Empowering business to do more

Schedule document

Disaster Recovery as a Service (DRAAS)

PUBLIC
Node4 limited
01/06/2024

Schedule Document

Disaster Recovery as a Service (DRaaS)

This schedule contains additional terms and conditions, service description and service levels applicable to the Disaster Recovery As A Service (DRAAS) and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy.

1. Overview

The Node4 DRaaS Service enables the Client to replicate virtual machines that are running on a VMware hypervisor ("source platform") so that they can be restarted on the Node4 n4Cloud platform should the source platform become unusable. The source platform may be:

- a Client VMware platform
- the n4Cloud platform running at another data centre (for example, virtual machines running on n4Cloud in DC3, may restart on n4Cloud in DC4).

The service provides the Client with access to a hosted software package which, when configured, will replicate the disks of a virtual machine on the source platform to the n4Cloud platform in a specified site.

The n4Cloud platform is described in a separate service schedule document.

In the event of a disaster, the Client may invoke a "disaster recovery event". When invoked, Node4 will boot the replicated copy of each virtual machine ("standby VMs") on the n4Cloud platform.

The Node4 service provides Clients with a target Recovery Time Objective (RTO) and Recovery Point Objective (RPO). These objectives:

- should be considered as "targets" which are not guaranteed or measured.
- cover the time to make the standby VM ready to be booted, and do not include the time taken to perform infrastructure tasks outside of the recovery software, such as booting the operating system in the standby VMs.
- may be affected if a large number of virtual machines (for a single Client or multiple Clients) experience a "disaster recovery event" at the same time.
- do not include any time involved to 'invoke' the disaster recovery process such as placing a call to the Node4 Service Desk.

All replicated virtual machines are provided a journal of historic checkpoints to recover from taken approximately every five seconds. The number of checkpoints is equal to either one day's history or 75% of the size of the source virtual machine.

The service is designed to recover the virtual machine image and additional time may be required for applications such as Microsoft SQL Server to become operational. Whilst the software does replicate applications as part of the virtual machine image, the service cannot guarantee that such applications will become operational again, and so it is strongly recommended that the Client performs disaster recovery tests to maximise the probability that service can be restored.

The service is designed to perform replication, but not backup. Therefore, if a source virtual machine becomes corrupted, this corruption will be replicated to the standby VM. In such an event, the standby VM would not be operational and the RTO/RPO would be null and void. Therefore, it is required that the Client has a backup system in place to protect their environment. The Client acknowledges that, if those backups are not also copied to a second site, it may not be possible to resume service if the only copy available is the replicated copy of a corrupt virtual machine.

There are various components to the DRaaS Service:

- Replication software which replicates source virtual machines to the n4Cloud platform. Node4 reserves the right to change technologies used from time to time if the functionality provided is similar or better (in the opinion of Node4).

Configuration of networking to redirect traffic to the standby VMs is not part of the scope of this service. It is the responsibility of the Client to ensure that they have a mechanism in place to be able to use/connect to the standby VMs if a disaster recovery event is invoked.

This service only currently supports VMware vSphere virtual machines.

The Client is entitled to perform two failover tests in any 12-month rolling period, starting from the Service Commencement Date. By providing not less than 30 days notice to Node4 the Client shall be entitled to boot their standby VMs to simulate a real disaster recovery event.

The failover tests should not exceed five working days in duration. If this is the case, the Client shall not be charged for the n4Cloud resource used during the failover test. In the event that a test does exceed five days, Node4 shall charge for the resource consumed on the n4Cloud platform at the rates on the Order From in full for each and every month the virtual machines are powered on.

Node4 recommends that at least one test is carried out per annum.

In the event that a Disaster Recovery Event is invoked due to loss of a Node4 data centre, fees for usage of the standby VMs on the n4Cloud platform shall not apply. In all other circumstances, the Client agrees to pay fees for the n4Cloud resource used.

Where the source platform is n4Cloud, the Client acknowledges that they may be required to "failback" to the original platform at a mutually agreed time after the source platform has been declared as having "resumed normal operations" by Node4.

In the event that failover is required, Clients can evoke in one of the following ways;

- Calling the Service Desk on 0345 123 2229 where a support ticket will be raised on the Client's behalf;
- Raising a support ticket via email to support@node4.co.uk. This option is not recommended where recovery is urgent, as delivery of e-mail cannot be guaranteed. If raising a ticket via e-mail, Clients are recommended to subsequently contact the Service Desk to ensure the appropriate level of urgency is applied.

The Client is responsible for ensuring that they are compliant with software licensing terms for software replicated to the n4Cloud platform, which may involve the need to purchase additional licenses.

2. Definitions

"Client Responsible Incidents" means in the event that a Service Affecting Incident or Non-Service Affecting Incident is identified as being attributable to Client provided equipment, Premises, Client power supplies, or the action of the Client, employees or agents of the Client, the Incident shall be deemed the responsibility of the Client. Any downtime shall not be included in service availability measurements and does not qualify for compensation.

"Contracted Support Hours" Bronze, Silver, Silver Plus and Gold support hours as identified in section 6 below.

"Incident" means an unplanned interruption to a service or a reduction in service quality

"Monthly Review Period" means the calendar monthly periods commencing on the 1st of each month during the Term, over which Service performance measurements are calculated, provided that the first Monthly Review Period will commence on when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client;

"**Node4 Monitoring System"** means Node4's network integrated Incident management system;

"Node4 Network" means the network wholly owned and managed by Node4;

"Non-Service Affecting Incident" means an Incident or condition which is not a Service Affecting Incident.

"Planned Outage" means proactive work required to maintain the service provided, Node4 may with reasonable notice require a temporary outage in service. Wherever possible Node4 will agree the outage with you in advance of the required work. Any planned downtime shall not be included in Incident or service reliability measurements.

"Service Affecting Incident" means any failure of Node4 service, which, in our reasonable opinion causes a loss of a Client's service. In all such cases the service shall be deemed unavailable and the length of downtime recorded by Node4 from when the Incident is registered by Node4 and a Service Ticket allocated.

"Service Availability" means the time for which a Node4 service is usable, expressed as a percentage of the total time in a given Service Measurement Period. The Node4 service shall be deemed available for the purposes of calculating Service Availability, even if it is not usable, due to:

- an event outside our reasonable control;
- a Client Responsible Incident;
- a Third Party Attributable Incident
- due to a Planned Outage including patching and software upgrades

"Service Desk" means the single point of entry for all Service Tickets and Service Requests which can be accessed over the phone, by email or via our portal.

"Service Request" means a request for a change for information or ***"Service Ticket"*** means the tickets which are raised in relation to Incident or Service Request

"Standard MAC" means a change to one device which can be completed within 30 minutes by a technical support engineer between 7am and 7pm Monday to Friday.

"Third Party Software Vendor" means the owner of software which is either licensed by Node4 or licensed by the Client in both cases for software deployed/used within the Services.

"Time To Resolve Incident" means the length of time from the issue of the Service Ticket to repair and resolution or the service.

3. Specific terms

The following terms and conditions shall apply when Node4 provides DRaaS services to the Client.

3.1 Client data

Client shall be liable for all the Client data that Client creates from its use of the DRaaS. Client represents and warrants that Client owns all Client data created within the DRaaS and that the Client has permission from the rightful owner for it use.

Node4 disclaims all liability relating to any Client data with the DRaaS service, and for all liability relating to unauthorized use (by other users) of Client data.

3.2 Third party software and licences

On invoking DR, it is the Client responsibility to ensure that appropriate licencing is in place and fully aligned with vendor rules in the use of DRaaS. The Client may not and is not licensed to install or use software or technology in any way that would infringe any Third Party Software Vendor's intellectual property, technology or licencing usage rights.

4. Fees

4.1 Fees payable by the Client

Fees will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client. Fees may comprise any or all of the following aspects.

4.2 Installation and set-up fees

Any applicable installation and set-up Fees for the implementation of the service shall be detailed on the Order Form.

4.3 Rental fees

Rental Fees are paid either monthly or annually in advance based on the options taken and any other related service and are identified on the Order Form.

4.4 Bandwidth fees

Bandwidth of 4Mbps to carry replication traffic is included by standard. This is a standard allowance and has not been sized or deemed appropriate for individual requirements.

4.5 Additional professional services

Additional tasks undertaken at the request of the Client by Node4 personnel, will be charged at rates agreed between the parties in advance.

5. Provision of service

5.1 Software updates & patches

As part of the service, Node4 shall apply software updates and patches to the following systems when they are required due to software defect (bug) or security vulnerability identified by the vendor:

- Network and storage devices used in the provision of the service by Node4.
- DRaaS software

The Client will be responsible for patching their virtual machines. It should be noted that a patch applied to a source virtual machine will be replicated to the failover virtual machine. The Client acknowledges that the service may no longer function if the virtual environment used by the Client is upgraded to a version that is not supported as part of this service. For example, an upgrade to the version of VMware used by the Client, or the virtual machine version, may prevent the service from working correctly. In such circumstances, the Client shall continue to pay the Fees for the service and the service shall continue to be considered as "available".

5.2 Hardware maintenance

Any Incident relating to hardware failure on the n4Cloud platform is covered by hardware maintenance which is provided as part of the service. The Client acknowledges that occasionally hardware maintenance may cause a loss of service, though Node4 will take reasonable measures to prevent this occurring as part of the design.

5.3 Monitoring

Node4 monitor the service elements managed by Node4 as standard via the Node4 monitoring system to provide pro-active Incident management by Node4 during the Contracted Support Hours. In the event that a Node4 device used in the provision of the service stops responding, or a monitored threshold is exceeded, Service Desk will pro-actively investigate:

- On a 24*7 basis, where the issue is deemed by the support engineer to be such that it shall prevent or is preventing a) the replication of data from the Client's virtual machines and/or b) the service from being able to failover virtual machines if required;
- During the Contracted Support Hours, for all other issues, including reduced performance.

Node4 will undertake capacity management to ensure the SLA targets can be met.

The Client shall not have access to monitoring or capacity data.

5.4 Power

Power to the n4Cloud platform is provided using dual feeds from a single provider. UPS and Generator back-up is also provided with a minimum N+1 configuration. The Client is responsible for ensuring that power supply to the environment for which failover is provided is sufficient to provide uninterrupted service, and acknowledges that should that environment fail, replication will temporarily cease, meaning that the recovery point objective (RPO) may be breached. In such a case the Client acknowledges that the service shall be deemed as operating normally.

5.5 Internet security

Node4 provide n4Cloud Clients with public internet access. Internet Security and Virus Protection is the responsibility of the Client. All internet usage is subject to the Acceptable Use Policy.

5.6 IP addresses

The number of public internet routable IP addresses assigned will identified on the Order Form. IP address usage is monitored and reported to RIPE database. The use of IP addresses must be justified. It is the Client's responsibility to use their assigned IP addresses. Use of non-assigned IP addresses will result in immediate disconnection from the Node4 Network.

Because the DRaaS Service is a shared platform that will involve elements managed by the Client and elements managed by Node4, the Client must agree the IP addressing scheme with Node4.

5.7 Service installation and provisioning

Standard set-up is provided. For more complex configurations a technical scope document will be agreed, and any relevant Fees are identified on the Order Form.

5.8 Site security

The following security measures are in place at Node4 data centres:

- Perimeter fencing with electric gates
- Access via photo swipe card system
- CCTV with 24 hour recording both external and internal to the data centre
- Access Control Procedure

- Data Centres are manned 24 hours a day.

5.9 Data centre access

Access to the data centre is not permitted for the DRaaS Service as the service is managed by Node4.

Where the Client has chosen to merge a Colocation Service with the DRaaS Service access will be provided to the Colocation elements as discussed in the Schedule Document for Colocation Services.

5.10 Client support

Node4 provides the service direct to the Client. The Client commits to fully manage all their customers and suppliers directly. Node4 will not interface directly with any third parties working with the Client. If the Client requires Node4 to provide their customers with a customer care or NOC service this is available on request and subject to the additional professional service Fees in section 4.5. Node4 shall not be liable in respect of any contract, agreement or relationship that Client may have with any third party. If a dispute arises between Client and a third party involving Node4's DRaaS Service, Node4 shall provide the Client with reasonable information and assistance (to the extent that such is not adverse to Node4's interests to Client (at Client's expense)) in the resolution of such dispute.

5.11 Essential Maintenance

Where Node4 plans to perform essential maintenance Node4 will endeavour to perform such works during periods of lower usage and will endeavour to give the Client ten (10) days prior notice. In the event of an emergency Change or Service Affecting Incident such notice may be less than 24 hours. This is without prejudice to or limitation of the definition of Planned Outage.

This notice may be provided on N4Status (www.n4status.co.uk) rather than a direct notification. Clients can subscribe to status updates on the N4Status website to receive automated direct notifications.

5.12 Changes

Moves, Adds & Changes (MAC) are not provided as part of the standard service. If "Full Management" is included on the Order Form Standard MACs are included (fair use policy applies).

Change requests conducted outside of the support contract, or change request implemented outside normal business hours will be dealt with as chargeable projects and subject to the Support and Professional Services Fess in 4.5.

6. Incident management

6.1 Incident handling

Incidents are handled as outlined in the Incident Management Schedule.

6.2 Hours of support

Node4 provides Gold Support as standard for these services which is 24/7 for Priority 1 and 2 and between 7am and 7pm weekdays, excluding bank and national holidays for Priority 3,4 and Service Requests.

6.3 Incident priority

Each new Incident will be assigned a priority level by the Service Desk based on the following definitions. These levels allow us to prioritise resources and escalate where appropriate.

Priority	Description
1 - Critical	A major Incident resulting in total loss of service.
2 - High	A major Incident resulting in a severe service degradation or loss of service to a significant percentage of users.
3 - Medium	A minor Incident resulting in a limited or degraded service or a single end user unable to work.
4 - Low	General, single user with degraded service, non-service affecting support.
5 - Service Request	Request for a change to an existing service or system, a request for information or simple questionnaire to be completed.

6.4 Time to repair

Node4 aims to respond, update and resolve incidents in relation to the DRaaS with the following times:

Priority	P1	P2	P3	P4	Change
Response / Acknowledgement	30 Mins	1 Hour	2 Hours	4 Hours	12 Hours
Commencement	1 Hour	2 Hours	4 Hours	N/A	N/A
Frequency of Updates	1 Hour	2 Hours	12 hours if Resolve / Target to Fix exceeded		
Resolve / Target to Fix	4 Hours	8 Hours	12 Hours	36 Hours	60 Hours

Resolution times in the table above do not apply where there is a Client Responsible Incident, a Third Party Attributable Incidents or events outside Node4's reasonable control, any incidents including these aspects will be excluded from reporting provided.

All priority 1 & 2 Incident should be raised via the tickets system by a phone call. Should a priority 1 or 2 incident be raised via the portal or e-mail, the Client is required to follow this up with a corresponding phone call to enable work to commence immediately on the issue.

* Acknowledgement refers to an automated service which generates a response and alerts engineers of a service failure; or where there is dialogue between the client and the engineer.

6.5 Incident duration

All incidents recorded by the Node4 monitoring system will be reconciled against the corresponding incident ticket raised by the Service Desk. The exact incident duration will be calculated as the elapsed time between the Service Ticket opened and the time when Service is restored.

7. SERVICE CREDITS

The following equation will be used to calculate the DRaaS replication availability. References to hours are to the number of minutes in the applicable Monthly Review Period:

((Total minutes – Total minutes Unavailable)/Total minutes) x 100

Node4 will provide the Client with service credits, as set out below, for the failure to meet the following targets:

7.1 DRaaS replication availability

Availability	Service Credits as % of Monthly DRaaS Service Charge
<99.99%-99.85%	5%
<99.85%-99.7%	10%
<99.7%-99.5%	20%
<99.5%-99.0%	25%
<99%	50%

7.2 Calculation of service credits

Where a Monthly Review Period incorporates part of a month, any service credit will apply to a pro-rated monthly Rental Fee.

Service credits will be calculated monthly, aggregated and credited to the Client on a quarterly basis.

If a Service is cancelled during a Monthly Review Period, no service credit will be payable in respect of the service for that Monthly Review Period.

The Client must claim any service credit due to a failure to meet the Service Levels, in writing, within twenty-one (21) Business Days of the date at which the Client could reasonably be expected to become aware of such failure, otherwise no service credits shall be payable. The Client shall not be entitled to any service credits in respect of a claim unless and until Node4 has received notice of the claim in writing in accordance with the above. Should Node4 require additional information from the Client, the Client shall assist, and shall not be entitled to any service credits until Node4 has received all the information it has reasonably requested.

7.3 Exclusions to payment of service credits

Without prejudice to or limitation of the definition of Service Availability, service credits will not be payable by Node4 to the Client in relation to the Service Availability for Incidents or disruptions to the Services caused by any of the following:

- The Incident, action or negligence of the Client, its employees, agents or contractors;
- The Client failing to comply with the provisions of the Agreement;
- An Incident in, or any other problem associated with, equipment connected on the Client's side of the Node4 Network termination point, except where such Incident or problem is directly caused by the Incident, action or negligence of Node4, its employees, agents or contractors;
- Any event described in Clause 10 (Force Majeure) of Node4's Terms and Conditions;
- Any Planned Outage.