GLOBAL CATALOG SERVICE IMPLEMENTATION IN FREEIPA

Alexander Bokovoy
Red Hat Inc.
May 4th, 2017
ABOUT:ME

Sr. Principal Software Engineer at Red Hat

• Samba Team member since 2003
• Core FreeIPA developer since 2011
WHAT IS THIS TALK ABOUT?
WHAT IS THIS ABOUT?

FreeIPA is a directory service for Linux and POSIX clients:

- 389-ds - The LDAP directory server (and a lot of plugins)
- Samba - as a traditional (NT4-style) domain controller with a twist (smbd and winbindd)
- MIT Kerberos - Kerberos KDC
- MS-KKDCP proxy
- Dogtag Certificate Authority
- Custodia (secrets management)
- SSSD - client side identity (nss, PAM, D-Bus, ...)
- FreeIPA management framework written in Python and running under Apache
WHAT IS THIS ABOUT?

FreeIPA supports forest trust to Active Directory:

• Active Directory sees FreeIPA as a "native Active Directory" deployment
• Since Samba 4.5 it is possible to establish a trust between Samba AD and FreeIPA
• Active Directory users can access resources on FreeIPA clients
• FreeIPA users cannot natively access resources in Active Directory
FreeIPA users cannot access resources in Active Directory:

- Access control in Active Directory uses SIDs of users/groups in ACLs
- "Security" tab in UI deals with user and group names
- Windows performs user or group SID lookup
- FreeIPA does not provide interfaces expected by Active Directory to perform name to SID lookups
ANATOMY OF A NAME RESOLUTION
FOUR STYLES OF CONVERSATION

Active Directory has four ways of discovering SIDs of users/groups:

• Domain controller LDAP ping allows user name validation ([MS-ADTS] 6.3.3.2 Domain Controller Response to an LDAP Ping) but doesn’t allow to discover SIDs
• DsCrackNames is part of DRSU API, Directory Replication Service of Active Directory. It is not implemented in \texttt{smbd}, only in Samba AD
• LsaLookupNames and SamLogon families of RPC calls
• LDAP queries to Global Catalog
DOMAIN CONTROLLER LOCATOR REQUEST

LDAP ping is used by all Windows clients to discover closest domain controller. As part of it clients may request a user name validation to avoid hitting domain controllers that don’t have that user replicated.
Windows UI seems to trigger CLDAP ping requests with random user names instead of the one you entered:
Windows UI seems to trigger CLDAP ping requests with random user names instead of the one you entered.
Windows UI seems to trigger CLDAP ping requests with random user names instead of the one you entered:
WHO IS ALICE?
DOMAIN CONTROLLER LOCATOR REQUEST

Alice is a fine random name, along with Marvin, Heather, Student, User2, Test, and many others seen on the wire.
The state of user inquiries in Windows is ... interesting.
If Global Catalog service is available, Windows will attempt to connect to it:
If search in a Global Catalog returns no results, Windows falls back to netr_LogonSamLogonWithFlags RPC call:
NETLOGON RESULTS

But the name passed to netr_LogonSamLogonWithFlags is totally different from what is entered in Windows UI

[2017/05/03 13:58:05.818919,  5, pid=17774, effective(0, 0), real(0, 0)] ../source3/lib/smbldap.c:1249(smbldap_search_ext: base => [dc=xs,dc=ipa,dc=cool], filter => [[(&objectClass=ipaNTUserAttr)(uid=USER))], pop_sec_ctx (99, 99) - sec_ctx_stack_ndx = 1

[2017/05/03 13:58:05.858058,  4, pid=17774, effective(99, 99), real(99, 0)] ../source3/smbd/sec_ctx.c:439(pop_sec_ctx: pop sec_ctx stack ndx = 1

check_sam_security: Couldn't find user 'USER' in passdb.

[2017/05/03 13:58:05.858119,  5, pid=17774, effective(99, 99), real(99, 0), class=auth] ../source3/auth/check_ntlm_password: sam authentication for user [USER] FAILED with error NT_STATUS_NO_SUCH_USER

[2017/05/03 13:58:05.858171, 10, pid=17774, effective(99, 99), real(99, 0), class=auth] ../source3/auth/check_auth_for: [USER]

[2017/05/03 13:58:05.858185,  3, pid=17774, effective(99, 99), real(99, 0), class=auth] ../source3/auth/check_winbind_security: Not using winbind, requested domain [XS] was for this SAM.

[2017/05/03 13:58:05.858195, 10, pid=17774, effective(99, 99), real(99, 0), class=auth] ../source3/auth/check_nlb_password: winbind had nothing to say

[2017/05/03 13:58:05.858204,  2, pid=17774, effective(99, 99), real(99, 0), class=auth] ../source3/auth/check_nlb_password: Authentication for user [USER] -> [USER] FAILED with error NT_STATUS_NO_SUCH_USER

[2017/05/03 13:58:05.858217,  5, pid=17774, effective(99, 99), real(99, 0), class=rpc_srv] ../source3/rpc_server netr_LogonSamLogonWithFlags: check password returned status NT STATUS NO SUCH USER

[2017/05/03 13:58:05.858229,  4, pid=17774, effective(99, 99), real(99, 0)] ../source3/smbd/sec_ctx.c:217(push_ctx_stack)
NAME RESOLUTION ORDER
NAME RESOLUTION ORDER

- CLDAP ping is an important operation but actual name resolution is done by querying Global Catalog
- If Global Catalog available, Windows will try to use that
- If search in Global Catalog does return no results, Windows will fall back to RPC calls
- FreeIPA does not provide a Global Catalog service
- As result, Windows does not even try to fall back to RPC calls
FREEIPA CHALLENGES
SASL GSS-SPNEGO

Samba implements own SASL code, FreeIPA components rely on Cyrus-SASL

- Cyrus-SASL GSS-SPNEGO implementation is compatible with itself, not Windows
- GSS-SPNEGO negotiates SSF based on GSSAPI flags, not separately
- This was fixed by Simo Sorce in February 2017: https://github.com/cyrusimap/cyrus-sasl/commit/67ca66685e11acc0f69d5ff8013107d4b172e67f
- No Cyrus-SASL release with the fix yet but Fedora 26 has it backported
Windows TGS-REQ requests use three-component principal names:

- ldap/host.example.com/example.com@EXAMPLE.COM
- **Real service name is** ldap/host.example.com@EXAMPLE.COM
- **FreeIPA 4.4+ added support for Kerberos principal aliases:**
  
  `ipa service-add-principal ldap/host.example.com@EXAMPLE.COM
  ldap/host.example.com/example.com@EXAMPLE.COM`
Windows always uses SASL GSS-SPNEGO for LDAP bind authentication

- Successful authentication means LDAP server needs to map authenticated identity to existing LDAP object
- There are no users or machines accounts from a trusted Active Directory in FreeIPA LDAP store
- Luckily, Global Catalog access for out-of-domain accounts is read-only
- We can map all authenticated but unknown identities to a single LDAP object with read-only rights
LDAP SCHEMA

• FreeIPA has its own LDAP schema and LDAP tree structure
• Active Directory LDAP schema is not compatible with FreeIPA LDAP schema
• Attributes and objects can be re-mapped but direct access is useless
389-DS LIMITATIONS

- 389-ds LDAP server only allows to listen on a single port per protocol
- TCP/389 for LDAP, TCP/636 for LDAPS
- Global Catalog is always TCP/3268 for LDAP access
FREEIPA GLOBAL CATALOG SERVICE
GLOBAL CATALOG SERVICE

- Runs as a separate 389-ds instance to serve port TCP/3268
- Transforms user and group data from primary FreeIPA LDAP instance to AD schema
- Access is read-only with SASL GSS-SPNEGO authentication
DATA TRANSFORMATION

• LDAP SYNCREPL is used to pick up changes from the primary FreeIPA LDAP instance running on the same IPA master
• Schema Compatibility plugin code is used to transform the changes to AD-compatible schema and DIT
• https://pagure.io/slapi-nis/
CURRENT STATE

- Design documents are available at https://www.freeipa.org/page/V4/Global_Catalog_Support
- SYNCREPL plugin almost ready
- Schema Compatibility plugin refactoring has started
- We plan to have working prototype ready for Redmond IOLab in June 2017
THANK YOU

Questions & Answers

https://samba.org/
https://freeipa.org/