Barracuda XDR - SentinelOne Linux Installation

Prerequisites

1. Ensure the device meets the system requirements.
    a. 2 GHz Dual-core CPU
    b. 4 GB RAM * subject to change depending on distro requirements.
    c. 2GB in /opt/sentinelone. 3GB is recommended.
    d. Instruction-supported CPU: SSE4_2
        i. SSE4a is not supported.
    e. If the Linux OS is customized:
        i. Get the list of requirements using one of the below commands:
        ii. rpm -qRp SentinelAgent_installerFileName.rpm
        iii. dpkg -I SentinelAgent_installerFileName.deb
2. The Linux Agent is compiled with 64-bit kernel and libraries. It supports Intel x86_64 compatible architecture and x64 hardware. ARM 64-bit architecture (also known as aarch64) is supported starting with Agent version 22.1.
    a. The Linux Agent does not support:
    b. 32-bit architecture
    c. CPU micro-architectures such as ppc64, x86_32, RISC, or MIPS
    d. UNIX OS version such as FreeBSD, AIX, or Solaris
3. Get the correct token to register the agent against the management console.
4. Make sure the machine does **NOT** reboot before you complete the full installation, association, and activation.
5. Confirm that you have the correct installer for your system and architecture.
    a. Installation of the Linux ARM Agent is the same as for the Linux Agent on x86, but make sure you use the correct installer. The Linux Agent uses the RPM and DEB package formats for both x86 and ARM. The x86 package **will not** install on ARM endpoints, and the ARM installer **will not** install on x86 endpoints.

i. If your package says “aarch64”, you are utilizing an installer tailored for the ARM architecture. If your device is not using ARM, please reach out for the correct installer.

b. RPM installation requires the --nodigest switch to prevent this error:

i. Package SentinelAgent_linux_version does not verify: no digest.

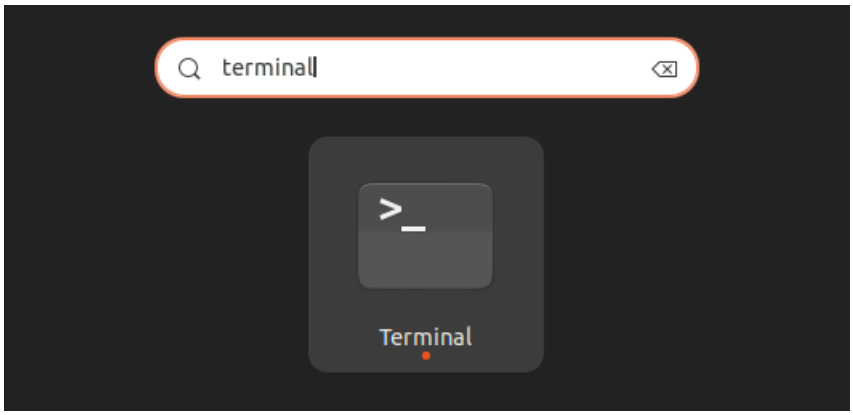
c. If you use yum to install on RHEL 8.2, the signed RPM installer is required.

6. If you are using SELinux, please reach out for the policy script for configuring SELinux.

Installing the Agent with dpkg

We are using Ubuntu 22.0.4.1 LTS for this guide.

1. Download the installer.
2. Open the terminal



3. CD into the directory where the installer is
   a. For example, if it is in the Downloads directory, you can use:

      cd ~/Downloads/

4. Perform the command:

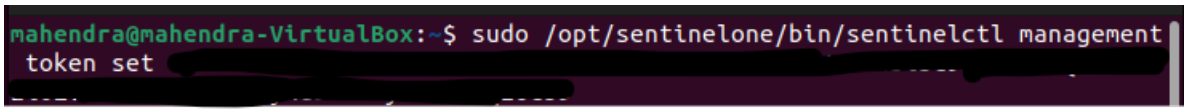
   sudo dpkg -I “PACKAGE NAME”

   You can use tab to auto-complete.

```
mahendra@mahendra-VirtualBox:~/Downloads$ sudo dpkg -i SentinelAgent_linux_v23_1_2_9.deb
```

5. If you are utilizing SELinux, you should have received the policy script from us by reaching out during the prerequisites phase.
6. Run the below command with the site token you have received:

sudo /opt/sentinelone/bin/sentinelctl management token set site_token



7. Start the agent services

   Run **sudo /opt/sentinelone/bin/sentinelctl control start**.

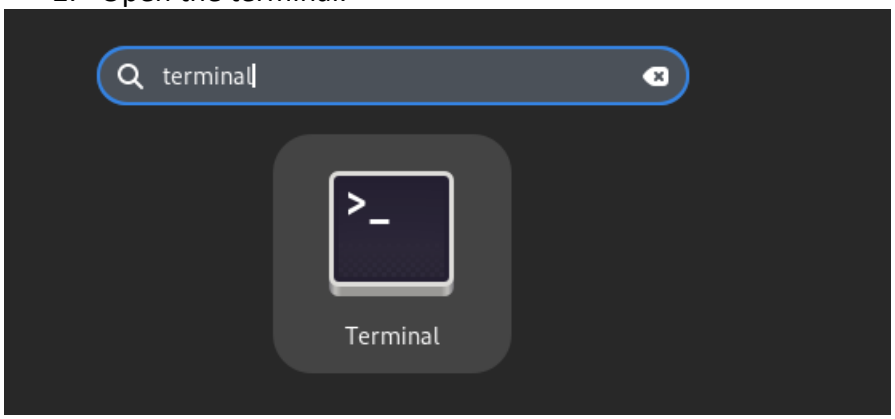
8. After a few minutes, check the Agent status. Other software may interfere with the startup.

   Run sudo /opt/sentinelone/bin/sentinelctl control status.

Installing the Agent with rpm

We are using Fedora Workstation 38 for this guide.

1. Download the installer.
2. Open the terminal.



3. CD into the directory that holds the package.

```
[mahendra@fedora ~]$ cd ~/Desktop
[mahendra@fedora Desktop]$ ls -la
total 88
drwxr-xr-x. 1 mahendra mahendra    66 Jul 12 17:06 .
drwx------. 1 mahendra mahendra   434 Jul 12 17:06 ..
-rw-r--r--. 1 mahendra mahendra 88131 Jul 12 17:05 SentinelAgent_linux_v23_1_2_9.rpm
[mahendra@fedora Desktop]$
```

4. Install the package.

   sudo rpm -i --nodigest package_pathname

   –nodigest is used to prevent the hash verification error.

5. Associate the Agent with the Management Console with the Group or Site Token.

   Run sudo /opt/sentinelone/bin/sentinelctl management token set site_token.

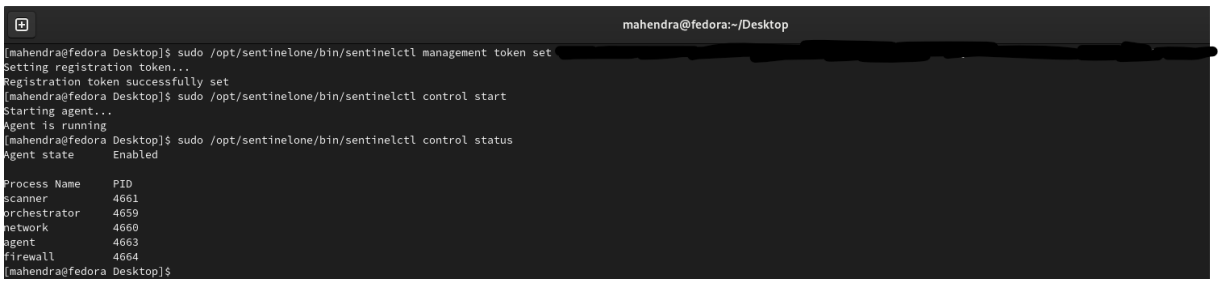
6. If you are utilizing SELinux, you should have received the policy script from us by reaching out during the prerequisites phase.

7. Start the agent services

   Run **sudo /opt/sentinelone/bin/sentinelctl control start**.

8. After a few minutes, check the Agent status. Other software may interfere with the startup.

   Run sudo /opt/sentinelone/bin/sentinelctl control status.



Scripting – Ansible

You can use a configuration file and Ansible to install the agent on multiple endpoints.

If you are looking to script the installation using Ansible, there is configurable code to perform this. Please reach out to the SOC for us to provide it to you.

Scripting – Deploying the Linux Agent with a Configuration File

You can create a configuration file to set environment variables that the agent can pull from during installation.

Version 21.5 of the Linux Agent supports an easier deployment. Rather than run the commands to install, associate, activate, and then set a proxy, you can set one configuration file to use these variables. Please reach out to the SOC for assistance with this.