NAC アプライアンス（CCA）： Active Directory Windows シングル サイン オン（SSO）の設定とトラブルシューティング

目次

概要

このドキュメントでは、Cisco Network Admission Control（NAC）アプライアンス（旧 Cisco Clean Access（CCA））の設定およびトラブルシューティングを行うために、Microsoft Windows Active Directory（AD）のシングル サインオン（SSO）を使用する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- DC で Windows 2000 SP4 または Windows 2003（Standard または Enterprise）SP1 または Windows 2003 R2 を実行していることを確認します。 SP1 をインストールしていない Windows 2003 はサポートされていません。
- Windows SSO が AD 環境でのみサポートされていることを確認します。 Windows NT 環境はサポートされていません。 Clean Access エージェントが必要です。
- 『Cisco NAC アプライアンス：Clean Access サーバ インストールおよび設定ガイド（リリース 4.1(2)）』の説明に従って、Clean Access Server（CAS）のアカウントを設定します。

使用するコンポーネント

このドキュメントの情報は、NAC アプライアンス ソフトウェア バージョン 4.x 以降に基づいています。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Windows SSO の設定

ここでの説明は、この文書で説明する機能を設定する方法について説明します。

AD SSO のプロバイダーの設定

- AD SSO プロバイダーまたは VPN SSO への認証テストを実行できません。
- LDAP ルックアップ サーバは、AD SSO 後に AD の属性に基づくロールがユーザに割り当てられるように AD SSO のルールをマッピングすることをユーザが希望する場合のみ必要です。 これは、基本 SSO を動作させるためには不要です（ロールのマッピングなし）。

DC での KTPass の実行

KTPass は、Windows 2000 および 2003 のサポート ツールの一部として使用可能なツールです。 詳細については、『Cisco NAC アプライアンス：Clean Access サーバ インストールおよび設定ガイド（リリース 4.1(2)）』を参照してください。

KTPass を実行するときは、常に「/」と「@」の間に表示されるコンピュータ名が、DC で [Control Panel] > [System] > [Computer Name] > [Full Computer Name] の下に表示される DC の名前と一致することに注意することが重要です。

強調表示されている @ の後に表示される領域名は常に大文字にあることも確認します。

```
C:\Program Files\Support Tools>ktpass -princ
 ccasso/prem-vm-2003.win2k3.local@WIN2K3.LOCAL -mapuser ccasso -pass Cisco123 -out
c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly Using legacy password setting method //confirms
ccasso acct is mapped Successfully mapped ccasso/prem-vm-2003.win2k3.local to ccasso. Key
created. Output keytab to c:\test.keytab Keytab version: 0x502 keysize 80 ccasso/prem-vm-
2003.win2k3.local@WIN2K3.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength
16 (0xf2e787d376cbf6d6dd3600132e9c215d) Account ccasso has been set for DES-only encryption.
```

Windows 7 をサポートするには、次の例に示すように KTPASS を実行する必要があります。

```
C:\Program Files\Support Tools>KTPASS.EXE -princ
newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out
c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

強調表示されている @ の後に表示される領域名は常に大文字にあることも確認します。

CAS での SSO の設定

[CCA Servers] > [Manage] > [Authentication] > [Windows Auth] > [Active Directory SSO] を選択して AD ウィンドウを開き、次の項目を確認します。

- [Active Directory Domain]： [Kerberos realm name] = 大文字にする必要があります。
- [Active Directory Server (FQDN)]： CAS が DNS を介してこの名前を解決できることを確認します。 このフィールドは、IP アドレスにはできません。 この例の値を使用してセキュアシェル（SSH）で CAS にログインでき、「nslookup prem-vm-2003.win2k3.local」を実行できます。 次に、正常に解決されることを確認します。
- FQDN が、[Control Panel] > [System] > [Computer Name] の下に表示される AD サーバ（DC）の名前と完全に一致していることを確認します | AD サーバ マシン（DC）のフル コンピュータ名。

SSO サービスが起動していることを確認する

次の手順を実行します。

1. SSO サービスが開始されていることを確認するには、[CCA Servers] > [Manage] > [Status] に移動します。
2. CAS が TCP 8910（Windows SSO に使用）をリッスンするようになったことを確認するには、次のコマンドを実行します。`[root@cs-ccas02 ~]#netstat -a | grep 8910 tcp 0 0 *:8910 *:* LISTEN`

DC へのポートの開放

DC への適切なポートを開くには、次の手順を実行します。

注: テストでは、常に DC への完全なアクセスを開きます。 その後、SSO が動作すれば、特定のポートに結びつけることができます。

1. Active Directory への次のポートが信頼できないロールで許可されていることを確認します。**TCP**： 88、135、445、389/636、1025、1026**UDP**： 88、389**注:** Windows のパスワードの再設定が正しく動作するためには、*TCP ポート 445* を開く必要があります。
2. クライアントが CCA エージェント 4.0.0.1 以降を実行していることを確認します。
3. Windows ドメインのクレデンシャルで PC にログインします。**注:** ローカル アカウントではなくドメインにログインしていることを確認します。

クライアントでエージェントによる SSO の実行を検出

SSO 完了

オンライン ユーザ リストにある SSO ユーザ

Windows SSO のトラブルシューティング

エラー： Could not start the SSO service. Please check the configuration.

問題

このエラーが発生します。

解決策

この問題を解決するには、次の手順を実行します。

1. KTPass が正しく実行されていることを確認します。 スライド X に示されているフィールドを確認することが重要です。 KTPass が正しく実行されなかった場合は、アカウントを削除し、AD で新しいアカウントを作成し、KTPass を再度実行します。
2. CAS の時刻が DC と同期していることを確認します。このステップは両方で同じタイム サーバを指すことで実行できます。 ラボ セットアップでは、CAS の時刻は DC 自体を指します（DC は Windows 時刻を実行）。 Kerberos はクロックの影響を受けやすく、スキューが 5 分（300 秒）を超えることはできません。**注:** CAS の AD SSO サービスを開始しようとするときに、時刻の同期、つまり NTP に関する問題が発生する可能性があります。 NTP が設定されており、クロックが同期していない場合、サービスは動作しません。 修正が終われればサービスは動作します。
3. Active Directory ドメインが大文字であり（レルム）、CAS で DNS の FQDN を解決できることを確認します。 ラボ セットアップでは、DNS を実行する DC を指すことができます（AD に 1 台以上の DNS サーバが必要）。
4. https://<CAS-IP-address>/admin として CAS に直接ログインします。 次に、[Support Logs] をクリックし、Active Directory 通信ログのログ レベルを [Info] に変更します。
5. 問題を再現させ、サポート ログをダウンロードします。

クライアント認証が機能しない

問題

AD SSO サービスは開始される一方で、クライアント認証は機能しません。

解決策

UDP のポートが未認証ロールで開放されていませんでした。 トラフィック ポリシーにこれらのポートを追加すれば認証が機能します。

Windows 7 PC で SSO を実行できない

問題

SSO は、Windows 7 オペレーティング システムを実行するマシンに対して動作しません。

解決策 1

この問題を解決するには、Windows 7 オペレーティング システムを実行するマシン上での DES 暗号化をイネーブルにしてから、KTPass を実行します。 Windows 7 PC で DES をイネーブルにするには、次の手順を実行します。

1. 管理者として Windows 7 クライアント マシンにログインします。
2. [Start] > [Control Panel] > [System and Security] > [Administrative Tools] > [Local Security Policy] > [Local Policies/Security] > [Options] に移動します。
3. [Network security] > [Configure encryption types allowed] を選択します。
4. [Local Security Settings] タブで、[Future encryption types] オプションを除くすべてのオプションをイネーブルにするように、チェックボックスをオンにします。

解決策 2

この問題を解決するには、Windows 2003 サーバでこのコマンドを実行します（Windows 7 もサポートする必要がある場合）。

```
C:\Program Files\Support Tools> ktpass.exe -princ
casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM-mapusercasuser -pass
Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL
```

詳細については、「Windows 7 環境での AD SSO の設定」を参照してください。

NAC 環境でユーザの Linux クライアント サポートを設定できない

問題

NAC 環境のユーザ用に Linux クライアント サポートを設定できません。

解決策

Web エージェントまたはエージェントは Linux ではサポートされていません。 NAC ではポスチャ アセスメントのない Web ログインを使用する Linux のみをサポートします。 Web ログインによってマシンが認証されると、設定した最終ユーザ ロールがユーザに割り当てられます。 その後、ユーザ ロールのトラフィック ポリシーに従ってユーザがアクセスできます。 詳細については、Cisco Bug ID CSCti54517（登録ユーザ専用）を参照してください。

SSO サービスは開始されているが、クライアントは SSO を実行しない

これは通常は DC とクライアント PC の間またはクライアント PC と CAS の間における通信の問題が原因です。

確認する必要のある事項を次に示します。

- クライアントに Kerberos の鍵がある。
- クライアントが接続でき、エージェントのログを受信でき、CAS 上のログを受信できるように DC へのポートが開放されている。
- クライアント PC の時刻またはクロックが DC と同期されている。

- CAS がポート 8910 でリッスンしていることを確認する。 クライアント PC 上のスニファ トレースも役立ちます。
- CCA エージェントは 4.0.0.1 以降。
- ユーザは、ローカル アカウントではなくドメイン アカウントを使用して実際にログインしている。

Kerbtray

Kerbtray はクライアントが Kerberos チケット（TGT および ST）を取得したことを確認するために使用できます。 問題は、DC で作成した CAS アカウント用のサービス チケット（ST）に関係しています。

Kerbtray は、Microsoft のサポートのツールで使用できるフリー ツールです。 クライアント マシン上の Kerberos チケットをパージするためにも使用できます。

システム トレイ上のグリーンの Kerbtray アイコンは、アクティブな Kerberos チケットがクライアントにあることを示します。 ただし、チケットが CAS アカウントに対して適切（有効）であることを確認する必要があります。

CAS のログ - SSO サービスを開始できない

CAS 上の該当するログ ファイルは、/perfigo/logs/perfigo-redirect-log0.log.0 です。

CAS で AD SSO サービスが開始されない場合は、CAS、DC 間の通信問題です。

1. **SEVERE: startServer - SSO Service authentication failed. Clock skew too great (37)** Aug 3, 2006 7:52:48 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC これは、クロックが CAS とドメイン コントローラ間で同期されていないことを意味します。
2. Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
   INFO: GSSServer - **SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]** Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC **SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos database (6)** Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer startServer **WARNING: GSSServer loginSubject could not be created.** これは、ユーザ名が正しくないことを意味します。 誤ったユーザ名「ccass」、エラー コード 6、および最後の警告に注意します。
3. Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
   INFO: GSSServer - SPN : [ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
   Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
   SEVERE: startServer - SSO Service authentication failed. Pre-authentication information was invalid (24) Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer startServer
   WARNING: GSSServer loginSubject could not be created. パスワードが正しくない、またはレルムが無効です（大文字でない）。 FQDN が正しくない。 KTPass が正しく実行されていない。 エラー 24 および最後の警告に注意します。**注:** KTPass のバージョンがリリース 5.2.3790.0 であることを確認します。 間違ったバージョンの KTPass が存在していると、スクリプトが正常に動作しても、SSO サービスは開始されません。

クライアント - CAS の通信の問題：

Aug 3, 2006 10:03:05 AM com.perfigo.wlan.jmx.admin.GSSHandler run
SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Clock skew too great (37))

このエラーは、クライアント PC の時刻が DC と同期されていない場合に発生します。

注: このエラーと CAS の時刻が DC と同期されていないエラーの違いに注意してください。

既知の問題

- Cisco Bug ID CSCse64395（登録ユーザ専用）：4.0 エージェントで Windows SSO の DNS が解決されません。この問題は CCA エージェント 4.0.0.1 解決されています。
- Cisco Bug ID CSCse46141（登録ユーザ専用）：起動時に CAS が AD サーバに到達できない場合 SSO は失敗します。回避策は、[CCA Servers] > [Manage [CAS_IP] Authentication] > Windows Auth] > [Active Directory SSO] に移動して、AD SSO サービスを再開するために [Update] をクリックすることです。
- CAS で service perfigo restart を実行します。 古いクレデンシャルが CAS 上にキャッシュされており、Tomcat が再起動されるまで新しいポリシーが使用されないというキャッシュに関連する問題があります。
- SSO に対するシングル ユーザ ログインは限定できません。 SSO は kerberos プロトコルであり、シングル ユーザのログインを制限するオプションが kerberos プロトコルないため、これは正常な動作です。
- *Windows 7* および *Windows 2008* では、SSO をサポートしません。これは、SSO では、**Windows 7 と Windows 2008 でサポートされていない DES 暗号化**を使用するためです。

関連情報

- Cisco NAC アプライアンス (Clean Access) に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems