This guide describes how to set up Red Hat Enterprise IPA 1.0 on each of the supported client platforms.
Preface .................................................................................................................... vii
1. Audience ...................................................................................................... vii
2. Document Conventions ................................................................................. vii
3. We Need Feedback! ...................................................................................... ix

1. Configuring Red Hat Enterprise Linux Clients .............................................. 1
   1.1. Downloading and Installing the IPA Packages ....................................... 1
   1.2. Configuring Client Authentication .......................................................... 1
   1.3. Configuring Kerberos ........................................................................... 2
   1.4. Configuring Client TLS on Red Hat Enterprise Linux 5 ....................... 3
   1.5. Configuring System Login ................................................................... 4
   1.6. Configuring NFS v4 with Kerberos ....................................................... 4
   1.7. Configuring Client SSH Access ............................................................ 5
   1.8. Configuring Host-Based Access Control ............................................... 6

2. Configuring Red Hat Enterprise Linux 4 as an IPA Client ................................ 7
   2.1. Downloading and Installing the IPA Packages ....................................... 7
   2.2. Configuring Client Authentication .......................................................... 7
   2.3. Configuring Kerberos ........................................................................... 7
   2.4. Configuring Client TLS on Red Hat Enterprise Linux 4 ....................... 8
   2.5. Configuring System Login ................................................................... 9
   2.6. Configuring NFS v4 with Kerberos ....................................................... 10
   2.7. Configuring Client SSH Access ........................................................... 11
   2.8. Configuring Host-Based Access Control .............................................. 12

2. Configuring Fedora as an IPA Client .................................................................. 15
   1. Downloading and Installing the IPA Packages ............................................. 15
   2. Configuring Client Authentication ............................................................. 15
   3. Configuring Kerberos ............................................................................... 16
   4. Configuring Client TLS on Fedora ............................................................. 16
   5. Configuring System Login ........................................................................ 18
   6. Configuring NFS v4 with Kerberos ............................................................ 18
   7. Configuring Client SSH Access ................................................................. 19
   8. Configuring Host-Based Access Control .................................................... 20

3. Configuring Solaris as an IPA Client ............................................................. 21
   1. Prerequisites ........................................................................................... 21
   2. Configuring Solaris 10 as an IPA Client ..................................................... 21
      2.1. Prerequisite Configuration ................................................................. 21
      2.2. Configuring PAM .............................................................................. 22
      2.3. Configuring LDAP .......................................................................... 22
      2.4. Configuring Kerberos ..................................................................... 22
      2.5. Configuring Client SSH Access ....................................................... 23
      2.6. Configuring NFS v4 ........................................................................ 24
   3. Configuring Solaris 9 as an IPA Client ....................................................... 25
   4. Configuring Solaris 8 as an IPA Client ....................................................... 25
   5. Testing the Configuration ........................................................................ 26
      5.1. Troubleshooting ............................................................................... 26
   4. Configuring AIX as an IPA Client ............................................................. 29
Preface

Welcome to the Red Hat Enterprise IPA Client Configuration Guide. This guide provides you with the information necessary to configure each of the supported client platforms to connect to the Red Hat Enterprise IPA server. This includes:

• System login (for accounts that exist in the IPA server)
• NFS v4 with Kerberos (for mounting remote filesystems)
• SSH access (secure client system access with Kerberos)
• Using Firefox to access the IPA web interface (for administrative operations)

1. Audience

The Red Hat Enterprise IPA Client Configuration Guide is intended for system administrators and those responsible for ensuring the successful configuration of Red Hat Enterprise IPA clients.

This guide assumes a good understanding of various operating systems, including Linux, Solaris and other UNIX systems, Macintosh and Microsoft Windows. It also assumes a working knowledge of LDAP and Red Hat Directory Server.

2. Document Conventions

Certain words in this manual are represented in different fonts, styles, and weights. This highlighting indicates that the word is part of a specific category. The categories include the following:

Courier font

Courier font represents commands, file names and paths, and prompts.

When shown as below, it indicates computer output:

<table>
<thead>
<tr>
<th>Desktop</th>
<th>about.html</th>
<th>logs</th>
<th>paulwesterberg.png</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>backupfiles</td>
<td>mail</td>
<td>reports</td>
</tr>
</tbody>
</table>

bold Courier font

Bold Courier font represents text that you are to type, such as: service jonas start

If you have to run a command as root, the root prompt (#) precedes the command:

# gconftool-2
**italic Courier font**
Italic Courier font represents a variable, such as an installation directory:
`install_dir/bin/`

**bold font**
Bold font represents **application programs** and **text found on a graphical interface**.

When shown like this: **OK**, it indicates a button on a graphical application interface.

Additionally, the manual uses different strategies to draw your attention to pieces of information. In order of how critical the information is to you, these items are marked as follows:

**Note**
A note is typically information that you need to understand the behavior of the system.

**Tip**
A tip is typically an alternative way of performing a task.

**Important**
Important information is necessary, but possibly unexpected, such as a configuration change that will not persist after a reboot.

**Caution**
A caution indicates an act that would violate your support agreement, such as recompiling the kernel.

**Warning**
A warning indicates potential data loss, as may happen when tuning hardware for maximum performance.
3. We Need Feedback!

If you find a typographical error in this manual, or if you have thought of a way to make this manual better, we would love to hear from you! Please submit a report in Bugzilla: http://bugzilla.redhat.com/bugzilla/ against the product Red_Hat_Enterprise_IPA.

When submitting a bug report, be sure to mention the manual’s identifier: Client_Configuration_Guide

If you have a suggestion for improving the documentation, try to be as specific as possible when describing it. If you have found an error, please include the section number and some of the surrounding text so we can find it easily.
Chapter 1.

Configuring Red Hat Enterprise Linux Clients

This chapter describes how to configure Red Hat Enterprise Linux as an IPA client. Red Hat Enterprise IPA 1.0 currently supports Red Hat Enterprise Linux 4 and 5 as IPA clients.

Note

Before starting the Red Hat Enterprise IPA installation, ensure that you update your system with all the latest packages.

The IPA client installation process requires that an IPA server already exist.

1. Configuring Red Hat Enterprise Linux 5 as an IPA Client

1.1. Downloading and Installing the IPA Packages

Procedure 1.1. To download and install the Red Hat Enterprise Linux 5 IPA packages:

1. Subscribe to the appropriate channels on the Red Hat Network. Refer to Red Hat Enterprise IPA Release Notes for information on the channels that you need to subscribe to.

2. After you have subscribed to the appropriate channels, use the following command to install the IPA client, tools, and dependencies:

   # yum install ipa-client ipa-admintools

3. If the IPA server is also configured as the DNS server, and is in the same domain as the client, add the server's IP address as the first entry in the client's /etc/resolv.conf file.

1.2. Configuring Client Authentication

Procedure 1.2. To configure client authentication on Red Hat Enterprise Linux 5, run the following command:
If DNS Discovery is configured correctly, the script should set up the client without prompting for any further information. This includes configuring the name service cache daemon (nscd) to start at boot time. The nscd caches the most common name service requests from the client, and reduces the load on the server. If DNS Discovery is not configured, the script will prompt you for the information it requires.

When the script has finished configuring the IPA client, it displays information about the realm, DNS domain, IPA server, and other related information, similar to the following:

```
Discovery was successful!
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipaserver.example.com
BaseDN: dc=example,dc=com
```

**Note**

Ensure that you run the correct command to set up the client. Separate scripts exist for Red Hat Enterprise Linux 4 and 5, and they are not interchangeable.

If the IPA server and client are not in the same domain, the setup script will prompt you for the information that it requires.

### 1.3. Configuring Kerberos

The installation script performs the Kerberos configuration automatically. This includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

The following is an example of a Kerberos configuration file for Red Hat Enterprise IPA:

```
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
forwardable = yes
ticket_lifetime = 24h

[realms]
EXAMPLE.COM = {
kdc = ipaserver.example.com:88
admin_server = ipaserver.example.com:749
default_domain = example.com
```
1.4. Configuring Client TLS on Red Hat Enterprise Linux 5

The SSL/TLS settings are only required if you want to use SSL between the clients and the server when performing operations such as account lookups.

Procedure 1.3. To configure a Red Hat Enterprise Linux 5 client for TLS:

1. Modify the following in the /etc/ldap.conf file:

```conf
URI   ldap://ipaserver.example.com
BASE  dc=example,dc=com
HOST  ipaserver.example.com
TLS_CACERTDIR /etc/cacerts/
TLS_REQCERT allow
```

Note

Ensure that the directory you specify for `TLS_CACERTDIR` actually exists.

2. On the IPA server, export the CA certificate to ASCII using the `certutil` utility with the `-a` option. For example, to export the certificate with the nickname "CA certificate", use the following command:

```
# certutil -L -d /etc/dirsrv/slapd-INSTANCE -n "CA certificate" -a
```

If you elected to create a self-signed CA during the installation process, then the CA certificate will be available on the server at http://ipaserver.example.com/ipa/errors/ca.crt

If you installed IPA using your own PKCS#12 files then this self-signed CA will not exist.

3. Copy this certificate to a temporary directory on the client machine, and install it in the /etc/cacerts directory as follows:

```
# cp cacert.asc /etc/cacerts/`openssl x509 -noout -hash -in cacert.asc`.0
```

The resulting file name is the hash of the contents of the certificate with a ".0" extension.

4. If the `TLS_CACERTDIR` directive does not work, set the cacert file directly:
# TLS_CACERT /etc/cacerts/cacert.asc

If more than one CA certificate is required, concatenate these certificates into a single file.

If you do not have access to the IPA server, you can still copy the CA certificate to the client.

**Procedure 1.4. To copy the CA certificate from the server to the client:**

1. Log in to the client machine, and become the root user.
2. Change to the directory where you need to install the CA certificate.
   ```bash
cd /etc/cacerts
   ```
3. Run the following command to copy the CA certificate from the server to the client:
   ```bash
   wget http://ipaserver.example.com/ipa/errors/ca.crt
   ```
4. After you have copied the certificate, install it as described previously.


### 1.5. Configuring System Login

No additional configuration is required to enable system login on Red Hat Enterprise Linux 5. Use the following tests to ensure that the configuration is working correctly:

- On the system console, log in as an IPA user. After you have logged in, open a shell and run the following commands:

  ```bash
  $ id (ensure that the user IDs and group IDs are correct)
  $ getent passwd
  $ getent group
  ```

If any of these tests fail, refer to the Troubleshooting\(^1\) section in the Administration Guide for information on how to locate any problems.

### 1.6. Configuring NFS v4 with Kerberos

---

Procedure 1.5. To configure NFS on the Red Hat Enterprise Linux 5 IPA client:

1. Obtain a Kerberos ticket for the admin user.
   
   ```bash
   # kinit admin
   ```

2. Add an NFS service principal on the client.
   
   ```bash
   # ipa-addservice nfs/ipaclient.example.com
   ```

3. Obtain a keytab for the NFS service principal.
   
   ```bash
   # ipa-getkeytab -s ipaserver.example.com -p nfs/ipaclient.example.com -k /etc/krb5.keytab
   ```

   **Note**

   The Linux NFS implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the `-e des-cbc-crc` option to the `ipa-getkeytab` command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

4. Add the following line to the `/etc/sysconfig/nfs` file:
   
   ```bash
   SECURE_NFS=yes
   ```

5. Start the rpcgssd daemon.
   
   ```bash
   # service rpcgssd start
   ```

The IPA client should now be fully configured to mount NFS shares using Kerberos credentials. Use the following command to test the configuration:

```bash
# mount -v -t nfs4 -o sec=krb5 ipaserver.example.com:/ /mnt
```

### 1.7. Configuring Client SSH Access

You can also configure the IPA client to accept incoming SSH requests and authenticate with the user's Kerberos credentials. After configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and
domain names with your own host and domain name.

**Procedure 1.6. To configure a Red Hat Enterprise Linux 5 IPA client for incoming SSH connections:**

1. The Red Hat Enterprise IPA client installation process configures the NTP service by default, but you should ensure that time on the IPA client and server is synchronized. If it is not, run the following commands on the IPA client:

```
# service ntpd stop
# ntpdate -s -p 8 -u ipaserver.example.com
# service ntpd start
```

**Note**
The `ntpdate` command does not work if `ntpd` is running.

2. Obtain a Kerberos ticket for the admin user.

```
# kinit admin
```

3. Add a host service principal on the IPA client.

```
# ipa-addservice host/ipaclient.example.com
```

4. Retrieve the keytab.

```
# ipa-getkeytab -s ipaserver.example.com -p host/ipaclient.example.com -k
/etc/krb5.keytab
```

The IPA client should now be fully configured to accept incoming SSH connections and authenticate with the user’s Kerberos credentials. Use the following command on another machine to test the configuration. This should succeed without asking for a password.

```
# ssh admin@ipaclient.example.com
```

**1.8. Configuring Host-Based Access Control**

You can configure Red Hat Enterprise Linux and Fedora to allow or deny access to Red Hat Enterprise IPA resources and services based on the configuration of the host from which access is attempted. Refer to the *Configuring Access Control* chapter of the Administration Guide for

2. Configuring Red Hat Enterprise Linux 4 as an IPA Client

Note
Before starting the Red Hat Enterprise IPA installation, ensure that you update your system with all the latest packages.
The IPA client installation process requires that an IPA server already exist.

2.1. Downloading and Installing the IPA Packages

Download and install the Red Hat Enterprise Linux 4 IPA Client RPM from the "Downloads" section of the appropriate Red Hat Enterprise IPA channel on the Red Hat Network.

2.2. Configuring Client Authentication

Procedure 1.7. To configure client authentication on Red Hat Enterprise Linux 4:

1. Create the /etc/ipa/ipa.conf file.
2. Use the following command to set up the IPA client:

   # ipa-client-setup --server ipaserver.example.com

3. Reboot the client machine.

Note
Ensure that you run the correct command to set up the client. Separate scripts exist for Red Hat Enterprise Linux 4 and 5, and they are not interchangeable.
The Red Hat Enterprise Linux 4 version of the IPA client installation script does not perform auto-discovery, and neither does it configure the client machine to perform auto-discovery.

2.3. Configuring Kerberos
The installation script performs the Kerberos configuration automatically. This includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

The following is an example of a Kerberos configuration file for Red Hat Enterprise IPA:

```plaintext
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
forwardable = yes
ticket_lifetime = 24h

[realms]
EXAMPLE.COM = {
kdc = ipaserver.example.com:88
    admin_server = ipaserver.example.com:749
default_domain = example.com
}

[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

2.4. Configuring Client TLS on Red Hat Enterprise Linux 4

The SSL/TLS settings are only required if you want to use SSL between the clients and the server when performing operations such as account lookups.

**Procedure 1.8. To configure a Red Hat Enterprise Linux 4 client for TLS:**

1. Modify the following in the `/etc/ldap.conf` file:

   ```plaintext
   URI       ldap://ipaserver.example.com
   BASE      dc=example,dc=com
   HOST      ipaserver.example.com
   TLS_CACERTDIR /etc/cacerts/
   TLS_REQCERT allow
   ```

   > **Note**
   
   Ensure that the directory you specify for `TLS_CACERTDIR` actually exists.

2. On the IPA server, export the CA certificate to ASCII using the `certutil` utility with the `-a` option. For example, to export the certificate with the nickname "CA certificate", use the
following command:

```
# certutil -L -d /etc/dirsrv/slapd-INSTANCE -n "CA certificate" -a
```

If you elected to create a self-signed CA during the installation process, then the CA certificate will be available on the server at http://ipaserver.example.com/ipa/errors/ca.crt

If you installed IPA using your own PKCS#12 files then this self-signed CA will not exist.

3. Copy this certificate to a temporary directory on the client machine, and install it in the /etc/cacerts directory as follows:

```
# cp cacert.asc /etc/cacerts/`openssl x509 -noout -hash -in cacert.asc`.0
```

The resulting file name is the hash of the contents of the certificate with a ".0" extension.

4. If the TLS_CACERTDIR directive does not work, set the cacert file directly:

```
# TLS_CACERT /etc/cacerts/cacert.asc
```

If more than one CA certificate is required, concatenate these certificates into a single file.

If you do not have access to the IPA server, you can still copy the CA certificate to the client.

**Procedure 1.9. To copy the CA certificate from the server to the client:**

1. Log in to the client machine, and become the root user.

2. Change to the directory where you need to install the CA certificate.

   ```
cd /etc/cacerts
   ```

3. Run the following command to copy the CA certificate from the server to the client:

   ```
   wget http://ipaserver.example.com/ipa/errors/ca.crt
   ```

4. After you have copied the certificate, install it as described previously.


**2.5. Configuring System Login**

No additional configuration is required to enable system login on Red Hat Enterprise Linux 4. Use the following tests to ensure that the configuration is working correctly:
\begin{itemize}
\item On the system console, log in as an IPA user. After you have logged in, open a shell and run the following commands:
\begin{verbatim}
$ id (ensure that the user IDs and group IDs are correct)
$ getent passwd
$ getent group
\end{verbatim}
\end{itemize}

If any of these tests fail, refer to the Troubleshooting\(^3\) section in the Administration Guide for information on how to locate any problems.

\section*{2.6. Configuring NFS v4 with Kerberos}

\subsection*{Procedure 1.10. To configure NFS on the Red Hat Enterprise Linux 4 IPA client:}

1. Obtain a Kerberos ticket for the admin user.

\begin{verbatim}
# kinit admin
\end{verbatim}

2. The ipa-admintools package is not available for Red Hat Enterprise Linux 4. Consequently, you need to perform the following steps on the IPA server.

   a. Add an NFS service principal for the client.

\begin{verbatim}
# ipa-addservice nfs/ipaclient.example.com
\end{verbatim}

   b. Retrieve the NFS keytab.

\begin{verbatim}
# ipa-getkeytab -s ipaserver.example.com -p nfs/ipaclient.example.com \\
- k /tmp/krb5.keytab
# klist -ket /tmp/krb5.keytab (to verify)
\end{verbatim}

\subsection*{Note}
The Linux NFS implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the \texttt{-e des-cbc-crc} option to the ipa-getkeytab command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

c. Copy the keytab from the server to the client.

    # scp /tmp/krb5.keytab root@ipaclient.example.com:/tmp/krb5.keytab

3. On the IPA client, use the `ktutil` command to import the keytab.

    # ktutil
    ktutil: read_kt /tmp/krb5.keytab
    ktutil: write_kt /etc/krb5/krb5.keytab
    ktutil: q

4. Add the following line to the `/etc/sysconfig/nfs` file:

    SECURE_NFS=yes

5. Start the `rpcgssd` daemon.

    # service rpcgssd start

The IPA client should now be fully configured to mount NFS shares using Kerberos credentials. Use the following command to test the configuration:

    # mount -v -t nfs4 -o sec=krb5 ipaserver.example.com:/ /mnt

### 2.7. Configuring Client SSH Access

You can configure the IPA client to accept incoming SSH requests and authenticate with the user's Kerberos credentials. After installing and configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and domain names with your own host and domain name.

**Procedure 1.11. To configure a Red Hat Enterprise Linux 4 IPA client for incoming SSH connections:**

1. The Red Hat Enterprise IPA client installation process configures the NTP service by default, but you should ensure that time on the IPA client and server is synchronized. If it is not, run the following commands on the IPA client:

    # service ntpd stop
    # ntpdate -s -p 8 -u ipaserver.example.com
    # service ntpd start
Note
The ntpdate command does not work if ntpd is running.

2. Obtain a Kerberos ticket for the admin user.

```
# kinit admin
```

3. The ipa-admintools package is not available for Red Hat Enterprise Linux 4. Consequently, you need to perform the following commands on the IPA server.

   a. Add a host service principal.

```
# ipa-addservice host/ipaclient.example.com
```

   b. Retrieve the host keytab.

```
# ipa-getkeytab -s ipaserver.example.com -p host/ipaclient.example.com -k /tmp/krb5.keytab
```

   c. Copy the keytab from the server to the client.

```
# scp /tmp/krb5.keytab root@ipaclient.example.com:/tmp/krb5.keytab
```

4. On the IPA client, use the ktutil command to import the keytab.

```
# ktutil
ktutil: read_kt /tmp/krb5.keytab
ktutil: write_kt /etc/krb5/krb5.keytab
ktutil: q
```

The IPA client should now be fully configured to accept incoming SSH connections and authenticate with the user’s Kerberos credentials. Use the following command on another machine to test the configuration. This should succeed without asking for a password.

```
# ssh admin@ipaclient.example.com
```

2.8. Configuring Host-Based Access Control

You can configure Red Hat Enterprise Linux and Fedora to allow or deny access to Red Hat Enterprise IPA resources and services based on the configuration of the host from which access is attempted. Refer to the Configuring Access Control chapter of the Administration Guide for
information on this topic.
Chapter 2.

Configuring Fedora as an IPA Client

This chapter describes how to configure Fedora as a Red Hat Enterprise IPA client. Red Hat Enterprise IPA 1.0 currently supports Fedora 7, 8, and 9 as IPA clients.

Note

Before starting the Red Hat Enterprise IPA installation, ensure that you update your system with all the latest packages.

The Red Hat Enterprise IPA client installation process requires that an IPA server already exist.

1. Downloading and Installing the IPA Packages

Procedure 2.1. To download and install the Fedora IPA packages and dependencies:

1. # yum install ipa-client ipa-admintools

2. If the IPA server is also configured as the DNS server, and is in the same domain as the client, add the server's IP address as the first entry in the client's /etc/resolv.conf file.

2. Configuring Client Authentication

Procedure 2.2. To configure client authentication on Fedora:

- Run the following command to set up the IPA client:

  # ipa-client-install

If DNS Discovery is configured correctly, the script should set up the client without prompting for any further information. This includes configuring the name service cache daemon (nscd) to start at boot time. The nscd caches the most common name service requests from the client, and reduces the load on the server. If DNS Discovery is not configured, the script will prompt you for the information it requires.

When the script has finished configuring the IPA client, it displays information about the realm,
DNS domain, IPA server, and other related information, similar to the following:

```
Discovery was successful!
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipaserver.example.com
BaseDN: dc=example,dc=com
```

**Note**
If the IPA server and client are not in the same domain, the setup script will prompt you for the information that it requires.

---

### 3. Configuring Kerberos

The installation script performs the Kerberos configuration automatically. This includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

The following is an example of a Kerberos configuration file for Red Hat Enterprise IPA:

```
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
forwardable = yes
ticket_lifetime = 24h

[realms]
EXAMPLE.COM = {
kdc = ipaserver.example.com:88
admin_server = ipaserver.example.com:749
default_domain = example.com
}

[domain_realm]
.example.com = EXAMPLE.COM
test.example.com = EXAMPLE.COM
```

### 4. Configuring Client TLS on Fedora

The SSL/TLS settings are only required if you want to use SSL between the clients and the server when performing operations such as account lookups.

**Procedure 2.3. To configure a Fedora client for TLS:**
1. Modify the following in the `/etc/ldap.conf` file:

```
URI     ldap://ipaserver.example.com
BASE    dc=example,dc=com
HOST    ipaserver.example.com
TLS_CACERTDIR /etc/cacerts/
TLS_REQCERT allow
```

**Note**

Ensure that the directory you specify for `TLS_CACERTDIR` actually exists.

2. On the IPA server, export the CA certificate to ASCII using the `certutil` utility with the `-a` option. For example, to export the certificate with the nickname "CA certificate", use the following command:

```
# certutil -L -d /etc/dirsrv/slapd-INSTANCE -n "CA certificate" -a
```

If you elected to create a self-signed CA during the installation process, then the CA certificate will be available on the server at

http://ipaserver.example.com/ipa/errors/ca.crt

If you installed IPA using your own PKCS#12 files then this self-signed CA will not exist.

3. Copy this certificate to a temporary directory on the client machine, and install it in the `/etc/cacerts` directory as follows:

```
# cp cacert.asc /etc/cacerts/`openssl x509 -noout -hash -in cacert.asc`.0
```

The resulting file name is the hash of the contents of the certificate with a ".0" extension.

4. If the `TLS_CACERTDIR` directive does not work, set the cacert file directly:

```
# TLS_CACERT /etc/cacerts/cacert.asc
```

If more than one CA certificate is required, concatenate these certificates into a single file.

If you do not have access to the IPA server, you can still copy the CA certificate to the client.

**Procedure 2.4. To copy the CA certificate from the server to the client:**

1. Log in to the client machine, and become the `root` user.

2. Change to the directory where you need to install the CA certificate.
cd /etc/cacerts

3. Run the following command to copy the CA certificate from the server to the client:

   wget http://ipaserver.example.com/ipa/errors/ca.crt

4. After you have copied the certificate, install it as described previously.

Refer to http://directory.fedora.redhat.com/wiki/Howto:SSL for more information on TLS Client Configuration for Linux clients.

5. Configuring System Login

No additional configuration is required to enable system login on Fedora. Use the following tests to ensure that the configuration is working correctly:

- On the system console, log in as an IPA user. After you have logged in, open a shell and run the following commands:

  $ id (ensure that the user IDs and group IDs are correct)
  $ getent passwd
  $ getent group

If any of these tests fail, refer to the Troubleshooting section in the Administration Guide for information on how to locate any problems.

6. Configuring NFS v4 with Kerberos

Procedure 2.5. To configure NFS on the Fedora IPA client:

1. Obtain a Kerberos ticket for the admin user.

   # kinit admin

2. Add an NFS service principal on the client.

   # ipa-addservice nfs/ipaclient.example.com
3. Obtain a keytab for the NFS service principal.

```
# ipa-getkeytab -s ipaserver.example.com -p nfs/ipaclient.example.com -k /etc/krb5.keytab
```

**Note**
The Linux NFS implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the `-e des-cbc-crc` option to the `ipa-getkeytab` command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

4. Add the following line to the `/etc/sysconfig/nfs` file:

```
SECURE_NFS=yes
```

5. Start the rpcgssd daemon.

```
# service rpcgssd start
```

The IPA client should now be fully configured to mount NFS shares using Kerberos credentials. Use the following command to test the configuration:

```
# mount -v -t nfs4 -o sec=krb5 ipaserver.example.com:/ /mnt
```

### 7. Configuring Client SSH Access

You can also configure the IPA client to accept incoming SSH requests and authenticate with the user’s Kerberos credentials. After installing and configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and domain names with your own host and domain name.

**Procedure 2.6. To configure a Fedora IPA client for incoming SSH connections:**

1. The Red Hat Enterprise IPA client installation process configures the NTP service by default, but you should ensure that time on the IPA client and server is synchronized. If it is not, run the following commands on the IPA client:

```
# service ntpd stop
```
# ntpdate -s -p 8 -u ipaserver.example.com
# service ntpd start

## Note
The `ntpdate` command does not work if `ntpd` is running.

2. **Obtain a Kerberos ticket for the admin user.**

   ```bash
   # kinit admin
   ```

3. **Add a host service principal on the IPA client.**

   ```bash
   # ipa-addservice host/ipaclient.example.com
   ```

4. **Retrieve the keytab.**

   ```bash
   # ipa-getkeytab -s ipaserver.example.com -p host/ipaclient.example.com -k /etc/krb5.keytab
   ```

The IPA client should now be fully configured to accept incoming SSH connections and authenticate with the user's Kerberos credentials. Use the following command on another machine to test the configuration. This should succeed without asking for a password.

```bash
# ssh admin@ipaclient.example.com
```

### 8. Configuring Host-Based Access Control

You can configure Red Hat Enterprise Linux and Fedora to allow or deny access to Red Hat Enterprise IPA resources and services based on the configuration of the host from which access is attempted. Refer to the *Configuring Access Control* chapter of the Administration Guide for information on this topic.

---

Configuring Solaris as an IPA Client

This chapter describes how to configure the various supported Solaris operating systems as Red Hat Enterprise IPA clients. Red Hat Enterprise IPA 1.0 is supported on the following Solaris platforms:

- Solaris 8, 9 & 10 (SPARC)
- Solaris 10 (x86)

1. Prerequisites

Before you begin the configuration, download and install the nss-ldap packages from the following locations:

- Solaris 8 packages: http://freeipa.org/downloads/solaris/nss_ldap/8/
- Solaris 9 packages: http://freeipa.org/downloads/solaris/nss_ldap/9/
- Solaris 10 packages: http://freeipa.org/downloads/solaris/nss_ldap/10/

For example, to install the RHATnss-ldap-253-12.i386.pkg, run the following command:

```
# pkgadd -d RHATnss-ldap-253-12.i386.pkg
```

2. Configuring Solaris 10 as an IPA Client

The following procedures describe how to configure Solaris 10 as a client for Red Hat Enterprise IPA. This requires modifications to the PAM, LDAP, and Kerberos configuration files. This section also includes instructions for configuring NFS, however this configuration is optional.

2.1. Prerequisite Configuration

Before you proceed with the main configuration, ensure that you make the following updates to your Solaris system:

**Configuring NTP.**

Ensure that NTP is correctly configured and enabled, and that time is synchronized between the client and the Red Hat Enterprise IPA server.

**Configuring DNS.**

Configure the /etc/resolv.conf file to include the correct DNS server. This server must be able to resolve the IPA Solaris client and IPA server names.
The following is an example of a valid `/etc/resolv.conf` file:

```plaintext
search example.com
nameserver bindserver.example.com
```

### Configuring Name Service Switch (NSS)

Configure the `/etc/nsswitch.conf` file to perform password and group lookup using LDAP.

The `/etc/nsswitch.conf` file should include the following lines:

```plaintext
passwd: files ldap[NOTFOUND=return]
group: files ldap[NOTFOUND=return]
```

### 2.2. Configuring PAM

Configure the `/etc/pam.conf` file to use PAM Kerberos first.

The following example shows how to set up PAM Kerberos authentication for console login:

```plaintext
login auth requisite pam_authtok_get.so.1
login auth sufficient pam_krb5.so.1
login auth required pam_dhkeys.so.1
login auth required pam_unix_cred.so.1
login auth required pam_unix_auth.so.1 use_first_pass
login auth required pam_dial_auth.so.1
```

### 2.3. Configuring LDAP

Configure the `/etc/ldap.conf` file as follows:

```plaintext
ldap_version 3
base dc=example,dc=com
nss_base_passwd dc=example,dc=com?sub
nss_base_group dc=example,dc=com?sub
nss_schema rfc2307bis
nss_map_objectclass shadowAccount posixAccount
nss_map_attribute uniqueMember member
nss_initgroups_ignoreusers root,dirsrv
nss_reconnect_maxsleeptime 8
nss_reconnect_sleeptime 1
bind_timelimit 5
timelimit 15
nss_srv_domain example.com
uri ldap://ipaserver.example.com
```

### 2.4. Configuring Kerberos
Configure the `/etc/krb5/krb5.conf` file as follows:

```conf
[libdefaults]
default_realm = EXAMPLE.COM
[realms]
EXAMPLE.COM = {
kdc = ipaserver.example.com:88
admin_server = ipaserver.example.com:749
}
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
[logging]
default = FILE:/var/krb5/kdc.log
kdc = FILE:/var/krb5/kdc.log
kdc_rotate = {
    period = 1d
    versions = 10
}
[appdefaults]
kinit = {
    renewable = true
    forwardable = true
}
```

The Kerberos configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

### 2.5. Configuring Client SSH Access

Use the following procedure to configure the Solaris IPA client to accept incoming SSH requests and authenticate with the user's Kerberos credentials. Remember to replace the example host and domain names with your own host and domain name.

The `ipa-admintools` package is not available for Solaris. Consequently, you need to perform the following steps on the IPA server.

**Procedure 3.1. To configure client SSH access:**

1. **Add a host service principal for the Solaris client.**

   ```bash
   # ipa-addservice host/solarisipaclient.example.com
   ```

2. **Create the host keytab file.**

   ```bash
   # ipa-getkeytab -s ipaserver.example.com -p
   host/solarisipaclient.example.com -k /tmp/krb5.keytab -e des-cbc-crc
   ```
3. Copy this keytab to the Solaris machine as /etc/krb5/krb5.keytab.

   # scp /tmp/krb5.keytab
   root@solarisipaclient.example.com:/etc/krb5/krb5.keytab

   **Note**
   After you have performed all of the preceding configuration steps, reboot the Solaris machine to ensure that all of the changes take effect.

2.6. Configuring NFS v4

   **Note**
   The NFS v4 configuration is only supported on Solaris 10.

Procedure 3.2. To configure NFS on the Solaris IPA client:

1. Obtain a Kerberos ticket for the admin user.

   # kinit admin

2. The ipa-admintools package is not available for Solaris. Consequently, you need to perform the following steps on the IPA server.

   a. Add an NFS service principal for the client.

      # ipa-addservice nfs/solarisipaclient.example.com

   b. Create the NFS keytab file.

      # ipa-getkeytab -s ipaserver.example.com -p nfs/solarisipaclient.example.com
      
      # klist -ket /tmp/krb5.keytab (to verify)
The Linux NFS implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the -e des-cbc-crc option to the ipa-getkeytab command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

c. Copy the keytab from the server to the client.

```bash
# scp /tmp/krb5.keytab
root@solarisipaclient.example.com:/tmp/krb5.keytab
```

3. On the IPA client, use the ktutil command to import the contents into the main host keytab.

```bash
# ktutil
ktutil: read_kt /tmp/krb5.keytab
ktutil: write_kt /etc/krb5/krb5.keytab
ktutil: q
```

The IPA client should now be fully configured to mount NFS shares using Kerberos credentials.

3. Configuring Solaris 9 as an IPA Client

Use the same configuration as that used for Solaris 10, but replace the PAM configuration with the following:

```
login auth requisite pam_authtok_get.so.1
login auth sufficient pam_krb5.so.1 use_first_pass
login auth sufficient pam_unix.so.1 use_first_pass
login auth required pam_dhkeys.so.1
login auth required pam_unix_auth.so.1
login auth required pam_dial_auth.so.1
```

4. Configuring Solaris 8 as an IPA Client

Use the same configuration as that used for Solaris 10, but replace the PAM configuration with the following:

```
login auth sufficient /usr/lib/security/pam_krb5.so
login auth required /usr/lib/security/pam_unix.so use_first_pass
login auth required /usr/lib/security/$ISA/pam_dial_auth.so.1
```
5. Testing the Configuration

Use the following tests to ensure that the configuration is working correctly:

**kinit.**
Obtain a Kerberos ticket for an IPA user.

```bash
$ kinit ipauser (provide the password when prompted)
$ klist (to verify that you received a ticket)
```

**getent.**
Run the following commands to ensure that `getent` in Solaris works with Red Hat Enterprise IPA.

```bash
$ getent passwd admin
$ getent group ipausers
```

**Console Login.**
On the system console, provide an IPA username and associated Kerberos password to log in.

**NFS v4.**
Use the following command to test the configuration:

```bash
# mount -F nfs -o vers=4 -o sec=krb5 ipaserver.example.com:/ /data
```

5.1. Troubleshooting

It is possible that the `mount` command will hang, and return the following error:

```
rpc.svcgssd[3366]: ERROR: GSS-API: error in handle_nullreq:
gss_accept_sec_context(): Unspecified GSS failure.
Minor code may provide more information - Unknown code krb5 230
```

If this occurs, try the following:

- Destroy the Kerberos cache, as follows:

  ```bash
  # rm -f /tmp/krb*
  ```

- Obtain a new keytab for the NFS service using `-e des-cbc-crc` for the IPA client.
• Obtain a new keytab for the NFS service principal with `-e des-cbc-crc` for the IPA server.
Configuring AIX as an IPA Client

This chapter describes how to configure AIX 5.3 as a Red Hat Enterprise IPA client.

1. Prerequisites

Before you begin the configuration, ensure that the following software is installed and up to date. This can be installed from your AIX media:

- v5.3 OS
- v5.3 Updates
- krb5 client packages
- openssh
- wget
- bash
- krb5 server
- ldap.client
- openssl
- modcrypt.base (for gssd)

2. Configuring Client Authentication

**Procedure 4.1. To configure client authentication on AIX:**

1. Ensure that NTP is correctly configured and enabled, and that time is synchronized between the client and the Red Hat Enterprise IPA server.

2. Edit the `krb5.conf` file as follows to configure Kerberos:

   ```
   [libdefaults]
   default_realm = EXAMPLE.COM
   [realms]
   EXAMPLE.COM = {
     kdc = ipaserver.example.com:88
     admin_server = ipaserver.example.com:749
   }
   [domain_realm]
   .example.com = EXAMPLE.COM
   example.com = EXAMPLE.COM
   ```
The Kerberos configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

### 3. Configuring Client SSH Access

You can also configure the IPA client to accept incoming SSH requests and authenticate with the user’s Kerberos credentials. After configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and domain names with your own host and domain name.

**Procedure 4.2. To configure an AIX IPA client for incoming SSH connections:**

1. **SSH syslog configuration:**

   ```
   auth.info /var/log/sshd.log
   auth.info /var/log/sshd.log
   auth.crit /var/log/sshd.log
   auth.warn /var/log/sshd.log
   auth.notice /var/log/sshd.log
   auth.err /var/log/sshd.log
   ```

2. **SSH logging configuration:**

   ```
   SyslogFacility AUTH
   LogLevel INFO
   ```

3. **Configure `sshd` for GSSAPI (`/etc/ssh/sshd_config`)**

   ```
   # Kerberos options
   KerberosAuthentication yes
   KerberosOrLocalPasswd yes
   KerberosTicketCleanup yes
   KerberosGetAFSToken no
   GSSAPI options
   ```
GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
UsePAM yes

4. Restart sshd

    # stopsrc -s sshd
    # startsrc -s sshd

5. Restart syslogd

    # stopsrc -s syslogd
    # startsrc -s syslogd

6. The ipa-admintools package is not available for AIX. Consequently, you need to perform the following steps on the IPA server.

   a. Add a host service principal for the client.

       # ipa-addservice host/ipaclient.example.com

   b. Retrieve the host keytab.

       # ipa-getkeytab -s ipaserver -p host/ipaclient.example.com -k
       /tmp/krb5.keytab -e des-cbc-crc

   c. Copy the keytab from the server to the client.

       # scp /tmp/krb5.keytab root@ipaclient.example.com:/tmp/krb5.keytab

7. On the IPA client, use the ktutil command to import the contents into the main host keytab.

    # ktutil
    ktutil: read_kt /tmp/krb5.keytab
    ktutil: write_kt /etc/krb5/krb5.keytab
    ktutil: q

8. Add a user that is only used for authentication. (This can be substituted with krb5 auth if that works from the ldap client). Otherwise go to the IPA server and use ldapmodify, bind as Directory Manager and create this user.

    dn: uid=nss,cn=sysaccounts,cn=etc,dc=example,dc=com
    objectClass: account
    objectClass: simplesecurityobject
objectClass: top
top
objectClass: nss
uid: nss
userPassword: Your own shared password here

9. On the IPA server, get a ticket for the admin user.

    # kinit admin

You should be able to log in as admin using SSH without providing a password.

    # ssh admin@ipaclient.example.com

4. Configuring System Login

No additional configuration is required to enable system login on AIX. Use the following tests to ensure that the configuration is working correctly:

On the system console, log in as an IPA user. After you have logged in, open a shell and run the following command:

    $ id (ensure that the user IDs and group IDs are correct)

If this test fails, refer to the Troubleshooting\(^1\) section in the Administration Guide for information on how to locate any problems.

---

Note

By default, the admin user is given /bin/bash as the shell to use and /home/admin as the home directory. You may need to install bash (or link sh to /bin/bash or modify admin to use /bin/sh or a shell available in all of your systems) to be able to log in.

---

Configuring HP-UX as an IPA Client

This chapter describes how to configure HP-UX as a Red Hat Enterprise IPA client. It also includes some verification tests to ensure that the configuration is working correctly.

**Note**
To install an HP-UX client you need administrator privileges in the form of the Directory Manager password. There is no other way to perform the installation.

Configuring NTP.
Before proceeding with the following configuration steps, ensure that NTP is correctly configured and enabled, and that time is synchronized between the client and the Red Hat Enterprise IPA server.

1. LDAP Client Configuration

**Procedure 5.1. To configure LDAP client authentication:**

1. Install the ldapux client on the HP-UX 11.23 machine.

   ```bash
   # swinstall -s J4269AA_B.04.15.01_HP-UX_B.11.23_IA_PA.depot
   ```

2. Change to the configuration directory and run the setup script.

   ```bash
   # cd /opt/ldapux/config/
   # ./setup
   ```

**Note**
The HP-UX guide for this procedure is located at http://docs.hp.com/en/J4269-90075/ch02s07.html

The following is a sample output from running the above script:

Would you like to continue with the setup? [Yes]
Select which Directory Server you want to connect to? [RedHat Directory]
Directory server host? [ipaserver.example.com]
Directory Server port number [389]
Would you like to extend the printer schema in this directory server? [No]
Would you like to install PublicKey schema in this directory server? [No]
Would you like to install the new automount schema? [No]
Profile Entry DN: [cn=ldapuxprofile,cn=etc,dc=example,dc=com]
User DN [cn=Directory Manager]
Password? [Directory Manager's Password]
Authentication method? [SIMPLE]
Enter the number of the hosts you want to specify [1]
Default Base DN? [dc=example,dc=com]
Accept remaining defaults? [n]
Client binding [Anonymous]
Search time limit [no limit]
Do you want client searches of the directory to follow referrals? [Yes]
Profile TTL [0 = infinite]
Do you want to remap any of the standard RFC 2307 attribute? [Yes]
Specify the service you want to map? [3=Group]
Specify the attribute you want to map? [3 for memberuid]
Type the name of the attribute memberuid should be mapped to [member]
Specify the service you want to map? [0 = exit]
Do you want to remap any of the standard RFC 2307 attribute? [no this time]
Do you want to create custom search descriptors? [No]

3. Ensure that the LDAP client daemon is running.

4. Run the following commands to ensure that the LDAP client is working:

```
# nsquery passwd admin (user should be visible)
# nsquery group admins (group and user should be visible)
```

5. Create a new group on the IPA server.

```
# ipa-addgroup testgroup
```

6. Add a test user to the new group created above.

```
# ipa-modgroup -a testuser testgroup
```

7. Run the `nsquery` commands again to validate the new user and group:

```
# nsquery passwd testuser (user should be visible)
# nsquery group testgroup (group and user should be visible)
```

This concludes the LDAP client configuration.

---

2. Kerberos and PAM Configuration

The Kerberos and PAM configuration process is completely manual. Sample configuration files are provided for reference, but you need to edit your own system files to reflect your deployment.

2.1. Kerberos Configuration

Edit the /etc/krb5.conf file to reflect the following example:

```
[libdefaults]
default_realm = EXAMPLE.COM
default_tkt_enctypes = DES-CBC-CRC
default_tgs_enctypes = DES-CBC-CRC
cache_type = 2

[realms]
EXAMPLE.COM = {
kpasswd_server = ipaserver.example.com
kdc = ipaserver.example.com:88
admin_server = ipaserver.example.com:749
default_domain = example.com
}

[domain_realm]
.example.com = EXAMPLE.COM
e.example.com = EXAMPLE.COM

[appdefaults]
kinit = {
forwardable = true
}
```

The Kerberos configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

2.2. PAM Configuration

The PAM configuration differs slightly between different versions of HP-UX. These configurations are described below.

HP-UX 11i v2.

Edit the /etc/pam.conf file to reflect the following example:

```
# PAM configuration
#
# This pam.conf file is intended as an example only.
# see pam.conf(4) for more details
```
This sample file will authenticate the user who belongs to either Kerberos or Unix system. Using this configuration file, if the user is authenticated through Kerberos then the Unix authentication will not be invoked. However, if the Kerberos authentication fails for the user, then the fallback authentication mechanism PAM-Unix will be invoked to authenticate the user. The assumption is the user is either present in Kerberos or in Unix system.

In case, the administrator wants the password for all the users to be synchronous between Kerberos and Unix systems, then the control flag should be set to "required" for all the entries with use_first_pass option set for pam_unix. If password synchronization is optional then try_first_pass option need to be set for pam_unix, so that the user can login using the appropriate passwords.

The module pam_hpsec(5) is stacked as mandatory module above all the modules for making security checks before authentication.

Authentication management

login auth required libpam_hpsec.so.1
login auth sufficient libpam_krb5.so.1
login auth required libpam_unix.so.1 try_first_pass
su auth required libpam_hpsec.so.1
su auth sufficient libpam_krb5.so.1
su auth required libpam_unix.so.1 try_first_pass
dtlogin auth required libpam_hpsec.so.1
dtlogin auth sufficient libpam_krb5.so.1
dtlogin auth required libpam_unix.so.1 try_first_pass
dtaction auth required libpam_hpsec.so.1
dtaction auth sufficient libpam_krb5.so.1
dtaction auth required libpam_unix.so.1 try_first_pass
ftp auth required libpam_hpsec.so.1
ftp auth sufficient libpam_krb5.so.1
ftp auth required libpam_unix.so.1 try_first_pass
sshd auth required libpam_hpsec.so.1
sshd auth sufficient libpam_krb5.so.1
sshd auth required libpam_unix.so.1 try_first_pass
OTHER auth required libpam_unix.so.1

Account management

login account required libpam_hpsec.so.1
login account sufficient libpam_krb5.so.1
login account required libpam_unix.so.1
su account required libpam_hpsec.so.1
su account sufficient libpam_krb5.so.1
su account required libpam_unix.so.1
dtlogin account required libpam_hpsec.so.1
dtlogin account sufficient libpam_krb5.so.1
dtlogin account required libpam_unix.so.1
dtaction account required libpam_hpsec.so.1
dtaction account sufficient libpam_krb5.so.1
dtaction account required libpam_unix.so.1
ftp account required libpam_hpsec.so.1
ftp account sufficient libpam_krb5.so.1
ftp account required libpam_unix.so.1
sshd account required libpam_hpsec.so.1
sshd account sufficient libpam_krb5.so.1
sshd account required libpam_unix.so.1
OTHER account required libpam_unix.so.1
#

# Session management
#
login session required libpam_hpsec.so.1
login session sufficient libpam_krb5.so.1
login session required libpam_unix.so.1
dtlogin session required libpam_hpsec.so.1
dtlogin session sufficient libpam_krb5.so.1
dtlogin session required libpam_unix.so.1
dtaction session required libpam_hpsec.so.1
dtaction session sufficient libpam_krb5.so.1
dtaction session required libpam_unix.so.1
sshd session required libpam_hpsec.so.1
sshd session sufficient libpam_krb5.so.1
sshd session required libpam_unix.so.1
OTHER session required libpam_unix.so.1
#

# Password management
#
login password required libpam_hpsec.so.1
login password sufficient libpam_krb5.so.1
login password required libpam_unix.so.1
passwd password required libpam_hpsec.so.1
passwd password sufficient libpam_krb5.so.1
passwd password required libpam_unix.so.1
dtlogin password required libpam_hpsec.so.1
dtlogin password sufficient libpam_krb5.so.1
dtlogin password required libpam_unix.so.1
dtaction password required libpam_hpsec.so.1
dtaction password sufficient libpam_krb5.so.1
dtaction password required libpam_unix.so.1
OTHER password required libpam_unix.so.1

HP-UX 11i v1.

Edit the /etc/pam.conf file to reflect the following example:
# PAM configuration
#
# This pam.conf file is intended as an example only.
# see pam.conf(4) for more details
#

This sample file will authenticate the user who belongs to #
either Kerberos or Unix system. Using this configuration file#
if the user is authenticated through Kerberos then the Unix #
authentication will not be invoked. However, if the Kerberos #
authentication fails for the user, then the fallback #
authentication mechanism PAM-Unix will be invoked to #
authenticate the user. The assumption is the user is either #
present in Kerberos or in Unix system. #
#
In case, the administrator wants the password for all the #
users to be synchronous between Kerberos and Unix systems, #
then the control flag should be set to "required" for all #
the entries with user_first_pass option set for pam_unix. #
If password synchronization is optional then try_first_pass #
option need to be set for pam_unix, so that the user can #
login using the appropriate passwords. #

# Authentication management
#
login auth sufficient /usr/lib/security/libpam_krb5.1
login auth required /usr/lib/security/libpam_unix.1 try_first_pass
su auth sufficient /usr/lib/security/libpam_krb5.1
su auth required /usr/lib/security/libpam_unix.1 try_first_pass
dtlogin auth sufficient /usr/lib/security/libpam_krb5.1
dtlogin auth required /usr/lib/security/libpam_unix.1 try_first_pass
dtaction auth sufficient /usr/lib/security/libpam_krb5.1
dtaction auth required /usr/lib/security/libpam_unix.1 try_first_pass
ftp auth sufficient /usr/lib/security/libpam_krb5.1
ftp auth required /usr/lib/security/libpam_unix.1 try_first_pass
OTHER auth required /usr/lib/security/libpam_unix.1
#

# Account management
#
login account sufficient /usr/lib/security/libpam_krb5.1
login account required /usr/lib/security/libpam_unix.1
su account sufficient /usr/lib/security/libpam_krb5.1
su account required /usr/lib/security/libpam_unix.1
dtlogin account sufficient /usr/lib/security/libpam_krb5.1
dtlogin account required /usr/lib/security/libpam_unix.1
dtaction account sufficient /usr/lib/security/libpam_krb5.1
dtaction account required /usr/lib/security/libpam_unix.1
ftp account sufficient /usr/lib/security/libpam_krb5.1
ftp account required /usr/lib/security/libpam_unix.1
OTHER account required /usr/lib/security/libpam_unix.1
#
3. Testing the Configuration

Use the following tests to validate the PAM and Kerberos configuration:

- On the HP-UX client machine, run `kinit admin` and enter the password.

  ```
  # kinit admin
  # klist (to verify that you received a valid ticket)
  ```

- From another Linux client machine, attempt to log in via SSH.

  ```
  # ssh admin@hpuxipaclient.example.com
  ```
  The `admin` user should be able to log in via SSH without being asked for a password.

- On the HP-UX client console, at the login prompt, enter the Administrator's login ID and password. The `admin` user should be able to log in from the console.

  **Note**

  By default, the `admin` user is given `/bin/bash` as the shell to use and
Use /home/admin as the home directory. You may need to install bash (or link sh to /bin/bash or modify admin to use /bin/sh or a shell available in all of your systems) to be able to log in.
Configuring Macintosh OS X as an IPA Client

This chapter describes how to configure Macintosh OS X as a Red Hat Enterprise IPA client. These instructions are specific to Mac OS X 10.4 (Tiger). This version of the OS includes a partial install of the Kerberos tools you need by default, especially if you perform an upgrade from 10.1 or 10.2.

Note
Before starting the IPA installation, ensure that you update the system with all the latest packages.

1. Configuring Kerberos Authentication

The current version of IPA does not provide for automatic configuration of Macintosh clients. Configuring authentication is a manual process, and is described in the following sections.

1.1. Configuring Kerberos

Configuring the Macintosh to use Kerberos for authentication with Red Hat Enterprise IPA is a two-step process: First, Kerberos needs to be correctly installed and configured, and second, the Kerberos authentication needs to be enabled.

Procedure 6.1. To configure the Macintosh to use Kerberos for authentication:

1. Ensure that /System/Library/CFMSupport/Kerberos is version 4.2 or higher. If that directory does not exist or is the wrong version, install the Kerberos Extras support.
2. Launch /System/Library/Coreservices/Kerberos
3. From the Edit menu, choose Edit Realms.
4. On the Settings tab, enter the IPA server's Kerberos realm (for example, EXAMPLE.COM).
5. On the Servers tab, leave two lines, whose hostnames you then need to replace with the IPA server's hostname (for example, ipaserver.example.com):

    kdc ipaserver.example.com 88
    admin ipaserver.example.com 749
6. On the **Domains** tab, replace the existing domains with the IPA server’s actual domain (such as example.com):

```
/example.com
example.com
```

7. Click **Make default**, and then close the Kerberos tool. This creates the files you need, but as they may not be 100% correct, it is recommended that you verify them manually.

The `/Library/Preferences/edu.mit.kerberos` file should look similar to the following. Remember to replace the example.com settings with your own IPA server name, Kerberos realm and domain details.

```
[domain.realm]
example.com = EXAMPLE.COM
.example.com = .EXAMPLE.COM

[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
forwardable = yes

[realms]
EXAMPLE.COM = {
    admin_server = ipaserver.example.com:749
    default_domain = example.com
    kdc = ipaserver.example.com:88
}
```

The Kerberos configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

### 1.2. Enabling Kerberos Authentication

You now need to modify the `/private/etc/authorization` file to allow Kerberos authentication.

**Procedure 6.2. To enable Kerberos authentication on the Macintosh:**

1. Log in as the `admin` user and launch the `/Applications/Utilities/Terminal` application.
2. Change to the `/private/etc` directory and make a backup of the existing authorization file.
3. Open the authorization file, and locate the string "system.login.console".

4. Locate the <dict> entry below this string, and then locate the <key>mechanisms</key> entry.

5. Change <string>authinternal</string> to <string>builtin:krb5authnoverify,privileged</string>

Caution
Several instances of authinternal may occur in this file. Ensure that you change the correct instance.

6. Save and close the file.

7. Restart the machine to enable Kerberos authentication.

2. Configuring LDAP Authorization

These instructions are specific to Mac OS X 10.4 (Tiger).

2.1. Creating the LDAP Configuration

Procedure 6.3. To configure the Macintosh for LDAP authorization:


2. On the Services tab, clear all checkboxes except LDAPv3 and Bonjour.

3. Select the LDAPv3 entry and click Configure.

4. Ensure the Add DHCP-supplied LDAP servers checkbox is not selected.

5. Click the arrow next to the Show Options label, and then click New.

6. Enter the Server Name (for example, ipaserver.example.com).

7. Clear the Encrypt using SSL checkbox, and then click Manual.

8. Enter the Configuration Name (for example, "IPA LDAP").
9. Ensure that the Enable checkbox is selected, and that the SSL checkbox is cleared.

2.2. Setting up the LDAP Service Configuration Options

Procedure 6.4. To configure the LDAP service configuration options:

1. Select the newly-created LDAP configuration and then click Edit.

2. On the Connection tab, specify the following:
   a. Open/close times out in: 10 seconds
   b. Query times out in: 10 seconds
   c. Re-bind attempted in: 10 seconds
   d. Connection idles out in: 1 minute
   e. Clear all checkboxes

3. On the Search & Mappings tab, specify the following:
   a. Access this LDAP server using: CUSTOM
   b. In the Record Types and Attributes panel, select Default Attribute Types, and then click Add.
   c. Select the Attribute Types option, select RecordName from the list, and then click OK.
   d. Select the newly-added RecordName attribute, and then click Add under the Map to any items in list panel.
   e. Type "uid" (without the quotes) in the text box. Click outside of the text box to set the value.

4. Add a Users record, as follows:
   a. Under the Record Types and Attributes panel, click Add.
   b. Select the Record Types option, select Users from the list, and then click OK.
   c. Select the newly-added Users record type, and then click Add under the Map to any
items in list panel.

d. Type "inetOrgPerson" (without the quotes) in the text box. Click outside of the text box to set the value.

e. In the Search base field, type "dc=example,dc=com" (without the quotes), and select the Search in all subtrees option.

5. Add attributes to the Users record as appropriate for your deployment. The following is an example of the required procedure.

a. Under the Record Types and Attributes panel, click Add.

b. Select the Attribute Types option, and then use Command-Click to select the attributes that you want to add. For example, a typical deployment might include the following attributes:

   • AuthenticationAuthority
   • PrimaryGroupID
   • RealName
   • RecordName
   • UniqueID
   • UserShell

c. Click OK to add the selected attributes to the Users record.

6. Specify appropriate mappings for the attributes that you just added. For example:

a. Select the Authentication Authority record type, and then click Add under the Map to any items in list panel.

b. Type "#;Kerberosv5::$uid$;EXAMPLE.COM" (without the quotes) in the text box. Click outside of the text box to set the value.

c. Use the same procedure to map PrimaryGroupID to gidNumber.

d. Use the same procedure to map UniqueID to uidNumber.

e. Continue until all required entries have been mapped, and then click OK.

7. Click OK finish setting up the LDAP service configuration options.
3. Configuring the LDAP Authorization Options

You now need to add the LDAP service to the list of locations used to search for user authentication information.

**Procedure 6.5. To add LDAP to the list of locations to search for authentication information:**

1. On the **Authentication** tab, change the **Search** value to **Custom path**, and then click **Add**.
2. Select the configuration that you added in the Creating the LDAP Configuration step, and then click **Add**.
3. Click **Apply** to update the LDAP configuration, and then exit the **Directory Access** application.

4. Configuring NTP

**Procedure 6.6. To configure the Macintosh to use NTP:**

- Open the Date&Time utility and point it to `ipaserver.example.com` to automatically set the date and time.

5. Accessing the IPA Server via SSH

After configuring client authentication, you should be able to use SSH to connect to the IPA server without being prompted for a password.

**Procedure 6.7. To test for correct SSH connectivity to the IPA server:**

1. Obtain a Kerberos ticket for the **admin** user.

   ```
   # kinit admin
   ```

2. If you have a valid Kerberos ticket, **SSH** should proceed with GSSAPI authentication without asking for a password:

   ```
   # ssh admin@ipaserver.example.com
   ```
6. Configuring System Login

Procedure 6.8. To configure the Macintosh for IPA system login:

1. On the Macintosh login window, log in as an IPA user.
2. After you have logged in, open a terminal and run the following commands:

   $ id (ensure that the userid and groupid are correct)
   $ klist (ensure that you have a valid Kerberos ticket)

Tip

To open the Terminal application, navigate to Applications/Utilities/Terminal.app or use the keyboard shortcut Command-Shift-U. You can also drag the Terminal icon to the Dock to make it permanently available on your Desktop.
Chapter 7.

Configuring Windows as an IPA Client

This chapter describes how to configure various versions of Microsoft Windows as an IPA client. Red Hat Enterprise IPA currently supports Windows XP Pro and Windows 2000 Pro as IPA clients.

1. Configuring Windows XP Pro and Windows 2000 Pro

Procedure 7.1. To configure both XP Pro and 2000 Pro:

1. Download the MIT Kerberos 3.x package for Windows to a known location, and then run the kfw-3.x-exe you downloaded to start the MIT Kerberos Installation Wizard.

2. Read the license agreement and then click I Agree to accept the agreement.

3. Ensure you choose to install KfW Client; the other components are optional.

4. Accept the default destination path.

5. Select Download from web path, and enter the following URL:

   http://<your IPA server's fully-qualified domain name>/ipa/config/

6. Select Autostart the Network Identity Manager each time you login to Windows.

7. Click Install to begin the installation. When the installation is complete, click Finish to exit the Wizard.

8. Edit the hosts file and add the IPA server. For example:

   <numerical IP address> ipaserver.example.com ipaserver

   Depending on the version of Windows, the HOSTS file could be located in different directories. For example:

   - Windows 2000 Pro: C:\WINNT\system32\drivers\etc\n   - Windows XP Pro: C:\WINDOWS\system32\drivers\etc\n
Configuring Your Browser

Firefox can use your Kerberos credentials for authentication, but you need to specify which domains you want to communicate with, and using which attributes. Red Hat Enterprise IPA provides a script that will automatically configure Firefox on Red Hat Enterprise Linux and Fedora; for other operating systems, you need to configure your browser manually.

Procedure 8.1. To automatically configure Firefox for use with Red Hat Enterprise IPA:

1. Open Firefox, and navigate to the IPA server (use the fully-qualified domain name, for example, http://ipaserver.example.com). If this is the first time you have attempted to connect to the site, you will see the "Kerberos Authentication Failed" page.

2. Click the IPA Certificate Authority link to import the Red Hat Enterprise IPA CA into the browser.

3. In the Downloading Certificate dialog, select the required trusts and then click OK.

4. Press F5 to reload the web page, and then click Configure Firefox.

5. In the Internet Security dialog, click Allow to enable the IPA script to automatically configure the browser settings.
Figure 8.1. Importing the Red Hat Enterprise IPA CA into Firefox

If you are using an operating system other than Red Hat Enterprise Linux or Fedora, use the following procedure to configure Firefox:

**Procedure 8.2. To configure Firefox for use with Red Hat Enterprise IPA:**

1. Open Firefox, and type "about:config" in the Address Bar.
2. In the Search field, type "negotiate".
3. Ensure the following lines reflect your setup. Replace ".example.com" with your own IPA server's domain, including the preceding period (.):

```
network.negotiate-auth.trusted-uris .example.com
network.negotiate-auth.delegation-uris .example.com
network.negotiate-auth.using-native-gsslib true
```

4. • If you are configuring Firefox on Microsoft Windows, make the following changes instead:

```
network.negotiate-auth.trusted-uris .example.com
network.auth.use-sspi false
```

5. In Firefox, navigate to the IPA server (use the fully-qualified domain name, for example, http://ipaserver.example.com). Ensure that there are no Kerberos authentication errors, and that you can see and interact with the Web interface.
### Appendix A. Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>28 July, 2008</td>
<td>David O'Brien</td>
</tr>
<tr>
<td>454034</td>
<td></td>
<td></td>
</tr>
<tr>
<td>455535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>456224</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy edit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>1 May, 2008</td>
<td>David O'Brien</td>
</tr>
<tr>
<td>Created</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Bugzilla 454034
Bugzilla 455535
Bugzilla 456224