VMware NSX Advanced Load Balancer Cloud Console Guide

VMware NSX Advanced Load Balancer

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Guide

NSX Advanced Load Balancer with Cloud Console provides multi-cloud load balancing, web application firewall, application analytics and container services from the data center to the cloud with enhanced operations delivered through SaaS.

NSX Advanced Load Balancer Cloud Console Overview and Architecture

1

This guide provides an overview of NSX Advanced Load Balancer Cloud Console.

NSX Advanced Load Balancer with Cloud Console provides multi-cloud load balancing, web application firewall, application analytics and container services from the data center to the cloud with enhanced operations delivered through SaaS. The solution can be deployed on premises and/ or in the Cloud and has three main components:

Software Control Plane (NSX Advanced Load Balancer Controller):

Responsible for placement of the Service Engines, elasticity, scale, automation, analytics, resiliency and more.

Software Data Plane (NSX Advanced Load Balancer Service Engine):

Provide the data plane functionality for local and global load balancing, application security, container ingress services, IPAM and DNS and more.

Cloud Console (NSX Advanced Load Balancer Cloud Console):

Enables SaaS capabilities to the NSX Advanced Load Balancer deployments simplifying customer's operations and enabling advanced security to workloads.

NSX Advanced Load Balancer Cloud Console Features

The following are the features of Cloud Console:

Central Licensing:

Enables zero-touch capacity management and Cloud bursting for globally distributed NSX Advanced Load Balancer deployments.

Proactive Support:

Enables a zero-touch support experience by monitoring NSX Advanced Load Balancer deployments and creating VMware support cases automatically upon detecting issues.

Live Security Threat Intelligence:

Provides multiple live security feeds, for instance, WAF, BOT, IP Reputation, and so on to distributed, disparate environments to protect applications against threats that evolve in real-time.

References

- VMware End User Terms and Conditions
- VMware Terms of Service
- NSX Advanced Load Balancer with Cloud Console Service Description
- NSX Advanced Load Balancer Support Request Creation Guide
- NSX Advanced Load Balancer Service – Privacy Datasheet

Getting Started

2

This section describes the steps to set up and start consuming an NSX Advanced Load Balancer with Cloud Console SaaS subscription.

Read the following topics next:

- Prerequisites
- Onboarding an NSX Advanced Load Balancer with Cloud Console Subscription
- Accessing NSX Advanced Load Balancer with Cloud Console Portal
- Registering NSX Advanced Load Balancer Controller with Cloud Console
- NSX Advanced Load Balancer SID Mobility

Prerequisites

This section documents prerequisites to activate and start consuming an NSX Advanced Load Balancer Cloud Console subscription.

Prerequisites for Enterprise Tier Subscription

You need to have an active/ trial subscription for NSX Advanced Load Balancer with Cloud Console,

Or,

You need to have an active NSX Advanced Load Balancer serial key license purchased before 31 December 2021.

Note VMware serial key licenses will only allow a limited set of services offered by NSX Advanced Load Balancer Cloud Console.

Connectivity Requirements (Ports and Protocols)

Source	Destination URL	Destination Port(s)	Reason
Browser	portal.avipulse.vmware.com	443	Customer access to NSX Advanced Load Balancer Cloud Console portal.
Browser	customerconnect.vmware.com	443	VMware IDP used for authentication.
NSX Advanced Load Balancer Controllers	portal.avipulse.vmware.com	443	Deliver services from NSX Advanced Load Balancer Cloud Console.

Prerequisites for Enterprise Cloud Console Subscription

- You need to have an active/ trial subscription for NSX Advanced Load Balancer with Cloud Console.
- Your Controller version must be 21.1.3 or higher.
- You have met the following connectivity requirement.

Note To successfully register the NSX Advanced Load Balancer with NSX Advanced Load Balancer Cloud Console, the user with organization member role must have 'support user' as an additional role.

Connectivity Requirements (Ports and Protocols)

Source	Destination URL	Destination Port(s)	Reason
Browser	portal.avipulse.vmware.com	443	Customer access to NSX Advanced Load Balancer Cloud Console portal.
Browser	console.cloud.vmware.com	443	VMware IDP used for authentication.
NSX Advanced Load Balancer Controllers	portal.avipulse.vmware.com	443	Deliver services from NSX Advanced Load Balancer Cloud Console.
NSX Advanced Load Balancer Controllers	downloads.avipulse.vmware.com	443	Optional, if Application Rule and IP reputation Database updates are requested.
NSX Advanced Load Balancer Controllers	cdn.prod.nsxti.vmware.com	443	Optional, if application rule and IP reputation Database updates are requested.

For debuglogs upload from the Controller you need to exempt below FQDN from firewall:

```
avisupportdata-prod.s3.<region>.amazonaws.com
```

where,

`<region>` in the urls evaluates to different regions like:

`eu-west-1`, `eu-central-1`, `ap-northeast-1`, `ap-southeast-1`, `us-west-1` and so on. For instance, `avisupportdata-prod.s3.eu-west-1.amazonaws.com`.

Enhance Security by configuring a Forward Proxy to access NSX Advanced Load Balancer Cloud Console

Customers can enable a Forward Proxy to proxy all traffic between the Controller and NSX Advanced Load Balancer Cloud Console. This allows further security control and visibility. NSX Advanced Load Balancer Controllers natively support integrating with a Forward Proxy.

The following are the three modes of using a Forward Proxy for NSX Advanced Load Balancer Cloud Console traffic:

No Proxy:

All Cloud Consoles are directly accessed without any proxy from the Controller.

System Proxy:

All Cloud Consoles will be accessed through the configured Forward Proxy from the Controller. This Forward Proxy will be used system wide for all services configured to utilize a Forward Proxy.

Split Proxy:

All Cloud Consoles will be accessed through the configured Forward Proxy from the Controller. This Forward Proxy will be dedicated to be used to access NSX Advanced Load Balancer Cloud Console. There can be another Forward Proxy configured at the system level for all other services requiring a Forward Proxy.

The following section demonstrates how to configure a Forward Proxy on the NSX Advanced Load Balancer Controller using CLI. See CLI Access section of the *Administration* guide for details on accessing CLI.

System Proxy:

```
[admin:controller]: > configure systemconfiguration
[admin:controller]: systemconfiguration> proxy_configuration
[admin:controller]: systemconfiguration:proxy_configuration> host <FORWARD_PROXY_IP_OR_FQDN>
[admin:controller]: systemconfiguration:proxy_configuration> port <FORWARD_PROXY_PORT>
[admin:controller]: systemconfiguration:proxy_configuration> username <FORWARD_PROXY_USER>
[admin:controller]: systemconfiguration:proxy_configuration> password <FORWARD_PROXY_PASSWORD>
[admin:controller]: systemconfiguration:proxy_configuration> save
[admin:controller]: systemconfiguration> save
[admin:controller]: > configure albservicesconfig
[admin:controller]: albservicesconfig> no use_split_proxy
Overwriting the previously entered value for use_split_proxy
[admin:controller]: albservicesconfig> no split_proxy_configuration
[admin:controller]: albservicesconfig> save
```

Split Proxy:

```
[admin:controller]: > configure albservicesconfig
[admin:controller]: albservicesconfig> use_split_proxy
Overwriting the previously entered value for use_split_proxy
[admin:controller]: albservicesconfig> split_proxy_configuration
[admin:controller]: albservicesconfig:split_proxy_configuration> host
<FORWARD_PROXY_IP_OR_FQDN>
[admin:controller]: albservicesconfig:split_proxy_configuration> port <FORWARD_PROXY_PORT>
[admin:controller]: albservicesconfig:split_proxy_configuration> username <FORWARD_PROXY_USER>
[admin:controller]: albservicesconfig:split_proxy_configuration> password
<FORWARD_PROXY_PASSWORD>
[admin:controller]: albservicesconfig:split_proxy_configuration> save
[admin:controller]: albservicesconfig> save
```

Onboarding an NSX Advanced Load Balancer with Cloud Console Subscription

This section documents the steps to onboard an NSX Advanced Load Balancer with Cloud Console subscription.

1. Open the onboarding email titled ‘Complete your registration: Welcome to NSX Advanced Load Balancer with Cloud Console’ and click **Complete your Registration Now** button.
2. Sign-in to VMware Cloud Services Portal (CSP) using your credentials. If you do not have a CSP account, click **Create Your VMware Account** and complete the account registration.
3. Select the NSX Advanced Load Balancer with Cloud Console subscription. At this point, if you want to invite other members to complete the onboarding process and manage this subscription, click **Edit** and add the required email IDs.
4. Select or create a CSP Organization where your NSX Advanced Load Balancer with Cloud Console SaaS subscription will be placed.

   Note Mapping a subscription to a CSP Organization is irreversible. Choose your CSP organization carefully.

5. You have successfully onboarded your NSX Advanced Load Balancer with Cloud Console subscription. You can see 'NSX Advanced Load Balancer with Cloud Services' under the ‘**Services**’ section of your CSP organization chosen/ created previously.

Request for a NSX Advanced Load Balancer with Cloud Console Trial

1. Customer requests for a trial of NSX Advanced Load Balancer with Cloud Console through their VMware account representative.
2. VMware sends a *Trial Invite* email to the customer with a pre-signed link to start the trial.

3 Customer starts the trial by using the pre-signed link and assigning the trial to a CSP Organization of choice.

   a Customer can forward the invite to another team member to complete this step.

   b Customer can choose to create a new CSP Organization if required.

4 VMware activates the trial by depositing trial capacity in the mapped CSP Organization in the Central Licensing service provided by NSX Advanced Load Balancer Cloud Console.

5 VMware sends a *Trial Activation* email to the customer and NSX Advanced Load Balancer with Cloud Console is now ready for trial.

Renewal of a NSX Advanced Load Balancer with Cloud Console Subscription

The following are the steps to renew a NSX Advanced Load Balancer with Cloud Console subscription:

1 The customer renews NSX Advanced Load Balancer with Cloud Console subscription.

2 VMware updates the renewed capacity and the new expiry date in the Central Licensing service provided by NSX Advanced Load Balancer Cloud Console.

Accessing NSX Advanced Load Balancer with Cloud Console Portal

You can access NSX Advanced Load Balancer with Cloud Console as follows:

1 Open portal.avipulse.vmware.com on your browser.

2 You will be redirected to CSP for authentication. Enter your CSP credentials and click **Next**.

3 You will land on the NSX Advanced Load Balancer with Cloud Services Portal, where you will be able to see license and related information.

   Note Upon completing your subscription onboarding, a blank screen might be seen on the NSX Advanced Load Balancer with Cloud Console Portal as it takes about one hour for licenses to reflect on the portal.

Downloading NSX Advanced Load Balancer Controller Software

You can download NSX Advanced Load Balancer Controller software as follows:

1 NSX Advanced Load Balancer with Cloud Console is supported by Controller version(s) 21.1.3 or later.

2 Download VMware NSX Advanced Load Balancer Controller software by following this KB article: https://kb.vmware.com/s/article/82049.

3 Contact your VMware sales representative if older software is desired to be used.

Installing NSX Advanced Load Balancer Controller Software

1 Install a NSX Advanced Load Balancer Controller cluster by following these guides:

   a Installing NSX Advanced Load Balancer in VMware NSX-T Environments section in the *NSX Advanced Load Balancer Installation Guide*.

   b Installing NSX Advanced Load Balancer in VMware vSphere Environments section in the *NSX Advanced Load Balancer Installation Guide*.

   c Installing NSX Advanced Load Balancer in Microsoft Azure section in the *NSX Advanced Load Balancer Installation Guide*.

   d Installing NSX Advanced Load Balancer in Amazon Web Services section in the *NSX Advanced Load Balancer Installation Guide*.

   e Installing NSX Advanced Load Balancer in Google Cloud Platform section in the *NSX Advanced Load Balancer Installation Guide*.

Note

1 Configure FQDNs for the NSX Advanced Load Balancer Controllers before registering with Cloud Console. Registration will not succeed if the Controllers only have IP Addresses configured.

2 If configuring FQDNs in your corporate DNS is not possible, you can create local FQDN entries on the workstation from which the browser will be launched to register NSX Advanced Load Balancer Controller with Cloud Console. For instance, you can edit `/etc/hosts` file on Mac OS.

Upgrading an existing NSX Advanced Load Balancer Controller Deployment

1 You can upgrade an existing NSX Advanced Load Balancer Controller deployment as follows:

   a Download VMware NSX Advanced Load Balancer Controller upgrade software by following this KB article: https://kb.vmware.com/s/article/82049.

   b Download upgrade software version 21.1.3 or later.

   c Contact your VMware sales representative if older software is desired to be used.

2 Upgrade NSX Advanced Load Balancer Controller cluster by following this guide.

Registering NSX Advanced Load Balancer Controller with Cloud Console

This section documents the process of registering and de-registering NSX Advanced Load Balancer with Cloud Console.

Process to register NSX Advanced Load Balancer with Cloud Console

Follow these steps to successfully register your NSX Advanced Load Balancer Controller cluster with NSX Advanced Load Balancer Cloud Console.

1 Open a browser tab and login to your Controller using its Fully Qualified Domain Name (FQDN).

2 Navigate to **Administration > Licensing**.

3 Click the gear icon and ensure that the **ENTERPRISE_WITH_CLOUD_SERVICES** tier is selected.

4 (Optional) Set the required **Number of Reserved Licenses** and **Maximum Allowed Licenses** for this NSX Advanced Load Balancer deployment.

5 Click **Save**.

> **Note** **Number of Reserved Licenses** allows you to partition your purchased subscriptions. The configured amount of license capacity will always be reserved for your Controller (assuming active license count is equal or greater than what is being reserved).
>
> **Maximum Allowed Licenses** allows you to setup maximum consumption for this Controller. The Controller will never consume more capacity that what is set here.

6 Navigate to **Administration > Cloud Services**.

7 Click on the pencil icon to rename your Controller cluster from cluster-0-1 to a more representative name. This name will be used on NSX Advanced Load Balancer Cloud Console portal to identify your Controller.

8 Click **SAVE**.

9 Click **REGISTER CONTROLLER**.

10 Enter your VMware CSP credentials to authenticate your Controller with NSX Advanced Load Balancer Cloud Console.

11 Once authenticated, choose the CSP Organization to associate this Controller with. This should be the same as CSP Organization which has an active NSX Advanced Load Balancer with Cloud Console subscription.

12 Choose a service contact. This contact will be used by the Proactive Support service (if enabled) when a support case is filed.

13 Optionally, enable other services delivered by NSX Advanced Load Balancer Cloud Console.

14 Click **SAVE** to complete registration.

Note

1 Registered Controllers regularly send their health metrics like CPU, memory, license usage information to the NSX Advanced Load Balancer Cloud Console portal. You can turn it off by disabling the inventory service using the following CLI:

```
configure albservicesconfig → operations_config → inventory_config → no enable
```

2 If your Controller deployment was upgraded, existing licenses (VMware serial keys) being used on this controller will be invalidated once license tier is switched to `ENTERPRISE_WITH_CLOUD_SERVICES`.

3 After Controller registration, you can verify your subscription by using `show license status` command on the NSX Advanced Load Balancer Controller CLI.

Note Re-registration might be required if the Controller was previously registered with NSX Advanced Load Balancer Cloud Console.

Validate if NSX Advanced Load Balancer Controller registration is complete from the NSX Advanced Load Balancer Cloud Console portal.

1 Launch the NSX Advanced Load Balancer Cloud Console portal.

2 Authenticate using your **CustomerConnect** credentials.

3 Navigate to the **Controllers** tab.

4 Validate that the NSX Advanced Load Balancer Controller from the previous step shows as registered.

5 After registering, you should verify that subscription is succeeded by using `show license status` command on the NSX Advanced Load Balancer Controller CLI.

Field	Value
uuid	default
name	license_status
saas_status	
enabled	True
reserve_service_units	0.0
connected	False
message	SAAS SUBSCRIBED
expired	False

Field	Value
configpb_attributes	
version	1

Note You can launch NSX Advanced Load Balancer Cloud Console from the CSP console at https://console.cloud.vmware.com, by navigating to the **CSP Organization** and clicking the **service** tile.

De-registering NSX Advanced Load Balancer with Cloud Console

De-registering through the Controller UI

1 Launch the NSX Advanced Load Balancer Controller UI.

2 Navigate to **Administration > Cloud Services**.

3 Click **DEREGISTER CONTROLLER**.

4 Click **OK** to confirm and complete de-registration.

De-registering through NSX Advanced Load Balancer Cloud Console Portal

1 Open portal.avipulse.vmware.com on your browser.

2 Navigate to **Controllers** tab.

3 Select the CSP Organization that is associated with your Controller.

4 Click **Deregister**.

Once de-registration is completed:

- All Cloud Consoles will be disconnected.
- NSX Advanced Load Balancer Service Engines will become unlicensed. However, existing Service Engines and virtual services will not be hampered and continue to function just as they were before opting out of this service.

- New Service Engine registrations will be blocked until tier is switched, for instance, ENTERPRISE or Central licensing is enabled again.

Note

- Customers must only de-register a registered Controller in the following situations:
  - Changing CSP Organization mapping for the Controller, to change where capacity is consumed from.
  - Changing licensing tier on the Controller.
- Customers must not continue to run an NSX Advanced Load Balancer Controller in a de-registered state, when it is in the `ENTERPRISE_WITH_CLOUD_SERVICES` Licensing Tier.
- De-registering the Controller through NSX Advanced Load Balancer Cloud Console portal must be done only when the Controller de-registration is not feasible through the Controller UI, for instance, when the Controller is deleted or inaccessible.
- Upon de-registration, any or all customer information, such as contact email, name will be cleared.

NSX Advanced Load Balancer SID Mobility

SID Mobility provides the ability to move a customer's subscription from one OrgID to another OrgID without impacting the subscription terms.

SID Mobility Workflow

In the event that a subscription is onboarded to the wrong organization, please engage the relevant account team to start the process.

Once the customer requests to move organization, Pulse should get notified. After receiving the notification, Pulse should move the subscriptions to the new organization and mark the older organization as dormant. After the subscription is migrated, customer should get notified and should be able to consume the subscriptions from the new organization.

Legacy Deployments

3

This section covers the services offered to Legacy NSX Advanced Load Balancer Controller deployments.

An NSX Advanced Load Balancer Controller deployment utilizing active VMware serial key licenses that were purchased on or before December 31st 2021 and registered with NSX Advanced Load Balancer Cloud Console (Previously known as PULSE) is considered as 'legacy add-on deployment'.

Services offered for 'Legacy Addon' Deployments

The following NSX Advanced Load Balancer Cloud Console are offered to 'legacy addon' deployments:

- Proactive Support
  - Basic Case Management
  - Tech Support Attachment
- Live Security Threat Intelligence
  - Web Application Firewall (WAF) Signatures Service
  - Application Rules Service
  - IP Reputation Service

Note All other Chapter 4 NSX Advanced Load Balancer Cloud Console Catalogue are included only with the purchase of NSX Advanced Load Balancer with Cloud Console subscriptions.

Requirements to Register Legacy Deployments with Cloud Console

Following are the requirements to register a NSX Advanced Load Balancer Controller deployment with NSX Advanced Load Balancer Cloud Console.

- Valid active VMware serial key license for NSX Advanced Load Balancer Enterprise Edition.
- Valid customerconnect account with an active support entitlement to the NSX Advanced Load Balancer product.

- Appropriate software version running on the NSX Advanced Load Balancer Controller. Minimum software version is 21.1.3.

Use Cases to avail Cloud Console for Legacy Deployments

Note All scenarios must meet the above stated requirements.

1. Existing deployments running versions 21.1.2 and earlier: Register with Cloud Console without any assistance.
2. Existing deployments being upgraded to versions 21.1.3 and later (from versions 21.1.2 or earlier): Register with Cloud Console without any assistance.
3. New deployments running versions 21.1.3 and later: Contact your VMware sales representatives before registering.
   a. VMware will generate a Cloud Console 'legacy' license for your use.
   b. Once this license is imported on the required NSX Advanced Load Balancer Controller, it can be registered with NSX Advanced Load Balancer Cloud Console.

Registering Legacy Addons Deployments with Cloud Console

The steps to register a legacy addon deployment with Cloud Console are as follows:

1. Launch the NSX Advanced Load Balancer Controller UI.
2. Navigate to **Administration** > **Licensing**.
3. Click the gear icon and ensure that the `ENTERPRISE` tier is selected.
4. Click **SAVE**.

The steps to register NSX Advanced Load Balancer Controller with Cloud Console are as follows:

1. Launch the NSX Advanced Load Balancer Controller UI.
2. Navigate to **Administration** > **Cloud Services**.
3. Click on the pencil icon to rename the cluster from **cluster-0-1** to a more representative name. This name will be used on the **Cloud Services** portal to identify the deployment.
4. Click **SAVE**.
5. Click **REGISTER CONTROLLER**.

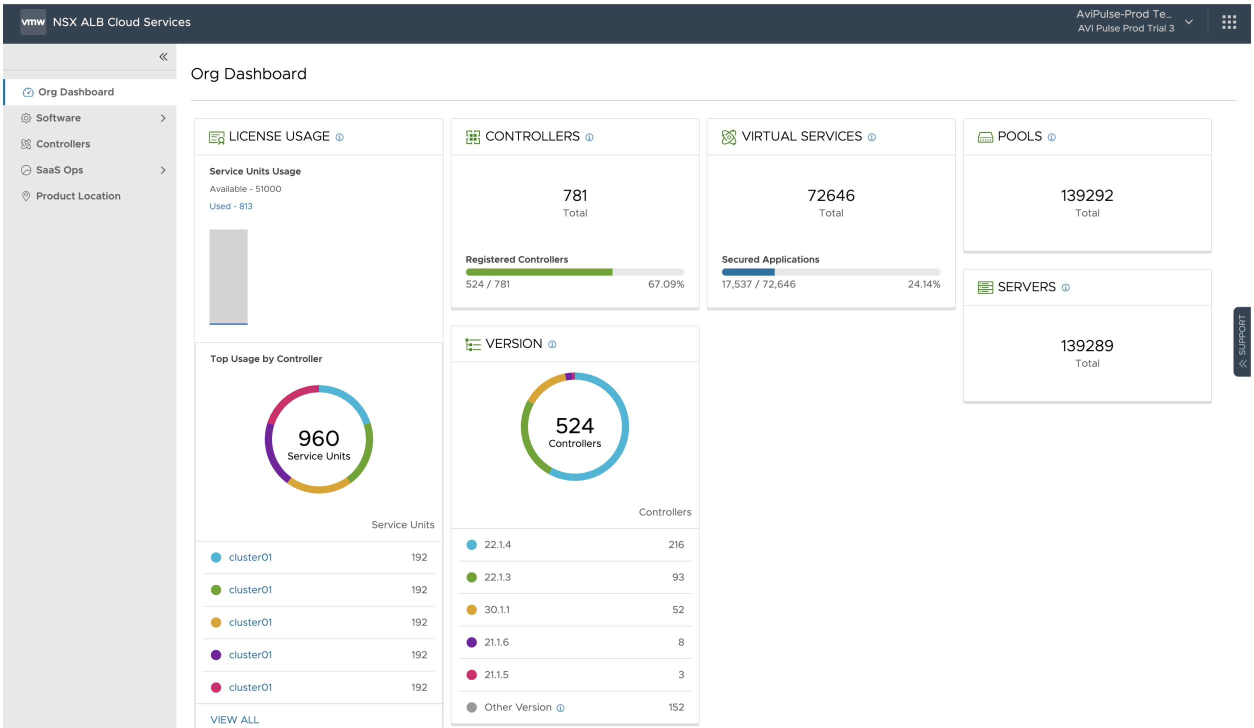
NSX Advanced Load Balancer Cloud Console Catalogue

4

This section provides information on each service offered by an NSX Advanced Load Balancer with Cloud Console subscription.

Organisation Dashboard

The NSX Advanced Load Balancer with Cloud Console Organisation dashboard provides details on the following. This service is OPT-IN.



	Service Units
cluster01	192
cluster01	192
cluster01	192
cluster01	192
cluster01	192

	Controllers
22.1.4	216
22.1.3	93
30.1.1	52
21.1.6	8
21.1.5	3
Other Version	152

- License Usage: Number of service units used
- Controllers: Number of registered Controllers and total usage by the Controller
- Virtual Services: Number of secured aplications
- Pools: Number of pools used
- Servers: Number of servers used

Data Collection and Retention Policy

Data Collection:

If customer opts-in basic inventory data is pushed to the Cloud Console portal from the Controller.

Data Retention:

Data is pushed once every hour and is cached for that hour. No data is kept beyond one-hour. This service has no access to customer infrastructure, including NSX, vCenter, and others. This service does not write any configurations on the registered NSX Advanced Load Balancer Controllers.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure (including NSX, vCenter, and others).
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

Read the following topics next:

- Central Licensing
- Live Security Threat Intelligence
- Proactive Support
- Inventory Service
- Other Services

Central Licensing

Central Licensing enables zero-touch capacity management and cloud bursting for globally distributed NSX Advanced Load Balancer deployments.

Feature Highlights

- Global capacity pool
- Eliminate duplicate licenses for Disaster Recovery
- Move licenses with your Apps
- Enable seamless Cloud Bursting

Data Collection and Retention Policy

Data Collection:

No data other than specifically outlined in Privacy document is collected by and for this service. As and when capacity is required on NSX Advanced Load Balancer deployments, request for capacity tokens originate from the Controller which are made available by the Central Licensing Service.

Data Retention:

Does not apply to this service.

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure, including NSX, vCenter, and others.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is a mandatory service and is enabled by default when a Controller is setup in the `ENTERPRISE_WITH_CLOUD_SERVICES` tier, and is registered with Cloud Services. Refer to the Registering NSX Advanced Load Balancer Controller with Cloud Console section.

Service Details

Central Licensing Service is available with NSX Advanced Load Balancer with Cloud Services subscription. When a customer onboards a purchased subscription and maps it to a CSP Organization, the said purchased subscription capacity is deposited into the Central Licensing Service.

Central Licensing Service then handles distribution of capacity across all registered Controller deployments. When capacity is required on Controller deployments, a request is made to Central Licensing Service to grant a capacity token. This capacity token is then used by the Controller to license Service Engines. These capacity tokens are automatically refreshed by the Controller. Capacity deposited in Central Licensing Service across different CSP Organizations is fully sandboxed and isolated.

NSX Advanced Load Balancer Controller deployments can 'reserve' required capacity upfront. Refer How to enable this service section for details.

Central Licensing Service grants a 10% built in buffer. For instance, if Customer-A purchases 100 units of NSX Advanced Load Balancer with Cloud Services subscription; 110 units of capacity will be deposited into Central Licensing Service.

Note Capacity is deposited into CSP Organizations within Central Licensing. For instance, if Customer-A purchases 100 units of NSX Advanced Load Balancer with Cloud Services and maps it to Org-1 and purchases another 50 units of NSX Advanced Load Balancer with Cloud Services and maps it to Org-2; NSX Advanced Load Balancer Controller deployments mapped to Org-1 can in total consume up to 110 units and deployments mapped to Org-2 can in total consume up to 55 units (10% buffer).

Subscription Expiry

During the term of the purchased subscription, customer has access to the new software releases (including software patches) published by VMware for NSX Advanced Load Balancer and access to 24/7 support. At the end of the specific SaaS subscription period, customer can purchase a new software SaaS subscription (annual or multi-year term). If a SaaS subscription expires, the following behavior applies:

- Existing operational virtual services that are deployed continue to operate for perpetuity.
- Ability to use the software within its existing configuration does not expire.
- NSX Advanced Load Balancer Controller does not automatically disable configuration.
- NSX Advanced Load Balancer Controller prevents creation of any new virtual services or Service Engines.
- VMware will not provide support for NSX Advanced Load Balancer.
- Access to all services delivered through NSX Advanced Load Balancer Cloud Services is halted including live security threat feeds.

Events of Interests

The following events are generated on the Controller for Central Licensing:

1. `LICENSE_SUBSCRIBED`: Controller successfully subscribed with portal for licenses.
2. `LICENSE_SUBSCRIPTION_FAILURE`: Controller failed to subscribe with portal.
3. `LICENSE_UNSUBSCRIBED`: Controller unsubscribed from portal for licenses.
4. `LICENSE_REFRESH_SUCCESS`: Controller refreshed portal issued license sucessfully.
5. `LICENSE_REFRESH_FAILURE`: Controller failed to refresh portal issued license.

Impact of Unavailability

During the period that Central Licensing service is down, for the first seven days:

1. All existing NSX Advanced Load Balancer Service Engines and the hosted load balanced applications will continue to function without any disruption for perpetuity.
2. New NSX Advanced Load Balancer Service Engines can continue to be created up to 100% of available active subscription capacity per registered NSX Advanced Load Balancer Controller with an additional 10% buffer.

After seven days the license lease expires and the Controller will not be able to pull new SU from the Central Licensing service.

Note Registered NSX Advanced Load Balancer Controllers can reserve required capacity upfront during registration and be protected from any Central Licensing availability impact.

Live Security Threat Intelligence

Live Security Threat Intelligence service delivers industry leading security threat feeds for various attack vectors in real time to protect applications from ever changing threats on enabled NSX Advanced Load Balancer deployments.

Application Rules Service

This section explains Application Rules service offered as part of Live Security Threat Intelligence. Application Rules are rules that are specifically designed to block attacks on known application vulnerabilities (many of them with CVEs) and are automatically updated. Customers can protect their applications from such vulnerabilities by enabling this service on their Controllers.

Note These rules are different from NSX Advanced Load Balancer’s Core Rule Set (CRS), where rules are protecting against generic attack classes.

Feature Highlights

- Protection for known vulnerabilities for over 5000 applications such as WordPpress, Drupal, Apache, and many more.
- Automatic rule updates.

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. Application Rules are pushed only to the NSX Advanced Load Balancer Controllers where this service is opted-in (enabled).

Data Retention:

Does not apply to this service.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure, including NSX, vCenter, and others.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is an 'opt-in' service and is disabled by default.

The stes to opt-in to this service and enable automatic support case creation are as follows:

1. Navigate to **Administration > Cloud Services**.
2. Click **EDIT**.

3 Under **Live Security Threat Intelligence**, select **Application Rules**.

4 Click **SAVE**.

Note You can opt-out of this service at any time and the Application Rules updates will stop.

Service Details

Once Application Rules service is opted in (enabled) on a NSX Advanced Load Balancer Controller, Application rules are automatically updated periodically.

Note By default Application Rules Sync Interval is set to 1 day (1440 minutes) (recommended) and 60 minutes is the minimum allowed value.

For more details on application rules, refer Application Rules section in *WAF* guide.

Events of Interest

The following events are generated on the NSX Advanced Load Balancer Controller when Application Rules service is enabled:

- `APPSIGNATURE_SYNC_SUCCESS`: Application Rules update is successful
- `APPSIGNATURE_SYNC_FAIL`: Application Rules update is not successful

Impact of Unavailability

During the period that this service is down, new application rule updates will not be pushed to enabled NSX Advanced Load Balancer Controllers. Load Balanced applications will continue to utilize cached application rules available on the NSX Advanced Load Balancer Controllers to protect against vulnerabilities.

IP Reputation Service

This section explains IP Reputation service offered as part of Live Security Threat Intelligence. With globally distributed NSX Advanced Load Balancer Controller clusters and with an ever changing landscape of insecure IP addresses, it is extremely channeling to maintain a real-time, up-to-date, consistent security posture and be protected from bad IPs. IP Reputation service solves this by providing a real-time feed of updated IP scores to globally distributed NSX Advanced Load Balancer deployments.

Feature Highlights

- Protection from bad IPs such as Botnets, Phishing, Spam, and many more.
- Real-time automatic IP Reputation updates.
- Used as a source for bot detection and classification.

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. IP Reputation is pushed only to NSX Advanced Load Balancer Controllers where this service is opted-in (enabled).

Data Collection:

Does not apply to this service.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure, inclsing NSX, vCenter, and others.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is an 'opt-in' service and is disabled by default.

The steps to opt-in to this service and enable IP Reputation updates are as follows:

1. Navigate to **Administration > Cloud Services**.
2. Click **EDIT**.
3. Under **Live Security Threat Intelligence** select **IP Reputation.**
4. Click **SAVE**.

Note You can opt-out of this service at any time and the User-Agent updates will stop.

Service Details

VMware utilizes **WebRoot** as its IP Reputation database source. IP reputation data is cached every five minutes on NSX Advanced Load Balancer Cloud Services portal. Registered NSX Advanced Load Balancer Controllers where this service is enabled, pull IP Reputation data from NSX Advanced Load Balancer Cloud Services portal. The Controllers immediately update connected Service Engines as part of its configuration update process.

Note **Frequency of IP Reputation updates**: **WebRoot** publishes a new IP Reputation database every day. Additionally, minor periodic updates (incremental) to the database are published every few minutes.

The database consists of the following two types of files:

The full database file (base file):

It contains both individual IP addresses and subnets. The size of this file is usually in MB.

The incremental file:

This database has a slightly different format and lesser entries than the full database file. It is available in the form of multiple files throughout the day (24 hours). It can contain additions to the base file or updates and removals of the existing entries. The incremental database files contain the individual IP addresses (/32 IP addresses).

Note This feature requires additional shared memory on the Service Engine. Refer to *Extra Shared Memory* in the NSX Advanced Load Balancer Configuration Guide to understand the additional memory requirements and configure the same.

For more details on IP Reputation, see IP Reputation section in *WAF* guide.

IP Reputation Sync Interval

The IP Reputation sync interval is the frequency at which the NSX Advanced Load Balancer Controllers poll for IP Reputation database updates. The following code shows how sync interval can be modified using NSX Advanced Load Balancer Controller CLI.

```
[admin:controller]: > configure albservicesconfig
[admin:controller]: albservicesconfig> ip_reputation_config
[admin:controller]: albservicesconfig:ip_reputation_config> ip_reputation_sync_interval 5
[admin:controller]: albservicesconfig:ip_reputation_config> save
[admin:controller]: albservicesconfig> save
```

The default value for the sync interval is 60 minutes. The value of sync interval can be between 2 and 60 minutes.

Events of Interest

The following events are generated on the NSX Advanced Load Balancer Controller when IP Reputation service is enabled:

- `IP_REPUTATION_DB_SYNC_SUCCESS`: IP Reputation update succeeded.
- `IP_REPUTATION_DB_SYNC_FAILURE`: IP Reputation update failed.

Impact of Unavailability

During the period that this service is down, new IP Reputation updates are not pushed to enabled NSX Advanced Load Balancer Controllers. Load Balanced applications continue to utilize cached IP Reputation available on NSX Advanced Load Balancer Controllers to protect against bad IPs.

BOT Management

This section explains bot detection, management, and configuration in NSX Advanced Load Balancer.

A Bot is a software application that runs autonomously and is programmed to perform certain repetitive tasks much faster than human users could. Bots are automated, that means, they run according to their instructions without any human intervention. Bots are mimicking real human work-flows across web applications to behave like real users.

Bots have evolved significantly over the last few years and have become more sophisticated than ever. There are different types of Bot, such as:

Type of Bot	Description
Web Crawlers	Bots scan content on web pages, for instance, Google Bot.
Social Bots	Automated accounts that use artificial intelligence to steer discussions and promote specific ideas or products on social media such as Twitter and Facebook.
Chat Bots	These are a common type of Bot that simulate human conversation by responding to queries with programmed responses.
Gaming Bots	These Bots are used in videos games. These are usually based on artificial intelligence and are programmed to assume vivid characters in a video game that a human player would interact with.
Malicious Bots	Responsible for perpetrating online fraud, credential stuffing, and so on.
Scalpers	These are malicious Bots that use automated methods to secure goods, such as event tickets that are bought in bulk, and complete the checkout process in a fraction of the time it would take any legitimate user. For instance, fraudulent holding and reselling of airplane seats affecting a major airline.
Scrapers	Scrape data from sites without permission in order to steal data, or duplicate a site in order to set up up a fraudulent phishing site or gain a competitive edge.

Bots are becoming an increasing problem for web presences, and Bot traffic has significantly increased over the last few years. According to the recent studies, only about 60% of the traffic on a given website coming from human beings. Out of the remaining 40%, 25% are categorized as bad Bots and 15% as good Bots.

Good Bots Example	Bad Bots Example
■ Search engine crawlers ■ Website health monitors ■ Vulnerability scanners ■ Copyright checks ■ Feeds	■ Scrapers ■ Spam ■ Click (Fraud) ■ Googlebot impersionators ■ Botnets

Bot Detection and Bot Management

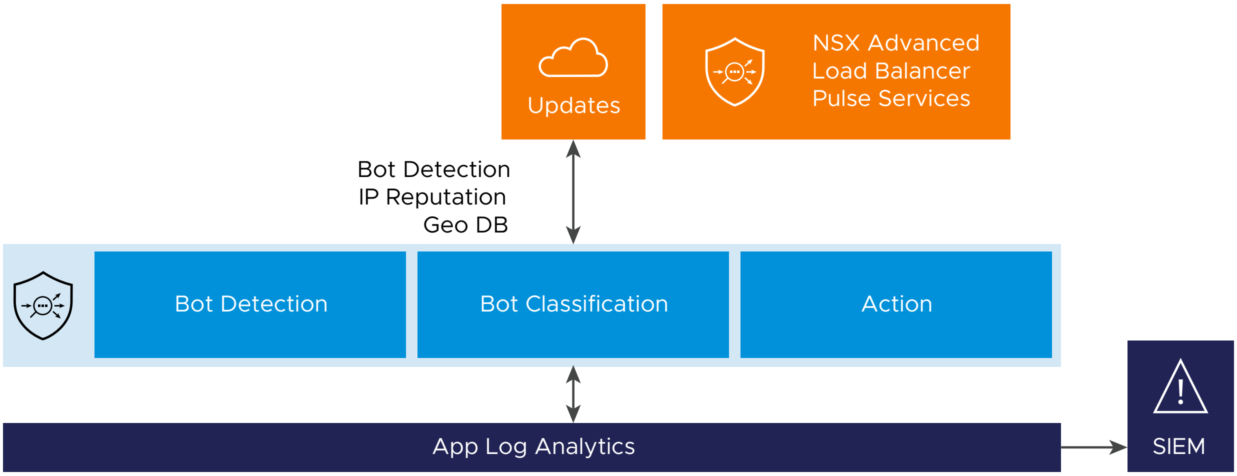
Good Bots can be useful but bad Bots are responsible for many of the most serious threats to online businesses. It is important to detect Bot traffic, determine its intent and mitigate bad Bots to enhance user experience.

Bot detection can be defined as a method to identify the client that is, whether the traffic is coming from a human or a Bot.

Once a Bot is detected, managing Bot traffic is equally important. Bot management is a strategy that enables you to filter which Bots are allowed to access your web assets and which should be rate-limited or blocked completely.

NSX Advanced Load Balancer Bot Management

The Bot management solution is introduced to mitigate bad Bots.



The figure above shows the Bot management pipeline that consists of three main steps:

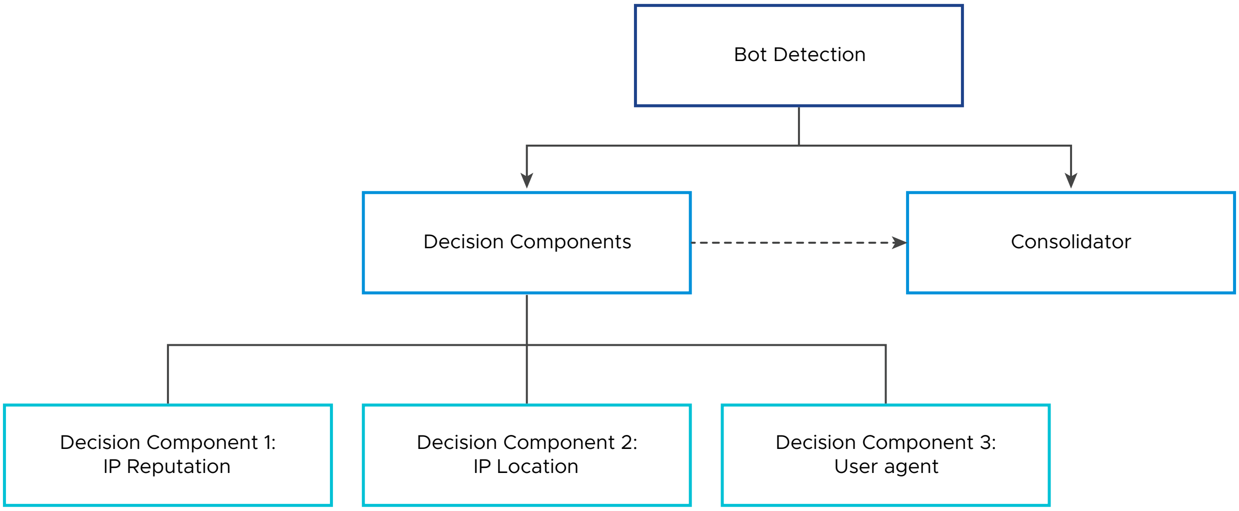
1 Bot Detection

2 Bot Classification

3 Actions

Bot Detection

This is the first and the most crucial step in the Bot management pipeline.


Bot Detection
Decision Components
Consolidator
Decision Component 1: IP Reputation
Decision Component 2: IP Location
Decision Component 3: User agent

In this step, the request goes through various checks. The checks are called decision components. Each decision component (Bot detector) provides some information to characterize the request like Client Class (`USER/ BOT/ undetermined`), Client Type (possible values depend on class, for instance, browser or app for USER and search engine/ monitor for Bot), Confidence level (High, Medium or Low).

Decision Components/ Detectors

IP reputation

This component uses an IP reputation database that gets updated by NSX Advanced Load Balancer Cloud Console. It matches the IP address of the client against the IP reputation database. If there is a match, then the client will be marked as Bot with high confidence level. If there is no match, then it is undetermined.

IP location

In this step, NSX Advanced Load Balancer uses the Client-IP and does a lookup in network location DB. As part of the process, the system matches the ISP and Organization name against known search engines and cloud providers. Once the lookup is done and decision is taken, the client is marked either as Bot or Undetermined. Confidence level is also assigned.

User-Agent

The system does a heuristic scan of the incoming user agent string to look for things like SQL injections etc. If found, the request is marked as a bad Bot of type web attack. Otherwise, the system checks the User-Agent Database that gets populated using NSX Advanced Load Balancer Console. Depending on the result of this check, the client is marked as either Bot or Human. If there is no information in the Database, a pattern match is made to identify common and typical browser user agents. If that fails too, the result is undetermined.

The User-Agent check in Bot management allows User-Agent strings with an uneven number of single quotes. For instance, Mozilla/5.0 (compatible; Let’s Encrypt validation server; +https://www.letsencrypt.org)

Note If there is any need to disable one of these decision components, it can be done using the steps mentioned in Bot Configuration section.

Consolidator

Consolidator is a built-in agent that takes results of all other decision components and creates its own client type and class based on certain logic. It inspects the data and looks for any contradictions and irregularities. It stores its own decision which is further referred by Bot mapping.

TLS Fingerprinting for Bot Detection

The user-agent decision component has been enhanced to not only take into account the User-Agent header as sent by the client, but to also match the TLS messages from the client against the TLS fingerprint expected for the given user agent.

This improves detection of bots that masquerade as human users by sending a valid browser User-Agent header. Therefore, this additional check is only carried out if the User-Agent is a browser according to the data in the user agent cache. Furthermore, it can of course only be carried out if the connection is via https, and not http.

If there is no TLS information for the user-agent in question, the client is classified as human with medium confidence.

If there is TLS information for the user-agent in question, and the clients TLS fingerprint matches that information, the client is classed as human with high confidence. If a mismatch is detected, the user-agent decision component labels the client a dangerous bot of type impersonator with high confidence.

TLS fingerprint information is maintained up-to-date through cloud console. The use of TLS fingerprint information can be disabled in the bot detection policy through the knob `use_tls_fingerprint`.

A new complex field for detailed client TLS information and fingerprint has been added to the application log; it can be enabled through the flag `collect_client_tls_fingerprint` in the application profile.

Bot Classification

Once the consolidator has provided its analysis, NSX Advanced Load Balancer classifies the Bot using a Bot Mapping Policy. The default Bot mapping is handled by configuration object called as System-BotMapping. Bot classification is the final outcome that is assigned by Bot mapping. Bots are classified as follows in NSX Advanced Load Balancer:

BOT Classification	Description
HUMAN	Browser, Application
GOOD_BOT	Search engines like Google Bot
BAD_BOT	Scanner, Botnets
DANGEROUS_BOT	When an attack is found in the user agent string, web attacks, Botnet, denial of service.
USER_DEFINED_BOT	Custom Bots defined in Bot mapping
UNKNOWN_CLIENT	Unidentified

Note If a user-defined bot mapping is specified in a bot detection policy, the system bot mapping reference can be left empty.

Bot Mapping

The Bot can be classified on the basis of the following:

- Bot Class
- Bot Type
- Bot Identifier

Bot Decision Component

You can select the Bot decision component that has assigned class, type or the identifier. The component can be the consolidator, the user-agent detector, the IP-reputation detector or the IP-location detector. Based on these characteristics, the Bot mapping selects one of the defined Bot classification types, such as, HUMAN, GOOD_BOT and so on. Selection of multiple properties implies logical AND, that is, all properties have to be fulfilled for a match to be successful.

All these properties are directly related to the Bot module. Bot classification type can be assigned in a Bot mapping based on general request properties like the source IP or an HTTP header value.

To fit this concept into the object model, an extra message type has been added to encapsulate the matching functionality of a `BotMappingRule: BotMappingRuleMatchTarget` code.

In addition to the three Bot results mentioned above, the following request properties can be used in Bot mappings:

- The client IP address. Here the full flexibility of the existing IpAddrMatch message is supported, that is, matching can be configured by individual IP, prefix, range and IP group. If multiple targets are configured, they are combined by logical OR.

Note Client IP is subject to the option `Use_True_Client_IP`. Client IP might be equal to source IP from layer-3 header or equal to the fetched IP from user-defined HTTP header. For more information, see *True Client IP in L7 Security Features* in the *VMware NSX Advanced Load Balancer Configuration Guide*.

- You can specify the HTTP method using a MethodMatch message. If multiple values are supplied, logical OR is implied.
- The path requested by the client. The usual string operations supported for a PathMatch message can be configured with the exception of regular expressions.
- A combination of HTTP headers can used for matching by using the existing HdrMatch message. Multiple headers are combined by logical OR.
- For convenience, the host header can be configured more easily by specifying a `HostHdrMatch` message.

As with the previously supported properties, all specified properties in a `BotMappingRuleMatchTarget` have to be matched for the overall match to be successful.

Actions

The last step is to define the action that needs to be taken to control the behavior of Bots that have been classified.

This is done using HTTP Security policies under *Policies* section in the *Virtual Service Policies* chapter in the *VMware NSX Advanced Load Balancer Configuration Guide*. The match condition can be one of the classified Bots, and the possible actions are:

- Allow

- Close Connection
- Rate Limit
- Send Custom Response and so on

Prerequisites

NSX Advanced Load Balancer Cloud Console must be enabled and NSX Advanced Load Balancer Controller should be registered with NSX Advanced Load Balancer Cloud Console.

Extra Memory Requirements

The following are the extra memory requirements:

- 4 GB of RAM extra needs to be allocated on SE.
- 600 MB extra config shared memory.
  - SE-Group property `extra_shared_config_memory`. Once extra shared config memory is allocated, you need to reboot the system.

    Note Rebooting can lead to disruption in traffic.

For more information, see *Extra Shared Memory* in the *VMware NSX Advanced Load Balancer Configuration Guide* to understand the additional memory requirements and configure the same.

System Limits for Bot Management

The details of system limits for Bot management is explained in VMware Configuration Limits. You can select the required version in VMware Configuration Limits and check for the system limits.

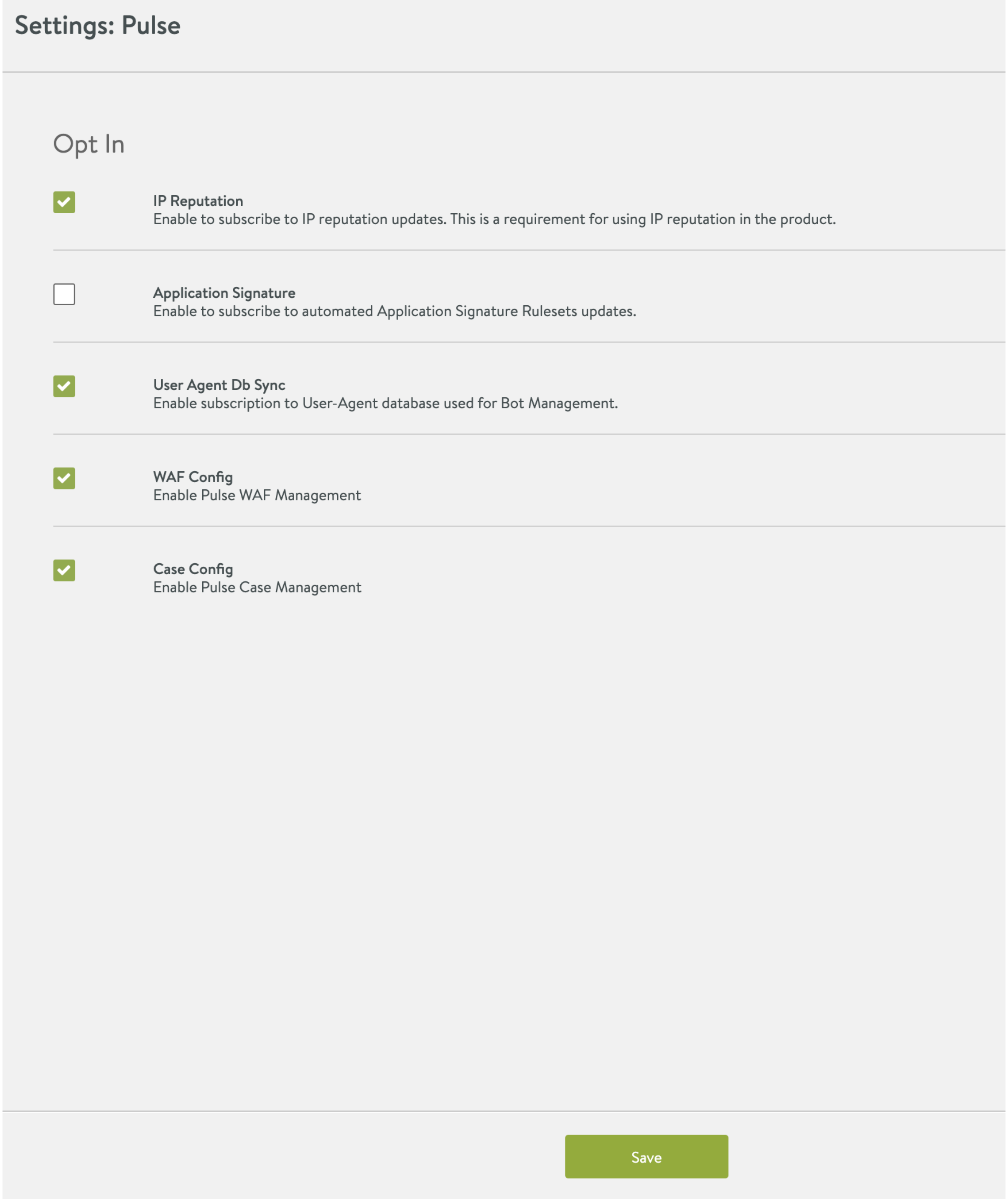
Bot Configuration

The following are the steps to enable the service on an NSX Advanced Load Balancer Controller:

1 Navigate to **Administration** > **Settings** > **Pulse**. If the NSX Advanced Load Balancer Controller is registered with the NSX Advanced Load Balancer Cloud Console, as shown below, move to the next step. If the NSX Advanced Load Balancer Controller is not registered with NSX Advanced Load Balancer Cloud Console, see Chapter 2 Getting Started for registration process.

2 Click on the edit NSX Advanced Load Balancer Pulse settings option.

3 Check **IP Reputation** and **User Agent Db Sync** check boxes in **Settings:Pulse** window, as shown below:



Settings: Pulse

Opt In

☑ **IP Reputation**
Enable to subscribe to IP reputation updates. This is a requirement for using IP reputation in the product.

□ **Application Signature**
Enable to subscribe to automated Application Signature Rulesets updates.

☑ **User Agent Db Sync**
Enable subscription to User-Agent database used for Bot Management.

☑ **WAF Config**
Enable Pulse WAF Management

☑ **Case Config**
Enable Pulse Case Management

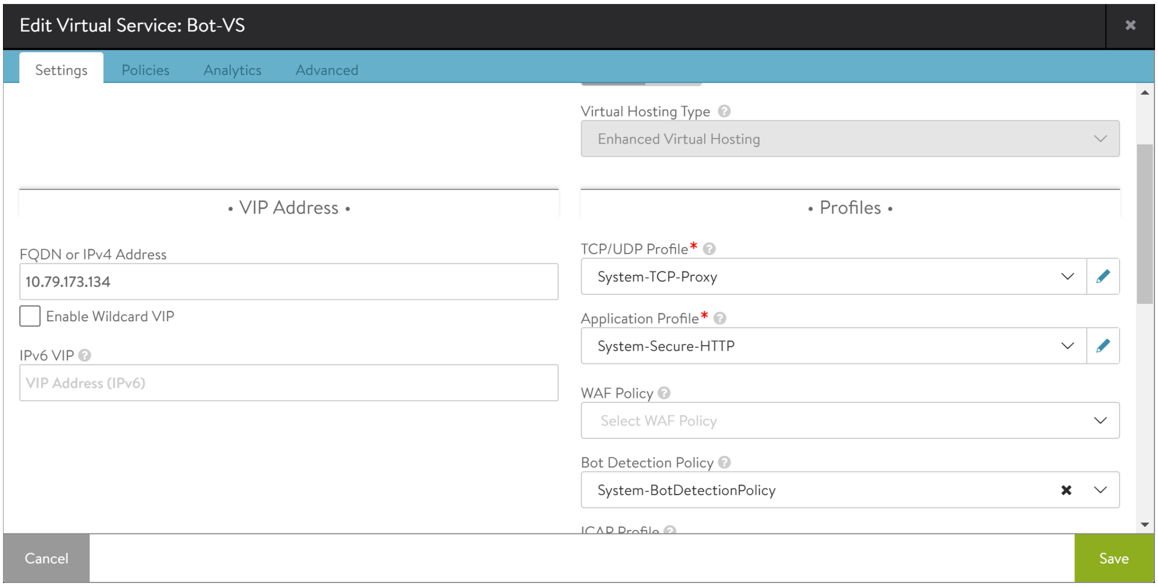
4 Click **Save**.

Once it is enabled, you can configure the rest of the entities using the following steps:

1 Bind the default botdetectionpolicy that is, `System-BotDetectionPolicy` to the virtual service using the following steps:

   a Navigate to **Applications > Virtual Services** . Click on Pencil icon to edit the virtual service.

b Bind the **System-BotDetectionPolicy** to the virtual service.



Edit Virtual Service: Bot-VS

Virtual Hosting Type: Enhanced Virtual Hosting

• VIP Address •

FQDN or IPv4 Address: 10.79.173.134

□ Enable Wildcard VIP

IPv6 VIP: VIP Address (IPv6)

• Profiles •

TCP/UDP Profile*: System-TCP-Proxy

Application Profile*: System-Secure-HTTP

WAF Policy: Select WAF Policy

Bot Detection Policy: System-BotDetectionPolicy

2 Add HTTP security policy to take the action on classified Bot.

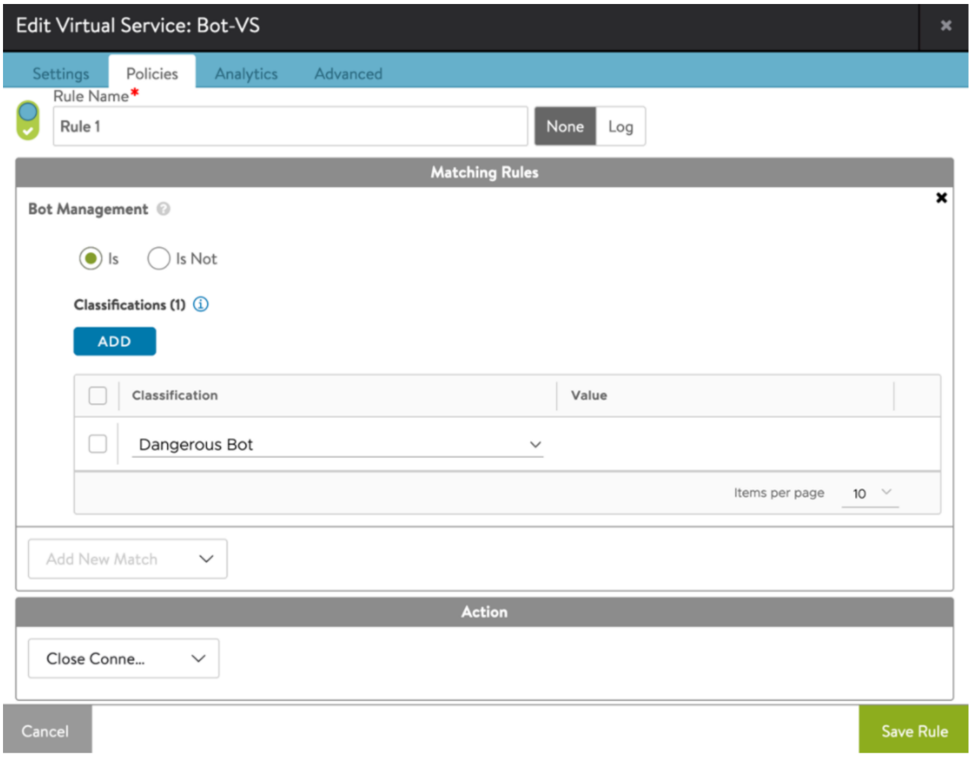
a Click on **Policies > HTTP Security**. Click on **+** icon under **Add HTTP Security Rule** section to add a new rule and assign a name to the rule.

b Select **Bot management** option as the match condition from the drop-down list in **Matching Rules** section.

c Click on **ADD** under classification and click on **Select Classification** drop-down menu.

d Select the Bot class from the drop-down menu.

e Select the required action.



Rule Name* Rule 1 | None | Log

Bot Management

● Is ○ Is Not

Classifications (1)

☐	Classification	Value
☐	Dangerous Bot	

Items per page 10

Close Conne...

f Click **Save Rule**.

g Click **Save**.

BOT Configuration using CLI

This section describes the steps to enable Bot Management through CLI.

The following are the steps to configure Bot using the CLI:

Procedure

1 Bind the Bot detection policy to the virtual service.

2 Add HTTP security policy to take the action on the classified Bot.

```
 [admin:ctrl]:> configure virtualservice Bot-VS
 [admin:ctrl]: virtualservice> bot_policy_ref System-BotDetectionPolicy
 [admin:ctrl]: virtualservice> save
```

3 Add HTTP security policy to take the action on the classified Bot.

```
[admin:ctrl]: > configure httppolicyset Demo
 [admin:ctrl]: httppolicyset> http_security_policy
 [admin:ctrl]: httppolicyset:http_security_policy> rules
 New object being created
 [admin:ctrl]: httppolicyset:http_security_policy:rules> name rule1
 [admin:ctrl]: httppolicyset:http_security_policy:rules> match
 [admin:ctrl]: httppolicyset:http_security_policy:rules:match>
 [admin:ctrl]: httppolicyset:http_security_policy:rules:match> bot_detection_result
match_operation is_in
```

```
 [admin:ctrl]: httppolicyset:http_security_policy:rules:match:bot_detection_result>
 [admin:ctrl]: httppolicyset:http_security_policy:rules:match:bot_detection_result>
classifications
 New object being created
 [admin:ctrl]:
httppolicyset:http_security_policy:rules:match:bot_detection_result:classifications> type
dangerous_bot
 [admin:ctrl]:
httppolicyset:http_security_policy:rules:match:bot_detection_result:classifications>
 [admin:ctrl]:
httppolicyset:http_security_policy:rules:match:bot_detection_result:classifications> save
 [admin:ctrl]: httppolicyset:http_security_policy:rules:match:bot_detection_result> save
 [admin:ctrl: httppolicyset:http_security_policy:rules:match> save
 [admin:ctrl]: httppolicyset:http_security_policy:rules> action
 [admin:ctrl]: httppolicyset:http_security_policy:rules:action> action
http_security_action_close_conn
 [admin:ctrl]: httppolicyset:http_security_policy:rules:action> save
 [admin:ctrl]: httppolicyset:http_security_policy:rules> save
 [admin:ctrl]: httppolicyset:http_security_policy> save
 [admin:ctrl]: httppolicyset> save
```

Note For each of the default objects in the system, the admin can supply their own logic that takes precedence.

- System-BotConfigConsolidator - Custom consolidation script
- System-BotMapping - Custom mapping
- System-BotIPReputationTypeMapping - Custom mapping

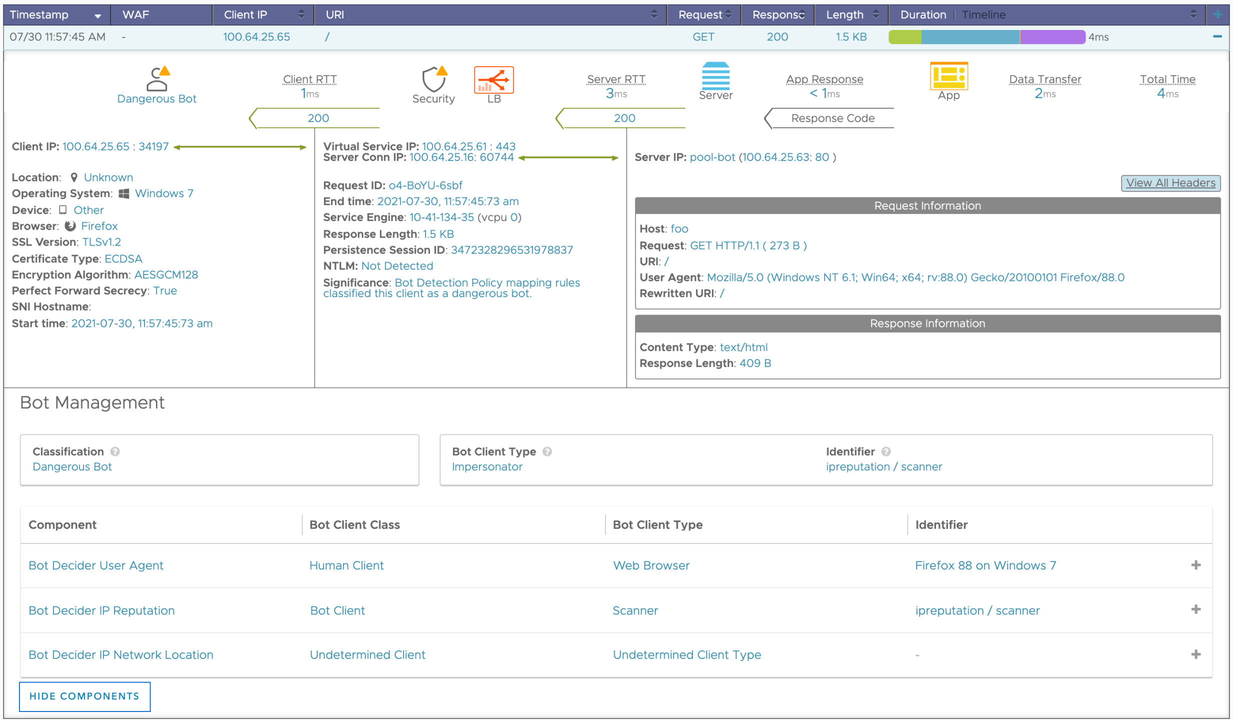
Creating the customized botdetectionpolicy, botmapping, botconfigconsolidator and so on is supported. However, if you need to custom any of these, you can contact the Support team. To learn about the support options available for you, visit the VMware Support Offerings and Services page.

Logs and Visibility Example

This section describes the examples for bot management logs.

Example: Example 1

In the example below, NSX Advanced Load Balancer logs displays all the important data points like classification, client type, identifier and confidence level.



Timestamp	WAF	Client IP	URI	Request	Response	Length	Duration | Timeline
07/30 11:57:45 AM	-	100.64.25.65	/	GET	200	1.5 KB	4ms

Client IP: 100.64.25.65 : 34197

Location: Unknown
Operating System: Windows 7
Device: Other
Browser: Firefox
SSL Version: TLSv1.2
Certificate Type: ECDSA
Encryption Algorithm: AESGCM128
Perfect Forward Secrecy: True
SNI Hostname:
Start time: 2021-07-30, 11:57:45:73 am

Virtual Service IP: 100.64.25.61 : 443
Server Conn IP: 100.64.25.16: 60744

Request ID: o4-BoYU-6sbf
End time: 2021-07-30, 11:57:45:73 am
Service Engine: 10-41-134-35 (vcpu 0)
Response Length: 1.5 KB
Persistence Session ID: 3472328296531978837
NTLM: Not Detected
Significance: Bot Detection Policy mapping rules classified this client as a dangerous bot.

Server IP: pool-bot (100.64.25.63: 80)

Request Information

Host: foo
Request: GET HTTP/1.1 (273 B)
URI: /
User Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Rewritten URI: /

Response Information

Content Type: text/html
Response Length: 409 B

Bot Management

Classification Dangerous Bot

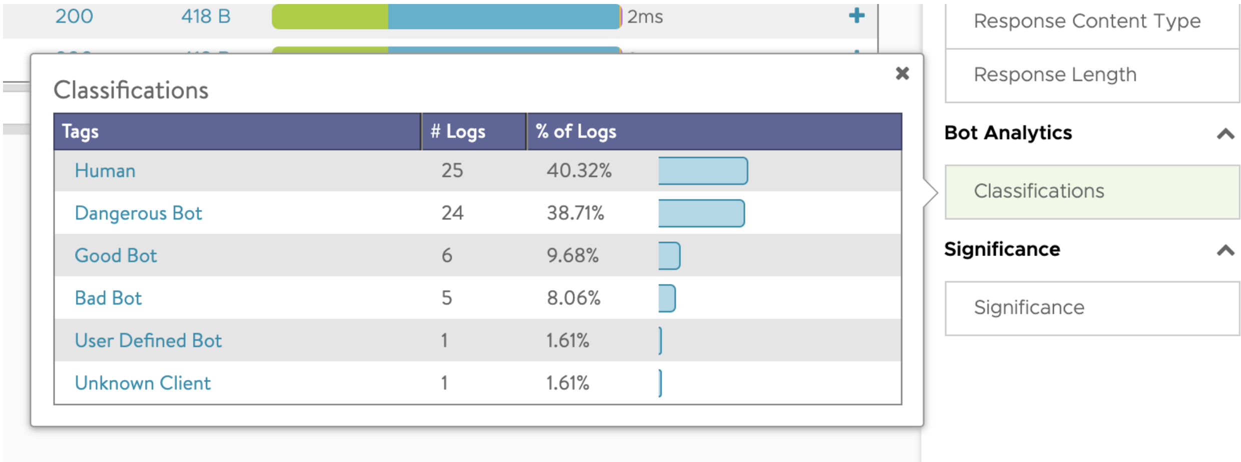
Bot Client Type Impersonator

Identifier ipreputation / scanner

Component	Bot Client Class	Bot Client Type	Identifier
Bot Decider User Agent	Human Client	Web Browser	Firefox 88 on Windows 7
Bot Decider IP Reputation	Bot Client	Scanner	ipreputation / scanner
Bot Decider IP Network Location	Undetermined Client	Undetermined Client Type	-

Example: Example 2

On the right side of the UI screen under logs, you can view the consolidated logs. Under summary, you can view Bot analytics. The Bot analytics displays the different types of Bot that is detected in the given period of time.



Classifications

Tags	# Logs	% of Logs
Human	25	40.32%
Dangerous Bot	24	38.71%
Good Bot	6	9.68%
Bad Bot	5	8.06%
User Defined Bot	1	1.61%
Unknown Client	1	1.61%

Special Cases

1 If the requirement is to skip Bot detection on certain requests, for instance, for requests coming from certain client IPs can be done by creating allow list in Bot policy.

The following are the configuration steps:

```
[admin:ctrl]: > configure botdetectionpolicy System-BotDetectionPolicy
 [admin:ctrl]: botdetectionpolicy> allow_list
 [admin:ctrl]: botdetectionpolicy:allow_list>
 [admin:ctrl]: botdetectionpolicy:allow_list> rules
 New object being created
 [admin:ctrl]: botdetectionpolicy:allow_list:rules> name rule1
 [admin:ctrl]: botdetectionpolicy:allow_list:rules> condition
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition>
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition> client_ip
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition:client_ip> match_criteria
is_in
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition:client_ip>
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition:client_ip> addrs 1.1.1.1
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition:client_ip>
save
 [admin:ctrl]: botdetectionpolicy:allow_list:rules:condition> save
 [admin:ctrl]: botdetectionpolicy:allow_list:rules>
 [admin:ctrl]: botdetectionpolicy:allow_list:rules> action bot_action_
 bot_action_bypass     Bypass BOT
detection.
 bot_action_continue   Stop allow-list processing and move on to BOT
detection.
 [admin:ctrl]: botdetectionpolicy:allow_list:rules> action bot_action_
 bot_action_bypass     Bypass BOT
detection.
 bot_action_continue   Stop allow-list processing and move on to BOT
detection.
 [admin:ctrl]: botdetectionpolicy:allow_list:rules> action bot_action_bypass
 [admin:ctrl]: botdetectionpolicy:allow_list:rules> save
 [admin:ctrl]: botdetectionpolicy:allow_list> save
 [admin:ctrl]: botdetectionpolicy> save
```

Similarly, you can create more rules to match on other criteria like path, host header, cookie, headers, protocol etc.

`allow_list` is a list of rules consisting of conditions mapped to the actions. In each rule, the condition can contain properties of the request like `client_ip`, host header etc. The actions can be “bypass” (skip all further bot detection) or “continue” (Stop allow-list processing and move on to BOT detection).

2 You need to disable one of the three decision components, for instance, you can disable IP location check component.

```
[admin:ctrl]:> configure botdetectionpolicy System-BotDetectionPolicy
 [admin:ctrl]:botdetectionpolicy> ip_location_detector
 [admin:ctrl]:botdetectionpolicy:ip_location_detector> no enabled
 +--------------------------------+--------------------------------+
 |           Field                |              Value             |
 +--------------------------------+--------------------------------+
 |   enabled                      |  False                         |
 |   ip_location_db_ref           |  System-GeoDB                  |
 |   system_cloud_providers_ref   |  System-BotCloudProviders      |
 |   system_search_engines_ref    |  System-BotSearchEngines      |
 +-------------------------------+-------------------------------+
 [admin:ctrl]:botdetectionpolicy:ip_location_detector> save
 [admin:ctrl]:botdetectionpolicy>save
```

Note The name of individual `BotMappingRule` objects in a `BotMapping` object is mandatory. Hence, you will not be able to create any new objects without a name. Existing objects are assigned an auto-generated name during the upgrade, following the pattern ‘Mapping Rule 0’, ‘Mapping Rule 1’ and so on, where the number in the name is the index of the rule.

BOT Management Service

This section explains Bot Management service offered as part of Live Security Threat Intelligence.

Bot management is a strategy that enables you to filter which Bots are allowed to access your web assets and which should be rate-limited or blocked completely. This service currently delivers real-time feed for the **User-Agent** database which is a critical bot detector component. Customers can protect their applications from bad bots by enabling this service on their Controller deployments.

Note It is important to enable IP Reputation service to obtain comprehensive protection from bad bots.

Feature Highlights

- Bot detection
- Bot classification
- Allow-deny, rate-limit bad bots

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. User-Agent database updates are pushed only to the Controllers where this service is opted-in (enabled).

Data Retention:

Does not apply to this service.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure, including, NSX, vCenter, and others.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is an **opt-in** service and is disabled by default. Customers needs to opt-in to enable this service. To opt-in to this service and enable User-Agent DB updates.

1. Navigate to **Administration > Settings > Cloud Services**.
2. Click **EDIT**.
3. Under **Live Security Threat Intelligence**, select **User Agent DB**.
4. Click **SAVE**.

Note Customers can opt-out of this service at any time to stop the IP Reputation updates.

Service Details

VMware utilizes `whatismybrowser` as its User-Agent database source. User-Agent database is cached on the NSX Advanced Load Balancer Cloud Console portal. Registered NSX Advanced Load Balancer Controllers where this service is enabled, pull User-Agent database data from NSX Advanced Load Balancer Cloud Console portal. The Controllers then immediately update connected Service Engines as part of its configuration update process.

Impact of Unavailability

During the period that this service is down, new User-Agent database updates are not pushed to enabled NSX Advanced Load Balancer Controllers. Load Balanced applications continue to utilize cached User-Agent database (in conjunction with other Bot detectors) available on the NSX Advanced Load Balancer Controllers to detect, classify and protect against bad bots.

Web Application Firewall (WAF) Signatures Service

This section explains Web Application Firewall (WAF) Signatures Service offered as part of Live Security Threat Intelligence.

NSX Advanced Load Balancer WAF protects web applications from common vulnerabilities as identified by Open Web Application Security Project (OWASP), such as SQL Injection (SQLi) and Cross-site Scripting (XSS), while providing the ability to customize the rule set for each application.

Feature Highlights

- Notify when new WAF CRS rules are available.
- Automatically download new WAF CRS rules when available.

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. WAF CRS Rules are pushed only to the NSX Advanced Load Balancer Controllers where this service is opted-in (enabled).

Data Retention:

Does not apply to this service.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure including NSX, vCenter, and others.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is an 'opt-in' service and is disabled by default.

The steps to opt-in to this service and enable automatic support case creation are as follows

1. Navigate to **Administration > Cloud Services**.
2. Click **EDIT**.
3. Under **Live Security Threat Intelligence** select **Enable Cloud Services WAF Management**.
4. Select **Receive notifications when new CRS data is available** to receive notifications when new updates are available.
5. Select **Enable auto download WAF Signatures** to automatically download new WAF CRS rules when available.
6. Click **SAVE**.

Note You can opt-out of this service at any time and the WAF CRS Rule notifications and updates will stop.

Service Details

NSX Advanced Load Balancer threat research team releases new WAF signatures (Core Rule Set) every quarter. These signatures can be consumed in one of the following two ways:

1. *Manual deployment*: User manual downloads WAF signatures from NSX Advanced Load Balancer Cloud Console Portal and then uploads them on required VNSX Advanced Load Balancer Controller clusters, or
2. *Automated deployment*: Web Application Firewall (WAF) Signatures Service automatically pushes new rules to registered NSX Advanced Load Balancer Controller clusters where this service is enabled. Steps are described in the 'How to enable this service' section.

For manual deployment, only enable the 'Receive notifications when new CRS data is available' Opt-In as described in the '*How to enable this service*' section. When new WAF CRS Rules are available, the 'CRS_UPDATE' event will be generated on the NSX Advanced Load Balancer Controller and will have a signed download link. You can click on this link to download the WAF CRS Rules and then upload the same to the NSX Advanced Load Balancer Controller as follows:

1. Navigate to **Templates WAF > CRS**.
2. Click on **Upload File**, select the downloaded WAF CRS Rules.
3. Click **Open**.

Events of Interest

The following events are generated on the Controller when WAF Signatures service is enabled:

`CRS_UPDATE`:

New WAF CRS Rules are available.

`CRS_DEPLOYMENT_SUCCESS`:

WAF CRS Rules deployment succeeded on the Controller.

`CRS_DEPLOYMENT_FAILURE`:

WAF CRS Rules deployment failed on the Controller.

Impact of Unavailability

During the period that this service is down, new WAF CRS Signatures will not be available. Load Balanced applications will continue to utilize WAF CRS Rules available on the Controllers.

Proactive Support

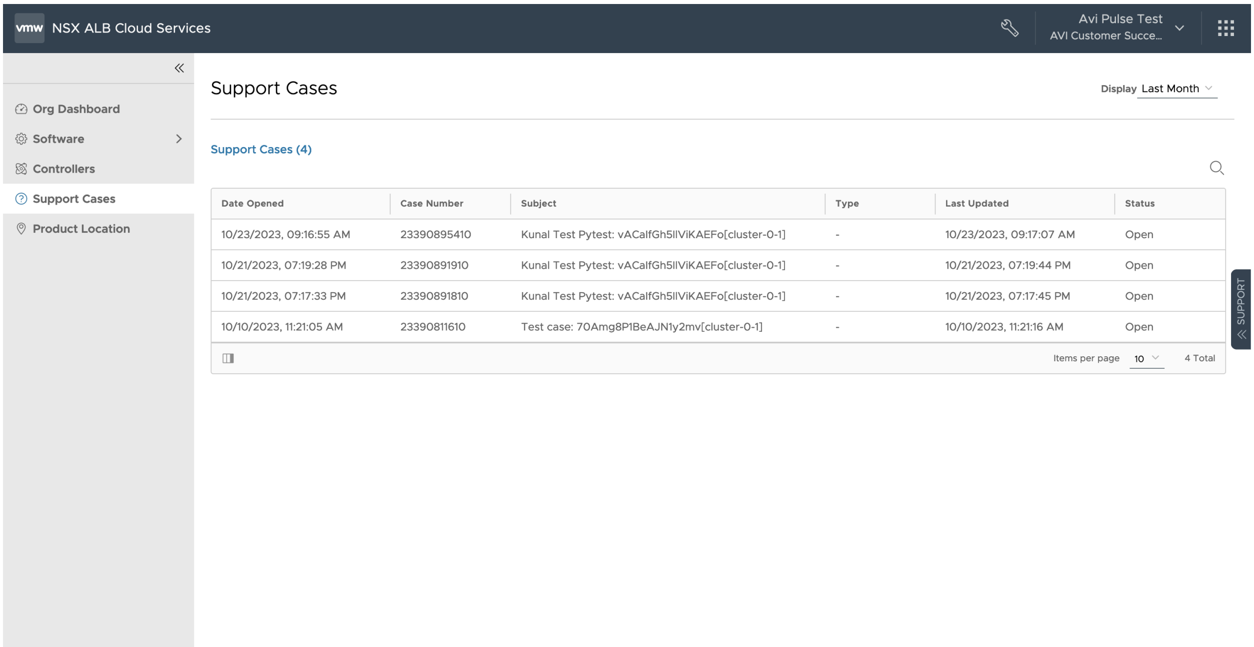
Proactive Support service offered as part of NSX Advanced Load Balancer Cloud Console delivers zero-touch support experience on enabled NSX Advanced Load Balancer deployments.

It takes lot of time and effort into initiating and tracking support queries and finding resolutions to issues related to the product.

It involves interacting with multiple entities such as the NSX Advanced Load Balancer to collect relavant information such as tech-support and the customer connect support portal to create cases and upload tech support. Additionally, there is scope for loss or mis-communication of vital information.

Proactive support provides a hassle-free experience and manages end-to-end experience for all support related tasks, including automatically creating a case, uploading relavant information to the case in a timely manner, and others. You can also use the NSX Advanced Load Balancer Controller to create a support case.

If the customer creates a case with a Basic case management or if it gets raised through proactive case management service than such open cases are listed on Cloud Console UI as shown below:



Support Cases

Display Last Month

Support Cases (4)

Date Opened	Case Number	Subject	Type	Last Updated	Status
10/23/2023, 09:16:55 AM	23390895410	Kunal Test Pytest: vACalfGh5llViKAEFo[cluster-0-1]	-	10/23/2023, 09:17:07 AM	Open
10/21/2023, 07:19:28 PM	23390891910	Kunal Test Pytest: vACalfGh5llViKAEFo[cluster-0-1]	-	10/21/2023, 07:19:44 PM	Open
10/21/2023, 07:17:33 PM	23390891810	Kunal Test Pytest: vACalfGh5llViKAEFo[cluster-0-1]	-	10/21/2023, 07:17:45 PM	Open
10/10/2023, 11:21:05 AM	23390811610	Test case: 70Amg8P1BeAJN1y2mv[cluster-0-1]	-	10/10/2023, 11:21:16 AM	Open

Items per page 10 4 Total

Basic Case Management

This section explains Basic Case Management service offered as part of Proactive Support. Basic Case Management helps customers create and manage VMware support cases directly from their NSX Advanced Load Balancer Controllers.

Feature Highlights

- Create, assign, edit and view VMware support cases from NSX Advanced Load Balancer Controller.
- Seamlessly attach files such as Tech-Support, TCP Dump, and so on to raise support cases from NSX Advanced Load Balancer Controller.

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. Support case data is directly sent to VMware's customer connect support portal.

Data Retention:

Does not apply to this service.

How to enable this service

This is an 'opt-in' service and is disabled by default.

The steps to opt-in to this service are as follows:

1. Navigate to **Administration > Cloud Services**.
2. Click **EDIT**.
3. Select **Enable Proactive Support**.
4. Click **SAVE**.

Service Details

Any logged in user can create support cases from the Controller. By default, the case will be viewed in the context of the Controller.

You can create a new case by navigating to **Administration > Support > Cases** and click on **Create** button. You can specify the necessary details.

You can view all active cases, and all operations such as add comment, attachments, through NSX Advanced Load Balancer. The open cases are listed on NSX Advanced Load Balancer Cloud Console too.

Events of Interests

The following events are generated on the NSX Advanced Load Balancer Controller when a support case is created:

- `ALBSERVICES_SUPPORT_CASE_CREATED`

Impact of Unavailability

During the period that this service is down, support cases cannot be logged from the NSX Advanced Load Balancer Controllers. However, support cases can be logged by customers through the customerconnect.vmware.com portal to get access to VMware technical support.

Tech Support Attachment

This section explains Tech Support Attachment service offered as part of Proactive Support. Tech Support Attachment helps customers seamlessly attach relavant debug log information to thier support cases directly from their NSX Advanced Load Balancer Controllers.

Feature Highlights

- Generate and attach Tech Supports to a new support case.
- Generate and attach Tech Supports to an existing support case.

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. Support case data is directly sent to VMware's customer connect support portal.

Data Retention:

Does not apply to this service.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure including NSX, vCenter, and others.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is an 'opt-in' service and is disabled by default.

The steps to opt-in to this service are as follows:

1. Navigate to **Administration > Cloud Services**.
2. Click **EDIT**.
3. Select **Enable Proactive Support**.
4. Click **SAVE**.

Service Details

You can trigger tech support bundles for an existing or new support case. You can also choose the type of tech support bundle and generate the same. The collection of tech support bundle is triggered in the background. After the bundle is successfully created, it is uploaded to the case.

You can create a tech-support and attach it to a case as follows:

1. Navigate to **Administration > Tech Support**.
2. Click on **Generate Tech Support**.
3. Select the **Type** of Tech Support to generate.
4. To attach the Tech Support to a support case, select **Attach to Support Case on Completion**.
   a. To attach the Tech Support to an existing support case, pick the appropriate support case from the drop-down list.
   b. To attach the Tech Support to a new support case:
      1. Click **Create** and fill the details to create a support case as explained in the Basic Case Management section.
      2. Created support case would be auto chosen in the Tech Support wizard.
5. Click **Generate**.

You can view the existing cases by navigating to **Administration** > **Support** > **Cases**.

Events of Interest

The following events are generated on the NSX Advanced Load Balancer Controller when a support case is created:

- `ALBSERVICES_SUPPORT_CASE_CREATED`

Impact of Unavailability

During the period that this service is down, technical support logs can be generated on the NSX Advanced Load Balancer Controllers. These Technical support logs cannot be attached to the specified support cases directly from the NSX Advanced Load Balancer Controllers. However, technical support logs can be attached to support cases by customers through the *customerconnect.vmware.com* portal.

Proactive Case Management

This section explains Proactive Case Management service offered as part of Proactive Support. Proactive Case Management enables zero-touch support experience on enabled NSX Advanced Load Balancer deployments by detecting faults and automatically creating support cases.

Feature Highlights

- Zero-Touch automatic support case creation.
- Ability to define custom faults via the Alerts framework to create support cases.
- Deduplication to avoid creating multiple support cases for the same issue.

Data Collection and Retention Policy

Data Collection:

No data is collected by and for this service. Support case data is directly sent to VMware's customer connect support portal.

Data Retention

Does not apply to this service.

Note

- This service does not store or exchange any customer data.
- This service has no access to customer infrastructure including NSX, vCenter, etc.
- This service does not read or write any configurations on the registered NSX Advanced Load Balancer Controllers.

How to enable this service

This is an 'opt-in' service and is disabled by default.

The steps to opt-in to this service and enable automatic support case creation are as follows:

1 Navigate to **Administration > Cloud Services**.

2 Click **EDIT**.

3 Select **Enable Proactive Support**.

4 Select **Enable automatic cases on system failure** or **Enable automatic cases on SE failure**.

5 Click **SAVE**.

Service Details

With Proactive Case Management, the NSX Advanced Load Balancer Controller creates a support case automatically whenever a critical event occurs in the system. Appropriate debug logs such as core archives and Tech Support bundles are automatically uploaded as well.

By default, creating support cases for the following critical events are available to be enabled through opt-ins.

1 NSX Advanced Load Balancer Service Engine Failure, and

2 NSX Advanced Load Balancer Controller Service Failure.

Once an opt-in is enabled, the Controller monitors for the respective Events or Alerts and creates a support case when a critical failure is detected.

Once either of the opt-in options are selected, the system enables the alert configuration which monitors the Audit Compliance Event.

Note Creating support cases for other critical events can be enabled by defining appropriate custom *Alerts*.

You can view the Proactive Case Management configuration as follows:

1 Navigating to **Operations > Alerts > Alert Config**.

2 Edit **System-Process-Crash-Proactive-Support** Alert Config object.

Events of Interest

The following events are generated on the NSX Advanced Load Balancer Controller when a support case is created:

- `ALBSERVICES_SUPPORT_CASE_CREATED`

Impact of Unavailability

During the period that this service is down, support case creation is not created automatically even if critical events are triggered. However, support cases for these critical events can be logged by customers by getting access to VMware technical support through the *customerconnect.vmware.com* portal.

Inventory Service

Inventory service gathers metrics, statistics and other Controller information regularly to be made available on Cloud Console dashboard.

Inventory information does not reflect real time status of the Controller, it can be several hours old. The dashboard shows metrics and statistics while allowing the users to search configuration information like VS, Pool or VIP by their name or IPs.

Feature Highlights

- Allows customers to search for specific VS, Pool across controllers.
- License usage, SE version and other metrics of multiple registered Controllers are available on the common dashboard.

Data Collection and Retention Policy

Data is gathered from the Controllers only after getting the consent from the users. This is done by enabling the corresponding opt-in post registration. By default this option is disabled. The Controller comes with multiple knobs to regulate the information gathered. Using these knobs, you can enable just metrics and statistics while disabling other information gathering.

Once the Controller is de registered, the data will be retained for not more than 30 days so that it can be reused if the Controller gets re-registered. After 30 days period, the data is cleaned up.

Enabling this Service

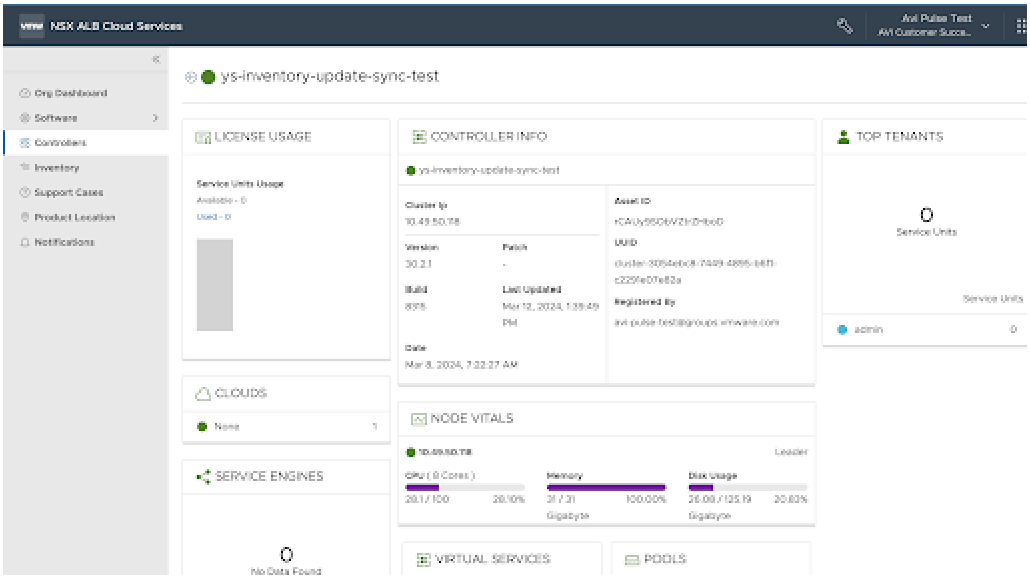
Starting with NSX Advanced Load Balancer version 22.1.6, the feature is shipped only for tech preview and available for selected users. The users with service enabled can opt in for it on their registered Controller by turning on inventory options using below CLI:

```
> configure albservicesconfig
albservicesconfig > operations_config
albservicesconfig.operations_config > inventory_config
albservicesconfig.operations_config.inventory_config > enable
albservicesconfig.operations_config.inventory_config > enable_search_info
albservicesconfig.operations_config.inventory_config > save
albservicesconfig.operations_config> save
albservicesconfig > save
```

Service Details

The Controller statistics are collected every two hours once. You can view the statistics by checking the specific Controller dashboard.

Note Work is in progress to allow users to refresh it immediately, if required.



Service Units Usage
Available - 0
Used - 0

ys-inventory-update-sync-test

Cluster Ip: 10.49.50.78
Version: 30.2.1
Patch: -
Build: 8375
Last Updated: Mar 12, 2024, 1:39:49 PM
Date: Mar 8, 2024, 7:22:27 AM
Asset ID: rCAUy9SObVZ1rDHboD
UUID: cluster-3054ebc8-7449-4895-b6f1-c229fe07e82a
Registered By: avi-pulse-test@groups.vmware.com

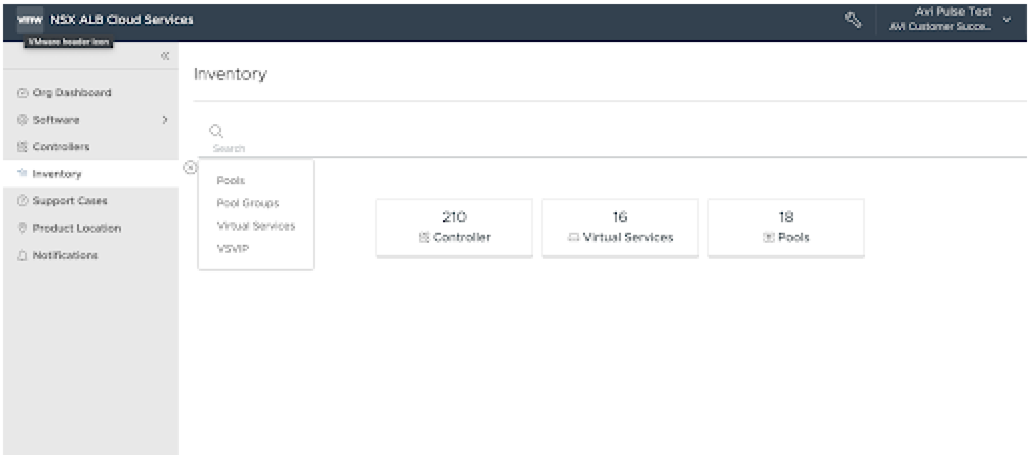
0 Service Units
Service Units
admin 0

None 1

0 No Data Found

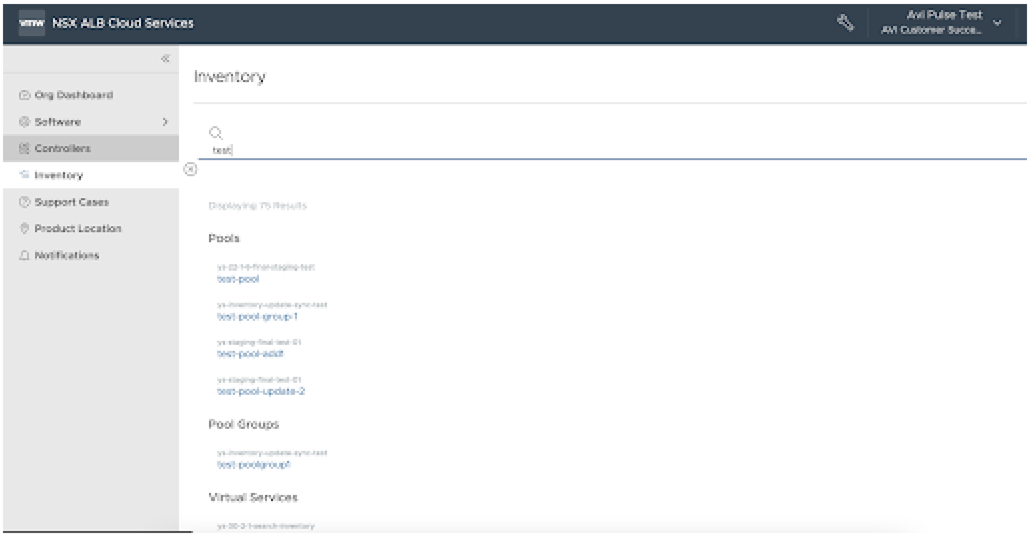
10.49.50.78 Leader
CPU (8 Cores): 20.1 / 100 20.10%
Memory: 31 / 31 Gigabyte 100.00%
Disk Usage: 26.08 / 125.19 Gigabyte 20.83%

In addition to statistics, if **Search Info** option is enabled then you can also search for the Controller configuration objects like virtual service, pool, servers and VIPs by name or IP. You can also search for specific object such as virtual service. The search can be extended to include all object types by default.

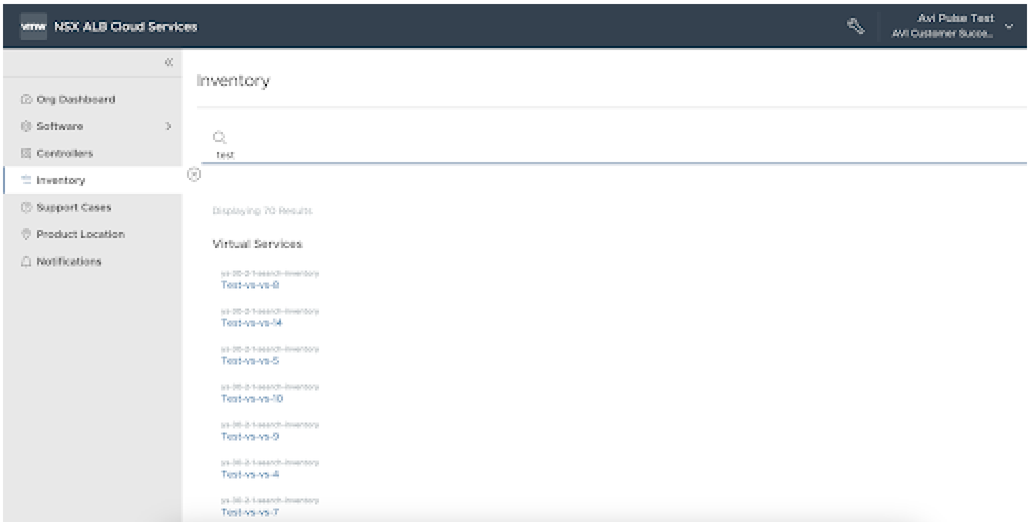


210 Controller
16 Virtual Services
18 Pools

By default the search looks for content across all object type, such as pools, virtual services and so on.



By selecting an object type, the search can be restricted to only configuration objects of that particular type, such as virtual service.



Other Services

This section explains other services provided by the Cloud Console.

Software Download Service

This service provides customers access to NSX Advanced Load Balancer software. Customers can access software by following these steps:

1. Launch https://portal.avipulse.vmware.com.
2. Authenticate using customerconnect credentials.
3. Navigate to **Software > NSX Advanced Load Balancer Vantage**.
4. Pick the release of choice.

5 Download the appropriate package.

Note WAF CRS Rules are also available for downloads.

Cloud Console API

5

This section lists the Cloud Console APIs.

For information on Cloud Console APIs, refer to Swagger UI (vmware.com).

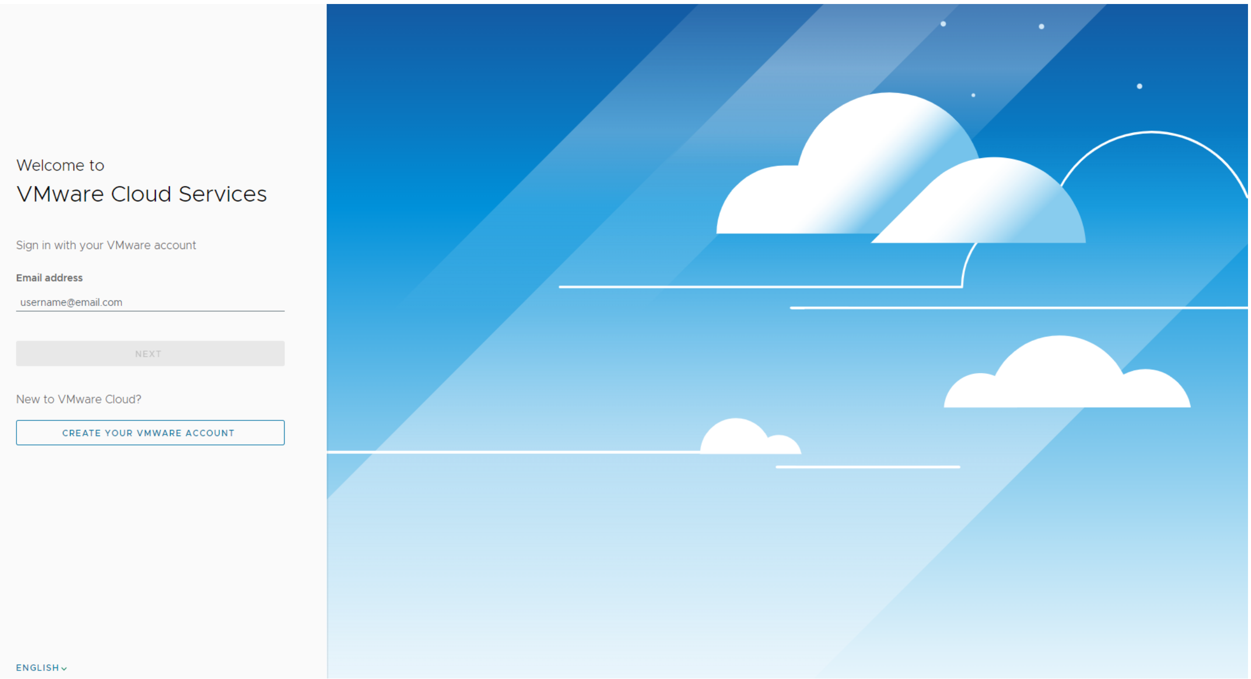
SaaS and Cloud Console FAQ

6

This section provides answers to, or clarifications on, potential issues encountered while onboarding NSX Advanced Load Balancer with Cloud Console.

The VMware Cloud Console Platform, or CSP, refers to VMware's support for Cloud Console. VMware Cloud Console enables you to integrate, manage, and secure applications on Cloud resources. These services work for any Cloud Console using VMware and can help you centralize the management and maintenance of hybrid or multi-cloud environments.

One of these Cloud Consoles is the NSX Advanced Load Balancer (formerly known as Avi Vantage). In order to utilize Central Licensing and the other Cloud capabilities you need access to the Cloud Console.



Welcome to

VMware Cloud Services

Sign in with your VMware account

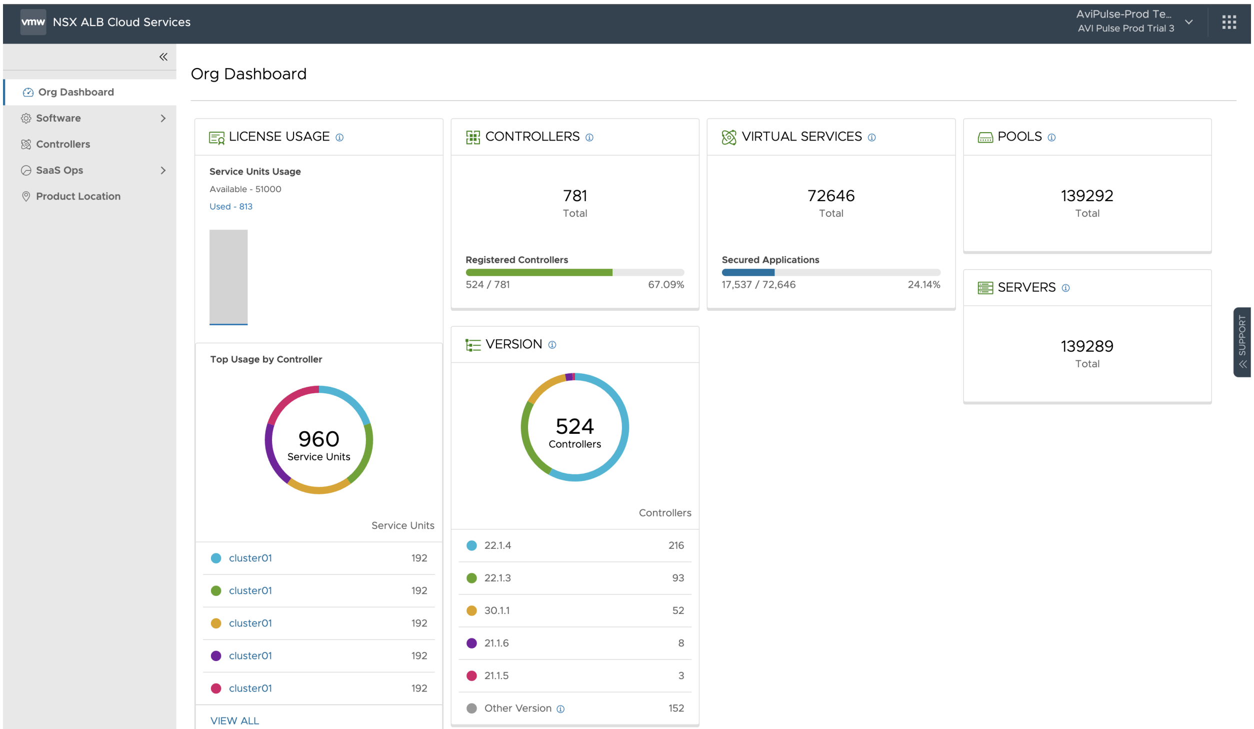
Email address: username@email.com

The VMware Cloud Services™ allows you to manage your VMware Cloud Console Portfolio across hybrid and native public clouds. Using this console allows you to manage users, groups and roles, identity and access management, as well as billing and subscriptions (see Cloud Documentation for more details).

Central Licensing

The concept of Central Licensing as a feature of the NSX Advanced Load Balancer SaaS offering refers to the ability to aggregate and store NSX Advanced Load Balancer licenses in a central location, allowing you to allocate/ de-allocate licenses (or service units) to various NSX Advanced Load Balancer Controllers registered with Cloud Console.

The Central Licensing dashboard is available at: https://portal.avipulse.vmware.com/dashboard/customer



Org Dashboard

LICENSE USAGE

Service Units Usage
Available - 51000
Used - 813

Top Usage by Controller

960 Service Units

	Service Units
cluster01	192
cluster01	192
cluster01	192
cluster01	192
cluster01	192

VIEW ALL

CONTROLLERS

781 Total

Registered Controllers
524 / 781 67.09%

VERSION

524 Controllers

	Controllers
22.1.4	216
22.1.3	93
30.1.1	52
21.1.6	8
21.1.5	3
Other Version	152

VIRTUAL SERVICES

72646 Total

Secured Applications
17,537 / 72,646 24.14%

POOLS

139292 Total

SERVERS

139289 Total

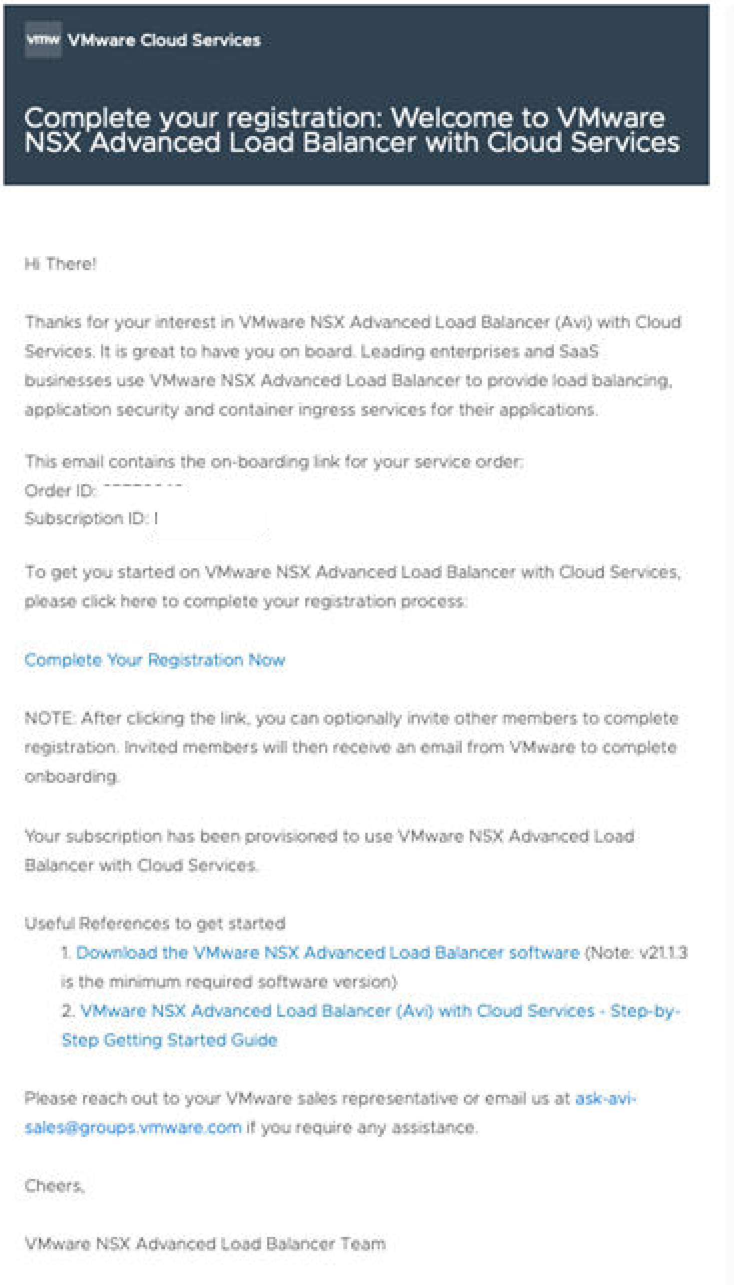
Read the following topics next:

- How to add users to my Cloud Services Portal (CSP) Organisation?
- What Version of NSX Advanced Load Balancer is compatible with Cloud Console?
- Can the CSP (Cloud Services Portal) Organization for NSX Advanced Load Balancer Licenses be changed?
- What if the Onboarding Invitation was sent to the wrong email address?
- My organization just purchased SaaS Licenses in Cloud Console, but upgrading our NSX Advanced Load Balancer to a version starting with 21.1.3 will take some time; what can we do?
- I logged in to my Cloud provider, but I cannot use my NSX Advanced Load Balancer Licenses to deploy Virtual Machines. Are there any issues with the Licenses?
- What Role and/ or Permissions do I need to register my Controller with Cloud Console?
- How do I check my NSX Advanced Load Balancer with Cloud Console Subscription Validity?

- Our systems are behind a proxy for security reasons. Will that block our Controller from communicating with the Central Licensing?
- Where can I find the Subscription ID for my NSX Advanced Load Balancer with Cloud Console Subscription?
- Can I designate completion of Cloud Console Registration process to someone else?
- My Controller was registered with Avi Pulse, do I need to register with Cloud Console?
- After I upgrade to NSX Advanced Load Balancer version 21.1.3 or greater, will my Controller automatically upgrade to Cloud Console?
- After upgrading to Cloud Console will I need to keep my old License files and information?
- I have SPP (Subscription Purchasing Program) Funds, can they be used to purchase NSX Advanced Load Balancer with Cloud Console Licenses?
- My old licenses were based on Service Cores; what is the difference between a Service Core and a Service Unit?

How to add users to my Cloud Services Portal (CSP) Organisation?

Before you begin with the process of registering with VMware Cloud Services, you will need a CSP Onboarding invitation email. This email will be automatically sent to you within 24 hours post purchase.



vmw VMware Cloud Services

Complete your registration: Welcome to VMware NSX Advanced Load Balancer with Cloud Services

Hi There!

Thanks for your interest in VMware NSX Advanced Load Balancer (Avi) with Cloud Services. It is great to have you on board. Leading enterprises and SaaS businesses use VMware NSX Advanced Load Balancer to provide load balancing, application security and container ingress services for their applications.

This email contains the on-boarding link for your service order:
Order ID:
Subscription ID: I

To get you started on VMware NSX Advanced Load Balancer with Cloud Services, please click here to complete your registration process:

Complete Your Registration Now

NOTE: After clicking the link, you can optionally invite other members to complete registration. Invited members will then receive an email from VMware to complete onboarding.

Your subscription has been provisioned to use VMware NSX Advanced Load Balancer with Cloud Services.

Useful References to get started

1. Download the VMware NSX Advanced Load Balancer software (Note: v21.1.3 is the minimum required software version)
2. VMware NSX Advanced Load Balancer (Avi) with Cloud Services - Step-by-Step Getting Started Guide

Please reach out to your VMware sales representative or email us at ask-avi-sales@groups.vmware.com if you require any assistance.

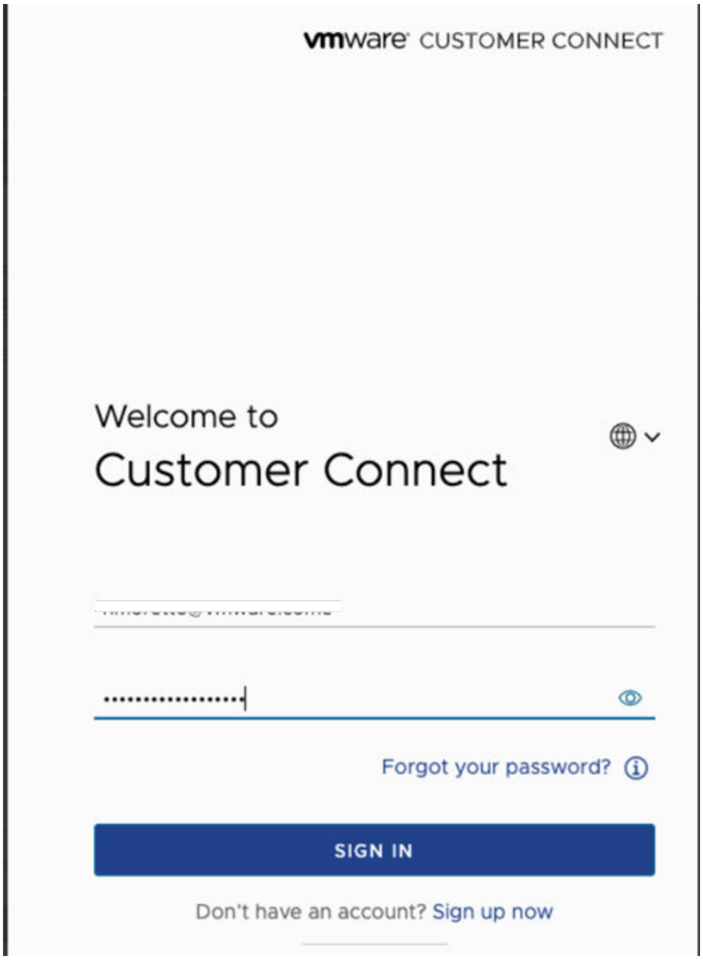
Cheers,

VMware NSX Advanced Load Balancer Team

The onboarding email is often sent to a purchasing agent, department director, or other personnel. Ensure that a member of the team who will support and configure the NSX Advanced Load Balancer is part of the onboarding process or added as an owner of the VMware CSP Organization where you can map your NSX Advanced Load Balancer subscription. Many customers map the subscriptions to all cloud-based products in the same Organization.

Note

- See Onboarding an NSX Advanced Load Balancer with Cloud Console Subscription to initiate the Onboarding process.
- During the process, you will be prompted with VMware Customer Connect link. You can log in using your VMware account or you can create one.

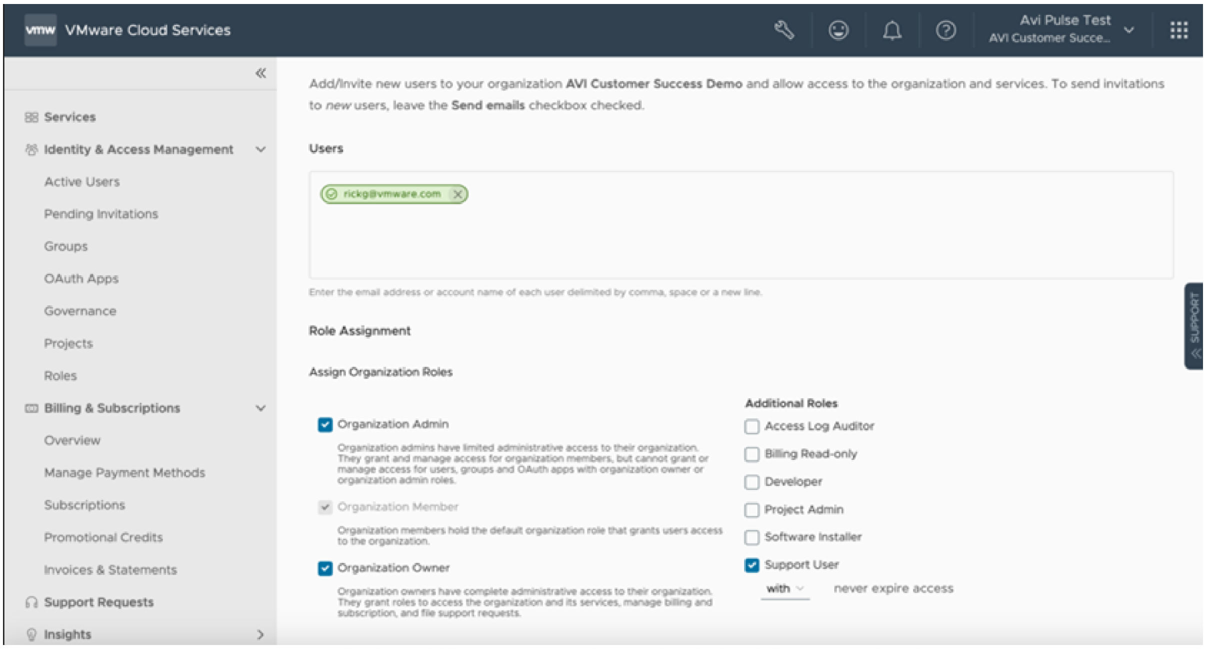


The steps to add users to a CSP organisation are as follows:

1. Navigate to **Identity & Access Management > Active Users** on the left hand side. Select **ADD USERS**.

   a. Enter the email address(es) of the new administrative user(s).

2. Under **Role Assignment**, check **Organization Admin** and **Organization Owner** boxes. This is a mandatory step.



Add/Invite new users to your organization **AVI Customer Success Demo** and allow access to the organization and services. To send invitations to *new* users, leave the **Send emails** checkbox checked.

Users

rickg@vmware.com

Enter the email address or account name of each user delimited by comma, space or a new line.

Role Assignment

Assign Organization Roles

☑ Organization Admin

Organization admins have limited administrative access to their organization. They grant and manage access for organization members, but cannot grant or manage access for users, groups and OAuth apps with organization owner or organization admin roles.

☑ Organization Member

Organization members hold the default organization role that grants users access to the organization.

☑ Organization Owner

Organization owners have complete administrative access to their organization. They grant roles to access the organization and its services, manage billing and subscription, and file support requests.

Additional Roles

☐ Access Log Auditor

☐ Billing Read-only

☐ Developer

☐ Project Admin

☐ Software Installer

☑ Support User

with never expire access

A user with organization member role must have 'support user' as an additional role.”

3 Under **Assign Service Roles**, click **ADD A SERVICE** to add the NSX Advanced Load Balancer, then click **ADD** button.

4 The recipient will receive an onboarding invitation (exactly like the one received by the original Organization Owner (above)) and complete the process of Onboarding the subscription.

What Version of NSX Advanced Load Balancer is compatible with Cloud Console?

NSX Advanced Load Balancer is compatible with versions 21.1.3 and later. This supports Cloud Console and Central Licensing. You can check the version by clicking on the icon in the upper right-hand corner of the user interface and select **About**NSX Advanced Load Balancer. See Upgrades and Patches section of the *Administration* guide for instructions on upgrading to a current version.

Can the CSP (Cloud Services Portal) Organization for NSX Advanced Load Balancer Licenses be changed?

During the onboarding process, the individual with Organization Owner rights can map the NSX Advanced Load Balancer subscription to the correct CSP Organization.

If you are an organisation owner, you can do this by clicking **Org Name** and then clicking **Manage Entitlements**. This will show you all CSP Organizations which have NSX Advanced Load Balancer with Cloud Console enabled. You can then choose any organization from that list to switch.

By default, Central Licensing fetches the default Organization from the CSP (Cloud Services Portal), which the user has previously mapped.

Note This is a one-time mapping that cannot be changed once selected.

What if the Onboarding Invitation was sent to the wrong email address?

If the subscription has not yet been redeemed, the invitation to register with Cloud Console can be resent to the correct email address. Your VMware account team can assist with arranging for the onboarding email to be sent to the correct individual(s).

My organization just purchased SaaS Licenses in Cloud Console, but upgrading our NSX Advanced Load Balancer to a version starting with 21.1.3 will take some time; what can we do?

It is strongly advised to upgrade to the minimum version that supports the SaaS licensing. Your VMware account team can discuss potential options to handle the interim period while the upgrade is being planned.

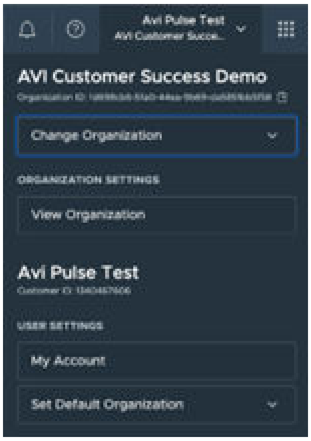
I logged in to my Cloud provider, but I cannot use my NSX Advanced Load Balancer Licenses to deploy Virtual Machines. Are there any issues with the Licenses?

There is a difference between NSX Advanced Load Balancer licensing and public cloud charges. You can deploy a Controller cluster in a production environment, On Prem or in the Cloud; then deploy Virtual Services, Service Engines and Server Pools on virtual machines or containers in the public Cloud. Those charges are independent of NSX Advanced Load Balancer subscription.

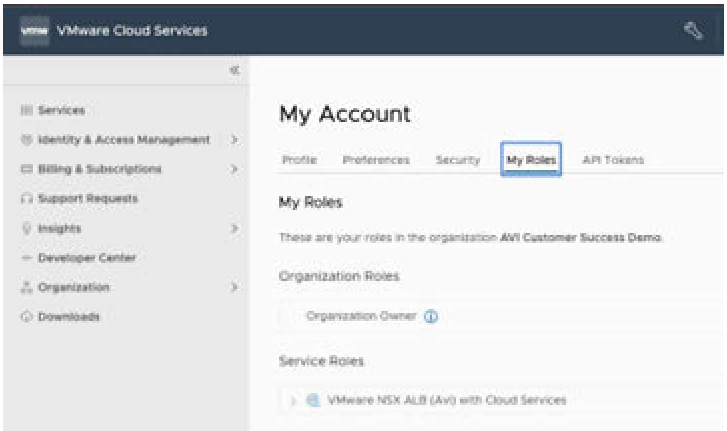
What Role and/ or Permissions do I need to register my Controller with Cloud Console?

You must have the role of an Organisation owner/ Organisation member with additional role of Support user/ Organisation administrator to be able to register an NSX Advanced Load Balancer Controller with Cloud Console. To check your current role:

- Go to the Cloud Services Portal, click on the user icon in the upper right-hand corner, from the drop-down select **My Account** under **User Settings**.



- Navigate to **My Roles** tab of **My Account** window. Check if **Organizational Roles** is set to **Organization Owner**. If it is not, then reach out to the Organisation Owner, to assign you the required rights. You may also reach out to your account team for assistance.



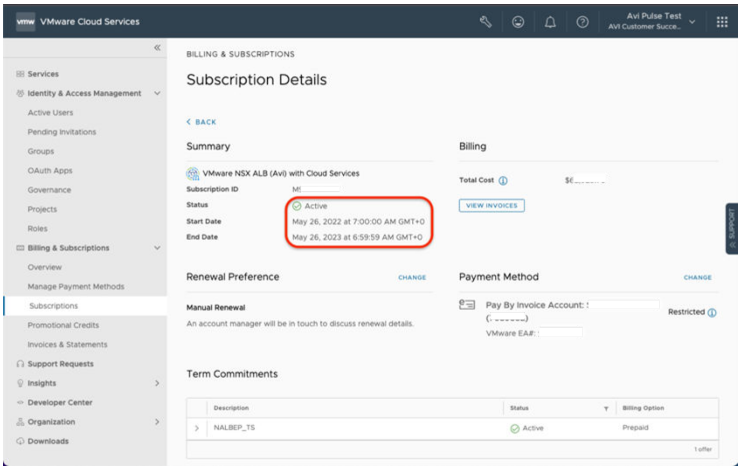
These are your roles in the organization **AVI Customer Success Demo**.

Organization Roles: Organization Owner

Service Roles: VMware NSX ALB (Avi) with Cloud Services

How do I check my NSX Advanced Load Balancer with Cloud Console Subscription Validity?

You can view your subscription information on the Cloud Services Portal. Navigate to **Billing & Subscriptions > Subscriptions**.



BILLING & SUBSCRIPTIONS

Subscription Details

Summary

VMware NSX ALB (Avi) with Cloud Services

Subscription ID	M[redacted]
Status	Active
Start Date	May 26, 2022 at 7:00:00 AM GMT+0
End Date	May 26, 2023 at 6:59:59 AM GMT+0

Billing

Total Cost $[redacted]

Renewal Preference

Manual Renewal

An account manager will be in touch to discuss renewal details.

Payment Method

Pay By Invoice Account: [redacted]
([redacted])
VMware EA#: [redacted]

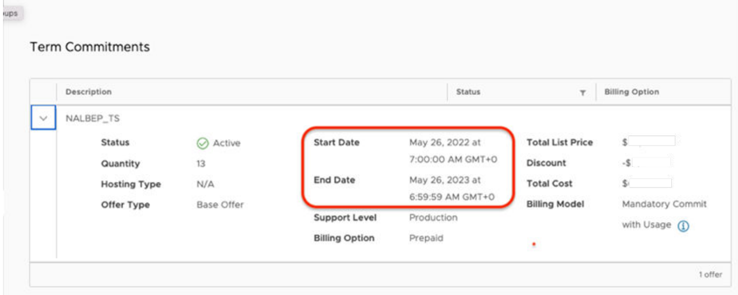
Restricted

Term Commitments

	Description	Status	Billing Option
>	NALBEP_TS	Active	Prepaid

1 offer

You can then view the details by clicking on the subscription hyperlink.



Term Commitments

Description	Status	Billing Option
NALBEP_TS		

Status	Active	Start Date	May 26, 2022 at 7:00:00 AM GMT+0	Total List Price	$[redacted]
Quantity	13			Discount	-$[redacted]
Hosting Type	N/A	End Date	May 26, 2023 at 6:59:59 AM GMT+0	Total Cost	$[redacted]
Offer Type	Base Offer			Billing Model	Mandatory Commit with Usage
		Support Level	Production		
		Billing Option	Prepaid		

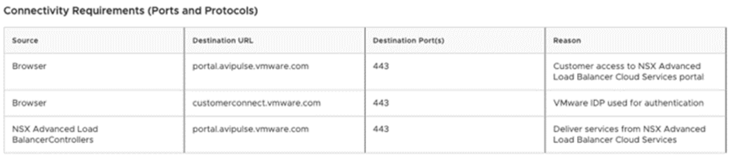
1 offer

Our systems are behind a proxy for security reasons. Will that block our Controller from communicating with the Central Licensing?

The NSX Advanced Load Balancer can be configured to use your proxy settings while communicating with Cloud Console. Navigate to **Administration > Cloud Services** and click **EDIT** button.

This will allow you to add settings for your proxy.

See Prerequisites for more details on the connectivity requirements and ensure that rules are configured in both directions.



Connectivity Requirements (Ports and Protocols)

Source	Destination URL	Destination Port(s)	Reason
Browser	portal.avipulse.vmware.com	443	Customer access to NSX Advanced Load Balancer Cloud Services portal
Browser	customerconnect.vmware.com	443	VMware IDP used for authentication
NSX Advanced Load BalancerControllers	portal.avipulse.vmware.com	443	Deliver services from NSX Advanced Load Balancer Cloud Services

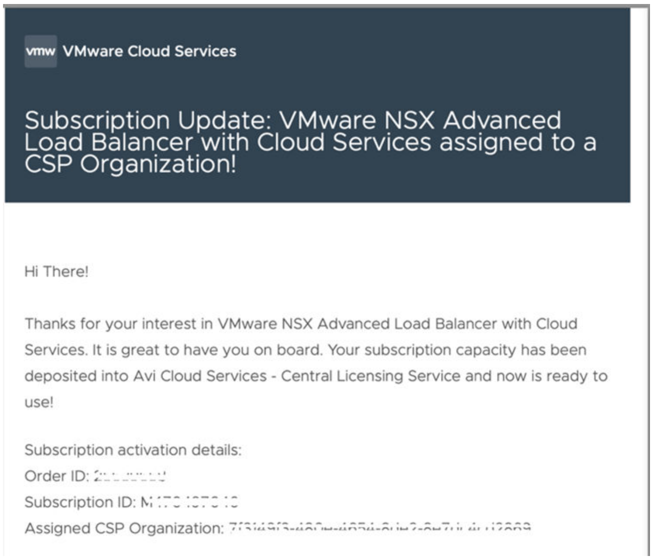
You can also configure the proxy parameters at the command shell as follows. For more details on accessing the command line, see CLI Access section in the *Administration* guide.

```
[admin:controller]: > configure systemconfiguration
[admin:controller]: systemconfiguration> proxy_configuration
[admin:controller]: systemconfiguration:proxy_configuration> host <FORWARD_PROXY_IP_OR_FQDN>
[admin:controller]: systemconfiguration:proxy_configuration> port <FORWARD_PROXY_PORT>
[admin:controller]: systemconfiguration:proxy_configuration> username <FORWARD_PROXY_USER>
[admin:controller]: systemconfiguration:proxy_configuration> password
<FORWARD_PROXY_PASSWORD>
[admin:controller]: systemconfiguration:proxy_configuration> save
[admin:controller]: systemconfiguration> save
[admin:controller]: > configure albservicesconfig
[admin:controller]: albservicesconfig> no use_split_proxy Overwriting the previously entered
value for use_split_proxy
[admin:controller]: albservicesconfig> no split_proxy_configuration
[admin:controller]: albservicesconfig> save
```

Where can I find the Subscription ID for my NSX Advanced Load Balancer with Cloud Console Subscription?

This information can be found by the customer and/or account team from the following:

- Purchase Order email
- Navigate to Cloud Console Portal under **Billing & Subscriptions > Subscriptions**.
- You can also find this in the Subscription Update email you received to register with VMware Cloud Console. You can contact yout account team for further details.



Subscription Update: VMware NSX Advanced Load Balancer with Cloud Services assigned to a CSP Organization!

Hi There!

Thanks for your interest in VMware NSX Advanced Load Balancer with Cloud Services. It is great to have you on board. Your subscription capacity has been deposited into Avi Cloud Services - Central Licensing Service and now is ready to use!

Subscription activation details:
Order ID: [redacted]
Subscription ID: [redacted]
Assigned CSP Organization: [redacted]

Can I designate completion of Cloud Console Registration process to someone else?

After clicking on registration link in the welcome email, you can optionally invite other members of your organization to complete the registration process. The invited member will receive an email with that invitation and can complete the registration thereafter.

My Controller was registered with Avi Pulse, do I need to register with Cloud Console?

Central Licensing and Cloud Console were intended to supercede the original Pulse Service. In addition, the Bot Management Service for WAF is only available with Cloud Console.

The following services are available through Avi Pulse and Cloud Console respectively:

Pulse Services

- IP Reputation service, a tool to identify, or categorize IP addresses based on the threats associated with them.
- Application Signature, database updates for Application Rules in WAF Policy.
- User Agent DB Sync, allows updates to the database used for BOT detection.
- Enable Pulse WAF Management, allows automatic updates to WAF signatures via Pulse Services.

Cloud Console

- Central Licensing, this enables zero-touch capacity management and cloud bursting (expand to the cloud for more capacity) for globally distributed NSX Advanced Load Balancer deployments.
- Proactive Support, enables a zero-touch support experience by monitoring NSX Advanced Load Balancer deployments and creating VMware support cases automatically upon detecting issues.
- Live Security Threat Intelligence, provides multiple live security feeds, for instance, WAF, BOT, IP Reputation, and so on to distributed, disparate environments to protect applications against threats that evolve in real-time.

While in some respects Cloud Console supplants the original Pulse Service, it is up to you as the customer to determine the solution for your environment.

After I upgrade to NSX Advanced Load Balancer version 21.1.3 or greater, will my Controller automatically upgrade to Cloud Console?

No, after upgrading to version 21.1.3 or later, the Controller will not automatically upgrade to Cloud Console. The Controller will remain licensed at Enterprise Tier and will require to be changed to Cloud Console tier after the software upgrade.

After upgrading to Cloud Console will I need to keep my old License files and information?

Changing to Cloud Console means that your licenses are managed centrally across the Internet. This implies that your old license files are no longer required. However, we recommend you retain these files and information as per your company's data retention policies.

I have SPP (Subscription Purchasing Program) Funds, can they be used to purchase NSX Advanced Load Balancer with Cloud Console Licenses?

Yes, SPP funds can be used to purchase NSX Advanced Load Balancer with Cloud Console Licenses. You can work with your account team to meet the following criteria:

- Have an account on VMware’s Cloud Console Portal.
- Have at least one Organization created within CSP.
- Designate the desired SPP Fund as the default SPP Fund.
- The CSP Organization into which the subscription is to be onboarded must have the required SPP fund configured as the default payment method.

My old licenses were based on Service Cores; what is the difference between a Service Core and a Service Unit?

The licensing unit is now called a Service unit. One Service unit is consumed for every vCPU that is deployed in the data plane, or one Service unit is consumed for every vCPU in a Service Engine.