Managed Private Cloud

The complete service is defined by the combination of the following items:
Client Service Description – service delivery operations that are common to all NTT Managed Services
Service-Specific Operations – service delivery operations that are specific to Managed Private Cloud solutions and other contracted services, as indicated in SOW

1 Overview of Service

Managed Private Cloud provides the design, configuration, monitoring, capacity and performance management of a private cloud infrastructure as either NTT Managed Services Platform or NTT Anywhere as specified in the SOW with extended functions and a set of modular features designed to meet Clients' unique requirements.

The Managed Private Cloud service is constituted on a per client basis using a *multi-layer* NIST security framework—addressing endpoints, operating system, application and network, in combination with NTT's architectural guides, blueprints and best practices to support in scope SOW use cases, where security, scalability and agility are the main drivers... and predictable cost, availability and management are paramount.

Managed Private Cloud features will vary per Client and must be expressly included as in scope in SOW from the following table, or any service below is out of scope:

Element	NTT Managed Services Platform (Multi-tenant Infrastructure)	NTT Anywhere Dedicated Private Cloud (Single-tenant Infrastructure)
Managed Private Cloud Foundation (Data Center and Internet)	Includes data center space and power in an NTT compliant data center as specified in the SOW (see locations below) for contracted Virtual Machine or dedicated resources, one Public IPv4 address, Highly Availability Internet bandwidth Committed Information Rate (CIR) burstable up to 5Gbps and charged in 10Mbps increments using 95% percentile billing model. Additional IPv4 Address, CIR (in 100Mbps increments) and dedicated circuit cross-connects are available for an additional fee and must be contracted separately.	Client-provided data center and Internet bandwidth, device location as defined in Managed IaaS Schedule in SOW (Client must contract for dedicated Network and Managed Defense in Depth infrastructure). Client must provide a Client-contracted third party colocation facility meeting the system requirements.
Managed Defense in Depth	Includes Highly Availability Firewall and IPS/IDS cluster, two (2) dedicated jump host and two (2) Active Directory and/or Free IPA servers (depending on environment) for NTT administration, and Standard Security Services (see section Security and Compliance of the Client Service Description.) IPsec Site-to-Site VPNs are available for an additional fee and contracted separately.	
Managed IaaS	The following may be selected as specified in the SOW: Virtual Machine - Defines the Production, Non-Production or Disaster Recovery vCPU and RAM allocated on a per virtual machine basis for Windows, Red Hat Enterprise Linux, and SuSe SLE and Oracle Linux servers. Dedicated Compute - Defines the Production, Non-Production or Disaster Recovery compute resources on a per physical server basis for Windows, Red Hat Enterprise Linux, and SuSe SLE and Oracle Linux servers, as defined in Managed IaaS Schedule in SOW. Virtual SAP HANA TDI - Defines the Production, Non-Production or Disaster Recovery Tailored Data Center Integration vCPU and RAM allocated on a per virtual machine basis for SAP HANA. Dedicated SAP HANA TDI - Defines the Production, Non-Production or Disaster Recovery Tailored Data Center Integration compute resources on a per physical server basis for SAP HANA, as defined in Managed IaaS Schedule in SOW. Storage Resource - Defines the Production, Non-Production or Disaster Recovery Block, File, Image, Object or Archive storage resources on a per GB basis. Dedicated Storage - Defines the Production, Non-Production or Disaster Recovery storage array resources on a storage array basis, as defined in Managed IaaS Schedule in SOW. Traffic Manager - Defines the Production, Non-Production or Disaster Recovery Local and/or Geographic Traffic Manager resource(s) on a per Mbps, Gbps or virtual appliance basis.	
NTT Anywhere Automation (Optional)	N/A	If specified as in scope in the SOW, the NTT Anywhere Automation Portal enables the Client to consume NTT Anywhere resources for Client managed VMs. NTT will maintain and administer Client access to the NTT Anywhere Automation Portal and

		provide the VM templates for NTT-Provided Operating System licenses. If specified as in scope on a separate SOW, Professional Services are available to help Client define VM creation workflows and to address business processes beyond the creation of a VM.
Managed Virtual Machine	Unless stated differently in the SOW, every Managed Private Cloud deployment requires: • Managed Active Directory and Free IPA service, must be specified as in scope in the SOW. See *Managed Active Directory and Free IPA* service description for more details. • All virtual machines require NTT provided Operating System licensing and Managed Operating System service must be purchased for every machine in the SOW. See *Managed Operating System* service description for more details.	
Managed Cloud Backup	Includes agent or agentless FIPS 140-2 Level 2 encrypted at-rest daily snapshot of virtual machine(s) (VM) retained for thirty (30) days, unless otherwise specified in the SOW, on NTT storage at the additional cost of storage or dedicated backup appliance (as defined in Managed IaaS Schedule in SOW). Secondary-copy at a remote archival (see locations below) data retention options are available for an additional fee and must be specified as in In-Scope. The service includes pre and post snapshot scripting to quiesce and restart applications for crash consistent backups/snapshots for NTT managed VMs. Disaster Recovery services are available and must be specified as in-scope in the SOW, see the *Managed Disaster Recovery* service description.	

2 Client Responsibilities

(a) Provide NTT with business process/context CI tagging information for all private cloud CIs, in the form of a Client reference for an application or IT service.

(i) e.g., web server-23 and database server-5 are used for the public web site. In this example, the "public web site" resource tag would be applied to web server-23's and database server-5's attributes in NTT's CMDB.

(b) Procurement, design, configuration, monitoring, capacity, performance management, or any other task for any Client private Cloud element not explicitly described in scope SOW.

(c) All required consent, authorization, license, use rights, software licenses, required for NTT to perform the Services in this service description.

(d) All access required for remote access and monitoring must be enabled by Client.

(e) Any action not specifically identified as in scope in this Service Description

(f) Client must maintain an active service agreement and provide access to NTT for any software or service provided by Client.

(g) Client must agree to any EULA, or other license terms for any software, license, or otherwise provided by NTT.

(h) Only applicable for NTT Anywhere Enterprise Client-provided data center and Client-contracted third party colocation facility in addition to the above:

(i) Take receipt of any NTT-provided equipment shipped directly to relevant data center

(ii) Immediately take pictures and report any damaged equipment to your NTT Service Delivery representative

(iii) Use commercial reasonable effort to securely store and protect NTT-provided equipment

(iv) Client-contracted third party colocation data centers - Provide a Letter of Authorization, commonly referred to as an LoA, to accept 3rd party (NTT) inquiries and requests on behalf of their clients.

(v) All Client's premises and third party colocation data centers must have a 24x7 onsite contact, responsible for visual inspection to confirm power outages, disconnected cables or to address other possible issues and/or requirements related NTT's ability to perform remote Incident Management

(vi) Provide NTT or NTT agent access to NTT-provided equipment to perform Standard Transition (see below) and maintenance activities

(vii) Disposal of any rubbish packing material resulting from NTT Anywhere Standard Transition

3 Service Specific Operations

3.1 Monitors

Using resource Tagging information provided by Client, NTT will group and monitor by applications and/or IT services resources in a Client aligned business process/context.

Any additional monitors, in the service specific “Monitors” section for the corresponding services’ service descriptions that constitute Client's specific Managed Private Cloud solution must be in scope in order to be provided. *e.g., Refer to Managed Operating System service description for Operating System Monitors.*

The following monitors are configured by default as available based on the hardware and software limitations:

Monitor	Description	Alert	Performance Info	Resolution and Analysis
Business Process - Availability	Network, CPU and Storage availability charts by business process/context	Yes	Graph of Network, CPU and Storage availability	Resolution - Engineering Teams will attempt to diagnose and solve the issue and escalate to the Client or vendor if needed. Monthly Analysis - Engineering Teams will trend availability and provide recommendations to improve availability of environment, any changes will be subject to the Change Control Process.
Business Process - Capacity	Network, CPU and Storage utilization charts by business process/context	Yes	Graph of Network, CPU and Storage utilization	Resolution - Engineering Teams will attempt to diagnose and solve the issue and escalate to the Client or vendor if needed. Monthly Analysis - Engineering Teams will trend capacity utilization and provide recommendations to improve utilization of environment (rightsize), any changes will be subject to the Change Control Process.
Business Process - Performance	Network, CPU and Storage performance charts by business process/context	Yes	Graph of Network, CPU and Storage performance	Resolution - Engineering Teams will attempt to diagnose and solve the issue and escalate to the Client or vendor if needed. Monthly Analysis - Engineering Teams will trend performance and provide recommendations to optimize environment, any changes will be subject to the Change Control Process.
Backup	Success/Fail	Yes		Resolution - Engineering Teams will attempt to diagnose and solve the issue and escalate to the Client or vendor if needed.

3.2 Service Requests

In addition to the service specific “Service Requests” section for the corresponding services’ service descriptions that constitute a Client's specific Managed Private Cloud solution. *e.g., Refer to Managed Operating System service description for Operating System Service Requests.* The fulfillment of the following types of requests are included:

Task	Description
Internet	Changes to Public IP Address DNS Record, only if NTT has Administrative or Technical DNS roles
Defense In Depth - Firewall	Creation, change and deletion to Firewall rules
Defense In Depth - Intrusion Detection / Prevention	Support Client requested signature / engine update schedule (Daily, Weekly, and Monthly)
Defense In Depth - Intrusion Detection / Prevention	Creation, change and deletion to exclusion rules

Defense In Depth - Intrusion Detection / Prevention	Creation, change and deletion to Client specific IDS/IPS rules
Defense In Depth - Network	Creation, change and deletion network communication between resources by providing specific details including the source IP/network, destination IP/network and application or network port.
Virtual Machine Settings - Operations	Start, Stop, Clone, Restart, Deletion of existing Virtual Machine. Deletion will create SOW change, per rate card
Virtual Machine Settings - Affinity rules	Creation, change, deletion and move guest affinity rules specific for virtual machine cluster properties
Virtual Machine Settings - Host migration	Perform live host migration for virtual machines is supported and does not require a change control process
Virtual Machine Settings - Snapshots	Virtual Machine Snapshots are available and will be subject to the Change Management Process at maximum allowed time for snapshot to exist is 48 hours at which time it will be deleted without warning. (Note: Snapshots may result in production performance degradation.)
Virtual Machine Settings - VM Template management for Managed Services Platform only	Creation Virtual Machine based on Client provided templates or Engineering Teams' templates. Creation will create SOW change, per rate card
Dedicated Storage Array Management	Creation, change and deletion of Block/CIFS/NFS/Object resource
Traffic Manager - VIPs and IP pools/ service groups	Creation, change and deletion to VIPs configured and the IPs of the web nodes; IP address configuration of web servers not managed by NTT is not included
Traffic Manager - Service checks	Creation, change and deletion to service checks configured in the traffic management policy. Connection to external web server to detect / configure the service response not included.
Traffic Manager - Traffic management policy	Creation, change and deletion traffic management policy (round robin, weights, etc.)
Traffic Manager- Management of SSL certificates	Creation, change and deletion of SSL certificates associated to the service
Traffic Manager - Geographic traffic management policy	Creation, change and deletion of failover policy with GTM (active, passive, etc.)

4 Supported Technologies

The following Server Operating System technologies are supported:

(a) Windows Server 2008 R2/2012 R2/2016/2019 x64, 2022

(b) Red Hat Enterprise Linux 7 and 8, x64

(c) SuSe SLE 12.x and 15.x for SAP (only for SAP solutions)

(d) Oracle Linux 6/7 x64

The following configurations are supported, if specifically in scope in an SOW:

(a) NTT Managed Services Platform, NTT Anywhere blueprints

(b) Standalone server: A standalone server or a set of standalone servers (managed independently from each other)

(c) Red Hat Cluster Services, Red Hat Global Filesystem: A cluster of up to 8 nodes running RHCS or GFS

(d) Windows Failover Cluster, Windows Terminal Services; require shared disks and dedicated heartbeat network segment and interface

(e) Application-aware backup and recovery is available through Microsoft VSS integration for Microsoft VSS-aware applications and Microsoft Active Directory

The following configurations are not supported:

(a) All 32-bit VSS applications (requesters, providers, and writers) must run as native 32-bit or 64-bit applications. Running them under WOW64 is not supported.

(b) Any configuration not listed above.

5 Supported Environments

The following environments are supported:

(a) Cloud Backup Archival Locations, with a separate Public Cloud agreement and NTT Public Cloud Management Agreement:

(i) Public Cloud: Amazon Web Services S3, S3-IA, S3-RRS and Glacier; Microsoft Azure Blob Storage LRS, ZRS and GRS; Google Cloud Platform Nearline, Coldline

(ii) Oracle Cloud Infrastructure Object Storage - Standard; Includes support for Government Cloud Options in AWS and Azure

(iii) Private Cloud (S3 Object Store): Managed NTT Private Cloud archives all data to an S3 compatible Cloudian archival tier storage. Other S3 compliant archival options are available on a consultation basis.

(b) NTT Managed Services Platform Data Center Common Features:

(i) Generator - Redundant configuration with N+1 or 2N and 48-hour continuous operation without refuel

(ii) UPS - Redundant configuration with N+1 or 2N

(iii) Power Provision - Dual power feeds from different PDUs

(iv) Air-conditioning - Highly efficient cooling systems, specifically for ICT equipment with N+1 or 2N redundancy. Set temperature and humidity values compliant with ASHRAE TC 9.9

(v) Fire Protection - Early warning smoke detection system and gas suppression systems

(vi) Security - Monitoring cameras and our security policy, which is compliant with ISO 27001 or ISAE3402/SSAE18

(vii) Connectivity - Carrier neutral data center with global Tier-1 and regional carriers on-site and large-bandwidth connectivity between Internet exchanges and other NTT data centers

(c) NTT Managed Services Platform Data Center Locations:

(i) Raging Wire (an NTT Ltd. Company) Dallas, Texas (US-TX1)

(ii) Raging Wire (an NTT Ltd. Company) Ashburn, Virginia (US-VA1)

(iii) Secure-24 (an NTT Ltd. Company) Plymouth, Michigan (US-MI1)

(iv) eShelter (an NTT Ltd. Company) Frankfurt, Germany (EU-DE1)

(v) eShelter (an NTT Ltd. Company) Zurich, Switzerland (EU-CH1)

(d) NTT Anywhere:

(i) NTT colocation services contracted separately or as part of Managed IaaS Schedule in SOW

(ii) Client-provided data center and Internet bandwidth (inclusive of Client-contracted third party colocation facility) with:

UPS - Redundant configuration with a minimum of 10 minute runtime under full load with VMware compatible shutdown software via USB cable or network connection

Power Provision - Dual power feeds from different PDUs

Air-conditioning - Temperature and humidity values compliant with ASHRAE TC 9.9

Termination of all data center centric network connections to the data center rack/cabinet where NTT-provided equipment will be installed

Out-of-band connectivity that meets NTT management requirements

6 Limitations and Out of Scope

In addition to the service specific “Limitations” section for the corresponding services’ service descriptions that constitute a Client's specific Managed Private Cloud solution. *e.g., Refer to Managed Operating System service description for Operating System Limitations.* The following limitations apply:

(a) NTT will provide virtualization management software monitoring. Client will not be allowed access to the NTT management console.

(b) Maximum of 80 vCPUs can be configured per individual VM

(c) Maximum of 1.8 TB disk size can be configured per individual VM

(d) Over-commitment of RAM is not supported

(e) IPv4 address space must comply with applicable regional Internet registry (RIR) policies

(f) IPv6 address space is not currently supported

(g) Cloud Backup data will not be held by NTT without a supporting active SOW. In the event of contract termination, all Cloud Backup data will be erased by NTT using Data Eraser software.

(h) Requests to restore from backup may not exceed NTT's Fair Use Policy or Acceptable Use Policy as stated in the Service Delivery section of the *Client Service Description.*

(i) Any tasks not expressly mentioned as in scope is out of Scope.

7 Tasks Included in the Standard Transition

As part of the Service, the following tasks are included if specifically listed as In-Scope in the SOW.

7.1 Cloud Environment

(a) Setup and configure clusters to be fully hardware redundant

(b) Allocated 100% contracted memory in a cluster

(c) Setup and configure dedicated storage array Block/CIFS/NFS/Object storage resource (only applicable to NTT Managed Services Platform - Dedicated Storage)

(d) Setup and configure VMs CPUs

(e) Setup and configure VMs disks

(f) Setup and configure VM Operating Systems

(g) Automated resource load-balancing to facilitate VM moves between physical hosts as necessary to accommodate for performance and maintenance requirements

(h) Setup and configure pre and post snapshot scripting to quiesce and restart applications for crash consistent backups/snapshots for NTT managed VMs

(i) Setup and configure VM daily backup/snapshot of VMs

(j) If specifically, in-scope in the SOW, setup and configure long-term and/or secondary-copy data retention at a remote archival site

7.2 Virtual Machine Settings

(a) Setup and configure guest affinity rules that keep together specific virtual machines within a cluster, or those that keep specific virtual machines apart within a cluster are supported. This requires prior NTT and Client approval

(b) Setup and configure virtual machines in high availability at the hypervisor layer

7.3 IP Management and Network Connectivity

(a) Provide public IPv4 address space (for NTT Managed Services Platform only)

(b) Allocate and provide private IP address ranges for all devices within the NTT data centers. NTT will work with Client to ensure IP address ranges are not in conflict with existing Client network or other NTT Clients. NTT cannot guarantee a specific Client requested range or IP will be available

(c) Setup and configure firewall rules based on NTT's best practices

(d) Setup and configure IPsec Site-to-Site VPN's (if specifically in scope in the SOW and provided in the SOW)

(e) Setup and configure MPLS Circuits (if specifically in scope in the SOW and provided in the SOW)

(f) Setup and configure Point-to-Point Circuits (if specifically in scope in the SOW and provided in the SOW)

(g) Setup and configure MPLS with VPN Backup (if specifically in scope in the SOW and provided in the SOW)

7.4 Defense In Depth

(a) Setup Client specific firewall rules

(b) Setup and configure Intrusion Detection/Prevention exclusion rules on a per firewall policy basis

(c) Setup Client specific IDS/IPS rules

(d) Setup and configure all Private Cloud virtual networks following the principle of least privilege

(e) Discover applications and ports to accommodate firewall policies for NTT managed applications where NTT is managing both source and destination application

7.5 NTT Anywhere Enterprise and NTT Anywhere Edge on site installation at the relevant data center

(a) Provide on-site engineer(s) to perform the physical installation and configuration of equipment defined in the Managed IaaS Schedule of SOW, inclusive of ancillary cabling within corresponding data center rack/cabinet, with approved travel and if specifically in scope in the SOW.

(b) Assist with registration of devices with Client Approval, Client must provide appropriate personal with approval authority.

(c) Connect and test NTT-provided equipment to data center centric network connections to enable Common Standard Transition Tasks (above).

(d) Tasks Included in the Takeover of an Existing Installation

8 Tasks Not Included in the Standard Transition

The following tasks are not included in the standard transition:

(a) Setup and configuration of any technology or third-party service not defined in SOW

(b) Client must maintain an active service agreement and provide access to NTT for any software or service provided by Client

(c) Client must agree to any EULA, or other license terms for any software, license, or otherwise provided by NTT