NetScaler ADC 14.x Fonctionnalités avancées (Sécurité et gestion)

Prix : 4 125 €HT

Durée : 5 jours

Code de Référence : NS301

Catalogue Citrix

Cette formation apporte les compétences nécessaires pour déployer et gérer le pare-feu d'application Web NetScaler, y compris les types d'attaques Web, les protections et les signatures, le moteur d'apprentissage adaptatif, les politiques et les profils du pare-feu d'application, le dépannage et les autres fonctionnalités de sécurité pertinentes de NetScaler.

Il permet aux participants d'apprendre à déployer AAA pour le trafic d'application avec nFactor et de comprendre les concepts liés aux schémas de connexion, aux étiquettes de politique et aux personnalisations.

Ils seront également en mesure de déployer la console NetScaler pour gérer un environnement NetScaler.

Versions Couvertes : NetScaler VPX v14.1 and NetScaler Console v14.1

Objectifs de la formation

A l'issue de cette formation Citrix, vous serez capable de :

- Configurer le pare-feu d'application Web NetScaler, y compris les politiques, les profils, les signatures et les pages d'erreur.
- Atténuer les différents types d'attaques à l'aide du pare-feu d'application Web NetScaler.
- Utiliser des fonctionnalités de sécurité supplémentaires de NetScaler telles que la gestion des robots, la limitation du débit, l'appel HTTP, la réputation IP et AppQoE.
- Déployer AAA pour le trafic d'application et nFactor pour contrôler l'accès aux ressources derrière NetScaler.
- Utiliser la console NetScaler pour surveiller et gérer un environnement NetScaler

Public

Cette formation Citrix s'adresse aux personnes qui déploieront et/ou géreront le pare-feu d'application (WAF), les mécanismes multiples d'authentification AAA pour le trafic d'application et NetScaler Console (ADM) dans leurs environnements NetScaler.

Prérequis

Il est recommandé d'avoir des connaissances de base sur les technologies et concepts suivants :

- Expérience avec la configuration de NetScaler v14.x (services, serveurs virtuels, politiques),
- Expérience avec des composants réseau tels que les routeurs et les commutateurs, connaissances des protocoles réseau et des applications connexes, ainsi que de la mise en place de réseaux (DMZ, vLANs, …),
- Connaissances de base des problèmes de sécurité réseau tels que les malwares, le phising, les attaques DDOS et bien d'autres
- Connaissances de base des composants de sécurité tels que les pare-feu, expérience et compréhension de la surveillance d'un réseau et des outils de gestion basé sur SNMP.

Il est également conseillé d'avoir de solides connaissances de base sur l'administration et la gestion du trafic de NetScaler ADC, et d'avoir suivi Citrix NS-201 : NetScaler ADC 14.x Administration ou d'avoir un niveau de connaissance équivalent.

Vous souhaitez faire vérifier vos prérequis ? Contactez-nous pour l'organisation d'un entretien téléphonique avec un de nos consultants formateurs.

Programme de la formation

Module 1 : Introduction à WAF

- Le problème commercial
- Normes de l'industrie
- Méthodologies de protection
- Présentation à NetScaler Web App Firewall

Module 2 : Profils WAF, Stratégies et Monitoring

- Stratégies, profils et apprentissage du pare-feu d'application Web NetScaler
- Journalisation et création de rapports
- Personnalisation des erreurs
- Suppression des signatures et des commentaires

Module 3 : Mise en oeuvre des protections

- Contrôles de sécurité et flux de données
- Protections d'URL
- Protections de niveau supérieur
- Contrôles avancés de protection des formulaires
- Règles et apprentissage adaptatif
- Vérification de la carte de crédit
- Objet sécurisé

Module 4 : Fonctionnalités de sécurités avancées

- Protection des robots
- Protection des API
- Journalisation des intervenants
- Inspection du contenu

Module 5 : Sécurité et filtrage

- Réputation IP
- Appel HTTP
- Limitation du débit IP
- Application Quality of Experience (AppQoE)

Module 6 : Introduction à AAA et présentation de nFactor

- Authentification, autorisation et audit
- Présentation de nFactor
- Libellé de la politique
- Schémas de connexion
- Politique et action d’authentification
- Protocole pris en charge

Module 7 : Cas d’utilisation de nFactor

- Présentation de l’authentification unique
- Stratégies de trafic
- Security Assertion Markup Language (SAML)
- Authentification par certificat
- OAuth

Module 8 : Personnalisation AAA

- Personnalisations du thème du portail
- Contrat de licence d’utilisateur final (CLUF)
- Messages d’erreur personnalisés

Module 9 : Intro to NetScaler Console

- Présentation de la console NetScaler
- Service de la console NetScaler
- Prise en main de la console NetScaler
- Configuration initiale
- Gestion des instances

Module 10 : Gestion et surveillance de la console NetScaler

- Gestion des utilisateurs
- Gestion des instances
- Gestion des événements
- Gestion des certificats SSL
- Tableau de bord de sécurité unifié
- Informations

Module 11 : Gestion des applications et des configurations à l’aide de la console NetScaler

- Stylebooks
- Gestion de la configuration
- Gestion de la configuration
- Audit de la configuration

Module 12 : Réglages et optimisations de performance

- Profils de connexion
- Profils SSL
- Profils réseau
- Gestion des certificats SSL
- Nœuds RPC

Méthodes pédagogiques

Cette formation Citrix est rythmée par une alternance d'exposés et de travaux pratiques. Les exercices réalisés lors des travaux pratiques permettent la mise en œuvre des connaissances acquises.

Méthodes d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques (des labs de formation fournis par Skillable, fournisseur officiel pour les labs validé par l'éditeur)
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.