THRIVE℠

SERVICE DESCRIPTION

Nimbus Data Recover

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 Data Recover is Thrive's Backup as a Service (BaaS) offering that provides one or more of the following managed options:

Option 1: Backup and recovery of servers hosted within Thrive's Nimbus Virtual cloud infrastructure. This option is referred to as ***Nimbus Virtual Data Recover***

Option 2: Management of a customer on premises Veeam backup and replication environment. This option is referred to as ***Nimbus Data Recover***

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

Nimbus Data Recover is a Backup as a Service solution that delivers secure and reliable protection of workloads located on virtual and physical machines. These machines can be either located at Thrive's datacentre and hosted within our Nimbus Virtual Service or located on your premises and managed by ThriveI as part of a managed service.

Option 1 - Nimbus Virtual Data Recover

Nimbus Virtual Data Recover provides a managed backup and recovery service for cloud servers hosted within Thrive's datacentre.

This Service, once provisioned, will provide assurance that on demand critical data and systems will be available to be restored. This is achieved by storing backup data at the primary DC site, with a copy also located at the secondary DC site.

Option 2 - Nimbus Data Recover

Nimbus data recover provides a managed backup service for customers who are running a Veeam Backup & Replication environment outside of Thrive's Nimbus Virtual service.

This service provides day to day monitoring, support and maintenance of backup and restore jobs to ensure that should you require it, your critical data is available for recovery as required.

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.

*Only applicable where backup data is hosted at Thrive's datacentres.

Connectivity

This component provides connectivity related to the service and is dependent on the service option being delivered:

Option 1 - Nimbus Virtual Data Recover

- Resilient DCI connection between the Thrive primary and secondary datacentres for the purpose of delivering a secondary offsite copy of backup data.

Option 2 – Nimbus Data Recover

Only applicable where backup data is hosted at Thrive's datacentres

- Cloud Gateways (optional),
- WAN Acceleration* (optional).
- Thrive Resilient Internet Connectivity (optional),

*Veeam Enterprise or Greater licensing required.

Storage

This component provides a storage repository for Veeam based backup data. The size and location of the storage repository will be dependent on the option taken and fully designed by Thrive's technical team.

Licensing

This component provides any relevant Veeam licensing required to deliver the service. Multiple licensing options are available and will be determined based on individual design. Considerations will be taken around perpetual licensing, service provider licensing and the relevant versions.

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?

Depending on the option(s) selected:

Option 1 – Nimbus Virtual Data Recover

A fully managed backup & recovery service protecting virtual machines located inside Thrive's Nimbus Virtual Cloud infrastructure. The standard offering comprises of the following elements:

- 2 copies of backup data across different physical locations,
- Backup job creation,
- Backup job scheduling,
- Backup repository,
- Backup job monitoring & alerting*,
- Service reporting,
- Restoration of VMs and files**.

*notification on error which will be internally reviewed and may result in an open service ticket.

**Service includes 25 restore request tickets per annum (additional MACDs available as a chargeable request)

Option 2 – Nimbus Data Recover

A fully managed backup & recovery service using Veeam to protect physical & virtual machines located outside Thrive's Nimbus Virtual Cloud infrastructure. The standard offering comprises of the following elements:

- Backup job creation,
- Backup job scheduling,
- Backup repository (optional),
- Backup job monitoring & alerting*,

- Service reporting,
- Restoration of VMs and files**,
- Offsite Nimbus Veeam Cloud Connect copy (optional).

*notification on error which will be internally reviewed and may result in an open service ticket.

**Service includes 25 restore request tickets per annum (additional MACDs available as a chargeable request)

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	Option 1 or 2
Installation & Initial Configuration of Veeam	No*	Thrive / Customer	2
To determine backup job selections (what to include/exclude). Agreed at contract start point then amended via change control request.	Yes	Customer	Both
Definition of schedule per backup. To be agreed at contract start point then amended via change control request.	Yes	Customer	Both
Definition of retention policy per backup job if different from default GFS retention. To be agreed at contract start point then amended via change control request.	Yes	Customer	Both
To schedule backup jobs in line with agreed requirements.	Yes	Thrive	Both
To provide scheduled reports of backup/success failures.	Yes	Thrive	Both**
To notify service provider of any application or server issue that may cause backup jobs to fail or not complete successfully	Yes	Customer	Both
To notify service provider of any moves, additions, changes or deletions (MACD's) to backup configuration for either job selection, schedule or retention policy.	Yes	Customer	Both***

To notify the customer of any planned maintenance that could impact the service.	Yes	Thrive / Customer	Both
To request restores (in line with file restore service)	Yes	Customer	Both
To perform restores (in line with file restore service)	Yes	Thrive	Both

*Thrive can complete as a separate chargeable project.
**Veeam ONE of Veeam Availability Suite required for Option 2.
***Failure to notify could result in unexpected failures, which will affect the SLA of certain components.

How do I access the service?

There is no direct access to the service as this is fully managed via Thrive's Technical Assistance Centre (TAC).

Upon contract commencement of the service a welcome pack will be issued with details on how and when to contact Thrive's TAC with regards to service related items.

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 in the welcome pack 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	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
Backup failure	Yes	24/7/365	Incident
Restore request	Yes	24/7/365	Service Request
Application level support	No	N/A	N/A
Reporting not working as expected	Yes	9-5.30 Mon-Fri*	Incident
Job creation/modification	Yes	9-5.30 Mon-Fri*	Service Request
Veeam Application Issues	Yes	24/7/365	Incident
Bare Metal Restore request	No*	9-5.30 Mon-Fri*	Service Request**

*Excluding England and Wales public holidays.

**To be scoped and defined as required.

Service Level and Key Performance Indicators Service Delivery

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 data restore commencement. This is defined as the maximum time from an acknowledged restore request. This is achieved when a TAC ticket is logged with Thrive and an acknowledgment sent to the customer.

Thrive runs with dual service levels depending on if the request was received during core business hours or outside of this time. These service levels are defined in the below table:

Description	9-5.30 Mon-Fri*	Non-Core Business Hours
Data restore commencement	≤2 Hours	≤ 4 Hours

*Excluding England and Wales public holidays, these will be treated as non-core business hours

Data Restore Commencement – 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:

Service Credits	9-5.30 Mon-Fri*	Non-Core Business Hours
10	2-3 Hours	4-5 Hours
15	3-4 Hours	5-6 Hours
20	4-5 Hours	6-7 Hours
25	>5 Hours	>7 Hours

*Excluding England and Wales public holidays, these will be treated as non-core business hours

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.

Service Delivery

Reporting

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

- Backup success over the preceding month*.
- Restore success over the preceding month*.

*If option 2 taken, Veeam ONE or Veeam Availability Suite (VAS) is required for reporting.

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 (Moves, Adds, Changes & Deletions)

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
Restore MACD	2	15 minutes	≤ 2 hours*	Variable**
Other MACD's	4	30 minutes	2 Working Days	5 Working Days
Service Cover Period	09:00 to 17:30 Monday to Friday (excluding public holidays).			

*In line with data restore commencement SLA 9-5.30 Mon-Fri (≤ 4 hours for non-core business hours).
**Dependant on size and type of restore.

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

Change
Additional restore request over and above the inclusive limit
Additional servers added/removed to/from backup service*
Changes to backup schedules & retention policies*
Backup infrastructure actions in line customer changes (e.g. adding additional proxy server) **

*May incur additional service costs, restrictions may apply in line with service contract.
**Option 2 service only.

Nimbus Options

To complement the Nimbus Data Recover Service, Thrive can offer the following additional services:

Nimbus Virtual – Infrastructure-as-a-Service cloud hosting, delivered from Thrive's UK base tier 3+ datacentre.

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.

Nimbus Veeam Cloud Connect - Secure cloud repository service, providing simple and cost-effective off-site backup.

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 6 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 describes the standard zero cost Nimbus Data Recover exit process.

Option 1 - Nimbus Virtual Data Recover

- Customer gives Thrive 90 days' notice of intention to exit the service
- On request, Thrive will upload up to 50TB of backup data in a Veeam format to an FTP server for retrieval by the customer. Data will remain on the FTP server for an agreed period dependant of the size of the data set*.
- Once the termination period is reached, any remaining data held within the storage repository will be securely erased by Thrive.

*Backup data more than 50TB will require customer provided storage and engagement with Thrive professional services at an additional cost.

Option 2 – Nimbus Data Recover

- Customer gives Thrive 90 days' notice of intention to exit the service
- Where backup data is hosted at Thrive's datacentres: On request, Thrive will upload up to 50TB of backup data in a Veeam format to an FTP server for retrieval by the customer. Data will remain on the FTP server for an agreed period dependant of the size of the data set*.
- Once the termination period is reached, any remaining data held within the Thrive storage repository will be securely erased by Thrive.

*Backup data more than 50TB will require customer provided storage and engagement with Thrive professional services at an additional cost.

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 set up of backup jobs, schedules, retention etc. See section 5.3.

How am I notified on backup successes & failures?

Backup notifications will be sent on a “failure only” basis. This means that an email notification will only be sent if the backup task did NOT complete successfully.

The notifications will be delivered to a pre-determined email address.

How are service tickets raised for backup failures?

Backups can fail for multiple reasons. Thrive provides a managed backup service. Therefore, Thrive will investigate all warnings and errors for all backup sets.

A ticket will be raised when a backup has failed and will remain open until a successful backup has been achieved.

Is my data secure?

Yes, as standard Thrive require that all backups must be encrypted. Our service uses 256-bit AES with a 256-bit key length in the CBC-mode.

The encryption password is securely stored in a password vault in line with Thrive’s security information policy as part of BS27001.

As this is a managed service, the customer has no need to access the password. The exception to this is on contract termination or service exit where the customer has requested access to their backup data.

Are application consistent backups included by default?

No, Thrive are an infrastructure service provider. As such this service delivers full server backups only by default. Should a customer require specific application backups, discussions can take place as part of the design process on how/whether this can be accommodated.