REFERENCE ARCHITECTURE

Rubrik and VMware vCloud Director

TABLE OF CONTENTS

3 INTRODUCTION

3 AUDIENCE

3 SOLUTION OVERVIEW

- 4 Declarative SLA Domains
- 5 Assigning SLA Domains
  - Protection at the vCloud Director instance level
  - Protection at the organization level
  - Protection at the organization virtual datacenter level
  - Protection at the vApp level
  - Protection at the virtual machine level
- 7 Recovery Methods
  - Export
  - Instant Recovery
  - Live Mount
  - File-Level Recovery

12 ARCHITECTURE OVERVIEW

- 14 Multi-Tenancy
  - Authentication
  - Mapping Resources

15 OPERATIONAL OVERVIEW

- 15 Use Cases
  - Tenant Self-Service
  - Protecting Isolated Workloads
  - CloudOut (Archival)
  - CloudOn (Instantiation)

19 CONCLUSION

20 ABOUT THE AUTHORS

INTRODUCTION

Rubrik Cloud Data Management (CDM) provides SLA driven data protection and management for VMware vCloud Director (vCD) vApps. vCloud Director is industry leading multi-tenant Cloud Management Platform used by Cloud Providers across the globe.

When a vCloud Director instance is added to a Rubrik cluster, the Rubrik cluster automatically discovers the vCloud Director constructs and resources, such as:

- Organizations
- Organization virtual data centers
- vApps
- Virtual machines

The constructs are the building blocks for deploying vCloud Director cloud and provide the basis for assigning SLA domain protection to the vApps. Rubrik CDM manages and protects the data in vApps using the same SLA Domain approach that it provides for vSphere virtual machines.

The Rubrik cluster provides full protection of vApps, backing up not just virtual machine data but also vApp data and configurations, including networks, boot order, and access lists.

AUDIENCE

This reference architecture is intended to provide CTOs, solutions architects, and administrators with information about the architecture, implementation, and benefits of an integrated Rubrik and VMware vCloud Director solution.

For the remainder of this document, “virtual machines” will be referred to as “VMs” and “disaster recovery” as “DR.”

SOLUTION OVERVIEW

At the heart of the Rubrik architecture lies the SLA domain. The SLA domain reduces daily operational management by enabling a single policy engine to orchestrate the protection and management of services across the entire data lifecycle. SLA domains can be applied anywhere in the vCloud Director hierarchy stack: the organization, the organization virtual data center (oVDC), vApp, or VM levels, allowing service providers to be as broad or as granular as they desire with data protection strategies.

End-to-end data management is provided by Rubrik for all vCloud Director provisioned workloads. End users can have instant and secured data-access, protection policy automation, and data orchestration across environments in a completely self-serving fashion.

VMware vCloud Director is a cloud service delivery platform that functions as a cloud management plane. vCD further abstracts the underlying virtualization platform in terms of virtual data centers: provider virtual data centers (pVDC) and organization virtual data centers (oVDC). Overall, vCD provides complete multi-tenancy features and self-service access for tenants through a native user interface (UI), or through the API. Recently, VMware has evolved the vCD UI and API to support ecosystem partners, like Rubrik, for further native integration. In essence, this provides seamless, self-service tenant capabilities through the native user interface from vCloud Director (vCD).

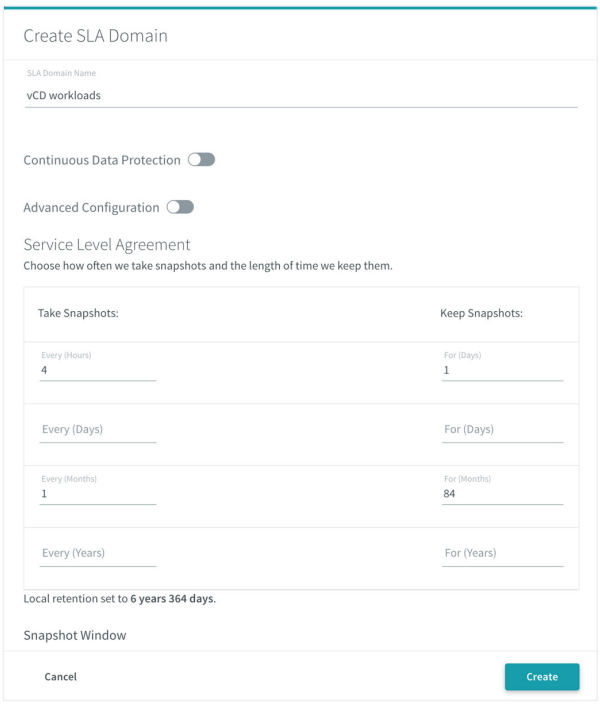
Rubrik leverages full power of vCloud Director's multi-tenant architecture to deliver simple and flexible and multi-tenant data protection service in a seamless Cloud experience. This empowers large service providers and their enterprise customers a full self-service experience directly through the cloud platform of their choice.

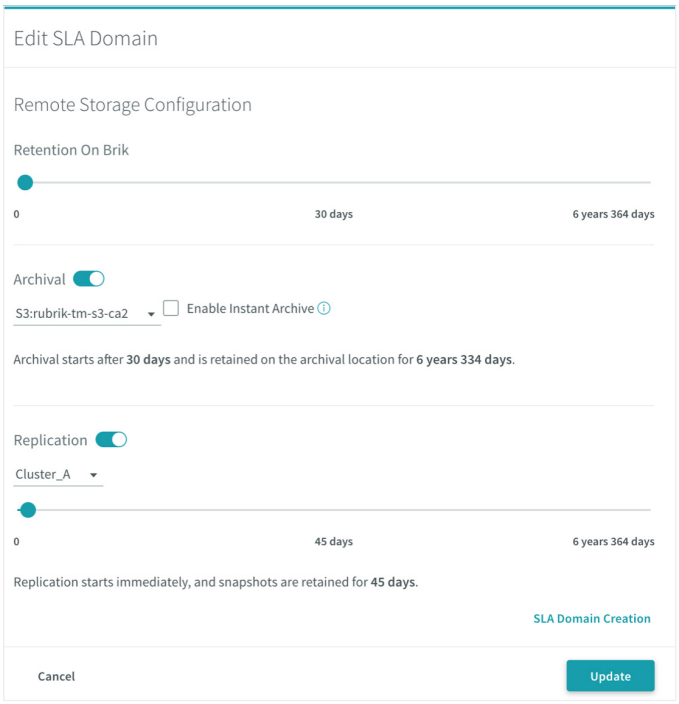
DECLARATIVE SLA DOMAINS

Rubrik orchestrates the movement of data from initial ingest and propagation of that data to other data locations, such as replicating to remote clusters or Rubrik Cloud Edition, as well as data archival. A single SLA policy is used to dictate all data lifecycle specifications, and the data control plane does the rest.

For this section, an example SLA policy is:

- Take a backup:
  - Run a snapshot every 4 hours and retain hourly backups for a day
  - Run a snapshot every month and retain monthly backups for 7 years
- Archive to Amazon S3 after 30 days
- Replicate data to another Rubrik cluster and retain for 45 days.





Data is ingested and retained according to the frequency specified in the SLA policy. The example policy is configured to store 30 days of data within the Rubrik cluster. Once that period has elapsed, data is archived to another location for long-term retention. In this case, data is archived to Amazon S3 for another 6 years and 335 days. There is no need for an administrator to manage, prune, or validate that data has been archived; these activities are all handled natively by Rubrik to reflect how they were expressed in the SLA.

The policy also specifies to replicate data from one Rubrik instance to another. For example, a remote office/branch office (ROBO) may replicate workloads into the main data center using Rubrik, or a primary site may replicate to a DR site.

This approach allows you to eliminate configuring and managing this functionality at the storage layer. Apply policy-based management to workloads and stop babysitting data residing across multiple data centers.

Regardless of where the data is archived, Rubrik ensures instant accessibility of data with real-time predictive search. Metadata is included in the archive to ensure the most cost-efficient way to recover data by removing the need for recovering full backups from archive before restoring. This provides the ability to recover archived data at a snapshot or file-level selectively without having to download the entire workload to restore a single file, and reduces cloud provider egress bandwidth charges.

Rubrik is firmly rooted in the declarative approach; as an administrator, you simply define the desired end state (RPO, retention, replication, archival, etc.) and allow the intelligent software to make it reality. In essence, govern infrastructure and applications using declarative policy rather than imperative jobs.

ASSIGNING SLA DOMAINS

VMs inside the vCloud Director are managed as a part of vApp. vApps allow for multiple VMs to be grouped together and apply multiple VM policies on them. Once the policy in Rubrik d has been created, it can provide protection for a VM or vApp by assigning an SLA Domain to it. Examples of policies could be configurations, such as power-on sequencing and networking configurations. The SLA domain assignment of a vApp can be either directly specified or can be derived from a higher-level component. SLA domains can be applied anywhere in the vCloud Director hierarchy stack: the organization, the organization virtual data center, vApp, or VM levels.

Assigning an SLA domain at a higher level in the organizational hierarchy results in the policy being assigned to all child object vApps and, ultimately, VMs in the hierarchy. This derived SLA domain is set through automatic protection.

Automatic protection occurs in one of the following ways:

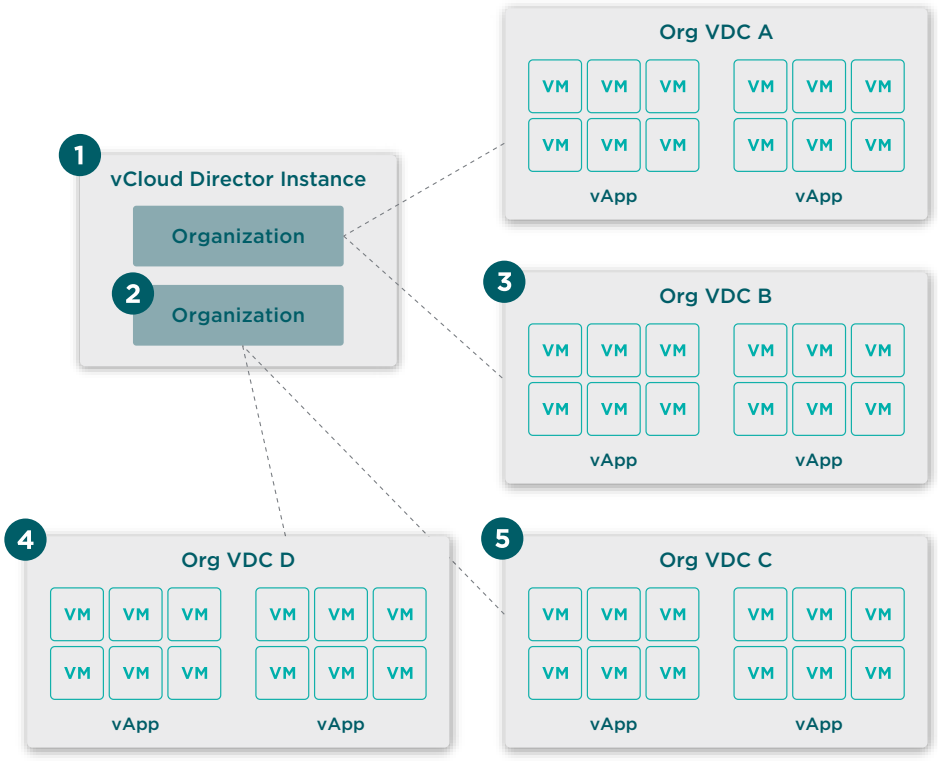
- An administrator assigns an SLA Domain to an object that contains the vApp or VM
- An administrator moves the vApp or VM into the hierarchy of an object that is assigned to an SLA Domain

This means that VMs will be protected through inheritance of the SLA Domain assigned to a parent object. If the Organization or oVDCs has an SLA assigned to it, the vApps and VMs underneath will automatically inherit the policy. The Rubrik data control plane detects the newly added VMs and automatically applies a protection policy, eliminating the need for any manual administrator interaction. This resolves the common issue of new workloads being brought online and going days or weeks without being protected.

SLA Domains may be assigned on any of the following object types:

1. vCD instance
2. Organization
3. oVDC
4. vApp
5. VM

The following image illustrates the protection hierarchy on which SLA Domains may be applied.



Assigning an SLA domain at a lower level in the hierarchy overrides an assignment made at a higher level. The following sections will provide more detailed information about inheritance at each hierarchical level.

PROTECTION AT THE VCLOUD DIRECTOR INSTANCE LEVEL

The Rubrik cluster applies the policies of the specified SLA Domain to all virtual machines within the constructs controlled by the vCloud Director instance. Any workload placed under this construct will automatically inherit the SLA Domain assigned.

PROTECTION AT THE ORGANIZATION LEVEL

The Rubrik cluster applies the policies of the specified SLA Domain to all virtual machines within the organization. Assigning an SLA Domain at this level overrides an SLA Domain assignment at the vCloud Director instance level.

PROTECTION AT THE ORGANIZATION VIRTUAL DATACENTER LEVEL

The Rubrik cluster applies the policies of the specified SLA Domain to all virtual machines within the organization virtual datacenter. Assigning an SLA Domain at this level overrides an SLA Domain assignment at the vCloud Director instance level and the organization level.

PROTECTION AT THE vAPP LEVEL

The Rubrik cluster applies the policies of the specified SLA Domain to all virtual machines within the vApp. Assigning an SLA Domain at this level overrides an SLA Domain assignment at the vCloud Director instance level, the organization level, and the organization virtual datacenter level.

PROTECTION AT THE VIRTUAL MACHINE LEVEL

The Rubrik cluster applies the policies of the derived or individually assigned SLA Domain assignment to the specified virtual machine. Essentially, the Rubrik cluster ignores that the virtual machine is part of a vApp. To do this, delete the vCloud Director instance from the Rubrik cluster.

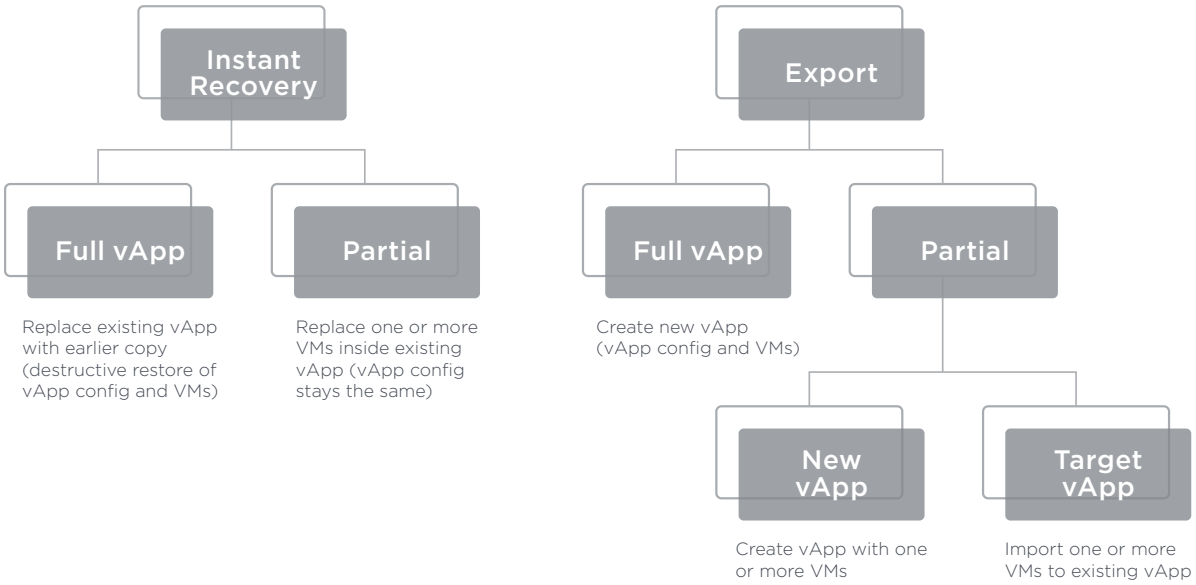
RECOVERY METHODS

An entire vApp, or one or more virtual machines in a vApp, can be replaced through recovery.

Recovery of a vApp can be either:

- Full – all of the vApp virtual machines and metadata are restored to replace the source vApp.
- Partial – one or more selected virtual machines and their metadata are restored to the source vApp.

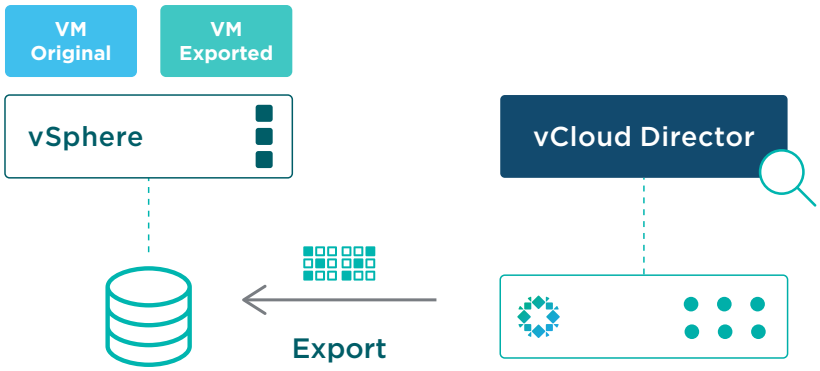
This integration also provides several recovery options at the vApp and VM level using Instant Recovery and Export. These are illustrated in the chart below.



Instant Recovery allows for restoring both the full vApp and partial recovery, enabling the replacement of one or more VMs inside an existing vApp. Similarly, the Export option allows for replacing the full vApp from a snapshot and a partial recovery. A new vApp may be created from one or more VMs, or VMs may be imported into an existing vApp.

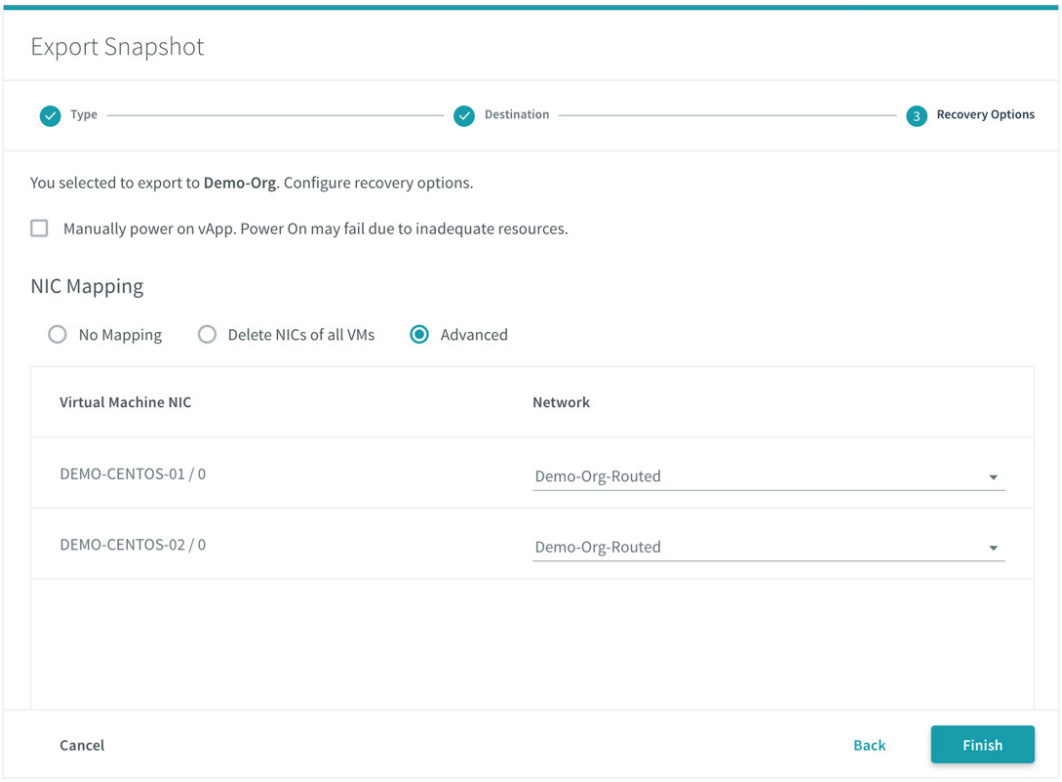
EXPORT

An Export creates a new vApp or VM from a point-in-time copy of the source. The chosen recovery organization allows the selection of applicable resources for the recovered vApp or VM.



vApp network settings may be restored during the recovery workflows. During an Export, Rubrik can:

- Recover
  - Isolated vApp networks
  - Direct vApp networks and NAT-Routed networks if the relevant Organization network still exists
- Connect VM NICs to the recovered networks



INSTANT RECOVERY

Rubrik's Instant Recovery can be used to recover vApps or VMs that are no longer functioning properly because of:

- Corruption or malware
- Accidental deletion
- Any other service disruption

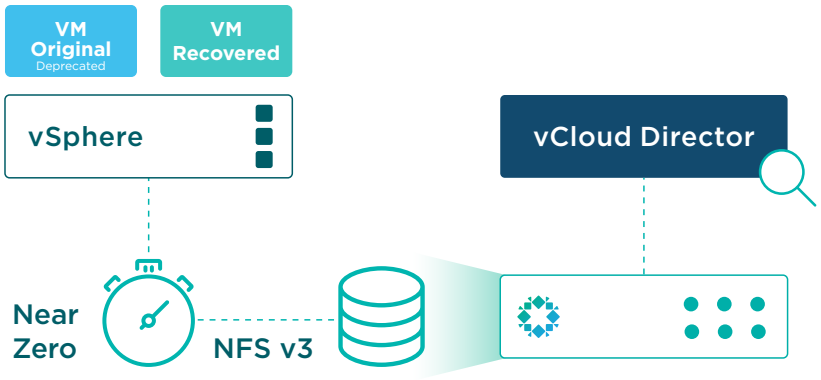
This functionality allows VMs needing to be restored to be mounted directly off the Rubrik system, thus reducing the recovery time.

WORKFLOW

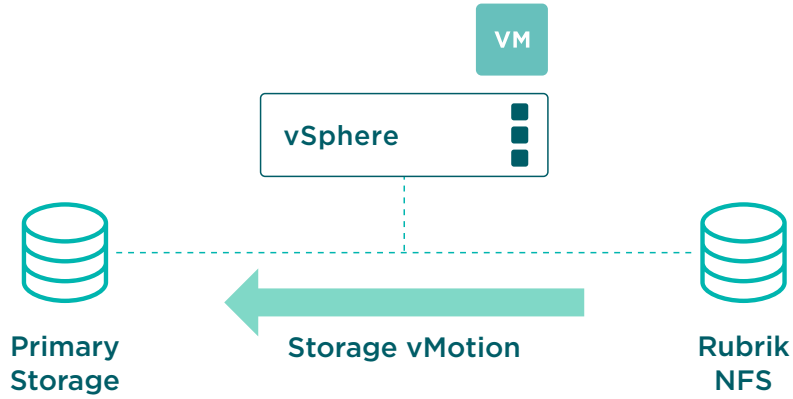
The process first begins by selecting the vApp or VM, snapshot date, and recovery host. You may choose to remove a virtual network device or select a different network if any networking changes or issues would prevent the VM from successfully powering on. This methodology also enables validation of certain services after recovery but before restoring the service.

At this point, the Rubrik system presents itself as an NFS v3 datastore to ESXi. The original VM is deprecated (renamed); however, keep in mind that the original VM may have been deleted, so this would not be necessary.

Rubrik coordinates the addition to the VM inventory in vCenter Server. A new copy of the VM running on Rubrik is presented and powered on and services resume.



Post-recovery, users can Storage vMotion to the primary storage array.

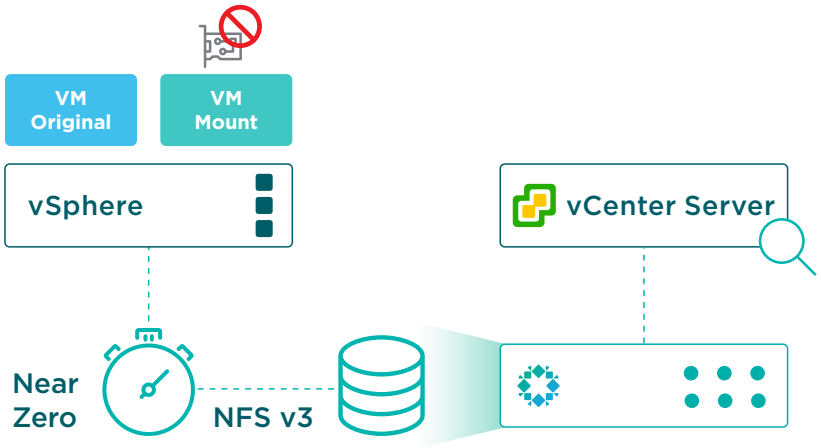


Ultimately, Rubrik serves as a storage endpoint to recover as many vCD vApps or VMs as needed, thus eliminating the complexity and time wasted in transferring data back into the production system. This functionality provides a near-zero recovery time and restores user access near instantly.

The instantly recovered VM derives protection from parent objects. When the recovered VM does not derive protection from any parent objects, add it to an SLA Domain. To protect it using the same SLA rules and policies as the source VM, add the recovered VM to the original SLA Domain or to another SLA Domain.

LIVE MOUNT

Like Instant Recovery, Rubrik becomes an NFS v3 datastore from vSphere ESXi hypervisor perspective. Instead of deprecating the original VM, a VM similar to the original is created but with a trailing date timestamp appending the VM name. The original VM is not altered. Additionally, in order to avoid IP or MAC address conflicts, the Live Mount VM has its NIC disabled by default.



This functionality appeals to application owners and operations teams in order to conduct:

- Functional or regression testing
- Application development
- Software release testing (upgrade the actual applications)

Build isolated environments and leverage the Live Mount feature to instantiate an identical environment in moments. Test VMware Tools or hardware version upgrade, failure scenario, or other use cases using your backup storage. When done, simply throw it away.

No additional configurations are needed on the hypervisor side for Live Mount functionality to work. Rubrik automates the entire process. VMs of any size can be recovered in the amount of time it takes for the OS to boot. Imagine having the ability to spin up an 8 TB VM in under 2 minutes so that a recovery point can be validated by an administrator or application owner.

Please note that Live Mount is currently only supported at the VM level.

FILE-LEVEL RECOVERY

The Rubrik cluster provides file-level restore (FLR) of files and folders from any local snapshot, replica, or archival snapshot that was successfully indexed.

To restore a file or folder, search for the file or folder by name across all local snapshots. You can also browse for the file or folder on a selected snapshot.

Note: The Rubrik cluster must download an archival snapshot before it can be browsed. Searching by name for a file or folder on an archival snapshot does not require that the archival snapshot be downloaded first.

Files and folders may be restored directly to the source system or by download.

DIRECT RESTORE

For supported Windows and Linux guest operating systems, the Rubrik cluster can restore files and folders directly to the source file system.

When restoring from a snapshot of a supported guest operating system, the web UI provides the option to restore a file or folder directly to the source file system. When this option is selected, the web UI provides a choice to overwrite the source file or folder, or to restore the file or folder to another location.

A restored file or folder inherits the access control of the parent folder and the same owner as the parent folder. The restored file or folder retains the modification time of the source file or folder at the time of the snapshot.

To successfully restore directly to the source file system, the Rubrik cluster must be provided the following information:

- Resolvable hostname or IP address of the authentication server
- Username of an account with Administrator privileges for the target
- Password for the account

When the Rubrik cluster has previously accepted the service credentials of a guest operating system, the restore job does not require additional credential information. This feature requires that the Rubrik cluster has successfully used the service credentials for at least one backup prior to the restore task. Otherwise, the credentials can be provided through the Restore File dialog during the restore task.

RESTORE BY DOWNLOAD

The Rubrik cluster generates download links to use for file-level restore (FLR) of files and folders from any local snapshot, replica, or archival snapshot that was successfully indexed. The guest OS of the source virtual machine must have a current version of VMware Tools running to enable successful indexing.

Restore a file from a data protection object through the Rubrik cluster web UI. Once the file is selected, the Rubrik cluster processes the request and provides a link for download of the file.

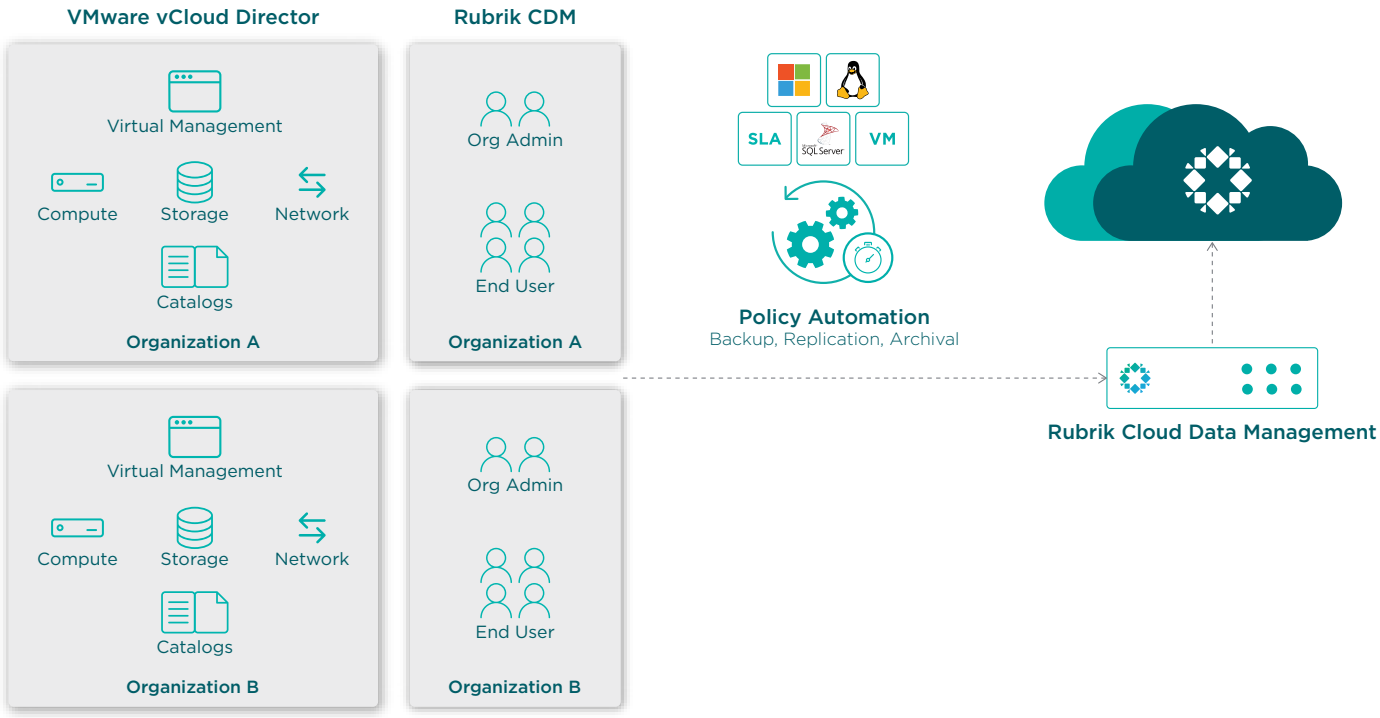
When restoring a folder, the Rubrik cluster generates a `.ZIP` file containing the folder and all its contents. The `.ZIP` file retains the hierarchy of the selected folder. The Rubrik cluster provides a link for downloading the `.ZIP` file.

ARCHITECTURE OVERVIEW

vCloud Director makes it easy for cloud service providers or managed service providers (MSPs) to manage and operate VDCs for multiple organizations, or tenants. The solution can automate the creation of VDCs based on consumer resource needs and assign the appropriate policies necessary to maintain a proper allocation and priority of resources. vCloud Director also provides a unique portal for tenants to manage various cloud services and workloads on their own.

Rubrik's integration with vCloud Director simplifies protection of VMs by recognizing vCD constructs, and provides granular recovery at the file-level so that users can choose whether to recover an entire vApp or a subset of VMs. Rubrik's integration with vCloud Director includes the following:

- Autodiscovery of vCD hierarchy
- SLA-based autoprotect at different levels of vCD hierarchyvCD instance
  - vCD organizations
  - Org VDC
  - vApp
- Recovery flows
  - Export and instant recovery
  - File restore
  - Network settings
- Tenant facing self-service management of backups enabling Backup-as-a-Service (BaaS) with Rubrik Envoy and/or Rubrik Extension for vCloud Director
- Reporting per vCD organization



The following provides a few requirements for this integration detailed in the reference architecture:

- VMware Software Solutions
  - VMware vCloud Director 9.1 or 9.5
    - » VMware vCloud Director 8.10 or later is supported, however, the ability to use a third-party extension is unavailable
    - » Rubrik Extension for vCloud Director
    - » See Compatibility Matrix for most up to date information
  - VMware vSphere 6.5 or later
    - » VMware vCenter 6.5 or later
    - » VMware ESXi 6.5 or later
  - VMware Tools
    - » The Rubrik cluster requires the current version of VMware Tools to perform administrative operations and enable application-consistent snapshots.
    - » If VMware Tools is out of date, the backup will proceed but may not be application consistent.
- Ethernet (IP) Network
  - A VMkernel port is required for NFS if using Live Mount or Instant Recovery functionality.
  - Additionally, a separate VMkernel network may be configured for Rubrik data traffic.
- Rubrik Cloud Data Management (CDM) 4.2 or later

Additionally, the following assumptions have been made in the writing of this document:

- Workloads are supported by VMware vCloud Director.
- Workloads are using supported versions of their operating system and application release(s).
- 10 GbE network connectivity exists between the ESXi Host(s) and Rubrik cluster.
- 4-node Rubrik cluster.

Lastly, a few constraints since Rubrik cannot protect data that exists on any of the following using native vSphere integration through APIs:

- VMDKs that are set to Independent-Persistent mode or to Independent-Nonpersistent mode.
- Network drives that are mounted on the file system of a protected virtual machine.
- Any VM for which the Rubrik cluster does not have snapshot creation permission because of settings on the VM or on a vSphere folder that contains the VM.
- Any VM data that resides on raw disk mappings (RDMs), where the RDM compatibility mode is set to Physical.

That being said, these constraints apply to protection using native vSphere APIs but can be backed up using an agent-based approach with Rubrik Backup Service (RBS).

These requirements and assumptions should be taken into account for the remainder of the document.

MULTI-TENANCY

Multi-tenancy enables the support of multiple customers on a single platform. This empowers lines of business to manage policies of their data while retaining control and compliance.

Rubrik's multi-tenancy approach employs Logical Data Isolation, shared resources with secure Roles-Based Access Control (RBAC), and simple scalability. Rubrik brings an innovative framework for secure data and metadata isolation to avoid data commingle. Rubrik is designed to give the best of both worlds; security benefits of physical boundaries and economic advantages of a real cloud computing model. It is made possible by virtualizing all resources so that tenants can share allocated resources in a secure, isolated fashion.

Each tenant or user can only see and manage objects that they are assigned. Rubrik ensures secure access control at the object and tenant level. The flexibility of the underlying architecture makes it very easy to scale and grow as you go. In addition, Rubrik eliminates complexity with an extremely easy-to-use software.

This flexible approach allows the service provider to determine whether resources are shared across tenants. Operate in a true cloud computing model, with shared resources virtualized to different tenants in secure, isolated fashion.

AUTHENTICATION

Rubrik and vCD both support local user databases or LDAP as an external user directory. Using the same external LDAP directory for both vCD and Rubrik is recommended to ease administrative overhead. If local user databases are used with a high number of users, consider automating user creation via REST API. Users will need to remember to change their password in both vCD and Rubrik if local databases are used.

MAPPING RESOURCES

Multi-tenancy on Rubrik is achieved by creating organizations, and assigning users and resources to the organization. An organization is made up of the following objects:

- Protected objects (i.e. a vCD vApp, Org, or VDC)
- Replication and archival targets
- SLA Domains
- Users (local or LDAP)
- Service credentials
- Reports

It is up to each administrator to determine the best operational model to deliver multi-tenancy. The simplest approach is a one-to-one mapping of vCD organizations to organizations on Rubrik, but more complicated scenarios are possible.

OPERATIONAL OVERVIEW

Rubrik and VMware vCloud Director product lines leverage a complementary progressive hybrid cloud enterprise architecture, with the goal of accelerating applications and business requirements. This section aims to highlight how lightweight the Rubrik and VMware vCloud Director joint solution is.

USE CASES

This section is intended to provide a few examples of how Rubrik and VMware vCloud Director may be used together. It is not intended to be an exhaustive list but merely a set of sample use cases.

TENANT SELF-SERVICE

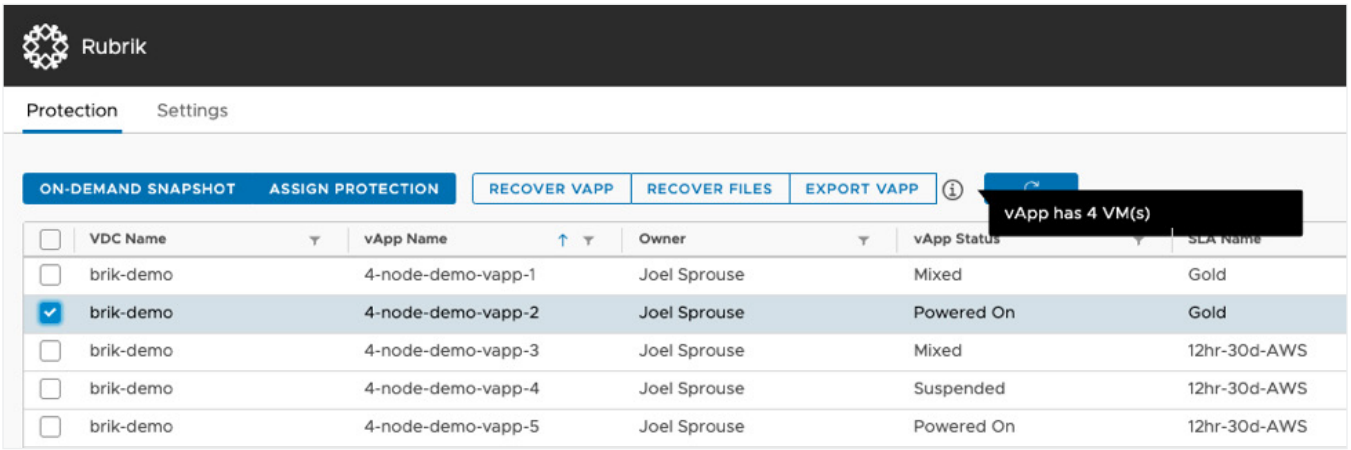
The Rubrik Extension for vCloud Director empowers the tenant to manage their own data protection and recovery. This plugin gives tenants the same simple and flexible multi-tenant self-service functionality that providers already enjoy from the vCloud Director UI without having to use the Rubrik UI.

As of 9.1, the vCloud Director user interface (UI) plugin management allows for integration of custom, third-party modules directly into the context of the vCloud Director interface. This has allowed Rubrik the ability to extend our functionality into vCloud Director by customizing the UI based upon HTML5 standards using Angular and Clarity.

Once the Rubrik Extension for vCloud Director is installed, the following actions can be made available to allow for tenant self-service:

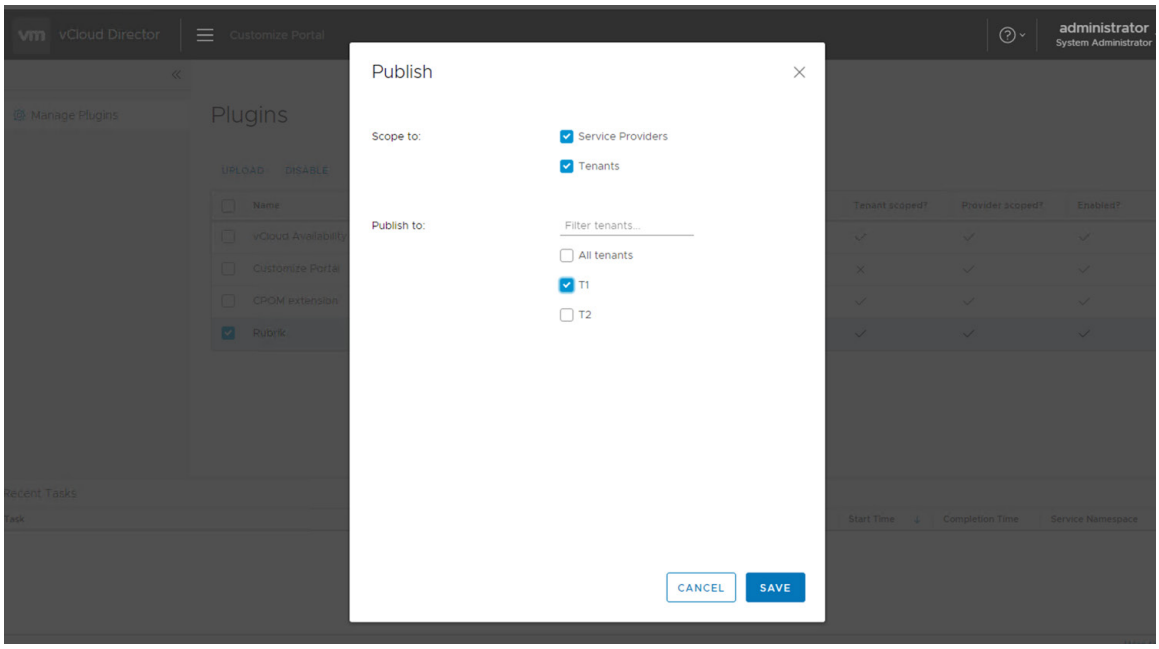
- On-demand Snapshots
- Assign SLA Protection
- Recover vApp
- File Recovery
- Export vApp
- Credential Management

The following image demonstrates some of the Rubrik functionality available from the tenant:

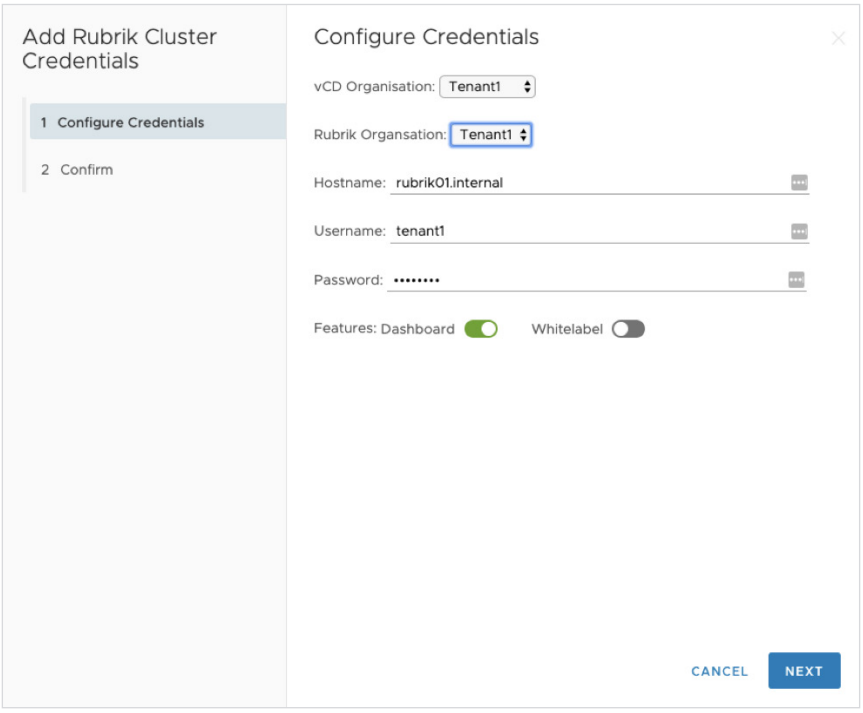


By leveraging the plugin registration process that is built into vCloud Director, service providers can dictate whether the plugins should be available to the provider portal or to the tenant portal. Additionally, the service provider can provide granular control of tenant accessibility. This allows for a wide range of extensibility and integration to be made available to the tenant.

Once the plugin has been uploaded, you can quickly and clearly specify to which tenants the plugin should be published.

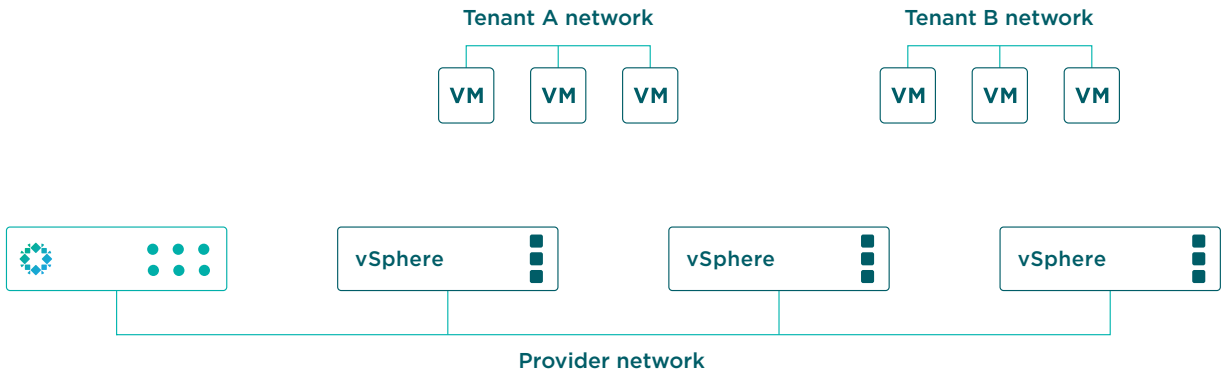


Once the plugin is installed and initial configuration is completed by the vCD administrator, each vCD Organization can be associated with its corresponding Rubrik Organization on the Settings page. When configuring credentials, choose corresponding Organizations in vCD and Rubrik and supply the credentials for that Organization on Rubrik. Note that associating a vCD Organization with the Global Organization on Rubrik will allow access to report data from all organizations, which could pose a security risk.



PROTECTING ISOLATED WORKLOADS

In many infrastructures, provider and tenant networks are isolated from each other. This lack of connectivity prevents tenants from managing various critical items (SLA domains, self-service recovery, etc.) on their own. This is illustrated in the following image:

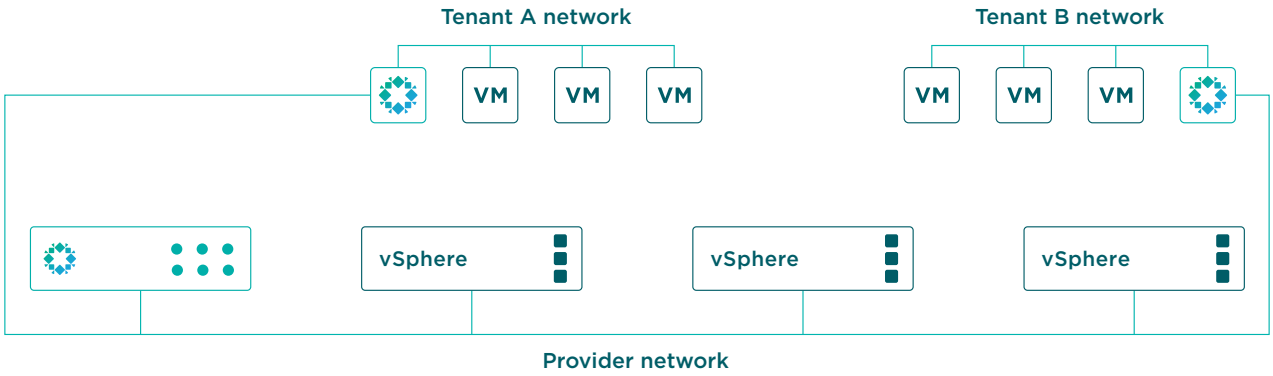


RUBRIK ENVOY

Rubrik Envoy addresses this architectural challenge. Rubrik Envoy is a trusted ambassador (its certificate is issued by the Rubrik cluster) that represents the service provider's Rubrik cluster in an isolated tenant network. Rubrik Envoy is deployed as a virtual appliance in a tenant network and acts as a proxy between the tenant network and the service provider network. After deployment, Rubrik Envoy provides secure managed access between the tenant network and the network used by the Rubrik cluster. Service Providers are able to offer backup-as-a-service (BaaS) to co-hosted tenants, enabling self-service SLA management with on-demand backup and recovery.

Once a tenant subscribes to BaaS from the service provider, an Envoy virtual appliance is deployed on the tenant's network. The tenant may log into Envoy, which will route the Rubrik UI to the service provider's Rubrik cluster. Envoy will only allow access to objects that belong to the tenant. The Rubrik cluster works with the tenant VMs, via Envoy, for tasks such as application quiescence, file restore, and point-in-time recovery.

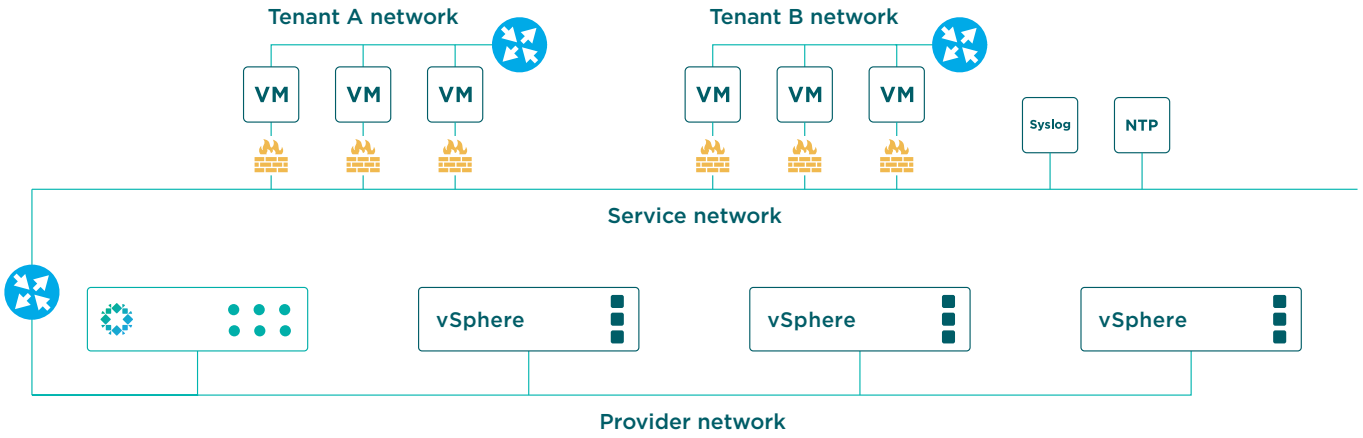
The following diagram illustrates this architecture:



Rubrik Backup Service (RBS) is deployed in tenant VMs from Envoy, thereby ensuring that RBS accepts connections only from Envoy. The actual ingestion uses Network Block Device (NBD) transport mode, making the solution agentless. Further details on deploying and configuring Rubrik Envoy are available in the Rubrik User Guide.

SERVICE NETWORK

Another approach to providing services to multiple tenants is by using a service network, similar to the approach outlined in Architecting a VMware vCloud Director Solution for VMware Cloud Providers. The diagram below illustrates VMs with secondary NICs connected to a service network, utilizing to NSX Distributed Firewall to maintain segmentation between tenants. The service network runs on a unique IP range so it does not interfere with tenant networks. Firewall rules are configured to allow communication between VMs and provider services. Some services, like syslog or NTP only need outbound (i.e. VM initiated) traffic allowed. When using RBS, Rubrik requires inbound traffic to be allowed as well, so firewall rules will need to configured to accommodate this.



CLOUDOUT (ARCHIVAL)

CloudOut is a capability within Rubrik CDM used to archive data to the cloud for short and long-term retention. Users may leverage Rubrik to intelligently and cost-effectively store backup data in Amazon S3, Microsoft Azure Blob storage, or Google Cloud Storage. More importantly, Rubrik is optimized to provide rapid and efficient data restores both on-premises and in the public cloud. Data is indexed by Rubrik CDM before it is stored in the cloud archive, enabling customers to quickly browse, search, and restore any file. During restores, Rubrik only retrieves the specific files that need to be recovered to minimize bandwidth and egress costs.

Rubrik customers typically leverage CloudOut as a solution to replace their tape storage infrastructure, eliminating the need to copy backup data to tapes which would then need to be manually stored offsite. CloudOut provides a tape-replacement solution that is more durable, available, cost-effective, and agile.

If on-premises archive solutions are preferred, Rubrik also supports NFS, tape, and object storage.

CLOUDON (INSTANTIATION)

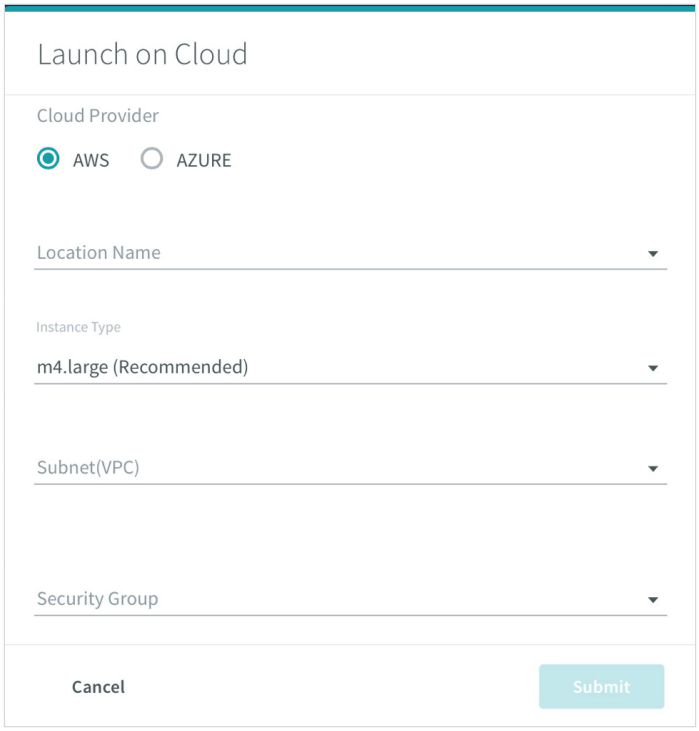
CloudOn, or instantiation, allows users to migrate existing on-premises workloads to the cloud for test/development or even disaster recovery purposes. Rubrik's CloudOn feature converts VM backups archived to the cloud into a provider-native compute instance format. There is no need to run Rubrik in the cloud to migrate workloads to the cloud for test/dev, increasing overall cloud savings.

Better yet, imagine not needing a separate cluster for test/development workloads or an identical physical infrastructure for disaster recovery. Using Rubrik CloudOn, workloads can be migrated at a VM level from on-premises to AWS or Azure.

Rubrik offers three options that can be applied to on-premises workloads that customers choose to instantiate in AWS or Azure:

- **On-Demand** - The default configuration in which Amazon Machine Images (AMIs) or Azure Virtual Hard Drives (VHDs) are created only at the time of a "power on in the cloud" request.
- **Auto Convert Latest Snapshot** - Keep One - Rubrik will automatically construct an AMI or VHD reflecting the latest snapshot to be archived into S3 or Azure. When a new snapshot is sent to the archive, a new AMI or VHD is constructed with the new archive data. Once completed, the older AMI or VHD is removed.
- **Auto Convert Latest Snapshot - Keep All** - Rubrik will automatically construct an AMI or VHD reflecting the latest snapshot to be archived into S3 or Azure. When a new snapshot is sent to the archive, a new AMI or VHD is constructed with the new archive data. The older AMI or VHD is retained if desired (configurable via policy), creating a series of AMIs or VHDs representing each snapshot.

The following screenshot demonstrates the required information to instantiate a workload in AWS:



Whether instantiating workloads on-demand or automatically with the latest snapshot, spinning up copies of workloads in the cloud results in faster development cycles as developers are unblocked from the constraints of physical infrastructure. Picture the cost savings garnered when avoiding a dedicated on-premises infrastructure for test/development. Developers can spin up instances when required and shut down when not in use.

CONCLUSION

Rubrik's support for VMware vCloud Director protection is robust and full-featured while extending Rubrik's market leading focus on simplicity. Using Rubrik and VMware vCloud Director together helps accelerate cloud service providers on their journey to meet business requirements by protecting workloads, providing archival and replication to public cloud, and to enable tenant self-service.

ABOUT THE AUTHORS

Matt Elliott is a Technical Marketing Engineer at Rubrik, with IT experience in several sectors including Healthcare, Manufacturing, Big Law and VAR/MSP. Matt is a vExpert, GCP Associate Cloud Engineer, and CCIE #56011. You can reach him on Twitter @NetworkBrouhaha.

Daniel Paluszek is a Staff Solutions Engineer at VMware in the Cloud Provider Program collaborating with strategic cloud service providers. With over 15 years in the IT industry, Daniel is part of the VMware Office of the CTO Ambassador program and holds VCIXs in DCV and NV. He frequently publishes at https://www.paluszek.com and can be found on Twitter @dpaluszek.

Rebecca Fitzhugh is the Principal Technologist at Rubrik. She is VCDX #243, a published author, and blogger. You can find her on Twitter @RebeccaFitzhugh.

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

20190822_v1