# NTT DATA Service Description

## NTT DATA Managed Cloud Services

### Introduction

NTT DATA is pleased to provide NTT DATA Managed Cloud Services (the "Service(s)") in accordance with this Service Description ("Service Description"). Your quote, order form or other mutually-agreed upon form of invoice or order acknowledgment (as applicable, the "Order Form") will include the name of the service(s) and available service options that you purchased. For additional assistance or to request a copy of your service contract(s), contact NTT DATA technical support or your sales representative.

### The scope of this service

NTT DATA Managed Cloud Services are designed to maximize the value of public and private cloud hosted services through pro-active operational and service management aligned to Information Technology Infrastructure Library (ITIL®) frameworks. This Service Description describes the Service being provided to you ("Customer" or "you").

### Definition of terms

These terms are used within this document.

| | |
|---|---|
| POC | The NTT DATA point of contact for reporting and logging incidents. |
| Priority of Incident | The method that NTT DATA uses to rank and prioritize incidents. The priority determines the order in which incidents should be attended to. |
| Incident Identification Number (IID) | This is a unique incident identification number that is used to track all incidents and service requests reported by the Customer or through automatically generated events or alerts. |
| Incident Owner | The person to whom an IID has been assigned. |
| Portal, Self-Service Portal, NTT DATA Cloud Portal | Multi-tenant software-as–a-service (SaaS) solution that delivers IT operations lifecycle management capabilities that spans public and private cloud infrastructure and application elements. Portal is available at https://dell.vistarait.com/ |

# Table of Contents

## Services

Managed Cloud Services offer four service coverage levels:

- Base Technical Support
- Cloud Monitoring and Alerting (CMA)
- Cloud Monitoring and Remediation (CMR)
- Cloud Operations Management (COM)

This section presents a combined view on the solution features that are included under each different service coverage level. Appendix B includes additional details categorized by solution. This Appendix provides additional descriptions for the Cloud Monitoring and Remediation service coverage level and the Cloud Operations Management service coverage level.

| | Base Technical Support | Cloud Monitoring and Alerting | Cloud Monitoring and Remediation | Cloud Operations Management |
|---|---|---|---|---|
| 1. Cross cloud compatibility | ✓ | ✓ | ✓ | ✓ |
| 2. Service desk (up to 5 named contacts) | ✓ | ✓ | ✓ | ✓ |
| 3. Portal access | ✓ | ✓ | ✓ | |
| 4. Customer Delivery Executive (CDE) | ✓ | ✓ | ✓ | |
| 5. Alert dashboard | ✓ | ✓ | ✓ | |
| 6. Visibility and auditability | | ✓ | ✓ | ✓ |
| 7. Standard monitoring | ✓ | ✓ | ✓ | |
| 8. Advanced monitoring | | ✓ | ✓ | |
| 9. Alert management | | ✓ | ✓ | |
| 10. Preventive maintenance | | ✓ | ✓ | |
| 11. Standard Operating Procedure (SOP) based remediation | | ✓ | ✓ | |
| 12. Troubleshooting with full remediation | | | ✓ | |
| 13. Root cause analysis of critical incidents | | | ✓ | |
| 14. Preventive health checks | | | ✓ | |
| 15. Move, Add and Changes (MAC) and Service Requests (SRs) | | | ✓ | |

## 1. Cross Cloud compatibility

Services are available across multiple cloud platforms:

- Public Clouds: Amazon Web Services, Google Cloud Platform Services, and Microsoft Azure
- Private Clouds: NTT DATA Cloud Dedicated
- On-premise cloud environments for supported technologies as agreed with the Customer

## 2. Service Desk

Customer may assign up to five (5) named contacts to contact the service desk on behalf of the

Customer. The Service Desk is a central point of contact for handling the following Customer issues:

- Incident ownership, initial troubleshooting and escalation of incidents within the defined Service Level Agreement (SLA);
- Respond to “how to” questions such as how to provision remove cloud instances and migrate data across cloud service providers;
- Respond to access issues and requests;

The service desk can be contacted at:-

- Toll-Free number (855-350-4372) with intelligent voice response (IVR) – available 24x7;
- Email at Managed.Cloud.Services@nttdata.com;

## 3. Portal access

It is a multi-tenant Software as a Service (SaaS) solution that delivers IT operations lifecycle management capabilities that spans public and private cloud infrastructure and application elements. NTT DATA Cloud Portal is available at https://dell.vistarait.com/.

## 4. Customer Delivery Executive (CDE)

The CDE will serve as the single point of accountability in delivering the Service, providing the following support:-

- Establish and manage relationship with identified Customer contacts;
- Work with the operations team proactively to identify opportunities and continually improve Customer experience with respect to the services under this Service Description;
- Define key measures and periodically review them with Customer
- Pro-actively explain any high severity incidents, root causes, and resolution efforts;
- Coordinate with service providers, as agreed, to help ensure a unified NTT DATA solution;
- Develop and review cloud plans with Customer including forecast and growth projections;

## 5. Alert dashboard

Allows Customer to view and manage alerts, create incident and problem tickets, and setup automated alert escalations.

## 6. Visibility and auditability

NTT DATA offers complete visibility of tickets and related metrics, including SLAs for response time, resolution time, and ticket post history. NTT DATA also offers monitoring and related statistics, including availability statistics and performance statistics.

Preconfigured views related to tickets and availability is part of the dashboard view of the Portal. In addition, the Portal presents additional customized views to this data based on various search/selection criteria.

All remote activities performed by NTT DATA engineers are recorded and available for the Customer to replay upon request.

The table below shows sample set of pre-generated, on-demand and scheduled set of reports:

| Report Category | Report Description | Pre-generated Report | On-demand Report | Scheduled Report |
|---|---|---|---|---|
| Audit reports | Console audit recordings | ✓ | | |
| | Login history report | | ✓ | |
| Device inventory reports | Device details report | | ✓ | |
| | Disk space report | ✓ | | |
| | Hardware report | | ✓ | |
| | Software report | | ✓ | |
| | Storage report | ✓ | ✓ | ✓ |
| | Virtualization report | ✓ | | ✓ |
| Network reports | Interface errors and discards | | ✓ | |
| | Interface utilization and traffic | | ✓ | |
| | IP SLA report | ✓ | ✓ | ✓ |
| | Network backup summary report | ✓ | ✓ | ✓ |
| | Network devices inventory report | | ✓ | |
| | Network executive report | ✓ | | |
| | Network Statistics report | ✓ | | ✓ |
| | VOIP QoS report | ✓ | ✓ | ✓ |
| | WLAN controller report | ✓ | | ✓ |
| | AD Health check report | | ✓ | |
| | Anti-Virus compliance report | | ✓ | |

| | | | | |
|---|---|---|---|---|
| Preventive maintenance reports | Anti-Virus status report | ✓ | | |
| | Disk defragment report | | ✓ | |
| | EXBPA report | | ✓ | |
| | Symantec backup report | | ✓ | |
| Service reports (per client) | Application audit report | | ✓ | |
| | Customer executive report | ✓ | ✓ | ✓ |
| | Device details summary report | ✓ | | ✓ |
| | End point security report | ✓ | | |
| | Ticket notification and resolution times report | ✓ | ✓ | ✓ |
| | URL monitoring report | ✓ | ✓ | ✓ |

## 7. Standard monitoring

Perform the below standard monitoring services for the agreed set of devices:

- Performance monitoring: Operating System (OS) and application metrics (limited metrics)
- Availability monitoring: instances, infrastructure, and cloud provider (ping and heartbeat)
- Track cloud Inventory: view cloud instances and private infrastructure

## 8. Advanced monitoring

Perform the below advanced monitoring services for the agreed set of devices at the agreed level of monitoring

- Network
- Storage
- Service topology monitoring

## 9. Alert management

Perform the below alert management services for the agreed set of devices:

- Alert correlation
- Validation
- Ticket creation
- Escalation

## 10. Preventive maintenance

Preventive maintenance is different by solution and comprises activities as defined in Appendix B. Most common activities for OS and applications include patch management and validation of anti-virus (AV) definition updates for supported AV products. For hardware, firmware upgrades are typically covered.

### 10.1 Validate Anti-Virus (AV) definition updates for supported AV Products (customer provided)

This activity comprises checking the antivirus definitions on the server and updating the definitions on a scheduled basis.

- Depending on the automation schedule (by default), antivirus/antimalware definitions will be updated on a daily basis
- Any issues (e.g. corruption or license expiry) that are observed with the antivirus/antimalware application or definition update will be alerted to the Customer
- If the antivirus/antimalware update event failed during the scheduled time, NTT DATA will validate and run the definition updates. If the machines have failed two (2) consecutive scheduled events or the definition versions are older than two (2) days, NTT DATA will remedy the issues within the defined SLA
- All antivirus definition update issues are categorized as Low (Sev 4) priority incidents as defined in Appendix A
- If the antivirus/antimalware update event caused system related issues, NTT DATA will be engaged within the defined SLA

**Supported Anti-Virus products:**
ThreatTrack VIPRE, McAfee, and Symantec

### 10.2 Patch management per customer approval

Patch management scope is defined in corresponding section of Appendix B. NTT DATA will scan the servers for missing patches according to the schedule defined in Appendix B and patch scan results will be uploaded to the Portal.

- If installation of the patch fails, NTT DATA will take corrective action and the failed patches will be reinstalled during the next scheduled patch maintenance schedule approved by the Customer
- Patches on the servers have to be approved by the Customer from the Portal
- NTT DATA will perform server reboot

**Note:**

- It is the responsibility of the Customer to ensure that the server carries a genuine license where applicable
- It is important to note that a device will be rebooted following any patch that requires rebooting. Therefore, patching time windows and approvals must anticipate the possibility of a device reboot
- **Patch Testing for Microsoft Windows OS**: Default patch management includes security and critical patches as defined by Microsoft. Security and critical patches are tested by NTT DATA using

the known IT standard practices and patches rated as “Whitelist” or “Blacklist”. Security and critical patches released by the vendor are installed in a limited test environment (with standard applications and tools) and tested for installation issues, standard application compatibility, and malfunction. NTT DATA will also review patch testing forums/email groups to better understand other known issues. NTT DATA testing procedures are performed with a best effort in a limited testing environment. **NTT DATA accepts no liability for any crashes or malfunction of devices or applications post installation of patches**

## 11. Standard Operating Procedure (SOP) based remediation

NTT DATA pre-defined and Customer customized SOP will be executed as soon as an alert is triggered.

- Incoming alerts will be initially validated in order to identify false alerts or alerts where no action is required
- Actionable alerts will be ticketed by the appropriate personnel and any SOPs will be executed as first-level of support
- If the SOPs fail to resolve the problem, the ticket will then be updated and immediately escalated to a designated partner contact as well as to the proper technician(s) for further troubleshooting and remediation

Appendix B includes additional details by solution.

## 12. Troubleshooting with full remediation

NTT DATA will remotely troubleshoot and fix issues for alerts:

- If the SOPs fail to resolve the problem, the ticket will then be updated and immediately escalated to the appropriate domain expert within NTT DATA in order to troubleshoot and remediate the issues comprehensively
- NTT DATA will contact software and hardware vendor tech support for further troubleshooting and full remediation. **Customers must have valid vendors’ maintenance/technical agreement where applicable. Service scope is limited if maintenance / technical support agreement is expired or if software / hardware is placed into ‘End of Life’.** SLAs are as per technical support contract with vendor. It is required that Customer authorize NTT DATA to act on their behalf when coordinating with the vendor’s support organization
- Incidents raised are responded to within the predefined SLA as defined in Appendix A
- All activities are logged into an ITIL based ticketing system and updated with complete chronology and steps it took to remediate the incident

## 13. Root cause analysis of Critical incidents

Root cause analysis of Critical (Sev 1) incidents (as defined in Appendix A) to identify underlying problem.

## 14. Preventive health checks

Preventive health checks are different by application and typically cover scanning of the application to check for possible issues. Appendix B includes additional details by solution.

## 15. Move, Add and Changes (MAC) and Service Requests (SR)

Simple MACs and SRs are supported. MAC procedures are different by solution and typically cover user creation and edits, password changes, etc. SRs are procedures that are not due to disruption of service (i.e. requests which are not due to any incidents identified in the infrastructure, monitored event or change requests due to root cause analysis).

SRs and MACs are limited to thirty (30) minutes in length and five (5) hours per calendar month maximum, per covered instance. SRs and MACs are assigned Low (Sev 4) Priority and provided with SLAs as defined in Appendix A.

Appendix B provides examples of SRs and MACs supported for each solution.

## Service delivery

NTT DATA Managed Cloud Services offer the following two operations management types based on ITIL best practices:

a. Self-managed: In the Cloud Monitoring and Alerting service coverage level, the Customer self manages all tasks related to incident and problem management. The Customer uses the self-service Portal to log and self-manage all incidents. In this service coverage level, ITIL best practices are delivered through cloud Service Desk Level 1 support.

b. NTT DATA managed: In the Cloud Monitoring and Remediation service coverage level, as well as in the Cloud Operations Management service coverage level, NTT DATA team members execute the following ITIL-based service operations processes: event management, incident management, problem management and change management.

   Event management includes:
   - Alert integration and aggregation
   - Alert validation
   - Alert/event correlation
   - Alert review and analysis
   - Event acknowledgement and initiation of incident management

   Incident management includes:
   - Incident handling
     - Incident classification
     - Incident prioritization
     - Incident notification
     - Incident escalation
   - Service request management including preventative maintenance (scheduled / unscheduled)

- Change management
- High criticality incident management
- Incident analysis & system root cause analysis

Problem management is comprised of advanced level analysis and problem remediation and includes the following tasks:

- Perform alert and incident analysis to reduce unnecessary noise in the environment
- Perform root-cause analysis to prevent repetitive incident occurrences
- Document analysis results for quick remediation in the future
- Develop SOPs for new incidents
- Provide insights to service delivery management team on best practice recommendations

Change management for the configuration changes include:

- Version upgrade, patch deployment, new installations, configuration changes
- Change Review Board (CRB) approves all the normal changes
- Emergency Review Committee (ERC) approves all the emergency changes
- Ticketing system used for tracking all the changes
- Domain lead approves break fix changes

## Exclusions

For the avoidance of doubt, the following activities are not included in the scope of this Service Description:

- Any services, tasks or activities other than those specifically noted in this Service Description.
- The development of any intellectual property created solely and specifically for the Customer.
- If Customer chooses to use its own element managers or management platforms, and integrate with the Portal, all limitations of those platforms will carry over and NTT DATA does not take any responsibility or liability for any problems, issues or breaches directly or indirectly resulting from those platforms.
- If Customer has non-standard architectures, does not follow industry best practices, or has insufficient capacity on their devices, NTT DATA service commitments will be restricted to response SLA only.
- If Customer has non-standard environments, unsupported by the technology principals, NTT DATA will not provide resolution SLA.
- If Customer does not implement NTT DATA recommendations for reducing alert and incident noise, service level commitments on those devices will not apply.
- Service level commitments will not apply to environments that are not current on recommended patch and firmware versions.
- Service level commitments do not apply to those devices that are out of currency on patch levels because of application requirements.
- NTT DATA will not be responsible for defects or malfunctions in third party software encountered during the process of troubleshooting, resolving, patching, upgrading or performing any other related service.

This Service Description does not confer on Customer any warranties which are in addition to the warranties provided under the terms of your master services agreement or Agreement, as applicable.

THESE SERVICES ARE NOT PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) COMPLIANT. CUSTOMER IS RESPONSIBILE FOR KEEPING PCI DSS DATA AND VIRTUAL MACHINES WITH PCI DSS DATA OUT OF THE ENVIRONMENT BEING MANAGED BY THIS SERVICE. As required by law or regulation, the Services are subject to the Business Associate Agreement set forth in Appendix C.

## Offer Specific Customer Responsibilities

Customer will support onboarding activities set forth herein for the Service. Onboarding activities include:

- Customer Requirements gathering
- Validation of configuration data and system integrations as applicable
- Review initial alert threshold values
- Provide escalation and notification contacts
- Customer will provide timely access to Customer resources, including but not limited to, virtualization administrators and engineering and project management. NTT DATA and the Customer will agree on standard access protocols.
- Customer is responsible for all design and implementation of network security settings and requirements definitions.
- Customer is responsible for all application development and management and performance monitoring and all database development and management.
- Customer is responsible for managing its virtual environment. Customer is responsible for any changes/modifications/deletions to Customer's virtual environment.

## General Customer Responsibilities

Authority to Grant Access. Customer represents and warrants that it has obtained permission for both Customer and NTT DATA to access and use, whether remotely or in-person, Customer-owned or licensed software, hardware, systems, the data located thereon and all hardware and software components included therein, for the purpose of providing these Services. If Customer does not already have that permission, it is Customer's responsibility to obtain it, at Customer's expense, before Customer asks NTT DATA to perform these Services.

Customer Cooperation. Customer understands that without prompt and adequate cooperation, NTT DATA will not be able to perform the Service or, if performed, the Service may be materially altered or delayed. Accordingly, Customer will promptly and reasonably provide NTT DATA with all cooperation necessary for NTT DATA to perform the Service. If Customer does not provide reasonably adequate cooperation in accordance with the foregoing, NTT DATA will not be responsible for any failure to perform the Service and Customer will not be entitled to a refund.

Data Backup. Customer will complete a backup of all existing data, software and programs on all affected systems prior to and during the delivery of this Service. Customer should make regular backup copies of

the data stored on all affected systems as a precaution against possible failures, alterations, or loss of data. NTT DATA WILL HAVE NO LIABILITY FOR:

- ANY OF YOUR CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION;
- LOST OR CORRUPTED DATA, PROGRAMS OR SOFTWARE;
- DAMAGED OR LOST REMOVABLE MEDIA;
- THE LOSS OF USE OF A SYSTEM OR NETWORK; AND/OR
- FOR ANY ACTS OR OMISSIONS, INCLUDING NEGLIGENCE, BY NTT DATA OR A THIRD-PARTY SERVICE PROVIDER.

NTT DATA will not be responsible for the restoration or reinstallation of any programs or data.

Third Party Warranties. These Services may require NTT DATA to access hardware or software that is not manufactured by NTT DATA. Some manufacturers' warranties may become void if NTT DATA or anyone else other than the manufacturer works on the hardware or software. Customer will ensure that NTT DATA's performance of Services will not affect such warranties or, if it does, that the effect will be acceptable to Customer. NTT DATA does not take responsibility for third party warranties or for any effect that the Services may have on those warranties.

## NTT DATA Services Terms & Conditions

This Service Description is entered between you, the customer ("you" or "Customer"), and the NTT DATA entity identified on your invoice for the purchase of this Service. This Service is provided subject to and governed by Customer's separate signed master services agreement with NTT DATA that explicitly authorizes the sale of this Service. In the absence of such agreement, depending on Customer's location, this Service is provided subject to and governed by NTT DATA's Cloud Solutions Agreement (as applicable, the "Agreement").

Please see the table below which lists the URL applicable to your Customer location where your Agreement can be located. The parties acknowledge having read and agree to be bound by such online terms.

| Customer Location | Terms & Conditions Applicable to Your Purchase of NTT DATA Services | |
|---|---|---|
| | Customers Purchasing NTT DATA Services Directly From NTT DATA | Customers Purchasing NTT DATA Services Through an Authorized NTT DATA Reseller |
| United States | www.nttdataservices.com/en-us/contracts | www.nttdataservices.com/en-us/contracts |
| Canada | Available on request | Available on request |
| Latin America & Caribbean Countries | Mexico: Your terms and conditions of sale will be sent to you along with your quote | Not applicable |
| Asia-Pacific-Japan | Available on request | Service Descriptions and other NTT DATA service documents which you may receive from your seller shall not constitute an agreement between you and NTT DATA but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other NTT DATA service document shall in this context be understood as a reference to you whereas any reference to NTT DATA shall only be understood as a reference to NTT DATA as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with NTT DATA with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller. |
| Europe, Middle East, & Africa | Available on request | Service Descriptions and other NTT DATA service documents which you may receive from your seller shall not constitute an agreement between you and NTT DATA but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other NTT DATA service document shall in this context be understood as a reference to you whereas any reference to NTT DATA shall only be understood as a reference to NTT DATA as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with NTT DATA with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller. |

Customer further agrees that by renewing, modifying, extending or continuing to utilize the Service beyond the initial term, the Service will be subject to the then-current Service Description available for review at www.nttdataservices.com/en-us/contracts.

To the extent that any terms of this Service Description conflict with any terms of the Agreement, the terms of this Service Description will prevail, but only to the extent of the specific conflict, and will not be read or deemed to replace any other terms in the Agreement which are not specifically contradicted by this Service Description.

By placing your order for the Services, receiving delivery of the Services, utilizing the Services or associated software or by clicking/checking the "I Agree" button or box or similar on the nttdataservices.com website in connection with your purchase or within a NTT DATA software or Internet interface, you agree to be bound by this Service Description and the agreements incorporated by reference herein. If you are entering this Service Description on behalf of a company or other legal entity, you represent that you have authority to bind such entity to this Service Description, in which case "you" or "Customer" shall refer to such entity. In addition to receiving this Service Description, Customers in certain countries may also be required to execute a signed Order Form.

## Supplemental Terms & Conditions Applicable to Cloud & SaaS Services

1. Term of Service. This Service Description commences on the date listed on your Order Form and continues through the term ("**Term**") indicated on the Order Form. As applicable, the number of systems, licenses, installations, deployments, managed end points or end-users for which Customer has purchased any one or more Services, the rate or price, and the applicable Term for each Service is indicated on Customer's Order Form. Unless otherwise agreed in writing between NTT DATA and Customer, purchases of Services under this Service Description must be solely for Customer's own internal use and not for resale or service bureau purposes.

2. Important Additional Information

   A. Payment for Hardware Purchased With Services. Unless otherwise agreed to in writing, payment for hardware shall in no case be contingent upon performance or delivery of cloud or SaaS services purchased with such hardware.
   B. Optional Services. Optional services (including point-of–need support, installation, consulting, managed, professional, support, security or training services) may be available for purchase from NTT DATA and will vary by Customer location. Optional services may require a separate agreement with NTT DATA. In the absence of such agreement, optional services are provided pursuant to this Service Description.
   C. Assignment. NTT DATA may assign this Service and/or Service Description to qualified third party service providers.
   D. Geographic Limitations and Relocation. This Service is not available at all locations. Service options, including service levels, technical support hours, and on-site response times will vary by geography and certain options may not be available for purchase in Customer's location, so please contact your sales representative for these details.

## Appendix A

### Service Level Agreements (SLA)

NTT DATA will follow SLA based service delivery model. For the avoidance of doubt, the parties hereby expressly acknowledge and agree that NTT DATA will use reasonable efforts to meet the response SLAs and resolution SLAs specified below in this Appendix A. It shall not be a breach of contract, nor shall NTT DATA be liable or responsible for breach of contract or for payment of any type of service credits to the Customer for not meeting any SLA or SLAs at any time during the term of the Service purchased by the Customer.

The Customer should inform NTT DATA of any device addition/deletion, or changes to environment that might impact the SLA. The following table describes the various priority levels associated with incidents. The sources of alerts are either from the monitoring system or from user requests entered via the ticketing system, phone calls or e-mails.

- Resolution SLAs do not apply for those cases that are escalated to vendor tech support / hardware vendor / Internet Service Provider (ISP) / third party vendors
- Resolution SLA is calculated from the time the ticket is assigned to the troubleshooting team (L2/L3/CoE)
- Resolution SLA timer is paused during the following ticket statuses: (a) “Waiting for SP or Client” (b) “On-Hold” (c) “Under Observation” (d) “Resolved”
- Individual Customer environments and processes influence service level compliances. In cases where the above SLAs cannot be met, NTT DATA will publish those details during the pretransition / planning phases
- SLAs will be effective after ninety (90) days of steady state operations or as published during pre-transition phases Priority

| Priority | Response SLA (Business Hours) | Resolution SLA* | Measured |
|---|---|---|---|
| P0: Critical (Sev 1) | 15 Min | 95% of the cases resolved in 4 hours | Monthly |
| P1: High (Sev 2) | 30 Min | 95% of the cases resolved in 8 hours | Monthly |
| P2: Medium (Sev 3) | 8 Hours | 95% of the cases resolved in 72 hours | Monthly |
| P3: Low (Sev 4) | 36 Hours | 95% of the cases resolved in 240 hours | Monthly |

* Resolution SLA applies only to solutions managed by NTT DATA.

The ‘Severity Levels’ section below describes the various levels of incidence severity in detail.

### Priority based escalations

| Priority | Phone | Ticket |
|---|---|---|
| P0: Critical (Sev 1) | ✓ | ✓ |
| P1: High (Sev 2) | | ✓ |
| P2: Medium (Sev 3) | | ✓ |
| P3: Low (Sev 4) | | ✓ |

## Severity levels

| **Priority Level 0 (P0) – Critical Incidents – Severity Level 1** |
|---|
| **Description**: This is an EMERGENCY condition that significantly restricts the use of the cloud platform itself to perform any critical business functions. This could mean that several departments of the Customer are impacted.<br><br>The ticket could have originated from multiple sources: an end-user or NTT DATA staff.<br><br>**Target for response**: Follow-up within fifteen (15) minutes of receiving notification. A voicemail is left with the appropriate Customer personnel if a representative is not available immediately. A status update will be provided within two (2) hours of the initial call.<br><br>**Target for resolution**: The target resolution time for is PO incident is four (4) hours. In some cases the solution may require a temporary workaround until the ultimate solution can be investigated and implemented. In these cases, the ticket will be closed after a workaround is implemented. A new ticket will be opened with a lower priority to evaluate alternative solutions. Target resolution time can depend on external parameters including coordination with outside vendors. In the event of an external vendor who does not respond in time, the Customer will be notified.<br><br>Inability to use any critical cloud instance(s) by the Customer will require immediate attention by NTT DATA.<br><br>**Status update**: A NTT DATA support team member will provide regular status updates throughout the day until a resolution or workaround can be found.<br><br>**Response procedure**: After a Critical Incident is reported to the POC:<br>• The POC will report the issue immediately to all key Customers. The POC logs the incident and assigns it to the appropriate owner.<br>• The POC will communicate regular status updates to the appropriate Customer personnel.<br>• If it is appropriate, the CDE will call an emergency coordination meeting with all the Incident Owners to discuss an action plan for resolution including possible recovery efforts.<br>• The result of this meeting will be reported to the appropriate personnel on the Customer IT team and NTT DATA account team. An update will also be provided to key Customer personnel by the close of business. The CDE or POC will provide each of these updates.<br><br>There will be a post-incident meeting to discuss the Priority 0 incident in detail. In addition, for Customers who have Cloud Operations Management level of service, the incident will be put through the problem management process.<br><br>**Escalation procedure**:<br>• Escalation will occur if the incident has not been resolved by the agreed upon due date or status updates do not occur by the Incident Owner. The user should contact the POC in these instances to get the latest status of the incident.<br>• The POC will obtain status updates from the Incident Owner and involve the appropriate Customer personnel and/or NTT DATA if satisfactory results are not achieved. |
| **Examples of Critical Incidents:**<br>• Several users or groups have incidents<br>• Mission-critical server is down<br>• Cloud instances are down<br>• Key application is down |

| **Priority Level 1 (P1) – High Priority Incidents – Severity Level 2** |
|---|
| **Description**: A major function or critical application or infrastructure device is severely impacted and there are no quick workarounds available. It is deemed high because of its business or financial impact. The ticket could have originated from multiple sources: an end-user or Customer IT or NTT DATA staff reporting a high priority incident, or an automatic notification from a monitor on server, network, or application. Substantially degraded performance of any critical system is also categorized as a Priority 1. The only difference between a P0 and P1 incident is how widespread the incident is. A P0 may impact the entire department or company whereas a P1 may impact just one (1) user. A P0 may impact an entire system or business process where, as a result, the business process reverts back to a manual or back-up process. There is no difference in the amount of resources that will be devoted to a P1 incident compared to a P0 incident.<br><br>**Target for response**: Follow-up within thirty (30) minutes of receiving notification. Voicemail is left with the appropriate Customer personnel if a representative is not available immediately. A status update will be provided by the close of business or sooner if one is available.<br><br>**Target for resolution**: Within eight (8) hours, but it is possible that the solution may require a temporary workaround instead of the final solution. In these cases, the ticket will be closed after workaround is implemented. A new ticket will be opened with a lower priority to evaluate all possible options. Target resolution time can depend on external parameters including co-ordination with outside vendors.<br><br>**Status update**: Will be provided by Incident Owners to the user by close of business and then on a daily basis.<br><br>Failure to respond or report status in a timely manner will result in escalation.<br><br>**Response procedure**: After a High Priority Incident is reported to the POC:<br>• The POC will report the incident to the appropriate managers and send an email to NTT DATA delivery manager. The POC logs the incident and assigns it to an Incident Owner. The Incident Owner will investigate the incident immediately.<br>• The Incident Owner that is responsible for the incident will then be responsible for communicating daily status to the POC until the incident is resolved or priority is downgraded based on findings of the initial investigation.<br>• It will be the responsibility of the Incident Owners to obtain status updates pertaining to the incident by the close of business each day and relay them to the user or reporter of the incident.<br>• These updates will continue until resolution of the incident or an acceptable workaround is found. The Incident Owner will close the incident when it is resolved.<br><br>**Escalation procedure**:<br>• Escalation will occur if the incident has not been resolved by the agreed upon due date or status updates do not occur by the Incident Owner. The user should contact the POC in these instances to get the latest status of the incident.<br>• The POC will obtain status from the Incident Owner and involve the appropriate Customer personnel and/or NTT DATA if satisfactory results are not achieved. |
| **Examples of High Priority incidents:**<br>• External user is not able to login or see network<br>• Non-mission critical server is down<br>• Non-core network element is down |

| **Priority Level 2 (P2) – Medium Priority Incidents – Severity Level 3** |
|---|
| **Description**: The reported incident may restrict the use of one or more features of the system, but the business or financial impact is not severe. The ticket could have originated from multiple sources: an end-user or Customer IT or NTT DATA staff reporting a medium priority incident, or an automatic notification from a monitor on server, network, or application. The reported incident may be of a critical nature, but sometimes the incident can be downgraded to a Priority 2 because a viable workaround is available as a temporary solution. Many incidents are categorized as a P2 because there is a business justification or a financial impact on completing the task within five (5) business days. Sometimes a critical enhancement to existing functionality can be categorized as a P2 based on the critical nature of its due date and severe impact on business.<br><br>**Target for response**: Within eight (8) hours<br><br>**Target for resolution**: Seventy two (72) hours (three (3) Business Days)<br><br>**Status update**: Will be provided to the user upon incident resolution. Failure to respond or report status on a timely manner will result in escalation.<br><br>**Response procedure**: After a Medium Priority Incident is reported to the POC:<br>• The POC will create the ticket for the incident and assign it to an Incident Owner.<br>• The Incident Owner that is responsible for the incident will then be responsible for managing the ticket and communicating status to users including approximate resolution date.<br>• It will be the responsibility of the Incident Owner to provide a status update pertaining to the major incident within seventy two (72) hours from the time the incident is originally reported.<br>• These updates by the Incident Owner will continue as agreed upon by the user or reporter of the ticket until resolution or an acceptable workaround is found. The Incident Owner will close the incident when there is confirmation of resolution.<br><br>**Escalation procedure**:<br>• Escalation will occur if the incident has not been resolved by the agreed upon due date or status updates do not occur as agreed by the Incident Owner. The user should contact the POC in these instances to get the latest status of the incident.<br>• The POC will obtain status from the Incident Owner responsible and involve the appropriate Customer and/or NTT DATA if satisfactory results are not achieved. |
| **Examples of Medium Priority Incidents:**<br>• Termination requests<br>• Customer can log in, but cannot access application<br>• An outside salesperson has a network incident, and/or VPN related incident<br>• Any request or incident that has a direct impact on Customer's daily operations |

| **Priority Level 3 (P3) – Low Incidents – Severity Level 4** |
|---|
| **Description**: The reported anomaly in the system does not substantially restrict the use of one or more features of the product to perform necessary business functions. The ticket could have originated from multiple sources: an end-user or Customer IT or NTT DATA staff reporting a minor incident, or an automatic notification from a monitor on server, network, or application that is deemed minor. This is a minor problem and will not significantly impact operations.<br><br>**Target for response**: Within thirty six (36) hours<br><br>**Target for resolution**: Agreed upon due date with the user or appropriate personnel (otherwise treated as ten (10) business days).<br><br>**Status update**: Will be provided to the user by the Incident Owner upon resolution of the incident.<br><br>**Response procedure**: After a Low Priority Incident is reported to the POC:<br>• The POC will create the ticket for the incident and assign it to an Incident Owner.<br>• The Incident Owner that is assigned will then be responsible for managing the ticket and communicating status to the user including the approximate resolution date.<br>• These updates by the Incident Owner will continue as agreed upon by the user or reporter of the ticket until resolution or an acceptable workaround is found. The Incident Owner will close the incident when there is confirmation of resolution.<br><br>**Escalation procedure**:<br>• Escalation will occur if the incident has not been resolved by the agreed upon due date or status updates do not occur as promised by the Incident Owner. The user should contact the POC in these instances to get the latest status of the incident.<br>• The POC will obtain status updates from the responsible Incident Owner and involve the appropriate Customer personnel and/or NTT DATA if satisfactory results are not achieved. |
| **Examples of Minor Incidents:**<br>• Low impact changes in IT processes that are of a non-critical nature<br>• Any server software or hardware incident for which a workaround exists |

## Appendix B

### Scope

Appendix B should be used when Cloud Monitoring and Remediation service coverage level or Cloud Operations Management service coverage level is purchased. Below is the list that outlines sections included in this Appendix.

| SKU Description | Operating System / Application | Corresponding section |
|---|---|---|
| **Backup Application Server** | Non-cloud Backup | Section 1 |
| **Add on Backup Agent** | | |
| **Operating System Only** | Windows Server | Section 2 |
| | Linux server | Section 3 |
| | Solaris OS | Section 4 |
| **Database (Types 1, 2)** | Microsoft SQL Database | Section 5 |
| | MySQL database | Section 6 |
| **Database (Type 3)** | Oracle databases | Section 7 |
| **Webservers** | Webservers | Section 8 |
| **Microsoft Exchange** | Microsoft Exchange Server | Section 9 |
| **Microsoft SharePoint** | Microsoft SharePoint | Section 10 |
| **Microsoft Active Directory** | Microsoft Active Directory | Section 11 |
| **Blackberry** | Blackberry | Section 12 |
| **Virtual Host Server / Hypervisor** | Server virtualization services | Section 13 |
| **Citrix Presentation Server [*500 users]** | Application virtualization services | |
| **Storage (Types 1, 2)** | Storage | Section 14 |
| **Network Devices (Types 1, 2, 3)** | Network Infrastructure | Section 15 |
| **Datacenter & Converged Infrastructure Practice – VCE vBlock, NetApp FlexPod, and EMC VSPEX** | Datacenter & Converged Infrastructure Practice - VCE vBlock, NetApp FlexPod, and EMC VSPEX | Section 16 |
| **VCAC Core Bundle [1* Identity Server + 1* vCloud Automation Center appliance + 1* IaaS + Plus support for up to 15 blueprints]** | vCAC Services | Section 17 |
| **VCAC ADD-ON [Choose any one: 1* Identity Server , 1* vCloud Automation Center appliance, or 1* IaaS]** | | |
| **VCO Core Bundle [1*VCO Server + 15 workflows]** | | |
| **VCO Workflows – 20 [Management only]** | | |
| **VCAC Blueprints – 20** | | |

| | | |
|---|---|---|
| **Openstack Hypervisor** | Openstack Services | Section 18 |
| **Openstack Controller** | | |
| **Hardware Blade (Type 1)** | Server Hardware | Section 19 |
| **Hardware Tower / Rack (Type 1)** | | |
| **Dell Hybrid Cloud System for Microsoft, Small 4 nodes (2x2) storage** | Dell Hybrid Cloud System for Microsoft | Section 20 |
| **Dell Hybrid Cloud System for Microsoft, Medium 8 nodes (2x3) storage** | | |
| **Dell Hybrid Cloud System for Microsoft, small 16 nodes (2x4) storage** | | |

Appendix B includes additional details categorized by solution and generally consists of the following sections:

- Supported environments / technologies
- Key monitoring parameters
- Standard Operating Procedures
- Move, Add and Changes and Service Requests
- Preventive maintenance scope
- Preventive maintenance schedules
- Preventive health checks
- Out-of-scope items

## Section 1: Non-Cloud Backup

**Supported environments**

| | |
|---|---|
| **Backup applications (Customer provided)** | Symantec NetBackup, Windows NT Backup, CA ARCserve, Veeam Backup |
| **Supported product versions** | Three (3) recent product versions of the supported backup application products |
| **Backup types supported** | Tape level backups, disk level backups, image backups, virtualized backups (snapshots, VMware vDR, VCB, vRanger) |

**Key monitoring parameters**

| |
|---|
| **Backup application server and agents availability**: up/down |
| **Backup application services**: up/down |
| **Backup hardware monitoring**: Tape Drives, Tapes, Hard Drives Status |
| **Backup job logs**: Validate Backup Job Status (Success/Failures) |
| **Backup job failures**: Validate Backup Schedules And Jobs; Notify Job Failures |
| **Backup job queue**: Validate And Monitor Queue |

**Standard Operating Procedures**

List of SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Backup application server status (up/down)** | NTT DATA will run diagnostics to check the status of the problematic backup application server from other server in the same network to eliminate any local area network (LAN)/wide area network (WAN) connectivity issues |
| **Backup application server shutdown (unexpected) Alerts** | NTT DATA will validate the event logs to identify if the sever shutdown is unexpected |
| **Backup application server in hung state** | NTT DATA will restart the server if it is hung ( through DRAC / ILO) |
| **Disk space management** | NTT DATA will validate the alert by logging into the server and identifying the folders which are occupying high disk space, remove old backup copies (basing on the retention policies) to free-up disk space. Providing estimates on the capacity and disk management to help ensure backups are running properly within the retention policies configured. |
| **Backup job monitoring** | NTT DATA will validate the backup jobs for job failures and restart the backup jobs if sufficient time is available to complete the job Off-site data transfer failures NTT DATA will run SOPs to check the off-site data transfer log and re-initiate transfer or increase bandwidth for faster transfer |
| **Waiting for media** | NTT DATA will run SOP to change the media from the catalog so backup can continue |

| | |
|---|---|
| **Hardware error** | NTT DATA will run hardware diagnostic check to validate the hardware fault Windows event log (critical) NTT DATA will execute set of instructions when specific critical event occurs |
| **VMware based backups/ using vDR, 3rd party backups** | NTT DATA will check disk space for backup jobs, verifying VMDK status and space for effective backups. Snapshot management and ensuring NFS mounts de-dup checks. |
| **Windows server status (up/down)** | NTT DATA runs diagnostics to check the status of the problematic Windows server from other servers in the same network in order to eliminate any LAN/WAN connectivity issues. |
| **Server shutdown (unexpected) alerts** | NTT DATA validates the event logs to identify if the sever shutdown is unexpected. |
| **Server in hung state** | NTT DATA restarts the server if it is hung (through DRAC / ILO). |
| **Memory utilization alert** | NTT DATA validates the high utilization, and identifies the process causing high memory utilization. |
| **Processor utilization alert** | NTT DATA validates the high utilization, and identifies the process causing high processor utilization. |
| **Disk space alert** | NTT DATA validates the alert by logging into server and identifying folders that occupy high disk space, runs disk clean-up to free-up disk space and notifies Customer of folders that occupy high disk space. |
| **Hardware error** | NTT DATA runs hardware diagnostic check to validate the hardware fault. |
| **Windows event log (critical)** | NTT DATA executes specific set of instructions when specific critical event occurs. |

**Move, Add and Changes and Service Requests**

Not Applicable

**Preventive maintenance scope**

- Backup Application Patch Updates

**Preventive maintenance schedules**

NTT DATA will install any required updates and service packs upon request or on an as needed basis to resolve any product issues with the backup application.

- If installation of the patch fails, a corrective action will be taken by NTT DATA and the failed patches will be reinstalled after resolving the issue
- NTT DATA can schedule patch installation on servers per Customers request

**Preventive health checks**

Not Applicable

**Custom on-demand services**

Custom on-demand services are available as an option. These will be executed on a time and material (T&M) basis. Contact NTT DATA for more details. Examples of custom on-demand services include:

- Data migration of data or servers from primary location to DR location
- On-demand restore request – test the backups and help ensure correct recovery plans are setup for restoring data or application. Recovery plan helps to identify issues with backup sets and applications. Test recoveries are performed to help ensure RPO (Recovery Point Objective), RTO (Recovery Time Objective), and SLAs are met for critical data restores
- VMware based restores for entire VMs from backup set
- Installation and configuration of new master servers, and advanced backup components
- Backup storage or SAN management, de-duplication of backup data sets, and new replicated targets for DR backups.

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Cloud Operations Management and Cloud Monitoring and Remediation packages, on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are out of scope – any request for customizations to monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- Any alert that arrives which has no associated SOPs is out of scope – such alerts will be escalated to the escalation contacts provided by Customer

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fixing problems
- Vendor management or escalation
- Root cause analysis

Out-of-scope Service Requests

- New backup server deployment, provisioning, new configurations and migrations
- New backup architect, design, or re-design of backup management
- Backup software agent or server installation or upgrades
- VMware vDR installation and configuration
- Replication configuration for disk-to-disk backups
- Restore of image backups across various hardware cross platforms
- Backup and restore on advanced applications (e.g. Oracle, MS SQL, MS Exchange, etc.,)

Any items not explicitly covered within this document are considered out of scope.

## Section 2: Windows Operating System

**Supported environments**

| | | |
|---|---|---|
| **Operating Systems** | Microsoft Windows | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above |

**Key monitoring parameters**

NTT DATA monitors the Windows server infrastructure utilizing standard Windows Management Instrumentation (WMI) data collection. The NTT DATA platform also enables NTT DATA to secure remote access to the monitored devices in order to perform SOPs or advanced troubleshooting services.

| |
|---|
| **Device availability:** up/down |
| **Device health:** CPU, memory and disk utilization |
| **Windows services:** up/down (Default: All services with start-up type “Automatic”) |
| **Windows event logs:** Critical application and system logs |
| **Server hardware monitoring:** Disk, memory modules, and chassis temperature |

**Standard Operating Procedures**

List of Windows Server SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Windows server status (up/down)** | NTT DATA runs diagnostics to check the status of the problematic Windows server from other servers in the same network in order to eliminate any LAN/WAN connectivity issues. |
| **Server shutdown (unexpected) alerts** | NTT DATA validates the event logs to identify if the sever shutdown is unexpected. |
| **Server in hung state** | NTT DATA restarts the server if it is hung (through DRAC / ILO). |
| **Memory utilization alert** | NTT DATA validates the high utilization, and identifies the process causing high memory utilization. |
| **Processor utilization alert** | NTT DATA validates the high utilization, and identifies the process causing high processor utilization. |
| **Disk space alert** | NTT DATA validates the alert by logging into server and identifying folders that occupy high disk space, runs disk clean-up to free-up disk space and notifies Customer of folders that occupy high disk space. |
| **Hardware error** | NTT DATA runs hardware diagnostic check to validate the hardware fault. |
| **Windows event log (critical)** | NTT DATA executes specific set of instructions when specific critical event occurs. |

**Move, Add and Changes and Service Requests**

Following are some examples of SRs:

- Disk clean-ups
- Disk defragmentation

**Preventive maintenance scope**

- Windows Patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

Not Applicable

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Cloud Operations Management and Cloud Monitoring and Remediation packages, on a T&M basis.

Out-of-scope monitoring:

- Customizations to the monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- Any alert with no SOPs will be escalated to the Customer's escalation contacts

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management/escalation and Root Cause Analysis are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- Obtaining and maintaining a genuine Windows license is the responsibility of the Customer

Out-of-scope Anti-Virus definition updates

- Reinstallation of AV software
- License management is the responsibility of the Customer
- Virus scan and removal on desktops and servers

Out-of-scope Service Requests

- New server deployment, provisioning, configurations and migrations
- New site architect/design/re-design/ migrations of Windows Servers, data to the remote office or branch office

- Server infrastructure changes
- Application installs on OS

Any items not explicitly covered within this document are considered out of scope.

## Section 3: Linux Operating System

**Supported environments**

| | | |
|---|---|---|
| **Operating Systems** | Linux | Centos, Redhat, Ubuntu Linux |

**Key monitoring parameters**

NTT DATA monitors the Linux server infrastructure utilizing standard Simple Network Management Protocol (SNMP) data collection. The NTT DATA platform also enables NTT DATA staff secure remote access to the monitored devices in order to perform standard operating procedures or advanced troubleshooting services.

| |
|---|
| **Device availability:** up/down |
| **Device health:** CPU, memory and disk utilization |
| **Linux interfaces:** up/down |
| **Logs:** Critical logs |
| **Server hardware monitoring:** Disk, memory modules, and chassis temperature |

**Standard Operating Procedures**

List of Linux Server SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Linux server availability (up/down)** | NTT DATA runs diagnostics to check the status of the problematic Linux server from other servers in the same network in order to eliminate any LAN/WAN connectivity issues. |
| **Network status unknown** | Using this SOP, NTT DATA engineer check the bonding status of NIC cards and also any other parameter that was directly affected. |
| **Server in hung state** | NTT DATA restarts the server if it is hung (through DRAC / ILO). |
| **Memory utilization alert** | NTT DATA validates the high utilization, and identifies the process causing high memory utilization. |
| **Processor utilization alert** | NTT DATA validates the high utilization, and identifies the process causing high processor utilization. |
| **Disk space alert** | Using the SOP, NTT DATA will validate the alert by logging into server and identifying folders that are occupy high disk space, clean-up to free-up disk space and notify Customer of folders occupying high disk space. |
| **Hardware error** | NTT DATA runs hardware diagnostic check to validate the hardware fault. |
| **Linux event log (critical)** | Executes set of instructions when specific critical event occurs. |

**Move, Add and Changes and Service Requests**

Following are some examples of SRs:

- Disk clean-ups

**Preventive maintenance scope**

- Linux Patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Patch scan | Monthly |
| Patch management (install) | Monthly |

**Preventive health checks**

Not Applicable

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Cloud Operations Management and Cloud Monitoring and Remediation packages, on a T&M basis.

Out-of-scope monitoring:

- Customizations to the monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- Any alert with no SOPs will be escalated to the Customer's escalation contacts

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management/escalation and Root Cause Analysis on Linus servers are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- It is the responsibility of the Customer to ensure that all servers carry the appropriate license

Out-of-scope Service Requests

- New server deployment, provisioning, configurations and migrations
- New site architect/design/re-design/ migrations of Windows Servers, data to the remote office or branch office
- Application installs on OS

Any items not explicitly covered within this document are considered out of scope.

## Section 4: Solaris Operating System

**Supported environments**

| | | |
|---|---|---|
| **Operating Systems** | Solaris | Versions 5.10, 5.11, and above |

**Key monitoring parameters**

NTT DATA monitors the Customer's infrastructure using standard SNMP data collection. The NTT DATA platform also enables the NTT DATA staff to remotely and securely access the monitored devices in order to perform SOPs or advanced troubleshooting.

| SOLARIS OPERATING SYSTEM |
|---|
| **Device availability:** up/down |
| **Device health:** CPU, memory and disk utilization |
| **Solaris interfaces:** up/down |
| **Logs:** Critical logs |
| **Server hardware monitoring:** Disk, memory modules, and chassis temperature |

**Standard Operating Procedures**

SOPs executed by NTT DATA for issues with Solaris OS

| | |
|---|---|
| **Solaris server availability (up/down)** | NTT DATA runs diagnostics to check status of problematic Solaris server from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **Network status unknown** | NTT DATA checks bonding status of NIC cards and other parameters that were affected |
| **Server in hung state** | NTT DATA restarts the server if it is hung (through DRAC / ILO). |
| **Memory utilization alert** | NTT DATA will validate high utilization, and identify process causing high memory utilization |
| **Processor utilization alert** | NTT DATA will validate high utilization, and identify process causing high processor utilization |
| **Disk space alert** | NTT DATA will validate alert by (a) login into server (b) identify folders that occupy high disk space (c) run disk clean-up to free up disk space and (d) notify Customer of folders that occupy high disk space |
| **Hardware error** | NTT DATA will run hardware diagnostic check to validate hardware fault. |
| **Solaris event log (critical)** | NTT DATA will execute a specific set of instructions when specific critical event occurs |

**Move, Add and Changes and Service Requests**

Following are some examples of SRs:

Cleanup disk

**Preventive maintenance scope**

- None

**Preventive maintenance schedules**

- None

**Preventive health checks**

- None

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Cloud Operations Management and Cloud Monitoring and Remediation packages, on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine license is responsibility of Customer

Out-of-scope Service Requests

- New server deployment, provisioning , configurations, and migrations
- Architect, design, re-design, and/or migrate Solaris servers and/or data to a new site, remote office, or branch office
- Server infrastructure changes

Any items not explicitly covered within this document are considered out of scope.

## Section 5: Microsoft SQL Databases

The service includes Non-Cloud Backup for corresponding service level – Monitoring and Remediation or Operations Management. For details on Non-Cloud Backup service scope, please review Appendix B Section 1.

**Supported environments**

| | | |
|---|---|---|
| **Operating Systems** | Windows | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above |
| **Database** | Microsoft SQL | MSSQL Express/Standard/Enterprise 2005, 2008 and 2008 R2 and above |

**Key monitoring parameters**

NTT DATA monitors the Microsoft SQL server infrastructure utilizing standard WMI data collection. The NTT DATA platform also enables NTT DATA staff to securely and remotely access the monitored devices to perform standard operating procedures or troubleshooting.

| WINDOWS OPERATING SYSTEM |
|---|
| **Server availability**: up/down<br>**Server health**: (CPU, memory and disk utilization)<br>**Windows event logs**: Critical application, system logs<br>**Server hardware monitoring**: disk, memory modules, chassis temperature |
| **DEVICE HEALTH** |
| Device/network/cluster availability |
| Device health (CPU and memory and disk utilization) |
| **SERVER THROUGHPUT METRICS** |
| Number of logical connections, logins/sec, logouts /sec, active transactions. transactions /sec, queued jobs , failed jobs and job success rate, open connections count |
| **SQL SERVER CACHE METRICS** |
| Cache hit ratio (MSSQL), cache objects, cache pages, and cache objects in use. |
| **SERVER DISK METRICS** |
| Average disk reads/writes/transfers in bytes, disk queue length, disk read/write queue, data space of db, |
| **SQL SERVER LOG METRICS** |
| Log file(s) size, log flush wait time, log flush waits/sec, log flushes/sec, log growth and shrink rate |

| SERVER MEMORY METRICS |
|---|
| Connection memory size, granted workspace memory, lock memory size/ blocks allocated, owner blocks allocated, maximum workspace memory, memory grants outstanding, optimizer memory alert, SQL cache memory size, total server memory size |
| **SQL SERVER LOCK METRICS** |
| Lock wait time (ms), lock requests/sec, lock timeouts/sec, deadlocks/sec |
| **SQL SERVER RESOURCE UTILIZATION METRICS** |
| Data file size , replication transaction rate , average and total latch wait time, number of replication pending transactions, user connections |
| **WINDOWS SERVICES MONITORING** |
| SQL server , agent service , integrations services, reporting services analysis services, full text services |
| **SQL SERVER PHYSICAL I/O PERFORMANCE** |
| Advanced Windows Extensions AWE lookup maps/sec, AWE stolen maps/sec, buffer cache hit ratio, checkpoint pages/sec, lazy writes/sec, page lookups, reads and writes/sec |
| **SQL SERVER HIGH AVAILABILITY MONITORING** |
| Monitors to track replication latency , mirror synchronization , lag in log shipping , cluster availability and failover/fail back |

**Standard Operating Procedures**

List of Microsoft SQL Server SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Windows server status (up/down)** | NTT DATA runs diagnostics to check the status of the problematic Microsoft SQL server from a different server in the same network to eliminate any LAN/WAN connectivity issues |
| **Server shutdown (unexpected) alerts** | NTT DATA will validate event logs to determine if server shutdown is unexpected |
| **Server in hung state** | Restart server if it is hung (through DRAC / ILO) |
| **Memory utilization alert** | Validate high utilization, and identify process causing high memory utilization |
| **Processor utilization alert** | Validate high utilization, and identify process causing high processor utilization |
| **Disk space alert** | Validate alert by logging into server and identify folders that occupy high disk space. Run disk clean-up to free-up disk space and notify Customer of folders that occupy high disk space. |
| **Hardware error** | Run hardware diagnostic check to validate hardware fault. |
| **Windows event log (critical)** | Execute set of instructions when specific critical event occurs |
| **Database log file Is 100% full** | Verify possible reason for log file full and run SOP to backup and shrink log file, or increase space, or move file to a different drive if required |
| **Database is in suspect mode** | Verify SQL log to identify possible reason for DB suspect mode and run SOP as first level resolution |
| **Temp DB is full** | Validate cause of Temp DB full and run SOP by shrinking or increasing temp DB, or moving Temp DB to a different drive based on situation |
| **Database blockings** | Validate blocking process on DB and notify Customer with details. Kill blocked process with confirmation if required. |
| **SQL services not running** | Validate services which are not running and start them as required (standard SQL services only) |
| **Unable to connect to SSMS** | Verify whether a valid login and password was used. Fix login issues. |
| **Enable/disable SQL server agent job** | Verify and identify job that needs to be Enable/Disable by connecting to management studio |
| **Job failure alert** | Validate job failure alert by viewing history and restarting jobs if required |
| **Mirroring suspended** | Run SOP to check server health and service status of secondary server |
| **Log Shipping failed** | Troubleshoot possible reasons for log shipping failure. If primary has problems, then manually perform failover to secondary. If secondary has problems, then run SOP to fix them and configure log shipping again. |
| **Replication Lag** | Run SOP to determine if there are any network issues or other possible reasons |
| **Cluster failover alerts** | Find out reasons for failover and fix them. Keep secondary server ready for future use. |

**Move, Add and Changes and Service Requests**

Following are some examples of SRs:

- Create or delete SQL server agent job

- Create a database with defined specifications and schema
- Enable or disable a SQL agent job
- Change schedule for SQL job
- Change location of data file or log from one drive to a different drive
- Add a secondary data file or log file
- Change location of an error log
- Run a default trace on a SQL server
- Perform an emergency SQL server shutdown and restart procedure
- Rebuild full-text catalogs
- Stop or start SQL full-text services
- Change SQL authentication modes

**Preventive maintenance scope**

- Windows patch management
- MS SQL patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

NTT DATA will run scheduled health checks on Microsoft SQL servers and their instances to scan for possible issues. If critical issues are identified, it will escalate to Customer and propose a possible solution. On receiving an approval from Customer NTT DATA will attempt to resolve the issue.

- **Log watch**
  As part of alert processing, NTT DATA database team will watch SQL logs and event logs for potential security or hardware issues. If any database related issues are found, it will escalate to Customer as appropriate.

- **SQL server audit**
  Analyze logins to SQL database and check for unauthorized logins

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Operations Management and Monitoring and Remediation packages, on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine Windows license is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- New database server deployment, provisioning, configurations, and migrations
- Backup restoration
- Server performance analysis and tuning, database optimization, and performance analysis
- Configure and document clustering; testing and verify fail-over
- Manually perform hot backups and cold backups
- Capacity and maintenance planning; disk storage optimization
- Configure and document mirroring/replication; verify data at remote site; replicate data back to primary site
- Configure and document cluster configurations
- Migrate or consolidate SQL server databases
- Clone databases
- Troubleshoot queries

Any items not explicitly covered within this document are considered out of scope.

## Section 6: MySQL database

The service includes Non-Cloud Backup for corresponding service level – Cloud Monitoring and Remediation or Cloud Operations Management. For details on Non-Cloud Backup service scope, please review Appendix B Section 1.

**Supported environments**

| | | |
|---|---|---|
| **Operating Systems** | Linux | Fedora , Centos, Debian, RedHat, SuSE, Ubuntu Linux |
| **Database** | MySQL | 3.23.x, 4.x, 5.x and above |

**Key monitoring parameters**

NTT DATA monitors the MySQL server infrastructure utilizing SNMP data collections and other monitors. The NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform SOPs or advanced trouble-shooting services.

**Key monitors supported for MySQL**

| |
|---|
| **DEVICE HEALTH** |
| Device availability |
| Device health (CPU and memory and disk utilization) |
| Network availability |
| **CONNECTION STATISTICS** |
| Average connection establishment time |
| Connection time out duration |
| Rate of open connections |
| Rate of connection abortion |
| Aborted clients |
| Maximum number of connections used |
| **KEY(INDEX) EFFICIENCY STATISTICS** |
| Key hit rate |
| Key buffer used |
| Key buffer size |
| Key reads |
| Number of waits for buffer pool |
| **THREAD USAGE STATISTICS** |
| Threads used per request |
| Threads in cache |
| Thread cache size |
| Threads connected |
| **REPLICATION STATISTICS** |
| Replication status |
| Status of slave IO process |
| Status of slave MySQL process |
| Master host, port and user details |
| **PROCESS MONITORING** |
| mysqld process |
| **CLUSTER AVAILABILITY MONITORING** |
| Availability – heartbeat of slave |

| |
|---|
| **REQUEST STATISTICS** |
| Request rate |
| Bytes received rate |
| Bytes sent rate |
| **REQUEST STATISTICS** |
| Queries inserted per min |
| Queries deleted per min |
| Queries updated per min |
| Queries selected per min |
| Number of full join queries executed |
| Number of slow queries |
| **TABLE STATISTICS** |
| Immediate locks acquired for a table |
| Number of lock waits on a table |
| Number of first row reads of the table index |
| Number of open tables |
| Number of temporary tables on disk |
| **QUERY CACHE HIT RATE** |
| Query cache hit rate |
| Query cache size |
| Query cache limit |
| Key reads |
| **IO PERFORMANCE STATISTICS** |
| Delayed writes per min |
| Delayed errors per min |
| Flush commands per min |
| Number of rows inserted/updated/deleted per min |
| Key reads/writes per min |
| **LOG MONITORING** |
| Error logs |
| General query log |
| Binary log |
| Relay and slow query log |

**Standard Operating Procedures**

List of Microsoft SQL Server SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Linux server availability (up/down)** | NTT DATA will run diagnostics to check status of problematic Linux server from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **Network status unknown** | NTT DATA will check bonding status of NIC cards and others parameter that were affected |
| **Server in hung state** | NTT DATA will restart server if it is hung ( through DRAC / ILO) |
| **Memory utilization alert** | NTT DATA will validate high utilization, and identify process causing high memory utilization |
| **Processor utilization alert** | NTT DATA will validate high utilization, and identify process causing high processor utilization |
| **Disk space alert** | NTT DATA will validate alert by (a) login into server (b) identify folders that occupy high disk space (c) run disk clean-up to free up disk space (d) notify Customer of folders that occupy high disk space |
| **Hardware error** | NTT DATA will run hardware diagnostic check to validate hardware fault |
| **Linux event log (critical)** | NTT DATA will execute a specific set of instructions when a specific critical event occurs |
| **Abnormal Increase In MySQL history length** | NTT DATA will validate and decrease history length |
| **MySQL process stopped** | NTT DATA will troubleshoot cause of service stoppage and restart service |

**Move, Add and Changes and Service Requests**

Following are examples of Service Requests for MySQL databases:

- Create or delete MySQL server agent job
- Create a database with defined specifications and schema
- Enable or disable a MySQL agent job
- Change schedule for MySQL job
- Change location of data file or log from one drive to a different drive
- Add a secondary data file or log file
- Change location of an error log
- Run a default trace on a MySQL server
- Perform an emergency MySQL server shutdown and restart procedure
- Rebuild full-text catalogs
- Stop or start MySQL full-text services
- Change MySQL authentication modes

**Preventive maintenance scope**

- Linux patch management
- MS SQL patch management

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

NTT DATA will run scheduled health checks on MySQL servers and their instances to scan for possible issues. If critical issues are identified, NTT DATA will escalate issue to Customer and propose a solution if one exists. Based on approval from Customer, NTT DATA will attempt to resolve the issue.

- **Log watch**
  As part of alert processing, NTT DATA database team will watch MySQL logs and event logs for potential security or hardware issues. If any database related issues are found, it will escalate to Customer as appropriate.

- **MySQL server audit**
  Analyze logins to MySQL database and check for unauthorized logins

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation for MySQL services. These activities can be delivered on a T&M basis, in conjunction with enterprise services Cloud Operations Management and Cloud Monitoring and Remediation service levels.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine OS license is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer

- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- New database server deployment, provisioning, configurations, and migrations
- Backup restoration
- Server performance analysis and tuning, database optimization, and performance analysis
- Configure and document clustering; testing and verify fail-over
- Manually perform hot backups and cold backups
- Capacity and maintenance planning; disk storage optimization
- Configure and document mirroring/replication; verify data at remote site; replicate data back to primary site
- Configure and document cluster configurations
- Migrate or consolidate MySQL server databases
- Clone databases
- Troubleshoot queries
- Any associated development activity

Any items not explicitly covered within this document are considered out of scope.

## Section 7: Oracle databases

The service includes Non-Cloud Backup for corresponding service level – Monitoring and Remediation or Operations Management. For details on Non-Cloud Backup service scope, please review Appendix B Section 1.

**Supported environments**

| | | |
|---|---|---|
| **Operating Systems** | Windows & Unix | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above Unix variant such as Solaris, Linux, AIX, HP-UX |
| **Database** | Oracle database | Oracle 8i, Oracle 9i, Oracle 10g, Oracle 11g ( Real Application Clusters(RAC) , Data Guard, Grid control and Automatic Storage Management (ASM)) |

**Key monitoring parameters**

NTT DATA monitors the Oracle database server infrastructure utilizing standard WMI data (for Windows), SNMP data collection, SNMP trap receivers, and/or syslog monitoring technologies for data collection. The NTT DATA platform also enables NTT DATA staff to securely and remotely access the monitored devices to perform SOPs or troubleshoot.

| WINDOWS OPERATING SYSTEM |
|---|
| **Server availability**: up/down<br>**Server health**: (CPU, memory and disk utilization)<br>**Windows event logs**: Critical application, system logs<br>**Server hardware monitoring**: disk, memory modules, chassis temperature |
| **System global area SGA metrics** |
| Buffer cache and shared pool size, redo log buffer size, data dictionary cache and library cache size, sql area and fixed area size, buffer hit ratio, data dictionary hit ratio, library hit ratio, free memory |
| **Table space metrics** |
| Table space status, allocated bytes and blocks, free bytes and blocks, reads/writes to/from the table space, single read operation, single write operation |
| **Rollback / undo metrics** |
| Rollback segment name and table space name, status and size, hit ratio, HWMSize - High Water Mark of rollback segment size, rollback segment shrinks, wraps and extends, undo table space name, undo rentision, undo advisor and segment advisor report |

| |
|---|
| **Service monitoring** |
| Oracle instance, listener, agent, scheduler |
| **Connection metrics** |
| Connection establishment time, number of users, number of processes, number of sessions. |
| **Session metrics** |
| Session status/CPU usage, memory sorts performed, table scans, physical reads, logical reads, commits, buffer cache hit ratio |
| **Data files performance metrics** |
| Data file status, bytes created, reads from the data file, writes from the data file, read time, write time |
| **Buffer and disk metrics** |
| Buffer Gets, executions on the object, buffer gets per execution, number of disk reads, disk reads per executions |
| **Cluster monitoring** |
| Availability , checking health of cluster ware |
| **Log File monitoring** |
| alert.log and listener.log |

### Standard Operating Procedures

List of Oracle database Server SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Database server status (up/down)** | NTT DATA will run diagnostics to check status of problematic Oracle database from a different server in same network to eliminate any LAN/WAN connectivity issues. |
| **Server shutdown (unexpected) alerts** | NTT DATA will validate event logs to identify if server shutdown is unexpected. |
| **Server in hung state** | NTT DATA will restart server if it is hung (e.g. through DRAC / ILO for Windows) |
| **Memory utilization alert** | NTT DATA will validate high utilization, and identify process causing high memory utilization. |
| **Processor utilization alert** | NTT DATA will validate high utilization, and identify process causing high processor utilization. |
| **Disk space alert** | NTT DATA will validate alert by (a) login into server and (b) identify folders that occupy high disk space, (c) run disk cleanup to free up disk space (d) notify Customer of folders that occupy high disk space. |
| **Hardware error** | NTT DATA will run hardware diagnostic checks to validate hardware fault. |
| **Event log (critical events)** | NTT DATA will execute set of instructions when specific critical event occurs. |
| **Database table space exceeds threshold** | NTT DATA DBA will check available disk space and run SOPs to add space to affected table space. |
| **Database blockings** | NTT DATA will validate blocking process on database and notify Customer with details, as well as kill blocked process with confirmation (if required). |
| **Database status** | NTT DATA will validate services that are not running and start them as required (Standard Oracle Services). |
| **Unable to connect to database** | NTT DATA will (a) verify whether a valid login and password are used (b) fix login issues and (c) help ensure proper connectivity alias is defined to connect from client to server. |
| **Database out of sync** | NTT DATA will troubleshoot possible reasons for failure (if primary has problems) and manually perform database sync to secondary. The secondary will run SOPs to fix them and configure Data Guard again. |
| **Cluster failover alerts** | NTT DATA will find possible reasons for failover and fix them, while keeping secondary server ready for future use. |

### Move, Add and Changes and Service Requests

Following are some examples of SRs for Oracle databases:

- Do tasks that drive high availability of database (e.g. clustering, Data Guard )
- Change schedule for Oracle database job
- Database file location change from one drive to another drive
- Add a secondary data file or log file

- Change location of an error log
- Add new table space and data file
- Run default trace on Oracle database server
- Emergency Oracle database server shutdown and restart procedures
- Rebuild full-text catalogs
- Start or stop Oracle database instance or services
- Change Oracle database authentication modes
- Rebuild unstructured indices

**Preventive maintenance scope**

- Windows Patch management
- [For Windows OS only] Validate Anti-Virus definition updates for supported AV products (customer provided)
- Unix Patch management
- Oracle Patch management

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

NTT DATA will run scheduled health checks on Oracle database servers and their instances to scan for possible issues. If critical issues are identified, it will escalate to Customer, and propose a possible solution. On receiving an approval from Customer, NTT DATA will attempt to resolve the issue.

- **Log watch**
  As part of alert processing, NTT DATA database team will watch Oracle logs and event logs for potential security or hardware issues. If any database related issues are found, it will be escalated to Customer as appropriate.

- **SQL server audit**
  Analyze logins to Oracle database and check for unauthorized logins

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Monitoring and Remediation and Cloud Operations Management for Oracle database services. These activities can be delivered on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine OS license for server (Windows, Linux, Unix, Oracle, etc.,) is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- New database server deployment, provisioning, configurations, and migrations
- Backup restoration; import and export data using data pump (impdb, expdp)
- Server performance analysis and fine tuning, database optimization, and performance analysis
- Configure and document clustering; test and verify fail-over
- Manually perform hot backups and cold backups
- Capacity and maintenance planning; disk storage optimization
- Configure and document mirroring/replication; verify data at remote site; replicate data back to primary site
- Configure and document cluster configurations
- Migrate or consolidate Oracle database servers
- Clone databases
- Troubleshoot queries

Any items not explicitly covered within this document are considered out of scope.

## Section 8: Webservers

**Supported environments**

**For Linux – based webservers**

| | | |
|---|---|---|
| **Operating Systems** | Linux | Fedora , Centos, Debian, RedHat, SuSE, Ubuntu Linux |
| Webservers | | Apache, Tomcat, Weblogic, JBoss, J2EE |

**For IIS Servers**

| | | |
|---|---|---|
| **Operating Systems** | Windows | Windows 2003 server and above SBS server (OS only) 2003 and above |
| **Server** | IIS Server | IIS 6.0 and above |

**Key monitoring parameters**

NTT DATA monitors the webserver infrastructure utilizing SNMP data collection for Linux based webservers, and Windows WMI for IIS webserver. The NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform SOPs or advanced trouble-shooting services.

**For Linux – based webservers**

| LINUX OPERATING SYSTEM | WEBSERVER |
|---|---|
| **Device availability:** up/down | Response Metrics( HTTP Response Time, HTTP Response Value, URL Monitoring) |
| **Device health:** CPU, memory and disk utilization | Server Metrics (Busy Workers, Idle Workers, SSL Certificate Expiration, Keep Alive Count, DNS Lookup Count) |
| **Linux interfaces:** up/down | Throughput Metrics (Requests Served per Minute, Bytes Served per Minute, Bytes Served per Request, Total Bytes, Total Accesses, Number of Concurrent Connections) |
| **Logs:** Critical logs | Website Monitoring (Synthetic Transaction) |
| **Server hardware monitoring:** Disk, memory modules, and chassis temperature | Mimics HTTP/SSL transactions and alerts on return codes, response times and page content (presence or absence). Checks the certificate integrity, validity period, etc. while validating a given user access |

**For IIS Servers**

| WINDOWS OPERATING SYSTEM |
|---|
| **Device availability**: up/down |
| **Device health**: CPU, memory and disk utilization |
| **Linux interfaces**: up/down |
| **Logs**: Critical logs |
| **Server hardware monitoring**: Disk, memory modules, and chassis temperature |

| WEB |
|---|
| Web service\bytes total/sec<br>Web service\total method requests/sec<br>Web service\current connections<br>Web service cache\file cache hits %<br>Web service cache\kernel:uri cache flushes<br>Web service cache\kernel:uri cache misses |
| **FTP** |
| FTP service\bytes sent/sec<br>FTP service\bytes received/sec<br>FTP service\bytes total/sec |

### Standard Operating Procedures

List of SOPs executed by NTT DATA for issues with webservers:

| | |
|---|---|
| **Server availability (up/down) (Linux or IIS server)** | NTT DATA will run diagnostics to check status of problematic webserver from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **Server shutdown (unexpected) alerts** | Validate event logs to check if server shutdown is unexpected |
| **Server in hung state** | Restart server if it is hung ( through DRAC / ILO) |
| **Memory utilization alert** | Validate high utilization, and identify process causing high memory utilization |
| **Processor utilization alert** | NTT DATA will validate high utilization, and identify process causing high processor utilization |
| **Disk space alert** | NTT DATA will validate alert by (a) login into server and (b) identify folders that occupy high disk space, (c) clean-up to free up disk space and (d) notify Customer of folders that occupy high disk space |
| **Hardware error** | Run hardware diagnostics to validate hardware fault |
| **Linux or Windows event log (critical)** | Execute a specific set of instructions when specific critical event occurs |
| **Site and server status** | Open site link from inside the server and outside the server to validate site status. Restart services to eliminate any hung issues. |
| **Certificate expire issues** | Verify certificate validity and other possible issues based on alert received |
| **Port status** | Port status Validate webserver process and port access issues |

### Move, Add and Changes and Service Requests

Following are examples of Service Requests for webservers:

- Generate certificate request and Install certificate for website
- Configure website redirection

- Perform a configuration backup

**Preventive maintenance scope**

- Linux patch management
- Windows patch management
- [For IIS Servers only] Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

For Linux – based Webservers

| Maintenance activity | Frequency |
|---|---|
| Patch scan | Monthly |
| Patch management (install) | Monthly |

For IIs Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

NTT DATA will run scheduled health checks on webservers and their instances to scan for possible issues. If critical issues are identified, NTT DATA will escalate issue to Customer and propose a solution if one exists. Based on approval from Customer, NTT DATA will attempt to resolve the issue. Health checks include:

- Validate overall functionality of webserver after code pushes
- Check validity of certificate for each site
- Maintain Steady State Statistics (SSS): (a) Build SSS (b) Compare each webserver's statistics with SSS (c) Fix any abnormalities

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Operations Management and Monitoring and Remediation packages on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA services team
- For Linux-based webservers, genuine Linux and webserver license is responsibility of Customer. For IIS, genuine Windows and IIS license is responsibility of Customer.

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- Deploy, provision, configure, and/or migrate new webserver
- Architect, design, re-design, and/or migrate webserver, and/or data to a new site, remote office, or branch office
- Make changes to webserver infrastructure

Any items not explicitly covered within this document are considered out of scope.

## Section 9: Microsoft Exchange Server

### Supported environments

| | | |
|---|---|---|
| **Operating Systems** | Windows | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above |
| **Application** | Microsoft Exchange | Microsoft Exchange 2003 and above |

### Key monitoring parameters

NTT DATA monitors the Microsoft Exchange server infrastructure utilizing standard windows WMI data collection. The NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform SOPs or advanced trouble-shooting services.

| WINDOWS OPERATING SYSTEM |
|---|
| **Device availability**: up/down |
| **Device health**: CPU, memory and disk utilization |
| **Linux interfaces**: up/down |
| **Logs**: Critical logs |
| **Server hardware monitoring**: Disk, memory modules, and chassis temperature |
| **PERFORMANCE COUNTERS FOR DATABASE DISKS** |
| Logical disk(*)\avg. disk sec/read and write, physical disk(*)\avg. disk sec/read and write |
| **INFORMATION STORE RPC PROCESSING COUNTERS** |
| MSExchangeIS\RPC Requests, MSExchangeIS\RPC Averaged Latency, MSExchangeIS\RPC Operations/sec, MSExchangeIS\RPC Num. of Slow Packets, MSExchangeIS Client (*)\RPC Average Latency |
| **MESSAGE QUEUING COUNTERS** |
| MSExchangeIS Mailbox(_Total)\Messages Queued for Submission, MSExchangeIS Public(_Total)\Messages Queued for Submission |

| EXCHANGE AND DC CONNECTIVITY |
|---|
| MS Exchange AD Access Domain Controllers(*)\LDAP Read Time, MS Exchange AD Access Domain Controllers(*)\LDAP Search Time, MS Exchange AD Access Processes(*)\LDAP Read Time, MS Exchange AD Access Processes(*)\LDAP Search Time, MS Exchange AD Access Domain Controllers(*)\LDAP Searches timed out per minute, MS Exchange AD Access Domain Controllers(*)\Long running LDAP operations/Min |
| **TRANSPORT QUEUE LENGTH COUNTERS** |
| \MSExchangeTransport Queues(_total)\Aggregate Delivery Queue Length (All Queues), \MSExchangeTransport Queues(_total)\Active Remote Delivery Queue Length, \MSExchangeTransport Queues(_total)\Active Mailbox Delivery Queue Length, \MSExchangeTransport Queues(_total)\Submission, \MSExchangeTransport Queues(_total)\Largest Delivery Queue Length |
| **OUTLOOK WEB ACCESS COUNTERS** |
| MS Exchange OWA\Average Response Time, MS Exchange OWA\Average Search Time |

### Standard Operating Procedures

List of Microsoft Exchange SOPs executed by NTT DATA (may include additional SOPs):

| | |
|---|---|
| **Windows server status (up/down)** | NTT DATA runs diagnostics to check status of problematic Windows server from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **Server shutdown (unexpected) alerts** | NTT DATA will validate event logs to identify if server shutdown is unexpected |

| | |
|---|---|
| **Server in hung state** | Restart server if it is hung (through DRAC / ILO) |
| **Memory utilization alert** | Validate high utilization, and identify process causing high memory utilization |
| **Processor utilization alert** | Validate high utilization, and identify process causing high processor utilization |
| **Disk space alert** | Validate alert by (a) login to server and identify folders that occupy high disk space (b) run disk clean-up to free-up disk space, and (c) notify Customer of folders that occupy high disk space |
| **Hardware error** | Run hardware diagnostic check to validate hardware fault |
| **Windows event log (critical)** | Execute set of instructions when specific critical event occurs |
| **Mail flow (queue management) in exchange** | Check mail queue and update Customer. Take further action based on Customer update. |
| **Mail NDR issues** | Check mail server to validate issue and run SOP to resolve |
| **Mail client login issues** | (a) Check if IIS is running (b) Check if able to resolve client URL internally (toidentify if it's an internal or external issue) (c) Run appropriate SOP as first level resolution |
| **Mail certificate expiry issues** | NTT DATA to run SOP to verify validity of certificate and for other possible issues based on alert received |
| **Exchange information store status** | Check status of information store based on alert received. Run SOPs to start IS service. |

**Move, Add and Changes and Service Requests**

Following are examples of SRs:

- Setup email forwarder to a different user
- Modify mailbox quota
- Perform database consistency checks
- Perform manual defragmentation of Exchange database
- Create public folder

**Preventive maintenance scope**

- Windows Patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

NTT DATA will run scheduled health checks on Microsoft Exchange server once every thirty (30) days to check for possible issues. If critical issues are identified, NTT DATA will escalate issue to Customer and

propose a solution if one exists. Based on approval from Customer, NTT DATA will attempt to resolve the issue.

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation for Microsoft SQL services. These activities can be delivered on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine Windows license is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- Deploy, provision, configure, and/or migrate new Exchange server
- Architect, design, re-design, and/or migrate Exchange servers and/or data to a new site, remote office, or branch office
- Make changes to Exchange server infrastructure
- Setup or install new Exchange 2007, 2010, or above environment
- Migrate or upgrade Exchange 2003 to 2007, 2010, or above environment
- Analyze Customer's Exchange environment and make best practices recommendation, or implement best practices (for Exchange 2003, 2007, 2010, or above)
- Upgrade or migrate from single role to multiple roles on Exchange (e.g. Exchange 2007 and above)
- Upgrade or migrate from non-clustered Exchange to clustered or fully redundant Exchange or email infrastructure (e.g. Exchange 2007 and above)
- Setup or manage various server roles – e.g. client access server role, hub transport server role, edge transport server role, unified message server role, etc.

Any items not explicitly covered within this document are considered out of scope.

## Section 10: Microsoft SharePoint

### Supported environments

| | | |
|---|---|---|
| **Operating Systems** | Windows | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above |
| **Application** | Microsoft SharePoint | SharePoint Foundation 2010 and above<br>SharePoint Server 2010 and above |

### Key monitoring parameters

NTT DATA monitors the Microsoft SharePoint server infrastructure utilizing standard WMI data collection. The NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform SOPs or advanced trouble-shooting services.

| | |
|---|---|
| **SharePoint performance** | Data connection query failure rate<br>Data connection query completed rate<br>Average data adapter query duration<br>Data connection submit failure rate<br>Data connection submit completed rate<br>Data connection submit started rate<br>Average data connection submit duration<br>Session completed rate<br>Session started rate<br>Average session duration<br>Transactions completed rate<br>Transactions started rate<br>Average transaction duration |

| | |
|---|---|
| **Server performance** | CPU utilization<br>Memory utilization<br>Page faults per sec<br>Page file usage<br>Processor queue length<br>Context switches per sec |
| **Server disk performance** | Average disk queue length<br>Average disk read queue length<br>Average disk write queue length<br>Disk reads per sec<br>Disk writes per sec<br>Disk idle time |
| **Server ASP Monitors** | Requests queued<br>Request wait time<br>Requests per sec<br>Percent time spent in garbage collection |
| **Server web service monitors** | Bytes received per sec<br>Bytes sent per sec<br>Current connections<br>Get requests per sec |

### Standard Operating Procedures

List of SOPs Executed by NTT DATA For Issues with Microsoft SharePoint Environment (may include additional SOPs):

| | |
|---|---|
| **IIS server status (up/down)** | NTT DATA will run diagnostics to check status of problematic IIS server from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **IIS certificate expired issues** | NTT DATA will run SOP to verify certificate validity and for other possible issues based on alert received |

| | |
|---|---|
| **Server unavailable** | NTT DATA will (a) Detect any LAN/WAN connectivity issue by checking status of problematic server from a different machine on same network (b) Contact Customer to get server back on network. |
| **Unexpected server shutdown** | NTT DATA will validate event logs to identify cause for unexpected shutdown |
| **Server in hung state** | NTT DATA will attempt to restart server if it is hung ( through DRAC / ILO) |
| **Memory utilization alert** | NTT DATA will validate high utilization and identify process causing high memory utilization |
| **Processor utilization alert** | NTT DATA will validate high utilization and identify process consuming high CPU |
| **Low disk space alert** | NTT DATA will validate alert by (a) login into server and (b) identify folders that occupy high disk space (c) run disk clean-up to free up disk space, and (d) notify Customer of folders that occupy high disk space. |
| **Hardware error** | NTT DATA will run a hardware diagnostic check to validate hardware fault |
| **Windows event log (critical)** | Execute set of instructions when specific critical event occurs |

**Preventive maintenance scope**

- Windows Patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health checks**

NTT DATA will run scheduled health checks on Microsoft Exchange server once every thirty (30) days to check for possible issues. If critical issues are identified, NTT DATA will escalate issue to Customer and propose a solution if one exists. Based on approval from Customer, NTT DATA will attempt to resolve the issue.

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation for Microsoft SharePoint services. These activities can be delivered on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation contacts

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine Windows license is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- Deploy, provision, configure, and/or migrate new SharePoint or IIS server
- Architect, design, re-design, and/or migrate SharePoint servers, IIS servers, and/or data to a new site, remote office, or branch office
- Make changes to SharePoint server infrastructure
- Setup or install new SharePoint environment
- Analyze Customer's SharePoint environment and make best practices recommendation, or implement best practices

Any items not explicitly covered within this document are considered out of scope.

## Section 11: Microsoft Active Directory Services

### Supported environments

| | | |
|---|---|---|
| **Operating Systems** | Windows | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above |
| **Application** | Microsoft Active Directory | All versions |

### Key monitoring parameters

NTT DATA monitors the Microsoft Active Directory server infrastructure utilizing using standard Windows WMI or SNMP data collection. NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform standard operating procedures or advanced trouble-shooting services.

| WINDOWS OPERATING SYSTEM |
|---|
| **Device availability**: up/down |
| **Device health**: CPU, memory and disk utilization |
| **Windows services**: up/down (default: all services with start-up type “automatic”) |
| **Windows event logs**: critical application, system logs |
| **Server hardware monitoring**: Disk, memory modules, and chassis temperature |

| Active Directory |
|---|
| Active Directory Database<br>Database Size(Total/Free)<br>Responsiveness of AD or LDAP<br>Availability of DNS Client Service<br>Availability of Kerberos Key Distribution<br>Availability of Net Log on Service<br>Health of File Replication Service<br>Replication Traffic (In/Out) |

### Standard Operating Procedures

List of SOPs executed by NTT DATA for issues with Microsoft Active Directory server:

| | |
|---|---|
| **Windows server status (up/down)** | NTT DATA runs diagnostics to check status of problematic Windows server from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **Server shutdown (unexpected) alerts** | NTT DATA will validate event logs to identify if server shutdown is unexpected |
| **Server in hung state** | Restart server if it is hung (through DRAC / ILO) |
| **Memory utilization alert** | Validate high utilization, and identify process causing high memory utilization |
| **Processor utilization alert** | Validate high utilization, and identify process causing high processor utilization |
| **Disk space alert** | Validate alert by (a) login to server and identify folders that occupy high disk space (b) run disk clean-up to free-up disk space, and (c) notify customer of folders that occupy high disk space |
| **Hardware error** | Run hardware diagnostic check to validate hardware fault |
| **Windows event log (critical)** | Execute set of instructions when specific critical event occurs |
| **RPC server problems (replication, win login, trust relationships)** | Check replication status. Run SOP to initiate failed replication. |

| | |
|---|---|
| **Fixing errors with sysvol** | Identify Sysvol errors and execute SOP for 1st level resolution |
| **Domain controllers not advertising itself** | Identify errors and execute SOP for 1st level resolution |
| **Object name conflicts** | Identify object conflict and run SOP to resolve. |
| **Excessive Disk And cpu usage by NTFRS.EXE** | Run SOP to resolve |

**Service Requests**

Following are examples of SRs:

- Reconnect a long-disconnected domain controller
- Relocate directory database files

**Preventive maintenance scope**

- Windows Patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Active Directory server health Checks**

NTT DATA will run scheduled health checks on Microsoft Active Directory server once every thirty (30) days to check for possible critical issues such as AD replication issues. For critical AD replication issues, NTT DATA will create a ticket and resolve the issue. (Note: AD replication issue checks for Windows SBS edition is not applicable, and will not be performed).

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation for Microsoft Active Directory services. These activities can be delivered on a T&M basis, in conjunction with Cloud Operations Management and Monitoring and Remediation service levels.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine Windows license is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- Perform an authoritative or non-authoritative restore of entire directory, sub-tree, or leaf object
- Restore original configuration of a domain controller
- Plan, prepare, and install an Active Directory installation
- Rename or decommission a domain controller
- Add or remove global catalog to a domain controller and verify global catalog readiness
- Move, restore, and/or rebuild SYSVOL manually or by using Active Directory installation wizard
- Create or remove trusts, and, add or remove a site or subnet to the network
- Link sites for replication and/or move a domain controller to a different site

Any items not explicitly covered within this document are considered out of scope.

## Section 12: Blackberry

### Supported environments

| | | |
|---|---|---|
| **Operating Systems** | Windows | Windows 2003 Server and above SBS Server (Operating System only) 2003 and above |
| **Application** | Blackberry | BlackBerry Enterprise Server, BlackBerry Enterprise Server Express |

### Key monitoring parameters

NTT DATA monitors the Blackberry Server infrastructure utilizing standard windows WMI data collection. The NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform standard operating procedures or advanced trouble-shooting services.

| WINDOWS OPERATING SYSTEM |
|---|
| **Device availability**: up/down |
| **Device health**: CPU, memory and disk utilization |
| **Windows services**: up/down BBAttachServer; BlackBerry controller; BlackBerry dispatcher; BlackBerry MDS connection service; BlackBerry policy service; BlackBerry router; BlackBerry server alert; BlackBerry sync server; MSSQLSERVER; TrkWks, BlackBerry mail store, BlackBerry administration service – native code container, BlackBerry administration services – application server |
| **Windows event logs**: critical application, system logs |
| **Server hardware monitoring**: Disk, memory modules, and chassis temperature |

| BES SRP connection State |
|---|
| besSysHealthSrpConnectedState, besSysHealthSrpLastConnectDate, besSysHealthSrpReconnectSuccess, besSysHealthSrpReconnectsFail, besSysHealthSrpTotalSecNotConnected, besSysHealthSrpLastErrorText, besSysHealthSrpLastErrorTime |
| **Blackberry Messaging** |
| Messages Error/Pending/Expired |

### Standard Operating Procedures

List of Blackberry server SOPs executed by NTT DATA:

| | |
|---|---|
| **Windows server status (up/down)** | NTT DATA runs diagnostics to check the status of the problematic Windows server from other server in the same network to eliminate any LAN/WAN connectivity issues |
| **Server shutdown (unexpected) alerts** | NTT DATA will validate the event logs to identify if the sever shutdown is unexpected |
| **Server in hung state** | Restarting the server if it is hung ( through DRAC / ILO) |
| **Memory utilization alert** | Validating the high utilization, and identify the process causing high memory utilization |
| **Processor utilization alert** | Validating the high utilization, and identify the process causing high memory utilization |
| **Disk space alert** | Validating the alert by logging into the server and identifying the folders which are occupying high disk space, run disk clean-up to |

| | |
|---|---|
| | free-up disk space and notify the customer of folders occupying high disk space |
| **Hardware error** | Run hardware diagnostic check to validate the hardware fault. |
| **Windows event log (critical)** | Execute set of instructions when specific critical event occurs |
| **Sync status (Blackberry)** | Verify the pending messages in Blackberry console, identify possible issue for pending messages and escalate to the customer |
| **Blackberry services not running** | Validating the services which are not running and starting them if Required |

**Service Requests**

Following are examples of Service Requests for Blackberry servers:

- Configure user Blackberry device and set activation password
- User lost BlackBerry device (need to erase data and lock the device)

**Preventive maintenance scope**

- Windows Patch management
- Validate Anti-Virus definition updates for supported AV products (customer provided)

**Preventive maintenance schedules**

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

**Preventive health Checks**

NTT DATA will run scheduled health checks on Blackberry server once every thirty (30) days to check for possible issues. If critical issues are identified, NTT DATA will escalate issue to customer and propose a solution if one exists. Based on approval from customer, NTT DATA will attempt to resolve the issue.

**Out-of-scope activities**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation for Blackberry services. These activities can be delivered on a T&M basis, in conjunction with enterprise services Cloud Operations Management and Cloud Monitoring and Remediation service levels.

Out-of-scope monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- A genuine Windows license is responsibility of Customer

Out-of-scope Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of Customer
- Virus scan and virus removal on desktops and server

Out-of-scope Service Requests

- Blackberry Server version upgrade(s)
- New Blackberry server installation and configuration
- Custom application deployed on Blackberry server

Any items not explicitly covered within this document are considered out of scope.

# Section 13: Virtualization

NTT DATA Managed Cloud Services for virtualization can be broadly categorized as follows:

- Server virtualization services
- Application virtualization services

## 13.1 Server virtualization services

### Supported environments

| | | |
|---|---|---|
| **Microsoft** | **Hyper-V** | Microsoft Hyper-V Server 2008, Hyper-V roles on Windows Server 2012, Windows Server 2008 R2 and Windows Server 2008 |
| **VMware** | **ESX** | VMware vSphere ESXi, VI Foundation/ Standard/ Enterprise/ Enterprise Plus |
| **Citrix** | **XenServer** | XenServer 6.0.2, 6.0, 5.6 and 5.5 - Platinum, Enterprise, Advanced and Free editions |

## Key parameters monitored

| Hyper-V based monitors | |
|---|---|
| **Memory** | Available Bytes<br>Average pressure<br>Hypervisor partition deposited pages<br>Hypervisor partition value 2MGPA pages<br>Hypervisor partition virtual processors<br>Hypervisor root partition deposited pages<br>Hypervisor root partition value 2MGPA pages<br>Hypervisor root partition virtual processors<br>Physical pages allocated<br>Remote physical pages |
| **Hypervisor** | Number of logical processors<br>Number of virtual machines<br>Number of virtual processors<br>Pages per second<br>Total pages<br>VM health summary |
| **Network** | Network interface utilization<br>Offloaded connections<br>Packets received errors<br>Packets outbound errors<br>Legacy network adapter bytes dropped<br>Legacy network adapter bytes received per sec<br>Legacy network adapter bytes sent per sec<br>Virtual switch bytes per sec<br>Virtual network adapter bytes per sec |
| **Processor** | CPU processor time<br>Logical processor guest run time<br>Logical processor hypervisor runtime<br>Logical processor idle time<br>Logical processor total runtime<br>Root virtual processor guest runtime<br>Root virtual processor hypervisor runtime<br>Root virtual processor total runtime<br>Virtual processor guest run time<br>Virtual processor hypervisor runtime<br>Virtual processor total runtime |
| **Storage** | Current disk queue length<br>Disk bytes parsec<br>Disk transfers per sec<br>Error count<br>Flush count<br>Virtual IDE controller read bytes per sec<br>Virtual IDE controller write bytes per sec<br>Virtual storage device read bytes per sec<br>Virtual storage device write bytes per sec |

| VMware ESX based monitors | |
|---|---|
| **System status** | System status<br>Memory status<br>Numeric sensor status<br>Processor status<br>Record logs<br>Discrete sensor status<br>Battery status<br>Controller status<br>SAS SATA port status<br>Storage extent status |
| **System status** | Storage volume status<br>Run time issues<br>Run time status |
| **System health** | Available storage space<br>CPU utilization<br>IO read rate<br>IO write rate<br>Memory utilization<br>Network utilization<br>Swap usage |

| XenServer monitors | | | |
|---|---|---|---|
| **XenServer health** | CPU utilization<br>CPU statistics<br>Disk utilization<br>Load statistics<br>Memory utilization | **XenServer pool monitors** | License expiry check<br>VM hosted on each host<br>XenServer host status |
| **Storage** | Storage utilization | | |

## Standard Operating Procedures for Virtual Server Incidents

List of SOPs Executed by NTT DATA for a Virtualization Server Incident (may include additional SOPs):

| | |
|---|---|
| **High memory utilization** | NTT DATA will validate high utilization, and identify process causing high memory utilization |
| **High processor utilization** | NTT DATA will validate high utilization, and identify process causing high processor utilization |
| **Low disk space** | NTT DATA will validate alert by (a) Login server and identify Logical Unit Numbers (LUNs) or folders that occupy high disk space, (b) Run SOP to free disk space and (c) Notify Customer |
| **Issues with environmental parameters (fans, power, voltage or temperature)** | NTT DATA will validate issue and provide details to Customer |
| **High IOPS or latency or bandwidth utilization on server** | NTT DATA will monitor usage trends for a period of sixty (60) minutes. If issue persists, NTT DATA will update Customer with suggestions to improve performance. |
| **Status down alerts** | NTT DATA will validate issue and based on impact will raise a high priority ticket with Customer |

## Move, Add and Changes and Service Requests

Customer can create ticket and assign it to NTT DATA for executing the following MAC requests:

- Change network ports for virtual machines
- Add additional VLANs to virtual switches
- Add new data stores or storage repositories
- Add new virtual disks to existing virtual machines

Following are some examples of SRs:

- Best practice analysis of Customer's deployment – check consolidation ratio
- Restore backup images and test for viability
- Install new ESX, Hyper-v, or XenServer
- Create and configure new cluster or pools
- Decommission unnecessary VMs

## Preventive maintenance scope

The following maintenance activities will be performed based on Customer requests or on as as-needed basis:

- Software and firmware upgrades as required
- Service packs or driver versions; or security and hotfix validations and compliance

### Preventive health checks

The following health checks will be performed on a periodic basis:

- Monitor resource utilization and performance trends on host and VMs - CPU, memory, disk, and data store usage and status
- Check for VM sprawl
- Do capacity planning based on usage trends
- Configure necessary backup and snapshots of VMs
- Cluster or pool configuration checks
- Perform network physical, virtual, or virtual switch configuration checks

## 13.2 Application Virtualization Services

Application virtualization provides users with access to applications without the need to install an application. It reduces the cost of application management by up to 50% and provides users with a similar experience as when compared to traditional application deployment models.

### Supported technologies

| | | |
|---|---|---|
| **Citrix** | **XenApp** | XenApp 6.5, XenApp 6.0 and XenApp 5.0 - Advanced, Enterprise and Platinum editions. |

## Key parameters monitored

| Citrix XenApp monitors | | | |
|---|---|---|---|
| **XenApp server health** | CPU utilization<br>Memory utilization<br>Disk utilization<br>Network Interface usage statistics<br>ICA connectivity<br>Server Load | **ICA session monitors** | Session average latency<br>Session latency deviation<br>Active sessions per server |
| **XenApp server performance** | Application enumerations per sec<br>Application resolution time<br>Application resolutions failed per sec<br>Data store connection failure<br>Data store bytes read and writes per sec<br>Dynamic store bytes read and writes per sec<br>Dynamic store gateway count<br>Dynamic store query count<br>Local host cache read and writes per sec<br>Total number of XML threads<br>Number of busy XML threads<br>Resolution work item queue executing count Resolution work item queue ready count<br>Work item queue executing count<br>Work item queue pending count<br>Work item queue ready count<br>Zone elections won | **Application monitoring** | Number of published<br>Enabled and disabled applications<br>User per applications<br>Servers per application |
| | | **XenApp server user monitoring** | Sessions per servers<br>Users per application<br>User resource usage - CPU entitled, CPU reserved, CPU shares, CPU usage, long term CPU usage<br>User latency metrics<br>Session bandwidth utilization |
| | | **License server** | Average license Check-in and Check- out response times<br>License server connection failure<br>Usage percent |
| | | **Web interface performance** | Request queued<br>Requests rejected<br>Request execution time |
| | | **Provisioning servers for terminal services** | Active sessions<br>Total sessions |
| | | **IMA networking** | In-bound and out-bound traffic rate<br>Active IMA Network connections |
| **Status checks** | Applications in disabled state<br>Disconnection sessions per server<br>Offline servers<br>Number of enabled applications per server | | |

## Standard Operating Procedures for virtualized application incidents

List of SOPs executed by NTT DATA for a virtualization application incident (may include additional SOPs):

| | |
|---|---|
| **XenApp server health – resource utilization issues** | NTT DATA will validate high utilization, and identify process causing high memory or CPU utilization. In case of high disk usage alerts, NTT DATA will validate alert by (a) Login server and identify LUNs or folders that occupy high disk space, (b) Run SOP to free disk space and (c) Notify Customer |
| **XenApp server performance issues** | NTT DATA will validate performance issues that impact users who access applications. Corresponding action will be taken to resolve performance issues. |
| **IMA networking issues** | NTT DATA will validate IMA related issues on XenApp servers and farm. NTT DATA will troubleshoot issues that affect IMA services such as network, database server, or LHC issues and resolve them accordingly. |
| **ICA session issues** | NTT DATA will validate and perform appropriate actions for any ICA session issues caused within XenApp environment. These could be session disconnections or reconnections, non-functional drive or printer mappings, etc. |
| **XenApp user issues** | NTT DATA will validate single user issues such as inability to login, slow logon, inability to launch applications etc., and will follow corresponding SOPs to remediate issues. |
| **License issues** | NTT DATA will validate license server issues and license expiration issues and notify Customer. |
| **Web Interface performance issues** | NTT DATA will validate issues with web interface server and follow SOPs accordingly to resolve issues. |

## Move, Add and Changes and Service Requests

Customer can create ticket and assign it to NTT DATA for executing the following MAC requests:

- Create, configure and manage Citrix policies to control user access and session environments

Following are some examples of SRs:

- Best practice analysis of deployment – optimize audio playback, video playback, image file throughput, image file display, keyboard & mouse responsiveness, etc.
- Maintain server farms - limiting number of server connections per user; enable or deny logons to servers
- Security – secure server farms, data stores, or client-server communications; configure session data encryption, etc.

## Preventive maintenance scope

The following maintenance activities will be performed based on Customer requests or on as as-needed basis

- Software and firmware upgrades as required
- Windows patch management and end point security updates, if applicable, on XenApp Servers

## Preventive health checks

The following health checks will be performed on a periodic basis:

- Check XenApp farm status using DSCHECK, QFARM, QueryHR and QueryDS
- Check for license usage
- Monitor resource utilization and performance trends on host and VMs
- Perform tests such as Citrix IMA service test, local host cache test, ICA listener test

## Section 14: Storage

### Supported technologies For Storage

| | |
|---|---|
| **Dell** | EqualLogic PS Series, MD Series, Compellent |
| **EMC** | VNX and VNX e, CLARiiON CX and AX, Celerra |
| **NetApp** | NetApp FAS 2xxx, 3xxx Series, NetApp F-500, F-600 & F-700 Series, and C Series |
| **HP** | Left Hand Solutions & MSA Series |
| **Cisco** | MDS Fabric switches |
| **Brocade** | DS,ED & DCX switches |
| **Netgear** | ReadyNAS |
| **QNAP** | TS series |
| **Buffalo** | TeraStation III Rackmount TS-RXL |
| **VMware** | VSAN |

### Key parameters monitored

| **EMC based monitors** | |
|---|---|
| **Storage system** | Device availability: up/down<br>Device health: (CPU, memory and disk utilization) |
| **Storage SAN performance** | Storage processor busy percentage<br>Storage processor idle percentage<br>SP dirty pages in cache |
| **Storage SAN status** | Status of storage processors<br>Storage processor cache status<br>Storage processor disk status storage processor faults state<br>Storage processor port state<br>HBA state |
| **NetApp based monitors** | |
| **System health** | CPU utilization<br>Cache age<br>Global status<br>Consistency points checks<br>Autosupport status |
| **Disk drive RAID information** | RAID disk status<br>RAID disk utilization<br>Number of spare disks<br>Number of out-of-service disks<br>Number of out-of-date disks<br>Failed disks<br>Number of active disks |
| **Protocol based performance monitoring - NFS** | % Read operations<br>% Write operations<br>% Commit operations<br>% Reads from cache<br>Rate of NFS calls |
| **Protocol based performance monitoring - CIFS** | % Read operations<br>% Write operations<br>Rate of CIFS calls |

| | |
|---|---|
| | Voltage status for each components |
| **Logical disk monitors** | VFiler status<br>Aggregate status<br>Volumes hosted on an aggregate<br>Volume status<br>Qtree status<br>Disk space utilization on Volumes and file system<br>Inode utilization on volumes and file systems<br>Status of volumes and file systems<br>File system overall status |
| **Filer inventory details** | Filer Product Model, File Product GUI URL, Total disks, Total, aggregates, Total volumes |
| **System hardware** | High Temperature alarm<br>Failed Fan count<br>Failed power supply unit count<br>NVRAM battery status<br>Enclosure – failed power supplies<br>Enclosure – failed fans<br>Enclosure – failure due to over-temperature<br>Enclosure – failure due to under-temperature<br>Enclosure – failed electronic elements |
| **Cluster failover** | Cluster failover state<br>Cluster failover partner status<br>Cluster failover interconnect status |
| **Snapmirror summary** | Snapmirror enabled state<br>Snapmirror job state<br>Snapmirror job last transaction time<br>Snapmirror job last transaction transfer size |
| **Snapvault summary** | Snapvault enabled state<br>Snapvault job status<br>Snapvault job last transaction time<br>Snapvault job last transaction transfer size<br>Snapvault lag<br>Snapvault host rate of successful, failed and deferred Snapvault transfers |
| **NDMP summary (tape backups)** | NDMP status<br>Number of successful NDMP backups<br>Number of failed NDMP backups<br>NDMP backup failure cause |
| **License enabled state** | NFS license, CIFS license, SnapMirror license, SnapVault Primary licensed, SnapVault Secondary licensed, |
| **Equallogic monitors** | |
| **Member details** | Member Health<br>Member Fan<br>Member Temperature<br>Member Power<br>Member Storage<br>Member Raid Status<br>Member iSCSI connections<br>Member Read Performance |
| **Disk** | Disk Status<br>Disk Performance |

| | |
|---|---|
| **Group** | Group Members<br>Group Pool Details |
| **Storage pools and volumes** | Volume status<br>Storage Pool<br>Storage Replication Space |
| **Hardware** | Controller Battery Status |
| **LeftHand SAN** | |
| **SAN hardware monitors** | Fan Status<br>Temperature Status<br>Power Status<br>Voltage Status<br>Cache Status<br>Raid Status<br>Storage Device Status |
| **SAN cluster monitors** | Cluster Space Monitor<br>Cluster Performance<br>Cluster Volume Space<br>Cluster Volume Performance<br>Cluster Virtual IP<br>Cluster Manager Monitor<br>Cluster Volume Snapshot Performance<br>Cluster Volume Snapshot Space |
| **Fiber channel switches** | |
| **Port monitors** | Fiber Channel Module Status<br>Fiber Channel Fabric Details<br>Fiber Channel Port Status<br>Fiber Channel Port Errors<br>Fiber Channel Port Traffic |

## Standard Operating Procedures for storage incidents

List of SOPs Executed by NTT DATA on occurrence of a storage incident (may include additional SOPs):

| | |
|---|---|
| **Storage device unavailable** | NTT DATA will check and validate status of storage device. If device is offline due to a hardware failure or malfunction, NTT DATA will collect diagnostic logs and conduct tests on device. If needed, storage vendor will be contacted with approval of Customer. Health checks will be performed on devices that are available but in a faulty state. All tasks will be performed either from storage console or management station. |
| **High memory utilization** | NTT DATA will validate high utilization, and identify process causing high memory utilization |
| **High processor utilization** | NTT DATA will validate high utilization, and identify process causing high processor utilization |
| **Low disk space** | NTT DATA will validate alert by (a) Log into server and identify LUNs or folders that occupy high disk space, (b) Run SOP to free disk space and (c) Notify Customer |
| **Issues with environmental parameters (fans, power, voltage or temperature)** | NTT DATA will validate issue and provide details to Customer |
| **Storage processor, ports, HBA, LUN, volume, or disks** | NTT DATA will access storage management console to validate incident by referring to logs and other indicators available. NTT DATA will attempt to revive element that is down. |

| | |
|---|---|
| **reported as unavailable or offline** | |
| **Fabric switch ports unavailable** | NTT DATA will access storage environment to determine criticality of affected port and attempt to revive port. |
| **High IOPS, latency, or bandwidth utilization on storage device or SAN switches** | NTT DATA will monitor usage trends for a period of sixty (60) minutes. If issue persists, NTT DATA will update Customer with suggestions to improve performance. |

## Move, Add and Changes and Service Requests

NTT DATA will perform administrative activities as part of Move, Add and Changes (MACs):

- Create LUNs and volumes as required
- Create aggregates and RAID groups
- Perform MAC for (a) VLAN & VSAN management, (b) Authentication configurations, (c) User management and (d) DNS management
- Add new disks
- Configure zones and masks on SAN
- Change root volume

Following are some examples of SRs:

- Setup new internal replication process
- Migrate data between LUNs
- Setup file archiving policies
- Migrate array data
- Perform architectural design work for SAN and NAS
- Implement or migrate storage deployments

## Preventive maintenance scope

The following maintenance activities will be performed based on Customer requests or on as as-needed basis:

- Reclaim storage monthly, on an as-needed basis, or on Customer request after a review of active and inactive LUNs by NTT DATA
- Resize NFS and VMFS data stores
- Backup configurations of storage system
- Upgrade storage controller firmware based on Customer approvals
- Update firmware on HBA drivers based on Customer approvals
- Update firmware on HBA disks based on Customer approvals
- Update storage OS with latest patches based on Customer approval

## Preventive health checks

The following health checks will be performed on a periodic basis:

- Check for multipath failover on HBA
- Track de-dupe schedules and notify Customer on the status of reclaim
- Perform status checks on snapshots for volumes and aggregates
- Enable auto-support
- Perform license management
- Review audit logs

## Out-of-scope services

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Operations Management and Monitoring and Remediation packages, on a T&M basis.

Out-of-scope monitoring:

- Customizations to monitoring templates are out of scope -- any request for customizations to monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope Standard Operating Procedure – only for Cloud Monitoring and Remediation

- Any alert that arrives which has no associated SOPs is out of scope – such alerts will be escalated to the escalation contacts provided by Customer

Out-of-scope problem management – only for Cloud Monitoring and Remediation

- Troubleshooting and fixing problems
- Vendor management or escalation
- Root cause analysis

Out-of-scope Service Requests

- Setup of new internal replication process
- Migration of data between LUNs
- Setup of file archiving policies
- Activities typically performed by Customer directly:
    - Swap out hard drives
    - Re-shelve drive enclosures
    - Re-wire storage array to SAN or back-end storage
- Migrate arrays (data)
- Perform architectural design work on SAN and NAS
- Perform implementation or migration of storage

Any items not explicitly covered within this document are considered out of scope.

## Section 15: Network Infrastructure

### Supported technologies & devices

| | | |
|---|---|---|
| **Switches** | LAN switches | **Cisco -** Catalyst Switches 2xxx, 3xxx<br><br>**Juniper:** EX2200, EX2500, EX3200, EX3300, EX4200, EX4500, EX6200, E320<br><br>**HP** – 1910, 2905, 1810, 1700, 1410, 1405, 12500, 9500, 5920, 5900AF, 5830, 5820, 5800, 6600, 6125G/XG Ethernet Blade Switch, 6125G/XG Blade Switch, 6120XG Blade Switch |
| | LAN switches – core, service provider switches - aggregation | **Cisco -** Catalyst Switches 4xxx, 45xx, 49xx, 5xxx, 65xx |
| **Routers** | Branch routers / service provider edge routers | **Dell** – Force10 S25n, S4810 ToR & S6000<br><br>**Cisco**- 8x,18xx, 19xx, 2800, 2900, 3200, 3800, 3900, 7200, 7300, 7500, 76xx Series<br><br>**Juniper** - M , E , ERX , J, T Series |
| **Firewalls & Security Devices** | Network security | **Cisco** - ASA 5500 series, Pix Firewall 5xx, SA 500 series, ACA Express<br>**Juniper** - SRX Series Services Gateway, Net Screen Series, SA Series SSL VPN Appliance, SSG VPN Security Platform<br>**Palo Alto Networks** – firewalls only***** - PA 200, 500, 2000, 3000, 5000, 7050 series<br>**Barracuda Networks** – Spam & Virus Firewall<br>**Fortinet** – FortiGate series (20C, 40C, 50B/51B, 60D, 60C-POE, 60C, 80C/CM, 100D, 5000 Security Blades, 5000 Netwirjubg Blades, 5000 Chassis)<br>**WatchGuard** – Fireware XTM, Fireware XTM Pro XTM Series<br>**Bluecoat** - Proxy SG Series |
| **WAP** | Wireless access points and controllers | **Cisco** – Access Point (15xx), Wireless Access Points (500 Series Wireless Express, Cisco Aironet Series), Wireless LAN Controllers (21xx, 25xx, 44xx, 55xx)<br>**Aruba** – Mobility Controllers -- 600, 3000, 7000, and 7200 series<br>**Aruba** – Mobility Access Switches – S1500, S2500, and S3500 series<br>**Meru** – MC1550, MC6000 |
| **Load balancers** | Load balancers | **A10** – load balancers only* - AX series<br>**F5 Networks** – LTM, GTM |

| | | |
|---|---|---|
| **WAN optimizers** | WAN optimizers | **Riverbed** - Steelhead Product Family<br>**Exinda** – 2051 Appliance |
| **Other** | Other | **Cisco** – Nexus 7000, UC520, UC540, UC560, Unified Communications Manager Express, Unity Express, UCS 21000 Series Fabric Extenders, Nexus 7000 Series Supervisor Module, Nexus 7000 Fabric Module, Nexus 7000 I/O module |

* Supported for Cloud Monitoring and Remediation service levels only (not for Cloud Operations Management)

## Key monitoring parameters

NTT DATA monitors the network infrastructure utilizing standard SNMP data collection, SNMP trap receiver, syslog monitoring, and synthetic transaction monitoring capabilities. The NTT DATA platform also provides NTT DATA staff with secure remote access to monitored devices, to perform SOPs or advanced troubleshooting services.

| WIRELESS NETWORKS |
| --- |
| Access Point availability |
| Access Points client statistics |
| Network Health – load, interference, noise and coverage status |
| **REAL-TIME NETWORK PERFORMANCE MONITORING (SYNTHETIC TRAFFIC)** |
| HTTP - URL response time |
| Network Health – load. interference, noise and coverage status |
| **ARUBA WIRELESS CONTROLLERS, SWITCHES, & WAPS** |
| **Controllers**: processor load, storage utilization, memory utilization, card status, fan status, power supply status, switch status, internal temperature, switch license count, total users<br>**Switches**: processor load, storage utilization, memory utilization<br>**Other**: AccessPoint up/down, AP Radio Attributes, Auth Max ACL Entries, Auth Max BW Contracts, Auth Max User Entries, Auth Server up/down, Auth Server Req Timed Out, Auth Server Timed Out, Channel Changed, Coverage Hole Detected, DB Communication Failure, ESI Server up/down, Fan Failure, Fan Tray Inserted/Removed, GBIC Inserted, IP Spoofing Detected, LC Inserted/Removed, License Expiry, Low Memory, Low On Flash Space, Out Of Range Temperature, Out Of Range Voltage, Power Supply Failure/Missing, Process Died, Process Exceeds Memory Limits, SC Inserted/Removed, Station Added/Removed To BlackList, Switch IP Changed, Switch Role Change, User Authentication Failed, User Entry Authenticated/Created/De-Authenticated/Deleted, VRRP State Change. |

| SWITCHES, ROUTERS AND FIREWALL |
| --- |
| **Device availability:** up/down |
| **Device health:** (CPU and Memory utilization) |
| **Interface Status:** up/down |
| **Interface Performance:** – Utilization, In/Out Traffic Rate |
| **Interface Errors:** Error and Discard Rate, CRC and Collision Errors |
| **Buffer Usage: –** Small, Medium, Large and Huger buffer utilization and failures |
| **VPN:** – IKE and IPsec Tunnel Availability |
| **Hardware Monitoring: disk, memory modules, chassis temperature**, Fan, Power, and Voltage Status |

## Standard Operating Procedures

List of Network Infrastructure SOPs executed by NTT DATA (may include additional SOPs):

| | | |
|---|---|---|
| **Switch/router/ firewall** | Device status (up/down) critical alerts | NTT DATA runs diagnostics to check status of problematic device from a different device in same network to eliminate any LAN/WAN issues. |
| **Switch/router/ firewall** | Memory, processor, buffer utilization high on any network device | NTT DATA validates utilization by logging into device, and identifying reason for high utilization. |
| **Switch/router/ firewall** | Inbound/outbound errors on interfaces | NTT DATA checks errors on interfaces and clears errors. If errors persist on WAN link at same rate, NTT DATA checks physical connectivity issue and then escalates to Telco or ISP. |
| **Switch/router/ firewall** | Interfaces or Link Down | NTT DATA logs in to device and checks if interface is “admin down” or “protocol down.” In case of “admin down,” NTT DATA alerts Customer and if “protocol down,” checks logs to see if issue is due to network flap. |
| **Router/firewall** | VPN tunnels (mainly for firewalls but can also be applied for routers) | NTT DATA checks tunnel status and find reason if tunnel goes down. |

## Move, Add and Changes and Service Requests

Customer can create ticket and assign it to NTT DATA for executing the following MAC requests:

- VPN user related MAC requests
- Parameter tuning of existing VPN tunnels
- SSID changes on WAP device

Following are some examples of supported SRs:

- Device configuration restore in case of misconfigurations or failed device replacement
- Upgrade of firmware for fixing security issues
- Configuration change requests (NAT, rules, VLANs, routes, access)
- Configuring VPNs (e.g. SSL VPN), site-to-site, remote access
- On-demand bandwidth control requests or as part of remediation
- Allow or deny IP and ports

## Preventive maintenance scope

Preventive maintenance scope is different by coverage level between Cloud Monitoring and Remediation (CMR) and Cloud Operations Management (COM).

| NTT DATA MANAGED CLOUD SERVICES | Switches | | Routers | | Firewall | | WAP | |
|---|---|---|---|---|---|---|---|---|
| | CMR | COM | CMR | COM | CMR | COM | CMR | COM |
| **Configuration backup of network devices** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| **Firmware Upgrades as Required** | | ✓ | | ✓ | | ✓ | | |

NTT DATA will provide periodic **configuration backup** of network devices along with a difference report between any two (2) revisions of configuration. NTT DATA will also conduct a backup of network device configuration every fifteen (15) days or on any change in device configuration. The configuration backup will be stored in the NTT DATA cloud for configuration management.

**Note:** Configuration backup is an automated process and has to be supported by the network device. If an automatic process is not supported by the network device, then NTT DATA will not be able to provide a backup of network device configuration.

Deliverables:

- If a configuration backup job did not run on a device during the scheduled time, NTT DATA will investigate the issue and resolve it. If the device has missed or failed two (2) consecutive scheduled jobs, NTT DATA will execute SOPs to resolve the issue
- If a backup configuration event results in device related issues, then NTT DATA will engage as per the defined SLA

## Preventive health checks

- None

## Telecommunications (Telco) or ISP Vendor Escalations and Follow-ups

For Cloud Operations Management service level, NTT DATA will support Telco or ISP vendor escalations for internet, leased lines, or MPLS circuits in the event of link down, high latency, or high interface errors. NTT DATA will create tickets with the Customer and escalate the issue to the Customer following the escalation matrix provided by the Customer.

**Note:** To support Telco or ISP vendor escalations by NTT DATA, it is mandatory that Customer purchase NTT DATA management services for internet or WAN links on interface of managed devices.

*Deliverables:*

To support the key objectives of SLA, NTT DATA will follow the process defined below as part of NTT DATA delivery model:

- NTT DATA will monitor WAN connectivity and call Customer or create an online ticket, as well as escalate the issue to Customer as per a standard escalation process
- All Customer related issues, such as internet or WAN link down, will be escalated to Telco or ISP either via phone call or a ticket created in online system of Telco or ISP
- Summary of conversations with Telco or ISP will be updated in ticket

- NTT DATA recommends that Customer maintain valid support contracts with Telcos or ISPs
- It is required that Customer authorize NTT DATA to act on their behalf during escalation
- Response and resolution SLAs of vendors are applicable to issues escalated by NTT DATA

## Out-of-scope services

**Telco or ISP vendor escalations are only available for Routers and Firewalls for Cloud Monitoring and Remediation and Operations Management. Telco or ISP vendor escalations for Switches and WAP are out of scope.**

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Operations Management and Monitoring and Remediation packages, on a T&M basis.

Out-of-scope for monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope for SOPs - Cloud Monitoring and Remediation Only

- An alert with no SOPs will be escalated to Customer as per escalation matrix

Out-of-scope for problem management – Monitoring and Remediation Only

- Troubleshooting, fix, vendor management, and root cause analysis on network devices are out of scope

Out-of-scope for Service Requests

- New device deployment, provisioning, configurations, and migrations
- New site architect/design/re-design/migration of network infrastructure, remote office or branch office
- New firewall rules and routing table modifications
- DNS changes and IP allocations
- Network topology changes

Any items not explicitly covered within this document are considered out of scope.

# Section 16: Datacenter & Converged Infrastructure Practice - VCE vBlock, NetApp FlexPod, and EMC VSPEX

## Supported Unified Computing infrastructure

| | |
|---|---|
| **Unified Computing (UCS)** | Cisco UCS 6100 Series Fabric Interconnects, Cisco UCS 5100 Series Blade Server Chassis, Cisco UCS 2100 Series Fabric Extenders, Cisco UCS B-Series Blade Servers, Cisco UCS B-Series Network Adapters, Cisco UCS C-Series Rack-Mount Servers, Cisco UCS C-Series Network Adapters, Cisco UCS Manager |
| **Virtualization** | VMware |
| **Network** | Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, Cisco Nexus 2000 Series, Cisco Nexus 1000V Virtual Switch |
| **Storage** | **EMC**: Connectrix Switches and Directors, EMC CLARiiON CX Series, FC, AX Series, Symmetrix DMX Series and V-Max Series<br>**NetApp**: NetApp FAS 2xxx, 3xxx Series, NetApp F-500, F-600 and F-700 Series, and C Series |

Configurations of VCE vBlock reference platforms for NTT DATA Managed Cloud Services

| | | Configurations of Reference Platforms of Cisco UCS (for VCE vBlock) for NTT DATA Managed Cloud Services | | | | | |
|---|---|---|---|---|---|---|---|
| | | UCS-vBlock reference platform 1 | | UCS-vBlock reference platform 2 | | UCS-vBlock reference platform 3 | |
| Reference Platform Components | | CMR | COM | CMR | COM | CMR | COM |
| **Compute – Cisco UCS** | Cisco UCS Blade Server Chassis | 1 | 1 | 2 | 2 | 4 | 4 |
| | Cisco UCS 2100 Series Fabric Extenders | 2 | 2 | 4 | 4 | 8 | 8 |
| | Cisco UCS B-Series Blades | 4 | 4 | 8 | 8 | 16 | 16 |
| | Cisco UCS Fabric Interconnects | 1 | 1 | 2 | 2 | 2 | 2 |
| | 6200 Series (UCS 6248UP, Cisco UCS 6296UP) | | | | | | |
| | 6100 Series (UCS 6120XP, Cisco UCS 6140XP) | | | | | | |
| **Network** | Cisco Nexus 5010 switches and /or MDS 9000 series switches | 2 | 2 | 2 | 2 | 2 | 2 |
| | Nexus 1000v Switch | 1 | 1 | 1 | 1 | 1 | 1 |
| **Storage** | EMC Celerra Unified Storage NS-120 Storage Array (up to 46 TB capacity) | 1 | 1 | | | | |
| | EMC Clariion CX4 (38-64 TB capacity) | | | 1 | 1 | | |
| | EMC Symmetrix VMAX (96-146 TB capacity) | | | | | 1 | 1 |
| **Virtualization software** | VMware vSphere 4 | | | | | | |
| | Max VM per vBlock | | | | | | |

Configurations of FlexPod reference platforms for NTT DATA Managed Cloud Services

| | | Configuration of Reference Platforms of Cisco UCS (for NetApp FlexPod) for NTT DATA Managed Cloud Services | |
|---|---|---|---|
| | | UCS-FLEXPOD reference platform 1 | |
| **Reference platform components** | | CMR | COM |
| **Compute – Cisco UCS** | Cisco UCS Blade Server Chassis | 4 | 4 |
| | Cisco UCS 2100 Series Fabric Extenders | 8 | 8 |
| | Cisco UCS B-Series Blades | 32 | 32 |
| | Cisco UCS Fabric Interconnects | 2 | 2 |
| | 6200 Series (UCS 6248UP, Cisco UCS 6296UP) | | |

| | | | |
|---|---|---|---|
| | 6100 Series (UCS 6120XP, Cisco UCS 6140XP) | | |
| **Network** | Cisco Nexus 5010 switches and /or MDS 9000 series switches | | |
| | Cisco Nexus 5548 | 2 | 2 |
| | Cisco Nexus 1010 | | |
| | Nexus 1000v Switch | 2 | 2 |
| **Storage** | NetApp FAS3210A (NetApp Complete Bundle) | 1 | 1 |
| **Virtualization Software** | VMware vSphere 4 | | |
| | Max VMs per vBlock | | |

## Key monitoring parameters

NTT DATA monitors Cisco based data center environments using SNMP and syslog. Comprehensive monitoring templates help ensure that all aspects of the environment are monitored for performance, availability, and capacity. The following metrics are monitored:

| **Monitored components** |
|---|
| Chassis |
| Chassis fan module |
| Chassis fans |
| Power supply units |
| IO modules |
| Blade servers |
| Blade server adaptor units |
| Blade server memory arrays |
| Blade server processors |
| Fabric interconnect fans |
| Fabric interconnect power supplies |
| Fabric interconnect IO modules and ethernet ports |
| Fabric interconnect IO module fiber channel ports |
| Fabric interconnect local storage and dynamic counters |
| **UCS hardware status monitoring** |
| Operational status for fans, LEDs, cards and memory |
| Fault condition - UCS error IDs, condition codes, rules, severity |
| Physical Switch I/O operational and administrative status |
| UCS 6100 chassis Management controller statistics |
| CPU Statistics |
| **UCS environmental status monitoring** |
| Power status for all components |
| UCS 6100 cooling fan type and condition |
| Temperature statistics on all components |
| Voltage status for each components |
| |
| **Storage RAID monitoring - SAN** |

| UCS HARDWARE INVENTORY |
|---|
| Model revision, serial number, vendor details for each chassis |
| Chassis ID, slot ID, model, revision, serial numbers and vendor details for each blade |
| Switch ID, slot ID, model, revision, serial number, vendor details for each fabric interconnect |
| Chassis ID, model, revision, serial number, vendor details for each fabric extender |
| chassis ID, model, revision, serial number, vendor details for each network adaptor |
| Number of chassis installed |
| Number of servers per chassis |
| Memory available on each server |
| Type and quantity of interface cards one each server |
| Virtual environment monitoring |
| Server availability |
| Server performance (**CPU**: Clock Speed, CPU utilization<br>**Memory**: Free, Total and Used Memory, and **Disk**: Free, Used, Total and Virtual Allocation) |
| Server Hardware monitoring |
| Network Interface – Total Bytes/sec |
| Network Interface – packets Outbound errors |
| VMware Hypervisor Host Storage: Storage Type, Availability<br>Storage size, used size and free size |
| **Hosted application monitoring** |
| Application availability |
| Other application specific parameters |
| **Storage hardware monitoring** |
| Disk, Memory Modules, Chassis Temperature |

| |
|---|
| Inventory – Storage Processors, Front end (FC, Gb) Ports, Back End (FC,SAS) Ports, Disk Drives |
| Configuration Details – LUN details, Raid Groups, Host-Port Mappings |
| Availability – SP Status, SP Port Status, FC/Gb/SAS Ports Status, Disk Drive Status, LUN Status and Raid Group Status |
| Performance – Array, Device Drive, LUN, Storage Pool and Storage Volume Statistics |

| **Storage RAID monitoring - NAS** |
|---|
| Latency Statistic Per Protocol - Average latency for NFS v3 and CIFS Operations, Average latency for iSCSI read/write, FCP read/write and NFS v3 read/write Operations |
| Disk – Average, Read, Write Volume Latency, Total, Read and Write Volume OPS, Total, Read and Write Aggregates, Aggregates CP Reads, Disk read/write Throughput |
| CPU – CPU Utilization, CPU Count |
| Network – Send/Receive Throughput, Send/Receive Packet Rate, Error rate, Packet Drop rate, Read/Write ops per sec |

## Standard Operating Procedures

List of Cisco UCS SOPs executed by NTT DATA:

| | |
|---|---|
| Hardware Failure SOP | NTT DATA will execute the SOP for Memory module Failures, BMC reset, Power supply failures, fabric extender failures, SFP failures, slot failure, fabric extender failure, fabric interconnect failure, Blade Failure |
| Server Booting SOP | NTT DATA will check booting sequence changes, improper service profile configuration, blade hardware problem, guest OS issue, Blade down |
| Server availability SOP | NTT DATA will execute the SOP to identify guest OS issue, Invalid network configuration on guest OS, invalid network configuration on UCS, Invalid network configuration issue on network devices, Spanning tree issue between UCS and uplink network devices |
| Inventory of a Blade from CLI | NTT DATA will get hardware details for inventory purpose / to get RMA |
| VSAN SOPs | NTT DATA will check SAN connectivity, NPIV issues, vSAN configuration issues |
| Authentication SOPs | NTT DATA will authenticate failures, user access issues |
| Storage Status (up/down) | NTT DATA will check and validate up/down status of the Storage Devices. If the device offline is due to hardware failure or malfunction, NTT DATA will collect diagnostic logs and tests will be performed for the problematic storage devices, with the help of Storage Vendor and after the approval of the Customer. Health Check will be performed for Storage Devices which are alerted but not down All these tasks will either be performed from the Storage Console or Management Station |
| Shutdown (unexpected) | NTT DATA will validate the logs to identify if the sever shutdown is unexpected |
| Server in hung state | NTT DATA will try to gather diagnostics logs or system logs if it is permissible for Non responding or hung Storage devices, perform initial analysis and further follow up with the Storage Vendor to analyze, isolate and bring back the server online. These tasks can be performed either from the Storage Console or the Management Station |
| Memory utilization alert | NTT DATA will validate the high utilization, and identify the process causing high memory utilization |
| Processor utilization alert | NTT DATA will validate the high utilization, and identify the process causing high processor utilization |

| | |
|---|---|
| Disk space alert | NTT DATA will validate the alert by logging into the server and identifying the LUNs/folders which are occupying high disk space, run SOP to free-up disk space and notify the customer |
| VMware Hypervisor Services not Running | NTT DATA will validate the services which are not running and starting them if required |
| VMware Hypervisor Exiting Host | NTT DATA will analyze logs in case of VMware Hypervisor Host exiting abnormally (hanging or crashing or reboot) |

## Move, Add and Changes and Service Requests

Customer can create ticket and assign to NTT DATA Services team for executing following MAC requests:

- Configurations for administrative access, call home, AAA, TACACS, LDAP
- Service profile management (creation / modification / deletion / assignment)
- Move, Add and Changes for VLAN and VSAN management, authentication configurations, user and DNS management
- User management: create / modify / delete users, groups and user permissions

## Preventive maintenance

Following preventive measure will be under taken on a periodic basis to prevent outages.

- Software and firmware upgrades as needed
- Ensure optimal service levels for applications hosted within the Cisco UCS environment with a complete view of underlying infrastructure and application performance.
- Archiving of events logs for historical analysis or investigation purpose
- Perform trend analysis on key performance data and review SLAs
- Periodic backups and checks on server configuration
- Patch management for VMware Hypervisors
- Monthly Storage Reclamation
- Storage Array Firmware Update Deployment

**Monthly Storage Reclamation**

Every month, reclamation of storage will take place on an as-needed basis or on customer request, after a review by NTT DATA of active and inactive LUNs. Migration and reclamation of storage will be conducted after approval from customer. The following steps are performed in the monthly storage reclamation process.

Scope:

- All storage (LUNs) within storage arrays in customer environment that are agreed upon at the start of engagement

NTT DATA Responsibility:

- Review active and inactive LUNs, and capacity used – prepare overview report
- Follow change management process to initiate change request to kick-off storage reclamation
- Start storage reclamation by migrating data to and from LUNs
- Reassign LUNs to storage ports and servers

Customer Responsibility:

- Approve change request for optimizing storage
- Provide time window for reclamation and send communication to affected parties

Deliverables:

- Generate report that shows updated assignment of LUN or data or servers for storage arrays

**Storage Array Firmware Update Deployment**

OS version updates for storage array are performed on an as-needed basis or on customer request, but only on approval by customer. This procedure is performed only for in-place or non-destructive updates.

Scope:

- All storage arrays in customer environment that was agreed upon at start of engagement

NTT DATA Responsibility:

- Verify availability and help ensure requirements for firmware update or upgrade are met
- Follow change management process to initiate change request to deploy updates. Confirm operational window for service delivery.
- Update or upgrade controllers for storage arrays
- Validate that controllers have rebooted and are operational
- Execute CIFS and NFS mounts

## Preventive maintenance schedules

| Maintenance activity | Frequency |
|---|---|
| Patch scan | Weekly |
| Patch management (install) | Monthly |

## Preventive health checks

NTT DATA will run scheduled health checks on UCS, VMware hypervisor and storage once every thirty (30) days and will escalate critical issues to the customer and present a possible solution. Based on the approval from the customer, NTT DATA will attempt to resolve the issue.

## Out-of-scope services

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered on a T&M basis, in conjunction with Cloud Operations Management and Monitoring and Remediation service levels.

Out-of-scope for monitoring:
Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-scope for Standard Operating Procedure – for Cloud Monitoring and Remediation only

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-scope for problem management – for Cloud Monitoring and Remediation only

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-scope for patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA services team
- Genuine windows license is responsibility of customer.

Out-of-scope for Anti-Virus definition updates

- Re-installation of AV software
- License management is responsibility of customer
- Virus scan and removal on desktops and servers

Out-of-scope for Service Request

Some SRs are out of scope. SRs are requests that originate outside of the scope of disruption of services. Examples of these SRs are:

- Design of UCS to business processes requirements
- New device deployments
- Provisioning, configurations and migrations
- New site architecture - design or re-design
- Migrations of UCS network infrastructure
- Remote office or branch office setup
- Setup of new firewall rules or routing table modifications
- DNS changes and IP allocations
- Network topology changes
- VMware hypervisor version upgrades
- New VMware hypervisor installation and configuration
- Manage storage repositories (SR) - resize, destroy, convert local fiber channel SR to shared SR, move virtual disk images between SRs, reclaim space on snapshots, deletion, etc.
- Backup and restore VMware ESX hosts and VMs, including their metadata
- Setup of new internal replication process
- Migration of data between LUNs
- Setup of new LUNs and RAID groups
- Setup of file archiving policies
- Setup a LUN and assign a storage port
- Swap out hard-drives, re-shelve drive enclosures, or re-wire storage array to SAN or back-end storage (these are typically performed by SP or end-client directly)
- Migrate arrays (data)
- Implement or migrate storage
- SAN and NAS architectural design work

Any items not explicitly covered within this document are considered out of scope.

## Section 17: vCAC Services

### Supported Technologies & Devices

| | | |
|---|---|---|
| **VMware** | vCAC (Identity Server, vCAC appliance, IaaS server) | Versions 6.0 & above. |
| **VMware** | VCO | Versions 5.5 & above |
| **Microsoft SQL** | MSSQL | Versions 2008 & above |
| **Postgress SQL** | PostgressSQL | |

### Key Monitoring Parameters

NTT DATA monitors the VMware vCAC server infrastructure utilizing using standard Windows WMI or SNMP data collection. NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform SOPs or advanced trouble-shooting services.

| WINDOWS OPERATING SYSTEM |
|---|
| **Server availability:** up/down<br>**Server health:** (CPU, memory and disk utilization)<br>**Windows event logs:** critical application, system logs<br>**Server hardware monitoring:** disk, memory modules, chassis temperature |
| **LINUX OPERATING SYSTEM** |
| **Server availability:** up/down<br>**Server health:** (CPU, memory and disk utilization)<br>**Linux interfaces**: up/down<br>**Logs**: critical logs<br>**Server hardware monitoring:** disk, memory modules, chassis temperature |
| **DEVICE HEALTH** |
| Device/network/cluster availability |
| Device health (CPU and memory and disk utilization) |
| **SERVER THROUGHPUT METRICS** |
| Number of logical connections, logins/sec, logouts /sec, active transactions. transactions /sec, queued jobs , failed jobs and job success rate, open connections count |
| **SQL SERVER CACHE METRICS** |
| Cache hit ratio (MSSQL), cache objects, cache pages, and cache objects in use. |
| **SERVER DISK METRICS** |

| SQL SERVER RESOURCE UTILIZATION METRICS |
|---|
| Data file size , replication transaction rate , average and total latch wait time , number of replication pending transactions, user connections |
| **WINDOWS SERVICES MONITORING** |
| SQL Server , Agent service , integrations services, Reporting services Analysis services, FULL text services |
| **SQL SERVER HIGH AVAILABILITY MONITORING** |
| Monitors to track Replication latency , Mirror synchronization , lag in log shipping , Cluster availability and failover/fail back |
| **IAAS SERVER** |
| web service\bytes total/sec<br>web service\total method requests/sec<br>web service\current connections<br>web service cache\file cache hits %<br>web service cache\kernel:uri cache flushes<br>web service cache\kernel:uri cache misses<br>web service cache\kernel:uri cache hits %<br>active server pages\request wait time<br>active server pages\requests queued<br>active server pages\transactions/sec |

| |
|---|
| Average disk reads/writes/transfers in bytes, disk queue length, disk read/write queue, data space of DB, |
| **SQL SERVER LOG METRICS** |
| Log file(s) size, log flush wait time, log flush waits/sec, log flushes/sec, log growth and shrink rate |

## Standard Operating Procedures (SOPs)

List of SOPs executed by NTT DATA for issues with vCAC services (may include additional SOPs):

| | |
|---|---|
| **Server Availability (Up/Down)** | NTT DATA will run diagnostics to check status of problematic server or appliance from a different server in same network to eliminate any LAN/WAN connectivity issues |
| **Server Shutdown (Unexpected) Alerts** | NTT DATA will validate event logs to identify if server shutdown is unexpected |
| **Server In Hung State** | Restart server if it is hung (through DRAC / ILO) |
| **Memory Utilization Alert** | Validate high utilization, and identify process causing high memory utilization |
| **Processor Utilization Alert** | Validate high utilization, and identify process causing high processor utilization |
| **Disk Space Alert** | Validate alert by (a) login to server and identify folders that occupy high disk space (b) run disk clean-up to free-up disk space, and (c) notify customer of folders that occupy high disk space |
| **Hardware Error** | Run hardware diagnostic check to validate hardware fault |
| **Windows Event Log (Critical)** | Execute set of instructions when specific critical event occurs |
| **Site And Server Status** | Open site link from inside the server and outside the server to validate site status. Restart services to eliminate any hung issues. |
| **Port Status** | Validate webserver process and port access issues |
| **Database Log File Is 100% Full** | Verify possible reason for log file full and run SOP to backup and shrink log file, or increase space, or move file to a different drive if required |
| **Temp DB Is Full** | Validate cause of Temp DB full and run SOP by shrinking or increasing temp DB, or moving Temp DB to a different drive based on situation |
| **Cluster Failover Alerts** | Find out reasons for failover and fix them. Keep secondary server ready for future use. |
| **vCAC login failure** | NTT DATA will log in to the Postgress Database and validate the hstore extension. And restarts the vCAC. |
| **vCAC unable to process worfklow** | NTT DATA with restart the vCAC agent services. |

## Move, Add and Changes (MAC) and Service Requests (SRs)

Customer can create ticket and assign to NTT DATA Services team for executing following SRs:

- Service catalogue and Blueprint management activities
- Add/Delete/Modify Tenants
- Add blueprints to service catalogues
- User creation and edits
- Password changes
- Workflow management via VCO

## Preventive Maintenance Scope

- Validate Anti-Virus definition updates

## Preventive Health Checks

NTT DATA will run scheduled health checks on VMware vCAC services to check for possible critical issues. For critical issues, NTT DATA will escalate issue to Customer and propose a possible solution. On receiving an approval from Customer, NTT DATA will attempt to resolve the issue.

## Out of Scope Services

The following list of service activities are not within scope of Operations Management and Monitoring and Remediation for vCAC services. These activities can be delivered on a time & material basis, in conjunction with Cloud Operations Management and Monitoring and Remediation service levels.

Out-of-Scope for Monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-Scope for Standard Operating Procedure (SOPs) – for Monitoring and Remediation only

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-Scope for Problem Management – for Monitoring and Remediation only

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-Scope for Patch Management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA services team
- Genuine windows license is responsibility of customer.

Out-of-Scope for Antivirus Definition Updates

- Re-installation of AV software
- License management is responsibility of customer
- Virus scan and removal on desktops and servers

Out-of-Scope for Service Requests

- Support for advance service designer
- Creation of new workflows
- Third party integrations for workflow management
- Integrations with other software & API's

## Section 18: Openstack Services

### Supported components

| | |
|---|---|
| **Openstack** | OpenStack Compute, Controller, Nova, Swift, Glacier, Glance, Cinder, Neutron, Keystone, Horizon, Heat |
| **Database** | RabbitMQ, mySQL (MariaDB), MongoDB |
| **Other services** | Membase, memcache, Apache, PaceMaker, Cronosync |
| **Operating systems** | RHEL, Ubuntu, KVM |

### Key monitoring parameters

NTT DATA monitors the Openstack infrastructure using standard SNMP and syslog. NTT DATA platform enables NTT DATA staff to securely and remotely access the monitored devices in order to perform standard operating procedures (SOPs) or advanced trouble-shooting services.

| Openstack services monitored |
|---|
| Openstack neutron services |
| Openstack ceilometer services |
| Openstack cinder services |
| Openstack image services |
| Openstack heat services |
| Openstack identity services |
| Openstack nova services |
| Openstack object storage (swift) services |
| Openstack vSwitch services |

| Linux operating system |
|---|
| Server availability: up/down |
| Server health: CPU, memory and disk utilization |
| Linux interfaces: up/down |
| Logs: critical logs |
| Server hardware monitoring: disk, memory modules, chassis temperature etc. |

| Apache Tomcat |
|---|
| Response metrics( HTTP response time, HTTP response value, URL monitoring); server metrics (busy workers, idle workers, SSL certificate expiration, keep alive count, DNS lookup count); throughput metrics (requests served per minute, bytes served per minute, bytes served per request, total bytes, total accesses, number of concurrent connections); website monitoring (synthetic |

| MongoDB |
|---|
| Uptime, activeclients, memory, lock, connections, heapusage, pagefaults, btree, networkrequests, currentqueue, opcounters, replicaprimary, replicationlag, replicationstate, journalcommitsinwl, size, asserts, backgroundavgflush, cursors, journaledstatus, the status of mongodb process, memory and cpu usage of mongodb process, the database connection pool usage, iostat(page faults), flush, replication, op counters, queues, oplogsize, monitor the 24K namespace limit - if we set 10GB oplogsize then 10GB of local files will be created in the /data folder, if we set oplogsize then data freshly has to build; to check oplogsize db.printreplicationinfo(). |

| Membase |
|---|
| Uptime, CurrentItems, CurrentConnections, MemoryUsed, OpsPersec, GetsPersec, SetsPersec, DeletesPersec, HitsPersec, MissesPersec, EvictionsPersec, ReadBytesPersec, WrittenBytesPersec, ConnectionsPersec, CASHitsPersec, CASMissesPersec, TempOOPersec, DiskReadsPersec, DiskCreatesPersec, DiskUpdatedPersec, HighWatermark, LowWatermark, vBuckets, vBucketItems, vBucketUserDataInRAM, vBucketMetaDataInRAM, vBucketNewItemsPersec, |

| |
|---|
| transactions) - mimics HTTP/SSL transactions and alerts on return codes, response times and page content (presence or absence). Checks the certificate integrity, validity period, etc. while validating a given user access. |

| |
|---|
| vBucketEjectionsPersec, DiskWriteQueue, DiskQueueItems, PendingQueueFillRate, PendingQueueDrainRate, CacheMissRatio, GetHitPercent, FillPercent, AvgItemSize, ResidentItemRatio |

| Memcache |
|---|
| Uptime, CurrentItems, CurrentConnections, MemoryUsed, OpsPersec, GetsPersec, SetsPersec, DeletesPersec, HitsPersec, MissesPersec, EvictionsPersec, ReadBytesPersec, WrittenBytesPersec, ConnectionsPersec, CASHitsPersec, CASMissesPersec, CachBadvalPersec, TempOOMPersec, DiskReadsPersec, CacheMissRatio, GetHitPercent, FillPercent, AvgItemSize, ResidentItemRatio |

| MySQL (MariaDB) |
|---|
| Device health – availability, cpu, memory, disk utilization, network availability, connection statistics, Key(index) efficiency statistics, thread usage statistics, replication statistics, process monitoring – mysqld process, cluster availability monitoring, request statistics, query statistics, table statistics, query cache hitrate, IO performance statistics, log monitoring etc. |

| Other services monitored |
|---|
| RabbitMQ services |
| PaceMaker services |
| Cronosync services |

## Standard Operating Procedures

List of SOP's executed by NTT DATA for issues with Openstack services

| | |
|---|---|
| **Known errors** | Look in relevant logs -- this includes the /var/log/nova logs, the /var/log/glance logs (if related to images), as well as /var/log/keystone logs. |
| **Authentication issues** | Drill down into specific service types using commands. For example, to show adminURL for compute service type in all regions use command "keystone catalog" |
| **Misconfigured endpoints** | When launching instances, specify a security group. If none specified, use security group named default. If network issues, then it may prevent access of cloud instances. |
| **Cannot ping or SSH to an instance** | In multi-host environment, help ensure there's a nova-api and a nova-network node running on nova-compute host. |
| **Instance fails to download meta information** | Majority of OpenStack services are web services and responses from services are well defined in /var/log/httpd/error.log leverage to troubleshoot. |

| | |
|---|---|
| **Error codes such as 401, 403, 500** | NTT DATA will execute SOP for memory module failures, power supply failures, fabric extender failures, SFP failures, slot failure, fabric extender failure, fabric interconnect failure, blade failure |
| **Hardware failure** | NTT DATA will check booting sequence changes, improper service profile configuration, blade hardware problem, guest OS issue, blade down |
| **Server booting problems** | NTT DATA will execute SOP to identify OS issue, Invalid network configuration, invalid network configuration on compute systems, invalid network configuration issue on network devices, spanning tree issue between compute systems and uplink network devices |
| **Server availability issues** | NTT DATA will validate logs to identify if server shutdown is unexpected |
| **Shutdown (unexpected)** | NTT DATA will (a) gather diagnostics logs or system logs for non-responding or hung storage devices (b) perform initial analysis and further follow up with storage vendor to analyze, isolate, and bring server back online. These tasks can be performed from storage console or management station. |
| **Server in hung state** | NTT DATA will validate high utilization, and identify process causing high memory utilization |
| **Memory utilization alert** | NTT DATA will validate high utilization, and identify process causing high processor utilization |
| **Processor utilization alert** | NTT DATA will validate alert by (a) login into server and identifying LUN's/folders that occupy high disk space, (b) run SOP to free-up disk space and (c) notify customer |

## Move, Add and Changes and Service Requests

Following are some examples of MACs:

- User management (creation/deletion/update)
- OpenStack project management (creation / modification / deletion / assignment)
- Snapshot management (creation/deletion)

Following are some examples of SRs:

- Security services for instances
- Tenant data privacy
- Database access control
- Convert between image formats
- Provision virtual machines (up to 5 VMs per month – additional VMs on a T&M basis)

## Preventive maintenance scope

- Validate Anti-Virus definition updates for supported AV products (customer provided)

## Preventive maintenance schedules

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |

## Preventive health checks

NTT DATA will run scheduled health checks on Openstack environment to check for possible critical issues. For critical issues, NTT DATA will escalate issue to Customer and propose a possible solution. On receiving an approval from Customer, NTT DATA will attempt to resolve the issue.

## Out-of-scope activities

The following list of service activities are not within scope of Operations Management and Monitoring and Remediation for Openstack environment. These activities can be delivered on a time & material basis, in conjunction with Cloud Operations Management and Monitoring and Remediation service levels.

Out-of-Scope for Monitoring:

- Customizations to monitoring templates are subject to review and acceptance by NTT DATA.

Out-of-Scope for Standard Operating Procedure (SOPs) – For Monitoring and Remediation only

- An alert with no SOPs associated with it will be escalated as per escalation matrix

Out-of-Scope for Problem Management – For Monitoring and Remediation only

- Troubleshooting and fix, vendor management and escalation, and root cause analysis on devices are out of scope

Out-of-Scope for Patch Management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA services team
- Genuine licenses for various Openstack components is responsibility of customer.

Out-of-Scope for Service Requests

- Create images
- Modify images
- Integrate identity with LDAP
- Perform major upgrades outside of agreed architecture
- Addition or removal of OpenStack services outside of standard or agreed architecture
- Addition or migration of Nova
- Migration of Cinder volumes
- Design of OpenStack to business processes requirements
- New device deployments
- Provisioning, configurations and migrations
- New site architecture - design or re-design
- Migrations of OpenStack infrastructure
- Remote office or branch office setup
- Setup of new firewall rules or routing table modifications
- DNS changes and IP allocations
- Network topology changes
- Backup and restore hypervisors, hosts, and VMs, including their metadata
- Setup of new internal replication process
- Setup of file archiving policies
- Swap out hard-drives, re-shelve drive enclosures, or re-wire of servers (typically performed by end-client)

Any items not explicitly covered within this document are considered out of scope.

## Section 19: Server Hardware Management

Note: Only Cloud Operations Management is available. Cloud Monitoring and Remediation is not supported.

### Supported environments

| | | |
|---|---|---|
| **Brand or Vendor** | HP | Blade servers; rack servers; blade chassis |
| | Dell | Blade servers; rack servers (e.g. Dell PowerEdge, etc.,); blade chassis<br>Dell VRTX models – blades & chassis |
| | Cisco | Cisco server hardware (e.g. UCS servers); blade chassis. |

### Key monitoring parameters

NTT DATA monitors server hardware utilizing standard IPMI, iLO, serial console, and/or other out-of-band capabilities available for that server hardware for remote monitoring and management. The NTT DATA platform enables remote access in a secure fashion to the monitored devices in order to perform standard operating procedures (SOPs) or advanced troubleshooting services.

- **Caveat:** Without access and control of the OS running on the server hardware, it is a difficult task for NTT DATA to comprehensively monitor all performance, capacity, and availability metrics for the server hardware. While remote access and remote control mechanisms such as IPMI, iLO, OOB, serial console and/or other methods alleviate the situation, they usually don't go all the way and are not entirely comprehensive in their capabilities for monitoring, access and control of the server hardware.
- **Assumptions:** For server hardware running Windows or Linux OS, NTT DATA will seek approval of the Customer in order to install NTT DATA Portal agents on the OS to enable granular monitoring and reporting of various failures in the server hardware. For server hardware running VMware, NTT DATA will seek access to vCenter for CIM information, to enable monitoring and reporting on the server hardware.

| Server Hardware |
|---|
| **Server Hardware Monitoring:** Disk, Memory Modules, Chassis Temperature |

### Standard Operating Procedures

Not Applicable because Cloud Monitoring and Remediation service level is out of scope

### Move, Add and Changes and Service Requests

Service Requests are out of scope

### Preventive maintenance scope

- BIOS firmware upgrades

## Preventive maintenance schedules

Preventive maintenance activities will be performed on-demand through Service Request initiated by the customer.

## Preventive health checks

Not Applicable

## Out-of-scope activities

Cloud Monitoring and Remediation service level is not supported. The following list of service activities are not within scope of Cloud Operations Management. These activities can be delivered upon request in conjunction with Operations Management package, on a T&M basis.

Out-of-scope monitoring:

- Customizations to the monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope Service Requests

- All Service Requests are out of scope

Any items not explicitly covered within this document are considered out of scope.

## Section 20: Dell Hybrid Cloud System for Microsoft

Note: Only Cloud Operations Management is available. Cloud Monitoring and Remediation is not supported

### Supported environments

| | |
|---|---|
| **Hardware** | Dell PowerEdge C6320, R730 |
| **Virtualization** | Microsoft Hyper-v |
| **Network** | Dell Force 10 – S4048 |
| **Storage** | Dell PowerVault MD |
| **Management Tools** | Microsoft SCVMM, SCOM, WSUS, Azure Pack |

### Key monitoring parameters

NTT DATA monitors the environment using SNMP, syslog, and other means. Comprehensive monitoring templates help ensure that all aspects of the environment are monitored for performance, availability, and capacity. The following metrics are monitored:

| Hardware Monitoring |
|---|
| Array Controller |
| Chassis |
| Power supply units |
| Hard Drive status |
| Memory Status DIMM |
| Processor Current Status |
| System Board BIOS Status |
| System Board Fan 1 Speed |
| Voltage Probe Status |
| **Hyper-V Monitoring** |
| Memory_availablebytes |
| Memory_averagepressure |
| Memory_HypervisorPartitionDepositedPages |
| Memory_HypervisorPartitionValue2MGPApages |
| CPU Utilization |
| LogicalProcessorPercentGuestRunTime |
| LogicalProcessorPercentHypervisorRunTime |
| LogicalProcessorPercentIdleTime |
| LogicalProcessorPercentTotalRunTime |
| VMHealthSummary |
| CurrentDiskQueueLength |
| Storage_DiskBytesPersec |
| Storage_DiskTransfersPersec |
| Storage_ErrorCount |

| SAN Monitoring |
|---|
| Build Number |
| Battery Status |
| Cache Status |
| Controller Status |
| Count of Servers |
| Count of Volumes |
| Device Count |
| Disk Folder Status |
| Disk Health |
| Disk Status |
| Enclosure Audible Alarm Status |
| Enclosure Fan Status |
| Enclosure Module Status |
| Enclosure Power Status |
| Enclosure Status |
| Enclosure Temperature Status |
| Fan Status |
| Global Status |
| Managed Server Status |
| Monitored UPS Status |
| Number of Disks |
| Power Status |
| Replay Count |

| |
|---|
| Network_VirtualSwitchBytesPersec |
| Network_Interface_TrafficIn |
| Network_Interface_TrafficOut |
| Network_Interface_TrafficTotal |
| Network_Interface_OffloadedConnections |
| Network_Interface_OutputQueueLength |
| Network_Interface_PacketsOutboundDiscarded |
| Network_Interface_PacketsOutboundErrors |
| Network_Interface_PacketsReceivedDiscarded |
| Network_Interface_PacketsReceivedErrors |
| Network Interface Utilization |

| |
|---|
| Storage Center Status |
| Temperature Status |
| Volume Status |
| **Network Monitoring** |
| CPU Utilization |
| Memory Utilization |
| Stack unit status |
| System Info |
| Unit fan status |
| Unit info |
| Unit info |
| Unit power supply |
| Unit temperature |
| Interface error and discard rate |
| Interface Status |
| Interface traffic |
| Interface utilization |

## Standard Operating Procedures

List of SOPs executed by NTT DATA for Dell Hybrid Cloud System for Microsoft (may include additional SOPs):

| | |
|---|---|
| **Hardware Failure SOP** | NTT DATA will execute SOP for memory module failures, power supply failures, slot failure, fan failures |
| **Server Booting SOP** | NTT DATA will check booting sequence changes, hardware problem, Hypervisor issue, server down |
| **Server Availability SOP** | NTT DATA will execute SOP to identify guest OS issue, invalid network configuration on guest OS, invalid network configuration on hyper-v, invalid network configuration issue on network devices |
| **Storage Status (Up/Down)** | NTT DATA will check and validate Up/Down status of storage devices. If device is offline is due to hardware failure or malfunction, NTT DATA will collect diagnostic logs and tests will be performed for problematic storage devices, with help of storage vendor and after approval of Customer. Health checks will be performed for storage devices that send alerts, but are not down. All these tasks will either be performed from storage console or management station. |
| **Shutdown (Unexpected)** | NTT DATA will validate logs to identify if server shutdown was unexpected |
| **Server in Hung State** | NTT DATA will attempt to gather diagnostics logs or system logs for non-responding or hung storage devices. It will perform initial analysis and further follow up with storage vendor to analyze, isolate, and bring back server online. These tasks can be performed either from storage console or management station. |
| **Memory Utilization Alert** | NTT DATA will validate high utilization, and identify process causing high memory utilization |
| **Processor Utilization Alert** | NTT DATA will validate high utilization, and identify process causing high processor utilization |

| | |
|---|---|
| **Disk Space Alert** | NTT DATA will validate alert by logging into server and identifying LUN's or folders that occupy high disk space. It will then run SOP to free-up disk space and notify customer. |
| **Microsoft Hyper-v Host Not Responding/Reboot (unexpected)** | NTT DATA will analyze logs in case of Hyper-v Host that exits abnormally (hanging or crashing or reboot) |

## Move, Add and Changes and Service Requests

Following is an example of SRs and MACs:

- Configurations for administrative access, call home, AAA, TACACS, LDAP
- Service profile management (creation / modification / deletion / assignment)
- Move, Add and Changes (MAC) for SAN management, authentication configurations, and user
- User management: create / modify / delete users, groups and user permissions

## Preventive maintenance scope

- Software and firmware upgrades as needed
- Ensure optimal service levels for applications hosted within the environment with a complete view of underlying infrastructure and application performance.
- Archiving of events logs for historical analysis or investigation purpose
- Perform trend analysis on key performance data and review SLAs
- Microsoft Hyper-V patch management

## Preventive maintenance schedules

Servers

| Maintenance activity | Frequency |
|---|---|
| Anti-Virus / Antimalware | Daily |
| Patch scan | Weekly |
| Patch management (install) | Monthly |

## Preventive health checks

NTT DATA will run scheduled health checks on hardware, Microsoft Hyper-V, network and storage once every thirty (30) days and will escalate critical issues to the customer and present a possible solution. Based on the approval from customer, NTT DATA will attempt to resolve the issue.

## Out-of-scope services

The following list of service activities are not within scope of Cloud Operations Management and Cloud Monitoring and Remediation. These activities can be delivered upon request in conjunction with Cloud Operations Management and Cloud Monitoring and Remediation packages on a T&M basis.

Out-of-scope monitoring:

- Customizations to the monitoring templates are subject to review and acceptance by NTT DATA

Out-of-scope patch management

- Service packs, updates, drivers, classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a new request to NTT DATA
- It is the responsibility of the customer to have genuine software, hardware, and application licenses in their environment

Out-of-scope Antivirus definition updates

- Re-installation of Antivirus software
- License management is the responsibility of the customer
- NTT DATA by default will not schedule anti-virus scan on desktops and servers

Out-of-scope Service Requests

- Service requests that originate outside of the services scope and may cause disruption of services. Examples of these SRs are below.
- Design of Dell Hybrid Cloud System for Microsoft to business processes requirements
- New device deployments
- Provisioning, configurations and migrations
- New site architecture - design or re-design
- Migrations of network infrastructure
- Remote office or branch office setup
- Setup of new firewall rules or routing table modifications
- DNS changes and IP allocations
- Network topology changes
- Microsoft Hypervisor version upgrades
- New hypervisor installation and configuration
- Manage storage repositories (SR) - resize, destroy, move virtual disk images between SRs, reclaim space on snapshots, deletion, etc.
- Backup and restore Hyper-v hosts and VMs, including their metadata
- Setup of new internal replication process
- Setup of new LUNs and RAID groups
- Setup a LUN and assign a storage port
- Swap out hard-drives, re-shelve drive enclosures, or re-wire storage array to SAN or back-end storage (these are typically performed by customer directly)
- Migrate arrays (data)
- Implement or migrate storage

Any items not explicitly covered within this document are considered out of scope.

## Appendix C

# Business Associate Agreement for NTT DATA Managed Cloud Services

This Business Associate Agreement is hereby effective upon your (a) execution of a Solution Description or an Order Form; (b) acceptance of the Cloud Solutions Agreement terms pursuant to an online or offline process; (c) accessing or using the Solution; or (d) acceptance of terms between you and a reseller that reference the Cloud Solutions Agreement, if you purchased through a reseller ("Effective Date"). This Business Associate Agreement is made between you and NTT DATA. "You," "your" or "Customer" means the end-user entity which you represent, and which may be further identified in the applicable Solution Description, Order Form, End User Acknowledgment Form or online order process, and includes any of your affiliates that expressly agree to, or are otherwise legally bound by, this Agreement. "NTT DATA" means NTT DATA Services LLC, on behalf of itself and its suppliers and licensors, or the NTT DATA entity identified on your Solution Description or Order Form and includes any NTT DATA affiliate with which you place an order for the Solution.

The parties desire through this Business Associate Agreement to supplement the terms of the Cloud Solutions Agreement between Customer and NTT DATA to address the requirements of the Health Insurance Portability and Accountability Act of 1996, as it may be amended from time to time, and its implementing regulations, as amended and supplemented by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, as it may be amended from time to time, and its implementing regulation (collectively, "HIPAA"). This Business Associate Agreement replaces any earlier Business Associate Agreement(s) entered into between the parties, and, as of the Effective Date, those Business Associate Agreements shall have no further effect. In the event that NTT DATA utilizes a third party for the Cloud Solutions, NTT DATA reserves the right to replace or supplement this BAA with additional terms and conditions.

**1. Definitions.**

(a) "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules set forth at 45 CFR Part 160 and Part 164, as each is amended from time to time. The "HIPAA Privacy Rule" is the Privacy of Individually Identifiable Health Information set forth at 45 CFR Part 160 and Part 164 (Subparts A and E) as amended from time to time. The "HIPAA Security Rule" is the HIPAA Security Standards for the Protection of Electronic Protected Health Information set forth at 45 CFR Part 160 and Part 164 (Subparts A & C) as amended from time to time. The "HIPAA Breach Notification Rule" is the Notification in the Case of Breach of Unsecured Protected Health Information as set forth at 45 CFR Part 164 (Subpart D).

(b) "Electronic PHI" or "ePHI" means PHI that is transmitted or maintained in Electronic Media.

(c) "Protected Health Information" or "PHI" shall mean Protected Health Information as defined in 45 CFR § 160.103 and is limited to the Protected Health Information received from, or received, maintained, created or transmitted on behalf of, Customer by NTT DATA within the scope of the Solution by NTT DATA.

(d) "Solution" shall have the same definition as in the Cloud Solutions Agreement.

(e) “Unsuccessful Security Incident Attempts” shall mean, without limitation pings and other broadcast attacks on Customer’s firewall, port scans, unsuccessful log-on attempts, denial of service attacks and any combination of the above that in each case do not result in any unauthorized access, acquisition, use or disclosure of PHI.

(f) Capitalized terms not otherwise defined in this Business Associate Agreement shall have the meanings given to them in the HIPAA Rules and those meanings are incorporated herein by reference.

**2. Obligations of NTT DATA.**

To the extent (if any) that NTT DATA receives from, or receives, creates, transmits, maintains or receives on behalf of, Customer any Protected Health Information, including ePHI, when performing the Solution, NTT DATA will maintain the privacy and security of such PHI as required by this Business Associate Agreement. Subject to the foregoing limitations, NTT DATA agrees:

(a) not to use or further disclose PHI other than to perform the Solution and its obligations under the agreement that governs the provision and use of the Solutions and as expressly permitted or required by this Business Associate Agreement or Required by Law and to the extent NTT DATA in performing the Solutions carries out the Customer’s obligations under the HIPAA Privacy Rule, NTT DATA will comply with the requirements of the HIPAA Privacy Rule that apply to Customer in the performance of those obligations;

(b) to use reasonable and appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided by this Business Associate Agreement and, with respect to Electronic PHI, comply with the applicable requirements of the HIPAA Security Rule;

(c) to report to Customer any use or disclosure of PHI not permitted by this Business Associate Agreement or any Security Incident of which NTT DATA becomes aware, other than Unsuccessful Security Incident Attempts, the ongoing existence and occurrence of which NTT DATA hereby provides notice to Customer;

(d) to report to Customer, following discovery and without unreasonable delay, any Breach of Unsecured Protected Health Information as required by the HIPAA Breach Notification Rule;

(e) in accordance with 45 CFR § 164.502(e)(1)(ii) and 45 CFR § 164.308(b)(2), help ensure that any subcontractors of NTT DATA that create, receive, maintain or transmit PHI on behalf of NTT DATA agree to substantially the same restrictions and conditions that apply to NTT DATA with respect to that PHI in this Business Associate Agreement;

(f) to the extent (if any) that NTT DATA maintains a Designated Record Set for Customer, to make available PHI maintained by NTT DATA in a Designated Record Set to Customer as required for Customer to comply with its obligation to give an Individual the right of access as set forth in 45 CFR § 164.524. Customer shall reimburse NTT DATA for the applicable reasonable costs incurred by NTT DATA in complying with such request. The provision of access to the Individual’s PHI and any denials of access to the PHI shall be the sole responsibility of Customer.

(g) to the extent (if any) that NTT DATA maintains a Designated Record Set for Customer, to make available PHI maintained by NTT DATA in a Designated Record Set to Customer as required for Customer to comply with its obligation to amend PHI as set forth in 45 CFR § 164.526. The amendment of an Individual’s PHI and all decisions related thereto shall be the sole responsibility of Customer;

(h) to make available to Customer information regarding disclosures made by NTT DATA for which an accounting is required under 45 CFR § 164.528 so Customer can meet its requirements to provide an accounting to an individual in accordance with 45 CFR § 164.528; and

(i) to make its internal practices, books and records relating to the HIPAA Rules available to the Secretary of Health and Human Services for purposes of determining Customer and NTT DATA's compliance with the HIPAA Rules.

**3. Other Authorized Uses and Disclosures of PHI.**

In addition to any other uses and disclosures authorized or required by this Business Associate Agreement, NTT DATA is authorized to:

(a) use and disclose PHI as necessary for the NTT DATA to perform the Solution and its obligations under the Cloud Solutions Agreement;

(b) use and disclose, if necessary, PHI for NTT DATA's proper management and administration or to carry out NTT DATA's legal responsibilities; provided that the disclosure is Required by Law or any third party to which NTT DATA discloses PHI under this Section provides reasonable assurances that the PHI will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to that third party. NTT DATA will further require that the third party to whom the PHI is disclosed notify the NTT DATA of any breach of confidentiality of that PHI;

(c) use and disclose PHI as necessary to report violations of Law to appropriate Federal and State authorities as permitted by the HIPAA Privacy Rule;

(d) use PHI to provide Data Aggregation services related to Customer's Health Care Operations in accordance with the HIPAA Privacy Rule; and

(e) de-identify PHI in accordance with the HIPAA Privacy Rule and use and disclose that deidentified information for any purpose without restriction or obligation under this Business Associate Agreement.

**4. Customer Obligations.**

In addition to any other obligations set forth in this Business Associate Agreement, Customer agrees:

(a) with respect to any PHI in a Designated Record Set provided by Customer to NTT DATA under this Business Associate Agreement, maintain a separate copy of that PHI if possible, pursuant to which Customer may respond to, and comply with, any requests by Individuals to access or amend that PHI under 45 CFR §§ 164.524 and 164.526 without reliance on NTT DATA or use of any PHI in the possession of NTT DATA;

(b) to not provide NTT DATA any PHI that is subject to any restrictions under 45 CFR § 164.522 or a notice of privacy practice under 45 CFR § 164.520 that prohibits or otherwise limits any use or disclosure of PHI by the NTT DATA permitted under this Business Associate Agreement;

(c) to comply with all applicable HIPAA Rules;

(d) to be solely responsible for deciding to render any PHI on its systems unusable, unreadable, or indecipherable to unauthorized individuals in accordance with the U.S. Department of Health & Human Services guidance

(e) to acknowledge that it is Customer's responsibility to remove or encrypt all data on NTT DATA systems and media components prior to returning them to NTT DATA for any reason including warranty support and in the event such removal or encryption is not feasible, sign up for Dell's Keep Your Hard Drive Service (http://www.dell.com/learn/us/en/555/services/support-services-keep-your-hard-drive) or make other arrangements to retain any drives or memory components that may contain Electronic PHI.

**5. Miscellaneous Provisions.**

(a) Term and Termination. The term of this Business Associate Agreement shall be the same as the term of the Cloud Solutions Agreement. In the event a party determines that the other party is in material breach of this Business Associate Agreement, the non-breaching party shall notify the other party of the breach in writing, and shall provide an opportunity for the breaching party to cure the breach or end the violation within thirty (30) business days of such notification; provided that if the breaching party fails to cure the breach or end the violation within such time period to the satisfaction of the non-breaching party, the non-breaching party shall have the right to immediately terminate this Business Associate Agreement and the Cloud Solutions Agreement upon written notice to the breaching party.

(b) Effect of Termination or Expiration. During the course of Customer's use of the Solution, Customer may download any of its data stored as part of the Solution, including, but not limited to PHI. Within sixty (60) days following the effective date of the expiration or termination of this Business Associate Agreement, NTT DATA shall delete such data from its servers. Notwithstanding the foregoing, in the event that NTT DATA determines in its sole discretion that return or deletion of PHI is not feasible, NTT DATA shall provide written notice to Customer and retain that PHI and extend to that PHI the protections of this Business Associate Agreement and limit further uses and disclosures of that PHI to those purposes that make the return or deletion of the PHI infeasible.

(c) No Third Party Beneficiaries. No provision of this Business Associate Agreement is intended to benefit any person or entity, nor shall any person or entity not a party to this Business Associate Agreement have any right to seek to enforce or recover any right or remedy with respect hereto.

(d) Conflicts. This Business Associate Agreement shall be subject to the terms and conditions of the Cloud Solutions Agreement. If there is a direct conflict between the terms of this Business Associate Agreement and the terms of the Cloud Solutions Agreement with respect to the matters covered in this Agreement, the terms of this Business Associate Agreement shall control. In the event that the meaning or intent of any term or condition of this Business Associate Agreement is ambiguous or otherwise uncertain, those terms and conditions shall be construed to allow both NTT DATA and Customer to comply with HIPAA.

(e) Independent Contractors. The parties are independent contractors. No provision of this Business Associate Agreement will be deemed to create an association, trust, partnership, joint venture or other entity or similar legal relationship between Customer and NTT DATA, or impose a trust, partnership, or fiduciary duty, obligation, or liability on or with respect to such entities.