DCA AGNI 200

Setup and Access Guide
CloudVision AGNI

Version 1.0

Arista.com

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA +1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2026 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

Chapter 1: Introduction....1
1.1 Prerequisites for Installing DCA AGNI 200....1
1.2 Rack Mounting the Appliance....3
1.3 Configuring the iDRAC....3

Chapter 2: Post Installation - AGNI Setup....4
2.1 Account Confirmation in Arista Cloud for AGNI....4
2.2 Login Credentials....5
2.3 Checking Time Synchronization....6
2.4 Updating the CLI....6
2.5 Bootstrap Configuration....7

Chapter 3: Cluster Configuration....13
3.1 Principal Node Setup....13
3.2 Joining other nodes to cluster....13
3.2.1 Standby and Auxiliary Node Setup....14
3.3 Uploading the Certificates....15
3.3.1 Uploading SSL Signed Certificate for UI....15
3.3.2 Uploading Custom EAP Server Certificate....18
3.4 Modifying the Cluster....18
3.4.1 Removing Nodes from the Cluster....19

Chapter 4: Organizational Login Activities....24
4.1 Local User Login....24
4.2 IDP Admin User Login....26
4.3 Local Account User Creation....26
4.4 API Token Generation....27

Chapter 5: Maintaining the Cluster....29
5.1 Managing and Monitoring the Cluster from the UI....29
5.2 AGNI Backup Operation....33
5.3 AGNI Restore Command....35
5.4 Restarting the cluster....38
5.5 Reboot Command....39
5.6 Shutdown Command....39

Chapter 6: AGNI Node Replacement (RMA)....40

Chapter 7: FAQs and Troubleshooting....41
7.1 How to synchronize time on an AGNI node?....41
7.2 Error During Bootstrapping Due to Incorrect Docker Version....42

Chapter 1

Introduction

This document provides information for adequately trained service personnel and technicians installing and configuring the Arista CloudVision AGNI (DCA-AGNI-200) Appliance.

1.1 Prerequisites for Installing DCA AGNI 200

- Configure the switch with the required VLANs before mounting the AGNI appliances to the rack.
- Have separate (different) IP addresses for Admin and Data interfaces:

Table 1: Interfaces and Services

Interface	Services
Admin(NIC1)	RADIUS, CLI, Replication, TACACS+, HTTPS for UI
Data(NIC2)	3rd Party Integrations, HTTPS, RADIUS, RadSec, TACACS+

- Static IP addresses:
  - Admin Interface (mandatory) - eno16895 (acts as a Management interface)
  - Data Interface (optional) - eno16905 (acts as a Data interface)



Note: The IP addresses of the Admin Interface and Data Interface should be from different Subnets.

For details, see the DCA-AGNI-200 Quick Start Guide, rear panel indicators.



Note: When you configure a **Data Interface**, it serves as the outgoing interface and the default gateway for the node. If you don't configure the data interface, the admin interface acts as the default gateway. You can verify this using the `ip route` command.

- Create **DNS entries** for the hostname FQDNs to assign to AGNI nodes.

  AGNI uses DNS to communicate with other nodes and to register with Arista Cloud. DNS is the preferred method over IP addresses; you must configure it before bootstrapping.

- The node should have connectivity to the Internet with the following allowed URLs in the firewall:

Table 2: Allowed URLs

Serial Number	URL	Notes
1	mc.ag03s01.onprem.agni.arista.io	AGNI region-specific URLs. Use one of the URLs corresponding to the customer region.
	mc.ag01c01.onprem.agni.arista.io	
	mc.ag02w03.onprem.agni.arista.io	
	mc.ag04s01.onprem.agni.arista.io/	
2	oauth2.googleapis.com	OAuth 2.0 authorization endpoint for on-premises accounts.
3	storage.googleapis.com	AGNI on-premises platform installation endpoints
4	serviceusage.googleapis.com	
5	iam.googleapis.com	
6	cloudresourcemanager.googleapis.com	
7	gkehub.googleapis.com	
8	compute.googleapis.com	
9	gcr.io	
10	logging.googleapis.com	
11	monitoring.googleapis.com	
12	servicecontrol.googleapis.com	
13	gkeconnect.googleapis.com	
14	us-docker.pkg.dev	
15	us-west2-docker.pkg.dev	
16	asia-south1-docker.pkg.dev	



Note: The node establishes a control channel with Arista Cloud for management and troubleshooting. This channel allows the **Arista SRE** to monitor the appliance's health. Therefore, the node needs outbound Internet connectivity to operate.

- Open the AGNI ports in the firewall for the SRE and Clustering traffic:

  Table 3: Port Details in AGNI

Service	Protocol	port
RADIUS	UDP	1645,1646,1812,1813
RadSec	TCP	2083
CoA	UDP	3799, 1700
TACACS+	UDP	49
Replication	TCP	5432 (not required to be externally available, only used by other AGNI nodes)
UI Access	HTTPS	443
3rd Party Integration	HTTPS	443 (for incoming notifications)
SSH	TCP	22
SRE Access	HTTPS	443
Syslog	TCP/UDP/TLS	601

- NTP server:

  Many AGNI operations rely on time synchronization. Configuring the NTP server and synchronizing the node time is mandatory.

- Customer account provisioning:

  The **Arista SRE** completes this process before the customer receives the appliance. Ensure you have your account details ready, as the bootstrapping process prompts for this information. Work with your account team if the SRE has not yet completed this process.

- Email address (individual or group):

  AGNI sends your login credentials, password tokens, and update details to your registered email address. The bootstrapping process will prompt you for this, so provide an email address you can access during bootstrapping.

1.2 Rack Mounting the Appliance

Rack-mount the AGNI server using the sliding rack-mounting rails. For details, see the QSG for DCA-AGNI-200 on the Arista Product Documentation page under the *CloudVision Appliance* table.

1.3 Configuring the iDRAC

Configure the Integrated Dell Remote Access Controller (iDRAC) interface on the CloudVision AGNI Appliance. For details, see the QSG for DCA-AGNI-200 on the Arista Product Documentation page under the *CloudVision Appliance* table.

Chapter 2

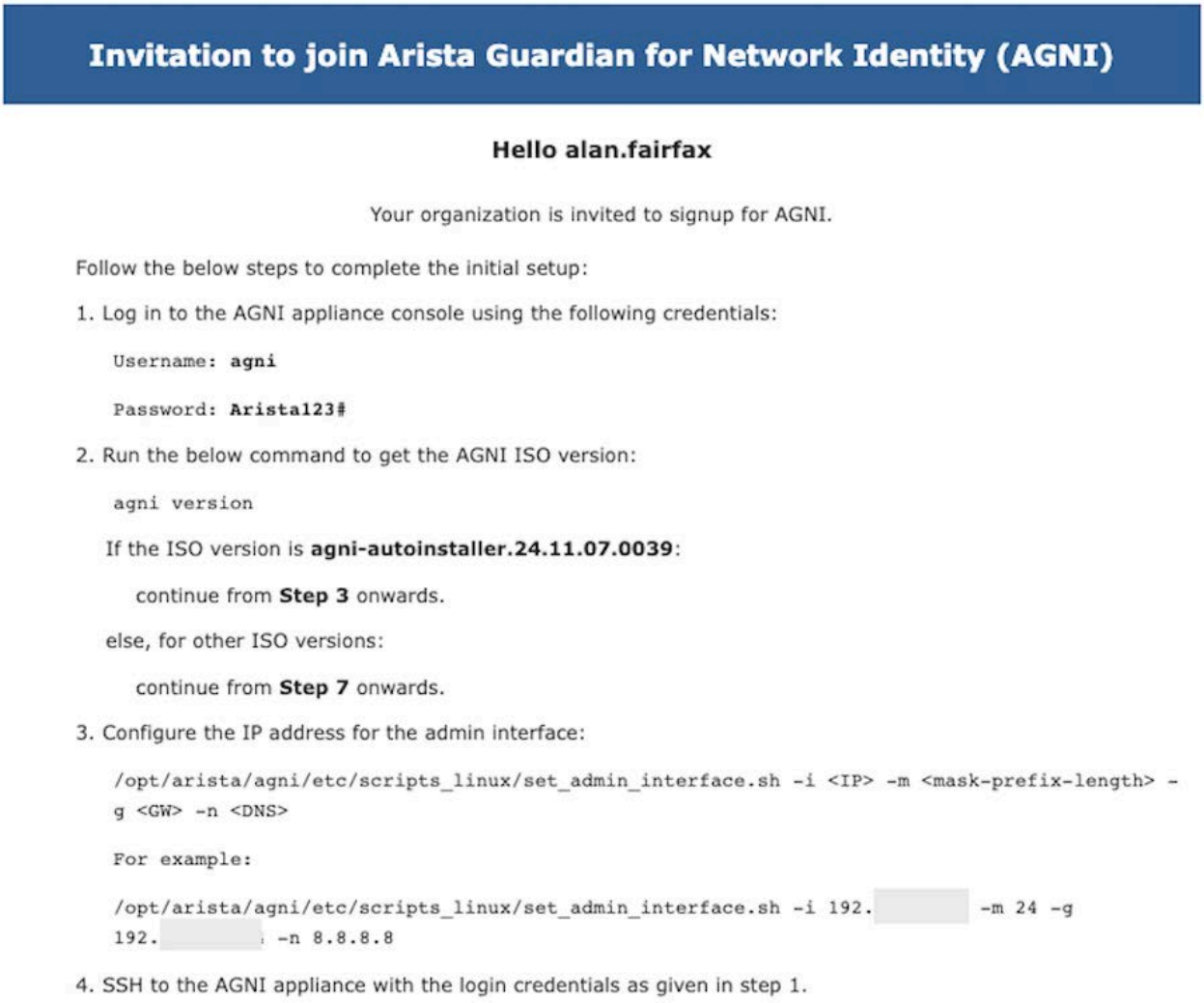
Post Installation - AGNI Setup

This section describes the set up and configuration details after installing the DCA-AGNI-200 appliance.

2.1 Account Confirmation in Arista Cloud for AGNI

After the AGNI Cloud team receives a request from the field, they create an Arista Cloud account for AGNI and email the next steps for registering and configuring AGNI to your registered email address.

Figure 2-1: Sample Invite Email to Join AGNI



Invitation to join Arista Guardian for Network Identity (AGNI)

Hello alan.fairfax

Your organization is invited to signup for AGNI.

Follow the below steps to complete the initial setup:

1. Log in to the AGNI appliance console using the following credentials:

   Username: **agni**

   Password: **Arista123#**

2. Run the below command to get the AGNI ISO version:

   `agni version`

   If the ISO version is **agni-autoinstaller.24.11.07.0039**:

   continue from **Step 3** onwards.

   else, for other ISO versions:

   continue from **Step 7** onwards.

3. Configure the IP address for the admin interface:

   `/opt/arista/agni/etc/scripts_linux/set_admin_interface.sh -i <IP> -m <mask-prefix-length> -g <GW> -n <DNS>`

   For example:

   `/opt/arista/agni/etc/scripts_linux/set_admin_interface.sh -i 192. -m 24 -g 192. -n 8.8.8.8`

4. SSH to the AGNI appliance with the login credentials as given in step 1.

5. If you use HTTP Proxy, run one of the following commands:

   Proxy without authentication:

   ```
   export https_proxy=http://<PROXY-IP>:<PROXY-PORT>
   ```

   Proxy with authentication:

   ```
   export https_proxy=http://<USERNAME>:<PASSWORD>@<PROXY-IP>:<PROXY-PORT>
   ```

6. Copy the below command and paste it into the SSH terminal and run it:

   ```
   wget -qO - https://mc.dev.agnieng.net/api/mc.onPrem.preUpdate.pkg.download?token=CiQAEEF1SG
   MLLmCysuHeVOJvKUOAAjAzBy7EQlqXjKhoYChDwe2GkIu%2BWFZUSA7RL9I3nEPf09dcL | bash
   ```

   The command will expire at 19 May 26 09:07 UTC.

7. Run the below command to bootstrap the AGNI appliance:

   ```
   agni bootstrap
   ```

8. To create a new cluster, run the below command:

   ```
   agni setup
   ```

   Alternatively, to join to an existing cluster, run the below command:

   ```
   agni join
   ```

Note: For help regarding the AGNI CLI, use the command '`agni -h`'

This is an automated email notification. Please do not reply to this message.

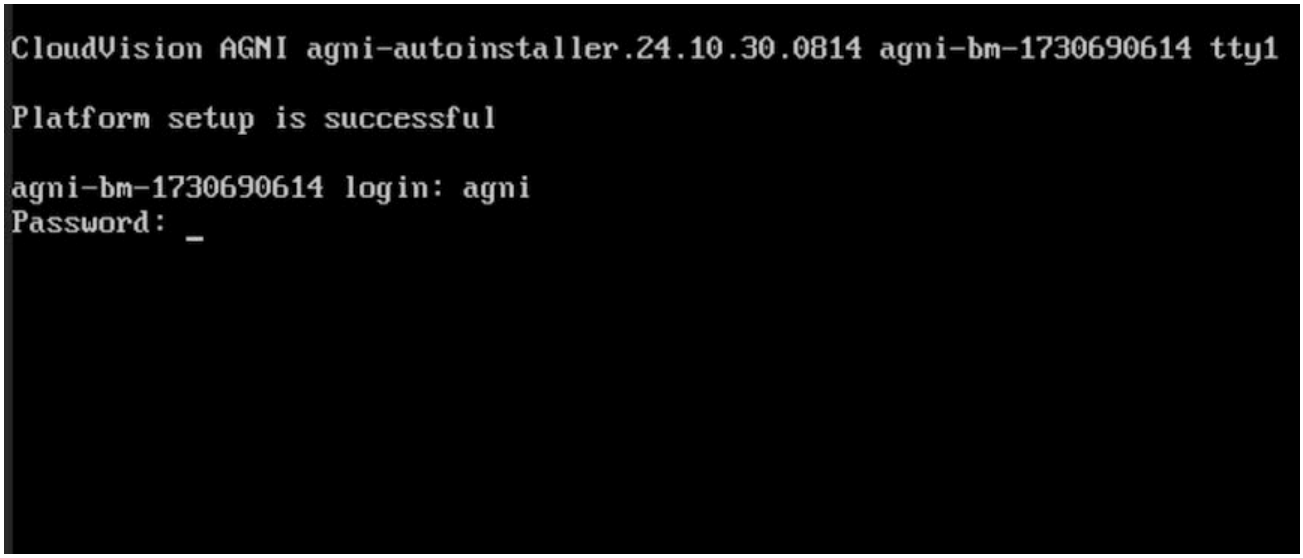
2.2 Login Credentials

The default credentials for the AGNI appliance nodes are:

- Username: **agni**
- Password: **Arista123#**

You can log in through the appliance console, iDRAC console, or SSH (after bootstrapping). To change the login password, follow the bootstrapping process.

Figure 2-2: Login Credentials



2.3 Checking Time Synchronization

Check if NTP server is synchronized or not by using the command `timedatectl status`.

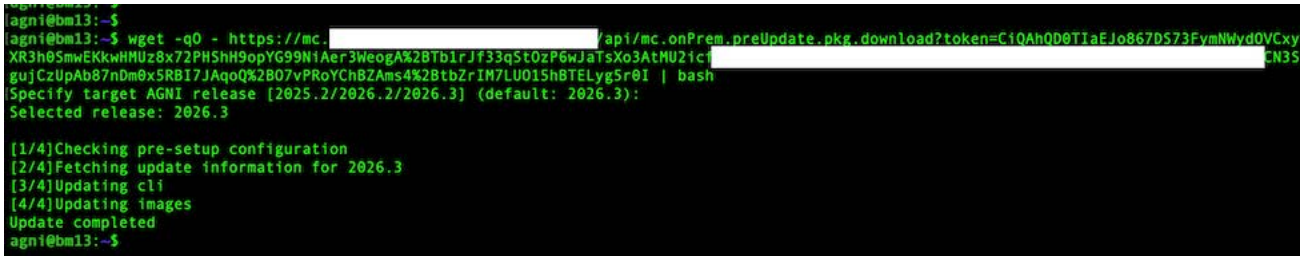
```
timedatectl status
               Local time: Wed 2026-01-07 06:38:15 UTC
           Universal time: Wed 2026-01-07 06:38:15 UTC
                 RTC time: Wed 2026-01-07 06:38:15
                Time zone: UTC (UTC, +0000)
System clock synchronized: no
              NTP service: active
          RTC in local TZ: no
```

If the system clock is not synchronized, then refer to the FAQ and Troubleshooting section.

2.4 Updating the CLI

Follow the instructions in your email and execute the `wget` command to download the latest version of the CLI before bootstrapping. After the CLI is updated, follow the bootstrap and set up commands to proceed with the cluster configuration.

Figure 2-3: WGET Command Output



2.5 Bootstrap Configuration

agni bootstrap—This command helps you configure the appliance with its system and network information, which completes the bootstrapping process. After you finish this step, the system will become accessible over the network and ready for set up.

In an enterprise environment, users on isolated networks typically have restricted Internet access. To reach external services, they must rely on HTTP proxy servers, which can be authenticated or unauthenticated.

AGNI appliances are generally deployed within these restricted networks. Because of this, they may not have direct Internet access depending on the set up. In such cases, you must configure AGNI appliances to use an HTTP proxy to access internet-hosted services.

The HTTP proxy feature is available from AGNI version P-2025.2.0 onwards.

Note: You can only set up an HTTP proxy server during the initial AGNI appliance set up. You cannot change these settings later. Because of this, you must decide whether to use an HTTP proxy before you set up the AGNI appliance. If you want to change the settings later, reset the appliance to its factory default and make your configuration changes.

AGNI uses several default networks for Docker and internal cluster communication. If any of these networks conflict with the customer's existing network, the default AGNI network can be changed as part of the bootstrap command. This feature is available from AGNI version P-2026.2.0 onwards.

Run the `agni bootstrap` command and enter the required details at the prompts (see image):

Figure 2-4: Bootstrap without HTTP Proxy

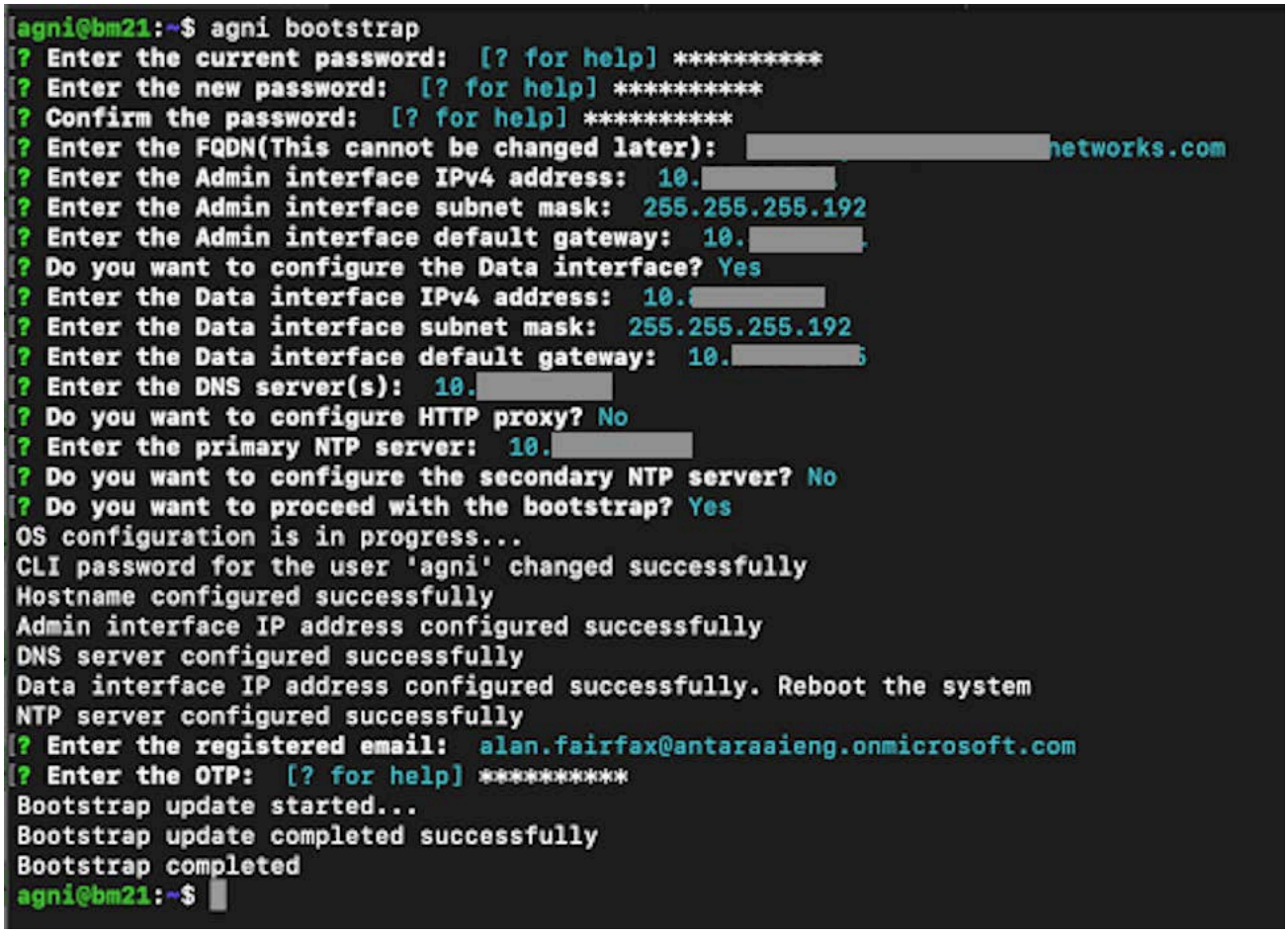


Figure 2-5: Bootstrap with Authenticated HTTP Proxy

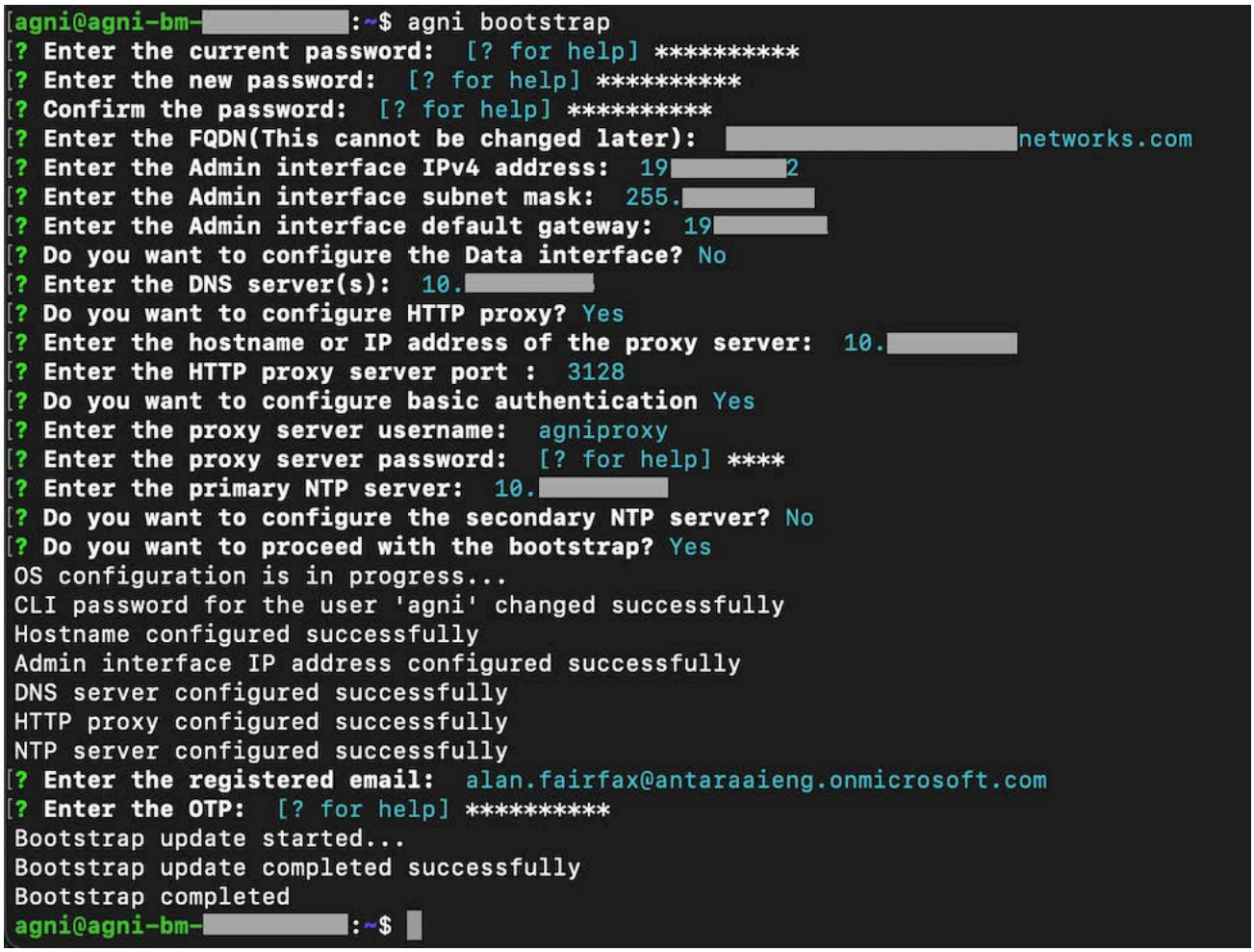


Figure 2-6: Bootstrap with Unauthenticated HTTP Proxy

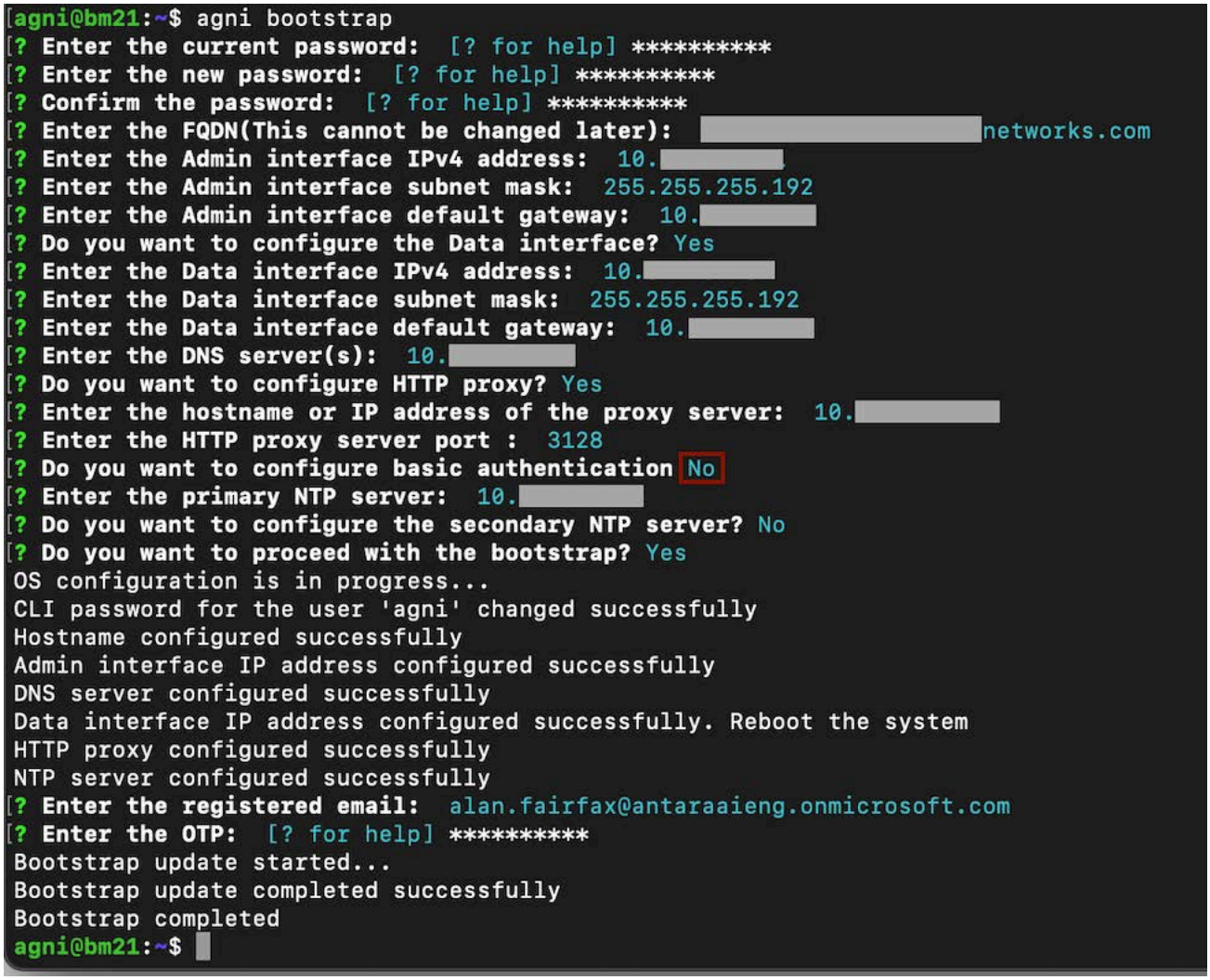
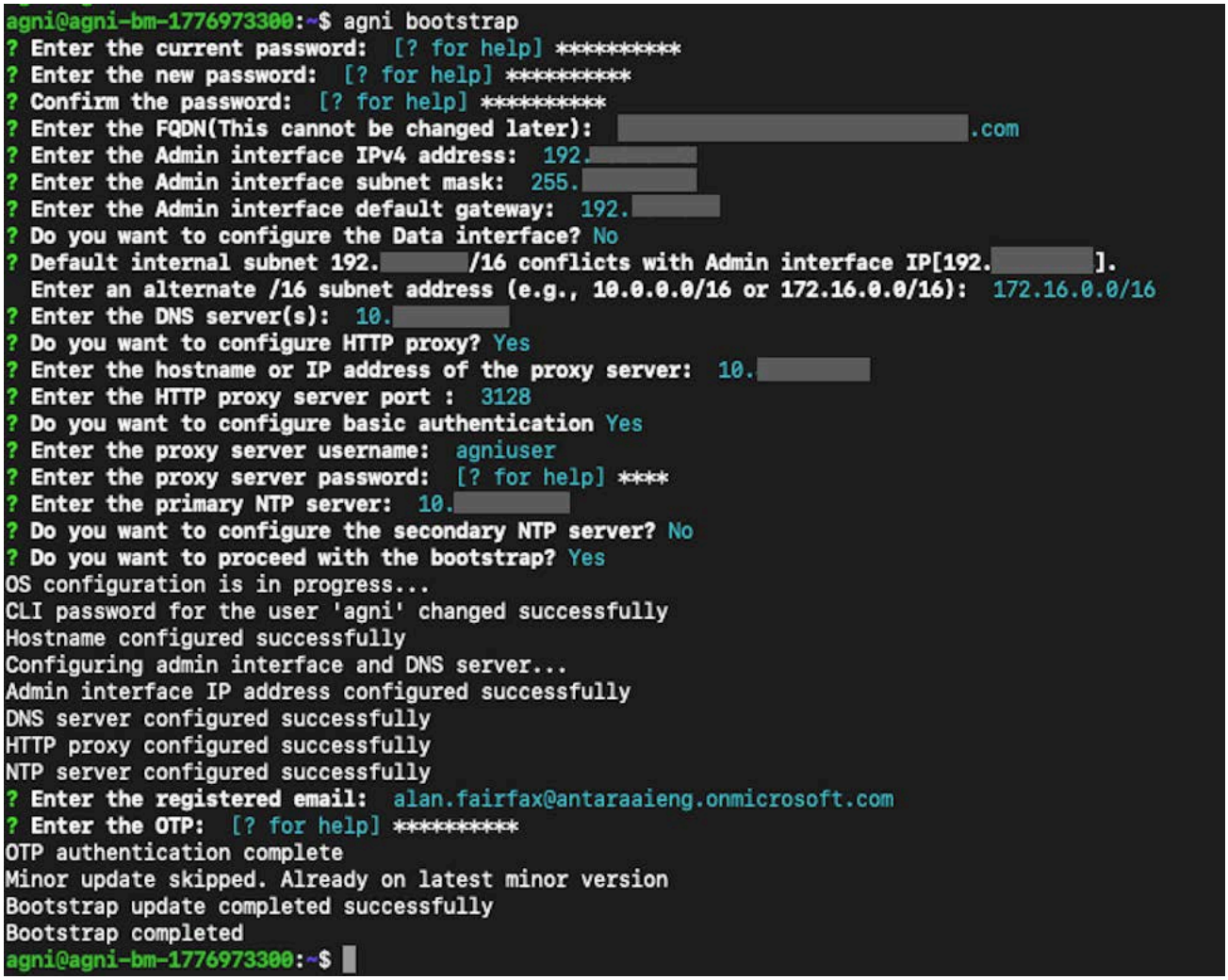


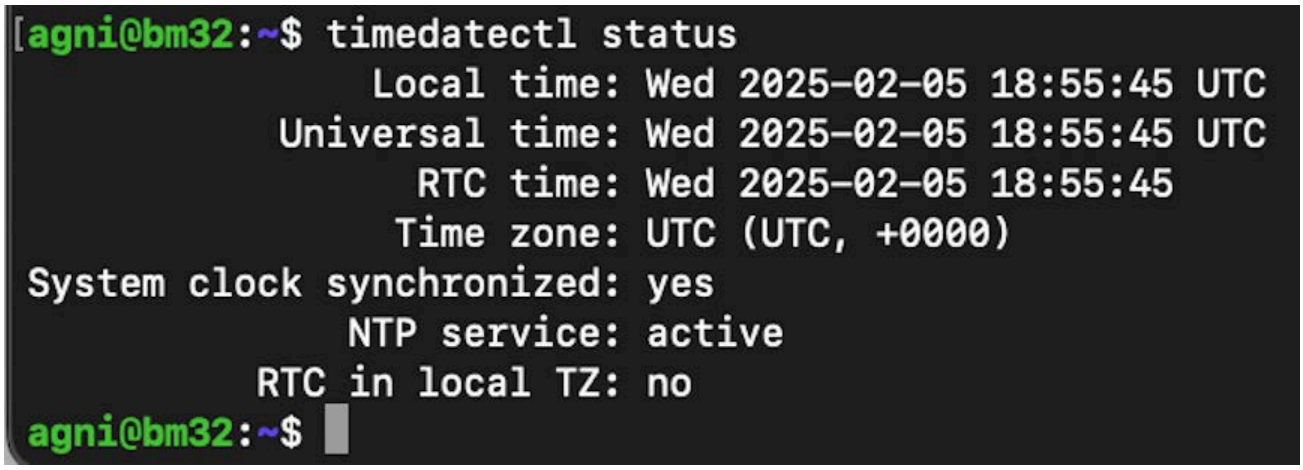
Figure 2-7: Bootstrap with Default network change



Post-Bootstrap Validations

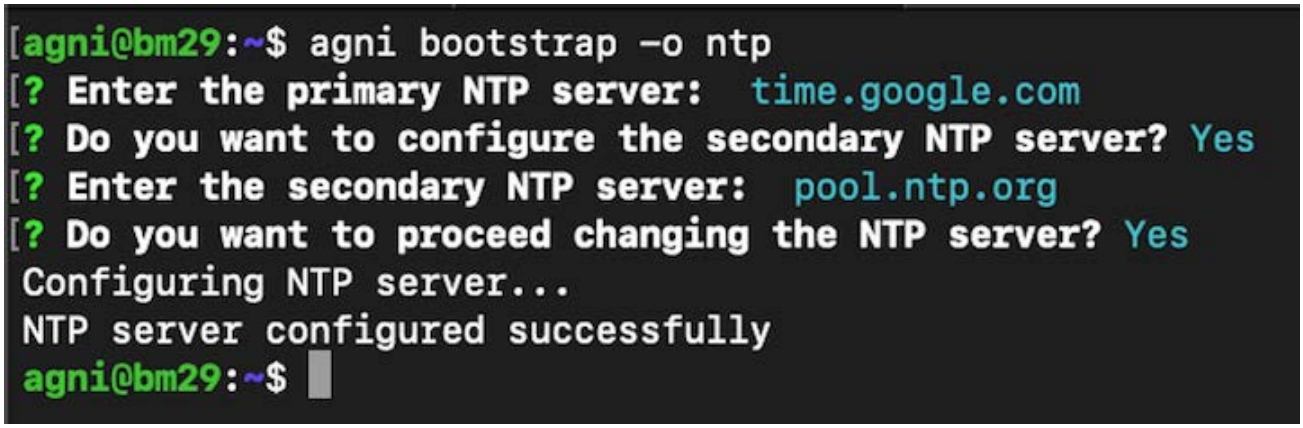
Note: To ensure Network Time Protocol (NTP) is synchronized, run `timedatectl status` command after completing the `agni bootstrap` command.

Figure 2-8: NTP Synchronization



If NTP is not synchronized, run the `agni bootstrap -o ntp` command and provide the correct NTP server.

Figure 2-9: NTP Synchronization (when not synched)



DNS and Networking Validations

Ensure that DNS and the default gateway are successfully configured. Try reaching internal hosts as well as external entities using the `ping`command. For example:

```
agni@bm18:~$ ping www.arista.com
agni@bm18:~$ ping www.google.com
PING www.google.com (172.217.12.100) 56(84) bytes of data.
64 bytes from sfo03s33-in-f4.1e100.net (172.217.12.100): icmp_seq=1 ttl=115 time=10.3 ms
```

Chapter 3

Cluster Configuration

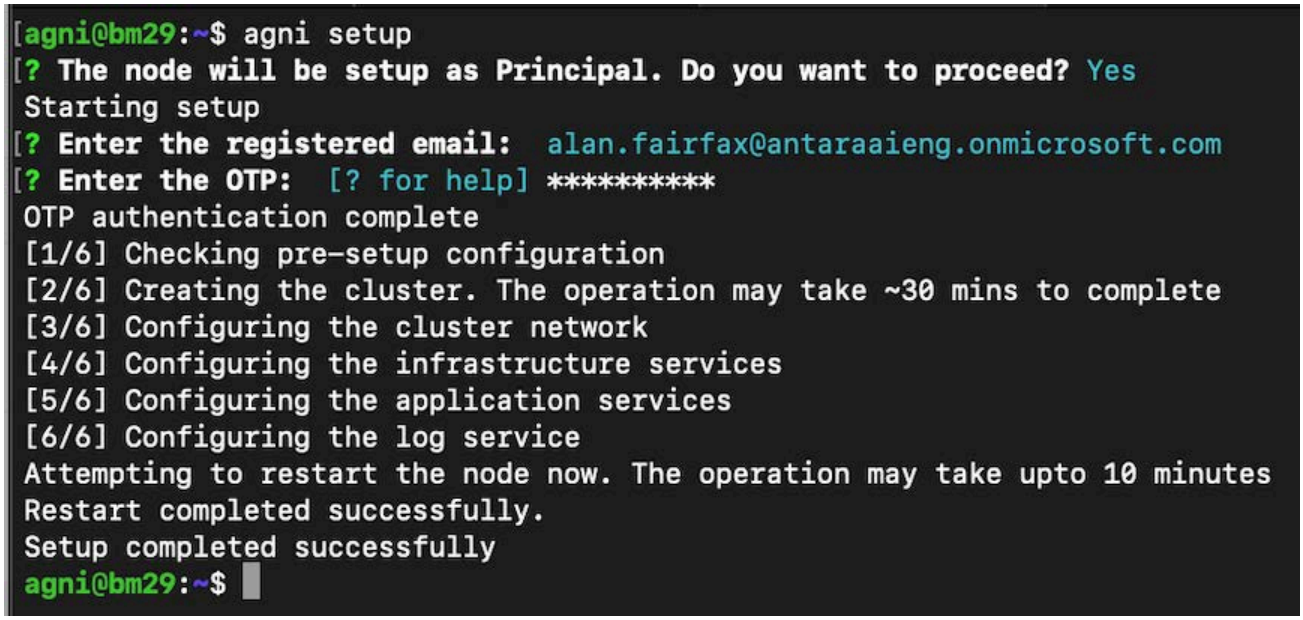
Configure AGNI appliances in the cluster to achieve load balancing and high availability. There are multiple flavors of AGNI clusters. To decide the cluster size and type, see the CloudVision AGNI Design Guide on the Arista website.

3.1 Principal Node Setup

`agni setup` - This command helps you (the administrator) to set up AGNI node as the *Principal* node (primary node) in an AGNI cluster. Only one node can act as the *Principal* node.

Enter the `registered email` address to identify the node and the cluster, followed by the received `OTP`. The set up process takes approximately 30 minutes to complete. After it finishes, AGNI will be set up and operational.

The Administrator will receive a **User Registration** email to the registered email address, containing the credentials to log in to the AGNI UI. You must log in to the AGNI UI and change the password.



3.2 Joining other nodes to cluster

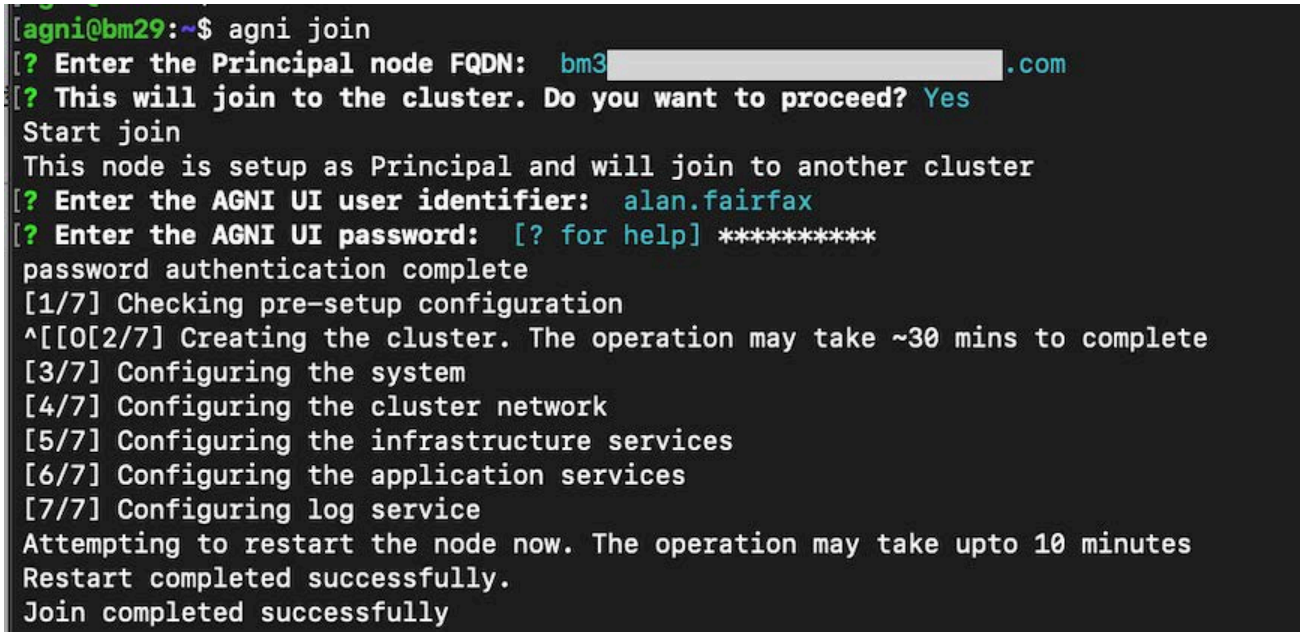
After configuring the Principal node, add multiple nodes into that cluster using the `agni join` command. You can add one node as a *standby* node and can add several *auxiliary* nodes.

3.2.1 Standby and Auxiliary Node Setup

`agni join` - This command helps you set up AGNI nodes as *Standby* or *Auxiliary* nodes. Only one node acts as a Standby node in the AGNI cluster. There can be multiple Auxiliary nodes. The first node that joins the Principal node becomes the Standby node, and the following nodes become Auxiliary nodes. The `agni join` command requires information about the:

- Principal node host FQDN
- Admin credentials of the Principal node. Refer to the Local User Login section for admin credentials.

This operation takes about 30 minutes, after which the current AGNI node will be clustered.



The `agni join` command is now prevented if the new joining node is on a different version than that of the Principal node in the cluster. An error is displayed as shown in the below figure.

```
[agni@bm18:~$ agni join
[? Enter the Principal node FQDN:                    s.com
[? This will join to the cluster. Do you want to proceed? Yes
Start join
This node is setup as Principal and will join to another cluster
[? Enter the AGNI UI (Local Account) Username:  alan.fairfax
[? Enter the AGNI UI (Local Account) Password:  [? for help] **********
password authentication complete
The Principal node is running version [P-2026.2.29], which is older than the current node version [P-2026.2.30]. Please update the Principal node to con
tinue.
Join failed. Error messages are captured in cli.log
Usage:
  agni join [FLAGS]

Flags:
  -c, --callHome CallHome   AGNI Instance Call Home server (dev|next|systest|eft) (default dev)
  -h, --help                help for join
      --timeout duration    Maximum time allowed for the command to run (ms|s|m|h) (default 1h0m0s)

Examples:
agni join                                                (Join AGNI node to the cluster)

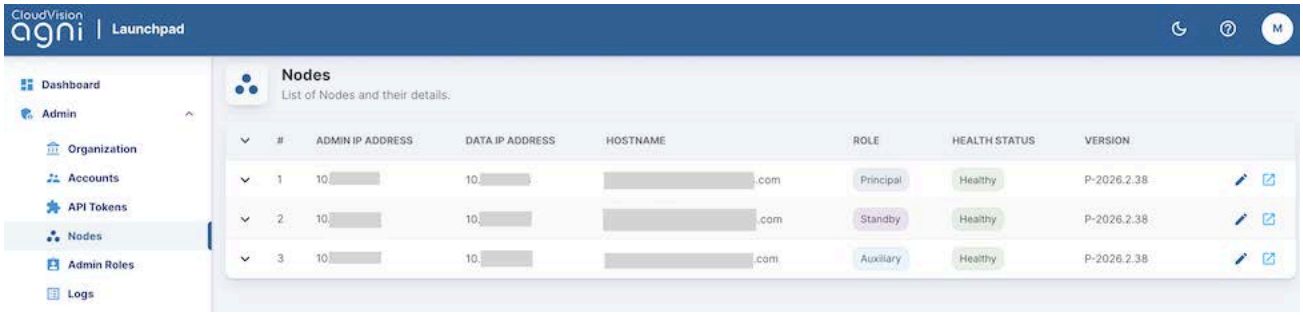

Error while executing command: Principal node version is older
```

Administrators can change the *Auxiliary node* role to *the Standby node* role by using the `agni role` command. The node on which this command is executed becomes the new *Standby node*. In a cluster, if an existing node acts as a Standby and the admin executes this command on another node, the new node becomes the Standby node of that cluster, and the old Standby node becomes the Auxiliary node.

```
[agni@bm29:~$ agni role
[? This node role will be changed to Standby. Existing Standby will become Auxiliary. Do you want to proceed? Yes
Start role update
Role updated successfully
agni@bm29:~$
```

After successful cluster creation, log in to the Principal node UI and navigate to **Admin** > **Nodes**.

The system displays the cluster details of the Principal, Standby, and Auxiliary nodes in the Nodes page.



CAUTION: Do not attempt to join nodes to a *Principal* node that is running a different AGNI version, as this operation will fail. We strongly recommend that you only join nodes when all of them, including the *Principal* node, run the same version.

3.3 Uploading the Certificates

This section includes the following topics:

- SSL Signed Certificate Upload from UI
- Custom EAP Server Certificate Upload

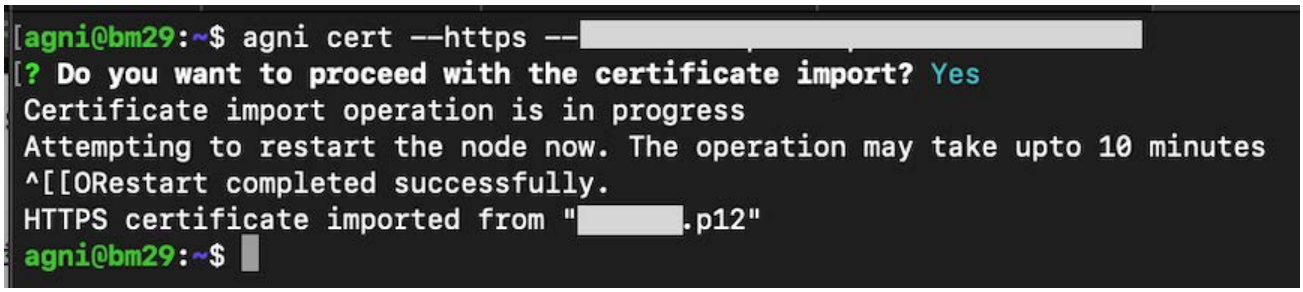
3.3.1 Uploading SSL Signed Certificate for UI

Upload the SSL certificate (signed by a well-known CA) to each AGNI server at `/home/agni` location using any SCP client.

Log in to **each** AGNI server to import the HTTPS certificate to AGNI:

```
agni cert --https --in xxxx.p12 --passin **********
```

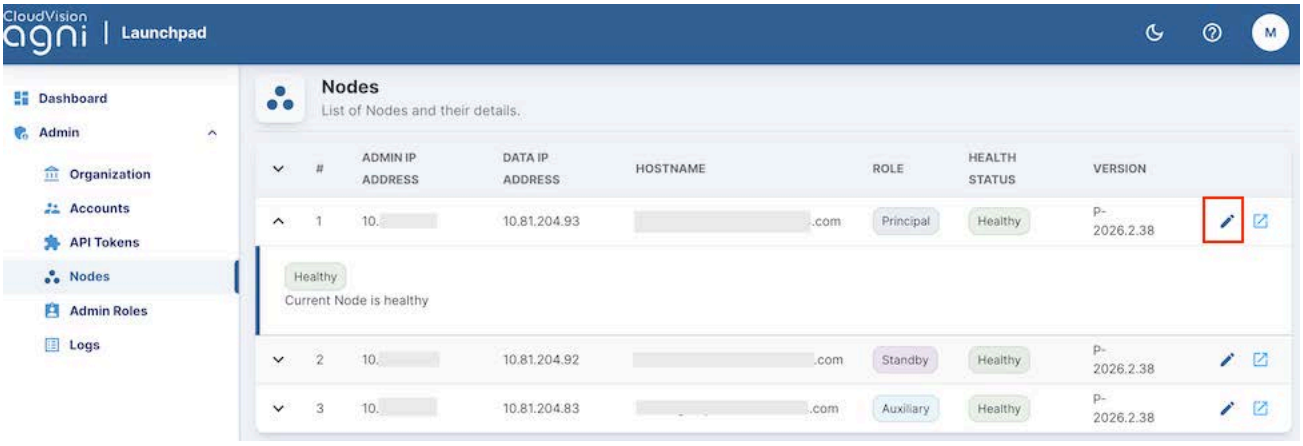
The image is an example of a cert import:



Additionally, from release 2026.2.0 onwards, you can also upload SSL certificate from AGNI user interface. To upload SSL certificate using the UI, perform the following steps:

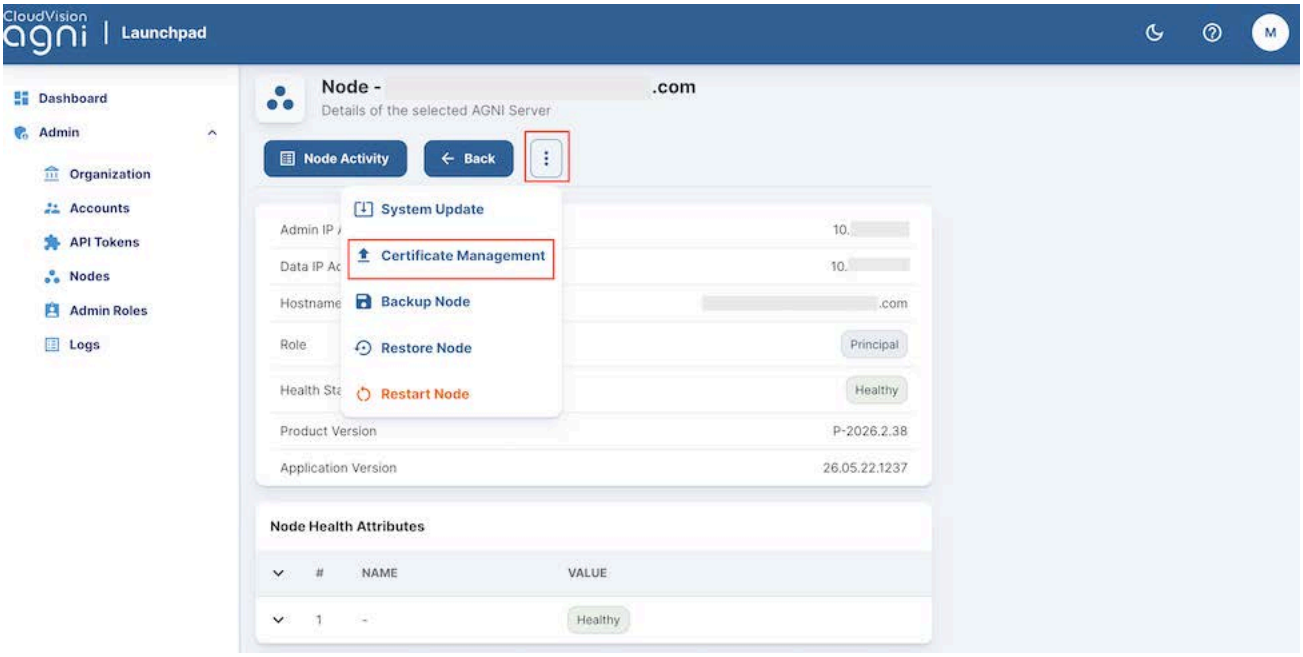
- Login to the Principal Node UI after the initial Bootstrap and Setup is done.
- From Launchpad, navigate to **Admin** > **Nodes**. Select the appropriate node and click edit.

  Figure 3-1: List of Nodes



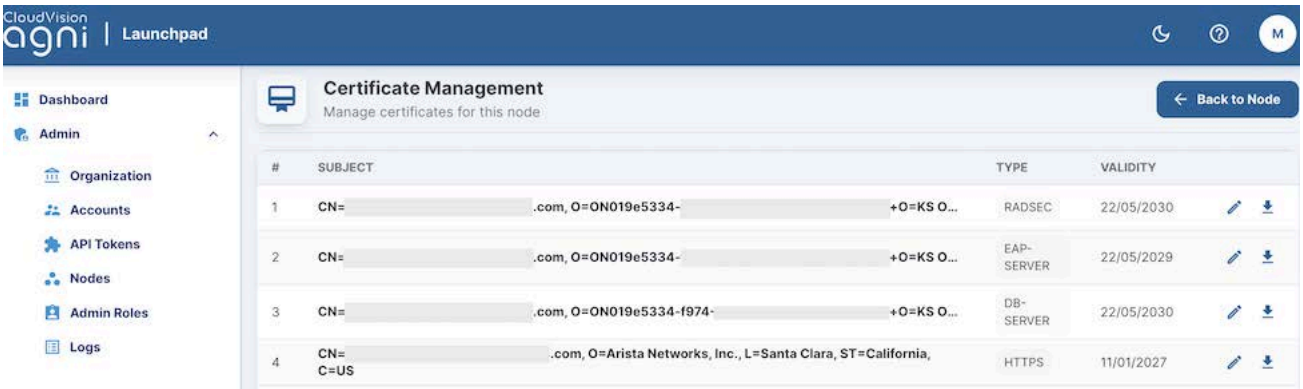
- In the node details window, click **More Actions** (three dots at the top), and select **Certificate Management**.

Figure 3-2: Edit Node-Select Certificate Management



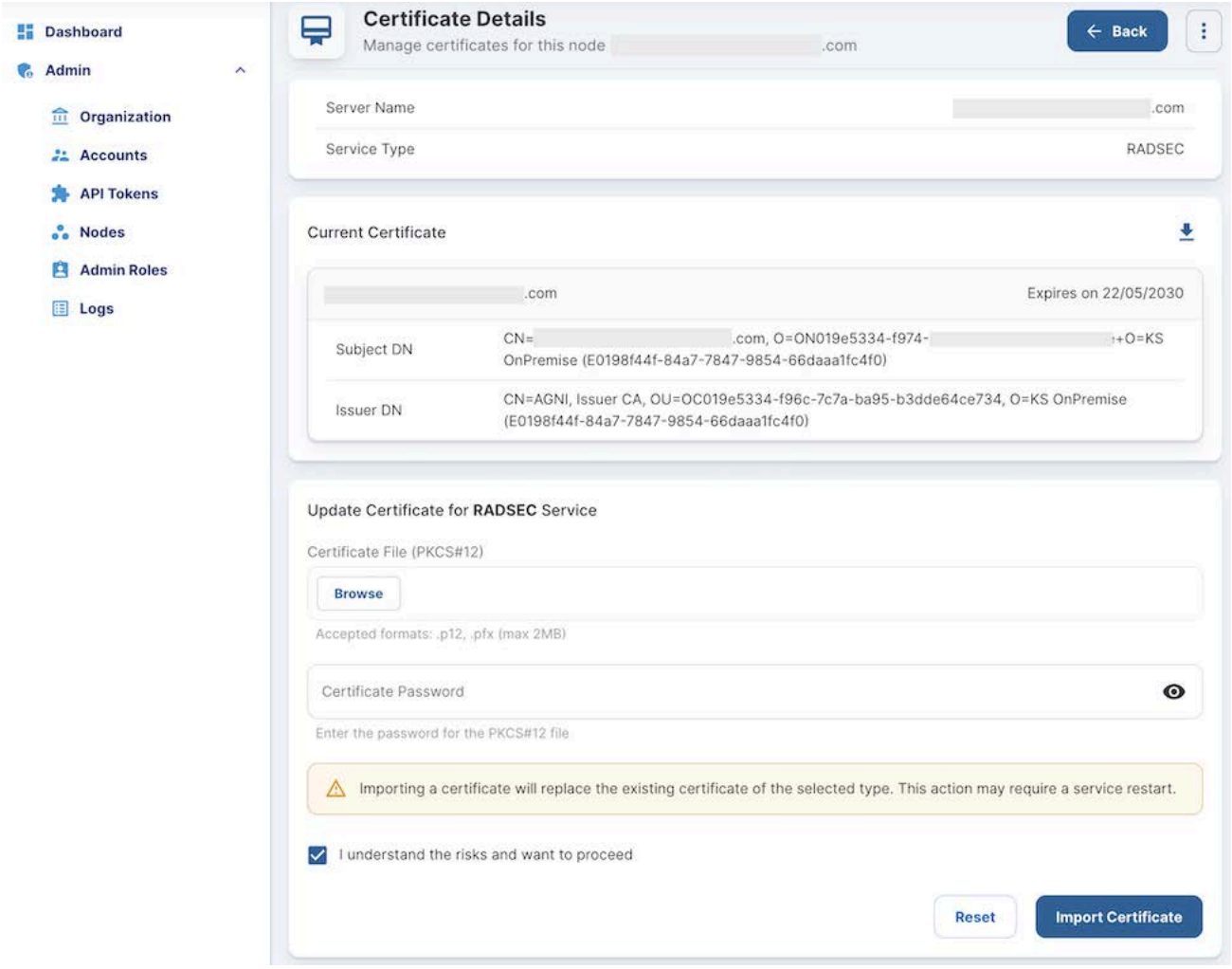
- Select the appropriate Certificate type to upload.

Figure 3-3: List of Certificates



- In the **Certificate Details** window, click the *I understand the risks and want to proceed* check-box and click the **Import Certificate** button.

Figure 3-4: Import Certificate page



3.3.2 Uploading Custom EAP Server Certificate

Starting with 2026.2.0 release, AGNI allows you to upload customized EAP server certificate, where you can upload your organization specific EAP server certificate for authentication. However, this configuration is optional and not required for normal operations.

Follow the same process described in the **SSL Signed Certificate Upload for UI** section to import the custom EAP server certificate uisng the CLI commands or from the AGNI UI.

For additional details, see the **Certificate Management** chapter in the AGNI User Guide.

3.4 Modifying the Cluster

The administrator is responsible for managing the cluster by adding new Auxiliary nodes or adjusting the existing Standby node as required. To incorporate multiple Auxiliary nodes into the cluster, use the `agni join` command. To create a new Standby node, use the `agni role` command.

If the Principal node fails, the administrator should promote the Standby node to the Principal node by using the `agni promote` command. This command is applicable solely to the Standby node. Upon execution, AGNI removes the current Principal node from the cluster and promotes the Standby node as the new Principal node. To establish a new Standby node within the cluster, use the `agni role` command on an Auxiliary node.

3.4.1 Removing Nodes from the Cluster

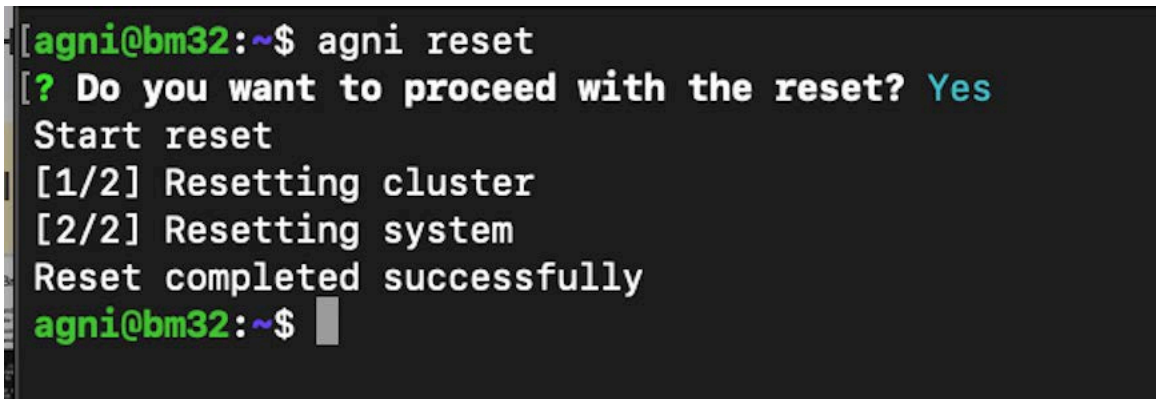
Admin can remove a node from the cluster by using the two commands: `agni drop` and `agni reset`.

3.4.1.1 AGNI Reset command

Use this command to reset and remove a node from the cluster. Admin can execute this command on the node's CLI to remove it from the cluster. After the `agni reset` command is executed, the node is removed from the cluster. System and network configurations will remain intact after this operation. If any of the cluster operations fail, this command assists in bringing the appliance back to the bootstrap stage.

Note: Execute this command with caution as the node loses its configuration as a part of the process.

Note: The CLI password gets reset to the default value after the `agni reset` command.

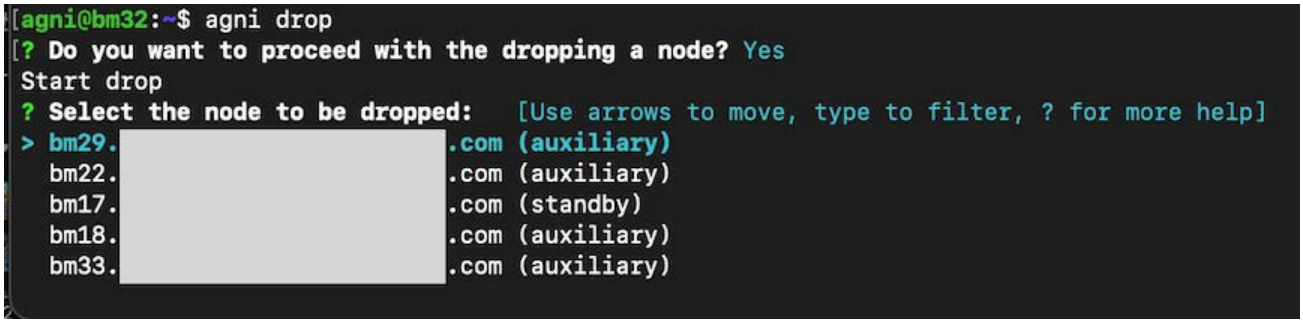


3.4.1.2 AGNI Drop Command

On the Principal node, use the `agni drop` command to remove a node from the cluster. Select the node that should be removed from the node list in that cluster. This command removes the replication slot for the node from the cluster. If the device response is not received from the dropped node, then after a timeout that node is removed from the cluster and the Principal node updates the cluster node list. After the node is dropped, it needs to be reset before it can either join back to the cluster or be set up as an independent Principal node.

Note: In a multi-node cluster, a standby node cannot be dropped from the Principal node. Before dropping it, another Auxiliary node should be made, the Standby node.

Note: The CLI password is reset to the default '**Arista123#**' after the node is dropped.







If a node becomes RMA or faulty, the admin can replace it with a new one using the `agni drop` and `agni join` commands.

3.4.1.3 AGNI Update Command

The `agni update *` command is used to update the AGNI version. All nodes will fetch updates from the cloud individually. You can also update the cluster using the **System Update** option from the user interface. For details, see the **System Update** section in the Managing and Monitoring the Cluster from the UI section.

To view the list of available updates for AGNI, use the `agni update --list` command:

Figure 3-5: AGNI Update -List Command

```
[agni@bm27:~$
[agni@bm27:~$ agni update --list
Fetching update information...

Current AGNI Release: P-2026.2
Product Version: P-2026.2.43

You are already on the latest minor update for this release.

Applicable major release(s) available:

 AGNI Release: P-2026.3
 Description: Update to 2026.3 release
 Release Date: August 2026

Refer https://www.arista.com/en/support/product-documentation for release notes

agni@bm27:~$
```

To update to a minor version, use the `agni update --minorrelease` command:

Figure 3-6: AGNI Update - Minor Release Command

```
[agni@bm22:~$ agni update --minorrelease
Fetching minor release update information...

Current AGNI Release: P-2026.2
Product Version: P-2026.2.12

Applicable minor update available is P-2026.2.14

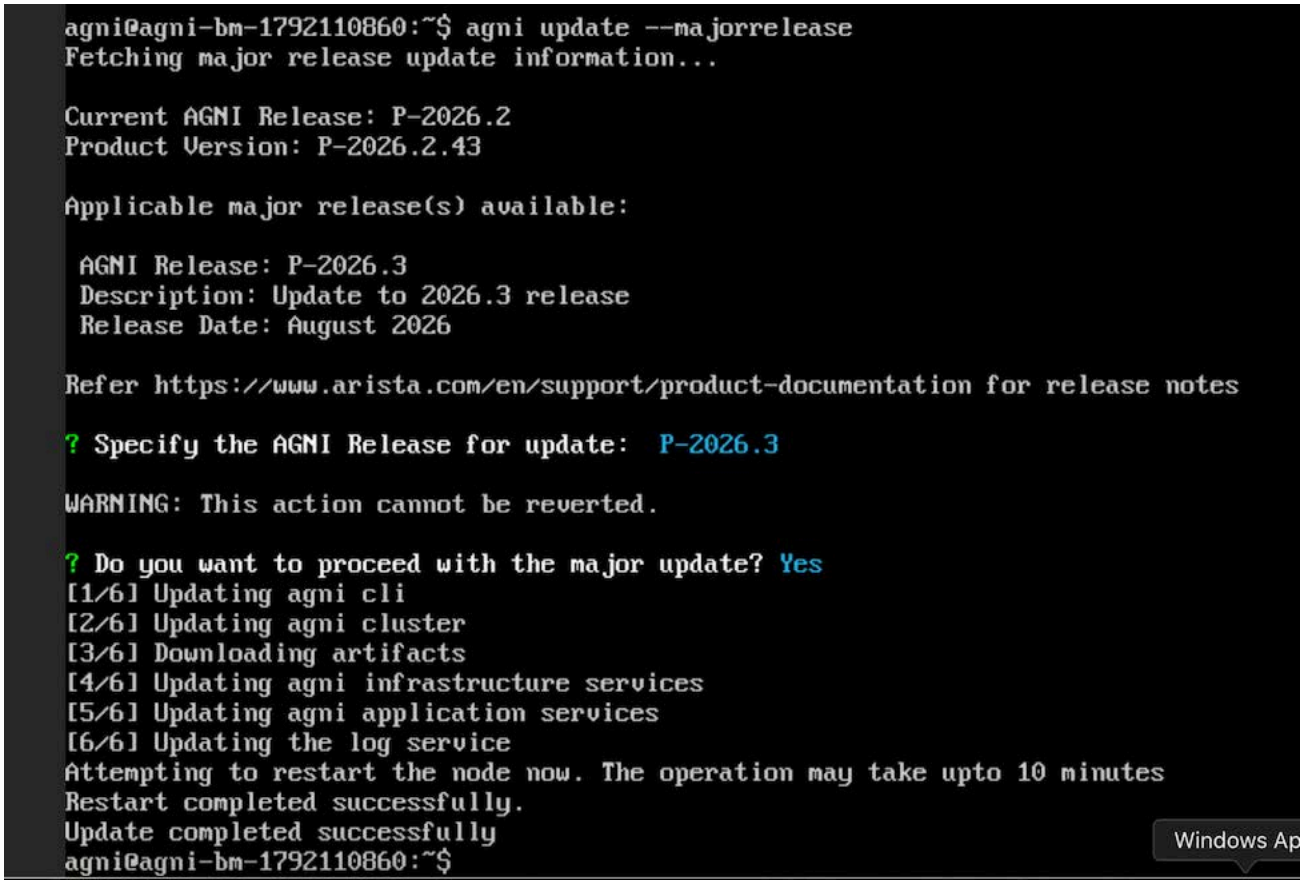
Refer https://www.arista.com/en/support/product-documentation for release notes

WARNING: This action cannot be reverted.

[? Do you want to proceed with the update? Yes
[1/6] Updating agni cli
[2/6] Updating agni cluster
[3/6] Downloading artifacts
[4/6] Updating agni infrastructure services
[5/6] Updating agni application services
[6/6] Updating the log service
Attempting to restart the node now. The operation may take upto 10 minutes
Restart completed successfully.
Update completed successfully
[agni@bm22:~$
```

To update to a major version, use the `agni update --majorrelease` command:

Figure 3-7: AGNI Update - Major Release Command

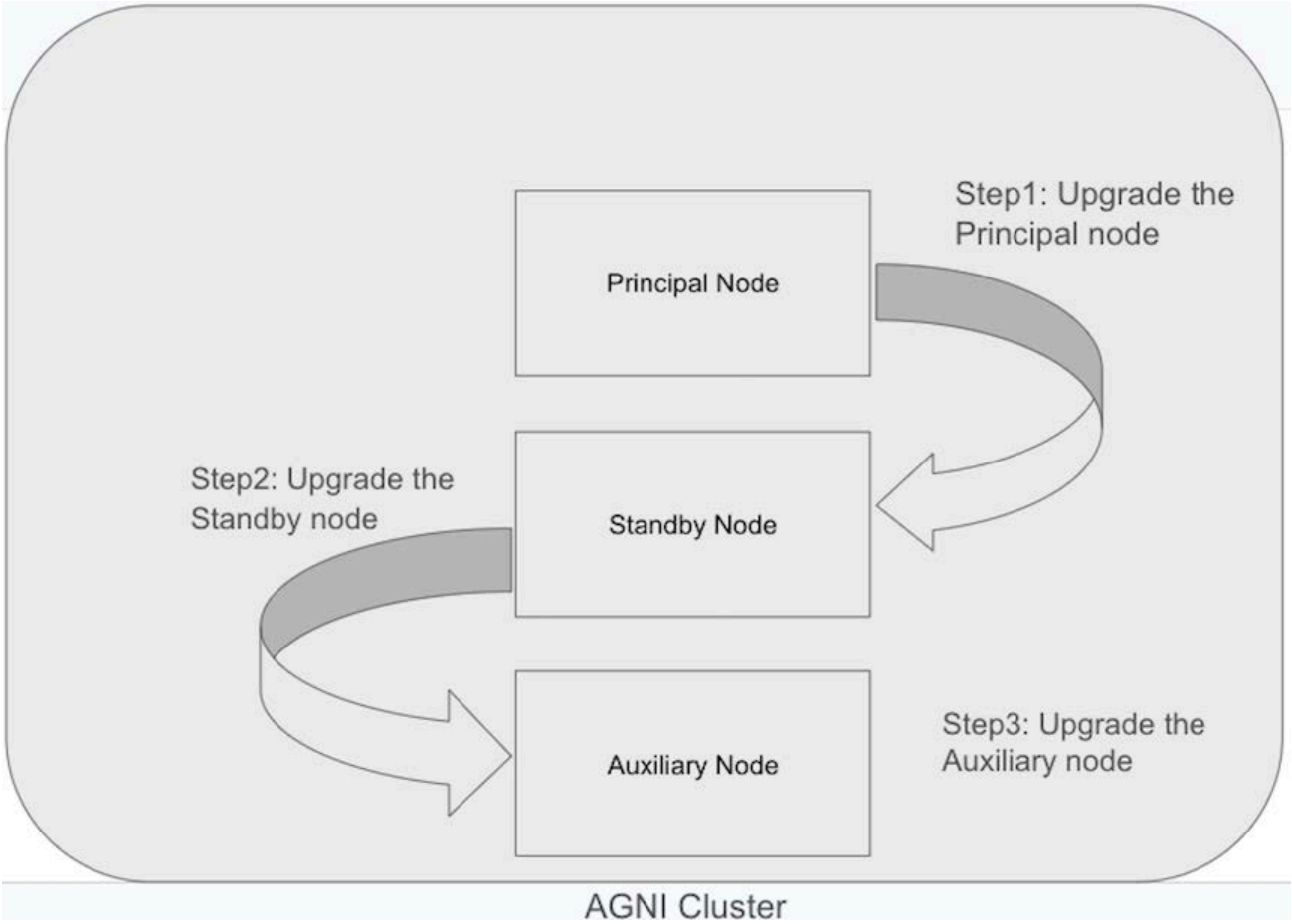


The `agni update` of a cluster should be done in the following sequence:

1. Update the cluster Principal node
2. Update the cluster Standby node

3. Update the cluster Auxiliary node

Figure 3-8: AGNI Update Flowchart



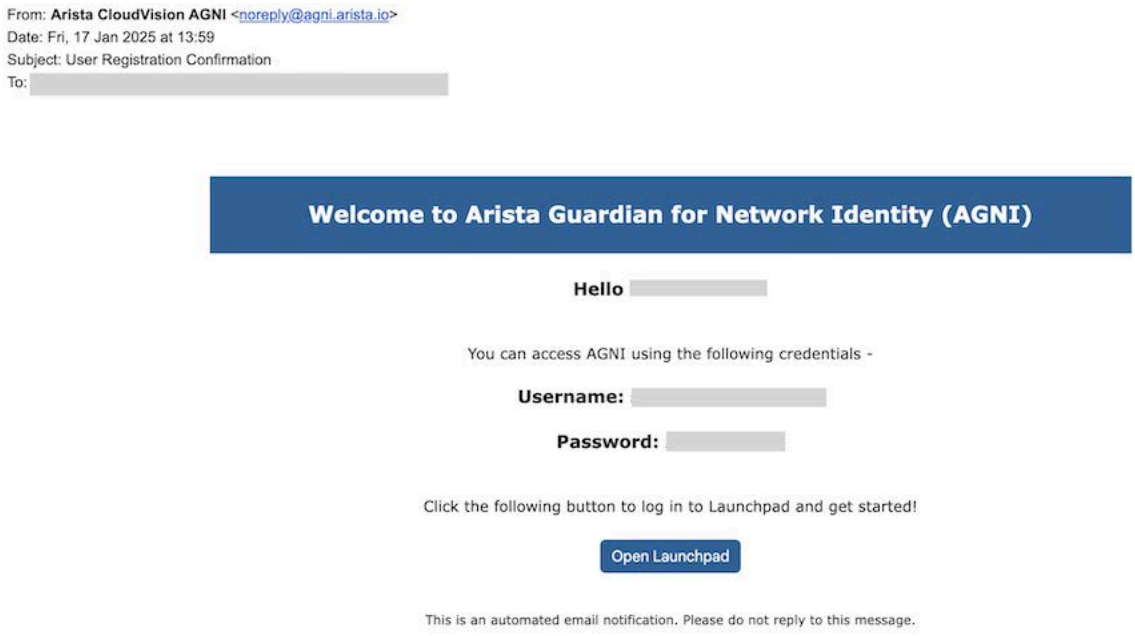
Chapter 4

Organizational Login Activities

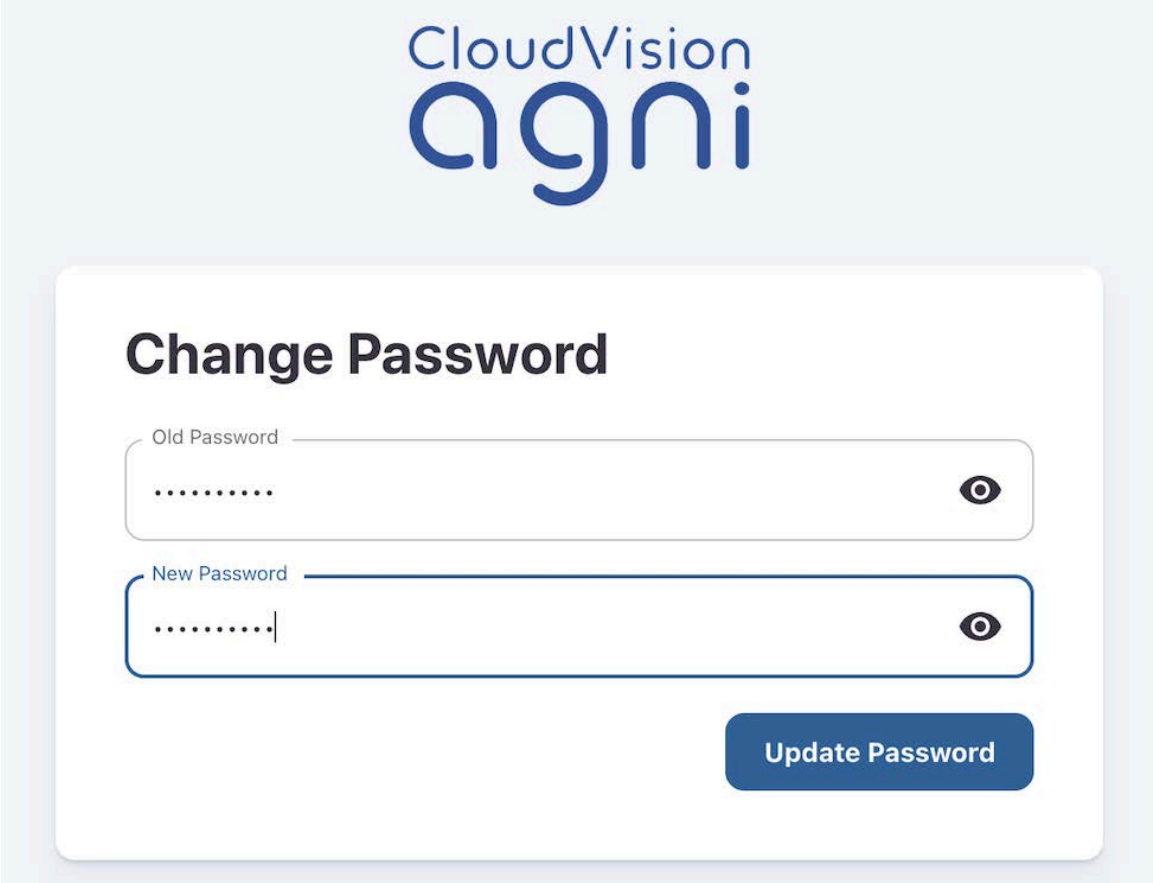
This section describes the different login methods and the API token generation process:

4.1 Local User Login

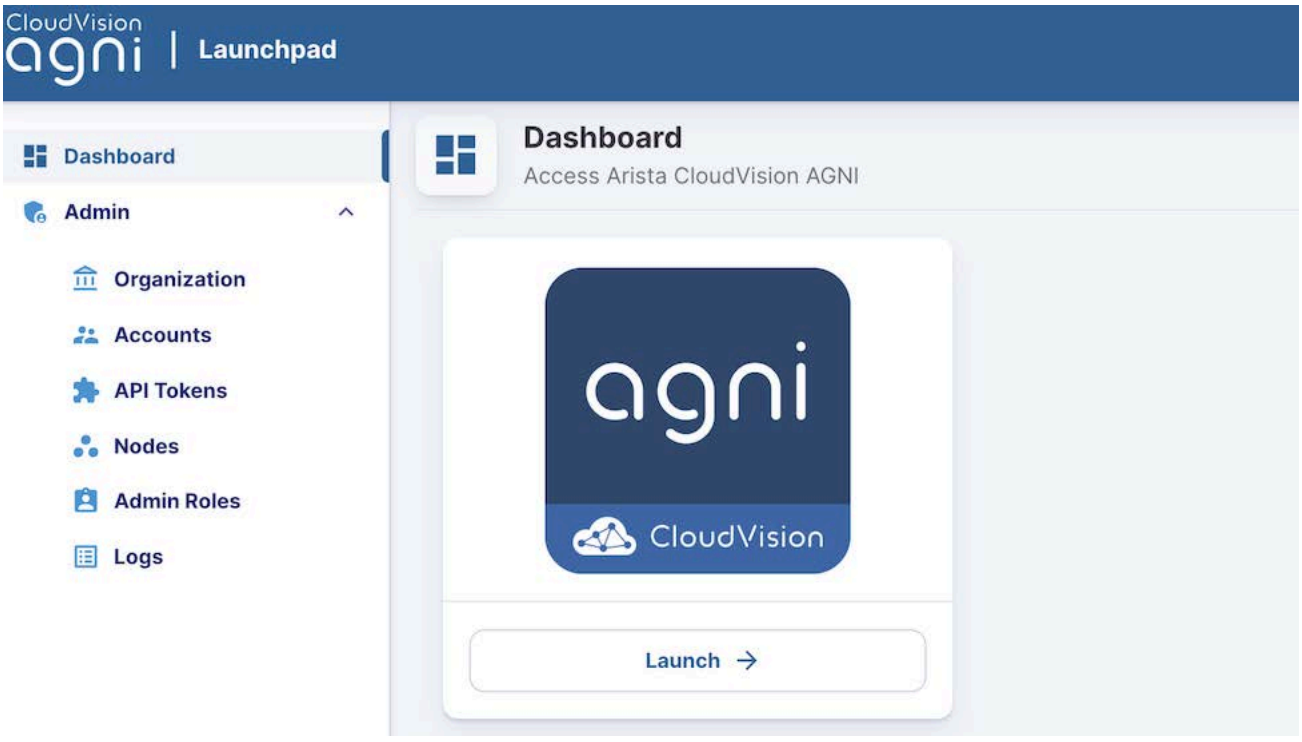
- Once setup is complete, as described in the earlier section, the admin user receives an email with login credentials.
- Click the **Open Launchpad** button, to take you to the Login URL.
- Provide Username & Password shared in the email for successful login.



After successful login, change the password credentials:



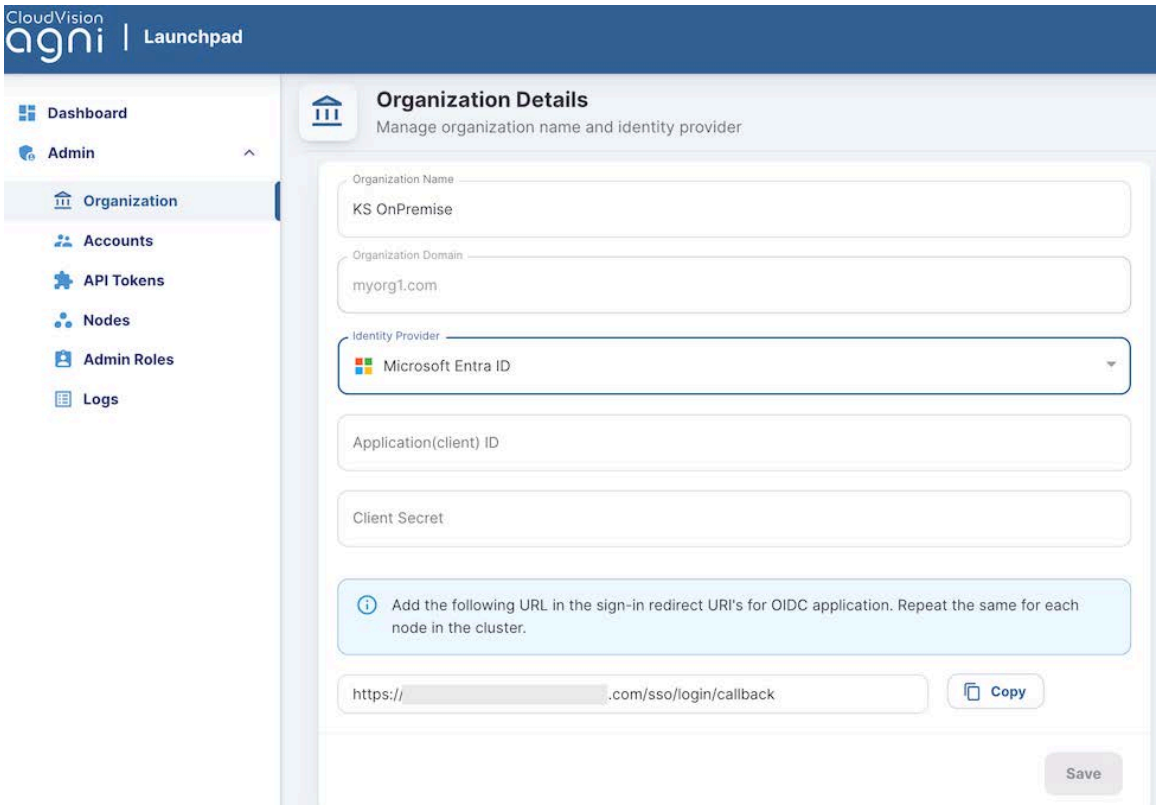
Once the password is changed, the user is redirected to the AGNI Launchpad.



Click the **Launch** button to navigate to the AGNI portal.

4.2 IDP Admin User Login

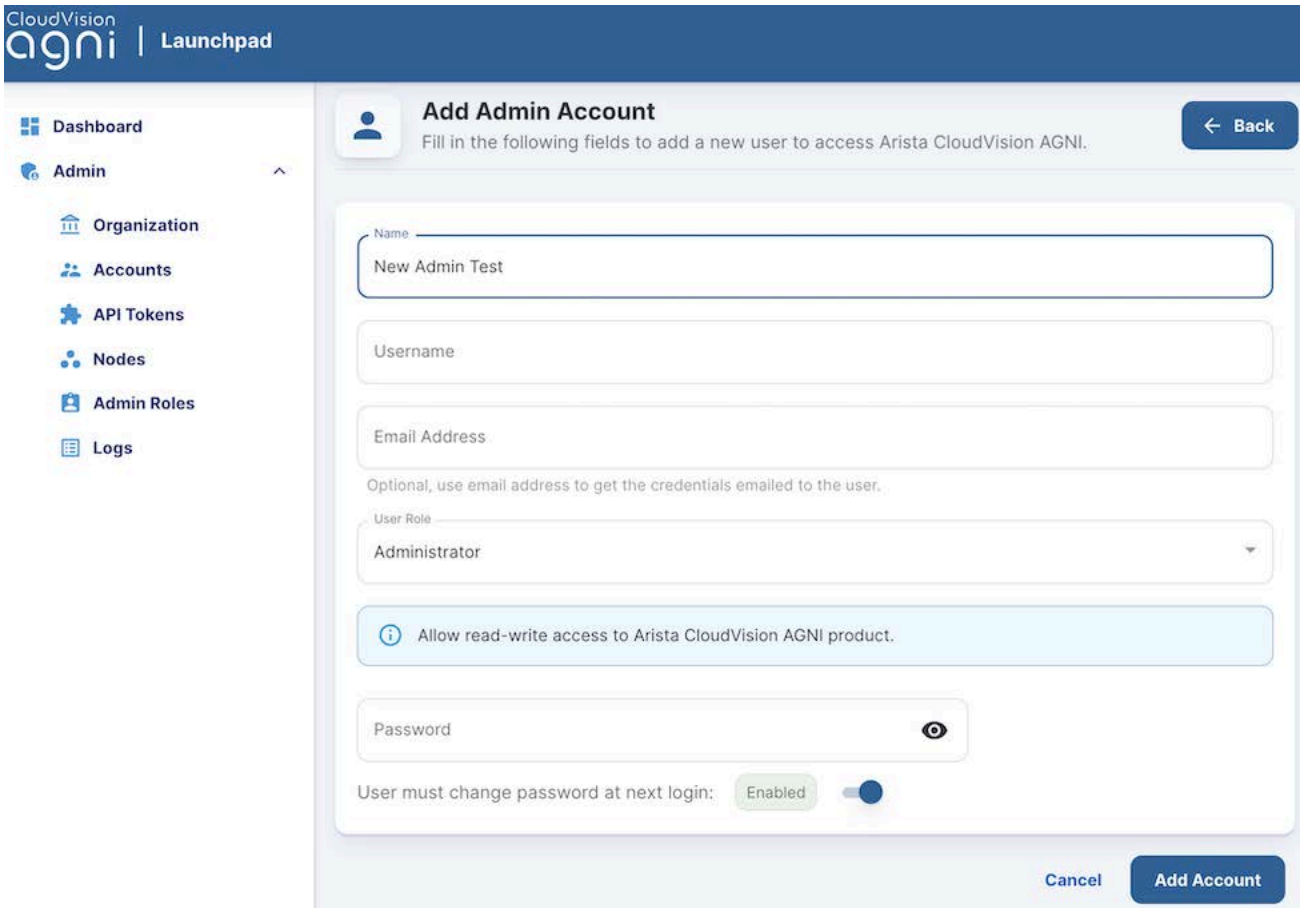
- After you log in as a Local user, navigate to **Admin** > **Organization** and provide the required **Client ID** and **Client Secret** for the IDP user to log in successfully.



- The AGNI launchpad is accessible to the user upon successful validation of their IDP credentials.

4.3 Local Account User Creation

- After login, navigate to **Admin** > **Accounts** and click the **+ Add Account** button.
- Admin can add a user with different user roles by providing the username, email address, and password.



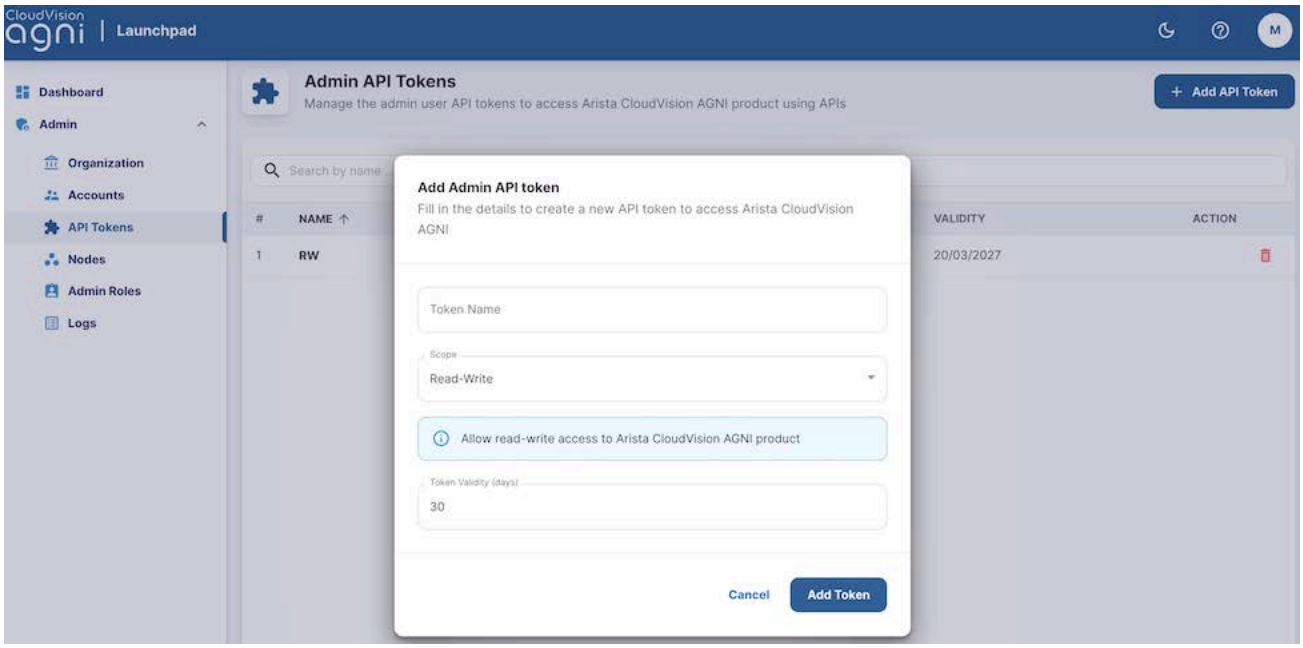
- User with *super administrator* role can add, modify, or delete the local user accounts from the user listing.

  Users with *Administrator* or *Operator* roles cannot access the **Admin** menu from AGNI launchpad.

Note: Refer to the AGNI (On-Premises) User Guide on Arista Product Documentation site to configure and use the newly introduced (version 2026.2.0) **Admin Roles**. These are custom roles that can be defined by the administrator in addition to the default user roles.

4.4 API Token Generation

- API Token addition and token generation can be done by navigating to the **Organization** > **Admin** > **API Token**.
- Provide the role and token validity to generate a token. This token can be used to integrate with AGNI through API.


CloudVision agni | Launchpad
M
Dashboard
Admin
Organization
Accounts
API Tokens
Nodes
Admin Roles
Logs
Admin API Tokens
Manage the admin user API tokens to access Arista CloudVision AGNI product using APIs
+ Add API Token
Search by name
NAME
1 RW
VALIDITY
ACTION
20/03/2027
Add Admin API token
Fill in the details to create a new API token to access Arista CloudVision AGNI
Token Name
Scope
Read-Write
Allow read-write access to Arista CloudVision AGNI product
Token Validity (days)
30
Cancel
Add Token

Chapter 5

Maintaining the Cluster

This section describes the AGNI backup, restore, reboot, and shutdown process and also monitoring and maintaining the cluster nodes:

5.1 Managing and Monitoring the Cluster from the UI

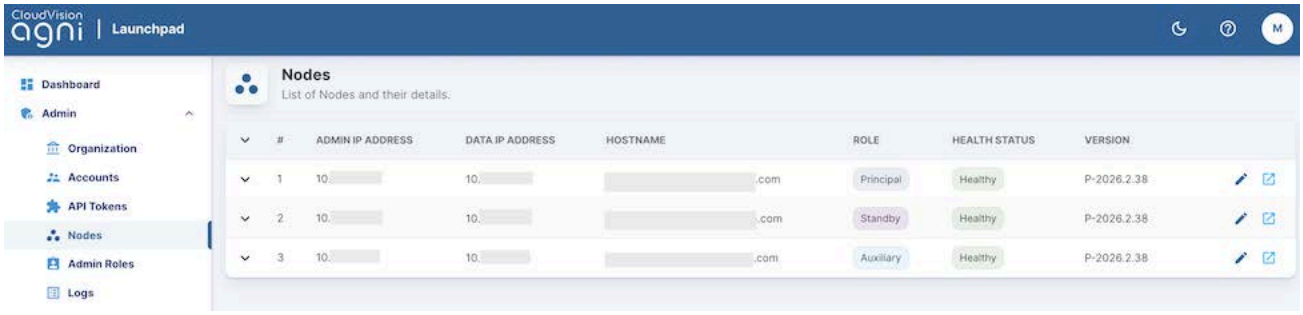
AGNI cluster includes a minimum of three nodes: one Principal node, one Standby node, and one or more Auxiliary nodes. Node is a single AGNI appliance that performs the basic product functionality. For details, see the Cluster Configuration chapter.

An AGNI administrator can perform various monitoring and management activities on the nodes in a cluster as explained in this section.

Monitoring Node Health - The administrators can monitor the cluster health by logging to AGNI and navigating to **Admin** > **Nodes**. This page displays the nodes in the cluster and their health. The system categorizes a node's health into one of three types:

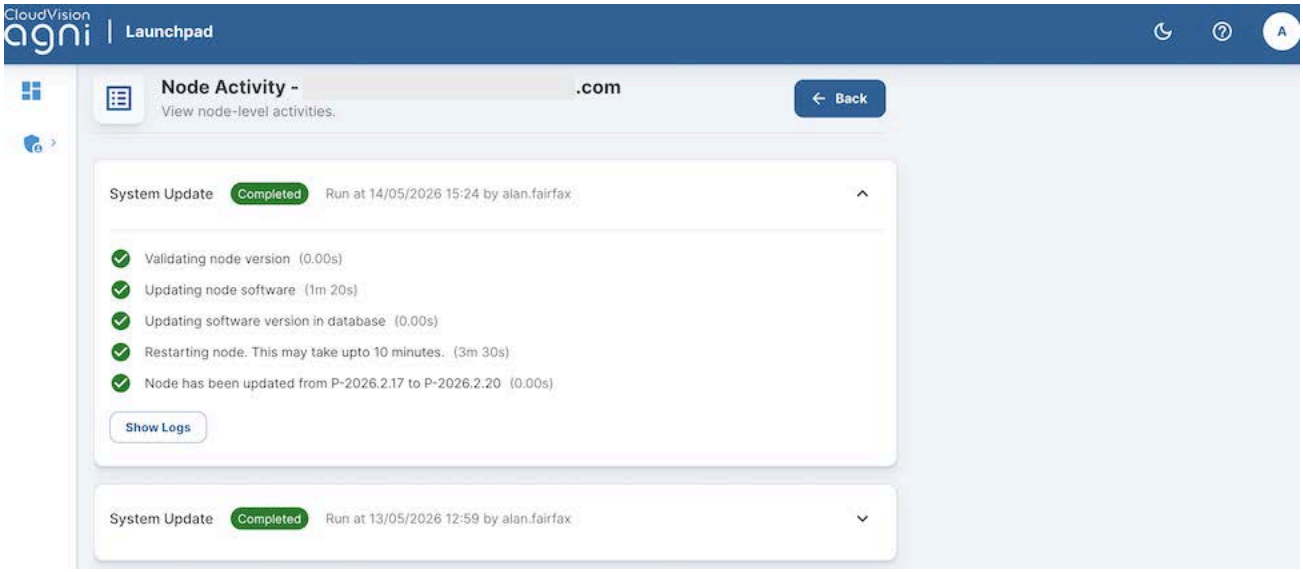
Table 4: Health Status

Status	Description
Healthy	All services are working as expected.
Needs Attention	Minor errors in the node.
Critical	Major errors in the node like node down or replication broken.



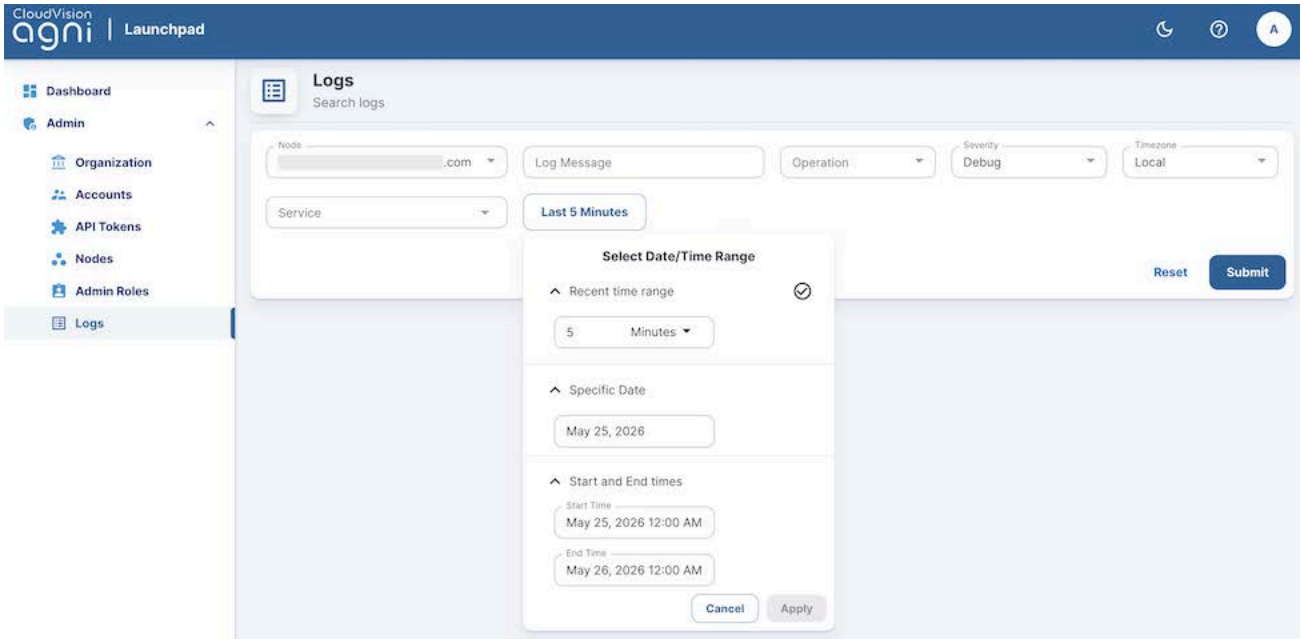
Monitoring Node Activity - To monitor the node activity, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, click the **Node Activity** button.

Figure 5-1: Node Activity



View and Download Logs - To view or download system level logs for various AGNI services, navigate to **Admin** > **Logs**. Enter the required details and click the **Submit** button to view and download the request logs. You can also specify the date and time range for the log details. The default time range is **last 5 minutes**.

Figure 5-2: Node Level Log Details

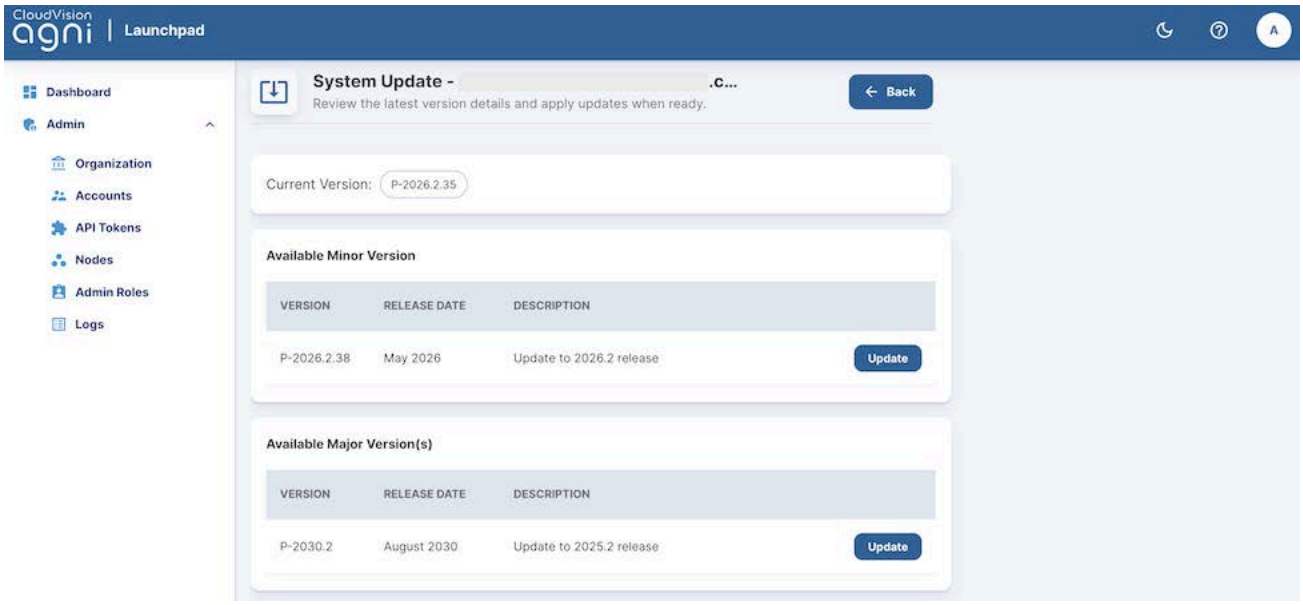


Perform **System Update** - AGNI version 2026.2.0 allows you to update the software version on a node from the UI also, apart from the CLI. To update the AGNI version on a node through the UI, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, click the **More Actions** (three dots) button and select **System Update**. AGNI page displays the current installed version, available minor

version and available major version. Choose the appropriate version and click the **Update** button to update the node to a higher version.

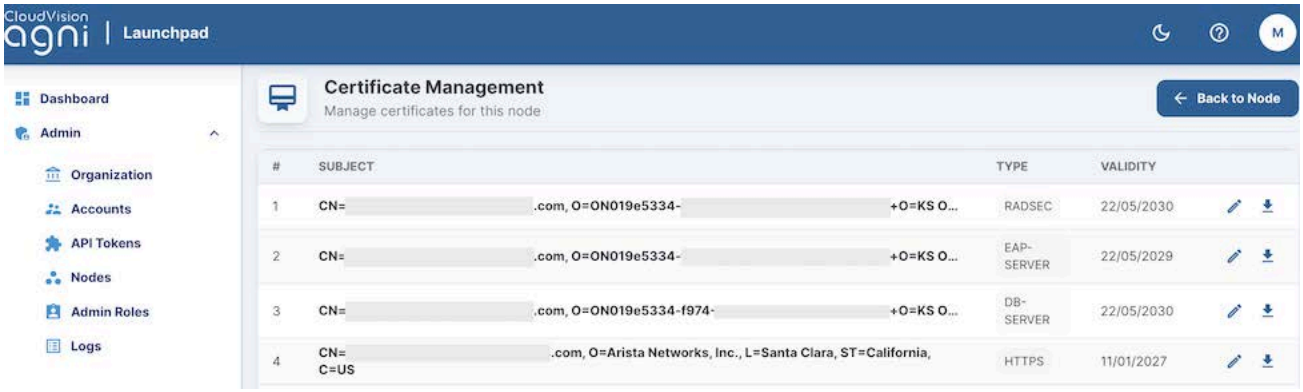
> **Note:** Update the Principal Node first, followed by Standby and Auxiliary nodes.

Figure 5-3: System Update of a Node



Certificate Management - To update the certificate on a node, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, click the **More Actions** (three dots) button and select **Certificate Management**. You can manage the following system certificates: **HTTPS**, **RADSEC**, **EAP-SERVER**, and **Database SERVER**.

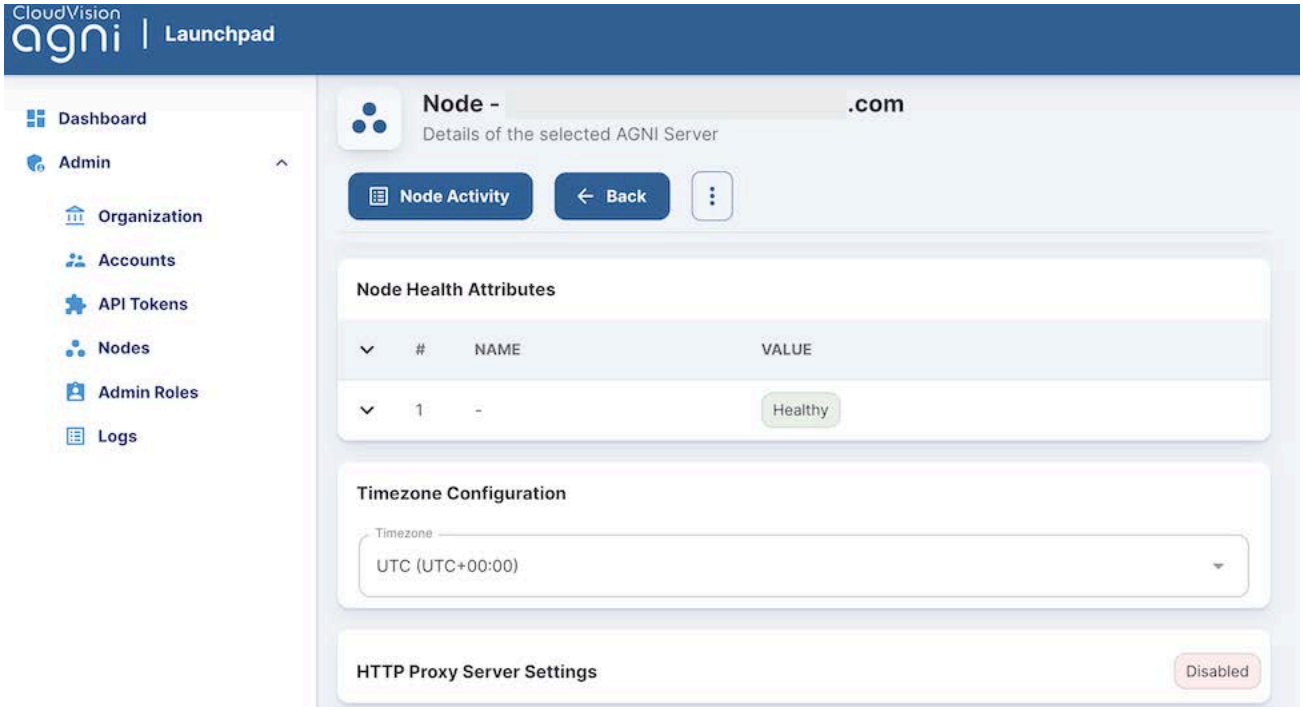
Figure 5-4: Certificate Management for a Node



For details on updating the server certificates, see the Uploading SSL Signed Certificate for UI section.

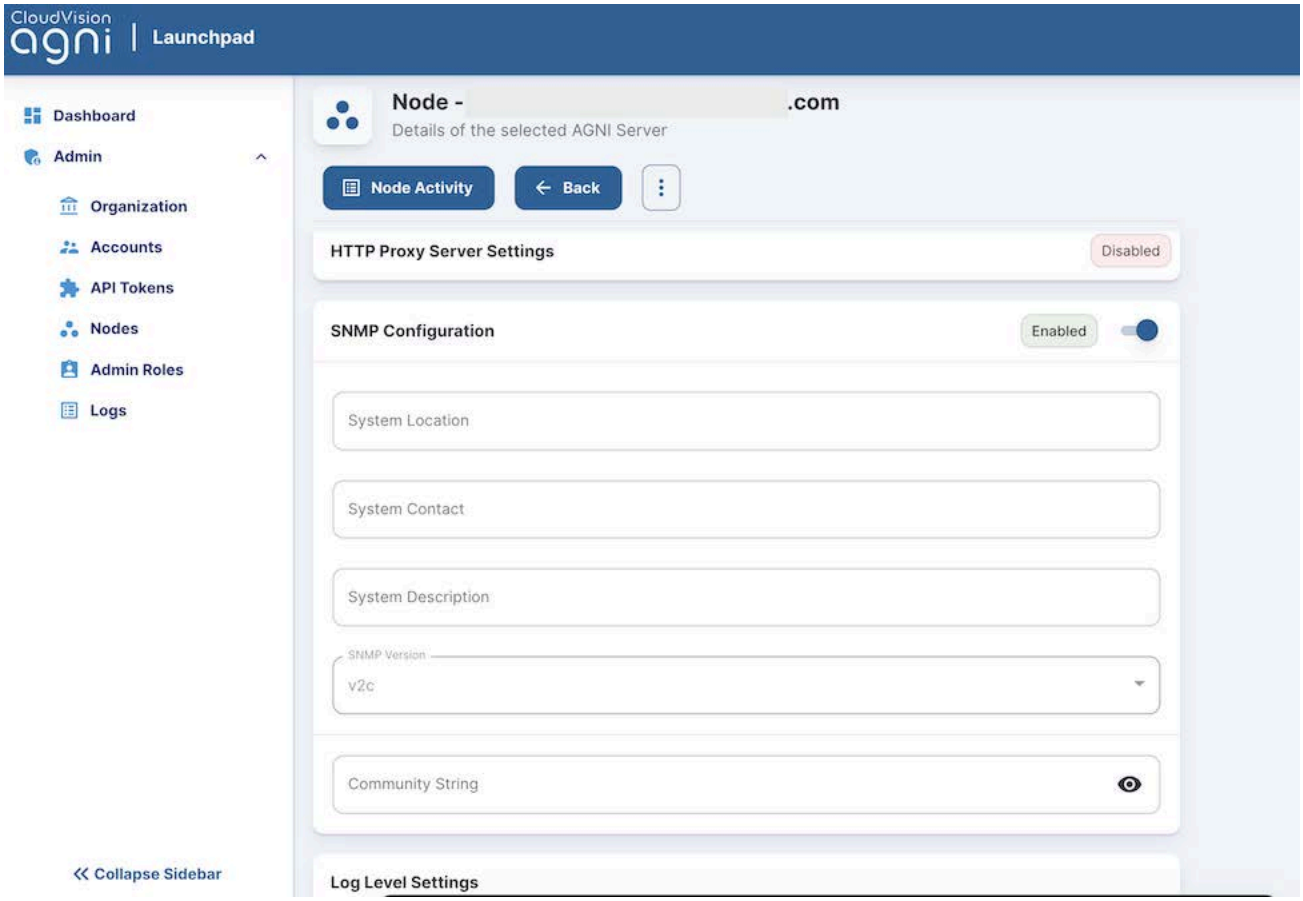
Timezone Configuration - To configure the timezone for a node, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, scroll down to the **Timezone Configuration** section. You must configure the system timezone for each node separately.

Figure 5-5: Node - Timezone Configuration



SNMP Configuration using the UI - To configure the SNMP details for a node, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, scroll down to the **SNMP Configuration** section. You can enable and configure SNMP system level MIBs such **sysDescription**, **sysContact**, and **sysLocation** using the UI . You must configure the SNMP details for each node separately.

Figure 5-6: Node - SNMP Configuration



5.2 AGNI Backup Operation

You can backup a node in an AGNI cluster by using the CLI or the UI.

Backup using CLI: The `agni backup` command allows the administrator to take a backup of the configuration data, identity data and activity data present in the AGNI database. This command backs-up all data by default. Note that AGNI also performs a daily backup of the data and saves it to the */var/arista/agni/backup* directory.

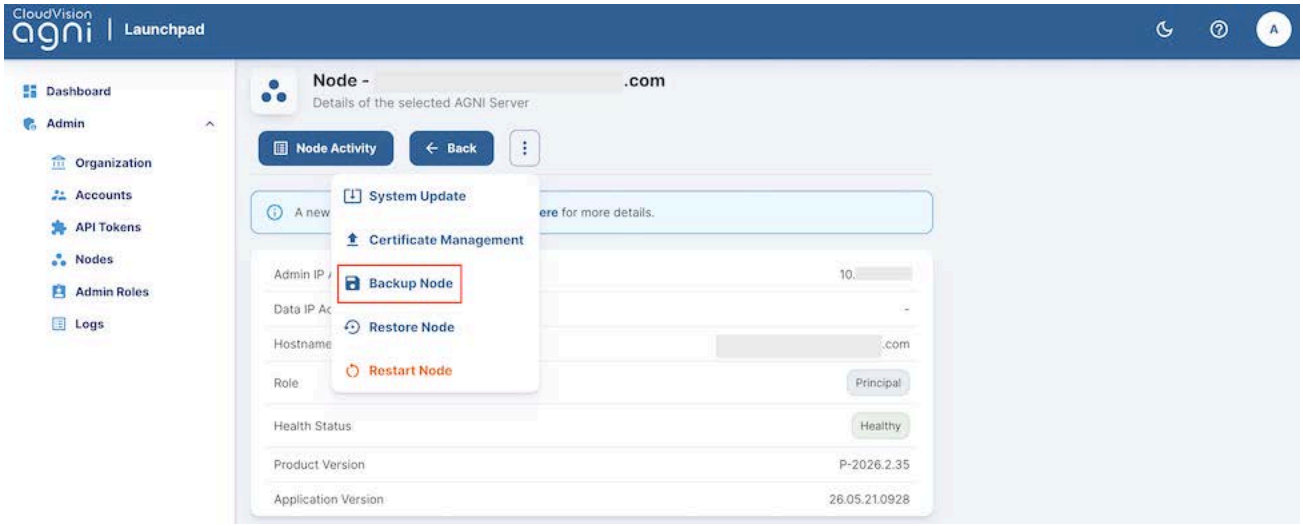
The database backup taken on the Principal node is similar to the cluster backup.

```
agni@bm33:~$ agni backup -f bm33_node_backup
? Do you want to proceed with the backup? Yes

[2025-02-05 14:54:01] File : /var/arista/agni/backup/bm33_node_backup_2025-02-05_14-54.tar.gz
[2025-02-05 14:54:01] Size : 2.0M
[2025-02-05 14:54:01] MD5 Sum : dc58430a9c169ab33842eae80c19f475
```

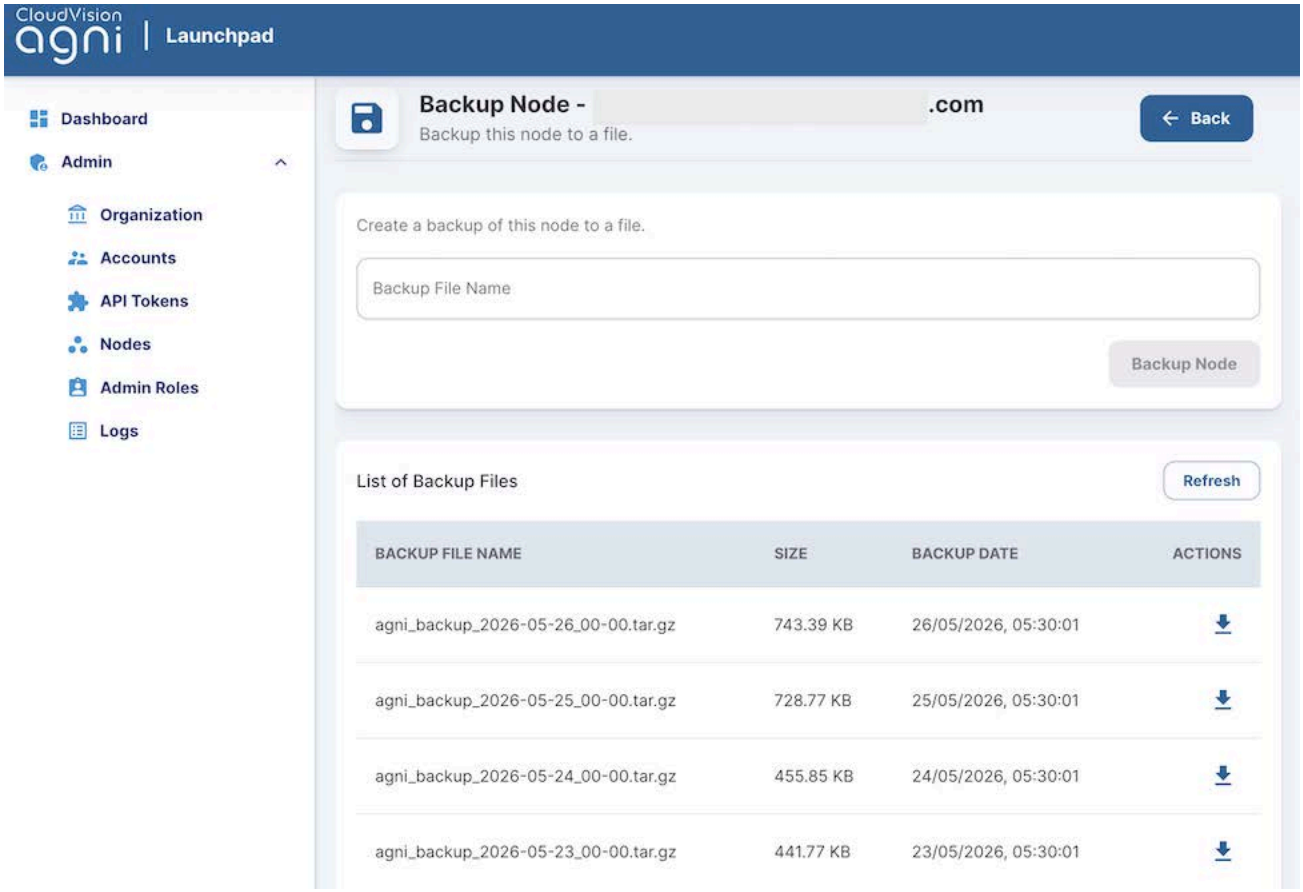
Backup using UI: To backup a node, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, click the **More Actions** (three dots) button and select **Backup Node**.

Figure 5-7: Backup Node



The **Backup Node** page lists the available backups that are taken in past, which can be used during system recovery to restore the configurations.

Figure 5-8: Backup Node Details



For details, see the AGNI (On-Premises) User Guide on the Arista Product Documentation site.

5.3 AGNI Restore Command

You can restore a node in an AGNI cluster by using the CLI or the UI.

Restore using CLI - The administrators can restore the database backup on the Principal node by using the `agni restore` command. Note that `agni restore` command can be performed only on the Principal node as the database is writable only on the Principal node. The other nodes in the cluster would replicate the data once the `agni restore` command is complete.

Note: Restoring session data from a backup is not supported currently.

Note: Use the `agni restart` command to restart all services after the database is restored. Also, the backup will not include SSL certificates, third-party CAs, issuer certificates, and user certificates, resulting in user re-onboarding.

```
agni@bm32:~$ agni restore -f /var/arista/agni/backup/bm32_primary_backup_2025-02-05_16-20.tar.gz
? Select the data to restore:  Identity, Configuration
Please note that the restore process will not restore the user/client certificates.
Also, the restore process will not overwrite the existing system certificates.
Restoring configuration to database...
Restoring identity information to database...

[2025-02-05 16:24:35] Log : Restore completed from 2025-02-05_16-20. It is recommended to restart AGNI using agni restart
agni@bm32:~$
```

Restore using UI: To restore a node, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, click the **More Actions** (three dots) button and select **Restore Node**.

Administrators can restore the previously generated backups using the UI. You can upload the backup file or select the backup file from the server. Alternately, you can restore types of data such as **Identity**, **Config** or both based on your requirement.

Figure 5-9: Node Restore using Upload Backup file

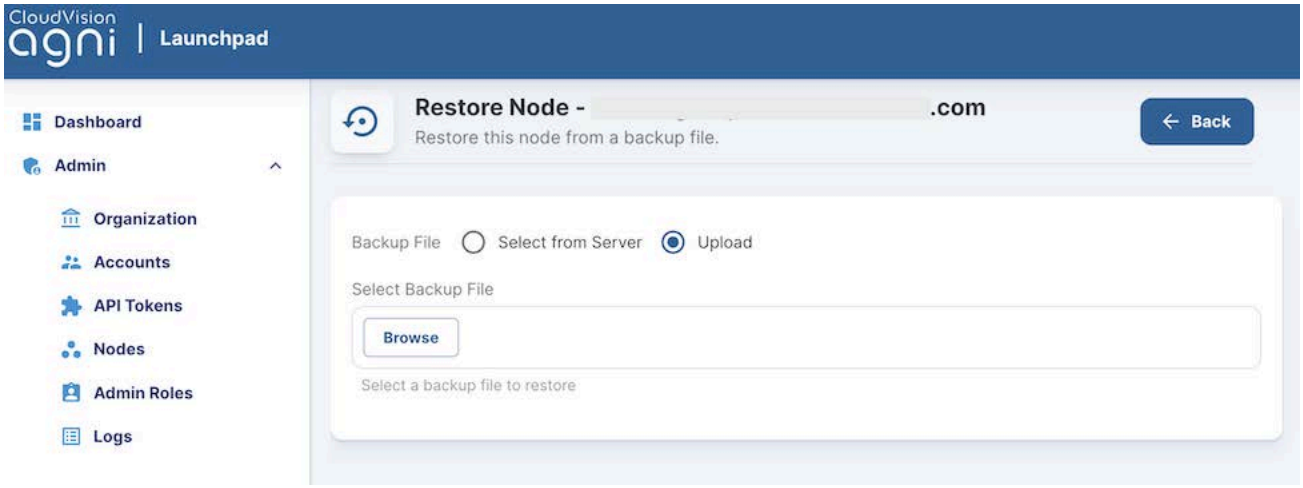


Figure 5-10: Node Restore using Backup file from server

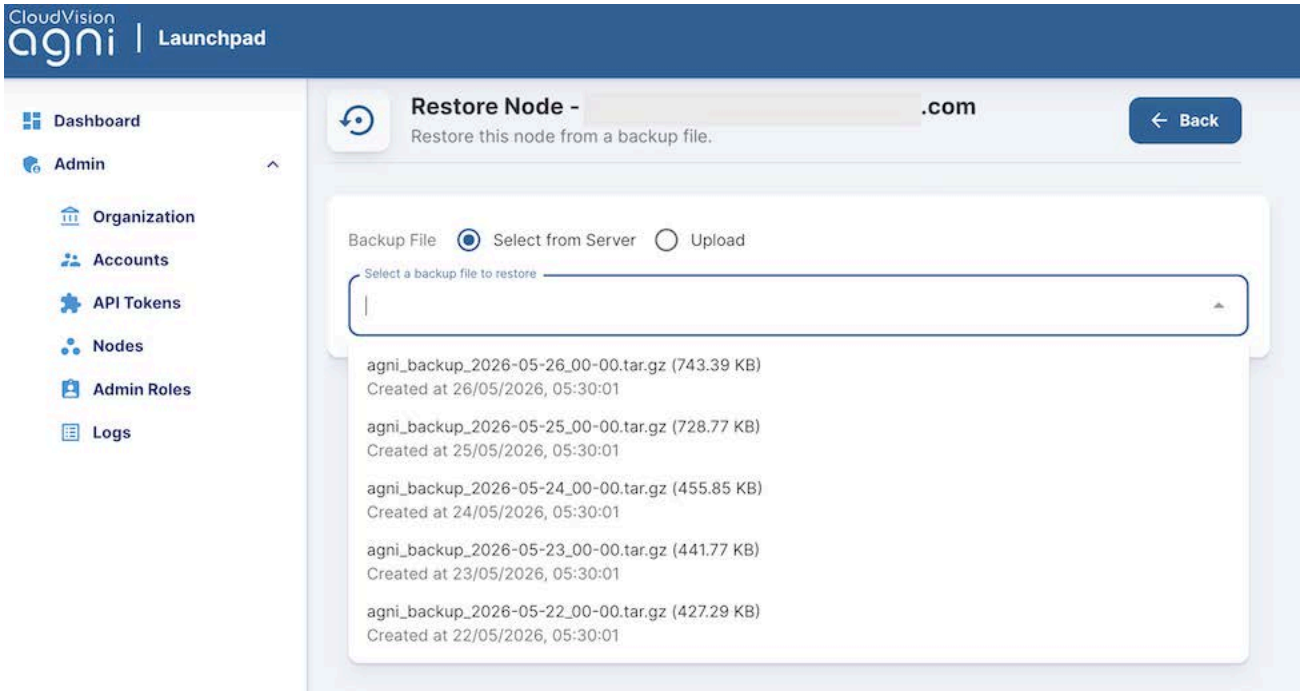
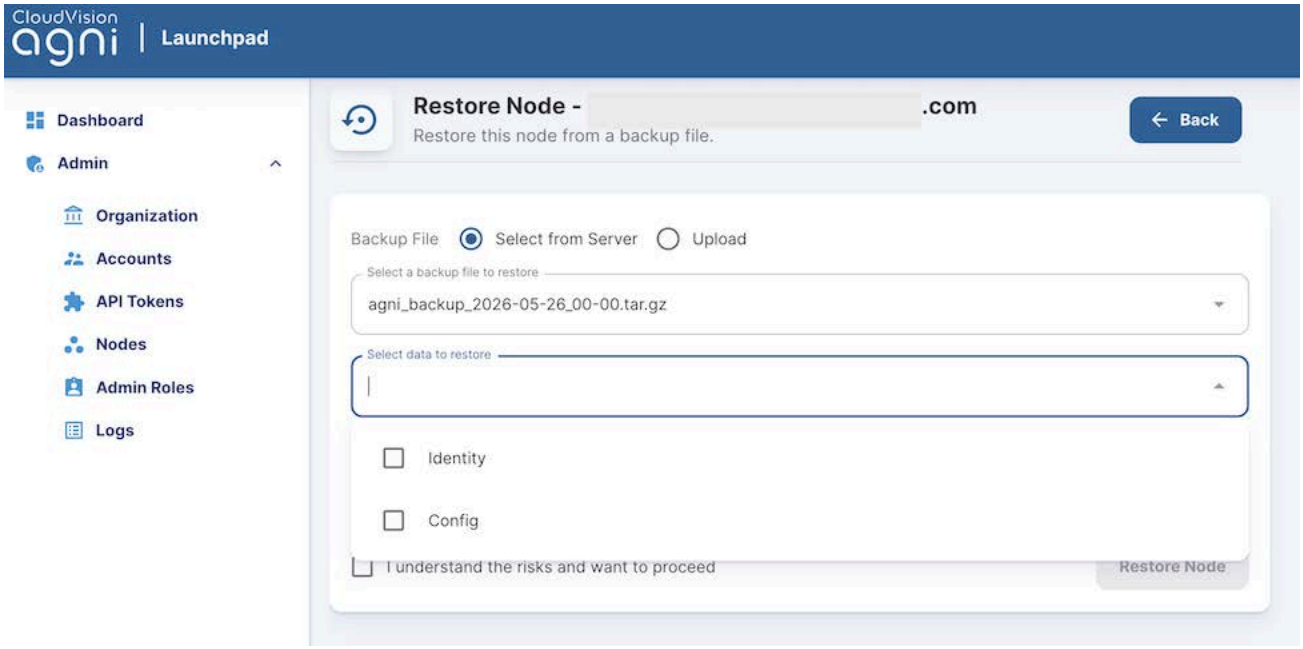
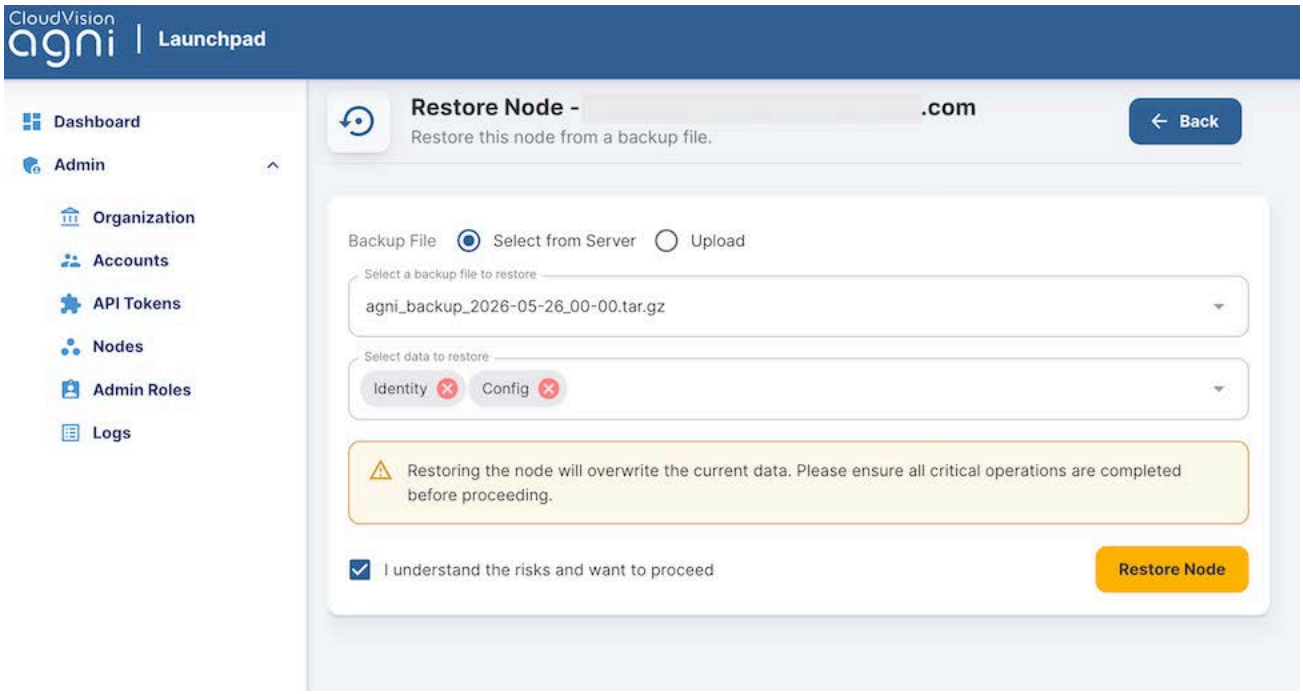


Figure 5-11: Node Restore - Select Data



Note: Restore node operation is available only on the Principal node. Restoring the node overwrites the existing data and hence perform this action with caution.

Figure 5-12: Restore Node after Accepting the Risk



5.4 Restarting the cluster

You can restart a node in an AGNI cluster by using the CLI or the UI.

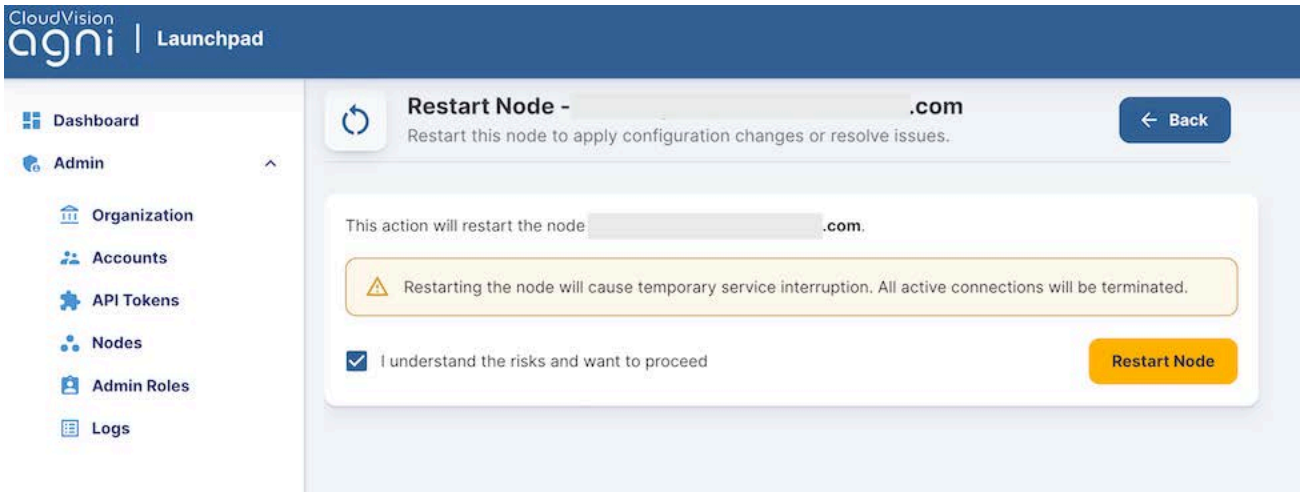
Restarting using CLI - Admin can restart the services of the nodes in the cluster for process issues or specific testing (HA testing or similar testing) using the `agni restart` command.

Note: To restart the cluster, restart all the individual nodes.

Restarting using UI: To restart a node, navigate to **Admin** > **Nodes** and click the edit icon for a desired node. In the node details page, click the **More Actions** (three dots) button and select **Restart Node**.

Note: Perform the Restart Node action with caution as it can cause temporary disruption to the services.

Figure 5-13: Restart Node



5.5 Reboot Command

The administrator can reboot a node using the `sudo shutdown -r now` command. This command reboots the node.

5.6 Shutdown Command

The administrator can gracefully shut down a node using the `sudo shutdown -f now` command.

Chapter 6

AGNI Node Replacement (RMA)

Admin can replace a faulty (RMA) node with a new one using the `agni drop` and `agni join` commands.



Note: AGNI nodes participating in a cluster should use the same AGNI software version.

Chapter 7

FAQs and Troubleshooting

This section covers some of the FAQs and troubleshooting details while setting up AGNI:

7.1 How to synchronize time on an AGNI node?

You can synchronize time on an AGNI node by using one of the following options:

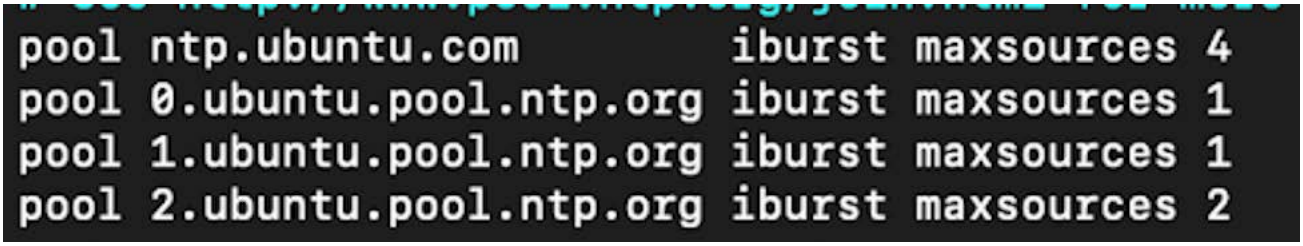
- Time synchronization using **Chrony**
- Time synchronization Using **timedatectl**

Option 1: Time synchronization using Chrony

- Update **chrony** with the correct NTP server by editing the /etc/chrony/chrony.conf file and providing the correct NTP server details. For example, *ntp.ubuntu.com*.

```
sudo vi /etc/chrony/chrony.conf
```

Figure 7-1: NTP Server Details



- Restart **chrony**.

```
sudo systemctl restart chronyd.service
```

Check if NTP is synchronized:

```
timedatectl status
                               Local time: Wed 2026-01-07 06:38:15 UTC
                               Universal time: Wed 2026-01-07 06:38:15 UTC
                               RTC time: Wed 2026-01-07 06:38:15
                               Time zone: UTC (UTC, +0000)
                               System clock synchronized: yes
                               NTP service: active
                               RTC in local TZ: no
```

Option 2: Time synchronization Using timedatectl

- When using **timedatectl** method, you must download and install the `timedatectl` Debian package from AGNI repository using the command below, if the required components are not installed on the server.

```
wget https://storage.googleapis.com/agni-prod-public/agni-repo/apt/systemd-timesyncd_amd64.deb
 && sudo apt -y remove chrony && sudo dpkg -i systemd-timesyncd_amd64.deb
```

- Edit the */etc/systemd/timesyncd.conf* file with sudo and update section below:

```
sudo vi /etc/systemd/timesyncd.conf
                        ---------------------
                        [Time]
                        NTP=<PRIMARY NTP SERVER>
                        FallbackNTP=<SECONDARY NTP SERVER (Optoonal)>
                        #RootDistanceMaxSec=5
                            #PollIntervalMinSec=32
                            #PollIntervalMaxSec=2048
```

- Restart **timedatectl** service:

```
sudo timedatectl set-ntp true
                        sudo systemctl restart systemd-timesyncd
```

- Check if NTP is synchronized:

```
timedatectl status
                        Local time: Wed 2026-01-07 06:38:15 UTC
                        Universal time: Wed 2026-01-07 06:38:15 UTC
                        RTC time: Wed 2026-01-07 06:38:15
                        Time zone: UTC (UTC, +0000)
                        System clock synchronized: yes
                        NTP service: active
                        RTC in local TZ: no
```

7.2 Error During Bootstrapping Due to Incorrect Docker Version

In rare cases, the `wget` operation can fail due to an incorrect docker version. The error in the `pre-update.log` file is as follows:

```
2025/12/30 19:05:09 INFO bootstrap(script) - waiting for 5 sec,reason=docker-registry restart
                2025/12/30 19:05:14 INFO bootstrap(script) - pushing image to registry,
 image=localhost:5000/redis:7.2.5
                The push refers to repository [localhost:5000/redis]
                09f376ebb190: Waiting
                3d36c165ff0a: Waiting
                3eba9ec960aa: Waiting
                9ae6a7172b01: Waiting
                493d196d734f: Waiting
                4f4fb700ef54: Waiting
                2c310454138b: Waiting

                Info -> You're trying to push a manifest list/index which references multiple
 platform specific manifests, but not all of them are available locally or available to the remote
 repository.
                Make sure you have all the referenced content and try again. You can also push
 only a single platform specific manifest directly by specifying the platform you want to push
 with the --platform flag.
                NotFound: content digest sha256:484e0560ae9065cf6b739458e971cd2a13eaf44868fa4
459af87457d429fb187: not found
                2025/12/30 19:05:14 INFO bootstrap(script) - writing to console=/var/log/arista/ag
ni/cli/pre-update.console
                2025/12/30 19:05:14 INFO bootstrap(script) - \nUpdate failed. Error messages are
 captured in pre-update.log\n
                /tmp/agni_tmp_env//8031.env: line 1:  7397 Killed  show_console "$$"
                2025/12/30 19:05:14 INFO bootstrap(script) - cleaning up
```

Solution: Execute the following commands at the CLI prompt:

```
agni@bm34:~$ sudo systemctl stop docker docker-registry
                agni@bm34:~$ sudo apt-get remove -y docker-ce docker-ce-cli containerd.io docker-
buildx-plugin
                agni@bm34:~$ docker-compose-plugin

                agni@bm34:~$ sudo mv  /etc/apt/sources.list.d/docker.list.disabled /etc/apt/sour
ces.list.d/docker.list
                agni@bm34:~$ sudo apt update

                agni@bm34:~$ sudo apt-get install -y --allow-downgrades \
                docker-ce=5:28.5.1-1~ubuntu.22.04~jammy \
                docker-ce-cli=5:28.5.1-1~ubuntu.22.04~jammy \
                containerd.io=1.7.28-1~ubuntu.22.04~jammy \
                docker-buildx-plugin \
                docker-compose-plugin

                Continue even if we get below error:
                mv: cannot stat '/etc/apt/sources.list.d/docker.list.disabled': No such file or
 directory
```