

Active Directory Federation Service

Aufbau und Betrieb einer IdP-Infrastruktur

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.at/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.

Stand 17.04.2024

Training		Preise zzgl. MwSt.
Termine in Deutschland	3 Tage	€ 2.195,-
Online Training	3 Tage	€ 2.195,-
Termin/Kursort	Kursprache Deutsch 	
16.10.-18.10.24  Frankfurt	16.10.-18.10.24  Online	

Inhaltsverzeichnis

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

1 Funktionsweise von Single Sign-on	4 Installation	6.6.9 Authorisation Rules
1.1 Autentisierung im Netzwerk	4.1 Zertifikat beantragen	7 Web Application Proxy
1.1.1 Zwischenspeicherung von Kennwörtern	4.1.1 CSR Erstellen	7.1 Reverse Proxy
1.1.2 Zugriff auf die Ressource	4.1.2 CSR einreichen	7.2 Installation
1.1.3 Authentifizierung	4.2 Installation der Rolle	7.2.1 Rolle installieren
1.1.4 Erzeugung des Tokens	4.3 Post-deployment configuration	7.2.2 Konfiguration abschließen
1.1.5 Zustellung des Tokens	4.3.1 Benutzer auswählen	7.2.3 Zertifikat auswählen
1.1.6 Authentisierung gegenüber der Ressource	4.3.2 IdP Namen festlegen	7.2.4 Namensauflösung
1.1.7 Erlauben des Zugriffs	4.3.3 Service Account angeben	7.3 Zugriffe auf Cloud-Applikationen
1.2 Die eigentlichen Herausforderungen	4.3.4 Datenbank	7.3.1 Zugriffe aus dem Internet
1.2.1 Erneute Authentisierung	4.3.5 Konfiguration abschließen	7.3.2 Zugriffe aus dem LAN
1.2.2 Übermittlung weitere Parameter nach der ersten Authentifizierung	4.4 Automatische Windows Authentication	7.4 Zugriffe auf Web Apps im LAN
1.2.3 Nächste Anmeldung	5 Identity Provider Konfiguration	7.4.1 Simple Web Apps
1.2.4 Neues Token	5.1 Lokaler Webserver	7.4.2 Web Apps mit Modern Authentication
1.3 Vertrauensstellung	5.2 Office 365	7.4.3 Web Apps mit Kerberos Authentication
1.3.1 Sichere Übertragung	5.2.1 Issuance Transform Rules	8 Zertifikatsbasierte Authentisierung
1.4 Single Sign-on	5.2.2 Abändern eines Claims	8.1 Authentisierung mit Client-Zertifikaten
2 Modern Authentication	5.2.3 Active Directory Authentication Library (ADAL)	8.1.1 Eigene Webseite
2.1 Claim-oriented Protocols	5.3 Google G-Suite	8.1.2 Server Name Indication
2.2 WS-Federation & WS-Trust	5.3.1 Relying Party Trust einrichten	8.1.3 Subject Alternative Name
2.3 Security Assertion Markup Language (SAML)	5.3.2 Service URL festlegen	8.1.4 Certificate Binding
2.3.1 Komponenten von SAML	5.3.3 Relying Party ID	8.1.5 Certificate Authentication
2.3.2 Ablauf einer SAML-Authentification	5.3.4 Access Control Policies	8.1.6 Client Certificate
2.3.3 Zugriff auf eine Ressource bei einer vorherigen Authentisierung	5.3.5 E-Mail-Adresse innerhalb des Claims nameidentifier übertragen	8.1.7 Certificate Revocation List
2.4 Open Authentication 2 (OAuth2)	5.3.6 Google Einstellungen	8.1.8 Certificate Trust List
2.4.1 Beispiel	5.3.7 Anmeldeseite	8.1.9 Anmeldung
2.4.2 Webseite für eine Authorization Prompt	5.3.8 Abmeldeseite	8.1.10 Automatische Zertifikats-Anmeldung
2.4.3 Ablauf einer OAuth Authorization – Authorization Code	5.3.9 Webseite für Kennwortänderungen	8.1.11 Zertifikat auswählen
2.4.4 Implicit Grant	5.3.10 Token-Signatur Zertifikat	8.1.12 Token
2.4.5 OAuth als Service Provider (Client) nutzen	6 Tokens & Claims	8.1.13 Tipp: Zertifikate
2.5 OpenID Connect	6.1 Die Claim Pipeline	8.2 Device Registration Service
3 Claim-based Identity	6.2 Acceptance Transform Rules	8.3 DRS: On-Premise
3.1 Identity Provider (IdP)	6.3 Authorization Rules	8.3.1 DRS Aktivieren
3.2 Relying Party (RP)	6.4 Issuance Rule	8.3.2 Proxy Aktualisieren
3.2.1 Metadata	6.5 Regel-Erstellung	8.3.3 Device Registrieren (Android)
3.2.2 Token	6.5.1 Acceptance und Issuing Rules	8.3.4 Certificate Trust List
3.3 Attribute Store	6.5.2 Issuance Authorization Rules	8.3.5 Token
3.4 Certification Authority	6.5.3 Access Control Policies	8.4 DRS: Kombination mit Office 365
3.5 Reverse Proxy	6.6 Claim Rule Language	8.4.1 Trust Relationship
3.5.1 Public Certificate	6.6.1 Bedingungen	8.4.2 DNS Name
3.6 High Availability	6.6.2 Verkettung der Regeln	8.4.3 Device Registration aktivieren
3.6.1 Identity Provider	6.6.3 Oder-Verknüpfung	8.4.4 Device Writeback
3.6.2 Network Load Balancer	6.6.4 Reguläre Ausdrücke	8.4.5 Device Registrieren (Windows)
3.6.3 High Availability (Reverse Proxy)	6.6.5 Aktionen	8.4.6 Registration Process
	6.6.6 Active Directory abfragen	8.4.7 AD Object
	6.6.7 Custom LDAP-Store abfragen	8.4.8 Authentication Process
	6.6.8 SQL-Store abfragen	8.4.9 Kombinierte Authentication

