Sincronizzazione dell'identità Cisco Secure Access con Active Directory e Microsoft EntraID

Sommario

Problema

Gli utenti hanno incontrato difficoltà durante il tentativo di effettuare il provisioning di utenti e gruppi da due origini di identità con lo stesso nome di dominio in Cisco Secure Access. Lo scenario specifico prevedeva la sincronizzazione delle identità da Active Directory locale e Microsoft EntraID (in precedenza Azure AD) in cui entrambe le origini utilizzavano lo stesso nome di dominio (ad esempio, domain.com).

Le principali preoccupazioni erano:

- Informazioni sul comportamento del mapping di appartenenza a gruppi e proprietà di identità quando gli stessi utenti e gruppi esistono in entrambe le origini di identità
- Garantire l'applicazione coerente e sicura dei criteri di accesso per gli utenti ibridi che accedono sia alle risorse locali che a quelle cloud
- Mantenimento della visibilità IP interna per gli utenti in questa configurazione di identità ibrida
- Determinare se la sincronizzazione simultanea da entrambe le origini potrebbe causare problemi in un ambiente di produzione

Nella documentazione è indicato che "la sincronizzazione simultanea degli stessi utenti e gruppi da Cisco AD Connector e dall'app Cisco User Management for Secure Access non è supportata e determina l'applicazione incoerente delle regole di accesso".

Ambiente

- Cisco Secure Access con integrazione AD Connector ed EntraID

- Active Directory locale con nome di dominio corrispondente al dominio EntraID
- Microsoft EntraID (Azure AD) con lo stesso nome di dominio di Active Directory locale
- Configurazione SSO SAML per la federazione delle identità
- Modulo Secure Web Gateway (SWG) per l'applicazione delle policy
- Ambiente ibrido che richiede l'accesso alle risorse locali e cloud

Risoluzione

Il seguente comportamento è stato confermato per la sincronizzazione simultanea da entrambe le origini Active Directory e EntraID:

Comportamento sincronizzazione gruppi

Quando si sincronizzano gruppi con lo stesso nome da entrambe le origini:

- In Cisco Secure Access vengono creati due oggetti gruppo distinti, uno per ogni origine
- I gruppi possono essere distinti in base al prefisso di origine nei criteri di accesso
- I gruppi AD locali vengono visualizzati come: AD-Dominio/NomeGruppo
- I gruppi EntraID vengono visualizzati come: NomeGruppo

La verifica del laboratorio ha dimostrato che la sincronizzazione è riuscita con il messaggio "Operazione riuscita. <<<< Sincronizzato" per gruppi da più domini EntraID.

Comportamento sincronizzazione utente

Quando si sincronizzano utenti con lo stesso ID utente da entrambe le origini:

- L'identità utente viene sovrascritta durante la sincronizzazione

- In Secure Access rimane visibile un solo ID utente univoco
- L'origine finale della sincronizzazione determina gli attributi dell'utente e le appartenenze ai gruppi
- La sincronizzazione EntraID in genere ha la precedenza su Active Directory locale quando entrambi sono configurati

Configurazione criteri di accesso

Entrambi i tipi di gruppo possono essere utilizzati nei criteri di accesso:

- Fare riferimento a gruppi AD locali utilizzando il percorso completo: AD-Dominio/NomeGruppo
- Fare riferimento ai gruppi EntraID utilizzando il nome semplice: NomeGruppo
- I criteri possono differenziare gli utenti in base all'origine dell'appartenenza al gruppo

La procedura di configurazione è indicata per molti clienti.

```
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
```

Causa

Durante il test, abbiamo confermato che ogni volta che un utente viene sincronizzato dal connettore AD locale, "dichiara" effettivamente tale identità nel dashboard Umbrella. Se lo stesso utente esiste già tramite la sincronizzazione di Azure AD, la sincronizzazione locale sovrascriverà i dati utente EntraID esistenti.

Questo comportamento è una limitazione documentata. Secondo la documentazione tecnica ufficiale di Cisco: https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

"La sincronizzazione simultanea delle stesse identità di utenti e gruppi da Umbrella AD Connector e dall'app Cisco Umbrella Azure AD non è supportata e determina un'applicazione dei criteri

incoerente."

Conclusione: L'installazione desiderata (visibilità VA per gli utenti esistenti sia in Azure che in locale) è stata confermata come una configurazione non supportata. Il percorso successivo richiede l'utilizzo di client mobili per garantire l'imposizione coerente delle identità.

Contenuto correlato

- Provisioning delle identità da Azure AD - Documentazione di Cisco Umbrella
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).