ORACLE

Using Advanced Intrusion Detection Environment with Oracle Linux Automation Manager

Technical Paper

May, 2022, Version 1.0

Purpose statement

This document provides an overview of how to integrate Advanced Intrusion Detection Environment (AIDE), which is an open source file and directory integrity checking utility, with Oracle Linux Automation Manager to automate checking configuration inconsistencies across a large number of hosts. This combination helps avoid configuration drift and increases the security of Linux systems.

Table of contents

Using Advanced Intrusion Detection Environment (AIDE) with Oracle Linux Automation Manager (OLAM)

Overview

Configuration drift, whether by the installation of a software package or the accidental or intentional edit of a key configuration file, can cause lost productivity and downtime as engineers troubleshoot code and operating system environments trying to identify the cause of unexpected behavior. An example could be the installation of an rpm or an edit to the sshd_config file allowing root login. Configuration drift could also be a sign of a security breach; the unexpected addition of files, software, or changed configuration may be a sign of an attack, or may open the door to an attack. Identifying file system changes that should not have happened is among one of the best solutions for configuration drift. The use of Oracle Linux Automation Manager and AIDE is a powerful combination for addressing configuration drift.

The Advanced Intrusion Detection Environment (AIDE) is a file and directory integrity checking utility which can be an effective warning system. AIDE takes a "snapshot" of the state of the system, this "snapshot" is used to build a database. When an administrator wants to run an integrity test, AIDE compares the database against the current status of the system. Should a change have happened to the system between the snapshot creation and the test, AIDE will detect it and report it.

AIDE has the following capabilities:

- Monitors file system permissions, inode, user, group, file size, mtime, atime, ctime, links and growing size
- Supports multiple checksums and hashes
- Configuration files stored in plain text
- Rules, variables, and macros that can be customized to local site or system policies
- Powerful regular expression support to selectively include or exclude files and directories to be monitored

AIDE is available for installation from both the Unbreakable Linux Network (ULN) and the Oracle Linux yum server repositories. Once AIDE is installed and initialized, a baseline must be created. This baseline is usually best created after a server's operating environment has been installed and configured to site specific requirements. Once the baseline is created, AIDE can report on inconsistencies. A baseline can also be re-created if, for example, a new software package is required to be installed. The following documentation (Chapter 4.10) is available with respect to the installation and usage of AIDE with Oracle Linux. My Oracle Support subscribers can refer to this My Oracle Support Note.

Oracle Linux Automation Manager and Oracle Linux Automation Engine are the latest additions to the Oracle Linux operating environment. Together, they provide a cost-effective, powerful, scalable, and secure infrastructure automation framework for enterprise environments. Additionally, they enable infrastructure as code, streamlining software provisioning. Also enabling configuration management, and application deployment, which in turn reduces deployment errors, time to resolve problems, and increases compliance with security, privacy, and other policies. Oracle Linux Automation Manager and Engine, based upon the open source AWX and Ansible projects respectively, are included with an Oracle Linux Premier Support subscription.

The remainder of this paper provides examples of using AIDE and Oracle Linux Automation Manager.

Installation and configuration of AIDE using Oracle Linux Automation Manager

The example files below need to exist within a Project on the Oracle Linux Automation Manager either in a GIT repository or stored locally. The target Oracle Linux 8 host needs to be part of the Oracle Linux Automation Manager inventory and Credentials must exist (with sudo enabled). Finally, Templates are created to drive the playbooks created in YAML format. For further information on Oracle Linux Automation Manager please refer to the Getting Started Guide.

The install and configure playbook which runs on an Oracle Linux 8 host will perform the following:

- Become the superuser.
- Check if the AIDE database exists. This is needed for idempotency, and will fail if the AIDE database exists.
- Install the AIDE package.
- Initialize AIDE, create a baseline, and enable the database.

A successful install would contain these sections of output from the Template Job:

```
TASK [Check if the aide database exists] ************************************ 12:48:55
ok: [129.159.      ]
ok: [10.0.      ]

TASK [Fail if aide database exists] ***************************************** 12:48:56
skipping: [10.0.      ]
skipping: [129.159.      ]

TASK [Install aide package] ************************************************* 12:48:56
changed: [129.159.      ]
changed: [10.0.      ]

TASK [Initialise aide] ****************************************************** 12:49:00
changed: [129.159.      ]
changed: [10.0.      ]

TASK [debug] **************************************************************** 12:49:18
ok: [10.0.      ] => {
    "command_output": {
        "changed": true,

TASK [Enable Database for aide] ********************************************* 12:49:18
changed: [129.159.      ]
changed: [10.0.      ]

PLAY RECAP ****************************************************************** 12:49:18
10.0.                      : ok=6    changed=3    unreachable=0    failed=0    skippe
d=1    rescued=0    ignored=0
129.159.                   : ok=6    changed=3    unreachable=0    failed=0    skippe
d=1    rescued=0    ignored=0
```

Image 1. Example of successful AIDE installation

A failed job where AIDE was already installed would contain these sections of output from the Template Job:

```
TASK [Fail if aide database exists] ******************************************* 12:50:15
fatal: [10.0.    ]: FAILED! => {"changed": false, "msg": "The aide database exists, t
herefore aide is installed, we need to exit"}
fatal: [129.159.      ]: FAILED! => {"changed": false, "msg": "The aide database exist
s, therefore aide is installed, we need to exit"}

PLAY RECAP ******************************************************************** 12:50:15
10.0.                    : ok=2    changed=0    unreachable=0    failed=1    skippe
d=0    rescued=0    ignored=0
129.159.                 : ok=2    changed=0    unreachable=0    failed=1    skippe
d=0    rescued=0    ignored=0
```

Image 2. Example of unsuccessful AIDE installation

The example installaide.yaml file:

```
---
- hosts: all
  become: yes
  tasks:
  - name: Check if the aide database exists
    stat:
      path: /var/lib/aide/aide.db.gz
    register: p
  - name: Fail if aide database exists
    fail:
      msg: The aide database exists, therefore aide is installed, we need to exit
    when: p.stat.exists
  - name: Install aide package
    yum:
      name: aide
      state: present
  - name: Initialise aide
    command: aide --init
    register: command_output
  - debug: var=command_output
  - name: Enable Database for aide
    command: mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Check the current AIDE configuration for inconsistencies using Oracle Linux Automation Manager

The check playbook which runs on an Oracle Linux 8 host will perform the following:

- Become the superuser
- Run the aide check command and report the result
- If no differences are found, then report no differences and pass the job
- If differences are found, then report differences and fail the job

The job needs to fail to alert users if differences are found.
A successful result, meaning there are no inconsistencies would contain these sections of output from the Template Job:

```
TASK [Run aide check] ********************************************************** 14:37:56
changed: [129.159.      ]
changed: [10.0.     ]

TASK [Report Aide OK] ********************************************************** 14:38:16
ok: [10.0.     ] => {
    "msg": "AIDE found NO differences between database and filesystem. Looks oka
y!!"
}
ok: [129.159.      ] => {
    "msg": "AIDE found NO differences between database and filesystem. Looks oka
y!!"
}

PLAY RECAP ********************************************************************* 14:38:16
10.0.      : ok=3    changed=1    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0
129.159.      : ok=3    changed=1    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0
```

Image 3. Example of successful AIDE check

An unsuccessful result, meaning there are inconsistencies, would cause a job failure and would contain these sections of output from the Template Job. Notice that on two hosts one of them fails due to someone editing the sshd_config file:

```
TASK [Run aide check] ********************************************************** 16:00:12
fatal: [129.159.      ]: FAILED! => {"changed": true, "cmd": ["aide", "--check"], "delta":
"0:00:15.960109", "end": "2022-03-01 16:00:29.243427", "msg": "non-zero return code", "r
c": 4, "start": "2022-03-01 16:00:13.283318", "stderr": "", "stderr_lines": [], "stdout":
"Start timestamp: 2022-03-01 16:00:13 +0000 (AIDE 0.16)\nAIDE found differences between da
tabase and filesystem!!\n\nSummary:\n  Total number of entries:\t170977\n  Added entries:\
t\t0\n  Removed entries:\t\t0\n  Changed entries:\t\t1\n\n
---------------------------------------------\nChanged entries:\n
---------------------------------------------\n\nf   ...    .C... : /etc/ssh/sshd_co
nfig\n\n---------------------------------------------\nDetailed information about ch
anges:\n---------------------------------------------\n\nFile: /etc/ssh/sshd_config\
n  SHA512   : hDwrdWOgi+8cQO3RnPhxzirdFkVHtu// | LKTVib5D/MNjlJqriwyVPQ7KYCiWhZ/1\n
UXdCez/N8Ihgbx6ylnuxDa3kej8S/OGr | n9xKrqixGSj8oetINk5Sp8pYIs4GGT//\n   …
changed: [10.0.     ]

TASK [Report Aide OK] ********************************************************** 16:00:32
ok: [10.0.     ] => {
    "msg": "AIDE found NO differences between database and filesystem. Looks oka
y!!"
}
```

Image 4. Example of unsuccessful AIDE check, inconsistencies identified (1 of 3)

```
TASK [Report Aide Error] ********************************************************** 16:00:33
ok: [129.159.      ] => {
    "msg": "AIDE found differences between database and filesystem!!"
}

TASK [Force a failure] ************************************************************ 16:00:33
fatal: [129.159.      ]: FAILED! => {"changed": true, "cmd": ["/bin/false"], "delta": "
0:00:00.001852", "end": "2022-03-01 16:00:33.358757", "msg": "non-zero return code", "r
c": 1, "start": "2022-03-01 16:00:33.356905", "stderr": "", "stderr_lines": [], "stdou
t": "", "stdout_lines": []}

PLAY RECAP ************************************************************************ 16:00:33
10.0.                      : ok=3    changed=1    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0
129.159.                   : ok=2    changed=0    unreachable=0    failed=1    skippe
d=0    rescued=1    ignored=0
```

Image 5. Example of unsuccessful AIDE check, inconsistencies identified (2 of 3)

A further example where a user installed HTTPD on both hosts:

```
TASK [Run aide check] ************************************************************ 12:51:04
fatal: [129.159.      ]: FAILED! => {"changed": true, "cmd": ["aide", "--check"], "delta":
"0:00:15.814623", "end": "2022-03-01 12:51:20.248391", "msg": "non-zero return code", "r
c": 5, "start": "2022-03-01 12:51:04.433768", "stderr": "", "stderr_lines": [], "stdout":
"Start timestamp: 2022-03-01 12:51:04 +0000 (AIDE 0.16)\nAIDE found differences between da
tabase and filesystem!!\n\nSummary:\n  Total number of entries:\t171542\n  Added entries:\
t\t565\n  Removed entries:\t\t0\n  Changed entries:\t\t8\n\n
---------------------------------------------------\nAdded entries:\n
---------------------------------------------------\n\nd++++++++++++++++: /etc/httpd/conf\
nf++++++++++++++++: /etc/httpd/conf/httpd.conf\nf++++++++++++++++: /etc/httpd/conf/magic\n
f++++++++++++++++: /etc/httpd/conf.d/autoindex.conf\nf++++++++++++++++: /etc/httpd/conf.d/
userdir.conf\nf++++++++++++++++: /etc/httpd/conf.d/welcome.conf\nf++++++++++++++++: /etc/h
ttpd/conf.modules.d/00-base.conf\nf++++++++++++++++: /etc/httpd/conf.modules.d…
fatal: [10.0.      ]: FAILED! => {"changed": true, "cmd": ["aide", "--check"], "delta": "0:0
0:19.344683", "end": "2022-03-01 12:51:23.818977", "msg": "non-zero return code", "rc": 5,
"start": "2022-03-01 12:51:04.474294", "stderr": "", "stderr_lines": [], "stdout": "Start
timestamp: 2022-03-01 12:51:04 +0000 (AIDE 0.16)\nAIDE found differences between database
and filesystem!!\n\nSummary:\n  Total number of entries:\t145699\n  Added entries:\t\t565\
n  Removed entries:\t\t0\n  Changed entries:\t\t8\n\n
---------------------------------------------------\nAdded entries:\n
---------------------------------------------------\n\nd++++++++++++++++: /etc/httpd/conf\
nf++++++++++++++++: /etc/httpd/conf/httpd.conf\nf++++++++++++++++: /etc/httpd/conf/magic\n
f++++++++++++++++: /etc/httpd/conf.d/autoindex.conf\nf++++++++++++++++: /etc/httpd/conf.d/
userdir.conf\nf++++++++++++++++: /etc/httpd/conf.d/welcome.conf\nf++++++++++++++++: /etc/h
ttpd/conf.modules.d/00-base.conf\nf++++++++++++++++: /etc/httpd/conf.modules.d/00-d…

TASK [Report Aide Error] ********************************************************** 12:51:23
ok: [10.0.      ] => {
    "msg": "AIDE found differences between database and filesystem!!"
}
ok: [129.159.      ] => {
    "msg": "AIDE found differences between database and filesystem!!"
}
```

Image 6. Example of unsuccessful AIDE check, inconsistencies identified (3 of 3)

The example checkaide.yaml file:

```
---
- hosts: all
  become: yes
  tasks:
  - name: Gather aide state
    block:
      - name: Run aide check
        command: aide --check
        register: result
      - name: Report Aide OK
        debug:
          msg: AIDE found NO differences between database and filesystem. Looks okay!!
        when: result.rc == 0
    rescue:
      - name: Report Aide Error
        debug:
          msg: AIDE found differences between database and filesystem!!
      - name: Force a failure
        command: /bin/false
```

Create a new AIDE baseline using Oracle Linux Automation Manager

A new service requirement may need multiple hosts to have additional software installed and configured, following this installation and configuration any subsequent AIDE checks will fail. The create new baseline playbook which runs on an Oracle Linux 8 host will perform the following:

- Become the superuser
- Run the initialize aide command
- Re-enable the database

A successful result, would contain these sections of output from the Template Job:

```
TASK [Initialise aide] ********************************************************* 14:37:13
changed: [129.159.      ]
changed: [10.0.     ]

TASK [Enable Database for aide] ************************************************ 14:37:31
changed: [129.159.      ]
changed: [10.0.     ]

PLAY RECAP ********************************************************************* 14:37:31
10.0.                      : ok=3    changed=2    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0
129.159.                   : ok=3    changed=2    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0
```

Image 7. Example output while creating new AIDE baseline

The example aide_create_new_baseline.yaml file:

```
---
- hosts: all
  become: yes
  tasks:
  - name: Initialise aide
    command: aide --init
  - name: Enable Database for aide
    command: mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Remove the AIDE configuration using Oracle Linux Automation Manager

If it is necessary to remove the AIDE configuration from multiple hosts, then the remove aide playbook which runs on an Oracle Linux 8 host will perform the following:

- Become the superuser
- Remove the AIDE package
- Clean up the AIDE file system

A successful result, would contain these sections of output from the Template Job:

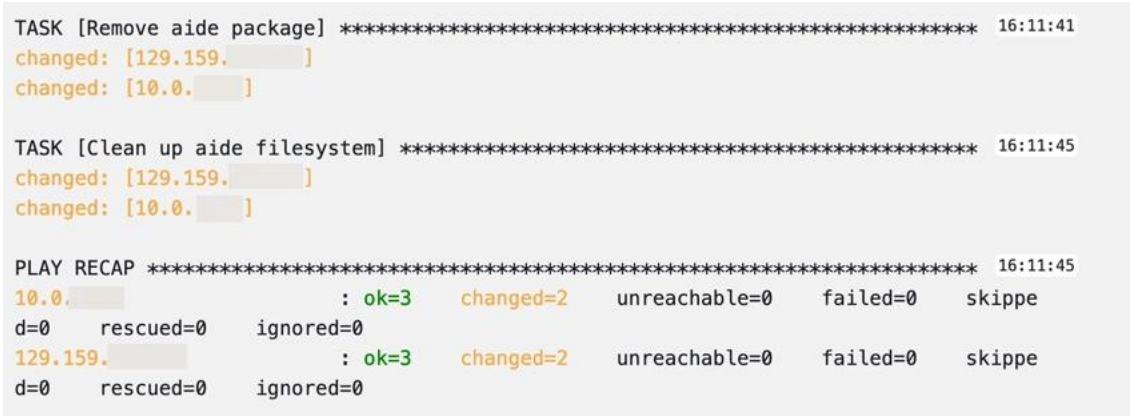

Image 8. Example output of removing AIDE configuration

The example removeaide.yaml file:

```
---
- hosts: all
  become: yes
  tasks:
  - name: Remove aide package
    yum:
      name: aide
      state: absent
  - name: Clean up aide filesystem
    file:
      path: /var/lib/aide
      state: absent
```

Summary

AIDE brings the following additional benefits to Oracle Linux Automation Manager possible across large numbers of hosts:

- Automated, repeatable, error free, and idempotent install of initial baseline configuration
- Scheduled, cadence-based, repeating report of inconsistencies
- Easily updated baseline for planned configuration changes
- Simple fixing of reported issues using playbooks such as reset firewalls or set back configuration files

An administrator may make a change to a server's operating environment which although small could result in a configuration that deviates from one that is considered secure and compliant. This small change could have potentially catastrophic consequences and detrimental effects on an organization. Configuration-drifted systems that continue supporting key services and go unnoticed and unrectified are very vulunerable to system outages, service issues due to misconfiguration, and security vulnerabilities.

AIDE together with Oracle Linux Automation Manager offer an extremely effective warning system for configuration drift.