nexpose®

Working with Project Sonar Data

in Nexpose 6.1.16

Release date: 03/23/2016

Working with Project Sonar in Nexpose 6.1.16

When Nexpose 5.17 was released back in October 2015, it introduced the ability to add data from Project Sonar, which is an initiative by the Rapid7 Labs team to actively scan public networks and provide access to that data to everyone. You can utilize Sonar data to find your organization's publicly facing assets and identify your external exposure surface area.

Working with Project Sonar pre-Nexpose 6.1.16

The initial release of the integration required you to perform several steps to add Sonar data to a Nexpose Console, including creating two sites and a dynamic asset group. If you've worked with Project Sonar in the past, you should be familiar with the steps required to import data.

To add Project Sonar data to Nexpose, you had to:

1. Create a site.

2. Select the Project Sonar connection to add assets.

3. Create a query using filters.

4. Save the site.

5. Manually scan the site using the Dynamic template.

6. Create a dynamic asset group for your Sonar assets.

7. Create a new site and add the dynamic asset group.

8. Scan the site with a template that performs vulnerability and policy checks.

9. Schedule the scan.

That's a lot of steps, and it's not the most intuitive process. With Nexpose 6.1.16, we've made some major changes to our integration with Project Sonar to improve the experience for you.

Working with Project Sonar in Nexpose 6.1.16

The improvements we've made have helped us streamline the process so that it is more inline with our other workflow paradigms. You'll notice that the new workflow is very similar to the one for dynamic assets:

1. Create a site.

2. Select the a Sonar connection to dynamically discover assets.

3. Add filters to refine the assets that are added to the site.

4. Save the site.

5. Scan the assets.

6. Schedule a scan.

The biggest change is that you now only need to create one site for a particular set of Sonar assets. We've eliminated the need for a secondary site and a dynamic asset group.

The other major change is that Nexpose Administrators are responsible for creating the query that pulls domain data into the Nexpose Console. Site Administrators can create sites and select the Sonar connection, but they cannot modify the query that imports data into the console. However, Site Administrators can add filters to refine the Sonar results even further.

What this means for you

The changes are meant to improve your overall experience with Project Sonar. You'll just need to make a few adjustments so that you can utilize the full benefits of the Project Sonar integration. Here are how the changes impact you:

- Nexpose Administrators set up the Sonar query. Site Administrators can create sites and refine the query, but cannot change the original query.

- You no longer need to create a secondary site or a dynamic asset group for Sonar data. All Sonar assets can be filtered, scanned, viewed, and tagged from the same site.

- All legacy sites that were created using the old workflow will be migrated as discovery queries. Any existing schedules on those sites will be disabled. You will need to go back and create schedules for these Sonar sites if you want to do live network scanning. All secondary sites that were created for dynamic asset groups will not be affected, but we recommended that you delete them.

- In previous versions of Nexpose, the assets were placed into the *Scanned* table with an *Assessed* status of 'No' after you create a Sonar site. Now, they are placed in the *Discovered by Connection* table, just like other assets that are dynamically discovered.

Setting up a Sonar query

Nexpose Administrators must set up queries to pull data from Sonar. These queries can also be used to set boundaries on the domains that Site Administrators have permissions to scan. All results from Sonar are added to the *Discovered by Connection* table on the *Assets* page.
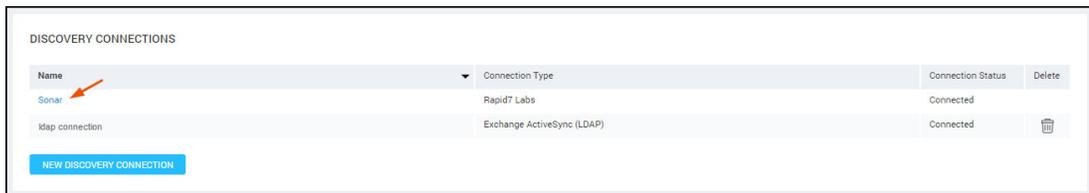
To set up a Sonar query:

1. Select **Administration** from the left navigation menu.
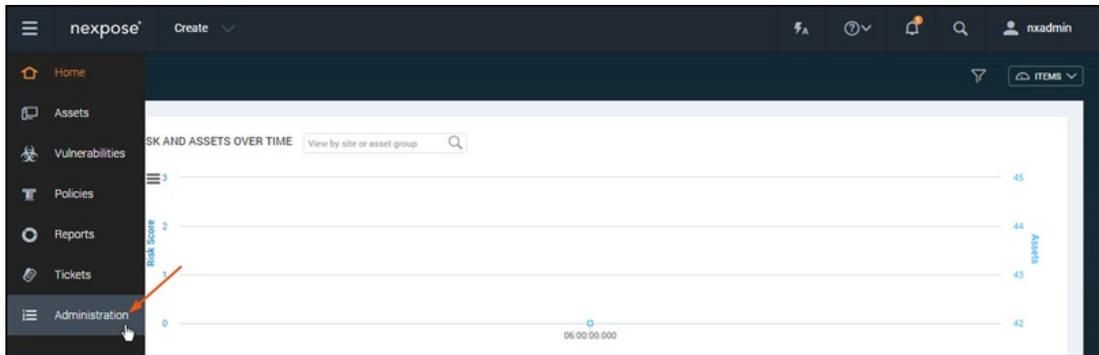
2. Under the *Discovery Options*, click the **manage** link for *Connections*.
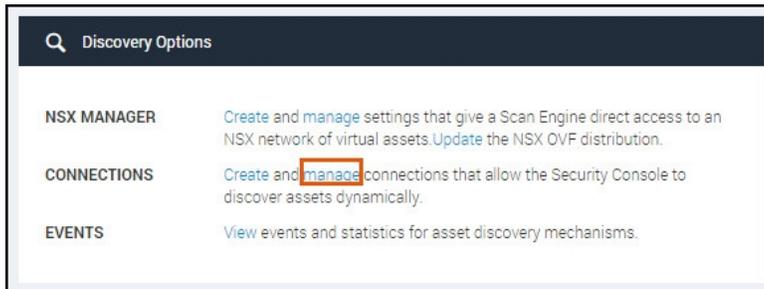
3. Click on the **Sonar** connection.

4. On the *Sonar Queries* page, click the **New Sonar Query** button.

5. Enter a name for the query.

6. Add a filter for the domain you want to query. It can be a top level domain, such as 'rapid7.com', or a subdomain, such as 'community.rapid7.com'.

You can also add a scan date filter if you want to control the staleness of your asset data. The shorter the range, the less likely the data will be stale.

7. Test the query by running it. It may take awhile to complete and will display any results in the table.

8. Save the query when you are done.

Learn more about Project Sonar

That's it! Those are all our changes. We hope that the improvements we've made will help you utilize Sonar data more easily. We've only covered the basics here in this document, so if you want to learn more, please visit our documentation. Site Administrators can read the Nexpose User's Guide, and Nexpose Administrators can read the Nexpose Admin Guide.