VMware NSX Advanced Load Balancer: Web Application Firewall Security Training

Course Duration: 3 Days/21 Hours per day

Course Overview

This three-day course provides comprehensive training on how to configure, maintain and troubleshoot the Web Application Firewall component of the VMware NSX Advanced Load Balancer (Avi Networks) solution as well as provide an understanding of additional security related functionality. This course covers key NSX Advanced Load Balancer (Avi Networks) Web Application Firewall features and functionality offered in the NSX Advanced Load Balancer 18.2 release, including the overall infrastructure, virtual services and application components as well as application troubleshooting and solution monitoring. Access to a software-defined data center environment is provided through hands-on labs to reinforce the skills and concepts presented in the course.

Objectives

- Describe NSX Advanced Load Balancer architecture
- Describe the NSX Advanced Load Balancer components and main functions
- Explain the NSX Advanced Load Balancer key features and benefits
- Describe NSX Advanced Load Balancer Web Application Firewall architecture
- Describe the NSX Advanced Load Balancer Web Application Firewall components and main functions
- Explain the NSX Advanced Load Balancer Web Application Firewall key features and benefits
- Explain and configure Local Load Balancing constructors such as Virtual Services, Pools, Health Monitors and related components
- Understand and modify application behavior leveraging Profiles, Policies and DataScripts
- Configure and customize the NSX Advanced Load Balancer Web Application Firewall

- Describe and leverage NSX Advanced Load Balancer REST API interfaces and related automation capabilities

- Describe and configure NSX Advanced Load Balancer Web Application Firewall application and infrastructure monitoring

- Gather relevant information and perform basic troubleshooting of Web Application Firewall applications leveraging built-in NSX Advanced Load Balancer tooling

Outline

1 Course Introduction

- Introductions and course logistics

- Course objectives

2 Introduction to NSX Advanced Load Balancer

- Introduce NSX Advanced Load Balancer

- Discuss NSX Advanced Load Balancer use cases and benefits

- Explain NSX Advanced Load Balancer architecture and components

- Explain the management, control, data, and consumption planes and their respective functions

3 Introduction to NSX ALB Web Application Firewall

- Introduce the NSX Advanced Load Balancer Web Application Firewall

- Discuss NSX Advanced Load Balancer Web Application Firewall use cases and benefits

4 Virtual Services Configuration Concepts

- Explain Virtual Service components

- Explain Virtual Service types

- Explain and configure basic virtual services components such as Application Profiles, Network Profiles,

Pools and Health Monitors

5 Attacking and Defending Web Applications

- Introduce the processes and methodologies used when attacking and defending web applications

- Introduce the tools used to attack web applications

- Explain with examples terminology such as Reflected XSS and SQL injection

6 Profiles and Policies

- Explain and deep dive on Advanced Virtual Service creation

- Explain and deep dive on Application Profiles and Types such as L4, DNS, Syslog and HTTP

- Explain and configure advanced application HTTP Profile options

- Deep dive on Network Profiles and Types

- Explain and configure SSL Profiles and Certificates

- Explain and Configure HTTP and DNS policies

7 DDOS Protection

- Introduce the NSX Advanced Load Balancer rate limiting functionality

- Explain the NSX Advanced Load Balancer rate limiting functionality

- Hands on examples of rate limiting in action

8 Customizing Application Delivery with Datascripts

- Introduce the concept of datascripts to manipulate data
- Explain the various components and inspection points

9 IWAF Deep Dive

- Describe the building blocks of the iWAF implementation
- Explain the various iWAF components
- Introduce both Positive and Negative security models
- Explain the iWAF Policies, profiles and rule sets

10 IWAF Core Rule Set

- Explain the history and rationale of the core rule set
- Describe the NSX ALB (Avi) Core Rule Set

11 IWAF Custom Rules

- Describe the power and complexity available via custom rules
- Explain the rule language
- Implement various use cases
- Explain common errors and possible solutions

12 IWAF Operations

- Describe the iWAF application onboarding process
- Tuning the iWAF policies
- Working with iWAF logs and analytics
- Explaining false positive mitigation tactics

13 IWAF Best Practices

- Provide guidance on how to get the best results