SELinux - Installation Issues

SELinux is a security mechanism that works on top of the native file and directory read/write/execute permissions within the Linux file system. It is available for most Linux distributions and is installed by default in newer RHEL (Red Hat Enterprise Linux) & Fedora distributions.

As SELinux may prevent the installation and/or operation of any software being executed, ensure that you create appropriate policy file for it.

> **Note**
>
> Ensure that you consult with your security team to determine the correct level of access for the APM.

SELinux allows you to set a finer granularity of restrictions on access and execution. This control is represented by "policy files", typically created and maintained by the SecOps team within your organisation. For more details about SELinux see https://selinuxproject.org/page/Main_Page.

The policy files are found in */etc/sestatus.conf* by default. To determine if SELinux is present on your system, run getenforce command which returns the string Enforcing if it is active.

Alternatively, you can run the following command:

```
sestatus
```

The above command produces following output:

```
SELinux status: enabled
SELinuxfs mount: /selinux
Current Mode: permissive
Policy version: 16
sestatus
```

If SELinux status is ***disabled***, it indicates that the system has not installed the package. However, if the status returned is ***enabled***, but the Current Mode is ***permissive***, then SELinux policy files are not enforced. To install and test the APM Agent:

- Set the mode to ***permissive*** and then enable it
- Follow the SELinux guidelines to create the appropriate policy statements for the agent in question

> For more details on how to customize your policy files see https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/sec-sel-policy-customizing.
>
> To enable SELinux, use the command ***setenforce 1*** to enable ***enforcing*** mode; to disable SELInux use ***setenforce 0*** (i.e. set to "***permissive***" mode).
>
> For more details about enabling/disabling SELinux: https://docs.fedoraproject.org/en-US/Fedora/11/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-Enabling_and_Disabling_SELinux.html