

Il login alla GUI di amministrazione ISE non riesce con il token RADIUS di federazione PingID

Sommario

Problema

L'accesso con interfaccia utente grafica (GUI) dell'amministratore a Cisco ISE non riesce quando si usa la federazione PingID come token RADIUS, nonostante le acquisizioni di pacchetti mostrino che la federazione Ping restituisce una risposta Access-Accept. L'errore di accesso si verifica anche se l'autenticazione RADIUS risulta riuscita dal punto di vista della rete, impedendo l'accesso amministrativo all'interfaccia ISE. L'analisi dei pacchetti di rete conferma che il server PingID (10.32.154.200) invia la risposta Access-Accept prevista a ISE (10.2.200.241), ma il processo di accesso dell'amministratore ISE non riesce comunque a completarsi.

Ambiente

- Patch 7 per Cisco Identity Services Engine (ISE) versione 3.3
- Installazione di VM a 4 nodi
- Federazione PingID configurata come autenticazione token RADIUS
- Indirizzo IP ISE: 10.2.200.241
- Indirizzo IP server PingID: 10.32.154.200
- La configurazione di Accesso amministratore è stata esaminata in Amministrazione > Accesso amministratore

Risoluzione

Il problema è stato risolto con l'applicazione di una soluzione che abilitava la funzionalità di accesso degli amministratori. Per risolvere il problema, procedere come descritto nelle sezioni seguenti.

Passaggio 1: Raccolta e analisi delle prove

Le prove di acquisizione dei pacchetti sono state raccolte e analizzate per confermare il flusso di autenticazione RADIUS tra ISE e il server PingID. L'analisi ha verificato che Ping Federate stava inviando correttamente le risposte di accettazione dell'accesso.

Passaggio 2: Evidenza da prrt-server.log

###

port-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

Passaggio 3: Che cos'è l'autenticatore del messaggio?

Message-Authenticator è un attributo di sicurezza utilizzato nei pacchetti RADIUS per garantire l'integrità e l'autenticità dei messaggi scambiati tra i dispositivi di rete e il server RADIUS. È una firma crittografica calcolata utilizzando HMAC-MD5 sull'intero pacchetto RADIUS con una chiave segreta condivisa. Questo attributo consente di proteggere i messaggi RADIUS da manomissioni e spoofing, in particolare quelli che riguardano i flussi di autenticazione EAP (Extensible Authentication Protocol).

Passaggio 4: Implementazione soluzione alternativa

Disabilitare "Autenticatore messaggi richiesto in risposta": Amministrazione / Gestione delle identità / Origini identità esterne / Token RADIUS. Fare clic sul nome del token RADIUS, quindi andare su Autenticazione. Deselezionare "Message Authenticator Required On Response".

Passaggio 5: Test di convalida

Dopo aver applicato la soluzione alternativa, sono stati eseguiti i test di accesso dell'amministratore per convalidare la risoluzione. Questi test hanno confermato la riuscita dell'autenticazione e l'accesso all'interfaccia grafica di amministrazione di ISE usando la federazione PingID come token RADIUS.

Passaggio 6: Periodo di monitoraggio

È stato stabilito un periodo di monitoraggio e convalida per garantire la stabilità della soluzione alternativa. Durante questo periodo, sono stati eseguiti test continui di accesso dell'amministratore senza errori o errori.

Causa

L'errore di accesso alla GUI di ISE Admin è stato causato da una mancata corrispondenza dell'applicazione della sicurezza del protocollo RADIUS tra Cisco ISE 3.3 Patch 7 e PingID (federazione Ping) durante l'autenticazione MFA.

In particolare:

- Cisco ISE richiede che l'attributo Message-Authenticator di RADIUS sia presente nella risposta Access-Accept dal server token RADIUS esterno.
- PingID restituiva risposte Access-Accept senza l'attributo Message-Authenticator.
- Poiché ISE ha abilitato l'impostazione Message Authenticator Required On Response, la risposta RADIUS è stata rifiutata automaticamente come non valida, anche se

l'autenticazione è riuscita sul lato PingID.

- Questa imposizione fa parte della protezione avanzata di Cisco ISE per mitigare la vulnerabilità Blast-RADIUS (CVE-2024-3596).

Contenuto correlato

- [Riduzione dello spoofing del protocollo Blast-RADIUS \(CVE-2024-3596\)](#)

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).