



PAM Administration

Accounts – Part 2



Agenda

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

- Describe and configure linked accounts:
 - Logon accounts
 - Reconcile accounts
- 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)

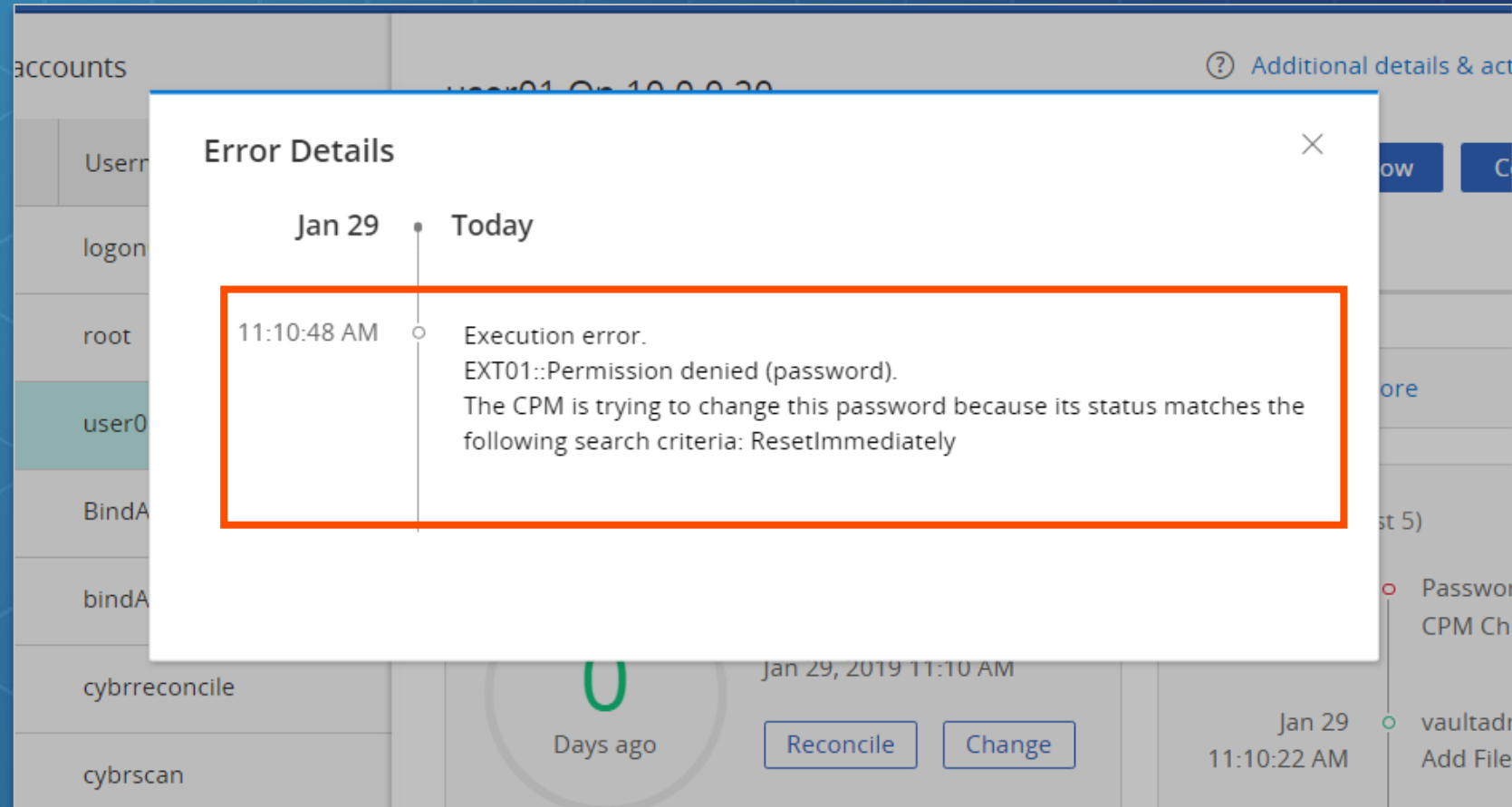
The solution is to log in as a user with the authorization to switch to root in order to perform the password change

```
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 ~]#
```



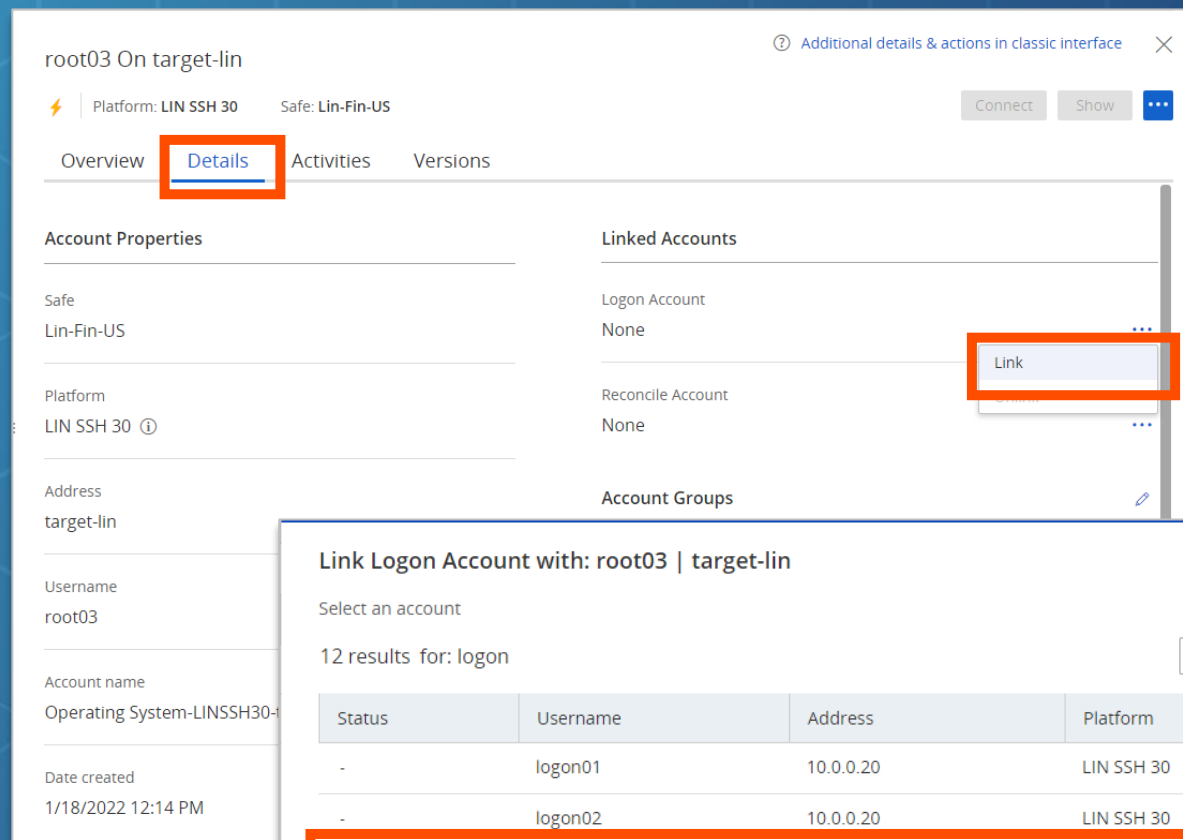
Root Password Change Failure

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 with the authorization to 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



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

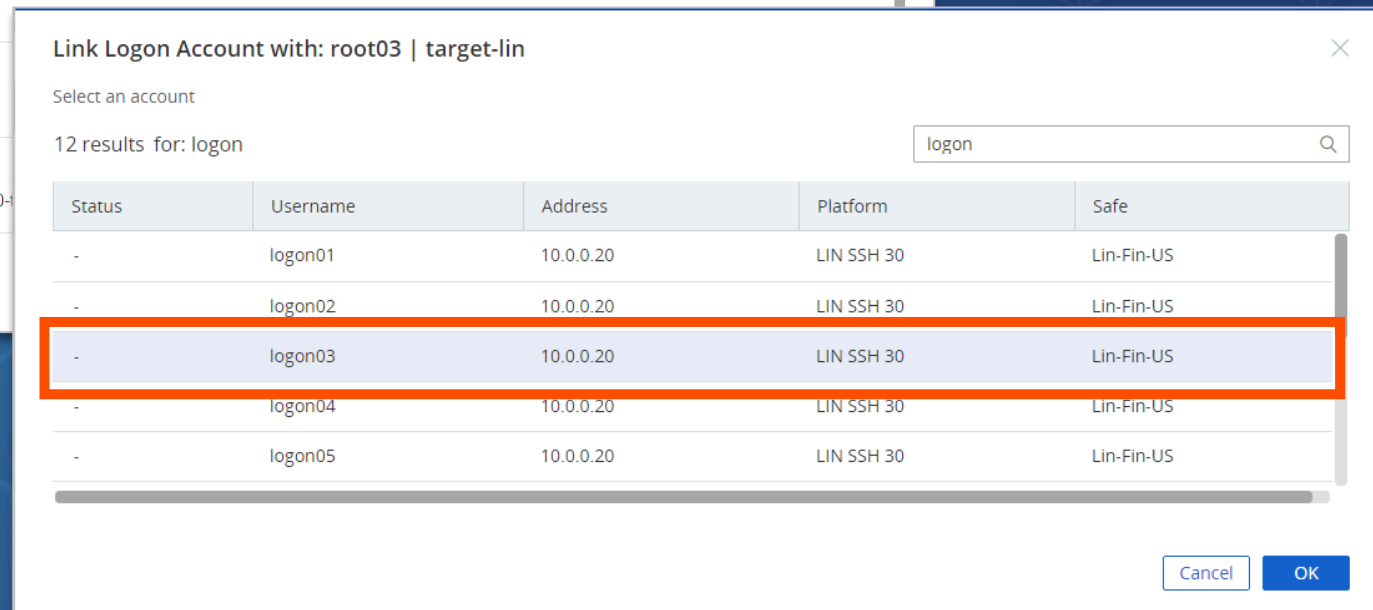
Linked Accounts

Logon Account
None

Reconcile Account
None

Account Groups

Link



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**

The screenshot displays the 'root03 On target-lin' account details in the CyberArk console. The interface includes a top bar with a help icon, a link to 'Additional details & actions in classic interface', and a close button. Below the title bar, there are tabs for 'Overview', 'Details' (selected), 'Activities', and 'Versions'. The 'Details' tab is divided into two columns: 'Account Properties' and 'Linked Accounts'.

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 (highlighted with an orange box)
- Reconcile Account: None

Account Groups:

- Group Name: None
- Group Platform: None

At the bottom right, there is a message: 'Activate Windows Go to Settings to activate Windows.'



Logon Account – Platform Settings

The screenshot displays the CyberArk Platform Settings application. On the left, a tree view shows the navigation structure, with 'LogonAccount' selected under 'Target Account Platform'. The main pane shows the 'Properties' tab for 'LogonAccount'. A table lists various settings, with 'LogonAccountName' highlighted by an orange box. A callout bubble points to this setting, stating: 'The logon account can be set on the individual account or via the Platform'.

Name	Value
ResetOverridesMinValidity	Yes
ResetOverridesTimeFrame	Yes
Timeout	90
UnlockIfFail	No
UnrecoverableErrors	8002,8003,8006,8007,8010,8011
MaximumRetries	5
LogonAccountSafe	
LogonAccountFolder	Root
LogonAccountName	

LogonAccountName
The name of the logon account or a dynamic rule to specify this value.



Reconcile Accounts



Reconciliation – Unknown Password

Reconciliation is used for situations where we don't know a password – for example, if the password in the **Vault** and on the Target machine have somehow become unsynchronized – or if the use of individual passwords would be too onerous – you have a fleet of Windows servers, each with its own local admin password, and you want to onboard them all at once, not one by one.

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

WIN SRV LCL ADM 45

Search... Go

- Target Account Platform
 - UI & Workflows
 - Automatic Password Management
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change
 - Password Verification
 - Password Reconciliation**
 - Notifications
 - Generate Password
 - General Properties

Name	Value
RCAllowManualReconciliation	Yes
RCAutomaticReconcileWhenUnsynced	Yes
RCReconcileReasons	2114,2115,2106,2101
RCFromHour	-1
RCToHour	-1
ReconcileAccountSafe	CyberArk-Service-Accounts
ReconcileAccountFolder	Root
ReconcileAccountName	Operating System-WINDOMADM15-acme.corp-cybrreconcile
RCExecutionDays	

Help Notifications

Password Reconciliation
Policy settings for reconciling passwords.

Apply OK Cancel

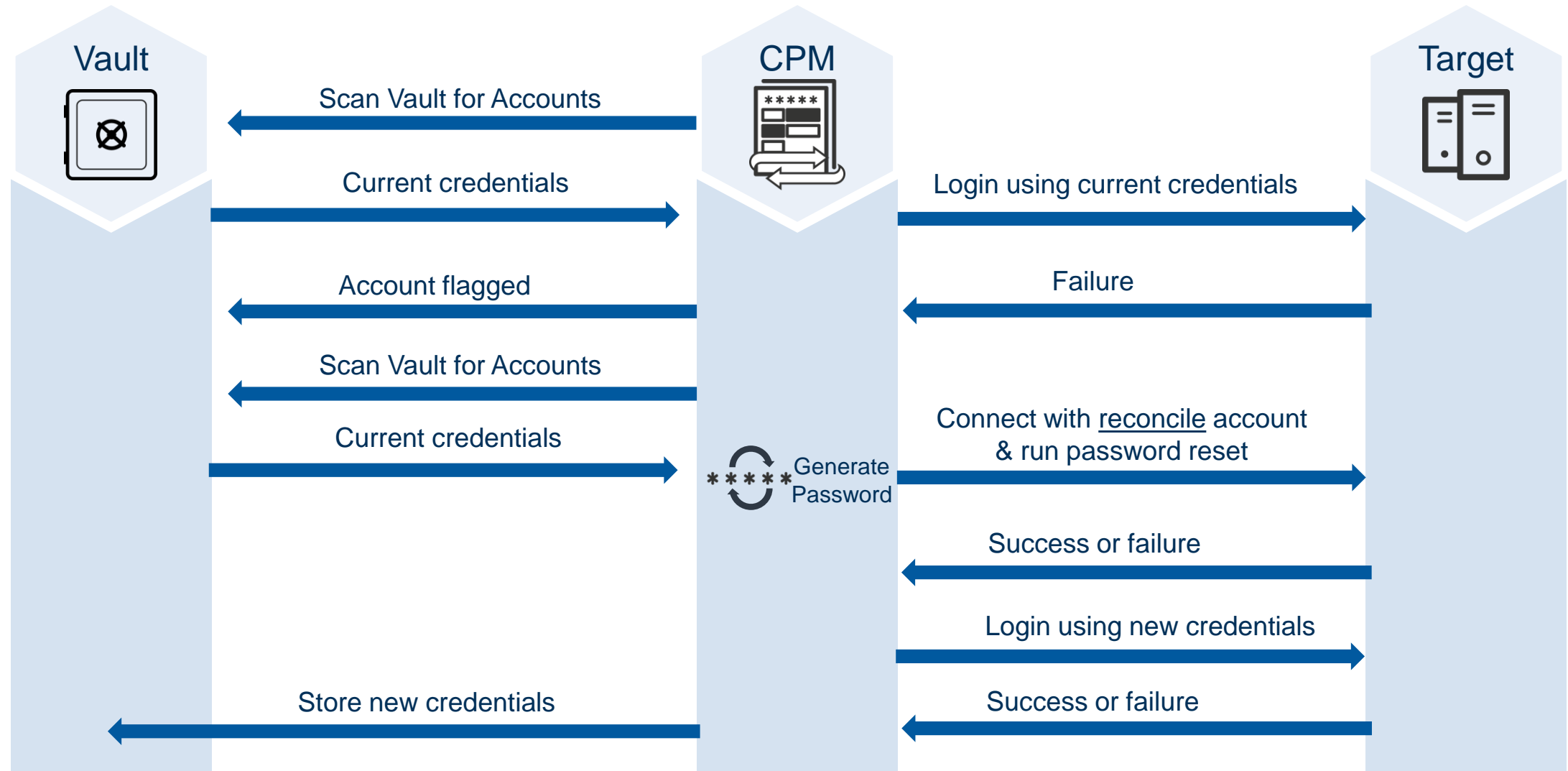
Manual reconciliation is enabled by default.

Automatic reconciliation must be enabled.

A reconcile account is typically a Domain account with sufficient rights to force a password change



Failed Verify and Reconcile Process



Manual Reconciliation

The screenshot displays the 'Accounts View' interface. On the left is a sidebar with navigation icons. The main header shows 'Accounts View' and user information 'Last sign in: 8/25/2021 | mike'. A search bar contains 'localadmin01', resulting in '1 results for: localadmin01'. A table lists account details:

☆	Status	Username	Address
☆	⚠️ ⚡	localadmin01	target-win.a

The details panel for 'localadmin01 On target-win.acme.corp' is open. It shows platform 'WIN SRV LCL ADM 45' and safe 'Win-Srv-Fin-US'. A red box highlights the error: 'CPM failed to reconcile this password Error in verifypass to user target-win.acme.corp\...More'. Below this, the 'Compliance Status' is 'Compliant' with a '6 Days ago' indicator. A red box highlights the 'Reconcile' button. The 'Activities' section shows recent events, including 'PasswordManager CPM Verify Password Failed' and 'Delete 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 (i.e. Domain Admin)
- 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.

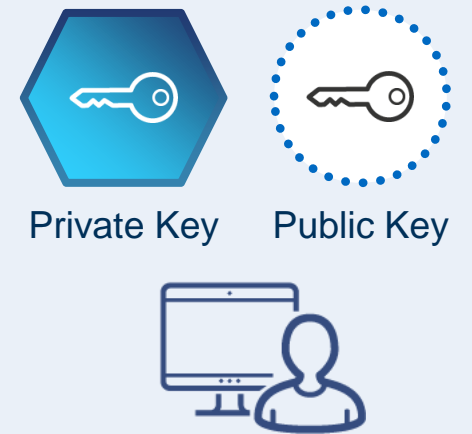
```
[root@centos-target01 ~]# ssh root@10.0.1.16
The authenticity of host '10.0.1.16 (10.0.1.16)' can't be
established.
RSA key fingerprint is
b0:38:8a:73:92:14:2a:92:f4:fa:25:68:5b:4e:80:77.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.16' (RSA) to the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



SSH – Asymmetric Key Authentication

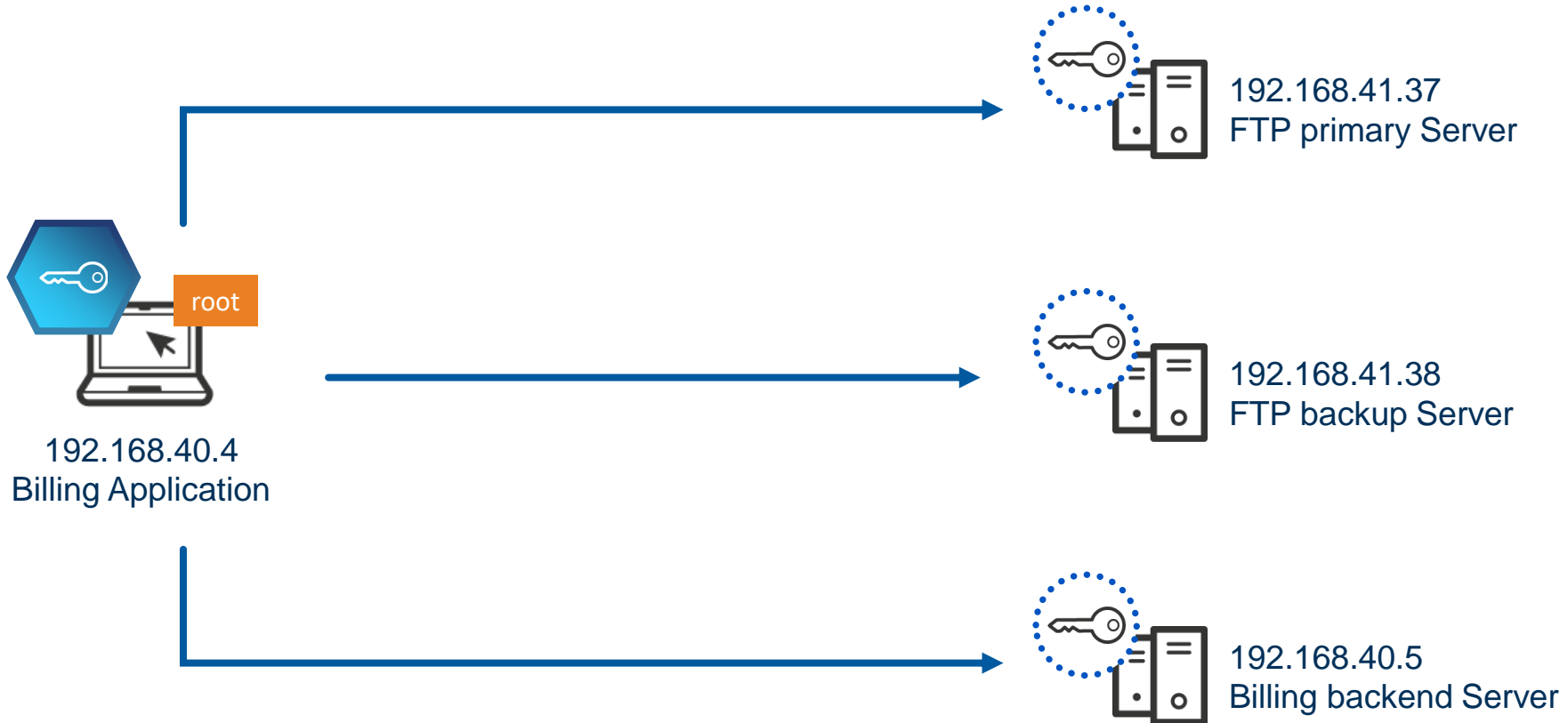
To authenticate with SSH keys, the user must first generate a public/private key-pair locally on her machine and then install the public key in her user directory on the target server (or servers) through a password authenticated session.

- 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 (because only the private key can decrypt what has been encrypted with the public key.)
- The server therefore allows the connection to be established.



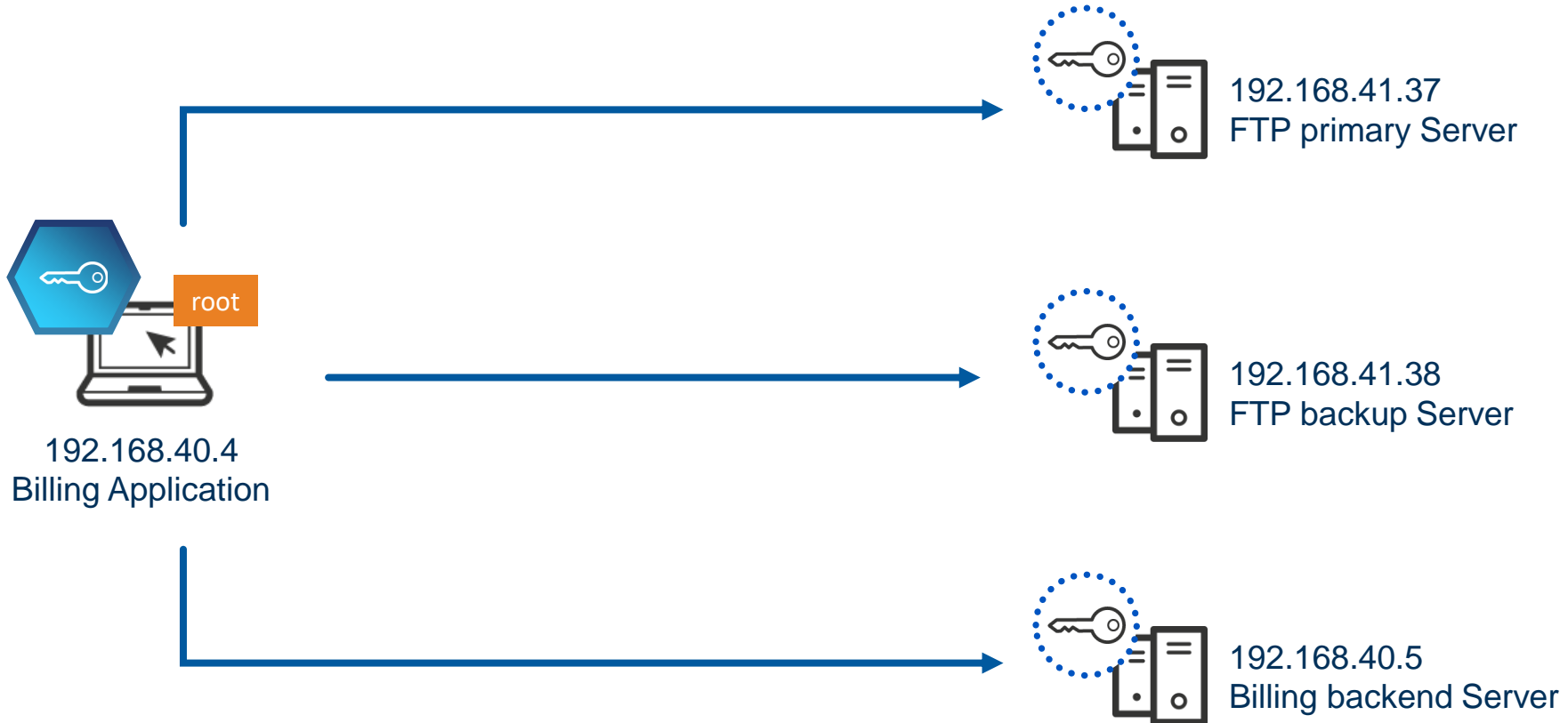
SSH Key Advantages

- 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

The screenshot shows the 'Add Account' interface in CyberArk. On the left, a sidebar contains icons for account management. The main area displays a progress bar with four steps: 'Select system type *NIX', 'Assign to platform LIN KEYS 90', 'Store in Safe Lin-Fin-US', and '4 Define properties'. The 'Define properties' step is highlighted with a red box. To the right, the 'Primary properties' form is shown, with fields for 'Address' (10.0.0.20) and 'Username' (root01). The 'SSH Private key' section is also highlighted with a red box, showing tabs for 'Select file' and 'Paste content', and a large dashed box with a plus icon and the text 'Drop file or click to browse'. A blue callout bubble points to the 'SSH Private key' section, stating: 'SSH keys can share a Safe with passwords, but they need their own Platforms'. Another blue callout bubble points to the 'Drop file or click to browse' area, stating: 'You can select the file containing the private key or copy and paste it.' At the bottom right, there are buttons for 'Cancel', '< Back', and 'Add'. A Windows watermark is visible in the bottom right corner.

Add Account

Last sign in: 7/19/2021 | paul

✓ Select system type
*NIX

✓ Assign to platform
LIN KEYS 90

✓ Store in Safe
Lin-Fin-US

4 Define properties

Primary properties

Address
10.0.0.20

Username
root01

SSH Private key

Select file Paste content

Drop file or click to browse

Customize account name ?

Cancel < Back Add

Activate Windows
Go to Settings to activate Windows.

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



Rotate Keys

Accounts View

Last sign in: 8/25/2021 | mike

Filter | root01

2 results for: root01

Status	Username	Address
⚡	root01	10.0.0.20
⚡	root02	target

root01 On 10.0.0.20

Platform: LIN KEYS 90 Safe: Lin-Fin-US

Connect Show

Overview Details Activities Versions

Compliance Status Compliant

1 Days ago

Changed by PasswordManager Aug 24, 2021 2:32 AM

Reconcile **Change**

Activities (Last 5)

- Aug 25 2:29:44 AM PasswordManager CPM Verify SSH Key
- Aug 24 6:30:01 AM PTAApUser Privileged Threat Analytics Event
- Aug 24 2:32:23 AM PasswordManager CPM Rotate SSH Key

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



Retrieve / Connect

Accounts View

Filter: root01

2 results for: root01

Status	Username	Address
⚡	root01	10.0.0.1
⚡	root02	target-lin

Platform: LIN KEYS 90 Safe: Lin-Fin-US

Buttons: Retrieve, Copy, ..., Connect

Overview Details Activities Versions

```
root@target-lin:~  
Using username "root01".  
Authenticating with public key "rsa-key-20210307"  
Last login: Sun Mar 7 13:56:52 2021 from pvwa.acme.corp  
[root@target-lin ~]#  
[root@target-lin ~]#
```

Activities (Last 5)

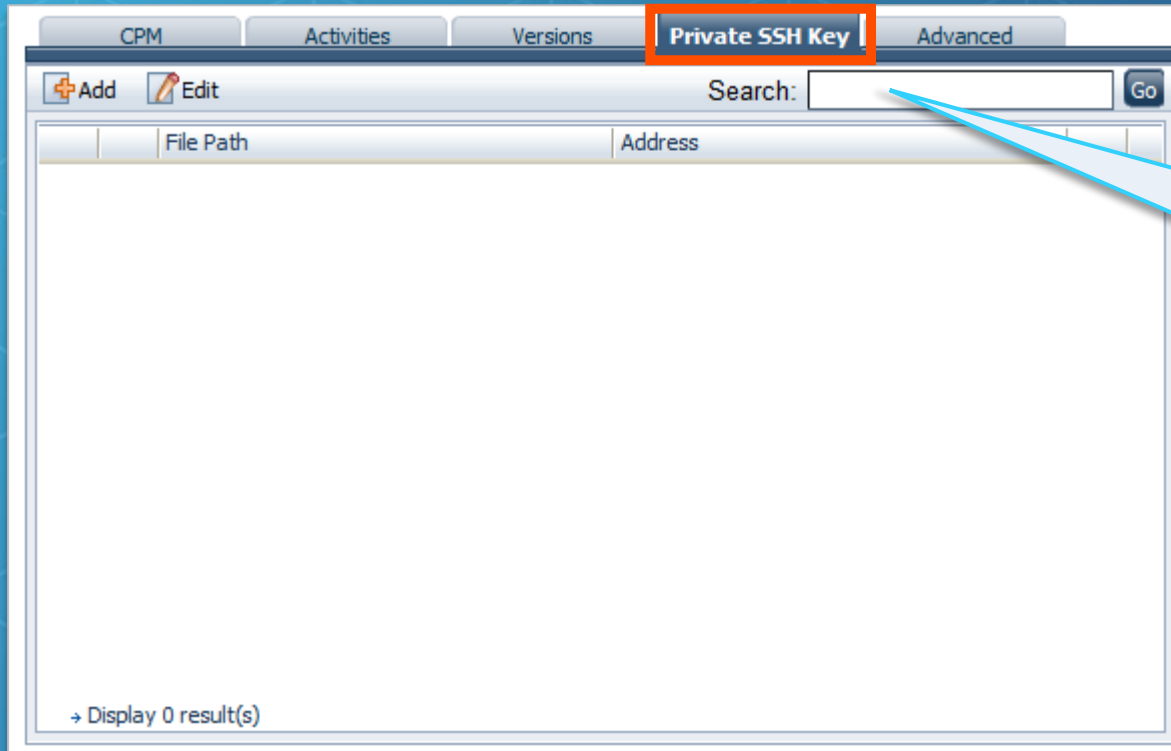
- Aug 25 2:29:44 AM PasswordManager CPM Verify SSH
- Aug 24 6:30:01 AM PTAAppl Privileged Access Event

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 PAS 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



eLearning

[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