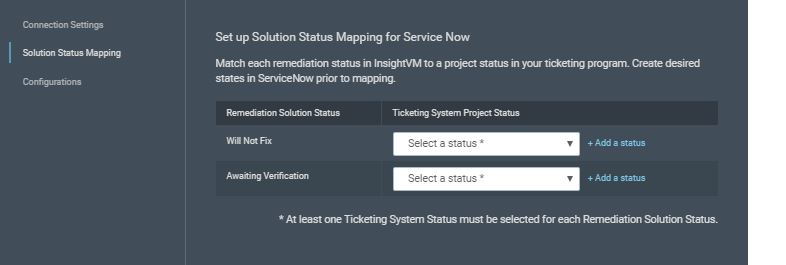
**Service Now Integration with RAPID7 Insight platform**

Below is the process we can follow to remediate vulnerabilities detected via Rapid7 InsighVM:

1. Create Remediation Project to categories the vulnerabilities
2. Assign ticketing template which will indeed help in filling configured details while creating automatic tickets in Servicenow
3. Respective user/group will be notified when ticket is created/ Due in Service Now
4. Once, user will complete all the tasks assigned for any particular ticket, will change ticket status and then, respective team will notified to verify whether issue is fixed, if fixed, ticket status will be updated in InsighVM will be updated automatically as per below configuration

[](https://files.readme.io/70349ec-ticketing_serviceNow_solution_status.JPG)

1. Validation will be done for same item, if vulnerability will be fixed ticket will be closed. If not, one more ticket will created in Service now.

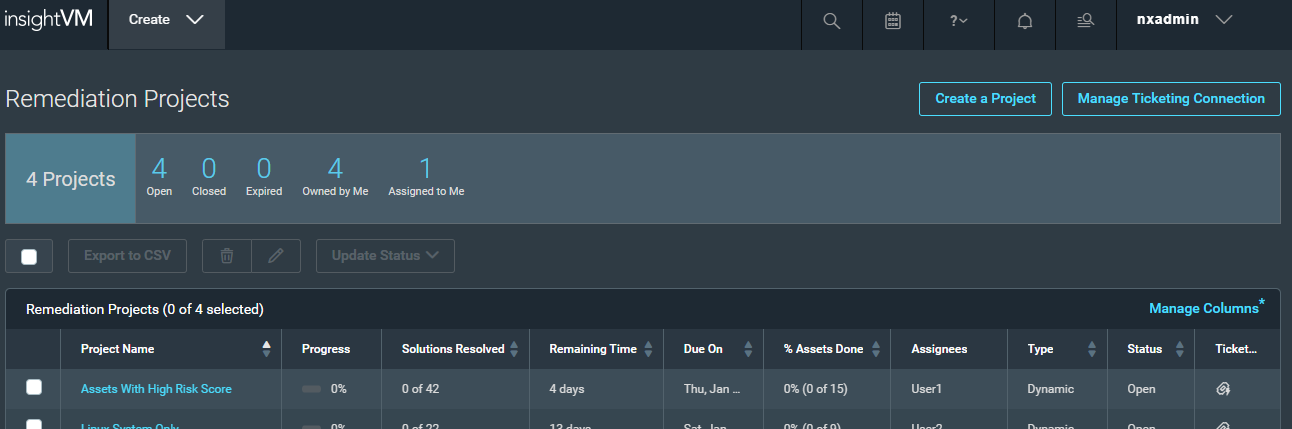
**Integration Requirements:**

1. Service now Instance URL with enabled inbound communication
2. An account with following role:

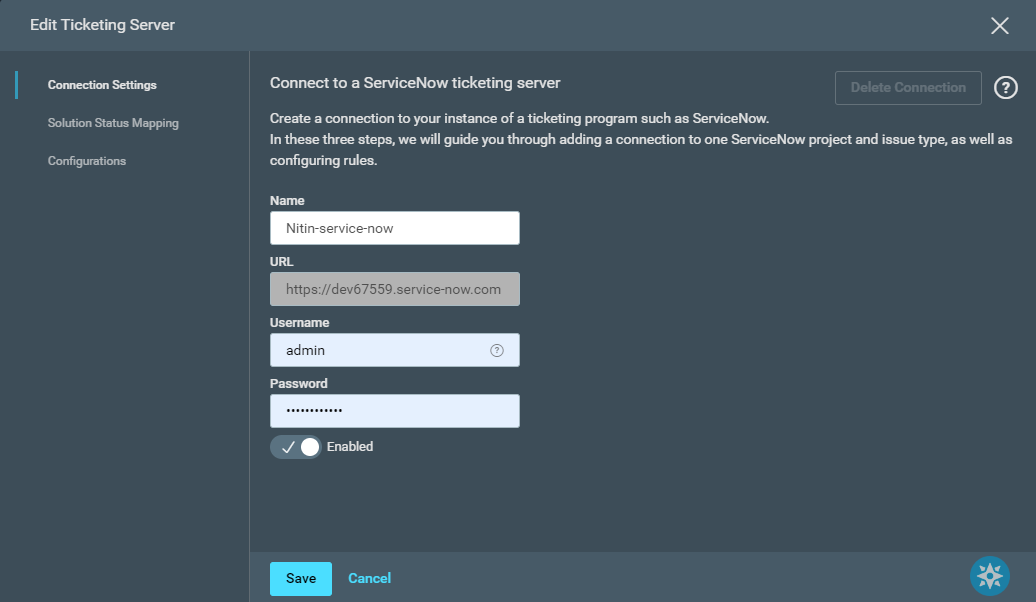
**Admin** or itil\_admin, itil, mid server, report\_admin, personalize\_choice

**Managing Ticket System in InsightVM:**

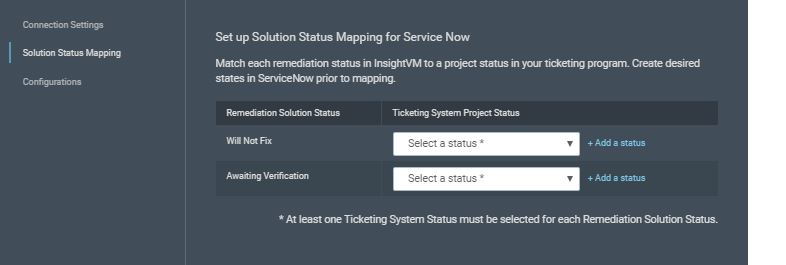
1. Click managing ticket Connection as shown:



1. On the **Settings** > **Connections** view, click the **Service Now** ticketing option in the ticketing area.
2. On the **Connection Settings** page, enter the URL of your Service Now server and the credentials to an account with the required permissions.



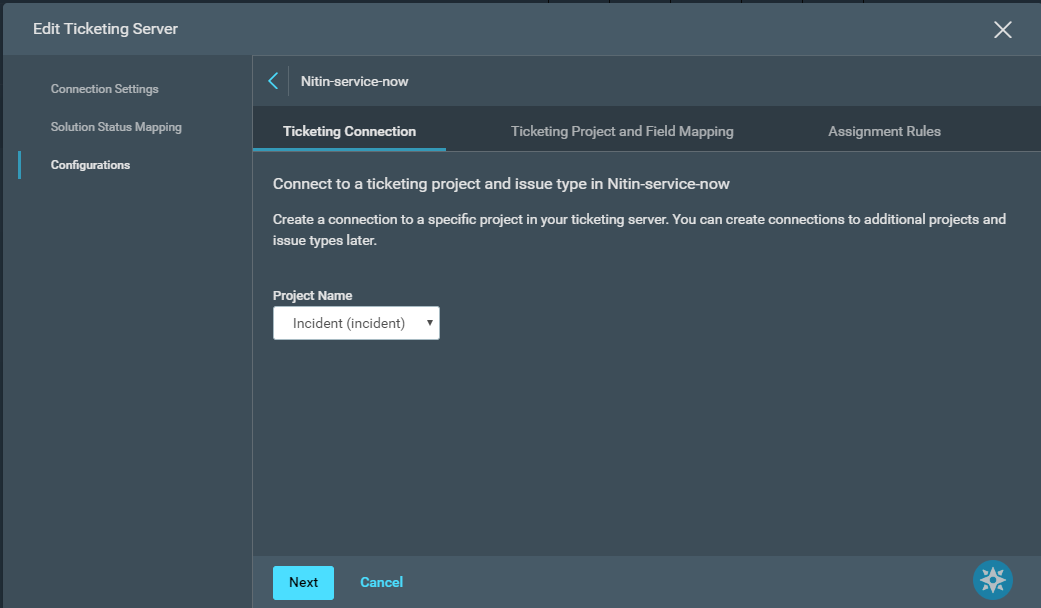
1. Click **Solution Status Mapping** to map one or more ServiceNow issues statuses to one of the following Remediation Project statuses:
   * **Awaiting Verification** - The remediator has taken action to mitigate the vulnerability and is now awaiting verification, the vulnerability no longer exists, or the remediation failed.
   * **Will Not Fix** - The item cannot be remediated.

[](https://files.readme.io/70349ec-ticketing_serviceNow_solution_status.JPG)

Note: Changing the status of a ServiceNow ticket can change the status of a remediation solution, but changing the solution status will not change a ServiceNow ticket's status.

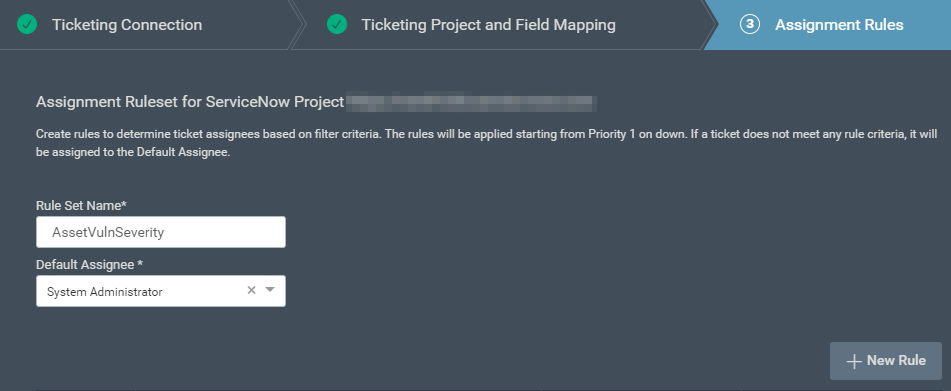
1. Click **Configurations**, and then click **New Configuration**.

6.1 Complete the **Ticketing Connection** page to select the ServiceNow project for automated ticketing. Click **Next** to continue to the **Ticketing Project and Field Mapping** page.



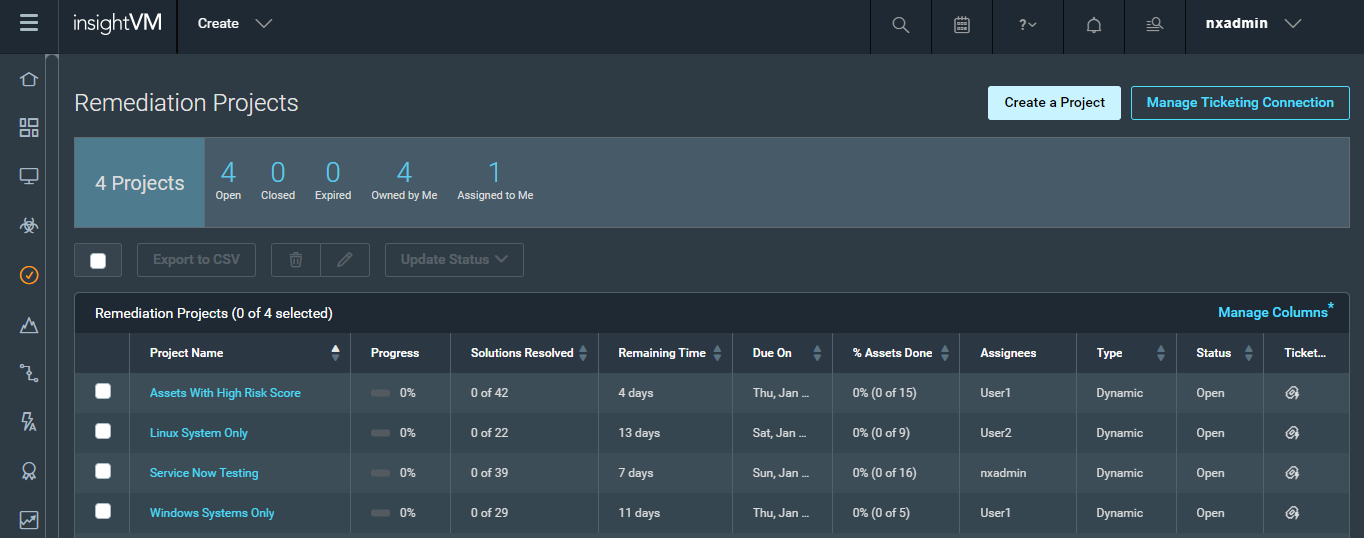
6.2: Click on **Ticketing Project and Field Mapping** page to draft a template of the ticket that you generate from your Remediation Project. Map the fields in Service Now to the scan related data here. You can configure how concise or detailed you want the summary and description to be with variables for information, such as a solution name ($SOL\_NAME), asset list ($ASSET\_NAME\_LIST), and other data related to your vulnerability scans.

6.3: Click on **Assignment Rules** page to create rules for assigning automatically generated tickets to your team based on factors like the ownership of assets and the expertise of the assignees. The list of rules ordered by **preference** as shown:

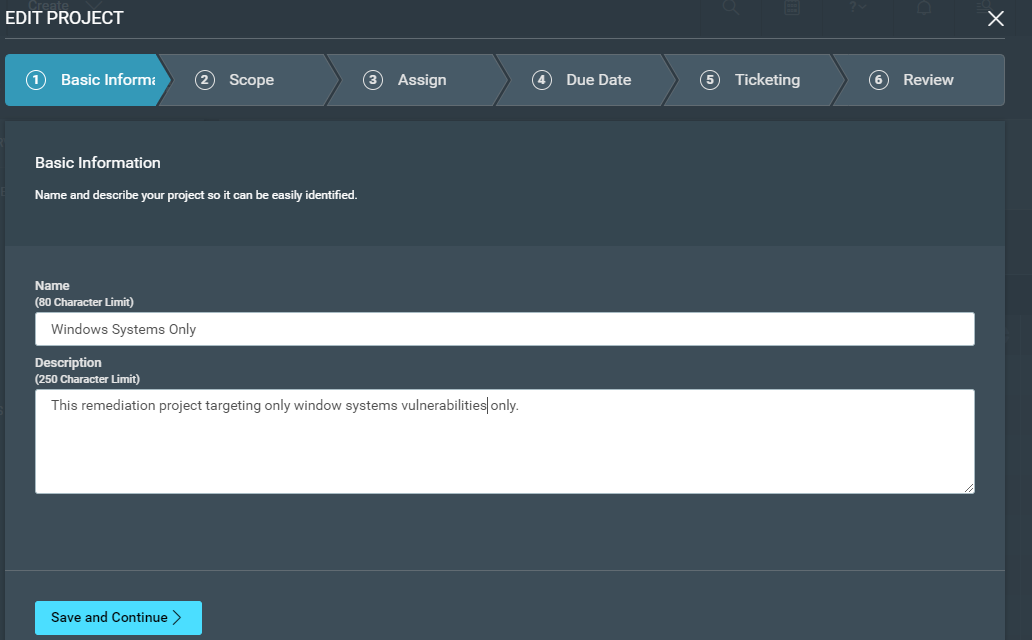
[](https://files.readme.io/057c8db-rw_sn_asset_filter_suggestions.PNG)

6.4: Once everything done click save and exit the wizard.

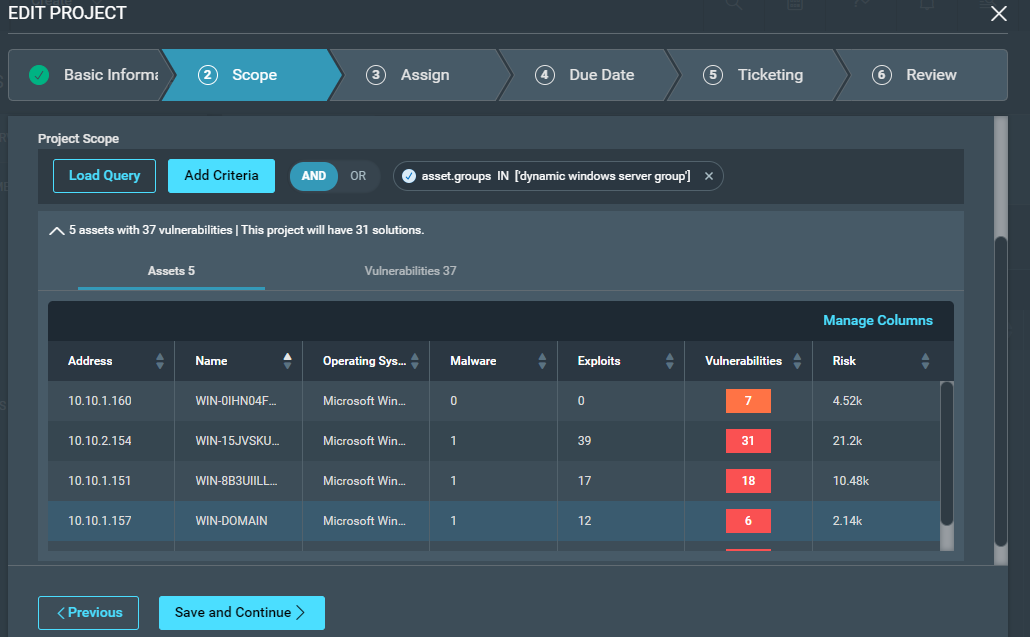
**Creating Remediation projects in InsightVM:**



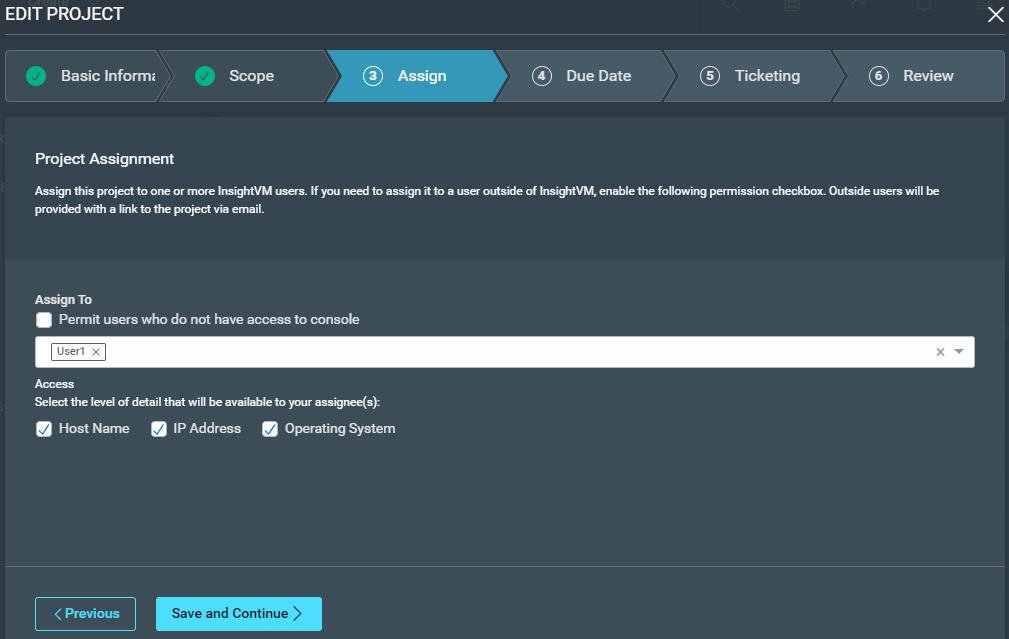
1. Give project a name and description and save and continue.



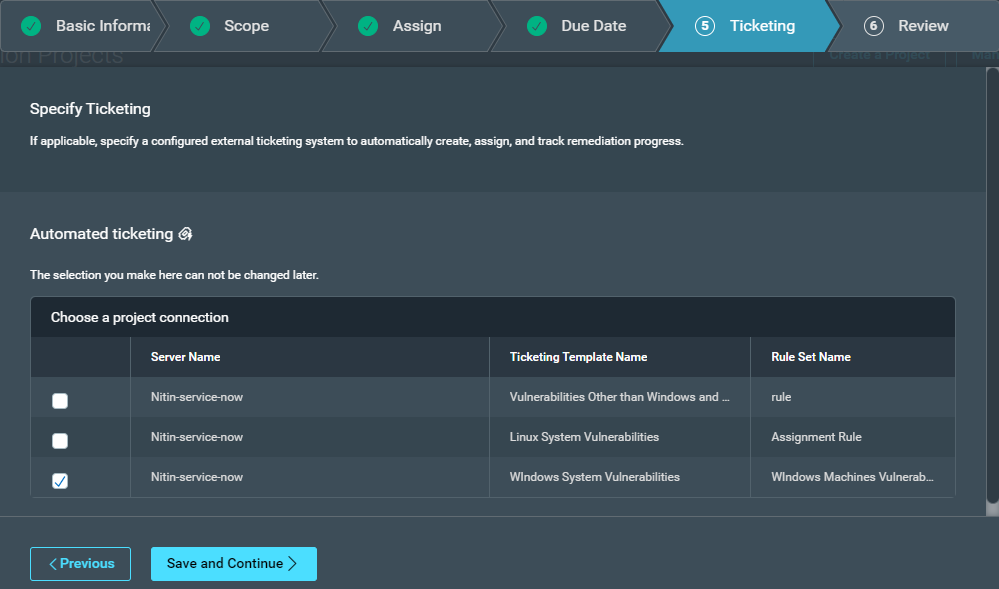
1. Scope the project by adding dynamic query or asset filtering criteria as shown and filtered assets will be shown below. Save and continue.



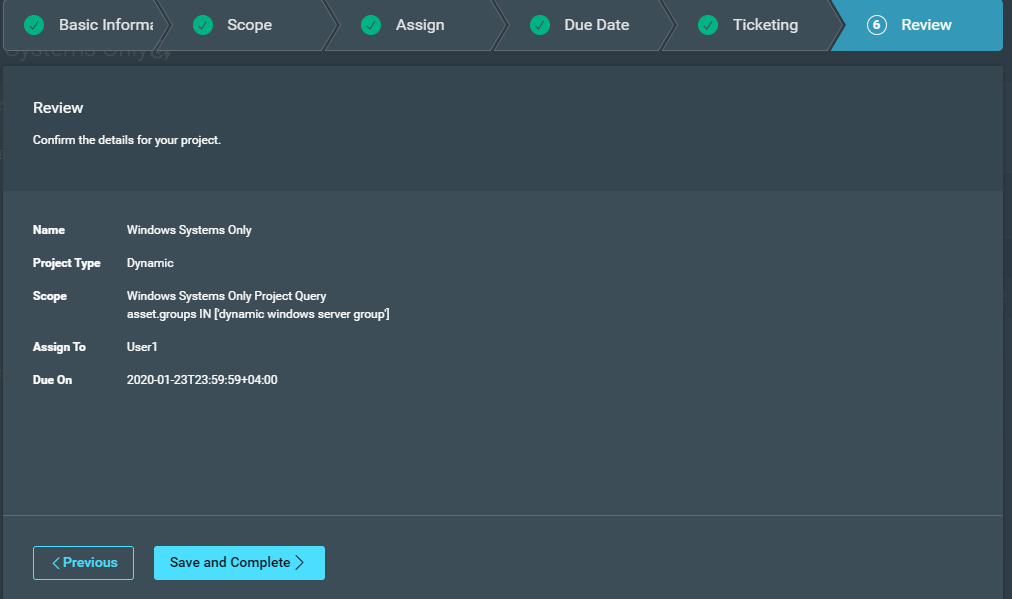
1. Assign project to respective handlers for InsightVM and assign Due Date for Project



1. Assign Ticketing template configured before and proceed.



1. Review the details and Save the Project.



**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF DOCUMENT \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***