SWAでのKerberos認証のトラブルシューティング

内容

はじめに

このドキュメントでは、Kerberos認証の基本と、Secure Web Appliance(SWA)でのKerberos認証のトラブルシューティング手順について説明します。

用語

SWA	Cisco Secure Web Appliance
CLI を使う場合：	コマンドライン インターフェイス
[AD]	Active Directory
DC	ドメイン コントローラ

SPN	サービスプリンシパル名
KDC	Kerberosキー配布センター
TGT	認証チケット（チケット認可チケット）
TG	チケット認可サービス
HA	ハイ アベイラビリティ
VRRP	仮想ルータ冗長プロトコル
鯉	共通アドレス冗長プロトコル
SPN	サービスプリンシパル名
[LDAP]	Lightweight Directory Access Protocol

前提条件

要件

次の項目に関する知識があることが推奨されます。

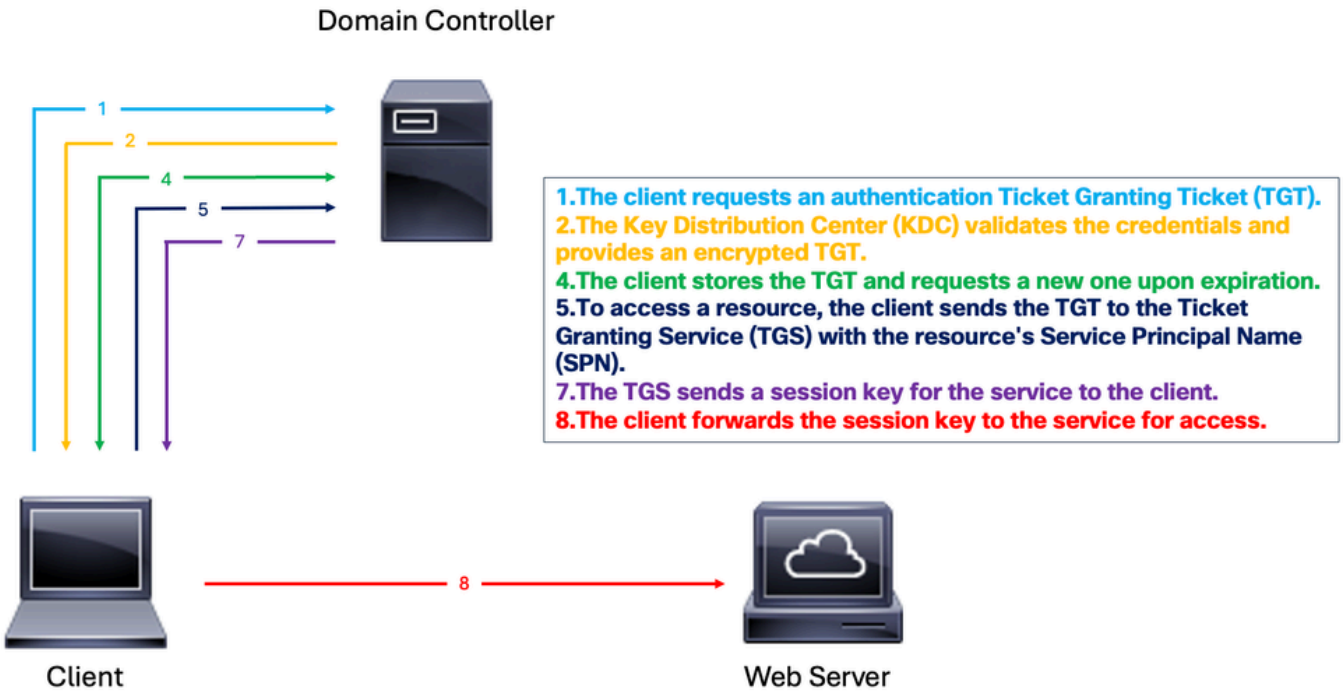
- Active DirectoryおよびKerberos認証。
- SWAの認証とレルム。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Kerberosネットワークフロー



イメージ：サンプルKerberosフロー

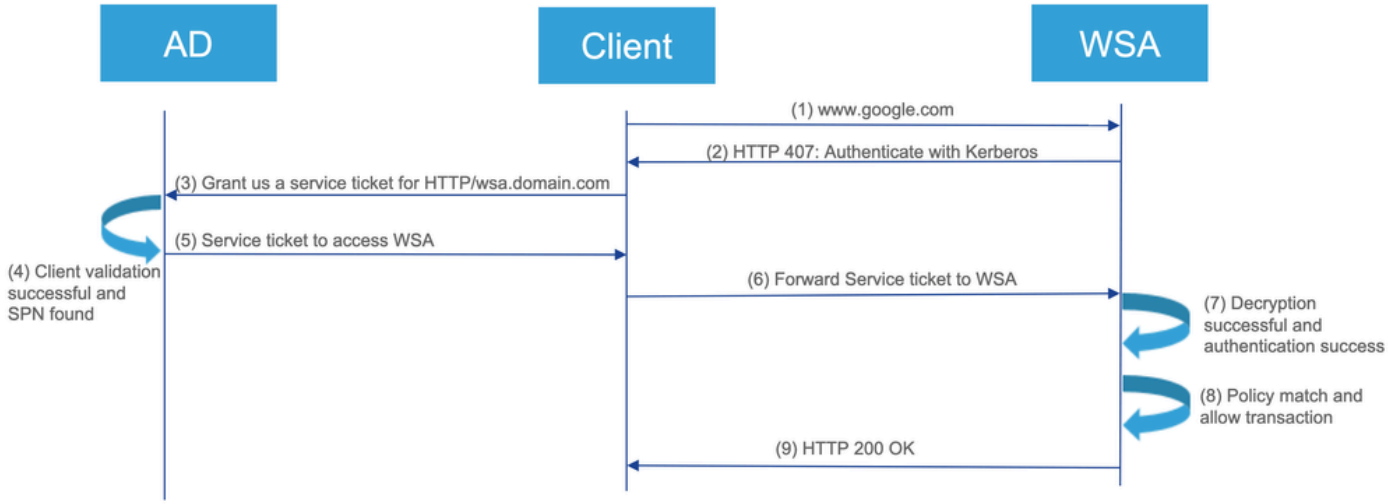
Kerberized環境での認証の基本的な手順を次に示します。

1. クライアントは、Key Distribution Center(KDC)にTicket Granting Ticket(TGT)を要求します。
2. KDCは、クライアントマシンのユーザクレデンシャルを検証し、暗号化されたTGTとセッションキーを返します。
3. TGTは、チケット認可サービス(TGS)の秘密鍵で暗号化されます。
4. クライアントはTGTを保存し、有効期限が切れると自動的に新しいTGTを要求します。

サービスまたはリソースにアクセスする場合：
1. クライアントは、目的のリソースのサービスプリンシパル名(SPN)とともにTGTをTGSに送信します。
2. KDCはTGTを検証し、ユーザークライアントマシンのアクセス権を確認します。

3. TGSはクライアントにサービス固有のセッションキーを送信します。
4. クライアントは、アクセスを証明するためにサービスにセッションキーを提供し、サービスはアクセスを許可します。

SWAでのKerberos認証のフロー



1. クライアントはSWA経由でのwww.google.comへのアクセスを要求します。
2. SWAは「HTTP 407」ステータスで応答し、認証を求めます。
3. クライアントは、ドメイン参加中に取得するTGTを使用して、HTTP/SWA.domain.comサービスのADサーバからのサービスチケットを要求します。
4. ADサーバはクライアントを検証し、サービスチケットを発行します。成功してSWAのSPN（サービスプリンシパル名）が見つかると、次のステップに進みます。
5. クライアントはこのチケットをSWAに送信します。
6. SWAはチケットを復号化し、認証を確認します。
7. 認証が成功すると、SWAによってポリシーが検証されます。
8. トランザクションが許可されると、SWAは「HTTP 200/OK」応答をクライアントに送信します。

SPNの目的は何ですか。

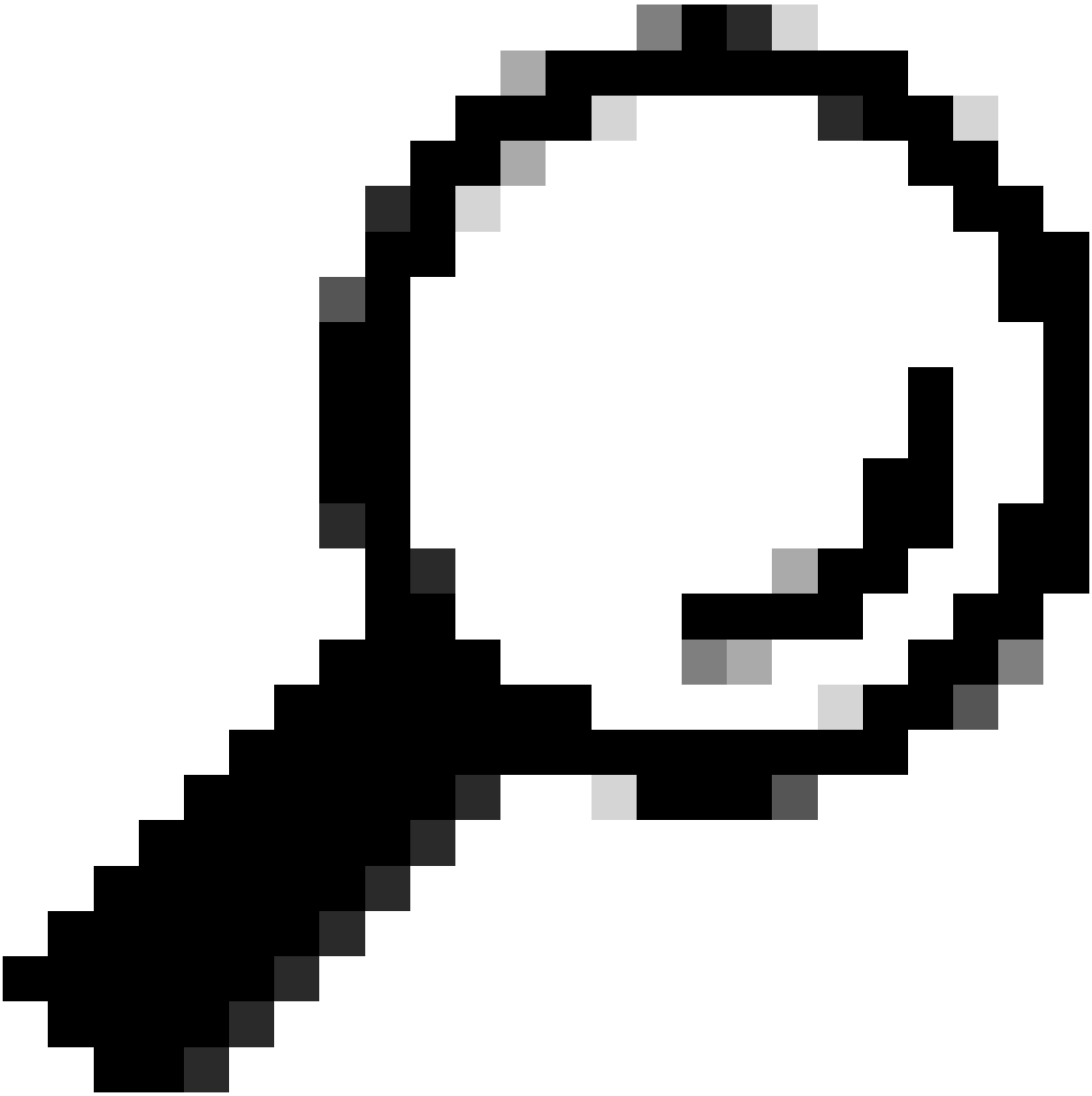
サービスプリンシパル名(SPN)は、Kerberos認証のサービスインスタンスを一意に識別します。サービスインスタンスをサービスアカウントにリンクするため、クライアントはアカウント名がなくてもサービスの認証を要求できます。ADやOpen LDAPなどのキー配布センター(KDC)実装の各アカウントには、SPNがあります。SPNはサービスを厳密に識別しますが、サービスがクライアントとしても機能するシナリオでクライアント名(UPN)を参照するために誤って使用されることがあります。

Kerberosでは、サービスプリンシパル名(SPN)によって、ネットワーク内のサービスインスタンスが一意に識別されます。クライアントが特定のサービスの認証を要求できる。SPNはサービスインスタンスをそのアカウントにリンクし、Kerberosがそのサービスへのアクセス要求を正しく認証および承認できるようにします。

Active Directoryサーバの設定

1. 新しいユーザーアカウントを作成するか、使用する既存のユーザーアカウントを選択します。

2. 選択したユーザーアカウントに対して使用するSPNを登録します。
3. 重複したSPNが登録されていないことを確認してください。



ヒント：ロードバランサまたはトラフィックマネージャ/トラフィックシェーパの背後にあるSWAを使用する場合のKerberosの相違点は何ですか。HA仮想ホスト名のSPNをユーザアカウントに関連付ける代わりに、HTTPトラフィックリダイレクトデバイス（例：LoadBalancerまたはTraffic Manager）のSPNをADのユーザアカウントに関連付けます。

Kerberosの実装に関するベストプラクティスについては、次を参照してください。

- セキュアなWebアプライアンスのベストプラクティス
- SWA接続用ファイアウォールポートの設定

トラブルシューティング

SPNコマンドを使用したKerberosのトラブルシューティング

次に、Kerberos環境でサービスプリンシパル名(SPN)を管理するのに役立つsetspnコマンドの一覧を示します。これらのコマンドは通常、Windows環境で管理者権限を持つコマンドラインインターフェイス(CLI)から実行されます。

特定のアカウントのSPNを一覧表示します：	setspn -L <ユーザー/コンピューターアカウント名> 指定したアカウントに登録されているすべてのSPNを一覧表示します。
アカウントにSPNを追加します：	setspn -A <SPN> <ユーザー/コンピューターアカウント名> 指定されたSPNを指定されたアカウントに追加します。
アカウントからSPNを削除します：	setspn -D <SPN> <ユーザー/コンピューターアカウント名> 指定されたSPNを指定されたアカウントから削除します。
SPNがすでに登録されているかどうかを確認します。	setspn -Q <SPN> 指定したSPNがドメインに既に登録されているかどうかを確認します。
ドメイン内のすべてのSPNを一覧表示します	setspn -L <ユーザー/コンピューターアカウント> ドメインのすべてのSPNを一覧表示します。
コンピューターアカウントのSPNを設定します：	setspn -S <SPN> <User/ComputerAccountName> コンピューターアカウントにSPNを追加し、重複したエントリがないようにします。
特定のアカウントのSPNをリセットします：	setspn -R <ユーザー/コンピューターのアカウント名> 指定されたアカウントのSPNをリセットし、重複するSPNの問題を解決するのに役立ちます。

SPNコマンドと出力の例

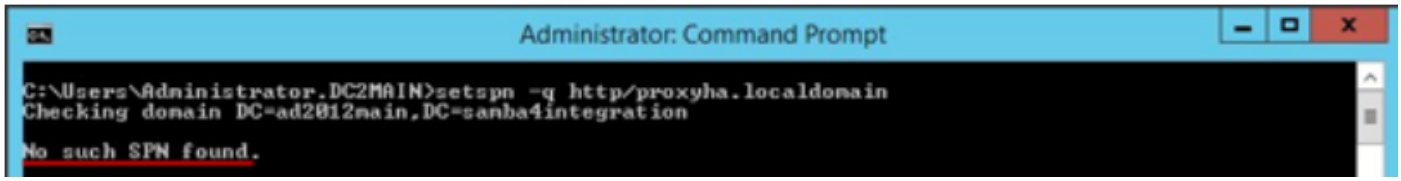
次に例を示します。

- ユーザ/コンピュータアカウント：vrrpserviceuser
- SPN:http/WsaHostname.comまたはhttp/proxyha.localdomain

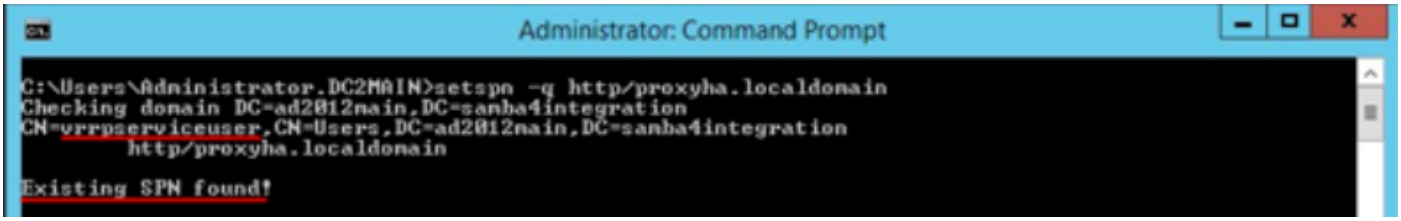
SPNが既にユーザーアカウントに関連付けられているかどうかを確認してください：
setspn -q <SPN>

setspn -q http/proxyha.localdomain

シナリオ1: SPNが見つかりません



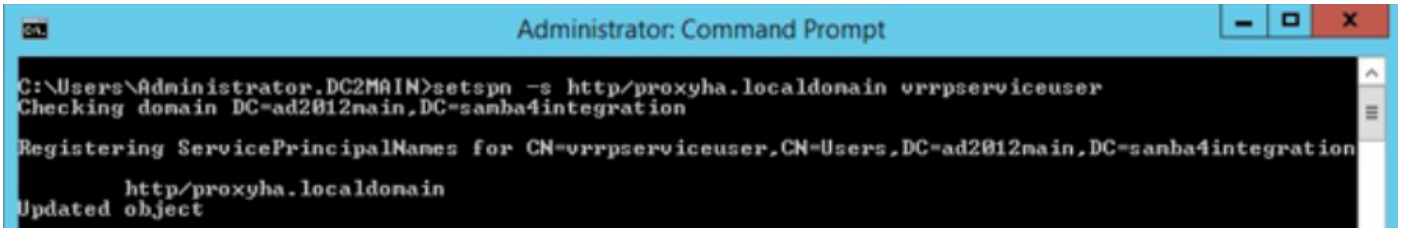
シナリオ2: SPNが見つかりました



- SPNを有効なユーザー/コンピューターアカウントに関連付けます：

構文: setspn -s <SPN> <ユーザー/コンピューターアカウント>

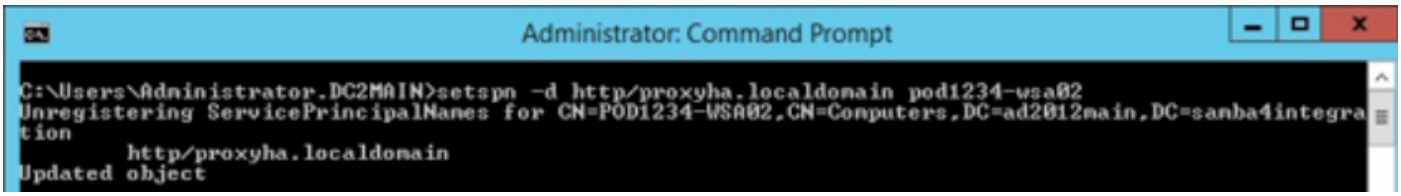
例:setspn -s http/proxyha.localdomain vrrpserviceuser



- ユーザーまたはコンピューターアカウントに既に関連付けられているSPNを削除します：

構文: setspn -d <SPN> <ユーザー/コンピューターアカウント>

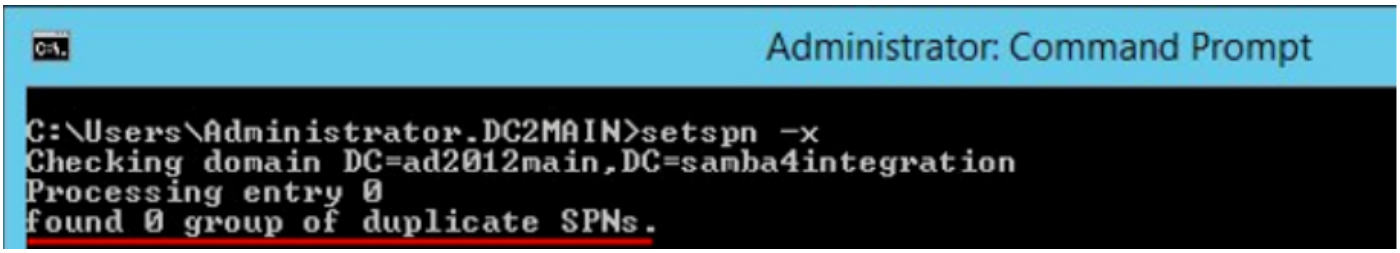
例:setspn -d http/proxyha.localdomain pod1234-wsa0

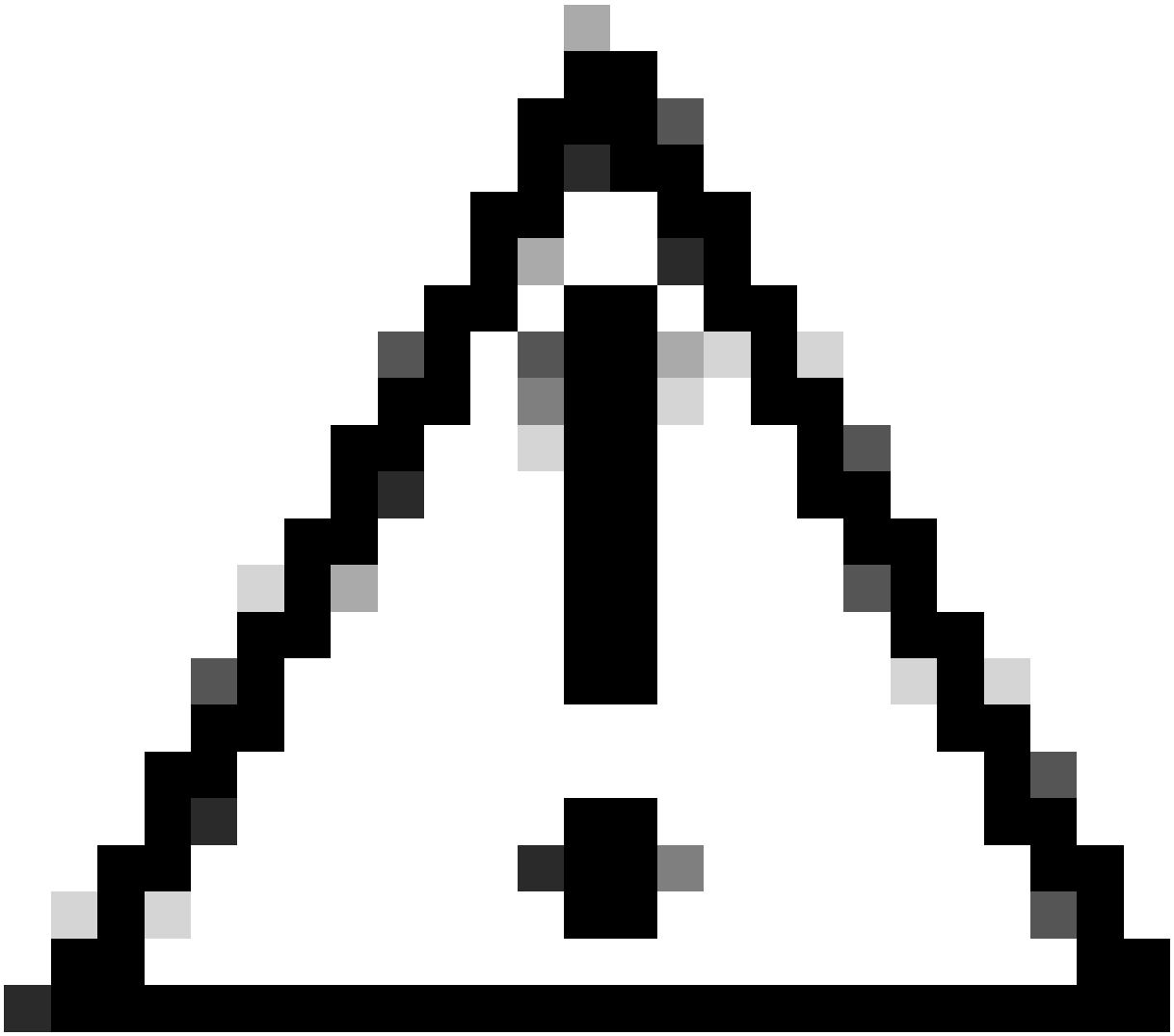


後で障害が発生する可能性があるため、HA仮想ホスト名に重複するSPNがないことを確認します。

- 使用するコマンド：setspn -x

その結果、Kerberosサービスチケットがクライアントに提供されず、Kerberos認証が失敗します。



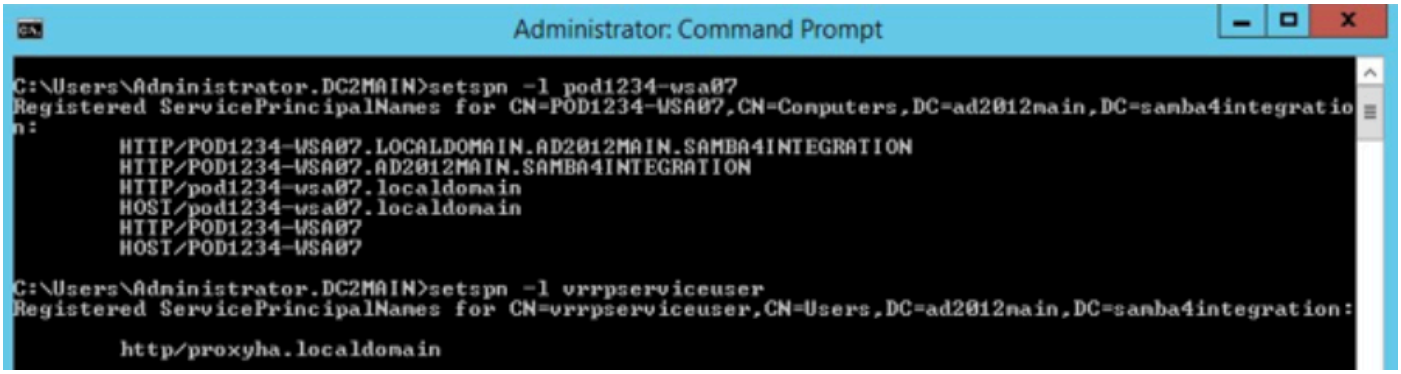


注意：重複が見つかった場合、setspn -dコマンドを使用して重複を削除してください。

- アカウントに関連付けられたすべてのSPNを一覧表示します：

構文: setspn -l <ユーザー/コンピューターアカウント>

例:setspn -l vrrpserviceuser



SWA上のKerberosのトラブルシューティング

Kerberos認証の問題をトラブルシューティングする際にシスコサポートが入手する必要がある情報：

- 現在の設定の詳細。
- 認証ログ（デバッグモードまたはトレースモードが望ましい）。
- 取得されたパケットキャプチャ（適切なフィルタを使用）：

  イクライアントデバイス

  口SWA

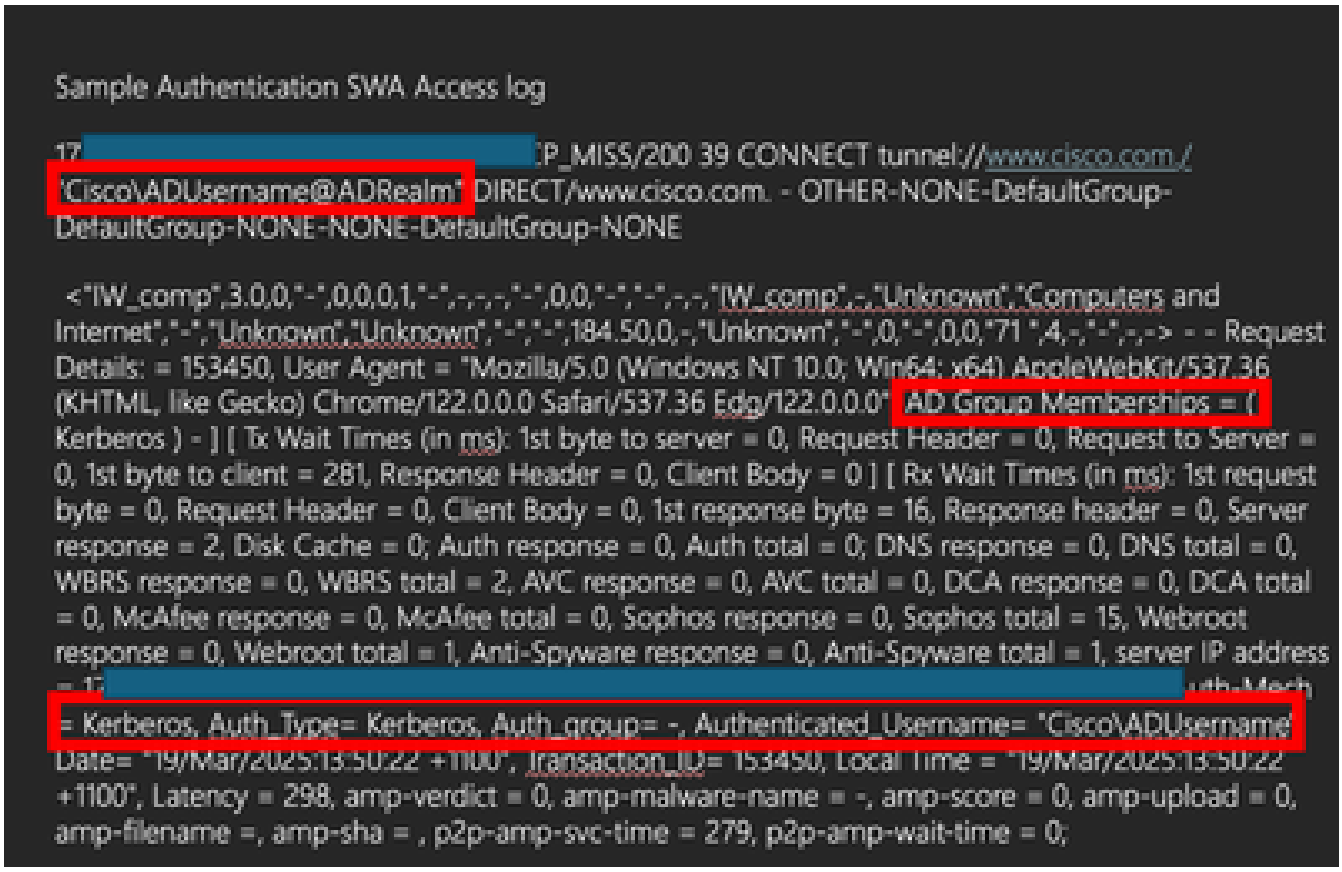
- %m個のカスタム形式指定子が有効になっているアクセスログ。これは、特定のトランザクションに使用された認証メカニズムを示す必要があります。
- 認証の詳細については、動作しているプロキシまたは動作していないプロキシのアクセスログにこれらのカスタムフィールドを追加して詳細を取得するか、「アクセスログにおけるパラメータの追加」のハイパーリンクを参照してください。
- SWA GUIで、System administration > Log subscription > Access logs > Custom fields > Add this string for authentication issuesの順に移動します。

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

```
a;
```

- ユーザ認証の詳細に関するSWAアクセスログ。

- Cisco SWAでは、認証されたユーザ名をDomain\username@authentication_realm:の形式で記録します。



- GUIからTest Authentication Realm Settingsを実行します。Network > Authenticationに移動し、Test Current Settingsセクションでレルムの名前をクリックします。Start Testをクリックします。

Kerberosデータベースにサーバが見つからない

よくあるエラーの例に、「Server not found in Kerberos database」で失敗するWeb要求があります。

```
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!
```

この場合、エラーは、プロキシアドレス値proxyha.localに対応するサービスプリンシパル名(SPN)がActive Directoryサーバに登録されていないことを示しています。この問題を解決するに

は、SPN http/proxyha.localがAD DCに登録され、適切なサービスアカウントに追加されていることを確認する必要があります。

その他の情報と参考資料

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。