Risoluzione dei problemi di autenticazione Kerberos in SWA

Sommario

- Introduzione
- Terminologia
- Prerequisiti
  - Requisiti
  - Componenti usati
- Flusso di rete Kerberos
  - Flusso dell'autenticazione Kerberos in SWA
  - Qual è lo scopo di SPN?
  - Configurazione server Active Directory
- Risoluzione dei problemi
  - Risoluzione dei problemi relativi a Kerberos con comandi SPN
  - Esempi di comandi e output SPN
    - Scenario 1: SPN non trovato
    - Scenario 2: SPN trovato
  - Risoluzione dei problemi di Kerberos su SWA
  - Server non trovato nel database Kerberos
- Ulteriori informazioni e riferimenti

Introduzione

In questo documento vengono descritte le nozioni di base dell'autenticazione Kerberos e la procedura per la risoluzione dei problemi relativi a tale autenticazione in Secure Web Appliance (SWA).

Terminologia

SWA	Secure Web Appliance
CLI	Interfaccia della riga di comando
ANNUNCIO	Active Directory
CD	Controller di dominio

SPN	Nome dell'entità servizio
KDC	Centro distribuzione chiavi Kerberos
TGT	Ticket di autenticazione (Ticket Granting Ticket)
TGS	Servizio di concessione ticket
HA	Alta disponibilità
VRRP	Protocollo di ridondanza router virtuale
CARPA	Protocollo Common Address Redundancy
SPN	Nome dell'entità servizio
LDAP	Lightweight Directory Access Protocol

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione di Active Directory e Kerberos.
- Autenticazione e realm su SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Flusso di rete Kerberos

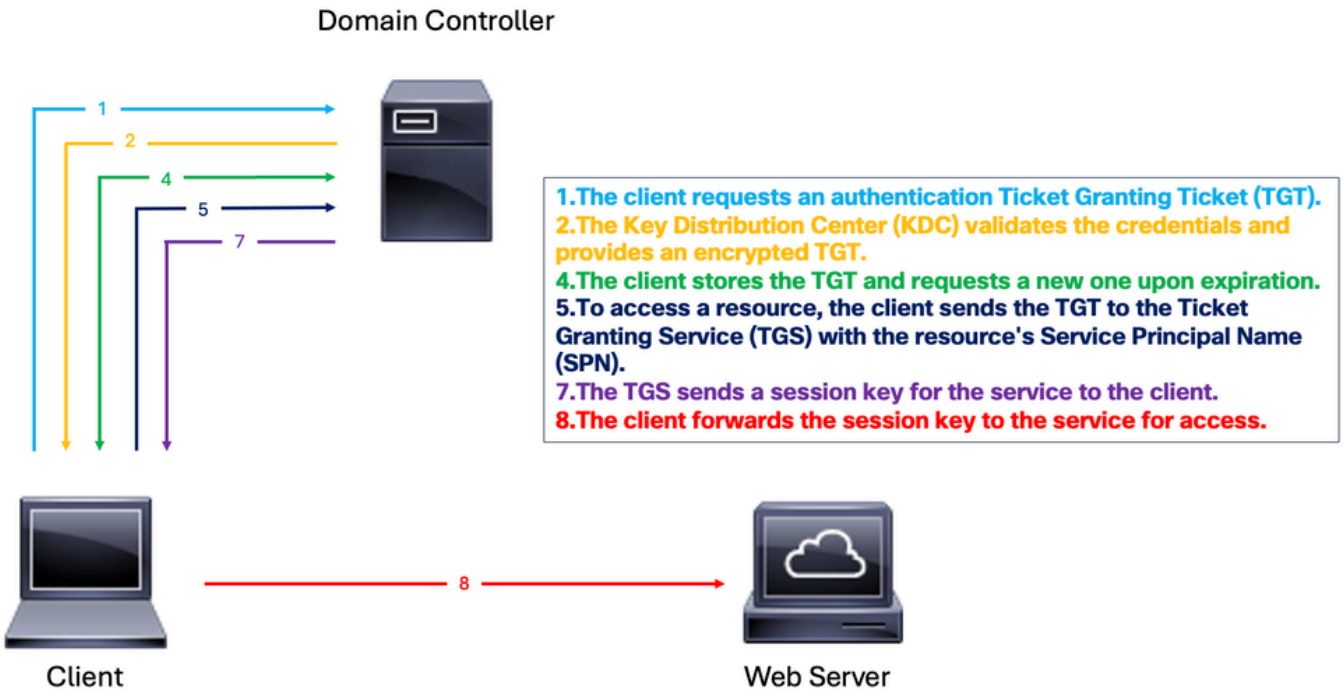


Immagine: Flusso Kerberos di esempio

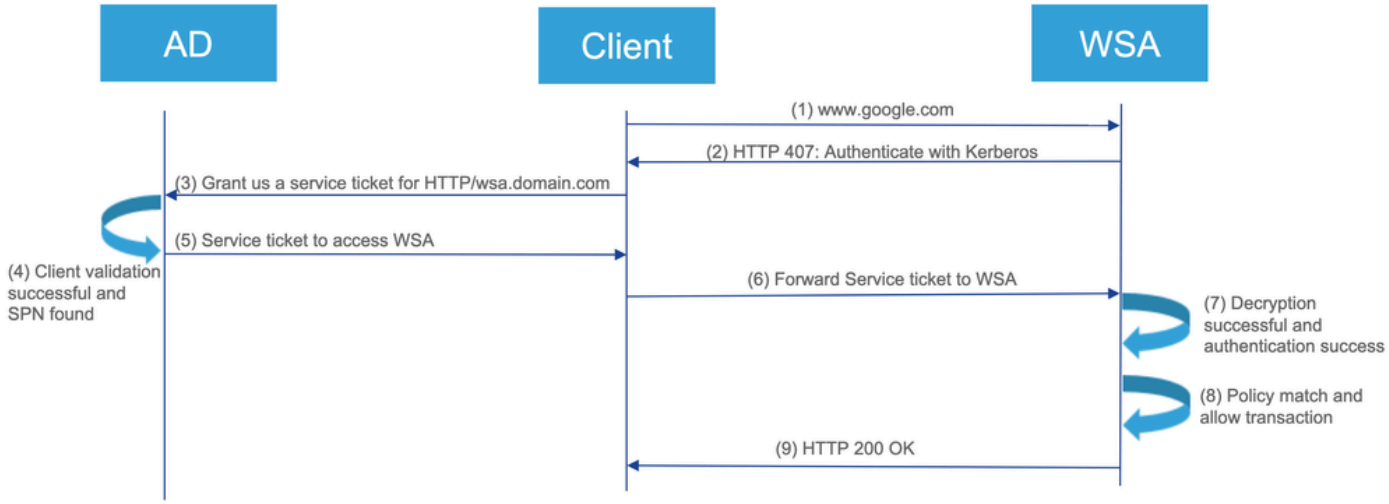
Di seguito sono riportati i passaggi di base per l'autenticazione in un ambiente kerberizzato:

1. Il client richiede un ticket di concessione ticket (TGT) dal centro distribuzione chiavi (KDC).
2. Il KDC verifica le credenziali utente del computer client e restituisce un TGT e una chiave di sessione crittografati.
3. Il TGT è crittografato con la chiave segreta TGS (Ticket Granting Service).
4. Il client memorizza il TGT e ne richiede automaticamente uno nuovo alla scadenza.

Per accedere a un servizio o a una risorsa:
1. Il client invia il TGT al TGS insieme al nome dell'entità servizio (SPN) della risorsa desiderata.
2. Il KDC verifica il TGT e controlla i diritti di accesso al computer client dell'utente.

3. Il TGS invia al client una chiave di sessione specifica del servizio.
4. Il client fornisce la chiave di sessione al servizio per provare l'accesso e il servizio concede l'accesso.

Flusso dell'autenticazione Kerberos in SWA



1. Il client richiede l'accesso a www.google.com tramite l'SWA.
2. L'SWA risponde con lo stato "HTTP 407", chiedendo l'autenticazione.
3. Il client richiede un ticket di servizio dal server AD per il servizio HTTP/SWA.domain.com utilizzando il TGT ottenuto durante l'aggiunta al dominio.
4. Il server AD convalida il client ed emette un ticket di servizio, se viene eseguito correttamente e viene trovato il nome SPN (Service Principal Name) dell'SWA, procede al passaggio successivo.
5. Il client invia questo ticket all'SWA.
6. L'SWA decrittografa il ticket e verifica l'autenticazione.
7. Se l'autenticazione ha esito positivo, l'SWA verifica i criteri.
8. L'SWA invia una risposta "HTTP 200/OK" al client se la transazione è consentita.

Qual è lo scopo di SPN?

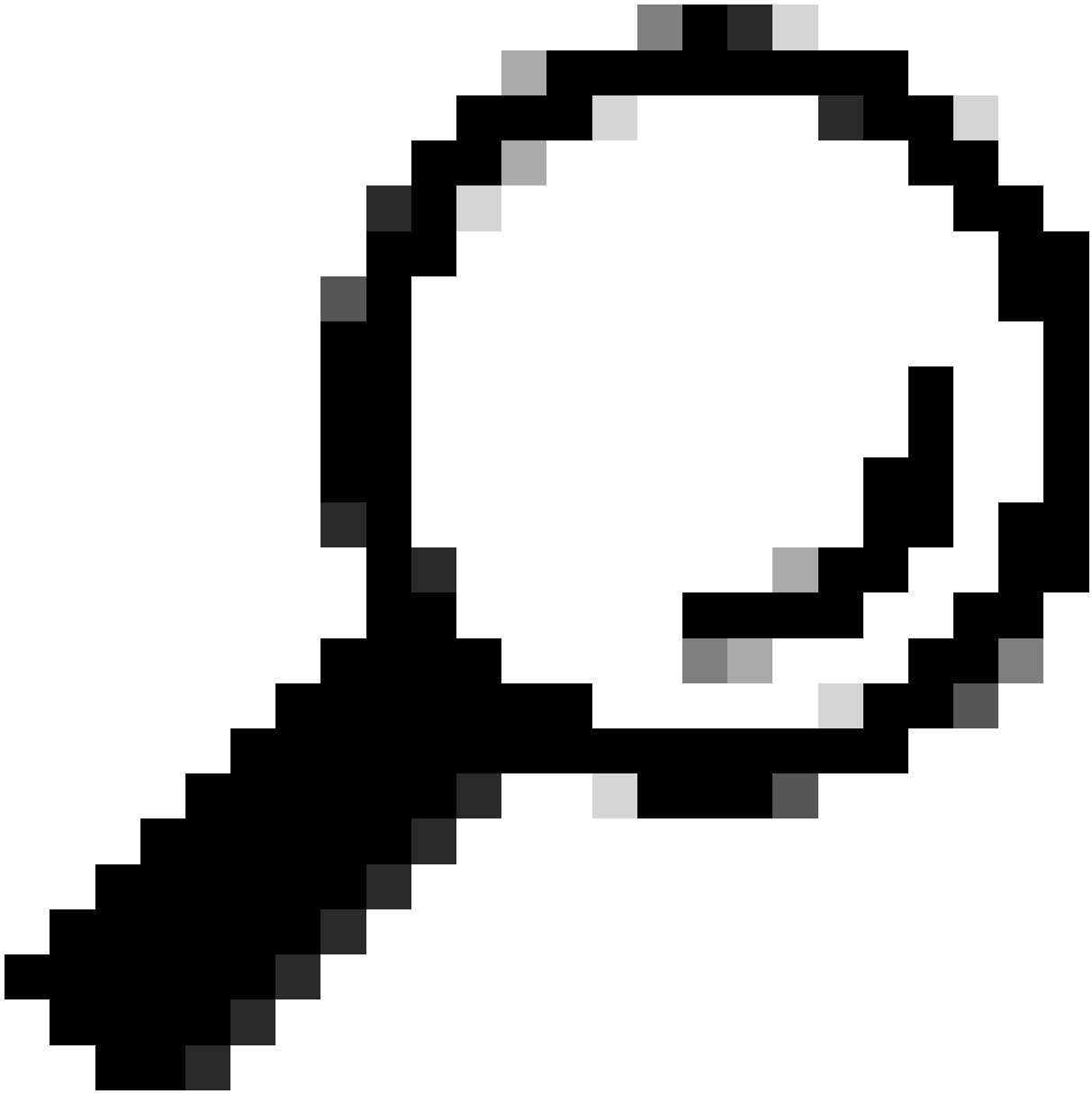
Un nome SPN (Service Principal Name) identifica in modo univoco un'istanza del servizio nell'autenticazione Kerberos. Collega un'istanza del servizio a un account del servizio, consentendo ai client di richiedere l'autenticazione per il servizio senza che sia necessario il nome dell'account. Ogni account nell'implementazione di un centro distribuzione chiavi (KDC), ad esempio AD o Open LDAP, e dispone di un SPN. Sebbene l'SPN identifichi in modo rigoroso un servizio, talvolta viene utilizzato erroneamente per fare riferimento al nome del client (UPN) in scenari in cui il servizio funge anche da client.

In Kerberos un nome SPN identifica in modo univoco un'istanza del servizio all'interno di una rete. Consente ai client di richiedere l'autenticazione per un servizio specifico. L'SPN collega l'istanza del servizio al relativo account, consentendo a Kerberos di autenticare e autorizzare correttamente le richieste di accesso a tale servizio.

Configurazione server Active Directory

1. Creare un nuovo account utente o scegliere un account utente esistente da utilizzare.

2. Registrare l'SPN da utilizzare con l'account utente scelto.
3. Verificare che non siano registrati SPN duplicati.



Suggerimento: Quali sono le differenze tra Kerberos con SWA dietro un load balancer o un Traffic Manager/Traffic Shaper? Anziché associare l'SPN per il nome host virtuale HA a un account utente, associare l'SPN per il dispositivo di reindirizzamento del traffico HTTP (ad esempio: LoadBalancer o Traffic Manager) con un account utente in Active Directory.

Le procedure ottimali per l'implementazione di Kerberos sono reperibili:

- Procedure ottimali per Secure Web Appliance
- Configurazione delle porte del firewall per le connessioni SWA

Risoluzione dei problemi

Risoluzione dei problemi relativi a Kerberos con comandi SPN

Di seguito è riportato un elenco di utili comandi setspn per la gestione dei nomi SPN (Service Principal Name) in un ambiente Kerberos. Questi comandi vengono in genere eseguiti da un'interfaccia della riga di comando con privilegi amministrativi in un ambiente Windows.

Elenca SPN per un account specifico:	setspn -L <NomeAccountUtente/Computer> Elenca tutti gli SPN registrati per l'account specificato.
Aggiungere un SPN a un account:	setspn -A <SPN> <NomeAccountUtente/Computer> Aggiunge l'SPN specificato all'account specificato.
Eliminare un SPN da un account:	setspn -D <SPN> <NomeAccountUtente/Computer> Rimuove l'SPN specificato dall'account specificato.
Verificare se un SPN è già registrato:	setspn -Q <SPN> Controlla se l'SPN specificato è già registrato nel dominio.
Elenca tutti gli SPN nel dominio	setspn -L <Account utente/computer> Elenca tutti gli SPN nel dominio.
Impostare un SPN per un account computer:	setspn -S <SPN> <NomeAccountUtente/Computer> Aggiunge un SPN a un account computer, verificando che non vi siano voci duplicate.
Reimposta SPN per un account specifico:	setspn -R <NomeAccountUtente/Computer> Reimposta gli SPN per l'account specificato, contribuendo a risolvere i problemi SPN duplicati.

Esempi di comandi e output SPN

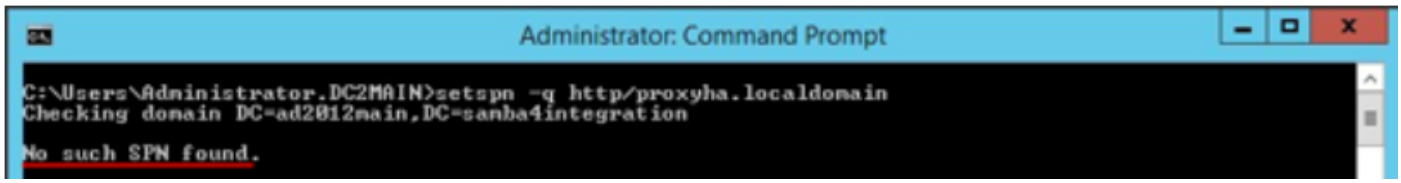
Gli esempi forniti dimostrano l'utilizzo:

- Account utente/computer: vrpserviceuser
- SPN: http/WsaHostname.com o http/proxyha.localdomain

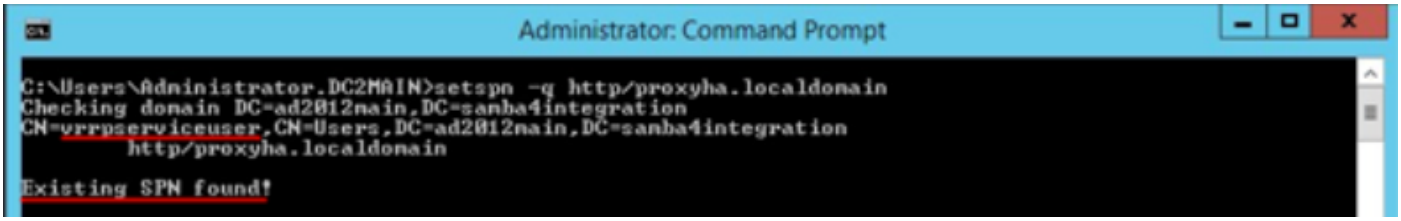
Verificare se l'SPN è già associato a un account utente:
setspn -q <SPN>

setspn -q http/proxyha.localdomain

Scenario 1: SPN non trovato



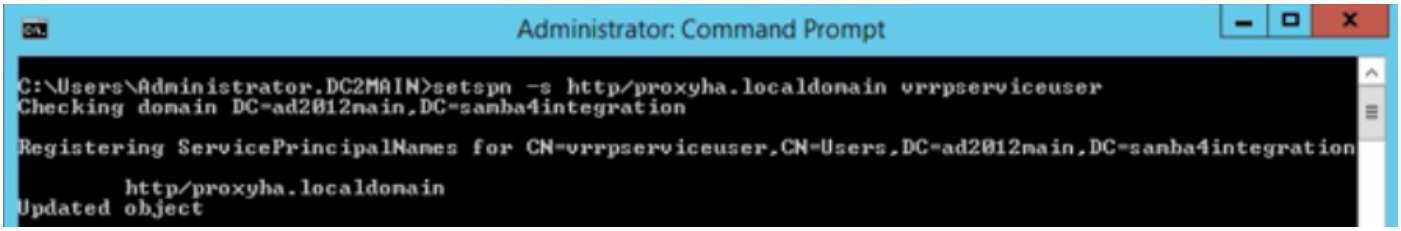
Scenario 2: SPN trovato



- Associare un SPN a un account utente/computer valido:

Sintassi: setspn -s <SPN> <Account utente/computer>

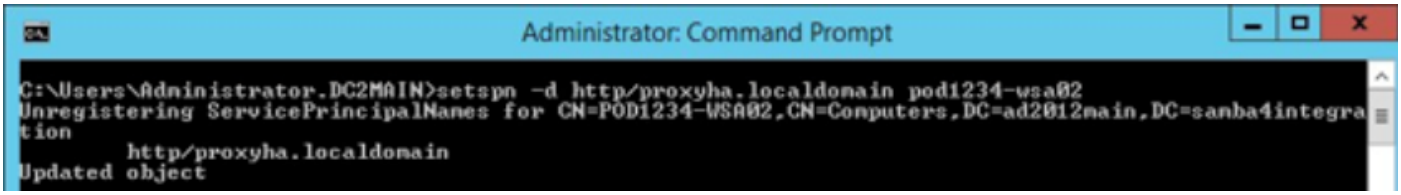
Ad esempio: setspn -s http/proxyha.localdomain utenterprrpserviceutente



- Eliminare/rimuovere un SPN già associato a un account utente o computer:

Sintassi: setspn -d <SPN> <Account utente/computer>

Ad esempio: setspn -d http/proxyha.localdomain pod1234-wsa0

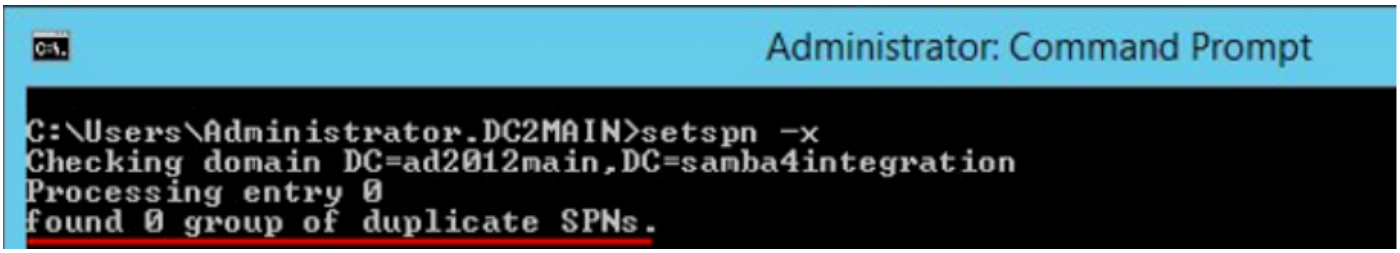


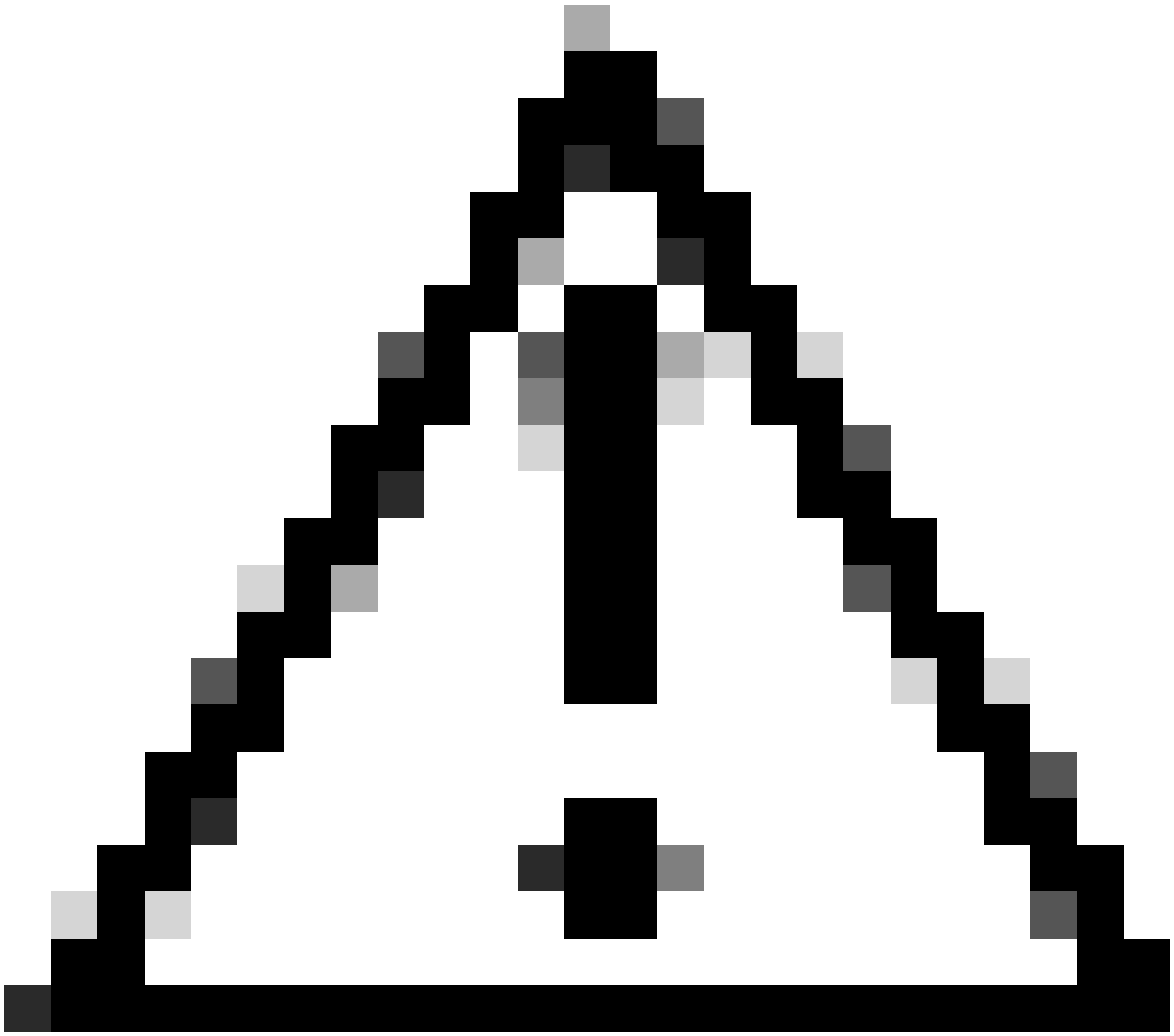
Verificare che non vi siano SPN duplicati per il nome host virtuale HA, in quanto gli errori possono

verificarsi in seguito.

- Comando da utilizzare: setspn -x

Di conseguenza, il ticket del servizio Kerberos non viene fornito al client e l'autenticazione Kerberos non riesce.



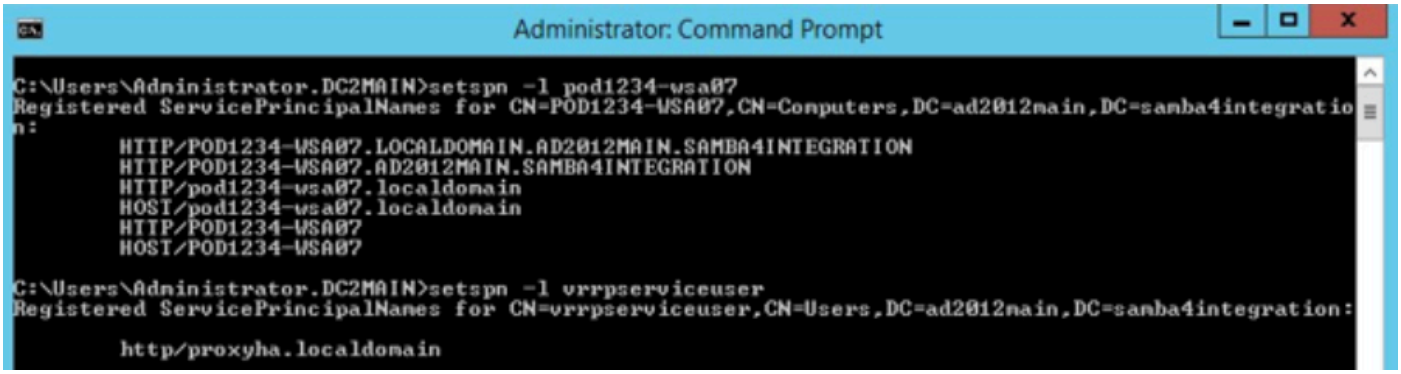


Attenzione: Se vengono rilevati duplicati, rimuoverli utilizzando il comando setspn -d.

- Elenca tutti gli SPN associati a un account:

Sintassi: setspn -l <Account utente/computer>

Ad esempio: setspn -l utenterprprserviceuser



Risoluzione dei problemi di Kerberos su SWA

Informazioni che il Supporto Cisco deve ottenere quando si risolvono i problemi di autenticazione Kerberos:

- Dettagli configurazione corrente.
- Log di autenticazione (preferibilmente in modalità debug o trace).
- Acquisizioni di pacchetti effettuate (con filtri appropriati):

  a) Dispositivo client

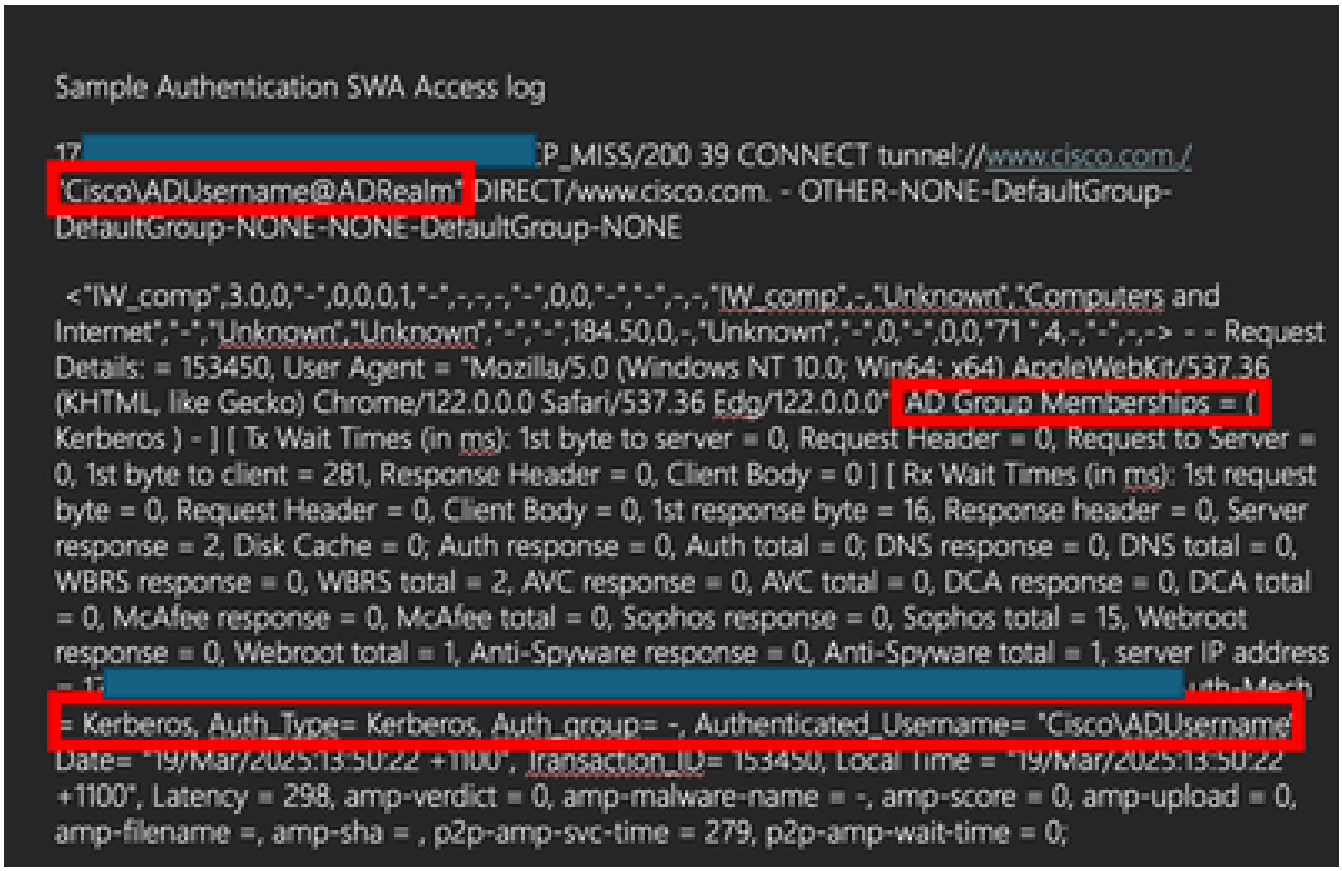
  b) SWA

- Log di accesso con identificatore di formato personalizzato %m abilitato. Deve essere indicato il meccanismo di autenticazione utilizzato per una transazione specifica.
- Per informazioni dettagliate sull'autenticazione, aggiungere questi campi personalizzati ai log degli accessi su proxy attivi/non attivi per ottenere ulteriori informazioni o fare riferimento all'aggiunta di parametri ai log degli accessi tramite collegamento ipertestuale.
- Nella GUI SWA, selezionare Amministrazione di sistema > Sottoscrizione log > Log degli accessi > Campi personalizzati > Aggiungi questa stringa per i problemi di autenticazione:

```
server IP address = %k, Client IP address= %a, Auth-Mech = %m, Auth_Type= %m, Auth_group= %g, Authentic
```

```
a;
```

- Registro degli accessi SWA per i dettagli di autenticazione utente.
- Cisco SWA registra i nomi utente autenticati nel formato Dominio\username@authentication_realm:



- Eseguire il test delle impostazioni del realm di autenticazione dalla GUI. Passare a Rete > Autenticazione, quindi fare clic sul nome del realm nella sezione Prova impostazioni correnti. Fare clic su Avvia test.

Server non trovato nel database Kerberos

Un caso di errore comune è rappresentato da richieste Web con errore "Server non trovato nel database Kerberos":

```
curl -vx proxyha.local:3128 --proxy-negotiate -u: http://www.cisco.com/
* About to connect() to proxy proxyha.localdomain port 3128 (#0)
* Connected to proxyha.local (10.8.96.30) port 3128 (#0)
< HTTP/1.1 407 Proxy Authentication Required
< Via: 1.1 pod1234-wsa02.local:80 (Cisco-SWA/10.1.2-003)
< Content-Type: text/html
gss_init_sec_context() failed: : Server not found in Kerberos database
< Proxy-Authenticate: Negotiate
< Connection: close
* HTTP/1.1 proxy connection set close!
```

In questo caso, l'errore indica che il nome dell'entità servizio corrispondente al valore dell'indirizzo proxy proxyha.local non è registrato nel server Active Directory. Per risolvere il problema, è necessario verificare che l'SPN http/proxyha.local sia registrato nel controller di dominio Active Directory e aggiunto a un account di servizio appropriato.

Ulteriori informazioni e riferimenti

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).