Getting started with the NSS ServiceNow app

Minimum supported versions

ServiceNow: Kingston. The app uses the SN CMDB as the source for machines that need to be protected

NSS: 8.1.1

NetBackup: 7.7

Installation

The NSS ServiceNow app is installed via an update set. In the future the app will available in the app store.

Required Skills and Access

ServiceNow Administrator, NSS administrator and NetBackup Administrator

Basic Configuration for NSS

The standard NSS installation and configuration process needs to be followed. ServiceNow relies on a fully function combination of NSS and NetBackup.

As ServiceNow is a cloud based app, the NSS REST API must be accessible over the internet.

ServiceNow requires an account to access NSS:

Configure an MSP level account with SUP as access profile

Create Access ID and Secret key for the account

Create a tenant

Create Protection Types and associated Protection Levels (One protection type and on protection level is required as a minimum)

Define Master Servers (one is the minimum) and ensure that the relevant policy templates exist.

Design Considerations

Tenants

ServiceNow is a single tenant application. Configuration items (Cis) can have properties like company and department and therefore it is possible that a Service Provider can use a single instance of SN to manage different companies.

The implementer of the solution will need to make a decision on how to map the ServiceNow ‘tenant’ to NSS tenants.

The mapping between SN ‘tenants’ and NSS tenants is implemented through the NSS CI Mapping functionality.

At the most basic and possibly most common scenario SN is mapped to single tenant in NSS. However if someone decides to map SN departments to NSS tenants, the CI mapping needs to include rules to cover all possible CI/tenant variations.

CMDB

The implementer must have a thorough understanding on how the CMDB is used by the client. The rules that will drive the registration of CMDB machines to NSS, need to cover all possibilities.

The recommendation is the order the conditions in a way of how many Cis are impacted by a rule in a descending way e.g. a condition the impacts 10 Cis must come before one that impacts 50 Cis.

Initially the auto-register option on rules should be left unchecked until the implementer is satisfied that all permutations have been covered.

Setup Order

Details on how to configure each section can be found in the "NSS ServiceNow App Configuration" document.

NSS Configuration

NSS Import Authentication

Master Servers

Tenants

Protection Types

Protection Levels

In most cases the sections above are set once.

Then depending on how the CMDB is setup and the number of Master Servers and Tenants, NSS CI Class Mappings and NSS OS Mapping Tables need to refined over a number of repetitions.

Dashboards

There are 5 reports that can be used to create dashboards:

NSS-Activities created each month

NSS-Attention Devices

NSS-Protected Devices

NSS-Registered Devices by Department

NSS-Unprotected Devices

Alerts

NSS monitors the backup health of protected devices. A change in the health status can be tracked and action taken.

The most important event is when a protected machine goes from status 'Green' to status 'Red'. This means that a machine that is in a scheduled policy and should be backed up, it does not.This change in status can be used by notifications or by flows in the Flow Designer.

The app ships with such a workflow," NSS-Device needs attention", that creates an incident when a machine turns from green to red. It is expected that this flow will be altered to suit a particular deployment (e.g. the group that is responsible for handling this)

Approvals

The NSS App uses workflows to fulfil BaaS requrests. The workflows can be altered to include approval steps that will meet the customer's requirements.