2. Request service tickets for a service within the IdM domain:

```
[root@ipaserver ~]# kvno -S host ipaserver.example.com
```

If the AD service ticket is successfully granted, there is a cross-realm ticket-granting ticket (TGT) listed with all of the other requested tickets. The TGT is named **krbtgt/*IPA.DOMAIN@AD.DOMAIN***.

```
[root@ipaserver ]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_hRtox00
Default principal: jsmith@AD.DOMAIN

Valid starting       Expires              Service principal
03.05.2016 18:31:06  04.05.2016 04:31:01
host/ipaserver.ipa.example.com@IPA.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:06 04.05.2016 04:31:01
krbtgt/IPA.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
03.05.2016 18:31:01  04.05.2016 04:31:01
krbtgt/AD.DOMAIN@AD.DOMAIN
 renew until 04.05.2016 18:31:00
```

The **localauth** plug-in maps Kerberos principals to local SSSD user names. This allows AD users to use Kerberos authentication and access Linux services, which support GSSAPI authentication directly.

Note

For more information about the plug-in, see Section 5.9.1, “Using SSH Without Passwords”.

5.3.4. Creating a Trust with a Shared Secret

A shared secret is a password that is known to trusted peers and can be used by other domains to join the trust. Trusts within Active Directory can be configured with a shared secret. In AD, the shared secret is stored as a *trusted domain object* (TDO) within the trust configuration.

IdM supports creating a trust using a shared secret instead of the AD administrator credentials. Setting up such trust requires the administrator to create the shared secret in AD and manually validate the trust on the AD side.

To create a trust with a shared secret:

1. Prepare the IdM server for the trust, as described in Section 5.3.3.1, “Preparing the IdM Server for Trust”.
2. Configure a trust in the **Active Directory Domains and Trusts** console. Use these settings:
   - Right-click the appropriate domain, and choose **Properties**.
   - Navigate to the **Trusts** tab, and click the **New Trust** button.
   - Enter the IdM DNS name. For example, **idm.example.com**.

- On the **Trust Type** page, select **Forest trust**.
- On the **Direction of Trust** page, choose **One-way: incoming**.
- On the **Sides of Trust** page, select **This domain only**.
- Set the **Trust Password**.

> **Note**
>
> The same password must be used when configuring the trust in IdM.

When asked to confirm the incoming trust, select **No**.

3. Create a trust agreement, as described in Section 5.3.3.2, "Creating a Trust Agreement". When running the **ipa trust-add** command, use the **--type** and **--trust-secret** options, and omit the **--admin** option. For example:

```
[root@ipaserver ~]# ipa trust-add --type=ad ad.example.com --
trust-secret
Shared secret for the trust:
----------------------------------------------------------
Added Active Directory trust for realm "ad.example.com"
----------------------------------------------------------
  Realm-Name: ad.example.com
  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-
23416912
  SID blacklist incoming: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-
1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-
5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12,
S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-
1-5-19, S-1-5-18
  SID blacklist outgoing: S-1-5-20, S-1-5-3, S-1-5-2, S-1-5-1, S-
1-5-7, S-1-5-6,
                          S-1-5-5, S-1-5-4, S-1-5-9, S-1-5-8, S-1-
5-17, S-1-5-16,
                          S-1-5-15, S-1-5-14, S-1-5-13, S-1-5-12,
S-1-5-11,
                          S-1-5-10, S-1-3, S-1-2, S-1-1, S-1-0, S-
1-5-19, S-1-5-18
  Trust direction: Trusting forest
  Trust type: Active Directory domain
  Trust status: Waiting for confirmation by remote side
```

4. In the **Domains and Trusts** console on the AD server, refresh the name suffix routing for the IdM server:
   - Right-click the appropriate domain, and choose **Properties**.
   - Navigate to the **Trusts** tab, select the incoming trust connection to the IdM domain, and click the **Properties** button.

- Open the **`Name Suffix Routing`** tab.
- Click the **`Refresh`** button, and the ***`*.idm.example.com`*** name suffix appears in the list.

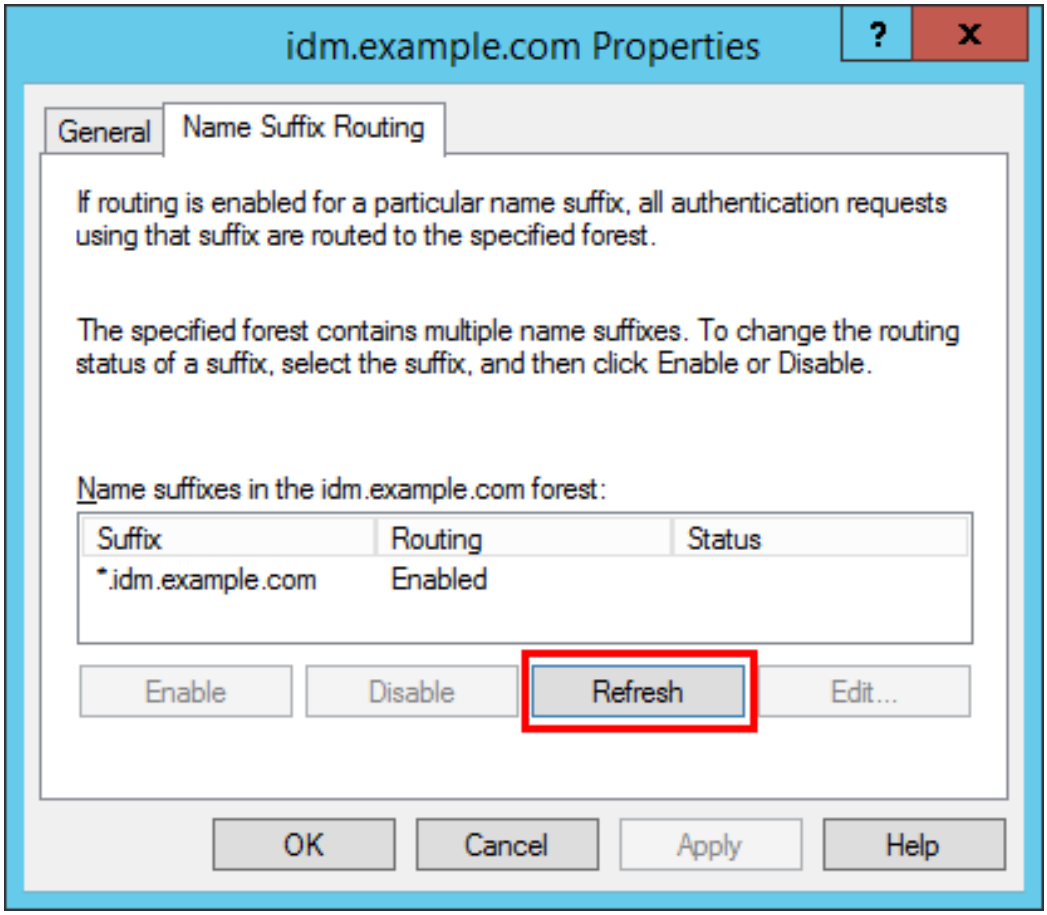

Figure 5.5. Refreshing the Name Suffix Routing

5. On the IdM server, verify that the trust relationship is established by using the **`ipa trust-show`** command.

```
[root@ipaserver ~]# ipa trust-show ad.example.com

  Domain NetBIOS name: AD
  Domain Security Identifier: S-1-5-21-796215754-1239681026-
23416912
  Trust direction: Trusting forest
  Trust type: Active Directory domain
```

Note

Before running **`ipa trust-show`**, you might be required to run the **`ipa trust-fetch-domains`** ***`ad_domain`*** command to ensure you obtain a Common Internet File System (CIFS) ticket-granting ticket.

6. Verify the Kerberos configuration, as described in Section 5.3.3.3, "Verifying the Kerberos Configuration".