



# CYBERARK UNIVERSITY

## PSM Load Balancing

CyberArk Training

# OBJECTIVES

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

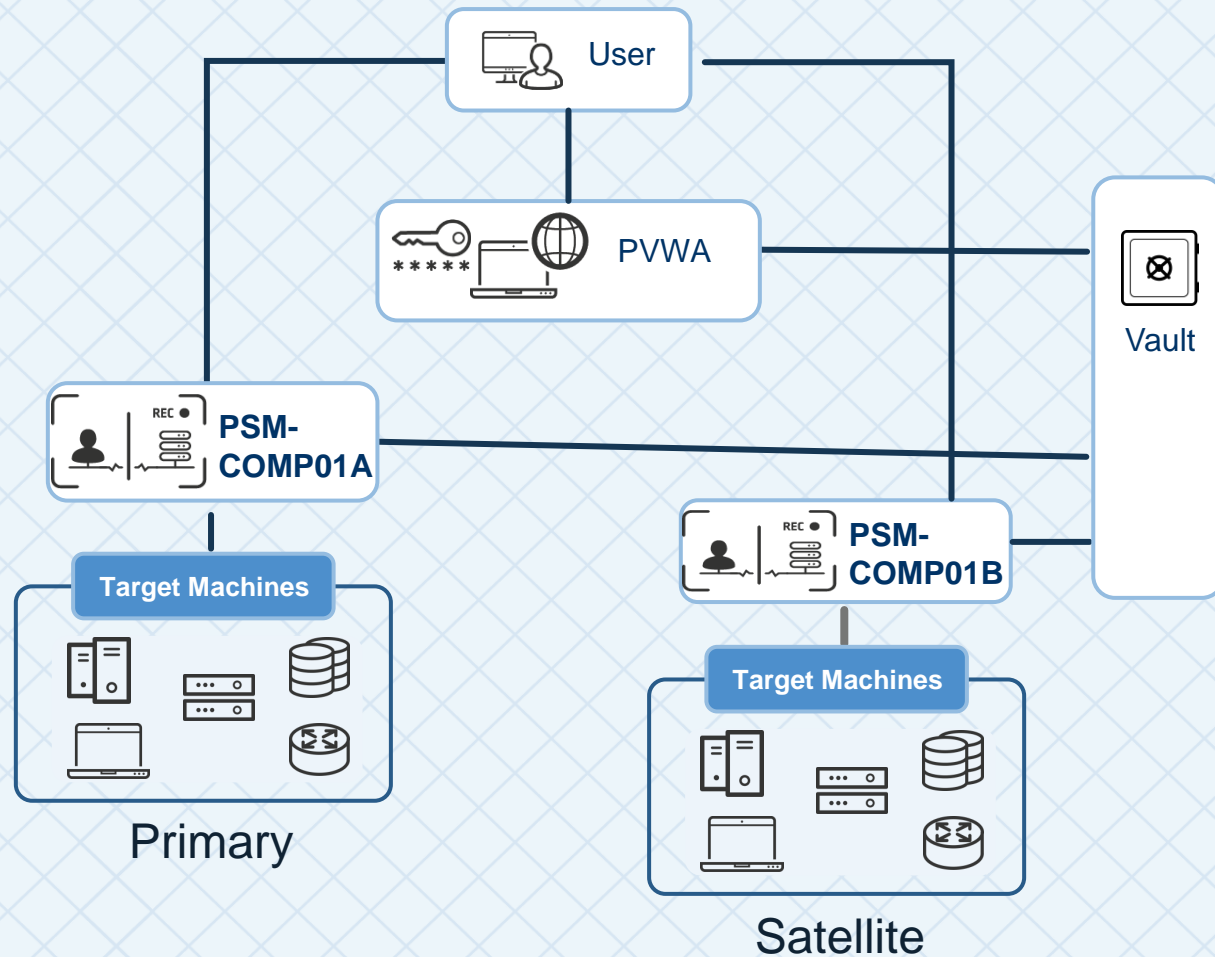
- Describe the different solutions for load balancing PSM
- Deploy PSM in Load Balancing mode

# USE CASES

# USE CASES

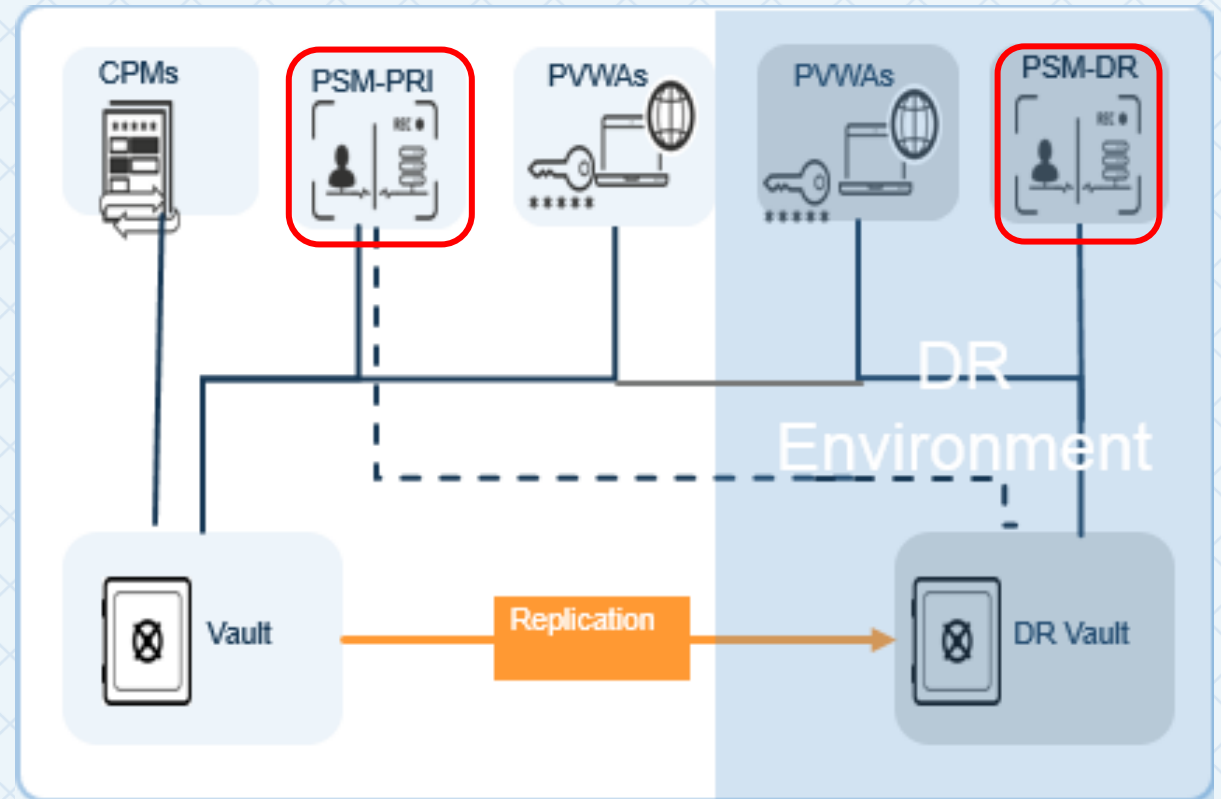
CyberArk Supports Multiple Instances of PSM Servers enabling flexibility in a deployment model

- Disaster Recovery deployment
- Fault tolerance
- Multiple sites
- Performance in a load balanced configuration



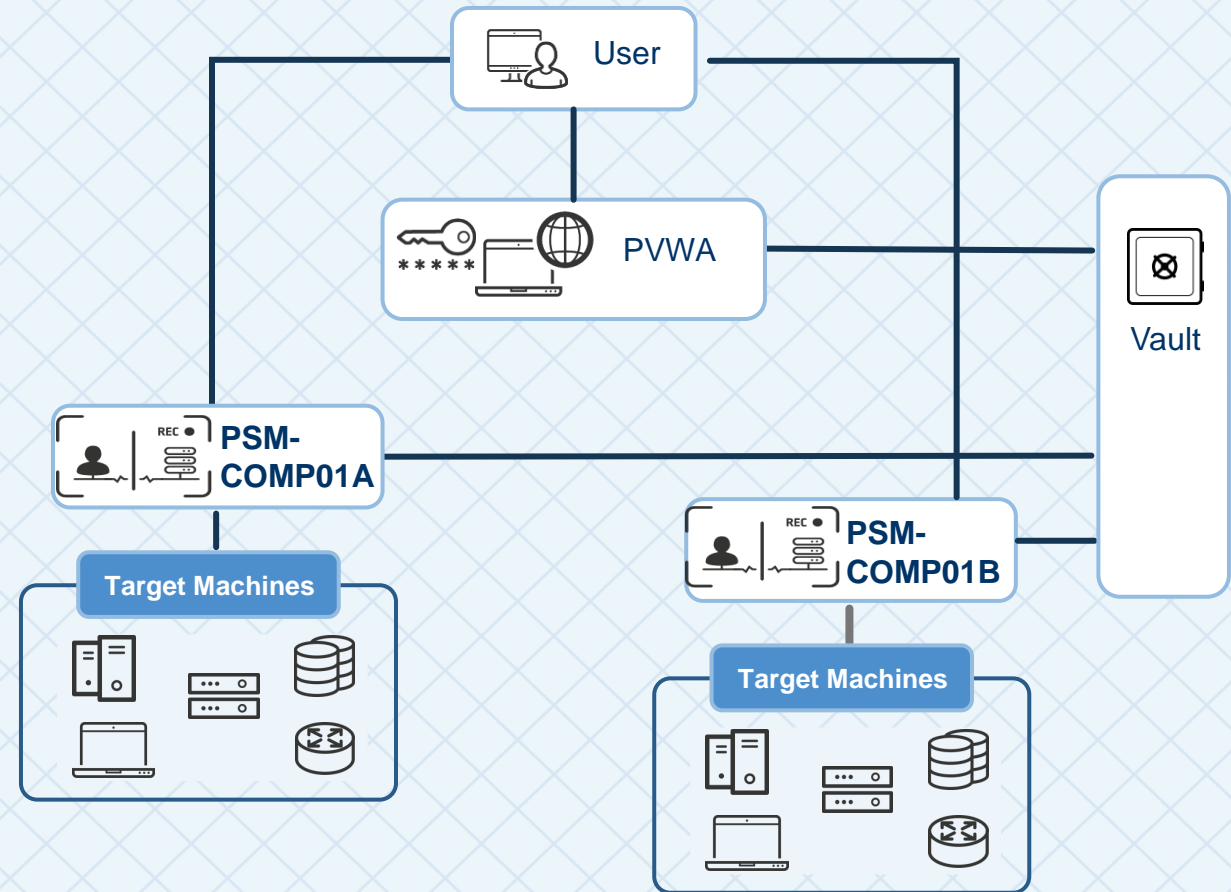
# MULTIPLE PSM SERVERS: DISASTER RECOVERY SITE

- PSM can be installed at the primary and DR site locations
- In the event of a disaster at the primary site, to enable the DR PSM the PSM SERVER ID in each Target Account Platform must be updated manually
- PSM Servers can also be configured to automatically failover to the DR vault in the event the primary Vault server is offline



## MULTIPLE PSM SERVERS – DISTRIBUTED

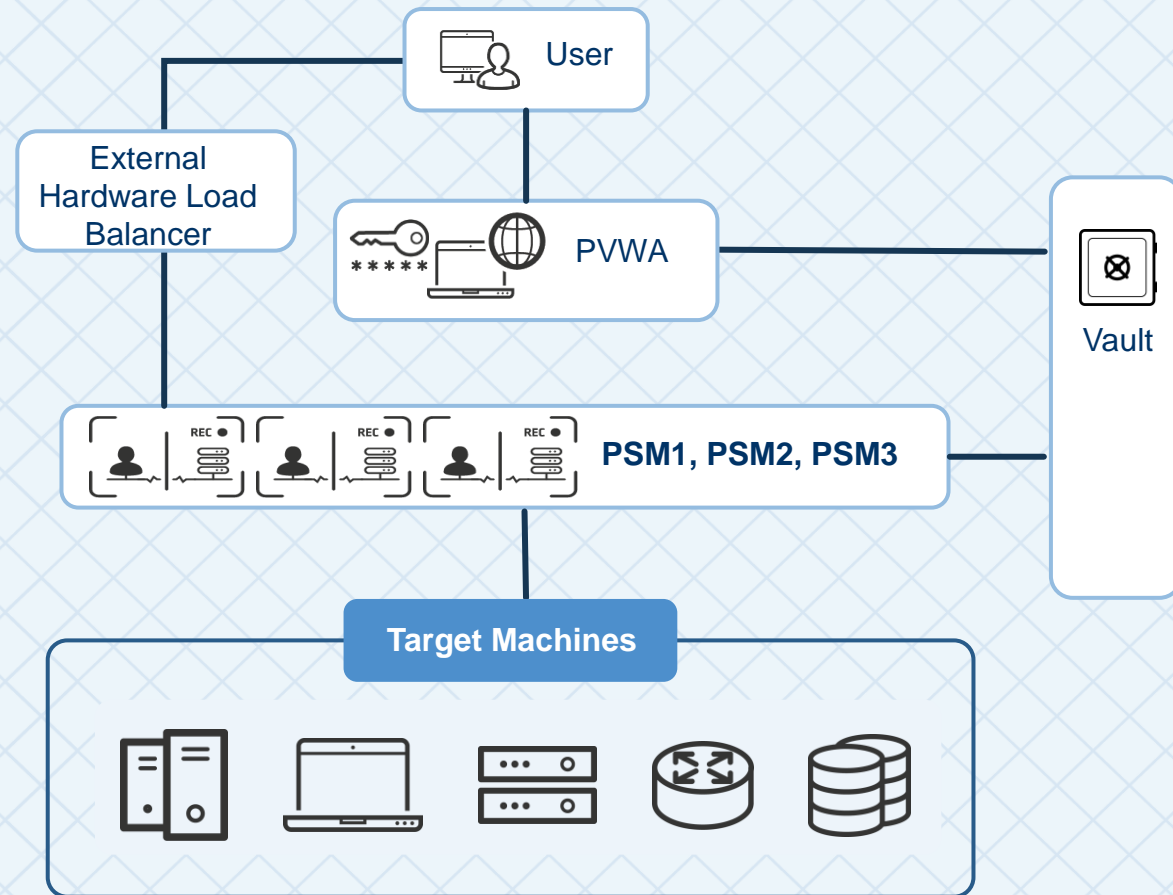
- Multiple PSMs can be active simultaneously as standalone or load balanced deployments
- Each PSM server can be assigned to specific Target Account Platforms servicing different target systems or locations
- PSM Servers should be deployed close to the target systems to reduce network traffic across WAN or MAN links





# MULTIPLE PSM SERVERS – LOAD BALANCED OR FARMED

- Multiple PSMs can be active simultaneously in a load balancing configuration
- PSMs can be load balanced using an external hardware load balancer

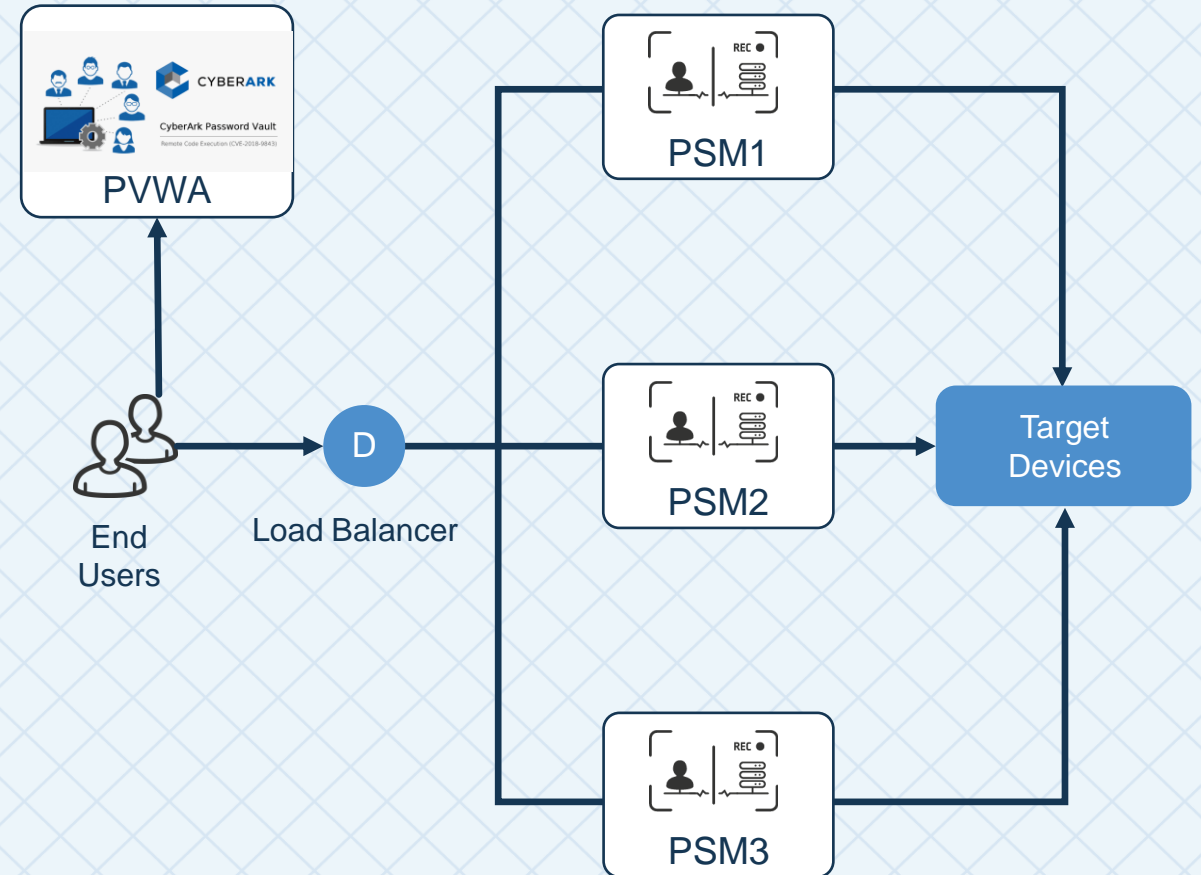


# PSM LOAD BALANCING



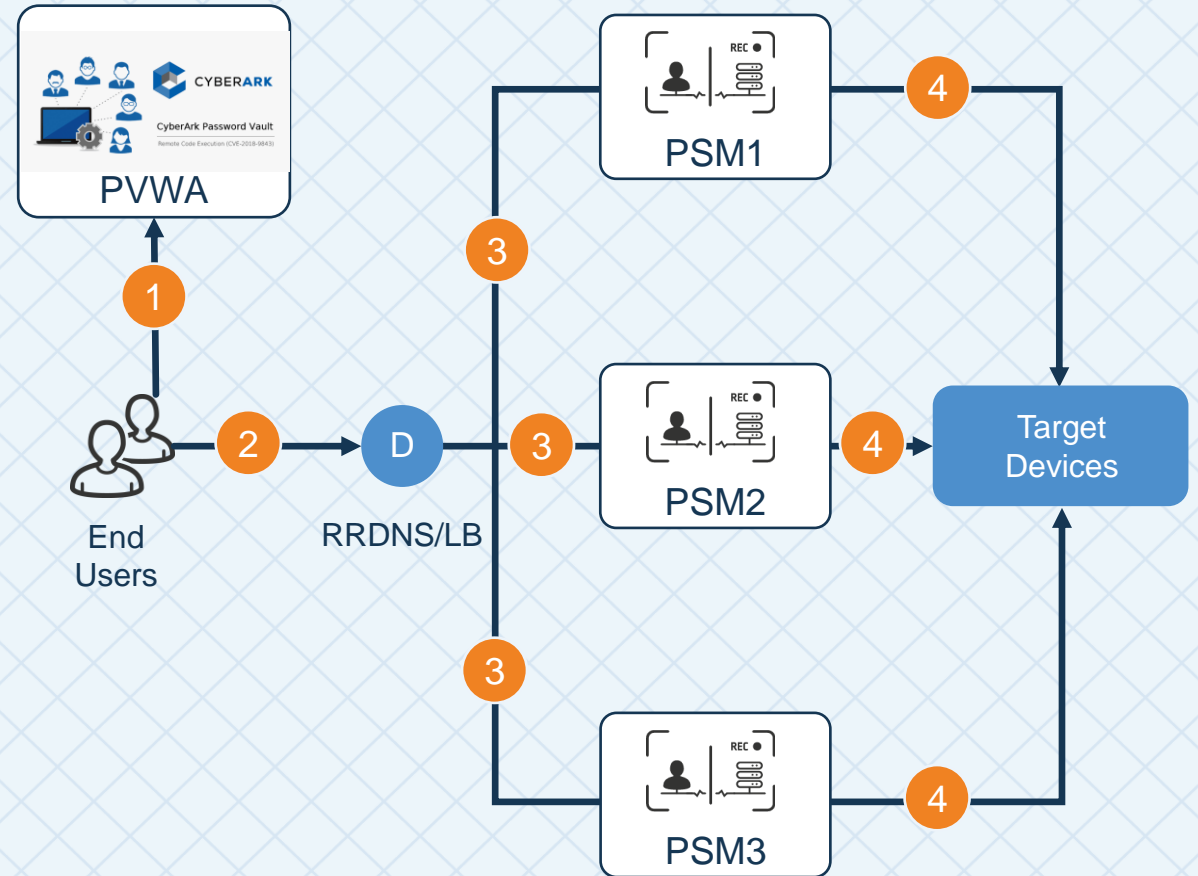
# LOAD BALANCING OPTION

- External Hardware Load Balancing:
- PSM connections are directed to a Virtual IP Address that belongs to a load balancer
- The load balancer redirects the incoming connection to a specific PSM server using a basic algorithm, much like a Round Robin DNS



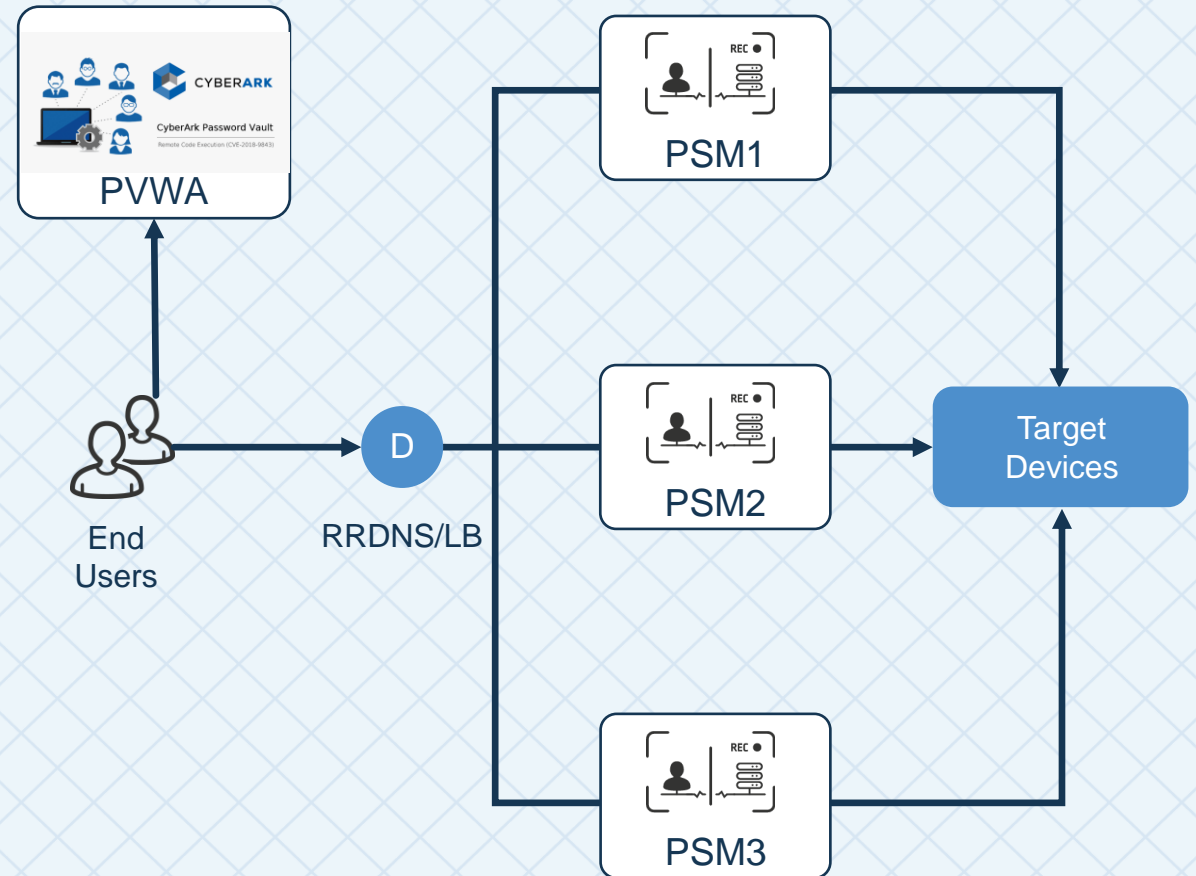
# EXTERNAL LOAD BALANCING WORKFLOW

1. It all starts from a user authenticating to the Vault via the PVWA and launching a Connection Component
2. The PVWA initiates an RDP connection sent to a Virtual IP address representing the Load Balancer
3. The Load Balancer algorithm determines which pool member will receive the request
4. The PSM connection process proceeds normally to the target device



# EXTERNAL LOAD BALANCING DEPLOYMENT

- Install individual PSMs in a standalone configuration
- Configure a 3<sup>rd</sup> party load balancer to handle incoming connections to a pool of standalone PSM servers
- In the PVWA, configure a logical PSM Server ID to represent the VIP
- Assign the logical PSM Server ID to the target platforms



# EXTERNAL HARDWARE LOAD BALANCER

	External LB
ActiveX	Yes
RDP File	Yes
RemoteApp	Yes
RDP Proxy	Yes
Supports out of domain deployments	Yes
Live Monitoring	Yes
Direct connection to PSM servers	<b>No</b> (Relies on bandwidth of LB to proxy all RDP sessions from end user to PSM)
Application layer load balancing	<b>No</b> (Potential lack of even load distribution across PSMs ("session stacking"))

# PROS/CONS –HARDWARE LOAD BALANCING

## PROS

- Simple to configure
- Supports majority of PSM capabilities (ActiveX, RDPFile, RemoteApp, RDGateway, Live Monitoring)
- Supported in out-of-domain (WORKGROUP) PSM deployments
- Fully documented on [docs.cyberark.com](https://docs.cyberark.com)
- Provides options for health monitoring of downed PSM servers (network availability, service availability)
- Live monitoring is supported

## CONS

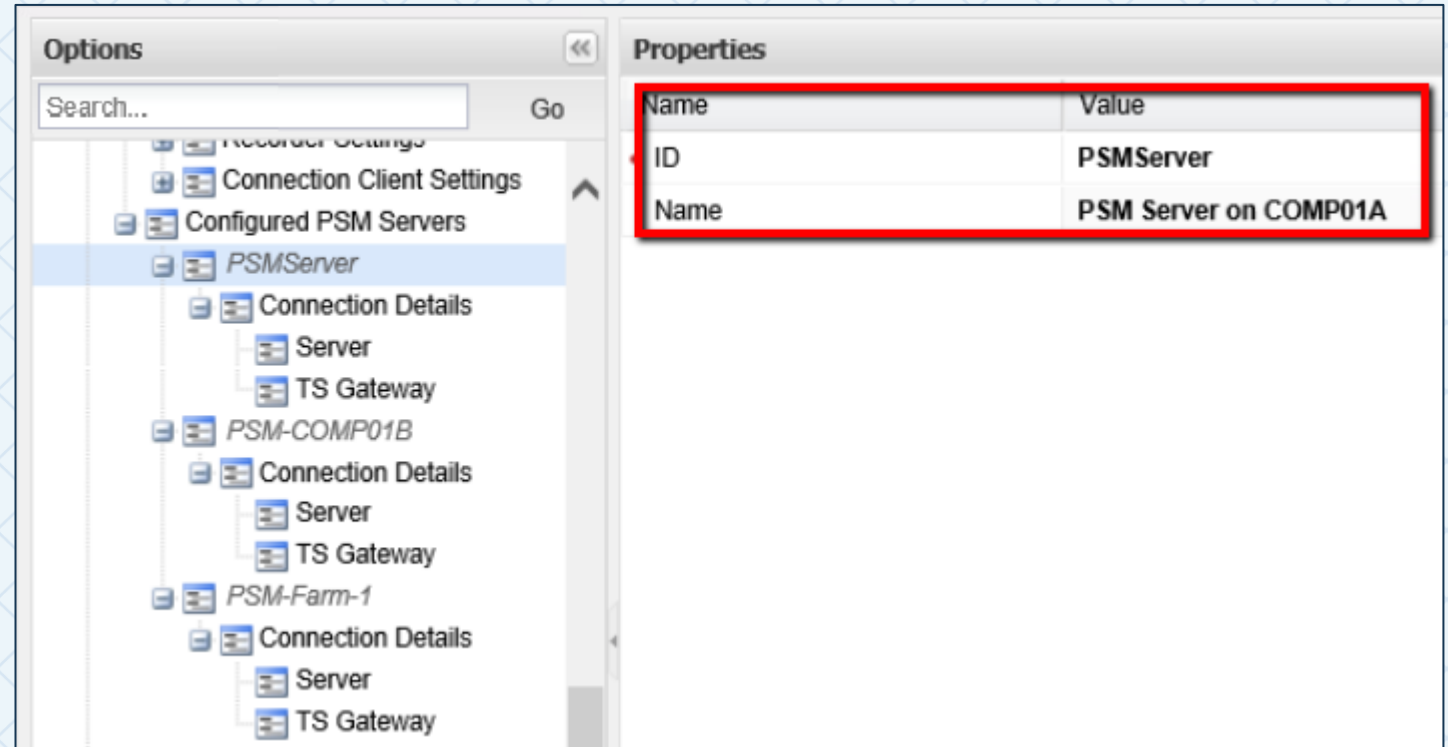
- Relies on load balancer algorithm for load distribution (“Round Robin” by default)
- Potential lack of even load distribution across PSMs (“session stacking”)
  - can be mitigated by configuring a “Least Connections” load balancing method on the load balancer instead of “Round Robin”, if supported
- Relies on throughput/bandwidth of load balancer to continuously proxy all RDP sessions from end user to PSM

# INSTALLATION AND CONFIGURATION



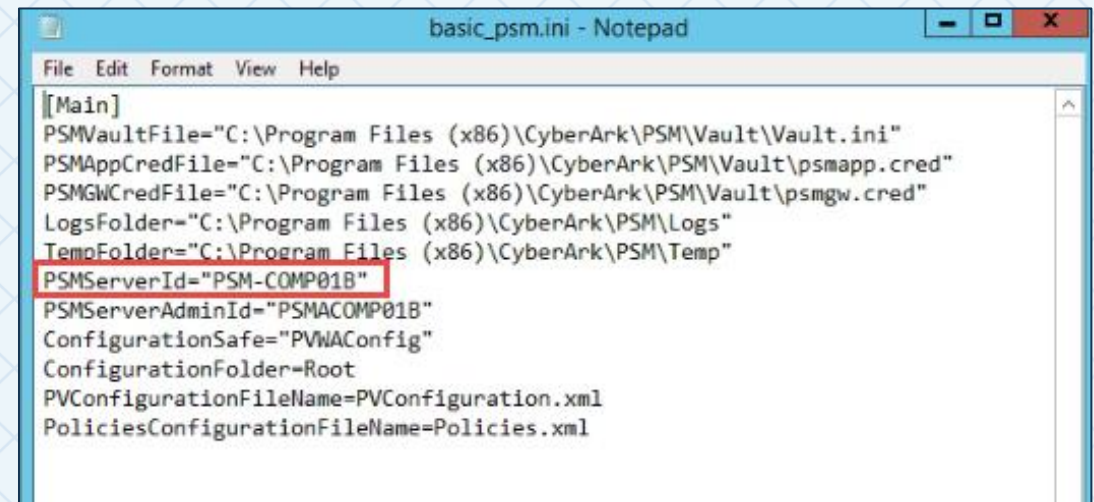
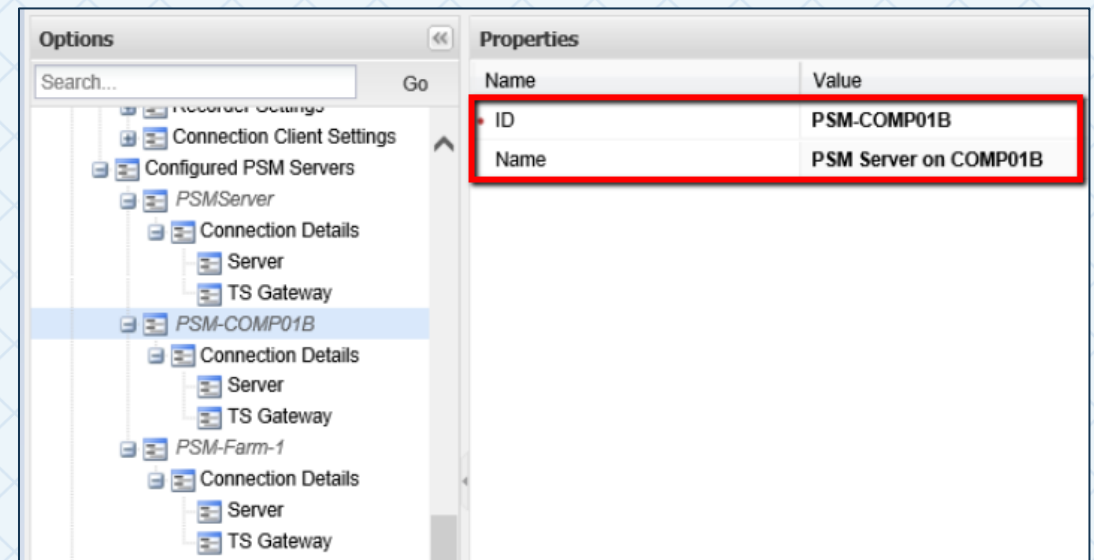
# INSTALLING MULTIPLE PSM SERVERS

- Step One: Install the first PSM. The default ID of the first PSM server is **PSMServer**



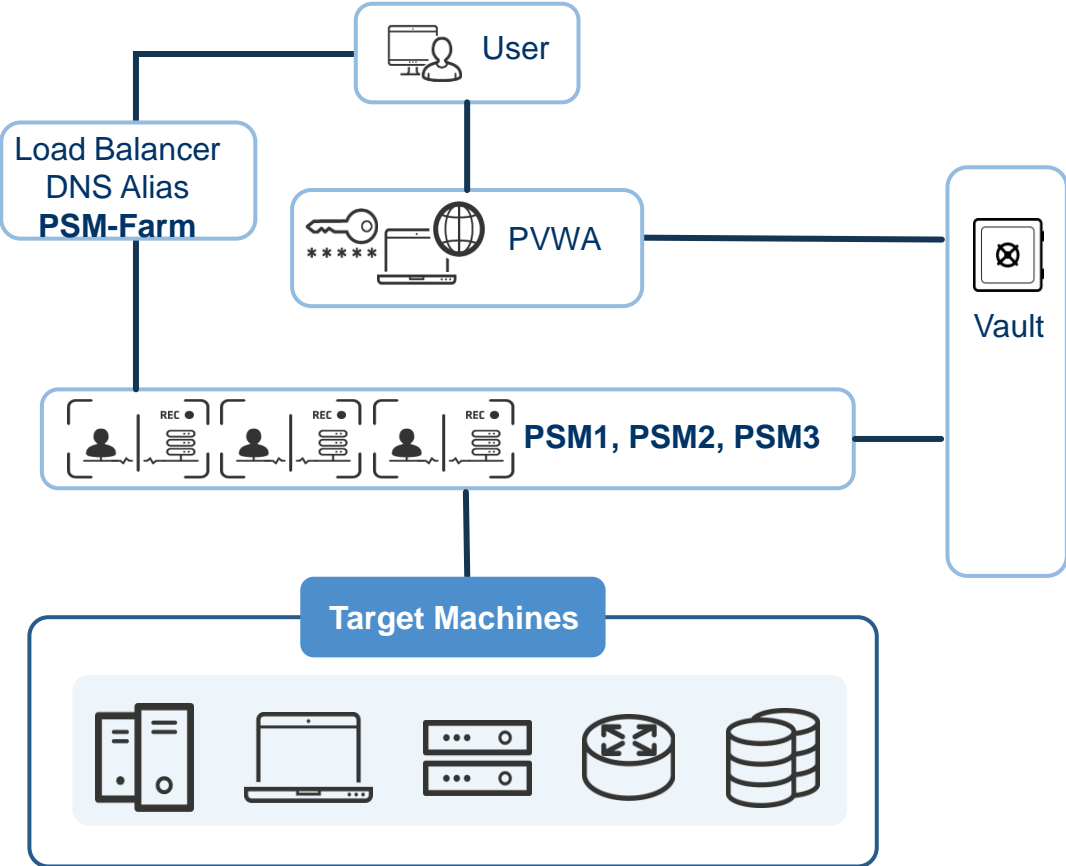
# INSTALLING MULTIPLE PSM SERVERS

- Step Two: Install additional PSM servers in identical configurations
  - Operating System
  - CyberArk software Version
  - Installation directory paths
  - Client software
- The IDs of additional PSM servers are by default **PSM-<computer name>**
- Renaming PSM servers is as easy as renaming the PSM Server ID in the PVWA, and in the PSM servers basic\_psm.ini
  - Restart the Cyber-Ark Privileged Session Manager service



# INSTALLING MULTIPLE PSMS: LOAD BALANCING

- Create a new entry for the load balanced Virtual IP, using the VIP as the server address and associate each platform with the PSM Server VIP name.



Two screenshots of the CyberArk console showing configuration steps for PSM-Farm.

**Screenshot 1: Privileged Session Management UI - PSM-Farm Properties**

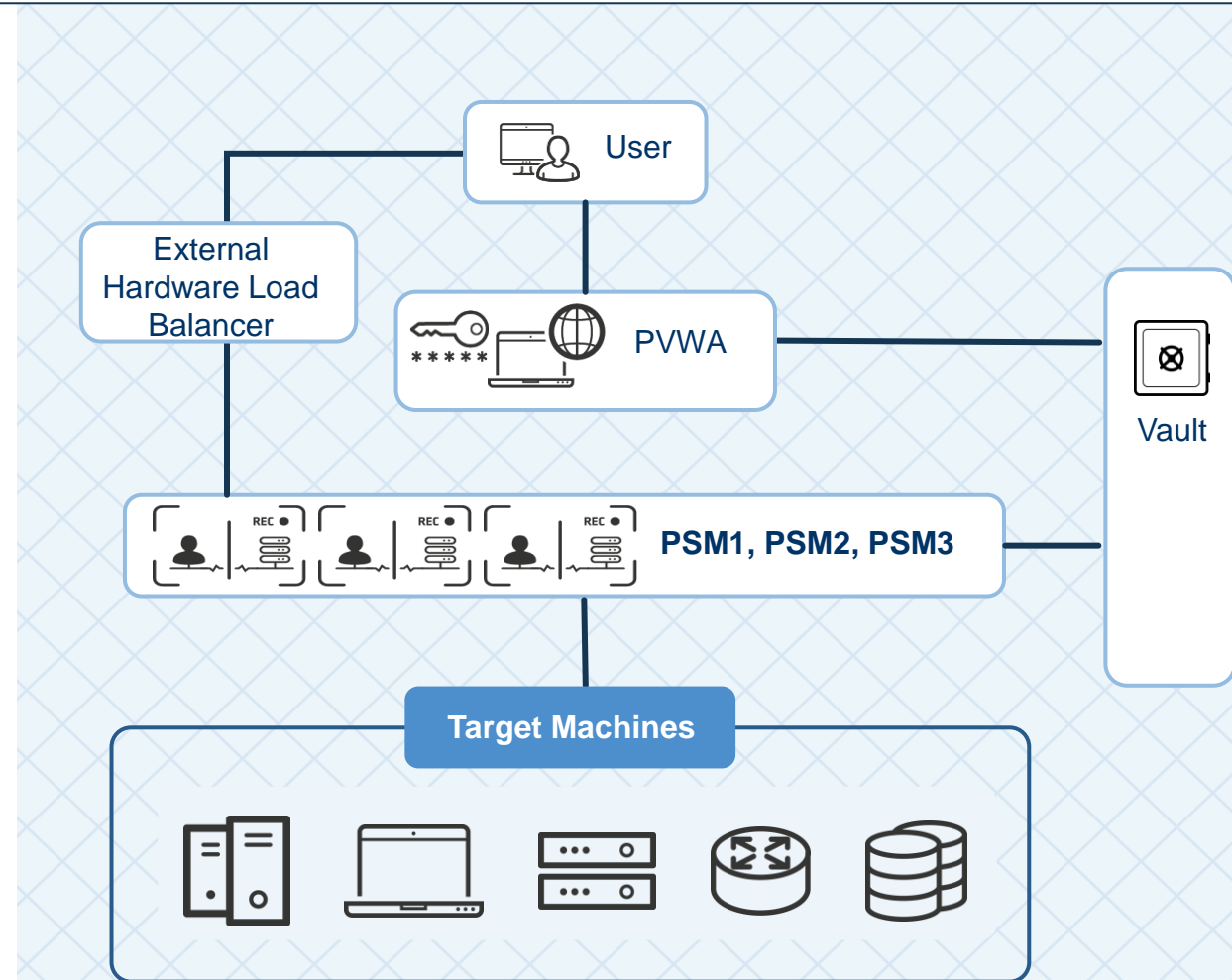
Name	Value
ID	PSM-Farm
Name	Load Balanced PSM Servers

**Screenshot 2: ACME Unix via SSH Accounts - Properties**

Name	Value
ID	PSM-Farm
SubnetPolicy	No
SessionRecorderSafe	PSMRecordings
SessionRecorderSafeRetention	180
MaxSessionDuration	-1
ShowRecordedSessionNotification	Yes
RecordedSessionNotificationDisplayTime	5
ShowLiveMonitoringNotification	Yes
LiveMonitoringNotificationDisplayTime	5

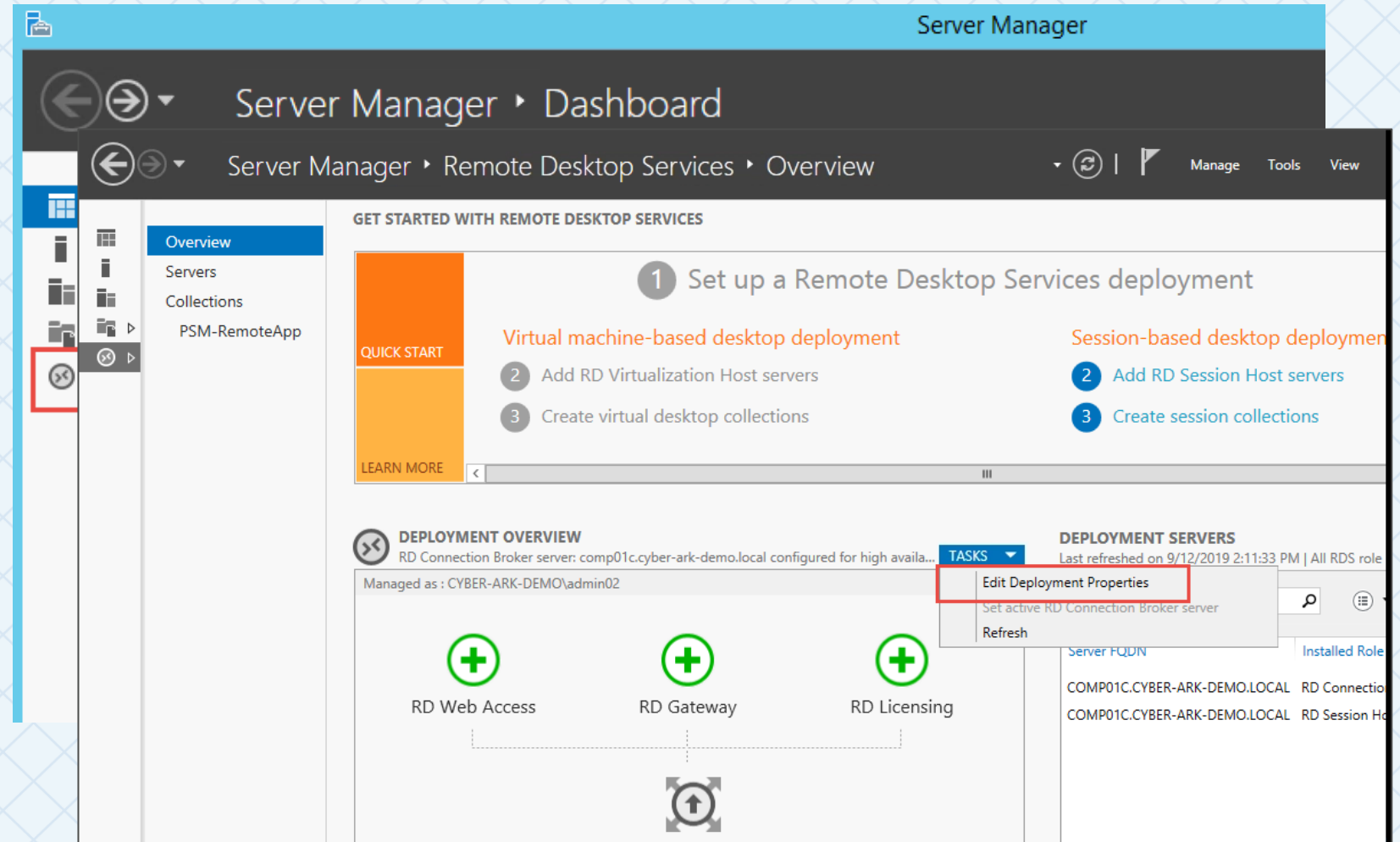
# MULTIPLE PSM SERVERS – DIGITAL CERTIFICATES

- A Digital Certificate from a Trusted Certificate Authority should be used for RDP/SSL Server Authentication
- When a load balancer is used, the Certificate must support Subject Alternative Names or SAN's to prevent Certificate Errors and allow an SSL connection to terminate at the PSM Server
- Prepare the customer to provision or acquire a Digital Certificate from a Trusted Certificate Authority
- Enable SSL passthrough to protect the communications between the load balancer and the PSM nodes
- See CyberArk Docs for more information. Search on “Example of how to configure a load balancer”



# MULTIPLE PSM SERVERS – DIGITAL CERTIFICATES

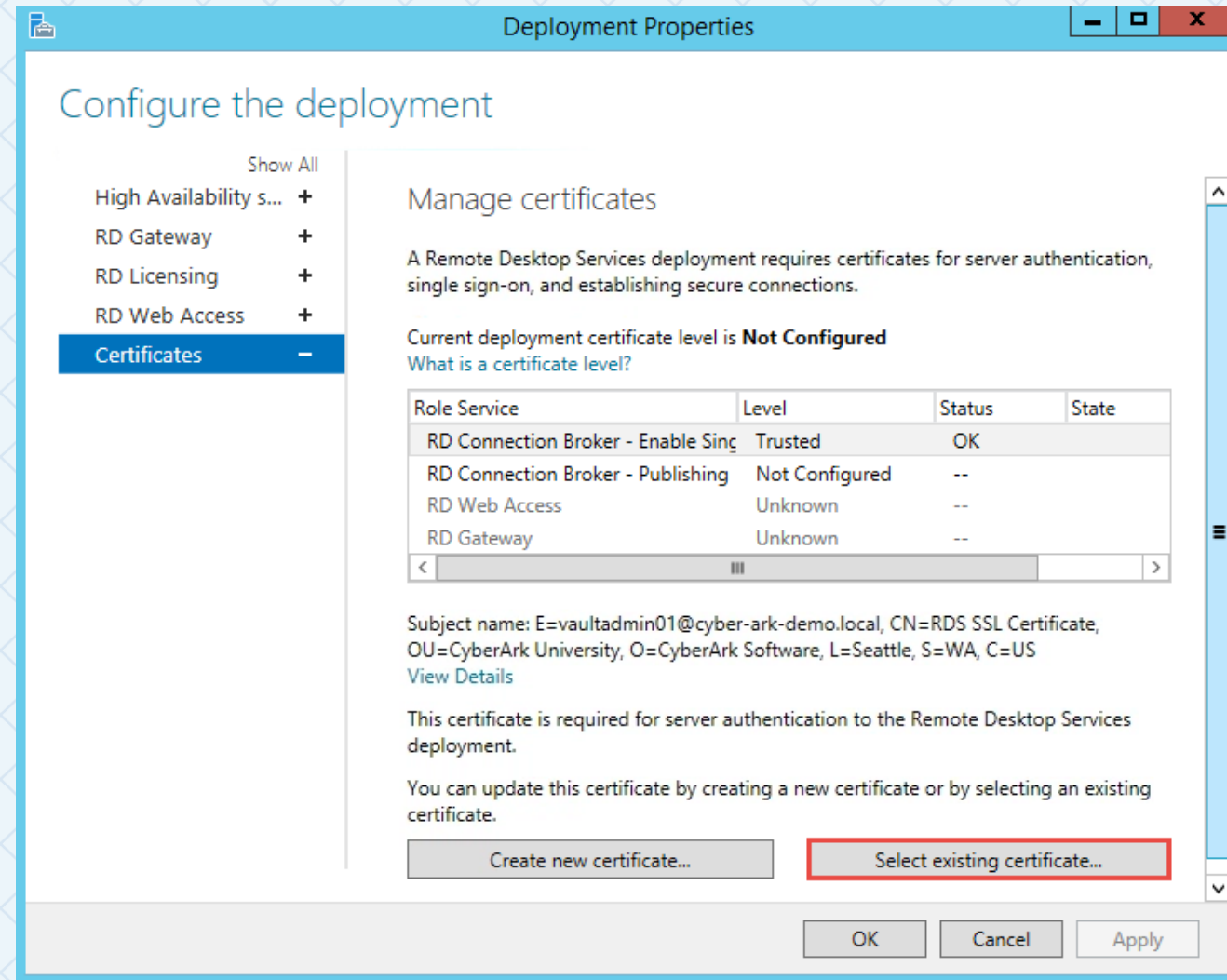
- Update the PSM Servers Remote Desktop Session Host with the new SSL Certificate
- Each PSM Server in the pool must have its own individual SSL Certificate with a Subject Alternative Name defined for the VIP





# MULTIPLE PSM SERVERS – DIGITAL CERTIFICATES

- Adding the RDS SSL certificate directly to the Windows Certificate Store will not be effective. The certificate must be updated in Server Manager RDS Deployment properties.





# MULTIPLE PSM SERVERS – DIGITAL CERTIFICATES

- Enter the password set by the Certificate Administrator for this certificate.

Select Existing Certificate

You can choose to apply the certificate that is currently stored on the RD Connection Broker server, or you can select a different certificate that is stored in a PKCS certificate file.

☐ Apply the certificate that is stored on the RD Connection Broker server

Password:

☒ Choose a different certificate

Certificate path:

C:\CyberArkInstallationFiles\comp01c\_RDS.pfx

Password:

.....

☒ Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers

# MOVING THE PSM USERS TO THE DOMAIN

- Moving the PSMConnect user to the domain is only required if ActiveX is the connection method, in a load balanced environment.
- If using RDP files or HTML5GW, there is no need to move PSMConnect to the domain.
- After creating the domain users, configure the load balancer and other PSM entries to use the new domain objects
- Note that to allow live session monitoring in a load balanced environment with RD connection broker, the PSMAdminConnect user must remain a local user

The screenshot displays the CyberArk console interface. The top panel, titled 'Account Details', shows the configuration for a 'Windows Domain Account'. The 'Name' field is set to 'PSMServer' and the 'Address' field is set to 'cyber-ark-demo.local'. The bottom panel, titled 'Options', shows a tree view of the configuration. The 'Server' node is selected, and the 'Properties' table on the right shows the configuration for the 'Server' object.

**Account Details**

Platform Name: Windows Domain Account  
Device Type: Operating System  
Safe: PSM  
Name: PSMServer  
Last verified: N/A  
Last modified: Administrator (8/21/2017 5:17:06 PM)  
Last used: Administrator (12/7/2017 5:05:43 PM)  
Username: PSMConnect  
Login To: CYBER-ARK-DEMO  
Address: cyber-ark-demo.local  
Limit Domain Access To:

**Options**

Search... Go

- Privileged Session Management UI
- Privileged Session Management
  - General Settings
  - Configured PSM Servers
    - PSMServer
    - PSM-COMP01B
    - PSM-Farm-1
  - Connection Details
    - Server
    - TS Gateway
  - PSM-COMP01C

**Properties**

Name	Value
Address	10.0.22.1
Port	3389
Safe	PSM
Folder	Root
Object	PSMServer
AdminObject	PSMAdmin

# THANK YOU