



Schedule Document

N4Cloud

PUBLIC
Node4 limited
01/04/2020

Schedule Document

N4Cloud

This schedule contains additional terms and conditions, service description and service levels applicable to the Cloud element of the Services and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy.

1. Overview

The N4Cloud service provides access to a self-service virtualisation platform hosted on infrastructure owned by Node4. The infrastructure is securely shared across multiple customers and hosted in three Node4 UK data centres which provide security and resilient power and cooling.

Node4 manage the infrastructure up to the Hypervisor and ensure a portal is available for provisioning.

By default, the Customer manages their Virtual Machines. Node4 can also provide management of virtual machine operating systems for an additional charge as part this service.

The components of the N4Cloud service are:

Self-Service Portal – web-based portal(s) and tools for self-service provisioning and management of the components of the Services.

Compute Resource (Shared) – a pool of memory (RAM) and processor (vCPU) on shared virtualisation hardware on which the Customer runs Virtual Machines.

Compute Resource (Standby) – a pool of memory (RAM) and processor (vCPU) on shared virtualisation hardware reserved for the Customer to run Virtual Machines if a Disaster Recovery Event occurs.

Compute Resource (Dedicated) – a pool of memory (RAM) and processor (vCPU) on virtualisation hardware dedicated to the Customer, on which the Customer runs Virtual Machines.

Virtual Machines – operating system instances running on Compute Resource.

Storage without Backup – a pool of disk storage on one or more performance tiers. This storage does not include backup.

Storage with Virtual Machine Backup – a pool of disk storage on one or more performance tiers that also includes backup of the Virtual Machine.

Storage for Replicated Virtual Machines – storage used to hold the replicated image of Virtual Machines so they can be restarted if a Disaster Recovery Event occurs. This is held on a storage device made by a manufacturer different to that used to provide other storage components.

Storage with Encryption - storage at the various tiers may be specified with encryption at rest applied.

Backup for Other Clouds – backup of remote servers and endpoint devices via the Internet.

Service component - Build – setup of the N4Cloud service with optional provisioning of Virtual Machines and installation of certain applications.

Service Component - Operate – management of the N4Cloud platform and Virtual Machines.

2. Definitions

“Additional Terms” means this Schedule Document forming part of the Master Agreement, which describes the Products and/or Services to be provided and the relevant service levels;

“Application Licence” means a License for software for an application installed on the N4 Cloud service. Examples of such software include: Microsoft SQL, Microsoft Office applications, Sage Plesk and Cpanel.

“Customer Responsible Incident” means in the event that a Service Affecting Incident or Non-Service Affecting Incident is identified as being attributable to Customer Provided Equipment, Premises, Customer power supplies, or the action of the Customer, employees or agents of the Customer, the Incident shall be deemed the responsibility of the Customer. Any downtime shall not be included in Service Availability measurements

and does not qualify for service credits, rebates or compensation.

“Contracted Support Hours” means Bronze, Silver, Silver Plus and Gold support levels as identified in section 10 below.

“Equipment” means, without limitation, any equipment, machinery, and apparatus provided by Node4 as part of the Services, and/or used in order to make available the N4Cloud service to the Customer;

“Encrypted Storage” means data-at-rest encryption using XTS-AES-256 based algorithm and validated to FIPS140-2 Level 1.

“Hypervisor” means hardware and software used to create and run Virtual Machines allowing multiple operating systems to run concurrently on a single host computer.

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

“License” means a perpetual or user based or other software license as required to be purchased under the terms of a software license agreement from a Third Party Software Vendor.

“License Fees” means a fee or charge from a License or Licenses including OS Licenses, Application Licenses and User-based Licenses.

“License Mobility” means an arrangement whereby Licenses owned by the Customer can be deployed/used within the Services. License Mobility must be permitted under the terms of any applicable License and must specifically permit Customer owned Licenses to be deployed on third party hardware (including the N4Cloud service).

“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 following the Ready For Service Notification;

“Non-Service Affecting Incident” means a Incident or condition which is not a Service Affecting Incident.

“OS Licence” means a License for software covering the operating system level of a virtual machine within the N4Cloud service. Examples of such software include Microsoft Windows Server and Red Hat Linux.

“Planned Outage” means in maintaining the service provided, Node4 may with reasonable notice require a temporary outage in service. Wherever possible Node4 will agree the outage with the Customer in advance of the required work. Any planned downtime shall not be included in fault or Service Availability measurements.

“Service Affecting Incident” means any failure of the Node4 network, equipment or service, which, in our reasonable opinion causes a loss of a Customer’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 Ticketer 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 if it is not usable due to an event outside our reasonable control, a Customer Responsible Incident, a Third Party Attributable Incident or is due to a Planned Outage.

“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 Measurement Period” means a calendar month for which the Service is available.

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

“Setup Charge” means Fees payable by the Customer for the setup of the Services as provided in the Order Form;

“Software Update” means a minor release of software that typically fixes bugs and increases stability but adds very little new functionality.

“Software Upgrade” means a major release of software that typically introduces new features.

“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 Attributable Incident” means in the Incident that a Service Affecting Incident or Non-Service Affecting Incident is identified as being attributable to a third party. Any downtime shall not be included in Service Availability measurements and does not qualify for service credits, rebates or compensation. Node4 will endeavour to resolve and rectify such Third Party Attributable Incidents as soon as possible.

“Third Party Software Vendor” means the owner of software which is either licensed by Node4 or licensed by the Customer 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 and/or associated equipment.

“User-based License” means a License for software sold on a user by user basis by the relevant Third Party Software Vendor. Examples of such software include Microsoft Office, Microsoft Office365, Microsoft Visual Studio.

3. Specific terms

The following terms and conditions shall apply when Node4 provides N4Cloud service to the Customer.

3.1 Customer data

Customer shall be liable for all the Customer data that Customer creates from its use of the N4Cloud service. Customer represents and warrants that Customer owns all Customer data created within the N4Cloud service and that the Customer has permission from the rightful owner for its use.

Node4 disclaims all liability relating to any Customer data with the N4Cloud service, and for all liability relating to unauthorized use (by other users) of Customer data.

3.2 Third parties

Node4 shall not be liable in respect of any contract, agreement or relationship that Customer may have with any third party. If a dispute arises between Customer and a third party involving Node4's N4Cloud service, Node4 shall provide, at Customer's expense, the Customer with reasonable information and assistance to the extent that such is not adverse to Node4's interests to Customer in the resolution of such dispute.

3.3 Third party software

Customer 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.

3.4 Software licenses

Where the Products or Services include software, the same is provided on a licensed basis in accordance with the License terms and conditions applicable thereto, which the Customer agrees that it will comply with.

Where Node4 are providing the Customer with Licences as part of the Service a monitoring agent will be installed in the Customer environment for monthly licence consumption and verification.

3.5 Software license audits

Where the relevant software License prescribes, Third Party Software Vendors (or their agents) may have a right to conduct audits on the deployment/usage of their software in the Services, the Customer shall support Node4 in compliance with such audits (as prescribed in the software License). If an audit reveals any unlicensed software then the Customer shall within 30 days of notice order sufficient software Licences to cover its unlicensed use and reimburse Node4 any resulting software Licence Fees which are incurred as a consequence. Where the Customer is unable or unwilling to comply with a Software License audit request then the Customer shall fully indemnify

Node4 for all internal costs and charges from Third Party Software Vendor which it incurs as a result.

3.6 License mobility

Where a relevant software License permits License Mobility, the Customer agrees that it will have complete responsibility and liability for all licensing matters in connection with such License Mobility and will indemnify Node4 in relation to all unlicensed use of software covered by License Mobility.

The Customer agrees that it will comply with all requirements of the Third Party Software Vendor in connection with such Licence Mobility and in particular the documentation and/or the Third Party Software Vendors verification process required for License Mobility. This includes the installation of monitoring agents to analyse licence consumption.

Customer will provide Node4 with details of the Licences used within its environment and support Node4 in the conduct of any software License audits as they apply to License Mobility. and will indemnify Node4 in relation to all unlicensed use of software covered by License Mobility.

Where Licence Mobility is used the Customer must provide Node4 with confirmation that the relevant Licence Mobility form has been submitted to the Third Party Software Vendor before the setup / implementation of the environment can commence and Node4 must receive confirmation of Licence Mobility from the Third Party Software Vendor before the environment is set live, if this is not received Node4 will provide the Licences and associated charges applied per month until the confirmation is received.

4. Fees

Fees will commence when a Ready For Service Notification is provided by Node4. This will follow either handover of a Service or notification from Node4 that the Service is available for Customer use. Fees may comprise any or all of the following aspects.

4.1 Installation and setup fees

Any applicable installation or set-up Fees as detailed on the Order Form.

4.2 Rental fees

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

4.3 License fees

Initial committed License Fees are identified on the Order Form and will be invoiced monthly.

Any increases in licence charges from the Third Party Software Vendors will be applied the month following the increase.

License Fees are charged for the complete month, any additional Licences consumed will be invoiced the month following identification.

4.4 Customer resource increases

Increases in the level of resources (CPU, memory, storage) in addition to those defined on the Order Form, which are activated directly by the Customer via the Self-Service Portal will be invoiced from the date of increase and included on the next invoice.

4.5 Professional service fees

Additional tasks undertaken by Node4 at the request of the Customer or activities undertaken by the Customer which require the remote support of Node4 personnel will be charged based on rates below

Time support required:	Per hour
Mon – Fri 07.00 – 19.00	£80.00 per hour
All other times	£120.00 per hour

Time is charged by the hour. These rates are for a trained technician and are subject to an annual review by Node4. For advanced engineers please contact Node4 for pricing.

5. General provision of service

5.1 Data centre security

Node4 will ensure the following security measures are in place at the Node4 data centres from which the N4Cloud service is provided:

- 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.
- Staff on-site 24 hours a day.

Access to the data centre and/or Node4 infrastructure is not necessary for use of the N4Cloud service and is not permitted.

5.2 Support

Node4 provides the Services direct to the Customer. The Customer commits to fully manage all their customers and suppliers directly. Node4 will not interface directly with any third parties working with the Customer.

If the Customer requires Node4 to provide their customers with a customer care, network operations or similar service this is available on request and subject to Professional Service Fees.

5.3 Maintenance windows

Where Node4 plans to perform essential works and the changes are service affecting, Node4 will use reasonable endeavours to perform such works between the hours of 00:00 and 04:00 and will use reasonable endeavours to give the Customer at least five (5) days prior notice for network related work and at least ten (10) days prior notice for Infrastructure related work. In the event of an emergency 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.

6. Service Components - Platform

6.1 Self-Service portals

Node4 will provide one or more Self-Service Portals ("portals") which the Customer can use to perform a set of provisioning and management tasks for their virtual machines, storage and backups.

Customers are allocated one or more usernames and passwords which are used to access the portals. Each username is assigned to a single user within the Customer's organisation.

The portals are secured using firewalls and Secure Sockets Layer (SSL) encryption.

Node4 may use multi-factor authentication to secure the portals. This requires the Customer to provide a

PIN number and enter this number into a mobile device, or answer an automated phone call, in order to be granted permission each time they login to the portal.

Node4 reserve the right to change the technology and look and feel of the portals from time to time. It is not permitted for users to remove copyright notices or change the look and feel of the portals.

This component is mandatory for all orders.

If specified on the Order Form, the portals will provide the ability for the Customer to increase the CPU, memory and storage virtual datacentre resources. By increasing the virtual datacentre resources via the portals the Customer agrees to an increase in the virtual data centre resources Fees. The Fees will increase from point of change on the portals until the end of the Term at the rates defined for the associated virtual datacentre resources on the Order Form.

A maximum increase of 20% of the existing virtual data centre resource can be completed each month within the portals.

6.2 Compute resource (Shared)

Node4 will reserve a pool of compute resource on physical hosts that form part of the N4Cloud service Hypervisor platform. These hosts are securely shared between multiple customers.

Customer Virtual machines run within this pool of resource.

The amount of resource required by the Customer must be specified on the Order Form, in the form of both:

- the amount of virtual processor cores (vCPU) required in each N4Cloud data centre; and
- the amount of gigabytes of virtual RAM (vRAM) required in each N4Cloud data centre.

Each pool is provided within a single datacentre and Virtual Machines cannot be transferred between sites without the use of disaster recovery technology.

The Customer may request to change the amount of vCPU and vRAM in the pool. A request to lower the amount of vCPU and/or vRAM must not violate any prior commitments made on any Order Form.

Virtual CPU is contended, meaning that a virtual CPU is not equivalent to a physical processor core. Memory is not usually contended.

If a pool is created with 4 vCPU and 8GB of RAM, and a single virtual machine is created with 2 vCPU and 4GB of RAM, then the pool is 50% full.

Node4 will reserve at least one physical Hypervisor host at each site as a failover node. The failover node will take the place of any of the other physical nodes if they fail, but some downtime may occur to machines running on the failed node as they are restarted on the failover node.

Ownership of the hardware remains with Node4 at all times. Node4 will provide the operating system and all applicable OS Licenses for this resource. These licenses shall remain the property of Node4 and are assigned to the Customer for each Virtual Machine charged under this component.

6.3 Compute resource (Standby)

If specified on the Order Form, Node4 will reserve a pool of standby resource. This component is the same as the *Compute Resource (Shared)* component except that the pool is not used for running Virtual Machines under normal circumstances. The pool can only be used by virtual machines in the event that a Disaster Recovery Event is invoked following relevant Node4 procedures.

Node4 will charge for the standby resource at a rate that is lower than the *Compute Resource (Shared)* component because Virtual Machines are not powered on in this pool unless a disaster recovery event is invoked. The lower rate is achieved because the same physical resource is reserved to protect Virtual Machines in different datacentres on the assumption that these sites are not likely to experience a disaster recovery event at the same time.

It is also possible to use spare capacity in the *Compute Resource (Dedicated)* component instead of this component for disaster recovery.

The amount of resource required by the Customer must be specified on the Order Form, in the form of both:

- the amount of virtual processor cores (vCPU) required in each N4Cloud data centre; and
- the amount of gigabytes of virtual RAM (vRAM) required in each N4Cloud data centre.

The amount of resource required may not necessarily be the same as that allocated to the *Compute Resource (Shared)* component if the Customer does not wish to perform disaster recovery replication for all of their Virtual Machines.

If Virtual Machines are booted within this pool in a disaster recovery event, they shall be charged at the same rate as the *Compute Resource (Shared)* component for any calendar month in which they are powered on, except during any period of testing that has been agreed in writing by Node4 and limited to a maximum of two calendar weeks per year. For clarification where the charge for the disaster recovery machines are applied, no charge will be applied for the BAU machines which are out of action.

Ownership of the hardware remains with Node4 at all times. Node4 will provide the operating system and all applicable OS Licenses for this resource. These licenses shall remain the property of Node4 and are assigned to the Customer for each virtual machine charged under this component.

6.4 Compute resource (Dedicated)

If specified on the Order Form, Node4 will reserve a set of physical hosts on the N4Cloud service Hypervisor platform that are dedicated for exclusive use by the Customer during the contract term.

Dedicated compute resource is provided via the Self-Service Portal as an allocation of resources within the Customer allocated virtual datacentre.

Node4 provide a CPU allocation ratio of 2:1 vCPU to physical core. Overcommitting contention ratios beyond this must be agreed through a variation to terms and conditions of the customer order.

Node4 provide an N+1 failover host as part of any dedicated compute Order up to 8 blades. Any further dedicated compute hosts the Customer requires beyond this include an additional failover host.

VMware licensing is applied to the level of installed memory capacity of the dedicated blade. This

ensures that that the blade is correctly licensed to the maximum potential loading of the VMware host blade. VMware licensing is not required on a dedicated failover host.

Customer Virtual Machines will run within this pool of resource. Selecting the number of hosts that are required is the responsibility of the Customer subject to the minimum failover capability (N+1) per eight hosts, the number of hosts must be specified on the Order Form.

The Customer may request to add additional hosts for an additional charge. The Customer may request to lower the amount of nodes but this must not violate any prior commitments made on any Order Form.

Ownership of the hardware remains with Node4 at all times. Node4 will provide the operating system and all applicable OS Licenses for this resource. These licenses shall remain the property of Node4 and are assigned to the Customer for each virtual machine charged under this component.

The Backup and Recovery license is required to perform backups using the Storage with Virtual Machine Backup component.

6.5 Software licenses

If specified on the Order Form, Node4 will provide Application Licences and User-based Licences for software to be installed and used in Customer Virtual Machines on the N4Cloud service. Application and Users Licences will be subject to change over time from, for example, changes in user numbers and/or as a result of software License audits. Increased License Fees will be invoiced the month following identification.

The Customer is responsible for ensuring that their Virtual Machines are appropriately licensed and informing Node4 of any changes that require additional licenses.

Some vendors may require that software used on the Node4 platform must be licensed by Node4. The Customer agrees that additional License Fees may be payable for such software deployed on Virtual Machines on the N4Cloud service.

Node4 reserve the right to change the licenses that are available from time to time and/or the units used to charge for licenses.

6.6 Anti-virus software

If specified on the Order Form, anti-virus software will be installed into any Virtual Machines provisioned by Node4. The Customer must install anti-virus software into Virtual Machines that are provisioned by the Customer.

The Customer may not remove this software, all Virtual Machines must be protected by anti-virus software at all times.

The Customer is responsible for applying anti-virus updates and for removing viruses from the operating system. The Customer must ensure that anti-virus updates are applied in a timely manner.

Anti-Virus software may not be able to detect and/or remove all threats. If the Customer requires that data can be recovered if permanently deleted or damaged by a virus or other threat, then the Customer is responsible for taking appropriate measures to protect their data (such as using a backup service).

6.7 Storage without backup

If specified on the Order Form, Node4 will allocate a pool of storage on one or more tiers on the N4Cloud storage platform, on which Customer Virtual Machine disks can be stored and run.

This component is used to provide storage for Virtual Machines for which virtual machine backup is not required.

There are four performance tiers, each consisting of a different type of disk.

The Self-Service Portal software is used to isolate a quota of capacity in each tier and ensure that it is only visible to the correct customer. A customer is not able to access storage used by other customers. Each pool of storage is limited to a single data centre.

The Order Form must specify the amount of required storage in useable GB for one or more of the following performance tiers:

- **Tier 0 Storage without Backup** – consists of flash (SSD) disk only for extreme performance. Typically used for workloads such as databases.
- **Tier 1 Storage without Backup** – consists of SAS disk together with a smaller flash (SSD) cache that is used to hold frequently accessed blocks to increase performance.
- **Tier 2 Storage without Backup** – consists of SAS disk only. Used for most workloads.
- **Tier 3 Storage without Backup** – consists of SATA disk only. Typically used for archiving of data.

Node4 reserve the right to select the vendor used to provide storage to the platform, which may change from time to time.

The Customer is charged for the space allocated to the pool and not for the actual space allocated to virtual machine disks. Storage must only be consumed by Virtual Machines and may not be presented out for consumption over the network from other devices, including those in colocation.

Storage without backup tiers 0 to 3 includes an option for encryption to be applied. If encrypted storage without backup is used with the replicated virtual machines option (DRaaS) then replicated storage with encryption must be used for the target storage as replication between encrypted and non-encrypted storage is not supported.

6.8 Storage with virtual machine backup

This component is identical to the *Storage without Backup* component except that it includes virtual machine backup.

If specified on the Order Form, Node4 will allocate a pool of storage on one or more tiers on the N4Cloud storage platform, on which Customer Virtual Machine disks can be stored and run.

There are four performance tiers, each consisting of a different type of disk.

The Order Form must specify the amount of required storage in useable GB for one or more of the following performance tiers:

- Tier 0 Storage with Virtual Machine Backup
- Tier 1 Storage with Virtual Machine Backup

- Tier 2 Storage with Virtual Machine Backup
- Tier 3 Storage with Virtual Machine Backup

Node4 will reserve a secondary pool of storage resource which is used to hold backups of the Virtual Machine data. The size of the pool will be determined by Node4 based on the amount of storage selected from the four tiers. All backup data is held on lower grade disks, usually SATA or NL-SAS disks, which are held in fully redundant disk arrays. Backup data is encrypted at rest with Node4 managed keys.

For Virtual Machine data to be backed up via this component, a backup software license is required. Node4 will provide a backup software license for each Virtual Machine covered by the *Virtual Machine* component. All licenses shall remain the property of Node4.

Any Virtual Machines that are added after the initial provisioning of the service will not be automatically be added to the backup job and it is the responsibility of the Customer to notify Node4 to include any additional Virtual Machines to the backup service.

Virtual Machines that are being backed up must be running on the *Compute Resource (Shared)* or *Compute Resource (Dedicated)* components.

The backup software runs on a Node4 managed platform that is securely shared by multiple customers and can only be used to perform backups of Virtual Machines running on the N4Cloud service.

If requested, the backup software can perform application aware processing of Virtual Machines to create transactionally consistent backups of Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange or Oracle. The Customer must provide operating system credentials with appropriate permissions. This may be a specific domain account or credentials for individual Virtual Machines.

All Virtual Machine and file level restores are undertaken by Node4 and can be performed to original or alternate N4Cloud location with settings changes, such as name, made if required. If application aware processing is enabled. The backup software allows for the recovery of individual items of data from a number of software packages (such as Microsoft Exchange, Microsoft SQL Server,

Microsoft SharePoint and Microsoft Active Directory) without the need to restore the whole dataset.

This service provides a 30 day retention period for in scope Virtual Machines and uses daily incremental backups. One backup is taken each day and incremental block changes are stored for 30 days.

By prior written agreement and at the discretion of Node4, Node4 may permit alternative retention periods and/or a grandfather-father-son retention policy. Such adjustments will require additional retention storage, which is charged separately. The amount required must be estimated by Node4 based on information provided by the Customer and will appear on the invoice as 'Additional Retention Storage'. This is charged per useable gigabyte per month of space on the Node4 storage array used to store the data, after deduplication and compression have been applied. Node4 reserve the right to change the amount required should the estimate prove insufficient based on actual Customer usage, for which additional Fees may apply.

Node4 have made an estimation of the amount of data required on disk after deduplication and compression that will be achieved when pricing this service. Node4 reserve the right to increase pricing if the Customer workload is found to have a rate of change that varies significantly from that estimation, either at a point in time or as part of a trend.

This component cannot be used if the Customer performs encryption of data on virtual machine disks as this will affect the deduplication and compression ratios which Node4 can achieve.

All Customer backup jobs run between 19:00 and 07:00. Node4 can provide custom backup windows if requested however this may incur additional charges. In the event that a virtual machine is deleted, Node4 shall retain the associated data for 5 calendar days, after which it is permanently deleted.

Any backup job failures will be automatically raised to the Node4 Service Desk and investigated by an engineer until resolved. In cases this may involve speaking to the Customer or re-running the backup job.

In the event that the Customer contract is cancelled for any reason, Node4 shall retain data until the last

day of the notice period during which normal Fees shall apply. On the first day following this period, the data shall be permanently deleted and the retention period shall immediately cease to apply.

Storage with virtual machine backup tiers 0 to 3 includes an option for encryption to be applied. If encrypted storage with virtual machine backup is used with the replicated virtual machines option (DRaaS) then replicated storage with encryption must be used for the target storage as replication between encrypted and non-encrypted storage is not supported.

6.9 Storage for replicated virtual machines

If specified on the Order Form, Node4 will reserve a pool of storage on a Node4 storage array to store replicated Virtual Machines on one of three performance tiers.

The pool will be presented to the Node4 Hypervisor as a datastore for use by Disaster Recovery Replication software. The software is configured to replicate active Virtual Machines to this datastore. In the event of a Disaster Recovery Event, Customer Virtual Machines will run from this storage.

The storage is sold in units of 1GB, and the amount of storage ordered via this component should be equal to the sum of all virtual disks on all replicated Virtual Machines. The amount of storage ordered should not be calculated based on the amount of space used within file systems inside the Virtual Machines.

Node4 will include in sufficient storage within the price to hold changes for a 5 day journaling window and average rate of data change. If the data used varies significantly from this estimation, Node4 reserve the right to review the requirement, which may require additional Fees or a reduction in the journaling window.

The same charge for this storage will apply regardless of whether a Disaster Recovery Event is currently occurring.

Backup is not available for this storage. Virtual Machines that are stored using the *Storage with Virtual Machine Backup* component will be backed up from the *Storage For Replicated Virtual Machines'*

component storage in the event of a Disaster Recovery Event.

Storage for replicated virtual machines tiers 1 to 3 includes an option for encryption to be applied and this must be used if encrypted storage is used for the source virtual machines (with or without backup) as replication between encrypted and non-encrypted storage is not supported.

6.10 Backup for other clouds

If specified on the Order Form, Node4 will provide a software application and credentials that allows the Customer to perform backup of:

- Files, folders and application data (for example for Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint Server, MySQL) held on physical servers in a Node4 data centre or on the Customer premises;;
- Files, folders and application data (for example Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint Server, MySQL) held on virtual servers in a Node4 data centre or on the Customer premises where the virtualisation platform is VMware vSphere or Microsoft Hyper-V;
- Data stored on endpoint devices such as laptops and desktop computers.

A different version of the software may be required for the backup of different types of data.

The Customer must install the software onto the operating system of each physical server, desktop or laptop that should be protected by backup and enter the credentials provided by Node4. For virtual machine backup, the software should be installed onto a physical or virtual machine that can communicate with the hypervisor and virtualisation management software (such as VMware vCenter). .

The software connects to Node4 infrastructure and backup data is transferred from that operating system to Node4 storage in a Node4 data centre. By default, data is stored on Node4 storage in a single off-site location only. Optionally, the Customer may request that this data is copied to a second location for an extra charge.

The Customer may specify a retention period for each system being backed up using the software application.

The Customer must purchase sufficient backup storage space in order to write backup data. This storage is sold at a price per gigabyte of data held in the backup repository (GB).

Data in the repository is calculated after compression processes have been applied. The backup software and backup storage do not perform deduplication.

Node4 recommends that the repository storage purchased is at least 100% of the size of the source data (typically the size of data 'used' on the file system) and that retention periods are limited to 30 days.

The Customer may decrease the amount of storage purchased if the space required is lower because a higher compression ratio has been achieved. The Customer cannot reduce this until at least one calendar month has elapsed since the first backup was taken.

The Customer is responsible to ensure they have sufficient space to perform backups. The software can be configured to issue automated e-mail alerts if the allocated quota of storage is starting to near full. If the Customer will not have sufficient space, they may reduce the retention period (in which case some old data is deleted) or purchase additional storage space. Backups will fail in the event that insufficient space is available.

The Customer creates a backup set for data that should be included in the backup and selects the data (such as e-mail mailboxes or file system folders) to backup. The Customer is responsible for operating and configuring the agent software that Node4 provides, including monitoring any alerts generated within it.

Node4 is responsible for ensuring that the backup repository service is operational to receive and send backup data to the software running in the Customer estate.

The server running the backup software must be able to communicate over the network and/or Internet with the Node4 repository. The Customer is responsible for ensuring network connectivity from the backup software to the Internet.

This component cannot be used for backing up Virtual Machines running on N4Cloud service, including those operating on the *Compute Resource (Dedicated)* component.

7. Service components – Build

7.1 Build: N4Cloud standard

This component is mandatory for all orders.

Node4 will perform the following before informing the Customer that the service is ready for use:

- Create a Customer account on the Self-Service Portals;
- Create an allocation (pool) of CPU, memory, storage as specified on the Order Form and agreed by Node4;
- Configure backup jobs for Virtual Machines using the *Storage with Virtual Machine Backup* component.
- Configure the portal to allow access by the Customer to provision their solution;

7.2 Build: N4Cloud advanced

This component is mandatory for all orders where the Customer is using the *Compute Resource (Dedicated)* component or a Disaster Recovery solution.

Node4 will perform one or more of the following additional activities before informing the Customer that the service is ready for use:

- Configure disaster recovery software to perform replication of Virtual Machines as required.
- Create an instance of the VMware vCenter software.
- Physically install compute nodes.
- Install the VMware hypervisor on the compute nodes.
- Join the compute nodes to the vCenter software and Self-Service Portals.

7.3 Build: Virtual machine provisioning

If specified on the Order Form, Node4 will provision Virtual Machines and install the operating system. A charge shall be levied for each virtual machine that is provisioned.

Node4 will not configure the operating system as part of this component other than the parameters needed in order to provision the virtual machine, such as an IP address and hostname.

Node4 will define a password at the time of provisioning which must be changed by the Customer after handover of the virtual machine to the Customer.

7.4 Build: Application installation (Windows)

If specified on the Order Form, Node4 will perform the installation of certain applications or software roles into the Microsoft Windows operating system of a virtual machine immediately after the *Build: Virtual Machine Provisioning* component and using the default credentials defined by Node4.

Installation is charged for every application in every virtual machine. The applications and software roles that are currently supported include:

- Microsoft Active Directory Domain Services (AD DS) – commonly known as installing a ‘domain controller’
- Microsoft Exchange
- Microsoft SQL Server

This component does not include the cost of any software licenses. Where a license is required, the Customer is responsible for ensuring sufficient licenses are available prior to installation. Node4 may install other applications at the discretion of Node4 and by prior written agreement.

7.5 Build: Application installation (Linux)

If specified on the Order Form, Node4 will perform the installation of certain applications or software roles into the Linux operating system of a virtual machine immediately after the *Build: Virtual Machine Provisioning* component and using the default credentials defined by Node4.

Installation is charged for every application in every virtual machine. The applications and software roles that are currently supported include:

- Apache web server
- NGINX web server
- MySQL database server

- Magento
- Drupal
- Wordpress
- Cpanel
- Plesk
- Webmin
- Zabbix

The list of supported applications and software roles may change from time to time. An updated list is available from Node4 upon request. Node4 may be able to provide support for applications or software roles that are not present on the list if requested by the Customer. This will be at the sole discretion of Node4 and subject to bespoke pricing.

This component does not include the cost of any software Licenses. Where a License is required, the Customer is responsible for ensuring sufficient Licenses are available prior to installation. Node4 may install other applications at the discretion of Node4 and by prior written agreement.

This component does not include any configuration of the software or patching of the application after installation.

8. Service components - Operate

Different operate models are available in order to provide increasing levels of service. Each incremental level includes the aspects defined, in addition to aspects included in preceding levels.

8.1 Operate Level 1

Node4 will perform a set of activities for the Node4 N4Cloud service infrastructure.

The Customer may request that Node4 does not perform one or more of the activities though this will not result in a price reduction.

The activities performed in this component are:

Monitoring

Node4 will monitor the Node4 infrastructure via the Node4 monitoring system to provide pro-active fault management up to the Hypervisor by Node4 during the contracted support hours.

As standard the following are monitored:

- device response time/device availability,
- interface statistics (utilisation & errors),
- CPU and Memory usage.

In the event the device stops responding, or a monitored threshold is exceeded, Service Desk will pro-actively investigate the issue during the contracted support hours.

Node4 will not monitor Customer Virtual Machines.

Incident management

Node4 will investigate and take reasonable commercial measures to resolve any service failure caused by the Node4 infrastructure. Incidents will be dealt with as described in section 10 of this document called "Incident Management".

Equipment used by Node4 to provide the service shall be covered by either a) hardware maintenance agreement that provides for repairs and replacement parts and/or b) the holding of spare parts which can be utilised by Node4 to restore service.

Software patching

Node4 will apply software updates and patches to the Node4 infrastructure when they are required due to software defect (bug) or security vulnerability.

The Customer will be responsible for software updates and patches to Virtual Machines.

Capacity management

Node4 will manage the N4Cloud service infrastructure to ensure there is sufficient capacity to meet Service Availability targets. Information regarding installed or active capacity of the infrastructure is not visible to the Customer.

Node4 do not provide capacity management of Customer Virtual Machines.

Customer support

Node4 will provide the level of support, identified on the Order Form and defined in section 10 below covering up to the hypervisor level only.

Backup job management

Node4 will set up automated monitoring of backup jobs for Virtual Machines running on the *Storage with Virtual Machine Backup* component. In the event that a backup job fails, a ticket is generated automatically and Node4 will investigate the cause and re-run the job. Node4 cannot guarantee that every backup will be successful. Whilst data is validated as part of the backup process, Node4 will not perform test restores of data or Virtual Machines unless by prior agreement for which a charge may be levied.

8.2 Operate Level 2

If specified on the Order Form, Node4 will perform the activities listed in this component for a group of Virtual Machines on N4Cloud service. The names of the Virtual Machines covered by this component should be captured on the Order Form and by default if this level is selected it should be selected for all Virtual Machines on the same platform.

This component is charged on a per virtual machine per month basis. All Virtual Machines that are dependent on each other must be included in the group. For example, both Virtual Machines for web servers and database servers used to deliver an application should be included in the same group.

The Customer may request that Node4 does not perform one or more of the activities though this will not result in a price reduction.

The activities performed in this component are:

Operating system management

Node4 will define and proactively monitor the following:

Metric	Measure	Priority	Thresholds
OS Availability	SNMP with ICMP failover	Critical P1	Offline after 2 cycles
CPU Average	SNMP	Minor P3	>90% after 3 cycles
CPU per Core Usage	SNMP	N/A	N/A
Physical Memory Utilization	SNMP	Minor P3	>90% after 3 cycles
Disk Space Usage	SNMP	Minor	>90% after 3 cycles
		Major	>95% after 3 cycles

Critical System Services – Windows	SNMP	Minor P3	Not running after 1 cycles
Critical System Services – Linux	SNMP	Minor P3	Not running after 1 cycles

Alerts will be generated in the event that pre-defined thresholds are breached. Thresholds will be set so that an alert is generated under normal circumstances before a 'critical' condition occurs.

Node4 will take action to diagnose the cause of the alarm and remediate the alarm condition where possible.

Node4 will require remote access to the operating system. Node4 may require that an agent is installed into the operating system in order to enable monitoring.

Incident management

In the event that an unplanned interruption to the normal operation of the:

- Operating system in a virtual machine is reported through monitoring alarms;
- Operating system in a virtual machine via notification from the Customer.

Node4 shall attempt to restore the service to normal operation on a reasonable commercial endeavours basis.

Incidents shall be handled by 1st line engineers in the first instance and appropriately escalated to 2nd or 3rd line engineers where appropriate.

Node4 will create a Service Ticket on the Service Desk system for each incident.

Service Tickets will be assigned a priority based on an assessment of impact, as determined at the discretion of Node4.

Node4 may offer advice on recommended actions to reduce the probability of Service Affecting Incident or incidents from occurring. If the Customer does not implement this advice, and the incident occurs frequently, Node4 reserve the right to cease responding to further occurrences.

All remediation work performed by Node4 will normally be performed using remote access technologies only. The Customer shall not prevent remote access to the Virtual Machines as this will prevent Node4 from assisting in the resolution of incidents.

Operating system patching

At an agreed frequency and during the maintenance window, Node4 will install critical patches into the operating system. Patches may require a reboot of the operating system which may result in downtime of the Customer Virtual Machines. This shall not be considered as downtime for the calculation of service levels or service credits. Where multiple servers are used for redundancy (for example a pair of web servers), the Virtual Machines shall be rebooted separately.

Operating system troubleshooting

Upon request, Node4 will help the Customer to troubleshoot issues with the operating system. Node4 will perform periodic reviews of event logs for critical alerts and investigate potential resolution.

All remediation work performed by Node4 will normally be performed using remote access technologies only. The Customer shall not prevent remote access to the Virtual Machines.

Operating system change management

Upon request, Node4 will work with the Customer to implement up to 5 Standard MAC or 150 minutes in total of changes to the operating system per month.

Additional Fees for changes will be subject to the Professional Services Fees defined in 3.3 for the following.

Node4 reserves the right to apply additional Fees if:

- a) Any Standard MACs above 5 or 150 minutes in total per month.;
- b) if the change fails and the Customer asks for additional troubleshooting rather than rollback of the change and/or
- c) the Customer requires these changes to be performed outside of normal working hours. Implementing changes outside of normal working hours shall be at the sole discretion of Node4 and by prior written agreement

only. For complex changes, or changes which require an implementation and/or rollback plan (specified at the discretion of Node4) that will allow service to be restored in the event the change is not successful

The implementation of changes by Node4 shall normally only be performed using remote access technologies. The Customer shall not prevent remote access to the Virtual Machines.

Object level recovery from backups

For Virtual Machines stored on the *Storage with Virtual Machine Backup* component, it is possible under normal conditions to recover individual items of data from Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint and Microsoft Active Directory without the need to restore the whole dataset.

Upon request, Node4 will perform up to two recoveries on behalf of the Customer per virtual machine per calendar month. Node4 will monitor the number of requests and should these be considered excessive, Node4 reserves the right to increase the Fees for the service.

The Customer is responsible for ensuring that sufficient detail is provided to allow for the data to be recovered to be quickly located – for example, the name of an e-mail, sender and folder in which it is located. The Customer may be required to join a screen sharing session with Node4 to assist in locating the data to be restored.

Disaster recovery invocation

Upon request, Node4 shall invoke virtual machine failover using the Disaster Recovery software.

Disaster recovery annual test

Upon request, Node4 shall invoke virtual machine failover using “test mode” in the Disaster Recovery software. This failover may be invoked for the platform up to a maximum of two times in any 12 calendar month period.

8.3 Operate Level 3

For more complex solutions, Node4 may propose a bespoke service that shall be defined in a separate Schedule Document and will incur additional Fees.

Typically this bespoke service may include the following types of activity for the Customer platform:

- Management of database & web server software
- Quarterly capacity planning
- Security assessments and counter-measures
- Automated configuration management
- Managed code deployment
- Application performance guidance
- Application monitoring

9. Additional services

It should be assumed that any activity or element of a service that is not described in this schedule is not provided as part of the N4Cloud service. Project work, other than that described, is specifically excluded from this service.

10. Incident Management

10.1 Incident handling

Incidents are handled as outlined as outlined in Node4's Incident Management Schedule Document.

10.2 Hours of support

The following table details the different Support Hours relating to the Support Level defined on the Order Form.

Support Level	Support Hours
Bronze	Standard business hours support 9am to 5.30pm week days, excluding bank and national holidays
Silver	Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Silver Plus	Priority 1 and 2 - Support hours between 7am and 7pm 7-days a week, including bank and national holidays, excluding Christmas day, Boxing day and new year's day

	Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays
Gold	Priority 1 and 2 - Support hours 24/7
	Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays

10.3 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.

10.4 Time to repair

Node4 aims to respond, update and resolve Incidents in relation to the Node4 Cloud service within the following times:

Priority	P1	P2	P3	P4	Service Request
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	30 Mins	2 Hours	12 hours if Resolve / Target to Fix exceeded		
Resolve / Target to Fix	4 Hours	8 Hours	12 Hours	36 Hours	60 Hours

All priority 1 & 2 Incidents should be raised via Service Desk system then followed by a phone call.

* 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.

10.5 Incident duration

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

11. Service credits

11.1 Compute resource (shared) availability

The component is considered available if all Hypervisor hosts hosting the Customer Virtual Machines are operating in a normal state.

If a Hypervisor node fails, and the Virtual Machines are migrated to another node, then downtime shall be considered as the time between a) the time the Hypervisor node is detected as no longer functioning and b) the time the Virtual Machines start to power on another host.

Availability levels apply to the Hypervisor platform and are not measured per virtual machine.

The following equation will be used to calculate the *Compute Resource (Shared) availability*. References to hours are to the number of minutes in the applicable Monthly Review Period:

$$\frac{((\text{Total minutes} - \text{Total minutes Unavailable}) / \text{Total minutes}) \times 100}{}$$

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

Service Availability	Service Credits as % of Monthly Rental Charge - Compute Resource (Shared)
<99.99%-99.85%	5%
<99.85%-99.7%	10%
<99.7%-99.5%	20%
<99.5%-99.0%	25%
<99%	50%

11.2 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 Customer on a quarterly basis.

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

The Customer must claim any service credit due to a failure to meet the Service Availability targets, in writing, within twenty one (21) Business Days of the date at which the Customer could reasonably be expected to become aware of such failure, otherwise no service credits shall be payable. The Customer 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 Customer, the Customer shall assist, and shall not be entitled to any service credits until Node4 has received all the information it has reasonably requested.

11.3 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 Customer 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 Customer, its employees, agents or contractors;
- The Customer failing to comply with the provisions of the Agreement;
- Any event described in Clause 11 (Force Majeure) of Node4's Terms and Conditions;
- Any Planned Outage.

Service credits are not applicable for more than one breach of any targets outlined in this document arising from the same occurrence.