



CYBERARK®
The Identity Security Company™

PAM Administration

Accounts – Part 2



Agenda

By the end of this session, you will be able to:

1. Describe and configure linked accounts:
 - Logon accounts
 - Reconcile accounts
2. Describe and configure SSH key management

Linked Accounts

There are two types of linked accounts commonly used and supported by default for most platforms:

- Logon account
- Reconcile account



Logon Account

Root Account Best Practices

```
Using username "root".  
root@10.0.0.20's password:  
Access denied
```

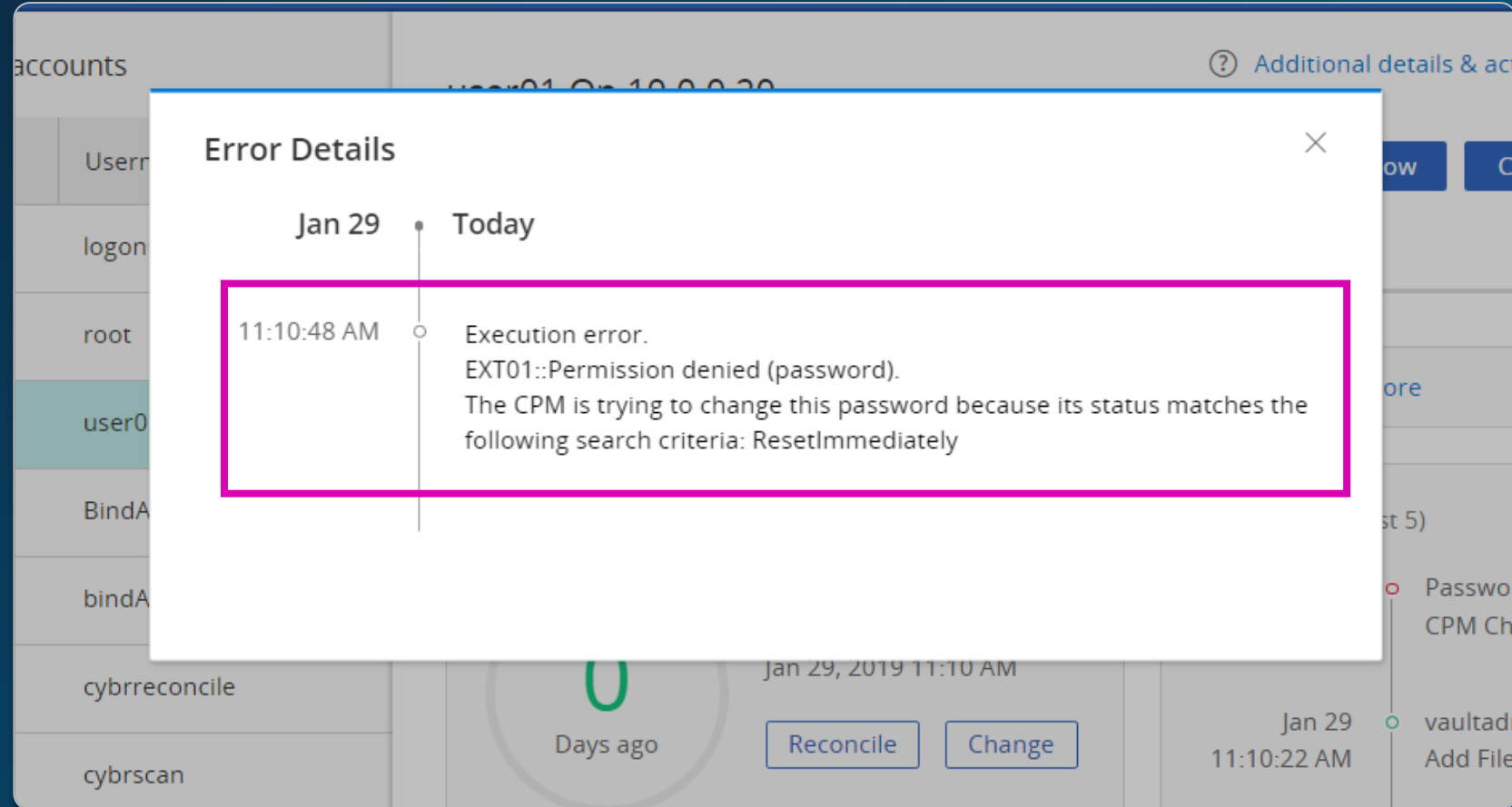
The root user is often prevented from logging in remotely as part of best practices (/etc/ssh/sshd_config > PermitRootLogin no)

The solution is to log in as a user with the authorization to switch to root in order to perform the password change

```
login as: logon01  
logon01@10.0.0.20's password:  
[logon01@centos-target01 ~]$ su - root  
Password:  
[root@centos-target01 ~]# passwd  
Changing password for user root.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@centos-target01 ~]#
```

Root Password Change Failure

If the SSH policy on the target machine forbids root log on, the **CPM** will not be able to verify or change the root password



Associate Logon Account

The solution is to onboard a non-privileged account that we can use to connect and then switch to root in order to perform the password change. This account is the **Logon Account**

To use a **Logon Account**, you need to link it to the root account

The screenshot displays the CyberArk console interface. The main window shows the details for the account 'root03 On target-lin'. The 'Details' tab is selected, and the 'Linked Accounts' section shows 'Logon Account' as 'None'. A 'Link' button is visible next to the 'Logon Account' field. A modal window titled 'Link Logon Account with: root03 | target-lin' is open, showing a search for 'logon' with 12 results. The results table lists several logon accounts, with 'logon03' highlighted. The 'logon03' row is highlighted with a red border.

root03 On target-lin

Platform: LIN SSH 30 Safe: Lin-Fin-US

Connect Show

Overview **Details** Activities Versions

Account Properties

Safe
Lin-Fin-US

Platform
LIN SSH 30

Address
target-lin

Username
root03

Account name
Operating System-LINSSH30+

Date created
1/18/2022 12:14 PM

Linked Accounts

Logon Account
None

Reconcile Account
None

Account Groups

Link
Unlink

Link Logon Account with: root03 | target-lin

Select an account

12 results for: logon

Status	Username	Address	Platform	Safe
-	logon01	10.0.0.20	LIN SSH 30	Lin-Fin-US
-	logon02	10.0.0.20	LIN SSH 30	Lin-Fin-US
-	logon03	10.0.0.20	LIN SSH 30	Lin-Fin-US
-	logon04	10.0.0.20	LIN SSH 30	Lin-Fin-US
-	logon05	10.0.0.20	LIN SSH 30	Lin-Fin-US

Cancel OK

Root Password Change Success

Now that we have specified a logon account, when we re-run a password change, we will see that the **PasswordManager** user has changed the password.

Note that the logon account is also used when connecting to the target system through the **PSM**

root03 On target-lin

⚡

Platform: LIN SSH 30

Safe: Lin-Fin-US

Connect

Show

⋮

Overview

Details

Activities

Versions

Account Properties

Safe

Lin-Fin-US

Platform

LIN SSH 30 ⓘ

Address

target-lin

Username

root03

Account name

Operating System-LINSSH30-target-lin-root03

Date created

1/18/2022 12:14 PM

Linked Accounts

Logon Account

LIN SSH 30-logon03-10.0.0.20

⋮

Reconcile Account

None

⋮

Account Groups

Group Name

None

Group Platform

None

ⓘ Additional details & actions in classic interface

✕

Activate Windows

Go to Settings to activate Windows.

Reconcile Accounts

Reconciliation – Unknown Password

Reconciliation is used for situations where we don't know a password or if the use of individual passwords would be too onerous

Error Details

Jan 18

Today

1:46:17 PM

Error in logon to user target-win.acme.corp\discovery01 on domain target-win.acme.corp(\\target-win.acme.corp).(winRc=1326) The user name or password is incorrect.
The CPM is trying to change this password because its status matches the following search criteria: ResetImmediately

Reconciliation – Unknown Password

The verification process will discover passwords that are not synchronized with their corresponding password in the **Vault** and we can configure the **CPM** to reset the password in the **Vault** and on the Target

discovery01 On target-win.acme.corp

Platform: WIN SRV LCL ADM 45 Safe: Win-Srv-Fin-US

Connect Show

Overview Details Activities Versions

Compliance Status Compliant

0 Days ago

Reconciled by PasswordManager
Jan 18, 2022 1:47 PM

Reconcile Change

Last Verified

1 Days ago

Verified by PasswordManager
Jan 17, 2022 11:01 AM

Verify

Activities (Last 5)

Jan 18 1:47:19 PM	PasswordManager	CPM Reconcile Password
Jan 18 1:46:17 PM	PasswordManager	CPM Change Password Failed
Jan 18 1:45:30 PM	mike	Delete File Category
Jan 18 1:45:30 PM	mike	Delete File Category
Jan 18 1:45:30 PM	mike	Delete File Category

Associating a Reconcile Account

The screenshot displays the 'WIN SVR ADM 45' console window. On the left, a tree view shows the configuration hierarchy: 'Target Account Platform' > 'UI & Workflows' > 'Automatic Password Management' > 'Password Reconciliation'. The 'Password Reconciliation' item is selected. The main pane shows the 'Properties' table for this configuration.

Name	Value
RCAAllowManualReconciliation	Yes
RCAutomaticReconcileWhenUnsynced	Yes
RCReconcileReasons	2114,2115,2106,2101
RCFromHour	-1
RCToHour	-1
ReconcileAccountSafe	CyberArk-Service-Accounts
ReconcileAccountFolder	Root
ReconcileAccountName	Operating System-WINDOMADM15-acme.corp-s-reconcile
RCExecutionDays	
IgnoreReconcileOnMissingAccount	No

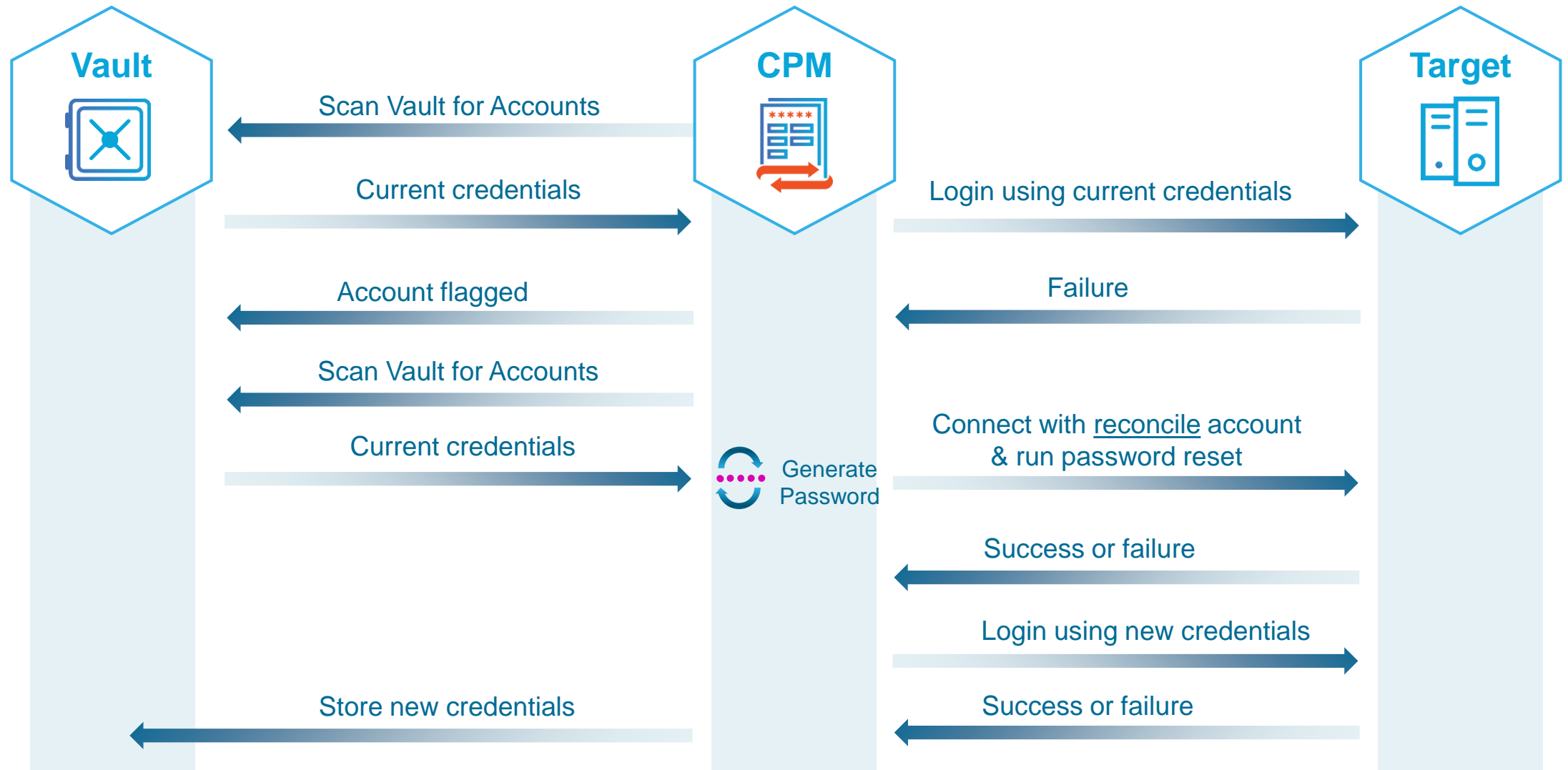
Callout 1 (top right): Manual reconciliation is enabled by default. Automatic reconciliation must be enabled.

Callout 2 (bottom right): A reconcile account is typically a Domain account with sufficient rights to perform a password change

Buttons: Apply, OK, Cancel (top left and bottom right)

Bottom section: Help, Notifications, Password Reconciliation Policy settings for reconciling passwords.

Failed Verify and Reconcile Process



Manual Reconciliation

Account view

Filter

localadmin

Last sign in: 10/20/2022 | tom

Ad hoc connectionAdd account

6 results for: localadmin ,

☆	Status	Username	Address
☆	-	localadmin01	target-win.a
☆	⚡	localadmin03	target-win.a
☆	⚡	localadmin04	target-win.a
☆	⚡	localadmin05	target-win.a
☆	⚠ ⚡	localadmin11	target-win.a
☆	⚡	localadmin09	target-win.a

localadmin11 On target-win.acme.corp

⚠ ⚡ Platform: WIN SVR PRV 30 Safe: Win-Srv-Fin-US

ShowCopy...Connect

OverviewDetailsActivitiesVersions

⚠ CPM failed to change this password Error in logon to user target-win.acme.corp\localad... More

Compliance Status Compliant

0

Days ago

Changed by tom
Oct 20, 2022 9:50 AM

ReconcileChange

Activities (Last 5)

Oct 20 9:51:44 AM

PasswordManager1

CPM Change Password Failed

Oct 20 9:50:57 AM

tom

Add File Category

Oct 20 9:50:56 AM

tom

Add File Category

Logon Account vs. Reconcile Account

Logon Account

- Used when a user is prevented from logging on and the password is known
- Used on a regular basis – i.e., it is common to block root access via SSH
- A 'super user' such as root should not be used as a logon account

Reconcile Account

- Used for 'lost' or unknown passwords
- Should be used infrequently
- Needs to have elevated privileges (member of local administrators)
- This account is usually a service account reserved for this purpose

SSH Key Management

SSH – Password Authentication

- Client launches the connection.
- Server presents its public key.
- Client and server negotiate a symmetric session key. All further communication is encrypted with the symmetric session key.
- User enters the account password and the Server authenticates it.

```
[root@centos-target01 ~]# ssh root@10.0.1.16
The authenticity of host '10.0.1.16 (10.0.1.16)' can't be
established.
RSA key fingerprint is
b0:38:8a:73:92:14:2a:92:f4:fa:25:68:5b:4e:80:77.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.16' (RSA) to the list of
known hosts.
root@10.0.1.16's password: *****
[root@psmp-psmgw ~]#
```



John

USER

SSH

TRUST



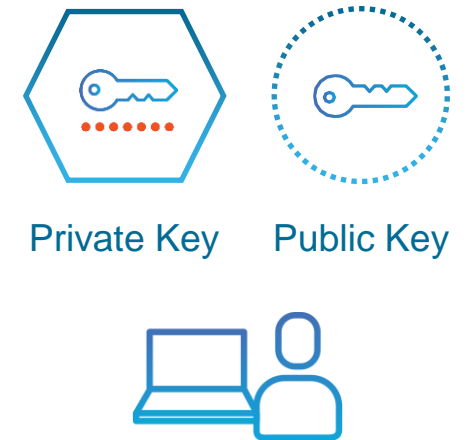
Linux Server
192.168.47.172

TARGET SERVER

SSH – Asymmetric Key Authentication

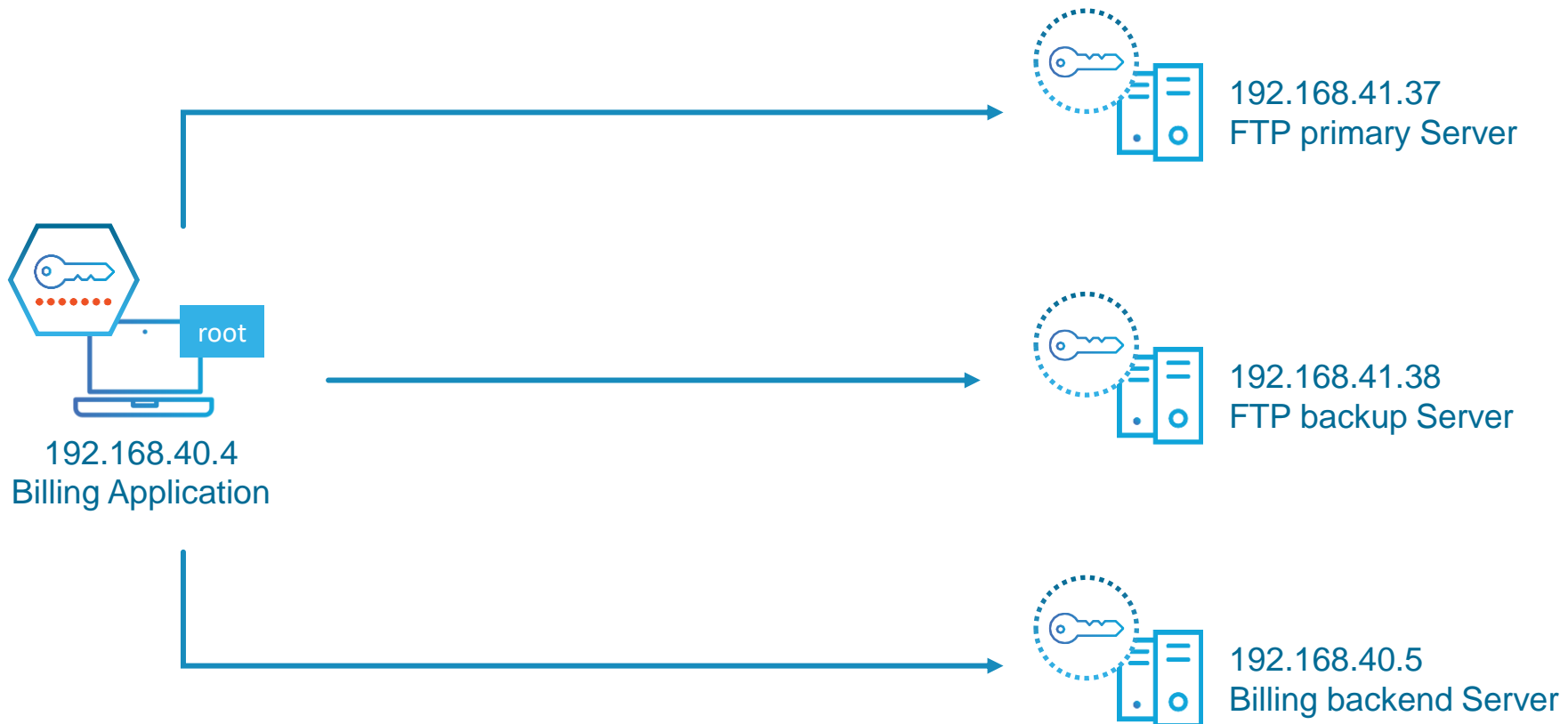
To authenticate with SSH keys, the user must first generate a public/private key-pair locally on her machine and then install the public key in her user directory on the target server (or servers) through a password authenticated session.

- Once that is done, the user can authenticate using the SSH keys.
- She launches a connection to the remote server.
- The server then encrypts a random prime number with the user's **public** key and transmits that back to the user, who must then decrypt the number with her corresponding private key.
- She then generates a hash of the prime number and returns it to the server.
- The server compares it with its own hash of the prime. If they match, then this proves that the user must have the private half of the key-pair
- The server therefore allows the connection to be established.



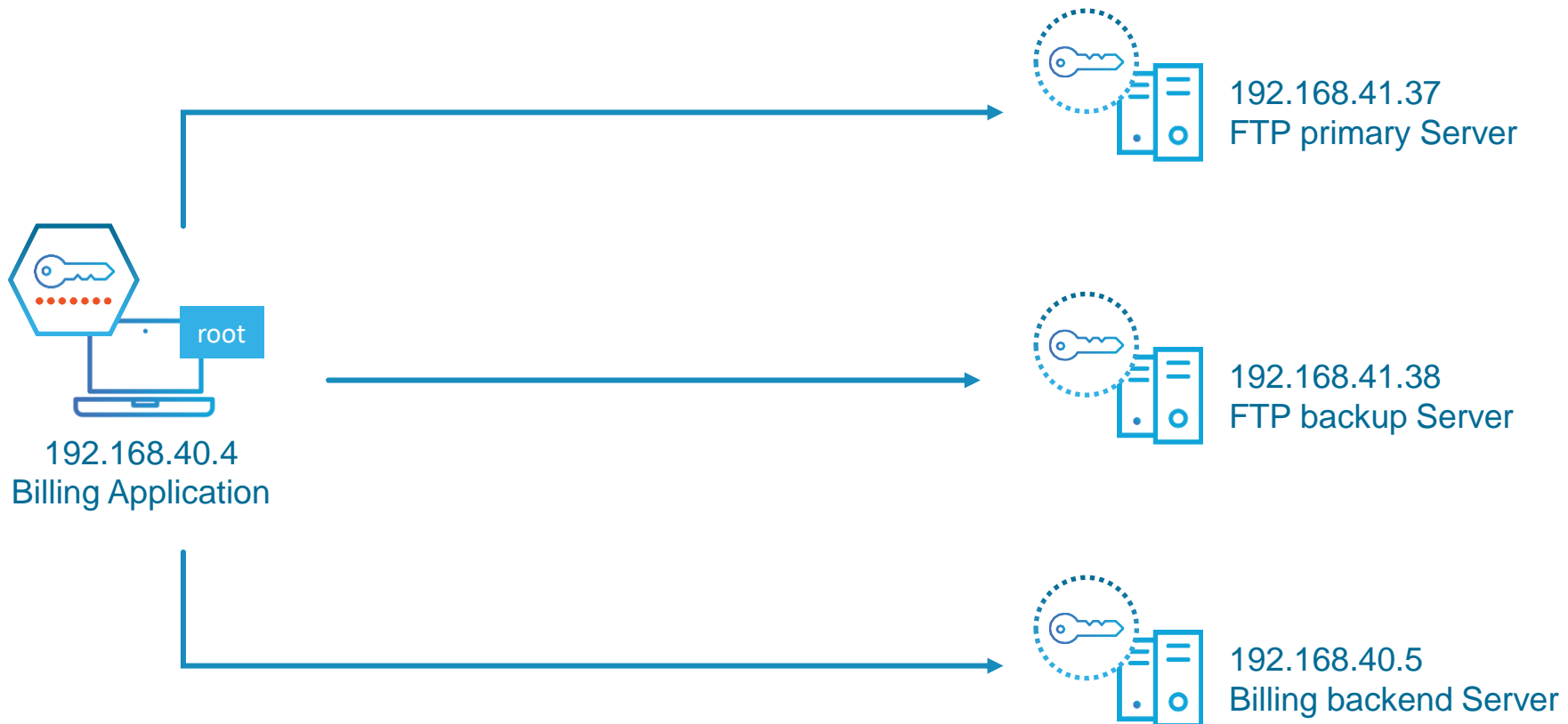
SSH Key Advantages

- SSH keys allow a substantially longer secret between client and server than a password.
- The secret is never transmitted over the network.
- One private key can be used to access multiple systems



SSH Key Disadvantages

- One private key can be used to access multiple systems. If it is compromised, all the systems that trust it are vulnerable
- SSH keys are more difficult to change than passwords



SSH Key Manager

- Creates unique key-pairs for each target system.
- Private keys are stored in the **Vault**, not on user workstations.
- The **CPM** changes key-pairs often and automatically disseminates public keys to target systems.
- End users retrieve the private key from the **Vault** to authenticate to the target system.



Adding Keys to the Vault

Add Account

✓ Select system type
*NIX

✓ Assign to platform
LIN KEYS 60

✓ Store in Safe
Lin-Fin-US

4 Define properties

SSH keys can share a Safe with passwords, but they need their own Platforms

Primary properties

Address

target-lin.acme.corp

Username

root01b

SSH Private key

Select file

Paste content



Drop file or click to browse



root01b.ppk ✓

☒ Customize account name ?

Additional properties

Sign in: 9/26/2022

👤 paul ▾

You can select the file containing the private key or copy and paste it.

Because entering the SSH keys into CyberArk exposes them, the old keys can no longer be considered secure and should be rotated immediately.

Cancel

< Back

Add ▾

Activate Windows
Go to Settings to activate

Rotate Keys

root01b On target-lin.acme.corp

⚡ Platform: LIN KEYS 60 Safe: Lin-Fin-US

Overview Details Activities Ver

Compliance Status **Compliant**

0 Days ago

Changed by PasswordManager
Sep 26, 2022 12:08 PM

Reconcile **Change**

Additional details & actions in classic interface

Retrieve Copy ... Connect | v

You can rotate the SSH keys using the **Change** button, just like with passwords

Activities (Last 5)

Sep 26 12:08:39 PM	○ PasswordManager CPM Rotate SSH Key
Sep 26 12:08:12 PM	○ paul Add File Category
Sep 26 12:08:12 PM	○ paul Add File Category
Sep 26 12:08:12 PM	○ paul Add File Category

Activate Windows
Go to Settings to activate Windows.

Retrieve / Connect

Account view

Filter | Search for accounts

5 results for: All accounts

☆	Status	Username	Address
☆	⚡	cpm-scan	acme.corp
☆	⚡	s-reconcile	acme.corp
☆	⚡	root01b	target-lin.ac
☆	⚡	logon01	target-lin.ac
☆	⚡	root01	target-lin.ac

root01b On target-lin.acme.corp

⚡ Platform: LIN KEYS 60 Safe: Lin-Fin-US

[Overview](#) [Details](#) [Activities](#) [Versions](#)

Compliance Status **Compliant**

Additional details & actions in classic interface

[Retrieve](#) [Copy](#) [...](#) [Connect](#)

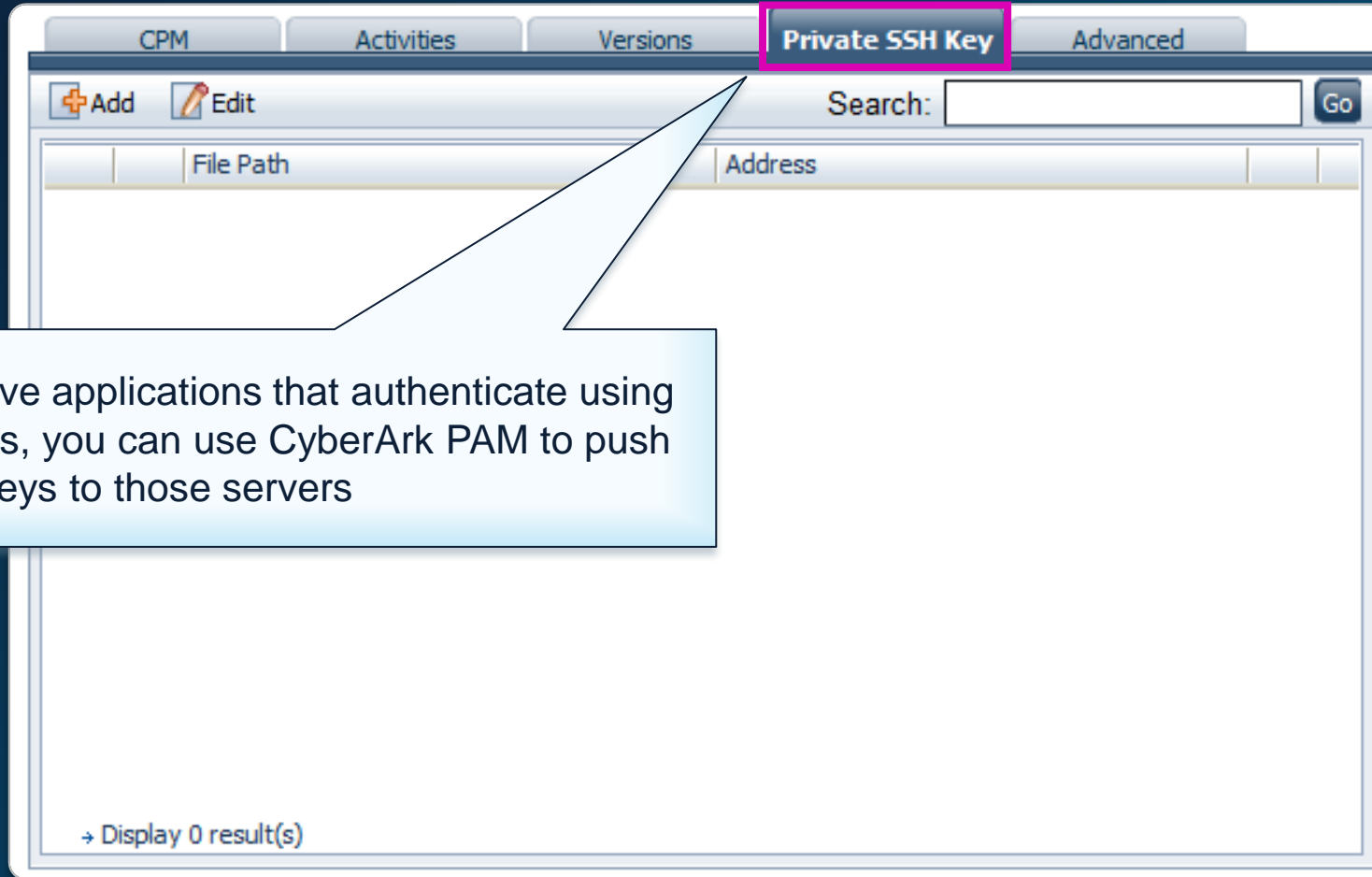
Activities (Last 5)

- Sep 26 12:08:39 PM PasswordManager CPM Rotate SSH Key
- Sep 26 12:08:12 PM paul Add File Category
- Sep 26 paul

Users who have the **Retrieve Accounts** permission can retrieve a copy of the private key

Users who have the **Use Accounts** permission can click on the **Connect** button to launch the session directly from the **PVWA**

Push Private Keys to Application Servers



If you have applications that authenticate using SSH keys, you can use CyberArk PAM to push private keys to those servers

Summary



Summary

In this session, we discussed:

- How to configure linked accounts
- How to use the SSH key manager

Additional Resources



Online Training

[Linked Accounts](#)

(login required)

You may now complete the following exercises:

Linked Accounts

- Securing SSH Accounts Using a Logon account
- Securing Windows Server Local Accounts via a Reconcile Account

Securing Unix Accounts With SSH Keys

- Generating a Key-Pair
- Verify you can login with the Private Key
- Duplicating a Platform
- Add an Account with an SSH Key