VMware Horizon Cloud Bronze Deployment Bundle Statement of Work (SOW)

Effective: October 1st, 2016

Introduction to your Service Agreement

This service provides for technical support related to the VMware Horizon Cloud offering. The services provide the capabilities as defined below in this service description (the "Service" or "Services"). The VMware Horizon Cloud solution allows customers to simplify the delivery of cloud-hosted desktops and apps to any device without the hassle and cost of managing their own infrastructure. This Statement of Work ("Service Agreement" or "SOW") is entered among you the customer ("you" or "Customer") and the VMware entity identified on your invoice for the purchase of this Service.

This Service is subject to and governed by Customer's separate signed EULA agreement with VMware that explicitly authorizes the sale of this Service. By placing your order for the Services or utilizing the Services and associated software, you agree to be bound by this Service Description and the agreements incorporated by reference herein. If you are entering this Service Description on behalf of a company or other legal entity you represent that you have authority to bind such entity to this Service Description, which case "you" or "Customer" shall refer to such entity.

This Statement of Work (SOW) replaces all prior versions of the VMware Horizon Cloud Bronze Deployment Bundle Statement of Work. VMware may update the content of the SOW from time to time. The new version will automatically apply once customers renew their respective support or services package.

Service Overview

The deployment will include implementation of a VMware hosted Horizon Cloud tenant. This project will be organized into four phases: 1) Introductions and Project Kick off 2) Capacity order and Network setup 3) Configuration and Knowledge Transfer 4) Environment Check and Wrap-Up.

The implementation scope includes:

- VMware Horizon Cloud Tenant Provisioning
- VPN Setup with Horizon Cloud
- Domain Bind and Join with Horizon Cloud
- Conversion of Desktop Images into Gold Pattern
- Creation of Desktop Pools and assignment to end users
- Assistance with low-complexity applications
- Knowledge Transfer on all Horizon Cloud Portals
- Install and Configuration of VMware User Environment Manager (UEM)
- Functionality validation with customer

Service Assumptions

- Horizon Cloud-Hosted subscription service level must be identified.
- Horizon Cloud-Hosted desktop license model must be identified. Windows 7, Windows 8, and Windows 10 desktop operating system.
- Windows 2008 R2, 2012 R2, server operating system, configured for Windows desktop presentation, or RDSH.
- All Windows operating system licensing requires data center licensing as outlined by Microsoft. Windows terminal server licenses (required when using the RDSH features of Horizon Cloud-Hosted) must be provided by the customer as part of this service. Customer is responsible for installing and configuring a Microsoft KMS server.
- The customer is responsible for licensing of all operating systems and software deployed on the Horizon Cloud-Hosted platform.
- The customer must provide either Microsoft Terminal Server licenses, or access from the Horizon Cloud-Hosted platform to a Microsoft Terminal Licensing Server.
- Verify that KMS is available and that desktops are activating as expected.
- Customer configures network connectivity to Horizon Cloud-Hosted, including the setup of any VPNs.
- Connectivity between customer premises and Horizon Cloud-Hosted tenant environment is in place. VPN (requires compliant VPN technologies between customer premises and the Horizon Cloud-Hosted tenant environment).
- Multiprotocol Label Switching (MPLS) (requires interaction with a telecommunications service provider for dedicated connectivity between client premises and the Horizon Cloud-Hosted tenant environment).
- Verify that the firewall is configured to allow access to and from the Horizon Cloud-Hosted environment.
- DHCP scope is configured for the Horizon Cloud-Hosted environment. DHCP Option 74 might be required and provided by VMware. Option 74 specifies the IP address of the tenant appliance.
- Customer provides the necessary information for the Horizon Cloud- Hosted environment to be configured properly.
- IP address space has been defined and trusted for the Horizon Cloud- Hosted tenant environment in the corporate network.
- VMware requests at least 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.
- Access method to Horizon Cloud-Hosted desktops must be identified. From the trusted corporate network only, or allow direct access from the Internet.
- Horizon Cloud-Hosted tenant environment must be configured and available to the customer.
- If using Active Directory to authenticate users, the customer must provide requested information in the onboarding worksheet related to Active Directory.
- Use of either PCoIP or BLAST as the display protocol has been identified.
- Contact information must be provided as requested in the onboarding worksheet.
- Provide access to technical resources with expertise in the following areas:
    - Desktop engineering
    - Network/security
    - Active Directory
    - Applications
- Customer-specific customization for VMware Identity Manager is out-of-scope of this SOW.
- 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.
- Customer-provided desktop image, or security hardening the desktop image is out-of-scope of this SOW.
- Design, deployment, and integration of server resources in the Horizon Cloud tenant space is out-of-scope of this SOW.
- Installation and configuration of the VMware View® Client is out-of-scope of this SOW.
- Generation, registration, or implementation of third-party or internal SSL certificates is out-of-scope of this SOW.
- Deployment to clients over low-speed or high-latency networks is out-of-scope of this SOW.
- Certificate usage for authentication to VMware Identity Manager is out-of-scope of this SOW.
- Any assessment, plan/design or implementation services/documentation outside of what is in the service offering, is not included in this SOW.
- 3D or Rich Media Services integration, including vSGA/vDGA solutions leveraging Horizon Unified Communications API, webcams / telephony solutions, Lync or other third-party collaboration products/solutions, and so on as well as Implementation or

integration of printers, headsets, microphones, or peripherals (USB or otherwise) is out-of-scope of this SOW.

- Design, implementation, or integration of VMware App Volumes™, VMware ThinApp®, ThinPrint, Persona Management, or any other VMware product not already explicitly listed is out-of-scope of this SOW.
- Implementation or integration of multifactor authentication technologies is out-of-scope of this SOW.
- High Availability (HA) is out-of-scope of this SOW.
- Disaster Recovery (DR) is out-of-scope of this SOW. One can purchase the associated service offering to incorporate DR into the scope of a deployment.
- Review of the portals will be provided throughout the configuration; however formal training is out of scope of this SOW.
- The scope of the project cannot be delivered in phases and items not implemented as part of the initial deployment will be considered out-of-scope.
- 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.
- The SOW tasks will be performed remotely, unless agreed upon by all parties. Travel expenses will be charged to client.
- All work, documentation and work product(s) will be conducted during typical, VMware local business hours and will be provided in English.
- 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 budged change request may be issues.
- Statement of Work is deemed to be complete upon any of the following:
    - Completion of all service deliverables below
    - Up to a maximum of one calendar year from purchase date; SOW expires after 12 months

Responsibilities

All supplier and client 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.

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.

Engagement Timeline

The *VMware EUC 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.

Week	Activities
One	• Introduction meeting • Scope definition and success criteria definition • Technical Architecture definition
Two	• Client completes training • Client completes technical pre-requisites • VPN Setup
Three - Six	• Kick off with EUC Deployments Team • Tenant Provisioning • Configuration and validation of client use cases • Knowledge Transfer • Environment Check and Wrap-Up

Service Deliverables

ID	Description	Tool / Deliverable	Primary Owner	Comments
Phase 1: Introductions and Project Kick off				
1.1	Register for MyVMware Id on myvmware.com	MyVMware access	CLIENT	Required to access resources and Client Downloads
1.2	Review Statement of Work	SOW	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	
2.6	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
2.5	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 upto 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	Defined scope	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 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 & 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 2 Image Designs	Convert Images to Gold Patterns	Joint	Assist in design and conversion of up to 2 images
3.8	Assist in creation of up to 2 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 3 low-complexity applications	Low complexity App assignment	Joint	Assist in deploying up to 3 low-complexity applications
3.15	Implementation of one (1) of the following three (3) options: • Fire Up to four (4) low complexity applications configured as RDS Hosted Applications • Optimization and configuration of up to one (1) RDS Host Server image with up to four (4) low complexity applications installed to be used for RDS Hosted Desktops • Optimization and configuration of up to one (1) RDS Host Server image with up to two (2) low complexity applications installed to be used for RDS Hosted • Desktops, and up to two (2) low complexity applications configured as RDS Hosted Applications	RDSH Applications	Joint	
3.16	Installation of User Environment Manager	UEM Install	VMware	Assist with Installation and Configuration of User Environment Manager
3.17	Assist in creating upto 1 User Configuration in User Environment Manager	UEM Configuration	Joint	User Configuration in VMware UEM
3.18	Assist in creating up to 5 application profile in User Environment Manager	UEM Configuration	Joint	Application Configuration in VMware UEM
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 to Desktops	RDP Access	VMware	RDP Access is helpful in looking at desktops as an alternative to PCOIP or BLAST
4.6	Discuss Virtual Machine and Usage Report Sections in Helpdesk Console	Virtual Machine and Usage Report	VMware	These Sections go over Statistics in the Helpdesk Console
4.7	Test Remote Assistance option	Remote Assistance	VMware	Test option for Remote Assistance in Helpdesk Console
4.8	Discuss Lakeside Software as a troubleshooting option	UEM Configuration	VMware	Discuss Lakeside Software as a troubleshooting option
4.9	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
4.10	Discuss DaaS Agent Logs	DaaS Agent Logs	VMware	Discuss location and keywords to check in DaaS Agent Logs as well as changing logging level
4.11	Go Over Support Options	Post Deployment Support	VMware	Go over Support Policies and Procedures as well as ticket creation