1 Complementary Services for AWS - Containers

This service description include the Service Descriptions for the Management of Containers services on Amazon Web Services (AWS) and is an add-on to *Public Cloud Management - Core Services for AWS* Service Description
Manage AWS Container services covers the following

1.1 Overview of Service

NTT's Managed Service for container platforms is designed to help Clients focus on application development. The Service provides the operation of a container platform, and may include a security and compliance 'wrapper' for container clusters so that containers are deployed with adherence to industry best-practices and any Client compliance requirements if expressly in scope in the SOW. Only the specified containers in the SOW are in scope, otherwise it is out of scope.

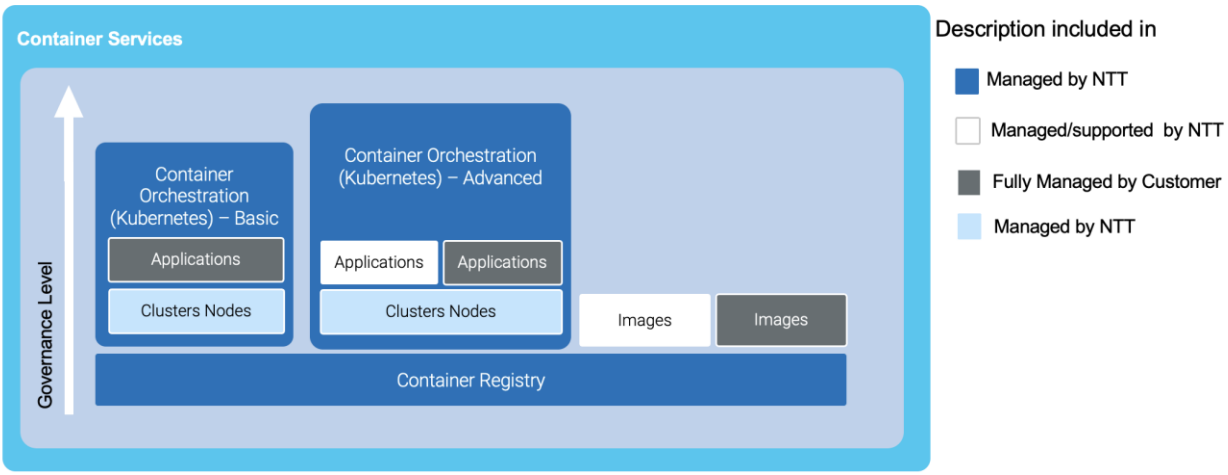
Management of underlying infrastructure including NTT Private Cloud (NTT Anywhere or MSP), Public Cloud "Core Services", operating systems and/or virtual servers is expressly out of scope and must be contracted separately.

1.2 Supported Services

Only the following solutions are supported and the selected service must be expressly identified as in scope in the SOW:

Managed Element	Supported Services
Managed Container Registry	Elastic Container Registry (ECR)
Managed Cloud-Container Orchestration (Kubernetes) - Basic	Elastic Kubernetes Services (EKS)
Managed Cloud-Container Orchestration (Kubernetes) - Advanced	Elastic Kubernetes Services (EKS)
Managed Public Cloud-Container as a Service	Amazon Elastic Container Service (Amazon ECS)
Container Image	N/A
Container Application	N/A

Container Services are based on several Managed Service elements shown in the diagram below:



(a) Managed Container Registry

(i) Managed Service Overview

This element of the service covers the configuration, monitoring and management of the Container Registry that hosts the container images used for the Container services.
Charges are based on number of Container registries

Container Registry	
Cloud Service Overview	Service to store multiple versions of private container images to be pulled from Container services.
	Deployment and configuration of container registry . May include parameters such as region replication, when available by the public cloud provider.

Container Registry	
Setup Activities	Access and RBAC configuration . Subject to NTT risk analysis NTT may setup Role Based Access Controls (RBAC), applying the least privilege principle, so the Client can autonomously deploy and update container images not managed by NTT; see Service Limitations section.
	Creation and configuration of image repositories . May include locking repositories or images or changing tag mutability, when available by the public could provider.
Recurrent Services	Management, monitoring and incident response of in scope container registry
Service Requests	Container registry configuration change
	Access and RBAC changes
	Creation, change and deletion of image repositories
Service Limitations	. Container image deployment is out of scope . Container image vulnerability scanning in scope only if feature is supported and limited to events originated by a Managed Container Image . Any other service request not expressly listed above is out of scope . Anything not expressly identified as above and in scope in the SOW is expressly out of scope. . Client access may be limited if in NTT's sole discretion it prevents or conflicts with NTT management activities . Container images, including the those used by the add-ons required for NTT management, will be pulled from private container registries only (public registries are not supported)
Client Responsibilities	. Client must provide NTT with a list of external container images to replicate

(b) Container Orchestration (Kubernetes)

(i) Managed Service Overview
This element of the service covers the configuration, monitoring and management of Kubernetes cluster nodes identified in scope in the SOW, service is available in two tiers (Basic and Advanced) selected in the SOW.
NTT will manage permissions and access, providing the Client with the least privileged access to the cluster based on the Client's agreed responsibilities.
Charges are based on the quantity of managed clusters within the solution

Client may select either the *Basic* or *Advanced* service level, based on their requirements which shall be stated as in scope in the SOW.

(ii) Supported Kubernetes Versions
NTT will only support major and every other (odd) minor Kubernetes versions while they remain supported by the vendor. If there are any additional resources required to upgrade, NTT will charge a Fee for the costs of the upgrade. New versions released by the vendor and matching the NTT version cadence will trigger NTT version certification process. Only one minor upgrade release will be provided annually, no major upgrade are included in the scope and are out of scope.

Public Cloud Container Orchestration (Kubernetes)		Basic	Advanced
Cloud Service Overview	Platform for managing containerized workloads and services, that facilitates both declarative configuration and automation The Advanced tier is required by Managed Container (Kubernetes) Applications and is recommended unless the Client has already implemented a mature Kubernetes practice and expects limited guidance and support from NTT. Mentions to the cluster can refer to the cluster as a whole or to one or several elements including but not limited to the control plane, the node groups (and its scaling), the nodes (and its types) or the pod or storage orchestration.		
Requirements	Managed Container Registry must be in scope in the SOW.		
	Deployment and configuration of cluster	✅	✅

Sensitivity Label: General

Public Cloud Container Orchestration (Kubernetes)		Basic	Advanced
Setup Activities	. Node types and node group scaling of node groups hosting Client workloads to be determined based on the in-scope of the SOW. . If NTT add-ons run on a dedicated node group, node types and node group scaling of that node group is at NTT's sole discretion based on NTT management requirements.		
	Deployment of NTT standard cluster policies . May include Pod Security Standards (three levels of cumulative policies ranging from highly-permissive to highly-restrictive) as selected by the Client within 30 days of the effective date of the SOW.	✓	✓
	Creation of custom cluster policies . Custom policies must not conflict with NTT standard cluster policies or NTT cluster management . NTT can optionally review, adapt and apply custom policies provided by the Client in NTT's sole discretion.	✗	✓
	Access and RBAC configuration . Subject to NTT risk analysis NTT may setup RBAC, applying the least privilege principle, so the Client can autonomously deploy manifests or applications not managed by NTT; see Service Limitations section.	✓	✓
	NTT Infrastructure & Service add-on deployment and configuration deployment and configuration . See *Kubernetes Add-ons* section.	✓	✓
	NTT Application add-on deployment and configuration . See *Kubernetes Add-ons* section.	✗	✓
Recurrent Services	Management, monitoring and incident response of cluster identified as in scope in the SOW	✓	✓
	Management of NTT standard cluster policies using an NTT selected tool set which include: . Pod Security Standards (three levels of cumulative policies ranging from highly-permissive to highly-restrictive) as selected by the Client within 30 days of the effective date of the SOW or . Catalog of NTT approved NTT standard cluster policies as updated by NTT from time to time in NTT's sole and absolute discretion.	✓	✓
	Management of custom cluster policies created by NTT or which NTT has agreed to manage . NTT will review and analyze a Client provided policy . In NTT's sole discretion it may determine a Client provide policy prevents or conflicts with NTT management activities and may not be implemented and may require that Client make changes	✗	✓
	Cluster patch management . Based on the Patch Management process defined in the *Client Service Description*. . Work with Client to establish a maintenance window to apply patches at a maximum of once per month. . Limited to patches that keep full-feature compatibility within the current cluster minor version. . In the event that enhancements or changes which are not required for patching are identified during the patch management process, they will be fulfilled following the Service Request process defined in the *Client Service Description*. . Patches are applied to non-production environments before doing so to production. Patches are applied to non-production environments during Business	✓	✓

Sensitivity Label: General

Public Cloud Container Orchestration (Kubernetes)		Basic	Advanced
	Hours only. Patches are applied in production during Business Hours by default. Applying them Out of Business Hours is out-of-scope and must be quoted separately upon client's request.		
	Cluster version upgrade . Limited to the next other (odd) minor version supported by NTT within the current cluster major version. . Unless required by NTT cluster management, after the version upgrade, all cluster elements must use the same version. . Limited to one minor upgrade per year. Major upgrades or additional minor upgrades are out-of-scope and must be quoted separately. . Upgrade to be managed as a project starting only after the required version becomes supported by NTT. . In the event that enhancements or changes which are not required for upgrading versions are identified during the version upgrade process, they will be fulfilled following the Service Request process defined in the *Client Service Description*. . Version upgrades are applied to non-production environments before doing so to production. Version upgrades are applied to non-production environments during Business Hours only. Version upgrades are applied in production during Business Hours by default. Applying them Out of Business Hours is out-of-scope and must be quoted separately upon client's request.	✓	✓
	NTT Infrastructure & Service add-on patch management . As part of cluster patch management and limited to patches that keep full-feature compatibility within the current add-on minor version.	✓	✓
	NTT Infrastructure & Service add-on version minor upgrade, major version upgrades are out of scope and require a separate project at NTT discretion. . Only as part of cluster version upgrades and limited to supported major and minor versions.	✓	✓
	NTT Application add-on patch management . As part of cluster patch management and limited to patches that keep full-feature compatibility within the current add-on minor version. . Limited to those NTT Application add-ons specified in the SOW and only if the required Managed Container (Kubernetes) Application is in scope. . See Kubernetes Add-ons section below.	✗	✓
	NTT Application add-on version upgrade . Only as part of cluster version upgrades and limited to supported major and minor versions. . Limited to those NTT Application add-ons specified in the SOW and only if the required Managed Container (Kubernetes) Application is in scope. . See Kubernetes Add-ons section below.	✗	✓
Service Requests	Control plane access change . As long as it doesn't conflict with NTT management and subject to risk analysis and NTT's sole discretion	✓	✓
	Node types and node group scaling change . Node types and node group scaling of node groups exclusively hosting Client workloads to be determined based on client requirements. . If NTT add-ons run on a dedicated node group, node types and node group scaling of that node group is at NTT's reasonable discretion based on NTT management requirements.	✓	✓
	Changes to NTT standard cluster policies	✓	✓

Sensitivity Label: General

Public Cloud Container Orchestration (Kubernetes)		Basic	Advanced
	. Custom policies must not conflict with NTT standard cluster policies or NTT cluster management . NTT can optionally review, adapt and apply custom policies provided by the client		
	Creation of new custom cluster policies or changes to existing custom policies that NTT has created or accepted to manage	✗	✓
	Creation, change or removal of client namespaces . Namespaces reserved for NTT management include but are not limited to kube-system, ntt*, ntt-	✓	✓
	Access and RBAC changes . See "Access and RBAC configuration"	✓	✓
	NTT Infrastructure & Service add-on patch management . Only on demand if waiting for the next cluster patch management iteration would pose excessive performance or security risk. . Limited to patches that keep full-feature compatibility within the current add-on minor version.	✓	✓
	NTT Application add-on patch management . Limited to those NTT Application add-ons specified in the SOW and only if the required Managed Container (Kubernetes) Application is in scope. . Only on demand if waiting for the next cluster patch management iteration would pose excessive performance or security risk. . Limited to patches that keep full-feature compatibility within the current add-on minor version.	✗	✓
	Request to manage a new Managed Container (Kubernetes) Application . Managed Container Applications are charged on a per Application basis . The Advanced tier is required by Managed Container (Kubernetes) Applications	✗	✓
Service Limitations	. Vendor-provided node OS images are used by default, custom node OS images are not included in the scope and must be contracted separately (OS Management) . Creation or removal of node groups is out of the scope of service requests, it is considered a new setup and must be quoted independently . Despite the fact that NTT can offer node types and node group scaling recommendations based on factors like client requirements and aggregated monitoring metrics, these doesn't constitute a guarantee of future performance . Managed Container (Kubernetes) Applications and Managed Container Images are not included in the service and are out of scope. . Managed Container (Kubernetes) Applications must have Container Orchestration (Kubernetes) - Advanced tier in Scope in the SOW if Managed Container (Kubernetes) Applications is selected In Scope. . Crash-consistent backups of the storage are supported as standard. Application-consistent backups are only available upon request and if the related Container (Kubernetes) Application is in scope. . Providing client with custom cluster monitoring is out of scope. If requested it will be quoted independently, it is at NTT's reasonable discretion to determine if it can be provided as a Managed Container (Kubernetes) Application and Client is responsible for required additional licenses . NTT will not takeover existing kubernetes deployments, a complete redeploy of the kubernetes services will be done using NTT procedures and tooling . Anything not expressly identified as above and in scope in the SOW is expressly out of scope.		
Client Responsibilities	. Client must provide NTT with clear requirements to define or adapt the policies. NTT consulting services are out of scope . Client access may be limited if in NTT's sole discretion it prevents or conflicts with NTT management activities		

Sensitivity Label: General

Public Cloud Container Orchestration (Kubernetes)	Basic	Advanced
	. Client is responsible for defining and deploying all of the services related to their applications. . Client is responsible for defining their applications' resource usage (requests and limits) to ensure cluster capacity. . Client is responsible for using the appropriated storage classes in their applications to ensure data performance and persistence.	

(c) Managed Container (Kubernetes) Application

(i) Managed Service Overview
This element of the service covers the guidance, monitoring and incident response of third-party or client-defined applications running on a managed Kubernetes cluster.
Charges are based on the quantity of applications under management.

Container (Kubernetes) Application	
Service Overview	For purposes of this service description, a Managed Container (Kubernetes) Application is defined as a Kubernetes Workload Resource, Operator or Operator instance and all its ancillary Kubernetes cluster resources implementing a self-contained unit of third-party or client-defined functionality based on Pods that is not required by or included in the contracted Container Orchestration (Kubernetes) cluster management. . Determining on a case by case basis what is a Managed Container (Kubernetes) Application is at NTT's sole discretion, considering factors including but not limited to application complexity. . This definition and the resources included in it are static at the date of the execution of the SOW. . Examples include but are not limited to: - Argo CD application using resources like Deployment, Service and Ingress route - DaemonSet running a 3rd party observability Pod on each cluster node . Application deployment using NTT add-ons
Requirements	. Container Orchestration (Kubernetes) - Advanced must be contracted and in scope in the SOW . Client application repository reachable from the cluster
Setup Activities	Deployment and configuration of required NTT Infrastructure & Service add-ons and NTT Application add-ons . Client must provide NTT with clear application requirements which shall be determined in NTT's sole discretion. NTT consulting services are out of scope . Limited to those NTT Application add-ons required by the application and specified in the SOW
	If required and defined by Client, application-consistent backups
	Application manifest definition recommendations . Application definition can't conflict with NTT Container Orchestration (Kubernetes) management . Application manifest definition recommendations can include but it is not limited to: resource types, resource assignation (request, limits, VPA), deployment and HA strategy (including HPA and PDB), probes (startup, readiness, liveness), etc.
	Optionally, guidance with initial application deployments
Recurrent Service	Monitoring and incident response of the application ancillary Kubernetes cluster resources and the exposed public endpoint, if any . Client must provide NTT with an escalation procedure matching the NTT required availability of the Service . The Managed Container (Kubernetes) Application ancillary Kubernetes cluster resources may need to be in a specific namespace
	Application Continuous Delivery (CD) using NTT add-ons
	If required and defined by Client, application-consistent backups
Service Requests	NTT Infrastructure & Service add-ons and NTT Application add-ons configuration changes . Limited to those NTT Application add-ons required by the application and specified in the SOW

Sensitivity Label: General

Container (Kubernetes) Application	
	Recommendation of minor changes as determined by NTT in its sole and absolute discretion to application manifest definition or NTT Application add-ons configuration
Service Limitations	. Client application repository out of the scope . Management of the SCM or repository hosting the client application is out of scope . Application code development, testing (unitary, integration, performance...) and custom monitoring / observability are out of scope . Full Managed Container (Kubernetes) Application design or definition is out of scope . Managed Container (Kubernetes) Applications cannot be grouped as a single Managed Container (Kubernetes) Application (like Argo CD can do by grouping applications into "application of applications"). Each Managed Container (Kubernetes) Application must implement a self-contained unit of third-party or client-defined functionality. . Anything not expressly identified as above and in scope is expressly out of scope.
Client Responsibilities	. Despite the fact that NTT can offer recommendations based on factors like client requirements and aggregated monitoring metrics, these doesn't constitute a guarantee of future performance and the Client is responsible for the application manifest definition and for adherence to best practices . If the application is Stateful and application-consistent backups are required, Client must state so and provide NTT with clear backup and restore requirements. Otherwise NTT will assume that either persistent data is hosted out of the Kubernetes cluster (for example in PaaS or IaaS instances) or that crash-consist backups of the storage suffice.

(d) Managed Container Images

(i) Managed Service Overview
This element of the service covers the definition and publication of container Images.
Charges are based on the quantity of container images under management.

Container Images	
Service Overview	Container image definition, periodic publication in a managed container registry and vulnerability scanning.
Requirements	. Managed Automation - CI/CD must also be contracted and in scope in the SOW. . Managed Container Registry must also be contracted and in scope in the SOW.
Setup Activities	Creation of container image definition with OS and middleware layers based on Client requirements . Client must provide NTT with clear requirements to define the container image which shall be determined in NTT's sole discretion.. NTT consulting services are out of scope
	Deployment and configuration of automation to periodically recreate the container image, publish it as a new version in a managed container registry and purge oldest versions . Container image publication frequency determined by NTT based on Patch Management process defined in the *Client Service Description* . Client must provide NTT with clear retention and tagging requirements which shall be determined in NTT's sole discretion.
Recurrent Services	Periodic container image recreation, publication in a managed container registry as a new version and purge of oldest versions
	Response to container image vulnerability notifications . If the container registry supports vulnerability scanning and if this is in scope
Service Requests	On demand container image recreation and publication as a new version in a managed container registry
	Minor changes to container image definition as determined by NTT in its sole and absolute
	Change of the container image publication frequency or retention and tagging requirements
	Share a copy of the latest version of the container image definition . While managed by NTT, to be used by the Client's internal teams for development purposes

Sensitivity Label: General

Container Images	
Service Limitations	. Client is responsible for all licenses (including but not limited to OS and middleware), based on Client container image definition requirements . Full rewrite or refactor of a container image definition or upgrade to a newer base OS image version is out of the scope of service requests, it is considered a new setup and must be quoted independently . Despite the fact that NTT can offer recommendations, NTT actions executed as response to container image vulnerability notifications are limited to the ones listed as Service Requests . Container image deployment is out of scope . Anything not expressly identified as above and in scope is expressly out of scope.

(e) Managed Public Cloud-Container as a Service

(i) Managed Service Overview
Public Cloud fully-managed Container-as-a-Service services that are a simpler alternative to Kubernetes services.
Charges are based on number of active Services and standalone Tasks.
Services and Tasks are hosted in ECS clusters.

ECS cluster	
Service Overview	AWS Elastic Container Service (ECS) is a fully-managed container orchestration service that simplifies container deployment and management at scale while integrating with other AWS services.
Requirements	. Managed Container Registry must also be contracted and in scope in the SOW. AWS Elastic Container Registry (ECR) is used by default. . Managed EC2 Autoscaling Group must also be contracted and in scope in the SOW when EC2 is used as a capacity provider.
Setup Activities	. Creation and setup of ECS cluster . Setup of capacity provider
Recurrent Services	N/A
Service Requests	. Update capacity provider configuration
Service Limitations	Amazon ECS Anywhere is out of scope of this service. ECS only provides very basic containers orchestration compared to Kubernetes, such us limited customizable and pluggable components, limited advance traffic routing and service discovery or lack of built-in support for stateful applications. Before committing on an ECS solution, please check Container Solution Guidance document.

ECS Service	
Service Overview	In the context of the Manage ECS service, the Managed Container Application provides the management of an ECS service and the underlying tasks within the managed ECS cluster
Requirements	. Managed ECS, Managed Container Registry and the related Managed Automation - CI/CD services must also be contracted and in scope in the SOW. . Managed Container Images service is recommended to be included as part of the SOW. . Managed AWS ELB Application Load Balancer must also be contracted and in scope in the SOW (when the service requires to be published via ALB).
Setup Activities	. Creation of application service (when required) . Creation of task definition (Client must provide with all the required details for their application to be run) . Setup service autoscaling . Setup ELB application load balancer used by the ECS service. . Setup of service interconnect (when required and only via Amazon ECS Service Connect) . Setup of container logging to CloudWatch Logs only (additional logging endpoints configuration are out of scope of this service)

Sensitivity Label: General

ECS Service	
	. Enable Amazon ECS CloudWatch Container Insights
Recurrent Services	None
Service Requests	. Update task definition (eg. adding new environment variables, adding secrets, changing reserved CPU and memory, etc...) . Update service (eg. changing desired count)
Service Limitations	. Stateful applications requiring application-consistent backups are not supported. Persistent data must be hosted out of the ECS cluster (for example in PaaS or IaaS instances) . Setup of Amazon ECS service discovery and/or AWS App Mesh is out of scope of this service. . Setup of logging endpoints or tools different from AWS CloudWatch Logs. . Setup of collection of trace data is out of scope of this service

1.3 Prerequisites for Public Cloud

All service levels require that managed services are also in Scope in the SOW for the underlying infrastructure supporting the Containers platform.
PaaS solutions (public cloud-native) - *Managed Azure - Core Services, Managed AWS - Core Services* or *Managed GCP - Core Services* must be also be In Scope in the SOW.

1.4 Service Description Specific Terms

By selecting this service as in Scope in the SOW Client and its End User explicitly agreeing to abide by the terms and conditions of Fluent D, Kubernetes and any other open source software selected by NTT in its sole and absolute discretion, which are Open Source Software. all Open Source Software is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In no event shall the NTT be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the Open Source Software or the use or other dealings in the open source software. All AWS, Azure and GCP services are subject to the terms and conditions provided by AWS, Azure and GCP through the method by which the Client obtains AWS, Azure and GCP, and Client Agrees to abide by those terms.

Sensitivity Label: General