Fehler bei der Registrierung für Gastbenutzer bei der Registrierung für persönliche Google-Konten in Cisco Secure Access

Inhalt

Problem

Während der Bereitstellung von Private Access mit ZTNA (Zero Trust Network Access) schlägt die Registrierung eines Gastbenutzers bei einem persönlichen Google-Konto nach der erfolgreichen Registrierung bei Entra ID und der Bereitstellung bei Secure Access fehl. Zu den spezifischen Symptomen gehören:

- Client-basierte Registrierung: Der Registrierungsprozess erreicht die SSO-Authentifizierung, Anmeldeinformationen werden bereitgestellt, aber ZTNA zeigt einen "E/A-Fehler" an und der Registrierungsprozess bleibt hängen.
- Client-loser Zugriff: Gibt die Fehlermeldung "Cisco Secure Access Login Failure" (Cisco Secure Access-Anmeldung fehlgeschlagen) zurück. IDP-Konfiguration" zusammen mit Transaktions-ID prüfen

Diese Fehler verhindern den Zugriff auf private Ressourcen und wirken sich auf die Prüfung der ZTNA-Funktionalität für den Zugriff im Auftragnehmerstil mit nicht firmeneigenen Identitäten aus.

Umwelt

- Cisco Secure Access mit ZTNA-Bereitstellung
- Microsoft Entra ID (ehemals Azure AD) als Identitätsanbieter
- Persönliches Google-Konto (@gmail.com), registriert als Gastbenutzer in Entra ID
- Gastkonto bereitgestellt und sichtbar in sicherem Zugriff
- SAML-Authentifizierung zwischen Entra ID und Cisco Secure Access konfiguriert

Auflösung

Der Registrierungsfehler wurde durch Ändern der Konfiguration der SAML-Attributzuordnung in der Microsoft Entra-ID behoben. Zur Lösung des Problems wurden die folgenden Schritte unternommen:

Schritt 1: Analyse des DART-Pakets und des Kundenverhaltens

Überprüfen Sie das DART-Paket, um sicherzustellen, dass die Komponenten von Cisco Secure Client und ZTA ordnungsgemäß funktionieren. Bei der Analyse sollte überprüft werden, ob der Registrierungsablauf Cisco Secure Access erreicht und der Fehler während der SAML-Authentifizierung beim Identity Provider auftritt.

Phase 2: Authentifizierungsprotokolle für die Entra-ID überprüfen

Überprüfen Sie die Entra ID-Authentifizierungsprotokolle, um sicherzustellen, dass der Authentifizierungsprozess aus Sicht des Identitätsanbieters erfolgreich abgeschlossen wurde. Die Protokolle sollten eine erfolgreiche Authentifizierung aufweisen, aber Secure Access lehnt die Anmeldung aufgrund einer nicht übereinstimmenden Attribute ab.

Schritt 3: SAML-Attributzuordnungsproblem identifizieren

Stellen Sie fest, dass die Entra-ID den UPN (User Principal Name) als SAML-Anspruch ausstellt, der nicht mit der persönlichen Gmail-Kontoidentität übereinstimmt, die von Secure Access erwartet wird. Das Asserted IdP-Attribut entspricht nicht der erwarteten Benutzerkennung.

Schritt 4: SAML-Attributzuordnung ändern

Ändern Sie die SAML-Attributzuordnung in Microsoft Entra ID von UPN in E-Mail-Adresse. Dadurch wird sichergestellt, dass der Anspruch auf die E-Mail-Adresse mit der persönlichen Google-Kontoidentität übereinstimmt.

Schritt 5: Bestätigung der erfolgreichen Registrierung

Wiederholen Sie nach der Implementierung der Attributzuordnungsänderung den ZTNA-Registrierungsprozess. Die Cisco Secure Access ZTA sollte nun die Gmail-Adresse erkennen und die Registrierung erfolgreich abschließen.

Ursache

Der Registrierungsfehler wurde durch eine Diskrepanz zwischen dem SAML-Attribut, das von der Microsoft Entra-ID geltend gemacht wird, und der erwarteten Benutzerkennung in Cisco Secure Access verursacht. Die Entra-ID wurde so konfiguriert, dass die UPN (User Principal Name, Benutzerprinzipalname) als SAML-Anspruch gesendet wurde. Bei persönlichen Google-Konten (@gmail.com) entsprach diese UPN jedoch nicht der tatsächlichen E-Mail-Adressidentität. Cisco Secure Access erwartete, dass die E-Mail-Adresse als identifizierendes Attribut für den Abgleich mit dem bereitgestellten Gastbenutzerkonto verwendet wird, was dazu führt, dass die Authentifizierung trotz erfolgreicher IdP-Authentifizierung abgelehnt wird.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.