example, if the Identity Management DNS domain is **ipa.example.com**, add a name server (NS) record to the **example.com** parent domain.

   IMPORTANT

   Repeat this step each time after an Identity Management DNS server is installed.

CHAPTER 5. INSTALLING AN IDENTITY MANAGEMENT SERVER: WITHOUT INTEGRATED DNS, WITH AN INTEGRATED CA

This chapter describes how you can install a new Identity Management server without integrated DNS.

5.1. INTERACTIVE INSTALLATION

During the interactive installation using the **ipa-server-install** utility, you are asked to supply basic configuration of the system, for example the realm, the administrator's password and the Directory Manager's password.

The **ipa-server-install** installation script creates a log file at **/var/log/ipaserver-install.log**. If the installation fails, the log can help you identify the problem.

This procedure installs a server:

- Without integrated DNS
- With integrated Identity Management certificate authority (CA) as the root CA, which is the default CA configuration

Procedure

1. Run the **ipa-server-install** utility.

   ```
   # ipa-server-install
   ```

2. The script prompts to configure an integrated DNS service. Press **Enter** to select the default **no** option.

   ```
   Do you want to configure integrated DNS (BIND)? [no]:
   ```

3. The script prompts for several required settings and offers recommended default values in brackets.

   - To accept a default value, press **Enter**.
   - To provide a custom value, enter the required value.

     ```
     Server host name [server.example.com]:
     Please confirm the domain name [example.com]:
     Please provide a realm name [EXAMPLE.COM]:
     ```

   WARNING

   Plan these names carefully. You will not be able to change them after the installation is complete.

4. Enter the passwords for the Directory Server superuser (**cn=Directory Manager**) and for the Identity Management administration system user account (**admin**).

   ```
   Directory Manager password:
   IPA admin password:
   ```

5. Enter **yes** to confirm the server configuration.

   ```
   Continue to configure the system with these values? [no]: yes
   ```

6. The installation script now configures the server. Wait for the operation to complete.

5.2. NON-INTERACTIVE INSTALLATION

This procedure installs a server:

- Without integrated DNS
- With integrated Identity Management certificate authority (CA) as the root CA, which is the default CA configuration

> **NOTE**
>
> The **ipa-server-install** installation script creates a log file at **/var/log/ipaserver-install.log**. If the installation fails, the log can help you identify the problem.

Procedure

1. Run the **ipa-server-install** utility with the options to supply all the required information. The minimum required options for non-interactive installation are:

   - **--realm** to provide the Kerberos realm name
   - **--ds-password** to provide the password for the Directory Manager (DM), the Directory Server super user
   - **--admin-password** to provide the password for **admin**, the Identity Management administrator
   - **--unattended** to let the installation process select default options for the host name and domain name

   For example:

   ```
   # ipa-server-install --realm EXAMPLE.COM --ds-password DM_password --admin-password admin_password --unattended
   ```

Additional resources

- For a complete list of options accepted by **ipa-server-install**, run the **ipa-server-install --help** command.

CHAPTER 6. UNINSTALLING AN IDENTITY MANAGEMENT SERVER

As an administrator, you can remove an Identity Management server from the topology.

This procedure describes how you can uninstall an example server named **server.idm.example.com**.

Prerequisites

- Before uninstalling a server that serves as a certificate authority (CA), key recovery authority (KRA), or DNS server, make sure these services are running on another server in the domain.

> **WARNING**
>
> Removing the last server that serves as a CA, KRA, or DNS server seriously disrupts the Identity Management functionality.

Procedure

1. On all the servers in the topology that have a replication agreement with **server.idm.example.com**, use the **ipa server-del** command to delete the replica from the topology:

   ```
   [root@another_server ~]# ipa server-del server.example.com
   ```

2. On **server.idm.example.com**, use the **ipa-server-install --uninstall** command:

   ```
   [root@server ~]# ipa-server-install --uninstall
   ...
   Are you sure you want to continue with the uninstall procedure? [no]: yes
   ```

3. Make sure all name server (NS) DNS records pointing to **server.idm.example.com** are deleted from your DNS zones. This applies regardless of whether you use integrated DNS managed by Identity Management or external DNS.

CHAPTER 7. RENAMING AN IDENTITY MANAGEMENT SERVER

You cannot change the host name of an existing Identity Management server. However, you can replace the server with a replica of a different name.

Procedure

1. Install a new replica that will replace the existing server, ensuring the replica has the required host name and IP address. For details, see Chapter 15, *Installing an Identity Management replica* .

   IMPORTANT

   If the server you are uninstalling is a CRL master server, make another server the CRL master server before proceeding. For details how this is done in the context of a migration procedure, see Stopping CRL generation on RHEL 7 and redirecting CRL requests to RHEL 8 and Starting CRL generation on RHEL 8 .

2. Stop the existing Identity Management server instance.

   ```
   [root@old_server ~]# ipactl stop
   ```

3. Uninstall the existing server as described in Chapter 6, *Uninstalling an Identity Management server*.

CHAPTER 8. PREPARING THE SYSTEM FOR IDENTITY MANAGEMENT CLIENT INSTALLATION

This chapter describes the conditions your system must meet to install an Identity Management client.

8.1. DNS REQUIREMENTS FOR IDENTITY MANAGEMENT CLIENTS

Client installer by default tries to search for **_ldap._tcp.DOMAIN** DNS SRV records for all domains that are parent to its hostname. For example, if a client machine has a hostname **client1.idm.example.com**, the installer will try to retrieve an Identity Management server hostname from **_ldap._tcp.idm.example.com**, **_ldap._tcp.example.com** and **_ldap._tcp.com** DNS SRV records, respectively. The discovered domain is then used to configure client components (for example, SSSD and Kerberos 5 configuration) on the machine.

However, the hostnames of Identity Management clients are not required to be part of the primary DNS domain. If the client machine hostname is not in a subdomain of an Identity Management server, pass the IdM domain as the **--domain** option of the **ipa-client-install** command. In that case, after the installation of the client, both SSSD and Kerberos components will have the domain set in their configuration files and will use it to autodiscover Identity Management servers.

Additional resources

- For details on DNS requirements in Identity Management, see Section 1.3, "Host name and DNS requirements for Identity Management".

8.2. PORT REQUIREMENTS FOR IDENTITY MANAGEMENT CLIENTS

Identity Management clients connect to a number of ports on Identity Management servers to communicate with their services.

On Identity Management client, these ports must be open *in the outgoing direction*. If you are using a firewall that does not filter outgoing packets, such as **firewalld**, the ports are already available in the outgoing direction.

Additional resources

- For information about which specific ports are used, see Section 1.4, "Port requirements for Identity Management".

8.3. PACKAGES REQUIRED TO INSTALL AN IDENTITY MANAGEMENT CLIENT

In RHEL8, the packages necessary for installing an Identity Management client are shipped as a module. Two IdM streams provide IdM client packages:

- the **idm:client** stream. For details, see Section 8.3.1, "Installing ipa-client packages from the idm:client stream".
- the **idm:DL1** stream. For details, see Section 8.3.2, "Installing ipa-client packages from the idm:DL1 stream".

8.3.1. Installing ipa-client packages from the idm:client stream

The **idm:client** stream is the default stream of the **idm** module. Use this stream to download the IdM client packages if you do not need to install server components on your machine. Using the **idm:client** stream is especially recommended if you need to consistently use IdM client software that is supported long-term, provided you do not need server components, too.

IMPORTANT

When switching to the **idm:client** stream after you previously enabled the **idm:DL1** stream and downloaded packages from it, you need to first explicitly remove all the relevant installed content and disable the **idm:DL1** stream before enabling the **idm:client** stream. Trying to enable a new stream without disabling the current one results in an error. For details on how to proceed, see Switching module streams to install a different version of content.

Procedure

- To download the packages necessary for installing an IdM client:

  ```
  # yum module install idm
  ```

8.3.2. Installing ipa-client packages from the idm:DL1 stream

The **idm:DL1** stream needs to be enabled before you can download packages from it. Use this stream to download the IdM client packages if you need to install IdM server components on your machine.

IMPORTANT

When switching to the **idm:DL1** stream after you previously enabled the **idm:client** stream and downloaded packages from it, you need to first explicitly remove all the relevant installed content and disable the **idm:client** stream before enabling the **idm:DL1** stream. Trying to enable a new stream without disabling the current one results in an error. For details on how to proceed, see Switching module streams to install a different version of content.

Procedure

1. To switch to the RPMs delivered through the **idm:DL1** stream:

   ```
   # yum module enable idm:DL1
   # yum distro-sync
   ```

2. To download the packages necessary for installing an IdM client:

   ```
   # yum module install idm:DL1/client
   ```

CHAPTER 9. INSTALLING AN IDENTITY MANAGEMENT CLIENT: BASIC SCENARIO

The following sections describe how to configure a system as an Identity Management (IdM) client by using the **ipa-client-install** utility. Configuring a system as an IdM client enrolls it into an IdM domain and enables the system to use IdM services on IdM servers in the domain.

Several options are available for a basic installation:

- For installing a client interactively using privileged user's credentials, see Section 9.3, "Installing a client by using user credentials: Interactive installation".
- For installing a client interactively using a one-time password, see Section 9.4, "Installing a client by using a one-time password: Interactive installation".
- For installing a client noninteractively using either a privileged user's credentials, a one-time password or a keytab from previous enrollment, see Section 9.5, "Installing a client: Non-interactive installation".

9.1. PREREQUISITES

Before you start installing the Identity Management client, make sure that you have met all the prerequisites. See Chapter 8, *Preparing the system for Identity Management client installation* .

9.2. AN OVERVIEW OF THE IDENTITY MANAGEMENT CLIENT INSTALLATION OPTIONS

To install an Identity Management client successfully, you must provide credentials that can be used to enroll the client. The following authentication methods are available:

- The credentials of a user authorized to enroll clients. This is the default option expected by **ipa-client-install**.
  - To provide the credentials of an authorized user directly to **ipa-client-install**, use the **--principal** and **--password** options. See Section 9.3, "Installing a client by using user credentials: Interactive installation" for a detailed procedure.
- A random, one-time password pre-generated on the server:
  - To use this authentication method, add the **--random** option to **ipa-client-install** option. See Section 9.4, "Installing a client by using a one-time password: Interactive installation" for a detailed procedure.
- The client principal from the previous enrollment:
  - This option is available if the system was previously enrolled as an Identity Management client. To use this authentication method, add the **--keytab** option to **ipa-client-install**. See Chapter 11, *Re-enrolling an Identity Management client* for details.

Additional resources

- For details on the options accepted by **ipa-client-install**, see the **ipa-client-install** (1) man page.

9.3. INSTALLING A CLIENT BY USING USER CREDENTIALS: INTERACTIVE INSTALLATION

This procedure describes installing an Identity Management client interactively by using the credentials of an authorized user to enroll the system into the domain.

Prerequisites

- Ensure you have the credentials of a user authorized to enroll clients into the Identity Management domain. This could be, for example, a **hostadmin** user with the Enrollment Administrator role.

Procedure

1. Run the **ipa-client-install** utility on the system that you want to configure as an Identity Management client.

   ```
   # ipa-client-install
   ```

   Add the **--enable-dns-updates** option to update the DNS records with the IP address of the client system if either of the following conditions applies:

   - The Identity Management server the client will be enrolled with was installed with integrated DNS
   - The DNS server on the network accepts DNS entry updates with the GSS-TSIG protocol

   ```
   # ipa-client-install --enable-dns-updates
   ```

   Enabling DNS updates is useful if your client:

   - has a dynamic IP address issued using the Dynamic Host Configuration Protocol
   - has a static IP address but it has just been allocated and the IdM server does not know about it

2. The installation script attempts to obtain all the required settings, such as DNS records, automatically.

   - If the SRV records are set properly in the IdM DNS zone, the script automatically discovers all the other required values and displays them. Enter **yes** to confirm.

     ```
     Client hostname: client.example.com
     Realm: EXAMPLE.COM
     DNS Domain: example.com
     IPA Server: server.example.com
     BaseDN: dc=example,dc=com

     Continue to configure the system with these values? [no]: yes
     ```

   - To install the system with different values, enter **no**. Then run **ipa-client-install** again, and specify the required values by adding command-line options to **ipa-client-install**, for example:

     - **--hostname**

  - **--realm**
  - **--domain**
  - **--server**
- If the script fails to obtain some settings automatically, it prompts you for the values.

> IMPORTANT
>
> The fully qualified domain name must be a valid DNS name:
>
> - Only numbers, alphabetic characters, and hyphens (-) are allowed. For example, underscores are not allowed and can cause DNS failures.
> - The host name must be all lower-case. No capital letters are allowed.

3. The script prompts for a user whose identity will be used to enroll the client. This could be, for example, a **hostadmin** user with the Enrollment Administrator role:

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

4. The installation script now configures the client. Wait for the operation to complete.

```
Client configuration complete.
```

Additional resources

- For details on how the client installation script searches for the DNS records, see the **DNS Autodiscovery** section in the **ipa-client-install**(1) man page.

9.4. INSTALLING A CLIENT BY USING A ONE-TIME PASSWORD: INTERACTIVE INSTALLATION

This procedure describes installing an Identity Management client interactively by using a one-time password to enroll the system into the domain.

Prerequisites

1. On a server in the domain, add the future client system as an Identity Management host. Use the **--random** option with the **ipa host-add** command to generate a one-time random password for the enrollment.

```
$ ipa host-add client.example.com --random
 --------------------------------------------------
 Added host "client.example.com"
 --------------------------------------------------
  Host name: client.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```

NOTE

The generated password will become invalid after you use it to enroll the machine into the Identity Management domain. It will be replaced with a proper host keytab after the enrollment is finished.

Procedure

1. Run the **ipa-client-install** utility on the system that you want to configure as an Identity Management client. Use the **--password** option to provide the one-time random password. Because the password often contains special characters, enclose it in single quotes (').

   ```
   # ipa-client-install
   ```

   Add the **--enable-dns-updates** option to update the DNS records with the IP address of the client system if either of the following conditions applies:

   - The Identity Management server the client will be enrolled with was installed with integrated DNS
   - The DNS server on the network accepts DNS entry updates with the GSS-TSIG protocol

   ```
   # ipa-client-install --password 'W5YpARl=7M.n' --enable-dns-updates
   ```

   Enabling DNS updates is useful if your client:

   - has a dynamic IP address issued using the Dynamic Host Configuration Protocol
   - has a static IP address but it has just been allocated and the IdM server does not know about it

2. The installation script attempts to obtain all the required settings, such as DNS records, automatically.

   - If the SRV records are set properly in the IdM DNS zone, the script automatically discovers all the other required values and displays them. Enter **yes** to confirm.

     ```
     Client hostname: client.example.com
     Realm: EXAMPLE.COM
     DNS Domain: example.com
     IPA Server: server.example.com
     BaseDN: dc=example,dc=com

     Continue to configure the system with these values? [no]: yes
     ```

   - To install the system with different values, enter **no**. Then run **ipa-client-install** again, and specify the required values by adding command-line options to **ipa-client-install**, for example:

     - **--hostname**
     - **--realm**
     - **--domain**

  - **--server**

- If the script fails to obtain some settings automatically, it prompts you for the values.

> IMPORTANT
>
> The fully qualified domain name must be a valid DNS name:
>
> - Only numbers, alphabetic characters, and hyphens (-) are allowed. For example, underscores are not allowed and can cause DNS failures.
> - The host name must be all lower-case. No capital letters are allowed.

3. The installation script now configures the client. Wait for the operation to complete.

```
Client configuration complete.
```

Additional resources

- For details on how the client installation script searches for the DNS records, see the **DNS Autodiscovery** section in the **ipa-client-install**(1) man page.

9.5. INSTALLING A CLIENT: NON-INTERACTIVE INSTALLATION

For a non-interactive installation, you must provide all required information to the **ipa-client-install** utility using command-line options. The following sections describe the minimum required options for a non-interactive installation.

Options for the intended authentication method for client enrollment

The available options are:

- **--principal** and **--password** to specify the credentials of a user authorized to enroll clients
- **--random** to specify a one-time random password generated for the client
- **--keytab** to specify the keytab from a previous enrollment

For details, see Section 9.2, “An overview of the Identity Management client installation options” .

The option for unattended installation

The **--unattended** lets the installation run without requiring user confirmation.
If the SRV records are set properly in the IdM DNS zone, the script automatically discovers all the other required values. If the script cannot discover the values automatically, provide them using command-line options, such as:

- **--hostname** to specify a static host name for the client machine

> IMPORTANT
>
> The fully qualified domain name must be a valid DNS name:
>
> - Only numbers, alphabetic characters, and hyphens (-) are allowed. For example, underscores are not allowed and can cause DNS failures.
> - The host name must be all lower-case. No capital letters are allowed.

- **--server** to specify the host name of the IdM server the client will be enrolled with
- **--domain** to specify the DNS domain name of the IdM server the client will be enrolled with
- **--realm** to specify the Kerberos realm name

An example of a basic **ipa-client-install** command for non-interactive installation:

```
# ipa-client-install --password 'W5YpARl=7M.n' --unattended
```

An example of an **ipa-client-install** command for non-interactive installation with more options specified:

```
# ipa-client-install --password 'W5YpARl=7M.n' --domain example.com --server
server.idm.example.com --unattended
```

Additional resources

- For a complete list of options accepted by **ipa-client-install**, see the **ipa-client-install**(1) man page.

9.6. REMOVING PRE-IDENTITY MANAGEMENT CONFIGURATION AFTER INSTALLING A CLIENT

The **ipa-client-install** script does not remove any previous LDAP and SSSD configuration from the **/etc/openldap/ldap.conf** and **/etc/sssd/sssd.conf** files. If you modified the configuration in these files before installing the client, the script adds the new client values, but comments them out. For example:

```
BASE   dc=example,dc=com
URI    ldap://ldap.example.com

#URI ldaps://server.example.com # modified by IPA
#BASE dc=ipa,dc=example,dc=com # modified by IPA
```

To apply the new Identity Management configuration values:

1. Open **/etc/openldap/ldap.conf** and **/etc/sssd/sssd.conf**.
2. Delete the previous configuration.
3. Uncomment the new Identity Management configuration.

4. Server processes that rely on system-wide LDAP configuration might require a restart to apply the changes. Applications that use **openldap** libraries typically import the configuration when started.

9.7. TESTING AN IDENTITY MANAGEMENT CLIENT

The Command-Line Interface informs you that the **ipa-client-install** was successful, but you can also do your own test.

To test that the Identity Management client can obtain information about users defined on the server, check that you are able to resolve a user defined on the server. For example, to check the default **admin** user:

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

To test that authentication works correctly, **su** to a root user from a non-root user:

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

9.8. CONNECTIONS PERFORMED DURING AN IDENTITY MANAGEMENT CLIENT INSTALLATION

Table 9.1, “Requests performed during an Identity Management client installation” lists the operations performed by **ipa-client-install**, the Identity Management (IdM) client installation tool.

Table 9.1. Requests performed during an Identity Management client installation

Operation	Protocol used	Purpose
DNS resolution against the DNS resolvers configured on the client system	DNS	To discover the IP addresses of IdM masters; (optionally) to add A/AAAA and SSHFP records
Requests to ports 88 (TCP/TCP6 and UDP/UDP6) on an IdM replica	Kerberos	To obtain a Kerberos ticket
JSON-RPC calls to the IdM Apache-based web-service on discovered or configured IdM masters	HTTPS	IdM client enrollment; retrieval of CA certificate chain if LDAP method fails; request for a certificate issuance if required
Requests over TCP/TCP6 to ports 389 on IdM servers, using SASL GSSAPI authentication, plain LDAP, or both	LDAP	IdM client enrollment; identity retrieval by SSSD processes; Kerberos key retrieval for the host principal
Network time protocol (NTP) discovery and resolution (optionally)	NTP	To synchronize time between the client system and an NTP server

9.9. IDENTITY MANAGEMENT CLIENT'S COMMUNICATIONS WITH THE SERVER DURING POST-INSTALLATION DEPLOYMENT

The client side of Identity Management (IdM) framework is implemented with two different applications:

- the **ipa** command-line interface (CLI)
- the browser-based web UI

The browser-based web UI is optional.

Table 9.2, "CLI post-installation operations" shows the operations performed by the CLI during an IdM client post-installation deployment. Table 9.3, "webUI post-installation operations" shows the operations performed by the web UI during an IdM client post-installation deployment.

Two daemons run on the IdM client, the **System Security Services Daemon** (SSSD) and **certmonger**. Section 9.9.1, "SSSD communication patterns" and Section 9.9.2, "Certmonger communication patterns" describe how these daemons communicate with the services available on the IdM and Active Directory servers.

Table 9.2. CLI post-installation operations

Operation	Protocol used	Purpose
DNS resolution against the DNS resolvers configured on the client system	DNS	To discover the IP addresses of IdM masters
Requests to ports 88 (TCP/TCP6 and UDP/UDP6) and 464 (TCP/TCP6 and UDP/UDP6) on an IdM replica	Kerberos	To obtain a Kerberos ticket; change a Kerberos password; authenticate to the IdM Web UI
JSON-RPC calls to the IdM Apache-based web-service on discovered or configured IdM masters	HTTPS	any **ipa** utility usage

Table 9.3. webUI post-installation operations

Operation	Protocol used	Purpose
JSON-RPC calls to the IdM Apache-based web-service on discovered or configured IdM masters	HTTPS	To retrieve the IdM web UI pages

9.9.1. SSSD communication patterns

The System Security Services Daemon (SSSD) is a system service to access remote directories and authentication mechanisms. If configured on an IdM client, it connects to the IdM server, which provides authentication, authorization and other identity and policy information. If the IdM server is in a trust relationships with Active Directory (AD), SSSD also connects to AD to perform authentication for AD users using the Kerberos protocol. By default, SSSD uses Kerberos to authenticate any non-local user. In special situations, SSSD might be configured to use the LDAP protocol instead.

The System Security Services Daemon (SSSD) can be configured to communicate with multiple servers. Table 9.4, “Communication patterns of SSSD on IdM clients when talking to IdM servers” and Table 9.5, “Communication patterns of SSSD on IdM servers acting as trust agents when talking to Active Directory Domain Controllers” show common communication patterns for SSSD in IdM.

Table 9.4. Communication patterns of SSSD on IdM clients when talking to IdM servers

Operation	Protocol used	Purpose
DNS resolution against the DNS resolvers configured on the client system	DNS	To discover the IP addresses of IdM masters
Requests to ports 88 (TCP/TCP6 and UDP/UDP6), 464 (TCP/TCP6 and UDP/UDP6), and 749 (TCP/TCP6) on an Identity Management replica and Active Directory domain controllers	Kerberos	To obtain a Kerberos ticket; to change a Kerberos password
Requests over TCP/TCP6 to ports 389 on IdM servers, using SASL GSSAPI authentication, plain LDAP, or both	LDAP	To obtain information about IdM users and hosts, download HBAC and sudo rules, automount maps, the SELinux user context, public SSH keys, and other information stored in IdM LDAP
(optionally) In case of smart-card authentication, requests to the Online Certificate Status Protocol (OCSP) responder, if it is configured. This often is done via port 80, but it depends on the actual value of the OCSP responder URL in a client certificate.	HTTP	To obtain information about the status of the certificate installed in the smart card

Table 9.5. Communication patterns of SSSD on IdM servers acting as trust agents when talking to Active Directory Domain Controllers

Operation	Protocol used	Purpose
DNS resolution against the DNS resolvers configured on the client system	DNS	To discover the IP addresses of IdM masters
Requests to ports 88 (TCP/TCP6 and UDP/UDP6), 464 (TCP/TCP6 and UDP/UDP6), and 749 (TCP/TCP6) on an Identity Management replica and Active Directory domain controllers	Kerberos	To obtain a Kerberos ticket; change a Kerberos password; administer Kerberos remotely
Requests to ports 389 (TCP/TCP6 and UDP/UDP6) and 3268 (TCP/TCP6)	LDAP	To query Active Directory user and group information; to discover Active Directory domain controllers

Operation	Protocol used	Purpose
(optionally) In case of smart-card authentication, requests to the Online Certificate Status Protocol (OCSP) responder, if it is configured. This often is done via port 80, but it depends on the actual value of the OCSP responder URL in a client certificate.	HTTP	To obtain information about the status of the certificate installed in the smart card

9.9.2. Certmonger communication patterns

Certmonger is a daemon running on IdM masters and IdM clients to allow a timely renewal of SSL certificates associated with the services on the host. The Table 9.6, “Certmonger communication patterns” shows the operations performed by IdM client’s **certmonger** utility on IdM masters.

Table 9.6. Certmonger communication patterns

Operation	Protocol used	Purpose
DNS resolution against the DNS resolvers configured on the client system	DNS	To discover the IP addresses of IdM masters
Requests to ports 88 (TCP/TCP6 and UDP/UDP6) and 464 (TCP/TCP6 and UDP/UDP6) on an IdM replica	Kerberos	To obtain a Kerberos ticket
JSON-RPC calls to the IdM Apache-based web-service on discovered or configured IdM masters	HTTPS	To request new certificates
Access over port 8080 (TCP/TCP6) on the IdM master	HTTP	To obtain an Online Certificate Status Protocol (OCSP) responder and certificate status
(on the first installed server or on the server where certificate tracking has been transferred) Access over port 8443 (TCP/TCP6) on the IdM master	HTTPS	To administer the Certificate Authority on the IdM master (only during IdM master and replica installation)

CHAPTER 10. INSTALLING AN IDENTITY MANAGEMENT CLIENT WITH KICKSTART

A Kickstart enrollment automatically adds a new system to the Identity Management domain at the time Red Hat Enterprise Linux is installed.

10.1. INSTALLING A CLIENT WITH KICKSTART

This procedure describes how to use a Kickstart file to install an Identity Management client.

Prerequisites

- Do not start the **sshd** service prior to the kickstart enrollment. Starting **sshd** before enrolling the client generates the SSH keys automatically, but the Kickstart file in Section 10.2, "Kickstart file for client installation" uses a script for the same purpose, which is the preferred solution.

Procedure

1. Pre-create the host entry on the Identity Management server, and set a temporary password for the entry:

   ```
   $ ipa host-add client.example.com --password=secret
   ```

   The password is used by Kickstart to authenticate during the client installation and expires after the first authentication attempt. After the client is successfully installed, it authenticates using its keytab.

2. Create a Kickstart file with the contents described in Section 10.2, "Kickstart file for client installation". Make sure that network is configured properly in the Kickstart file using the **network** command.

3. Use the Kickstart file to install the Identity Management client.

10.2. KICKSTART FILE FOR CLIENT INSTALLATION

This section describes the contents of a kickstart file that you can use to install an Identity Management client.

The **ipa-client** package in the list of packages to install

Add the **ipa-client** package to the %packages section of the kickstart file. For example:

```
%packages
...
ipa-client
...
```

Post-installation instructions for the Identity Management client

The post-installation instructions must include:

- An instruction for ensuring SSH keys are generated before enrollment

- An instruction to run the **ipa-client-install** utility, while specifying:

   - All the required information to access and configure the Identity Management domain services
   - The password which you set when pre-creating the client host on the Identity Management server. in Section 10.1, “Installing a client with Kickstart” .

For example, the post-installation instructions for a kickstart installation that uses a one-time password and retrieves the required options from the command line rather than via DNS can look like this:

```
%post --log=/root/ks-post.log

# Generate SSH keys; ipa-client-install uploads them to the IdM server by default
/usr/sbin/sshd-keygen

# Run the client install script
/usr/sbin/ipa-client-install --hostname=client.example.com --domain=EXAMPLE.COM --enable-dns-updates --mkhomedir -w secret --realm=EXAMPLE.COM --server=server.example.com
```

Optionally, you can also include other options in the Kickstart file, such as:

- For a non-interactive installation, add the **--unattended** option to **ipa-client-install**.
- To let the client installation script request a certificate for the machine:
   - Add the **--request-cert** option to **ipa-client-install**.
   - Set the system bus address to **/dev/null** for both the **getcert** and **ipa-client-install** utility in the Kickstart **chroot** environment. To do this, add these lines to the post-installation instructions in the Kickstart file before the **ipa-client-install** instruction:

```
# env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null getcert list
# env DBUS_SYSTEM_BUS_ADDRESS=unix:path=/dev/null ipa-client-install
```

10.3. TESTING AN IDENTITY MANAGEMENT CLIENT

The Command-Line Interface informs you that the **ipa-client-install** was successful, but you can also do your own test.

To test that the Identity Management client can obtain information about users defined on the server, check that you are able to resolve a user defined on the server. For example, to check the default **admin** user:

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

To test that authentication works correctly, **su** to a root user from a non-root user:

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

CHAPTER 11. RE-ENROLLING AN IDENTITY MANAGEMENT CLIENT

If a client virtual machine has been destroyed and lost connection with the Identity Management (IdM) servers, for example due to the client's hardware failure, and you still have its keytab, you can re-enroll the client. In this scenario, you want to get the client back in the IdM environment with the same hostname.

During the re-enrollment, the client generates new certificates, but the identity of the client in the LDAP database remains unchanged. After the re-enrollment, the host has its keys and other information in the same LDAP object with the same **fqdn** as previously, before the machine's loss of connection with the IdM servers.

IMPORTANT

You can only re-enroll clients whose domain entry is still active. If you uninstalled a client (using **ipa-client-install --uninstall**) or disabled its host entry (using **ipa host-disable**), you cannot re-enroll it.

You cannot re-enroll a client after you have renamed it. This is because in Identity Management, the key attribute of the client's entry in LDAP is the client's hostname, its **fqdn**. As opposed to re-enrolling a client, during which the client's LDAP object remains unchanged, the outcome of renaming a client is that the client has its keys and other information in a different LDAP object with a new fqdn. Thus the only way to rename a client is to uninstall the host from IdM, change the host's hostname, and install it as an IdM client with a new name. For details on how to rename a client, see Chapter 13, *Renaming Identity Management client systems*.

11.1. WHAT HAPPENS DURING CLIENT RE-ENROLLMENT

During re-enrollment, Identity Management:

- Revokes the original host certificate
- Generates a new host certificate
- Creates new SSH keys
- Generates a new keytab

11.2. RE-ENROLLING A CLIENT BY USING USER CREDENTIALS: INTERACTIVE RE-ENROLLMENT

This procedure describes re-enrolling an Identity Management client interactively by using the credentials of an authorized user.

1. Re-create the client machine with the same host name.
2. Run the **ipa-client-install --force-join** command on the client machine:

   ```
   # ipa-client-install --force-join
   ```

3. The script prompts for a user whose identity will be used to re-enroll the client. This could be, for example, a **hostadmin** user with the Enrollment Administrator role:

```
User authorized to enroll computers: hostadmin
Password for hostadmin@EXAMPLE.COM:
```

Additional resources

- For a more detailed procedure on enrolling clients by using an authorized user's credentials, see Section 9.3, "Installing a client by using user credentials: Interactive installation" .

11.3. RE-ENROLLING A CLIENT BY USING THE CLIENT KEYTAB: NON-INTERACTIVE RE-ENROLLMENT

Prerequisites

- Back up the original client keytab file, for example in the /**tmp** or /**root** directory.

Procedure

This procedure describes re-enrolling an Identity Management client non-interactively by using the keytab of the client system. For example, re-enrollment using the client keytab is appropriate for an automated installation.

1. Re-create the client machine with the same host name.

2. Copy the keytab file from the backup location to the /**etc**/ directory on the re-created client machine.

3. Use the **ipa-client-install** utility to re-enroll the client, and specify the keytab location with the **--keytab** option:

   ```
   # ipa-client-install --keytab /etc/krb5.keytab
   ```

   NOTE

   The keytab specified in the **--keytab** option is only used when authenticating to initiate the enrollment. During the re-enrollment, IdM generates a new keytab for the client.

11.4. TESTING AN IDENTITY MANAGEMENT CLIENT

The Command-Line Interface informs you that the **ipa-client-install** was successful, but you can also do your own test.

To test that the Identity Management client can obtain information about users defined on the server, check that you are able to resolve a user defined on the server. For example, to check the default **admin** user:

```
[user@client ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

To test that authentication works correctly, **su** to a root user from a non-root user:

```
[user@client ~]$ su -
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[root@client ~]#
```

CHAPTER 12. UNINSTALLING AN IDENTITY MANAGEMENT CLIENT

As an administrator, you can remove an Identity Management client from the environment.

12.1. UNINSTALLING AN IDENTITY MANAGEMENT CLIENT

Uninstalling a client removes the client from the Identity Management domain, along with all of the specific Identity Management configuration of system services, such as System Security Services Daemon (SSSD). This restores the previous configuration of the client system.

Procedure

1. Run the **ipa-client-install --uninstall** command:

   ```
   # ipa-client-install --uninstall
   ```

2. Remove the DNS entries for the client host manually from the server:

   ```
   # ipa dnsrecord-del
   Record name: old-client-name
   Zone name: idm.example.com
   No option to delete specific record provided.
   Delete all? Yes/No (default No): yes
   ------------------------
   Deleted record "old-client-name"
   ```

CHAPTER 13. RENAMING IDENTITY MANAGEMENT CLIENT SYSTEMS

The following sections describe how to change the host name of an Identity Management client system.

> **WARNING**
>
> Renaming a client is a manual procedure. Do not perform it unless changing the host name is absolutely required.

Renaming an Identity Management client involves:

1. Preparing the host. For details, see Section 13.1, “Prerequisites”
2. Uninstalling the IdM client from the host. For details, see Section 13.2, “Uninstalling an Identity Management client”
3. Renaming the host. For details, see Section 13.3, “Renaming the host system”
4. Installing the IdM client on the host with the new name. For details, see Section 13.4, “Re-installing an Identity Management client”
5. Configuring the host after the IdM client installation. For details, see Section 13.5, “Re-adding services, re-generating certificates, and re-adding host groups”

13.1. PREREQUISITES

Before uninstalling the current client, make note of certain settings for the client. You will apply this configuration after re-enrolling the machine with a new host name.

- Identify which services are running on the machine:
  - Use the **ipa service-find** command, and identify services with certificates in the output:

    ```
    $ ipa service-find old-client-name.example.com
    ```

  - In addition, each host has a default *host service* which does not appear in the **ipa service-find** output. The service principal for the host service, also called a *host principal*, is **host/*old-client-name.example.com***.
- For all service principals displayed by **ipa service-find *old-client-name.example.com***, determine the location of the corresponding keytabs on the ***old-client-name.example.com*** system:

  ```
  # find / -name "*.keytab"
  ```

  Each service on the client system has a Kerberos principal in the form *service_name/host_name@REALM*, such as **ldap/*old-client-name.example.com@EXAMPLE.COM***.

- Identify all host groups to which the machine belongs.

  ```
  # ipa hostgroup-find old-client-name.example.com
  ```

13.2. UNINSTALLING AN IDENTITY MANAGEMENT CLIENT

Uninstalling a client removes the client from the Identity Management domain, along with all of the specific Identity Management configuration of system services, such as System Security Services Daemon (SSSD). This restores the previous configuration of the client system.

Procedure

1. Run the **ipa-client-install --uninstall** command:

   ```
   # ipa-client-install --uninstall
   ```

2. Remove the DNS entries for the client host manually from the server:

   ```
   # ipa dnsrecord-del
   Record name: old-client-name
   Zone name: idm.example.com
   No option to delete specific record provided.
   Delete all? Yes/No (default No): yes
   ------------------------
   Deleted record "old-client-name"
   ```

1. For each identified keytab other than **/etc/krb5.keytab**, remove the old principals:

   ```
   [root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
   ```

   See TBD <removing-keytabs>>.

2. On an IdM server, remove the host entry. This removes all services and revokes all certificates issued for that host:

   ```
   [root@server ~]# ipa host-del client.example.com
   ```

13.3. RENAMING THE HOST SYSTEM

Rename the machine as required. For example:

```
# hostnamectl set-hostname new-client-name.example.com
```

You can now re-install the Identity Management client to the Identity Management domain with the new host name.

13.4. RE-INSTALLING AN IDENTITY MANAGEMENT CLIENT

Install an client on your renamed host following the procedure described in Chapter 9, *Installing an Identity Management client: Basic scenario*.

13.5. RE-ADDING SERVICES, RE-GENERATING CERTIFICATES, AND RE-ADDING HOST GROUPS

1. On the Identity Management server, add a new keytab for every service identified in Section 13.1, “Prerequisites”.

   ```
   [root@server ~]# ipa service-add service_name/new-client-name
   ```

2. Generate certificates for services that had a certificate assigned in Section 13.1, “Prerequisites”. You can do this:

   - Using the Identity Management administration tools
   - Using the **certmonger** utility

3. Re-add the client to the host groups identified in Section 13.1, “Prerequisites”.

CHAPTER 14. PREPARING THE SYSTEM FOR IDENTITY MANAGEMENT REPLICA INSTALLATION

The following sections list the requirements to install an Identity Management replica. Before the installation, make sure your system meets these requirements.

A system where you want to install a replica must meet the general requirements for servers:

- Chapter 1, *Preparing the system for Identity Management server installation*

For additional requirements specific to replicas, see:

- Section 14.1, “Replica version requirements”

14.1. REPLICA VERSION REQUIREMENTS

Red Hat Enterprise Linux (RHEL) 8 replicas only work with IdM masters running on RHEL 7.4 and later. Before introducing IdM replicas running on RHEL 8 into an existing deployment, upgrade all IdM servers to RHEL 7.4 or later, and change the domain level to 1.

In addition, the replica must be running the same or later version of Identity Management. For example:

- The master server is installed on Red Hat Enterprise Linux 8 and uses the Identity Management 4.x packages.
- You must install the replica also on Red Hat Enterprise Linux 8 or later and use Identity Management version 4.x or later.

This ensures that configuration can be properly copied from the server to the replica.

CHAPTER 15. INSTALLING AN IDENTITY MANAGEMENT REPLICA

The following sections describe how to install an Identity Management replica based on an existing server. The replica installation process copies the configuration of the existing server, and installs the replica based on that configuration.

NOTE

Install one Identity Management replica at a time. The installation of multiple replicas at the same time is not supported.

Before installing a replica, the target system must be authorized for enrollment in the Identity Management domain. See:

- Section 15.1, “Prerequisites for installing a replica on an Identity Management client”
- Section 15.2, “Prerequisites for installing a replica on a system outside the Identity Management domain”

For the replica installation procedures, see:

- Section 15.3, “Installing an Identity Management replica with integrated DNS”
- Section 15.5, “Installing an Identity Management replica without a CA”

After the installation, see:

- Section 15.6, “Testing an Identity Management replica”

15.1. PREREQUISITES FOR INSTALLING A REPLICA ON AN IDENTITY MANAGEMENT CLIENT

When installing a replica on an existing client, choose one of the following authorization methods.

A privileged user’s credentials

Choose this method to authorize the replica installation by providing a privileged user’s credentials:

- Log in as the privileged user before running the **ipa-replica-install** utility. The default privileged user is **admin**:

```
$ kinit admin
```

- Let Identity Management prompt you for the credentials interactively. This is the default behavior.

The **ipaservers** host group

Choose this method to authorize the replica installation by adding the client to the **ipaservers** host group. Membership in **ipaservers** grants the machine elevated privileges analogous to the administrator’s credentials.
To add the client as a member of **ipaservers**:

```
$ kinit admin
```

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.idm.example.com, client.example.com
-------------------------
Number of members added 1
-------------------------
```

15.2. PREREQUISITES FOR INSTALLING A REPLICA ON A SYSTEM OUTSIDE THE IDENTITY MANAGEMENT DOMAIN

When you run the **ipa-replica-install** utility on a system that has not yet been enrolled in the Identity Management domain, **ipa-replica-install** first enrolls the system as a client and then installs the replica components.

When installing a replica on a system outside the Identity Management domain, choose one of the following authorization methods.

A privileged user's credentials

Using this method, the replica installation is authorized by providing a privileged user's credentials. The default privileged user is **admin**.
To use this method, add the principal name and password options (**--principal *admin* --admin-password *password***) to **ipa-replica-install** directly during the installation.

A random password generated on an Identity Management server

Using this method, the replica installation is authorized by providing a random password for one-time enrollment.
To generate the random password for the future replica and add the future replica system to the **ipaservers** host group, use these commands on any server in the domain:

1. Log in as the administrator.

```
$ kinit admin
```

2. Add the new machine as an IdM host. Use the **--random** option with the **ipa host-add** command to generate a random one-time password to be used for the replica installation.

```
$ ipa host-add replica.example2.com --random
--------------------------------------------------
Added host "replica.example2.com"
--------------------------------------------------
  Host name: replica.example2.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.example.com
```

The generated password will become invalid after you use it to enroll the machine into the IdM domain. It will be replaced with a proper host keytab after the enrollment is finished.

3. Add the machine to the **ipaservers** host group.

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example2.com
  Host-group: ipaservers
  Description: IPA server hosts
  Member hosts: server.example.com, replica.example2.com
-------------------------
Number of members added 1
-------------------------
```

   Membership in **ipaservers** grants the machine elevated privileges required to set up the necessary server services.

15.3. INSTALLING AN IDENTITY MANAGEMENT REPLICA WITH INTEGRATED DNS

This procedure describes installing a replica:

- With integrated DNS
- Without a certificate authority (CA) in an Identity Management (IdM) environment in which a CA is already installed. The replica will forward all certificate operations to the Identity Management IdM server with a CA installed.

Procedure

1. Run **ipa-replica-install** with these options:
   - **--setup-dns** to configure the replica as the DNS server
   - **--forwarder** to specify a forwarder, or **--no-forwarder** if you do not want to use any forwarders. To specify multiple forwarders for failover reasons, use **--forwarder** multiple times.

   For example, to set up a replica with an integrated DNS server that forwards all DNS requests not managed by the IdM servers to the DNS server running on IP 192.0.2.1:

```
# ipa-replica-install --setup-dns --forwarder 192.0.2.1
```

NOTE

The **ipa-replica-install** utility accepts a number of other options related to DNS settings, such as **--no-reverse** or **--no-host-dns**. For more information about them, see the **ipa-replica-install**(1) man page.

15.4. INSTALLING AN IDENTITY MANAGEMENT REPLICA WITH A CA

This procedure describes installing a replica:

- Without integrated DNS
- With a certificate authority (CA)

IMPORTANT

When configuring a replica with a CA, the CA configuration of the replica must mirror the CA configuration of the master server.

For example, if the server includes an integrated Identity Management CA as the root CA, the replica must also be installed with an integrated CA as the root CA. No other CA configuration is available in this case.

The inclusion of the **--setup-ca** option in the **ipa-replica-install** command takes care of copying the CA configuration of the initial server.

Procedure

1. Run **ipa-replica-install** with the **--setup-ca** option.

```
# ipa-replica-install --setup-ca
```

15.5. INSTALLING AN IDENTITY MANAGEMENT REPLICA WITHOUT A CA

This procedure describes installing a replica:

- Without integrated DNS
- Without a certificate authority (CA) by providing the required certificates manually. The assumption here is that the master server was also installed without a CA.

IMPORTANT

You cannot install a server or replica using self-signed third-party server certificates because the imported certificate files must contain the full CA certificate chain of the CA that issued the LDAP and Apache server certificates.

Procedure

- Run **ipa-replica-install**, and provide the required certificate files by adding these options:
  - **--dirsrv-cert-file**
  - **--dirsrv-pin**
  - **--http-cert-file**
  - **--http-pin**

  For details about the files that are provided using these options, see Section 4.1, “Certificates required to install an Identity Management server without a CA”.

  For example:

```
# ipa-replica-install \
    --dirsrv-cert-file /tmp/server.crt \
    --dirsrv-cert-file /tmp/server.key \
--dirsrv-pin secret \
--http-cert-file /tmp/server.crt \
--http-cert-file /tmp/server.key \
--http-pin secret
```

NOTE

Do not add the **--ca-cert-file** option. The **ipa-replica-install** utility takes this part of the certificate information automatically from the master server.

15.6. TESTING AN IDENTITY MANAGEMENT REPLICA

After creating a replica, check if the replica replicates data as expected. You can use the following procedure.

Procedure

1. Create a user on the new replica:

```
[admin@new_replica ~]$ ipa user-add test_user
```

2. Make sure the user is visible on another replica:

```
[admin@another_replica ~]$ ipa user-show test_user
```

15.7. CONNECTIONS PERFORMED DURING AN IDENTITY MANAGEMENT REPLICA INSTALLATION

Table 15.1, “Requests performed during an Identity Management replica installation” lists the operations performed by **ipa-replica-install**, the Identity Management (IdM) replica installation tool.

Table 15.1. Requests performed during an Identity Management replica installation

Operation	Protocol used	Purpose
DNS resolution against the DNS resolvers configured on the client system	DNS	To discover the IP addresses of IdM masters
Requests to ports 88 (TCP/TCP6 and UDP/UDP6) on the discovered IdM masters	Kerberos	To obtain a Kerberos ticket
JSON-RPC calls to the IdM Apache-based web-service on the discovered or configured IdM masters	HTTPS	IdM client enrollment; replica keys retrieval and certificate issuance if required
Requests over TCP/TCP6 to port 389 on the IdM server, using SASL GSSAPI authentication, plain LDAP, or both	LDAP	IdM client enrollment; CA certificate chain retrieval; LDAP data replication

Operation	Protocol used	Purpose
Requests over TCP/TCP6 to port 22 on IdM server	SSH	To check if the connection is working
(optionally) Access over port 8443 (TCP/TCP6) on the IdM master	HTTPS	To administer the Certificate Authority on the IdM master (only during IdM master and replica installation)

CHAPTER 16. UNINSTALLING AN IDENTITY MANAGEMENT REPLICA

As an administrator, you can remove an Identity Management server from the topology.

This procedure describes how you can uninstall an example server named **server.idm.example.com**.

Prerequisites

- Before uninstalling a server that serves as a certificate authority (CA), key recovery authority (KRA), or DNS server, make sure these services are running on another server in the domain.

> ⚠ **WARNING**
>
> Removing the last server that serves as a CA, KRA, or DNS server seriously disrupts the Identity Management functionality.

Procedure

1. On all the servers in the topology that have a replication agreement with **server.idm.example.com**, use the **ipa server-del** command to delete the replica from the topology:

```
[root@another_server ~]# ipa server-del server.example.com
```

2. On **server.idm.example.com**, use the **ipa-server-install --uninstall** command:

```
[root@server ~]# ipa-server-install --uninstall
...
Are you sure you want to continue with the uninstall procedure? [no]: yes
```

3. Make sure all name server (NS) DNS records pointing to **server.idm.example.com** are deleted from your DNS zones. This applies regardless of whether you use integrated DNS managed by Identity Management or external DNS.

PART II. MIGRATING IDM FROM RHEL 7 TO RHEL 8 AND KEEPING IT UP-TO-DATE

CHAPTER 17. MIGRATING IDENTITY MANAGEMENT FROM RHEL 7 TO 8

This procedure describes how to migrate all Identity Management data and configuration from a Red Hat Enterprise Linux (RHEL) 7 server to a RHEL 8 server. The migration procedure includes:

1. Installing an Identity Management server on the RHEL 8 system. For details, see Section 17.2, “Installing the RHEL 8 Replica”.
2. Making the RHEL 8 server the CA renewal master. For details, see Section 17.3, “Moving the CA renewal master to RHEL 8”.
3. Stopping the generation of the certificate revocation list (CRL) on the RHEL 7 server and redirecting CRL requests to RHEL 8. For details, see Section 17.4, “Stopping CRL generation on RHEL 7 and redirecting CRL requests to RHEL 8”.
4. Starting the generation of the certificate revocation list (CRL) on the RHEL 8 server. For details, see Section 17.5, “Starting CRL generation on RHEL 8” .
5. Stopping and decommissioning the original RHEL 7 CA master. For details, see Section 17.6, “Stopping and decomissioning the RHEL 7 server”.

In the following procedures:

- **rhel8.example.com** is the RHEL 8 system that will become the new CA master.
- **rhel7.example.com** is the original RHEL 7 CA master.

NOTE

To identify which Red Hat Enterprise Linux 7 server is the master CA server, run this command on any IdM server:

```
[root@rhel7 ~]# ipa config-show | grep "CA renewal master"
IPA CA renewal master: rhel7.example.com
```

17.1. PREREQUISITES FOR MIGRATING IDENTITY MANAGEMENT FROM RHEL 7 TO 8

On **rhel7.example.com**:

1. Upgrade the system to the latest RHEL 7 version.
2. Update the **ipa-*** packages to their latest version:

```
[root@rhel7 ~]# yum update ipa-*
```

> **WARNING**
>
> When upgrading multiple Identity Management servers, wait at least 10 minutes between each upgrade.
>
> When two or more servers are upgraded simultaneously or with only short intervals between the upgrades, there is not enough time to replicate the post-upgrade data changes throughout the topology, which can result in conflicting replication events.

On **rhel8.example.com**:

1. Make sure the **rhel8.example.com** system meets the requirements listed in Chapter 1, *Preparing the system for Identity Management server installation* .
2. Make sure that the replica is part of the domain for which the IdM DNS server is authoritative.
3. Update the **ipa-*** packages to their latest version:

```
[root@rhel8 ~]# yum update ipa-*
```

Related Information

- For details on using the **yum** utility, see the **yum(8)** manual pages.

17.2. INSTALLING THE RHEL 8 REPLICA

1. List which server roles are present in your RHEL 7 environment:

```
[root@rhel7 ~]# ipa server-role-find --status enabled
----------------------
4 server roles matched
----------------------
  Server name: rhel7.example.com
  Role name: CA server
  Role status: enabled

  Server name: replica7.example.com
  Role name: DNS server
  Role status: enabled

  Server name: rhel7.example.com
  Role name: DNS server
  Role status: enabled

  Server name: rhel7.example.com
  Role name: NTP server
  Role status: enabled
[... output truncated ...]
```

2. Install the IdM server on **rhel8.example.com** as a replica of the IdM RHEL 7 server, including all the server roles present on your **rhel7.example.com**. To install all the roles from the example above, use these options with the **ipa-replica-install** command:

    - **--setup-ca** to set up the Certificate System component

    - **--setup-dns** and **--forwarder** to configure an integrated DNS server and set a forwarder to take care of DNS queries that go outside the IdM domain
      To set up an IdM server with the ip address of 192.0.2.1 which uses a forwarder with the ip address of 192.0.2.20:

      ```
      [root@rhel8 ~]# ipa-replica-install --setup-ca --ip-address 192.0.2.1 --setup-dns --
      forwarder 192.0.2.20
      ```

    You do not need to specify the RHEL 7 IdM server because if DNS is working correctly, **rhel8.example.com** will find it using DNS autodiscovery.

3. After the installation completes, verify that the Identity Management services are running on **rhel8.example.com**:

    ```
    [root@rhel8 ~]# ipactl status
    Directory Service: RUNNING
    [... output truncated ...]
    ipa: INFO: The ipactl command was successful
    ```

4. Verify that **rhel7.example.com** and **rhel8.example.com** CAs are both configured as master servers:

    ```
    [root@rhel8 ~]$ kinit admin
    [root@rhel8 ~]$ ipa-csreplica-manage list
    rhel7.example.com: master
    rhel8.example.com: master
    ```

5. Optionally, to display details about the replication agreement between **rhel7.example.com** and **rhel8.example.com**:

    ```
    [root@rhel8 ~]# ipa-csreplica-manage list --verbose rhel8.example.com
    Directory Manager password:

    rhel7.example.com
    last init status: None
    last init ended: 1970-01-01 00:00:00+00:00
    last update status: Error (0) Replica acquired successfully: Incremental update succeeded
    last update ended: 2019-02-13 13:55:13+00:00
    ```

17.3. MOVING THE CA RENEWAL MASTER TO RHEL 8

On **rhel8.example.com**, configure **rhel8.example.com** as the new CA renewal master:

- Configure **rhel8.example.com** to handle CA subsystem certificate renewal:

  ```
  [root@rhel8 ~]# ipa config-mod --ca-renewal-master-server rhel8.example.com
    ...
    IPA masters: rhel7.example.com, rhel8.example.com
  ```

```
IPA CA servers: rhel7.example.com, rhel8.example.com
IPA NTP servers: rhel7.example.com, rhel8.example.com
IPA CA renewal master: rhel8.example.com
```

The output confirms that the update was successful.

17.4. STOPPING CRL GENERATION ON RHEL 7 AND REDIRECTING CRL REQUESTS TO RHEL 8

Stop the generation of the Certificate Revocation List (CRL) on the **rhel7.example.com** CA master and configure Apache on **rhel7.example.com** to redirect CRL requests to the new master, **rhel8.example.com**:

1. Stop the CA service.

   ```
   [root@rhel7 ~]# systemctl stop pki-tomcatd@pki-tomcat.service
   ```

2. Disable CRL generation on **rhel7.example.com**. Edit the **/etc/pki/pki-tomcat/ca/CS.cfg** file, setting the values of the **ca.crl.MasterCRL.enableCRLCache** and **ca.crl.MasterCRL.enableCRLUpdates** parameters to **false**.

   ```
   ca.crl.MasterCRL.enableCRLCache=false
   ca.crl.MasterCRL.enableCRLUpdates=false
   ```

3. Start the CA service.

   ```
   [root@rhel7 ~]# systemctl start pki-tomcatd@pki-tomcat.service
   ```

4. Configure Apache to redirect CRL requests to the new master. Open the **/etc/httpd/conf.d/ipa-pki-proxy.conf** file and uncomment the **RewriteRule** argument, replacing the server host name with the **rhel8.example.com** host name in the server URL:

   ```
   # Only enable this on servers that are not generating a CRL
   RewriteRule ^/ipa/crl/MasterCRL.bin https://rhel8.example.com/ca/ee/ca/getCRL?
   op=getCRL&crlIssuingPoint=MasterCRL [L,R=301,NC]
   ```

5. Restart Apache.

   ```
   [root@rhel7 ~]# systemctl restart httpd.service
   ```

17.5. STARTING CRL GENERATION ON RHEL 8

Configure **rhel8.example.com** to generate certificate revocation lists (CRLs):

1. Stop the CA service:

   ```
   [root@rhel8 ~]# systemctl stop pki-tomcatd@pki-tomcat.service
   ```

2. Enable CRL generation on the server. Edit the **/etc/pki/pki-tomcat/ca/CS.cfg** file, setting the values of the **ca.crl.MasterCRL.enableCRLCache** and **ca.crl.MasterCRL.enableCRLUpdates** parameters to **true**:

```
ca.crl.MasterCRL.enableCRLCache=true
ca.crl.MasterCRL.enableCRLUpdates=true
```

3. Start the CA service:

```
[root@rhel8 ~]# systemctl start pki-tomcatd@pki-tomcat.service
```

4. Configure Apache to disable redirecting CRL requests. Open the **/etc/httpd/conf.d/ipa-pki-proxy.conf** file and comment out the **RewriteRule** argument:

```
# Only enable this on servers that are not generating a CRL
#RewriteRule ^/ipa/crl/MasterCRL.bin https://rhel7.example.com/ca/ee/ca/getCRL?
op=getCRL&crlIssuingPoint=MasterCRL [L,R=301,NC]
```

   Before, all CRL requests were routed to the previous CA master. Now, this server will respond to CRL requests.

5. Restart Apache:

```
[root@rhel8 ~]# systemctl restart httpd.service
```

17.6. STOPPING AND DECOMISSIONING THE RHEL 7 SERVER

1. Make sure that all, even the latest data is correctly migrated from **rhel7.example.com** to **rhel8.example.com**. For example:

   a. Add a new user on **rhel7.example.com**:

   ```
   [root@rhel7 ~]# ipa user-add random_user
   First name: random
   Last name: user
   ```

   b. Check that the user has been replicated to **rhel8.example.com**:

   ```
   [root@rhel8 ~]# ipa user-find random_user
   --------------
   1 user matched
   --------------
     User login: random_user
     First name: random
     Last name: user
   ```

2. Stop all service on **rhel7.example.com** to force domain discovery to the new **rhel8.example.com** server.

```
[root@rhel7 ~]# ipactl stop
Stopping CA Service
Stopping pki-ca:                                   [  OK  ]
Stopping HTTP Service
Stopping httpd:                                    [  OK  ]
Stopping MEMCACHE Service
Stopping ipa_memcached:                                 [  OK  ]
Stopping DNS Service
```

```
Stopping named: .                    [  OK  ]
Stopping KPASSWD Service
Stopping Kerberos 5 Admin Server:          [  OK  ]
Stopping KDC Service
Stopping Kerberos 5 KDC:                [  OK  ]
Stopping Directory Service
Shutting down dirsrv:
  EXAMPLE-COM...                       [  OK  ]
  PKI-IPA...                      [  OK  ]
```

After this, the **ipa** utility will contact the new server through a remote procedure call (RPC).

3. Remove the RHEL 7 server from the topology by executing the removal commands on the RHEL 8 server. For details, see Chapter 6, *Uninstalling an Identity Management server*.

CHAPTER 18. UPDATING AND DOWNGRADING IDENTITY MANAGEMENT

You can use the **yum** utility to update the Identity Management (IdM) packages on the system.

- To update all IdM packages that are relevant for your profile and that have updates available:

  ```
  # yum upgrade ipa-*
  ```

- Alternatively, to install or update packages to match the latest version available for your profile from any enabled repository:

  ```
  # yum distro-sync ipa-*
  ```

After you update the IdM packages on at least one server, all other servers in the topology receive the updated schema, even if you do not update their packages. This ensures that any new entries which use the new schema can be replicated among the other servers.

> **WARNING**
>
> When updating multiple IdM servers, wait at least 10 minutes after updating one server before updating another server. However, the actual time required for a server's successful update depends on the topology deployed, the latency of the connections, and the number of changes generated by the update.
>
> When two or more servers are updated simultaneously or with only short intervals between the upgrades, there is not enough time to replicate the post-upgrade data changes throughout the topology, which can result in conflicting replication events.

Downgrading IdM packages manually is not supported. Use **yum distro-sync** to update and downgrade packages in modules.

> **IMPORTANT**
>
> Do not run the **yum downgrade** command on any of the **ipa-*** packages.

Related Information

- For details on using the **yum** utility, see the **yum(8)** manual pages.