

ISE 3.5 EntraID External Groups: query sui problemi di prestazioni e risoluzione delle autorizzazioni dell'API Microsoft Graph

Sommario

Problema

Patch2 di Cisco ISE 3.5 con configurazione EntraID REST ID Store: ritardi significativi nell'autenticazione EAP-TLS durante l'esecuzione di query su EntraID.ExternalGroups. Il completamento della fase PIP - EntraID.ExternalGroups interrogata richiede più di 30 secondi, determinando il timeout dei client EAP e il riavvio dell'autenticazione, che impedisce il completamento corretto della sessione.

Inoltre, quando si tenta di salvare gli attributi del gruppo nella configurazione EntraID REST ID Store, viene visualizzato questo messaggio di errore:

```
java.rmi.RemoteException: null; nested exception is: java.lang.NullPointerException
```

I registri di autenticazione mostrano gli errori PIP asincroni e la sospensione del motore dei criteri durante il processo di ricerca dei gruppi esterni. Il problema si manifesta come flussi di lavoro di autenticazione non riusciti in cui i client non possono completare le sessioni EAP a causa dei tempi estesi delle query.

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.5.0.527 con patch 2
- Integrazione di Microsoft EntraID (Azure Active Directory) tramite l'archivio di ID REST
- autenticazione EAP-TLS configurata

- Origine REST configurata per EntraID con recupero attributo gruppo
- Problema osservato in ISE 3.4 patch4/patch5 e ISE 3.5 patch2/patch3

Risoluzione

La risoluzione implica la concessione delle autorizzazioni API di Microsoft Graph corrette all'applicazione Azure utilizzata dall'integrazione dell'archivio di ID REST di EntraID ISE.

Passaggio 1: Concedi autorizzazioni API di Microsoft Graph obbligatorie

Passare al portale di Azure e individuare la registrazione dell'applicazione utilizzata per l'integrazione ISE. Concedi questa autorizzazione API di tipo applicazione:

`Directory.Read.All`

Accertarsi che il consenso dell'amministratore sia concesso per questa autorizzazione.

Passaggio 2: Riavviare i servizi ISE

Dopo aver concesso l'autorizzazione `Directory.Read.All`, riavviare i servizi su tutti i nodi ISE per rendere effettive le nuove autorizzazioni.

Passaggio 3: Verifica risoluzione

Eseguire il test del processo di autenticazione per verificare che la fase PIP - `EntraID.ExternalGroups` sottoposta a query venga completata entro intervalli di tempo accettabili e che gli attributi Group possano essere salvati senza errori.

I registri di risoluzione devono essere completati senza `AsynchronousPIPErrors`:

Causa

Il problema è causato dall'ID bug Cisco CSCwu13703, che influisce sulla patch 3 di ISE 3.5 e sulle versioni correlate. Il bug è dovuto alle autorizzazioni API di Microsoft Graph insufficienti per l'integrazione di EntraID. Senza l'autorizzazione Directory.Read.All appropriata, ISE non è in grado di eseguire query efficienti sui gruppi esterni da EntraID, determinando condizioni di timeout e sospensione del motore dei criteri tramite eccezioni AsynchronousPIPEError.

Il processo di autenticazione ha esito negativo perché ogni valutazione non riuscita provoca l'esecuzione di AsynchronousPIPEError da parte del motore dei criteri e la sospensione del flusso di lavoro di autenticazione, con conseguente aumento dei tempi di query ed eventuale timeout del client.

Contenuto correlato

- [ID bug Cisco CSCwu13703](#)
- [Guida alla configurazione di Cisco ISE con Microsoft Active Directory Entra ID e Intune](#)

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).