Documentation › User manual › Capabilities › Agentless monitoring › How it works

How it works

Connection

First of all, agentless monitoring must be enabled:

```
/var/ossec/bin/ossec-control enable agentless
```

In order to connect the manager to the device using SSH authentication, the following script should be used: `register_host.sh`, which is located in: `/var/ossec/agentless/` This script has two options: `list` and `add`.

Using the `list` option will list all hosts already included.

```
/var/ossec/agentless/register_host.sh list
```

Using the `add` option will specify a new device to be added to the manager. `NOPASS` may be entered as the password to use public key authentication rather than using a password. For Cisco devices, such as routers or firewalls, `enablepass` should be used to specify the enable password.

```
/var/ossec/agentless/register_host.sh add root@example_address.com example_password [enablepass]
```

Public key authentication can be used with the following command:

```
sudo -u ossec ssh-keygen
```

Once created, the public key must be copied into the remote device.

Monitoring

After devices have been added to the list, the manager must be configured to monitor them. To view additional configuration options for the `ossec.conf` file, please refer to agentless.

The four types of agentless checks.

BSD Integrity Check

For BSD systems, set the `type` as `ssh_integrity_check_bsd` as referenced below. A space-separated list of directories may be referenced in the configuration section using the arguments tag. Using this configuration, Wazuh will do an integrity check on the remote box.

```
<agentless>
  <type>ssh_integrity_check_bsd</type>
  <frequency>20000</frequency>
  <host>root@test.com</host>
  <state>periodic</state>
  <arguments>/bin /var/</arguments>
</agentless>
```

Linux Integrity Check

For Linux systems, set the `type` as `ssh_integrity_check_linux` as referenced below. A space-separated list of directories may be referenced in the configuration section using the arguments tag. Using this configuration, Wazuh will do an integrity check on the remote box.

```
<agentless>
  <type>ssh_integrity_check_linux</type>
  <frequency>36000</frequency>
  <host>root@test.com</host>
  <state>periodic</state>
  <arguments>/bin /etc/ /sbin</arguments>
</agentless>
```

Generic Diff

A set of commands can also be configured to run on a remote device. Wazuh will alert you if the output of those commands changes. In order to use this option, set `type` as `ssh_generic_diff`, as shown below.

```
<agentless>
  <type>ssh_generic_diff</type>
  <frequency>20000</frequency>
  <host>root@test.com</host>
  <state>periodic_diff</state>
  <arguments>ls -la /etc; cat /etc/passwd</arguments>
</agentless>
```

> **Note**
>
> To use `su` in a command as an argument, `use_su` must be set before the hostname. In the previous example, this would appear as: `<host>use_su root@example_address.com</host>`

Pix config

This option will alert if a Cisco PIX/router configuration changes. Set the `type` to `ssh_pixconfig_diff`, as shown below.

```
<agentless>
  <type>ssh_pixconfig_diff</type>
  <frequency>36000</frequency>
  <host>pix@pix.fw.local</host>
  <state>periodic_diff</state>
</agentless>
```

Checking the setup

Finally, the `expect` package must be present on the manager for this feature to work.

When the `expect` package is present and Wazuh is restarted, the following is shown in the `/var/ossec/logs/ossec.log` file:

```
ossec-agentlessd: INFO: Test passed for 'ssh_integrity_check_linux'.
```

When Wazuh has connected to the remote device, the following will be shown in the same log file:

```
ossec-agentlessd: INFO: ssh_integrity_check_linux: root@example_adress.com: Starting.
ossec-agentlessd: INFO: ssh_integrity_check_linux: root@example_adress.com: Finished.
```

Alert

Once configured as above, Wazuh alerts will be triggered when changes occur within the directories, configuration or outputs based on the above examples:

Examples of alerts are as follows:

Integrity check BSD/Linux example alert:

```
** Alert 1486811998.93230: - ossec,syscheck,pci_dss_11.5,
2017 Feb 11 03:19:58 ubuntu->(ssh_integrity_check_linux) root@192.168.1.3->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: '/etc/.hidden'
Size changed from '0' to '10'
Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e'
New md5sum is : 'cc7bd56aba1122d0d5f9c7ef7f96de23'
Old sha1sum was: 'da39a3ee5e6b4b0d3255bfef95601890afd80709'
New sha1sum is : 'b570fbdf7d6ad1d1e95ef57b74877926e2cdf196'

File: /etc/.hidden
Old size: 0
New size: 10
New permissions:   1204
New user: 0
New group: 0
Old MD5: d41d8cd98f00b204e9800998ecf8427e
New MD5: cc7bd56aba1122d0d5f9c7ef7f96de23
Old SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709
New SHA1: b570fbdf7d6ad1d1e95ef57b74877926e2cdf196
```

Generic Diff example alert:

```
** Alert 1486811190.88243: - ossec,syscheck,agentless,pci_dss_11.5,pci_dss_10.6.1,
2017 Feb 11 03:06:30 ubuntu->(ssh_generic_diff) root@192.168.1.3->agentless
Rule: 555 (level 7) -> 'Integrity checksum for agentless device changed.'
ossec: agentless: Change detected:
3c3
< drwxr-xr-x. 77 root root    8192 Feb 27 10:44 .
---
> drwxr-xr-x. 77 root root    8192 Feb 27 10:47 .
176a177
> -rw-r--r--.  1 root root       0 Feb 27 10:47 test
```