Uptime Services
Onsite Alerting

With over 6,000 clients, our Uptime is a globally trusted IT support and maintenance offering. Uptime is a portfolio of support services designed to assist in maintaining the availability of your technology and offers enhancements through proactive service options to drive down the complexity of your infrastructure and lower your costs in operating your technology.

Our portfolio is designed to give you the flexibility of service levels per asset from each of the four service plans. These plans range from Remote, our entry offering right through to Mission Critical for your most critical systems. All these can be further enhanced with a set of additional Proactive Support Services to help you manage your estate more effectively.

The individual plans are designed for:

- **Remote** – designed primarily for the support of software products for which incidents are handled remotely. Remote support is provided on a 24x7 basis.
- **Parts Only** – for organizations who have sufficient skills to perform an on-site repair when needed, but don't have the scale to stock their own spares or the logistics capabilities to get parts to the right location at the right time. Remote support is provided on a 24x7 basis and when delivery of parts to site is required you're able to select from a set of service target options.
- **Onsite** – for organizations who require a combination onsite labour and/or parts in addition to remote support providing a complete onsite solution for either hardware or software assets. This is suited to organizations who do not have local teams, parts, and/or engineering expertise to perform onsite repairs.
- **Mission Critical** – this plan is for both hardware and software assets in your network that must have minimum downtime and, when down, represent a significant impact on your business operations. This service plan provides an elevated level of support intimacy with fast track access to senior technical resources saving critical time when incidents occur.

The scope of this white paper is to provide you with an overview of the technology and security posture which will enable you to benefit from our Uptime Onsite Alerting service plan.

Table of contents

List of Figures

List of Tables

Our Onsite Alerting services

Whether or not you have your own monitoring system or service in place, including one of our lightweight monitoring capabilities, or other online services; our Uptime Onsite Alerting service greatly improves the mean-time-to-repair and ensures maximum uptime of your assets.

Uptime Onsite Alerting is a lightweight 'phone home' style monitoring feature included in the Onsite service plan and is available for all service plans. Through Uptime alerting, which is a trap-based monitoring, we receive hardware failure alerts from Cisco assets in your IT environment. These alerts, generated through traps, will enable you to locate where your business is impacted and take the necessary actions.

Delivery model

We adopt a global operating model which allows us to leverage our experts centrally from our global delivery centers. This provides you with the quickest possible response through multiple channels to suit your business preferences, and access to our technical expertise together with deployment of local experts to give you the best possible service experience.

With an onsite presence in 147 countries, we can dispatch engineers and/or hardware to your premises within agreed timeframes and are able to track them using advanced field mobility tools.

Your service experience is available to you in real-time via your Manage Centre logon. This will provide you not only access to your Mission Critical service elements, but also give you the ability to track open tickets, log a new request, or talk direct to one of our experts via our integrated chat function and much more.

Compliance to industry standards

Our global delivery centers are industry certified in **ISO:20000, ISO:27001** and **ISO:9000** to adhere to industry best practices on service management, security and quality standards and are subject to annual audits keep them that way.

Global services oriented architecture (GSOA)

GSOA is comprised of the foundational toolsets and platforms we use to support our processes and people in delivering services to your business. It provides a global, multi-tenanted solution that supports our Services – from support to outsourcing – on a common platform, as well as support local delivery requirements with global delivery capability.

The automation platform, which is part of GSOA, will ensure maximum events are handled by a virtual engineer and will ensure only business-impacting events are converted to incidents.

Figure 1 depicts the high-level architecture of our GSOA, which is used for monitoring your infrastructure.

At a high level, GSOA has three components:

- **Remote infrastructure management** (RIM) is the layer where the network management function is carried out. We use EMC Smarts assurance manager for this function which receives the Simple Network Management Protocol (SNMP) traps from your devices.
- **IT service management** (ITSM) is the layer used for managing ITIL processes for all client interactions. ServiceNow is the platform used for this.
- **Enterprise messaging routing** (EMR) is the service integration layer through which the RIM and ITSM communicate with each other.

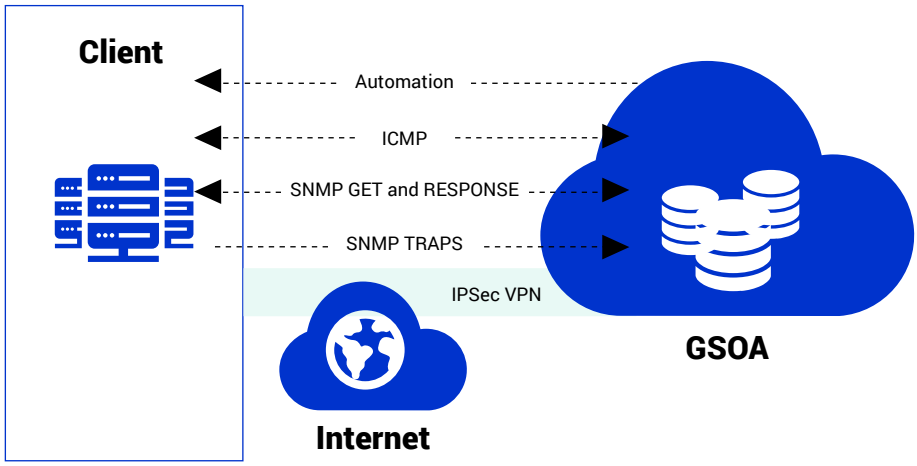

Figure 1: GSOA architecture

Network management protocols

Our Onsite Alerting service is designed to deliver a number of proactive services to your environment. To achieve this we depend on SNMP traps to proactively receive alerts your network.

SNMP agents are required to be activated in order to generate traps and your devices will need to be configured accordingly for the type of events, and traps that will be generated. For security purposes, the SNMP communication between your device and our GSOA need to be authenticated and SNMP community strings are used for this. We need 'read-only' community strings for monitoring. In addition to this, a SNMP trap destination also need to be configured pointing to our GSOA IP address.

This configuration has to be done on individual devices and if requested, we can help you execute this using automated scripts.

Connectivity

Our proactive services will ensure your network is available 24x7 by continuously monitoring your devices via our GSOA platform. IP reachability is required between your network and ours. We have the flexibility to achieve this using one of the three methods in Figure 2.

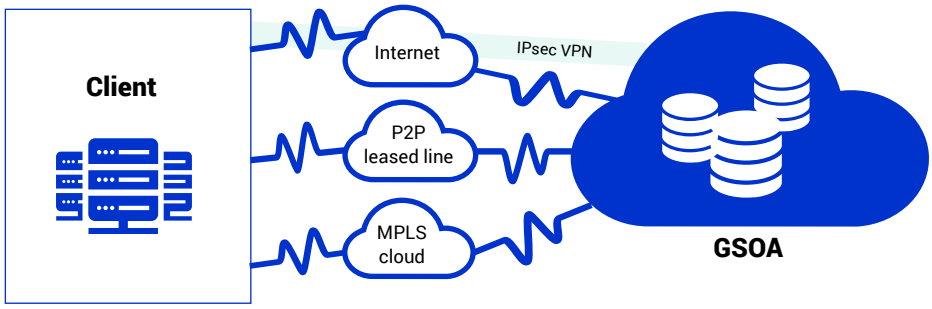

Figure 2: Flexible connectivity

Option one: IPsec virtual private network (VPN) over internet

Our recommended option is to establish a secure encrypted VPN connection over internet based on IPSec which gives advantage over the below three parameters:

Time – It is quick to establish a VPN. According to our experience, the configuration for setting up the VPN generally gets completed in less than two hours.

Flexibility – There is no dependency on the underlying internet media type for this VPN. The only requirement is to have your network able to reach our public IP address and identify as a VPN termination point.

Cost - Existing infrastructure is used for this and there is no need of additional investment in terms of a new physical circuits or terminating device.

The VPN connection is encrypted using the parameters indicated in Table 1 to ensure confidentiality, integrity, and availability (CIA) for all communication between NTT and your network.

Encryption parameters	
Encryption algorithm	3DES
Hash algorithm	SHA1
Diffie Hellman Group	2

Table 1: Encryption parameters

Since the SNMP is a lightweight protocol, the bandwidth requirement through this VPN connection is minimal.

Option two: Point to point leased line

If a VPN connection is not suitable, we can provision a dedicated point to point private leased line between your location and NTT.

Option three: MPLS Cloud

We can also connect to your network by being part of your existing MPLS cloud you have (if any). In this scenario, NTT will be treated as one of the spoke or branch location in your private cloud.

Automation

One of the values that our GSOA platform offers is its automation capabilities. We use automation which will analyse the events generated out of SNMP traps and take action without the need for human intervention. This helps eliminate false events as well as avoiding any potential human error.

For some automation, we will need to login to your device automatically and execute some show commands to validate the event and verify its latest status. To do this, we will require you to open the ports indicated and provide credentials. Please note that all the logins will be available for audits from our platform and can be shared as and when required.

Firewall rules

Necessary firewall rules are required to be created in your infrastructure to ensure smooth communication of the ICMP, SNMP traps/polling and SSH/ Telnet between your network and our GSOA platform, as shown in Table 2 and 3.

Source IP	Destination IP	Protocol	Service	Port	Description
Client network range	NTT LAN IP address range	UDP	SNMP	162	SNMP trap

Table 2: Firewall rules - Outbound for traffic going out through VPN to NTT's GSOA

Source IP	Destination IP	Protocol	Service	Port	Description
NTT LAN IP address range	Client network range	TCP	SSH Telnet	22 23	Running show commands for automation

Table 3: Firewall rules - Inbound for traffic coming in through VPN from NTT's GSOA

Access to client devices

For receiving proactive alerts with regard to your infrastructure, we will not require access to your infrastructure devices. However, in the event of an incident where you require our engineers to remotely troubleshoot, we will require access to your network based on your approval. This can be done in two ways:

Option one: Access through the VPN link

If you are able to provide credentials to your network devices for our engineers in advance, they will be able to remotely login to the devices through the established VPN link using these credentials and start diagnosis immediately.

All logins will be done only on the basis of approval from your side. Based on our extensive experience in managing millions of assets, this method will significantly improve the mean-time-to-repair of your infrastructure and ensure maximum uptime for your business.

For immediate access our engineers will require access to your devices via the VPN connection as per the port indicated in Table 4.

Option two: Access by having a webconference with your team members

If credentials cannot be provided to our engineers, we can also support you by inviting your support team to a Cisco Webex session to start diagnosis. This way access and credentials are controlled by your teams.

Source IP	Destination IP	Protocol	Service	Port	Description
NTT LAN IP address range	Client network range	TCP	SSH Telnet	22 23	Device access

Table 4: Device access - Inbound for traffic coming in through VPN from NTT's GSOA

Data privacy

For proactive monitoring, your specified IT users will have access to our Manage Centre Portal. This will enable visibility of you IT health, active incidents and the ability to raise tickets as well as other benefits.

For devices, we need the IP address, serial number, location, hostname, SNMP details, etc., which will be stored in our configuration management database (CMDB) where we maintain your asset base. The device credentials are also required to perform periodic backup using NCM.

Please note: We do not maintain any personally identifiable information nor monitor any traffic passing through any device.

Data in transit

Proactive monitoring is enabled through continuous polling of your devices using industry standard protocols.

The below traffic will be in transit during the normal operations of our Mission critical service plan:

- ICMP traffic for device availability
- SNMP polling and traps for device availability and performance related data. Only device diagnostics data which contains information related to the health and status of that particular device
- Device configuration files during configuration backup
- SSH and Telnet traffic using device logins either manually or by our automations

Data at rest

All the operational data is stored in ITSM and encrypted at rest. The IT user and device information which is stored in ITSM is protected by edge encryption, meaning that not even ServiceNow has access to the keys to decrypt the data.

The device health and performance data resides in RIM and is prevented using strict authentication mechanisms.

The EMR communication between ITSM and RIM are based on HTTPS.

Manage Centre, which is our client portal, also does not store any information. It acts as the presentation layer for the data residing within ITSM and RIM.

Summary

Our Services are designed to deliver maximum uptime to your organization. This requires our platforms to have basic access to your devices so that we can poll and collect critical system information that will allow our experts to immediately resolve any issues.

Through an encrypted VPN connection, NTT's GSOA platform will be able to poll your devices or receive SNMP traps from them and will be attended to by our remote delivery team in our global delivery centers.

Security is important to us and we have several controls in place to ensure that your data is stored safely and encrypted securely in our systems.

We give utmost importance to the security of your data and infrastructure. Your data will be stored securely with encryption at all levels in our ITSM platform and does not include any personal identifiable information.

To successfully integrate with our GSOA environment, we require you to open necessary firewall ports and configure SNMP in your infrastructure devices. Table 5 summarizes how the measures deployed by NTT can address your security concerns.

Your security concern:	How we address this:
Traffic between NTT and you	Encrypted IPsec VPN between both NTT and you.
SNMP communication between your devices and NTT's GSOA	SNMP community strings for authentication.
Unauthorised traffic between NTT and you	Inbound and outbound firewalls rules configured on both your and NTT's enterprise firewalls.
Data privacy	We store only device diagnostics data. No personally identifiable information is stored.
Data storage	All your data stored in our system are encrypted.
Compliance to standards	ISO:20000, ISO:27001 and ISO:9000 certifications for our global delivery centers.

Table 5: Our approach to addressing common security concerns

Frequently asked questions from clients

Why do you need connectivity for the Onsite Alerting plan?

Onsite Alerting is a proactive plan which depends on SNMP traps being received from your devices. This requires IP reachability, hence the need for connectivity.

Do I need to procure a physical link to connect to NTT?

The only requirement is to have IP reachability between your network and ours. A physical link will also serve the purpose, but an encrypted VPN over your existing internet link will be a cost-effective option and much faster and easier to configure.

Isn't it difficult and complex to setup a VPN?

In our experience, we believe this to be a simple setup on configuration between security devices, as long as they support the security parameters defined. This can take as little as two hours to configure.

Do I need to configure SNMP commands in all my devices?

Yes, every device will be sending SNMP traps, so they need to be configured the same way. We have some automated scripts which can be used to configure a large number of devices in a short amount of time.

How much bandwidth is required for network management traffic through VPN?

SNMP is a light-weight protocol. Bandwidth usage per device will be ~1 kbps.

Since NTT has connectivity to my network, my network is exposed to you. How do we insure against any sort of attacks through this network?

The security of our client's infrastructure is of prime importance to us. We consider it a joint effort to ensure availability of your network.
We ensure only the traffic required for our Services is allowed through the VPN. Similarly, we request that you configure the firewalls in your enterprise to allow only the traffic which we have specified above.

How do your engineers access my devices during any incident diagnosis?

We prefer that you give us credentials to access your devices through the VPN link, since this will reduce the mean-time-to-repair considerably. However, we have alternate methods using Cisco WebEx, etc., where your engineers can give access during the troubleshooting.

You support other clients using the same infrastructure. How do you ensure my data is not accessible to others?

Our global services operating architecture is a multi-tenanted platform which uses domain segregation and role-based access control to ensure the client data is completely segregated and only authorized users can access relevant client data.

Together we do great things