CA Access Control Premium Edition

トラブルシューティング ガイド

12.6.02

サードパーティに関する通知

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

サンプル スクリプトおよびサンプル SDK コード

CA Access Control 製品に含まれているサンプル スクリプトおよびサンプル SDK コードは、情報提供のみを目的として現状有姿のまま提供されます。これらは特定の環境で調整が必要な場合があるため、テストや検証を実行せずに実稼働システムにデプロイしないでください。

CA Technologies では、これらのサンプルに対するサポートを提供していません。また、これらのスクリプトによって引き起こされるいかなるエラーにも責任を負わないものとします。

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 Access Control Premium Edition
- CA Access Control
- CA Single Sign-On （CA SSO）
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management （CA NSM、旧 Unicenter NSM and Unicenter TNG）
- CA Software Delivery （旧 Unicenter Software Delivery）
- CA Service Desk （旧 Unicenter Service Desk）
- CA User Activity Reporting Module （旧 CA Enterprise Log Manager）
- Identity Manager

ドキュメントの表記規則

CA Access Control のドキュメントには、以下の規則があります。

形式	意味
等幅フォント	コードまたはプログラムの出力
斜体	強調または新規用語
太字	表示されているとおりに入力する必要のある要素
スラッシュ（/）	UNIX および Windows のパスの記述で使用される、プラットフォームに依存しないディレクトリの区切り文字

また、本書では、コマンド構文およびユーザ入力の説明に（等幅フォントで）以下の特殊な規則を使用します。

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ（[]）で囲まれた文字列	オプションのオペランド
中かっこ（{}）で囲まれた文字列	必須のオペランドセット
パイプ（|）で区切られた選択項目	代替オペランド（1 つ選択）を区切ります。 たとえば、以下の例は「*ユーザ名*または*グループ名*のいずれか」を意味します。 {*username*|*groupname*}
…	前の項目または項目のグループが繰り返し可能なことを示します
下線	デフォルト値
スペースに続く、行末の円記号（¥）	本書では、コマンドの記述が 1 行に収まらない場合があります。 このような場合、行末の空白とそれに続く円記号（¥）は、そのコマンドが次の行に続くことを示します。 **注**: このような円記号はコピーしないでください。また、改行はコマンドに含めないようにしてください。 これらの文字は、実際のコマンド構文の一部ではありません。

例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

この例の内容

- 標準的な等幅フォントで表示されているコマンド名（ruler）は表示されているとおりに入力します。
- 斜体で表示されている *className* オプションは、クラス名（USER など）のプレースホルダです。

- 2 番目の角かっこで囲まれた部分を指定しなくても、コマンドは実行できます。この部分は、オプションのオペランドを示します。
- オプションのパラメータ（props）を使用する場合は、キーワード *all* を選択するか、またはカンマで区切られたプロパティ名を 1 つ以上指定します。

ファイル ロケーションに関する規則

CA Access Control のドキュメントには、ファイル ロケーションに関する以下の規則があります。

- *ACInstallDir* -- CA Access Control のデフォルトのインストール ディレクトリ。
  - Windows -- <インストール パス>
  - UNIX -- <インストール パス 2>
- *ACSharedDir* -- CA Access Control for UNIX で使用される、デフォルトのディレクトリ。
  - UNIX -- /opt/CA/AccessControlShared
- *ACServerInstallDir* -- CA Access Control エンタープライズ管理 のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir* -- デフォルトの配布サーバ インストール ディレクトリ。
  - /opt/CA/DistributionServer
- *JBoss_HOME* -- デフォルトの JBoss インストール ディレクトリ。
  - /opt/jboss-4.2.3.GA

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

以下のドキュメントのアップデートは、本書の最新のリリース以降に行われたものです。

- CA Access Control エンドポイントおよびサーバ コンポーネントのインストール - この章を更新し、以下の変更を行いました。
  - CA Access Control へのアップグレード時にライセンス エラーが発生します

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

本書では、CA Access Control Premium Edition に関する一般的な問題の解決策および回避策を示します。

用語を簡潔に示すために、本書の全体を通してこの製品を CA Access Control と呼びます。

本書の対象読者

本書は、CA Access Control によって保護される環境の実装、設定、およびメンテナンスを行うときに発生する問題に対処するセキュリティ管理者およびシステム管理者を対象としています。

第 2 章: CA Access Control エンドポイントおよびサーバ コンポーネントのインストール

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 Access Control エンタープライズ管理 インストール中の「不正なインタープリタ」エラー メッセージ

UNIX および Linux に該当

症状:

CA Access Control エンタープライズ管理 をインストールしようとすると、以下のエラー メッセージを受信します。

`/bin/sh： 不正なインタープリタ： 許可が拒否されました。`

解決方法:

一部の UNIX と Linux のリリースでは、noexec オプションを指定すると、オペレーティング システムが光ディスク ドライブを自動マウントします。CA Access Control エンタープライズ管理 をインストールするには、光ディスク ドライブが noexec オプションでマウントされていないことを確認します。

CA Access Control エンタープライズ管理 データベース パスワードに文字「$」を使用できない

症状:

CA Access Control エンタープライズ管理 のインストール時に、データベース パスワードを入力すると「データベースのバージョンを検出できませんでした」というエラーメッセージが表示されます。

解決方法:

パスワードの末尾に「$」記号を指定すると、CA Access Control エンタープライズ管理 インストールがこのエラー メッセージを表示します。 パスワードの末尾に「$」記号を指定する場合は、インストール後にデータベース パスワードを変更する必要があります。

CA Access Control サーバ コンポーネントを開けない

症状:

必要なすべての CA Access Control サービスの起動後に、Web ブラウザで CA Access Control エンタープライズ管理、CA Access Control エンドポイント管理、または CA Access Control パスワード マネージャを開くことができません。 同じサーバには JBoss および Oracle をインストールしました。

解決方法:

Oracle と JBoss はどちらもデフォルト ポートの 8080 を使用します。 この問題を修正には、Oracle と JBoss 間のポートの競合を解決する必要があります。 Oracle または JBoss のポートを変更する前に、より簡単に自社に実装できる変更はどちらであるかを検討する必要があります。

デフォルトの JBoss および Oracle ポートを変更するには、以下の手順に従います。

デフォルトのポート番号を変更する方法

1. コマンドウィンドウを開き、以下のディレクトリに移動します（*JBossInstallDir* は JBoss のインストール ディレクトリ）。

   JBossInstallDir/bin

2. JBoss を停止します。
   - （Windows） shutdown.bat -S
   - （UNIX） shutdown.sh -S
3. テキストエディタで次のファイルを開きます。

   JBossInstallDir/server/default/deploy/jbossweb-tomcat55.sar/server.xml
4. 以下のセクションのポート番号を変更します。

   ```
   <!-- A HTTP/1.1 Connector on port 8080 -->
       <Connector port="8080" address="${jboss.bind.address}"
   ```
5. ファイルを保存して閉じます。
6. テキストエディタで次のファイルを開きます。

   JBossInstallDir/server/default/deploy/httpha-invoker.sar/META-INF/jboss-service.xml

7. 以下の各行のポート番号を変更します。

```
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerHAServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/readonly/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerHAServlet</attribute>
```

8. ファイルを保存して閉じます。
9. JBoss を起動します。
10. （Windows）CA Access Control エンタープライズ管理、CA Access Control エンドポイント管理、CA Access Control パスワード マネージャの ショートカットを以下の手順に従って変更します。
    a. ［スタート］-［プログラム］-［CA］-［Access Control］をクリックし、該当するショートカットを右クリックします。

       たとえば、CA Access Control エンタープライズ管理 ショートカットを変更するには、［スタート］-［プログラム］-［CA］-［Access Control］を選択し、［エンタープライズ管理］を右クリックします。
    b. ［プロパティ］をクリックします。
    c. URL フィールドのポート番号を新しい JBoss ポート番号に変更します。

デフォルトのポート番号を変更する方法

1. SQL コマンド ラインを起動します。
2. sysdba として Oracle に接続します：

```
connect / as sysdba
```

3. HTTP 通信に現在使用されているポートを確認します。

```
select dbms_xdb.gethttpport from dual;
```

4. 目的のポート番号に設定します。

```
exec dbms_xdb.sethttpport('portNumber');
```

5. データベースを停止して再起動します。

```
shutdown immediate
startup
```

CA Access Control エンタープライズ管理 にタブが表示されない

Active Directory ユーザ ストアに該当

症状:

CA Access Control エンタープライズ管理 のインストールは正常終了しました。インストール中に指定したシステム ユーザとしてログインすると、インターフェースにタブが表示されません。

解決方法:

CA Access Control エンタープライズ管理 をインストールする際、以下の Active Directory パラメータを指定してください。

- ホスト
- ポート
- 検索ルート
- ユーザ DN （およびこのユーザのパスワード）
- システム ユーザ

この問題は、Active Directory の検索ルートが、ディレクトリ ツリー内でユーザ DN およびシステム ユーザの DN （識別名）と同じノード内にある場合に発生します。この問題を解決するには、ユーザ DN およびシステム ユーザの DN よりもディレクトリ ツリー内で 1 ノード以上上位に検索ルートを指定してください。

例: Active Directory の検索ルート

この例では以下のユーザ DN およびシステム ユーザの DN を使用します。

- ユーザ DN： CN=MyQueryUser,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
- システム ユーザ： CN=MySystemManager,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB

以下の検索ルートは、ユーザ DN およびシステム ユーザの DN よりもディレクトリ ツリー内で 1 ノード上位に指定されています。 検索ルートを以下のように指定すると、CA Access Control エンタープライズ管理 が正常にインストールされ、インターフェースにタブが表示されます。

```
OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

以下の検索ルートは、ディレクトリ ツリー内でユーザ DN およびシステム ユーザの DN と同じノードにあります。検索ルートを以下のように指定すると、CA Access Control エンタープライズ管理 は正常にインストールされますが、インターフェースにタブが表示されません。

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

例: Active Directory 検索ルートをディレクトリ ツリー内で 1 ノード上位に設定する

この例では、上述の例と同じユーザ DN およびシステム ユーザの DN を使用します。

この例では、CA Access Control エンタープライズ管理 のインストール時に、以下の検索ルートを指定しています。

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

この検索ルートは、ディレクトリ ツリー内でユーザ DN およびシステム ユーザの DN と同じノードにあるので、ディレクトリ ツリー内で 1 ノード上位に指定する必要があります。

Active Directory 検索ルートをディレクトリ ツリー内で 1 ノード上位に設定する方法

1. Identity Manager 管理コンソールを有効にします。
2. Identity Manager 管理コンソールを開きます。
3. ディレクトリをクリックし、ac-dir ディレクトリをクリックします。

   ディレクトリ プロパティのダイアログ ボックスが表示されます。
4. ディレクトリ プロパティのダイアログ ボックスの下部にある [エクスポート] をクリックします。
5. メッセージが表示されたら、XML ファイルを保存し、編集用に開きます。

   注: ファイル名は ac-dir.xml です。
6. インストール中に指定した検索ルートが含まれるタグを指定します。以下に例を示します。

   ```
   <LDAP searchroot="OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB"
   secure="false"/>
   ```

7. 既存の検索ルートを新しい検索ルートで置き換えます。以下に例を示します。

   ```
   <LDAP searchroot="OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB" secure="false"/>
   ```

   注: エンタープライズ OU (組織の単位) を削除したので、この検索ルートは、ディレクトリ ツリー上で前の検索ルートより 1 ノード上位に配置されています。

8. ファイルを保存して閉じます。

9. Identity Manager 管理コンソールのディレクトリのプロパティ ダイアログボックスで、［更新］をクリックします。

   ディレクトリの更新ページが表示されます。

10. ファイルの選択をクリックし、編集した XML ファイルを指定して、［開く］、［完了］をクリックします。

    Identity Manager 管理コンソールは XML ファイルを検証し、ディレクトリ設定出力フィールドにステータス情報を表示します。

    注: インポート失敗のエラーを受信した場合は、「ac-dir.xml ディレクトリ設定ファイルをインポートできない」のトピックを参照してください。

11. ［続行］をクリックします。

    ［ディレクトリ］ページが表示されます。

12. ac-dir をクリックし、［環境］セクションで ac-env をクリックします。

    環境プロパティ ページが表示されます。

13. ［再起動］をクリックします。

    Identity Manager 管理コンソールで環境が再起動され、変更が適用されます。

注: Identity Manager 管理コンソールを有効にし、開始する方法の詳細については、「*実装ガイド*」を参照してください。

詳細情報:

ac-dir.xml ディレクトリ設定ファイルをインポートできない (P. 22)

ac-dir.xml ディレクトリ設定ファイルをインポートできない

症状:

Identity Manager 管理コンソールから ac-dir.xml ディレクトリ設定ファイルをエクスポートしました。ファイルをインポートしようとすると、ディレクトリ設定出力フィールドに以下のエラー メッセージが表示されます。

```
Deploying directory configuration...

Parsing input stream...
Error: (140:67): cvc-complex-type.4: Attribute "value" must appear on element
"Container".
Error: Failed to import

*********
1 error(s), 0 warning(s)
```

解決方法:

ac-dir.xml ディレクトリ設定ファイルには、ユーザ ストアの構造と内容が記述されています。 このファイルは、CA Access Control エンタープライズ管理 によるユーザ ストアの制御方法を変更するために使用します。たとえば、ユーザ ディレクトリ パスワードや Active Directory 検索ルートの変更などです。 また、CA Access Control エンタープライズ管理 を SSL 通信用に設定したり、Active Directory をフェールオーバ用に設定したりする場合にも、ac-dir.xml ファイルを編集します。

この問題を解決するには、以下の手順に従います。

1. ac-dir.xm ファイルを編集用に開きます。
2. 以下のタグを検索します。

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou"/>
   ```

3. 上述のタグを以下のタグで置き換えます。

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

4. ファイルを保存して閉じます。

これで、ディレクトリ設定ファイルを Identity Manager 管理コンソールにインポートできるようになりました。 ディレクトリ設定ファイルの変更を適用するには、ファイルのインポート後に、環境を再起動する必要があります。

CA Access Control エンタープライズ管理 が DMS に接続できない

症状:

CA Access Control エンタープライズ管理 にログインすると、以下のようなメッセージが表示されます。

エラー： ログインできませんでした。
エラー： ターゲット上のパスワードがクライアントのパスワードと一致しません。

解決方法:

ユーザ ac_entm_pers は DMS にログインできません。 このユーザは、エンタープライズ管理サーバと DMS の間の通信およびデータ フローを認証します。

注: ac_entm_pers ユーザには、以下の権限属性があります。 ADMIN、AUDITOR、IGN_HOL、LOGICAL

この問題を解決するには、以下の手順に従います。

1. selang を開きます。
2. DMS に接続します。

   ```
   host DMS__@entM_host_name
   ```

3. ac_entm_pers のパスワードを変更します。

   ```
   eu ac_entm_pers password(password) nonative grace-
   ```

4. エンタープライズ管理サーバがインストールされているホストに ac_entm_pers がログインすることを許可します。

   ```
   authorize TERMINAL entM_host_name uid(ac_entm_pers) access(a)
   ```

5. ac_entm_pers がエンタープライズ管理サーバにログインできることを確認します。

   ```
   host DMS_@entM_host_name uid(ac_entm_pers) password(password) logical
   ```

6. ac_entm_pers の新しいパスワードを使用して、エンタープライズ管理サーバの DMS 接続設定を更新します。

   DMS によって ac_entm_pers が認証され、CA Access Control エンタープライズ管理 は DMS に接続します。

   注: DMS への接続を設定する方法の詳細については、CA Access Control エンタープライズ管理 オンライン ヘルプを参照してください。

接続設定の更新時にエラーを受信した場合、DMS では ac_entm_pers を認証できません。 この問題を解決するには、以下の手順に従います。

1. これまでの手順で、各手順に同じパスワードを入力したことを確認します。
2. 前述の手順 4 で、エンタープライズ管理サーバ（*entM_host_name*）のホスト名が正しいことを確認します。

   たとえば、手順 4 でエンタープライズ管理サーバの完全修飾ホスト名を指定した場合、エンタープライズ管理サーバの TERMINAL レコードで簡略ホスト名を使用していると、ホスト名は解決されず、ac_entm_pers はエンタープライズ管理サーバにログインできません。
3. CA Access Control 監査ファイルを確認します。

   ```
   seaudit -a
   ```
4. DMS 監査ファイルを確認します。

   ```
   seaudit -a -fn DMS_log_file
   ```

   注: 監査レコードには、エンタープライズ管理サーバの TERMINAL レコードの正しいホスト名に関する情報が提供されている場合があります。

例: DMS 監査ファイルの表示

以下の例は、DMS__ という名前の DMS 用監査ファイルを表示します。

```
seaudit -a -fn "C:¥Program
Files¥CA¥AccessControlServer¥APMS¥AccessControl¥Data¥DMS__¥pmd.audit"
```

CA Access Control エンタープライズ管理 タブで疑問符が表示される

症状:

CA Access Control エンタープライズ管理 を開くと、タブに疑問符が表示されます。

解決方法:

この問題を解決するには、ブラウザのデフォルト言語を米国英語に変更します。

InfoView に表示される「NULL ページ」エラー

症状：

CA Access Control レポートへのアクセスを試みると、InfoView に次のエラーが表示されます。

NULL ページ： レポート ソースからページを作成できません。

解決方法：

Windows の場合、CA Access Control Universe が適切に定義されていないか、またはインストールされていない場合があります。 CA Access ControlUniverse 用の接続をテストします。接続が正常ではない場合は接続を編集し、正常である場合は接続を置き換えます。

Solaris の場合、bouser としてログインし、CASHCOMP/CommonReporting/bobje/setup/env.sh を以下のとおり編集します。

1. 以下の LIBRARYPATH を追加します。

   ```
   $MWHOME/lib-sunos5_optimized
   ```

2. BusinessObjects サービスを再起動します。

   ```
   cd$CASHCOMP/CommonReporting/bobje
   ./stopservers
   ./startservers
   ```

UNIX へのインストール後に CA Access Control が自動的に起動しない

UNIX に該当

症状:

UNIX エンドポイントへのインストール後に CA Access Control が自動的に起動しません。

解決方法:

デフォルトでは、CA Access Control は UNIX エンドポイントでは自動的に起動しません。

UNIX コンピュータの起動時に seosd デーモンが自動的に起動するように設定するには、*ACInstallDir*/samples/system.init/*sub-dir* ディレクトリを使用します。*sub-dir* はご使用のオペレーティング システムに対応したディレクトリです。 各サブディレクトリには、オペレーティング システム上で CA Access Control を自動的に起動する方法を説明した Readme ファイルがあります。

注: CA Access Control の起動の詳細については、「*実装ガイド*」を参照してください。

Linux s390 エンドポイント上でデーモンを開始できない

Linux s390 および Linux s390x に該当

症状:

seosd または ReportAgent デーモンを開始できません。

解決方法:

CA Access Control で、エンドポイント上の Java 環境を特定できません。 この問題を解決するには、以下の手順に従います。

1. accommon.ini ファイル内の global セクションの java_home 設定に、Java 環境へのパスが含まれていることを確認します。
2. LD_LIBRARY_PATH 環境変数の値を、Java 環境の共有ライブラリへのパスに設定します。

インストール後に selang に接続できない

症状:

CA Access Control のインストール後に selang を起動するか、CA Access Control データベースに接続しようとすると、以下のエラーが発生します。

```
エラー： 初期化に失敗しました。終了します。
(localhost)
エラー: ログインできませんでした。
エラー： 端末 example.com からこのサイトを管理する権限がありません。
```

解決方法:

端末ルールが正しく定義されていません。 端末ルールをトラブルシューティングして問題を特定します。

端末ルールをトラブルシューティングする方法

1. CA Access Control を停止します。

   ```
   secons -s
   ```

2. selang をローカル モードで起動します。

   ```
   selang -l
   ```

   注: UNIX コンピュータ上で selang をローカル モードで実行するには、root ユーザである必要があります。

3. ローカル端末（*terminal_name*）用の TERMINAL レコードが作成されており、端末のアクセス権限が以下のように正しく定義されていることを確認します。

   ```
   showres TERMINAL terminal_name
   ```

   - レコードが存在しない場合は、ローカル端末用の TERMINAL レコードを作成します。

     ```
     editres TERMINAL terminal_name owner (name) defaccess (accessAuthority)
     ```

     注: 所有者はユーザまたはグループのいずれかです。 TERMINAL レコードに対するデフォルト アクセス権は none であるため、レコードの作成時にデフォルト アクセスを指定して、ユーザが端末からロックアウトされないようにしてください。

   - 端末アクセス権限が正しくない場合は、端末に対する正しいアクセス権限を定義します。

     ```
     authorize TERMINAL terminal_name uid(name) access(accessType)
     ```

4. （UNIX） [seosd] セクション中の terminal_default_ignore 設定の値を確認します。

   この設定値は、管理アクセスを許可するときに、CA Access Control が _default TERMINAL および特定の TERMINAL レコードの defaccess 値を考慮するかどうかを指定します。

   注: terminal_default_ignore 設定の詳細については、「*リファレンス ガイド*」を参照してください。

5. （UNIX）以下の手順に従って、lookaside データベースが端末を反映していることを確認します。

   a. ホスト名固有の lookaside データベースを構築します。

      ```
      sebuilda -h
      ```

   b. lookaside データベースの端末エントリとホスト名が同じであることを確認します。

      ```
      sebuilda -H | grep hostname
      ```

      hosts lookaside データベース ファイルの内容が一覧表示されます。

6. CA Access Control を起動します。

   - （UNIX） seload
   - （Windows） seosd -start

注: これでもなお selang を起動できないか、または CA Access Control データベースに接続できない場合は、ご使用の OS 用の hosts ファイルの変更が必要な場合があります。 システム管理者またはネットワーク管理者に連絡してサポートを受けてください。

Solaris 10 ログ ファイルに記録されたメッセージ

Solaris 10 で有効

症状:

「secons -s」を使用して CA Access Control を停止すると、「/var/adm/messages」ログ ファイルに記録されている CA Access Control メッセージが Solaris 10 コンピュータに表示されます。 使用しているコンピュータの SEOS_use_streams の値が yes に設定されます。

解決方法:

これらのメッセージは参考メッセージであり、障害またはエラーを示すものではありません。 対処の必要はありません。 メッセージとその意味を以下に示します。

- "SEOS: Restored tcp wput" "SEOS: Restored strrhead rput"

  SEOS_syscall 機能により、ネットワーク フックが無効にされたことを示します。

- "SEOS: Replaced tcp wput" "SEOS: Replaced strrhead rput"

  SEOS_syscall 機能により、ネットワーク フックが有効にされたことを示します。

アンインストール中に手動でレジストリ キーを削除するときにエラーが発生する

Windows で該当

症状:

CA Access Control のアンインストール中にレジストリ キーを削除しようとすると、以下のエラー メッセージが表示されます。
データを開けません。キーを開こうとしてエラーが発生しました。

解決方法:

RemoveAC.exe ユーティリティを実行して CA Access Control レジストリ キーおよびディレクトリを削除します。 RemoveAC.exe ユーティリティでは製品はアンインストールされませんが、すべての CA Access Control レジストリ キーおよびディレクトリがコンピュータから削除されます。

注: RemoveAC.exe ユーティリティは、CA Access Control インストール パッケージには含まれていません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

ProductExplorer が開始されない

症状:

Windows 用の CA Access Control Premium Edition Server Components DVD を光学ドライブに挿入しても、ProductExplorer が起動しません。

解決方法:

以下の手順を実行します。

- 光学ディスク ドライブのディレクトに移動して、ProductExplorerx86.EXE ファイルをダブルクリックします。
- 自動実行を有効にして、ProductExplorer を自動的に起動します。

CA Licensing 1.9.04 にアップグレードするときにライセンス エラーが発生する

UNIX で有効

症状:

CA Access Control をアップグレードするとき、新しい CA Licensing rpm スクリプト（1.9.04）が最初に実行されます。 その後、以前の rpm スクリプト用のアンインストーラが実行され、UNIX syslog に以下のエラー メッセージが記録されます。

```
<Error opening lic98.err - /opt/CA/SharedComponents/ca_lic/lic98.err, original
code=5000>2E2U eTrust Access Control for UNIX <Error opening lic98.err -
/opt/CA/SharedComponents/ca_lic/lic98.err, original code=5000>  LRF=2E2U,
000000000000, Linux_x86.64_1_*, ismelx84, 0
```

解決方法:

CA Licensing バージョン 1.9.03 またはそれ以前のインストーラでは、リンクとフォルダが削除され、エラーが発生します。 アップグレードを実行せずに、CA Licensing バージョン 1.9.04 を直接インストールすることを推奨します。

次の手順に従ってください:

1. CA Access Control が実行中である場合は、管理者としてログインし、以下のコマンドを入力して CA Access Control を停止します。

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. 以下のファイルを一時フォルダにバックアップします。
   - /etc/profile
   - /etc/profile.CA
   - /etc/csh_login.CA
   - 以下のエントリのすべてのシンボリック リンク情報を書き留めます。
     - /usr/local/CAlib
     - /opt/CA/CAlib
     - $CASHCOMP/CAlib
     - /ca_lic

- /opt/CA/ca_lic
- $CASHCOMP/ca_lic
- $CASHCOMP/lib

3. すべてのシンボリック ディレクトリをバックアップします。
4. サポート Web サイトから最新の CA Licensing パッケージをダウンロードします。
5. 圧縮ファイルの内容を一時ディレクトリに解凍します。
6. 新しい lic98_install ディレクトリに移動します。
7. 以下のコマンドを入力して、CA Licensing をインストールします。

   ```
   ./install <インストール ディレクトリ>
   ```

8. 以下のコマンドを入力して、/etc/profile に source コマンドを実行します。

   ```
   ./etc/profile
   ```

9. 以下の手順に従って、ca.olf ファイルをリストアします。
   a. 以下のコマンドを実行します。

      ```
      rpm -e --nodeps ca-lic
      ```

   b. 手順 2 でバックアップされたディレクトリを、以下のディレクトリにリストアします。

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   c. 手順 2 （d）で書き留めたシンボリック リンクを、以下のディレクトリにリストアします。

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   d. バックアップした /etc/profile、/etc/profile.CA、および /etc/csh_login.CA ファイルを以下のディレクトリにリストアします。

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   CA Licensing 1.9.04 が正常にインストールされ、すべての登録済み CA 製品の使用を開始できます。

第 3 章: ポリシーおよびアクセス権限の作成

このセクションには、以下のトピックが含まれています。

ネットワークドライブと共有ドライブへのユーザ アクセスのブロック

Windows で有効

症状:

システム ドライブへのユーザ アクセスはブロックできますが、ネットワーク ドライブと共有ドライブへのユーザ アクセスを停止できません。

解決方法:

Windows 2008 上のネットワーク/共有ドライブへのユーザ アクセスをブロックするには、以下の selang コマンドをポリシーに追加します。

```
newres FILE ¥Device¥Mup¥*
```

Windows 2003 上のネットワーク/共有ドライブへのユーザ アクセスをブロックするには、以下の selang コマンドをポリシーに追加します。

```
newres FILE ¥Device¥LanmanRedirector¥*
```

保護されたリソースにユーザがアクセスできる

症状:

あるリソースのデフォルト アクセス権限として none を作成しましたが、スーパーユーザが今までどおりそのリソースにアクセスできます。

解決方法:

リソース アクセスに関する問題のトラブルシューティングを行います (P. 131)。

読み取りアクセス チェックで /etc/passwd および /etc/group ファイルがバイパスされる

UNIX で該当

症状:

/etc/passwd および /etc/group ファイルに対するデフォルト アクセス権限 none を設定したルールを作成したにもかかわらず、これらのファイルに読み取りアクセスできてしまいます。

解決方法:

デフォルトでは、CA Access Control 認証エンジンは /etc/passwd および /etc/group システム ファイルに対する読み取りアクセス チェックをバイパスします。CA Access Control がこれらのシステム ファイルに対する読み取りアクセス チェックをバイパスしないようにするには、seos.ini ファイルの [seosd] セクション中の bypass_system_files の値を no に変更します。

重要: CA Access Control がこれらのシステム ファイルに対する読み取りアクセス チェックをバイパスしないようにする場合、適切な許可が設定されていることを確認します。 適切な許可を設定せず、読み取りアクセス チェックのバイパスを停止した場合、CA Access Control 管理者と root ユーザを含むユーザがシステムにアクセスできなくなり、重要なシステム処理に失敗する場合があります。

エンタープライズ ユーザまたはグループがリソースにアクセスできないが、正しいアクセス ルールが設定されている

Windows で該当

症状:

エンタープライズ ユーザまたはグループがリソースにアクセスする許可を持っているのに、アクセスできません。

解決方法:

エンタープライズ アカウントが再利用されている可能性があります。データベース内の許可は、名前が同一で SID が異なる新規アカウントではなく、古いアカウントに適用されています。 この状況をチェックするには、再利用エンタープライズ アカウントを解決します。

注: 再利用エンタープライズ アカウントの詳細については、「*Windows エンドポイント管理ガイド*」を参照してください。

ログインに失敗したユーザをロックアウトできない

UNIX で該当

症状:

ログインの失敗が指定の回数に達した後にパスワード PMD でユーザを禁止するように serevu を設定しています。 しかし、正しくログインできない場合でもユーザがロックアウトされません。 pam_failed_logins.log ファイルを参照するために nodaemon オプションを指定して serevu を起動したときに、サーバが応答しません。

解決方法:

seos.ini ファイルの [seos] セクション中の passwd_pmd の値が正しくありません。 passwd_pmd の値を、sepass がパスワード更新を送るパスワード PMD の名前に設定します。

ユーザが時間制限を超えてコマンドを実行できる

症状:

グループに対して時間制限を設定したにもかかわらず、グループ メンバが許可された時間を超えて CA Access Control コマンドを実行できてしまいます。

解決方法:

制限期間中、CA Access Control はユーザが新しいログイン セッションを開始するのを防止しますが、切断を強制することはできません。 ユーザが制限期間中にリソースまたはコマンドにアクセスするのを防止するには、リソースまたはコマンドのリソース レコードを変更して時間制限を指定します。

注: CA Access Control は、ユーザの USER または XUSER レコードに時間制限が存在するかどうかを確認してから、そのユーザが属する GROUP または XGROUP に対する時間制限が存在するかどうかを確認します。

CA Access Control がすべてのユーザを root として認識する

UNIX で該当

症状:

root 以外のユーザに対して sewhoami ユーティリティを実行した場合、CA Access Control はこのユーザを root ユーザとして認識してしまいます。

解決方法:

この問題をトラブルシューティングするには、ログイン アプリケーションの LOGINAPPL レコードで以下を検証します。

- LOGINAPPL レコードの名前がログイン アプリケーションの名前である。
- LOGINAPPL レコードの LOGINPATH パラメータがログイン アプリケーションへの正確なフル パスを指定している。

  ログイン アプリケーションへのパスを調べるには、トレースを実行 (P. 135)し、次にログイン アプリケーションを使用して CA Access Control にログインしてログアウトします。 トレースを参照してパスを取得します。
- LOGINAPPL レコードの LOGINSEQUENCE パラメータに、ログイン アプリケーション用の正しいログイン シーケンスが指定されている。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

注: CA Access Control は、サードパーティ ログイン アプリケーション用の LOGINAPPL レコードを定義しません。 サードパーティ ログイン アプリケーションを使用する場合は、そのアプリケーション用の LOGINAPPL レコードを手動で定義してください。

1 つのグループだけにユーザをパスワード管理者として追加できない

症状:

あるユーザを特定のグループのパスワード管理者として指定したいのですが、以下のコマンドを実行すると、そのユーザがすべてのグループのパスワード管理者になってしまいます。

```
editusr userName pwmanager
```

解決方法:

ユーザをパスワード管理者として追加する対象グループの名前を以下のように指定します。

```
join userName group(groupName) pwmanager
```

Windows 管理者が CA Access Control パスワードを変更できる

Windows で該当

症状:

CA Access Control で保護された自分の Windows 環境で Windows 管理者が <eAC の> パスワードを変更できてしまいます。

解決方法:

CA Access Control で指定するユーザだけが CA Access Control パスワードを変更できるようにするには、以下のキー EnforceViaeTrust レジストリ エントリの値を 1 に設定します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥passwd
```

このレジストリ エントリは、CA Access Control を通さなければユーザ パスワードの更新または作成ができないかどうかを指定します。 このレジストリ エントリのデフォルト値は 0 です。この場合、CA Access Control を使用しなくてもユーザ パスワードを更新または変更できます。

グローバル パスワード ポリシーにより、保護されたシステムからユーザがロックされる

症状:

グローバル パスワード ポリシーを実装した場合、そのパスワード ポリシーが原因で、CA Access Control で保護されたシステムからユーザがロックされてしまいます。

解決方法:

<eAC の> で保護されたシステムにアクセスする必要があるユーザ用のパスワード ポリシーを別個に作成します。 これらのユーザに対するパスワード ポリシーを作成するには、プロファイル グループを使用します。

プロファイル グループを使用してパスワード ポリシーを実装するには、以下の手順に従います。

1. プロファイル グループを作成します。
2. プロファイル グループ用のパスワード ポリシーを設定します。
3. プロファイル グループにユーザを割り当てます。

   プロファイル グループに対して設定したパスワード ポリシーは、そのプロファイル グループに関連付けられているユーザに適用されます。

対話式アプリケーションに関するタスク委任がハングする

Windows で該当

症状:

ユーザが notepad.exe などの対話式アプリケーションを実行するためのタスク委任ルールを書いた場合、 ユーザがアプリケーションを実行しようとすると、タスク委任がハングします。

解決方法:

ユーザがアプリケーションを実行できるようにするには、対話式フラグが SUDO クラス レコードに設定されている必要があります。タスク委任を使用して対話式 Windows アプリケーションを実行する場合、対話式フラグが設定されていないと、アプリケーションはバックグラウンドで実行されユーザが操作することができません。

この問題を解決するには、以下の手順に従います。

1. SUDO レコードの対話式フラグを設定します。

   ```
   er SUDO resourceName interactive
   ```

   resourceName

   ユーザがアプリケーションを起動できるようにするリソース レコードの名前を指定します。

   指定されたリソースの対話式フラグが設定されます。

2. 以下の手順でタスク委任サービスを再起動します。

   a. 対話式アプリケーションを強制終了します。

   b. タスク委任がまだハングしている場合は、CA Access Control を再起動します。

注: タスク委任および SUDO レコードの定義の詳細については、「Windows エンドポイント管理ガイド」を参照してください。

第 4 章: CA Access Control データベースの管理

このセクションには、以下のトピックが含まれています。

selang クエリで返されるレコードが最大 100 個に限られる

症状:

100 を超えるレコードを返すはずの selang クエリを実行したときに、以下のメッセージが表示されます。

警告: 100 (クエリ サイズ制限) 項目のみが表示されています。

解決方法:

query_size 設定のデフォルト値は 100 です。 CA Access Control が selang クエリに対して返すレコードの数を増やすには、query_size 設定値を変更します。

query_size 設定は、以下の場所に存在します。

- （UNIX） seos.ini ファイルの [lang] セクション
- （Windows）以下の lang サブキー

  HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥lang

データベース バックアップ後の監査ログ内の UTimes および拒否されたレコード

症状:

CA Access Control の実行中に OS バックアップ ツールを使用して CA Access Control データベースをバックアップした場合、CA Access Control は以下のメッセージのようなエントリを監査ログに送ります。

```
03 Mar 2008 15:58:01 D FILE            UTimes     69 10
/opt/CA/AccessControl/seosdb/seos_pvf.fre /usr/sbin/fbackup
```

注: 上記の例では UNIX パス名が使用されていますが、以下の解決方法は Windows コンピュータにも適用されます。

解決方法:

上記の監査メッセージは、バックアップ処理による UTimes ファイル日付スタンプの更新を CA Access Control が妨げたことを示しています。 CA Access Control はバックアップ自体を妨げてはいません。

このメッセージが監査ログに表示されないようにするには、以下の手順に従います。

- バックアッププログラムが非スーパーユーザによって実行される場合は、そのユーザに対して OPERATOR 属性が設定されていることを確認します。
- バックアッププログラムがスーパーユーザによって実行される場合は、バックアッププログラムに pgmtype （バックアップ）プロパティが指定された SPECIALPGM レコードが存在することを確認します。

データベースが正しくバックアップされるようにするには、dbmgr ユーティリティを使用してバックアップを実行します。

CA Access Control データベースが破損している

UNIX で該当

症状:

CA Access Control エラー ログに以下のようなメッセージが示されます。

```
seoswd: [ID 973226 auth.error] seosd との通信がタイムアウトになりました。 seosd を実行しています。
FATAL!
Inseosrt_InitDatabase (0x270)
警告: パス Access Control/seosdb/seos_cdf.dat が破損しました
```

解決方法:

以下の手順に従って、データベースの破損を修復します。

注: この手順は、データベースがデフォルトのインストール場所、/opt/CA/AccessControl/ にインストールされていることを前提としています。

CA Access Control データベース破損を修復する方法

1. CA Access Control を停止します。

   ```
   secons -s
   ```

2. （オプション）必須な場合はテクニカル サポートにデータベースを提供できるように、データベースを別の場所にバックアップします。

3. データベースがクローズとしてマークされていることを確認します。

   ```
   cd /opt/CA/AccessControl//seosdb

   dbmgr -util -close
   ```

   注: CA Access Control が正しくシャットダウンされない場合、データベースがオープンとしてマークされる場合があります。

4. データベースをチェックします。

   ```
   dbmgr -util -check
   ```

5. 以下の*いずれか*の操作を実行します。
   - データベースをチェックしたときにエラー メッセージが表示されない場合は、ステップ 6 に進みます。
   - データベースをチェックしたときにエラー メッセージが表示された場合は、ステップ 6 および 7 を実行せず、代わりにデータベースを再構築 (P. 138)します。
6. データベース ファイルを再構築します。

   ```
   dbmgr -util -build all
   ```
7. データベース エンジンを再チェックします。

   ```
   dbmgr -util -check
   ```
8. CA Access Control を起動します。

   ```
   seload
   ```

注: データベースがまだ破損している場合は、さらに詳しい調査が必要となります。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

第 5 章: リモート コンピュータへの接続

このセクションには、以下のトピックが含まれています。

リモートコンピュータから接続できない

症状:

リモート CA Access Control コンピュータに接続できません。

解決方法:

接続に関する問題のトラブルシューティングを行います (P. 131)。

seosd との通信タイムアウトが syslog に継続的に表示される

Windows で該当

症状:

CA Access Control を実行しているときにコンピュータが遅くなり、以下のメッセージが syslog に表示されることがあります。

```
seoswd: seosd との通信がタイムアウトになりました。 seosd を実行しています。
seoswd: seosd に対して返された 5378 [Success] との間に通信上の問題が発生しました。
seoswd: 説明: seosd との通信がタイムアウトになりました。
```

解決方法:

CA Access Control がタイムアウトになる原因は、コンピュータ上のアンチウイルス ソフトウェアです。 アンチウイルス ソフトウェアで、以下の手順を行います。

- リアルタイム スキャンから CA Access Control ディレクトリを除外します。
- CA Access Control ディレクトリのリアルタイム (オン アクセス) スキャンを停止します。

CA Access Control がデフォルトで CA Access Control レジストリ キー、ファイル、およびインストール ディレクトリを保護するので、上記の操作を行ってもウイルスの脅威が増大することはありません。

アンチウイルス ソフトウェア用の SPECIALPGM レコードを作成し、SPECIALPGM レコードの PGMTYPE プロパティを pbf に設定することをお勧めします。 pbf プログラム タイプは、ファイル処理イベントに対するデータベース チェックをバイパスします。

最初の受信 FTP 接続を制御できない

UNIX で該当

症状:

CA Access Control を起動したときに、vsftpd からの最初の受信 FTP 接続を制御できません。 FTP 用の TCP ルールおよび vsftpd 用の HOST ルールは作成済みであり、vsftpd からの以後の FTP 接続は、その TCP または HOST ルールに基づいて CA Access Control によってすべて制御されます。

解決方法:

CA Access Control を起動する前に vsftpd を起動した場合、vsftpd は受信 FTP 接続に対する受け入れシステム コールにフックを配置します。 このフックが存在する場合、CA Access Control がインターセプトする前に vsftpd は最初の受信 FTP 接続を処理します。

FTP 接続の処理後、vsftpd は次の FTP 接続のために受け入れシステム コールを呼び出そうとします。 しかし、CA Access Control はこのシステム コールをインターセプトするので、以後の FTP 接続をすべて制御できます。

最初の受信 FTP 接続をインターセプトするには、以下のいずれかの回避策を使用します。

- vsftp を起動する前に CA Access Control を起動します。
- inetd や xinetd などのスーパーサーバ デーモンを使用して vsftpd を起動します。

  注: スーパーサーバ デーモンの設定の詳細については、ご使用の OS のベンダーに問い合わせてください。
- CA Access Control の起動後に tripAccept ユーティリティを実行します。

  tripAccept ユーティリティを実行するには、seos.ini ファイルの [SEOS_syscall] セクション中の call_tripAccept_from_seload トークンを有効にする必要があります。これを実行する前に、tripAccept ユーティリティ用の SPECIALPGM レコードを定義しておくことをお勧めします。

ローカル ホストとターゲット ホストのターゲットページが異なる

UNIX で該当

症状:

CA Access Control ホストに接続しようとすると、以下のメッセージが表示されます。

警告: ローカル マシンのコード ページがターゲット ホストのコード ページと異なっています。

解決方法:

ローカル ホストとターゲット ホストで、seos.ini ファイルの [seos] セクション中のロケール設定値が同じであることを確認します。

selang を使用してエンドポイントに接続できない

症状:

selang を使用してエンドポイントに接続しようとすると、以下のようなエラー メッセージが表示されます。

データをアンパックできませんでした

解決方法:

コンポーネント間通信を保護するために使用される暗号化に関する問題が存在します。 CA Access Control コンピュータで、暗号化キーおよび暗号化方法の変更が最近加えられたかどうかを確認します。

注: 暗号化方法の詳細については、「*実装ガイド*」を参照してください。

第 6 章: PMD からのルールのデプロイ

このセクションには、以下のトピックが含まれています。

サブスクライバ PMDB がマスタ PMDB から更新を受信できない

症状:

階層 PMDB アーキテクチャを使用しています。サブスクライバ PMDB がマスタ PMDB から更新を受信しません。 マスタ PMDB のエラー ログには以下のメッセージがあります。

親ではない PMDB からの更新を受け付けることはできません。

解決方法:

サブスクライバ PMDB がマスタ PMDB から更新を受信しない場合、以下の手順に従って問題をトラブルシューティングしてください。

PMDB の更新に関する問題をトラブルシューティングする方法

1. マスタ PMDB（*master_pmdb_name*）のサブスクライバのリストとそのステータスを表示します。

   ```
   sepmd -L master_pmdb_name
   ```

   注: このコマンドは、マスタ PMDB コンピュータで実行します。

2. サブスクライバのリストを参照して、使用できないサブスクライバを特定します。

3. 使用できない各サブスクライバで、parent_pmd 設定値が正しいことを確認します。

   parent_pmd 設定は以下の場所に存在します。

   - （UNIX） seos.ini および pmd.ini ファイルの [seos] セクション
   - （Windows）以下のレジストリ キー

     ```
     HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl
     ```

   注: parent_pmd トークンに指定するホスト名は、マスタ PMDB のホスト名と正確に一致する必要があります。 ホスト名解決が正しく設定されていることを確認することによって、この問題を解決できる場合があります。 UNIX コンピュータを使用している場合、sehostinf ユーティリティを使用してマスタ PMDB のホスト名を検出できます。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

問題がまだ存在する場合は、以下の手順に従います。

1. マスタ PMDB エラー ログを表示します。

   ```
   sepmd -e master_pmdb_name
   ```

2. エラー ログを参照し、使用できないサブスクライバについてレポートされたエラー コードをメモします。
3. 使用できないサブスクライバごとに、エラー コードに基づいて問題をトラブルシューティングします。

問題がまだ存在する場合は、以下の手順に従います。

1. マスタ PMDB が保持する使用できないサブスクライバのリストから問題のサブスクライバを削除します。

   ```
   sepmd -r pmdb_name subscriber_name
   ```

   親 PMDB は、そのサブスクライバに更新を送ろうとします。
2. 前の手順を繰り返します。
3. サブスクライバのリストまたは親 PMDB エラー ログに変更がある場合は、その変更に基づいて問題をトラブルシューティングします。

サブスクライバ エンドポイントの監査ログ中の失敗イベント

症状:

サブスクライバがマスタ PMDB から更新を受信しません。サブスクライバの CA Access Control 監査ログに*失敗*イベントが記録されています。

解決方法:

PMDB ユーザは ADMIN 属性を持っていません。 PMDB ユーザに ADMIN 属性を付与するには、以下の selang コマンドを使用してユーザ レコードを編集します。

```
chusr userName admin
```

注: selang コマンドを実行するには、ADMIN 属性が必要です。 PMDB 更新をサブスクライバにデプロイするときに CA Access Control は TERMINAL ルールを省略します。

第 7 章: ポリシーのデプロイ

このセクションには、以下のトピックが含まれています。

ポリシーのデプロイのトラブルシューティング

ホストにポリシーを割り当てる場合、policyfetcher がデプロイメント タスクを取得し、ポリシー スクリプトを実行するまで、ポリシーは割り当てられたエンドポイント上にデプロイされません。 したがって、エンドポイントでポリシーが転送されたりデプロイされたりするときに、さまざまな理由でデプロイ エラーが発生する可能性があります。

ポリシー デプロイメント エラーを解決するために、拡張ポリシー管理では以下のようなトラブルシューティング アクションが用意されています。これらのアクションは、CA Access Control エンタープライズ管理 または policydeploy ユーティリティのいずれかを使用して実行できます。 CA Access Control エンタープライズ管理 では、トラブルシューティング アクションは［ポリシー管理］タブの［ポリシー］サブタブにあります。

以下のようなトラブルシューティング アクションがあります。

- **Redeploy** - ポリシー スクリプトを含む新規デプロイメント タスクを作成し、作成したタスクをエンドポイントにデプロイします。

  エンドポイントでのポリシー デプロイ中にエラーが発生した場合に、このオプションを使用します。 つまり、selang ポリシー スクリプトの実行に失敗した場合です。 ポリシーのデプロイ解除を行うには、エンドポイントにおけるスクリプト エラーの原因を手動で解決しておく必要があります。

  注: このオプションは CA Access Control エンタープライズ管理 でのみ利用可能で、policydeploy ユーティリティではサポートされていません。

- **Undeploy** - ポリシーを対応するホストから割り当て解除せずに、指定されたエンドポイントからポリシーをデプロイ解除します。

  このオプションは、DMS 上のホストに割り当てられていないエンドポイントから任意のポリシーを削除するために使用します。

- **Reset** - エンドポイントをリセットします。 CA Access Control はホスト ステータスをリセットし、有効なポリシーをすべてデプロイ解除します。また、GPOLICY、POLICY、RULESET の各オブジェクトをすべて削除します。

  このオプションを使用すると、すべてのポリシー デプロイ からエンドポイントと DMS 上にあるエンドポイントのステータスを削除します。

  注: 監査に必要な場合があるため、このオプションでは DEPLOYMENT オブジェクトや GDEPLOYMENT オブジェクトはエンドポイントまたは DMS から 削除されません。 dmsmgr -cleanup 機能を使用すると、エンドポイントをリセットした後に DEPLOYMENT オブジェクトと GDEPLOYMENT オブジェクトを削除することができます。 エンドポイントをリセットした後、そのエンドポイントにポリシーを通常どおり割り当てることができます。

- **Restore** - 指定したホスト上のポリシーをすべてデプロイ解除します。次に、新規デプロイ タスクを作成し、そのタスクを実行するホストに送信することによって、ホスト上にデプロイする（アサインまたは直接デプロイする）必要のあるすべてのポリシーをリストアします。

  DMS がエンドポイント上で有効であることを示すポリシーをすべて再デプロイするために、CA Access Control やオペレーティング システムをエンドポイント上に再インストールする場合、またはバックアップからエンドポイントをリストアする場合には、このオプションを使用します。

ポリシーをすべてのエンドポイントに正常にデプロイできない

症状:

ホスト グループにポリシーをデプロイしました。 ホスト グループ内の一部のホストにはポリシーが正常にデプロイされましたが、一部のホストでエラーが発生しました。

解決方法:

この問題を解決するには、以下の手順に従います。

- デプロイに失敗したホスト数が少ない場合は、それらのホストにポリシーを再度デプロイします。

  ポリシーを再度デプロイするには、対象のホストのデプロイ エラーの原因を手動で解決しておく必要があります。

- デプロイに失敗したホスト数が多い場合は、エンドポイントごとに policydeploy -fix 関数を実行します。

  policydeploy -fix 関数は、指定されたデプロイ タスクまたはパッケージを修正して再度デプロイします。 この関数を使用するには、デプロイ タスクの名前を指定する必要があります。

注: policydeploy ユーティリティの詳細については「リファレンス ガイド」を参照してください。

例: policydeploy -fix 関数

以下の例は、エンドポイント上で指定されたデプロイ パッケージを修正します。

```
policydeploy -fix -task 1266471565#0f6a3cec-a37d-47d9-bde3-0112a49b714a
```

DH または障害回復 DMS が再サブスクライブに失敗する

症状:

障害回復プロセスの一部として、DH を DMS に再サブスクライブするか、または障害回復 DMS を本稼働 DMS に再サブクライブしています。以下のメッセージが表示されます。

サブスクライバ (*dms@host* 上) の再サブスクライブに失敗しました。
リストア操作を完了するには、*subscriber@host* (*dms@host* 上) の再サブスクライブをオフセット*値*で手動で実行してください。

解決方法:

このメッセージは、DH または障害復旧 DMS を実行中ではない親 DMS に再サブスクライブするときに表示されます。 メッセージ中のオフセット値を使用して、手動で DH を DMS に再サブスクライブするか、障害回復 DMS を実行中の DMS に再サブスクライブする必要があります。 オフセット値を指定すると、サブスクライバには、復元時にそのデータベースに存在しなかったコマンドだけが送られます。

親 DMS に DH または障害回復 DMS を再サブスクライブするには、親 DMS ホストで以下のコマンドを実行します :

```
sepmd -s parent_name child_name@host offset
```

例: DMS への DH のサブスクライブ

以下の例では、オフセット値 18028 で DMS__ に DH__@test.com をサブスクライブします。 以下のコマンドを DMS__ で実行します。

```
sepmd –s DMS__ DH__@test.com 18028
```

ポリシー ステータスが「実行されていません」になる

症状:

ポリシー検証を有効にしています。 ポリシーをデプロイするときに、そのポリシーがデプロイされず、ポリシー ステータスは「実行されていません」になります。

解決方法:

ポリシー検証によって 1 つ以上のエラーがポリシーに見つかりました。ポリシーを正常にデプロイできるようにするには、これらのエラーを修正する必要があります。

ポリシーを正常にデプロイするには、以下の手順に従います。

1. エラーを確認します。

   エラーを修正する前に、それらがポリシーまたは CA Access Control データベースのどちらで発生したかを特定する必要があります。

   a. CA Access Control エンタープライズ管理 で、［ポリシー管理］、［ポリシー］サブタブを順にクリックし、左側のタスク メニューにある［デプロイ］ツリーを展開して、［デプロイ監査］をクリックします。

      ［デプロイ監査］ページが表示されます。

   b. 検索範囲を定義して、［実行］をクリックします。

      定義した検索範囲と一致したデプロイ タスクのリストが表示されます。

   c. デプロイされなかったデプロイ タスクの名前をクリックします。

      デプロイに関する情報（ポリシー中のエラーを含む）が表示されます。

2. （オプション）エラーが CA Access Control データベースにある場合は、以下を実行します。

   a. CA Access Control データベース中のエラーを修正します。

   b. 以下の*いずれか*の操作を実行します。

      - policydeploy ユーティリティを使用してデプロイ タスクを修正します。

        デプロイ タスクを修正するとその失敗ステータスが削除され、その後デプロイが正常に実行されると、そのエンドポイントのポリシーのステータスが「デプロイされました」に変更されます。

      - CA Access Control エンタープライズ管理 または policydeploy ユーティリティを使用してポリシーをもう一度デプロイします。

        ポリシーを再デプロイすると、別のデプロイ タスクが作成されます。 エラーが発生した前のデプロイ タスクのステータスは失敗のままです。デプロイが成功した場合、エンドポイント上のポリシー ステータスは「デプロイされました」です。

3. （オプション）エラーがポリシーにある場合は、以下を実行します。

   a. エラーを含んでいないポリシー バージョンを新しく作成します。

   b. CA Access Control エンタープライズ管理 または policydeploy ユーティリティを使用してポリシーをアップグレードします。

ポリシーのステータスが「デプロイ解除されましたがエラーがあります」になる

症状:

エンドポイントからのポリシーのデプロイを解除した後、ステータスに「デプロイ解除されましたがエラーがあります」と示されています。

解決方法:

「デプロイ解除されましたがエラーがあります」というステータスは、エンドポイントで、ポリシーのデプロイは解除されたが、デプロイ解除スクリプトに含まれている 1 つ以上のルールの実行に失敗したことを示しています。このポリシー ステータスは CA Access Control エンタープライズ管理 で削除できません。

この問題を解決するには、ポリシー バージョンのステータスを手動で削除します。

詳細情報:

ポリシー バージョンのステータスを削除できない (P. 61)

ポリシー バージョンのステータスを削除できない

症状:

ポリシー バージョンがホスト上で有効ではありませんが、ポリシー バージョンのステータスを削除することができません。 このため、ポリシー バージョンを削除できません。

解決方法:

この問題を解決するには、ポリシー ステータスを手動で削除する必要があります。

ポリシー ステータスを手動で削除するには、以下の手順に従います。

1. エンドポイント上でポリシー バージョンのステータスを削除します。
   a. エンドポイントで以下の selang コマンドを実行します。

      ```
      sr HNODE __local__
      ```

   b. 出力の「ポリシー ステータス」セクションにあるポリシーの名前を確認し、その「更新者」ユーザを書きとめます。
   c. エンドポイントで以下の selang コマンドを実行します。

      ```
      er HNODE __local__ policy(name(policyName#policyVersion) status(undeployed)
      updator(userName))
      ```

      policyName#policyVersion

      削除するポリシー バージョンの名前およびバージョン番号を定義します。

      userName

      「更新者」ユーザの名前を定義します。

      エンドポイント上でポリシー バージョンのステータスが削除されます。
2. DMS 上でポリシー バージョンのステータスを削除します。
   a. DMS で以下の selang コマンドを実行します。

      ```
      sr HNODE hnodeName
      ```

      hnodeName

      ポリシー バージョンがデプロイされたホストの名前を定義します。

   b. 出力の「ポリシー ステータス」セクションにあるポリシーの名前を確認し、その「更新者」ユーザを書きとめます。
   c. DMS で以下の selang コマンドを実行します。

      ```
      er HNODE hnodeName policy(name(policyName#policyVersion) status(undeployed)
      updator(userName))
      ```

   DMS 上でポリシー バージョンのステータスが削除されます。

例: エンドポイント上のポリシー バージョンのステータスの削除

以下の例は、エンドポイント上で、mypolicy という名前のポリシーのバージョン 01 のステータスを削除します:

```
AC> sr HNODE __local__
(localhost)
Data for HNODE '__local__'
------------------------------------------------------------
Defaccess         : R
Audit mode        : Failure
Owner             : Domain¥Administrator (USER)
Create time       : 28-Feb-2010 12:34
Update time       : 04-Mar-2010 05:10
Updated by        : +policyfetcher (USER)
Effective UID     : superadmin
Policy Status     :
    mypolicy#01   : Deployed              Updated by: superadmin  On: 04-Mar-2010
05:10
    Deviation     : Unset                  Updated on: N/A

AC> er HNODE __local__ policy(name(mypolicy#01) status(undeployed)
updator(superadmin))
(localhost)
Successfully updated HNODE __local__
```

変数を含むルールがエンドポイント上でデプロイされない

症状:

変数が定義されたルールが含まれているポリシーを作成してエンドポイントにデプロイしましたが、そのルールがエンドポイントで実装されません。

解決方法:

ポリシーのデプロイに関する問題を解決するには、以下の手順に従います。

1. エンドポイントで policyfetcher セクション中の policyfetcher_enabled 設定の値が 1 であることを確認します。

   この値が 1 に設定されている場合、policyfetcher の実行が指定されています。 policyfetcher が実行されていない場合は、エンドポイントにポリシーをデプロイできません。

2. policyfetcher ログでエラーをチェックします。

   注: policyfetcher ログは *ACInstallDir*/Log ディレクトリにあります。ここで *ACInstallDir* は CA Access Control をインストールしたディレクトリです。

3. CA Access Control エンドポイント管理 を使用して、変数がエンドポイントで定義されていることを確認します。

   注: 変数がエンドポイントで定義されていない場合、ポリシー ステータスは 「デプロイの一時停止中」です。

   変数がエンドポイント上で定義されない場合は、変数を定義する selang ルールを含む新規ポリシー バージョンを作成してエンドポイントにデプロイします。

4. 以下が真であることを確認します。

   - ポリシーがエンドポイントに割り当てられている。

     ポリシーがエンドポイントに割り当てられていない場合は、CA Access Control エンタープライズ管理 を使用してポリシーを割り当てます。

   - ポリシーのデプロイ スクリプトにエラーが存在しない。

     ポリシーのデプロイ スクリプトにエラーが含まれている場合は、エラーを修正する新規ポリシー バージョンを作成してエンドポイントにデプロイします。

   - ポリシー ステータスが非同期ではない。

     ポリシー ステータスが非同期の場合、変数値は CA Access Control エンドポイントで変更された可能性があります。 ポリシーを再デプロイして非同期ステータスをクリアします。

5. デプロイ情報を監査して、以下を確認します。

   - エンドポイントが正しくポリシーをコンパイルした。
   - ポリシー用の DEPLOYMENT オブジェクトにデプロイ エラーが存在しない。

   ポリシーが正しくコンパイルしなかったか、DEPLOYMENT オブジェクトにエラーが存在する場合は、エラーを修正してポリシーを再デプロイします。

6. CA Access Control を再起動します。

ビルトイン変数がリフレッシュされない

症状:

CA Access Control エンドポイントのシステム設定を変更しました。しかし、ビルトイン変数の値が新しいシステム設定の値に変わっていません。

解決方法:

この問題を解決するには、以下の手順に従います。

1. エンドポイントで policyfetcher セクション中の policyfetcher_enabled 設定の値が 1 であることを確認します。

   この値が 1 に設定されている場合、policyfetcher の実行が指定されています。 policyfetcher が実行されていない場合、CA Access Control データベース中の更新された変数をチェックできません。

2. 以下の手順に従って、システム設定の変更後に policyfetcher がハートビートを送信したことを確認します。

   a. CA Access Control エンタープライズ管理 で、［ワールド ビュー］をクリックし、ワールド ビュー タスクをクリックします。

      検索画面が表示されます。

   b. 必要に応じて、特定のデータを見つけるための検索条件を定義して、［実行］をクリックします。

      定義した検索条件と合致した結果がカテゴリ別に表示されます。

   c. ［前回のステータス］列の更新時間が、システム設定を変更した時間より後であることを確認します。

      ［前回のステータス］列の更新時間がシステム設定の変更時間より前である場合、policyfetcher はハートビートを送信しておらず、更新された変数値をまだチェックしていません。

      注: endpoint_heartbeat 設定を変更することでハートビートの間隔を変更できます。

3. CA Access Control を再起動してシステム設定が変更されたことを確認します。

DNSDOMAINNAME 変数に値が設定されない

症状:

ビルトイン <!DNSDOMAINNAME> 変数に値が設定されません。

解決方法:

エンドポイントに DNS ドメインが設定されていることを確認します。

Windows エンドポイントに DNS ドメインが設定されていることを確認するには、以下の手順に従います。

1. コマンドプロンプトを開き、以下のコマンドを実行します。

   ```
   ipconfig/all
   ```

2. プライマリ DNS サフィックスが正しい値に設定されていることを確認します。

UNIX エンドポイントに DNS ドメインが設定されていることを確認するには、/etc/resolv.conf ファイルを開いてドメインが適切な値に設定されていることを検証します。

DOMAINNAME 変数に値が設定されない

症状:

ビルトイン <!DOMAINNAME> 変数に値が設定されません。

解決方法:

エンドポイントがドメインに接続されていることを確認します。

Windows エンドポイントがドメインに接続されていることを確認するには、以下の手順に従います。

1. ［マイ コンピュータ］を右クリックして［プロパティ］をクリックし、［コンピュータ名］タブをクリックして［変更］ボタンをクリックします。
2. ［ドメイン］フィールドにドメインが表示されていることを確認します。

UNIX エンドポイントがドメインに接続されていることを確認するには、以下の手順に従います。

1. 以下のコマンドを実行します。

   ```
   ypcats hosts
   ```

2. エンドポイントがドメインに接続されていることを確認します。

HOSTNAME 変数に値が設定されない

症状:

ビルトイン <!HOSTNAME> 変数に値が設定されない、または完全修飾されません。

解決方法:

エンドポイントに完全修飾ホスト名が設定されていることを確認します。

Windows エンドポイントに全修飾ホスト名が設定されていることを確認するには、以下の手順に従います。

1. コマンドプロンプトを開き、以下のコマンドを実行します。

   ```
   ipconfig/all
   ```

2. プライマリ DNS サフィックスが正しい値に設定されていることを確認します。

UNIX エンドポイントがドメインに接続されていることを確認するには、以下のファイルにホスト名が完全修飾名で定義されていることをチェックします。

- /etc/hosts
- /etc/resolv.conf

HOSTIP 変数に値が設定されない

症状:

ビルトイン <!HOSTIP> 変数に値が設定されない、またはエンドポイント用のすべての IP アドレスが設定されません。

解決方法:

IP アドレスがエンドポイントに存在することを確認します。

IP アドレスが Windows エンドポイント上に存在することを確認するには、以下の手順に従います。

1. コマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ipconfig/all
   ```

2. IP アドレス（1 つまたは複数）が正しいことを確認します。

IP アドレスが UNIX エンドポイント上に存在することを確認するには、以下の手順に従います。

1. 以下のコマンドを実行します。

   ```
   ifconfig -a
   ```

2. IP アドレス（1 つまたは複数）が正しいことを確認します。

オペレーティング システム変数に値が設定されない

症状:

CA Access Control オペレーティング システム変数を定義してエンドポイントの場所を指定しました。 このオペレーティング システム変数をポリシーのルールの中で使用した場合、この変数に値が設定されないため、CA Access Control はルールを実行しません。

解決方法:

環境変数がエンドポイント上のオペレーティング システムに存在することを確認します。

環境変数がオペレーティング システムに存在することを検証する方法

1. CA Access Control 変数がオペレーティング システム変数（OSVAR タイプ）として定義されていることを確認します。
2. オペレーティング システム変数がオペレーティング システムに存在することを以下の手順に従って確認します。
   - （Windows）コマンド プロンプトを開き、以下のコマンドを実行します。

     set
   - （UNIX）コマンド プロンプトを開き、以下のコマンドを実行します。

     env

     注: このコマンドを実行するには root ユーザである必要があります。

レジストリ変数に値が設定されない

Windows で該当

症状:

CA Access Control レジストリ変数を定義してエンドポイントの場所を指定しました。 このレジストリ変数をポリシーのルールの中で使用した場合、この変数に値が設定されないため、CA Access Control はルールを実行しません。

解決方法:

レジストリ変数（REGVAL タイプ変数）は REG_SZ または REG_EXPAND_SZ のレジストリ タイプを指している必要があります。 レジストリ変数中に指定されているレジストリ値が REG_SZ または REG_EXPAND_SZ タイプであることを確認します。

第 8 章: 監査レコードの収集

このセクションには、以下のトピックが含まれています。

一部の監査ログ メッセージを収集サーバが受信しない

UNIX で該当

症状:

CA Access Control にエンドポイントを設定して、それらのローカル監査ログをセントラル ログ収集サーバにルーティングしていますが、サーバが一部の監査ログを受信しません。 selogrd は監査レコードを送出するように設定し、selogrcd は監査レコードを収集するように設定してあります。

解決方法:

selorgd （CA Access Control ログ ルーティング システム用の送出デーモン）をトラブルシューティングするには、以下の手順に従います。

- selogrd.cfg ファイルを確認します。 このファイルには、CA Access Control がセントラル ログ コレクタにルーティングする監査メッセージが指定されています。

- 各エンドポイントの監査ログを確認します。監査ログに監査イベントが見当たらない場合は、audit.cfg ファイルを確認します。audit.cfg ファイルには、CA Access Control が監査ログに書き込む監査イベントが設定されています。audit.cfg ファイルによって、CA Access Control がある監査イベントを監査ログに書き込むことが禁止されている場合、その監査イベントはルーティングできません。
- selogrd （ログ ルーティング システム用の送出デーモン）を設定してデバッグ メッセージを出力し、問題を再現します。デバッグ メッセージを出力するように selogrd を設定するには、以下のコマンドを使用します。

  ```
  selogrd -d
  ```

監査ログ メッセージを収集サーバが受信しない

UNIX で該当

症状:

CA Access Control にエンドポイントを設定して、それらのローカル監査ログをセントラル ログ収集サーバにルーティングしていますが、サーバが監査ログをまったく受信しません。 selogrd は監査レコードを送出するように設定し、selogrcd は監査レコードを収集するように設定してあります。

解決方法:

selogrcd がログ収集サーバ上で実行中であることを確認します。

注: selogrcd が長期間にわたって実行されない場合、監査イベントがエンドポイントによって破棄されることがあります。

SID の解決に失敗する（イベント ビューア警告）

Windows で該当

症状:

Windows イベント ビューアのアプリケーション ログを表示すると、特定の SID のアカウント名への解決に失敗しましたという、CA Access Control からの警告メッセージが見つかります。

解決方法:

セキュリティ識別子 (SID) とは、オペレーティング システムに対してユーザまたはグループを識別する数値です。 システム アクセス制御リスト（DACL）の各エントリは SID を持っていて、これによって、アクセスを許可、拒否、または監査するユーザまたはグループを識別します。

この警告は、オペレーティング システムが SID をアカウント名に変換できなかったとき（SID が指し示すユーザまたはグループが存在しなくなった場合など）に表示されます。 問題のシステムおよび対応するドメイン コントローラが、SID 解決を正常に行えるように設定されていることを確認してください。

SID 解決タイムアウト（イベント ビューア警告）

Windows で該当

症状:

イベント ビューアのアプリケーション ログを表示すると、特定の SID のアカウント名への解決がタイムアウトしましたという、CA Access Control からの警告メッセージが見つかります。

解決方法:

セキュリティ識別子 (SID) とは、オペレーティング システムに対してユーザまたはグループを識別する数値です。 システム アクセス制御リスト（DACL）の各エントリは SID を持っていて、これによって、アクセスを許可、拒否、または監査するユーザまたはグループを識別します。

この警告メッセージは、あらかじめ定義されたタイムアウト時間内に、オペレーティング システムが SID をアカウント名に変換できなかった場合に表示されます。 以下を確認してください。

- 問題のシステムおよび対応するドメイン コントローラが、SID 解決を正常に行えるように設定されている
- ネットワーク設定が正常に設定されている

さらに、以下のレジストリ キー中の DefLookupTimeout 環境設定の変更により、タイムアウトを増加させることができます。

```
HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥SeOSD
```

注: SID 解決のタイムアウトを延長すると、CA Access Control のパフォーマンスが低下する可能性があります。

selogrd を起動しようとするとエラー コード 4631 が表示される

UNIX で該当

症状:

selogrd を起動しようとしました。 しかし selogrd は起動せず、以下のエラー メッセージが表示されます。

エラー 4631 (0x1217) が /opt/CA/AccessControl/bin/selogrd の初期化中に発生しました。

解決方法:

selogrd を起動する前にローカル ホスト名を解決します。 ホスト名を解決するには、ホスト名をオペレーティング システム hosts ファイルに追加するか、NIS または DNS に対してホスト名を定義します。

監査ファイル サイズが 2GB を超えると監査ログが停止する

症状:

監査ファイル サイズが 2GB を超えると、CA Access Control は監査レコードの監査ファイルへの書き込みを停止します。

解決方法:

監査ファイルのサイズが 2GB を超えた場合、CA Access Control は監査レコードを監査ファイルに書き込むことができません。 CA Access Control 監査ファイルの最大サイズは、logmgr セクションの audit_size 設定によって KB 単位で指定されています。

seos.audit ファイルの最大サイズを 2GB に設定するには、logmgr セクションの audit_size 設定の値を 2097151 に設定します。

CA Access Control が監査ログに書き込むときにシステムが遅くなる

症状:

CA Access Control が監査ログに書き込むときにコンピュータが遅くなります。

解決方法:

CA Access Control が監査およびトレース データを書き込む間、システム内のほとんどのプロセスがブロックされる可能性があります。 CA Access Control が監査データおよびトレース データを書き込む時間を短縮するには、以下を実行します。

- 必要なリソースおよびアクセスのみに監査モードを設定します。
- 必要な場合にのみ、トレースを開きます。
- 処理速度が最も速いファイル システムに、監査ファイル、トレース ファイル、CA Access Control データベース ファイルを格納します。

ホストに複数の IP アドレスが割り当てられている場合にフィルタが適用されない

症状:

ホスト名を使用して、複数の IP アドレスが割り当てられたホスト上の TCP イベントをフィルタするために、audit.cfg を設定しました。フィルタ適用後、すべての IP アドレスの TCP ログを参照できません。

解決方法

audit.cfg フィルタを適用すると、監査システムはホスト名をホストの IP アドレスに、ホストの IP アドレスをホスト名に解決します。 複数の IP アドレスでホストを設定すると、audit.cfg は最初の IP アドレスのみをフィルタします。

audit.cfg フィルタをすべての IP アドレスに 適用するには、フィルタに、ホスト名ではなく、すべての IP アドレスのみを指定します。以下に例を示します。

```
TCP;*;192.168.30.138;*;R;P
TCP;*;192.168.30.139;*R;P
```

第 9 章: パフォーマンスの調整

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 Access Control の実行時にパフォーマンスが低下する

症状:

CA Access Control の実行中にコンピュータが遅くなります。 CA Access Control を停止すると、パフォーマンスは通常通りに戻ります。

解決方法:

性能の問題を診断するおよび修正するには、性能に関する問題のトラブルシューティングを行います (P. 133)。

CA Access Control サーバ上のシステム負荷が高すぎる

症状:

CA Access Control サーバのシステム負荷を軽減する必要があります。

解決方法:

システム負荷を軽減するには、以下を行います。

- データベースの階層を深くしないようにします。

  ユーザおよびリソースの階層が深い場合、すべての依存関係を取得およびチェックするにはシステム負荷がかかります。

- 頻繁に使用されるディレクトリに対して一般的なルールの適用を避けます。

  頻繁に使用されるディレクトリに対して一般的なルールを定義した場合、CA Access Control は数多くのシステム アクションをチェックすることになります。 たとえば、/usr/lib/* を保護する一般的な保護ルールを記述した場合、CA Access Control はシステムのすべてのアクションをチェックします。

- （Solaris のみ）プロセス ファイル システム（/proc）に属するファイルに対するアクセス チェックを CA Access Control が省略するように指定します。

  プロセス ファイル システムに属するファイルに対するアクセス チェックを CA Access Control が省略するように指定するには、seos.ini ファイルの［SEOS_syscall］セクションの proc_bypass 設定値が 1 であることを確認します。

  注: seos.ini ファイルのトークンの詳細については、「リファレンス ガイド」を参照してください。

第 10 章: UNAB の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。

UNAB のインストールに失敗する

症状:

インストール パッケージをカスタマイズしましたが、UNAB をエンドポイントへインストールしようとした時に、インストールに失敗しました。

解決方法:

この問題を解決するには、以下の手順に従います。

1. エラーがないか UNAB インストール ログ ファイル、uxauth_install.log を確認します。 デフォルトでは、ファイルは以下のディレクトリにあります。

   ```
   /opt/CA/uxauth
   ```

2. UNAB インストール ログ ファイルをエクスポートし、エクスポートしたファイルを CA サポートに送信します。
3. デバッグ モードでインストール処理を実行します。
   - ネイティブ パッケージのインストールについては、seos_debug_on という名前のファイルを /tmp ディレクトリに作成し、0 から 9 の範囲でファイルにデバッグ レベルを割り当てます。
4. デバッグ モードでネイティブ パッケージを実行します。
   - AIX — -e<*log_file_name*> フラグをインストール コマンドに追加します
   - HP-UX — swinstall が swjob 用に生成するインストール ログ ファイルを確認します
   - Linux — -vv フラグをインストール コマンドに追加します
   - Solaris — -v フラグをインストール コマンドに追加します

UNAB 登録のトラブルシューティング

以下のセクションには、Active Directory への UNAB 登録時に発生する問題をトラブルシューティングするために役立つ情報が含まれています。

不正なパスワードが原因で UNAB 登録が失敗する

症状:

Active Directory に UNAB を登録しようとすると、以下の内容のエラー メッセージで登録が失敗します。

初期クレデンシャルの取得中に事前認証に失敗しました/<Administrator> を使用した Kerberos 事前認証が失敗しました。

解決方法:

不正なパスワードが原因で UNAB 登録が失敗しました。 この問題を解決するには、管理者のパスワードを確認し、UNAB を登録します。

正しくないクロック スキューが原因で UNAB 登録が失敗する

症状:

Active Directory に UNAB を登録しようとすると、以下の内容のエラー メッセージが表示されます。

クロック スキューが大きすぎます/<Administrator> を使用した Kerberos 事前認証が失敗しました。

解決方法:

Active Directory と UNAB エンドポイント間のクロック スキューが設定された値より大きいため、UNAB 登録に失敗しました。

この問題を解決するには、以下の手順に従います。

1. UNAB エンドポイント クロックを Active Directory のクロックと手動で同期します。
2. uxauth.ini の [Agent] セクションで、use_time_sync トークンの値を yes に設定し、時間の同期を自動設定します。

正しくない NTP サーバ設定が原因で UNAB 登録が失敗する

症状:

Active Directory に UNAB を登録しようとすると、以下の内容のエラー メッセージが表示されます。

警告： NTP サービスの場所が間違って指定されています。

解決方法:

Network Time Protocol（NTP）サーバが間違って設定されているため、UNAB 登録に失敗しました。

この問題を解決するには、uxauth.ini の [Agent] セクションで ntp_server トークンが NTP サーバを指すように設定します。

無効な設定が原因で UNAB 登録が失敗する

症状:

Active Directory に UNAB を登録しようとすると、以下の内容のエラー メッセージが表示されます。

Kerberos 5 ライブラリの初期化エラー。'/opt/CA/uxauth/uxauth.ini' を確認してください。
<Administrator> を使用した Kerberos 事前認証が失敗しました。

症状:

uxauth.ini ファイルに無効な Kerberos 値が含まれているため、UNAB 登録に失敗しました。

この問題を解決するには、uxpreinstall ユーティリティを実行して Kerberos 設定を確認します。

DNS 設定がないため UNAB 登録が失敗する

症状:

Active Directory に UNAB を登録しようとすると、以下の内容のエラー メッセージが表示されます。

<domain_name> ドメインに LDAP サービスのリソース レコードが見つかりません。

解決方法:

DNS 設定が Active Directory に設定されていないため、UNAB 登録に失敗しました。

この問題を解決するには、以下の手順に従います。

1. uxpreinstall ユーティリティを実行し、DNS 設定を確認します。
2. uxpreinstall ユーティリティの出力を参照し、DNS 設定を確認します。
3. 設定が正しくない場合は、以下のファイルの DNS 設定を更新します。

   /etc/resolv.conf

uxconsole -register が失敗する

UNIX で該当

症状:

UNAB エンドポイントを登録するために uxconsole -register を実行すると、以下の内容のエラー メッセージが表示されます。

```
Active Directory と通信するための DC として使用できるサーバがありません。
[ad] セクションで lookup_dc_list と ignore_dc_list のトークンを確認してください。
```

解決方法:

uxconsole が Active Directory に UNAB エンドポイントを登録する際、エンドポイントの物理的な場所に最も近い Active Directory サイトが検出されます。 しかし、uxauth.ini ファイルの ad セクションの ignore_dc_list 設定は、UNAB エンドポイントが通信しないドメイン コントローラのリストを示します。 検出された Active Directory サイト内のすべてのドメイン コントローラが ignore_dc_list 設定のリストに含まれている場合、登録は失敗します。

この問題を解決するには、検出された Active Directory サイトのドメイン コントローラの名前を ignore_dc_list 設定から削除し、uxconsole ユーティリティを再実行します。

注: uxconsole ユーティリティは、検出された Active Directory サイトの名前を uxauth.ini ファイル内の ad セクションの ad_site 設定に書き込みます。 UNAB の Active Directory サイト サポートの詳細については、「*実装ガイド*」を参照してください。

UNAB のログイン ポリシーが配布されない

症状:

UNAB のログイン ポリシーを UNAB のエンドポイントに配布しようとしましたが、ポリシーが配布されません。

解決方法:

この問題を解決するには、以下の手順に従います。

1. UNAB がエンドポイントで起動していることを確認します。
   a. エンドポイントでコマンド プロンプト ウィンドウを開きます。
   b. 以下のコマンドを実行します。

      ```
      ./uxauthd.sh status
      ```

   UNAB の現在のステータスを示すメッセージが表示されます。
2. ポリシーがホストにダウンロードされたことを確認します。
   a. エンドポイント上でコマンド プロンプト ウィンドウから、以下のコマンドを実行します。

      ```
      ./uxconsole -status -detail
      ```

   エンドポイントに展開する場合、この情報にポリシー名を含めます。
3. エンタープライズ管理サーバが UNAB エンドポイントに送信したポリシー許可コマンドを確認します。
   - エンドポイント上でコマンド プロンプト ウィンドウから、以下のコマンドを実行します。

     ```
     ./uxaudit -a
     18 Jan 2011 11:03:23 S UPDATE□□□□□□ TERMINAL□□ ac_entm_pers□ 338 10
     _default□□□□□□□□□□□□ acmanager.forwardinc.com auth terminal _default
     xuid(yaeyu01)access(read) (OS user)
     ```

   ルールが変更されていないことを確認します。
4. メッセージ キュー通信エラーがないかどうか syslog ファイルを検索します。
5. ユーザ アカウントのログイン許可およびステータスを確認します。
6. コマンド プロンプト ウィンドウから以下のコマンドを実行します。

   ```
   uxconsole –manage –show –user <AD_user_account>
   ```

ReportAgent がエンタープライズ管理サーバへのレポートの送信に失敗する

症状:

UNAB を起動し、ReportAgent デーモンは実行されているが、CA Access Control エンタープライズ管理 でレポートを表示できないことを確認しました。

解決方法:

この問題を解決するには、以下のプロシージャを使用します。

1. syslog の「UNAB EP communication problems with ENTM （ENTM との UNAB EP 通信の問題）」セクションで、メッセージ キュー サーバ通信に関連するエラー メッセージがないかどうか確認します。
2. レポート データを CA Enterprise Log Manager に送信する場合は、accommon.ini ファイルの［ReportAgent］セクションにある audit_enabled トークンが 1 に設定されていることを確認します。
3. ReportAgent のデバッグを有効にします。
4. accommon.ini ファイルの［ReportAgent］セクションにあるデバッグ トークンを 1 に設定します。
5. UNAB レポートのデバッグ ファイル、unab2xml.log を確認します。 このファイルは以下のディレクトリにあります。

   ```
   /opt/CA/AccessControlShared/log
   ```

6. ReportAgent を手動で実行して、UNAB データベース スナップショットを生成します。

   ```
   /opt/CA/AccessControlShared/bin/ReportAgent -debug 0 -task 2 –now
   ```

   以下の点に注意してください。

   - ReportAgent を手動で実行する前に、パス '/opt/CA/AccessControlShared/lob' を $LD_LIBRARY_PATH に追加します。
   - ReportAgent を手動で実行する前に、/opt/CA/AccessControlShared/data/audit2txt/ ディレクトリから .dat ファイルを削除します。
   - ReportAgent ユーティリティのデバッグ モードの詳細については、「リファレンス ガイド」を参照してください。

UNAB ホストの登録時に Kerberos Preauthentication に失敗する

UNIX で該当

症状:

uxconsole -register コマンドを使用すると、以下の内容のエラー メッセージが表示されます。

krb5_set_config_files が /opt/CA/uxauth/uxauth.ini で失敗しました。プロファイルに左中かっこがありません。
<Administrator> を使用した Kerberos preauthentication に失敗しました。

解決方法:

uxauth.ini ファイルに設定されていない項目があります。 この問題を解決するには、uxauth.ini ファイル内の環境設定すべてに値が存在することを確認します。

UNAB の登録または開始でエラー コード 2803 を受信する

UNIX で該当

症状:

Active Directory で UNAB ホストを登録、または UNAB を開始しようとすると、以下の内容のエラー メッセージが表示されます。

nss を開けないか、nss キャッシュを作成できません。 エラー コード 2803

解決方法:

/var ディレクトリに十分なメモリがありません。この問題を解決するには、/var の使用率が 95% に達していないことを確認し、コマンドを再試行します。

Active Directory ユーザが UNAB エンドポイントにログインできない

UNIX で該当

症状:

UNIX 属性を持つ Active Directory ユーザが UNAB エンドポイントにログインできません。

解決方法:

この問題を解決するには、以下の手順に従います。

1. ユーザのコンテナが以下のいずれかであることを確認します。
   - user_container 環境設定に指定されているコンテナ。
   - user_container 環境設定に指定されているコンテナの下にあるサブコンテナ。

     注: user_container 環境設定は、uxauth.ini ファイルの AD セクションにあります。
2. Active Directory 内で、ユーザに UID および GID があることを確認します。
3. ユーザが保留されていないことを確認します。
4. UNAB がエンドポイントで起動していることを確認します。
   a. エンドポイントでコマンド プロンプト ウィンドウを開きます。
   b. 以下のコマンドを実行します。

      ```
      ./uxauthd.sh status
      ```

      UNAB の現在のステータスを示すメッセージが表示されます。
5. エンドポイントが Active Directory に登録されていることを確認します。

   注: エンドポイントが Active Directory に登録されていない場合、uxconsole -register ユーティリティを使用してホストを登録してください。

6. エンドポイント上の OS 用の名前またはパスワード キャッシュ デーモンを以下の手順に従って停止します。

   a. UNAB を停止します。

      ```
      ./uxauthd.sh stop
      ```

   b. NSS キャッシュ データベースを削除します。

      ```
      rm -rf /opt/CA/uxauth/etc/nss.db
      ```

   c. OS 用の名前またはパスワード キャッシュ デーモンがエンドポイント上で実行中かどうかを確認します。

      たとえば、Linux または Solaris エンドポイントの場合は nscd デーモンが実行中かどうかを確認します。 HP-UX エンドポイントの場合は、pwgrd デーモンが実行中かどうかを確認します。

   d. OS 用の名前またはパスワード キャッシュ デーモンが実行中の場合は、プロセスを強制終了します。

   e. UNAB を起動します。

      ```
      ./uxauthd.sh start
      ```

7. 別の Active Directory ユーザ アカウントを使用して、Ticket Granting Ticket （TGT）を取得します。

   管理者アカウントを使用して、Active Directory に接続するための以下のコマンドを実行します。

   ```
   ./uxconsole -krb -init Administrator
   ```

   注: TGT は、たとえば以下のように、エージェント keytab を使用して取得できます。

   ```
   ./uxconsole -krb -init -k
   ```

8. Active Directory ユーザ アカウントを直接解決します。

   - 以下の検索を実行します。

     ```
     ./uxconsole -ldap -search "(&(objectClass=user)(sAMAccountName=johndoe))"
     ```

     期待される結果と、実際のユーザ アカウント名の不一致をチェックします。

9. 必要に応じて、他のドメインでユーザ アカウントを検索します。

   - 以下のコマンドを実行します。

     ```
     ./uxconsole -ldap -search -b DC=unabca,DC=test,DC=co,DC=il
     "(&(objectClass=user)(objectCategory=person))"
     ```

10. ユーザ アカウント UNIX 属性が Active Directory と UNIX 上で同一であることを確認します。

UNAB エンドポイントでコマンドを実行できない

症状:

UNAB エンドポイントに正常にログインでき、UNAB では、このログインに対応して uxaudit（UNAB 監査ファイル）に P（permitted）レコードが作成されました。 それにも関わらず、エンドポイントで UNIX コマンドを実行できません。

解決方法:

ユーザが同じエンドポイントに同じユーザ名で以前にログインしたときに、違う UID を使用していた場合、そのユーザは自分の /home ディレクトリにアクセスすることができません。

この問題を解決するには、以下の手順に従います。

1. ユーザの /home ディレクトリを削除します。

   注: /home ディレクトリは、/home/userName に位置している場合があります。

2. ユーザがエンドポイントにログインします。

   新しい /home ディレクトリが作成されます。 これで、UNAB エンドポイント上で UNIX コマンドを実行できるようになりました。

ワールド ビューで UNAB エンドポイントを表示できない

UNIX で該当

症状:

UNAB エンドポイントを管理するために CA Access Control エンタープライズ管理 を使用していますが、ワールド ビューに UNAB エンドポイントが表示されません。

解決方法:

UNAB エンドポイントが配布サーバと通信できることを確認します。
UNAB エンドポイント上で以下を実行します。

1. Distribution_Server 設定の値が配布サーバ コンピュータの名前に設定されていることを確認します。

   Distribution_Server 設定は、accommon.ini ファイルの communication セクションにあります。

   例： ssl://ds.comp.com:7243

   注: 配布サーバはデフォルトではエンタープライズ管理サーバ上にインストールされています。

2. メッセージ キューのパスワードが正しいことを確認します。エンドポイントでは、このパスワードを使用して配布サーバと通信します。 以下の手順を実行します。

   a. コマンド プロンプト ウィンドウを開きます。

   b. 以下のコマンドを実行します。

      ```
      acuxchkey -t pwd "password"
      ```

      password

      メッセージ キューのパスワードを定義します。 デフォルトでは、このパスワードは、CA Access Control エンタープライズ管理 をインストールするときに指定した通信用パスワードです。

3. UNAB エージェントを以下の手順で再起動します。

   a. UNAB lbin ディレクトリに移動します。

      デフォルトでは、このディレクトリは /opt/CA/uxauth の下にあります。

   b. UNAB エージェントを再起動します。

      ```
      ./uxauthd.sh restart
      ```

4. メッセージ キュー サーバが実行されていることを以下の手順で確認します。

   - Windows -- CA Access Control メッセージ キュー サービスが実行されていることを確認します。
   - UNIX -- tibemsd プロセスが実行されていることを確認します。

5. メッセージ キュー サーバの通信エラーがないかどうかを syslog またはイベント ビューアで確認します。

6. メッセージ キュー サーバの通信関連メッセージがログ ファイルに記録されるように設定します。 以下の手順を実行します。
   - UNIX の場合
     a. pmd.ini を開きます。
     b. [endpoint_management] セクションの debug_mode トークンを 1 に設定します。
   - Windows の場合
   a. 以下のレジストリ キーに移動します。

      HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd¥ DMS_NAME¥endpoint_management

   b. debug_mode トークン値を 1 に変更します。
7. エンタープライズ管理サーバを再起動して変更を反映させます。 DMS ディレクトリ内の endpoint_management.log ファイルを参照して通信メッセージがないかどうかを確認します。

   UNAB エンドポイントが配布サーバと通信できることが確認されました。

Linux s390 エンドポイント上でデーモンを開始できない

Linux s390 および Linux s390x で有効

症状:

uxauthd や ReportAgent デーモンを開始できません。

解決方法:

UNAB でエンドポイント上の Java 環境を特定できません。この問題を解決するには、以下の手順に従います。

1. accommon.ini ファイル内の global セクションの java_home 設定に、Java 環境へのパスが含まれていることを確認します。
2. LD_LIBRARY_PATH 環境変数の値を、Java 環境の共有ライブラリへのパスに設定します。

ユーザによるログインまたはパスワードの変更ができない

UNIX で該当

症状:

UNAB エンドポイント上でログインやパスワードの変更を試みると、以下のエラー メッセージが表示されます。

```
passwd: 認証トークン操作エラー
```

解決方法:

PAM モジュールは、uxauthd によるパスワードの変更要求への応答待機中にタイムアウトになりました。

この問題を解決するには、以下の手順に従います。

1. uxauth.ini ファイルの pam セクション内の pam_receive_timeout 設定セット値を増加させます。

   たとえば、pam_receive_timeout=100

2. UNAB を停止および再起動します。

注: uxauth.ini ファイルの詳細については、「*リファレンス ガイド*」を参照してください。

第 11 章: PUPM の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。

Break Glass 承認ワークフロー

症状:

シングル ステップの Break Glass ワークフローを設定することにより、ユーザのマネージャではなく、要求が適用される PUPM エンドポイント システム管理者に通知されるようにする必要があります。

解決方法:

シングル ステップの Break Glass ワークフローを設定し、Break Glass 要求がデフォルトの承認者ではなく、システム管理者によって承認されるように指定することができます。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、［ユーザおよびグループ］-［タスク］-［管理タスクの変更］を選択します。

   管理タスクの変更 - 管理タスクの検索ウィンドウが表示されます。

2. プルダウン メニューから［カテゴリ］を選択し、テキスト ボックス領域に「*home*」と入力します。 ［検索］をクリックします。

   CA Access Control エンタープライズ管理 は、検索条件に一致するタスクを表示します。

3. Break Glass タスクを選択し、［選択］をクリックします。

   Break Glass プロパティ ウィンドウが表示されます。

4. ［イベント］タブに移動し、右向き矢印をクリックします。

   ワークフロー マッピング ウィンドウが表示されます。

5. ［ワークフロー プロセス］プルダウン メニューから SingleStepApproval を選択します。

6. ［プライマリ承認者］セクションで以下の手順に従います。

   a. ［承認タスク］プルダウン メニューから［Break Glass 特権アカウントを承認］を選択します。

   b. ［参加者リゾルバ］プルダウン メニューから［カスタム：PrivilegedAccountOwnerResolver］を選択します。

      参加者リゾルバ設定パラメータが設定されていないことを通知するメッセージが表示されます。

   c. ［新規のパラメータ名］テキスト ボックスに「SourceObject」を指定します。

d. ［値］テキスト ボックスに「TaskAdmin」を指定します。

e. ［パラメータの追加］をクリックします。

CA Access Control エンタープライズ管理 は承認者タスクを追加します。

f. 以下のパラメータ名および値を使用して、手順 c から e までを繰り返します。

- SourceObjectAttribute -- tblUser.manager
- TargetType -- USER

7. ［OK］をクリックします。

シングル ステップの Break Glass ワークフローが設定され、システム管理者が承認者として定義されました。

RunAs パスワード コンシューマ要求がタイムアウトする

Windows で該当

症状:

あるユーザが RunAs ユーティリティを使用してタスクを実行できるように Windows RunAs パスワード コンシューマを設定しています。 このユーザが RunAs ユーティリティを実行すると、パスワード要求がタイムアウトになり、ユーティリティを実行できません。

解決方法:

この問題を解決するには、以下のレジストリ エントリの値を増やします。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥Plugins¥RunAsPlg¥CommunicationWaitTimeout

このレジストリ エントリは、パスワード コンシューマが PUPM エージェントからの応答を待つ時間を秒単位で指定します。

例: CommunicationWaitTimeout レジストリ エントリの値を変更する

以下の例は、CommunicationWaitTimeout レジストリ エントリの値を 30 に増やします。

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation¥PlugIns¥RunAsPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
正常に、トークンを設定しました。
```

ODBC、OLEDB、または OCI データベース パスワード コンシューマ要求のタイムアウト

Windows で該当

症状:

ODBC、OLEDB、または OCI データベース パスワード コンシューマをエンドポイント上で設定しています。 エンドポイント上のアプリケーションがデータベースに接続するとき、パスワード コンシューマはパスワードを要求します。 しかし、アプリケーションがデータベースに接続しようとするとき、パスワード要求はタイムアウトになります。

解決方法:

この問題を解決するには、以下のレジストリ エントリの値を増やします。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥Plugins¥plugin¥CommunicationWaitTimeout
```

プラグイン

接続の試行をインターセプトするプラグインの名前を指定します。

値： OCIPlg、ODBCPlg、OLEDBPlg

このレジストリ エントリは、パスワード コンシューマが PUPM エージェントからの応答を待つ時間を秒単位で指定します。

例: CommunicationWaitTimeout レジストリ エントリの値を変更する

以下の例は、OCI データベース パスワード コンシューマに合わせて、CommunicationWaitTimeout レジストリ エントリの値を 30 に増やします。

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation¥PlugIns¥OCIPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
正常に、トークンを設定しました。
```

PUPM SSH デバイスがタイムアウトする

Red Hat 5 で該当

症状:

日本語版 Red Hat 5 を PUPM SSH デバイス エンドポイントとして設定し、運用管理者のユーザ ログインおよび運用管理者のパスワードを使用するように指定した後に、エンドポイントの作成タスクがタイムアウトします。

解決方法

この問題を解決するには、以下の手順に従います。

1. 以下のディレクトリに移動します。ここで *ACServerInstallDir* は、エンタープライズ管理サーバをインストールしたディレクトリです。

   ACServerInstallDir/Connector Server/conf/override/sshdyn

2. ssh_connector_conf.xml ファイルを開いて、編集します。
3. <array name="oChangePassword"> の下に以下の項目を追加します。

   ```
   <item>
       <param name="sCommand" value="set LANG=C" />
       <param name="iWait" value="500" />
       </item>
   ```

4. ファイルを保存して閉じます。

承認ワークフローがトリガされることなく要求されたパスワードがチェックアウトで利用可能になる

SunOne で該当

症状:

特権アカウント パスワード リクエストの入力後、まずマネージャがそのリクエストを承認することなく、パスワードがチェックアウトで利用可能になります。

解決方法:

デフォルトでは、エンタープライズ管理サーバを SunOne ユーザ ディレクトリと共にインストールすると、ワークフロー サポートが無効になります。 ユーザが特権アカウント パスワードのリクエストをサブミットするには、ワークフロー サポートを有効にする必要があります。

SunOne ディレクトリのワークフロー サポートを有効にするには、以下の手順に従います。

1. これまでそうしなかった場合は、Identity Manager 管理コンソールを有効にします。
2. Identity Manager 管理コンソールを開きます。
3. ［環境］-［ac-env］-［詳細設定］-［ワークフロー］を選択します。

   ［ワークフロー プロパティ］ウィンドウが表示されます。
4. ［有効］フィールドの横のチェック ボックスを選択します。
5. ［保存］を選択してから［再起動］を選択して、環境を再起動します。

   これで、SunOne ディレクトリのワークフロー サポートを有効にしました。

Windows エージェントレス エンドポイント作成時のアクセス拒否メッセージ

Windows 7 Enterprise Edition で該当

症状:

Windows 7 エンドポイントを Windows エージェントレス エンドポイント タイプとして定義すると、「アクセスが拒否されました」というメッセージが表示され、プロセスが失敗します。

解決方法:

指定したアカウントが管理者アカウントではなく Administrators グループのメンバであるので、エンドポイント作成プロセスは失敗します。

この問題を回避するには、次の操作を行ってください。

1. Administrators グループのメンバとして、管理するエンドポイントにログインします。
2. ［コントロール パネル］-［ユーザー アカウント］-［ユーザ アカウント制御設定の変更］を選択します。

   ［ユーザー アカウント制御の設定］ウィンドウが表示されます。
3. 通知レベルを［デフォルト］に設定し、次に、［OK］をクリックします。

   変更が有効になるには、コンピュータの再起動が必要になる場合があります。
4. ［管理ツール］-［コンピュータの管理］-［サービスとアプリケーション］を選択します。
5. ［WMI コントロール］を右クリックしてから、［プロパティ］を選択します。

   WMI コントロールの［プロパティ］ウィンドウが表示されます。
6. ［セキュリティ］タブに移動します。

   ［ネームスペース］ナビゲーション ウィンドウが表示されます。
7. ［ルート］を選択してから、［セキュリティ］を選択します。

   ［セキュリティ］ダイアログ ボックスが表示されます。

8. ［グループ名］または［ユーザ名］セクションから［認証されたユーザー ］を選択します。
9. ［許可］列から、［メソッドの実行］チェック ボックスをオフにします。
10. ［OK］をクリックして、変更を適用します。

第 12 章: レポート サービスの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。

レポート サービスの問題を解決する方法

CA Access Control レポート サービスを使用すると、各エンドポイント（ユーザ、グループ、およびリソース）のセキュリティ ステータスを一括して確認できます。 レポート サービスをトラブルシューティングする場合は、そのコンポーネントを 1 つずつ確認します。

レポート サービスのトラブルシューティングに役立つプロセスを以下に示します。

1. エンドポイントのオペレーティング システムに応じて、以下のいずれかを行います。
   - UNIX コンピュータ上のレポート エージェントのトラブルシューティング (P. 106)
   - Windows コンピュータ上のレポート エージェントのトラブルシューティング (P. 110)
2. 配布サーバをトラブルシューティングします (P. 115)。
3. JBoss をトラブルシューティングします (P. 117)。
4. レポート ポータルをトラブルシューティングします (P. 118)。

UNIX コンピュータ上のレポート エージェントのトラブルシューティング

UNIX で該当

レポート エージェントは、エンドポイント上のローカル CA Access Control データベースおよびすべての Policy Model データベース（PMDB）のスケジュールされたスナップショットを収集し、次にこのスナップショットを配布サーバのレポート キューに XML 形式で送信します。

注: レポート エージェントは他のタスクも実行します。 レポート エージェントの詳細については、「*リファレンス ガイド*」を参照してください。

UNIX コンピュータ上のレポート エージェントをトラブルシューティングする方法

1. ライブラリ パス環境変数が正しく設定されていることを確認します。以下の手順を実行します。
   a. su コマンドで root になります。
   b. *ACSharedDir*/lib にライブラリ パス環境変数を設定します。 デフォルトでは、*ACSharedDir* は以下のディレクトリです。

      ```
      /opt/CA/AccessControlShared
      ```

   c. ライブラリ パス環境変数をエクスポートします。

2. 以下の設定が正しいことを確認します。これらの設定は、accommon.ini ファイルの［ReportAgent］セクションにあります。

   注: CA Access Control エンドポイント管理 または selang コマンドのいずれかを使用して、この設定値を検証できます。 しかし、この手順については、config 環境で selang コマンドを使用して設定を変更する方法をお勧めします。selang コマンドを使用すると、CA Access Control の停止および再起動を行わずに設定値を変更できます。

   reportagent_enabled

   ローカル コンピュータでレポートが有効（1）になっているかどうかを指定します。

   デフォルト： 0

   重要: レポート エージェントの自動実行を有効にするには、この値を 1 に設定する必要があります。 この設定値が 0 である場合、レポート エージェントは配布サーバに対してデータベースのスケジュールされたスナップショットを送信しません。 しかし、この値が 0 である場合は、レポート エージェントをこのままデバッグ モードで実行できます。

   schedule

   レポートが生成されて配布サーバに送信される日時を定義します。

   この設定は、次の形式で指定します。time@day[,day2][...]

   デフォルト： 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   例: 「19:22@Sun,Mon」と指定すると、レポートは毎日曜日と毎月曜日の午後 7:22 に生成されます。

   send_queue

   レポート エージェントがローカル データベースのスナップショットを送信する配布サーバ上のメッセージ キューの名前を定義します。

   デフォルト： queue/snapshots

   重要: この設定のデフォルト値は変更しないでください。

3. 以下の設定が正しいことを確認します。これらの設定は、accommon.ini ファイルの［communication］セクションにあります。

   注: CA Access Control エンドポイント管理 または selang コマンドのいずれかを使用して、この設定値を検証できます。 しかし、この手順については、config 環境で selang コマンドを使用して設定を変更する方法をお勧めします。selang コマンドを使用すると、CA Access Control の停止および再起動を行わずに設定値を変更できます。

   Distribution_Server

   配布サーバの URL を定義します。

   注: TCP 通信用のデフォルト ポートは 7222、SSL 通信用のデフォルト ポートは 7243 です。 配布サーバの URL に通信タイプ用の正しいポート番号が指定されていることを確認する必要があります。

   デフォルト： none

   例： ssl://172.24.176.145:7243 この URL では、レポート エージェントは SSL プロトコルを使用して、IP アドレス 172.24.176.145 の配布サーバと ポート 7243 上で通信します。

4. 以下の行が seos.ini ファイルの［daemons］セクションに存在することを確認します。

   ```
   ReportAgent = yes, ACSharedDir/lbin/report_agent.sh start
   ```

   この行が存在する場合、レポート エージェント デーモンは CA Access Control の起動時に自動的に実行されます。

   注: デフォルトでは、*ACSharedDir* ディレクトリは /opt/CA/AccessControlShared にあります。

5. CA Access Control を停止します。

   ```
   secons -s
   ```

   CA Access Control およびレポート エージェントが停止します。

6. 以下のディレクトリに移動します。

   ```
   ACSharedDir/bin
   ```

7. 以下のコマンドを使用して、レポート エージェントをデバッグ モードで実行します。

   ```
   ./ReportAgent -debug 0 -task 0 -now
   ```

   ReportAgent

   レポート エージェントを実行します。

   -debug 0

   レポート エージェントをデバッグ モードで実行し、出力をコンソールに表示するよう指定します。

   注: レポート エージェント デーモンが有効になっている場合は、レポート エージェントをデバッグ モードで実行できません。

   -task 0

   レポート エージェントによって、CA Access Control データベースおよびすべてのローカル PMDB に関する情報が収集され送信されることを指定します。 この情報は、CA Access Control レポートの生成に使用されます。

   -now

   レポート エージェントを今すぐ実行します。

8. レポート エージェントの出力を以下の手順に従って調べます。
   - 出力にエラーが含まれているかどうかを確認する
   - Send レポート パラメータ セクションの Send Queue および Report File パラメータに正しい名前が指定されていることを確認する
9. CA Access Control を起動します。

   ```
   seload
   ```

   CA Access Control およびレポート エージェントが起動します。

例: レポート エージェントの出力

以下のレポート エージェントの出力では、Send Queue および Report File のパラメータが表示されています。

```
------------------------------------------------------------------------
Send report parameters:
------------------------------------------------------------------------
Send Queue.................. queue/snapshots
Report File..................
/work/opt/CA/AccessControlShared/data/db2xml/ACDB.xml
------------------------------------------------------------------------
start sending report to queue 'queue/snapshots'...
```

Windows コンピュータ上のレポート エージェントのトラブルシューティング

Windows で該当

レポート エージェントは、エンドポイント上のローカル CA Access Control データベースおよびすべての Policy Model データベース（PMDB）のスケジュールされたスナップショットを収集し、次にこのスナップショットを配布サーバのレポート キューに XML 形式で送信します。

注: レポート エージェントは他のタスクも実行します。 レポート エージェントの詳細については、「*リファレンス ガイド*」を参照してください。

Windows コンピュータ上のレポート エージェントをトラブルシューティングする方法

1. 以下の設定が正しいことを確認します。 この設定は、以下のレジストリ キーに存在します。

   HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥ReportAgent

   注: CA Access Control エンドポイント管理 または selang コマンドのいずれかを使用して、この設定値を検証できます。 しかし、この手順については、config 環境で selang コマンドを使用して設定を変更する方法をお勧めします。selang コマンドを使用すると、CA Access Control の停止および再起動を行わずに設定値を変更できます。

   reportagent_enabled

   ローカル コンピュータでレポートが有効（1）になっているかどうかを指定します。

   デフォルト： 0

   重要: レポート エージェントの自動実行を有効にするには、この値を 1 に設定する必要があります。 この設定値が 0 である場合、レポート エージェントは配布サーバに対してデータベースのスケジュールされたスナップショットを送信しません。 しかし、この値が 0 である場合は、レポート エージェントをこのままデバッグ モードで実行できます。

   schedule

   レポートが生成されて配布サーバに送信される日時を定義します。

   この設定は、次の形式で指定します。time@day[,day2][...]

   デフォルト： 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   例: 「19:22@Sun,Mon」と指定すると、レポートは毎日曜日と毎月曜日の午後 7:22 に生成されます。

   send_queue

   レポート エージェントがローカル データベースのスナップショットを送信する配布サーバ上のメッセージ キューの名前を定義します。

   デフォルト： queue/snapshots

   重要: この設定のデフォルト値は変更しないでください。

2. 以下の設定が正しいことを確認します。 この設定は、以下のレジストリ キーに存在します。

   HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Common¥communication

   Distribution_Server

   配布サーバの URL を定義します。

   注: TCP 通信用のデフォルト ポートは 7222、SSL 通信用のデフォルト ポートは 7243 です。 配布サーバの URL に通信タイプ用の正しいポート番号が指定されていることを確認する必要があります。

   デフォルト： none

   例： ssl://172.24.176.145:7243 この URL では、レポート エージェントは SSL プロトコルを使用して、IP アドレス 172.24.176.145 の配布サーバと ポート 7243 上で通信します。

3. CA Access Control レポート エージェント サービスが開始されたことを確認します。

   注: CA Access Control レポート エージェント サービスが自動的に開始するよう設定するには、reportagent_enabled 環境設定を 1 に設定する必要があります。

4. コマンド プロンプト ウィンドウを開き、CA Access Control を停止します。

   ```
   secons -s
   ```

   レポート エージェント サービスを含む CA Access Control が停止します。

5. 以下のコマンドを使用して、レポート エージェントをデバッグ モードで実行します。

   ```
   reportagent -debug 0 -task 0 -now
   ```

   reportagent

   レポート エージェントを実行します。

   -debug 0

   レポート エージェントをデバッグ モードで実行し、出力をコンソールに表示するよう指定します。

   注: レポート エージェント サービスが起動している場合は、レポート エージェントをデバッグ モードで実行できません。

   -task 0

   レポート エージェントによって、CA Access Control データベースおよびすべてのローカル PMDB に関する情報が収集され送信されることを指定します。 この情報は、CA Access Control レポートの生成に使用されます。

   -now

   レポート エージェントを今すぐ実行します。

6. レポート エージェントの出力を以下の手順に従って調べます。
   - 出力にエラーが含まれているかどうかを確認する
   - Send レポート パラメータ セクションの Send Queue および Report File パラメータに正しい名前が指定されていることを確認する

7. CA Access Control を起動します。

   ```
   seosd -start
   ```

   CA Access Control が起動し、レポート エージェント サービスが開始されます。

例: レポート エージェントの出力

以下のレポート エージェントの出力では、Send Queue および Report File のパラメータが表示されています。

```
------------------------------------------------------------------------
Send report parameters:
------------------------------------------------------------------------
Send Queue.................. queue/snapshots
Report File................. C:¥Program
Files¥CA¥AccessControl¥data¥db2xml¥ACDB.xml
------------------------------------------------------------------------
start sending report to queue 'queue/snapshots'...
```

ライブラリ パス環境変数の例

以下の例は、Linux または Solaris コンピュータ上でライブラリ パス環境変数の設定およびエクスポートを実行します。

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/AccessControlShared/lib
export LD_LIBRARY_PATH
```

以下の例は、AIX コンピュータ上でライブラリ パス環境変数の設定およびエクスポートを実行します。

```
export LIBPATH=$LIBPATH:/opt/CA/AccessControlShared/lib
```

以下の例は、HP-UX コンピュータ上でライブラリ パス環境変数の設定およびエクスポートを実行します。

```
export SHLIB_LATH=$SHLIB_PATH:/opt/CA/AccessControlShared/lib
```

配布サーバのトラブルシューティング

配布サーバでは、レポート エージェントがエンドポイントから送信する情報をメッセージ キューが受信します。その後、メッセージドリブン Java Beans（MDB）がメッセージ キュー内のデータを読み取り、中央データベースに書き込みます。

配布サーバをトラブルシューティングする方法

1. （UNIX） Tibco EMS 管理ツールを以下の手順に従って起動します。
   a. 以下のディレクトリに移動します。
      `/opt/CA/AccessControlServer/MessageQueue/tibco/ems/5.1/bin`
   b. 以下のコマンドを実行します。

      ```
      ./tibemsadmin
      ```

2. （UNIX） Tibco EMS 管理ツールを以下の手順に従って起動します。
   a. 以下のディレクトリに移動します。
      `C:¥Program Files¥CA¥AccessControlServer¥MessageQueue¥tibco¥ems¥5.1¥bin`
   b. 以下のコマンドを実行します。

      ```
      tibemsadmin.exe
      ```

3. 以下のいずれかのコマンドを使用して、現在の環境に接続します。
   - 配布サーバがポート 7222 （デフォルト ポート）でレポート エージェントをリスニングする場合は、以下のコマンドを使用します。

     ```
     connect
     ```

   - 配布サーバがポート 7243 でレポート エージェントを SSL モードでリスニングする場合は、以下のコマンドを使用します。

     ```
     connect SSL://7243
     ```

4. ユーザ名およびパスワードを入力します。

   注: デフォルトのユーザ名は admin で、デフォルトのパスワードは CA Access Control エンタープライズ管理 または配布サーバのインストール時に指定した通信用パスワードです。

   配布サーバ上のメッセージ キューに接続します。

5. 以下のコマンドを入力します。

   ```
   show queues
   ```

   配布サーバ上のキューのリストが表示されます。

6. エンドポイントでコマンド プロンプト ウィンドウを開きます。

7. （UNIX）ライブラリ パス環境変数を以下のように設定します。
   a. su コマンドで root になります。
   b. *ACSharedDir*/lib にライブラリ パス環境変数を設定します。 デフォルトでは、*ACSharedDir* は以下のディレクトリです。

      ```
      /opt/CA/AccessControlShared
      ```

   c. ライブラリ パス環境変数をエクスポートします。
8. （UNIX）以下のディレクトリに移動します。

   ```
   ACSharedDir/bin
   ```

9. エンドポイント上でレポート エージェントを実行します。以下のいずれかの操作を実行します。
   - （Windows）以下のコマンドを入力します。

     ```
     ReportAgent -report snapshot
     ```

   - （UNIX）以下のコマンドを入力します。

     ```
     ./ReportAgent -report snapshot
     ```

   レポート エージェントは、CA Access Control データベースのスナップショットおよびローカル PMDB を配布サーバ上のレポート キューに送信します。
10. レポート エージェントの実行中に、tibemsadmin ユーティリティで queue/snapshots というキューを確認します。

    キューが増大する一方で縮小しない場合、JBoss が動作していない可能性があります。 JBoss をトラブルシューティングする必要があります。

JBoss のトラブルシューティング

JBoss Web アプリケーション サーバ環境には、メッセージ駆動型 Java Beans（MDB）が含まれます。これは、メッセージ キューからデータを読み取って中央データベースに書き込みます。 中央データベースにはレポート データが格納されます。

JBoss をトラブルシューティングする方法

1. JBoss が正しく起動することを以下のとおり確認します。
   - コマンド プロンプトから JBoss を起動する場合は、JBoss が起動するときの最初の出力を確認します。 出力にエラーが含まれていないことを確認します。
   - サービスとして JBoss を起動する場合は、ログ ファイルまたは tail コマンドを使用して、JBoss が起動したときの最初の出力を確認します。 出力にエラーが含まれていないことを確認します。
2. 以下のファイルを開いてエラーがあるかどうかを確認します（*JBossInstallDir* は JBoss をインストールしたディレクトリ）。

   JBossInstallDir/server/default/log/boot.log

   このファイルには、JBoss がマイクロカーネルをブートするたびに行ったステップが記録されます。
3. JAVA_HOME 変数が正しい場所に設定されていることを確認します。

   注: JAVA_HOME 変数が正しい場所に設定されているが、JBoss がこの変数を解決しない場合、JAVA_HOME 変数をより下位の場所（JDK インストール パス下の bin ディレクトリなど）に設定します。
4. 以下のファイルを開き、エラーが存在するかどうかを確認します。

   JBossInstallDir/server/default/log/server.log

   このファイルには、JBoss が JBoss Web アプリケーション サーバ環境で実行したアクションの一覧が記録されます。

   注: JBoss を起動するたびに新しい server.log ファイルが作成されます。
5. JBoss ポートが他のサービスで使用されるポートと競合していないことを確認します。

6. （オプション） JNP ポートが別のサービスと競合している場合は、以下の手順に従って JNP ポート 1099 を別のポートに変更します。
   a. テキストエディタで次のファイルを開きます。

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. 以下のセクションのポート番号を変更します。

      ```
      <!-- The listening port for the bootstrap JNP service. Set this to -1 to run
      the NamingService without the JNP invoker listening port.-->
      <attribute name="Port">1099</attribute>
      ```

   c. ファイルを保存して閉じます。
7. （オプション） RMI ポートが別のサービスと競合している場合は、以下の手順に従って RMI ポート 1098 を別のポートに変更します。
   a. テキストエディタで次のファイルを開きます。

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. 以下のセクションのポート番号を変更します。

      ```
      <!-- The port of the RMI naming service, 0 == anonymous -->
      <!-- attribute name="RmiPort">1098</attribute -->
      <attribute name="RmiPort">1098</attribute>
      ```

   c. ファイルを保存して閉じます。

レポート ポータルのトラブルシューティング

レポート ポータルを利用すると、配布サーバが中央データベースに格納するエンドポイント データにアクセスして、ビルトイン レポートを作成したり、そのデータを取得してカスタム レポートを作成したりできます。そのために、CA Business Intelligence を使用します。

レポート ポータルをトラブルシューティングする方法

1. レポート インターフェース（BusinessObjects InfoView）にアクセスするための正しい URL を使用していることを確認します。正しい URL は以下のとおりです。

   http://*host*:*port*/businessobjects/enterprise115/desktoplaunch

2. （Windows）InfoView にアクセスするための正しいメニュー オプションを使用していることを確認します。

   InfoView にアクセスするには、［スタート］-［プログラム］-［BusinessObjects XI Release 2］-［BusinessObjects Enterprise］-［BusinessObjects Enterprise Java InfoView］を選択します。

3. 以下のサービスが開始されることを確認します。
   - Apache Tomcat
   - Central Management Server
   - Connection Server
   - Crystal Reports Cache Server
   - Crystal Reports Job Server
   - Crystal Reports Page Server
   - Desktop Intelligence Cache Server
   - Desktop Intelligence Job Server
   - Desktop Intelligence Report Server
   - Destination Job Server
   - Event Server
   - Input File Repository Server
   - List of Values Job Server
   - Output File Repository Server
   - Program Job Server
   - Report Application Server
   - Web Intelligence Job Server
   - Web Intelligence Report Server

4. CA Access ControlUniverse への接続をテストします。

   注: CA Access ControlUniverse が BusinessObjects Designer に表示されない場合、レポート パッケージはデプロイしないことがあります。 レポート パッケージをデプロイする方法の詳細については、「実装ガイド」を参照してください。

CA Access Control Universe Connection をテストします

CA では、CA Access Control レポート サービス中央データベースに基づくレポート作成を簡略化するため、CA Access Control Universe を提供しています。

注: CA Access Control Universe の詳細については、「*エンタープライズ管理ガイド*」を参照してください。

CA Access Control の標準レポートをインストールした後で、レポート サービスの接続に関する問題が発生した場合は、 必要に応じて接続のテストおよび接続の設定変更を行う必要があります。

CA Access Control Universe Connection をテストする方法

1. ［スタート］-［プログラム］-［Business Objects XI Release 2］-［BusinessObjects Enterprise］-［Designer］を選択します。

   ［User Identification］ダイアログ ボックスが表示され、BusinessObjects Designer にログインできるようになります。

2. クレデンシャルを入力し、［OK］をクリックします。

   Quick Design ウィザードの開始画面が表示されます。

3. ［Run this Wizard at Startup］チェック ボックスをオフにし、［Cancel］をクリックします。

   空の Designer セッションが開きます。タイトル バー内にユーザ名およびリポジトリ名が表示されます。

4. ［ファイル］-［インポート］をクリックし、CA Access Control Universe を含むディレクトリに移動し、CA Access Control Universe を選択し、［OK］をクリックします。

   CA Access Control Universe は正常にインポートされると、現在の Designer ウィンドウで開きます。

   注: CA Access Control Universe は、デフォルトの Universe ファイル ストアとして指定されたディレクトリ内で CA Universe¥CA Access Control の下に格納されています。

5. ［ツール］-［接続］をクリックします。

   ［Wizard Connection］ダイアログ ボックスが表示されます。

6. テストする Access_Control1 接続を選択し、［テスト］をクリックします。

   接続が応答していることをメッセージで確認します。接続が応答していない場合、エラー メッセージが表示されます。

7. エラーが表示されたら、［編集］をクリックして接続の設定を変更します。

   - ［Database Middleware Selection］ - Oracle¥Oracle 10¥Oracle Client
   - ［タイプ］ - Secured
   - ［名前］ - Access_Control1
   - ［ユーザ名］ - *Oracle_adminUserName*
   - ［パスワード］ - *Oracle_adminUserPass*
   - ［サービス］ - Oracle_TNS_Name

   必要に応じて、手順 6 を繰り返し、接続をテストします。

レポート サーバがダウンしているか到達不能

症状:

CA Business Intelligence または CA Access Control エンタープライズ管理 でレポートを表示しようとすると、以下の内容のエラー メッセージが表示されます。

レポート サーバがダウンしているか到達不能です。

解決方法:

この問題を解決するには、以下の手順に従います。

1. JBoss ログ ファイルを開きます。JBoss ログ ファイルは以下のディレクトリにあります。*JBossInstallDir* は、JBoss をインストールしたディレクトリです。

   JBossInstallDir/server/default/log/server.log

   このファイルには、JBoss が JBoss Web アプリケーション サーバ環境で実行したアクションの一覧が記録されます。

   注: JBoss を起動するたびに新しい server.log ファイルが作成されます。

2. ログ ファイルでエラーの原因を特定します。

3. エラーに示されているコンピュータの名前を大文字と小文字を区別して書きとめます。

   名前は、ログ ファイルに表示されているとおりに正確に記録する必要があります。

4. hosts ファイルを開きます。 hosts ファイルはデフォルトでは以下のディレクトリにあります。

   - （UNIX） /etc/hosts
   - （Windows） C:¥WINDOWS¥system32¥drivers¥etc

5. ファイルの新しい行で、コンピュータの IP アドレスと、大文字と小文字を区別した名前を入力し、スペースで区切ります。

   コンピュータ名は手順 3 で記録しました。

6. ファイルを保存して閉じます。

例: hosts ファイル

以下のスニペットは hosts ファイルの例です。

```
127.0.0.1       localhost
```

MS SQL を使用した CA Business Intelligence でレポートを表示できない

症状:

中央データベースとして MS SQL データベースを使用している場合、CA Business Intelligence でレポートを表示できません。 レポートを表示しようとすると、以下の内容のエラー メッセージが表示されます。

接続に失敗しました

解決方法:

以下のプロセスは、CA Business Intelligence での問題のトラブルシューティングに役立ちます。

1. 以下の手順で BusinessObjects バージョン番号を確認します。
   a. 以下の URL を開きます。

      `http://hostname:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      hostname

      レポート ポータル ホスト名を定義します。

      Central Management Console のログオン ページが表示されます。

   b. ユーザ名とパスワードを入力し、［ログオン］をクリックします。

      Central Management Console が表示されます。

   c. ［Servers］-［*hostname*］-［Web_IntelligenceReportServer］-［Metrics］をクリックします。

      BusinessObjects のバージョン番号が表示されます。

   d. BusinessObjects のバージョン番号が 11.5.8.1061 以上、または 11.5.10.1263 以上のいずれかであることを確認します。

2. 以下の手順で CA Business Intelligence バージョン番号を確認します。
   a. レポート ポータル上の以下のファイルを開きます。

      - （Windows） C:¥Program Files¥CA¥SC¥CommonReporting¥version.txt
      - （UNIX） /opt/CA/SC/CommonReporting/version.txt

   b. CA Business Intelligence バージョンが 2.1.13 であることを確認します。

3. 以下の手順でデータベース クレデンシャルが正しいことを確認します。
   a. ［スタート］-［プログラム］-［Microsoft SQL Server］-［SQL Server Management Studio 2005］をクリックします。

      SQL Server 2005 ログイン ページが表示されます。

   b. CA Access Control エンタープライズ管理 用のデータベースを準備したときに作成した RDBMS 管理者ユーザのユーザ名およびパスワードを入力します。

   c. ［接続］をクリックします。

      SQL Server Management Studio にログインします。 ログインできない場合、データベース クレデンシャルが正しくありません。

4. 以下の手順で、*import_biar_config*.xml ファイルに正しい値が含まれていることを確認します。
   a. レポート ポータル上でレポート パッケージをデプロイするのに使用した *import_biar_config*.xml ファイルを開きます。

   b. 以下のプロパティの値が、手順 3 で指定した値に対応していることを確認します。
      - <username> が、入力したユーザ名と同じ。
      - <password> が、入力したパスワードと同じ。
      - <datasource> が、入力したデータベースの名前と同じ。
      - <server> が、レポート サーバ コンピュータの名前と同じ。

Oracle データベースを使用する CA Business Intelligence でレポートを表示できない

症状:

中央データベースとして Oracle データベースを使用している場合、CA Business Intelligence でレポートを表示できません。 レポートを表示しようとすると、以下の内容のエラー メッセージが表示されます。

接続に失敗しました

解決方法:

以下のプロセスは、CA Business Intelligence での問題のトラブルシューティングに役立ちます。

1. 以下の手順で BusinessObjects バージョン番号を確認します。
   a. 以下の URL を開きます。

      `http://hostname:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      hostname

      レポート ポータル ホスト名を定義します。

      Central Management Console のログオン ページが表示されます。

   b. ユーザ名とパスワードを入力し、［ログオン］をクリックします。

      Central Management Console が表示されます。

   c. ［Servers］-［*hostname*］-［Web_IntelligenceReportServer］-［Metrics］をクリックします。

      BusinessObjects のバージョン番号が表示されます。

   d. BusinessObjects のバージョン番号が 11.5.8.1061 以上、または 11.5.10.1263 以上のいずれかであることを確認します。

2. 以下の手順で CA Business Intelligence バージョン番号を確認します。
   a. レポート ポータル上の以下のファイルを開きます。
      - （Windows） C:¥Program Files¥CA¥SC¥CommonReporting¥version.txt
      - （UNIX） /opt/CA/SC/CommonReporting/version.txt

   b. CA Business Intelligence バージョンが 2.1.13 であることを確認します。

3. Oracle システム環境変数が以下のとおり定義されていることを確認します。*Oracle_home* は Oracle をインストールしたディレクトリです。
   - ORACLE_HOME が *Oracle_home* ディレクトリを指している。
   - PATH に *Oracle_home*/bin ディレクトリが指定されている。
   - TNS_ADMIN が *Oracle_home*/network/admin ディレクトリを指している。

4. 以下の手順で、TNS が正しく定義されていることを確認します。
   a. コマンド プロンプト ウィンドウを開きます。
   b. 以下のコマンドを実行します。

      `tnsping TNSname`

      TNSname

      TNS の名前を定義します。

      エラー メッセージが表示された場合、TNS は正しく定義されていません。

5. データベースへのアクセスに正しいクレデンシャルを使用していることを以下の手順で確認します。
   a. コマンド プロンプト ウィンドウを開きます。
   b. 以下のコマンドを実行します。

      `sqlplus user/password@TNSname`

      ユーザ

      CA Access Control エンタープライズ管理 用にデータベースを準備したときに作成した RDBMS 管理者ユーザの名前を定義します。

      password

      ユーザ パスワードを定義します。

      SQL コマンド ラインにログオンできない場合は、データベース クレデンシャルが正しくありません。

6. 以下の手順で、*import_biar_config*.xml ファイルに正しい値が含まれていることを確認します。
   a. レポート ポータル上でレポート パッケージをデプロイするのに使用した *import_biar_config*.xml ファイルを開きます。
   b. 以下のプロパティの値が、手順 5 で指定した値に対応していることを確認します。
      - <username> が *user* と同じ
      - <password> が *password* と同じ
      - <datasource> が *TNSname* と同じ
7. （UNIX） CA Business Intelligence をインストールしたときに指定したユーザとして、手順 4 および手順 5 でコマンドを実行します。

   このユーザは、CA Business Intelligence インストール ウィザードの CMS データベース設定ページで指定します。 この手順によって、ユーザが *Oracle_home* ディレクトリ全体に対して読み取り権限および実行権限を持っているかどうかを確認できます。

CA Access Control エンタープライズ管理 でレポートを表示できない

症状:

CA Access Control エンタープライズ管理 でレポートを表示しようとすると、Business Objects のログオン ダイアログ ボックスが表示され、［プライバシー レポート］アイコンがブラウザに表示されます。

解決方法:

ブラウザで、レポート ポータルからの Cookie がブロックされています。この問題を解決するには、レポート ポータルからの Cookie を許可するようにブラウザの Cookie 設定を調整します。

注: プライバシー レポートでは、ブラウザがブロックする cookies より多くの情報が提供されます。 プライバシー レポートを表示するには、［プライバシー レポート］アイコンをダブルクリックします。

付録 A: トラブルシューティングおよび保守の手順

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 Access Control が正しくインストールされていることを確認する方法

Windows で該当

CA Access Control をインストールしたら、正しくインストールされていることをただちに確認する必要があります。 CA Access Control が正しくインストールされていることを確認するには、以下の手順に従います。

CA Access Control のインストールが正常に完了したら、以下の変更点に注目してください。

- 以下の Windows レジストリに新しいキーが追加されています。

  HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl

  CA Access Control が実行されている間、CA Access Control のキーおよびサブキーは保護されています。また、キーを変更できるのは、CA Access Control エンドポイント管理 を使用するか、selang コマンドの使用する場合のみです。 しかしながら、キーと値を読み取るために CA Access Control エンドポイント管理 または selang コマンドを使用する必要はありません。

- コンピュータを再起動すると、CA Access Control の複数の新しいサービスが自動的に開始されます。これらのサービスには、Watchdog、Engine、および Agent が含まれます。この 3 つのサービスは必ずインストールされます。 タスクの委任などのその他のサービスは、インストール時に選択したオプションによってインストールされるかどうかが決まります。 CA Access Control サービスの表示名はすべて、「CA Access Control」で始まります。 Windows サービス マネージャを使用すれば、インストールされているサービスを確認し、それらのサービスが動作中であることを検証できます。

リソース アクセスの問題をトラブルシューティングする方法

リソース アクセスに関する問題の最も一般的な原因は、不適切なアクセス権限です。 リソース アクセス問題の一例として、保護されたリソースに対するデフォルト アクセス権が none であるにもかかわらず、root ユーザがこれらのリソースにアクセスできてしまうことがあります。 リソース アクセスの問題のトラブルシューティングに役立つプロセスを以下に示します。

1. 保護されたリソースの監査モードを「すべて監査」に変更します。

   ```
   chres CLASS ResourceName audit(all)
   ```

   監査モードを「すべて監査」に変更すると、監査ログが参照しやすくなります。

2. トレースを実行 (P. 135) して問題を再現します。

3. トレース ファイルおよび監査ログで、保護されたリソースに対するアクセスを確認します。ファイル中の情報に基づいて、リソース アクセスの問題の原因を解決します。

   注: SPECIALPGM オブジェクトは監査されないバイパスを提供しますが、これらのバイパスはトレース ファイルに表示されます。

注:詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

接続の問題をトラブルシューティングする方法

CA Access Control コンピュータ間の接続は、さまざまな要因の影響を受けます。 接続の問題には、リモート CA Access Control コンピュータに接続できない、リモート コンピュータとの接続がタイムアウトになる、といった現象が含まれます。 接続の問題の原因を特定するのに役立つプロセスを以下に示します。

注:詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

1. CA Access Control コンピュータで、以下の項目に対して最近変更が加えられたかどうかをチェックします。
   - 暗号化キー
   - 暗号化方法
   - TCP および UDP ポート
2. TCP、CONNECT、HOSTNET、または HOST クラスで、新しいルールまたは最近変更されたルールを確認します。
3. 接続の問題が存在するポートを特定します。
4. トレースを実行 (P. 135) し、トレース ファイルで以下を確認します。
   - CA Access Control が TCP ルールまたは他のルールに基づいてブロックした接続
   - 接続の問題があるポート番号の隣に表示される P （許可）以外のコード
5. CA Access Control 監査ログで、問題があるポートを示す D （拒否）レコードを確認します。
6. ファイアウォールが問題を抱えるポートをブロックしていないことを確認します。
7. OS のログ ファイルで、バインドできないポートによって発生したエラー メッセージを確認します。

詳細情報:

CA Access Control エージェント通信用のポート番号の変更 (P. 139)

パフォーマンスの問題をトラブルシューティングする方法

パフォーマンスに関する問題の原因を特定するには、以下の手順に従います。

注:詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

1. パフォーマンスの問題がいつ発生するかを特定します。パフォーマンスが低下するのはいつですか?
   - OS を起動するとき
   - CA Access Control を起動するとき
   - CA Access Control の起動後しばらく経過したとき
   - CA Access Control または OS がスケジュールされたプロセスを実行するとき
   - （UNIX） CA Access Control カーネル拡張機能がロードされるとき
   - CA Access Control デーモンまたはサービスがロードされるとき
2. CA Access Control がパフォーマンスの問題の原因であると特定した場合は、以下の事項を調べます。
   - パフォーマンスが低下したときに最もリソースを消費しているプロセスは何ですか?
   - その CA Access Control プロセスはライフサイクルを通して同じプロセス ID を保持していますか?
   - サードパーティのフィルタ ドライバがコンピュータにインストールされていますか?
   - システム監視アプリケーションがコンピュータにインストールされていますか?

3. CA Access Control データベースをチェックします。
   a. CA Access Control を停止します。
   b. データベースをチェックします。

      ```
      dbmgr -util -all
      ```

   c. データベースのインデックスを再作成します (P. 137)。
   d. データベースを再構築します (P. 138)。
   e. CA Access Control を再起動して、問題がまだ存在するかどうかを確認します。
4. （Windows） ドライバ インターセプトを無効にします。
   a. CA Access Control を停止します。
   b. UseFsiDrv レジストリ エントリの値を 0 に変更します。UseFsiDrv レジストリ エントリは次のレジストリ キーにあります。

      ```
      HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl
      ```

   c. CA Access Control を再起動して、問題がまだ存在するかどうかを確認します。
5. トレースを実行 (P. 135)して問題を再現します。 トレース ファイルで以下の事項を確認します。
   - 短期間中に繰り返されたイベント（数秒中の多数のファイル アクセスなど）。
   - 強制終了されたプロセス。
   - 以下の値のいずれか。
     - ACEEH -1
     - U= 負の値

     これらの値によって、CA Access Control がユーザ名を解決できない、または値をリソースに割り当てることができないことが指定される場合があります。

注: UNIX コンピュータ上での CA Access Control パフォーマンスの改善の詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

トレースの実行

トレースを実行することで問題を解決できる場合があります。 CA Access Control は、seos.trace ファイル（*ACInstallDir*/log ディレクトリに存在する）にトレース レコードを書き込みます。

トレースを実行するには、以下の手順に従います。

1. トレース ファイルからレコードをすべて取り除きます。

   ```
   secons -tc
   ```

2. トレースを開始します。

   ```
   secons -t+
   ```

3. 問題を再現します。
4. トレースを停止します。

   ```
   secons -t-
   ```

5. トレース ファイルを参照します。

注: seosd セクション中の設定値でトレース ファイルを設定します。seosd セクションの詳細については、「*リファレンス ガイド*」を参照してください。

CA Access Control Web サービス コンポーネント上でのトレースの実行

Windows で該当

CA Access Control Web サービス コンポーネント上でトレースを実行すると、問題のトラブルシューティングに役立つ場合があります。たとえば、CA Access Control エンタープライズ管理 が DMS に接続できない場合、トレースを実行して、これらの 2 つのコンポーネント間で交換されるメッセージを確認できます。

CA Access Control では、Web サービス コンポーネントのトレース レコードを、WebService セクションの logFileName 設定に定義されているファイルに書き込みます。 この設定のデフォルト値は「C:¥Program Files¥CA¥AccessControlServer¥WebService¥log¥WebService.log」 です。

CA Access Control Web サービス コンポーネント上でトレースを実行する方法

1. CA Access Control および CA Access Control Web サービスを停止します。
2. 以下の場所にレジストリ キーを作成します。

   HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥WebService¥TraceEnabled
3. キーの値を 1 に設定します。
4. CA Access Control および CA Access Control Web サービスを開始します。

   CA Access Control Web サービス コンポーネントでトレースが開始されます。
5. 問題を再現します。
6. CA Access Control および CA Access Control Web サービスを停止します。

   CA Access Control Web サービス コンポーネントでトレースが停止されます。
7. キーの値を 0 に設定します。
8. トレース ファイルを参照します。

CA Access Control データベースのインデックスの再作成

CA Access Control データベースには数多くの更新が加えられるので、データベース ファイルは次第に断片化していく場合があります。 データベースを最適化して速度と信頼性を高めるには、インデックスの再作成およびデータベースの再構築 (P. 138)を行います。 データベースのインデックス再作成は、3 ー 6 か月ごとに定期保守の一環として行い、さらにパフォーマンス上の問題が発生するたびに行ってください。

注: この手順では、CA Access Control データベースはデフォルトの場所（UNIX の場合は /opt/CA/AccessControl/seosdb、Windows の場合は C：¥Program Files¥CA¥AccessControl¥Data¥seosdb）にインストールされます。この手順を実行するには、root ユーザ（UNIX）または管理者（Windows）としてログインする必要があります。

CA Access Control データベースのインデックスを再作成する方法

1. CA Access Control を停止します。
2. 以下のディレクトリに移動します。
   - （UNIX） /opt/CA/AccessControl/seosdb
   - （Windows） C:¥Program Files¥CA¥AccessControl¥Data¥seosdb
3. データベースをバックアップします。

   ```
   dbmgr -backup backup_directory
   ```

4. データベースにインデックスを付けます。

   ```
   dbmgr -util -build seos_cdf.dat
   dbmgr -util -build seos_odf.dat
   dbmgr -util -build seos_pdf.dat
   dbmgr -util -build seos_pvf.dat
   ```

注: UNIX コンピュータ上のデータベースのサイズをさらに縮小するには、sepurgdb ユーティリティを使用して未定義レコードの参照をデータベースから削除します。sepurgdb ユーティリティの詳細については、「*リファレンス ガイド*」を参照してください。

CA Access Control データベースの再構築

CA Access Control データベースには数多くの更新が加えられるので、データベース ファイルは次第に断片化していきます。 データベースを最適化して速度と信頼性を高めるには、インデックスの再作成 (P. 137)およびデータベースの再構築を行います。 データベースの再構築は、3 ー 6 か月ごとに定期保守の一環として行ってください。

注: この手順では、CA Access Control データベースはデフォルトの場所（UNIX の場合は /opt/CA/AccessControl/seosdb、Windows の場合は C：¥Program Files¥CA¥AccessControl¥Data¥seosdb）にインストールされます。この手順を実行するには、root ユーザ（UNIX）または管理者（Windows）としてログインする必要があります。

CA Access Control データベースを再構築する方法

1. CA Access Control を停止します。
2. 以下のディレクトリに移動します。
   - （UNIX） /opt/CA/AccessControl/seosdb
   - （Windows） C:¥Program Files¥CA¥AccessControl¥Data¥seosdb
3. データベースをバックアップします。

   ```
   dbmgr -backup backup_directory
   ```
4. データベースからの既存のルールとユーザ関連データをエクスポートします。

   ```
   dbmgr -export -l -f exported_filename
   dbmgr -migrate -r migrated_filename
   ```
5. 以下のディレクトリに移動して、その下に seosdb_new という名前のディレクトリを作成します。
   - （UNIX） /opt/CA/AccessControl
   - （Windows） C:¥Program Files¥CA¥AccessControl¥Data
6. seosdb_new ディレクトリにデータベースを作成します。

   ```
   dbmgr -create -cq
   ```
7. *exported_filename* および *migrated_filename* ファイルを seosdb_new ディレクトリにコピーします。
8. 古いデータベースからエクスポートした既存のルールとユーザ関連データを新しいデータベースにインポートします。

```
selang -l -f exported_filename
dbmgr -migrate -w migrated_filename
```

9. seosdb ディレクトリの名前を seosdb_old に変更します。
10. seosdb_new ディレクトリの名前を seosdb に変更します。
11. CA Access Control を起動します。

CA Access Control エージェント通信用のポート番号の変更

CA Access Control クライアント アプリケーション（selang、policydeploy、devcalc など）および CA Access Control エージェントは、ポート 8891 上で通信します。 このポートを変更することはお勧めしません。 このポートを変更する必要がある場合は、以下の手順に従います。

CA Access Control エージェント通信用のポート番号を変更する方法

1. テキストエディタで次のファイルを開きます。
   - （UNIX） /etc/services
   - （Windows） %SystemRoot%¥drivers¥etc¥services
2. このファイルに以下のファイルを追加します。

   ```
   seoslang2 port-number/ tcp
   ```
3. ファイルを保存して閉じます。
4. CA Access Control デーモンまたはサービスを再起動します。

メッセージ キューの TCP ポートの設定

CA Access Control エンタープライズ管理 をインストールするときは、デフォルトで、SSL ポート（7243）と連携するようメッセージ キューを設定します。 このデフォルトの動作を変更し、TCP ポート（7222）を使用するようメッセージ キューを設定することができます。

メッセージ キュー TCP ポートに接続する方法

1. エンタープライズ管理サーバで、メッセージ キューおよび JBoss サーバを停止します。
2. tibemsd.conf ファイルを開いて、編集します。 このファイルは以下の場所にあります。

   ```
   C:¥Program Files¥CA¥AccessControl¥/MessageQueue/tibco/tibco/cfgmgmt/ems/data
   ```

3. エントリ「listen=」を確認し、既存の値を削除して、「tcp://7222」を入力します。
4. エントリ「authorization=」を確認し、既存の値を削除して、「disabled」を入力します。
5. ファイルを保存して閉じます。
6. factories.conf ファイルを開き、タグ［SSLXAQueueConnectionFactory］を確認します。
7. エントリ「url=」を確認し、既存の値を削除して、「tcp://7222」と入力します。
8. ファイルを保存して閉じます。
9. tibco-jms-ds.xml ファイルを編集できる形で開きます。 このファイルは以下の場所にあります。

   ```
   JBoss_HOME/server/default/deploy/jms
   ```

10. SSL ポート番号（7243）を示すすべての値を検索し、TCP ポート番号 7222 で置き換えます。
11. 値 SSLXA を示すすべてのエントリを検索し、XA で置き換えます。
12. 以下の 2 つのエントリをコメント（<!--）にします。

    ```
    com.tibco.tibjms.naming.security_protocol=ssl
    com.tibco.tibjms.naming.ssl_enable_verify_host=false
    ```

13. ファイルを保存して閉じます。
14. メッセージ キューおよび JBoss サーバを開始します。

CA サポートに提供する必要がある情報

CA サポートに連絡すると、問題の診断に使用するために、お使いの環境に対する変更について情報提供を求められます。たとえば、ホストとユーザ名の変更、およびオペレーティング システムの変更は、CA Access Control に影響する可能性があります。 CA サポートは、さらに詳細の診断情報を CA Access Control サポート ユーティリティを使用して提供するよう依頼する場合があります。

CA サポートに提供する必要がある情報には以下があります。

- CA Access Control バージョン
- オペレーティング システム名、バージョン、アーキテクチャ、更新レベル
- コンピュータにインストールされたすべての CA Access Control パッチの詳細
- CPU の数

注: CA Access Control がサポートするオペレーティング システム、バージョン、アーキテクチャ、および更新レベルの詳細については、CA サポート サイト上の CA Access Control 製品ページで提供される CA Access Control Compatibility Matrix を参照してください。

また、CA サポートから以下の情報を求められる可能性があります。

- 問題の影響度。
- 最初に問題が発生したのはいつか。
- 問題は再現可能か。
- 問題が発生する前に、その環境に追加、削除、変更されたものがあるか。
- 問題が発生する前に、コンピュータを再起動したか。
- 問題は何回発生したか。
- 問題が発生するときは、システム上で何が起きるか。 たとえば、特定のプロセスまたはコマンドを実行すると問題が発生する、など。
- 問題は一貫して発生するか、またはランダムに発生するか。
- CA Access Control コマンドを実行すると、セグメンテーション エラーまたはアクセス違反が発生するか。

- CA Access Control でその問題が発生した原因に心当たりがあるか。
- 問題がオペレーティング システムの問題である場合、オペレーティング システムのベンダーに問題を報告したか。した場合、オペレーティング システム ベンダーからのクラッシュ分析を提供できるか。

Windows エンドポイントに関する診断情報の生成

CA Access Control サポート ユーティリティは、CA サポートが問題を診断するのを助けるため、お使いの CA Access Control インストールに関する情報を収集します。CA Access Control サポート ユーティリティが収集する情報は、ACSupport ダイアログ ボックスで指定します。

以下のシステム情報を収集できます。

- システム情報レポート
- イベント ログ

以下の CA Access Control 情報を収集できます。

- CA Access Control バージョン、ホーム ディレクトリ、CA Access Control サービスのステータスに関する一般的な情報
- CA Access Control レジストリ
- 監査、トレース、共存ユーティリティ用の環境設定ファイル
- 監査ログおよびトレース ログ（ローカル PMDB または DMS の監査ログ、インストルメンテーション トレースを含む）
- 許可とキャッシュの統計
- コンピュータにインストールされた CA Access Control 実行ファイルと DLL のリスト
- CA Access Control データベースのスナップショット（ローカル PMDB および DMS を含む）

  注: CA Access Control データベースのコピーを収集する場合、CA Access Control サポート ユーティリティは、データベースのスナップショットを取得する前に CA Access Control を停止し、スナップショットの取得が完了したら CA Access Control を再起動します。

Windows エンドポイントに関する診断情報の生成方法

1. 以下のディレクトリに移動します（*ACInstallDir* は CA Access Control をインストールしたディレクトリです）。

   ACInstallDir¥bin

2. ACSupport.exe をダブルクリックします。

   ACSupport ダイアログ ボックスが開きます。

3. ダイアログ ボックスへの入力を完了し、続行します。

   CA Access Control サポート ユーティリティは、インストールのスナップショットを取得し、*ACInstallDir*¥ACSupport ディレクトリに出力します。

UNIX エンドポイントに関する診断情報の生成

CA Access Control サポート ユーティリティは、CA サポートが問題を診断するのを助けるため、お使いの CA Access Control インストールに関する情報を収集します。 CA Access Control データベースをスナップショットに含める場合、CA Access Control のサポート ユーティリティはデータベースのスナップショットを作成する前に CA Access Control を停止し、スナップショットが完成すると、 CA Access Control を開始します。

この CA Access Control サポート ユーティリティは、UNIX エンドポイントに関する以下の情報を常時収集します。

- seos.ini -- CA Access Control の初期設定ファイル
- tmpetc -- CA Access Control/etc ディレクトリにあるファイルで、以下が含まれます。
  - audit.cfg -- 監査フィルタファイル
  - auditroute.cfg -- 監査ルート フィルタ ファイル
  - nfsdevs.init -- 各オペレーティング システムのメジャー デバイス番号の NFS デフォルト値が含まれているファイル
  - osvert -- オペレーティング システムのバージョン
  - sereport.cfg -- sereport 環境設定ファイル
  - serevu.cfg -- serevu 環境設定ファイル
  - trcfilter.init -- トレース フィルタ ファイル
- versions.txt -- キー CA Access Control バイナリのバージョンが含まれているファイル
- 一部のオペレーティング システム ファイル、たとえば変数ファイル

CA Access Control サポート ユーティリティで CA Access Control データベースに関する情報を収集するように指定すると、以下の情報が収集されます。

- seosdb -- CA Access Control データベース
- seosdb.tar -- CA Access Control データベースの圧縮ファイル
- グループ、ホスト、サービスおよびユーザの lookaside データベース

CA Access Control サポート ユーティリティで CA Access Control ログに関する情報を収集するように指定すると、以下の情報が収集されます。

- tmplog -- CA Access Control のログ ファイル
- log.tar -- CA Access Control ログ ディレクトリの圧縮ファイル

UNIX エンドポイントに関する診断情報の生成方法

1. 以下のディレクトリに移動します（*ACInstallDir* は CA Access Control をインストールしたディレクトリです）。

   ACInstallDir/lbin

2. 次のコマンドを実行します。

   ```
   ./support.sh [-db] [-log] [-all] [-none]
   ```

   -db

   seosdb、すなわち CA Access Control データベースに関する情報は収集しますが、監査ログに関する情報は収集しません。

   -log

   監査ログに関する情報は収集しますが、seosdb に関する情報は収集しません。

   -all

   seosdb と監査の両方のログに関する情報を収集します。

   -none

   seosdb と監査ログのいずれに関する情報も収集しません。

   注: オプションを指定しない場合、CA Access Control サポート ユーティリティは対話モードで実行されます。

   CA Access Control サポート ユーティリティは、インストールのスナップショットを作成し、*ACInstallDir* ディレクトリに出力します。