Technical Guide: **September 2023**

NSX Advanced Load Balancer

Hardening Guide

vmware®

Table of Contents

Purpose

VMWARE NSX Advanced Load Balancer is one of the critical components in network infrastructure. It provides enterprise-level load balancing including local and global load balancing, application acceleration, security, application visibility, performance monitoring, and container networking services.

Due to the crucial role that NSX ALB plays, it is imperative to configure the product components securely, to minimize the risk to the organization, it is necessary to configure the product components securely to reduce risk to the organization.

This document includes configuration settings and best practices in NSX ALB (Control and data plane) that will improve the overall security of the product. The purpose of this document is to provide System/Network administrator and security professionals with guidance on configuring NSX ALB from a security standpoint.

The document consists of recommendations and not mandates. This guide is specific to NSX Advanced Load Balancer version 22.1.x.

Out of scope

This section documents details related to topics not included or intended for the hardening guide.

- NSX ALB OS level hardening.
- This document is not meant to be used as a guide to meet the compliance needs of the customer.

Recommendation

Before implementing these configuration settings in your infrastructure, it's essential to conduct a comprehensive review.

Document Notation and Formatting

- Blue Boxes

Purpose: These boxes serve the purpose of providing specific configuration details related to the secure controls. These boxes offer concise and focused insights into how secure controls can be configured within the NSX ALB.

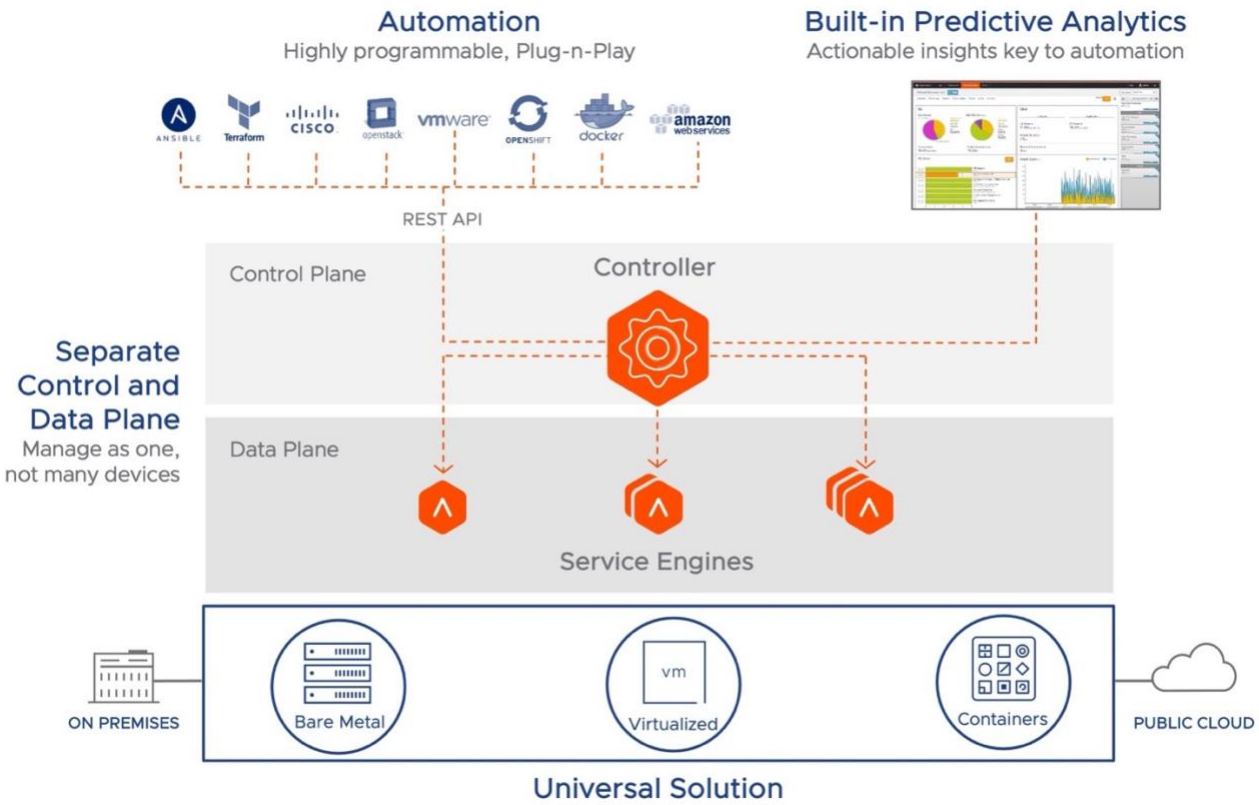
Usage: These boxes are placed under each secure control section.

NSX ALB Architecture

NSX Advanced Load Balancer is a software-defined Application Delivery Controller (ADC), providing local load balancing, global load balancing (GSLB (Global Server Load Balancing)), and application security features such as Web Application Firewall (WAF), Bot Detection and Management, and DDoS (Distributed denial of service) mitigation.

NSX Advanced Load Balancer can be deployed in various environments including private cloud (on-premises in vCenter, OpenStack SDDCs (Software-Defined Data Centers) or x86-based Linux servers), public clouds (Amazon Web Services, Microsoft Azure, Google Cloud Platform, and many others) as well as container platforms like Kubernetes/OpenShift.

The solution includes two major components – the Controller, which is the point of configuration and management, and the Service Engines, which provide the actual load-balancing capabilities. Architecturally, the solution provides separation between the management (control plane) and the end-user (data plane) traffic.



Modern Distributed Architecture – High Level View

NSX ALB Controller

The NSX ALB Controller is the single point of management and control that serves as the "brain" of the system. The Controller is a virtual appliance form factor (e.g.: OVA (Open Virtual Appliance) file for a vCenter-based deployment). Typically, three Controllers are deployed as a cluster for high availability and redundancy.

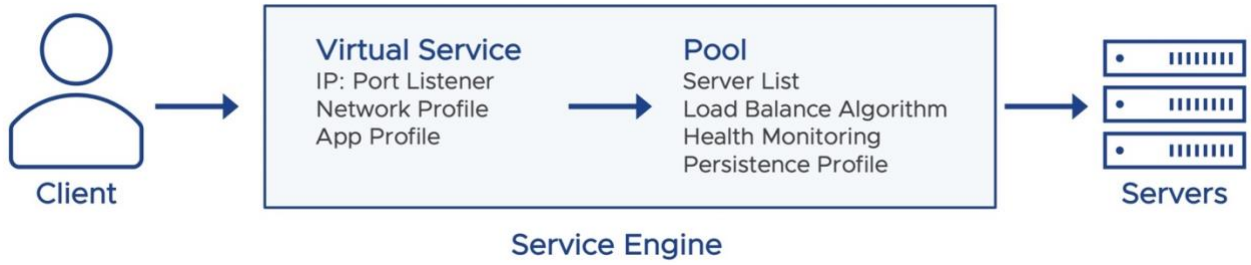
The Controller, based on configured options and requirements, deploys the data path engines (the Service Engines) and pushes the configuration to these Service Engines.

In cases where full automation and deployment of the Service Engines by the Controller is not needed, the Service Engines can be deployed manually (e.g.: deploying the Service Engine OVA for a vCenter Environment). In this scenario, the Service Engine connects to the Controller based on the configuration, and the Controller then pushes the configuration to the SEs (Service Engines).

Service Engines

NSX ALB Service Engines (SEs) handle all data plane operations within NSX ALB by receiving and executing instructions from the Controller. The SEs perform load balancing and all client- and server-facing network interactions. It collects real-time application telemetry from application traffic flows. High availability is supported.

In a typical load balancing scenario, a client will communicate with a virtual service, which is an IP address and port hosted in NSX ALB by an SE. The virtual service internally passes the connection through a number of profiles. For HTTP traffic, the SE may terminate and proxy the client TCP connection, terminate SSL/TLS, and proxy the HTTP request. Once the request is validated, it is forwarded internally to a pool, which will choose an available back-end server. A new TCP connection then originates from the SE, using an IP address of the SE on the internal network as the request's source IP address. Return traffic takes the same path back. The client communicates exclusively with the virtual service IP address, not the back-end server IP.



Best Practices and Guidelines for secure deployment

The Security Guidelines are divided into two categories:

1. Physical and Software Security

   This includes configuration guidelines and generic best practices for the physical environment where NSX ALB will be installed, as well as software-related recommendations for NSX ALB.

2. Network Security

   This includes configuration and generic best practices for both NSX ALB control and data plane network which are related to security settings of NSX ALB or Network Security Design.

Physical and Software Security

1. Deploy NSX ALB in a Secure Location

   NSX ALB must be installed on a hypervisor/hardware that provides sufficient access control to safeguard against tampering through unauthorized access.

   Configuration Details

   Not Applicable

   The secure control is applicable for private clouds and datacenter deployments for which customer has control and access.

2. Redundant Power Supplies

   The hardware on which NSX ALB is deployed should be installed with redundant power supplies to prevent any power outage resulting in loss of resiliency.

   Configuration Details

   Not Applicable

   The secure control is applicable for private clouds and datacenter for which customer has control and access.

3. Secure rack and stack

   The hardware where NSX ALB is deployed should be placed in a rack with a lock to prevent access to physical ports or getting access to the console etc.

   Configuration Details

   Not Applicable

   The secure control is applicable for private clouds and datacenter for which customer has control and access.

4. Private Key Protection

   If the requirement is to protect the private key for an application hosted on NSX ALB, it is recommended to use an external Hardware Security Module (HSM) that is compliant with FIPS (Federal Information Processing Standards) 140-2 Level 2.

   Configuration Details

   Thales Luna (formerly SafeNet Luna) HSM

5. Perform regular Software updates

   It is recommended that appliances be updated with a software version that includes bug fixes for enhanced security or functionality.

   Configuration Details

   Upgrade and Patches

Network Security

Generic recommendation

1. Do not expose the management interface to the internet.
   This is appliable in case NSX ALB is installed in DMZ/External Facing Zone.

   Access to NSX ALB management Interface is recommended to be through jump servers so that it is easy to lock down the subnet for management access.

   NSX ALB Configuration Details

   Not Applicable

2. Third party packages
   Installing any python or other third-party package for custom script is not supported as it can increase the attack surface of both the NSX ALB Control and data plane where packages are installed and hinder successful migration to newer NSX ALB versions.

   Configuration Details

   Not Applicable

3. Standard NSX ALB Object Naming
   Standard naming conventions for the NSX ALB objects such as virtual servers, monitor, profile etc. can include information such as datacenter, line of business names etc.

   This practice will improve inventory management, facilitate separation based on various criteria, and enable automation.

   For example, if there is a datacenter in Mumbai, which has a service engine hosting virtual service for Application team. Naming convention for virtual service objects inventory could be mum-01-app-<app name>-vs.

   Configuration Details

   Not Applicable

4. Segment Management and the data traffic
   It is recommended to have separation of the vNIC to physical NICs mapping. That is, the management and data vNICs should be mapped to different physical interfaces if possible. This is intended to provide better security and separation for different types of traffic.

   Configuration Details

   Not Applicable

GUI and SSH Interface secure configuration and best practices

By default, SE to Controller communication is secured with SSH and TLS. The initial connection from SE to the Controller using HTTP on Port 8443 involves authentication through TLS Mutual Authentication. Subsequent connections between the SE and the Controller occur through an authenticated SSH tunnel.

If a firewall is placed between the SE and Controller, it is recommended to define permissive rules for their IPs and include the necessary ports. For port details, see Appendix.

For more details related to the NSX ALB controller and SE Communication, see the Appendix.

1. Ensure that the GUI (Graphical User Interface) and API portal permit secure TLS protocols and ciphers
   It is recommended to allow TLS (Transport Layer Security) 1.3 and 1.2 protocols.

   The rationale behind configuring both TLS protocols resides in the potential existence of clients (mainly non-browser clients) that lack the support of TLS 1.3.

   In such cases, clients can downgrade to use TLS 1.2 ciphers and continue with connecting to the NSX API/GUI without any interruption.

   NOTE:

   - The Portal SSL profile not only applies to the GUI access but also impacts the access to API portal.
   - NSX ALB supports TLS1.0 and TLS 1.1 protocols and ciphers as well for cases where there is legacy client support required.

Configuration Details

System-Standard-Portal SSL profile is assigned by default for configuring the SSL ciphers and protocols.
Below commands are to configure a **custom ssl profile** based on the above recommendation:

Login to the AVI Shell | Create a new custom SSL profile

> configure sslprofile <name of the profile>
> type SSL_PROFILE_TYPE_SYSTEM
> accepted_versions
> accepted_versions index 1 type ssl_version_tls1_2
> save
> accepted_versions index 2 type ssl_version_tls1_3
> save
>accepted_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384
>ciphersuites TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256
> save

Continue in the AVI Shell | Assign above SSL Profile to the system configuration

> configure systemconfiguration
> portal_configuration
> sslprofile_ref <name of the SSL profile>
> save
> save

2. Use a custom internal/external signed Controller certificate
   It is recommended to replace the default certificates with Custom internal CA signed certs.

Configuration Details

Changing the Default Certificate of the Controller

3. Ensure idle timeout is configured
   It is recommended to configure the idle timeout for UI and API to 10 minutes or less.

   Prolonged or indefinite timeout increases the risk of attackers exploiting the session to take control.

   Configuration Details

   Login to NSX ALB Shell.
   > configure controller properties
   > api_idle_timeout 10
   > save

4. Login Banner for UI and SSH
   It is recommended to configure Login/MOTD for providing information to the internal users and warn the external/attacker of legal actions in case of unauthorized access.

   Configuration Details

   Login to NSX ALB Shell
   > configure systemconfiguration
   > linux_configuration
   > motd --
   Please input the value for field motd (Enter END to terminate input): Sample MOTD
   provide multiline
   END
   Overwriting the previously entered value for motd
   > save
   > linux_configuration
   > banner --
   Please input the value for field banner (Enter END to terminate input):
   <Provide the banner>
   <Here>
   END
   > save
   > save

5. Configure SSH with the SSH Encryption and MAC (Message Authentication Code) algorithm
   NSX ALB provides a way to configure SSH service to use desired set of encryption ciphers, KEX algorithms, and MAC algorithms to meet the security policy enforced in your environment.

   Below KB article provides ciphers and HMAC which are supported by NSX ALB.

It is recommended to choose the ciphers and HMAC for SSH configuration listed below:

SSH Ciphers

- chacha20-poly1305@openssh.com
- aes128-gcm@openssh.com and aes256-gcm@openssh.com
- aes128-ctr, aes192-ctr and aes256-ctr

HMACs

- Skip anything with MD5 and SHA1
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-256
- hmac-sha2-512
- umac-128@openssh.com

Configuration Details

https://avinetworks.com/docs/latest/securing-management-ip-access/#restricting-the-allowed-ciphers

https://avinetworks.com/docs/latest/securing-management-ip-access/#restricting-the-allowed-hmacs

6. SSH and GUI should be restricted to trusted IP address
An attacker who has gained access to a network, can gain illegal access to abuse the existing vulnerabilities.

Configuration Details

Login to NSX ALB Shell.

```
> configure systemconfiguration
> mgmt_ip_access_control
> ssh_access
> match_criteria is_in
> match_criteria is_in prefixes 10.2.5.6/24
> save
> save
> save
```

NOTE: In the existing setup with Controller and Service Engines, the SSH access list should contain an existing Controller and Service engine IPs.

Guidelines and Best Practices for Securing Client Traffic

1. Secure the load balancing persistence cookie
   It is recommended to encrypt the cookie which are inserted by NSX ALB in addition to using TLS/SSL encryption to prevent information disclosure about the remote host.

   Cookies set by NSX ALB are encrypted by default.

   Configuration Details

   NA

2. Session protection
   Session protection is enabled by default when NSX ALB is configured to proxy the connection and requires no further configuration. For example, in the case of System Proxy TCP Profile, NSX ALB creates a stateful connection.

   NSX ALB connection table contains details about the sessions that are currently setup. Sessions found in the connection table will be responded to by the NSX ALB, while packets that are not present will be discarded.

   Configuration Details

   NA

3. Enable HTTP Only
   It is recommended to insert HTTP only flag in a cookie set by NSX ALB. This indicates that cookie is non-scriptable, and any third-party applications /client script should not be able to access the cookies. This prevents cross site scripting/cookie theft.

   NOTE: In case there are applications with client-side scripts requiring access to the cookies, create a new custom HTTP Application profile for those applications. The HTTP only parameter will be deactivated by default.

   Configuration Details

   Login to the AVI Shell using CLI

   ```
   > configure applicationpersistenceprofile http-cookie
   > http_cookie_persistence_profile http_only
   > save
   > save
   ```

4. Secure Cookies
   Recommended to insert secure flag in a cookie since this option forces the browser to return the cookie's value when the connection is encrypted. This assists in preventing cookie theft through connection snooping.

   Configuration Details

   Login to the AVI Shell using CLI

   > configure applicationprofile <profile name>
   > type application_profile_type_http
   > http_profile
   > secure_cookie_enabled
   > save
   > save

5. Enable HSTS (HTTP Strict Transport Security)
   It is recommended to enable HSTS to protect the application/virtual server from various attacks like cookie hijacking, SSL (Secure Sockets Layer) stripping, and protocol downgrade.

   By adding the 'includeSubdomains' directive, the user agent is informed that the HSTS policy extends to both HSTS host and its subdomains. Before enabling this directive, ensure that all the subdomains are TLS enabled.

   Configuration Details

   Login to the AVI Shell using CLI

   > configure applicationprofile <profile name>
   > type application_profile_type_http
   > http_profile
   > hsts_enabled
   > hsts_max_age <number of days client should regard this virtual service as known hsts host.>
   > hsts_subdomains_enabled
   > save
   > save

6. End-to-End SSL
   It is recommended to have SSL on both the client and server side for the application in the DMZ/external facing perimeter zone.

   Configuration Details

   Overview of SSL/TLS termination

7. RSA and ECC certificates for System and Application Profile
   It is recommended to configure/deploy with RSA and ECC certificates simultaneously. This provides best of both worlds in terms of performance and compatibility.

   Configuration Details

   EC versus RSA Certificate Priority

8. Recommended Ciphers
   NSX ALB by default ships with cipher suites and protocols in form of SSL profiles which are performant and secure. Below are a few recommendations:
   - Use PFS enabled ciphers, that is, ECDHE_RSA, ECDHE_ECDSA, DHE_RSA, DHE_DSS ,and all TLS 1.3 ciphers.
   - The recommended Key Exchange algorithm preference should be in the following order:
   - DHE > ECDHE > RSA
   - Use AEAD Ciphers for providing strong authentication and key exchange with 128 bits of encryption like CHACHA20_POLY1305, GCM and CCM.
   - Use secure protocols. TLS 1.2 and TLS 1.3 should be enabled only unless there is a use case for legacy clients which require SSLv3 or TLS 1.0.

9. Use Web Application Firewall
   It is recommended to use web application firewall for an external facing web application in enforcement mode.

   Configuration Details

   WAF Support

User management and Access secure configuration

1. Change the default password
   It is recommended is to change the default password for the inbuilt accounts.

   Configuration Details

   By default, during the first login Controller will prompt to change the admin credentials.

   However, NSX ALB Controller does not have the option to set/change admin password during initial set up when deployed in AWS.

   You must log in using an SSH key and password configured during Controller creation in AWS.

   Configuration Details

   AWS Initial Password Change

2. Password Strength
   It is recommended to have a password policy as per the company policies for the local users if any.

   This is applicable for local users. External users will be governed by external AAA Server policies.

   Configuration Details

   Login to the NSX ALB Shell

   > configure systemconfiguration
   > portal_configuration
   > systemconfiguration:portal_configuration> password_strength_check
   > systemconfiguration:portal_configuration> minimum_password_length 10
   > systemconfiguration:portal_configuration> save
   > systemconfiguration > save

3. Use protocols like Radius, TACACS+. etc. for Authentication/Authorization
   It is recommended to use Centralized AAA (Authentication, Authorization and Accounting).

   Configuration Details

   TACACS+ Auth
   LDAP Auth

4. Use Multiple Authentication servers
   It is recommended to use multiple AAA remote servers since a single authentication server reduces the availability of NSX ALB for the Network admin and other admins performing their tasks.

   Configuration Details

   TACACS+ Auth
   LDAP Auth

5. Default Local admin accounts should be maintained
   If an attacked has gained access to a network, they can gain illegal access to abuse existing vulnerabilities.

   It is recommended to maintain your local accounts in a secure vault which stores the Local account password, provides access to the account only during break/fix issues and rotates the password regularly.

6. Deactivate Unused or Dormant Accounts
   It is recommended to deactivate or remove any dormant local accounts created on NSX ALB.

   This approach supports the principle of least privilege as a result reducing the attack surface of the NSX ALB.

   Configuration Details

   Login to NSX ALB Shell

   > delete user <local user name>

   NOTE: This is appliable only for local users created in NSX ALB.

1.

7. Use of Role based Access control (RBAC)
   It is recommended to use RBAC since RBAC provides separation of duties and least privileges.

   Configuration Details

   Extended Granular RBAC
   Granular Access Control per Fields
   User Role

8. Enforce to lockout accounts (Local or Remote user)
   It is recommended to prevent brute force attacks against NSX ALB Management Plane.

   Configuration Details

   This field Maximum login failure count can be set in user profiles and enforced by
   - Mapping user profile to remote Authentication profile.
   - Mapping to the user in case of Local user account.

   User Profile

9. External Users tenant Access
   It is recommended to configure the correct tenant in role mapping for external users and limit access to the required tenant only.

   Configuration Details

   Tenant Mapping

10. Super User Access
    Only Network Administrators or the group of users who will manage the operations of NSX ALB should be provided the Super user access.

    Configuration Details

    Super User Access

11. User Account for Cloud Connector Orchestration
    Use separate service accounts for NSX ALB integration with vcenter, NSX Manager and other ecosystems.

Configuration Details

NA

Monitoring and Auditing

1. SNMP access is allowed from certain trusted IPs.
   It is recommended to protect the SNMP service from unauthorized access.

Configuration Details

Login to the NSX ALB Shell
> configure systemconfiguration
> mgmt_ip_access_control
> snmp_access
#Depending on the requirement IP address, prefixes or IP address group can be refrenced.
> prefixes 10.2.4.0/23
> match_criteria is_in
> save
> save
> save

2. Use SNMP v3 wherever possible.
   It is recommended to use SNMPv3, prior/v1-2 protocol lacked authentication and encryption.

Configuration Details

SNMP Support

3. Remote syslog servers
   System event logs should be sent to the remote syslog server with details related to the transaction.

Configuration Details

Syslog Notifications

4. Use syslog over TLS
   It is recommended to syslog over TLS in case there is a sensitive data transferred in the logs.

   Configuration Details

   Syslog over TLS

5. Redundant syslog servers
   It is recommended to use multiple syslog servers to have a high availability to capture Client logs which would be ingested by different teams.

   Configuration Details

   Configure Syslog Server

System Related Secure Configuration and Best Practices

1. Configure NTP (Network Time Protocol)
   It is recommended to configure NTP on the NSX ALB Controller. The analytics functionality in the Controller relies on the fact that the Controller(s) in the cluster and SE(s) are synchronized.

   Configuration Details

   NTP/DNS Settings

2. Automated Backup to remote locations
   It is recommended to configure backup to a remote SCP/FTP server to restore the NSX ALB fabric i.e., Controllers and Service Engines in case of failure.

   You can find the details related to NSX ALB encrypting the data at rest in the backup file. Sensitive fields that are encrypted contain password-like user account(local), cloud connector credentials, private key, user-defined variables which are configured as “Sensitive”.

   - The admin-provided passphrase given during the NSX ALB Controller setup is used to derive a Key.
   - PBKDF2 (Password-Based Key Derivation Function 2) is used to generate a cryptographic key from the admin-provided passphrase, salt (fixed-length cryptographically strong random value), iteration, and more. as input.
   - The key derived from the previous step will be used to encrypt the sensitive fields in the backup configuration.
   - NSX ALB uses AES-256-CBC for encrypting sensitive data at rest. The encryption algorithm takes the derived key and applies it to the sensitive fields in backup configuration.
   - Salt, Derived key etc will be stored in database securely in the NSX ALB Controller.

   In this way, even if an attacker gains unauthorised access to the backup configuration of NSX ALB, they will not be able to retrieve the passphrase itself.

NOTE: Configuring complex and random admin- provided passphrase determines the strength of the encryption of the sensitive fields in the backup.

Configuration Details

Backup and restore NSX ALB Configuration

VMware Ecosystem Specific Controls

1. Updating Security Patches
   It is recommended that appliances are updated with a firmware version which has bug fixes for high security or functionality. This also applies for the Hardware host on which NSX ALB is hosted. A vulnerable host can lead to comprise of VNF hosted on it.
2. Limit console and Hypervisor Access
   The virtualization team should only grant network administrators who are responsible for managing NSX ALB components (Controller and SE) access to the virtual console in vCenter.
3. vCenter specific folder access only
   To have better security, NSX ALB components should be kept in separate folders in vCenter and access to that specific folder should be configured. This keeps in least privilege security best practice.

Compliance Modes and Settings

These are the modes in which NSX ALB Controller and Service Engine add/remove some settings to meet the compliance set by an authority like CIS.

NOTE:

- Enabling compliance modes introduces caveats and functionality limitations for the product.
- Review the limitations prior to enabling these compliance modes. Otherwise, it can lead to unexpected results during regular operation or upgrade processes.
- Compliance modes should only be enabled when there is a strict requirement to do so.

1. CIS Mode

   Center for internet security (CIS) provides general and specific standards for all to implement the best practices. These are best practices to mitigate the most prevalent cyber-attacks against systems and networks.

   - NSX ALB is complaint with CIS benchmarks by default with a few exceptions which are documented in this KB article.
   - The primary use case for the CIS mode is in scenarios where customers need to independently perform the CIS benchmark test.
   - Enabling the CIS mode in NSX ALB Controller enables the AUDITD service/process on both the controller and SE, which allows the CIS benchmark test to succeed.

- These are the other settings which are added when CIS mode is enabled.
  - The Iptables enabled on the Controller and Service Engine. These iptables are configured as the CIS guidelines for the Firewall configuration for “Independent Linux Benchmark”.
  - Ldaps_utils package is removed.

Configuration Details

CIS Compliance for NSX ALB

2. FIPS Mode

FIPS federal information Processing Standard/FIPS 140-2 is a set of guidelines created by NIST to validate and document cryptographic standards.

NSX ALB uses specific cipher and crypto modules which are FIPS compliant when the FIPS mode is enabled.

There are four levels of security in the FIPS 140-2 standard, and for each level there are different areas related to the design and implementation of a tool’s cryptographic design.

NSX ALB crypto stack is compiled with VMware distributed VMware FIPS module version 2.0.20 which is FIPS Level 1 certified.

NSX ALB supports FIPS Level 1 and supports it for both Controller and Service Engine.

Pre-Checks before enabling FIPS

- Certain features are not available in FIPS complaint mode, please review them. Details in the KB link.
- Caveats during the upgrade, disabling the FIPS mode etc. should be reviewed before enabling the mode.
- Only a few ecosystems support FIPS complaint mode, review before implementing.
- TLS1.3 is not supported when FIPS mode is enabled.

NOTE:

- While some of the FIPS approved configurations are checked during configuration , it is possible to come up with configurations that can put NSX ALB outside of the FIPS approved mode.
- FIPS security level 2-4 speak of the standards and requirements for physical security like tamper resistance etc. Hence, these security levels do not apply to software solutions like NSX ALB.

Configuration Details

FIPS Compliance

NSX ALB Security Advisory

https://www.vmware.com/security/advisories.html

References

Port Details for NSX ALB communication	Port Details
NSX ALB Controller to Se communication	SE-Controller Communication
Adding Required HMAC to the Allowed HMACs Lists	HMAC details
Login Banner and MOTD	Banner and MOTD
Securing Management IP access	Secure Mgmt Access
Access CLI as non-Admin user	SSH Access
Configure Strong TLS Cipher	Cipher

Copyright © 2023 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001
VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at vmware.com/go/patents.
Item No: vmw-wp-tech-temp-uslet-word-2023 1/23