Active Directory integration with Linux

Tips and tools, including PowerBroker (PBIS).

See also

- Mac OS Installation
- Configuring restricted user folders on file share folders

Summary table of options

Method	Pros	Cons	How-to summary	Notes
PBIS Open (free app)	Automatic configuration. No CU AD change required.	Rare NetID name conflicts visible in UI (does not affect operational use).	Use app's GUI- easy! (is this correct?!)	Method preferred by Chemistry IT
SSSD - System Security Services Daemon https://fedorahosted.org/sssd/	The CIT-approved method. No NetID name conflicts.	Manual configuration. CU AD change requires coordinating CIT making changes within AD Q: What of person using Linux accounts within two departments, with only one NetID, thus only one CU AD entry?	(need this!)	Method preferred by CIT and Biotech IT.
winbind	No CU AD change required. No NetID name conflicts.	Manual configuration.	(need this!)	Anyone prefer this method?

PowerBroker (PBIS)

12/3/13:

- The educational server pricing for the "Enterprise" version is $239 and $47.80 for the annual support.
    - The "Open" version is free.
- PBIS Open/Enterprise comparison document.

Oliver's understanding about this software: The free ("Open", vs. "Enterprise") version of BeyondTrust's PowerBroker (PBIS = PowerBroker Identity Services) tool is apparently easy to use, but presents some "name collision" issues here at Cornell for reasons the vendor couldn't explain fully. Perhaps just cripple-ware, even though their tech staff and comparison documentation (linked above) says otherwise? Their fee-based, "Enterprise" software doesn't have this behavior, I understand.

Error, and thus limitation, in source code within "Open" found

1/23/17: Chemistry IT reviewed the source code and found the source causing the rare but very real NetID collisions. Instead of 20-bits stored for the user ID, only the first 19-bits are stored. Attempts made to contact the vendor. Also, we're testing out a recompiled version we hand-corrected. (Hard and uncertain outcomes since this limitation has been hard-coded in multiple locations within the code and not abstracted to just on location.)

Chemistry IT's notes regarding alternatives we've heard about in use at Cornell

1/23/17: Some folks on campus have a Boolean value CU AD for "edsvaOIT-IsUnixEnabled" marked as "Yes".

Other resources Oliver has found or heard about

Question: What happens if that person has a *nix system in more than one department? Won't that create a collision regarding home directory storage, etc?

Integrating RHEL With Active Directory

- http://www.chriscowley.me.uk/blog/2013/12/16/integrating-rhel-with-active-directory/

Getting Control of Linux/Unix with Sudo and AD Integration

Free relevant training is offered by Randy Franklin Smith, whom I trust. Examples:

Webinar: "Configuring Linux and Macs to Use Active Directory for Users, Groups, Kerberos Authentication and even Group Policy", Tuesday, January 24, 2017 1:00 - 2:30 PM ET:

- https://www.ultimatewindowssecurity.com/webinars/register.aspx?id=1411

Webinar: "Getting Control of Linux/Unix with Sudo and AD Integration" , 5/15/2014 11:00:00 AM [(GMT-05:00) Eastern Time (US & Canada)]

- http://www.ultimatewindowssecurity.com/webinars/register.aspx?id=259

Tip: Randy encourages registering for an event even if one can't make the live event in order to receive a link to the recording.

Experiences from others on campus:

Original Message:
From: Martin Berggren [mjb43]
Sent: Friday, April 25, 2014 4:35 PM
To: Oliver B. Habicht; gaarder@math---; Martin J. Berggren
Subject: Re: FW: Getting Control of Linux/Unix with Sudo and AD Integration

Hi,

We're using Cornell AD for both authorization and authentication with some extensions through Quest for our Linux hosts. This is part of the mention that engineering is working with Moe on a project. Anyway, this means that there aren't any local accounts on the Linux hosts (RH &Ubuntu) other than the service account that we add. We wanted a way to remotely log on for when there were configuration mistakes. We're using puppet to manage our Linux systems.

martin

==========

Original Message:
From: On Behalf Of Devin A. Bougie
Sent: Thursday, April 24, 2014 3:17 PM
To: RITMG-L
Subject: Re: Getting Control of Linux/Unix with Sudo and AD Integration

Hi, All. For what it's worth, at CLASSE we're using SSSD to authenticate our Scientific Linux 6 systems with our Active Directory domain. We migrated over 200 SL6 systems over night without any reboots or interruptions in service, all using stock software provided in EL6. So far it's worked very well, other than the pain of moving from an MIT Kerberos domain to what Active Directory provides (losing support for kadmin, etc.).

We're then using Puppet for configuration management of our Windows and Linux (and eventually OS X) systems.

Devin

On Apr 24, 2014, at 11:15 AM, James I. Vanee <jiv2> wrote:
[...]
> As far as AD integration We have used PBIS (formerly likewise) but there are several problems that we live with for now but want to move. I know there are more native integrations coming from engineering in collaboration with Moe and the AD folks. maybe some of you already use that.
> I'll admit openly that we (I) do not have the discipline to manage using only sudo - I will say that living inside the managed/hosted server environment from CIT will help break old habits.