# 1 Public Cloud Management - Managed Azure - Core Services

This service provides the configuration, monitoring and management of the core services in an Azure environment for systems specified as in scope in the SOW.

1.1 Supported Configurations

(a) Azure subscription owned by NTT via CSP channel or EA

(b) Azure subscription owned by the Client via Direct or Enterprise Agreement (EA), with Owner or Contributor privileges provided to the Engineering Teams (with SLA limitation)

1.2 Azure Access Management Prerequisites

In order for NTT to manage the Client's Azure environment, the following requirements must be met:

(a) Azure Subscription (provided by CSP, Direct or EA) with Owner/Contributor role

(i) In case of Client EA Enrollment, the Governance Hierarchy must be defined and provided by the Client; the Services Administrator role must be provided to NTT

(b) As NTT uses Azure Lighthouse to deliver the service, Client must delegate all resources under management to NTT with a Contributor role

(c) Allow Application registration in Azure AD for monitoring and consumption tooling

1.3 Core Services

Managed Azure Core Services covers the following services:

(a) Governance Management

(b) Managed IaaS Resources

(i) Managed Compute

(ii) Managed Storage

(iii) Managed Network

(iv) Managed Network Security

(c) Managed Cloud Identity

As Public Cloud technology evolves at such a rapid pace, it is not possible to maintain a fully up-to-date list of supported features and services. This description, therefore, serves as a baseline across common categories.

The services listed below are supported as part of this service description. The exact scope of the solution being delivered to the Client and related charges are clearly stated in the Statement of Work (SOW) and anything not in specifically included as In Scope in the SOW is specifically excluded as out of scope.

| Category | Managed Element | Supported Services |
|---|---|---|
| Governance | Cloud Base Service | . Azure Policy<br>. Azure Management Groups<br>. Azure Log Analytics<br>. Role-Based Access Control<br>. Azure Subscriptions |
| | Cloud Region | . VNets within the region<br>. DNS Services<br>. VPN Gateways<br>. Azure Storage Accounts<br>. Azure Load Balancer<br>. Azure KeyVault |
| Networking | Cloud PaaS & SaaS Networking | . Azure CDN<br>. Azure Front Door<br>. Azure Application Gateway<br>. Traffic Manager |
| | Direct Connectivity | . Azure ExpressRoute<br>. Azure Virtual WAN |
| Network Security | Cloud PaaS & SaaS Network Security | . Azure Firewall<br>. Azure DDoS |
| Compute | Cloud IaaS - Scaling Group (Elastic) | . Azure Virtual Machine Scale Set |

| Category | Managed Element | Supported Services |
|---|---|---|
| | Cloud IaaS - VM (Static) | . Azure Virtual Machine |
| Automation | Cloud VM Scheduling | . Azure Automation (start/stop vms) |
| Storage | Cloud PaaS File Storage | . Azure File<br>. Azure File Sync |
| | Cloud NetApp File Storage | . Azure NetApp File |
| Identity | Cloud Identity & Domain | . Azure Active Directory<br>. Azure AD Connect |
| | Cloud Hybrid Identity | . Azure AD B2C |
| Data Protection | Cloud Backup | . Azure Backup |

*Table 1 Azure Core Services Summary*

1.4 Governance

(a) Base Cloud Managed Services

(i) Overview

This element of the service covers the configuration, and management of the Governance and general "guardrails" of the Azure environments. Charges are based on the number of subscriptions that the Client has regardless if the resources deployed are managed or unmanaged as specified in the SOW .

(ii) Supported Technologies

- Azure Policy
- Azure Management Groups
- Role Based Access Control
- Azure Subscriptions

| Azure Policy | |
|---|---|
| **Overview** | Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. |
| **Setup Activities** | Following vendor best practices, NTT has developed a standard set of policies under its "Core Initiative" which it will configure as part of setup. A complete list of policies included in NTT Core initiative is available upon request. |
| **Service Request** | Deactivate/reactivate specific NTT Core Initiative policies. |
| **Available Monitors** | N/A |
| **Service Limitation** | Custom policies can be added; complexity and pricing will be analyzed on a case by case basis and are out of scope by default. |

*Table 2 Azure Policy*

| Azure Management Groups | |
|---|---|
| **Overview** | Managed Groups are a structure or container to organize subscriptions and provide a level of scope above subscriptions. |
| **Setup Activities** | Create management group |
| **Service Request** | . Move subscriptions or management groups<br>. Manage /Change the Managed Groups Limits |
| **Available Monitors** | N/A |

| Azure Management Groups | |
|---|---|
| **Service Limitation** | Design of Management Group strategy is not included as part of this service and is out of scope. |

*Table 3 Management Group*

| Azure Log Analytics | |
|---|---|
| **Overview** | Azure Log Analytics is a tool  used to edit and run log queries with data in Azure Monitor Logs. |
| **Setup Activities** | . Create Log Analytics Workspace<br>. Enable/ Install VM Extension for Azure Monitor (Insights) |
| **Service Request** | . Send logs to Azure Event Hubs or Azure Storage<br>. Increase / Decrease Retention period |
| **Available Monitors** | N/A |
| **Service Limitation** | |

*Table 4 Azure Log Analytics*

| Role Access Base Control | |
|---|---|
| **Overview** | Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. |
| **Setup Activities** | . Audit Role assignment<br>. Assign Roles |
| **Service Request** | . Scope RBAC roles to specific subscription, Resource Group or resource<br>. Assign or change RBAC roles to restrict permissions via scopes (Owner, Contributor, Reader)<br>. Create Custom Role |
| **Available Monitors** | There is no active monitor for this service by can be audited through Activity Log, for:<br>. Create role assignment<br>. Delete role assignment<br>. Create or update custom role definition<br>. Delete custom role definition |
| **Service Limitation** | |

*Table 5 Role Access Base Control*

| Azure Subscription | |
|---|---|
| **Overview** | An Azure subscription is a logical container used to provision resources in Azure. |
| **Setup Activities** | . Create or takeover Azure subscription<br>. Create the subscription demarcations<br>. Associate the subscription to an existing tenant<br>. Create Resources Groups<br>. Add tag information for resources<br>. Enable Cloud monitoring tools: Register Application in Azure AD |
| **Service Request** | . Move resources between resources groups; assign resources to a Resource Group<br>. Perform changes to the hierarchy and access inheritance for subscription management and correct cost allocation<br>. Create and assign new tags to the resources in the subscription<br>. . Manage /Change the subscription limits (quotas) |
| **Available Monitors** | Azure_Storage_ServiceLimits : Monitors Storage Limits and utilization. Instances are listed by subscription ID. |

| Azure Subscription | |
|---|---|
| | . StorageAccountsLimit: Maximum number of Storage Accounts per subscription<br>. StorageAccountsUsage: Current number of Storage Accounts in use per subscription<br>. PercentStorageAccountUsage: Calculates and monitors the utilization percentage of Storage Accounts<br><br>Azure_VM_ServiceLimits: Monitors Azure Virtual Machine Service Limits by subscription and service region<br><br>. VMLimit: Virtual Machine limit for the region and subscription as reported by Azure<br>. VMUsage: Number of Virtual Machine instances in use for the region and subscription<br>. AvailabilitySetLimit: Availability Set limit for the region and subscription as reported by Azure<br>. AvailabilitySetUsage: Number of Availability Set instances in use for the region and subscription<br>. CoresLimit: Virtual Machine Core Limit for the region and subscription as reported by Azure<br>. CoresUsage: Number of Virtual Machine Cores in use for the region and subscription<br>. VMScaleSetLimit: Virtual Machine Scale Set limit for the region and subscription as reported by Azure<br>. VMScaleSetUsage: Number of Virtual Machine Scale Set instances in use for the region and subscription<br>. PercentageAvailabilitySetUsage: Calculates and monitors the utilization percentage of Availability Sets<br>. PercentageCoresUsage: Calculates and monitors the utilization percentage of Cores<br>. PercentageVMScaleSetUsage: Calculates and monitors the utilization percentage of Virtual Machine Scale Sets<br>. PercentageVMUsage: Calculates and monitors the utilization percentage Virtual Machines |
| **Service Limitation** | The following are not included and are Out of Scope:<br><br>. Purchase of reservation orders for subscriptions under Client owned Enrollment Agreements; Client responsibility<br>. Creation of specific dashboards and personalized views of reports<br>. Cost Advisory or Security Advisory<br>. Design Subscription Strategy |

*Table 6 Azure Subscription*

| Azure Application Insight | |
|---|---|
| **Overview** | Application Insights is an extension of Azure Monitor and provides Application Performance Monitoring (also known as “APM”) features |
| **Setup Activities** | . Provide access to Workspace used for Application Insight<br>. Install Agents on defined VMs to be monitored by the service |
| **Service Request** | . Install Agents for Auto-instrumentation on Azure VMs (Windows) |
| **Available Monitors** | N/A |
| **Service Limitation** | . Proactively actions using App Insight as a APM Service are not included as part of this service, Other NTT Services can be added to cover this need such as Observability Services<br><br>. Dashboard creation is not included in this service, Setup activities may have extra cost |

*Table 7 Azure X Insights*

(b) Cloud Region

(i) Overview

This element of the service covers the configuration, monitoring and management of the general infrastructure elements presents in each Cloud Region. Charges are based on the number of regions where resources are deployed specified in the SOW. The management of all of services described in this section are covered, regardless of the number of resources deployed within the region where Managed IaaS resources or other cloud management services are contracted.

(ii) Supported Technologies

- Azure Virtual Network
- DNS Services

- VPN Gateways
- Azure Storage Accounts

| Azure Virtual Network | |
|---|---|
| **Overview** | Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. |
| **Setup Activities** | . Add tag information for resources<br>. Create Virtual Networks and peering between regions<br>. Create route tables and user-defined routes<br>. Create rules for NSG (if ACL is not set at firewall appliance level)<br>. Create VNet peering<br>. Create subnets |
| **Service Request** | . Create, change or delete a virtual network or subnets<br>. Create, change or delete route tables or user-defined routes<br>. Create, change or delete rules for NSG<br>. Create, change or delete VNet peering<br>. Create, change or delete subnet<br>. Enable Cloud monitoring tools: Register Application in Azure AD, Configure Azure Monitor, Diagnostic Log, Activity Log, create Log Analytics workspace |
| **Available Monitors** | **Available Monitors**<br><br>Azure_Network_ServiceLimits: Monitors Azure Network Service Limits by subscription and service region<br><br>. PublicIPAddressesLimit: Maximum amount of Dynamic Public IP Addresses for the region and subscription as reported by Azure<br>. PublicIPAddressesUsage: Number of Dynamic Public IP Addresses in use for the region and subscription<br>. LoadBalancersLimit: Maximum amount of Load Balancers for the region and subscription as reported by Azure<br>. LoadBalancersUsage: Number of Load Balancer instances in use for the region and subscription<br>. NetworkInterfacesLimit: Maximum amount of Network Interface Groups for the region and subscription as reported by Azure<br>. NetworkInterfacesUsage: Number of Network Interface instances in use for the region and subscription<br>. NetworkSecurityGroupsLimit: Maximum amount of Network Security Groups for the region and subscription as reported by Azure<br>. NetworkSecurityGroupsUsage: Number of Network Security Group instances in use for the region and subscription<br>. StaticPublicIPAddressesLimit: Maximum amount of Static Public IP Addresses for the region and subscription as reported by Azure<br>. StaticPublicIPAddressesUsage: Number of Static Public IP Addresses in use for the region and subscription<br>. VirtualNetworksLimit: Maximum amount of Virtual Networks for the region and subscription as reported by Azure<br>. VirtualNetworksUsage: Number of Virtual Network instances in use for the region and subscription<br>. ApplicationGatewaysLimit: Application Gateway limit for the region and subscription as reported by Azure<br>. ApplicationGatewaysUsage: Number of Application Gateway instances in use for the region and subscription<br>. NetworkWatchersLimit: Maximum amount of Network Watchers for the region and subscription as reported by Azure<br>. NetworkWatchersUsage: Number of Network Watcher instances in use for the region and subscription<br>. PacketCapturesLimit: Maximum amount of Packet Capture instances for the region and subscription as reported by Azure<br>. PacketCapturesUsage: Number of Packet Capture instances in use for the region and subscription<br>. RouteFiltersLimit: Maximum amount of Route Filters for the region and subscription as reported by Azure<br>. RouteFiltersUsage: Number of Route Filter instances in use for the region and subscription<br>. RouteTablesLimit: Maximum amount of Route Tables for the region and subscription as reported by Azure<br>. RouteTablesUsage: Number of Route Table instances in use for the region and subscription<br>. PercentApplicationGatewaysUsage: Calculates and monitors the utilization percentage of Application Gateways<br>. PercentLoadBalancersUsage: Calculates and monitors the utilization percentage of Load Balancers<br>. PercentNetworkInterfacesUsage: Calculates and monitors the utilization percentage of Network Interface Instances |

| Azure Virtual Network | |
|---|---|
| | . PercentNetworkSecurityGroupsUsage: Calculates and monitors the utilization percentage of Network Security Groups<br>. PercentNetworkWatchersUsage: Calculates and monitors the utilization percentage of Network Watcher Instances<br>. PercentPacketCapturesUsage: Calculates and monitors the utilization percentage of Packet Capture Instances<br>. PercentPublicIPAddressesUsage: Calculates and monitors the utilization percentage of Dynamic Public IP Addresses<br>. PercentRouteFiltersUsage: Calculates and monitors the utilization percentage of Router Filters<br>. PercentRouteTablesUsage: Calculates and monitors the utilization percentage of Route Tables<br>. PercentStaticPublicIPAddressesUsage: Calculates and monitors the utilization percentage of Static Public IP Addresses<br>. PercentVirtualNetworksUsage: Calculates and monitors the utilization percentage of Virtual Network Instances |
| **Service Limitation** | . Create specific dashboards and personalized views of reports |

*Table 8 Azure Virtual Network*

| Azure Storage Account | |
|---|---|
| **Overview** | An Azure storage account contains the storage data objects: blobs, files, queues, tables, and disks. |
| **Setup Activities** | . Create storage account |
| **Service Request** | . Create storage container<br>. Download a blob from Azure Storage<br>. Change the Size of a volume |
| **Available Monitors** | . Availability<br>. Egress<br>. Ingress<br>. Status<br>. Success E2E Latency<br>. Success Server Latency<br>. Transactions |
| **Service Limitation** | . Create specific dashboards and personalized views of reports |

*Table 9 Azure Storage Account*

| DNS Services | |
|---|---|
| **Overview** | Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure |
| **Setup Activities** | . Create DNS Zones<br>. Create DNS records<br>. Delegation of DNS zones |
| **Service Request** | . Create, change or delete DNS zones<br>. Create, change or delete DNS records |
| **Available Monitors** | . Availability State<br>For other Azure DNS monitoring is needed Azure Monitor and the logs can be route to:<br>• Azure Storage Account: For long term retention<br>• Event Hub: for integration with Splunk (not included in the services)<br>• Azure Log Analytics Workspace: to analyze the data and create dashboards and alert on specific events |
| **Service Limitation** | Event Hub Management or Log Analytics Workspace management are not included under this service. |

*Table 10 DNS Services*

| VPN Gateway | |
|---|---|
| **Overview** | A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. |
| **Setup Activities** | . Create VPN gateway<br>. Configure point-to-site VPN connection<br>. Configure site-to-site VPN connection<br>. Configure IPSec/IKE policy |
| **Service Request** | . Resize a VPN gateway<br>. Reset tunnels<br>. Addition of or changes to point-to-site or site-to-site VPN connection in the same gateway |
| **Available Monitors** | . Tunnel Average Bandwidth<br>. Tunnel Egress Bytes<br>. Tunnel Egress Packet Drop TS Mismatch<br>. Tunnel Egress Packets<br>. Tunnel Ingress Bytes<br>. Tunnel Ingress Packet Drop TS Mismatch<br>. Tunnel Ingress Packets |
| **Service Limitation** | |

*Table 11 VPN Gateway*

| Azure Load Balancer | |
|---|---|
| **Overview** | **a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs**. |
| **Setup Activities** | . Create public or Internal Load balancer<br>. Set VMs inbound NAT rules<br>. Integrate NAT gateway to a load balancer |
| **Service Request** | . Add Vms in to existing Load balancer<br>. Add new LoadBalancers in-front of vms. |
| Available Monitors | . byteTransmissionRateionRate<br>. DataPathAvailability<br>. HealthProbeStatus<br>. PacketTransmissionRate<br>. SNATAllocatedPorts<br>. SNATConnectionCount<br>. SNATUsedPorts<br>. SYNCount<br>. SNATUsedPortsPercentage |
| **Service Limitation** | . Load balancers are under scope when the services behind them are in scope |

*Table 12 Azure Load Balancer*

| Azure Key Vault | |
|---|---|
| **Overview** | Azure Key Vault safeguards cryptographic keys and other secrets used by cloud apps and services.<br>This Services can be integrated with:<br>. Azure Disk Encryption<br>. Always-encrypted and Transparent Data Encryption functionality in SQL server and Azure SQL Database<br>. Azure App Service |

| Azure Key Vault | |
|---|---|
| | . Storage accounts<br>. Event hub, and log analytics |
| **Setup Activities** | . Create Key vault service<br>. Set a certificate from key vault<br>. Set a key from key vault<br>. Set a secret |
| **Service Request** | . Import HSM- protected keys |
| **Available Monitors** | . Vault Availability<br>. Vault Saturation<br>. Service API Latency<br>. Total Service API Hits (Filter by Activity Type)<br>. Error Codes (Filter by Status Code) |
| **Service Limitation** | All Azure services integrated with key vault must be managed by NTT MHIS. |

*Table 13 Azure Key Vault*

1.5 Managed Infrastructure Services (Networking)

(a) PaaS and SaaS Networking

(i) Overview

This element of the service covers the configuration, monitoring and management of PaaS and SaaS Networking services. Charges are based on the number of instances of each technology present in the environment specified in the SOW.

(ii) Supported Technologies

- Azure CDN
- Azure Front Door
- Azure Application Gateway
- Traffic Manager

| Azure CDN | |
|---|---|
| **Overview** | Azure CDN provides secure and reliable global content delivery and acceleration. |
| **Setup Activities** | . Create a Profile and endpoint<br>. Create alias record for zone apex<br>. Register Client domain on CDN<br>. Enable HTTPS on client Domain<br>. Enable compression<br>. Create cache rules<br>. Configure time to live (TTL) |
| **Service Request** | . Create/Change/Delete alias record for zone apex<br>. Restrict content by country/region<br>. Purge/Preload content |
| **Available Monitors** | . Resource health |
| **Service Limitation** | Design of optimization choices is not included as part of the service. |

*Table 14 Azure CDN*

| Azure Front Door | |
|---|---|
| **Overview** | Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. |
| **Setup Activities** | . Create Front Door Resource<br>. Add custom domain to Front Door<br>. Configure HTTPS on the Front Door service |

| Azure Front Door | |
|---|---|
| | . Setup Geo-filtering WAF policy for Front Door<br>. Configure rules engine |
| **Service Request** | . Configure Geo-filtering WAF policy for Front Door<br>. Change rule engine |
| **Available Monitors** | . Request count<br>. Request size<br>. Response size<br>. Total latency<br>. Backend request count<br>. Backend request latency<br>. BackendHealthPercentage<br>. Web Application Firewall request count |
| **Service Limitation** | Design and routing architecture is not included in this service. |

*Table 15 Azure Front Door*

| Azure Application Gateway | |
|---|---|
| **Overview** | Azure Application Gateway is a web traffic load balancer that enables management traffic through web applications. |
| **Setup Activities** | . Create the application gateway<br>. Configure Front-ends and backend pool<br>. Add routing rules<br>. Create a self-signed certificate |
| **Service Request** | . Add/remove or change routing rules |
| **Available Monitors** | . Current Connections: Count of current connections established with application gateway<br>. Failed Requests: Count of failed requests that the application gateway has served<br>. Healthy Host Count: Number of unhealthy backend hosts<br>. Total Requests: Count of successful requests that application gateway has served<br>. Unhealthy Host Count: Count of failed requests that application gateway has serve<br>. Throughput:  Number of bytes per second the application gateway has served |
| **Service Limitation** | |

*Table 16 Application Gateway*

| Azure Traffic Manager | |
|---|---|
| **Overview** | Azure Traffic Manager is a DNS-based traffic load balancer that enables the optimal distribution of traffic to services across global Azure regions, while providing high availability and responsiveness. |
| **Setup Activities** | . Create a Traffic Manager profile<br>. Add endpoints<br>. Configure endpoint monitoring<br>. Configure load balancing method |
| **Service Request** | . Delete Traffic Manager profile<br>. Add Traffic Manager endpoints<br>. Change load balancing method |
| **Available Monitors** | . Probe agent current endpoint state<br>. Queries by endpoint |
| **Service Limitation** | |

*Table 17 Azure Traffic Manager*

(b) Cloud Direct Connectivity

(i) Overview

This element of the service covers the configuration, monitoring and management of Express Route and Azure Virtual WAN. Charges for ExpressRoute are based on individual ExpressRoute redundant circuits specified in the SOW. Charges for Azure Virtual WAN are based on each individual Virtual Wan Hub, plus the number of individual circuits attached to the Hub as specified in the SOW.

(ii) Supported Technologies

- Azure ExpressRoute
- Azure Virtual WAN

| ExpressRoute | |
|---|---|
| **Overview** | ExpressRoute services allow the extension from on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. |
| **Setup Activities** | . Create and provision ExpressRoute circuit<br>. Create peering configuration<br>. Configure routing |
| **Service Request** | . Link a VNet to an ExpressRoute circuit<br>. Creation and management of routes<br>. Changes to the contracted bandwidth (additional cost from Azure) |
| **Available Monitors** | . Bits-In Per Second: Amount of data ingressing Azure, in bits per second<br>. Bits-Out Per Second: Amount of data egressing Azure, in bits per second<br>. Bandwidth BPS: Service provider circuit fixed bandwidth, in bits per second<br>. Bandwidth Utilization: Percent utilization of the fixed bandwidth<br>. Total Bit: Total combined bandwidth of ingressing and egressing data, in bits per second |
| **Service Limitation** | On-prem Edge devices management are not included in this service and must be contracted separately. |

*Table 18 ExpressRoute*

| Azure Virtual WAN | |
|---|---|
| **Overview** | Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface.<br><br>These functionalities include branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE), site-to-site VPN connectivity, remote user VPN (point-to-site) connectivity, private (ExpressRoute) connectivity, intra-cloud connectivity (transitive connectivity for virtual networks), VPN ExpressRoute inter-connectivity, routing, Azure Firewall, and encryption for private connectivity. |
| **Setup Activities** | . Create a Virtual WAN<br>. Create the Virtual Hub<br>. All the activities included for Express Route and Virtual WAN are included |
| **Service Request** | . Upgrade Virtual WAN SKU<br>. All Service Request for ExpressRoute and VPN Gateway are included |
| **Available Monitors** | <u>Site to Site VPN Gateway:</u><br><br>. Gateway Bandwidth – Average site-to-site aggregate bandwidth of a gateway in bytes per second<br>. Tunnel Bandwidth – Average bandwidth of a tunnel in bytes per second<br>. Tunnel Egress Bytes – Outgoing bytes of a tunnel<br>. Tunnel Egress Packets – Outgoing packet count of a tunnel<br>. Tunnel Egress TS Mismatch Packet Drop – Outgoing packet drop count from traffic selector mismatch of a tunnel<br>. Tunnel Ingress Bytes – Incoming bytes of a tunnel<br>. Tunnel Ingress Packet – Incoming packet count of a tunnel<br>. Tunnel Ingress TS Mismatch Packet Drop – Incoming packet drop count from traffic selector mismatch of a tunnel<br><br><u>Point To Site VPN Gateway:</u><br><br>. Gateway P2S Bandwidth – Average point-to-site aggregate bandwidth of a gateway in bytes per second<br>. P2S Connection Count – point-to-site connection count of a gateway |

| Azure Virtual WAN | |
|---|---|
| | Express Route Gateway:<br><br>. BitsInPerSecond – Ingress Bits per second<br>. BitsOutPerSecond – Egress Bits per second |
| **Service Limitation** | |

*Table 19 Azure Virtual WAN*

1.6 Managed Infrastructure Services (Security)

(a) PaaS and SaaS Network Security

(i) Overview

This element of the service covers the configuration, monitoring and management of PaaS and SaaS Network Security services. Charges are based on the number of instances present in the environment as specified in the SOW.

(ii) Supported Technologies

- Azure Firewall
- Azure DDoS

| Azure Web Application Firewall | |
|---|---|
| **Overview** | Web Application Firewall (WAF) provides centralized protection of Client web applications from common exploits and vulnerabilities.<br><br>This Azure service can be deployed on Azure Application Gateway, Azure Front Door, Azure CDN |
| **Setup Activities** | . Create WAF policies<br>. Customize WAF Rules<br>. Configure IP Restriction rule (for Front Door)<br>. Setup Geo-filtering WAF policy (for Front Door)<br>. Configure DDoS Attack mitigation reports |
| **Service Request** | . Change or delete WAF policy<br>. Change a WAF Rules |
| **Available Monitors** | |
| **Service Limitation** | Azure App Gateway, Azure Front Door or Azure CDN Management should be contracted<br>No Security or SOC activities are included in this services. |

*Table 20 Azure Web Application Firewall*

| Azure Firewall | |
|---|---|
| **Overview** | Azure Firewall is a managed, cloud-based network security service that protects Azure Virtual Network resources |
| **Setup Activities** | . Deploy Azure Firewall<br>. Create Network rules<br>. Create application rules<br>. Create NAT rules (only destination NAT from Internet to Azure)<br>. Active Threat intelligence |
| **Service Request** | . Create change and delete access rules |
| **Available Monitors** | . Availability State<br>. Advance Monitoring with Azure Monitor and the logs can be route to:<br>• Azure Storage Account: For long term retention<br>• Event Hub: for integration with Splunk (not included in the services)<br>• Azure Log Analytics Workspace: to analyze the data and create dashboards and alert on specific events |

| Azure Firewall | |
|---|---|
| **Service Limitation** | . Security policy definition: this is a consultancy task which must be contracted in addition to the Service<br>. Event Hub Management and Log Analytics Workspace management are not included as part of the Service. |

*Table 21 Azure Firewall*

| Azure DDoS | |
|---|---|
| **Overview** | Distributed Denial of Service (DDoS) Protection as a service for Azure Resources |
| **Setup Activities** | . Create a DDoS protection plan<br>. Enable DDoS for virtual networks<br>. Configure the alert for DDoS notification<br>. Configure Central Security Log Management<br>. Enable Audit Logging<br>. Configure security log storage retention |
| **Service Request** | . Disable DDoS on specific Virtual Network<br>. Request Log information for postmortem analysis |
| **Available Monitors** | Monitoring with Azure Monitor and the logs can be route to:<br>. Azure Storage Account: For long term retention<br>. Event Hub: for integration with Splunk (not included in the services)<br>. Azure Log Analytics Workspace: to analyze the data and create dashboards and alert on specific events |
| **Service Limitation** | . Security and Networking design are not included as part of this service<br>. Postmortem analysis<br>. Penetration Test is not included as part of this service.<br>. Event hub, Log Analytics Management are not included in this service |

*Table 22 Azure DDoS*

1.7 Managed Infrastructure Services (Compute)

(a) IaaS Scaling Group (Elastic)

(i) Overview

This element of the service covers the configuration, monitoring and management of elastic scaling groups. Charges are based on the number of Scaling Groups, regardless of the number of VMs that may be running during a certain period of time.

(b) Supported Technologies

- Virtual Machine Scale Set

| Azure Virtual Machine Scale Set | |
|---|---|
| **Overview** | Scales Sets allow for on-demand creation and management of a group of identical, load balanced VMs. |
| **Setup Activities** | . Creation of scale set profile<br>. Creation of Autoscale out/in rules<br>. Configure network security group<br>. Configure Availability Set<br>. Configure Autoscaling<br>. Configure Azure Load Balancer<br>. Generate CPU load, to test the Autoscale automation or the Autoscale rules in a Scale Set |
| **Service Request** | . Change the capacity of a scale set<br>. Change rules to scale out/scale in<br>. Start/restart, stop and de-allocate VM instances in a scale set<br>. Creation or changes to Azure Load Balancer policies for Scale Sets<br>. Changes to the assigned public IP address and port number |

| Azure Virtual Machine Scale Set | |
|---|---|
| | . Creation or changes to Network security groups<br>. Generate CPU load, to test the Autoscale automation or the Autoscale rules in a Scale Set |
| **Available Monitors** | Individual and Total aggregate disk operations and CPU utilization metrics.<br>. Disk Read Operations Per Sec (individual VMs in scale set): Average disk read IOPS on the VM<br>. Disk Write Operations Per Sec (individual VMs in scale set): Average disk write IOPS on the VM<br>. Percentage CPU (individual VMs in scale Set): The percentage of allocated compute units that are currently in use by the VM<br>. Disk Read Operations Per Sec (scale set aggregation): Average disk read IOPS on the scale set aggregation<br>. Disk Write Operations Per Sec (scale set aggregation): Average disk write IOPS on the scale set aggregation<br>. Percentage CPU (scale set aggregation): The percentage of allocated compute units that are currently in use by the on the scale set aggregation |
| **Service Limitation** | Operating System Management is not included and must be contracted separately. |

*Table 23 Azure Virtual Machine Scale Set*

(c) IaaS- VM (Static)

(i) Overview

This element of the service covers the configuration, monitoring and management of static VMs. Charges are based on the number of virtual machines under management as specified in the SOW.

(ii) Supported Technologies

- Azure Virtual Machine

| Azure virtual Machine | |
|---|---|
| **Overview** | On-demand, scalable computing resources |
| **Setup Activities** | . Creation of Virtual Machines<br>. Create Virtual Machine images<br>. Configure network security groups<br>. Configure NICs, private IPs, public IP address<br>. Configure Availability Set<br>. Configure Azure Load Balancer (if it necessary) |
| **Service Request** | . Creation of new Virtual Machines (additional monthly fees may apply)<br>. Start/restart, stop and delete Virtual Machines<br>. Creation or changes to Virtual Machine images (included only if OS is managed)<br>. Creation or changes to Network security groups<br>. Management of reserved or NICs, private and public IP address<br>. Changes to Azure Load Balancer policies |
| **Available Monitors** | . Percentage CPU: The average percentage of allocated compute units that are currently in use by the Virtual Machine(s)<br>. Network In: The average number of bytes received, per second, on all network interfaces by the Virtual Machine(s)<br>. Network Out: The average number of bytes sent, per second, on all network interfaces by the Virtual Machine(s)<br>. Disk Read Bytes: Average number of bytes, per second, read from the disk<br>. Disk Write Bytes: Average number of bytes, per second, written to disk<br>. Disk Read Operations Per Sec: Average number of read operations, per second, on the disk<br>. Disk Write Operations Per Sec: Average number of write operations, per second, on the disk |
| **Service Limitation** | Operating System Management is not included and must be contracted separately. |

*Table 24 Azure Virtual Machine*

(d) Cloud VM Scheduling

(i) Overview

This element of the service covers the configuration, of start/stop scheduling for Azure VMs. Charges are based on the number of virtual machines with scheduling as specified in the SOW.

(ii) Supported Technologies

- Azure Automation

| VM Scheduling | |
|---|---|
| **Overview** | Cloud-based automation and configuration service |
| **Setup Activities** | . Creation of Automation Account<br>. Enable start/stop Vms schedule |
| **Service Request** | . Add or exclude VMs from the schedule<br>. Modify schedules<br>. Configure email notifications |

*Table 25 VM Scheduling*

1.8 Managed Infrastructure Services (Storage)

(a) Cloud PaaS File Storage

(i) Overview

This element of the service covers the configuration, monitoring and management of Azure File and Azure File Sync. Charges are based on the number of instances present in the environment as specified in the SOW.

(ii) Supported Technologies

- Azure File
- Azure File Sync

| Azure File | |
|---|---|
| **Overview** | Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments. |
| **Setup Activities** | . Create a File Shares<br>. Mount SMB or NFS file share on a VM (VM, and OS management is needed for this option)<br>. Configure Azure Files Network endpoints<br>. Configure DNS forwarding<br>. Enable AD SD authentication<br>. Assign share-level permission<br>. Assign directory/file - level permission<br>. Create a storage account failover |
| **Service Request** | . Change share-level permission<br>. Add and azure file sync server endpoint |
| **Available Monitors** | . Storage Read. Storage Write<br>. Storage Delete |
| **Service Limitation** | |

*Table 26 Azure File*

| Azure File Sync | |
|---|---|
| **Overview** | Azure File Sync centralizes your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of an Azure file share. |
| **Setup Activities** | . Configure Network Endpoints<br>. Create a sync group<br>. Configure file sync proxy and firewall settings<br>. Install the Azure File Sync agent in the server<br>. Install the Azure File Sync agent updates<br>. Deploy the storage sync service<br>. Register Windows server with storage sync service |

| Azure File Sync | |
|---|---|
| **Service Request** | . Add and azure file sync server endpoint<br>. Change the auto-upgrade setting |
| **Available Monitors** | . Bytes Synced<br>. Cloud Tiering recall<br>. Cloud tiering recall size<br>. Cloud tiering recall size by application<br>. Cloud tiering recall throughput<br>. Files not syncing<br>. Files synced<br>. Server online status<br>. Sync session result |
| **Service Limitation** | This services requires VM management and OS Management (OS Management contracted separately). |

*Table 27 Azure File Sync*

(b) Azure NetApp File Storage

(i) Overview

This element of the service covers the configuration, monitoring, and management of Azure NetApp File storage. Charges are based on number of Netapp File services present in the environment as specified in the SOW.

(ii) Supported Technologies

- Azure NetApp File

| Azure NetApp File | |
|---|---|
| **Overview** | Enterprise file storage, powered by NetApp |
| **Setup Activities** | . Registration for Azure NetApp Files and NetApp Resources Provider<br>. Create a NetApp Account<br>. Set Up a capacity Pool<br>. Create NFS volume<br>. Create AD connection<br>. Mount a volume for VMs<br>. Create volume replication |
| **Service Request** | . Resize a capacity pool or a volume<br>. Mount or unmount a volume for VMs<br>. Create an on-demand snapshot for a volume<br>. Delete volume replication |
| **Available Monitors** | . Pool Allocated Size<br>. Pool Allocated to Volume Size<br>. Pool Consumed Size<br>. Total Snapshot Size for the Pool<br>. Percentage Volume Consumed Size<br>. Volume Allocated Size<br>. Volume Quota Size<br>. Volume Consumed Size<br>. Volume Snapshot Size<br>. Average Read Latency<br>.Average Write Latency<br>.Read IOPS<br>.Write IOPS<br>. Is volume replication status healthy<br>. Is volume replication transferring<br>. Volume replication lag time<br>. Volume replication last transfer duration<br>. Volume replication last transfer size<br>. Volume replication progress<br>. Volume replication total transfer |

| Azure NetApp File | |
|---|---|
| **Service Limitation** | Mounting and unmounting volumes on active VMs are only covered when VM and OS management are also contracted. |

*Table 28 Azure NetApp File*

1.9 Cloud Identity

(a) Cloud Identity & Domain

(i) Overview

This element of the service covers the configuration, monitoring and management of Cloud Identity services. Charges are based on the number of features enabled in the environment as specified in the SOW.

(ii) Supported Technologies

- Azure Active Directory
- Azure AD Connect

| Azure Active Directory | |
|---|---|
| **Overview** | Azure Active Directory is a cloud-based identity and access management service which manages end-user authentication and access.<br><br>. External resources, such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications<br><br>. Internal resources, such as apps on a corporate network and intranet, along with cloud apps developed |
| **Setup Activities** | . Create a new tenant in Azure AD<br>. Create Groups and users for external users<br><br><u>For Azure Active Directory Basic tier:</u><br><br>. Register Applications on a Azure AD<br>. Installation Application Proxy Connector on the Application Proxy Server*<br>. Configure Single Sign-on for Application Proxy application<br>. Enable Azure AD Multifactor Authentication<br>. Enable self-Service password reset<br><br><u>For Azure AD Premium P1 Licenses</u><br><br>All previous activities are included, plus:<br><br>. Apply Conditional Access policies<br>. Install Azure AD Connect at on-prem environment (only if management of on-premises AD is also contracted)<br><br>. Install Azure AD Connect on the server<br>. Install Azure AD Connect Health agent<br>. Configure staging mode<br>. Enabling device/group writeback<br>. Configure AD SD connector account permissions<br>. Create synchronization rules<br>. Configure scheduler<br>. Enable on-prem integration with Azure AD password Protection<br><br>. Deploy azure AD multi-factor Authentication using Conditional Access policies<br><br><u>For Azure AD Premium P2 Licenses</u><br><br>All previous activities are included, plus:<br><br>. Enable risk-based conditional access<br>. Enable Azure AD Identity Protection and risk policies<br>. Enable Azure AD Privilege Identity Management (PIM)<br>. Give eligible assignments<br>. Allow eligible users to activate their Azure AD Role Just-in-time<br>. Configure security alerts for azure Ad roles<br>. Configure Azure AD PIM Alers |
| **Service Request** | <u>For Azure Active Directory Basic tier:</u> |

| Azure Active Directory | |
|---|---|
| | . Change or add additional domain names to Azure AD<br>. Add or delete groups, members and users<br>. Change MFA policy<br>. Creation, deletion and changes of the users and groups in the system, including changing home directories, group assignment, shell and password maintenance in case of non-Active Directory User (external AD User)<br><br>For Azure AD Premium P1 Licenses<br>. Map Client organizational roles to Azure technical roles; if on-premise Active Directory management is also contracted, management for hybrid identity solution.<br>. Change synchronization options for Azure AD connect<br>. Refresh directory schema<br>. enable / disable staging mode<br>. Upgrade AD Connect<br>. change filtering option<br>. Change synchronization rules<br><br>For Azure AD Premium P2 Licenses<br>. Change risk policy<br>. Test policies impact by risk simulation (only with Premium P2)<br>. Respond to Azure AD PIM Alerts |
| **Proactive Tasks** | . AD synchronisation; according to Client requirements, in case of Hybrid Identity Management |
| **Available Monitors** | Sync status for Azure AD Connect<br>For Azure AD advance monitoring is not included by default, Azure AD monitoring logs can be routed to:<br>. Azure Storage Account: For long term retention<br>. Event Hub: For integration with Splunk<br>. Azure Log Analytics Workspace: To analyze the data and create dashboards and alert on specific events |
| **Service Limitation** | .OS Management are needed for managing Application Proxy Connector<br>.AD design and best practice for Client organisational requirements are not included as part of this service, consultancy sprints can be added separately<br>. Hybrid identity solution design is not included as part of this service.<br>Event Hub Management and is not included under this service. |

*Table 29 Azure Active Directory*

| Azure AD External Identities | |
|---|---|
| **Overview** | External Identities is a set of capabilities that enables organizations to secure and manage any external user, including Clients and partners (B2C and B2B).<br>• Azure AD B2C is a cloud-based identity and access management service that manages end-user authentication and access to resources using their preferred social, enterprise, or local account identities<br>• Azure AD B2B is collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization |
| **Setup Activities** | for Azure AD B2C<br>. Create a new tenant Azure B2C tenant<br>. Register web applications<br>. Client secrets creation<br>. Create sign-in user flows<br>. Create sign-up user flows<br>. Enable multi-factor authentication<br>. Enable self-service password reset<br>for Azure AD B2B . Add guest users<br>. Enable MFA for guest users<br>. Enable B2B external collaboration |

| Azure AD External Identities | |
|---|---|
| | . Assign the Guest inviter role to a Client user<br>. Create conditional access policy for guest users |
| **Service Request** | for Azure AD B2C . Create or edit users flow<br>. Add identity providers<br>. Change MFA policy<br>. Setup Identity protección<br><br>for Azure AD B2B . Add guest users<br>. Run script to send invitations in bulk (Client need to provide the CSV file with user information)<br>. change conditional access policies for guest users |
| **Available Monitors** | Azure AD B2C and monitoring logs can be route to:<br><br>. Azure Storage Account: For long term retention<br>. Event Hub: for integration with Splunk<br>. Azure Log Analytics Workspace: to analyze the data and create dashboards and alert on specific events |
| **Service Limitation** | . Users migrations<br>. Event hub or advance Analytics management is not included as part of this service |

*Table 30 Azure AD External Identities*

1.10 Managed Data Protection

(a) Cloud Backup

(i) Overview

This element of the service covers the configuration, monitoring and management of Cloud Backup. Charges are based on the number of regions where managed resources are protected, regardless of the number of VMs protected as specified in the SOW.

(ii) Technology Supported

- Azure Backup for Azure VMs Using Backup Extensions

| Azure Backup | |
|---|---|
| **Overview** | Azure Backup is a simple, secure, and cost-effective solution for backing up and recovery of data for Azure.<br><br>NTT Supports using Azure Backup for protecting Azure VMs using the backup extension |
| **Setup Activities** | . Create a recovery Service Vault<br>. Install Backup Extension on VMs<br>. Configure Backup Policy<br>. Enable Soft delete<br>. Create recovery service vault<br>. Enable Backups for VMs<br>. Create the backup policy (Scheduling and retention)<br>. Set storage redundancy option |
| **Service Request** | . Restore a VM<br>. Add Modify/Delete Backup policy<br>. Stop Backup and retain data.<br>. Request Soft Delete<br>. Enable / disable soft delete .Request on-demand backup<br>. Restore from recovery point<br>. Add/remove VM's to/from the backup policy |
| **Available Monitors** | . Azure Backup Job Duration<br>. Azure Backup Job Status<br>. Hours Since Last Backup<br>. Protection Status<br>. Protection State |
| **Service Limitation** | Azure VMs |

| Azure Backup | |
|---|---|
| | . VMs are backed up no more than once-a-day<br>. Restore VMs only at disk level or file level<br>. Requests to restore from backup may not exceed NTT's Fair Use Policy as stated in the Service Delivery section of the *Client Service Description.*<br><br>Azure Backup On-Prem (MARS)<br>• No central management<br>• Heavy touch – each machine needs configuration, and management/monitoring isn't centralized<br>• No application awareness<br>• RTO and RPO will be higher than a standard backup solution |

*Table 31 Azure Backup*

## 1.11 Disclaimer

Please note that Service Requests and monitors described in this service description represent only a sample and are subject to change due the rapidly evolving offering from Microsoft.

Monitors are subject to change as per the Service Improvement Process.

All scope is subject to the limitations of the Microsoft Online Service Terms, the SOW, and the Agreement under which the Microsoft services are procured by Client.