VMWARE HORIZON CLOUD DEPLOYMENT – PROFESSIONAL DATASHEET

Effective October 2020

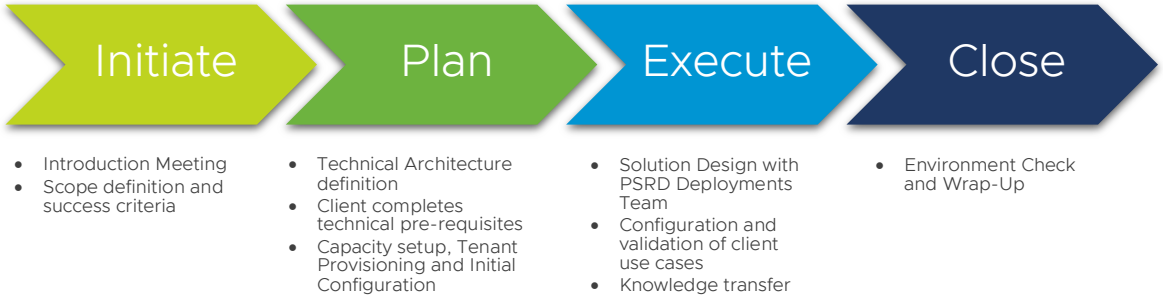
1. Service Overview

VMware will provide implementation services for one (1) **of the following services**. Please review the associated Appendix for the respective service for additional details. This project will be organized into four phases: 1) Initiate 2) Plan 3) Execute 4) Close.

- A – VMware Horizon Cloud-Hosted Provisioning
- B – VMware Horizon Cloud on Microsoft Azure

2. Engagement Timeline

The VMware Product Deployment service typically takes 4-6 weeks to fully deliver with the pre-defined scope. The estimated timeline for the engagement is outlined in the following table. The tasks defined each week can shift based on client readiness and availability of both the client and the Deployments team.



3. Change Management

Should the scope of the initiative change, VMware will document the change and provide in writing a "change order" document to the client requesting confirmation of the change and any applicable costs associated with the agreed upon change

4. Responsibilities

All VMware and Customer responsibilities are listed in the Service Deliverables section. The ownership is defined as follows:

1. **Primary Owner = VMware**: VMware is responsible for delivery of the component, with minimal assistance from the client's project team.
2. **Joint**: VMware and the client's project team are jointly responsible for delivery of the component.

3. **Primary Owner = Client**: VMware is responsible for assisting the client project team as needed to deliver the component.

5. Terms & Conditions

This Datasheet is for informational purposes only. VMWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DATASHEET. This Datasheet replaces all prior versions of the VMware Horizon Cloud Silver Datasheet. VMware may update the content of the Datasheet from time to time and the new version will apply for the future purchase of the Consulting Services referenced in this Datasheet. All VMware service engagements are governed by the VMware Professional Services General Terms and Conditions (see http://www.vmware.com/files/pdf/services/tc.pdf). If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside the United States, the VMware contracting entity will be VMware International Limited.

For More Information

More information about the VMware Horizon Cloud Silver Datasheet and related services is available from local VMware representatives and www.vmware.com/services.

About VMware Professional Services

VMware Professional Services transform IT possibilities into business outcomes. Our comprehensive portfolio of services uncovers and exploits the unique opportunities made possible by VMware technology. Drawing on our unparalleled product expertise and customer experience, we collaborate with your team to address the technical, people, process and financial considerations for IT transformation to deliver results that are positive, tangible, and material to IT and your business.

APPENDIX A – VMWARE HORIZON CLOUD-HOSTED

1. Service Assumptions

1. The customer is responsible for licensing of all operating systems, applications and software deployed on the Horizon Cloud platform.
2. Multiprotocol Label Switching (MPLS) (requires interaction with a telecommunications service provider for dedicated connectivity between client premises and the Horizon Cloud tenant environment).
3. Low-complexity applications are defined as simple applications that install in standard Windows locations, do not depend on other applications, and have limited integration with operating system components. Examples include Mozilla Firefox, Ipswitch WS_FTP, and Google Chrome.
4. Customer provides access to technical resources with expertise in the following areas:
    - Desktop engineering
    - Network/security
    - Active Directory
    - Application Management
5. Customer must provide requested information related to Active Directory for authentication.
6. Customer-specific customization for VMware Identity Manager is out-of-scope of this SOW.
7. Design, implementation, or integration of multi-domain or multi-forest configuration, or troubleshooting issues with Active Directory or group policies is out-of-scope of this SOW.
8. Modifications to the environment or troubleshooting items like Custom Images, Desktop Image Hardening, Quota Changes and VPN setup are out-of-scope of this SOW.
9. Generation, registration, implementation or troubleshooting of third-party or internal SSL certificates by VMware is out-of-scope of this SOW.
10. Deployment to clients over low-speed or high-latency networks is out-of-scope of this SOW.
11. Custom documentation, architecture diagrams or Project Management are out-of-scope of this SOW.
12. 3D or Rich Media Services integration, including vSGA/vDGA solutions, webcams / telephony solutions, Lync or other third-party collaboration products/solutions as well as implementation or integration of printers, headsets, microphones, or peripherals (USB or otherwise) is out-of-scope of this SOW.
13. Design, implementation, or integration of VMware ThinApp®, ThinPrint, Persona Management, or any other VMware product not already explicitly listed is out-of-scope of this SOW.
14. Implementation or integration of multifactor authentication technologies is out-of-scope of this SOW.
15. High Availability (HA) and Disaster Recovery (DR) setup are out-of-scope of this SOW.
16. Formal training is out of scope of this SOW; however, review of the portals will be provided throughout the configuration.
17. The scope of the project will be delivered as a packaged Service in the specified phases. Items not included as a part of the Solution Design will be considered out-of-scope.
18. VMware and the client's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis. The Deployments team will not provide a project manager as a role of this SOW.

19. All work, documentation and work product(s) will be conducted remotely during typical. VMware local business hours and will be provided in English.
20. The staffing for this SOW assumes all work will be completed within 12 weeks of project initiation. Should the duration of the engagement be extended, or should the product scope materially change, a formal change request may be adopted.
21. Statement of Work is deemed to be complete upon any of the following:
    - Completion of all service deliverables below
    - Up to a maximum of twelve (12) weeks after the initiation of Phase 2: Plan.
    - Up to a maximum of one calendar year from purchase date; SOW expires after twelve (12) months
    - If the services were purchased using PSO credits the services expire the same time the credits expire, unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension
22. Verify that KMS is available and that desktops are activating as expected.
23. The customer is responsible for configuring network connectivity to Horizon Cloud Hosted, including the setup of any VPNs.
24. The customer is responsible for verifying that the firewall is configured to allow access to and from the Horizon Cloud-Hosted environment.
25. The customer is responsible for allocating IP address space for the Horizon Cloud Hosted tenant environment in the corporate network.
26. The customer is responsible for configuring the following two networks:
    - One /24 network for desktops obtaining IPs from a DHCP server.
    - One /26 or above for a services network for placing static IP machines, such as tenant appliances, utility servers, such as Active Directory, file servers, and application servers.
27. Access method to Horizon Cloud-Hosted desktops must be identified (i.e. from the trusted corporate network only and/or allow direct access from the Internet).
28. Customer must provide requested information related to Active Directory for authentication.
29. Use of either PCoIP or BLAST or BLAST Extreme as the display protocol has been identified.
30. Any feature not listed in Services Deliverables is out of scope, unless discussed and agreed to with the Product Deployment Team prior to purchase.

2. Service Deliverables

ID	Description	Tool/Deliverable	Primary Owner	Comments
Phase 1: Introduction and Project Kickoff				
1.1	Register for MyVMware Id on myvmware.com	My VMware Access	Client	Required to access resources and Client Downloads

1.2	Review datasheet	Datasheet	Client	Understand service assumptions and scope
1.3	Discuss Technical Architecture and Deployment Workbook requirements	Online Deployment Workbook	VMware	Goes over Datacenter preference, VPN Setup and architecture
1.4	Identify Desktop OSs and Models for implementation as well as additional features	Images for Desktop Deployment	VMware	Discuss Desktops to be implemented out of the supported models
1.5	Complete and Submit the online Deployments Workbook with the required architecture and desktop information	Online Deployments Workbook	Client	Online Deployments Workbook required for tenant provisioning
1.6	If applicable, return 3rd Party SSL Cert with Private Key for Tenant Appliance Provisioning	3rd Party SSL Cert with Private Key	Client	3rd Party SSL Cert required in case of Horizon Cloud Tenant being externally available
Client requirements to proceed to the Network setup and Capacity Order Phase				
1.7	Complete and Submit Technical Architecture Deployment Workbook as well as 3rd Party SSL Cert	Architecture and Network Requirements	Client	Client certifies completion and comes prepared to Design phase
Phase 2: Network setup and Capacity Order				
2.1	Network Design implementation and VPN configuration	VPN and architecture configuration	Joint	VPN and architecture configuration for Horizon Cloud access and functionality
2.2	Provision Tenant Appliance and order capacity	Horizon Cloud Tenant Appliance	VMware	Tenant Appliance and capacity are setup after receiving Deployments Workbook
2.3	Validate Tenant Appliance Access externally (if applicable)	Environment Access	VMware	
2.4	Validate necessary Desktop Images have been uploaded in the environment	Desktop Images	VMware	
2.5	Modify monitor.ini File on the Desktop Images for connection to Tenant Appliance	Connectivity between Desktops and Tenant	VMware	File will contain IP Addresses to directly communicate with the Tenant Appliance
2.6	Validate Tenant Appliance access from desktop Images	Connectivity between Desktops and Tenant	VMware	

2.7	Bootstrap Desktop Images	Tenant Appliance Certificate	VMware	Adds Tenant certificate for DaaS Agent – Appliance connection
2.8	Verify Gold Patterns have up to date Agents	DaaS, View and Health Agents	VMware	Verify Gold Pattern has up to date View, DaaS & Health Agents
2.9	Discuss Display Protocols - PCOIP, BLAST and BLAST Extreme	Display Protocols	VMware	Supported Display Protocol(s) for Desktop and Application access
2.10	Summarize pre-work, next steps and schedule handoff for Phase 3	Client action items and Handoff call	VMware	Handoff for Configuration will be scheduled with the Deployments Team
Client requirements to proceed to the Configuration Phase				
2.11	Provision Domain Bind Account	Domain Bind Account	Client	Active Directory Integration for Environment Access
2.12	Provision Domain Join Account	Domain Join Account	Client	Account for joining Desktops to the Domain
2.13	Identify Display Protocol(s) for Desktop and Application access	Identify Display Protocol(s) from PCOIP, BLAST and BLAST Extreme	Client	
2.14	Set up necessary Licensing for Desktops and Applications	Desktop and Application licenses	Client	VMware will only provide validation of the desktops. All licensing requirements will be completed by client
2.15	Finalize Project Scope and return signed solution design document	Solution Design Document	Client	Scope of project cannot be modified without agreed change control
Phase 3: Configuration and Knowledge Transfer				
3.1	Configure Active Directory Integration & Sync	Active Directory Integration	Joint	Configure Domain Bind for LDAP Access to Admin & Desktop Portals
3.2	Configure AD Groups for Administrative Accounts	AD Group sync for Administrators	Joint	AD Groups for access to Admin Portals
3.3	Configure AD Groups for User Accounts	AD Group sync for Administrators	Joint	AD Groups for access to User Desktop Portal
3.4	Validate Access to all Portals	Portal Access	VMware	Access to Admin, Helpdesk and Desktop Portals
3.5	Discuss Best Practices for the following: • Domain Bind • Domain Join & Desktop Naming • Images & Gold Patterns • Applications assignment • Miscellaneous Horizon Cloud Management	Best Practices for Horizon Cloud Deployment	VMware	

3.6	Define up to two use cases for Deployment	Use Cases	Joint	
3.7	Assist in up to 3 Image Designs	Convert Images to Gold Patterns	Joint	Assist in design and conversion of up to 3 images
3.8	Assist in creation of up to 3 Desktop Pools	Desktop Pools	Joint	Assist in creating Static or Floating Desktop Pools
3.9	Assignment using Configured Desktop Pools	Desktops Assignment	Joint	
3.10	Validate desktops are accessible from Windows & Mac workstations	Multi-Platform access	Joint	
3.11	Demonstrate Editing Desktop Images and Re-sealing a Gold Pattern to end users	Edit & Re-publish Gold Pattern	Joint	Edit as well as re-seal a Gold Pattern and validate changes by pushing to test user
3.12	Discuss Application Assignments and identify low complexity applications	Application use case	Joint	Discuss typical use cases and Best Practices for Application Assignment
3.13	Discuss typical use cases and Best Practices for Application Assignment	Identify Apps for assignment	Joint	Identify up to 3 low-complexity applications
3.14	Assistance with up to 5 low-complexity applications on a Gold Pattern	Low complexity App assignment	Joint	Assist in deploying up to 5 low-complexity applications
3.15	Optimization and configuration of up to 1 RDS Host Server image with up to 5 low complexity applications installed to be used for desktops	RDSH Applications	Joint	
3.16	Installation of Dynamic Environment Manager	DEM Install	VMware	Assist with Installation and Configuration of Dynamic Environment Manager
3.17	Assist in creating up to 1 User Configuration in Dynamic Environment Manager	DEM Configuration	Joint	User Configuration in VMware DEM
3.18	Assist in creating up to 3 application profiles in Dynamic Environment Manager	DEM Configuration	Joint	Application Configuration in VMware DEM
3.19	Assist in setting up WS1 Access Connector	Connector setup for AD Integration	Joint	Workspace ONE Access
3.20	Assist in Directory Integration of VMware WS1 Access	AD Integration	Joint	Workspace ONE Access
3.21	Assist in Integrating Horizon Cloud with VMware Workspace ONE Access	Horizon Cloud SSO with VMware Workspace ONE	Joint	Integrate Horizon Cloud with existing tenant of VMware Workspace ONE

3.22	Create entitlements for Horizon Cloud desktops of up to 2 desktops pools in Workspace ONE Access	Desktop entitlements	Joint	Add user entitlements in Workspace ONE for desktops
3.23	Configure Single Sign-on for Horizon Cloud desktops from Workspace ONE Access	Single Sign on for desktops	Joint	Validate Single Sign-on for desktops in Workspace ONE Access
3.24	Workspace ONE Access as Trusted IDP for a Third party IDP	Third Party IDP Integration	Joint	Includes testing for up to 3 apps
3.25	Assist with integration of desired applications	Workspace ONE Access	Joint	10 integration units may be used according to the Application Integration Units table in Section below
Phase 4: Environment Check and Wrap-Up				
4.1	Assist in adding second Admin account for up to two Images for Gold Patterns	Desktop backup Admin Access	VMware	The account will act as a backup in case Sysprep disables the primary local admin account
4.2	Assist in OS optimization of up to two Images using VMware OS Optimization Tool	OS Optimization	Joint	OS optimization of Desktop Images for Gold Patterns
4.3	Validate KMS Server exists and desktops are being validated after setup is complete on client side	Desktop validation	Client	VMware will only provide validation of the desktops. All licensing requirements will be completed by client
4.4	Assist in Basic and Advanced GPO Optimization by providing ADM templates	GPO Optimization	Joint	VMware will only provide ADM templates for Group Policies
4.5	Go over RDP Access for Admins to Base Images	RDP Access	VMware	RDP Access is helpful in accessing base images using and Admin Account.
4.6	Discuss Virtual Machine and Usage Report Sections	Virtual Machine and Usage Report	VMware	These Sections go over Statistics in the Console
4.7	Discuss Lakeside Software as a troubleshooting option	DEM Configuration	VMware	Discuss Lakeside Software as a troubleshooting option
4.8	Discuss View Agent Logs	View Agent and PCOIP logs	VMware	Discuss location and keywords to check in View Agent Logs. Discuss PCOIP logs as well
4.9	Discuss DaaS Agent Logs	DaaS Agent Logs	VMware	Discuss location and keywords to check in DaaS Agent Logs as well as changing logging level
4.10	Go Over Support Options	Post Deployment Support	VMware	Go over Support Policies and Procedures as well as ticket creation

3. App Integration Units

Units	Integration Type	Comments
1	• Standard Enterprise Web Application	Per Application
2	• Third-Party Web Application • Internally Developed Web Application	Per Application
3	• VMware View Integration • VMware ThinApp Integration • Citrix XenApp Integration • Office 365 Integration	Per Connection Broker / Connection Server
4	• Native Application One-Touch SSO	Per Native Application

APPENDIX B – VMWARE HORIZON CLOUD ON MICROSOFT AZURE

1. Service Assumptions

1. The customer is responsible for licensing of all operating systems, applications and software deployed on the Horizon Cloud platform.
2. ExpressRoute (requires interaction with a telecommunications service provider for dedicated connectivity between client premises and the Horizon Cloud tenant environment).
3. Low-complexity applications are defined as simple applications that install in standard Windows locations, do not depend on other applications, and have limited integration with operating system components. Examples include Mozilla Firefox, Ipswitch WS_FTP, and Google Chrome.
4. Customer provides access to technical resources with expertise in the following areas:
    - Desktop engineering
    - Network/security
    - Active Directory
    - Application Management
5. Customer must provide requested information related to Active Directory for authentication.
6. Customer-specific customization for VMware Identity Manager is out-of-scope of this SOW.
7. Design, implementation, or integration of multi-domain or multi-forest configuration, or troubleshooting issues with Active Directory or group policies is out-of-scope of this SOW.
8. Modifications to the environment or troubleshooting items like Custom Images, Desktop Image Hardening, Quota Changes and VPN setup are out-of-scope of this SOW.
9. Generation, registration, implementation or troubleshooting of third-party or internal SSL certificates by VMware is out-of-scope of this SOW.
10. Deployment to clients over low-speed or high-latency networks is out-of-scope of this SOW.
11. Custom documentation, architecture diagrams or Project Management are out-of-scope of this SOW.
12. 3D or Rich Media Services integration, including vSGA/vDGA solutions, webcams / telephony solutions, Lync or other third-party collaboration products/solutions as well as implementation or integration of printers, headsets, microphones, or peripherals (USB or otherwise) is out-of-scope of this SOW.
13. Design, implementation, or integration of VMware ThinApp®, ThinPrint, Persona Management, or any other VMware product not already explicitly listed is out-of-scope of this SOW.
14. Implementation or integration of multifactor authentication technologies is out-of-scope of this SOW.
15. High Availability (HA) and Disaster Recovery (DR) setup are out-of-scope of this SOW.
16. Formal training is out of scope of this SOW; however, review of the portal will be provided throughout the configuration.
17. The scope of the project will be delivered as a packaged Service in the specified phases. Items not included as a part of the Solution Design will be considered out-of-scope.
18. VMware and the client's project management will work closely together to ensure that project scope remains consistent and issues are resolved on a timely basis. The Deployments team will not provide a project manager as a role of this SOW.

19. All work, documentation and work product(s) will be conducted remotely during typical. VMware local business hours and will be provided in English.
20. The staffing for this SOW assumes all work will be completed within 12 weeks of project initiation. Should the duration of the engagement be extended, or should the product scope materially change, a formal change request may be adopted.
21. Statement of Work is deemed to be complete upon any of the following:
    - Completion of all service deliverables below
    - Up to a maximum of twelve (12) weeks after the initiation of Phase 2: Plan.
    - Up to a maximum of one calendar year from purchase date; SOW expires after twelve (12) months
    - If the services were purchased using PSO credits the services expire the same time the credits expire, unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension
22. The customer is responsible for purchasing Microsoft Azure hosting for setup with Horizon Cloud.
23. The customer is responsible to attach their own Microsoft Azure subscription to the Horizon Cloud Service.
24. The customer is responsible for determining their Microsoft Azure deployment model and the subscription type.
25. Verify that the Network Security Group is configured to allow access to and from the Horizon Cloud environment.
26. Customer provides the necessary information for the Horizon Cloud environment to be configured properly.
27. The customer is responsible for allocating IP address space for the Horizon Cloud tenant environment in the corporate network.
28. The customer is responsible for configuring 3 non-overlapping subnets reserved in CIDR format (created on VNet during Horizon Cloud deployment)
    - Management subnet – /28 minimum
    - Tenant subnet – /28 minimum with /24 - /22 preferred, based on number of RDS servers
    - DMZ subnet – /28 minimum when Unified Access Gateway is deployed (optional)
29. Access method to Horizon Cloud desktops must be identified. From the trusted corporate network only, or allow direct access from the Internet.
30. Any feature not listed in Services Deliverables is out of scope, unless discussed and agreed to with the Product Deployment Team prior to purchase.

2. Service Deliverables

ID	Description	Tool/Deliverable	Primary Owner	Comments
Phase 1: Introduction and Project Kickoff				
1.1	Register for MyVMware Id on myvmware.com	My VMware Access	Client	Required to access resources and Client Downloads
1.2	Review datasheet	Datasheet	Client	Understand service assumptions and scope

1.3	Discuss Technical Architecture and Deployment Workbook requirements	Online Deployment Workbook	VMware	Goes over Datacenter preference, VPN Setup and architecture
1.4	Identify RDSH OS versions for implementation	Images for Deployment	VMware	Discuss RDSH Servers to be implemented out of the supported models
1.5	Complete and Submit the required architecture and deployment information requested by VMware	Architecture and Deployment information	Client	Online Deployments Workbook required for tenant provisioning
Client requirements to proceed to the Network setup and Capacity Order Phase				
1.7	Determine and obtain Microsoft Azure deployment model and subscription	Microsoft Azure Subscription	Client	Client obtains their Microsoft Azure deployment model and the subscription type from Microsoft
Phase 2: Plan				
2.1	Validate access to VMware Horizon Cloud Admin Portal	Admin Portal Access	VMware	
2.2	Deploy a Node for VMware Horizon Cloud on Microsoft Azure	Horizon Cloud Node on Azure	Joint	Add Horizon Cloud Node and capacity on Microsoft Azure
2.3	Validate necessary Images uploaded in the environment	Images	VMware	
2.4	Validate Horizon Cloud Portal access from Images	Connectivity between Images and Admin Portal	VMware	
2.5	Validate Images have up to date Agents	DaaS and View Agents	VMware	Verify Images have up to date View & DaaS Agents
2.6	Discuss Display Protocols – PCOIP and BLAST Extreme	Display Protocols	VMware	Supported Display Protocol(s) for Desktop and Application access
2.7	Summarize pre-work, next steps and schedule handoff for Phase 3	Client action items and Handoff call	VMware	Handoff for Configuration will be scheduled with the Deployments Team
Client requirements to proceed to the Configuration Phase				
2.8	Provision Domain Bind Account	Domain Bind Account	Client	Active Directory Integration for Environment Access

2.9	Provision Auxiliary Domain Bind Account	Auxiliary Domain Bind Account	Client	
2.10	Provision Domain Join Account	Domain Join Account	Client	Account for joining Desktops to the Domain
2.11	Identify Display Protocol(s) for Desktop and Application access	Identify Display Protocol(s) from PCOIP, BLAST and BLAST Extreme	Client	
2.12	Set up necessary Licensing for Desktops and Applications	Desktop and Application licenses	Client	VMware will only provide validation of the desktops. All licensing requirements will be completed by client
2.13	Finalize Project Scope and return signed solution design document	Solution Design Document	Client	Scope of project cannot be modified without agreed change control
Phase 3: Execute				
3.1	Configure Active Directory Integration & Sync	Active Directory Integration	Joint	Configure Domain Bind for LDAP Access to Admin & Desktop Portals
3.2	Configure AD Groups for Administrative Accounts	AD Group sync for Administrators	Joint	AD Groups for access to Admin Portals
3.3	Configure AD Groups for User Accounts	AD Group sync for Users	Joint	AD Groups for access to User Desktop Portal
3.4	Validate Access to all Portals	Portal Access	VMware	Access to Admin, Helpdesk and Desktop Portals
3.5	Discuss Best Practices for the following: • Domain Bind • Domain Join & Desktop Naming • Images • Farms assignment • Miscellaneous Horizon Cloud Management	Best Practices for Horizon Cloud Deployment	VMware	
3.6	Define up to two use cases for Deployment	Use Cases	Joint	
3.7	Assist in up to 3 Image Designs	Convert Images to Gold Patterns	Joint	Assist in design and conversion of up to 3 images
3.8	Assist in creation of up to 3 Desktop Assignments	Desktops	Joint	Assist in creating Session-Based Desktops
3.9	Assignment using Configured Farms	Assignment	Joint	
3.10	Validate desktops are accessible from Windows & Mac workstations	Multi-Platform access	Joint	

3.11	Demonstrate Editing Images and Resealing an image and assigning to end users	Edit & Re-publish Images	Joint	Edit as well as re-seal an Image and validate changes by publishing to test user
3.12	Discuss Application Assignments and identify low complexity applications	Application use case	Joint	Discuss typical use cases and Best Practices for Application Assignment
3.13	Discuss typical use cases and Best Practices for Application Assignment	Identify Apps for assignment	Joint	Identify up to 5 low-complexity applications
3.14	Assistance with up to 5 low-complexity applications on one Image	Low complexity App assignment	Joint	Assist in deploying up to 5 low-complexity applications
3.15	Optimization and configuration of up to 1 RDS Host Server image with up to 5 low complexity applications installed to be used for desktops	RDSH Applications	Joint	
3.16	Installation of Dynamic Environment Manager	DEM Install	VMware	Assist with Installation and Configuration of Dynamic Environment Manager
3.17	Assist in creating up to 1 User Configuration in Dynamic Environment Manager	DEM Configuration	Joint	User Configuration in VMware DEM
3.18	Assist in creating up to 3 application profiles in Dynamic Environment Manager	DEM Configuration	Joint	Application Configuration in VMware DEM
3.19	Enable App Volumes	App Volumes Setup	VMware	
3.20	Creating an App Volumes AppStack Provisioning VM	App Volumes	VMware	
3.21	Updating up to 2 Golden/Master Image with App Volumes Agent	App Volumes	VMware	
3.22	Creating & Publishing up to 2 AppStacks with up to 2 Low complexity applications per AppStack	App Volumes	VMware	
3.23	Assist in setting up VMware WS1 Access Connector	Connector setup for AD Integration	Joint	Workspace ONE Access
3.24	Assist in Directory Integration of VMware WS1 Access	AD Integration	Joint	Workspace ONE Access
3.25	Assist in Integrating Horizon Cloud with VMware Workspace ONE Access	Horizon Cloud SSO with VMware Workspace ONE Access	Joint	Integrate Horizon Cloud with existing tenant of VMware Workspace ONE Access
3.26	Create entitlements for Horizon Cloud desktops of up to 2 desktops pools in Workspace ONE Access	Desktop entitlements	Joint	Add user entitlements in Workspace ONE Access for desktops

3.28	Configure Single Sign On for Horizon Cloud desktops from Workspace ONE Access	Single Sign on for desktops	Joint	Validate Single Sign On for desktops in Workspace ONE Access
3.29	Workspace ONE Access as Trusted IDP for a Third party IDP	Third Party IDP Integration	Joint	Includes testing for up to 3 apps
Phase 4: Close				
4.1	Assist in adding second Admin account for up to two Images	Desktop backup Admin Access	VMware	The account will act as a backup in case Sysprep disables the primary local admin account
4.2	Assist in OS optimization of up to two Images using VMware OS Optimization Tool	OS Optimization	Joint	OS optimization of Desktop Images for Gold Patterns
4.3	Assist in Basic and Advanced GPO Optimization by providing ADM templates	GPO Optimization	Joint	VMware will only provide ADM templates for Group Policies
4.4	Discuss Statistics & Report Sections in Admin Portal	Usage Statistics & Reports	VMware	These Sections go over Statistics in the Admin Portal
4.5	Discuss Lakeside Software as a troubleshooting option	DEM Configuration	VMware	Discuss Lakeside Software as a troubleshooting option
4.6	Discuss View Agent Logs	View Agent and PCOIP logs	VMware	Discuss location and keywords to check in View Agent Logs. Discuss PCOIP logs as well
4.7	Discuss DaaS Agent Logs	DaaS Agent Logs	VMware	Discuss location and keywords to check in DaaS Agent Logs as well as changing logging level
4.8	Go Over Support Options	Post Deployment Support	VMware	Go over Support Policies and Procedures as well as ticket creation

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com