



---

# Unified Assurance and Analytics On-Prem Deployment Guide

Release 23.08.64

Issue 1.1 | December 14, 2023 | 450-3704-300-2308

# Table of Contents

Publication history . . . . .	5
Installation overview . . . . .	6
Other installation notes . . . . .	6
High-level installation steps . . . . .	8
Installation requirements . . . . .	9
Server hardware and VM requirements . . . . .	10
Notes for HA . . . . .	10
Required open ports . . . . .	11
Incoming Ports . . . . .	11
Outgoing Ports . . . . .	12
Geo Redundancy ports . . . . .	13
Georedundancy Notes . . . . .	13
Downloading the installation files . . . . .	14
Required installation files . . . . .	14
Downloading the installation files from Ciena Portal . . . . .	15
Installing the operating system . . . . .	18
Pre-installation procedures . . . . .	22
Creating the bpadmin user . . . . .	23
Configuring the swappiness kernel parameter . . . . .	24
Installing the LinuxIntel system bundle . . . . .	25
Transferring the installation files to the host . . . . .	26
Host setup and BPUAA installation (non-GR deployments) . . . . .	28
Updating the hosts file . . . . .	30
Modifying the volume group name . . . . .	32
Configuring a time source . . . . .	33
Modifying system logging path . . . . .	36
Configuring the Blue Planet email service . . . . .	37
Modifying the ILAN NET interface . . . . .	38
Modifying the default BPUAA interface . . . . .	39
Specifying the external license server . . . . .	40
Setting up users . . . . .	41
Configuring the BPUAA hosts . . . . .	42
Verifying Configuration . . . . .	43
Configure the Sharding options before installing BPUAA . . . . .	43
Installing the BPUAA platform and solutions . . . . .	45
Verifying installation . . . . .	46
Host setup and BPUAA installation (GR deployment - automatic) . . . . .	47
Updating the hosts file . . . . .	48
Modifying the volume group name . . . . .	53
Configuring a time source . . . . .	55
Configuring geographical redundancy . . . . .	58
Modifying system logging path . . . . .	60
Configuring the Blue Planet email service . . . . .	61

Modifying the ILAN NET interface . . . . .	63
Modifying the default BPUAA interface. . . . .	64
Specifying the external license server . . . . .	65
Setting up users . . . . .	66
Validating the hosts . . . . .	67
Configuring BPUAA hosts on active and standby sites. . . . .	68
Installing Core Platform and Extended Platform Solution on active and standby sites . . . . .	70
Installing BPUAA and configuring georedundancy on active and standby sites (automatic procedure) . . . . .	71
Post-installation procedures . . . . .	77
Changing the Sharding options after installing BPUAA. . . . .	78
Modifying ZooKeeper Configuration . . . . .	80
Changing the default passwords . . . . .	81
Enabling Kafka log messages for file import (Optional) . . . . .	82
Clean up BPUAA installation. . . . .	83
Installing RDC (Light Weight Data Collector) . . . . .	84
Installation pre-requisites . . . . .	84
Installing RDC (LWDC). . . . .	84
Installing and Configuring RDC (LWDC) . . . . .	85
Configuring BP firewall . . . . .	89
Overview . . . . .	89
Configuring Custom Rules . . . . .	89
Configuring an Open TCP and UDP port . . . . .	89
Activating bpfirewall Configuration Changes . . . . .	90
Life-cycle Management of the bpfirewall Service . . . . .	90
Examples. . . . .	91
Appendices . . . . .	92
Host setup and BPUAA installation (GR deployment manual) . . . . .	93
Updating the hosts file . . . . .	96
Modifying the volume group name . . . . .	98
Configuring a time source. . . . .	99
Configuring geographical redundancy . . . . .	102
Configuring the Blue Planet email service . . . . .	103
Modifying the ILAN NET interface . . . . .	105
Modifying the default BPUAA interface. . . . .	107
Specifying the external license server. . . . .	108
Setting up users . . . . .	109
Installing SNMP packages in UAA containers . . . . .	110
Example Node action Script . . . . .	111
Validating the hosts. . . . .	113
Configuring BPUAA hosts on active and standby sites. . . . .	114
Installing Core Platform and Extended Platform Solution on active and standby sites . . . . .	115
Installing BPUAA on geographical redundant sites (manual procedure). . . . .	116
Configuring GR on the active site. . . . .	118
Configuring GR on the standby site . . . . .	118
Uninstalling. . . . .	120

Uninstalling BPUAA software (non-GR deployments) . . . . .	121
Uninstalling BPUAA (deployment with GR) . . . . .	122
Adding and replacing BPUAA hosts . . . . .	124
Adding and replacing hosts in non-geored or for geo-red hosts 1 or 2 . . . . .	124
Adding and replacing BPUAA geored hosts . . . . .	128
Troubleshooting . . . . .	133
Displaying installation logs . . . . .	137
Contacting Blue Planet . . . . .	138
LEGAL NOTICES . . . . .	139

# Publication history

The following table lists the 23.08.64 *Blue Planet BPUAA Installation Guide* publication history.

Table 1. Publication history

DATE	VERSION	NOTES
14-Dec-2023	1.1	Initial 23.08.64 (MR2) release  Updated the below section with swagger API details: <ul style="list-style-type: none"><li>• Installing BPUAA and configuring georedundancy on active and standby sites (automatic procedure)</li></ul>
21-Nov-2023	1.0	Initial 23.08.64 (MR2) release
25-Oct-2023	1.0	Initial 23.08.61 (MR1) release
14-Aug-2023	1.0	Initial 23.08 release

# Installation overview

This guide provides procedures to install the Unified Assurance and Analytics platform and solutions in a single-host or multi-host deployment on any of the following operating systems:

- Red Hat Enterprise Linux (RHEL) 7.9
- CentOS 7.9
- Oracle Linux 7.9

You can install BPUAA on the operating systems that qualify CIS level 1.

- Blue Planet requires vanilla, base ISO DVD RHEL/CentOS/Oracle Linux, DVD installation not patched for updates. The installation files provide the necessary RPM repos. Disable all existing repos in `/etc/yum.repos.d/` before you begin the BPUAA installation to ensure the correct versions of Docker, Open vSwitch and BPUAA files are installed. The future OS updates are supported by BPUAA (via yum updates), updates can also be done after BPUAA is installed, the only requirement is that BPUAA should be correctly stopped before you perform the OS update operation.
- Disable all firewalls and firewalld daemons. BPUAA implements specific iptables rules for Docker and other solutions during installation. If you want to add firewall functionality to the site, use the supported bpfirewall service. Documentation for bpfirewall is provided upon request.
- Installing requires root-level access. The bpadmin user is created with passwordless sudoers access as detailed during the install guide below. During installation, the bpadmin user will create the bpuser user which has a limited set of sudoers access to run Docker and infrastructure operations specifically. Modifying bpuser permissions is prohibited.
- During installation, specific directories, such as `/opt/ciena`, are created. Modification the permissions of these directories is prohibited.

## Other installation notes

- The installation procedures explained in this guide refers to an example of a three node cluster solution. However, you can install BPUAA on a single VM for LAB/POC testing or more than single VM in production environment.
- Contact Blue Planet Support to install BPUAA with large node clusters.
- Before you begin installation, ensure that you have an understanding of the Linux systems and commands and the BPUAA systems.




- For better experience and reduced copy errors of the commands, we recommend you use Adobe Reader to open the document.
- Unified Assurance and Analytics is a combination of BP Assurance or vSure and BP Analytics or NHP. This is a new fully integrated micro-service architecture, which is packaged into multiple containers as opposed to the previously used format RPM's with third party dependencies with BP Assurance.

The following table compares older Assurance RPM's with the new BP containers

*Table 2. Comparison*

CLUSTER/CONTAINER NAME	VSURE
uaa-core-db	Master DB
uaa-pm-db	Shard DB
uaa-pm-db-scheduler	PM loaders
uaa-graph-db	Graph DB
uaa-cache	Redis server
uaa-core	Application server
uaa-fme	Application server
uaa-med-fme	Mediation server
uaa-sbc	Mediation server
uaa-med-core	Mediation server
uaa-med-sae	Mediation server
uaa-logstash	Mediation server
uaa-med-pme	Mediation server
uaa-ui	Client
kafka	Kafka
zookeeper	Zookeeper

# High-level installation steps

<b>Step 1</b> 	<a href="#">Installation requirements</a>  Ensure your server meets the requirements and firewall ports are open
<b>Step 2</b> 	<a href="#">Download the installation files</a>  Download the files you need for installation
<b>Step 3</b> 	<a href="#">Install the operating system</a>  Install RHEL, CentOS or Oracle Linux
<b>Step 4</b> 	<a href="#">Perform pre-installation procedures</a>  Perform tasks such as creating the bpadmin user, configuring the swappiness kernel parameter, transferring files to the host, and installing the license server.  <div data-bbox="500 1192 565 1255">  </div> <div data-bbox="641 1161 1365 1287"> <p>Make sure to follow <a href="#">Configuring the Blue Planet email service</a> to configure SMTP emails which are used for alarm notifications and forgotten password assistance.</p> </div>
<b>Step 5</b> 	<a href="#">Setup hosts and install BPUAA (non-GR deployments)</a> or <a href="#">Setup hosts and install BPUAA (GR deployments)</a>  Setup and configure the hosts, set up licenses, and install the software

Additional procedures:

- [Installing BPUAA on geographical redundant sites \(manual procedure\)](#)
- [Uninstalling](#)
- [Displaying installation logs](#)



# Installation requirements

BPUAA installation requires:

- That your server meets the requirements listed in the [Server hardware and VM requirements](#) topic.
- That firewall ports listed in the [Required open ports](#) topic are open so communication among the Blue Planet BPUAA hosts and components are not blocked.
- Proficiency using UNIX commands including use of the vi editor.
- Have downloaded the 23.08 Blue Planet Security Guide.
- Are aware of OS hardening restrictions as described in “Host OS CIS hardening, Special Considerations” section of the 23.08 Blue Planet Security Guide.

# Server hardware and VM requirements

This section discusses the BPUAA server hardware and virtual machine (VM) requirements.

Requirements are based on the following two environments:

- Production—Appropriate for horizontally-scaled high availability environments in enterprise business deployments and operations.
- Lab development—Appropriate for testing a full BPUAA solution stack in a complete service lab with a small number of representative services that are not at the production scale. Lab development hosts are typically used for training, testing, and proof of concept tasks.

Requirements notes:

- Ensure that the server meets the requirements for BPUAA as provided in the *BP\_Engineering\_Guide.pdf*.
- Ensure that the disk space requirements are specific to BPUAA; they do not include operating system requirements. For total disk space, use the requirements from your OS vendor and site administrator.
- If there are separate hardware volumes, place BPUAA on a volume that is separate from your OS volume.
- You must install the feature licenses on the license server to access different BPUAA features. For more information, see the *License Server Documentation (External License Server 10.1-14)*.
- Never use lab development servers in production environments. Conversely, if lab development hosts will emulate a production environment, they should meet production host requirements.
- VMs must have dedicated virtual CPUs (vCPUs) and RAM, and storage. Do not use shared disks. Do not share CPUs with other VMs on the host. The number of vCPUs available on a physical CPU is equal to the number of threads or logical processors. For example, a system with 2xE5-2640v4 (2.4 GHz/10-core) CPUs has 40 vCPUs total because the cores are dual-threaded: 2 CPUs x 10 cores x 2 threads/core. The required CPU resources must be fully reserved for BPUAA and not over subscribed.

## Notes for HA

To ensure that the HA functionality works properly:

- At least three nodes must exist in the cluster so that in case of a failure, remaining nodes can identify a leader and maintain a quorum while continuing to provide service.

- LANs must pass GRE protocol packets since Blue Planet builds its own Layer 2 network over Layer 3 with generic routing encapsulation (GRE) tunnels for intra-site and intra-component communications.
- Latency between nodes in the cluster must be less than 2ms 100% of the time and less than 1ms 99.9% of the time .
- LANs must be secure since traffic on this network is not encrypted. Each Blue Planet site owns a logical IP address that can be reassigned to any node. This ensures no disruption occurs during the communication with external entities.

## Required open ports

The ports listed in the following table must be open to allow communication among BPUAA hosts and components, which indicates communication within the network. Ports include:

- Incoming ports—The bpfirewall service manages only incoming ports in the firewall settings once the BPUAA is installed and the default system firewall should not be enabled.



In case, bpfirewall needs to be configured for any custom incoming ports, please contact blue planet support for assistance. Alternatively, the users can access the BP Firewall section for help in configuring bpfirewall.

- Outgoing Ports—By default, all outgoing ports are managed by the customers and bpfirewall does not play any role in managing outgoing ports.
- Georedundancy (GR) ports—Used for communication between two GR sites.

## Incoming Ports

The following table lists default incoming ports that are managed by bpfirewall service. .BPUAA default open incoming ports

PORT	PROTOCOL	SERVICE
22	TCP	SSH server - Used for BPUAA server administrative access
443	TCP	REST API, HTTPS
162	UDP	SNMP Trap
5514	TCP	Syslog TCP listener

PORT	PROTOCOL	SERVICE
5045	TCP	Telemetry PM
5046	TCP	Telemetry Fault
9443	TCP	SBC Site to Site Protocol - Used for remote LWDC connection

## Outgoing Ports

The following table lists the default outgoing ports used by BPUAA. Based on the requirements such as using a different port for SNMP device communication than 161 mentioned in the table, customers can configure them accordingly.

*Table 3. BPUAA outgoing ports*

PORT	PROTOCOL	SERVICE
53	UDP/TCP	DNS client - Allows the BPUAA server to resolve names
67, 68	UDP	DHCP client (optional) - Allows the BPUAA server to get IP addresses through DHCP
123	UDP	NTP client - Used to set the time on the BPUAA server.
7071	TCP	License client – Allows communication with license server
23	TCP	TL1
80	TCP	HTTP
161	UDP	SNMP
443	TCP	Resource Adapter installation
9443	TCP	SBC Site to Site Protocol - Used for remote LWDC connection

## Geo Redundancy ports

Table 4. BPUAA Georedundancy ports

PORT	PROTOCOL	SERVICE
22	TCP	SSH
443	HTTPS	
500	UDP	Standard IPsec Internet Key Exchange (IKE) port

## Georedundancy Notes

If a firewall exists on the network path between georedundant (GR) sites, you (or your administrator) must configure it to allow IPsec traffic. You can usually do this by configuring the following:

- Port 500—Must be open for IPsec IKE and Internet Security Association and Key Management Protocol (ISAKMP) communication.
- ACL lists—Must permit IP IDs 50 and 51 on both inbound and outbound filters. IDs 50 and 51 must be enabled in firewalls, VPN gateways, and routers.
- IP ID 50—Must allow IPsec Encapsulating Security Protocol (ESP) communication.
- IP ID 51—Must allow Authentication Header (AH) communication.



Port Address Translation (PAT) is not supported between GR sites. ESP (IP ID 50) is used for encryption. Blue Planet does not recommend using VPNs with Network Address Translation (NAT) on the network path between georedundant sites.

//IMPORTANT README: BEFORE YOU EDIT THIS PAGE, READ ALL THE COMMENTED SENTENCES, BECAUSE, SEPARATE SECTIONS ARE CREATED FOR ROA, BPI and BPO

# Downloading the installation files

## Required installation files

You must download the following files that are required to install BPUAA.

*Table 5. Installation files*

FILENAME	DESCRIPTION	CIENA PART #
LinuxIntel_2023_39_0.tar	Contains updated host applications required by BPUAA including Docker, OpenVswitch, and bp2hosttools.	LINUX_2023_x_x
bpi-<bpi-version>.sh	Contains the Blue Planet installation scripts	BPI_23.08-xx
<lineup file>.yaml	Lineup file which contains the list of solutions to be downloaded and installed	Included in solution tar file

The following table lists the solutions and lineup files that are extracted from the `bp_uaa_23.08.00-72.tar` file. The software package prepared for you will be based on one of these lineups:

*Table 6. Lineup files*

LINEUP FILE NAME	DESCRIPTION
lineup-uaa-single-rhel.yaml	Installs only BPUAA without integrators on a single host machine.
lineup-uaa-multi-rhel.yaml	Installs only BPUAA without integrators on a multi host machine.



While `LinuxIntel_2023_39_0.tar` and `bpi-23.08-15.sh` are the current versions, later versions might be available at the time you download the file. If so, use the later version.

# Downloading the installation files from Ciena Portal

Before you begin, verify that you have:

- A computer with web access separate from the host server where you will install BPUAA.



Download the installation files on a computer separate from the BPUAA host. Do not transfer them to the BPUAA host until instructed to do so.

- Ciena portal (<https://my.ciena.com>) account for your organization and the ability to log in as a registered user. If you do not have an account, visit <https://my.ciena.com/CienaPortal/s/SelfRegisterForm>.

## To download files

1. As a registered user, log in to <https://my.ciena.com>.
2. Navigate to your web browser's preferences and configure it to allow popups for my.ciena.com. (Files will not download if popups are blocked.)
3. Click the **Support** tab.
4. Select **Software**.
5. Select the company from the **Browse Downloads** list.
6. Click **Proceed**.
7. In the AVAILABLE DOWNLOADS list, select the solution to install:
  - **Blue Planet Unified Assurance and Analytics**,
8. Find the following file. (To facilitate the search, click the **CIENA PART #** column heading to sort the results by part number.)

Ciena Part #	File name	Description
LINUX_2023_39_0	LinuxIntel_2023_39_0.tar	Ciena Linux system bundle



LINUX\_2023\_39\_0 is the minimum version. Later versions could be posted at the time of your download. If you download a later version, replace LINUX\_2023\_39\_0 with the version you downloaded.

9. Click the LinuxIntel\_2023\_39\_0.tar link.
10. On the Software Download for LinuxIntel\_2023\_39\_0.tar (or later version) window, read the Ciena Software License, then:
  - a. Select a country in the Select Your Location list.
  - b. Check **I understand and accept these conditions**.
  - c. On the Software Download for LinuxIntel\_2023\_39\_0.tar, copy the MD5 checksum to a text file and save it. (The checksum is also provided in the Release Info document.)
  - d. Click **Download**.

The LinuxIntel\_2023\_39\_0.tar (or later version) file is downloaded to your computer Downloads directory.



Many factors can affect download speed including internet connection throughput and other variables. If you cancel or lose your connection, you must start the download process again.

- e. In the RELEASE INFO column, click the PDF icon to display, then save this file to your computer for future reference.
- f. Verify the checksum recorded in step 10c.

```
md5sum LinuxIntel_2023_39_0.tar
```

- g. If the checksum does not match the value recorded in step 10c, download the file again and repeat this step. Otherwise, continue with the next step.
11. On the Ciena Portal, find the software package of BPUAA prepared for your organization by Ciena Part #.

CIENA PART #	FILE NAME	DESCRIPTION
BPUAA_MR2_23_08	bp_uua_23.08.00-72.tar	Blue Planet Unified Assurance and Analytics 23.08.64

- a. Click the software package link and complete steps 10a-10d to download the file to your computer. When you display the Release Info document, check whether bpi-23.08-15.sh is the version you should download. If not, record the later version. You will download it next.
12. On the Ciena Portal, find the Blue Planet installer file or bpi-23.08-xx.sh.



---

Ciena Part #	File name	Description
BPI_23_08_02	bpi-23.08-15.sh	Blue Planet Installer 23.08.64

- a. Click the BPI\_23\_08\_02 software link and complete steps 10a-10d to download the file.
13. Retain the files in their current location. You will transfer them to the BPUAA host after you install RHEL and complete other preparation procedures.

# Installing the operating system

BPUEA requires one of the following operating systems with the Infrastructure Server package:

- Red Hat Enterprise Linux (RHEL) 7.9
- Oracle Linux 7.9
- CentOS 7.9



Throughout this procedure, "OS" refers to the supported RHEL, Oracle Linux, and CentOS releases listed above.



Ciena requires that the OS Infrastructure Server package be based on the baseline ISO DVD image for each release. Installing an updated Infrastructure Server package is not supported.

During the OS installation, you choose options that facilitate the installation and operations. If the OS is already installed, review the installation steps to ensure the selected options are provisioned on your host. If you have any questions, contact Ciena Customer Support.

In this procedure you will:

- Download the OS ISO image and place it on a USB stick.
- Boot the server from the USB.
- Set the server date and time.
- Select the software to install and the install destination.
- Set the disk partitioning scheme.
- Configure the root partition.
- Set the root password.

Before you begin, verify that:

- All hosts where you will install the OS meet the requirements listed in the [Installation requirements](#) topic.
- You can download the OS Infrastructure Server base package, or the Oracle Linux Red Hat Compatible Kernel.



This is an example. Modify the steps to fit your OS media.

## To install the operating system

1. Download the [Red Hat](#) x86\_64bit server ISO image.
2. Place the downloaded OS image on a USB stick. For Unix, enter the correct device (for example, `/dev/sdb` or `/dev/sdc`). For Mac OSX, select the correct USB device `/dev/disk number`. For more information, see the [Red Hat Customer Portal](#).

### Unix machine:

```
sudo dd if=rhel-server-7.7-x86_64-dvd.iso of=/dev/sdb bs=8M
sudo fdisk -l
```

### Mac OSX:

```
diskutil list
sudo dd if=rhel-server-7.7-x86_64-dvd.iso of=/dev/disk4 bs=4096
```

3. Set up the BIOS to boot from the USB stick, then restart your computer.
4. After the host boots, the OS welcome screen displays. Select the language, English (United States), for example, then click **Continue**.

The Installation Summary window displays.

5. On the Installation Summary window, click **DATE & TIME** then, on the DATE & TIME window, select the region to use for the server timezone. Ciena recommends that you set the timezone to **GMT**.
6. Click **Done**.
7. On the Installation Summary window, click **Software Selection**.
8. On the Software Selection window, select the **Infrastructure Server** installation. Do not select any options in the Add-ons for the selected Environment panel.



Failing to choose the Infrastructure Server option will cause the installation to fail.

9. Click **Done**.

The system automatically detects the live network interface for Network & Host Name.

10. On the Installation Summary window, click **Installation Destination**. The Installation Destination window displays.
11. On the Installation Destination window, be sure that the Local Standard Disk option displayed is selected, then select the option in **Other Storage Options**—Select **I will configure partitioning**.

12. Click **Done**. The Manual Partitioning window displays.
13. For the partitioning scheme, select **LVM**.
14. Select **Click here to create them automatically** to specify the LVM mount points. The Manual Partitioning window displays the information shown below. On the Manual Partitioning window, complete the following steps:
  - a. Record the amount of home storage space.
  - b. Select the **/home** partition, then click "-" to delete.
  - c. Verify the swap partition meets the requirements specified in the server hardware and VM requirements table in [Server hardware and VM requirements](#) .
  - d. Verify the / (root) partition and add the space that was assigned to the /home partition in step a. Leave 200 GB of disk space for Docker storage. This space can be in the form of an additional unpartitioned disk.
  - e. Select the **/boot** partition and increase the partition to 1024 MB.
  - f. Click "+" to add the `/opt/ciena` mount point, set the Desired Capacity as specified in the *Engineering Guide* and click **Add mount point**.
  - g. Click "+" to add the `/opt/ciena/bp2` mount point, set the Desired Capacity as specified in the *Engineering Guide* and click **Add mount point**.
  - h. Click "+" to add the `/var/log` mount point, set the Desired Capacity as specified in the *Engineering Guide* and click **Add mount point**.

```
lvcreate -L +100G --name var vg_sys  
lvcreate -L +600G --name optcienabp2 vg_sys  
lvcreate -L +200G --name optciena vg_sys
```

15. Click the / (root) partition.
16. Next to Volume Group (rhel), click **Modify**. The Configure Volume Group window displays.
  - a. In the Name field, enter the volume name, which is used during installation.
  - b. From the Size Policy list, select **As large as possible**.
  - c. Click **Save**. The Partitioning window displays.
17. Click **Done**. The Summary of Changes window displays.
18. Click **Accept Changes**.
19. On the Installation Summary window, select **Network & Host Name**.
  - a. Verify that the network interface device correctly identifies the default, **KDUMP** (kernel crash dumping mechanism).

- b. Enable the Ethernet port.
  - c. Click **Done**.
20. In the Installation Summary window, click **Begin Installation**. The Configuration window displays.
21. During the installation, set the root password. (You will create a non-root bpadmin user during the Blue Planet installation.)
- a. Click **Root Password**.
  - b. Enter a password in Root Password, then enter the password again to confirm.
  - c. Click **Done**. If the password is weak, click **Done** twice to accept the weak password.



A weak password is acceptable because you will restrict the server to sshkeys access and the Red Hat or CentOS user will not have remote SSH access. You can change the password later.

- d. Click **Done** again.

# Pre-installation procedures

Before you install Blue Planet BPUAA, perform the following procedures on host 0 in sequence. For multihost installations, you do not need to repeat these procedures on other hosts unless specified in the procedure.



Ensure that you enable the features related to CIS hardening before installation. If you want to enable any other specific feature after installation, then contact Ciena support.

This section covers:

- [Creating the bpadmin user](#)
- [Configuring the swappiness kernel parameter](#)
- [Installing the LinuxIntel system bundle](#)
- [Transferring the installation files to the host](#)

The following table provides an overview to the pre-installation procedures, where you perform them, and key notes.

*Table 7. BPUAA pre-installation procedures*

PROCEDURE	LOCATION	NOTES
<a href="#">Creating the bpadmin user</a>	CLI	Required
<a href="#">Configuring the swappiness kernel parameter</a>	<code>/etc/sysctl.d/</code>	Required; creates <code>bp2-sysctl.conf</code>
<a href="#">Installing the LinuxIntel system bundle</a>	temporary directory	Required; reboot server
<a href="#">Transferring the installation files to the host</a>	<code>/home/bpadmin</code> and <code>/opt/Ciena/loads/23.08.64</code>	Required

To view the list of commands used in these procedures, see [\[Quick Reference for Commands\]](#).

## Creating the bpadmin user

The bpadmin user is given full passwordless sudo privileges. For multi-host installations, use the same bpadmin password on all hosts. The bpadmin user with full sudo access is needed to install the BPUAA applications and to create the buser, which has limited sudo access.

Complete the following procedure to create the bpadmin user on each host where you will install BPUAA. This is a mandatory procedure.

This procedure also creates the bpmain user that has privileges to perform various maintenance tasks. The bpmain user has read-only access to the product folders and it does not have sudo access.

Before you begin, ensure that you have a password that you want to assign for the bpadmin user.

### ***To create the bpadmin user***

1. Log in to the host 0 as root.
2. Create a new group:

```
groupadd bpadmin
```

3. Create the bpadmin user:

```
useradd -d <user_home> -g bpadmin -s /bin/bash -m bpadmin
```

where

<user\_home>

Is the directory of the bpadmin user. Set /home/bpadmin as the bpadmin user home directory. If you use another directory, adapt the steps through the BPUAA installation to point to that directory, as required.

4. Set the password for the bpadmin user:

```
passwd bpadmin
```

5. Enter the password, then enter it again to confirm.

6. Assign the bpadmin user full sudo privileges:

```
echo "bpadmin ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers.d/bpadmin
```

7. Disable the TTY requirement:

```
sed -i "s/^.*requiretty/#Defaults requiretty/" /etc/sudoers
```

8. Exit the root user:

```
exit
```

9. Log in to host 0 as the bpadmin user.

10. Verify that you can use the sudo command without entering a password:

```
sudo su -
```

11. For multi-host deployments, repeat this procedure on each host. Use the same bpadmin password on all hosts.

After you complete the BPUAA installation, you can optionally delete the bpadmin user and use bpuser for ongoing Docker, solman, and bp2-site operations.

## Configuring the swappiness kernel parameter

Swappiness is the kernel parameter that defines how much and how frequently your Linux kernel copies RAM contents to swap. The higher the swappiness parameter, the more aggressively your kernel will swap. Ciena recommends that you set the kernel swappiness value for each BPUAA host to 10.

This is a mandatory procedure.

### ***To configure the swappiness kernel parameter***

1. Log in to host 0 as the root user.
2. Create the `bp2-sysctl.conf` file.

```
touch /etc/sysctl.d/bp2-sysctl.conf
```



3. In the `bp2-sysctl.conf` file, set the swappiness value to 10.

```
echo "vm.swappiness = 10" >> /etc/sysctl.d/bp2-sysctl.conf
```

4. Reload the system control. This should return a 10 value.

```
sysctl -p /etc/sysctl.d/bp2-sysctl.conf
```

5. For multi-host installations, complete steps 1-4 at each host.

## Installing the LinuxIntel system bundle

The Ciena Linux system bundle contains host applications required by BPUAA including Docker, OpenVswitch, and bp2hosttools.

Complete the following procedure to install the LinuxIntel system bundle. This is a mandatory procedure.

### ***To install the LinuxIntel system bundle***

1. Log in to the computer where you downloaded the BPUAA files in the [Downloading the installation files](#) procedure.
2. Transfer the `LinuxIntel_2023.xx.x.tar`(or later version) file to a directory of your choice on the target BPUAA host. The directory must have a minimum of 2 GB of space.
3. Log in to the BPUAA host as the root user.
4. Extract the LinuxIntel bundle:

```
tar -xf LinuxIntel_2023.xx.x.tar
```

A `LinuxIntel_2023.xx.x.0` (or later) directory is created.

5. Change to the LinuxIntel directory:

```
cd LinuxIntel_2023.xx.x
```

6. Install the LinuxIntel bundle:

```
./cienabundle.sh
```

## 7. Reboot the server:

```
reboot
```

## 8. If you are installing a multi-host cluster, repeat steps 1-7 at each host.

# Transferring the installation files to the host

You need to create the BPUAA installation file directories, transfer the following files to them, and then extract the files. This is a mandatory procedure.

- **bp\_uaa\_23.08.00-72.tar**
- **bpi-23.08-15.sh (or later)**
- **LinuxIntel\_2023\_39\_0.tar (or later)**



These are the files you downloaded in the [Downloading the installation files](#) procedure.

### **To extract the files**

1. Log in to the host 0 as the bpadmin user.
2. Create the `/opt/ciena/loads/23.08.64` directory:

```
sudo mkdir -p /opt/ciena/loads/23.08.64
```

3. Change the ownership of `/opt/ciena/loads/23.08.64` to bpadmin:

```
sudo chown bpadmin:bpadmin /opt/ciena/loads/23.08.64
```

4. Log in to the computer containing the files you downloaded in the [Downloading the installation files](#) procedure.
5. As bpadmin user, perform the following steps,
  - a. The `bp_uaa_23.08.00-72.tar` file to the `/opt/ciena/loads/23.08.64` directory.
  - b. The `bpi-23.08-15.sh` file to the `/home/bpadmin` directory.
  - c. The `LinuxIntel_2023_39_0.tar` file to the `/opt/ciena/loads/23.08.64` directory.
6. Change to the `/home/bpadmin` directory:

```
cd /home/bpadmin
```

7. Extract the bp\_uaa\_23.08.00-72.tar file:

```
bash {bpi-file-name}
```

The extraction creates the bpi directory: /home/bpadmin/bpi.

8. Change to the /opt/ciena/loads/23.08.64 directory:

```
cd /opt/ciena/loads/23.08.64
```



The installation procedures that follow assumes you placed the bpi-23.08-15.sh and bp\_uaa\_23.08.00-72.tar into the directories listed above. If you use other directories, modify the steps to point to your directories, as required.

9. Extract the bp\_uaa\_23.08.00-72.tar file, where bp\_uaa\_23.08.00-72.tar is the file you transferred in step 6.

```
tar -xf bp_uaa_23.08.00-72.tar
```



Do **not** untar the bp\_uaa\_23.08.00-72.tar.gz.bin file; it will be untarred by the Blue Planet installer during installation.

# Host setup and BPUAA installation (non-GR deployments)

To install Blue Planet BPUAA, perform the following procedures on host 0 in sequence. For multi-host installations, you do not need to repeat these procedures on other hosts unless specified in the procedure.

The following table provides an overview to the installation procedures, where you perform them, and key notes.

Table 8. BPUAA installation procedures

PROCEDURE	LOCATION	NOTES
<b>Initial host setup</b>		
<a href="#">Updating the hosts file</a>	/home/bpadmin/bpi/hosts	Required
<b>Installation variables</b>		
<a href="#">Modifying the volume group name</a>	/home/bpadmin/bpi/playbooks/group_vars/cluster	If needed
<a href="#">Configuring a time source</a>	/home/bpadmin/bpi/playbooks/group_vars/cluster	Required
<a href="#">Configuring the Blue Planet email service</a>	/home/bpadmin/bpi/playbooks/group_vars/cluster	Required
<a href="#">Modifying the ILAN NET interface</a>	/home/bpadmin/bpi/playbooks/group_vars/cluster	If needed
<a href="#">Modifying the default BPUAA interface</a>	/home/bpadmin/bpi/playbooks/group_vars/cluster	If needed

PROCEDURE	LOCATION	NOTES
<a href="#">Specifying the external license server</a>	/home/bpadmin/bpi/playbooks/group_vars/cluster	If needed
<b>Installation preparation</b>		
<a href="#">Setting up users</a>	<a href="#">Validating the hosts</a>	/home/bpadmin/bpi/

To view the list of commands used in these procedures, see [\[Quick Reference for Commands\]](#).

# Updating the hosts file

The Blue Planet installer uses the hosts file entries to perform the BPUAA installation.

Complete this procedure to add the host(s) where you want to install BPUAA to the hosts file. This is a mandatory procedure.



You can enter only IPv4 IP addresses in the hosts file.

## To update the hosts file

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. Open the hosts file with a text editor.
3. If your installation is single host, complete the following steps. If your installation is multi host deployment, proceed to step 4
  - a. Uncomment and set the `host0` entry to the IP address for that host. Use the host IP address IP4 (not IPv6 or the hostname).
  - b. Uncomment and set the `site_IP` variable to the IP address and subnet mask of host0.
  - c. Uncomment the `site_name` entry and replace `mysite` with your site name. Valid characters are letters, numbers, and dashes.

`site_name` allows you to associate a meaningful name with the cluster. It is not required for normal BPUAA operations, apart from certain Blue Planet microservices, such as Message Relay. Allowed characters are the same as hostnames, that is, a-z, A-Z, 0-9, and dashes.

Example of hosts file "before" the edit

```
[cluster]
#host0 ansible_host=a.b.c.d controller=True

[cluster:vars]
#site_ip=a.b.c.d/42

#site_name=mysite
```

Example of hosts file "after" the edit are made for an installation where the subnet mask is 22 (255.255.252.0):

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True

[cluster:vars]
site_ip=10.186.0.1/22
site_name=BPSite1
```

4. If your installation is multiple hosts, complete the following steps.
- Uncomment and set one host entry (for each host) to the IP address for that host. Use the host IP address of each host IP4 (not IPv6 or the hostname).
  - Set `controller=True` (the default) for up to three hosts, then `controller=False` for remaining hosts.



All cluster hosts must be on the same subnet.

- Uncomment and set the `site_IP` variable to an IP address and subnet mask for the cluster. The site IP must be an IP address on the same subnet as the host IP addresses.
- Uncomment the `site_name` entry and replace `mysite` with your site name. Valid characters are letters, numbers, and dashes.

`site_name` allows you to associate a meaningful name to the cluster. It is not required for normal BPUAA operations, apart from certain Blue Planet microservices, such as Message Relay. Allowed characters are the same as hostnames, that is, a-z, A-Z, 0-9, and dashes.

Refer to BP Engineering Guide to decide on simple vs hybrid deployments.

The following shows a sample active hosts file after the multi-host edits are made for an installation where the subnet mask is 22 (255.255.252.0):

#### Example: Simple hosts

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True

[cluster:vars]
site_ip=10.186.0.4/22

site_name=BPSite1
```

The following shows a sample hosts file (hybrid deployment). The below example is by considering 6 node cluster (3 *uaa-pm-db* only hosts).

### Example: Hybrid hosts

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True
host3 ansible_host=10.186.0.4 controller=False solution=uaa_pm_storage
host4 ansible_host=10.186.0.5 controller=False solution=uaa_pm_storage
host5 ansible_host=10.186.0.6 controller=False solution=uaa_pm_storage
[cluster:vars]
site_ip=10.186.0.4/22
site_name=BPSite1
```

5. Save the hosts file.

## Modifying the volume group name

Ciena recommends using unique names for volume group that can be recognized and avoid name conflicts across multiple virtual groups.

Complete this procedure to modify the volume group name where the unallocated physical extents space is left free for BPUAA to create and configure the Docker thin pool. This procedure is needed if you want to change the default values.



This is the first of five procedures requiring edits to the cluster file, which is `all.yml` file located in the `/home/bpadmin/bpi/playbooks/group_vars` directory. Most of the edits are "as required" by your specific network environment and BPUAA installation.

Remaining procedures include [Configuring a time source](#), [Configuring the Blue Planet email service](#), [Modifying the ILAN NET interface](#), and [Modifying the default BPUAA interface](#)

Before you begin, verify that you know the name of the volume group where the unallocated physical extents space is available for BPUAA to create and configure the Docker thin pool.



You can use the Linux `vgdisplay` command to display volume group information.

### **To modify the volume group name**



1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. Uncomment and set the `vgdockerpool` to the name of your volume group.

Example **before** the edit:

```
#bpdockerdevs: /dev/xvdb
#vgdockerpool: blueplanet
```

Example **after** the edit with `vgdockerpool` set to `my_vgname`.

```
#bpdockerdevs: /dev/xvdb
vgdockerpool: my_vgname
```

4. Save the cluster file.

## Configuring a time source

BPUAA hosts can use a local or remote time source. For example:

- In environments where an enterprise NTP source is available, you can configure the BPUAA hosts as NTP clients of the enterprise NTP host.
- If your BPUAA hosts have internet access, you can use public NTP servers as the BPUAA timing source.
- If no enterprise NTP host is available and BPUAA hosts do not have internet access, you can configure one of the BPUAA VMs to act as an NTP server. See your operating system documentation for more information.



Configure NTP in accordance with your site timeserver infrastructure. The Blue Planet installer can apply a simple configuration with one, three, or four time servers. If NTP is already configured on BPUAA host, skip this procedure and continue with the [Installation requirements](#) procedure. During the [Configuring the BPUAA hosts](#) procedure, you will add a skip NTP tags option. Details are given in the procedure.

By default, the Blue Planet installer sets up four NTP servers:

```
ntp_servers_default:
  - 0.rhel.pool.ntp.org
  - 1.rhel.pool.ntp.org
  - 2.rhel.pool.ntp.org
  - 3.rhel.pool.ntp.org
```

While you can specify your own NTP servers, or use fewer servers, Ciena recommends that you always have a minimum of three—and preferably four—timing servers for optimal BPUAA timing synchronization. The number of upstream servers, in order of most to least preferred, is given below.

- 4—Allows for one or more servers to be a "false ticker" and for one server to be unreachable.
- 3—The minimum number required to allow ntpd to detect if one is a false ticker.
- 2—Are not allowed and will be blocked. With two NTP servers, you cannot determine which timing source is better because no reference exists to compare them to.
- 1—Provides no debate as to which server is correct, but also provides no redundancy.



Disable all other timing synchronization methods including, but not limited to, VMware Tools periodic time synchronization.



Following installation, you can use the bp2-site check-platform or bp2-site check-clock-drift commands to check BPUAA timing synchronization.

Complete this procedure to configure the Network Time Protocol (NTP) server(s) to serve as the timing source for BPUAA hosts. This is a mandatory procedure.

All BPUAA hosts must be synchronized to an accurate timing source. If you want to use a local time source or custom remote time sources (different than the default ones provided), then perform this procedure.

### **To configure a time source**

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. To use a local time source, uncomment `ntp_server_type` and change its value to `local`. The default `ntp_server_type` is `remote`.

Example **before** the edit:

```
#ntp_server_type: remote
```

Example **after** the edit:

```
ntp_server_type: local
```

4. Go to step 6.
5. To use custom remote time sources, uncomment and edit the **ntp\_servers\_custom** list to include the NTP server URLs or IP addresses that you want used as the BPUAA host timing source.

Example **before** the edit for the custom remote time sources. The example focuses on the section to be edited.

```
#ntp_servers_custom:
# - <host a>
# - <host b>
# - <host c>
# - <host d>
```

Example **after** the edit using hostnames. In this example, the first NTP server to be contacted will be the one with the fully qualified domain name of 0.mycustomer.ntp.com:

```
ntp_servers_custom:
- 0.mycustomer.ntp.com
- 1.mycustomer.ntp.com
- 2.mycustomer.ntp.com
- 3.mycustomer.ntp.com
```

Example **after** the edit using IP addresses. In this example the first NTP server to be contacted will be the one with an IP address of 10.128.8.89:

```
ntp_servers_custom:
- 10.128.8.89
- 10.128.8.90
- 10.128.8.91
- 10.128.8.92
```



For all AWS and Azure servers, make sure that the IPs are custom defined by the admin and not using the default IPs.

6. By default, the **ntp\_server\_options** entry default is iburst. For details about the ntp\_server\_options, see <https://linux.die.net/man/5/ntp.conf>. If you want to change the default value, uncomment

ntp\_server\_options and edit its value.

7. Save the cluster file.

## Modifying system logging path



This is an optional procedure

By default, the path to the system logging (syslog) file for the Blue Planet UAA application is `/var/log/ciena/blueplanet.log`. If you want to modify this path, perform the following procedure to keep current release logs separate.

To modify the default system logging path:

1. Log in to host 0 as bpadmin.
2. Navigate to directory `/home/bpadmin/bpi/playbooks/group_vars`.
3. Open the `all.yml` file in a text editor.
4. In the **Logging** section, uncomment the `bp_log_dir` and `bp_log_file` parameters and modify the logging path.

Here is an example before the edit:

```
##Logging
#BluePlanet apps log file location
#'/var/log/syslog' is an invalid choice for RedHat/Oracle Linux/CentOS systems
#'/var/log/messages' is an invalid choice for Ubuntu systems
#bp_log_dir: /var/log/ciena
#bp_log_file: "{{ bp_log_dir }}/blueplanet.log"
```

Here is an example after the edit:

```
##Logging
#BluePlanet apps log file location
#'/var/log/syslog' is an invalid choice for RedHat/Oracle Linux/CentOS systems
#'/var/log/messages' is an invalid choice for Ubuntu systems
bp_log_dir: /opt/CustomLog/Pune/ciena
bp_log_file: "{{ bp_log_dir }}/bp_syslog.log"
```

5. Save the `all.yml` file and exit the text editor.

# Configuring the Blue Planet email service

BPUAA requires that you configure a Simple Mail Transfer Protocol (SMTP) server, so BPUAA can send system email to users. Emails are used for alarm notifications and forgotten password assistance.



If password expirations are enabled and the SMTP server is not configured, users will not be able to log in after their password expires. Ciena recommends if you cannot complete the configuration now, ensure you do it within 60 days to avoid causing users to be locked out with no way to reset their passwords.

For information on configuring password notifications, see the *Blue Planet BPUAA Administrator Guide*.

Complete the following procedure to configure Blue Planet email service. This is a mandatory procedure.

Before you begin, verify that you understand the SMTP server requirements at your site.

## To configure email service

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file and edit the following SMTP parameters:

Table 9. SMTP parameters

PARAMETER	DESCRIPTION
<code>smtp_username</code>	The SMTP server account username used for sending emails.
<code>smtp_password</code>	The SMTP server account password.
<code>smtp_staticPath</code>	The staticPath value must be <code>/bp2/src/static</code> . Do not change this value.
<code>smtp_authen</code>	The SMTP server authentication. Set the value to true.
<code>smtp_transport</code>	The SMTP server transport security. Set the value to true or false, as applicable.
<code>smtp_mail_server</code>	The SMTP server fully qualified domain name (FQDN), such as <code>smtp.gmail.com</code> or, if a dedicated SMTP server, an FQDN that you own.
<code>smtp_mailer_name</code>	Must be set to Blue Planet Mailer. Do not change this value.

PARAMETER	DESCRIPTION
smtp_port	The SMTP server port number. Depending on the server, this port can be 25, 465, or 587.
smtp_email	The SMTP server email account from which reset password emails will be sent. Some SMTP servers, such as Gmail, allow you to use an alias that is not set on the server. For example, the account could be "bphostmonitor@abccompany.com", but the value could be "api-crinoid@ciena.com". Of course, you can enter the true value, "bphostmonitor@abccompany.com". The Amazon Web Services (AWS) SMTP server restricts the entry to the correct value.

Example **before** the edit:

```
# SMTP configuration details for 'Forgot Password' feature
smtp_username: USERNAME
smtp_password: PASSWORD
smtp_staticPath: /bp2/src/static
smtp_authen: SMTP_AUTHENTICATION
smtp_transport: SMTP_TRANSPORTSECURITY
smtp_mail_server: MAILSERVER.COM
smtp_mailer_name: MAILER_NAME
smtp_port: SMTP_PORT
smtp_email: MAILER@EMAIL.COM
```

Example **after** the edit:

```
# SMTP configuration details for 'Forgot Password' feature
smtp_username: GmailUser
smtp_password: AnyPassword
smtp_staticPath: /bp2/src/static
smtp_authen: true
smtp_transport: true
smtp_mail_server: smtp.gmail.com
smtp_mailer_name: Blue Planet Mailer
smtp_port: 587
smtp_email: api-crinoid@AnyCompany.com
```

## Modifying the ILAN NET interface

BPUAA uses the address, 172.16.0.0/16/24, for its internal LAN (iLAN).

Complete this procedure if your network already uses 172.16.0.0/16/24, in which case, a conflict with the BPUAA iLAN will occur.

If your network does not use 172.16.0.0/16/24, you can skip this procedure and continue with the [Modifying the default BPUAA interface](#) procedure.

Before you begin, verify that you have a new address for the iLAN.

### **To modify the iLAN interface**

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. Uncomment the `ilannet` option, then enter the IP network address you want BPUAA to use, for example, 172.29.0.0/16/24.

Example **before** the edit:

```
#####  
# install #  
#####  
# The ilannet to use on hosts  
# ilannet: 172.16.0.0/16/24
```

Example **after** the edit:

```
#####  
# install #  
#####  
# The ilannet to use on hosts  
ilannet: 172.29.0.0/16/24
```

4. Save the cluster file.

## Modifying the default BPUAA interface

By default, BPUAA uses the first network interface, for Blue Planet activities. Complete the following procedure if you want to set a new default interface. Otherwise, you can skip this procedure and proceed with the next procedure.

Before you begin, verify that you can access the `/home/bpadmin/bpi/playbooks/group_vars`

directory as the bpadmin user.



To display a list of interfaces, use the `ip a s` command.

### **To modify the default interface**

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. Uncomment the `bp_interface` option and replace `eth0` with the interface you want used.

Example **before** the edit:

```
#bp_interface: eth0
```

Example **after** the edit:

```
bp_interface: eth3
```

4. Save the file.

## Specifying the external license server

Complete the following procedure if you want to set up the external license server IP address in the bpi cluster file. Perform this procedure only if needed.

1. Log in to host 0 as the bpadmin user and navigate to `/home/bpadmin/bpi/playbooks/group_vars`.
2. Open the `all.yml` file with a text editor.
  - a. Uncomment the following line:

```
#license_server:a.b.c.d
```

- b. Replace with the license server IP address. For example:

```
license_server:10.10.10.10
```



- c. Replace with the license server IP address of the backup license server. For example:

```
license_server_backup: 12.12.12.12
```

- d. Add the license server default port

```
license_server_default_port: 7071
```

3. Save the file.

## Setting up users

Complete this procedure to manage keys of the bpadmin user and the root user, and to create the bpuser user (sudo restricted Docker install user) and manage its sudo permissions and keys. This is a mandatory procedure. The setup script skips this step if you have previously manually created the bpuser user. This script also creates the bpmaint user without sudo permission, which has read only access to other product folders. The bpmaint user has the write permission to edit the bpmaint home directory to fetch and store data. You can export this data from the host using scp.

Before you begin, verify that you know the bpadmin user password and the password you want to assign to the bpuser.

### **To set up users**

1. Log in to the host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. Start the setup users script:

```
./bpi --setup-users
```

3. If prompted, enter the bpadmin user password.



You can access the single-host deployments without entering the password. For multi-host deployments, you must enter the bpadmin password for each host other than Host 0.

4. If you have not previously completed the procedure to manually create the bpuser user, then:
  - a. When prompted, enter the bpuser password.

The same password is set on all hosts.

- b. Re-enter the password for the bpuser user.

The script sets the bpadmin and bpuser authentication keys and several sudo privileges for the bpuser user. See the files in `/home/bpadmin/bpi/roles/setup-users/sudoers/templates` to see the settings.

5. If you have not previously completed the procedure to manually create the bpmaint user:
  - a. When prompted, enter the bpmaint password.
  - b. Confirm the password for bpmaint.

## Configuring the BPUAA hosts

Configuring the BPUAA host(s) creates the following directories and ensures they are owned by bpuser:

- `/etc/bp2`
- `/etc/bp2/site`
- `/etc/bp2/solutionmanager`
- `/opt/ciena/loads`

Complete the following procedure to configure the BPUAA host(s) for the BPUAA software installation. This is a mandatory procedure. This procedure also performs minor configuration changes including updates to syslog, rsyslog, sshd, and NTP to prepare the host for BPUAA installation.

If you chose not to implement the Blue Planet NTP option in the [Configuring a time source](#) procedure and will use your network NTP for BPUAA host timing, add the playbook arguments shown in the following procedure.

### ***To configure the hosts***

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. Execute one of the following commands depending on whether your installation is single-host or multi-host and your NTP timing preference.

#### **UAA without integrators on a single host machine:**

```
./bpi --site /opt/ciena/loads/23.08.64/lineup-uaa-single-rhel.yml
```

**UAA without integrators on multi-host:**

```
./bpi --site /opt/ciena/loads/23.08.64/lineup-uaa-multi-rhel.yml
```

3. If you are provisioning your own NTP timing, add the following playbook arguments:

```
./bpi --site /opt/ciena/loads/23.08.64/<lineup_file> --playbook-args='--skip
-tags ntp'
```



The lineup files used in this procedure, are also used in the [Installing the BPUAA platform and solutions](#). These files contain a customer-specific list of BPUAA solutions to install. The lineup files apply to all supported operating systems, RHEL, Oracle Linux, and CentOS.

## Verifying Configuration

After entering the command to configure, you see an output similar to the following, which indicates whether the configuration succeeded:

```
PLAY RECAP
*****
<host>                                : ok=102    changed=47    unreachable=0    failed=0
```

If no failures occur, indicated by failed=0, continue with the next step. If failures occurred, contact Ciena Customer Support for guidance.



You can see logs in the `/home/bpadmin/bpi/logs` directory.

## Configure the Sharding options before installing BPUAA

Starting UAA 22.02+, UAA-PM-DB (Clickhouse container) will by default have the following Sharding config,

- Shard and 3 Replica in case of HA deployments
- Shard and 1 Replica in case of Non-HA/Standalone deployments

Please follow the below steps to change the default Sharding config,

1. Create a new file overrides.json in /etc/bp2/uaa-pm-db/private/ in all the hosts individually and add the required Sharding option (available options mentioned below), using the below command, (ROOT permission required),

```
echo '{ "sharding_option": "3S-2R" }' > /etc/bp2/uaa-pm-db/private/overrides.json]
```

Using “3S-2R” as an example above. Please use the required option as per the deployment from one of the available options here ['1S-1R','1S-3R','3S-2R','5S-2R','5S-3R'.

Here “S” = Shard and “R” = Replica. The numbers preceding the letters indicate the corresponding count. Above example means 3 Shards and 2 Replicas for each Shard, so the deployment would need 6 UAA-PM-DB instances to have 3 Shards x 2 Replicas configured.

**Error scenario:**

1. If the UAA-PM-DB instances count do not match after installation, UAA-PM-DB would not start and an error will be shown in Nagios with appropriate message.
2. To fix this error, user would need to scale out the UAA-PM-DB to match the instances count using the below command

```
solution_app_scale artifactory.ciena.com.blueplanet.uaa_pm_storage:23.08.xy uaa-pm-db <total_number_of_instances>
```

# Installing the BPUAA platform and solutions

Complete this procedure to install the BPUAA platform and solutions. This is a mandatory procedure.

Before you begin, verify that no error displays in the [Configuring the BPUAA hosts](#) procedure.



For installing optional solutions on 23.08.xx server, copy the required solutions along with its version from `lineup-uaa-<multi/single>-optional-solutions.yml` present in BP\_UAA-TAR file to the main lineup file `lineup-uaa-<single/multi>-rhel.yml`

## Example:

For installing upgrade solution along with normal lineup, copy below snippet from `lineup-uaa-<multi/single>-optional-solutions.yml` and paste in `lineup-uaa-<single/multi>-rhel.yml`

```
uaa_upgrade_from_20_02:
  name: uaa_upgrade_from_20_02
  vendor: blueplanet
  version: 23.08.07
  scale: false
```

Make sure to add the solution name under `order_additional_solution attributes`

```
order_additional_solutions:
- uaa_upgrade_from_20_02
```

## To install BPUAA

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. Enter one of the following commands, depending on installation type.



For details about component-specific lineup files, see [Required installation files](#).

### UAA without integrators on a single host machine:

```
./bpi --install /opt/ciena/loads/23.08.64/lineup-uaa-single-rhel.yml
```

### UAA without integrators on multi-host:

```
./bpi --install /opt/ciena/loads/23.08.64/lineup-uaa-multi-rhel.yml
```



In case of errors, you need to install BPUAA afresh. For more information, see [Clean-up BPUAA installation](#).



The lineup files contain a customer-specific list of BPUAA solutions to install. The lineup files apply to all supported operating systems: RHEL, Oracle Linux, and CentOS.

## Verifying installation

After entering the command to install, you see an output similar to the following, which indicates whether the installation succeeded:

```
PLAY RECAP
*****
<host>                : ok=102    changed=47    unreachable=0    failed=0
```

# Host setup and BPUAA installation (GR deployment - automatic)

Complete the same procedures for either single- or multi-geographical redundant configurations, with the only difference being the lineup file.

These files contain a customer-specific list of BPUAA solutions to install. The lineup files apply to all supported operating systems: RHEL, Oracle Linux, and CentOS.

This section uses the following designation:

- Site A (active)
- Site B (standby)

The following table provides an overview to the installation procedures, where you perform them, and key notes.

Table 10. BPUAA installation procedures

PROCEDURE	LOCATION	NOTES
<b>Initial host setup</b>		
<a href="#">Updating the hosts file</a>	/home/bpadmin/bpi/hosts	Required
<b>Installation variables</b> These procedures require edits to the all.yml file of the active site and to the standby_cluster file of the standby site. These files are located in the /home/bpadmin/bpi/playbooks/group_vars directory of host 0 of the active site. Most of the edits are as required by your specific network environment and BPUAA installation. You might not need complete many of them unless you want to change the default values.		
<a href="#">Modifying the volume group name</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<a href="#">Configuring a time source</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	Required

PROCEDURE	LOCATION	NOTES
<a href="#">Configuring the Blue Planet email service</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	Required
<a href="#">Modifying the ILAN NET interface</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<a href="#">Modifying the default BPUAA interface</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<a href="#">Specifying the external license server</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<b>Installation preparation</b>		
<a href="#">Setting up users</a>	<a href="#">Validating the hosts</a>	/home/bpadmin/bpi/

## Updating the hosts file

This procedure adds the host(s) of active and standby sites where you want to install the BPUAA to the hosts file. The Blue Planet installer uses the host file entries to perform the BPUAA installation on both active and standby sites. This is required for all installations performed from host 0 of the active (Site A) site.

### Requirements

Before you start this procedure, you must complete the [Transferring the installation files to the host procedure](#) . NOTE: You can enter only IPv4 IP addresses in the hosts file.

### Steps

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to /home/bpadmin/bpi.



2. To copy hosts.gr file to hosts file enter:

```
cp -p hosts.gr hosts
```

3. Open the hosts file with a text editor.
4. If your installation is multi-host, complete following steps.



If your installation is single host deployment continue with step 5.

- a. Uncomment and set one host entry (for each host of active site) to the IP address for that host under the **cluster** group. Use the host IP address of each host (IPv4, not IPv6), not the hostname. Set controller=True (the default) for up to three hosts, then controller=False for remaining hosts.



All cluster hosts of active site must be on the same subnet.

- b. Uncomment and set the `site_IP` variable of active site to an IP address and subnet mask for the site under the **cluster:vars** variable. The `site_IP` of active site must be an IP address on the same subnet as the active site host IP addresses.
- c. Uncomment the **site\_name** entry and replace <mysite> with your site name of active site under the **cluster:vars** variable. Valid characters are letters, numbers, and dashes.

`site_name` allows you to associate a meaningful name to the cluster. It is not required for normal BPUAA operations, except for certain Blue Planet microservices, such as Message Relay. Allowed characters are the same as hostnames, that is, a-z, A-Z, 0-9, and dashes.

- d. Uncomment and set one host entry (for each host of standby site) to the IP address for that host under the **standby\_cluster** group. Use the host IP address of each host (IPv4, not IPv6), not the hostname. Set controller=True (the default) for up to three hosts, then controller=False for remaining hosts.



All cluster hosts of standby site must be on the same subnet.

- e. Uncomment and set the `site_IP` variable of standby site to an IP address and subnet mask for the site under the **standby\_cluster:vars** variable. The `site_IP` of standby site must be an IP address on the same subnet as the standby site host IP addresses.
- f. Uncomment the **site\_name** entry and replace <mysite> with your site name of standby site under the **standby\_cluster:vars** variable. Valid characters are letters, numbers, and dashes.

`site_name` allows you to associate a meaningful name to the cluster. It is not required for normal

BPUAA operations, except for certain Blue Planet microservices, such as Message Relay. Allowed characters are the same as hostnames, that is, a-z, A-Z, 0-9, and dashes.

The following shows an active host 0 file **before** the multi-host edits are made:

```
[cluster]
#host0 ansible_host=a.b.c.d controller=True
#host1 ansible_host=a.b.c.d controller=True
#host2 ansible_host=a.b.c.d controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False

[cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
#site_ip=a.b.c.d/XX

# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
#site_name=mysite

[standby_cluster]
#standby_host0 ansible_host=a.b.c.d controller=True
#standby_host1 ansible_host=a.b.c.d controller=True
#standby_host2 ansible_host=a.b.c.d controller=True
#standby_host3 ansible_host=a.b.c.d controller=False
#standby_host4 ansible_host=a.b.c.d controller=False
#
[standby_cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
#site_ip=a.b.c.d/XX
# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
#site_name=mysite
```

The following shows a sample of active host 0 file **after** the multi-host edits of active and standby sites are made for an installation where the subnet mask is 22 (255.255.252.0)

```

[cluster]
host0 ansible_host=10.186.34.157 controller=True
host1 ansible_host=10.186.32.105 controller=True
host2 ansible_host=10.186.33.150 controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False

[cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
site_ip=10.186.35.8/22

# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
site_name=BPSite1

[standby_cluster]
standby_host0 ansible_host=10.186.33.248 controller=True
standby_host1 ansible_host=10.186.34.218 controller=True
standby_host2 ansible_host=10.186.32.242 controller=True
#standby_host3 ansible_host=a.b.c.d controller=False
#standby_host4 ansible_host=a.b.c.d controller=False
#
[standby_cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
site_ip=10.186.35.16/22
#
# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
site_name=BPSite2

```

5. If you are installing single-host georedundancy, complete the same steps with the active and standby hosts as with multi-host and uncomment only one host as noted below. Make the Site\_IP = the host IP of that instance with a unique host name. If it is multihost, continue with step 6.
  - a. Uncomment and set the active host0 of entry to the required IP address for the active host under **cluster** group. Use the host IP address of each host (IPv4, not IPv6), not the hostname.
  - b. Uncomment and set the `site_IP` variable of active host to an IP address and subnet mask for the site under **cluster:vars** variable. For single hosts, the `site_ip` must be the host or VM IP address.
  - c. Uncomment the **site\_name** entry and replace <mysite> with your site name of active site under the **cluster:vars** variable. Valid characters are letters, numbers, and dashes.
  - d. Uncomment and set the standby host0 of entry to the required IP address for the standby host under **standby\_cluster** group. Use the host IP address of each host (IPv4, not IPv6), not the hostname.
  - e. Uncomment and set the `site_IP` variable of standby host to an IP address and subnet mask for the site under **standby\_cluster:vars** variable. For single hosts, the `site_ip` must be the host or VM IP address.

The following shows a single active host 0 example **before** the host file edit:

```
[cluster]
#host0 ansible_host=a.b.c.d controller=True
#host1 ansible_host=a.b.c.d controller=True
#host2 ansible_host=a.b.c.d controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False

[cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
#site_ip=a.b.c.d/XX

# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
#site_name=mysite

[standby_cluster]
#standby_host0 ansible_host=a.b.c.d controller=True
#standby_host1 ansible_host=a.b.c.d controller=True
#standby_host2 ansible_host=a.b.c.d controller=True
#standby_host3 ansible_host=a.b.c.d controller=False
#standby_host4 ansible_host=a.b.c.d controller=False
#
[standby_cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
#site_ip=a.b.c.d/XX
# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
#site_name=mysite
```

The following shows a single active host 0 example **after** the host file edit:

```

[cluster]
host0 ansible_host=10.186.34.157 controller=True
#host1 ansible_host=a.b.c.d controller=True
#host2 ansible_host=a.b.c.d controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False

[cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
site_ip=10.186.34.157/22

# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
#site_name=mysite

[standby_cluster]
standby_host0 ansible_host= 10.186.33.248 controller=True
#standby_host1 ansible_host=a.b.c.d controller=True
#standby_host2 ansible_host=a.b.c.d controller=True
#standby_host3 ansible_host=a.b.c.d controller=False
#standby_host4 ansible_host=a.b.c.d controller=False
#
[standby_cluster:vars]
# If uncommented, the Site IP address will be set via the set-site-ip command
# Format is IP Address/CIDR mask - e.g. 1.1.1.1/22
site_ip= 10.186.33.248/22
# If uncommented, the Site Name will be set via the set-site-name command
# Valid characters for site_name are letters, numbers and dashes.
#site_name=mysite

```

- f. Uncomment the **site\_name** entry and replace <mysite> with your site name of standby site under the **standby\_cluster:vars** variable. Valid characters are letters, numbers, and dashes.

6. Save the hosts file.

## Modifying the volume group name

Ciena recommends using unique names that can be recognized and avoid name conflicts across multiple virtual groups.

Complete the following steps to modify the volume group name where the unallocated physical extents space is left free for BPUAA to create and configure the Docker thin pool.



This is the first of six procedures requiring edits to the `all.yml` file of the active site and to the `standby_cluster` file of the standby site. These files are located in the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of the active site. Most of the edits are as required by your specific network environment and BPUAA installation. You might not need complete many of them unless you want to change the default values.

Remaining procedures include [Configuring a time source](#) , [Configuring geographical redundancy](#) , [Configuring the Blue Planet email service](#) , [Modifying the ILAN NET interface](#) , and [Modifying the default BPUAA interface](#) .

Before you begin, verify that you:

- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of the active site as the `bpadmin` user.
- Know the name of the volume group where the unallocated physical extents (PE) space is available for BPUAA to create and configure the Docker thin pool.



You can use the Linux `vgdisplay` command to display volume group information.

### ***To modify the volume group name***

1. Log in to Host 0 of Site A (active site) as `bpadmin` (do not use the Site IP; use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **`all.yml`** file.
3. Uncomment and set the **`vgdockerpool`** to the name of your volume group. Save the **`all.yml`** file.
4. Using a text editor, open the `standby_cluster` file.
5. Uncomment and set the **`vgdockerpool`** to the name of your volume group. Save the **`standby_cluster`** file.

Example **before** the edit:

```
#bpdockerdevs: /dev/xvdb
#vgdockerpool: blueplanet
```

Example **after** the edit with `vgdockerpool` set to `my_vgname`.

```
#bpdockerdevs: /dev/xvdb
vgdockerpool: my_vgname
```

# Configuring a time source

BPUAA hosts can use a local or remote time source. For example:

- In environments where an enterprise NTP source is available, you can configure the BPUAA hosts as NTP clients of the enterprise NTP host.
- If BPUAA hosts have internet access, you can use public NTP servers as the BPUAA timing source.
- If no enterprise NTP host is available and BPUAA hosts do not have internet access, you can configure one of the BPUAA VMs to act as an NTP server. See your operating system documentation for more information.



Configure NTP in accordance with your site timeserver infrastructure. The Blue Planet installer can apply a simple configuration with one, three, or four timeservers. If NTP is already configured on BPUAA host, skip this procedure.

By default, the BPUAA installer sets up four NTP servers:

```
ntp_servers_default:  
  
- 0.rhel.pool.ntp.org  
- 1.rhel.pool.ntp.org  
- 2.rhel.pool.ntp.org  
- 3.rhel.pool.ntp.org
```

While you can specify your own NTP servers, or use fewer servers, Ciena recommends that you always have a minimum of three—and preferably four—timing servers for optimal BPUAA timing synchronization. The number of upstream servers, in order from most to least preferred, is listed below.

- 4—Allows for one or more servers to be a "false ticker" and for one server to be unreachable.
- 3—The minimum number required to allow ntpd to detect if one is a false ticker.
- 2—Are not allowed and will be blocked. With two NTP servers, you cannot determine which timing source is better because no reference exists to compare them to.
- 1—Provides no debate as to which server is correct, but also provides no redundancy.



Disable all other timing synchronization methods including, but not limited to, VMware Tools periodic time synchronization.



Following installation, you can use the bp2-site check-platform or bp2-site check-clockdrift commands to check BPUAA timing synchronization. For more information, see the *Blue Planet BPUAA User Guide*.

Complete this procedure to configure the Network Time Protocol (NTP) server(s) to serve as the timing source for BPUAA hosts. This is a mandatory procedure.

All BPUAA hosts must be synchronized to an accurate timing source. If you want to use a local time source or custom remote time sources (different than the default ones provided), then perform this procedure.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of active site as the bpadmin user.

### **To configure a time source**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. To use a local time source, uncomment `ntp_server_type` and change its value to local and save the `all.yml` file. The default `ntp_server_type` is remote. If you do not want to use a local time source, then skip this step and go to step 7.
4. Using a text editor, open the `standby_cluster` file.
5. To use a local time source, uncomment `ntp_server_type` and change its value to local and save the `standby_cluster` file. The default `ntp_server_type` is remote.

Here is an NTP section **before** the edit for the local time source.

```
## NTP
# There are 2 options 'remote' (default) and 'local'. The default configuration
# (remote) will set up NTP to connect
# to a set of remote, Operating System specific, servers. If local is specified,
# host0 will be used as the ntp clock
# reference for all nodes in the cluster. This is controlled via the
# 'ntp_server_type' outlined below.
#
ntp_server_type: remote
#
```



Here is an NTP section **after** the edit for the local time source.

```
## NTP
# There are 2 options 'remote' (default) and 'local'. The default configuration
# (remote) will set up NTP to connect
# to a set of remote, Operating System specific, servers. If local is specified,
# host0 will be used as the ntp clock
# reference for all nodes in the cluster. This is controlled via the
# 'ntp_server_type' outlined below.
#
ntp_server_type: local
#
```

6. If you are working with only local time source, go to step 10. If not, go to step 7.
7. To use custom remote time sources, uncomment and edit the **ntp\_servers\_custom** list to include the NTP server URLs or IP addresses that you want used as the BPUAA host timing source in active site. Save the **all.yml** file.
8. Using a text editor, open the **standby\_cluster** file.
9. To use custom remote time sources, uncomment and edit the **ntp\_servers\_custom** list to include the NTP server URLs or IP addresses that you want used as the BPUAA host timing source in standby site. Save the **standby\_cluster** file.



For all AWS and Azure servers, make sure that the IPs are custom defined by the admin and not using the default IPs.

Example **before** the edit for the custom remote time sources. The example focuses on the section to be edited.

```
# In the 'remote' case, you can also override the set of remote servers by
# uncommenting and setting the
# 'ntp_servers_custom' variable and configuring 1,3 or 4 NTP servers to connect
# to. To do so, uncomment
# the 'ntp_servers_custom' variable and uncomment and configure the appropriate
# number of hosts. e.g. change
# '<host a>' (and optionally host b, host c and host d) to the IP address or
# hostname of a valid NTP server.
#ntp_servers_custom:
# - <host a>
# - <host b>
# - <host c>
# - <host d>
```

Example **after** the edit using hostnames. In this example, the first NTP server to be contacted will be the one with the fully qualified domain name of 0.mycustomer.ntp.com:

```
# In the 'remote' case, you can also override the set of remote servers by
uncommenting and setting the
# 'ntp_servers_custom' variable and configuring 1,3 or 4 NTP servers to connect
to. To do so, uncomment
# the 'ntp_servers_custom' variable and uncomment and configure the appropriate
number of hosts. e.g. change
# '<host a>' (and optionally host b, host c and host d) to the IP address or
hostname of a valid NTP server.
ntp_servers_custom:
- 0.mycustomer.ntp.com
- 1.mycustomer.ntp.com
- 2.mycustomer.ntp.com
- 3.mycustomer.ntp.com
```

Example **after** the edit using IP addresses. In this example the first NTP server to be contacted will be the one with an IP address of 10.128.8.89:

```
# In the 'remote' case, you can also override the set of remote servers by
uncommenting and setting the
# 'ntp_servers_custom' variable and configuring 1,3 or 4 NTP servers to connect
to. To do so, uncomment
# the 'ntp_servers_custom' variable and uncomment and configure the appropriate
number of hosts. e.g. change
# '<host a>' (and optionally host b, host c and host d) to the IP address or
hostname of a valid NTP server.
ntp_servers_custom:
- 10.128.8.89
- 10.128.8.90
- 10.128.8.91
- 10.128.8.92
```

10. By default, the **ntp\_server\_options** entry default is `iburst`. For details about the **ntp\_server\_options**, see <https://linux.die.net/man/5/ntp.conf>. If you want to change the default value, uncomment **ntp\_server\_options** and edit its value in both `all.yml` file for active site and **standby\_cluster** file for standby site and save the files.

## Configuring geographical redundancy

This section describes the configuration of geographical redundancy functions which are given below. These parameters need to be configured in **all.yml** file for active site and **standby\_cluster** file for standby site.

1. `geored_site_state` - It can be in `ACTIVE` or `STANDBY` state.
2. `geored_site_id` – It identifies a site from a geographical context. You can use the variables such as `Toronto`, `DataCenter_1`, `Zone-East`. You can use letters, numbers, underscores and dashes and must

---

be at least 3 characters in length to define it.



You must have GR SiteId and SiteState, before creating the geored\_site\_id. geored\_site\_id uniquely identifies a site from a GR context. This variable should be set to something meaningful for your deployment, for example, Toronto, DataCenter\_1, Zone-East. Application deployments will not be fully functional until the GR SiteId and SiteState are configured. Valid characters for geored\_site\_id are letters, numbers, underscores and dashes and must be at least 3 characters in length. For example, geored\_site\_id: SiteA.

3. **geored\_local\_site\_ip**- It is used with the geored\_site\_id and geored\_site\_state to provision the local site from a geographical point of view.



The specification of this variable is optional and if not set will default to site\_ip defined in the host's file. This IP address is the same as the site\_ip and will not need to be overridden. The IP is not functionally significant (no GR operations depend on it).

4. **geo\_nagios\_checks** – It is used to verify nagios checks for GeoRed installation. Set geo\_nagios\_checks to false in the `all.yml` and `standby_cluster` files.

## Requirements

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of active site as the bpadmin user.

## Steps:

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. Edit **geored\_site\_id**, **geored\_site\_state**, **geored\_local\_site\_ip** and **geo\_nagios\_checks** in `all.yml` file and save it. **geored\_site\_state** is always set to ACTIVE in `all.yml` file.
4. Using a text editor, open the `standby_cluster` file.
5. Edit **geored\_site\_id**, **geored\_site\_state**, **geored\_local\_site\_ip** and **geo\_nagios\_checks** in `standby_cluster` file and save it. **geored\_site\_state** is always set to STANDBY in `standby_cluster` file.

# Modifying system logging path



This is an optional procedure

By default, the path to the system logging (syslog) file for the Blue Planet UAA application is `/var/log/ciena/blueplanet.log`. If you want to modify this path, perform the following procedure to keep current release logs separate.

To modify the default system logging path:

1. Log in to host 0 of site A (Active site) as bpadmin.
2. Navigate to directory `/home/bpadmin/bpi/playbooks/group_vars`.
3. Using a text editor open the `all.yml` file.
4. Uncomment and then edit the `bp_log_file` and `bp_log_dir` parameters.

Here is an example before the edit:

```
##Logging
#BluePlanet apps log file location
#'/var/log/syslog' is an invalid choice for RedHat/Oracle Linux/CentOS systems
#'/var/log/messages' is an invalid choice for Ubuntu systems
#bp_log_dir: /var/log/ciena
#bp_log_file: "{{ bp_log_dir }}/blueplanet.log"
```

Here is an example after the edit:

```
##Logging
#BluePlanet apps log file location
#'/var/log/syslog' is an invalid choice for RedHat/Oracle Linux/CentOS systems
#'/var/log/messages' is an invalid choice for Ubuntu systems
bp_log_dir: /opt/CustomLog/Pune/ciena
bp_log_file: "{{ bp_log_dir }}/bp_syslog.log"
```

5. Save the `all.yml` file and exit the text editor.
6. Using a text editor, open the `standby_cluster` file.
7. Uncomment and then edit the `bp_log_file` and `bp_log_dir` parameters as shown in Step 4.
8. Save the `standby_cluster` file.

# Configuring the Blue Planet email service

BPUAA requires that you configure a Simple Mail Transfer Protocol (SMTP) server so BPUAA can send system email to users. Emails are used for alarm notifications and forgotten password assistance.



If password expirations are enabled and the SMTP server is not configured, users will not be able to log in after their password expires. Ciena recommends if you cannot complete the configuration now, ensure you do it within 60 days to avoid causing users to be locked out with no way to reset their passwords. For information on configuring password notifications see the *Blue Planet BPUAA User Guide*.

Complete the following procedure to configure Blue Planet email service. This is a mandatory procedure.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of active site as the bpadmin user.
- Understand the SMTP server requirements at your site.

## To configure the Blue Planet email service

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **all.yml** file and edit the SMTP parameters mentioned in table SMTP parameters. Save the **all.yml** file.
3. Using a text editor, open the **standby\_cluster** file and edit the SMTP parameters mentioned in table SMTP parameters. Save the **standby\_cluster** file.

Table 11. SMTP parameters

PARAMETER	DESCRIPTION
smtp_username	The SMTP server account username used for sending emails.
smtp_password	The SMTP server account password.
smtp_staticPath	The staticPath value must be <code>/bp2/src/static</code> . Do not change this value.
smtp_authen	The SMTP server authentication. Set the value to true.

PARAMETER	DESCRIPTION
smtp_transport	The SMTP server transport security. Set the value to true or false, as applicable.
smtp_mail_server	The SMTP server fully qualified domain name (FQDN), such as smtp.gmail.com or, if a dedicated SMTP server, an FQDN that you own.
smtp_mailer_name	Must be set to Blue Planet Mailer. Do not change this value.
smtp_port	The SMTP server port number. Depending on the server, this port can be 25, 465, or 587.
smtp_email	The SMTP server email account from which reset password emails will be sent. Some SMTP servers, such as Gmail, allow you to use an alias that is not set on the server. For example, the account could be "bphostmonitor@abccompany.com", but the value could be "api-crinoid@ciena.com". Of course, you can enter the true value, "bphostmonitor@abccompany.com". The Amazon Web Services (AWS) SMTP server restricts the entry to the correct value.

Example before the edit:

```
# SMTP configuration details for 'Forgot Password' feature
smtp_username: USERNAME
smtp_password: PASSWORD
smtp_staticPath: /bp2/src/static
smtp_authen: SMTP_AUTHENTICATION
smtp_transport: SMTP_TRANSPORTSECURITY
smtp_mail_server: MAILSERVER.COM
smtp_mailer_name: MAILER_NAME
smtp_port: SMTP_PORT
smtp_email: MAILER@EMAIL.COM
```

Example after the edit:

```
# SMTP configuration details for 'Forgot Password' feature
smtp_username: GmailUser
smtp_password: AnyPassword
smtp_staticPath: /bp2/src/static
smtp_authen: true
smtp_transport: true
smtp_mail_server: smtp.gmail.com
smtp_mailer_name: Blue Planet Mailer
smtp_port: 587
smtp_email: api-crinoid@AnyCompany.com
```

---

# Modifying the iLAN NET interface

BPUAA uses the address 172.16.0.0/16/24 for its internal LAN (iLAN).

Complete this procedure if:

- Your network uses 172.16.0.0/16/24, in which case, a conflict with the BPUAA iLAN will occur, or,
- You are implementing georedundancy. Georedundancy requires different iLAN addresses for the active and standby sites.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the /home/bpadmin/bpi/playbooks/group\_vars directory of host 0 of active site as the bpadmin user.
- Have a new address for the iLAN.

## ***To modify the iLAN interface***

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to **/home/bpadmin/bpi/playbooks/group\_vars** directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment the ilannet option, then enter the IP network address you want BPUAA to use, for example, 172.19.0.0/16/24. Save the **all.yml** file.
4. Using a text editor, open the **standby\_cluster** file.
5. Uncomment the ilannet option, then enter the IP network address you want BPUAA to use, for example, 172.29.0.0/16/24. Save the **standby\_cluster** file.

Example **before** the edit:

```
#####  
# install #  
#####  
# The ilannet to use on hosts  
# ilannet: 172.16.0.0/16/24
```

Example **after** the edit:

```
#####  
# install #  
#####  
# The ilannet to use on hosts  
ilannet: 172.19.0.0/16/24
```



If you are installing georedundancy, the active and standby sites must have different iLAN addresses. The active site can use the default (or user-assigned) address. The standby site must be on a different network.

For example: Active → ilannet:172.19.0.0/16/24 (default) and Standby → ilannet: 172.29.0.0/16/24. Do not modify the /24 subnet value.

## Modifying the default BPUAA interface

By default, BPUAA uses the first network interface, eth0, for Blue Planet activities. Complete the following steps if you want to set a new default interface. Otherwise, you can skip this procedure and continue with the [Specifying the external license server](#) procedure.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of active site as the bpadmin user.



To display a list of interfaces, use the "ip a" command.

### **To modify the default BPUAA interface**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment the `bp_interface` option and replace eth0 with the interface you want used for example eth3. Save the **all.yml** file.
4. Using a text editor, open the **standby\_cluster** file.
5. Uncomment the `bp_interface` option and replace eth0 with the interface you want used for example eth3. Save the **standby\_cluster** file.



---

Example **before** the edit:

```
# specify the Blue Planet Interface
# if not defined, the ansible default interface
# will be used, which is typically your first interface
#bp_interface: eth0
```

Example **after** the edit:

```
# specify the Blue Planet Interface
# if not defined, the ansible default interface
# will be used, which is typically your first interface
bp_interface: eth3
```

6. Save the file.

## Specifying the external license server

Use this procedure to set up the external license server IP address in cluster and standby\_cluster files.

### Requirements

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of active site as the bpadmin user.

### Steps

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment the **license\_server** parameter and replace a.b.c.d with external license server IP.
4. Uncomment the **license\_server\_backup** parameter and replace a.b.c.d with external backup license server IP. Save the **all.yml** file.
5. Using a text editor, open the **standby\_cluster** file.
6. Uncomment the **license\_server** parameter and replace a.b.c.d with external license server IP.

7. Uncomment the **license\_server\_backup** parameter and replace a.b.c.d with external backup license server IP. Save the **standby\_cluster** file.

Example **before** the edit:

```
# License Server details for unbundling encrypted offline archives and runtime
requirements
#license_server: a.b.c.d
#license_server_backup: a.b.c.d
```

Example **after** the edit:

```
# License Server details for unbundling encrypted offline archives and runtime
requirements
license_server: 10.10.10.10
license_server_backup: 12.12.12.12
```

## Setting up users

Complete this procedure to manage keys of the bpadmin user and the root user, and to create the bpuser user (sudo restricted Docker install user) and manage its sudo permissions and keys. This is a mandatory procedure. The setup script skips this step if you have previously manually created the bpuser user. This script also creates the bpmaint user without sudo permission, which has read only access to other product folders. The bpmaint user has the write permission to edit the bpmaint home directory to fetch and store data. You can export this data from the host using scp.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Know the bpadmin user password.
- Can access the /home/bpadmin/bpi directory of host 0 of active site as the bpadmin user

### To set up users

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to **/home/bpadmin/bpi/** directory.
2. To start the setup users' script enter:

```
./bpi --setup-users
```

3. If prompted, enter the bpadmin user password.



For multi-host deployments, you must enter the bpadmin password for each host.

4. If you have not previously completed the procedure to manually create the bpuser user, then:
  - a. When prompted, enter the bpuser password. The same password is set on all hosts.
  - b. Re-enter the password for the bpuser user.

The script sets the bpadmin and bpuser authentication keys as well as several sudo privileges for the bpuser user. See the files in `/home/bpadmin/bpi/roles/setup-users/sudoers/templates` to see the settings.

5. If you have not previously completed the procedure to manually create the bpmaint user:
  - a. When prompted, enter the bpmaint password. The same password is set on all hosts.
  - b. Re-enter the password for the bpmaint user.

## Validating the hosts

This procedure verifies that the host hardware and software where you will install the BPUAA meet Ciena requirements. The validation is based upon requirements described in the [Server hardware and VM requirements](#) topic.

The validation phase checks the following areas and related requirements:

- Hardware (CPU, RAM, and SWAP)
- Operating system (type, architecture, version, system-level packages for bpi execution, and SELinux mode)
- Disk (mountpoints, size, and Docker volume group [if required])
- Network (ports and unique hostnames)

Before you begin this procedure, verify that you:

- Completed [Setting up users](#) procedure.
- Can access the `/home/bpadmin/bpi` directory of host 0 of active site as the bpadmin user.

### **To validate the hosts**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to /home/bpadmin/bpi/ directory.
2. Validate the system by executing command.

```
./bpi --validate <profile>
```

where

<profile>	is the validation profile.
-----------	----------------------------

3. If prompted, enter the bpadmin user password.



For multi-host deployments, you must enter the bpadmin password for each host.

The system displays various task-related outputs as the validation progresses. At the end of the validation process, the system displays a summary.

4. If elements display a Failed status, correct them, then repeat step 2 and 3 until all elements display a Passed status.
5. If all elements display a Passed status and "failed=0" at the end of the summary, continue with the next procedure .

## Configuring BPUAA hosts on active and standby sites

Complete this procedure to configure the BPUAA host(s) on active and standby sites for the BPUAA software installation from host 0 of active site.

Configuring the BPUAA hosts creates the following directories on active and standby sites. It also ensures they are owned by bpuser on both active and standby sites:

- /etc/bp2
- /etc/bp2/site
- /etc/bp2/solutionmanager

This procedure also performs minor configuration changes including updates to syslog, rsyslog, sshd,

---

and NTP to prepares the hosts for BPUAA installation on active and standby sites.

Before you begin this procedure, verify that you:

- Completed [Setting up users](#) procedure.
- Know the bpadmin user password.
- Can access the /home/bpadmin/bpi directory of host 0 of active site as the bpadmin user
- If you chose not to implement the Blue Planet NTP option in the [Configuring a time source](#) procedure and will use your network NTP for BPUAA host timing, add the playbook arguments shown in step 2c.

### **To configure the BPUAA hosts**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to /home/bpadmin/bpi/ directory.
2. Execute one of the following commands, depending on whether your installation is single-host or multi-host and your NTP timing preference.

#### **UAA without integrators on a single host machine:**

```
./bpi --site /opt/ciena/loads/23.08.64/lineup-uaa-single-rhel.yml
```

#### **UAA without integrators on multi-host:**

```
./bpi --site /opt/ciena/loads/23.08.64/lineup-uaa-multi-rhel.yml
```

3. If you are provisioning your own NTP timing, add the following playbook arguments:

```
./bpi --site /opt/ciena/loads/23.08.64/<lineup_file> --playbook-args='--skip-tags ntp'
```

If no failures occur, indicated by failed=0, continue with the next step. If failures occurred, contact Ciena Customer Support for guidance.

If all elements display a **Passed** status and "failed=0" at the end of the summary, continue with the next procedure.

---

# Installing Core Platform and Extended Platform Solution on active and standby sites

Complete this procedure to install core platform and platform solution on active and standby sites from host 0 of the active site.

Before you begin this procedure, verify that you:

- Completed [Configuring BPUAA hosts on active and standby sites](#) procedure.
- Know the bpadmin user password.
- Can access the `/home/bpadmin/bpi` directory of host 0 of active site as the bpadmin user

## ***To install BPUAA platform and solutions***

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/` directory.
2. Install the Core Platform and Platform Solution for BPUAA 23.08.64 on active and standby sites by entering (on a single line):

```
./bpi --install /opt/ciena/loads/23.08.64/<lineup file> --playbook-args='--skip  
-tags bp2-solution'
```

If all elements display a Passed status and "failed=0" at the end of the summary, continue with [Installing BPUAA and configure georedundancy on active and standby sites \(automatic procedure\)](#) .

# Installing BPUAA and configuring georedundancy on active and standby sites (automatic procedure)

Complete this procedure to install BPUAA solution on active and standby sites. This procedure also automatically sets up geographical redundant configuration between active and standby.

This procedure performs:

- Share the keys with standby site.
- Create an IP security tunnel between the active and standby sites.
- Install and deploy the BPUAA application solution & additional solutions on active and standby sites.
- Verify system health of active and standby sites.
- Configure geographical redundancy on active site.
- Configure geographical redundancy on standby site.

Before you begin this procedure, verify that you:

- Completed [Installing Core Platform and Platform Solution on active and standby sites](#) procedure.
- Know the bpadmin user password.
- Can access the /home/bpadmin/bpi directory of host 0 of active site as the bpadmin user.
- The lineup files are saved in the /opt/ciena/loads/23.08.64 directory on both the Active and standby clusters.
- The lineup and tar ball permissions are world READABLE on both the Active and standby clusters.

To install BPUAA and configure georedundancy:

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to **/home/bpadmin/bpi/** directory.
2. Start automatically geographical redundant configuration setup between active and standby sites by executing command (on single line):
  - a. For OS hardened servers:

```
./bpi --geo-keys <standby_siteIp> --playbook-args="--limit cluster"
```

```
./bpi --autoinstall-geo /opt/ciena/loads/23.08/<lineup file> --playbook  
-args='--skip-tags geowhitelist -e geo_user=admin -e geo_password=adminpw'
```

where <lineup file> refers to the one saved in the /opt/ciena/loads/23.08.64 directory.

This is the default password you use for the first time. If you forget to specify the password here, then you are asked for the password.

b. For non OS hardened servers:

```
./bpi --autoinstall-geo /opt/ciena/loads/23.08/<lineup file> --playbook  
-args='-e geo_user=admin -e geo_password=adminpw'
```

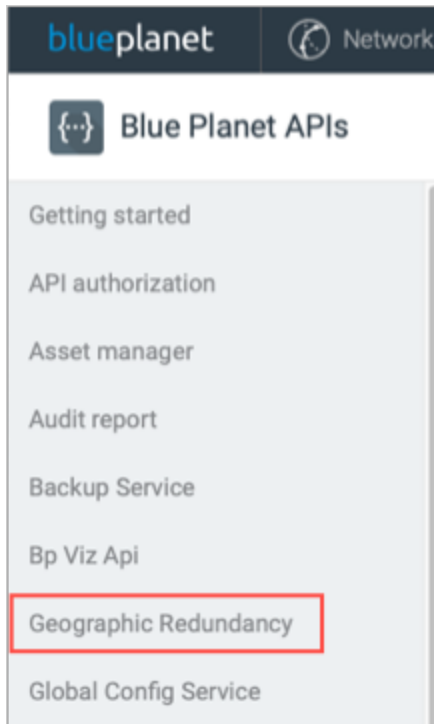
where <lineup file> refers to the one saved in the /opt/ciena/loads/23.08.64 directory. If all elements display a Passed status and "failed=0" at the end of the summary, continue with the next step. If failures occurred, contact Ciena Customer Support for guidance.

3. Execute below script to copy bpi directory to host 0 of standby site which enable standby site to keep its original bpi configuration for example hosts file and all.yml file.

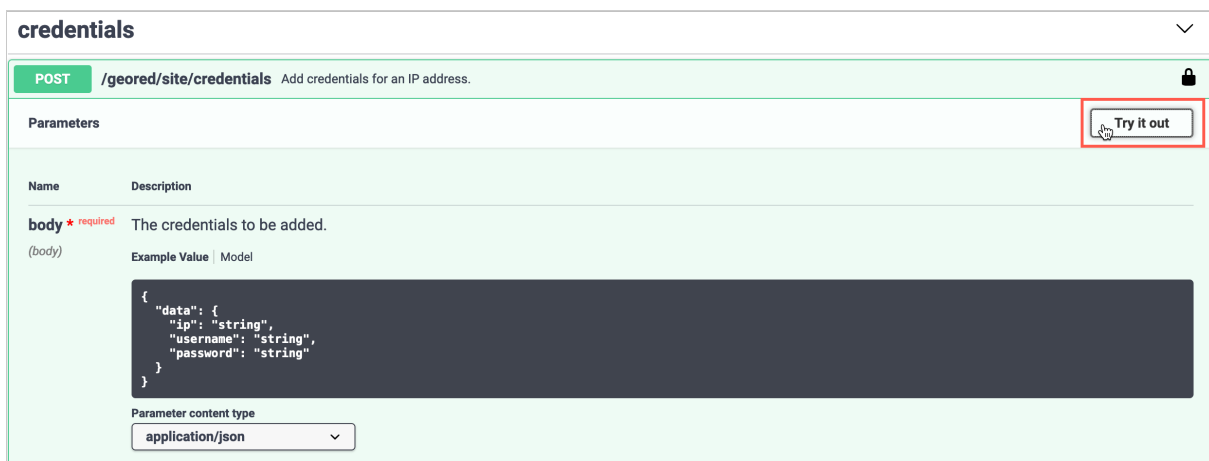
```
./setup-bpi-standby.sh
```

4. Check Nagios to make sure all services are running in the GREEN state on both active and standby sites.
5. On the active host UI, select **System > Platform > Swagger UI** and then click Geographic Redundancy from the left panel.





6. On the right pane, expand the POST `/geored/credentials` API and then click the Try it out button.




The JSON data in the API body section becomes editable.

**POST**
**/geored/site/credentials**
Add credentials for an IP address.

**Parameters**

Name	Description
<b>body</b> * required (body)	The credentials to be added. Edit Value   Model



```

{
  "data": {
    "ip": "string",
    "username": "string",
    "password": "string"
  }
}

```

7. Enter the following data for the active site:

where	
<ip>	Put the site IP of active site.
<username>	Put the username that used to login active site host to perform GR installation command.
<password>	Put the password of username that used to login active site host to perform GR installation command.

8. Click **Execute**.

Name	Description
<b>body</b> <span style="color: red;">★ required</span>	The credentials to be added.
(body)	<div> <div>Edit Value   Model</div> <div> <pre>{   "data": {     "ip": "&lt;active site IP&gt;",     "username": "user1",     "password": "userpw"   } }</pre> </div> <div> <div>Cancel</div> <div> Parameter content type  <div>application/json ▼</div> </div> </div> </div>
<div>Execute</div>	

9. Once the above step is executed successfully with response code 200, enter standby site data on the same REST API body field.

where	
<ip>	Put the site IP of standby site.
<username>	Put the username that used to login standby site host to perform GR installation command.
<password>	Put the password of username that used to login standby site host to perform GR installation command.

10. Click **Execute**.

```
{
  "data": {
    "ip": "<standby site IP>",
    "username": "user1",
    "password": "userpw"
  }
}
```

**Cancel**

Parameter content type

application/json ▼

**Execute**

Continue with the post-installation procedures.

---

# Post-installation procedures

After you have completed the installation of BPUAA, perform the following procedure.

# Changing the Sharding options after installing BPUAA

Warning: If this option is used, all the existing PM DB data will be deleted. To configure the required Sharding configuration, please follow the procedure to configure required sharding options without losing any PM data on page #45 prior to installation.

Starting UAA 22.02+, UAA-PM-DB (Clickhouse container) will by default have the following Sharding config,

1. Shard and 3 Replica in case of HA deployments
2. Shard and 1 Replica in case of Non-HA/Standalone deployments

Please follow the below steps to change the default Sharding config post BPUAA installation,

1. Create a new file overrides.json in /etc/bp2/uaa-pm-db/private/ in all the hosts individually and add the required Sharding option (available options mentioned below), using the below command,

```
echo '{ "sharding_option": "3S-2R" }' > /etc/bp2/uaa-pm-db/private/overrides.json
```

Using "3S-2R" as an example above. Please use the required option as per the deployment from one of the available options here ['1S-1R','1S-3R','3S-2R','5S-2R','5S-3R'].

Here "S" = Shard and "R" = Replica. The numbers preceding the letters indicate the corresponding count. Above example means 3 Shards and 2 Replicas for each Shard, so the deployment would need 6 UAA-PM-DB instances to have 3 Shards x 2 Replicas configured.

1. After doing the above step, User would need to re-deploy the UAA-PM-DB using the purge option (`--purge`) as mentioned below,

```
solution_redeploy artifactory.ciena.com.blueplanet.uaa_pm_storage:23.08.xx --purge -y
```

## Error scenario:

- User would need to scale out the UAA-PM-DB to match the instances count using the below command
- If the UAA-PM-DB instances count do not match after installation, UAA-PM-DB would not start and an error will be shown in Nagios with appropriate message.

- To fix this error, please follow the below steps,
  - {}User would need to scale out the UAA-PM-DB to match the instances count using the below command{}  

```
solution_app_scale artifactory.ciena.com.blueplanet.uaa_pm_storage:23.08.xy uaa-pm-db  
<total_number_of_instances>
```

### **Mandatory steps post the above changes**

#### **1. Restart UAA-PM-DB-SCHEDULER**

```
solution_app_restart artifactory.ciena.com.blueplanet.uaa_storage:23.08.xx uaa-  
pm-db-scheduler
```

#### **2. Run the following command to re-migrate the SA data from UAA-CORE-DB to UAA-PM-DB**

```
python3 /bp2/scripts/pg2ch.py
```

# Modifying ZooKeeper Configuration

Perform the following to modify the XMS and XMX configurations for the ZooKeeper database:

1. Log in to solman.

```
sudo su  
solman
```

2. From the command line, enter the following command to check Leader ZooKeeper instance.

```
api clusters zookeeper get
```

3. From the command line, enter the following command to update the ZooKeeper configuration.



Ensure that you run each command in a single line.

```
curl -X PUT -d ' [{"application":"zookeeper","instance":"-", "partition":"java", "name":"XMX", "value":"4096m"}] '  
http://<HAProxyIp>/gcs/api/v1/config  
  
curl -X PUT -d ' [{"application":"zookeeper","instance":"-", "partition":"java", "name":"XMS", "value":"2048m"}] '  
http://<HAProxyIp>/gcs/api/v1/config
```



# Changing the default passwords

After you install BPUAA, it is recommended that you change the default passwords of all the accounts such as, BP User, BP admin or Nagios admin. For more information, see the "Changing the nagios admin password" topic of the Blue Planet Security Guide.

# Enabling Kafka log messages for file import (Optional)

- Log in to host 0 (for multi host setup, repeat the steps in all hosts) as bpadmin. Do not use the site IP; use the IP address of host 0.
- Enter uaa-core container -

```
sudo solman  
enter_container uaa-core_23.08.xx_x
```

Example:

```
enter_container uaa-core_23.08.xx_x
```

- Edit the install.properties file –

```
vi /bp2/conf/install.properties
```

- Change the *file\_import\_staus\_kafka\_message* value from false to true
- Restart the container

```
solution_app_restart artifactory.ciena.com.blueplanet.uaa:ha-23.08.xx
```

Example:

```
solution_app_restart artifactory.ciena.com.blueplanet.uaa:ha-23.08.xx
```

---

# Clean up BPUAA installation

This section discusses the procedure to clean up the UAA installation in case you see errors during installation and you want to install BPUAA afresh.

The clean up process works only if the user have reached the [Configuring the BPUAA hosts](#) section of installation.

1. Log in as bpadmin user.
2. Navigate to the `/home/bpadmin/bpi/` directory.
3. From the command line, enter the following to clean-up bpi:

```
./bpi --uninstall && ./bpi --utility playbooks/docker-clean.yml
```

# Installing RDC (Light Weight Data Collector)

Light weight data collector or RDC (LWDC) supports management of devices with different IP addresses and poll from other sites such as, government agencies, where you can deploy a remote collector.

RDC (LWDC) can also manage companies with the same instance, where the RDC (LWDC) need to be in the other network.

RDC (LWDC) requires to be setup on a different host. For information on sizing and characterization recommendations, see *BP Engineering Guide*.

## Installation pre-requisites

- The server meets the requirements for RDC (LWDC) as provided in the BPUAA server sizing document. Please refer the document for details.
- User is proficient using UNIX commands.
- See the [Downloading the installation files](#) section to download LINUX\_2023\_39\_0, BPI\_23.08.64-x, BPUAA\_LWDC\_MR2\_23\_08 from my.ciena.com portal.
- Since the installation of LWDC is done on a separate server, you must setup the BP environment. For more information, see [Host setup and BPUAA installation \(non-GR deployments\)](#).
  - Use LWDC tar file instead of the BPUAA tar file on page 41 step 8 to untar the RDC (LWDC) tar file.

```
Example:  
tar -xf bp_uaa-remote-lwdc_23.08.00-72.tar
```

## Installing RDC (LWDC)

The following table shows different options to install RDC (LWDC) and the corresponding lineup files available.

BPUAA SOLUTION	LINEUP FILE NAME (SINGLE HOST)	LINEUP FILE NAME (MULTI HOST)
Light Weight Data Collector	lineup-uaa-remote-lwdc-single-rhel.yml	lineup-uaa-remote-lwdc-multi-rhel.yml

- lineup\_single\_LWDC\_rhel.yml: This lineup file is meant to install LWDC on a single host machine.
- lineup\_multi\_LWDC\_rhel.yml: This lineup file is meant to install LWDC on a multi host machine.

## Installing and Configuring RDC (LWDC)

To install and configure the RDC (LWDC) host for the RDC (LWDC) 23.08.64 software installation:

1. Log in to the host as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. From the command line, enter the following command to install the bpi setup users.

```
./bpi --setup-users
```

3. From the command line, enter the following command to install required solution (change the lineup file as per the requirement above):

```
./bpi --site /opt/ciena/loads/23.08.64/<lineup_file_name>
```

Output, similar to the following, indicates whether the configuration succeeded:

```
PLAY RECAP
*****
<host>                                : ok=102    changed=47    unreachable=0    failed=0
```



Follow the BPUAA Installation Guide to install remote collector and make sure to follow the below steps before performing `./bpi --install <lineup.yml>`.

---

**Follow the below steps if the version is greater than or equal to 23.08**



Site should be created in UAA UI sites page before configuring the site key in remote data collector site-to-site.yml

- Follow the BPUAA Installation Guide to install remote collector based on version and make sure to follow the below steps before performing `./bpi --install <lineup.yml>`.
- Refer [Host setup and BPUAA installation \(GR deployment - automatic\)](#) for GR installation. The site-to-site.yml should be copied to standby hosts also.

1. Navigate to the path in host `/etc/bp2/`
2. Create the directories with name `uaa-sbc` and `remote-collector` using below command

```
mkdir -p uaa-sbc/remote-collector
```

3. Navigate to `/etc/bp2/uaa-sbc/remote-collector` and create a file with name `site-to-site.yml`.
4. Add the content inside the file `site-to-site.yml` (Make sure every host should have this file and update the file with required values as mentioned).

If `site-to-site.yml` creating from `bpadmin` user its mandatory to do

```
sudo vi site-to-site.yml
```

5. Under the property `uaa_sbc_hosts` provide the vm ips where the UAA is installed and sbc is running.
6. Provide the customised site key which is created in UAA UI before installing the remote collector.

If the site key is **site1** in yml file, then before running the install command, create **site1** in UAA UI sites page and make sure the **site1** is also created in NIFI UI.



Make sure there are **NO** indentations while editing the yml file (i.e., only # should be removed and NO spaces to be removed between "#" and "-" or "-" and IP while adding UAA IPs)

```

---
main_site:
# Main site active and standby host ip/ips where sbc is running if the main
site is a gr setup.
# If not gr setup please provide main site host ip/ips under active_hosts.
# Configure gr user and password under api_creds if the main site is a gr set
up. (Note: default values will be admin/adminpw)
uaa_sbc_hosts:
#active_hosts:
# - ip1
# - ip2
# - ip3
#standby_hosts:
# - ip1
# - ip2
# - ip3
#Api credentials is used to check the geo-red state of a main site
#api_creds:
# user: ""
# password: ""
remote_site:
# key should not be empty.
# key should be same as the site key created in UAA ui sites page.
# eg: site_key: "site1"
site_key: ""

```



No need to execute any script inside container.

7. To install remote collector use this lineup based on respective version.

From the command line, enter the following command to install the lineup file.

```
./bpi --install /opt/ciena/loads/23.08/<lineup_file_name>
```



No need to execute any script inside container.

8. Execute the procedure described in the [Installing Core Platform and Extended Platform Solution on active and standby sites](#) section. *Make sure to use the RDC lineup file while following the procedure described in the link.*
9. Execute the procedure described in the [Installing BPUAA and configuring georedundancy on active and standby sites \(automatic procedure\)](#) section. *Make sure to use the RDC lineup file while following the procedure described in the link.*

---

## Logstash configurations in Remote Data Collector

Send the log messages from Remote Data Collector and follow the below steps:

1. From RDC host navigate to the path

```
"cd /opt/ciena/bp2/uaa-logstash_23.08.12_0/data"
```

2. Edit the file

```
"vi logstash-conf.conf"
```

3. At the EOF siteKey should be edited with respect to the siteKey configured in "site-to-site.yml"

The editable line in "logstash-conf.conf" looks like below

```
"{ format => "{ \"messageType\": \"LOG_EVENT\", \"message\": \"%{message}\",  
  \"ipaddress\": \"%{host}\", \"siteKey\": \"Default\" }" }
```

Default should be replaced with "site\_key" value in "site-to-site.yml"



---

# Configuring BP firewall

The `bp2hosttools` package provides a `systemd` service called `bpfirewall` to restrict access to host ports. The `bpfirewall` service was designed to operate without interfering with the `iptables` rules needed by `docker` and Blue Planet applications. Other services that manage `iptables`, specifically `firewalld` and `iptables`. Services are incompatible with the correct operation of a site and must not be used.



This document makes references to BP configuration files under the `/etc/bp2` directory. If a site is configured with an alternate base config directory, the location of the referenced config file will need to be updated accordingly.

## Overview

When started, `bpfirewall` sets the default policy on the `INPUT`, `FORWARD` and `OUTPUT` chain to "DROP" and adds `ACCEPT` rules for ports needed for operation of the site and additional `ACCEPT` rules as per the `/etc/bp2/site/bpfirewall` config file.

When stopped, `bpfirewall` sets the default policy on the `INPUT`, `FORWARD` and `OUTPUT` chain to "ACCEPT" and removes `ACCEPT` rules that it had added when last started.

## Configuring Custom Rules

The `bpfirewall` service can be configured to add additional rules to the `INPUT`, `FORWARD` and `OUTPUT` chains to allow access for non-standard, customer-specific purposes. All custom rules must be added to the `/etc/bp2/site/bpfirewall` configuration file.

## Configuring an Open TCP and UDP port

Example `/etc/bp2/site/bpfirewall` content for opening `tcp` port 5556 and `udp` port 8001 on `INPUT` chain and allow any packet leaving via output interface `lo` on `OUTPUT` chain.

```
INPUT -p tcp --dport 5556 -j ACCEPT # Open access to tcp port 5556
-p udp --dport 8001 -j ACCEPT # Open access to udp port 8001, INPUT could be
omitted by default
OUTPUT -o lo -j ACCEPT
```

---

## Activating bpfirewall Configuration Changes

After editing the bpfirewall configuration the following two steps are required in order to activate any changes.

1. The /etc/bp2/site/bpfirewall config file must be distributed to all of the hosts on the site using the following command:

```
sudo bp2-site sync-site-config
```

2. The bp2firewall must be restarted on all hosts in the site using the following command:

```
sudo bpssh systemctl restart bpfirewall
```



Custom rules should not be used to provide port forwarding to a bp app. All BP apps should utilize the natd service to enable any needed port access and redirection.

## Life-cycle Management of the bpfirewall Service

The bpfirewall service is implemented as a systemd service. Standard systemd commands should be used to manage the bpfirewall service.

### Starting the bpfirewall service

```
sudo bpssh systemctl start bpfirewall.service
```

### Stopping the bpfirewall service

```
sudo bpssh systemctl stop bpfirewall.service
```

### Configuring bpfirewall to be Enabled on Start Up/Reboot

```
sudo bpssh systemctl enable bpfirewall.service
```

### Configuring bpfirewall to be Disabled on Start Up/Reboot

```
sudo bpssh systemctl disable bpfirewall.service
```

**Getting Status** Some status information about the service can be obtained from systemd:

```
bpssh systemctl status bpfirewall.service
```

Instantaneous status information must be queried by root directly from the init script (since systemd only reports its own internal statistics plus messages generated by the service at start/stop):

```
sudo /usr/local/bin/bpssh bpfirewall status
```

## Examples

Configuring an allow list for access to haproxy. To allow access to haproxy from IP addresses 1.1.1.1 and 2.2.2.2 only:

```
FORWARD -s 1.1.1.1 -p tcp --dport 443 -j ACCEPT  
FORWARD -s 2.2.2.2 -p tcp --dport 443 -j ACCEPT  
FORWARD -p tcp --dport 443 -j DROP  
FORWARD -j ACCEPT
```

---

# Appendices

# Host setup and BPUAA installation (GR deployment manual)

Complete the same procedures for either single or multi-geographical redundant configurations, with the only difference being the lineup file.

These files contain a customer-specific list of BPUAA solutions to install. The lineup files apply to all supported operating systems: RHEL, Oracle linux, and CentOS.



Perform all the pre-requisites steps such as, *Installing the LinuxIntel system bundle* and *Transferring the installation files to the host* on both active and standby servers if the geo-redundancy mode of deployment is manual.

This section uses the following designation:

- Site A (active)
- Site B (standby)

The following table provides an overview to the installation procedures, where you perform them, and key notes.

Table 12. BPUAA installation procedures

PROCEDURE	LOCATION	NOTES
<b>Initial host setup</b>		
<a href="#">Updating the hosts file</a>	/home/bpadmin/bpi/hosts	Required
<b>Installation variables</b> These procedures require edits to the all.yml file of the active site and to the standby_cluster file of the standby site. These files are located in the /home/bpadmin/bpi/playbooks/group_vars directory of Host 0 of the active site. Most of the edits are as required by your specific network environment and BPUAA installation. You might not need complete many of them unless you want to change the default values.		
<a href="#">Modifying the volume group name</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed

PROCEDURE	LOCATION	NOTES
<a href="#">Configuring a time source</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	Required
<a href="#">Configuring the Blue Planet email service</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	Required
<a href="#">Modifying the ILAN NET interface</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<a href="#">Modifying the default BPUAA interface</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<a href="#">Specifying the external license server</a>	home/bpadmin/bpi/playbooks/group_vars/all.yml	If needed
<b>Installation preparation</b>		
<a href="#">Setting up users</a>	CLI	Required; creates bpuser
<a href="#">Validating the hosts</a>	/home/bpadmin/bpi/	--validate command
<b>Installation</b>		
<a href="#">Configuring BPUAA hosts on active and standby sites</a>	/home/bpadmin/bpi/	Required; execute the lineup file for your situation
<a href="#">Installing Core Platform and Extended Platform Solution on active and standby sites</a>	/opt/ciena/loads/23.08.64	Required; execute the lineup file for your situation

PROCEDURE	LOCATION	NOTES
<a href="#">Installing BPUAA on geographical redundant sites (manualprocedure)</a>	/opt/ciena/loads/23.08.64	Required; execute the lineup file for your situation

# Updating the hosts file

This procedure adds the host(s) of active and standby sites where you want to install the BPUAA to the hosts file. The Blue Planet installer uses the host file entries to perform the BPUAA installation on both active and standby sites. This is required for all installations performed from Host 0 of the active (Site A) site and Host 0 of the standby(Site B) site

Complete this procedure to add the host(s) where you want to install BPUAA to the hosts file. This is a mandatory procedure.



You must perform all the steps given in this procedure on Host 0 of Site A(Active) and Host 0 of SiteB(Standby)

## To update the hosts file

1. Log in to Host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. Open the hosts file with a text editor.
3. If your installation is single host, complete the following steps. If your installation is multi host deployment, proceed to step 4
  - a. Uncomment and set the `host0` entry to the IP address for that host. Use the host IP address IP4 (not IPv6 or the hostname).
  - b. Uncomment and set the `site IP` variable to the IP address and subnet mask of host0.
  - c. Uncomment the `site_name` entry and replace `mysite` with your site name. Valid characters are letters, numbers, and dashes.

`site_name` allows you to associate a meaningful name with the cluster. It is not required for normal BPUAA operations, apart from certain Blue Planet microservices, such as Message Relay. Allowed characters are the same as hostnames, that is, a-z, A-Z, 0-9, and dashes.

Example of hosts file "before"the edit

```
[cluster]
#host0 ansible_host=a.b.c.d controller=True

[cluster:vars]
#site_ip=a.b.c.d/42

#site_name=mysite
```

Example of hosts file "after" the edit are made for an installation where the subnet mask is 22



(255.255.252.0):

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True

[cluster:vars]
site_ip=10.186.0.1/22
site_name=BPSite1
```

4. If your installation is multiple hosts, complete the following steps.

- a. Uncomment and set one host entry (for each host) to the IP address for that host. Use the host IP address of each host IP4 (not IPv6 or the hostname).
- b. Set `controller=true` (the default) for up to three hosts, then `controller=False` for remaining hosts.



All cluster hosts must be on the same subnet.

- c. Uncomment and set the `site IP` variable to an IP address and subnet mask for the cluster. The site IP must be an IP address on the same subnet as the host IP addresses.
- d. Uncomment the `site_name` entry and replace `mysite` with your site name. Valid characters are letters, numbers, and dashes.

`site_name` allows you to associate a meaningful name to the cluster. It is not required for normal BPUAA operations, apart from certain Blue Planet microservices, such as Message Relay. Allowed characters are the same as hostnames, that is, a-z, A-Z, 0-9, and dashes.

The following shows a sample active hosts file after the multi-host edits are made for an installation where the subnet mask is 22 (255.255.252.0):

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True

[cluster:vars]
site_ip=10.186.0.4/22

site_name=BPSite1
```

5. Save the hosts file.

# Modifying the volume group name

Ciena recommends using unique names that can be recognized and avoid name conflicts across multiple virtual groups.

Complete the following steps to modify the volume group name where the unallocated physical extents space is left free for BPUAA to create and configure the Docker thin pool.

Before you begin, verify that you:

- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of Host 0 of Site A (active site) as the bpadmin user.
- Know the name of the volume group where the unallocated physical extents (PE) space is available for BPUAA to create and configure the Docker thin pool.



You can use the Linux `vgdisplay` command to display volume group information.

## **To modify the volume group name**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP; use the IP address of the Host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment and set the **vgdockerpool** to the name of your volume group. Save the **all.yml** file.

Example **before** the edit:

```
#bpdockerdevs: /dev/xvdb
#vgdockerpool: blueplanet
```

Example **after** the edit with vgdockerpool set to my\_vgname.

```
#bpdockerdevs: /dev/xvdb
vgdockerpool: my_vgname
```

4. Repeat steps 1 to 3 on **Host 0 of Site B(standby site)**.

# Configuring a time source

BPUAA hosts can use a local or remote time source. For example:

- In environments where an enterprise NTP source is available, you can configure the BPUAA hosts as NTP clients of the enterprise NTP host.
- If BPUAA hosts have internet access, you can use public NTP servers as the BPUAA timing source.
- If no enterprise NTP host is available and BPUAA hosts do not have internet access, you can configure one of the BPUAA VMs to act as an NTP server. See your operating system documentation for more information.



Configure NTP in accordance with your site timeserver infrastructure. The Blue Planet installer can apply a simple configuration with one, three, or four timeservers. If NTP is already configured on BPUAA host, skip this procedure.

By default, the BPUAA installer sets up four NTP servers:

```
ntp_servers_default:  
  
- 0.rhel.pool.ntp.org  
- 1.rhel.pool.ntp.org  
- 2.rhel.pool.ntp.org  
- 3.rhel.pool.ntp.org
```

While you can specify your own NTP servers, or use fewer servers, Ciena recommends that you always have a minimum of three—and preferably four—timing servers for optimal BPUAA timing synchronization. The number of upstream servers, in order from most to least preferred, is listed below.

- 4—Allows for one or more servers to be a "false ticker" and for one server to be unreachable.
- 3—The minimum number required to allow ntpd to detect if one is a false ticker.
- 2—Are not allowed and will be blocked. With two NTP servers, you cannot determine which timing source is better because no reference exists to compare them to.
- 1—Provides no debate as to which server is correct, but also provides no redundancy.



Disable all other timing synchronization methods including, but not limited to, VMware Tools periodic time synchronization.



Following installation, you can use the `bp2-site check-platform` or `bp2-site check-clockdrift` commands to check BPUAA timing synchronization. For more information, see the *Blue Planet BPUAA User Guide*.

Complete this procedure to configure the Network Time Protocol (NTP) server(s) to serve as the timing source for BPUAA hosts. This is a mandatory procedure.

All BPUAA hosts must be synchronized to an accurate timing source. If you want to use a local time source or custom remote time sources (different than the default ones provided), then perform this procedure.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of Host 0 of active site as the bpadmin user.

### To configure a time source

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. To use a local time source, uncomment `ntp_server_type` and change its value to local and save the `all.yml` file. The default `ntp_server_type` is remote. If you do not want to use a local time source, then skip this step and go to step 7.

Here is an NTP section **before** the edit for the local time source.

```
## NTP
# There are 2 options 'remote' (default) and 'local'. The default configuration
# (remote) will set up NTP to connect
# to a set of remote, Operating System specific, servers. If local is specified,
# host0 will be used as the ntp clock
# reference for all nodes in the cluster. This is controlled via the
# 'ntp_server_type' outlined below.
#
ntp_server_type: remote
#
```

Here is an NTP section **after** the edit for the local time source.

```
## NTP
# There are 2 options 'remote' (default) and 'local'. The default configuration
# (remote) will set up NTP to connect
# to a set of remote, Operating System specific, servers. If local is specified,
# host0 will be used as the ntp clock
# reference for all nodes in the cluster. This is controlled via the
# 'ntp_server_type' outlined below.
#
ntp_server_type: local
#
```

4. If you are working with only local time source, go to step 10. If not, go to step 7.
5. To use custom remote time sources, uncomment and edit the **ntp\_servers\_custom** list to include the NTP server URLs or IP addresses that you want used as the BPUAA host timing source in active site. Save the **all.yml** file.

Example **before** the edit for the custom remote time sources. The example focuses on the section to be edited.

```
# In the 'remote' case, you can also override the set of remote servers by
# uncommenting and setting the
# 'ntp_servers_custom' variable and configuring 1,3 or 4 NTP servers to connect
# to. To do so, uncomment
# the 'ntp_servers_custom' variable and uncomment and configure the appropriate
# number of hosts. e.g. change
# '<host a>' (and optionally host b, host c and host d) to the IP address or
# hostname of a valid NTP server.
ntp_servers_custom:
#   - <host a>
#   - <host b>
#   - <host c>
#   - <host d>
```

Example **after** the edit using hostnames. In this example, the first NTP server to be contacted will be the one with the fully qualified domain name of 0.mycustomer.ntp.com:

```
# In the 'remote' case, you can also override the set of remote servers by
# uncommenting and setting the
# 'ntp_servers_custom' variable and configuring 1,3 or 4 NTP servers to connect
# to. To do so, uncomment
# the 'ntp_servers_custom' variable and uncomment and configure the appropriate
# number of hosts. e.g. change
# '<host a>' (and optionally host b, host c and host d) to the IP address or
# hostname of a valid NTP server.
ntp_servers_custom:
- 0.mycustomer.ntp.com
- 1.mycustomer.ntp.com
- 2.mycustomer.ntp.com
- 3.mycustomer.ntp.com
```

Example **after** the edit using IP addresses. In this example the first NTP server to be contacted will be the one with an IP address of 10.128.8.89:

```
# In the 'remote' case, you can also override the set of remote servers by
uncommenting and setting the
# 'ntp_servers_custom' variable and configuring 1,3 or 4 NTP servers to connect
to. To do so, uncomment
# the 'ntp_servers_custom' variable and uncomment and configure the appropriate
number of hosts. e.g. change
# '<host a>' (and optionally host b, host c and host d) to the IP address or
hostname of a valid NTP server.
ntp_servers_custom:
- 10.128.8.89
- 10.128.8.90
- 10.128.8.91
- 10.128.8.92
```

6. By default, the **ntp\_server\_options** entry default is iburst. For details about the **ntp\_server\_options**, see <https://linux.die.net/man/5/ntp.conf>. If you want to change the default value, uncomment **ntp\_server\_options** and edit its value in both **all.yml** file for active site and **standby\_cluster** file for standby site and save the files.
7. Repeat the steps 1 to 6 on **Host 0 of Site B(standby site)**.

## Configuring geographical redundancy

This section describes the configuration of geographical redundancy functions which are given below. These parameters need to be configured in **all.yml** file.

1. **geored\_site\_state** - It can be in ACTIVE or STANDBY state.
2. **geored\_site\_id** – It identifies a site from a geographical context. You can use the variables such as Toronto, DataCenter\_1, Zone-East. You can use letters, numbers, underscores and, dashes and must be at least 3 characters in length to define it.



You must have GR SiteId and SiteState, before creating the geored\_site\_id. geored\_site\_id uniquely identifies a site from a GR context. This variable should be set to something meaningful for your deployment, for example, Toronto, DataCenter\_1, Zone-East. Application deployments will not be fully functional until the GR SiteId and SiteState are configured. Valid characters for geored\_site\_id are letters, numbers, underscores and dashes and must be at least 3 characters in length. For example, geored\_site\_id: SiteA.

3. `geored_local_site_ip`- It is used with the `geored_site_id` and `geored_site_state` to provision the local site from a geographical point of view.



The specification of this variable is optional and if not set will default to `site_ip` defined in the host's file. This IP address is the same as the `site_ip` and will not need to be overridden. The IP is not functionally significant (no GR operations depend on it).

## Requirements

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of host 0 of active site as the bpadmin user.

## Steps:

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the `all.yml` file.
3. Edit `geored_site_id`, `geored_site_state`, and `geored_local_site_ip` in `all.yml` file and save it.  
`geored_site_state` is always set to ACTIVE in `all.yml` file for active site.  
`geored_site_state` is always set to STANDBY in `all.yml` file for standby site
4. Repeat steps 1 to 3 on host0 of Site B(standby site).

# Configuring the Blue Planet email service

BPUAA requires that you configure a Simple Mail Transfer Protocol (SMTP) server so BPUAA can send system email to users. Emails are used for alarm notifications and forgotten password assistance.



If password expirations are enabled and the SMTP server is not configured, users will not be able to log in after their password expires. Ciena recommends if you cannot complete the configuration now, ensure you do it within 60 days to avoid causing users to be locked out with no way to reset their passwords. For information on configuring password notifications see the *Blue Planet BPUAA User Guide*.

Complete the following procedure to configure Blue Planet email service. This is a mandatory procedure.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of Host 0 of active site as the bpadmin user.
- Understand the SMTP server requirements at your site.

### **To configure the Blue Planet email service**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **all.yml** file and edit the SMTP parameters mentioned in table SMTP parameters. Save the **all.yml** file.

*Table 13. SMTP parameters*

PARAMETER	DESCRIPTION
smtp_username	The SMTP server account username used for sending emails.
smtp_password	The SMTP server account password.
smtp_staticPath	The staticPath value must be <code>/bp2/src/static</code> . Do not change this value.
smtp_authen	The SMTP server authentication. Set the value to true.
smtp_transport	The SMTP server transport security. Set the value to true or false, as applicable.
smtp_mail_server	The SMTP server fully qualified domain name (FQDN), such as <code>smtp.gmail.com</code> or, if a dedicated SMTP server, an FQDN that you own.
smtp_mailer_name	Must be set to Blue Planet Mailer. Do not change this value.
smtp_port	The SMTP server port number. Depending on the server, this port can be 25, 465, or 587.



PARAMETER	DESCRIPTION
smtp_email	The SMTP server email account from which reset password emails will be sent. Some SMTP servers, such as Gmail, allow you to use an alias that is not set on the server. For example, the account could be "bphostmonitor@abccompany.com", but the value could be "api-crinoid@ciena.com". Of course, you can enter the true value, "bphostmonitor@abccompany.com". The Amazon Web Services (AWS) SMTP server restricts the entry to the correct value.

Example before the edit:

```
# SMTP configuration details for 'Forgot Password' feature
smtp_username: USERNAME
smtp_password: PASSWORD
smtp_staticPath: /bp2/src/static
smtp_authen: SMTP_AUTHENTICATION
smtp_transport: SMTP_TRANSPORTSECURITY
smtp_mail_server: MAILSERVER.COM
smtp_mailer_name: MAILER_NAME
smtp_port: SMTP_PORT
smtp_email: MAILER@EMAIL.COM
```

Example after the edit:

```
# SMTP configuration details for 'Forgot Password' feature
smtp_username: GmailUser
smtp_password: AnyPassword
smtp_staticPath: /bp2/src/static
smtp_authen: true
smtp_transport: true
smtp_mail_server: smtp.gmail.com
smtp_mailer_name: Blue Planet Mailer
smtp_port: 587
smtp_email: api-crinoid@AnyCompany.com
```

3. Repeat steps 1 and 2 on the **Host 0 of Site B(standby site)**.

## Modifying the iLAN NET interface

BPUAA uses the address 172.16.0.0/16/24 for its internal LAN (iLAN).

Complete this procedure if:

- Your network uses 172.16.0.0/16/24, in which case, a conflict with the BPUAA iLAN will occur, or,
- You are implementing georedundancy. Georedundancy requires different iLAN addresses for the active and standby sites.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the `/home/bpadmin/bpi/playbooks/group_vars` directory of Host 0 of active site as the bpadmin user.
- Have a new address for the iLAN.

### **To modify the iLAN interface**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to `/home/bpadmin/bpi/playbooks/group_vars` directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment the `ilannet` option, then enter the IP network address you want BPUAA to use, for example, 172.19.0.0/16/24. Save the **all.yml** file.

Example **before** the edit:

```
#####
# install #
#####
# The ilannet to use on hosts
# ilannet: 172.16.0.0/16/24
```

Example **after** the edit:

```
#####
# install #
#####
# The ilannet to use on hosts
ilannet: 172.19.0.0/16/24
```



If you are installing georedundancy, the active and standby sites must have different iLAN addresses. The active site can use the default (or user-assigned) address. The standby site must be on a different network.

For example: Active → `ilannet:172.19.0.0/16/24` (default) and Standby → `ilannet: 172.29.0.0/16/24`. Do not modify the /24 subnet value.

4. Repeat steps 1 to 3 on the **Host 0 of Site B(standby site)**.

## Modifying the default BPUAA interface

By default, BPUAA uses the first network interface, eth0, for Blue Planet activities. Complete the following steps if you want to set a new default interface. Otherwise, you can skip this procedure and continue with the [Specifying the external license server](#) procedure.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the /home/bpadmin/bpi/playbooks/group\_vars directory of Host 0 of active site as the bpadmin user.



To display a list of interfaces, use the "ip a" command.

### **To modify the default BPUAA interface**

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to **/home/bpadmin/bpi/playbooks/group\_vars** directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment the bp\_interface option and replace eth0 with the interface you want used for example eth3. Save the **all.yml** file.

Example **before** the edit:

```
# specify the Blue Planet Interface
# if not defined, the ansible default interface
# will be used, which is typically your first interface
#bp_interface: eth0
```

Example **after** the edit:

```
# specify the Blue Planet Interface
# if not defined, the ansible default interface
# will be used, which is typically your first interface
#bp_interface: eth3
```

4. Save the file.

5. Repeat steps 1 to 4 on the **Host 0 of Site B(standby site)**.

## Specifying the external license server

Use this procedure to set up the external license server IP address in cluster and standby\_cluster files.

### Requirements

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Can access the /home/bpadmin/bpi/playbooks/group\_vars directory of Host 0 of active site as the bpadmin user.

### Steps

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to **/home/bpadmin/bpi/playbooks/group\_vars** directory.
2. Using a text editor, open the **all.yml** file.
3. Uncomment the **license\_server** parameter and replace a.b.c.d with external license server IP.
4. Uncomment the **license\_server\_backup** parameter and replace a.b.c.d with external backup license server IP. Save the **all.yml** file.

Example **before** the edit:

```
# License Server details for unbundling encrypted offline archives and runtime
requirements
#license_server: a.b.c.d
#license_server_backup: a.b.c.d
```

Example **after** the edit:

```
# License Server details for unbundling encrypted offline archives and runtime
requirements
license_server: 10.10.10.10
license_server_backup: 12.12.12.12
```

5. Repeat steps 1 to 4 on the **Host 0 of Site B(standby site)**.

# Setting up users

Complete this procedure to manage keys of the bpadmin user and the root user, and to create the bpuser user (sudo restricted Docker install user) and manage its sudo permissions and keys. This is a mandatory procedure. The setup script skips this step if you have previously manually created the bpuser user.

Before you begin this procedure, verify that you:

- Completed [Updating the hosts file](#) procedure.
- Know the bpadmin user password.
- Can access the /home/bpadmin/bpi directory of Host 0 of active site as the bpadmin user

## To set up users

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to **/home/bpadmin/bpi/** directory.
2. To start the setup users' script enter:

```
./bpi --setup-users
```

3. If prompted, enter the bpadmin user password.



For multi-host deployments, you must enter the bpadmin password for each host.

4. If you have not previously completed the procedure to manually create the bpuser user, then:
  - a. When prompted, enter the bpuser password. The same password is set on all hosts.
  - b. Re-enter the password for the bpuser user.

The script sets the bpadmin and bpuser authentication keys as well as several sudo privileges for the bpuser user. See the files in /home/bpadmin/bpi/roles/setup-users/sudoers/templates to see the settings.

5. If you have not previously completed the procedure to manually create the bpmaint user:
  - a. When prompted, enter the bpmaint password. The same password is set on all hosts.
  - b. Re-enter the password for the bpmaint user.
6. Repeat steps 1 to 4 on the **Host 0 of Site B(standby site)**.

# Installing SNMP packages in UAA containers

1. Enter uaa-amc container:

```
enter_container uaa-amc_23.08.xx_x
```

2. Edit the below file and add the below line at the start of the file and save:

```
vi /etc/apt/sources.list
```

```
deb http://archive.ubuntu.com/ubuntu/ focal main restricted
```

3. Install snmp packages by running the below command:

```
apt update -y
```

```
apt install -y snmp
```

4. To verify the snmp modules installation try to do a `snmpbulkget`
5. Repeat above command in rest of the uaa-appmon-collector containers
6. Place the node action script files on host at path:

```
/opt/ciena/bpuaa/node-actions/
```

7. Configure the node action script path in UAA UI as below:

```
/bp2/data/scripts/node-actions/
```

8. Enter the node action script name in UI and save.

# Example Node action Script

```
snmpbulkget:
#!/bin/bash
snmpbulkget-v2c -c public $1:$2 -On $
```

Node Actions > My Script

PropertiesPermissions

NameMy Script

Description

Timeout30(Seconds)

DomainDefault

Script Directory/bp2/data/scripts/applications

Script Namesnmpbulkget.sh

Remote Script☐

Enable Confirmation Message☐

Script Arguments: "Snodelp\$" "SnodePort\$" "Soid\$"

\* Node fields can be sent as arguments to the script by putting the column name within \$\$, E.g. \$Name\$ \$Primary IPv4/6\$ etc., As a best practice enclose the tokens with double quotes("), E.g. "\$Name\$" "\$Primary IPv4/6\$" etc., Refer help page for all the supported fields.

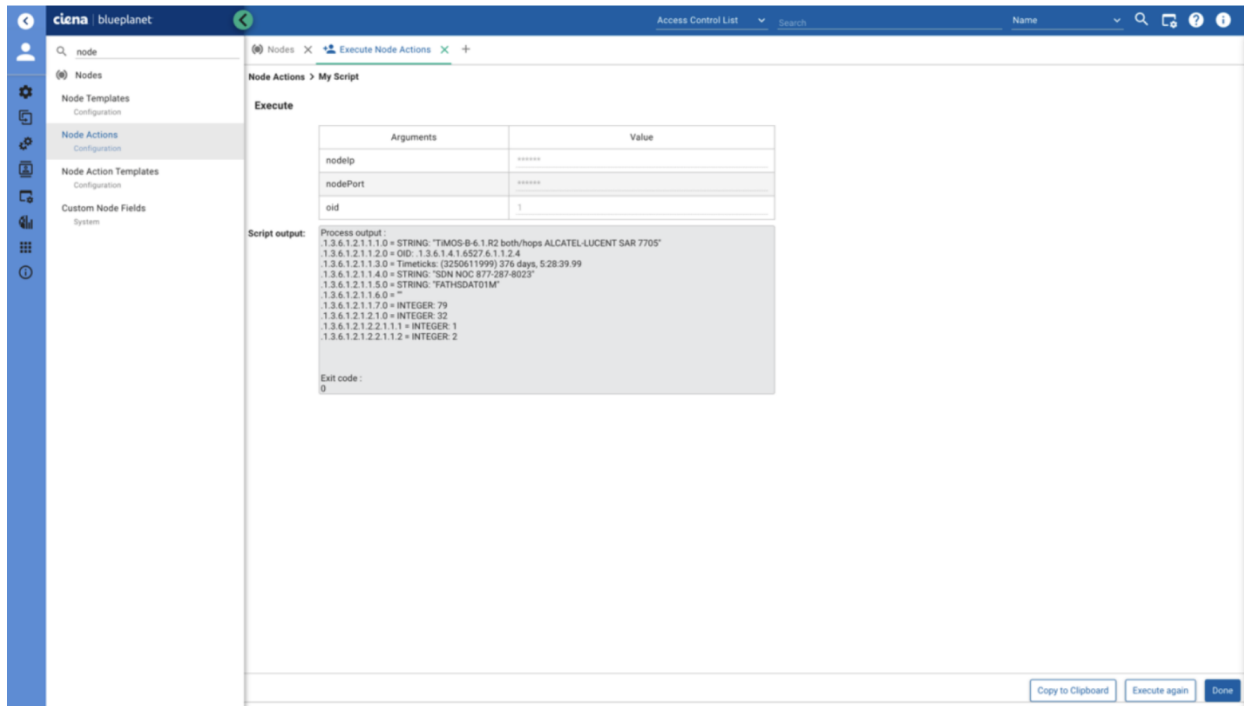
Arguments	Data Form	Default Value
nodelp	Node Properties	Primary IPv4/6
nodePort	Node Properties	Primary Port
oid	User Input	1

Reset

Close

Execute

Update and Close



snmpset:

```
#!/bin/bash
snmpset -v2c -c $1 $2:$3 $4 s $5
$1-Community
$2-Node IP
$3-Node Port
$4-OID
s-accept
$5-Value
```



# Validating the hosts

This procedure verifies that the host hardware and software where you will install the BPUAA meet Ciena requirements. The validation is based upon requirements described in the [Server hardware and VM requirements](#) topic.

The validation phase checks the following areas and related requirements:

- Hardware (CPU, RAM, and SWAP)
- Operating system (type, architecture, version, system-level packages for bpi execution, and SELinux mode)
- Disk (mountpoints, size, and Docker volume group [if required])
- Network (ports and unique hostnames)

Before you begin this procedure, verify that you:

- Completed [Setting up users](#) procedure.
- Can access the `/home/bpadmin/bpi` directory of Host 0 of active site as the bpadmin user.

## To validate the hosts

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to `/home/bpadmin/bpi/` directory.
2. Validate the system by executing command.

```
./bpi --validate <profile>
```

where	
<profile>	is the validation profile.  Possible values are: <b>orch-dev</b> (lab environment) or <b>orch-prod</b> (production environment).

3. If prompted, enter the bpadmin user password.



For multi-host deployments, you must enter the bpadmin password for each host.

The system displays various task-related outputs as the validation progresses. At the end of the

validation process, the system displays a summary.

4. If elements display a Failed status, correct them, then repeat step 2 and 3 until all elements display a Passed status.
5. If all elements display a Passed status and "failed=0" at the end of the summary, continue with the next procedure.
6. Repeat steps 1 to 5 on the **Host 0 of Site B(standby site)**.

## Configuring BPUAA hosts on active and standby sites

Complete this procedure to configure the BPUAA host(s) on active and standby sites for the BPUAA software installation from Host 0 of active site.

Configuring the BPUAA hosts creates the following directories on active and standby sites. It also ensures they are owned by bpuser on both active and standby sites:

- /etc/bp2
- /etc/bp2/site
- /etc/bp2/solutionmanager

This procedure also performs minor configuration changes including updates to syslog, rsyslog, sshd, and NTP to prepares the hosts for BPUAA installation on active and standby sites.

Before you begin this procedure, verify that you:

- Completed [Setting up users](#) procedure.
- Know the bpadmin user password.
- Can access the /home/bpadmin/bpi directory of Host 0 of active site as the bpadmin user
- If you chose not to implement the Blue Planet NTP option in the [Configuring a time source](#) procedure and will use your network NTP for BPUAA host timing, add the playbook arguments shown in step 2c.

### ***To configure the BPUAA hosts***

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to /home/bpadmin/bpi/ directory.
2. Execute one of the following commands, depending on whether your installation is single-host or multi-host and your NTP timing preference.

a. Single-host:

```
./bpi --site <lineup file>
```

b. Multi-host:

```
./bpi --site <lineup file>
```

c. If you are provisioning your own NTP timing, add the following playbook arguments by executing command (on single line):

```
./bpi --site <lineup file> -- playbook-args='--skip-tags ntp'
```

If no failures occur, indicated by failed=0, continue with the next step. If failures occurred, contact Ciena Customer Support for guidance.

3. Copy the following Postgres credential files from the active site and paste them to the standby site in the same location where these files are saved in the active site.

```
/etc/bp2/bpocore/private/users.json  
/etc/bp2/bpopg/private/users.json  
/etc/bp2/metricsdb/private/users.json  
/etc/bp2/postgres/private/users.json  
/etc/bp2/chetak/private/postgres.json
```

4. Repeat steps 1 and 2 on the **Host 0 of Site B (standby site)**.

If all elements display a **Passed** status and "failed=0" at the end of the summary, continue with the next procedure.

## Installing Core Platform and Extended Platform Solution on active and standby sites

Complete this procedure to install core platform and platform solution on active and standby sites from host 0 of the active site.

Before you begin this procedure, verify that you:

- Completed [Configuring BPUAA hosts on active and standby sites](#).
- Know the bpadmin user password.
- Can access the `/home/bpadmin/bpi` directory of host 0 of active site as the bpadmin user

To install BPUAA platform and solutions:

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the host 0) and navigate to `/home/bpadmin/bpi/` directory.
2. Install the Core Platform and Platform Solution for BPUAA 23.08.64 on active and standby sites by entering (on a single line):

```
./bpi --install <lineup file> --playbook-args='--skip-tags bp2-solution'
```

If all elements display a Passed status and "failed=0" at the end of the summary, continue with [Installing BPUAA on geographical redundant sites \(manual procedure\)](#).

3. Repeat steps 1 and 2 on the **Host 0 of Site B(standby site)**.

## Installing BPUAA on geographical redundant sites (manual procedure)

Complete the same procedure for either single or multi geographical redundant configurations, with the only difference being the lineup file:

1. Log in to Host 0 of Site A (active site) as bpadmin (do not use the Site IP, use the IP address of the Host 0) and navigate to the `/home/bpadmin/bpi/` directory:
  - a. Share the keys with the standby site or the active host:

```
$ ./bpi --geo-keys <standby_site_ip>
```



For single host deployment <Site IP> is always the same as host0, for HA setup the <Site IP> must be different than host IP.

- b. Start the georedundancy setup and tunnel creation:

```
$ ./bpi --setup-geo <standby_site_ip> --playbook-args='--tags geo:tunnel'
```

Where `standby_site_ip` is the site ip of standby cluster

- c. Install the BPUAA solutions on the active host. Enter this command on a single line.

```
./bpi --install <lineup file> --playbook-args='--tags bp2-solution'
```

Output, similar to the following, indicates whether the BPUAA solution installation succeeded:

```
PLAY RECAP
*****
***
<host>                                : ok=102    changed=47    unreachable=0
failed=0
```

- d. If no failures occur, indicated by `failed=0`, continue with the next step. If failures occurred, contact Ciena Customer Support for guidance.
- e. Log in to the active site Nagios.

```
https://<active_site_ip>/nagios
```

Wait until Nagios is in a stable state before proceeding. All nagios checks should be green.



Do not continue until all alarms are resolved.

2. Log in to Host 0 of Site B (standby site) as `bpadmin` (do not use the Site IP, use the IP address of the Host 0) and navigate to `/home/bpadmin/bpi/` directory:
- a. Install the BPUAA solutions on the standby host:

```
./bpi --install <lineup file> --playbook-args='--tags bp2-solution'
```

- b. If no failures occurred, continue with the next step. If failures occurred, contact Ciena Customer Support for guidance.
- c. Log in to the standby host Nagios.

```
https://<standby_site_ip>/nagios
```

Verify that no applications are in the Pending state. Wait until Nagios is in a stable state before proceeding.



Some Critical/Warnings alarms are expected. The BP UI is disabled for the standby host except for the geographical redundant UI

## Configuring GR on the active site

1. Log in to Host 0 of site A (Active) as bpadmin. Do not use the site IP; use the IP address of Host 0.
2. Navigate to /home/bpadmin/bpi.
3. Start the setup of GR from site A:

```
./bpi --setup-geo < site IP of standby site B > --playbook-args='--skip-tags
geo:notify_standby'
```

4. Enter the username and password as an administrator (default: admin).
5. Alternatively, you can use the following command:

```
./bpi --setup-geo < site IP of standby site B > --playbook-args='--skip-tags
geo:notify_standby -e geo_user=<user> -e geo_password=<password>'
```



After starting the setup of GR, and before site A is added to the site B configuration (a later step), some services can be in a temporarily degraded (warning or critical) state in Nagios of site A. This will continue until you complete the GR setup.

6. Wait for few minutes before proceeding with further steps.

## Configuring GR on the standby site

1. From site A (active) Host 0, continue the setup of GR:

```
./bpi --setup-geo < Standby site B IP > --playbook-args='--tags
geo:notify_standby'
```

2. Enter the username and password as an administrator (default: admin).
3. Alternatively, you can use the following command:

```
./bpi --setup-geo < Standby site B IP > --playbook-args='--tags
geo:notify_standby -e geo_user=<user> -e geo_password=<password>'
```

4. Access the site B (standby) GR UI from a web browser to verify the Active and Standby status.

```
https://<site IP of standby site B>/bp-platform-ui/#/geored-ui
```

5. Log in with the default Blue Panet UI. The default username and password for the login are admin and adminpw, respectively.
6. In the site A (active) Nagios([http://<active\\_site\\_ip>/nagios](http://<active_site_ip>/nagios)), verify that the status of all services displays OK (green). In site B (standby) Nagios([http://<standby\\_site\\_ip>/nagios](http://<standby_site_ip>/nagios)), verify that none of the applications are in Pending/Critical state.
7. Check Nagios to make sure all services are running in the GREEN state on both active and standby sites.



Nagios can take 30 minutes or more to display the status of all services. The status of services waiting for the health check to run displays in a gray color.

# Uninstalling

- [Uninstalling BPUAA software \(deployment without GR\)](#)
- [Uninstalling BPUAA \(deployment with GR\)](#)



# Uninstalling BPUAA software (non-GR deployments)

Complete this procedure to uninstall the BPUAA software, optionally fix a reversible site configuration issue such as a misconfigured ILAN NET interface, and re-install the BPUAA software. This procedure is for a multi-host deployment without georedundancy (GR).

The four main phases of the installation workflow are:

1. system setup
2. system validation
3. site configuration
4. installation

When you uninstall the BPUAA software, you undo phase 4 (installation) of the installation workflow. Phases 1 to 3 remain complete.

## **To uninstall**

1. Back up the BPUAA software solution data. For details, see the "Backing up and restoring" procedure in the *Blue Planet BPUAA Administrator Guide*. Make sure to save the backup file in a safe location.
2. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
3. Start the uninstallation by entering:

```
./bpi --uninstall
```

4. When the uninstallation is complete, make sure that the `/opt/ciena/bp2` directory is empty.
5. Optionally fix a reversible site configuration issue such as a misconfigured ILAN NET interface (see the [Modifying the ILAN NET interface](#) procedure).
6. Re-install the BPUAA software, see the [Installing the BPUAA platform and solutions](#) procedure.
7. Restore the BPUAA solution data. For details, see the "Backing up and restoring" chapter in the *Blue Planet BPUAA Administrator Guide*.

# Uninstalling BPUAA (deployment with GR)

Use this procedure to uninstall the BPUAA software, optionally fix a reversible site configuration issue such as a misconfigured ILAN NET interface, and re-install the BPUAA software. This procedure is for a multi-host deployment with georedundancy (GR).

The four main phases of the installation workflow are:

1. system setup
2. system validation
3. site configuration
4. installation

When you uninstall the BPUAA, you undo phase 4 (installation) of the installation workflow. Phases 1 to 3 remain complete.

## **To uninstall BPUAA**

1. Back up the BPUAA solution data on Site A (active). For details, see the "Backing up and restoring" procedure in the *Blue Planet BPUAA Administrator Guide*. Make sure to save the backup file in a safe location.

## **Uninstalling BPUAA from Site A (active)**

2. Log in to host 0 of Site A (active) as badmin and navigate to the /home/bpadmin/bpi directory.
3. Check the geored-tunnel status by entering:

```
sudo geored-tunnel-status
```

4. If the output shows a `===Remote Site Nodes===` section with details, it means that the geored-tunnel is configured between the local and remote sites, and you need to go to [step 5](#). Otherwise, go to [step 8](#).
5. Stop the geored-tunnel by entering:

```
sudo geored-tunnel-stop
```

6. Check the geored-tunnel status by entering:

```
sudo geored-tunnel-status
```

7. Clean-up the tunnel configuration by entering:

```
./bpi --utility playbooks/geo-clean.yml
```

8. To confirm that the geored-tunnel is stopped, review the `===Remote Site Nodes===` section in the output. That section should be empty.
9. Start the uninstallation by entering:

```
./bpi --uninstall
```

10. When the uninstallation is complete, make sure that the `/opt/ciena/bp2` directory is empty.
11. Optionally fix a reversible site configuration issue such as a misconfigured ILAN NET interface (see the "[Modifying the ILAN NET interface](#)" procedure).
12. Perform the "[Installing BPUAA on geographical redundant sites \(manual procedure\)](#)" procedure.

### Uninstalling BPUAA from Site B (standby)

12. Log in to host 0 of Site B (standby) as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
13. Start the uninstallation by entering:

```
./bpi --uninstall
```

14. When the uninstallation is complete, make sure that the `/opt/ciena/bp2` directory is empty.
15. Optionally fix a reversible site configuration issue such as a misconfigured ILAN NET interface (see the "[Modifying the ILAN NET interface](#)" procedure).
16. Perform the "[Configuring the BPUAA hosts \(non-GR deployments\)](#)" procedure.
17. Perform the [Installing BPUAA on geographical redundant sites \(manual procedure\)](#) procedure.
18. Restore the BPUAA solution data. For details, see the "Backing up and restoring" chapter in the *Blue Planet BPUAA Administrator Guide*.

# Adding and replacing BPUAA hosts

Complete this procedure to add or replace BPUAA hosts.

- [Adding and replacing hosts in non-geored or for geo-red hosts 1 or 2](#)
- [Adding and replacing BPUAA geored hosts](#)



If the system is built on Azure server with a floating IP, make sure to configure floating IP on hosts. Refer *Configure floating private IP for microsoft Azure*.

## Adding and replacing hosts in non-geored or for geo-red hosts 1 or 2

Complete this procedure to add or replace BPUAA hosts in a non-geored HA installation, or replace host 1 or host 2 in a geored HA installation.

For details on how to perform these steps for a single-node geored installation or for replacing host 0 of either the Active or Standby configuration of a geored HA cluster, see [Adding and replacing BPUAA geored hosts](#) below.

Adding and replacing BPUAA hosts using the Blue Planet installer (bpi) is accomplished in five general steps:

- Host file set up
- System validation
- User and key management
- System configuration
- Application software installation

Before you begin, ensure that:

- You perform the following pre-installation steps described in the [Pre-installation procedures](#) section if you are replacing host 0 in non-geored installation..
  - [Creating the bpadmin user](#)
  - [Configuring the swappiness kernel parameter](#)

- [Installing the LinuxIntel system bundle](#)
- [Transferring the installation files to the host](#)
- You configure existing installation variable as mentioned in section [Host setup and BPUAA installation \(non-GR deployments\)](#) or [Host setup and BPUAA installation \(GR deployment - automatic\)](#) if you are replacing host 0 in non-geored installation.
- You perform the following pre-installation steps described in the [Pre-installation procedures](#) section, if you are replacing host 1 and host 2 in non-geored or geored HA installation.
  - [Creating the bpadmin user](#)
  - [Configuring the swappiness kernel parameter](#)
  - [Installing the LinuxIntel system bundle](#)
- You have the lineup file that was used for the last installation/deployment. This is the lineup file you will use in the following steps. Verify that the versions specified in the lineup file match what is currently deployed on the hosts. If the lineup doesn't match, any solution not in the lineup file but currently deployed, will not be properly deployed on the replacement host.

### **To add or replace hosts**

1. Set up the hosts file:
  - a. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
  - b. Use a text editor, such as `vi`, to open the hosts file.
    - To add a host(s), uncomment and set a host entry to the required IP address for that host. Make sure to use the IP address (IPv4, not IPv6), not the hostname.

Before:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
#host1 ansible_host=10.186.0.2 controller=False
#host2 ansible_host=10.186.0.3 controller=False
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False
```

After:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True
#host3 ansible_host=10.186.0.4 controller=False
#host4 ansible_host=a.b.c.d controller=False
```

- To replace a host, replace the host entry/entries in the hosts file. In the following example, host2 10.186.0.3 is replaced with 10.186.0.9.

Before:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False
```

After:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.9 controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False
```

2. Save the hosts file and exit the text editor.

After the hosts file is updated and accurately reflects the current system inventory, proceed to the next step.

3. Validate the system:

```
./bpi --validate <profile>
```

where

<profile>	is the validation profile.
-----------	----------------------------

The validation displays a series of checks, the status of each check, Passed or Failed, then details about the check. If checks fail, details about the failure are provided.

4. When the system validation script is complete, start the setup users script to manage users and keys:

```
./bpi --setup-users
```

This command:

- Performs all required actions on the new/replacement host(s).
  - Performs any required actions against the existing host(s) including sharing of the root key(s) from the new/replacement host(s) with the existing host(s).
5. When prompted, enter the password for the bpadmin user once for each added host.
6. Configure the site:

```
./bpi --site <lineup file>
```

where

<lineup.yml>

is the location of this file. For example,  
/opt/ciena/loads/<UAA\_version>/lineup-multi-rhel.yml.

This command:

- Performs all required actions on the new/replacement host(s).
  - Performs any required actions against the existing host(s) including:
    - Adding/modifying host keys for the new/replacement host(s) to the known\_hosts file on the existing host(s).
    - Adding/modifying an entry to the /etc/hosts file on the existing host(s) for new/replacement host(s).
7. When the site script is complete, start the installation script:

```
./bpi --install <lineup file>
```

This command:

- Performs all required actions on the new/replacement host(s).
- Performs any required actions against the existing host(s) including:
  - Adding/updating the hosts config for new/replacement host(s) on the existing host(s).
  - Updating the iLAN configuration on the existing host(s) for new/replacement host(s).

Solution scaling after a host(s) addition/replacement follow the default scale behavior:

- The BPUAA core platform scales to num\_hosts.
- The platform solution scales to num\_hosts.

- Additional solutions scale to num\_hosts only if the scale option is set to *true* in the lineup.yml file.



Refer UAA Administrator Guide - Maintenance Procedures (UAA) section to *stop* all the solutions and *start* them. Make sure that the solutions are stopped first before starting.

## Adding and replacing BPUAA geored hosts

This section describes how to add or replace BPUAA hosts for either single-node geored installations or when replacing host 0 of either the Active or Standby configuration of a GR HA cluster.

For details on how to perform these steps for a non-geored HA installation, or replace host 1 or host 2 in a geored HA installation, see [Adding and replacing hosts in non-geored or for geo-red hosts 1 or 2](#) above.

This procedure allows you to replace your existing Active site if it fails, or take down the Active site for server maintenance.

Adding and replacing BPUAA hosts using the Blue Planet installer (bpi) is accomplished in five general steps:

- Host file set up
- System validation
- User and key management
- System configuration
- Application software installation

For georedundant sites, you must check or update the following in the hosts file:

- active/standby status
- IP (done previously)
- site IP (for cluster; must be unique for active/standby cluster)
- geored\_site\_id (must be unique for active/standby cluster)
- on both the new Active and the new Standby /etc/bp2/geored/config.json:
  - if no failover has occurred (on each host in the cluster or each host in single geored)
  - if in an HA cluster geored config and failover has occurred (on each host in the standby cluster).



- the BPUAA internal LAN (ILAN) in the all.yml file. See the [Modifying the ILAN NET interface](#) procedure for more information.

Before you begin, ensure that:

- You perform the following pre-installation steps described in the [Pre-installation procedures](#) section if you are replacing host 0 in geored HA installation
  - [Creating the bpadmin user](#)
  - [Configuring the swappiness kernel parameter](#)
  - [Installing the LinuxIntel system bundle](#)
  - [Transferring the installation files to the host](#)
- You configure existing installation variable as mentioned in section [Host setup and BPUAA installation \(GR deployment - automatic\)](#) if you are replacing host 0 in geored installation.
- You have the lineup file that was used for the last installation/deployment. This is the lineup file you will use in the following steps. Verify that the versions specified in the lineup file match what is currently deployed on the hosts. If the lineup doesn't match, any solution not in the lineup file but currently deployed, will not be properly deployed on the replacement host.

### ***To add or replace hosts***

#### **1. Set up the hosts file:**

- a. Log in to host 0 as bpadmin and navigate to the /home/bpadmin/bpi directory.
- b. Use a text editor, such as vi, to open the hosts file.
  - To add a host(s), uncomment and set a host entry to the required IP address for that host. Make sure to use the IP address (IPv4, not IPv6), not the hostname.

Before:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
#host1 ansible_host=10.186.0.2 controller=False
#host2 ansible_host=10.186.0.3 controller=False
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False
##site_ip=a.b.c.d/42
+
After:
+
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True
#host3 ansible_host=10.186.0.4 controller=False
#host4 ansible_host=a.b.c.d controller=False
site_ip=10.186.0.1/22
```

- To replace a host, replace the host entry/entries in the hosts file. In the following example, host2 10.186.0.3 is replaced with 10.186.0.9.

Before:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.3 controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False
#site_ip=a.b.c.d/42
#geored_site_id=<site name>
# Valid options for #geored_site_state are ACTIVE or STANDBY.
#geored_site_state=<choose state>
```

After:

```
[cluster]
host0 ansible_host=10.186.0.1 controller=True
host1 ansible_host=10.186.0.2 controller=True
host2 ansible_host=10.186.0.9 controller=True
#host3 ansible_host=a.b.c.d controller=False
#host4 ansible_host=a.b.c.d controller=False
site_ip=10.186.0.1/22
geored_site_id=SiteA
# Valid options for geored_site_state are ACTIVE or STANDBY.
geored_site_state=ACTIVE
```

After the hosts file is updated and accurately reflects the current system inventory, proceed to the next step.

## 2. Validate the system:

```
./bpi --validate <profile name>
```

where	
<profile>	is the validation profile.

The validation displays a series of checks, the status of each check, Passed or Failed, then details about the check. If checks fail, details about the failure are provided.

## 3. When the system validation script is complete, start the setup users script to manage users and keys:

```
./bpi --setup-users
```

This command:

- Performs all required actions on the new/replacement host(s).
- Performs any required actions against the existing host(s) including sharing of the root key(s) from the new/replacement host(s) with the existing host(s).

## 4. When prompted, enter the password for the bpadmin user once for each added host.

## 5. Configure the site:

```
./bpi --site /opt/ciena/loads/xx.xx/lineup.yml
```

where	
<lineup.yml>	is the location of this file. For example, /opt/ciena/loads/<uaa_version>/lineup-multi-rhel.yml.

This command:

- Performs all required actions on the new/replacement host(s).
- Performs any required actions against the existing host(s) including:
  - Adding/modifying host keys for the new/replacement host(s) to the known\_hosts file on the existing host(s).

- Adding/modifying an entry to the `/etc/hosts` file on the existing host(s) for new/replacement host(s).
6. Update the `geored_site_id` and the `geored_site_state` for both the new active and the standby.
  7. Update (each host on the new Active cluster or all of the hosts on both Active/Standby clusters) `/etc/bp2/geored/config.json` in the ha-cluster geored config depending on whether failover has occurred.
  8. Update the BPUAA internal LAN (ILAN) in the `all.yml` file to ensure they are both unique. See the [Modifying the ILAN NET interface](#) procedure for more information.
  9. To clean up the existing georedundant tunnel on both the active and standby single or HA cluster, Use the following

```
./bpi --utility playbooks/geo-clean.yml
```



You must run this many times and check the geored status with `sudo geored-tunnel-status` command from either the active or standby site.

10. Complete the [Installing BPUAA on georedundant sites](#) procedure if installing on the Active/new host0. Otherwise, to install on the Standby new host0, repeat this procedure starting with step 3 and skipping step 4c (since geored has already been installed on the active host).



Refer UAA Administrator Guide - Maintenance Procedures (UAA) section to *stop* all the solutions and *start* them. Make sure that the solutions are stopped first before starting.

# Troubleshooting

## Checking Kafka topics

If you receive Nagios alerts for Kafka indicating an issue with a Kafka broker (the one that is lost during the host replacement) and ractrl and trapf alerts indicating under-replicated partitions for their respective topics in Kafka, run the following procedures.

*To check whether the Kafka topics require replication to the replacement host*

1. On **Host 0 (if replacing Host 1 or Host 2)** or **Host 1 or Host 2 (if replacing Host 0)**, access the Solution Manager (solman) as *bpadmin* by entering:

```
sudo solman
```

2. Determine the version of the kafka container and instance by entering:

```
sps | grep kafka
```

*Example of system output*

```
artifactory.ciena.com/blueplanet/kafka:3.1.6-k1.1.9 kafka_3.1.6-k1.1.9-1_0
Started 172.16.2.18 11 days, 19:24:35.913239 kafka
artifactory.ciena.com/blueplanet/kafka:3.1.6-k1.1.9 kafka_3.1.6-k1.1.9-1_1
Started 172.16.0.18 11 days, 19:47:14.090817 kafka
artifactory.ciena.com/blueplanet/kafka:3.1.6-k1.1.9 kafka_3.1.6-k1.1.9-1_2
Started 172.16.1.10 11 days, 19:47:13.673350 kafka
artifactory.ciena.com/blueplanet/kafkacomet:1.0.20 kafkacomet_1.0.20
Started 172.16.0.13 11 days, 19:47:15.741129 kafkacomet
artifactory.ciena.com/blueplanet/kafkacomet:1.0.20 kafkacomet_1.0.20_1
Started 172.16.1.27 11 days, 19:47:08.363930 kafkacomet
```

3. Take note of the kafka instance that is on Host 0 (if replacing Host 1 or Host 2) or Host 1 or Host 2 (if replacing Host 0).
4. Enter the kafka container by entering:

```
enter_container kafka_<kafka_instance>
```

WHERE	
<kafka_instance>	is the kafka instance on Host 0 (if replacing Host 1 or Host 2) or Host 1 or Host 2 (if replacing Host 0).  Example: 3.2.2-k1.1.9-1_0

5. Go to the /opt/kafka/bin directory.
6. Start the replication health check by entering:

```
./replica-health-check.sh
```

#### Example of system output

```

Collecting ZooKeeper information...
zookeeper host 172.16.0.30:2181 is ok
zookeeper host 172.16.1.44:2181 is ok
Using zk host 172.16.1.44:2181
Collecting broker info from ZooKeeper
Active broker ids: 1001,1002,1004
Checking for under-replicated-partitions...
found 1586 under-replicated partitions
calculating outstanding replicas...
Outstanding replicas: 1001 1002 1003
Replica 1001 present
Replica 1002 present
Replica 1003 MISSING
Preparing to rebalance partitions to brokers: 1001 1002 1004
Dumping list of topics to /bp2/tmp/topicsToMove.json...
Creating partition reassignment plan in /bp2/tmp/plan.json

About to execute partition reassignment to brokers: 1001
1002 1004

Press Enter to continue, Ctrl-C to cancel:

```

7. Select your next step:

IF THE SCRIPT	THEN GO TO
exits and indicates that there are no under-replicated partitions	<a href="#">step 10.</a>
does not exit	<a href="#">step 8.</a>

8. At the prompt, press **Enter** to continue.
9. When the replication check is complete, the system output displays the following message:

```
Save this to use as the --reassignment-json-file option during rollback
Successfully started reassignment of partitions.

The above rollback plan was saved in /bp2/tmp/rollback.json
To rollback, execute the following:
kafka-reassign-partitions.sh --bootstrap-server localhost:9092 --zookeeper
172.16.1.44:2181/kafka --reassignment-json-file /bp2/tmp/rollback.json --execute
```

10. Exit the kafka container by entering:

```
exit
```

To restart the racrl and trapf services:

1. Enter

```
solution_app_restart <orchestrate_version> racrl,trapf
```

#### WHERE

<orchestrate\_version> is the version of the orchestrate solution.

Example: 20.06.2-47

## Clearing GlusterFS alerts

The GlusterFS alerts should clear on their own. If you want to clear them immediately, use this procedure.

To clear GlusterFS alerts:

1. Enter the glusterfs container by entering:

```
enter_container glusterfs_<version>_<instance>
```

2. Launch file system replication:

```
gluster volume heal gfsvol full
```

3. Monitor progress with the following command:

```
gluster volume heal gfsvol info
```

Replication is complete once output shows "Number of entries: 0" on all 3 bricks.

4. Exit the glusterfs container by entering:

```
exit
```



# Displaying installation logs

Complete this procedure to display the BPUAA installation logs.

1. Log in to host 0 as bpadmin and navigate to the `/home/bpadmin/bpi` directory.
2. Change to the logs directory:

```
cd logs
```

3. Display any of the following log files:

Log file name	Description	Associated procedure
setup_YYYY-MM-DD.log	Records the setup of the bpi tool.  The <i>bash bpi-&lt;version&gt;.sh</i> script creates this log file.	<a href="#">Downloading the installation files</a>
setup_users_YYYY-MM-DD.log	Records the user setup phase.  The <i>./bpi --setup-users</i> script creates this log file.	<a href="#">Setting up users</a>
bpi-YYYY-MM-DD.log	Records all other bpi actions.  The following scripts create this log file:  <i>./bpi --site &lt;lineup_file&gt;</i>  <i>./bpi --install &lt;lineup_file&gt;</i>	<a href="#">Configuring the BPUAA hosts</a>  <a href="#">Installing the BPUAA platform and solutions</a>

---

## Contacting Blue Planet

Blue Planet Division Headquarters	7035 Ridge Road Hanover, MD 21076 +1 800-921-1144
Blue Planet Support	<a href="https://www.blueplanet.com/support">https://www.blueplanet.com/support</a>
Sales and General Information	<a href="https://www.blueplanet.com/contact">https://www.blueplanet.com/contact</a>
Training	<a href="https://www.blueplanet.com/learning">https://www.blueplanet.com/learning</a>

For additional information, please visit <https://www.blueplanet.com>.

---

# LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION, INCLUDING ITS SUBSIDIARY, BLUE PLANET SOFTWARE, INC., AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION OR BLUE PLANET SOFTWARE, INC IS STRICTLY FORBIDDEN.

EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PUBLISHING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, BLUE PLANET PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. For the most up-to-date technical publications, visit <https://my.ciena.com>.

Copyright© 2023 Ciena® Corporation. All Rights Reserved

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of Blue Planet. Ciena®, the Ciena logo, Blue Planet®, and other trademarks and service marks of Ciena, Blue Planet, and/or their affiliates appearing in this publication are the property of Ciena and Blue Planet. Trade names, trademarks, and service marks of other companies appearing in this publication are the property of the respective holders.

The usage of elasticsearch interface for any purpose other than the documented and intended Blue Planet usage is strictly forbidden and a violation of our terms of service.

**Security** Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.