Service Description: Cisco Managed Services for Data Center: Virtual Desktop Interface

Technology Addendum to Cisco Managed Services for Enterprise Common Service Description

This document referred to as a Technology Addendum describes the Cisco Managed Services for Data Center: Virtual Desktop Interface.

Related Documents: This document is an addendum to the Cisco Managed Services for Enterprise Common Service Description posted at www.cisco.com/go/servicedescriptions.

Direct Sale from Cisco

If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. If not already covered in your MSA or equivalent services agreement, this document should be read in conjunction with the Related Documents identified above. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller

If you have purchased these Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you.

The Service

This Technology Addendum is designed to be read in conjunction with the Cisco Managed Services for Enterprise Common Service Description that provides a baseline understanding of and sets expectations about the Cisco Managed Services, hereinafter referred to as the Service, provided by Cisco. In addition to the activities and deliverables outlined in the Common Service Description, this Technology Addendum outlines the unique activities and deliverables for the Customer's Virtual Desktop Infrastructure (VDI) Solution that is being managed by Cisco. Both service descriptions should be read in combination to fully understand the scope of the Service being purchased.

The Service described herein and other optional services are intended to supplement a current support agreement for Cisco products, and only available where all the Managed Components in a Customer's Virtual Desktop Infrastructure (VDI) Solution are supported through a minimum of core services such as Cisco's SMARTnet. Cisco shall provide the Service described below as selected and detailed on the purchase order for which Cisco has been paid the appropriate fee.

Cisco will provide a Quote setting out the extent of the Service and the term for which Cisco will provide the Service. Cisco will receive a purchase order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Cisco only provides support for Managed Components, unless specifically noted. For any device, component or solution element not specifically designated as a Managed Component, Cisco shall have no responsibilities whatsoever.

This Technology Addendum describes the services capabilities, supported devices, elective changes, and reports delivered.

Two managed service packages are available:

- Standard Managed Services
- Comprehensive Managed Services

These service packages are described in detail in the Common Service Description. In addition to these two service packages, the Customer can also purchase Optional services as needed to augment the package. The table below outlines the specific activities and deliverables provided under the Virtual Desktop Infrastructure (VDI) Solution as well as Optional Services available for the Service.

Activities / Deliverables	Standard Services	Comprehensive Services	Optional Services
Remote Monitoring	X	X	
Cisco Device Config Backups	X	X	
VDI Reports	X	X	
End User Quality of Experience (QoE)		X	
Defined Changes			X
Custom Changes			X

1 VDI Remote Monitoring

Overview

- 24x7x365 monitoring and management by Cisco Managed Services (CMS) for Data Center Network Operations Center (NOC) of the relevant Cisco VDI solution components.
- Single point of contact and operations escalation for Cisco VDI and third party technology components and applications.
- End User Quality of Experience (QoE) monitoring and ticketing. The capability provides for monitoring of QoE metrics like bandwidth, latency and virtual desktop performance.

The Service provides real-time monitoring on supported VDI Solution devices under the service packages and proactively declares Incident Events for:

- Unified Fault and Performance Management across:
  - Citrix XenDesktop Application Suite
  - Network Infrastructure
  - UCS Servers and Fabric Interconnects
  - Storage Components
  - VMware Hypervisor
- VDI Availability
- VDI Performance
- VDI Capacity
- Proactive Threshold Crossing Alerts

- Hardware Environmentals
- Syslog and traps

2 Cisco Device Config Backups

Backup activities include backup of the supported Cisco NX-OS device's configuration (Cisco Nexus Switching Family – Nexus 9000/7000/6000/5000/4000/2000/1000). NX-OS backup services do not include the backup of non NX-OS products, or the backup of any 3rd party devices and/or software.

3 VDI Reports

The Cisco Managed Service Platform (CMSP) constantly gathers device level information from the Managed Components covered within the Service. This information is compiled and made available via reports available on the CMSP Portal. Device level reports available are listed below.

Compute/Virtualization Level Reports

- **Server Asset Details Report** – Server name, model, manufacturer, operating system, operating system revision, total random access memory, percent of memory used, Amount of physical memory available, total virtual memory, percent of virtual memory used, amount of virtual memory available
- **Server System Reports and Operating Systems** – physical and virtual memory stats, CPU usage, interface utilization, file system utilization, configuration reports and change alerts, installed software, running processes, services running/not running, open ports, hardware profile (processors, disks, memory, installed components) for Windows and Linux hosts
- **UCS Device Specific Real-Time Reports** – Real-time, UCS specific reports that can graph up to 12 months of device metrics. The data can be exported for analyzing. Examples of data points are CPU utilization, interface statistics, environmental sensor values, memory statistics, and many others.
- **UCS Faults** – Consuming all faults raised by the UCS system. Examples include adapter unit problems, chassis environmental alarms, UCS blade equipment and bios alarms, various fan/power supply alerts, memory alarms, servers discovered/removed/unassociated, port problems, NIC failures, storage capacity, and disk concerns
- **UCS Configuration** – Tracking and alarming on state change for a subset of devices exposed through the API
- **VMWare Faults** – ESX/ESXi and Virtual Center/Sphere errors, Virtual Center/Sphere system utilization, high availability, and DRS performance
- **vMotion Sickness** – vMotion failures where VM oscillation or flapping occurs
- **Virtualization Infrastructure** – VMware ESX/ESXI server information, VMs grouped by ESX/ESXI Server and showing info for each VM, including: guest OS; CPU allocation and utilization; memory allocation and utilization; bandwidth utilization; file systems and their utilization
- **VM Health Report** – Health and availability for VMs showing CPU, memory and network activity
- **VM Migration Report** – For each VM a history of where it was, where it is now and when it moved
- **VM Interface Utilization Report** – Bandwidth utilized by each VM and each ESX/ESXI server

- **VM Top Utilization Report** – CPU, memory and swap for the top most utilized VMs based on resources for CPU, memory and Swap per blade or chassis

Storage Level Reports

- **File Service Performance Details Report** – Server operating system, volume name (logical partition), volume size for each logical storage volume under management.
- **Storage Fiber Switches** – FC interface status, FC interface errors, FC switch status, SNMP uptime , FC interface utilization, SNMP trap handler. Generic monitor that allows for the capture of SNMP traps from a storage head device and maps to error conditions
- **SAN Standard** – SAN array disk group status, SAN hardware status, SAN diskshelf status, and SAN controller status
- **NAS NetApp and EMC** – faults for NetApp and EMC on the following NVRAM, fan, temperature, CPU, disk, disk status, and shares. EMC also includes more hardware and array status alerts
- **Storage Device Capacity Planning Report** – system name, number of disks, capacity, and percent allocated

4 End User Quality of Experience (QoE) (Comprehensive Only)

End User Quality of Experience (QoE) monitoring is an important element of the CMS VDI offer. The capability provides for monitoring of QoE metrics like bandwidth, latency and virtual desktop performance as it relates to infrastructure availability and performance. This is indicated with a Mean Opinion Score (MOS) monitored by Cisco.

The Cisco service delivery platform analyzes key VDI user experience metrics—ranking individual QoE attributes and corresponding scores across the VDI Infrastructure—providing Cisco with an estimation of the virtual desktop experience as it may have been perceived by the end user.

The QoE engine is tunable within the Cisco Cloud and Managed Service Platform (CMSP) to map directly to the level of QoE that a support organization wishes to establish as the benchmark. Benchmarks, and/or threshold criteria, is configured to match the level of monitoring mutually agreed by the Customer and Cisco.

Customer Responsibilities

- CMS requires WMI access to the Virtual Desktops in order to ensure a complete view of the VDI infrastructure and to best monitor Quality of Experience metrics.
    - WMI access is not mandatory. If not provided, CMS will use QoE metrics across the infrastructure, excluding any Virtual Desktop metrics to determine QoE scoring.
- Management of the User Virtual Desktop Operating System (O/S) and Applications within the VDI containers.

5 Third Party Managed Components

- Cisco incident resolution of third party software issues that require patches, updates, and upgrades must be vendor recommended and Customer approved
- Troubleshooting Incidents for third party Managed Components may be dependent on collaboration with third party organizations

- Cisco requires applicable Letters of Agency in order to coordinate on Customer's behalf for the management of third party components

As part of its role in providing support for third party Managed Components, Cisco will:

- Engage Customer third parties as necessary to maintain service and resolve issues, including escalation to Customer for third party non-responsiveness
- Provide and coordinate requisition and fulfillment activities for Managed Component replacement with third party vendors as needed
- Triage and escalate problems to appropriate support staff or third party suppliers for resolution subject to Customer entitlements and established Letter of Agency between Customer and Cisco

Customer Responsibilities

- Provide Letter of Agency (LOA) for 3rd party devices and applications and ensure Cisco NOC Engineers have appropriate privileges with the third party vendor
- Provide System Administration (SysAdmin) of the VDI environment
- Perform first call triage via an End user Helpdesk/Service desk
- Manage the User OS and Applications within the VDI containers
- Perform file system backup of all infrastructure and User VMs (including the Microsoft SQL DB)
- Create, deploy and update the Master Template (Golden Image)

6 Customer Requested Change Management

Customers purchase a block of hours that can be leveraged across all Move, Add, Change, Delete (MACD) categories and Custom Scoped Elective Changes that a customer has under the Service. The customer must have sufficient balance of support hours on account to cover the requested change. Additional hours maybe purchased if required.

6.1 Defined Changes

Defined Changes are categorized into Small, Medium, and Large activities. A Defined Change is a requested change by the Customer. Defined Changes are not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the needed type of change and submits a Defined Change Request on the Portal. MACD are considered Defined Changes.

6.1.1 MACD Changes

Small MACD (Type 1)

- Add configure, change VM resources
- Assign user accounts to Desktop VM's
- VLAN changes

Medium MACD (Type 4)

- Apply Server VM Application patches
- Deploy new Desktop VM's from a standard template

Large MACD (Type 8)

- Upgrade new Hypervisor
- Upgrade new OS for Server VM's
- Apply Cisco managed application upgrade

6.2 Custom-Scoped Changes

Custom Scoped Elective Changes are customer requested changes that fall outside Incident and Problem (Standard) changes for restoring service. Custom Scoped Elective changes will require a mutually agreed upon statement of work (SOW). See Cisco Managed Services for Enterprise Common Service Description for more details of Custom Scoped Elective Change support.