Migrazione dei connettori AD ad accesso sicuro dall'autenticazione legacy all'autenticazione API

Sommario

Problema

Le organizzazioni che utilizzano Cisco Secure Access con Active Directory (AD) Connector ricevono notifiche che indicano che l'autenticazione API è consigliata per Active Directory e le appliance virtuali, con l'autenticazione legacy impostata per scadere il 29 maggio 2026. Gli utenti necessitano di assistenza nella configurazione per eseguire la migrazione dall'autenticazione legacy all'autenticazione API prima della data di scadenza e desiderano comprendere il potenziale impatto sulla sincronizzazione di AD e Virtual Appliance durante il processo di migrazione. Il problema principale è se l'implementazione di questa modifica durante l'orario di lavoro potrebbe causare errori nelle operazioni di sincronizzazione di AD e VA che possono influire sulle operazioni dipendenti da identità e criteri.

Ambiente

- Cisco Secure Access (in precedenza Cisco Umbrella)
- Connettori di Active Directory distribuiti
- Metodo di autenticazione legacy attualmente in uso
- Migrazione dell'autenticazione API richiesta prima del 29 maggio 2026
- Ambiente ad-only (in alcuni casi senza appliance virtuali)

Risoluzione

La migrazione dall'autenticazione legacy all'autenticazione API implica la generazione di chiavi API nel portale Secure Access e la relativa configurazione corretta. Il processo richiede la creazione di chiavi API di amministrazione e chiavi API client per i connettori AD e le appliance virtuali.

Passaggio 1: Genera chiave API di amministrazione

Passare a Amministrazione > Chiavi API nel portale Accesso sicuro e generare una nuova Chiave API di amministrazione e un nuovo segreto chiave di amministrazione. Memorizzare queste credenziali in modo sicuro in quanto sono necessarie per generare la coppia di chiavi API client.

Passaggio 2: Genera coppia di chiavi API client

Passare a Utenti e gruppi > Gestione configurazione > Impostazioni avanzate e individuare la sezione Autenticazione API. Immettere la chiave dell'API di amministrazione e il segreto della chiave di amministrazione generati nel passaggio 1, quindi fare clic su Genera coppia di chiavi dell'API client. In questo modo vengono generati la chiave API client e il segreto client utilizzati dai connettori AD e dalle appliance virtuali.

Passaggio 3: Configurazione dell'autenticazione API nelle impostazioni avanzate

Copiare la chiave API client e il segreto client generati nella sezione Impostazioni avanzate autenticazione API del portale Secure Access. Salvare queste credenziali in modo sicuro, in quanto necessarie per tutte le configurazioni di AD Connector e Virtual Appliance.

Passaggio 4: Aggiorna connettori AD e appliance virtuali

Applicare la chiave API client appena generata e il segreto client a tutti i connettori AD e le appliance virtuali distribuite. Ciò garantisce che possano autenticarsi correttamente per la registrazione e i controlli di integrità utilizzando il nuovo metodo di autenticazione API.

Impatto della migrazione e best practice

La generazione di chiavi API nel portale Secure Access non comporta in genere interruzioni. Tuttavia, l'impatto operativo si verifica durante il momento di passaggio in cui i connettori AD e le appliance virtuali vengono aggiornati in modo da utilizzare la nuova chiave e il nuovo segreto dell'API client.

Impatto previsto durante il taglio:

- È possibile che si verifichino errori temporanei di sincronizzazione e di controllo dello stato per i componenti che utilizzano ancora l'autenticazione legacy.
- Errore o ritardo di sincronizzazione di AD/VA durante la finestra di transizione.
- Se la sincronizzazione non riesce, è possibile che le decisioni relative ai criteri che si basano su dati di identità/gruppo aggiornati vengano influenzate.

Approccio di implementazione consigliato:

- Eseguire la migrazione durante l'orario di lavoro o le finestre di manutenzione, quando possibile.
- Per l'implementazione dell'orario di lavoro, utilizzare un approccio di aggiornamento in sequenza controllato.
- Aggiornare un connettore/VA alla volta e verificare lo stato integro prima di procedere.
- Evitare di aggiornare tutti i nodi contemporaneamente.
- Garantire una ridondanza adeguata con più connettori/VA per aggiornamenti in sequenza.

Compatibilità e requisiti:

- L'autenticazione API può essere utilizzata solo con le distribuzioni AD e non richiede appliance virtuali.
- I metodi di autenticazione legacy e API rimangono attivi durante il periodo di migrazione.
- I connettori AD devono essere in grado di eseguire la sincronizzazione con Umbrella tramite api.opendns.com e passare a api.umbrella.com.

Causa

Cisco Secure Access sta passando dai metodi di autenticazione legacy all'autenticazione API come meccanismo di autenticazione standard. Per il metodo di autenticazione legacy è stata pianificata una data di deprecazione il 29 maggio 2026. L'autenticazione API diventa infine l'unico metodo di autenticazione supportato e le organizzazioni devono eseguire la migrazione prima della scadenza del metodo legacy per evitare interruzioni del servizio e potenziali errori di sincronizzazione di AD/VA che potrebbero richiedere la reinstallazione completa per il ripristino.

Contenuto correlato

- Documentazione sull'autenticazione API Cisco Secure Access
- Configurazione avanzata di Cisco Secure Access
- Gestione della configurazione di Cisco Secure Access
- 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).