OSSEC Installation for Windows Clients

INTRODUCTION

OSSEC is a host-based Intrusion Detection system, with the following core functionality:

- Log Monitoring and Collection
- File Integrity Checking
- Windows Registry Integrity Checking
- Active Response

The currently supported version of OSSEC distributed with AlienVault USM/OSSIM is 2.8. AlienVault OSSIM/USM integrates OSSEC as a key component for providing extended visibility to monitored systems via these functions and to assign in Identity Management - mapping User Accounts to Actions via the information gathered by OSSEC.

OSSEC operates via server/agent architecture, with some limited support for agentless operation with certain operating systems for log retrieval only.

Agents are deployed to client systems and run as a continuous in-memory service, communicating with the central server via UDP port 1514

Agent/Server authentication is done via Keys, which resemble the following:

6687cf219a97c5ccf5b476f1f1283bfe18901c12516b3c124dd0e8ae78a46fd2

PREREQUISITES

There are three main components needed in order to perform bulk deployments of the OSSEC Agent to windows clients:

- OSSEC Installation File
- Client Key List - From AlienVault Server
- AlienVault OSSEC Deployment Kit

The OSSEC Client will be required to be downloaded from the OSSEC website by clicking on the links below:

OSSEC Direct Download:

OSSEC Agent version 2.8
Ossec-agent-win32-2.8

The AlienVault OSSEC Deployment Kit can be downloaded form the following link.
Download AlienVault OSSEC Deployment Kit

ADDING CLIENTS TO USM

- Create a CSV file with IP and hostname using the following format "**IP,NAME**"

Example:
192.168.1.100,CLIENT001
192.168.1.101,CLIENT002
192.168.1.102,CLIENT003

Copy list file into AlienVault at the following location **/var/ossec**

NOTE: To add agents on a DHCP environment use the network CIDR on the IP field.
Example:
192.168.1.0/24,CLIENT001

- Import client list by running the following command:
  /var/ossec/bin/manage_agents -f /"Filename"

You should see an output similar to the one below for each client that gets added to the AlienVault Database

```
Bulk load file: /filename
Opening: [/filename]
Agent information:
   ID:001
   Name:CLIENT001
   IP Address:192.168.1.100
Agent added.
```

- Verify agents were created successfully by executing the following command
  /var/ossec/bin/manage_agents –l

You should see an output similar to the one bellow

```
Available agents:
   ID: 001, Name: CLIENT001, IP: 192.168.1.100
   ID: 002, Name: CLIENT002, IP: 192.168.1.101
   ID: 003, Name: CLIENT003, IP: 192.168.1.102
```

- Restart OSSEC Service by executing the following command:
  /var/ossec/bin/ossec-control restart

- Verify OSSEC services are running by executing the following command:
  /var/ossec/bin/ossec-control status

- Copy the **client.keys** file located under **/var/ossec/etc** to your machine in the same location as the deployment kit and name it **client.list**

- Open **Config.ini** provided inside "AlienVault OSSEC Deployment Kit" and enter the server/sensor IP address where the clients will communicate.

Example:
[AVCONFIG]
Server=192.168.1.8

All needed configuration is now completed, make sure all files on this list are in the same location during deployment.

1. **AV-Ossec.exe**
2. **CLIENT.LIST**
3. **CONFIG.INI**
4. **Ossec-agent.XXX.exe**

- Configure your deployment tool to run **AV-Ossec.exe**
  The AlienVault OSSEC Deployment kit will run silently on the client machine, configure client communication settings and install the client key.

NOTES:
For testing purposes manually execute av-ossec.exe to verify deployment works ok.
There is built in error checking on the deployment tool that will validate the following:

1. **ossec-agent setup exist in deployment directory.**
2. **Config.ini is configured with server address**
3. **Config.ini exist in deployment directory**
4. **Client.list exist in deployment directory.**

Make sure to create a client.list duplicate somewhere else while testing as the tool will delete the list once it extract the client data for security purposes.