Mandiant

CONFIGURE THE LINUX ENVIRONMENT TO SUPPORT INSTALLATION OF THE SECURITY VALIDATION ACTOR

Once you have the OS installed, configure the environment to support the installation of the Actor. This task includes the following items:

- Create or designate a system account to own the Validation Platform programs, data, and log files.
  - Follow your system policy for user account creation, if applicable.
  - This user account must have sudo abilities. This privilege requirement is easily accomplished using a predefined sudoers group. On most Linux systems, members of the wheel group are usually granted sudo access. You can confirm this access by looking at the /etc/sudoers file. For example, you see something like the following:

    ```
    ## Allows users in group wheel to run all commands
    ```

    ```
    %wheel ALL=(ALL) ALL
    ```
  - The user must have non-tty capabilities. This capability is the default behavior, but you can add the following line to explicitly set it (if necessary):

    ```
    Defaults:username !requiretty
    ```
  - The user must have shell capability. If the shell of the user is set to `/bin/nologin`, you won't be able to install the Director or Actors. To configure an interactive shell, you can run the following command:

    ```
    chsh -s /bin/bash postgres
    ```
  - To create and add a new account to the wheel group, use the following command:

    ```
    $ sudo useradd -G wheel username
    ```
  - To add an existing account to the wheel group, use the following command:

    ```
    $ sudo usermod -g wheel username
    ```

    

    For Linux Endpoint Actors, Mandiant recommends installing as root to ensure that all Actions can run as designed. Installing as a non-root user limits the number of Actions that can be run effectively.

- Verify that sudo is enabled and configured correctly.

  

  The Validation Platform creates a sudoers file during installation to support proper functionality. To use this file, your `/etc/sudoers` file must contain `#includedir /etc/sudoers.d`.

  

  Sudo alternatives such as PowerBroker are supported, but are not configured during installation. For the specific access that needs to be provided when using a sudo alternative, review the **contents of the sudoers file. (https://docs.mandiant.com/home/msv-sudo-commands-explained-actor)** This file can also be located here (modify the path if you changed the install location): `/opt/apps/verodin/node/settings/verodin_sudoers`.

- For your management interface, ensure that ports 443 and 22 are not blocked by the system's firewall rules.

  

  Consult your system documentation for details about allowing traffic for those ports and about making the configuration persist across reboots.

Port 22 is used to communicate with the system through SSH. Port 443 allows the HTTPS protocol, which is how your browser communicates with the Director and how the Director communicates with Actors. You can check your system's firewall rules by using the following command:

- RHEL 8-9 or CentOS 9

```
$ sudo nft list ruleset
```

- All other supported operating systems

```
$ sudo iptables --list
```

- Determine if you have access to your operating system's software repositories. This access could be directly through the internet or to a repository that your company maintains. For more information about using a repository, see **Handling Software Dependencies (https://docs.mandiant.com/home/msv-handling-software-dependencies)**.