Red Hat Enterprise Linux 8

Identity Management のインストール

Identity Management の使用

Last Updated: 2019-05-07

Red Hat Enterprise Linux 8 Identity Management のインストール

Identity Management の使用

法律上の通知

概要

本書は、Red Hat Enterprise Linux 8 (RHEL) に Identity Management をインストールする方法と、RHEL 7 からアップグレードする方法を説明します。

目次

RED HAT ドキュメントへのフィードバック

ドキュメントの改善に関するご意見やご要望をお聞かせください。

- 特定の文章に簡単なコメントを記入する場合は、ドキュメントが Multi-page HTML 形式になっているのを確認してください。コメントを追加する部分を強調表示し、そのテキストの下に表示される **Add Feedback** ポップアップをクリックし、表示された手順に従ってください。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
    1. Bugzilla の Web サイトにアクセスします。
    2. Component で **Documentation** を選択します。
    3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも記入してください。
    4. **Submit Bug** をクリックします。

パート I. IDENTITY MANAGEMENT のインストール

第1章 IDENTITY MANAGEMENT サーバーをインストールするためのシステムの準備

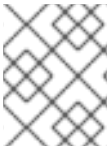
ここでは、Identity Management サーバーのインストール要件を取り上げます。インストールを行う前に、システムがこれらの要件を満たしていることを確認してください。

1.1. ハードウェア推奨事項

ハードウェアでは、RAM の容量を適切に確保することが最も重要になります。システムに十分な RAM があるようにしてください。一般的な RAM の要件は次のとおりです。

- 10,000 ユーザーおよび 100 グループには、最低 3 GB の RAM と 1 GB のスワップスペースを割り当てます。
- 100,000 ユーザーおよび 50,000 グループには、最低 16 GB の RAM と 4 GB のスワップスペースを割り当てます。

大規模なデプロイメントでは、データのほとんどがキャッシュに保存されるため、ディスクスペースを増やすよりも RAM を増やす方が効果的です。



注記

基本的なユーザーエントリーまたは証明書のあるシンプルなホストエントリーのサイズは約 5 ~ 10 KB になります。

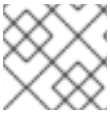
1.2. IDENTITY MANAGEMENT のカスタム設定要件

DNS、Kerberos、Apache、Directory Server などのサービスのカスタム設定をせずに、クリーンシステムに Identity Management をインストールします。

Identity Management サーバーのインストールは、システムファイルを上書きして Identity Management ドメインを設定します。Identity Management は、元のシステムファイルを **/var/lib/ipa/sysrestore/** にバックアップします。ライフサイクルの最後に Identity Management サーバーをアンインストールすると、このファイルが復元します。

1.2.1. Identity Management における IPv6 要件

IdM システムでは、カーネル内で IPv6 プロトコルが有効になっている必要があります。IPv6 が無効になっていると、IdM サービスが使用する CLDAP プラグインが初期化に失敗します。



注記

ネットワーク上で IPv6 を有効にする必要はありません。

1.3. IDENTITY MANAGEMENT のホスト名および DNS の要件

ここでは、サーバーおよびレプリカシステムのホスト名および DNS の要件と、システムが要件を満たしていることを検証する方法も説明します。

ここで取り上げている要件は、統合 DNS の有無に関わらず、すべての Identity Management サーバーに適用されます。

警告

DNS レコードは、稼働中の LDAP ディレクトリー、Kerberos、Active Directory 統合など、ほぼすべての Identity Management ドメイン機能で必須となります。以下の点を確認し、十分注意してください。

- テスト済みの機能する DNS サービスが利用可能であること。
- サービスが適切に設定されていること。

この要件は、統合 DNS の **有無に関係なく**、Identity Management サーバーに適用されます。

サーバーのホスト名の検証

ホスト名は、**server.example.com**. のように完全修飾ドメイン名である必要があります。
完全修飾ドメイン名は、以下の条件を満たす必要があります。

- 数字、アルファベット、およびハイフン (-) のみが使用される有効な DNS 名であること。ホスト名でアンダーライン (_) を使用すると DNS が正常に動作しません。
- すべてが小文字であること。大文字は使用できません。
- ループバックアドレスに解決されないこと。**127.0.0.1** ではなく、システムのパブリック IP アドレスに解決される必要があります。

ホスト名を検証するには、インストールするシステムで **hostname** ユーティリティーを使用します。

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

hostname の出力は、**localhost** または **localhost6** 以外になる必要があります。

正引きおよび逆引きの DNS 設定の確認

1. サーバーの IP アドレスを取得します。**ip addr show** コマンドを実行すると、IPv4 アドレスと IPv6 アドレスの両方が表示されます。以下の例では、スコープがグローバルであるため、対応する IPv6 アドレスは **2001:DB8::1111** です。

```
[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
...
```

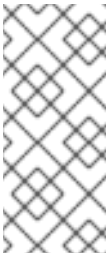
1. **dig** ユーティリティーを使用して、正引き DNS 設定を確認します。

   a. **dig +short server.example.com A** コマンドを実行します。返される IPv4 アドレスは、**ip addr show** により返される IP アドレスと一致する必要があります。

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

   b. **dig +short server.example.com AAAA** コマンドを実行します。このコマンドに返されるアドレスは、**ip addr show** により返される IPv6 アドレスと一致する必要があります。

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

   注記

   dig により AAAA レコードの出力が返されなくても、設定が間違っているわけではありません。出力されないのは、DNS にシステムの IPv6 アドレスが設定されていないためです。ネットワークで IPv6 プロトコルを使用する予定がない場合は、この状況でもインストールを続行できます。

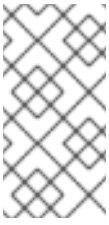
2. 逆引き DNS 設定 (PTR レコード) を確認します。**dig** ユーティリティーを使用し、IP アドレスを追加します。
   以下のコマンドを実行して、異なるホスト名が表示された場合や、前の手順で **dig +short server_host_name** を実行して IP アドレスが返されてもホスト名が表示されない場合は、逆引き DNS 設定が正しくありません。

   a. **dig +short -x IPv4_address** コマンドを実行します。以下の例のように、出力にサーバーのホスト名が表示されるはずです。

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

   b. 前の手順で実行した **dig +short -x server.example.com AAAA** コマンドにより IPv6 アドレスが返された場合、**dig** を使用して IPv6 アドレスのクエリーを実行します。以下の例のように、出力にサーバーホスト名が表示されるはずです。

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

   注記

   前の手順で **dig +short server.example.com AAAA** コマンドにより IPv6 アドレスが返されなかった場合は、AAAA レコードのクエリーを実行しても、何も出力されません。この場合、これは正常な動作で、誤った設定を示すものではありません。

DNS フォワーダーの基準準拠の確認 (統合 DNS の場合のみ必要)

Identity Management DNS サーバーで使用するすべての DNS フォワーダーが EDNS0 (Extension Mechanisms for DNS) および DNSSEC (DNS Security Extensions) の基準に準拠していることを確認します。具体的には、フォワーダーごとに、以下のコマンドの出力を確認します。

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

コマンドの出力には、以下の情報が含まれます。

- 状態 - **NOERROR**
- フラグ - **ra**
- EDNS フラグ - **do**
- **ANSWER** セクションには **RRSIG** レコードが必要です。

出力に上記のいずれかの項目がない場合は、使用している DNS フォワーダーのドキュメントに従い、EDNS0 と DNSSEC がサポートされ、有効になっていることを確認してください。BIND サーバーの最新バージョンでは、**dnssec-enable yes;** オプションが **/etc/named.conf** ファイルに設定されている必要があります。

dig により生成された出力の例

```
;; ->>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 [...]
```

/etc/hosts ファイルの確認

重要

/etc/hosts ファイルは手動で変更しないでください。以前に **/etc/hosts** を手動で変更したことがある場合は、コンテンツが以下のルールに準拠していることを確認してください。

以下は、適切に設定された **/etc/hosts** ファイルの例になります。

- ホストの IPv4 および IPv6 ローカルホストエントリーを適切に記述します。
- これらのエントリーの後に、Identity Management サーバーの IP アドレスとホスト名が最初のエントリーとして続きます。
- Identity Management サーバーのホスト名を、**localhost** エントリーには追加できないことに注意してください。

```
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. IDENTITY MANAGEMENT におけるポート要件

Identity Management は、複数のポートを使用して、そのサービスと対話します。Identity Management が動作するには、このようなポートを開いて Identity Management サーバーへの受信接続に利用できるようにする必要があります。別のサービスで現在使用されているポートや、ファイアウォールによりブロックされているポートは使用しないでください。

表1.1 Identity Management ポート

サービス	ポート	プロトコル
HTTP/HTTPS	80、443	TCP
LDAP/LDAPS	389、636	TCP
Kerberos	88、464	TCP および UDP
DNS	53	TCP および UDP (任意)
NTP	123	UDP (任意)

さらに、内部で使用されるポート 8080、8443、および 749 が未使用である必要があります。これらのポートは開かず、ファイアウォールによりブロックされたままにしてください。

表1.2 firewalld サービス

サービス名	詳細参照先
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**

必要なポートの開放

1. **firewalld** サービスが実行中である必要があります。
   - **firewalld** が実行中であることを確認するには、以下を実行します。

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

   - **firewalld** を起動し、システム起動時に自動的に起動するように設定するには、以下を実行します。

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

2. **firewall-cmd** ユーティリティーを使って必要なポートを開きます。以下のいずれかのオプションを選択します。

   a. **firewall-cmd --add-port** コマンドを使用して個別のポートをファイアウォールに追加します。たとえば、デフォルトゾーンでポートを開くには、以下を実行します。

   ```
   # 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. **firewall-cmd --add-service** コマンドを使用して、**firewalld** サービスをファイアウォールに追加します。たとえば、デフォルトのゾーンでポートを開くには以下を行います。

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

   firewall-cmd を使用してシステムでポートを解放する方法は、man ページの **firewall-cmd**(1) を参照してください。

3. **firewall-cmd** 設定を再ロードして、変更が即座に反映されるようにします。

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

   実稼働システムで **firewalld** を再ロードすると、DNS の接続がタイムアウトになる可能性があることに注意してください。必要な場合は、以下の例のように **firewall-cmd** コマンドで **--runtime-to-permanent** オプションを使用して、タイムアウトが発生しないようにし、変更を永続化します。

   ```
   # 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. **必要に応じて**、ポートが現在利用可能であるかを確認するには、**nc** ユーティリティー、**telnet** ユーティリティー、または **nmap** ユーティリティーを使用して、ポートへの接続またはポートスキャンの実行を行います。

注記

さらに、受信および送信トラフィックの両方でネットワークベースのファイアウォールを開く必要があることに注意してください。

1.5. IDENTITY MANAGEMENT サーバーに必要なパッケージのインストール

RHEL 8 では、 Identity Management (IdM) サーバーのインストールに必要なパッケージはモジュールとして同梱されています。IdM サーバーモジュールストリームは **DL1** ストリームと呼ばれ、このストリームからパッケージをダウンロードする前に、このストリームを有効にする必要があります。以下の手順は、Identity Management の環境設定に必要なパッケージのダウンロード方法を示しています。

前提条件

- RHEL システムを新たにインストールし、IdM モジュールストリームは有効にしていない。

手順

1. **idm:DL1** ストリームを有効にします。

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

2. **idm:DL1** ストリーム経由で配信される RPM に切り替えます。

```
# yum distro-sync
```

3. IdM の要件に応じて、以下のいずれかのオプションを選択します。

- 統合 DNS のない IdM サーバーのインストールに必要なパッケージをダウンロードします。

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

- 統合 DNS のある IdM サーバーのインストールに必要なパッケージをダウンロードします。

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

- Active Directory と信頼関係のある IdM サーバーのインストールに必要なパッケージをダウンロードします。

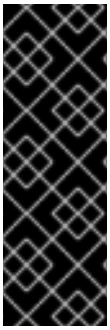
```
# yum module install idm:DL1/adtrust
```

- **adtrust** や **dns** などの複数のプロファイルからパッケージをダウンロードします。

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

- IdM クライアントのインストールに必要なパッケージをダウンロードします。

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



重要

別のストリームが有効になっていて、そのストリームからパッケージをダウンロードしたあとに、新しいモジュールストリームに切り替える場合は、インストール済みの関連コンテンツをすべて明示的に削除し、現在のモジュールストリームを無効にしてから、新しいモジュールストリームを有効にする必要があります。現在のストリームを無効にせずに新しいストリームを有効にしようとすると、エラーが発生します。詳細方法は「Switching module streams to install a different version of content」 を参照してください。

警告

モジュールからパッケージを個別にインストールすることは可能ですが、そのモジュールの「API」外のパッケージをインストールすると、Red Hat のサポート範囲は、そのモジュールに関連する場合に制限されます。たとえば、カスタム 380 Directory Server をセットアップするため、リポジトリーから直接 **bind-dyndb-ldap** をインストールした場合に発生した問題は、Identity Management でも発生する場合を除きサポートされません。

第2章 IDENTITY MANAGEMENT サーバーのインストール: 統合 DNS と統合 CA の場合

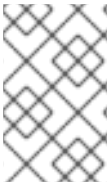
統合 DNS のある新しい Identity Management サーバーをインストールすると、次のような利点があります。

- ネイティブの Identity Management ツールを使用すると、メンテナンスおよび DNS レコードの管理のほとんどを自動化できます。たとえば、DNS SRV レコードは、セットアップ中に自動的に作成され、その後は自動的に更新されます。
- Identity Management サーバーのインストール中にグローバルフォワーダーを設定すると、インターネットと安定した接続を確立できます。グローバルフォワーダーは、Active Directory との信頼関係にも便利です。
- Identity Management ドメイン外で使用しているドメインに属する電子メールサーバーからのメールをスパムであると見なされないように、DNS 逆引きゾーンを設定できます。

統合 DNS のある Identity Management のインストールにはいくつかの制限があります。

- Identity Management DNS は、汎用の DNS サーバーとして使用するように設計されていないため、高度な DNS 機能の一部はサポートされません。

本章では、統合 CA をルート CA として新しい Identity Management サーバーをインストールする方法を説明します。



注記

ipa-server-install コマンドのデフォルト設定は、統合 CA をルート CA とします。**--external-ca** や **--ca-less** が指定された場合など、CA オプションがない場合は、Identity Management サーバーは統合 CA とインストールされます。

2.1. 対話型インストール

ipa-server-install ユーティリティーを使用して対話型インストールを実行している間、レルム、管理者のパスワード、Directory Manager のパスワードなど、システムの基本設定の提供を求められます。

ipa-server-install インストールスクリプトにより、 **/var/log/ipaserver-install.log** にログファイルが作成されます。ログは、インストールに失敗した時の問題特定に役立ちます。

手順

1. **ipa-server-install** ユーティリティーを実行します。

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

2. このスクリプトは、統合 DNS サービスを設定するかどうかを尋ねてくるため、**yes** と入力します。

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

3. このスクリプトは、設定をいくつか尋ねてきます。括弧で囲まれた値が推奨されるデフォルト値になります。
   - デフォルト値を使用する場合は **Enter** を押します。

- カスタム値を指定する場合は、指定の値を入力します。

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

警告

これらの名前は慎重に指定してください。インストール完了後に変更することはできません。

4. Directory Server のスーパーユーザー (**cn=Directory Manager**) のパスワードと、Identity Management の管理者システムユーザーアカウント (**admin**) のパスワードを入力します。

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

5. DNS フォワーダー設定のプロンプトが出されます。

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

- DNS フォワーダーを設定するには、**yes** を入力して表示されたコマンドラインの指示に従います。インストールプロセスにより、インストールした Identity Management サーバーの **/etc/named.conf** ファイルに、フォワーダーの IP アドレスが追加されます。
  - フォワードポリシーのデフォルト設定は、man ページの **ipa-dns-install**(1) に記載される **--forward-policy** の説明を参照してください。
- DNS 転送を使用しない場合は、**no** と入力します。
  DNS フォワーダーがないと、ご使用の環境は隔離され、インフラストラクチャー内の他の DNS ドメインからは名前が解決されません。

6. そのサーバーと関連する IP アドレスの DNS 逆引き (PTR) レコードを設定する必要性を確認するプロンプトが出されます。

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

検索を実行して逆引きゾーンが見つかると、PTR レコードの逆引きゾーンを作成するかどうかを尋ねられます。

```
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.
```

注記

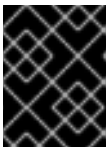
逆引きゾーンの管理に Identity Management を使用するのは任意です。代わりに、外部 DNS サービスを使用することもできます。

7. サーバー設定をする場合は、**yes** と入力します。

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

8. インストールスクリプトにより、サーバーが設定されます。動作が完了するまで待ちます。

9. インストールスクリプトが完了したら、親ドメインから Identity Management DNS ドメインに DNS 委譲 (delegation) を追加します。たとえば、Identity Management DNS ドメインが **ipa.example.com** の場合は、ネームサーバー (NS) レコードを **example.com** 親ドメインに追加します。



重要

この手順は、Identity Management DNS サーバーをインストールするたびに実行します。

2.2. 非対話型インストール

注記

ipa-server-install インストールスクリプトにより、 **/var/log/ipaserver-install.log** にログファイルが作成されます。ログは、インストールに失敗した時の問題特定に役立ちます。

手順

1. オプションで必要な情報をすべて指定して、**ipa-server-install** ユーティリティーを実行します。非対話型インストールで最低限必要なオプションは次のとおりです。

   - **--realm** - Kerberos レルム名を指定します。
   - **--ds-password** - Directory Server のスーパーユーザーである Directory Manager (DM) のパスワードを指定します。
   - **--admin-password** - Identity Management の管理者である **admin** のパスワードを指定します。
   - **--unattended** - インストールプロセスでホスト名およびドメイン名のデフォルトオプションを選択するようにします。

   統合 DNS のあるサーバーをインストールする場合は、以下のオプションも追加します。

   - **--setup-dns** - 統合 DNS名 を設定します。
   - **--forwarder** または **--no-forwarders** - DNS フォワーダーを設定するかを指定します。
   - **--auto-reverse** または **--no-reverse** - Identity Management DNS で作成する必要がある逆引き DNS ゾーンの自動検出を設定するかどうかを指定します。

   以下に例を示します。

```
# 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. インストールスクリプトが完了したら、親ドメインから Identity Management DNS ドメインに DNS 委譲 (delegation) を追加します。たとえば、Identity Management DNS ドメインが **ipa.example.com** の場合は、ネームサーバー (NS) レコードを **example.com** 親ドメインに追加します。

重要

この手順は、Identity Management DNS サーバーをインストールするたびに実行します。

関連資料

- ipa-server-install で使用できるオプションの完全リストを表示するには、**ipa-server-install --help** コマンドを実行します。

第3章 IDENTITY MANAGEMENT サーバーのインストール: 統合 DNS と外部 CA の場合

統合 DNS のある新しい Identity Management サーバーをインストールすると、次のような利点があります。

- ネイティブの Identity Management ツールを使用すると、メンテナンスおよび DNS レコードの管理のほとんどを自動化できます。たとえば、DNS SRV レコードは、セットアップ中に自動的に作成され、その後は自動的に更新されます。
- Identity Management サーバーのインストール中にグローバルフォワーダーを設定すると、インターネットと安定した接続を確立できます。グローバルフォワーダーは、Active Directory との信頼関係にも便利です。
- Identity Management ドメイン外で使用しているドメインに属する電子メールサーバーからのメールをスパムであると見なされないように、DNS 逆引きゾーンを設定できます。

統合 DNS のある Identity Management のインストールにはいくつかの制限があります。

- Identity Management DNS は、汎用の DNS サーバーとして使用するように設計されていないため、高度な DNS 機能の一部はサポートされません。

本章では、外部 CA をルート CA として新しい Identity Management サーバーをインストールする方法を説明します。

3.1. 対話型インストール

ipa-server-install ユーティリティーを使用して対話型インストールを実行している間、レルム、管理者のパスワード、Directory Manager のパスワードなど、システムの基本設定の提供を求められます。

ipa-server-install インストールスクリプトにより、 **/var/log/ipaserver-install.log** にログファイルが作成されます。ログは、インストールに失敗した時の問題特定に役立ちます。

この手順では、以下に該当するサーバーのインストール方法を説明します。

- 統合 DNS のあるサーバー
- 外部認証局 (CA) をルート CA とするサーバー

前提条件

- 使用する外部 CA のタイプを決定している (**--external-ca-type** オプション)。詳細は、man ページの **ipa-server-install**(1) を参照してください。
- もしくは、Active Directory Certificate Service (AD CS) テンプレートを指定して **--external-ca-profile** オプションを選択することもできます。たとえば、AD CS のインストール固有のオブジェクト識別子を指定するには、以下を実行します。

```
[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
```

手順

1. **--external-ca** オプションを使用して **ipa-server-install** ユーティリティーを実行します。

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

Microsoft Certificate Services の CA を使用している場合は、**--external-ca-type** オプションも使用してください。詳細は man ページの **ipa-server-install**(1) を参照してください。

2. スクリプトにより、統合 DNS サービスの設定が求められます。**yes** または **no** を入力します。この手順では、統合 DNS のあるサーバーをインストールします。

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

注記

統合 DNS のないサーバーをインストールする場合は、以下の手順にある DNS 設定のプロンプトが表示されません。DNS のないサーバーをインストールする手順の詳細は、*5章Identity Management サーバーのインストール: 統合 DNS がなく統合 CA がある場合*を参照してください。

3. このスクリプトは、設定をいくつか尋ねてきます。括弧で囲まれた値が推奨されるデフォルト値になります。

- デフォルト値を使用する場合は **Enter** を押します。
- カスタム値を指定する場合は、指定の値を入力します。

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

警告

これらの名前は慎重に指定してください。インストール完了後に変更することはできません。

4. Directory Server のスーパーユーザー (**cn=Directory Manager**) のパスワードと、Identity Management の管理者システムユーザーアカウント (**admin**) のパスワードを入力します。

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

5. DNS フォワーダー設定のプロンプトが出されます。

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

- DNS フォワーダーを設定するには、**yes** を入力して表示されたコマンドラインの指示に従います。インストールプロセスにより、インストールした Identity Management サーバーの **/etc/named.conf** ファイルに、フォワーダーの IP アドレスが追加されます。
  - フォワードポリシーのデフォルト設定は、man ページの **ipa-dns-install**(1) に記載される **--forward-policy** の説明を参照してください。

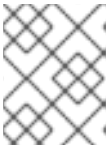
- DNS 転送を使用しない場合は、**no** と入力します。
  DNS フォワーダーがないと、ご使用の環境は隔離され、インフラストラクチャー内の他の DNS ドメインからは名前が解決されません。

6. そのサーバーと関連する IP アドレスの DNS 逆引き (PTR) レコードを設定する必要性を確認するプロンプトが出されます。

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

検索を実行して逆引きゾーンが見つかると、PTR レコードの逆引きゾーンを作成するかどうかを尋ねられます。

```
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.
```



注記

逆引きゾーンの管理に Identity Management を使用するのは任意です。代わりに、外部 DNS サービスを使用することもできます。

7. サーバー設定をする場合は、**yes** と入力します。

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

8. Certificate System インスタンスの設定時、このユーティリティーが証明書署名要求 (CSR) の場所 (**/root/ipa.csr**) を出力します。

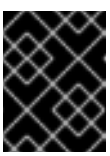
```
...

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
```

この場合は、以下を行います。

a. **/root/ipa.csr** にある CSR を外部 CA に提出します。このプロセスは、外部 CA として使用するサービスにより異なります。

b. 発行した証明書と、Base64 エンコードされたブロブ (PEM ファイルか Windows CA からの Base_64 証明書) で CA を発行する CA 証明書チェーンを取得します。プロセスは証明書サービスにより異なりますが、通常は Web ページか通知メールにダウンロードリンクがあり、管理者が必要なすべての証明書をダウンロードできるようになっています。



重要

CA 証明書のみではなく、CA 用の完全な証明書チェーンを取得してください。

c. **ipa-server-install** を再度実行し、新たに発行された CA 証明書と CA チェーンファイルの場所と名前を指定します。例を示します。

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

9. インストールスクリプトにより、サーバーが設定されます。動作が完了するまで待ちます。

注記

ipa-server-install --external-ca コマンドは、以下のエラーにより失敗する場合があります。

```
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
```

この失敗は、***_proxy** 環境設定が設定されていると発生します。この問題の解決方法は「トラブルシューティング: 外部 CA インストールの失敗」を参照してください。

3.2. トラブルシューティング: 外部 CA インストールの失敗

ipa-server-install --external-ca コマンドが、以下のエラーにより失敗します。

```
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
```

env|grep proxy を実行すると、以下のような変数が表示されます。

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

エラー内容:
***_proxy** 環境変数が原因でサーバーをインストールできません。

解決方法:

1. 以下のシェルスクリプトを使用して ***_proxy** 環境変数の設定を解除します。

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

2. **pkidestroy** ユーティリティーを実行して、インストールに失敗した CA サブシステムを削除します。

```
# 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. インストールに失敗した Identity Management サーバーを削除します。

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

4. **ipa-server-install --external-ca** を再度実行します。

第4章 IDENTITY MANAGEMENT サーバーのインストール: 統合 DNS があり CA がない場合

統合 DNS のある新しい Identity Management サーバーをインストールすると、次のような利点があります。

- ネイティブの Identity Management ツールを使用すると、メンテナンスおよび DNS レコードの管理のほとんどを自動化できます。たとえば、DNS SRV レコードは、セットアップ中に自動的に作成され、その後は自動的に更新されます。
- Identity Management サーバーのインストール中にグローバルフォワーダーを設定すると、インターネットと安定した接続を確立できます。グローバルフォワーダーは、Active Directory との信頼関係にも便利です。
- Identity Management ドメイン外で使用しているドメインに属する電子メールサーバーからのメールをスパムであると見なされないように、DNS 逆引きゾーンを設定できます。

統合 DNS のある Identity Management のインストールにはいくつかの制限があります。

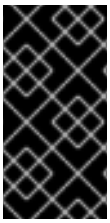
- Identity Management DNS は、汎用の DNS サーバーとして使用するように設計されていないため、高度な DNS 機能の一部はサポートされません。

本章では、CA がない場合に新しい Identity Management サーバーをインストールする方法を説明します。

4.1. CA なしで IDENTITY MANAGEMENT サーバーをインストールするために必要な証明書

ここでは、以下について記述します。

- 認証局 (CA) なしで Identity Management サーバーをインストールするために必要な証明書
- それらの証明書を **ipa-server-install** ユーティリティーに提供するのに使用されるコマンドラインオプション



重要

インポートした証明書ファイルには、LDAP サーバーおよび Apache サーバーの証明書を発行した CA の完全な証明書チェーンが含まれている必要があるため、自己署名のサードパーティーサーバー証明書を使用してサーバーまたはレプリカをインストールすることはできません。

LDAP サーバー証明書およびプライベートキー

- **--dirsrv-cert-file** - LDAP サーバー証明書の証明書、およびプライベートキーファイルを提供します。
- **--dirsrv-pin** - **--dirsrv-cert-file** に指定されたファイルにあるプライベートキーにアクセスするパスワードを提供します。

Apache サーバー証明書およびプライベートキー

- **--http-cert-file** - Apache サーバー証明書の証明書、およびプライベートキーファイルを提供します。

- **--http-pin** - **--http-cert-file** に指定したファイルにあるプライベートキーにアクセスするパスワードを提供します。

LDAP および Apache サーバー証明書を発行した CA の完全な CA 証明書チェーン

- **--dirsrv-cert-file** および **--http-cert-file** - 完全な CA 証明書チェーンまたはその一部を持つ証明書ファイルを提供します。

--dirsrv-cert-file および **--http-cert-file** を使用して提供されるファイルには、厳密に 1 つのサーバー証明書と 1 つの秘密キーが含まれている必要があります。**--dirsrv-cert-file** と **--http-cert-file** を使用して提供されるファイルのコンテンツは同一であることがよくあります。

完全な CA 証明書チェーンを提供する証明書ファイル (一部の環境では必要ありません)

- **--ca-cert-file** - LDAP、Apache Server、および Kerberos KDC の証明書を発行した CA の CA 証明書が含まれるファイル。他のオプションにより提供される証明書ファイルに CA 証明書が存在しない場合に、このオプションを使用してください。

--ca-cert-file で提供されるファイルと組み合わせて、**--dirsrv-cert-file** および **--http-cert-file** を使用して提供されるファイルには、LDAP および Apache サーバー証明書を発行した CA の完全 CA 証明書チェーンが含まれる必要があります。

Kerberos 鍵配布センター (KDC) の PKINIT 証明書およびプライベートキー (任意)

- **--pkinit-cert-file** - Kerberos KDC SSL の証明書およびプライベートキーを提供します。
- **--pkinit-pin** - **--pkinit-cert-file** に指定されたファイルにある Kerberos KDC のプライベートキーにアクセスするパスワードを提供します。
- **--no-pkinit** - pkinit 設定手順を無効にします。

PKINIT 証明書を提供しないと、**ipa-server-install** は自己署名証明書を使用するローカル KDC で IdM サーバーを設定します。

関連資料

- これらのオプションで使用できる証明書ファイル形式に関する詳細は、man ページの **ipa-server-install**(1) を参照してください。

4.2. 対話型インストール

ipa-server-install ユーティリティーを使用して対話型インストールを実行している間、レルム、管理者のパスワード、Directory Manager のパスワードなど、システムの基本設定の提供を求められます。

ipa-server-install インストールスクリプトにより、 **/var/log/ipaserver-install.log** にログファイルが作成されます。ログは、インストールに失敗した時の問題特定に役立ちます。

手順

1. **ipa-server-install** ユーティリティーを実行し、必要な証明書をすべて提供します。以下に例を示します。

```
[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
```

提供される証明書の詳細は「CA なしで Identity Management サーバーをインストールするために必要な証明書」を参照してください。

2. スクリプトにより、統合 DNS サービスの設定が求められます。**yes** または **no** を入力します。この手順では、統合 DNS のあるサーバーをインストールします。

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

注記

統合 DNS のないサーバーをインストールする場合は、以下の手順にある DNS 設定のプロンプトが表示されません。DNS のないサーバーをインストールする手順の詳細は、*5章Identity Management サーバーのインストール: 統合 DNS がなく統合 CA がある場合*を参照してください。

3. このスクリプトは、設定をいくつか尋ねてきます。括弧で囲まれた値が推奨されるデフォルト値になります。

- デフォルト値を使用する場合は **Enter** を押します。
- カスタム値を指定する場合は、指定の値を入力します。

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

警告

これらの名前は慎重に指定してください。インストール完了後に変更することはできません。

4. Directory Server のスーパーユーザー (**cn=Directory Manager**) のパスワードと、Identity Management の管理者システムユーザーアカウント (**admin**) のパスワードを入力します。

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

5. DNS フォワーダー設定のプロンプトが出されます。

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

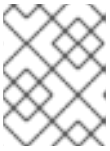
- DNS フォワーダーを設定するには、**yes** を入力して表示されたコマンドラインの指示に従います。インストールプロセスにより、インストールした Identity Management サーバーの **/etc/named.conf** ファイルに、フォワーダーの IP アドレスが追加されます。
    - フォワードポリシーのデフォルト設定は、man ページの **ipa-dns-install**(1) に記載される **--forward-policy** の説明を参照してください。
- DNS 転送を使用しない場合は、**no** と入力します。
  DNS フォワーダーがないと、ご使用の環境は隔離され、インフラストラクチャー内の他の DNS ドメインからは名前が解決されません。

6. そのサーバーと関連する IP アドレスの DNS 逆引き (PTR) レコードを設定する必要性を確認するプロンプトが出されます。

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

検索を実行して逆引きゾーンが見つかると、PTR レコードの逆引きゾーンを作成するかどうかを尋ねられます。

```
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.
```



注記

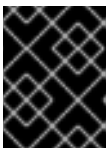
逆引きゾーンの管理に Identity Management を使用するのは任意です。代わりに、外部 DNS サービスを使用することもできます。

7. サーバー設定をする場合は、**yes** と入力します。

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

8. インストールスクリプトにより、サーバーが設定されます。動作が完了するまで待ちます。

9. インストールスクリプトが完了したら、親ドメインから Identity Management DNS ドメインに DNS 委譲 (delegation) を追加します。たとえば、Identity Management DNS ドメインが **ipa.example.com** の場合は、ネームサーバー (NS) レコードを **example.com** 親ドメインに追加します。



重要

この手順は、Identity Management DNS サーバーをインストールするたびに実行します。

第5章 IDENTITY MANAGEMENT サーバーのインストール: 統合 DNS がなく統合 CA がある場合

本章では、統合 DNS なしで新しい Identity Management サーバーをインストールする方法を説明します。

5.1. 対話型インストール

ipa-server-install ユーティリティーを使用して対話型インストールを実行している間、レルム、管理者のパスワード、Directory Manager のパスワードなど、システムの基本設定の提供を求められます。

ipa-server-install インストールスクリプトにより、 **/var/log/ipaserver-install.log** にログファイルが作成されます。ログは、インストールに失敗した時の問題特定に役立ちます。

この手順では、以下のサーバーをインストールします。

- 統合 DNS のないサーバー
- 統合 Identity Management 認証局 (CA) をルート CA とするサーバー (デフォルトの CA 設定)

手順

1. **ipa-server-install** ユーティリティーを実行します。

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

2. このスクリプトにより、統合 DNS サービスを設定するように求められるため、**Enter** を押してデフォルトの **no** オプションを選択します。

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

3. このスクリプトは、設定をいくつか尋ねてきます。括弧で囲まれた値が推奨されるデフォルト値になります。
   - デフォルト値を使用する場合は **Enter** を押します。
   - カスタム値を指定する場合は、指定の値を入力します。

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

警告

これらの名前は慎重に指定してください。インストール完了後に変更することはできません。

4. Directory Server のスーパーユーザー (**cn=Directory Manager**) のパスワードと、Identity Management の管理者システムユーザーアカウント (**admin**) のパスワードを入力します。

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

5. サーバー設定をする場合は、**yes** と入力します。

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

6. インストールスクリプトにより、サーバーが設定されます。動作が完了するまで待ちます。

5.2. 非対話型インストール

この手順では、以下のサーバーをインストールします。

- 統合 DNS のないサーバー
- 統合 Identity Management 認証局 (CA) をルート CA とするサーバー (デフォルトの CA 設定)

注記

ipa-server-install インストールスクリプトにより、 **/var/log/ipaserver-install.log** にログファイルが作成されます。ログは、インストールに失敗した時の問題特定に役立ちます。

手順

1. オプションで必要な情報をすべて指定して、**ipa-server-install** ユーティリティーを実行します。非対話型インストールで最低限必要なオプションは次のとおりです。
   - **--realm** - Kerberos レルム名を指定します。
   - **--ds-password** - Directory Server のスーパーユーザーである Directory Manager (DM) のパスワードを指定します。
   - **--admin-password** - Identity Management の管理者である **admin** のパスワードを指定します。
   - **--unattended** - インストールプロセスでホスト名およびドメイン名のデフォルトオプションを選択するようにします。

   以下に例を示します。

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

関連資料

- ipa-server-install で使用できるオプションの完全リストを表示するには、**ipa-server-install --help** コマンドを実行します。

第6章 IDENTITY MANAGEMENT サーバーのアンインストール

管理者は、トポロジーから Identity Management サーバーを削除できます。

この手順では、**server.idm.example.com** という名前のサンプルサーバーをアンインストールする方法を説明します。

前提条件

- 認証局 (CA)、鍵回復機関 (KRA)、または DNS サーバーとして機能するサーバーをアンインストールする前に、これらのサービスがドメインの別のサーバーで実行していることを確認している。

警告

CA、KRA、または DNS サーバーとして機能する唯一のサーバーを削除すると、Identity Management 機能に深刻な不具合が生じます。

手順

1. トポロジーにあり、**server.idm.example.com** とのレプリケーションアグリーメントを持つすべてのサーバーで **ipa server-del** コマンドを使用し、トポロジーからレプリカを削除します。

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

2. **server.idm.example.com** で、**ipa-server-install --uninstall** コマンドを使用します。

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

3. **server.idm.example.com** を参照するすべてのネームサーバー (NS) の DNS レコードが DNS ゾーンから削除されていることを確認します。使用する DNS が Identity Management により管理される統合 DNS であるか、または外部 DNS であるかに関わらず、確認を行なってください。

第7章 IDENTITY MANAGEMENT サーバーの名前変更

既存の Identity Management サーバーのホスト名を変更することはできませんが、サーバーを、別の名前のレプリカに置き換えることは可能です。

手順

1. 既存のサーバーの代わりになる新しいレプリカをインストールします。必ず、レプリカに必要なホスト名と IP アドレスを指定するようにしてください。詳細は 15章*Identity Management レプリカのインストール* を参照してください。

重要

アンインストールするサーバーが CRL マスターサーバーである場合は、作業を続ける前に別のサーバーを CRL マスターサーバーにしてください。

2. 既存の Identity Management サーバーインスタンスを停止します。

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

3. 6章*Identity Management サーバーのアンインストール* の説明に従って、既存のサーバーをアンインストールします。

第8章 IDENTITY MANAGEMENT クライアントをインストールするためのシステムの準備

本章では、Identity Management クライアントをインストールするのに必要なシステムの条件を説明します。

8.1. IDENTITY MANAGEMENT クライアントの DNS 要件

デフォルトでは、クライアントインストーラーは、ホスト名の親であるすべてのドメインの **_ldap._tcp.DOMAIN** DNS SRV レコードを検索します。たとえば、クライアントマシンのホスト名が **client1.idm.example.com** である場合、インストーラーは **_ldap._tcp.idm.example.com**、**_ldap._tcp.example.com**、および **_ldap._tcp.com** の DNS SRV レコードから Identity Management サーバーのホスト名を取得しようとします。その後、検出されたドメインを使用して、クライアントコンポーネント (SSSD や Kerberos 5 設定など) をマシン上で設定します。

しかし、Identity Management クライアントのホスト名を、プライマリー DNS ドメインの一部にする必要はありません。クライアントマシンのホスト名が Identity Management サーバーのサブドメインでない場合、IdM ドメインを **ipa-client-install** コマンドの **--domain** オプションとして渡します。これにより、クライアントのインストール後に、SSSD および Kerberos コンポーネントの両方の設定ファイルにドメインが設定され、 Identity Management サーバーの自動検出に使用されます。

関連資料

- Identity Management の DNS 要件に関する詳細は、「Identity Management のホスト名および DNS の要件」 を参照してください。

8.2. IDENTITY MANAGEMENT クライアントの ポート要件

Identity Management クライアントは、Identity Management サーバーの複数のポートに接続し、サービスと通信します。

Identity Management クライアントでこれらのポートを **送信方向** に開く必要があります。**firewalld** などの、送信パケットをフィルターしないファイアウォールを使用している場合は、ポートはすでに送信方向で使用可能です。

関連資料

- 使用されるポートに関する詳細は、「Identity Management におけるポート要件」 を参照してください。

8.3. IDENTITY MANAGEMENT クライアントのインストールに必要なパッケージ

RHEL8 では、Identity Management クライアントのインストールに必要なパッケージはモジュールとして同梱されます。以下の 2 つの IdM ストリームが IdM クライアントパッケージを提供します。

- **idm:client** ストリーム。詳細は 「idm:client ストリームからの ipa-client パッケージのインストール」 を参照してください。
- **idm:DL1** ストリーム。詳細は 「idm:DL1 ストリームからの ipa-client パッケージのインストール」 を参照してください。

8.3.1. idm:client ストリームからの ipa-client パッケージのインストール

idm:client ストリームは、**idm** モジュールのデフォルトのストリームです。マシンにサーバーコンポーネントをインストールする必要がない場合は、このストリームを使用して IdM クライアントパッケージをダウンロードします。長期的にサポートされる IdM クライアントソフトウェアを一貫して使用する必要があり、サーバーコンポーネントが必要でない場合は、**idm:client** ストリームの使用が推奨されます。

手順

1. (任意手順) **idm:DL1** ストリームを有効にしたことがなければ、クライアントパッケージをダウンロードする前に **idm:client** ストリームを有効にする必要はありません。**idm:DL1** ストリームが有効である場合は、デフォルトの **idm:client** ストリームから配信される RPM に切り替えます。

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

2. IdM クライアントのインストールに必要なパッケージをダウンロードします。

```
# yum module install idm
```

8.3.2. idm:DL1 ストリームからの ipa-client パッケージのインストール

idm:DL1 からパッケージをダウンロードするには、このストリームを有効にする必要があります。マシン上に IdM サーバーコンポーネントをインストールする必要がある場合は、このストリームを使用して IdM クライアントパッケージをダウンロードしてください。

手順

1. **idm:DL1** ストリームから配信される RPM に切り替えていない場合は、切り替えます。

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

2. IdM クライアントのインストールに必要なパッケージをダウンロードします。

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

第9章 IDENTITY MANAGEMENT クライアントのインストール: 基本的なシナリオ

ここでは、**ipa-client-install** ユーティリティーを使用して、システムを Identity Management (IdM) クライアントとして設定する方法を説明します。システムを IdM クライアントとして設定すると、IdM ドメインに登録され、システムがドメインの IdM サーバーで IdM サービスを使用できるようになります。

基本インストールには複数のオプションがあります。

- 特権ユーザーのクレデンシャルを使用してクライアントを対話的にインストールする場合は、「ユーザークレデンシャルを使用したクライアントのインストール: 対話的なインストール」 を参照してください。
- ワンタイムパスワードを使用してクライアントを対話的にインストールする場合は、「ワンタイムパスワードを使用したクライアントのインストール: 対話的なインストール」 を参照してください。
- 特権ユーザーのクレデンシャル、ワンタイムパスワード、または前回登録時のキータブのいずれかを使用してクライアントを非対話的にインストールする場合は、「クライアントのインストール: 非対話的なインストール」 を参照してください。

9.1. 前提条件

Identity Management クライアントをインストールする前に、すべての前提条件を満たしていることを確認してください。8章*Identity Management クライアントをインストールするためのシステムの準備* を参照してください。

9.2. IDENTITY MANAGEMENT クライアントのインストールオプションの概要

Identity Management クライアントを正しくインストールするには、クライアントの登録に使用できるクレデンシャルを提供する必要があります。以下の認証方法を使用できます。

- クライアントを登録する権限のあるユーザーのクレデンシャル。これは、**ipa-client-install** が想定するデフォルトオプションです。
  - 登録権限のあるユーザーのクレデンシャルを直接 **ipa-client-install** に提供するには、**--principal** および **--password** オプションを使用します。詳細手順は 「ユーザークレデンシャルを使用したクライアントのインストール: 対話的なインストール」 を参照してください。
- サーバーで無作為に事前生成されるワンタイムパスワード
  - この認証方法を使用するには、**--random** オプションを **ipa-client-install** オプションに追加します。詳細手順は 「ワンタイムパスワードを使用したクライアントのインストール: 対話的なインストール」 を参照してください。
- 前回登録時のクライアントプリンシパル
  - このオプションは、システムが Identity Management クライアントとして登録されたことがある場合に使用できます。この認証方法を使用するには、**--keytab** オプションを **ipa-client-install** に追加します。詳細は 11章*Identity Management クライアントの再登録* を参照してください。

関連資料

- **ipa-client-install** により許可されるオプションの詳細は、man ページの **ipa-client-install**(1) を参照してください。

9.3. ユーザークレデンシャルを使用したクライアントのインストール: 対話的なインストール

この手順では、登録権限のあるユーザーのクレデンシャルを使用してシステムをドメインに登録し、Identity Management クライアントを対話的にインストールする方法を説明します。

前提条件

- クライアントを Identity Management ドメインに登録する権限を持つユーザーのクレデンシャルがある。たとえば、登録管理者 (Enrollment Administrator) ロールを持つ **hostadmin** ユーザーなどが該当します。

手順

1. Identity Management クライアントとして設定するシステムで **ipa-client-install** ユーティリティーを実行します。

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

以下のいずれか条件に該当する場合は、**--enable-dns-updates** オプションを追加して、クライアントシステムの IP アドレスで DNS レコードを更新します。

- クライアントを登録する Identity Management サーバーが、統合 DNS とともにインストールされた場合。
- ネットワーク上の DNS サーバーが、GSS-TSIG プロトコルを用いた DNS エントリー更新を受け入れる場合。

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

DNS 更新を有効にすると、クライアントが以下の条件に当てはまる場合に便利です。

- クライアントに、DHCP (Dynamic Host Configuration Protocol) を使用して発行した動的 IP アドレスがある。
- クライアントに、静的 IP アドレスが割り当てられたばかりで、IdM サーバーがそのアドレスを認識していない。

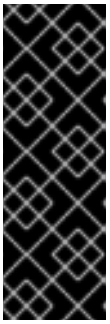
2. インストールスクリプトは、DNS レコードなどの必要な設定をすべて自動的に取得しようとします。

- IdM DNS ゾーンで SRV レコードが正しく設定されていると、スクリプトはその他に必要な値をすべて自動的に検出し、表示します。**yes** を入力して確定します。

```
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
```

- システムを別の値でインストールする場合は **no** を入力します。その後、**ipa-client-install** を再度実行し、コマンドラインオプションを **ipa-client-install** に追加して必要な値を指定します。以下に例を示します。
  - **--hostname**
  - **--realm**
  - **--domain**
  - **--server**
- スクリプトが一部の設定を自動的に取得できなかった場合は、値を入力するように求められます。



重要

完全修飾ドメイン名は、有効な DNS 名である必要があります。

- 数字、アルファベット、およびハイフンのみを使用できます。たとえば、アンダーラインは許可されないため、DNS の障害が発生する原因となる可能性があります。
- ホスト名はすべて小文字である必要があります。大文字は使用できません。

3. スクリプトにより、アイデンティティーがクライアントの登録に使用されるユーザーの入力が求められます。たとえば、登録監理者 (Enrollment Administrator) ロールを持つ **hostadmin** ユーザーなどが該当します。

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

4. インストールスクリプトにより、クライアントが設定されます。動作が完了するまで待ちます。

```
Client configuration complete.
```

関連資料

- クライアントインストールスクリプトが DNS レコードを検索する方法は、man ページの **ipa-client-install**(1) にある **DNS Autodiscovery** セクションを参照してください。

9.4. ワンタイムパスワードを使用したクライアントのインストール: 対話的なインストール

この手順では、ワンタイムパスワードを使用してシステムをドメインに登録し、Identity Management クライアントを対話的にインストールする方法を説明します。

前提条件

1. ドメインのサーバー上で、クライアントシステムを Identity Management ホストとして追加している。**ipa host-add** コマンドに **--random** オプションを使用して、登録のワンタイムパスワードを無作為に生成します。

```
$ 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
```

注記

生成されたパスワードは、マシンを Identity Management ドメインに登録するために使用した後は無効になります。登録の完了後、このパスワードは適切なホストキータブに置き換えられます。

手順

1. Identity Management クライアントとして設定するシステム上で **ipa-client-install** ユーティリティーを実行します。**--password** オプションを使用して、無作為に生成されたワンタイムパスワードを提供します。パスワードに特殊文字が含まれることが多いため、パスワードを一重引用符 (') で囲みます。

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

以下のいずれか条件に該当する場合は、**--enable-dns-updates** オプションを追加して、クライアントシステムの IP アドレスで DNS レコードを更新します。

- クライアントを登録する Identity Management サーバーが、統合 DNS とともにインストールされた場合。
- ネットワーク上の DNS サーバーが、GSS-TSIG プロトコルを用いた DNS エントリー更新を受け入れる場合。

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

DNS 更新を有効にすると、クライアントが以下の条件に当てはまる場合に便利です。

- クライアントに、DHCP (Dynamic Host Configuration Protocol) を使用して発行した動的 IP アドレスがある。
- クライアントに、静的 IP アドレスが割り当てられたばかりで、IdM サーバーがそのアドレスを認識していない。

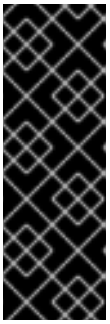
2. インストールスクリプトは、DNS レコードなどの必要な設定をすべて自動的に取得しようとします。
   - IdM DNS ゾーンで SRV レコードが正しく設定されていると、スクリプトはその他に必要な値をすべて自動的に検出し、表示します。**yes** を入力して確定します。

```
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
```

- システムを別の値でインストールする場合は **no** を入力します。その後、**ipa-client-install** を再度実行し、コマンドラインオプションを **ipa-client-install** に追加して必要な値を指定します。以下に例を示します。
  - **--hostname**
  - **--realm**
  - **--domain**
  - **--server**
- スクリプトが一部の設定を自動的に取得できなかった場合は、値を入力するように求められます。



重要

完全修飾ドメイン名は、有効な DNS 名である必要があります。

- 数字、アルファベット、およびハイフンのみを使用できます。たとえば、アンダーラインは許可されないため、DNS の障害が発生する原因となる可能性があります。
- ホスト名はすべて小文字である必要があります。大文字は使用できません。

3. インストールスクリプトにより、クライアントが設定されます。動作が完了するまで待ちます。

```
Client configuration complete.
```

関連資料

- クライアントインストールスクリプトが DNS レコードを検索する方法は、man ページの **ipa-client-install**(1) にある **DNS Autodiscovery** セクションを参照してください。

9.5. クライアントのインストール: 非対話的なインストール

非対話的なインストールでは、コマンドラインオプションを使用して、**ipa-client-install** ユーティリティーに必要な情報をすべて提供する必要があります。ここでは、非対話的なインストールに最低限必要なオプションを説明します。

クライアント登録の認証方法のオプション

利用可能なオプションは以下のとおりです。

- **--principal** および **--password** - クライアントを登録する権限のあるユーザーのクレデンシャルを指定します。
- **--random** - クライアントに対して無作為に生成されたワンタイムパスワードを指定します。
- **--keytab** - 前回登録時のキータブを指定します。

詳細は 「Identity Management クライアントのインストールオプションの概要」 を参照してください。

無人インストールのオプション

--unattended - ユーザーによる確認を必要とせずにインストールを実行できるようにします。SRV レコードが IdM DNS ゾーンで正しく設定されている場合は、スクリプトが自動的に必要な値をすべて検出します。スクリプトが自動的に値を検出できない場合は、以下のようなコマンドラインオプションを使用して指定してください。

- **--hostname** - クライアントマシンの静的ホスト名を指定します。

重要

完全修飾ドメイン名は、有効な DNS 名である必要があります。

- 数字、アルファベット、およびハイフンのみを使用できます。たとえば、アンダーラインは許可されないため、DNS の障害が発生する原因となる可能性があります。
- ホスト名はすべて小文字である必要があります。大文字は使用できません。

- **--server** - クライアントが登録される IdM サーバーのホスト名を指定します。
- **--domain** - クライアントが登録される IdM サーバーの DNS ドメイン名を指定します。
- **--realm** - Kerberos レルム名を指定します。

非対話的なインストールを行う基本的な **ipa-client-install** コマンドの例は次のとおりです。

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

非対話的なインストールを行う、追加のオプションを指定した **ipa-client-install** コマンドの例は次のとおりです。

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

関連資料

- **ipa-client-install** により許可されるオプションの完全リストは、man ページの **ipa-client-install**(1) を参照してください。

9.6. クライアントインストール後の事前設定された IDENTITY MANAGEMENT の削除

ipa-client-install スクリプトは、**/etc/openldap/ldap.conf** および **/etc/sssd/sssd.conf** ファイルから、以前の LDAP および SSSD 設定を削除します。クライアントをインストールする前にこれらのファイルの設定を変更すると、スクリプトにより新しいクライアントの値が追加されますが、コメントアウトされます。以下に例を示します。

-

```
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
```

Identity Management の新しい設定値を適用するには、以下を行います。

1. **/etc/openldap/ldap.conf** および **/etc/sssd/sssd.conf** を開きます。
2. 以前の設定を削除します。
3. 新しい Identity Management 設定をアンコメントします。
4. システム全体の LDAP 設定に依存するサーバープロセスの中には、再起動しないと変更が適用されない場合があります。**openldap** ライブラリーを使用するアプリケーションでは通常、起動時に設定がインポートされます。

9.7. IDENTITY MANAGEMENT クライアントのテスト

コマンドラインインターフェースにより、**ipa-client-install** が正常に実行されたことが通知されますが、独自のテストを行うこともできます。

Identity Management クライアントが、サーバー上で定義されたユーザーに関する情報を取得できることをテストするには、サーバー上で定義されたユーザーを解決できることをチェックします。たとえば、デフォルトの **admin** ユーザーをチェックするには、以下を実行します。

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

認証が適切に機能することをテストするには、root 以外のユーザーで **su** を実行し、root になります。

```
[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. IDENTITY MANAGEMENT クライアントのインストール中に実行される接続

表9.1「Identity Management クライアントのインストール中に実行されるリクエスト」 には、Identity Management (IdM) のクライアントインストールツールである **ipa-client-install** により実行される操作の一覧が記載されています。

表9.1 Identity Management クライアントのインストール中に実行されるリクエスト

操作	使用プロトコル	目的
クライアントシステムに設定した DNS リゾルバーに対する DNS レゾリューション	DNS	IdM マスターの IP アドレスを検出。(任意) A/AAAA および SSHFP レコードを追加。

操作	使用プロトコル	目的
IdM レプリカ上のポート 88 (TCP/TCP6 および UDP/UDP6) へのリクエスト	Kerberos	Kerberos チケットの取得。
検出または設定された IdM マスター上の IdM Apache ベースの Web サービスへの JSON-RPC 呼び出し	HTTPS	IdM クライアント登録。LDAP の方法が失敗した場合に CA 証明書チェーンを取得。必要な場合は証明書の発行を要求。
SASL GSSAPI 認証、プレーン LDAP、またはこの両方を使用した、IdM サーバー上のポート 389 (TCP/TCP6) へのリクエスト	LDAP	IdM クライアント登録、SSSD プロセスによるアイデンティティーの取得、ホストプリンシパルの Kerberos キーの取得。
ネットワークタイムプロトコル (NTP) の検出および解決 (任意)	NTP	クライアントシステムと NTP サーバー間の時間を同期。

9.9. ポストインストールのデプロイメント実行時の IDENTITY MANAGEMENT クライアントのサーバーとの通信

Identity Management (IdM) フレームワークのクライアント側は 2 つの異なるアプリケーションで実装されます。

- **ipa** コマンドラインインターフェース (CLI)
- ブラウザーベースの Web UI

ブラウザーベースの Web UI は任意です。

表9.2「CLI のポストインストール操作」 には、IdM クライアントのポストインストールのデプロイメント実行時に、CLI により実行される操作が記載されています。表9.3「webUI のポストインストール操作」 には、IdM クライアントのポストインストールのデプロイメント実行時に Web UI により実行される操作が記載されています。

IdM クライアントでは、の 2 つのデーモン (**System Security Services Daemon** (SSSD) と **certmonger**) が実行します。「SSSD 通信パターン」 および 「Certmonger の通信パターン」 には、このデーモンが IdM および Active Directory サーバーで使用できるサービスと通信する方法が記載されています。

表9.2 CLI のポストインストール操作

操作	使用プロトコル	目的
クライアントシステムに設定した DNS リゾルバーに対する DNS レゾリューション	DNS	IdM マスターの IP アドレスの検出。

操作	使用プロトコル	目的
IdM レプリカ上のポート 88 (TCP/TCP6 および UDP/UDP6) およびポート 464 (TCP/TCP6 および UDP/UDP6) へのリクエスト	Kerberos	Kerberos チケットの取得。Kerberos パスワードの変更。IdM Web UI への認証。
検出または設定された IdM マスター上の IdM Apache ベースの Web サービスへの JSON-RPC 呼び出し	HTTPS	**ipa** ユーティリティーの使用。

表9.3 webUI のポストインストール操作

操作	使用プロトコル	目的
検出または設定された IdM マスター上の IdM Apache ベースの Web サービスへの JSON-RPC 呼び出し	HTTPS	IdM Web UI ページの取得。

9.9.1. SSSD 通信パターン

SSSD (System Security Services Daemon、システムセキュリティーサービスデーモン) は、リモートディレクトリーと認証メカニズムにアクセスするシステムサービスです。IdM クライアントに設定すると、認証、認可、その他のアイデンティティー情報、およびその他のポリシー情報を提供する IdM サーバーに接続します。IdM サーバーと Active Directory (AD) が信頼関係にある場合、SSSD は AD にも接続し、Kerberos プロトコルを使用して AD ユーザーの認証を実行します。デフォルトでは SSSD は Kerberos を使用してローカル以外のユーザーを認証します。特別な状況では、代わりに LDAP プロトコルを使用するように SSSD を設定することがあります。

SSSD (System Security Services Daemon、システムセキュリティーサービスデーモン) を設定すると、複数のサーバーと通信できます。表9.4「IdM サーバーとの通信時における IdM クライアントの SSSD の通信パターン」 および 表9.5「Active Directory ドメインコントローラーとの通信時におけるトラストエージェントとして機能する IdM サーバー上の SSSD の通信パターン」 には、IdM の SSSD の一般的な通信パターンが説明されています。

表9.4 IdM サーバーとの通信時における IdM クライアントの SSSD の通信パターン

操作	使用プロトコル	目的
クライアントシステムに設定した DNS リゾルバーに対する DNS レゾリューション	DNS	IdM マスターの IP アドレスの検出。
Identity Management レプリカおよび Active Directory ドメインコントローラー上のポート 88 (TCP/TCP6 と UDP/UDP6)、464 (TCP/TCP6 と UDP/UDP6)、および 749 (TCP/TCP6) へのリクエスト	Kerberos	Kerberos チケットの取得。Kerberos パスワードの変更。

操作	使用プロトコル	目的
SASL GSSAPI 認証、プレーン LDAP、またはこの両方を使用した、IdM サーバー上のポート 389 (TCP/TCP6) へのリクエスト	LDAP	IdM ユーザーおよびホストの情報を取得。HBAC および sudo ルールのダンロード。マップ、SELinux ユーザーコンテキスト、パブリック SSH キー、および IdM LDAP に保存されるその他の情報の自動マウント。
(任意) スマートカード認証の場合、OCSP (Online Certificate Status Protocol) レスポンダーへのリクエスト (設定されている場合)。通常、ポート 80 で行われますが、クライアント証明書にある OCSP レスポンダー URL の実際の値により異なります。	HTTP	スマートカードにインストールされた証明書の状態に関する情報の取得。

表9.5 Active Directory ドメインコントローラーとの通信時におけるトラストエージェントとして機能する IdM サーバー上の SSSD の通信パターン

操作	使用プロトコル	目的
クライアントシステムに設定した DNS リゾルバーに対する DNS レゾリューション	DNS	IdM マスターの IP アドレスの検出。
Identity Management レプリカおよび Active Directory ドメインコントローラー上のポート 88 (TCP/TCP6 と UDP/UDP6)、464 (TCP/TCP6 と UDP/UDP6)、および 749 (TCP/TCP6) へのリクエスト	Kerberos	Kerberos チケットの取得。Kerberos パスワードの変更。Kerberos をリモートで管理。
ポート 389 (TCP/TCP6 および UDP/UDP6) およびポート 3268 (TCP/TCP6) へのリクエスト	LDAP	Active Directory ユーザーおよびグループ情報のクエリー。Active Directory ドメインコントローラーの検出。
(任意) スマートカード認証の場合、OCSP (Online Certificate Status Protocol) レスポンダーへのリクエスト (設定されている場合)。通常、ポート 80 で行われますが、クライアント証明書にある OCSP レスポンダー URL の実際の値により異なります。	HTTP	スマートカードにインストールされた証明書の状態に関する情報の取得。

9.9.2. Certmonger の通信パターン

Certmonger は、IdM マスターおよび IdM クライアント上で実行するデーモンで、ホスト上のサービスに関連する SSL 証明書の更新を適時に更新できるようにします。表9.6「Certmonger の通信パターン」 には、IdM マスター上で IdM クライアントの **certmonger** ユーティリティーにより実行される操

作が説明されています。

表9.6 Certmonger の通信パターン

操作	使用プロトコル	目的
クライアントシステムに設定した DNS リゾルバーに対する DNS レゾリューション	DNS	IdM マスターの IP アドレスの検出。
IdM レプリカ上のポート 88 (TCP/TCP6 および UDP/UDP6) およびポート 464 (TCP/TCP6 および UDP/UDP6) へのリクエスト	Kerberos	Kerberos チケットの取得。
検出または設定された IdM マスター上の IdM Apache ベースの Web サービスへの JSON-RPC 呼び出し	HTTPS	新しい証明書のリクエスト。
IdM マスターのポート 8080 (TCP/TCP6) でのアクセス	HTTP	OCSP (Online Certificate Status Protocol) レスポンダーおよび証明書の状態の取得。
(最初にインストールされたサーバーまたは証明書の追跡が移動されたサーバー上) IdM マスターのポート 8443 (TCP/TCP6) でのアクセス	HTTPS	IdM マスター上での認証局の管理 (IdM マスターおよびレプリカのインストール中のみ)。

第10章 キックスタートによる IDENTITY MANAGEMENT クライアントのインストール

キックスタートの登録により、Red Hat Enterprise Linux のインストール時に新しいシステムが自動的に Identity Management ドメインに追加されます。

10.1. キックスタートによるクライアントのインストール

この手順では、キックスタートファイルを使用して Identity Management クライアントをインストールする方法を説明します。

前提条件

- キックスタートの登録前に **sshd** サービスを開始しない。クライアントを登録する前に **sshd** を開始すると、SSH キーが自動的に生成されますが、「クライアントインストール用のキックスタートファイル」 のキックスタートファイルは同じ目的でスクリプトを使用し、これが推奨される方法になります。

手順

1. Identity Management サーバー上でホストエントリーを事前作成し、エントリーの一時パスワードを設定します。

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

   キックスタートがこのパスワードを使用して、クライアントのインストール時に認証し、最初の認証試行後に無効にします。クライアントが正常にインストールされると、keytab を使用して認証が行われます。

2. 「クライアントインストール用のキックスタートファイル」 に記載されている内容でキックスタートファイルを作成します。**network** コマンドを使用して、ネットワークがキックスタートファイルで適切に設定されているようにしてください。

3. キックスタートファイルを使用して、Identity Management クライアントをインストールします。

10.2. クライアントインストール用のキックスタートファイル

ここでは、Identity Management クライアントのインストールに使用できるキックスタートファイルの内容を説明します。

インストールするパッケージ一覧に含まれる ipa-client パッケージ

キックスタートファイルの %packages セクションに、**ipa-client** パッケージを追加します。以下に例を示します。

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

Identity Management クライアントのポストインストール手順

ポストインストール手順には以下が含まれている必要があります。

- 登録前に SSH キーが確実に生成されるようにする手順
- 以下を指定して **ipa-client-install** ユーティリティーを実行する手順
  - Identity Management ドメインサービスのアクセスおよび設定に必要なすべての情報
  - 「キックスタートによるクライアントのインストール」 に従って、Identity Management サーバーにクライアントホストを事前作成する際に設定するパスワード

たとえば、ワンタイムパスワードを使用し、DNS からではなくコマンドラインから必要なオプションを取得するキックスタートインストールのポストインストール手順は次のようになります。

```
%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
```

任意で、キックスタートファイルに以下のような他のオプションを含めることもできます。

- 非対話的なインストールでは、**--unattended** オプションを **ipa-client-install** に追加します。
- クライアントのインストールスクリプトがマシンの証明書を要求できるようにするには、以下を行います。
  - **--request-cert** オプションを **ipa-client-install** に追加します。
  - キックスタートの **chroot** 環境で、**getcert** ユーティリティーおよび **ipa-client-install** ユーティリティーの両方に対して **/dev/null** にシステムバスのアドレスを設定します。これには、キックスタートファイルのポストインストール手順で **ipa-client-install** 手順の前に次の行を追加します。

    ```
    # 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. IDENTITY MANAGEMENT クライアントのテスト

コマンドラインインターフェースにより、**ipa-client-install** が正常に実行されたことが通知されますが、独自のテストを行うこともできます。

Identity Management クライアントが、サーバー上で定義されたユーザーに関する情報を取得できることをテストするには、サーバー上で定義されたユーザーを解決できることをチェックします。たとえば、デフォルトの **admin** ユーザーをチェックするには、以下を実行します。

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

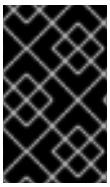
認証が適切に機能することをテストするには、root 以外のユーザーで **su** を実行し、root になります。

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

第11章 IDENTITY MANAGEMENT クライアントの再登録

クライアントのハードウェア障害などの理由で、クライアント仮想マシンが破壊され、 Identity Management (IdM) サーバーとの接続が失われた場合、キータブがあればクライアントを再登録できます。この場合、同じホスト名でクライアントを IdM 環境に戻します。

再登録の間、クライアントは新しい証明書を生成しますが、LDAP データベースのクライアントのアイデンティティーは変更されません。再登録後、ホストは、IdM サーバーとの接続を失う前と同じ **fqdn** を持つ同じ LDAP オブジェクトに、キーとその他の情報を保持します。



重要

ドメインエントリーがアクティブなクライアントのみを再登録できます。クライアントをアンインストール (**ipa-client-install --uninstall** を使用) した場合や、ホストエントリーを無効 (**ipa host-disable** を使用) にした場合は再登録できません。

クライアントの名前を変更すると、再登録することができません。これは、Identity Management では LDAP にあるクライアントのエントリーのキー属性はクライアントのホスト名 **fqdn** であるためです。クライアントの再登録中はクライアントの LDAP オブジェクトは変更されませんが、クライアントの名前を変更すると、クライアントのキーとその他の情報は新しい fqdn を持つ異なる LDAP オブジェクトに格納されます。そのため、IdM からホストをアンインストールし、ホストのホスト名を変更して、新しい名前で IdM クライアントとしてインストールするのが、クライアントの名前を変更する唯一の方法です。クライアントの名前を変更する方法は 13章*Identity Management クライアントシステムの名前変更* を参照してください。

11.1. クライアント再登録中に行われること

Identity Management は再登録中に以下を行います。

- 元のホスト証明書を破棄します。
- 新規ホストの証明書を生成します。
- 新規の SSH 鍵を作成します。
- 新規の keytab を生成します。

11.2. ユーザークレデンシャルを使用したクライアントの再登録: 対話的な再登録

この手順では、権限のあるユーザーのクレデンシャルを使用して、Identity Management クライアントを対話的に再登録する方法を説明します。

1. 同じホスト名のクライアントマシンを再作成します。
2. クライアントマシンで **ipa-client-install --force-join** コマンドを実行します。

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

3. スクリプトにより、アイデンティティーがクライアントの再登録に使用されるユーザーの入力が求められます。たとえば、登録監理者 (Enrollment Administrator) ロールを持つ **hostadmin** ユーザーなどが該当します。

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

関連資料

- 特権ユーザーのクレデンシャルを使用してクライアント再登録するための詳細手順は、「ユーザークレデンシャルを使用したクライアントのインストール: 対話的なインストール」 を参照してください。

11.3. クライアントのキータブを使用したクライアントの再登録: 非対話的な再登録

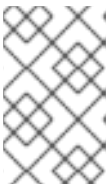
前提条件

- **/tmp** や **/root** などのディレクトリーに元のクライアントキータブファイルをバックアップします。

手順
この手順では、クライアントシステムのキータブファイルを使用して、Identity Management クライアントを非対話的に再登録する方法を説明します。たとえば、クライアントのキータブを使用した再登録は自動インストールに適しています。

1. 同じホスト名のクライアントマシンを再作成します。
2. キータブファイルをバックアップした場所から再作成したクライアントマシンの **/etc/** ディレクトリーにコピーします。
3. **ipa-client-install** ユーティリティーを使用してクライアントを再登録し、**--keytab** オプションでキータブの場所を指定します。

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



注記

登録を開始するために認証する場合は、**--keytab** オプションで指定するキータブのみが使用されます。再登録中、IdM はクライアントに対して新しいキータブを生成します。

11.4. IDENTITY MANAGEMENT クライアントのテスト

コマンドラインインターフェースにより、**ipa-client-install** が正常に実行されたことが通知されますが、独自のテストを行うこともできます。

Identity Management クライアントが、サーバー上で定義されたユーザーに関する情報を取得できることをテストするには、サーバー上で定義されたユーザーを解決できることをチェックします。たとえば、デフォルトの **admin** ユーザーをチェックするには、以下を実行します。

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

認証が適切に機能することをテストするには、root 以外のユーザーで **su** を実行し、root になります。

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

第12章 IDENTITY MANAGEMENT クライアントのアンインストール

管理者は、環境から Identity Management クライアントを削除できます。

12.1. IDENTITY MANAGEMENT クライアントのアンインストール

クライアントをアンインストールすると、クライアントは Identity Management ドメインから削除され、SSSD (System Security Services Daemon) などのシステムサービスの Identity Management 設定もすべて削除されます。これにより、クライアントシステムの以前の設定が復元します。

手順

1. **ipa-client-install --uninstall** コマンドを実行します。

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

2. クライアントの DNS エントリーを、手動でサーバーから削除します。

```
# 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"
```

第13章 IDENTITY MANAGEMENT クライアントシステムの名前変更

ここでは、Identity Management クライアントシステムのホスト名を変更する方法を説明します。

警告

クライアントの名前は手動で変更します。ホスト名の変更が絶対に必要である場合のみ実行してください。

Identity Management クライアントの名前を変更するには、以下を行う必要があります。

1. ホストを準備します。詳細は 「前提条件」 を参照してください。
2. ホストから IdM クライアントをアンインストールします。詳細は 「Identity Management クライアントのアンインストール」 を参照してください。
3. ホストの名前を変更します。詳細は 「ホストシステムの名前変更」 を参照してください。
4. 新しい名前でホストに IdM クライアントをインストールします。詳細は 「Identity Management クライアントの再インストール」 を参照してください。
5. IdM クライアントのインストール後にホストを設定します。詳細は「サービスの再追加、証明書の再生成、およびホストグループの再追加」 を参照してください。

13.1. 前提条件

現在のクライアントをアンインストールする前に、クライアントの設定をメモします。新しいホスト名のマシンを再登録した後にこの設定を適用します

- マシンで実行されているサービスを特定します。
  - **ipa service-find** コマンドを使用して、証明書のあるサービスを特定して出力します。

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

  - さらに、各ホストには **ipa service-find** の出力に表示されないデフォルトの **host service** があります。ホストサービスのサービスプリンシパルは **ホストプリンシパル** とも呼ばれ、**host/old-client-name.example.com** になります。
- **ipa service-find old-client-name.example.com** により表示されるすべてのサービスプリンシパルは、**old-client-name.example.com** 上の対応するキータブの場所を決定します。

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

  クライアントシステムの各サービスには、**ldap/old-client-name.example.com@EXAMPLE.COM** のように service_name/host_name@REALM の形式を取る Kerberos プリンシパルがあります。

- マシンが所属するすべてのホストグループを特定します。

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

13.2. IDENTITY MANAGEMENT クライアントのアンインストール

クライアントをアンインストールすると、クライアントは Identity Management ドメインから削除され、SSSD (System Security Services Daemon) などのシステムサービスの Identity Management 設定もすべて削除されます。これにより、クライアントシステムの以前の設定が復元します。

手順

1. **ipa-client-install --uninstall** コマンドを実行します。

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

2. クライアントの DNS エントリーを、手動でサーバーから削除します。

```
# 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"
```

13.3. ホストシステムの名前変更

必要に応じてマシンの名前を変更します。以下に例を示します。

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

これで、新しいホスト名で、Identity Management クライアントを Identity Management ドメインに再インストールできるようになります。

13.4. IDENTITY MANAGEMENT クライアントの再インストール

9章*Identity Management クライアントのインストール: 基本的なシナリオ* の手順に従って、名前を変更したホストにクライアントをインストールします。

13.5. サービスの再追加、証明書の再生成、およびホストグループの再追加

1. Identity Management サーバーで、「前提条件」 に定義された各サービスに新しいキータブを追加します。

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

2. 「前提条件」 で割り当てた証明書のあるサービスに対して証明書を生成します。これには、以下を行います。

   - Identity Management の管理ツールを使用します。

- **certmonger** ユーティリティーを使用します。

3. 「前提条件」 で特定されたホストグループにクライアントを再追加します。

第14章 IDENTITY MANAGEMENT レプリカをインストールするためのシステムの準備

ここでは、Identity Management レプリカのインストール要件を取り上げます。インストールを行う前に、システムがこれらの要件を満たしていることを確認してください。

レプリカをインストールするシステムが、サーバーの一般的な要件を満たしている必要があります。

- 1章*Identity Management サーバーをインストールするためのシステムの準備*

レプリカ固有のその他の要件は、以下を参照してください。

- 「レプリカバージョンの要件」

14.1. レプリカバージョンの要件

Red Hat Enterprise Linux (RHEL) 8 レプリカは、RHEL 7.4 以上で実行している IdM マスターとのみ機能します。RHEL 8 で実行している IdM レプリカを既存のデプロイメントに導入する前に、すべての IdM サーバーを RHEL 7.4 以上にアップグレードし、ドメインレベルを 1 に変更します。

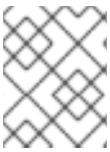
さらに、レプリカが、同じまたはそれ以降のバージョンの Identity Management を実行している必要があります。以下に例を示します。

- マスターサーバーが Red Hat Enterprise Linux 8 にインストールされ、Identity Management 4.x パッケージを使用する。
- このとき、レプリカが Red Hat Enterprise Linux 8 以上にインストールされ、バージョン 4.x 以上の Identity Management を使用する必要もあります。

これにより、設定が適切にサーバーからレプリカにコピーされます。

第15章 IDENTITY MANAGEMENT レプリカのインストール

ここでは、既存のサーバーを基にして Identity Management レプリカをインストールする方法を説明します。レプリカのインストールプロセスでは、既存のサーバーの設定をコピーし、その設定をベースにレプリカをインストールします。



注記

Identity Management レプリカは一度に 1 つずつインストールしてください。同時に複数のレプリカをインストールすることはサポートされません。

レプリカをインストールする前に、ターゲットシステムが Identity Management ドメインでの登録に対して承認されている必要があります。以下を参照してください。

- 「Identity Management クライアントにレプリカをインストールするための前提条件」
- 「Identity Management ドメイン外部のシステムにレプリカをインストールするための前提条件」

レプリカのインストール手順は、以下を参照してください。

- 「統合 DNS のある Identity Management レプリカのインストール」
- 「CA のある Identity Management レプリカのインストール」

インストール後は、以下を参照してください。

- 「Identity Management レプリカのテスト」

15.1. IDENTITY MANAGEMENT クライアントにレプリカをインストールするための前提条件

既存のクライアントにレプリカをインストールする場合は、以下の認可方法のいずれかを選択してください。

特権ユーザーのクレデンシャル

特権ユーザーのクレデンシャルを提供してレプリカのインストールを承認する場合は、この方法を選択してください。

- 特権ユーザーとしてログインしてから **ipa-replica-install** ユーティリティーを実行します。デフォルトの特権ユーザーは **admin** です。

  ```
  $ kinit admin
  ```

- Identity Management により、対話的にクレデンシャルが要求されます。これはデフォルトの動作です。

ipaservers ホストグループ

クライアントを **ipaservers** ホストグループに追加して、レプリカのインストールを承認する場合は、この方法を選択します。**ipaservers** のメンバーシップは、マシンの権限を管理者のクレデンシャルと同様の権限に昇格します。
クライアントを **ipaservers** のメンバーとして追加します。

-

```
$ 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. IDENTITY MANAGEMENT ドメイン外部のシステムにレプリカをインストールするための前提条件

Identity Management ドメインに登録されていないシステムで **ipa-replica-install** ユーティリティーを実行する場合、**ipa-replica-install** は最初にシステムをクライアントとして登録してから、レプリカコンポーネントをインストールします。

アイデンティティー管理ドメインの外部にあるシステムにレプリカをインストールする場合は、以下の認可方法のいずれかを選択します。

特権ユーザーのクレデンシャル

この方法では、特権ユーザーのクレデンシャルを提供して、レプリカのインストールが承認されます。デフォルトの特権ユーザーは **admin** です。
この方法を使用するには、インストール中にプリンシパル名とパスワードのオプション (**--principal admin --admin-password password**) を **ipa-replica-install** に直接追加します。

Identity Management サーバーで生成される無作為なパスワード

この方法では、一度限りの登録に無作為なパスワードを提供して、レプリカのインストールが承認されます。
レプリカのランダムパスワードを生成し、レプリカシステムを **ipaservers** ホストグループに追加するには、ドメインのいずれかのサーバーで以下のコマンドを実行します。

1. 管理者としてログインします。

```
$ kinit admin
```

2. 新しいマシンを IdM ホストとして追加します。**ipa host-add** コマンドに **--random** オプションを使用して、レプリカのインストールに使用される無作為なワンタイムパスワードを生成します。

```
$ 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
```

生成パスワードは、IdM ドメインへのマシン登録に使用した後は無効になります。登録が完了すると正しいホストの keytab に置き換えられます。

3. マシンを **ipaservers** のホストグループに追加します。

```
$ 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
-------------------------
```

ipaservers のメンバーは、必須サーバーサービスの設定に必要な特権にマシンを昇格します。

15.3. 統合 DNS のある IDENTITY MANAGEMENT レプリカのインストール

この手順は、以下に該当するレプリカのインストール方法を説明します。

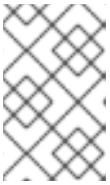
- 統合 DNS あり。
- Identity Management (IdM) 環境にはすでに認証局 CA がインストールされていて、レプリカには CA を導入しない。レプリカは、すべての証明書操作を、CA がインストールされている Identity Management IdM サーバーに転送します。

手順

1. 以下のオプションを使用して、**ipa-replica-install** を実行します。
   - **--setup-dns** - レプリカを DNS サーバーとして設定します。
   - **--forwarder** - フォワーダーを指定します。**--no-forwarder** フォワーダーを使用しない場合に指定します。フェイルオーバーのために複数のフォワーダーを指定するには、**--forwarder** を複数回使用します。

   たとえば、IdM サーバーにより管理されないすべてのリクエストを、 IP アドレス 192.0.2.1 で実行している DNS サーバーに転送する、統合 DNS サーバーを持つレプリカを設定するには、以下を実行します。

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



注記

ipa-replica-install ユーティリティーは、**--no-reverse** や **--no-host-dns** などの DNS 設定に関する複数のオプションを受け入れます。詳細は、man ページの **ipa-replica-install**(1) を参照してください。

15.4. CA のある IDENTITY MANAGEMENT レプリカのインストール

この手順は、以下に該当するレプリカのインストール方法を説明します。

- 統合 DNS のないサーバー

- 認証局 (CA) あり

重要

CA のあるレプリカを設定する場合は、レプリカの CA 設定がマスターサーバーの CA 設定を反映する必要があります。

たとえば、サーバーに統合された Identitiy Mananagement CA がルート CA として含まれている場合、レプリカも統合 CA をルート CA としてインストールする必要があります。この場合、他の CA 設定は使用できません。

ipa-replica-install コマンドに **--setup-ca** オプションを使用すると、初期サーバーの CA 設定がコピーされます。

手順

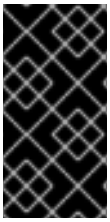
1. **--setup-ca** オプションを指定して **ipa-replica-install** を実行します。

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

15.5. CA のある IDENTITY MANAGEMENT レプリカのインストール

この手順は、以下に該当するレプリカのインストール方法を説明します。

- 統合 DNS のないサーバー
- 必要な証明書を手動で用意し、認証局 (CA) なし。マスターサーバーも CA なしでインストールされたことを前提とします。



重要

インポートした証明書ファイルには、LDAP サーバーおよび Apache サーバーの証明書を発行した CA の完全な証明書チェーンが含まれている必要があるため、自己署名のサードパーティーサーバー証明書を使用してサーバーまたはレプリカをインストールすることはできません。

手順

- **ipa-replica-install** を実行して、以下のオプションを追加して必要な証明書ファイルを指定します。
  - **--dirsrv-cert-file**
  - **--dirsrv-pin**
  - **--http-cert-file**
  - **--http-pin**

  これらのオプションを使用して提供されるファイルに関する詳細は、「CA なしで Identity Management サーバーをインストールするために必要な証明書」 を参照してください。

  以下に例を示します。

```
# 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
```

注記

--ca-cert-file オプションを追加しないでください。**ipa-replica-install** ユーティリティーは、マスターサーバーから証明書のこの部分の情報を自動的に取得します。

15.6. IDENTITY MANAGEMENT レプリカのテスト

レプリカの作成後、レプリカが想定どおりにデータを複製するか確認します。以下の手順を使用できます。

手順

1. 新しいレプリカでユーザーを作成します。

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

2. ユーザーが他のレプリカでも表示されるようにします。

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

15.7. IDENTITY MANAGEMENT レプリカのインストール中に実行される接続

表15.1「Identity Management レプリカのインストール中に実行されるリクエスト」 には、Identity Management (IdM) のレプリカインストールツール **ipa-replica-install** により実行される操作の一覧が記載されています。

表15.1 Identity Management レプリカのインストール中に実行されるリクエスト

操作	使用プロトコル	目的
クライアントシステムに設定した DNS リゾルバーに対する DNS レゾリューション	DNS	IdM マスターの IP アドレスの検出。
検出された IdM マスターのポート 88 (TCP/TCP6 および UDP/UDP6) へのリクエスト	Kerberos	Kerberos チケットの取得。
検出または設定された IdM マスター上の IdM Apache ベースの Web サービスへの JSON-RPC 呼び出し。	HTTPS	IdM クライアントの登録。必要な場合はレプリカキーの取得および証明書の発行。

操作	使用プロトコル	目的
SASL GSSAPI 認証、プレーン LDAP、またはこれら両方を使用した、IdM サーバー上のポート 389 (TCP/TCP6) へのリクエスト	LDAP	IdM クライアントの登録。CA 証明書チェーンの取得。LDAP データの複製。
IdM サーバー上のポート 22 (TCP/TCP6) へのリクエスト	SSH	接続が機能していることを確認。
(任意) IdM マスターのポート 8443 (TCP/TCP6) でのアクセス	HTTPS	IdM マスター上での認証局の管理 (IdM マスターおよびレプリカのインストール中のみ)。

第16章 IDENTITY MANAGEMENT レプリカのアンインストール

管理者は、トポロジーから Identity Management サーバーを削除できます。

この手順では、**server.idm.example.com** という名前のサンプルサーバーをアンインストールする方法を説明します。

前提条件

- 認証局 (CA)、鍵回復機関 (KRA)、または DNS サーバーとして機能するサーバーをアンインストールする前に、これらのサービスがドメインの別のサーバーで実行していることを確認している。

警告

CA、KRA、または DNS サーバーとして機能する唯一のサーバーを削除すると、Identity Management 機能に深刻な不具合が生じます。

手順

1. トポロジーにあり、**server.idm.example.com** とのレプリケーションアグリーメントを持つすべてのサーバーで **ipa server-del** コマンドを使用し、トポロジーからレプリカを削除します。

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

2. **server.idm.example.com** で、**ipa-server-install --uninstall** コマンドを使用します。

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

3. **server.idm.example.com** を参照するすべてのネームサーバー (NS) の DNS レコードが DNS ゾーンから削除されていることを確認します。使用する DNS が Identity Management により管理される統合 DNS であるか、または外部 DNS であるかに関わらず、確認を行なってください。

パート II. RHEL 7 から RHEL 8 へ IDM を移行し、最新に維持

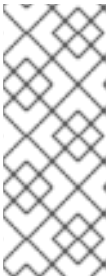
第17章 RED HAT ENTERPRISE LINUX 7 から 8 への IDENTITY MANAGEMENT の移行

この手順では、Identity Management のデータと設定を Red Hat Enterprise Linux (RHEL) 7 サーバーから RHEL 8 サーバーへ移行する方法を説明します。移行手順には、以下が含まれます。

1. Identity Management サーバーを RHEL 8 システムにインストールする。詳細は「RHEL 8 レプリカのインストール」を参照してください。
2. RHEL 8 サーバーを CA 更新マスターにする。詳細は「CA 更新マスターの RHEL 8 への移動」を参照してください。
3. RHEL 7 サーバーで証明書失効リスト (CRL) の生成を停止し、CRL 要求を RHEL 8 にリダイレクトする。詳細は「RHEL 7 での CRL 生成を停止し、CRL 要求を RHEL 8 へリダイレクト」 を参照してください。
4. RHEL 8 サーバーで証明書失効リスト (CRL) の生成を開始する。詳細は「RHEL 8 で CRL 生成の開始」を参照してください。
5. 元の RHEL 7 CA マスターを停止して使用を中止する。詳細は「RHEL 7 サーバーの停止および使用停止」を参照してください。

手順では、以下を前提としています。

- **rhel8.example.com** は、新しい CA マスターとなる RHEL 8 システムです。
- **rhel7.example.com** は、元の RHEL 7 CA マスターです。



注記

マスター CA サーバーである Red Hat Enterprise Linux 7 サーバーを特定するには、任意の IdM サーバーでこのコマンドを実行します。

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

17.1. RHEL 7 から 8 への IDENTITY MANAGEMENT の移行の前提条件

rhel7.example.com:

1. システムを最新の RHEL 7 バージョンへアップグレードしている。
2. **ipa-*** パッケージを最新バージョンへ更新している。

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

警告

複数の Identity Management サーバーをアップグレードする場合は、各アップグレードで少なくとも 10 分の間隔を空けてください。

複数のサーバーで同時または間隔をあまりあけないでアップグレードを行うと、トポロジー全体でアップグレード後のデータ変更を複製する時間が足りず、複製イベントが競合する可能性があります。

rhel8.example.com:

1. **rhel8.example.com** システムが、*1章Identity Management サーバーをインストールするためのシステムの準備* にある要件を満たしている。
2. レプリカが、IdM DNS サーバーが権限を持つ信頼できるドメインに含まれている。
3. **ipa-*** パッケージを最新バージョンへ更新している。

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

関連情報

- **yum** ユーティリティーの使用方法は、man ページの **yum(8)** を参照してください。

17.2. RHEL 8 レプリカのインストール

1. RHEL 7 環境に存在するサーバーの一覧を表示します。

```
[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. IdM RHEL 7 サーバーのレプリカとして **rhel8.example.com** に IdM サーバーをインストールし、**rhel7.example.com** のサーバーロールをすべて含みます。上記の例からすべてのロールをインストールするには、**ipa-replica-install** コマンドでこのオプションを使用します。

   - Certificate System コンポーネントを設定する **--setup-ca**

   - 統合 DNS サーバーを設定し、IdM ドメインの外に出る DNS クエリーを処理するようにフォワーダーを設定する **--setup-dns** および **--forwarder**
   IP アドレスが 192.0.2.20 のフォワーダーを使用する、IP アドレスが 192.0.2.1 の IdM サーバーを設定するには、以下のコマンドを設定します。

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

   DNS が正常に機能している場合は、**rhel8.example.com** が DNS の自動検出を使用してそれを見つけるため、RHEL 7 IdM サーバーを指定する必要はありません。

3. インストールが完了したら、Identity Management サービスが **rhel8.example.com** で稼働していることを確認します。

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

4. **rhel7.example.com** および **rhel8.example.com** の CA がいずれもマスターサーバーとして設定されていることを確認します。

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

5. 必要に応じて、**rhel7.example.com** と **rhel8.example.com** との間でレプリカ合意の詳細を表示するには、次のコマンドを実行します。

   ```
   [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. CA 更新マスターの RHEL 8 への移動

rhel8.example.com で、新しい CA 更新マスターとして **rhel8.example.com** を設定します。

- CA サブシステム証明書の更新を処理するように **rhel8.example.com** を設定します。

  ```
  [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
```

出力で更新が成功したことを確認します。

17.4. RHEL 7 での CRL 生成を停止し、CRL 要求を RHEL 8 へリダイレクト

rhel7.example.com CA マスターで Certificate Revocation List (CRL) の生成を停止し、**rhel7.example.com** で、CRL 要求を新しいマスター **rhel8.example.com** にリダイレクトするように Apache を設定します。

1. CA サービスを停止します。

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

2. **rhel7.example.com** で CRL 生成を無効にします。**/etc/pki/pki-tomcat/ca/CS.cfg** ファイルを編集し、**ca.crl.MasterCRL.enableCRLCache** パラメーターおよび **ca.crl.MasterCRL.enableCRLUpdates** パラメーターの値を **false** に設定します。

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

3. CA サービスを起動します。

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

4. 新しいマスターに CRL 要求をリダイレクトするように Apache を設定します。**/etc/httpd/conf.d/ipa-pki-proxy.conf** ファイルを開いて、**RewriteRule** 引数のコメントを解除し、サーバー URL のサーバーホスト名を、**rhel8.example.com** ホスト名に置き換えます。

```
# 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. Apache を再起動します。

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

17.5. RHEL 8 で CRL 生成の開始

rhel8.example.com を設定して、証明書失効リスト (CRL) を生成します。

1. CA サービスを停止します。

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

2. このサーバーで CRL 生成を有効にします。**/etc/pki/pki-tomcat/ca/CS.cfg** ファイルの **ca.crl.MasterCRL.enableCRLCache** パラメーターおよび **ca.crl.MasterCRL.enableCRLUpdates** パラメーターの値を **true** に設定します。

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

3. CA サービスを起動します。

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

4. Apache で、CRL 要求のリダイレクトを無効にします。**/etc/httpd/conf.d/ipa-pki-proxy.conf** ファイルを開いて、**RewriteRule** 引数をコメントアウトします。

```
# 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]
```

この手順の前までは、CRL 要求はすべて以前の CA マスターにルーティングされていましたが、これで、このサーバーは CRL 要求に応答します。

5. Apache を再起動します。

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

17.6. RHEL 7 サーバーの停止および使用停止

1. 最新のデータも含むすべてのデータが、**rhel7.example.com** から **rhel8.example.com** に正しく移行されていることを確認してください。以下に例を示します。

   a. **rhel7.example.com** に新しいユーザーを追加します。

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

   b. ユーザーが **rhel8.example.com** に複製されていることを確認します。

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

2. **rhel7.example.com** 上の全サービスを停止して、新しい **rhel8.example.com** サーバーへのドメイン検索を実施します。

```
[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  ]
```

この後に、**ipa** ユーティリティーを使用すると、Remote Procedure Call (RPC) で新規サーバーに接続します。

3. RHEL 8 サーバーで削除コマンドを実行して、トポロジーから RHEL 7 サーバーを削除します。詳細は6章*Identity Management サーバーのアンインストール*を参照してください。

第18章 IDENTITY MANAGEMENT の更新およびダウンロード

yum ユーティリティーを使用して、システムの Identity Management (IdM) パッケージを更新できます。プロファイルに関連し、利用可能な更新がある IdM パッケージをすべて更新するには、次のコマンドを実行します。

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

または、次のコマンドを実行します。

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

有効になっているリポジトリーから、プロファイルで利用可能な最新バージョンに合わせて、パッケージをインストールまたは更新します。

少なくとも 1 台のサーバーで IdM パッケージをアップデートすると、トポロジー内のその他のすべてのサーバーでパッケージを更新しなくても、更新されたスキーマを受け取ります。これは、新しいスキーマを使用する新しいエントリーを、その他のサーバー間で確実に複製できます。

警告

複数の IdM サーバーを更新する場合は、サーバーを更新してから別のサーバーを更新するまで、10 分以上お待ちください。ただし。サーバーの更新が成功するまでに必要な時間は、展開されたトポロジー、接続のレイテンシー、更新で生成した変更の数により異なります。

複数のサーバーで、同時、またはあまり間隔を開けずに更新を行うと、トポロジー全体でアップグレード後のデータ変更を複製する時間が足りず、複製イベントが競合する可能性があります。

IdM パッケージを手動でダウンロードすることはサポートされていません。**yum distro-sync** を使用して、モジュールのパッケージを更新およびダウンロードします。

重要

ipa-* パッケージで **yum downgrade** コマンドを実行しないでください。

関連情報

- **yum** ユーティリティーの使用方法は、man ページの **yum(8)** を参照してください。