Veritas NetBackup™ plug-in for VMware vRealize™ 2.0

Installation and Configuration Guide

Last Updated: April 07, 2021

Contents

1. INTRODUCTION

This document describes the installation and configuration of the Veritas NetBackup™ plug-in for VMware vRealize™ 2.0. Customers can embed NetBackup™ backup and recovery services in the vRealize™ Automation (vRA) portal, or their related workflows.

The plug-in uses the NetBackup™ REST API. It includes workflows and the actions which service designers can use to configure tailored solutions. Examples include provision and protect orchestration, and "day 2 operation" wrappers, such as backup and restore VM.

The following services are provided:

- Protect VMware VM, MS SQL Server Database, Amazon Web Services (AWS) VM, and AWS Volume.
- Unprotect VMware VM, MS SQL Server Database, AWS VM, and AWS Volume.
- Restore VMware VM, Deleted VMware VM, MS SQL Server Database, AWS VM, and AWS Volume.
- Agentless VMware file restore.
- Backup Now for VMware VM, MS SQL Server Database, AWS VM and AWS Volume.

The Backup Now feature requires NetBackup™ 8.2+, MS SQL Server features require NetBackup™ 8.3+

Additional workflows are included. These support the core services that are listed above and aid system monitoring and configuration.

2. PREREQUISITES

The plug-in has been developed with vRealize™ Orchestrator (vRO) 8.3. The plug-in supports NetBackup™ 8.2 and above.

The NetBackup™ REST API must be accessible by vRO.

Protection functionality requires the definition of Protection Plans for the relevant Asset Classes within NetBackup™. You must firstly perform this configuration through the NetBackup™ Web UI.

Agentless file restore requires additional software to be installed on the NetBackup™ backup server. Please refer to the NetBackup™ documentation.

Authentication supports API key in addition to user id / password and this is the recommended approach.

If AWS is used, the AWS plug-in for vRO must be installed first. The plug-in must be minimum version 1.2

3. Design Considerations

The plug-in supports multiple backup servers. Each backup server can run different versions of NetBackup™.

The plug-in also supports the ability to define different credentials for a backup server. This ability enables the designer to take advantage of NetBackup™ RBAC to restrict the available protection plans. If you require this feature, you must create multiple backup server connection entries to the same backup server, each with different credentials.

Note: you should not use RBAC to restrict asset visibility. Visibility is controlled in vRO/A, outside NetBackup™.

For more information on managing accounts and RBAC at NetBackup, you should reference the Web UI Security Administrator's Guide (https://www.veritas.com/support/en_US/doc/135031700-135031704-0/index).

You must create the rules that determine which backup server is responsible for an asset in VMware or AWS.

All operational workflows look for the presence of a selected asset in the NetBackup™ asset store as a pre-validation step. If the asset is not present in NetBackup™, the asset is created by the plug-in with enough information to enable its protection. Standard NetBackup™ asset discovery functionality will augment the attributes held against the asset in due course.

4. Installation

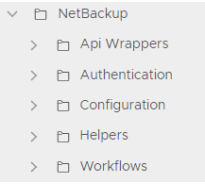
The vRO plug-in is provided as a vRO package and is installed using the standard package import functionality.

1. Open the vRealize™ Orchestrator; log on as a user with administrative rights
2. Expand the side menu, from the Assets section, click Packages then the import button. Select the file *com.veritas.netbackup.v2.package,* trust the certificate and import all the content

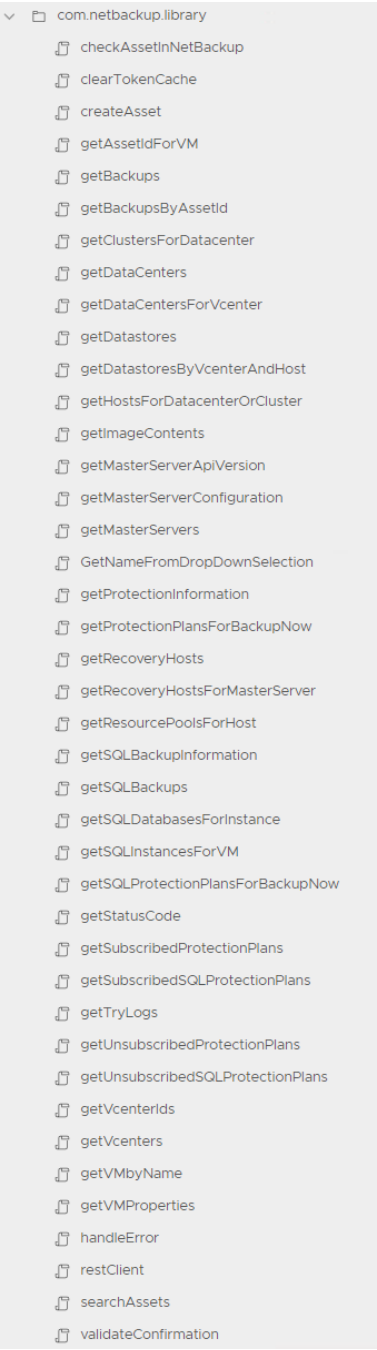
Once the import completes, you see new folders in Workflow, Actions, Configuration, and Resources tabs.

Note: all screenshots have been taken in “folder view” mode.

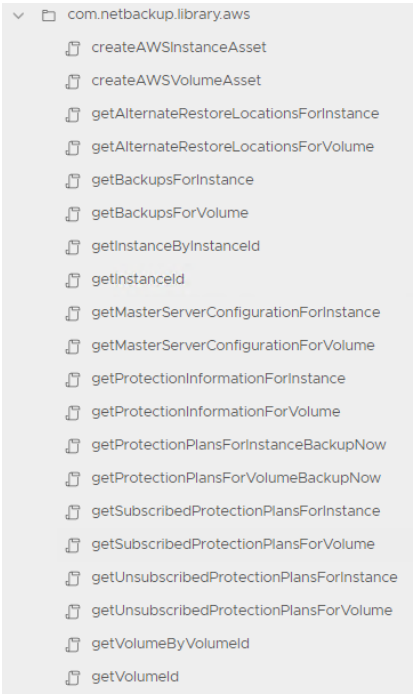
In the Workflow / Library folder, found in the library folder:



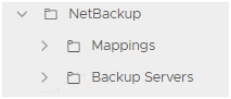
In the Actions folder, the actions for core functionality and VMware assets:



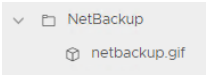
Also, in the Actions folder, the actions for AWS assets:



In the Assets/Configurations folder, found in the library folder:



In the Assets/Resources folder:



5. CONFIGURATION

5.1 BACKUP SERVER

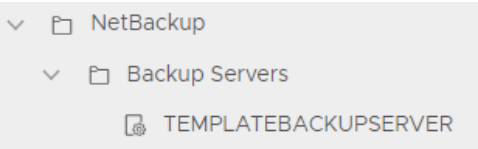
The plug-in requires a NetBackup™ user account that has the *Backup Administrator* role.

Before entering the user credentials, you must consider the different authentication schemes:

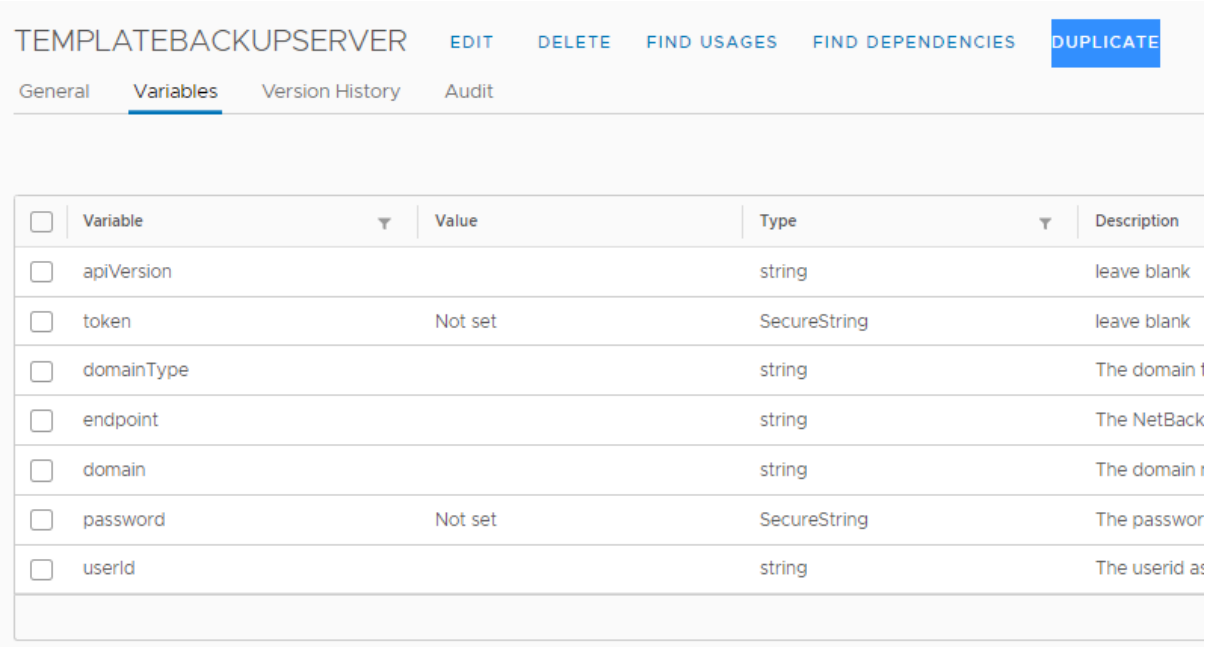
- User ID and password.
- User ID and API Key. This option is recommended.

Use the following link to find out more information on managing NetBackup™ user accounts.
https://www.veritas.com/support/en_US/doc/135031700-135031704-0/index

Your first step in the configuration process is to define one or more backup server(s). Under the Configurations tab, you should expand the “NetBackup” folder. You can find this in the library folder. Now you can access the Backup Servers subfolder.

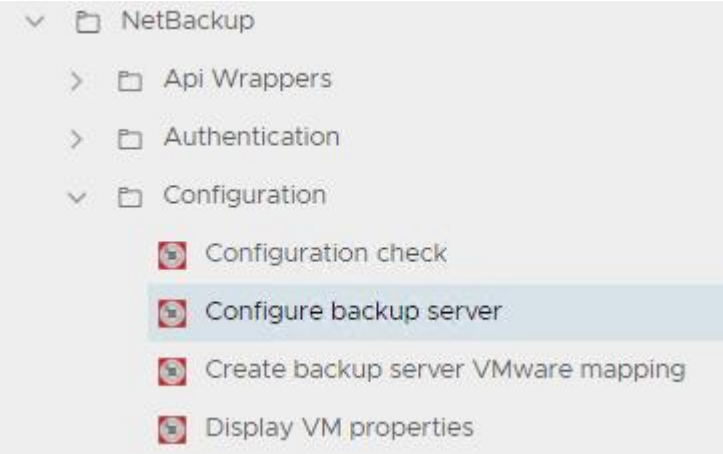


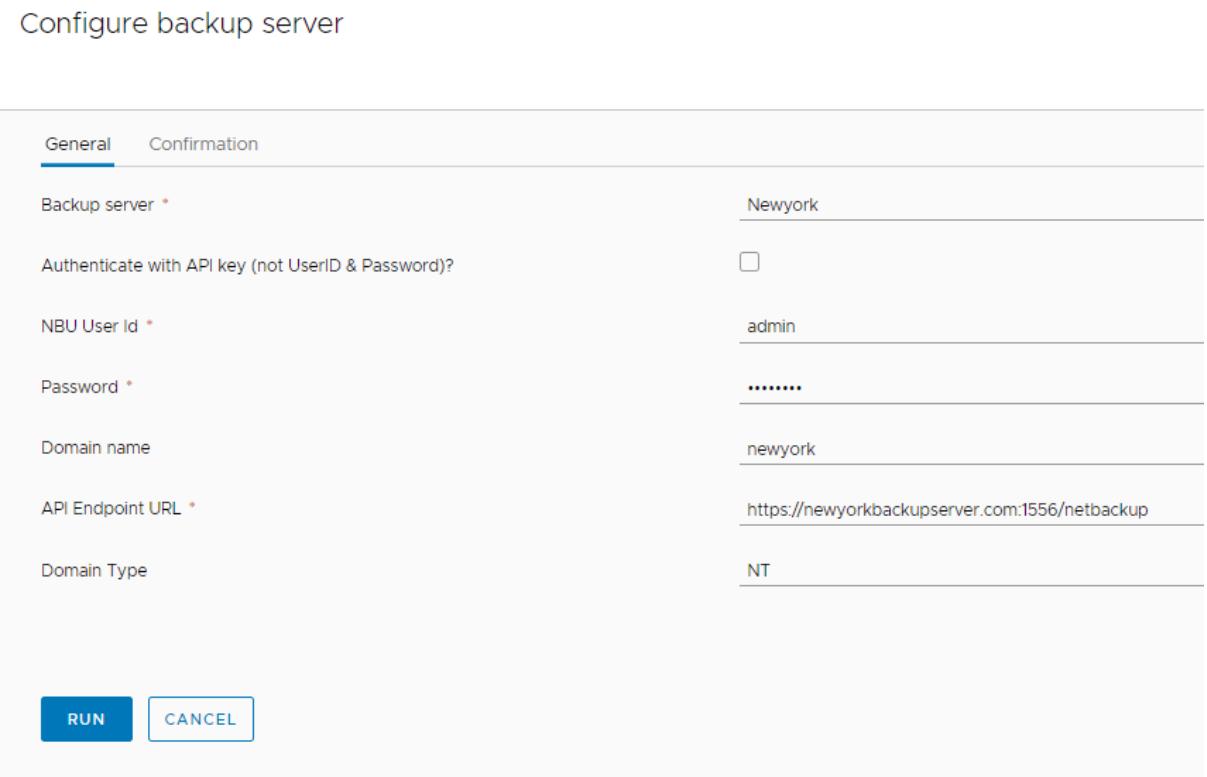
TEMPLATEBACKUPSERVER is an empty configuration element that contains all the settings that are required to connect to a NetBackup™ backup server. You can duplicate and edit this element to create a new backup server entry. You must not rename, delete, or edit the TEMPLATEBACKUPSERVER configuration element.



By default, the duplicate will be called TEMPLATEBACKUPSERVER Copy, this should be renamed to something meaningful.

Once the new backup server configuration has been created, you can use the “Configure backup server workflow” to set the NetBackup™ API endpoint and credentials.





You should fill out all the fields, including replacing *backupserveraddress.com* in the API Endpoint URL field. Click on the confirmation tab and confirm the operation before you click Submit.

On submission, the workflow updates the backup server’s configuration and runs the Configuration Check workflow. You can see this below.

5.3 MAPPINGS

The Mappings section in the Configuration tab contains the rules for an asset's attributes to determine the backup server.

You should create subfolders within the Mappings / AWS or Mappings / VMware sections. Within each folder create a configuration element, setting its name to the target backup server. The following two sections explain this principle in detail.

Note: you must use lowercase letters for folder names.

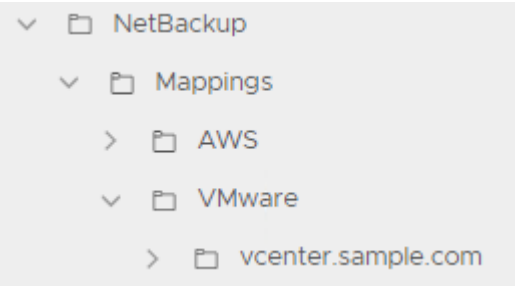
5.3.1 VMware

The mappings can use up to three VM attributes to determine the backup server:

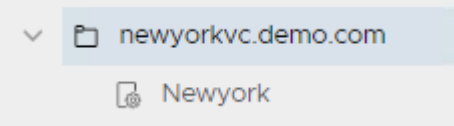
- vCenter Instance
  - Datacenter
    - Resource Pool

You can map to a backup server at any level. You should create one mapping at vCenter level, to act as a default. This configuration can be helpful where lower-level mappings do not match all the assets in the asset base.

In this example, three vCenter instances are defined. *vcenter.sample.com* is shipped with the package, and you can delete or amend this instance, as required:

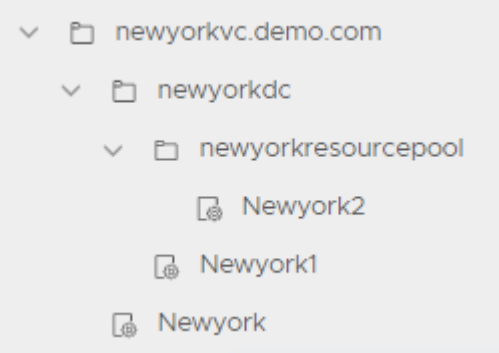


The first vCenter instance uses only a vCenter level mapping:



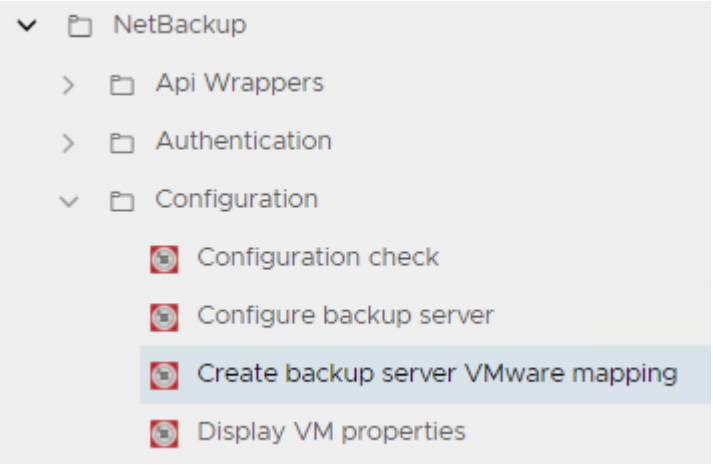
This example shows that the Backup server configured as *Newyork* manages any VMware VM from this vCenter.

The second mapping includes mappings at different levels:



In this example, if a VM belongs to the resource pool newyorkresourcepool in the datacenter *newyorkdc*, the backup server 'Newyork2' manages it. A VM in the same datacenter, but in a different resource pool, is assigned to backup server 'Newyork1'. The 'Newyork' server manages all other VMs for vCenter *newyorkvc.demo.com* that the previous two rules do not cover.

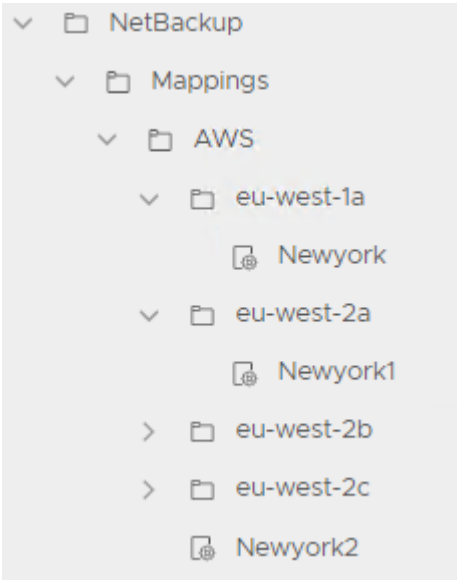
A workflow is provided to assist in the creation of vCenter & Datacenter level mappings:



5.3.2 AWS

The AWS mappings let you specify a backup server at AWS region level. You can also define a default setting for the regions that are not included in the region-specific sections.

You can create the mapping as:

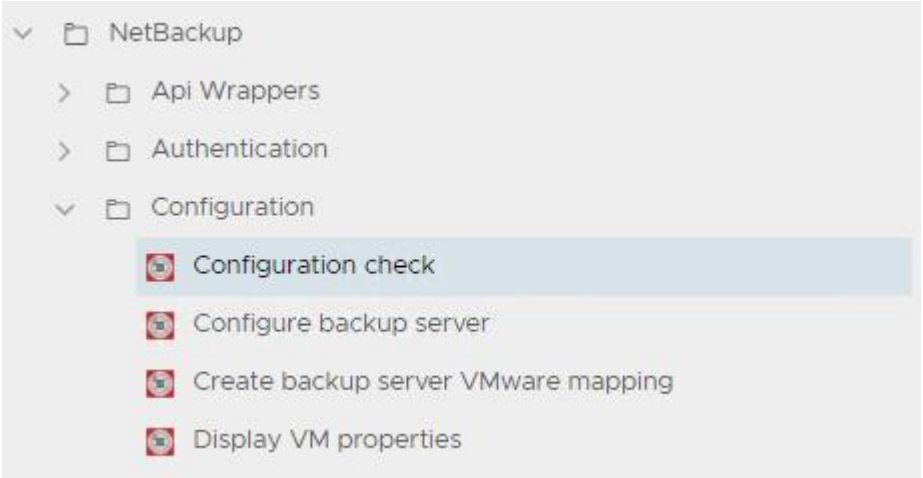


In this example, the backup server 'Newyork2' manages any AWS VM or volume that does not belong to any of the AWS regions listed.

The backup server 'Newyork' manages a VM or volume from AWS region *eu-west-1a*.

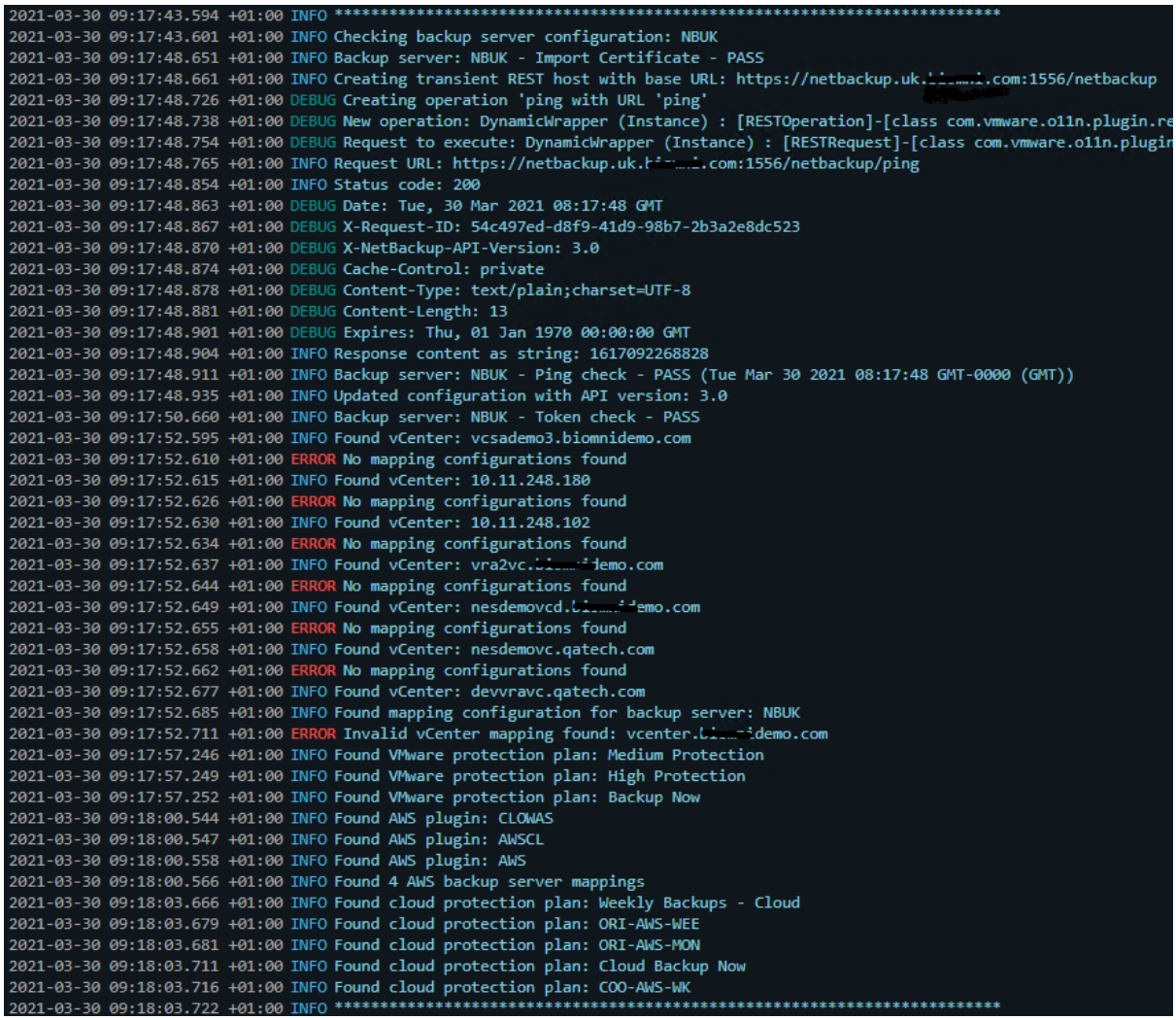
5.3.3 Configuration Check

Once you have completed the configuration, you must run the Configuration Check workflow.



This workflow checks the connection to, and credentials for, all defined backup servers. For each backup server it also checks the existence of Protection Plans for the different asset classes. This process requires the backup server to be included in any mappings.

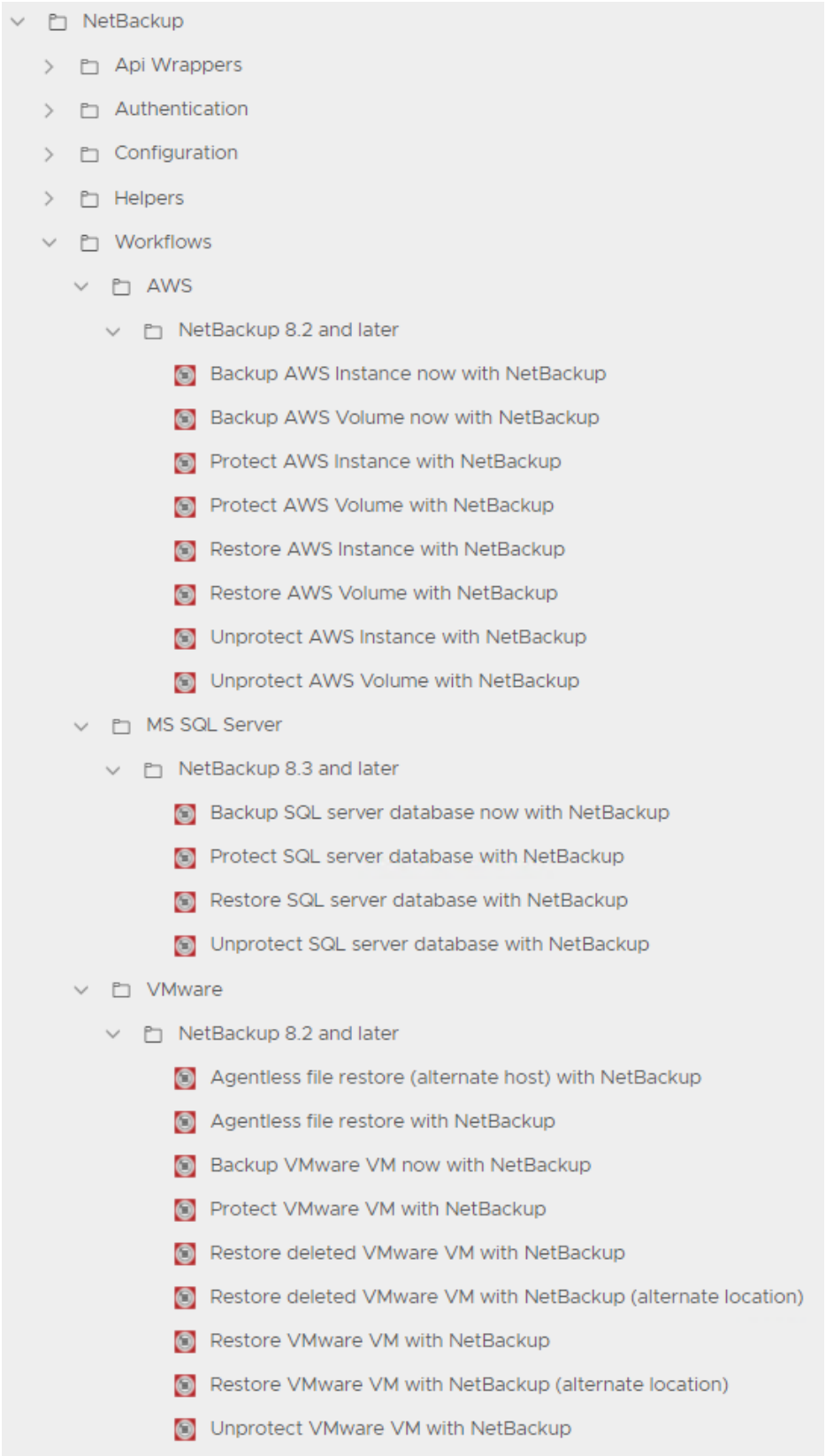
Sample output for a single backup server check:



This workflow is run every time a new backup server is added, to ensure that all data entered is correct. It can be run at any time to validate the current configuration.

6. Operational Workflows

The plug-in contains workflows for VMware, MS SQL Server and AWS asset classes, with sub folders for the relevant NetBackup version (see below).



6.1 VMware Workflows

The operations that are supported are:

- Protect VM
- Unprotect VM
- Restore VM - Restores the VM to the original location, with the option to rename the restored VM
- Restore VM Alternate – Restores the VM to an alternate location / name
- Restore deleted VM – Restores a previously deleted the VM to the original location, with the option to rename the restored VM
- Restore deleted VM alternate – Restores a previously deleted the VM to an alternate location/name
- Backup Now
- Agentless file restore to original host
- Agentless file restore to alternate host

Protection and Backup Now require NetBackup™ VMware Protection Plans.

6.2 AWS Workflows

The operations that are supported include:

- Protect Instance
- Unprotect Instance
- Protect Volume
- Unprotect Volume
- Restore Instance - Restore instance back to its original location or to an alternative Virtual Private Cloud (VPC) or Subnet
- Restore Volume - Restore volume back to an alternative Virtual Private Cloud (VPC) or Subnet
- Backup Instance Now
- Backup Volume

Protection and Backup Now require NetBackup™ Cloud Protection Plans.

6.3 MS SQL Server workflows

The operations that are supported are:

- Protect database
- Unprotect database
- Restore database
- Backup database

Protection and Backup Now require NetBackup™ MS SQL Server Protection Plans.

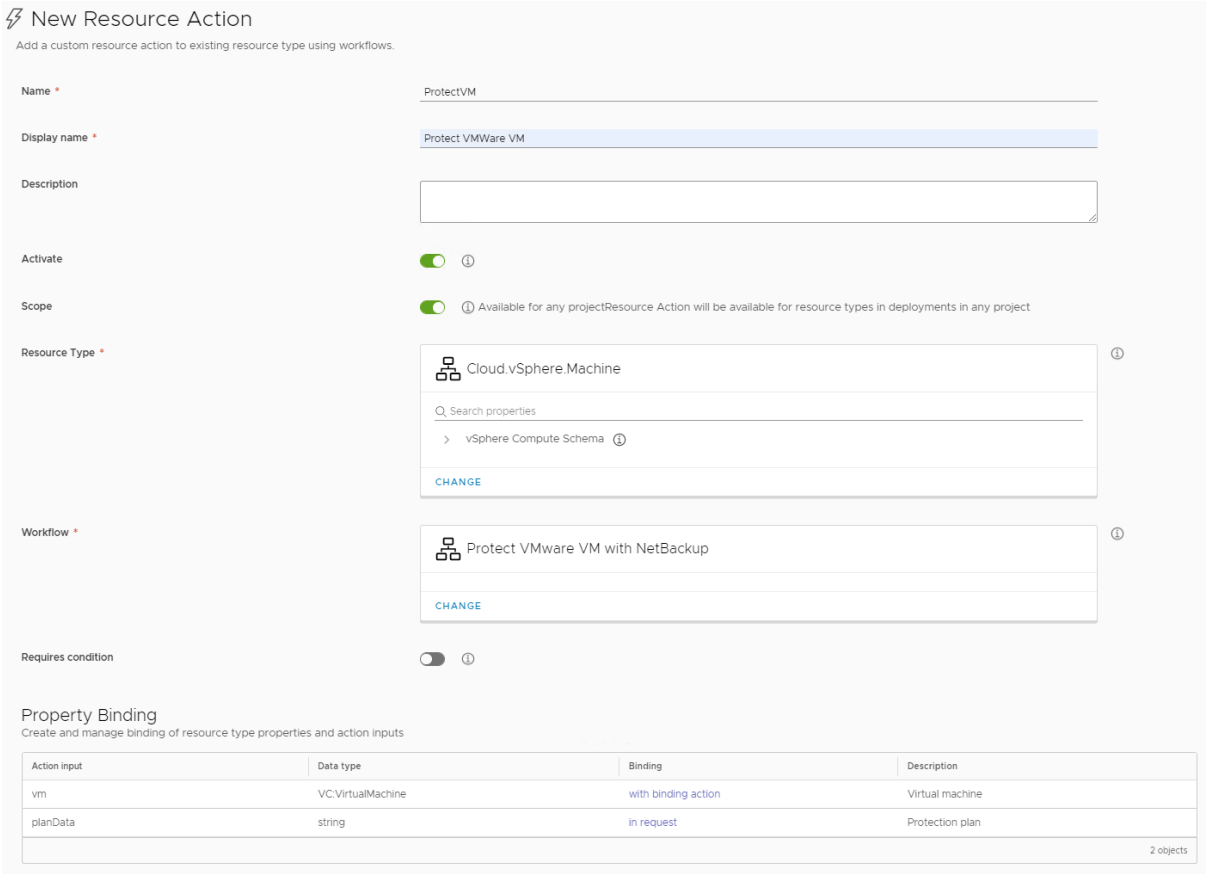
7. vREALIZE AUTOMATION

vRealize™ Automation (vRA) Resource Actions can be created to enable users of vRA Cloud Assembly and Service Broker to utilize the supplied workflows from Deployed VMware VM's and AWS Instances/Volumes.

Any of the workflows can be used within a Resource Action, but it is recommended that the ones that allow restoration to Alternative locations are avoided as infrastructure that the user should not have access to may be available.

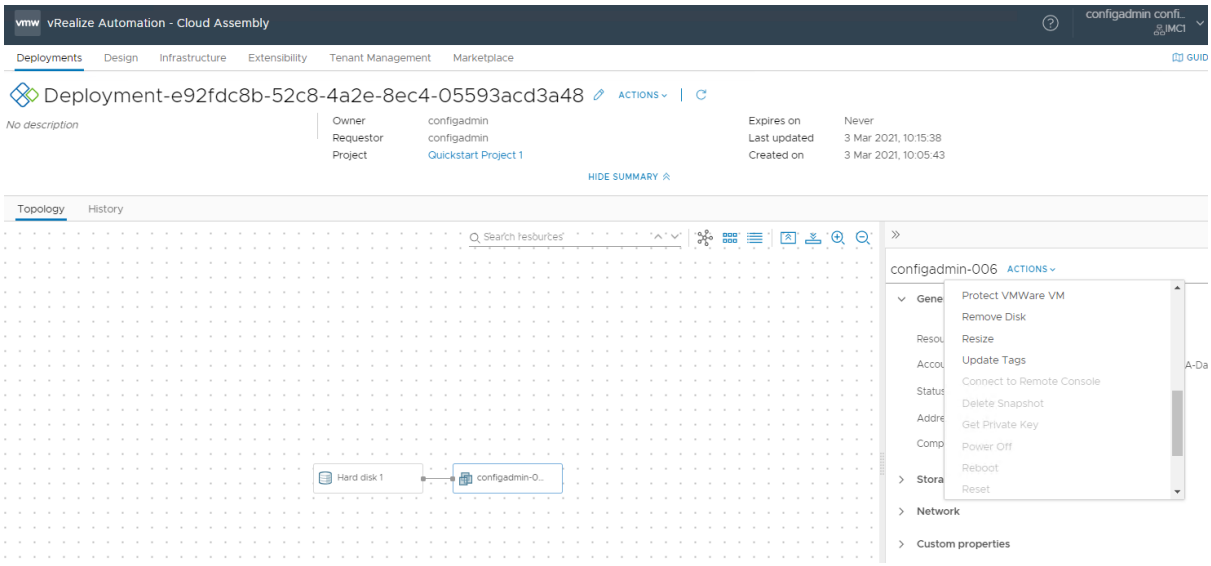
Resource actions are created using Cloud Assembly, from the Design, Resource Actions menu item.

This is an example how to create a Resource action to add protection for a VMware VM:

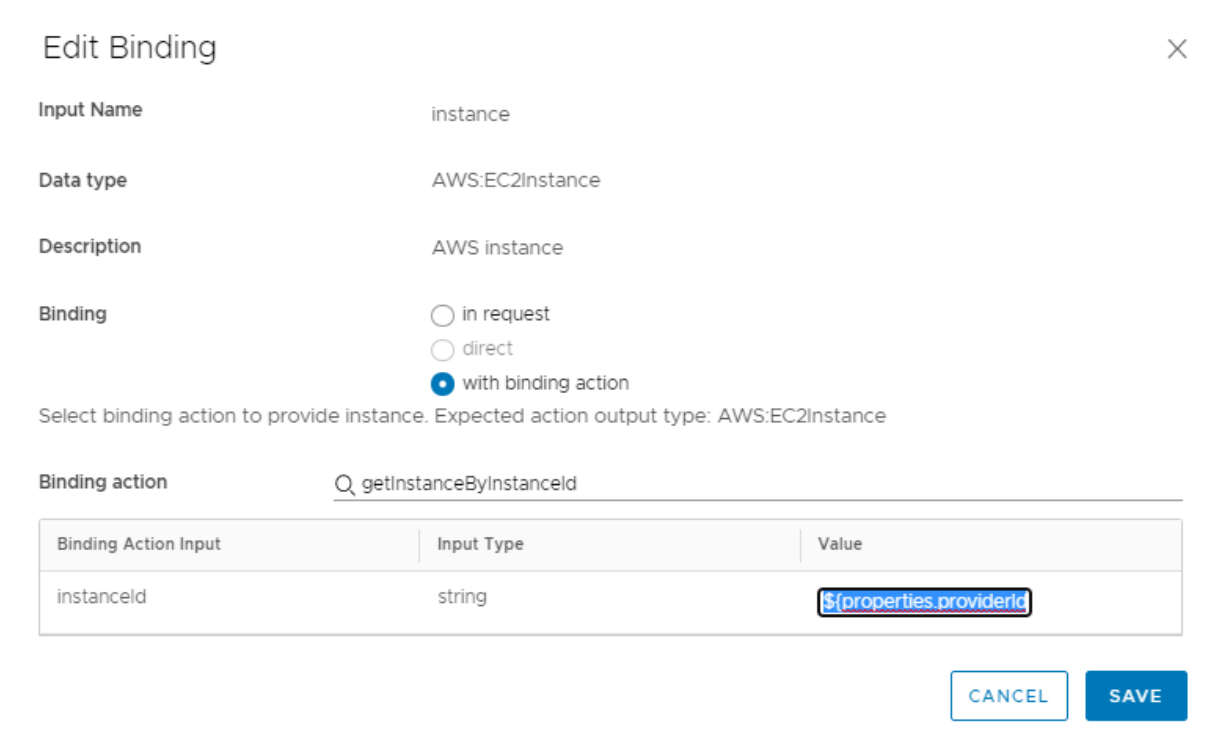


Resource type must be set to Cloud.vSphere.Machine, select the "Protect VMware VM with NetBackup" workflow, in property bindings set the vm binding to "with binding action". It will automatically select the findVcVmByVcAndVmUuid action and set the appropriate properties.

The new resource action will be available to all deployed components of type Cloud.vSphere.Machine



Configuration for AWS instances is similar, apart from the Resource Type is Cloud.AWS.EC2.Instance, the property binding for the instance should use the action named getInstanceByInstanceId and the action input Value property should be set to ${properties.providerId}



For AWS volumes the Resource Type is Cloud.AWS.Volume and the property binding for the volume should use the action named getVolumeByVolumeId and the action input Value property should be ${properties.providerId}

8. Upgrading a Backup Server

After upgrading a NetBackup™ backup server, it is important to run the "configure backup server" workflow again. As well as checking that endpoints / credentials are still valid it also updates some other configuration data.

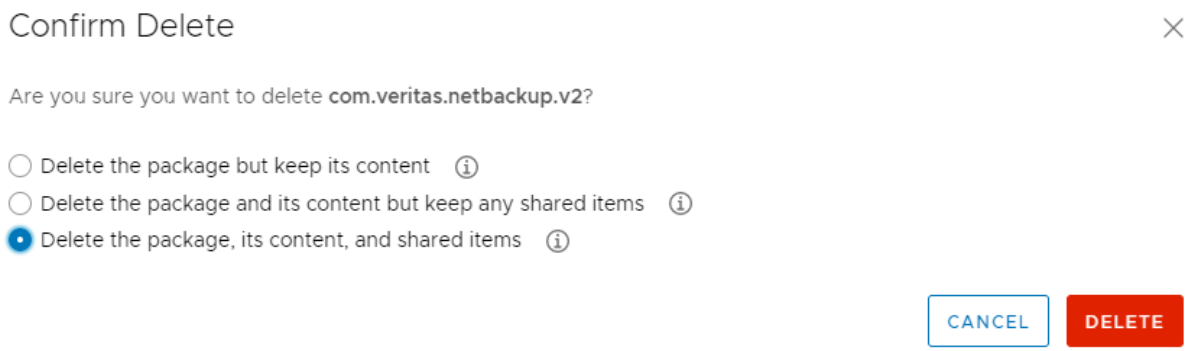
Any backup server mappings will be preserved.

9. Upgrading the plug-in

Due to major changes in vRO/vRA there is no upgrade path from versions v1.0 / v1.1 of the plugin, if old versions exist after an upgrade, they should be uninstalled (see section 10) before installing v2.0

10. Uninstalling the Plug-in

The plug-in can be removed by deleting the com.veritas.netbackup.v2 package, selecting the "Delete the package, its content, and shared items" option as below:



After the package has been deleted there may still be empty folder structures, these can be deleted (see section 4 for locations of all installed items).

11. Troubleshooting

11.1 Backup Server Connectivity and Authentication

All workflows require access to the NetBackup™ API and, for each defined Backup Server, credentials to an account with the Manage NetBackup™ permission.

The Configuration Check workflow checks all required connections as well as the supplied credentials and mappings. It also lists registered vCenters and installed AWS plug-ins.

If problems persist connecting to a backup server, check the NetBackup™ logs. Details of how to do this can be found in the Web UI Security Administrator's Guide (https://www.veritas.com/content/support/en_US/doc/135031700-135031704-0/index).

11.2 Mappings

The Mapping Rules may not contain certain permutations of a VM's properties.

The "Display VM properties" workflow allows the discovery of a VM's properties that the Mapping Rules may use.

You are advised to use a default rule to ensure that rules always return a valid backup server instance.

11.3 Errors

Any errors are displayed to the end-user in the format "There has been an error - please notify support". Errors are logged as normal in vRO as "NetBackup Error:" along with the error message. A vRO administrator can examine the relevant workflow and see the full error in the workflow logs via the vRO Control Center. You can access this by browsing to https://<vroserveraddress>:<port>/vco-controlcenter, then selecting *Export Logs* or *Live Log Stream*).