Configuring Vormetric on Neo4j

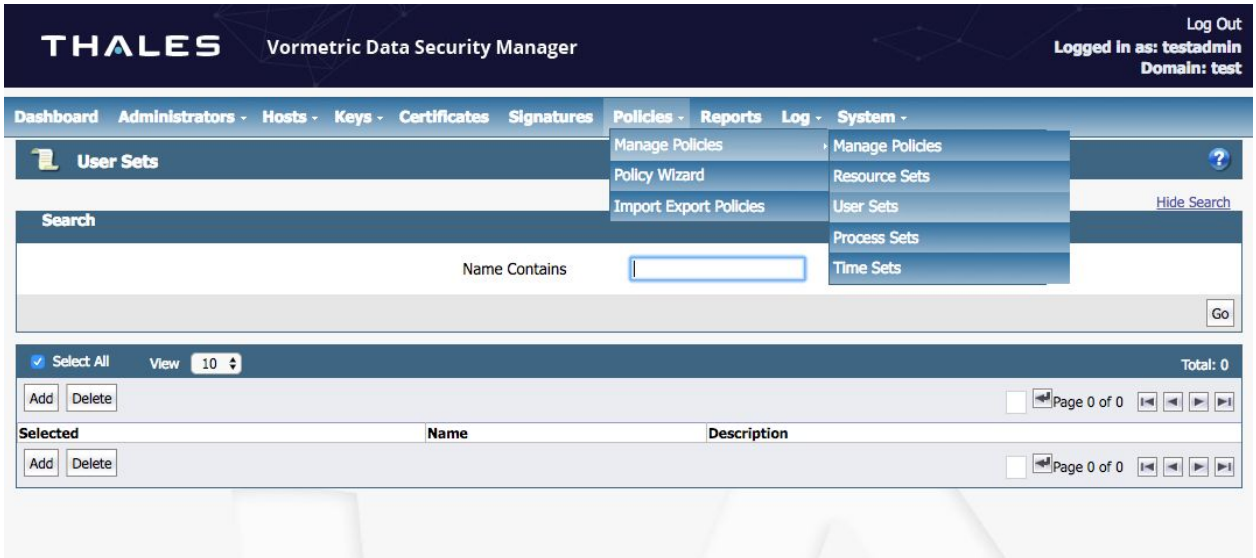
This document describes how to configure Neo4j-specific rules for the VTE agent software. Following these instructions requires that you have DSM installed and configured, and that the VTE agent has also already been installed on the host, and that the host has been registered into a DSM domain.

Table of Contents

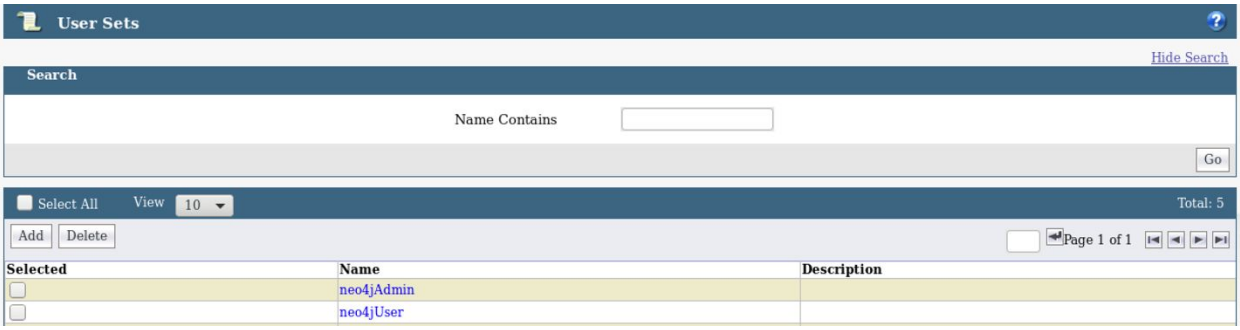
Setup

Configure User and Process Sets

Log in as the domain administrator, and in the top nav bar select Policies -> Manage Policies -> User Sets.



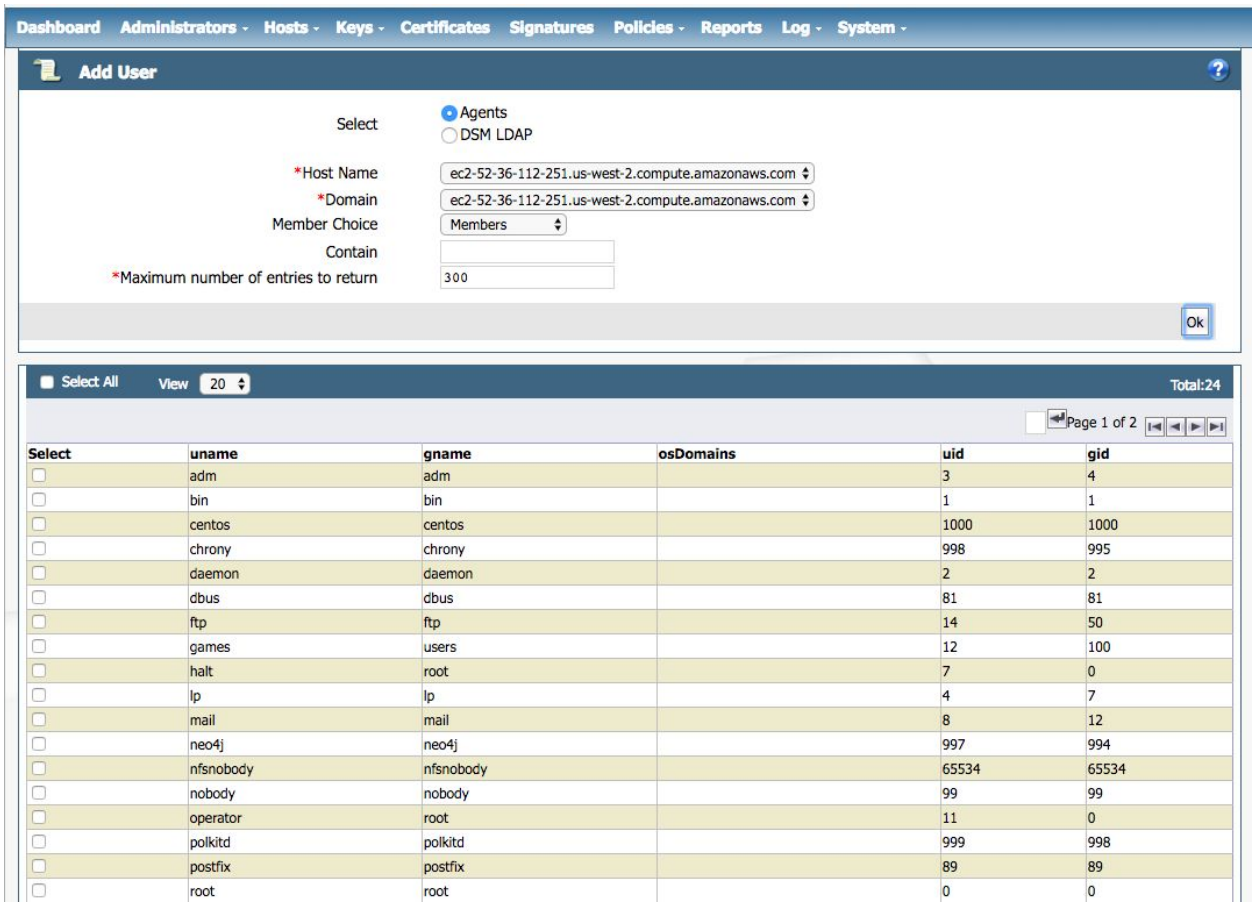
We need to create specific user sets to allow or deny access to different guard points. We will create a user group for the user that will be running Neo4j. We will also create a Neo4j admin group that will have access to read files (configuration and logs).



These user sets will be associated with rule enforcement. To make sure that local users on the host can access files, you must next select a user set, and associate host-based users to that user set.

- For the neo4jAdmin user set, you should assign the root user or other “sudo” / administrator, and the neo4j user which is typically built-in with a neo4j install.
- For the neo4jUser user set, you should assign only the “neo4j” user.

You can do this by clicking on the user set you created, and then hitting the “Browse Users” button.

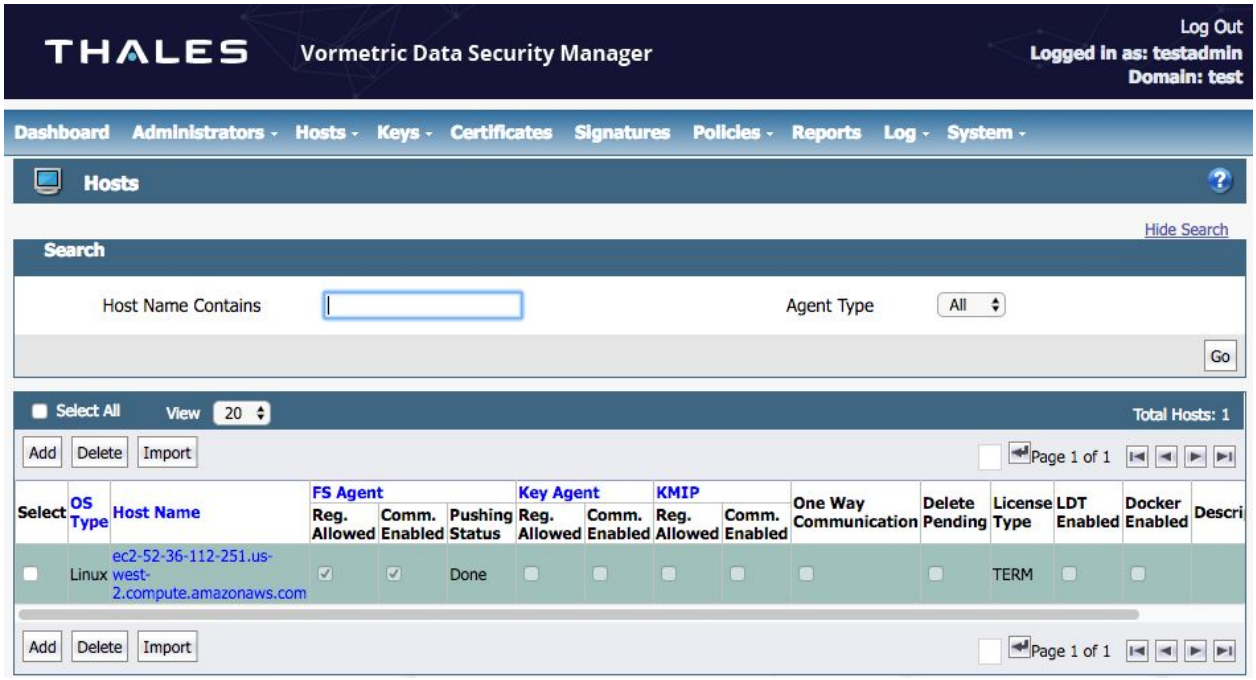


Select	uname	gname	osDomains	uid	gid
	adm	adm		3	4
	bin	bin		1	1
	centos	centos		1000	1000
	chrony	chrony		998	995
	daemon	daemon		2	2
	dbus	dbus		81	81
	ftp	ftp		14	50
	games	users		12	100
	halt	root		7	0
	lp	lp		4	7
	mail	mail		8	12
	neo4j	neo4j		997	994
	nfsnobody	nfsnobody		65534	65534
	nobody	nobody		99	99
	operator	root		11	0
	polkitd	polkitd		999	998
	postfix	postfix		89	89
	root	root		0	0

We now have two user groups established, and have assigned the neo4j user to both, and the admin (root) to only the admin group.

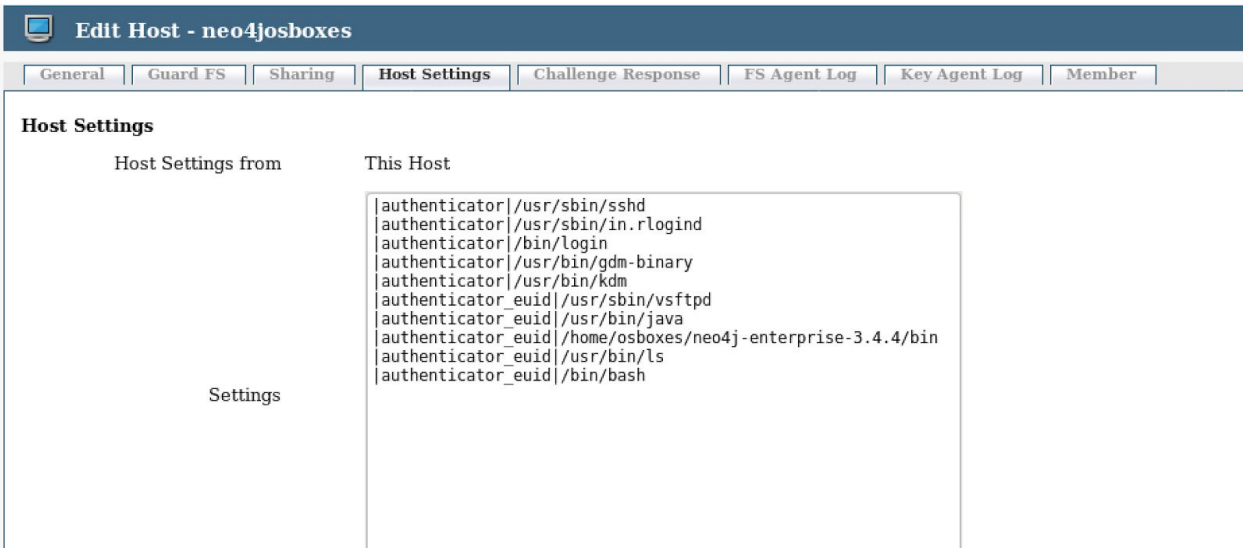
Setup Host File Settings (Linux)

Log into Vormetric DSM as the domain administrator. Navigate to the hosts dialog (top nav bar: Hosts -> Hosts) and find the Neo4j host that was registered as part of the VTE Agent registration step, and click on that host.



Click on the “Host Settings” tab, and add the following four lines to the Host File settings.

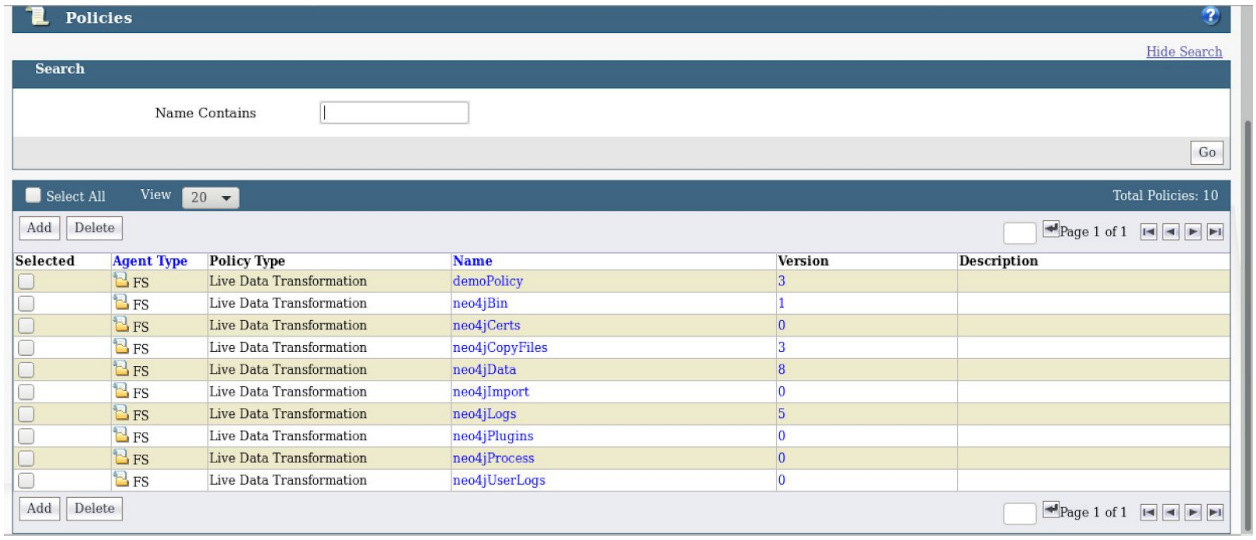
|authenticator_euid|/usr/bin/java
|authenticator_euid|<neo4j-home>/bin
|authenticator_euid|/usr/bin/ls
|authenticator_euid|/bin/bash



Create Neo4j Policy

We need to create specific Neo4j security policies that will include the user sets we defined above. These Neo4j security policies will be used by the guard points to enforce read, write, and execution of files in the protected paths. For debugging, it will allow the *neo4jAdmin* group to read files (e.g. configuration and log files).

To setup the Neo4j policies, go to the Policies -> Manage Policies -> Manage Policies in the DSM manager. Create the policy names as shown in the dialog below.



Add Security Rules Per Policy

We then add security rules for each policy, as shown in the screenshot below.

The specifics of which actions should be permitted versus blocked will differ depending on local security policy. At a minimum, the neo4j UNIX user will need full access to the core directories in order for the database software to function. Most other choices are up to local preference security requirements, and any additions to the software baseline you may have made.

For example, if you run regular backups and put them in a particular directory, consider protecting that directory, and so on.

Assign Policies to Guard Points

We will assign policies to guard points to enforce read, write, and execution of files in the protected paths. The following table documents the recommended policy and guard point for a Neo4j installation.

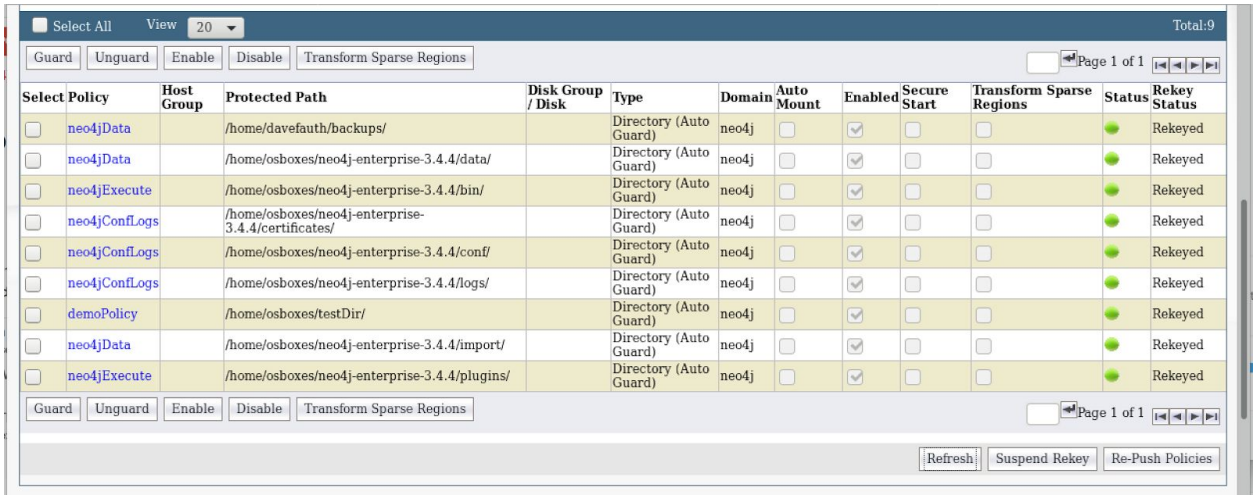
It is when these policies are assigned to the guard points that the rules will take effect on the machine.

> **!!! Important: ensure that the users and permissions are assigned correctly in the above steps before performing this step. If they are mis-assigned, this can result in database unavailability; for example if the "neo4j" user gets locked out of the ability to write data to disk while the database is still operational, data loss may occur!**

Prior to guarding the key paths on a running system, you may wish to test an intermediate directory first.

Policy	User Set	Guard Point	Comment
Neo4jExecute	neo4jUser	<neo4j-home>/bin	Protect who can start/stop Neo4j and execute admin functions
Neo4jConfLogs	neo4jUser	<neo4j-home>/certificates	Protect who can read or modify SSL certificates
Neo4jConfLogs	neo4jUser & neo4jAdmin	<neo4j-home>/conf	Protect who can read or modify the Neo4j configuration
Neo4jData	neo4jUser	<neo4j-home>/data	Protect who can gain access to the Neo4j database and Neo4j local auth files
Neo4jData	neo4jUser	<neo4j-home>/import	Protect who can access files to import data into Neo4j
Neo4jConfLogs	neo4jUser & neo4jAdmin	<neo4j-home>/logs	Protect who can view neo4j log files

Neo4jExecute	neo4jUser	<neo4j-home>/plugins	Protect who can add plugins to the Neo4j application
Neo4jData	neo4jUser	Neo4j backup directory	Protect who can access Neo4j backups



Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Secure Start	Transform Sparse Regions	Status	Rekey Status
	neo4jData		/home/davefauth/backups/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jData		/home/osboxes/neo4j-enterprise-3.4.4/data/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jExecute		/home/osboxes/neo4j-enterprise-3.4.4/bin/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jConfLogs		/home/osboxes/neo4j-enterprise-3.4.4/certificates/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jConfLogs		/home/osboxes/neo4j-enterprise-3.4.4/conf/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jConfLogs		/home/osboxes/neo4j-enterprise-3.4.4/logs/		Directory (Auto Guard)	neo4j						Rekeyed
	demoPolicy		/home/osboxes/testDir/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jData		/home/osboxes/neo4j-enterprise-3.4.4/import/		Directory (Auto Guard)	neo4j						Rekeyed
	neo4jExecute		/home/osboxes/neo4j-enterprise-3.4.4/plugins/		Directory (Auto Guard)	neo4j						Rekeyed

To setup the Neo4j Guard Points, go to the Hosts menu, click on the Neo4j Host, and select the Guard FS tab in the DSM manager.

For each entry shown in the table above, click the “Guard” button. Select the policy from the drop-down, and fill the details out as shown in the table.

Testing / Verification

If everything is configured correctly, then Neo4j will continue to run as normal, and the guard points will have taken effect. This can be verified by switching users on the host and inspecting the filesystem while the system is running:

```
[centos@ip-10-0-0-119 ~]$ ls -l /var/lib/neo4j
ls: cannot access /var/lib/neo4j/data: Permission denied
total 8
drwxr-xr-x. 2 neo4j neo4j   41 Dec 17 13:09 certificates
d?????????? ? ?     ?        ?            ? data
drwxr-xr-x. 2 neo4j neo4j    6 Oct 12 15:14 import
drwxr-xr-x. 2 neo4j neo4j 4096 Dec 29 17:39 metrics
drwxr-xr-x. 2 neo4j neo4j    6 Oct 12 15:14 plugins
[centos@ip-10-0-0-119 ~]$ sudo /bin/bash
[root@ip-10-0-0-119 centos]# whoami
root
[root@ip-10-0-0-119 centos]# ls -l /var/lib/neo4j
total 8
drwxr-xr-x. 2 neo4j neo4j   41 Dec 17 13:09 certificates
```

```
drwxr-xr-x. 4 neo4j neo4j   35 Dec 17 13:08 data
drwxr-xr-x. 2 neo4j neo4j    6 Oct 12 15:14 import
drwxr-xr-x. 2 neo4j neo4j 4096 Dec 29 17:39 metrics
drwxr-xr-x. 2 neo4j neo4j    6 Oct 12 15:14 plugins
```

In the above example, the CentOS user cannot access even the directory metadata about /var/lib/neo4j/data (where the DBMS contents reside) but the root user can.

Neo4j Causal Cluster

Using Vormetric DSM with Neo4j in a Causal Cluster scenario is no different than when Neo4j is running in single mode. Each host must be individually registered