

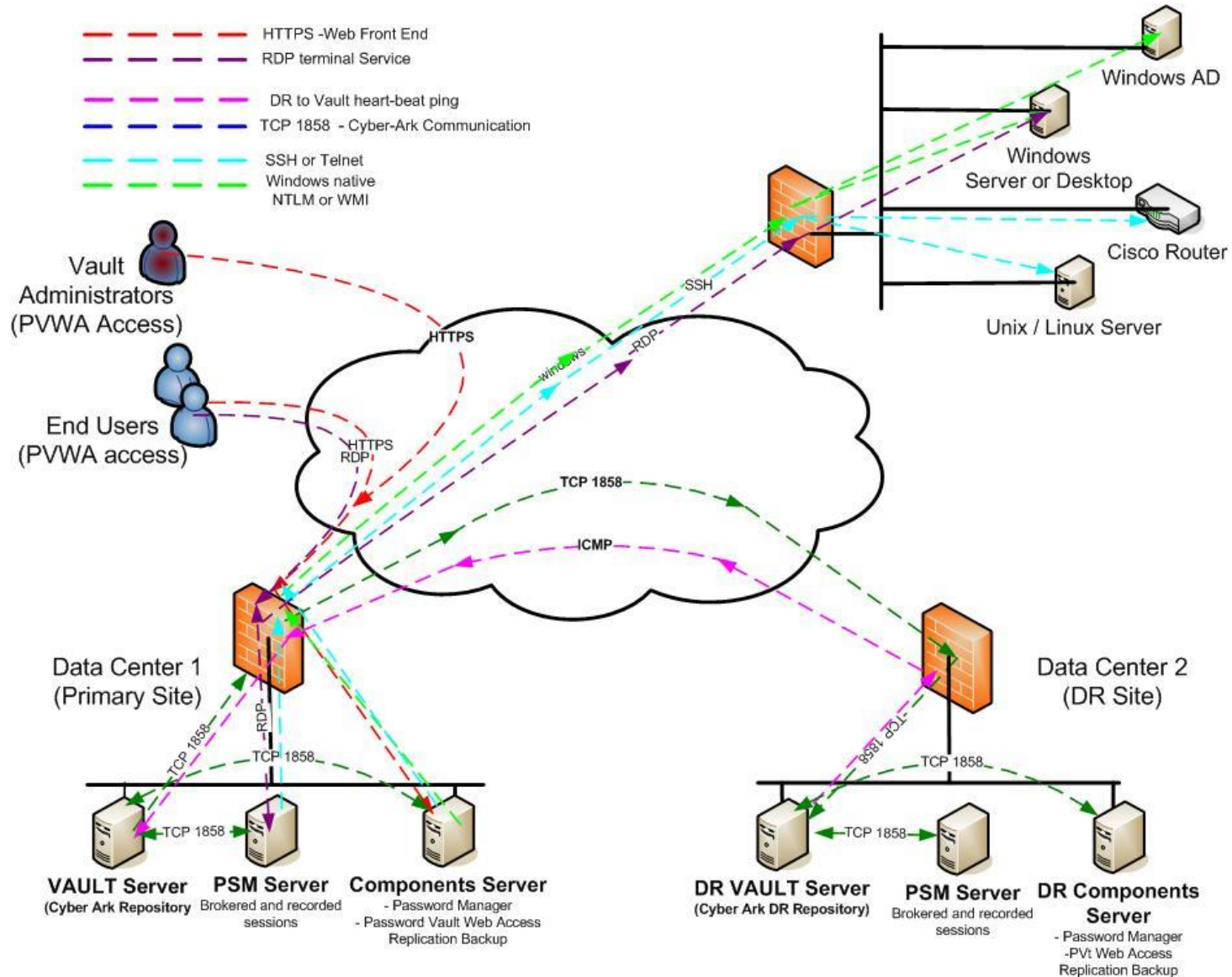


# CYBERARK UNIVERSITY

## Pre-Implementation

CyberArk Training

# PAM SUITE BASIC ARCHITECTURE



# PRIVILEGED ACCESS MANAGER SYSTEM REQUIREMENTS

# SAMPLE SYSTEM REQUIREMENTS: VAULT AND DR SERVERS


- The table lists the recommended specifications for standalone Vault servers and standalone DR Vault servers
- Hardware and software specifications for the Vault Server are detailed in the Privileged Access Manager System Requirements available online at [docs.cyberark.com](https://docs.cyberark.com)

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
<ul style="list-style-type: none"><li>• Quad core processor (Intel compatible)</li><li>• 8GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li><li>• Additional storage for PSM (optional) [1]</li></ul>	<ul style="list-style-type: none"><li>• 2X Quad core processor (Intel compatible)</li><li>• 16GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li><li>• Additional storage for PSM (optional) [1]</li></ul>	<ul style="list-style-type: none"><li>• 2X Eight core processors (Intel compatible)</li><li>• 32GB RAM</li><li>• Two 250GB SAS hot-swappable drives (15K RPM)</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li><li>• Additional storage for PSM (optional) [1]</li></ul>	<ul style="list-style-type: none"><li>• 4X Eight core processors (Intel compatible)</li><li>• 64GB RAM</li><li>• Two 500GB SAS hot-swappable drives (15K RPM)</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li><li>• Additional storage for PSM (optional) [1]</li></ul>
Hardware and software prerequisites			
For details, see <a href="#">Digital Vault Server</a>			



# SAMPLE SYSTEM REQUIREMENTS: PVWA SERVER

- The following table lists the recommended specifications for the PVWA server
- PVWA can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms
- Hardware and software specifications for PVWA servers are detailed in the Privileged Access Manager System Requirements available online at [docs.cyberark.com](https://docs.cyberark.com)

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
<ul style="list-style-type: none"><li>• Quad core processor (Intel compatible)</li><li>• 8GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 2X Quad core processor (Intel compatible)</li><li>• 16GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 2X Eight core processors (Intel compatible)</li><li>• 32GB RAM</li><li>• 2X 80GB SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 4X Eight core processors (Intel compatible)</li><li>• 64GB RAM</li><li>• 2X 80GB SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>
Software prerequisites			
<ul style="list-style-type: none"><li>• Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter)</li><li>• IIS 10.0, 8.5</li><li>• .NET Framework 4.8</li><li>• Internet Explorer 11.0</li><li>• Chrome (any version released in the last six months on Windows and Linux/UNIX)</li><li>• Firefox (any version released in the last six months on Windows and Linux/UNIX)</li><li>•  Not supported for the Monitoring module.</li><li>• PVWA can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms</li></ul>			


# SAMPLE SYSTEM REQUIREMENTS: CPM SERVER

- The following table lists the recommended specifications for the CPM server
- CPM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms
- Hardware and software specifications for CPM servers are detailed in the Privileged Access Security System Requirements available online at [docs.cyberark.com](https://docs.cyberark.com)

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
<ul style="list-style-type: none"><li>• Quad core processor (Intel compatible)</li><li>• 8GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 2X Quad core processor (Intel compatible)</li><li>• 16GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 2X Eight core processors (Intel compatible)</li><li>• 32GB RAM</li><li>• 2X 80GB SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 4X Eight core processors (Intel compatible)</li><li>• 64GB RAM</li><li>• 2X 80GB SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>
Software prerequisites			
<ul style="list-style-type: none"><li>• Windows 2019, Windows 2016, Windows 2012 R2 (Standard and Datacenter)</li><li>• .NET Framework 4.8</li><li>• CPM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms</li></ul>			

# SAMPLE SYSTEM REQUIREMENTS: PSM SERVERS

- The following table lists the recommended specifications for PSM servers
- The maximum concurrency is lower (up to 40%) when installing the PSM server on a virtual machine
- Optimal performance can be achieved on physical dedicated hardware

Small implementation (1-10 concurrent RDP/SSH sessions)	Mid-range implementation (11-50 concurrent RDP/SSH sessions)	Large implementation (51-100 concurrent RDP/SSH sessions)
Hardware Specifications: Physical Servers		
<ul style="list-style-type: none"><li>• 8 core processor (Intel compatible)</li><li>• 8GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 16 core processors (Intel compatible)</li><li>• 16GB RAM</li><li>• 2X 80GB SATA/SAS hot-swappable drives</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>	<ul style="list-style-type: none"><li>• 32 core processors (Intel compatible 2.1 GHz - 2.6 GHz)</li><li>• 32GB RAM</li><li>• 2X 250GB SAS hot-swappable drives (15K RPM)</li><li>• RAID Controller</li><li>• Network adapter (1Gb)</li><li>• DVD ROM</li></ul>
Chrome concurrent sessions		
 <ul style="list-style-type: none"><li>• When adding concurrent sessions per user, make sure to increase the default timeout per session accordingly.</li><li>• When increasing the number of Chrome sessions, regardless of PSM usage, make sure to follow best practices regarding machine CPU and server capabilities.</li></ul>		
<ul style="list-style-type: none"><li>• Maximum number of Chrome sessions per user - 5 concurrent connections</li><li>• Maximum total number of Chrome sessions per PSM server - 10 concurrent connections</li></ul>	<ul style="list-style-type: none"><li>• Maximum number of Chrome sessions per user - 7 concurrent connections</li><li>• Maximum total number of Chrome sessions per PSM server - 15 concurrent connections</li></ul>	<ul style="list-style-type: none"><li>• Maximum number of Chrome sessions per user - 10 concurrent connections</li><li>• Maximum total number of Chrome sessions per PSM server - 20 concurrent connections</li></ul>

# VAULT SERVERS SETUP

Review the document “[Digital Vault Security Standard](https://docs.cyberark.com/)” at <https://docs.cyberark.com/>:

- The Digital Vault should be installed on a dedicated physical machine (recommended) from original Microsoft installation media
- Built from the original Microsoft installation media
- No third-party software, such as anti-virus or remote management solutions
- The Digital Vault Server shall not be a member of any enterprise domain
- Isolate the Digital Vault Server, in a secure VLAN



# PRIVILEGED ACCESS MANAGER INTEGRATIONS

# LDAP INTEGRATION

- Create an LDAP Bind account with READ ONLY access to the directory
  - Have the Username, Password, and DN available
  - Interactive logon is not required
- Create four LDAP groups to serve as roles for granting access to the vault
  - Cyberark Administrators
  - Cyberark Safe Managers
  - Cyberark Auditors
  - Cyberark Users
- In support of LDAP/S, Install all relevant Root and Intermediate Certificates for the CA that issued the certificate on the directory servers to the Vault Servers
  - Update hosts file on the vault servers with directory server names
- Have a resource from the team responsible for LDAP directory servers available

# EMAIL INTEGRATION

- Have the IP address of all SMTP Gateways Available.
- Ensure that any Layer 3 firewall rules or ACLs allow communications from the Vault Servers to the SMTP Gateway
  - The Vault Server must be authorized to send SMTP messages to the SMTP Gateway
  - Schedule SMTP gateway administrator to be available during the integration
  - Please refer to the “Standard Ports and Protocols” at <https://docs.cyberark.com/>
- Have a resource from the team responsible for SMTP Gateways available

# SNMP MONITORING INTEGRATION

- Have IP Addresses of all servers that can accept SNMP traps available.
- Upload SNMP v1 or v2 MIB files.
- Have Community String available.
- Have a resource from the team responsible for SNMP servers available.

# SIEM MONITORING INTEGRATION

- Find out the relevant SIEM vendor for the organization in question.
- Have IP addresses of all servers that can accept SYSLOG information available.
- Have a resource from the team responsible for SYSLOG servers available.



# RADIUS OR RSA INTEGRATION

- Have the IP addresses of all RSA or RADIUS servers available
- Create host entries in RSA or RADIUS for all Vault servers
- Have the “secret” that was used during host entry creation available
- Have a resource from the team responsible for SYSLOG servers available.

# NTP INTEGRATION

- Have the IP addresses of all NTP servers available

# **SAMPLE AGENDA AND CONSIDERATIONS**

# SAMPLE AGENDA FOR “GETTING STARTED” - 4 DAY ENGAGEMENT

- **Onsite Day 1** – Install and perform initial configuration of the Production and DR Vaults including advanced Vault integration such as SNMP, SMTP, SYSLOG and any others the were agreed upon.
- **Onsite Day 2** – Install and perform initial configuration of the Central Policy Manager, Password Vault Web Access 1 and 2, Privileged Session Manager, Secure Replication Utility and the Private-Ark Client.
- **Onsite Day 3** – Perform advanced configuration for the CPM, PVWAs and PSM. Test CPM management on 3-5 types of the out-of-the-box plug-ins. Test PSM workflows on 3-5 types of the out-of-the-box connectors.
- **Onsite Day 4** – Troubleshoot any issues discovered during the CPM testing and PSM workflows. Perform overview session with administrators. Go over and assist in documenting the Master Policy, Access Control Model data and permission structures. Set up and go over support access and procedures.
- This agenda is intended as a general example.

# OTHER CONSIDERATIONS

- Have test accounts available for CPM testing
  - Windows local administrator
  - Windows Domain Account
  - Linux SSH or Cisco
  - Other relevant accounts
- Make sure firewalls will not interfere with communication between Cyberark servers or with clients
- Get an estimate of how many accounts will be managed and what type they might be. (Windows domain or enterprise admin, Unix root, Oracle SYS,etc.)



# SAMPLE CONTACT INFO REQUEST

Could I please have the following items so we can effectively communicate about our engagement?

Contact Name:

Contact Phone:

Contact Email:

Contact Site Location (if onsite):

# SUMMARY

This session covered:

- Reviewed general system hardware requirements
- Reviewed integration requirements
- Reviewed a sample 4 day agenda

# THANK YOU