

ARISTA

DCA AGNI 100

Setup and Access Guide CloudVision AGNI

Version P-2025.2.0



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

© 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..... 1
 - 1.2 Rack Mounting of the Appliance..... 3
 - 1.3 Configuring the iDRAC..... 3

- Chapter 2: Post Installation - AGNI Set Up..... 4**
 - 2.1 Account Confirmation in Arista Cloud for AGNI..... 4
 - 2.2 Login Credentials..... 4
 - 2.3 Check Time Synchronization..... 4
 - 2.4 Update the CLI..... 5
 - 2.5 Bootstrap Configuration..... 7

- Chapter 3: Cluster Configuration..... 12**
 - 3.1 Principal Node Setup..... 12
 - 3.2 Joining other nodes to cluster..... 12
 - 3.2.1 Standby/Auxiliary Node Setup..... 13
 - 3.3 SSL signed cert upload for UI..... 14
 - 3.4 Modifying the Cluster..... 14
 - 3.4.1 Removing Nodes from the Cluster..... 14

- Chapter 4: Organization Login.....21**
 - 4.1 Local User Login..... 21
 - 4.2 IDP Admin User Login..... 23
 - 4.3 Local Account User Creation..... 23
 - 4.4 API Token Generation.....24

- Chapter 5: Maintaining the Cluster..... 26**
 - 5.1 Monitoring the Cluster..... 26
 - 5.2 AGNI Backup Command..... 26
 - 5.3 AGNI Restore Command..... 27
 - 5.4 Restarting the cluster..... 27
 - 5.5 Reboot Command.....27
 - 5.6 Shutdown Command..... 27

- Chapter 6: AGNI Node Replacement (RMA)..... 28**

- Chapter 7: FAQs and Troubleshooting.....29**
 - 7.1 How to synchronize time on an AGNI node?..... 29
 - 7.2 When Customer Network Uses Same network as AGNI Docker?..... 30
 - 7.3 Error During Bootstrapping Due to Incorrect Docker Version..... 32

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-bound (Data)	3rd Party Integrations, HTTPS, RADIUS, RadSec, TACACS+
South-bound (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: The IP addresses of the Admin Interface and Data Interface should be from different Subnets.



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

- 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 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.

Post Installation - AGNI Set Up

This section describes the set up and configuration details after installing the DCA-AGNI-100 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.

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.

```
CloudVision AGNI agni-autoinstaller.24.10.30.0814 agni-bm-1730690614 tty1
Platform setup is successful
agni-bm-1730690614 login: agni
Password: _
```

2.3 Check 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 Update the CLI

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



Note: Before running `wget` command, run the `docker version` command to check the docker version. The required docker version should be 28.x.x. A sample command output is provided below.

If the version is 29.x.x, refer to the [FAQ and Troubleshooting](#) section for the error and solution.

```
agni@bmxx:~$ docker version
Client: Docker Engine - Community
Version: 28.5.1
API version: 1.51
Go version: go1.24.8
Git commit: e180ab8
Built: Wed Oct 8 12:17:03 2025
OS/Arch: linux/amd64
Context: default

Server: Docker Engine - Community
Engine:
Version: 28.5.1
API version: 1.51 (minimum version 1.24)
Go version: go1.24.8
Git commit: f8215cc
Built: Wed Oct 8 12:17:03 2025
OS/Arch: linux/amd64
Experimental: false
containerd:
Version: v1.7.28-gke.0
GitCommit: b98a3aace656320842a23f4a392a33f46af97866
runc:
Version: 1.3.0
GitCommit: v1.3.0-0-g4ca628d1
docker-init:
Version: 0.19.0
GitCommit: de40ad0
agni@bmxx:~$
```

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/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 192.168.1.1 -m 24 -g 192.168.1.1 -n 8.8.8.8
```

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

5. 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=CiQAE  
Lh%2FMwGOXJRMU2kE0MKS5AimydXgLm7STNoze%2FYQnJQ0LLnovAgaGAoQa9qFRSE00M0WgsXs8G2mGRDXwvm  
TAW%3D%3D | bash
```

The command will expire at 25 Aug 25 13:43 UTC.

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

```
agni bootstrap
```

7. 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 set up commands to proceed with the cluster configuration.

Figure 2-1: WGET Command Output

```

agni@agni-hb-1756489771:~$ wget --no-check-certificate https://api.mc.onprem.preupdate.pkg.download7tokannC10AhQ08TLwPKUN2F0T7py0VR0CqEdynbStJ651c3M3FA0cDN2FKgY8gEqzEKFAmSu31
7ydyqozIhe3k2BE1qhkV8DEpw8Cm8w8igVauMzR1sFrofsN28fISsJPo23rPRZkuA28ti4Qdxc28
2aAHdE61M2FPRIe73DGc2DFONipyt088cECctfUCUgE1N2F2kvINGhKKEYZeSe0N2FLSyREBONFk2FS4jg05Pm2FLVAYN3D | bash
Specify target AGNI release (2024.4/2025.2) (default: 2025.2):
Selected release: 2025.2

[1/4]Checking pre-setup configuration
[2/4]Fetching update information for 2025.2
[3/4]Updating cli
[4/4]Updating images
Update completed
agni@agni-hb-1756489771:~$

```

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 networks must be customized before running the `agni bootstrap` command. For details on supported network changes and configuration steps, refer to the [FAQ and Troubleshooting](#) section.

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

Figure 2-2: Bootstrap without HTTP Proxy

```
agni@bm21:~$ 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): [redacted]networks.com
? Enter the Admin interface IPv4 address: 10.[redacted]
? Enter the Admin interface subnet mask: 255.255.255.192
? Enter the Admin interface default gateway: 10.[redacted]
? Do you want to configure the Data interface? Yes
? Enter the Data interface IPv4 address: 10.[redacted]
? Enter the Data interface subnet mask: 255.255.255.192
? Enter the Data interface default gateway: 10.[redacted]
? Enter the DNS server(s): 10.[redacted]
? Do you want to configure HTTP proxy? No
? Enter the primary NTP server: 10.[redacted]
? 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
? Enter the registered email: alan.fairfax@antaraaieng.onmicrosoft.com
? Enter the OTP: [? for help] *****
Bootstrap update started...
Bootstrap update completed successfully
Bootstrap completed
agni@bm21:~$
```

Figure 2-3: Bootstrap with Authenticated HTTP Proxy

```
agni@agni-bm-:~$ 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): networks.com
[?] Enter the Admin interface IPv4 address: 192
[?] Enter the Admin interface subnet mask: 255.
[?] Enter the Admin interface default gateway: 192
[?] Do you want to configure the Data interface? No
[?] Enter the DNS server(s): 10.
[?] Do you want to configure HTTP proxy? Yes
[?] Enter the hostname or IP address of the proxy server: 10.
[?] Enter the HTTP proxy server port : 3128
[?] Do you want to configure basic authentication Yes
[?] Enter the proxy server username: agniproxy
[?] Enter the proxy server password: [?] for help] ****
[?] Enter the primary NTP server: 10.
[?] 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
HTTP proxy configured successfully
NTP server configured successfully
[?] Enter the registered email: alan.fairfax@antaraaieng.onmicrosoft.com
[?] Enter the OTP: [?] for help] *****
Bootstrap update started...
Bootstrap update completed successfully
Bootstrap completed
agni@agni-bm-:~$
```

Figure 2-4: Bootstrap with Unauthenticated HTTP Proxy

```
[agni@bm21:~]$ 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): [redacted] networks.com
[?] Enter the Admin interface IPv4 address: 10.[redacted]
[?] Enter the Admin interface subnet mask: 255.255.255.192
[?] Enter the Admin interface default gateway: 10.[redacted]
[?] Do you want to configure the Data interface? Yes
[?] Enter the Data interface IPv4 address: 10.[redacted]
[?] Enter the Data interface subnet mask: 255.255.255.192
[?] Enter the Data interface default gateway: 10.[redacted]
[?] Enter the DNS server(s): 10.[redacted]
[?] Do you want to configure HTTP proxy? Yes
[?] Enter the hostname or IP address of the proxy server: 10.[redacted]
[?] Enter the HTTP proxy server port : 3128
[?] Do you want to configure basic authentication  No
[?] Enter the primary NTP server: 10.[redacted]
[?] 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
HTTP proxy configured successfully
NTP server configured successfully
[?] Enter the registered email: alan.fairfax@antaraaieng.onmicrosoft.com
[?] Enter the OTP: [?] for help] *****
Bootstrap update started...
Bootstrap update completed successfully
Bootstrap completed
agni@bm21:~$
```

Post-Bootstrap Validations

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

If NTP is not synchronized, run the `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:~$
```

DNS and Networking Validations

Ensure that DNS and 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
```

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.

```
[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. You can add one node as a *standby* node and can add several *auxiliary* nodes.

3.2.1 Standby/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.

```
[agni@bm29:~]$ agni join
[?] Enter the Principal node FQDN: bm3[REDACTED].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 user identifier: alan.fairfax
[?] Enter the AGNI UI password: [?] for help] *****
password authentication complete
[1/7] Checking pre-setup configuration
^[0[2/7] Creating the cluster. The operation may take ~30 mins to complete
[3/7] Configuring the system
[4/7] Configuring the cluster network
[5/7] Configuring the infrastructure services
[6/7] Configuring the application services
[7/7] Configuring log service
Attempting to restart the node now. The operation may take upto 10 minutes
Restart completed successfully.
Join completed successfully
```

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.

#	ADMIN IP	DATA IP	HOSTNAME	ROLE	HEALTH STATUS	VERSION
1	10.10.10.1	-	in-10.10.10.1.com	Principal	Healthy	P-2025.2.23
2	10.10.10.5	-	bm-10.10.10.5.com	Auxiliary	Healthy	P-2025.2.23
3	10.10.10.0	10.10.10.0	in-10.10.10.0.com	Auxiliary	Healthy	P-2025.2.19

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 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.

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:

```

[agni@bm29:~]$ agni cert --https --[redacted]
[?] Do you want to proceed with the certificate import? Yes
Certificate import operation is in progress
Attempting to restart the node now. The operation may take upto 10 minutes
^[[ORestart completed successfully.
HTTPS certificate imported from "[redacted].p12"
[agni@bm29:~]$

```

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.

```
[agni@bm32:~$ agni reset
[? Do you want to proceed with the reset? Yes
Start reset
[1/2] Resetting cluster
[2/2] Resetting system
Reset completed successfully
agni@bm32:~$
```

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.

```
[agni@bm32:~]$ agni drop
[?] Do you want to proceed with the dropping a node? Yes
Start drop
? Select the node to be dropped: [Use arrows to move, type to filter, ? for more help]
> bm29. [REDACTED].com (auxiliary)
  bm22. [REDACTED].com (auxiliary)
  bm17. [REDACTED].com (standby)
  bm18. [REDACTED].com (auxiliary)
  bm33. [REDACTED].com (auxiliary)
```

```
[agni@bm32:~]$ agni drop
[?] Do you want to proceed with the dropping a node? Yes
Start drop
? Select the node to be dropped: bm33.[REDACTED].com (auxiliary)
? Node bm33.[REDACTED].com will be dropped from the cluster. Do you want to proceed? (y/N) y
```

```
[agni@bm32:~]$ agni drop
[?] Do you want to proceed with the dropping a node? Yes
Start drop
? Select the node to be dropped: bm33.[REDACTED].com (auxiliary)
? Node bm33.[REDACTED].com will be dropped from the cluster. Do you want to proceed? Yes
Dropping node 'bm33.[REDACTED].com' from the cluster
Node 'bm33.[REDACTED].com' is successfully dropped from the cluster. Run 'agni reset' on 'bm33.[REDACTED].com' to complete the operation
Drop node successful
agni@bm32:~$
```

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.

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

Figure 3-1: AGNI Update -List Command

```
agni@bm18:~$ agni update --list
Fetching update information...

Current AGNI Release: P-2025.2
Product Version: P-2025.2.22

Applicable minor update available is P-2025.2.23

Applicable major release(s) available:

AGNI Release: P-2025.4
Description: update to 2025.4 release, without bmctl update
Release Date: August 2025

AGNI Release: P-2026.2
Description: upgrade to 2026.2 release,
Release Date: February 2026

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

agni@bm18:~$
```

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

Figure 3-2: AGNI Update - Minor Release Command

```
[agni@bm18:~]$ agni update --minorrelease
Fetching minor release update information...

Current AGNI Release: P-2025.2
Product Version: P-2025.2.22

Applicable minor update available is P-2025.2.23

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@bm18:~$ █
```

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

Figure 3-3: AGNI Update - Major Release Command

```

agni@bm19:~$ agni update --majorrelease
Fetching major release upgrade information...

Current AGNI Release: P-2024.4
Software Version: P-2024.4

Applicable major release(s) available:

AGNI Release: P-2025.2
Description: Update to 2025.2 release
Release Date: August 2025

AGNI Release: P-2025.4
Description: update to 2025.4 release, without bmctl update
Release Date: August 2025

AGNI Release: P-2026.2
Description: upgrade to 2026.2 release, with bmctl update to 1.32
Release Date: February 2026

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

? Specify the AGNI Release for upgrade: P-2025.2

WARNING: This action cannot be reverted.

? Do you want to proceed with the upgrade? Yes
[1/7] Fetching the update information...
[2/7] Updating agni cli
[3/7] Updating agni cluster
[4/7] Downloading artifacts
[5/7] Updating agni infrastructure services
[6/7] Updating agni application services
[7/7] Updating the log service
Attempting to restart the node now. The operation may take upto 10 minutes
Restart completed successfully.
Update completed successfully
agni@bm19:~$

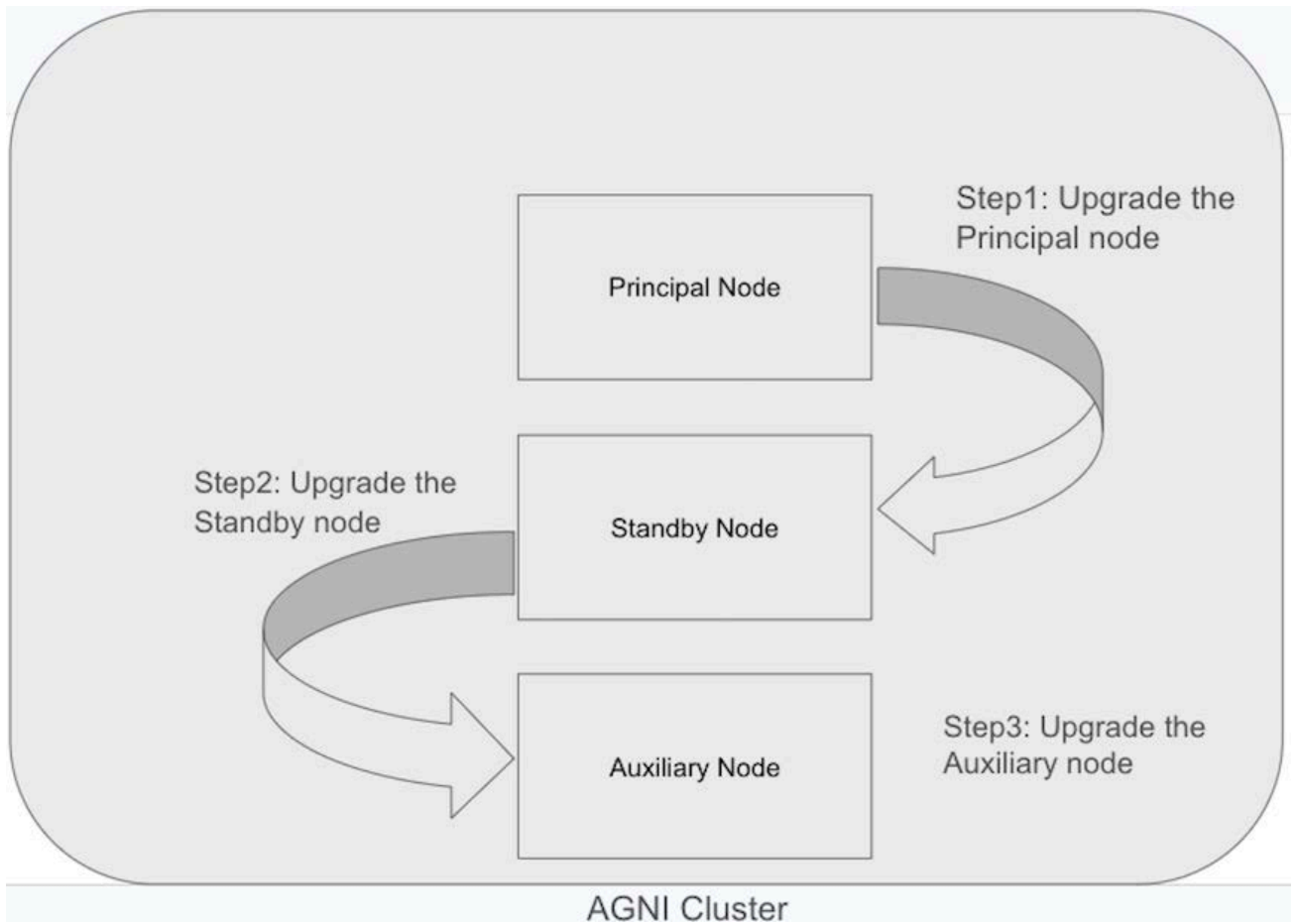
```

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 3-4: AGNI Update Flowchart



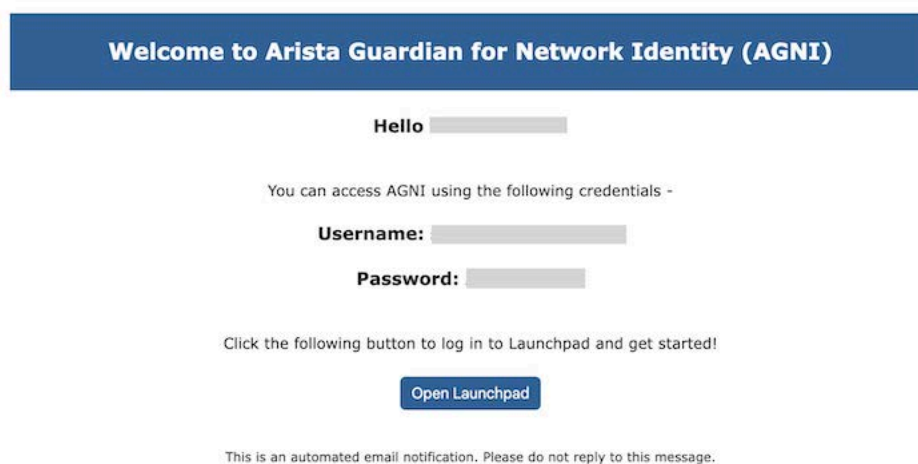
Organization Login

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

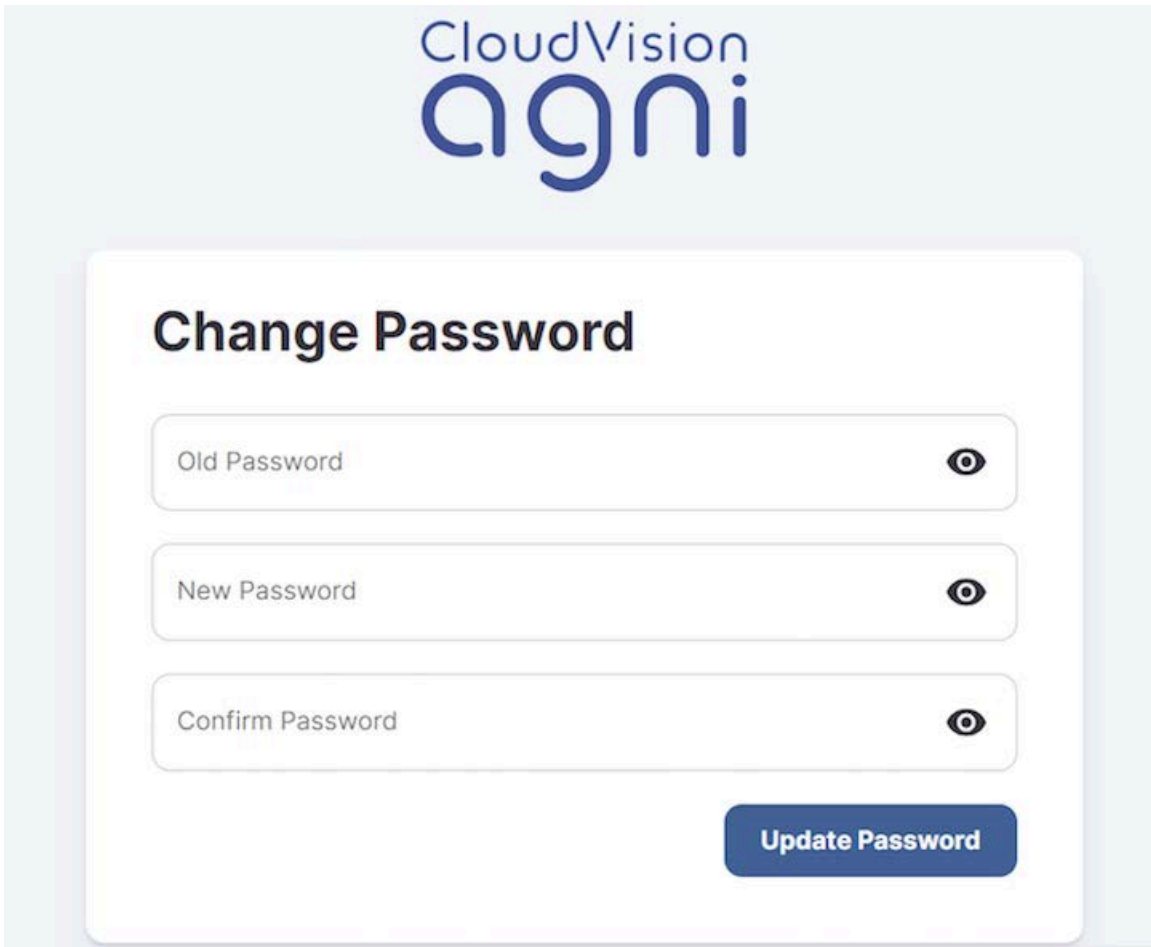
4.1 Local User Login

- 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.

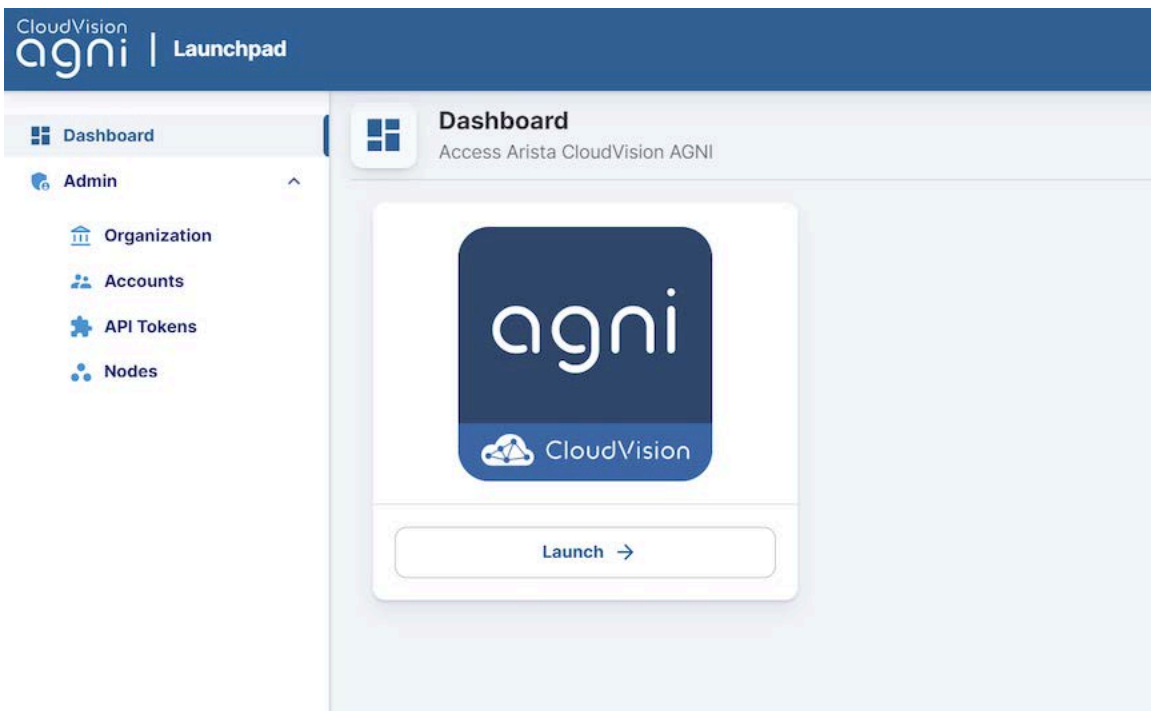
From: Arista CloudVision AGNI <noreply@agni.arista.io>
Date: Fri, 17 Jan 2025 at 13:59
Subject: User Registration Confirmation
To: [REDACTED]



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

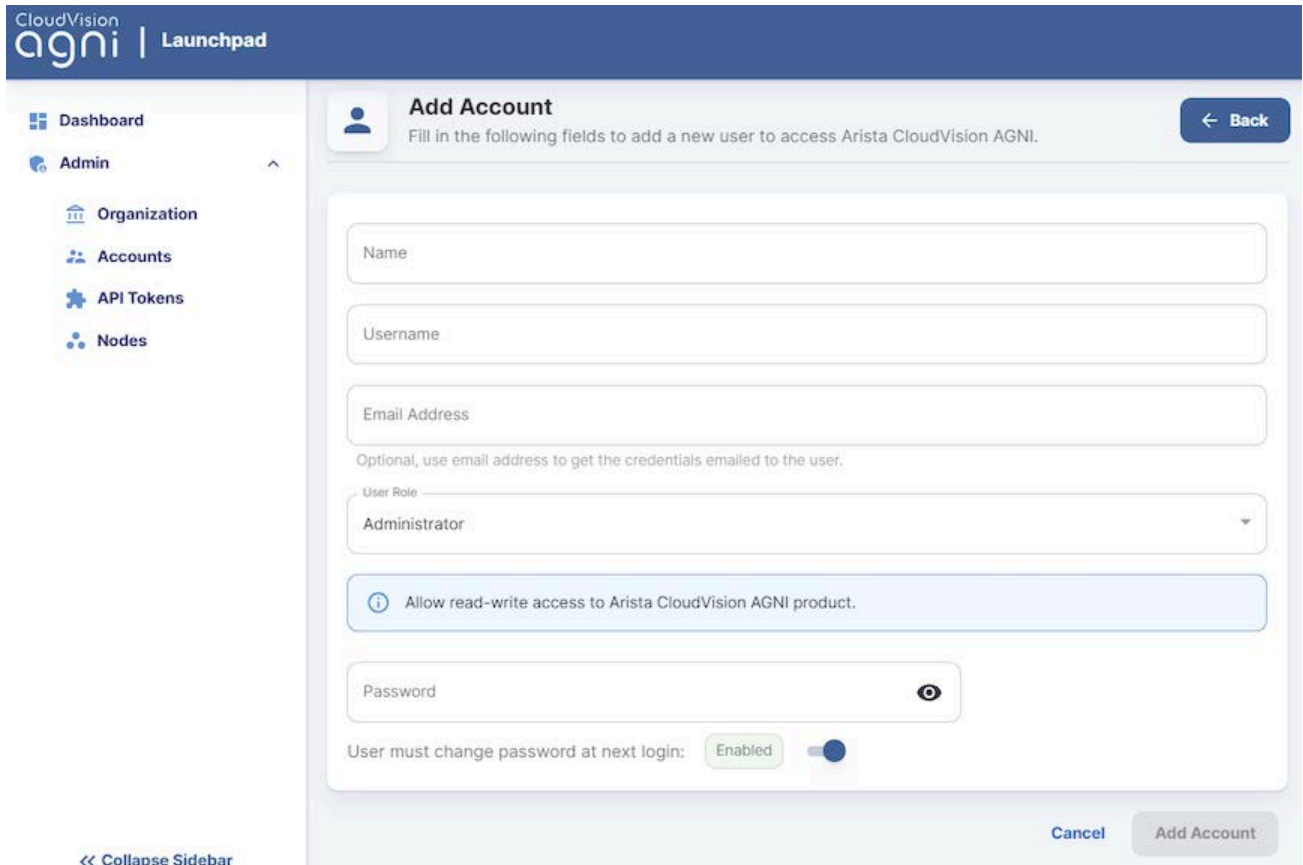
- After you log in as a Local user, navigate to **Admin > Organization** and provide the required **Client ID** and **Client Secret** for the IDP user to log in successfully.

The screenshot displays the 'Organization Details' page in the AGNI Launchpad. The page title is 'Organization Details' with a subtitle 'Manage organization name and identity provider'. The left sidebar shows navigation options: Dashboard, Admin, Organization (selected), Accounts, API Tokens, and Nodes. The main content area contains several input fields: 'Organization Name' (OnPremise Testing), 'Organization Domain' (antarabang.onmicrosoft.com), 'Identity Provider' (Microsoft Entra ID), 'Application(Client) ID' (b213aeed-b856-4c41-a895-6cd45ed186f9), and 'Client Secret' (masked with dots). Below these fields is a blue box with an information icon and text: 'Add the following URL in the sign-in redirect URI's for OIDC application. Repeat the same for each node in the cluster.' Below this text is a text input field containing 'https://bm22.agni.com/sso/login/callback' and a 'Copy' button. A 'Save' button is located at the bottom right of the form.

- 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.



- 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.

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.

The screenshot shows the 'Admin API Tokens' page in the Arista CloudVision AGNI Launchpad. A modal window titled 'Add Admin API token' is open, prompting the user to create a new API token. The modal contains the following fields and options:

- Token Name:** A text input field.
- Scope:** A dropdown menu currently set to 'Read-Write'.
- Permissions:** A checkbox labeled 'Allow read-write access to Arista CloudVision AGNI product' which is checked.
- Token Validity (days):** A text input field containing the value '30'.

At the bottom of the modal, there are two buttons: 'Cancel' and 'Add Token'.

In the background, the 'Admin API Tokens' table is visible with the following data:

#	NAME ↑
1	OnPrem-blr
2	Test-RW
3	Test-Read
4	Test1

Maintaining the Cluster

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

5.1 Monitoring the Cluster

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.



#	ADMIN IP	DATA IP	HOSTNAME	ROLE	HEALTH STATUS	VERSION
1	10.10.10.1	-	in-10.10.10.1.com	Principal	Healthy	P-2025.2.23
2	10.10.10.5	-	bm-10.10.10.5.com	Auxiliary	Healthy	P-2025.2.23
3	10.10.10.0	10.10.10.0	in-10.10.10.0.com	Auxiliary	Healthy	P-2025.2.19

5.2 AGNI Backup Command

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

```

5.3 AGNI Restore Command

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:~$
```

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

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.

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.

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

```
pool ntp.ubuntu.com iburst maxsources 4
pool 0.ubuntu.pool.ntp.org iburst maxsources 1
pool 1.ubuntu.pool.ntp.org iburst maxsources 1
pool 2.ubuntu.pool.ntp.org iburst maxsources 2
```

- 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 (Optional)>
#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 When Customer Network Uses Same network as AGNI Docker?

Customize the default networks on AGNI appliances before running `agni bootstrap` command. AGNI uses the following networks by default:

```
172.16.0.0/16  k8s Pod Network
172.17.0.0/16          Docker Bridge Network
192.168.0.0/16       k8s Node Network
10.96.0.0/20        k8s Services Network
172.18.0.0/16       Docker Kind Network
```

When the AGNI appliances are shipped, the bare metal appliances are configured with the following networks:

- Docker Bridge 172.17.0.0/16 on dev docker0
- VLAN 192.168.0.200/24 on dev eno8303.100

Customers can change the pre-configured networks if required. For example, if the customer is already using 172.17.0.0/16 or 192.168.0.0/16 network locally, follow the instructions to change the network addresses:

1. **Change Docker Bridge Network** - Change the Bridge IP address before configuring the admin interface IP address. This is required if you are using the 172.17.0.0/16 network locally.

- Verify the current appliance docker0 IP address by running `ip addr show` command:

```
$ ip addr show docker0
8: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 06:4f:9f:29:3e:c2 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::44f:9fff:fe29:3ec2/64 scope link
        valid_lft forever preferred_lft forever
```

- Check if this IP address clashes with the local network setup and then get an available alternate IP address, for example **172.20.0.1/16**.



Note: The IP address must be a host IP within the chosen subnet, not the network address itself.

- Verify the file, `/etc/docker/daemon.json` exists and has the following contents. If unavailable, create the file with the same contents as below:

```
$ cat /etc/docker/daemon.json
{
  "insecure-registries": [],
  "registry-mirrors": [],
  "insecure-registries": ["localhost:5000"]
}
```

- Copy and run the following code after changing the value of **NEW_IP**:

```
NEW_IP=172.20.0.1/16
DFILE=/etc/docker/daemon.json
sudo systemctl stop docker
sudo sed -i '/\"bip\"/d' $DFILE
sudo sed -i "2i \\ \"bip\": \"\\$NEW_IP\", \" $DFILE
cat $DFILE
sudo systemctl daemon-reload
sudo systemctl start docker
```

- Verify the appliance docker0 IP has changed:

```
$ ip addr show docker0
8: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 06:4f:9f:29:3e:c2 brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::44f:9fff:fe29:3ec2/64 scope link
        valid_lft forever preferred_lft forever
```

2. Change VLAN Network: Change the VLAN IP address before configuring the IP address for the admin interface:

- Run the below code by replacing `VLAN_MASK` with your new 24-bit network mask (For example, 192.168.3):

```
$ sudo sed -i "s/192.168.0/$VLAN_MASK/" /etc/netplan/00-installer-config.yaml
$ sudo netplan apply
```

- Verify that the appliance VLAN Network has changed:

```
$ ifconfig eno8303.100
eno8303.100: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.200 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::d246:cff:fe71:26de prefixlen 64 scopeid 0x20<link>
    ether d0:46:0c:71:26:de txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3230 bytes 175236 (175.2 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Note: When you change the Docker subnet, the log retrieval from the UI may stop working because the required service gets blocked by the local firewall.

- To resolve the issue, allow TCP port **9000** in **UFW (Uncomplicated Firewall)** on the AGNI appliance. Run the following command:

```
$ sudo ufw allow 9000/tcp
```

You can now configure the IP address for the admin interface.

7.3 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 sha256:484e0560ae9065cf6b739458e971cd2a13eaf44868fa4459af87457d429fb187:
not found
2025/12/30 19:05:14 INFO bootstrap(script) - writing to console=/var/log/arista/agni/cli/pre-up
date.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
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/sources.list.d/do
cker.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
```