Configure Startup Scripts to Access Encrypted MySQL Databases

This article explains how to configure a Vormetric resource set to securely allow MySQL startup scripts to access encrypted GuardPoints.

Why do startup scripts need access to GuardPoints?

When Linux starts a service, Linux also runs a startup script. The startup script runs when the machine powers on or when a service manually starts. The startup script typically runs tasks that relate to the starting, stopping, and restarting of a service.

For database services, the startup script typically runs tasks that occur in folders that hold database files. With encrypted database files, you must allow the startup script to access the database folders. If not, the database will not start properly, and in some cases, interfere with the power on process for the machine.

As part of the startup process, the operating system needs permission to view and change file / folder ownership and permissions. As a result, if you want to guard **var/lib/mysql**, you must create two rules in your policy.

Common GuardPoints

The system needs to access the commonly guarded (encrypted) folders inside of **/var/lib/mysql**.

Access to GuardPoints

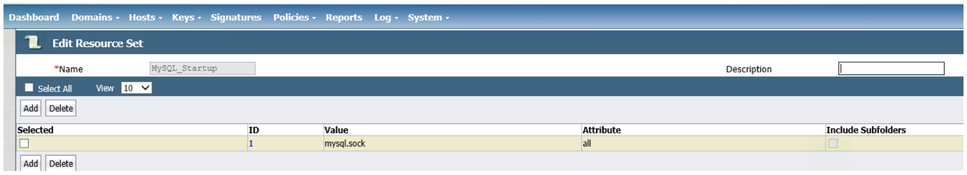
The resource is relative to the GuardPoint. In other words, if the GuardPoint is **/var/lib/mysql**, and you want to allow access to a particular file in that directory, you would only need to specify that specific file in your resource parameter.

For instance if the GuardPoint is **/var/lib/mysql/**, then your resource would only be **mysql.sock**.

Allow startup scripts to access encrypted MySQL databases

> ⚠ In the instructions below, you will create and add two rules to your policy.

1. Log into your DSM as Security Administrator.
2. In the menu bar, click **Polices**, and then click **Manage Policies**.
3. Mark the policy that guards your databases, such as **/var/ib/sql/data**, and then click **Add**.
4. Under **Security Rules**, click **Add**.
5. Next to **Resource**, click **Select**.
6. In the window that appears, click **Add**.
7. In **Name**, enter a descriptive name for your Resource Set.
8. Click **Add** to specify a resource that will need to be accessed in the GuardPoint upon startup.
9. In **Directory**, enter a slash: ****
10. In **File**, enter the mysql.sock file that needs to be accessed upon startup, and then click **Ok**. These resource must be added one at a time.
11. (Optional) To add resources, repeat steps 8 - 10.
12. Mark the newly created Resource Set, and then click **Select Resource Set**. In the window that appears, **Resource** is populated with the newly created Resource Set.



Edit Resource Set

*Name MySQL_Startup

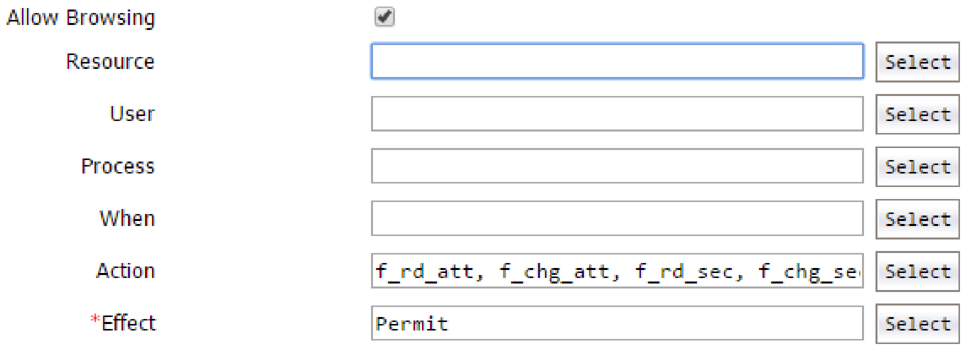
Description

☐ Select All View 10

Selected	ID	Value	Attribute	Include Subfolders
☐	1	mysql.sock	all	☐

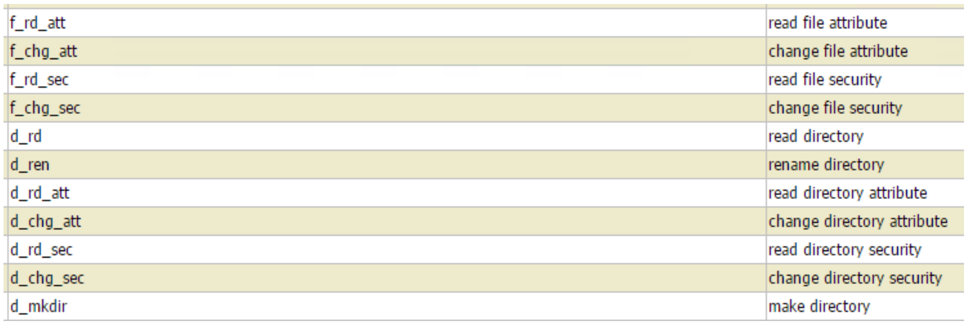
13. Next to **Effect**, click **Select**.
14. Mark **Permit** and **Apply Key**.
15. Click **Select Effect**.
16. Click **Ok**.
17. Mark the rule, and then click **Up** to move the new rule above the catch-all rule.

> ⚠ For your reference you have just created and added the first rule.



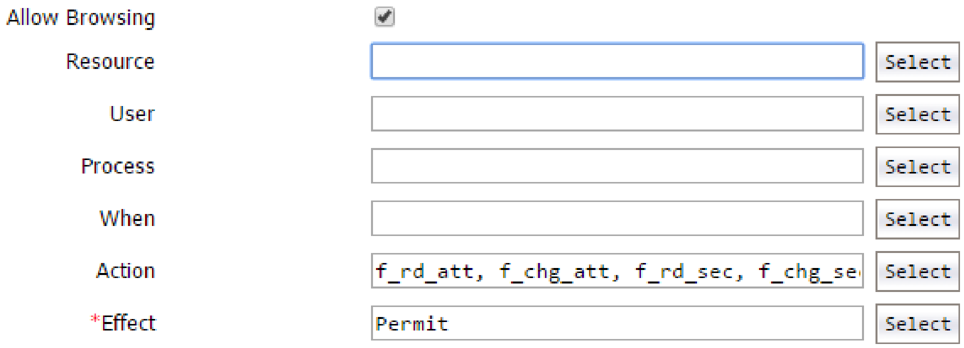
Allow Browsing	☑	
Resource		Select
User		Select
Process		Select
When		Select
Action	f_rd_att, f_chg_att, f_rd_sec, f_chg_se	Select
*Effect	Permit	Select

18. Inside your policy editor, click **Add** to create the second security rule.
19. Next to **Action**, click **Select**.
20. Using the image below for, mark all the rules listed below.



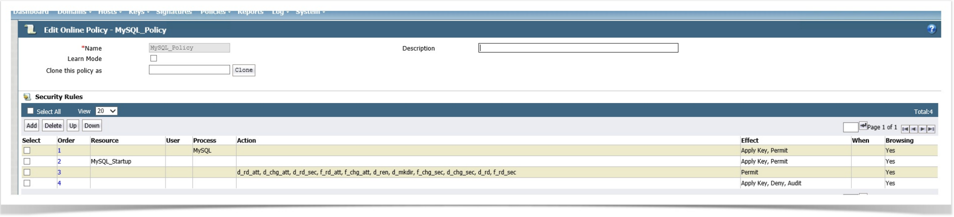
f_rd_att	read file attribute
f_chg_att	change file attribute
f_rd_sec	read file security
f_chg_sec	change file security
d_rd	read directory
d_ren	rename directory
d_rd_att	read directory attribute
d_chg_att	change directory attribute
d_rd_sec	read directory security
d_chg_sec	change directory security
d_mkdir	make directory

21. Click **Select Action**.
22. Next to **Effect**, click **Select**.
23. Mark **Permit**, and then click **Ok**.



Allow Browsing	☑	
Resource		Select
User		Select
Process		Select
When		Select
Action	f_rd_att, f_chg_att, f_rd_sec, f_chg_se	Select
*Effect	Permit	Select

24. Click **Ok**.
25. Mark the rule, and then click **Up** to move the new rule up one entry.



Edit Online Policy - MySQL_Policy

*Name	MySQL_Policy		Description	
Learn Mode	□			
Clone this policy as		Clone		

Security Rules

□ Select All View 20 Total:4

Add Delete Up Down Page 1 of 1

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
□	1			MySQL		Apply Key, Permit		Yes
□	2	MySQL_Startup				Apply Key, Permit		Yes
□	3				d_rd_att, d_chg_att, d_rd_sec, f_rd_att, f_chg_att, d_ren, d_mkdir, f_chg_sec, d_chg_sec, d_rd, f_rd_sec	Permit		Yes
□	4					Apply Key, Deny, Audit		Yes

26. Click **Apply** to save, and then click **Ok.**
27. (Optional) You should test to make sure your system is running properly.

Was this helpful?

Your Rating: ☆☆☆☆☆ Results: ★★★★★ 2 rates