ServiceNow™ app 1.0 for Veritas NetBackup™

Installation and Configuration Guide

Last Updated: March 18, 2020

1. Introduction 3
2. Prerequisites 3
3. Required Skills and Access 3
4. Installation 4
Minimum NetBackup™ Configuration 4
Installation Instructions 5
5. Design Considerations 5
6. Configuration 6
Setup Sequence 6
Configuring NetBackup™ 6
Protection Plans 7
RBAC Object Groups 7
NetBackup™ User Accounts 7
Access Rules 7
Configuring ServiceNow™ 7
NetBackup™ Properties 7
Setting up Authorization Records 8
7. ServiceNow™ Service Catalog 9

1. Introduction

The ServiceNow™ app for NetBackup™ enables the protection of cloud and VMware workloads from within the ServiceNow™ user interface. The app communicates directly to one or more NetBackup™ master servers using the NetBackup™ REST API.

The app includes the service catalog items which administrators can make available to their end-users in ServiceNow™.

The following services are provided:

- Protect VMware VM, Amazon Web Services (AWS) VM, Azure VM, and Google cloud VM.
- Unprotect VMware VM, Amazon Web Services (AWS) VM, Azure VM, and Google cloud VM.
- Restore VMware VM, Amazon Web Services (AWS) VM, Azure VM, and Google cloud VM.

This document describes the installation and configuration of the ServiceNow™ app for NetBackup™.

2. Prerequisites

The prerequisites for using the ServiceNow app are:

- NetBackup™ 8.2+
- ServiceNow™ “Madrid” or “New York”

The NetBackup™ REST API must be accessible by ServiceNow™.

Protection functionality requires the definition of protection plans for the relevant asset classes within NetBackup™. You must perform this action through the NetBackup™ web UI.

Authentication for NetBackup™ 8.2 supports API key.

3. Required Skills and Access

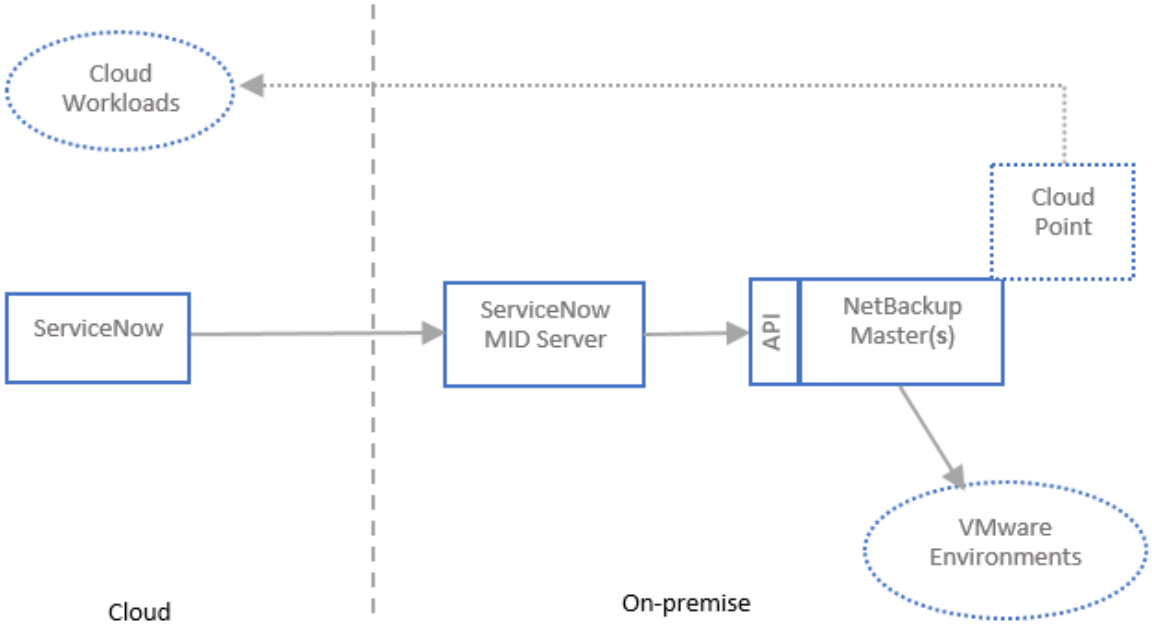
The person who installs the ServiceNow™ app needs the appropriate level of permissions: these permissions should include the ability to access the update set and configure the required user and authorization records.

This person needs to work with a NetBackup™ Administrator, to ensure the initial data set up in NetBackup™ is correct. This data setup includes user and service accounts, RBAC, asset, and protection plans.

Operating system user accounts are required for NetBackup™ user accounts created and used in the configuration process.

4. INSTALLATION

The diagram shows the architecture between ServiceNow™, NetBackup™, and the protected cloud workloads.



MINIMUM NETBACKUP™ CONFIGURATION

The ServiceNow™ app requires:

- At least one master server.
- At least one protection plan.
- VMware and, or, cloud endpoints defined.
- At least one NetBackup™ account, with corresponding operating system account. The ServiceNow™ app uses this account.

ServiceNow™ uses a MID server to access the NetBackup™ REST API. If the NetBackup™ REST API is internet facing, then a MID server is not required. You must use a valid SSL certificate.

For each master server, the NetBackup™ administrator must provide the following:

- The master server API endpoint for example https://[masterServer.company.com]:1556.
- User credentials.

The NetBackup™ API offers two methods for authentication:

User name and API key, or

User name and password.

Veritas recommend that you use the API key method. The account's API key is created using the NetBackup™ web UI.

INSTALLATION INSTRUCTIONS

The ServiceNow™ app is installed by using an update set, named *netbackupIntegration.xml*. You should import it into your ServiceNow™ instance and commit the set.

During the preview phase, you may see one or more errors. Errors normally occur due to data linking not being performed correctly in the preview stage. Select the *Accept remote update* link to rectify.

Once the action completes, search for "NetBackup" to find the application you have installed.

5. DESIGN CONSIDERATIONS

The app uses NetBackup™ RBAC to provide asset and protection plan visibility. The app lets you link a NetBackup™ account record to one or more ServiceNow User Groups.

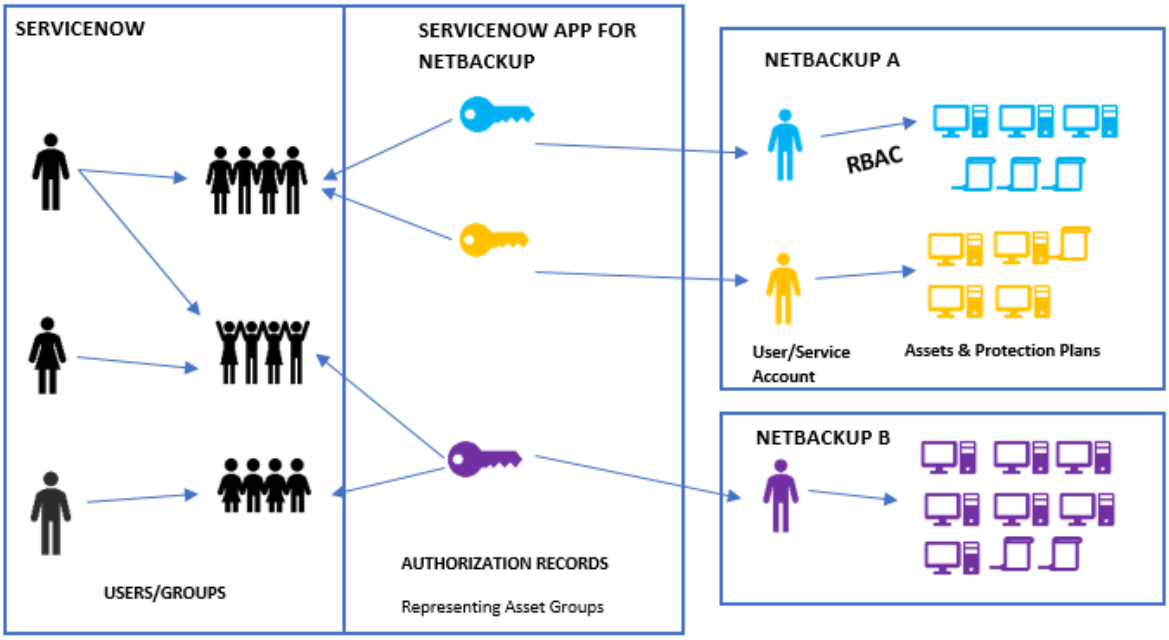
Before you begin the ServiceNow™ app configuration it is important that you configure NetBackup™.

In NetBackup™, an asset group is represented as a combination of a NetBackup™ user or group, and an RBAC object group. You should configure each asset group to be managed from ServiceNow™ to reflect the access rights of ServiceNow™ user groups.

In ServiceNow™, the app allows the creation and configuration of one or more authorization records. These records each represent the asset group where the target master server and the associated user credentials are stored within ServiceNow™. You can link these authorization records to one or more ServiceNow™ user groups.

The design needs to define ServiceNow™ User groups, NetBackup™ asset groups, and the mapping between them.

The diagram shows an example of the relationship between ServiceNow™ users, user groups and Authorization records, and NetBackup™ users, assets, and protection plans.



6. Configuration

Setup Sequence

The actions you must take in NetBackup™ are:

- Create one or more protection plans.
- Create one or more RBAC object groups.
- Create an access rule to associate object groups to the user accounts you want to use.

The actions you must take in ServiceNow™ are:

- Create an authorization record and link the group authorization to a ServiceNow™ user group.

Authorization records define a master server and the relevant credentials. Group authorizations link authorization records to ServiceNow™ user groups.

Configuring NetBackup™

The ServiceNow™ app protects VMware and cloud assets. You must register the relevant endpoints within NetBackup™. You should follow the steps that are listed to ensure correct setup and minimal issues.

The app leverages NetBackup™ protection plans to protect assets. You must therefore create protection plans for the supported asset classes.

You must create the account ServiceNow™ uses within NetBackup™. This account needs access to the relevant assets and protection plans. Once this account is created, you should create an API key for the account.

You can use multiple master servers, and multiple accounts per server.

The term asset group represents all object groups that a NetBackup™ user account has access to.

The NetBackup™ and ServiceNow™ administrator must work together to define the content of the asset group.

For example, the ServiceNow™ administrator wants to allow all North American ServiceNow™ user groups access to North American VMware assets.

1. The NetBackup™ administrator creates an RBAC object group that includes all North American assets and protection plans. The administrator also creates a NetBackup™ user account for this group, and an access rule to link the user account to the object group.
2. The ServiceNow™ administrator creates an authorization record, using the NetBackup™ user's credentials. The administrator links this record to the ServiceNow™ North American user groups.

Protection Plans

Protection is supported through the use of a protection plan. The administrator creates the relevant plans, using the NetBackup™ web UI.

RBAC Object Groups

The administrator creates an RBAC object group, using the NetBackup™ web UI. The RBAC object group represents a subset of assets and protection plans.

NetBackup™ User Accounts

The administrator creates a separate NetBackup™ user account, to represent an asset group. The credentials for each user account that is created for this purpose is used in ServiceNow™ authorization records.

The administrator creates an API key for each of the accounts that are used for ServiceNow™ integration.

Access Rules

The administrator links the NetBackup™ User Accounts to one or more object groups, using the NetBackup™ web UI.

CONFIGURING SERVICENOW™

This section guides you through the setup of the app within ServiceNow™. You are encouraged to follow the steps shown to ensure correct setup and minimal issues.

NetBackup™ Properties

By default, the app expects a MID Server to be available. The MID server should have the best possible access to the NetBackup™ API. If there are several MID servers, you may need to test which one is the most appropriate.

Enter a suitable server name for your environment. If you leave the server name blank, ServiceNow™ attempts to send the REST request directly to the service endpoint. This option is useful if you plan to expose the NetBackup™ REST API to the internet, bypassing the need for a MID server.

Setting up Authorization Records

Authorization records allow a ServiceNow™ user to access a subset of assets and protection plans. Authorization records are associated with ServiceNow™ user groups. This controls user access to an asset subset when a request such as "Protect an Asset" is created.

You must first ensure that you have correctly configured the authorization records for the application. You can find the authorization records under the menu item named "Authorization Records". Select *New* to create a new authorization record.

Item	**Details**
Name	The name that is displayed to users.
Description	Enter an additional explanation for this record.
Domain Name	The value you should enter is dependent upon the authorization scheme being used. If you use an API key, you should enter *vrts.apikey* If you use a user name and password, you should enter the NT domain name for this account.
Domain Type	The value you should enter is dependent upon the authorization scheme being used. If you use an API key, you should enter *vx* If you use a user name and password, you should enter **nt**
Content Type Version	This setting represents the version of the API that is used. For NetBackup™ 8.2, select *3.0*
Endpoint	The NetBackup™ REST API URL. For example, https://masterserver.company.com:1556
Username	The user name that is provided by the NetBackup™ administrator.
Password	The value you should enter is dependent upon the authorization scheme being used. If you use an API key, you should enter the API key. If you use a user name and password, you should enter the user name and password.

Save the record and select *Test Connection* to test the connection.

7. SERVICENOW™ SERVICE CATALOG

The app offers the following services that can be incorporated into your Service Catalog:

- Protect Asset

  A user can select one or more assets of a specific class, and subscribe to a protection plan.

- Unprotect Asset

  A user can select an asset of a specific class, and view the subscribed plans. The user can select the appropriate plan and unsubscribe.

- Restore Asset

  A user can restore an asset which has a backup image. The user selects the relevant asset and chooses a recovery point. The user can restore any asset class to the original location. Additionally, the user can restore a VMware asset to an alternative location.

  The services support both VMware and Cloud asset classes. “Cloud” encompasses assets in AWS, Azure, and Google Cloud.