Samba as the default directory

Rethinking our Identity Infrastructure

William Brown
Senior Software Engineer
SUSE Labs Australia
ldapwhoami -D CN=William

- displayName: Firstyear
- o: SUSE Labs
- c: Australia
- st: Queensland
- memberOf: O=389 Directory Server
- drink: Iced Coffee
- mail: wbrown@suse.de
- preferredTimeZone: UTC+10:00
Progression of Servers
So how are people approaching this?
So how are people approaching this?
So how are people approaching this?

SAML
Where do we fit in?
How should we think about this problem?

- Humans and people at every level
- Psychology and behaviours of people

- SSH keys are paramount
- Fits well with usability

- Applications and servers are stateless
- Automation and dynamic environments

- BYOD is popular - and sometimes required
- Return of the thin client
How to achieve this with Samba?

- Samba contains an LDAP server - let's use it!
  - It’s a replicated user and group database
  - Trust is based on CA (LDAPS)
  - SSSD + LDAPS for SSH keys distribution
  - OAuth for web application integration
  - Still integrates with RADIUS + enterprise applications
  - Doesn't change our existing static integrations
Lets have some examples!

```
/usr/local/samba/bin/samba-tool domain provision
   --server-role=dc
   --use-rfc2307
   --dns-backend=SAMBA_INTERNAL
   --realm=SAMDOM.EXAMPLE.COM
   --domain=SAMDOM
   --adminpass=Passw0rd
```
Setup anonymous binding

/usr/local/samba/bin/samba-tool

  forest directory_service
dsheuristics 0000002

  --H ldaps://ldapkdc.example.com

  --simple-bind-dn='administrator@samdom.example.com'
Setup anonymous reads

```
/usr/local/samba/bin/samba-tool
dsacl set
    --objectdn=DC=samdom,DC=example,DC=com
    --sddl='(A;;RPLCLORC;;;AN)'
    --simple-bind-dn="administrator@samdom.example.com"
    --password=Passw0rd

Repeat with:
    --objectdn=CN=Users,DC=samdom,DC=example,DC=com
    --sddl='(A;CI;RPLCLORC;;;AN)'
    --objectdn=CN=Builtin,DC=samdom,DC=example,DC=com
    --sddl='(A;CI;RPLCLORC;;;AN)'
```
Configure LDAPS

Configure the files in /var/lib/samba/private and restart
Configure Schema

```bash
/usr/local/samba/bin/samba-tool fsmo show
  -H ldaps://ldapkdc.example.com
  --simple-bind-dn='administrator@samdom.example.com'
  --password=Password1
```

SchemaMasterRole owner: CN=NTDS
Settings,CN=LDAPKDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=com
Configure Schema

[global]
dsdb:schema update allowed = yes
Add Schema

dn: CN=sshPublicKey,CN=Schema,CN=Configuration,DC=adt,DC=blackhats,DC=net,DC=au
changetype: add
objectClass: top
objectClass: attributeSchema
attributeID: 1.3.6.1.4.1.24552.500.1.1.1.13
cn: sshPublicKey
name: sshPublicKey
ldapDisplayName: sshPublicKey
description: MANDATORY: OpenSSH Public key
attributeSyntax: 2.5.5.10
oSyntax: 4
isSingleValued: FALSE
searchFlags: 8

dn: CN=ldapPublicKey,CN=Schema,CN=Configuration,DC=adt,DC=blackhats,DC=net,DC=au
changetype: add
objectClass: top
objectClass: classSchema
governsID: 1.3.6.1.4.1.24552.500.1.1.2.0
cn: ldapPublicKey
name: ldapPublicKey
description: MANDATORY: OpenSSH LPK objectclass
ldapDisplayName: ldapPublicKey
subClassOf: top
objectClassCategory: 3
defaultObjectCategory: CN=ldapPublicKey,CN=Schema,CN=Configuration,DC=adt,DC=blackhats,DC=net,DC=au
mayContain: sshPublicKey

dn: CN=User,CN=Schema,CN=Configuration,DC=adt,DC=blackhats,DC=net,DC=au
changetype: modify
replace: auxiliaryClass
auxiliaryClass: ldapPublicKey
Add SSH keys

```bash
/usr/local/samba/bin/samba-tool
  user edit william
    -H ldaps://ldapkdc.example.com
    --simple-bind-dn='administrator@samdom.example.com'

objectClass: ldapPublicKey
sshPublicKey: ecdsa-sha2-nistp521 AAAA.....
```
Configure SSSD - Part 1

```ini
[domain/samdom.example.com]
ignore_group_members = False

cache_credentials = True
id_provider = ldap
auth_provider = ldap
access_provider = ldap
chpass_provider = ldap
ldap_search_base = dc=example,dc=com

# This prevents an infinite referral loop.
ldap_referrals = False

# Enable AD UUID -> Uid mapping
ldap_id_mapping = True
ldap_schema = ad
```
Configure SSSD - Episode 2

# Rather that being in domain users group, create a user private group
# automatically on login.
# This is very important as a security setting on unix!!!
# See this bug if it doesn't work correctly.
# https://pagure.io/SSSD/sssd/issue/3723
auto_private_groups = true

ldap_uri = ldaps://ldapkdc.example.com
ldap_tls_reqcert = demand
ldap_tls_cacert = /etc/pki/tls/certs/ad_ldap.crt

# Workstation access
ldap_access_filter = (memberOf=CN=Workstation Users,CN=Users,DC=example,DC=com)
Configure SSSD - The Finale

ldap_user_member_of = memberof
ldap_user_gecos = cn
ldap_user_uuid = objectGUID
ldap_group_uuid = objectGUID
# This is really important as it allows SSSD to respect AD account locking
ldap_account_expire_policy = ad
ldap_access_order = filter, expire
# Setup for ssh keys
ldap_user_ssh_public_key = sshPublicKey
# This is required for the homeDirectory to be looked up in the sssd schema
ldap_user_home_directory = homeDirectory

[sssd]
services = nss, pam, ssh, sudo
config_file_version = 2

domains = example.com
[nss]
homedir_substring = /home
Configure SSH

/etc/ssh/sshd_config

    AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys
    AuthorizedKeysCommandUser nobody

test:
    /usr/bin/sss_ssh_authorizedkeys <username>
Keycloak / Ipsilon
What really underpins all of this?

- Simple and generic will always win
- Psychology and human interaction design principles
- Empathy for our users and admins
Future?
Future
Touch ID is ready. Your print can be used for unlocking your iPhone.
What is next for OpenSource IDM?
wbrown@suse.de