FreeIPA Global Catalog challenges

Samba XP - 2020 May 27

Alexander Bokovoy
Red Hat / Samba team

Florence Blanc-Renaud
Red Hat
Who we are?

Alexander:
- Samba team member since 2003
- FreeIPA core developer since 2011

Florence
- LDAP server technology engineer since 2007
- FreeIPA core developer since 2016
Thank you all!

This work wouldn’t be possible without contribution of many engineers across multiple projects

Samba:
- Andreas Schneider
- Isaac Boukris
- Simo Sorce

389-ds LDAP server
- Thierry Bordaz
- William Brown
- Mark Reynolds
- Ludwig Krispenz

MIT Kerberos
- Greg Hudson
- Robbie Harwood
- Isaac Boukris
- Simo Sorce

and many others
Why a need for a Global Catalog with FreeIPA

Allow access to Active Directory resources for IPA users and services
Frankenstein’s Active Directory: for Linux clients, not Windows

Uses 389–ds LDAP server, MIT Kerberos, and Samba NT domain controller code base to implement what Active Directory domain controller sees as a separate Active Directory forest

- LDAP schema optimized for Linux clients and POSIX identity management use cases
  - Flat directory information tree for users, groups, and services
  - No compatibility with Active Directory schema
  - LDAP objects specific to POSIX environment use cases (SUDO rules, own access control rules, etc)

- KDC based on MIT Kerberos, native two-factor authentication and modern pre-authentication methods

- NetLogon and LSA pipes with enough support to allow AD DCs to interoperate via a forest trust

- Integrated DNS server and Certificate Authority
Global Catalog: just a LDAP server?

It is not that simple...
Global Catalog: just a LDAP server?

Global Catalog Entries

LDAP is a communication protocol designed with flexibility and extensibility in mind

- Schema:
  - Syntaxes
  - Attribute types
  - Object Classes
  - Matching rules
- Organizational structure
- Extended operations
- Extended controls
Global Catalog Schema

Subset of Active Directory LDAP schema

Incompatible with quite a few traditional POSIX LDAP schemas

dn: CN=Common-Name,CN=Schema,CN=Configuration,DC=X
objectClass: top
objectClass: attributeSchema
cn: Common-Name
distinguishedName: CN=Common-Name,CN=Schema,CN=Configuration,DC=X
attributeID: 2.5.4.3
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
1LDAPDisplayName: cn
name: Common-Name
Global Catalog Entries

Global Catalog replicates partial set of attributes for all users, groups, and machines (and more, if needed) from the whole Active Directory forest

- objectGUID
- objectSid
- userAccountControl
- sAMAccountName
- sAMAccountType
- objectCategory
- nTSecurityDescriptor
- ...

Global Catalog: just a LDAP server?
Global Catalog: just a LDAP server?

Global Catalog Organizational Structure

In Active Directory, Global Catalog service exposes users and groups in the same container, with a cn=.. naming format

Global Catalog
- dc=ad,dc=com
  - cn=users
    - cn=oneuser
    - cn=onegroup

FreeIPA primary LDAP instance
- dc=ipa,dc=com
  - cn=accounts
    - cn=users
      - uid=oneuser
    - cn=groups
      - cn=onegroup
Global Catalog Behavior

In Active Directory, LDAP server has a special handling for search filters for many attributes by allowing alternative representations of attribute values and additional matching rules

- **(objectCategory=type)**
  Handled as `(objectCategory=CN=type,CN=Schema,CN=Configuration,DC=X)`

- **(objectSID=S-1-5-21-3005052257-2375221410-442149667-1380)**
  Transformed into `(objectSID=AQUAAAAAAAUVAAAAAYXUds6IAk40jq1oaZAUAAA==)` as objectSID is an octetString

- **(member:1.2.840.113556.1.4.1941:=cn=oneuser,cn=users,DC=X)**
  Find all the groups that `oneuser` is a member of (direct or indirect membership)
Global Catalog: just a LDAP server?

Global Catalog: FreeIPA's implementation

3 main components

**Schema converter**
- Takes AD schema as input
- Maps syntaxes
- Maps matching and ordering rules
- Handles conflicts
- Outputs a 389-ds compatible schema

**Separate 389-ds instance**
- Uses ports 3268 and 3269
- GC schema
- Specific indexes
- SASL auth mapped to read-only user

**Synchronization daemon**
- Based on syncrepl (RFC 4533)
- Monitors primary LDAP instance
- Applies transformations
- Updates entries in GC
Global Catalog: demo
Global Catalog Demo

Connect as IDM user on a windows machine

- member.win2016.test is a (machine) member of win2016.test domain
- idmuser@ipa.test is a user defined in IPA
- Scenario:
  - On member.win2016.test, add idmuser to the “Remote Desktop Users” local group
  - Use `runas /user:ipa.test\idmuser whoami` to check the user can be resolved
  - Connect to member.win2016.test with rdesktop as idmuser
  - Check idmuser properties with whoami
Global Catalog Demo

Access resources as IDM user

- member.win2016.test is a (machine) member of win2016.test domain
- idmuser@ipa.test is a user defined in IPA
- Scenario:
  - On member.win2016.test, aduser allows access to his doc.txt to idmuser
  - Connect to member.win2016.test with rdesktop as idmuser
  - Edit doc.txt as idmuser
Behind the scenes

Lookup an object in Global Catalog
Translate an object name to SID
Authenticate and authorize
Kerberos extensions over trust boundary
Allow access to Active Directory resources for IPA users

Look up in IPA Global Catalog service

“Security Tab”

- To add a user to a permission, Windows client component will
  - look up a name in Global Catalog
  - Resolve name to SID via LSA call
  - Add SID to an ACL
- The connection is done as the currently logged in user
  - Must be authenticated and authorized by the remote DC (IPA master)
  - Two-way forest trust and Kerberos authentication are required
  - LSA pipe connection implies successful Samba authentication and authorization
    - Authenticated identity must have POSIX identity
    - Requested name for SID translation must make sense to Samba
Global Catalog: behind the scenes

Lookup a name in Global Catalog

Expected LDAP server extensions

- Not enough to just have the same schema
- You cannot change clients’ behavior
  - Filter rewriters
    - `objectCategory` support available in 389-ds 1.4.3.6 or later
  - `objectSID` support available in 389-ds git master now
- No support for AD-specific matching rules yet
Allow access to Active Directory resources for IPA users

Look up in IPA Global Catalog service

- Requested name to SID translation must make sense to Samba
  - For a forest lookup user or group name would be qualified with forest name instead of NetBIOS name for the forest root domain
    -IPA\admins, not IPA\admins
  - Samba will fail this lookup as it expects only NetBIOS name here

```c
lsa_LookupNames3: struct lsa_LookupNames3

handle : handle: struct policy_handle : 0x00000000 (0)

uuid : 00000000e-0000-0000-0000-1c5e-a750e5810000

num_names : 0x00000001 (1)

names: ARRAY(1)

names: struct lsa_String

length : 0x001e (30)

size : 0x0020 (32)

string : *: 0x51a0011

sids: struct lsa_TransSidArray3

count : 0x00000000 (0)

level : LSA_LOOKUP_NAMESUPLEVEL_TRUSTS ONLY2 (6)

count : 0x00000000 (0)

lookup_options : LSA_LOOKUP_OPTION_SEARCH_ISOLATED NAMES (0)

client_revision : LSA_CLIENT_REVISION 2 (2)
```
Global Catalog: behind the scenes

Authentication and authorization

Logon to Windows workstation

- Windows logon uses enterprise principal name type
  - Any UPN associated with the trusted forest would work
- Windows workstation attempts to authenticate against own DC
  - AD DC issues cross-realm client referral to IPA KDC
- IPA KDC handles AS-REQ and then TGS-REQ for cross-realm TGT back to AD
  - Windows workstation asks own DC to lookup user name to SID with LSA
    LookupNames3 call, level 6 (LOOKUP_NAMES_UPLEVEL_TRUSTS_ONLY2)
    - This call gets relayed to IPA DC for a response over the trust link
    - Same happens for the SID obtained from LookupNames3, by using LSA
      LookupSids2 request
- Actual logon process goes forward, relying on MS-PAC content of the original
  Kerberos ticket

several times

Other user

idmuser@ipa.test

Sign in to: ipa.test

How do I sign in to another domain?
Authorization

Logon to Windows workstation

- Windows requires PAC record presence in the Kerberos tickets
  - Content of PAC is important but there is a level of acceptance
- FreeIPA issues tickets with PAC for users and selected Kerberos services
  - Didn’t work for S4U2Self protocol transition over trust
  - Still issues with MIT Kerberos and User-to-User authentication
- KERB_VALIDATION_INFO (INFO3 structure) needs to be properly set up
  - Logon time must be set to a reasonable value (or a password reset will be recommended by Windows)
  - Group membership should include also a primary group
  - Optional but expected: extra SIDs should encode asserted identities
- UPN_DNS_INFO buffer has to exist
Kerberos extensions over trust boundary

- Windows applications rely on S4U extensions
  - A lot: workstation to workstation requests, remote terminal access, security token refreshes
- S4U2Proxy delegation is supported in FreeIPA
- Constrained delegation support added in MIT Kerberos 1.18
  - Not integrated yet in FreeIPA
- S4U2Self
  - Recently fixed in FreeIPA for cross-realm operations
  - User-to-User still fails when aliases are used in the second ticket (remote terminal access)
- No support for claims yet
Future plans

- Add group lookup support in FreeIPA PASSDB module
- Add group lookup support to tdbsam and tests to Samba to allow lookup of groups via PASSDB
- Complete 389-ds support for matching rules required by Active Directory clients
- Fix principal aliases lookup in MIT Kerberos
  - Needed for MIT-based Samba AD DC as well
- Teach SSSD to use IPA global catalog when trust is between IPA and IPA domains
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.