Implementing NAC Appliance (Cisco Clean Access)

Cursusduur: 3 Dagen  Cursuscode: CANAC

Beschrijving:
This course is designed to teach delegates how to design & implement a Cisco NAC Appliance solution to suit your network. You will learn basic configuration tasks such as NAM and NAS deployment modes, authentication (including Windows SSO), role-based access control, posture assessment, and remediation.

Doelgroep:
This course will be of interest for anyone responsible for the design, implementation, or support of a Cisco NAC Appliance installation and Cisco Channel Partners preparing for CCSP and NAC Specialist certification.

Doelstelling:
- At the end of the course delegates will be able to:
  - Given client network security requirements, explain how a NAC Appliance (Cisco Clean Access) deployment scenario will meet or exceed network security requirements
  - Configure the common elements of a NAC Appliance (Cisco Clean Access) solution
  - Configure the NAC Appliance (Cisco Clean Access) in-band and out-of-band implementation options
  - Implement a highly available NAC Appliance (Cisco Clean Access) solution to mitigate network threats and facilitate network access for those users that meet corporate security requirements
  - Maintain a highly available NAC Appliance (Cisco Clean Access) deployment in medium and enterprise network environments

Vereiste kennis en vaardigheden:
The knowledge and skills that a learner must have before attending this course are as follows:
- Fundamental knowledge of implementing network security or CCSP or Cisco Security CSQ
- SNRS or working knowledge of digital certificates
- BCSI or working knowledge of HSRP.

Examens en certificering
This course will prepare delegates for the following exam;
(Now part of the CCSP Certification and one of the three possible electives)
Cursusinhoud:

Cisco Self-Defending Networks
- The Changing Landscape of Security
- The Cisco Host-Protection Strategy
- The Cisco SDN Initiative
- Trust : Identity
- Cisco NAC Products

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

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

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

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

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

NAC Appliance Implementation: Implement Cisco NAC Appliance In-Band Deployment
- In-Band Process Flow
- In-Band Deployment Configurations
- Configure the Cisco NAS for In-Band Deployment
- Add the Cisco NAS to the Managed Domain
- Configure the Cisco NAS Interfaces
- Add Managed Subnets and Configure Cisco NAS VLAN Settings

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

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

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

Manage Switches
- Implement Switch Management
- Configure the Network for OOB Deployment
- Configure Group, Switch, and Port Profiles
- Configure Port Profiles Adding Switches

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

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

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

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

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

Administer Cisco NAM
- Define the Cisco NAM Administration Module
- Set Network and Failover Parameters
- Manage Administration Groups
- Manage Administration Users
- Manage User Passwords
- Administer the System Time
- Manage SSL Certificates
- Manage the Cisco NAC Appliance

CANAC
www.globalknowledge.nl info@globalknowledge.nl 030 - 60 89 444
<table>
<thead>
<tr>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect Your NAM Configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAC Appliance Implementation Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement Cisco NAC Appliance</td>
</tr>
<tr>
<td>General Setup Tab</td>
</tr>
<tr>
<td>User Pages</td>
</tr>
<tr>
<td>Configure Cisco NAA Support</td>
</tr>
<tr>
<td>Manage Certified Devices</td>
</tr>
<tr>
<td>Device Exemption</td>
</tr>
<tr>
<td>Viewing User Reports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>to the Managed Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SNMP Advanced Settings</td>
</tr>
<tr>
<td>Configure Switch Ports to Use Port Profiles</td>
</tr>
<tr>
<td>Manage Switch Configuration Settings</td>
</tr>
</tbody>
</table>

---

**Nadere informatie:**

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444  
info@globalknowledge.nl  
www.globalknowledge.nl  
Iepenhoeve 5, 3438 MR Nieuwegein