GETTING STARTED WITH THE NETBACKUP SELF SERVICE API

NetBackup Self Service version 8.1

INTRODUCTION

In every NetBackup Self Service (NSS) implementation there is a requirement to provide some form of integration with the host environment.

The most common requirement is to register the infrastructure within NSS. This action protects the infrastructure. The sources for such information can vary enormously; it can be a CMDB, a cloud management platform, or even NetBackup client based policies.
Many customers have their own portal within which they wish to embed backup and restore services to NetBackup. For example, you can extend a VM provisioning portal to offer bundled protection services as you provision new infrastructure.

NetBackup Self Service along with its integral REST API provides a flexible solution for a variety of customer scenarios. NSS is well suited for customers either who want a new dedicated backup and restore portal or who want to extend their existing portal and workflow solutions.

This document introduces the capabilities of the NSS API.

GETTING STARTED

Before you can use the NSS API, you must install and configure NSS. In doing so, at least one NetBackup master server or appliance must be registered at NSS and be operational. NSS must additionally have at least one User, Tenant and Protection Type configured.

ABOUT MULTI-TENANCY

NSS is multi-tenant, allowing you to divide users and infrastructure into logical groups with associated access control. Within an Enterprise, you can configure existing business units as tenants or, where no division is required, you can configure a single all-encompassing structure.

The simplest option is to create a single "tenant" in NSS and have all backup/restore activities performed through this "tenant". You perform all activities in NSS and its REST API at tenant level, so you must configure at least one tenant.

Where you require multiple tenants, it may be desirable to integrate NSS to automate the management.

NSS infers the tenant when authenticating with the NSS API. The user's role and tenant access rights set the tenant.

All usage reporting in NSS is grouped by tenant and available via the API.

USING THE NSS API

Once NSS has been configured and tenants defined, most methods center around the machine object.

NSS needs to know about the computers (machines) in the environment under protection. With the exception of vCloud Director where NSS can automatically discover machines, for all other environments the machines need to be registered with NSS. (Additional NSS auto discovery add-ons are available, please contact your technical account representative for more information).

Where an existing machine provisioning/de-provisioning system exists, processes can typically be extended to include machine registration/deregistration in NSS. Usually an initial bulk import of existing machines is required and the information for this can be retrieved from whatever system has a record of all existing machines.

Machine registration with NSS results in the machine being given a unique id. This id is used to all subsequent calls regarding this machine.

The implementer has two options:

1. Registering the customer unique identifier with NSS in the MachineCode property
2. Store the NSS id against the machine in the customer system

NSS API methods support OData filters so to find a machine with machine code 'XYZ' the following filter can be appended to the machines REST API URL:

```
?$filter=MachineCode eq 'XYZ'
```

NSS API methods return data in JSON format and several also accept parameters in JSON. Please refer to the Swagger API browser for detailed information (see "Further Documentation" below).

Once you configure NSS and define the tenants, most methods center on the machine object.

NSS needs to know about the computers (machines) in the environment under protection. With the exception of vCloud Director where NSS can automatically discover machines, for all other environments you must register the machines with NSS. (Additional NSS auto discovery add-ons are available. Please contact your technical account representative for more information).

Where an existing machine provisioning and de-provisioning system exists, you can typically extend processes to include machine registration and deregistration in NSS. Usually an initial bulk import of existing machines is required. You can retrieve this information from whatever system has a record of all existing machines.

NSS assigns a unique ID to the machine when you register it within NSS. This ID is used to all subsequent calls regarding this machine.

The implementer has two options:

1. Registering the customer unique identifier with NSS in the MachineCode property

2. Store the NSS ID against the machine in the customer system

NSS API methods support OData filters so to find a machine with machine code 'XYZ' you can append the following filter to the machines REST API URL:

```
?$filter=MachineCode eq 'XYZ'
```

NSS API methods return data in JSON format and several methods accept parameters in JSON. Please refer to the Swagger API browser for detailed information (see "Further Documentation" below).

AUTHENTICATION

Authentication can be made using OAuth2 either passing a `User Name` and `Password`, or an `Access Key Id` and `Secret Access Key`. Either way, a valid User account is required at NSS. To configure an Access Key visit the My Account page of the NSS console.

You can call the following method to obtain an API access token. You must provide that token in subsequent API calls.

```
POST /auth/token
```

REGISTER MACHINE

This is the minimum information you must provide to NSS to register a machine.

A machine always belongs to a tenant and you protect it in a specified location (master server).

Its Protection Type defines the type of protection available to this machine.

{	
"MachineCode": "string",	Unique Id from source system
"CustomerCode": "string",	NSS tenant ref
"Location": "string",	NSS location code
"Hardware": "string",	NBU HW (for agent based backups only not VMs)
"OS": "string",	NBU OS (for agent based backups only not VMs)
"NetBackupClientName": "string",	FQDN, name used to access the agent on machine
"VMDisplayName": "string",	VM DisplayName from vCenter
"DisplayName": "string",	NSS visible machine name
"ProtectionTypeId": 0	Protection Type ID as defined in NSS
}	

API Endpoint: /machines, method POST

ADD PROTECTION

To protect a machine, you must firstly assign a Protection Type. You assign the Protection Type either at registration or after registration with a "register for protection" action. Each Protection Type has one or more level available (e.g. gold, silver, bronze). Using the machine's ID, you can retrieve the available protection levels as follows.

```
GET v6/machines/{id}/protection/levels
```

Once you identify the level, you can protect the machine.

```
POST /v6/machines/{id}/protect
```

You define the protection level id in parameters.

REMOVE PROTECTION

You can protect a machine with multiple protection levels. Before it can be unprotected, you must identify the current protection levels.

```
GET /v6/machines/{id}/protected
```

After identifying the level, you can unprotect the machine.

```
POST /v6/machines/{id}/unprotect
```

You define the protection level ID in parameters.

RESTORE VM

You can perform an ad-hoc backup of a machine at any time with the command shown:

```
GET /v6/machines/{id}/backupimages
```

After you identify the image, you can restore the machine with the command shown:

```
POST /v6/machines/{id}/restorevm/vmware
```

You define the selected backup image details as Parameters.

There are separate endpoints for Hyper-V and vCloud Director VMs.

BACKUP NOW

You can perform an ad-hoc backup of a machine at any time with the command shown:

```
POST /v6/machines/{id}/backup
```

You define the retention level information as Parameters.

You can monitor the outcome of Backup Now through the API activities sections. .

UNREGISTER MACHINE

If the machine no longer exists in the source system, you have two options:

1. You can delete the machine outright
2. You can keep the machine while there are still active images.

You must remove all protection before you delete a machine or before it is marked at the source as no longer available.

Once the unprotect activity completes, you delete the machine with the command shown:

```
DELETE /v6/machines/{id}
```

If you need to keep the machine, then the machine property `IsDeletedFromImportSource` must be set to true. This allows the machine to be available for restores.

The implementer needs to monitor the backup images for this machine. When there are no longer active backup images, you can delete the machine.

GET DASHBOARD DATA

All data represented in the NSS dashboards is also available using the NSS REST API. This includes daily/monthly backup utilization data and protection status data (traffic light summary).

You can retrieve backup utilization data for an individual machine, tenant, or the whole system. You can retrieve the information either by day or by month time period. The example shown retrieves all the data for 2016:

```
GET V6/utilization/systemmonths?filter=Year eq 2016
```

The example below gets the number of machines protected, unprotected and at status attention for the current tenant:

```
GET /v6/trafficlights/self
```

TRACK ACTIVITY

Where Activities are returned when calling REST API methods, they can be subsequently tracked using the Activities set of methods. NSS monitors the underlying NetBackup jobs initiated by API calls and the Activities methods allow clients to check for completion or errors.

CREATE TENANT / USER

You can create a tenant along with the initial user via the SOAP API. A sample script is available in the SDK folder. Create additional users for the tenant with separate API calls.

Calls to the REST API must pass an access token retrieved from an initial NSS user authentication call.

FURTHER DOCUMENTATION

The installation places a readme file on the NSS server containing the locations of the API. You can find the file in the following location:

```
Program Files\Biomni\NetBackup Self Service Adapter 8.1
```

NSS uses a tool called Swagger that allows a user to explore the API in a dynamic way. You can access the Swagger pages with a browser at the location shown:

```
https://<MachineName>/<SiteName>NetbackupAdapterPanels/Api/help/index
```

NSS includes a number of example scripts in the SDK folder to highlight usage of the API.

An additional SOAP API is available for the management of users, tenants, and locations (although you normally configure these through the NSS console). The SOAP API is accessible through a SDK at the below folder. The create-tenant.ps1 script shows an example of how the SDK is used. You can find the details on the SDK for the SOAP API in this folder:

```
C:\Program Files\Biomni\Front Office 8.8\Sdk
```

The SOAP API is directly accessible through the following URL:

```
http://<MachineName>/<SiteName>PublicWebService/DirectaApi.svc
```

A link to the WSDL is also available through the above URL.