

Risoluzione dell'errore di accesso utente

“Autenticazione utente su Active Directory non riuscita perché l'account utente è bloccato”

Sommario

[Problema](#)

[Ambiente](#)

[Risoluzione](#)

[Causa](#)

[Contenuto correlato](#)

- [Problema](#)
 - [Ambiente](#)
 - [Risoluzione](#)
 - [Causa](#)
 - [Contenuto correlato](#)
-

Problema

Active Directory genera questo errore quando un utente supera la soglia di blocco dell'account di Active Directory in Windows Server immettendo più volte una password non corretta:

“24408 User authentication against Active Directory failed since user has entered the wrong password”

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.2.0 e successive
- Integrazione di Active Directory per l'autenticazione degli utenti
- Ambienti di autenticazione sia cablati che wireless

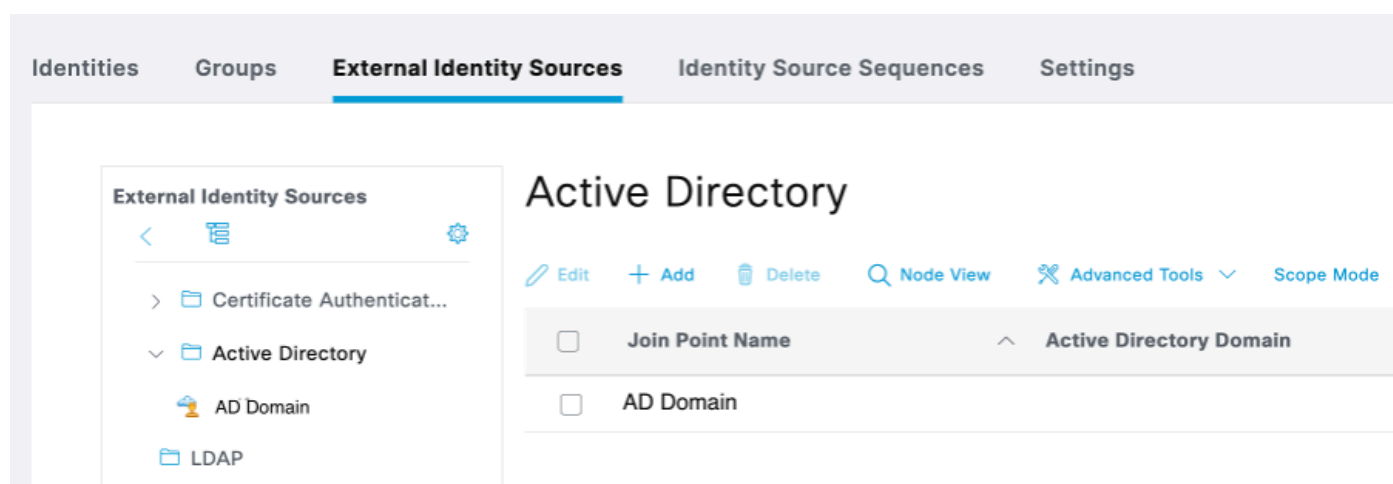
- Autenticazione basata su RADIUS con dispositivi di accesso alla rete (NAD)

Risoluzione

Passaggio 1: Abilitare la funzione "Impedisci blocco utente Active Directory" nella distribuzione ISE:

Questa funzionalità interrompe l'invio delle autenticazioni utente ad Active Directory per impedire il blocco dell'account utente configurando il numero massimo di tentativi di password non validi consentiti e confrontando questo limite con il numero di password non valide correnti (attributo badPwdCount) in Active Directory prima di inviare una richiesta di autenticazione.

1. Accedere all'interfaccia grafica di ISE.
2. Passare a Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory. Selezionare il dominio AD per abilitare la funzionalità.



3. Vai alla scheda Impostazioni avanzate.

* Join Point Name

AD Domain



4. Nella sezione Impedisci blocco utente Active Directory, selezionare la casella Abilita protezione autenticazione non riuscita.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum attempts

☒ Wireless

☒ Wired

5. Inserire il numero massimo di tentativi di password non validi consentiti.

- Questo numero deve essere inferiore al numero massimo di tentativi di password non valide configurato come valore dell'attributo badPwdCount in Active Directory.
- Assicurarsi di selezionare la casella di controllo Cablato o Wireless o Entrambi in base al tipo di connessione di autenticazione.

6. Fare clic su Salva.



Nota: ISE continuerà a rifiutare le richieste di autenticazione degli utenti finché l'attributo badPwdCount di Active Directory non verrà reimpostato su zero.

Causa

Ciò può avvenire per i seguenti motivi:

- L'utente immette una password non corretta durante l'autenticazione sull'endpoint.
- L'utente modifica le credenziali di Active Directory e non aggiorna le credenziali di Active Directory nell'endpoint wireless che esegue l'autenticazione EAP-PEAP.

Contenuto correlato

- [Configura numero massimo tentativi di password per l'account di Active Directory](#)

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).