

BigGuy Corp – Multi-Login Authentication System Proposal

Made for: Ryan Lockhart, CEO

Prepared by: Ramtin Moghaddam

Table of contents:	Page:
Executive Summary	3
Problem Overview	4
Implemented Solution	5 – 6
Benefits and Drawbacks	6 – 7
Issues Encountered and Resolution Steps	8 – 10
Technical Documentation	10 - 15
Conclusion	15

Executive Summary

BigGuy Corporation has been facing operational difficulties because of the fragmented authentication systems across Windows and Linux environments; employees are facing issues with multiple login credentials which led to increasing frustration and support overhead. We were tasked with implementing centralized authentication by integrating Microsoft Active Directory (AD) with Linux systems to help enable users to log into both platforms using a single set of credentials.

The chosen solution to implement involved using Windows Server 2019 domain controller to replace the outdated Windows Server 2008, this was very important to ensure improved security and compatibility with more modern systems and also ensure that smoother integration existed with Linux clients via SSSD and Kerberos. We installed services and configured two Linux client machines and one Windows 10 client to authenticate users directly through Active Directory furthermore selective and shared login policies were also implemented for the two AD accounts that were created: shareduser (which grants universal login across all clients) and restricteduser1 (limited to specific linux systems).

This brought several benefits such as simplified user management, improved our user experience, enhanced security through centralized control, and a scalable authentication model. The solution also allows for password changes from a single location, which propagates across all client machines, this positions BigGuy Corporation for a more improved and efficient IT management moving forward in the future.

Problem overview

The core of the issue was the lack of a centralized or unified authentication for employees accessing through different systems. As stated BigGuy Corporation relied on Microsoft Active Directory meanwhile ABC Co. used OpenLDAP, and these systems were not integrated leading to users having to remember and use multiple credentials which obviously leads to further frustration and poor user experience. It also caused delay logins, increasing the risk of password fatigue, and higher reports of login failures. To address these issues, the solutions aimed to:

- . enable Linux systems to authenticate through Active Directory
- . reducing the credential redundancy across systems
- . implement selective access based on the machines and policies
- . improve the administrative control over passwords and account management which the previous system lacked in.

Implemented Solution

I used four virtual machines:

1. Windows Server 2019: Upgraded from the original Windows Server 2008 to make sure there is better compatibility and to improve our modern security standards. I installed DNS and DHCP roles as it served as our AD domain controller for the domain created called 'bigguy.local' with IP statically set to 192.168.100.10 . Two users, shareduser and restricteduser1, were created in ADUC.
2. Windows 10 Client: Used to verify that seamless domain login and password sync works from the user perspective. It's static IP was set to 192.168.100.20 with host-only networking, with it's gateway and DNS were both pointed to DC to ensure it would communicate and join the domain successfully.
3. Linux Mint 1: First client machine configured for centralized authentication. Configured with static IP 192.168.100.30 and host-only networking to communicate with DC after installing the required services with NAT networking. /etc/resolv.conf was updated to use my DC's IP (192.168.100.10).
4. Linux Mint 2: Same setup as Mint 1. Second Linux client to test selective user access. Its ip was statically set to 192.168.100.40. DNS was also set in /etc/resolv.conf.

On Windows server 2019, I installed and configured Linux systems with these services: realmd, sssd, krb5-user, packagekit, adcli, and oddjob. First to install these packages we used NAT networking and then switched to host-only with Static Ips to communicate with the DC (Windows Server 2019).

Each Linux client joined the AD through 'realm join' command and was configured through /etc/sss/sss.conf file where we used access_provider = simple to control which AD users were allowed on both linux machines, for example, shareduser was allowed on both Linux machines and Windows 10 meanwhile restricteduser1 was only limited to Windows 10 and Linux mint 1 but not Linux mint 2.

I also modified LightDM to use lightdm-gtk-greeter with manual login enabled because Linux mint by default does not allow typing in usernames as this ensures that we could type full AD usernames to be able to log in.

Benefits and Drawbacks

Benefits:

Unified credentials: Each user can log into both windows and Linux using their own single set of AD credentials

Centralized password changes: A single password change from AD applied successfully across all systems

Selective access control: Using sssd.conf, we could restrict certain users to specific linux machines.

Improved Security: implementing centralized authentication in turn improved our password policies and account control as they are standardized.

Scalability: The solution can be expanded to include more Windows and Linux machines or more AD users with minimal configuration

Drawbacks:

Complex Configuration: To enforce selective access policies on Linux clients it requires manual intervention, which may not scale easily in larger environments. Implementing the solution requires expertise as configuring system files and authentication settings may be non-trivial for the general support staff but this could be mitigated with following our technical documentation step by step as an guide.

Limited Linux GUI integration: Even after successful AD integration, Linux systems provide minimal graphical feedback for domain login attempts as errors are not always clearly displayed, making it difficult for users or staff to find out what's causing login failures without using command-line tools or log file analysis.

Lack of native GUI tools on Linux: Linux mint lacks built-in graphical tools to simplify the process of domain joining or AD user filtering as it requires administrators to use command-line tools and manually edit configurations files which in turn increases the risk of errors and setup complexity

Issues Encountered and Resolution Steps

- 1. Initial authentication failure on Linux Mint:** after successfully joining the domain, I still couldn't log in with the AD users via the GUI or terminal. I confirmed domain membership, and the issue persisted across the different login formats.

Upon a closer look, I determined that the login was failing because the SSSD service was rejecting access even though the authentication was successful, I found out that this was because of the default 'access_provider = ad' configuration was not permitting login unless there was a group-based access filtering configured and implemented correctly.

Logs like 'sssd_pam', 'lightdm', and 'journalctl' were analyzed repeatedly, which helped further isolate the issue and confirm that it was due to SSSD.

Resolution: I switched the 'access_provider' setting in /etc/sss/sssd.conf from 'ad' into 'simple', and specified to only allow users using the 'simple_allow_users' directive. This helped enable login functionality for AD users by bypassing the complex group membership checks that happens. (next page)

- 2. Linux Mint 2 not syncing password changes:** after changing the password for shareduser account on the domain controller, Linux mint 2 could still accept the old password, leading to inconsistent login behaviour and security concerns

I investigated and found that Mint 2 could not resolve domain queries. We used the 'nslookup bigguy.local' command and it failed with a 'SERVFAIL' response.

Resolution: edited the /etc/resolv.conf file to set the correct DNS to our domain controller's IP address, resolving and restoring resolution. After this Mint 2 was able to successfully sync with password changes from the DC.

- 3. Windows 10 accepting old password post-change:** After the password was changed from the DC (Domain controller), Windows 10 allowed login with the old password , but only for the first login as on subsequent attempts, the old password was rejected.

I found out this behaviour occurred due to Window's credential caching mechanism for offline login support.

Resolution: I disabled cache credentials by running 'reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v CachedLogonsCount /t REG_SZ /d 0 /f' , forcing windows to authenticate directly with AD each time.

- 4. Home Directory not created for new AD users:** On Linux mint 1, I first couldn't log in with shareduser or restricteduser1 despite the correct credentials and the fact that we verified domain membership.

The root cause was due to the absence of home directory for the AD account.

Resolution: I ran the command 'sudo pam-auth-update', as this would ensure that we would have a home directory created upon the first successful login for any AD user.

Technical Documentation

Windows Server 2019 Setup:

- . Set static IP of 192.168.100.10/24 or a IP of your choice.
- . Launch Server Manager and select "Add Roles and Features"
- . Proceeded through the wizard and install the following roles:
 - . Active Directory Domain Services (AD DS)
 - . DNS Server
- . After the installation of these roles you should see a notification flag in server manager, select it to promote the server to a domain controller
- . Do the following in Active Directory Domain Services Configuration Wizard:
 - . Select "Add a new forest"
 - . Name the root domain 'bigguy.local'
 - . Set the password for Directory Services Restore Mode
 - . Accept default NetBIOS name

- . review and confirm the prerequisites to make sure and then complete the promotion

- . After rebooting, open Active Directory Users and Computers (ADUC) application to create these two user accounts:

- . shareduser : granted login access to all clients
- . restricteduser1: configured for selective access

Linux Mint client setup (Mint 1 and Mint 2):

- . Switch to NAT temporarily to gain internet access to download necessary services

- . Open 'Advanced Network Configuration' application -> Edit the adapter -> Click on 'IPv4 Settings' -> click on 'method' and ensure its on 'Automatic (DHCP)' to get internet access

- . Install the required packages running the following command:

- . `sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss krb5-user packagekit adcli oddjob oddjob-mkhomedir`

- . Switch to Host-only networking and assign static Ips through Advanced Network Configuration application (edit the adapter and go to ipv4 settings as stated before and set mode to manual):

- . Linux Mint 1: 192.168.100.30
- . Linux Mint 2: 192.168.100.40
- . Set DNS to 192.168.100.10 (windows server)

- . Update /etc/resolv.conf with:

- . `nameserver 192.168.100.10`
- . `options edns0 trust-ad`

```
search bigguy.local
```

. Join domain:

```
sudo realm join -U Administrator bigguy.local
```

. Configure /etc/sss/sss.conf with the following:

```
[sss]
domains = bigguy.local
config_file_version = 2
services = nss, pam, pac

[domain/bigguy.local]
ad_domain = bigguy.local
krb5_realm = BIGGUY.LOCAL
realmd_tags = manages-system joined-with-adcli
id_provider = ad
access_provider = simple
ad_access_filter = (memberOf=CN=Domain
Users,CN=Users,DC=bigguy,DC=local)
cache_credentials = True
default_shell = /bin/bash
fallback_homedir = /home/%u@%d
use_fully_qualified_names = True
ldap_id_mapping = True
krb5_store_password_if_offline = True
simple_allow_users = shareduser@bigguy.local,
restricteduser1@bigguy.local
debug_level = 9
```

NOTE: for simple_allow_users do not include
'restricteduser1@bigguy.local' on Linux mint 2, only
[shareduser@bigguy.local](#) for Linux Mint 2 for selective access.

. Edit /etc/lightdm/lightdm.conf with the following:

```
[Seat:*]  
greeter-session=lightdm-gtk-greeter  
user-session=linuxmint  
greeter-show-manual-login=true  
allow-guest=false  
allow-user-switching=true
```

. Restart the services :

```
sudo systemctl restart sssd  
sudo systemctl restart lightdm
```

. It should log you out automatically once you restart lightdm,
confirm AD user login works by typing [shareduser@bigguy.local](#)
as username and provide the password, once it logs you in
without any error then it has worked.

. Confirm that you're in the correct AD account by opening
terminal and running:

```
klist  
whoami
```

. To test password change, go to ADUC application on the DC and
change password on AD account shareduser, hover to domain
and click on it -> click on users -> right-click on shareduser and select

reset password and provide the new password.

- . confirm new password works on all clients
- . make sure DNS is resolving correctly on linux (run nslookup bigguy.local)

Windows 10 client setup:

- . Make sure the VM is set to host-only networking just as we did with all machines
- . open search bar and type in 'View network connections' and open the setting that pops up
- . Double click on the ethernet and select properties -> select 'Internet Protocol Version 4' -> set the IP addresses to the following:
 - . IP address : 192.168.100.20
 - . Subnet Mask: 255.255.255.0
 - . Default Gateway: 192.168.100.10
 - . Use the following DNS server address: 192.168.100.10
- . Open 'system properties' -> select 'Computer name' tab -> click 'Change'
- . select domain and enter 'bigguy.local'
- . Provide credentials for the domain Administrator password when prompted
- . A welcome message should appear when you succeed, so proceed to restart the system to apply the changes

. At login screen click 'Other user' -> username :
BIGGUY\shareduser and provide the password to log into the AD
user account.

. Finally disable cached credentials to be in sync with DC when
the password changes by running the following command in
administrator command prompt/powershell:

```
. reg add "HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon" /v CachedLogonsCount /t REG_SZ /d 0 /f
```

Conclusion:

This solution helped unify authentication across Windows and Linux using Active Directory, got rid of redundant credentials, and improved our security controls. Through enforcing selective access policies and configuration of domain services, BigGuy Corporation now can benefit from having a streamlined login process and a centralized user management system furthermore the solution is also scalable and ready for future expansions.