Managed Log Management Technology Service Description

Overview

This document provides information relating to the management and monitoring of Log Management under the standard MCN offering. The monitoring, configuration, limitations, and available service requests are outlined hereunder.

The Managed Log Management service offering is an add-on offering to the MCN base offering and provides clients the capability to send system logs or event messages to a centralized server hosted in the NTT MSP.

In addition to providing additional information about the device operation (depending on the logging level) it can also be used in problem management (especially for intermittent outages), for troubleshooting faults, and for auditing compliance and review.

The Managed Log Management offering is available to any model and vendor of routers, switches, security appliances, wireless LAN controllers and so forth managed by NTT under the MCN offering provided that the device is capable of supporting Syslog logging and is located on-premises, in the Client's Datacenter or in a co-lo Datacenter (i.e. Cloud hosted /SaaS devices are excluded)

Client Responsibilities and Prerequisites

In addition to the pre-requisites documented in the MCN Statement of Work, the following technology specific pre-requisites are applicable.

- Ensure that the level of logging selected for any device is not in contravention of any policies, laws or standards in terms of the information that is logged e.g. credit card information.

Service Description

When an event is generated by a Syslog enabled device, the event message is forwarded to the NTT MSP Syslog server and stored within a file where the entry is timestamped. These log files are forwarded by an agent and securely stored within the NTT MSP for later perusal, on request.

The level of detail contained in the log file that is generated by the Syslog and the type of events that will trigger the generation of a log file depends on the level of logging configured on the device.

There are several levels of logging that can be enabled on a device. Logging levels of the Management Log Management feature are shown in the table below:

Code/Level	Severity	Description	Condition
0	Emergency	System is unusable	A panic condition.
1	Alert	Action must be taken immediately.	A condition that should be corrected immediately.
2	Critical	Critical conditions	Signifies a critical condition(s) that demands intervention to prevent system failure.
3	Error	Error conditions	Indicates error conditions that impair some operation but are less severe than critical situations.
4	Warning	Warning conditions	signifies potential issues that may lead to errors or unexpected behavior in the future if not addressed.
5	Notice	Normal but significant condition	Conditions that are not error conditions, but that may require special handling.

Code/Level	Severity	Description	Condition
6	Informational	Informational messages	Confirmation that the environment / device is operating as expected.
7	Debug	Debug-level messages	Messages that contain information normally of use only when debugging.

Syslog messages include standard attributes, such as:

- Timestamp
- Hostname
- Severity level
- Source IP

It is assumed that all devices subscribed to the Managed Log Management offer are synchronizing their local clocks with the network via time protocols such as NTP, SNTP or an equivalent protocol. The criteria for selecting the level of logging of a device can be based on one or more of the following:

- device type
- device role / function
- device location

For example, routers and switches could be configured to log events at the Error level (3) while security appliances could be configured to log events at the Notice level (5), or all devices at the edge are configured to log events at the warning level and all devices in the aggregation layer of the network are configured to log at the notice level of logging.

Technology Specific Operations

There are no service specific monitors that are enabled for the Managed Log Management offering; however, all Syslog platforms are monitored in accordance with standard NTT platform practices.

Managed Log Management is not intended as a replacement for the monitoring of devices, as described in the respective technology service description under "Technology Specific Operations", but complements the information collected through the normal monitoring process of devices under NTT management.

It is only available for devices that are managed by NTT as an additional subscription under the MCN contract. It is a separate, billable offering and therefore not included by default in the MCN service offer. It is therefore possible to enable logging for only certain devices and not necessarily all devices.

All logs generated by devices under this offering will be retained for a period of one (1) year on a sliding scale. These logs may be perused by requesting the logs through the logging of a Service Request through the normal request process.

There are several considerations that need to be considered when deciding what level of logging to select for a device (or type of device or location of device):

- The higher the level of logging selected; the more types of events are logged. Therefore, more storage and bandwidth are required to store these events.
- The greater the number of events that are logged, the more data is generated/consumed.
- More data consumption typically requires more bandwidth.
- High storage volumes are required for greater volumes of log files.
- Logging can have an impact on the CPU utilization of a device and should be considered.

It is therefore crucial to ensure that there is sufficient bandwidth available for the selected level of logging (and number of devices) so that the additional data does not affect throughput during daily operation or monitoring and management of the device(s).

When calculating the amount of storage and bandwidth required, several factors must be taken into account:

- The number of devices configured for logging.
- The level of logging configured on each device.
- The expected number of events generated by each device over a specific period.

A typical Syslog message is no greater than 1024 bytes and typically consumes 100 bytes of bandwidth for each message.

This, along with the frequency and expected number of messages that will be generated by each device which has been enabled with the feature, should be taken into account when calculating the amount of bandwidth and storage required.

The amount of bandwidth and storage is calculated during the pre-sales phase and is included in the cost of the service.

The Log Management offering is a consumption-based model meaning that the cost thereof increases as the amount of storage required increases. Clients are responsible to ensure that there is always sufficient bandwidth to ensure reliable transmission of the log data to the NTT MSP and that the transmission of the log data does not negatively impact daily operations and monitoring of the environment or are discarded as a result of insufficient bandwidth.

The Client is responsible for providing the level of logging to be enabled on each device that is subscribed to the Managed Log Management offering. The NTT Log Management solution auto-scales the storage, therefore, should the subscribed Syslog storage be exceeded, the platform will auto-provision additional storage to ensure that any logs received are not discarded, however, this will incur additional costs. NTT will therefore inform the client, through the monitoring of the Syslog storage platform, when storage volumes are being depleted so that the Client can be made aware of any impending increase in storage requirements.

Logging levels of each device can be varied by each device individually, by the type of device, by the function of the device or by the location of the device (or a combination thereof). NTT recommends that devices are configured to log at the error level (4) and where more detailed logging information is required that this only be enabled on specific devices (such as security appliances) or on demand through the logging of a Service Request using the normal request fulfilment processes. For example, to enable higher logging level temporarily on a specific device to troubleshoot an intermittent issue. This can help in reducing the total amount of bandwidth and storage required.

It must also be noted that application-level logging is not supported by under this offer. This ensure that no sensitive information such as personal information, financial information is logged or collected and exposed in any way.

Syslog in itself cannot encrypt or mask the type of information contained in the log messages during transmission therefore the offer is only available for on-premises devices, (this includes devices hosted the Client's data center or co-lo data center).

The Syslog messages will be forwarded from the Client environment to NTT over the site-to-site encrypted connection thereby ensuring that the information contained in the logs is secured and not exposed to any unauthorized parties.

The Log Management solution is UDP based, therefore when connectivity between the device and the Syslog server is disrupted, or the device fails, any logs generated during this time are discarded and will not be retransmitted upon recovery. This is a limitation of the protocol and not a fault in NTTs platform(s).

Whenever a new device or group of devices is included in the service, the available bandwidth and Log storage must be reviewed and where necessary, upgraded to facilitate the additional bandwidth and storage requirements.

Configuration Management

Device configuration backups are not applicable to the offering and are therefore excluded from the standard offering.

Firmware Maintenance

Firmware maintenance is not applicable to the offering and therefore excluded from the standard offering.

Supported Configurations

Is not applicable to the offering.

Limitations

The following limitations apply for devices managed for the Managed Log Management offering:

- Logging of applications is not supported.
- Parsing logs to identify any security events or incidents is excluded from the offering.
- A device must be operational and reachable through the network for the logs to be received and recorded by the logging server.
- Devices sending lo information must be synchronized to the network to ensure accurate time stamps are recorded in the log files.
- Logs are reviewed on an ad-hoc basis for the purposes of troubleshooting and problem management.
- The service is only available for on-prem devices and SaaS (Cloud) based solutions (devices) are excluded.
- Compliance to any legal, territorial or Regional policies such as GDPR are excluded.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual appliances.

Service Requests

A list of service requests available for this technology can be found in the MCN Request Catalogue.

Technology Transition Tasks

In addition to the standard transition tasks described in the MCN Statement of Work, the following technology specific transition tasks are included:

- Configuration of devices to enable logging as agreed by the Client.
- Setup and configuration of logging server
- Testing of logs to logging server

Note:

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