Securing SAMBA with IPA

A Bit of History

Central authentication and identity management has been something that has been nearly impossible to achieve within most companies. It could be related to history, where every vendor and brand used it's own proprietary solutions, hoping to tie customers to their products.

Kerberos and Directories

In the early 1980's, Kerberos was developed as part of project Athena at MIT (Massachusetts's Institute of Technologies) which goals were to unify the various operating systems that MIT had acquired.
Ironically, the non-proprietary X.400 and X.500 standards that were developed also around the same time by two collaborating organisations, ITU and ISO, resulted in the widely accepted LDAP server. Today, the combination of Kerberos and LDAP forms the basis of the best central authentication and identity management solutions available, such as Red Hat Enterprise IPA.

Samba

Samba was started by Andrew Tridgell in the early 90's to mount disk space from Sun systems onto his PC using the DEC Pathworks client, which normally could only connect to VMS and Ultrix Pathworks file and printer servers.
Samba today is the standard SMB/CIFS file- and printer server and client for Linux, UNIX and other derivatives.

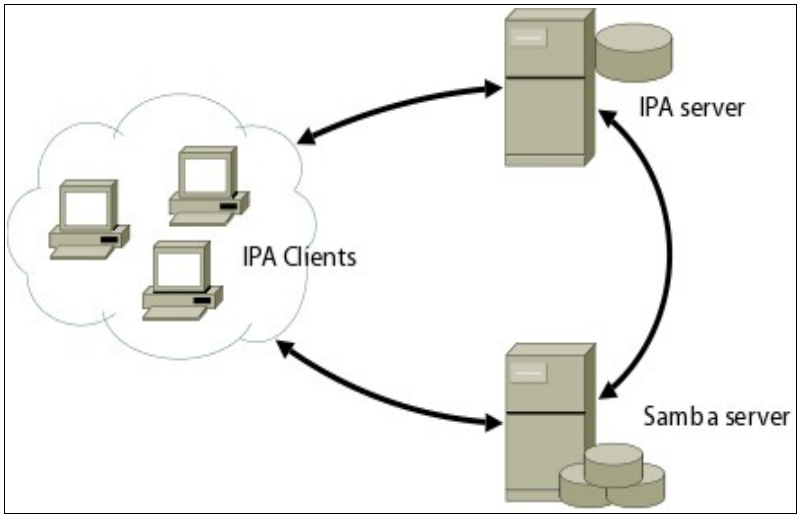
Identity, Policy, and Audit

Red Hat started the Open Source project FreeIPA, which released it's stable version 1.0 in April of 2008. FreeIPA is an integrated security information management solution, which is extremely easy to setup and use on both clients and (multi-master) servers.

FreeIPA binds together a number of technologies and adds a web interface and command-line administration tools. Version 1 supports Identity management, with Policy and Auditing management to follow in future versions.

Red Hat Enterprise IPA is the supported and quality assured version of FreeIPA, and can be obtained from the Red Hat Network.

The Recipe



As with good food, the recipe should be simple and easy to reproduce, and the cooking should be prepared well. The ingredients you need are entries in your DNS, an IPA server, an IPA client, and a Samba server. The whole trick is that the Samba server will also be an IPA client. You could install the IPA server, client, and Samba server onto one or two systems, but that would not make much sense from a network point of view. Since this paper is meant for both Free IPA on Fedora 9 and Red Hat Enterprise IPA on Red Hat Enterprise Linux 5, there are just a few steps needed for the installation procedure. Since the IPA installation will modify lots of files on your systems, it is advised to use a fresh installation of the operating system.

IPA and the DNS system

IPA's components, such as Kerberos, rely heavily on a correct Domain Name System setup. You will have to make sure that DNS entries, both *forward* and *reverse,* for your new systems exist prior to running the IPA Server installer. For your convienience, a *zone file* for ISC Bind, the name server, will be generated by the IPA server installation program. This example zone file contains so called *DNS service records*, or *SRV* records, which the IPA clients use to find and discover the IPA servers for specific protocols, such as Kerberos and LDAP.

```
$TTL 1H
@       SOA   example.com.  root.example.com. (
        2 3H 1H 1W 1H )
                        NS     ipaserver.example.com.
ipaserver               A   192.168.1.1
samba                   A   192.168.1.2
client                  A   192.168.1.3

$ORIGIN example.com.
_kerberos               TXT EXAMPLE.COM
_ldap._tcp              SRV 0 100 389   ipaserver
_kerberos._tcp          SRV 0 100 88    ipaserver
_kerberos._udp          SRV 0 100 88    ipaserver
_kerberos-master._tcp   SRV 0 100 88    ipaserver
_kerberos-master._udp   SRV 0 100 88    ipaserver
_kpasswd._tcp           SRV 0 100 464   ipaserver
_kpasswd._udp           SRV 0 100 464   ipaserver
```

Example DNS zone file for ISC Bind

IPA Server Installation and Configuration

On your Red Hat Enterprise Linux or on Fedora 9, you can install the Red Hat or Fedora Directory Server and the IPA server in one command.

On Red Hat Enterprise Linux 5:

```
[ipaserver]# yum -y install redhat-ds ipa-server
```

On Fedora 9:

```
[ipaserver]# yum -y install fedora-ds ipa-server
```

The only thing that needs to be done now, is to provide the IPA server with information about your environment, which can be done by executing the *ipa-server-install* command on your IPA server. We use the

"*--setup-bind*" parameter, to let the installer generate the example zone file for your DNS server.

```
[ipaserver]# ipa-server-install --setup-bind

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will setup the FreeIPA Server.

This includes:
  * Configure the Network Time Daemon (ntpd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure TurboGears

Server host name []:ipaserver.example.com
The domain name has been calculated based on the host name.

Please confirm the domain name [example.com]: example.com

The IPA Master Server will be configured with
Hostname:    ipaserver.example.com
IP address:  192.168.1.1
Domain name: example.com

Please provide a realm name [EXAMPLE.COM]: EXAMPLE.COM

Directory Manager password: **********
Password (confirm): **********

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

IPA admin password: ********
Password (confirm): ********

The following operations may take some minutes to complete.
Please wait until the prompt is returned.

...
Setup complete

You can now obtain a kerberos ticket using the command: 'kinit admin'
This ticket will allow you to use the IPA tools (e.g., ipa-adduser)
and the web user interface.
```

IPA Client Installation

One of the greatest features of IPA is that when you install the IPA client, all "Kerberised" services on that client can directly use it. The only thing you need to do is tell the service that it should use Kerberos. This is the reason why we will install the IPA client onto both the client, and the Samba server. The Samba server may be a "server", but to the IPA server, it's a client.

Simply run the following commands, which will install and configure the IPA and Samba client software:

```
[client]# yum -y install ipa-client samba-client
[client]# ipa-install-client
```

Remember, the IPA client software should be installed on both your IPA client and the Samba server.

Using the IPA Web Interface

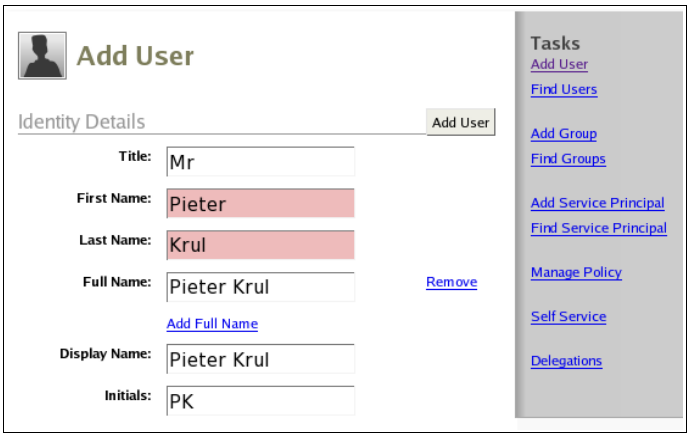
You can administer the IPA server from both server and clients, the latter being the preferred one. Before you fire up your web browser and navigate to the IPA server's web interface, you will need to follow the instructions given by the IPA server installer. This means that you will need to obtain a Kerberos ticket for the Administrative User first.

To obtain the credentials for the Administrative User, *admin*, run the following command on the IPA client:

```
[client]# kinit admin@EXAMPLE.COM
Password for admin@EXAMPLE.COM:
```

Your web browser should be able to use your Kerberos credentials for authenticating against the IPA server. Simply start for example Firefox, and navigate to the provided address, in our example *http://ipaserver.example.com.* Using Firefox version 3, you will have to add an exception to connect to the IPA web server. With he instructions and links on the web page will providecarefully, and follow them.

Adding a user to the IPA domain



To create users within your IPA domain, you can use the IPA web interface and the IPA command line tools. From the IPA web interface, select *Add User* from the *Tasks* menu. Fill in the required fields, and press the *Add User* button.
Please note that If you haven't configured automatic creation of home directories on your IPA clients, then you will have to create these home directories by hand.
The first time the user logs on to an IPA client, he or she will have to change the initial password.

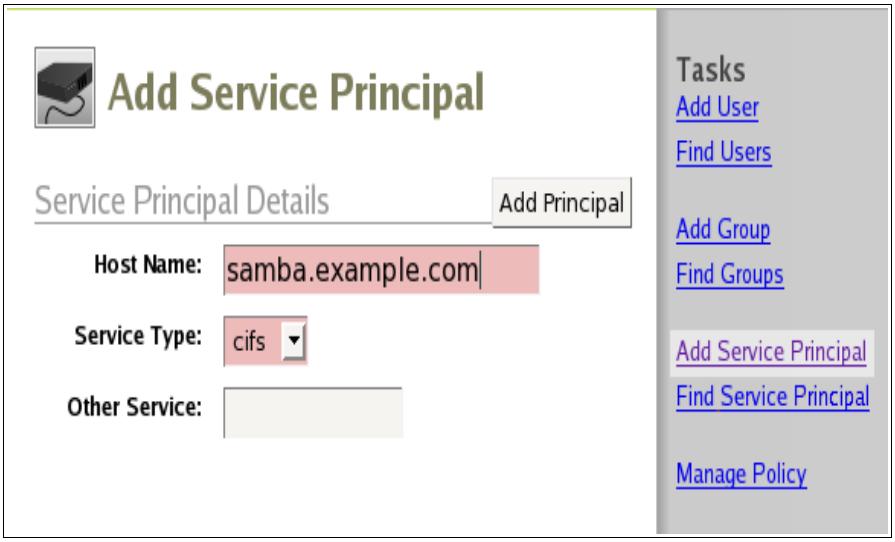
Samba Server Software Installation and Configuration

Since the IPA client software already has been installed, the only software you will need is the Samba server, which can be installed by running the following command:

```
[samba]# yum -y install samba
```

Service Principals

Using Kerberos *Service Principals* with IPA will allow your clients to obtain Kerberised access to all sorts of services, providing managed single-signon (SSO) connectivity from the clients to these services, and in this case, to Samba shares. It is also possible to add Service Principals for services such as NFS, SSH, and more.



To create the Service Principal for your Samba service from the IPA web interface, select *Add Service Principals* from the *Tasks* menu on the right-hand side of the screen.

Enter the full Host Name of your new Samba Server, including the domain name, and select *CIFS* for the Service Type.

Simply press the *Add Principal* button to add the Service Principal to the IPA server.

Creating the keytab file on the Samba server

What the Samba server needs to perform Kerberos authentication for it's CIFS service, is a so called *Kerberos keytab*. A keytab file is an encrypted, local copy of the Samba server's key from the IPA Kerberos database. Our keytab will hold the key for the CIFS service principal on samba.example.com, which we just generated in the IPA server's web interface. The default location for the keytab file on Linux systems is /etc/krb5.keytab.

From the command-line prompt of your Samba server execute the following IPA command, which will store the CIFS Service key for your Samba server in the local file /etc/krb5.keytab:

```
[samba]# ipa-getkeytab --server ipaserver.example.com –principal
cifs/samba.example.com --keytab /etc/krb5.keytab
```

Creating the Samba configuration file

The only thing that needs to be done from this point on, is that Samba needs to be told to make use of this Kerberos keytab. There are two parameters within the Samba configuration file, */etc/samba/smb.conf*, that are of special importance; "*realm*" and "*use kerberos keytab*". Please note that in this example, the Samba server is a Domain Master, and not an ADS domain member.

```
[global]
        workgroup           = EXAMPLE.COM
        server string       = Samba Server Version %v
        security            = user
        passdb backend      = smbpasswd
        socket options      = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        os level            = 33
        domain logons       = yes
        domain master       = yes
        local master        = yes
        preferred master    = yes
        wins support        = yes
        template shell      = /bin/false
        realm               = EXAMPLE.COM
        use kerberos keytab = yes
        load printers       = yes
```

```
        cups options        = raw
        log level           = 3 passdb:5 auth:10

[homes]
        comment             = Home Directories
        browseable          = no
        writable            = yes

[printers]
        comment             = All Printers
        path                = /var/spool/samba
        browseable          = no
        guest ok            = no
        writable            = no
        printable           = yes

[share]
        comment             = Share
        path                = /share
        browseable          = yes
        guest ok            = no
        writable            = yes
        valid users         = pkrul
```

After the modification of /etc/samba/smb.conf you may start, or need to restart, the Samba service

```
[samba]# service smb start
Starting SMB services:                                     [  OK  ]
```

Testing your Kerberised Samba Server

Log into your IPA client using the account you have created earlier, in this example *pkrul*. You can now use the *smbclient* command, and examine the services that are available on your Samba server. Note the "*-k*" parameter, which is needed to authenticate against the IPA server.

```
[ipaclient]$ smbclient -k -L samba.example.com
OS=[Unix] Server=[Samba 3.0.28-0.el5.8]

        Sharename       Type     Comment
        ---------       ----     -------
        share           Disk     Share
        IPC$            IPC      IPC Service (Samba Server Version 3.0.28-0.el5.8)
        testprinter     Printer  Xerox Workcenter
        pkrul           Disk     Home Directories

OS=[Unix] Server=[Samba 3.0.28-0.el5.8]
        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        EXAMPLE.COM          SAMBA
```

You can also build an FTP-like remote connection to the Samba server with *smbclient* from the IPA client, and while connected, you can examine the status on the Samba server with the *smbstatus* command.

```
[ipaclient]$ smbclient -k //samba.example.com/share
OS=[Unix] Server=[Samba 3.0.28-0.el5.8]
smb: \>
```

```
[samba]# smbstatus
Processing section "[homes]"
Processing section "[printers]"
Processing section "[share]"

Samba version 3.0.28-0.el5.8
PID     Username      Group         Machine
-------------------------------------------------------------------
22056   pkrul         ipausers      192.168.1.222 (192.168.1.222)

Service      pid     machine       Connected at
-------------------------------------------------------
share        22056   192.168.1.222  Thu Jul 10 10:08:57 2008

No locked files
```

The Samba log file should also display entries of your attempts to connect to the Samba services:

```
[samba]# view /var/log/samba/smbd.log
[2008/07/10 10:07:55, 3] libads/kerberos_verify.c:ads_keytab_verify_ticket(144)
  ads_keytab_verify_ticket: krb5_rd_req_return_keyblock_from_keytab succeeded for
principal cifs/samba.example.com@EXAMPLE.COM
[2008/07/10 10:07:55, 3] smbd/sesssetup.c:reply_spnego_kerberos(321)
  Ticket name is [pkrul@EXAMPLE.COM]
```

Related links and documentation

- http://www.freeipa.org – The Free IPA project home page
- http://www.redhat.com/enterprise_ipa – The Red Hat Enterprise IPA product page
- http://www.redhat.com/docs/en-US/Red_Hat_Enterprise_IPA – The Red Hat Enterprise IPA manuals
- http://www.samba.org – The Samba Project home page