Title:

# **Install and Configure PSAD**

Description:

Workflow for handling packages related to the installation of PSAD. This bundle has dependency on Core and Validation KI bundles. For more information related to PSAD and related installation steps, please check https://www.thefanclub.co.za/how-to/how-install-psad-intrusion-detection-ubuntu-1204-lts-server

Readme

**Important**: The Knowledge Items of this bundle try to simulate Workflows seen in frameworks such as Chef, Puppet and Ansible.

For this reason, Workflow KIs seem to not follow traditional best practices of KI Creation in terms of reusability. They are, however atomic pieces of knowledge, meaning the knowledge cannot be broken down further while still maintaining the same level of functionality.

Due to the controlled nature of the Workflow approach, the Workflow KIs try to structure Tasks like steps in a sequence rather than letting AutoPilot pick the path to a solution.

In order to simulate these Workflows, the Knowledge Items are split into 3 groups:

* Workflow KIs
* Validation KIs and
* Core KIs.

This bundle intends to install PSAD with all its related application and libraries on the given host.

Dependencies

1. Core KIs bundle
2. Validation KIs bundle

For this bundle to run, you will need MARS nodes in AutoPilot engine. For your reference, please see sample nodes below (at the end of this readme).

Steps to run

1. Put the validation KIs bundle in AutoPilot engine
2. Put the core KIs bundle in AutoPilot engine
3. Put the Workflow KI PSADWorkflowHandlePKG.xml (attached with this bundle) in AutoPilot engine
4. Put the Issue in AutoPilot engine to trigger this KI
   * For your reference, please see sample issue below
5. This will trigger the KI and run the workflow to install PSAD on your machine (as specified in the Issue)

Workflow KI in this bundle, runs below installation steps (as per the link mentioned in the description) on the target machine (as specified in the Issue)

1. Download psad tar file
2. Extract psad tar file
3. Rename install.answers.example file
4. Install psad
5. Configure INPUT iptables
6. Configure FORWARD iptables
7. Configure syslog in psad.conf file
8. Configure EmailID in psad.conf file
9. Configure Hostname in psad.conf file
10. Configure PORT in psad.conf file
11. Restart the PSAD service
12. Update psad's signature
13. Update psad

Sample Issue

Issue:

NodeID: OpexSoftware:Workflow:Application:PSADApplication

xmlns: http://www.arago.de/IssueSchema

IssueSubject: 'Please Install and Configure PSAD'

PSADWorkflowHandlePKG:

TargetApp: PSADApplication

TargetMachine: Puja

TargetState: Created

EmailID: pujasalampuria@gmail.com

HostName: puja-Inspiron-3542

TargetTarFileName: psad-2.2.tar.gz

TargetPath: /tmp/.psad

DownloadUrl: http://cipherdyne.org/psad/download/psad-2.2.tar.gz

UntarFolder: psad-2.2

User: puja

Host: 192.168.1.86

Machine Node

<Linux xmlns="http://mars-o-matic.com" ID="OpexSoftware:Workflow:Machine:Puja"

HasAgentType\_WatchMe="False" MachineArchitecture="x86\_64"

NodeType="Machine" MachineClass="Linux" NodeName="Puja">

<Dependencies>

<Node ID="OpexSoftware:Workflow:Software:PSAD" />

</Dependencies>

<CustomerInformation ID="opex.com" Name="opex"/>

<Extensions>

<ssh User="puja" />

<PasswordPolicy MinLength="8" MaxLength="14" CharSet="alnum" />

</Extensions>

<OSInformation Name="Ubuntu" MajorVersion="14" Vendor="Ubuntu" />

<NetworkInformation>

<InterfaceInformation>

<Interface Name="eth1" IP="172.27.220.23" />

</InterfaceInformation>

</NetworkInformation>

</Linux>

Software Node

<AutoPilot xmlns="http://mars-o-matic.com" ID="OpexSoftware:Workflow:Software:PSAD"

NodeType="Software" SoftwareClass="Automation"

SoftwareSubClass="AutoPilot" NodeName="PSAD">

<Dependencies>

<Node ID="OpexSoftware:Workflow:Machine:Puja" />

<Node ID="OpexSoftware:Workflow:Resource:PSADResource" />

</Dependencies>

<CustomerInformation ID="opex.com" Name="opex"/>

</AutoPilot>

Resource Node

<Security xmlns="http://mars-o-matic.com" ID="OpexSoftware:Workflow:Resource:PSADResource"

NodeType="Resource" ResourceClass="Security" NodeName="PSADResource">

<Dependencies>

<Node ID="OpexSoftware:Workflow:Software:PSAD" />

<Node ID="OpexSoftware:Workflow:Application:PSADApplication" />

</Dependencies>

<CustomerInformation ID="opex.com" Name="OpexSoftware" />

</Security>

Application Node

<ApplicationSuite xmlns="http://mars-o-matic.com" ID="OpexSoftware:Workflow:Application:PSADApplication"

NodeType="Application" ApplicationClass="Enterprise"

ApplicationSubClass="ApplicationSuite" NodeName="PSADApplication">

<Dependencies>

<Node ID="OpexSoftware:Workflow:Resource:PSADResource" />

</Dependencies>

<CustomerInformation ID="opex.com" Name="OpexSoftware" />

</ApplicationSuite>