Disclaimer

This document is for informational purposes only and is subject to change at any time without notice. The information in this document is proprietary to Actian and no part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of Actian.

This document is not intended to be binding upon Actian to any particular course of business, pricing, product strategy, and/or development. Actian assumes no responsibility for errors or omissions in this document. Actian shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. Actian does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
EMA – Support Overview
Enterprise Monitoring Appliance
Dean Vernon
Principal Support Engineer
• What is EMA?
• Docker Overview
• What is Nagios?
• Monitoring Ingres/Vector using EMA and Nagios
What is EMA?

Actian Enterprise Monitoring Appliance (EMA) is a Nagios Core based, single interface for monitoring Ingres environments. EMA can be configured to monitor and display Ingres, Vector, Operating System, Network, and HVR data points.

It is delivered as a Docker container.
What is a Docker container?

- Docker is a software technology that allows us to run applications in an isolated manner.
- A container is a running instance of an image.
What is a Docker image?

• An image is the “model” or “template” for the container
• An image is actually built (think created and compiled) but is in effect static.
• We do not run the image, when we run a container we run an instance of the image.
• The image is built via the Dockerfile
What is a Dockerfile?

- A set of instructions on how to build the image
- The image based on the instructions in the Dockerfile is built by the command “docker build”
- The image is then stored in the image repository
A container is a process?

- There is a process associated with the container.
- However, any process which runs “inside” the container runs on the host – as you can see with `ps`.

```bash
[actian@verde02-mapr2 ~]$ docker ps
CONTAINER ID   IMAGE                      COMMAND                  CREATED          STATUS    PORTS                                                 NAMES
3e0ec87fd632   actian/ema:4.2.0             /usr/local/nagios...   45 hours ago    Up 45 hours 0.0.0.0:80->80/tcp ema

[actian@verde02-mapr2 ~]$ ps -efl|grep docker |grep 3e0ec87fd632
  0 S root 10864 2432 0 80 0 86928 futex Oct11 ? 00:00:01 docker-runc
r-containerd-shim 3e0ec87fd6322706ec855c42660a5d19e164b07ab9de4d1e354f90adf3639f6a /var/run/docker/libcontainerd/3e0ec87fd6322706ec855c42660a5d19e164b07ab9de4d1e354f90adf3639f6a docker-runc

[actian@verde02-mapr2 ~]$ 
```
What is Nagios?

• An Open Source system and network monitoring application
• Allows monitoring of host resources (processor load, disk usage, etc.)
• Has a plugin design that allows users to easily develop their own service checks
• Has contact notifications when service or host problems occur and get resolved (via email, pager etc.)

With these capabilities it’s a perfect fit for monitoring Ingres and Vector.
Installing and Running EMA

• Ensure to have the Docker software installed on your OS:
  
  rpm -qa |grep -i docker
  docker-engine-selinux-1.13.0-1.el7.centos.noarch
  docker-engine-1.13.0-1.el7.centos.x86_64

• Unzip the docker tar file to a directory

• ./install.sh [-r external_directory]

• During the installation we will be prompted to enter hosts/instances we wish to monitor.

• Install will build and deploy the Docker container for us
Installing and Running EMA

EMA INSTALLATION (4.2.0)

Checking EMA distribution validity: action_ema.4.2.0.docker.tar.gz: OK
Loading the Docker image from the distribution: Loaded image: action_ema:4.2.0
Completed loading EMA docker image action_ema:4.2.0
ema

What is the desired port number for the Web dashboard [default: 80] ?
ema
Removing previous container
ema
Starting Docker container ID 3e9ec87fd6322706ecb35c42660a5d19e164b7ab9d4d1e354f90af8f3639f6a
Wait for the container to start up.
ema

EMA CONFIGURATION

--------------

* Gathering information - please enter details for email contact, hosts and instances to monitor:
ema

EMA generates email when there is an alarm. Enter a name (for readability) and an email address to receive the notifications
ema

Contact name: Dean
Contact email: dean.vernon@actian.com

Hosts and instances to be monitored can be configured through the EMA web console or may be added now.
ema
Do you wish to add instances to monitor now? [N]n

* Generating configuration within the container:

* Re-performing Nagios
Running configuration check...
ema
Starting nagios: done.
ema
Waiting for the Nagios web services to start up...

* Confirming Nagios is up and running:
  "nagios_pid": 200,
  "daemon_mode": true,

* Web Console

Please enter a new password for the EMA web console user 'ema'
ema
New password:
Re-type new password:
ema
Updating password for user ema
You can find the EMA web console at http://verde02-mapr2:80/nagios
The login name is 'ema' and the password is the one just supplied above
ema

[actian@verde02-mapr2 media]$
Installing and Running EMA

- `[-r external_directory]`
- This is where external storage for the EMA is saved and where we can manually configure instances to be monitored.
- This is also where we can make manual config changes to Nagios.

```bash
[actian@verde02-mapr2 ~]$ ls -R ema.docker/ema/nagios/etc
ema.docker/ema/nagios/etc:
cgi.cfg ema_resource.cfg htpasswd.users nagios.cfg objects plugins.ini ssh
ema.docker/ema/nagios/etc/objects:
contact.cfg ema_commands.cfg ema_templates.cfg os_templates.cfg
contact.cfg.@@ ema_contacts.cfg ema_timeperiods.cfg uksl-vector11-02.ingres.prv
contactgroups.cfg ema_hosts.cfg.@@ host.cfg.@@ uksl-vector11-02.ingres.prv.config
contactgroups.cfg.@@ ema_localhost.cfg ingres.cfg verde02-mapr2.actian.com
databases.cfg ema_service_groups.cfg installation.cfg.@@ verde02-mapr2.actian.com.config

ema.docker/ema/nagios/etc/objects/uksl-vector11-02.ingres.prv:
host.cfg installation.a2.cfg installation.DV.cfg

ema.docker/ema/nagios/etc/objects/verde02-mapr2.actian.com:
host.cfg installation.I3.cfg installation.II.cfg

ema.docker/ema/nagios/etc/ssh:
id_rsa id_rsa.pub known_hosts
[actian@verde02-mapr2 ~]$`
```
Installing and Running EMA
Installing and Running EMA

It appears as though you do not have any instances defined. Click the 'Add a new EMA monitored instance' link to define an instance...

If you have defined instances then you may need to restart Nagios for the new services to be loaded...
Monitoring of instances via EMA Web Console
Installing and Running EMA

C:\Windows\system32> powershell -ExecutionPolicy Bypass -File "%\i\i\plugins\enableps.ps1"
hostname = DVERNON-X1
Powershell Remoting is already enabled.
HTTPS listener already exists
Basic auth is already enabled. If this was done for some other application or purpose then
do not disable it when offered to do so by the EMA appliance installer.

C:\Windows\system32>

C:\WINDOWS\system32>powershell -ExecutionPolicy Bypass -File "%\i\i\plugins\enableps.ps1"
hostname = PMASON-W541
Powershell Remoting is already enabled.
HTTPS listener already exists
Basic auth support is required to copy the certificate files from the EMA appliance during setup
You may disable it again after this has been done.
Enabled basic auth support.

C:\WINDOWS\system32>
• Service checks are defined in the Nagios config files. Checks are for things like disk, CPU, locks, Error log etc.

• EMA comes with pre-defined service checks. Can be customised. See EMA manual/Nagios docs/Actian Services!

• Checks are run at intervals. They are implemented as native scripts provided with Ingres 11.0 - $II_SYSTEM\inges\iiema\plugins (unix) or %II_SYSTEM%/inges/iiema/plugins (Windows)

• Nagios remotely executes the scripts at the specified intervals. Intervals are specific to checks e.g. CPU every 15mins, Checkpoint every 24 hours. Can also be customised.

• Remote execution is via SSH for Unix/Linux and WinRM (“Windows Remote Management”) for Windows
Remote Execution – Unix/Linux via SSH

- Uses standard SSH protocol.
- Means sshd must be running, port 22 open.
- EMA creates public/private key on installation.
- Public key copied to target machine via ssh-copy-id
- this step requires the password of the user we want to use for monitoring. Usually instance owner ('ingres', 'actian')
- Once key is copied it is used for authentication.
Remote Execution – Windows via WinRM

• Uses WS-Management (WSMAN) protocol for communication. Comes as part of Windows Vista and above.
• Uses Powershell (3.0 or higher) for remote execution.
• Means service “Windows Remote Management” should be available and port 5986 open.
• “enableps” –
  • checks WinRM service available and running
  • creates a “listener” on 5986
  • adds firewall rule for 5986
  • enables authentication via certificate
  • enables Powershell “remoting” (remote execution of PS scripts)
  • Enable basic authentication – authentication via user/password.
Remote Execution – Windows via WinRM


• EMA creates certificate pair for each unique username.

• When adding a new Windows instance:
  • Create a new certificate if needed (new user?)
  • Copy public certificate to Windows machine to be monitored
  • Import certificate
  • Create an encrypted credential (username/password)
  • Associate certificate with credential
  • Disable basic auth – if requested

• Basic auth used for these steps. Once done use the public certificate
Remote Execution – Windows via WinRM

• Which user for monitoring?

• As with SSH would normally use instance owner (‘ingres’, ‘actian’)

• However WinRM requires we *not* use a domain user. If your Actian X instance owner is a domain user, create a new user for EMA use:
  • Must be a local Administrator (needed to monitor CPU etc)
  • Add as ingres user via accessdb
  • Give it “Security Administrator” privilege
Remote Execution – Windows via WinRM

- Because certificate is associated with a credential if you change password of the monitoring user must re-run the certificate import process
- Can be done with install script, “install –p”

```
-- uks1-lv12maspa05-64:ema_install $ ./install.sh -p
In order to associate a new set of credentials with a certificate we need to re-import the certificate file
Please enter the hostname of the Windows machine: pmason-w541
Please enter the username of the login used for EMA monitoring [ingres]: ema
Please enter the password for ema:
In order to re-import the certificate with the new password for ema on pmason-w541 we need to enable basic authentication for powershell.
To do this you must run the powershell script 'enableps.ps1' on the Windows host
This script is in the plugins directory of your Ingres instance.
log in to pmason-w541 as an Administrator and run:
    powershell -executionpolicy bypass %II_SYSTEM%\ingres\iiema\plugins\enableps.ps1
Press enter once this has been done
Copying and importing the certificate file to the Windows host pmason-w541
```

- Or by adding instance again via Web console.
Monitoring of instances via EMA Web Console
Monitoring of instances via EMA Web Console

### Current Network Status
- **Last Updated:** Tue May 30 02:02:00 CDT 2017
- **Updated every 30 seconds**
- **Nagios Censys™ 4.4 - www.nagios.org**
- **Logged in as admin**

### Service Status Details For All Hosts

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>Last Check</th>
<th>Duration</th>
<th>Attempt</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DV Checkpoint</td>
<td>CRITICAL</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>30 s</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>DV DiB process</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>14.2 ms</td>
<td>Correct number of logins servers running</td>
</tr>
<tr>
<td>DV Error Log</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.3 ms</td>
<td>No significant login errors reported</td>
</tr>
<tr>
<td>DV Lock Wits</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.2 ms</td>
<td>No waiting locks were identified</td>
</tr>
<tr>
<td>DV Sessions</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.2 ms</td>
<td>No waiting locks were identified</td>
</tr>
<tr>
<td>DV Transaction Log</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.2 ms</td>
<td>User sessions: 2 System threads: 10</td>
</tr>
<tr>
<td>DS CPU Load</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.2 ms</td>
<td>CPU load 15 minute average: 0.00</td>
</tr>
<tr>
<td>DS Data Usage</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.2 ms</td>
<td>SS 10.1.4.4.1</td>
</tr>
<tr>
<td>DS Memory</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>698 ms</td>
<td>13.2 ms</td>
<td>SS 10.1.4.4.1</td>
</tr>
<tr>
<td>x2 Checkpoint</td>
<td>UNKNOWN</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>x2 DiB Process</td>
<td>UNKNOWN</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>x2 Error Log</td>
<td>UNKNOWN</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>x2 Lock Wits</td>
<td>UNKNOWN</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>x2 Sessions</td>
<td>UNKNOWN</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>x2 Transaction Log</td>
<td>UNKNOWN</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>There are checkpoint failures</td>
</tr>
<tr>
<td>DSM DiB Process</td>
<td>CRITICAL</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>Correct number of logins servers running</td>
</tr>
<tr>
<td>DSM Error Log</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>Correct number of logins servers running</td>
</tr>
<tr>
<td>DSM Lock Wits</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>Correct number of logins servers running</td>
</tr>
<tr>
<td>DSM Sessions</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>Correct number of logins servers running</td>
</tr>
<tr>
<td>DSM Transaction Log</td>
<td>CRITICAL</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>Correct number of logins servers running</td>
</tr>
<tr>
<td>Error Log</td>
<td>UNREACHABLE</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>Remote command execution failed: /opt/Adapic/ingress/examples/plgmon/remote_check_inged: line 415: l: exec: binary operator expected</td>
</tr>
<tr>
<td>Lock Wits</td>
<td>OK</td>
<td>2017-05-30 02:02:30</td>
<td>556 ms</td>
<td>32.5 ms</td>
<td>No waiting locks were identified</td>
</tr>
</tbody>
</table>
Inside the EMA Docker container
Useful Docker commands

- **docker run <image>**
  Creates the container from the image (via docker create <image> and then it starts it (via docker start).

- **docker stop <container>**
  Stops the running container

- **docker start <container>**
  Starts the container

- **docker exec -it <container> bash**
  Attaches a shell to the container
Useful Docker commands

- `docker ps`
  Shows running containers

- `docker ps -a`
  Shows running and stopped containers

- `docker rm <container>`
  Deletes a container (You will lose all data )

- `docker images`
  Shows all images

- `docker rmi <image>`
  Deletes an image (no container must be using this image)