McAfee Security Connected

Integrating EPO and MAM

Table of Contents

Overview

Integration between McAfee ePolicy Orchestrator and McAfee Asset Manager provides added network visibility for the enterprise, enabling comprehensive security, configuration, compliance, and risk management on the network.

The McAfee Asset Manager ePO extension is used to update the McAfee ePO asset database in near real-time, allowing the McAfee ePO platform to become the single source of truth about the network. The integration makes use of the rogue system detector (RSD) API.

The McAfee Asset Manager ePO extension is used to communicate with the McAfee Asset Manager Console’s PostgreSQL database on a regular basis (down to 1 minute intervals) and to receive delta updates about the network, its devices, and its users.

User Accounts & Privileges

Administrative rights to McAfee ePO

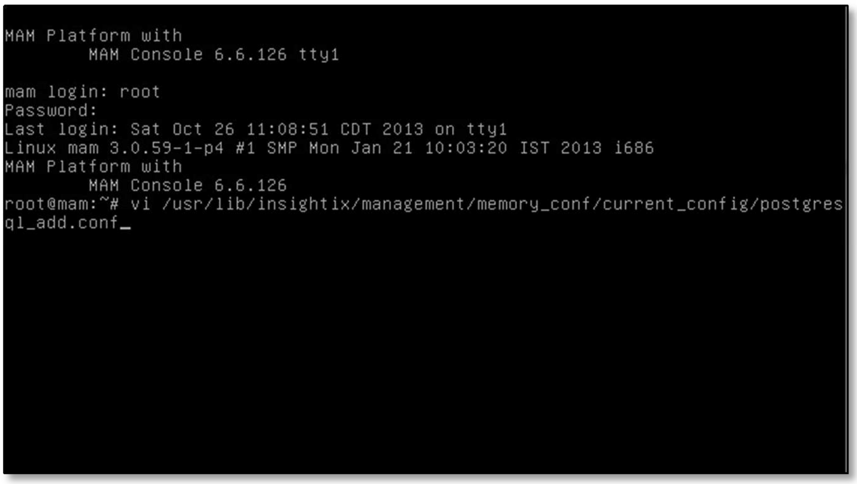
Root account for MAM Console

Prerequisites

MAM Extension for ePO 4.6 and above

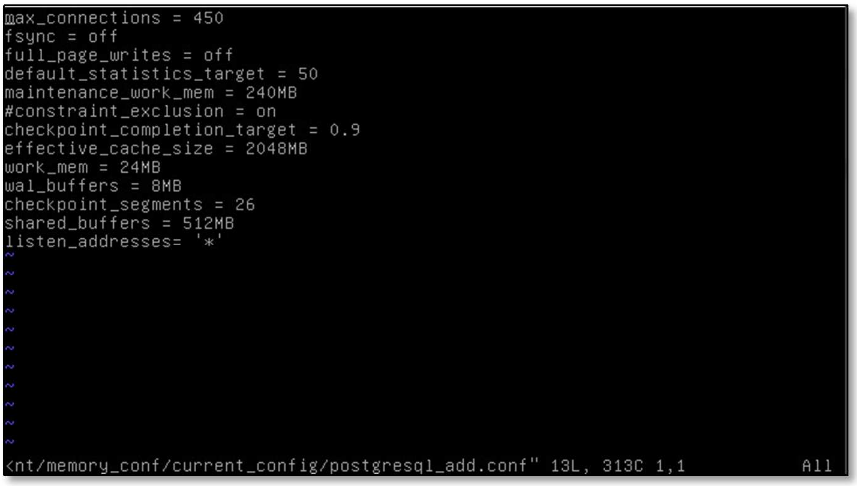
Configuration Steps

1. Log in to the McAfee Asset Manager Console with the root user account
2. Using VI, open the following file for editing
    a. /usr/lib/insightix/management/memory_config/current_config/postgresql_add.conf



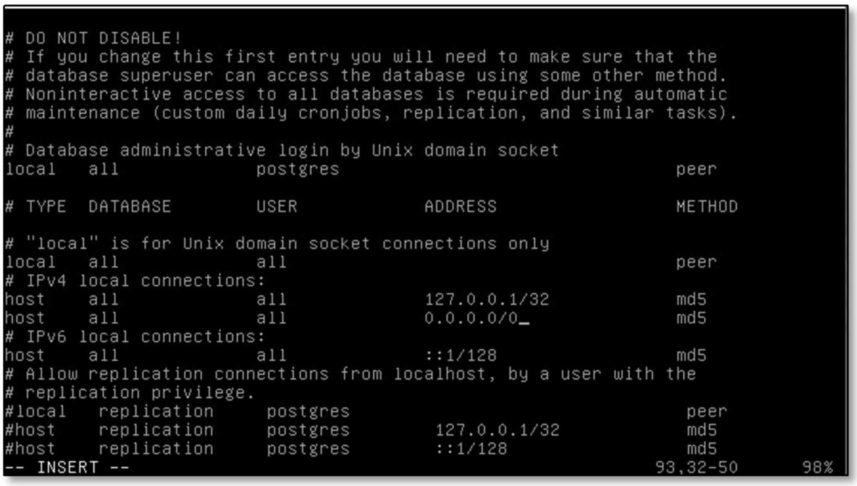
```
MAM Platform with
        MAM Console 6.6.126 tty1

mam login: root
Password:
Last login: Sat Oct 26 11:08:51 CDT 2013 on tty1
Linux mam 3.0.59-1-p4 #1 SMP Mon Jan 21 10:03:20 IST 2013 i686
MAM Platform with
        MAM Console 6.6.126
root@mam:~# vi /usr/lib/insightix/management/memory_conf/current_config/postgres
ql_add.conf_
```

3. Add the following line to the file
   a. Press the Insert Key on the keyboard to begin editing mode
   b. Listen_addresses= ‘*’
   c. To save press *Shift :* on the keyboard → Type wq to write and quit



```
max_connections = 450
fsync = off
full_page_writes = off
default_statistics_target = 50
maintenance_work_mem = 240MB
#constraint_exclusion = on
checkpoint_completion_target = 0.9
effective_cache_size = 2048MB
work_mem = 24MB
wal_buffers = 8MB
checkpoint_segments = 26
shared_buffers = 512MB
listen_addresses= '*'
~
~
~
~
~
~
~
~
~
~
~
~
<nt/memory_conf/current_config/postgresql_add.conf" 13L, 313C 1,1          All
```

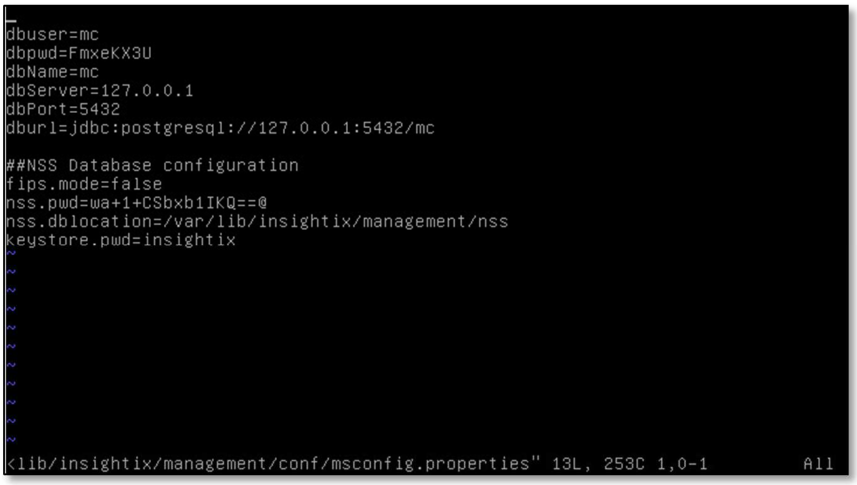
4. Using VI, open the following file for editing
   a. /etc/postgresql/9.1/main/pg_hba.conf
   b. Press the Insert Key on the keyboard to begin editing mode
   c. Under IPv4 local connections add the following line if it does not exist
   d. Host all all 0.0.0.0/0 md5
   e. To save press *Shift* : on the keyboard → Type wq to write and quit



```
# DO NOT DISABLE!
# If you change this first entry you will need to make sure that the
# database superuser can access the database using some other method.
# Noninteractive access to all databases is required during automatic
# maintenance (custom daily cronjobs, replication, and similar tasks).
#
# Database administrative login by Unix domain socket
local   all             postgres                                peer

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
host    all             all             0.0.0.0/0_              md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
#local   replication     postgres                                peer
#host    replication     postgres        127.0.0.1/32            md5
#host    replication     postgres        ::1/128                 md5
-- INSERT --                                          93,32-50      98%
```

5. Type Exit one time
6. Type monit stop all
7. Type /etc/init.d/postgresql restart
8. Type monit start all

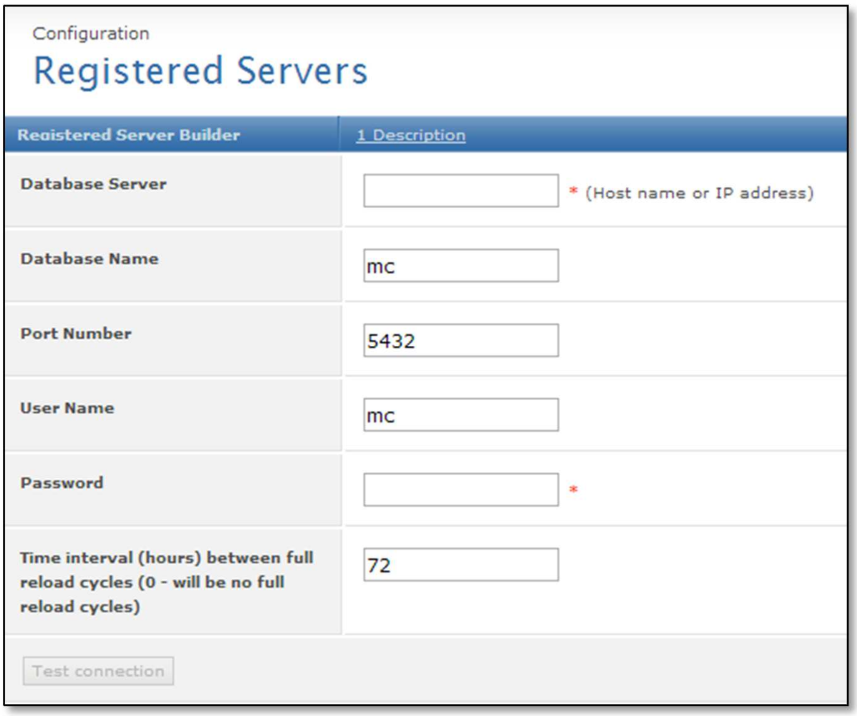
9. Using VI, open the following file to gather needed information to configure the ePO Server
    a. /usr/lib/insightix/management/conf/msconfig.properties
    b. Take note of the username under dbuser and the database password under dbpwd



```
dbuser=mc
dbpwd=FmxeKX3U
dbName=mc
dbServer=127.0.0.1
dbPort=5432
dburl=jdbc:postgresql://127.0.0.1:5432/mc

##NSS Database configuration
fips.mode=false
nss.pwd=wa+1+CSbxb1IKQ==@
nss.dblocation=/var/lib/insightix/management/nss
keystore.pwd=insightix
~
~
~
~
~
~
~
~
~
~
~
<lib/insightix/management/conf/msconfig.properties" 13L, 253C 1,0-1         All
```

10. Log in to the ePO server console with an administrator account
11. Using VI, open the following file to gather needed information to configure the ePO Server
12. Browse to Menu → Extensions → Install Extension
13. Check in the MAM Extension
14. Browse to Menu → Registered Servers → New
15. Select MAM Console Server from the drop down menu
16. Enter a name for the server → Next
17. Enter the IP Address of the MAM Console Server

18. Enter the Password for the database that was noted in step 9



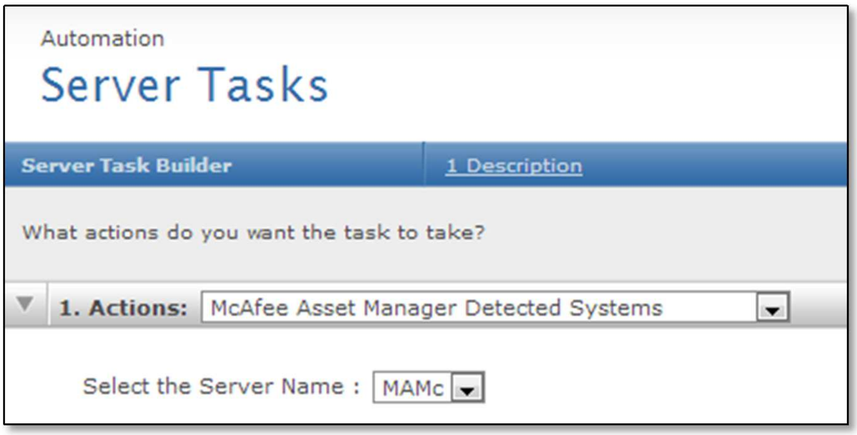
Configuration

Registered Servers

Registered Server Builder | 1 Description

Database Server	* (Host name or IP address)
Database Name	mc
Port Number	5432
User Name	mc
Password	*
Time interval (hours) between full reload cycles (0 - will be no full reload cycles)	72

19. Click Test Connection
20. If the connection is successful click Save
21. Browse to Menu → Server Tasks → New Task
22. Name the Task (This task is to pull data from MAM)
23. Click Next
24. Select McAfee Asset Manager Detected Systems from the drop down menu
25. Ensure the correct registered MAM server is selected



Automation

Server Tasks

Server Task Builder | 1 Description

What actions do you want the task to take?

1. Actions: McAfee Asset Manager Detected Systems

Select the Server Name : MAMc

26. Click Next
27. Configure the schedule frequency for ePO to pull data from MAM
28. Click Next → Save

Value Add

McAfee Asset Manager augments McAfee’s visibility of devices connected to the network, enabling comprehensive security, configuration, compliance, and risk management on the network. McAfee has achieved this by integrating McAfee Asset Manager with McAfee ePO software, the centralized platform that manages all endpoint security and compliance solutions from McAfee.
As part of the integration with the McAfee ePO platform, McAfee Asset Manager updates the McAfee ePO asset database in near real-time, allowing the McAfee ePO platform to maintain a more complete, accurate, and up-to-date inventory of the devices, their profiles, and the identities of those using the devices.

Combining the data from existing McAfee solutions and McAfee Asset Manager, the McAfee ePO platform now becomes the single source of truth about the network. This integration provides the foundation for effectively managing security, compliance, and risk against all devices across your entire network.