TECHNICAL WHITE PAPER

How It Works: Rubrik vCloud Director Extension

Andrew Draper
August 2020
RWP-0562

TABLE OF CONTENTS

3 INTRODUCTION

3 AUDIENCE

3 OBJECTIVE

3 BACKUP AND RECOVERY FOR VCLOUD DIRECTOR

- 3 Out of the Box
- 4 Service Provider Solutions
- 4 Advantages of Self-Service
  - 4 Help Desk Tickets
  - 4 Tenant Insight
  - 4 User Empowerment

4 ARCHITECTURE & COMPONENTS

- 4 High Level Architecture
  - 5 Network Considerations for Extension
- 5 Components
  - 5 Rubrik vCloud Director Extension
  - 6 Metadata Storage
  - 7 VMware VCD Ext SDK
  - 7 Rubrik Organizations
  - 7 CORS and Proxy
  - 8 Certificates

9 HOW IT WORKS

- 9 Service Provider Workflows
  - 9 Extension Installation
  - 9 Configuring Tenants
  - 9 Base Configuration
  - 11 Provider Actions
- 12 Tenant Workflows
  - 12 SLA Management & On-Demand Snapshots
  - 13 Instant Recovery & Export
  - 16 File Recovery
  - 18 Reporting & Events

20 CONCLUSION

21 GLOSSARY

21 SOURCES AND NOTES

22 VERSION HISTORY

INTRODUCTION

The Rubrik CDM platform is built on top of a rich suite of RESTful APIs, allowing easy integration with third-party services. VMware vCloud Director (vCD) is deployment, automation and management software for virtual infrastructure resources in multi-tenant cloud environments. Many customers today are already protecting VMware vCloud Director (vCD) environments with Rubrik, so providing additional self-service capabilities is a natural next step.

Allowing end users to access and manage their own backups without relying on support or service desks, provides a significant increase in productivity and visibility into their environments.

AUDIENCE

The intended audience for this document includes sales engineers, field consultants, professional services, partner engineering, customer architects, and engineers who wish to learn more about Rubrik's integration with vCloud Director through the Rubrik vCloud Director Extension, and the benefits it can provide.

OBJECTIVE

This whitepaper describes the Rubrik vCloud Director Extension and how they can provide self-service capabilities to their customers to be able to manage and interact with their own infrastructure within vCloud Director. This will also provide a deeper understanding into how the vCloud Director extension works under the covers, how it interacts with Rubrik and vCloud Director, and how to implement it providing a better understanding of how

BACKUP AND RECOVERY FOR VCLOUD DIRECTOR

OUT OF THE BOX

VMware provides a few solutions in order to be able to perform backup and recovery of vApps and VMs within vCloud Director. Within a typical environment, vCloud Director will use one or more vCenter server(s) to manage the virtualized resources in the environment, as well as providing its own service for the multi-tenancy aspects such as the virtual data centres, networks, storage, etc... through its internal metadata platform.

In order to perform backup and recovery, there are various elements that require protection; these include the data that belongs to the virtual machines residing within vSphere, and the virtual machine information, and then protection of the metadata which is maintained by the vCloud Director appliance.

Using VMware vStorage APIs for Data Protection, the virtual machines are able to be protected at the vSphere layer, however, there is also a requirement to protect the associated metadata that those virtual machines belong to within vCloud Director.

The vCloud Director backed database (this may reside on PostgreSQL or Microsoft SQL Server) can then be protected, followed by the vCloud Director appliances, however, this only provides a bare minimum protection. For specific protection of vApps, it requires reaching into the VMware API's at both vSphere and vCloud Director and protecting both machines and metadata.

SERVICE PROVIDER SOLUTIONS

Since vCloud Director is aimed at Service Providers, there will be a requirement to provide some level of support and maintenance for the environments to ensure that it is protected, and available for the tenant at all times. Data protection is typically required and usually falls on to the service provider to protect the data and ensure there are always backups available for restore under agreed SLAs. Since the provider will be responsible for these services, it is in the providers interest to provide some self-service capabilities providing tenants with insight into their own environments, with backups being a core element of said insights.

ADVANTAGES OF SELF-SERVICE

Self-Service brings a wealth of benefits to both providers and tenants, providing a positive experience and removing some of the typical legacy issues around lack of control in an 'as-a-service' platform.

HELP DESK TICKETS

Reducing reliance on a help desk allows for tenants to carry out actions that would normally be a help desk ticket, this could be something such as ensuring a backup has been taken before major upgrades take place, recovering a bad VM, or restoring a file that was deleted by mistake. This also allows the provider to focus on more important issues, such as managing and enhancing the service, benefitting both provider and tenant for better overall service.

TENANT INSIGHT

Having access to events, notifications and reporting provides tenants with greater insight as to how their environment is both being protected and consumed. Reporting metrics such as capacity growth shows a tenant how the cost of their service is growing through the consumption of the backups. They are also able to react to notifications such as failed backups, allowing the tenant to first investigate a potential issue before needing to reach out to the provider.

USER EMPOWERMENT

Allowing the end user to have some control over their own environment provides levels of user empowerment which typically would only be available if the tenant was running their own environment. This provides great benefit to the tenant since they can have some say and control over their own data and platform, allowing them to change and control backup policies and control restores without needing to rely on the provider.

ARCHITECTURE & COMPONENTS

HIGH LEVEL ARCHITECTURE

There are various architectural designs that work for customers, with some environments consisting of multiple architectures. Rubrik works with the majority of these architectures and further details can be referenced from the already published Reference Architecture paper available here.

Once Rubrik is configured and protection of the environment is working, the Rubrik vCloud Director Extension can be installed into the vCloud Director Cell via the Customize Portal extension provided by VMware. Once installed, the extension is capable of reaching both vCloud Director APIs and Rubrik APIs over HTTPS (443).

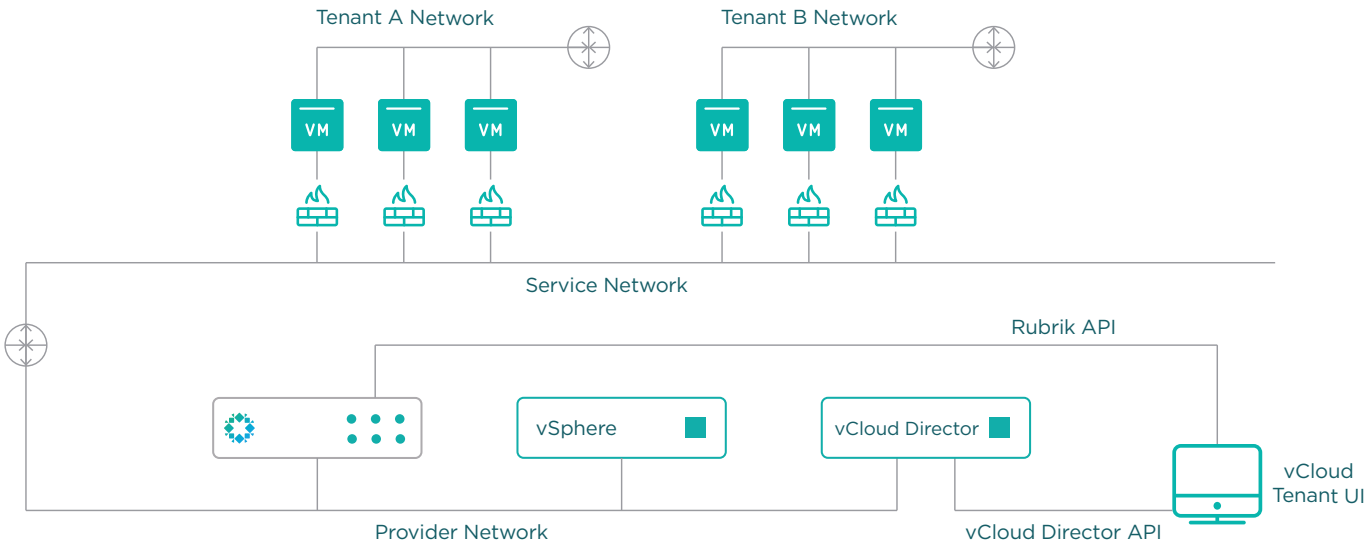
vCloud Director's UI Element is an AngularJS application that runs within the client browser, and as a result all API calls made to both vCloud Director and Rubrik are executed from the client's browser. This introduces some challenges since the client may not always be situated on the local network.

NETWORK CONSIDERATIONS FOR EXTENSION

The most common network environments that will be provisioned within vCloud Director are:

- Completely Isolated Networks - no access to the provider network
- Provider Backed Tenant Networks - firewall rules allowing very restricted access to provider networks

In both cases, with the extension, wherever the extension is being accessed from, the extension will need to be able to reach both vCloud Director APIs and Rubrik APIs in order to work. This may require the use of a proxy or firewall rule to allow traffic to flow from the client to the Rubrik cluster, for example:



COMPONENTS

There are various components that are leveraged and used with the extension, these are outlined in sections below to understand how the end-to-end functionality fits together.

RUBRIK VCLOUD DIRECTOR EXTENSION

The HTML5 portal of vCloud Director uses the Angular Javascript (AngularJS) framework, meaning all extensions also need to be developed as AngularJS applications.

VMware also develops a design system that outlines design principles and guidelines for User Experience (UX) and User Interface (UI) design; named Clarity, and is used throughout all HTML5 products in the VMware suite such as vSphere, vRealize Automation, vRealize Log Insight, etc... The ensures that user interface and experience maintain the VMware feel, ensuring that the extension fits into the existing framework for vCloud Director.

The extension framework allows for a front-end application to run inside of a container set by vCloud Director. However, there is no access to make the extension to make requests on the back-end of vCloud Director. This introduces a set of challenges around persistent storage, and connectivity.

METADATA STORAGE

Since there is no persistent storage that can be accessed such as a database, the Rubrik vCloud Director Extension requires a set of values to provide self-service capability.

These include:

- Rubrik IP/DNS Address - this is where the all API requests will be sent for the specific tenant
- Username, Password or API Key - Authentication is required in all cases when using the Rubrik API. Either Username and Password or API Key will be set in the **Authorization** header with each API call made to Rubrik
- Organization - This is the identifier for the Rubrik Organization that is configured for the specific tenant
- Features - To allow providers to enable and disable features on their tenants, we also need to store an additional JSON string that will automatically enable and disable features within the extension

In order to store the above values, vCloud Director's built-in metadata system is used, which allows extensions to store data types such as strings, integers, date/time, etc and can then be read using the API.

Using the metadata concept within vCloud Director allows the extension to continue to follow the RBAC model outlined by the provider since, in almost all cases, the end user will have access to read the metadata set within a virtual data center (VDC) in vCloud Director.

The Rubrik extension will add an additional 2 read-only string fields to the VDC metadata:

- *rbk-feature* - this is the string that maintains features as they are enabled or disabled (Encrypted)
- *rbk-connection* - this is the connection string which contains all rubrik connection details required to make the required API calls:
    - Username (Encrypted)
    - Password (Encrypted)
    - API Key (Encrypted)
    - Rubrik DNS/IP Address
    - Rubrik Organization ID

Metadata

Name	Value	Type	User Access
rbk-feature	U2FsdGVkX1/l0T6My1+DTVifTxmw0e0fcbWg9BsT4RiOyU...	Text	Read only
rbk-connection	{"dns":"172.21.8.59","username":"U2FsdGVkX19mkQXGuZm...	Text	Read only

Making use of this feature allows for the above values to be written on a VDC by VDC use case, since not all users will be able to access all VDCs inside a tenant. However, due to the sensitive nature of the values, it's important to ensure these are encrypted; therefore using specific identifiers, all sensitive strings are salted, hashed and stored in an encrypted format using AES256 encryption standards. This applies to Username, Password, API Keys and Features.

VMWARE VCD EXT SDK

The Rubrik vCloud Director extension is based on the VMware SDK for building vCloud Director Extensions. This is maintained by VMware and ensures that requests made within the tool to vCloud Director are done in a supported method provided by VMware. This is also a requirement for the extension to be certified by VMware. This SDK is maintained in a public repository and can be found here.

RUBRIK ORGANIZATIONS

Organizations within Rubrik act similarly to tenants within vCloud Director. This will allow for the configuration of role based access control to resources that align with the specific tenant. This can include resources outside of vCloud Director such as Application Consistent products such as Oracle, Microsoft SQL Server, etc...

A typical organizational structure will provide control over the following:

- vSphere Virtual Machines
- vCD vApps
- Support Applications
- Physical Hosts
- NAS Shares
- Managed Volumes
- Cloud Instances
- Restore Targets
- SLA Objects
- Archive and Replication Sources and Targets
- Users and Domains
- Envoy Configurations

All of the above constructs can be assigned to an individual organization and access can be granted using either local accounts or by connecting any LDAP domain to Rubrik.

The vCloud Director Extension will make use of Organizations within Rubrik to ensure visibility of objects is limited to the vCloud Director Organization as well as required SLA domains, replication targets and domains.

CORS AND PROXY

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served. This applies to extensions installed to vCloud Director that are making requests outside of the vCloud Director appliance. In order to support this, the responding web server must be configured to accept CORS requests with verified values such as:

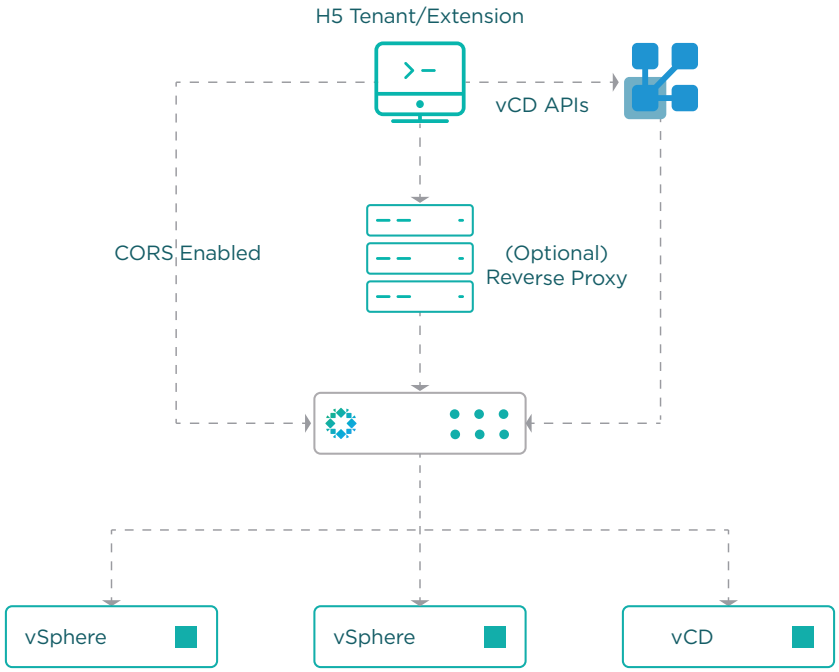
- Permitted Domain Names e.g. vcd-appliance.com is permitted to access rubrik-cluster.com
- Permitted Headers e.g. Authorization and x-vcloud-authorization are allowed to be added to the headers for CORS requests.

There are some exceptions to CORS whereby simple requests can still be permitted without the need to configure anything, more details of this can be found in the mozilla HTTP documentation here.

With Rubrik, CORS was added in 5.2 and prior to the 5.2 release, there was an enforcement to use a proxy that responded to the CORS requests and then forwarded the original API requests to the Rubrik cluster. This allows for CORS to be supported by off-loading the CORS portion of the request to the proxy server, accepting the request which uses the HTTP Request Type **OPTIONS** to validate the request before sending the actual HTTP request e.g. **GET**, **POST**, **PATCH** or **DELETE**.

Initially, the proxy server was a requirement for CORS, however, it also serves an additional purpose when dealing with complex networking situations, as the server is able to middleware requests from one place to another. Therefore, with CORS enabled, there still may be benefits to using a proxy server.

Lastly, there are no restrictions to the proxy server type, it is possible to use any hardware device such as a load balancer, or software as long as either support proxying of HTTPS requests. For example, a physical firewall or load balancer could route requests whilst also applying more advanced networking concepts such as Access Control Lists or Network Address Translation.

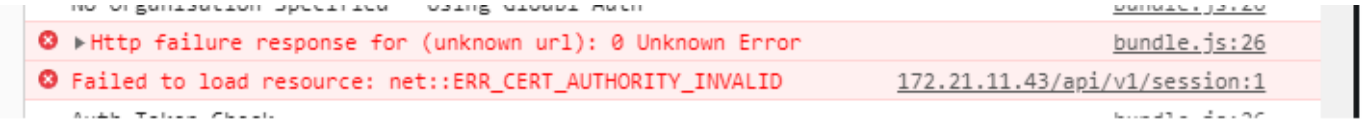


CERTIFICATES

Certificates are a key element when working with any type of HTTP request whether it's displaying a webpage or making an API request. Browsers will always protect when certificates are not valid, whatever the reason may be. Certificates are typically recommended when dealing with any type of web request to protect the requests from attacks such as man-in-the-middle (MITM) where attackers are able to intercept the requests and gather information. With certificates, the request is encrypted ensuring that the information being sent in the HTTP request is protected from anybody attempting to listen in.

With the Rubrik extension, API calls made from the browser to rubrik will need to complete certificate validation or the request may be blocked by the browser with no feedback to the user and is therefore important to ensure valid certificates are used with Rubrik prior to configuring the Rubrik vCloud Director Extension.

Without valid certificates, the result of any request will throw errors in the browser console log if the certificate has not already been accepted by the client or browser:



This can lead to error messages appearing within the extension until the end user has accepted that the certificate is trusted either by visiting the page directly and accepting the browsers security warning, or install the certificates into their local trusted store on the machine they are operating.

HOW IT WORKS

SERVICE PROVIDER WORKFLOWS

EXTENSION INSTALLATION

As of vCloud Director 9.0, the HTML5 extensibility platform was introduced, however, extension installation was only available through VMware's APIs. In order to assist with this, VMware created an extension that could be installed via these APIs providing management of all extensions without needing to use the APIs any further.

Previously known as **Plugin lifecycle Management**, This was later revised and integrated into the base vCloud Director product as of 9.7; titled **Customize Portal**. The customize portal is still required in versions of vCloud Director earlier than 9.7 which can be installed with instructions from VMware; these instructions can be found here.

CONFIGURING TENANTS

Configuration of tenants within the extension requires various tasks to be completed before the extension is ready for use:

- Creation of Rubrik Credentials
- Creation of Rubrik Organization
- Rubrik Organization RBAC permissions
- Tenant Configuration from within the Rubrik vCloud Director Extension

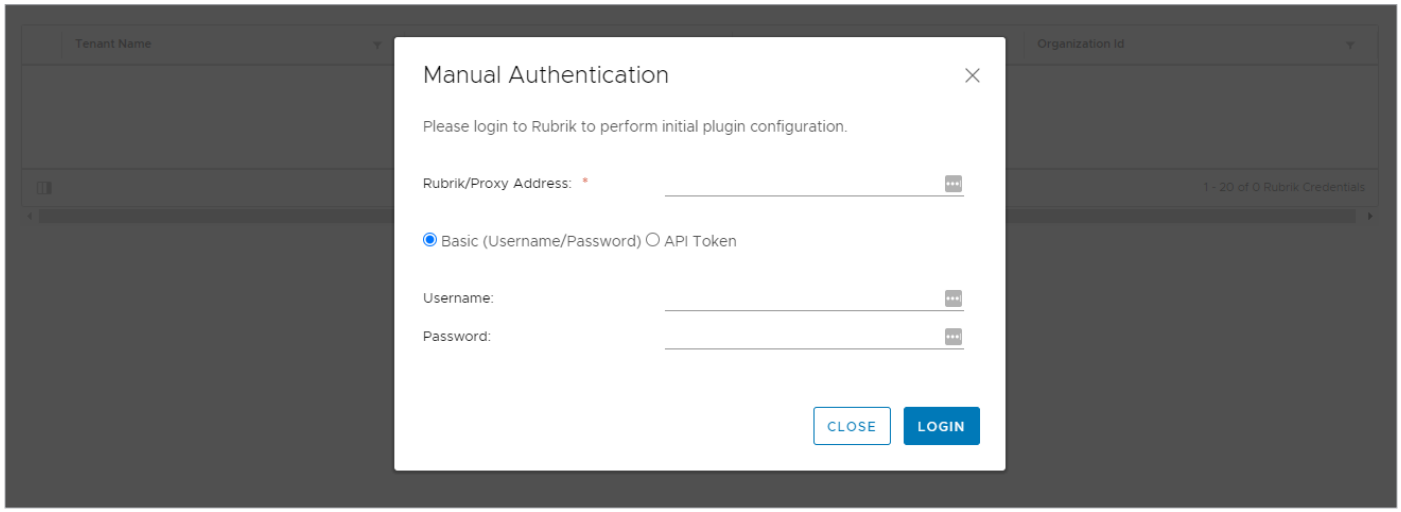
Rubrik's multi-tenant organizations allow for an extremely similar approach to vCloud Director tenants, whereby specific objects can be granted to an organization, and access is entirely segregated from other tenants on the same platform.

It is important to leverage this construct when it comes to providing self-service capabilities to vCloud Director, since the tenant will only be able to perform actions against their own environments and not cross-pollinate access on the same platform. The vCloud Director extension is fully integrated with Rubrik Organizations and vCloud Director Organizations providing the capability to set up and have a 1:1 relationship with Rubrik Organizations to vCloud Director Organizations.

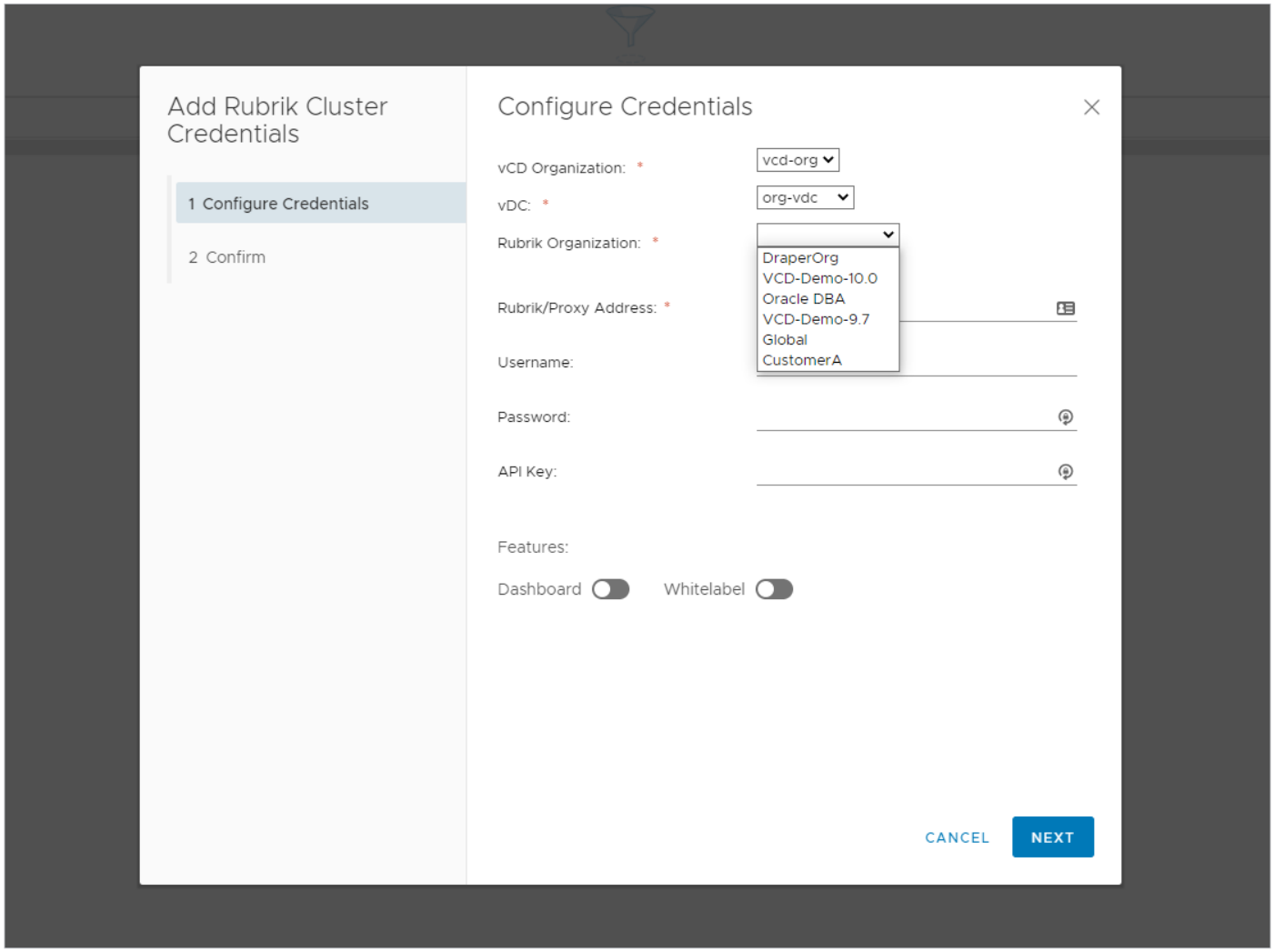
BASE CONFIGURATION

Once the extension has been installed and is visible within vCloud Director, some initial configuration is required before it should be shared out with tenants. As a provider running the extension grants access to a page within the extension called "Settings". This page is required to add new credentials to a virtual data centre (vDC), allowing for the specific vDC to perform actions within the extension.

Using the wizard model, adding a tenant should be as simple as first authentication with Rubrik; this is a manual step required by the provider, and allows the tenant to use their Rubrik administrative privileges to configure the tenants.



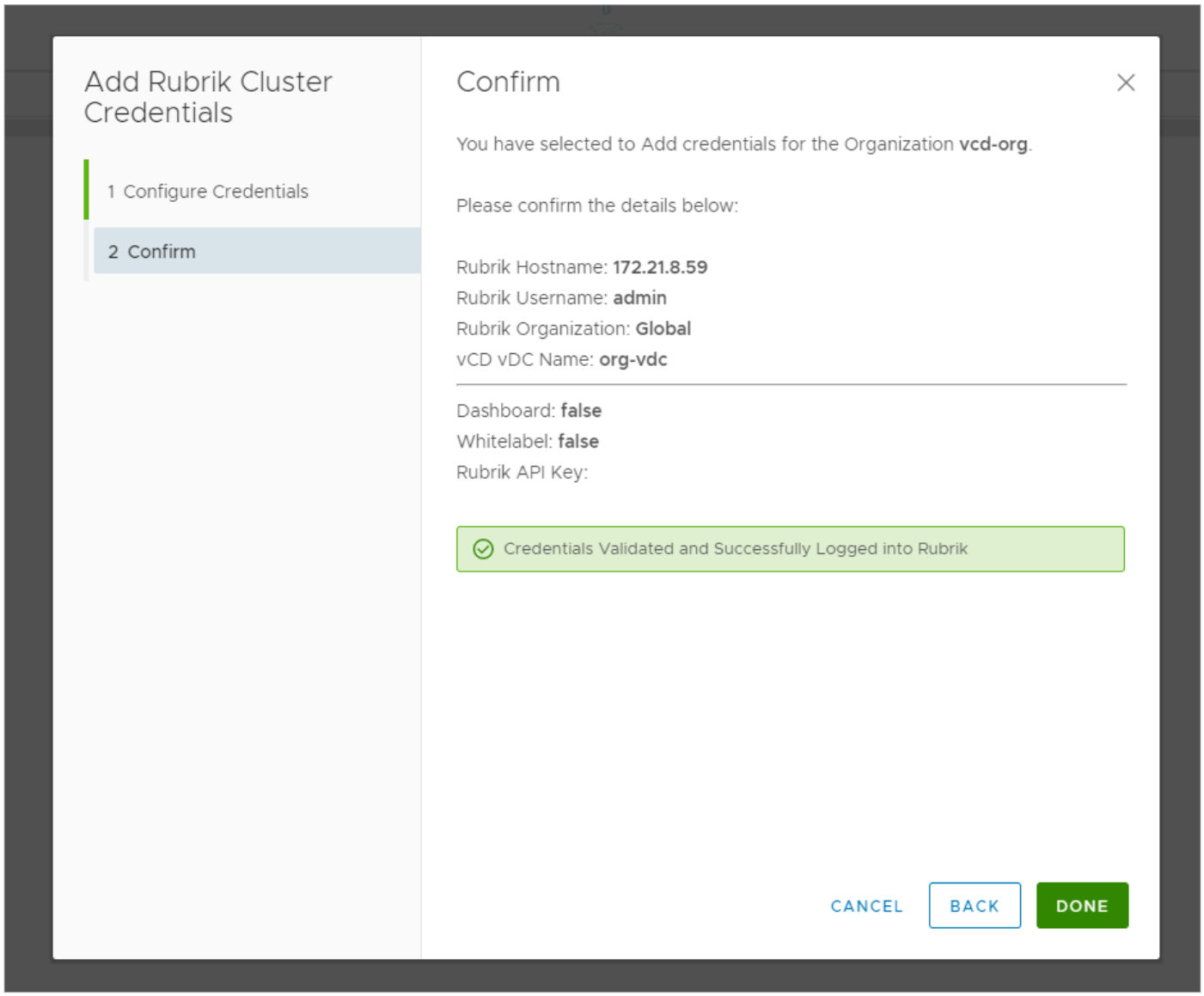
Once successfully authenticated, tenant configuration can begin. Using the wizard under "Add/Update Cluster Credentials" allows for the specific VDCs to be configured; using the wizard, set the vCloud Director Organization to be configured, and the vDCs list will populate with the available vDCs to that Organization. Selecting the vDC will configure that specific vDC for use with the extension. Lastly, we select the Rubrik Organization; it is worth noting that there is a default organization for Rubrik, titled "Global". This will not use the organization, and instead directly authenticate to the Rubrik cluster.



To complete the configuration, the IP Address or the Rubrik Cluster or Proxy is required, and then a username and password or API key is required to be used for authentication.

If the tenant does not require access to reporting, the dashboard can be enabled or disabled using the feature toggles and whitelabel will also remove rubrik branding from the extension.

In the final screen, the configuration will be tested and a message box will confirm if the configuration is valid and the credentials are successful. Completing the wizard will confirm and write the metadata out to the vDC.



This completes configuration of a vDC for use with the extension. Note that if this wizard is run and metadata already exists, it will be overwritten with the new values.

PROVIDER ACTIONS

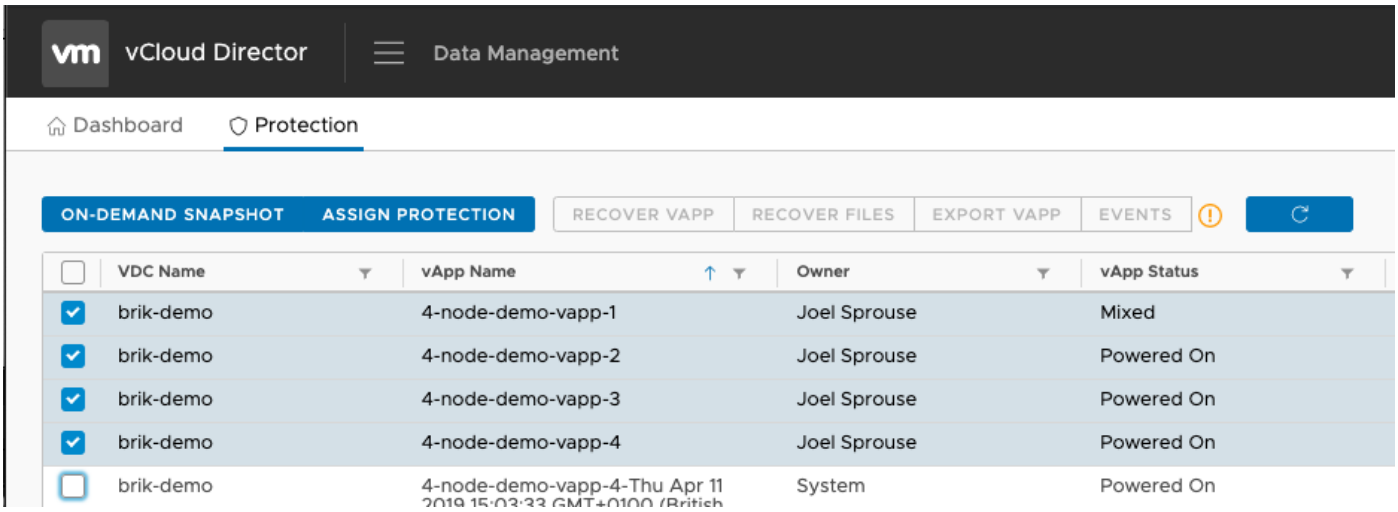
Providers are able to use the vCloud Director Extension tenant workflows as a tenant, however, they will be granted additional capabilities if they have a large permission set than just a specific tenant. Using the extension as a provider and as an administrator for Rubrik, provides can list all vApps for all tenants, regardless of VDC or tenant, and in addition, can perform actions based on their access in Rubrik, meaning provides are able to take vApps that exist in one tenant or VDC, and export to another tenant.

TENANT WORKFLOWS

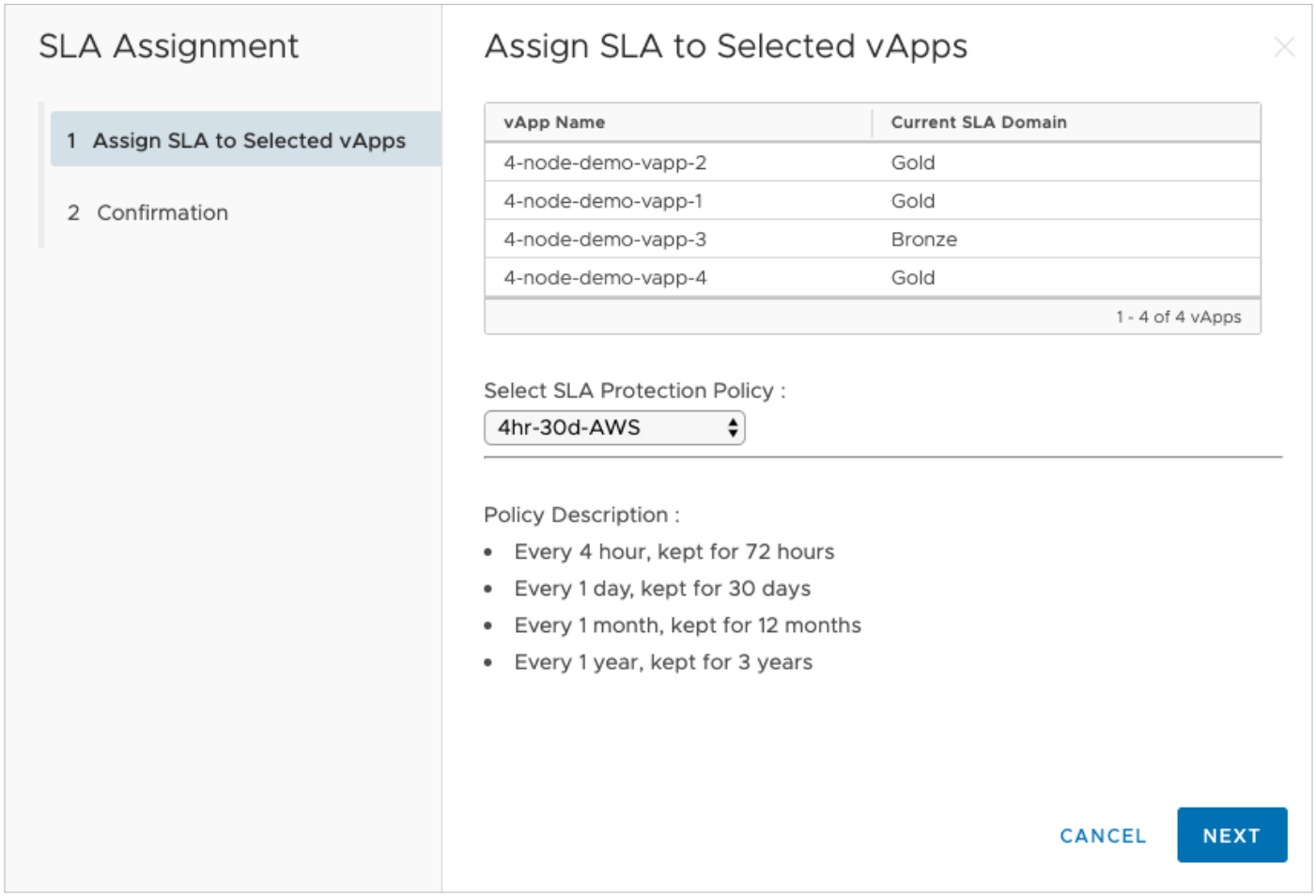
Tenant workflows outline the capability that a tenant will be able to carry out using the Rubrik vCloud Director Extension. These workflows attempt to mirror the workflows that exist today within Rubrik Cloud Data Management executing the same API calls and wizard flows from within the vCloud Director interface.

SLA MANAGEMENT & ON-DEMAND SNAPSHOTS

SLA management and on-demand snapshots are the only two mechanisms that allow for actions to be performed against multiple vApps. These wizards allow the tenant to bulk select a set of vApps inside of the virtual data centre and either apply a specific SLA or take a one-off snapshot using said SLA. In order to perform this workflow, it's as simple as selecting the vApps using the checkbox, and opening the wizard.



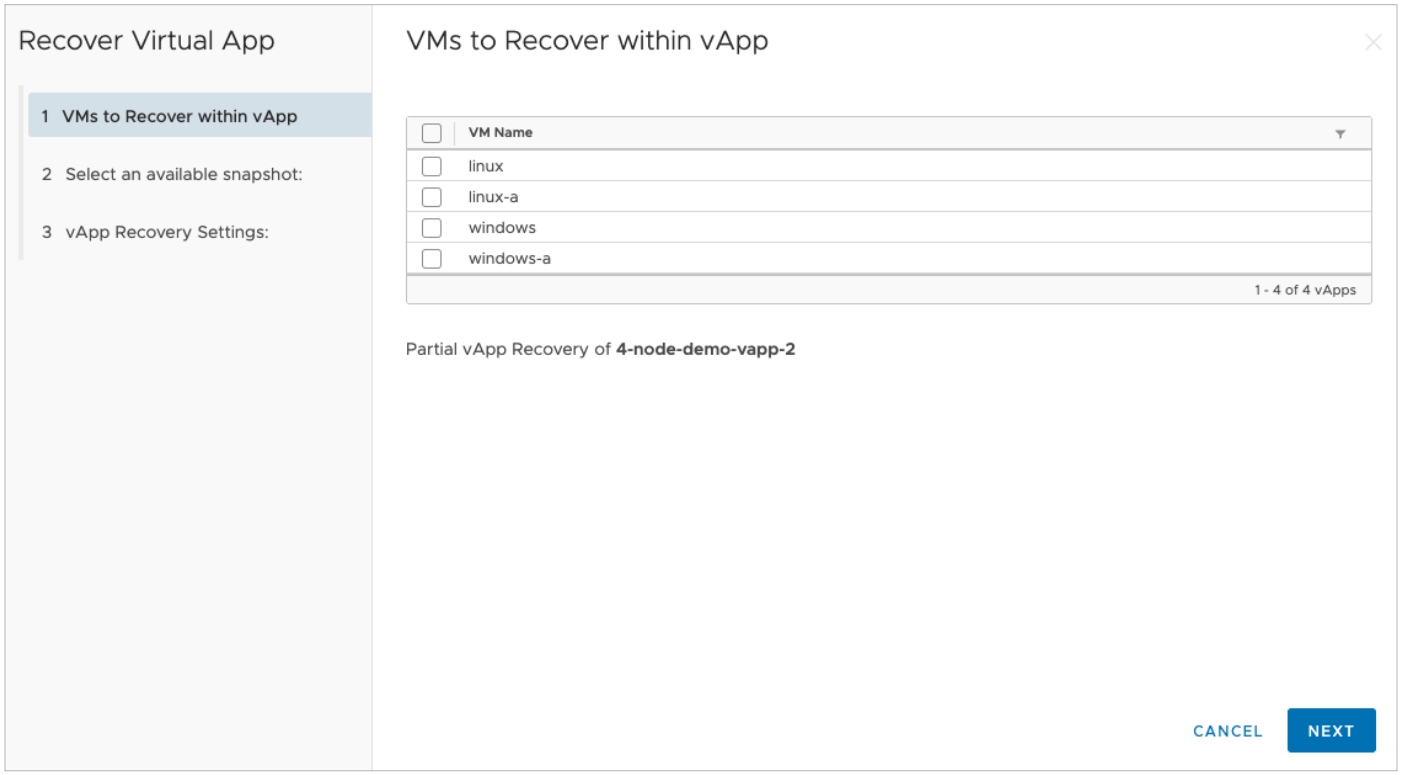
The wizard will prompt for which SLA you would like to use and that's it! The vApps will update as the SLAs are applied asynchronously.

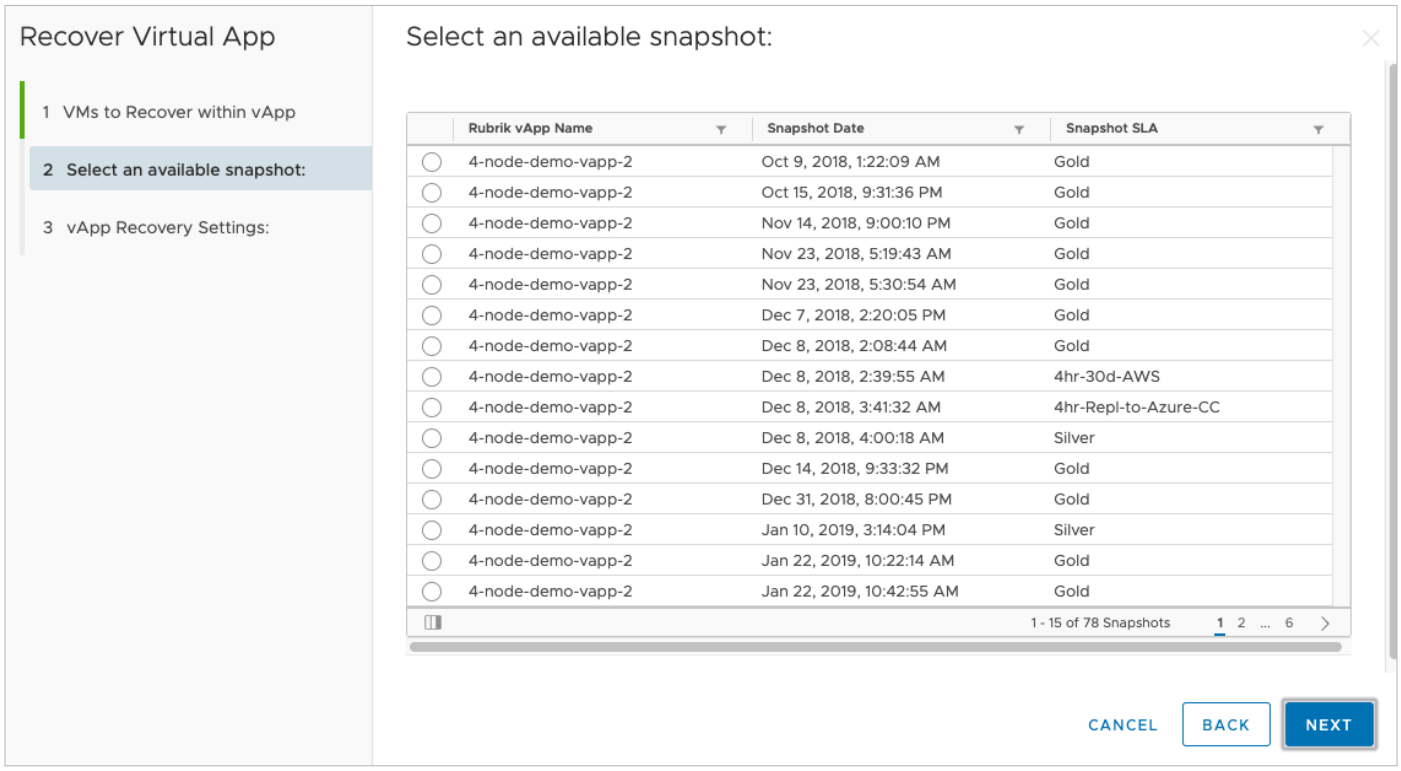


INSTANT RECOVERY & EXPORT

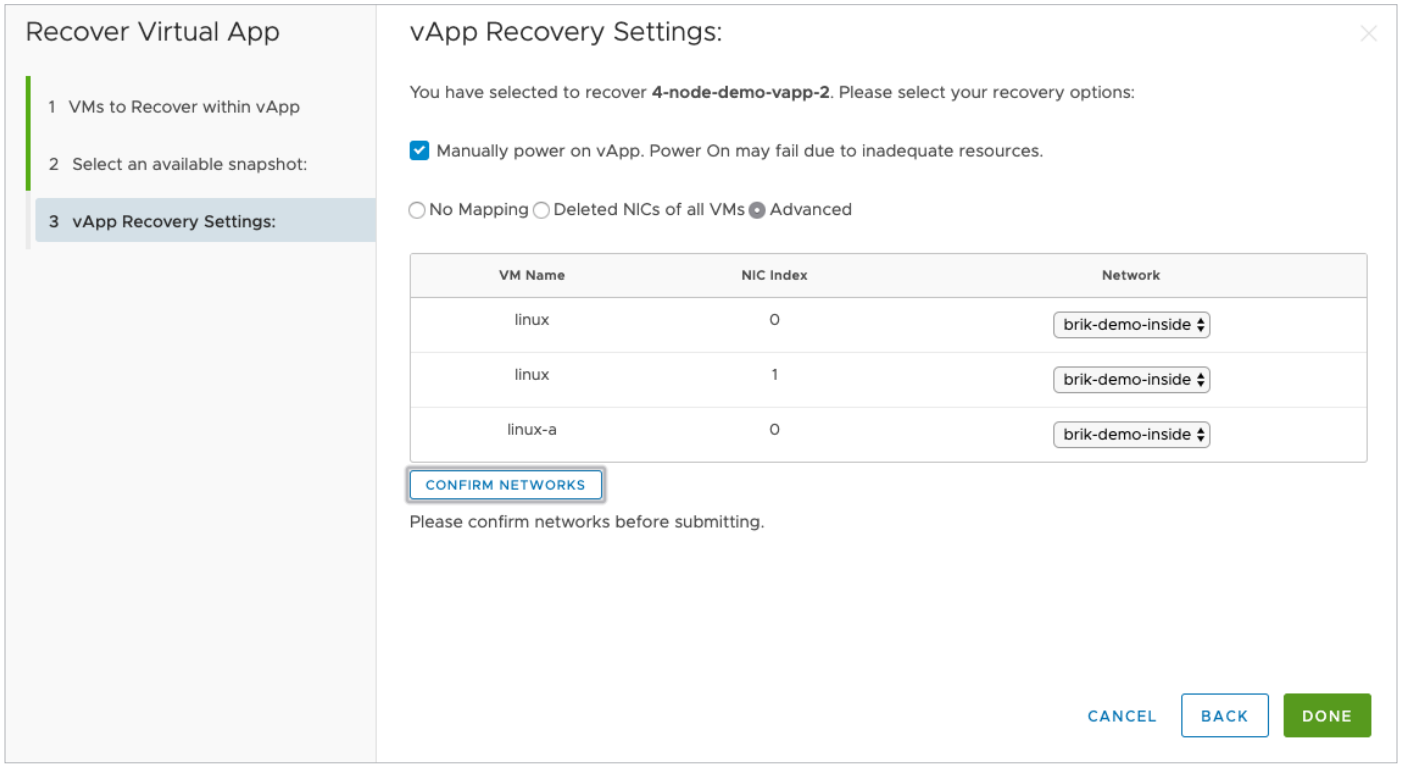
Instant Recovery and Export are both workflows that can only be performed on a per vApp basis; the vApps consist of virtual machines therefore parameters need to be specified for each virtual machine residing inside of the vApp.

When performing an instant recovery, the specific virtual machines to recover need to be specified and a recovery point to recover the virtual machine.

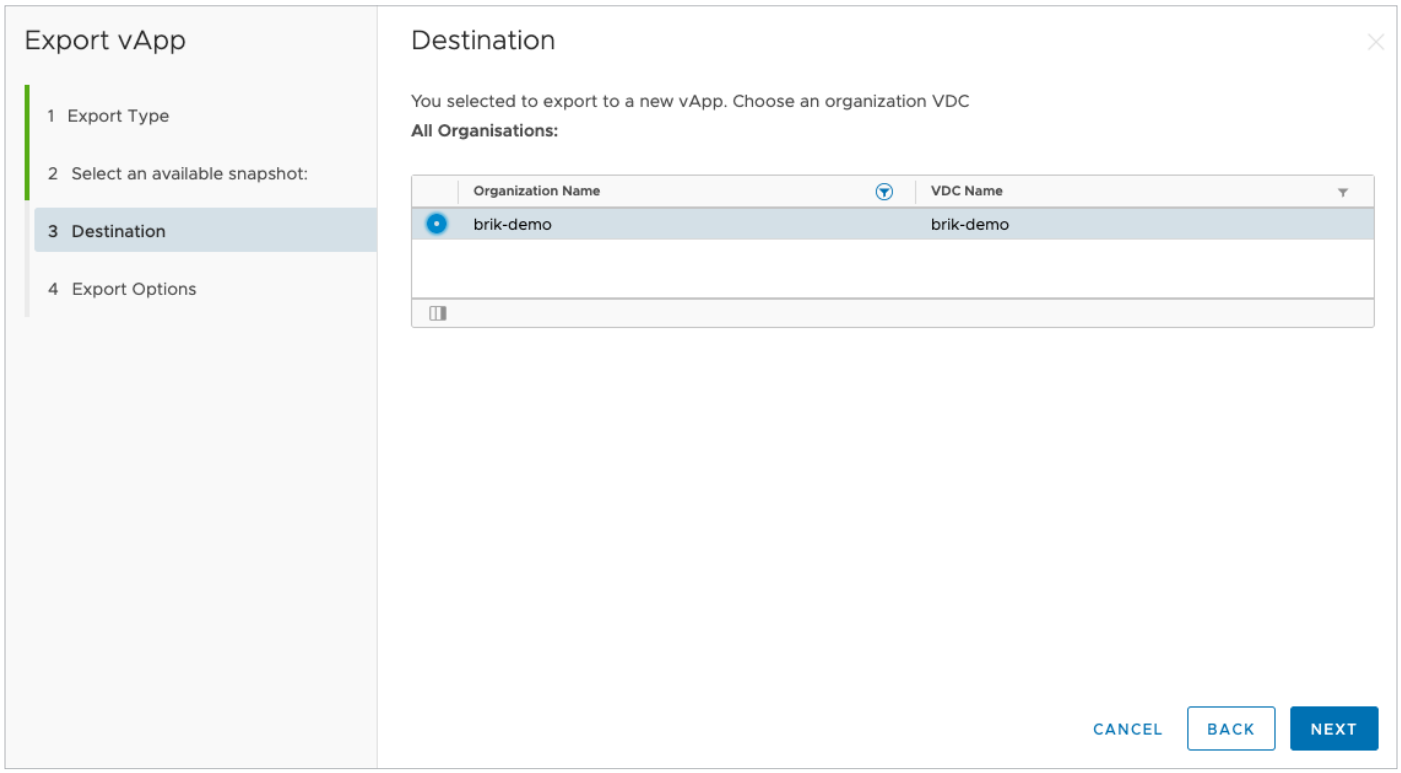




Lastly, network configuration is required for each Network Interface on the virtual machines.



Upon completion, the API request will be sent to Rubrik with the desired configuration for the restore. It is possible to track progress using the Events menu, which will be covered in a later section. Export follows a very similar approach however, we can choose either vApp or VM to export, and we also have the ability to specify the new location (this can be an existing or new vApp).

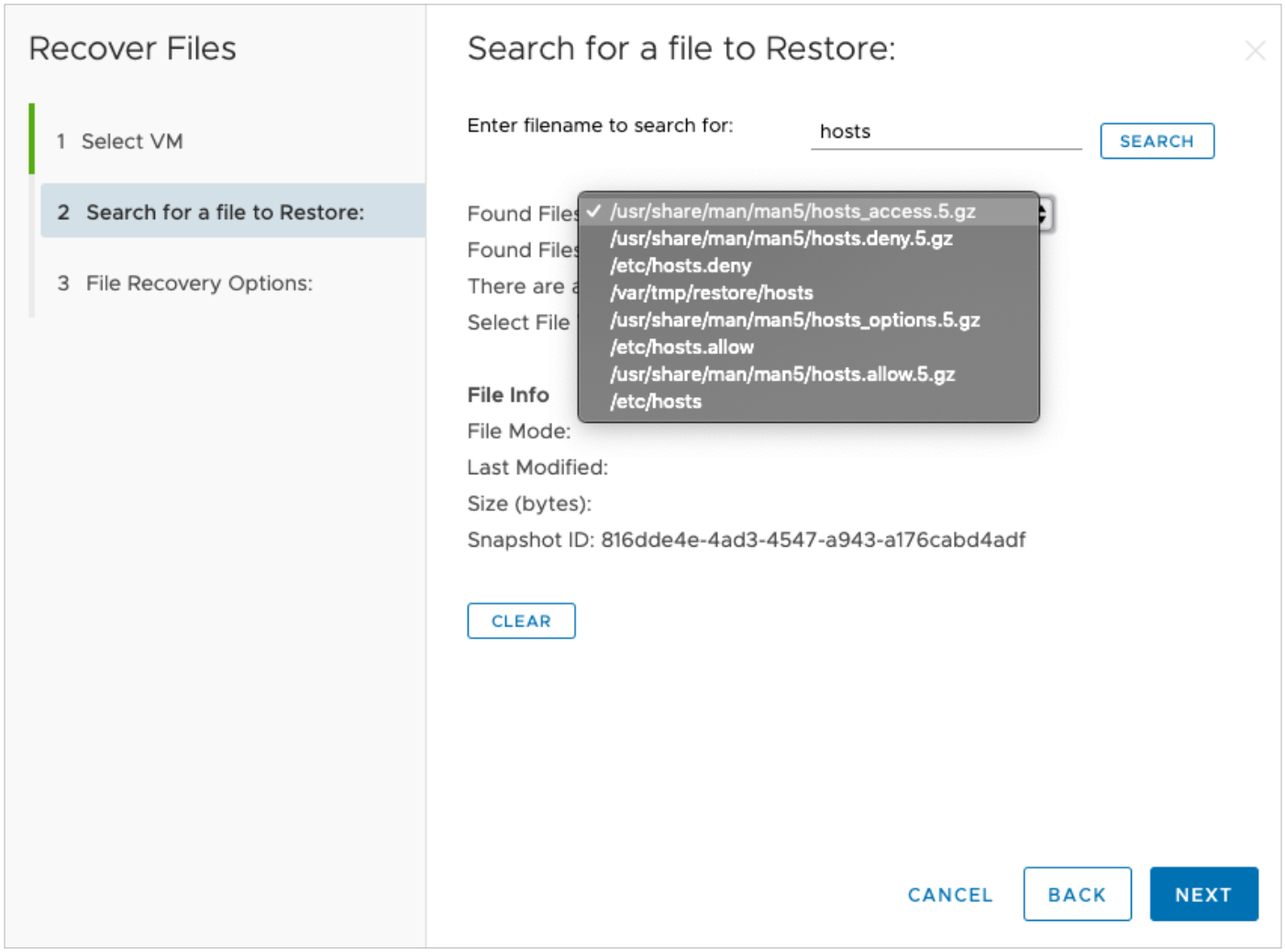


FILE RECOVERY

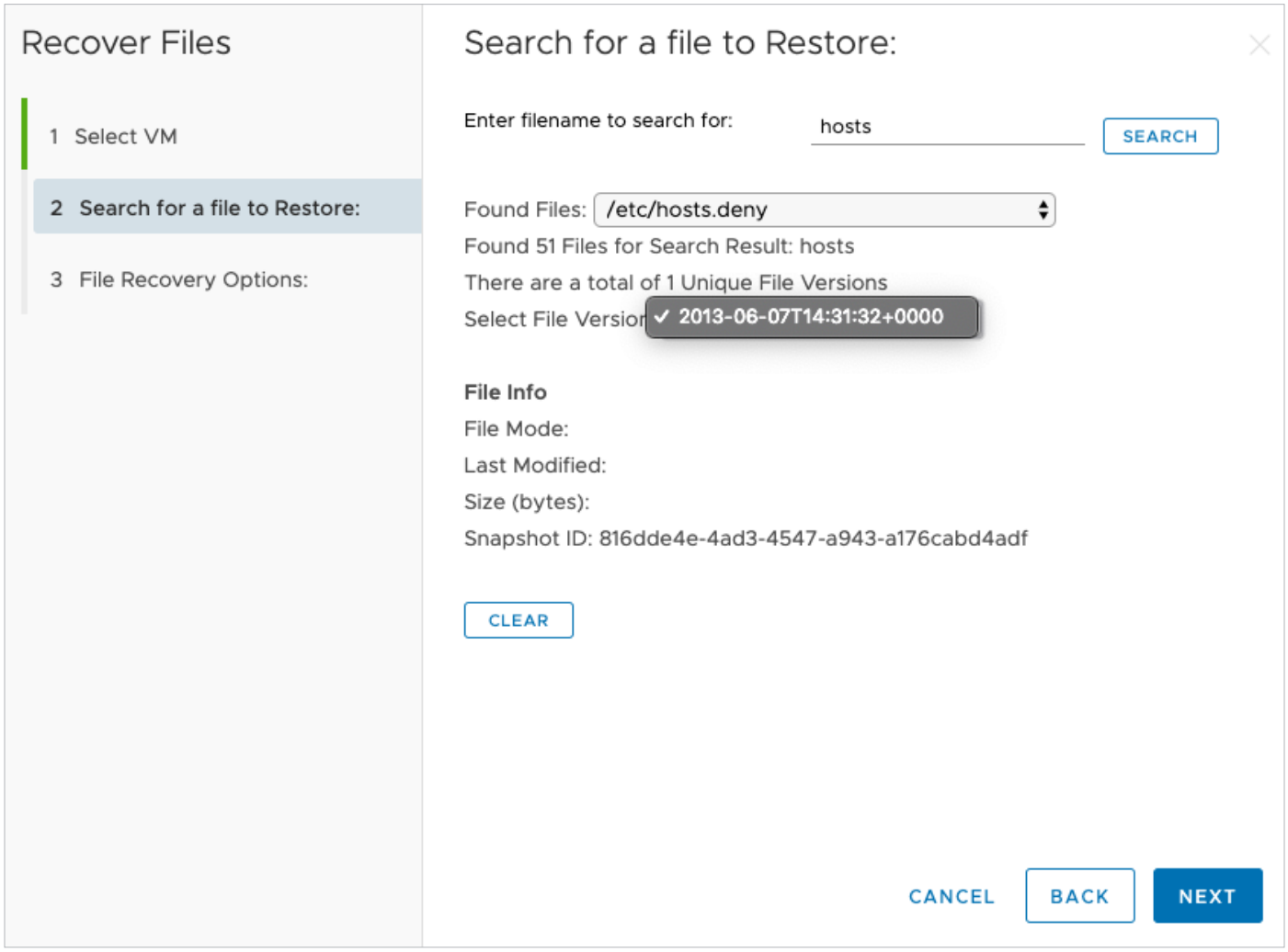
File Recovery is the last recovery workflow available in the extension. This is a specific workflow that applies to a single virtual machine and allows for files to be recovered replacing the original file or to an alternative location on the same virtual machine.

Using File Recovery, we are able to search for files against a specific virtual machine and understand a file's history leveraging the Rubrik metadata to understand file changes across the various snapshot points for the virtual machine.

Opening the wizard for File Recovery will ask to identify the virtual machine on which the file restore is to occur, and the next screen has a free-text search to match files against from the snapshot.



After selecting the file, the extension will calculate unique file versions based on the file change stored within the metadata from the Rubrik API and display the date and time of each unique file. This allows for the most relevant snapshot to be identified and used to perform the file restores.

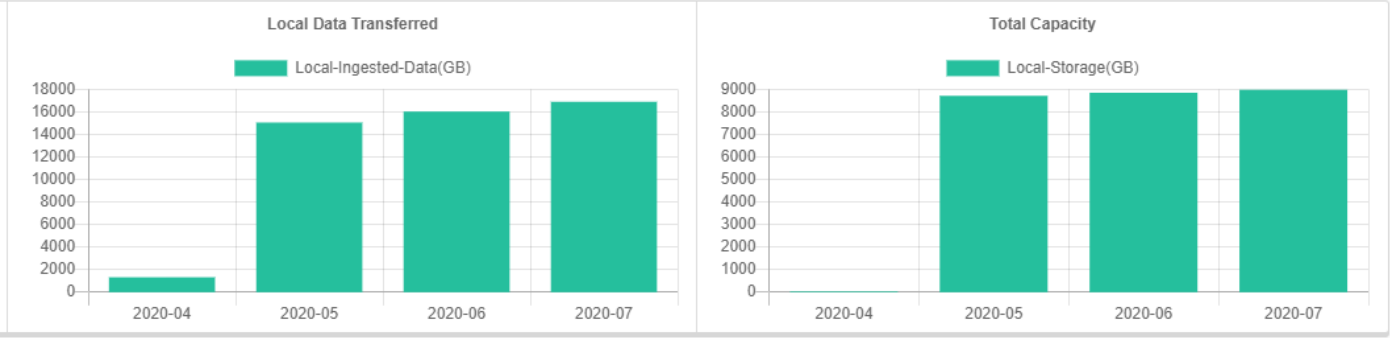


Lastly, the workflow will provide options for the file recovery process, once selected, the extension provides the ability to either overwrite the current file, if it exists or not, or restore to an alternative location, providing the capability to ensure the restored file is correct. For both of these options, it is also possible to choose to either restore the file using VMware tools or via the Rubrik Backup Service (RBS) agent (that would need to be installed prior to performing the restore). Using VMware tools requires credentials to be specified for the restore, whereas RBS leverages the service account that has been configured to run with to carry out recovery.

REPORTING & EVENTS

Event monitoring and reporting are key elements when providing self-service capabilities; both empower the tenant or end user to have insight into the protection of their data. In addition, this is almost real-time to monitor a job progression such as an important restore that is service affecting or data recovery that may have been lost. This ensures that the tenant is aware of everything on-going as it able understand and track tasks where required without the need to reach out the service provider.

Within Rubrik, there are many reports that provide different insights such as SLA compliance, object backup and recovery tasks, and capacity consumption over time. Leveraging these report APIs, and the rubrik organizations, it is easy to provide these metrics to the tenant and provide some graphs giving a simple visual representation of the reports.



The extension currently leverages the following reports provided out of the box by Rubrik:

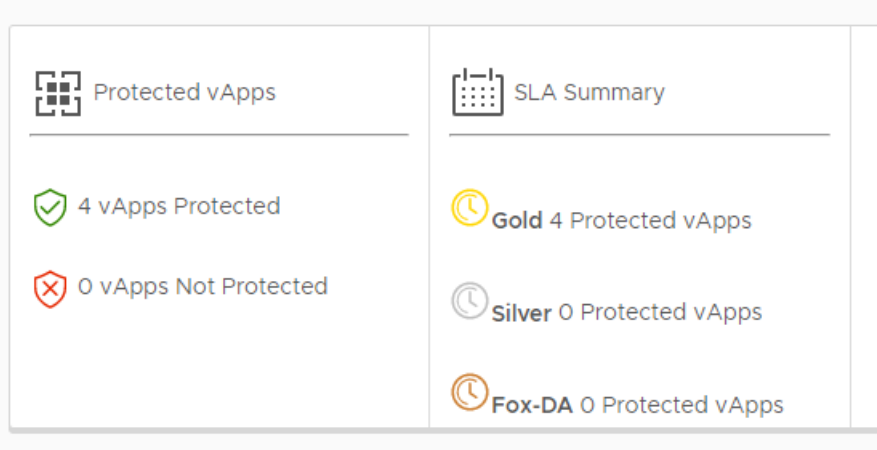
- Protection Task Details
- SLA Compliance Summary
- Recovery Task Details
- Capacity Over Time

REPORTS Current Report: **Capacity Over Time**

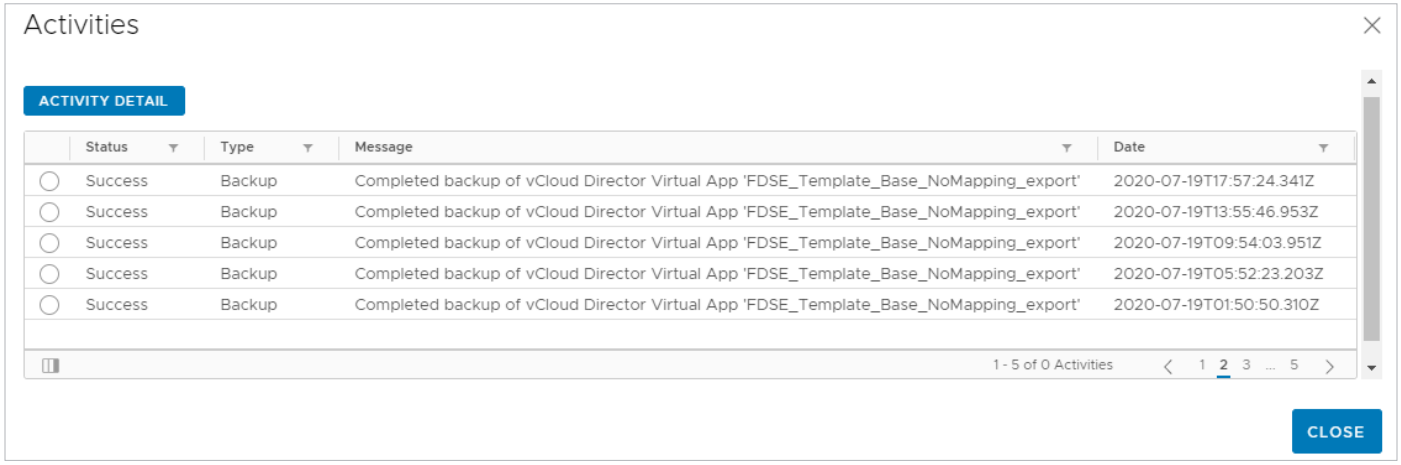
Month	Organization	Local Storage	Archive Storage	Local Storage Growth	Archive Storage Growth
2020-04	VCD-Demo-10.0	1.28 GiB	0.00 bytes	1.28 GiB	0.00 bytes
2020-04	VCD-Demo-9.7	16.81 GiB	0.00 bytes	16.81 GiB	0.00 bytes
2020-04	Global	18.09 GiB	0.00 bytes	18.09 GiB	0.00 bytes
2020-04	Global	21.71 GiB	0.00 bytes	15.51 GiB	0.00 bytes
2020-05	VCD-Demo-10.0	6.70 GiB	0.00 bytes	5.42 GiB	0.00 bytes
2020-05	CustomerA	18.20 GiB	0.00 bytes	18.20 GiB	0.00 bytes
2020-05	Global	23.12 GiB	0.00 bytes	1.41 GiB	0.00 bytes
2020-05	VCD-Demo-9.7	33.12 GiB	0.00 bytes	16.31 GiB	0.00 bytes
2020-05	Oracle DBA	97.71 GiB	0.00 bytes	34.81 GiB	0.00 bytes
2020-05	Global	8.69 TiB	7.06 TiB	8.53 TiB	7.06 TiB

1 - 10 of 22 1 2 3

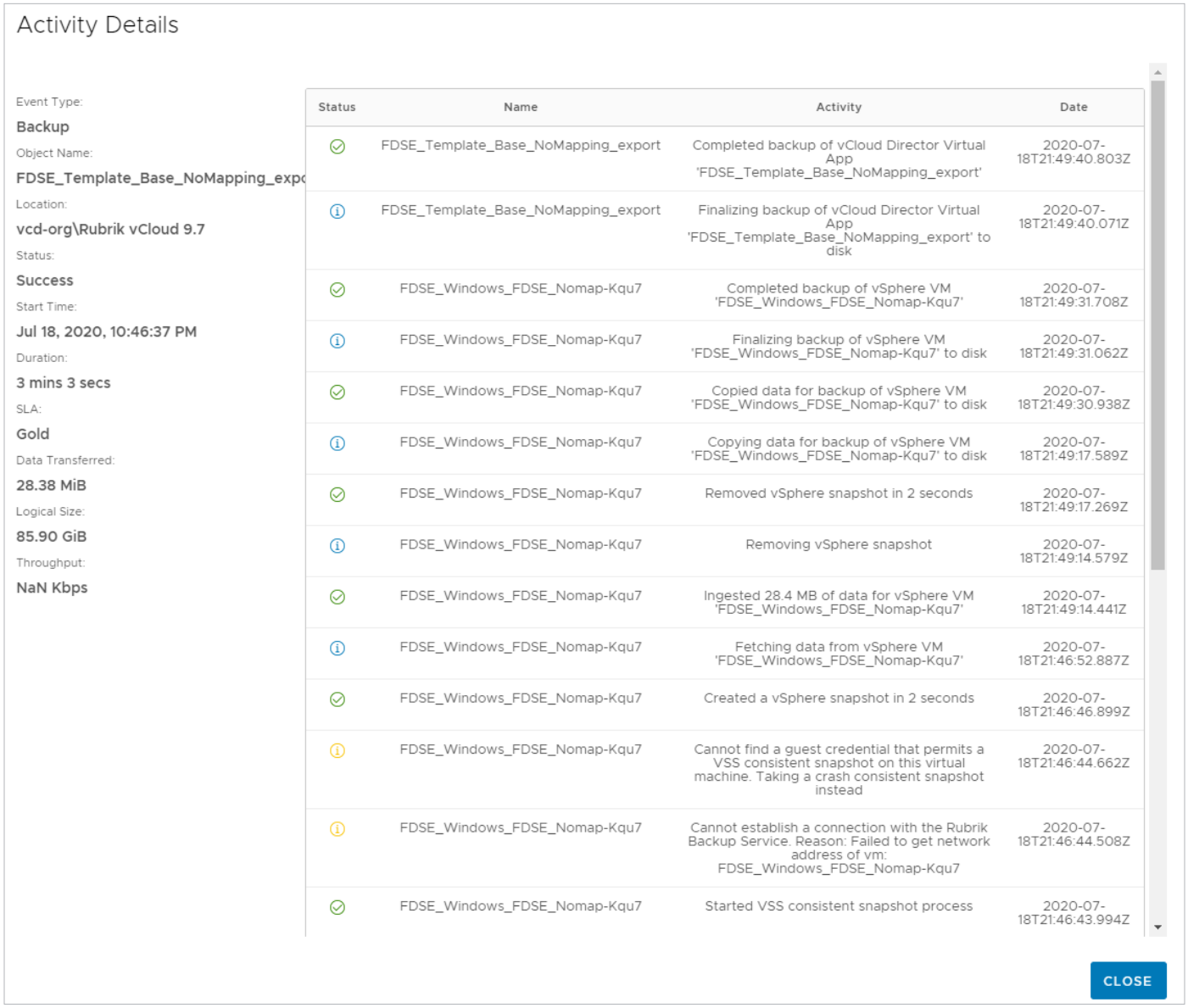
In addition, there are also high level metrics which provide a quick high level insight into the environment, such as protected objects and SLA assignment:



In addition to the reports, each vApp has an associated set of events, and each event also has an event series. Leveraging the events and event series, provides the near real-time progression of on-going events.



Within each event, we can see the specifics with a task by task status, and a state for each task. In addition, summary metrics are also available:



CONCLUSION

In summary, the vCloud Director extension provides a single self-service portal for providers and tenants allowing them to manage and understand their own environments without the need to raise support requests and without delays.

GLOSSARY

Acronym	Description
vCD	vCloud Director
VDC	Virtual Data Centre
vApp	Virtual Application
JS	Javascript
AngularJS	Angular Javascript Framework
HTML5	Hyper text markup language v5.0
SLA	Service Level Agreement
RBS	Rubrik Backup Service
API	Application Programming Interface
CORS	Cross Object Resource Sharing
LDAP	Lightweight Directory Access Protocol
MITM	Man-in-the-middle
UX	User Experience
UI	User Interface
NAS	Network Attached Storage
ACL	Access Control List
NAT	Network Address Translation

SOURCES AND NOTES

- VMware VCD Ext SDK
- VMware Samples - Customize Portal
- VMware vCD Snapshot
- AngularJS
- Clarity Design System

VERSION HISTORY

Version	Date	Summary of Changes
1.0	August 2020	Initial Release

rubrik

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

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

20200901_v1