

Cloud Web Security: Konfigurieren von Benutzer-/Gruppenattributen mit PingFederate und ADFS bei Verwendung von SAML

Inhalt

[Einführung](#)

[Anforderungen](#)

[Konfiguration](#)

[PingFed](#)

[ADFS](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie PingFederate- und ADFS-IDP-Server (Active Directory Federated Services) konfigurieren, um Benutzer-/Gruppendetails an den Cloud Web Security-Service zu senden, um präzise Richtlinien zu filtern.

Anforderungen

Cisco empfiehlt, die folgenden Punkte zu verstehen.

- Administrative Anmeldung/Zugriff auf den PingFed/ADFS-Server
- Informationen zur Navigation auf dem PingFed/ADFS-Server
- Damit die Genauigkeit bei HTTPS-Datenverkehr gewährleistet ist, muss die HTTPS-Prüfung für den gesamten Datenverkehr durchgesetzt werden.

Konfiguration

Führen Sie die folgenden Schritte aus, um Benutzer-/Gruppenattribute mit PingFederate und ADFS zu konfigurieren.

PingFed

Unter **Attributquellen** > Registerkarte **Benutzersuche**:

- Attributvertrag: **AUTHENTIFIZIERTE_GRUPPEN**
Quelle: **LDAP**

Wert: **Mitglied von**

- Attributvertrag: **SAML_SUBJECT**

Quelle: **LDAP**

Wert: **sAMAccountName**

ADFS

Registerkarte **Vertrauenswürdige Beziehungen** > **Vertrauenswürdige Partei - Vertrauenswürdige Beziehungen**:

- LDAP-Attributvertrag: **SAM-Kontoname**
Ausgehender Anspruchstyp LDAP: **Name-ID**
- LDAP-Attributvertrag: **Token-Gruppen**
Ausgehender Anspruchstyp LDAP: **Gruppe**

Überprüfen

Fehlerbehebung

Für dieses Dokument gibt es keinen Abschnitt zur Fehlerbehebung.