

MULTI-TENANCY IN WAZUH

Multi-tenancy in Wazuh allows multiple organizations or users to share the same system while keeping their data and settings separate. Each tenant can access only their own logs, alerts, and configurations. This setup helps save resources by using one system for many groups. It also improves security by isolating data between tenants. Users with different roles can be given specific permissions. Multi-tenancy makes it easier to manage and scale the system for multiple clients or departments. Overall, it provides a secure and efficient way to handle multiple users in one Wazuh deployment.

# **How to enable Multi-Tenancy in WAZUH**

Step 01: Open the Configuration File

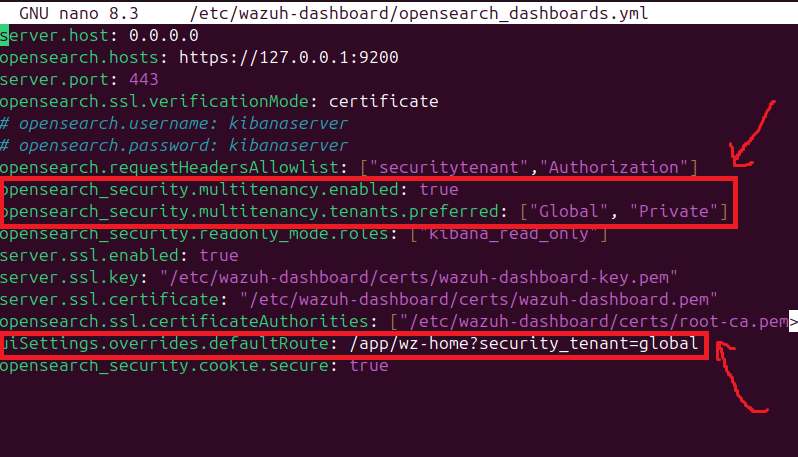
* Use a text editor to open the configuration file:

sudo nano /etc/wazuh-dashboard/opensearch\_dashboards.yml

Step 02: Enable Multi-Tenancy

* Find or add the following line in the file:
* Make sure it is not commented out (remove # if present).

opensearch\_security.multitenancy.enabled: true



Step 03: Save and Close

* After editing, save the file and exit:

For nano: press CTRL + O, then ENTER, then CTRL + X.

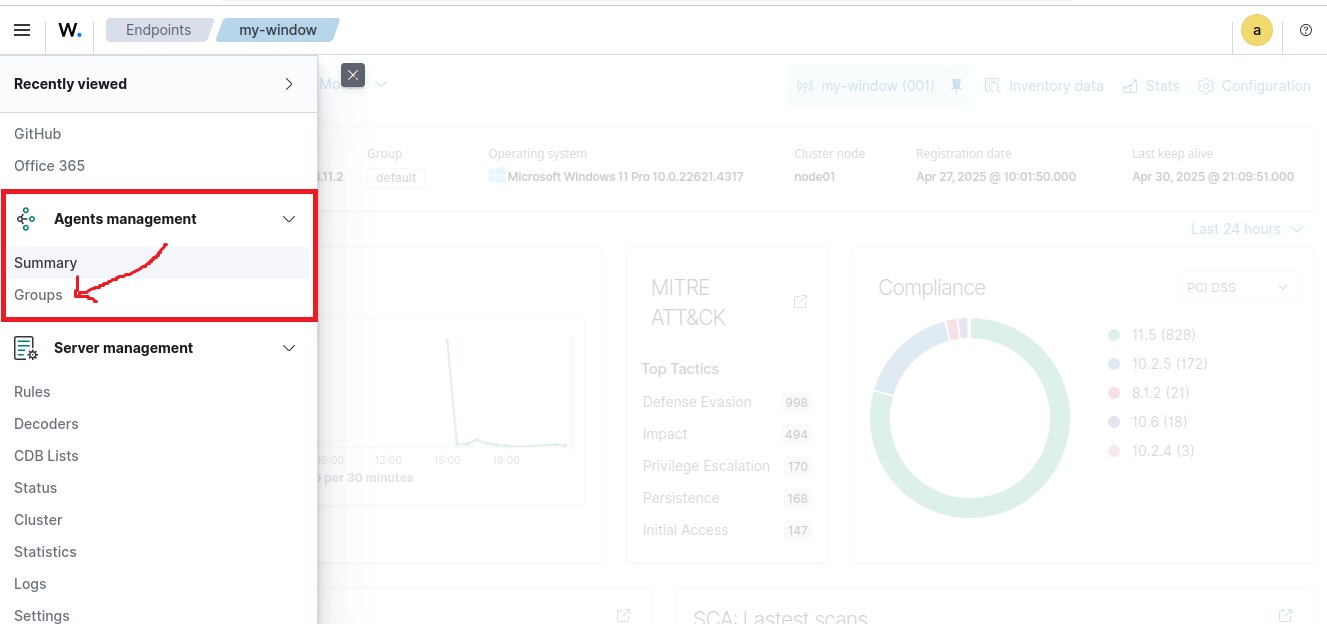
Step 04: Restart the wazuh dashboard so changes can take effect

* systemctl restart wazuh-dashboard

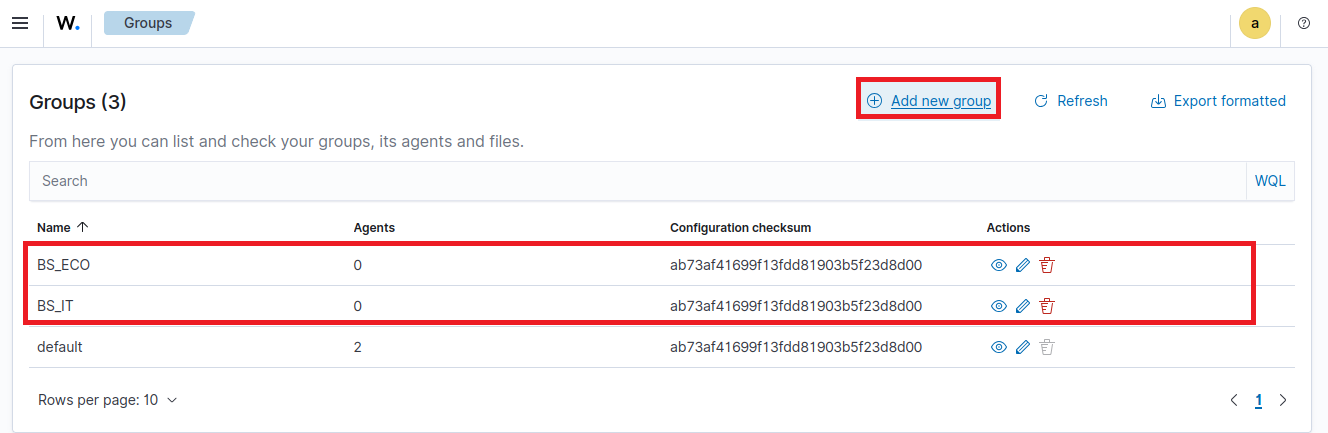
**Task 1:**

Create the two groups BS\_IT and BS\_ECO in the group configuration, you must use the label to distinguish the groups. Add the agents to these groups.

1. Log into the wazuh dashboard as admin
2. Select Agents management > Endpoint groups to open the page



1. Create the group BS\_IT and BS\_ECO.



1. Select group and click Edit group configuration.
2. Add a label to identify the group, for example

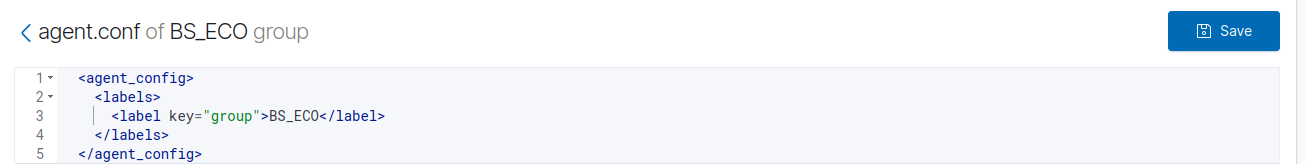
<agent\_config>

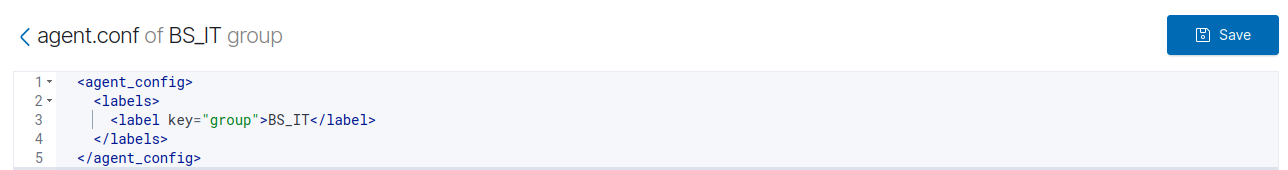
<labels>

<label key=”group”>BS\_IT</label>

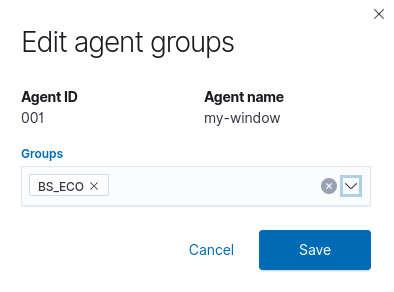
<labels>

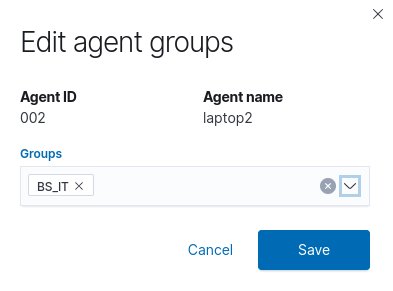
</agent\_config>





1. Select the agent and assign them to the groups that are created just before.

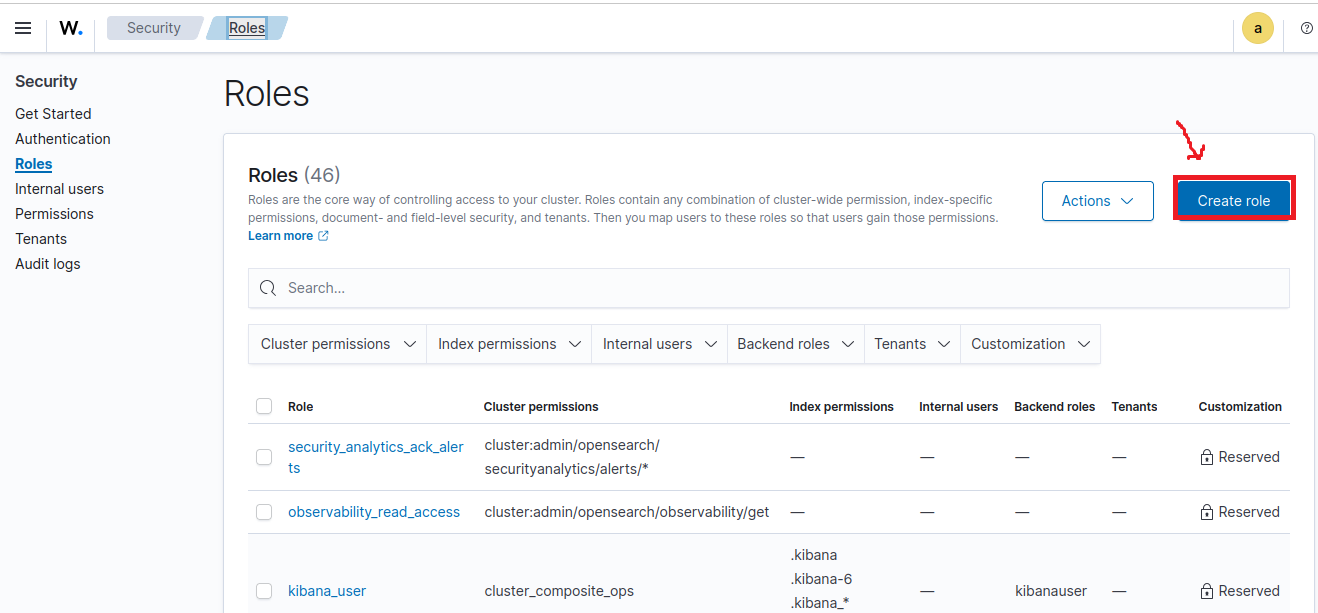




**Task 2:**

Define the roles for both group in the OpenSearch security section then map these roles to internal user.

1. Click the  to open the menu on the Wazuh Dashboard, and go to the index management > Security, and then Roles to see the roles page and click on create role.



Name: Assign a name to the role.

* Name: Assign a name to the role.(SOC-IT)
* Cluster permissions: cluster\_composite\_ops\_ro
* Index: \*
* Index permissions: read
* Click Add another index permission and unfold the new section Add index

permission. Complete the empty fields with the following parameters and

make sure to replace your group name accordingly:

* Index: wazuh-alerts\*

* Index permissions: read

* Document level security:

{

"bool": {

"must": {

"match": {

"agent.labels.group": "BS\_IT"

}

}

}

}

* Click Add another index permission and unfold the new section Add index

permission. Complete the empty fields with the following parameters and

make sure to replace your group name accordingly:

* Index: wazuh-monitoring\*
* Index permissions: read
* Document level security:

{

"bool": {

"must": {

"match": {

"group": "BS\_IT"

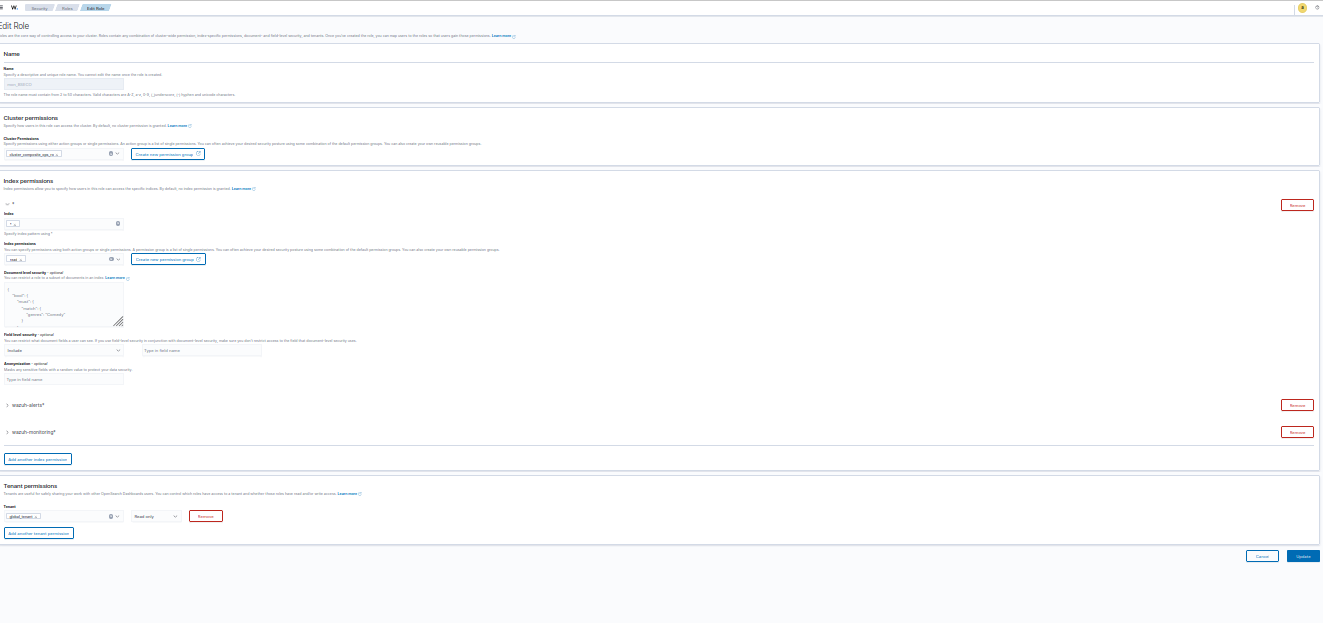
}

}

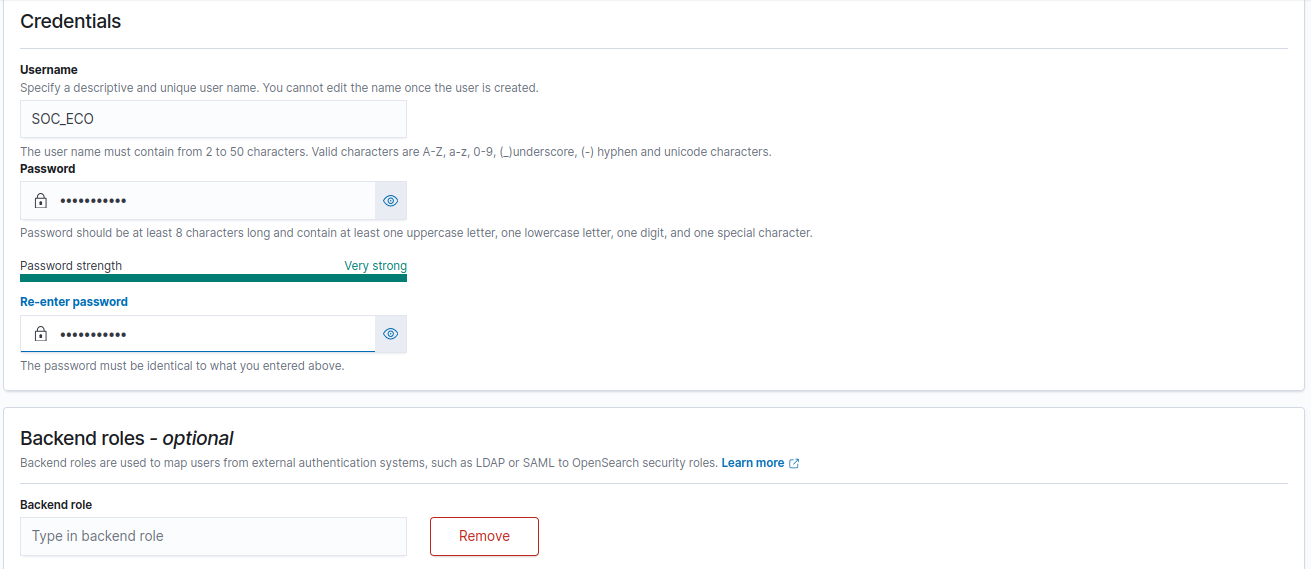
}

}

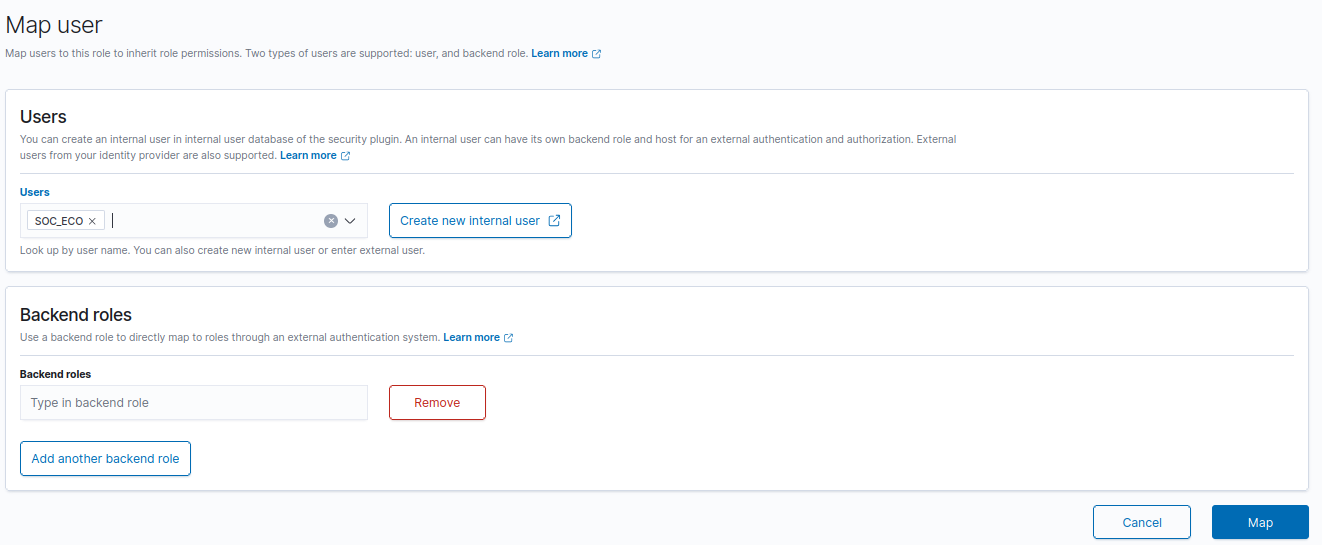
* Under Tenant permissions, select Tenant: global\_tenant and the Read only option.
* Click Create to complete the task



1. Click select Mapped users tab, click Manage Mapping, and create new internal user.



1. Go to the user page and map the user that are created in previous step.

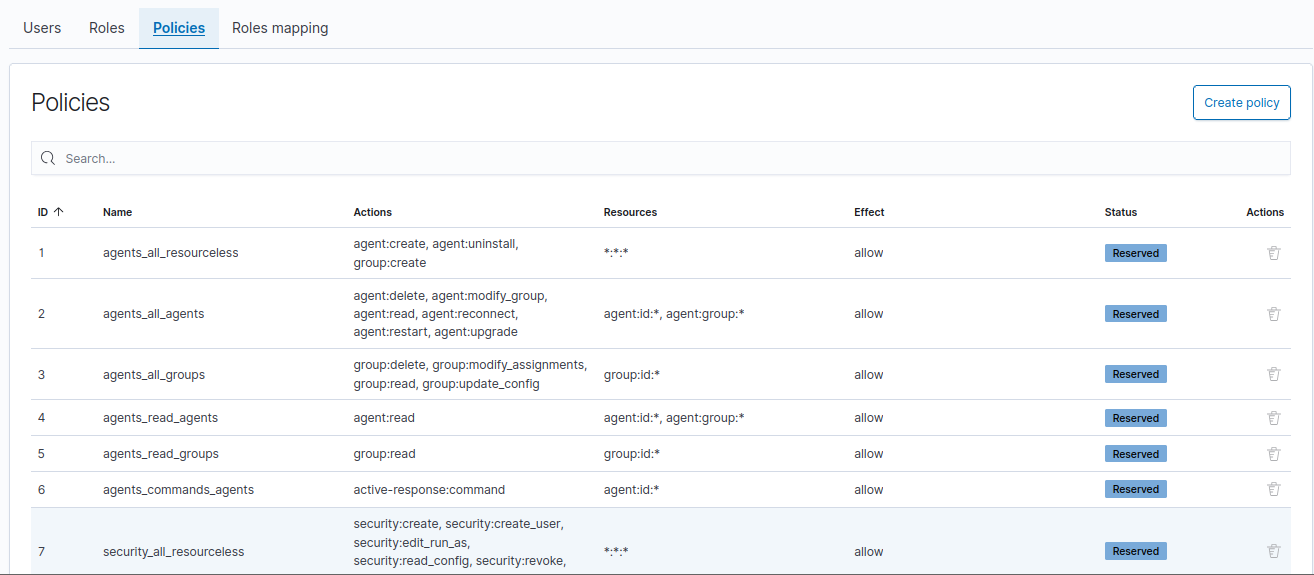


Finally created the role and mapped user for group one. Now you can create the role and mapped user by following the previous steps.

**Task 03:**

Create new policies for each group and then assign it to each role that is we created previous task.

1. Click  to open the menu on the wazuh dashboard go to the server management > Security and then policies to open the policies page



1. Click on the Create policy and complete the empty fields with the requested information.

* Policy name: Assign a name to the new policy (mon\_BSIT).

* Action: Select the actions that the user is allowed to perform, for example,

agent:read, and click Add. Select as many actions as needed.

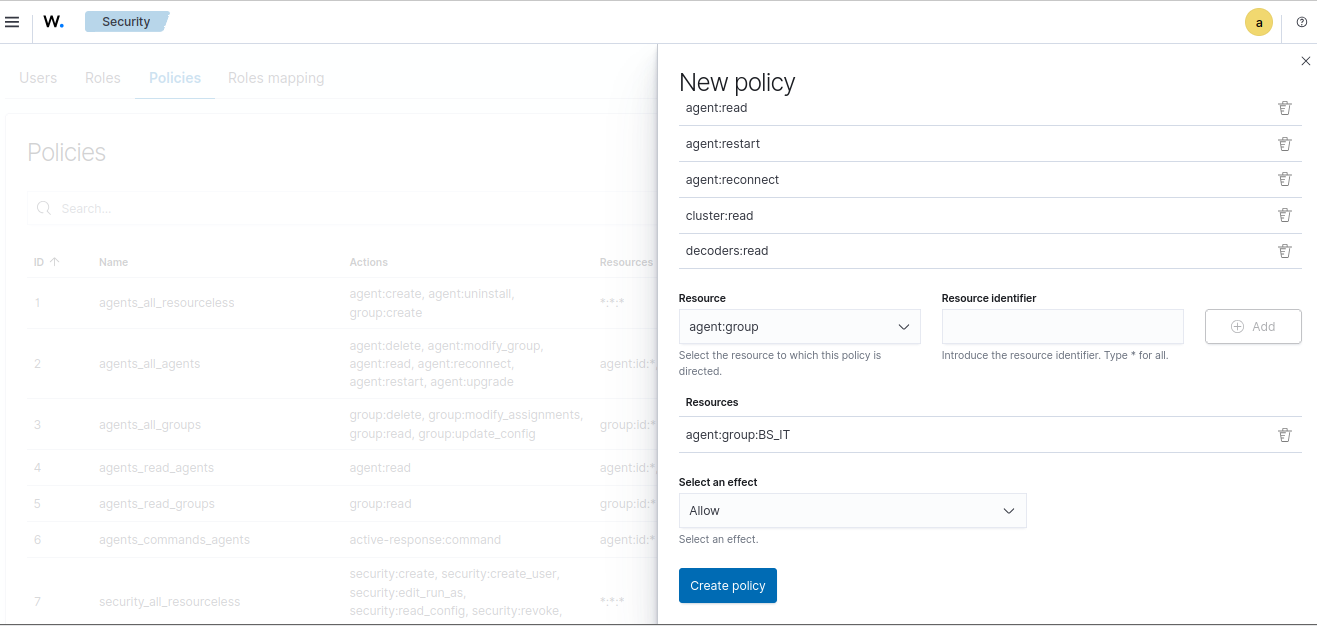
* Resource: Select agent:group.

* Resource identifier: Write the name of the agents' group, for example,

BS\_IT, and click Add. You can add as many resources as needed.

* Select an effect: Select Allow.

* Click **Create policy** to complete the action



Policy name: Assign a name to the new policy (mon\_BSIT).

Action: Select the actions that the user is allowed to perform, for example,

agent:read, and click Add. Select as many actions as needed.

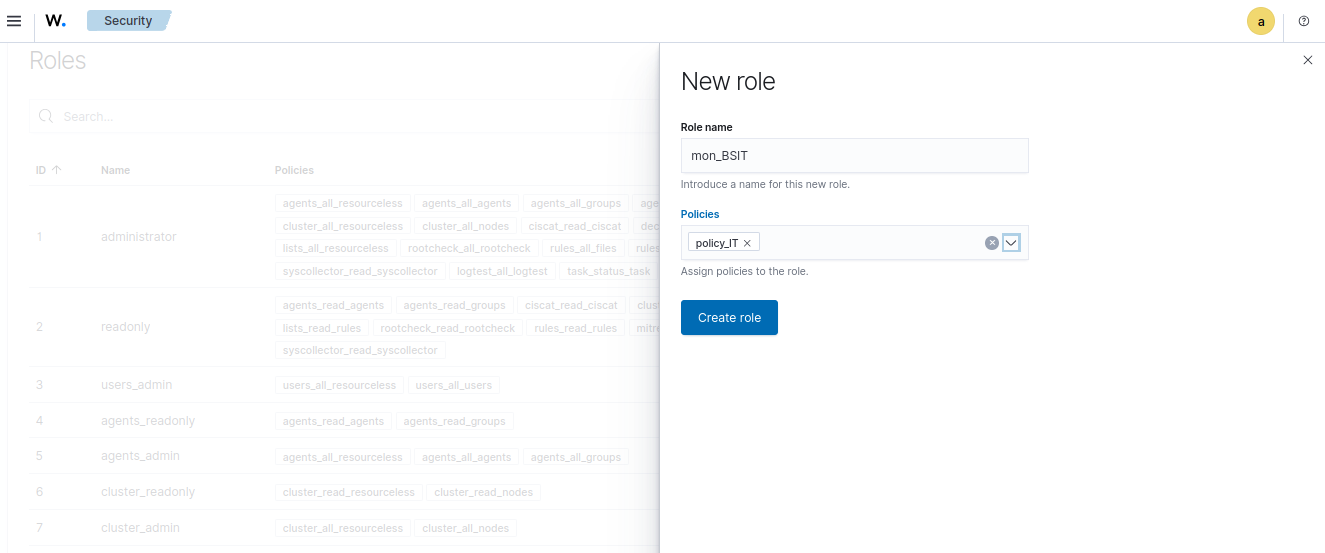
Resource: Select agent:group.

Resource identifier: Write the name of the agents' group, for example,

BS\_IT, and click Add. You can add as many resources as needed.

Select an effect: Select Allow.

Click **Create policy** to complete the action



I created policy, role and then mapping the role for group one (Team\_A) now you can

create for second group (BS\_ECO) through these same steps.

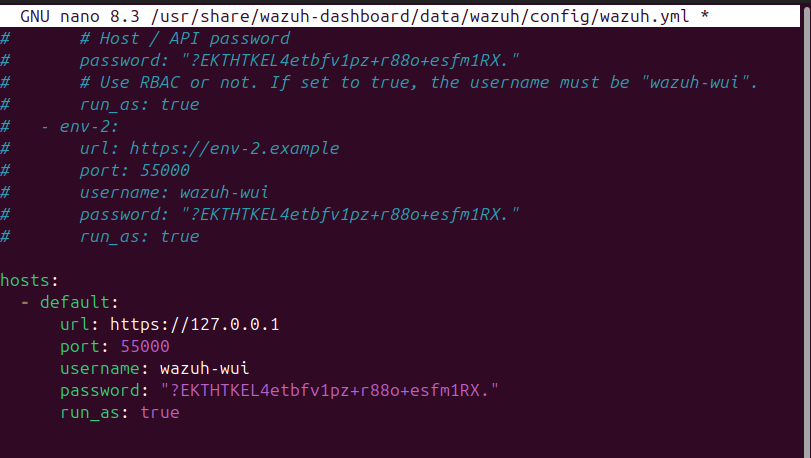
**Task 4:**

For Wazuh App permissions, you will have to do the following:

Make sure that run\_as is set to true in the /usr/share/wazuh

dashboard/data/wazuh/config/wazuh.yml configuration file. Restart the Wazuh

dashboard service and clear your browser cache and cookies.

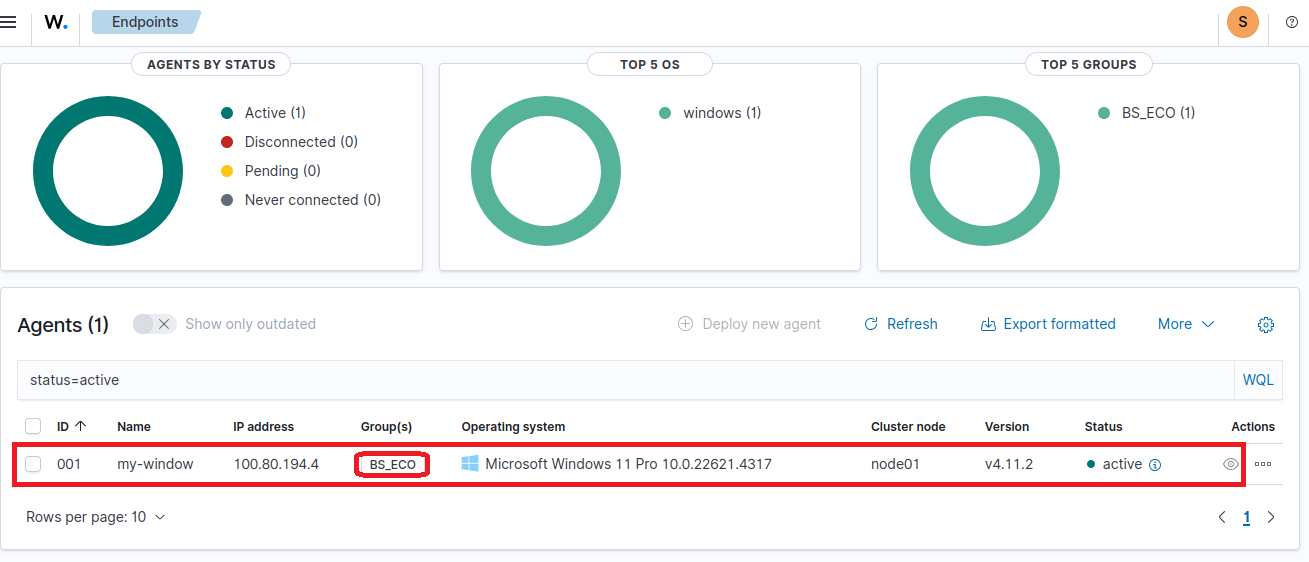


Finally, we enabled the multi-tenancy in wazuh now we will verify it through login the

both group’s users. Logout from administrator account and login from Team\_A user.



Now you can see and manage the ECO department group agents that is verify we successfully created the Two different multi-tenant.



**Conclusion**

In this document, we explained what multi-tenancy is, how it works, its benefits and

limitations, and how to enable and configure it in Wazuh using OpenSearch Dashboards.

Multi-tenancy is very useful in real-world environments where different teams or clients

need to use the same system but with isolated data and access. It allows organizations

to manage multiple users or groups securely, all from a single Wazuh server.

By following the step-by-step guide, we successfully created separate users and roles for

different groups and verified that each user can only see their own data. This confirms

that multi-tenancy was configured correctly in Wazuh.

This setup is especially useful for enterprises and security providers who want to save

resources while keeping their environments secure and organized.