

Device Administration mit Cisco ISE

Use Cases, Konfiguration und Troubleshooting

Device Administration mit Cisco ISE

Der administrative Zugriff auf Network-Devices, wie Router, Switches oder Firewalls, z. B. via Konsole oder SSH, kann lokal auf diesen Devices authentisiert werden. Deutlich flexibler, sicherer und skalierbarer ist allerdings eine Kontrolle durch die Cisco ISE. Im Rahmen der Device Administration können Benutzer von der ISE selbst oder über eine angebundene Benutzer-Datenbank zentral verwaltet werden. Hierbei spielt neben der Authentisierung die Zuweisung der Rechte an die Administratoren (Autorisierung) eine wesentliche Rolle. Mit RADIUS lässt sich das Verhalten der Shell, mit TACACS+ sogar einzelne Kommandos zentral kontrollieren. Über ein zentrales Reporting und Accounting sind aussagekräftige Audit-Logs verfügbar, wie sie in ISO-zertifizierten Umgebungen erforderlich sein können. In diesem Kurs werden die Vor- und Nachteile von TACACS+ sowie RADIUS bei der Device Administration beleuchtet, und die Konfigurationsmöglichkeiten auf der ISE erklärt. Hierzu wird eine Basis-Konfiguration eines Distributed Deployments mit den unterschiedlichen ISE Nodes beschrieben, und Maintenance-Maßnahmen sowie die Einrichtung von Role Based Access Control (RBAC) erläutert. Basierend darauf werden die Authentisierung- insbesondere aber auch die Autorisierungs-Policy mit ihren unterschiedlichen Conditions und Results angesprochen. Auch die notwendige Peripherie, wie ein Active Directory und eine Microsoft PKI werden mit einbezogen.

Kursinhalt

- Device Administration, Komponenten und Abläufe
- RADIUS vs. TACACS+
- Überblick über die Identity Service Engine
- Lizenzierung und Smart Licensing
- Installation und Basis-Konfiguration einer ISE
- Node Types in ISE Deployments
- Device Administration – Konfiguration von Network Devices
- Authentisierungs-Varianten
- Nutzung externer Datenbanken
- Policy-basierte Kontrolle auf der ISE
- Authentisierungs- und Autorisierungs-Regeln,
- Conditions und Results
- Möglichkeiten der Shell Profiles
- Wildcards und Regular Expressions in Command Sets

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Der Kurs ist für diejenigen gedacht, die die Cisco ISE für eine zentrale Device-Administration-Kontrolle einsetzen wollen, und/oder zentrale Audit-Logs benötigen.

Voraussetzungen

Neben grundlegenden Netzwerk- und IP-Kenntnissen sollte ein Grundverständnis zum Betrieb eines Cisco-Netzes vorhanden sein.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/ISED

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in Deutschland	3 Tage CHF 2.415,-
Online Training	3 Tage CHF 2.415,-
Termin/Kursort	Kurssprache Deutsch 
28.10.-30.10.24  Frankfurt	28.10.-30.10.24  Online

Stand 26.04.2024



Inhaltsverzeichnis

Device Administration mit Cisco ISE – Use Cases, Konfiguration und Troubleshooting

- 1 AAA und Device Administration**
 - 1.1 Zentrale Zugriffskontrolle auf Network Devices**
 - 1.1.1 Hintergründe
 - 1.1.2 Zugriffskontrolle in der Praxis
 - 1.2 RADIUS**
 - 1.2.1 Das Paketformat
 - 1.2.2 RADIUS-Authentisierung und Autorisierung
 - 1.2.3 RADIUS Accounting
 - 1.2.4 Funktion der RADIUS Attribute
 - 1.3 TACACS+**
 - 1.3.1 Das Paketformat
 - 1.3.2 TACACS+ Authentisierung
 - 1.3.3 TACACS+ Autorisierung
 - 1.3.4 TACACS+ Accounting
 - 1.4 Konfiguration der Network Devices**
 - 1.4.1 Einrichten der Radius Clients
 - 1.4.2 Einrichten der TACACS+ Clients
- 2 ISE Grundkonfiguration**
 - 2.1 ISE-Konzept**
 - 2.1.1 Das ISE 3.x Lizenzmodell
 - 2.2 Installation der ISE (1/3)**
 - 2.2.1 ADE OS-Konfiguration
 - 2.2.2 Die ISE über die CLI verwalten
 - 2.3 ISE-Access**
 - 2.3.1 ISE GUI
 - 2.3.2 Launch Menü
 - 2.3.3 Zertifikate und ISE
 - 2.4 ISE– Basic Device Admin Settings**
 - 2.4.1 PSN-Konfiguration
 - 2.4.2 Device Admin – Overview
 - 2.5 Deployments**
 - 2.5.1 Node Registration
 - 2.5.2 Zertifikatsverwaltung im Deployment
 - 2.5.3 Redundanz in ISE-Deployments
- 3 Administration und Maintenance**
 - 3.1 Admin Access**
 - 3.1.1 Administrator Groups
 - 3.1.2 Admin Policies
 - 3.1.3 Admin Permissions
 - 3.2 Maintenance**
 - 3.2.1 Backup
 - 3.2.2 Scheduled Backups
 - 3.3 Network Access Devices**
 - 3.3.1 NAD für TACACS+ konfigurieren
 - 3.3.2 Network Device Groups
 - 3.3.3 Im- und Export von Network Devices
- 4 Authentication und Authorization bei der Device Administration**
 - 4.1 Das ISE AAA-Konzept**
 - 4.2 Device Admin Policy Sets**
 - 4.2.1 Condition Elements
 - 4.2.2 Allowed Protocols
 - 4.3 Die Authentication Policy**
 - 4.3.1 Authentication Condition Elements
 - 4.3.2 Identity Stores in der Authentication Policies
 - 4.3.3 Fallback-Szenarien
 - 4.4 User Stores**
 - 4.4.1 Interne User
 - 4.4.2 Interne Gruppen
 - 4.4.3 Externe Datenbanken
 - 4.4.4 Identity Source Sequence
 - 4.5 Device Admin – Authorization Policy**
 - 4.5.1 Authorization Condition
 - 4.5.2 Device Admin Result – Shell Profiles
 - 4.5.3 Device Admin Result – Command Set
 - 4.6 Device Administration per Radius**
 - 4.6.1 Network Access Policy Sets
 - 4.6.2 Radius Authentication
 - 4.6.3 Radius Authorization
- 5 Logging, Monitoring und Troubleshooting**
 - 5.1 Operationen im Überblick**
 - 5.2 TACACS+ Logging**
 - 5.2.1 TACACS+ Reports
 - 5.2.2 TACACS+ Accounting
 - 5.3 Radius Logging**
 - 5.3.1 Radius Authentication und Authorization
 - 5.3.2 Radius Accounting
 - 5.4 Audit Reports**
 - 5.5 Troubleshooting mit TCP Dump**
 - 5.6 Log und Alarm-Einstellungen**
 - 5.6.1 Log Categories
 - 5.6.2 Alarm Settings

