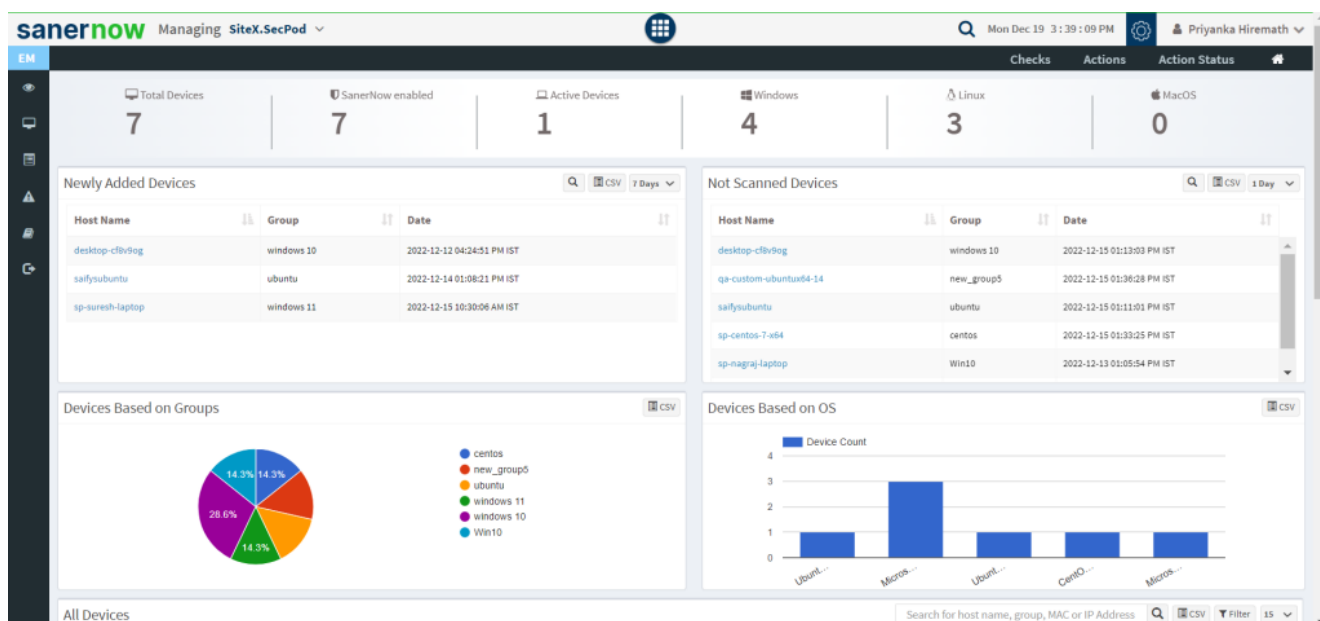


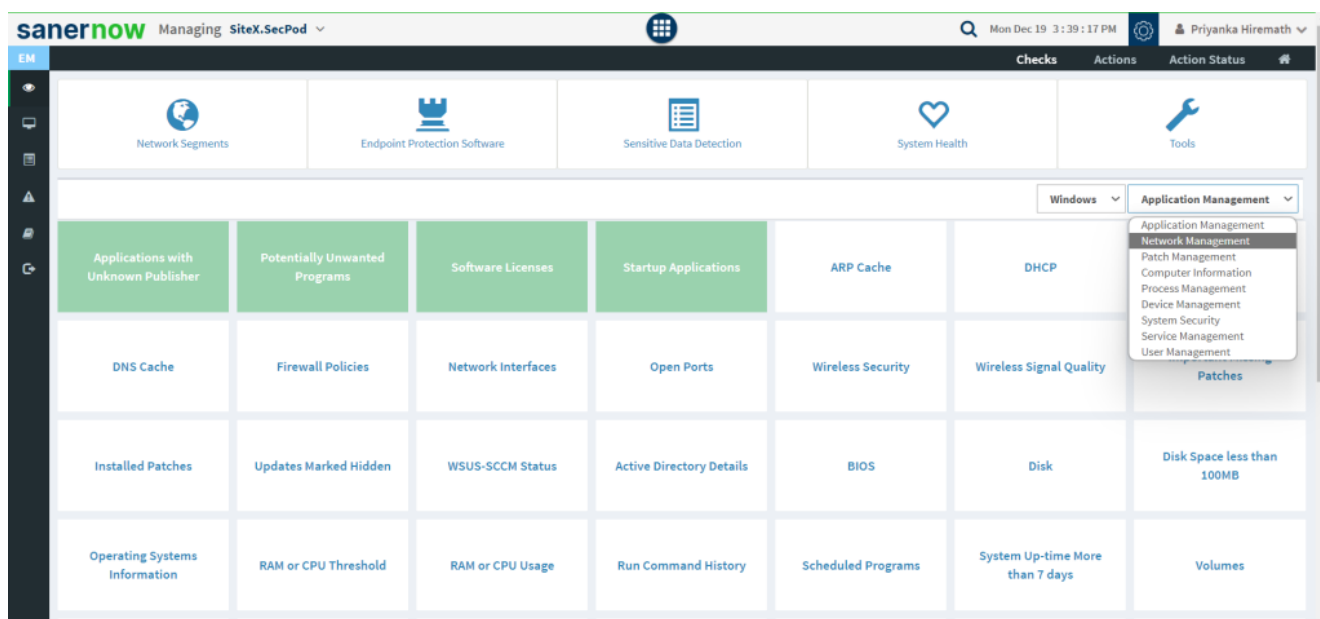
How to collect ARP entries that are created when a hostname is resolved to an IP address and then to a MAC addressing in Linux?

1. Go to **Endpoint Management** module in SanerNow.

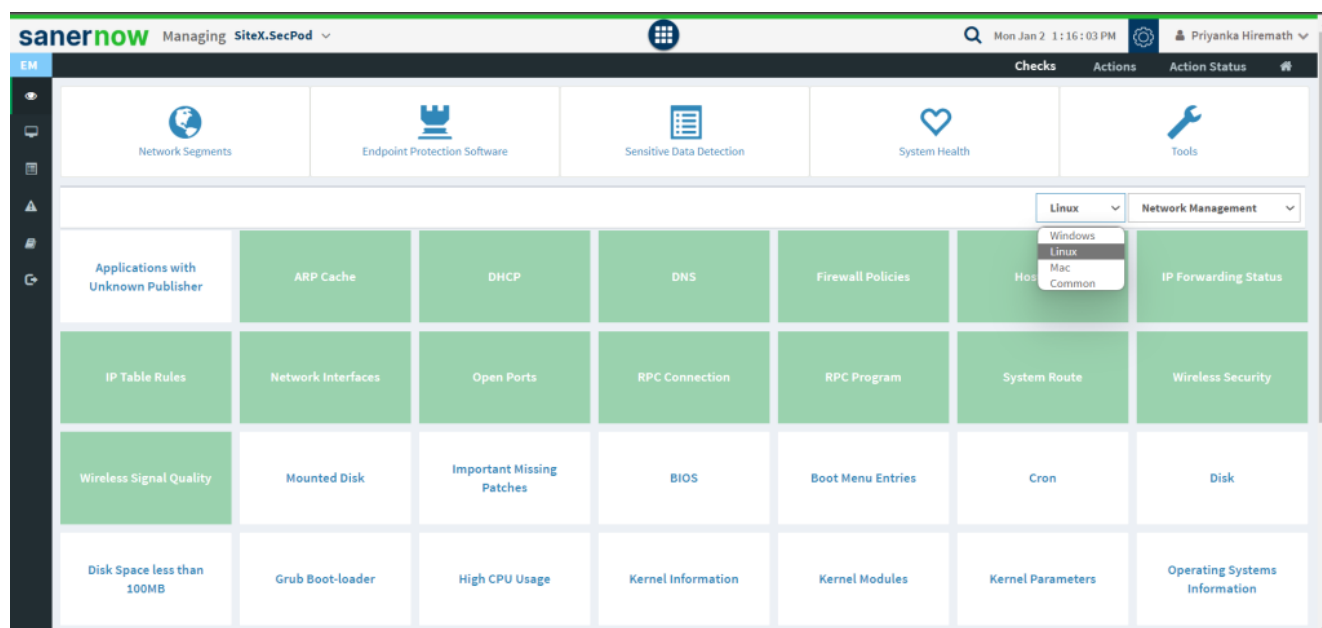


2. Click on **Checks**.

3. In the right side, select '**Network Management**' from the dropdown list.



4. Also, select the operating system: Linux.



5. The checks corresponding to this filter will be highlighted in green.

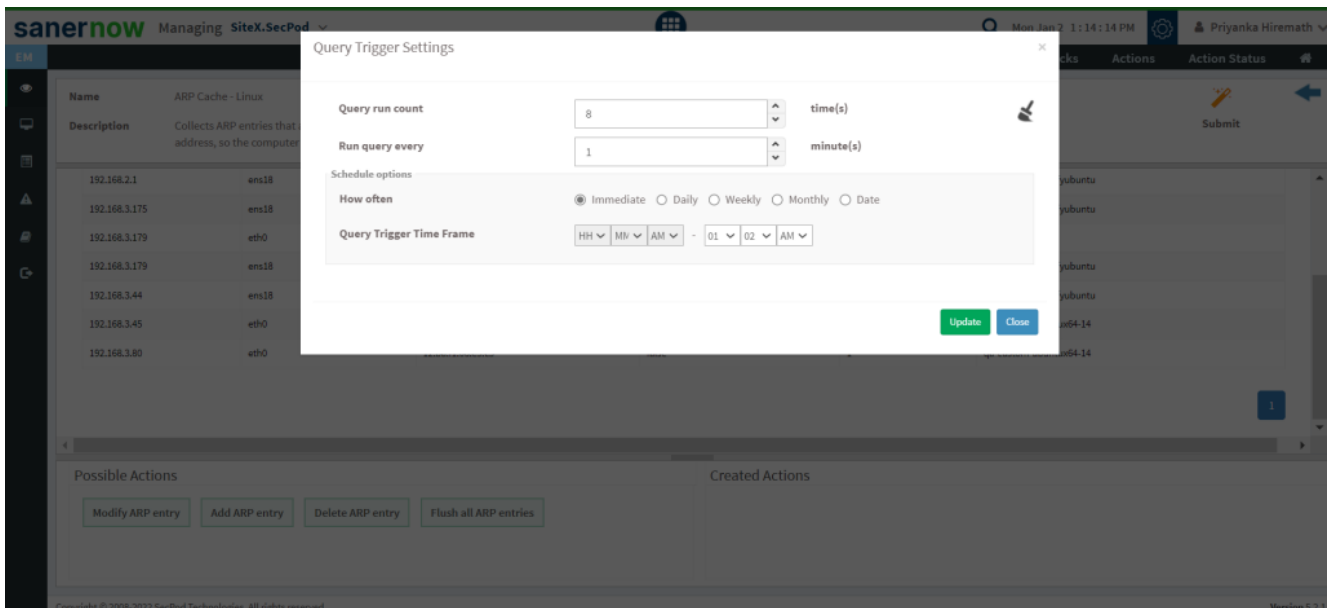
6. Select the '**ARP Cache**' check.

7. You will be displayed with the check name, description, result pane, and possible actions after triggering the check.

8. To schedule the query execution for the agent, click on **Trigger**.

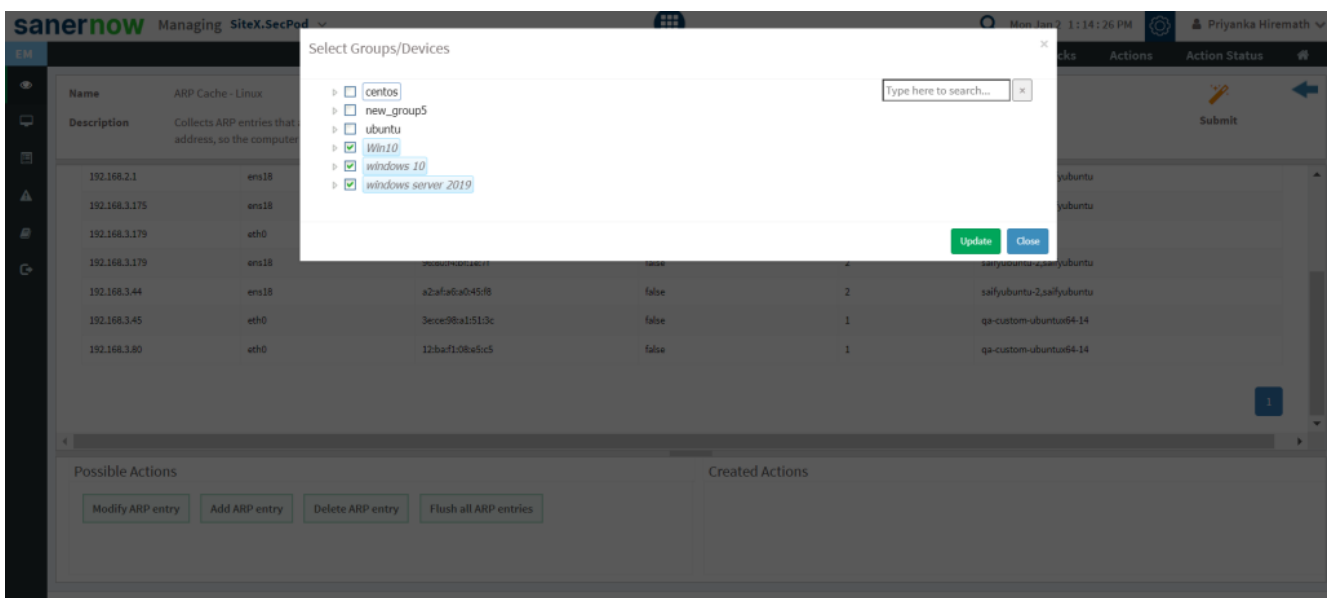
9. Update the query trigger settings:

- Set the Query run count time in seconds.



- Set the time in minutes to run the query often.
- In Schedule options pane, set the **Query Trigger Time Frame**.
- Click on **Update**.

10. Select the **Scope** to assign the query to the group/devices.



11. To send query to the agent, click on **Submit**.

12. In **Result pane**, you will be displayed with ARP entries that are created when a hostname is

resolved to an IP address and then to a MAC addressing in Linux.

13. You can take possible actions according to the results. Possible actions are specified at the bottom pane. Click on the desired action, you will be redirected to Create Response page. In Created Actions, you will find all the responses created for the following check.

The screenshot displays the 'Create Response' interface in the SanerNow application. The top navigation bar includes the 'sanernow' logo, 'Managing SiteX.SecPod', a search icon, the date 'Mon Jan 2 1:14:42 PM', and the user 'Priyanka Hiremath'. The main content area is titled 'Create Response' and contains several input fields and a list of actions.

- Operating System Family***: A dropdown menu with 'Linux' selected.
- Response Name***: A text input field with 'name *' as a placeholder.
- Response Description***: A text input field with 'Action for ARP Cache - Linux' as a placeholder.
- Action***: A dropdown menu with 'Flush all ARP entries' selected. A list of actions is visible, including 'Add ARP entry', 'Add entry into host file', 'Add /etc/protocol Entry', 'Add Route', 'Add Service Entry', 'Block Domain', 'Delete ARP entry', 'Delete entry from host file', 'Delete /etc/protocol Entry', 'Delete Route', 'Delete Service Entry', 'Disable IP Forwarding', 'Enable IP Forwarding', 'Flush all ARP entries', 'Flush all entries from host file', 'Modify ARP entry', 'Modify entry from host file', 'Modify NTP Server', 'Modify /etc/protocol Entry', and 'Modify Route'.
- How often**: Radio buttons for 'Immediate' (selected), 'Daily', 'Weekly', 'Monthly', and 'Date'.
- Operating Systems**: A list of operating systems with checkboxes: 'centos', 'new_group5', 'ubuntu', 'Win10', 'windows 10', and 'windows server 2019'.

The footer of the page contains the text 'Copyright © 2008-2022 SecPod Technologies. All rights reserved.' and 'Version 5.2.1.5'.

Now you know how to collect ARP entries that are created when a hostname is resolved to an IP address and then to a MAC addressing in Linux.