Active Directory Federation Service

Aufbau und Betrieb einer IdP-Infrastruktur

Microsoft Partner
Gold Communications
Gold Project and Portfolio Management
Silver Application Integration
Silver Small and Midmarket Cloud Solutions

Active Directory Federation Service

Um Benutzern einer On-Premise Microsoft-Infrastruktur Zugriff auf Azure bzw. Microsoft 365 zu geben, bieten sich verschiedene Möglichkeiten an. Eine davon ist die Synchronisation der Konten mittels Azure AD Connect sowie der Einsatz eines Active Directory Federation Service (AD FS), welcher für die Authentisierung sowie Autorisierung verantwortlich ist. Diese Variante zeichnet sich dadurch aus, dass keine Kennwörter in die Cloud synchronisiert werden müssen. Dieser Kurs beschäftigt sich mit dem Aufbau einer AD FS-Infrastruktur, der Einbindung von lokalen Anwendungen sowie Cloud Services, der Konfiguration von Access Tokens mit Hilfe der Claim Rule Language sowie der Steuerung der Berechtigung mit Hilfe von Access Rules.

Kursinhalt

- Konfiguration von Azure AD Connect
- Aufbau und Funktionsweise einer AD FS-Infrastruktur
- Installation und Ersteinrichtung von AD FS Server und Web Application Proxy
- Anbindung von Cloud Services
- Anbindung von lokalen Anwendungen
- Anpassen der Authentisierungsmethoden
- Steuerung von Zugriffsrechten
- Beeinflussen von Claims mit Hilfe der Claim Pipeline und der Claim Rule Language
- Bereitstellen von Non-Claims Aware Applications
- Zertifikatsbasierte Authentisierung
- Device Registration Service

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 richtet sich an Administratoren, welche mit Hilfe des Active Directory Federation Service eine Identity Provider- (IdP-) Infrastruktur aufbauen wollen, um Cloud Service Provider wie Azure anzubinden.

Voraussetzungen

Die Teilnehmer sollten Vorkenntnisse im Bereich Benutzerverwaltung, Authentisierung und Autorisierung aufweisen können. Der Kurs Active Directory Fundamentals & LDAP – Protokolle, Architektur und Funktionsweise ist eine gute Basis.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/**ADFS**

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**	**€ 2.195,-**
Online Training	**3 Tage**	**€ 2.195,-**
Termin/Kursort		Kurssprache Deutsch
16.10.-18.10.24 HY Frankfurt	16.10.-18.10.24 HY Online	

Stand 17.04.2024

Microsoft

ExperTeach

Inhaltsverzeichnis

Active Directory Federation Service – Aufbau und Betrieb einer IdP-Infrastruktur

1 Funktionsweise von Single Sign-on
1.1 Autentisierung im Netzwerk
1.1.1 Zwischenspeicherung von Kennwörtern
1.1.2 Zugriff auf die Ressource
1.1.3 Authentifizierung
1.1.4 Erzeugung des Tokens
1.1.5 Zustellung des Tokens
1.1.6 Authentisierung gegenüber der Ressource
1.1.7 Erlauben des Zugriffs
1.2 Die eigentlichen Herausforderungen
1.2.1 Erneute Authentisierung
1.2.2 Übermittlung weitere Parameter nach der ersten Authentifizierung
1.2.3 Nächste Anmeldung
1.2.4 Neues Token
1.3 Vertrauensstellung
1.3.1 Sichere Übertragung
1.4 Single Sign-on

2 Modern Authentication
2.1 Claim-oriented Protocols
2.2 WS-Federation & WS-Trust
2.3 Security Assertion Markup Language (SAML)
2.3.1 Komponenten von SAML
2.3.2 Ablauf einer SAML-Authentication
2.3.3 Zugriff auf eine Ressource bei einer vorherigen Authentisierung
2.4 Open Authentication 2 (OAuth2)
2.4.1 Beispiel
2.4.2 Webseite für eine Authorization Prompt
2.4.3 Ablauf einer OAuth Authorization – Authorization Code
2.4.4 Implicit Grant
2.4.5 OAuth als Service Provider (Client) nutzen
2.5 OpenID Connect

3 Claim-based Identity
3.1 Identity Provider (IdP)
3.2 Relying Party (RP)
3.2.1 Metadata
3.2.2 Token
3.3 Attribute Store
3.4 Certification Authority
3.5 Reverse Proxy
3.5.1 Public Certificate
3.6 High Availability
3.6.1 Identity Provider
3.6.2 Network Load Balancer
3.6.3 High Availability (Reverse Proxy)

4 Installation
4.1 Zertifikat beantragen
4.1.1 CSR Erstellen
4.1.2 CSR einreichen
4.2 Installation der Rolle
4.3 Post-deployment configuration
4.3.1 Benutzer auswählen
4.3.2 IdP Namen festlegen
4.3.3 Service Account angeben
4.3.4 Datenbank
4.3.5 Konfiguration abschließen
4.4 Automatische Windows Authentication

5 Identity Provider Konfiguration
5.1 Lokaler Webserver
5.2 Office 365
5.2.1 Issuance Transform Rules
5.2.2 Abändern eines Claims
5.2.3 Active Directory Authentication Library (ADAL)
5.3 Google G-Suite
5.3.1 Relying Party Trust einrichten
5.3.2 Serivce URL festlegen
5.3.3 Relying Party ID
5.3.4 Access Control Policies
5.3.5 E-Mail-Adresse innerhalb des Claims nameidentifier übertragen
5.3.6 Google Einstellungen
5.3.7 Anmeldeseite
5.3.8 Abmeldeseite
5.3.9 Webseite für Kennwortänderungen
5.3.10 Token-Signatur Zertifikat

6 Tokens & Claims
6.1 Die Claim Pipeline
6.2 Acceptance Transform Rules
6.3 Authorization Rules
6.4 Issuance Rule
6.5 Regel-Erstellung
6.5.1 Acceptance und Issuing Rules
6.5.2 Issuance Authorization Rules
6.5.3 Access Control Policies
6.6 Claim Rule Language
6.6.1 Bedingungen
6.6.2 Verkettung der Regeln
6.6.3 Oder-Verknüpfung
6.6.4 Reguläre Ausdrücke
6.6.5 Aktionen
6.6.6 Active Directory abfragen
6.6.7 Custom LDAP-Store abfragen
6.6.8 SQL-Store abfragen
6.6.9 Authorisation Rules

7 Web Application Proxy
7.1 Reverse Proxy
7.2 Installation
7.2.1 Rolle installieren
7.2.2 Konfiguration abschließen
7.2.3 Zertifikat auswählen
7.2.4 Namensauflösung
7.3 Zugriffe auf Cloud-Applikationen
7.3.1 Zugriffe aus dem Internet
7.3.2 Zugriffe aus dem LAN
7.4 Zugriffe auf Web Apps im LAN
7.4.1 Simple Web Apps
7.4.2 Web Apps mit Modern Authentication
7.4.3 Web Apps mit Kerberos Authentication

8 Zertifikatsbasierte Authentisierung
8.1 Authentisierung mit Client-Zertifikaten
8.1.1 Eigene Webseite
8.1.2 Server Name Indication
8.1.3 Subject Alternative Name
8.1.4 Certificate Binding
8.1.5 Certificate Authentication
8.1.6 Client Certificate
8.1.7 Certificate Revocation List
8.1.8 Certificate Trust List
8.1.9 Anmeldung
8.1.10 Automatische Zertifikats-Anmeldung
8.1.11 Zertifikat auswählen
8.1.12 Token
8.1.13 Tipp: Zertifikate
8.2 Device Registration Service
8.3 DRS: On-Premise
8.3.1 DRS Aktivieren
8.3.2 Proxy Aktualisieren
8.3.3 Device Registrieren (Android)
8.3.4 Certificate Trust List
8.3.5 Token
8.4 DRS: Kombination mit Office 365
8.4.1 Trust Relationship
8.4.2 DNS Name
8.4.3 Device Registration aktivieren
8.4.4 Device Writeback
8.4.5 Device Registrieren (Windows)
8.4.6 Registration Process
8.4.7 AD Object
8.4.8 Authentication Process
8.4.9 Kombinierte Authentication

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de