Errori di autenticazione controllo postura controllo certificato di accesso sicuro

Sommario

Problema

Quando si tenta di distribuire Secure Access con il profilo di postura dell'endpoint utilizzando la funzionalità di ispezione dei certificati, tutti i tentativi di accesso hanno esito negativo nonostante non sia possibile identificare le cause specifiche dell'errore nei log del bundle DART. Gli utenti stanno tentando di utilizzare l'autenticazione IDP SAML e allo stesso tempo desiderano applicare la convalida dei certificati tramite il meccanismo di verifica della postura, ma questa configurazione genera errori di autenticazione coerenti anche quando le corrispondenze dei certificati back-end hanno esito positivo.

Ambiente

- Cisco Secure Access - Accesso remoto sicuro del client (VPN, postura, risorsa privata)
- Integrazione autenticazione IDP SAML
- Profilo postura endpoint con funzionalità di ispezione dei certificati abilitata
- Certificati utente con campo UPN nella rete SAN corrispondente a indirizzi e-mail
- Configurazione del tenant Secure Access con utenti, gruppi e dispositivi endpoint

Risoluzione

Le verifiche dell'endpoint del certificato nella postura vengono applicate solo quando si utilizza l'autenticazione con più certificati, che richiede sia la convalida del certificato utente che quella del certificato del computer. Poiché lo scenario di distribuzione coinvolge utenti con solo certificati utente che devono utilizzare un singolo profilo VPN, la soluzione prevede l'implementazione

dell'autenticazione SAML + singolo certificato invece di affidarsi alla verifica del certificato di postura.

Procedura di configurazione dell'autenticazione

Passaggio 1: Configurazione di SAML + Autenticazione con certificato singolo

Configurare il metodo di autenticazione in modo che utilizzi l'autenticazione SAML combinata con l'autenticazione a certificato singolo anziché tentare di applicare la convalida del certificato tramite controlli della postura.

Passaggio 2: Configura corrispondenza UPN certificato

Verificare che il campo UPN nella SAN (Subject Alternative Name) del certificato contenga l'indirizzo di posta elettronica dell'utente corrispondente alla proprietà auth configurata per l'utente in Accesso sicuro in Utenti, Gruppi e Dispositivi endpoint.

Passaggio 3: Imposta campo autenticazione primaria

Configurare il campo primario per l'autenticazione utilizzando l'UPN del certificato, verificando che corrisponda all'indirizzo di posta elettronica dell'utente nel database utenti di Secure Access.

Requisiti della struttura del certificato

La struttura del certificato deve essere configurata in modo che il valore UPN o secondario nel certificato corrisponda alla proprietà auth per l'utente in Accesso sicuro. Se un utente presenta un certificato con un valore UPN o secondario che non corrisponde alla proprietà di autenticazione configurata per l'utente in Accesso sicuro, l'autenticazione verrà rifiutata.

Note importanti sulla configurazione

L'autenticazione con più certificati (IDP SAML + Multi-Cert Auth) è necessaria se è richiesta l'imposizione del controllo dei certificati di postura, ma sono richiesti sia i certificati utente che i certificati del computer. Per le distribuzioni in cui gli utenti dispongono solo di certificati utente e

devono utilizzare un singolo profilo VPN, SAML + Single Certificate Authentication offre la soluzione appropriata mantenendo al contempo i controlli di sicurezza basati sui certificati.

Causa

Le verifiche dell'endpoint del certificato nella postura vengono applicate solo quando è configurata l'autenticazione con più certificati. Quando si utilizza l'autenticazione SAML con il controllo del certificato di postura, il sistema richiede la presenza di certificati utente e computer per la convalida. Poiché la distribuzione utilizza solo certificati utente con autenticazione SAML, i tentativi di autenticazione non sono riusciti nonostante la corrispondenza del certificato back-end, poiché il meccanismo di postura non è stato progettato per funzionare con scenari di autenticazione a certificato singolo.

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).