

# Polishing Active Directory Integration

Stef Walter, Red Hat

My name is Stef Walter. I work at Red Hat.

- \* I'm interested in making stuff just work.

- \* On Linux we have so many great projects. People doing amazing work. Boggles the mind.

- \* But often people don't take the time to do the last little bit of work and make glue it all together, polish stuff, and just work out of the box.

- \* Latest thing I've been helping polish is Active Directory authentication support in Linux.

**Polishing = Tough**

- \* Polishing anything is tough.
- \* Polishing software doubly so.
- \* You have to go through and fix awkward stuff in various projects.
- \* Contribute everywhere.
- \* You have to make sure defaults work well.
- \* People need to get installed/started with things without a big learning curve.



Not really like this



It's more like this



**The Use Case is King**

- \* You have to examine how you want a feature to look from the top down.
- \* What the experience should be.
- \* "How will someone use this thing."
- \* Then go through and polish all the various components to achieve that.
- \* This is top down.
- \* Obviously not everyone can develop completely driven by use cases.
- \* Eg: some people have to worry about doing security right.
- \* In security in fact most people are taking that approach.
- \* So I don't feel bad concentrating on the use cases knowing that bottom up is covered.

Use case: **Large deployment**

- \* Deploying tens to hundreds of servers
- \* Administrators don't want to have to flit around like a bee from machine to machine.
- \* Bring up a new machine already joined to the directory.

Use case: **Personal laptop/workstation**

- \* Bringing a laptop into an environment, and using your domain account on it.
- \* If domain policy allows, does not need administrator involvement.

Use case: **Server management**

\* Remotely connect to a server and configure Active Directory there.





**Active Directory:** the empire

- \* Active Directory is hard to ignore. Although in the Linux world some people pretend that is possible
- \* In my integration work, sometimes people balk about integrating with it, but it's vital.

# **Active Directory**

the most used domain

- \* Active directory is everywhere.
- \* It's not something we're getting away from.

**Active Directory**  
but not the only one

- \* But there are also other directory systems and we need to treat them equally.
- \* So just as a disclaimer this integration works with other systems like FreeIPA and so on.

**CLI**

**CIM**

**GNOME**

dbus

dbus

dbus

**Kickstart**

**realmd** the configuration service

configures

joins

**PAM**

**nsswitch**

**winbind**  
or  
**sss**

the AD Client

kerberos

ldap



**Active Directory**

- \* Polishing is tedious. You end up touching lots of various pieces.
- \* Here are some of the pieces that we polished when working on this project.
- \* I'll talk about several of these.
- \* If you have questions about how these interact then, I'd be happy to go into more detail.
- \* Just interrupt me.



**winbind, sssd**

the AD clients

- \* Makes the users and groups available on the local machine
- \* Authenticates users against the directory
- \* sssd does more than just AD so it's a handy when that's desirable
- \* solid solutions way better what came before

**pam\_krb5, pam\_ldap**

bad AD clients

broken security more often than not

- \* If you can hijack DNS or DHCP on the network you can log into any machine using pam\_krb5 unless it's very tediously configured.
- \* Even if tediously configured, not all applications can use it.
- \* No need to integrate with every possible configuration



**Removing needless obstacles**

- \* Security may always be an obstacle in some way. That's just reality.
- \* But not all obstacles represent security.
- \* Some are just plain dumb needless obstacles.



**Kerberos:** no mo' clock skew

- \* Kerberos historical problem.
- \* If you're going to design a protocol, don't make it depend on clock syncing.
- \* If syncing clocks was a security feature, it's almost never done securely, especially when joining a domain.



# Clock time becomes a nonce

Kerberos with clocks adrift:

[http://static.usenix.org/publications/compsystems/1996/win\\_davis.pdf](http://static.usenix.org/publications/compsystems/1996/win_davis.pdf)

It turns out this obstacle is not a security feature.

Finished implementing this in MIT kerberos

The preauth response returns the server time, we send that back to the server

**krb5:** no reverse dns  
reverse dns is usually wrong  
canonizing host names via dns is insecure

Again an obstacle that's not a security feature  
Configuration is still possible. But don't assume you need it, and  
don't assume that your config won't be broken.

**Use DNS to find KDC's**  
and site discovery, when necessary

# **Kerberos: many more tweaks**

Descriptive messages, many other bugs fixed, etc.

- \* Worked on making active directory password policy messages show through
- \* Fixed lots of bugs related to keytabs, corner cases, and stuff that nobody should ever have to care about.

# realm

the configuration service



\* Realmd configures your machine to be part of a domain like Active Directory.

realmd: it's on de bus



\* It's an autostarted Dbus service, comes and goes away as needed.

## Part II. Developer Reference

### Table of Contents

#### DBus Interface Reference

[org.freedesktop.realmd.Provider](#) — a realm provider

[org.freedesktop.realmd.Realm](#) — a realm

[org.freedesktop.realmd.Kerberos](#) — a kerberos realm

[org.freedesktop.realmd.KerberosMembership](#)

[org.freedesktop.realmd.Service](#) — the realmd service

#### Raw DBus Interfaces

---

- \* Documented DBus API
- \* This is the real interface to realmd
- \* Many things integrate with this API



**realmd does auto discovery**

# Active Directory discovery

- \* Resolving: \_ldap.\_tcp.dc.\_msdcs.borg.thewalter.lan
- \* Sending MS-CLDAP ping to: 10.34.36.170
- \* Sending MS-CLDAP ping to: 10.34.4.130
- \* Successfully discovered: borg.thewalter.lan

- \* Detects Active Directory by looking at DNS records
- \* Also supports looking up servers directly



# FreeIPA discovery

- \* Resolving: `_ldap._tcp.dc._msdcs.gorn.thewalter.lan`
- \* Resolving: `_ldap._tcp.gorn.thewalter.lan`
- \* Performing LDAP DSE lookup on: `10.38.48.1`
- \* Performing LDAP DSE lookup on: `10.38.48.3`
- \* Successfully discovered: `gorn.thewalter.lan`

\* Detects FreeIPA by connecting to LDAP and doing lookups

root@stef-redhat:~

File Edit View Search Terminal Help

[root@stef-redhat ~]# █

I

**joins domains with no muss no fuss**

(muss, fuss, diagnostics available on request)

**Uses other components to do join**

samba, ipa-client-install, adcli

**Can install needed packages**  
with PackageKit

```
root@stef-redhat:/data
File Edit View Search Terminal Help
server-software: active-directory
client-software: winbind
type: kerberos
realm-name: BORG.THEWALTER.LAN
domain-name: borg.thewalter.lan
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]# realm discover
realm: No default realm discovered
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]# realm join borg.thewalter.lan
Password for Administrator:
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]# getent passwd 'BORG\Fry'
BORG\fry:*:1344601112:1344600513:Philip J. Fry:/home/BORG/fry:
[root@stef-redhat data]#
[root@stef-redhat data]#
[root@stef-redhat data]# realm leave
Password for Administrator:
```

command line interface

"Look ma, no reboots"



\* Not rebooting is important because stuff using realmd wants to do stuff after joining a domain

Use case: **Large deployment**







**Kickstart** with one time passwords

```
%packages
samba-common
samba-winbind
%end
authconfig --update --kickstart --enablewinbind --enablewinbindauth
--smbsecurity=ads --smbworkgroup=[WORKGROUP] --smbrealm=[DOMAIN]
--smbservers=[SERVER] --winbindjoin=[ADMIN]%[PASSWORD]
--winbindtemplatehomedir=/home/%U --winbindtemplateshell=/bin/bash
--enablewinbindusedefaultdomain --enablelocauthorize
--enablewinbindoffline --enablemkhomedir
```

**becomes:**

```
realm join --one-time-password=xxx domain.com
```

als  
ounts

 hendrix	Computer
 kickstart	Computer
 LIVE-USER	Computer
 stef-live	Computer
 stef-redhat	Computer
 stef-ubuntu	Computer
 test	

### Active Directory Domain Services



Are you sure you want to reset this computer account?

Yes

No

- \* You can reset accounts in order to make this work.
- \* Not super secure

# Tool for setting up one time password:

```
$ adcli preset --domain=mydomain.com  
              --one-time-password="blah"  
host1.mydomain.com host2.mydomain.com ...
```


\* You have to preset accounts to do this.



Use case: **Personal laptop/workstation**

# User Accounts



 Lock

## My Account



**Stef Walter**

stef

## Other Accounts



**Turanga Leela**

BORG\leela



**Turanga Leela**

Account Type Standard

Language Unspecified [ANSI\_X3.4-1968]

## Login Options

Password ●●●●●

Use case: **Server management**

**OpenLMI provider** for realmd  
aka CIM

File Edit View Search Tools Documents

60\_LMI\_Realmd.mof x realmd-talk.pin x

```
1 [ Description (
2   "Access to the Realmd Service. "
3   "Realmd is used to discover realms available for joining as well as "
4   "providing a mechanism for joining and leaving a realm."),
5   Provider("cmpi:cmpiLMI_Realmd") ]
6 class LMI_RealmdService : CIM_Service
7 {
8   [Description (
9     "The name of the domain that this computer is a member of "
10    "or NULL if not a member of any domain.")]
11   string Domain;
12
13   [Description (
14     "Join the computer to a domain.")]
15   uint32 JoinDomain(
16     [In, Description (
17       "The name of the domain to join.")]
18     string Domain,
19     [In, Description (
20       "The administrative user who is authorizing joining the domain. "
21       "Or NULL for a one time password based join.")]
22     string User,
23     [In, Description (
24       "Either NULL for an automatic join, a one time password, or the "
25       "password for the administrative user in the User parameter.")]
26     string Password,
27     [In, ArrayType ( "Indexed" ), Description (
28       "This array is correlated with the OptionalValue array. "
```

# **adcli**

a simple lightweight AD command line tool

Uses kerberos and OpenIdap (CLDAP too)





**Samba:** sharing components  
components that can be used on their own  
pretty please :)

**More to come!**

More to come with Active Directory integration

Talk a bit about the concept of central management and representing that effectively.



<http://freedesktop.org/software/realmd>

Credits: <http://flickr.com/photos/oliharwood/>  
<http://flickr.com/photos/25477528@N00/>  
[http://flickr.com/photos/thomas\\_hackl](http://flickr.com/photos/thomas_hackl)  
<http://flickr.com/photos/Somma>  
Done in pinpoint