SERVICE DESCRIPTION FOR

Assured Data Protection

08/02/2023

Andrew Eva
andrew.eva@assured-dp.com

Assured Data Protection Overview

Assured Data Protection Inc. (Assured) brings over 100 years of working experience specializing in the Data Protection market. Assured leverages that extensive experience protecting the data of the largest enterprises and the smallest, most remote, offices, to bring the best of breed Data Protection and Business continuity services to its customers. Industry and regulatory changes continue to push data into the spotlight and increase the pressure for availability. Assured's breadth of scope sets it apart from point products and solutions, providing the confidence its customers need to know their business is protected.

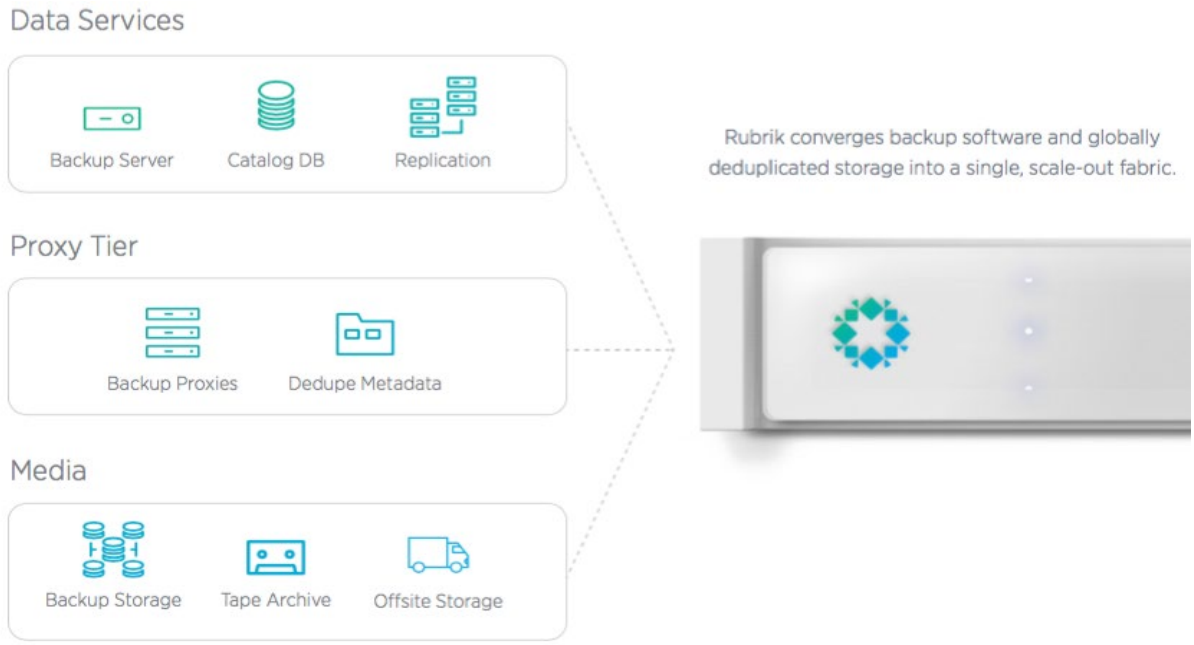
Rubrik Overview

Rubrik redefines data management capabilities throughout the data lifecycle from creation to destruction. Enabling simple control over data retention, recovery, and discovery, Rubrik packages best-in-breed capabilities in a single solution with an industry first Converged Data Management Platform. Combining backup software and globally de-duplicated storage into a single, scale-out fabric allows Rubrik to scale horizontally to thousands of nodes.

Based in Palo Alto, CA, Rubrik collapses backup software, catalog management, replication, and de-duplicated storage into a single appliance. Distributed architecture means Data Protection and management services scale in-line with your production workloads to maximize efficiency and deliver near zero recovery times at scale. Global file search capabilities within Rubrik extends the reach of an IT administrator into their backup platform to satisfy the most challenging restore and compliance requirements.

Converged Data Management Platform

Rubrik combines backup software and globally deduplicated storage into a single scale-out fabric to form the industry's first converged data management platform. Distributed design allows for horizontal scale out capability to thousands of nodes to support the largest backup environments.



Software Convergence: Management, media servers, data pools, and metadata cataloging are all converged into a single platform.

Simplicity: Intuitive UI that displays the most immediately relevant data to the IT Admin, reducing time spent managing backups.

Scale-out: Distributed architecture like that used by Google, Facebook and Amazon, allows the platform to scale simply and easily by adding nodes. Forklift upgrades and load balancing across nodes is no longer required, freeing admins to focus on more important projects.

Efficiency: Integrating deduplication as a core function, Rubrik makes the most efficient use of both local storage, as well as tiered object storage as only the needed files and data are stored and transferred throughout the ecosystem.

Key Features & Topology

Rubrik delivers backups, instant recovery, replication and archiving as key features of the converged data fabric. Rubrik removes the traditional 'backup job' setup with policy driven management; admins can automate the protection of their entire virtual estate through a handful of policies that ensure SLAs are met.

Protection

Flash-optimized Ingest: Ingest large volumes rapidly, minimizing impact to production and eliminating application stun for highly transactional apps.
Scale-out Deduplication: Maximize storage efficiency with global deduplication across the platform and extended to the cloud.
App-Consistent Snapshots: Take application-consistent snapshots for Microsoft Exchange, SharePoint, SQL Server, Active Directory and Oracle RDBMS
Encryption:

- **Inflight:** Data transmission between nodes in a secure cluster is encrypted with the Transport Layer Security (TLS) protocol, preventing attackers from access to the transmitted data even when the transmission is intercepted.
- **At Rest:** Assured replication clusters secure data with the Advanced Encryption Standard (AES) symmetric-key algorithm, using a 256-bit key length (AES-256).

Immutable Backups: Data stored in the Rubrik Filesystem is unable to be altered once it is written, ensuring that backup data cannot be changed once committed.

Management

Policy-based Management: click to assign out-of-the-box SLA policies to protect your VMs. Additionally, create custom SLA policies for snapshot capture frequency, retention duration, and data location to meet the needs of your business.
Unified Console: Manage your data through responsive and modern web console, delivering clear visibility into VM protection status, snapshots, SLA policies, storage usage, ingest throughput, and more.
Compliance Reporting and Alerts: Track SLA compliance, backup tasks and system capacity. Detailed reporting and notification for process workflow and ease of management.

Assured ProtectView

The Assured ProtectView portal provides a unified view into multiple deployed Rubrik clusters, including those on a customer premise or the replication target in an Assured hosting facility. ProtectView allows customers quick visibility into the health of their Data Protection landscape. The Dashboard in ProtectView shows a high-level summary of the system health with an intuitive click-through investigation method for diving into the root cause of any backup issue.

White-Label capability of Assured ProtectView enables customers who operate as internal service providers, or customers who are service providers, to apply their own branding to ProtectView.

Steady State Operation

Steady state operation is considered achieved once all initial backups have been successfully completed and data is flowing to the archive targets. DR customers are considered to be in steady state once the initial seed of DR data has been successfully transmitted to the replication target.

Daily Backup Operations

Assured provides a daily report view via the ProtectView platform that provides the customer with a 24-hour view of the current backup status. Assured's Support team is proactively watching active alerts via the ProtectView portal to discover and remediate issues surrounding backup, replication, archive, and hardware issues that may be causing an impact to the customer's retention schedules. Customers have full access to the Rubrik CDM UI for the purpose of self-servicing tasks such as on-demand backups, restores, or configuration changes. Customers can request these tasks be performed by the support desk as well, service level response times vary based on the severity of the issue and are described in the Service Guidelines.

Modifying Data Retention Rules

Customers can alter the retention rules via their local access in the standard level of service. The customer can opt to enable the Rubrik feature Two-Person Rule (TPR), which requires two separate logins to validate any changes retention rules. Assured can configure the TPR feature via a support request and will create local approver accounts on the customer's side based on named persons provided by the customer. Assured support can also make changes to the retention rules at the request of the customer. Any request that will result in the deletion of data or the reduction of overall retention requires written approval from the customer. Requests can be made via the normal support desk request process.

Help Desk Support and Ticket Submission

Tickets are submitted to the Assured Global Support Desk to receive support and are handled in accordance with Appendix E, Support Guidelines. Technical Account managers, generally the installing engineer, are also engaged for any support issues to ensure that tickets are worked to satisfactory completion.

Support

Main Support: +1 (833) 539 3501
support@assured-dp.com

Monitoring

Assured monitors all managed Rubrik clusters 24/7. Leveraging proprietary tools and Assured ProtectView, Assured detects hardware, software, and backup issues in the customer environment. Triggered issues are converted into internal tickets and worked by the Assured support team. The customer is contacted on any issues and changes required to be made to the deployed Rubrik systems.

Update and Patch Management

Assured tracks all deployed software versions of managed Rubrik clusters to ensure that patches and updates are applied as needed to keep the platform both secure and up to date. Management tools included with the Assured solution are also updated for OS and application fixes as available to keep them as reasonable current and stable as possible.

Log Retention within ProtectView is extended beyond the Rubrik 60-day retention to six months by default. Customers can optionally choose to extend activity log retention up to 7 years as required by their compliance policies.

Recovery

Instant Recovery: Instantly recover VMs and application by mounting directly from Rubrik to your virtual environment. No rehydration or data copying to be back online.

Global Real-Time Search: Instantly search for files across all snapshots with predictive search that delivers suggested search results as you type.

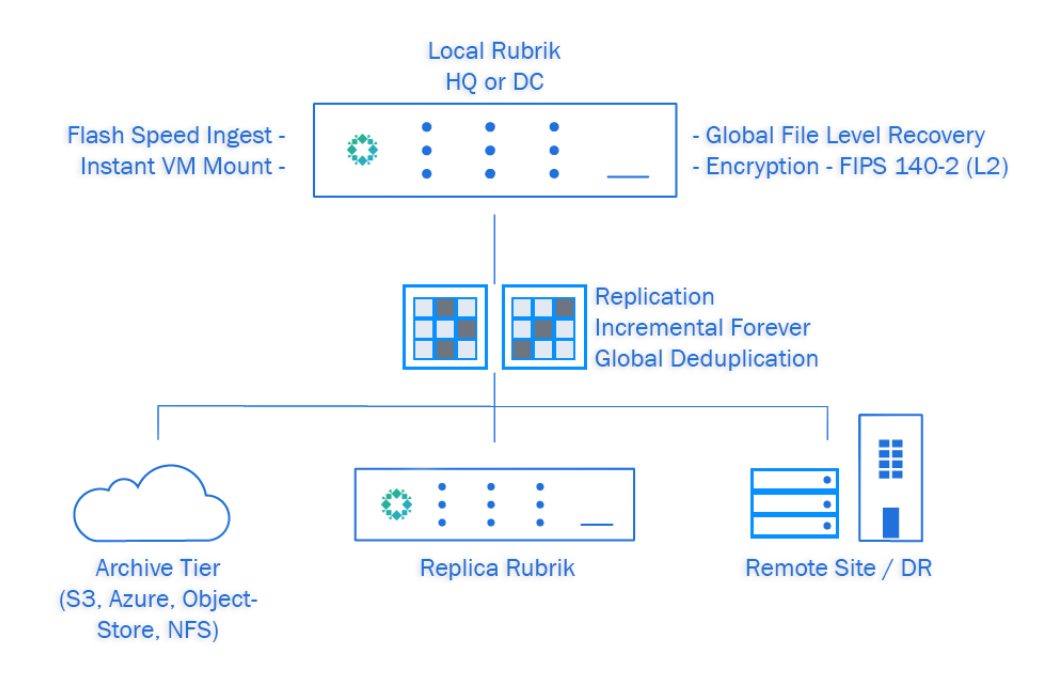
EXHIBIT 1

DESCRIPTION OF SERVICE

Summary

Managed Rubrik and archiving provided by Assured combines multiple components into a single platform service. Each component leverages modern, scale-out, technology to grow linearly with the growth of the Client's business demands. Delivered as a monthly service, the Assured components are delivered as a hosted solution connected to the Client environment via secure layer 3 protocols.

Deployment Diagram



Components

Management Appliance	Assured provided (separate from Rubrik appliance) 1U appliance deployed to customer premises for the purpose of monitoring and management of the Rubrik Solution

Network Connectivity Requirements

Internet Connectivity

Requires routable Internet connectivity via HTTPS

Recommended minimum 1Mbps of Internet for every 100GB of data stored on the source Rubrik. Additional bandwidth required for archive consolidation option.

Management and Support

Initial Install and Configuration

Archiving platform will be connected at the Assured location via object storage. The Client will be engaged to enter and establish the archiving encryption key at the time of setup.

Ongoing Support

Assured will provide ongoing support for the components of the services. Support issues discovered by the Client will be emailed to the support email address below. Client will have access to the Assured web-based help desk for submitting tickets as well. Client will supply users who have access to the helpdesk portal and who is authorized to request changes on the platform.

Support Email Address	globalsupport@assured-dp.com
Standard Support Hours	24 hours a day, seven days a week

Included Support Services

Service	**Description**
Rubrik Solution Support	All Rubrik software updates • Assured receives "early release" code up to six (6) months prior to GA • All upgrades run in our lab before recommended deployment • Customer is briefed on new features, changes, improvements, bug fixes prior to update • Actual update is pre-scheduled with the customer Rubrik backup activity • "Best practice" assistance is provided during backup activity setup to include retention and archive policy creation Trouble Ticketing • Assured provides Tier I/II support • Assured manages any Tier III (Rubrik) trouble tickets on behalf of customer New user training as required Proactive quarterly business reviews Customer access to Assured "ProtectView" monitoring solution
Availability Monitoring	24/7 Monitoring of Rubrik appliance • Uptime • Performance availability • Error and logging • Backup success/failure Archive target availability
Capacity Monitoring	• Capacity monitoring of Rubrik appliance • Daily alerts at and above 85% capacity

	• Archive consumption - monthly
Reporting	Daily Report • Backup activity reporting Backup activity failure alert • Customer is notified as soon as our solution discovers a problem. The Assured management appliance polls the Rubrik once every five (5) minutes

Pricing for Components

Components for Assured services are billed based on the following methods as described in the table below

Part	Description	Pricing
Management Appliance	Assured 1U appliance deployed to customer premises for the purpose of monitoring and management of the Rubrik Solution	Per Month, and based on the number of Rubrik Nodes under management

Appendix C: Customer Provided Information

Customer Action	Description
Power	Management Server requires 2x NEMA 5-15 or C13 available outlets (specified type in advance) Rubrik appliance requires 2x NEMA 5-15 or C13 available outlets.
Rack Space	Rack Units expected standard 19” width rack with standard depth. 1 Rack Unit for Assured Management Server 2 Rack Units per physical Rubrik appliance
vSphere Credentials	vSphere local or domain user with the appropriate rights to perform backup and recovery (Appendix B)
Server / Application Credentials	Local or domain credentials for target physical or application only Data Protection targets (SQL, Linux)
Provision IP Addresses	IP Addresses on the customer’s internal network are required for the following devices (Base install is 8 IPs): 1) 1 IP per node for Rubrik. Middle number in model indicates number of nodes (R348 = 4 nodes) 2) 1 IP for Lights Out controller of management server 3) 1 IP for management ESX 4) 2 IP for management collectors
Network Ports	3x 100/1000Gbps Copper Ethernet connections: 1x Management Lights Out (optional) 1x Assured Monitoring Node Manage port 1x Rubrik Management per Appliance 2(4)x 10Gbps SFP+ compatible ports (w/SFPs installed) 2x 10Gbps SFP+ per Rubrik Appliance 2x 10Gbps SFP+ per Management node (optional if management only, recommended if EDGE installation)
VLAN Configuration	Assigned VLANs for (can all be the same): Management Network Data Protection Network
Firewall Configuration All ports: Appendix A	Outbound 443 for: Rubrik Call Home / Remote Support Assured ProtectView remote support / logging Bi-directional 7785 TCP to Assured for: Rubrik Replication (if enabled)
Archival Target Preparation	S3 Targets:

Customer Action	Description
	AWS access ID and Secret with appropriate permissions for bucket creation, read, and write capabilities. Generated RSA key also required for encryption. NFS Targets: NFS path with available permissions for Rubrik Cluster IPs
Protection Scheme	Base SLA: The Base SLA is the default backup policy that will "catch" any created VM to ensure backups are being completed at a minimum level for any created VM. Critical Data SLA: The Critical Data SLA is the most stringent data retention policy that should be applied to any targets (virtual machines, filesets, or databases) that need to meet compliance or strict company restrictions for retention. Other SLAs: Any additional SLAs the customer requires.

Appendix D: RACI matrix

RACI = Responsible; Accountable; Consulted; Informed

Description	Assured Data Protection	Customer
Design and Planning		
Document the design	RA	CI
Define backup and retention policies	CI	RA
Determine topology	ACI	R
Set schedule and Milestones	RA	CI
Identify data to be protected under which policy	CI	RA
Provide technical resource for solution	RA	I
Provide networking requirements	RA	CI
Provide technical resource for customer environment	I	RA
Provide documentation for networking	RA	I
Provide business resource for customer environment	I	RA
Implementation		
Provide hardware for backup solution	RA	CI
Provide power and rack space for backup solution	CI	RA
Provide physical access for installation	I	RA
Provide networking infrastructure	CI	RA
Rack and cable hardware	RA	CI
Perform initial setup and configuration of backup system	RA	CI
Train customer on the usage of the backup system	RA	CI
Configure networking	CI	RA
Connect to Archive locations	RA	CI
Connect to replication locations	RA	RCI
Provide Active Directory credentials	I	RA
Provide vCenter Credentials	I	RA
Build DR Run Book	RA	RCI
Configure DR environment	RA	CI
Complete test plan	RA	RI
Steady State Operations		
Break/fix for backup hardware	RA	CI
Break/fix for backup software	RA	CI
Software updates for backup and monitoring software	RA	CI
Notification of DR Test	CI	RA
Notification of DR invocation	I	RA
Execution of DR Runbook	RA	CI
Notification of discontinuing DR	CI	RA
Discontinuation of DR Environment	RA	CI
Notification of network changes on customer side	CI	RA
Contract Completion		
Notification of non-renewal	I	RA
Provide options for existing data	RA	CI
Select option for existing retained data	CI	RA

Appendix E: Service Guidelines

Overview

The Assured Data Protection Inc. (Assured) Support Guidelines document outlines the support provided by service component across the Assured portfolio. The Support Guidelines documentation is superseded by any called out items in the Master Services and License Agreement.

Severity and Response Guidelines

Severity levels are determined by the level of impact related to the customer's usage of the Services. Severity level is assigned by the responding engineer based on the described or determined impact based on the initiating event. Customer may request a change in severity if there is a change in the impact during the course of trouble resolution.

Definitions

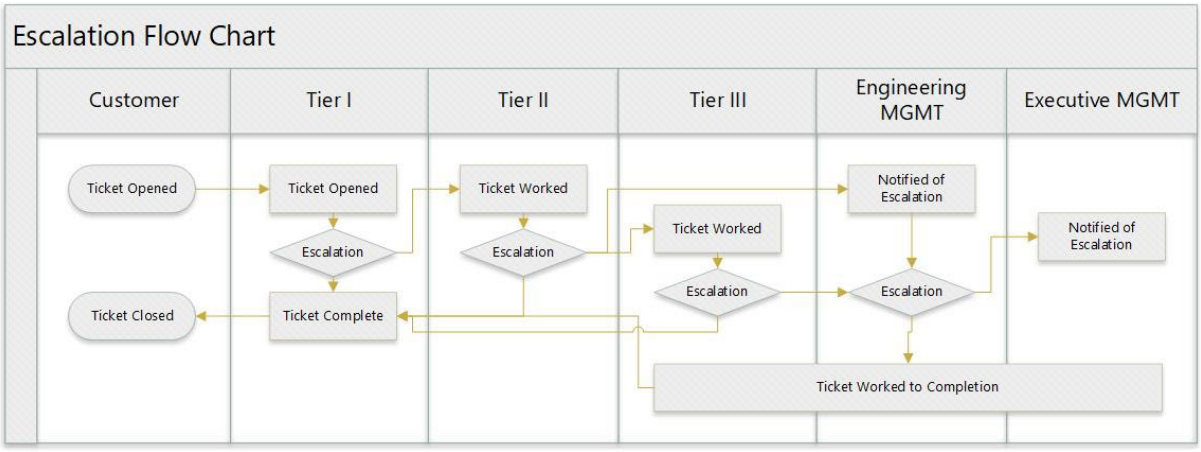
Severity

Severity is defined as the business level impact of the ticketed event. Business impact levels are determined by engineering analysis against the severity levels defined below.

Escalation

Escalation is defined as the increased visibility and urgency to correct a problem as it relates to the amount of time the ticketed event has existed. Escalation does not change the severity of a ticketed event without request by customer or change in the nature of the event. The Escalation path is shown in table below:

Escalation Path



Response Time

Response Time is defined as the amount of time between the initiation of a ticketed event and the confirmation by the Assured-Data Protection support team that the ticket has been received and being worked by an engineer. Tickets can be initiated by programmatic alerting or via direct customer contact through e-mail, telephone, or web-based ticketing.

Severity Levels

Severity	Description of Classification
P1 – Critical	Service unavailable preventing a recovery action or where there is a direct impact to business functionality. Examples: 1. Disaster Recovery environment offline during a live event 2. Hardware failure of on-site appliance where data is unable to be restored. 3. Failure to restore an object due to service availability
P2 – High	Service degraded or unavailable with potential impact to business function or capability. Examples: 1. Replication link down 2. Hardware failure causing intermittent interruption to backups 3. Errors across many object backups
P3 – Standard	Service degraded but still meeting continuing service levels. Examples: 1. Hardware redundancy failure (HD in RAID group, redundant node, etc) 2. Errors in isolated object backups (single VM, single fileset, etc..) 3. Disaster Recovery environment performance of On Demand resources
P4 – Low	Non-service impacting or degraded issue or concern. Examples: 1. Request version upgrade 2. Change or modify SLA set 3. Schedule a DR test

Severity levels are set upon ticket creation by the responding engineer based upon the generated alert or customer request.

Response and Escalation Time Guidelines

Severity	Response Time	Escalation Time
P1 – Critical	Within 60 Minutes	2 hours
P2 – High	Within 90 Minutes	6 hours
P3 – Standard	Within 1 Business Day	24 hours
P4 – Low	Within 2 Business Days	48 hours

Hardware Servicing and Repair

Assured Data Protection hardware servicing is included as part of managed services delivered to a customer on Assured Data Protection provided equipment. Any hardware furnished by the customer is outside the scope of this section of the support guidelines.

Rubrik OEM Hardware

Hardware provided by Rubrik is subject to the Rubrik Return Materials Authorization (RMA) process. The Rubrik RMA process provides next business day replacement for all parts requiring replacement with end customer acting as the “Smart Hands” to perform the replacement of the failed component. Assured Data Protection acts as the intermediary on the customer’s behalf to contact Rubrik upon a ticketed event found to be a hardware issue and facilitate the RMA.

Assured Data Protection Provided Hardware

Hardware provided by Assured as part of the service is provided with a next business day advance-delivery parts warranty. Assured facilitates any hardware RMA through ticketed events where the issue is found to be hardware related. Physical replacement of the part is contract dependent. Customers with on-premises engineers can care for physical replacement. Customers with no on-site engineers can request this option be added in the contract.

Hardware Support Table

Hardware Type	Responsible	Part Delivery Time	Part Replacement
Rubrik OEM Hardware	Assured Data Protection	Next Business Day	Contract Dependent
Assured Provided Hardware	Assured Data Protection	Next Business Day	Contract Dependent
Customer Provided Hardware	Customer	Customer OEM Provider	Customer / OEM

Support Contact Information

Assured Data Protection Support Center operates on a 24/7/365 basis. Customers are encouraged to reach out to their account team during normal business hours but can always contact the standard support lines as described below based on the location of the service.

Global Support Desk

US Toll Free	+1-833-539-3501
UK Toll Free	+44 (0)800 0485201
Global Email	support@assured-dp.com