VMware NSX Advanced Load Balancer Cloud Services

VMware NSX Advanced Load Balancer 21.1.3

vmware®

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

https://docs.vmware.com/

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

Contents

NSX Advanced Load Balancer Cloud Services Overview and Architecture

1

This guide provides an in-depth overview into NSX Advanced Load Balancer Cloud Services.

NSX Advanced Load Balancer with Cloud Services 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:

1. Software Control Plane (NSX Advanced Load Balancer Controller): Responsible for placement of the Service Engines, elasticity, scale, automation, analytics, resiliency and more.
2. 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.
3. Cloud Services (NSX Advanced Load Balancer Cloud Services): 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 Services Features

The following are the features of Cloud Services:

- 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 Services Service Description
- NSX Advanced Load Balancer Support Request Creation Guide

Getting Started

2

This section documents the prerequisites and high level steps to begin consuming NSX Advanced Load Balancer with Cloud Services.

This chapter includes the following topics:

This chapter includes the following topics:

- Prerequisites
- How to consume NSX Advanced Load Balancer with Cloud Services

Prerequisites

This section documents prerequisites to start consuming NSX Advanced Load Balancer with Cloud Services.

Prerequisites

The following are the prerequisites to register a NSX Advanced Load Balancer Controller with NSX Advanced Load Balancer Cloud Services.

1. NSX Advanced Load Balancer cluster deployment - You can download the Controller software by following this KB article.
2. Ability to register a NSX Advanced Load Balancer Controller with NSX Advanced Load Balancer Cloud Services. This capability is granted by any of:
   a. Having an active subscription for NSX Advanced Load Balancer with Cloud Services.
   b. Having an active trial for NSX Advanced Load Balancer with Cloud Services.
   c. Having an active NSX Advanced Load Balancer serial key license purchased before Dec 31 2021 - Refer to Legacy Addons for more details.

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

3 Connectivity between NSX Advanced Load Balancer Controllers and NSX Advanced Load Balancer Cloud Services portal.

Table 2-1. 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

Enhance Security by configuring a forward Proxy to access NSX Advanced Load Balancer Cloud Services

Customers can enable a Forward Proxy to proxy all traffic between the Controller and NSX Advanced Load Balancer Cloud Services. 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 Services traffic:

- No Proxy: All Cloud Services are directly accessed without any proxy from the Controller.
- System Proxy: All Cloud Services 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 Services 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 Services. 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:

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
```

How to consume NSX Advanced Load Balancer with Cloud Services

This section documents the high-level steps to begin consuming NSX Advanced Load Balancer with Cloud Services.

Purchase or Request for a Trial for NSX Advanced Load Balancer with Cloud Services

You can either purchase a NSX Advanced Load Balancer with Cloud Services subscription or request for a trial.

Purchase a NSX Advanced Load Balancer with Cloud Services Subscription

1. Customer purchases a NSX Advanced Load Balancer with Cloud Services subscription.
2. VMware sends an 'Onboarding' email to the customer with a pre-signed link to redeem the purchased subscription.
3. Customer 'onboards' the subscription by using the pre-signed link to map the purchased subscription to the CSP Organization of choice.
   a. Customer can forward the invite to another team member to complete onboarding.
   b. Customer can choose to create a new CSP Organization if required.
4. VMware deposits purchased capacity to be used in the mapped CSP Organization in the Central Licensing service provided by NSX Advanced Load Balancer Cloud Services.
5. VMware sends a subscription activation email to the customer stating, 'NSX Advanced Load Balancer with Cloud Services is now ready to use'.

Request for a NSX Advanced Load Balancer with Cloud Services Trial

1 Customer requests for a trial of NSX Advanced Load Balancer with Cloud Services 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 Services.

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

Setup a NSX Advanced Load Balancer Controller Deployment

You can either create a new or upgrade an existing deployment of NSX Advanced Load Balancer Controller to register with Cloud Services.

Note

- Minimum version requirement 21.1.3.
- Contact your VMware sales representative if an older software release is desired to be used.

Create a new NSX Advanced Load Balancer Controller Deployment

You can create a new NSX Advanced Load Balancer Controller deployment as follows:

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

   a Download software version 21.1.3 or later.

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

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

   a VMware NSX Advanced Load Balancer Controller in a vCenter environment with NSX-T

   b VMware NSX Advanced Load Balancer Controller in a vCenter environment without NSXT

   c VMware NSX Advanced Load Balancer Controller in Azure

   d VMware NSX Advanced Load Balancer Controller in AWS

e VMware NSX Advanced Load Balancer Controller in GCP

Note

1 Configure FQDNs for the NSX Advanced Load Balancer Controllers before registering with Cloud Services. 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 Services. For instance, you can edit `/etc/hosts` file on Mac OS.

Upgrade 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.

Register NSX Advanced Load Balancer Controller with Cloud Services

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

Registering NSX Advanced Load Balancer with Cloud Services

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

Ensure that the Controller is setup in the `ENTERPRISE_WITH_CLOUD_SERVICES` license tier and setup Central Licensing quotas and limits.

1 Launch the Controller UI.

2 Navigate to **Administration > Settings > 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

1 Starting with NSX Advanced Load Balancer version 21.1.3, a new Controller deployment will be setup in the `ENTERPRISE_WITH_CLOUD_SERVICES` license tier.

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

3 **Number of Reserved Licenses** allows you to partition your purchases subscriptions. This NSX Advanced Load Balancer deployment will always reserve the configured amount of capacity (assuming active subscription count is equal or greater than what is being reserved).

4 **Maximum Allowed Licenses** allows you to setup maximum consumption for this NSX Advanced Load Balancer deployment. This NSX Advanced Load Balancer deployment will never consume more capacity that what is set here.

Register NSX Advanced Load Balancer Controller with NSX Advanced Load Balancer Cloud Services as follows:

1 Launch NSX Advanced Load Balancer Controller UI.

2 Navigate to **Administration > Settings > 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**.

6 Enter **CustomerConnect** credentials to authenticate the Controller with NSX Advanced Load Balancer Cloud Services.

7 Once authenticated, choose the CSP Organization to associate this Controller with. This should be mapped to the CSP Organization which has an active NSX Advanced Load Balancer with Cloud Services subscription.

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

9 Optionally, enable other services delivered by NSX Advanced Load Balancer Cloud Services.

10 Click **SAVE** to complete registration.

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

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

1 Launch the NSX Advanced Load Balancer Cloud Services 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
configpb_attributes	
version	1

Note You can launch NSX Advanced Load Balancer Cloud Services 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 Services

Customers can deregister NSX Advanced Load Balancer Controller with Cloud Services. Once deregistered,

1 All Cloud services will be disconnected.

2 NSX Advanced Load Balancer Service Engines will become unlicensed.

3 However, existing Service Engines and virtual services will be unhampered and continue to function just as they were before opting out of this service.

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

Note Customers should only deregister a registered Controller in the following situations:

1 Changing CSP Organization mapping for the Controller, to change where capacity is consumed from.

2 Changing Licensing Tiers on the Controller.

Note Customers should not continue to run a NSX Advanced Load Balancer Controller in a deregistered state, when it is in the `ENTERPRISE_WITH_CLOUD_SERVICES` Licensing Tier.

Steps to de-register a NSX Advanced Load Balancer Controller from NSX Advanced Load Balancer Cloud Services:

1 Launch the NSX Advanced Load Balancer Controller UI.

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

3 Click **DEREGISTER CONTROLLER** .

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

Legacy Deployments

3

This section explains how NSX Advanced Load Balancer Cloud Services handles legacy deployments.

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

Services offered for 'Legacy Addon' Deployments

The following NSX Advanced Load Balancer Cloud Services 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 services are included only with the purchase of NSX Advanced Load Balancer with Cloud Services subscriptions.

Requirements to Register Legacy Deployments with Cloud Services

Requirements to register a NSX Advanced Load Balancer Controller deployment with NSX Advanced Load Balancer Cloud Services.

- 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 20.1.3.

Example: Scenarios to avail Cloud Services 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 Services 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 Services 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 Services '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 Services.

Registering Legacy Addons Deployments with NSX Advanced Load Balancer Cloud Services

The following are the steps to register the Controller to NSX Advanced Load Balancer Cloud services:

Ensure that NSX Advanced Load Balancer Controller is setup in the `ENTERPRISE` license tier.

1 Launch the NSX Advanced Load Balancer Controller UI.

2 Navigate to **Administration > Settings > Licensing**.

3 Click the gear icon and ensure that the `ENTERPRISE` tier is selected.

4 Click **SAVE**.

The following are the steps to register NSX Advanced Load Balancer Controller with NSX Advanced Load Balancer Cloud Services:

1 Launch the NSX Advanced Load Balancer Controller UI.

2 Navigate to **Administration > Settings > 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 Services Catalogue

4

This section will provide detailed documentation on each service offered by NSX Advanced Load Balancer Cloud Services.

This chapter includes the following topics:

Central Licensing

This section explains Central Licensing Service offered as part of NSX Advanced Load Balancer Cloud Services. 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 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.

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 a mandatory service and is enabled by default when the Controllers are setup in the `ENTERPRISE_WITH_CLOUD_SERVICES` tier. Refer to the Register NSX Advanced Load Balancer Controller with Cloud Services section.

Service Details

Central Licensing Service handles subscriptions purchased for NSX Advanced Load Balancer with Cloud Services. 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 SaaS subscription purchased, 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 this service is down,

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.

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 every 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. You need to opt-in to enable this service.

To opt-in to this service and enable automatic support case creation:

1 Navigate to **Administration > Settings > 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 opt-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 to Application Rules 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 challenging to maintain a real-time, up-to-date, consistent security posture and be protected from bad IPs. The 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 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 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.

To opt-in to this service and enable IP Reputation updates:

1 Navigate to **Administration > Settings > 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 IP Reputation 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 NSX Advanced Load Balancer Controllers support other IP Reputation database service providers in addition to **WebRoot**.

For more details on IP Reputation, see IP Reputation guide.

IP Reputation Sync Interval

The IP Reputation sync interval is the frequency at which the NSX Advanced Load BalancerControllers 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 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 Services portal. Registered NSX Advanced Load Balancer Controllers where this service is enabled, pull User-Agent database data from NSX Advanced Load Balancer Cloud Services portal. The Controllers then immediately update connected Service Engines as part of its configuration update process.

For more details on BOT management, see BOT Management guide.

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 they become 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.

To opt-in to this service and enable automatic support case creation:

1 Navigate to **Administration > Settings > 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 Services 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 is generated on the NSX Advanced Load Balancer Controller with a signed download link. You can click this link to download the WAF CRS Rules and upload it to the NSX Advanced Load Balancer Controller as follows:

1 Navigate to **Templates WAF > CRS**.

2 Click **Upload File** and 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 the service is down, new WAF CRS Signatures are not available. Load Balanced applications continue to utilize WAF CRS Rules available on the Controllers.

Proactive Support

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

Significant time and effort is involved in initiating and tracking support queries and finding resolutions to issues related to the product.

It also involves interaction with multiple entities such as the NSX Advanced Load Balancer to collect relevant 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 miscommunication of vital information.

Proactive support provides a hassle-free experience by providing support for end-to-end management of all support related tasks (as they related to the NSX Advanced Load Balancer), including automatically creating a case, uploading relevant information to the case in a timely manner, etc.. You can also use the NSX Advanced Load Balancer Controller to create a support case.

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, etc. to support cases from the 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 the VMware 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.

To opt-in to this service (enable the service)

1 Navigate to **Administration > Settings > 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 is viewed in the context of the Controller.

You can create a new case by navigating to **Administration > Support > Cases** and click **Create** button.

You can specify the following details:

- **Subject** - Specify the subject of the new case.
- **Contact** - Select the contacts from the drop-down list.
- **Customer Tag** - Specify the custom tag.
- **Type** - Select the case type from the drop-down menu. The options are as follows:
  - **Bug**
  - **Configuration Help**
  - **Feature Request**
  - **Issue**
  - **Question**
- **Severity Level** - Select the severity level from the drop-down menu.
- **Version** - Specify the version number.
- **Ecosystem** - Select the ecosystem details from the drop-down menu.
- **Description** - Specify the description of the case to be created.

You can view all active cases and all operations such as add comment, attachments, through the NSX Advanced Load Balancer.

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 to seamlessly attach relevant debug log information to their support cases, directly from their NSX Advanced Load Balancer Controllers.

Feature Highlights

- Generate and attach Tech Support to a new support case.
- Generate and attach Tech Support 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 the VMware 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. You need to opt-in to enable this service.

To opt-in to this service,

1 Navigate to **Administration > Settings > 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 > System > 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 will 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 through 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 customer connect support portal of VMware.

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.

To opt-in to this service and enable automatic support case creation:

1. Navigate to **Administration > Settings > 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.

Other Services

This section explains the other services provided by the Cloud services.

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 > Vantage**.

4 Pick the release of choice.

5 Download the appropriate package.

Note WAF CRS Rules are also available for downloads.