PROACT

Service Definition Document

Backup as a Service

SDXBK-001 Published 19 June 2017

Public - Freely Distributable

Acknowledgements

CommVault and Simpana are registered trademarks or trademarks of Commvault Systems, Inc. in the United States and-or other countries.

EMC and VNX are registered trademarks or trademarks of EMC Corporation in the United States and-or other countries.

ITIL® is a registered trademark of AXELOS Limited. All rights reserved

Linux ® is a registered trademark of Linus Torvalds administered by Linux Marks Foundation

Microsoft and Windows are registered trademarks of Microsoft Corporation

NetApp® and SnapShot are registered trademarks and-or trademarks of NetApp, Inc., registered in the U.S. and/or other countries.

VMware® are vSphere® are registered trademarks and-or trademarks of VMware, Inc.

Any other brand or product trademarks (registered or otherwise) referenced within this document – but not explicitly acknowledged here – are the intellectual property of their respective holders and should be treated as such.

Phone: +46 (0)8 410 666 00
Fax: +46 (0)8 410 668 80
Email: info@proact.eu
www.proact.eu

Proact IT Group AB
Kistagången 2
Box 1205
SE-164 28 KISTA

PROACT

Contents

Chapters

1 Service overview **1**
2 Service scope **3**
3 Available service levels **13**
4 Service deliverables **14**
5 Service transition **20**
6 Service charging policy **22**
7 Additional services **23**
8 Service demarcation **24**
Glossary **25**
Appendices ..... **I**
Appendix A: Supported devices and applications II
Appendix B: Technical limits and constraints V
Appendix C: Self-service management portal functionality IX
Appendix D: Data deletion and extraction X

Tables

Table 1: Available service level measures 13
Table 2: Service charging-model 22
Table 3: Service change options 23
Table 4: Local vault sizing V
Table 5: Local vault server specification V
Table 6: Agentless Proxy Spec VI
Table 7: NAS Agent Local Proxy Spec VII
Table 8: SAN Agent Local Proxy spec VIII
Table 9: Source-side de-dupication cache sizing VIII

Figures

Figure 1: BaaS architecture schematic 2
Figure 2: Stage 0-6 transition model 20

PROACT

1 Service overview

Proact's Backup as a Service (*BaaS*) solution provides a remote backup solution that enhances traditional options with inbuilt resilience and robust *ITIL*® based support and service management processes.

Proact BaaS is available in three storage configurations:

- *Remote Only* – Minimise storage footprint – store backups offsite
- *Remote & Secondary* – Minimise storage footprint and maximise resilience– replicate off-site backups to two locations.
- *Local & Remote* – Minimise storage footprint and maximise recall speed – replicate local backups off-site

Secure

- Data backed up to a secure ISO 27001[1] certified Proact datacentre
- All data – in-flight and at rest – is encrypted
- All data remains within the Proact datacentre's national boundary, assuring data sovereignty
- You retain full control through a Self-service management portal (Simpana).
- End of term data handback or deletion policy

Available

- Highly-available storage capacity:
- 24x7x365 infrastructure support from Proact Service Desk located in an ISO 27001[1] certified Proact National Operation Centre (*NOC*)
- 24x7x365 Proact Service Desk monitoring the customer's backup data.
- Added resilience of off-site storage in a Remote vault and (optionally) Secondary vault.

In all configurations the solution:

- Stores encrypted customer data in a secure ISO 27001 accredited Proact datacentre in accordance with defined storage policies.
- Transfers data using encrypted links
- Employs de-duplication and compression techniques for security and efficiency
- Helps balance growing storage footprints against the need for data security and resilience.

Flexible

Data can be stored in one of three configurations:

- Remote Only – for offsite for protection
- Remote & Secondary – mirrored to a separate location for added resilience
- Local & Remote – onsite (in a managed Local vault) and offsite for speed of recall and resilience.

Flexible storage retention policy.

Proact perform data restores on receipt of a customer's restore request submitted through the Self-service support portal or direct to the Proact Service Desk.

Files can be restored to the original location, or to a different location, by agreement. Restores use *Local vault* copies (where they exist) to minimise restore time.

What is the charging policy?

Cost are per GB (Gigabyte) of data to be stored.

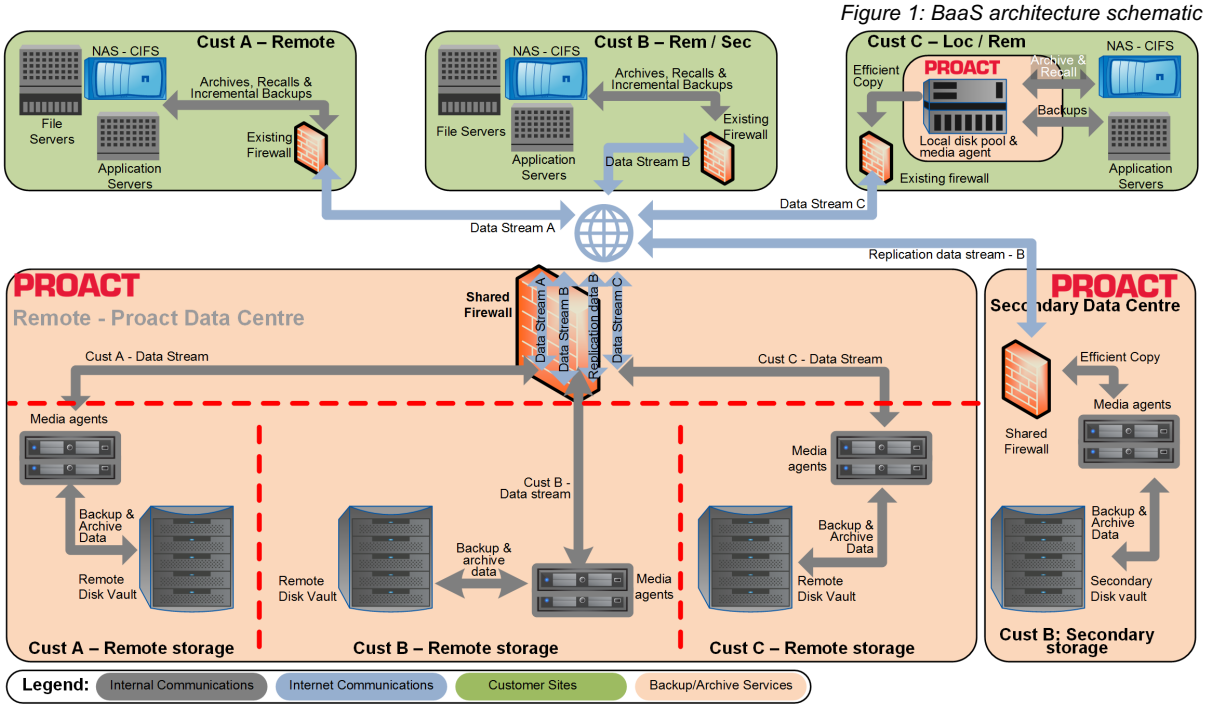
Vendor terms

This service is subject to vendor terms, which customers can view in full at these links:

http://www.proact.eu/terms/vendor

[1] ISO27001-certified Datacentres and *NOCs* are available in selected Proact delivery countries only

Figure 1: BaaS architecture schematic



2 Service scope

This chapter identifies and describes the high-level components that make-up the service, which comprise the:

- Service package – which defines the service, capabilities and options.
- Service platform infrastructure - which defines the service delivery mechanism, such as:
  - Service architecture
  - Backup components
  - Connectivity
  - Applications and licensing
- Supporting services - any processes or resources that support the delivery of the service, such as the Self-service support portal, through which the customer's authorised users can log cases and change requests.

Further information …

See Service deliverables (Chapter 4 on page 14) for more detail on the components.

2.1 Service package

Objective	To provide a remote backup solution that enhances traditional options with inbuilt resilience and robust ITIL based support and management processes.
Hosted-in	A Proact datacentre on a secure multi-tenant platform. Proact's ISO 27001 certification assures security.

Supported backup targets	▪ Servers
	  ▪ Microsoft Windows & Microsoft Windows Server
	  ▪ Linux (CentOS, Debian, Fedora, Gentoo, OpenSuSE, Oracle Linux, RedHat, Scientific Linux, SuSE, Ubuntu)
	  ▪ Solaris
	▪ Hypervisors (for agentless virtual server backups)
	  ▪ VMware ESX/ESXi
	▪ Storage devices
	  ▪ EMC VNX
	  ▪ IBM N-Series
	  ▪ NetApp – FAS
	▪ Applications
	  ▪ Lotus Notes
	  ▪ Microsoft Active Directory
	  ▪ Microsoft Exchange
	  ▪ Microsoft SharePoint
	  ▪ Microsoft SQL
	  ▪ Oracle
	For a full list of supported versions, see Appendix A: Supported devices and applications (on page II)

Supported-from	All support and management is delivered remotely from a secure, accredited *Proact National Operations Centre (NOC).*
Support level	Monitoring, support and service management of the infrastructure only.
Required connection types	All connection is by encrypted (HTTPS/SSL/TLS) public internet links using existing shared firewalls.
Engagement	▪ Use the Proact Self-service management portal – see Appendix C: (on page IX) – to monitor and manage backup activity, including initiating restores ▪ Use the Proact Self-service support portal to carry out data restores ▪ Proact Service Desk will restore data as part of the managed service on receipt of a customer restore request.

Complementary services	You can combine BaaS with other Proact service offerings – Ch. 7 (on page 23) – such as Proact Disaster Recovery as a Service (DRaaS) or Proact Infrastructure as a Service (IaaS)
Service architecture options	
Available Architectures	▪ Remote Only ▪ Remote & Secondary ▪ Local & Remote
Remote Only architecture	▪ Backups are taken directly from the customer's devices over the public internet to a dedicated Remote Vault in Proact's datacentre ▪ Proact provide the customer with storage capacity in line with the contracted backup capacity. The capacity is provisioned from Proact's multi-tenant shared remote vault in a Proact datacentre ▪ Proact provide the customer with the software infrastructure (for example CommVault Simpana) at the Proact datacentre to manage the backup process and perform restore requests
Remote & Secondary architecture	▪ Backups are taken directly from the customer's devices over the public internet to a dedicated Remote Vault in Proact's datacentre ▪ Proact provide remote capacity as above ▪ Proact provide secondary storage capacity in line with the contracted backup capacity in a second Proact datacentre, for resilience. ▪ Proact configure daily replication between the remote and secondary storage using (for example, Dash Copy technology) over Proact's inter-datacentre communications links
Local & Remote architecture	▪ Backups are taken locally from the customer's devices to a Local Vault - an onsite backup store which Proact installs at the customer's site to provide a local copy of the data, delivering a quicker restore time and resilience. ▪ Proact provide remote capacity as above ▪ Proact configure daily replication between the local and remote storage vaults using (for example, Dash Copy technology) over encrypted (HTTPS/SSL/TLS) internet links ▪ Proact provide, install and configure a remote monitoring hub on the customer-site(s) to provide monitoring information on the local vault
Service capabilities	

Backup policy	▪ Proact offer flexible backup policies, configurable per backup target, to meet the customer's contracted requirements (within the operating parameters of the product). The default policies are:
	  ▪ Server & Application Backup – a weekly synthetic full backup plus six daily incremental backups
	  ▪ Storage Backup – initial full backup plus daily incremental forever backups
	▪ The incremental-forever and synthetic-full backup solution provides efficient use of backup capacity

Retention policy	▪ Proact configure and maintain a flexible retention policy configuration to meet the customer's contracted retention requirements (within the operating parameters of the product and consistent with the contract term). Note: The managed service contract only commits Proact to retaining data in line with the policy configuration while the managed service contract is current and does not commit to retain the data after the contract ends. See also: Appendix D: Data deletion and extraction (on page IX) Exclusion 1: Retention of backup data after the contract termination date

Data replication	▪ Replication uses DASH copy [2] source-side data de-duplication, which: ▪ Replicates only changed blocks (using finger-printing) from the clients once the initial full backup operation (that is, data seeding) is complete ▪ Ensures efficient use of storage capacity and replication of data over the internet. ▪ Requires a local de-duplication cache to store the source side de-duplication data – see Appendix B.1.5: (on page VIII) ▪ Runs on each agent and local proxy server (*Remote Only* and *Remote & Secondary*) or on the Local vault server only (*Local & Remote*). Replicates data daily to the Remote vault.
Self-service management portal	The customer is provided use (via the internet, or locally) of a Self-service management portal to view and-or manage backup activities, including: ▪ User management ▪ Client auditing and settings ▪ Job configuration ▪ Job history and status (active jobs) ▪ Retention policy management ▪ Recovery of data See also: Appendix C: Self-service management portal functionality (on page IX)
Backup methods	
Server backups	▪ The solution provides both agent-based and *agentless* models, but agents must be used with physical servers and where the data must be made *application consistent* ▪ For agent deployments a *backup agent* (Virtual server agent) is installed within the *host OS* ▪ To avoid potential conflict between backup applications, the customer should remove any existing backup agents from each backup target See also: Hypervisor Agentless backups (on page 20) Prerequisite 1: Remove existing backup applications
Hypervisor Agentless backups	▪ Agentless operation is available for Windows and Linux VMs running on a VMware vSphere farm, with Hypervisor versions listed in Appendix A: Supported devices and applications (on page II) ▪ The agentless option removes the need for a backup agent to be installed in each guest ▪ Each VMware vSphere deployment at each site requires a Virtual Server Agent Proxy Server (Proact-provided VM, running on the customer's hypervisor). ▪ This requires the customer to provide compute capacity on each vSphere cluster to run the VSA Proxy Server, in line with specification given in Agentless proxy VM specification (App B.1.2:, on page VI) ▪ The VMware guest operating systems to be backed up must be running the latest version of VMware tools for hypervisor agentless restores to take place. ▪ Reduces storage requirements – no agents, nor local de-duplication cache (the agentless proxy serves as a cache for all virtual servers) Note: Not available with application consistent backups or on physical servers Responsibility 1: [Agentless] Ensure VMware OS running latest version of VMware tools

[2] Deduplication Accelerate Streaming Hash

Application consistent backups	▪ Application agents must be used if the data requires application consistency. These agents:
	  ▪ Ensure application consistency where the source data demands it (for example, a SQL database)
	  ▪ Minimise the rate of backup data change compared to flat file backups, which may otherwise have an adverse impact on replication performance
	  ▪ See Appendix A: (on page II) for supported devices
	▪ File system agents must be used to back up OS files when application agents are used for application data.
	
	Exclusion 2: The solution does not support flat file dumps of application data
	Exclusion 3: The solution does not support application consistency with agentless backup

Storage Array backups (NAS data)	▪ The *Storage Array Backup - NAS Data method* :
	  ▪ Backs up CIFS and NFS file data such as shared areas and home directories
	  ▪ Uses a NAS agent running on either the Local Vault Server or a NAS Agent Local Proxy Server (for solutions other than the *Local & Remote* option)
	▪ Storage arrays offering non-Windows based CIFS NAS functionality can be backed up using the CIFS protocol
	▪ NFS data backup is supported only for NFS data configured in *mixed-mode* when the CIFS protocol can be used to access the file data (neither *LUN*s nor *VMDK*s are supported).
	▪ The customer must provide appropriate credentials to access the NAS by the NDMP and a user with access to the CIFS data and is part of the “Backup Operators” group
	▪ Where antivirus is configures on the NSA storage array, a duplicate set of CIFS shares must be created with antivirus scanning disabled. This prevents the Anti-Virus engine intercepting the backup data transfers and unnecessarily prolonging the run time.
	  ▪ For example, on NetApp storage arrays, the duplicate shares should be created with the “`-novscan`” option enabled.
	
	See also Appendix B.1.3: (on page VII) – NAS Agent Local Proxy Server minimum specification
	
	Exclusion 4: NFS data backup where NFS not configured in mixed-mode with CIFS access
	Prerequisite 2: [NAS] Provide NAS credentials
	Prerequisite 3: [NAS] Create duplicate CIFS shares with antivirus scanning disabled

Storage Arrays backups (SAN data)	▪ The *Storage Array Backup - SAN Data method:*
	  ▪ Uses agents to back-up servers with storage on a SAN (for example, NetApp).
	  ▪ Uses a SAN agent running on either the Local Vault Server or a SAN Agent Local Proxy Server (for solutions other than the *Local & Remote* architecture)
	▪ The agent:
	  ▪ Uses SAN-based SnapShots for backups where applicable
	  ▪ Requests the storage array take an application consistent backup using Storage array SnapShots
	  ▪ Mounts the SnapShot and replicate the data to the backup vault.
	▪ Restoration of data is always to a pre-existing LUN. If the entire LUN is lost, the customer must enable restore by creating and mounting an empty LUN on the server.
	▪ Where a storage vendor's application consistency backup tools are used for DR (for example NetApp SnapManager for SQL), the customer must:
	  ▪ Configure the vendor's tools to operate in "copy-only" mode, resulting in application consistent backups that do not truncate the logs or update the applications catalogue. This allows Proact's BaaS to fully manage the backup and log truncation.
	  ▪ Minimise the risk of both the BaaS backup and SnapShot agents running at the same time by setting the RPO of the each to be a maximum of 8 hours (this allows an alternating schedule of 4 hours between the BaaS backup and SnapShot backup).
	▪ The SAN Agent Local Proxy server(s) (or the Local Vault, for *Local & Remote* deployments) require access to the same storage networks as the servers being backed-up. For example, if the servers have LUNs attached via an iSCSI network, the SAN Agent Local Proxy must also have access to it in order to mount the LUNs to perform the offloaded backup.
	See also: Appendix B.1.4: (on page VII) – SAN Agent Local Proxy Server minimum specification
	Prerequisite 4: [SAN] Set copy-only on third-party DR backup tools
	Prerequisite 5: [SAN] Set SAN Scheduling of third-party backup tool
	Prerequisite 6: [SAN] Provide access to SAN Storage Networks
	Exclusion 5: Creation by Proact of new LUNs for data restoration

2.2 Service infrastructure

2.2.1 Service platform

Platform	▪ A secure multi-tenant platform ▪ Utilises proven CommVault Simpana software
Compute	Compute resources are provided in the form of: ▪ Local vault server (for *Local & Remote* option only) ▪ Remote support VM server ▪ VSA (Virtual server agent) Proxy VM ▪ NAS agent local proxy server VM [3] ▪ SAN agent proxy server VM [3]

[3] The customer can opt to use a physical server if they wish.

Storage	Backup data storage resources are provided as follows: ▪ Remote vault, Secondary Vault High capacity, low performance storage capacity provided in Proact datacentres from Proact's shared platforms, chargeable based on the used capacity consumed in the remote vault. ▪ Local vault Storage capacity on the *local vault server* provided, supported and managed by Proact.
Software	▪ All backup operations are provided by the CommVault Simpana software suite

2.2.2 Components

Remote vault	▪ Stores backups remotely ▪ High capacity, low performance storage capacity from Proact's shared platform ▪ Located in a Proact datacentre ▪ [Optionally] Replicates to Secondary vault
Secondary vault	▪ Stores a copy of a Remote vault ▪ High capacity, low performance storage capacity from Proact's shared platform ▪ Located in a geographically separate Proact datacentre to its associated Remote vault.
Local vault	▪ Stores backups locally on a Local vault server at the customer's premises or other non-Proact datacentre ▪ Replicates to a Remote vault ▪ Can have a different data retention period to that set for the Remote vault ▪ Can be provide in different sizing tiers (from 5-200 TB) depending upon the required backend capacity – see Table 4 (on page V) for further information on storage capacity sizing.
Local vault server	▪ Located on customer site ▪ Contains local storage to run the required application software ▪ Also hosts local de-duplication cache and NAS/SAN Agent(s) as applicable. ▪ See: B.1: (on page V) for minimum specification
Local de-duplication cache	▪ For *Remote Only* and *Remote & Secondary* deployments, Proact provide efficient replication of the data across the internet using source-side de-duplication ▪ The local de-duplication cache stores the source-side de-duplication data ▪ This requires the customer provides disk space for a local de-duplication cache on each server running an agent or a proxy to store the cache data – see Table 9 (on page VIII). Note: Remote Only and Remote & Secondary deployments only See also: Appendix B.1.5: Local de-duplication cache (on page VIII) Prerequisite 7: Provide disk space for local de-duplication cache
Virtual server agent (VSA)	The Virtual Server Agent Proxy Server for VMware is a VM installed on the customer's vSphere farm to enable Agentless backups. Note: Required only for Agentless VM backup. See also: Appendix B.1.2: Agentless proxy VM specification (on page VII) Prerequisite 8: [Agentless] Provide hypervisor compute resource to run VSA Proxy server
NAS agent	▪ Controls backup of NAS data from storage arrays ▪ Runs on NAS Agent local proxy server or Local vault (if available).

NAS agent local proxy server	A NAS Agent Local Proxy Server (VM or physical) installed on the customer's premises with LAN connectivity to the NAS devices being backed-up. Note: Required only for NAS file (CIFS/NFS) backup. See also: Appendix B.1.3: NAS Agent Local Proxy Server (on page VII) Prerequisite 9: [NAS] Provide compute resource (physical or virtual) to run NAS Proxy server
SAN agent	▪ SAN agent to control backup of SAN data from storage arrays ▪ Runs on NAS Agent local proxy server or Local vault (if available).
SAN agent local proxy server	A SAN Agent Local Proxy Server (VM or physical) installed on the customer's premises with LAN connectivity to the SAN devices being backed-up. Note: Required only for SAN SnapShot based backups See also: Appendix B.1.4: SAN Agent Local Proxy Server (on page VII) Prerequisite 10: [SAN] Provide compute resource (physical or virtual) to run SAN Proxy server
Remote support VM server	Provides remote management functionality for support purposes for the Local Vault where the *Local & Remote* option is selected ▪ Support and management traffic uses secure internet site-to-site IPsec VPN between Proact and the customer-site(s). Note: Local & Remote deployments only

2.2.3 Service connectivity

Connectivity options	▪ Backup data is transferred / replicated from the customer's site(s) to Proact datacentre(s) over encrypted (HTTPS/SSL/TLS) public internet links using Proact shared firewalls. ▪ Self-service management portal connections are over encrypted (HTTPS/SSL/TLS) public internet links and use Two Factor Authentication (2FA)

Customer firewall	▪ Open port requirements – TCP 8400, 8600-8620
	  ▪ For the *Local & Remote* option, these ports need to be opened only for traffic outbound from the Local vault servers
	  ▪ For the *Remote Only* and *Remote & Secondary* options, these ports need to be opened for outbound traffic from all deployed CommVault agents and proxies at the customer site
	▪ Requires a separate internet connection and firewall for each site location unless the site(s) are connected through an internal WAN.
	Prerequisite 11: Provide an administrator to assist with firewall configuration as necessary
	Prerequisite 12: Open required firewall ports

Proact datacentre firewall	Proact manage the centralised firewall, which defines the open ports and blocks unwanted traffic for the entire service.

Connecting for management of Local Vault	For the *Local & Remote* option: ▪ Proact operate an IPsec VPN over the Public Internet to facilitate remote management of the Local Vault server. The VPN is established between Proact's shared-platform firewalls and the customer's dedicated firewall or other shared or tenant firewall in a third-party or Public Cloud environment ▪ Unless the customer's firewall is also under Proact Service Management, the customer must provide appropriate technical resource to assist Proact with the configuration of VPNs ▪ Proact support specialists use an *RDP session* from a customer dedicated *Customer Support Server* in a Proact datacentre to connect to the Local Vault server at the customer's site ▪ In the event of VPN failure, a customer-assisted *remote support session* utility is used to connect. An appropriately experienced customer administrator must be available to: ▪ Host all remote support sessions for assigned Proact support specialists ▪ Provide access to the systems for which the incident has been raised ▪ Connect into the environment (over an existing LAN, WAN or VPN connection) to access the systems for which support is needed ▪ Give control of their computer to the Proact support specialist who will proceed to diagnose the issue with the administrator. Note: Local & Remote deployments only Prerequisite 13: [Local] Provide a static public IP address on the firewall Prerequisite 14: [Local] Provide a firewall that supports IPsec VPN Responsibility 2: [Local] Provide resource to assist Proact with VPN configuration Responsibility 3: [Local] Provide administrator for remote support utility sessions (as required)
Bandwidth use	▪ Internet bandwidth is required for data seeding, replication and retrieval activities, unless (for retrieval and where applicable) the data is available in the Local vault ▪ Data change rates and available bandwidth dictate the time required for replication Proact endeavour to minimise potential monopolisation of bandwidth by spreading data seeding activities and scheduled backup runs over customer-defined periods of time
Interoperability with Customer-managed systems	Where this service interacts with any system, application or environment not managed by Proact, it is the customer's responsibility to ensure that it remains compatible with any Proact-managed systems/applications at the hardware, firmware, *OS*, and application version levels – as recommended by Proact or its vendors as best practice. Responsibility 4: Maintain compatibility of interacting external systems or environments at all times

2.2.4 Service security

The security of the customer's data assets is paramount, and Proact endeavour to maintain its approach to security in line with established industry standard practice.

See also …

Further details are available in the technical white paper Proact Managed Service Security Policy.

Anti-virus protection	▪ Proact's infrastructure incorporates enterprise level antivirus protection. ▪ Proact do not provide antivirus protection for the Local vault server, and we recommend that the customer deploy their own antivirus protection to the local vault server where the *Local & Remote* option is selected
Patching	▪ Proact patch and update all infrastructure software, firmware and hardware under their management in order to minimise security vulnerabilities.

Data encryption	▪ Secure HTTPS/TLS encryption is applied to all data connections between Proact and their customers ▪ In all architecture models data is stored in encrypted format (using a Proact-generated passphrase) to ensure its security, whether at rest or in-flight
Audit capability	▪ Proact provide regular reports confirming the status of backup jobs, which together form an audit trail of job success or failure. ▪ The CommVault software itself has an inventory of every file backed up, which is accessible by Proact Service Desk operatives and through the Self-service management portal
Application Consistency	It is the customer's responsibility to ensure that all data is application consistent and that all data protection processes are in place and adhered to. Responsibility 5: Ensure application consistency.

2.2.5 Service continuity

Planned maintenance	Proact endeavour to provide, by email, advanced notification of any planned maintenance activities at least five working days in advance of the maintenance commencement – see: Service deliverables (Ch.4 on page 14).
Disaster recovery	Proact's Disaster Recovery as a Service (DRaaS) solution is available as an option if the customer requires a managed disaster recovery solution. Exclusion 6: No disaster recovery included in BaaS

2.2.6 Applications and licensing

Software licensing is categorised by *data type*. Data can belong to only one licensing category; that is, a given data set cannot be both *File System* and *Application Tier 1*; it must be one or the other.

For servers containing multiple data types, the backup for each data type must be licensed appropriately.

Backup Method Licensing	▪ Licensing for backup methods and agents used is included in the cost per GB per month usage charge ▪ Backups using Storage based SnapShots require an additional license.
File System licensing	Flat files, which do not require an application agent to make the data consistent. ▪ File system data for all operating systems ▪ Hypervisor agentless backups.
Applications Tier 1 licensing	Business Application – licensing is application-specific ▪ Microsoft Active Directory on Windows ▪ Microsoft SQL on Windows ▪ Microsoft Exchange on Windows ▪ Lotus Notes on Windows ▪ Oracle on Windows ▪ Microsoft SharePoint on Windows
Applications Tier 2 licensing	Enterprise Application – licensing is application-specific ▪ Lotus Notes on Unix ▪ Oracle on Unix

2.3 Supporting services

Monitoring	▪ The *Proact Monitoring platform* monitors the service infrastructure and the status of backup related tasks. Its near-real-time monitoring raises alerts (for example for a failed backup jobs), which are forwarded to the Proact Service Desk.
	▪ Monitored items include the CommVault success status of backup jobs, to identify whether an issue requiring an alert has occurred.
	▪ Proact monitor the backup targets (that is, the servers, storage and applications being backed up) ONLY where the customer has separately contracted cover through either *Proact Premium Support Plus* or *Proact Service Management for Servers.*
	▪ Proact define and deploy a set of alert thresholds at implementation. These thresholds
	  ▪ Can be varied by Proact (with agreement from the customer) to ensure that appropriate alerts are being generated
	  ▪ Are reviewed as part of the Service Transition workshop.

	Exclusion 7: Monitoring of backup targets
Proact Service desk	▪ Provides 24x7x365 support and management of the service and supporting infrastructure – see Service infrastructure (Section 2.2, on page 7) ▪ Restores data in response to authorised user requests ▪ Handles events, requests, queries and incidents raised by authorised users only, whether by phone, e-mail or self-service support portal ▪ Handles Change Requests (CR) in accordance with Proact's Change Management process. ▪ Resolves problems with, applies changes to and maintains the patch state of, the service platform in accordance with Proact's change management process ▪ Makes configuration changes on request (for example, changes to schedules).
Proact Self-service support portal	Proact provides customer-nominated administrators with access to a Self-service support portal through which they can: ▪ Request data restores ▪ Create new and update existing incidents for investigation ▪ Create new and update existing changes from a change catalogue The credentials assigned to users are for their sole use. Shared accounts are not available.
Proact Self-service monitoring portal	Proact provide access to monitoring and statistical information in relation to the Local vault server and internet bandwidth utilisation

3 Available service levels

This chapter identifies the service level measures applicable to the service – see Table 1 (below)

You should consider these measures in the context of the general terms and conditions described in full in the ***Proact Service Level Agreement*** document, which customers may view at this web address: http://www.proact.eu/terms.

Table 1: Available service level measures

Availability	▪ BaaS ▪ Comms – Internet

Response time	▪ Incidents
	  ▪ P1
	  ▪ P2
	  ▪ P3
	▪ Changes
	  ▪ Standard
	  ▪ Normal
	  ▪ Emergency

4 Service deliverables

This chapter provides more detail about the deliverables that make up the Service package described in *Section 2.1 (on page 3)*.

4.1 ITIL processes

Proact monitor, support and manage the service infrastructure using processes aligned with the ITIL framework for IT Service Management.

This section summarise the processes' key capabilities and deliverables.

> The Proact Customer Service Operations Guide provides full detail on how Proact deliver and operate these processes.

Event management	**Near real-time monitoring**	The Proact monitoring platform continuously monitors the service infrastructure to: ▪ Deliver near-real-time device monitoring ▪ Collect metrics for analysis ▪ Identify alert conditions and thresholds breaches ▪ Send triggered alarms to the Service Desk
	Alert notifications	The Proact Service Desk responds to triggered alarms, analysing, investigating and taking appropriate remedial action.
	Event handling	Proact process all alerts (not just critical alerts), taking the appropriate action to resolve the issue (if required.
Incident Management	**Service desk**	The Proact Service Desk provides an escalation path for the customer's administrators when assistance is required with software issues, firmware issues and hardware faults on CIs.
	Incident Response	▪ Proact Service Desk escalates alerts to its technical teams for resolution as appropriate ▪ Proact Service Desk inform the customer's nominated contact of any service impacting alerts and the resolution timeframe ▪ For incidents categorised as P1, Proact take whatever action is required to restore operation and-or to minimise any service down time. ▪ Proact co-ordinate any product vendor involvement necessary to achieve resolution of an issue.
Change Management	**Controls**	▪ All changes to the service infrastructure are performed under the Proact Change Management process ▪ Proact perform changes to the service infrastructure only when authorised to do so by a CAB approved Change Request (CR)
	Tools	▪ Proact use orchestration appliances to perform changes where compatible and appropriate.
Problem Management	**Pre-emptive maintenance**	▪ Proact's proactive problem management processes help avoid recurring issues. ▪ Proact applying patches, bug-fixes and upgrades to the service infrastructure in line with best practice. ▪ Proact maintain problem records in the CMDB to aid identification and prompt resolution of issue.
	Trend analysis	Proact perform regular incident *trend analysis* to proactively identify any reoccurring service infrastructure problems and their root causes.
Capacity management	Proact monitor and respond to service infrastructure threshold breaches and growth forecasts to maintain agreed performance levels and adequate capacity for growth.	
Service reporting	Proact provide quarterly service review reports through their Service Delivery team	

Continual Service Improvement	Proact manage service improvement plans which track recommendations for changes to improve service provision.
Configuration & Knowledge Management	▪ Proact maintain a definitive record of the service infrastructure in a CMDB ▪ Proact maintain a knowledge database to allow support teams to efficiently resolve known issues and find supporting information.

4.2 Resources

Deliverable	Frequency	Description and content summary
Service Desk – contact number	Continuous	▪ Proact provide the customer with a 24x7x365 service desk telephone number for the purpose of reporting incidents and raising Change Requests (CRs) for Configuration Items (CIs) ▪ Calls are logged on receipt, and will be acted upon within the customer's contractual service window ▪ The Proact Service Desk and Proact Self-service support portal are accessible to named individuals only; not to the customer's users in general. Proact do not offer *end-user* support. Exclusion 8: Unauthorised use of the Proact Self-service support portal and-or Service Desk
Proact Self-service support portal	Continuous	The customer is provided with access to the *Proact Self-service support portal* via the internet. Using the portal the customer can: ▪ Create new and update existing incidents for investigation ▪ Create new and update existing CRs from a change catalogue ▪ View their CIs on the CMDB Proact provide each named individual with an account for their sole use, with their username being their email address. No shared accounts are provided.

Proact Self-service management portal	Continuous	▪ Proact provide a Self-service management portal to enable the customer to perform data restores and to amend job configuration, such as scheduling or filtering file inclusion or exclusion parameters
		▪ Proact provide appropriate login credentials to the customer's nominated authorised representatives, which includes use of two-factor authentication (2FA). Authorised users are issued:
		  ▪ A unique username, which must be changed upon first login and then –at least– every 90 days.
		  ▪ A software token, used to generate One Time Passwords (OTP) for each access session
		▪ Where the "Local" option is selected, the self-service portal can alternatively be provided directly through the local vault on the customer's site, which does not require 2FA authentication and provides an enhanced user experience. If this option is selected, the portal username format may be changed to match the customer's user email address format.
		See also: Self-service management portal (Appendix C:, on page IX)
		Prerequisite 15: Use Windows 7 SP1 or newer to access Self-service management portal

Proact Self-service monitoring portal	Continuous	Proact provide the customer with access to the Proact Self-service monitoring portal, showing monitoring metrics for in-scope systems, to allow customer administrators to view trends and manage infrastructure resources.

4.3 Operational Activities

Deliverable	Frequency	Description and content summary

Incident Management – Job failures	Continuous	▪ Proact monitor the success state of jobs (for example, replications and backup or restore jobs) using the Proact Monitoring platform, which:
		  ▪ Generates alerts for failed backup jobs
		  ▪ Forwards alerts to the Proact Service Desk
		▪ Proact will ensure that any jobs which have failed due to issues with the backup targets are re-run, and for repeat failures will contact the customer to jointly troubleshoot the problem.

Maintain platform infrastructure resources	Continuous	▪ Proact maintain the infrastructure to a standard that enables its availability to at least match the agreed service level ▪ Proact provide planning and implementation of upgrades and-or patches to software and firmware on the underlying platform infrastructure ▪ Proact make configuration changes to customer IP addressing, certificate changes and IP routing on Proact communication devices located in a Proact datacentre when requested by the change control process
Planned maintenance	As required	▪ Proact endeavour to provide, by email, advanced notification of any planned maintenance activities, either by Proact or by its third-party providers, at least five working days in advance of the maintenance commencement ▪ Where maintenance is required more urgently, to prevent a longer outage or a security incident, or due to third-party provider timescales, Proact may give less notice than five working days ▪ The customer must inform Proact whenever they intend to perform any maintenance to sites, networks or other devices that may affect the availability, communicability, performance or integrity of any system monitored or managed by Proact **See also**: Proact's Customer Service Operations Guide, where this requirement is described further Responsibility 6: Provide at least 24-hours' notice of planned maintenance
Change Management	Continuous	All changes to the customer's backup architecture or policy configuration are planned and implemented according to the Proact Change Management processes
Storage Capacity Management	As required	Proact extend storage capacity in line with contractual limits where storage volumes reach certain thresholds to ensure that they do not run out of space.
Data restore activities	On request	▪ The customer may use the Self-service support portal to perform data restores, or may request Proact do this. ▪ Proact can perform restore activities on behalf of the customer on receipt, by the Proact Service Desk, of an authorised restore request through telephone, email or the Self-service support portal ▪ Proact can restore files to the original server and location or to a different location or client (if that client is also being backed up) ▪ Where the data to be restored is on the Local vault (if selected) this copy of the data will be used first to minimise restore time.

Deliverable	Frequency	Description and content summary
Backup client Installation	As required	Proact perform the installation of backup clients remotely to ensure that they are configured correctly with the shared infrastructure. The customer will need to be available to provide a server account with elevated privileges as part of the installation. Proact will perform the client installation of new backup clients remotely where: ▪ The software vendor supports remote deployment ▪ A working remote deployment method exists ▪ Appropriate pre-built software packages (configuration and binaries) are available in the central management console.
		Responsibility 7: Assist in installation of backup clients by providing elevated privileges

4.4 Service Guides, Documents and Reports

Proact provide – and maintain as required throughout the contract term – the following service guides, operational documents and reports:

Deliverable	Frequency	Description and content summary
Service Specification	Contract	A schedule of the customer's contracted services and associated charges.
Service Level Agreements	Contract	Proact's standard Service Level Agreements.
Terms and conditions	Contract	Proact's terms and conditions for all services.
Managed Service Transition Guide	Start-up	How customer services are transitioned into live operation.
Customer Prerequisites Guide	Start-up	The activities the customer must perform before the service can be commissioned.
Customer Service Operations Guide	Ongoing	A guide to how Proact operate customer service, how to communicate with Proact and how to best use the service.
Service Operations Manual	Ongoing	Proact produce and maintain a *SOM* document, which details the scope of the services provided including: ▪ Services and service levels ▪ Customer contacts ▪ Locations and environments ▪ CIs ▪ Change management contacts and classifications ▪ Incident management processes and contacts ▪ *Monitoring Thresholds* and defined event response actions ▪ Regular scheduled operational activities ▪ Data protection schedules.

Deliverable	Frequency	Description and content summary
Service Review Report (SR)	Quarterly	A quarterly Service Review Report showing backup performance statistics, for example: ▪ Incident & change statistics ▪ Incident response times ▪ Incident by category ▪ Incident logged by method ▪ Incident and change log ▪ Bandwidth usage ▪ Vault capacity reports **Note**: This is an example report. Technical content is subject to change
Major Incident Report	Per Major Incident	▪ In the event that a major incident occurs, for which Proact are responsible, Proact provide a *MIR* detailing the following: ▪ Timeline of the incident ▪ Root cause analysis ▪ Workarounds employed ▪ Remedial actions ▪ Lessons learned ▪ SLA status ▪ Proact aim to complete the MIR and deliver it to the customer within ten working days of the resolution of the incident.
Service Transfer Policy	Contract	Proact's policy for handling data and asset returns at end-of-contract.
Service Transfer Plan	End of contract	A plan for handling data and asset returns for the customer, in accordance with the ***Proact Service Transfer Policy***.

4.5 Meetings

The following meetings are held between the customer and Proact as part of this service:

Deliverable	Frequency	Description and content summary
Service Review Meeting	Quarterly	A Service Review teleconference meeting is held between the customer, their assigned SDM and Account Manager to discuss the performance and use of the service, and identify any future requirements for expansion, integration or additional services. This meeting takes place following delivery, by email, of each period's Service Review report and covers the following agenda items at a minimum: ▪ Review of Proact's performance against SLAs ▪ Review of any high-impact Incidents or Problems from the reporting period ▪ Review of capacity (where relevant) ▪ Recommendations by Proact for any non-essential remedial work or upgrades that should be considered ▪ Review new Proact technologies / services as appropriate ▪ Overview from the customer of any relevant forthcoming projects and plans that may require assistance from Proact ▪ Overview from the customer of key priorities for the next period ▪ Review usage and consumption of licence entitlements where relevant ▪ Review of the SOM, and any other service-specific documentation that requires regular customer review. ▪ A review of system capacity growth, performance, risks and other technical observations and recommendations.

Deliverable	Frequency	Description and content summary
Service Improvement Plan Meeting	Weekly, Fortnightly or Monthly, as preferred by the customer	▪ Proact hold a teleconference meeting to review the SIP with the customer ▪ The frequency of this meeting is jointly agreed between Proact and the customer, and may be varied throughout the term of the contract as required.
Other Meetings by Request	Upon Request	Proact join teleconference meetings and, according to availability, any other meetings requested by the customer. Meetings may involve third parties of either Proact or the customer, but there must always be a representative of both Proact and the customer in attendance.

5 Service transition

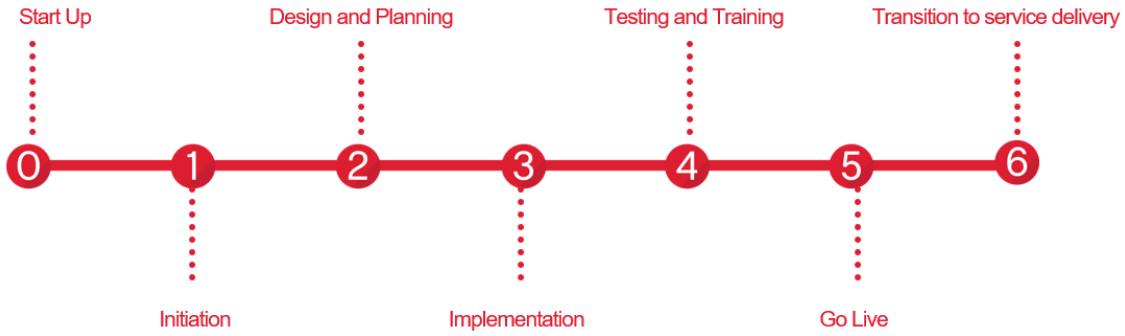
Proact use a standard methodology for transitioning the customer's services into live operation.

This methodology is described in full in the ***Proact Managed Service Transition Guide***.

Transition prerequisites
▪ General prerequisites are detailed in the ***Proact Customer Prerequisites Guide***
▪ Service-specific *prerequisites* are summarised in Chapter 8 (Service demarcation) of this document.

Proact follow a Stage 0-6 model for all Service Transitions (Figure 2 below).

Figure 2: Stage 0-6 transition model



Meetings	**Service transition workshop** The Customer is required to attend a Service Transition workshop and any further workshops required to complete the detailed service and technical design, and make available appropriate service and technical personnel with suitable skill sets at these meetings. ▪ Service owners and-or technical owners for any applications or systems that utilise the infrastructure to be managed by Proact ▪ Technical owners for any supporting infrastructure needed to allow Proact to access and monitor the in-scope CIs (for example, network engineers, for creating VPNs and firewall rules) ▪ Project manager, if the customer has chosen to use one. **Project Closedown** The Customer is required to attend a Project Closedown meeting to formally close projects for transitioning new services into operation.
	Prerequisite 16: Provide appropriate customer representation at transition workshops Responsibility 8: Provide appropriate representation at project closedown workshop
Data migration	Migration of workloads and datasets from legacy systems to systems under Proact service management is not included in this service – see Additional services (Ch. 7, on page 23)
	Exclusion 9: Data migration is excluded from the scope of service transition

Training sessions	▪ Using the Proact Self-service management portal A Proact engineer will provide a single remote web-based training session to the customer's administrator(s) covering the access and use of Proact's Self-service management portal for BaaS, which will include: ▪ How to view backup job statuses ▪ How to initiate restore operations ▪ Using the Proact Self-service support portal Proact provide, on request, a single remote web-based training session to the customer's administrator(s) covering the access and use of Proact's Proact Self-service support portal, to supplement the instructions provided in the ***Proact Customer Service Operations Guide*** ▪ Using the Proact Self-service monitoring portal ▪ Proact provide, on request, a single remote web-based training session to the customer's administrator(s) covering the access and use of Proact's Proact Self-service monitoring portal, to supplement the instructions provided in the ***Proact Customer Service Operations Guide***

6 Service charging policy

Proact's monthly invoicing and flexible usage models free the customer's capital budgets.

Self-service portals and intrinsic infrastructure support minimise mundane operational tasks, freeing the customer's focus for strategic business projects.

Proact base the charges for the solution on usage information provided and on assumptions made on the basis of that information, all of which forms part of the contractual agreement. Any prolonged and significant variation in usage may require a reassessment of the charges.

Table 2: Service charging-model

Item	Pay-per-use model	Allocation model
Contract term	Monthly	12 – 60 months
Charging basis	Cost per GB (Gigabyte) of used capacity data to be backed up	Cost per GB (Gigabyte) of used capacity data to be backed up
Minimum commitment	None	Minimum contracted commitment
Maximum commitment	Technical limitations	Technical limitations
Billing schedule	Billed monthly in arrears at the end of each month	Billed monthly in arrears at the end of each month
Flexible resource allocation	Fully flexible (grow & shrink)	Flexible (grow & shrink) above the minimum commitment (burst capacity)
Fixed monthly charged items	Backup method licencing (as applicable) ▪ File system ▪ Application tier 1 ▪ Application tier 2 ▪ Storage-array based SnapShots additive license (as applicable) See: Section 2.2.6 (on page 11) for more on licensing options.	Backup method licencing (as applicable) ▪ File system ▪ Application tier 1 ▪ Application tier 2 ▪ Storage-array based SnapShots additive license (as applicable) See: Section 2.2.6 (on page 11) for more on licensing options.
Set-up fee	Yes	Yes
Best use scenario	Ideal for short term or dynamic workloads	Best for long-term workloads relatively static in nature that fluctuate as part of routine growth and changes in the environment
Features	▪ No upfront commitment ▪ No resource limits ▪ No contract term limits ▪ Scalable up or down ▪ Billing based on resources used ▪ Resources can be equivalent to any agreed value. ▪ No reserved resources	▪ Guaranteed minimum amount of resource available for whole contract ▪ Flexibility of having a burst space for workload peaks ▪ Available resources can be equal to, or greater than, the minimum commitment.

7 Additional services

Customers should contact their Proact Account Manager to discuss the available options, some of which are shown Table 3 (below).

Table 3: Service change options

Service change	▪ Increasing the capacity of the Local Vault ▪ Adding new features or services requires updating the service design and-or architecture, unless otherwise specified in this document. Proact can perform this on a separately chargeable consultancy basis.
Service upgrade	Service review upgrade – A quarterly remote service review meeting is included as standard. It can be upgraded to monthly and-or delivered onsite instead of via teleconference at additional cost.
Bespoke services	Proact Professional Services can be engaged to assist with a range of bespoke services including, but not limited to: ▪ Migration of workloads, datasets and monitoring configurations from legacy systems to systems under Proact service management ▪ Out of scope support – Proact can provide support and professional services for out of scope equipment ▪ Service transfer and end-of-life – Any bespoke activities required by the customer outside of the ***Service Transfer Plan*** can be provided using Proact Professional Services – See also: ***Proact Service Transfer Policy***

Complementary services	Proact provides a range of services complementary to BaaS, including, but not limited to:
	▪ Monitoring, Support and Service management
	  ▪ Proact Premium Support Plus
	  ▪ Proact Service Management for Servers
	▪ Disaster Recovery (DRaaS)
	  ▪ Uses enterprise-class technology
	  ▪ Deliver a highly available platform for the customer's crucial information
	  ▪ Replicates the customer's mission-critical data to a secure Proact datacentre and-or the customer's own secondary datacentre
	  ▪ Contractual SLAs ensure the customer's services are recovered according to a strict *recovery time objective* (*RTO*).

8 Service demarcation

This chapter identifies the prerequisites, responsibilities and exclusions upon which the delivery of the service defined in this document depends.

Prerequisites	Prerequisite 1: Remove existing backup applications....5 Prerequisite 2: [NAS] Provide NAS credentials....6 Prerequisite 3: [NAS] Create duplicate CIFS shares with antivirus scanning disabled....6 Prerequisite 4: [SAN] Set copy-only on third-party DR backup tools....7 Prerequisite 5: [SAN] Set SAN Scheduling of third-party backup tool....7 Prerequisite 6: [SAN] Provide access to SAN Storage Networks....7 Prerequisite 7: Provide disk space for local de-duplication cache....8 Prerequisite 8: [Agentless] Provide hypervisor compute resource to run VSA Proxy server....8 Prerequisite 9: [NAS] Provide compute resource (physical or virtual) to run NAS Proxy server....9 Prerequisite 10: [SAN] Provide compute resource (physical or virtual) to run SAN Proxy server....9 Prerequisite 11: Provide an administrator to assist with firewall configuration as necessary....9 Prerequisite 12: Open required firewall ports....9 Prerequisite 13: [Local] Provide a static public IP address on the firewall....10 Prerequisite 14: [Local] Provide a firewall that supports IPsec VPN....10 Prerequisite 15: Use Windows 7 SP1 or newer to access Self-service management portal....15 Prerequisite 16: Provide appropriate customer representation at transition workshops....20 Prerequisite 17: [Local] Provide appropriate datacentre environment for local vault. V
Responsibilities	Responsibility 1: [Agentless] Ensure VMware OS running latest version of VMware tools....5 Responsibility 2: [Local] Provide resource to assist Proact with VPN configuration.10 Responsibility 3: [Local] Provide administrator for remote support utility sessions (as required)....10 Responsibility 4: Maintain compatibility of interacting external systems or environments at all times....10 Responsibility 5: Ensure application consistency....11 Responsibility 6: Provide at least 24-hours' notice of planned maintenance....16 Responsibility 7: Assist in installation of backup clients by providing elevated privileges....17 Responsibility 8: Provide appropriate representation at project closedown workshop....20
Exclusions	Exclusion 1: Retention of backup data after the contract termination date....4 Exclusion 2: The solution does not support flat file dumps of application data....6 Exclusion 3: The solution does not support application consistency with agentless backup....6 Exclusion 4: NFS data backup where NFS not configured in mixed-mode with CIFS access....6 Exclusion 5: Creation by Proact of new LUNs for data restoration....7 Exclusion 6: No disaster recovery included in BaaS....11 Exclusion 7: Monitoring of backup targets....12 Exclusion 8: Unauthorised use of the Proact Self-service support portal and-or Service Desk....15 Exclusion 9: Data migration is excluded from the scope of service transition....20

Glossary

Term		Definition
Agentless		A type of backup for virtual machines, achieved by backing up those machines directly from the hypervisor instead of using installable backup agents in each VM
Application consistent		A type of backup whereby an application is quiesced (put into a consistent state with all transactions committed) prior to the data being backed up
Application tier		A classification of an application that can be backed up
Availability SLA		Availability service level agreements, typically defined in terms of service up-time, are particularly applicable for infrastructure and service provision arrangement where a continuous IT service is provided.
Backup agent		A software package installed on a server operating system for the purposes of backing up file systems and applications within that operating system
Backup methods		In the context of this document, Backup methods refers to the type of data being backed up and the associated method for achieving that backup.
Break-fix		Break-fix is a reactionary IT business support model in which the repair of an IT device or system component is done only when it fails (for example, a disk drive or server or router ceases to function).
Change advisory board	CAB	Delivers support to a change management team by approving requested changes and assisting in the assessment and prioritisation of changes.
Change request	CR	A document requesting a change to an item within the scope of the contracted service, or to the service itself
Clustering		Connecting two or more computers together in such a way that they behave like a single computer. Clustering is used for parallel processing, load balancing and fault tolerance.
Configuration item	CI	A hardware, firmware, software or other item monitored, supported and-or managed by Proact. That is, it is included in the agreed list of in-scope items as an item covered by the selected service
Configuration management database	CMDB	A repository for information technology installations. It holds data relating to a collection of IT assets
Contract change note	CCN	Contract change notes are used to legally document amendments to contractual commitments during the contract term
Contractual SLA		A Contractual service level agreement defines the boundaries of responsibility between customer and supplier, sets standards of performance and defines the measurement of service performance. It commits the supplier to delivering to required service levels and identifies the consequences of failure, usually in the form of service credits or other compensation.
Customer service operations guide	CSOG	The Proact Customer Service Operations Guide. A guide to how Proact operate customer service, how to communicate with Proact and how to best use the service.
Customer service specification		Defines the service configuration to be deployed for a specific customer

Term		Definition
Customer support server		The Customer Support Server is a Proact provided remote server used for remote service management activities
Customer-site	Site	Customer-site refers to a geographically-local collection of in-scope customer networks, devices or resources, whether they are physically located on customer premises, in a Proact or third-party provider datacentre, or in a Proact or third-party public or private cloud.
Dashboard		A view presented via a Proact Portal or application that shows the current service status and a summary of performance and usage.
Data type		A type of data that can be backed up, such as a filesystem, application or storage volume
Datacentre	DC	A data centre is a facility used to house computer systems and associated components, such as telecommunications and storage systems
Disaster recovery	DR	The process of restoring and assuring the continuation of essential IT services in the event of a disaster disrupting normal operation/
Exclusion		Exclusions are, for the purposes of this document, items outside of the scope of this service contract for which Proact are not liable.
File system		A partition or volume created on a disk or LUN for holding files
Host OS		The host operating system of a server on which a Backup Agent is installed.
ITIL	Information Technology Infrastructure Library	A set of practices for IT service management that focuses on aligning IT services with the needs of business.
ITMS	IT Service Management system	The system used by the Proact Service desk to manage events, incidents, problems and changes
LUN		A data container within a storage system, mounted to a host OS for storage of data
Major incident		The parties and process for declaring an incident a major incident are agreed during service transition. Whilst no formal ITIL definition exists these are typically incidents with significant corporate impact over and above a P1 incident, which do not require invocation of disaster recovery.
Major incident report	MIR	Major incident reports identify incident timeline, root cause, workarounds and-or remedial actions and lessons learned
Monitoring threshold		The monitoring threshold is the trigger value beyond which an alert will be raised. See also – threshold breach
NAS	Network attached storage	A NAS is a storage device that serves data as files
National operations centre	NOC	A location from which Proact deliver their monitoring, support and or management services.

Term		Definition
Near-real-time		Near real-time (in telecommunications and computing) refers to the time delay introduced by automated data processing or network transmission between the occurrence of an event and the use of the processed data (for example, for display or feedback & control purposes).
Operating System	OS	The program which, after initially loading, manages the other programs in a (virtual) machine. The installed applications make use of the operating system. For example, Microsoft ® Windows ®, Windows Server ® and Linux ®
Prerequisite		Prerequisites are, for the purposes of this document, tangible resources, actions or commitments without which the service cannot be initiated and whose provision and maintenance (where applicable) is the responsibility of the customer for the duration of the contract.
Proact Premium Support	PS	Proact Premium Support is Proact's proven break-fix support solution
Proact Premium Support Plus	PSP	Proact Premium Support Plus is Proact's proven monitoring solution
Public IP Address		IP address that can be accessed from the public internet.
Remote desktop protocol	RDP	Remote desktop protocol provides remote display and input capabilities over network connections for Windows-based applications running on a server.
Response-time SLA		Response time service level agreements define the time taken to respond to a reported event.
Responsibility		Responsibilities are, for the purposes of this document, ongoing actions or commitments necessary to sustain service delivery, which must be maintained for the duration of the contract
RTO	Recovery time objective	The targeted duration of time within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity
SAN	Storage area network	A NAS is a storage device that serves data as blocks
Service delivery manager	SDM	Proact service delivery managers oversee the delivery of a service or service technology to the customer. The SDM establishes policies designed to ensure consistently high service performance, monitors the delivery and responds to customer feedback to develop quality improvement processes.
Service improvement plan	SIP	The Proact maintained service improvement plan logs and tracks the status of any technical or service issues highlighted by the customer or by Proact in relation to the service provided
Service operations manual	SOM	The Service operations manual details the scope of the services provided.
Service transition		The process of transitioning a contracted service from planning through to a live delivery state.
SLA	Service level agreement	An official commitment to the level of service provision that prevails between a service provider and their customer

Term		Definition
Threshold breach		In the context of the Proact Monitoring Platform a threshold breach occurs when an event on a monitored item exceeds a pre-set threshold. For services that include monitoring, Proact define these thresholds and agree them with the customer during the service transition stage, they are maintained throughout the contract term. See also – Monitoring thresholds
Trend analysis		Analysis of data to identify patterns. Trend analysis is used in problem management to identify common points of failure or fragile configuration items.
User		A user is a customer defined entity that allows an administrator to login to Proact's Self-Service Portals.
Virtual Servers		A Virtual Server, or Virtual Machine, is an Operating System which runs in a container within a hypervisor host, and imitates a hardware server.
VMDK		A virtual machine disk file

PROACT

Appendices

Appendix A: Supported devices and applications II
Appendix B: Technical limits and constraints V
Appendix C: Self-service management portal functionality IX
Appendix D: Data deletion and extraction X

Appendix A: Supported devices and applications

This section contains a list of devices and applications supported by the BaaS solution. The list is included for reference purposes. The appropriate Support Matrix remains the reference document.

A.1: Storage Arrays

The table below lists the devices supported when either "Storage array backup – NAS data" or "Storage array backup – SAN data" backup method is required.

Product	Version	NAS	SAN
EMC - VNX	OE 05.32 or Higher	✗	✓
	DART OS 7.1.x or Higher	✓	✗
IBM N-Series	7-Mode, 7.3.x or Higher	✓	✗
	7-Mode, 7.3.5 or Higher	✓	✓
	7-Mode, 8.x or Higher	✓	✓
	C-Mode, 8.2P3 or Higher	✗	✓
NetApp - FAS	7-Mode, 7.3.x or Higher	✓	✗
	7-Mode, 7.3.5 or Higher	✓	✓
	7-Mode, 8.x or Higher	✓	✓
	C-Mode, 8.2P3 or Higher	✗	✓

A.2: Hypervisor

The table below lists the devices supported when the "Hypervisor Agentless Backups" backup method is used:

Product	Version	Storage Array Based SnapShot [5]
ESX [4]	ESX/ESXi 4.x (non-free version)	✓
ESX	ESX/ESXi 5.x (non-free version)	✓
ESX	ESX/ESXi 6.x (non-free version)	✓

A.3: Applications

The table below lists the applications supported when the "Application Consistent Backups" backup method is used:

Product	Version	Storage array-based SnapShot 5
Lotus Notes	IBM Domino 9	✓
Lotus Notes	Lotus Domino 8.02	✓
Lotus Notes	Lotus Domino 8.5	✓
Microsoft Active Directory	Windows 2003	✗
Microsoft Active Directory	Windows 2008	✗
Microsoft Active Directory	Windows 2012	✗
Microsoft Exchange	Exchange 2003	✓
Microsoft Exchange	Exchange 2007	✓
Microsoft Exchange	Exchange 2010	✓
Microsoft Exchange	Exchange 2013	✓
Microsoft SharePoint	FAST Search Server 2010	✗
Microsoft SharePoint	Office Forms Server 2007	✗

[4] VMware vSphere Essential or higher licensing is required, the free version of ESXi is not supported.

[5] Storage Array Based SnapShot" is required if the "Storage Array Backup – SAN Data" backup method is used as described in the "Storage Array Backup – SAN Data" section.

Product	Version	Storage array-based SnapShot 5
Microsoft SharePoint	Office Project Server 2007	✗
Microsoft SharePoint	Office Project Server 2010	✗
Microsoft SharePoint	Office SharePoint Server 2007	✗
Microsoft SharePoint	Search Server 2008	✗
Microsoft SharePoint	Search Server 2008 Express	✗
Microsoft SharePoint	Search Server 2010	✗
Microsoft SharePoint	Search Server 2010 Express	✗
Microsoft SharePoint	SharePoint 2010 Standard and Enterprise	✗
Microsoft SharePoint	SharePoint Foundation 2010	✗
Microsoft SharePoint	SharePoint Server 2010	✗
Microsoft SharePoint	SharePoint Server 2013	✗
Microsoft SharePoint	Windows SharePoint Services vn 3.0	✗
Microsoft SQL	SQL Server 2005	✓
Microsoft SQL	SQL Server 2008	✓
Microsoft SQL	SQL Server 2008 R2	✓
Microsoft SQL	SQL Server 2012	✓
Oracle	Oracle 10g (R1 or higher) Databases	✓
Oracle	Oracle 11g (R1 or higher) Databases	✓
Oracle	Oracle 12c Database	✓

A.4: Unix

The table below lists the Unix Operating Systems which are support:

Product	Version	Storage Array Based SnapShot [5]
Solaris	Solaris 10.x	Yes
Solaris	Solaris 11.x	Yes

A.5: Linux

The table below lists the supported Linux Operating Systems.

Product	Version	Storage Array Based SnapShot 5
CentOS	CentOS 4.x	×
CentOS	CentOS 5.x	×
CentOS	CentOS 6.x	✓
Debian	Debian 5.x	×
Debian	Debian 6.x	×
Debian	Debian 7.x	×
Fedora	Fedora release 10	×
Fedora	Fedora release 11	×
Fedora	Fedora release 12	×
Fedora	Fedora release 13	×
Fedora	Fedora release 14	×
Fedora	Fedora release 15	×
Fedora	Fedora release 16	×
Fedora	Fedora release 17	×

Product	Version	Storage Array Based SnapShot 5
Fedora	Fedora release 8	✗
Fedora	Fedora release 9	✗
Gentoo	Gentoo release 10.1	✗
Gentoo	Gentoo release 11	✗
OpenSuSE	OpenSuSE 11.0	✗
OpenSuSE	OpenSuSE 11.1	✗
OpenSuSE	OpenSuSE 11.2	✗
OpenSuSE	OpenSuSE 11.3	✗
OpenSuSE	OpenSuSE 12.1	✗
OpenSuSE	OpenSuSE 12.2	✗
Oracle Linux	Oracle Linux 4.x	✗
Oracle Linux	Oracle Linux 5.x	✓
Oracle Linux	Oracle Linux 6.x	✓
Red Flag Linux	Red Flag Linux 4.x	✗
Red Flag Linux	Red Flag Linux 5.x	✗
Red Hat Enterprise Linux	Red Hat Enterprise Linux 4.x	✓
Red Hat Enterprise Linux	Red Hat Enterprise Linux 5.x	✓
Red Hat Enterprise Linux	Red Hat Enterprise Linux 6.x	✓
Scientific Linux	Scientific Linux SL 5.x	✗
SuSE Linux (SLES)	SuSE Linux 10.x Enterprise Server	✓
SuSE Linux (SLES)	SuSE Linux 11.x Enterprise Server	✓
Ubuntu	Ubuntu 10.04 LTS	✗
Ubuntu	Ubuntu 11.04	✗
Ubuntu	Ubuntu 11.10	✗
Ubuntu	Ubuntu 12.04 LTS	✗
Ubuntu	Ubuntu 12.10	✗
Ubuntu	Ubuntu 8.04	✗
Ubuntu	Ubuntu 8.10	✗
Ubuntu	Ubuntu 9.04	✗
Ubuntu	Ubuntu 9.10	✗

A.6: Windows

The table below lists the supported Windows Operating Systems.

Product	Version	Storage Array Based SnapShot [5]	Supports Backups	Supports File Archiving
Desktop	Windows 7	✓	✓	✓
Desktop	Windows 8	✓	✓	✓
Desktop	Windows Vista	✓	✓	✓
Desktop	Windows XP	✓	✓	✓
Server	Windows 2003	✓	✓	✓
Server	Windows 2008	✓	✓	✓
Server	Windows 2008 R2	✓	✓	✓
Server	Windows 2012	✓	✓	✓

Appendix B: Technical limits and constraints

B.1: Minimum server specifications

B.1.1: Local vault server

For *Local & Remote* solutions, Proact provide each site a Local vault server (also referred to as a CommVault Media Agent server), which:

- Provides storage for data backed up from the source servers and-or storage devices.
- Provides storage for the local cache de-duplication database.

See also: Table 9 (on page VIII) for de-duplication cache size required

The RAID controllers are not battery backed. So, if no UPS will be available, the customer should request an alternative Local Vault specification.

The cost of the hardware is included in the service charges, so there is no capital upfront cost. However, as it is to be racked in the customer's Data Centre, the customer is required to provide:

Prerequisite 17: [Local] Provide appropriate datacentre environment for local vault

- Sufficient rack, power, networking (including management ports and patch cables) to accommodate the above devices.
- A climatically controlled environment appropriate for the server, with a clean Uninterruptable Power Supply (UPS).

  The UPS should provide sufficient run time for a graceful shutdown of the local vault.

The exact specification of the Local vault Server can vary, but will meet or exceed the specification given in Table 5 (below).

Sizing of the vault is simplified by use of Proact Marketing Tiers (see Table 4 and Table 5), which provide an approximation of the capacity required to store customer data, taking into account all appropriate overheads.

Table 4: Local vault sizing

Local vault Server Model	Maximum (TB) Backend Capacity [6]
vault server tier-5	5
vault server tier-10	10
vault server tier-15	15
vault server tier-20	20
vault server tier-30	30
vault server tier-50	50
vault server tier-100	100
vault server tier-150	150
vault server tier-200	200

Table 5: Local vault server specification

Local vault Server	Tier-5	Tier-10	Tier-15	Tier-20	Tier-30	Tier-50	Tier-100
Proact Marketing Capacity	5 TB	10 TB	15 TB	20 TB	30 TB	50 TB	100 TB
Available Capacity	5 TB	12 TB	18 TB	23 TB	36 TB	58 TB	114 TB
CPU	1 x 6 core 1.9 GHz					2 x 6 Core 2.4 GHz	
RAM (GB)	16			32			64
Storage – OS/Dedupe DB	5 x 450GB 15K HD			5 x 600GB 15K HD		5 x 480GB SSD	6 x 480GB SSD
OS/Dedupe DB RAID Configuration	1 x RAID 10 with 1 x Hot Spare					1 x RAID 5 with 1 x Hot Spare	
Storage – Data vault (7.2K SATA)	5 x 2TB	9 x 2TB	12 x 2TB	15 x 2TB	13 x 4TB	21 x 4TB	28 x 6TB

[6] Backend capacity: Maximum capacity after storage efficiencies and policies are applied.

Local vault Server	Tier-5	Tier-10	Tier-15	Tier-20	Tier-30	Tier-50	Tier-100
Data vault RAID Configuration	1 x RAID 5 with 1 x Hot Spare				1 x RAID 6 with 1 x Hot Spare	2 x RAID 6 with 1 x Hot Spare	3 x RAID 6 with 1 x Hot Spare
Management	Intelligent Platform Management Interface (IPMI) by 1Gb LAN Port						
Operation System	Windows 2012 R2 Storage Server Standard Edition 64Bit (Provided by Proact)						
Server Model	CyberStore 316S		CyberStore 424S			CyberStore 436S	
Rack Units	3U		4U				
Power Supply	2 x 900W PSU					2 x 1,400W PSU	
Generic Specification	▪ 1 x Rail Kit for 19” Racks ▪ 2 x 0.6 Meter C13 to C14 Power Cables ▪ 1 x LSI MegaRAID PCI Card (no battery backup) ▪ 1 x KVM Port (separate cable required) ▪ 1 x VGA Port ▪ 2 x Serial Port ▪ 1 x 1Gb Management LAN Port (RJ45) ▪ 2 x 10/1Gb LAN Ports (RJ45) – Used for LAN Connectivity by default ▪ 2 x 10Gb LAN Ports (SFP+) ▪ 2 x USB Ports						

Future Expansion: The above configuration is not expandable, but customers can add multiple local vault servers, so for example:

- Tier-150 would comprise 1xTier-100 and 1xTier-50 Local vault Servers.
- Tier-200 would comprise 2xTier-100 Local vault Servers.

B.1.2: Agentless proxy VM specification

If Hypervisor agentless deployments are required, a Virtual Server Agent (VSA) proxy server is required for each VMware vSphere deployment at each site – see specification in Table 6 (below).

See also: Table 9 (on page VIII) for de-duplication cache size required

The VSA Proxy Server will support up to 100 VMs with up to 5TB of source data to backup. For larger deployments, additional VSA Proxy Servers can be deployed.

The customer must provide storage and compute capacity at each site to create VM(s) in line with the following specification:

Table 6: Agentless Proxy Spec

Server Component	Specification
Server Type	Virtual
CPU	4 *vCPU*
Memory	16 GB
Hard Disk	▪ 40 GB - OS ▪ Variable – For source-side de-duplication cache (see below)
Network Interfaces	1 x 1 *Gbps*
Operating System	▪ Windows 2008 R2 64bit Standard (provided by the customer) or ▪ Windows 2012 All Editions (provided by the customer).

B.1.3: NAS Agent Local Proxy Server

The NAS Agent:

- Handles security authentication

  Authentication to the CIFS NAS requires appropriate CIFS permission and NDMP to access the data (handled by the NAS Agent Local Proxy Server or local vault server if available)
- Traverses the CIFS UNC path
- Backs up relevant data
- Performs source-side data de-duplication – see Table 9 (on page VIII) for the cache size required
- Transmits de-duplicated encrypted data to the Remote vault.

The basis for the sizing of the NAS Agent Local Proxy Server – see specification in Table 7 (below) – is the amount of data transmitted. It is recommended that one NAS Local Proxy Server be configured per site and per two NAS Controllers. If additional controllers exist at a particular site, the number of NAS Local Proxy Servers may need to be increased.

Source-side signature cache: The source-side de-duplication process requires a source-side signature cache – see Table 9 (on page VIII) for the De-duplication Cache size required on backed up.

See also: Table 9 (on page VIII) for de-duplication cache size required

Table 7: NAS Agent Local Proxy Spec

Server Component	Specification
Server Type	Virtual (or Physical)
CPU	2 vCPU
Memory	8 GB
Hard Disk	▪ 40 GB – OS ▪ 2 GB – Job and Log store ▪ Variable – For Source-side de-duplication cache (see below).
Network Interfaces	1 x Virtual 1 Gbps
Operating System	▪ Windows 2008 R2 64bit Standard (provided by the customer) or ▪ Windows 2012 All Editions (provided by the customer).

B.1.4: SAN Agent Local Proxy Server

The SAN Agent:

- Communicates with a target storage array and an application to take an Application Consistent Backup within a storage array SnapShot
- The storage array takes a SnapShot when instructed to do so by the agent installed on the server.
- Mounts storage array SnapShots on the SAN Agent Local Proxy Server – see server minimum specification in Table 8 (on page VIII).
- Performs source-side data de-duplication – see Table 9 (on page VIII) for the cache size required

- Transmits de-duplicated encrypted data to the Remote vault.

The basis for the sizing of the SAN Agent Local Proxy Server – see specification in Table 8 (on page VII) – is the amount of data transmitted. It is recommended that one SAN Local Proxy Server be configured per site and per two SAN Controllers. If additional controllers exist at a particular site, the number of SAN Local Proxy Servers may need to be increased.

Source-side signature cache: The source-side de-duplication process requires a source-side signature cache – see Table 9 (below) for the De-duplication Cache size required on backed up.

See also: Table 9 (below) for de-duplication cache size required

Table 8: SAN Agent Local Proxy spec

Server Component	Specification
Server Type	Virtual (or Physical)
CPU	2 vCPU
Memory	8 GB
Hard Disk	▪ 40 GB – OS ▪ 2 GB – Job and log store ▪ Variable – for source-side de-duplication cache (see below).
Network Interfaces	1 x Virtual 1 Gbps
Operating System	▪ Windows 2008 R2 64bit Standard (provided by the customer) ▪ Windows 2012 All Editions (provided by the customer)

B.1.5: Local de-duplication cache

Source-side signature cache: The source-side de-duplication process requires a source-side signature cache on each server running an agent or a proxy.

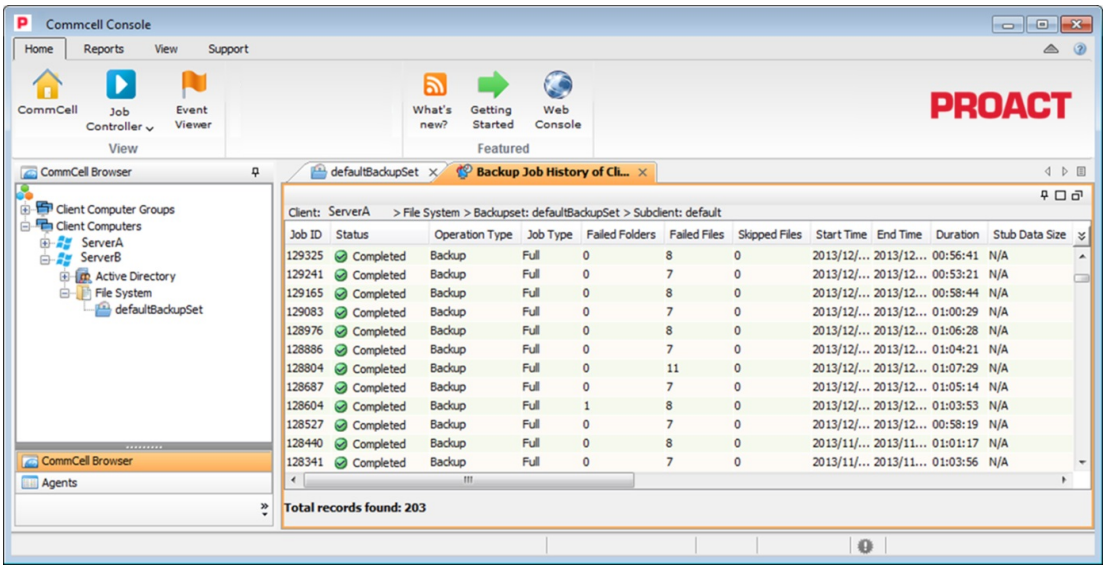
See Table 9 (below) for the De-duplication cache size required on the local proxy server for various amount of data to be backed up.

Table 9: Source-side de-dupication cache sizing

Total Source Data (TB)	De-duplicationCache(GB)
0.5	4
1	4
2	4
3	5
4	7
5	8
10	16
15	25
25	40
50	80
75	120
100	160

Appendix C: Self-service management portal functionality

The Self-service Management Portal provides the following functionality:



- Client Auditing and Settings
  - List Clients,
  - Client OS,
  - Client agent version and if an update is available,
  - Browse/list data objects stored in the vault (i.e. files);
- Job Configuration
  - Scheduling information,
  - Included/Excluded paths,
  - File filters;
- Job History and Status (active jobs)
  - Job Status (i.e. Success, Complete, Running),
  - Job Type (i.e. Full),
  - Failed or Skipped Items,
  - Start, End Time and duration of the job,
  - Agent type (i.e. Microsoft SQL),
  - Progress (active jobs only),
  - Job stats (i.e. number of files transferred, data transferred),
  - Job efficiency (i.e. compression);
- Recovery of Data
  - Initiate File Retrieve,
  - Perform In-Place Restore,
  - Perform Out-of-Place Restore.

Appendix D: Data deletion and extraction

D.1.1: Data deletion

Where the customer elects not to retain the data that has been stored, Proact expire the policies in the repository early, effectively deleting the data. Proact advise the customer when the deletion is complete.

The customer may also choose to have their data deleted at the time of giving notice to terminate the managed service contract; there is no additional charge for this option.

D.1.2: Data Extraction

At the end of the contract, the customer can choose to retain a copy of the data (for example, for compliance reasons) by extracting the backup data from Proact's BaaS platform to a customer-provided platform.

Training option
Any training required for a customer's administrators to access the data can (optionally) be included in the scope of the project.

Proact Professional Services perform migrate work as a standalone project, scoped and costed at the time of contract termination.

Depending on the scope of the process and the volume of data stored, considerable time may be required to complete this task, which also requires the customer's participation, both in agreeing the logistics of extraction and in organising provision of any necessary hardware, software and-or human resources

Proact migrate the data (in CommVault-proprietary format) into a customer-accessible, standalone environment. The customer will need to provision:

- Appropriate compatible software and hardware (that is, operating-systems, servers and-or storage) to accommodate the data
- Compatible applications and clients to facilitate data restore.

PROACT