(CNS-301) Citrix NetScaler 11 Advance Implementation

Overview

Designed for students with previous NetScaler experience, this course is best suited for individuals who will be deploying or managing advanced NetScaler environments.

Learn the skills required to configure and manage advanced NetScaler features through hands-on lab exercises. Students will learn how to implement advanced NetScaler components including Application Firewall, Advanced Traffic Management features including Http Callouts, and Troubleshooting. At the end of the course students will be able to configure their NetScaler environments to address advanced traffic delivery and management requirements including application security, optimization, and NetScaler operation management.

Recommended pre-requisite courses:

- CNS-205 Citrix NetScaler 11.0 Essentials and Networking

Note: This course is based on the Citrix NetScaler 11 product, but the skills and fundamental concepts learned are common to earlier product versions.

Key Skills

- Upon successful completion of this course, students will be able to:
- Identify common web attacks and vulnerabilities
- Write PERL compatible regular expressions
- Configure Citrix Application Firewall to protect web applications
- Troubleshoot Citrix Application Firewall
- Install and configure NetScaler Insight Center to monitor performance
- Install, configure, and use Citrix Command Center to manage NetScaler devices
- Configure and use additional advanced features of NetScaler including NetScaler Web Logging, HTTP callout, and AAA authentication for web applications

Audience

Students interested in learning how to implement and manage the advanced NetScaler features using leading practices. Specifically:

- Administrators
- Implementers / Engineers
- Architects

Instructional Method

This course is offered in instructor-led training (ILT)/virtual instructor-led training (vILT) formats with application of concepts through hands-on exercises in a live lab environment.

Course Length

5 days

Course Materials

As part of this course, students will receive the following materials:

- Access to a lab environment for the duration of the course
- Lab exercise guide
- Access to final course deliverables once the course is available in general availability including copies of all official materials presented by the instructor with additional notes and references as well as videos with experts throughout Citrix around course topics and lab exercises.

Preparatory Recommendations

Citrix recommends students prepare for this course by taking the following course:

- [CNS-205 Citrix NetScaler Essentials and Networking](#)

It is also recommended to gain a basic understanding of the following concepts and technologies:

- Experience configuring NetScaler systems, including an understanding of services, virtual servers, and policies
- Experience with network devices, such as routers and switches, various networking protocols, and aspects of application and site architectures (such as DMZs and VLANs)
- Knowledge of network security threats and site protection concepts such as firewalls, worms, and DDoS attacks
- Understanding of concepts related to monitoring and management including basics of SNMP

Certification Preparation

In addition to field experience, this course helps prepares candidates for the 1Y0-351: Citrix NetScaler 10.5 Essentials for Networking exam. By passing the 1Y0-351: Citrix NetScaler 10.5 Essentials for Networking exam, candidates will gain the Citrix Certified Professional – Networking (CCP-N) certification.

Topic Outline

- Getting Started
    - Introduction to the NetScaler System
- Advanced Troubleshooting
    - Troubleshooting Resources
    - NetScaler System Overview
    - nCore Configuration Architecture

- Form Field Consistency Protection
- Forceful Browsing
- Start URLs
- Backdoors and Misconfigurations
- URL Closure
- Identity Theft Attacks
- Credit Card Protection
- Protecting Credit Cards
- Errors Triggering Sensitive Information Leaks
- Safe Object Protection
- Application Firewall Troubleshooting
  - Application Firewall and
  - Configuration Issues
- Queuing and Connection Tuning
  - HTTP Connections
  - HTTP Connection Management and NetScaler
  - HTTP Behavior
  - TCP Buffering
  - Surge Queue
  - Surge Protection
  - Priority Queuing
  - HTTP Denial-of-Service Protection
- Authentication, Authorization, and Auditing
  - Users, Groups and Command Policies
  - External Authentication for System Users
  - AAA for Traffic Management
  - Configuration
  - Audit Logging
- AppExpert Rate Limiting, HTTP Service Callout, and Policy-based Logging
  - HTTP Callouts
  - Configuring HTTP Callouts
  - HTTP Callout Use Cases
  - Configuring Rate Control
  - Rate Control Policy Scenarios
  - Policy-based Logging
- Command Center
  - Command Center Introduction
  - Command Center Clients

- Server Requirements
- Port Setting Requirements
- Command Center Installation
- Command Center Functionality
- Command Center Administration
- Insight Center
  - Insight Center Overview
  - AppFlow on the NetScaler System
  - How Insight Center Collects AppFlow Data
  - HDX Insight
  - HTML Injection
- NetScaler Web Logging
  - NetScaler Web Logging Introduction
  - NetScaler System Configuration
  - NSWL Client Installation
  - NSWL Client Configuration
  - Troubleshooting Web Logging