Cisco Secure Access Identity Synchronization mit Active Directory und Microsoft EntraID

Inhalt

Problem

Bei der Bereitstellung von Benutzern und Gruppen aus zwei identitätsbasierten Quellen mit demselben Domänennamen in Cisco Secure Access traten Probleme auf. Das spezifische Szenario umfasste das Synchronisieren von Identitäten aus dem lokalen Active Directory und Microsoft EntraID (ehemals Azure AD), wobei beide Quellen denselben Domänennamen verwendeten (z. B. domain.com).

Die wichtigsten Bedenken waren:

- Verständnis des Verhaltens von Identitätseigentum und Gruppenmitgliedschaftszuordnung, wenn in beiden Identitätsquellen dieselben Benutzer und Gruppen vorhanden sind
- Konsistente Durchsetzung von Zugriffsrichtlinien für Hybridbenutzer mit Zugriff auf Ressourcen vor Ort und in der Cloud
- Aufrechterhaltung der internen IP-Transparenz für Benutzer in dieser Hybrididentitätskonfiguration
- Bestimmen, ob die gleichzeitige Synchronisierung von beiden Quellen Probleme in einer Produktionsumgebung verursachen würde

Aus der Dokumentation geht hervor, dass "die gleichzeitige Synchronisierung derselben Benutzer und Gruppen über den Cisco AD Connector und die Cisco User Management for Secure Access-Anwendung nicht unterstützt wird und zu einer inkonsistenten Durchsetzung von Zugriffsregeln führt."

Umwelt

- Cisco Secure Access mit AD Connector- und EntraID-Integration

- Active Directory am Standort mit Domänenname, der mit der EntraID-Domäne übereinstimmt
- Microsoft EntraID (Azure AD) mit demselben Domänennamen wie standortbasiertes AD
- SAML-SSO-Konfiguration für Identitätsverbund
- Secure Web Gateway (SWG)-Modul für die Richtliniendurchsetzung
- Hybride Umgebung, die Zugriff auf Ressourcen am Standort und in der Cloud erfordert

Auflösung

Das folgende Verhalten wurde für die gleichzeitige Synchronisierung von Active Directory- und EntraID-Quellen bestätigt:

Verhalten der Gruppensynchronisierung

Wenn Gruppen mit demselben Namen aus beiden Quellen synchronisiert werden:

- In Cisco Secure Access werden zwei separate Gruppenobjekte erstellt - eines für jede Quelle
- Gruppen können in Zugriffsrichtlinien durch ihr Quell-Präfix unterschieden werden
- Standortbasierte AD-Gruppen werden angezeigt als: AD-Domäne/Gruppenname
- EntraID-Gruppen werden angezeigt als: Gruppenname

Bei der Laborüberprüfung wurde die Synchronisierung mit der Meldung "Success" erfolgreich durchgeführt. <<<< Synchronisiert" für Gruppen aus mehreren EntraID-Domänen.

Verhalten der Benutzersynchronisierung

Wenn Benutzer mit derselben Benutzer-ID aus beiden Quellen synchronisiert werden:

- Die Benutzeridentität wird während der Synchronisierung überschrieben
- Nur eine eindeutige Benutzer-ID bleibt in Secure Access sichtbar.
- Die endgültige Synchronisierungsquelle bestimmt die Attribute und Gruppenmitgliedschaften des Benutzers.
- Die EntraID-Synchronisierung hat in der Regel Vorrang vor AD am Standort, wenn beide konfiguriert sind.

Konfiguration der Zugriffsrichtlinie

Beide Gruppentypen können in Zugriffsrichtlinien verwendet werden:

- Verweis auf lokale AD-Gruppen über den vollständigen Pfad: AD-Domäne/Gruppenname
- Verweisen Sie mit dem einfachen Namen auf EntraID-Gruppen: Gruppenname
- Richtlinien können je nach Gruppenmitgliedschaft unterschiedliche Benutzer verwenden.

Die anschließende Einrichtung funktioniert bei vielen Kunden gut.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

Ursache

Während unseres Tests haben wir bestätigt, dass ein Benutzer, der über den standortbasierten AD Connector synchronisiert wird, diese Identität im Umbrella Dashboard effektiv "beansprucht". Wenn derselbe Benutzer bereits über die Azure AD-Synchronisierung vorhanden ist, werden die vorhandenen EntraID-Benutzerdaten durch die standortbasierte Synchronisierung überschrieben.

Dieses Verhalten stellt eine dokumentierte Einschränkung dar. Offiziellen technischen Dokumentationen von Cisco zufolge:
https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

"Die gleichzeitige Synchronisierung derselben Benutzer- und Gruppenidentitäten vom Umbrella

AD Connector und der Cisco Umbrella Azure AD-App wird nicht unterstützt und führt zu einer inkonsistenten Richtliniendurchsetzung."

Fazit: Die gewünschte Konfiguration (VA-Transparenz für Benutzer, die sowohl in Azure als auch vor Ort vorhanden sind) wird als nicht unterstützte Konfiguration bestätigt. Für den weiteren Pfad ist die Verwendung von Roaming-Clients erforderlich, um eine konsistente Identitätsdurchsetzung sicherzustellen.

Verwandte Inhalte

- Bereitstellung von Identitäten aus Azure AD - Cisco Umbrella-Dokumentation
- 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.