Red Hat Enterprise Linux 8

Identity Management のインストール

IdM サーバーとクライアントのインストール方法

Last Updated: 2024-06-26

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

IdM サーバーとクライアントのインストール方法

法律上の通知

概要

環境に応じて、Red Hat Identity Management (IdM) をインストールして DNS および認証局 (CA) サービスを提供することも、既存の DNS および CA インフラストラクチャーを使用するように IdM を設定することもできます。 IdM サーバー、レプリカ、およびクライアントを手動で、または Ansible Playbook を使用してインストールできます。さらに、キックスタートファイルを使用して、システムのインストール中にクライアントを IdM ドメインに自動的に参加させることができます。

目次

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **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追加してください。
5. ダイアログの下部にある **Create** をクリックします。

第1章 このガイドの使い方

Identity Management (IdM) ドメインには、レプリカとも呼ばれる IdM サーバーと IdM クライアントが含まれます。IdM デプロイメントの インストールは常にプライマリー IdM サーバーのインストールから始まりますが、次のインストール手順の順序は対象のトポロジーによって異なります。たとえば、IdM クライアントをインストールする前または後に IdM レプリカをインストールできます。さらに、特定の IdM デプロイメントでは Active Directory との信頼 が必要ですが、そうでないものもあります。

関連情報

- Identity Management の計画

パート I. IDENTITY MANAGEMENT のインストール

第2章 IDM 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 Managementt (IdM) サーバーのインストール要件を取り上げます。インストールの前に、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。

2.1. 前提条件

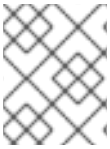
- ホストコンピューターに Identity Management (IdM) サーバーをインストールするには、**root** 特権が必要です。

2.2. 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 4 GB の RAM と 4 GB のスワップ領域を割り当てます。
- 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 のスワップ領域を割り当てます。

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。通常、メモリーを増やすと、キャッシュ機能により、サイズが大きいデプロイメントでパフォーマンスが改善されます。



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。

2.3. IDM 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行わずに、クリーンなシステムに Identity Managementt (IdM) をインストールします。

IdM 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、IdM ドメインを設定します。IdM 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。

IdM における IPv6 要件

IdM システムでは、カーネルで IPv6 プロトコルが有効になっている必要があり、localhost (::1) はそれを使用できます。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。必要に応じて、IPv6 アドレスを有効にせずに IPv6 スタックを有効にすることができます。

IdM における暗号化タイプのサポート

Red Hat Enterprise Linux (RHEL) は、Advanced Encryption Standard (AES)、Camel、Data Encryption Standard (DES) などの暗号化タイプをサポートする Kerberos プロトコルのバージョン 5 を使用します。

サポート対象の暗号化タイプのリスト

IdM サーバーおよびクライアントの Kerberos ライブラリーは、より多くの暗号化タイプに対応している可能性がありますが、IdM Kerberos Distribution Center (KDC) は以下の暗号化タイプのみに対応します。

- **aes256-cts:normal**
- **aes256-cts:special** (デフォルト)
- **aes128-cts:normal**
- **aes128-cts:special** (デフォルト)
- **aes128-sha2:normal**
- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**
- **camellia128-cts-cmac:normal**
- **camellia128-cts-cmac:special**
- **camellia256-cts-cmac:normal**
- **camellia256-cts-cmac:special**

RC4 暗号化タイプがデフォルトで無効

以下の RC4 暗号化は、新しい暗号化タイプ AES-128 および AES-256 よりも安全ではないと見なされるため、RHEL 8 では非推奨となり、デフォルトで無効にされています。

- **arcfour-hmac:normal**
- **arcfour-hmac:special**

以前の Active Directory 環境と互換性を確保するために RC4 サポートを手動で有効にする方法は、AD および RHEL で一般的な暗号化タイプに対応 を参照してください。

DES および 3DES 暗号化のサポートが削除される

セキュリティー上の理由から、DES アルゴリズムへの対応は RHEL 7 では非推奨となりました。RHEL 8.3.0 で最近、Kerberos パッケージがリベースされ、RHEL 8 からシングル DES (DES) およびトリプル DES (3DES) 暗号化タイプのサポートが削除されました。

注記

標準の RHEL 8 IdM インストールでは、DES または 3DES 暗号化タイプはデフォルトでは使用されず、Kerberos のアップグレードによる影響はありません。

DES や 3DES 暗号化 **のみ** を使用するようにサービスまたはユーザーを手動で設定すると (レガシークライアントなど)、最新の Kerberos パッケージに更新した後にサービスが中断される可能性があります。

- Kerberos 認証エラー
- **unknown enctype** 暗号化エラー
- DES で暗号化されたデータベースマスターキー (**K/M**) を使用する KDC が起動に失敗する

Red Hat では、お使いの環境で DES または 3DES 暗号化を使用しないことを推奨します。

注記

DES および 3DES 暗号化タイプは、ご利用環境で使用するように設定している場合に限り無効にする必要があります。

IdM でのシステム全体の暗号化ポリシーへの対応

IdM は、**DEFAULT** システム全体の暗号化ポリシーを使用します。このポリシーは、現在の脅威モデルに安全な設定を提供します。TLS プロトコルの 1.2 と 1.3、IKEv2 プロトコル、および SSH2 プロトコルが使用できます。RSA 鍵と Diffie-Hellman パラメーターは長さが 2048 ビット以上であれば許容されます。このポリシーでは、DES、3DES、RC4、DSA、TLS v1.0、およびその他の弱いアルゴリズムを使用できません。

注記

FUTURE システム全体の暗号化ポリシーの使用中は、IdM サーバーをインストールできません。IdM サーバーをインストールする場合は、**DEFAULT** システム全体の暗号化ポリシーを使用していることを確認してください。

関連情報

- システム全体の暗号化ポリシー
- man IPV6(7)

2.4. FIPS コンプライアンス

RHEL 8.3.0 以降では、連邦情報処理規格 (FIPS) 140 モードが有効になっているシステムに、新しい IdM サーバーまたはレプリカをインストールできます。

IdM を FIPS モードでインストールするには、まずホストで FIPS モードを有効にしてから、IdM をインストールします。IdM インストールスクリプトは、FIPS が有効かどうかを検出し、IdM が FIPS 140 標準に準拠する暗号化タイプのみを使用するように設定します。

- **aes256-cts:normal**
- **aes256-cts:special**
- **aes128-cts:normal**
- **aes128-cts:special**
- **aes128-sha2:normal**

- **aes128-sha2:special**
- **aes256-sha2:normal**
- **aes256-sha2:special**

IdM 環境が FIPS に準拠するには、**すべて** の IdM レプリカで FIPS モードが有効になっている必要があります。

特にクライアントを IdM レプリカにプロモートする場合、Red Hat では IdM クライアントでも FIPS モードを有効にすることを推奨します。最終的には、管理者が FIPS 要件を満たす方法を判別する必要があります。Red Hat は FIPS 基準を強要しません。

FIPS 準拠の IdM への移行
既存の IdM インストールを非 FIPS 環境から FIPS 準拠のインストールに移行することはできません。これは技術的な問題ではなく、法的および規制上の制限です。

FIPS 準拠のシステムを運用するには、すべての暗号化キー素材を FIPS モードで作成する必要があります。さらに、暗号鍵マテリアルは、安全にラップされ、非 FIPS 環境でラップ解除されない限り、FIPS 環境から決して出てはなりません。

シナリオで FIPS 非準拠の IdM レルムから FIPS 準拠の IdM レルムへの移行が必要な場合は、次のことを行う必要があります。

1. FIPS モードで新しい IdM レルムを作成します。
2. すべてのキーマテリアルをブロックするフィルターを使用して、非 FIPS レルムから新しい FIPS モードレルムへのデータ移行を実行します。

移行フィルターは以下をブロックする必要があります。

- KDC マスターキー、キータブ、および関連するすべての Kerberos キーマテリアル
- ユーザーパスワード
- CA、サービス、ユーザー証明書を含むすべての証明書
- OTP トークン
- SSH キーと指紋
- DNSSEC KSK および ZSK
- すべての Vault エントリー
- AD 信頼関連のキーマテリアル

事実上、新しい FIPS インストールは別のインストールとなります。厳密なフィルタリングを行ったとしても、このような移行は FIPS 140 認定を通過できない可能性があります。FIPS 監査人がこの移行にフラグを立てる場合があります。

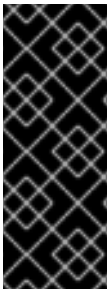
関連情報

- RHEL オペレーティングシステムでの FIPS 140 実装の詳細は、**RHEL セキュリティー強化** ドキュメントの 連邦情報処理標準 140 と FIPS モードを 参照してください。

2.5. FIPS モードが有効なフォレスト間の信頼のサポート

FIPS モードが有効な場合に Active Directory (AD) ドメインでフォレスト間の信頼を確立するには、以下の要件を満たす必要があります。

- RHEL 8.4.0 以降の IdM サーバーを使用する。
- 信頼の設定時に、AD 管理アカウントで認証する必要がある。FIPS モードが有効な場合には、共有シークレットを使用して信頼を確立することはできません。



重要

RADIUS 認証は FIPS に準拠していません。RADIUS プロトコルは MD5 ハッシュ機能を使用してクライアントとサーバー間のパスワードを暗号化し、FIPS モードでは、OpenSSL は MD5 ダイジェストアルゴリズムの使用を無効にするためです。ただし、RADIUS サーバーが IdM サーバーと同じホストで実行されている場合は、How to configure FreeRADIUS authentication in FIPS mode で説明されている手順を実行して、問題を回避して MD5 を有効にすることができます。

関連情報

- RHEL オペレーティングシステムの FIPS モードの詳細については、**セキュリティー強化** ドキュメントの FIPS モードでのシステムのインストール を参照してください。
- FIPS 140-2 標準の詳細については、米国標準技術研究所 (NIST) Web サイトの Security Requirements for Cryptographic Modules を参照してください。

2.6. IDM のタイムサービス要件

以下のセクションでは、**chronyd** を使用して、IdM ホストを中央タイムソースと同期させる方法を説明します。

2.6.1. IdM で chronyd を同期に使用する方法

chronyd を使用して、ここで説明するように、IdM ホストを中央タイムソースと同期させることができます。

IdM の基礎となる認証メカニズムである Kerberos は、プロトコルの一部としてタイムスタンプを使用します。IdM クライアントのシステム時間が、KDC (Key Distribution Center) のシステム時間と比べて 5 分以上ずれると、Kerberos 認証に失敗します。

IdM インストールスクリプトは、IdM サーバーおよびクライアントが中央タイムソースと同期したままになるように、**chronyd** Network Time Protocol (NTP) クライアントソフトウェアを自動設定します。

IdM インストールコマンドに NTP オプションを指定しないと、インストーラーは、ネットワークの NTP サーバーを参照する **_ntp._udp** DNS サービス (SRV) レコードを検索し、その IP アドレスで **chrony** を設定します。**_ntp._udp** SRV レコードがない場合は、**chronyd** は **chrony** パッケージに同梱の設定を使用します。

注記

RHEL 8 では **chronyd** が優先されるため、**ntpd** は非推奨となっており、IdM サーバーは Network Time Protocol (NTP) サーバーとして設定されず、NTP クライアントとしてのみ設定されます。RHEL 7 の **NTP サーバー** の IdM サーバーロールも、RHEL 8 では非推奨になりました。

関連情報

- NTP の実装
- Chrony スイートを使用した NTP の設定

2.6.2. IdM インストールコマンドの NTP 設定オプションのリスト

chronyd を使用して、IdM ホストを中央タイムソースと同期させることができます。

IdM インストールコマンド (**ipa-server-install**、**ipa-replica-install**、**ipa-client-install**) のいずれかを指定して、設定時に **chronyd** クライアントソフトウェアを設定できます。

表2.1 IdM インストールコマンドの NTP 設定オプションのリスト

オプション	動作
--ntp-server	これを使用して NTP サーバーを 1 つ指定します。複数回使用して、複数のサーバーを指定できます。
--ntp-pool	複数の NTP サーバーのプールを指定して、1 つのホスト名として解決する場合には、これを使用します。
-N, --no-ntp	**chronyd** の設定、起動、有効化はしないでください。

関連情報

- NTP の実装
- Chrony スイートを使用した NTP の設定

2.6.3. IdM が NTP タイムサーバーを参照できるようにする方法

この手順では、Network Time Protocol (NTP) タイムサーバーとの同期できるように、IdM で必要とされる設定があるかどうかを確認します。

前提条件

- お使いの環境で NTP タイムサーバーを設定している。この例では、以前に設定したタイムサーバーのホスト名は **ntpserver.example.com** である。

手順

1. 環境内で NTP サーバーの DNS サービス (SRV) レコード検索を実行します。

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

2. 以前の **dig** 検索でタイムサーバーが返されない場合は、ポート **123** でタイムサーバーを参照する **_ntp._udp** SRV レコードを追加します。このプロセスは、お使いの DNS ソリューションにより異なります。

検証手順

- **_ntp._udp** SRV レコードの検索時に、DNS がポート **123** でタイムサーバーのエントリーが返されることを確認します。

```
[user@server ~]$ dig +short -t SRV _ntp._udp.example.com
0 100 123 ntpserver.example.com.
```

関連情報

- NTP の実装
- Chrony スイートを使用した NTP の設定

2.6.4. 関連情報

- NTP の実装
- Chrony スイートを使用した NTP の設定

2.7. IDM のホスト名および DNS 要件

サーバーおよびレプリカシステムのホスト名と DNS 要件を以下に示します。また、システムが要件を満たしていることを確認する方法も説明します。

これらの要件は、統合 DNS のある Identity Management (IdM) サーバーおよび統合 DNS のないすべての Identity Management (IdM) サーバーに適用されます。

警告

DNS レコードは、稼働中の LDAP ディレクトリーサービス、Kerberos、Active Directory 統合など、ほぼすべての IdM 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。
- サービスが適切に設定されている。

この要件は、統合 DNS の **有無に関わらず**、IdM 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、完全修飾ドメイン名 (例: **server.idm.example.com**) である必要があります。

重要

.company など、単一ラベルのドメイン名を使用しないでください。IdM ドメインは、トップレベルドメインと、1 つ以上のサブドメイン (**example.com** や **company.example.com** など) で設定する必要があります。

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、アルファベット文字、およびハイフン (-) のみが使用される有効な DNS 名である。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。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。**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** 以外である必要があります。

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。
   a. **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** となります。

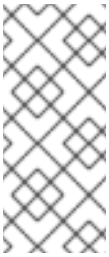
```
[root@server ~]# ip addr show
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP group default qlen 1000
 link/ether 00:1a:4a:10:4e:33 brd ff:ff:ff:ff:ff:ff
 inet 192.0.2.1/24 brd 192.0.2.255 scope global dynamic eth0
  valid_lft 106694sec preferred_lft 106694sec
 inet6 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
...
```

2. **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.idm.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.idm.example.com A
192.0.2.1
```

b. **dig +short server.idm.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.idm.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。

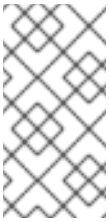
3. 逆引き DNS 設定 (PTR レコード) を確認します。**dig** ユーティリティーを使用し、IP アドレスを追加します。
以下のコマンドで別のホスト名が表示されたり、ホスト名が表示されない場合、逆引き DNS 設定は正しくありません。

a. **dig +short -x IPv4_address** コマンドを実行します。出力には、サーバーホスト名が表示されるはずです。以下に例を示します。

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

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

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



注記

前の手順で **dig +short server.idm.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。

警告

逆引き DNS (PTR レコード) の検索が複数のホスト名を返すと、**httpd**、および IdM に関連付けられた他のソフトウェアで予期しない動作が表示される場合があります。Red Hat は、1 つの IP につき 1 つの PTR レコードを設定することを強く推奨します。

DNS フォワーダーの規格準拠の確認 (統合 DNS の場合のみ必要)

IdM 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) の規格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、次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。

- ステータス - **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 に対応し、ともに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

/etc/hosts ファイルが以下のいずれかの条件を満たすことを確認します。

- このファイルには、ホストのエントリーが含まれません。ホストの IPv4 および IPv6 の localhost エントリーリストのみを表示します。
- このファイルには、ホストのエントリーが含まれ、ファイルには以下の条件がすべて満たされます。
  - 最初の 2 つのエントリーは、IPv4 および IPv6 の localhost エントリーです。
  - その次のエントリーは、IdM サーバーの IPv4 アドレスとホスト名を指定します。
  - IdM サーバーの **FQDN** は、IdM サーバーの省略名の前に指定します。
  - IdM サーバーのホスト名は、localhost エントリーには含まれません。

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

```
127.0.0.1   localhost localhost.localdomain \
localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain \
```

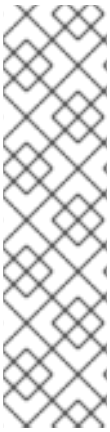
```
localhost6 localhost6.localdomain6
192.0.2.1 server.idm.example.com server
2001:DB8::1111 server.idm.example.com server
```

2.8. IDM のポート要件

Identity Management (IdM) は、複数の ポート を使用して、そのサービスと対話します。IdM サーバーが動作するには、このようなポートを開いて IdM サーバーへの着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2.2 IdM 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)



注記

IdM はポート 80 および 389 を使用します。これは、以下のような安全なプラクティスです。

- IdM は通常、ポート 80 に到着するリクエストをポート 443 にリダイレクトします。ポート 80 (HTTP) は、Online Certificate Status Protocol (OCSP) 応答および証明書失効リスト (CRL) の提供にのみ使用されます。いずれもデジタル署名されているため、中間者攻撃に対してセキュリティーが保護されます。
- ポート 389 (LDAP) は、暗号化に STARTLS および Generic Security Services API (GSSAPI) を使用します。

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2.3 firewalld サービス

サービス名	詳細は、次を参照してください。
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**

2.9. IDM で必要なポートの開放

手順

1. **firewalld** サービスが実行されていることを確認します。
   - **firewalld** が実行中であることを確認するには、次のコマンドを実行します。

     ```
     # 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、次のコマンドを実行します。

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

2. **firewall-cmd** ユーティリティーを使用し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、次のコマンドを実行します。

      ```
      # 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}
      ```

   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、デフォルトゾーンでポートを開くには、次のコマンドを実行します。

      ```
      # firewall-cmd --permanent --add-service={freeipa-4,dns}
      ```

      firewall-cmd を使用してシステムでポートを開く方法は **firewall-cmd**(1) の man ページを参照してください。

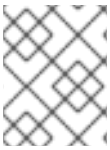
3. **firewall-cmd** 設定を再ロードして、変更が即座に反映されるようにします。

   ```
   # 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** オプションを指定して、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
   ```

4. **オプション:**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、着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。

2.10. IDM 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、IdM 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 システムを新しくインストールしている。
- 必要なリポジトリーを利用できるようにしている。
  - RHEL システムがクラウドで稼働していない場合は、Red Hat Subscription Manager (RHSM) でシステムを登録している。詳細は、Subscription Manager コマンドラインでサブスクリプションの登録、割り当て、および削除 を参照してください。IdM が使用する **BaseOS** リポジトリーおよび **AppStream** リポジトリーも有効にしている。

    ```
    # subscription-manager repos --enable=rhel-8-for-x86_64-baseos-rpms
    # subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms
    ```

    RHSM を使用して特定のリポジトリーを有効または無効にする方法は、Red Hat Subscription Manager でオプションの設定 を参照してください。
  - RHEL システムがクラウドで実行している場合は、登録を省略します。必要なリポジトリーは、Red Hat Update Infrastructure (RHUI) から入手できます。
- IdM モジュールストリームを有効にしていない。

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するには、次のコマンドを実行します。

     ```
     # 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するには、次のコマンドを実行します。

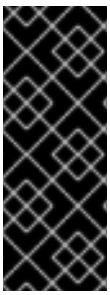
     ```
     # yum module install idm:DL1/adtrust
     ```

- **adtrust** プロファイルや **dns** プロファイルからパッケージをダウンロードするには、次のコマンドを実行します。

```
# 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するには、次のコマンドを実行します。

```
# 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。続行方法の詳細は 後続のストリームへの切り替え 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、**bind-dyndb-ldap** をリポジトリーから直接インストールして、カスタムの 389 Directory Server セットアップで使用する場合に発生した問題は、IdM でも発生する場合を除きサポートされません。

2.11. IDM インストール用の正しいファイルモード作成マスクの設定

Identity Management (IdM) のインストールプロセスでは、**root** アカウントのファイルモード作成マスク (**umask**) が **0022** に設定されている必要があります。これにより、**root** 以外のユーザーがインストール中に作成されたファイルを読み取ることができます。別の **umask** が設定されている場合は、IdM サーバーをインストールすると警告が表示されます。インストールを続行すると、サーバーの一部の機能が正しく実行されません。たとえば、このサーバーから IdM レプリカをインストールすることはできません。インストール後、**umask** を元の値に戻すことができます。

前提条件

- **root** 権限があります。

手順

1. (オプション) 現在の **umask** を表示します。

```
# umask
0027
```

2. **umask** を **0022** に設定します。

```
# umask 0022
```

3. (オプション) IdM のインストールが完了したら、**umask** を元の値に戻します。

```
# umask 0027
```

2.12. FAPOLICYD ルールが IDM インストールおよび操作をブロックしないようにする

RHEL ホストで **fapolicyd** ソフトウェアフレームワークを使用してユーザー定義のポリシーに基づいてアプリケーションの実行を制御する場合、Identity Management (IdM)サーバーのインストールに失敗する可能性があります。インストールおよび操作が正常に完了するには Java プログラムが必要になるため、Java および Java クラスが **fapolicyd** ルールによってブロックされていないことを確認してください。

詳細は、fapolicy restrictions causing IdM installation failures KCS を参照してください。

2.13. IDM インストールコマンドのオプション

ipa-server-install、**ipa-replica-install**、**ipa-dns-install**、**ipa-ca-install** などのコマンドには、対話型インストールに関する追加情報の確認に使用できる数多くのオプションがあります。これらのオプションを使用して、無人インストールのスクリプトを作成することもできます。

以下の表は、異なるコンポーネントで最も一般的なオプションの一部を示しています。特定のコンポーネントのオプションは、複数のコマンド間で共有されます。たとえば、**ipa-ca-install** コマンドおよび **ipa-server-install** コマンドの両方で **--ca-subject** オプションを使用できます。

オプションの完全なリストについては、**ipa-server-install (1)**、**ipa-replica-install (1)**、**ipa-dns-install (1)**、および **ipa-ca-install (1)** の man ページを参照してください。

表2.4 一般的なオプション: ipa-server-install および ipa-replica-installで利用できます。

引数	説明
-d、--debug	詳細な出力のためにデバッグロギングを有効にします。
-U、--unattended	ユーザー入力を要求しない無人インストールセッションを有効にします。
--hostname=server.idm.example.com	IdM サーバーマシンの完全修飾ドメイン名。数字、小文字のアルファベット、およびハイフン (-) のみが使用できます。
--ip-address 127.0.0.1	サーバーの IP アドレスを指定します。このオプションでは、ローカルインターフェイスに関連付けられている IP アドレスのみを使用できます。
--dirsrv-config-file <LDIF_file_name>	ディレクトリーサーバーインスタンスの設定を変更するのに使用する LDIF ファイルへのパス。
-n example.com	IdM ドメインに使用する LDAP サーバードメインの名前。これは、通常 IdM サーバーのホスト名に基づいています。

引数	説明
-p <directory_manager_password>	LDAP サービス用のスーパーユーザーの **cn=Directory Manager** のパスワード。
-a <ipa_admin_password>	Kerberos レルムに対して認証する **admin** IdM 管理者アカウントのパスワード。**ipa-replica-install** の場合は、代わりに **-w** を使用します。
-r <KERBEROS_REALM_NAME>	**EXAMPLE.COM** など、IdM ドメイン用に作成する Kerberos レルムの名前を大文字で入力します。**ipa-replica-install** では、既存の IdM デプロイメントの Kerberos レルムの名前を指定します。
--setup-dns	IdM ドメイン内に DNS サービスを設定するように、インストールスクリプトに指示します。
--setup-ca	このレプリカに CA をインストールして設定します。CA が設定されていないと、証明書操作は CA がインストールされている別のレプリカに転送されます。**ipa-server-install** の場合、CA はデフォルトでインストールされ、このオプションを使用する必要はありません。

表2.5 CA オプション: ipa-ca-install および ipa-server-installで利用できます。

引数	説明
--ca-subject=<SUBJECT>	CA 証明書のサブジェクト識別名を指定します (デフォルト：CN=Certificate Authority,O=REALM.NAME)。相対識別名 (RDN) は LDAP 順で、最も具体的な RDN が最初に使用されます。
--subject-base=<SUBJECT>	IdM によって発行される証明書のサブジェクトベースを指定します (デフォルト O=REALM.NAME)。相対識別名 (RDN) は LDAP 順で、最も具体的な RDN が最初に使用されます。
--external-ca	外部 CA によって署名される証明書署名要求を生成します。
--ca-signing-algorithm=<ALGORITHM>	IdM CA 証明書の署名アルゴリズムを指定します。使用できる値は SHA1withRSA、SHA256withRSA、SHA512withRSA です。デフォルトは SHA256withRSA です。外部 CA がデフォルトの署名アルゴリズムをサポートしていない場合は、**--external-ca** でこのオプションを使用します。

表2.6 DNS オプション: ipa-dns-install、または --setup-dnsを使用する場合は ipa-server-install および ipa-replica-install で利用できます。

引数	説明
--forwarder=192.0.2.1	DNS サービスで使用する DNS フォワーダーを指定します。複数のフォワーダーを指定するには、このオプションを複数回使用します。

引数	説明
--no-forwarders	フォワーダーではなく DNS サービスを使用するルートサーバーを使用します。
--no-reverse	DNS ドメインの設定時に、逆引き DNS ゾーンが作成されないようにします。逆引き DNS ゾーンがすでに設定されている場合は、既存の逆引き DNS ゾーンが使用されます。 このオプションを使用しない場合、デフォルト値は **true** になります。これにより、インストールスクリプトで逆引き DNS を設定するように指示します。

関連情報

- **ipa-server-install(1)** の man ページ
- **ipa-replica-install(1)** の man ページ
- **ipa-dns-install (1)** の man ページ
- **ipa-ca-install (1)** の man ページ

第3章 IDM サーバーのインストール: 統合 DNS と統合 CA を ROOT CA として使用する場合

統合 DNS のある新しい Identity Management (IdM) 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 IdM 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。
- IdM サーバーのインストール時にグローバルフォワーダーを設定して、安定した外部インターネット接続を実現できます。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。
- IdM ドメインからのメールが、IdM ドメイン外のメールサーバーによってスパムと見なされないように、DNS 逆ゾーンを設定できます。

統合 DNS のある IdM のインストールにはいくつかの制限があります。

- IdM DNS は、一般用途の DNS サーバーとして使用することは想定されていません。高度な DNS 機能の一部はサポートされていません。詳細は、IdM サーバーで利用可能な DNS サービスを 参照してください。

本章では、認証局 (CA) をルート CA として新しい IdM 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、IdM サーバーは統合 CA とインストールされます。

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を指定するように求められます。

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. 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** を入力します。

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

3. このスクリプトでは、いくつかの設定を入力することが求められます。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

- 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、指定する値を入力します。

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

警告

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 (IdM) 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. スクリプトにより、サーバーごとの DNS フォワーダー設定のプロンプトが表示されます。

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

- サーバーごとの 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、IdM LDAP 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、 **ipa-dns-install**(1) の man ページに記載されている **--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、IdM ドメインのホストは、インフラストラクチャー内にある他の内部 DNS ドメインから名前を解決できません。ホストは、DNS クエリーを解決するためにパブリック DNS サーバーでのみ残ります。

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スクリプトプロンプトが出されます。

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

検索を実行して欠落している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が尋ねられます。

```
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

オプションで、逆引きゾーンの管理に IdM を使用できます。代わりに、この目的で外部 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、次の方法で DNS レコードを更新します。

   a. 親ドメインから IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **idm.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

重要

IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

   b. タイムサーバーの **_ntp._udp** サービス (SRV) レコードを IdM DNS に追加します。IdM DNS に新たにインストールした IdM サーバーのタイムサーバーの SRV レコードが存在すると、このプライマリー IdM サーバーが使用するタイムサーバーと同期するように、今後のレプリカおよびクライアントインストールが自動的に設定されます。

3.2. 非対話型インストール

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 (IdM) 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** - IdM 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 IDM.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、次の方法で DNS レコードを更新します。

   a. 親ドメインから IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **idm.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

   重要

   IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

   b. タイムサーバーの **_ntp._udp** サービス (SRV) レコードを IdM DNS に追加します。IdM DNS に新たにインストールした IdM サーバーのタイムサーバーの SRV レコードが存在すると、このプライマリー IdM サーバーが使用するタイムサーバーと同期するように、今後のレプリカおよびクライアントインストールが自動的に設定されます。

関連情報

- 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4章 IDM サーバーのインストール: 統合 DNS と外部 CA を ROOT CA として使用する場合

統合 DNS のある新しい Identity Management (IdM) 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 IdM 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。
- IdM サーバーのインストール時にグローバルフォワーダーを設定して、安定した外部インターネット接続を実現できます。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。
- IdM ドメインからのメールが、IdM ドメイン外のメールサーバーによってスパムと見なされないように、DNS 逆ゾーンを設定できます。

統合 DNS のある IdM のインストールにはいくつかの制限があります。

- IdM DNS は、一般用途の DNS サーバーとして使用することは想定されていません。高度な DNS 機能の一部はサポートされていません。詳細は、IdM サーバーで利用可能な DNS サービスを 参照してください。

本章では、外部の認証局 (CA) をルート CA として新しい IdM サーバーをインストールする方法を説明します。

4.1. 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を指定するように求められます。

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。

以下の手順に従って、サーバーをインストールします。

- 統合 DNS 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

- **--external-ca-type** オプションで指定する外部 CA のタイプを決定している。詳細は、**ipa-server-install** (1) の man ページを参照すること。
- Microsoft 証明書サービス認証局 (MS CS CA) を外部 CA として使用している場合は、**--external-ca-profile** オプションで指定する証明書プロファイルまたはテンプレートを決定している。デフォルトでは、**SubCA** テンプレートが使用される。
  --external-ca-type および **--external-ca-profile** オプションの詳細は、ルート CA として外部 CA と共に IdM CA をインストールする際に使用されるオプション を参照してください。

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 証明書サービス (MS CS) CA を使用している場合は、**--external-ca-type** オプションと、任意で **--external-ca-profile** オプションを使用します。

```
[root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-profile=<oid>/<name>/default
```

- MS CS を使用して IdM CA の署名証明書を生成していない場合は、他のオプションは必要ありません。

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

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、*6章IdM サーバーのインストール: 統合 DNS がなく統合 CA が root CA としてある場合* を参照してください。

3. このスクリプトでは、いくつかの設定を入力することが求められます。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、指定する値を入力します。

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

警告

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 (IdM) 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. スクリプトにより、サーバーごとの DNS フォワーダー設定のプロンプトが表示されます。

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

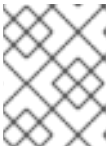
- サーバーごとの DNS フォワーダーを設定するには、**yes** を入力して表示されたコマンドラインの指示に従います。インストールプロセスにより、IdM LDAP にフォワーダーの IP アドレスが追加されます。
  - フォワードポリシーのデフォルト設定は、 **ipa-dns-install**(1) の man ページに記載されている **--forward-policy** の説明を参照してください。
- DNS 転送を使用しない場合は、**no** と入力します。
  DNS フォワーダーがないと、IdM ドメインのホストは、インフラストラクチャー内にある他の内部 DNS ドメインから名前を解決できません。ホストは、DNS クエリーを解決するためにパブリック DNS サーバーでのみ残ります。

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スクリプトプロンプトが出されます。

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

検索を実行して欠落している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が尋ねられます。

```
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

オプションで、逆引きゾーンの管理に IdM を使用できます。代わりに、この目的で外部 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。繰り返しになりますが、プロセスは各証明書サービスによって異なります。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. 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て **ipa-server-install** を再度実行します。以下に例を示します。

```
# 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。

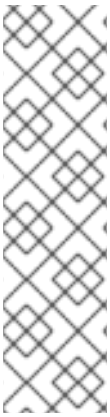
10. インストールスクリプトが完了したら、次の方法で DNS レコードを更新します。

a. 親ドメインから IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **idm.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

重要

IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

b. タイムサーバーの **_ntp._udp** サービス (SRV) レコードを IdM DNS に追加します。IdM DNS に新たにインストールした IdM サーバーのタイムサーバーの SRV レコードが存在すると、このプライマリー IdM サーバーが使用するタイムサーバーと同期するように、今後のレプリカおよびクライアントインストールが自動的に設定されます。



注記

ipa-server-install --external-ca コマンドは、次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** 環境変数が設定されていると発生します。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。

4.2. 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、次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. 次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認証局 (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 (IdM) 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5章 IDM サーバーのインストール: 統合 DNS があり外部 CA がない場合

統合 DNS のある新しい Identity Management (IdM) 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 IdM 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。
- IdM サーバーのインストール時にグローバルフォワーダーを設定して、安定した外部インターネット接続を実現できます。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。
- IdM ドメインからのメールが、IdM ドメイン外のメールサーバーによってスパムと見なされないように、DNS 逆ゾーンを設定できます。

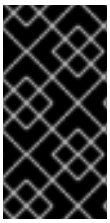
統合 DNS のある IdM のインストールにはいくつかの制限があります。

- IdM DNS は、一般用途の DNS サーバーとして使用することは想定されていません。高度な DNS 機能の一部はサポートされていません。詳細は、IdM サーバーで利用可能な DNS サービスを 参照してください。

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

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

認証局(CA)なしで Identity Management (IdM) サーバーをインストールするために必要な証明書を提供する必要があります。説明されているコマンドラインオプションを使用すると、これらの証明書を **ipa-server-install** ユーティリティーに提供できます。



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。

LDAP サーバー証明書および秘密鍵

- **--dirsrv-cert-file** - LDAP サーバー証明書の証明書ファイルおよび秘密鍵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秘密鍵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秘密鍵

- **--http-cert-file** - Apache サーバー証明書の証明書および秘密鍵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秘密鍵にアクセスするパスワードを提供します。

LDAP および Apache の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が含まれる証明書ファイルを提供します。

以下の形式の **--dirsrv-cert-file** オプションおよび **--http-cert-file** オプションを指定して、ファイルを指定できます。

- PEM (Privacy-Enhanced Mail) がエンコードした証明書 (RFC 7468)。Identity Management インストーラーは、連結した PEM エンコードオブジェクトを受け付けることに注意してください。
- 識別名エンコーディングルール (DER)
- PKCS #7 証明書チェーンオブジェクト
- PKCS #8 秘密鍵オブジェクト
- PKCS #12 アーカイブ

--dirsrv-cert-file オプションおよび **--http-cert-file** オプションを複数回指定して、複数のファイルを指定できます。

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。このオプションは、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使用します。

--ca-cert-file を使用して提供されるファイルと、**--dirsrv-cert-file** と **--http-cert-file** を使用して提供されるファイルには、LDAP および Apache の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 証明書および秘密鍵

- PKINIT 証明書がある場合は、次の 2 つのオプションを使用します。
  - **--pkinit-cert-file** - Kerberos KDC SSL の証明書および秘密鍵を提供します。
  - **--pkinit-pin** - **--pkinit-cert-file** に指定されたファイルにある Kerberos KDC の秘密鍵にアクセスするパスワードを提供します。
- PKINIT 証明書がなく、自己署名証明書を使用してローカル KDC で IdM サーバーを設定する場合は、次のオプションを使用します。
  - **--no-pkinit** - pkinit 設定手順を無効にします。

関連情報

- こ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、**ipa-server-install**(1) の man ページを参照すること。
- RHEL IdM PKINIT 証明書の作成に必要な PKINIT 拡張機能の詳細は、RHEL IdM PKINIT KDC 証明書と拡張機能 を参照すること。

5.2. 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を指定するように求められます。

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 IdM 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、IdM サーバーのインストール: 統合 DNS がなく統合 CA が root CA としてある場合 を参照してください。

3. このスクリプトでは、いくつかの設定を入力することが求められます。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、指定する値を入力します。

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

警告

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 (IdM) 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. スクリプトにより、サーバーごとの DNS フォワーダー設定のプロンプトが表示されます。

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

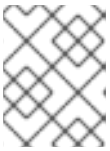
- サーバーごとの DNS フォワーダーを設定するには、**yes** を入力して表示されたコマンドラインの指示に従います。インストールプロセスにより、IdM LDAP にフォワーダーの IP アドレスが追加されます。
  - フォワードポリシーのデフォルト設定は、 **ipa-dns-install**(1) の man ページに記載されている **--forward-policy** の説明を参照してください。
- DNS 転送を使用しない場合は、**no** と入力します。
  DNS フォワーダーがないと、IdM ドメインのホストは、インフラストラクチャー内にある他の内部 DNS ドメインから名前を解決できません。ホストは、DNS クエリーを解決するためにパブリック DNS サーバーでのみ残ります。

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スクリプトプロンプトが出されます。

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

検索を実行して欠落している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が尋ねられます。

```
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

オプションで、逆引きゾーンの管理に IdM を使用できます。代わりに、この目的で外部 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、次の方法で DNS レコードを更新します。

   a. 親ドメインから IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **idm.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

   重要

   IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

   b. タイムサーバーの **_ntp._udp** サービス (SRV) レコードを IdM DNS に追加します。IdM DNS に新たにインストールした IdM サーバーのタイムサーバーの SRV レコードが存在すると、このプライマリー IdM サーバーが使用するタイムサーバーと同期するように、今後のレプリカおよびクライアントインストールが自動的に設定されます。

第6章 IDM サーバーのインストール: 統合 DNS がなく統合 CA が ROOT CA としてある場合

本章では、統合 DNS を使用しないで新しい Identity Management (IdM) サーバーをインストールする方法を説明します。

注記

Red Hat では、IdM デプロイメントにおける基本的な使用のために IdM 統合 DNS をインストールすることを強く推奨します。IdM サーバーが DNS も管理する場合には、DNS とネイティブの IdM ツールが密接に統合されるため、DNS レコード管理の一部が自動化できます。

詳細は、Planning your DNS services and host names を参照してください。

6.1. 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を指定するように求められます。

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 (IdM) の認証局 (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. 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。**Enter** を押して、**no** オプションを選択します。

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

3. このスクリプトでは、いくつかの設定を入力することが求められます。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、指定する値を入力します。

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

警告

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、IdM 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. このスクリプトでは、いくつかの設定を入力することが求められます。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、指定する値を入力します。

```
NetBIOS domain name [EXAMPLE]:
Do you want to configure chrony with NTP server or pool address? [no]:
```

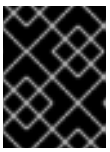
6. サーバー設定をする場合は、**yes** と入力します。

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

7. 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。

8. インストールスクリプトは、以下の出力例の DNS リソースレコード でファイル (**/tmp/ipa.system.records.UFRPto.db**) を生成します。これらのレコードを既存の外部 DNS サーバーに追加します。DNS レコードの更新プロセスは、特定の DNS ソリューションによって異なります。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



重要

既存の DNS サーバーに DNS レコードを追加するまで、サーバーのインストールは完了しません。

関連情報

- DNS システムに追加する必要がある DNS リソースレコードの詳細は、外部 DNS システムの IdM DNS レコード を参照してください。

6.2. 非対話型インストール

この手順では、統合 DNS のないサーバー、または統合 Identitiy Management (IdM) 認証局 (CA) を root CA (デフォルトの CA 設定) として持つサーバーをインストールします。

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. 必要に応じて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。

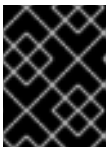
   - **--realm** - Kerberos レルム名を指定します。
   - **--ds-password** - Directory Server のスーパーユーザーである Directory Manager (DM) のパスワードを指定します。
   - **--admin-password** - IdM 管理者である **admin** のパスワードを指定します。
   - **--unattended** - インストールプロセスでホスト名およびドメイン名のデフォルトオプションを選択するようにします。

   以下に例を示します。

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

2. インストールスクリプトは、以下の出力例の DNS リソースレコード でファイル (**/tmp/ipa.system.records.UFRPto.db**) を生成します。これらのレコードを既存の外部 DNS サーバーに追加します。DNS レコードの更新プロセスは、特定の DNS ソリューションによって異なります。

   ```
   ...
   Restarting the KDC
   Please add records in this file to your DNS system:
   /tmp/ipa.system.records.UFRBto.db
   Restarting the web server
   ...
   ```



重要

既存の DNS サーバーに DNS レコードを追加するまで、サーバーのインストールは完了しません。

関連情報

- DNS システムに追加する必要がある DNS リソースレコードの詳細は、外部 DNS システムの IdM DNS レコード を参照してください。

- 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。

6.3. 外部 DNS システムの IDM DNS レコード

統合 DNS を使用せずに IdM サーバーをインストールした後、IdM サーバーの LDAP リソースレコードおよび Kerberos DNS リソースレコードを外部 DNS システムに追加する必要があります。

ipa-server-install インストールスクリプトは、ファイル名が **/tmp/ipa.system.records.<random_characters>.db** 形式の DNS リソースレコードのリストを含むファイルを生成し、そのレコードを追加する手順を表示します。

```
Please add records in this file to your DNS system: /tmp/ipa.system.records.6zdjqxh3.db
```

以下は、ファイルの内容の例になります。

```
_kerberos-master._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos-master._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos.example.com. 86400 IN TXT "EXAMPLE.COM"
_kpasswd._tcp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_kpasswd._udp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_ldap._tcp.example.com. 86400 IN SRV 0 100 389 server.example.com.
```

注記

IdM サーバーの LDAP リソースレコードおよび Kerberos DNS リソースレコードを DNS システムに追加したら、DNS 管理ツールが **ipa-ca** の PTR レコードを追加していないことを確認します。DNS に **ipa-ca** の PTR レコードが存在すると、その後の IdM レプリカのインストールに失敗する場合があります。

第7章 IDM サーバーのインストール: 統合 DNS なしで外部 CA を ROOT CA として使用する場合

本章では、統合 DNS なしで、外部認証局 (CA) をルート CA として使用する Identity Management (IdM) サーバーを新規インストールする方法を説明します。

注記

Red Hat では、IdM デプロイメントにおける基本的な使用のために IdM 統合 DNS をインストールすることを強く推奨します。IdM サーバーが DNS も管理する場合には、DNS とネイティブの IdM ツールが密接に統合されるため、DNS レコード管理の一部が自動化できます。

詳細は、Planning your DNS services and host names を参照してください。

7.1. ルート CA として外部 CA と共に IDM CA をインストールする際に使用されるオプション

以下の条件のいずれかが該当する場合、ルート CA として外部 CA と共に Identity Management IdM 認証局 (CA) をインストールすることができます。

- **ipa-server-install** コマンドを使用して、新しい IdM サーバーまたはレプリカをインストールしようとしている。
- **ipa-ca-install** コマンドを使用して、CA コンポーネントを既存の IdM サーバーにインストールしようとしている。

ルート CA として外部 CA と共に IdM CA をインストールする際に証明書署名要求 (CSR) を作成するのに使用できる次の両方のコマンドオプションを使用可能です。

--external-ca-type=TYPE

外部 CA のタイプ。設定可能な値は **generic** および **ms-cs** です。デフォルト値は **generic** です。生成される CSR に Microsoft Certificate Services (MS CS) で必要なテンプレート名を追加するには、**ms-cs** を使用します。デフォルト以外のプロファイルを使用するには、**--external-ca-type=ms-cs** と共に **--external-ca-profile** オプションを使用します。

--external-ca-profile=PROFILE_SPEC

IdM CA の証明書を発行する際に MS CS が適用する証明書プロファイルまたはテンプレートを指定します。
--external-ca-profile オプションは、**--external-ca-type** が ms-cs の場合にのみ使用できます。

MS CS テンプレートは、以下のいずれかの方法で特定できます。

- **<oid>:<majorVersion>[:<minorVersion>]**:証明書テンプレートは、オブジェクト識別子 (OID) およびメジャーバージョンで指定できます。任意でマイナーバージョンを指定することもできます。
- **<name>**:証明書テンプレートは、名前で指定できます。名前には : 文字を含めることができず、OID を指定できません。そうでなければ、OID ベースのテンプレート指定子構文が優先されます。
- **default**:この指定子を使用する場合には、テンプレート名 **SubCA** が使用されます。

特定のシナリオでは、Active Directory (AD) 管理者は、AD CS に組み込まれているテンプレートである **Subordinate 認証局** (SCA) テンプレートを使用して、組織のニーズにより適した一意のテンプレートを作成できます。たとえば、新しいテンプレートでは有効期間や拡張機能をカスタマイズできます。関連付けられたオブジェクト識別子 (OID) は、AD **証明書テンプレート** コンソールにあります。

AD 管理者が元の組み込みテンプレートを無効にしている場合は、IdM CA の証明書を要求する際に新しいテンプレートの OID または名前を指定する必要があります。AD 管理者に、新しいテンプレートの名前または OID を提供するよう依頼します。

元の SCA AD CS テンプレートがまだ有効にされている場合は、追加で **--external-ca-profile** オプションを使用せずに **--external-ca-type=ms-cs** を指定して使用できます。この場合、**subCA** 外部 CA プロファイルが使用されます。これは、SCA AD CS テンプレートに対応するデフォルトの IdM テンプレートです。

7.2. 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を指定するように求められます。

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。

以下の手順に従って、サーバーをインストールします。

- 統合 DNS のないサーバー
- 外部認証局 (CA) をルート CA とするサーバー

前提条件

- **--external-ca-type** オプションで指定する外部 CA のタイプを決定している。詳細は、**ipa-server-install** (1) の man ページを参照すること。
- Microsoft 証明書サービス認証局 (MS CS CA) を外部 CA として使用している場合は、**--external-ca-profile** オプションで指定する証明書プロファイルまたはテンプレートを決定している。デフォルトでは、**SubCA** テンプレートが使用される。
  --external-ca-type および **--external-ca-profile** オプションの詳細は、ルート CA として外部 CA と共に IdM CA をインストールする際に使用されるオプション を参照してください。

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。
   - Microsoft 証明書サービス (MS CS) CA を使用している場合は、**--external-ca-type** オプションと、任意で **--external-ca-profile** オプションを使用します。

     ```
     [root@server ~]# ipa-server-install --external-ca --external-ca-type=ms-cs --external-ca-profile=<oid>/<name>/default
     ```

   - MS CS を使用して IdM CA の署名証明書を生成していない場合は、他のオプションは必要ありません。

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

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。**Enter** を押して、**no** オプションを選択します。

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

3. このスクリプトでは、いくつかの設定を入力することが求められます。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、指定する値を入力します。

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

警告

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、IdM 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. 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。繰り返しになりますが、プロセスは各証明書サービスによって異なります。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。

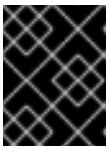
c. 新たに発行された CA 証明書と CA チェーンファイルの場所と名前を指定して **ipa-server-install** を再度実行します。以下に例を示します。

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

7. 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。

8. インストールスクリプトは、以下の出力例の DNS リソースレコード でファイル (**/tmp/ipa.system.records.UFRPto.db**) を生成します。これらのレコードを既存の外部 DNS サーバーに追加します。DNS レコードの更新プロセスは、特定の DNS ソリューションによって異なります。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



重要

既存の DNS サーバーに DNS レコードを追加するまで、サーバーのインストールは完了しません。

関連情報

- DNS システムに追加する必要がある DNS リソースレコードの詳細は、外部 DNS システムの IdM DNS レコード を参照してください。
- **ipa-server-install --external-ca** コマンドは、次のエラーにより失敗する場合があります。

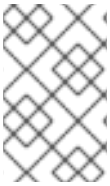
```
ipa         : CRITICAL failed to configure ca instance Command '/usr/sbin/pkispawn -s CA -f /tmp/pass:quotes[configuration_file]' returned non-zero exit status 1
Configuration of CA failed
```

この失敗は、***_proxy** 環境変数が設定されていると発生します。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。

7.3. 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
- 外部認証局 (CA) をルート CA とするサーバー



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。

前提条件

- **--external-ca-type** オプションで指定する外部 CA のタイプを決定している。詳細は、**ipa-server-install** (1) の man ページを参照すること。
- Microsoft 証明書サービス認証局 (MS CS CA) を外部 CA として使用している場合は、**--external-ca-profile** オプションで指定する証明書プロファイルまたはテンプレートを決定している。デフォルトでは、**SubCA** テンプレートが使用される。
  --external-ca-type および **--external-ca-profile** オプションの詳細は、ルート CA として外部 CA と共に IdM CA をインストールする際に使用されるオプション を参照してください。

手順

1. 必要に応じて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。外部 CA をルート CA として使用する IdM サーバーを非対話的にインストールする場合の最小要件オプションは以下のとおりです。
   - **--external-ca** - 外部 CA をルート CA として指定します。
   - **--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** - IdM 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 --external-ca --realm IDM.EXAMPLE.COM --ds-password
     DM_password --admin-password admin_password --unattended
     ```

   Microsoft 証明書サービス (MS CS) CA を使用している場合は、**--external-ca-type** オプションと、任意で **--external-ca-profile** オプションを使用します。詳細は、root CA として外部 CA と共に IdM CA をインストールする際に使用されるオプション を参照してください。

2. 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。

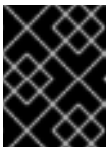
   ```
   ...

   Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes
     [1/11]: configuring certificate server instance
   The next step is to get /root/ipa.csr signed by your CA and re-run /usr/sbin/ipa-server-install
   ```

```
as:
/usr/sbin/ipa-server-install --external-cert-file=/path/to/signed_certificate --external-cert-
file=/path/to/external_ca_certificate
The ipa-server-install command was successful
```

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。繰り返しになりますが、プロセスは各証明書サービスによって異なります。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。

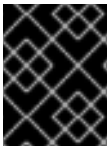
c. 新たに発行された CA 証明書と CA チェーンファイルの場所と名前を指定して **ipa-server-install** を再度実行します。以下に例を示します。

```
# ipa-server-install --external-cert-file=/tmp/servercert20170601.pem --external-cert-
file=/tmp/cacert.pem --realm IDM.EXAMPLE.COM --ds-password DM_password --
admin-password admin_password --unattended
```

3. 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。

4. インストールスクリプトは、以下の出力例の DNS リソースレコードでファイル (**/tmp/ipa.system.records.UFRPto.db**) を生成します。これらのレコードを既存の外部 DNS サーバーに追加します。DNS レコードの更新プロセスは、特定の DNS ソリューションによって異なります。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



重要

既存の DNS サーバーに DNS レコードを追加するまで、サーバーのインストールは完了しません。

関連情報

- DNS システムに追加する必要がある DNS リソースレコードの詳細は、外部 DNS システムの IdM DNS レコード を参照してください。

7.4. 外部 DNS システムの IDM DNS レコード

統合 DNS を使用せずに IdM サーバーをインストールした後、IdM サーバーの LDAP リソースレコードおよび Kerberos DNS リソースレコードを外部 DNS システムに追加する必要があります。

ipa-server-install インストールスクリプトは、ファイル名が **/tmp/ipa.system.records.<random_characters>.db** 形式の DNS リソースレコードのリストを含むファイルを生成し、そのレコードを追加する手順を表示します。

> Please add records in this file to your DNS system: **/tmp/ipa.system.records.6zdjqxh3.db**

以下は、ファイルの内容の例になります。

```
_kerberos-master._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos-master._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos._tcp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos._udp.example.com. 86400 IN SRV 0 100 88 server.example.com.
_kerberos.example.com. 86400 IN TXT "EXAMPLE.COM"
_kpasswd._tcp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_kpasswd._udp.example.com. 86400 IN SRV 0 100 464 server.example.com.
_ldap._tcp.example.com. 86400 IN SRV 0 100 389 server.example.com.
```

注記

IdM サーバーの LDAP リソースレコードおよび Kerberos DNS リソースレコードを DNS システムに追加したら、DNS 管理ツールが **ipa-ca** の PTR レコードを追加していないことを確認します。DNS に **ipa-ca** の PTR レコードが存在すると、その後の IdM レプリカのインストールに失敗する場合があります。

第8章 LDIF ファイルからのカスタムデータベース設定を使用した IDM サーバーまたはレプリカのインストール

Directory Server データベースのカスタム設定を使用して、IdM サーバーおよび IdM レプリカをインストールできます。以下の手順は、データベース設定で LDAP データ交換形式 (LDIF) ファイルを作成する方法と、その設定を IdM サーバーおよびレプリカインストールコマンドに渡す方法を示しています。

前提条件

- IdM 環境のパフォーマンスを向上させるカスタムの Directory Server 設定を行っている。IdM Directory Server パフォーマンスの調整 を参照してください。

手順

1. カスタムデータベース設定で LDIF 形式のテキストファイルを作成します。LDAP 属性の変更はダッシュ (-) で区切ります。この例では、idle タイムアウトおよび最大ファイルディスクリプターにデフォルト以外の値を設定します。

```
dn: cn=config
changetype: modify
replace: nsslapd-idletimeout
nsslapd-idletimeout=1800
-
replace: nsslapd-maxdescriptors
nsslapd-maxdescriptors=8192
```

2. **--dirsrv-config-file** パラメーターを使用して、LDIF ファイルをインストールスクリプトに渡します。

   a. IdM サーバーをインストールするには、次のコマンドを実行します。

```
# ipa-server-install --dirsrv-config-file filename.ldif
```

   b. IdM レプリカをインストールするには、次のコマンドを実行します。

```
# ipa-replica-install --dirsrv-config-file filename.ldif
```

関連情報

- **ipa-server-install** コマンドおよび **ipa-replica-install** コマンドのオプション

第9章 IDM サーバーのインストールに関するトラブルシューティング

次のセクションでは、失敗した IdM サーバーのインストールについての情報を収集する方法、一般的なインストールの問題を解決する方法を説明します。

9.1. IDM サーバーインストールエラーログの確認

Identity Management (IdM) サーバーをインストールすると、以下のログファイルにデバッグ情報が追加されます。

- **/var/log/ipaserver-install.log**
- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-INSTANCE-NAME/access**
- **/var/log/dirsrv/slapd-INSTANCE-NAME/errors**

ログファイルの最後の行は成功または失敗を報告し、**ERROR** および **DEBUG** エントリーで追加のコンテキストを把握できます。

失敗した IdM サーバーのインストールをトラブルシューティングするには、ログファイルの最後でエラーを確認し、この情報を使用して、対応する問題を解決します。

前提条件

- IdM ログファイルの内容を表示するには、**root** 権限が必要である。

手順

1. **tail** コマンドを使用して、ログファイルの最後の行を表示します。以下の例では、**/var/log/ipaserver-install.log** の最後の 10 行を表示しています。

```
[user@server ~]$ sudo tail -n 10 /var/log/ipaserver-install.log
[sudo] password for user:
value = gen.send(prev_value)
File "/usr/lib/python3.6/site-packages/ipapython/install/common.py", line 65, in _install
for unused in self._installer(self.parent):
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/init.py", line 564, in main
master_install(self)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/install.py", line 291, in decorated
raise ScriptError()

2020-05-27T22:59:41Z DEBUG The ipa-server-install command failed, exception:
ScriptError:
2020-05-27T22:59:41Z ERROR The ipa-server-install command failed. See
/var/log/ipaserver-install.log for more information
```

2. ログファイルを対話的に確認するには、**less** ユーティリティーを使用してログファイルの最後を開き、↑ および ↓キーを使用して移動します。以下の例では、**/var/log/ipaserver-install.log** ファイルを対話的に開きます。

```
[user@server ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

3. ログファイルの残りで、このレビュープロセスを繰り返して、追加のトラブルシューティング情報を収集します。

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access

[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

関連情報

- Red Hat テクニカルサポートサブスクリプションがあり、IdM サーバーのインストール失敗の問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、サーバーの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

9.2. IDM CA インストールエラーの確認

Identity Management (IdM) サーバーに認証局 (CA) サービスをインストールすると、デバッグ情報が以下の場所 (推奨される優先順位) に追加されます。

場所	説明
/var/log/pki/pki-ca-spawn.$TIME_OF_INSTALLATION.log	問題の概要と、**pkispawn** インストールプロセスの Python トレース
journalctl -u pki-tomcatd@pki-tomcat の出力	**pki-tomcatd@pki-tomcat** サービスからのエラー
/var/log/pki/pki-tomcat/ca/debug.$DATE.log	公開鍵インフラストラクチャー (PKI) 製品のアクティビティーの大規模な JAVA スタックトレース
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit ログファイル	PKI 製品の監査ログ
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.$DATE.log**	証明書を使用するサービスプリンシパル、ホスト、およびその他のエンティティーの証明書操作の低レベルのデバッグデータ

注記

オプションの CA コンポーネントのインストール中に IdM サーバー全体のインストールに失敗した場合に、ログには CA の詳細が記録されません。全体的なインストールプロセスに失敗したことを示すメッセージが **/var/log/ipaserver-install.log** ファイルに記録されます。Red Hat では、CA インストールの失敗に関する詳細は、上記に記載のログファイルを確認することを推奨します。

CA サービスをインストールしてルート CA が外部 CA の場合は唯一例外で、この動作に該当しません。外部 CA の証明書に問題がある場合は、エラーが **/var/log/ipaserver-install.log** に記録されます。

失敗した IdM CA インストールをトラブルシューティングするには、これらのログファイルの最後でエラーを確認し、その情報を使用して、対応する問題を解決します。

前提条件

- IdM ログファイルの内容を表示するには、**root** 権限が必要である。

手順

1. ログファイルを対話的に確認するには、**less** ユーティリティーを使用してログファイルの最後を開き、↑ および ↓キーを使用して移動し、**ScriptError** を検索します。以下の例では、**/var/log/pki/pki-ca-spawn.$TIME_OF_INSTALLATION.log** を開きます。

```
[user@server ~]$ sudo less -N +G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. 上記のすべてのログファイルを使用してこの確認プロセスを繰り返して、追加のトラブルシューティング情報を収集します。

関連情報

- Red Hat テクニカルサポートサブスクリプションがあり、IdM サーバーのインストール失敗の問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、サーバーの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

9.3. 部分的な IDM サーバーインストールの削除

IdM サーバーのインストールに失敗した場合は、設定ファイルの一部が残される場合があります。IdM サーバーのインストールを再度試みて失敗し、インストールスクリプトでは IPA が設定済みと報告されます。

既存の部分的な IdM 設定を使用したシステムの例

```
[root@server ~]# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-server-install command failed. See /var/log/ipaserver-install.log for more information
```

この問題を解決するには、部分的な IdM サーバー設定をアンインストールし、インストールプロセスを再試行します。

前提条件

- **root** 権限があること。

手順

1. IdM サーバーとして設定するホストから、IdM サーバーソフトウェアをアンインストールします。

```
[root@server ~]# ipa-server-install --uninstall
```

2. インストールに繰り返し失敗したことが原因で IdM サーバーのインストールに問題が生じた場合は、オペレーティングシステムを再インストールします。
カスタマイズなしの新規インストールシステムというのが、IdM サーバーのインストール要件の 1 つとなっています。インストールに失敗した場合は、予期せずにシステムファイルが変更されてホストの整合性が保てない可能性があります。

関連情報

- IdM サーバーのアンインストールの詳細は IdM サーバーのアンインストール を参照してください。
- Red Hat テクニカルサポートサブスクリプションをお持ちで、アンインストールを何度か試みた後にインストールに失敗した場合には、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、サーバーの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

9.4. 関連情報

- IdM レプリカのインストールに関するトラブルシューティング
- IdM クライアントのインストールに関するトラブルシューティング
- IdM のバックアップおよび復元

第10章 IDM サーバーのアンインストール

以下の手順に従って、**server123.idm.example.com** (server123) という名前の Identity Management (IdM) サーバーをアンインストールします。この手順では、他のサーバーが重要なサービスを実行していること、アンインストールを実行する前にトポロジーが引き続き冗長であることを最初に確認します。

前提条件

- server123 への **root** アクセス権限がある。
- IdM 管理者の認証情報がある。

手順

1. IdM 環境で統合 DNS が使用されている場合は、server123 が唯一の **有効な** DNS サーバーではないことを確認してください。

```
[root@server123 ~]# ipa server-role-find --role 'DNS server'
----------------------
2 server roles matched
----------------------
  Server name: server456.idm.example.com
  Role name: DNS server
  Role status: enabled
[...]
----------------------------
Number of entries returned 2
----------------------------
```

   トポロジー内の残りの DNS サーバーが server123 だけの場合は、DNS サーバーロールを別の IdM サーバーに追加します。詳細は、**ipa-dns-install(1)** man ページを参照してください。

2. IdM 環境で統合認証局 (CA) が使用されている場合は、以下を行います。

   a. server123 が唯一の **有効** な CA サーバーではないことを確認します。

```
[root@server123 ~]# ipa server-role-find --role 'CA server'
----------------------
2 server roles matched
----------------------
  Server name: server123.idm.example.com
  Role name: CA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: CA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

   トポロジー内の残りの CA サーバーが server123 だけの場合は、CA サーバーロールを別の IdM サーバーに追加します。詳細は、**ipa-ca-install(1)** man ページを参照してください。

b. IdM 環境で vault を有効にしている場合は、server123.idm.example.com が唯一の **有効な** Key Recovery Authority (KRA) サーバーではないことを確認します。

```
[root@server123 ~]# ipa server-role-find --role 'KRA server'
----------------------
2 server roles matched
----------------------
  Server name: server123.idm.example.com
  Role name: KRA server
  Role status: enabled

  Server name: r8server.idm.example.com
  Role name: KRA server
  Role status: enabled
----------------------------
Number of entries returned 2
----------------------------
```

トポロジー内の残りの KRA サーバーが server123 だけの場合は、KRA サーバーロールを別の IdM サーバーに追加します。詳細は、**man ipa-kra-install(1)** を参照してください。

c. server123.idm.example.com が CA 更新サーバーではないことを確認します。

```
[root@server123 ~]# ipa config-show | grep 'CA renewal'
  IPA CA renewal master: r8server.idm.example.com
```

server123 が CA 更新サーバーである場合は、CA 更新サーバーロールを別のサーバーに移動する方法の詳細について、IdM CA 更新サーバーの変更およびリセット を参照してください。

d. server123.idm.example.com が現在の証明書失効リスト (CRL) パブリッシャーではないことを確認します。

```
[root@server123 ~]# ipa-crlgen-manage status
CRL generation: disabled
```

出力に、CRL の生成が server123 で有効になっていることが示されている場合は、CRL パブリッシャーロールを別のサーバーに移動する方法の詳細について、IdM CA サーバーでの CRL の生成 を参照してください。

3. トポロジー内の別の IdM サーバーに接続します。

```
$ ssh idm_user@server456
```

4. サーバーで、IdM 管理者の認証情報を取得します。

```
[idm_user@server456 ~]$ kinit admin
```

5. トポロジー内のサーバーに割り当てられた DNA ID 範囲を表示します。

```
[idm_user@server456 ~]$ ipa-replica-manage dnarange-show
server123.idm.example.com: 1001-1500
server456.idm.example.com: 1501-2000
[...]
```

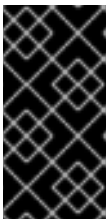
出力は、DNA ID 範囲が server123 と server456 の両方に割り当てられていることを示しています。

6. server123 がトポロジー内で DNA ID 範囲が割り当てられた唯一の IdM サーバーである場合、server456 でテスト IdM ユーザーを作成して、サーバーに DNA ID 範囲が割り当てられていることを確認します。

```
[idm_user@server456 ~]$ ipa user-add test_idm_user
```

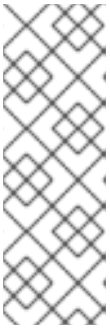
7. トポロジーから server123.idm.example.com を削除します。

```
[idm_user@server456 ~]$ ipa server-del server123.idm.example.com
```



重要

server123 を削除してトポロジーが切断されると、スクリプトが警告を発します。削除を続行できるようにするために、残りのレプリカ間でレプリカ合意を作成する方法は、CLI を使用した 2 台のサーバー間のレプリケーションの設定 を参照してください。



注記

ipa server-del コマンドを実行すると、**ドメイン** と **ca** 接尾辞の両方について、server123 に関連するすべてのレプリケーションデータと合意が削除されます。これは、最初に **ipa-replica-manage del server123** コマンドを使用してこれらのデータを削除する必要があったドメインレベル 0 IdM トポロジーとは対照的です。ドメインレベル 0 の IdM トポロジーは、RHEL 7.2 以前で実行されているトポロジーです。**ipa domainlevel-get** コマンドを使用して、現在のドメインレベルを表示します。

8. server123.idm.example.com に戻り、既存の IdM インストールをアンインストールします。

```
[root@server123 ~]# ipa-server-install --uninstall
...
Are you sure you want to continue with the uninstall procedure? [no]: true
```

9. server123.idm.example.com を指定しているネームサーバー (NS) の DNS レコードがすべて DNS ゾーンから削除されていることを確認してください。使用する DNS が IdM により管理される統合 DNS であるか、外部 DNS であるかに関わらず、確認を行なってください。IdM から DNS レコードを削除する方法は、Deleting DNS records in the IdM CLI を参照してください。

関連情報

- RHEL 7 ドキュメントで のドメインレベルの表示と引き上げ
- レプリカトポロジーの計画
- IdM CA 更新サーバーの説明
- IdM CA サーバーでの CRL の生成

第11章 IDM サーバーの名前変更

既存の Identity Management (IdM) サーバーのホスト名は変更できません。異なる名前のレプリカでサーバーを置き換えます。

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、このレプリカに必要なホスト名と IP アドレスが指定されるようにします。詳細は、IdM 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証明書失効リスト (CRL) パブリッシャーサーバーである場合は、続行する前に別のサーバーを CRL パブリッシャーサーバーに指定してください。

移行手順のコンテキストでこの設定を行う方法は、以下のセクションを参照してください。

- RHEL 7 IdM CA サーバーでの CRL 生成の停止
- 新しい RHEL 8 IdM CA サーバーでの CRL 生成の開始

2. 既存の IdM サーバーインスタンスを停止します。

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

3. IdM 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12章 IDM の更新およびダウンロード

12.1. IDM パッケージの更新

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。

前提条件

- RHEL システムに関連するこれまでにリリース済みのエラータをすべて適用している。詳細は、KCS 記事 RHEL システムにパッケージの更新を適用する方法 を参照してください。

手順

- 以下のオプションのいずれかを選択します。
  - 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-*
```

  - 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するには、次のコマンドを実行します。

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

少なくとも 1 台のサーバーで IdM パッケージを更新すると、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、デプロイメントされたトポロジー、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あ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。

重要

Red Hat は、次のバージョンにアップグレードすることのみを推奨します。たとえば、RHEL 8.8 の IdM にアップグレードする場合は、RHEL 8.7 の IdM からアップグレードすることを推奨します。以前のバージョンからアップグレードすると、問題が発生する可能性があります。

12.2. IDM パッケージのダウングレード

Red Hat は、Identity Management のダウングレードをサポートしていません。

12.3. 関連情報

- **yum(8)** man ページ

第13章 IDM 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 (IdM) 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。

13.1. IDM クライアントのインストールをサポートする RHEL のバージョン

IdM サーバーが Red Hat Enterprise Linux 8 の最新マイナーバージョンで実行されている Identity Management デプロイメントでは、以下の最新マイナーバージョンで実行されているクライアントがサポートされます。

- RHEL 7
- RHEL 8
- RHEL 9

注記

他のクライアントシステム (Ubuntu など) は IdM 8 サーバーと連携できますが、Red Hat では、これらのクライアントのサポートを提供していません。

重要

IdM デプロイメントを FIPS 準拠にする予定の場合、Red Hat は環境を RHEL 9 に移行することを強く推奨します。RHEL 9 は、FIPS 140-3 に準拠する予定の最初の RHEL メジャーバージョンです。

13.2. IDM 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 DNS SRV レコード **_ldap._tcp.DOMAIN** 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** である場合は、インストーラーが **_ldap._tcp.idm.example.com**、**_ldap._tcp.example.com**、および **_ldap._tcp.com** の DNS SRV レコードから IdM 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、IdM 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 IdM サーバーのサブドメインでない場合は、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 コンポーネントと 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、IdM サーバーの自動検出に使用されます。

関連情報

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

13.3. IDM クライアントのポート要件

Identity Management (IdM) クライアントは、IdM 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。

IdM 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、送信パケットにフィルターを設定しないファイアウォールを使用している場合は、ポートを送信方向で使用できます。

関連情報

- 使用されるポートに関する詳細は、IdM のポート要件 を参照してください。

13.4. IDM クライアントの IPV6 要件

Identity Management (IdM) では、IdM に登録するホストのカーネルで **IPv6** プロトコルを有効にする必要はありません。たとえば、内部ネットワークで **IPv4** プロトコルのみを使用する場合には、System Security Services Daemon (SSSD) が **IPv4** だけを使用して IdM サーバーと通信するように設定できます。**/etc/sssd/sssd.conf** ファイルの **[domain/NAME]** セクションに次の行を追加して、これを設定できます。

```
lookup_family_order = ipv4_only
```

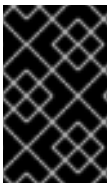
関連情報

- **lookup_family_order** オプションの詳細は、**sssd.conf(5)** の man ページを参照してください。

13.5. IDM:CLIENT ストリームからの IDM クライアントパッケージのインストール

RHEL 8 では、Identity Management (IdM) 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。

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。お使いの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。長期サポート対象の 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。



重要

ホストに IdM レプリカをインストールする予定がある場合は、**idm:client** ストリームを使用しないでください。その場合は、代わりに **idm:DL1** ストリームを使用して ください。

前提条件

- 以前に **idm:DL1** ストリームを有効にし、そこからパッケージをダウンロードした場合は、**idm:client** ストリームに切り替える際に、関連するインストール済みコンテンツをすべて排他的に削除し、**idm:DL1** を無効にしてから、**idm:client** ストリームを有効にする必要があります。
  続行方法の詳細は 後続のストリームへの切り替え を参照してください。

重要

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。

手順

- 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するには、次のコマンドを実行します。

```
# yum module install idm
```

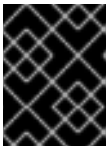
13.6. IDM:DL1 ストリームからの IDM クライアントパッケージのインストール

RHEL 8 では、Identity Management (IdM) 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。

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。

前提条件

- 以前に **idm:client** ストリームを有効にし、そこからパッケージをダウンロードした場合は、**idm:DL1** ストリームに切り替える際に、関連するインストール済みコンテンツをすべて排他的に削除し、**idm:client** を無効にしてから、**idm:DL1** ストリームを有効にする必要がある。続行方法の詳細は 後続のストリームへの切り替え を参照してください。



重要

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。

手順

1. **idm:DL1** ストリーム経由で配信される RPM に切り替えるには、次のコマンドを実行します。

```
# 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するには、次のコマンドを実行します。

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

第14章 IDM クライアントのインストール

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。

Identity Management (IdM) 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認証情報を指定する必要があります。

14.1. 前提条件

- これで、IdM クライアントをインストールするためのシステムが準備できました。詳細については、IdM 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。

14.2. ユーザー認証情報でクライアントのインストール: 対話的なインストール

この手順に従い、登録権限のあるユーザーの認証情報を使用してシステムをドメインに登録し、Identity Management (IdM) クライアントを対話的にインストールします。

前提条件

- クライアントを IdM ドメインに登録する権限を持つユーザーの認証情報がある。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する。

手順

1. IdM 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 --mkhomedir
```

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 IdM 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 --mkhomedir
```

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**
  - **--mkhomedir**

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 (**-**) のみを使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
- ホスト名がすべて小文字である。大文字は使用できません。

- 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。

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、登録管理者 (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.
```

関連情報

- 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、**ipa-client-install**(1) の man ページにある **DNS Autodiscovery** セクションを参照してください。

14.3. ワンタイムパスワードでクライアントのインストール: 対話的なインストール

以下の手順に従って、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 (IdM) クライアントを対話的にインストールします。

前提条件

- ドメインのサーバーに、クライアントシステムを IdM 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。

注記

ipa host-add <client_fqdn> コマンドでは、クライアントの FQDN が DNS を介して解決可能である必要があります。解決できない場合は、**--ip address** オプションを使用して IdM クライアントシステムの IP アドレスを指定するか、**--force** オプションを使用します。

```
$ 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、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. IdM 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。
   --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 --mkhomedir --password=password
```

   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 IdM 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 --mkhomedir
```

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**
  - **--mkhomedir**

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 (**-**) のみを使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
- ホスト名がすべて小文字である。大文字は使用できません。

- 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。

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.
```

関連情報

- 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、**ipa-client-install**(1) の man ページにある **DNS Autodiscovery** セクションを参照してください。

14.4. 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認証情報を指定します。
- **--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。

無人インストールのオプション

--unattended オプション - 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完全修飾ドメイン名 (FQDN) を指定します。

重要

FQDN 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る。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
  - ホスト名がすべて小文字である。大文字は使用できません。

- **--domain** - 既存の IdM デプロイメントのプライマリー DNS ドメインを指定します (例: **example.com**)。この名前は、IdM Kerberos レルム名を小文字で表しています。
- **--server** - 接続する IdM サーバーの FQDN を指定します。このオプションが使用されると、Kerberos の DNS 自動検出が無効になり、KDC および管理サーバーの固定リストが設定されます。通常の状態では、サーバーのリストはプライマリー IdM DNS ドメインから取得されるため、このオプションは必須ではありません。
- **--realm** - 既存の IdM デプロイメントの Kerberos レルムを指定します。通常、IdM インストールで使用するプライマリー DNS ドメインを大文字で表したものです。通常の状態では、レルム名は IdM サーバーから取得されるため、このオプションは必須ではありません。

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' --mkhomedir --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 idm.example.com --server
server.idm.example.com --realm IDM.EXAMPLE.COM --mkhomedir --unattended
```

関連情報

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

14.5. クライアントインストール後に事前設定された IDM の削除

ipa-client-install スクリプトは、**/etc/openldap/ldap.conf** ファイルおよび **/etc/sssd/sssd.conf** ファイルから、以前の LDAP 設定および System Security Services Daemon (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 (IdM) 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 IdM 設定のコメントを解除します。
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。

14.6. IDM クライアントのテスト

コマンドラインインターフェイスにより、**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 (IdM) クライアントが、サーバーに定義し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、サーバーに定義したユーザーを解決できることを確認します。たとえば、デフォルトの **admin** ユーザーを確認するには、次のコマンドを実行します。

```
[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 に切り替えます。

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

14.7. IDM クライアントのインストール時に実行する接続

IdM クライアントのインストール時に実行する要求 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14.1 IdM クライアントのインストール時に実行する要求

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 解決	DNS	IdM サーバーの IP アドレスを検出。(任意) A/AAAA および SSHFP レコードを追加。
IdM レプリカ上のポート 88 (TCP/TCP6 および UDP/UDP6) への要求	Kerberos	Kerberos チケットの取得。
検出または設定された IdM サーバー上の 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) への要求	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。

14.8. インストール後のデプロイメント実行時の IDM 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イス (CLI)
- (**オプション**) ブラウザーベースの Web UI

CLI のインストール後の操作 は、IdM クライアントのインストール後のデプロイメント実行時に CLI により実行される操作を表示します。Web UI のインストール後の操作 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を示します。

表14.2 CLI のインストール後の操作

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 解決	DNS	IdM サーバーの IP アドレス検出。
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) への要求	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 サーバー上の 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14.3 Web UI のインストール後の操作

操作	使用プロトコル	目的
検出または設定された IdM サーバー上の 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。

関連情報

- **SSSD** デーモンが IdM および Active Directory サーバーで利用可能なサービスと通信する方法の詳細は、SSSD 通信パターン を参照してください。
- **certmonger** デーモンが IdM および Active Directory サーバーで利用可能なサービスと通信する方法の詳細は、Certmonger 通信パターン を参照してください。

14.9. SSSD 通信パターン

システムセキュリティーサービスデーモン (System Security Services Daemon: SSSD) 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。Identity Management (IdM) クライアントに設定すると、認証、認可、その他の ID 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 は、複数のサーバーと通信するように設定できます。以下の表は、IdM での SSSD の一般的な通信パターンを示しています。

表14.4 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 解決	DNS	IdM サーバーの IP アドレス検出。

操作	使用プロトコル	目的
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) への要求	Kerberos	Kerberos チケットの取得。Kerberos パスワードの変更。
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) への要求	LDAP	IdM ユーザーおよびホストの情報を取得。HBAC および sudo ルールのダウンロード。マップ、SELinux ユーザーコンテキスト、SSH 公開鍵、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) レスポンダーへの要求 (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14.5 Active Directory ドメインコントローラーとの通信時における信頼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 解決	DNS	IdM サーバーの IP アドレス検出。
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) への要求	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) への要求	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) レスポンダーへの要求 (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。

操作	使用プロトコル	目的

関連情報

- インストール後のデプロイメント実行時の IdM クライアントのサーバーとの通信

14.10. CERTMONGER の通信パターン

Certmonger は、Identity Management (IdM) サーバーおよび 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更新できるようにします。表 14.6「Certmonger の通信パターン」 は、IdM サーバーで **certmonger** ユーティリティーにより実行される操作を示しています。

表14.6 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 解決	DNS	IdM サーバーの IP アドレス検出。
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) への要求	Kerberos	Kerberos チケットの取得。
検出または設定された IdM サーバー上の IdM Apache ベースの Web サービスへの JSON-RPC 呼び出し	HTTPS	新しい証明書の要求。
IdM サーバーのポート 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したサーバー上) IdM サーバーのポート 8443 (TCP/TCP6) でのアクセス	HTTPS	IdM サーバー上での認証局の管理 (IdM サーバーおよびレプリカのインストール時のみ)。サーバーの **certmonger** は、CA 関連の証明書の更新のために、ポート 8080 および 8443 上の独自のローカルサーバーにのみ接続します。

関連情報

- インストール後のデプロイメント実行時の IdM クライアントのサーバーとの通信

第15章 キックスタートによる IDM 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 (IdM) ドメインに追加されます。

15.1. キックスタートによるクライアントのインストール

以下の手順に従って、キックスタートファイルを使用して Identity Management (IdM) クライアントをインストールします。

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. IdM サーバー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、キータブ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、IdM クライアントをインストールします。

15.2. 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

キックスタートファイルを使用して、Identity Management (IdM) クライアントをインストールできます。キックスタートファイルの内容は、こちらで概説されている特定の要件を満たしている必要があります。

インストールするパッケージリストに含まれる 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
...
```

IdM クライアントのインストール後の手順

インストール後の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
  - IdM 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、IdM 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/libexec/openssh/sshd-keygen rsa

# 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
    ```

15.3. IDM クライアントのテスト

コマンドラインインターフェイスにより、**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 (IdM) クライアントが、サーバーに定義し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、サーバーに定義したユーザーを解決できることを確認します。たとえば、デフォルトの **admin** ユーザーを確認するには、次のコマンドを実行します。

```
[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 に切り替えます。

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

第16章 IDM クライアントのインストールに関するトラブルシューティング

次のセクションでは、失敗した IdM クライアントのインストールについての情報を収集する方法、一般的なインストールの問題を解決する方法を説明します。

16.1. IDM クライアントのインストールエラーの確認

Identity Management(IdM) クライアントをインストールすると、デバッグ情報が **/var/log/ipaclient-install.log** に追加されます。クライアントのインストールに失敗した場合には、インストーラーは障害をログに記録し、変更をロールバックしてホストに変更を加えます。インストールが失敗する理由は、インストーラーがロールバック手順も記録するため、ログファイルの最後には存在しない可能性があります。

失敗した IdM クライアントのインストールをトラブルシューティングするには、**/var/log/ipaclient-install.log** ファイルの **ScriptError** とラベルが付いた行を確認し、この情報を使用して、対応する問題を解決します。

前提条件

- IdM ログファイルの内容を表示するには、**root** 権限が必要である。

手順

1. **grep** ユーティリティーを使用して、**/var/log/ipaserver-install.log** ファイルからキーワード **ScriptError** があれば、すべて取得します。

```
[user@server ~]$ sudo grep ScriptError /var/log/ipaclient-install.log
[sudo] password for user:
2020-05-28T18:24:50Z DEBUG The ipa-client-install command failed, exception:
ScriptError: One of password / principal / keytab is required.
```

2. ログファイルを対話的に確認するには、**less** ユーティリティーを使用してログファイルの最後を開き、↑ および ↓キーを使用して移動します。

```
[user@server ~]$ sudo less -N +G /var/log/ipaclient-install.log
```

関連情報

- Red Hat テクニカルサポートサブスクリプションがあり、IdM クライアントのインストール失敗の問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、クライアントの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

16.2. クライアントインストールが DNS レコードの更新に失敗した場合の問題の解決

IdM クライアントインストーラーは、**nsupdate** コマンドで PTR、SSHFP、および追加の DNS レコードを作成します。ただし、クライアントソフトウェアのインストールおよび設定後にクライアントが DNS レコードを更新できない場合には、インストールプロセスは失敗します。

この問題を修正するには、**/var/log/client-install.log** で設定を確認し、DNS エラーを確認します。

前提条件

- IdM 環境の DNS ソリューションとして IdM DNS を使用している。

手順

1. クライアントが所属する DNS ゾーンの動的更新が有効になっていることを確認します。

```
[user@server ~]$ ipa dnszone-mod idm.example.com. --dynamic-update=TRUE
```

2. DNS サービスを実行している IdM サーバーで、TCP プロトコルと UDP プロトコルの両方でポート 53 が開かれていることを確認します。

```
[user@server ~]$ sudo firewall-cmd --permanent --add-port=53/tcp --add-port=53/udp
[sudo] password for user:
success
[user@server ~]$ firewall-cmd --runtime-to-permanent
success
```

3. **grep** ユーティリティーを使用して、**/var/log/client-install.log** から **nsupdate** コマンドの内容を取得し、どの DNS レコードの更新に失敗しているかを確認します。

```
[user@server ~]$ sudo grep nsupdate /var/log/ipaclient-install.log
```

関連情報

- Red Hat テクニカルサポートサブスクリプションがあり、インストール失敗の問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、クライアントの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

16.3. クライアントのインストールが IDM KERBEROS レルムへの参加に失敗した場合の問題の解決

クライアントが IdM Kerberos レルムに参加できない場合には、IdM クライアントのインストールプロセスに失敗します。

```
Joining realm failed: Failed to add key to the keytab
child exited with 11

Installation failed. Rolling back changes.
```

空の Kerberos キータブが原因で、これに失敗します。

前提条件

- システムファイルを削除するには、**root** 権限が必要です。

手順

1. **/etc/krb5.keytab** を削除します。

```
[user@client ~]$ sudo rm /etc/krb5.keytab
[sudo] password for user:
[user@client ~]$ ls /etc/krb5.keytab
ls: cannot access '/etc/krb5.keytab': No such file or directory
```

2. IdM クライアントのインストールを再試行します。

関連情報

- Red Hat テクニカルサポートサブスクリプションがあり、インストール失敗の問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、クライアントの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

16.4. 関連情報

- 最初の IdM サーバーのインストールに関するトラブルシューティングは、IdM サーバーのインストールに関するトラブルシューティング を参照してください。
- IdM レプリカのインストールに関するトラブルシューティングは、IdM レプリカのインストールに関するトラブルシューティング を参照してください。

第17章 IDM 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、クライアントマシンが破壊され、IdM サーバーとの接続が失われた場合は、キータブがあればクライアントを再登録できます。この場合は、同じホスト名でクライアントを IdM 環境に戻します。

17.1. IDM における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、クライアントマシンが破壊され、IdM サーバーとの接続が失われた場合は、キータブがあればクライアントを再登録できます。この場合は、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鍵 (Kerberos および SSH) 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、IdM では、LDAP にあるクライアントのエントリーのキー属性が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、クライアントの鍵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 IdM クライアントシステムの名前変更 を参照してください。

クライアント再登録中に行われること

再登録時に、IdM は以下を行います。

- 元のホスト証明書を破棄する。
- 新規の SSH 鍵を作成する。
- 新規のキータブを生成する。

17.2. ユーザー認証情報でクライアントの再登録: 対話的な再登録

以下の手順に従って、承認されたユーザーのクレデンシャルを使用して、Identity Management (IdM) クライアントを対話的に再登録します。

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、登録管理者 (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:
```

関連情報

- 許可されたユーザーの認証情報を使用してクライアントを登録する方法は、ユーザー認証情報で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。

17.3. クライアントのキータブでクライアントの再登録: 非対話的な再登録

前提条件

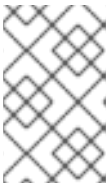
- **/tmp** や **/root** などのディレクトリーに元のクライアントキータブファイルをバックアップします。

手順

以下の手順に従って、クライアントシステムのキータブを使用して、Identity Management (IdM) クライアントを非対話的に再登録します。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. 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/** ディレクトリーにキータブファイルをコピーします。
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。

17.4. IDM クライアントのテスト

コマンドラインインターフェイスにより、**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 (IdM) クライアントが、サーバーに定義し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、サーバーに定義したユーザーを解決できることを確認します。たとえば、デフォルトの **admin** ユーザーを確認するには、次のコマンドを実行します。

```
[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 に切り替えます。

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

第18章 IDM 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 (IdM) クライアントを削除できます。

18.1. IDM 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、クライアントが Identity Management (IdM) ドメインから削除され、SSSD (System Security Services Daemon) などの特定のシステムサービスの IdM 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** コマンドを入力します。

```
[root@client ~]# ipa-client-install --uninstall
```

2. (オプション) IdM ユーザーの Kerberos Ticket-granting Ticket (TGT) を取得できないことを確認します。

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@client ~]#
```

Kerberos TGT チケットが正常に返された場合には、IdM クライアントのアンインストール: 以前に複数回インストールを行った場合の追加手順 にあるアンインストール手順を実行してください。

3. クライアントで、特定した Keytab から以前の Kerberos プリンシパル (**/etc/krb5.keytab** を除く) を削除します。

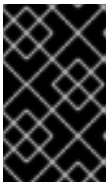
```
[root@client ~]# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.COM
```

4. IdM サーバーで、IdM からクライアントホストの DNS エントリーをすべて削除します。

```
[root@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): true
----------------------
Deleted record "old-client-name"
```

5. IdM サーバーで、IdM LDAP サーバーからクライアントホストエントリーを削除します。これにより、すべてのサービスが削除され、そのホストに発行されたすべての証明書が無効になります。

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



重要

クライアントホストエントリーを、別の IP アドレスまたは別のホスト名を使用して今後再登録する場合に、IdM LDAP サーバーからクライアントホストエントリーを削除することが重要です。

18.2. IDM クライアントのアンインストール: 以前に複数回インストールを行った場合の追加手順

ホストを Identity Management (IdM) クライアントとして複数回、インストールしてアンインストールすると、アンインストール手順で IdM Kerberos 設定が復元されない可能性があります。

このような場合は、IdM Kerberos 設定を手動で削除する必要があります。極端なケースでは、オペレーティングシステムを再インストールする必要があります。

前提条件

- **ipa-client-install --uninstall** コマンドを使用して、ホストから IdM クライアント設定をアンインストールしている。ただし、IdM サーバーから IdM ユーザーの Kerberos Ticket-granting Ticket (TGT) をまだ取得できます。
- **/var/lib/ipa-client/sysrestore** ディレクトリーが空で、ディレクトリー内のファイルを使用してシステムの以前の IdM クライアント設定を復元できないことを確認している。

手順

1. **/etc/krb5.conf.ipa** ファイルを確認します。
   - **/etc/krb5.conf.ipa** ファイルの内容が、IdM クライアントのインストール前の **krb5.conf** ファイルの内容と同じ場合は、以下の手順を実行します。
     i. **/etc/krb5.conf** ファイルを削除します。

     ```
     # rm /etc/krb5.conf
     ```

     ii. **/etc/krb5.conf.ipa** ファイルの名前を **/etc/krb5.conf** に変更します。

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - **/etc/krb5.conf.ipa** ファイルの内容が、IdM クライアントのインストール前の **krb5.conf** ファイルの内容と同じでない場合には、オペレーティングシステムのインストール直後の状態には Kerberos 設定を復元できます。
     i. **krb5-libs** パッケージを再インストールします。

     ```
     # yum reinstall krb5-libs
     ```

     このコマンドは、依存関係として **krb5-workstation** パッケージと、**/etc/krb5.conf** ファイルの元のバージョンを再インストールします。
2. **var/log/ipaclient-install.log** ファイルが存在する場合は削除します。

検証手順

- IdM ユーザー認証情報の取得を試みます。取得には失敗するはずです。

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial
credentials
[root@r8server ~]#
```

/etc/krb5.conf ファイルは、出荷時状態に復元されています。したがって、ホスト上の IdM ユーザーの Kerberos TGT を取得できません。

第19章 IDM クライアントシステムの名前変更

ここでは、Identity Management (IdM) 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。

IdM クライアントの名前を変更するには、以下を行います。

1. ホストを準備します。詳細は、名前を変更するための IdM クライアントの準備 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。詳しくは 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。詳しくは クライアントの名前の変更 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。詳しくは 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。詳しく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。

19.1. 名前を変更するための IDM クライアントの準備

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書き留めます。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

- マシンで実行し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
```

19.2. IDM 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、クライアントが Identity Management (IdM) ドメインから削除され、SSSD (System Security Services Daemon) などの特定のシステムサービスの IdM 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** コマンドを入力します。

```
[root@client ~]# ipa-client-install --uninstall
```

2. (オプション) IdM ユーザーの Kerberos Ticket-granting Ticket (TGT) を取得できないことを確認します。

```
[root@client ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@client ~]#
```

Kerberos TGT チケットが正常に返された場合には、IdM クライアントのアンインストール: 以前に複数回インストールを行った場合の追加手順 にあるアンインストール手順を実行してください。

3. クライアントで、特定した Keytab から以前の Kerberos プリンシパル (**/etc/krb5.keytab** を除く) を削除します。

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

4. IdM サーバーで、IdM からクライアントホストの DNS エントリーをすべて削除します。

```
[root@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): true
----------------------
Deleted record "old-client-name"
```

5. IdM サーバーで、IdM LDAP サーバーからクライアントホストエントリーを削除します。これにより、すべてのサービスが削除され、そのホストに発行されたすべての証明書が無効になります。

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

重要

クライアントホストエントリーを、別の IP アドレスまたは別のホスト名を使用して今後再登録する場合に、IdM LDAP サーバーからクライアントホストエントリーを削除することが重要です。

19.3. IDM クライアントのアンインストール: 以前に複数回インストールを行った場合の追加手順

ホストを Identity Management (IdM) クライアントとして複数回、インストールしてアンインストールすると、アンインストール手順で IdM Kerberos 設定が復元されない可能性があります。

このような場合は、IdM Kerberos 設定を手動で削除する必要があります。極端なケースでは、オペレーティングシステムを再インストールする必要があります。

前提条件

- **ipa-client-install --uninstall** コマンドを使用して、ホストから IdM クライアント設定をアンインストールしている。ただし、IdM サーバーから IdM ユーザーの Kerberos Ticket-granting Ticket (TGT) をまだ取得できます。
- **/var/lib/ipa-client/sysrestore** ディレクトリーが空で、ディレクトリー内のファイルを使用してシステムの以前の IdM クライアント設定を復元できないことを確認している。

手順

1. **/etc/krb5.conf.ipa** ファイルを確認します。
   - **/etc/krb5.conf.ipa** ファイルの内容が、IdM クライアントのインストール前の **krb5.conf** ファイルの内容と同じ場合は、以下の手順を実行します。
     i. **/etc/krb5.conf** ファイルを削除します。

     ```
     # rm /etc/krb5.conf
     ```

     ii. **/etc/krb5.conf.ipa** ファイルの名前を **/etc/krb5.conf** に変更します。

     ```
     # mv /etc/krb5.conf.ipa /etc/krb5.conf
     ```

   - **/etc/krb5.conf.ipa** ファイルの内容が、IdM クライアントのインストール前の **krb5.conf** ファイルの内容と同じでない場合には、オペレーティングシステムのインストール直後の状態には Kerberos 設定を復元できます。
     i. **krb5-libs** パッケージを再インストールします。

     ```
     # yum reinstall krb5-libs
     ```

     このコマンドは、依存関係として **krb5-workstation** パッケージと、**/etc/krb5.conf** ファイルの元のバージョンを再インストールします。
2. **var/log/ipaclient-install.log** ファイルが存在する場合は削除します。

検証手順

- IdM ユーザー認証情報の取得を試みます。取得には失敗するはずです。

```
[root@r8server ~]# kinit admin
kinit: Client 'admin@EXAMPLE.COM' not found in Kerberos database while getting initial credentials
[root@r8server ~]#
```

/etc/krb5.conf ファイルは、出荷時状態に復元されています。したがって、ホスト上の IdM ユーザーの Kerberos TGT を取得できません。

19.4. 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 (IdM) クライアントを IdM ドメインに再インストールできるようになります。

19.5. IDM クライアントの再インストール

クライアントのインストール 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。

19.6. 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

手順

1. Identity Management (IdM) サーバーで、名前を変更するための IdM クライアントの準備 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. 名前を変更するための IdM クライアントの準備 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。
   - IdM 管理ツールの使用
   - **certmonger** ユーティリティーの使用
3. 名前を変更するための IdM クライアントの準備 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20章 IDM 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 (IdM) レプリカのインストール要件を取り上げます。インストールの前に、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. ターゲットシステムが、IdM サーバーのインストールに関する一般的な要件を満たしている ことを確認してください。
2. ターゲットシステムが、IdM レプリカのインストールに関する追加のバージョン要件を満たしている ことを確認してください。
3. ターゲットシステムを IdM ドメインに登録する権限を付与します。詳細については、ニーズに最適な次のセクションのいずれかを参照してください。
   - IdM クライアントでのレプリカのインストールの認可
   - IdM に登録されていないシステムでのレプリカのインストールの認可

関連情報

- レプリカトポロジーの計画

20.1. 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 以降で実行している Identity Management (IdM) サーバ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 以降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 IdM を実行している必要があります。以下に例を示します。

- Red Hat Enterprise Linux 8 に IdM サーバーをインストールし、IdM 4.x パッケージを使用している。
- レプリカが Red Hat Enterprise Linux 8 以降にインストールされ、バージョン 4.x 以降の IdM を使用している。

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。

IdM ソフトウェアバージョンの表示方法は、IdM ソフトウェアのバージョンを表示する方法 を参照してください。

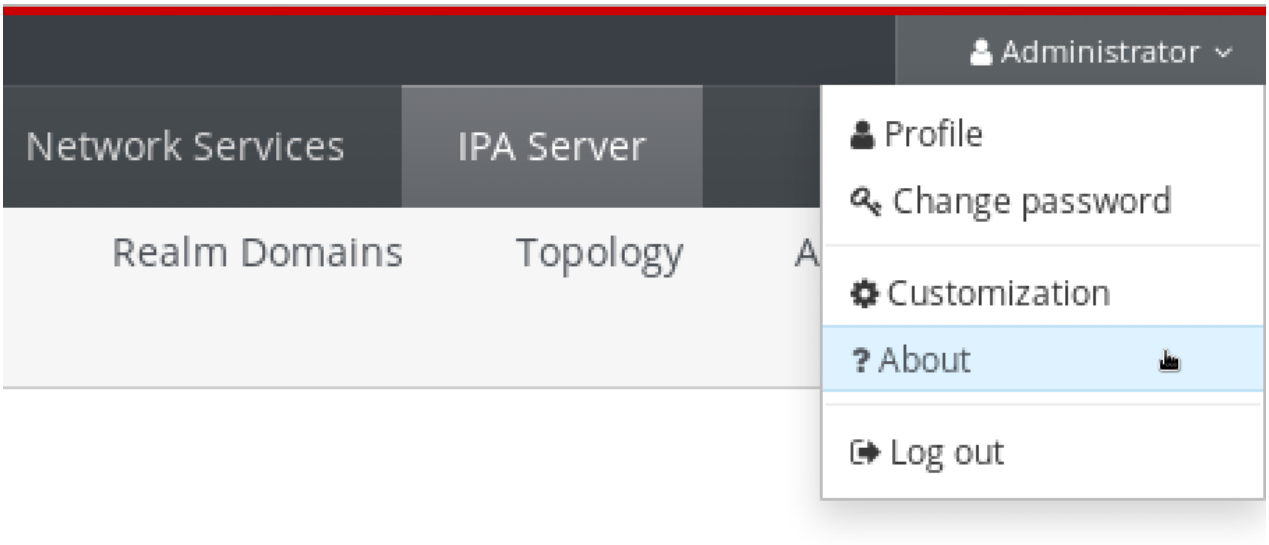
20.2. IDM ソフトウェアのバージョンを表示する方法

IdM バージョン番号は次の方法で表示できます。

- IdM WebUI
- **ipa** コマンド
- **rpm** コマンド

WebUI を介したバージョンの表示

IdM WebUI では、右上のユーザー名メニューから **About** を選択して、ソフトウェアバージョンを表示できます。



ipa コマンドによるバージョンの表示

コマンドラインから、**ipa --version** コマンドを使用します。

```
[root@server ~]# ipa --version
VERSION: 4.8.0, API_VERSION: 2.233
```

rpm コマンドによるバージョンの表示

IdM サービスが適切に動作していない場合は、**rpm** ユーティリティーを使用して、現在インストールされている **ipa-server** パッケージのバージョン番号を確認できます。

```
[root@server ~]# rpm -q ipa-server
ipa-server-4.8.0-11.module+el8.1.0+4247+9f3fd721.x86_64
```

20.3. IDM クライアントでのレプリカのインストールの認可

ipa-replica-install ユーティリティーを実行して既存の Identity Management (IdM) クライアントを レプリカのインストール する場合は、以下の **方法 1** または **方法 2** を選択して、レプリカのインストールを認証します。以下のいずれかが当てはまる場合は、**方法 1** を選択します。

- 上級システム管理者に手順の初期部分を実行させ、下級システム管理者にその他の作業を実行させたい場合。
- レプリカのインストールを自動化する。

方法 1 - ipaservers ホストグループ

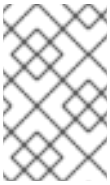
1. IdM 管理者として IdM ホストにログインします。

```
$ kinit admin
```

2. クライアントマシンを **ipaservers** ホストグループに追加します。

```
$ ipa hostgroup-add-member ipaservers --hosts client.idm.example.com
  Host-group: ipaservers
```

```
  Description: IPA server hosts
  Member hosts: server.idm.example.com, client.idm.example.com
-------------------------
Number of members added 1
-------------------------
```



注記

ipaservers グループのメンバーシップは、管理者の認証情報と同様に、マシンに昇格した特権を付与します。したがって、次の手順では、**ipa-replica-install** ユーティリティーを、経験豊富ではないシステム管理者が、ホストで正常に実行できます。

方法 2 - 特権ユーザーの認証情報

特権ユーザーの認証情報を提供することで、レプリカのインストールを認可するには、以下のいずれかの方法を選択します。

- **ipa-replica-install** ユーティリティーを起動したら、Identity Management (IdM) から認証情報の入力を求められます。これがデフォルトの動作です。
- **ipa-replica-install** ユーティリティーを実行する直前に、特権ユーザーとしてクライアントにログインします。デフォルトの特権ユーザーは **admin** です。

```
$ kinit admin
```

関連情報

- インストール手順を開始する方法は、IdM レプリカのインストール を参照してください。
- Ansible Playbook を使用して、IdM レプリカをインストールできます。詳細は Ansible Playbook を使用した Identity Management レプリカのインストール を参照してください。

20.4. IDM に登録されていないシステムでのレプリカのインストールの認可

Identity Management (IdM) ドメインに登録されていないシステムで レプリカのインストール を行う場合、**ipa-replica-install** ユーティリティーはまず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。このシナリオでは、以下の **方法 1** または **方法 2** を選択して、レプリカのインストールを認証します。以下のいずれかが当てはまる場合は、**方法 1** を選択します。

- 上級システム管理者に手順の初期部分を実行させ、下級システム管理者にその他の作業を実行させたい場合。
- レプリカのインストールを自動化する。

方法 1 - IdM サーバーで生成されたランダムなパスワード

ドメイン内の任意のサーバーで、次のコマンドを入力します。

1. 管理者としてログインします。

```
$ kinit admin
```

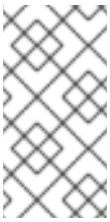
2. 外部システムを IdM ホストとして追加します。**ipa host-add** コマンドに **--random** オプションを使用して、後続のレプリカのインストールに使用される無作為なワンタイムパスワードを生成します。

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

生成されたパスワードは、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。

3. システムを **ipaservers** ホストグループに追加します。

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



注記

ipaservers グループのメンバーシップは、管理者の認証情報と同様に、マシンに昇格した特権を付与します。したがって、次の手順では、生成されたランダムパスワードを提供する経験豊富ではないシステム管理者により、ホストで **ipa-replica-install** ユーティリティーを正常に実行できます。

方法 2 - 特権ユーザーの認証情報

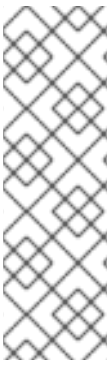
この方法を使用し、特権ユーザーの認証情報を提供してレプリカのインストールを承認してください。デフォルトの特権ユーザーは **admin** です。
IdM レプリカインストールユーティリティーを実行する前に、アクションは必要ありません。インストール時に、**ipa-replica-install** コマンドにプリンシパル名およびパスワードのオプション (**--principal admin --admin-password パスワード**) を直接追加します。

関連情報

- インストール手順を開始する方法は、IdM レプリカのインストール を参照してください。
- Ansible Playbook を使用して、IdM レプリカをインストールできます。詳細は Ansible Playbook を使用した Identity Management レプリカのインストール を参照してください。

第21章 IDM レプリカのインストール

次のセクションでは、コマンドラインインターフェイス (CLI) を使用して、Identity Management (IdM) レプリカを対話的に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、その設定を基にしてレプリカをインストールします。



注記

Red Hat は、Ansible ロールを使用してレプリカをインストールする ことを推奨します。Ansible ロールを使用すると、常に複数のレプリカをインストールし、カスタマイズできます。

Ansible を使用しない対話型および非対話型のメソッドは、レプリカの準備がユーザーまたはサードパーティーに委任される場合などのトポロジーで役に立ちます。これらの方法は、Ansible コントローラーノードからアクセスできない地理的に分散されたトポロジーでも使用できます。

前提条件

- 一度に 1 つの IdM レプリカがインストールされている。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。
- システムで IdM レプリカのインストールの準備 が完了していることを確認します。

重要

この準備を行わないと、IdM レプリカのインストールに失敗します。

各タイプの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 および CA を使用した IdM レプリカのインストール」
- 「統合 DNS を使用し CA を省略した IdM レプリカのインストール」
- 「統合 DNS を省略し CA を使用した IdM レプリカのインストール」
- 「統合 DNS および CA を使用しない IdM レプリカのインストール」
- 「IdM 非表示レプリカのインストール」

レプリカのインストール手順をトラブルシューティングするには、以下を参照してください。

- *22章IdM レプリカのインストールに関するトラブルシューティング*

インストール後は、以下を参照してください。

- 「IdM レプリカのテスト」
- IdM のバックアップおよび復元

21.1. 統合 DNS および CA を使用した IDM レプリカのインストール

以下の手順に従って、Identity Management (IdM) レプリカをインストールします。

- 統合 DNS あるサーバー

- 認証局 (CA) あり

これは、たとえば、統合 CA で IdM サーバーをインストールした後に、耐障害性のために CA サービスを複製します。

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 IdM CA がルート CA として含まれている場合は、新しいレプリカも統合 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** オプションを含めると、初期サーバーの CA 設定がコピーされます。

前提条件

- システムで IdM レプリカのインストールの準備 が完了していることを確認します。

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。
   - レプリカを DNS サーバーとして設定する **--setup-dns**
   - **--forwarder** - サーバーごとのフォワーダーを指定します。サーバーごとのフォワーダーを使用しない場合は **--no-forwarder** を指定します。フェイルオーバーのためにサーバーごとのフォワーダーを複数指定するには、**--forwarder** を複数回使用します。

     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、**ipa-replica-install**(1) の man ページを参照してください。

   - レプリカに CA を含める **--setup-ca**

   たとえば、IdM サーバーが管理していないすべての DNS 要求を、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 サーバーおよび CA にレプリカをセットアップするには、次のコマンドを実行します。

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

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 IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **ipa.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

   重要

   IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

21.2. 統合 DNS を使用し CA を省略した IDM レプリカのインストール

以下の手順に従って、Identity Management (IdM) レプリカをインストールします。

- 統合 DNS あるサーバー
- 認証局 (CA) がすでにインストールされている IdM 環境に CA がない場合。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 IdM サーバーに転送します。

前提条件

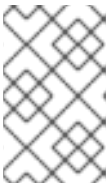
- システムで IdM レプリカのインストールの準備 が完了していることを確認します。

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。
   - レプリカを DNS サーバーとして設定する **--setup-dns**
   - **--forwarder** - サーバーごとのフォワーダーを指定します。サーバーごとのフォワーダーを使用しない場合は **--no-forwarder** を指定します。フェイルオーバーのためにサーバーごとのフォワーダーを複数指定するには、**--forwarder** を複数回使用します。

   たとえば、IdM サーバーが管理していないすべての DNS 要求を、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 サーバーにレプリカをセットアップするには、次のコマンドを実行します。

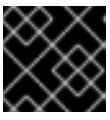
   ```
   # ipa-replica-install --setup-dns --forwarder 192.0.2.1
   ```

   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、**ipa-replica-install**(1) の man ページを参照してください。

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 IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **ipa.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

   重要

   IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

21.3. 統合 DNS を省略し CA を使用した IDM レプリカのインストール

以下の手順に従って、Identity Management (IdM) レプリカをインストールします。

- 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 IdM CA がルート CA として含まれている場合は、新しいレプリカも統合 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** オプションを含めると、初期サーバーの CA 設定がコピーされます。

前提条件

- システムで IdM レプリカのインストールの準備 が完了していることを確認します。

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
```

2. 新規作成された IdM DNS サービスレコードを DNS サーバーに追加します。
   a. IdM DNS サービスレコードを **nsupdate** 形式のファイルにエクスポートします。

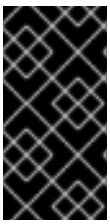
```
$ ipa dns-update-system-records --dry-run --out dns_records_file.nsupdate
```

   b. **nsupdate** ユーティリティーおよび **dns_records_file.nsupdate** ファイルを使用して DNS サーバーに DNS 更新リクエストを送信します。詳細は、RHEL 7 ドキュメントの nsupdate を使用した外部 DNS レコード更新 を参照してください。または、DNS レコードの追加については、お使いの DNS サーバーのドキュメントを参照してください。

21.4. 統合 DNS および CA を使用しない IDM レプリカのインストール

以下の手順に従って、Identity Management (IdM) レプリカをインストールします。

- 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。最初のサーバーが CA なしでインストールされている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。

前提条件

- システムで IdM レプリカのインストールの準備 が完了していることを確認します。

手順

- **ipa-replica-install** を実行して、次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**

  このような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 IdM 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-pin secret \
   --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、インストールした最初のサーバーから証明書のこの部分を自動的に取得します。

21.5. IDM 非表示レプリカのインストール

非表示の (予期しない) レプリカは、実行中で利用可能なサービスをすべて備えた Identity Management (IdM) サーバーです。ただし、DNS に SRV レコードがなく、LDAP サーバーロールが有効になっていません。そのため、クライアントはサービス検出を使用して非表示のレプリカを検出することができません。

非表示のレプリカの詳細は、The hidden replica mode を参照してください。

前提条件

- システムで IdM レプリカのインストールの準備 が完了していることを確認します。

手順

- 非表示のレプリカをインストールするには、次のコマンドを実行します。

```
ipa-replica-install --hidden-replica
```

このコマンドは、DNS SRV レコードがなく、LDAP サーバーのロールが無効になっているレプリカをインストールすることに注意してください。

また、既存のレプリカモードを非表示にすることもできます。詳細は 非表示レプリカの降格または昇格 を参照してください。

21.6. IDM 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どうかを確認します。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
```

21.7. IDM レプリカのインストール時に実行する接続

IdM レプリカのインストール時に実行する要求 には、Identity Management (IdM) のレプリカインストールツールである **ipa-replica-install** により実行される操作のリストが記載されています。

表21.1 IdM レプリカのインストール時に実行する要求

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 解決	DNS	IdM サーバーの IP アドレス検出。
検出された IdM サーバーのポート 88 (TCP/TCP6 および UDP/UDP6) への要求	Kerberos	Kerberos チケットの取得。
検出または設定された IdM サーバー上の 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。
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) への要求	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) への要求	SSH	接続が機能していることを確認。
(任意) IdM サーバーのポート 8443 (TCP/TCP6) でのアクセス	HTTPS	IdM サーバー上での認証局の管理 (IdM サーバーおよびレプリカのインストール時のみ)

第22章 IDM レプリカのインストールに関するトラブルシューティング

以下のセクションでは、失敗した IdM レプリカのインストールに関する情報を収集するプロセスと、一般的なインストールの問題を解決する方法を説明します。

22.1. IDM レプリカのインストールエラーログファイル

Identity Management (IdM) レプリカをインストールすると、**レプリカ** の以下のログファイルにデバッグ情報が追加されます。

- **/var/log/ipareplica-install.log**
- **/var/log/ipareplica-conncheck.log**
- **/var/log/ipaclient-install.log**
- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-INSTANCE-NAME/access**
- **/var/log/dirsrv/slapd-INSTANCE-NAME/errors**
- **/var/log/ipaserver-install.log**

レプリカのインストールプロセスでは、レプリカが接続している IdM **サーバー** の次のログファイルにデバッグ情報を追加します。

- **/var/log/httpd/error_log**
- **/var/log/dirsrv/slapd-INSTANCE-NAME/access**
- **/var/log/dirsrv/slapd-INSTANCE-NAME/errors**

各ログファイルの最後の行では成功または失敗を報告し、**ERROR** および **DEBUG** エントリーで追加のコンテキストを把握できます。

関連情報

- IdM レプリカのインストールエラーの確認

22.2. IDM レプリカのインストールエラーの確認

IdM レプリカのインストールの失敗をトラブルシューティングするには、新しいレプリカとサーバーのインストールエラーログファイルの最後にあるエラーを確認し、この情報を使用して対応する問題を解決します。

前提条件

- IdM ログファイルの内容を表示するには、**root** 権限が必要である。

手順

1. **tail** コマンドを使用して、プライマリーログファイル **/var/log/ipareplica-install.log** からの最新のエラーを表示します。以下の例は、最後の 10 行を表示しています。

```
[user@replica ~]$ sudo tail -n 10 /var/log/ipareplica-install.log
[sudo] password for user:
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 424, in
decorated
  func(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 785, in
promote_check
  ensure_enrolled(installer)
File "/usr/lib/python3.6/site-packages/ipaserver/install/server/replicainstall.py", line 740, in
ensure_enrolled
  raise ScriptError("Configuration of client side components failed!")

2020-05-28T18:24:51Z DEBUG The ipa-replica-install command failed, exception:
ScriptError: Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR Configuration of client side components failed!
2020-05-28T18:24:51Z ERROR The ipa-replica-install command failed. See
/var/log/ipareplica-install.log for more information
```

2. ログファイルを対話的に確認するには、**less** ユーティリティーを使用してログファイルの最後を開き、↑ および ↓キーを使用して移動します。

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-install.log
```

3. (オプション) **/var/log/ipareplica-install.log** は、レプリカのインストールの主なログファイルですが、レプリカおよびサーバーの追加のファイルを使用して、このレビュープロセスを繰り返して、追加のトラブルシューティング情報を収集できます。

   レプリカの場合:

```
[user@replica ~]$ sudo less -N +G /var/log/ipareplica-conncheck.log
[user@replica ~]$ sudo less -N +G /var/log/ipaclient-install.log
[user@replica ~]$ sudo less -N +G /var/log/httpd/error_log
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@replica ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
[user@replica ~]$ sudo less -N +G /var/log/ipaserver-install.log
```

   サーバーの場合:

```
[user@server ~]$ sudo less -N +G /var/log/httpd/error_log
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/access
[user@server ~]$ sudo less -N +G /var/log/dirsrv/slapd-INSTANCE-NAME/errors
```

関連情報

- IdM レプリカのインストールエラーログファイル
- Red Hat テクニカルサポートサブスクリプションがあり、IdM レプリカのインストールが失敗する問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、レプリカの **sosreport** サーバーとレプリカの **sosreport** を提供します。

- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

22.3. IDM CA インストールエラーログファイル

Identity Management (IdM) レプリカに認証局 (CA) サービスをインストールすると、レプリカの複数の場所にデバッグ情報と、レプリカが通信する IdM サーバーが追加されます。

表22.1 レプリカの場合 (推奨される優先順位):

場所	説明
/var/log/pki/pki-ca-spawn.$TIME_OF_INSTALLATION.log	問題の概要と、**pkispawn** インストールプロセスの Python トレース
journalctl -u pki-tomcatd@pki-tomcat の出力	**pki-tomcatd@pki-tomcat** サービスからのエラー
/var/log/pki/pki-tomcat/ca/debug.$DATE.log	公開鍵インフラストラクチャー (PKI) 製品のアクティビティーの大規模な JAVA スタックトレース
/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit	PKI 製品の監査ログ
• **/var/log/pki/pki-tomcat/ca/system** • **/var/log/pki/pki-tomcat/ca/transactions** • **/var/log/pki/pki-tomcat/catalina.$DATE.log**	証明書を使用するサービスプリンシパル、ホスト、およびその他のエンティティーの証明書操作の低レベルのデバッグデータ

レプリカが問い合わせするサーバー:

- **/var/log/httpd/error_log** ログファイル

既存の IdM レプリカに CA サービスをインストールすると、以下のログファイルにデバッグ情報が書き込まれます。

- **/var/log/ipareplica-ca-install.log** ログファイル

注記

オプションの CA コンポーネントのインストール中に IdM レプリカ全体のインストールに失敗した場合に、ログには CA の詳細が記録されません。全体的なインストールプロセスに失敗したことを示すメッセージが **/var/log/ipareplica-install.log** ファイルに記録されます。Red Hat では、CA インストールの失敗に関する詳細は、上記に記載のログファイルを確認することを推奨します。

CA サービスをインストールしてルート CA が外部 CA の場合は唯一例外で、この動作に該当しません。外部 CA の証明書に問題がある場合は、エラーは **/var/log/ipareplica-install.log** に記録されます。

関連情報

- IdM CA インストールエラーの確認

22.4. IDM CA インストールエラーの確認

IdM CA インストールの失敗をトラブルシューティングするには、CA インストールエラーログファイルの最後にあるエラーを確認し、この情報を使用して対応する問題を解決します。

前提条件

- IdM ログファイルの内容を表示するには、**root** 権限が必要である。

手順

1. ログファイルを対話的に確認するには、**less** ユーティリティーを使用してログファイルの最後を開き、↑ および ↓キーを使用して移動し、**ScriptError** を検索します。以下の例では、**/var/log/pki/pki-ca-spawn.$TIME_OF_INSTALLATION.log** を開きます。

```
[user@server ~]$ sudo less -N +G /var/log/pki/pki-ca-spawn.20200527185902.log
```

2. すべての CA インストールエラーログファイルでこのレビュープロセスを繰り返して、追加のトラブルシューティング情報を収集します。

関連情報

- IdM CA インストールエラーログファイル
- Red Hat テクニカルサポートサブスクリプションがあり、IdM サーバーのインストール失敗の問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、サーバーの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

22.5. 部分的な IDM レプリカインストールの削除

IdM レプリカのインストールに失敗した場合は、設定ファイルの一部が残される可能性があります。IdM レプリカのインストールを試みる追加の試行に失敗し、インストールスクリプトで IPA がすでに設定されていると報告されます。

既存の部分的な IdM 設定を使用したシステムの例

```
[root@server ~]# ipa-replica-install
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

IPA server is already configured on this system.
If you want to reinstall the IPA server, please uninstall it first using 'ipa-server-install --uninstall'.
The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

この問題を解決するには、レプリカから IdM ソフトウェアをアンインストールし、IdM トポロジーからレプリカを削除し、インストールプロセスを再試行します。

前提条件

- **root** 権限があること。

手順

1. IdM レプリカとして設定するホストで IdM サーバーソフトウェアをアンインストールします。

```
[root@replica ~]# ipa-server-install --uninstall
```

2. トポロジー内の他のすべてのサーバーで **ipa server-del** コマンドを使用して、適切にインストールされていないレプリカへの参照を削除します。

```
[root@other-replica ~]# ipa server-del replica.idm.example.com
```

3. レプリカのインストールを試行します。

4. インストールに繰り返し失敗したことが原因で IdM レプリカのインストールに問題が生じた場合は、オペレーティングシステムを再インストールします。
カスタマイズなしの新規インストールシステムというのが、IdM レプリカのインストール要件の 1 つとなっています。インストールに失敗した場合は、予期せずにシステムファイルが変更されてホストの整合性が保てない可能性があります。

関連情報

- IdM レプリカのアンインストールの詳細は IdM レプリカのアンインストール を参照してください。

- Red Hat テクニカルサポートサブスクリプションをお持ちで、アンインストールを何度か試みた後にインストールに失敗した場合には、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、レプリカの **sosreport** およびサーバーの **sosreport** を提供します。

- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

22.6. 無効な認証情報エラーの解決

IdM レプリカのインストールが **Invalid credentials** エラーで失敗すると、ホスト上のシステムクロックが相互に同期しなくなる可能性があります。

```
[27/40]: setting up initial replication
Starting replication, please wait until this has completed.
Update in progress, 15 seconds elapsed
[ldap://server.example.com:389] reports: Update failed! Status: [49 - LDAP error: Invalid credentials]

[error] RuntimeError: Failed to start replication
Your system may be partly configured.
Run /usr/sbin/ipa-server-install --uninstall to clean up.

ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    Failed to start replication
ipa.ipapython.install.cli.install_tool(CompatServerReplicaInstall): ERROR    The ipa-replica-install command failed. See /var/log/ipareplica-install.log for more information
```

クロックと同期されていないタイミングで、**--no-ntp** または **-N** オプションを使用して、レプリカのインストールを試みると、サービスは Kerberos で認証できないため、インストールに失敗します。

この問題を解決するには、両方のホストのクロックを同期し、インストールプロセスを再試行します。

前提条件

- システム時間を変更するには、**root** 権限が必要です。

手順

1. システムクロックは、手動または **chronyd** により同期します。

   手動同期

   サーバー上のシステム時間を表示し、この時間と一致するようにレプリカの時間設定します。

   ```
   [user@server ~]$ date
   Thu May 28 21:03:57 EDT 2020

   [user@replica ~]$ sudo timedatectl set-time '2020-05-28 21:04:00'
   ```

   - **chronyd** と同期します。
     chrony ツールでシステム時間を設定および設定するには、Chrony スイートを使用した NTP の設定を参照してください。

2. IdM レプリカのインストールを再試行します。

関連情報

- Red Hat テクニカルサポートサブスクリプションがあり、IdM レプリカのインストールが失敗する問題を解決できない場合は、Red Hat カスタマーポータル でテクニカルサポートケースを作成し、レプリカの **sosreport** サーバーとレプリカの **sosreport** を提供します。
- **sosreport** ユーティリティーは、設定の詳細、ログ、およびシステム情報を RHEL システムから収集します。**sosreport** ユーティリティーの詳細については、sosreport の概要、および、Red Hat Enterprise Linux で sosreport を作成する方法 を参照してください。

22.7. 関連情報

- 最初の IdM サーバーインストールのトラブルシューティング
- IdM クライアントのインストールに関するトラブルシューティング
- IdM のバックアップおよび復元

第23章 IDM レプリカのアンインストール

IdM 管理者は、トポロジーから Identity Management (IdM) レプリカを削除できます。詳細は IdM サーバーのアンインストール を参照してください。

第24章 既存の IDM サーバーへの DNS のインストール

この手順に従って、もともと DNS サービスなしでインストールされた Identity Management (IdM) サーバーに DNS サービスをインストールします。

前提条件

- IdM サーバーのインストール: 統合 DNS と統合 CA を root CA として使用する場合 で説明されているように、統合 DNS で IdM を使用する利点と制限を理解している。
- IdM サーバーへの **root** アクセス権限がある。

手順

1. (必要に応じて)DNS が IdM サーバーにまだインストールされていないことを確認します。

```
[root@r8server ~]# ipa server-role-show r8server.idm.example.com
Role name: DNS server
  Server name: r8server.idm.example.com
  Role name: DNS server
  Role status: absent
```

   この出力で、IdM DNS がサーバーで利用できないことが確認できます。

2. **idm:DL1** ストリームを有効にします。

```
[root@r8server ~]# yum module enable idm:DL1
```

3. **ipa-dns-server** パッケージとその依存関係をダウンロードします。

```
[root@r8server ~]# yum module install idm:DL1/dns
```

4. スクリプトを起動して、サーバーに DNS をインストールします。

```
[root@r8server ~]# ipa-dns-install
```

   a. スクリプトにより、サーバーごとの DNS フォワーダー設定のプロンプトが表示されます。

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

   - サーバーごとの 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、IdM LDAP 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、 **ipa-dns-install**(1) の man ページに記載されている **--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、IdM ドメインのホストは、インフラストラクチャー内にある他の内部 DNS ドメインから名前を解決できません。ホストは、DNS クエリーを解決するためにパブリック DNS サーバーでのみ残ります。

   b. 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スクリプトプロンプトが出されます。

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

検索を実行して欠落している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が尋ねられます。

```
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

オプションで、逆引きゾーンの管理に IdM を使用できます。代わりに、この目的で外部 DNS サービスを使用することもできます。

関連情報

- **man ipa-dns-install(1)**

第25章 IDM サーバーからの統合 IDM DNS サービスのアンインストール

Identity Management (IdM) デプロイメントに統合 DNS を備えたサーバーが複数ある場合は、サーバーの 1 つから統合 DNS サービスを削除することに決定する場合があります。削除するためには、まず IdM サーバーの使用を完全に停止してから、統合 DNS なしで IdM を再インストールする必要があります。

注記

IdM サーバーに DNS ロールを追加することはできますが、IdM では、IdM サーバーから DNS ロールのみを削除する方法はありません。**ipa-dns-install** コマンドには **--uninstall** オプションがありません。

前提条件

- IdM サーバーに統合 DNS がインストールされている。
- 当該統合 DNS が、IdM トポロジー内の最後の統合 DNS サービスではない。

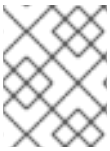
手順

1. 冗長な DNS サービスを特定し、当該サービスをホストする IdM レプリカで IdM サーバーのアンインストール の手順を実行します。
2. 同じホスト上で、ユースケースに応じて、統合 DNS なしで統合 CA をルート CA とするサーバー または 統合 DNS なしで、外部 CA をルート CA とするサーバー のいずれかの手順を実行します。

第26章 CA を使用しないデプロイメントで IDM CA サービスを IDM サーバーに追加

以前に認証局 (CA) コンポーネントなしで Identity Management (IdM) ドメインをインストールした場合は、**ipa-ca-install** コマンドを使用して IdM CA サービスをドメインに追加できます。要件に応じて、次のいずれかのオプションを選択できます。

- IdM 証明書サーバー CA をルート CA として追加
- IdM 証明書サーバー CA を従属 CA として追加し、外部 CA をルート CA として追加



注記

サポートされている CA 設定の詳細については、CA サービスの計画 を参照してください。

26.1. ルート CA として最初の IDM CA を既存の IDM ドメインにインストール

以前に認証局 (CA) コンポーネントなしで Identity Management (IdM) をインストールした場合は、後で CA を IdM サーバーにインストールできます。この手順に従って、外部ルート CA に従属しない IdM CA を**idmserver** サーバーにインストールします。

前提条件

- **idmserver** に対する **root** 権限がある。
- IdM サーバーが **idmserver** にインストールされている。
- IdM デプロイメントには CA がインストールされていません。
- IdM **Directory Manager** パスワードを把握している。

手順

1. **idmserver** に、IdM Certificate Server CA をインストールします。

```
[root@idmserver ~] ipa-ca-install
```

2. トポロジー内の各 IdM ホストで、**ipa-certupdate** ユーティリティーを実行して、IdM LDAP からの新しい証明書に関する情報でホストを更新します。

重要

IdM CA 証明書の生成後に **ipa-certupdate** を実行しない場合、証明書は他の IdM マシンに配布されません。

26.2. ルート CA として外部 CA を使用する最初の IDM CA を既存の IDM ドメインにインストール

以前に認証局 (CA) コンポーネントなしで Identity Management (IdM) をインストールした場合は、後で CA を IdM サーバーにインストールできます。この手順に従って、**idmserver** サーバーに外部ルート CA に従属する IdM CA をインストールし、その間に 0 個または複数の中間 CA を配置します。

前提条件

- **idmserver** に対する **root** 権限がある。
- IdM サーバーが **idmserver** にインストールされている。
- IdM デプロイメントには CA がインストールされていません。
- IdM **Directory Manager** パスワードを把握している。

手順

1. インストールを開始します。

```
[root@idmserver ~] ipa-ca-install --external-ca
```

2. コマンドラインインターフェイスから、証明書署名要求 (CSR) が保存されたことが通知されるまで待ちます。
3. CSR を外部 CA に送信します。
4. 発行された証明書を IdM サーバーにコピーします。
5. 外部 CA ファイルへの証明書および完全パスを **ipa-ca-install** に追加してインストールを続行します。

```
[root@idmserver ~]# ipa-ca-install --external-cert-file=/root/master.crt --external-cert-file=/root/ca.crt
```

6. トポロジー内の各 IdM ホストで、**ipa-certupdate** ユーティリティーを実行して、IdM LDAP からの新しい証明書に関する情報でホストを更新します。

重要

IdM CA 証明書の生成後に **ipa-certupdate** を実行できないということは、証明書が他の IdM マシンに配布されないことを意味します。

第27章 CA を使用したデプロイで IDM CA サービスを IDM サーバーに追加

Identity Management (IdM) 環境にすでに IdM 認証局 (CA) サービスがインストールされているが、特定の IdM サーバー **idmserver** が CA なしの IdM レプリカとしてインストールされている場合は、 **ipa-ca-install** を使用して CA サービスを **idmserver** に追加できます。

注記

この手順は、次の両方のシナリオで同じです。

- IdMCA はルート CA です。
- IdM CA は、外部のルート CA に従属しています。

前提条件

- **idmserver** に対する **root** 権限がある。
- IdM サーバーが **idmserver** にインストールされている。
- IdM デプロイメントには、別の IdM サーバーに CA がインストールされています。
- IdM **Directory Manager** パスワードを把握している。

手順

- **idmserver** に、IdM Certificate Server CA をインストールします。

```
[root@idmserver ~] ipa-ca-install
```

第28章 IDM サーバーからの IDM CA サービスのアンインストール

トポロジー内に **CA ロール** を持つ Identity Management (IdM) レプリカが 5 つ以上あり、冗長な証明書のレプリケーションが原因でパフォーマンスの問題が発生する場合、(RH) は IdM レプリカから冗長な CA サービスインスタンスを削除することを推奨します。そのためには、当該 IdM レプリカの使用を完全に停止してから、CA サービスを使用せずに IdM を再インストールする必要があります。

注記

IdM レプリカに CA ロールを **追加** することはできますが、IdM では、IdM レプリカから CA ロールのみを **削除** する方法はありません。**ipa-ca-install** コマンドには **--uninstall** オプションがありません。

前提条件

- トポロジー内の 5 つ以上の IdM サーバーに IdM CA サービスがインストールされている。

手順

1. 冗長な CA サービスを特定し、当該サービスをホストする IdM レプリカで IdM サーバーのアンインストール の手順を実行します。
2. 同じホストで、IdM サーバーのインストール: 統合 DNS があり外部 CA がない場合 の手順に従います。

第29章 レプリケーショントポロジーの管理

本章では、Identity Management(IdM) ドメイン内のサーバー間のレプリケーションを管理する方法を説明します。

関連情報

- レプリカトポロジーの計画

29.1. レプリカ合意、トポロジー接尾辞、およびトポロジーセグメントの説明

レプリカを作成すると、Identity Management (IdM) が初期サーバーとレプリカ間にレプリカ合意を作成します。複製されるデータはトポロジーの接尾辞に保存され、2 つのレプリカの接尾辞間でレプリカ合意があると、接尾辞がトポロジーセグメントを形成します。これらの概念は、以下のセクションで詳細に説明されています。

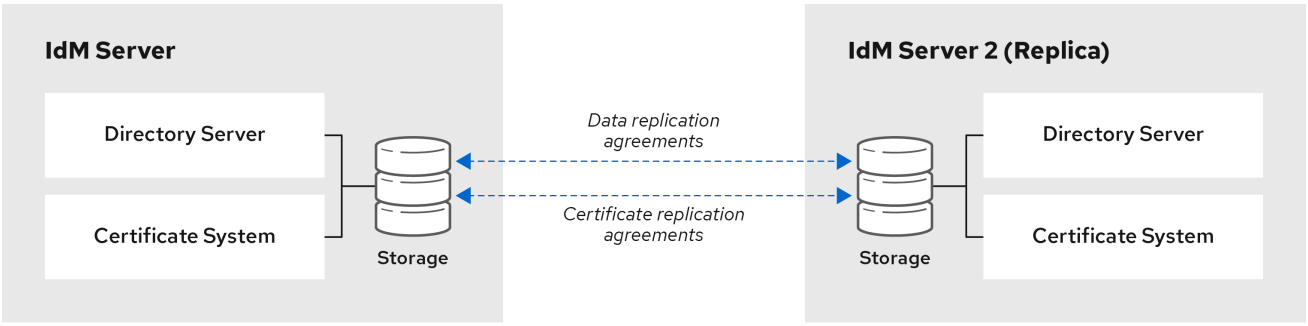
- レプリカ合意
- トポロジー接尾辞
- トポロジーセグメント

29.1.1. IdM レプリカ間のレプリカ合意

管理者が、既存のサーバーに基づいてレプリカを作成すると、Identity Management (IdM) は、初期サーバーとレプリカとの間に **レプリカ合意** を作成します。レプリカ合意は、データと設定が 2 台のサーバー間で継続的に複製されることを保証します。

IdM は、**複数の読み取り/書き込みレプリカ複製** を使用します。この設定では、レプリカ合意に参加しているすべてのレプリカが更新の受信と提供を行うので、サプライヤーとコンシューマーとみなされます。レプリカ合意は常に双方向です。

図29.1 サーバーとレプリカ合意



IdM は、2 種類のレプリカ合意を使用します。

ドメインのレプリカ合意

この合意は、識別情報を複製します。

証明書のレプリカ合意

この合意は、証明書情報を複製します。

両方の複製チャンネルは独立しています。2 台のサーバー間で、いずれかまたは両方の種類のレプリカ合意を設定できます。たとえば、サーバー A とサーバー B にドメインレプリカ合意のみが設定されている場合は、証明書情報ではなく ID 情報だけが複製されます。

29.1.2. トポロジー接尾辞

トポロジー接尾辞は、レプリケートされるデータを保存します。IdM は、**domain** と **ca** の 2 種類のトポロジー接尾辞に対応します。それぞれの接尾辞は、個別のサーバーである個別のレプリケーショントポロジーを表します。

レプリカ合意が設定されると、同じタイプのトポロジー接尾辞を 2 つの異なるサーバーに結合します。

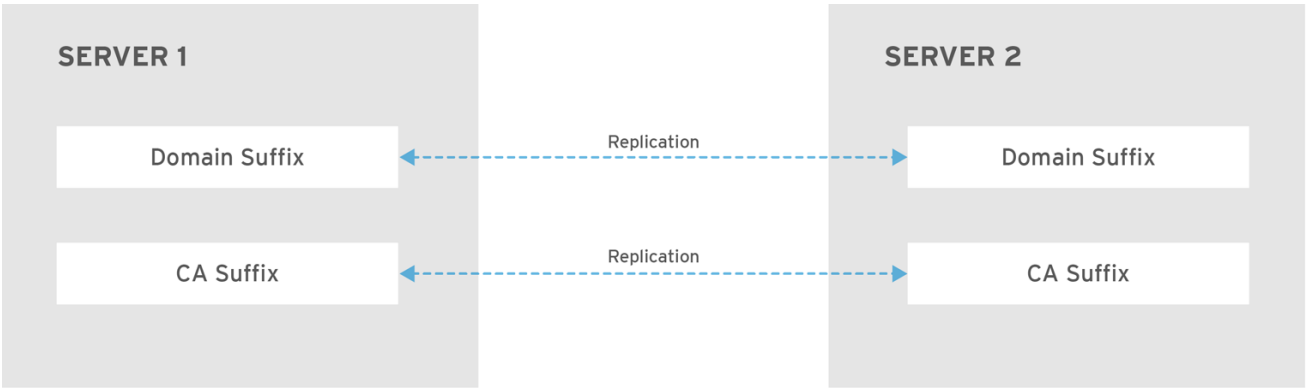
domain 接尾辞: dc=example,dc=com

domain 接尾辞には、ドメイン関連のデータがすべて含まれています。
2 つのレプリカの **domain** 接尾辞間でレプリカ合意が設定されると、ユーザー、グループ、およびポリシーなどのディレクトリーデータが共有されます。

ca 接尾辞: o=ipaca

ca 接尾辞には、Certificate System コンポーネントのデータが含まれます。これは認証局 (CA) がインストールされているサーバーにのみ存在します。
2 つのレプリカの **ca** 接尾辞間でレプリカ合意が設定されると、証明書データが共有されます。

図29.2 トポロジー接尾辞



新規レプリカのインストール時には、**ipa-replica-install** スクリプトが 2 つのサーバー間に初期トポロジーレプリカ合意をセットアップします。

例29.1 トポロジー接尾辞の表示

ipa topologysuffix-find コマンドでトポロジー接尾辞のリストが表示されます。

```
$ ipa topologysuffix-find
----------------------------
2 topology suffixes matched
----------------------------
  Suffix name: ca
  Managed LDAP suffix DN: o=ipaca

  Suffix name: domain
  Managed LDAP suffix DN: dc=example,dc=com
```

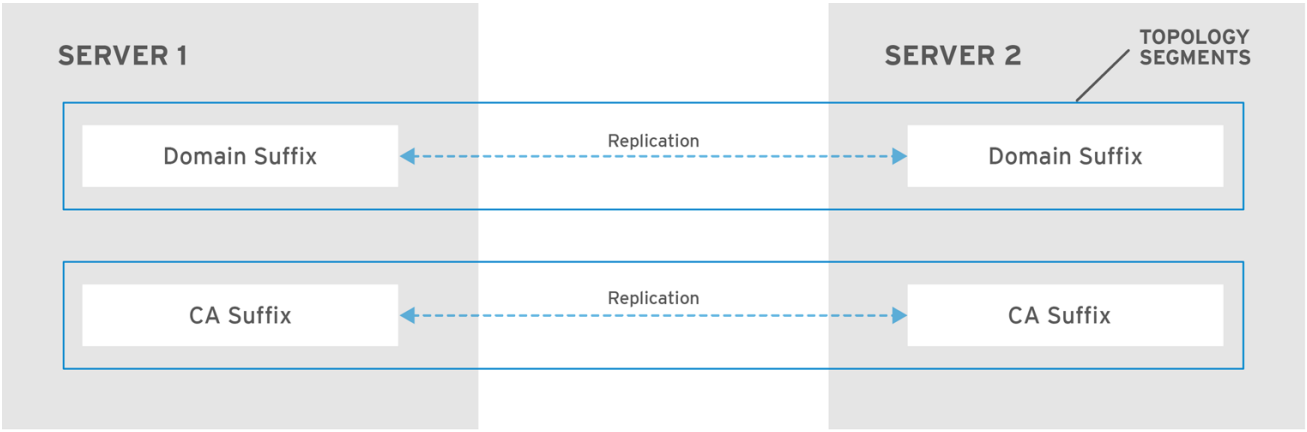
```
----------------------------
Number of entries returned 2
----------------------------
```

29.1.3. トポロジーセグメント

2 つのレプリカの接尾辞間でレプリカ合意があると、接尾辞は **トポロジーセグメント** を形成します。各トポロジーセグメントは、**左ノード**と**右ノード** で設定されます。ノードは、レプリカ合意に参加しているサーバーを表します。

IdM のトポロジーセグメントは常に双方向です。各セグメントは、サーバー A からサーバー B、およびサーバー B からサーバー A への 2 つのレプリカ合意を表します。そのため、データは両方の方向でレプリケートされます。

図29.3 トポロジーセグメント



例29.2 トポロジーセグメントの表示

ipa topologysegment-find コマンドで、ドメインまたは CA 接尾辞に設定されたトポロジーセグメントが表示されます。たとえば、ドメイン接尾辞の場合は、以下のようになります。

```
$ ipa topologysegment-find
Suffix name: domain
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

この例では、ドメイン関連のデータのみが **server1.example.com** と **server2.example.com** の 2 つのサーバー間で複製されます。

特定セグメントの詳細を表示するには、**ipa topologysegment-show** コマンドを使用します。

```
$ ipa topologysegment-show
```

```
Suffix name: domain
Segment name: server1.example.com-to-server2.example.com
  Segment name: server1.example.com-to-server2.example.com
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

29.2. トポロジーグラフを使用したレプリケーショントポロジーの管理

Web UI のトポロジーグラフは、ドメイン内のサーバー間の関係を表示します。Web UI を使用すると、トポロジーの表現を操作および変換できます。

トポロジーグラフへのアクセス

トポロジーグラフにアクセスするには、以下を実行します。

1. **IPA Server → Topology → Topology Graph** を選択します。
2. トポロジーに加えた変更がグラフに反映されていない場合は、**Refresh** をクリックします。

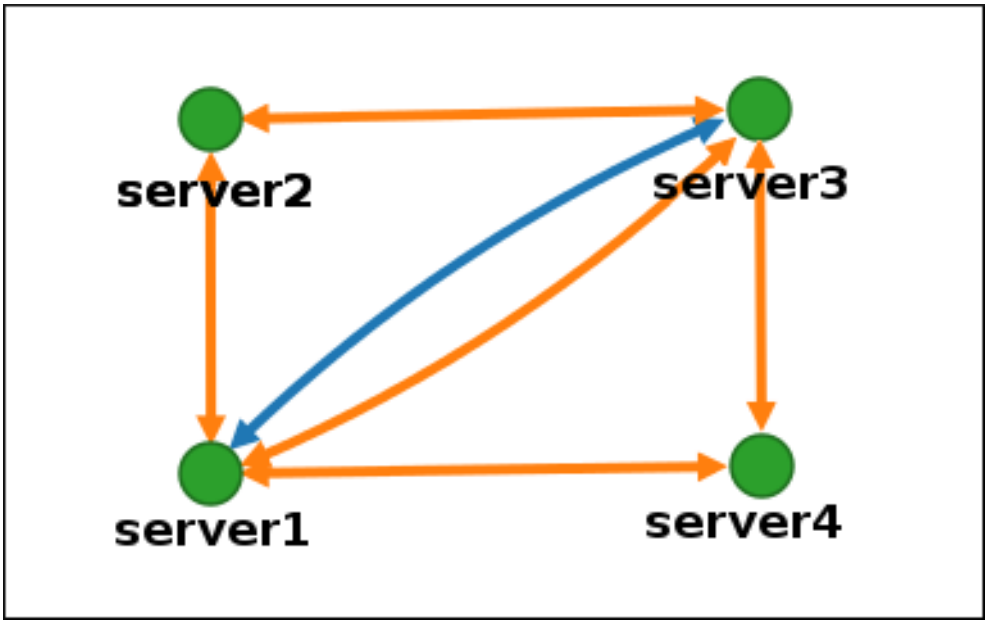
トポロジーグラフの解釈

ドメインのレプリカ合意に参加しているサーバーは、オレンジ色の矢印によって接続されます。CA のレプリカ合意に参加しているサーバーは、青色の矢印によって接続されます。

トポロジーグラフの例: 推奨されるトポロジー

以下の推奨トポロジーの例は、4 台のサーバーに対して考えられる推奨トポロジーの 1 つを示しています。各サーバーは少なくとも 2 つの他のサーバーに接続されており、複数のサーバーが CA サーバーです。

図29.4 推奨されるトポロジーの例

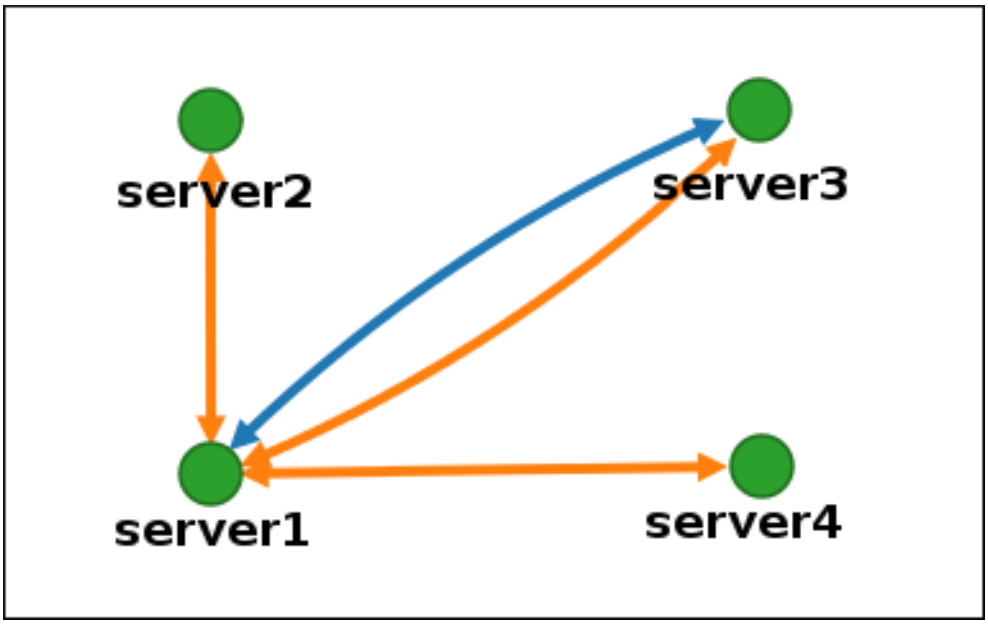


トポロジーグラフの例: 推奨されないトポロジー

推奨されないトポロジーの例では、**server1** が単一障害点になります。その他のすべてのサーバーは、このサーバーとのレプリカ合意がありますが、他のサーバーとは合意がありません。したがって、**server1** が失敗すると、他のすべてのサーバーは分離されます。

このようなトポロジーの作成は避けてください。

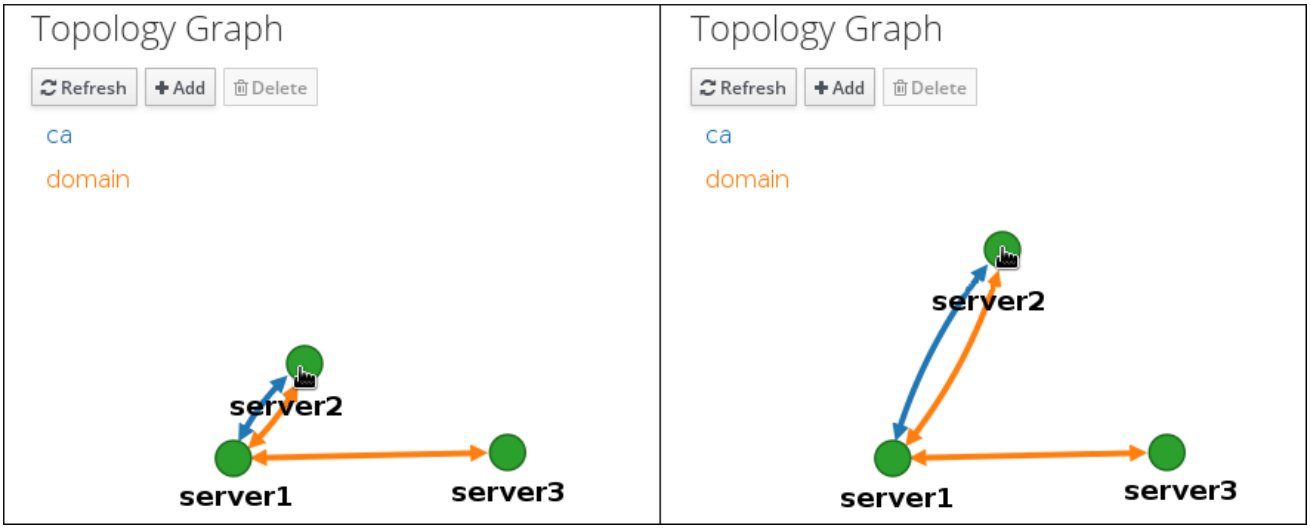
図29.5 推奨されないトポロジーの例: 単一障害点



トポロジービューのカスタマイズ

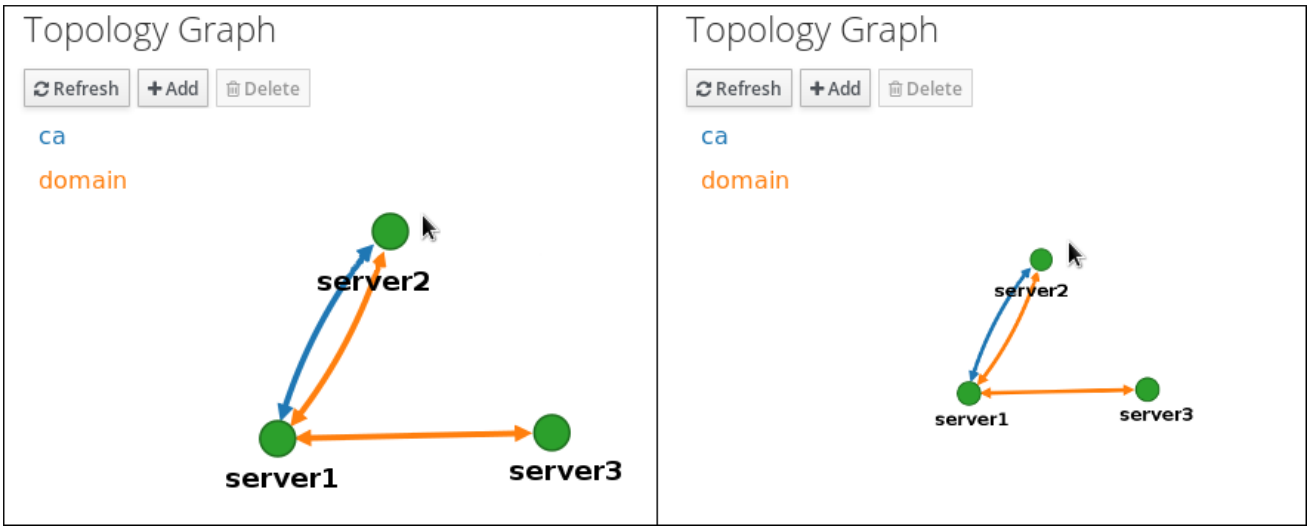
マウスをドラッグして、個別のトポロジーノードを移動できます。

図29.6 トポロジーグラフのノードの移動



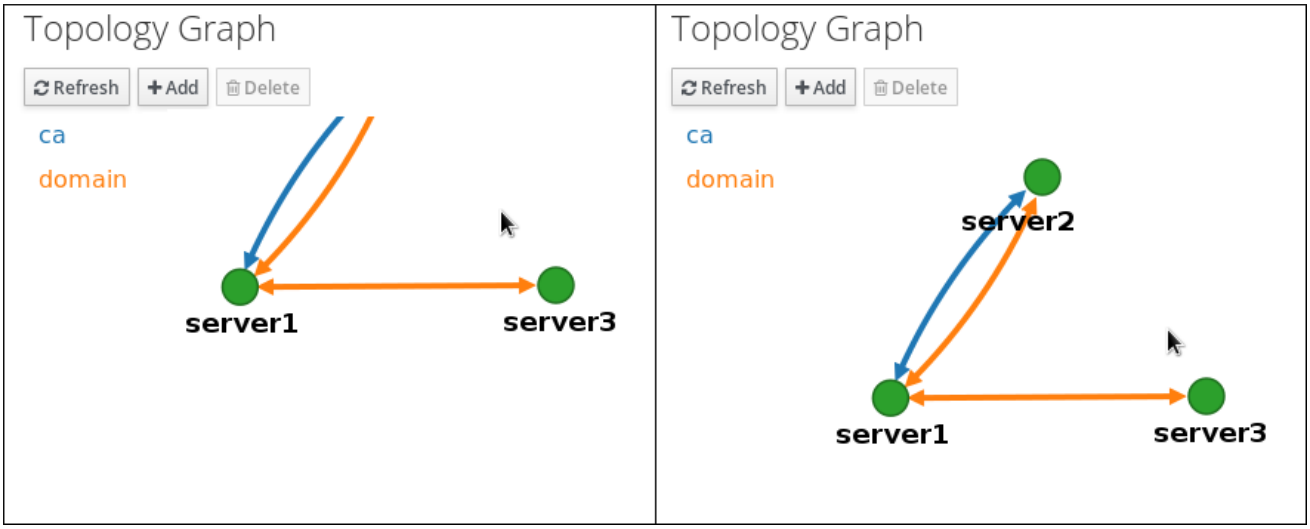
マウスのホイールを使用して、トポロジーグラフを拡大および縮小できます。

図29.7 トポロジーグラフのズーム



マウスの左ボタンを保持することで、トポロジーグラフのキャンバスを移動できます。

図29.8 トポロジーグラフのキャンバスの移動



29.3. WEB UI を使用した 2 台のサーバー間のレプリケーションの設定

Identity Management (IdM) の Web インターフェイスを使用すると、2 つのサーバーを選択し、そのサーバー間に新しいレプリカ合意を作成できます。

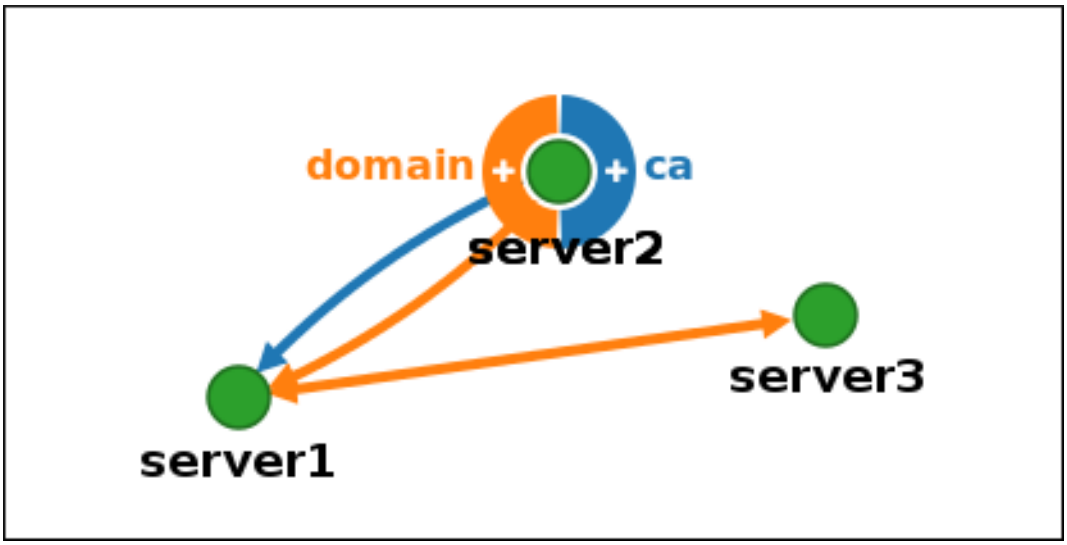
前提条件

- IdM 管理者認証情報がある。

手順

1. トポロジーグラフで、サーバーノードの 1 つにマウスを合わせます。

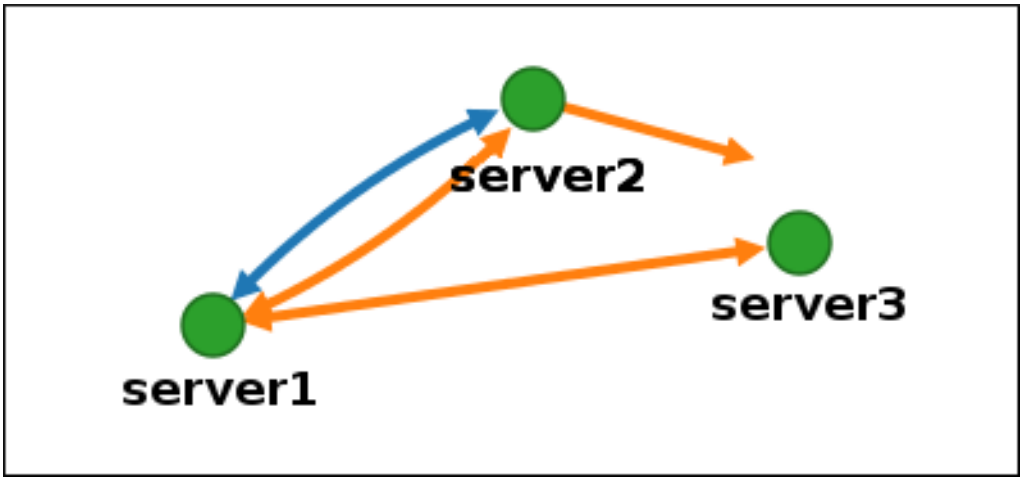
図29.9 ドメインまたは CA オプション



2. 作成するトポロジーセグメントのタイプに応じて、**domain** または円の **ca** 部分をクリックします。

3. 新しいレプリカ合意を表す新しい矢印が、マウスポインターの下に表示されます。マウスを他のサーバーノードに移動し、そこでクリックします。

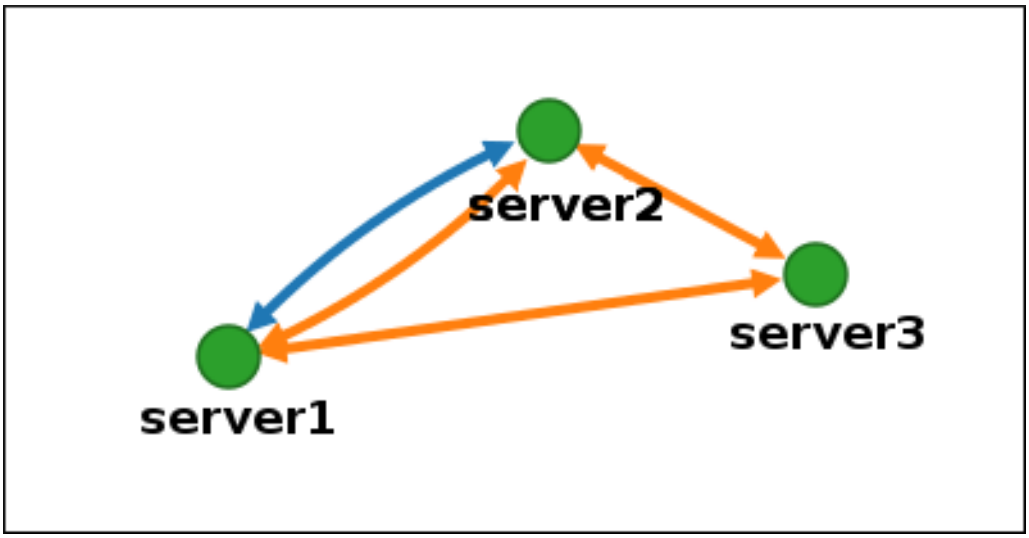
図29.10 新規セグメントの作成



4. **Add Topology Segment** ウィンドウで **Add** をクリックして、新規セグメントのプロパティーを確認します。

2 台のサーバー間の新しいトポロジーセグメントは、サーバーをレプリカ合意に参加させます。トポロジーグラフには、更新されたレプリケーショントポロジーが表示されるようになりました。

図29.11 新規に作成されたセグメント



29.4. WEB UI を使用した 2 台のサーバー間のレプリケーションの停止

Identity Management (IdM) の Web インターフェイスを使用して、サーバーからレプリカ合意を削除できます。

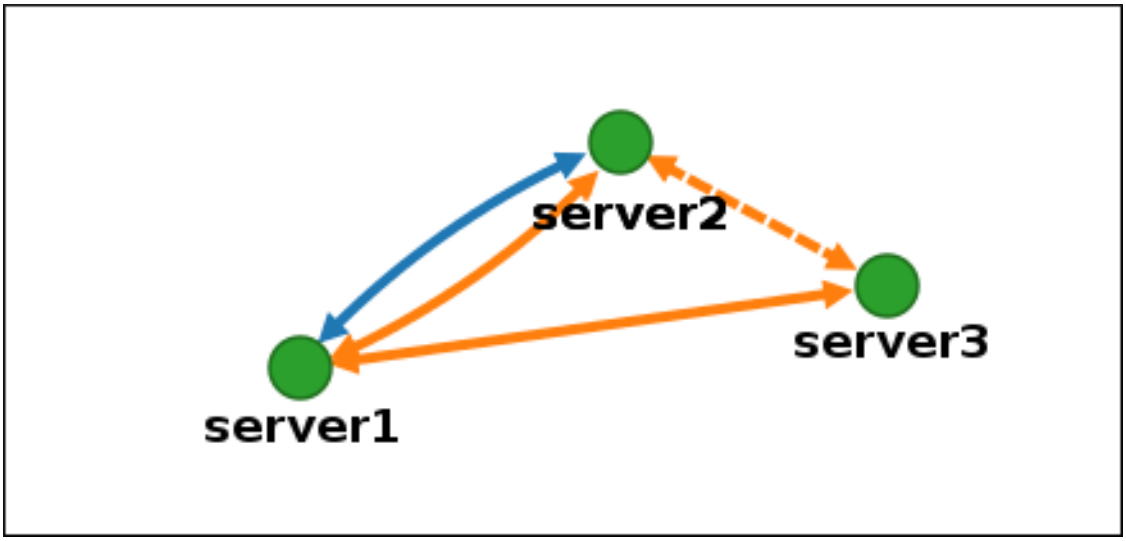
前提条件

- IdM 管理者認証情報がある。

手順

1. 削除するレプリカ合意を表す矢印をクリックします。これにより、矢印がハイライト表示されます。

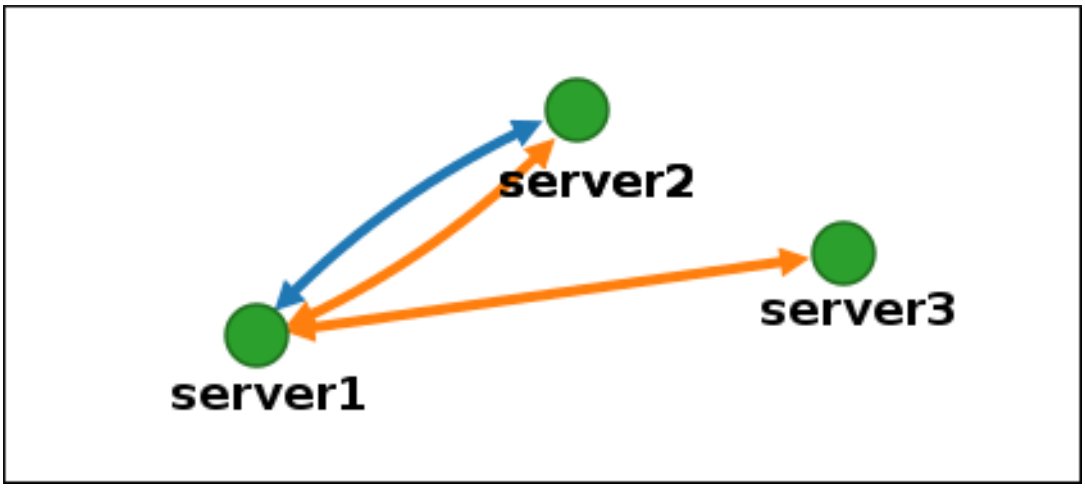
   図29.12 トポロジーセグメントのハイライト表示

2. **Delete** をクリックします。
3. **Confirmation** ウィンドウで **OK** をクリックします。

IdM は、2 台のサーバー間のトポロジーセグメントを削除します。これにより、そのレプリカ合意が削除されます。トポロジーグラフには、更新されたレプリケーショントポロジーが表示されるようになりました。

図29.13 トポロジーセグメントの削除



29.5. CLI を使用した 2 つのサーバー間のレプリケーションの設定

ipa topologysegment-add コマンドを使用して、2 台のサーバー間のレプリカ合意を設定できます。

前提条件

- IdM 管理者認証情報がある。

手順

1. **ipa topologysegment-add** コマンドを使用して、2 つのサーバーのトポロジーセグメントを作成します。プロンプトが表示されたら、以下を指定します。
   - 必要なトポロジー接尾辞: **domain** または **ca**
   - 2 つのサーバーを表す、左ノードと右のノード
   - オプションで、セグメントのカスタム名
     以下に例を示します。

     ```
     $ ipa topologysegment-add
     Suffix name: domain
     Left node: server1.example.com
     Right node: server2.example.com
     Segment name [server1.example.com-to-server2.example.com]: new_segment
     ----------------------------
     Added segment "new_segment"
     ----------------------------
       Segment name: new_segment
       Left node: server1.example.com
       Right node: server2.example.com
       Connectivity: both
     ```

     新しいセグメントを追加すると、サーバーをレプリカ合意に参加させます。

2. **オプション:ipa topologysegment-show** コマンドを使用して、新しいセグメントが設定されたことを確認します。

   ```
   $ ipa topologysegment-show
   ```

```
Suffix name: domain
Segment name: new_segment
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both
```

29.6. CLI を使用した 2 つのサーバー間のレプリケーションの停止

ipa topology_segment-del コマンドを使用して、コマンドラインからレプリカ合意を終了できます。

前提条件

- IdM 管理者認証情報がある。

手順

1. レプリケーションを停止するには、サーバー間の対応するレプリケーションセグメントを削除する必要があります。これを実行するには、セグメント名を知っている必要があります。
名前が分からない場合は、**ipa topologysegment-find** コマンドを使用してすべてのセグメントを表示し、出力で必要なセグメントを見つけます。プロンプトが表示されたら、必要なトポロジー接尾辞 (**domain** または **ca**) を指定します。以下に例を示します。

```
$ ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
  Left node: server1.example.com
  Right node: server2.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 8
----------------------------
```

2. **ipa topologysegment-del** コマンドを使用して、2 台のサーバー間のトポロジーセグメントを削除します。

```
$ ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
----------------------------
Deleted segment "new_segment"
----------------------------
```

セグメントを削除すると、レプリカ合意が削除されます。

3. **オプション:ipa topologysegment-find** コマンドを使用して、セグメントが表示されなくなったことを確認します。

```
$ ipa topologysegment-find
Suffix name: domain
------------------
7 segments matched
------------------
  Segment name: server2.example.com-to-server3.example.com
  Left node: server2.example.com
  Right node: server3.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 7
----------------------------
```

29.7. WEB UI を使用したトポロジーからのサーバーの削除

Identity Management (IdM) の Web インターフェイスを使用して、トポロジーからサーバーを削除できます。

前提条件

- IdM 管理者認証情報がある。
- 削除するサーバーが、残りのトポロジーで他のサーバーに接続する **唯一のサーバーではない**。この場合、他のサーバーが分離されますが、これは許可されていません。
- 削除するサーバーが、最後の CA または DNS サーバー **ではない**。

警告

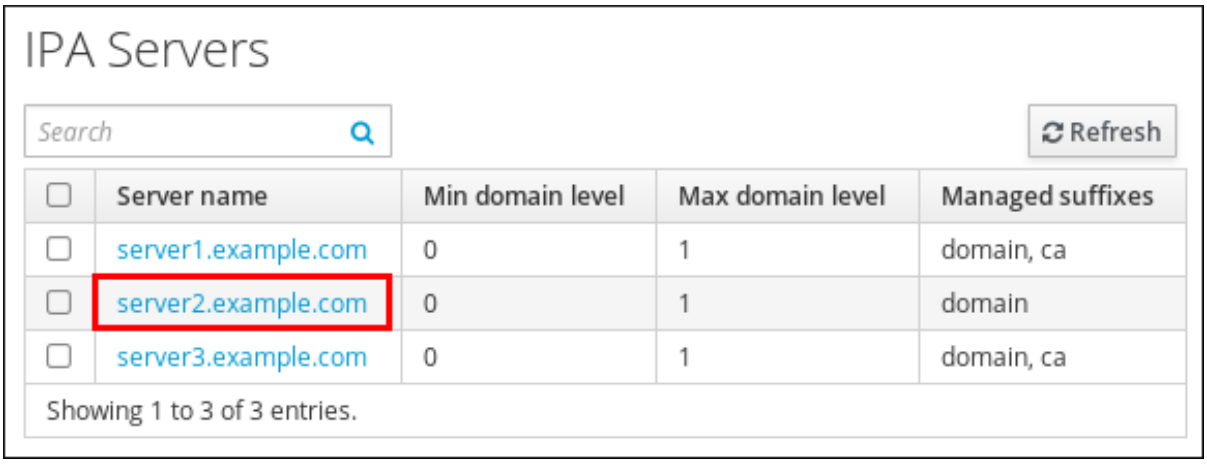
サーバーの削除は元に戻せないアクションです。サーバーを削除すると、トポロジーに戻す唯一の方法は、マシンに新しいレプリカをインストールすることです。

手順

サーバーコンポーネントをマシンからアンインストールせずにトポロジーからサーバーを削除するには、以下を実行します。

1. **IPA Server → Topology → IPA Servers** を選択します。
2. 削除するサーバーの名前をクリックします。

図29.14 サーバーの選択



3. **Delete Server** をクリックします。

29.8. CLI を使用したトポロジーからのサーバーの削除

コマンドラインインターフェイスを使用して、トポロジーからサーバーを削除できます。

前提条件

- IdM 管理者認証情報がある。
- 削除するサーバーが、残りのトポロジーで他のサーバーに接続する **唯一のサーバーではない**。この場合、他のサーバーが分離されますが、これは許可されていません。
- 削除するサーバーが、最後の CA または DNS サーバー **ではない**。

重要

サーバーの削除は元に戻せないアクションです。サーバーを削除すると、トポロジーに戻す唯一の方法は、マシンに新しいレプリカをインストールすることです。

手順

server1.example.com を削除するには、次のコマンドを実行します。

1. 別のサーバーで **ipa server-del** コマンドを実行して、**server1.example.com** を削除します。このコマンドは、サーバーを参照するすべてのトポロジーセグメントを削除します。

```
[user@server2 ~]$ ipa server-del
Server name: server1.example.com
Removing server1.example.com from replication topology, please wait...
-----------------------------------------------------------
Deleted IPA server "server1.example.com"
-----------------------------------------------------------
```

2. **オプション**: **server1.example.com** で、**ipa server-install --uninstall** コマンドを実行して、マシンからサーバーコンポーネントをアンインストールします。

```
[root@server1 ~]# ipa server-install --uninstall
```

29.9. WEB UI を使用した IDM サーバーでのサーバーロールの表示

IdM サーバーにインストールされるサービスに基づいて、さまざまな **サーバーロール** を実行できます。以下に例を示します。

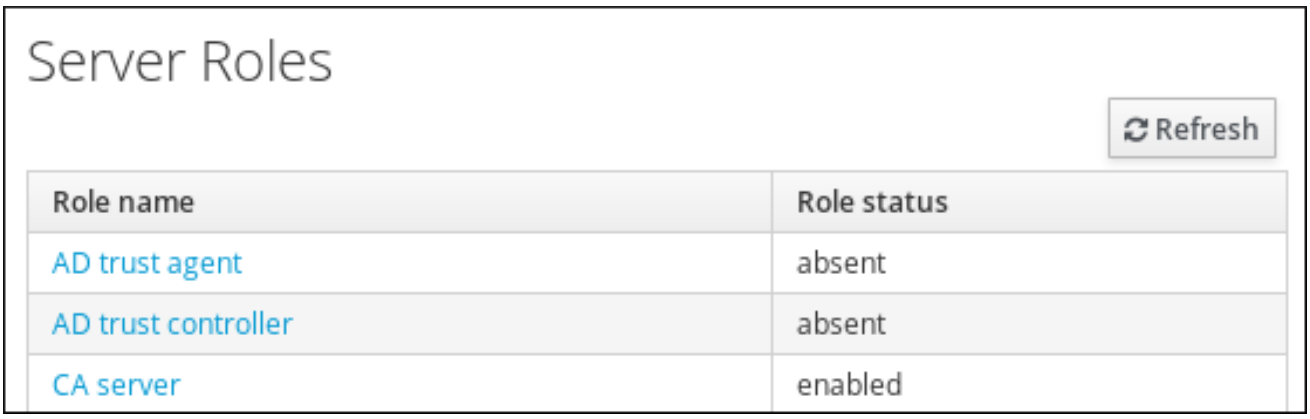
- CA サーバー
- DNS サーバー
- キーリカバリー認証局 (KRA) サーバー

サポートされるサーバーロールの完全なリストは、**IPA Server → Topology → Server Roles**を参照してください。

注記

- Role status が **absent** の場合は、トポロジー内でそのロールを実行しているサーバーがないことを示しています。
- Role status が **enabled** の場合は、トポロジー内でそのロールを実行しているサーバーが 1 台以上あることを示しています。

図29.15 Web UI でのサーバーロール



29.10. CLI を使用した IDM サーバーでのサーバーロールの表示

IdM サーバーにインストールされるサービスに基づいて、さまざまな **サーバーロール** を実行できます。以下に例を示します。

- CA サーバー
- DNS サーバー
- キーリカバリー認証局 (KRA) サーバー

以下のコマンドを使用して、トポロジー内でどのサーバーがどのロールを実行するかを表示できます。

- **ipa config-show** コマンドを実行すると、すべての CA サーバーおよび現行の CA 更新サーバーが表示されます。

```
$ ipa config-show
  ...
  IPA masters: server1.example.com, server2.example.com, server3.example.com
```

```
IPA CA servers: server1.example.com, server2.example.com
IPA CA renewal master: server1.example.com
```

- **ipa server-show** コマンドは、特定のサーバーで有効なロールのリストを表示します。たとえば、server.example.com で有効にしたロールのリストは、以下のようになります。

```
$ ipa server-show
Server name: server.example.com
  ...
Enabled server roles: CA server, DNS server, KRA server
```

- **ipa server-find --servrole** は、特定のサーバーロールが有効になっているすべてのサーバーを検索します。たとえば、すべての CA サーバーを検索するには、以下を実行します。

```
$ ipa server-find --servrole "CA server"
---------------------
2 IPA servers matched
---------------------
  Server name: server1.example.com
  ...

  Server name: server2.example.com
  ...
----------------------------
Number of entries returned 2
----------------------------
```

29.11. レプリカの CA 更新サーバーおよび CRL パブリッシャーサーバーへのプロモート

IdM デプロイメントで組み込み認証局 (CA) を使用する場合は、IdM CA サーバーの 1 つが CA サブシステム証明書の更新を管理する CA 更新サーバーとして機能します。IdM CA サーバーの 1 つは、証明書失効リストを生成する IdM CRL パブリッシャーサーバーとしても機能します。デフォルトでは、CA 更新サーバーおよび CRL パブリッシャーサーバーロールは、システム管理者が **ipa-server-install** または **ipa-ca-install** コマンドを使用して CA ロールをインストールした最初のサーバーにインストールされます。

前提条件

- IdM 管理者認証情報がある。

手順

- 現在の CA 更新サーバーを変更します。
- CRL を生成するようにレプリカを設定します。

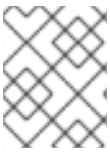
29.12. 非表示レプリカの降格または昇格

レプリカのインストール後、レプリカの表示状態を設定できます。

非表示のレプリカの詳細は、非表示のレプリカモード を参照してください。

レプリカが CA 更新サーバーである場合は、このレプリカを非表示にする前に、サービスを別のレプリカに移動します。

詳細は Changing and resetting IdM CA renewal server を参照してください。



注記

RHEL 8.1 で導入された非表示のレプリカ機能は、RHEL 8.2 以降で完全にサポートされています。

手順

- レプリカを非表示にするには、次のコマンドを実行します。

```
# ipa server-state replica.idm.example.com --state=hidden
```

次のコマンドを実行すれば、レプリカを表示できます

```
# ipa server-state replica.idm.example.com --state=enabled
```

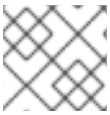
トポロジー内のすべての非表示のレプリカのリストを表示するには、次のコマンドを実行します。

```
# ipa config-show
```

すべてのレプリカが有効になっている場合は、コマンドの出力に非表示のレプリカは記載されません。

第30章 IDM HEALTHCHECK ツールのインストールおよび実行

IdM Healthcheck ツールと、ツールのインストールおよび実行方法について詳しく説明します。



注記

- Healthcheck ツールは、RHEL 8.1 以降でのみ利用できます。

30.1. IDM の HEALTHCHECK

Identity Management (IdM) の Healthcheck ツールは、IdM 環境の健全性に影響を与える可能性のある問題を検出するのに役立ちます。

注記

Healthcheck ツールは、Kerberos 認証なしで使用できるコマンドラインツールです。

独立したモジュール

Healthcheck は、以下をテストする独立したモジュールで構成されています。

- レプリケーションの問題
- 証明書の有効性
- 認証局インフラストラクチャーの問題
- IdM および Active Directory の信頼の問題
- ファイルのパーミッションと所有権の正しい設定

2 つの出力形式

Healthcheck では、以下の出力が生成されます。これは、**output-type** オプションを使用して設定できます。

- **JSON**: マシンが判読できる出力 (デフォルト)
- **human**: 人間が判読できる出力

--output-file オプションで別の出力先ファイルを指定できます。

結果

Healthcheck の各モジュールは、次のいずれかの結果を返します。

SUCCESS
: 想定どおりに設定されています。

WARNING
: エラーではありませんが、注意または評価することを推奨します。

ERROR
: 想定どおりに設定されていません。

CRITICAL

想定どおりに設定されておらず、影響が受ける可能性が高いと見られます。

30.2. IDM HEALTHCHECK のインストール

以下の手順に従って、IdM Healthcheck ツールをインストールします。

手順

- **ipa-healthcheck** パッケージをインストールします。

```
[root@server ~]# yum install ipa-healthcheck
```

注記

RHEL 8.1 および 8.2 システムでは、代わりに **yum install /usr/bin/ipa-healthcheck** コマンドを使用します。

検証手順

- **--failures-only** オプションを使用して、**ipa-healthcheck** にエラーのみを報告させます。IdM インストールが完全に機能していれば、空の結果 **[]** が返されます。

```
[root@server ~]# ipa-healthcheck --failures-only
[]
```

関連情報

- **ipa-healthcheck --help** を使用して、サポートされるすべての引数を表示します。

30.3. IDM HEALTHCHECK の実行

Healthcheck は、ログローテーション を使用して手動で実行することも、また自動でも実行できます。

前提条件

- Healthcheck ツールがインストールされている。IdM Healthcheck のインストール を参照してください。

手順

- Healthcheck を手動で実行するには、**ipa-healthcheck** コマンドを実行します。

```
[root@server ~]# ipa-healthcheck
```

関連情報

すべてのオプションは、**man ipa-healthcheck** の man ページを参照してください。

30.4. 関連情報

- IdM Healthcheck の使用例は、Identity Management の設定および管理 の以下のセクションを参照してください。
  - サービスの確認
  - IdM および AD 信頼設定の確認
  - 証明書の確認
  - システム証明書の確認
  - ディスク領域の確認
  - IdM 設定ファイルの権限の確認
  - レプリケーションの確認
- また、1つのガイドにまとめられたこれらの章 (IdM Healthcheck を使用した IdM 環境の監視) も表示できます。

第31章 ANSIBLE PLAYBOOK で IDENTITY MANAGEMENT サーバーのインストール

Ansible を使用してシステムを IdM サーバーとして設定する方法を説明します。システムを IdM サーバーとして設定すると、IdM ドメインを確立し、システムが IdM クライアントに IdM サービスを提供できるようになります。**ipaserver** Ansible ロールを使用してデプロイメントを管理できます。

前提条件

- Ansible と IdM の一般的な概念を理解しています。

31.1. ANSIBLE と、IDM をインストールする利点

Ansible は、システムの設定、ソフトウェアのデプロイ、ローリング更新の実行に使用する自動化ツールです。Ansible には Identity Management (IdM) のサポートが含まれるため、Ansible モジュールを使用して、IdM サーバー、レプリカ、クライアント、または IdM トポロジー全体の設定などのインストールタスクを自動化できます。

IdM のインストールに Ansible を使用する利点
以下のリストは、手動インストールとは対照的に、Ansible を使用して Identity Management をインストールする利点を示しています。

- 管理ノードにログインする必要はありません。
- デプロイする各ホストに個別に設定する必要はありません。代わりに、完全なクラスターをデプロイするためのインベントリーファイルを 1 つ使用できます。
- ユーザーおよびホストを追加するなど、後で管理タスクにインベントリーファイルを再利用できます。IdM には関係のないタスクであっても、インベントリーファイルを再利用できます。

関連情報

- Automating Red Hat Identity Management installation
- Identity Management の計画
- IdM サーバーをインストールするためのシステムの準備

31.2. ANSIBLE-FREEIPA パッケージのインストール

以下の手順に従って、Identity Management (IdM) をインストールおよび管理する Ansible ロールとモジュールを提供する **ansible-freeipa** パッケージをインストールします。

前提条件

- コントローラーが、有効なサブスクリプションを備えた Red Hat Enterprise Linux システムである。そうでない場合は、公式の Ansible ドキュメントの Installation guide で、代替のインストール方法を参照してください。
- コントローラーから、**SSH** プロトコルで管理ノードに到達できる。管理ノードが、コントローラーの **/root/.ssh/known_hosts** ファイルのリストに記載されていることを確認します。

手順

Ansible コントローラーで以下の手順を使用します。

1. システムが RHEL 8.5 以前で実行されている場合は、必要なリポジトリーを有効にします。

```
# subscription-manager repos --enable ansible-2.8-for-rhel-8-x86_64-rpms
```

2. システムが RHEL 8.5 以前で実行されている場合は、**ansible** パッケージをインストールします。

```
# yum install ansible
```

3. **ansible-freeipa** パッケージをインストールします。

```
# yum install ansible-freeipa
```

ロールとモジュールは、**/usr/share/ansible/roles/** および **/usr/share/ansible/plugins/modules** ディレクトリーにインストールされます。

31.3. ファイルシステム内の ANSIBLE ロールの場所

デフォルトでは、**ansible-freeipa** ロールは **/usr/share/ansible/roles/** ディレクトリーにインストールされます。**ansible-freeipa** パッケージの構造は以下のとおりです。

- **/usr/share/ansible/roles/** ディレクトリーには、Ansible コントローラーの **ipaserver** ロール、**ipareplica** ロール、および **ipaclient** ロールが保存されています。各ロールディレクトリーには、サンプル、基本的な概要、ライセンス、および Markdown ファイルの **README.md** のロールに関する情報が保存されています。

```
[root@server]# ls -1 /usr/share/ansible/roles/
ipaclient
ipareplica
ipaserver
```

- **/usr/share/doc/ansible-freeipa/** ディレクトリーには、Markdown ファイルの **README.md** に、各ロールおよびトポロジーに関する情報が保存されています。また、**playbooks/** サブディレクトリーも保存されています。

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/
playbooks
README-client.md
README.md
README-replica.md
README-server.md
README-topology.md
```

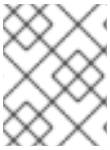
- **/usr/share/doc/ansible-freeipa/playbooks/** ディレクトリーは、Playbook のサンプルを保存します。

```
[root@server]# ls -1 /usr/share/doc/ansible-freeipa/playbooks/
install-client.yml
install-cluster.yml
install-replica.yml
install-server.yml
uninstall-client.yml
```

```
uninstall-cluster.yml
uninstall-replica.yml
uninstall-server.yml
```

31.4. 統合 DNS と、ROOT CA としての統合 CA を使用したデプロイメントのパラメーターの設定

以下の手順に従って、IdM 統合 DNS ソリューションを使用する環境で、統合 CA を持つ IdM サーバーを root CA としてインストールするようにインベントリーファイルを設定します。



注記

この手順のインベントリーは、**INI** 形式を使用します。または、**YAML** 形式または **JSON** 形式を使用できます。

手順

1. ~/**MyPlaybooks**/ ディレクトリーを作成します。

```
$ mkdir MyPlaybooks
```

2. ~/**MyPlaybooks**/**inventory** ファイルを作成します。

3. 編集するインベントリーファイルを開きます。IdM サーバーとして使用するホストの完全修飾ドメイン名 (**FQDN**) を指定します。**FQDN** が以下の基準を満たしていることを確認してください。

   - 英数字およびハイフン (-) のみが使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
   - ホスト名がすべて小文字である。

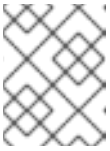
4. IdM ドメインおよびレルムの情報を指定します。

5. 以下のオプションを追加して、統合 DNS を使用することを指定します。

```
ipaserver_setup_dns=true
```

6. DNS 転送設定を指定します。以下のいずれかのオプションを選択します。

   - インストーラーが **/etc/resolv.conf** ファイルからのフォワーダーを使用する場合は、**ipaserver_auto_forwarders=yes** オプションを使用します。**/etc/resolv.conf** ファイルで指定する nameserver が localhost 127.0.0.1 アドレスである場合、または仮想プライベートネットワークにあり、使用している DNS サーバーが通常パブリックインターネットから到達できない場合は、このオプションは使用しないでください。
   - **ipaserver_forwarders** を使用して、フォワーダーを手動で指定します。インストールプロセスにより、インストールした IdM 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。
   - 代わりに使用する root DNS サーバーを設定する場合は、**ipaserver_no_forwarders=yes** オプションを使用します。



注記

DNS フォワーダーがないと、環境は分離され、インフラストラクチャー内の他の DNS ドメインからの名前は解決されません。

7. DNS の逆引きレコードとゾーンの設定を指定します。次のいずれかのオプションを選択します。

   - ゾーンがすでに解決可能であっても、**ipaserver_allow_zone_overlap=yes** オプションを使用して (リバース) ゾーンの作成を許可します。
   - **ipaserver_reverse_zones** オプションを使用して、手動でリバースゾーンを指定します。
   - インストーラーが DNS ゾーンを逆引きで作成しない場合は、**ipaserver_no_reverse=yes** オプションを使用します。

注記

オプションで、逆引きゾーンの管理に IdM を使用できます。代わりに、この目的で外部 DNS サービスを使用することもできます。

8. **admin** と **Directory Manager** のパスワードを指定します。Ansible Vault を使用してパスワードを保存し、Playbook ファイルから Vault ファイルを参照します。あるいは、安全性は低くなりますが、インベントリーファイルにパスワードを直接指定します。

9. (必要に応じて) IdM サーバーで使用する個別の **firewalld** ゾーンを指定します。カスタムゾーンを設定しないと、サービスがデフォルトの **firewalld** ゾーンに追加されます。事前定義されたデフォルトゾーンは **public** です。

重要

指定する **firewalld** ゾーンは存在し、永続的でなければなりません。

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを除く)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
[...]
```

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを含む)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
```

```
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

カスタムの firewalld 損を使用したインベントリーファイルの例

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

Ansible Vault ファイルに保存された admin パスワードおよび Directory Manager パスワードを使用して IdM サーバーを設定する Playbook の例

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

インベントリーファイルの admin パスワードおよび Directory Manager パスワードを使用して IdM サーバーを設定する Playbook の例

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    state: present
```

関連情報

- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.5. 外部 DNS と、ROOT CA としての統合 CA を使用したデプロイメントのパラメーターの設定

以下の手順に従って、外部 DNS ソリューションを使用する環境で、統合 CA の IdM サーバーを root CA としてインストールするようにインベントリーファイルを設定します。

注記

この手順のインベントリーファイルは、**INI**形式を使用します。または、**YAML** 形式または **JSON** 形式を使用できます。

手順

1. ~/**MyPlaybooks**/ ディレクトリーを作成します。

```
$ mkdir MyPlaybooks
```

2. ~/**MyPlaybooks**/**inventory** ファイルを作成します。
3. 編集するインベントリーファイルを開きます。IdM サーバーとして使用するホストの完全修飾ドメイン名 (**FQDN**) を指定します。**FQDN** が以下の基準を満たしていることを確認してください。
   - 英数字およびハイフン (-) のみが使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
   - ホスト名がすべて小文字である。
4. IdM ドメインおよびレルムの情報を指定します。
5. **ipaserver_setup_dns** オプションが **no** に設定されているか、存在しないことを確認します。
6. **admin** と **Directory Manager** のパスワードを指定します。Ansible Vault を使用してパスワードを保存し、Playbook ファイルから Vault ファイルを参照します。あるいは、安全性は低くなりますが、インベントリーファイルにパスワードを直接指定します。
7. (必要に応じて) IdM サーバーで使用する個別の **firewalld** ゾーンを指定します。カスタムゾーンを設定しないと、サービスがデフォルトの **firewalld** ゾーンに追加されます。事前定義されたデフォルトゾーンは **public** です。

重要

指定する **firewalld** ゾーンは存在し、永続的でなければなりません。

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを除く)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを含む)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

カスタムの firewalld 損を使用したインベントリーファイルの例

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone
```

Ansible Vault ファイルに保存された admin パスワードおよび Directory Manager パスワードを使用して IdM サーバーを設定する Playbook の例

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml

  roles:
  - role: ipaserver
    state: present
```

インベントリーファイルの admin パスワードおよび Directory Manager パスワードを使用して IdM サーバーを設定する Playbook の例

```
---
- name: Playbook to configure IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    state: present
```

関連情報

- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.6. ANSIBLE PLAYBOOK を使用して、統合 CA を ROOT CA として備えた IDM サーバーをデプロイメント

以下の手順に従って、Ansible Playbook を使用して、統合された認証局 (CA) を備えた IdM サーバーをデプロイします。

前提条件

- 管理ノードが、静的 IP アドレスと作業パッケージマネージャーを備えた Red Hat Enterprise Linux 9 システムである。
- 以下のいずれかの手順を選択して、シナリオに対応するパラメーターを設定している。
  - 統合 DNS を使用した手順
  - 外部 DNS を使用した手順

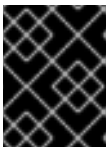
手順

1. Ansible Playbook の実行:

```
$ ansible-playbook -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-server.yml
```

2. 以下のいずれかのオプションを選択します。
   - IdM デプロイメントで外部 DNS を使用する場合: **/tmp/ipa.system.records.UFRPto.db** ファイルに含まれる DNS リソースレコードを、既存の外部 DNS サーバーに追加します。DNS レコードの更新プロセスは、特定の DNS ソリューションによって異なります。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```



重要

既存の DNS サーバーに DNS レコードを追加するまで、サーバーのインストールは完了しません。

   - IdM デプロイメントで統合 DNS を使用している場合は、次のコマンドを実行します。
     - 親ドメインから IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **idm.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

重要

IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

- タイムサーバーの **_ntp._udp** サービス (SRV) レコードを IdM DNS に追加します。IdM DNS に新たにインストールした IdM サーバーのタイムサーバーの SRV レコードが存在すると、今後のレプリカおよびクライアントインストールが、このプライマリー IdM サーバーが使用するタイムサーバーと同期するように自動的に設定されます。

31.7. 統合 DNS と、ルート CA としての外部 CA を使用したデプロイメントのパラメーターの設定

以下の手順に従って、IdM 統合 DNS ソリューションを使用する環境で、外部 CA を持つ IdM サーバーを root CA としてインストールするようにインベントリーファイルを設定します。

注記

この手順のインベントリーファイルは、**INI**形式を使用します。または、**YAML** 形式または **JSON** 形式を使用できます。

手順

1. ~/**MyPlaybooks**/ ディレクトリーを作成します。

```
$ mkdir MyPlaybooks
```

2. ~/**MyPlaybooks**/**inventory** ファイルを作成します。
3. 編集するインベントリーファイルを開きます。IdM サーバーとして使用するホストの完全修飾ドメイン名 (**FQDN**) を指定します。**FQDN** が以下の基準を満たしていることを確認してください。
   - 英数字およびハイフン (-) のみが使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
   - ホスト名がすべて小文字である。
4. IdM ドメインおよびレルムの情報を指定します。
5. 以下のオプションを追加して、統合 DNS を使用することを指定します。

```
ipaserver_setup_dns=true
```

6. DNS 転送設定を指定します。以下のいずれかのオプションを選択します。
   - インストールプロセスで **/etc/resolv.conf** ファイルのフォワーダーを使用する場合は、**ipaserver_auto_forwarders=yes** を使用します。**/etc/resolv.conf** ファイルで指定する nameserver が localhost 127.0.0.1 アドレスである場合、または仮想プライベートネットワークにあり、使用している DNS サーバーが通常パブリックインターネットから到達できない場合は、このオプションを使用することが推奨されません。

- **ipaserver_forwarders** を使用して、フォワーダーを手動で指定します。インストールプロセスにより、インストールした IdM 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。
- 代わりに使用する root DNS サーバーを設定する場合は、**ipaserver_no_forwarders=yes** オプションを使用します。

注記

DNS フォワーダーがないと、環境は分離され、インフラストラクチャー内の他の DNS ドメインからの名前は解決されません。

7. DNS の逆引きレコードとゾーンの設定を指定します。次のいずれかのオプションを選択します。
   - ゾーンがすでに解決可能であっても、**ipaserver_allow_zone_overlap=yes** オプションを使用して (リバース) ゾーンの作成を許可します。
   - **ipaserver_reverse_zones** オプションを使用して、手動でリバースゾーンを指定します。
   - インストールプロセスで DNS ゾーンの逆引きを作成しない場合は、**ipaserver_no_reverse=yes** オプションを使用します。

注記

オプションで、逆引きゾーンの管理に IdM を使用できます。代わりに、この目的で外部 DNS サービスを使用することもできます。

8. **admin** と **Directory Manager** のパスワードを指定します。Ansible Vault を使用してパスワードを保存し、Playbook ファイルから Vault ファイルを参照します。あるいは、安全性は低くなりますが、インベントリーファイルにパスワードを直接指定します。
9. (必要に応じて) IdM サーバーで使用する個別の **firewalld** ゾーンを指定します。カスタムゾーンを設定しないと、サービスがデフォルトの**firewalld** ゾーンに追加されます。事前定義されたデフォルトゾーンは **public** です。

重要

指定する **firewalld** ゾーンは存在し、永続的でなければなりません。

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを除く)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
[...]
```

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを含む)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

カスタムの firewalld 損を使用したインベントリーファイルの例

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=true
ipaserver_auto_forwarders=true
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

10. インストールの最初ステップ用の Playbook を作成します。証明書署名要求 (CSR) を生成し、それをコントローラーからマネージドノードにコピーする指示を入力します。

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: true

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: true
```

11. インストールの最終ステップ用に、別の Playbook を作成します。

```
---
```

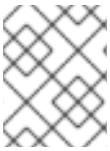
```
- name: Playbook to configure IPA server Step 2
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files:
      - "/root/servercert20240601.pem"
      - "/root/cacert.pem"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] }}-{{ item }}" to "/root/{{ item }}" on node
    ansible.builtin.copy:
      src: "{{ groups.ipaserver[0] }}-{{ item }}"
      dest: "/root/{{ item }}"
      force: true
    with_items:
    - servercert20240601.pem
    - cacert.pem

  roles:
  - role: ipaserver
    state: present
```

関連情報

- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.8. 外部 DNS と、ルート CA としての外部 CA を使用したデプロイメントのパラメーターの設定

以下の手順に従って、外部 DNS ソリューションを使用する環境で、外部 CA を持つ IdM サーバーを root CA としてインストールするようにインベントリーファイルを設定します。



注記

この手順のインベントリーファイルは、**INI**形式を使用します。または、**YAML** 形式または **JSON** 形式を使用できます。

手順

1. **~/MyPlaybooks/** ディレクトリーを作成します。

```
$ mkdir MyPlaybooks
```

2. **~/MyPlaybooks/inventory** ファイルを作成します。
3. 編集するインベントリーファイルを開きます。IdM サーバーとして使用するホストの完全修飾ドメイン名 (**FQDN**) を指定します。**FQDN** が以下の基準を満たしていることを確認してください。

- 英数字およびハイフン (-) のみが使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
- ホスト名がすべて小文字である。

4. IdM ドメインおよびレルムの情報を指定します。
5. **ipaserver_setup_dns** オプションが **no** に設定されているか、存在しないことを確認します。
6. **admin** と **Directory Manager** のパスワードを指定します。Ansible Vault を使用してパスワードを保存し、Playbook ファイルから Vault ファイルを参照します。あるいは、安全性は低くなりますが、インベントリーファイルにパスワードを直接指定します。
7. (必要に応じて) IdM サーバーで使用する個別の **firewalld** ゾーンを指定します。カスタムゾーンを設定しないと、サービスがデフォルトの **firewalld** ゾーンに追加されます。事前定義されたデフォルトゾーンは **public** です。

重要

指定する **firewalld** ゾーンは存在し、永続的でなければなりません。

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを除く)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
[...]
```

必要なサーバー情報を含むインベントリーファイルの例 (パスワードを含む)

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234

[...]
```

カスタムの firewalld 損を使用したインベントリーファイルの例

```
[ipaserver]
server.idm.example.com

[ipaserver:vars]
ipaserver_domain=idm.example.com
ipaserver_realm=IDM.EXAMPLE.COM
```

```
ipaserver_setup_dns=no
ipaadmin_password=MySecretPassword123
ipadm_password=MySecretPassword234
ipaserver_firewalld_zone=custom zone

[...]
```

8. インストールの最初ステップ用の Playbook を作成します。証明書署名要求 (CSR) を生成し、それをコントローラーからマネージドノードにコピーする指示を入力します。

```
---
- name: Playbook to configure IPA server Step 1
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_ca: true

  roles:
  - role: ipaserver
    state: present

  post_tasks:
  - name: Copy CSR /root/ipa.csr from node to "{{ groups.ipaserver[0] + '-ipa.csr' }}"
    fetch:
      src: /root/ipa.csr
      dest: "{{ groups.ipaserver[0] + '-ipa.csr' }}"
      flat: true
```

9. インストールの最終ステップ用に、別の Playbook を作成します。

```
---
- name: Playbook to configure IPA server Step 2
  hosts: ipaserver
  become: true
  vars_files:
  - playbook_sensitive_data.yml
  vars:
    ipaserver_external_cert_files:
      - "/root/servercert20240601.pem"
      - "/root/cacert.pem"

  pre_tasks:
  - name: Copy "{{ groups.ipaserver[0] }}-{{ item }}" to "/root/{{ item }}" on node
    ansible.builtin.copy:
      src: "{{ groups.ipaserver[0] }}-{{ item }}"
      dest: "/root/{{ item }}"
      force: true
    with_items:
    - servercert20240601.pem
    - cacert.pem
```

```
roles:
- role: ipaserver
  state: present
```

関連情報

- IdM サーバーのインストール: 統合 DNS なしで外部 CA を root CA として使用する場合
- man **ipa-server-install(1)**
- **/usr/share/doc/ansible-freeipa/README-server.md**

31.9. 外部 CA を ROOT CA として備えた IDM サーバーの ANSIBLE PLAYBOOK を使用したデプロイメント

以下の手順に従って、Ansible Playbook を使用して、外部認証局 (CA) を備えた IdM サーバーをデプロイします。

前提条件

- 管理ノードが、静的 IP アドレスと作業パッケージマネージャーを備えた Red Hat Enterprise Linux 9 システムである。
- 以下のいずれかの手順を選択して、シナリオに対応するパラメーターを設定している。
  - 統合 DNS を使用した手順
  - 外部 DNS を使用した手順

手順

1. インストールの最初のステップの指示に従って Ansible Playbook を実行します (例: **install-server-step1.yml**)。

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
~/MyPlaybooks/install-server-step1.yml
```

2. コントローラー上の **ipa.csr** 証明書署名要求ファイルを見つけ、これを外部 CA に送信します。
3. 外部 CA が署名した IdM CA 証明書をコントローラーファイルシステムに配置して、次のステップの Playbook で見つけられるようにします。
4. インストールの最終ステップの指示に従って Ansible Playbook を実行します (例: **install-server-step2.yml**)。

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-server-
step2.yml
```

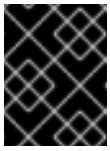
5. 以下のいずれかのオプションを選択します。
   - IdM デプロイメントで外部 DNS を使用する場合: **/tmp/ipa.system.records.UFRPto.db** ファイルに含まれる DNS リソースレコードを、既存の外部 DNS サーバーに追加します。DNS レコードの更新プロセスは、特定の DNS ソリューションによって異なります。

```
...
Restarting the KDC
Please add records in this file to your DNS system:
/tmp/ipa.system.records.UFRBto.db
Restarting the web server
...
```

重要

既存の DNS サーバーに DNS レコードを追加するまで、サーバーのインストールは完了しません。

- IdM デプロイメントで統合 DNS を使用している場合は、次のコマンドを実行します。
  - 親ドメインから IdM DNS ドメインに DNS 委譲を追加します。たとえば、IdM DNS ドメインが **idm.example.com** の場合は、ネームサーバー (NS) レコードを親ドメイン **example.com** に追加します。

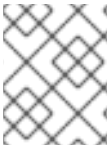
    

    重要

    IdM DNS サーバーをインストールするたびに、この手順を繰り返します。

  - タイムサーバーの **_ntp._udp** サービス (SRV) レコードを IdM DNS に追加します。IdM DNS に新たにインストールした IdM サーバーのタイムサーバーの SRV レコードが存在すると、今後のレプリカおよびクライアントインストールが、このプライマリー IdM サーバーが使用するタイムサーバーと同期するように自動的に設定されます。

31.10. ANSIBLE PLAYBOOK を使用した IDM サーバーのアンインストール



注記

既存の Identity Management (IdM) デプロイメントでは、**レプリカ** と **サーバー** は置き替え可能な用語です。

以下の手順に従って、Ansible Playbook を使用して IdM レプリカをアンインストールします。この例では、以下が適用されます。

- IdM 設定は、**server123.idm.example.com** からアンインストールされます。
- **server123.idm.example.com** と関連するホストエントリーが IdM トポロジーから削除されます。

前提条件

- コントロールノードでは、
  - Ansible バージョン 2.14 以降を使用している。
  - **ansible-freeipa** パッケージをインストールしている。

- ~/MyPlaybooks/ ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成した。この例では、FQDN は **server123.idm.example.com** です。
- **secret.yml** Ansible vault に **ipaadmin_password** が保存されている。
- **ipaserver_remove_from_topology** オプションを機能させるには、システムが RHEL 8.9 以降で実行されている必要があります。

- マネージドノードでは、
  - システムは RHEL 8 上で実行されています。

手順

1. Ansible Playbook ファイル **uninstall-server.yml** を次の内容で作成します。

```
---
- name: Playbook to uninstall an IdM replica
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    ipaserver_remove_from_domain: true
    state: absent
```

ipaserver_remove_from_domain オプションは、IdM トポロジーからホストを登録解除します。

注記

server123.idm.example.com を削除するとトポロジーが切断される場合は、削除は中止されます。詳細は、Ansible Playbook を使用した IdM サーバーのアンインストール (トポロジーが切断された場合でも) を参照してください。

2. レプリカをアンインストールします。

```
$ ansible-playbook --vault-password-file=password_file -v -i
<path_to_inventory_directory>/inventory <path_to_playbooks_directory>/uninstall-
server.yml
```

3. **server123.idm.example.com** を指しているネームサーバー (NS) DNS レコードがすべて DNS ゾーンから削除されていることを確認してください。使用する DNS が IdM により管理される統合 DNS であるか、外部 DNS であるかに関わらず、確認を行なってください。IdM から DNS レコードを削除する方法は、 Deleting DNS records in the IdM CLI を参照してください。

31.11. ANSIBLE PLAYBOOK を使用した IDM サーバーのアンインストール (トポロジーが切断された場合でも)

注記

既存の Identity Management (IdM) デプロイメントでは、**レプリカ** と **サーバー** は置き替え可能な用語です。

IdM トポロジーが切断されたとしても、Ansible Playbook を使用して IdM レプリカをアンインストールするには、以下の手順を実行します。この例では、**server456.idm.example.com** を使用して、レプリカと、トポロジーから **server123.idm.example.com** の FQDN を持つ関連付けられたホストエントリーを削除します。これにより、特定のレプリカが **server456.idm.example.com** および残りのトポロジーから切断されます。

注記

remove_server_from_domain のみを使用してトポロジーからレプリカを削除しても、トポロジーは切断されないため、他のオプションは必要ありません。トポロジーが切断される結果となった場合は、ドメインの保持したい部分を指定する必要があります。その場合、以下を実行する必要があります。

- **ipaserver_remove_on_server** 値を指定します。
- **ipaserver_ignore_topology_disconnect** を True に設定します。

前提条件

- コントロールノードでは、
  - Ansible バージョン 2.14 以降を使用している。
  - システムが RHEL 8.9 以降で実行されている。
  - **ansible-freeipa** パッケージをインストールしている。
  - **~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成した。この例では、FQDN は **server123.idm.example.com** です。
  - **secret.yml** Ansible vault に **ipaadmin_password** が保存されている。
- マネージドノードでは、
  - システムは 8 以降で実行されています。

手順

1. Ansible Playbook ファイル **uninstall-server.yml** を次の内容で作成します。

```
---
- name: Playbook to uninstall an IdM replica
  hosts: ipaserver
  become: true

  roles:
  - role: ipaserver
    ipaserver_remove_from_domain: true
```

```
ipaserver_remove_on_server: server456.idm.example.com
ipaserver_ignore_topology_disconnect: true
state: absent
```

注記

通常の状況では、server123 を削除してもトポロジーが切断されない場合で、**ipaserver_remove_on_server** の値が設定されていない場合は、server123 が削除されたレプリカは server123 のレプリカ合意を使用して自動的に決定されます。

2. レプリカをアンインストールします。

```
$ ansible-playbook --vault-password-file=password_file -v -i
<path_to_inventory_directory>/hosts <path_to_playbooks_directory>/uninstall-
server.yml
```

3. **server123.idm.example.com** を指しているネームサーバー (NS) DNS レコードがすべて DNS ゾーンから削除されていることを確認してください。使用する DNS が IdM により管理される統合 DNS であるか、外部 DNS であるかに関わらず、確認を行なってください。IdM から DNS レコードを削除する方法は、 Deleting DNS records in the IdM CLI を参照してください。

31.12. 関連情報

- レプリカトポロジーの計画
- Ansible Playbook を使用した IdM サーバーのバックアップおよび復元
- インベントリーの基本: 形式、ホスト、およびグループ

第32章 ANSIBLE PLAYBOOK で IDENTITY MANAGEMENT レプリカのインストール

Ansible を使用してシステムを IdM レプリカとして設定すると、IdM ドメインに登録され、ドメインの IdM サーバーにある IdM サービスをシステムが使用できるようになります。

デプロイメントは、Ansible ロール **ipareplica** で管理されます。このロールは、自動検出モードを使用して、IdM サーバー、ドメイン、およびその他の設定を識別できます。ただし、複数のレプリカを階層のようなモデルでデプロイし、そのレプリカのグループを異なるタイミングでデプロイする場合には、グループごとに特定のサーバーまたはレプリカを定義する必要があります。

前提条件

- Ansible コントロールノードに ansible-freeipa パッケージがインストールされている。
- Ansible と IdM の一般的な概念を理解しています。
- デプロイメント内のレプリカトポロジーを計画し ました。

32.1. IDM レプリカをインストールするためのベース変数、サーバー変数、およびクライアント変数の指定

IdM レプリカをインストールするためのインベントリーファイルを設定するには、以下の手順を完了します。

前提条件

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。

手順

1. 編集するインベントリーファイルを開きます。IdM レプリカとなるホストの完全修飾ドメイン名 (FQDN) を指定します。FQDN 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 (-) のみを使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
   - ホスト名がすべて小文字である。

   レプリカの FQDN のみが定義されている単純なインベントリーホストファイルの例

   ```
   [ipareplicas]
   replica1.idm.example.com
   replica2.idm.example.com
   replica3.idm.example.com
   [...]
   ```

   IdM サーバーがデプロイされており、SRV レコードが IdM DNS ゾーンに適切に設定されている場合、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ます。

2. [オプション] トポロジーの設計方法に基づいて、インベントリーファイルに追加情報を入力します。

シナリオ 1

自動検出を回避し、**[ipareplicas]** セクションに記載されているすべてのレプリカが特定の IdM サーバーを使用するようにするには、インベントリーファイルの **[ipaservers]** セクションにそのサーバーを設定します。

IdM サーバーとレプリカの FQDN が定義されているインベントリーホストファイルの例

```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]
```

シナリオ 2

または、自動検出を回避して、特定のサーバーで特定のレプリカをデプロイする場合は、インベントリーファイルの **[ipareplicas]** セクションに、特定のレプリカのサーバーを個別に設定します。

特定のレプリカ用に特定の IdM サーバーが定義されたインベントリーファイルの例

```
[ipaservers]
server.idm.example.com
replica1.idm.example.com

[ipareplicas]
replica2.idm.example.com
replica3.idm.example.com ipareplica_servers=replica1.idm.example.com
```

上記の例では、**replica3.idm.example.com** が、すでにデプロイされた **replica1.idm.example.com** を複製元として使用します。

シナリオ 3

1 つのバッチに複数のレプリカをデプロイする場合は、多層レプリカのデプロイメントが役に立ちます。インベントリーファイルにレプリカの特定グループ (例: **[ipareplicas_tier1]** および **[ipareplicas_tier2]**) を定義し、Playbook **install-replica.yml** で各グループに個別のプレイを設計します。

レプリカ階層が定義されているインベントリーファイルの例

```
[ipaservers]
server.idm.example.com

[ipareplicas_tier1]
replica1.idm.example.com
```

```
[ipareplicas_tier2]
replica2.idm.example.com \
ipareplica_servers=replica1.idm.example.com,server.idm.example.com
```

ipareplica_servers の最初のエントリーが使用されます。次のエントリーは、フォールバックオプションとして使用されます。IdM レプリカのデプロイに複数の層を使用する場合は、最初に tier1 からレプリカをデプロイし、次に tier2 からレプリカをデプロイするように、Playbook に個別のタスクが必要です。

レプリカグループごとに異なるプレイを定義した Playbook ファイルの例

```
---
- name: Playbook to configure IPA replicas (tier1)
  hosts: ipareplicas_tier1
  become: true

  roles:
  - role: ipareplica
    state: present

- name: Playbook to configure IPA replicas (tier2)
  hosts: ipareplicas_tier2
  become: true

  roles:
  - role: ipareplica
    state: present
```

3. [オプション] **firewalld** と DNS に関する追加情報を入力します。

シナリオ 1

レプリカで指定された **ファイアウォール** ゾーン (内部ゾーンなど) を使用するようにする場合は、インベントリーファイルで指定できます。カスタムゾーンを設定しないと、サービスがデフォルトの **firewalld** ゾーンに追加されます。事前定義されたデフォルトゾーンは **public** です。

重要

指定する **firewalld** ゾーンは存在し、永続的でなければなりません。

カスタム firewalld 帯を持つシンプルなインベントリーホストファイルの例

```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_firewalld_zone=custom zone
```

シナリオ 2

レプリカが IdM DNS サービスをホストするようにする場合は、**ipareplica_setup_dns=yes** 行を **[ipareplicas:vars]** セクションに追加します。また、サーバーごとの DNS フォワーダーを使用するかどうかを指定します。

- サーバーごとのフォワーダーを設定するには、**ipareplica_forwarders** 変数と文字列のリストを **[ipareplicas:vars]** セクションに追加します (例: ipareplica_forwarders=192.0.2.1,192.0.2.2)。
- サーバーごとにフォワーダーを設定しない場合は、ipareplica_no_forwarders=yes の行を **[ipareplicas:vars]** セクションに追加します。
- レプリカの **/etc/resolv.conf** ファイルにリスト表示されているフォワーダーに基づいてサーバーごとにフォワーダーを設定するには、**[ipareplicas:vars]** セクションに **ipareplica_auto_forwarders** を追加します。

レプリカに DNS とサーバーごとのフォワーダーを設定する手順を含むインベントリーファイルの例

```
[ipaservers]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com
replica3.idm.example.com
[...]

[ipareplicas:vars]
ipareplica_setup_dns=true
ipareplica_forwarders=192.0.2.1,192.0.2.2
```

シナリオ 3

ipaclient_configure_dns_resolve および **ipaclient_dns_servers** オプション (使用可能な場合) を使用して DNS リゾルバーを指定し、クラスターのデプロイメントを簡素化します。これは、IdM デプロイメントが統合 DNS を使用している場合に特に便利です。

DNS リゾルバーを指定するインベントリーファイルスニペット:

```
[...]
[ipaclient:vars]
ipaclient_configure_dns_resolver=true
ipaclient_dns_servers=192.168.100.1
```

注記

ipaclient_dns_servers リストには IP アドレスのみを含める必要があります。ホスト名を含めることはできません。

関連情報

- **/usr/share/ansible/roles/ipareplica/README.md**

32.2. ANSIBLE PLAYBOOK を使用して IDM レプリカをインストールするための認証情報の指定

この手順は、IdM レプリカのインストールに認可を設定します。

前提条件

- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。

手順

1. **レプリカをデプロイする権限のあるユーザーのパスワード** (IdM の **admin** など) を指定します。
   - Red Hat は、Ansible Vault を使用してパスワードを保存し、Playbook ファイルから Vault ファイルを参照する (**install-replica.yml** など) ことを推奨します。

     Ansible Vault ファイルのインベントリーファイルおよびパスワードのプリンシパルを使用した Playbook ファイルの例

     ```
     - name: Playbook to configure IPA replicas
       hosts: ipareplicas
       become: true
       vars_files:
       - playbook_sensitive_data.yml

       roles:
       - role: ipareplica
         state: present
     ```

     Ansible Vault の使用方法は、公式の Ansible Vault ドキュメントを参照してください。
   - あまり安全ではありませんが、インベントリーファイルで **admin** の認証情報を直接提供します。インベントリーファイルの **[ipareplicas:vars]** セクションで **ipaadmin_password** オプションを使用します。インベントリーファイルと、Playbook ファイル **install-replica.yml** は以下のようになります。

     インベントリーの hosts.replica ファイルの例

     ```
     [...]
     [ipareplicas:vars]
     ipaadmin_password=Secret123
     ```

     インベントリーファイルのプリンシパルおよびパスワードを使用した Playbook の例

     ```
     - name: Playbook to configure IPA replicas
       hosts: ipareplicas
       become: true
     ```

```
  roles:
  - role: ipareplica
    state: present
```

- または、安全性は低くなりますが、レプリカをインベントリーファイルに直接デプロイすることを許可されている別のユーザーの認証情報を提供します。別の認証ユーザーを指定するには、ユーザー名に **ipaadmin_principal** オプションを使用し、パスワードに **ipaadmin_password** オプションを使用します。インベントリーファイルと、Playbook ファイル **install-replica.yml** は以下のようになります。

  インベントリーの hosts.replica ファイルの例

```
[...]
[ipareplicas:vars]
ipaadmin_principal=my_admin
ipaadmin_password=my_admin_secret123
```

  インベントリーファイルのプリンシパルおよびパスワードを使用した Playbook の例

```
- name: Playbook to configure IPA replicas
  hosts: ipareplicas
  become: true

  roles:
  - role: ipareplica
    state: present
```

関連情報

- **/usr/share/ansible/roles/ipareplica/README.md**

32.3. ANSIBLE PLAYBOOK で IDM レプリカのデプロイメント

以下の手順に従って、Ansible Playbook を使用して IdM レプリカをデプロイします。

前提条件

- 管理ノードが、静的 IP アドレスと作業パッケージマネージャーを備えた Red Hat Enterprise Linux 9 システムである。
- IdM レプリカをインストールするためのインベントリーファイル を設定しました。
- IdM レプリカをインストールするための認証 を設定しました。

手順

- Ansible Playbook の実行:

```
$ ansible-playbook -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-replica.yml
```

32.4. ANSIBLE PLAYBOOK を使用した IDM レプリカのアンインストール

注記

既存の Identity Management (IdM) デプロイメントでは、**レプリカ** と **サーバー** は置き替え可能な用語です。IdM サーバーをアンインストールする方法の詳細は、Ansible Playbook を使用した IdM サーバーのアンインストール または トポロジーが切断される場合でも Ansible Playbook を使用して IdM サーバーをアンインストールする を参照してください。

関連情報

- IdM のサーバーおよびクライアントの概要

第33章 ANSIBLE PLAYBOOK で IDENTITY MANAGEMENT クライアントのインストール

Ansible 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。

デプロイメントは、Ansible ロール **ipaclient** により管理されます。デフォルトでは、ロールは自動検出モードを使用して、IdM サーバー、ドメイン、およびその他の設定を特定します。ロールは、Ansible Playbook がインベントリーファイルなどに指定した設定を使用するように変更できます。

前提条件

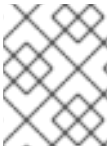
- Ansible コントロールノードに ansible-freeipa パッケージがインストールされている。
- Ansible バージョン 2.14 以降を使用している。
- Ansible と IdM の一般的な概念を理解しています。

33.1. 自動検出クライアントインストールモードでインベントリーファイルのパラメーターの設定

Ansible Playbook を使用して Identity Management クライアントをインストールするには、インベントリーファイルでターゲットホストパラメーターを設定します (例: **inventory/hosts**)。

- ホストに関する情報
- タスクの承認

インベントリーファイルは、所有するインベントリープラグインに応じて、多数ある形式のいずれかになります。**INI-like** 形式は Ansible のデフォルトで、以下の例で使用されています。



注記

RHEL でグラフィカルユーザーインターフェイスでスマートカードを使用するには、Ansible Playbook に **ipaclient_mkhomedir** 変数を含めるようにします。

手順

1. **インベントリー** ファイルを開いて編集します。
2. IdM クライアントになるホストの完全修飾ホスト名 (FQDN) を指定します。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 (-) のみを使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
   - ホスト名がすべて小文字である。大文字は使用できません。

   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。

   クライアントの FQDN のみが定義されている単純なインベントリーホストファイルの例

```
[ipaclients]
client.idm.example.com
[...]
```

3. クライアントを登録するための認証情報を指定します。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パスワード**。以下はデフォルトのオプションになります。
  - Red Hat は、Ansible Vault を使用してパスワードを保存し、Playbook ファイル (**install-client.yml** など) から Vault ファイルを直接参照することを推奨します。

    Ansible Vault ファイルのインベントリーファイルおよびパスワードのプリンシパルを使用した Playbook ファイルの例

    ```
    - name: Playbook to configure IPA clients with username/password
      hosts: ipaclients
      become: true
      vars_files:
      - playbook_sensitive_data.yml

      roles:
      - role: ipaclient
        state: present
    ```

  - あまり安全ではありませんが、**inventory/hosts** ファイルの **[ipaclients:vars]** セクションに **ipaadmin_password** オプションを使用して、**admin** の認証情報を提供します。また、別の認証ユーザーを指定するには、ユーザー名に **ipaadmin_principal** オプション、パスワードに **ipaadmin_password** オプションを使用します。**inventory/hosts** インベントリーファイルと、Playbook ファイル **install-client.yml** は以下のようになります。

    インベントリーホストファイルの例

    ```
    [...]
    [ipaclients:vars]
    ipaadmin_principal=my_admin
    ipaadmin_password=Secret123
    ```

    インベントリーファイルのプリンシパルおよびパスワードを使用した Playbook の例

    ```
    - name: Playbook to unconfigure IPA clients
      hosts: ipaclients
      become: true

      roles:
      - role: ipaclient
        state: true
    ```

- 以前登録した **クライアントキータブ** が利用できる場合は、以下を行います。
  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、**#ipaclient_keytab** オプションのコメントを解除して、キータブを保存するファイルへのパスを指定します (例:

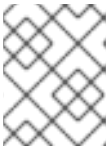
inventory/hosts の **[ipaclient:vars]** セクション)。

- 登録時に生成される **ランダムなワンタイムパスワード** (OTP)。この認証方法を使用するには、インベントリーファイルの ipaclient_use_otp=yes オプションを使用します。たとえば、**inventory/hosts** ファイルの [ipaclients:vars] セクションで ipaclient_use_otp=yes オプションのコメントを解除できます。OTP では、以下のいずれかのオプションも指定する必要があります。
  - **クライアントを登録する権限のあるユーザーのパスワード** (例: **inventory/hosts** ファイルの **[ipaclients:vars]** セクションに **ipaadmin_password** の値を指定)。
  - **管理者キータブ** (例: **inventory/hosts** の **[ipaclients:vars]** セクションに **ipaadmin_keytab** の値を指定)。

4. (オプション) **ipaclient_configure_dns_resolve** および **ipaclient_dns_servers** オプション (使用可能な場合) を使用して DNS リゾルバーを指定し、クラスターのデプロイメントを簡素化します。これは、IdM デプロイメントが統合 DNS を使用している場合に特に便利です。

   DNS リゾルバーを指定するインベントリーファイルスニペット:

   ```
   [...]
   [ipaclients:vars]
   ipaadmin_password: "{{ ipaadmin_password }}"
   ipaclient_domain=idm.example.com
   ipaclient_configure_dns_resolver=true
   ipaclient_dns_servers=192.168.100.1
   ```

   注記

   ipaclient_dns_servers リストには IP アドレスのみを含める必要があります。ホスト名を含めることはできません。

5. RHEL 8.9 以降では、**ipaclient_subid: true** オプションを指定して、IdM ユーザーのサブ ID 範囲を IdM レベルで設定することもできます。

関連情報

- **/usr/share/ansible/roles/ipaclient/README.md**
- subID 範囲の手動管理

33.2. クライアントのインストール時に自動検出ができない場合に備えてインベントリーファイルのパラメーターの設定

Ansible Playbook を使用して Identity Management クライアントをインストールするには、インベントリーファイルでターゲットホストパラメーターを設定します (例: **inventory/hosts**)。

- ホストと、IdM サーバーおよび IdM ドメインまたは IdM レルムに関する情報
- タスクの承認

インベントリーファイルは、所有するインベントリープラグインに応じて、多数ある形式のいずれかになります。**INI-like** 形式は Ansible のデフォルトで、以下の例で使用されています。

注記

RHEL でグラフィカルユーザーインターフェイスでスマートカードを使用するには、Ansible Playbook に **ipaclient_mkhomedir** 変数を含めるようにします。

手順

1. IdM クライアントになるホストの完全修飾ホスト名 (FQDN) を指定します。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 (**-**) のみを使用できる。たとえば、アンダーラインは使用できないため、DNS の障害が発生する原因となる可能性があります。
   - ホスト名がすべて小文字である。大文字は使用できません。
2. **inventory/hosts** ファイルの関連セクションに、他のオプションを指定します。
   - **[ipaservers]** セクションのサーバーの FQDN は、クライアントが登録される IdM サーバーを示します。
   - 以下のいずれかのオプションを使用できます。
     - クライアントが登録される IdM サーバーの DNS ドメイン名を指定する **[ipaclients:vars]** セクションの **ipaclient_domain** オプション
     - IdM サーバーが制御する Kerberos レルムの名前を示す **[ipaclients:vars]** セクションの **ipaclient_realm** オプション

       クライアント FQDN、サーバーの FQDN、およびドメインが定義されているインベントリーホストファイルの例

       ```
       [ipaclients]
       client.idm.example.com

       [ipaservers]
       server.idm.example.com

       [ipaclients:vars]
       ipaclient_domain=idm.example.com
       [...]
       ```
3. クライアントを登録するための認証情報を指定します。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パスワード**。以下はデフォルトのオプションになります。
     - Red Hat は、Ansible Vault を使用してパスワードを保存し、Playbook ファイル (**install-client.yml** など) から Vault ファイルを直接参照することを推奨します。

       Ansible Vault ファイルのインベントリーファイルおよびパスワードのプリンシパルを使用した Playbook ファイルの例

       ```
       - name: Playbook to configure IPA clients with username/password
         hosts: ipaclients
         become: true
         vars_files:
       ```

```
- playbook_sensitive_data.yml

roles:
- role: ipaclient
  state: present
```

- 安全性は低くなりますが、**inventory/hosts** ファイルの **[ipaclients:vars]** セクションの **ipaadmin_password** オプションを使用して、**admin** の認証情報が提供されます。また、別の認証ユーザーを指定するには、ユーザー名に **ipaadmin_principal** オプション、パスワードに **ipaadmin_password** オプションを使用します。これにより、Playbook ファイル **install-client.yml** は、以下のようになります。

  インベントリーホストファイルの例

  ```
  [...]
  [ipaclients:vars]
  ipaadmin_principal=my_admin
  ipaadmin_password=Secret123
  ```

  インベントリーファイルのプリンシパルおよびパスワードを使用した Playbook の例

  ```
  - name: Playbook to unconfigure IPA clients
    hosts: ipaclients
    become: true

    roles:
    - role: ipaclient
      state: true
  ```

- 以前登録した **クライアントキータブ** が利用できる場合は、以下を行います。
  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、**ipaclient_keytab** オプションをコメント解除します。たとえば、**inventory/hosts** の **[ipaclient:vars]** セクションにあるように、キータブを格納しているファイルへのパスを指定します。

- 登録時に生成される **ランダムなワンタイムパスワード** (OTP)。この認証方法を使用するには、インベントリーファイルの ipaclient_use_otp=yes オプションを使用します。たとえば、**inventory/hosts** ファイルの [ipaclients:vars] セクションで ipaclient_use_otp=yes オプションのコメントを解除できます。OTP では、以下のいずれかのオプションも指定する必要があります。

  - **クライアントを登録する権限のあるユーザーのパスワード** (例: **inventory/hosts** ファイルの **[ipaclients:vars]** セクションに **ipaadmin_password** の値を指定)。

  - **管理者キータブ** (例: **inventory/hosts** の **[ipaclients:vars]** セクションに **ipaadmin_keytab** の値を指定)。

4. RHEL 8.9 以降では、**ipaclient_subid: true** オプションを指定して、IdM ユーザーのサブ ID 範囲を IdM レベルで設定することもできます。

関連情報

- **/usr/share/ansible/roles/ipaclient/README.md**

- subID 範囲の手動管理

33.3. ANSIBLE PLAYBOOK で IDM クライアント登録の認可オプション

次のいずれかの方法を使用して、IdM クライアントの登録を承認できます。

- クライアントを登録する権限を持つユーザーのパスワード: Ansible vault に保存されているパスワード
- クライアントを登録する権限を持つユーザーのパスワード: インベントリーファイルに保存されているパスワード
- ランダムなワンタイムパスワード (OTP)+ 管理者パスワード
- ランダムなワンタイムパスワード (OTP)+ 管理者キータブ
- 前回登録時のクライアントキータブ

以下は、これらのメソッドのサンプルインベントリーファイルと **install-client.yml** Playbook ファイルです。

表33.1 クライアントを登録する権限を持つユーザーのパスワード: Ansible vault に保存されているパスワード

インベントリーファイルの例	Playbook ファイル **install-client.yml** の例

[ipaclients:vars]
[...]
	- name: Playbook to configure IPA clients with username/password
	  hosts: ipaclients
	  become: true
	  vars_files:
	  - playbook_sensitive_data.yml
	
	  roles:
	  - role: ipaclient
	  state: present

表33.2 クライアントを登録する権限を持つユーザーのパスワード: インベントリーファイルに保存されているパスワード

インベントリーファイルの例	Playbook ファイル **install-client.yml** の例

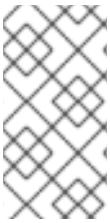
[ipaclients:vars]
ipaadmin_password=Secret123
	- name: Playbook to configure IPA clients
	  hosts: ipaclients
	  become: true
	
	  roles:
	  - role: ipaclient
	  state: true

表33.3 ランダムなワンタイムパスワード (OTP)+ 管理者パスワード

インベントリーファイルの例	Playbook ファイル **install-client.yml** の例
[ipaclients:vars] ipaadmin_password=Secret123 ipaclient_use_otp=true Playbook の実行中に OTP を生成する場合 **または、以下を実行します。** [ipaclients:vars] ipaclient_otp=<W5YpARl=7M.> インストール前に IdM **管理者** によって OTP がすでに生成されている場合	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true

表33.4 ランダムなワンタイムパスワード (OTP)+ 管理者キータブ

インベントリーファイルの例	Playbook ファイル **install-client.yml** の例
[ipaclients:vars] ipaadmin_keytab=/root/admin.keytab ipaclient_use_otp=true	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true



注記

RHEL 8.8 以降、上記の 2 つの OTP 承認シナリオでは、**kinit** コマンドを使用した管理者の TGT の要求は、最初に指定または検出された IdM サーバーで行われます。したがって、Ansible コントロールノードを追加変更する必要はありません。RHEL 8.8 より前は、制御ノードに **krb5-workstation** パッケージが必要でした。

表33.5 前回登録時のクライアントキータブ

インベントリーファイルの例	Playbook ファイル **install-client.yml** の例

インベントリーファイルの例	Playbook ファイル **install-client.yml** の例
[ipaclients:vars] ipaclient_keytab=/root/krb5.keytab	- name: Playbook to configure IPA clients hosts: ipaclients become: true roles: - role: ipaclient state: true

33.4. ANSIBLE PLAYBOOK を使用した IDM クライアントのデプロイ

Ansible Playbook を使用して IdM 環境に IdM クライアントをデプロイするには、この手順を完了します。

前提条件

- 管理ノードが、静的 IP アドレスと作業パッケージマネージャーを備えた Red Hat Enterprise Linux 9 システムである。
- IdM クライアントのデプロイメントのパラメーターを、デプロイメントシナリオに対応するように設定している。
  - 自動検出クライアントインストールモードでインベントリーファイルのパラメーターの設定
  - クライアントのインストール時に自動検出ができない場合に備えてインベントリーファイルのパラメーターの設定

手順

- Ansible Playbook の実行:

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory ~/MyPlaybooks/install-client.yml
```

33.5. ANSIBLE のワンタイムパスワード方式を使用して IDM クライアントをインストールする

アイデンティティー Management (IdM) で新しいホストのワンタイムパスワード (OTP) を生成し、それを使用してシステムを IdM ドメインに登録できます。この手順では、別の IdM ホストで IdM クライアントの OTP を生成した後、Ansible を使用して IdM クライアントをインストールする方法について説明します。

IdM クライアントをインストールするこの方法は、組織内に異なる権限を持つ 2 人のシステム管理者が存在する場合に便利です。

- IdM 管理者の認証情報を持つもの。
- IdM クライアントになるためのホストへの **ルート** アクセスを含む、必要な Ansible 認証情報を持つ別のもの。

IdM 管理者は、OTP パスワードが生成される手順の最初の部分を実行します。Ansible 管理者は、OTP を使用して IdM クライアントをインストールする手順の残りの部分を実行します。

前提条件

- IdM **管理者の** 認証情報、または少なくとも **ホスト登録** 権限と、IdM に DNS レコードを追加する権限を持っている必要があります。
- IdM クライアントをインストールできるように、Ansible 管理対象ノードでユーザーエスカレーションメソッドを設定しました。
- Ansible コントロールノードが RHEL 8.7 以前で実行されている場合は、Ansible コントロールノードにパッケージをインストールできる必要があります。
- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイルを作成しました。
- 管理ノードが、静的 IP アドレスと作業パッケージマネージャーを備えた Red Hat Enterprise Linux 9 システムである。

手順

1. **ホスト登録** 権限と DNS レコードを追加する権限を持つ役割を持つ IdM ユーザーとして IdM ホストに **SSH 接続します**。

```
$ ssh admin@server.idm.example.com
```

2. 新しいクライアントの OTP を生成します。

```
[admin@server ~]$ ipa host-add client.idm.example.com --ip-address=172.25.250.11 --
random
 ----------------------------------------------------
 Added host "client.idm.example.com"
 ----------------------------------------------------
  Host name: client.idm.example.com
  Random password: W5YpARl=7M.n
  Password: True
  Keytab: False
  Managed by: server.idm.example.com
```

--ip-address= <your_host_ip_address> オプションは、指定された IP アドレスを持つホストを IdM DNS に追加します。

3. IdM ホストを終了します。

```
$ exit
logout
Connection to server.idm.example.com closed.
```

4. Ansible コントローラーで、ランダムパスワードを含めるようにインベントリーファイルを更新します。

```
[...]
[ipaclients]
client.idm.example.com

[ipaclients:vars]
ipaclient_domain=idm.example.com
ipaclient_otp=W5YpARl=7M.n
[...]
```

5. Ansible コントローラーが RHEL 8.7 以前を実行している場合は、**krb5-workstation** パッケージによって提供される **kinit** ユーティリティーをインストールします。

```
$ sudo dnf install krb5-workstation
```

6. Playbook を実行してクライアントをインストールします。

```
$ ansible-playbook -i inventory install-client.yml
```

33.6. ANSIBLE インストール後の 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イス (CLI) により、**ansible-playbook** コマンドが成功したことが表示されますが、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、サーバーに定義し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、サーバーに定義したユーザーを解決できることを確認します。たとえば、デフォルトの **admin** ユーザーを確認するには、次のコマンドを実行します。

```
[user@client1 ~]$ id admin
uid=1254400000(admin) gid=1254400000(admins) groups=1254400000(admins)
```

認証が適切に機能していることをテストするには、別の既存 IdM ユーザーで **su -** を実行します。

```
[user@client1 ~]$ su - idm_user
Last login: Thu Oct 18 18:39:11 CEST 2018 from 192.168.122.1 on pts/0
[idm_user@client1 ~]$
```

33.7. ANSIBLE PLAYBOOK での IDM クライアントのアンインストール

以下の手順に従って、Ansible Playbook を使用して IdM クライアントと機能していたホストをアンインストールします。

前提条件

- IdM 管理者の認証情報
- 管理対象ノードは、静的 IP アドレスを持つ Red Hat Enterprise Linux 8 システムです。

手順

- クライアントをアンインストールするための手順を記述した Ansible Playbook を実行します (例: **uninstall-client.yml**)。

```
$ ansible-playbook -v -i ~/MyPlaybooks/inventory ~/MyPlaybooks/uninstall-client.yml
```

重要

クライアントをアンインストールすると、基本的な IdM 設定のみがホストから削除されますが、クライアントの再インストールを行うことになった場合に備え、ホストに設定ファイルが残されます。また、アンインストールには以下の制限があります。

- IdM LDAP サーバーからクライアントホストエントリーは削除されない。アンインストールすると、ホストの登録が解除されるだけである。
- クライアントにあるサービスは、IdM から削除されない。
- クライアントの DNS エントリーは、IdM サーバーから削除されない。
- **/etc/krb5.keytab** を除き、以前の Keytab のプリンシパルは削除されない。

アンインストールを行うと、IdM CA がホスト向けに発行した証明書がすべて削除されることに注意してください。

関連情報

- IdM クライアントのアンインストール

パート II. IDM および AD の統合

第34章 IDM と AD との間の信頼のインストール

Identity Management IdM サーバーと Active Directory (AD) の間の信頼を作成する方法について詳しく説明します。この場合、両方のサーバーは同じフォレスト内にあります。

注記

RHEL 7 では、**同期** と **信頼** は、RHEL システムを Active Directory (AD) へ間接的に統合する場合に考えられる 2 つの方法でした。RHEL 8 では、同期は非推奨になりました。IdM と AD を統合するには、代わりに信頼アプローチを使用します。同期から信頼に移行する場合は、Linux ドメインと Active Directory ドメインを統合する際の同期から信頼への既存環境の移行 を参照してください。

前提条件

- Planning a cross-forest trust between Identity Management and Active Directory を読んでいる。
- ドメインコントローラーとともに、AD がインストールされている。
- IdM サーバーがインストールされ、実行している。
  - 詳細は、Installing Identity Management を参照してください。
- Kerberos では、通信に最大 5 分の遅延が必要になるため、AD サーバーおよび IdM サーバーの両方でクロックが同期されている必要がある。
- NetBIOS 名は、Active Directory ドメインの特定に不可欠であるため、各サーバーで一意の NetBIOS 名を信頼に配置する。
  - Active Directory または IdM ドメインの NetBIOS 名は通常、対応する DNS ドメインの最初の部分になります。DNS ドメインが **ad.example.com** の場合、NetBIOS 名は通常 **AD** になります。ただし、必須ではありません。重要なのは、NetBIOS 名がピリオドなしの 1 つの単語であるということです。NetBIOS 名は最長 15 文字です。
- 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る。
  - 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。

34.1. サポート対象の WINDOWS SERVER バージョン

以下のフォレストおよびドメイン機能レベルを使用する Active Directory (AD) フォレストとの信頼関係を確立できます。

- フォレスト機能レベルの範囲 - Windows Server 2012 ~ Windows Server 2016
- ドメイン機能レベルの範囲: Windows Server 2012 - Windows Server 2016

Identity Management (IdM) は、以下のオペレーティングシステムを実行している Active Directory ドメインコントローラーとの信頼の確立に対応しています。

- Windows Server 2022 (RHEL 8.7 以降)
- Windows Server 2019
- Windows Server 2016

- Windows Server 2012 R2
- Windows Server 2012

重要

RHEL 8.4 では、Identity Management (IdM) は、Windows Server 2008 R2 以前のバージョンを実行している Active Directory ドメインコントローラーとの間で Active Directory への信頼を確立することに対応していません。RHEL IdM との信頼関係を確立する際に、SMB 暗号化が必要になりました。これは、Windows Server 2012 以降でのみ対応しています。

34.2. 信頼の仕組み

Identity Management (IdM) と Active Directory (AD) の間の信頼は、レルム間の Kerberos 信頼で確立されます。このソリューションでは、Kerberos 機能を使用して、異なる ID ソース間で信頼関係を確立します。したがって、すべての AD ユーザーは次のことができます。

- ログインして、Linux システムおよびリソースにアクセスする。
- シングルサインオン (SSO) を使用する。

IdM オブジェクトはすべて、信頼の IdM で管理されます。

AD オブジェクトはすべて、信頼の AD で管理されます。

複雑な環境では、1 つの IdM フォレストを、複数の AD フォレストに接続できます。この設定により、組織のさまざまな機能の作業を、より適切に分離できます。Linux 管理者は Linux インフラストラクチャーを完全に制御できますが、AD 管理者はユーザーと、ユーザーに関連するポリシーに集中できます。このような場合、IdM が制御する Linux レルムは、AD リソースドメインまたはレルムに似ていますが、Linux システムが含まれています。

AD の観点から観ると、Identity Management は、1 つの AD ドメインを持つ個別の AD フォレストを表します。AD フォレストの root ドメインと IdM ドメインとの間にフォレスト間の信頼が確立されると、AD フォレストドメインのユーザーは、IdM ドメインの Linux マシンおよびサービスと相互作用できます。

注記

信頼環境では、IdM は ID ビューを使用して、IdM サーバーの AD ユーザーの POSIX 属性を設定できます。

34.3. AD 管理者権限

AD (Active Directory) と IdM (Identity Management) との間で信頼を構築する場合は、適切な AD 権限のある AD 管理者アカウントを使用する必要があります。

このような AD 管理者は、以下のいずれかのグループのメンバーである必要があります。

- AD フォレスト内のエンタープライズ管理グループ
- AD フォレスト用のフォレストルートドメインのドメイン管理グループ

関連情報

- エンタープライズ管理の詳細は、Enterprise Admins を参照してください。
- ドメイン管理の詳細は、Domain Admins を参照してください。
- AD 信頼の詳細は、How Domain and Forest Trusts Work を参照してください。

34.4. AD および RHEL で一般的な暗号化タイプに対応

デフォルトでは、Identity Management は RC4、AES-128、および AES-256 の Kerberos 暗号化タイプに対応するレルム間の信頼を確立します。さらに、デフォルトでは、SSSD と Samba Winbind は RC4、AES-128、および AES-256 の Kerberos 暗号化タイプに対応します。

RC4 暗号化は、新しい暗号化タイプ AES-128 および AES-256 よりも安全ではないと見なされるため、デフォルトで非推奨となり、無効にされています。一方、Active Directory (AD) ユーザーの認証情報と AD ドメイン間の信頼は RC4 暗号化をサポートしており、すべての AES 暗号化タイプには対応していない可能性があります。

一般的な暗号化タイプがないと、RHEL ホストと AD ドメイン間の通信が機能しないか、一部の AD アカウントが認証できない可能性があります。この状況に対処するには、次のセクションで説明する設定のいずれかを実行します。

重要

IdM が FIPS モードの場合、IdM-AD 統合は機能しません。これは、AD は RC4 または AES HMAC-SHA1 暗号化の使用しかサポートしない一方で、FIPS モードの RHEL 9 は、デフォルトでは AES HMAC-SHA2 しか許可しないためです。RHEL 9 で AES HMAC-SHA1 の使用を有効にするには、**# update-crypto-policies --set FIPS:AD-SUPPORT** と入力してください。

IdM は、より制限の厳しい **FIPS:OSPP** 暗号化ポリシーはサポートしていません。このポリシーは、Common Criteria で評価されたシステムでしか使用できません。

34.4.1. AD での AES 暗号化の有効化 (推奨)

AD フォレストの Active Directory (AD) ドメイン間の信頼を確保して、強力な AES 暗号化の種類に対応するには、Microsoft の記事 AD DS: Security: Kerberos "Unsupported etype" error when accessing a resource in a trusted domain を参照してください。

34.4.2. GPO を使用した Active Directory で AES 暗号化タイプの有効化

本セクションでは、グループポリシーオブジェクト (GPO) を使用して、Active Directory (AD) で AES 暗号化タイプを有効にする方法を説明します。IdM クライアントで Samba サーバーを実行するなど、RHEL の特定の機能には、この暗号化タイプが必要です。

RHEL は、弱い DES および RC4 の暗号化タイプをサポートしなくなった点に注意してください。

前提条件

- グループポリシーを編集できるユーザーとして AD にログインしている。
- **Group Policy Management Console** がコンピューターにインストールされている。

手順

1. **Group Policy Management Console** を開きます。

2. **デフォルトドメインポリシー** を右クリックして、**編集** を選択します。**Group Policy Management Editor** を閉じます。

3. **コンピューターの設定 → ポリシー → Windows の設定 → セキュリティーの設定 → ローカルポリシー → セキュリティーオプション** に移動します。

4. **ネットワーク セキュリティー: Kerberos で許可する暗号化の種類を設定する** をダブルクリックします。

5. **AES256_HMAC_SHA1** を選択し、必要に応じて、**将来の暗号化タイプ** を選択します。

6. **OK** をクリックします。

7. **Group Policy Management Editor** を閉じます。

8. **デフォルトのドメインコントローラーポリシー** に対して手順を繰り返します。

9. Windows ドメインコントローラー (DC) がグループポリシーを自動的に適用するまで待ちます。または、GPO を DC に手動で適用するには、管理者権限を持つアカウントを使用して次のコマンドを入力します。

```
C:\> gpupdate /force /target:computer
```

34.4.3. RHEL での RC4 サポートの有効化

AD ドメインコントローラーに対する認証が行われるすべての RHEL ホストで、以下に概説する手順を実行します。

手順

1. **update-crypto-policies** コマンドを使用して、**DEFAULT** 暗号化ポリシーに加え **AD-SUPPORT** 暗号化サブポリシーを有効にします。

```
[root@host ~]# update-crypto-policies --set DEFAULT:AD-SUPPORT
Setting system policy to DEFAULT:AD-SUPPORT
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
```

2. ホストを再起動します。

重要

AD-SUPPORT 暗号化サブポリシーは、RHEL 8.3 以降でのみ利用できます。

- RHEL 8.2 以前は RC4 のサポートを有効にするには、**cipher = RC4-128+** でカスタム暗号化モジュールポリシーを作成および有効にします。詳細は、サブポリシーを使用したシステム全体の暗号化ポリシーのカスタマイズ を参照してください。
- RHEL 8.0 および RHEL 8.1 で RC4 のサポートを有効にするには、**/etc/crypto-policies/back-ends/krb5.config** ファイルの **permitted_enctypes** オプションに **+rc4** を追加します。

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac +rc4
```

34.4.4. 関連情報

- Using system-wide cryptographic policies を参照してください。
- 信頼コントローラーおよび信頼エージェント を参照してください。

34.5. IDM と AD との間の通信に必要なポート

Active Directory (AD) 環境と Identity Management (IdM) 環境間の通信を有効にするには、AD ドメインコントローラーおよび IdM サーバーのファイアウォールで次のポートを開きます。

表34.1 AD 信頼に必要なポート

サービス	ポート	プロトコル
エンドポイント解決ポートマッパー	135	TCP
NetBIOS-DGM	138	TCP および UDP
NetBIOS-SSN	139	TCP および UDP
Microsoft-DS	445	TCP および UDP
動的 RPC	49152-65535	TCP
AD グローバルカタログ	3268	TCP
LDAP	389	TCP および UDP

注記

信頼のために IdM サーバーで TCP ポートの 389 を開く必要はありませんが、IdM サーバーと通信しているクライアントに必要です。

TCP ポート 135 は、DCE RPC エンドポイントマッパーが機能するために必要であり、IdM-AD 信頼の作成中に使用されます。

ポートを開くには、以下の方法を使用できます。

- **firewalld** サービス - 特定ポートを有効にするか、そのポートが含まれる以下のサービスを有効にすることができます。
  - freeipa 信頼の設定
  - LDAP を用いた FreeIPA
  - Kerberos
  - DNS

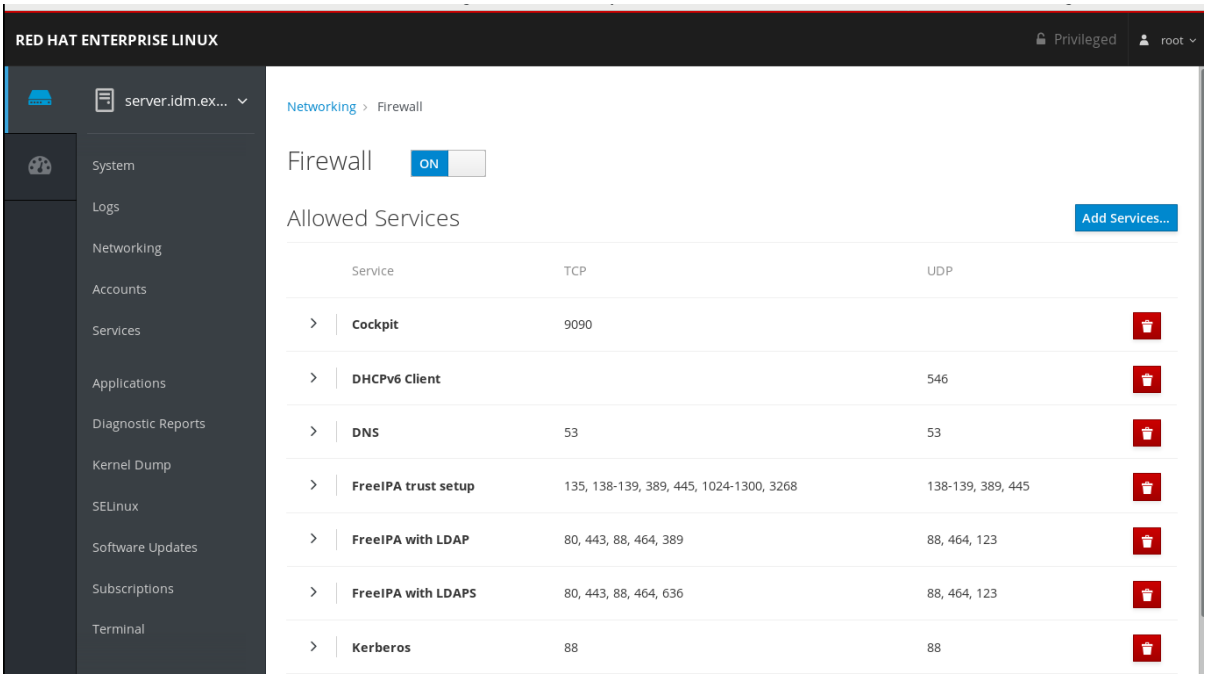
  詳細は、**firewall-cmd** の man ページを参照してください。

注記

RHEL 8.2 以前を使用している場合、**freeipa-trust** firewalld サービスには **1024-1300** の RPC ポート範囲が含まれていますが、これは正しくありません。RHEL 8.2 以前では、**freeipa-trust** firewalld サービスを有効にすることに加えて、TCP ポート範囲 **49152-65535** を手動で開く必要があります。

この問題は、RHEL8.3 以降の バグ 1850418 - freeipa-trust.xml 定義を更新して正しい動的 RPC 範囲を含める で修正されています。

- RHEL Web コンソール。**firewalld** サービスに基づくファイアウォール設定を含む UI です。



Web コンソールを使用したファイアウォール設定の詳細は、Web コンソールを使用したファイアウォールでのサービスの有効化 を参照してください。

注記

RHEL 8.2 以前を使用している場合、**FreeIPA Trust Setup** サービスには **1024-1300** の RPC ポート範囲が含まれていますが、これは正しくありません。RHEL 8.2 以前では、RHEL Web コンソールで **FreeIPA Trust Setup** サービスを有効にすることに加えて、TCP ポート範囲 **49152-65535** を手動で開く必要があります。

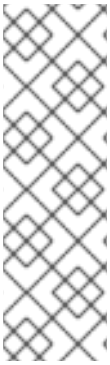
この問題は、RHEL8.3 以降の バグ 1850418 - freeipa-trust.xml 定義を更新して正しい動的 RPC 範囲を含める で修正されています。

表34.2 信頼の IdM サーバーで必要なポート

サービス	ポート	プロトコル
Kerberos	88、464	TCP および UDP
LDAP	389	TCP
DNS	53	TCP および UDP

表34.3 AD 信頼で IdM クライアントに必要なポート

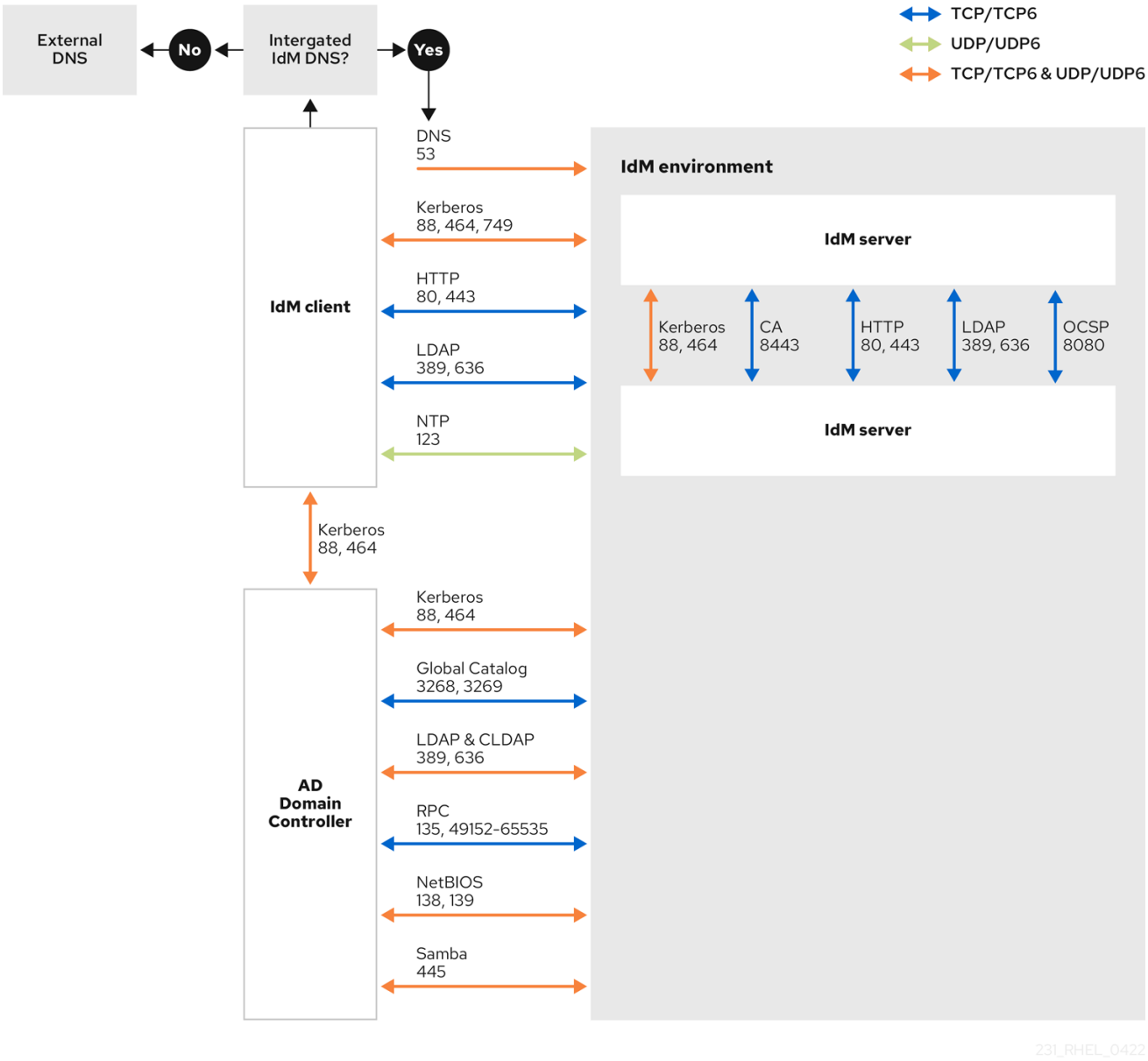
サービス	ポート	プロトコル
Kerberos	88	UDP および TCP



注記

libkrb5 ライブラリーは UDP を使用し、KDC (Key Distribution Center) から送信されるデータが大きすぎると、TCP プロトコルにフォールバックします。Active Directory は、PAC (Privilege Attribute Certificate) を Kerberos チケットに割り当てます。これによりサイズが増加し、TCP プロトコルを使用する必要があります。要求のフォールバックと再送信を回避するため、デフォルトでは、Red Hat Enterprise Linux 7.4 以降の SSSD ではユーザー認証に TCP が使用されます。**libkrb5** が TCP を使用する前にサイズを設定する場合は、**/etc/krb5.conf** ファイルに **udp_preference_limit** を設定します。詳細は、man ページの **krb5.conf(5)** を参照してください。

以下の図は、IdM クライアントによって送信され、IdM サーバーと AD ドメインコントローラーによって受信および応答された通信を示しています。ファイアウォールで受信および送信ポートとプロトコルを設定するには、Red Hat は、FreeIPA サービスの定義がすでにある **firewalld** サービスを使用することを推奨しています。



関連情報

- Windows Server 2008 以降の Dynamic RPC ポート範囲の詳細は、The default dynamic port range for TCP/IP has changed since Windows Vista and in Windows Server 2008 を参照してください。

34.6. 信頼用の DNS およびレルムの設定の設定

信頼で Identity Management (IdM) と Active Directory (AD) を接続する前に、サーバーが相互に認識し、ドメイン名を正しく解決できるようにする必要があります。次の間でドメイン名を使用できるように DNS を設定するには:

- 統合 DNS サーバーおよび認証局を使用する 1 台のプライマリー IdM サーバー
- 1 台の AD ドメインコントローラー

DNS 設定には以下が必要です。

- IdM サーバーに DNS ゾーンの設定

- AD での条件付き DNS 転送の設定
- DNS 設定の正確性の確認

34.6.1. 一意のプライマリー DNS ドメイン

Windows では、すべてのドメインが Kerberos レルムと DNS ドメインを同時に設定します。ドメインコントローラーが管理するすべてのドメインには、独自の専用 DNS ゾーンが必要です。Identity Management (IdM) がフォレストとして Active Directory (AD) に信頼される場合も同様です。AD は、IdM に独自の DNS ドメインがあることを想定します。信頼の設定を機能させるには、DNS ドメインを Linux 環境専用にする必要があります。

各システムには、独自の固有プライマリー DNS ドメインが設定されている必要があります。以下に例を示します。

- **ad.example.com** (AD の場合) および **idm.example.com** (IdM の場合)
- **example.com** (AD の場合) および **idm.example.com** (IdM の場合)
- **ad.example.com** (AD の場合) および **example.com** (IdM の場合)

最も便利な管理ソリューションは、各 DNS ドメインが統合 DNS サーバーで管理されている環境ですが、規格に準拠した DNS サーバーも使用できます。

Kerberos レルム名は、プライマリー DNS ドメイン名を大文字にしたもの

Kerberos レルム名は、プライマリー DNS ドメイン名と同じで、すべて大文字にする必要があります。たとえば、AD のドメイン名が **ad.example.com** で、IdM のドメイン名が **idm.example.com** の場合、Kerberos レルム名は **AD.EXAMPLE.COM** および **IDM.EXAMPLE.COM** になります。

DNS レコードが信頼内の全 DNS ドメインから解決可能である

すべてのマシンが、信頼関係内で関連するすべての DNS ドメインの DNS レコードを解決できるようにする必要があります。

IdM ドメインおよび AD DNS ドメイン

IdM に参加しているシステムは、複数の DNS ドメインに分散できます。Red Hat では、Active Directory が所有するクライアントとは異なる DNS ゾーンに IdM クライアントをデプロイすることを推奨しています。プライマリー IdM DNS ドメインには、AD 信頼に対応するのに適切な SRV レコードが必要です。

注記

IdM と Active Directory との間の信頼がある一部の環境では、Active Directory DNS ドメインの一部であるホストに IdM クライアントをインストールできます。ホストは、これにより、Linux に焦点を合わせた IdM の機能の恩恵を受けることができます。これは推奨される設定ではなく、いくつかの制限があります。詳細は Active Directory DNS ドメインで IdM クライアントの設定 を参照してください。

次のコマンドを実行して、システム設定に必要な固有の SRV レコードのリストを取得できます。

```
$ ipa dns-update-system-records --dry-run
```

生成されるリストは、たとえば以下のようになります。

```
IPA DNS records:
  _kerberos-master._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
```

```
_kerberos-master._udp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos._tcp.idm.example.com. 86400 IN SRV 0 100 88 server.idm.example.com.
_kerberos.idm.example.com. 86400 IN TXT "IDM.EXAMPLE.COM"
_kpasswd._tcp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_kpasswd._udp.idm.example.com. 86400 IN SRV 0 100 464 server.idm.example.com.
_ldap._tcp.idm.example.com. 86400 IN SRV 0 100 389 server.idm.example.com.
_ipa-ca.idm.example.com. 86400 IN A 192.168.122.2
```

同じ IdM レルムにあるその他の DNS ドメインでは、AD への信頼を設定する際に SRV レコードを設定する必要はありません。これは、AD ドメインコントローラーが、KDC の検索に SRV レコードではなく、信頼の名前接尾辞のルーティング情報を使用するためです。

34.6.2. IdM Web UI での DNS 正引きゾーンの設定

IdM Web UI を使用して Identity Management (IdM) サーバーに DNS 転送ゾーンを追加するには、次の手順に従います。

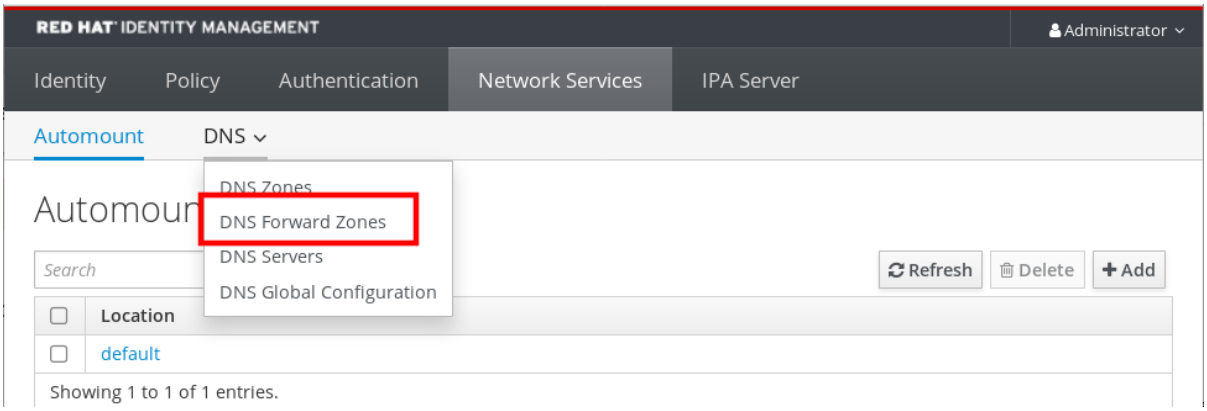
DNS 正引きゾーンを使用すると、特定のゾーンの DNS クエリーを別の DNS サーバーに転送できます。たとえば、Active Directory (AD) ドメインの DNS クエリーを AD DNS サーバーに転送することができます。

前提条件

- 管理者権限のあるユーザーアカウントを使用して IdM Web UI にアクセスする。
- DNS サーバーを正しく設定している。

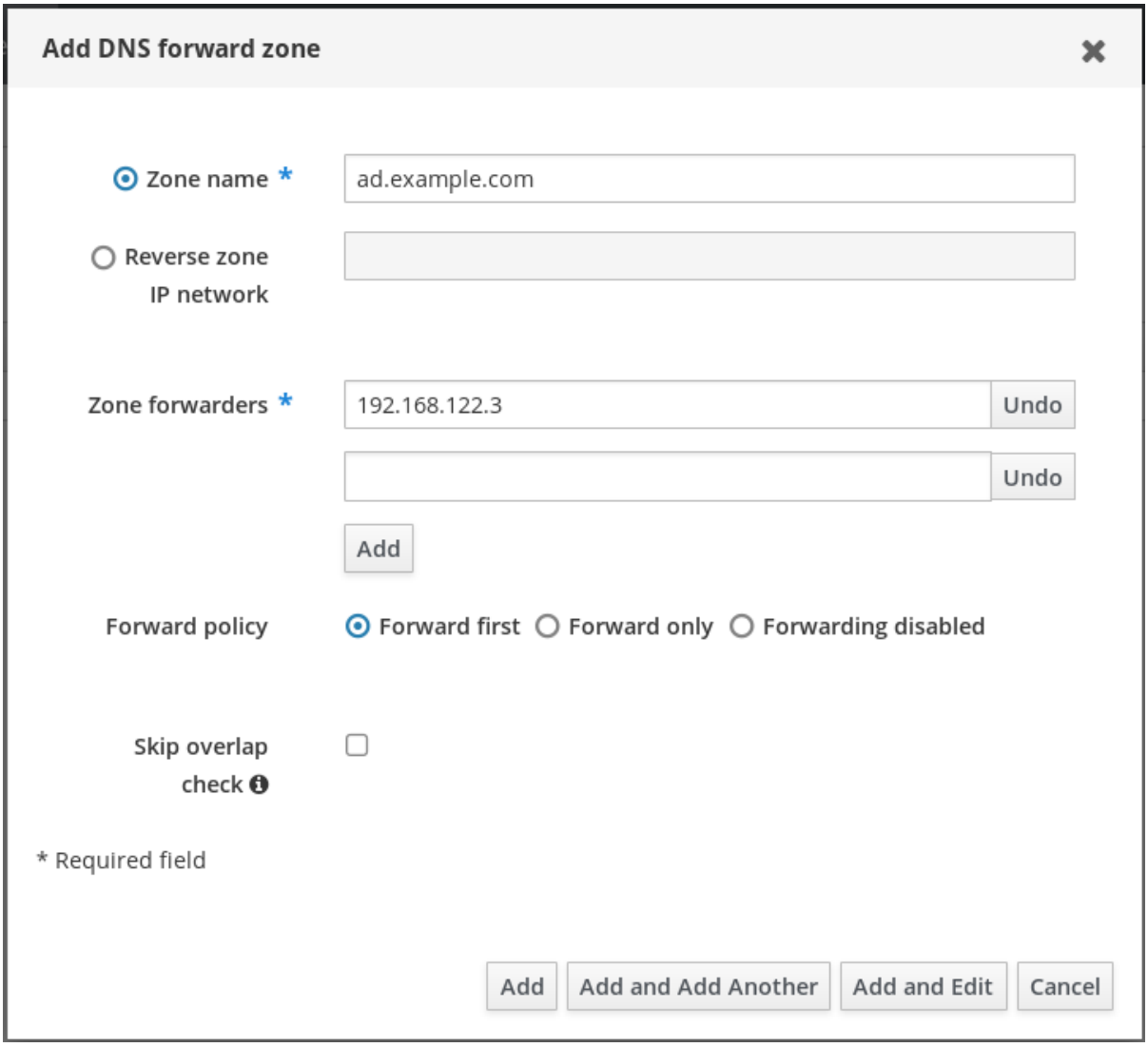
手順

1. 管理者権限で IdM Web UI にログインします。詳細は Web ブラウザーで IdM Web UI へのアクセス を参照してください。
2. **Network Services** タブをクリックします。
3. **DNS** タブをクリックします。
4. ドロップダウンメニューで、**DNS Forward Zones** 項目をクリックします。



5. **Add** ボタンをクリックします。
6. **Add DNS forward zone** ダイアログボックスにゾーン名を追加します。
7. **Zone forwarders** 項目で、**Add** ボタンをクリックします。

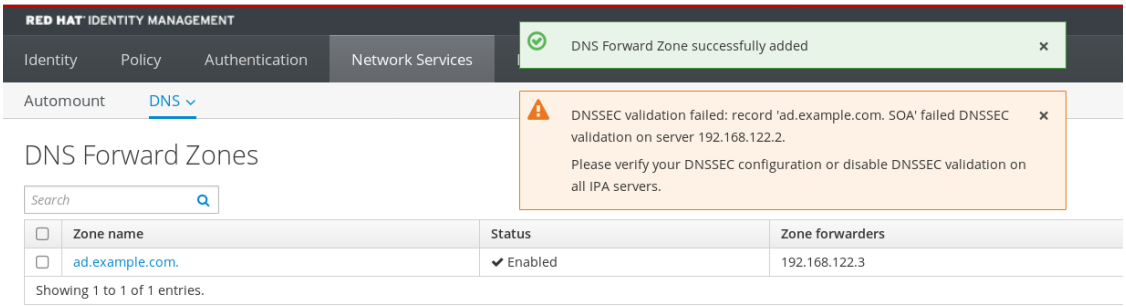
8. **Zone forwarders** フィールドに正引きゾーンを作成するサーバーの IP アドレスを追加します。
9. **Add** ボタンをクリックします。



正引きゾーンが DNS 設定に追加されており、DNS 正引きゾーン設定で確認できます。Web UI は、ポップアップメッセージ **DNS Forward Zone successfully added.** で、成功を通知します。

注記

設定に正引きゾーンを追加した後に、Web UI に DNSSEC 検証の失敗に関する警告が表示される場合があります。



DNSSEC (Domain Name System Security Extensions) は、DNS データをデジタル署名で保護し、攻撃から DNS を保護します。このサービスは、IdM サーバーでデフォルトで有効になっています。リモート DNS サーバーが DNSSEC を使用していないため、警告が表示されます。Red Hat は、リモート DNS サーバーで DNSSEC を有効にすることを推奨します。

リモートサーバーで DNSSEC 検証を有効にできない場合は、IdM サーバーで DNSSEC を無効にすることができます。

1. 編集する適切な設定ファイルを選択します。
   - IdM サーバーが RHEL 8.0 または RHEL 8.1 を使用している場合は、**/etc/named.conf** ファイルを開きます。
   - IdM サーバーが RHEL 8.2 以降を使用している場合は、**/etc/named/ipa-options-ext.conf** ファイルを開きます。
2. 以下の DNSSEC パラメーターを追加します。

```
dnssec-enable no;
dnssec-validation no;
```

3. 設定ファイルを保存して閉じます。
4. DNS サービスを再起動します。

```
# systemctl restart named-pkcs11
```

検証手順

- **nslookup** コマンドを、リモート DNS サーバーの名前で使用します。

```
$ nslookup ad.example.com
Server:         192.168.122.2
Address:        192.168.122.2#53

No-authoritative answer:
Name:           ad.example.com
Address:        192.168.122.3
```

ドメイン転送を正しく設定すると、リモート DNS サーバーの IP アドレスが表示されます。

34.6.3. CLI での DNS 正引きゾーンの設定

コマンドラインインターフェイス (CLI) を使用して、新しい DNS 転送ゾーンを Identity Management (IdM) サーバーに追加するには、次の手順に従います。

DNS 正引きゾーンを使用すると、特定のゾーンの DNS クエリーを別の DNS サーバーに転送できます。たとえば、Active Directory (AD) ドメインの DNS クエリーを AD DNS サーバーに転送することができます。

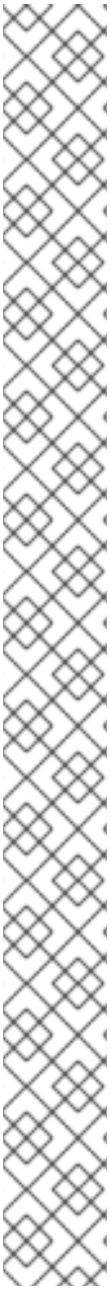
前提条件

- 管理者権限のあるユーザーアカウントを使用して CLI にアクセスする。
- DNS サーバーを正しく設定している。

手順

- AD ドメインの DNS 正引きゾーンを作成し、**--forwarder** オプションを使用してリモート DNS サーバーの IP アドレスを指定します。

```
# ipa dnsforwardzone-add ad.example.com --forwarder=192.168.122.3 --forward-policy=first
```



注記

設定に新しい正引きゾーンを追加した後に、**/var/log/messages** システムログに DNSSEC 検証の失敗に関する警告が表示される場合があります。

```
named-pkcs11[2572]: no valid DS resolving 'host.ad.example.com/A/IN':
192.168.100.25#53
```

DNSSEC (Domain Name System Security Extensions) は、DNS データをデジタル署名で保護し、攻撃から DNS を保護します。このサービスは、IdM サーバーでデフォルトで有効になっています。リモート DNS サーバーが DNSSEC を使用していないため、警告が表示されます。Red Hat は、リモート DNS サーバーで DNSSEC を有効にすることを推奨します。

リモートサーバーで DNSSEC 検証を有効にできない場合は、IdM サーバーで DNSSEC を無効にすることができます。

1. 編集する適切な設定ファイルを選択します。
   - IdM サーバーが RHEL 8.0 または RHEL 8.1 を使用している場合は、**/etc/named.conf** ファイルを開きます。
   - IdM サーバーが RHEL 8.2 以降を使用している場合は、**/etc/named/ipa-options-ext.conf** ファイルを開きます。
2. 以下の DNSSEC パラメーターを追加します。

   ```
   dnssec-enable no;
   dnssec-validation no;
   ```

3. 設定ファイルを保存して閉じます。
4. DNS サービスを再起動します。

   ```
   # systemctl restart named-pkcs11
   ```

検証手順

- **nslookup** コマンドを、リモート DNS サーバーの名前で使用します。

  ```
  $ nslookup ad.example.com
  Server:        192.168.122.2
  Address:       192.168.122.2#53

  No-authoritative answer:
  Name:          ad.example.com
  Address:       192.168.122.3
  ```

  ドメイン転送が正しく設定されている場合、**nslookup** 要求はリモート DNS サーバーの IP アドレスを表示します。

34.6.4. AD での DNS 転送の設定

Active Directory (AD) で Identity Management (IdM) サーバーの DNS 転送を設定するには、次の手順に従います。

前提条件

- AD を使用する Windows Server がインストールされている。
- 両方のサーバーで DNS ポートが開いている。

手順

1. Windows サーバーにログインします。
2. **Server Manager** を開きます。
3. **DNS Manager** を開きます。
4. **Conditional Forwarders** で、以下を含む新しい条件フォワーダーを追加します。
   - IdM サーバーの IP アドレス
   - **server.idm.example.com** などの完全修飾ドメイン名
5. 設定を保存します。

34.6.5. DNS 設定の確認

信頼を設定する前に、Identity Management (IdM) サーバーおよび Active Directory (AD) サーバーが自身を解決でき、相互に解決できることを確認します。

前提条件

- sudo パーミッションでログインする必要があります。

手順

1. UDP サービスレコードの Kerberos、および TCP サービスレコード上の LDAP に、DNS クエリーを実行します。

```
[admin@server ~]# dig +short -t SRV _kerberos._udp.idm.example.com.
0 100 88 server.idm.example.com.

[admin@server ~]# dig +short -t SRV _ldap._tcp.idm.example.com.
0 100 389 server.idm.example.com.
```

   コマンドは、すべての IdM サーバーをリストで表示する必要があります。

2. IdM Kerberos レルム名を使用して、TXT レコードに DNS クエリーを実行します。取得した値は、IdM のインストール時に指定した Kerberos レルムと一致することが予想されます。

```
[admin@server ~]# dig +short -t TXT _kerberos.idm.example.com.
"IDM.EXAMPLE.COM"
```

   前の手順で想定されるレコードがすべて返されなかった場合は、欠落しているレコードで DNS 設定を更新します。

   - IdM 環境で統合 DNS サーバーを使用する場合は、システムレコードを更新するオプションを指定せずに **ipa dns-update-system-records** コマンドを実行します。

```
[admin@server ~]$ ipa dns-update-system-records
```

- IdM 環境で統合 DNS サーバーを使用しない場合は、以下を行います。

  1. IdM サーバーで、IdM DNS レコードをファイルにエクスポートします。

     ```
     [admin@server ~]$ ipa dns-update-system-records --dry-run --out
     dns_records_file.nsupdate
     ```

     このコマンドは、関連する IdM DNS レコードで **dns_records_file.nsupdate** という名前のファイルを作成します。

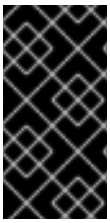
  2. **nsupdate** ユーティリティーおよび **dns_records_file.nsupdate** ファイルを使用して DNS サーバーに DNS 更新リクエストを送信します。詳細は、RHEL 7 ドキュメントの nsupdate を使用した外部 DNS レコード更新 を参照してください。または、DNS レコードの追加については、お使いの DNS サーバーのドキュメントを参照してください。

3. IdM が、TCP サービスレコードで Kerberos および LDAP の DNS クエリーを実行するコマンドを使用して、AD のサービスレコードを解決できることを確認します。

```
[admin@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[admin@server ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

34.7. ACTIVE DIRECTORY DNS ドメインで IDM クライアントの設定

Active Directory が制御する DNS ドメインにクライアントシステムがあり、そのクライアントが RHEL 機能の恩恵を受けるために IdM Server に参加できるようにする必要がある場合は、Active Directory DNS ドメインのホスト名を使用してクライアントにアクセスするようにユーザーを設定できます。



重要

これは推奨される設定ではなく、いくつかの制限があります。Red Hat は、Active Directory が所有する DNS ゾーンとは異なる DNS ゾーンに常に IdM クライアントをデプロイメントし、IdM ホスト名を介して IdM クライアントにアクセスすることを推奨します。

IdM クライアントの設定は、Kerberos でシングルサインオンを必要とするかどうかによって異なります。

34.7.1. Kerberos シングルサインオンを使用しない IdM クライアントの設定

パスワード認証は、IdM クライアントが Active Directory DNS ドメインに存在する場合に、IdM クライアントのリソースにアクセスするためにユーザーが利用できる唯一の認証方法です。Kerberos Single Sign-On を使用せずにクライアントを設定するには、次の手順に従います。

手順

1. **--domain=IPA_DNS_Domain** を指定して IdM クライアントをインストールし、SSSD (System Security Services Daemon) が IdM サーバーと通信できるようにします。

```
[root@idm-client.ad.example.com ~]# ipa-client-install --domain=idm.example.com
```

このオプションは、Active Directory DNS ドメインの SRV レコードの自動検出を無効にします。

2. **/etc/krb5.conf** 設定ファイルの **[domain_realm]** セクションで、Active Directory ドメインの既存のマッピングを見つけます。

```
.ad.example.com = IDM.EXAMPLE.COM
ad.example.com = IDM.EXAMPLE.COM
```

3. 両方の行を、Active Directory DNS ゾーンの Linux クライアントの完全修飾ドメイン名 (FQDN) を IdM レルムにマッピングするエントリーに置き換えます。

```
idm-client.ad.example.com = IDM.EXAMPLE.COM
```

デフォルトのマッピングを置き換えても、Kerberos が Active Directory ドメインの要求を IdM Kerberos Distribution Center (KDC) に送信しないようにします。Kerberos は、SRV DNS レコードを介して自動検出を使用して KDC を見つけます。

34.7.2. シングルサインオンなしで SSL 証明書の要求

SSL ベースのサービスでは、元 (A/AAAA) のレコードと CNAME レコードの両方が証明書に含まれている必要があるため、すべてのシステムホスト名に対応する **dNSName** 拡張レコードを持つ証明書が必要です。現在、IdM は、IdM データベース内のオブジェクトをホストする証明書のみを発行します。

シングルサインオンが利用できない説明されたセットアップでは、IdM は、データベースに FQDN のホストオブジェクトをすでに持っており、**certmonger** はこの名前を使用して証明書を要求できます。

前提条件

- Kerberos シングルサインオンを使用しない IdM クライアントの設定 での手順に従って、IdM クライアントをインストールし、設定します。

手順

- **certmonger** を使用して、FQDN を使用して証明書をリクエストします。

```
[root@idm-client.ad.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=ipa-client.ad.example.com \
    -D ipa-client.ad.example.com \
    -K host/idm-client.ad.example.com@IDM.EXAMPLE.COM \
    -U id-kp-serverAuth
```

certmonger サービスは、**/etc/krb5.keytab** ファイルに保存されているデフォルトのホストキーを使用して、IdM 認証局 (CA) に対して認証を行います。

34.7.3. Kerberos シングルサインオンで IdM クライアントの設定

IdM クライアントのリソースにアクセスするために Kerberos シングルサインオンが必要な場合、クライアントは **idm-client.idm.example.com** などの IdM DNS ドメイン内になければなりません。IdM クライアントの A/AAAA レコードを参照する Active Directory DNS ドメインで CNAME レコード **idm-**

client.ad.example.com を作成する必要があります。

Kerberos ベースのアプリケーションサーバーの場合、MIT Kerberos は、アプリケーションのキータブで利用可能なホストベースのプリンシパルの受け入れを可能にする方法をサポートします。

手順

- IdM クライアントでは、**/etc/krb5.conf** 設定ファイルの **[libdefaults]** セクションにある次のオプションを設定して、Kerberos サーバーのターゲットに使用される Kerberos プリンシパルに関する厳格なチェックを無効にします。

```
ignore_acceptor_hostname = true
```

34.7.4. シングルサインオンで SSL 証明書の要求

SSL ベースのサービスでは、元 (A/AAAA) のレコードと CNAME レコードの両方が証明書に含まれている必要があるため、すべてのシステムホスト名に対応する **dNSName** 拡張レコードを持つ証明書が必要です。現在、IdM は、IdM データベース内のオブジェクトをホストする証明書のみを発行します。

この手順に従って、IdM で **ipa-client.example.com** のホストオブジェクトを作成し、実際の IdM マシンのホストオブジェクトがこのホストを管理できることを確認します。

前提条件

- Kerberos シングルサインオンで IdM クライアントの設定 で説明されているように、Kerberos サーバーのターゲットに使用される Kerberos プリンシパルに関する厳格なチェックを無効にしています。

手順

1. IdM サーバーに新しいホストオブジェクトを作成します。

```
[root@idm-server.idm.example.com ~]# ipa host-add idm-client.ad.example.com --force
```

ホスト名は CNAME であり、A/AAAA レコードではないため、**--force** オプションを使用します。

2. IdM サーバーで、IdM DNS ホスト名が、IdM データベースの Active Directory ホストエントリーを管理できるようにします。

```
[root@idm-server.idm.example.com ~]# ipa host-add-managedby idm-client.ad.example.com
\
    --hosts=idm-client.idm.example.com
```

3. これで、Active Directory DNS ドメイン内のホスト名に **dNSName** 拡張レコードを使用して、IdM クライアントの SSL 証明書を要求できるようになります。

```
[root@idm-client.idm.example.com ~]# ipa-getcert request -r \
    -f /etc/httpd/alias/server.crt \
    -k /etc/httpd/alias/server.key \
    -N CN=`hostname --fqdn` \
    -D `hostname --fqdn` \
```

```
-D idm-client.ad.example.com \
-K host/idm-client.idm.example.com@IDM.EXAMPLE.COM \
-U id-kp-serverAuth
```

34.8. 信頼の設定

本セクションでは、コマンドラインを使用して、IdM に Identity Management (IdM)/Active Directory (AD) 信頼を設定する方法を説明します。

前提条件

- DNS が正しく設定されている。IdM サーバーおよび AD サーバーはどちらも、相手の名前を解決できる。詳細は 信頼用の DNS およびレルム設定の設定 を参照してください。
- 対応しているバージョンの AD および IdM がデプロイされている。詳細は サポート対象の Windows Server バージョン を参照してください。
- Kerberos チケットを取得している。詳細は、Using kinit to log in to IdM manually を参照してください。

34.8.1. 信頼用の IdM サーバーの準備

AD との信頼を確立する前に、IdM サーバーで **ipa-adtrust-install** ユーティリティーを使用して IdM ドメインを準備する必要があります。

注記

ipa-adtrust-install コマンドを自動的に実行するシステムは、AD 信頼コントローラーになります。ただし、**ipa-adtrust-install** は、IdM サーバーで 1 回のみ実行する必要があります。

前提条件

- IdM サーバーがインストールされている。
- パッケージをインストールし、IdM サービスを再起動するには、root 権限が必要です。

手順

1. 必要なパッケージをインストールします。

```
[root@ipaserver ~]# yum install ipa-server-trust-ad samba-client
```

2. IdM 管理ユーザーとして認証します。

```
[root@ipaserver ~]# kinit admin
```

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

```
[root@ipaserver ~]# ipa-adtrust-install
```

統合 DNS サーバーとともに IdM がインストールされていると、DNS サービスレコードが自動的に作成されます。

IdM が統合 DNS サーバーなしで IdM をインストールすると、**ipa-adtrust-install** は、続行する前に DNS に手動で追加する必要があるサービスレコードのリストを出力します。

4. スクリプトにより、**/etc/samba/smb.conf** がすでに存在し、書き換えられることが求められます。

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your existing
Samba configuration.

Do you wish to continue? [no]: yes
```

5. このスクリプトは、従来の Linux クライアントが信頼できるユーザーと連携できるようにする互換性プラグインである **slapi-nis** プラグインを設定するように求めるプロンプトを表示します。

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
This will allow clients older than SSSD 1.9 and non-Linux clients to work with trusted users.

Enable trusted domains support in slapi-nis? [no]: yes
```

6. プロンプトが表示されたら、IdM ドメインの NetBIOS 名を入力するか、**Enter** を押して提案された名前を使用します。

```
Trust is configured but no NetBIOS domain name found, setting it now.
Enter the NetBIOS name for the IPA domain.
Only up to 15 uppercase ASCII letters, digits and dashes are allowed.
Example: EXAMPLE.

NetBIOS domain name [IDM]:
```

7. SID 生成タスクを実行して、既存ユーザーに SID を作成するように求められます。

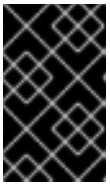
```
Do you want to run the ipa-sidgen task? [no]: yes
```

これはリソースを集中的に使用するタスクであるため、ユーザー数が多い場合は別のタイミングで実行できます。

8. **(必要に応じて)** デフォルトでは、Windows Server 2008 以降での動的 RPC ポートの範囲は **49152-65535** として定義されます。ご使用の環境に異なる動的 RPC ポート範囲を定義する必要がある場合は、Samba が異なるポートを使用するように設定し、ファイアウォール設定でそのポートを開くように設定します。以下の例では、ポート範囲を **55000-65000** に設定します。

```
[root@ipaserver ~]# net conf setparm global 'rpc server dynamic port range' 55000-65000
[root@ipaserver ~]# firewall-cmd --add-port=55000-65000/tcp
[root@ipaserver ~]# firewall-cmd --runtime-to-permanent
```

9. 信頼の DNS 設定の確認 に従って、DNS が適切に設定されていることを確認します。



重要

Red Hat では、IdM または AD が統合 DNS サーバーを使用しない場合に、**ipa-adtrust-install** を実行してから 信頼に対する DNS 設定の確認 に従って DNS 設定を検証することが強く推奨されます。

10. **ipa** サービスを再起動します。

```
[root@ipaserver ~]# ipactl restart
```

11. **smbclient** ユーティリティーを使用して、Samba が IdM からの Kerberos 認証に応答することを確認します。

```
[root@ipaserver ~]# smbclient -L ipaserver.idm.example.com -U user_name --use-kerberos=required
lp_load_ex: changing to config backend registry
    Sharename       Type      Comment
    ---------       ----      -------
    IPC$            IPC       IPC Service (Samba 4.15.2)
...
```

34.8.2. コマンドラインで信頼関係の設定

コマンドラインを使用して信頼関係を設定するには、次の手順に従います。Identity Management (IdM) サーバーには、3 種類の信頼関係を設定できます。

- **一方向の信頼** – デフォルトのオプション。一方向の信頼により、Active Directory (AD) ユーザーおよびグループは IdM のリソースにアクセスできますが、その逆はできません。IdM ドメインは AD フォレストを信頼しますが、AD フォレストは IdM ドメインを信頼しません。

- **双方向の信頼** – 双方向の信頼により、AD ユーザーおよびグループが IdM のリソースにアクセスできるようになります。
  信頼境界を使用して Kerberos プロトコルに **S4U2Self** および **S4U2Proxy** の Microsoft 拡張を必要とする、Microsoft SQL Server などのソリューションに、双方向の信頼を設定する必要があります。RHEL IdM ホスト上にあるアプリケーションは、AD ユーザーに関する **S4U2Self** または **S4U2Proxy** の情報を Active Directory ドメインコントローラーから要求する場合があり、双方向の信頼でこの機能が提供されます。

  この双方向の信頼機能では、IdM ユーザーは Windows システムにログインできないだけでなく、IdM の双方向信頼では、AD の一方向信頼ソリューションと比較して、権限が追加でユーザーに付与されるわけではありません。

  - 双方向の信頼を作成するには、コマンドに **--two-way=true** オプションを追加します。

- **外部信頼**: 異なるフォレストの IdM と AD ドメインとの間の信頼関係です。フォレストの信頼では常に IdM と Active Directory フォレストのルートドメインとの間で信頼関係を確立する必要がありますが、IdM からフォレスト内の任意のドメインへの外部の信頼関係も確立できます。管理上または組織上の理由で、フォレストの root ドメイン間でフォレストの信頼を確立できない場合に限り、これが推奨されます。

  - 外部の信頼を作成するには、コマンドに **--external=true** オプションを追加します。

以下の手順では、一方向の信頼関係を作成する方法を示します。

前提条件

- Windows 管理者のユーザー名およびパスワード
- 信頼用の IdM サーバーの準備ができている。

手順

- **ipa trust-add** コマンドを使用して、AD ドメインと IdM ドメインに信頼関係を作成します。
  - SSSD が SID に基づいて AD ユーザーの UID および GID を自動的に生成できるようにするには、**Active Directory domain** ID 範囲タイプとの信頼関係を作成します。これが最も一般的な設定です。

```
[root@server ~]# ipa trust-add --type=ad ad.example.com --admin
<ad_admin_username> --password --range-type=ipa-ad-trust
```

  - Active Directory でユーザーに POSIX 属性を設定し (**uidNumber**、**gidNumber**など)、SSSD でこの情報を処理する場合は、**Active Directory domain with POSIX attributes** ID 範囲タイプとの信頼関係を作成します。

```
[root@server ~]# ipa trust-add --type=ad ad.example.com --admin
<ad_admin_username> --password --range-type=ipa-ad-trust-posix
```

警告

信頼の作成時に ID 範囲タイプを指定しないと、IdM はフォレストルートドメインの AD ドメインコントローラーから詳細を要求することで、適切な範囲タイプを自動的に選択しようとします。IdM が POSIX 属性を検出しない場合、信頼インストールスクリプトは **Active Directory domain** ID 範囲を選択します。

IdM がフォレストルートドメインの POSIX 属性を検出すると、信頼インストールスクリプトは、**Active Directory domain with POSIX attributes** ID 範囲を選択し、UID および GID が AD に正しく定義されていることを前提とします。POSIX 属性が AD で正しく設定されていない場合は、AD ユーザーを解決できません。

たとえば、IdM システムへのアクセスを必要とするユーザーおよびグループがフォレストルートドメインの一部ではなく、フォレストドメインの子ドメインにある場合は、インストールスクリプトで、子 AD ドメインで定義された POSIX 属性が検出されない場合があります。この場合、Red Hat は、信頼の確立時に POSIX ID 範囲タイプを明示的に選択することを推奨します。

34.8.3. IdM Web UI で信頼関係の設定

IdM Web UI を使用して IdM 側で Identity Management (IdM)/Active Directory (AD) 信頼関係を設定するには、次の手順に従います。

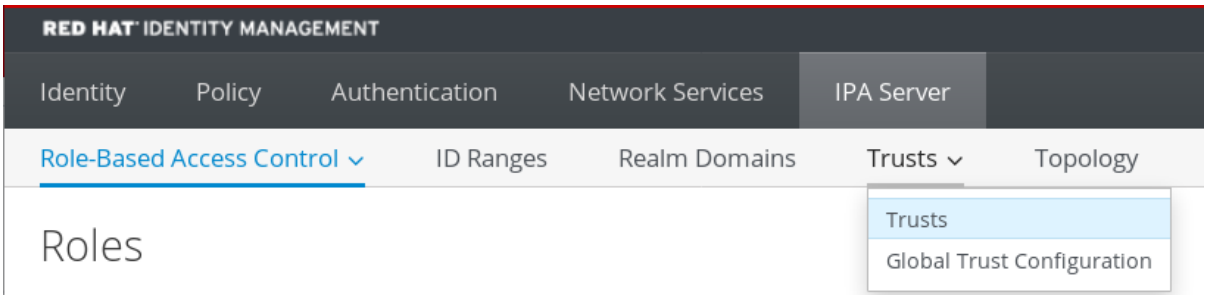
前提条件

- DNS が正しく設定されている。IdM サーバーおよび AD サーバーはどちらも、相手の名前を解決できる。
- 対応しているバージョンの AD および IdM がデプロイされている。
- Kerberos チケットを取得している。
- Web UI で信頼を作成する前に、信頼用の IdM サーバーの準備 に従って、信頼用に IdM サーバーを準備している。

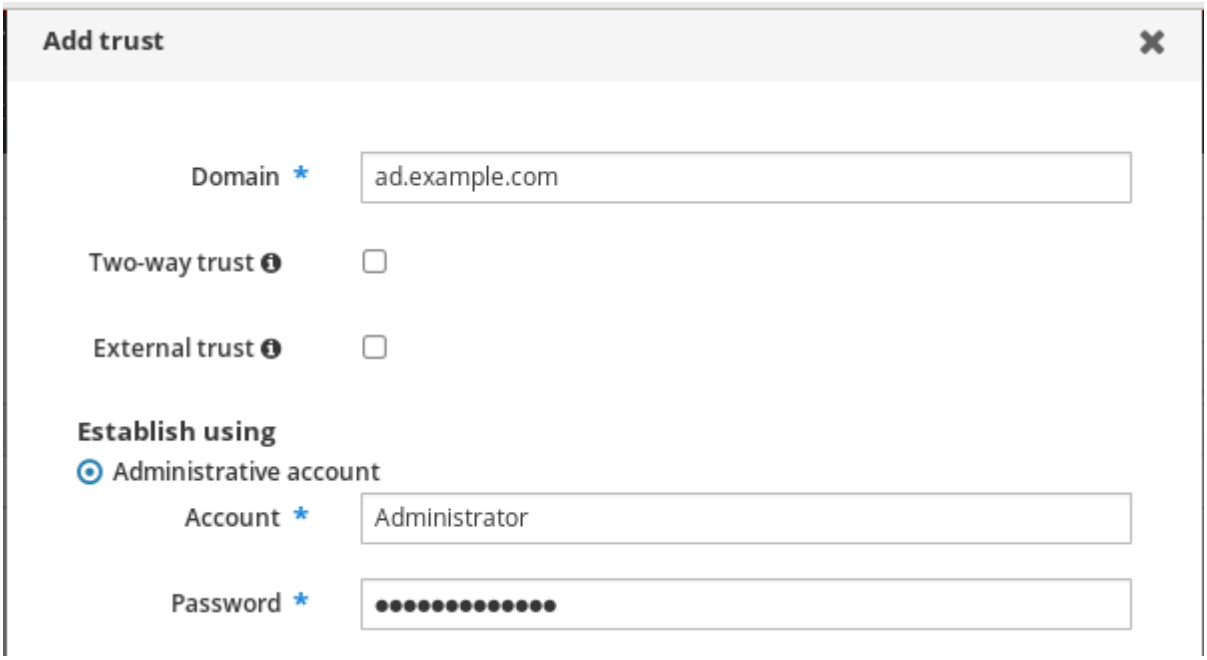
- IdM 管理者としてログインしている。

手順

1. 管理者権限で IdM Web UI にログインします。詳細は Web ブラウザーで IdM Web UI へのアクセス を参照してください。
2. IdM Web UI で、**IPA Server** タブをクリックします。
3. **IPA Server** タブで、**Trusts** タブをクリックします。
4. ドロップダウンメニューで、**Trusts** オプションを選択します。



5. **Add** ボタンをクリックします。
6. **Add Trust** ダイアログボックスで、Active Directory ドメインの名前を入力します。
7. **Account** フィールドおよび **Password** フィールドに、Active Directory 管理者の管理者認証情報を追加します。

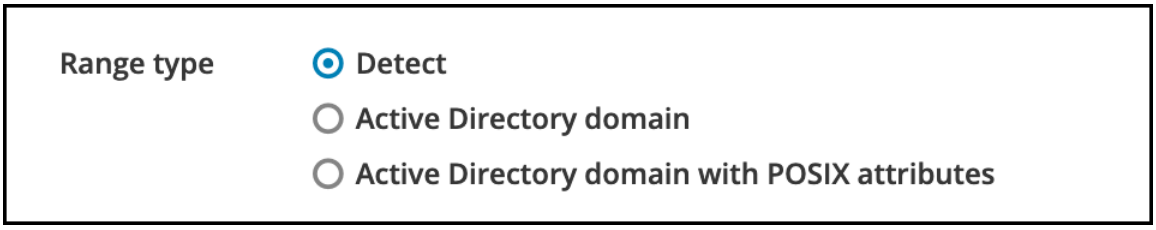


8. **(オプション)** AD ユーザーおよびグループが IdM のリソースにアクセスできるようにする場合は、**Two-way trust** を選択します。ただし、IdM の双方向の信頼では、AD の一方向の信頼ソリューションと比較して、ユーザーに追加の権限が付与されません。デフォルトのフォレスト間信頼の SID フィルタリング設定により、両方のソリューションの安全性は同じであると見なされます。
9. **(オプション)** AD フォレストのルートドメインではない AD ドメインで信頼を設定する場合は、**External trust** を選択します。フォレストの信頼では常に IdM と Active Directory フォレストのルートドメインとの間で信頼関係を確立する必要がありますが、IdM から AD フォレスト内の任意のドメインへの外部の信頼関係も確立できます。

10. **(オプション)** デフォルトでは、信頼インストールスクリプトは適切な ID 範囲タイプの検出を試みます。以下のオプションのいずれかを選択して、ID 範囲タイプを明示的に設定することもできます。

    a. SSSD が SID に基づいて AD ユーザーの UID および GID を自動的に生成するには、**Active Directory domain** ID 範囲タイプを選択します。これが最も一般的な設定です。

    b. Active Directory でユーザーに POSIX 属性を設定し (**uidNumber**、**gidNumber**など)、SSSD がこの情報を処理する必要がある場合は、**Active Directory domain with POSIX attributes** ID 範囲タイプを選択します。



警告

Range type 設定をデフォルトの **Detect** オプションに残すと、IdM はフォレストルートドメインの AD ドメインコントローラーから詳細を要求することで、適切な範囲タイプを自動的に選択しようとします。IdM が POSIX 属性を検出しない場合、信頼インストールスクリプトは **Active Directory domain** ID 範囲を選択します。

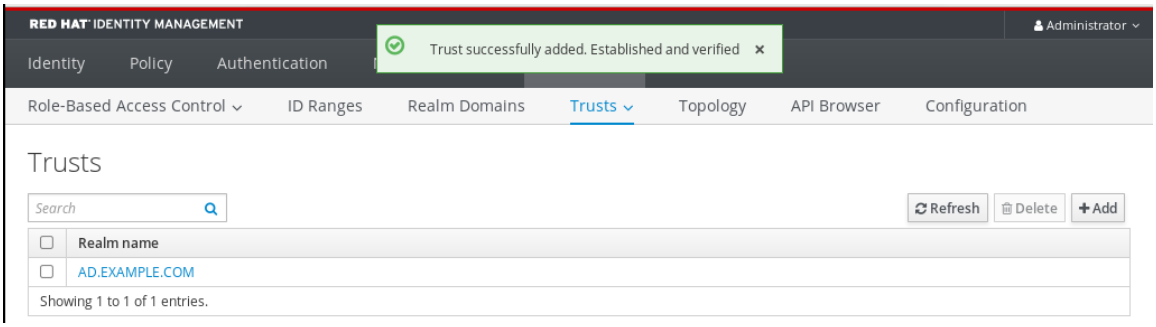
IdM がフォレストルートドメインの POSIX 属性を検出すると、信頼インストールスクリプトは、**Active Directory domain with POSIX attributes** ID 範囲を選択し、UID および GID が AD に正しく定義されていることを前提とします。POSIX 属性が AD で正しく設定されていない場合は、AD ユーザーを解決できません。

たとえば、IdM システムへのアクセスを必要とするユーザーおよびグループがフォレストルートドメインの一部ではなく、フォレストドメインの子ドメインにある場合は、インストールスクリプトで、子 AD ドメインで定義された POSIX 属性が検出されない場合があります。この場合、Red Hat は、信頼の確立時に POSIX ID 範囲タイプを明示的に選択することを推奨します。

11. **Add** をクリックします。

検証手順

- 信頼が IdM サーバーに正常に追加されると、IdM Web UI で緑色のポップアップ画面が表示されます。これは、以下を示しています。
  - ドメイン名が存在する。
  - Windows Server のユーザー名およびパスワードが正しく追加されている。



これで、信頼接続と Kerberos 認証のテストを続行します。

34.8.4. Ansible を使用した信頼関係の設定

Ansible Playbook を使用して Identity Management (IdM) と Active Directory (AD) の間に一方向の信頼協定を設定するには、次の手順に従います。3 種類の信頼関係を設定できます。

- **一方向の信頼** – デフォルトのオプション。一方向の信頼により、Active Directory (AD) ユーザーおよびグループは IdM のリソースにアクセスできますが、その逆はできません。IdM ドメインは AD フォレストを信頼しますが、AD フォレストは IdM ドメインを信頼しません。

- **双方向の信頼** – 双方向の信頼により、AD ユーザーおよびグループが IdM のリソースにアクセスできるようになります。
  信頼境界を使用して Kerberos プロトコルに **S4U2Self** および **S4U2Proxy** の Microsoft 拡張を必要とする、Microsoft SQL Server などのソリューションに、双方向の信頼を設定する必要があります。RHEL IdM ホスト上にあるアプリケーションは、AD ユーザーに関する **S4U2Self** または **S4U2Proxy** の情報を Active Directory ドメインコントローラーから要求する場合があり、双方向の信頼でこの機能が提供されます。

  この双方向の信頼機能では、IdM ユーザーは Windows システムにログインできないだけでなく、IdM の双方向信頼では、AD の一方向信頼ソリューションと比較して、権限が追加でユーザーに付与されるわけではありません。

  - 双方向の信頼を作成するには、**two_way: true** の変数を Playbook タスクに追加します。

- **外部信頼**: 異なるフォレストの IdM と AD ドメインとの間の信頼関係です。フォレストの信頼では常に IdM と Active Directory フォレストのルートドメインとの間で信頼関係を確立する必要がありますが、IdM からフォレスト内の任意のドメインへの外部の信頼関係も確立できます。管理上または組織上の理由で、フォレストの root ドメイン間でフォレストの信頼を確立できない場合に限り、これが推奨されます。

  - 外部信頼を作成するには、以下の変数を **external: true**の Playbook タスクに追加します。

前提条件

- Windows 管理者のユーザー名およびパスワード
- IdM **admin** パスワード。
- 信頼用の IdM サーバーの準備ができている。
- IdM 4.8.7 バージョン以降の IdM を使用している。サーバーにインストールされている IdM のバージョンを表示するには、**ipa --version** を実行します。
- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。

- Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
- この例では、**~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成したことを前提としている。
- この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。

- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

手順

1. **~/MyPlaybooks/** ディレクトリーに移動します。

```
$ cd ~/MyPlaybooks/
```

2. ユースケースに基づいて、以下のいずれかのシナリオを選択します。

- SSSD が SID に基づいて AD ユーザーおよびグループの UID および GID を自動的に生成する ID マッピング信頼合意を作成するには、以下の内容で **add-trust.yml** Playbook を作成します。

```
---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        range_type: ipa-ad-trust
        state: present
```

上記の例では、以下のようになります。

- **realm** は、AD レルム名文字列を定義します。
- **admin** は AD ドメイン管理者文字列を定義します。
- **Password** は、AD ドメイン管理者のパスワード文字列を定義します。

- SSSD が AD に保存されている POSIX 属性 (**uidNumber** や **gidNumber** など) を処理する POSIX 信頼合意を作成するには、以下の内容で **add-trust.yml** Playbook を作成します。

```
---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
```

```
  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        range_type: ipa-ad-trust-posix
        state: present
```

- フォレストルートドメインの AD ドメインコントローラーからの詳細を要求して、IdM が適切な範囲タイプ **ipa-ad-trust** または **ipa-ad-trust-posix** を選択しようとする信頼合意を作成するには、以下の内容を含む **add-trust.yml** Playbook を作成します。

```
---
- name: Playbook to create a trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is present
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        admin: Administrator
        password: secret_password
        state: present
```

警告

信頼の作成時に ID 範囲タイプを指定せず、IdM が AD フォレストルートドメインの POSIX 属性を検出しない場合は、信頼インストールスクリプトで **Active Directory ドメイン** ID 範囲を選択します。

IdM がフォレストルートドメインの POSIX 属性を検出すると、信頼インストールスクリプトは、**Active Directory domain with POSIX attributes** ID 範囲を選択し、UID および GID が AD に正しく定義されていることを前提とします。

ただし、POSIX 属性が AD で正しく設定されていない場合は、AD ユーザーを解決できません。たとえば、IdM システムへのアクセスを必要とするユーザーおよびグループがフォレストルートドメインの一部ではなく、フォレストドメインの子ドメインにある場合は、インストールスクリプトで、子 AD ドメインで定義された POSIX 属性が検出されない場合があります。この場合、Red Hat は、信頼の確立時に POSIX ID 範囲タイプを明示的に選択することを推奨します。

3. ファイルを保存します。

4. Ansible Playbook を実行します。Playbook ファイル、**secret.yml** ファイルを保護するパスワードを格納するファイル、およびインベントリーファイルを指定します。

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory add-trust.yml
```

関連情報

- /usr/share/doc/ansible-freeipa/README-trust.md
- /usr/share/doc/ansible-freeipa/playbooks/trust

34.8.5. Kerberos 設定の確認

Kerberos 設定を確認するには、Identity Management (IdM) ユーザーのチケットを取得できるかどうか、および IdM ユーザーがサービスチケットを要求できるかどうかを検証します。

手順

1. Active Directory (AD) ユーザーのチケットを要求します。

```
[root@ipaserver ~]# kinit user@AD.EXAMPLE.COM
```

2. IdM ドメイン内のサービスのサービスチケットを要求します。

```
[root@server ~]# kvno -S host server.idm.example.com
```

AD サービスチケットが正常に許可されると、その他の要求されたすべてのチケットと共に記載されたレルム間の TGT (Ticket-Granting Ticket) があります。TGT の名前は、krbtgt/IPA.DOMAIN@AD.DOMAIN です。

```
[root@server ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: user@AD.EXAMPLE.COM

Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01  host/server.idm.example.com@IDM.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01 krbtgt/IDM.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01  krbtgt/AD.EXAMPLE.COM@AD.EXAMPLE.COM
 renew until 04.05.2016 18:31:00
```

localauth プラグインは、Kerberos プリンシパルをローカルの System Security Services Daemon (SSSD) ユーザー名にマッピングします。これにより、AD ユーザーは Kerberos 認証を使用し、GSSAPI 認証に対応する Linux サービスに直接アクセスできます。

34.8.6. IdM で信頼設定の確認

信頼を設定する前に、Identity Management (IdM) サーバーおよび Active Directory (AD) サーバーが自身を解決でき、相互に解決できることを確認します。

前提条件

- 管理者権限でログインしている。

手順

1. UDP サービスレコード上の MS DC Kerberos、および TCP サービスレコード上の LDAP に、DNS クエリーを実行します。

```
[root@server ~]# dig +short -t SRV _kerberos._udp.dc._msdcs.idm.example.com.
0 100 88 server.idm.example.com.

[root@server ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.idm.example.com.
0 100 389 server.idm.example.com.
```

以下のコマンドは、**ipa-adtrust-install** を実行した IdM サーバーをリスト表示します。**ipa-adtrust-install** が IdM サーバーで実行していない場合、通常は最初の信頼関係を確立する前に出力が空になります。

2. TCP サービスレコード上の Kerberos と LDAP で DNS クエリーを実行して、IdM が AD のサービスレコードを解決できることを確認します。

```
[root@server ~]# dig +short -t SRV _kerberos._tcp.dc._msdcs.ad.example.com.
0 100 88 addc1.ad.example.com.

[root@ipaserver ~]# dig +short -t SRV _ldap._tcp.dc._msdcs.ad.example.com.
0 100 389 addc1.ad.example.com.
```

.

34.8.7. AD で信頼設定の確認

信頼の設定後に、以下を確認します。

- Identity Management (IdM) がホストするサービスが、Active Directory (AD) サーバーから解決できる。
- AD サービスは、AD サーバーで解決できる。

前提条件

- 管理者権限でログインしている。

手順

1. AD サーバーに、サービスレコードを検索する **nslookup.exe** ユーティリティーを設定します。

```
C:\>nslookup.exe
> set type=SRV
```

2. UDP サービスレコード上の Kerberos、および TCP サービスレコード上の LDAP に、ドメイン名を入力します。

```
> _kerberos._udp.idm.example.com.
_kerberos._udp.idm.example.com.       SRV service location:
    priority                = 0
```

```
    weight              = 100
    port                = 88
    svr hostname   = server.idm.example.com
> _ldap._tcp.idm.example.com
_ldap._tcp.idm.example.com      SRV service location:
    priority            = 0
    weight              = 100
    port                = 389
    svr hostname   = server.idm.example.com
```

3. サービスの種類を TXT に変更し、IdM Kerberos レルム名で TXT レコードに DNS クエリーを実行します。

```
C:\>nslookup.exe
> set type=TXT
> _kerberos.idm.example.com.
_kerberos.idm.example.com.      text =

    "IDM.EXAMPLE.COM"
```

4. UDP サービスレコード上の MS DC Kerberos、および TCP サービスレコード上の LDAP に、DNS クエリーを実行します。

```
C:\>nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.idm.example.com.
_kerberos._udp.dc._msdcs.idm.example.com.      SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = server.idm.example.com
> _ldap._tcp.dc._msdcs.idm.example.com.
_ldap._tcp.dc._msdcs.idm.example.com.      SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = server.idm.example.com
```

Active Directory は、その他の AD ドメインコントローラーや IdM 信頼コントローラーなど、AD 固有のプロトコル要求に応答できるドメインコントローラーの検出のみを想定します。**ipa-adtrust-install** ツールを使用して、IdM サーバーを信頼コントローラーに昇格し、どのサーバーが信頼コントローラーであるかを確認するには、**ipa server-role-find --role 'AD trust controller'** コマンドを使用します。

5. AD サービスが AD サーバーで解決可能であることを検証します。

```
C:\>nslookup.exe
> set type=SRV
```

6. UDP サービスレコード上の Kerberos、および TCP サービスレコード上の LDAP に、ドメイン名を入力します。

```
> _kerberos._udp.dc._msdcs.ad.example.com.
_kerberos._udp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
```

```
    weight = 100
    port = 88
    svr hostname = addc1.ad.example.com
> _ldap._tcp.dc._msdcs.ad.example.com.
_ldap._tcp.dc._msdcs.ad.example.com.  SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = addc1.ad.example.com
```

34.8.8. 信頼エージェントの作成

信頼エージェントは、AD ドメインコントローラーに対して ID ルックアップを実行できる IdM サーバーです。

たとえば、Active Directory と信頼できる IdM サーバーのレプリカを作成する場合は、そのレプリカを信頼エージェントとして設定できます。レプリカには、AD 信頼エージェントロールが自動的にインストールされていません。

前提条件

- IdM は、Active Directory 信頼でインストールされます。
- **sssd-tools** パッケージがインストールされている。

手順

1. 既存の信頼コントローラーで、**ipa-adtrust-install --add-agents** コマンドを実行します。

   ```
   [root@existing_trust_controller]# ipa-adtrust-install --add-agents
   ```

   このコマンドは、対話型設定セッションを開始し、エージェントの設定に必要な情報の入力を求めます。

2. 信頼エージェントで IdM サービスを再起動します。

   ```
   [root@new_trust_agent]# ipactl restart
   ```

3. 信頼エージェントの SSSD キャッシュからすべてのエントリーを削除します。

   ```
   [root@new_trust_agent]# sssctl cache-remove
   ```

4. レプリカに AD 信頼エージェントロールがインストールされていることを確認します。

   ```
   [root@existing_trust_controller]# ipa server-show new_replica.idm.example.com
   ...
   Enabled server roles: CA server, NTP server, AD trust agent
   ```

関連情報

- **--add-agents** オプションの詳細は、man ページの **ipa-adtrust-install(1)** を参照してください。

- 信頼エージェントの詳細は、Planning Identity Management の Trust controllers and trust agents を参照してください。

34.8.9. CLI での POSIX ID 範囲の自動プライベートグループマッピングの有効化

デフォルトでは、SSSD は、AD に保存されている POSIX データに依存する POSIX 信頼を確立している場合は、Active Directory(AD) ユーザーのプライベートグループをマッピングしません。AD ユーザーにプライマリーグループが設定されていない場合、IdM はこれを解決できません。

この手順では、コマンドラインで **auto_private_groups** SSSD パラメーターに **hybrid** オプションを設定して、ID 範囲の自動プライベートグループマッピングを有効にする方法を説明します。これにより、IdM は、AD にプライマリーグループが設定されていない AD ユーザーを解決できます。

前提条件

- IdM 環境と AD 環境との間で、POSIX フォレスト間の信頼が正常に確立されました。

手順

1. すべての ID 範囲を表示し、変更する AD ID 範囲を書き留めます。

```
[root@server ~]# ipa idrange-find
----------------
2 ranges matched
----------------
  Range name: IDM.EXAMPLE.COM_id_range
  First Posix ID of the range: 882200000
  Number of IDs in the range: 200000
  Range type: local domain range

  Range name: AD.EXAMPLE.COM_id_range
  First Posix ID of the range: 1337000000
  Number of IDs in the range: 200000
  Domain SID of the trusted domain: S-1-5-21-4123312420-990666102-3578675309
  Range type: Active Directory trust range with POSIX attributes
----------------------------
Number of entries returned 2
----------------------------
```

2. **ipa idrange-mod** コマンドを使用して、AD ID 範囲の自動プライベートグループの動作を調整します。

```
[root@server ~]# ipa idrange-mod --auto-private-groups=hybrid
AD.EXAMPLE.COM_id_range
```

3. SSSD キャッシュをリセットして、新しい設定を有効にします。

```
[root@server ~]# sss_cache -E
```

関連情報

- Options for automatically mapping private groups for AD users

34.8.10. IdM WebUI での POSIX ID 範囲の自動プライベートグループマッピングの有効化

デフォルトでは、SSSD は、AD に保存されている POSIX データに依存する POSIX 信頼を確立している場合は、Active Directory(AD) ユーザーのプライベートグループをマッピングしません。AD ユーザーにプライマリーグループが設定されていない場合、IdM はこれを解決できません。

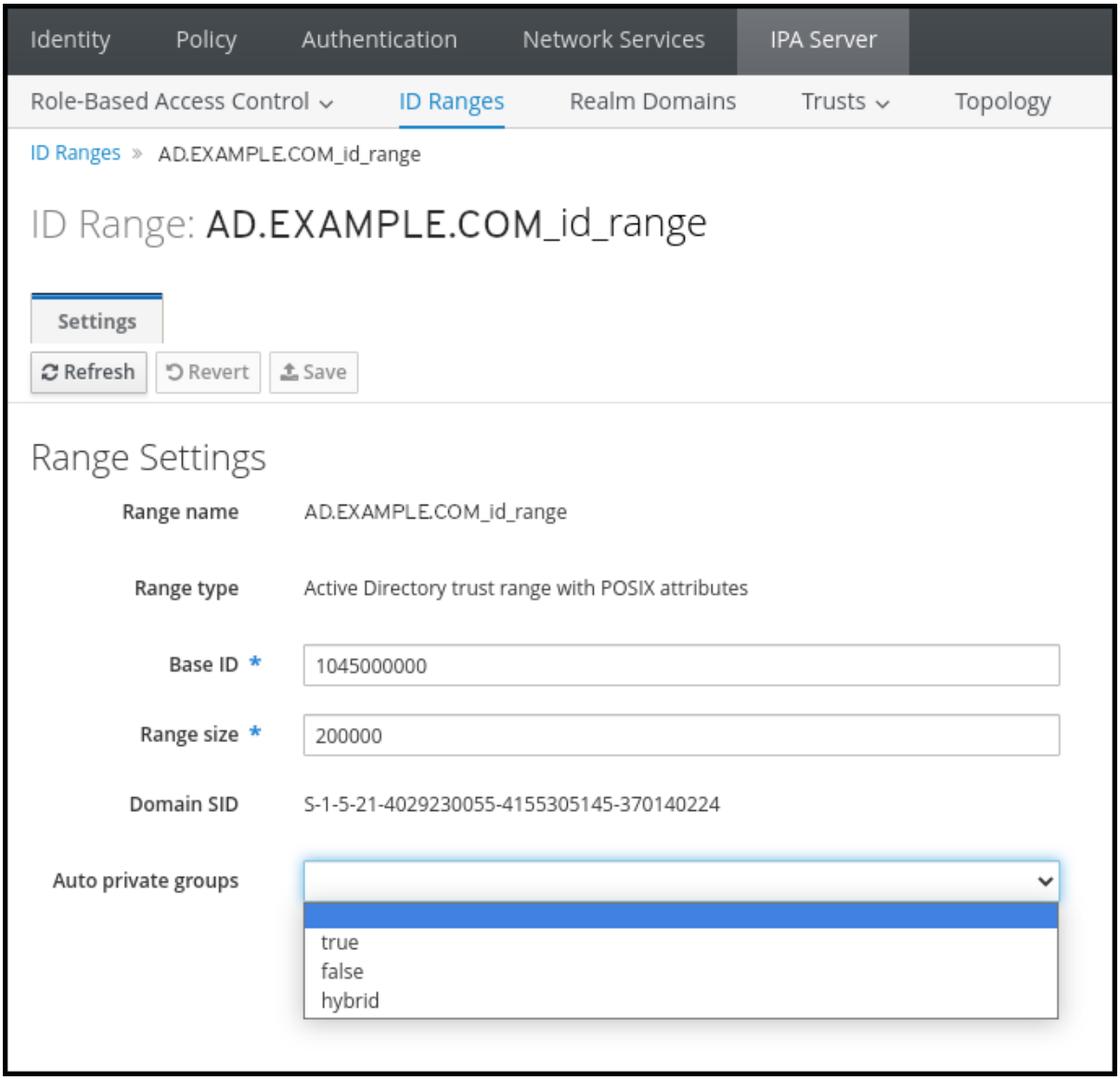
この手順では、Identity Management(IdM)WebUI の **auto_private_groups** SSSD パラメーター の **hybrid** オプションを設定して、ID 範囲の自動プライベートグループマッピングを有効にする方法を説明します。これにより、IdM は、AD にプライマリーグループが設定されていない AD ユーザーを解決できます。

前提条件

- IdM 環境と AD 環境との間で、POSIX フォレスト間の信頼が正常に確立されました。

手順

1. ユーザー名とパスワードを使用して IdM Web UI にログインします。
2. **IPA Server → ID Ranges** タブを開きます。
3. **AD.EXAMPLE.COM_id_range** など、変更する ID 範囲を選択します。
4. **Auto private groups** ドロップダウンメニューから、**hybrid** オプションを選択します。



5. **Save** ボタンをクリックして変更を保存します。

関連情報

- Options for automatically mapping private groups for AD users

34.9. フォレスト間の信頼設定に関するトラブルシューティング

Identity Management (IdM) 環境と Active Directory (AD) フォレストの間で、フォレスト間で信頼を設定するプロセスのトラブルシューティングについて詳しく説明します。

34.9.1. AD とのフォレスト間の信頼を確立する際の一連のイベント

ipa trust-add コマンドを使用して、Active Directory (AD) ドメインコントローラー (DC) とのフォレスト間の信頼を確立すると、コマンドを実行したユーザーに代わってコマンドが動作し、IdM サーバーで次のアクションを実行します。フォレスト間の信頼を確立する際に問題が発生した場合は、このリストを使用して、問題を絞り込み、トラブルシューティングすることができます。

パート 1: コマンドによる設定と入力の確認

1. IdM サーバーに **Trust Controller** のロールがあることを確認します。

2. **ipa trust-add** コマンドに渡されたオプションを確認します。

3. 信頼されたフォレストルートドメインに関連付けられている ID 範囲を確認します。ID 範囲の種類とプロパティーを **ipatrust-add** コマンドのオプションとして指定しなかった場合、それらは Active Directory から検出されます。

パート 2: コマンドによる Active Directory ドメインへの信頼確立の試行

4. 信頼方向ごとに個別の信頼オブジェクトを作成します。各オブジェクトは両サイド (IdM と AD) で作成されます。一方向の信頼を確立する場合、各サイドに 1 つのオブジェクトのみが作成されます。

5. IdM サーバーは Samba スイートを使用して Active Directory のドメインコントローラー機能を処理し、ターゲット AD PDC 上に信頼オブジェクトを作成します。

   a. IdM サーバーは、ターゲット DC 上の **IPC$** 共有への安全な接続を確立します。RHEL 8.4 以降、接続には、セッションに使用される AES ベースの暗号化で接続が十分に保護されていることを保証するために、少なくとも WindowsServer2012 以降での SMPB3 プロトコルが必要です。

   b. IdM サーバーは、**LSA QueryTrustedDomainInfoByName** 呼び出しを使用して、信頼されたドメインオブジェクト (TDO) の存在をクエリーします。

   c. TDO がすでに存在する場合は、**LSA DeleteTrustedDomain** 呼び出しを使用してその TDO を削除します。

注記

信頼の確立に使用される AD ユーザーアカウントに、**Incoming Forest Trust Builders** グループのメンバーなど、フォレストルートに対する完全な **Enterprise Admin (EA)** または **Domain Admin (DA)** 特権がない場合、この呼び出しは失敗します。古い TDO が自動的に削除されない場合、AD 管理者は手動で AD から削除する必要があります。

   d. IdM サーバーは、**LSA CreateTrustedDomainEx2** 呼び出しを使用して新しい TDO を作成します。TDO クレデンシャルは、Samba が提供する 128 文字のランダムなパスワードジェネレーターを使用してランダムに生成されます。

   e. 次に、新しい TDO を **LSA SetInformationTrustedDomain** 呼び出しで変更し、信頼でサポートされている暗号化タイプが適切に設定されていることを確認します。

      i. Active Directory の設計に基づき、RC4 キーが使用されていない場合でも、**RC4_HMAC_MD5** 暗号化タイプが有効になっている。

      ii. **AES128_CTS_HMAC_SHA1_96** および **AES256_CTS_HMAC_SHA1_96** 暗号化タイプが有効になっている。

6. フォレストの信頼の場合、**LSA SetInformationTrustedDomain** 呼び出しでフォレスト内のドメインに推移的に到達できることを確認します。

7. **LSA RSetForestTrustInformation** 呼び出しを使用して、他のフォレスト (AD と通信する場合は IdM、IdM と通信する場合は AD) に関する信頼トポロジー情報を追加します。

注記

この手順により、次の 3 つの理由のいずれかで競合が発生する可能性があります。

1. **LSA_SID_DISABLED_CONFLICT** エラーとして報告される SID namespace の競合。この競合は解決できません。
2. **LSA_NB_DISABLED_CONFLICT** エラーとして報告される NetBIOS namesapce の競合。この競合は解決できません。
3. **LSA_TLN_DISABLED_CONFLICT** エラーとして報告される、DNS namespace とトップレベル名 (TLN) の競合。別のフォレストが原因で TLN の競合が発生した場合、IdM サーバーは自動的に解決できます。

TLN の競合を解決するために、IdM サーバーは次の手順を実行します。

1. 競合するフォレストのフォレスト信頼情報を取得します。
2. IdM DNS namespace 間の除外エントリーを AD フォレストに追加します。
3. 競合するフォレストのフォレスト信頼情報を設定します。
4. 元のフォレストへの信頼確立を再試行します。

IdM サーバーは、フォレストの信頼を変更できる AD 管理者の権限で **ipa trust-add** コマンドを認証した場合にのみ、これらの競合を解決できます。これらの権限にアクセスできない場合、元のフォレストの管理者は、Windows UI の **Active Directory Domains and Trusts** セクションで上記の手順を手動で実行する必要があります。

8. 存在しない場合は、信頼されたドメインの ID 範囲を作成します。
9. フォレストの信頼については、フォレストのトポロジーの詳細について、フォレストのルートから Active Directory ドメインコントローラーにクエリーします。IdM サーバーはこの情報を使用して、信頼されたフォレストから追加のドメインの追加 ID 範囲を作成します。

関連情報

- 信頼コントローラーおよび信頼エージェント
- Overview Documents (Microsoft)
- Technical Documents (Microsoft)
- Privileged Accounts and Groups in Active Directory (Microsoft)

34.9.2. AD の信頼を確立するための前提条件のチェックリスト

次のチェックリストを使用して、AD ドメインとの信頼を作成するための前提条件を確認できます。

表34.4 テーブル

コンポーネント	Configuration	詳細
製品バージョン	Active Directory ドメインは、サポートされているバージョンの Windows Server を使用しています。	サポート対象の Windows Server バージョン
AD 管理者権限	Active Directory 管理アカウントは、次のいずれかのグループのメンバーです。 ● AD フォレストの **Enterprise Admin (EA)** グループ ● AD フォレスト用のフォレストルートドメインの **Domain Admins (DA)** グループ	
ネットワーク	IPv6 サポートは、すべての IdM サーバーの Linux カーネルで有効になっています。	IdM における IPv6 要件
日時	両方のサーバーの日付と時刻の設定が一致していることを確認します。	IdM のタイムサービス要件
暗号化タイプ	次の AD アカウントに AES 暗号化キーがあります。 ● AD 管理者 ● AD ユーザーアカウント ● AD サービス 最近 AD で AES 暗号化を有効にした場合は、次の手順で新しい AES キーを生成します。 1. フォレスト内の AD ドメイン間の信頼関係を再確立します。 2. AD 管理者、ユーザーアカウント、およびサービスのパスワードを変更します。	● IdM における暗号化タイプのサポート ● GPO を使用した Active Directory で AES 暗号化タイプの有効化

コンポーネント	Configuration	詳細
ファイアウォール	双方向通信のために、IdM サーバーと AD ドメインコントローラーで必要なすべてのポートを開いています。	IdM と AD との間の通信に必要なポート
DNS	• IdM と AD には、それぞれ固有のプライマリー DNS ドメインがあります。 • IdM ドメインと AD DNS ドメインは重複していません。 • LDAP および Kerberos サービスの適切な DNS サービス (SRV) レコード。 • 信頼内のすべての DNS ドメインから DNS レコードを解決できます。 • Kerberos レルム名は、プライマリー DNS ドメイン名を大文字にしたものです。たとえば、DNS ドメイン **example.com** には、対応する Kerberos レルム **EXAMPLE.COM** があります。	信頼用の DNS およびレルムの設定の設定
トポロジー	信頼コントローラーとして設定した IdM サーバーとの信頼を確立しようとしていることを確認します。	信頼コントローラーおよび信頼エージェント

34.9.3. AD の信頼を確立する試みのデバッグログを収集

IdM 環境と AD ドメイン間の信頼確立で問題が発生した場合は、次の手順を使用して詳細なエラーログを有効にし、信頼を確立する試みのログを収集できるようにします。これらのログを確認してトラブルシューティング作業に役立てたり、Red Hat テクニカルサポートケースで提供したりできます。

前提条件

- IdM サービスを再起動するには root 権限が必要です。

手順

1. IdM サーバーのデバッグを有効にするには、次の内容でファイル **/etc/ipa/server.conf** を作成します。

```
[global]
debug=True
```

2. **httpd** サービスを再起動して、デバッグ設定をロードします。

```
[root@trust_controller ~]# systemctl restart httpd
```

3. **smb** および **winbind** サービスを停止します。

```
[root@trust_controller ~]# systemctl stop smb winbind
```

4. **smb** および **winbind** サービスのデバッグログレベルを設定します。

```
[root@trust_controller ~]# net conf setparm global 'log level' 100
```

5. IdM フレームワークで使用される Samba クライアントコードのデバッグログを有効にするには、**/usr/share/ipa/smb.conf.empty** 設定ファイルを編集して次の内容にします。

```
[global]
log level = 100
```

6. 以前の Samba ログを削除します。

```
[root@trust_controller ~]# rm /var/log/samba/log.*
```

7. **smb** サービスおよび **winbind** サービスを起動します。

```
[root@trust_controller ~]# systemctl start smb winbind
```

8. 詳細モードを有効にして信頼の確率を試みる際に、タイムスタンプを出力します。

```
[root@trust_controller ~]# date; ipa -vvv trust-add --type=ad ad.example.com
```

9. 失敗したリクエストについては、次のエラーログファイルを確認してください。

   a. **/var/log/httpd/error_log**

   b. **/var/log/samba/log.***

10. デバッグを無効にします。

```
[root@trust_controller ~]# mv /etc/ipa/server.conf /etc/ipa/server.conf.backup
[root@trust_controller ~]# systemctl restart httpd
[root@trust_controller ~]# systemctl stop smb winbind
[root@trust_controller ~]# net conf setparm global 'log level' 0
[root@trust_controller ~]# mv /usr/share/ipa/smb.conf.empty
/usr/share/ipa/smb.conf.empty.backup
[root@trust_controller ~]# systemctl start smb winbind
```

11. **(オプション)** 認証問題の原因を判断できない場合は、以下を行います。

    a. 最近生成したログファイルを収集してアーカイブします。

```
[root@trust_controller ~]# tar -cvf debugging-trust.tar /var/log/httpd/error_log
/var/log/samba/log.*
```

b. Red Hat テクニカルサポートケースを開き、試行からのタイムスタンプとデバッグログを提供します。

関連情報

- IPA - AD Trust Troubleshooting

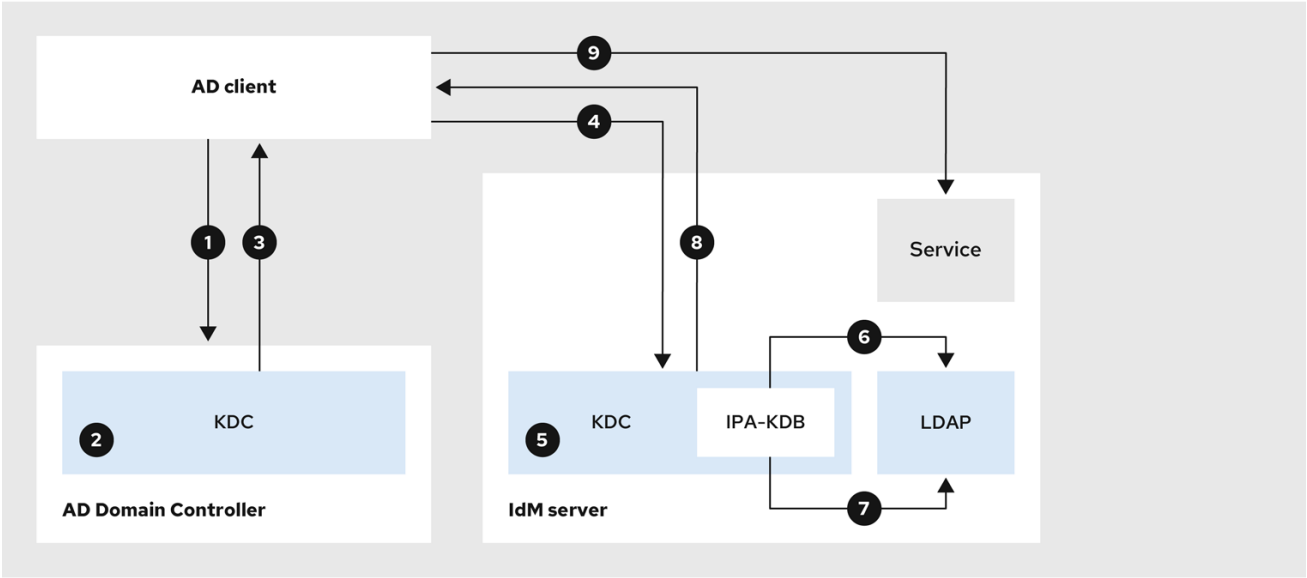
34.10. 他のフォレストのサービスへのクライアントアクセスに関するトラブルシューティング

Identity Management (IdM) 環境と Active Directory (AD) 環境の間に信頼を設定した後、一方のドメインのクライアントがもう一方のドメインのサービスにアクセスできないという問題が発生する場合があります。次の図を使用して、問題のトラブルシューティングを行ってください。

34.10.1. AD フォレストルートドメイン内のホストが IdM サーバーのサービスをリクエストする場合の情報の流れ

次の図は、Active Directory (AD) クライアントが Identity Management (IdM) ドメインのサービスをリクエストする際の情報の流れを説明しています。

AD クライアントから IdM サービスにアクセスする際に問題が発生した場合は、この情報を使用してトラブルシューティングの作業を絞り込み、問題の原因を特定できます。



231_RHEL_0422

1. AD クライアントは AD Kerberos Distribution Center (KDC) に接続して、IdM ドメインのサービスに対して TGS リクエストを実行します。
2. AD KDC は、サービスが信頼された IdM ドメインに属していることを認識します。
3. AD KDC は、信頼された IdM KDC への参照とともに、クライアントにレルム間のチケット保証チケット (TGT) を送信します。

4. AD クライアントは、レルム間 TGT を使用して IdM KDC へのチケットをリクエストします。
5. IdM KDC は、クロスレルム TGT で送信される特権属性証明書 (MS-PAC) を検証します。
6. IPA-KDB プラグインは、LDAP ディレクトリーをチェックして、外部プリンシパルがリクエストされたサービスのチケットを取得できるかどうかを確認する場合があります。
7. IPA-KDB プラグインは、MS-PAC をデコードし、データを検証およびフィルタリングします。LDAP サーバーで検索を行い、、ローカルグループなどの追加情報で MS-PAC を拡張する必要があるかどうかを確認します。
8. 次に、IPA-KDB プラグインは PAC をエンコードして署名し、サービスチケットに添付して AD クライアントに送信します。
9. AD クライアントは、IdM KDC によって発行されたサービスチケットを使用して IdM サービスに接続できるようになります。

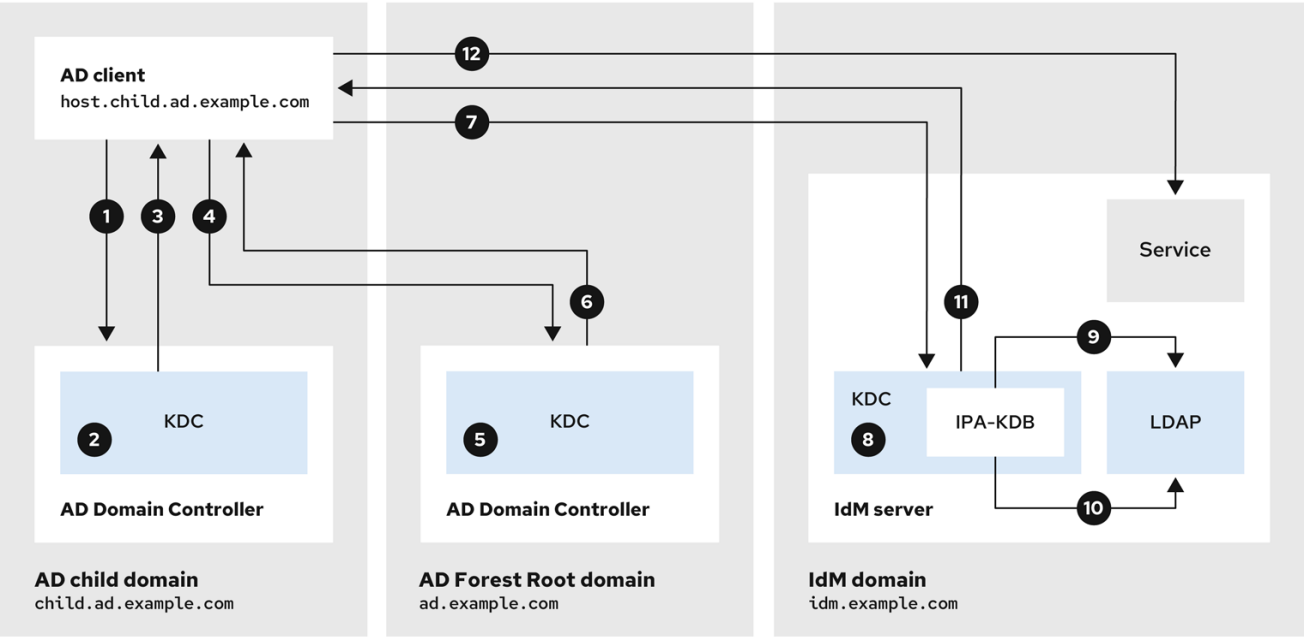
関連情報

- Flow of information when a host in an AD child domain requests services from an IdM server

34.10.2. AD 子ドメイン内のホストが IdM サーバーのサービスをリクエストする場合の情報の流れ

次の図は、子ドメイン内の Active Directory (AD) ホストが Identity Management (IdM) ドメインのサービスをリクエストする際の情報の流れを説明しています。このシナリオでは、AD クライアントは子ドメインの Kerberos Distribution Center (KDC) に接続し、次に AD フォレストルートの KDC に接続し、最後に IdM KDC に接続して IdM サービスへのアクセスをリクエストします。

AD クライアントから IdM サービスにアクセスする際に問題が発生し、AD クライアントが AD フォレストルートの子ドメインであるドメインに属する場合、この情報を使用してトラブルシューティングの作業を絞り込み、問題の原因を特定できます。



1. AD クライアントは 独自ドメイン内の AD Kerberos Distribution Center (KDC) に接続して、IdM ドメインのサービスに対して TGS リクエストを実行します。
2. 子ドメインである **child.ad.example.com** 内の AD KDC は、サービスが信頼された IdM ドメインに属していることを認識します。
3. 子ドメイン内の AD KDC は、AD フォレストルートドメイン **ad.example.com** の参照チケットをクライアントに送信します。
4. AD クライアントは、IdM ドメインのサービスについて、AD フォレストルートドメインの KDC に接続します。
5. フォレストルートドメインの KDC は、サービスが信頼された IdM ドメインに属していることを認識します。
6. AD KDC は、信頼された IdM KDC への参照とともに、クライアントにレルム間のチケット保証チケット (TGT) を送信します。
7. AD クライアントは、レルム間 TGT を使用して IdM KDC へのチケットをリクエストします。
8. IdM KDC は、クロスレルム TGT で送信される特権属性証明書 (MS-PAC) を検証します。
9. IPA-KDB プラグインは、LDAP ディレクトリーをチェックして、外部プリンシパルがリクエストされたサービスのチケットを取得できるかどうかを確認する場合があります。
10. IPA-KDB プラグインは、MS-PAC をデコードし、データを検証およびフィルタリングします。LDAP サーバーで検索を行い、、ローカルグループなどの追加情報で MS-PAC を拡張する必要があるかどうかを確認します。
11. 次に、IPA-KDB プラグインは PAC をエンコードして署名し、サービスチケットに添付して AD クライアントに送信します。
12. AD クライアントは、IdM KDC によって発行されたサービスチケットを使用して IdM サービスに接続できるようになります。

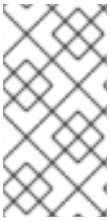
関連情報

- AD フォレストルートドメイン内のホストが IdM サーバーのサービスをリクエストする場合の情報の流れ

34.10.3. IdM クライアントが AD サーバーのサービスをリクエストする場合の情報の流れ

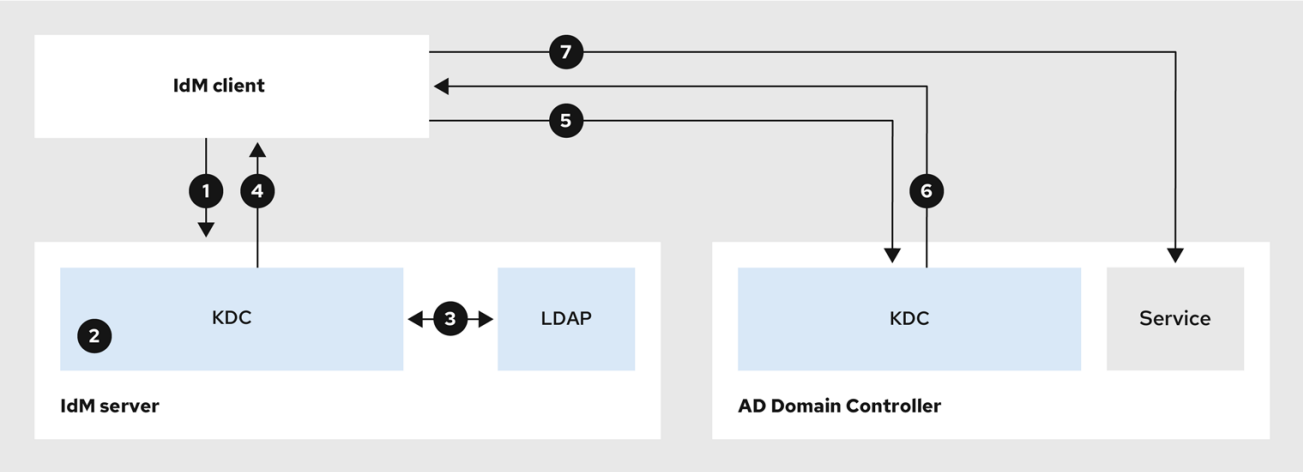
次の図は、Identity Management (IdM) と Active Directory (AD) の間に双方向の信頼を設定した場合に、IdM クライアントが AD ドメインでサービスをリクエストする場合の情報の流れを説明しています。

IdM クライアントから AD サービスにアクセスする際に問題が発生した場合は、この情報を使用してトラブルシューティングの取り組みを絞り込み、問題の原因を特定できます。



注記

デフォルトでは、IdM は AD への一方向の信頼を確立します。つまり、AD フォレスト内のリソースに対してレルム間のチケット保証チケット (TGT) を発行することはできません。信頼された AD ドメインからサービスへのチケットをリクエストできるようにするには、双方向の信頼を設定します。



231_RHEL_0422

1. IdM クライアントは、接続する AD サービスの IdM Kerberos Distribution Center (KDC) にチケット保証チケット (TGT) を要求します。
2. IdM KDC は、サービスが AD レルムに属していることを認識し、レルムが既知で信頼されていること、およびクライアントがそのレルムからサービスをリクエストできることを確認します。
3. IdM Directory Server からのユーザープリンシパルに関する情報を使用して、IdM KDC は、ユーザープリンシパルに関する特権属性証明書 (MS-PAC) レコードを使用してレルム間 TGT を作成します。
4. IdM KDC は、レルム間 TGT を IdM クライアントに送り返します。
5. IdM クライアントは AD KDC に接続して、AD サービスのチケットをリクエストし、IdM KDC によって提供される MS-PAC を含むレルム間 TGT を提示します。
6. AD サーバーは PAC を検証およびフィルタリングし、AD サービスのチケットを返します。
7. これで、IPA クライアントは AD サービスに接続できます。

関連情報

- 一方向および双方向の信頼

34.11. コマンドラインを使用した信頼の削除

コマンドラインインターフェイスを使用して IdM 側の Identity Management (IdM)/Active Directory (AD) 信頼を削除するには、次の手順に従います。

前提条件

- IdM 管理者として Kerberos チケットを取得している。詳細は Web UI で IdM にログイン: Kerberos チケットの使用 を参照してください。

手順

1. **ipa trust-del** コマンドを使用して、IdM から信頼設定を削除します。

```
[root@server ~]# ipa trust-del ad_domain_name
-----------------------------
Deleted trust "ad_domain_name"
-----------------------------
```

2. Active Directory 設定から信頼オブジェクトを削除します。

注記

信頼設定を削除しても、IdM が AD ユーザー用に作成した ID 範囲は自動的に削除されません。この場合、信頼を再度追加すると、既存の ID 範囲が再利用されます。また、AD ユーザーが IdM クライアントでファイルを作成した場合、その POSIX ID はファイルのメタデータに保持されます。

AD 信頼に関連するすべての情報を削除するには、信頼設定と信頼オブジェクトを削除した後、AD ユーザー ID 範囲を削除します。

```
# ipa idrange-del AD.EXAMPLE.COM_id_range
# systemctl restart sssd
```

検証手順

- **ipa trust-show** を実行して、信頼が削除されたことを確認します。

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

関連情報

- AD への信頼を削除した後の ID 範囲の削除

34.12. IDM WEB UI を使用した信頼の削除

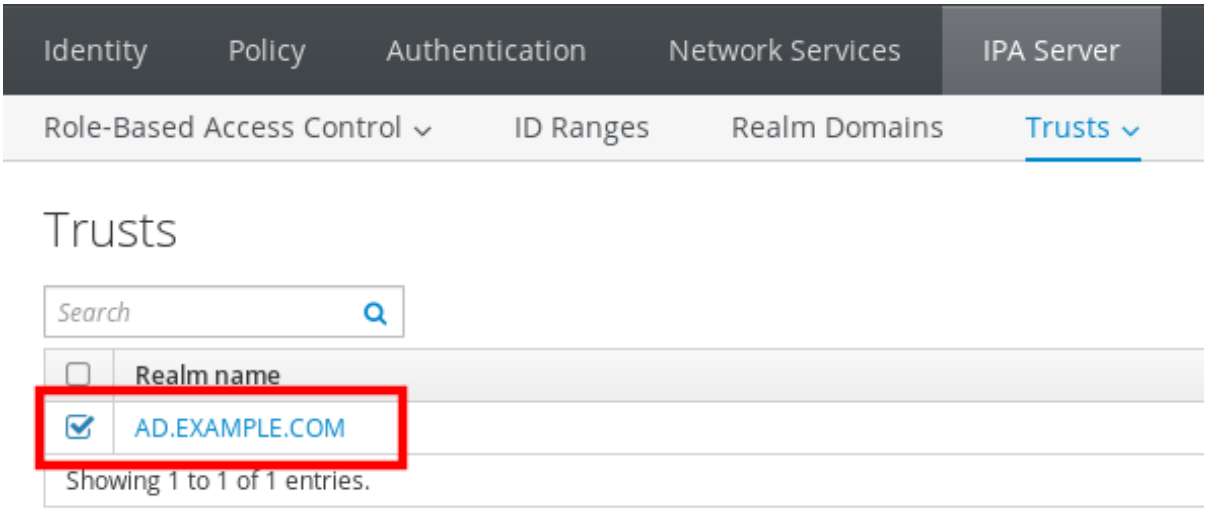
IdM Web UI を使用して Identity Management (IdM)/Active Directory (AD) 信頼を削除するには、次の手順に従います。

前提条件

- Kerberos チケットを取得している。詳細は Web UI で IdM にログイン: Kerberos チケットの使用 を参照してください。

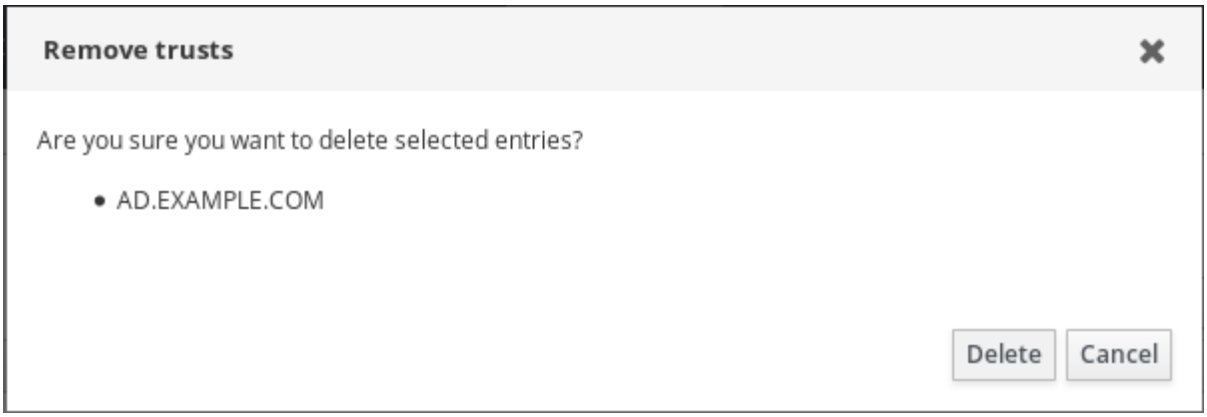
手順

1. 管理者権限で IdM Web UI にログインします。詳細は Web ブラウザーで IdM Web UI へのアクセス を参照してください。
2. IdM Web UI で、**IPA Server** タブをクリックします。
3. **IPA Server** タブで、**Trusts** タブをクリックします。
4. 削除する信頼を選択します。

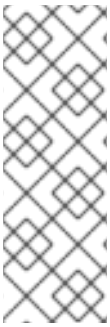


5. **Delete** ボタンをクリックします。

6. **Remove trusts** ダイアログボックスで、**Delete** をクリックします。



7. Active Directory 設定から信頼オブジェクトを削除します。



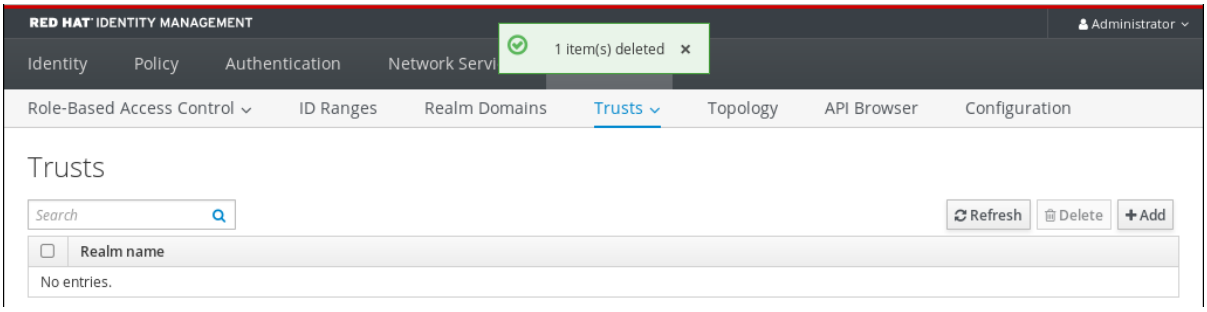
注記

信頼設定を削除しても、IdM が AD ユーザー用に作成した ID 範囲は自動的に削除されません。この場合、信頼を再度追加すると、既存の ID 範囲が再利用されます。また、AD ユーザーが IdM クライアントでファイルを作成した場合、その POSIX ID はファイルのメタデータに保持されます。

AD 信頼に関連するすべての情報を削除するには、信頼設定と信頼オブジェクトを削除した後、**ID Ranges** タブで AD ユーザー ID 範囲を削除します。

検証手順

- 信頼が正常に削除されていると、Web UI はテキストが付いた緑色のポップアップを表示します。



関連情報

- AD への信頼を削除した後の ID 範囲の削除

34.13. ANSIBLE を使用した信頼の削除

Ansible Playbook を使用して IdM 側の Identity Management (IdM)/Active Directory (AD) 信頼を削除するには、次の手順に従います。

前提条件

- IdM 管理者として Kerberos チケットを取得している。詳細は Web UI で IdM にログイン: Kerberos チケットの使用 を参照してください。
- 次の要件を満たすように Ansible コントロールノードを設定している。
  - Ansible バージョン 2.14 以降を使用している。
  - Ansible コントローラーに **ansible-freeipa** パッケージがインストールされている。
  - この例では、**~/MyPlaybooks/** ディレクトリーに、IdM サーバーの完全修飾ドメイン名 (FQDN) を使用して Ansible インベントリーファイル を作成したことを前提としている。
  - この例では、**secret.yml** Ansible vault に **ipaadmin_password** が保存されていることを前提としています。
- ターゲットノード (**ansible-freeipa** モジュールが実行されるノード) が、IdM クライアント、サーバー、またはレプリカとして IdM ドメインに含まれている。

手順

1. **~/MyPlaybooks/** ディレクトリーに移動します。

```
$ cd ~/MyPlaybooks/
```

2. 以下の内容を含む **del-trust.yml** Playbook を作成します。

```
---
- name: Playbook to delete trust
  hosts: ipaserver

  vars_files:
  - /home/user_name/MyPlaybooks/secret.yml
  tasks:
    - name: ensure the trust is absent
      ipatrust:
        ipaadmin_password: "{{ ipaadmin_password }}"
        realm: ad.example.com
        state: absent
```

この例では、**realm** は AD レルム名の文字列を定義します。

3. ファイルを保存します。

4. Ansible Playbook を実行します。Playbook ファイル、**secret.yml** ファイルを保護するパスワードを格納するファイル、およびインベントリーファイルを指定します。

```
$ ansible-playbook --vault-password-file=password_file -v -i inventory del-trust.yml
```

注記

信頼設定を削除しても、IdM が AD ユーザー用に作成した ID 範囲は自動的に削除されません。この場合、信頼を再度追加すると、既存の ID 範囲が再利用されます。また、AD ユーザーが IdM クライアントでファイルを作成した場合、その POSIX ID はファイルのメタデータに保持されます。

AD 信頼に関連するすべての情報を削除するには、信頼設定と信頼オブジェクトを削除した後、AD ユーザー ID 範囲を削除します。

```
# ipa idrange-del AD.EXAMPLE.COM_id_range
# systemctl restart sssd
```

検証手順

- **ipa trust-show** を実行して、信頼が削除されたことを確認します。

```
[root@server ~]# ipa trust-show ad.example.com
ipa: ERROR: ad.example.com: trust not found
```

関連情報

- /usr/share/doc/ansible-freeipa/README-trust.md
- /usr/share/doc/ansible-freeipa/playbooks/trust
- AD への信頼を削除した後の ID 範囲の削除

34.14. AD への信頼を削除した後の ID 範囲の削除

IdM 環境と Active Directory (AD) 環境間の信頼を削除している場合は、それに関連付けられている ID 範囲を削除することを推奨します。

警告

信頼できるドメインに関連付けられた ID 範囲に割り当てられた ID は、IdM に登録されているシステムのファイルおよびディレクトリーの所有権に引き続き使用される可能性があります。

削除した AD 信頼に対応する ID 範囲を削除すると、AD ユーザーが所有するファイルおよびディレクトリーの所有権を解決できなくなります。

前提条件

- AD 環境への信頼を削除している。

手順

1. 現在使用されている ID 範囲をすべて表示します。

```
[root@server ~]# ipa idrange-find
```

2. 削除した信頼に関連付けられた ID 範囲の名前を識別します。ID 範囲の名前の最初の部分は、信頼の名前 (**AD.EXAMPLE.COM_id_range** など) になります。

3. 範囲を削除します。

```
[root@server ~]# ipa idrange-del AD.EXAMPLE.COM_id_range
```

4. SSSD サービスを再起動して、削除した ID 範囲への参照を削除します。

```
[root@server ~]# systemctl restart sssd
```

関連情報

- コマンドラインを使用した信頼の削除 を参照してください。
- Removing the trust using the IdM Web UI を参照してください。