CA SiteMinder Federation Standalone

Windows 認証用エージェント ガイド

r12.52 SP1

ca technologies

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

マニュアルの変更点

CA SiteMinder® Federation Standalone の以前のリリースでの問題の結果として 12.52 のドキュメントの更新は行われていません。

目次

第 1 章: Windows 認証用フェデレーション エージェント

Windows 用フェデレーション エージェントの概要

Windows 認証用のフェデレーション エージェントは、統合 Windows 認証（IWA）プロトコルの 1 つを実装するシステム上でビジネス パートナーとのフェデレーションを可能にします。

ユーザが保護されているリソースへのアクセスをリクエストすると、フェデレーション システムはサードパーティ Web アクセス管理（WAM）システムからのログオン ID 情報を使用します。 サードパーティ WAM を使用するこのプロセスは、委任認証として知られています。 フェデレーション システムは、フェデレーション エージェントにリクエストをリダイレクトします。 エージェントはユーザのアイデンティティを確認し、オープン形式の Cookie を作成し、Cookie をフェデレーション システムに渡します。 次に SAML アサーションが生成され、依存パーティに渡されます。

注: 委任認証の詳細については、「Federation Standalone ガイド」を参照してください。

IWA は Windows NT LAN Manager（NTLM）および Kerberos 暗号化プロトコルをサポートします。 Windows システムの場合、フェデレーション エージェントは NTLM または Kerberos を使用できます。UNIX システムの場合、フェデレーション エージェントは Kerberos のみを使用できます。

CA SiteMinder® Federation Standalone がインストールされているのと同じ Windows または UNIX システムにフェデレーション エージェントがインストールされます。 以下の制限が適用されます。

- SiteMinder コネクタを使用するフェデレーション インストールとフェデレーション エージェントは互換性がありません。
- シングル サインオン（SSO）リクエストを発行するブラウザをフェデレーション システムと同じシステムに置くことはできません。

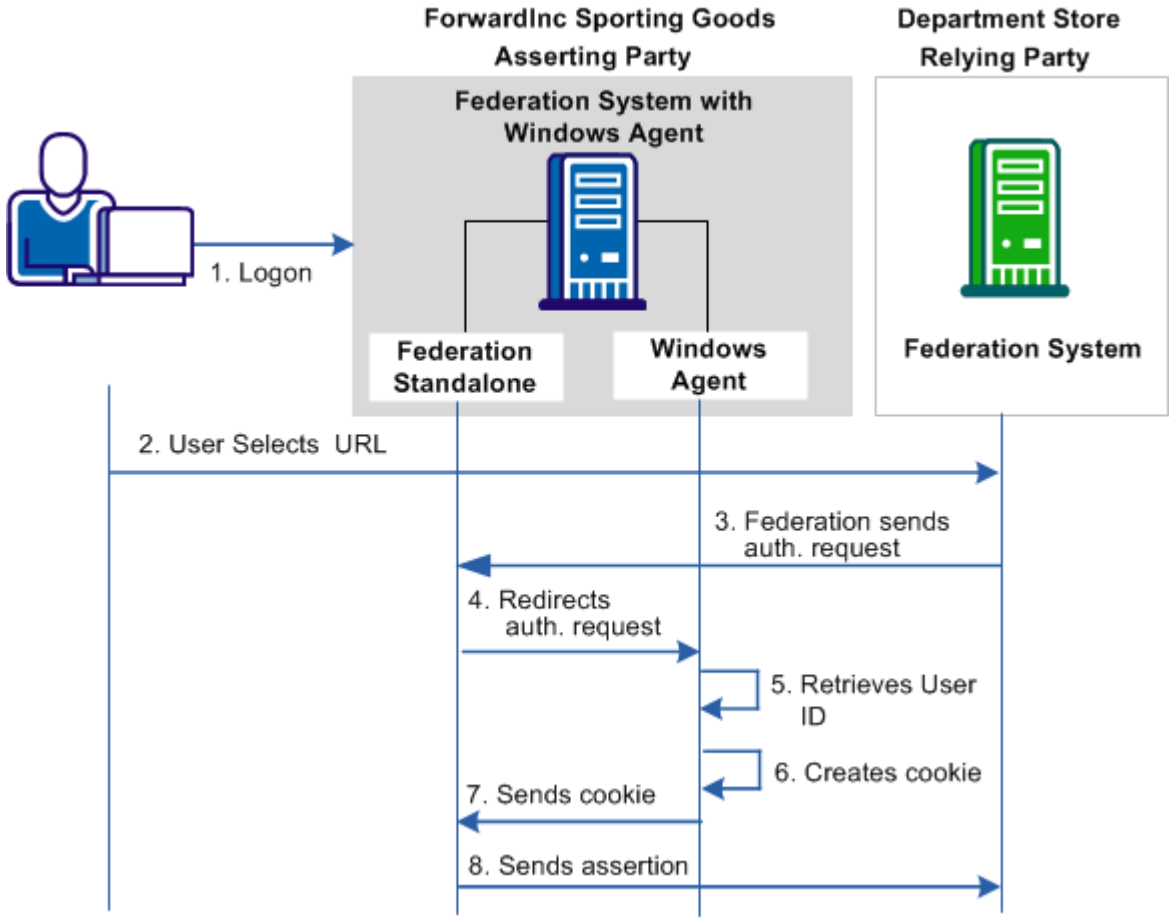
管理者は統合 Windows 認証プロトコル（NTLM および Kerberos）のことを知っている必要があります。 さらに、読者はフェデレーションの概念および CA SiteMinder® Federation Standalone 管理に精通している必要があります。

IWA を使用するシステムとビジネス パートナー間の SSO

委任認証のユース ケースは、フェデレーション エージェントがどのように動作するかを示します。 デパートでは、特別な割引を提供するため、サプライヤ（ForwardInc Sporting Goods）の従業員にシングル サインオン アクセスを付与しようとしています。

デパートおよび ForwardInc Sporting Goods はフェデレーション パートナーシップを確立しています。 ForwardInc Sporting Goods の従業員は、通常ドメイン ユーザ名およびパスワードで勤務中のアカウントにログインします。 従業員がデパートの Web サイトを参照する場合、従業員は認証情報を要求されずに、IWA プロトコルの 1 つによってアクセスを付与されます。

以下の図は、フェデレーション パートナーシップにおけるフェデレーション エージェントの役割を示します。



図で表示されるようなトランザクションを以下に示します。

1. ユーザは、ForwardInc Sporting Goods の Web アクセス管理（WAM）システムにログインします。
2. ユーザはブラウザを開き、依存パーティであるデパートの URL に移動します。

   注: ブラウザは、Windows エージェントがインストールされているフェデレーション システムと同じシステムに配置することはできません。
3. 依存パーティは、アサーティング パーティに認証リクエストを送信します。 アサーティング パーティのフェデレーション システムは、委任された認証がこのパートナーシップに対して設定されていることを確認します。

4. フェデレーション システムは、フェデレーション エージェントにリクエストを送信します。エージェントは、ユーザのセキュリティ コンテキストを検証します。
5. Windows エージェントはリクエストから検証された情報を抽出します。
6. Windows エージェントはオープン形式の Cookie へユーザ情報を配置します。
7. Windows エージェントはフェデレーション システムに Cookie を送信します。
8. アサーティング パーティのフェデレーション システムはユーザ情報を抽出し、アサーションにそれを設定し、依存パーティにアサーションを送信します。

ユーザは、ログインしなくてもデパート Web サイトへのアクセスを許可されます。

用語

このガイドは、Windows 認証に関連する以下の用語を使用します。

認証サーバ（AS）

認証サーバは、クライアントからの初期認証リクエストに返答する Key Distribution Center （KDC）の一部です。 ユーザが認証された後、認証サーバは Ticket Granting Ticket （TGT）を発行します。 TGT を使用すると、ユーザはパスワードを再入力する必要なしに、他の Kerberos サービス チケットを取得できます。

統合 Windows 認証（IWA）

統合 Windows 認証はユーザのログオン クレデンシャルからの認証情報を Windows クライアント アプリケーションを提供します。 認証交換がユーザを識別することに失敗した場合、ブラウザは Windows の ID およびパスワードをユーザに求めます。統合 Windows 認証は標準または認証プロトコルではありません。Kerberos プロトコルまたは NTLM プロトコルを使用します。

Kerberos

Kerberos 認証プロトコルを使用すると、ユーザは任意のネットワーク上で安全に通信できます。 Kerberos は、またこのプロトコルを実装するマサチューセッツ工科大学（MIT）によって発行された無料ソフトウェア一式でもあります。Kerberos はユーザ ID を確認することに対してチケットを使用します。Kerberos プロトコル メッセージは盗聴およびリプレイ攻撃に対して保護されています。 Kerberos は対称キー暗号化法に基づいて構築され、信頼されたサードパーティ（Key Distribution Center）を必要とします。

Key Distribution Center（KDC）

Key Distribution Center は暗号システムの一部です。暗号システムには認証サーバおよびチケット交付サーバが含まれます。 Key Distribution Center の目的はキー交換固有のリスクを減らすことです。 多くの場合、Key Distribution Center は、一部のユーザが特定の時間にサービスを使用し、それ以外の時間には使用しない権限を所有できるシステムで作動します。

キータブ

キータブは Kerberos プリンシパルおよび Kerberos パスワードから派生した暗号化キーのペアで構成されるファイルです。 このファイルは Key Distribution Center へのログインに使用されます。

NTLM

NTLM は、シングル サインオン用のさまざまな Microsoft ネットワーク実装で使用される認証プロトコルです。 NTLM は、認証に対してチャレンジ レスポンス メカニズム（クライアントはサーバにパスワードを送信せずに、そのアイデンティティを証明する）を使用します。 NTLM は、一般にタイプ 1 （ネゴシエーション）、タイプ 2 （チャレンジ）およびタイプ 3 （認証）と呼ばれる 3 つのメッセージから構成されます。タイプ 3 メッセージ内の応答ではクライアント ユーザがアカウント パスワードを知っていることをサーバに証明するので、この応答が最も重要になります。

Ticket Granting Ticket（TGT）

Ticket Granting Ticket （TGT）は、有効期間に制限のある、暗号化された小さい識別ファイルです。 認証の後、このファイルは KDC 認証サーバによってデータ トラフィック保護用に、ユーザに付与されます。 Ticket Granting Ticket ファイルにはセッション キー、チケットの有効期限日およびユーザ IP アドレスが含まれます。

チケット交付サーバ（TGS）

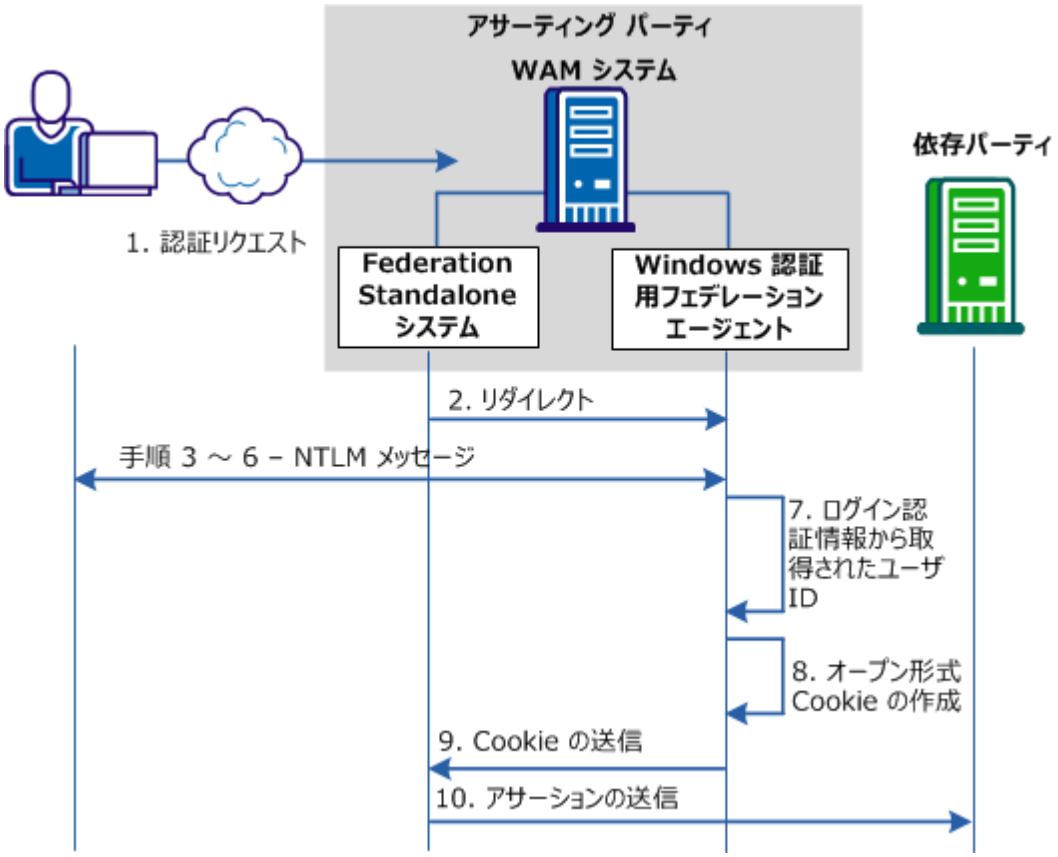
チケット交付サーバは、有効な Ticket Granting Ticket （TGT）を持ったクライアントにサービス チケットを配布する KDC コンポーネントです。 チケット交付サーバは、サービスとしてチケットを発行するアプリケーション サーバに似ています。

NTLM プロトコル

NTLM にはさまざまな認証およびセッション セキュリティ プロトコルが含まれます。 NTML は、以下の順に交換される 3 種類のメッセージから構成される、チャレンジ レスポンス モデルに基づいています。

1. クライアントはサーバにタイプ 1 メッセージ（ネゴシエーション）を送信します。 タイプ 1 メッセージは、クライアントによってサポートされ、サーバからリクエストされた機能を指定します。
2. サーバはクライアントにタイプ 2 メッセージ（チャレンジ）を送信します。 このメッセージの主な機能はクライアント ユーザの ID を要求することです。
3. クライアントはサーバにタイプ 3 メッセージ（認証）を送信します。タイプ 3 メッセージには、クライアント ユーザのドメインおよびユーザ名が含まれ、タイプ 2 メッセージのチャレンジに応答します。

以下の画像は、フェデレーション エージェントが搭載されたフェデレーション システムでの NTLM プロトコルの使用方法を示します。



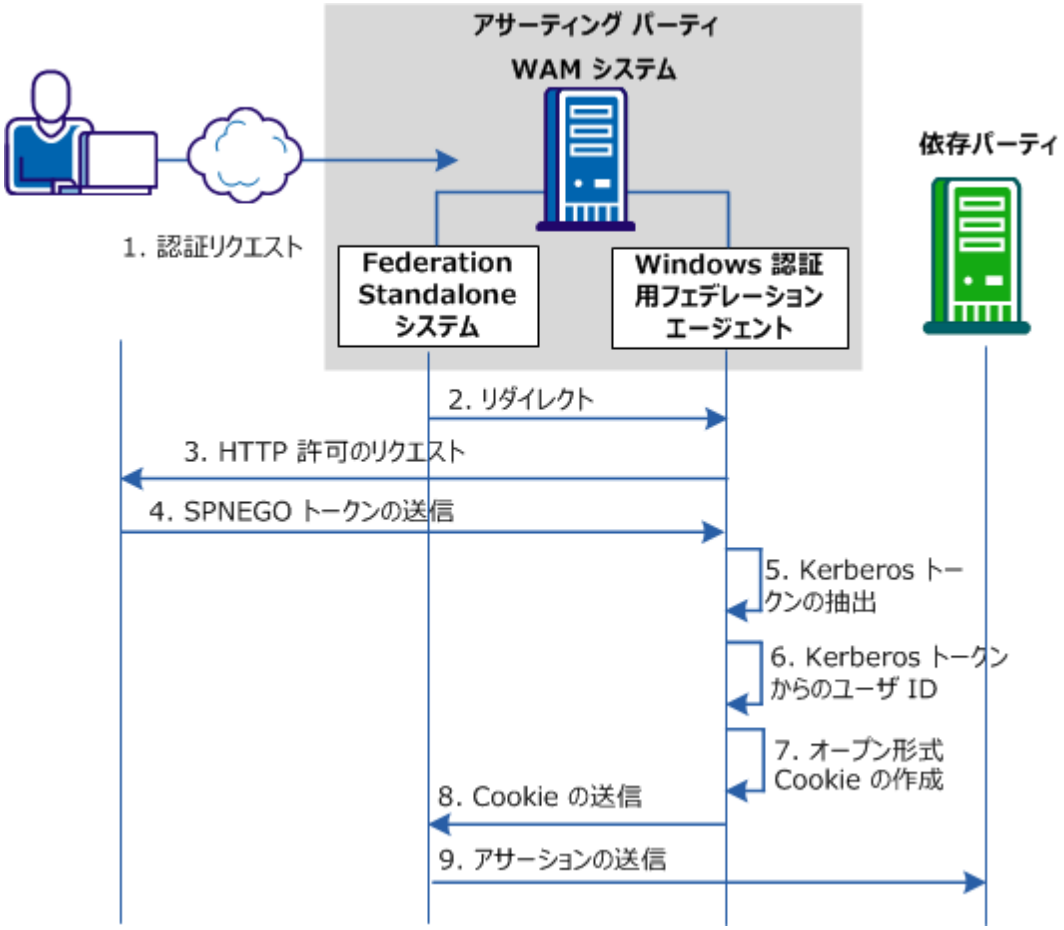
以下のプロセスは、前の図での注釈を参照しています。

1. 認証リクエストは、アサーティング パーティの CA SiteMinder® Federation Standalone に対して行われます。
2. フェデレーション システムは、委任認証リクエストとしてこの要求を認識し、リクエストをフェデレーション エージェントにリダイレクトします。
3. エージェントはブラウザに応答を送信します。
4. ブラウザが IWA に対して設定されている場合、ブラウザは NTLM ネゴシエート トークン（タイプ 1 メッセージ）を認証ヘッダでフェデレーション エージェントに送信します。
5. フェデレーション エージェントは、NTLM チャレンジ トークン（タイプ 2 メッセージ）をブラウザに送信します。

6. ブラウザは、NTLM 認証トークン（タイプ 3 メッセージ）をフェデレーション エージェントに送信します。
7. セキュリティ コンテキストがユーザと関連付けられている場合、フェデレーション エージェントは確立されたコンテキストからユーザ ID を取得します。
8. エージェントは、ユーザ ID 情報が含まれるオープン形式の Cookie を作成します。
9. エージェントはこの Cookie をフェデレーション システムに送信します。
10. フェデレーション システムは、フェデレーション処理を完了するためにアサーションを依存パーティに送信します。

Kerberos プロトコル

以下の図は、フェデレーション エージェントが搭載されたフェデレーション システムでの Kerberos プロトコルの使用方法を示します。



以下のプロセスは、前の図での注釈を参照しています。

1. 認証リクエストは、アサーティング パーティのフェデレーション システムに対して行われます。

   フェデレーション システムは、このリクエストが委任認証リクエストであることを認識します。

2. フェデレーション システムは、フェデレーション エージェントにリダイレクトします。

3. フェデレーション エージェントはブラウザから HTTP 認証をリクエストします。

4. ブラウザが IWA に対して設定されている場合、SPNEGO トークンがフェデレーション エージェントに送信されます。このトークンは、開始者および受け入れ側が Kerberos を使用するか NTLM を使用するかをネゴシエートすることを可能にします。
5. フェデレーション エージェントは SPNEGO トークンから Kerberos トークンを抽出します。
6. セキュリティ コンテキストが Kerberos トークンから確立された後、エージェントはユーザ ID 情報を取得します。
7. エージェントはオープン形式の Cookie を作成し、リダイレクト URL を構築します。
8. エージェントはこの Cookie をフェデレーション システムに送信します。
9. フェデレーション システムは必要な処理を実行し、依存パーティにアサーションを送信します。

第 2 章: Windows 用フェデレーション エージェントのインストール前提条件

CA SiteMinder® Federation Standalone がインストールされているのと同じ Windows または UNIX システムにフェデレーション エージェントをインストールします。 以下の制限が適用されます。

- CA SiteMinder® コネクタを使用するフェデレーション インストールとフェデレーション エージェントは互換性がありません。
- シングル サインオン（SSO）リクエストを発行するブラウザをフェデレーション サーバと同じシステムに置くことはできません。

認証プロトコルの選択に応じて、CA SiteMinder® フェデレーション Windows エージェントには 3 つの動作モードがあります。

- NTLM モード（Windows でのみサポート）
- Kerberos モード（Windows および UNIX でサポート）
- NTLM へのフェールオーバがある Kerberos モード（Windows でのみサポート）

エージェント設定ウィザードを実行する際に動作モードを選択します。

フェデレーション Windows エージェントのセットアップ プロセスには、以下の手順が含まれます。

1. インストールの前提条件をすべて実行します。前提条件は動作モードおよび動作環境に応じて変わります。
   - Windows 上のエージェントを持った NTLM
   - Windows 上のエージェントおよび Windows 上の KDC を持った Kerberos
   - Windows 上のエージェントおよび UNIX 上の KDC を持った Kerberos
   - UNIX 上のエージェントおよび Windows 上の KDC を持った Kerberos
   - UNIX 上のエージェントおよび UNIX 上の KDC を持った Kerberos
2. Windows 用フェデレーション エージェントのインストール
3. Windows（39P. ）用フェデレーション エージェントを設定します。
4. フェデレーション システム用の委任認証を設定します。

Windows システム上の NTLM モード

NTLM を使用して、フェデレーション Windows エージェントを Windows システムにインストールする前に、インストールの前提条件をすべて完了します。

1. Windows に NTLM 用のドメイン コントローラをセットアップする
2. Internet Explorer を設定します。

Windows に NTLM 用のドメイン コントローラをセットアップする

Windows 2003 SP 1 Active Directory は Windows ドメイン用のプライマリ ドメイン コントローラです。このホストは、ユーザ、サービス アカウント、認証情報および Windows ドメイン サービス用のストレージを提供します。

フェデレーション エージェントは、依存パーティによって送信された NTML チャレンジ メッセージへの NTLM 応答メッセージを生成します。依存パーティでのサーバはチャレンジおよび応答をドメイン コントローラへ渡します。 応答はユーザ パスワードのハッシュを使用したチャレンジの暗号化されたバージョンです。 ドメイン コントローラはパスワードの同じハッシュを使用してチャレンジを暗号化し、それをアサーティング パーティで生成された応答と比較します。 それらが一致する場合、認証は完了です。 ドメイン コントローラは依存パーティのサーバに通知します。

以下の手順に従います。

1. Windows dcpromo ユーティリティを使用して、Windows 2003 SP 1 Server をドメイン コントローラに昇格させます。
2. 管理ツールから［Active Directory ユーザとコンピュータ］ダイアログ ボックスを開きます。
3. ユーザ アカウントの作成を選択します。
4. このアカウントの作成用のパスワードを入力します。
5. ［ユーザは次回ログオン時にパスワード変更が必要］チェック ボックスをオフにします。

ドメイン コントローラが NTLM に対して展開されます。

シングル サインオン用の Internet Explorer を設定します。 この手順は、NTLM または Kerberos を認証プロトコルとして使用している場合にも適用されます。

詳細情報:

Internet Explorer の構成設定 (P. 28)

Windows KDC を使用した Windows システム用の Kerberos モード

Kerberos モードを使用して、フェデレーション エージェント用のインストール前提条件を Windows システムで完了します。 KDC は Windows システム上にあります。 Windows に Kerberos 用のドメイン コントローラをセットアップします。

1. Windows に Kerberos 用のドメイン コントローラをセットアップします。
2. Windows 上の Kerberos 用の追加設定の完了
3. Internet Explorer を設定します。

Windows に Kerberos 用のドメイン コントローラをセットアップする

Kerberos を使用する場合、ドメイン コントローラは Kerberos レルムの Key Distribution Center （KDC）です。 純粋な Windows 2003 環境では、Kerberos レルムは Windows ドメインに相当します。 ドメイン コントローラ ホストは、ユーザ、サービス アカウント、認証情報、Kerberos チケッティング サービス、および Windows ドメイン サービスのためのストレージを提供します。

Kerberos 認証には keytab ファイルが必要です。keytab ファイルによりフェデレーション システムにログオンしたユーザはパスワードを要求されることなく KDC により認証できます。 keytab ファイルは ktpass ユーティリティで作成されます。 ktpass コマンド ツール ユーティリティは Windows サポート ツールです。 デフォルト暗号化タイプは RC4-HMAC-NT です。これは、コマンド プロンプトで **ktpass /?** を実行して確認できます。 また、Kerberos バージョン番号を確認します。

以下の手順に従います。

1. Windows dcpromo ユーティリティを使用して、Windows 2003 SP 1 Server をドメイン コントローラに昇格させます。
2. 管理ツールから［Active Directory ユーザとコンピュータ］ダイアログ ボックスを開きます。
3. ユーザ アカウントの作成を選択します。
4. このアカウント用のパスワードを入力します。

5. ［ユーザは次回ログオン時にパスワード変更が必要］チェック ボックスをオフにします。
6. サーバ プリンシパル名（たとえば HTTP/IWAConnectorHostName.idp.com@IDP.COM）と Windows 2003 ワークステーション アカウントを関連付けます。
7. コマンド プロンプト ウィンドウを開いて keytab ファイルを作成し、以下のコマンドを入力します。

   ```
   ktpass -out output_keytab_location -princ SPN_name -ptype
   KRB5_NT_PRINCIPAL -mapuser username -pass password
   ```

   手順 4 で入力したパスワードを使用します。

   keytab ファイルが作成されます。

   例：

   ```
   ktpass -out c:¥workstation.keytab -princ HTTP/
   IWAConnectorHostName.idp.com@IDP.COM
   -ptype KRB5_NT_PRINCIPAL -mapuser testkrb -pass password
   標的ドメイン コントローラ： winkdc.idp.com
   Using legacy password setting method
   正常に、testkrb に HTTP/ IWAConnectorHostName.idp.com をマップしました。
   Key created.
   c:¥workstation.keytab への出力キータブ
   Keytab version: 0x502
   keysize 67 HTTP/ IWAConnectorHostName.idp.com@IDP.COM ptype 1
   (KRB5_NT_PRINCIPAL) vno 2 etype 0x17 (RC4-HMAC) keylength 16
   (0xfd77a26f1f5d61d1fafd67a2d88784c7)
   ```

8. アサーティング パーティでフェデレーション システム上の安全な場所に keytab ファイルをコピーします。

   重要: フェデレーション エージェントの設定中に［Keytab Location］フィールドで keytab ファイルのフル パス名を指定する必要があります。

Kerberos 用のドメイン コントローラが Windows を実行するシステムに展開されます。

Windows 上の Kerberos 用の追加設定の完了

Windows で Kerberos を使用する場合、以下のアクションがフェデレーション システムで必要です。

1. Kerberos 設定ファイル（krb5.ini）を設定します。Windows システム ルート パスに krb5.ini ファイルを配置します。
   a. Windows 2003 ドメイン コントローラを使用するために Windows 2003 Kerberos レルム（ドメイン）用の KDC を設定します。
   b. ワークステーション プリンシパルの認証情報が含まれる Windows 2003 KDC keytab ファイルを使用するために krb5.ini を設定します。

```
[libdefaults]
default_realm = IDP.COM
default_keytab_name = C:¥WINDOWS¥krb5.keytab
default_tkt_enctypes = des-cbc-md5 rc4-hmac
default_tgs_enctypes = des-cbc-md5 rc4-hmac
[realms]
IDP.COM = {
kdc = winkdc.idp.com:88
default_domain = IDP.COM
}
[domain_realm]
.idp.com=IDP.COM
```

2. 安全な場所に Windows 2003 KDC keytab ファイルを展開します（krb5.ini の記述に従う）。

シングル サインオン用の Internet Explorer を設定します。 この手順は、NTLM または Kerberos を認証プロトコルとして使用している場合にも適用されます。

詳細情報:

Internet Explorer の構成設定 (P. 28)

UNIX KDC を使用した Windows システム用の Kerberos モード

Kerberos モードで Windows を実行するシステムでフェデレーション エージェント用のインストール前提条件を完了します。 KDC は UNIX システム上にあります。

1. UNIX システムで KDC を設定します。
2. Windows 上の Kerberos 用の追加設定の完了
3. Internet Explorer を設定します。

UNIX システム上の KDC の設定

フェデレーション システムをサポートするように Kerberos Key Distribution Center（KDC）をホストする UNIX サーバを設定する必要があります。このプロセスには keytab ファイルの作成も含まれます。Kerberos 認証には keytab ファイルが必要です。

以下の手順に従います。

1. コマンド プロンプト ウィンドウを開きます。
2. コマンドライン プロンプトで、以下のコマンドを入力します。

   ```
   usr/sbin/kadmin.local
   ```

3. 以下のコマンドで CA SiteMinder® Federation Standalone システム サービス プリンシパル名を追加します。

   ```
   addprinc -pw <password> HTTP/AgentHost Name.domainname.com@DOMAINNAME.COM
   ```

4. コマンド プロンプト ウィンドウを開いて keytab ファイルを作成し、以下のコマンドを入力します。

   ```
   ktadd -k output_keytab_location SPN name
   ```

   keytab ファイルが作成されます。

5. quit を入力します。

UNIX KDC サーバ上でフェデレーションの設定が完了しました。

UNIX 上の Kerberos 用の追加設定の完了

Kerberos を設定するには、以下のコマンドが UNIX システム上のフェデレーション システムに対して必要です。

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

UNIX システムは Kerberos 認証に対して設定されます。

シングル サインオン用の Internet Explorer を設定します。 この手順は、NTLM または Kerberos を認証プロトコルとして使用している場合にも適用されます。

詳細情報:

Internet Explorer の構成設定 (P. 28)

Windows KDC を使用した UNIX システム用の Kerberos モード

Kerberos モードで実行する UNIX システムへのフェデレーション エージェントのインストール前提条件を完了します。 KDC は Windows システム上にあります。

1. Windows に Kerberos 用のドメイン コントローラをセットアップします。
2. UNIX 上の Kerberos 用の追加設定
3. Internet Explorer を設定します。

Windows に Kerberos 用のドメイン コントローラをセットアップする

Kerberos を使用する場合、ドメイン コントローラは Kerberos レルムの Key Distribution Center （KDC）です。 純粋な Windows 2003 環境では、Kerberos レルムは Windows ドメインに相当します。 ドメイン コントローラ ホストは、ユーザ、サービス アカウント、認証情報、Kerberos チケッティング サービス、および Windows ドメイン サービスのためのストレージを提供します。

Kerberos 認証には keytab ファイルが必要です。keytab ファイルによりフェデレーション システムにログオンしたユーザはパスワードを要求されることなく KDC により認証できます。 keytab ファイルは ktpass ユーティリティで作成されます。 ktpass コマンド ツール ユーティリティは Windows サポート ツールです。 デフォルト暗号化タイプは RC4-HMAC-NT です。これは、コマンド プロンプトで **ktpass /?** を実行して確認できます。 また、Kerberos バージョン番号を確認します。

以下の手順に従います。

1. Windows dcpromo ユーティリティを使用して、Windows 2003 SP 1 Server をドメイン コントローラに昇格させます。
2. 管理ツールから［Active Directory ユーザとコンピュータ］ダイアログ ボックスを開きます。
3. ユーザ アカウントの作成を選択します。
4. このアカウント用のパスワードを入力します。
5. ［ユーザは次回ログオン時にパスワード変更が必要］チェック ボックスをオフにします。
6. サーバ プリンシパル名（たとえば HTTP/IWAConnectorHostName.idp.com@IDP.COM）と Windows 2003 ワークステーション アカウントを関連付けます。
7. コマンド プロンプト ウィンドウを開いて keytab ファイルを作成し、以下のコマンドを入力します。

   ```
   ktpass -out output_keytab_location -princ SPN_name -ptype
   KRB5_NT_PRINCIPAL -mapuser username -pass password
   ```

   手順 4 で入力したパスワードを使用します。

   keytab ファイルが作成されます。

例：

```
ktpass -out c:¥workstation.keytab -princ HTTP/
IWAConnectorHostName.idp.com@IDP.COM
-ptype KRB5_NT_PRINCIPAL -mapuser testkrb -pass password
標的ドメイン コントローラ： winkdc.idp.com
Using legacy password setting method
正常に、testkrb に HTTP/ IWAConnectorHostName.idp.com をマップしました。
Key created.
c:¥workstation.keytab への出力キータブ
Keytab version: 0x502
keysize 67 HTTP/ IWAConnectorHostName.idp.com@IDP.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 2 etype 0x17 (RC4-HMAC) keylength 16
(0xfd77a26f1f5d61d1fafd67a2d88784c7)
```

8. アサーティング パーティでフェデレーション システム上の安全な場所に keytab ファイルをコピーします。

   重要: フェデレーション エージェントの設定中に［Keytab Location］フィールドで keytab ファイルのフル パス名を指定する必要があります。

Kerberos 用のドメイン コントローラが Windows を実行するシステムに展開されます。

UNIX 上の Kerberos 用の追加設定の完了

Kerberos を設定するには、以下のコマンドが UNIX システム上のフェデレーション システムに対して必要です。

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

UNIX システムは Kerberos 認証に対して設定されます。

シングル サインオン用の Internet Explorer を設定します。 この手順は、NTLM または Kerberos を認証プロトコルとして使用している場合にも適用されます。

詳細情報:

Internet Explorer の構成設定 (P. 28)

UNIX KDC を使用した UNIX システム用の Kerberos モード

Kerberos モードで実行する UNIX システムへのフェデレーション エージェントのインストール前提条件を完了します。 KDC は UNIX システム上にあります。

1. UNIX システムで KDC を設定します。
2. UNIX 上の Kerberos 用の追加設定
3. Internet Explorer を設定します。

UNIX システム上の KDC の設定

フェデレーション システムをサポートするように Kerberos Key Distribution Center（KDC）をホストする UNIX サーバを設定する必要があります。このプロセスには keytab ファイルの作成も含まれます。Kerberos 認証には keytab ファイルが必要です。

以下の手順に従います。

1. コマンド プロンプト ウィンドウを開きます。
2. コマンドライン プロンプトで、以下のコマンドを入力します。

   ```
   usr/sbin/kadmin.local
   ```

3. 以下のコマンドで CA SiteMinder® Federation Standalone システム サービス プリンシパル名を追加します。

   ```
   addprinc -pw <password> HTTP/AgentHost Name.domainname.com@DOMAINNAME.COM
   ```

4. コマンド プロンプト ウィンドウを開いて keytab ファイルを作成し、以下のコマンドを入力します。

   ```
   ktadd -k output_keytab_location SPN name
   ```

   keytab ファイルが作成されます。

5. quit を入力します。

UNIX KDC サーバ上でフェデレーションの設定が完了しました。

UNIX 上の Kerberos 用の追加設定の完了

Kerberos を設定するには、以下のコマンドが UNIX システム上のフェデレーション システムに対して必要です。

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

UNIX システムは Kerberos 認証に対して設定されます。

シングル サインオン用の Internet Explorer を設定します。 この手順は、NTLM または Kerberos を認証プロトコルとして使用している場合にも適用されます。

詳細情報:

Internet Explorer の構成設定 (P. 28)

Internet Explorer の構成設定

シングル サインオン展開で機能させるには、いくつかの特定の Internet Explorer 設定を構成します。

ローカル イントラネット プロパティ セットアップ

Internet Explorer がシングル サインオン展開で機能するには、いくつかの特定の設定が必要です。 ブラウザのセットアップでは、ローカル イントラネット プロパティを設定してイントラネット認証を設定する必要があります。 Kerberos と NTLM のどちらの認証プロトコルを使用しても、これらの設定は適用されます。

以下の手順に従います。

1. Internet Explorer ブラウザを開きます。
2. Internet Explorer メニュー バーから［ツール］を選択します。
3. ドロップダウン メニューから［インターネット オプション］を選択します。

4. ［セキュリティ］タブをクリックします。
5. ［ローカル イントラネット］ボタンをクリックします。
6. ［サイト］ボタンをクリックします。
7. ［プロキシ サーバーを使用しないサイトをすべて含める］チェック ボックスがオンになっていることを確認します。
8. ［詳細設定］ボタンをクリックします。
9. AgentHostName.domainname.com など、イントラネットで使用されるドメイン名をすべて入力します。
10. ［詳細設定］タブを選択します。
11. ［セキュリティ］セクションにスクロールします。
12. ［統合 Windows 認証を使用する (再起動が必要)］をオンにします。
13. システムを再起動します。
14. ［OK］をクリックします。

ローカル イントラネット プロパティが設定されます。

イントラネット認証セットアップ

Internet Explorer をシングル サインオン ソリューションで機能させるには、いくつかの特定の設定が必要です。 これらのクライアント ブラウザ設定はイントラネット環境を前提とします。 ブラウザのセットアップでは、ローカル イントラネット プロパティを設定してイントラネット認証を設定する必要があります。

以下の手順に従います。

1. Internet Explorer ブラウザを開きます。
2. Internet Explorer メニュー バーから［ツール］メニューを選択します。
3. ドロップダウン メニューから［インターネット オプション］を選択します。
4. ［セキュリティ］タブをクリックします。
5. ［ローカル イントラネット］ボタンをクリックします。

6. ［レベルのカスタマイズ］ボタンをクリックします。
7. ［セキュリティ］タブを選択します。
8. ［ユーザ認証］セクションまでスクロール ダウンします。
9. ［イントラネット ゾーンでのみ自動的にログオンする］を選択します。
10. ［OK］をクリックします。

ユーザはイントラネット ゾーンで認証されます。

プロキシ サーバによるブラウザ認証（オプション）

アサーティング パーティで、ブラウザとエージェントを持ったフェデレーション システムの間にプロキシ サーバが挿入されると、認証は機能しなくなります。 この場合、相対ドメイン名を持った URL はすべてプロキシ サーバを通過しないように設定する必要があります。

以下の手順に従います。

1. Internet Explorer ブラウザを開きます。
2. Internet Explorer メニュー バーから［ツール］メニューを選択します。
3. ドロップダウン メニューから［インターネット オプション］を選択します。
4. ［詳細設定］タブをクリックします。
5. ［セキュリティ］セクションにスクロールします。
6. ［統合 Windows 認証を使用する］がオンになっていることを確認します。
7. ［接続］タブをクリックします。
8. ［LAN の設定］ボタンをクリックします。
9. プロキシ サーバ アドレスおよびポート番号が正しいことを確認します。
10. ［詳細設定］ボタンをクリックします。

11. ［例外］フィールドに関連するドメイン名をすべて指定します。
12. ［OK］をクリックします。

ブラウザは指定されたドメインに対してプロキシ サーバを使用しないように設定されます。

ポート仕様（オプション）

設定にフェデレーション エージェントおよびドメイン コントローラの間のファイアウォールがある場合、通信を可能にするために以下の静的ポートを開く必要があります。

- Microsoft-DS トラフィック （445/tcp、445/udp）
- Lightweight Directory Access Protocol （LDAP） ping （389/udp）
- ドメイン ネーム システム（DNS）（53/tcp、53/udp）
- Kerberos 認証プロトコル（88/tcp、88/udp）
- NetBIOS データグラム サービス（138/tcp、138/udp）
- NetBIOS-ns サービス（137/tcp、137/udp）
- epmap （135/tcp、135/udp）

さらに、以下の Local Security Authority （LSA）ポートが動的であり、レジストリ エントリの変更により静的にする必要があります。

- Local Security Authority Service （NTDS）（1025/tcp、1025/udp）：NTLM に必要な設定可能ポート
- Local Security Authority Service （NetLogin）（1026/tcp、1026/udp）：Kerberos に必要な設定可能ポート

LSA ポートの詳細については、以下のサイトを参照してください。

http://support.microsoft.com/kb/224196/

第 3 章: Windows 認証用フェデレーション エージェントのインストール

インストール要件

以下のシステム要件を考慮します。

- CA SiteMinder® Federation Standalone がすでにインストールされているシステムにフェデレーション エージェントをインストールする必要があります。
- CA SiteMinder® Federation Standalone が SiteMinder コネクタを使用しているシステムにフェデレーション エージェントをインストールしないでください。

重要: CA SiteMinder® Federation Standalone を現在のバージョンにアップグレードする場合は、Agent を同じバージョンにアップグレードします。アップグレードしないと、エージェントは正しく動作しません。

インストール実行ファイル

以下の表に、フェデレーション エージェントのインストール実行ファイルを示します。

注: インストール実行可能ファイルおよびフォルダ名には文字列 **iwa** が含まれます。iwa は、統合 Windows 認証技術のサポートを参照します。

プラットフォーム	インストール実行ファイル
Solaris	ca-fedmgr-iwa-*version*-sol.bin
Linux	ca-fedmgr-iwa-*version*-rhel30.bin
Windows	ca-fedmgr-iwa-*version*-win32.exe

サポートされているオペレーティング システムの詳細については、テクニカル サポート サイトで「プラットフォーム サポート マトリクス」を参照してください。

フェデレーション エージェントのインストール（Windows）

インストーラを実行します。

インストール キットを見つける方法

1. テクニカル サポート サイトに移動します。
2. サイトにログオンします。
3. ［Download Center］をクリックします。
4. インストール キットの［Download Center］を検索し、ローカル システムにダウンロードします。

エージェントを Windows にインストールする方法

1. 実行中のすべてのアプリケーションを終了します。
2. インストール実行ファイルが置かれている場所に移動します。
3. オペレーティング プラットフォーム用のインストール実行可能ファイルを実行します。

   実行可能ファイルのリストはここで参照できます。

   インストール ウィザードが起動されます。
4. インストール ウィザードのプロンプトに従います。

   システムに Windows エージェントがインストールされます。
5. インストールが完了した後、設定ウィザード (P. 41) を実行します。

フェデレーション エージェントのインストール（UNIX）

インストーラを実行します。

インストール キットを見つける方法

1. テクニカル サポート サイトに移動します。
2. サイトにログオンします。
3. ［Download Center］をクリックします。
4. インストール キットの［Download Center］を検索し、ローカル システムにダウンロードします。

UNIX システムにエージェントをインストールする方法

1. 実行中のすべてのアプリケーションを終了します。
2. インストール実行ファイルが置かれている場所に移動します。
3. オペレーティング プラットフォーム用のインストール実行可能ファイルを実行します。

   実行可能ファイルのリストはここで参照できます。

   インストール ウィザードが起動されます。
4. インストール ウィザードのプロンプトに従います。

   システムに Windows エージェントがインストールされます。
5. インストールが完了した後、設定ウィザードを実行します。

フェデレーション エージェントの無人インストール

Windows エージェントを手動でインストールした後は、同じシステム、または別のシステムに無人インストール モードを使用してエージェントをインストールすることができます。 無人インストールはユーザ介在を必要としません。 このインストールは、ユーザの要件に応じて変更できるインストール プロパティ ファイルに依存します。

無人インストール プロセスはすべてのプラットフォームで同じです。 実行可能ファイル名のみが異なります。

次の手順に従ってください:

1. インストール実行可能ファイルが存在するディレクトリへ移動します。
2. コマンド プロンプトから、以下のコマンドを入力します。
   ```
   installation_executable -i silent -f
   ca-fedmanager-iwa-installer.properties
   ```
   -f

   Windows エージェントインストーラ プロパティ ファイルの名前を指定します。 プロパティ ファイルがインストールの実行可能ファイルと同じディレクトリにない場合は、プロパティ ファイルへの相対パスを指定します。

   -i

   インストール モードを指定します。

   インストールが実行され、プロパティ ファイルに設定が書き込まれます。

無人インストールが完了しました。

フェデレーション エージェントのアンインストール（Windows）

必要でなくなった場合は、Windows システムからフェデレーション エージェントを削除します。

次の手順に従ってください:

1. ［スタート］-［すべてのプログラム］-［CA］-［Federation Standalone］-［Uninstall CA SiteMinder® Federation Standalone Windows Authentication Agent］を選択します。

   ウィザードが開始します。
2. ウィザードの指示に従います。
3. 必要な場合、Program Files¥CA¥Federation Standalone¥connector ディレクトリに移動し、IWA フォルダおよびサブフォルダを削除します。
4. システムを再起動します。

Windows 認証用フェデレーション エージェントがシステムから削除されます。

フェデレーション エージェントのアンインストール（UNIX）

必要としなくなった場合、UNIX システムから Windows エージェントを削除します。

次の手順に従ってください:

1. コマンド ウィンドウを開きます。
2. Windows 認証用フェデレーション エージェントのホーム ディレクトリに移動します。
3. 以下のコマンドを入力します。

   ./ca-federation-iwa-uninstall.sh
4. 必要に応じて、残りのフォルダおよびすべてのサブフォルダを削除します。

フェデレーション エージェントがシステムから削除されます。

フェデレーション エージェントの r12.52 SP1 へのアップグレード

インストール プログラムは、Windows 認証用フェデレーション エージェントのバージョンをアップグレードすることもできます。 フェデレーション エージェントは、CA SiteMinder® Federation Standalone がすでにインストールされているシステムにインストールしてください。

重要: フェデレーション エージェントは CA SiteMinder® Federation Standalone と同じバージョンである必要があります。 フェデレーション システムをアップグレードする場合は、エージェントをアップグレードしてください。 アップグレードしないと、エージェントは正しく動作しません。

次の手順に従ってください:

1. 主要なフェデレーション システムが、アップグレード予定のエージェントと同じバージョンであることを確認します。 異なる場合、最初に CA SiteMinder® Federation Standalone をアップグレードします。
2. オペレーティング プラットフォーム用の Windows エージェント インストール実行可能ファイルを実行します。

   追加設定は必要ありません。
3. 設定ウィザード (P. 39) を実行します。

第 4 章: Windows 認証用フェデレーション エージェントの設定

設定ウィザードに必要な情報

フェデレーション エージェントをインストールした後、設定ウィザードを実行します。 Windows システムの場合、認証プロトコル（Kerberos または NTLM）を選択できます。 UNIX システムの場合、サポートされているプロトコルは Kerberos だけです。

注: 設定実行可能ファイルおよびフォルダ名には文字列 **iwa** が含まれます。 iwa は、統合 Windows 認証技術のサポートを参照します。

以下のパラメータは NTLM および Kerberos の設定に必要です。

重要: これらのパラメータの値は、管理 UI の展開設定で指定された値に一致する必要があります。 フェデレーション エージェントを設定する前に、これらの設定の値を CA SiteMinder® Federation Standalone 管理者から入手します。

Cookie ゾーン

シングル サインオン セキュリティ ゾーン名を指定します。

デフォルト： FED

値： 英数文字列

Cookie 名

オープン形式の Cookie の名前を指定します。

デフォルト： ""

値： 英数文字列

暗号化パスワード

Cookie の暗号化に対するキーを取得するためのパスワードを指定します。

デフォルト： ""

値： 英数文字列

暗号化変換タイプ

FIPS 準拠の暗号変換を指定します。

デフォルト： AES128/CBC/PKCS5Padding

制限： AES128/CBC/PKCS5Padding、AES192/CBC/PKCS5Padding、AES256/CBC/PKCS5Padding、3DES_EDE/CBC/PKCS5Padding

UseHMAC

ハッシュ メッセージ認証コード（HMAC）を使用するべきかどうかを指定します。

デフォルト：: false

制限： true または false

注: Windows を実行するシステム上で Kerberos 認証プロトコルを選択した場合、必要に応じてフェールオーバ オプションとして NTLM を選択できます。

Kerberos プロトコルを指定する場合、以下のパラメータの値を指定します。

KDC アドレス

Key Distribution Center （KDC）の完全修飾ドメイン名を指定します。

KDC レルム

KDC が置かれているシステムのドメイン名を指定します。

キータブの場所

キータブ ファイルのパスを指定します。 このファイルは、KDC システムに作成され、フェデレーション エージェント がインストールされているシステムに移動されます。

プリンシパル

HTTP/host.abc.com など、一意にサービスのインスタンスを識別するサービス プリンシパル名（SPN）を指定します。 HTTP はサービスの名前です。また、host.abc.com はサービスが存在するホストの名前です。

キータブの場所およびプリンシパル パラメータは login.conf ファイルに書き込まれています。 他のパラメータは IWAConnectorConfig.conf ファイルに書き込まれています。

注: login.conf ファイルを確認する場合は、isInitiator パラメータの値を変更しないでください。

Windows での設定ウィザードの実行

インストールの後にフェデレーション エージェントの設定ウィザードを実行します。 ウィザードは、認証プロトコルおよび Cookie 仕様に関連するパラメータの値を確立します。

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. 設定コマンド ファイルが置かれている場所に移動します。

   federation_installation_dir¥connectors¥IWA.
3. ca-fedmanager-iwa-config.cmd をダブルクリックします。

   設定ウィザードが起動します。
4. ウィザードのプロンプトに従います。

設定が完了しました。

UNIX での設定ウィザードの実行

フェデレーション エージェント用の設定ウィザードは、認証プロトコルおよび Cookie 仕様に関連するパラメータの値を確立します。

インストール処理を完了するために設定ウィザードを実行します。

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. 設定コマンド ファイルが置かれている場所に移動します。

   federation_installation_dir/connectors/IWA
3. スクリプト ca-fedmanager-iwa-config.sh を実行します。

   設定ウィザードが起動します。
4. ウィザードに提供されたプロンプトに従い、設定を完了します。

5. エージェントが正しく動作するように、以下のスクリプトを実行します。

   ```
   . /federation_install_dir/connectors/IWA/ca_fedmgr_iwa_env.ksh
   ```

6. フェデレーション サービスの再起動

   a. コマンド ウィンドウを開きます。

   b. 以下のスクリプトを実行します。

      federation_install_dir/fedmanager.sh stop

      federation_install_dir/fedmanager.sh start

   注: root ユーザとしてサービスを停止したり開始したりしないでください。 root 以外のユーザである必要があります。

無人設定（Windows）

ウィザードを使用してフェデレーション エージェントを設定した後、無人モードを使用して、同じシステムまたは別のシステムでエージェントを設定できます。 無人モード設定はユーザ介在を必要としません。 これは設定プロパティ ファイルを使用します。 要件に合わせて設定プロパティを変更できます。

次の手順に従ってください:

1. 設定実行可能ファイルが存在するディレクトリへ移動します。

   federation_installation_dir¥connectors¥IWA¥install_config_info

2. コマンド プロンプトから、以下のコマンドを入力します。

   ```
   ca-fedmanager-iwa-confg.bin i-silent -f ca-fedmanager-iwa-config.properties
   ```

   -f

   フェデレーション エージェント設定プロパティ ファイルの名前を指定します。 プロパティ ファイルが実行可能ファイルと同じディレクトリにない場合は、プロパティ ファイルへの相対パスを指定します。

   -i

   設定モードを指定します。 無人モードの場合、値は silent です。

無人設定が完了しました。

無人設定(UNIX)

ウィザードを使用してフェデレーション エージェントを設定した後、無人モードを使用して、同じシステムまたは別のシステムでエージェントを設定できます。 無人モード設定はユーザ介在を必要としません。 これは設定プロパティ ファイルを使用します。 要件に合わせて設定プロパティ ファイルを変更します。

次の手順に従ってください:

1. 設定実行可能ファイルが存在するディレクトリへ移動します。

   federation_installation_dir/connectors/IWA/install_config_info

2. コマンド プロンプトから、以下のコマンドを入力します。

   ```
   ca-fedmanager-iwa-confg.bin i-silent -f ca-fedmanager-iwa-config.properties
   ```

   -f

   フェデレーション エージェント設定プロパティ ファイルの名前を指定します。 プロパティ ファイルが実行可能ファイルと同じディレクトリにない場合は、プロパティ ファイルへの相対パスを指定します。

   -i

   設定モードを指定します。 無人モードの場合、値は silent です。

無人設定が完了しました。

フェデレーション エージェント用設定ファイルの変更(オプション)

設定ウィザードを実行した後、指定した値は IWAConnectorConfig.conf ファイルに書き込まれています。 いつでもウィザードを再実行して、ほとんどすべてのパラメータ値を変更できます。

いくつかのパラメータ値は設定ウィザードで設定されません。 以下の値を更新する場合、ファイルを直接変更できます。

context_cleanup_interval

クリーンアップ スレッドが期限切れコンテキストを削除し始める間隔を指定します。 この値を減少させると、クリーンアップの頻度は多くなり、メモリ可用性が向上します。

デフォルト： 30000 ミリ秒

値： 多くの未完了リクエストが予想される場合、値を低くすることを推奨します。

context_expiration_interval

コンテキストが期限切れであると仮定される時間を指定します。 NTLM については、コンテキストは、最大で 1 分有効です。

デフォルト： 60000 ミリ秒

値： このパラメータの値は、1 分未満には設定できません。 大きい値を指定すると、古くなったコンテキストがクリーンアップされないことがあります。

context_cleanup_thread_priority

コンテキスト クリーンアップ スレッドの優先度を指定します。

デフォルト： 5

値： 多くの未完了リクエストが予想される場合、優先度を高くすることを推奨します。

第 5 章: 委任認証セットアップ

フェデレーション エージェントは、CA SiteMinder® Federation Standalone との連携により、IWA コンテキストでユーザを認証できるようにします。フェデレーション エージェントはサードパーティ認証サービスとして機能するため、委任認証を使用するようにフェデレーション システムを設定します。

次の手順に従ってください:

1. 管理 UI にログインします。
2. 編集する SAML 1.1 または SAML 2.0 パートナーシップを選択します。プロデューサからコンシューマ パートナーシップ、または IDP から SP パートナーシップを編集します。
3. パートナーシップ ウィザードの以下のいずれかの手順に移動します。
   - SAML1.1: シングル サインオン
   - SAML 2.0： SSO と SLO
4. ［認証モード］を［委任］に設定します。
5. ［委任された認証タイプ］を［オープン形式の Cookie］に設定します。

   以下の情報に注意してください。
   - フェデレーション エージェントはオープン形式 Cookie に基づいた委任認証を必要とします。 SiteMinder コネクタを使用するようにフェデレーション システムを設定した場合、このオプションは使用できません。
   - エージェント設定中に指定した Cookie 設定の値は、管理 UI の展開設定の値に一致する必要があります。
6. 委任認証 URL を入力します。

   例： http://*hostname:portnum*/iwa/IWARedirect

委任認証が有効になります。

注: 委任認証の詳細については、「CA SiteMinder® Federation Standalone ガイド」を参照してください。

第 6 章: エージェント トレース ログ ファイルを使用したトラブルシューティング

トレース ログ ファイル（IWAConnectorTrace.log）を参照してフェデレーション エージェントをトラブルシューティングします。

トレース ログ ファイルをセットアップする方法

1. %FEDROOT%¥connectors¥IWA¥Config¥login.conf に移動します。
2. login.conf ファイルを開き、以下の変更を加えます。

   debug=true
3. フェデレーション サービスを再起動します。

ログ ファイルはディレクトリ %FEDROOT%¥logs¥connectors¥IWA¥IWAConnectorTrace.log に書き込まれます。

ログ ファイルには、以下のメッセージのいずれかが含まれることがあります。

症状:

構成ファイルが見つかりません。

解決方法:

IWAConnectorConfig.conf ファイルが *federation_install_dir*¥connectors¥IWA¥config フォルダに含まれていることを確認します。

症状:

無効な authtype が指定されました。

解決方法:

認証タイプが NTLM または Kerberos として指定されていることを確認します。 必要な場合、設定ウィザードを再度実行します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

NTLM は Windows 以外のプラットフォームではサポートされていません。

解決方法:

設定ウィザードを再度実行し、認証タイプとして Kerberos を指定します。この値を変更するために手動で設定ファイルを編集しないでください。

症状:

パスワードは IWAEncryptPassword ユーティリティを使用して暗号化します。

解決方法:

設定ウィザードを再度実行し、パスワードを入力します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

AuthType は空にはできません。

解決方法:

設定ウィザードを再度実行し、認証タイプを選択します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

暗号化キーは空にはできません。

解決方法:

設定ウィザードを再度実行し、暗号化キーを選択します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

無効な暗号化変換が指定されました。

解決方法:

設定ウィザードを再度実行し、別の暗号化変換を指定します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

無効な HMAC 値が指定されました。 true または false のみ指定できます。

解決方法:

設定ウィザードを再度実行し、HMAC を有効にするかどうかに対して true または false を選択します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

Kerberos 設定は無効です。

解決方法:

以下のパラメータが正しく指定されていることを確認します。

- Kerberos レルム
- KDC アドレス
- Kerberos 設定ファイルの場所（login.conf ファイル）

必要な場合、設定ウィザードを再度実行します。 これらの値を変更するために手動で設定ファイルを編集しないでください。

症状:

コンテキスト有効期限間隔を 1 分未満にすることはできません。

解決方法:

設定ウィザードを再度実行し、1 分より長いコンテキスト有効期限間隔を指定します。 この値を変更するために手動で設定ファイルを編集しないでください。

症状:

無効な設定です。 サーバが初期化されていません。

解決方法:

以下の値が正しく指定されていることを確認します。

- 認証タイプ
- 暗号化キー
- 暗号化変換
- Kerberos レルム
- KDC アドレス
- Kerberos 設定ファイルの場所（login.conf ファイル）

必要な場合、設定ウィザードを再度実行します。 これらの値を変更するために手動で設定ファイルを編集しないでください。

症状:

リクエストが IP アドレスで開始されているため、リクエストを中止します。

解決方法:

SSO リクエストが完全修飾ドメイン名で常に開始されていることを確認します。

症状:

Kerberos 初期化は失敗しました、設定パラメータを確認してください。

解決方法:

以下の値が正しく指定されていることを確認します。

- 認証タイプ
- 暗号化キー
- 暗号化変換
- Kerberos レルム
- KDC アドレス
- Kerberos 設定ファイルの場所（login.conf ファイル）

必要な場合、設定ウィザードを再度実行します。 これらの値を変更するために手動で設定ファイルを編集しないでください。

症状:

Cookie が見つかりませんでした。期限切れになったか削除されました。

解決方法:

ブラウザの設定が正しくない場合、このメッセージが表示されます。NTLM に対するブラウザ設定が完了しており、Cookie が無効ではないことを確認します。

症状:

NTLM 認証情報 Cookie が見つかりません。

解決方法:

ブラウザの設定が正しくない場合、このメッセージが表示されます。NTLM に対するブラウザ設定が完了しており、Cookie が無効ではないことを確認します。

症状:

ユーザ ドメインまたはワークステーション情報が見つかりません。

解決方法:

ドメイン名またはワークステーション名が NTLM タイプ 3 メッセージ内に見つからなかったとき、このメッセージが表示されます。このメッセージが変更されていないことを確認します。

症状:

ユーザはドメイン情報を入力していません。

解決方法:

NTLM 認証用のブラウザ設定が完了していることを確認します。プロンプト ベースの認証を使用している場合、ドメイン名がユーザ名と共に指定されていることを確認します。

症状:

Keytab k*eytab_path* のキーを使用して KDC *KDC_address* へのプリンシパル *SPN_Name* 用の認証を試行する間に、認証に失敗しました。

解決方法:

以下のパラメータが正しいことを確認します。

- プリンシパル名
- KDC アドレス
- keytab パス

症状:

ユーザ名が見つかりません。お使いのブラウザがフェデレーション サーバ以外のマシン上にあることを確認します。

解決方法:

SSO リクエストがアサーティング パーティのフェデレーション サーバ以外のシステムから常に行われていることを確認します。