Veritas NetBackup™ plug-in for VMware vRealize™ 1.0

Installation and Configuration Guide

Last Updated: March 18, 2020

Contents

1. INTRODUCTION

This document describes the installation and configuration of the Veritas NetBackup™ plug-in for VMware vRealize™ 1.0. 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, Amazon Web Services (AWS) VM, and AWS Volume.
- Unprotect VMware VM, AWS VM, and AWS Volume
- Restore VMware VM, AWS VM, and AWS Volume
- Agentless VMware file restore
- Backup Now for VMware VM, Backup Now for AWS VM, and Backup Now for AWS Volume. The Backup Now feature requires NetBackup™ 8.2

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

Note: the processes and screen shots below refer to the Java-based vRO client.

2. PREREQUISITES

The plug-in has been developed with vRealize™ Orchestrator (vRO) 7.5 and 7.6. The plug-in supports NetBackup™ 8.1.2 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™ master server. Please refer to the NetBackup™ documentation.

Authentication for NetBackup™ 8.2 master servers support 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 1.1.0.

3. Design Considerations

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

The plug-in also supports the ability to define different credentials for a master 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 master server connection entries to the same Master 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 master 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.

The plug-in includes the following Actions which provide information on the protection status of a selected asset:

- For VMware assets: *getProtectionInformation*
- For AWS assets: *getProtectionInformationForVolume* and *getProtectionInformationForInstance*

These actions can be included in vRealize Automation custom forms to enable a user to make an informed decision when they protect an asset.

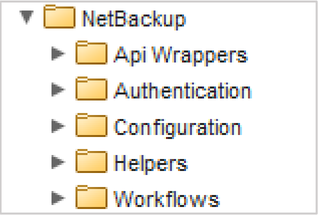
4. Installation

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. Select Design mode from the drop-list. This option can be found on the top left of the screen.
3. Click on the Packages tab. Import all contents from *com.veritas.netbackup.v1.package*

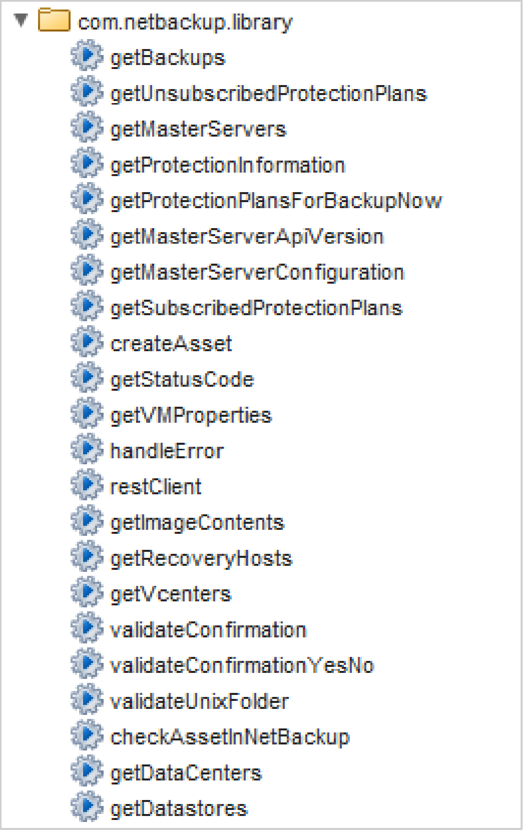
Once the import completes, you see new folders in Workflow, Actions, Configuration, and Resources tabs.

In the Workflow tab, found in the library folder:



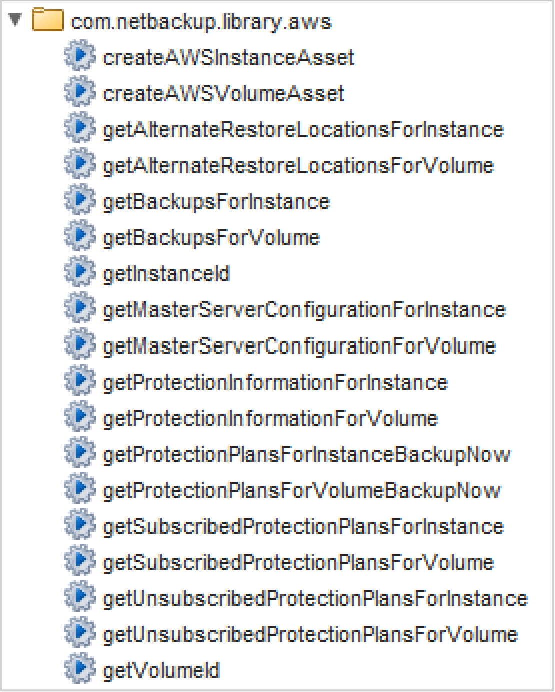
- NetBackup
  - Api Wrappers
  - Authentication
  - Configuration
  - Helpers
  - Workflows

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



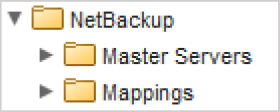
- com.netbackup.library
  - getBackups
  - getUnsubscribedProtectionPlans
  - getMasterServers
  - getProtectionInformation
  - getProtectionPlansForBackupNow
  - getMasterServerApiVersion
  - getMasterServerConfiguration
  - getSubscribedProtectionPlans
  - createAsset
  - getStatusCode
  - getVMProperties
  - handleError
  - restClient
  - getImageContents
  - getRecoveryHosts
  - getVcenters
  - validateConfirmation
  - validateConfirmationYesNo
  - validateUnixFolder
  - checkAssetInNetBackup
  - getDataCenters
  - getDatastores

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



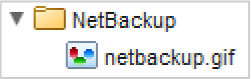
- com.netbackup.library.aws
  - createAWSInstanceAsset
  - createAWSVolumeAsset
  - getAlternateRestoreLocationsForInstance
  - getAlternateRestoreLocationsForVolume
  - getBackupsForInstance
  - getBackupsForVolume
  - getInstanceId
  - getMasterServerConfigurationForInstance
  - getMasterServerConfigurationForVolume
  - getProtectionInformationForInstance
  - getProtectionInformationForVolume
  - getProtectionPlansForInstanceBackupNow
  - getProtectionPlansForVolumeBackupNow
  - getSubscribedProtectionPlansForInstance
  - getSubscribedProtectionPlansForVolume
  - getUnsubscribedProtectionPlansForInstance
  - getUnsubscribedProtectionPlansForVolume
  - getVolumeId

In the Configuration tab, found in the library folder:



- NetBackup
  - Master Servers
  - Mappings

In the Resources area:



- NetBackup
  - netbackup.gif

5. Configuration

5.1 Master Server

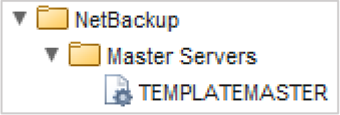
The plug-in requires a NetBackup™ user account that has the *Backup Administrator* role.

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

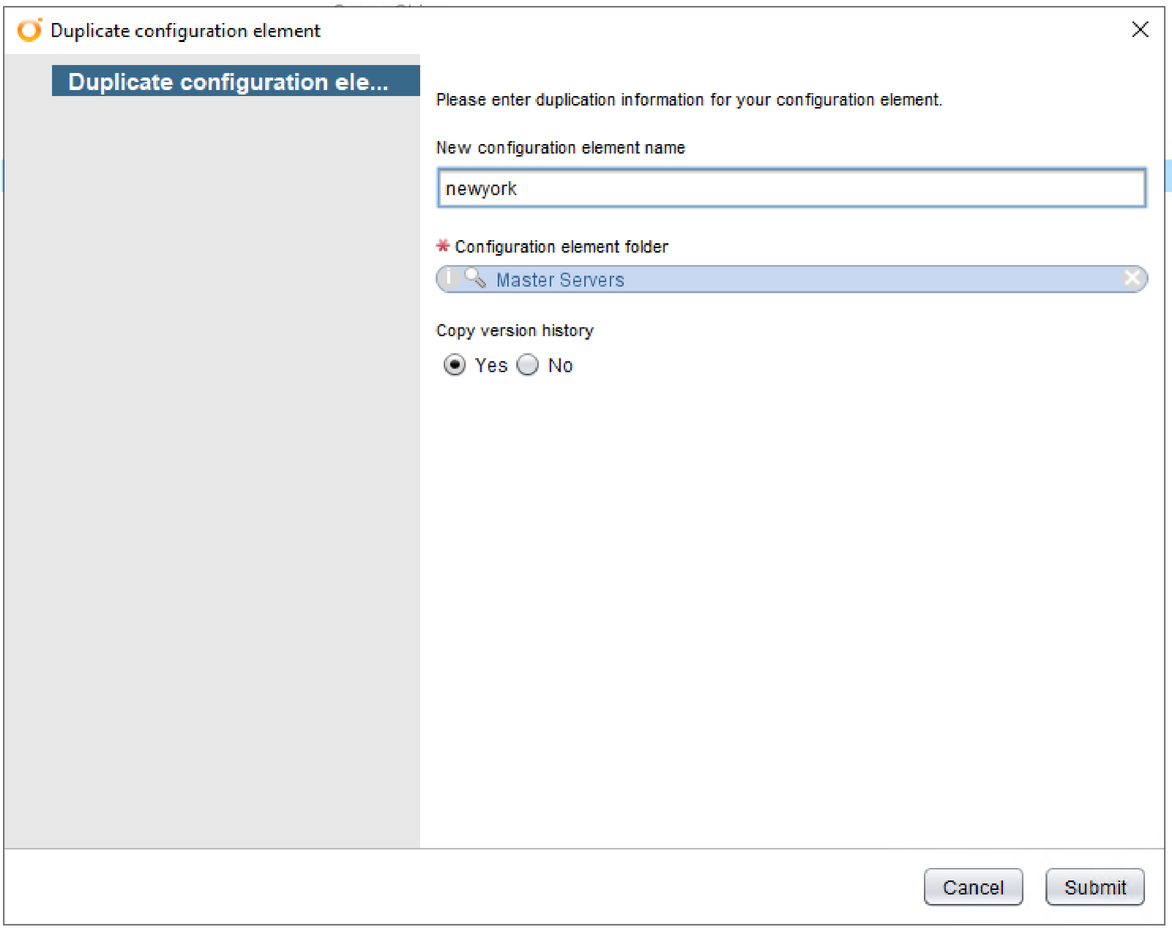
- User ID and password. This option is supported in NetBackup™ 8.1.2 and NetBackup™ 8.2.
- User ID and API Key. This option is only supported in NetBackup™ 8.2 and is recommended.

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 master 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 Master Servers subfolder.



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


Duplicate configuration element
Duplicate configuration ele...
Cancel
Submit

Please enter duplication information for your configuration element.

New configuration element name

newyork

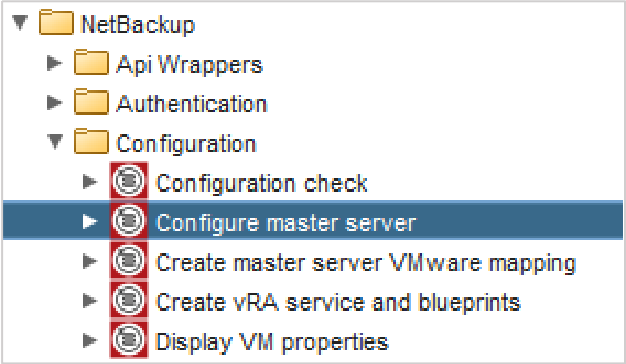
* Configuration element folder

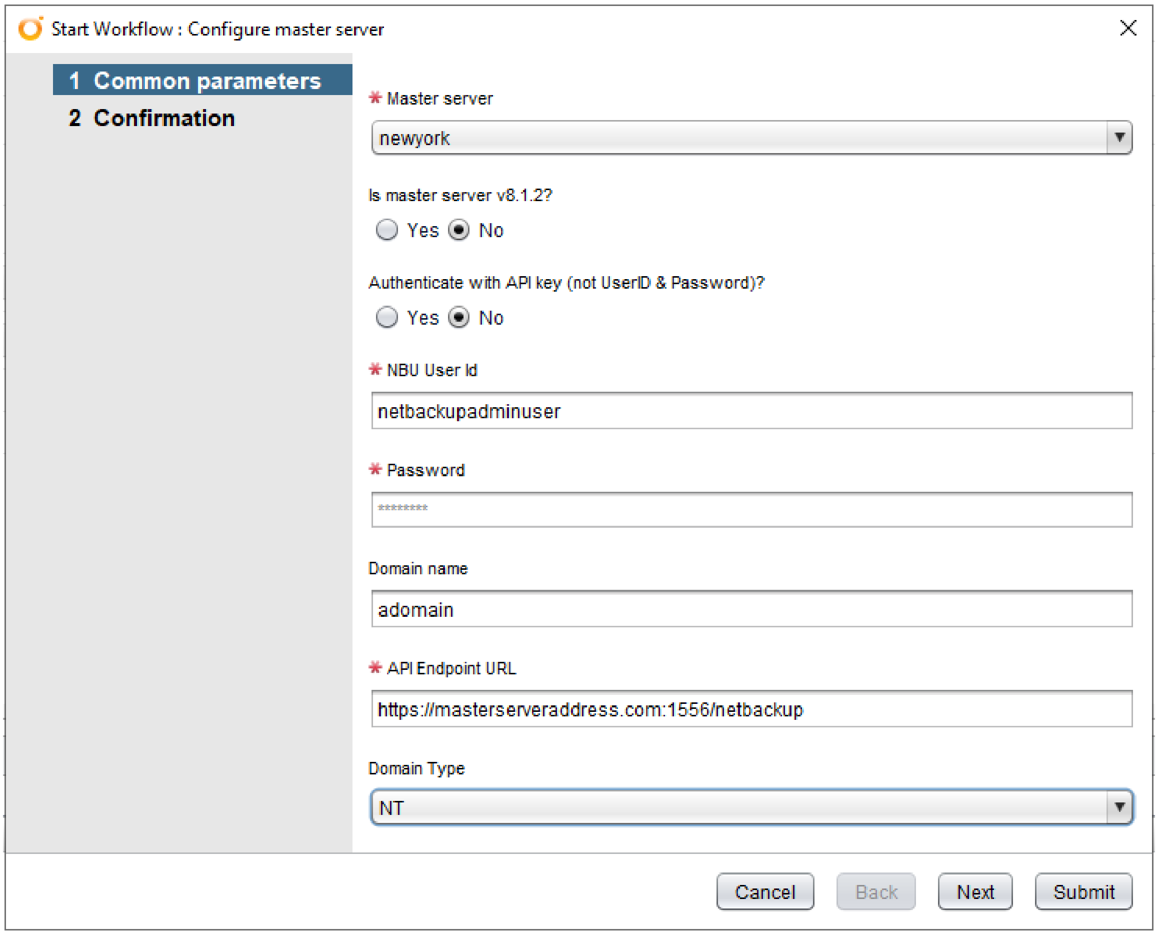
Master Servers

Copy version history

● Yes ○ No

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




Start Workflow : Configure master server

1 Common parameters
2 Confirmation

* Master server: newyork

Is master server v8.1.2? ○ Yes ● No

Authenticate with API key (not UserID & Password)? ○ Yes ● No

* NBU User Id: netbackupadminuser

* Password: ********

Domain name: adomain

* API Endpoint URL: https://masterserveraddress.com:1556/netbackup

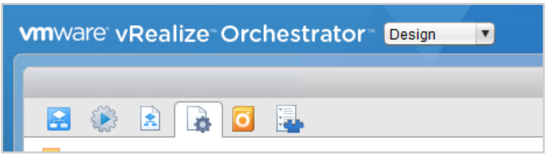
Domain Type: NT

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

On submission, the workflow updates the master server's configuration and runs a 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 master 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 master server. The following two sections explain this principle in detail.

Note: you must use lowercase letters for your folder names.

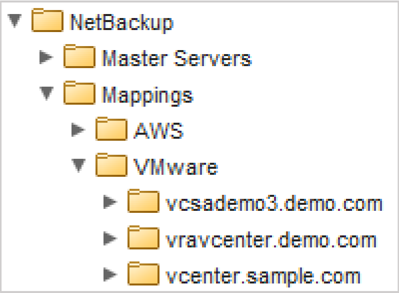
5.3.1 VMware

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

- vCenter Instance
  - Datacenter
    - Resource Pool

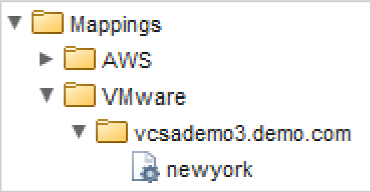
You can map to a master server at any level. You should create one mapping at vCenter level, to act as a default. This configuration can be helpful where lower-level mappings do not match all the assets in the asset base.

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:



- NetBackup
  - Master Servers
  - Mappings
    - AWS
    - VMware
      - vcsademo3.demo.com
      - vravcenter.demo.com
      - vcenter.sample.com

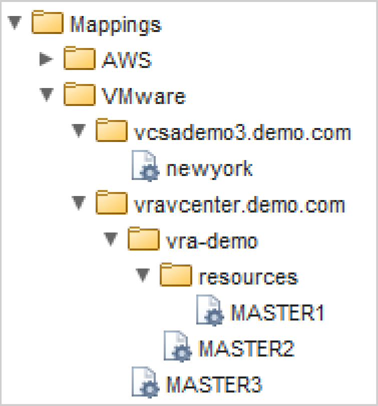
The first vCenter instance uses only a vCenter level mapping:



- Mappings
  - AWS
  - VMware
    - vcsademo3.demo.com
      - newyork

This example shows that the Master Server configured as *newyork* manages any VMware VM from this vCenter.

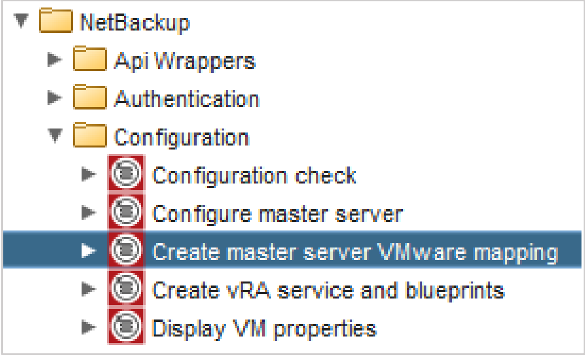
The second mapping includes mappings at different levels:



- Mappings
  - AWS
  - VMware
    - vcsademo3.demo.com
      - newyork
    - vravcenter.demo.com
      - vra-demo
        - resources
          - MASTER1
        - MASTER2
      - MASTER3

In this example, if a VM belongs to the resource pool *resources* in the datacenter *vra-demo*, the master server 'MASTER1' manages it. A VM in the same datacenter, but in a different resource pool, is assigned to master server 'MASTER2'. The 'MASTER3' server manages all other VMs for vCenter *vravcenter.demo.com* that the previous two rules do not cover.

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

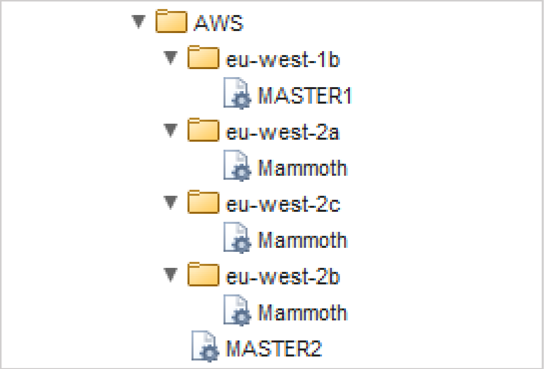


- NetBackup
  - Api Wrappers
  - Authentication
  - Configuration
    - Configuration check
    - Configure master server
    - Create master server VMware mapping
    - Create vRA service and blueprints
    - Display VM properties

5.3.2 AWS

The AWS mappings let you specify a master 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:



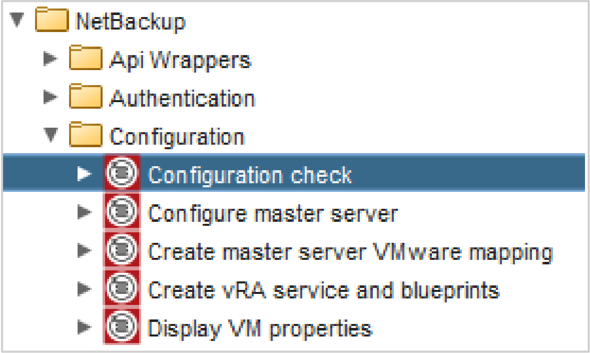
- AWS
  - eu-west-1b
    - MASTER1
  - eu-west-2a
    - Mammoth
  - eu-west-2c
    - Mammoth
  - eu-west-2b
    - Mammoth
  - MASTER2

In this example, the master server ‘MASTER2’ manages any AWS VM or volume that does not belong to any of the AWS regions listed.

The master server ‘MASTER1’ manages a VM or volume from AWS region *eu-west-1b*.

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 master servers. For each master server it also checks the existence of Protection Plans for the different asset classes. This process requires the master server to be included in any mappings.

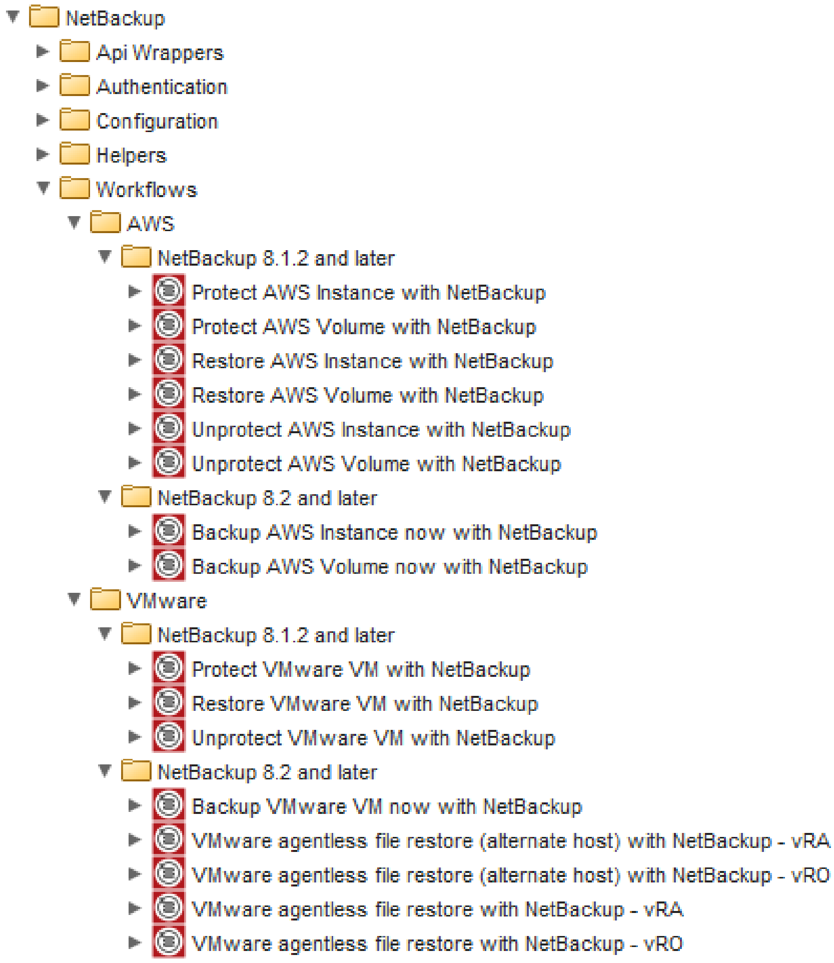
Sample output for a single master check:

```
[2019-05-20 15:24:10.668] [I] Checking master server configuration: MASTER1

[2019-05-20 15:24:11.408] [I] Master server: MASTER1 - Import Certificate - PASS

[2019-05-20 15:24:11.725] [I] Master server: MASTER1 - Ping check - PASS (Mon May 20 2019 14:25:08 GMT-0000 (UTC))

[2019-05-20 15:24:12.076] [I] Master server: MASTER1 - Token check - PASS

[2019-05-20 15:24:12.716] [I] Found vCenter: vravcenter.demo.com

[2019-05-20 15:24:12.726] [I] Found mapping configuration for master server: MASTER1

[2019-05-20 15:24:12.729] [I] Found vCenter: demovc1.demo.com

[2019-05-20 15:24:12.733] [E] No mapping configurations found

[2019-05-20 15:24:12.737] [I] Found vCenter: 10.11.248.180

[2019-05-20 15:24:12.743] [E] No mapping configurations found

[2019-05-20 15:24:12.747] [I] Found vCenter: 10.11.248.102

[2019-05-20 15:24:12.756] [E] No mapping configurations found

[2019-05-20 15:24:12.760] [I] Found vCenter: demovcd1.demo.com

[2019-05-20 15:24:12.770] [E] No mapping configurations found

[2019-05-20 15:24:13.342] [I] Found VMware protection plan: Medium Protection

[2019-05-20 15:24:13.343] [I] Found VMware protection plan: High Protection

[2019-05-20 15:24:13.344] [I] Found VMware protection plan: Backup Now

[2019-05-20 15:24:14.372] [I] Found AWS plugin: CLOWAS

[2019-05-20 15:24:14.378] [I] Found 4 AWS master server mappings

[2019-05-20 15:24:14.827] [I] Found cloud protection plan: Weekly Backups - Cloud

[2019-05-20 15:24:14.828] [I] Found cloud protection plan: Cloud Backup Now
```

This workflow is run every time a new master 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 both VMware and AWS asset classes, with sub folders for the relevant NetBackup version (see below).



- NetBackup
  - Api Wrappers
  - Authentication
  - Configuration
  - Helpers
  - Workflows
    - AWS
      - NetBackup 8.1.2 and later
        - Protect AWS Instance with NetBackup
        - Protect AWS Volume with NetBackup
        - Restore AWS Instance with NetBackup
        - Restore AWS Volume with NetBackup
        - Unprotect AWS Instance with NetBackup
        - Unprotect AWS Volume with NetBackup
      - NetBackup 8.2 and later
        - Backup AWS Instance now with NetBackup
        - Backup AWS Volume now with NetBackup
    - VMware
      - NetBackup 8.1.2 and later
        - Protect VMware VM with NetBackup
        - Restore VMware VM with NetBackup
        - Unprotect VMware VM with NetBackup
      - NetBackup 8.2 and later
        - Backup VMware VM now with NetBackup
        - VMware agentless file restore (alternate host) with NetBackup - vRA
        - VMware agentless file restore (alternate host) with NetBackup - vRO
        - VMware agentless file restore with NetBackup - vRA
        - VMware agentless file restore with NetBackup - vRO

6.1 VMware Workflows

The operations that are supported are:

- Protect VM
- Unprotect VM
- Restore VM. This option restores the VM to the original location, with the option to rename the restored VM

For version 8.2+ master servers, the following operations are also supported:

- Backup Now
- Agentless file restore to original host (vRA and VRO versions to cater for UX variances)
- Agentless file restore to alternate host (vRA and VRO versions to cater for UX variances)

Protection and Backup Now require NetBackup™ VMware Protection Plans.

6.2 AWS Workflows

The operations that are supported include:

- Protect Instance
  - Subscribe instance to a Protection Plan
- Unprotect Instance
  - Unsubscribe instance from a Protection Plan
- Protect Volume
  - Subscribe volume to a Protection Plan
- Unprotect Volume
  - Unsubscribe volume from a Protection Plan
- 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

For version 8.2+ master servers the following operations are also available:

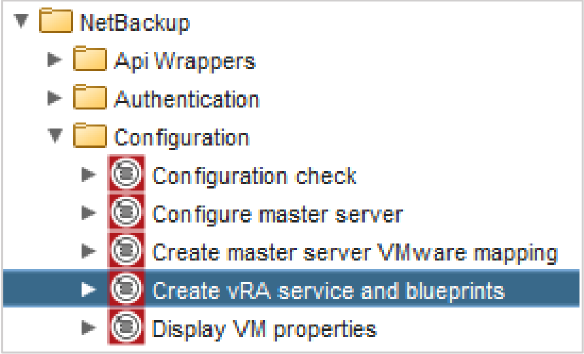
- Backup Instance Now
  - Subscribe instance to a Protection Plan for an immediate backup. Remove subscription once backup completes.
- Backup Volume Now
  - Subscribe volume to a Protection Plan for an immediate backup. Remove subscription once backup completes.

Protection and Backup Now require NetBackup™ Cloud Protection Plans.

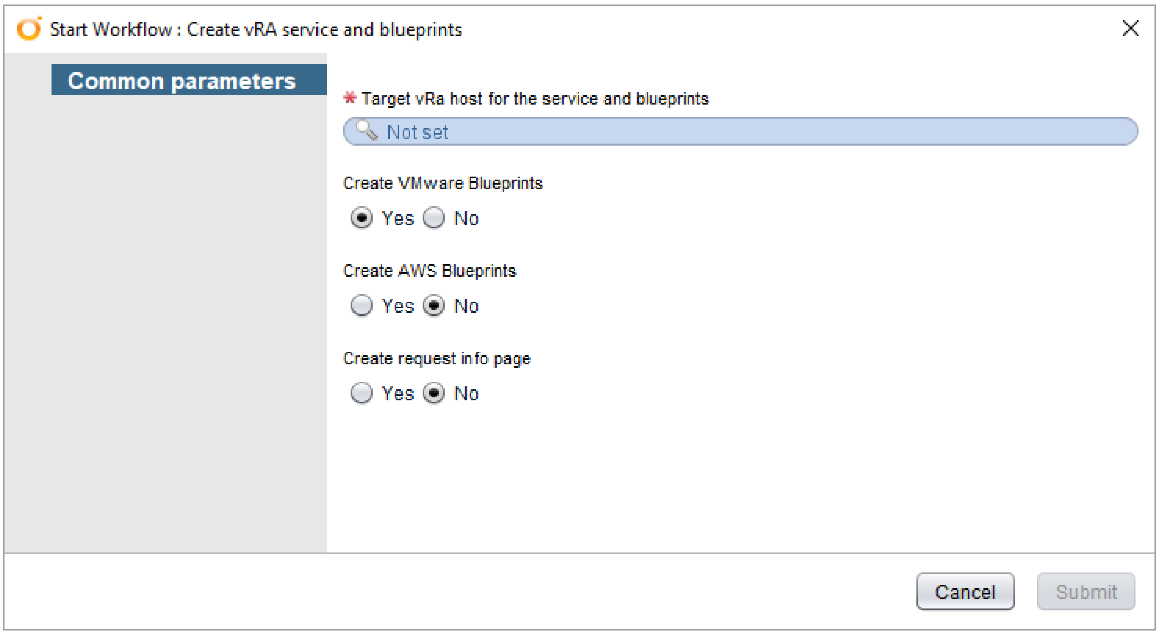
7. vRealize Automation

vRealize™ Automation (vRA) provides a portal that enables an end-user to request a variety of services. You can convert the plug-in's operational workflows to vRA XaaS Blueprints or Resource Actions.

The workflow *Create vRA service and blueprints* generates a new vRA service named "Veritas NetBackup", and a Catalog Item for each operational workflow.



The workflow allows the administrator to select the target vRA instance, and choose the relevant workflows corresponding to the main asset classes.



Start Workflow : Create vRA service and blueprints

Common parameters

* Target vRa host for the service and blueprints

Not set

Create VMware Blueprints

● Yes ○ No

Create AWS Blueprints

○ Yes ● No

Create request info page

○ Yes ● No

By default, the VMware blueprint creation is enabled, and the AWS blueprint creation is disabled. The “request info” page refers to an optional additional page that could be presented to users when raising a service request in vRA. This page has no relevance to NetBackup™.

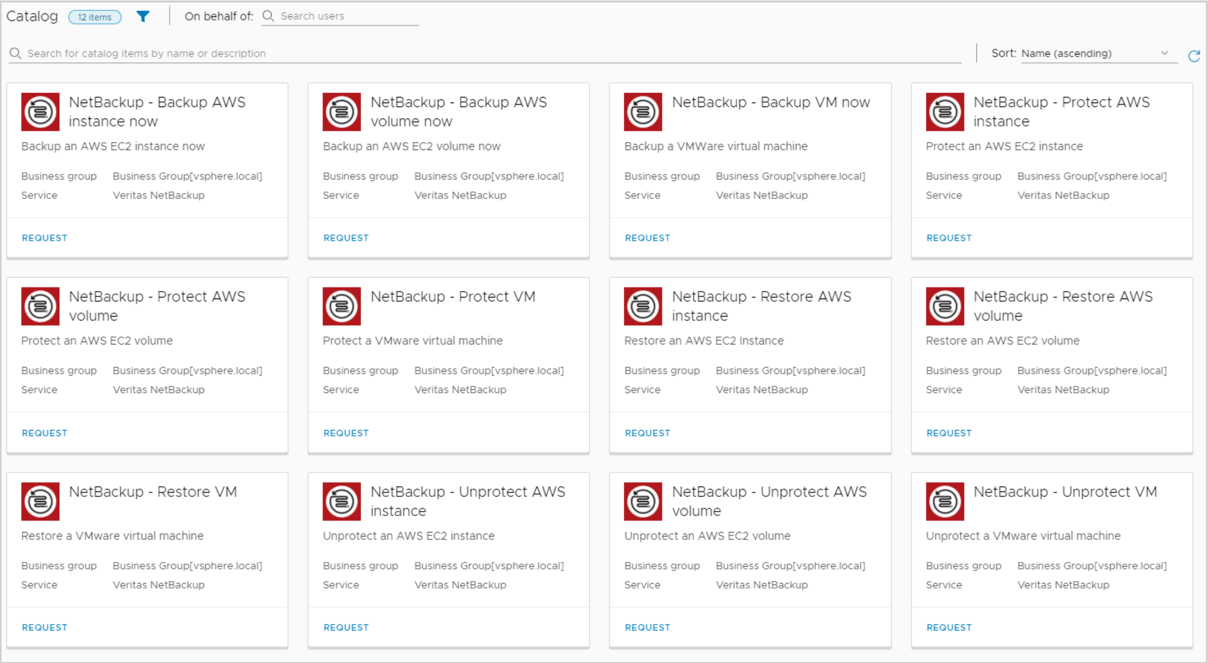
All the actions appear in the Log:

```
[2019-05-20 14:39:08.593] [I] Creating a service: Veritas NetBackup...

[2019-05-20 14:39:08.655] [I] Service: Veritas NetBackup created.

[2019-05-20 14:39:09.443] [I] Created service blueprint NetBackup - Protect VM.

[2019-05-20 14:39:09.882] [I] Created service blueprint NetBackup - Restore VM.

[2019-05-20 14:39:10.245] [I] Created service blueprint NetBackup - Unprotect VM.

[2019-05-20 14:39:10.628] [I] Created service blueprint NetBackup - Backup VM now.

[2019-05-20 14:39:10.630] [I] Created service blueprint NetBackup - VM file restore (alternate host).

[2019-05-20 14:39:10.632] [I] Created service blueprint NetBackup - VM file restore (original host).

[2019-05-20 14:39:11.058] [I] Created service blueprint NetBackup - Protect AWS instance.

[2019-05-20 14:39:11.987] [I] Created service blueprint NetBackup - Protect AWS volume.

[2019-05-20 14:39:12.588] [I] Created service blueprint NetBackup - Restore AWS instance.

[2019-05-20 14:39:13.054] [I] Created service blueprint NetBackup - Restore AWS volume.

[2019-05-20 14:39:13.528] [I] Created service blueprint NetBackup - Unprotect AWS instance.

[2019-05-20 14:39:14.086] [I] Created service blueprint NetBackup - Unprotect AWS volume.

[2019-05-20 14:39:14.702] [I] Created service blueprint NetBackup - Backup AWS instance now.

[2019-05-20 14:39:15.169] [I] Created service blueprint NetBackup - Backup AWS volume now.

[2019-05-20 14:39:15.386] [I] Added NetBackup - Protect AWS volume to service

[2019-05-20 14:39:15.470] [I] Added NetBackup - Restore AWS instance to service
```

```
[2019-05-20 14:39:15.526] [I] Added NetBackup - Unprotect VM to service

[2019-05-20 14:39:15.598] [I] Added NetBackup - Backup VM now to service

[2019-05-20 14:39:15.671] [I] Added NetBackup - Unprotect AWS volume to service

[2019-05-20 14:39:15.775] [I] Added NetBackup - Protect VM to service

[2019-05-20 14:39:15.862] [I] Added NetBackup - Restore VM to service

[2019-05-20 14:39:15.987] [I] Added NetBackup - Protect AWS instance to service

[2019-05-20 14:39:16.048] [I] Added NetBackup - Restore AWS volume to service

[2019-05-20 14:39:16.127] [I] Added NetBackup - Unprotect AWS instance to service

[2019-05-20 14:39:16.192] [I] Added NetBackup - Backup AWS instance now to service

[2019-05-20 14:39:16.266] [I] Added NetBackup - Backup AWS volume now to service

[2019-05-20 14:39:16.270] [I] Added NetBackup - VM file restore (alternate host) to service

[2019-05-20 14:39:16.275] [I] Added NetBackup - VM file restore (original host) to service
```

In this example both VMware and AWS blueprints were created.

Once the workflow completes, you must add the new service to the appropriate entitlements. After the entitlements are configured it is visible in the catalog:



Catalog 12 items

On behalf of: Search users

Search for catalog items by name or description

Sort: Name (ascending)

NetBackup - Backup AWS instance now
Backup an AWS EC2 instance now
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Backup AWS volume now
Backup an AWS EC2 volume now
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Backup VM now
Backup a VMWare virtual machine
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Protect AWS instance
Protect an AWS EC2 instance
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Protect AWS volume
Protect an AWS EC2 volume
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Protect VM
Protect a VMware virtual machine
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Restore AWS instance
Restore an AWS EC2 Instance
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Restore AWS volume
Restore an AWS EC2 volume
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Restore VM
Restore a VMware virtual machine
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Unprotect AWS instance
Unprotect an AWS EC2 instance
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Unprotect AWS volume
Unprotect an AWS EC2 volume
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

NetBackup - Unprotect VM
Unprotect a VMware virtual machine
Business group Business Group[vsphere.local]
Service Veritas NetBackup
REQUEST

8. Upgrading a 8.1.2 Master Server

After upgrading a NetBackup™ master server from 8.1.2, it's important to run the "configure master server" workflow again and modify the version attribute. This ensures the correct workflows are used to take advantage of the latest API changes within NetBackup™ 8.2.

Any master server mappings will be preserved.

9. Uninstalling the Plug-in

The plug-in can be removed by deleting all the sections that were created during the installation process. Make sure that you have the “Delete non-empty folder permitted” option enabled. This option can be found in vRO Tools/User preferences.

10. Troubleshooting

9.1 Master Server Connectivity and Authentication

All workflows require access to the NetBackup™ API and, for each defined Master 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 master 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).

9.2 Mappings

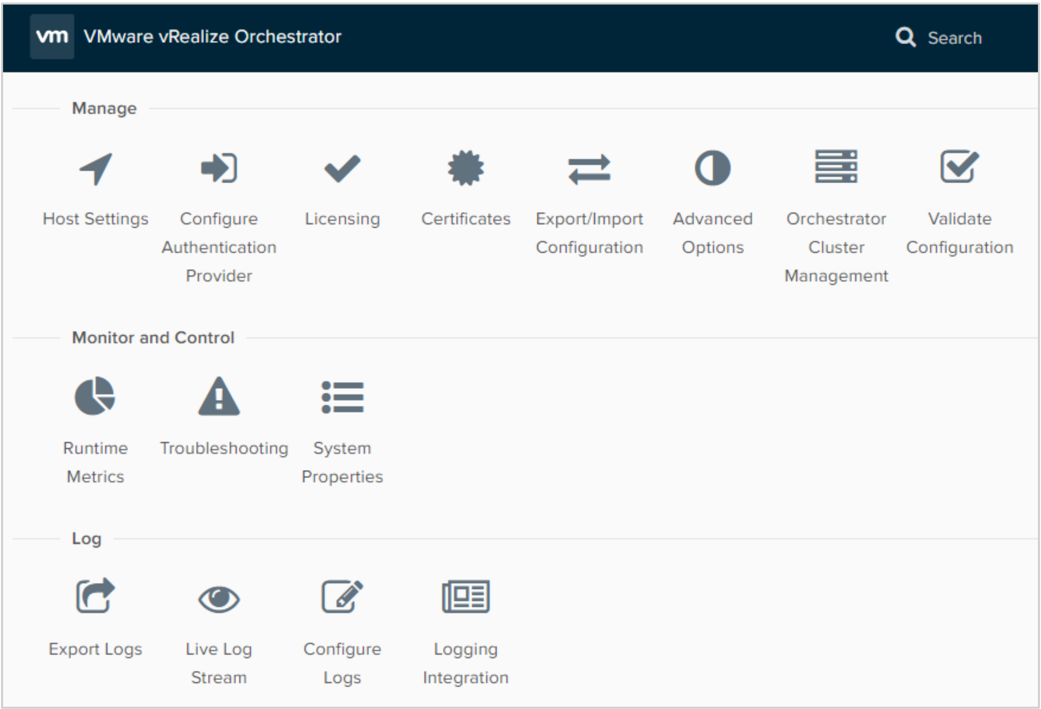
The Mapping Rules may not contain certain permutations of a VM’s properties.

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 master server instance.

9.3 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*).


VMware vRealize Orchestrator
Search
Manage
Host Settings
Configure Authentication Provider
Licensing
Certificates
Export/Import Configuration
Advanced Options
Orchestrator Cluster Management
Validate Configuration
Monitor and Control
Runtime Metrics
Troubleshooting
System Properties
Log
Export Logs
Live Log Stream
Configure Logs
Logging Integration