ArcSight Management Center (ArcMc) Administration (ARCMCA)

ID ARCMCA **Preis** 3.750,– € (exkl. MwSt.) **Dauer** 5 Tage

Wichtige Hinweise für die Buchung von Open-Text-Trainings

Bitte beachten Sie, dass für die Teilnahme an einem Open-Text-Training Vorkasse zu leisten ist. Eine Teilnahme an einem Training ist für 12 Monate nach Kursbuchung möglich. Stornierungen sind ausgeschlossen. Weitere Informationen entnehmen Sie bitte **unseren** Allgemeinen Geschäftsbedingungen.

Dieser Text wurde automatisiert übersetzt. Um den englischen Originaltext anzuzeigen, klicken Sie bitte hier.

Kursüberblick

Dieser Kurs wurde entwickelt, um ArcSight-Systemadministratoren die grundlegenden und praktischen Fähigkeiten zu vermitteln, die sie benötigen, um die Verwaltung und Überwachung verschiedener ArcSight-Komponenten wie Transformation Hub, Logger, SmartConnectors, FlexConnectors und anderer eigenständiger ArcSight Management Center (ArcMC)-Geräte im ArcSight-Ökosystem effektiv zu zentralisieren.

Es umfasst ArcMC Version 24.1: Core ArcMC (früher bekannt als Fusion) und Software ArcMC (Standalone).

Höhepunkte:

- Installieren und Konfigurieren der Software ArcMC
- Konfigurieren von Core ArcMC in einer ArcSight Platform-Instanz
- Zentrale Konfiguration, Überwachung und Bereitstellung von Konnektoren
- Verwendung von Konfigurationsvorlagen zur Vereinfachung der Verwaltung von ArcSight-Komponenten
- Werkzeuge zur Verwaltung von Benutzern und Gruppen in eigenständigen ArcMCs und Loggern
- Implementierung der Überwachung verschiedener Metriken für ArcSight-Komponenten und -Geräte

Zielgruppe

Systemadministratoren, die daran interessiert sind, ArcSight-Komponenten zentral zu verwalten.

Voraussetzungen

Um an diesem Kurs erfolgreich teilnehmen zu können, sollten Sie über die folgenden Voraussetzungen oder Kenntnisse verfügen:

- Vertraut mit der Installation und Konfiguration von ArcSight Connectors
- Grundlegendes Verständnis der ArcSight Logger-Funktionalität wie Ereignissuche, Empfänger und Benutzerverwaltung
- Grundlegendes Verständnis der ArcSight Platform Solution und der Transformation Hub-Komponente

Kursziele

Nach Abschluss dieses Kurses sollten die Teilnehmer in der Lage sein:

- Beschreiben Sie die ArcMC-Produkteigenschaften
- Durchführung der Installation und Verwaltung von eigenständigen ArcMC-Geräten
- Führen Sie die Konfiguration von Core ArcMC in einer ArcSight Platform-Instanz durch
- Implementierung eines rollenbasierten Zugriffs zur Verwaltung von Benutzern und Gruppen für Logger und ArcMCs
- Identifizieren Sie die Szenarien für die Verwendung von ArcMC Node Management und Configuration Management Funktionen
- Schnelle Installation von Konnektoren mit der ArcMC Instant Connector Deployment Funktion
- Zentrale Aktivierung von Überwachung und Alarmen für verwaltete ArcSight-Komponenten
- Erstellen Sie Konfigurationsvorlagen, um Abonnenten schnell zu konfigurieren und nicht konforme verwaltete Komponenten zu identifizieren.
- Verstehen des Upgrade-Prozesses für Konnektoren, Logger und eigenständige ArcMCs

Kursinhalt

- Einführung in Produktmerkmale und Architektur
- Installation der Software ArcMC (nicht containerisiert)
- Systemverwaltung für ArcMC (nicht containerisiert)
- Knotenverwaltung mit Fusion ArcMC (containerisiert) - ArcMC und Logger-Knoten
- Node Management - Importieren von Hosts mit Konnektoren unter Verwendung von Core- und Software-ArcMC-Konsolen
- Knotenverwaltung - Verwaltung von Konnektorparametern mit der ArcMC-Konsole
- Konfigurationsmanagement
- Verwalten von Benutzern auf verwalteten Produkten
- Dokumentieren von Fähigkeiten in der ArcSight-Plattform-Instanz
- Verwalten des Transformation Hub - Importieren eines Hosts in Core ArcMC
- Verwalten des Transformation Hub - Routing von Ereignissen zwischen Themen
- Verwaltung von Verstoßregeln und Überwachung von Dashboards in ArcMC
- Generator-ID-Verwaltung in ArcMC
- ArcMC Produktverwaltung - Anwendungswerkzeuge
- ArcMC Produktverwaltung - Repositories und Knoten-Upgrades

Detaillierter Kursinhalt

Kapitel 1: Einführung in Produktfunktionen und Architektur

- Beschreiben Sie die Probleme, die ArcSight Management Center löst
- Erkennen der Architektur der ArcSight-Plattform
- Beschreiben Sie, wo ArcMC in die ArcSight-Plattform passt
- Verstehen der Bereitstellungsoptionen für ArcMC-Funktionalität: containerisiert oder eigenständig (auch bekannt als nicht containerisiert)

Kapitel 2. Installation der Software ArcMC (nicht containerisiert)

- Erkennen der Voraussetzungen für die Installation von Software ArcMC
- Beschreiben Sie die Installationsschritte für die Software ArcMC
- Erkennen des Hochladens von ArcMC-Lizenzen und Starten/Stoppen von ArcMC-Prozessen
- Beschreiben Sie, wie die Benutzeroberfläche des ArcMC-Produkts aufgebaut ist
- Loggen Sie sich in die ArcMC UI ein, um einen gesunden Betriebszustand zu überprüfen

Kapitel 3: Systemverwaltung für ArcMC (nicht containerisiert)

- Beschreiben Sie die Optionen des Systemverwaltungs-Untermenüs auf der Benutzeroberfläche
- Unterscheidung zwischen ArcMC Appliance und Software ArcMC System Admin Fähigkeiten
- Suchen und Konfigurieren von ArcMC-Geräteeinstellungen
- Definieren Sie eine Passwortrichtlinie und ein Login-Banner für ArcMC-Benutzer
- Überprüfen und Konfigurieren der Sys-Admin-Einstellungen, einschließlich der Definition einer Kennwortrichtlinie und eines Anmeldebanners

Kapitel 4: Knotenverwaltung mit Fusion ArcMC (containerisiert) - ArcMC und Logger-Knoten

- Erkennen, wie ArcMC Node Management verwendet, um ArcMC (nicht containerisierte) Instanz- und Logger-Knotentypen zu verwalten
- Beschreiben Sie die in der ArcMC-Konsole verfügbaren Knotenmanagement-Aufgaben
- Verstehen, wie man Knoten von einem Host aus hinzufügt
- Erfahren Sie, wie man Hosts aus einer CSV-Datei importiert
- Identifizieren, Hinzufügen und Organisieren von ArcSight-Hosts und -Knoten anhand von Standorten
- Beschreibung der ArcMC-Agent-Funktionalität sowie der Installations- und Upgrade-Schritte
- Verstehen, wie die Erstkonfigurationsfunktion als schnelle und einheitliche Einrichtung für mehrere ArcSight Logger dient
- Erstellen von Standortverwaltungseinheiten
- Import der Software ArcMC und der Logger-Knoten mit manuellen und Massenoperationen
- Probleme mit Anmeldeinformationen und Aktualisierung der ArcMC-Agentenversion

Kapitel 5: Knotenverwaltung - Importieren von Hosts mit Konnektoren unter Verwendung von Core- und Software-ArcMC-Konsolen

- Erkennen, wie ArcMC Node Management verwendet, um Hosts mit dem Knotentyp Connectors zu verwalten.
- Erfahrungen mit der Installation und Konfiguration von Connectors sammeln
- Erfahren Sie, wie Sie einen Host mit Konnektoren importieren können
- Identifizieren Sie die Schritte zum erneuten Scannen eines Hosts, um neue Connectors als verwaltete Knoten einzubinden
- Untersuchen Sie, wie ein einzelner Host mehrere Knoten (Konnektoren) für Verwaltungszwecke umfassen kann.
- Beschreiben Sie die Node Management Tools zur Verwaltung von Konnektoren, Containern und Zielen über

die ArcMC-Schnittstelle
- Erkennen Sie die Gesundheitsindikatoren im ArcMC Monitory Summary Dashboard
- Installieren Sie einen Anschluss über den SmartConnector-Assistenten
- Beschreiben Sie die Schritte zum Importieren von Windows- und Linux-Hosts mit Konnektoren als ArcMC-verwaltete Knoten

Kapitel 6: Knotenverwaltung - Verwalten von Anschlussparametern mit der ArcMC-Konsole

- Erkennen, wie ArcMC das Node Management nutzt, um die Konfigurationseinstellungen von Konnektoren zentral zu verwalten
- Beschreibung der wichtigsten Komponenten für die Verwaltung des Connectors: Container, Konfiguration des Connectors und Konfiguration des Ziels
- Verwalten der Connector-Parameter mit der Core ArcMC-Konsole
- Abrufen und Überprüfen von Audit-Protokollen, die von Konnektoren über die Core ArcMC-Konsole generiert werden
- Beschreiben Sie, wie die Knotenverwaltung den täglichen Betrieb und die Feinabstimmung von Hosts mit Connector-Knoten regelt.

Kapitel 7: Konfigurationsmanagement

- Beschreiben Sie, wie ArcMC Configuration Management funktioniert
- Identifizieren Sie die Unterschiede zwischen Anfangskonfigurationen und Teilnehmerkonfigurationen
- Erstellen verschiedener Teilnehmerkonfigurationen
- Besprechung von Best Practices für die Verwendung von Konfigurationsmanagement
- Erstellen von Konfigurationsvorlagen für die Verwaltung von Einstellungen in der verwalteten Software ArcMC, Logger und Connectors
- Erstellen Sie Richtlinien, um verschiedene Arten von Empfängern in Logger-Knoten zu verwalten
- Filter-Ressourcen in Logger-Knoten konsolidieren
- Erstellen einer Mapping-Datei-Konfiguration für verwaltete Konnektoren
- Erstellen von Konfigurations-Baselines für verwaltete Knoten
- Verwalten von ArcSight-Netzwerkmodell-Ressourcen wie Netzwerk- und Zoneneinstellungen für verwaltete Konnektoren

Kapitel 8. Verwalten von Benutzern auf verwalteten Produkten

- Beschreiben Sie, wie die Benutzerverwaltung und die rollenbasierte Zugriffskontrolle auf die Verwaltung von Benutzern in einer ArcSight-Bereitstellung angewendet werden
- Beschreiben Sie die verschiedenen Komponenten, aus denen die Benutzerverwaltung besteht
- Ausführen und Untersuchen von nicht konformen Benutzerkonfigurationen
- Implementierung der rollenbasierten Zugriffskontrolle RBAC für eigenständige ArcMCs und Logger-Geräte
- Beschreiben Sie die Schritte zur Erstellung von Konformitätsberichten zur Auflistung und Validierung von Benutzern/Gruppen/Rollen, die in verwalteten Knoten implementiert sind

Kapitel 9: Dokumentieren von Fähigkeiten in der ArcSight-Plattforminstanz

- Identifizierung der Fähigkeiten der ArcSight-Plattform mithilfe von ITOM und Core Interfaces
- Beschreiben Sie die Konfiguration der ArcSight-Plattform zur Aktivierung der ArcMC-Funktionalität, die als Core ArcMC bekannt ist.
- Erklären Sie, wie die Hauptbenutzeroberfläche organisiert ist.
- Beschreiben Sie, wie Sie den Status von ArcSight Platform-Komponenten (Pods) mithilfe von CLI und ITOM-Schnittstelle validieren.
- Dokumentieren Sie die Fähigkeiten, die in Ihrer ArcSight Platform-Instanz eingesetzt werden
- Identifizierung der Versionen von Core (Fusion) und Transformation Hub-Funktionen
- Erkennen Sie die Abhängigkeiten zwischen Fusion, Transformation Hub und ArcMC

Kapitel 10: Verwalten des Transformation Hub - Importieren eines Hosts in Core ArcMC

- Beschreiben Sie die Schritte zur Integration von Transformation Hub (TH) und ArcMC
- Beschreiben und konfigurieren Sie Produzenten und Konsumenten in TH
- Identifizieren Sie den Status von TH in der Übersichtstabelle
- Import von Transformation Hub als verwalteter Knoten über die Core ArcMC-Schnittstelle
- Verwalten von Konnektoren mit Transformation Hub Destinationen
- Identifizieren Sie die Schritte zur Konfiguration von ESM und Logger als Transformation Hub Consumers

Kapitel 11: Verwalten von Transformation Hub - Weiterleiten von Ereignissen zwischen Themen

- Erkennen der Konfigurationseigenschaften von Ressourcen für Themen und Routingregeln

- Beschreiben Sie die Schritte zur Erstellung von Kafka-Themen im Transformation Hub über die Core ArcMC-Schnittstelle
- Konfigurieren der Weiterleitung und des Filterns von Ereignissen zwischen Themen über die Core ArcMC-Schnittstelle
- Beschreiben Sie die Schritte, um einen Logger-Konsumenten so einzustellen, dass er Ereignisse aus einem neu erstellten Thema bezieht
- Erkennen Sie die ArcMC Monitoring Dashboards, um die Konfiguration und den Betrieb des Event Routings zu überprüfen

Kapitel 12: Verwaltung von Verstoßregeln und Überwachungs-Dashboards in ArcMC

- Beschreiben Sie die Schritte zum Erstellen von Verstoßregeln für verwaltete Knoten und Geräte
- Identifizieren Sie die integrierten Überwachungsregeln und Dashboards
- Erkennen von ArcMC Monitoring Dashboards zur Ermittlung des Knoten- und Gerätezustands
- Beschreiben Sie die Schritte zur Inspektion von Audit-Protokollen in ArcMC, die von Verletzungsregeln generiert werden

Kapitel 13: Generator-ID-Verwaltung in ArcMC

- Erkennen von Global Event ID Design und Funktionen
- Beschreiben Sie die Schritte zur Konfiguration von ArcMC als Generator-ID-Manager
- Erkennen, wie ArcMC den Manage Nodes Generator IDs zuweist
- Beschreiben Sie die Schritte zur Zuweisung von Generator-IDs zu Software-ArcMC- (nicht containerisiert) und Logger-Prozessen über den ArcMC Generator ID Manager
- Identifizieren Sie die zugewiesenen Generator-IDs über das Bedienfeld Generator-ID-Manager

Kapitel 14: ArcMC-Produktverwaltung - Anwendungswerkzeuge

- Beschreiben Sie die ArcMC-Werkzeuge unter dem Menü Verwaltung > Anwendung: Sichern, Wiederherstellen Snapshot Logger Datenverbrauchsbericht
- Beschreiben Sie die Schritte zur schnellen Installation von Konnektoren mit Hilfe der ArcMC-Funktion "Instant Deployment".
- Erkennen, wie Audit-Ereignisse von einer eigenständigen ArcMC-Software-Instanz weitergeleitet werden
- Beschreiben Sie die Schritte zur Installation und Konfiguration eines Syslog Connectors über Configuration Management Templates
- Identifizierung von ArcMC-Audit-Ereignissen in eigenständiger ArcMC-Software und Logger-Schnittstellen

Kapitel 15: ArcMC-Produktverwaltung - Repositories und Knoten-Upgrades

- Erkennen, wie ArcMC-Repositories zum Hochladen von Upgrade- oder Content-Update-Dateien verwendet werden
- Identifizieren Sie die Schritte zum Upgrade von Logger und eigenständig verwalteten ArcMC-Software-Knoten
- Upgrade von Connectors Framework und Parser mit ArcSight Update Files durchführen
- Beschreiben Sie die Schritte zur Durchführung des Remote-Upgrades von Loggern, Software ArcMC und Konnektoren über die Core (Fusion) ArcMC-Schnittstelle.
- Beschreiben Sie die Schritte zur Installation, Konfiguration und Aktualisierung von Syslog Connectors über die ArcMC-Schnittstelle

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch