May 02, 2019

Novel approach to store and use the rotated passwords for authentication for a privileged SSO in a distributed unsynchronized environment

Saikrushna Samal

Gulshan Vaswani

Srivathsa Rao

Novel approach to store and use the rotated passwords for authentication for a privileged SSO in a distributed unsynchronized environment

Saikrushna Samal, Gulshan Vaswani, Srivathsa Rao

Abstract

There is a feature developed which would rotate the passwords of privileged accounts. Based on an organization's compliance policy, the password rotation can be scheduled in an interval of time e.g. every 90 days or can be rotated immediately based on admin actions. As part of password rotation process, the new password is updated in the target system as well as its own primary and backup Credential Vault database. The primary credential vault synchronizes the updated password(s) to backup credential vault(s). While initiating a privileged session for an end user the invention uses the password stored in credential vault and injects in user's session for a privileged SSO to target systems.

Following explains the Password Management use case: One can grant privileged access to users either by elevating the user privilege or by providing privileged account credential for checkout. The resource and credential details that are required to provide privileged access are stored securely in the Credential Vault. The password of these credentials can be rotated periodically based on the compliance rule of the organization. The credentials that are used to perform SSO are hidden from the end users. Hence, these credentials must be rotated automatically to improve security.

In an erroneous scenario, if the password of an account is not synchronized across primary and backup vault managers, any password injection by backup vault manager would fail to authenticate against target system. As an approach to solve this, each time the password for any account is rotated a future password is also generated and synchronized across primary and backup vault managers. By default, the future password is used to set password for the account on target system whenever the password rotation schedule happens. Any access request to the target by the end user, where the account is injected by backup vault manager, the scheduled password rotation time and last time when the password was updated for the account to be injected is checked. If the current system time is WELL past the scheduled time, and password is not updated post the scheduled time, then this indicates that there is a synchronization issue and the future password is injected for providing privileged SSO to the target. In case the above password change timing conditions do not hold true then the value for current password is used for injection. If the current password fails to authenticate against the target, then there is a probability that administrator had triggered an instant password rotation and primary vault manager has rotated the password but the same is not communicated to the backup vault manager. In such scenario, after one failed attempt, the backup vault manager uses the future password for authentication to the target, because as per the approach when the password of an account has to be rotated, it is always done with the future password. Once backup vault manger successfully authenticates using future password, it injects the future password for user's session and updates the current password field with the future password. So that next time when the account is to be injected, one step of failed attempt can be eliminated.

Problems Solved

As mentioned, while initiating a privileged session for an end user the invention uses the password stored in its credential vault and injects it in user's session for a privileged SSO to target systems. But in a distributed environment, there may exist network issues and other technical problems wherein the synchronization of updated password(s) from Primary Credential Vault to backup Credential Vaults may fail or get delayed.

In such scenarios, if the password stored with backup Credential Vaults is used, it will result in authentication failure for privileged account in target system and may result in locking the privileged account by the target system. This can result in denial of end user's access to the target and prevent him/her in executing any critical task on target system and end up in some downtime till the problem is solved. This invention solves this problem by injecting the correct password for user's session though synchronization issues persist in an unsynchronized distributed environment, without impacting end user experience.

Description

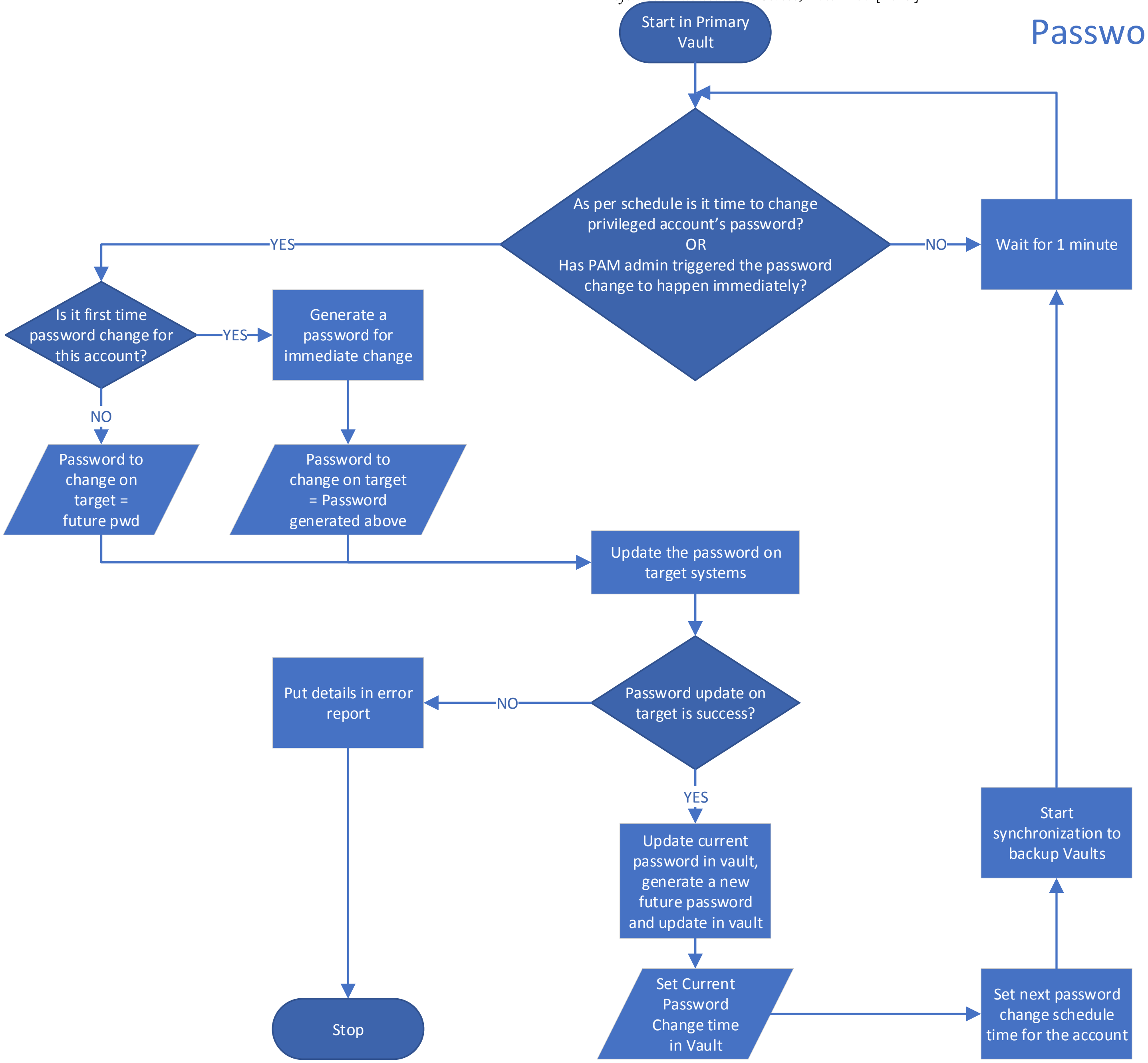
a. For providing elevated access to any particular target, the corresponding privileged accounts should be created in Vault.
b. After completing the required policy configuration, the entitled users can get elevated access to the target.
c. For the elevated access the invention stores the privileged credentials of the target in its local database in a secure and encrypted way.
d. When a user requests to access the target, the SSO is served by a proxy by injecting the privileged credential. The selection of vault manager to provide the privileged credential for SSO is done by predefined load balancing algorithm. For this, the credentials should be synchronized across all Vault managers so the authentication to the target machine should go through via any Vault manager.
e. When password rotation is enabled for privileged accounts, to rotate a password, a Manager is selected to change the password on the target based on load balance logic.
f. While enabling password management for an account primary vault manager generates a "current and future password" for the account.
g. Primary or Backup Vault manager uses "Future Password" of the account to rotate the password on the target. Thus vault manager doesn't generate a new password to update on the target instead it uses already generated password in past known as "future password". This password would be well-known to all back vault managers as well as if any momentarily sync issues must have got resolved during past few days or hours.
h. When a password is successfully rotated on the target by a Manager the same is communicated to the Primary Manager (Vault) which in turn is responsible for synchronizing the passwords to other backup managers.
i. On successful password change on the target, primary vault manager sets the present "Future Password" as the current password for the account and generates a new "Future Password" for the account.
j. Any access request to the target by the end user, where the account is injected by backup Vault manager following logic is used to select the password for injection:
If the current system time is past (more than) the scheduled time, and password of account in vault is not updated post the scheduled time, then there is a synchronization issue and the "Future Password Mode" is used otherwise the "Current Password Mode" is used as explained below.

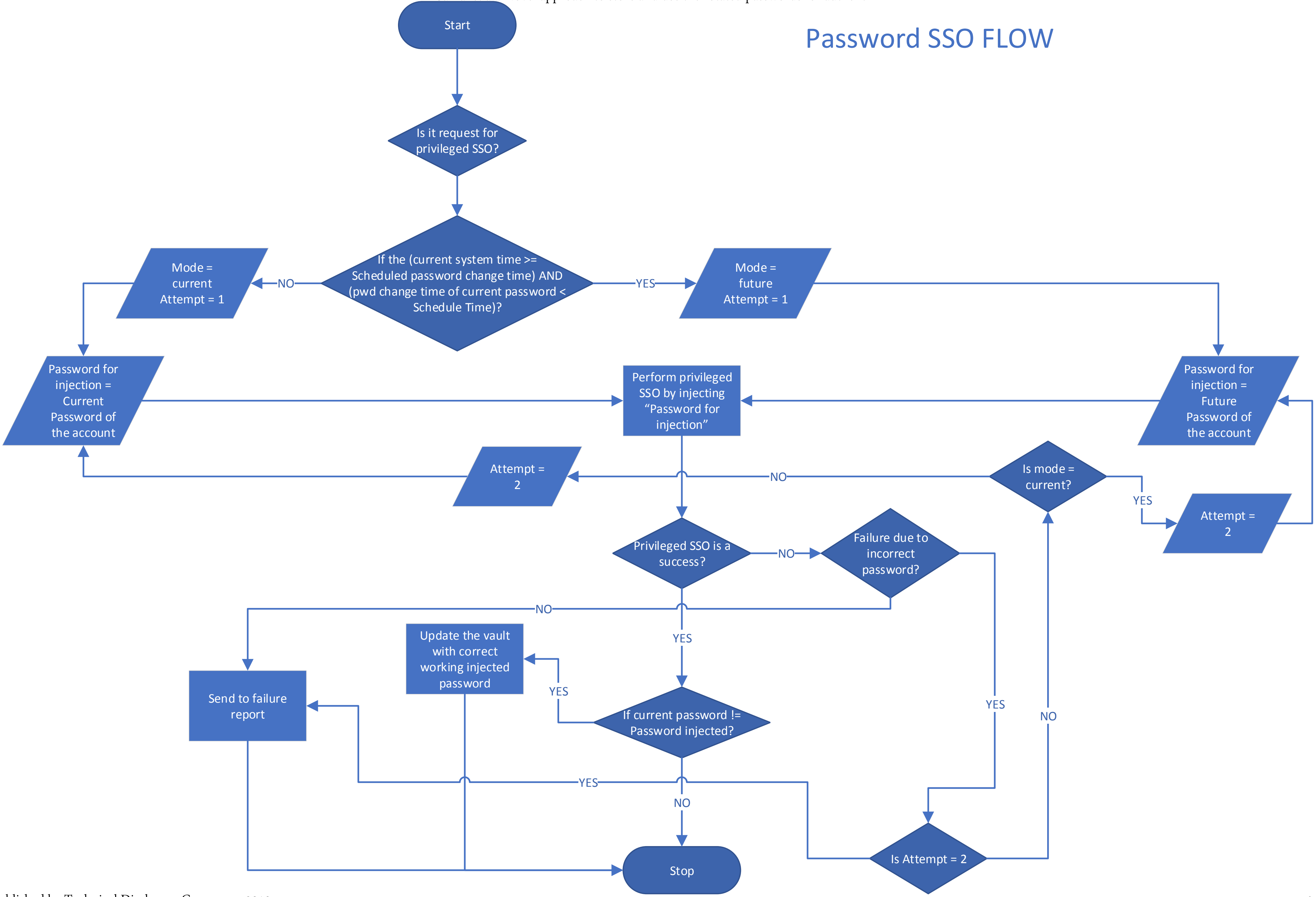
Future Password Mode: In this condition there is a near 100% probability that the account password is rotated and not synchronized across the distributed backup managers.
a. The "Future Password" is injected for privileged SSO.

b. If the authentication goes through, then the assumption of synchronization turns out to be correct.
c. The backup Vault manager uses the "Future Password" as current password until synchronization happens from primary vault manager. In next synchronization, the backup vault managers are updated with next "Future Password".
d. In case the authentication fails even with the "Future Password", that means, though the rotation was scheduled but it was not executed due to some issue or may be due to any update in the scheduler.
e. In such case, the backup manager tries authentication with the current password. If it goes through successfully then the current password is injected for user's session, else an error is reported and user won't get privileged access.

Current Password Mode: In this condition, the current system time, the scheduled time and the last time when the password was updated do not indicate any synchronization issue.
a. Here the backup vault manager proceeds with injecting current password for user's access to the target.
b. A failure of authentication in this case will happen if the administrator had triggered an instant password change and the rotation of password is over but the update is not communicated or delay in communication from Primary Vault manager to backup managers.
c. As the password is rotated in the target system, the current password will fail to authenticate.
d. The backup Vault manager now uses the "Future Password" it has for the account for authentication.
e. If the authentication is successful the "Future Password" is injected for user's session and "Future Password" is set as current password. The backup Vault manager will be updated with next "Future Password" once synchronization happens from primary manger.

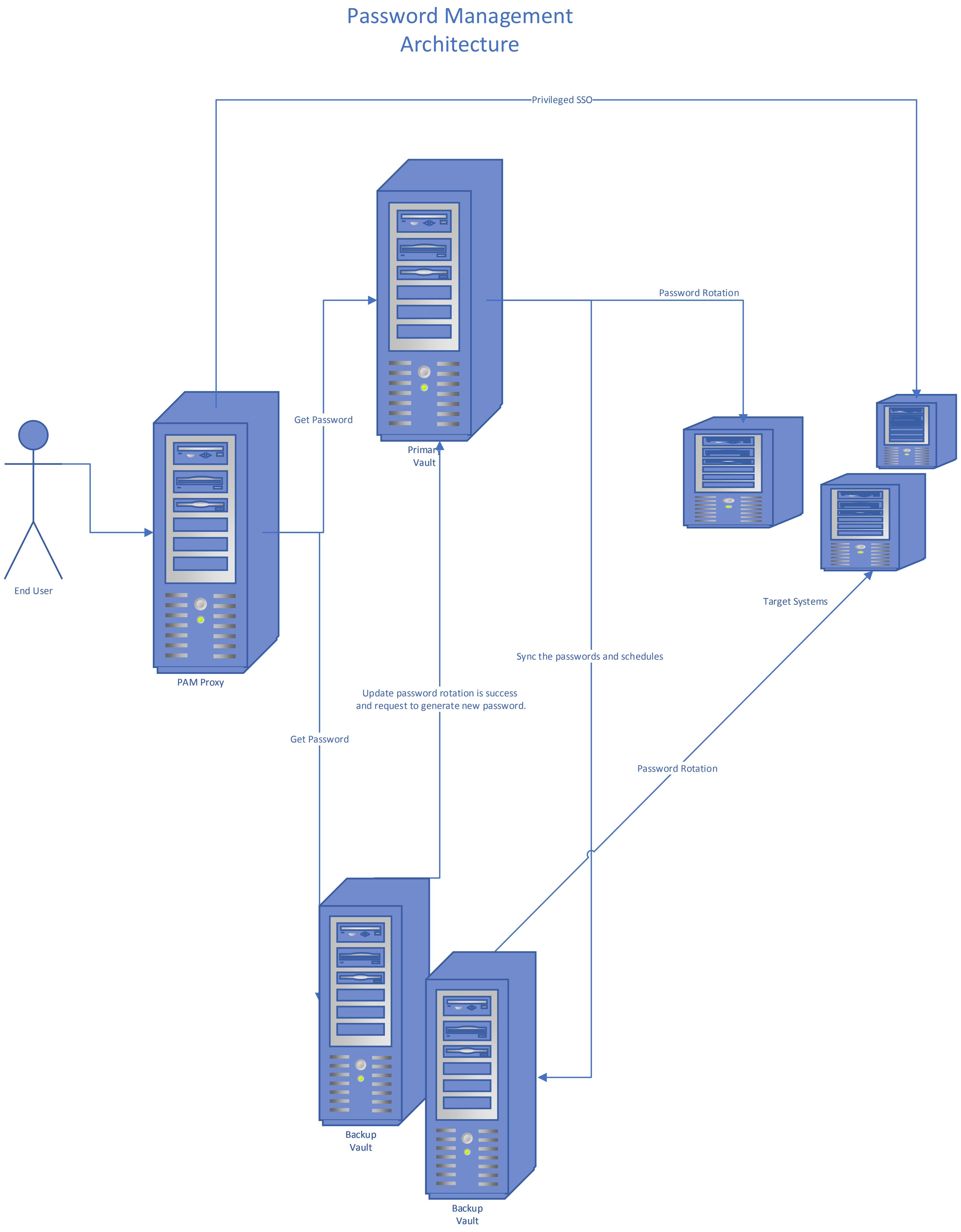
Password Generation FLOW


Start in Primary Vault
As per schedule is it time to change privileged account's password? OR Has PAM admin triggered the password change to happen immediately?
NO
Wait for 1 minute
YES
Is it first time password change for this account?
YES
Generate a password for immediate change
NO
Password to change on target = future pwd
Password to change on target = Password generated above
Update the password on target systems
Password update on target is success?
NO
Put details in error report
Stop
YES
Update current password in vault, generate a new future password and update in vault
Set Current Password Change time in Vault
Set next password change schedule time for the account
Start synchronization to backup Vaults



Password SSO FLOW

Start
Is it request for privileged SSO?
If the (current system time >= Scheduled password change time) AND (pwd change time of current password < Schedule Time)?
NO
Mode = current Attempt = 1
YES
Mode = future Attempt = 1
Password for injection = Current Password of the account
Perform privileged SSO by injecting "Password for injection"
Password for injection = Future Password of the account
Attempt = 2
NO
Is mode = current?
YES
Attempt = 2
Privileged SSO is a success?
NO
Failure due to incorrect password?
NO
YES
Update the vault with correct working injected password
YES
Send to failure report
If current password != Password injected?
YES
YES
NO
NO
Is Attempt = 2
Stop


Password Management
Architecture
Privileged SSO
Password Rotation
Get Password
Primary
Vault
End User
PAM Proxy
Target Systems
Sync the passwords and schedules
Update password rotation is success
and request to generate new password.
Get Password
Password Rotation
Backup
Vault
Backup
Vault