DCA AGNI 100

Setup and Access Guide
CloudVision AGNI

Version P-2024.4.0

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

Contents

Chapter 1

Introduction

This document provides information for adequately trained service personnel and technicians installing and configuring the Arista CloudVision AGNI (DCS-AGNI-100) Appliance.

1.1 Prerequisites

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

Table 1: Interfaces and Services

Interface	Services
North (Data)	3rd Party Integrations, HTTPS, RADIUS, TACACS+
South (Admin)	RADIUS, CLI, Replication, TACACS+

- Static IP addresses:
  - Admin Interface (mandatory) - eno8303 / eth0 acts as a management interface
  - Data Interface (optional) - eno8403 / eth1 is a data interface.

Note: Data Interface (when configured) serves as an outgoing interface and will be used as the default gateway for the node to communicate. If this is not configured, then the admin interface will act as a default gateway for the node to communicate. This can be verified by the ip route command.

- Create DNS entries for the host-name FQDNs to be assigned to AGNI nodes.

  AGNI uses DNS to communicate with other nodes and register with Arista Cloud. DNS is preferred over IP addresses and must be configured before bootstrapping.

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

Table 2: Allowed URLs

Serial Number	URL
1	https://logging.googleapis.com
2	https://monitoring.googleapis.com
3	https://gkeconnect.googleapis.com
4	https://www.googleapis.com
5	https://oauth2.googleapis.com
6	https://cloudresourcemanager.googleapis.com
7	https://mc.ag01c01.onprem.agni.arista.io
8	https://mc.ag03s01.onprem.agni.arista.io
9	https://prod-registry-k8s-io-us-east-2.s3.dualstack.us-east-2.amazonaws.com
10	https://registry.k8s.io
11	https://us-south1-docker.pkg.dev
12	https://gcr.io
13	https://gkehub.googleapis.com
14	https://storage.googleapis.com/agni-prod-public/agni-repo/ubuntu
15	https://api.fingerbank.org/api/v2
16	https://download.docker.com
17	https://securetoken.googleapis.com
18	https://servicecontrol.googleapis.com
19	https://serviceusage.googleapis.com
20	https://motd.ubuntu.com
21	https://storage.googleapis.com
22	https://compute.googleapis.com
23	https://iam.googleapis.com
24	https://dl.google.com

Note: The node establishes a control channel with Arista Cloud for management and troubleshooting purposes. The Arista SRE can monitor appliance health through the channel. Hence, outbound internet connectivity is a must for the node's operation.

- 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

- NTP server:

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

- Customer account provisioning:

  Arista SRE will do this before the customer receives the appliance. Ensure you have the account details ready, as this will be prompted as part of the bootstrapping process. If this process has not been completed already, work with your account team.

- Email address (individual or group):

  AGNI sends login credentials, password tokens, and update details to the registered email address. This will be prompted during the bootstrapping process and hence provide an email address to which you have access.

1.2 Rack Mounting of the Appliance

Rack mount the AGNI server using the sliding rack mounting rails. For details, see the QSG for DCA-AGNI-100 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-100 on the Arista Product Documentation page under the *CloudVision Appliance* table.

Chapter 2

Post Installation - AGNI Set Up

This section describes the setup and configuration details after the installation of DCA-AGNI-100 appliance.

2.1 Confirmation of Account in Arista Cloud for AGNI

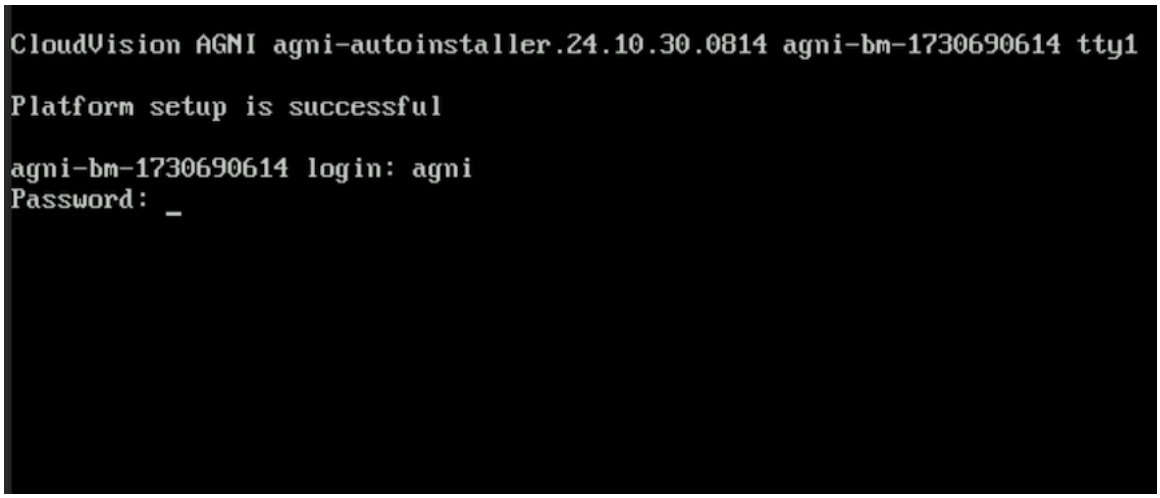
After receiving a request from the field, the AGNI Cloud team will create an Arista Cloud account for AGNI. An email is sent to your registered email address with the details of next steps to follow for registering and configuring AGNI.

2.2 Login Credentials

The default credentials for the AGNI appliance node are:

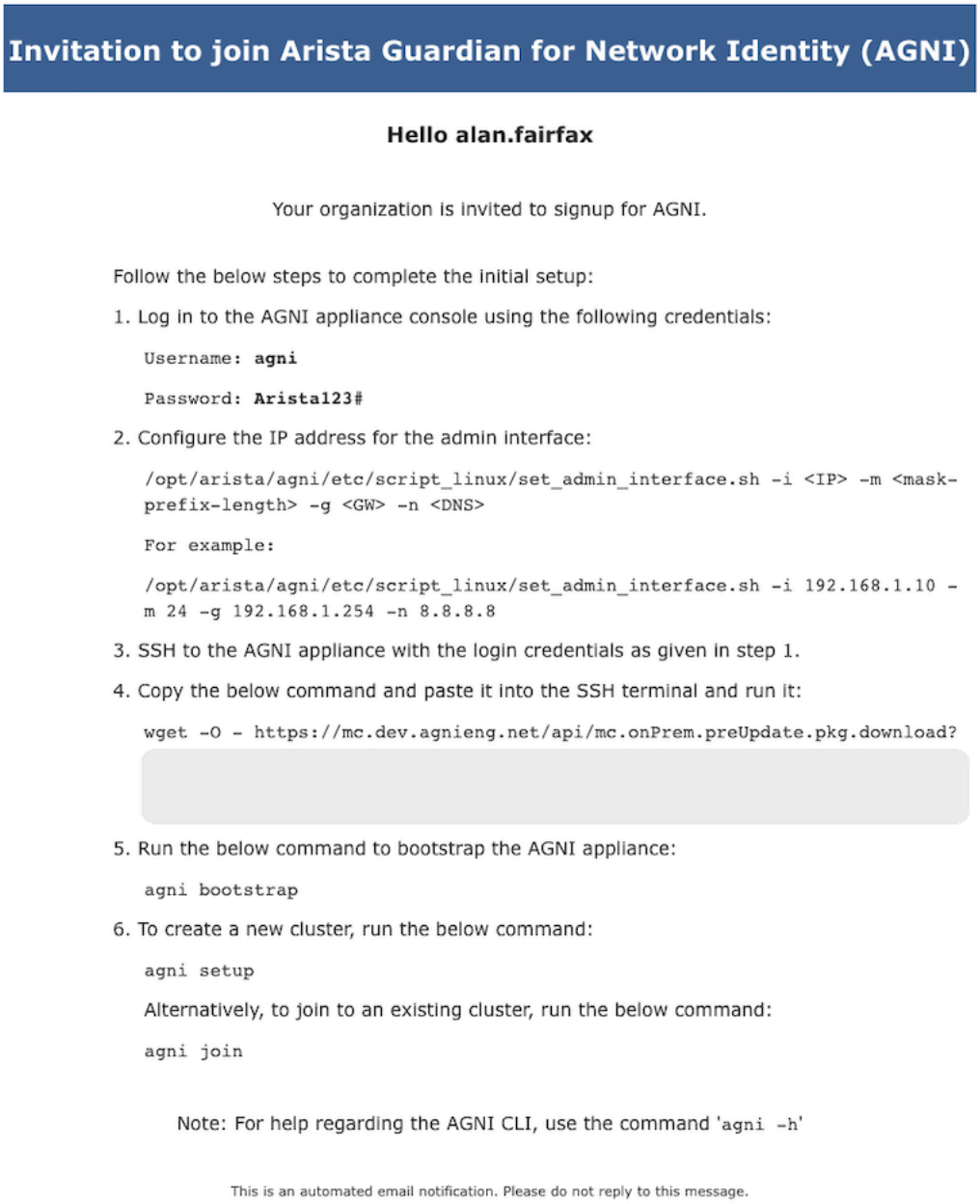
- Username: **agni**
- Password: **Arista123#**

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



2.3 Update the CLI

Follow the instructions in your email and execute the `wget` command to download the latest version of the CLI before bootstrapping.



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. Configure the IP address for the admin interface:

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

   For example:

   ```
   /opt/arista/agni/etc/script_linux/set_admin_interface.sh -i 192.168.1.10 -m 24 -g 192.168.1.254 -n 8.8.8.8
   ```

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

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

   ```
   wget -O - https://mc.dev.agnieng.net/api/mc.onPrem.preUpdate.pkg.download?
   ```

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

   ```
   agni bootstrap
   ```

6. 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.

After the CLI is updated, follow the bootstrap and setup commands to proceed with the cluster configuration.

2.4 Bootstrap Configuration

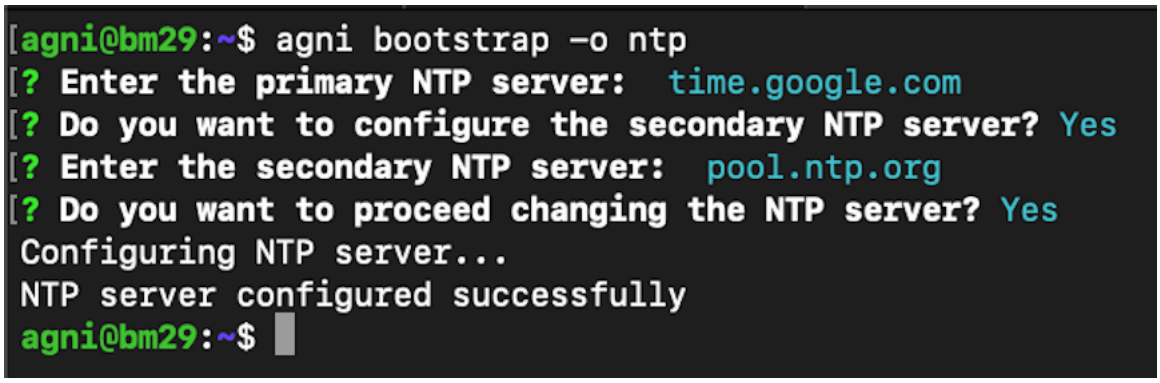
agni bootstrap—This command assists in configuring the appliance with system and network information and completing the bootstrapping process. After this command is completed, the system should be accessible over the network and ready to be set up.

```
[agni@agni-bm-1740163003:~$ agni bootstrap
[? Enter the current password:  [? for help] **********
[? Enter the new password:  [? for help] **********
[? Confirm the password:  [? for help] **********
[? Enter the FQDN(This cannot be changed later):  bm29.[redacted]com
[? Enter the Admin interface IPv4 address:  10.[redacted].29
[? Enter the Admin interface subnet mask:  255.255.255.192
[? Enter the Admin interface default gateway:  10.[redacted].1
[? Do you want to configure the Data interface? Yes
[? Enter the Data interface IPv4 address:  10.[redacted].91
[? Enter the Data interface subnet mask:  255.255.255.192
[? Enter the Data interface default gateway:  10.[redacted].65
[? Enter the DNS server(s):  10.[redacted].56
[? Enter the primary NTP server:  time.google.com
[? Do you want to configure the secondary NTP server? No
[? Do you want to proceed with the bootstrap? Yes
OS configuration is in progress...
CLI password for the user 'agni' changed successfully
Hostname configured successfully
Admin interface IP address configured successfully
DNS server configured successfully
Data interface IP address configured successfully. Reboot the system
NTP server configured successfully
Bootstrap completed
agni@agni-bm-1740163003:~$
```

Note: Ensure that Network Time Protocol (NTP) is synchronized by executing the command `timedatectl status` after running `agni bootstrap` command.

```
[agni@bm32:~$ timedatectl status
               Local time: Wed 2025-02-05 18:55:45 UTC
           Universal time: Wed 2025-02-05 18:55:45 UTC
                 RTC time: Wed 2025-02-05 18:55:45
                Time zone: UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
agni@bm32:~$
```

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


agni@bm29:~$ agni bootstrap -o ntp
[? Enter the primary NTP server: time.google.com
[? Do you want to configure the secondary NTP server? Yes
[? Enter the secondary NTP server: pool.ntp.org
[? Do you want to proceed changing the NTP server? Yes
Configuring NTP server...
NTP server configured successfully
agni@bm29:~$

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 assists in setting up the AGNI node as the Principal node. The Principal is the primary node in an AGNI cluster. Only one node acts as a Principal node. With Admin privileges, provide the registered email address which can be used to identify the node and the cluster respectively. This command takes approximately 30 minutes to complete. After the completion of the command, AGNI is set up and will be operational.

```
[agni@bm29:~$ agni setup
[? The node will be setup as Principal. Do you want to proceed? Yes
 Starting setup
[? Enter the registered email:  alan.fairfax@antaraaieng.onmicrosoft.com
[? Enter the OTP:  [? for help] **********
 OTP authentication complete
 [1/6] Checking pre-setup configuration
 [2/6] Creating the cluster. The operation may take ~30 mins to complete
 [3/6] Configuring the cluster network
 [4/6] Configuring the infrastructure services
 [5/6] Configuring the application services
 [6/6] Configuring the log service
 Attempting to restart the node now. The operation may take upto 10 minutes
 Restart completed successfully.
 Setup completed successfully
 agni@bm29:~$
```

3.2 Joining other nodes to cluster

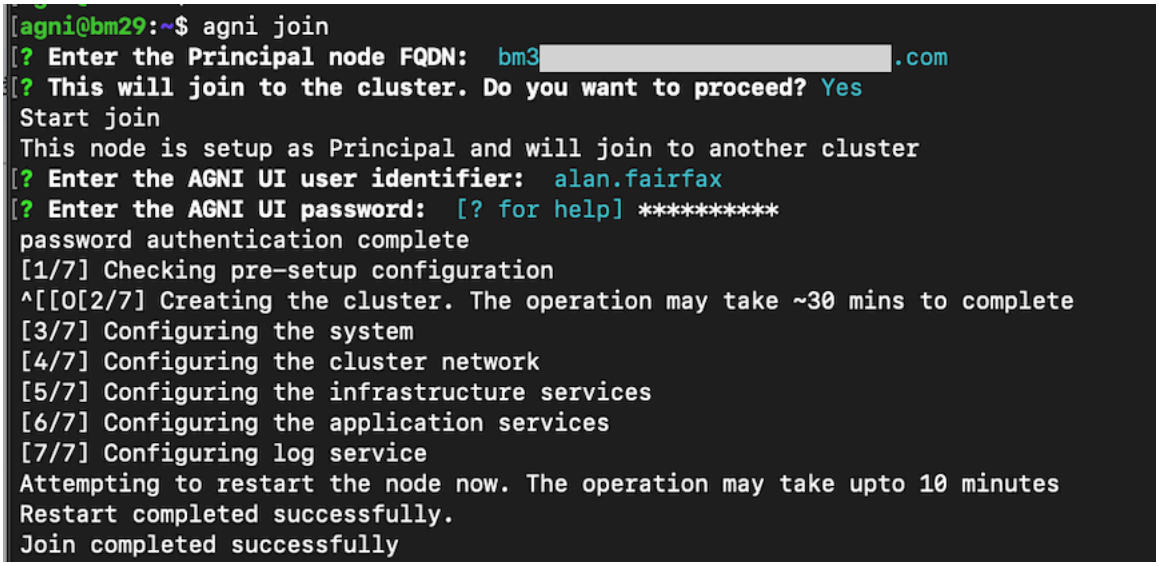
After configuring the Principal node, add multiple nodes into that cluster using the `agni join` command. These additional nodes act as standby node and auxiliary nodes.

3.2.1 Standby/Auxiliary Node Setup

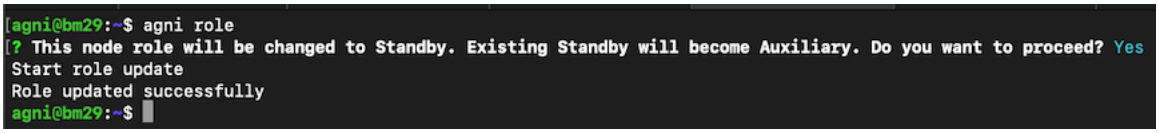
`agni join` - This command assists in setting up AGNI nodes either as Standby or Auxiliary nodes. Only one node acts as a Standby node in the AGNI cluster. There can be multiple Auxiliary nodes. The first node that joins the Principal node becomes the Standby node and the following nodes become Auxiliary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

- Principal node host FQDN
- Admin credentials of the Principal node

This operation takes about 30 minutes to complete. After the command is completed, the current AGNI node will be clustered.

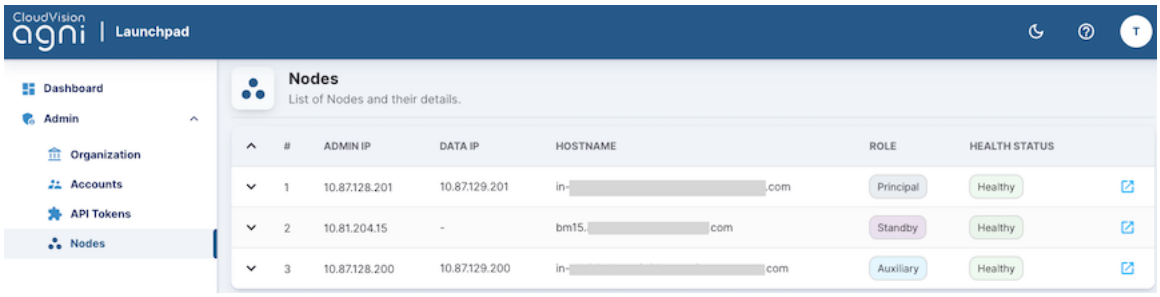


Admin can change the Auxiliary node role to Standby using the agni role command. The instance on which this command is executed becomes the new Standby node. In a cluster, if an existing node acts as a Standby and the admin executes this command on another node, then the new node becomes the Standby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



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

The cluster details with the Principal, Standby, and Auxiliary nodes are listed under the Nodes.



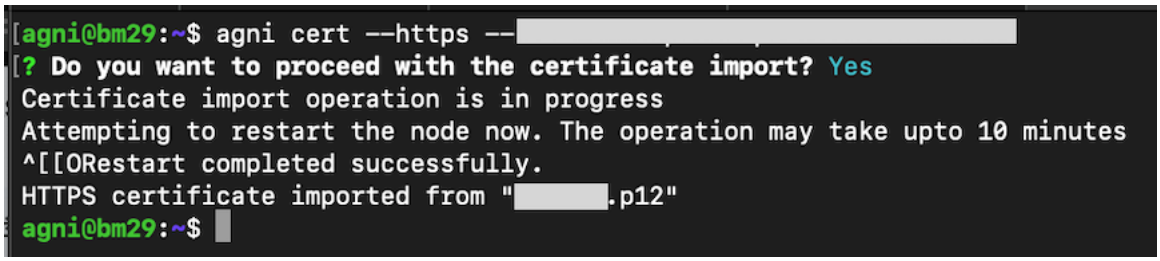
3.3 SSL signed cert upload for UI

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

Login to **each** AGNI server to import the HTTPS certificate to AGNI:

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

An example of a cert import:



3.4 Modifying the Cluster

Admin can modify the cluster by adding a new Auxiliary node or by changing the Standby node.

Use the `agni join` command to add multiple Auxiliary nodes to the cluster. Create a new Standby by using the `agni role` command.

If the Principal node goes down, the admin must promote the Standby node as the Principal node using the `agni promote` command. This command works only on the Standby node. After executing this command, the existing Principal node is removed from the cluster, and the Standby node is promoted to the new Principal node. Use the `agni role` command on an Auxiliary node to create a new Standby node in the cluster.

3.4.1 Removing Nodes from the Cluster

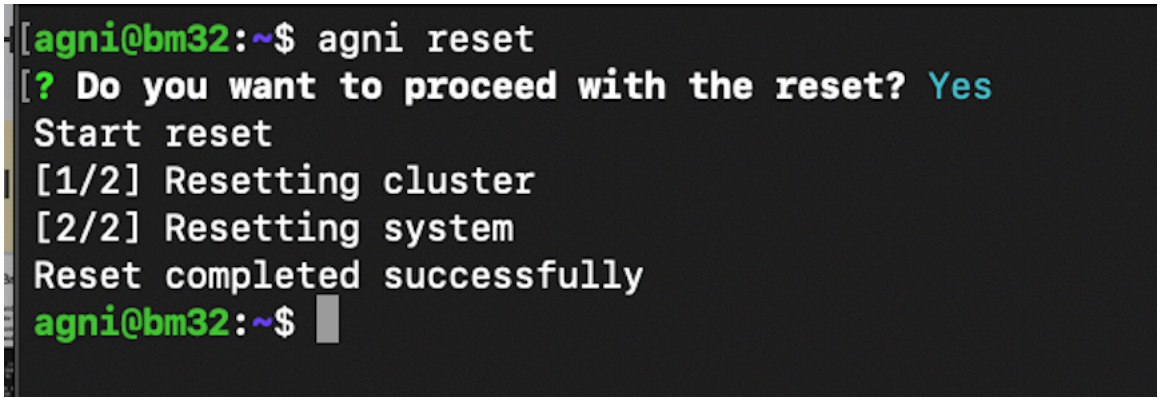
Admin can remove a node from the cluster by using the two commands: `agni drop` and `agni reset`.

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.

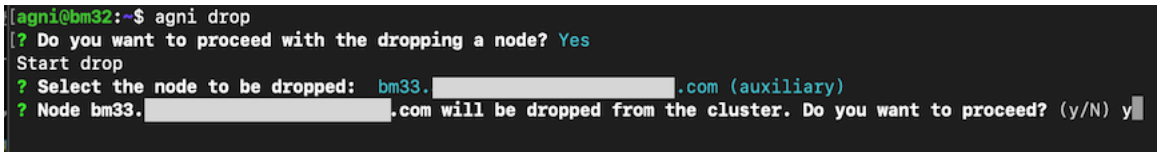


3.4.1.2 AGNI Drop Command

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.

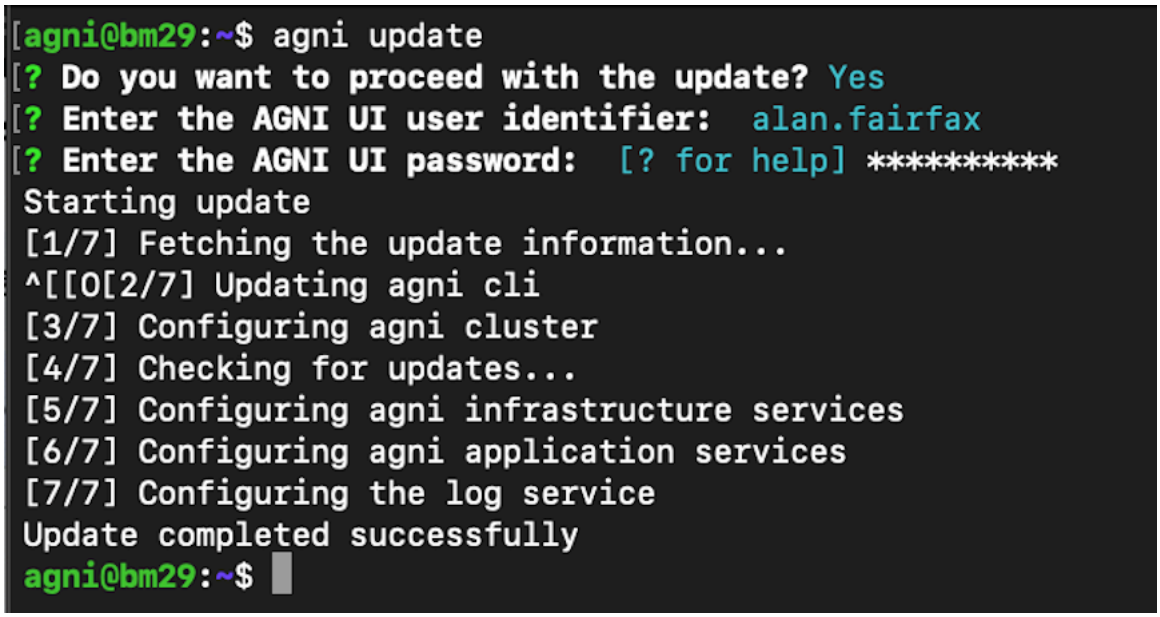
Note: The CLI password is reset to the default '**Arista123#**' after the node is dropped.



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

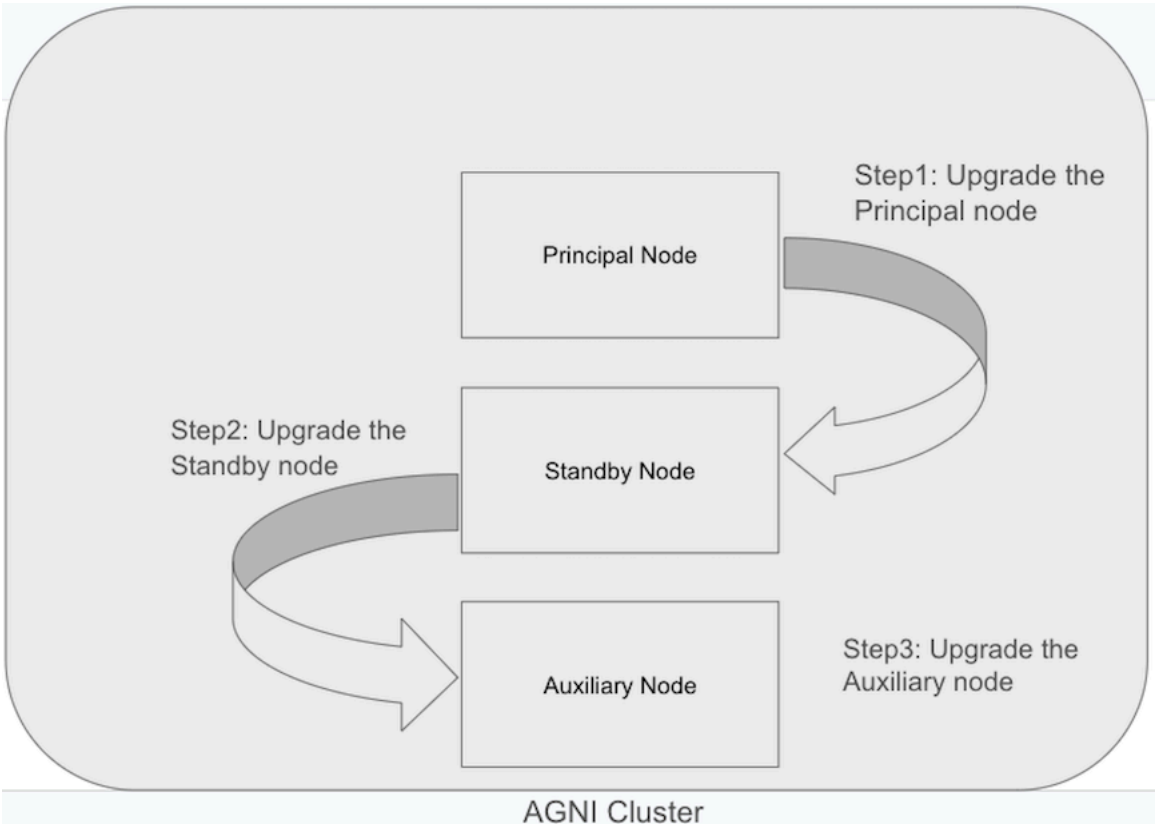
3.5 AGNI Update Command

The `agni update` command is used to update the AGNI version. All nodes will fetch updates from the cloud individually.



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


Step1: Upgrade the Principal node
Principal Node
Step2: Upgrade the Standby node
Standby Node
Auxiliary Node
Step3: Upgrade the Auxiliary node
AGNI Cluster

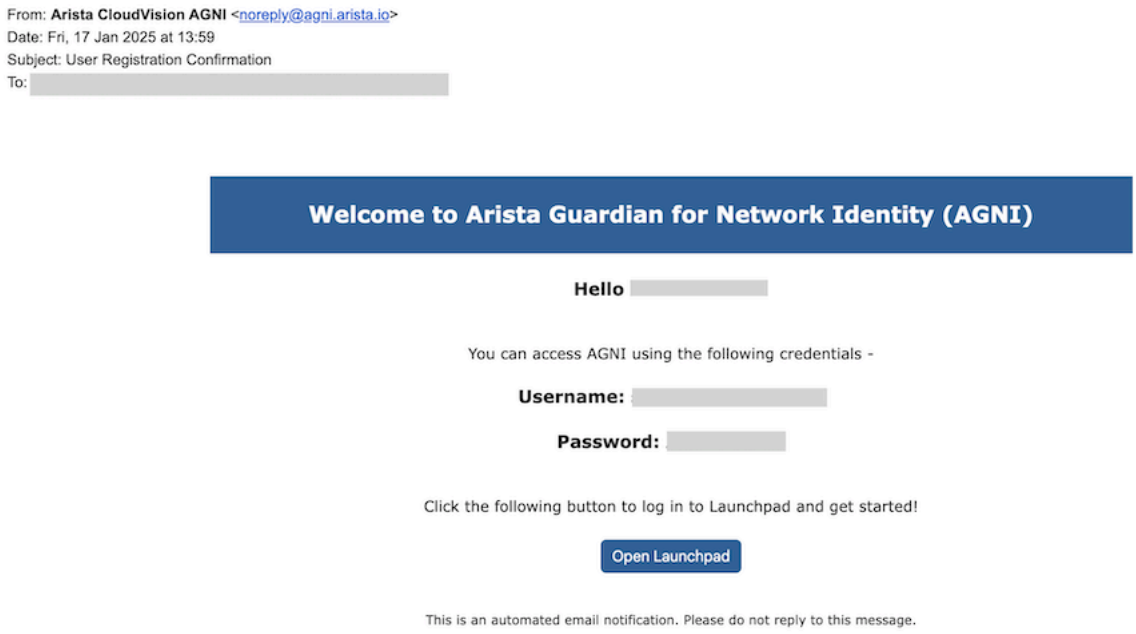
Chapter 4

Organization Login

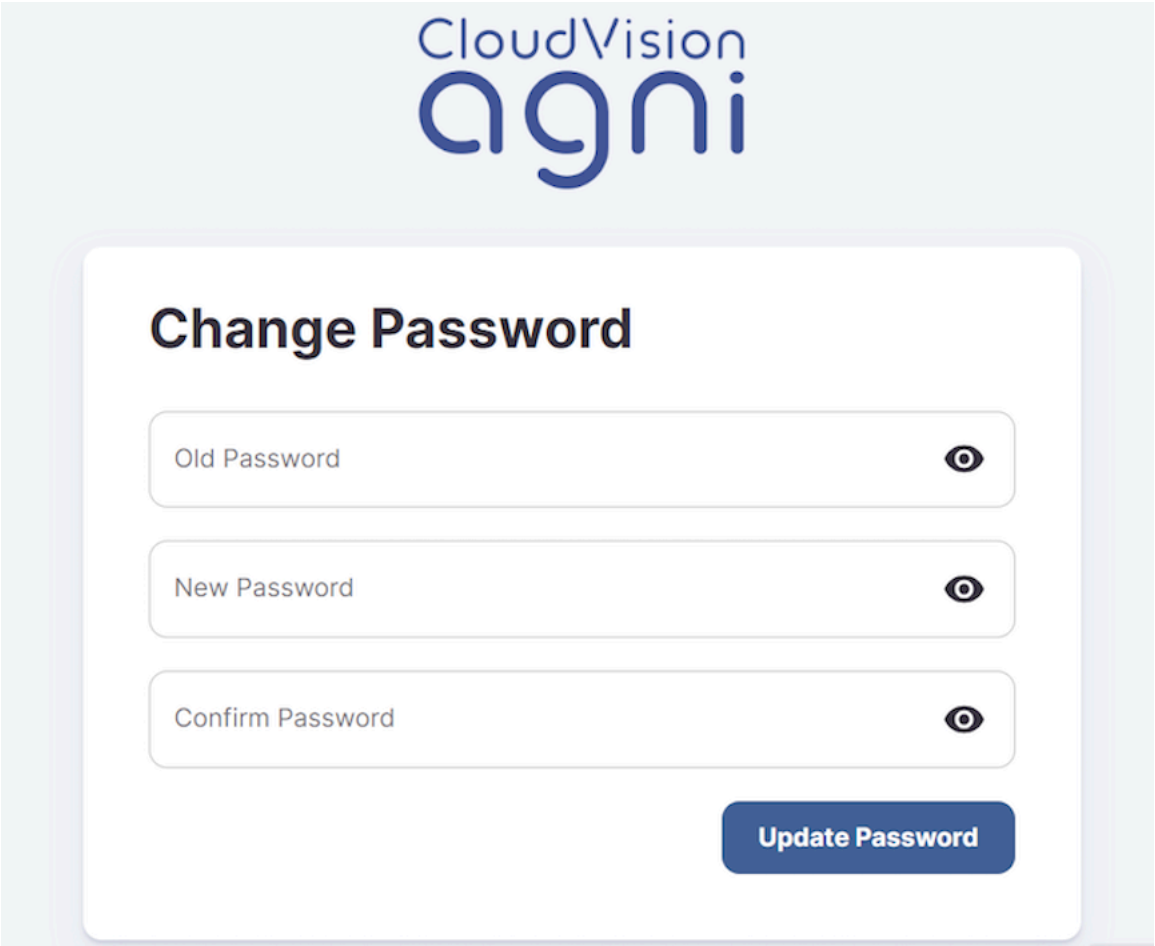
This section describes the different login methods and the API token generation process:

4.1 Local User Login

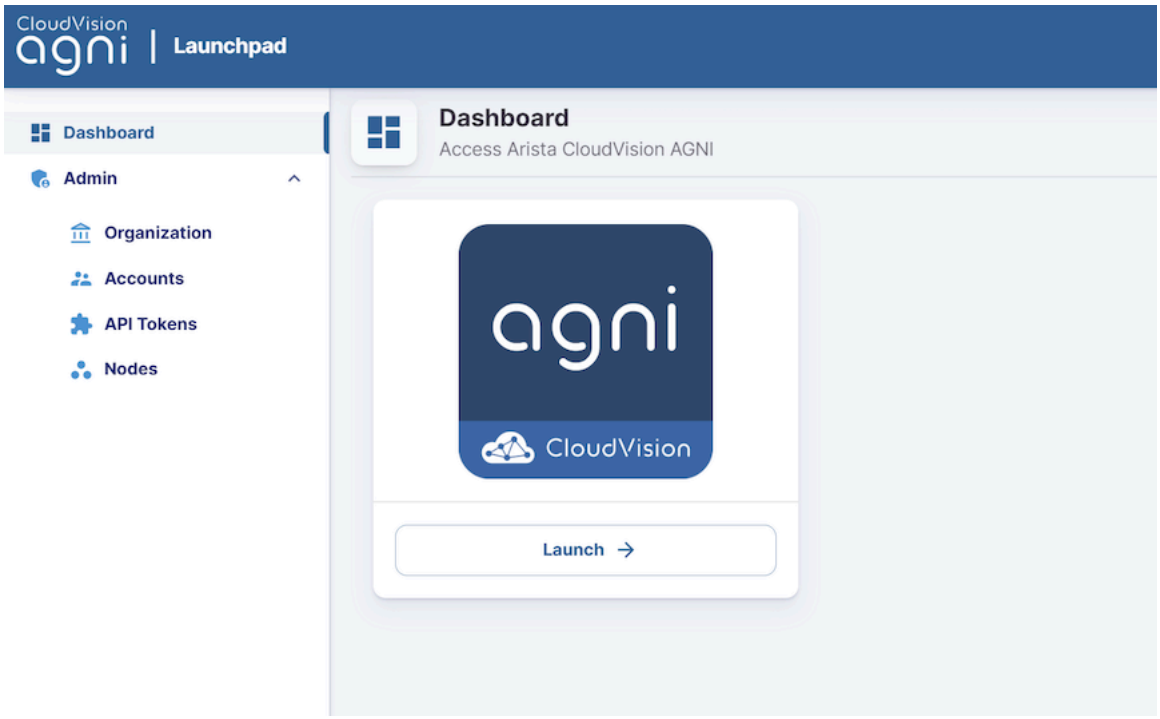
- Once setup is complete, as described in the earlier section, the admin user receives an email with login credentials.
- Click the **Open Launchpad** button, to take you to the Login URL.
- Provide Username & Password shared in the email for successful login.



After successful login, change the password credentials:



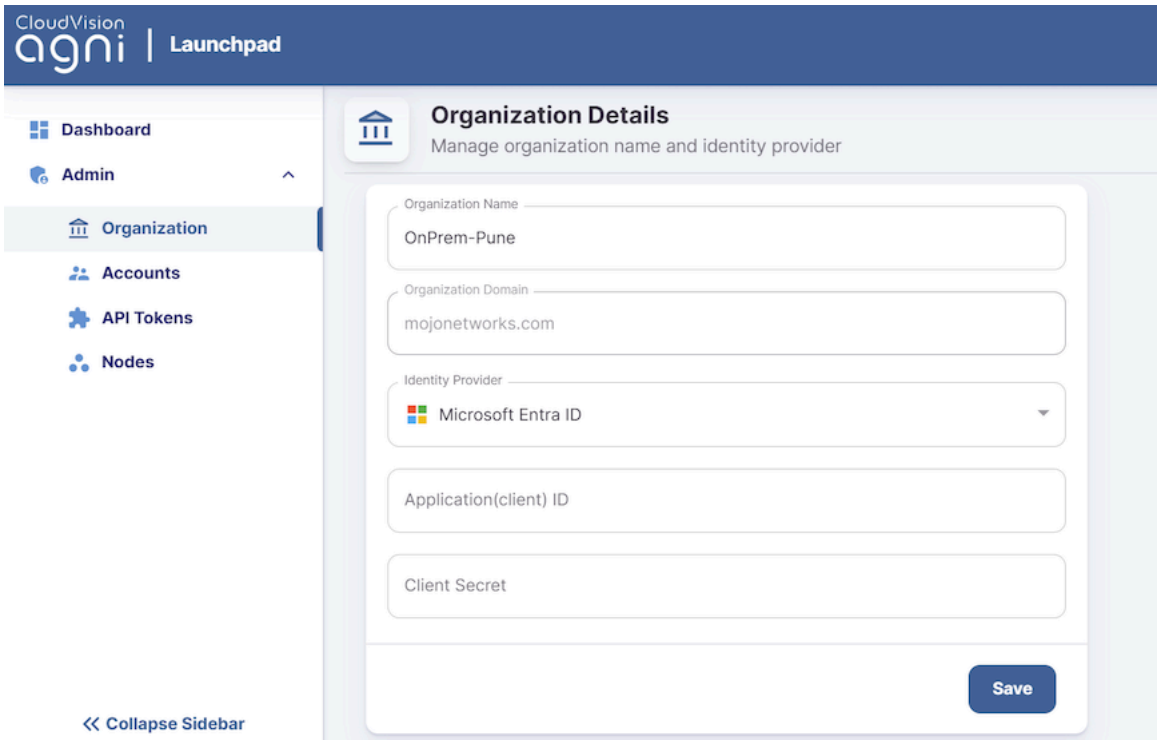
Once the password is changed, the user is redirected to the AGNI Launchpad.



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

4.2 IDP Admin User Login

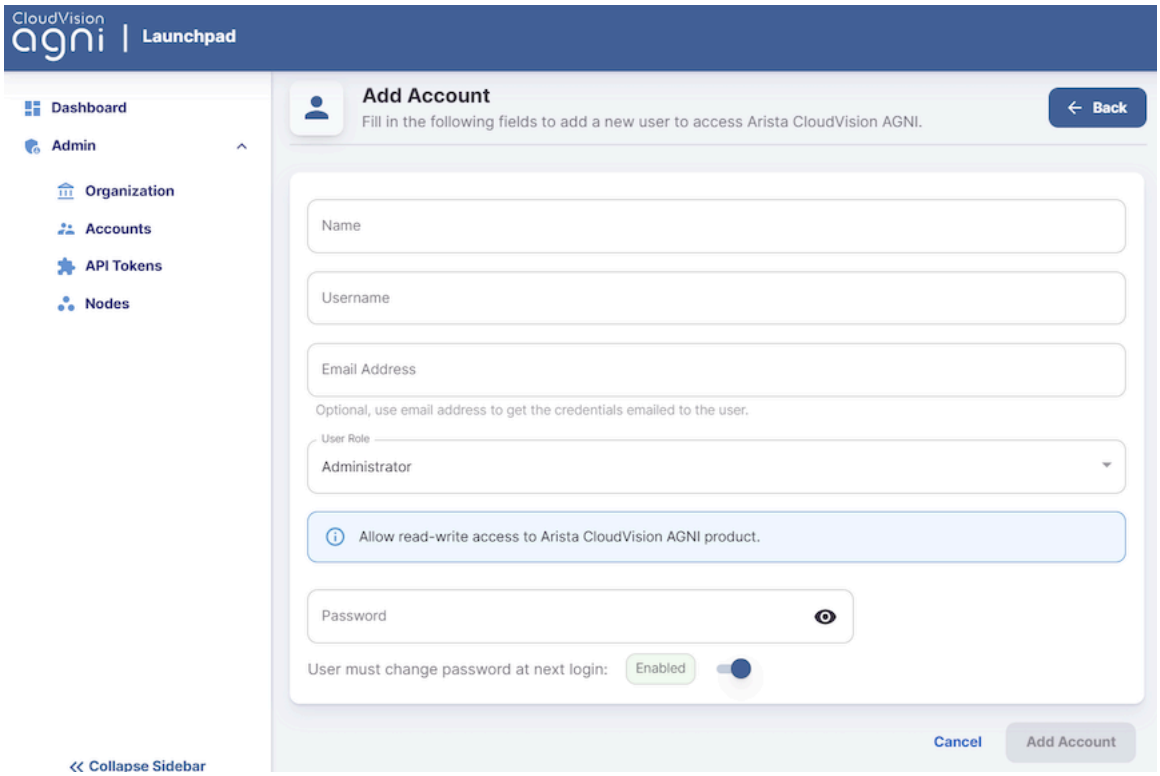
- After you log in as a Local user, navigate to **Admin** > **Organization** and provide the required **Client ID** and **Client Secret** for the IDP user to log in successfully.



- 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** option.
- Admin can add a user with different user roles by providing the username, email address, and password.

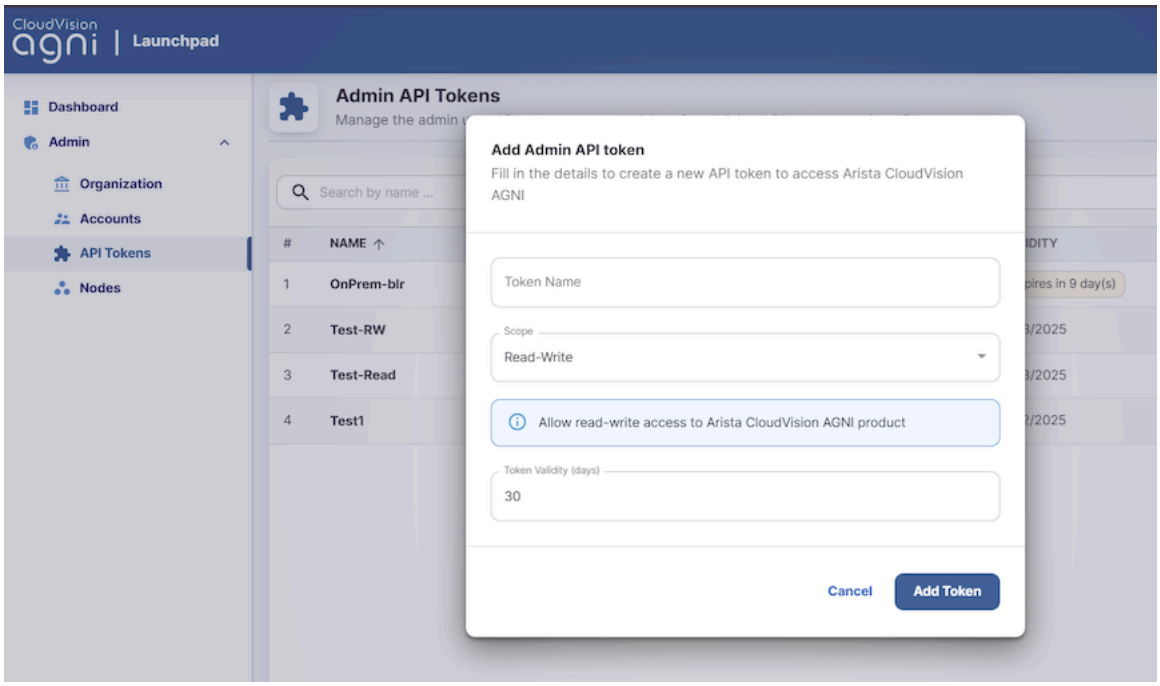


- Super-admin can add, modify, or delete the local user accounts from the user listing.

  (Administrator and Operator user roles cannot access the Admin tab from AGNI launchpad).

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
Dashboard
Admin
Organization
Accounts
API Tokens
Nodes
Admin API Tokens
Search by name ...
NAME
1 OnPrem-blr
2 Test-RW
3 Test-Read
4 Test1
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

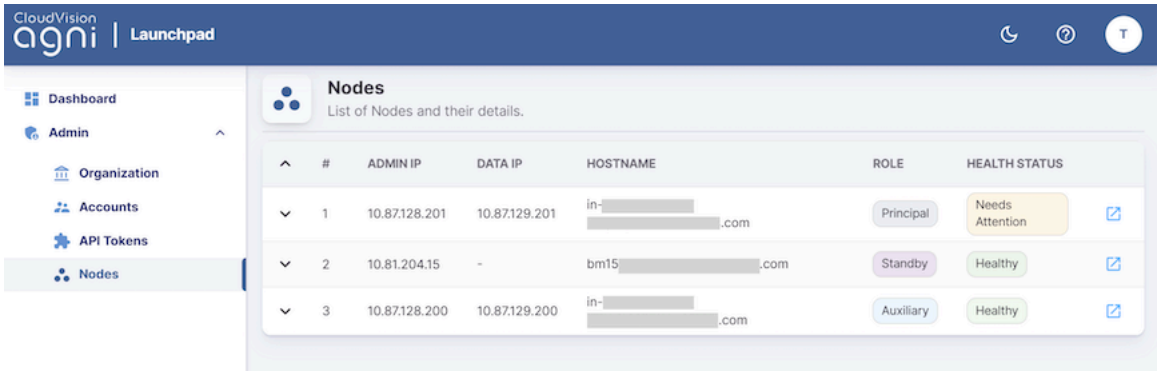
This section describes the AGNI backup, restore, reboot, and shutdown process:

5.1 Monitoring the Cluster

Admin can monitor the cluster health using UI. Login to AGNI UI and navigate to **Admin** > **Nodes**. This tile displays the nodes from the cluster and the health of these nodes. There are three types of node health:

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.



5.2 AGNI Backup Command

The `agni backup` command allows the admin to take the database backup on the AGNI node. This command allows the user to select the activity, identity, and configuration backup. The user can take a backup of all of them. The admin needs to take a backup of each node in the cluster. There are no service disruptions while taking the database backup.

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
```

5.3 AGNI Restore Command

Admin can restore the database backup on the AGNI node using the `agni restore` command. This command restores the configuration and identity backups on the node. Admin can choose the type of database to restore on the Principal node.

Use the Principal node backup file to restore it to the Principal node to have a cluster restore as identity and configuration backups will be replicated on the Standby and Auxiliary nodes of the cluster.

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:~$
```

5.4 Restarting the cluster

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.

5.5 Reboot Command

Admin can reboot the node using the `sudo shutdown -f now` command. This command reboots the node.

5.6 Shutdown Command

Admin can gracefully shut down the node using the `sudo shutdown -r 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.