blueplanet®
a division of ciena

UAA Remote Data Collector

Upgrade MOP

Release 23.08.64

Issue 1.0 | November 21, 2023 | 450-3704-327-2308

Table of Contents

Publication History

The following table lists the 23.08.64 RDC Upgrade history.

DATE	VERSION	NOTES
21-Nov-2023	1.0	Maintenance Release 23.08.64

System Requirements

UAA-RDC supports the following versions of Operating Systems:

UAA-RDC version	Supported OS and versions		
Upgrade from 23.04.xx, 23.08.xx to 23.08.64	CentOS versions	RHEL versions	Oracle Enterprise Linux versions
	CentOS 7.9	RHEL 7.9	OEL 7.9

Patch Install Instructions (Non-GR)

The upgrade of RDC is not directly supported from the previous versions. User will require to un-deploy the currently installed RDC from their servers and install the latest version.

NOTE The following command should be executed in one line.

1. To un-deploy the currently installed RDC on the servers, login to LWDC/RDC server as bpadmin user and execute the following command to un-deploy RDC solution –

```
solutions=`sudo solman sps | grep ^artifactory.ciena.com|grep -e 23.08`; for s in
$solutions; do sudo solman "solution_undeploy $s --purge --yes"; done;
```

   The above command will un-deploy all the containers from the LWDC/RDC server.

2. Verify the RDC solution is undeployed by logging into UI.
3. Use the latest **Installing Light Weight Data Collector (LWDC/ RDC)** section of **UAA Deployment Guide (Cloud or On-Prem)** to deploy the latest RDC solution on the server.

Patch Install Instructions (GR)

Pre-requisites

1. Make sure you have reviewed the Blue Planet Release Notes for information about features and functions and any requirements not listed below.
2. Make sure Solution Manager authentication (proxyauth) is not enabled.
3. Make sure you have Ciena Portal access (http://my.ciena.com). This is required to download the new Linux system bundle and the RDC software.
4. Make sure you can use your existing license file to download the new software release. If you have not installed the Standalone License Server or do not have an active software license, refer **BP Engineering Guide** for the licensing procedure.
5. Ensure that the server meets the requirements for RDC as provided in the **BP Engineering Guide**.
6. All the commands should be run with root or sudo privileges.
7. The user should be able to SSH to all the UAA-RDC servers without password (password-less authentication must be set) from the server where the upgrade is planned to be executed.
8. It is recommended to run the upgrade from host *(leader instance)*.
9. Make sure to have at least 50% free disk space before upgrading.
10. Make sure to have at least 40+ GB free disk space under */opt/ciena* before upgrading.
11. Make sure that the user group names are not exceeding 30 characters before upgrading else the upgrade will fail.
12. Recommended network guidelines Between GR sites are less than 20ms latency but GR is supported up to 100ms.
    Note that having more than 20ms latency will have an impact on time taken to setup new standby site. It might take up to couple of days depending on FM data size.
13. The UAA-RDC 23.08 upgrade workflows for multi-host deployment with geographic redundancy uses the following designations:
    - Site A (active)
    - Site B (standby)

Upgrade with Geographical Redundancy

To upgrade the single-host or multi-host deployment with geographic redundancy, you need to perform the following procedures -

- Updating Site for Upgrade
- Upgrading Site A (Active) to 23.08
- Upgrading site B and setting up geographical redundancy

Updating Site for Upgrade

You need to update the site and bring it to the state from where you can start the upgrade. Following are the steps to update site.

- Downloading the installation files
- Transferring the Installation Files to Host
- Disabling geographical redundancy configuration
- Activating site B (standby) (optional)
- Preparing hosts for upgrade (on site A)

Downloading Installation Files

To install the UAA-RDC 23.08 platform and solutions, you need the following files:

- bp_uaa-remote-lwdc_23.08.00-xx.tar - Contains the RDC solutions specific for customer installation.
- bpi_23.08-xx.sh - Contains the Blue Planet installer scripts and commands that will install RDC 23.08.
- LinuxIntel_2023_xx_x.tar - Contains Blue planet platform files required for installation/upgrade.

Before you begin, verify that you have:

- A computer with web access separate from the host server where you will install UAA-RDC.
- 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 and select **Software.**
4. Select the company name from the download list and click **Proceed**.
5. In the **AVAILABLE DOWNLOADS** list, select **Blue Planet Unified Assurance and Analytics (UAA)** to download the following solutions -
    a. BPUAA_LWDC_MR2_23_08
    b. BPI_23_08
    c. LINUX_2023_xx_x
6. In the **RELEASE INFO** column, click the PDF icon to display, then save this file to your computer for future reference.
7. Retain the files in their current location. You need to transfer them to the UAA-RDC host in the next procedure: Transferring software installation files.

Transferring the Installation Files to Host

Log in to the computer where you downloaded the UAA-RDC files in the Downloading the installation files procedure.

NOTE This procedure assumes you extracted the bpi installer and the upgrade tar file into the directory listed above. If you use other directories for installation, modify the steps to point to your directories, as required.

To extract files –

1. Log in to the UAA-RDC host 0 as the bpadmin user. Do not use the site IP; use the IP address of host 0.
2. As bpadmin user, perform the following steps,
    a. the bp_uaa-remote-lwdc_23.08.00-xx.tar file to the **/opt/ciena/loads/23.08** directory.
    b. the bpi-23.08-xx.sh file to the **/home/bpadmin** directory.
    c. the LinuxIntel_2023_xx_x.tar file to the **/opt/ciena/loads/23.08** directory.

3. Extract the bp_uaa-remote-lwdc_23.08.00-xx.tar file:

```
tar -xf bp_uaa-remote-lwdc_23.08.00-xx.tar
```

The extraction creates an bp_uaa-remote-lwdc_23.08.00-xx folder containing a bp_uaa-remote-lwdc_23.08.00-xx.tar.gz.bin file and required YML files.

NOTE Do **NOT** untar the bp_uaa-remote-lwdc_23.08.00-xx.tar.gz.bin file; it will be untarred by the Blue Planet installer during installation.

4. Change to the /home/bpadmin/bpi directory:

```
cd /home/bpadmin/bpi
```

5. Record the current bpi version:

```
./bpi --version
```

In the following example, the version is recorded as 23.08-10.

```
[bpadmin@bp-prod-test-1 bpi]$ ./bpi --version
bpi version 23.08-10
ansible-playbook 2.3.0.0
config file = /home/bpadmin/bpi/ansible.cfg configured
module search path = Default w/o overrides
python version = 2.7.5 (default, Nov 1 2018, 03:12:47) [GCC 4.8.5 20150623
(Red Hat 4.8.5-36.0.1)]
[bpadmin@bp-prod-test-1 bpi]$
```

6. Enter the following command to clean up the bpi virtual environment:

```
./scripts/cleanup.sh
```

7. Change the directory to /home/bpadmin/:

```
cd /home/bpadmin
```

8. Rename the bpi directory:

```
mv bpi bpi-<version>
```

Here, version recorded in step 5.

9. Remove the old bpi installer, if it exists:

   ```
   rm bpi-<version>.sh
   ```

   Here, version recorded in step 5.

10. Extract the latest bpi version, which is transferred to **/home/bpadmin/** directory

    ```
    bash bpi-23.08-xx.sh
    ```

    The extraction creates the bpi directory for the latest bpi version.

Disabling Geographical Redundancy Configuration

To prepare for UAA-RDC upgrade, you need to disable geographical redundancy (GR) between site A (active) and site B (standby).

Use this procedure to disable GR. This procedure includes following tasks:

- Removing the standby configuration from site A (active)
- Removing the active configuration from site B (standby)
- Disabling the tunnel between site A (active) and site B (standby)

Steps

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. Change the directory to **/home/bpadmin/bpi**

```
cd /home/bpadmin/bpi
```

3. Start disabling geographical redundancy by executing the below command –

```
nohup ./bpi --remove-geored <siteB_IP_address> --playbook-args='-e geo_user=<user> -e
    geo_password=<password>' &
```

4. Fetch a valid token from tron by executing the below command *(make sure to execute the whole command in one line)* –

```
curl -sSk -X POST https://<siteA_IP_address>/tron/api/v1/tokens -d
'username=<username>&password=<password>' | python -m json.tool
```

Example

```
curl -sSk -X POST https://localhost/tron/api/v1/tokens -d
'username=admin&password=adminpw' | python -m json.tool
```

Record the token value. The token value is 825697e4c6475d0887e1 in the following example.

```
{
    "createdTime": "2021.12-24T05:47:27Z",
    "failedLoginAttempts": 0,
    "inactiveExpirationTime": null,
    "isSuccessful": true,
    "lastSuccessIpAddress": "172.16.0.1",
    "lastSuccessLogin": "2021.12-24 05:45:00+00:00",
    "loginDetail": {
        "ipAddress": "172.16.0.1",
        "sessionId": "ccd8879c-4264-4606-bb80-49e210c5c5fe",
        "sessionType": "Machine",
        "time": "2021.12-24T05:47:27Z",
        "userAgent": "curl/7.29.0"
    },
    "timeout": 86400,
    "token": "825697e4c6475d0887e1",
    "user": "7a9ca679-59f3-4c6e-a31f-1a505cf7218a",
    "userTenantUuid": "056c8d72-2e14-49e5-85c7-5e65ec086567"
}
```

5. Verify the configured remote site from site A (active) –

   ```
   curl -sSk -X GET -H 'Authorization: Bearer <token>'
   https://<siteA_IP_address>/geored/site/remotes | python -m json.tool
   ```

   Example

   ```
   curl -sSk -X GET -H 'Authorization: Bearer 825697e4c6475d0887e1'
   https://10.186.32.187/geored/site/remotes?site_id=Chennai | python -m json.tool
   ```

   The system provides the configured remote site and other information.

   ```
   {
       "message": "Listing all currently configured sites",
       "remote_sites": null,
       "success": true
   }
   ```

6. remote_sites from the above command should be reported as null as show in the system response as shown in the above example. If site B is listed under remote_sites, execute the following command to remove it from site A configuration –

```
curl -sSk -X DELETE -H 'Authorization: Bearer <token>'https://<siteA_IP_address>/geored/site/remotes?site_id=<remote_site_id>
```

7. Repeat step 5 to verify the configured remote site again. If the response is null, proceed to Activating site B (standby).

Activating Site B (standby) Optional

Before you activate site B (standby), ensure you complete the following procedure: Disabling geographical redundancy configuration.

Steps

To activate site B (standby) using Blue Planet UI, use the following:

1. Open your web browser and access the geographical redundancy window for site B (standby) by entering the following:

   `https://<siteB_IP_address>/bp-platform-ui/#/geored-ui`

2. When the dialog box displays, perform the following steps:
   a. Enter your username and password.
   b. Click Sign in. The Geographical Redundancy window displays.
   c. Verify that site B (standby) is the only site listed as standby.
   d. Click the checkbox next to the site B (standby).
   e. Click Activate.
3. Wait for site B (standby) to become fully active. This activation can take a few minutes to complete, as the process activates all applications.
4. Use Nagios to monitor the system applications on site B (standby). Wait for the status of all services to display OK (green)
   a. Open your browser and go to Nagios by entering: https://<siteB_IP_address>/nagios.
   b. Enter the Nagios username and password. The system displays the Nagios window. The Nagios dashboard displays the container status and status information.
   c. Navigate to Current Status from the list on the left and select Services.
   d. Wait for the status of all services to display OK (green).
   e. When the status of all services displays OK (green), login to the Blue Planet UI to verify that all data exists, and all applications work as expected.

Preparing Hosts for Upgrade (on site A)

This section provides information to prepare the hosts for performing upgrade. To prepare the hosts for upgrade, you need to perform the following procedures:

- Updating the hosts file
- Modifying the volume group name (Optional)
- Updating configured parameters
- Setting up users on site A (Active)
- Modifying system logging path (Optional)
- Updating Site Configuration

Updating the Hosts File

Perform the following procedure to update the hosts file parameters as per the existing, pre-upgrade UAA-RDC setup.

Requirements
Before you update the hosts file, ensure you complete the following procedure: Transferring the installation files to host.

Steps

1. Log in to host 0 as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to the **/home/bpadmin/bpi** directory.
3. Update the host or hosts in the hosts file as per the existing pre-upgrade setup. Get the hosts file:

   ```
   get-hosts-config
   ```

   Example system output:

   ```
   [bpadmin@bp-prod-test-1 bpi]$ get-hosts-config

   Host         Ip        Interface       sched_labels
   ------------------------------------------------------
   0      10.186.32.101 ens192      controller=True
   1      10.186.33.14  ens192      controller=True
   2      10.186.32.108 ens192      controller=True
   [bpadmin@bp-prod-test-1 bpi]$
   ```

4. Update `site_ip` parameter in the hosts file as per the existing pre-upgrade setup. Get the site IP details:

   ```
   get-site-ip
   ```

5. Update site_name parameter in the hosts file if it's defined on the existing pre-upgrade setup. Get the site name details:

   ```
   get-site-name
   ```

Modifying the Volume Group Name (Optional)

Blue Planet 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 UAA-RDC to create and configure the Docker thin pool. This procedure is needed if you want to change the default values.

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

NOTE | 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.

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

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

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

4. Save the all.yml file.

Updating Configured Parameters

Perform the following procedure to configure the parameters of a site. These parameters are defined in the file: **/home/bpadmin/bpi/playbooks/group_vars/all.yml**.

Requirements
Before you start updating the configured parameters, ensure you complete the following procedures:

- Renaming the bpi directory
- Updating the hosts file

Steps

1. Log in to host 0 as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to the **/home/bpadmin/bpi/playbooks/group_vars**.
3. Record the ilannet configured value:

   ```
   get-ilannet
   ```

   Example system output:

   ```
   [bpadmin@bp-prod-test-1 group_vars]$
   get-ilannet 172.28.0.0/16/24
   [bpadmin@bp-prod-test-1 group_vars]$
   ```

4. Record the siteId and siteState configured values

   ```
   cat /etc/bp2/geored/config.json | python -m json.tool
   ```

5. Open the **all.yml** file with a text editor and perform the following:
    a. Uncomment the following line and replace a.b.c.d with your license server IP address, for example:

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

    ```
    license_server:10.10.10.10
    ```

    NOTE IP address that is, 10.10.10.10 can be onxv0288.ott.ciena.com or license server IP address of the customer.

    b. Enter the `ilannet` configured value recorded in step 3.

    ```
    ilannet: 172.28.0.0/16/24
    ```

    c. Enter the geored_site_id value, recorded as the siteId configured value in

    ```
    geored_site_id: siteA
    ```

    d. Enter the geored_ site_state value, recorded as the siteState configured

    ```
    geored_site_state: ACTIVE
    ```

NOTE Setting the parameter to false requires more disk space but provides more flexibility to encounter the problems. Setting the parameter to true does not require additional disk space but limits the data recovery options. Do not set bp_upgrade_host_volume_move value in site B (standby).

    e. Save the file and exit.

Setting Up Users (Site A)

This procedure performs the following tasks:

- Manages keys of the bpadmin user
- Manages keys of the root user
- Creates the bpuser (sudo-restricted Docker install user) and manages the bpuser sudo permissions and keys. The setup script skips this step, if the bpuser is already created.

Requirements

Before setting up the users, ensure you complete the following:

- Know the bpadmin user password
- Know the bpuser password, which is provided to the bpuser

Steps

1. Log in to host 0 as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to the **/home/bpadmin/bpi** directory.
3. Start the `setup-users` script:

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

4. Enter the bpadmin user password, *if needed*.
5. Enter the bpuser user password, *if needed*.

Modifying System Logging Path (Optional)

By default, the path to the system logging (syslog) file for the UAA-RDC applications is **/var/log/ciena/blueplanet.log**. If you want to modify this path, perform the following optional procedure: To keep current release logs separate, this procedure can be followed.

Steps

1. Log in to host 0 as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to directory **/home/bpadmin/bpi/playbooks/group_vars**.
3. Update the **all.yml** file located at **/home/bpadmin/bpi/playbooks/group_vars/** by removing the commenting and editing the bp_log_file option.

   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: /var/log/Ciena
   #bp_log_file: "{{ bp_log_dir }}/bp_syslog.log"
   ```

4. Save the **all.yml** file and exit the text editor.
5. To enable changes, navigate to directory **/home/bpadmin/bpi**:

   ```
   nohup ./bpi --site lineupfile --playbook-args='--tags logging' &
   ```

Updating Site Configurations

This procedure describes how to install the Ciena Linux system bundle, PostgreSQL and license files update on an existing, pre-upgraded setup.

Requirements

Before you start to install the Ciena Linux system bundle, complete the following procedures:

- Downloading the UAA-RDC software installation files
- Transferring software installation files
- Updating the hosts file
- Setting up users on site A
- Modifying system logging path (Optional)

Steps

1. Log in to host 0 as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to **/opt/ciena/loads/23.08/**.
3. Ensure that the LinuxIntel_2023_xx_x.tar Ciena Linux bundle tar file is available in the **/opt/ciena/loads/23.08/** directory:

```
ls -lrt LinuxIntel_2023_xx_x.tar
```

4. Change the directory to /home/bpadmin/bpi:

```
cd /home/bpadmin/bpi
```

5. Select the appropriate lineup file for your deployment, lineup file to update the Ciena Linux bundle:

```
nohup ./bpi --site /opt/ciena/loads/23.08/lineupfile &
```

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

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

6. Verify the cienabundle.<DATE>.<TIME>.log located in /var/opt/ciena/logs/ directory to ensure that no errors occurred in host or hosts during the Linux bundle installation.

7. Verify the Ciena Linux bundle is updated on all hosts:

```
sudo su -

bpssh checkOSversion
```

Example system output:

```
[bpadmin@bp-prod-test-1 ~]$ sudo su -
Last login: Thu Feb 13 11:41:57 UTC 2020 on pts/0
[root@bpprodtest-1 ~]# bpssh checkOSversion host-0 ec: 0
Base Operating System Version:     Red Hat Enterprise Linux Server release 7.9 (Maipo)
                                           Oracle Linux Server release 7.9 64-bit
Operating System Bundle:                   2020.35.0
host-1 ec:                                 0
Base Operating System Version:     Red Hat Enterprise Linux Server release 7.9 (Maipo)
                                           Oracle Linux Server release 7.9 64-bit
Operating System Bundle:                   2020.35.0
host-2 ec:                                 0
Base Operating System Version:     Red Hat Enterprise Linux Server release 7.9 (Maipo)
                                           Oracle Linux Server release 7.9 64-bit
```

```
Operating System Bundle:                   2020.35.0
```

8. Verify license server configuration. It must have the same server defined earlier.

```
sudo su -

bpssh cat /etc/bp2/solutionmanager/nbis.d/licsvr.yaml
```

Example system output:

```
root@bp-prod-test-1:~# bpssh cat
/etc/bp2/solutionmanager/nbis.d/licsvr.yaml
host-0 ec: 0
url:         https://onxv0288.ott.ciena.com:7071
ip:          onxv0288.ott.ciena.com
port:        7071
publish:     true
# Created by bpi --site
host-1 ec: 0
url:         https://onxv0288.ott.ciena.com:7071
ip:          onxv0288.ott.ciena.com
port:        7071
publish:     true
# Created by bpi --site
host-2 ec: 0
url:         https://onxv0288.ott.ciena.com:7071
ip:          onxv0288.ott.ciena.com
port:        7071
publish:     true
# Created by bpi --site
```

Upgrading UAA-RDC Platform and Solution on Site A (Active)

The following table shows different UAA-RDC install options and the corresponding lineup files available –

UAA-RDC SOLUTION	LINEUP FILE NAME (SINGLE HOST)	LINEUP FILE NAME (MULTI HOST)
Remote Data Collector	lineup-uaa-remote-lwdc-single-rhel.yml	lineup-uaa-remote-lwdc-multi-rhel.yml

- **lineup-uaa-remote-lwdc-single-rhel.yml:** This lineup file is meant to install only UAA-RDC without integrators on a single host machine.
- **lineup-uaa-remote-lwdc-multi-rhel.yml:** This lineup file is meant to install only UAA-RDC without integrators on a multi host machine.

NOTE Make sure **/opt/ciena/loads/** have enough free space (Recommended 60GB).
Make sure LinuxIntel bundle, bp installer and latest UAA-RDC tar files are in the same location (host 0).

1. Log in to host 0 as bpadmin and navigate to the **/home/bpadmin/bpi** directory.
2. Execute the following command to audit solution (change the lineup file as per the requirement)

   ```
   nohup ./bpi --upgrade-audit /opt/ciena/loads/23.08/lineupfile &
   ```

   Verify the upgrade audit summary is accurate – new solution(s) and app(s) to be upgraded, etc.

3. Execute the following command to upgrade the desired solution (change the lineup file as per the requirement) –

   ```
   nohup ./bpi --upgrade-execute /opt/ciena/loads/23.08/lineupfile &
   ```

   Verify the system is in the desired state: new apps are deployed, deprecated apps are undeployed and non-upgraded apps are unaffected.

   This step is service affecting. UAA-RDC will not be available during this step.
4. Open your browser and navigate to Nagios by entering the following:

   https://<site_IP_address>/nagios

   a. Enter the host username and password. Nagios displays the current network, host, and service status.
   b. Navigate to **Current Status** from the list on the left and select **Services**.
   c. Wait for the status of all services to display OK (green).
   d. If any service displays WARNING, UNKNOWN, PENDING, or CRITICAL as a status, then resolve the issue before proceeding further.

5. Verify all data after the upgrade. If you find any issues, follow the **Backup and Restore** (**Restore** section) in the **UAA Administrator's Guide.**

6. Execute the following command to commit the desired solution (change the lineup file as per the requirement)

   NOTE Once the commit is done, the system **cannot be restored**. Make sure that the upgrade was completely successful before proceeding.

   ```
   nohup ./bpi --upgrade-commit /opt/ciena/loads/23.08/<lineup file> &
   ```

7. Proceed to Upgrading site B and setting up geographical redundancy.

Upgrading site B and setting up geographical redundancy (Automatic Procedure)

This section describes how to upgrade site B (standby) and set up a post-upgrade geographical redundancy (GR) between site A and site B.

To upgrade site B (standby) and set up a post-upgrade GR between site A and site B, you need to perform the following procedures -

- Preparing site B (standby) for upgrade
- Installing Core Platform and Extended Platform Solution on Active and Standby Sites
- Connecting site A and site B for geographical redundancy

Preparing Site B (standby) for Upgrade

This section provides a procedure to prepare site B (standby) for upgrade. You need to perform the following procedures -

- Getting site B information for upgrade
- Updating hosts file on site A (Active)
- Setting up users of site B (standby)
- Purging solutions from Site B (standby) on Pre-upgrade UAA-RDC
- Updating Site Configurations on Site B (standby)

Before you prepare site B (standby) for upgrade, ensure you complete following procedures on site A.

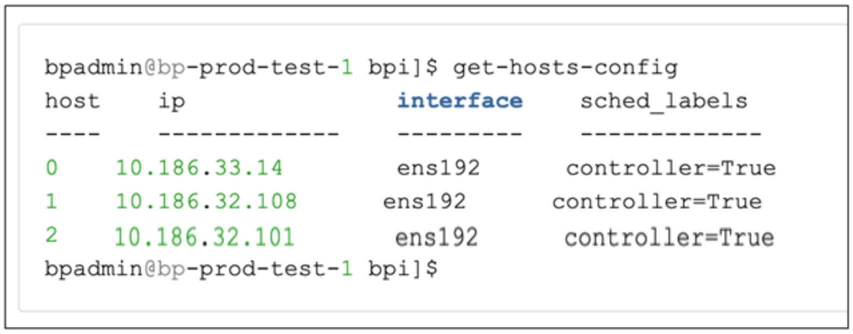
- Downloading the installation files
- Transferring software installation files

Getting Site B Information for upgrade

1. Log in to host 0 of site B (Standby) as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Get the server details of standby site and save it for later use.

   ```
   get-hosts-config
   ```

   Example

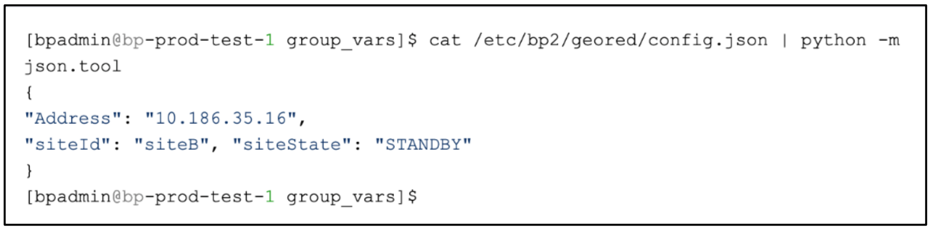
   

   ```
   bpadmin@bp-prod-test-1 bpi]$ get-hosts-config
   host    ip               interface   sched_labels
   ----    -------------    ---------   -------------
   0    10.186.33.14        ens192      controller=True
   1    10.186.32.108       ens192      controller=True
   2    10.186.32.101       ens192      controller=True
   bpadmin@bp-prod-test-1 bpi]$
   ```

3. Record the siteId and siteState configured values

   ```
   cat /etc/bp2/geored/config.json | python -m json.tool
   ```

   Example



```
[bpadmin@bp-prod-test-1 group_vars]$ cat /etc/bp2/geored/config.json | python -m
json.tool
{
"Address": "10.186.35.16",
"siteId": "siteB", "siteState": "STANDBY"
}
[bpadmin@bp-prod-test-1 group_vars]$
```

In above example, the siteId configured value is siteB and siteState configured value is STANDBY.

4. Get the ilannet information of standby site and save it for later use.

```
get-ilannet
```

Updating Hosts File on Site A (active)

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 /bpi/playbooks/group_vars and modify standby_cluster file.
3. Add ilannet information and site B information for upgrade section. geored_site_state must be STANDBY

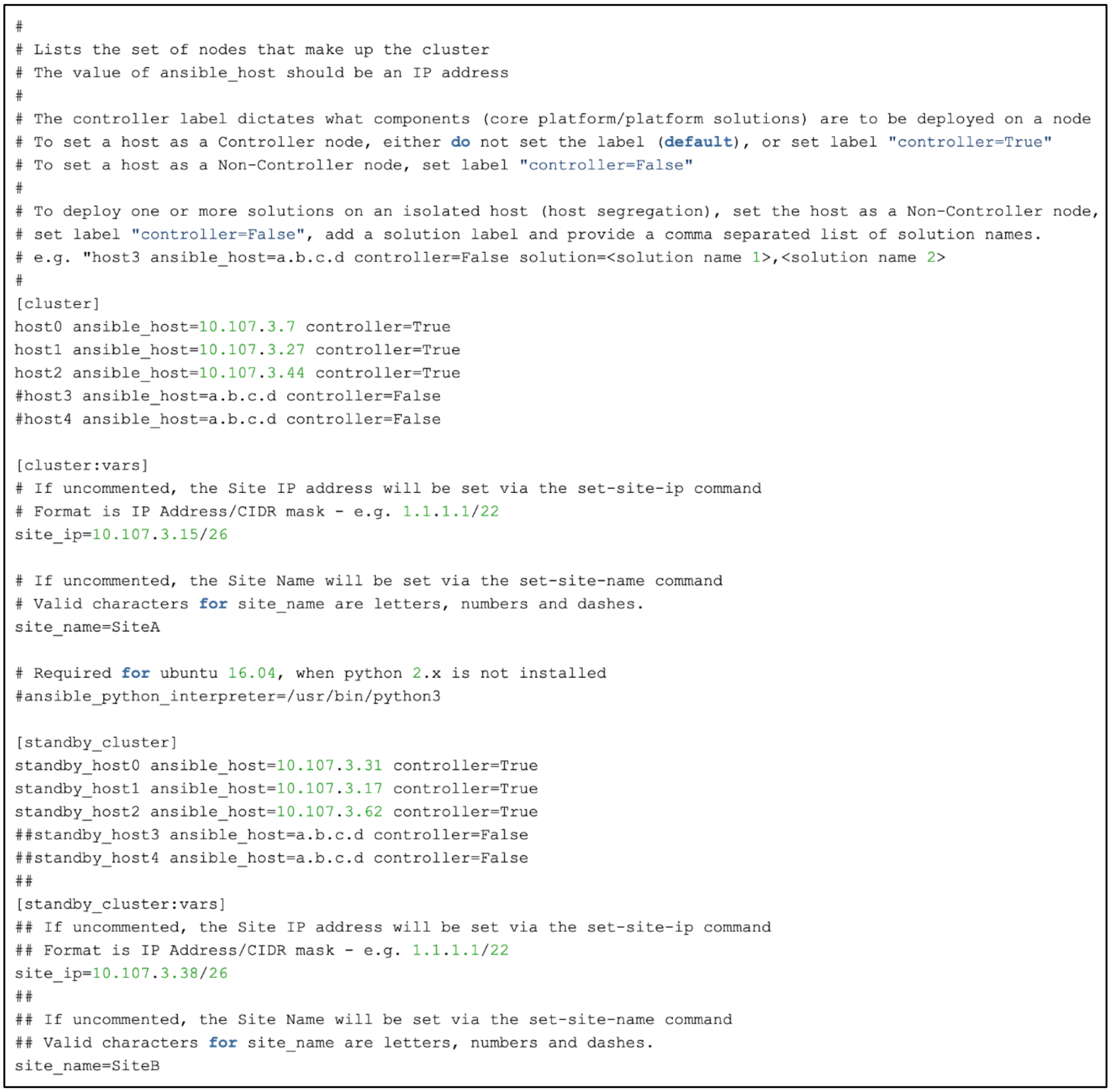
```
Ilannet: 172.XX.XX.XX/XX/XX
geored_site_id: SiteB
geored_site_state: STANDBY
```

4. Navigate to the /home/bpadmin/bpi directory.
5. Copy hosts.gr file to hosts file enter.

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

6. Open the hosts file with a text editor, add Site A (Active) hosts IP, site IP and Site B (Standby) hosts IP, site IP.

```
Following is an example of hosts file of multi-host setup on host0 of site A
```



```
#
# Lists the set of nodes that make up the cluster
# The value of ansible_host should be an IP address
#
# The controller label dictates what components (core platform/platform solutions) are to be deployed on a node
# To set a host as a Controller node, either do not set the label (default), or set label "controller=True"
# To set a host as a Non-Controller node, set label "controller=False"
#
# To deploy one or more solutions on an isolated host (host segregation), set the host as a Non-Controller node,
# set label "controller=False", add a solution label and provide a comma separated list of solution names.
# e.g. "host3 ansible_host=a.b.c.d controller=False solution=<solution name 1>,<solution name 2>
#
[cluster]
host0 ansible_host=10.107.3.7 controller=True
host1 ansible_host=10.107.3.27 controller=True
host2 ansible_host=10.107.3.44 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=10.107.3.15/26

# 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=SiteA

# Required for ubuntu 16.04, when python 2.x is not installed
#ansible_python_interpreter=/usr/bin/python3

[standby_cluster]
standby_host0 ansible_host=10.107.3.31 controller=True
standby_host1 ansible_host=10.107.3.17 controller=True
standby_host2 ansible_host=10.107.3.62 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=10.107.3.38/26
##
## 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=SiteB
```

Setting Up Users of Site B (standby)

This procedure performs the following tasks -

- Manages keys of the bpadmin user
- Manage keys of the root user
- Creates the bpuser (sudo-restricted Docker install user) manage the bpuser sudo permissions and keys. The setup script skips this step, if the bpuser is already created.
- Creates the bpmaint user which manages the bpmaint sudo permissions and keys. The setup script skips this step, if the bpmaint is already created.

Before setting up the users, ensure you complete the following -

- Perform the Updating the hosts file on site A (Active) procedure
- Know the bpadmin user password
- Know the bpuser password, which is provided to the bpuser

Steps

1. Log in to host 0 of siteA(Active) as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to the /home/bpadmin/bpi directory.
3. Start the setup-users script

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

4. Enter the bpadmin user password, if needed.
5. Enter the bpuser user password, if needed.

You will purge solutions from site B (standby) in the next procedure.

Purging solutions from Site B (standby) on Pre-upgrade UAA-RDC

Before you purge the solutions from site B (standby), ensure you complete following procedure: Setting up users of site B (standby).

Steps

1. Log in to host 0 of site A as bpadmin. Do not use the site IP; use the IP address of host 0.
2. Navigate to /home/bpadmin/bpi.
3. To purge solutions

```
nohup ./bpi --utility  playbooks/solution-undeploypurge.yml --playbook-args='--limit standby_cluster' &
```

This raises a query to the solution manager for all running solutions to purge solutions from the site and to remove related images and host volumes.

Updating Site Configurations on Site B (standby)

Before you start to install the Ciena Linux system bundle, complete the following procedures:

- Getting site B information for upgrade
- Updating the hosts file on site A (Active)
- Setting up users on site B (standby)
- Purging solutions from site B (standby) on pre-upgrade UAA-RDC

Steps

To update site configurations on site B (standby):

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. Change the directory to /home/bpadmin/bpi

```
cd /home/bpadmin/bpi
```

3. Select the appropriate lineup file for your deployment, lineup file to update the Ciena Linux bundle *(make sure to enter the whole command in one line)*

```
nohup ./bpi --site /opt/ciena/loads/23.08/<lineup file> --playbook-args='--limit standby_cluster' &
```

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

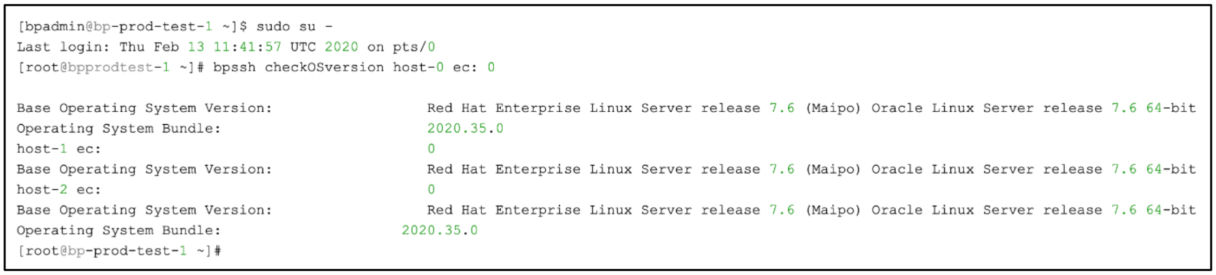
```
nohup ./bpi --site /opt/ciena/loads/23.08/<lineup file> --playbook-args='--skip-tags ntp --limit standby_cluster' &
```

4. Verify the cienabundle.<DATE>.<TIME>.log located in /var/opt/ciena/logs/ directory to ensure that no errors occurred in host or hosts during the Linux bundle installation

5. Verify the Ciena Linux bundle is updated on all hosts of Site B. Login host0 of site B then run below commands -

   ```
   sudo su –

   bpssh checkOSversion
   ```

   Example

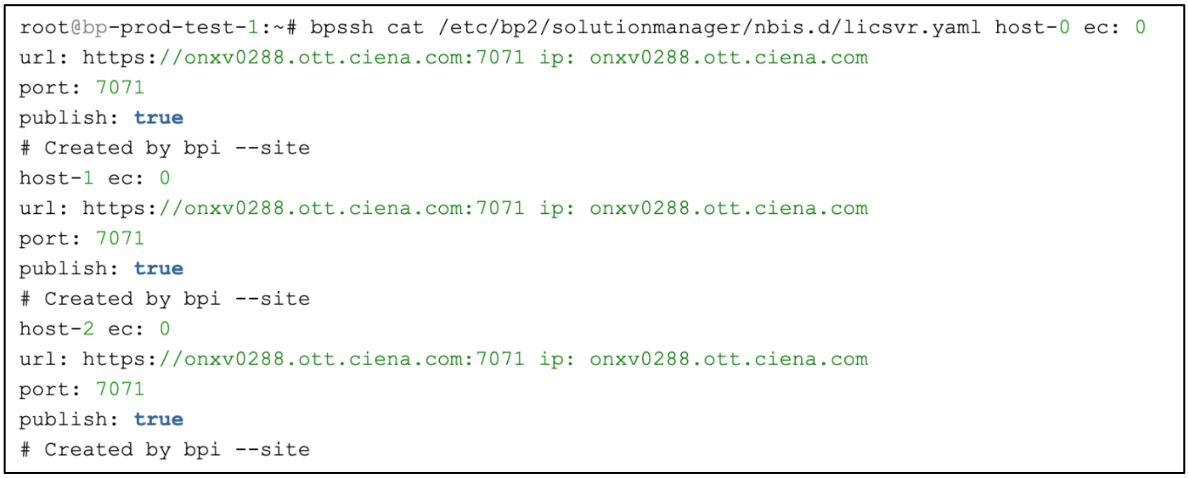


```
[bpadmin@bp-prod-test-1 ~]$ sudo su -
Last login: Thu Feb 13 11:41:57 UTC 2020 on pts/0
[root@bpprodtest-1 ~]# bpssh checkOSversion host-0 ec: 0

Base Operating System Version:                    Red Hat Enterprise Linux Server release 7.6 (Maipo) Oracle Linux Server release 7.6 64-bit
Operating System Bundle:                          2020.35.0
host-1 ec:                                        0
Base Operating System Version:                    Red Hat Enterprise Linux Server release 7.6 (Maipo) Oracle Linux Server release 7.6 64-bit
host-2 ec:                                        0
Base Operating System Version:                    Red Hat Enterprise Linux Server release 7.6 (Maipo) Oracle Linux Server release 7.6 64-bit
Operating System Bundle:                       2020.35.0
[root@bp-prod-test-1 ~]#
```

6. Verify license server configuration of site B. It must have the same server defined earlier. Login host 0 of site B, then run below commands –

   ```
   sudo su –

   bpssh cat /etc/bp2/solutionmanager/nbis.d/licsvr.yaml
   ```

   Example



```
root@bp-prod-test-1:~# bpssh cat /etc/bp2/solutionmanager/nbis.d/licsvr.yaml host-0 ec: 0
url: https://onxv0288.ott.ciena.com:7071 ip: onxv0288.ott.ciena.com
port: 7071
publish: true
# Created by bpi --site
host-1 ec: 0
url: https://onxv0288.ott.ciena.com:7071 ip: onxv0288.ott.ciena.com
port: 7071
publish: true
# Created by bpi --site
host-2 ec: 0
url: https://onxv0288.ott.ciena.com:7071 ip: onxv0288.ott.ciena.com
port: 7071
publish: true
# Created by bpi --site
```

7. If no error is reported, reboot all standby hosts.

Installing Core Platform and Platform Solution for UAA-RDC 23.08 on Site B (standby)

Before you install the core platform and platform solution, ensure you complete the following procedure: Preparing site B (standby) for upgrade.

Steps

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 the /home/bpadmin/bpi directory
3. Install the core platform and extended-platform solution for UAA-RDC 23.08 on site B (standby) –

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

Connecting Site A and Site B for Geographical Redundancy (automatic procedure)

Before you connect site A and site B for geographical redundancy, ensure you complete the following procedure -

- Complete Installing core platform and platform solution for UAA-RDC 23.08 on site B (standby) procedure.
- Have the bpadmin user password.
- Can access the /home/bpadmin/bpi directory of host 0 of active site as the bpadmin user.

Steps

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 the /home/bpadmin/bpi.
3. Start automatically geographical redundant configuration setup between active and standby sites by executing command (on single line) –

   For OS hardened servers

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

   ```
   nohup ./bpi --autoinstall-geo <lineup file> --playbook-args='--skip-tags geowhitelist --skip-tags active-install -e geo_user=admin -e geo_password=adminpw' &
   ```

   For Non-OS hardened servers

   ```
   nohup ./bpi --autoinstall-geo <lineup file> --playbook-args='--skip-tags active-install -e geo_user=admin -e geo_password=adminpw'&
   ```

4. 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
   ```

Logstash Configuration (Optional)

NOTE This step must be performed only once after upgrading to 23.08 and Logstash version is 8.x

Logstash package upgrade from v7 to v8, Elastic Common Schema (ECS) compatibility mode is enabled by default on v8. The availability of **host** field in the event input is changed accordingly. This field is required for Resource Adapter Log Translator.

The user must check whether the Logstash version is 8.x.

Steps:

To check the Logstash Version

1. Login to `uaa-logstash` container (if it is HA instance login to all the `uaa-logstash containers)`

2. Type the below command.

   ```
   versionroot@uaa-logstash:/bp2/src# logstash/bin/logstash --version

   Using system java: /usr/bin/java
   ```

   If the Logstash is for example:

   ```
   logstash 8.6.2
   ```

3. To add host field in the input by taking from the fields available as per ECS compatibility mode. The following configuration must be added as a part of filter configuration in /bp2/data/logstash-conf.conf file.

   ```
   # v7 to v8 upgrade: ecs_compatibility mode is enabled by default on v8 and the
   availablility of 'host' field in the event input got changed.
       # Added 'host' field in the event input by taking it from the fields available
   as per ECS compatibility mode.    # TCP plugin input
       if [@metadata][input][tcp][source] and ![host] {
           mutate {
               copy => {
                   "[@metadata][input][tcp][source][name]" => "[host]"
               }
           }
       }    # UDP plugin input
       if [host][ip] {
           mutate {
               copy => {
                   "[host][ip]" => "[host]"
               }
           }
       }
   ```

NOTE Follow the **Example of complete Logstash Configuration File** provided below to paste the above content in the filter plugin {}.

4. Restart the Logstash container.

   ```
   solution_app_restart artifactory.ciena.com.blueplanet.uaa_collector:23.08.XX uaa-
   logstash
   ```

Example of complete Logstash Configuration File:

```
#The changes to this configuration file should be copied to all the instances of
uaa-logstash container in case of HA
input {
    beats {
            port => 5044
            }
    tcp {
            port => 5514
            type => syslog
        }
    udp {
            port => 5514
            type => syslog
            #codec => plain {
            #   charset => "ISO-8859-1"
            # }
        }
}filter {    # Spec handling of " characters in logs. Standard escape is stripped
somewhere on the way to vsure
    # Msg shows logstash log like this     "message txt \"quoted strng\" more
message txt" (logstash log)
    # But in vsure log translator it is    "message txt "quoted strng" more
message txt" (med debug log)
    # So the mutate is required to make it "message txt \\\"quoted strng\\\" more
message txt"
    # Not sure why, but when mutate is used, actually see \\\\\"quoted
string\\\\\" in logstash log.
    # This ends up in med debug log as the desired \"quoted string\"
    mutate {
           gsub => ["message","\"","\\\""]
    }    # v7 to v8 upgrade(BPUAA -17170): ecs_compatibility mode is enabled by
default on v8 and the availablility of 'host' field in the event input got
changed.
    # Added 'host' field in the event input by taking it from the fields available
as per ECS compatibility mode.    # TCP plugin input
    if [@metadata][input][tcp][source] and ![host] {
        mutate {
            copy => {
                "[@metadata][input][tcp][source][name]" => "[host]"
            }
        }
    }    # UDP plugin input
    if [host][ip] {
        mutate {
            copy => {
                "[host][ip]" => "[host]"
            }
        }
    }}output{    file {
        path => "/bp2/log/logstash-plain.log"
        codec => rubydebug {
            metadata => true
        }
    }    kafka {
        topic_id => "com.ciena.bp.uaa.logEvents"
    bootstrap_servers => "kafka.docker:9092"
        codec =>  line { format => "{\"message\": \"%{message}\", \"ipaddress\":
\"%{host}\"}" }
    }
}
```

Creating a New Standby Site for Geographical Redundancy

After activating a Standby site during a geographical redundancy (GR) failover, use this procedure to create a new Standby site for GR (not the former Active site, referred to in the Activating a Standby site for a geographical redundancy failover procedure).

If you want to reuse the former Active site, then go to the Restoring the former Active site as the new Standby site.

Cleaning up Old Georedundancy Settings

1. Clean up tunnel configuration on the new Active site, run the following command on host0 of new active site as a **bpadmin** user –

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

2. Clean up geored configuration files –
   a. Delete contents of the /etc/bp2/site/bpfirewall.conf file on the new active site –

      ```
      sudo bpssh "sudo truncate -s 0 /etc/bp2/site/bpfirewall.conf
      ```

   b. Delete the /etc/ipsec.d/GeoRed-*.conf files on all hosts of the new active site –

      ```
      sudo bpssh "rm -f /etc/ipsec.d/GeoRed-*.conf"
      ```

To set up a new Standby site, complete the following procedures available in the Blue Planet UAA-RDC Installation Guide.

- Creating the bpadmin user
- Configuring the Security-Enhanced Linux mode and disabling firewalld
- Downloading and installing the Ciena Linux system bundle
- Downloading software files for UAA-RDC installation

After the above procedures are completed, follow the below mentioned procedures to complete setting up the Standby site from the Active site –

- Updating hosts file
- Modifying the volume group name
- Configuring a time source
- Configuring geographical redundancy
- Configuring the Blue Planet email service
- Modifying the ILAN NET interface
- Modifying the Default UAA-RDC Interface
- Specifying the external license server
- Setting up users
- Validating the hosts
- Configuring UAA-RDC Hosts on Active and Standby Sites
- Installing Core Platform and Extended Platform Solution on active and standby sites
- Installing UAA-RDC and Configuring Georedundancy on Active and Standby Sites (automatic procedure)

Updating Hosts 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.
2. Navigate to /home/bpadmin/bpi.
3. Add the standby section on hosts file –

```
# StandBy Cluster Details
#
#Lists the set of nodes that make up the cluster
#The value of ansible_host should be an IP address
#
#The controller label dictates what components (core platform/platform solutions) are to
be deployed on a node
# To set a host as a Controller node, either do not set the label (default), or set label
"controller=True"
# To set a host as a Non-Controller node, set label "controller=False"
#
#To deploy one or more solutions on an isolated host (host segregation), set the host as a
Non-Controller node,
# set label "controller=False", add a solution label and provide a comma separated list of
solution names.
# e.g. "host3 ansible_host=a.b.c.d controller=False solution=<solution name 1>,<solution
name 2>
#
#
[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
#
#Required for ubuntu 16.04, when python 2.x is not installed
#ansible_python_interpreter=/usr/bin/python3
```

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=10.186.34.246 controller=True
host1 ansible_host=10.186.33.108 controller=True
host2 ansible_host=10.186.32.60 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=10.186.35.15/22
# StandBy Cluster Details
##
[standby_cluster]
standby_host0 ansible_host=10.186.34.235 controller=True
standby_host1 ansible_host=10.186.32.44 controller=True
standby_host2 ansible_host=10.186.33.120 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
#
#Required for ubuntu 16.04, when python 2.x is not installed
#ansible_python_interpreter=/usr/bin/python3
```

4. Save the hosts file.

Modifying the Volume Group Name

Blue Planet 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 UAA-RDC to create and configure the Docker thin pool.

NOTE

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 UAA-RDC installation.

You might not need to 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 UAA-RDC interface.

Before you begin, verify that you -

1. Know the name of the volume group where the unallocated physical extents (PE) space is available for UAA-RDC to create and configure the Docker thin pool.

   NOTE 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 the /home/bpadmin/bpi/playbooks/group_vars directory.
2. Using a text editor, open the standby_cluster file.
3. 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

UAA-RDC hosts can use a local or remote time source. For example -

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

NOTE 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 UAA-RDC host, skip this procedure.

By default, the UAA-RDC 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 UAA-RDC 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.

NOTE 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 checkclockdrift commands to check UAA-RDC timing synchronization.

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

All UAA-RDC 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 the Updating 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 standby_cluster file.
3. 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
```

4. If you are working with only local time source, go to step 10. If not, go to step 7.
5. Using a text editor, open the standby_cluster file.
6. 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 UAA-RDC host timing source in standby site.

   Save the standby_cluster 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>
```

   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
```

   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:
- 0.10.128.8.89
```

7. 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 standby_cluster and save the file.

Configuring Geographical Redundancy

This section describes the configuration of geographical redundancy functions which are given below. These parameters need to be configured in 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 You can use letters, numbers, underscores and, dashes and must be at least 3 characters in length to define it.

NOTE

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.

NOTE

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. If it is set to false, nagios checks will not be verified for active and standby sites during auto GR configuration setup.

Requirements

Before you begin this procedure, verify that you -

- Completed the Updating 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 the /home/bpadmin/bpi/playbooks/group_vars directory.
2. Using a text editor, open the standby_cluster file.
3. 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.

Configuring the Blue Planet email Service

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

NOTE

If password expirations are enabled and the SMTP server is not configured, users will not be able to log in after their password expires. Blue Planet 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.

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

Before you begin this procedure, verify that you -

- Completed the Updating 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 the /home/bpadmin/bpi/playbooks/group_vars directory.
2. Using a text editor, open the standby_cluster file and edit the SMTP parameters mentioned in table SMTP parameters. Save the standby_cluster file.

ISSUE	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 /bp2/src/static. 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 smtp.gmail.com or, if
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

UAA-RDC 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 UAA-RDC 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 the Updating hosts file procedure.
- 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 standby_cluster file.
3. Uncomment the ilannet option, then enter the IP network address you want UAA-RDC 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
   ```

NOTE 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 UAA-RDC Interface

By default, UAA-RDC 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 the Updating hosts file procedure.

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

To modify the default UAA-RDC 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 standby_cluster file.
3. 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
   ```

4. 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 the Updating hosts file procedure.

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 standby_cluster 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.
5. 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 thi step if you have previously manually created the bpuser user.

Before you begin this procedure, verify that you -

- Completed the Updating 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.

   NOTE 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.

Validating the Hosts

This procedure verifies that the host hardware and software where you will install the UAA-RDC meet Blue Planet requirements. The validation is based upon requirements described in the Hardware and software requirements chapter.

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.

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

   where,

   <profile> is the validation profile. Possible values are: uaa-dev (lab environment) or uaa-prod (production environment).
3. If prompted, enter the bpadmin user password.

   NOTE 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 UAA-RDC Hosts on Active and Standby Sites

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

Configuring the UAA-RDC 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 UAA-RDC 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 Site A (active site) 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 UAA-RDC host timing, add the playbook arguments shown in step 2.

To configure the UAA-RDC 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.

```
nohup ./bpi --site <lineup file> --playbook-args='--limit standby_cluster' &
```

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

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

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

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 the Configuring UAA-RDC 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 UAA-RDC 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 UAA-RDC 23.08 on standby site by entering (on a single line)

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

If all elements display a Passed status and "failed=0" at the end of the summary, continue with Installing UAA-RDC and configuring georedundancy on active and standby sites (automatic procedure).

Installing UAA-RDC and Configuring Georedundancy on Active and Standby Sites (automatic procedure)

Complete this procedure to install UAA-RDC 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 UAA-RDC 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 the Installing Core Platform and Extended 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.

To install UAA-RDC 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:

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

```
nohup ./bpi --autoinstall-geo <lineup file> --playbook-args='--skip-tags geowhitelist --
skip-tags active-install -e geo_user=admin -e geo_password=adminpw' &
```

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 -

```
nohup ./bpi --autoinstall-geo <lineup file> --playbook-args='--skip-tags active-install -e
geo_user=admin -e geo_password=adminpw' &
```

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 Blue Planet 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. Verify the system health by logging into Nagios for both active and standby sites.

   ```
   https://<active_site_IP_address>/nagios
   ```

   ```
   https://<standby_site_IP_address>/nagios
   ```

NOTE Ignore the containers showing an Unknown status. Nagios can take up to 30 minutes to display the status of all services as GREEN.

Revert Override Configuration in Postgres

To revert override configuration in postgres -

1. 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).
2. Remove /etc/bp2/bpopg/overrides.json.
3. Delete monitor_task_startup_wait_time_in_mins entry from the /etc/bp2/postgres/overrides.json file.
4. Confirm that you have the right json in these files by running the following command –

   ```
   cat /etc/bp2/postgres/overrides.json | python -m json.tool
   ```
   This command should not return an error, it will display the JSON content.
5. Execute the below command to sync it to all hosts –

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

Contacting Blue Planet

Blue Planet Division Headquarters	7035 Ridge Road Hanover, MD 21076 +1 800-921-1144
Blue Planet Support	https://www.blueplanet.com/support
Sales and General Information	https://www.blueplanet.com/contact
Training	https://www.blueplanet.com/learning

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.

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.

Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.