SERVICE DESCRIPTION

Nimbus Virtual

RESTRICTIONS ON DISCLOSURE

Information contained and built within this services description remains the property of Thrive unless strict permissions to the contrary have been provided. Information shall not be released nor disclosed either in part or as whole without strict consent of Thrive. or otherwise in accordance with the General Terms and Conditions.

SERVICE SUMMARY

Nimbus Virtual is Thrives Infrastructure as a Service (IaaS), which provides the hosting of critical servers and applications out of Thrive's Tier 3+ Data Centres.

The Nimbus Virtual platform has been designed to conform to industry best practice, providing a total cloud separation between our supported client communities.

Our platforms are built with full redundancy and are patched and secured according to best practice guidelines. Our validated architecture provides enhanced levels of availability, security and resiliency to our clients.

This service is intended for enterprise business consumption and therefore is not a direct consumer-based service.

SERVICE DEFINITION

The Nimbus Virtual Infrastructure as a Service platform delivers secure hosting of virtual machines. As standard these virtual machines are hosted using a VMWare hypervisor. Virtual machines must be either Microsoft Windows or Linux operating systems and consist of the following components:

- CPU,
- RAM,
- Storage,
- Operating System.

Within Nimbus Virtual all virtual machines are grouped into securely separated virtual datacentres. Virtual datacentres consist of the following components:

- One or a group of virtual machines,
- Firewall,
- Connectivity,
- Self Service Web Access Portal.

SERVICE COMPONENTS

This section is comprised of a description of each of the components that make up the overall service.

Physical Data Centre

This component provides Tier 3 + hosting for the service including:

- Resilient Power,
- Resilient Cooling,
- Fire detection and suppression,
- 24/7 Physical Security,
- Resilient Connectivity.

Connectivity

This component provides the external connectivity into the Thrive datacentre facilities for the purpose of accessing the service. This can include:

- Dedicated customer links:
  - MPLS,
  - SD-WAN,
  - Point to Point,
  - Dedicated internet circuit,
  - VPN on Dedicated internet circuits,
  - SIP.
- Resilient Shared Thrive Provided Internet service,
- VPN on Resilient Shared Internet service.

Virtual Data Centre

This component is a securely contained pool of infrastructure resources required to run virtual machines as part of the service:

- Networking,
- Compute & Memory (CPU & RAM),
- Storage.

Networking

This component provides the secure private networking for each virtual datacentre and consists of the following:

- Dedicated, secure private networking between virtual servers,
- External connectivity to and from the virtual datacentre.

External Connectivity is provided via a virtual firewall. This includes all the methods described above in the connectivity section.

The service has a pre-defined range of firewalls delivered in the following options:

- Managed - Thrive Managed firewall with no customer access to the device. (Default option),
- Un Managed - A self-service firewall, all configuration will be the responsibility of the end customer.

Service/Feature	Managed	Un-Managed
Licence & vendor support	Yes	Yes
Installation / Deployment	Yes	Yes
Initial Configuration	Yes*	No
In Life configuration	Yes	No
Apply Software/firmware updates	Yes	No
Configuration backups	Yes	No
Monitoring, CPU Utilisation	Yes	No
Reporting	Yes	No
Moves, Adds, Changes, Deletions (MACD)	No**	No

*Includes limits of number of VPN's and firewall rules (reasonable use on a discretionary basis applies)
**MACD's Can be procured separately

Compute & Memory

This component provides CPU & RAM resources required to run the virtual machines as part of the service.

Storage

This component provides storage resources required to run the virtual machines and associated functions (e.g. snapshots) as part of the service.

Multiple tiers of storage are available and will be discussed during the design phase.

SERVICE SCOPE

This section details how the service is ordered, consumed and delivered.

How do I order the service?

The service is ordered by engagement with our design consultants whose role is to help design and right size the service to match your requirements and budget. The information gathered will be used to create a formal quote, leading to a contract and order.

What am I ordering?

The right-sized design will be an amount of CPU, RAM and Storage resource within a virtual datacentre with a virtual firewall and the required connectivity. The resource allocation can be varied to a minimum of 80% and a maximum of 200% of the resources specified in the Order Confirmation, Project Scope or Quotation.

How do I get setup on the service?

The service will be setup as per the ordered design. The following table shows the inclusions and exclusions along with roles and responsibilities:

Task	Included	Responsibility
vDC Creation	Yes	Thrive
Firewall Deployment	Yes	Thrive
Firewall Initial Configuration	Yes*	Thrive
VM Deployment from Template	Yes	TBC by Project***
VM Migration of existing servers	No**	N/A
Web Portal configuration	Yes	Thrive
Web Portal User Setup	No	Customer
Service Handover	Yes	Thrive / Customer

*If managed firewall procured
**Bespoke chargeable project carried out by Thrive – This would be scoped specifically to each individual customer requirement.
***Either Thrive or the customer has the ability to complete, this will be confirmed as to who carries out as part of migration/on-boarding project planning.

How do I access the service?

The service is typically accessed via the self-service web portal. An admin user logon for your company will be provided to access your pre-built vDC.

Once the service is live virtual machines can be accessed via alternative remote connectivity methods (e.g. RDP, SSH).

SERVICE DELIVERY

Service Availability

The service is available 24 x 7 x 365*.

*Excluding planned maintenance work. Planned maintenance work is any type of maintenance work that is not performed in response of a Problem or Incident reported by the Customer.

Where planned maintenance work is required, Thrive will provide a minimum notice of 14 calendar days.

In the event of urgent or immediate maintenance being required, Thrive may be unable to provide notice of 14 calendar days. In these circumstances, Thrive will seek to provide reasonable notice. This could be less than 24 hours, but Thrive will seek to provide a minimum notice period of 48 hours.

Support Scenarios

The service is supported by Thrive's Technical Assistance Centre (TAC). Contact details for the TAC will be detailed in the customer guide provided at the commencement of the service.

Thrive manages Problems, Incidents, Service Requests and Change Requests according to the ITIL framework.

Each call raised will be classified in advance of fault being assigned to the appropriate resource.

Below we have provided call definitions and priorities for incidents. These include our response times, and responsibilities.

These targets, while not contractual, ensure that Thrive strive to resolve incidents in a prompt and timely manner.

Priority	Receipt Confirmation	Engineering Response	Mean Time to Resolve Target
1	15 minutes	30 minutes	2 hours
2	15 minutes	30 minutes	4 hours
3	30 minutes	2 hours	8 hours

Incident Priority	Thrive Responsibility	Customer Responsibility	Examples
Priority 1 - Critical	Resource dedicated until resolution or a workaround has been implemented under emergency change.	Customer must align a resource for the duration of P1 outage. Provide all necessary remote access and support Provide assistance around internal policies such as change control.	Severely impacting or total loss of service.
Priority 2 - High	Resource dedicated until resolution or a workaround has been implemented under emergency change.	Customer must align a resource for the duration of P2 outage. Provide all necessary remote access and support Provide assistance around internal policies such as change control	Problems affecting part of the service being provided
Priority 3 - Medium	Resources available during TAC operational hours to support outage.	Support will be required on an ad-hoc basis including remote access and any internal process requirements	Service affecting but not of a serious nature

Problem Management

The objective of problem management as deployed by Thrive is to diagnose the root cause of incidents as required by incident management. Problem management is provided during TAC operational hours. It is also deployed to ensure that there are appropriate control processes in place to implement permanent fixes; these control processes include change management.

As part of our service in support of operations we maintain an in-house developed problem register which is managed by our problem management function. Problem management is responsible for the identification, management and resolution of all identified problems throughout the duration of its lifecycle.

Below is a table of common support scenarios for this service.

Scenario	Supported by default	Coverage	Type
Unable to power on existing virtual machine	Yes	24/7/365	Incident
Unable to deploy new virtual machine	Yes	9-5.30 Mon-Fri*	Incident
Creation/Deletion of snapshot	Self-managed	9-5.30 Mon-Fri*	Service Request**
Unable to create/delete snapshot	Yes	9-5.30 Mon-Fri*	Incident
Unable to modify virtual datacentre / virtual machine	Yes	24/7/365	Incident
Self-service portal is down	Yes	24/7/365	Incident
Unable to log on to self-service portal (forgotten password)	Self-managed	9-5.30 Mon-Fri*	Service request**
Unable to log on to self-service portal (other reason)	Yes	24/7/365	Incident
Unable to upload template/ISO	Yes	9-5.30 Mon-Fri*	Incident
Assistance with upload of template/ISO	Self-managed	9-5.30 Mon-Fri*	Service Request
Unable to access virtual machine(s)	Yes	24/7/365	Incident
Operating system is corrupted	No**	N/A	N/A
Recovery of virtual machine from previous state	No***	N/A	N/A
Poor Virtual Server Performance	Yes	24/7/365	Incident
Unable to access virtual machine console	Yes	24/7/365	Incident
Application Level Issues	No****	N/A	N/A

*Excluding England and Wales public holidays
**Would require a MACD Contract to carry out request
***Unless complementing service has been procured (OS support/Nimbus Data Recover)
****Would require Thrive additional Support Services contract (See the: Thrive Monitoring, Patching and Support Service Description)

Service Level and Key Performance Indicators

Within this section we detail service levels, KPIs and any associated statements relating to service credits.

The Service Levels for this service are based upon the Nimbus Virtual Datacentre (vDC) Availability. This is defined as the ability to run virtual machines within your virtual datacentre up to the currently allocated levels.

Description	Service Level
vDC Availability	100%

Virtual Datacentre Availability – Service credits

The following Service Level and Service Credits are applicable in respect of the number of minutes in a calendar month the virtual datacentre is unavailable:

vDC Unavailability (per month)	Service Credits
0 to 60 minutes	10
60 to 120 minutes	15
120 to 180 minutes	20
Over 180 minutes	25

Connectivity – Service Credits

Resilient Connectivity Services

Where the customer has elected for Thrive to provide resilient connectivity services as an integral part of the Nimbus service the following Service Level and Service Credits are applicable in respect of the number of minutes in a calendar month that Connectivity to the Nimbus Service is not available.

Connectivity Unavailability (per month)	Service Credits
0 to 60 minutes	10
60 to 120 minutes	15
120 to 180 minutes	20
Over 180 minutes	25

Thrive resilient connectivity services are designed so that in the event of an outage of a single circuit, re-convergence of networks will take place onto the back-up circuit. There will be a known and expected period of downtime whilst this re-convergence takes place. In this instance only, the first five minutes of downtime following the circuit failure is excluded from any service level measurement.

Non-resilient Connectivity Services

Where the customer has elected for Thrive to provide Connectivity Services over a single bearer or carrier link as an integral part of the Nimbus service the following Service Credits are applicable in respect of the number of minutes in a calendar month that Connectivity to the Nimbus Service is not available:

Fibre Ethernet

Fibre Ethernet Unavailability (per month)	Service Credit
6 hours or less	0
6 to 10 hours	3
Over 10 hours	8

Copper EFM

Copper EFM Unavailability (per month)	Service Credit
8 hours or less	0
8 to 30 hours	3
Over 30 hours	8

Where the customer has elected to provision their own connectivity service to access the Nimbus Service, no service credit will apply.

Notes

The minutes that the virtual datacentre is unavailable each month do not need to occur consecutively in order to give rise to service credits.

A Service Credit is defined as 1% of the Price payable in a calendar month, for the specific Client Service or Services, which have not met the defined Service Level. For clarity if the customer has elected for a resilient connectivity service as part of the Nimbus Service, any Service Credits due for unavailability of the connectivity services will apply to the Price Payable in a calendar month for the complete Nimbus Service.

A maximum of 100 Service Credits can be claimed in one calendar month. Service Credits can only be claimed for the calendar month in which they occur and cannot be rolled into subsequent months.

All Claims for Service Credits must be initiated by the Client to Thrive's Representative in writing.

The Client will have 30 Working Days from the receipt of a Monthly KPI report of the month in which the event occurred to claim for Service Credits.

All claims for Service Credits must be supported by the appropriate Monthly KPI report.

Where Service Credits claims are not made within the notified period no Service Credits will apply.

Applicable Service Credits will be paid one month in arrears in the form of a credit note, which can be set off against the Client's next monthly invoice. If the Service Credits relate to the final months of the Contract, the credit note will be paid within 30 days of receiving a valid claim for Service Credits of the Client.

Clients will have 30 Working Days to query any Service Credits issued. Where supplementary Service Credits are due, these will appear on the following monthly invoice.

Where Thrive inadvertently issues an overpayment of Service Credits, Thrive reserves the right to have these refunded. This will take place on the following monthly invoice after notification to the Customer.

The Service Credit shall be the sole financial remedy to the Customer in respect of the unavailability of Services.

Service Level agreements will be subject to section 14.1 force majeure contained within Thrive General Terms and Conditions. Service Credits will not be invoked in the event defined within force majeure including: war, strike, riot, crime, act of God etc. The optional Site Recover products have been designed to be utilised in such an event.

Service Delivery Management

Reporting

Clients will be provided with a report by the 2nd working day of each month including the following elements for the preceding month.

- vDC Performance Report – performance overview of your virtual datacentre,

- Snapshot Report – lists currently provisioned snapshots of VM's with their age and size,

- Under provisioned VM Report – details VM's showing a lack of resources that would benefit from an increase.

Reviews

Clients will be provided with a quarterly review with a service delivery manager. Logistics to be agreed at the start of a contract.

MACD

MACD (Moves, Adds, Changes & Deletions) are mostly achievable by the admin user via the self-service portal. Thrive can carry out any of the changes below for an additional charge. Each MACD request is charged at £75 per request and the written authorisation of the Customer will be required to carry this out. The payment for this will be added to the next monthly invoice.

The below table defines the MACD service level target

Definition	Priority	Receipt Confirmation	Engineering Response	Request Fulfilment
MACD	4	30 minutes	2 Working Days	5 Working Days
Service Cover Period	09:00 to 17:00 Monday to Friday (excluding public holidays).			

Included MACD (Moves, Adds, Changes & Deletions) are defined as per the following table

Change
Creation / Deletion of snapshots on a virtual machine
Deployment of a virtual server from an existing defined template
Removal of an existing virtual server
Add / Remove of a virtual server
Deployment of a virtual server from a packed OVA/OVF template (not achievable by self-service portal)
Allocation pool adjustment

NIMBUS OPTIONS

To complement the Nimbus Virtual Service, Thrive have available and recommend the following:

Nimbus Virtual Data Recover- Server and application level item recovery from backups stored within our data centres.

Nimbus Virtual Site Recover Premium – Continuous based replication, geo-redundant copies of running virtual servers to Thrive's secondary data centre for increased resilience for critical servers and applications.

Nimbus Virtual Site Recover Standard – Schedule based replication, geo-redundant copies of running virtual servers to Thrive's secondary data centre for increased resilience for critical servers and applications.

Microsoft Operating System and Application Support - Monthly updates, security patches, service and performance monitoring for Microsoft operating systems.

BUSINESS OPERATIONS

Billing

How do I receive my bill?

All invoices will be sent monthly in arrears for the service, the logistics for the delivery will be agreed at the commencement of the contract.

Renewal

How do I renew an existing service?

Within 12 months of the end of your existing contract term, our design consultants will re-engage with you to help confirm the design and right-size the service to match your requirements and budget. The information gathered will be used to create a formal renewal quote, which may lead to a new order.

Termination

How do I exit the service?

The following process flow describes the standard zero cost Nimbus Virtual exit process.
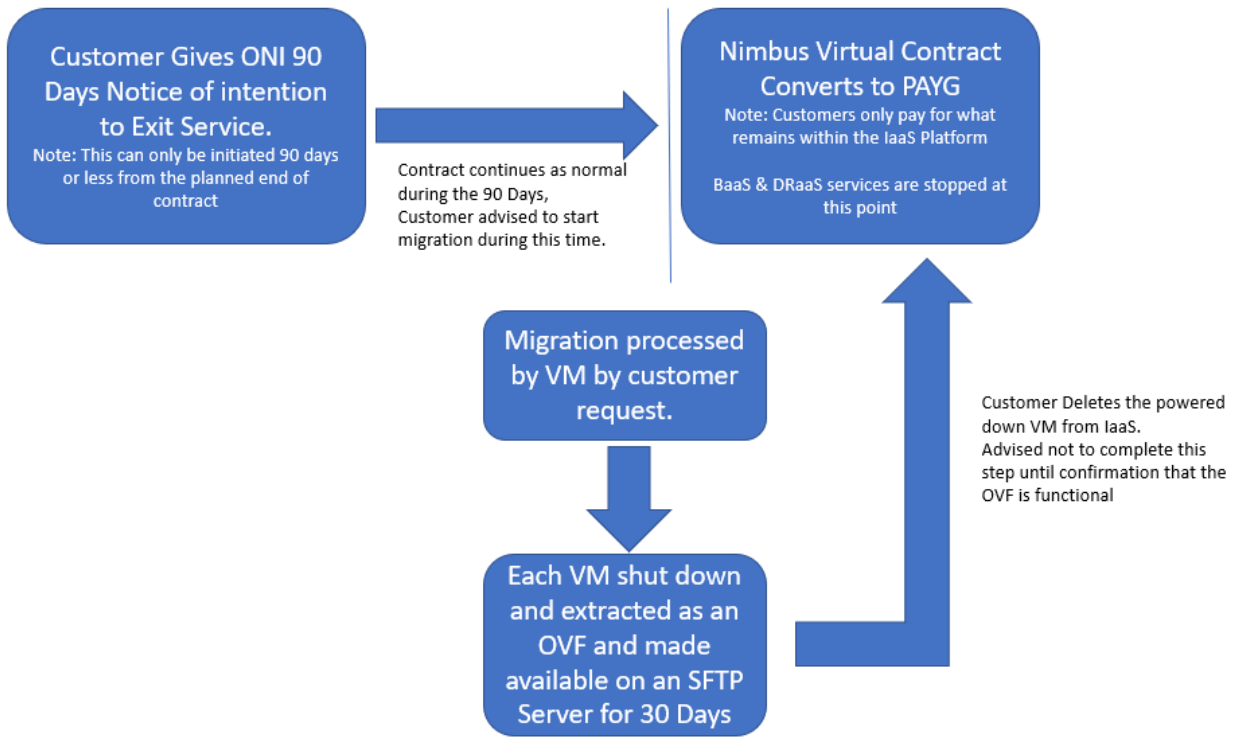
A Chargeable Bespoke exit process is also available, to be discussed as required.

CONTINUOUS SERVICE IMPROVEMENT

Service Annual Review

Review of the service will be conducted annually. The service owner is accountable for initiating this review and managing and initiating continuous improvement opportunities through to a successful conclusion.

FAQ

What is included in standard setup?

- A WebEx based kick-off meeting to validate client information and to define setup criteria,
- Service Provisioning, including,
    o Firewall setup
    o Virtual datacentre setup
    o Connectivity
    o Windows server templates
    o Reporting setup
    o Portal logon details

The above items will be agreed as part of the design phase

How does a customer migrate to the service?

Any migration onto Nimbus virtual is not part of standard setup. This would be a separate project and charged accordingly depending upon requirements.

As part of the migration project Thrive shall provide the Customer all reasonable information in order to enable the Customer to migrate to the service.

What is the Thrive Self Service Web Portal?

The Thrive Self Service Web Portal is a management interface whereby you can perform several management tasks related to the service. This includes common tasks such as:

- vDC modification
- Console access to virtual servers
- Snapshots
- Power on/off
- Deployment of new virtual servers