Pre-Implementation Checklist

|  |  |  |
| --- | --- | --- |
| Check | Date |  |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer confirms that they have received the Product box which contains:   * The Product CD, containing all the software purchased as well as digital versions of the documentation. * (2) Sets of Operator and Master keys * The CyberArk License agreement |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer confirms they have been given access to the CyberArk Support Vault and are able to login and access the following safes:   * Customer Safe * CyberArk PAS Solution * CyberArk Documentation |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer has secured following dedicated servers with system levels according to the attached System Requirements document:   * 2x Vault Servers (Prod, DR) – Windows 2008 R2 SP1 64-bit Standard Edition   + The Vault servers should be installed on physical servers for security and performance purposes. If this is an issue, please contact CyberArk Professional Services management.   + .NET Framework 3.5.1 Feature Installed   + No third party software should be installed (this includes Antivirus, Spyware, Backup, Monitoring software or any patches) and the server should not be part of the domain (The server should be a clean image, rather than a normal domain image that’s been cleaned to avoid any GPO impact)   + Create Emergency Password Recovery Disk (Control Panel\User Accounts\User Accounts\Create a password reset disk)   + Following patches should be installed in addition to SP1:     - MS13-049, MS13-065     - MS12-020     - MS11-083, MS11-064, MS11-048 * 2x Front End Component Servers – Windows 2008 R2 SP1 64-bit Standard   + These servers should be built per your normal domain build instructions with all third party software you normally install and domain membership as normal   + IIS with ASP.NET should be installed with all authentication methods checked   + .NET Framework 3.5.1 Feature should be installed   + .NET Framework 4.0 package should be installed for PVWA component   + SSL Certificate should be available or installed   + RDS Service with access to an RDS Licensing server if PSM is being installed (Optional) * **(If PSMP is purchased/used)** - 2x Front End Component Servers (PSM SSH Proxy) - Red Hat Enterprise Linux 5.6, 6.4 (64-bit) or 6.5   + Redhat-lsb (32-bit version) should be installed * **(If PTA is purchased)** - 1x Front End Component Server (PTA)   + System provided as a VM image by CyberArk   + Virtual infrastructure and a VM admin resource to import the VM Image must be provided by customer   + 500 GB disk allocation |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | Event Notification Engine Integration (Optional):   * The customer provided the IP address of the SMTP server that will be utilized for Event Notification. * The customer ensured that ACL on the SMTP server is updated to allow communications from all Vault servers |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | NTP Integration (Required)   * The customer provided the IP address of the NTP server that will be utilized for time synchronization on the Vault and DR Vault servers * The customer ensured that ACL’s in the network allow for communication from all Vault and DR Vault servers to the NTP server |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | SNMP Monitoring Integration (Optional):   * The customer provided the IP address/es of all servers that can accept SNMP traps. * The customer provided community string that will be used for SNMP integration. |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | SYSLOG Monitoring Integration (Optional):   * The customer provided the IP address/es of all servers that can accept SYSLOG information * The customer provided a resource from a team responsible for the system if ArcSight or RSA enVision systems are available |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | LDAP Integration and Authentication:   * The customer has created an AD “Bind User” account with privileges to read directory of users that will be integrated into vault. * The customer has created a CyberArk Administrator, CyberArk Auditor and Cyber-Ark User groups. Recommended naming convention is gEPVr\_Administrator, gEPVr-Auditor and gEPVr\_EndUser, but if the customer has a predefined naming convention, names can be changed as long as an indication is made that it is an EPV >g<roup for >r<ole assignment for the specific (Admin, Auditor or EndUser) role * The customer will provide the Distinguished Name for the “Bind User” account and its credentials. * The customer will provide the IP address/es and Hostname/s of all Directory servers that the Vault may query from. * If SSL connection from the Vault to the Directory is required, the customer should provide a Root Certificate for the CA that issued the certificate on the directory server(s) * If wanting to perform auto-detection of local admin accounts, auto-detection of service accounts, or reconciliation of account passwords in Windows. A domain account will need to be provisioned with permissions to reset passwords of domain accounts with membership in the Local Administrators group on all servers you wish to perform reconciliation and auto-detection. Typically this account is provisioned as a Domain Admin. Note: This account should be separate from the Bind User. |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | RADIUS or RSA over RADIUS Authentication (Optional):   * The customer provided the IP address/es of all RSA or RADIUS servers. * The customer created host entries for all Vault Nodes. * The customer provided “secret” used during host entries creation |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | PKI Authentication (Optional):   * The customer provided the IP address/es of all PKI servers * The customer provided Root and Client certificates for users and Vault servers. |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer has prepared test accounts for CPM Testing (For example: a Local Administrator on a Windows server, a Root account on a UNIX server etc.). One of each type will be tested (Optional) |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer has arranged for firewall ports per the attached System Requirements document to be opened between all relevant servers. |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer has arranged for physical access to all relevant Data Centers (as needed) or access to any systems needed during implementation |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer has configured out-of-band access for the Vault servers and will maintain having out-of-band console access throughout the duration of the deployment.  Examples of out-of-band access are iLO, iDRAC, IP-KVM, etc.  RDP access is NOT considered remote out-of-band access and will not function after the Vault installation hardening process |
| \_\_\_\_\_\_ | \_\_\_/\_\_\_/\_\_\_ | The customer has made Vault Administrators, needed for training and deployment of the Vault and its components, exclusively available for the whole duration of the engagement |

Customer Project Manager or

Vault Administrator \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date of Completion \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_