CNS-320: Citrix ADC 12.x Advanced Concepts - Security, Management and Optimization

Duration: 5 Days

Prerequisites:

To ensure that participants can fully benefit from the CNS-320: Citrix ADC 12.x Advanced Concepts - Security, Management, and Optimization course, the following prerequisites are recommended:

- Basic understanding of networking concepts, including routing and switching
- Familiarity with the Citrix ADC platform, including its deployment and basic configuration
- Knowledge of web server fundamentals, such as what web servers do and how they function
- Experience with Citrix ADC load balancing, SSL offloading, and content switching concepts
- Prior completion of the CNS-220 (Citrix ADC 12.x Essentials and Traffic Management) course or equivalent knowledge
- Understanding of the OSI model and the role of application layer protocols such as HTTP/HTTPS
- Basic knowledge of cybersecurity concepts and common web application vulnerabilities
- Some experience with command-line interfaces and basic system administration

These prerequisites are intended to provide participants with the foundational knowledge required to grasp the advanced concepts covered in the CNS-320 course. With this background, learners will be equipped to engage with the course material effectively and apply what they learn in practical scenarios.

Course Description:

The CNS-320: Citrix ADC 12.x Advanced Concepts - Security, Management and Optimization course is a comprehensive training program designed to equip learners with the skills to secure, manage, and optimize Citrix ADC 12.x environments. Covering a range of advanced topics from the Citrix Web App Firewall and its security features to Application Delivery Management and optimization techniques, the course provides in-depth knowledge and hands-on experience. Participants will learn about common attacks, compliance with standards like PCI-DSS, and how to establish robust Web App Firewall policies and profiles. Regular expressions, attack protections, monitoring, and troubleshooting are also key components of the curriculum. Additionally, the course delves into security and filtering, configuration management using StyleBooks, web logging, integrated caching, front-end optimization, and system tuning practices. By completing the CNS-320 course, learners will develop the expertise necessary for securing and enhancing the performance of web applications using Citrix ADC 12.x advanced concepts security measures, ensuring efficient and secure delivery of services.

Target Audience:

The CNS-320 course offers in-depth training on Citrix ADC's security and optimization, ideal for IT professionals focused on network and application security.

- Network Engineers
- Security Specialists
- System Administrators
- Infrastructure Architects
- Citrix Administrators
- Compliance Officers
- IT Managers overseeing network operations
- Cybersecurity Analysts
- Application Developers with a focus on security
- DevOps Engineers involved in deployment and security automation
- Security Consultants providing web application and network security solutions
- IT Professionals aiming for Citrix certifications

Course Outlines:

Module 1: Citrix Web App Firewall Overview

- The Business Problem
- Industry Standards
- Protection Methodologies
- Introducing Citrix Web App Firewall
-

Module 2: Citrix Web App Firewall Profiles and Policies

- Citrix Web App Firewall Policies
- Citrix Web App Firewall Profiles
- Citrix Web App Firewall Learning
- Citrix Web App Firewall Engine Settings

Module 3: Implementing Citrix Web App Firewall Protections

- Security Checks and Data Flow
- Rules and Adaptive Learning
- Signatures and Comment Stripping
- Top-Level Protections

Module 4: Additional Citrix Web App Firewall Protections

- Cookie Consistency
- Advanced Form Protection Checks
- URL Protections
- Protecting Sensitive Data

Module 5: Monitoring and Troubleshooting Citrix Web App Firewall

- Web App Firewall and Web Applications
- Logging and Reporting
- Customizing Errors
- Troubleshooting

Module 6: Security and Filtering

- Application-level Quality of Experience (AppQoE)
- IP Reputation
- Rate Limiting
- HTTP Callout

Module 7: Authentication with Security Assertion Markup Language (SAML)

- What is SAML?
- Configuring SAML on Citrix ADC

Module 8: Authentication with OAuth, OpenID, and nFactor

- OAuth and OpenID
- Configuring OAuth on Citrix ADC
- Multi-Factor Authentication with nFactor
- Configuring nFactor

Module 9: Application Delivery Management Introduction

- An introduction to Application Delivery Management
- Application Delivery Management Deployment and
- Configuration
- Deploying Citrix Application Delivery Management in High Availability
- Citrix Application Delivery Management Instance
- Management

REGISTER NOW!
training@trends.com.ph
(+632) 8863-2123
www.trendsacademy.com.ph

Module 10: Managing and Monitoring Application Delivery Management

- Inventory Management
- User Management
- Analytics and Automation
- SSL Certificate Management

Module 11: Managing Citrix ADC Configuration

- Application Management
- StyleBooks
- Configuration Management

Module 12: Citrix ADC Web Logging

- Understanding Web Traffic
- Installing and configuring ADC 12.x Web Logging
- Troubleshooting ADC 12.x Web Logging

Module 13: Integrated Caching

- Introduction to Integrated Caching
- Static and Dynamic Content
- Request and Response Process Flow
- Understanding Cache Policies
- Identifying Content Group Settings

Module 14: Front End Optimization

- Improving Content Delivery
- Front-End Optimization Use Cases
- Understanding Minification
- CSS Optimizations

Module 15: Tuning and Optimization

- Connections on the Citrix ADC
- Connection Profiles
- Queuing on the Citrix ADC
- Connection Tuning Practices

REGISTER NOW!

training@trends.com.ph
(+632) 8863-2123
www.trendsacademy.com.ph