

Autenticazione RAVPN di Secure Access non riuscita con l'integrazione SAML Duo

Sommario

Problema

Quando si tenta di connettersi a Cisco Secure Access Remote Access VPN (RAVPN) utilizzando Duo come provider di identità (IDP) con integrazione Active Directory in background, gli utenti riscontrano errori di autenticazione nonostante l'autenticazione riuscita a livello di portale Duo.

I sintomi specifici includono:

- Duo Portal visualizza un messaggio di riuscita per l'autenticazione.
- Cisco SecureClient visualizza un messaggio di errore "Autenticazione non riuscita" subito dopo il completamento di Duo.
- I log Duo mostrano lo stato "accesso concesso".
- I log del portale Cisco Secure Access mostrano lo stato "errore AAA".

In questo modo viene creata una disconnessione in cui il provider di identità esterno conferma la riuscita dell'autenticazione, ma il client VPN non è in grado di stabilire la connessione a causa di errori di convalida dell'autenticazione nell'infrastruttura di accesso sicuro.

Ambiente

- Implementazione di Cisco Secure Access VPN
- Duo Security come provider di identità SAML
- Integrazione di Active Directory con Duo
- Cisco Secure Client per connettività VPN

- Flusso di autenticazione basata su SAML

Risoluzione

L'errore di autenticazione è stato risolto correggendo il mapping degli attributi utente tra Duo e Cisco Secure Access. Le misure descritte nelle sezioni successive sono state adottate per identificare e risolvere il problema.

Passaggio 1: Verifica ricerca attività

- 1.- Accedere a Cisco Secure Access Dashboard. Fare clic su Monitor > Log Accesso remoto.
- 2.- Controllare il campo username sotto i messaggi di errore del controllo autorizzazione.
- 3.- Confrontarlo con il valore UPN in Connect > User and Groups (Connetti > Utente e gruppi).

Cisco Secure Access analizza il valore del nome dell'entità utente per verificare l'autorizzazione.

Il nome dell'entità utente passato da Duo non corrisponde al valore del nome dell'entità utente per tale utente in User and Groups.

Dall'inchiesta è emerso che:

- Indirizzo e-mail utente: user@gmail.com
- Nome entità utente (UPN nomeutente)

Passaggio 2: Duo Configuration Adjustment

La risoluzione ha comportato la modifica della configurazione SAML Duo per garantire la corretta mappatura degli attributi utente:

- Accedere al Pannello Duo Admin.

- Passare alla configurazione dell'applicazione SAML per Cisco Secure Access.
- Modificare il mapping degli attributi utente per inviare l'indirizzo di posta elettronica che deve corrispondere al valore del nome dell'entità utente per l'utente in Utenti e gruppi.
- Salvare le modifiche alla configurazione.

Passaggio 4: Verifica

Dopo aver regolato la configurazione Duo, il flusso di autenticazione è stato testato e verificato correttamente. L'utente è riuscito a connettersi utilizzando la VPN di accesso remoto senza errori di autenticazione.

Causa

La causa principale dell'errore di autenticazione è stata una mancata corrispondenza del mapping degli attributi utente tra le asserzioni SAML Duo e le aspettative di Cisco Secure Access. Duo è stato configurato per l'invio del nome utente in User Principal Name (UPN) nelle asserzioni SAML, mentre Cisco Secure Access è stato configurato in modo da prevedere l'indirizzo di posta elettronica dell'utente. Questa mancata corrispondenza ha causato il mancato completamento dell'autenticazione al livello Secure Access nonostante l'autenticazione a livello Duo IDP abbia avuto esito positivo, con un conseguente "errore AAA" durante l'accesso protetto, mentre nei log Duo è stato visualizzato "accesso concesso".

Contenuto correlato

- [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).