

CANAC (IMPLEMENTING CISCO NAC APPLIANCE) 2.1

Objetivo

Este treinamento apresenta a solução NAC Appliance (Cisco Clean Access), que cuida do controle de admissão de usuários à rede através do reconhecimento e validação de postura das estações de trabalho. Nele são apresentados os componentes da solução e formas de configuração. Com aulas teóricas e práticas o profissional terá todos os conhecimentos necessários para entender o funcionamento da solução e implementá-la da forma eficiente, reconhecendo usuários, bem como seus dispositivos e direitos de acesso, além do controle dinâmico das estações de trabalho. Após completar este treinamento o profissional será capaz de:

- Levantar os requerimentos necessários e descrever a distribuição correta do dispositivo NAC Appliance (Access Clean Access) dentro da rede
- Configurar a solução NAC Appliance (Cisco Clean Access)
- Implementar a solução NAC com alta disponibilidade para detectar possíveis ameaças a rede e para facilitar o acesso dos usuários que se enquadram às políticas de segurança
- Manter a solução com alta disponibilidade em diferentes ambientes

Público Alvo

Este treinamento é voltado para profissionais que buscam sólidos conhecimentos para implementação da solução Cisco NAC Appliance e aos candidatos a certificação Cisco CCSP.

Pré-Requisitos

Para total aproveitamento neste treinamento é altamente recomendado que o aluno possua certificação Cisco CCNA e tenha assistido os treinamentos BSCI, BCMSN e SNRS ou possua os conhecimentos equivalentes.

Carga Horária

24 horas (3 dias).

Conteúdo Programático

THE CISCO NAC APPLIANCE SOLUTION

- Cisco Self-Defending Networks
 - o The Changing Landscape of Security
 - o The Cisco Host-Protection Strategy
 - o The Cisco SDN Initiative
 - o Trust & Identity
 - o Cisco NAC Products
- Cisco NAC Appliance
 - o Cisco NAC Appliance Solution
 - o Cisco NAC Appliance Features

- o Cisco NAC Appliance Components
- o Compliance Scenarios
- o Deployment Options
- o Configuration Overview
- o User Interface

- Cisco NAC Appliance Deployment Options
- o Cisco NAC Appliance Out-of-Band (OOB) Deployment
- o Cisco NAC Appliance In-Band Deployment
- o Compare Cisco NAC Appliance Deployment Options
- o Cisco NAS Operating Modes
- o Virtual Gateway vs. Real-IP Gateway
- o Layer 2 vs. Layer 3

- Configure User Roles
- o What is a User Role?
- o Create User Roles
- o Define Traffic Policies for User Roles
- o Configure Traffic Policies for User Roles
- o Create Local User Accounts

- Configure External Authentication
- o Configure External Authentication Providers
- o Authenticate Cisco NAC Appliance Users with Kerberos
- o Authenticate Cisco NAC Appliance Users with RADIUS
- o Authenticate Cisco NAC Appliance Users with LDAP
- o Authenticate Cisco NAC Appliance Users with NT Domain
- o Map Users to User Roles
- o Test User Authentication
- o Configure RADIUS Accounting for Users
- o Adding Custom RADIUS Attributes

- Configure DHCP
- o Cisco NAS DHCP Modes
- o Enable the DHCP Module
- o Configure IP Ranges (IP Address Pools)
- o Work with Subnets
- o Reserve IP Addresses
- o Configure User-Specified DHCP Options

NAC APPLIANCE IMPLEMENTATION

- Implement Cisco NAC Appliance In-Band Deployment
- o In-Band Process Flow
- o In-Band Deployment Configurations
- o Configure the Cisco NAS for In-Band Deployment
- o Add the Cisco NAS to the Managed Domain
- o Configure the Cisco NAS Interfaces
- o Add Managed Subnets

- o Configure Cisco NAS VLAN Settings

- Implement Windows Active Directory Single Sign-On (AD SSO)
 - o Kerberos Ticket Exchange
 - o Confirming a NAS Ticket
 - o Communications between the NAS and Active Directory
 - o AD SSO Configuration Checklist
 - o TCP & UDP Ports Required for AD SSO
 - o Configure the NAS for AD SSO
 - o Install Support Tools for Windows 2000 or 2003 Server
 - o Configure the Domain Controller with ktpass.exe

- Implement Virtual Private Network Single Sign-On (VPN SSO)
 - o Configuration Checklist
 - o Configure a Traffic Filter
 - o Add VPN Authentication Server to NAM
 - o Map VPN Users to Roles on NAM
 - o Enable VPN SSO on the NAS
 - o Adding a VPN Device to the NAS
 - o Configure RADIUS Accounting
 - o Configure the VPN Gateway as a Floating Device
 - o Test VPN SSO

- Implement Cisco NAC Appliance Out-of-Band Deployment
 - o OOB Process Flow
 - o OOB Deployment Considerations
 - o Layer 2 Central & Edge Deployment
 - o Layer 3 Virtual Gateway & Real-IP Gateway
 - o Layer 2 & 3 Clientless Host Options
 - o Differences between Cisco NAC Appliance OOB Setup and In-Band Setup
 - o Implement Cisco NAS OOB Operating Modes

- Manage Switches
 - o Implement Switch Management
 - o Configure the Network for OOB Deployment
 - o Configure Group, Switch, and Port Profiles
 - o Configure Port Profiles Adding Switches to the Managed Domain
 - o Configuring SNMP Advanced Settings
 - o Configure Switch Ports to Use Port Profiles
 - o Manage Switch Configuration Settings
 - o NAC Appliance Implementation Options

- Implement Cisco NAC Appliance on a Network
 - o Implement Cisco NAC Appliance
 - o General Setup Tab
 - o User Pages
 - o Configure Cisco NAA Support
 - o Manage Certified Devices

- o Device Exemption
- o Viewing User Reports

- Implement Network Scanning
 - o Configure the Quarantine Role
 - o Implement Nessus Plug-Ins
 - o Test a Scanning Configuration
 - o Customize the User Agreement Page
 - o View Scan Reports

- Configure the NAM to Implement Cisco NAC Appliance Agent on User Devices
 - o Configure the Cisco NAM to Implement the Cisco NAC Appliance Agent (NAA)
 - o Retrieve Updates
 - o Require the Use of the Cisco NAA
 - o Configure the Cisco NAA Temporary Role
 - o Introduce Checks, Rules, and Requirements
 - o Create a Check, Rules, and Requirements
 - o Map Requirements to Rules and Roles

- Configure NAM High Availability (HA)
 - o Introduce HA for Cisco NAMs
 - o Establish a Serial Connection Between Managers
 - o Digital Certificate Requirements
 - o Configure the Primary Cisco NAM
 - o Configure the Standby Cisco NAM

- Configure Cisco NAC Appliance Server (NAS) HA
 - o Introduce HA for NASs
 - o Implementation Considerations
 - o Digital Certificate Requirements
 - o Configure the Primary and Standby NAS
 - o Complete the Standby NAS HA Configuration
 - o Test the NAS HA Configuration
 - o Configure DHCP Failover
 - o NAC Appliance Monitoring and Administration

- Monitor a Cisco NAC Appliance Deployment
 - o Cisco NAC Appliance Monitoring
 - o Monitor Online Users
 - o Monitor NAS Health Event Logs
 - o Configure Basic SNMP Support
 - o Configure Syslog Support

- Administer Cisco NAM
 - o Define the Cisco NAM Administration Module
 - o Set Network and Failover Parameters
 - o Manage Administration Groups
 - o Manage Administration Users

- o Manage User Passwords
- o Administer the System Time
- o Manage SSL Certificates
- o Manage the Cisco NAC Appliance Software
- o Protect Your NAM Configuration

- Labs:
 - o Lab 1: Remote Lab Familiarization
 - o Lab 2: Bootstrap Primary NAM & NAS
 - o Lab 3: Configuring User Roles and Traffic Policies
 - o Lab 4: Configure NAS In-Band Virtual Gateway
 - o Lab 5: Create a High Availability NAM Cluster
 - o Lab 6: Configuring Active Directory Single Sign-On (AD SSO)
 - o Lab 7: Configuring VPN Remote Access
 - o Lab 8: Configuring NAC VPN SSO
 - o Lab 9: Configure Switch for Out-Of-Band Operation
 - o Lab 10: Configuring the NAC Appliance Agent (NAA) for Specific Threats
 - o Lab 11: Enhanced SSO with LDAP Group Authorization