Errori di registrazione ZTNA per utenti guest con account Google personali in Cisco Secure Access

Sommario

Problema

Durante la distribuzione di Private Access con ZTNA (Zero Trust Network Access), la registrazione di un utente guest con un account Google personale non riesce dopo la corretta registrazione in Entra ID e il provisioning in Secure Access. I sintomi specifici riscontrati includono:

- Iscrizione basata sul client: Il processo di registrazione raggiunge l'autenticazione SSO, vengono fornite le credenziali, ma ZTNA visualizza un "errore di I/O" e il processo di registrazione si blocca
- Accesso senza client: Restituisce il messaggio di errore "Cisco Secure Access Login failure". Verifica configurazione IDP" insieme a un ID transazione

Questi errori impediscono l'accesso a risorse private e influiscono sui test delle funzionalità ZTNA per l'accesso di tipo collaboratore esterno utilizzando identità non aziendali.

Ambiente

- Implementazione di Cisco Secure Access con ZTNA
- ID Entra Microsoft (in precedenza Azure AD) come provider di identità
- Account Google personale (@gmail.com) registrato come utente guest in Entra ID
- Account Guest attivato e visibile in Accesso protetto
- Autenticazione SAML configurata tra Entra ID e Cisco Secure Access

Risoluzione

L'errore di registrazione è stato risolto modificando la configurazione del mapping degli attributi SAML in Microsoft Entra ID. Per risolvere il problema sono state adottate le seguenti misure:

Passaggio 1: Analisi del bundle DART e del comportamento del client

Esaminare il bundle DART per verificare che i componenti Cisco Secure Client e ZTA funzionino correttamente. L'analisi deve verificare che il flusso di registrazione raggiunga correttamente Cisco Secure Access e che l'errore si verifichi durante l'autenticazione SAML con il provider di identità.

Passaggio 2: Esamina registri di autenticazione Entra ID

Controllare i registri di autenticazione Entra ID per verificare che il processo di autenticazione sia stato completato correttamente dal punto di vista del provider di identità. L'autenticazione dei log dovrebbe essere corretta, ma Secure Access rifiuta l'accesso a causa di una mancata corrispondenza degli attributi.

Passaggio 3: Identifica problema di mapping attributi SAML

Determinare che Entra ID sta emettendo l'UPN (User Principal Name) come attestazione SAML, che non corrisponde all'identità dell'account Gmail personale prevista da Secure Access. L'attributo IdP dichiarato non corrisponde all'identificatore utente previsto.

Passaggio 4: Modifica mapping attributi SAML

Modificare il mapping degli attributi SAML in Microsoft Entra ID da UPN a Indirizzo e-mail. In questo modo l'attestazione basata sull'indirizzo di posta elettronica corrisponde all'identità dell'account Google personale.

Passaggio 5: Verifica registrazione riuscita

Dopo aver implementato la modifica del mapping degli attributi, riprovare il processo di registrazione ZTNA. A questo punto, Cisco Secure Access ZTA dovrebbe riconoscere l'indirizzo Gmail e consentire il completamento della registrazione.

Causa

L'errore di registrazione è stato causato da una mancata corrispondenza tra l'attributo SAML dichiarato da Microsoft Entra ID e l'identificatore utente previsto in Cisco Secure Access. L'ID di accesso è stato configurato per inviare l'UPN (User Principal Name) come attestazione SAML, ma per gli account Google personali (@gmail.com) questo UPN non corrisponde all'identità dell'indirizzo e-mail effettivo. Cisco Secure Access prevede di ricevere l'indirizzo di posta elettronica come attributo di identificazione da abbinare all'account utente guest di cui è stato eseguito il provisioning, con conseguente rifiuto dell'autenticazione nonostante la riuscita dell'autenticazione IdP.

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).