freeIPA 1.2.1

Release Notes

Latest release information for freeIPA 1.2.1

freeIPA 1.2.1 Release Notes
Latest release information for freeIPA 1.2.1
Edition 1.0

Copyright © 2008 Red Hat. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later. The latest version of the OPL is presently available at *http://www.opencontent.org/openpub/*.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive
Raleigh, NC 27606-2072
USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park, NC 27709
USA

These Release Notes contain important information available at the time of release of freeIPA 1.2.1. Known problems, resources, and other issues are discussed here. Read this document before using freeIPA 1.2.1.

System Requirements

This section contains information related to installing freeIPA 1.2.1, including prerequisites and hardware and platform requirements.

1.1. Software Requirements

The freeIPA 1.2.1 server depends on:

- Fedora Directory Server 1.1; installed as an IPA dependency
- Fedora 9 or 10
- MIT Kerberos 1.6; typically installed as part of Fedora 9 or 10

All other IPA requirements are installed as dependencies during the IPA installation process.

1.2. Hardware Requirements

The following table lists the recommended minimum hardware required to successfully deploy freeIPA 1.2.1.

Criteria	< 250,000 Entries	250,000 - 1,000,000 Entries	> 1,000,000 Entries
CPU Type (minimum)		P3; 500MHz	
RAM (minimum)	256 MB	512 MB	1 GB
Disk Space (minimum)	2 GB	4 GB	8 GB

Table 1.1. Minimum hardware requirements for freeIPA 1.2.1.

1.3. Platform Availability

The following sections detail the various platforms and supporting technologies for which freeIPA 1.2.1 is available.

1.3.1. Server Platform Availability

freeIPA 1.2.1 is available for the following server platforms:

- Fedora 9 and 10 (i386, AMD64 and Intel® 64)
- Fedora Directory Server 1.1

  Because freeIPA 1.2.1 depends on Fedora Directory Server, you should also refer to the Fedora Directory Server Release Notes.

1.3.2. Client Platform Availability

The freeIPA 1.2.1 client is only available for the following platforms:

- Fedora 9 and 10 (i386, AMD64 and Intel® 64)
- `Solaris` 10 (x86)
- `Solaris` 8, 9, & 10 (SPARC)

- HP-UX 11i v1 & v2 (PA-RISC)
- AIX 5.3
- Mac OS X 10.4 (Tiger) (Intel)

In addition, the following platforms support the use of Mozilla Firefox™ versions 1.5, 2.0, and 3.0 to manage freeIPA 1.2.1:

- Red Hat Enterprise Linux 4.6, 5, 5.1, and 5.2 (i386, AMD64, and Intel® 64)
- Mac OS X 10.4 (Tiger) (Intel)
- Microsoft Windows Vista & XP (i386 only)

What's New in freeIPA 1.2.1?

The following are some of the most important new features in freeIPA 1.2.1. Full details are available in the product manuals, available at *www.freeipa.com/page/DocumentationPortal*[1]

2.1. Active Directory Synchronization

IPA now provides bidirectional user identity and password synchronization with Microsoft Active Directory. For this to occur, IPA employs a plug-in that extends the functionality of the Fedora Directory Server Windows Sync utility. This plug-in allows IPA to perform the data manipulation necessary to achieve synchronization between Fedora Directory Server and Windows Active Directory.

Refer to the following resources for more information on this new feature:

- Refer to the IPA Administrator's Reference for more information on the IPA Windows Sync plug-in.
- Refer to the *Red Hat Directory Server Administration Guide*[2] for more information on the Windows Sync utility.
- Refer to the IPA Installation and Deployment Guide for information on how to set up synchronization between IPA and Active Directory.

2.2. Schema Compatibility Plug-in

IPA uses the current revision of RFC 2307 to determine the representation of groups within a directory. This representation modifies the contents of a group so that it no longer contains the names of its members in the *memberUid* attribute, but rather uses the *member* attribute to list the distinguished names of the entries which represent the individual members. A client is typically expected to search the named entries to determine the names of the group's member users.

This representation is not well supported by the native LDAP client software supplied with UNIX and UNIX-like operating systems. A client that does not support reading group membership from the *member* attribute can still look up a group and read its name and ID, but is unable to see the members of the group.

An IPA server can be configured to use the Schema Compatibility Plug-in to resolve group membership at the server. The plug-in examines the group entries stored in the server and reads the distinguished names of the members of those groups. It examines the named entries and reads from them the names of the members of the group. It then uses that data to create an in-memory entry, elsewhere in the directory tree, which contains the group membership information in a form which the client can process.

[1] http://www.freeipa.com/page/DocumentationPortal

Upgrading from Previous Versions

3.1. Introduction

Upgrading to freeIPA 1.2.1 is a seamless operation that has minimal impact on a production environment. The IPA instance on the server needs to be stopped during the upgrade, and several services need to be restarted to effect all of the changes. The impact of an upgrade on IPA clients is also minimal, but varies according to the platform in question.

3.2. Upgrade Scenarios

Multiple upgrade scenarios exist, depending on your IPA deployment, but typically two primary upgrade scenarios can be identified:

- Single master with clients
- Multiple masters with clients

The upgrade process is similar in each case.

3.3. Understanding the Upgrade Process

Upgrading an IPA deployment is a multi-stage process, which consists of updating the master server and any replicas, and updating the IPA clients. You should upgrade the master and any replicas before you update any IPA clients.

Updating an IPA server is a two-step process, which consists of updating the *ipa-server* package and then running the appropriate script to perform the actual update.

Updating IPA clients consists only of updating the *ipa-client* package on those platforms that support RPM package management. Other platforms require manual updates to the necessary configuration files. These updates are described in the following sections.

3.3.1. Updating the Packages

Updated packages are released through the normal Fedora repository. Install the new packages using the **Software Updater** utility or by running **`yum update`** as the root user.

After you have installed the new packages, run the update script to effect all of the necessary configuration changes. This is described in *Section 3.3.2, “Running the Update Script”*.

3.3.2. Running the Update Script

freeIPA 1.2.1 includes an update script, **`ipa-ldap-updater`**, that you need to run on each server to apply the necessary configuration changes. The **`ipa-ldap-updater`** command reads the files in **`/usr/share/ipa/updates`** to determine what changes need to be applied.

If the update script fails for any reason, or there is an interruption to the update process, run the **`ipa-ldap-updater`** command again to restart the update process.

Note

You can pass the *-t* (test) parameter to the **ipa-ldap-updater** command to test the update without actually applying any changes. Refer to the **ipa-ldap-updater** man page for more information on the options available.

3.4. Performing the Upgrade

3.4.1. Single-Master Systems

The following procedure applies where your IPA deployment consists of a single master and any number of IPA clients.

Procedure 3.1. To upgrade IPA in a single-master deployment:

1. Download and install the updated packages using the **Software Updater** utility or by running **yum update ipa-server** as the `root` user.
2. Run the update script to apply the necessary configuration changes:

   ```
   # /usr/sbin/ipa-ldap-updater
   ```

3. Restart the IPA instance.

   ```
   # service dirsrv restart
   ```

3.4.2. Multi-Master Systems

Multi-master deployments consist of a master, one or more replicas, and any number of IPA clients. The procedure for upgrading multi-master deployments is essentially the same as for single-master deployments. Each server needs to be updated separately, using the same process.

In a multi-master upgrade scenario, no restrictions apply with respect to the order in which the servers should be upgraded. Neither is it necessary to terminate any connections between masters and replicas.

Procedure 3.2. To upgrade IPA in a multi-master deployment:

1. Identify the first server in your deployment that you want to upgrade. This can be any master or replica.
2. Upgrade the server as described in *To upgrade IPA in a single-master deployment:*
3. After you have successfully upgraded the server, proceed to the next server in your deployment, and repeat the upgrade process. Continue in this fashion until all servers have been upgraded.

3.4.3. Upgrading IPA Clients

No special procedures are required to update IPA clients. For those systems that support RPM packages, you need to download any updated packages and run the appropriate installation script.

Refer to the IPA Client Configuration Guide for information on client installation scripts.

3.5. Validating the Upgrade

When you upgrade the masters and replicas, the **`ipa-ldap-updater`** utility will display any errors that occur. If no errors are reported it means the updates were successful.

To further validate the upgrade process, you can take a "snapshot" of the database (using the **`ldap2db`** command) immediately before and after you perform the server update. Compare the two snapshots to verify that the update made no changes to the database.

Note

These validation procedures only apply to servers.

Known Issues

The following are some of the most important known issues in freeIPA 1.2.1. If applicable, supported workarounds are also described.

Bug Number	Description	Workaround
None	If you use password authentication (no GSSAPI authentication, no ticket on the client) with a new user or a user whose password has expired, you need to enable Challenge-Response authentication. Otherwise, the password changing dialog will not display. This is not enabled by default because some older SSH clients may not support Challenge-Response authentication, and it is needed only if the password is expired.	Set *`ChallengeResponseAuthentication`* to "yes" in **`/etc/ssh/sshd_config`**.
432865	Inability to handle enforced password changes using **krb5-auth-dialog.** This has been observed as a result of an uninstall and reinstall, but may also occur at other times. If a `Kerberos` dialog displays that prompts you to log in again, and this occurs at the same time that a password change is required, the `Kerberos` dialog may not be able to process the password change. It may continue to prompt you to log in again and change your password.	Log in and change the password using the **`kinit`** command from the command line.
451116	On a master-replica setup, the configuration is not yet by RANGE. It is possible for the master and any replicas to add new users with the same userid. IPA uses a plugin to solve the problem of creating unique IDs across multiple masters. It does this by ensuring that each master chooses from a different pool of IDs. This is yet to be worked into the replica creation code, and so at present masters and replicas allocate userids from the same pool. Further, the plugin does not check if the ID is already in use before allocating it to a new user.	Currently all servers try to assign IDs from 1101 up to 1,000,000,000. Before you start to use a replica, you need to change the DNA plugin configuration to use a different set of ranges. Refer to *Section 4.2, "Modifying the DNA Plug-in Configuration"* for instructions on how to update the DNA plugin configuration.

Table 4.1. Known Issues in freeIPA 1.2.1

4.1. Manually Replacing Self-Signed Certificates

Procedure 4.1. To replace the Directory Server certificate:

1. Change to the directory where the Directory Server database is located. In the following commands, the "-d ." option refers to this directory.

   ```
   # cd /etc/dirsrv/slapd-<INSTANCE>
   ```

2. Save the old database.

   ```
   # mkdir backup
   ```

   ```
   # mv *.db backup
   ```

3. Create a new database with the same password.

   ```
   # certutil -N -d . -f pwdfile.txt
   ```

4. Import the certificate from a pkcs#12 file.

   ```
   # pk12util -i <filename> -d .
   ```

5. Use the following command sequence if you need to add the CA certificate as well (for example, if it was not in the pkcs#12 file).

   ```
   # certutil -A -d . -n "CA Certificate" -t CT,, -a < <ca_filename>
   ```

6. If the CA *was* in the pkcs#12 file (it should be) you need to explicitly trust it:

   ```
   # certutil -M -d . -t CT,, -n "CA certificate"
   ```

   The nickname here may vary. To determine the nickname:

   ```
   # certutil -L -d .
   ```

Procedure 4.2. Use a similar procedure to replace the Apache certificate:

1. Change to the directory where the database is located, and make a backup as before.

   ```
   # cd /etc/httpd/alias
   ```

   ```
   # mkdir backup
   ```

   ```
   # mv *.db backup
   ```

2. Create a new database

   ```
   # certutil -N -d .
   ```

3. Press **ENTER** twice to set no password, or refer to the mod_nss documentation on how to set up the **password.conf** file.

4. Import the certificate.

   ```
   # pk12util -i <filename> -d .
   ```

5. Import the CA certificate the same way as above. The nickname "CA Certificate" is not special in any way.

Server Certificate Nicknames

The nicknames of the server certificates in both cases must be set to Server-Cert (the servers are pre-configured this way).

Use the following command to list all of your certificates:

```
# certutil -L -d .
```

```
Server-Cert u,u,u
CA certificate c,c,c
```

The server nickname in this case is "Server-Cert". You need to set the value of `NSSNickname` in **`/etc/httpd/conf.d/nss.conf`** to the same value as the server certificate nickname. If the nickname includes any spaces, you need to enclose the entire nickname in spaces for **Apache** to process it correctly.

For Directory Server, the value of `nsSSLPersonalitySSL` in the entry cn=RSA,cn=encryption,cn=config needs to be set to the nickname.

Specifying the Database Permissions

You need to ensure that the new databases have the correct permissions, as follows:

- The permissions of **`/etc/httpd/alias`** should be: root:apache mode 0640
- The permissions of **`/etc/dirsrv/slapd-INSTANCE`** should be DSUSER:root mode 0600

  where DSUSER is the login name of the user configured to run Directory Server when IPA was installed. (You can determine this by inspecting the old database.)

4.2. Modifying the DNA Plug-in Configuration

Before you start using replicas to create users and assign userids, you need to update DNA plugin configuration to ensure that each replica chooses IDs from a specific pool. For example, you need to configure the second replica to use IDs 1,000,000,001 to 2,000,000,000 and the third replica to use IDs 2,000,000,001 to 3,000,000,000, and so on.

Note

You do not need to specify these exact ranges. You can distribute ranges of IDs across replicas to best suit your deployment.

You need to change the following entries:

- dn: cn=Accounts,cn=Posix,cn=ipa-dna,cn=plugins,cn=config
- dn: cn=Groups,cn=Posix,cn=ipa-dna,cn=plugins,cn=config

For each entry, you need to change the following attributes:

- dnaNextValue
- dnaMaxValue

The following is an example ldif file that you can use to reconfigure the first replica:

```
dn: cn=Accounts,cn=Posix,cn=ipa-dna,cn=plugins,cn=config
changetype: modify
replace: dnaNextValue
dnaNextValue: 1000000001

dn: cn=Accounts,cn=Posix,cn=ipa-dna,cn=plugins,cn=config
changetype: modify
replace: dnaMaxValue
dnaMaxValue: 2000000000

dn: cn=Groups,cn=Posix,cn=ipa-dna,cn=plugins,cn=config
changetype: modify
replace: dnaNextValue
dnaNextValue: 1000000001

dn: cn=Groups,cn=Posix,cn=ipa-dna,cn=plugins,cn=config
changetype: modify
replace: dnaMaxValue
dnaMaxValue: 2000000000
```

You need to make these changes as `Directory Manager`. Assuming you save the above file as **`dna.ldif`**, you can use the following command to effect the required changes on the first replica:

```
$ ldapmodify -x -D "cn=Directory Manager" -W -f dna.ldif
```

Warning

Only execute this command with this file on the first replica. Each replica needs its own range of userids.

You should also be aware that when one master's *`dnaNextValue`* reaches the *`dnaMaxValue`* value, that master will stop servicing new IDs and user/group creation may fail. To alleviate this problem, assign a new free range to the server that depleted the ID space.

Fixed in freeIPA 1.2.1

The following are some of the most important issues that were resolved in freeIPA 1.2.1.

Bug Number	Description
431603	The **`getent group`** did not return any members on Red Hat Enterprise Linux 4 and 5. This was due to a misconfiguration in the **`/etc/ldap.conf`** file during client setup. An additional mapping has been added to this file to ensure group members are returned.
435152	Renaming groups may have led to problems with *`ACI`*s. If you renamed a group used in an *`ACI`*, the *`ACI`* itself was not updated, the result being that the group fell out of the *`ACI`* scope. IPA does not currently support per-user *`ACI`*s, so this issue only affected groups.
437566	The **`ipa-addservice`** command failed if the realm name was included in the principal name. The realm name is now silently dropped if it matches the IPA realm.
440475	The `ipa_webgui` service did not start after the initial installation. This was due to a timing issue with the creation of the **`/etc/ipa/ipa.conf`** file. This file is now created earlier in the installation process, and the `ipa_webgui` service starts as expected.
441579	On 64-bit Red Hat Enterprise Linux 5.2 systems, the *krb5libs* package did not automatically update when the *ipa-server* package was installed. Before installing the *ipa-server* package, it was necessary to manually update the *krb5libs* package.
450613	IPA does not handle group names with spaces properly. If you create a group that contains any spaces in its name, for example "Group Name", you will see a "Group show failed: Group%20Name not found" error when you try to save the group. The group was, in fact, created successfully and you can search for and find the group, add members to it and work with it normally. Each time you save the group, however, you will see the same error message.
450941	The Directory Server installation previously did not correctly detect ports that are already in use. This has been rectified.
451318	The **`ipa-moduser -f`** command may not change the appearance of the user's first name when shown as the full name. If you use the **`ipa-finduser -a`** command to search for and display a user's details after you have changed their first name, the value of *`First Name`* should be correct, but the value of *`Full Name`* might still appear as the original name.

Bug Number	Description
451358	The potential existed for Directory Server to crash if you nested groups too deeply. This was possible if you attempted to nest groups more than 19 or 20 levels deep. This has now been rectified.
468732	IPA replicas did not fully synchronize in single-master, dual-replica topology environments. This was due to replicas not being assigned unique, global replica IDs in a given topology. This has been rectified.
471940	There was a problem with the schema compat plug-in, part of the *slapi-nis* package, where a thread tried to obtain a read lock before releasing a write lock, resulting in a slapd deadlock. This was probably related to multiple plug-ins being called in the plug-in processing chain. This has now been rectified.
472107	There was a problem with the **`ipa-replica-manage`** man page and usage message, where the description of the `init` option stated that it would force a full initialization of the IPA server on HOST from SERVER, where the opposite was actually true. This has now been rectified. Running the **`ipa-replica-manage init`** command prompts for the Directory Manager password, and, if omitted, also prompts for the hostname of the master that should be initialized. This is accurately documented in the man page.
474426	There was a problem with the schema compat plug-in, part of the *slapi-nis* package, where it failed to pick up slapd internal write operations. This is required for operations such as AD winsync edits and memberof internal write operations. This has now been rectified.
474478	If you added a user to a group, and then added that group to a second group, the user only appeared in the first group of which it was made a member. This was a result of the schema-compat referred memberUid mapping not working correctly. Users should appear in all groups of which they are members, either directly or indirectly. This has now been rectified.

Table 5.1. Resolved Issues in freeIPA 1.2.1

Appendix A. Revision History

Revision 1.1 10 Dec, 2008 David O'Brien *davido@redhat.com*

BZ 468788. Update list of known and resolved issues.

Revision 1.0 3 June, 2008 David O'Brien *davido@redhat.com*

Created.