

BPPM – Patrol Agent Installation Steps on Linux and Automation Integration

Author: Karlis Peterson, Software Consultant, BMC Software

Version: 1.0

Date: May 12, 2013

DISCLAIMER NOTICE

This is Field Developed Documentation.

CONTENTS

Overview.....	3
Requirements	3
Patrol Agent Installation Pre-Reqs.....	4
IPTables or Firewall	4
Required OS Libraries.....	4
Creating a User for Patrol Agent	5
Creating a Sudo User for post installation scripts	5
Creating Patrol Installable Image.....	7
Installing Image (Silent Install).....	17
Integrating with Automation Tools	19
Create Compressed (Tar) Files from Running Agent.....	19
Extracting Compressed (Tar) Files on a Target Host	19
Feedback and Enhancements.....	22

OVERVIEW

The purpose of this document is to show how to step through installing Patrol Agents on Linux. Also, the steps show how you can create 2 tar files from an installed agent and use that for deployments with automation tools such as Puppet or Chef.

REQUIREMENTS

The following are required:

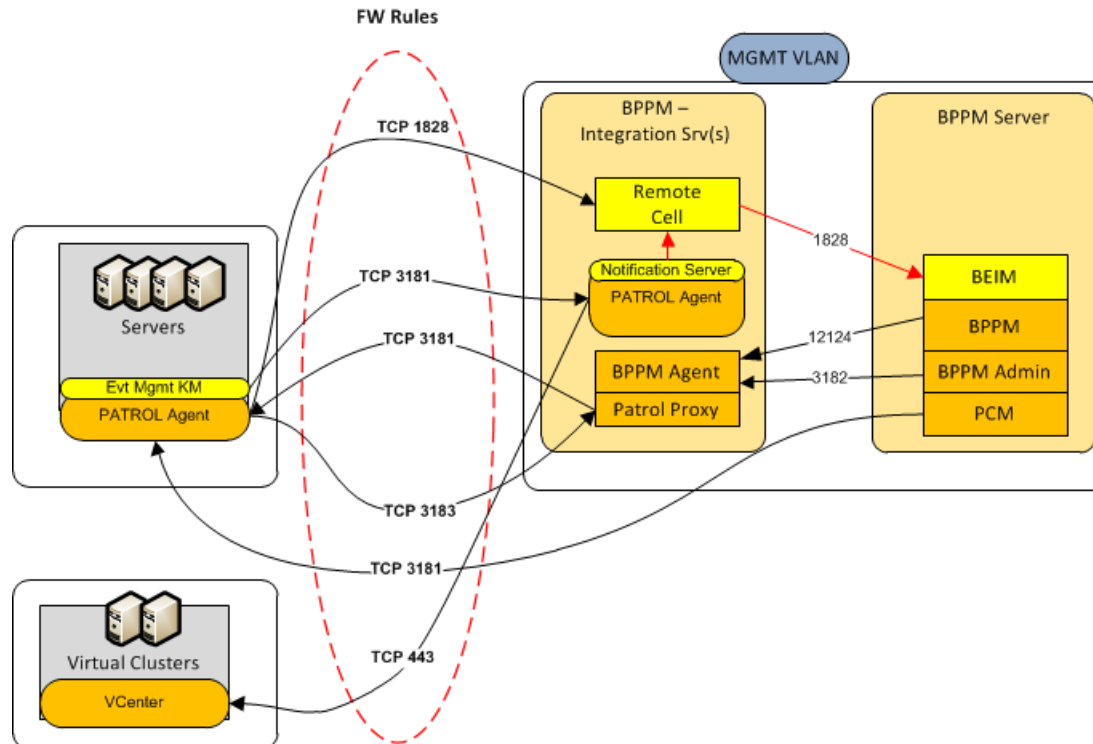
- BPPM CMA (*not required, but these steps assume BPPM Repository is installed)
- Patrol Agent User Account
- Sudo Account for running privileged commands
- Firewall or IpTables open for required ports (incoming and outgoing)

PATROL AGENT INSTALLATION PRE-REQS

This section describes the steps for creating an installable image for Linux.

IPTABLES OR FIREWALL

IP Tables or Firewall Ports need to open. Below is a summary of ports:



Here is an example of shutting off the iptables. You may just want to add the incoming and outgoing rules per the diagram above.

```
[root@bldb01 bmc]# /etc/init.d/iptables stop
```

```
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
```

REQUIRED OS LIBRARIES

Install the following packages which are required for the agent to run properly. This document has attached the RPMs for your convenience.

Linux 32bit OS	compat-libstdc++-33-3.2.3-55.fc5.i386.rpm
Linux 64bit OS	compat-libstdc++-33-3.2.3-55.fc5.i386.rpm AND compat-libstdc++-33-3.2.3-61.x86_64.rpm

1. Log in as root or *sudo user* and type the following command at a shell prompt. In this example, a sudo user is installing the rpms on a 64bit System.

```
sudo rpm -Uvh compat-libstdc++-33-3.2.3-55.fc5.i386.rpm
sudo rpm -Uvh compat-libstdc++-33-3.2.3-61.x86_64.rpm
```

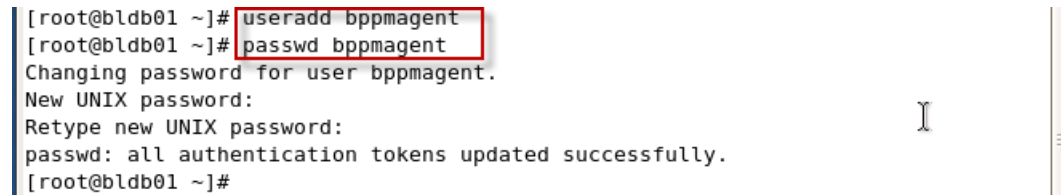
Note: you may see that the package is already installed – if so, just move on the next section.

CREATING A USER FOR PATROL AGENT

Steps for creating a regular user which will be used to run the Patrol Agent:

1. As root or sudo user type the following. Below is an example of adding a user “bppmagent” which will be used to run the Patrol Agent.

```
adduser bppmagent
passwd bppmagent
```



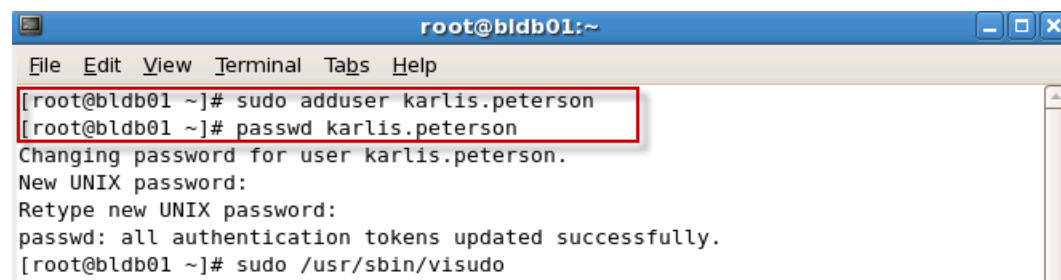
```
[root@bldb01 ~]# useradd bppmagent
[root@bldb01 ~]# passwd bppmagent
Changing password for user bppmagent.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@bldb01 ~]#
```

CREATING A SUDO USER FOR POST INSTALLATION SCRIPTS

Steps for creating a sudo user or validating sudoers file for an *existing* sudo user:

2. As root type the following – a sudo account is probably already created for the user logging in. Skip this step and goto step #2 to validate sudoers file. Below is an example of adding a user.

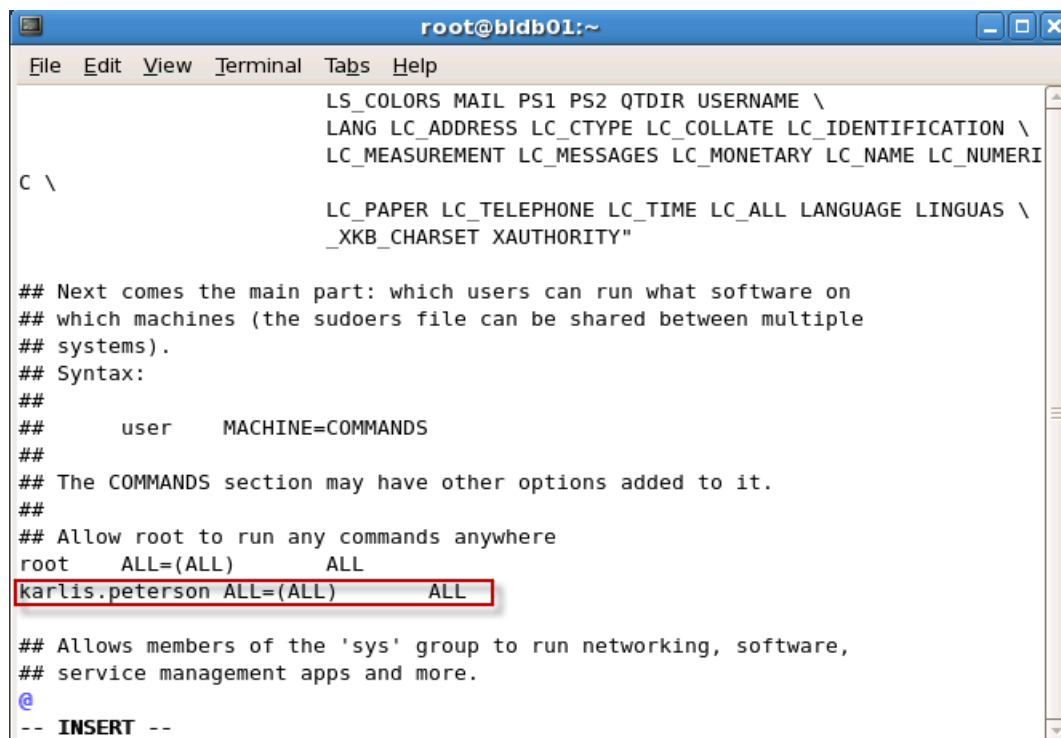
```
adduser karlis.peterson
passwd karlis.peterson
```



```
root@bldb01:~
File Edit View Terminal Tabs Help
[root@bldb01 ~]# sudo adduser karlis.peterson
[root@bldb01 ~]# sudo passwd karlis.peterson
Changing password for user karlis.peterson.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@bldb01 ~]# sudo /usr/sbin/visudo
```

3. You can create the sudo user by opening the sudoers file with this command. On the computer where you install sudo, enter the following lines for the User. Privilege specification in the sudoers file located in the local /etc directory:

```
sudo /usr/sbin/visudo
```



```
root@bldb01:~
File Edit View Terminal Tabs Help
LS_COLORS MAIL PS1 PS2 QDIR USERNAME \
LANG LC_ADDRESS LC_CTYPE LC_COLLATE LC_IDENTIFICATION \
LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERI
C \
LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS \
_XKB_CHARSET XAUTHORITY"
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user      MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root  ALL=(ALL)      ALL
karlis.peterson ALL=(ALL)      ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
@
-- INSERT --
```

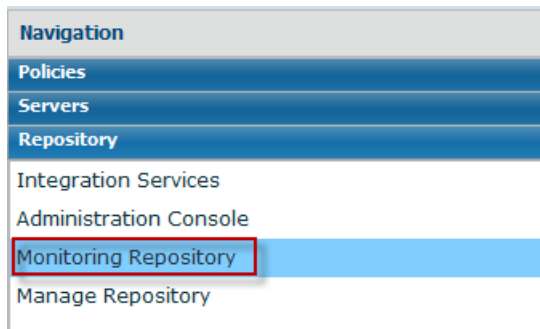
CREATING PATROL INSTALLABLE IMAGE

This section requires you to login to the BPPM CMA and create an Installable image

1. Login to the BPPM CMA Console:

http://<BPPM_Hostname>/admin
admin / admin

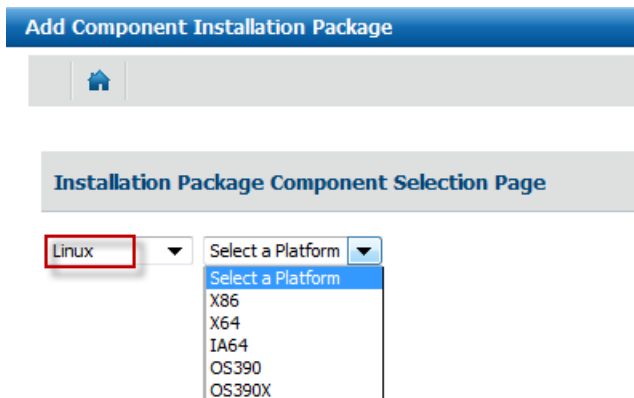
2. Click on Monitoring Repository



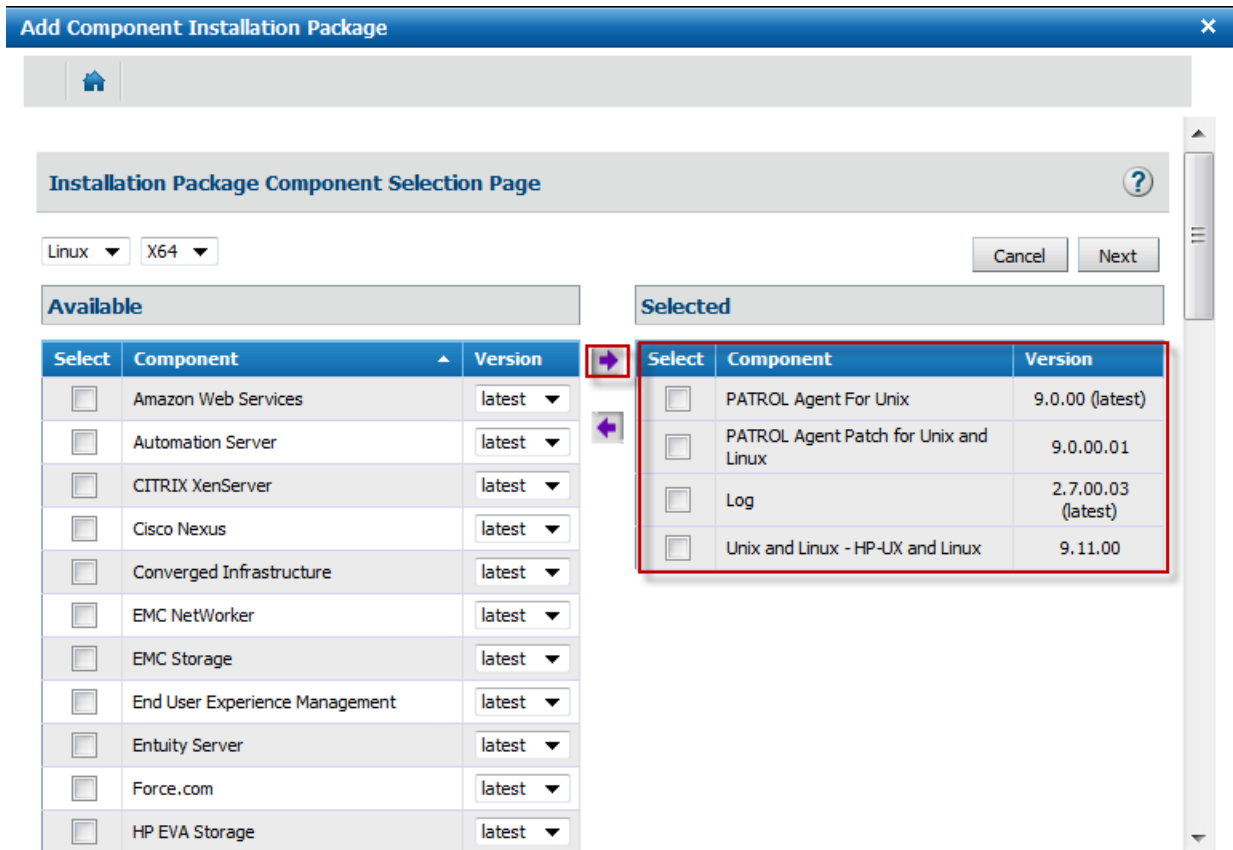
3. Click on the “+” to Add a Monitoring Solution



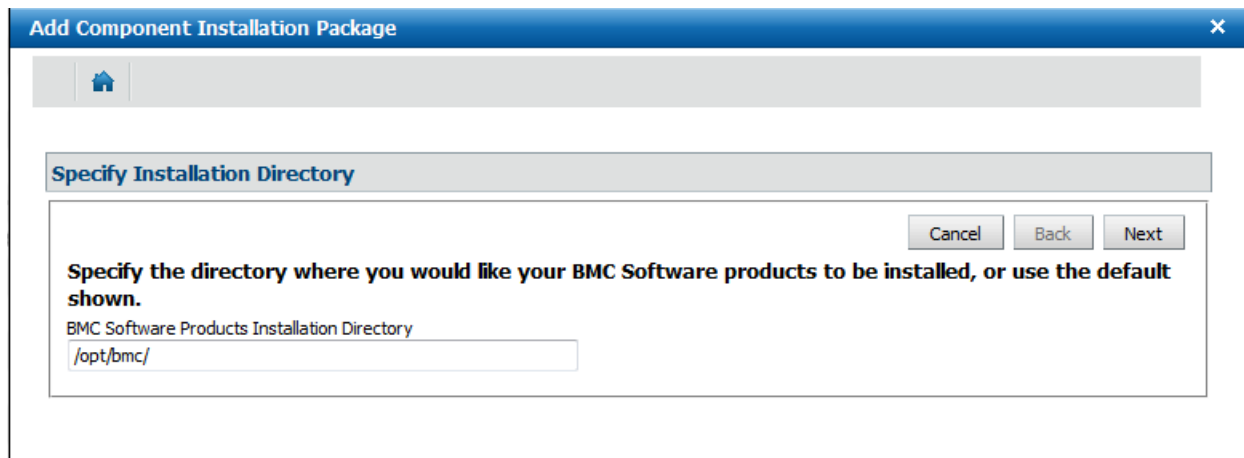
4. Select OS and Linux:



5. Select components for the Silent Install:



6. Click Next
7. Type the installation directory and click next:



8. Leave this section BLANK for System Root (or root privileged via sudo) and click Next:

Add Component Installation Package [X]

Home

Provide the System Root (or root privileged via sudo) Account Properties [Cancel] [Back] [Next]

The root account is used to install one or more of the products you selected. Enter the ID and password for the root account (or root privileged account via sudo - see installation notes) in the fields below. If you wish to continue without specifying the root password then select continue. Note: you will need to complete the root configuration at a later time before the products you selected will run correctly.

Root Login Name
Root Login Password
Re-enter the Root Login Password

Leave this blank.

9. Leave default and click Next:

Add Component Installation Package [X]

Home

Root Password Entry is blank. [Cancel] [Back] [Next]

Continue with a blank root password.
Root Password Specified.

Continue, I will finish configuring this product at a later time.
 Take me back to the previous screen

10. Leave default and click Next:

Add Component Installation Package [X]

Home

Root Password Entry is blank. [Cancel] [Back] [Next]

Continue with a blank root password.
Root Password Specified.

Continue, I will finish configuring this product at a later time.
 Take me back to the previous screen

11. Type in the User created to run the agent:

Add Component Installation Package

Provide the PATROL Default Account Properties

The PATROL component being installed requires a default account.

You must create this account manually before continuing with the installation. If you plan to use a domain account, enter `DOMAIN_NAME\account name`; otherwise, only enter the local account.

PATROL Default Account Login Name
bppmagent

PATROL Default Account Password
.....

Re-enter the PATROL Default Account Password
.....

Type in user for agent

Cancel Back Next

12. Select Advanced Security Options and select Next:

Add Component Installation Package

Select Level of Security

The PATROL Security User Guide explains the various security options. The default level of security is appropriate for most environments.

Please select the appropriate level of security for your environment.

Security option

Advanced security options

Basic security (default)

Security configuration includes security policy files, `patrol.conf` and `config.default`.

Overwrite current security configuration (keys, certificates and trusted roots)?

Yes

No

Cancel Back Next

13. Select **Security Level 2** and click Next:

The screenshot shows a dialog box titled "Add Component Installation Package" with a close button (X) in the top right corner. Below the title bar is a home icon. The main content area is titled "Select Advanced Level of Security" and contains the following text:

Select one of the following advanced levels of security or click the Back button to select the default level of security (recommended for most environments).

Note: In order to properly install and operate PATROL, it is essential that you select a security level that is appropriate for your environment. Consult the PATROL Security User Guide for detailed information.

security level

- Level 1 Uses Diffie-Hellman protocol, integrity validation and audit logging. No authentication of console or agent.
- Level 2 Uses SSL protocol. No authentication of console or agent.
- Level 3 Uses SSL protocol. Provides agent-side authentication.
- Level 4 Highest level of security. Uses SSL protocol. Provides console-side and agent-side authentication.

Note: For PATROL Perform, selecting any advanced security level will disable network communication between the PATROL Performance Manager and the Perform agent.

Buttons: Cancel, Back, Next

14. Leave Default and select Next:

The screenshot shows a dialog box titled "Add Component Installation Package" with a close button (X) in the top right corner. Below the title bar is a home icon. The main content area is titled "Provide Information for the PATROL Agent" and contains the following text:

The port number is used by the PATROL Agent to communicate with the console. If you are installing a new version of the PATROL Agent on top of an existing version, you must use the same port number that was used by the previous agent.

PATROL Agent Port Number

3181

Start the PATROL Agent after installation?

- Start the PATROL Agent automatically after the installation is completed.
- I will start the PATROL Agent manually using a command line.

Buttons: Cancel, Back, Next

15. Type in "tcp:changeme:3181" – the *changeme* host will be configured after the agent is installed and running.

Add Component Installation Package ✕

BMC ProactiveNet Integration Configuration

Cancel Back Next

INTEGRATIONSERVICE Variable: If you have not configured an Integration Service for your PATROL environment, the following field can be left blank.
INTEGRATIONSERVICE variable is used for Auto-Registration of PATROL Agent with BMC ProactiveNet.

Using this variable PATROL Agent will get registered automatically with the Integration Service on ProactiveNet Agent.

Below you may enter one or more known Integration Service(s) to connect to. Each entry is separated by a comma and has a format of 'Protocol:IntegrationServiceHostname:PortNumber'. For example 'tcp:Integration Service Hostname:3183'. Whereas 3183 is the port on which Integration Service host is listening for incoming PATROL Agent connection for Auto-Registration.

INTEGRATIONSERVICES Variable
 tcp:changeme:3181

Central Monitoring Administration Tag(s): If you have not configured Central Monitoring Administration in your BMC ProactiveNet - PATROL environment, the following field can be left blank.

Please provide comma separated tags that PATROL Agent will use to get configuration from Central Monitoring Administration. Each tag should follow the format TagName:Description. If there is a space in description surround it with Quotes (")e.g WinOS:"Windows OS Monitoring"

Central Monitoring Administration Tag(s)

16. Leave Default and select Next:

Add Component Installation Package ✕

BMC ProactiveNet Performance Management Cell Configurations

Cancel Back Next

If you have not configured a BMC ProactiveNet cell for your PATROL environment, the following fields can be left blank.

The BMC ProactiveNet cell is used to auto-register the PATROL Agent with BMC ProactiveNet.

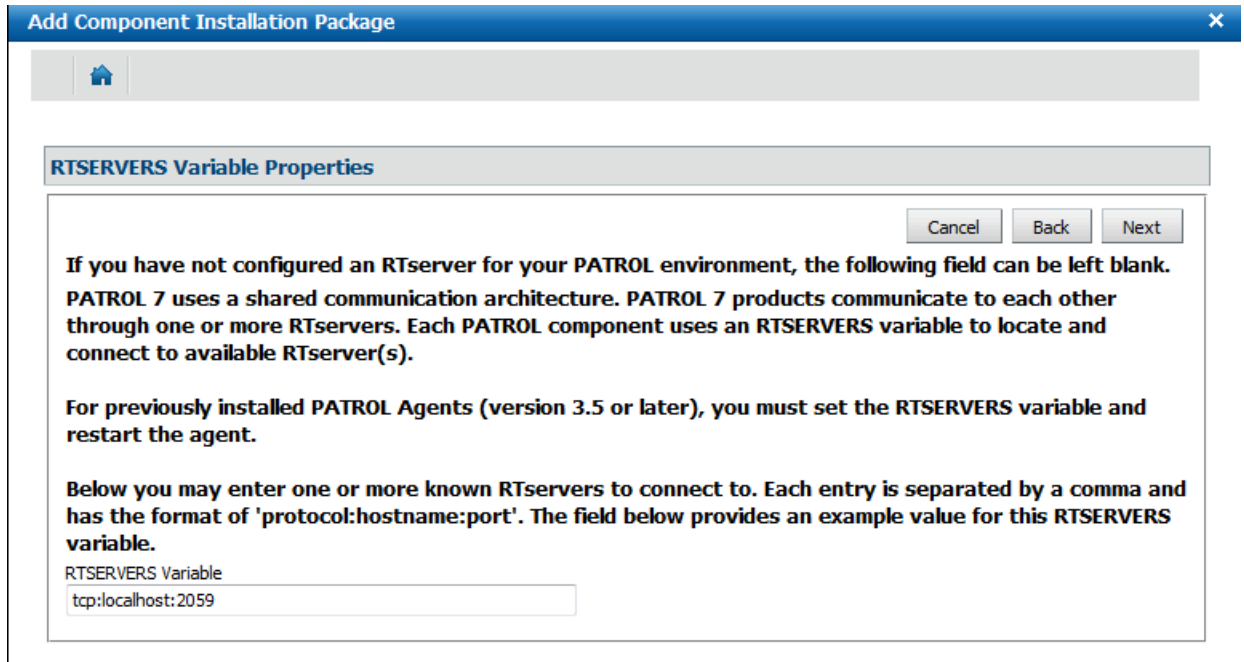
Enter the BMC ProactiveNet cell details in the following fields to connect with the encryption key (Please use cell format as Host/Port):

BMC ProactiveNet - Encryption Key
 mc

BMC ProactiveNet - Primary Cell
 localhost/1828

BMC ProactiveNet - Secondary Cell

17. Leave Default and select Next:



The screenshot shows a window titled "Add Component Installation Package" with a close button (X) in the top right corner. Below the title bar is a home icon. The main content area is titled "RTSERVERS Variable Properties" and contains the following text:

Cancel Back Next

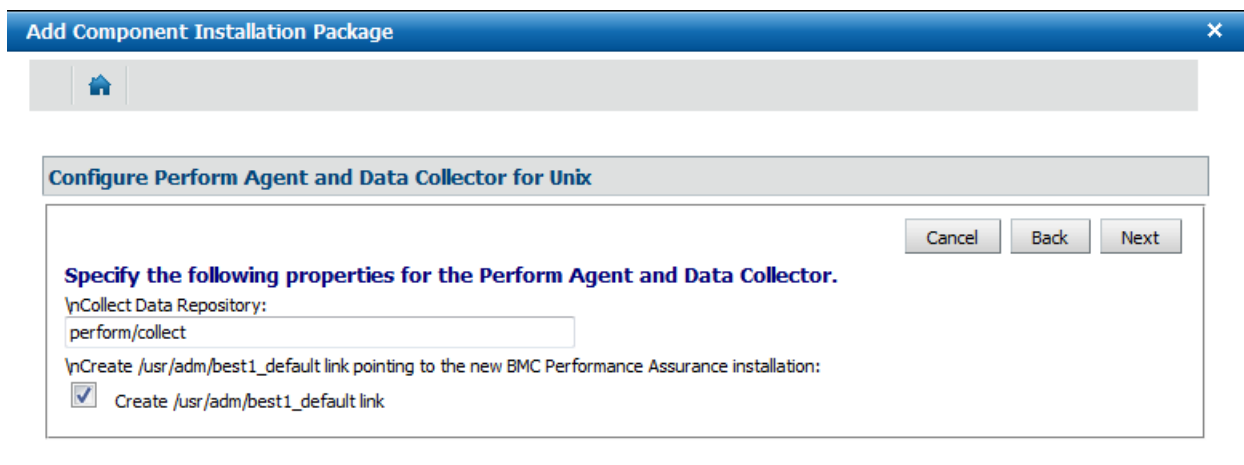
If you have not configured an RTserver for your PATROL environment, the following field can be left blank. PATROL 7 uses a shared communication architecture. PATROL 7 products communicate to each other through one or more RTservers. Each PATROL component uses an RTSERVERS variable to locate and connect to available RTserver(s).

For previously installed PATROL Agents (version 3.5 or later), you must set the RTSERVERS variable and restart the agent.

Below you may enter one or more known RTservers to connect to. Each entry is separated by a comma and has the format of 'protocol:hostname:port'. The field below provides an example value for this RTSERVERS variable.

RTSERVERS Variable
tcp:localhost:2059

18. Leave Default and select Next:



The screenshot shows a window titled "Add Component Installation Package" with a close button (X) in the top right corner. Below the title bar is a home icon. The main content area is titled "Configure Perform Agent and Data Collector for Unix" and contains the following text:

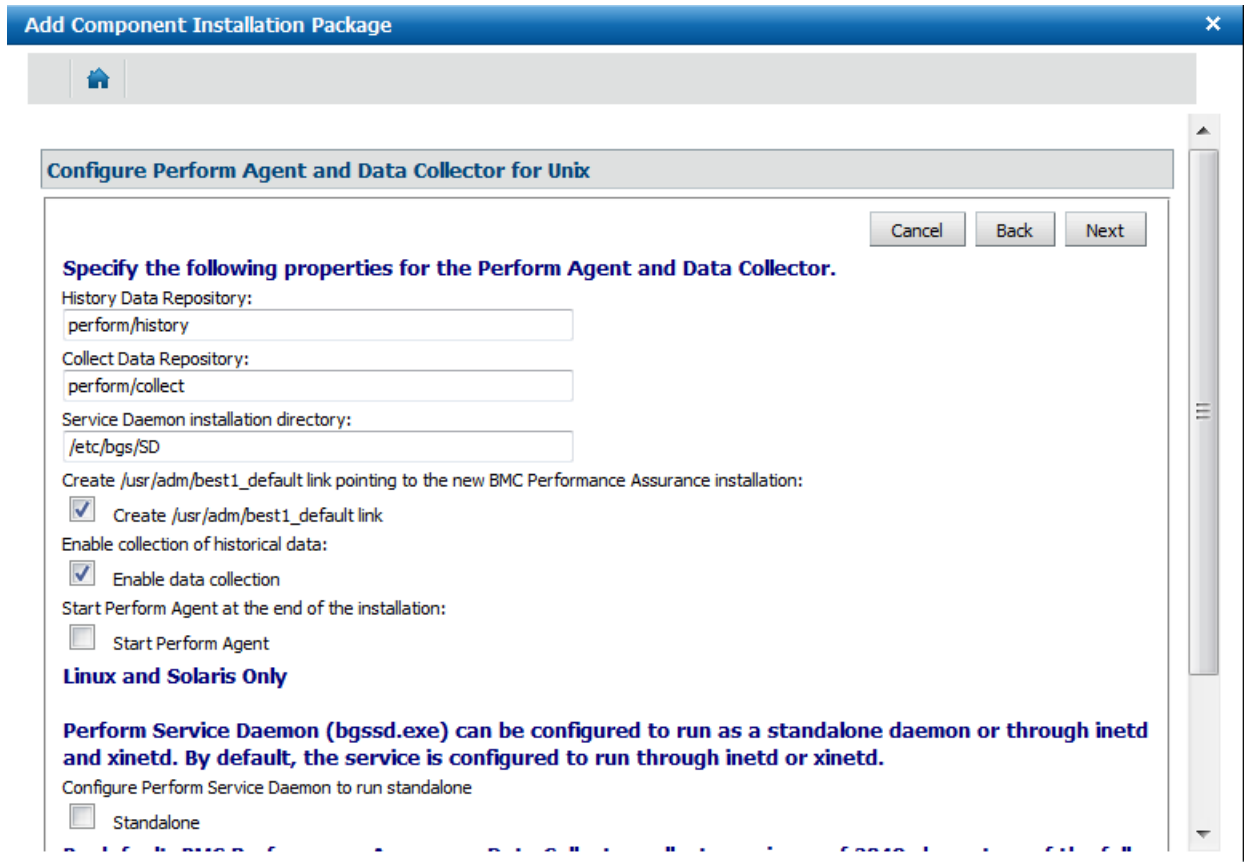
Cancel Back Next

Specify the following properties for the Perform Agent and Data Collector.

Collect Data Repository:
perform/collect

Create /usr/adm/best1_default link pointing to the new BMC Performance Assurance installation:
 Create /usr/adm/best1_default link

19. Leave Default and select Next:



Add Component Installation Package

Configure Perform Agent and Data Collector for Unix

Cancel Back Next

Specify the following properties for the Perform Agent and Data Collector.

History Data Repository:
perform/history

Collect Data Repository:
perform/collect

Service Daemon installation directory:
/etc/bgs/SD

Create /usr/adm/best1_default link pointing to the new BMC Performance Assurance installation:
 Create /usr/adm/best1_default link

Enable collection of historical data:
 Enable data collection

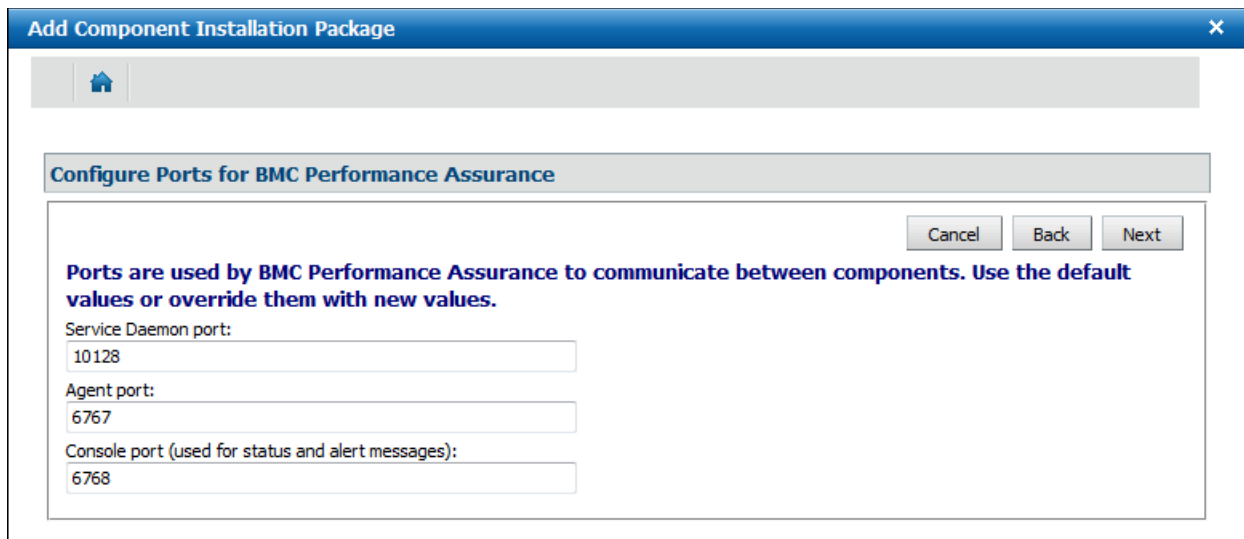
Start Perform Agent at the end of the installation:
 Start Perform Agent

Linux and Solaris Only

Perform Service Daemon (bgssd.exe) can be configured to run as a standalone daemon or through inetd and xinetd. By default, the service is configured to run through inetd or xinetd.

Configure Perform Service Daemon to run standalone
 Standalone

20. Leave Default and select Next:



Add Component Installation Package

Configure Ports for BMC Performance Assurance

Cancel Back Next

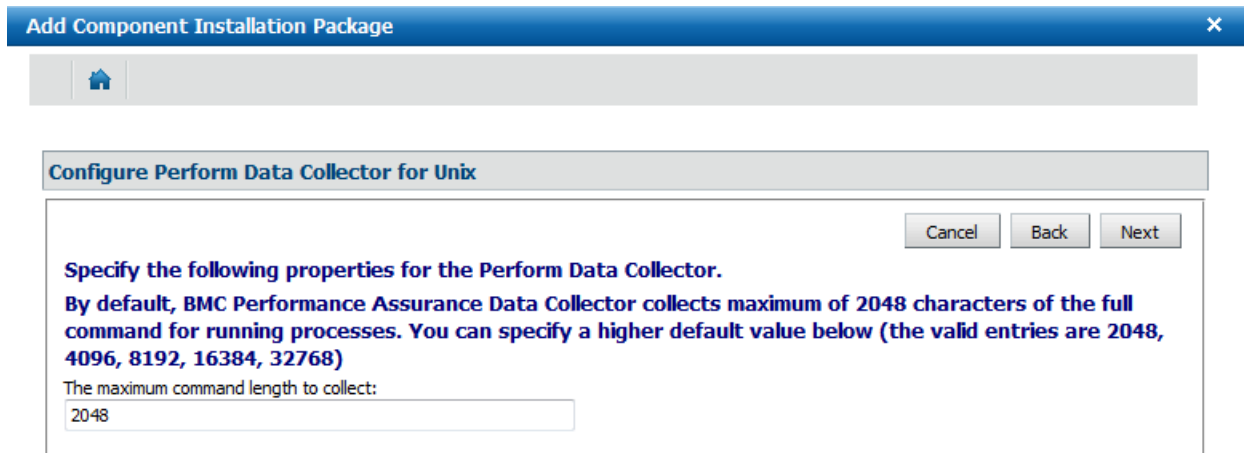
Ports are used by BMC Performance Assurance to communicate between components. Use the default values or override them with new values.

Service Daemon port:
10128

Agent port:
6767

Console port (used for status and alert messages):
6768

21. Leave Default and select Next:



Add Component Installation Package [X]

Home

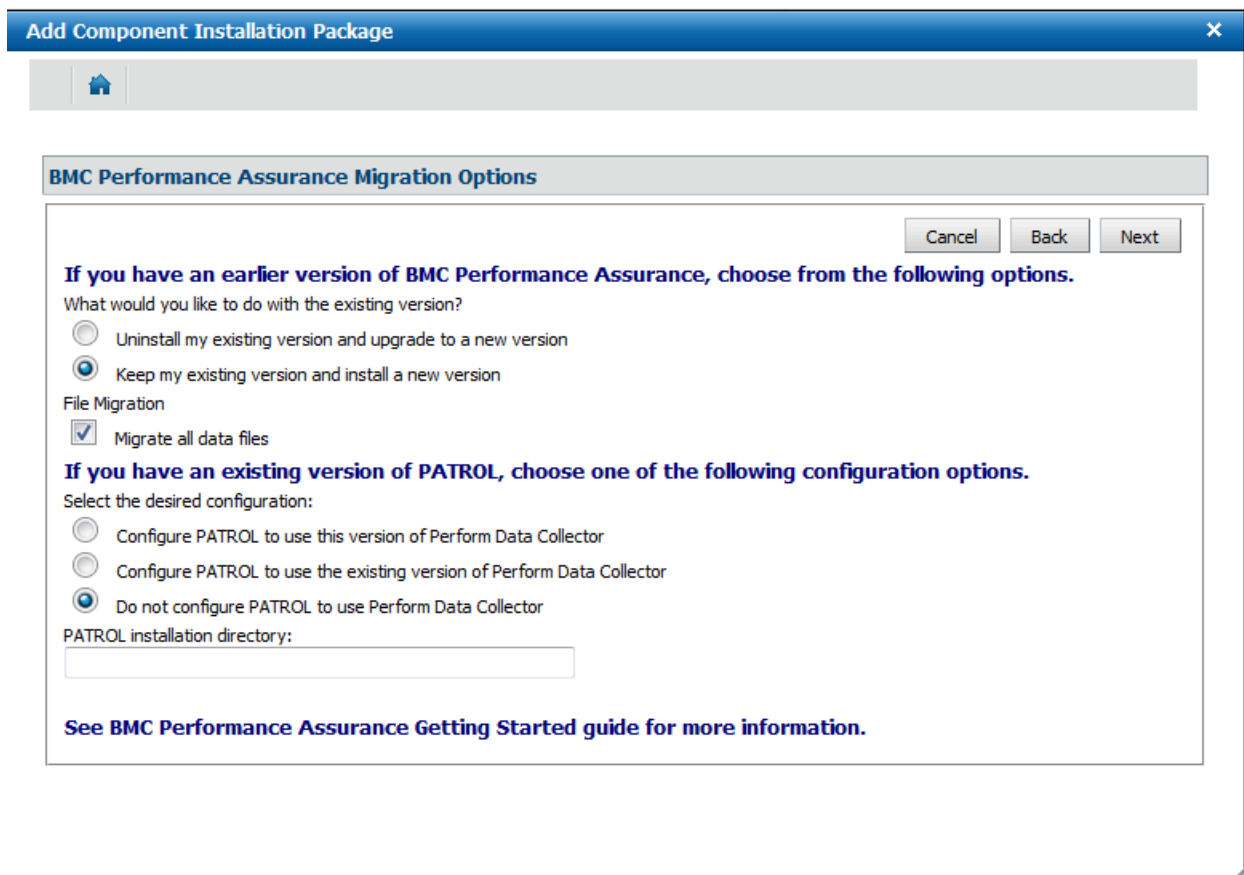
Configure Perform Data Collector for Unix

Cancel Back Next

Specify the following properties for the Perform Data Collector.
By default, BMC Performance Assurance Data Collector collects maximum of 2048 characters of the full command for running processes. You can specify a higher default value below (the valid entries are 2048, 4096, 8192, 16384, 32768)

The maximum command length to collect:
2048

22. Leave Default and select Next:



Add Component Installation Package [X]

Home

BMC Performance Assurance Migration Options

Cancel Back Next

If you have an earlier version of BMC Performance Assurance, choose from the following options.
What would you like to do with the existing version?
 Uninstall my existing version and upgrade to a new version
 Keep my existing version and install a new version

File Migration
 Migrate all data files

If you have an existing version of PATROL, choose one of the following configuration options.
Select the desired configuration:
 Configure PATROL to use this version of Perform Data Collector
 Configure PATROL to use the existing version of Perform Data Collector
 Do not configure PATROL to use Perform Data Collector

PATROL installation directory:
[]

See BMC Performance Assurance Getting Started guide for more information.

23. Name the Installation Package and Save.

Add Component Installation Package
✕

Close

Installation Package Details

Operating System	Linux
Platform	X64

Included Components	Version
PATROL Agent For Unix	9.0.00 (latest)
PATROL Agent Patch for Unix and Linux	9.0.00.01
Log	2.7.00.03 (latest)
Unix and Linux - HP-UX and Linux	9.11.00

Name: *
 The installation package **Name** can only contain alphanumeric Latin characters and underscores.

Description:

Format: *

*.zip
 *.tar
 *.tar.gz

Download
Save Installation Package

* Mandatory fields

24. Download the package and SCP/SFTP to a “target” Linux host. The file size of the tar file will be +550 MB in size. SCP the file as the **bppmagent user** to bppmagent home directory on target server.

INSTALLING IMAGE (SILENT INSTALL)

This section will step through installing the image created from the previous section.

User for running the agent: **bppmagent**
Sudo sser to run post scripts: **karlis.peterson**

```
[bppmagent@bldb01 bmc]$ cd /home/bppmagent
```

```
[bppmagent@bldb01 ~]$ ls
```

```
Linux64_Base.tar
```

```
[bppmagent@bldb01 ~]$ mv Linux64_Base.tar /tmp/Linux64_Base.tar
```

```
[bppmagent@bldb01 ~]$ cd /tmp
```

```
[bppmagent@bldb01 tmp]$ tar -xvf Linux64_Base.tar
```

```
[bppmagent@bldb01 tmp]$ su karlis.peterson
```

```
Password:
```

```
[karlis.peterson@bldb01 tmp]$ sudo chown bppmagent /opt/bmc
```

```
[sudo] password for karlis.peterson:
```

```
[karlis.peterson@bldb01 tmp]$ su bppmagent
```

```
Password:
```

```
[bppmagent@bldb01 tmp]$ cd /tmp/bmc_products/
```

```
[bppmagent@bldb01 bmc_products]$ ./RunSilentInstall.sh
```

```
...
```

```
Unable to run script [root@/opt/bmc/Patrol3//bin/PtDLLSecurity /opt/bmc/Patrol3/] as user [root] because the login name was not specified. The script has to be run manually later as root.
```

```
[bppmagent@bldb01 bmc_products]$ su karlis.peterson
```

```
Password:
```

```
[karlis.peterson@bldb01 2013_05_11_23_37_28_install]$ sudo chmod +x bldb01_3181_install_rootscripts
```

```
[sudo] password for karlis.peterson:
```

```
[karlis.peterson@bldb01 2013_05_11_23_37_28_install]$ sudo ./bldb01_3181_install_rootscripts
```

```
...
```

```
PatrolAgent V9.0.00.1i, built at 20:32:03, Jul 6 2012
Copyright (C) 1997-2012 BMC Software, Inc.
Configuration successfully loaded "/opt/bmc/Patrol3/lib/integrationservice.cfg"

PatrolAgent V9.0.00.1i, built at 20:32:03, Jul 6 2012
Copyright (C) 1997-2012 BMC Software, Inc.

Configuration successfully loaded "/opt/bmc/Patrol3/lib/eventintegration.cfg"
[LOG]:[23:46 05/11/2013]:INFO:[PtDLLSecurity]: [/etc/patrol.d/patrol.conf] allows all dll's. Nothing further to do.
[DONE]
```

***For Linux you must run this additional command.*

```
[karlis.peterson@bldb01 Patrol3]$ sudo /opt/bmc/Patrol3/b1config9000.sh
```

```
...
Changing ownership and permissions of files in bin directory
Changing ownership and permissions of files in bin directory
Changing permissions of files in bin directory
Changing permissions of files in local directory
Changing permissions and ownership of bgs/log directory
Security Level > 1
Creating link from: '/opt/bmc/Patrol3/Linux-2-6-x86-64/best1/9.0.00' to: '/usr/adm/best1_default'
Creating link from: '/opt/bmc/Patrol3/Linux-2-6-x86-64/best1/9.0.00' to: '/usr/adm/best1_9.0.00'
Linking /usr/adm/best1_9.0.00/bgs/bin/perl to /etc/bgs/PERL/perl
Enabling continuous disk IO history
Configuring permissions and ownership of /opt/bmc/Patrol3/Linux-2-6-x86-64/best1/9.0.00
Installation complete
[VIEWLOG_MSG]b1config.sh: Changing permissions on b1config.sh.LOG file
[VIEWLOG_MSG]b1config.sh: Changing ownership of b1config.sh.LOG file
[VIEWLOG_MSG]b1config.sh: Done
```

```
[karlis.peterson@bldb01 Patrol3]$ su bppmagent
```

```
[bppmagent@bldb01 Patrol3]$ /opt/bmc/Patrol3/PatrolAgent &
```

```
[1] 392
[bppmagent@bldb01 Patrol3]$
PatrolAgent V9.0.00.1i, built at 20:32:03, Jul 6 2012
Copyright (C) 1997-2012 BMC Software, Inc.

[1]+ Done          /opt/bmc/Patrol3/PatrolAgent
```

```
[bppmagent@bldb01 Patrol3]$ ps -ef | grep Patrol
```

```
502  416  1 0 07:26 ?    00:00:00 PatrolAgent
502  500 351 0 07:38 pts/1 00:00:00 grep Patrol
```

INTEGRATING WITH AUTOMATION TOOLS

Once the Patrol Agent has been installed and running, you can now create 2 smaller compressed (tar) files which can be leveraged by tools such as Puppet and Chef. The size of the files will be ~1/3 of the size of the installable image from the previous section.

CREATE COMPRESSED (TAR) FILES FROM RUNNING AGENT

Logon to a Linux server with a Patrol Agent running and follow the steps to create 2 compressed files.

```
[karlis.peterson@bldb01 tmp]$ tar -pcvzf /tmp/Linux64_AgentBase.tar.gz /opt/bmc
```

```
[karlis.peterson@bldb01 tmp]$ tar -pcvzf /tmp/Linux64_AgentBase2.tar.gz /etc/patrol.d
```

```
[karlis.peterson@bldb01 tmp]$ ls -la Linux*
```

```
-rw-r--r-- 1 karlis.peterson karlis.peterson 185441217 May 12 10:37 Linux64_AgentBase.tar.gz
```

```
-rw-rw-r-- 1 karlis.peterson karlis.peterson 2977 May 12 15:08 Linux64_AgentBase2.tar.gz
```

Now copy (SCP/SFTP) the 2 files to a remote location, where the files will be distributed with an automation tool.

EXTRACTING COMPRESSED (TAR) FILES ON A TARGET HOST

This section will walk through manually uncompressing the files and running a script. These steps can be easily automated with other tools.

Once the 2 files have been copied to a target host system (with SAME user credentials for Patrol Agent), follow the next steps. In this example, the sudo user “karlis.peterson” used WinSCP to move the files to home directory (/home/karlis.peterson). Open an ssh session as the sudo user and then goto root directory. You will need to extract files from ‘/’.

```
[karlis.peterson@bldb01 /]$ cd /
```

```
[karlis.peterson@bldb01 /]$ sudo tar -pxvf /home/karlis.peterson/Linux64_AgentBase.tar
```

```
....
opt/bmc/Install/insthist/uninst_ux/uninstal.xml
opt/bmc/webcentral/
opt/bmc/webcentral/km_services/
opt/bmc/webcentral/km_services/html/
opt/bmc/webcentral/km_services/html/default/
opt/bmc/webcentral/km_services/html/default/lib/
opt/bmc/webcentral/km_services/html/default/lib/help/
opt/bmc/webcentral/km_services/html/default/lib/help/EN_USA/
opt/bmc/webcentral/km_services/html/default/lib/help/EN_USA/puk_9.11.00_en_usa.jar
opt/bmc/webcentral/install/
opt/bmc/webcentral/install/kmuaddhelp.sh
opt/bmc/webcentral/install/kmudeletehelp.sh
opt/bmc/log/
opt/bmc/log/2013_05_11_23_37_28_install/
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install_user
```

```
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install-output.log
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install-product.log
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install_rootscripts
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install-user.log
opt/bmc/log/2013_05_11_23_37_28_install/bldb01_3181_install-display
```

```
[karlis.peterson@bldb01 /]$ sudo tar -pxvf /home/karlis.peterson/Linux64_AgentBase2.tar.gz
```

```
etc/patrol.d/
etc/patrol.d/dlls.conf
etc/patrol.d/patrol.conf
etc/patrol.d/bak/
etc/patrol.d/security_policy_v3.0/
etc/patrol.d/security_policy_v3.0/site.plc
etc/patrol.d/security_policy_v3.0/signer.plc
etc/patrol.d/security_policy_v3.0/verifier.plc
etc/patrol.d/security_policy_v3.0/proxy.plc
etc/patrol.d/security_policy_v3.0/client.plc
etc/patrol.d/security_policy_v3.0/agent.plc
etc/patrol.d/security_policy_v3.0/bak/
etc/patrol.d/security_policy_v3.0/esi.plc
```

```
[karlis.peterson@bldb01 /]$ cd /opt/bmc/log
```

```
[karlis.peterson@bldb01 log]$ ls (**this is a dynamic created folder based!)
```

```
2013_05_11_23_37_28_install
```

```
[karlis.peterson@bldb01 log]$ cd 2013_05_11_23_37_28_install/
```

```
[karlis.peterson@bldb01 2013_05_11_23_37_28_install]$ ls
```

```
bldb01_3181_install      bldb01_3181_install_rootscripts
bldb01_3181_install-display  bldb01_3181_install_user
bldb01_3181_install-output.log  bldb01_3181_install-user.log
bldb01_3181_install-product.log
```

```
[karlis.peterson@bldb01 2013_05_11_23_37_28_install]$ sudo ./bldb01_3181_install_rootscripts
```

```
[sudo] password for karlis.peterson:
```

```
...
[LOG] Begin execution of policy_install.sh
[LOG] Parameters passed in:
[LOG] 1. Source Policy File: /opt/bmc/common/security/config_v3.0/client.plc
[LOG] 2. Dest Policy File: client.plc
[LOG] 3. Overwrite Flag: FALSE
[LOG] OVERWRITE = FALSE. Do not update security policy.
```

```
./bldb01_3181_install_rootscripts: line 46: /opt/bmc/Patrol3/scripts.d/mod_patrolconf.sh: No such file or directory
```

```
PatrolAgent V9.0.00.1i, built at 20:32:03, Jul 6 2012  
Copyright (C) 1997-2012 BMC Software, Inc.
```

```
Configuration successfully loaded "/opt/bmc/Patrol3/lib/integrationservice.cfg"
```

```
PatrolAgent V9.0.00.1i, built at 20:32:03, Jul 6 2012  
Copyright (C) 1997-2012 BMC Software, Inc.
```

```
Configuration successfully loaded "/opt/bmc/Patrol3/lib/eventintegration.cfg"
```

```
[LOG]:[15:30 05/12/2013]:INFO:[PtDLLSecurity]: [/etc/patrol.d/patrol.conf] allows all dll's. Nothing further to do.  
[DONE]
```

```
[karlis.peterson@bldb01 2013_05_11_23_37_28_install]$ su bppmagent
```

```
Password:
```

```
[bppmagent@bldb01 2013_05_11_23_37_28_install]$ cd /opt/bmc/Patrol3
```

```
[bppmagent@bldb01 Patrol3]$ ./PatrolAgent &
```

```
PatrolAgent V9.0.00.1i, built at 20:32:03, Jul 6 2012  
Copyright (C) 1997-2012 BMC Software, Inc.
```

```
[1]+ Done ./PatrolAgent
```

```
[bppmagent@bldb01 Patrol3]$ ps -ef | grep PatrolAgent
```

```
502 17399 1 0 15:34 ? 00:00:00 PatrolAgent  
502 17434 17357 0 15:36 pts/1 00:00:00 grep PatrolAgent
```

FEEDBACK AND ENHANCEMENTS

Please provide feedback or enhancements to karlis.peterson@bmc.com