Upgrade of Azure SecPack on a Standalone Linux Box.

Note: Before Proceeding to the upgrade, it is highly recommended to take a backup of current configuration file /etc/default/mdsd.

Now install the upgrade Packages.

1. Add the Microsoft Azure Security Pack repositories to the VM.  
   echo 'deb [arch=amd64] <http://packages.microsoft.com/repos/azurecore/> trusty main' | sudo tee -a /etc/apt/sources.list.d/azure.list
2. Now, Add repo GPG key.  
   Over the network (requires access to apt-mo.trafficmanager.net over port 11371)   
   sudo apt-key adv --keyserver packages.microsoft.com --recv-keys 417A0893
3. Update the Package list now  
   sudo apt-get update
4. Install azsec-mdsd, azure-security, azure-monitor and clamav packages  
   sudo apt-get install -y azure-security azsec-mdsd azsec-monitor azsec-clamav  
   Note: When it asks to remove the current package and update with the new version, proceed to upgrade.
5. Now, after the package were installed successfully, Configure syslog forwarding.  
   sudo config-mdsd syslog -e rsyslog
6. Transfer gcscert.pem, gcskey.pem, and mdsd.xml to VM (Optional, as we are upgrading the package, current certificate pemfiles and xml file are already resides in the proper location).  
   Copy files into /etc/mdsd.d  
   sudo cp gcscert.pem gcskey.pem mdsd.xml /etc/mdsd.d/
7. Set ownership and permissions for mdsd files: (This step is also optional as the files are already there)  
   sudo chown syslog /etc/mdsd.d/gcskey.pem   
   sudo chmod 400 /etc/mdsd.d/gcskey.pem
8. Now Edit /etc/default/mdsd and set the parameters. (Here you can verify the existing mdsd file which you have already backup in the beginning, and set the parameters as per the old document.  
   NOTE: Be sure to preserve the values for SSL\_CERT\_DIR and SSL\_CERT\_FILE. These are set by the installer and mdsd will not work if these values are cleared (or changed to incorrect values.

Here is the reference mdsd file to change the config values. ( in Blue).

# Check 'mdsd -h' for details.

MDSD\_ROLE\_PREFIX=/var/run/mdsd/default

# MDSD\_OPTIONS="-d -r ${MDSD\_ROLE\_PREFIX}"

MDSDLOG=/var/log

MDSD\_OPTIONS="-A -c /etc/mdsd.d/mdsd.xml -d -r $MDSD\_ROLE\_PREFIX -e $MDSDLOG/mdsd.err -w $MDSDLOG/mdsd.warn -o $MDSDLOG/mdsd.info"

export MONITORING\_GCS\_ENVIRONMENT=DiagnosticsProd

export MONITORING\_GCS\_ACCOUNT=BAGCommunity

export MONITORING\_GCS\_REGION=westus2

# or, pulling data from IMDS

# imdsURL="http://169.254.169.254/metadata/instance/compute/location?api-version=2017-04-02&format=text"

# export MONITORING\_GCS\_REGION="$(curl -H Metadata:True --silent $imdsURL)"

# see <https://jarvis.dc.ad.msft.net/?section=b7a73824-bbbf-49fc-8c3e->a97c27a7659e&page=documents&id=66b7e29f-ddd6-4ab9-ad0a-dcd3c2561090

export MONITORING\_GCS\_CERT\_CERTFILE=/etc/mdsd.d/gcscert.pem # update for your cert on disk

export MONITORING\_GCS\_CERT\_KEYFILE=/etc/mdsd.d/gcskey.pem # update for your private key

# Below are to enable GCS config download

export MONITORING\_GCS\_NAMESPACE=BAGCommunity

export MONITORING\_CONFIG\_VERSION=1.0

export MONITORING\_USE\_GENEVA\_CONFIG\_SERVICE=true

Note: These values can also be achieved by BAGCommunity Warmpath account Config xml file.

1. Configure azsecd.  
   sudo azsecd config -s baseline -d P1D   
   sudo azsecd config -s software -d P1D   
   sudo azsecd config -s clamav -d P1D

After upgrading the packages and set the mdsd parameters, now restart the Services.  
sudo service mdsd restart   
sudo service azsecd restart  
  
Check the below file that there are no mdsd errors.  
/var/log/mdsd/mdsd.err  
Note: If the last line contains "START mdsd daemon" then there are no errors.

1. Manually create heartbeat (The warning about lastScan.xml can be ignored)  
   sudo azsecd manual -s heartbeat  
   wait for 60 Sec.  
   Check that there are no mdsd errors   
   /var/log/mdsd/mdsd.err  
   If the last line contains "START mdsd daemon" then there are no errors.

Azure Secpack Upgrade is completed.