FreeIPA Training Series

FreeIPA v3: Trust

Basic trust setup

Sumit Bose

January 2013

How to set up trust between FreeIPA and AD

- Enable FreeIPA for Trust
  # ipa-adtrust-install
- Add Trust to AD
  # ipa trust-add ...

Of course there are a number of requirements ...

Before you enable FreeIPA for Trust

- It is highly recommended to use the internal FreeIPA DNS service
- Check installed Samba packages
  - Trust requires Samba4
  - Some platforms offer Samba3 and Samba4
  - Uninstall all Samba3 packages to avoid conflicts
- Install ipa-server-trust-ad on all your FreeIPA servers

Plan DNS integration

- DNS is the cornerstone for FreeIPA and Windows to discover services in the local and remote domains
- For trust, different DNS zones for FreeIPA and Windows are needed
- Delegation is preferred for production environments
- Conditional forwarding useful for test environments

Q&A for ipa-adtrust-install

Q&A for ipa-adtrust-install

- What is a NetBIOS name and why do I need it?
  - It's a short version of the domain name
  - It's used by various protocols needed by Windows to manage trusts
  - It must be unique (like the DNS domain name)
  - It's automatically generated by ipa-adtrust-install

Q&A for ipa-adtrust-install

- Do I want to use –no-msdcs?
  - No!
  - The special service records should always be created
  - Otherwise they must be managed manually in a different DNS server (see man page and command output)

Q&A for ipa-adtrust-install

- What is a RID base and why do I need two of them?
  - On Windows, users and group are identified by unique Security Identifiers (SID)
  - A SID for a user or a group is build with the domain SID and a Relative ID (RID)
  - A RID is an unsigned 32bit integer
  - FreeIPA UIDs and GIDs must be translated into SIDs:
    - RID = RID-Base + (ID – Base-ID)
  - Since a UID and a GID can have the same value, a second base is needed to avoid conflicts

Q&A for ipa-adtrust-install

- Why is the admin password needed?
  - After ipa-adtrust-install is run, the FreeIPA KDC will add a PAC to the Kerberos tickets
  - The PAC is needed to successfully run 'ipa trust-add ...'
  - Ipa-adtrust-install reinits the admin Kerberos tickets to make sure the admin does not forget it

Q&A for ipa-adtrust-install

- Why is –add-sids not enabled by default
  - --add-sids starts a Directory Server task to add SIDs to all user and group objects
  - The new attributes must be sent to all replica servers
  - With many users, groups and replica servers; the network traffic might lead to temporary performance degradation
  - Directory Server task should be started manually for active production environments (see next slide)

Q&A for ipa-adtrust-install

- How do I start the add-sids Directory Server task
  - Copy /usr/share/ipa/ipa-sidgen-task-run.ldif
  - Edit nsslapd-basedn and delay:
    - nsslapd-basedn
      - Use value returned by
        'grep basedn /etc/ipa/default.conf | cut -d= -f2-'
    - delay
      - 0 = maximum speed and high CPU and network load
      - Positive integer value, reduced load and speed
  - (as root) ldapmodify -H ldapi://... -f your_copy.ldif

Q&A for ipa-adtrust-install

- Do I have to run ipa-adtrust-install on all replicas?
  - Yes
  - To avoid bottlenecks and single-point-of-failures, ipa-adtrust-install must currently be run on all replicas
  - More flexible setups are planned for future versions
  - If clients connect to a replica where ipa-adtrust-install wasn't run, external users cannot be resolved
  - Ipa-adtrust-install is never run automatically; it must always be run manually

Q&A for ipa trust-add

Q&A for ipa trust-add

- Do I have to give a trust-secret?
  - No!
  - The –trust-secret option allows to create only the local part of the trust
  - With Windows 2003 (not supported by FreeIPA) it was possible to create the local part of the trust on Windows as well
  - Current Windows versions do not offer to create the local part of the trust with a shared secret

Q&A for ipa trust-add

- What is an ID range?
  - ID ranges are used:
    - to reserve POSIX ID for users and groups from a specific domain
    - to map users and groups from AD domains to a POSIX IDs
  - ipa trust-add will find a suitable range automatically
  - Must be only used manually if a specific range should be used, e.g. when migrating from a different product

Q&A for ipa trust-add

- Do I have to validate the trust from the Windows side?
  - No, validation is done by ipa trust-add
  - Nevertheless, it is an easy way to check if all is working on the Windows side

Q&A for ipa trust-add

- ipa trust-add was successful, but getent passwd does not return external users what do I miss?
  - Winbind is used behind the scenes on the FreeIPA server to lookup up users in trusted AD domains
  - Winbind has a 5 minute time-out before updating the list of trusted domains (winbind cache time in smb.conf)
  - Restarting winbind is the workaround for the impatient

Adding external user to local groups

Adding users from trusted domains to local groups

- Create a group for external users
  - ipa group-add –external gr_ext
- Add external users or groups
  - ipa group-add-member –external 'ADDOM\user' gr_ext
- Add group for external users to a local group
  - Ipa group-add-member –groups=gr_ext local_group
- If the local group is used e.g. in a HBAC rule the rule applies to the remote users as well
- If the local groups is a POSIX group, the remote user will be a member of this POSIX group

Q&A External users and local groups

- Why do I need a special group for external users?
  - Only objects managed by FreeIPA can be a member of an FreeIPA group
  - External users and groups must be associated with an object manages by FreeIPA first
  - Groups created with ipa group-add –external used for this

Q&A External users and local groups

- Can I add external users before I call ipa trust-add?
  - No!
  - The given user or group name or the SID of the external object are checked on the remote server
  - Since AD in general does not allow anonymous access, this can only be done if the trust is established

Q&A External users and local groups

- What are the strange S-1-5-21-... strings listed as 'External member' by ipa group-show?
  - They are the SIDs of the external users and groups
  - SIDs are unique and cannot be changed and therefore used to reference an external object
  - Future versions of FreeIPA might translate the SIDs to the names of the external users and groups

Q&A External users and local groups

- Why does 'getent group local_group' not show external user ADDOM\XYZ?
  - The full group membership of an external user is only evaluated when the user logs in
  - Full group membership of an external user is not stored on the server but only cached on the client
  - The full group membership of an external user can be found in the PAC of the Kerberos ticket
  - Sorry, currently there is no tool which can display the PAC in tickets stored in the credential cache

SSH access with users from trusted domains

SSH access with users from trusted domains

- Putty is a widely used SSH client for Windows
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
- There are customized versions by Quest and Centrify

Q&A SSO with putty from Windows

- SSO with putty does not work; what am I doing wrong?
  - The fully qualified host name must be used
    - To find the matching Kerberos service ticket the host name entered in putty's 'Host name (or IP address)' field is used
  - User principal name (UPN) or Down-Level Logon Name should be used
    - Both standard Windows name types[1] are supported
      - UPN: username@domain.name
      - Down-Level Logon Name: DOMAIN\username
- Remember to save the session!

[1] http://msdn.microsoft.com/de-de/library/windows/desktop/aa380525(v=vs.85).aspx

Q&A SSO with putty from Windows

- SSO with putty does not work; what am I doing wrong?
  - Destination host must be able to map Kerberos UPN to POSIX user name
    - Users can create .k5login file with the UPN in their home-directory, i.e.
      - Log in with password first
      - Create .k5login file
      - Now log in with SSO
    - Admin can add auth_to_local mapping in krb5.conf:

```
[realms]
  IPA.DOMAIN = { ...
   auth_to_local = RULE:[1:$1@$0](^.*@AD_DOMAIN$)s/@AD_DOMAIN/@ad_domain/
   auth_to_local = DEFAULT
  }
```

Q&A SSO with putty from Windows

- SSO with putty does not work; what am I doing wrong?
  - If HBAC is used in the FreeIPA domain trusted users must be added to HBAC rules
    - Add user to a group for external users
    - Add this group to a local group
    - Use the local group in a HBAC rule to allow access

Q&A SSO with putty from Windows

- My credentials are not forwarded/delegated; what is missing?
  - Putty's Checkbox 'Allow GSSAPI credential delegation' must be checked
  - Windows requires the ok_as_delegate Kerberos flag in the service ticket to delegate credentials
    - On an FreeIPA server run:
      - kadmin.local -q 'modprinc +ok_as_delegate \ host/destinationhost.domain@REALM'
      - Ticket https://fedorahosted.org/freeipa/ticket/3329 ask for a better integration of Kerberos flags into FreeIPA
  - Flags can be checked with klist

Q&A SSO with putty from Windows

- Group membership of external user does not change after it was changed on the FreeIPA server; why?
  - Group memberships are extracted from the PAC of the service ticket
  - If group memberships are modified, a new service ticket must be requested to see the changes
  - Call 'klist purge' on the Windows command prompt to drop old tickets