SERVICE DESCRIPTION FOR

Assured Data Protection

Andrew Eva
andrew.eva@assured-dp.com

07/05/2023

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.

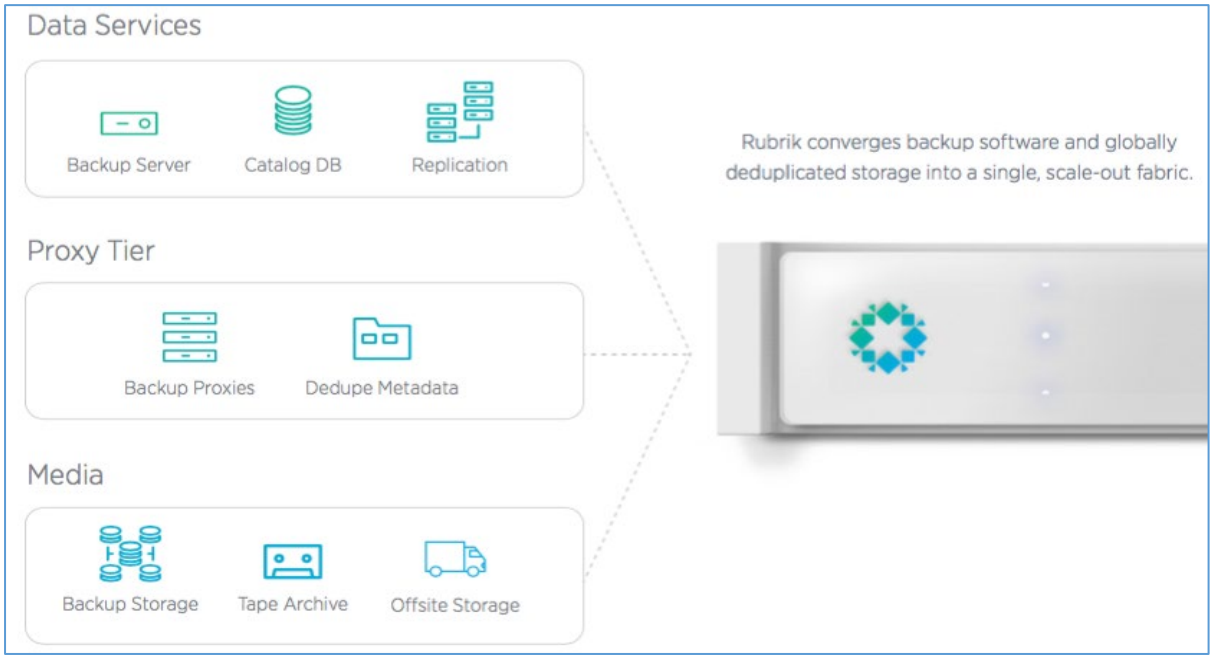
Rubrik Overview

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 are 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 accessing 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.

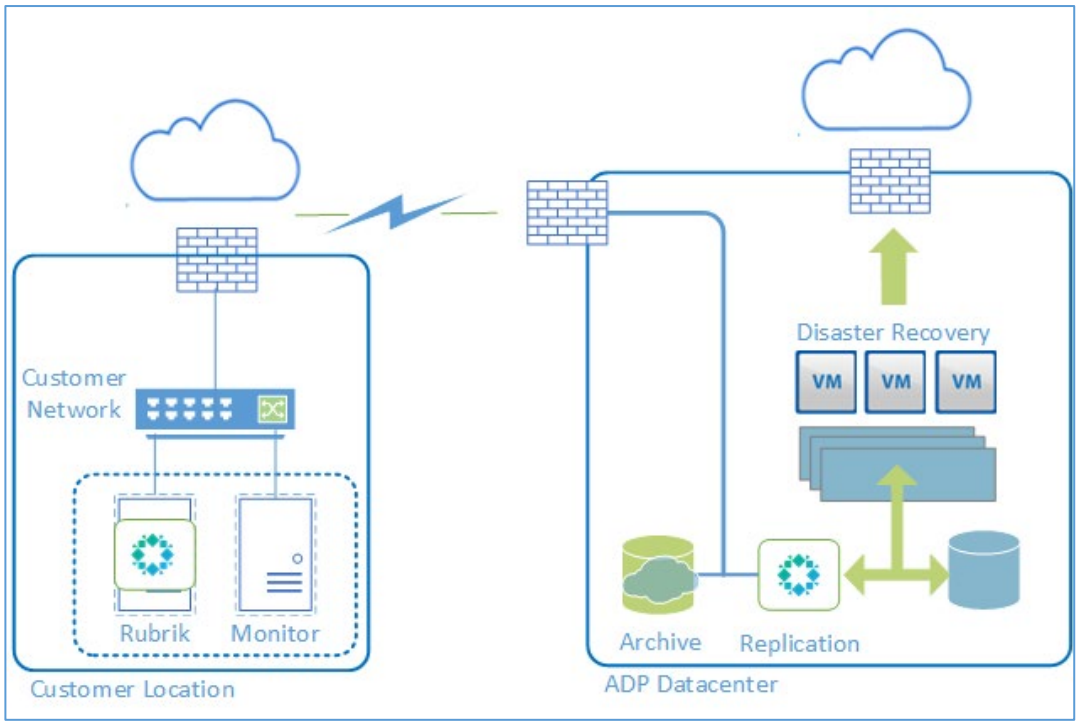
Management

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.

Recovery

Instant Recovery: Instantly recover VMs and applications 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.

Assured Data Protection Managed Solution Overview



The Assured Managed Solution is a suite of services delivered to Assured customers as a unified data protection strategy. Employing the Rubrik converged data management platform as the base of the Assured Solution delivers a disk-only topology to meet the demands of the most challenging backup environments. The converged disk-only topology treats data as it lives, paving the way to efficiently deliver deduplication, intelligent archiving, and near-instant recovery. Intelligent design principles based on RESTful APIs and process simplification allows automation of data protection strategies to be easily considered and deployed with existing strategies, creating an internal service delivery platform for any enterprise.

The Assured Managed Solution brings simplicity, automation, and performance to protecting workloads, enabling IT staff to allocate their valuable time on managing production, instead of troubleshooting backups.

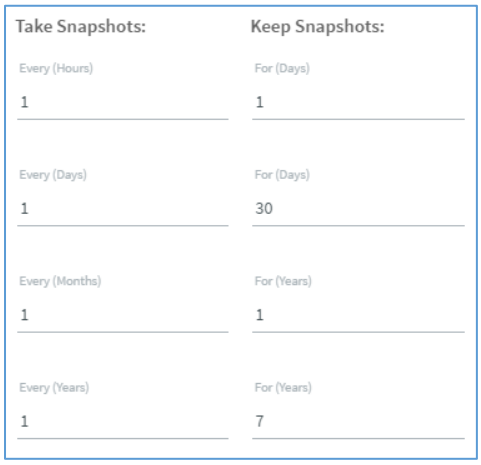
Data Protection Service

Assured's Data Protection Service includes the Rubrik converged backup solution as well as the Assured ProtectView portal.

Data Retention

Assured leverages the Rubrik data retention methodology of SLAs to govern the retention history of protected data in the Assured ecosystem. Rubrik SLAs provide the option to select the frequency the data is collected and the length of time those points in time, or snapshots, are kept. Retained data is stored in a deduplicated state on the Rubrik appliance (physical or virtual) until the SLA moves the data to a configured archive target.

Recovering data from the local appliance or from the archive repository is performed the same way through the user interface, intelligently pulling only the required data from the remote storage locations to minimize the required network traffic and to ensure speed of recovery for the workload.



Data can be replicated to a partner Rubrik cluster that is paired with the source cluster and the customer can set via the UI the amount of retention to keep on that destination cluster.

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.

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.

Disaster Recovery Service

Providing Disaster Recovery (DR) services creates an avenue for your business to be back to full operations after suffering an outage. Comparing DR services starts with understanding the difference between a true DR and a business continuity service. Business continuity allows your business to limp along after a disaster, typically running at partial capacity with just enough resources to keep your services available. DR service allows your business to run at full speed, creating the experience for your customers of no degradation in performance or functionality.

Assured's DR Service allows customers to select whether a given part of their service requires full DR, or simply continuity. Reserving resources and guaranteeing performance allows those workloads designated for full DR to perform as they would in production. Whereas those workloads specified for business continuity leverage on-demand resources that may contend with other cloud-workloads for full performance. Customers are enabled to design a solution to meet the needs of their business with well-defined costs.

Disaster Recovery Resources

Customers leveraging the Assured DR solution have the option to leverage Reserved or available On-Demand resources. Resources can be enabled by recovering any of the protected images stored in the replicated Rubrik platform, or by deploying an available template from the Assured catalog. Reserved resources are dedicated to specific customers and not oversubscribed On-Demand resources leverage available capacity in the Assured infrastructure and are subject to fluctuations in available performance.

Assured Data Protection Service Options

Available Service Options

Customers have access to the full suite of available Assured service delivery configurations. Standard offerings are defined below. Additionally, custom service options can be configured and documented with a custom statement of work.

Standard Service Options

Assured delivers data protection in three, simple to comprehend and define, tiers. Each tier calls out specific service delivery components from the Assured Data Protection Service Delivery section that follows.

	Tier I	Tier II	Tier III
Rubrik Appliance on Premises	✓	✓	✓
Management	✓	✓	✓
Archive (Cloud or ADP)	✓	✓	✓
Second Site Replication		✓	✓
DRaaS			✓

Disaster Recovery Services (Tier III)

Assured provided Disaster Recovery Services are delivered on top of Replication customers. The customer is responsible for all the same responsibilities as described in the Replication Only service option. Assured Disaster Recovery Services include all the components listed as part of the Assured disaster services and are provided out of the Assured facilities on Assured equipment. Disaster Recovery services delivered on top of 3rd party clouds, are not underneath this umbrella and are considered custom.

Disaster Recovery Services Include

- Custom runbook & automated boot order scripting
- Single public IP address
- Dedicated virtual firewall instance
- Two DR Test per year
    - Waiver of OnDemand resource consumption charges for a period of up to six days per test
- Dedicated bundle of resources (RAM & vCPU)

Additional Service Options

Additional Service Options are available for Customers that do not fit into the specified Tiered service offerings above as a fully managed service.

Management Only

Existing Rubrik installations are eligible to be managed in place by Assured. Assured Management Only option overlays the Assured management and includes all monitoring and troubleshooting involved in the management component services. The customer is

responsible for ensuring that the Rubrik maintenance is kept current for any managed installation.

Replication Only

Existing Rubrik installations in search of a secondary target for replication can leverage Assured for Replication Only services. Assured provides a Rubrik target and bandwidth to receive replication traffic for Customer owned Rubrik installations. The customer is responsible for ensuring the source environment is under Rubrik support and within the supported release schedules. Replication Only can stand alone (Hybrid Tier II) or coupled with our Disaster Recovery Services (Hybrid Tier III).

Archive Storage

Customers can also utilize Assured hosted object storage for the purposes of establishing an archive storage target for the purposes of removing data from the expensive primary disk subsystem associated with Rubrik or other backup platforms. This process is typically process driven and mirrors the data lifecycle and provides an appropriate repository for data that has migrated from a "critical" category to that of "important". Customers connect via standard S3 or NFS over private circuit (VPN, MPLS, fiber, etc…)

Assured Data Protection Service Delivery

Installation and Initial Configuration

Assured Engineers perform the installation and initial configuration in cooperation with the customer. Installation and configuration time is generally considered to be less than a half day of time if all the required prerequisites are available.

Customer Provided Information

The customer is required to provide and configure their environment ahead of installation so that the install can go smoothly. Detailed in Appendix C, this information is critical to ensuring that an installation can be performed without delay.

Appliance Installation

Assured Data Protection will either bring or ship in advance the hardware required to perform the installation. Included in that hardware will be mid-length cabling for both power and connectivity, as well as any required connectors needed on the hardware provided by Assured. Any required SFPs in the customer hardware will be provided by the customer as per the table above.

Data Protection Service Deployment

Installation of the Assured Data Protection Managed Solution is performed by an Assured engineer via remote connection or on the customer premise. Ensuring that all steps are completed properly, the Assured engineer will leverage the installation checklist and the RACI matrix provided in Appendix D.

Target time to complete the installation is estimated at around 4 hours, but it is advised for the customer to clear the day in the event there are any unexpected issues or if all the information required to complete is not able to be obtained within the time allotted. The below list is an abbreviated version of the checklist that provides a baseline of what will be completed during the installation. These tasks will be performed by the Assured engineer with the customer engineer on hand as a training exercise.

1) All equipment racked, cabled and configured.
2) Configure monitoring platform and validate connectivity.
3) Base SLA created.
4) Critical Data SLA created.
5) Assign Base and Critical Data SLAs to the initial backup targets requested by the customer to begin the initial ingest of data.
6) Set initial ingest windows for remaining data.
7) Educate customer on the portal

Disaster Recovery Installation

Assured Data Protection Disaster Recovery services consist of a replication target for the customer premise Rubrik cluster, network connectivity, and available compute capacity for recovery. Disaster Recovery is configured if the customer has purchased the service as part of their on-premise installation, or if the customer is an Edge installation where DR is included. Customers who are existing Rubrik customers can add replication to Assured's DR services and become configured in the same manner as described here.

Environment Design Baseline

Assured Engineers engage with the customer to build a design baseline of the customer's DR environment. The Design Baseline is a joint exercise where the customer audits the workloads, they will require in DR so that the networks and base environment can be built. Included in this design baseline is determining the appropriate method of connectivity between the customer environment and the Assured DR platform. Once the Design Baseline is complete, the Assured team will build the base environment in their DR platform and a date for initial connectivity will be set.

Connectivity

Connectivity between the Customer environment and the Assured DR environment facilitates the consistent communication between the source and destination replication Rubrik clusters as well as creating the avenue for connectivity needed during a DR event. Assured can support almost any connectivity the option preferred by the customer. The primary methods are broken out as follows below:

Layer 3

Layer 3 connectivity refers to a type of connectivity where traffic is routed from the customer's environment to the DR environment. Connectivity of this type are typically VPN or private line type connections. The advantage to a Layer 3 topology is they are quick to configure and allow the customer to create a well-defined logical network space for their DR environment. The disadvantage to Layer 3 environments comes with duplicate IP addresses produced by recovered virtual machines. Such duplicates either need to be isolated or re-addressed, both of which create significant effort at the time of DR.

Layer 2

Layer 2 connectivity refers to an extension of the customer's network into the DR space. Connectivity of this type are typically performed over MPLS, Private Line, SD-WAN (Software Defined Wide Area Network), or a 3rd party service such as Equinix Cloud Exchange. Layer 2 connectivity can be blended with Layer 3 to offer customers both the ability to route traffic into devices on isolated networks within the Assured

DR platform as well as extend existing virtual networks (VLANs) from their primary locations. The key advantage to layer 2 connectivity is enabling the recovery of a single VM on a network segment without needing to change IP addresses or routing choices. The primary disadvantage to layer 2 connectivity is the time to configure.

Initial Ingest of Data

Established communication between the customer location and the Assured environment enables the initial ingest of data from the customer premise Rubrik platform and the Assured repository. Sizing of the initial ingest and the amount of bandwidth available plays a large part in the method of consuming the initial ingest of data. Most customers grow their bandwidth at a rate consistent with the size of their environment, making the available bandwidth for performing the initial ingest to be appropriate at the onset. Many bandwidth providers also bursting capabilities to facilitate the ingest.

Customers who have a significant data set can be seeded using a physical appliance for transportation. Physical seeding leverages local networks to ingest the first round of data. Once ingested, the physical appliance would then be transported to the Assured facility and incremental updates would pick up from that point forward.

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.

US Support
Main Support: +1 (908) 603-8049
Toll Free Support: +1 (866) 318-9787
US HQ Office: +1 (703) 888-4783
us-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 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.

Appendix A: All Rubrik Port Requirements

Port	Source	Destination	Description
22 TCP	a. Rubrik cluster b. Local client	a. proxy.rubrik.com b. Rubrik cluster	a. Provides a tunnel with Rubrik support. b. Provides the ability to launch an SSH session for support and administration.
25 TCP	Rubrik cluster	Email server	Allows the Rubrik cluster to send email alerts to administrators. Only required when the email server supports this port.
53 UDP	Rubrik cluster	DNS server	Permits hostname resolution.
80 TCP	a. Rubrik cluster b. Web UI clients	a. proxy.rubrik.com b. Rubrik cluster	a. Permits transmission of statistics. b. Handles redirection of Rubrik web UI clients to HTTPS.
88 TCP/UDP	Rubrik cluster	Active Directory server	Permit Kerberos communication.
111 TCP	VMware ESXi hosts	Rubrik cluster	Provides an NFS datastore for ESXi hosts.
123 UDP	Rubrik cluster	NTP server	Provides access to network time protocol (NTP) servers for time synchronization.
389 TCP/UDP	Rubrik cluster	Active Directory server	Permit LDAP communication.
443 TCP	a. Rubrik cluster b. Rubrik cluster c. Web UI clients d. Rubrik cluster e. Rubrik cluster f. Local web browser	a. s3.amazonaws.com b. logs.rubrik.com c. Rubrik cluster d. Amazon S3 URL e. VMware vCenter server f. IPMI on a Rubrik node	Required for: a. Uploading support bundles. b. Uploading error logs. c. Secure communication between web UI client and Rubrik cluster. d. Transmitting data to the archival location. e. Information queries about virtual machines. f. Web interface with IPMI on a Rubrik node.
464 TCP/UDP	Rubrik cluster	Active Directory server	Permit Kerberos password set/change communication.
465 TCP	Rubrik cluster	Email server	Allows the Rubrik cluster to send email alerts to administrators. Only required when the email server supports this port.
587 TCP	Rubrik cluster	Email server	Allows the Rubrik cluster to send email alerts to administrators. Only required when the email server supports this port.
623 UDP	Remote management tool	IPMI on Rubrik node	Provides access to the IPMI system on a Rubrik node.

Port	Source	Destination	Description
902 TCP	Rubrik cluster	VMware ESXi hosts	Permits network block device (NBD) data transfers.
2013 TCP	Rubrik cluster	Rubrik cluster	Allows sharing of statistics between the nodes of a Rubrik cluster.
2014 TCP	Rubrik cluster	Rubrik cluster	Allows sharing of statistics between the nodes of a Rubrik cluster.
2200 TCP	Rubrik node	Rubrik node	Allows node to node SSH communication during upgrade.
2049 TCP	Rubrik cluster	NFS server	Permits communication with a NAS device that is being used as an archival location.
3260 TCP	Rubrik cluster	iSCSI targets	Permits iSCSI data transfers.
5900 TCP	VNC client	IPMI on Rubrik node	Permits a virtual networking connection with the IPMI interface on a Rubrik node.
7000 TCP	Rubrik cluster	Rubrik cluster	Allows process arbitration between the nodes of a Rubrik cluster.
7781 TCP	Rubrik cluster	Rubrik cluster	Permits the Rubrik cluster to load basic software and configuration information (bootstrap) during cluster configuration.
7785 TCP	a. Replication source b. Replication target	a. Replication target b. Replication source	a. Replication data transmission. b. Replication data transmission.
10000 TCP	Rubrik cluster	Rubrik cluster	Allows sharing of Rubrik cluster file system (SDFS) data between the nodes of a Rubrik cluster.
12800 TCP	Rubrik cluster	a. Physical Linux host b. Windows Server host	a. Permits contact with the Rubrik Backup Service software on the Linux host. b. Permits contact with the Rubrik Backup Service software on the Windows Server host.
12801 TCP	Rubrik cluster	a. Physical Linux host b. Windows Server host	a. Permits contact with the Rubrik Backup Service software on the Linux host. b. Permits contact with the Rubrik Backup Service software on the Windows Server host.

Appendix B: vSphere Permissions

The vCenter role that is assigned to a Rubrik cluster must provide specific privileges on the vCenter. Table below describes the minimum privileges on the vCenter Server that are required by the vCenter role that is assigned to the Rubrik cluster. The table uses an asterisk (*) to indicate a privilege that Rubrik does not require in the current release but anticipates requiring in a later release.

Privilege category	Privilege	Description
Datastore	Allocate space	Used by Rubrik to create virtual machines for export. Also used by Rubrik to provide space for delta files on the datastore when creating a snapshot.
Datastore	Browse datastore	Permits Rubrik to find and download the vmware.log file for a virtual machine after a failed snapshot and to send the vmware.log file out for support.
Datastore	Configure datastore	Allows Rubrik to connect the datastore on a Rubrik cluster to the vCenter for Live Mount and Instant Recovery.
Datastore	Low level file operations	Permits Rubrik to ingest and to export the contents of snapshot VMDKs.
Datastore	Move datastore*	Allows Rubrik to place a Live Mount datastore into a vCenter folder to enhance manageability.
Datastore	Remove datastore	Used by Rubrik to detach a Live Mount datastore that is no longer in use.
Global[a]	Disable methods	Permits the Rubrik cluster to provide VMware vStorage API (VADP) license information to the vCenter. Required when using VADP to transfer VMDK contents.
Global	Enable methods	Permits the Rubrik cluster to provide VADP license information to the vCenter. Required when using VADP to transfer VMDK contents.
Global	Licenses	Permits the Rubrik cluster to provide VADP license information to the vCenter. Required when using VADP to transfer VMDK contents.
Host	Configuration: a. Storage partition configuration	Configuration privileges: a. Used by Rubrik for storage partition configuration when attaching Live Mount datastores to ESXi hosts.
Network	Assign network	Permits Rubrik to connect Instant Recovery virtual machines to a network when powering on the virtual machines.
Resource	Assign virtual machine to resource pool	Allows Rubrik to allocate resources on an ESXi host for powering on virtual machines that are created through the Export, Live Mount, and Instant Recovery features.
Sessions	Validate session	Used by Rubrik to discover, cache, and reuse previous vCenter sessions.
Sessions	View and stop sessions	Used by Rubrik to discover, cache, and reuse previous vCenter sessions.

Privilege category	Privilege	Description
Virtual machine	Configuration: a. Add existing disk b. Add new disk c. Change resource d. Disk change tracking e. Disk lease f. Rename* g. Settings h. Swapfile placement	Configuration privileges: a. Used by Rubrik when creating virtual machines through the Export, Live Mount, and Instant Recovery features. b. Used by Rubrik when creating virtual machines for the Export, Live Mount, and Instant Recovery features. c. Permits Rubrik to configure virtual machine resources that are created in resource pools. d. Used by Rubrik to enable incremental snapshots, and to reset CBT when required. e. Allows Rubrik to acquire leases to permit using VADP for transferring VMDK contents. f. Permits Rubrik to rename the Live Mount datastore to enhance manageability. g. Used by Rubrik to configure virtual machines that are created through the Export, Live Mount, and Instant Recovery features. h. Allows Rubrik to power on virtual machines that are created through the Export, Live Mount, and Instant Recovery features.
Virtual machine	Guest Operations: a. Guest Operation Modifications b. Guest Operation Program Execution c. Guest Operation Queries	Guest Operations privileges: a. Permits Rubrik to deploy the Rubrik VSS agent into guest operating systems when creating application consistent snapshots. b. Permits Rubrik to start the Rubrik VSS agent on guest operating systems when creating application consistent snapshots. c. Allows Rubrik to monitor and manage the Rubrik VSS agent while the agent is running on guest operating systems.
Virtual machine	Interaction: a. Answer question* b. Backup operation on virtual machine c. Device connection d. Guest operating system management by VIX API e. Power Off f. Power On g. Reset* h. Suspend* i. VMware Tools install*	Interaction privileges: a. Permits Rubrik to automatically handle situations where a virtual machine is in a stuck state waiting for a question to be answered. b. Used by Rubrik to perform backup operations on virtual machines. c. Used by Rubrik to connect and disconnect devices which are attached to virtual machines that are created through the Export, Live Mount, and Instant Recovery features. d. Permits Rubrik to manage a guest operating system along with the Rubrik VSS agent when creating application consistent snapshots. e. Allows Rubrik to power off Live Mount virtual machines and Instant Recovery virtual machines before deleting the virtual machine. f. Allows Rubrik to power on Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines after creating the virtual machine. g. Permits Rubrik to manage Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines after creating the virtual machine. h. Permits Rubrik to manage Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines after creating the virtual machine. i. Allows Rubrik to upgrade VMware Tools on a guest OS as needed to prevent the guest OS from hanging or crashing when quiescing for a snapshot.

Privilege category	Privilege	Description
Virtual machine	Inventory: a. Create new b. Move c. Register d. Remove e. Unregister	Inventory privileges: a. Used by Rubrik to create Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines. b. Permits Rubrik to move an original virtual machine into a "deprecated" folder before replacing the original with an Instant Recovery virtual machine. c. Used by Rubrik to create Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines. d. Allows Rubrik to remove Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines. e. Allows Rubrik to remove Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines.
Virtual machine	Provisioning: a. Allow disk access b. Allow read-only disk access c. Allow virtual machine download d. Allow virtual machine files upload	Provisioning privileges: a. Permits Rubrik to write the VMDK contents of Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines. b. Permits Rubrik to read the VMDK contents of Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines when backing up the virtual machines. c. Allows Rubrik to download the non-VMDK files of protected source virtual machines, including configuration files and support logs. d. Allows Rubrik to upload non-VMDK files of Export virtual machines, Live Mount virtual machines and Instant Recovery virtual machines, when creating and configuring the virtual machines.
Virtual machine	Snapshot management: a. Create snapshot b. Remove snapshot c. Rename snapshot* d. Revert to snapshot	Snapshot management privileges: a. Permits Rubrik to create temporary snapshots of virtual machines for ingest into Rubrik cluster storage. b. Permits Rubrik to remove temporary snapshots of virtual machines that were created for ingest into Rubrik cluster storage. c. Allows Rubrik to manage the temporary snapshots of virtual machines that were created for ingest into Rubrik cluster storage. d. Used by Rubrik to prepare an Export virtual machine with data from a Rubrik snapshot.

a. The Global privileges **Disable methods**, **Enable methods**, and **Licenses**, are only required for VDDK 5.1 and VDDK 5.5. Upgrading to vSphere 5.1 U3 eliminates the requirement. Refer to the VMware Knowledgebase article: Restoring or backing up virtual machines using VDDK API fails with the error: Not licensed to use this function. Error 16064 at 2357 (2063054).

b. Resetting CBT is required when a known VMware issue occurs that results in vSphere failing to maintain the setting.

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

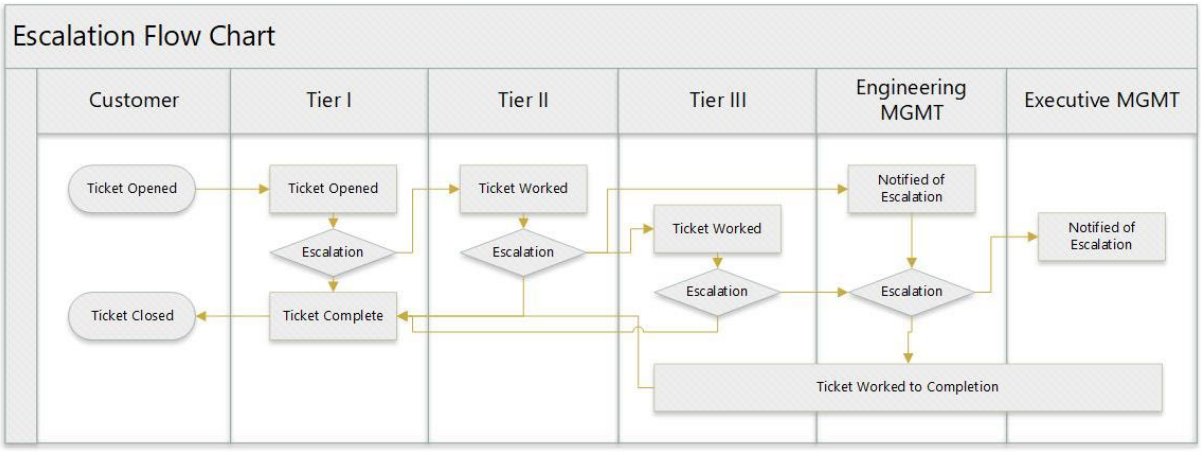
Severity

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 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 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