

## CNS-300-2I Advanced Administration for Citrix<sup>®</sup> NetScaler<sup>™</sup> 9.0 Platinum Edition

This course provides the foundation to manage, configure and monitor advanced features and components of Citrix NetScaler 9.0 Platinum Edition. Interactive discussion and hands-on labs guide learners through advanced administration tasks such as troubleshooting, configuring application security with the Citrix Application Firewall<sup>™</sup> feature, tuning the NetScaler for high traffic, configuring Authentication Authorization and Accounting for system management, and configuring Advanced Policies using service callouts. Advanced monitoring and management tasks such as configuring and using EdgeSight<sup>™</sup> for NetScaler, Command Center, and NetScaler Web Logging are also covered. Prior NetScaler knowledge is strongly recommended.

### Audience

This course is intended for system administrators or network operations personnel, who configure and administer Citrix NetScaler products.

### Preparatory Recommendations

Before taking this course, Citrix recommends that learners have the following knowledge and experience:

- Experience with 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
- Attended one of the following courses
  - CNS-200-11 - Basic Administration for Citrix NetScaler 9.0
  - NS-BOA Citrix NetScaler Basic Operations and Administration
  - CTX-1730 Citrix NetScaler: Basic Operations, and CTX-1731 Citrix NetScaler: Administration
  - Or, equivalent experience with Citrix NetScaler version 6.1, 7.0, 8.0, 8.1 or 9.0

### Key Skills

Upon successful completion of this course, learners are able to complete the following:

- Identify common web attacks and vulnerabilities
- Write PERL compatible regular expressions
- Configure Citrix Application Firewall<sup>™</sup> 9.0 to protect web applications
- Troubleshoot Citrix Application Firewall 9.0
- Install and configure Citrix EdgeSight for NetScaler to monitor web application performance
- Install, configure, and use Citrix Command Center to manage NetScaler devices
- Configure and use additional advanced features of NetScaler 9.0 including NetScaler Web Logging, HTTP Callout, and AAA authentication for web applications

### Instructional Method

This course is an instructor-led training course with classroom discussion, demonstrations and the practical application of concepts through hands-on exercises.

### Course Length

5 days

### Certification Preparation

This course is not associated with any current Citrix certification program.

## Registration

For more information and to register for this course, please go to [www.citrixeducation.com](http://www.citrixeducation.com).

## Topic Outline

Provided is the topic outline for CNS-300-2I:

- Advanced Troubleshooting
  - Troubleshooting Resources
    - Citrix Knowledge Center
    - Citrix Product Documentation
    - Citrix Technical Support
    - Collected NetScaler Data
    - Troubleshooting Log
  - NetScaler System Overview
    - NetScaler Processes
  - nCore Configuration Architecture
  - Built-In Tools
    - Nsconmsg
    - Network Traffic Capture
    - show and stat Commands
    - Reporting Tool
    - Shell Tools
    - Command-Line Interface Tools
    - Configuration Utility Tools
  - Third-Party Tools
    - Network Protocol Analyzers
    - Web Browser Plug-ins
    - SNMP Browsers
    - FTP Clients
- Introducing Application Firewall
  - Application Attacks
    - Application Attack Description
    - Goals of Application Attacks
    - Most Common Types of Web Application Attacks
    - The Application Firewall Solution
    - Business Problems
  - The Benefits of Application Firewall
    - Application Layer Protection
    - Positive Security Model
    - Negative Security Model
    - Deep Stream Inspection
    - Adaptive Learning Engine
    - Web Application Vulnerabilities
    - Security Audits and Application Firewalls
  - Payment Card Industry Data Security Standard
    - Importance of PCI
    - Common Coding Vulnerabilities
    - PCI-DSS Report
    - Packet Processing and Inspection
    - Request Process
    - Response Process
    - Deployment Considerations
  - Profiles and Policies
    - Profiles
    - Policies
- Profiles and Policies
  - Profiles
    - Profile Types
    - Default Profiles
    - Creating a Profile in the Configuration Utility

- Creating a Profile in the Command-Line Interface
    - Action Settings
    - Sessionization and Security Checks
    - Profile Settings
    - Error Page
    - HTML Comment Stripping
    - XML Error Object
    - Other Profile Settings
  - Policies
    - Policy Creation
    - Policy Binding
    - Policy State
    - Policy Priorities
    - Creating a Policy in the Configuration Utility
    - Creating Policies in the Command-Line Interface
    - Binding and Prioritizing a Policy in the Configuration Utility
    - Binding Policies in the Command-Line Interface
  - Engine Settings
- Regular Expressions
  - Regular Expressions
  - Forms of Regular Expressions
  - Using Regular Expressions
  - Metacharacters and Literal Characters
  - Metacharacters
  - Escapes
  - Quantifiers
  - Backreferencing
  - Lookaheads
  - Regular Expression Scope
- Attacks and Protections
  - Security Checks
    - Profile Types
    - Common Security Checks
    - HTML Security Checks
    - XML Security Checks
    - Request-Side and Response-Side Checks
  - HTTPS Web Applications
  - Buffer Overflow Exploits
    - Goals of a Buffer Overflow Attack
    - Consequences of a Buffer Overflow Attack
  - Buffer Overflow Protection
    - Default Maximum Values
    - Modifying Buffer Overflow Settings
  - Parameter Manipulation
    - Parameter Manipulation Example
  - Server Misconfiguration
  - Deny URL Protection
    - The Deny URL List
    - Adding a Deny URL in the Command-Line Interface
    - Deleting a Deny URL in the Command-Line Interface
  - SQL Injection
    - How SQL Injection Works
  - HTML SQL Injection Protection
    - SQL Keywords and Special Characters
    - Modifying SQL Injection Action Settings
    - XML SQL Injection Security Check
    - Cross-Site Scripting
    - Attacking the Trust Relationship
    - How Cross-Site Scripting Attacks Work

- Results of a Cross-Site Scripting Attack
  - Preventing Cross-Site Scripting Attacks
  - HTML Cross-Site Scripting Protection
  - Cross-Site Scripting Action Settings
  - Transform Cross-Site Scripts
  - Check Complete URLs for Cross-Site Scripting
  - Additional Action Settings
  - Relaxations
  - Modifying Cross-Site Scripting Action Settings
  - Adding a Cross-Site Scripting Relaxation Using the Command-Line Interface
  - Deleting a Cross-Site Scripting Relaxation Using the Command-Line Interface
  - XML Cross-Site Scripting Security Check
- Command Injection
  - Command Injection Examples
- Field Format Protection
  - Field Types and Field Formats
  - Predefined Field Types
  - Custom Field Types
  - Field Format Configuration
  - Default Field Format
  - Confidential Fields
  - Adding a Custom Field Type
  - Setting a Default Field Type
  - Modifying Field Format Settings
  - Adding a Confidential Field
  - Modifying a Confidential Field
- Cookie Tampering and Poisoning
  - Types of Cookies
  - How Cookies Are Added
  - Web Server Sessions
- Cookie Consistency Protection
  - Sessionization and Cookies
  - Relaxations
  - Adding a Cookie Consistency Relaxation in the Command-Line Interface
  - Deleting a Cookie Relaxation in the Command-Line Interface
- Form/Hidden Field Manipulation
  - Example of Hidden Field Manipulation
- Form Field Consistency Protection
  - Field Consistencies
  - User Sessions
  - Adding a Form Field Consistency Relaxation Using the Command-Line Interface
  - Deleting a Form Field Consistency Relaxation Using the Command-Line Interface
- Forceful Browsing
  - Forceful Browsing Protection
- Start URLs
  - The Start URL List
  - Sessionization and Start URLs
  - Modify Start URL Check
  - Adding a Start URL in the Command-Line Interface
  - Deleting a Start URL in the Command-Line Interface
- Backdoors and Misconfigurations
- URL Closure
  - Enforcing URL Closure in the Configuration Utility
  - Enforcing URL Closure in the Command-Line Interface
- Identity Theft Attacks
  - Types of Identity Theft Attacks
  - Application Firewall Protection Against Identity Theft
- Credit Card Protection
  - Predefined Credit Cards

- Credit Card Settings
  - Protecting Credit Cards
    - Protecting Credit Cards in the Configuration Utility
    - Protecting Credit Cards in the Command-Line Interface
  - Errors Triggering Sensitive Information Leaks
  - Safe Object Protection
    - Defining a Safe Object
    - Adding a Safe Object
    - Adaptive Learning for Security
    - Learning Over Time
    - Learning Thresholds
    - Generalized and Simple Rules
    - Learned Rules
    - Enabling Learning
    - Setting Learning Thresholds
    - Managing Learned Rules
- Application Firewall Troubleshooting
  - Application Firewall and Applications
    - HTTP Headers
    - HTML Comment Stripping
  - Configuration Issues
    - Policy Issues
    - Profile Issues
    - Suggested Actions
- Queuing and Connection Tuning
  - HTTP Connections
    - Keep-alive HTTP Connections
    - HTTP 1.0 and 1.1 Behavior
    - Pipelined Requests
  - HTTP Connection Management and NetScaler HTTP Behavior
    - Client Keep-Alive
    - Connection IP Address Control
    - Maximum Requests and Maximum Connections
    - Connection Idle Settings
    - Trackable Connections
  - TCP Buffering
    - Down-State Flush and Access Down Connection Settings
    - TCP Optimization
    - Advertised Window Size
    - Window Scaling
    - Selective Acknowledgement
  - Surge Queue
  - Surge Protection
    - Request and Response Rates
    - Throttle Rate
    - Disabling Surge Protection in the Configuration Utility
    - Disabling Surge Protection for a Service in the Configuration Utility
    - Setting Thresholds in the Configuration Utility
  - Priority Queuing
    - Enabling Priority Queuing in the Configuration Utility
    - Creating a Priority Queuing Policy in the Configuration Utility
    - Binding Priority Queuing Policies in the Configuration Utility
    - Weighted Queuing
  - HTTP Denial-of-Service Protection
    - Enabling HTTP DoS Protection in the Configuration Utility
    - Adding a HTTP DoS Policy in the Configuration Utility
    - Challenged JavaScript Responses
    - Client Detection Tuning and JavaScript Challenge Response Rate
    - HTTP DoS Protection Deployment Guidelines

- Attack Characteristics
  - IP Rate Limiting
    - Rate Control by Subnet Example
    - IP Rate Limiting Best Practices
- Authentication, Authorization, and Auditing
  - Users, Groups and Command Policies
    - Authentication, Authorization, and Auditing
    - Systems and AAA Users Groups
    - Local Accounts
    - External Authentication
  - External Authentication for System Users
    - Authentication Actions and Policies
    - Configuring Local Authentication
    - Configuring External Authentication with Explicit Accounts
    - Configuring External Authentication with Group Extraction
    - Creating an External Authentication Policy
    - Creating local groups in the Command-Line Interface
    - Binding Groups in the Command-Line Interface
    - Creating an LDAP Authentication Action in the Command-Line Interface
    - Creating an Authentication Policy in the Command-Line Interface
    - Binding the Policy in the Command Line Interface
    - Authentication Troubleshooting
    - External Authentication Common Issues
  - AAA for Traffic Management
    - Enabling AAA for Traffic Management
    - AAA for Application Traffic
    - Basic AAA Setup for Application Traffic
    - Workflow for AAA Traffic Management
  - Configuration
    - Creating an Authentication Virtual Server
    - Creating an Authentication Virtual Server in the Command-Line Interface
    - Binding an SSL Certificate in the Command-Line Interface
    - Binding a Virtual Server to an Authentication Policy in the Command-Line Interface
    - Configuring a Virtual Server to use an Authentication Virtual Server in the Command-Line Interface
    - Configuring Authorization Policies for Traffic Management
    - Setting the Default Traffic Management Authentication Action to Deny in the Command-Line Interface
    - Creating an Authorization Policy to Allow Access
  - Audit Logging
    - Audit Logging Troubleshooting
- HTTP Service Callouts
  - HTTP Callouts
  - Configuring HTTP Callouts
    - Configuring HTTP Callouts in the Configuration Utility
    - Configuring HTTP Callouts in the Command-Line Interface
    - Callout Examples
    - HTTP Callout Response Parsing
  - HTTP Callout Use Cases
    - Scenario 1: Filter Clients Based on an IP Address Blacklist
    - Scenario 2: Fetch and Update Content
    - HTTP Callout Auditing
- EdgeSight for NetScaler
  - Data Flow Overview
  - JavaScript Response Injection
    - User Metrics
    - NetScaler Metrics
    - NetScaler Metric Example

- Data Validity
  - EdgeSight for NetScaler Server Components
    - Component Installation Scenarios
  - EdgeSight for NetScaler Installation Considerations
    - Installing EdgeSight for Netscaler
    - SQL Server
    - SQL Reporting Services
    - EdgeSight for NetScaler Components
    - Installing EdgeSight Database Components
    - Installing EdgeSight Report Console and Data Collector Components
    - EdgeSight Post-Installation Wizard
    - Upgrading EdgeSight for NetScaler
  - Reporting Services Initial Configuration
    - NetScaler Configuration Overview
    - Configuring HTML Injection
    - Editing the prebody.js script
    - Configuration Example in the Command-Line Interface
    - Add NetScaler System to EdgeSight for NetScaler Data Collector
    - Topology Data Collectors with SSL
  - EdgeSight Charts and Reports
  - EdgeSight Troubleshooting
    - Troubleshooting OS Components
    - Troubleshooting HTML Injection
    - Troubleshooting Injection Request
    - Troubleshooting Unknown Device
    - Troubleshooting from the NetScaler Command-Line Interface
- Command Center
  - Command Center Introduction
    - Command Center NetScaler Features
    - NetScaler and WANScaler Support
  - Command Center Clients
    - Connecting to Command Center
  - Server Requirements
    - Disk Space Requirements
    - MySQL Considerations
    - Microsoft SQL Server 2005 Considerations
  - Port Setting Requirements
    - Command Center Installation
    - Linux Considerations
    - Installation
    - Capacity Planning
    - Backup
    - Installation Modes
    - Installation Considerations
  - Command Center Functionality
    - Command Center Home Page
    - Discovery
    - Fault Management
    - Configuration Management
    - Change Management
    - Centralized Certificate Management
    - Performance Monitoring
  - Command Center Administration
    - Security Administration
    - Administration Operations
    - Administration Configuration
    - Server Details
  - Command Center Troubleshooting
    - Microsoft SQL Database Issues
    - Discovery Issues

- Performance Data Issues
  - Linux Command-Line Interface Access Issues
  - Reporting Issues
- NetScaler Web Logging
  - NetScaler Web Logging Introduction
    - Architecture Overview
    - Communication Process
  - NetScaler System Configuration
    - Enabling Web Logging in the Configuration Utility
    - Enabling Web Logging in the Command-Line Interface
    - Configuring the Buffer Size in the Configuration Utility
    - Configuring the Buffer Size in the Command-Line Interface
  - NSWL Client Installation
    - Logging System Components
    - Installing the NSWL Client on Windows
    - NSWL Options
    - Windows Service Registry Key
  - NSWL Client Configuration
    - NetScaler IP Addresses
    - Log Filters
    - Defining Log Properties
    - Running NSWL
    - Verifying the Configuration
  - Troubleshooting Web Logging
    - NSWL Troubleshooting
    - NetScaler Troubleshooting
    - Buffer Overflow