



VMware NSX Advanced Load Balancer: Web Application Firewall Security

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.

Course Contents

- Course Introduction
- Introduction to NSX Advanced Load Balancer
- Introduction to NSX ALB Web Application Firewall
- Virtual Services Configuration Concepts
- Attacking and Defending Web Applications
- Profiles and Policies
- DDOS Protection
- Customizing Application Delivery with Datascripts
- IWAF Deep Dive
- IWAF Core Rule Set
- IWAF Custom Rules
- IWAF Operations
- IWAF Best Practices

E-Book You will receive the documentation of VMware in English language as an e-book.

Target Group

Experienced system administrators or network administrators and security professionals

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:
www.experteach-training.com/go/VLWF

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	3 Days	€ 2,250
Online Training	3 Days	€ 2,250
Dates upon request		

Status 03/08/2024



Table of Contents

VMware NSX Advanced Load Balancer: Web Application Firewall Security

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

