CA Performance Center

Single Sign-On ユーザ ガイド

2.4

ca technologies

このドキュメント（組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。 本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、（i）本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。 いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。 また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

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。

目次

第 1 章: CA Performance Center での認証のカスタマイズ 7

CA Single Sign-On 7
- CA Performance Center 認証とセキュリティ 8
- 認証方式 8
- データ ソースのサポート 9
- Single Sign-On 設定ツール 9
- Single Sign-On 設定ファイルのバックアップ 10

Single Sign-On Web サイト設定の更新 11
CA Performance Center Web サイト設定の更新 17

第 2 章: LDAP 認証のセットアップ 21

LDAP サポート 21
認証メカニズムなしの LDAP 認証の有効化 22
GSSAPI を使用した LDAP サーバ接続の暗号化 28
暗号化メカニズムを使用した LDAP 認証の有効化 29
LDAPS 認証の有効化 35
- LDAP 証明書のインポート 41

LDAP 設定の検証 42

第 3 章: SAML 2.0 サポートのセットアップ 45

SAML 2.0 について 45
Single Sign-On での SAML 2.0 サポート 46
- SAML 2.0 の Single Sign-On サポートの仕組み 47

SAML 認証のセットアップ方法 49
- IdP アグリーメントの準備 50
- セキュリティ プロパティ ファイルの準備 50
- Single Sign-On での SAML 2.0 サポートの設定 52
- IdP の設定 56
- SAML 2.0 セットアップの完了 58

第 4 章: Single Sign-On での HTTPS の使用 59

SSL （Secure Sockets Layer）暗号化： HTTPS 59
CA Single Sign-On に HTTPS をセットアップする方法 60

SSL 証明書の設定 61
SSL 用のポートおよび Web サイトの設定 67
HTTPS を使用する CA Performance Center の設定 68
Single Sign-On 設定の更新およびサービスの再起動 71

第 5 章 : トラブルシューティング 75

ブラウザのエラー表示 75
ログ 76
監査ログの確認 77

用語集 79

第 1 章: CA Performance Center での認証のカスタマイズ

このセクションには、以下のトピックが含まれています。

CA Single Sign-On (P. 7)
Single Sign-On Web サイト設定の更新 (P. 11)
CA Performance Center Web サイト設定の更新 (P. 17)

CA Single Sign-On

Single Sign-On は、CA Performance Center およびすべてのサポート対象データ ソースで使用される認証スキームです。 ユーザは CA Performance Center に認証されると、再びサインインする必要なく、コンソールや登録されているデータ ソース間を移動できます。

Single Sign-On を使用すると、個別の製品インターフェース間を移動することができ、パフォーマンスやステータス データを分析するオペレータは、シームレスなドリルダウン操作が可能になります。たとえば、ユーザが CA Performance Center にログインし、次にデータ ソース インターフェースへのドリル ダウン パスに従う場合、そのユーザは再度ログインする必要がありません。

CA Performance Center は分散アーキテクチャを使用します。 Single Sign-On Web サイトのインスタンスは、サポート対象データ ソースまたは CA Performance Center がインストールされているすべてのサーバに自動的にインストールされます。 分散アーキテクチャによって、個別の CA データ ソース製品へのログインは、これらが実行しているサーバへのログインによって可能になります。

CA Performance Center 認証とセキュリティ

Single Sign-On は、CA Performance Center およびサポートされたデータ ソースへの認証サービスを提供します。 また、LDAP や SAML 2.0 などの外部認証スキームもサポートします。 このサポートにより、企業全体で CA Performance Center および他の CA データ ソース製品を同じ認証スキームへ統合できます。

Single Sign-On のセキュリティ監査機能は、ログイン ユーザとログイン日時に関する情報を記録します。 Linux サーバでは、ログは以下の場所に保存されます。
`[InstallationDirectory]/PerformanceCenter/sso/logs`

データ ソースがインストールされている Windows サーバでは、ログは以下のディレクトリに保存されます。
`[InstallationDirectory]¥Portal¥SSO¥logs`

認証方式

Single Sign-On コンポーネントでは、CA Performance Center およびデータ ソース製品でユーザ認証をサポートするログイン ページが提供されます。 Single Sign-On は以下の認証方式をサポートします。

- 製品認証（ユーザ アカウントに基づく）
- LDAP
- Security Assertion Markup Language (SAML) 2.0

CA Performance Center 管理者は、Single Sign-On の個別のインスタンスに対する設定を変更できます。 たとえば、Single Sign-On に LDAP 認証をセットアップできます。 また、Secure Sockets Layer （SSL）でオプションの暗号化を設定したり、デフォルト仮想ディレクトリを変更することもできます。

注: 分散アーキテクチャの結果、Single Sign-On Web サイトに対するすべての更新は、同じサーバ上で実行されているデータ ソース製品にのみ影響します。

データ ソースのサポート

CA Single Sign-On では、以下のデータ ソースをすべてサポートします。

- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

Single Sign-On 設定ツールは、Linux システムで実行されるように設計されました。 ただし、データ ソースがインストールされている Windows サーバにも展開できます。設定ツールを Windows サーバから起動する場合は、そのサーバの管理者としてログインします。

また、Linux 上で設定ツールを実行し、［リモート値］オプションを使用して、Windows 上で実行されるデータ ソースに設定手順を送信できます。

設定ツールは Linux 上で以下のディレクトリにインストールされます。
`[InstallationDirectory]/CA/PerformanceCenter`

データ ソースがインストールされている Windows サーバでは、設定ツールは以下のディレクトリにインストールされます。
`[InstallationDirectory]¥Portal¥SSO¥bin¥SsoConfig.exe`

Single Sign-On 設定ツール

Single Sign-On 設定ツールは、管理者が Single Sign-On Web サイトおよび関連する CA データ ソース製品の設定を調整できるようにするコマンド ライン アプリケーションです。

注: 設定ツールの［リモート値］オプションは、登録済みの各データ ソースに設定を反映します。 選択したサーバに伝達された設定を上書きするには、［ローカル上書き］オプションを使用します。

Single Sign-On 設定ツールは、Linux システムで実行されるように設計されました。 ただし、データ ソースがインストールされている Windows サーバにも展開できます。設定ツールを Windows サーバから起動する場合は、そのサーバの管理者としてログインします。

以下のタスクを実行するには、Single Sign-On 設定ツールを使用します。

- LDAP 認証を使用するようにデータ ソース製品を設定します。

  各製品の LDAP 設定はすべてこのツールを使用して更新されます。 また、現在の LDAP 設定をテストして設定を確認できます。

- SAML 2.0 認証を使用するようにデータ ソース製品を設定します。

  設定ツールの使用に加えて、管理者は、SAML 2.0 認証をセットアップするためにアイデンティティ プロバイダ上でいくつかの手順を実行する必要があります。

- 各製品によって参照される Single Sign-On 仮想ディレクトリを更新します。

  暗号化スキームを追加したか、Single Sign-On 仮想ディレクトリを変更した場合は、このツールを使用してデータ ソース製品を同期します。たとえば、変更されたサーバ上のデータ ソースは、正常に認証できないユーザのリダイレクト先に関する指示を必要とします。

- HTTPS を使用して、CA ソフトウェア製品を実行するサーバ間での通信を有効にします。

  この変更は、Single Sign-On の URL スキームおよびポートに影響します。Single Sign-On 設定ツールでは、管理者は必要なすべてのデータ ソース製品でこれらの値を容易に更新できます。

Single Sign-On 設定ファイルのバックアップ

設定ツールを使用して設定を変更する場合、ユーザの設定は設定ファイルに保存されます。 これらのファイルのバックアップ コピーを定期的に作成して、Single Sign-On 設定が失われないようにしてください。 rsync または別の推奨される方法（スクリプトなど）を使用して、これらのファイルを自動的に、またはアップグレード前にバックアップします。

バックアップ手順には、以下のファイルを追加します。

インストール ディレクトリ`/CA/PerformanceCenter/sso/start.ini`
インストール ディレクトリ`/CA/PerformanceCenter/PC/start.ini`

また、以下のディレクトリをバックアップします。

インストール ディレクトリ
/CA/PerformanceCenter/sso/webapps/sso/configuration
インストール ディレクトリ/CA/PerformanceCenter/sso/etc
インストール ディレクトリ/CA/PerformanceCenter/sso/conf
インストール ディレクトリ/CA/PerformanceCenter/PC/etc
インストール ディレクトリ/CA/PerformanceCenter/PC/conf

注: デフォルトのインストール ディレクトリは /opt/CA です。

Single Sign-On Web サイト設定の更新

Single Sign-On 設定ツールでは、Single Sign-On Web サイト用のデフォルト設定を変更できます。 たとえば、Single Sign-On Web サイト用の仮想ディレクトリを変更できます。 仮想ディレクトリは、CA サーバ間の通信に暗号化スキームを使用するために必要です。

ユーザのログイン試行時に Single Sign-On 動作に影響する、他の設定を変更できます。 一部のパラメータは、非アクティブ状態に応じてユーザを自動的にログ アウトするタイムアウト期間など、ユーザ インターフェースの動作にも影響します。

重要: Single Sign-On Web サイトの更新は、ソフトウェアの分散アーキテクチャにより、同じサーバで実行されている CA データ ソース製品にのみ影響します。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   ルートとしてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

3. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）
4. CA Performance Center を設定するために 1 を入力します。

   オプションを選択するように促されます。

```
SSO Configuration/CA Performance Center:
1. LDAP Authentication
2. SAML2 Authentication
3. Performance Center
4. Single Sign-On
5. Test LDAP
6. Export SAML2 Service Provider Metadata
Choose an option >
```

5. Single Sign-On の 4 を入力します。

   優先度を指定するように促されます。

   ［優先度］パラメータは CA Performance Center のみに適用されます。
6. 以下のオプションのいずれかを入力します。

   1. リモート値

   管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. ローカル上書き

   すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。

7. 以下のプロパティの 1 つ以上を入力します。 プロンプトが表示されたら、値を更新するために u を入力し、新しい値を指定します。

   1. **匿名ユーザ有効**

      データ ソースのインターフェースへのログインを試行するときに、サインイン ページが表示されるかどうかを指定します。 このパラメータが有効な場合、［匿名ユーザ ID］パラメータの値が必要です。 ログイン試行時には、サインイン ページは表示されません。 ユーザは、［匿名ユーザ ID］パラメータに関連付けられたユーザとしてログインされます。

      以下の条件が満たされるとき、［ローカル ホスト ユーザ有効］パラメータが優先されます。

      - ユーザは Single Sign-On サーバからログインしています。
      - ［ローカル ホスト ユーザ有効］パラメータと［匿名ユーザ有効］パラメータが両方とも有効になっています。

      デフォルト： 無効。

      注: 匿名ユーザのログインは Windows 認証よりも優先されます。

   2. **匿名ユーザ ID**

      ユーザを自動認証するために使用するユーザ名を、サインイン ページをバイパスして指定します。 このパラメータが使用されるのは、［匿名ユーザ有効］パラメータが有効な場合のみです。 以下の値のいずれかを選択します。

      - **1** - デフォルト管理者アカウント（管理者）用のユーザ名。
      - **2** - デフォルト ユーザ アカウント（ユーザ）用のユーザ名。
      - CA Performance Center データベースに存在する別のユーザ名。

3. **ローカル ホスト ユーザ サインイン ページ有効**

   Single Sign-On がインストールされているサーバからログインするときに、サインイン ページが表示されるかどうかを指定します。

   このパラメータが有効な場合、Single Sign-On サーバからログインしても、サインイン ページが表示されます。

   このパラメータが無効な場合、以下のルールが適用されます。

   - ［ローカル ホスト ユーザ有効］パラメータが有効である必要があります。
   - ［ローカル ホスト ユーザ ID］パラメータの値には、有効な製品ユーザ名が含まれる必要があります。この値は、サインイン ページを省略してソフトウェア インタフェースにログインするために使用されます。

   デフォルト： 無効。

4. **ローカル ホスト ユーザ有効**

   Single Sign-On サーバからログインするときに、サインイン ページを省略して自動的にサインインするかどうかを指定します。 このパラメータが有効な場合、［ローカル ホスト ユーザ ID］パラメータの値が必要です。

   - ［ローカル ホスト ユーザ サインイン ページ有効］パラメータが有効な場合、このパラメータは、ユーザ名やパスワードを入力せずにサインインをクリックする場合に使用されます。その後、［ローカル ホスト ユーザ ID］パラメータと関連付けられたユーザとしてソフトウェアにログインします。
   - ユーザがユーザ名とパスワードを指定する場合、それらの認証情報が認証に使用されます。
   - このパラメータが有効で、［ローカル ホスト ユーザ サインイン ページ有効］パラメータが無効な場合、サインイン ページは省略されます。 代わりにユーザは、［ローカル ホスト ユーザ ID］パラメータの値を使用して、インターフェースへログインされます。
   - ユーザが Single Sign-On サーバからログインしており、［ローカル ホスト ユーザ有効］および［匿名ユーザ有効］パラメータの両方が有効な場合、［ローカル ホスト ユーザ有効］パラメータが優先されます。

   デフォルト： 無効。

5. **ローカル ホスト ユーザ ID**

   ユーザが Single Sign-On サーバにログインするときに、サインインページをバイパスしてユーザを自動認証するために使用するユーザ ID を指定します。 このパラメータが使用されるのは、［ローカル ホスト ユーザ有効］パラメータが有効な場合のみです。 以下のいずれかの値を入力します。

   1 - デフォルト管理者アカウント（管理者）用のユーザ名。

   2 - デフォルト ユーザ アカウント（ユーザ）用のユーザ名。

6. **クッキー タイムアウト時間（分）**

   Single Sign-On クッキーが期限切れになるまでの時間（分）を指定します。ユーザがデータ ソース インターフェースでアクションを実行するたびに、クッキー タイムアウトがリセットされます。 タイムアウト時間が期限切れになると、ユーザはログアウトされ再認証する必要があります。

   デフォルト： 20 分

7. **暗号化復号キー**

   Single Sign-On クッキーの暗号化および復号化に使用するキーを指定します。

8. **暗号化アルゴリズム**

   Single Sign-On クッキーの暗号化および復号化に使用する暗号化アルゴリズムを指定します。 値に DES または AES のいずれかを指定します。

9. **失敗したスリープ秒数**

   サインイン試行に失敗した後に Single Sign-On アプリケーションが待機する秒数を指定します。

10. **ログイン状態の保存を有効化**

    ログイン状態を保存するチェック ボックスをサインイン ページに表示するかどうかを指定します。 ログイン状態の保存の設定では、クッキー タイムアウトが期限切れになるときにユーザが自動的にログアウトされるかどうかが決定されます。

    デフォルト： 有効

11. **ログイン状態の保存のタイムアウト日数**

    サインイン ページでログイン状態の保存を選択したユーザが再認証するまでに経過する日数を指定します。 このパラメータが使用されるのは、［ログイン状態の保存を有効化］パラメータが有効な場合のみです。 0 の値は、ログイン状態の保存の設定が期限切れにならないことを示します。ユーザは、データ ソース製品インターフェース内の［サイン アウト］リンクをクリックする必要があります。

12. **スキーム**

    Single Sign-On アプリケーションにアクセスするためにデータ ソース製品が使用できる URL スキームを指定します。SSL を使用している場合は、値に「https：」を指定します。

13. **ポート**

    Single Sign-On アプリケーションにアクセスするためにデータ ソース製品が使用できる URL ポートを指定します。

14. **仮想ディレクトリ**

    Single Sign-On 用の仮想ディレクトリの名前を指定します。

    デフォルト： SingleSignOn。

    注: 以前のパラメータのいずれかの値を変更しても、デフォルト値は置き換えられませんが、新しい値が優先されるようになります。新しい値は実際にはローカル上書きです。

8. デフォルト設定の変更を終了してから、b を入力します。
9. 前のオプション セットに戻ります。
10. 再度 b を入力して、最初のオプション セットに戻ります。
11. q を入力して、Single Sign-On 設定ツールを閉じます。

    Single Sign-On 設定ツールが閉じます。

    CA Performance Center は、ユーザが指定した新しい値を使用してすべての非認証ユーザを Single Sign-On Web サイトにダイレクトします。

CA Performance Center Web サイト設定の更新

Single Sign-On 設定ツールでは、CA Performance Center Web サイトおよび Web サービスのデフォルト設定を変更できます。 たとえば、CA Performance Center Web サービスに別のホストまたはポート番号を指定できます。 これらの設定は、CA Performance Center への接続方法を Single Sign-On アプリケーションに示します。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   ルートとしてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

3. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）

4. CA Performance Center を設定するために 1 を入力します。

   設定オプションを選択するように促されます。

   ```
   SSO Configuration/CA Performance Center:
   1. LDAP Authentication
   2. SAML2 Authentication
   3. Performance Center
   4. Single Sign-On
   5. Test LDAP
   6. Export SAML2 Service Provider Metadata
   Choose an option >
   ```

5. Performance Center の 3 を入力します。

   優先度を指定するように促されます。

   ［優先度］パラメータは CA Performance Center のみに適用されます。

6. 以下のオプションのいずれかを入力します。

   1. **リモート値**

      管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. **ローカル上書き**

      すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。

7. 以下のプロパティの 1 つ以上を入力します。 プロンプトが表示されたら、値を更新するために u を入力し、新しい値を指定します。

   1. Web **サービス スキーム**

      CA Performance Center Web サービスにアクセスするために Single Sign-On アプリケーションが使用できる URL スキームを指定します。 暗号化に SSL を使用している場合は、この値を「https」に変更します。

   2. Web **サービス ホスト**

      Single Sign-On アプリケーションが CA Performance Center Web サービスにアクセスできるホストの URL を指定します。

   3. Web **サービス ポート**

      CA Performance Center Web サービスにアクセスするために Single Sign-On アプリケーションが使用できる URL ポートを指定します。

   4. Web **サービス インベントリ**

      CA Performance Center インベントリ Web サービスにアクセスするために Single Sign-On アプリケーションが使用できる URL パスを指定します。

   5. Web **サービス製品リクエスト**

      CA Performance Center 製品リクエスト Web サービスにアクセスするために Single Sign-On アプリケーションが使用できる URL パスを指定します。

6. Web サイト スキーム

   CA Performance Center にアクセスするために Single Sign-On アプリケーションが使用できる URL スキームを指定します。SSL をセットアップした場合は、「https://」を使用します。

7. Web サイト ホスト

   CA Performance Center にアクセスするために Single Sign-On アプリケーションが使用できる URL ホストを指定します。

8. Web サイト ポート

   CA Performance Center にアクセスするために Single Sign-On アプリケーションが使用できる URL ポートを指定します。

9. Web サイト パス

   CA Performance Center にアクセスするために Single Sign-On アプリケーションが使用できる URL パスを指定します。

10. SMTP 有効

    CA Performance Center オペレータがレポートおよびイベント通知を電子メールできるように、Simple Mail Transfer Protocol （SMTP）を有効化するかどうかを指定します。

    デフォルト： 無効。

11. SMTP サーバ アドレス

    SMTP サーバの IP アドレスです。

    デフォルト： 無効。

12. SMTP ポート:

    SMTP リクエストに使用するポートを指定します。

    デフォルトは、ポート 25 です。

13. SMTP SSL

    CA Performance Center または他の CA データ ソース製品から電子メールを送信するときに、SSL 暗号化を使用するかどうかを指定します。 このオプションを有効にする前に、システム上で SSL が正しくセットアップされていることを確認します。

    デフォルト： 無効。

14. 電子メール返信アドレス

    CA Performance Center によって生成される電子メール メッセージに使用する返信用アドレスを指定します。 値を更新するために u を入力し、電子メール アドレスを指定します。
    「username@mydomain.com」の形式を使用します。

15. 電子メール形式

    CA Performance Center によって送信される電子メール メッセージに使用する形式を指定します。 値を更新するには u を入力して、HTML またはテキストのいずれかを指定します。

16. SMTP ユーザ名

    電子メール サーバが SMTP リクエストのチャレンジを行うときに使用するユーザ名を指定します。 ユーザ名を指定するか、またはクライアント側認証を無効にするために空の文字列を指定します。

17. SMTP パスワード

    電子メール サーバが SMTP リクエストのチャレンジを行うときに使用するユーザ名を指定します。 任意の有効なパスワードを指定します。 ［SMTP ユーザ名］パラメータは必須です。

8. デフォルト設定の変更を終了してから、b を入力します。

   前のオプション セットに戻ります。

9. オプションの最初のセットに戻るために再度 b を入力します。

10. 終了するために q を入力します。

    Single Sign-On 設定ツールが閉じます。

    CA Performance Center は、指定された新しい値を使用して、すべてのユーザを Single Sign-On Web サイトに転送します。

第 2 章: LDAP 認証のセットアップ

このセクションには、以下のトピックが含まれています。

LDAP サポート (P. 21)
認証メカニズムなしの LDAP 認証の有効化 (P. 22)
GSSAPI を使用した LDAP サーバ接続の暗号化 (P. 28)
暗号化メカニズムを使用した LDAP 認証の有効化 (P. 29)
LDAPS 認証の有効化 (P. 35)
LDAP 設定の検証 (P. 42)

LDAP サポート

Single Sign-On では、ユーザの環境で実行中の Lightweight Directory Access Protocol（LDAP）サーバへのオペレータ認証を可能にする、LDAP 統合が提供されます。 認証後、管理者が指定できるユーザ アカウント： 事前定義済みユーザ アカウントまたはカスタム アカウントのトいずれかにマップされます。

Single Sign-On 設定ツールでは、Single Sign-On サーバの LDAP サーバへの接続方法を正確に指定できます。 また、機密データの保護中に、個別の CA Performance Center ユーザをそれらのワークフローをサポートするユーザ アカウントにマップすることもできます。

注: シングル サインオン設定ツールでの変更は、新しく作成された LDAP ユーザにのみ影響します。 CA Performance Center 内に登録された既存の LDAP ユーザには適用されません。

Single Sign-On 設定ツールで利用可能な LDAP パラメータにより、CA Infrastructure Management とすべての登録済みデータ ソースを既存の認証スキームへ統合できます。 たとえば、LDAP サーバは、CA Performance Center 内の単一のカスタム ユーザ アカウントにマップされるユーザのグループを許可できます。 実際のアカウント名および LDAP グループは広範囲にカスタマイズできます。 ［検索範囲］パラメータでは、ユーザがディレクトリ検索の実行方法を決定できます。 また、ユーザの検証時に考慮されるユーザ アカウント プロパティを選択できます。

認証メカニズムなしの LDAP 認証の有効化

登録済みデータ ソースで同じ LDAP スキームを使用してユーザを認証するように指示するには、Single Sign-On 設定ツールを使用します。 Single Sign-On 設定ツールでは、CA サーバを LDAP サーバに安全に接続できるようにするパラメータを指定できます。 設定ツールを使用すると、LDAP カタログのユーザと、CA Performance Center 内の事前定義済みユーザ アカウントまたはカスタム ユーザ アカウントのいずれかを関連付けることもできます。

GSSAPI などの認証メカニズムを使用 (P. 28)している場合、LDAP 認証を有効にするための手順はわずかに異なります。認証メカニズムなしで、サービス アカウントを使用して LDAP サーバにバインドする必要があります。このアカウントには、LDAP サーバへの読み取りおよび検索のアクセス権が必要です。 接続ユーザの完全な DN （識別名）を提供する必要があります。また、［ユーザ バインド］パラメータを有効にする必要があります。

シングル サインオンは、［接続ユーザ］および［接続パスワード］パラメータに指定した認証情報を使用して、LDAP サーバにバインドします。次にシングル サインオンは、［検索文字列］パラメータに指定された文字列に基づいてディレクトリ検索を実行します。検索結果には、ユーザの DN が含まれます。シングル サインオンは、この DN とパスワードを使用して LDAP サーバへの 2 回目のバインドを実行します。

重要: 認証メカニズムが使用されない場合は、LDAP サーバに対して SSL 接続を確立することを強くお勧めします。 そうしないと、パスワードがクリア テキストで LDAP サーバに転送されます。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   root としてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   InstallationDirectory/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

3. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）
4. CA Performance Center を設定するために 1 を入力します。

   オプションを選択するように促されます。
5. LDAP 認証に対する 1 を入力します。

   優先度を指定するように促されます。

   優先度パラメータは CA Performance Center のみに適用されます。
6. 以下のオプションのいずれかを入力します。

   1. **リモート値**

      管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. **ローカル上書き**

      すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。
7. 以下のプロパティの 1 つ以上を入力します。 プロンプトが表示されたら、値を更新するために u を入力し、新しい値を指定します。

   1. **接続ユーザ**

      LDAP サーバに接続するためにログイン サーバが使用するユーザ ID（この場合、サービス アカウントのユーザ ID）を定義します。この LDAP ユーザ名はサーバにバインドするために使用されます。

      重要: GSSAPI などの認証メカニズムを使用していない場合、このパラメータには、LDAP サーバの読み取りおよび検索アクセス権を持つサービス アカウントが必要です。

2. **接続パスワード**

   ログイン サーバで LDAP サーバへの接続に使用するパスワードを定義します。

   例： ログイン サーバで固定されたアカウントを使用する場合は、以下の例のようなテキストを入力します。

   `SomePassword`

3. **検索ドメイン**

   CA Single Sign-On が接続する LDAP サーバおよびポートを特定します。 ユーザ アカウントの認証情報を確認する場合にディレクトリツリー内でユーザを検索する場所も特定します。 文字列内でサーバの後にポート番号を指定しない場合、ポート 389 が使用されます。

   検索ドメインには以下の形式を使用します。

   `LDAP://`*`ldap_server`*`:`*`port`*`/`*`path_to_search`*

   注: 検索パスは*必須*です。

4. **検索文字列**

   ユーザの正しいレコードを検索するために使用する条件を指定します。 ［検索範囲］パラメータと共に動作します。 LDAP ユーザのサブセットのみがログインできるようにする場合は、検索文字列を使用して、レコード内の複数のプロパティを検索できます。 このパラメータの値には、任意の有効な LDAP 検索条件を含めることができます。

   例：

   `(saMAccountName={0})`

5. 検索範囲

ユーザの正しいレコードを検索するために使用する条件を指定します。［検索文字列］パラメータと共に使用されます。LDAP サーバがユーザ アカウントに対して実行する検索の範囲を決定します。以下の値のいずれかを入力します。

onelevel

現在のディレクトリを検索に含めます。現在のディレクトリでオブジェクトと一致し、ディレクトリ内でさらに予期しない一致が生じないようにします。

subtree

すべてのサブディレクトリを検索に含めます。ほとんどのインストール環境にお勧めします。

ベース

検索をベース オブジェクトに制限します。

6. ユーザ バインド

指定した認証情報を検証するために、ユーザの識別名（DN）およびパスワードを使用して追加の認証ステップ（バインド）を実行するかどうかを指定します。

重要：手順 1 と 2 でサービス アカウントを入力した場合、このパラメータは「有効」に設定する必要があります。

デフォルト： 無効。

7. 暗号化

LDAP サーバに再度バインドするときに使用する認証メカニズムを指定します。

デフォルト： Simple

指定可能な値： Simple、GSSAPI、DIGEST-MD5

8. アカウント ユーザ

グループ メンバシップのない検証済みの LDAP ユーザをマップする CA Performance Center デフォルト アカウントを指定します。［アカウント パスワード］パラメータと共に動作します。 有効なユーザがグループ定義に一致しない場合、このパラメータに対して指定されたデフォルト ユーザ ID でログインされます。

すべてのユーザが自分のユーザ名でログインできるようにするには、以下のように入力します。

- {saMAccountName}
- {saMAccountName} または {CN}

注: ［アカウント ユーザ］パラメータは、このユーザ用のディレクトリ エントリからのフィールドに対応します。 通常、値はユーザの検索フィルタに一致します。

9. アカウント ユーザ デフォルト クローン

検証済みの LDAP ユーザが［グループ］パラメータに指定されていないグループのメンバである場合に、クローンを作成するユーザ アカウントを指定します。

例： そのようなユーザに最小の権限を付与する場合は、「user」を入力します。

注: 既存のユーザ アカウントが必要です。

10. グループ

選択したユーザ アカウントまたはアカウントのグループに対して処理するデフォルト アカウントを決定できます。

例： グループのすべてのメンバが管理者アカウントを使用してログインできるようにするには、以下のように入力します。

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

11. タイムアウト

LDAP サーバへの認証を確認をする間に、CA Performance Center が待機する時間を指定します。 認証確認がタイムアウトになる場合、ログインしようとするユーザはアクセスが拒否されます。 エラーを参照するには、SSOService.log ファイルを開きます。 タイムアウトのデフォルト値は 10000 です。

8. LDAP ステータスが［有効］に設定されていることを確認します。LDAP ステータスが［無効］に設定されている場合、認証は内部 Performance Center ユーザ データベースを使用します。
9. 終了するために q を入力します。

   設定ツールが閉じます。

設定例

1. 接続ユーザ： CN=********,OU=Role-Based,OU=North America,DC=ca,DC=com [サービス アカウントの完全な DN]
2. 接続パスワード： ******* [サービス アカウントのパスワード]
3. 検索ドメイン： LDAP://******.ca.com/DC=ca,DC=com
4. 検索文字列： (sAMAccountName={0})
5. 検索範囲： Subtree
6. ユーザ バインド： 有効
7. 暗号化： false
8. アカウント ユーザ： {sAMAccountName}
9. アカウント ユーザ デフォルト クローン： user
10. グループ： すべての従業員（All Employees）
11. Krb5ConfigFile: krb5.conf

GSSAPI を使用した LDAP サーバ接続の暗号化

CA Single Sign-On では、DIGEST-MD5 または GSSAPI を使用して、暗号化された接続をサポートします。 ディレクトリ サーバへの暗号化された接続を使用する場合、LDAP サーバにバインドするためのサービス アカウント（Single Sign-On 設定ツールで設定した UserBind パラメータ）を使用する必要はありません。

暗号化に GSSAPI を使用するには、設定ファイル内のいくつかの設定を変更する必要があります。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   ルートとしてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリに移動します。
   `[Installation Dir]/webapps/sso/Configuration/`

3. そのディレクトリ内の krb5.conf ファイルを編集用に開きます。

4. 以下の必須パラメータを設定します。

```
[libdefaults]
        default_realm = CA.COM
[realms]
        CA.COM  = {
               kdc = EXAMPLE.CA.COM
               default_domain = CA.COM
}

[domain_realm]
       .CA.COM = CA.COM
}
```

   各値は以下のとおりです。

   [libdefaults]

   Kerberos V5 ライブラリのデフォルト値が含まれています。

   default_realm

   サブドメインおよびドメイン名を Kerberos 領域名にマップします。プログラムは、完全修飾ドメイン名に基づいてホストの領域を決定できます。 この例では、デフォルトの領域は CA.COM です。

realms

Kerberos 領域名に関する情報が含まれています。Kerberos サーバの場所を記述し、その他の領域固有の情報が含まれます。

kdc

認証サービスをサポートする Kerberos キー配布センターです。例: EXAMPLE.CA.COM

default_domain

デフォルト IP ドメインです。 例： CA.COM

注: 必要に応じて、Active Directory または LDAP の管理者に krb5.conf ファイルを提供してもらうか、または krb5.conf ファイル作成の支援を依頼します。

5. 変更を保存します。
6. 「暗号化メカニズムを使用した LDAP 認証の有効化 (P. 29)」の手順に従って、CA Single Sign-On を使用した LDAP 認証を設定します。

暗号化メカニズムを使用した LDAP 認証の有効化

登録済みデータ ソースで同じ LDAP スキームを使用してユーザを認証するように指示するには、Single Sign-On 設定ツールを使用します。 Single Sign-On 設定ツールでは、CA サーバを LDAP サーバに安全に接続できるようにするパラメータを指定できます。 Digest-MD5 または GSSAPI を使用して LDAP サーバへの接続を暗号化する場合、ユーザが指定した単一のバインド操作が発生します。

設定ツールを使用すると、LDAP カタログのユーザと、CA Performance Center 内の事前定義済みユーザ アカウントまたはカスタム ユーザ アカウントのいずれかを関連付けることもできます。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   root としてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   InstallationDirectory/CA/PerformanceCenter

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

3. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）

4. CA Performance Center を設定するために 1 を入力します。

   オプションを選択するように促されます。

5. LDAP Authentication の 1 を入力します。

   優先度を指定するように促されます。

   ［優先度］パラメータは CA Performance Center のみに適用されます。

6. 以下のオプションのいずれかを入力します。

   1. **リモート値**

      管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. **ローカル上書き**

      すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。

7. 以下のプロパティの 1 つ以上を入力します。 プロンプトが表示されたら、値を更新するために u を入力し、新しい値を指定します。

   1. **接続ユーザ**

      ログイン サーバで LDAP サーバへの接続に使用するユーザ ID を定義します。この LDAP ユーザ名はサーバにバインドするために使用されます。 サービス アカウントは通常、GSSAPI などの認証メカニズムを使用する接続では必要ではありません。

      例： ログイン サーバで固定されたアカウントを使用する場合は、以下の構文でテキストを入力します。

      ```
      CN=The User,cn=Users,dc=domain,dc=com
      ```

      または、この接続では認証メカニズムを使用しているので、以下の値を入力できます。

      ```
      {0}
      ```

      複雑な設定では、ユーザを識別するためにユーザ プリンシパル名が必要です。 「{0}」を指定し、その電子メール アドレスをドメイン名として使用します。 以下に例を示します。

      ```
      {0}@domain.com
      ```

      LDAP サーバでは通常、暗号化された接続の完全な DN は必要ではありません。

      注: セキュリティのため、接続ユーザを静的アカウントにしないでください。 LDAP 認証では、サーバにバインドする場合にのみパスワードが確認されます。 静的アカウントを使用すると、LDAP ツリー内に存在するすべてのユーザが任意のパスワードでログインできます。

   2. **接続パスワード**

      ログイン サーバで LDAP サーバへの接続に使用するパスワードを定義します。

      例： ログイン サーバで固定されたアカウントを使用する場合は、以下の例のようなテキストを入力します。

      ```
      SomePassword
      ```

      または、この接続では認証メカニズムを使用しているので、以下の値を入力できます。

      ```
      {1}
      ```

3. **検索ドメイン**

   CA Single Sign-On が接続する LDAP サーバおよびポートを特定します。 ユーザ アカウントの認証情報を確認する場合にディレクトリ ツリー内でユーザを検索する場所も特定します。 文字列内でサーバの後にポート番号を指定しない場合、ポート 389 が使用されます。

   検索ドメインには以下の形式を使用します。

   `LDAP://ldap_server:port/path_to_search`

   注: 検索パスは*必須*です。

4. **検索文字列**

   ディレクトリ内で正しいユーザを検索するために使用する条件を指定します。［検索範囲］パラメータと共に動作します。LDAP ユーザのサブセットのみがログインできる場合、検索文字列を使用して複数プロパティのレコードを検索できます。 このパラメータの値には、任意の有効な LDAP 検索条件を含めることができます。

   例：

   ```
   (saMAccountName={0})
   ```

5. **検索範囲**

   ユーザの正しいレコードを検索するために使用する条件を指定します。 ［検索文字列］パラメータと共に使用されます。 LDAP サーバがユーザ アカウントに対して実行する検索の範囲を決定します。以下の値のいずれかを入力します。

   onelevel

   現在のディレクトリを検索に含めます。現在のディレクトリでオブジェクトと一致し、ディレクトリ内でさらに予期しない一致が生じないようにします。

   subtree

   すべてのサブディレクトリを検索に含めます。ほとんどのインストール環境にお勧めします。

   base

   検索をベース オブジェクトに制限します。

6. **ユーザ バインド**

   指定した認証情報を検証するために、ユーザの識別名（DN）およびパスワードを使用して追加の認証ステップ（バインド）を実行するかどうかを指定します。

   デフォルト： 無効。 この値は暗号化された接続で指定できます。

7. **暗号化**

   LDAP サーバに再度バインドするときに使用する認証メカニズムを指定します。

   この場合（すなわち、認証メカニズムを使用）、LDAP サーバのメカニズムに基づいて、「GSSAPI」または「DIGEST-MD5」を入力します。

   デフォルト： Simple

   指定可能な値： Simple、GSSAPI、DIGEST-MD5

8. **アカウント ユーザ**

   グループ メンバシップのない検証済みの LDAP ユーザをマップする CA Performance Center デフォルト アカウントを指定します。［アカウント パスワード］パラメータと共に動作します。 有効なユーザがグループ定義に一致しない場合、このパラメータに対して指定されたデフォルト ユーザ ID でログインされます。

   すべてのユーザが自分のユーザ名でログインできるようにするには、以下のように入力します。

   - {saMAccountName}
   - {saMAccountName} または {CN}

   注: ［アカウント ユーザ］パラメータは、このユーザ用のディレクトリ エントリからのフィールドに対応します。 通常、値はユーザの検索フィルタに一致します。

9. **アカウント ユーザ デフォルト クローン**

   検証済みの LDAP ユーザが［グループ］パラメータに指定されていないグループのメンバである場合に、クローンを作成するユーザ アカウントを指定します。

   例： そのようなユーザに最小の権限を付与する場合は、「user」を入力します。

   注: 既存のユーザ アカウントが必要です。

10. グループ

    選択したユーザ アカウントまたはアカウントのグループに対して処理するデフォルト アカウントを決定できます。

    例： グループのすべてのメンバが管理者アカウントを使用してログインできるようにするには、以下のように入力します。

    ```
    <LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
    Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
    userClone="admin"/></LDAPGroups>
    ```

11. タイムアウト

    LDAP サーバへの認証を確認をする間に、CA Performance Center が待機する時間を指定します。 認証確認がタイムアウトになる場合、ログインしようとするユーザはアクセスが拒否されます。 エラーを参照するには、SSOService.log ファイルを開きます。 タイムアウトのデフォルト値は 10000 です。

8. LDAP ステータスが［有効］に設定されていることを確認します。 LDAP ステータスが［無効］に設定されている場合、認証は内部 Performance Center ユーザ データベースを使用します。
9. 終了するために q を入力します。

   設定ツールが閉じます。

設定例

1. SSO 設定/CA Performance Center/LDAP 認証/リモート値：
2. 接続ユーザ： {0}
3. 接続パスワード： {1}
4. 検索ドメイン： LDAP://******.ca.com/DC=ca,DC=com
5. 検索文字列： (sAMAccountName={0})
6. 検索範囲： Subtree
7. ユーザ バインド： 無効
8. 暗号化： DIGEST-MD5
9. アカウント ユーザ： {sAMAccountName}
10. アカウント ユーザ デフォルト クローン： user
11. グループ： すべての従業員（All Employees）
12. Krb5ConfigFile: krb5.conf

詳細:

GSSAPI を使用した LDAP サーバ接続の暗号化 (P. 28)

LDAPS 認証の有効化

安全なユーザ認証のため、登録済みデータ ソースに LDAP over SSL（LDAPS）を使用するよう指示するには、Single Sign-On 設定ツールを使用します。デフォルトでは、LDAP トラフィックの送信は保護されません。認証機関（CA）からの証明書をインストールして、LDAPS を有効にします。 CA Single Sign-On では、Java 信頼済みキーストアに証明書をインポートする必要があります。

Single Sign-On 設定ツールでは、CA サーバを LDAP サーバに安全に接続できるようにするパラメータを指定できます。設定ツールを使用すると、LDAP カタログのユーザと、CA Performance Center 内の事前定義済みユーザ アカウントまたはカスタム ユーザ アカウントのいずれかを関連付けることもできます。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   root としてログインするか、または「sudo」コマンドでログインします。

2. トピック「LDAP 証明書のインポート（P. 41）」の手順に従い証明書を入手し、Java キーストアにインポートします。

3. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   InstallationDirectory/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

4. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）
5. CA Performance Center を設定するために 1 を入力します。

   オプションを選択するように促されます。
6. LDAP Authentication の 1 を入力します。

   優先度を指定するように促されます。

   ［優先度］パラメータは CA Performance Center のみに適用されます。
7. 以下のオプションのいずれかを入力します。

   1. **リモート値**

      管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. **ローカル上書き**

      すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。

8. 以下のプロパティの 1 つ以上を入力します。 プロンプトが表示されたら、値を更新するために u を入力し、新しい値を指定します。

   1. **接続ユーザ**

      ログイン サーバで LDAP サーバへの接続に使用するユーザ ID を定義します。この LDAP ユーザ名はサーバにバインドするために使用されます。 サービス アカウントは通常、GSSAPI などの認証メカニズムを使用する接続では必要ではありません。

      例： ログイン サーバで固定されたアカウントを使用する場合は、以下の構文でテキストを入力します。

      ```
      CN=The User,cn=Users,dc=domain,dc=com
      ```

      または、この接続では認証メカニズムを使用しているので、以下の値を入力できます。

      ```
      {0}
      ```

      複雑な設定では、ユーザを識別するためにユーザ プリンシパル名が必要です。 「{0}」を指定し、その電子メール アドレスをドメイン名として使用します。 たとえば、以下のようになります。

      ```
      {0}@domain.com
      ```

      LDAP サーバでは通常、暗号化された接続の完全な DN は必要ではありません。

      注: セキュリティのため、接続ユーザを静的アカウントにしないでください。 LDAP 認証では、サーバにバインドする場合にのみパスワードが確認されます。 静的アカウントを使用すると、LDAP ツリー内に存在するすべてのユーザが任意のパスワードでログインできます。

   2. **接続パスワード**

      ログイン サーバで LDAP サーバへの接続に使用するパスワードを定義します。

      例： ログイン サーバで固定されたアカウントを使用する場合は、以下の例のようなテキストを入力します。

      ```
      SomePassword
      ```

      または、この接続では認証メカニズムを使用しているので、以下の値を入力できます。

      ```
      {1}
      ```

3. **検索ドメイン**

   CA Single Sign-On が接続する LDAP サーバおよびポートを特定します。 ユーザ アカウントの認証情報を確認する場合にディレクトリ ツリー内でユーザを検索する場所も特定します。 文字列内でサーバの後にポート番号を指定しない場合、ポート 389 が使用されます。

   検索ドメインには以下の形式を使用します。
   LDAPS:*//ldap_server*:*port/path_to_search*

   注: 検索パスは必須です。

   LDAP サーバへの SSL 接続を確立するには、636、または LDAP サーバの別の SSL 接続ポートを使用します。

   ```
   LDAPS://LDAP Server:636/OU=Users,OU=North
   America,DC=ca,DC=com
   ```

4. **検索文字列**

   ディレクトリ内で正しいユーザを検索するために使用する条件を指定します。［検索範囲］パラメータと共に動作します。LDAP ユーザのサブセットのみがログインできる場合、検索文字列を使用して複数プロパティのレコードを検索できます。 このパラメータの値には、任意の有効な LDAP 検索条件を含めることができます。

   例：

   ```
   (saMAccountName={0})
   ```

5. **検索範囲**

   ユーザの正しいレコードを検索するために使用する条件を指定します。 ［検索文字列］パラメータと共に使用されます。 LDAP サーバがユーザ アカウントに対して実行する検索の範囲を決定します。以下の値のいずれかを入力します。

   onelevel

   現在のディレクトリを検索に含めます。現在のディレクトリでオブジェクトと一致し、ディレクトリ内でさらに予期しない一致が生じないようにします。

   subtree

   すべてのサブディレクトリを検索に含めます。ほとんどのインストール環境にお勧めします。

   base

   検索をベース オブジェクトに制限します。

6. **ユーザ バインド**

   指定した認証情報を検証するために、ユーザの識別名（DN）およびパスワードを使用して追加の認証ステップ（バインド）を実行するかどうかを指定します。

   デフォルト： 無効。 この値は暗号化された接続で指定できます。

7. **暗号化**

   （オプション） LDAP サーバに再度バインドするときに使用する認証メカニズムを指定します。

   LDAPS では、デフォルト（単純認証）を使用できます。

8. **アカウント ユーザ**

   グループ メンバシップのない検証済みの LDAP ユーザをマップする CA Performance Center デフォルト アカウントを指定します。 ［アカウント パスワード］パラメータと共に動作します。 有効なユーザがグループ定義に一致しない場合、このパラメータに対して指定されたデフォルト ユーザ ID でログインされます。

   すべてのユーザが自分のユーザ名でログインできるようにするには、以下のように入力します。

   - {saMAccountName}
   - {saMAccountName} または {CN}

   注: ［アカウント ユーザ］パラメータは、このユーザ用のディレクトリ エントリからのフィールドに対応します。 通常、値はユーザの検索フィルタに一致します。

9. **アカウント ユーザ デフォルト クローン**

   検証済みの LDAP ユーザが［グループ］パラメータに指定されていないグループのメンバである場合に、クローンを作成するユーザ アカウントを指定します。

   例： そのようなユーザに最小の権限を付与する場合は、「user」を入力します。

   注: 既存のユーザ アカウントが必要です。

10. グループ

    選択したユーザ アカウントまたはアカウントのグループに対して処理するデフォルト アカウントを決定できます。

    例： グループのすべてのメンバが管理者アカウントを使用してログインできるようにするには、以下のように入力します。

    ```
    <LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
    Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
    userClone="admin"/></LDAPGroups>
    ```

9. 終了するために q を入力します。

   設定ツールが閉じます。

設定例

1. SSO 設定/CA Performance Center/LDAP 認証/リモート値
2. 接続ユーザ： {0}
3. 接続パスワード： {1}
4. 検索ドメイン： LDAPS://******.ca.com:636/OU=Users,OU=North America,DC=ca,DC=com
5. 検索文字列： (sAMAccountName={0})
6. 検索範囲： Subtree
7. ユーザ バインド： 無効
8. 暗号化： 単純
9. アカウント ユーザ： {sAMAccountName}
10. アカウント ユーザ デフォルト クローン： user
11. グループ： すべての従業員（All Employees）
12. Krb5ConfigFile: krb5.conf

LDAP 証明書のインポート

LDAPS で実行するには、Java キーストアへ LDAP 証明書をインポートする必要があります。

SSL 証明書がない場合は、keytool コマンドを使用して証明書を生成できます。 この手順では、CA から証明書をインポートし、キーストアにインストールする方法を説明します。

次の手順に従ってください:

1. LDAP サーバ管理者から証明書を取得します。
2. 以下のコマンドを使用して、この証明書を Java の信頼された証明書キーストアにインポートします。

   ```
   keytool -importcert -keystore installDirectory/jre/
   lib/security/cacerts -storepass cacertspasswd -alias
   alias -file filename.cer
   ```

   keystore

   キーストア ファイル（.ks）の場所

   cacertspasswd

   cacerts キーストアのパスワードを指定します。

   デフォルト： changeit

   filename.cer

   証明書のファイル名
3. cacerts ファイルのバックアップを作成します。
4. （オプション）セキュリティを強化するために、以下のコマンドを使用して、java の信頼された証明書キーストアのパスワードを変更します。

   ```
   keytool -storepasswd -keystore installDirectory/
   jre/lib/security/cacerts
   ```

   既存のパスワードと新しいパスワードの入力を求められます。

5. インポートした証明書が利用可能であることを確認します。 以下のコマンドを使用します。

   ```
   keytool -importcert -keystore installDirectory/jre/
   lib/security/cacerts
   ```

   重要: Web サービスを有効にするには、証明書が cacerts キーストアに存在する必要があります。 そうでない場合、PKIX は証明書を見つけることができなかったというエラーがログに表示されます。

LDAP 設定の検証

Single Sign-On 設定ツールでは、入力した LDAP 設定をテストできます。 LDAP 認証が正しく設定されることを確認できます。LDAP テスト スクリプトにより、LDAP 認証に現在の設定を使用してテストするユーザ名とパスワードの組み合わせを指定するように求められます。 設定ツールを使用して LDAP 認証設定をまだ変更していない場合、デフォルトが使用されます。

次の手順に従ってください:

1. CA Performance Center またはサポート対象データ ソース製品がインストールされているサーバにログインします。

   ルートとしてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

3. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）
4. CA Performance Center を設定するために 1 を入力します。

   オプションを選択するように促されます。
5. ［LDAP のテスト］オプションに 5 を入力します。

   ユーザ名の入力を求められます。
6. LDAP を使用して認証できると確認済みのユーザ名およびパスワードを入力します。

   LDAP サーバに接続してユーザ アカウントを検証するように LDAP 認証を設定すると、入力したパラメータが Single Sign-On で使用されます。テストが成功すると、多数のステップがログに記録されます。

   認証が成功したか失敗したかを示すメッセージがレポートされます。
7. 終了するために q を入力します。

第 3 章: SAML 2.0 サポートのセットアップ

このセクションには、以下のトピックが含まれています。

SAML 2.0 について (P. 45)
Single Sign-On での SAML 2.0 サポート (P. 46)
SAML 認証のセットアップ方法 (P. 49)

SAML 2.0 について

Security Assertion Markup Language（*SAML*）は XML に基づいたセキュリティ プロトコルです。 基本概念には、セキュア ドメインへのアクセスをリクエストする対象である個人またはコンピュータに関するセキュリティ アサーションの交換が含まれます。アサーションには、対象が特定のリソースにアクセスできるかどうかと、ポリシー ストアなどの外部データ ソースが使用されているかどうかが含まれています。

SAML ベースの認証の典型的な使用例は、企業ネットワーク内でセキュリティの追加レイヤが必要なクラウド ベース サービスなどの統一した環境にあります。 しかし、どの SAML 実装にも少なくとも 3 つのコンポーネント役割が含まれます。

Relying パーティ

許可されたユーザにシステムへのアクセスを取得させるには、別のサーバ上に格納されたアイデンティティ情報を使用します。 「サービス プロバイダ」とも呼ばれます。 Single Sign-On が認証で SAML を使用するように設定されている場合、CA Performance Center にこの役割があります。

Asserting パーティ

アイデンティティまたはセキュリティ情報が格納されており、認証目的でリクエストされたときに提供されます。 このコンポーネント用の SAML 期間は*アイデンティティ プロバイダ*（*IdP*）です。 たとえば、CA SiteMinder サーバにこの役割があります。

件名

IdP によって格納されたアイデンティティ情報と関連付けられたユーザ（またはコンピュータ）です。

Single Sign-On での SAML 2.0 サポート

CA Single Sign-On では、Security Assertion Markup Language （SAML）、バージョン 2.0 での認証をサポートします。Single Sign-On サービスでは、SAML 2.0 トークンを受理およびてデコードして、SAML 標準に準拠する認証エージェントに提示できます。

SAML 2.0 の Single Sign-On サポートには、シングル ログアウトのサポートが含まれます。 このサポートにより、複数のユーザ インターフェースにログインしているユーザは、それらのすべてから同時にログアウトできます。たとえば、CA Performance Center にログインした後に CA Network Flow Analysis のフロー データにドリル ダウンするユーザは、1 つのインターフェースからログアウトするときにもう一方のインターフェースから自動的にログアウトできます。

Single Sign-On では標準ベースの SAML 2.0 ライブラリが使用されます。 その結果、それは、SAML 2.0 標準に依存するさらに多くの製品を潜在的にサポートします。ただし、以下の CA 製品のみが、CA Single Sign-On でテストされたアイデンティティ プロバイダです。

- CA SiteMinder Federation Manager
- CA Arcot A-OK™ On-Demand

SAML 環境では、複数の認証方式から選択できます。CA Performance Center ユーザは、Single Sign-On で典型的な（「製品」）認証方式を使用してログインするか、SAML トークンを使用できます。 製品方式は、すべてのアクティブなユーザ アカウントに対してデフォルトで有効です。 ユーザは CA Single Sign-On 用の標準的な URL を使用して、CA Performance Center ユーザ インターフェースにアクセスします。

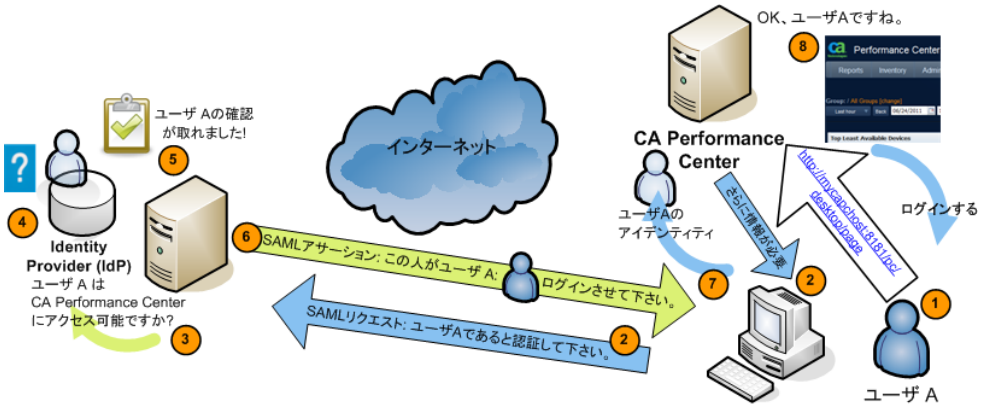
ユーザが SAML 2.0 を使用して認証するように、管理者は設定ツールを使用していくつかの Single Sign-On 設定を変更する必要があります。 管理者はまた、すべてのユーザ アカウントと SAML 2.0 をサポートするすべての登録済みデータ ソースに対して、外部認証を有効にする必要もあります。

CA データ ソース製品の一部は SAML 2.0 をサポートしていません。 Single Sign-On で外部認証用に SAML 2.0 を設定し、SAML サポートがないデータ ソースを登録する場合、CA Performance Center ユーザはデータ ソースへのドリル ダウン時に再認証する必要があります。

SAML 2.0 の Single Sign-On サポートの仕組み

Single Sign-On を使用する標準的な CA Performance Center 認証処理は、SAML 2.0 サポートを利用する認証とは異なります。 SAML 2.0 認証では、CA Performance Center ログイン ページが表示されません。 代わりに、IdP で提供されたインターフェースへリダイレクトされます。 他のすべてのサポート対象認証方式については、Single Sign-On でログイン ページが提供されています。

以下の図に、Single Sign-On、CA Performance Center、および SAML 2.0 標準をサポートする IdP（CA SiteMinder など）を使用した SAML 2.0 認証処理を示します。



以下の一般的なプロセスでは、CA Performance Center における SAML 2.0 認証のサポート方法について説明します。 デジタル署名証明書や転送バインディングなど、実装に固有のオプションは省略されています。

1. たとえば、http://mycapchost:8181/pc/desktop/page に移動することにより、ユーザは CA Performance Center へのアクセスを試行します。
2. CA Performance Center は、アイデンティティ プロバイダ（IdP）による認証用の SAML リクエストで応答します。
3. ブラウザはリクエストを処理し、IdP サーバ上で実行中の認証ソフトウェアと接続します。
4. IdP では、既存のログオン セキュリティ コンテキストがユーザにあるかどうか -- つまり、ユーザがすでにログオンされているかどうかが判別されます。

5. ユーザがログオンしていない場合、IdP は実装に固有の方法でユーザを認証します。

   たとえば、IdP はブラウザと通信してユーザに認証情報の提供を要求する場合があります。 認証のこの段階は CA Single Sign-On とは無関係です。

6. IdP は、ユーザのログオン セキュリティ コンテキストを表す SAML アサーションを作成してブラウザに送信します。

   アサーションには、必須属性 subjectNameId とオプションの属性 ClonedUser が含まれます。

   subjectNameId の値は承認されたユーザです。

   アサーションには、クローン ユーザ アカウントの名前を含めることができます。 この属性は、承認された SAML ユーザがマップされるユーザ アカウントを定義します。

7. ブラウザは SAML アサーションを CA Performance Center に送信します。

8. CA Performance Center はアサーションを取得して処理します。

9. アサーションが有効な場合、CA Performance Center でユーザ用のセッションが確立されます。ブラウザはターゲット ページ (ユーザのホーム ダッシュボード ページ) へリダイレクトします。

SAML 認証のセットアップ方法

Single Sign-On で SAML 2.0 認証を有効にするには、管理者は以下の手順に従う必要があります。

1. アイデンティティ プロバイダ（IdP）に固有のガイドラインに従って、IdP と Single Sign-On 間にアグリーメントを確立するメタデータ ファイルを作成します。

   詳細については、「IdP アグリーメントの準備 (P. 50)」を参照してください。

2. （オプション）CA ソフトウェアを実行する IdP とサーバ間の通信でデジタル署名および暗号化を有効にするには、プロパティ ファイルを作成します。

   詳細については、「セキュリティ プロパティ ファイルの準備 (P. 50)」を参照してください。

3. SAML 認証用のパラメータを設定するには、Single Sign-On 設定ツールを使用します。

   詳細については、「Single Sign-On での SAML サポートの設定 (P. 52)」を参照してください。

4. IdP サーバ上のパラメータを設定します。 たとえば、SAML をサポートするすべてのデータ ソース製品 Web サイトを、信頼されたサイトのリストへ追加します。

   詳細については、「IdP の構成 (P. 56)」を参照してください。

5. 外部認証を使用する手順を追加するには、CA Performance Center 管理内のユーザ アカウントを更新します。

   詳細については、「SAML セットアップの完了 (P. 58)」を参照してください。

IdP アグリーメントの準備

XML 形式のメタデータ ファイルは、IdP とサービス プロバイダ間のアグリーメントを確立するのに必要です。 この場合、SAML 2.0 をサポートする CA Performance Center およびすべての登録済みデータ ソースでこのアグリーメントが必要です。 メタデータ ファイルには、IdP の説明とそれがサポートするプロファイルの情報が含まれています。 このファイルには、サービス プロバイダからリクエストするサービスに関するデータも含まれます。

Single Sign-On では、IdP との関係をセットアップするためにこのファイルをインポートできます。

CA SiteMinder など一部のタイプの IdP では、これらのファイルの作成およびエクスポートを支援するユーティリティが提供されています。 あるいは、ユーザが設定したパラメータに基づいて、アグリーメントが自動的に作成されます。

IdP でこのタスクを実行するには、マニュアルを参照してください。

セキュリティ プロパティ ファイルの準備

CA Performance Center と IdP 間の通信用に暗号化およびデジタル証明書を使用する場合は、プロパティ ファイルが必要です。 このファイルでは、署名と暗号化に使用する証明書と、暗号化を有効にする他のパラメータを指定します。

SAML プロパティ ファイルは Single Sign-On のホーム ディレクトリに保存されます。

```
/opt/CA/PerformanceCenter/sso/webapps/sso
```

たとえば、以下のようなファイルが必要です。

```
/opt/CA/PerformanceCenter/sso/webapps/sso/configuration/saml.properties
```

プロパティ ファイルには以下のパラメータが含まれている必要があります。

- 署名証明書のディレクトリ場所およびファイル名。
- 証明書にアクセスするための検証証明書エイリアスおよびパスワード。
- CA Performance Center サーバのホスト名。
- IdP からエクスポートしたアグリーメントのディレクトリ場所およびファイル名。
- IdP に設定されたタイムアウト期間の長さ。 値は Single Sign-On の［SAML2 IDP セッション タイムアウト］パラメータと一致する必要があります。

構文の例を以下に示します。

```
# Location of the certificate used for signing SAML documents
saml.sp.certificate.location=/opt/CA/saml2configuration/[Certificate filename]
saml.sp.certificate.password=[password]
saml.sp.certificate.alias=[alias]

saml.sp.metadata.hostname=[Full Hostname of CA Performance Center server]
saml.sp.metadata.entityID=[Name of the CA Performance Center server without IP
domain]
saml.sp.metadata.organizationName=[Name of your organization]
saml.sp.metadata.contactPerson=[First and last name of administrator]
saml.sp.metadata.email=[Email address of contact person]

# ログイン サイトのメタデータ ファイルの場所
saml.idp.metadata.file=/opt/CA/saml2configuration/[Filename].xml
# Session timeout with the IdP in minutes. Use this value for auto-reauthentication
and logout requests
saml.idp.sessionTimeout=[Length of timeout period in minutes]
```

saml.properties ファイルを変更する場合は常に、メタデータ ファイル（IdP とのアグリーメントを確立するファイル）を再エクスポートします。 詳細については、「Single Sign-On での SAML 2.0 サポートの設定 (P. 52)」を参照してください。 Single Sign-On を再起動する必要もあります。

Single Sign-On での SAML 2.0 サポートの設定

CA Performance Center 管理者は、Single Sign-On 設定ツールを使用して、SAML 認証用のパラメータを設定する必要があります。データ ソースがインストールされ、かつ SAML 2.0 でユーザが認証されるすべてのサーバで以下の手順を実行します。

注: 複数の認証スキームは同時に使用できます。 たとえば、CA Network Flow Analysis データ ソースのユーザはログインに LDAP を使用できますが、一方 CA Infrastructure Management のユーザは SAML 2.0 を使用します。

次の手順に従ってください:

1. CA Performance Center または CA データ ソース製品がインストールされているサーバにログインします。

   ルートとしてログインするか、または「sudo」コマンドでログインします。

2. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。 利用可能なオプションは、ローカル サーバ上で実行される CA アプリケーションに対応します。

3. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）

4. 設定するデータ ソースに対応する値を入力します。 たとえば、CA Performance Center を設定するには 1 を入力します。

   オプションを選択するように促されます。

5. SAML 認証に 2 を入力します。

   優先度を指定するように促されます。

   ［優先度］パラメータは CA Performance Center のみに適用されます。

6. 以下のオプションのいずれかを入力します。

   1. **リモート値**

      管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. **ローカル上書き**

      すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。

   SAML2 プロパティに対する値を指定するには、値を更新するために u を入力してから、新しい値を入力します。

7. ［SAML2 認証の有効化］パラメータを選択するために 1 を入力します。

   オプションを選択するように促されます。

8. 値を変更するために u を入力し、SAML 2.0 認証を有効にするために 1 を入力します。

9. ［デフォルト ユーザ アカウントのクローン作成］パラメータを設定するために 2 を入力します。

   2. **デフォルト ユーザ アカウントのクローン作成**

      許可された SAML ユーザがマップされるユーザ アカウントを定義します。 指定するユーザ アカウントに関連付けられる役割および製品の権限は、正常に認証されるすべてのユーザに適用されます。

      デフォルト： 未指定。

      例： すべてのユーザがユーザ レベル権限でログイン可能にするには、「ユーザ」を入力します。

      注: 既存のユーザ アカウントが必要です。

   IdP 上で設定されたユーザ アカウントは、アグリーメントが確立されるときに CA Performance Center に送信されます。 編集可能な場合は、［ユーザの管理］管理ページのユーザ リストに表示されます。

10. セキュリティ パラメータを有効にするために 3 を入力します。

    3. SAML2 シグネチャと暗号化有効

    CA Performance Center と IdP の間の通信のセキュリティおよび暗号化を有効にします。

    デフォルト： 無効

    オプションを選択するように促されます。

11. 値を変更するために u を入力し、それを有効にするために 1 を入力します。

    注: この設定は、IdP 上の設定に一致する必要があります。

12. 自動再認証を有効にするために 4 を入力します。

    4. SAML2 自動再認証

    タイムアウト期間が期限切れになった後に、ユーザが再認証する必要があるかどうかを指定します。 このパラメータを有効にすると、ユーザの介入なしで IdP でパッシブ再認証（「自動再認証」）を実行できるようになります。

    次のパラメータでは、タイムアウト期間を設定できます。

    デフォルト： 無効。

13. 値を変更するために u を入力し、それを有効にするために 1 を入力します。

14. 再認証タイムアウト期間を設定するために 5 を入力します。

    5. 自動再認証期間

    パッシブ再認証が実行される前に経過する時間の長さを設定します。［SAML2 自動再認証］パラメータが無効な場合、このパラメータは無視されます。

    値： ［IDP セッション タイムアウト］パラメータの値よりも小さい値にする必要があります。

    デフォルト： なし。

15. 値を変更するために u を入力し、新しい値を入力します。
16. アイデンティティ プロバイダにセッションのタイムアウト期間を設定するために 6 を入力します。

    6. IdP **セッション タイムアウト**

    CA Performance Center とアイデンティティ プロバイダの間で確立されたセッションが自動的に閉じられるまでに経過する時間の長さを設定します。 たとえば、10 分のタイムアウトを設定するには「10」を入力します。

    ［自動再認証期間］パラメータに対して指定された値よりも大きい値にする必要があります。そうしないと、再認証を実行するセッションは存在しません。 また、値は［saml.idp.sessionTimeout］パラメータのセキュリティ プロパティ ファイルで設定された値に一致する必要があります。 詳細については、「セキュリティ プロパティ ファイルの準備 (P. 50)」を参照してください。

    デフォルト： なし。
17. 値を変更するために u を入力し、新しい値を入力します。
18. 初期プロンプトに戻るために 2 回 b を入力します。
19. IdP とのアグリーメントを確立するメタデータ ファイルをエクスポートするために 6 を入力します。

    メタデータ ファイルでは、ユーザ認証時に使用するパラメータがアイデンティティ プロバイダに提供されます。

    ディレクトリ パスとファイル名を指定するように指示されます。
20. ファイル名を入力します。 たとえば、以下のように入力します。

    ```
    /tmp/CAPCMetadata.xml
    ```

    このファイルは、設定ツールで選択した設定に基づいて自動的に生成されます。

    エクスポート操作が成功すると、XML のプリントアウトが表示されます。 操作が失敗すると、エラー メッセージが表示されます。
21. 終了するために q を入力します。

    設定ツールが閉じます。

IdP の設定

CA Performance Center でのユーザ認証に SAML 2.0 を使用するには、アイデンティティ プロバイダ（IdP）上でいくつかのパラメータを設定します。SAML 2.0 標準をサポートするすべての IdP で動作するはずですが、テストは CA SiteMinder でのみ行われています。

IdP は手動で設定するか、または Single Sign-On サーバから IdP アグリーメントをインポートすることができます。

IdP の手動設定

次の手順に従ってください:

1. IdP で SAML2 認証モードを有効にします。
2. Single Sign-On がインストールされたサーバ上で実行されている、アサーション コンシューマ サービスの URL を指定します。 以下に例を示します。

   `http://MyServerName:8381/sso/saml2/UserAssertionService`

   ここで 8381 は Single Sign-On が使用するポートです。
3. バインド方法を「HTTP リダイレクト」に設定します。

   注: HTTP リダイレクトは Single Sign-On でサポートされる唯一のバインディング方式です。
4. シングル ログアウト サービスの URL を指定します。

   ログアウト サービスとレスポンス場所は共に必須です。これらのサービスは、Single Sign-On がインストールされているサーバ上で実行されています。

   以下の例を使用します。

   ```
   http://MyServerName:8381/sso/saml2/LogoutService
   http://MyServerName:8381/sso/saml2/LogoutServiceResponse
   ```
5. SAML 2.0 をサポートするすべてのデータ ソース製品 Web サイトを、信頼されたサイトのリストへ追加します。

   このステップでは、これらの Web サイトを連携パートナシップ エンティティのリストへ追加することもできます。
6. （*オプション*）デジタル署名および暗号化の設定を確認します。また、これらの設定を Single Sign-On でも行う必要があります。

IdP アグリーメント ファイルのインポート

次の手順に従ってください:

1. Single Sign-On サーバ上で設定した場所から、IdP アグリーメント ファイルをインポートします。

   このファイルは、Single Sign-On 設定ツールを使用してその他の設定手順を完了した後にエクスポート済みです。 詳細については、「Single Sign-On での SAML サポートの設定 (P. 52)」を参照してください。

2. SAML 2.0 をサポートするすべてのデータ ソース製品 Web サイトを、信頼されたサイトのリストへ追加します。

   このステップでは、これらの Web サイトを連携パートナシップ エンティティのリストへ追加することもできます。

3. （*オプション*）デジタル署名および暗号化の設定を確認します。また、これらの設定を Single Sign-On でも行う必要があります。

トラブルシューティング

問題:

SAML の設定後、以下のエラー メッセージが表示されます。

```
RelayState is either null or a blank string. RelayState must be set
for SSO to work correctly.
```

```
Invalid syntax, RelayState=<value>
```

```
RelayState does not have parameter SsoRedirectUrl,
RelayState=<value>
```

原因:

一部の IdP は、認証の確認中に CA Performance Center が IdP へ送信する RelayState= 値を返しません。

解決方法:

IdP の RelayState を手動で設定します。 以下の構文を使用します。

```
SsoProductCode=pc&SsoRedirectUrl=http://[assign the value for
CAPC in your book]:8181/pc/desktop/page
```

注: 安全な通信のために、http: を https: に変更し、ポート番号も置き換えてください。

SAML 2.0 セットアップの完了

SAML 2.0 認証を有効にするには、外部認証を使用するようにユーザ アカウントを編集します。 CA Performance Center の新規ユーザ アカウントは、デフォルトで Performance Center Authentication を使用するよう設定されています。 管理者は、SAML 2.0 を使用して認証するすべてのオペレータのアカウントを更新する必要があります。

SAML 2.0 の設定中に、IdP で「クローン作成」の対象となる既存の CA Performance Center ユーザ アカウントを指定します。 すでに IdP で定義されているユーザは、指定するユーザ アカウントと同じレベルの製品権限を受信します。 これらのアカウントも CA Performance Center に継承され、そこでユーザ リストの新規ユーザとして表示されます。 多くの場合、これらのアカウントを編集して、これらのユーザがジョブの実行に必要なデータのみにアクセスできようにする必要があります。

次の手順に従ってください:

1. CA Performance Center に管理者権限を持つユーザとしてログインします。
2. ［管理］-［ユーザ設定］を選択し、［ユーザ］をクリックします。

   ［ユーザの管理］ページが開きます。
3. 編集するユーザ アカウントを選択します。
4. ［編集］をクリックします。

   ［ユーザの編集］ウィザードが開きます。
5. ［認証タイプ］として［外部］を選択します。
6. ユーザ アカウントに必要な変更を他に加えるには、ウィザードを使用します。 たとえば、このユーザに別の［製品権限］を選択するには、3 番目のウィザード ダイアログ ボックスに進みます。
7. ［保存］をクリックします。

   ユーザ アカウントへの変更が保存されます。

第 4 章: Single Sign-On での HTTPS の使用

このセクションには、以下のトピックが含まれています。

SSL （Secure Sockets Layer）暗号化： HTTPS (P. 59)
CA Single Sign-On に HTTPS をセットアップする方法 (P. 60)

SSL（Secure Sockets Layer）暗号化: HTTPS

デフォルトでは、Single Sign-On は、ユーザのブラウザと CA Performance Center 間の通信に HTTP（Hyper Text Transfer Protocol）を使用します。 TLS （Transport Layer Security）、およびその前身である SSL （Secure Sockets Layer）は、インターネット上のデータ送信を保護するために広くサポートされている暗号化プロトコルです。 TLS と SSL は、HTTP と共に使用して HTTPS （HTTP-Secure）を形成できます。 このガイドでは、「TLS と SSL」を意味する総称的な用語として *SSL* を使用しています。

HTTP の代わりに HTTPS を使用するように Single Sign-On を設定することによって、監視システムのセキュリティを強化できます。

HTTPS を使用するように CA Single Sign-On を設定することはオプションです。HTTPS を使用するように Single Sign-On の Web サイトを設定するには、事前にサーバ証明書を取得する必要があります。 可能な場合、組織のセキュリティ ポリシーを作成して実施するチームから、これらの手順について支援を受けてください。

CA Single Sign-On に HTTPS をセットアップする方法

SSL を有効にするには、いくつかの手順が必要です。 はじめに、サーバのアイデンティティを検証する証明書をインストールします。 次に、CA Performance Center が Single Sign-On の正しいポートおよびスキームに（および逆方向にも）正しくリダイレクトするように、データベースを変更します。 最後に、新しいポートおよびスキームを反映するように CA Performance Center と Single Sign-On の両方のサービスを変更します。

これらの手順では以下の 2 つのポートが重要です： CA Performance Center ポート（デフォルトで 8181）および Single Sign-On ポート（デフォルトで 8381）。 ポート 8181 は CA Performance Center 接続ポートです。 ユーザに認証が必要な場合、サーバによってポート 8381 の Single Sign-On にリダイレクトされ、［ログイン］ページが表示されます。 ユーザが正常にログインすると、ポート 8181 の元の URL にリダイレクトされます。

したがって、設定の各手順で同じポートを使用することはできません。そうでない場合、CA Performance Center と Single Sign-On の間に競合が発生します。

CA Performance Center と Single Sign-On の HTTPS を有効にするには、以下の手順に従います。

1. サーバ証明書を取得して Web サーバのキーストアにインストールします（P. 61）。
2. Single Sign-On 設定ツールを使用して、必要なプロパティを更新します（P. 67）。
3. CA Performance Center コンソールで HTTPS をセットアップします（P. 68）。
4. Single Sign-On での HTTPS をセットアップします（P. 71）。
5. サービスを停止し、再起動します。

SSL 証明書の設定

Single Sign-On Web サイトを設定して HTTPS を使用するには、先に秘密鍵および関連する公開証明書を取得してインストールする必要があります。 SSL では、自己署名証明書、または信頼された証明機関が署名した証明書のいずれかを使用できます。 この手順は通常、組織およびセキュリティチームのポリシーによって異なります。 ただし、これらの手順では、ユーザの設定に役立つ情報が提供されます。

ご使用の環境に適した手順を選択してください。

- 新しい証明書を生成してインポートします (P. 61)。
- 既存の証明書をインポートします (P. 65)。

注: これらの手順で使用される keytool コマンドの詳細については、Oracle の Web サイトの Java ドキュメントを参照してください。

証明書の生成およびインポート

SSL 証明書がない場合は、keytool コマンドを使用して証明書を生成できます。 この手順では、自己署名証明書を生成してキーストアにインストールする方法について説明します。

次の手順に従ってください:

1. 以下のコマンドを実行します。

   cd *インストール ディレクトリ*/PerformanceCenter/jetty/etc

2. 以下のコマンドを使用してファイル名を変更し、既存の jetty キーストア ファイルのバックアップを作成します。

   mv *インストール ディレクトリ*/PerformanceCenter/jetty/etc/keystore *インストール ディレクトリ*/PerformanceCenter/jetty/etc/keystore.bak

   重要: 古いキーストアは削除する必要があります。 削除しない場合、後の手順で次のエラーが表示されます： "Keystore was tampered with, or password was incorrect."

3. 以下のコマンドを使用して、秘密鍵、および公開された自己署名証明書を生成します。

   ```
   keytool -genkeypair -keystore keystore_file.ks -storepass storepasswd -keyalg RSA -keysize 2048 -keypass keypasswd -alias alias_name
   ```

   storepasswd

   キーストアのパスワードを指定します。

   keypasswd

   キーストア内の秘密キー用のパスワードを指定します。

   重要: これらのパスワードは忘れないようにしてください。パスワードを回復することはできません。

4. 以下のコマンドを使用して、キーストアから自己署名証明書をエクスポートします。

   ```
   keytool -exportcert -keystore keystore_file.ks -storepass storepasswd -alias alias_name -file filename.cer
   ```

   alias

   キーを保存するために作成する、キーストア エントリ参照用のエイリアスを指定します。

   filename.cer

   証明書がエクスポートされるファイルを指定します。 フルパス名を使用して、現在のディレクトリにはファイルを配置しないことをお勧めします。

   例： /tmp/capcCert.cer

   注: 続行前に cacerts ファイルをバックアップしておくことをお勧めします。

5. 以下のコマンドを使用して、自己署名証明書を java の信頼された証明書キーストアにインポートします。

   ```
   keytool -importcert -keystore インストール ディレクトリ/jre/lib/security/cacerts
   -storepass cacertspasswd -alias capcSelfSigned -file filename.cer
   ```

   注: cacerts キーストアのデフォルト パスワードは「changeit」です。

   cacertspasswd

   cacerts キーストアのパスワードを指定します。

   デフォルト： changeit

   filename.cer

   前の手順で証明書がエクスポートされたファイル。

6. cacerts ファイルをバックアップします。

7. （オプション）セキュリティを強化するために、以下のコマンドを使用して、java の信頼された証明書キーストアのパスワードを変更します。

   ```
   keytool -storepasswd -keystore インストール ディレクトリ/jre/lib/security/cacerts
   ```

   既存のパスワードと新しいパスワードの入力を求められます。

8. インポートされたキーストアが利用可能であることを確認します。 以下のコマンドを使用します。

   ```
   keytool -list -keystore インストール ディレクトリ/jre/lib/security/cacerts
   ```

   重要: Web サービスを有効にするには、自己署名証明書が cacerts キーストアに存在する必要があります。 そうでない場合、PKIX は証明書を見つけることができなかったというエラーがログに表示されます。

9. 以下のコマンドを使用して、それぞれの CA Performance Center サービスを再起動します。

   ```
   /sbin/service caperfcenter_sso restart
   /sbin/service caperfcenter_devicemanager restart
   /sbin/service caperfcenter_console restart
   ```

   自己署名された SSL 証明書が生成され、キーストアにインストールされます。

次の手順：

- （オプション）自己署名証明書の証明機関 SSL 証明書への変換（P. 64）
- HTTPS をサポートするためのポートおよび Web サイトの設定（P. 67）

自己署名証明書の証明機関 SSL 証明書への変換

CA Performance Center を開くときに、自己署名証明書ではブラウザ警告が表示されます。 ユーザは手動で警告を解除して続行できます。 ただし、信頼された証明機関が署名した証明書であれば、ブラウザ警告は表示されません。 以下の手順では、自己署名証明書を、信頼された証明機関が署名した証明書に変換する方法について説明します。

次の手順に従ってください:

1. 以下のコマンドを実行します。

   ```
   cd installDirectory/PerformanceCenter/jetty/etc
   ```

2. 以下のコマンドを使用して、証明書シグネチャ リクエストをエクスポートします。

   ```
   keytool -certreq -keystore keystore_file.ks -storepass storepasswd -alias
   alias_name -keypass keypasswd -file requestFileName.csr
   ```

   requestFileName.csr

   エクスポートされたシグネチャ リクエストのパスとファイル名を指定します。

3. リクエストされた他の情報と共に、結果ファイル（*requestFileName*.csr）を適格な署名機関に送信します。

   証明機関から、署名された証明書（*signedCert*.cer）が送信されます。また、署名された証明書を認証するために、ルート証明機関の証明書（*rootCA*.cer）が提供される場合があります。

4. （*オプション*）以下のコマンドを使用して、ルート証明機関の証明書が Java のデフォルトで信頼された証明機関に含まれているかどうかを確認します。

   ```
   keytool -list -v -keystore installDirectory/jre/lib/security/cacerts -storepass
   cacertspasswd
   ```

5. （*オプション*）コマンドの出力から、ユーザの証明書に署名した証明機関を検索します。 証明機関がリストに含まれていない場合は、以下のコマンドを使用して、信頼された証明機関のリストに追加します。

   ```
   keytool -importcert -keystore installDirectory/jre/lib/security/cacerts
   -storepass cacertspasswd -alias myRootCa -file rootCA.cer
   ```

6. 以下のコマンドを使用して、署名証明書をインポートします。

   ```
   keytool -importcert -trustcacerts -keystore keystore -storepass storepasswd
   -alias alias_name -keypass keypasswd -file signedCert.cer
   ```

7. 以下のコマンドを使用して、jetty キーストアのコンテンツを検証します。

   ```
   keytool -list -keystore installDirectory/PerformanceCenter/jetty/etc/keystore
   ```

   インポートした単一の証明書がリストに表示されます。

8. 以下のコマンドを使用して、それぞれの CA Performance Center サービスを再起動します。

   ```
   /sbin/service caperfcenter_sso restart
   /sbin/service caperfcenter_devicemanager restart
   /sbin/service caperfcenter_console restart
   ```

   キーストア内の自己署名証明書は、証明機関の SSL 証明書によって置き換えられます。

次の手順： HTTPS をサポートするためのポートおよび Web サイトの設定 (P. 67)

キーおよび既存の証明書のインポート

異なるソースからの秘密鍵および公開証明書（自己署名証明書または認証機関の証明書のいずれか）を使用できます。たとえば、セキュリティ チームが、組織のためにカスタマイズされた SSL 証明書を提供します。この SSL 証明書を使用するには、秘密鍵および署名された証明書をインポートします。

次の手順に従ってください:

1. 以下のコマンドを実行します。

   ```
   cd /opt/CA/PerformanceCenter/jetty-version/etc
   ```

2. 以下のコマンドを使用して、古いキーストアを削除します。

   ```
   rm keystore
   ```

3. 以下のコマンドを使用して、秘密鍵と証明書から PKCS#12 キーストアを作成します。

   ```
   openssl pkcs12 -export -in certificate.pem -inkey privatekey.pem -name MyAlias
   -out keystore.pkcs12
   ```

   certificate.pem

   提供された証明書を指定します。

   privatekey.pem

   提供された秘密鍵を指定します。

   注: このコマンドは Linux のみで動作します。

4. 以下のコマンドを使用して、鍵と証明書を CA Performance Center キーストアにインポートします。

   ```
   keytool -importkeystore -destkeystore keystore_file -deststorepass storepasswd
   -srckeystore keystore.pkcs12 -srcstoretype pkcs12 -srcalias src_alias_name
   -destalias dest_alias_name -destkeypass keypasswd
   ```

5. 以下のコマンドを使用して、それぞれの CA Performance Center サービスを再起動します。

   ```
   /sbin/service caperfcenter_sso restart
   /sbin/service caperfcenter_devicemanager restart
   /sbin/service caperfcenter_console restart
   ```

   既存の SSL 証明書がキーストアにインポートされます。

次の手順： HTTPS をサポートするためのポートおよび Web サイトの設定 (P. 67)

注: 証明書に、キーストア内の証明書で終了するチェーンが含まれない場合は、Java cacerts キーストアに証明書をインポートします。 以下のコマンドを実行して、証明書にチェーンが含まれるかどうかを判断します。

```
keytool -printcert -file filename
```

ファイル名

証明書の名前を指定します。

Java cacerts キーストアに証明書をインポートする手順については、「証明書の生成およびインポート (P. 61)」を参照してください。

SSL 用のポートおよび Web サイトの設定

デフォルトでは、Single Sign-On はポート 8381 を使用します。HTTPS をセットアップするには、Single Sign-On 設定ツールを使用して、暗号化の設定と一致するようにデフォルトの Web サイト スキームおよびポートを更新します。

データ ソースがインストールされているすべてのサーバに対して、この手順のタスクを実行します。

次の手順に従ってください:

1. 以下のディレクトリで「./SsoConfig」コマンドを実行し、Single Sign-On 設定ツールを起動します。

   ```
   [InstallationDirectory]/CA/PerformanceCenter
   ```

   オプションを選択するように促されます。

2. 設定を選択している間、必要に応じて以下のコマンドを使用します。
   - q （終了）
   - b （前のメニューに戻る）
   - u （更新）
   - r （リセット）
3. CA Performance Center を選択するために 1 を入力します。
4. Single Sign-On を設定するために 4 を入力します。

   優先度を指定するように促されます。

5. 以下のオプションのいずれかを入力します。

   1. リモート値

   管理者のみが変更できる設定を参照します。 そのような設定は、CA Performance Center のこのインスタンスに登録された他のすべての CA 製品に継承されます。 対応する［ローカル上書き］値が存在しない場合、［リモート値］設定のみが使用されます。

   2. ローカル上書き

   すべての製品に対して変更できる設定を参照します。 ［ローカル上書き］値が存在する場合、［リモート値］とデフォルト設定のいずれよりも優先されます。

   設定するプロパティを選択するように促されます。

6. スキーム プロパティの 12 を入力します。
7. 値を更新するために「u」を入力します。
8. 値に「https」と指定します。
9. ポート プロパティの 13 を入力します。
10. 値を「8382」に更新します。
11. ［SSO 設定］/CA Performance Center メニューに戻るために「b」を 2 回入力します。
12. Performance Center を設定するために 3 を入力します。

    優先度を指定するように促されます。
13. リモート値の 1 を入力するか、またはローカル上書きの 2 を入力します。
14. Web サイト スキームを選択するために 6 を入力します。
15. 値を「https」に更新します。
16. Web サイト ポートを選択するために 8 を入力します。
17. 値を「8182」に更新します。
18. 終了するために q を入力します。

この後、HTTPS を使用するように CA Performance Center ファイルを設定する必要があります。

HTTPS を使用する CA Performance Center の設定

新しい Web サイトおよびポート設定を反映するには、一部の設定ファイルを編集する必要があります。 HTTP コネクタを HTTPS コネクタに置き換えるために設定ファイルを編集します。また、変更を有効にするために、CA Performance Center サービスを再起動する必要があります。

次の手順に従ってください:

1. 以下のディレクトリに移動します。

   ```
   cd /[インストール ディレクトリ]/CA/PerformanceCenter/PC
   ```
2. 編集する start.ini ファイルを開きます。

3. 以下の行を検索し、その行をアクティブにするために「#」を削除します。

   ```
   #/opt/CA/PerformanceCenter/PC/etc/jetty-ssl.xml
   ```

   ここで「/opt/CA」はデフォルト インストール ディレクトリです。

4. start.ini を保存します。

5. 以下のディレクトリに移動します。

   ```
   cd /[インストール ディレクトリ]/CA/PerformanceCenter/PC/etc
   ```

6. そのディレクトリに、以下の内容を持つ「jetty-ssl.xml」という名前のファイルを作成します。

   ```
   <?xml version="1.0"?>
   <!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
   "http://www.eclipse.org/jetty/configure.dtd">
   <Configure id="Server" class="org.eclipse.jetty.server.Server">
     <Call name="addConnector">
       <Arg>
         <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
            <Set name="Port">8182</Set>
            <Set name="maxIdleTime">30000</Set>
           <Set name="Keystore"><Property name="jetty.home" default="."
   />/etc/keystore</Set>
           <Set name="Password">***PASSWORD***</Set>
            <Set name="KeyPassword">***PASSWORD***</Set>
           <Set name="truststore"><Property name="jetty.home" default="."
   />/etc/keystore</Set>
           <Set name="trustPassword">***PASSWORD***</Set>
           <Set name="allowRenegotiate">true</Set>
         </New>
       </Arg>
     </Call>
   </Configure>
   ```

7. すべてのインスタンスの「***PASSWORD***」値を、システムで使用中のパスワードに置換します。

8. ファイルを保存します。

9. 編集する jetty.xml ファイルを開きます。

10. デフォルト HTTP コネクタ用の以下の行を削除します。

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. jetty.xml を保存します。

12. 以下のディレクトリに移動します。

```
cd /[インストール ディレクトリ]/CA/PerformanceCenter/PC/conf
```

13. ファイル wrapper.conf を編集します。 以下の行で「8181」を「8182」に置換し、前述の jetty-ssl.xml に定義されているポートに一致するようにします。

```
  wrapper.java.additional.2=-Djetty.port=8181
```

14. wrapper.conf を保存します。

15. 以下のディレクトリに移動します。

```
cd /[インストール ディレクトリ]/CA/PerformanceCenter/sso/webapps/
sso/configuration
```

16. ファイル「CAPerformanceCenter.xml」を編集します。

17. <Scheme> および <Port> の値を SSL の適切な設定に置換します。

```
<?xml version="1.0" encoding="utf-8" ?>
<Configuration>
     <SingleSignOnEnabled>True</SingleSignOnEnabled>
     <SingleSignOnProductCode>pc</SingleSignOnProductCode>
     <SignInPageProductDefaultUrl>
```

```
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/desktop/page</PathAndQuery>
        </SignInPageProductDefaultUrl>
        <SingleSignOnWebServiceUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/center/webservice/sso</PathAndQuery>
        </SingleSignOnWebServiceUrl>
    </Configuration>
```

Single Sign-On 設定の更新およびサービスの再起動

Single Sign-On で SSL 暗号化をサポートするために、一部のスタートアップファイルを編集します。 また、設定を更新するために、CA Performance Center および Single Sign-On のすべてのサービスを再起動する必要があります。

次の手順に従ってください:

1. 以下のディレクトリに移動します。

   ```
   cd /[インストール ディレクトリ]/CA/PerformanceCenter/sso
   ```

2. 編集する start.ini ファイルを開きます。
3. 以下の行を検索し、その行をアクティブにするために「#」を削除します。

   ```
   #/opt/CA/PerformanceCenter/sso/etc/jetty-ssl.xml
   ```

   ここで「/opt/CA」はデフォルト インストール ディレクトリです。

4. start.ini を保存します。
5. 以下のディレクトリに移動します。

   ```
   cd /[インストール ディレクトリ]/CA/PerformanceCenter/sso/etc
   ```

6. そのディレクトリに、以下の内容を持つ「jetty-ssl.xml」という名前のファイルを作成します。

```
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure.dtd">
<Configure id="Server" class="org.eclipse.jetty.server.Server">
  <Call name="addConnector">
    <Arg>
      <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
         <Set name="Port">8382</Set>
         <Set name="maxIdleTime">30000</Set>
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="Password">***PASSWORD***</Set>
        <Set name="KeyPassword">***PASSWORD***</Set>
       <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="trustPassword">***PASSWORD***</Set>
        <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. すべてのインスタンスの「***PASSWORD***」値を、システムで使用中のパスワードに置換します。

8. jetty-ssl.xml を保存します。

9. ファイル jetty.xml を開きます。

10. デフォルト HTTP コネクタ用の以下の行を削除します。

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host">><Property name="jetty.host" />></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port">><SystemProperty name="jetty.port"
default="8181"/>></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. jetty.xml を保存します。
12. 以下のディレクトリに移動します。

    [インストール ディレクトリ]/CA/PerformanceCenter/sso/conf

13. ファイル wrapper.conf を編集します。 以下の行で「8381」を「8382」に置換し、前述の jetty-ssl.xml に定義されているポートに一致するようにします。

    ```
    wrapper.java.additional.2=-Djetty.port=8381
    ```

14. wrapper.conf を保存します。
15. 以下のコマンドを入力して、コンソール、デバイス マネージャ、および SSO の各サービスを停止します。

    ```
    service caperfcenter_console stop
    service caperfcenter_devicemanager stop
    service caperfcenter_sso stop
    ```

16. 以下のコマンドを入力して、サービスを再起動します。

    ```
    service caperfcenter_sso start
    service caperfcenter_devicemanager start
    service caperfcenter_console start
    ```

第 5 章: トラブルシューティング

このセクションには、以下のトピックが含まれています。

ブラウザのエラー表示 (P. 75)
ログ (P. 76)
監査ログの確認 (P. 77)

ブラウザのエラー表示

症状:

［ログイン］ページでパスワードを入力したときに、Web ブラウザのエラー ページにリダイレクトされました。 誤ったパスワードを入力してしまったのでしょうか。

解決方法:

この症状は、誤った SAML 認証情報を入力したことを示すものではありません。その代わり、ブラウザ エラー（401、500 など）は、Single Sign-On によってブラウザがログイン URL へリダイレクトされたが、アイデンティティ プロバイダ（IdP）サーバがダウンしていることを示します。

以下の手順を実行します。

- IdP サーバが稼動していることを確認します。
- CA Performance Center サーバと IdP サーバ間のネットワーク接続をテストします。

ログ

ログ ファイルを日単位または週単位確認することで、通常の操作に影響が出る前に問題を解決できます。すべてのログは、サービス（またはデーモン）に対応するサブフォルダ内に格納されます。以下のパスのログ ファイルを検索します。

```
CA/PerformanceCenter/servicename/logs
```

servicename パラメータを以下のいずれかのサービス名に置換します。

DM

デバイス マネージャ。

- DMService.log - デバイス マネージャからの出力（主に同期に関連）。
- wrapper.log - caperfcenter_devicemanager プロセスのログ。

EM

イベント マネージャ。

- EMService.log - イベント マネージャからの出力。イベントおよびアラームの詳細を含みます。
- wrapper.log - caperfcenter_eventmanager プロセスのログ。

PC

メインのコンソール プログラム。

- PCService.log - CA Performance Center 関連のログ。ユーザ インターフェースとビュー コンポーネントで構成されます。
- wrapper.log - caperfcenter_console プロセスのログ。

SSO

Single Sign-On 認証ソフトウェア。

- SSOService.log - Single Sign-On のログ。HTTPS（Secure Sockets Layer）の設定に関する HTTPS 情報が含まれます。
- wrapper.log - caperfcenter_sso プロセスのログ。

Single Sign-On 設定ツールに関する問題については、以下の場所にあるアプリケーション ログを確認します。

```
/opt/CA/PerformanceCenter/sso/logs/application.log
```

ログ ファイル名には、関連する日付と時間が含まれます。

新しいログ ファイルは、毎日自動的に生成されます。 ディスク領域を過剰に消費しないよう、14 日を経過すると古いログ ファイルから順に自動的に削除されます。

データベースまたはデータ ソースの同期に関連するエラーを見つけるには、最新のログ ファイルにアクセスします。まず始めに、［ダッシュボード］タブの［イベント］ダッシュボードを開き、［ステータス］でソートします。 関連するログ ファイルを確認する場合は、イベント タイプおよび障害の日時に注意します。 ログ ディレクトリで、ファイル名に対応する日付のログ ファイルを開きます。

監査ログの確認

Single Sign-On では、ユーザのログイン アクティビティに関する日単位の詳細をファイルに記録することで、セキュリティ監査をサポートします。ユーザ アクティビティを確認するためにログを確認します。

次の手順に従ってください:

1. CA データ ソース製品がインストールされているサーバにログインします。
2. コマンド プロンプトを開き、以下のディレクトリに移動します。

   ```
   [InstallationDirectory]/PerformanceCenter/sso/logs
   ```

   注: 監査ログは Windows サーバ上の以下の場所に保存されます。
   `[InstallationDirectory]¥Portal¥SSO¥logs`
3. dir と入力し、ディレクトリのコンテンツを参照します。

   ログ ファイルのファイル名は SingleSignOnAuditLogyyyy-mm-dd.log です。
4. 表示する監査ファイルの名前を入力します。

   ローカルのテキスト エディタ アプリケーションでファイルが開きます。

用語集

LDAP

LDAP （Lightweight Directory Access Protocol）は、ディレクトリを検索および編集し、IP ネットワークにディレクトリ情報を格納する方式を指定するプロトコルです。 また、LDAP には認証コンポーネントが含まれるため、ネットワーク アクセスの保護によく使用されます。 LDAP ディレクトリは通常、論理的な単位グループへ編成されます。 Microsoft Active Directory は LDAP を使用するディレクトリ アプリケーションの顕著な例です。

SAML

Security Assertion Markup Language（*SAML*）は XML に基づいたセキュリティ プロトコルです。 基本概念には、セキュア ドメインへのアクセスをリクエストする対象である個人またはコンピュータに関するセキュリティ アサーションの交換が含まれます。アサーションには、対象が特定のリソースにアクセスできるかどうかと、ポリシー ストアなどの外部データ ソースが使用されているかどうかが含まれています。

Single Sign-On

Single Sign-On は、CA Performance Center およびすべてのサポート対象データ ソースで使用される認証スキームです。 ユーザは CA Performance Center に認証されると、再びサインインする必要なく、コンソールや登録されているデータ ソース間を移動できます。

SSL

SSL （Secure Sockets Layer）は、多くの Web ブラウザがインターネット上のデータ セキュリティに対してサポートする暗号化プロトコルです。 サーバでは、交換されるデータを暗号化する公開鍵とそれを判読する秘密鍵が含まれる SSL 証明書が交換されます。 SSL により、Web ブラウザはブラウザ、クライアント コンピュータおよびサーバ機能に基づいて使用する暗号化のレベルを指定できます。 最大のレベルは、判読することが最も難しい 256 ビット暗号化です。

TLS

TLS（Transport Layer Security）、およびそれより以前の SSL（Secure Sockets Layer）は、インターネット上のデータ送信を保護する暗号化プロトコルであり、広くサポートされています。 SSL/TLS は、HTTP と共に使用して HTTPS（HTTP-Secure）を形成できます。

アイデンティティ プロバイダ（**IdP**）

アイデンティティ プロバイダ（IdP）にはアイデンティティまたはセキュリティ情報が格納されており、認証目的でリクエストされたときに提供されます。「Asserting パーティ」（SAML 認証に必要な 3 つのコンポーネント役割の 1 つ）とも呼ばれます。

設定ツール

*設定ツール*とは、Single Sign-On Web サイトと関連 CA データ ソース製品で使用される設定を管理者が調整できる、コマンド ライン アプリケーションです。