Managed Juniper Mist Technology Service Description

Overview of Service

This document provides information relating to the management and monitoring of Juniper Mist devices under the standard MCN offering. The monitoring, configuration, limitations, and available service requests are outlined hereunder. The scope of the Juniper Mist offering includes:

- Juniper Mist Wi-Fi Assurance including
  - Mist enabled AP series Access Points
- Juniper Mist Wired Assurance including
  - Mist enabled Switch series
- Juniper Mist WAN Assurance including
  - Mist enabled SRX Gateways
- Juniper Mist Cloud Controller

Client Responsibilities and Pre-requisites

There are no technology specific pre-requisites required, however, a description of the standard pre-requisites for the offering are documented in the MCN Statement of Work.

Technology Specific Operations

All Juniper Mist physical and virtual devices are managed via the Mist Cloud platform, which acts as a centralized control plane. The Juniper Mist Cloud platform controls all endpoints, providing centralized functions like

- Automated template provisioning and updates
- De-commissioning
- Single screen administration
- Web-scale reporting
- Monitoring and alerting.

Although there are many alerts that can be generated by the Mist Controller, only those described in the respective Monitors sections of this document are sent to NTT's ticketing system to provide pro-active notifications.

Mist Controller Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Alarms	Mist alarms generated	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	600
License	Status of Mist Licenses	✓	N/A	Engineering Teams will notify the client 30 days in advance, if any of the licenses is going to expire	86400
Certificates	Monitor the status of certificates	✓	N/A	Engineering Teams will notify the client 30 days in advance, if any of the certificates is going to expire	86400

Juniper Mist Security Appliances

Juniper Mist SRX gateway devices provide security and routing functionality for the Mist network.

Security Appliance Specific Monitors

The following monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Interfaces	Status of device interfaces (virtual or physical), sent / received packets and bytes	✓	Graphs of the parameter measured over time	Engineering Teams will solve the issue	300
Availability	Device is available	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	60
Device Status and Operational State	Operational status of the device	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
Disk (if any)	Disk usage in %	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	300
HA Status (if any)	Check the status of High Availability	✓	N/A	Engineering Teams will solve the issue	180

Security Appliance Supported Configurations

- Physical devices
- Virtual devices
- HA security appliance configurations - two compatible physical or virtual security appliances in an active / passive configuration, both connected at the same time.

Security Appliance Standard Service Requests

Standard service requests are pre-defined, pre-approved changes relating to a specific technology and are defined in the MCN Statement of Work. A list of standard service requests available for this technology can be found in the MCN Request Catalogue, however, the following needs to be noted:

IDS / IPS

IDS and other advanced security features' correct operation is heavily dependent on the application(s) being protected, which means that the ones applying the intelligence on the security policy must be the Client's relevant contacts. The scope of the managed IDS and advanced security features will be limited to applying changes based on what the Client requests. NTT expects the Client will identify the changes to perform based on the SIEM (or whatever the log management tool the Client uses). On the SIEM, the reason why applications are blocked generating false positives, or not blocked when these should, would be identified by the Client. As part of the ongoing management of an Advanced Security device, it is not included in the review of all the logs for an unidentified error or false positive. This is an activity for the Client to perform. While NTT will make all attempts to reduce the number of false positives, it will not be responsible for authentic users being denied access to the Client application.

SIEM Services

A SIEM independent log management system or SOC threat analyst team is not included as part of the Mist SRX Management Service. This means that the detection of vulnerabilities, threats and similar security activities are limited to the features included in the devices under management and that NTT

will not include additional tooling. As such, the following is not part of the Service unless additionally contracted:

- Log Management Service
- Log Correlation Service
- Threat Correlation, Collaborative Intelligence, Monitoring and Analysis of Logs with SOC analysts to detect and/or investigate alerts

Security Appliance Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Optional Tasks

The following tasks do not form part of the standard Managed Network Service offering, however, these are offered by other NTT Data Service offerings and contracts.

- Security policy definition: this is a consultancy task which must be contracted in addition to the Service
- Analysis of the Clients applications, consultancy, audits and advisory services are not included in the setup fee
- SIEM and SOC services
- Hardware, Software and/or support around it

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Juniper Mist Switches

Juniper Mist switches provide wired switching functionality in Juniper Mist network. This may include either or both Layer two and Layer 3 capabilities of the various switching models.

Switch Specific Monitors

The following switch monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Availability	Device is available	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	60
Interfaces	Status of device interfaces (virtual or physical), sent / received packets and bytes	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300
DNS	Check that the collector is able to resolve the IP address to the applied host.	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	120

Switch Supported Configurations

- Single switch (standalone switch) or a set of standalone switches (managed independently from each other)
- Stacked switch.
- Set of switches in high availability configuration i.e. two or more switches of compatible models in an HA configuration

Switch Standard Service Requests

Standard service requests are pre-defined, pre-approved changes relating to a specific technology and are defined in the MCN Statement of Work. A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Switch Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Juniper Mist Campus Fabric

The Managed Juniper Mist offering includes Mist's Campus Fabric capabilities, however, this will incur additional costs. Mist's Campus Fabric refers to the virtualisation (overlay) capabilities of the technology. Campus Fabric enables the extension of Layer two connectivity over Layer three boundaries. This provides features such as micro segmentation and networkwide Group Based Policies (GBP) by leveraging standards-based features such as EVPN-VXLAN. This provides organisations flexibility, efficiency and simplification of their network across multiple locations.

Campus Fabric Specific Monitors

The following switch monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
BGP Site Summary	BGP Status of device Site Device	✗	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180
BGP Peers	Status of BGP peers	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	180

Campus Fabric Supported Configurations

- EVPN Multihoming (collapsed core replacement).
- Campus Fabric Core-Distribution (EVPN-VXLAN extension across core and distribution). Both ERB and CRB are supported.
- Campus Fabric IP Clos (EVPN-VXLAN extension down to the edge)

Campus Fabric Standard Service Requests

Standard service requests are pre-defined, pre-approved changes relating to a specific technology and are defined in the MCN Statement of Work. A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Campus Fabric Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Juniper Mist Access Points (AP)

Juniper Mist AP Wireless infrastructure provides the cloud-based control plane, as well as wireless Access Points (AP's) that form part of a Juniper Mist network.

Access Point Specific Monitors

The following switch monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Availability	Device is available.	✓	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.	180

Access Point Supported Configurations

Juniper Mist APs will only be managed from the Mist Cloud platform.

Access Point Standard Service Requests

Standard service requests are pre-defined, pre-approved changes relating to a specific technology and are defined in the MCN Statement of Work. A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Access Point Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Juniper Mist Access Assurance

Juniper Mist's Access Assurance service provides secure network access control (NAC) for the wired and wireless network. The solution is Cloud-based and therefore does not require a separate hardware appliance. Mist Access Assurance The solution integrates into IdP solutions such as Okta, Microsoft Entra and Google Workspace.

Access Assurance Specific Monitors

The following Access Assurance monitors are configured by default:

Monitor	Description	Included	Performance Info	Resolution	Poll Interval (sec)
Total NAC Clients	Monitor the total number of NAC Clients in an organisation where clients are the devices connected to the network and authenticated through the Access Assurance feature.	✓	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.	180
Network Interfaces	Collects network interface performance and operational stats	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed	120
Certificates status	Monitoring of certificate expiry	✓	N/A	Engineering Teams will notify the client 30 days in advance, if any of the certificates is going to expire	86400

Access Assurance Supported Configurations

There are no specific supported configurations because the Juniper Mist Access Assurance is a micro-services-based cloud solution provided by Juniper Mist. The solution incorporates a high availability, autoscaling architecture and has the intelligence to direct authentication requests to the nearest Access Assurance instance. The solution is supported through integration with external directory services such as Okta, Google Workspace, Microsoft Azure AD. Consult the Juniper Mist documentation for more information about supported providers.

Access Assurance Standard Service Requests

Standard service requests are pre-defined, pre-approved changes relating to a specific technology and are defined in the MCN Statement of Work. A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Access Assurance Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work.

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.

Configuration Management

Juniper Mist is a fully SaaS offering, therefore device configuration backups are inherent to the solution and are executed automatically with the built-in toolsets to the Juniper Mist Cloud. All Juniper Mist configuration backups are stored in the Juniper Mist Cloud itself as part of Management Orchestration.

The specifics of Mist Cloud Management Portal do not allow execution of the standard and typical backup and restore processes. As this is a cloud-based Service, the configuration is stored in the Mist Cloud. Backup during configuration changes is an automated process by Juniper Mist and NTT is not responsible for taking configuration backups.

For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

Firmware Maintenance

Firmware maintenance for the Juniper Mist solution is an automated process and is included within the technology. Keeping firmware updated allows the utilisation of the latest features and ensures that the latest security enhancements are operating on the device(s). Firmware schedules and frequencies are determined and managed by the Juniper Mist vendor but can be scheduled to take place outside of critical business hours from the Dashboard. For further details in this regard refer to the vendor's relevant documentation.

Juniper Mist Marvis

Marvis is a Virtual Network Assistant AI for Juniper Mist environments and provides visibility and clarity into real time insights. Marvis provides analysis and diagnosis capabilities to the Mist solution thereby offering Clients additional insights into how their network is performing. NTT recommends this functionality is added for all clients.

Limitations

The following limitations apply:

- End user support and end user facing activities, including quarantining, un-quarantining, individual network revocation, OS and PKI related issues are excluded from the Service. It is expected that all End-user support will be provided by the Client. NTT will support the client in troubleshooting these issues where it is suspected that the cause is network related.
- Movement of individual users between segmentation groups within Juniper Access Assurance. It is expected that the client will perform these functions in the IAM source (and not in Juniper Access Assurance).
- Creation of any customised portals or portal workflows.
- Access Assurance is only supported in the AWS Juniper Mist Cloud.
- Any Campus Fabric configuration breaching Juniper Mist validated design principles are not supported.
- Configurations for any third-party infrastructure is excluded.