Eaton Intelligent Power® Manager as a Virtual Appliance

Deployment's Guide

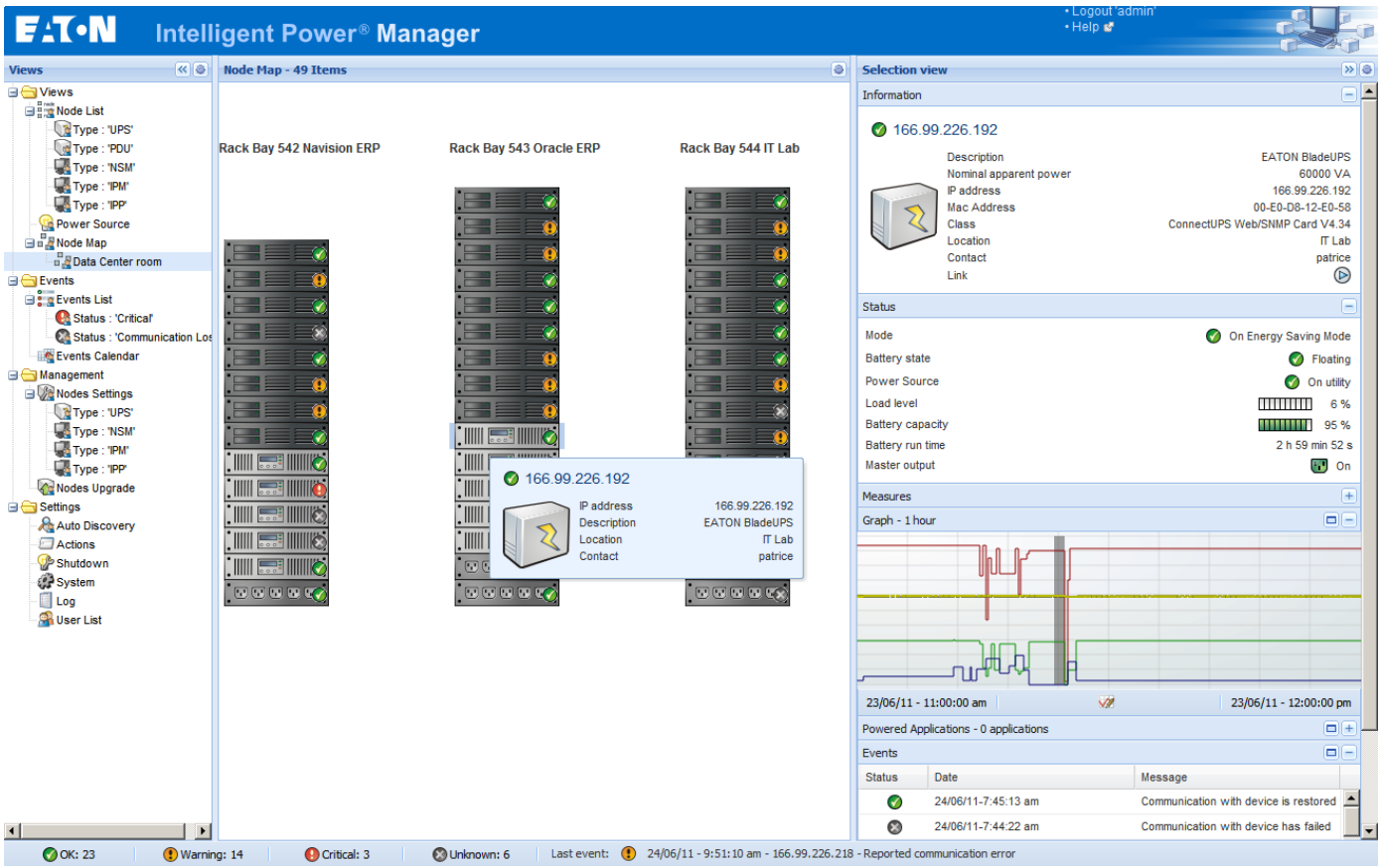


Table of Contents

1 Introduction 3
2 Free Version Limitation 3
3 Virtualization Platform Supported 3
4 Requirements 3
5 Deploying a Virtual Appliance in VMware vSphere 4
6 Configure the Virtual Appliance 5
6.1 Log into the Virtual Appliance 5
6.2 Security 5
6.2.1 Firewall 6
7 Configure IPM 7
8 References 7
8.1 VMware Studio 7
8.2 Firewall (Iptables) 7

1 Introduction

This Quick Setup Guide explains how to deploy Intelligent Power Manager as a Virtual Appliance.

Intelligent Power® Manager (IPM) is Eaton's power device supervision tool for IT environments.

For additional information about IPM, refer the *User Guide* on the Eaton website.

2 Free Version Limitation

IPM as a virtual appliance is delivered as a "Free" version with the limitation of 10 nodes (UPS/PDU devices).

To supervise more than 10 nodes, please contact sales representative.

- 10 to 100 nodes need an upgrade with the Silver License (Ref:66925)
- Unlimited License need an upgrade with the Gold License (Ref:66926)

3 Virtualization Platform Supported

The virtualization features is supported on:

- VMware ESX 4.1, ESXi 4.1 and ESXi 5.0/5.5

Note: Microsoft SCVMM feature is not supported on this virtual appliance.

4 Minimum System Requirements

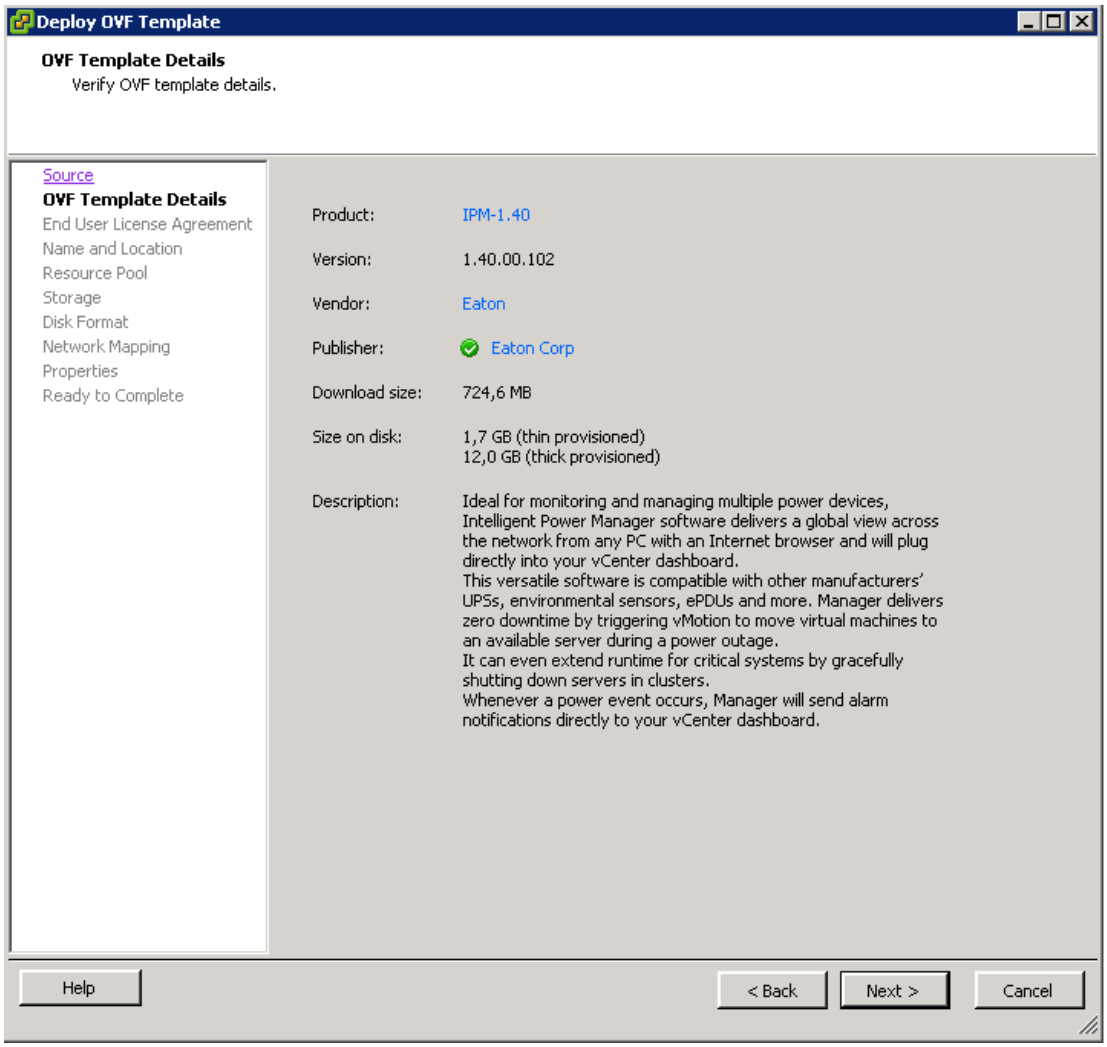
The IPM virtual appliance can be installed on all hypervisor than support OVF/OVA templates.

- 14 GB datastore
- 1GB free memory

5 Deploying a Virtual Appliance in VMware vSphere

To deploy the IPM virtual appliance, you need to:

1. Download the virtual appliance on http://pqsoftware.eaton.com
2. Connect to the ESX/ESXi or vCenter from your client computer using vSphere.
3. Log in as a user that has permission to create, start, and stop virtual machines.
4. Choose File > Deploy OVF Template.
5. Choose either **Deploy from URL** or **Deploy from file**, based on the location of OVA file.
6. Select the .OVA file. Click Next.
7. You will see the screenshot below. Click Next.
8. Follow the instructions provided on the screen



6 Configuration of Virtual Appliance

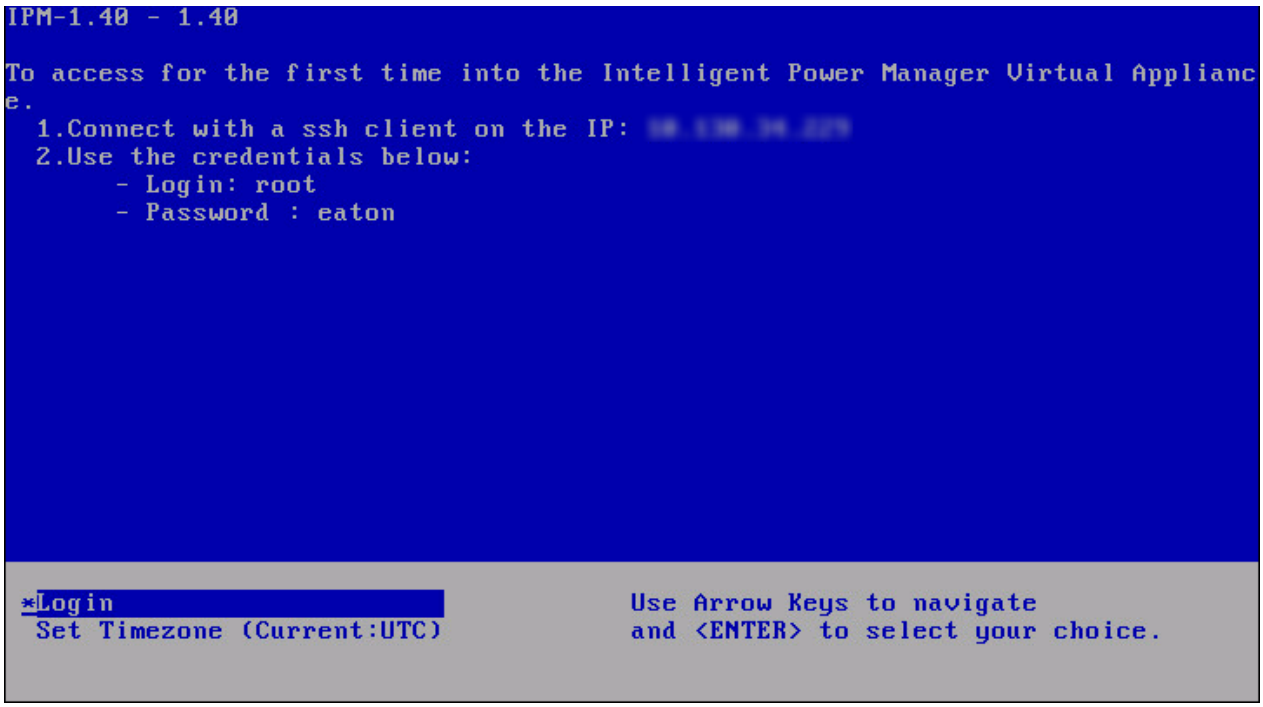
User is suggested to modify the default password.

6.1 Log into the Virtual Appliance

To log into the virtual appliance you can use:

- Standard Console of your Hypervisor
- SSH Client

With a Standard Console, you will see the screen below.



With SSH Client use the following credentials:

- Login: root
- Password: eaton

Note: To enable the first remote access, the root access is enabled for the SSH daemon.
For security issue, you can disallow the connection of the root user in "/etc/ssh/sshd_config" and set "PermitRootLogin" to **no**.

6.2 Security

6.2.1 Firewall

To minimize security issue, Eaton has installed and pre-configured the firewall.

6.2.1.1 Basic Configuration

The firewall is pre-configured to drop all connection except SSH and Eaton web and devices connection.

You can only connect on the virtual appliance through Eaton Web Page or SSH connection.

For example, The Virtual Appliance doesn't respond to "Ping" (ICMP response is not allowed).

6.2.1.2 Advanced Configuration

If you want to customize the firewall configuration, you need to have:

- Knowledge of Iptables
- Credentials to connect on the Virtual Appliance
- SSH Client

The firewall is already configured as below:

```
[root@localhost ~]# iptables -L -v
Chain INPUT (policy DROP 655 packets, 61197 bytes)
 pkts bytes   target     prot opt in     out     source    destination
127K   79M    ACCEPT     all  --  any    any     anywhere   anywhere     state RELATED,ESTABLISHED
  3   144     ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:ssh
 1316 78424   ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:mgesupervision
 0     0      ACCEPT     tcp  --  any    any     anywhere   anywhere     tcp dpt:mgemanagement
 7638   17M  ACCEPT     udp  --  any    any     anywhere    anywhere     udp dpt:mgesupervision
 3856  461K  ACCEPT     udp  --  any    any     anywhere    anywhere     udp dpt:mgemanagement
 0     0     ACCEPT  udp  --  any       any     anywhere    anywhere     udp dpt:bpcp-poll
 0     0     ACCEPT     udp  --  any    any     anywhere    anywhere     udp dpt:bpcp-trap
 0     0     ACCEPT     tcp  --  any    any     anywhere    anywhere     tcp dpt:61616
 0     0     ACCEPT     tcp  --  any    any     anywhere    anywhere     tcp dpt:rmiregistry

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 45494 packets, 12M bytes)
 pkts bytes target     prot opt in     out     source               destination
```

To modify the default configuration, you need to edit the script in /etc/init.d/firewall

You can see below "firewall" is configured to be launched after each startup:

```
[root@localhost ~]#chkconfig --list
Eaton-IPM       0:off   1:off   2:on    3:on    4:off   5:on    6:off
firewall        0:off   1:off   2:on   3:on    4:off   5:on   6:off
.
.
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
.
```

```
vmware-tools    0:off   1:off   2:on    3:on    4:off   5:on    6:off
```

To start the firewall:

```
[root@localhost ~]# /etc/init.d/firewall start
```

To stop the firewall:

```
[root@localhost ~]# /etc/init.d/firewall stop
```

Ps: After upgrading IPM software (1.28 to 1.40 for example) you must add these 2 rules in the firewall:
/sbin/iptables -A INPUT -p tcp --dport 61616 -j ACCEPT #EMC4J MessageBus
/sbin/iptables -A INPUT -p tcp --dport 1099 -j ACCEPT #rmiregistry

7 Configuration of IPM

To configure IPM, please refer the User Guide on http://pqsoftware.eaton.com

8 References

8.1 VMware Studio

You can see user guide of Virtual Appliance on VMware website

http://www.vmware.com/support/developer/studio/

8.2 Firewall (Iptables)

You can see on the project Iptable on the NetFilter website

Project
http://www.netfilter.org/projects/iptables/index.html

Documentation
http://www.netfilter.org/documentation/index.html