



HP Universal CMDB および Configuration Manager

ソフトウェア・バージョン : 10.20

強化ガイド

ドキュメント・リリース日 : 2015年1月
ソフトウェア・リリース日 : 2015年1月

ご注意

保証

HP 製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的、編集上の誤り、または欠如について、HP はいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータ・ソフトウェアです。これらを所有、使用、または複製するには、HP からの有効な使用許諾が必要です。商用コンピュータ・ソフトウェア、コンピュータ・ソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211 および 12.212 の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

© Copyright 2002 - 2015 Hewlett-Packard Development Company, L.P.

商標

Adobe™ は、Adobe Systems Incorporated の商標です。

Microsoft® および Windows® は、Microsoft Corporation の米国登録商標です。

UNIX® は、The Open Group の登録商標です。

本製品には、Copyright © 1995-2002 Jean-loup Gailly and Mark Adler である「zlib」汎用圧縮ライブラリのインターフェースが含まれています。

文書の更新

このマニュアルの表紙には、以下の識別番号が記載されています。

- ソフトウェアのバージョン番号は、ソフトウェアのバージョンを示します。
- ドキュメント・リリース日は、ドキュメントが更新されるたびに更新されます。
- ソフトウェア・リリース日は、このバージョンのソフトウェアのリリース期日を表します。

最新のアップデートまたはドキュメントの最新版を使用していることを確認するには、次の URL にアクセスしてください：<https://softwaresupport.hp.com>

このサイトでは、HP Passport に登録してサインインする必要があります。HP Passport ID の登録は、次の URL にアクセスしてください。<https://hpp12.passport.hp.com/hppcf/createuser.do>

または、HP ソフトウェア・サポート・ページの上にある【登録】リンクをクリックします。

適切な製品サポート・サービスに登録すると、更新情報や最新情報も入手できます。詳細については HP の営業担当にお問い合わせください。

サポート

次の HP ソフトウェアのサポート・オンラインの Web サイトをご覧ください。

<https://softwaresupport.hp.com>

この Web サイトでは、連絡先情報と、HP ソフトウェアが提供する製品、サービス、およびサポートについての詳細が掲載されています。

HP ソフトウェア・オンライン・ソフトウェア・サポートでは、お客様にセルフ・ソルブ機能を提供しています。ビジネス管理に必要な、インタラクティブなテクニカル・サポート・ツールに迅速かつ効率的にアクセスできます。有償サポートをご利用のお客様は、サポート・サイトの次の機能をご利用いただけます。

- 関心のある内容の技術情報の検索
- サポート・ケースおよび機能強化要求の提出および追跡
- ソフトウェア・パッチのダウンロード
- サポート契約の管理
- HP サポートの連絡先の表示
- 利用可能なサービスに関する情報の確認
- ほかのソフトウェア顧客との議論に参加
- ソフトウェアのトレーニングに関する調査と登録

ほとんどのサポート・エリアでは、HP Passport ユーザとして登録し、ログインする必要があります。また、多くの場合、サポート契約も必要です。HP Passport ID を登録するには、次の Web サイトにアクセスしてください。

<https://hpp12.passport.hp.com/hppcf/createuser.do>

アクセスレベルに関する詳細は、以下の Web サイトにアクセスしてください。

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software Solutions Now は、HPSW のソリューションと統合に関するポータル Web サイトです。このサイトでは、お客様のビジネスニーズを満たす HP 製品ソリューションを検索したり、HP 製品間の統合に関する詳細なリストや ITIL プロセスのリストを閲覧することができます。この Web サイトの URL は **<http://h20230.www2.hp.com/sc/solutions/index.jsp>** です

目次

第1章: 強化の紹介	7
強化の概要	7
強化の準備	8
安全なアーキテクチャへの UCMDb のデプロイ	8
システムのアクセス権	9
Java JMX Access の強化	9
JMX コンソールのシステム・ユーザ名またはパスワードの変更	11
HP Universal CMDB Server サービス・ユーザの変更	12
Configuration Manager のデータベース・パスワードの暗号化	14
Configuration Manager データベースのパスワード暗号化のためのパラメータ	14
第2章: Secure Sockets Layer (SSL) 通信の有効化	17
自己署名証明書を使ったサーバ・マシンの SSL 有効化 - UCMDb	17
自己署名証明書を使ったサーバ・マシンの SSL 有効化 - Configuration Manager	19
認証局から取得した証明書を使ったサーバ・マシンの SSL 有効化 - UCMDb	20
認証局から取得した証明書を使ったサーバ・マシンの SSL 有効化 - Configuration Manager	22
クライアント・マシンでの SSL の有効化 - UCMDb	23
クライアント証明書で SSL を有効化 - Configuration Manager	24
クライアント SDK での SSL の有効化	25
SDK の相互証明書認証の有効化	25
UCMDb での CAC (スマート・カード/PKI 認証) サポートの設定	27
サーバ・キー・ストアのパスワードの変更	29
HTTP/HTTPS ポートの有効化と無効化	30
UCMDb Web コンポーネントのポートへのマップ	31
SSL を使用して UCMDb の作業を行うための Configuration Manager の設定	32
SSL で使用する UCMDb KPI アダプタの有効化	34
UCMDb Browser の SSL サポートの構成	35
第3章: リバース・プロキシの使用	36
リバース・プロキシの概要	36
リバース・プロキシ・サーバの使用のセキュリティ面	37
リバース・プロキシの設定	38
相互認証を使用するリバース・プロキシまたはロード・バランサによる、Data Flow Probe の接続	41
リバース・プロキシによる UCMDb の CAC サポートの構成	43
第4章: データ・フロー資格情報管理	49
データ・フロー資格情報管理の概要	50

セキュリティ上の基本的な前提条件	51
別々のモードで実行されている Data Flow Probe	51
資格情報キャッシュを最新に保つ	51
すべてのプローブでの設定変更の同期	52
プローブ上の安全なストレージ	52
資格情報の表示	53
資格情報のアップグレード	53
機密マネージャ・クライアント認証と暗号化設定の設定	54
LW-SSO 設定の構成	54
機密マネージャ・コミュニケーション暗号化の設定	54
プローブでの手動での機密マネージャ・クライアントの認証設定および暗号化設定	56
サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化	56
プローブでの機密マネージャ・クライアントの認証設定および暗号化設定	57
プローブでの資格情報マネージャ通信の暗号化の設定	57
資格情報マネージャ・クライアントのキャッシュの設定	58
プローブでの機密マネージャ・クライアントのキャッシュ・モードの設定	58
プローブでの機密マネージャ・クライアントのキャッシュ暗号化文字列の設定	59
暗号化された形式による、資格情報および範囲情報のエクスポートとインポート	60
資格情報マネージャ・クライアントのログ・ファイル・メッセージ・レベルの変更	61
機密マネージャ・クライアント・ログ・ファイル	62
LW-SSO ログ・ファイル	62
暗号鍵の生成または更新	63
新規暗号鍵の生成	63
UCMDB サーバでの暗号鍵の更新	64
プローブでの暗号鍵の更新	65
Probe Manager とプローブ・ゲートウェイが別々のマシンにインストールされている場合における暗号鍵の手動による変更	66
複数の JCE プロバイダの定義	66
資格情報マネージャの暗号化設定	67
トラブルシューティングおよび制限事項	68
第5章: Data Flow Probe の強化	69
PostgreSQL データベースの暗号化パスワードの変更	69
clearProbeData スクリプト: 使用法	71
JMX コンソールに暗号化パスワードを設定	71
UploadScanFile のパスワード設定	72
PostgreSQL サーバへのリモート・アクセス	73
UCMDB サーバと Data Flow Probe 間の SSL の有効化	73
概要	74
キー・ストアとトラスト・ストア	74
サーバ認証 (一方向) での SSL の有効化	75

サーバ証明書認証（双方向）の有効化	77
エージェントまたはスキャナに対する aioptionrc ファイルの権限の変更方法	84
Data Flow Probe のキー・ストアの作成	84
プローブのキー・ストアとトラスト・ストアのパスワードを暗号化	85
サーバと Data Flow Probe のデフォルトのキー・ストアとトラスト・ストア	85
UCMDB サーバ	86
Data Flow Probe	86
エージェントまたはスキャナに対する aioptionrc ファイルの権限の変更方法	86
第6章: Lightweight シングル・サインオン（LW-SSO）認証	88
LW-SSO 認証の概要	88
LW-SSO のシステム要件	89
LW-SSO のセキュリティに関する警告	90
トラブルシューティングおよび制限事項	91
既知の問題	91
制限事項	92
第7章: HP Universal CMDB ログイン認証	95
認証メソッドの設定	95
HP Universal CMDB への LW-SSO によるログインを有効化	96
SSL（Secure Sockets Layer）プロトコルによるセキュア接続の設定	96
JMX コンソールを使用した LDAP 接続のテスト	98
LDAP 認証メソッドを有効化および定義する方法	98
JMX コンソールを使用して LDAP 認証メソッドを有効化および定義する方法	100
LDAP 認証設定 - 例	101
分散化環境における現在の LW-SSO 設定の取得	102
第8章: 機密マネージャ	103
機密マネージャの概要	103
セキュリティの考慮事項	103
HP Universal CMDB Server の設定	104
定義	105
暗号化プロパティ	105
第9章: 可用性の高い強化	108
クラスタ認証	108
クラスタ・メッセージの暗号化	109
トラブルシューティング	110
key.bin の鍵の変更	110
ドキュメントに関するフィードバックの送信	112

第1章: 強化の紹介

本章の内容

- [強化の概要](#) 7
- [強化の準備](#) 8
- [安全なアーキテクチャへの UCMDB のデプロイ](#) 8
- [システムのアクセス権](#) 9
 - [Java JMX Access の強化](#) 9
 - [JMX コンソールのシステム・ユーザ名またはパスワードの変更](#) 11
 - [HP Universal CMDB Server サービス・ユーザの変更](#) 12
 - [Configuration Manager のデータベース・パスワードの暗号化](#) 14
 - [Configuration Manager データベースのパスワード暗号化のためのパラメータ](#) 14

強化の概要

本項では、セキュリティで保護された HP Universal CMDB アプリケーションの概念について紹介し、セキュリティを実装するために必要な計画とアーキテクチャについて説明します。セキュリティ強化について説明する次のセクションに進む前に、このセクションを読むことを強くお勧めします。

HP Universal CMDB は、セキュリティ保護アーキテクチャの一部となるように設計されており、さらされる可能性のあるセキュリティ上の脅威に対処するという課題に対応しています。

セキュリティ強化のガイドラインでは、より安全な（セキュリティ強化された）HP Universal CMDB の実装に必要な設定作業について取り上げます。

提供されるセキュリティ強化の情報は主に、セキュリティ強化の手順を開始する前にセキュリティ強化の設定と推奨事項について精通している HP Universal CMDB 管理者を対象としています。

HP Universal CMDB にリバース・プロキシを組み合わせて使用して、セキュリティ保護アーキテクチャを実現することを強くお勧めします。HP Universal CMDB でリバース・プロキシを使うための設定方法の詳細については、「[リバース・プロキシの使用](#)」(36ページ)を参照してください。

HP Universal CMDB で、このドキュメントで説明する以外の別の安全なアーキテクチャを使用する必要がある場合は、どのアーキテクチャが最良かを決定するために HP ソフトウェア・サポートにお問い合わせください。

Data Flow Probe のセキュリティ強化の詳細については、「[Data Flow Probe の強化](#)」(69ページ)を参照してください。

注:

- このセキュリティ強化の手順は、これらの章で提供された指示だけを実装し、他の文書に記述されているセキュリティ強化の手順は実行しないことを前提としています。
- セキュリティ強化手順が、特定の分散アーキテクチャを前提としている場合であっても、そのアーキテクチャがユーザの組織のニーズに合う最適なアーキテクチャであるとは限りません。
- 以降の章に含まれる手順は、HP Universal CMDB 専用のマシンで実行されることを想定しています。コンピュータを HP Universal CMDB 以外の用途に使用した場合、問題が生じることがあります。
- 本項に示すセキュリティ強化に関する情報は、ご利用のコンピュータ・システムのセキュリティ・リスク評価を行うためのガイドラインを意図したものではありません。

強化の準備

- 利用するネットワーク全体のセキュリティ上の危険やセキュリティの状態の評価を行い、その評価結果に基づいて、HP Universal CMDB をネットワークに最適な形で統合する方法を判断します。
- HP Universal CMDB の技術フレームワークと HP Universal CMDB のセキュリティ機能についてよく理解してください。
- セキュリティ強化ガイドラインのすべての内容に目を通します。
- HP Universal CMDB が完全に機能していることを確認してから、セキュリティ強化手順を開始します。
- セキュリティ強化手順は、各章に記載されている順序どおりに実行します。たとえば、HP Universal CMDB サーバで SSL をサポートするには、[「Secure Sockets Layer \(SSL\) 通信の有効化」\(17ページ\)](#) をまず読んでから、記載されている順序のとおり手順を実行します。
- HP Universal CMDB では、空のパスワードでの基本認証をサポートしていません。基本認証の接続パラメータを設定するときは、パスワードを省略しないでください。

ヒント: セキュリティ強化手順を印刷して、作業時に確認しながら作業してください。

安全なアーキテクチャへの UCMDB のデプロイ

HP Universal CMDB サーバを安全にデプロイするのに、いくつかの方法を推奨します。

- **ファイアウォールを使用する DMZ アーキテクチャ**

ここでのセキュリティ保護アーキテクチャとは、デバイスをファイアウォールとして使用する典型的な DMZ アーキテクチャのことです。アーキテクチャの基本的な概念は、HP Universal CMDB ク

クライアントと HP Universal CMDB サーバを完全に切り離し、これらの間の直接アクセスをなくすことです。

- **安全なブラウザ**

Windows 環境での Internet Explorer および Firefox は、Java スクリプト、アプレット、cookie を安全に処理するように設定されている必要があります。

- **SSL 通信プロトコル**

Secure Sockets Layer プロトコルは、クライアントとサーバ間の通信を保護します。SSL 通信を必要とする URL は、ハイパーテキスト転送プロトコルのセキュリティ保護されたバージョン (HTTPS) を使用します。詳細については、「[Secure Sockets Layer \(SSL\) 通信の有効化](#)」(17 ページ)を参照してください。

- **リバース・プロキシ・アーキテクチャ**

より安全で推奨されるソリューションの1つは、リバース・プロキシを使用して HP Universal CMDB をデプロイすることです。HP Universal CMDB は安全なリバース・プロキシ・アーキテクチャを完全サポートしています。詳細については、「[リバース・プロキシの使用](#)」(36ページ)を参照してください。

システムのアクセス権

本章の内容

- [Java JMX Access の強化](#) 9
- [JMX コンソールのシステム・ユーザ名またはパスワードの変更](#) 11
- [HP Universal CMDB Server サービス・ユーザの変更](#) 12
- [Configuration Manager のデータベース・パスワードの暗号化](#) 14
- [Configuration Manager データベースのパスワード暗号化のためのパラメータ](#) 14

Java JMX Access の強化

注: ここに記載の手順は Data Flow Probe JMX にも使用できます。

ユーザ資格情報を提供する場合のみに JMX RMI ポートへのアクセスを可能にするには、次の手順を実行してください。

1. **C:\hp\UCMDB\UCMDBServer\bin**にあるサーバ上の **wrapper.conf** ファイルで次を設定します。

wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

この設定では、JMX が認証を要求する必要があります。

- **Data Flow Probe JMX** の場合は、次を実行します。

C:\hp\UCMDB\DataFlowProbe\binにある **WrapperGateway.conf** および **WrapperManager.conf** のファイルで次の設定を行います。

wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. ファイル **jmxremote.password.template** (場所:**C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) の名前を **jmxremote.password** に変更します。

注: Data Flow Probe JMX の場合、このファイルは次の場所にあります:**C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**。

3. **jmxremote.password** で **monitorRole** および **controlRole** の各ルールのパスワードを追加します。

例:

monitorRole QED

controlRole R&D

ではパスワード **QED** が **monitorRole** に、パスワード **R&D** が **controlRole** に割り当てられます。

注: パスワードがクリア・テキストで保存されますので、必ず所有者のみが **jmxremote.password** を読み書きする権限を持つようにしてください。ファイル所有者は、必ず UC MDB を実行しているユーザと同じでなければなりません。

4. **jmxremote.access** (場所:**C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) で **monitorRole** および **controlRole** にアクセス権を割り当てます。

例:

monitorRole readonly

controlRole readwrite

では読み取り専用アクセス権が **monitorRole** に、読み書きアクセス権が **controlRole** に割り当てられます。

注: Data Flow Probe JMX の場合、このファイルは次の場所にあります:**C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**。

5. ファイルは次のようにしてセキュアにします。
 - **Windows のみの場合:** コマンド・ラインから次のコマンドを実行してファイルをセキュアにします。

icacls jmxremote.password /grant Administrator:F

icacls jmxremote.access /grant Administrator:R

この場合、<ユーザ名> は両方のファイルのプロパティで確認できるファイル所有者です。これらのファイルのプロパティを開いて、内容が正しいことと、所有者が1人しかいないことを確認してください。

- **Solaris および Linux オペレーティング・システムの場合** : 次を実行してパスワードのファイル権限を設定します。

```
chmod 600 jmxremote.password
```

6. **サービス・パックのアップグレード、サーバ移行および障害回復の場合** : `jmxremote.access` (場所 `C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management\`) ファイルの所有権を、アップグレードまたは移行インストールを実行するオペレーティング・システムのユーザに変更します。

注:

- Data Flow Probe JMX の場合、このファイルは次の場所にあります:`C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management\`。
- 製品をアンインストールする前に、<UCMDB のインストール・フォルダ>`\bin\jre\lib\management\jmxremote.password` のファイル権限を編集して、ログインしているユーザが編集できるようにします。

JMX コンソールのシステム・ユーザ名またはパスワードの変更

JMX コンソールでは、複数顧客環境において顧客をまたがって有効であるユーザである、システム・ユーザが使用されます。JMX コンソールには、任意のシステム・ユーザ名でログインできます。標準設定の名前およびパスワードは `sysadmin/sysadmin` です。

パスワードは、JMX コンソールまたはサーバ管理ツールで変更できます。

JMX コンソールで標準設定のシステム・ユーザ名またはパスワードを変更するには、次の手順を実行します。

1. Web ブラウザを起動し、アドレスに `http://localhost.<ドメイン名>:8080/jmx-console` を入力します。
2. JMX コンソールの認証資格情報を入力します。
3. **UCMDB:service=Authorization Services** を見つけ、リンクをクリックして [操作] ページを開きます。
4. **resetPassword** 操作を見つめます。
 - [ユーザ名] フィールドに `sysadmin` を入力します。
 - [パスワード] フィールドに新しいパスワードを入力します。
5. [Invoke] をクリックして変更内容を保存します。

サーバ管理ツールで標準設定のシステム・ユーザ名またはパスワードを変更するには、次の手順を実行します。

1. **Windows の場合:** 次のファイルを実行します。 `C:\hp\UCMDB\UCMDBServer\tools\server_management.bat`
Linux の場合 : 次のフォルダにある `server_management.sh` を実行します。
`/opt/hp/UCMDB/UCMDBServer/tools/`
2. 次の認証資格情報を使用してツールにログインします。 `sysadmin/sysadmin`
3. [ユーザ] リンクをクリックします。
4. システム・ユーザを選択し、[ログオン ユーザのパスワードを変更] をクリックします。
5. 古いパスワードと新しいパスワードを入力し、[OK] をクリックします。

HP Universal CMDB Server サービス・ユーザの変更

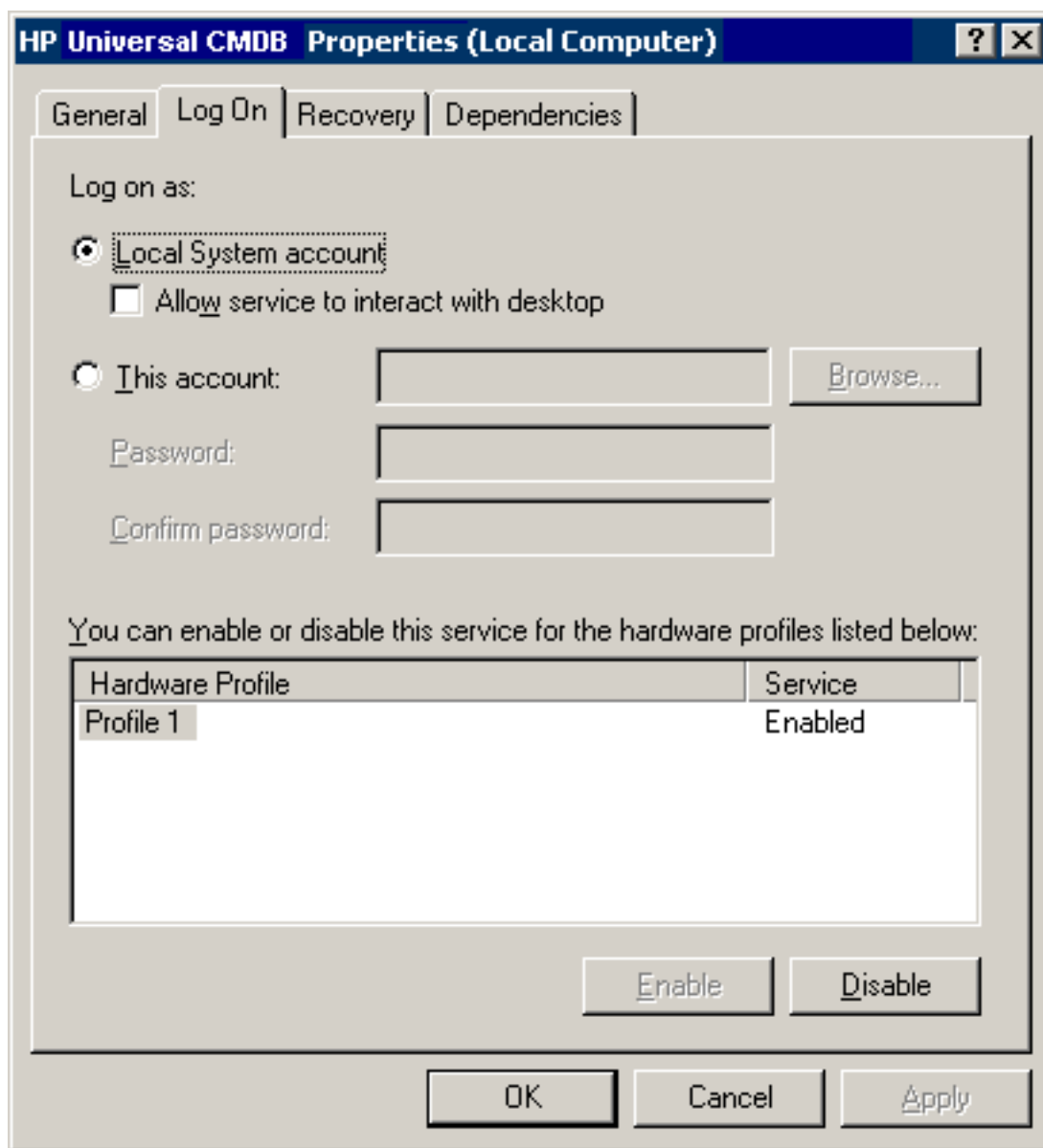
Windows プラットフォームでは、HP Universal CMDB サービス（すべての HP Universal CMDB サービスとプロセスを実行します）は、Server and Database Configuration ユーティリティの実行時にインストールされます。標準設定では、このサービスは local system ユーザのもとで実行されます。しかし、別のユーザがサービスを実行するように割り当てる必要がある場合があります（NTLM 認証を使用している場合など）。

サービスを実行するように割り当てるユーザは、次の権限を持っている必要があります。

- 十分なデータベース権限（データベース管理者によって定義されます）
- 十分なネットワーク権限
- ローカル・サーバでの管理者権限

サービス・ユーザを変更するには、次の手順を実行します。

1. [スタート] メニュー（[スタート] > [すべてのプログラム] > [HP UCMDB] > [HP Universal CMDB サーバの停止]）を使用するか、HP Universal CMDB サーバ・サービスを停止して HP Universal CMDB を無効にします。詳細については、『HP Universal CMDB 管理ガイド』で UCMDB サーバ・サービスの開始および停止方法について説明している項を参照してください。
2. Windows の [サービス] ウィンドウで、[UCMDB_Server] をダブルクリックします。[UCMDB Serverのプロパティ] ダイアログ・ボックスが開きます。
3. [ログオン] タブをクリックします。



4. **【アカウント】** を選択し、マシンで有効なユーザのリストから別のユーザを参照して選択します。
5. 選択したユーザの Windows パスワードを入力し、このパスワードを確認します。
6. **【適用】** をクリックして設定を保存し、**【OK】** をクリックしてダイアログ・ボックスを閉じます。
7. **【スタート】** メニュー（**【スタート】** > **【すべてのプログラム】** > **【HP UCMDB】** > **【HP Universal CMDB サーバの開始】**）を使用するか、HP Universal CMDB サーバ・サービスを開始して HP Universal CMDB を有効にします。詳細については、『HP Universal CMDB 管理ガイド』で UCMDB サーバ・サービスの開始および停止方法について説明している項を参照してください。

Configuration Manager のデータベース・パスワードの暗号化

CM のデータベース・パスワードは、**<Configuration Manager のインストール・ディレクトリ>\conf\database.properties** ファイルに保存されます。パスワードを暗号化する場合、デフォルトの暗号化アルゴリズムは FIPS 140-2 の基準に準拠します。

暗号化はキーを用いて行われ、このキーを通してパスワードが暗号化されます。そして、キー自体もマスタ・キーと呼ばれる別のキーを使用して暗号化されます。いずれのキーも、同じアルゴリズムによって暗号化されます。暗号化プロセスで使用されるパラメータの詳細については、「[Configuration Manager データベースのパスワード暗号化のためのパラメータ](#)」(14ページ)を参照してください。

注意: 暗号化アルゴリズムを変更すると、これまでに暗号化されたパスワードはすべて使用できなくなります。

データベース・パスワードの暗号化を変更するには、次の手順を実行します。

1. **<Configuration Manager のインストール・ディレクトリ>\conf\database.properties** ファイルを開き、次のフィールドを編集します。
 - **engineName** : 暗号化アルゴリズムの名前を入力します。
 - **keySize** : 選択したアルゴリズムのマスタ・キーのサイズを入力します。
2. **generate-keys.bat** スクリプトを実行して **<Configuration Manager のインストール・ディレクトリ>\security\encrypt_repository** ファイルを作成して、暗号鍵を生成します。
3. **bin\encrypt-password.bat** ユーティリティを実行してパスワードを暗号化します。-h フラグを設定して利用可能なオプションを確認します。
4. パスワード暗号化ユーティリティの結果をコピーして **conf\database.properties** ファイルに結果の暗号化を貼り付けます。

Configuration Manager データベースのパスワード暗号化のためのパラメータ

次のテーブルに、CM データベースのパスワード暗号化に使用する**encryption.properties** ファイルに含まれるパラメータの一覧を示します。データベースのパスワード暗号化の詳細については、「[Configuration Manager のデータベース・パスワードの暗号化](#)」(14ページ)を参照してください。

パラメータ	詳細
cryptoSource	暗号化アルゴリズムを実装するインフラストラクチャを示します。次のオプションを使用できます。

パラメータ	詳細
	<ul style="list-style-type: none"> • lw。 [Uses Bouncy Castle lightweight implementation] (標準設定) • jce。 [Java Cryptography Enhancement] (標準 Java 暗号化方式インフラストラクチャ)
storageType	<p>キー保存のタイプを示します。</p> <p>現在は、バイナリ・ファイルのみがサポートされています。</p>
binaryFileStorageName	<p>マスタ・キーが保存されているファイル内の場所を示します。</p>
cipherType	<p>暗号化のタイプです。現在は、symmetricBlockCipherのみがサポートされています。</p>
engineName	<p>暗号化アルゴリズムの名前です。</p> <p>次のオプションを利用できます。</p> <ul style="list-style-type: none"> • AES。 American Encryption Standard。 この暗号化は FIPS 140-2 に準拠しています。(標準設定) • Blowfish • DES • 3DES。(FIPS 140-2 準拠) • Null。 暗号化なし
keySize	<p>マスタ・キーのサイズです。サイズは次のアルゴリズムによって決定されます。</p> <ul style="list-style-type: none"> • AES。 128, 192 または 256 (標準設定は 256) • Blowfish。 0-400 • DES。 56 • 3DES。 156
encodingMode	<p>バイナリ暗号化結果の ASCII エンコーディング。</p> <p>次のオプションを利用できます。</p> <ul style="list-style-type: none"> • Base64 (標準設定) • Base64Url • Hex
algorithmModeName	<p>アルゴリズムのモードです。現在は、CBCのみがサポートされています。</p>
algorithmPaddingName	<p>使用するパディング・アルゴリズムです。</p> <p>次のオプションを利用できます。</p>

パラメータ	詳細
	<ul style="list-style-type: none">• PKCS7Padding (標準設定)• PKCS5Padding
jceProviderName	JCE 暗号化アルゴリズムの名前です。 注: cryptSource が jce の場合のみ該当します。lw の場合は engineName が使用されます。

第2章: Secure Sockets Layer (SSL) 通信の有効化

本章の内容

- 自己署名証明書を使ったサーバ・マシンの SSL 有効化 - UCMDB 17
- 自己署名証明書を使ったサーバ・マシンの SSL 有効化 - Configuration Manager 19
- 認証局から取得した証明書を使ったサーバ・マシンの SSL 有効化 - UCMDB 20
- 認証局から取得した証明書を使ったサーバ・マシンの SSL 有効化 - Configuration Manager 22
- クライアント・マシンでの SSL の有効化 - UCMDB 23
- クライアント証明書で SSL を有効化 - Configuration Manager 24
- クライアント SDK での SSL の有効化 25
- SDK の相互証明書認証の有効化 25
- UCMDB での CAC (スマート・カード/PKI 認証) サポートの設定 27
- サーバ・キー・ストアのパスワードの変更 29
- HTTP/HTTPS ポートの有効化と無効化 30
- UCMDB Web コンポーネントのポートへのマップ 31
- SSL を使用して UCMDB の作業を行うための Configuration Manager の設定 32
- SSL で使用する UCMDB KPI アダプタの有効化 34
- UCMDB Browser の SSL サポートの構成 35

自己署名証明書を使ったサーバ・マシンの SSL 有効化 - UCMDB

本項では、Secure Sockets Layer (SSL) チャネルを使用した通信をサポートするよう HP Universal CMDB を設定する方法について説明します。

1. 前提条件

- a. 次の手順を開始する前に、**C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore** にある古い **server.keystore** を削除してください。
- b. HP Universal CMDB キーストア (JKS タイプ) を **C:\hp\UCMDB\UCMDBServer\conf\security** フォルダに置きます。

2. サーバ・キーストアの生成

a. 自己署名証明書および一致する秘密鍵を使用してキーストア (JKS タイプ) を作成します。

- **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** から次のコマンドを実行します。

```
keytool -genkey -alias hpcert -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

コンソール・ダイアログ・ボックスが開きます。

- キーストアのパスワードを入力します。パスワードが変更された場合は、**UCMDB:service=Security Services** で JMX 操作 **changeKeystorePassword** を実行します。パスワードが変更されていない場合、標準設定のパスワード **hppass** を使用します。
- 「**What is your first and last name?**」という質問に回答します。HP Universal C MDB の Web サーバ名を入力します。所属する組織に応じて、ほかのパラメータを入力します。
- キーのパスワードを入力します。キーのパスワードは、キーストアのパスワードと一致する必要があります。

JKS キーストアが **server.keystore** という名前で、**hpcert** という名前のサーバ証明書とともに作成されます。

b. 自己署名証明書をファイルにエクスポートします。

C:\hp\UCMDB\UCMDBServer\bin\jre\bin から次のコマンドを実行します。

```
keytool -export -alias hpcert -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <your password> -file  
hpcert
```

3. クライアントのトラスト・ストアへの証明書の配置

server.keystore を生成してサーバ証明書をエクスポートした後、自己署名証明書を使用して HP Universal C MDB と SSL 通信をする必要のあるすべてのクライアントで、この証明書をクライアントのトラスト・ストアに配置します。

注: **server.keystore** でのみ、サーバ証明書を1つ持つことができます。

4. HTTP ポート 8080 の無効化

詳細については、「[HTTP/HTTPS ポートの有効化と無効化](#)」(30ページ)を参照してください。

注: HTTP ポートを閉じる前に、HTTPS 通信が動作していることを確認します。

5. サーバの再起動

6. HP Universal C MDB の表示

UCMDB サーバがセキュアであることを確認するには、Web ブラウザに次の URL を入力します
:https://<UCMDB サーバ名または IP アドレス>:8443/ucmdb-ui

自己署名証明書を使ったサーバ・マシンのSSL有効化 - Configuration Manager

本項では、Secure Sockets Layer (SSL) チャネルを使用した認証および暗号化をサポートするよう Configuration Manager を設定する方法について説明します。

Configuration Manager では Tomcat 7.0.19 がアプリケーション・サーバとして使用されます。

1. 前提条件 (初回インストール時は関連しません)

次の手順を開始する前に、<Configuration Manager のインストール・ディレクトリ>\java\windows\x86_64\lib\security\ フォルダまたは<Configuration Manager のインストール・ディレクトリ>\java\linux\x86_64\lib\security\ フォルダ (いずれか関連するほう) に古い tomcat.keystore ファイルがあれば削除します。

2. サーバ・キーストアの生成

自己署名証明書および一致する秘密鍵を使用してキーストア (JKS タイプ) を作成します。

- <Configuration Manager のインストール・ディレクトリ>\java\windows\x86_64\bin または <Configuration Manager のインストール・ディレクトリ>\java\linux\x86_64\bin から、次のコマンドを実行します。

```
keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\security\tomcat.keystore
```

コンソール・ダイアログ・ボックスが開きます。

- キーストアのパスワードを入力します。パスワードが変更されている場合はファイル内で手動で変更します。
- 「What is your first and last name?」という質問に回答します。Configuration Manager の Web サーバ名を入力します。所属する組織に応じて、ほかのパラメータを入力します。
- キーのパスワードを入力します。キーのパスワードは、キーストアのパスワードと一致する必要があります。
JKS キーストアが tomcat.keystore という名前で、hpcert という名前のサーバ証明書とともに作成されます。

3. クライアントのトラスト・ストアへの証明書の配置

使用しているコンピュータの Internet Explorer 内のクライアントの信頼済みストアに証明書を追加します ([ツール] > [インターネット オプション] > [コンテンツ] > [証明書])。これを行わないと、最初に Configuration Manager を使用しようとしたときに証明書を追加するよう要求されます。

制限事項 :tomcat.keystore でのみ、サーバ証明書を1つ持つことができます。

4. server.xml ファイルの修正

<Configuration Manager のインストール・ディレクトリ>\servers\server-0\conf にある server.xml ファイルを開きます。次で始まるセクションを見つけます。

```
Connector port="8143"
```

これはコメントに表示されます。コメント文字を削除してスクリプトをアクティブ化し、次の属性を HTTPS 接続に追加します。

```
keystoreFile="<tomcat.keystore file location>" (ステップ2参照)
```

```
keystorePass="<password>"
```

次のラインをコメント・アウトします。

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
```

注: HTTP 接続ポートをブロックしないでください。HTTP 通信をブロックしたい場合は、ファイアウォールが使用できます。

5. サーバの再起動

Configuration Manager のサーバを再起動します。

6. サーバ・セキュリティの確認

Configuration Manager のサーバがセキュアであることを確認するには、Web ブラウザに次の URL を入力します :**https://<Configuration Manager サーバの名前または IP アドレス>:8143/cnc**。

7. Configuration Manger で、**【設定】 > 【アプリケーション管理】 > 【メール設定】** に移動して、前述の値に従って **【Configuration Manager の完全な URL】** のプロトコルおよびポートを変更します。

8. UCMDB で、**【インフラストラクチャ設定マネージャ】 > 【全般設定】** に移動して、前述の値に従って **【構成マネージャ URL】** のプロトコルおよびポートを変更します。

ヒント: 接続を確立できない場合は、別のブラウザを使用してみるかブラウザのバージョンを更新してみてください。

認証局から取得した証明書を使ったサーバ・マシンの SSL 有効化 - UCMDB

認証局 (CA) が発行した証明書を使用するには、キーストアが Java 形式である必要があります。次の例を使って、Windows マシンでキーストアをフォーマットする方法を説明します。

1. 前提条件

次の手順を開始する前に、**C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore** にある古い **server.keystore** を削除してください。

2. サーバ・キーストアの生成

- a. 認証局署名証明書を生成して、Windows にインストールします。
- b. Microsoft 管理コンソール (**mmc.exe**) を使って、証明書を ***.pfx** ファイルに (秘密鍵を含めて) エクスポートします。

pfx ファイルのパスワードとして任意の文字列を入力します (キーストアのタイプを **JAVA** キーストアに変換するとき、このパスワードを入力する必要があります)。これで **.pfx** ファイルには公開証明書と秘密鍵が含まれ、パスワードで保護されます。

- c. 作成した **.pfx** ファイルを次のフォルダにコピーします
:C:\hp\UCMDB\UCMDBServer\conf\security。
- d. コマンド・プロンプトを開いて、ディレクトリを **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** に変更します。

次のコマンドを実行して、キーストアのタイプを **PKCS12** から **JAVA** キーストアに変更します。

```
keytool -importkeystore -srckeystore c:\hp\UCMDB\UCMDBServer\conf\security\
```

ソース (**.pfx**) キーストアのパスワードを入力するメッセージが表示されます。このパスワードは、手順 **b** で **pfx** ファイルを作成したときに指定したものです。

- e. 変換先キーストアのパスワードを入力します。ここでは、セキュリティ・サービスで **JMX** メソッド **changeKeystorePassword** に先ほど定義したものと同一パスワードを使う必要があります。パスワードが変更されていない場合、標準設定のパスワード **hppass** を使用します。

注: ソース・キーストアのパスワードは、変換先キーストアのパスワードと一致する必要があります。

- f. 証明書を生成した後、HTTP ポート 8080 を無効にします。詳細については、[「HTTP/HTTPS ポートの有効化と無効化」 \(30ページ\)](#)を参照してください。
- g. **hppass** または **.pfx** ファイルで使ったパスワード以外のパスワードを使用した場合、**JMX** メソッド **changeKeystorePassword** を実行して、キーが同じパスワードを持つようにします。

注: HTTP ポートを閉じる前に、HTTPS 通信が動作していることを確認します。

3. サーバの再起動

4. サーバ・セキュリティの確認

UCMDB サーバがセキュアであることを確認するには、Web ブラウザに次の URL を入力します
:https://<UCMDB サーバ名または IP アドレス>:8443/ucmdb-ui

注意: **server.keystore** でのみ、サーバ証明書を 1 つ持つことができます。

認証局から取得した証明書を使ったサーバ・マシンの SSL 有効化 - Configuration Manager

Configuration Manager の場合、認証局 (CA) が発行した証明書を使用するには、キーストアが Java 形式である必要があります。次の例を使って、Windows マシンでキーストアをフォーマットする方法を説明します。

1. 前提条件

次の手順を開始する前に、**<Configuration Manager のインストール・ディレクトリ>\java\windows\x86_64\lib\security** フォルダまたは **<Configuration Manager のインストール・ディレクトリ>\java\linux\x86_64\lib\security** フォルダ (いずれか関連するほう) に古い **tomcat.keystore** ファイルがあれば削除します。

2. サーバ・キーストアの生成

- a. 認証局署名証明書を生成して、Windows にインストールします。
- b. Microsoft 管理コンソール (**mmc.exe**) を使って、証明書を ***.pfx** ファイルに (秘密鍵を含めて) エクスポートします。

pfx ファイルのパスワードとして任意の文字列を入力します (キーストアのタイプを JAVA キーストアに変換するとき、このパスワードを入力する必要があります)。

これで **.pfx** ファイルには公開証明書と秘密鍵が含まれ、パスワードで保護されます。

作成した **.pfx** ファイルを次のフォルダにコピーします : **<Configuration Manager のインストール・ディレクトリ>\java\windows\x86_64\lib\security**。

- c. コマンド・プロンプトを開き、ディレクトリを **<Configuration Manager のインストール・ディレクトリ>\java\bin** に変更します。

次のコマンドを実行して、キーストアのタイプを **PKCS12** から **JAVA** キーストアに変更します。

```
keytool -importkeystore -srckeystore <Configuration Manager のインストール・ディレクトリ>\conf\security\
```

ソース (**.pfx**) キーストアのパスワードを入力するメッセージが表示されます。このパスワードは、手順 b で **pfx** ファイルを作成したときに指定したものです。

3. server.xml ファイルの変更

<Configuration Manager のインストール・ディレクトリ>\servers\server-0\conf にある **server.xml** ファイルを開きます。次で始まるセクションを見つけます。

```
Connector port="8143"
```

これはコメントに表示されます。コメント文字を削除してスクリプトをアクティブ化し、次のラインを追加します。

```
keystoreFile="../../java/lib/security/tomcat.keystore"  
keystorePass="password" />
```

次のラインをコメント・アウトします。

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
```

注: HTTP 接続ポートをブロックしないでください。HTTP 通信をブロックしたい場合は、ファイアウォールが使用できます。

4. サーバの再起動

Configuration Manager のサーバを再起動します。

5. サーバ・セキュリティの確認

Configuration Manager のサーバがセキュアであることを確認するには、Web ブラウザに次の URL を入力します :**https://<Configuration Manager のサーバの名前または IP アドレス>:8143/cnc**。

6. Configuration Manger で、【設定】>【アプリケーション管理】>【メール設定】に移動して、前述の値に従って【Configuration Manager の完全な URL】のプロトコルおよびポートを変更します。
7. UCMDB で、【インフラストラクチャ設定マネージャ】>【全般設定】に移動して、前述の値に従って【構成マネージャ URL】のプロトコルおよびポートを変更します。

制限事項 : tomcat.keystore でのみ、サーバ証明書を1つ持つことができます。

クライアント・マシンでの SSL の有効化 - UCMDB

HP Universal CMDB Web サーバによって使用されている証明書が良く知られている認証局 (CA) で発行されたものである場合、使用している Web ブラウザは特別なアクションを行わずに検証することができます。

認証局が Web ブラウザに信頼されていない場合は、証明書のトラスト・パス全体または HP Universal CMDB によって使用されている証明書を、ブラウザのトラスト・ストアに明示的にインポートする必要があります。

次の例では、自己署名 **hpcert** 証明書を Windows のトラスト・ストアにインポートして、Internet Explorer で使用できるようにする方法について説明します。

証明書を Windows のトラスト・ストアにインポートするには、次の手順を実行します。

1. **hpcert** 証明書を **hpcert.cer** という名前に変更します。

Windows Explorer に、ファイルがセキュリティ証明書であることを示すアイコンが表示されません。

2. **hpcert.cer** をダブルクリックして、Internet Explorer の [証明書] ダイアログ・ボックスを開きます。
3. Certificate Import Wizard で証明書をインストールすることによってトラストを有効にするための指示に従います。

注: UCMDB サーバが発行した証明書を Web ブラウザにインポートするには、別の方法もあります。これには、まず UCMDB にログインし、信頼されていない証明書であるという警告が表示されたときに証明書をインストールします。

クライアント証明書で SSL を有効化 - Configuration Manager

Configuration Manager Web サーバによって使用されている証明書が良く知られている認証局 (CA) で発行されたものである場合は、使用している Web ブラウザは特別なアクションを行わずに検証することができます。

CA がサーバ・トラスト・ストアによって信頼されていない場合は、CA 証明書をサーバ・トラスト・ストアにインポートします。

次の例では、自己署名 **hpcert** 証明書をサーバ・トラスト・ストア (cacerts) にインポートする方法について説明します。

証明書をサーバ・トラスト・ストアにインポートするには、次の手順を実行します。

1. クライアント・マシン上で **hpcert** 証明書を見つけ、名前を **hpcert.cer** に変更します。
2. **hpcert.cer** を <Configuration Manager_インストール_ディレクトリ>\java\windows\x86_64\bin フォルダにあるサーバ・マシンにコピーします。
3. 次のコマンドによりキーツール・ユーティリティを使用して、サーバ・マシン上で CA 証明書をトラスト・ストア (cacerts) にインポートします。

```
<Configuration Manager のインストール・ディレクトリ>\java\bin\keytool.exe -import  
-alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
```

4. (<Configuration Manager のインストール・ディレクトリ>\servers\server-0\conf フォルダにある) **server.xml** ファイルを、次のとおり変更します。
 - a. 「[server.xml ファイルの変更](#)」(22ページ)で説明している変更を行います。
 - b. これらの変更後すぐに、次の属性を HTTPS コネクタに追加します。

```
truststoreFile="../../java/lib/security/cacerts"  
truststorePass="changeit" />
```
 - c. `clientAuth="true"` を設定します。
5. 「[サーバ・セキュリティの確認](#)」(23ページ)の説明に従ってサーバ・セキュリティを確認します。

クライアント SDK での SSL の有効化

クライアント SDK とサーバ SDK の間では、HTTPS 通信を利用することができます。

1. クライアント・マシンで、クライアント SDK を埋め込んだ製品から通信設定を開き、HTTP ではなく HTTPS を使うよう設定します。
2. 認証局署名証明書または自己署名証明書をクライアント・マシンにダウンロードし、サーバに接続する JRE の **cacerts** トラスト・ストアにインポートします。

次のコマンドを使います。

```
Keytool -import -alias <CA 名> -trustcacerts -file <サーバの公開証明書のパス> -keystore <クライアント JRE の信頼済み cacerts ストアのパス (x:\program files\java\jre\lib\security\cacerts など) >
```

SDK の相互証明書認証の有効化

このモードでは SSL を使用し、UCMDB によるサーバ認証と UCMDB-API クライアントによるクライアント認証の両方を有効化します。サーバおよび UCMDB-API クライアントはどちらも、認証のためにほかのエンティティに証明書を送信します。

注: SDK で SSL を使用して相互認証を有効化する次の方法は、最も安全で、推奨される通信モードです。

1. UCMDB の UCMDB-API クライアント・コネクタのセキュリティを強化します。
 - a. UCMDB JMX コンソールにアクセスします。Web ブラウザを起動し、アドレスに「**http://<UCMDB マシンの名前または IP アドレス>:8080/jmx-console**」と入力します。ユーザ名とパスワードを使用してログインする必要がある場合もあります（標準設定は `sysadmin/sysadmin`）。
 - b. **UCMDB:service=Ports Management Services** を見つけ、リンクをクリックして [操作] ページを開きます。
 - c. **PortsDetails** 操作を見つて、[Invoke] をクリックします。クライアント認証に使用する HTTPS のポート番号を記録します。標準設定は 8444 で、有効になっている必要があります。
 - d. [操作] ページに戻ります。
 - e. `ucmdb-api` コネクタを相互認証モードにマップするには、次のパラメータを指定して **mapComponentToConnectors** メソッドを呼び出します。
 - `componentName:ucmdb-api`
 - `isHTTPSWithClientAuth: true`
 - ほかのすべてのフラグ: `false`

次のメッセージが表示されます。

Operation succeeded.ucmdb-api コンポーネントは、現在次のポートにマップされています
:HTTPS_CLIENT_AUTH ポート。

- f. [操作] ページに戻ります。
2. **ping** コンポーネントに対して**手順 1** を繰り返します。
3. UCMDB-API クライアントを実行する JRE に、クライアント証明書を含むキー・ストアがあることを確認します。
4. キー・ストアから UCMDB-API クライアント証明書をエクスポートします。
5. エクスポートした UCMDB-API クライアント証明書を UCMDB サーバのトラスト・ストアにインポートします。
 - a. UCMDB マシンで、作成した UCMDB-API クライアント証明書ファイルを UCMDB の次のディレクトリにコピーします。
C:\HP\UCMDB\UCMDBServer\conf\security
 - b. 次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <エクスポートされた  
UCMDB-API クライアント証明書> -alias ucmdb-api
```
 - c. UCMDB サーバのトラスト・ストア・パスワード（標準設定は **hppass**）を入力します。
 - d. **[Trust this certificate?]** と表示された場合は、**[y]** を押して **Enter** キーを押します。
 - e. 出力が **[証明書がキー・ストアに追加されました]** であることを確認します。
6. サーバ・キー・ストアから UCMDB サーバ証明書をエクスポートします。
 - a. UCMDB マシンで、次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert  
-keystore  
C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore  
-file C:\HP\UCMDB\conf\security\server.cert
```
 - b. UCMDB サーバのトラスト・ストア・パスワード（標準設定は **hppass**）を入力します。
 - c. 証明書が次のディレクトリに作成されていることを確認します。
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
7. エクスポートした UCMDB 証明書を UCMDB-API クライアントのトラスト・ストアの JRE にインポートします。
8. API クライアントによって使用される証明書は、その **[共通名 (CN)]** フィールドに UCMDB に存在するユーザの名前を含んでいる必要があります。

このユーザはパスワードは空で、SDK アクセスのための必要な権限をすべて持っている必要があります。

既存の UCMDB ユーザに空のパスワードを設定するには、次の手順を実行します。

- a. **JMX コンソール > UCMDB:service=URM Services > listResourceTypes** の順に移動します。
 - b. **Auth_USER** をクリックします。
 - c. 該当ユーザをクリックして、ロードする XML を待機します。
 - d. XML で、パスワードを **s39t30*tfoZXg30xd/nvJGL5is8=** で置き換えます。
 - e. **[リソースの保存]** をクリックします。
9. UCMDB サーバおよび UCMDB-API クライアントを再起動します。
 10. UCMDB-API クライアントから UCMDB-API サーバに接続するには、次のコードを使用します。

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
(default:8444>));
UcmdbService ucmdbService = provider.connect(provider.createCertificateCredentials(<TheClientKeystore.
e.g:"c:\\client.keystore">, <KeystorePassword>), provider.createClientContext(<ClientIdentification>));
```

UCMDB での CAC (スマート・カード/PKI 認証) サポートの設定

本項では、UCMDB にスマート・カード認証または PKI 認証 (CAC) サポートを設定する方法について説明します。

注: CAC サポートは、Internet Explorer 8, 9, または 10 を使用している場合にのみ利用できません。

1. 次のように、ルート CA および中間証明書を UCMDB サーバのトラスト・ストアにインポートします。
 - a. UCMDB マシンで、証明書ファイルを UCMDB の次のディレクトリにコピーします。

C:\HP\UCMDB\UCMDBServer\conf\security

注: 証明書が Microsoft p7b 形式の場合、PEM 形式に変換する必要が生じる場合があります。

- b. 各証明書について、次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file
<証明書> -alias <証明書エイリアス>
```
 - c. UCMDB サーバのトラスト・ストア・パスワード (標準設定は **hppass**) を入力します。
 - d. **[Trust this certificate?]** と表示された場合は、**[y]** を押して **Enter** キーを押します。
 - e. 出力が **[証明書がキー・ストアに追加されました]** であることを確認します。
2. Web ブラウザを起動して、次のとおりサーバ・アドレスを入力することによって、JMX コン

ソールを開きます。http://<UCMDB サーバ・ホスト名または IP>:8080/jmx-console
ユーザ名とパスワードを使用してログインする必要がある場合もあります。

3. UCMDB で、**UCMDB:service=Ports Management Services** をクリックして [操作] ページを開きます。
 - (任意) [**ComponentsConfigurations**] をクリックします。次の操作を実行します。
 - **HTTPSSetPort** を **8444** に設定して、[**Invoke**] をクリックします。
 - [**Back to MBean**] をクリックします。
 - [**mapComponentToConnectors**] をクリックします。次の操作を実行します。
 - mapComponentToConnectors サービスで、**componentName** を **ucmdb-ui** に設定します。
 - **isHTTPSWithClientAuth** のみを **true** に設定して、[**Invoke**] をクリックします。
 - [**Back to MBean**] をクリックします。
 - mapComponentToConnectors サービスで、**componentName** を **root** に設定します。
 - **isHTTPSWithClientAuth** のみを **true** に設定して、[**Invoke**] をクリックします。
4. UCMDB で、**UCMDB:service=Security Services** をクリックして [操作] ページを開きます。**loginWithCAC** サービスで、次の手順を実行します。
 - **loginWithCAC** を **true** に設定して、[**Invoke**] をクリックします。
 - [**Back to MBean**] をクリックします。
 - (任意) **usernameField** をクリックして、UCMDB がユーザ名の抽出に使用するフィールドを証明書内から指定し、[**Invoke**] をクリックします。

注: フィールドを指定しない場合、標準設定の PRINCIPAL_NAME_FROM_SAN_FIELD が使用されます。

- [**Back to MBean**] をクリックします。
- **pathToCRL** をクリックして、(証明書にある) オンライン・リストが使用できない場合に使用されるオフライン証明書執行リスト (CRL) へのパスを設定して、[**Invoke**] をクリックします。

注: ローカル CRL で作業しており、UCMDB サーバへの動作中のインターネット接続がある場合は、ローカル CRL が使用されます。証明書の検証は、(無効になっていない場合でも) 次のような状況では失敗します。

- CRL パスが設定されているが、CRL ファイル自体がない
- CRL の期限が切れている
- CRL に不正な署名がある

パスをオフライン CRL に設定せず、UCMDB サーバでオンライン CRL にアクセスできない場合には、(URL にアクセスできず、無効化のチェックが失敗するため) CRL または OCSP URL を含むすべての証明書が拒否されます。UCMDB サーバでインターネット・アクセスを利用できるようにするには、**wrapper.conf** ファイルで次の行のコメントを解除し、有効なプロキシとポートを設定します。

```
#wrapper.java.additional.40=-Dhttp.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.41=-Dhttp.proxyPort=<ポート>
#wrapper.java.additional.42=-Dhttps.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.43=-Dhttps.proxyPort=<ポート>
```

- **[Back to MBean]** をクリックします。
- (任意) **onlyCACerts** を **true** に設定して、**[Invoke]** をクリックします。
この操作を **true** に設定して、物理 CAC デバイスからの証明書のみを受け入れるようにします。

`https://<UCMDB サーバのホスト名または IP>.<ドメイン名>:8444` で UCMDB にログインできるようになりました。

5. UCMDB を LW-SSO 認証を使用するように設定して、UCMDB サーバを再起動します。

LW-SSO 認証の詳細については、[「HP Universal CMDB への LW-SSO によるログインを有効化」\(96 ページ\)](#)を参照してください。

サーバ・キー・ストアのパスワードの変更

サーバをインストールすると、HTTPS ポートが開き、弱いパスワード (標準設定の **hppass**) でストアが保護されます。SSL のみを使用する場合は、パスワードを変更する必要があります。

次に、**server.keystore** パスワードだけを変更する方法について説明します。ただし、**server.truststore** パスワードの変更でも同じ手順を実行します。

注: この操作ではすべての手順を実行する必要があります。

1. UCMDB サーバを開始します。
2. JMX コンソールでパスワード変更を実行します。
 - a. Web ブラウザを起動して、次のサーバ・アドレスを入力します :`http://<UCMDB サーバのホスト名または IP>:8080/jmx-console`。
ユーザ名とパスワードを使用してログインする必要がある場合もあります。
 - b. UCMDB で、**UCMDB:service=Security Services** をクリックして [操作] ページを開きます。
 - c. **changeKeystorePassword** 操作を実行します。

このフィールドは空白にすることはできません。少なくとも 6 文字以上の長さである必要があります。パスワードはデータベースのみで変更されます。

- UCMDB サーバを停止します。
- コマンドを実行します。

C:\hp\UCMDB\UCMDBServer\bin\jre\bin から次のコマンドを実行します。

- ストアのパスワードを変更します。

keytool -storepasswd -new <新しいキーストアのパスワード> -keystore

C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <現在のキーストアのパスワード>

- 次のコマンドで、キーストアの内部キーを表示します。最初のパラメータはエイリアスです。次のコマンドで必要なので、このパラメータを保存しておいてください。

keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

- (ストアが空ではない場合) キーのパスワードを変更します。

keytool -keypasswd -alias <別名> -keypass <現在のパスワード> -new <新しいパスワード> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

- 新しいパスワードを入力します。
- UCMDB サーバを開始します。
- サーバのトラスト・ストアでこの手順を繰り返します。

HTTP/HTTPS ポートの有効化と無効化

ユーザ・インタフェースまたは JMX コンソールから HTTP ポートおよび HTTPS ポートを有効化 / 無効化できます。

ユーザ・インタフェースから HTTP ポートまたは HTTPS ポートを有効化 / 無効化するには、次の手順を実行します。

- HP Universal CMDB にログオンします。
- 【管理】 > 【インフラストラクチャ設定】** を選択します。
- 【フィルタ】** (名前を使用) ボックスで **http** または **https** を入力して、HTTP 設定を表示します。
 - HTTP 接続を有効化 :True の場合** :ポートは有効になっています。**False の場合** :ポートは無効になっています。
- サーバを再起動して、変更を適用します。

注意: HTTPS ポートは標準設定で開いています。このポートを閉じると、**Server_Management.bat** が動作しなくなります。

JMX コンソールから HTTP ポートまたは HTTPS ポートを有効化 / 無効化するには、次の手順を実行します。

1. Web ブラウザを起動し、アドレスに `http://localhost.<ドメイン名>:8080/jmx-console` を入力します。
2. JMX コンソールの認証資格情報を入力します。標準設定の資格情報は次のとおりです。
 - ログイン名 = **sysadmin**
 - パスワード = **sysadmin**
3. **UCMDB:service=Ports Management Services** を見つけ、リンクをクリックして [操作] ページを開きます。
4. HTTP ポートを有効化 / 無効化するには、**HTTPSetEnable** 操作を見つて、値を設定します。
 - **True にすると**、ポートは有効になっています。
 - **False にすると**、ポートは無効になっています。
5. HTTPS ポートを有効化 / 無効化するには、**HTTPSSetEnable** 操作を見つて、値を設定します。
 - **True にすると**、ポートは有効になっています。
 - **False の場合** :ポートは無効になっています。
6. クライアント認証を使用して HTTPS ポートを有効化 / 無効化するには、**HTTPSClientAuthSetEnable** 操作を見つて、値を設定します。
 - **True にすると**、ポートは有効になっています。
 - **False にすると**、ポートは無効になっています。

UCMDB Web コンポーネントのポートへのマップ

各 UCMDB コンポーネントで、JMX コンソールから利用可能なポートへのマップを設定できます。

現在のコンポーネント設定を表示するには、次の手順を実行します。

1. Web ブラウザを起動し、アドレスに `http://localhost.<ドメイン名>:8080/jmx-console` を入力します。
2. JMX コンソールの認証資格情報を入力します。標準設定の資格情報は次のとおりです。
 - ログイン名 = **sysadmin**
 - パスワード = **sysadmin**
3. **UCMDB:service=Ports Management Services** を見つけ、リンクをクリックして [操作] ページを開きます。

4. **ComponentsConfigurations** メソッドを見つけ、**[Invoke]** をクリックします。
5. コンポーネントごとに、有効なポートおよび現在マップされているポートが表示されます。

コンポーネントをマップするには、次の手順を実行します。

1. **UCMDB:service=Ports Management Services** を見つけ、リンクをクリックして **[操作]** ページを開きます。
2. **mapComponentToConnectors** メソッドを見つけます。
3. **[値]** ボックスにコンポーネントの名前を入力します。選択項目に対応するポートごとに **[True]** または **[False]** を選択します。 **[Invoke]** をクリックします。選択したコンポーネントが選択したポートにマップされます。 **serverComponentsNames** メソッドを呼び出して、コンポーネント名を検索できます。
4. 関連するコンポーネントごとにこのプロセスを繰り返します。

注:

- すべてのコンポーネントを少なくとも1つのポートにマップする必要があります。コンポーネントをどのポートにもマップしない場合は、標準設定でHTTPポートにマップされます。
- クライアント認証を使用してHTTPポートとHTTPSポートの両方にコンポーネントをマップすると、クライアント認証オプションのみがマップされます（この場合、ほかのオプションは無視されます）。
- UCMDB UI コンポーネントで **isHTTPSWithClientAuth** を **True** に設定する場合、ルート・コンポーネントでも **True** に設定する必要があります。

また、各ポートに割り当てる値を変更することもできます。

ポートの値を設定するには、次の手順を実行します。

1. **UCMDB:service=Ports Management Services** を見つけ、リンクをクリックして **[操作]** ページを開きます。
2. HTTPポートの値を設定するには、**HTTPSetPort** メソッドを見つけ、**[値]** ボックスに値を入力します。 **[Invoke]** をクリックします。
3. HTTPSポートの値を設定するには、**HTTPSSetPort** メソッドを見つけ、**[値]** ボックスに値を入力します。 **[Invoke]** をクリックします。
4. クライアント認証を使用してHTTPSポートの値を設定するには、**HTTPSClientAuthSetPort** メソッドを見つけ、**[値]** ボックスに値を入力します。 **[Invoke]** をクリックします。

SSL を使用して UCMDB の作業を行うための Configuration Manager の設定

SSL (Secure Sockets Layer) を使用して UCMDB の作業を行うために Configuration Manager の設定を行うことができます。ポート 8443 の SSL コネクタは UCMDB の標準設定で有効化されています。

1. **<UCMDB インストール・ディレクトリ>\bin\jre\bin** に移動して次のコマンドを実行します。

```
keytool -export -alias hpcert -keystore <UCMDB_サーバ_ディレクトリ>\conf\security\server.keystore -storepass hppass -file <証明書ファイル>
```
2. 証明書ファイルをローカル Configuration Manager マシンの一時ロケーションにコピーします。
3. 新しいインストールを実施するか、既存の Configuration Manager のインストールを再設定します。その方法については、対話型の『HP Universal CMDB デプロイメント・ガイド』の関連セクションを参照してください。
UCMDB 設定画面で、プロトコルを HTTPS に設定し、ステップ 2 でコピーした証明書ファイルを選択します。
4. **hpcert.cer** を **<Configuration Manager_インストール_ディレクトリ>\java\windows\x86_64\bin** フォルダにあるサーバ・マシンにコピーします。
5. 次のコマンドによりキーツール・ユーティリティを使用して、サーバ・マシン上で証明書をトラスト・ストア (cacerts) にインポートします。

```
<Configuration_Manager_インストール_ディレクトリ>\java\bin\keytool.exe -import -alias hp -file hpcert.cer -keystore <Configuration_Manager_インストール_ディレクトリ>\java\windows\x86_64\lib\security\cacerts
```
6. **hpcert.cer** を **<Configuration Manager のインストール・ディレクトリ>\java\windows\x86_64\lib\security** フォルダにあるサーバ・マシンにコピーします。
7. 自己署名証明書および一致する秘密鍵を使用してサーバ・キーストア (JKS タイプ) を作成します。 **<Configuration_Manager_インストール_ディレクトリ>\java\windows\x86_64\bin** フォルダから、次のコマンドを実行します。

```
keytool -genkey -alias tomcat -keyalg RSA -keystore <Configuration_Manager_インストール_ディレクトリ>\java\windows\x86_64\lib\security\tomcat.keystore
```

 - a. キーストアのパスワードを入力します。
 - b. 次に、What is your first and last name? という質問に対して、Configuration Manager の Web サーバ名を入力し、所属する組織に応じてその他のパラメータを入力します。
 - c. キーのパスワードを入力します。キーのパスワードは、キーストアのパスワードと一致する必要があります。JKS キーストアが **tomcat.keystore** という名前で、**hpcert** という名前のサーバ証明書とともに作成されます。
8. **server.xml** ファイルを次のように修正します。
 - a. **<Configuration_Manager_インストール_ディレクトリ>\servers\server-0\conf** フォルダにある **server.xml** ファイルを開きます。次で始まるセクションを検索します。

```
Connector port="8143"
```

これはコメントとして表示されます。コメント文字を削除してスクリプトをアクティブ化し、次の行を追加します。

```
keystoreFile="<Configuration_Manager_インストール_ディレクトリ>\java\windows\x86_64\lib\security\tomcat.keystore"  
keystorePass="password"  
truststoreFile="<Configuration_Manager_インストール_ディレクトリ>\java\windows\x86_
```

```
64\lib\security\cacerts"  
truststorePass="changeit" />
```

- b. 次のラインをコメント・アウトします。

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
```

9. サーバを再起動します。

SSL を使用してその他の製品（ロード・バランサなど）の作業を行うよう Configuration Manager を設定するには、次のコマンドを実行して製品のセキュリティ証明書を Configuration Manager のトラスト・ストア（標準設定の jre トラスト・ストア）にインポートします。

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore  
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <証明書ファイル>
```

SSL で使用する UCMDB KPI アダプタの有効化

SSL (Secure Sockets Layer) を使用して送信されるよう UCMDB KPI アダプタ情報を設定することができます。

1. Configuration Manager 証明書のエクスポート:

```
<CM JAVA の HOME>\bin\keytool -export -alias tomcat -keystore  
<CM JAVA の HOME>\lib\security\tomcat.keystore -storepass  
<キーストアのパスワード> -file <証明書のファイル名>
```

2. Configuration Manager のからエクスポートした証明書を次のように UCMDB トラスト・ストアにインポートします。

```
<UCMDB サーバのディレクトリ>\bin\jre\bin keytool -import -trustcacerts  
-alias tomcat -keystore <UCMDB サーバのディレクトリ>\bin\jre\lib  
\security\cacerts -storepass changeit -file <証明書ファイル>
```

3. Configuration Manager のからエクスポートした証明書を次のようにプローブのトラスト・ストアにインポートします。

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
<DataFlowProbe のディレクトリ>\bin\jre\bin\keytool.exe -import -v -keystore  
<DataFlowProbe のディレクトリ>\conf\security\hprobeTrustStore.jks -file  
<証明書ファイル> -alias tomcat
```

- b. キーストアのパスワード、logomania を入力します。
- c. **[Trust this certificate?]** と表示された場合は、**[y]** を押して **Enter** キーを押します。
次のメッセージが表示されます。

証明書がキーストアに追加されました。

Data Flow Probe のセキュリティ強化の詳細については、「[Data Flow Probe の強化](#)」(69ページ)を参照してください。

4. UCMDB, Data Flow Probe, Configuration Manager を再起動します。

UCMDB Browserの SSL サポートの構成

注: ここに記載の指示は UCMDB Browser のバージョン 1.95 に対応しています。他の UCMDB 製品スイートとは別にアップグレードされた、新しいバージョンの UCMDB Browser を使用している場合は、当該バージョンの『HP UCMDB Browser のインストールおよび構成ガイド』に記載されている SSL サポートの構成についてのセクションを参照してください。

Tomcat で SSL サポートをインストール、構成するには

1. 次のコマンドの1つを実行し、サーバのプライベート・キーと自己署名証明書を保存するキーストア・ファイルを作成します。

- Windows の場合:`%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA`
- UNIX の場合:`$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA`

両方のコマンドで、パスワード値 `changeit` を使用します (開いているコンソール・ダイアログ・ボックスの他のすべてのフィールドについても、同じ値を使用できます)。

2. `$CATALINA_BASE/conf/server.xml` の **SSL HTTP/1.1 Connector** エントリからコメント行指定を解除します (`$CATALINA_BASE` は Tomcat をインストールしたディレクトリ)。

注: `server.xml` を構成して SSL を使用する方法の詳細については、Apache Tomcat オフィシャル・サイトを参照してください。 <http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html> (英語サイト)

3. Tomcat サーバを再起動します。

UCMDB サーバへの接続に HTTPS プロトコルを使用するには:

1. `ucmdb_browser_config.xml` で、タグ `<protocol>` に値 `https` を割り当て、タグ `<port>` に UCMDB サーバ HTTPS ポート値 (デフォルトでは 8443) を割り当てます。
2. UCMDB Browser ・マシンに UCMDB サーバの公開証明書をダウンロードします (UCMDB-Server で SSL を使用している場合、UCMDB 管理者がこの証明書を提供できます)。そして次のコマンドを実行して、サーバに接続しようとしている JRE の `cacerts` トラスト・ストアに公開証明書をインポートします。

```
"%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB サーバの証明書ファイル> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"
```

`<UCMDB サーバの証明書ファイル>` は、UCMDB サーバ公開証明書ファイルへのフルパスです。

3. Tomcat サーバを再起動します。

第3章: リバース・プロキシの使用

本項では、リバース・プロキシのセキュリティとの関係について概説し、HP Universal CMDB および Configuration Manager でリバース・プロキシを使用する手順について説明します。リバース・プロキシのセキュリティの側面については説明しますが、その他の側面については取り上げません。

本章の内容

• リバース・プロキシの概要	36
• リバース・プロキシ・サーバの使用のセキュリティ面	37
• リバース・プロキシの設定	38
• 相互認証を使用するリバース・プロキシまたはロード・バランサによる、Data Flow Probe の接続	41
• リバース・プロキシによる UCMDDB の CAC サポートの構成	43

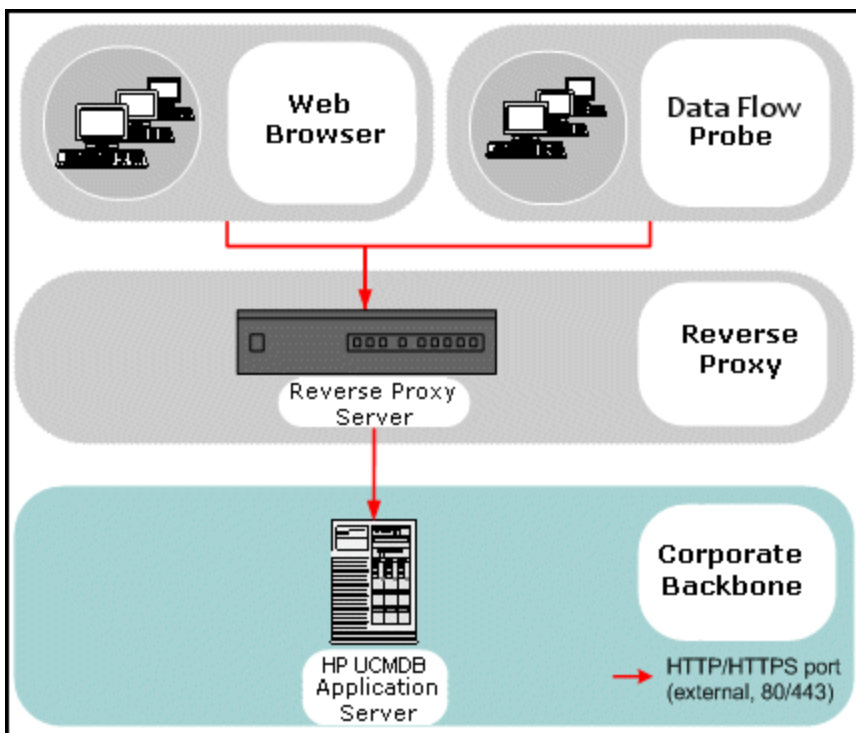
リバース・プロキシの概要

リバース・プロキシは、クライアント・マシンと Web サーバ間に位置する中間サーバです。リバース・プロキシは、クライアント・マシンからはクライアント・マシンの HTTP プロトコル要求を処理する通常の Web サーバのように見えます。

クライアント・マシンは、Web サーバ名の代わりにリバース・プロキシ名を使用して、Web コンテンツのための通常の要求を送信します。リバース・プロキシはその要求を Web サーバの 1 つに送信します。応答はリバース・プロキシによってクライアント・マシンに戻されますが、クライアント・マシンには応答が Web サーバから送信されたように見えます。

異なる URL で同じ UCMDDB/CM インスタンスを表す複数のリバース・プロキシを持つことが可能です。または、単一のリバース・プロキシを使用して各 UCMDDB/CM サーバに異なるルート・コンテキストを設定することで複数の UCMDDB/CM サーバにアクセスすることも可能です。

HP Universal CMDB および Configuration Manager は、DMZ アーキテクチャのリバース・プロキシをサポートしています。リバース・プロキシは、Data Flow Probe と Web クライアントおよび HP Universal CMDB/CM サーバ間の HTTP 仲介役です。



注:

- リバース・プロキシの種類によって、必要な構成の構文が異なります。Apache 2.0.x リバース・プロキシ設定の例については、「例:Apache 2.0.x 設定」(39ページ)を参照してください。
- フロント・エンド URL の設定は、スケジューラを使用したレポートへの直接リンク作成時のみ必要となります。

リバース・プロキシ・サーバの使用のセキュリティ面

リバース・プロキシ・サーバは、要塞ホストとして機能します。リバース・プロキシは外部クライアントから直接宣言される唯一のマシンとして設定されるため、残りの内部ネットワークは外部から見えなくなります。リバース・プロキシを使うことで、アプリケーション・サーバを内部ネットワークの別のマシンへ置くことが可能になります。

本項では、バック・ツー・バック・トポロジ環境でのリバース・プロキシと DMZ の使用について解説します。

このような環境でのリバース・プロキシの使用には、主に次のような利点があります。

- DMZ でのプロトコル変換が発生しない。受信プロトコルと送信プロトコルが同一（ヘッダの変更のみ発生）。

- リバース・プロキシに対する HTTP アクセスのみを許可することにより、ファイアウォールのステートフル・パケットインスペクションによる通信の高度な保護が可能。
- 静的な制限付きのリダイレクト要求の設定をリバース・プロキシにおいて定義が可能。
- Web サーバのセキュリティ機能のほとんどが、リバース・プロキシで利用可能（認証方式や暗号化など）。
- リバース・プロキシにより、実際のサーバの IP アドレスと内部ネットワークのアーキテクチャが見えなくなる。
- Web サーバにアクセスが可能なクライアントはリバース・プロキシのみ。
- この構成はほかのソリューションとは異なり、NAT 型ファイアウォールをサポートする。
- リバース・プロキシでは、ファイアウォールに開いておく必要のあるポートの数は最小限で済む。
- リバース・プロキシは、ほかの要塞ホスト・ソリューションと比較して高度なパフォーマンスを提供。

リバース・プロキシの設定

本項では、リバース・プロキシを設定する方法について説明します。UCMDB バージョン 10.01 では、UCMDB で設定を行う必要はありません。リバース・プロキシ側で、リバース・プロキシのドキュメントに従って設定ファイルを編集します。例については、「例:Apache 2.0.x 設定」(39ページ)を参照してください。

UCMDB バージョン 10.01 より前に作成されたスケジュール済みジョブの場合、次のように UCMDB の設定を行う必要があります。

インフラストラクチャ設定を使用したリバース・プロキシの設定

次に、インフラストラクチャ設定にアクセスしてリバース・プロキシを設定にする方法について説明します。この設定は、スケジューラを使用したレポートへの直接リンク作成時にのみ必要となります。

リバース・プロキシを設定するには、次の手順を実行します。

1. **【管理】 > 【インフラストラクチャ設定】 > 【全般設定】** カテゴリを選択します。
2. **【フロントエンド URL】** 設定を変更します。**https://my_proxy_server:443/** などのアドレスを入力します。

注: この変更を行うと、クライアントから直接 HP Universal CMDB サーバにアクセスできなくなります。リバース・プロキシの設定を変更するには、サーバ・マシンで JMX コンソールを使用します。詳細については、次の「[JMX コンソールを使用したリバース・プロキシの設定](#)」を参照してください。

JMX コンソールを使用したリバース・プロキシの設定

HP Universal CMDB サーバ・マシンで JMX コンソールを使用してリバース・プロキシの設定を変更できます。この設定は、スケジューラを使用したレポートへの直接リンク作成時にのみ必要となります。

リバース・プロキシの設定を変更するには、次の手順を実行します。

1. HP Universal CMDB サーバ・マシンで Web ブラウザを起動し、次のアドレスを入力します。

http://<マシン名または IP アドレス>.<ドメイン名>:8080/jmx-console

<マシン名または IP アドレス>には、HP Universal CMDB がインストールされているマシンを指定します。ユーザ名とパスワードでログインする必要がある場合もあります。

2. **[UCMDB-UI] > [UCMDB-UI:name=UI Server frontend settings]** リンクをクリックします。

[setUseFrontendURLBySettings] フィールドに、**https://my_proxy_server:443/** などのサーバ・プロキシ URL を入力します。

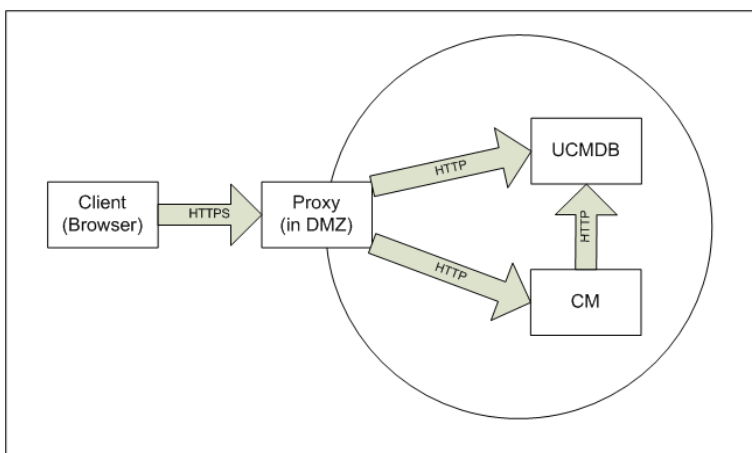
3. **[Invoke]** をクリックします。

4. この設定の値を確認するには、**showFrontendURLInSettings** メソッドを使用します。

例 :Apache 2.0.x 設定

本項では、Data Flow Probe プローブとアプリケーション・ユーザの両方が、HP Universal CMDB に接続する場合の、Apache 2.0.x リバース・プロキシの使用をサポートする設定ファイルの例を説明します。

次の図には、Configuration Manager および UCMDB のリバース・プロキシの設定プロセスを示しています。



注:

- この例では、HP Universal CMDB マシンの DNS 名およびポートは UCMDB_server です。
- この例では、HP Configuration Manager の DNS 名およびポートは UCMDB_CM_server です。

- この変更は、Apache 管理の知識を持つユーザのみが行なえます。

1. <Apache マシンのルート・ディレクトリ>\Webserver\conf\httpd.conf ファイルを開きます。
2. 次のモジュールを有効にします。
 - **LoadModule proxy_module modules/mod_proxy.so**
 - **LoadModule proxy_http_module modules/mod_proxy_http.so**
3. **httpd.conf** ファイルに、次の行を追加します。

```
ProxyRequests off
<Proxy *>
    Order deny,allow
    Deny from all
    Allow from all
</Proxy>
```

```
ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
```



```
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser  
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
```

4. 変更を保存します。

相互認証を使用するリバース・プロキシ またはロード・バランサによる, Data Flow Probe の接続

相互認証によるリバース・プロキシまたはロード・バランサを使用して Data Flow Probe に接続するには、次の手順を実行します。この手順は次の構成に適用されます。

- プロブによって提供され、リバース・プロキシまたはロード・バランサによって要求されるクライアント証明書に基づいた、プロブとリバース・プロキシまたはロードバランサの間の相互 SSL 認証。
- リバース・プロキシまたはロード・バランサおよび UCMDB サーバとの間の通常の SSL 接続。

注: 次の手順では、**cKeyStoreFile** キー・ストアをプロブ・キー・ストアとして使用します。これは Data Flow Probe インストールの一部である、事前定義されたクライアント・キー・ストアで、セルフ署名証明書が含まれています。詳細については、「[サーバと Data Flow Probe のデフォルトのキー・ストアとトラスト・ストア](#)」(85ページ)を参照してください。

新たに生成された秘密鍵を含む新しい一意のキー・ストアを作成することをお勧めします。詳細については、「[Data Flow Probe のキー・ストアの作成](#)」(84ページ)を参照してください。

証明権限から証明書を取得

CA ルート証明書を取得し次の場所にインポートします。

- Data Flow Probe のトラスト・ストア
 - Data Flow Probe JVM cacerts
 - UCMDB サーバのトラスト・ストア
 - リバース・プロキシのトラスト・ストア
1. CA ルート証明書を Data Flow Probe トラスト・ストアにインポートします。
 - a. CA ルート証明書を次のディレクトリに置きます:<Data Flow Probe のインストール・ディレクトリ>\conf\security\<証明書ファイル名>。
 - b. 次のスクリプトを実行して、CA ルート証明書を Data Flow トラスト・ストアにインポートします。

```
<Data Flow Probe のインストール・ディレクトリ>\bin\jre\bin\keytool.exe -import -trustcacerts -  
alias <エイリアス> -file C:\hp\UCMDB\DataFlowProbe\conf\security\<証明書ファイル名> -
```

```
keystore <Data Flow Probe のインストール・ディレクトリ>\conf\security\hprobeTrustStore.jks
```

標準設定のパスワード:**logomania**。

2. 次のスクリプトを実行して、CA ルート証明書を Data Flow Probe JVM cacerts にインポートします。

```
<Data Flow Probe のインストール・ディレクトリ>\bin\jre\bin\keytool.exe -import -trustcacerts -alias <エイリアス> -file <Data Flow Probe のインストール・ディレクトリ>\conf\security\<証明書ファイル名> -keystore <Data Flow Probe のインストール・ディレクトリ>\bin\jre\lib\security\cacerts
```

標準設定のパスワード:**changeit**。

3. CA ルート証明書を UCMDB トラスト・ストアにインポートします。
 - a. CA ルート証明書を次のディレクトリに置きます:<UCMDB のインストール・ディレクトリ>\conf\security\<証明書ファイル名>。
 - b. 次のスクリプトを実行して、CA ルート証明書を UCMDB トラスト・ストアにインポートします。

```
<UCMDB のインストール・ディレクトリ>\bin\jre\bin\keytool.exe -import -trustcacerts -alias <エイリアス> -file <UCMDB のインストール・ディレクトリ>\conf\security\<証明書ファイル名> -keystore <UCMDB のインストール・ディレクトリ>\conf\security\sever.truststore
```

標準設定のパスワード:**hppass**。

4. CA ルート証明書をリバース・プロキシのトラスト・ストアにインポートします。このステップはベンダによって異なります。

証明書の Java キーストアへの変換

Data Flow Probe のクライアント証明書（および秘密鍵）を使用している証明書権限（CA）から PFX/PKCS12 形式で取得し、次のスクリプトを実行して Java キーストアに変換します。

```
<Data Flow Probe のインストール・ディレクトリ>\bin\jre\bin\keytool.exe -importkeystore -srckeystore <PFX キーストアのフル・パス> -destkeystore <新しい対象キーストアのフル・パス> -srcstoretype PKCS12
```

ソースおよび対象キーストアのパスワードの入力を求められます。

ソース・キーストアのパスワードの場合は、PFX キーストアをエクスポートした際と同じパスワードを使用します。

Data Flow Probe キー・ストアの標準の対象キー・ストア・パスワード:**logomania**。

注: 標準の Data Flow Probe キーストア・パスワード (logomania) から異なる対象キーストア・パスワードを入力した場合、**<Data Flow Probe のインストール・ディレクトリ>\conf\ssl.properties** ファイル (javax.net.ssl.keyStorePassword) に暗号化された形式で新しいパスワードを入力しなければなりません。詳細については、「[プローブのキー・ストアとトラスト・ストアのパスワードを暗号化](#)」(85ページ)を参照してください。

新しいキー・ストアを次のディレクトリに置きます:<Data Flow Probe のインストール・ディレクトリ>\conf\security。

注意: `hprobeKeyStore.jks` ファイルは上書きしないでください。

新規作成したキーストアを使用するための SSL プロパティ・ファイルの変更

<Data Flow Probe のインストール・ディレクトリ>\conf\ssl.properties のファイルにクライアント証明書を含んでいるキーストアを `javax.net.ssl.keyStore` に設定します。

キーストアのパスワードが標準の Data Flow Probe キーストア・パスワード (logomania) ではない場合、暗号化後に `javax.net.ssl.keyStorePassword` を更新します。パスワード暗号化の詳細については、「[プローブのキー・ストアとトラスト・ストアのパスワードを暗号化](#)」(85ページ)を参照してください。

Data Flow Probe 設定の確認

<Data Flow Probe のインストール・ディレクトリ>\conf\DataFlowProbe.properties ファイルを次のように編集します。

```
appilog.agent.probe.protocol = HTTPS
```

```
serverName = <リバース・プロキシ・サーバ・アドレス>
```

```
serverPortHttps = <UCMDB に要求をリダイレクトするためにリバース・プロキシがリッスンする HTTPS ポート>
```

SSL を使用して作業するための UCMDB の設定

詳細については、「[Secure Sockets Layer \(SSL\) 通信の有効化](#)」(17ページ)を参照してください。

この手順で残りの証明書を作成した CA と同じ CA によって UCMDB サーバ証明書が作成された場合、リバース・プロキシまたはロード・バランサは UCMDB 証明書を信頼します。

リバース・プロキシによる UCMDB の CAC サポートの構成

本項では、リバース・プロキシを使用して UCMDB に共通アクセスカード (CAC) サポートを設定する方法について説明します。

1. Web ブラウザを起動して、次のとおりサーバ・アドレスを入力することによって、JMX コンソールを開きます。 `http://<UCMDB サーバ・ホスト名または IP>:8080/jmx-console`
ユーザ名とパスワードを使用してログインする必要がある場合もあります。
2. UCMDB で、**UCMDB:service=Ports Management Services** をクリックして [操作] ページを開きます。
 - (任意) **[ComponentsConfigurations]** をクリックします。次の操作を実行します。
 - **HTTPSetPort** を **8080** に設定して、**[Invoke]** をクリックします。
 - **[Back to MBean]** をクリックします。

- **[mapComponentToConnectors]** をクリックします。次の操作を実行します。
 - mapComponentToConnectors サービスで、**componentName** を **ucmdb-ui** に設定します。
 - **isHTTP** のみを **true** に設定して、**[Invoke]** をクリックします。
 - **[Back to MBean]** をクリックします。
 - mapComponentToConnectors サービスで、**componentName** を **root** に設定します。
 - **isHTTP** のみを **true** に設定して、**[Invoke]** をクリックします。
- 3. UCMDB で、**UCMDB:service=Security Services** をクリックして **[操作]** ページを開きます。
 - **loginWithCAC** を **true** に設定して、**[Invoke]** をクリックします。
 - **[Back to MBean]** をクリックします。
 - **withReverseProxy** を **true** に設定して、**[Invoke]** をクリックします。

この設定によって、UCMDB で使用するユーザ名と認証に使用する証明書を UCMDB_SSL_CLIENT_CERT ヘッダから抽出するように、UCMDB サーバを設定できます。
 - **[Back to MBean]** をクリックします。
 - (任意) **onlyCAC Certs** を **true** に設定して、**[Invoke]** をクリックします。

この操作を **true** に設定して、物理 CAC デバイスからの証明書のみを受け入れるようにします。
 - (任意) **usernameField** をクリックして、UCMDB がユーザ名の抽出に使用するフィールドを証明書内から指定し、**[Invoke]** をクリックします。

注: フィールドを指定しない場合、標準設定の PRINCIPAL_NAME_FROM_SAN_FIELD が使用されます。

- 4. UCMDB サーバを再起動します。

例: Apache 2.4.4 の構成

本項では、Apache 2.4.4 のサンプル構成ファイルについて説明します。

注: この例では、Apache サーバが **c:\Apache24** にインストールされたことを前提としています。別のフォルダにインストールされている場合、すべての事例で正しい場所を指定するように変更する必要があります。

この例の相互認証用のポートは 443 です。 **c:\Apache24\conf** フォルダで、次をコピーします。

- Apache サーバによって使用される証明書 (**server.crt**)
- Apache サーバの秘密鍵 (**server.key**)
- Apache サーバの信頼できる CA (**ssl.crt**)
- 証明書失効リスト (**ssl.crt**)。

注: これらの4ファイルはすべて PEM 形式である必要があります。

c:\Apache24\conf\httpd.conf の内容を次と置き換える必要があります ([APACHE_MACHINE_FQD]は適宜変更します)。

```
ServerRoot "c:/Apache24"
Listen 80
LoadModule access_compat_module modules/mod_access_compat.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule allowmethods_module modules/mod_allowmethods.so
LoadModule asis_module modules/mod_asis.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authn_core_module modules/mod_authn_core.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authz_core_module modules/mod_authz_core.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule cgi_module modules/mod_cgi.so
LoadModule dir_module modules/mod_dir.so
LoadModule env_module modules/mod_env.so
LoadModule headers_module modules/mod_headers.so
LoadModule include_module modules/mod_include.so
LoadModule isapi_module modules/mod_isapi.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
LoadModule xml2enc_module modules/mod_xml2enc.so
<IfModule unixd_module>
User daemon
Group daemon
</IfModule>
ServerAdmin admin@example.com
ServerName [APACHE_MACHINE_FQD]:80
<Directory />
    AllowOverride none
    Require all denied
</Directory>
DocumentRoot "c:/Apache24/htdocs"
<Directory "c:/Apache24/htdocs">
    Options Indexes FollowSymLinks
```

```

    AllowOverride None
    Require all granted
</Directory>
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>
<Files ".ht*">
    Require all denied
</Files>
ErrorLog "logs/error.log"
LogLevel warn
<IfModule log_config_module>
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%[Referer]i\" \"%[User-Agent]i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    <IfModule logio_module>
        LogFormat "%h %l %u %t \"%r\" %>s %b \"%[Referer]i\" \"%[User-Agent]i\" %l %O" combinedio
    </IfModule>
    CustomLog "logs/access.log" common
</IfModule>
<IfModule alias_module>
    ScriptAlias /cgi-bin/ "c:/Apache24/cgi-bin/"
</IfModule>
<IfModule cgid_module>
</IfModule>
<Directory "c:/Apache24/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
<IfModule mime_module>
    TypesConfig conf/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
</IfModule>
<IfModule proxy_html_module>
    Include conf/extra/proxy-html.conf
</IfModule>
    Include conf/extra/httpd-ssl.conf
<IfModule ssl_module>
    SSLRandomSeed startup builtin
    SSLRandomSeed connect builtin
</IfModule>

```

また、**c:\Apache24\conf\httpd-ssl.conf** の内容を次と置き換える必要があります ([APACHE_MACHINE_FQD], [UCMDB_SERVER_NAME], および[UCMDB_CM_SERVER_NAME]は適宜変更します)。

```

Listen 443
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
SSLPassPhraseDialog builtin
SSLSessionCache "shmcb:c:/Apache24/logs/ssl_scache(512000)"

```

```
SSLSessionCacheTimeout 300
<VirtualHost _default_:443>
DocumentRoot "c:/Apache24/htdocs"
ServerName [APACHE_MACHINE_FQD]:443
ServerAdmin admin@example.com
ErrorLog "c:/Apache24/logs/error.log"
TransferLog "c:/Apache24/logs/access.log"
SSLEngine on
SSLCertificateFile "c:/Apache24/conf/server.crt"
SSLCertificateKeyFile "c:/Apache24/conf/server.key"
SSLCACertificateFile "c:/Apache24/conf/ssl.crt"
SSLCARevocationFile "c:/Apache24/conf/ssl.crl"
SSLCARevocationCheck leaf
SSLVerifyClient require
SSLVerifyDepth 10
SSLOptions +ExportCertData
<FilesMatch "\.(cgi|shtml|phtml|php)$">
  SSLOptions +StdEnvVars
</FilesMatch>
<Directory "c:/Apache24/cgi-bin">
  SSLOptions +StdEnvVars
</Directory>
BrowserMatch "MSIE [2-5]" \
  nokeepalive ssl-unclean-shutdown \
  downgrade-1.0 force-response-1.0
CustomLog "c:/Apache24/logs/ssl_request.log" \
  "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
RequestHeader set UCMDB_SSL_CLIENT_CERT %{SSL_CLIENT_CERT}e
ProxyRequests off
<Proxy *>
  Order deny,allow
  Deny from all
  Allow from all
</Proxy>
ProxyPass / http://[UCMDB_SERVER_NAME]:8080/
ProxyPassReverse / http://[UCMDB_SERVER_NAME]:8080/
ProxyPass /mam http://[UCMDB_SERVER_NAME]:8080/mam
ProxyPassReverse /mam http://[UCMDB_SERVER_NAME]:8080/mam
ProxyPass /mam_images http://[UCMDB_SERVER_NAME]:8080/mam_images
ProxyPassReverse /mam_images http://[UCMDB_SERVER_NAME]:8080/mam_images
ProxyPass /mam-collectors http://[UCMDB_SERVER_NAME]:8080/mam-collectors
ProxyPassReverse /mam-collectors http://[UCMDB_SERVER_NAME]:8080/mam-collectors
ProxyPass /ucmdb http://[UCMDB_SERVER_NAME]:8080/ucmdb
ProxyPassReverse /ucmdb http://[UCMDB_SERVER_NAME]:8080/ucmdb
ProxyPass /site http://[UCMDB_SERVER_NAME]:8080/site
ProxyPassReverse /site http://[UCMDB_SERVER_NAME]:8080/site
ProxyPass /ucmdb-ui http://[UCMDB_SERVER_NAME]:8080/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://[UCMDB_SERVER_NAME]:8080/ucmdb-ui
```

```
ProxyPass /status http://[UCMDB_SERVER_NAME]:8080/status
ProxyPassReverse /status http://[UCMDB_SERVER_NAME]:8080/status
ProxyPass /jmx-console http://[UCMDB_SERVER_NAME]:8080/jmx-console
ProxyPassReverse /jmx-console http://[UCMDB_SERVER_NAME]:8080/jmx-console
ProxyPass /axis2 http://[UCMDB_SERVER_NAME]:8080/axis2
ProxyPassReverse /axis2 http://[UCMDB_SERVER_NAME]:8080/axis2
ProxyPass /icons http://[UCMDB_SERVER_NAME]:8080/icons
ProxyPassReverse /icons http://[UCMDB_SERVER_NAME]:8080/icons
ProxyPass /ucmdb-api http://[UCMDB_SERVER_NAME]:8080/ucmdb-api
ProxyPassReverse /ucmdb-api http://[UCMDB_SERVER_NAME]:8080/ucmdb-api
ProxyPass /ucmdb-docs http://[UCMDB_SERVER_NAME]:8080/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://[UCMDB_SERVER_NAME]:8080/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://[UCMDB_SERVER_NAME]:8080/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://[UCMDB_SERVER_NAME]:8080/ucmdb-api/8.0
ProxyPass /cm http://[UCMDB_SERVER_NAME]:8080/cm
ProxyPassReverse /cm http://[UCMDB_SERVER_NAME]:8080/cm
ProxyPass /cnc http://[UCMDB_CM_SERVER_NAME]/cnc
ProxyPassReverse /cnc http://[UCMDB_CM_SERVER_NAME]/cnc
ProxyPass /docs http://[UCMDB_CM_SERVER_NAME]/docs
ProxyPassReverse /docs http://[UCMDB_CM_SERVER_NAME]/docs
ProxyPass /ucmdb-browser http://[UCMDB_CM_SERVER_NAME]/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://[UCMDB_CM_SERVER_NAME]/ucmdb-browser
</VirtualHost>
```

[https://\[APACHE_MACHINE_FQD\]](https://[APACHE_MACHINE_FQD]) に移動することによって、リバース・プロキシを介して UCMDB サーバにアクセスできるようになりました。

注: Internet Explorer にインポートされた有効な証明書が必要です。有効な証明書は、Apache の信頼された CA の中の 1 つの CA によって署名されたものです (**ssl.crt** ファイル内に提示されている必要があります)。

第4章: データ・フロー資格情報管理

本章の内容

• データ・フロー資格情報管理の概要	50
• セキュリティ上の基本的な前提条件	51
• 別々のモードで実行されている Data Flow Probe	51
• 資格情報キャッシュを最新に保つ	51
• すべてのプローブでの設定変更の同期	52
• プローブ上の安全なストレージ	52
• 資格情報の表示	53
• 資格情報のアップグレード	53
• 機密マネージャ・クライアント認証と暗号化設定の設定	54
• LW-SSO 設定の構成	54
• 機密マネージャ・コミュニケーション暗号化の設定	54
• プローブでの手動での機密マネージャ・クライアントの認証設定および暗号化設定	56
• サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化	56
• プローブでの機密マネージャ・クライアントの認証設定および暗号化設定	57
• プローブでの資格情報マネージャ通信の暗号化の設定	57
• 資格情報マネージャ・クライアントのキャッシュの設定	58
• プローブでの機密マネージャ・クライアントのキャッシュ・モードの設定	58
• プローブでの機密マネージャ・クライアントのキャッシュ暗号化文字列の設定	59
• 暗号化された形式による、資格情報および範囲情報のエクスポートとインポート	60
• 資格情報マネージャ・クライアントのログ・ファイル・メッセージ・レベルの変更	61
• 機密マネージャ・クライアント・ログ・ファイル	62
• LW-SSO ログ・ファイル	62
• 暗号鍵の生成または更新	63
• 新規暗号鍵の生成	63
• UCMDB サーバでの暗号鍵の更新	64
• プローブでの暗号鍵の更新	65
• Probe Manager とプローブ・ゲートウェイが別々のマシンにインストールされている場合における暗号鍵の手動による変更	66

- [複数の JCE プロバイダの定義](#) 66
- [資格情報マネージャの暗号化設定](#) 67
- [トラブルシューティングおよび制限事項](#) 68

データ・フロー資格情報管理の概要

ディスカバリを操作またはインテグレーションを実行するには、リモート・システムにアクセスするための資格情報を設定する必要があります。資格情報は [Data Flow Probe 設定] ウィンドウで設定され、UCMDB サーバに保存されます。詳細については、『HP Universal CMDB データ・フロー管理ガイド』で、Data Flow Probe のセットアップについて説明した項を参照してください。

資格情報のストレージは、資格情報マネージャ・コンポーネントによって管理されます。詳細については、『[機密マネージャ](#) (103ページ)を参照してください。

Data Flow Probe は機密マネージャ・クライアントを使用して資格情報にアクセスできます。機密マネージャ・クライアントは Data Flow Probe 上にあり、UCMDB サーバ上にある機密マネージャ・サーバと通信します。機密マネージャ・クライアントと機密マネージャ・サーバ間の通信は暗号化され、機密マネージャ・サーバに接続するときには機密マネージャ・クライアントの認証が必要になります。

機密マネージャ・サーバ上での機密マネージャ・クライアントの認証は、LW-SSO コンポーネントに基づいています。機密マネージャ・サーバに接続する前に、機密マネージャ・クライアントはまず LW-SSO クッキーを送信します。機密マネージャ・サーバはクッキーを検証し、検証にパスしたら、機密マネージャ・クライアントとの通信が開始されます。LW-SSO の詳細については、『[LW-SSO 設定の構成](#) (54ページ)を参照してください。

機密マネージャ・クライアントと機密マネージャ・サーバ間の通信は暗号化されます。暗号化設定の更新の詳細については、『[機密マネージャ・コミュニケーション暗号化の設定](#) (54ページ)を参照してください。

注意: 機密マネージャの認証では、コンピュータ上に定義された世界時 (UTC) が使用されません。認証を正常に行うには、Data Flow Probe と UCMDB サーバ上の世界時を同じにしてください。UTC はタイムゾーンやサマータイムとは独立しているため、サーバとプローブは異なるタイムゾーンでも可能です。

機密マネージャ・クライアントは資格情報のローカル・キャッシュを保持します。機密マネージャ・クライアントは、機密マネージャ・サーバからすべての資格情報をダウンロードしてキャッシュに保存するように設定されます。資格情報の変更は、機密マネージャ・サーバから継続的に自動同期されます。キャッシュは、事前設定によってファイルシステム・キャッシュまたはメモリ内キャッシュを使用できます。また、キャッシュは暗号化され、外部からはアクセスできません。キャッシュ設定の更新の詳細については、『[プローブでの機密マネージャ・クライアントのキャッシュ・モードの設定](#) (58ページ)を参照してください。キャッシュの暗号化の更新の詳細については、『[プローブでの機密マネージャ・クライアントのキャッシュ暗号化文字列の設定](#) (59ページ)を参照してください。

トラブルシューティングの詳細については、「[資格情報マネージャ・クライアントのログ・ファイル・メッセージ・レベルの変更](#)」(61ページ)を参照してください。

資格情報を UCMDDB サーバ間でコピーできます。詳細については、「[暗号化された形式による、資格情報および範囲情報のエクスポートとインポート](#)」(60ページ)を参照してください。

注: プローブで (UCMDDB バージョン 9.01 以前で) 資格情報のストレージに使用されていた **DomainScopeDocument** (DSD) に、資格情報に関する機密情報が含まれなくなりました。現在、このファイルにはプローブのリストとネットワーク範囲情報が含まれます。各ドメインの資格情報エントリのリストも含まれます。各エントリには資格情報 ID とネットワーク範囲 (この資格情報エントリに定義されている) のみが含まれます。

本項の内容

- 「[セキュリティ上の基本的な前提条件](#)」(51ページ)
- 「[別々のモードで実行されている Data Flow Probe](#)」(51ページ)
- 「[資格情報キャッシュを最新に保つ](#)」(51ページ)
- 「[すべてのプローブでの設定変更の同期](#)」(52ページ)
- 「[プローブ上の安全なストレージ](#)」(52ページ)

セキュリティ上の基本的な前提条件

セキュリティ上の前提条件は次のとおりです。

UCMDDB サーバおよびプローブ JMX コンソールのセキュリティが確保されていて、UCMDDB システム管理者だけがアクセスを許可されるようになっている。localhost からのアクセスに限定されているのが望ましい。

別々のモードで実行されている Data Flow Probe

Probe Gateway とマネージャを個別のプロセスとして実行する場合、資格情報マネージャ・クライアント・コンポーネントはマネージャ・プロセスの一部となります。資格情報はキャッシュされ、Probe Manager によってのみ使用されます。UCMDDB システムで機密マネージャ・サーバにアクセスする場合、ゲートウェイ・プロセスで機密マネージャ・クライアント要求が処理され、そこから UCMDDB に転送されます。

プローブが個別のモードで設定されている場合、この設定は自動的に行なわれます。

資格情報キャッシュを最新に保つ

機密マネージャ・サーバへの初回接続時、機密マネージャ・クライアントは関連するすべての資格情報をダウンロードします (プローブのドメインで設定されているすべての資格情報)。初回通信に成功した後、機密マネージャ・クライアントは機密マネージャ・サーバとの同期状態を維持します。1

分間隔で差分同期が実行され、機密マネージャ・サーバと機密マネージャ・クライアント間の差異のみが同期されます。UCMDB サーバ側で資格情報が変更されると（新しい資格情報の追加、または既存の資格情報の更新 / 削除など）、機密マネージャ・クライアントは UCMDB サーバから直ちに通知を受信し、追加の同期を実行します。

すべてのプローブでの設定変更の同期

正常に通信するためには、機密マネージャ・クライアントを機密マネージャ・サーバの認証設定（LW-SSO 初期化文字列）および暗号化設定（機密マネージャ通信の暗号化）で更新する必要があります。たとえば、サーバで初期化文字列が変更された場合、プローブは認証するために新しい初期化文字列を認識する必要があります。

UCMDB サーバは機密マネージャ通信の暗号化設定および機密マネージャ認証設定の変更を常に監視します。このモニタリングは 15 秒毎に実施され、変更が発生すると、更新された設定がプローブに送信されます。設定は暗号化された形式でプローブに渡され、プローブ側の安全なストレージに保存されます。送信される設定は、対称暗号鍵を使用して暗号化されます。標準設定では、UCMDB サーバと Data Flow Probe は同じ標準設定の対称暗号鍵を使用してインストールされます。最適なセキュリティを実現するために、システムに資格情報を追加する前に、この鍵を変更することをお勧めします。詳細については、「[暗号鍵の生成または更新](#)」(63ページ)を参照してください。

注: 監視間隔は 15 秒であるため、プローブ側の機密マネージャ・クライアントに 15 秒間、最新の設定が反映されない可能性があります。

UCMDB サーバと Data Flow Probe 間の機密マネージャ通信および認証設定の自動同期を無効にする場合、UCMDB サーバ側で機密マネージャ通信および認証設定を更新するたびに、すべてのプローブも新しい設定で更新する必要があります。詳細については、「[サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化](#)」(56ページ)を参照してください。

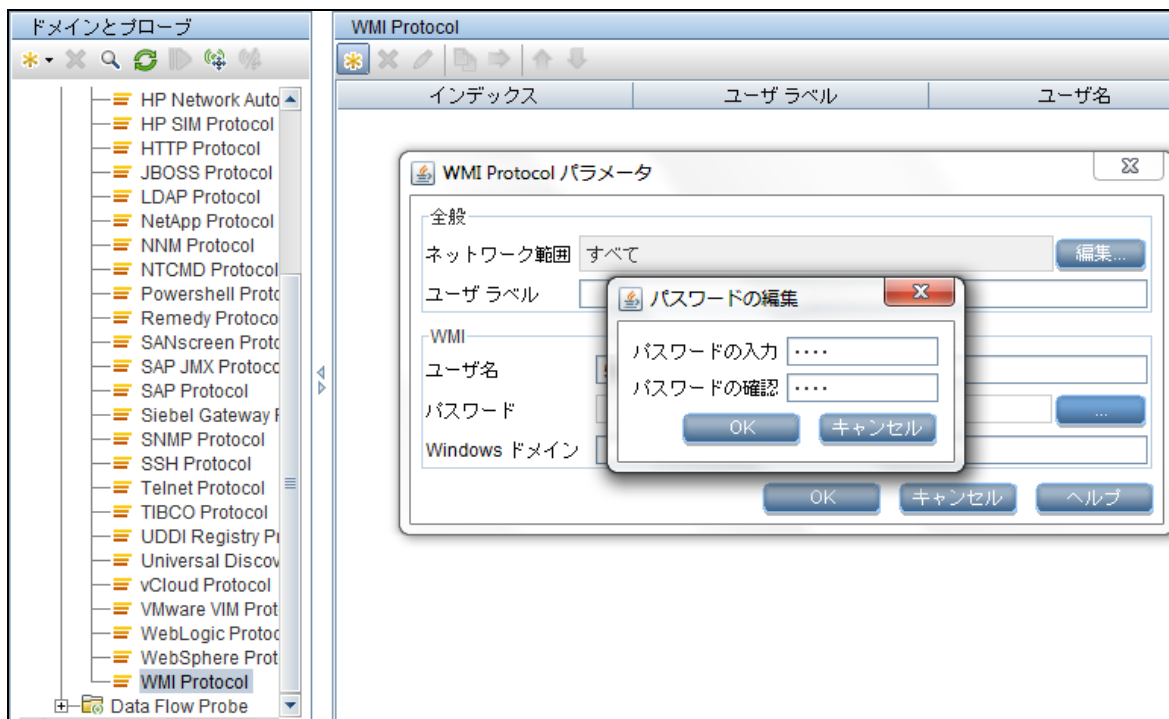
プローブ上の安全なストレージ

慎重に扱う必要があるすべての情報（機密マネージャ通信および認証設定と暗号化の鍵など）は、プローブで安全な保管場所の `C:\hp\UCMDB\DataFlowProbe\conf\security` にある `secured_storage.bin` ファイルに格納されます。このセキュリティ保護された保管場所は DPAPI を使用して暗号化されません。DPAPI は、暗号化のプロセスでは Windows のユーザ・パスワードに依存します。DPAPI は、Windows システム上で証明書と秘密鍵などの機密データを保護する標準の方法です。パスワードが変更されてもセキュリティ保護された保管場所からプローブが情報を読み出せるように、プローブは常に同じ Windows ユーザで実行してください。

資格情報の表示

注: 本項では、データの方向が CMDB から HP Universal CMDB である場合の資格情報の表示について説明します。

パスワードは、CMDBからアプリケーションへは送信されません。つまり、HP Universal CMDB は、パスワード・フィールドの内容に関係なくアスタリスク (*) を表示します。



資格情報のアップグレード

注: 本項では、データの方向が HP Universal CMDB から CMDB である場合の資格情報の更新について説明します。

- この方向の通信は暗号化されないため、UCMDB サーバへは HTTPS/SSL を使用して接続するか、信頼されたネットワークを通して接続する必要があります。
通信は暗号化されませんが、パスワードはネットワークでクリア・テキストとしては送信されません。パスワードは標準設定の鍵で暗号化されるため、送信中の機密性を高めるために SSL を使用することを強くお勧めします。
- パスワードには特殊文字が使用できます。英字以外の文字も使用できます。

機密マネージャ・クライアント認証と暗号化設定の設定

このタスクは、UCMDB サーバ上の機密マネージャのクライアント認証および暗号化設定について記述するものであり、次のステップが含まれます。

- [「LW-SSO 設定の構成」 \(54ページ\)](#)
- [「機密マネージャ・コミュニケーション暗号化の設定」 \(54ページ\)](#)

LW-SSO 設定の構成

次の手順では、UCMDB サーバで LW-SSO init 文字列を変更する方法について説明します。変更を自動送信しないように UCMDB サーバが設定されている場合を除き、この変更はプロンプトに（暗号化文字列として）自動的に送信されます。詳細については、[「サーバとプロンプト間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化」 \(56ページ\)](#)を参照してください。

1. UCMDB サーバで、Web ブラウザを起動して次のアドレスを入力します。
http://localhost:8080/jmx-console
2. **UCMDB-UI:name=LW-SSO Configuration** をクリックして [JMX MBEAN View] ページを開きます。
3. **setInitString** メソッドを見つけます。
4. 新しい LW-SSO init 文字列を入力します。
5. [Invoke] をクリックします。

機密マネージャ・コミュニケーション暗号化の設定

次の手順では、UCMDB サーバで機密マネージャ・コミュニケーション暗号化の設定を変更する方法について説明します。この設定では、機密マネージャ・クライアントと機密マネージャ・サーバ間の通信を暗号化する方法を指定します。変更を自動送信しないように UCMDB サーバが設定されている場合を除き、この変更はプロンプトに（暗号化文字列として）自動的に送信されます。詳細については、[「サーバとプロンプト間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化」 \(56ページ\)](#)を参照してください。

1. UCMDB サーバで、Web ブラウザを起動して次のアドレスを入力します。
http://localhost:8080/jmx-console
2. **UCMDB:service=Security Services** をクリックして、[JMX MBEAN View] ページを開きます。
3. **CMGetConfiguration** メソッドをクリックします。
4. [Invoke] をクリックします。

現在の機密マネージャ設定のXMLが表示されます。

5. 表示されたXMLの内容をコピーします。
6. **セキュリティ・サービス**の [JMX MBEAN View] ページに戻ります。
7. **CMSetConfiguration** メソッドをクリックします。
8. コピーしたXMLを [値] フィールドに貼り付けます。
9. 関連する転送関連の設定を更新して, [Invoke] をクリックします。

例:

```
<transport>
  <encryptTransportMode>true</encryptTransportMode>
  <CMEncryptionDecryption>
    <encryptDecryptInitString>radiohead</encryptDecryptInitString>
    <cryptoSource>lw</cryptoSource>
    <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
    <cipherType>symmetricBlockCipher</cipherType>
    <engineName>AES</engineName>
    <algorithmModeName>CBC</algorithmModeName>
    <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
    <keySize>256</keySize>
    <pbeCount>20</pbeCount>
    <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
    <encodingMode>Base64Url</encodingMode>
    <useMacWithCrypto>>false</useMacWithCrypto>
    <macType>hmac</macType>
    <macKeySize>256</macKeySize>
    <macHashName>SHA256</macHashName>
  </CMEncryptionDecryption>
</transport>
```

更新可能な値の詳細については, [「資格情報マネージャの暗号化設定」\(67ページ\)](#)を参照してください。

プローブでの手動での機密マネージャ・クライアントの認証設定および暗号化設定

本項の内容

- ・ [「サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化」](#) (56ページ)
- ・ [「プローブでの機密マネージャ・クライアントの認証設定および暗号化設定」](#) (57ページ)
- ・ [「プローブでの資格情報マネージャ通信の暗号化の設定」](#) (57ページ)

サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化

標準設定では、UCMDB サーバは機密マネージャ / LW-SSO 設定をすべてのプローブに自動送信するように設定されています。この情報は暗号化された文字列としてプローブに送信され、取得時に復号化されます。機密マネージャ/LW-SSO 設定ファイルをすべてのプローブに自動送信しないように、UCMDB サーバを設定できます。この場合、ユーザが手動で、すべてのプローブを新しい機密マネージャ / LW-SSO 設定で更新する必要があります。

機密マネージャ / LW-SSO 設定の自動同期を無効にするには、次の手順を実行します。

1. UCMDB で、**【管理】** > **【インフラストラクチャ設定マネージャ】** > **【全般設定】** をクリックします。
2. **【Enable automatic synchronization of CM/LW-SSO configuration and init string with probe】** を選択します。
3. **【値】** フィールドをクリックして、**【True】** から **【False】** に変更します。
4. **【保存】** ボタンをクリックします。
5. UCMDB サーバを再起動します。

プローブでの機密マネージャ・クライアントの認証設定および暗号化設定

次の手順は、UCMDB サーバが LW-SSO / 機密マネージャ設定をプローブに自動送信しないように設定されている場合に使用します。詳細については、「[サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化](#)」(56ページ)を参照してください。

1. プローブ・マシンで Web ブラウザを起動し、次のアドレスを入力します。 **http://localhost:1977**

注: Probe Manager とプローブ・ゲートウェイが個別のプロセスとして実行されている場合は、Probe Manager が実行されているマシンでアドレスを入力する必要があります。

http://localhost:1978

2. **type=CMClient** をクリックして、[JMX MBEAN View] ページを開きます。
3. **setLWSSOInitString** メソッドを見つけて、UCMDB の LW-SSO 設定で指定した init 文字列を指定します。
4. [setLWSSOInitString] ボタンをクリックします。

プローブでの資格情報マネージャ通信の暗号化の設定

次の手順は、UCMDB サーバが LW-SSO / 機密マネージャ設定をプローブに自動送信しないように設定されている場合に使用します。詳細については、「[サーバとプローブ間の機密マネージャ・クライアント認証設定および暗号化設定の自動同期を無効化](#)」(56ページ)を参照してください。

1. プローブ・マシンで Web ブラウザを起動し、次のアドレスを入力します。 **http://localhost:1977**

注: Probe Manager とプローブ・ゲートウェイが個別のプロセスとして実行されている場合は、Probe Manager が実行されているマシンでアドレスを入力する必要があります。

http://localhost:1978

2. **type=CMClient** をクリックして、[JMX MBEAN View] ページを開きます。
3. 次の転送関連の設定を更新します。

注: UCMDB サーバで更新した設定と同じ設定を更新する必要があります。その際、プローブで更新するメソッドの中には、複数のパラメータが必要なものもあります。プローブの現在の設定を確認するには、[JMX MBEAN View] ページで **displayTransportConfiguration** をクリックします。詳細については、「[機密マネージャ・コミュニケーション暗号化の設定](#)」(54ページ)を参照してください。更新可能な値の詳細については、「[資格情報マネージャの暗号化設定](#)」(67ページ)を参照してください。

- a. **setTransportInitString** は **encryptDecryptInitString** の設定を変更します。
 - b. **setTransportEncryptionAlgorithm** は次のマップに従ってプローブの機密マネージャ設定を変更します。
 - **エンジン名**は <engineName> エントリに対応します
 - **鍵サイズ**は <keySize> エントリに対応します
 - **アルゴリズム・パディング名**は <algorithmPaddingName> エントリに対応します
 - **PBE カウント**は <pbeCount> エントリに対応します
 - **PBE ダイジェスト・アルゴリズム**は <pbeDigestAlgorithm> エントリに対応します
 - c. **setTransportEncryptionLibrary** は次のマップに従ってプローブの機密マネージャ設定を変更します。
 - **暗号化ライブラリ名**は <cryptoSource> エントリに対応します
 - **軽量暗号化方式の以前のバージョンのサポート**は <lwJCEPBCECompatibilityMode> エントリに対応します
 - d. **setTransportMacDetails** は次のマップに従ってプローブの機密マネージャ設定を変更します。
 - **暗号化方式で MAC を使用**は <useMacWithCrypto> エントリに対応します
 - **MAC 鍵サイズ**は <macKeySize> エントリに対応します
4. **[reloadTransportConfiguration]** ボタンをクリックしてプローブで変更を有効にします。
- さまざまな設定とその値の詳細については、「[「資格情報マネージャの暗号化設定」\(67ページ\)](#)」を参照してください。

資格情報マネージャ・クライアントのキャッシュの設定

本項の内容

- [「プローブでの機密マネージャ・クライアントのキャッシュ・モードの設定」\(58ページ\)](#)
- [「プローブでの機密マネージャ・クライアントのキャッシュ暗号化文字列の設定」\(59ページ\)](#)

プローブでの機密マネージャ・クライアントのキャッシュ・モードの設定

機密マネージャ・クライアントは資格情報をキャッシュに保存し、サーバ上で情報が変更されると情報を更新します。キャッシュはファイル・システムまたはメモリ内に保存できます。

- **ファイル・システムに保存する場合**、プローブが再起動されサーバに接続できない場合であっても資格情報を利用できます。

- ・ **メモリ内に保存する場合**、プローブを再起動すると、キャッシュはクリアされすべての情報がサーバから再度取得されます。サーバを使用できない場合、プローブに資格情報は含まれないため、ディスカバリまたは統合は実行できません。

この設定を変更するには、次の手順を実行します。

1. **DataFlowProbe.properties** ファイルをテキスト・エディタで開きます。このファイルは、**c:\hp\UCMDB\DataFlowProbe\conf** フォルダにあります。
2. 次の属性を見つけます。 **com.hp.ucmdb.discovery.common.security.storeCMDData=true**
 - ・ ファイル・システムに情報を保存するには、標準設定 (**true**) をそのまま使用します。
 - ・ 情報をメモリに保存するには、「**false**」と入力します。
3. **DataFlowProbe.properties** ファイルを保存します。
4. Probe を再起動します。

プローブでの機密マネージャ・クライアントのキャッシュ暗号化文字列の設定

次の手順では、機密マネージャ・クライアントのファイル・システム・キャッシュ・ファイルの暗号化設定を変更する方法について説明します。機密マネージャ・クライアントのファイル・システム・キャッシュの暗号化設定を変更すると、ファイル・システム・キャッシュ・ファイルが再作成されます。再作成プロセスでは、プローブを再起動してUCMDBサーバと完全同期する必要があります。

1. プロブ・マシンで Web ブラウザを起動し、次のアドレスを入力します。 **http://localhost:1977**

注: Probe Manager とプローブ・ゲートウェイが個別のプロセスとして実行されている場合は、Probe Manager が実行されているマシンでアドレスを入力する必要があります。
http://localhost:1978

2. **type=CMClient** をクリックして、[JMX MBEAN View] ページを開きます。
3. 次のキャッシュ関連の設定を更新します。

注: プロブで更新するメソッドの中には、複数のパラメータが必要なものもあります。プローブの現在の設定を確認するには、[JMX MBEAN View] ページで **displayCacheConfiguration** をクリックします。

- a. **setCacheInitString** はファイル・システム・キャッシュの `<encryptDecryptInitString>` の設定を変更します。
- b. **setCacheEncryptionAlgorithm** は次のマップに従ってファイル・システム・キャッシュの設定を変更します。
 - **エンジン名**は `<engineName>` エントリに対応します
 - **鍵サイズ**は `<keySize>` エントリに対応します

- **アルゴリズム・パディング名**は <algorithmPaddingName> エントリに対応します
 - **PBE カウント**は <pbeCount> エントリに対応します
 - **PBE ダイジェスト・アルゴリズム**は <pbeDigestAlgorithm> エントリに対応します
- c. **setCacheEncryptionLibrary** は次のマップに従ってキャッシュ・ファイル・システムの設定を変更します。
- **暗号化ライブラリ名**は <cryptoSource> エントリに対応します
 - **軽量暗号化方式の以前のバージョンのサポート**は <lwJCEPBCompatibilityMode> エントリに対応します
- d. **setCacheMacDetails** は次のマップに従ってキャッシュ・ファイル・システムの設定を変更します。
- **暗号化方式で MAC を使用**は <useMacWithCrypto> エントリに対応します
 - **MAC 鍵サイズ**は <macKeySize> エントリに対応します
4. **[reloadCacheConfiguration]** ボタンをクリックしてプローブで変更を有効にします。これによりプローブが再起動されます。

注: この操作中は、プローブでジョブを実行しないようにしてください。

さまざまな設定とその値の詳細については、「[資格情報マネージャの暗号化設定](#)」(67ページ)を参照してください。

暗号化された形式による、資格情報および範囲情報のエクスポートとインポート

UCMDB サーバ間で資格情報をコピーするために、資格情報およびネットワーク範囲情報を暗号化形式でエクスポートおよびインポートできます。この操作は、システム・クラッシュ後のリカバリ、またはアップグレードのときなどに実行します。

- **資格情報をエクスポートする場合**、選択したパスワードを入力する必要があります。情報はこのパスワードで暗号化されます。
- **資格情報をインポートする場合**、DSD ファイルをエクスポートするときに設定したパスワードを使用する必要があります。

注: エクスポートした資格情報ドキュメントには、ドキュメントのエクスポート元システムで指定された範囲情報も含まれます。資格情報ドキュメントのインポート時には、範囲情報もインポートされます。

UCMDB サーバから資格情報をエクスポートするには、次の手順を実行します。

1. UCMDB サーバで、Web ブラウザを起動して次のアドレスを入力します。
http://localhost:8080/jmx-console ユーザ名とパスワードを使用してログインする必要がある場合もあります。

2. **UCMDB:service=DiscoveryManager** をクリックして、[JMX MBEAN View] ページを開きます。
3. **exportCredentialsAndRangesInformation** 操作を見つけます。次の操作を実行します。
 - 顧客 ID を入力します（標準設定は1）。
 - エクスポートしたファイルの名前を入力します。
 - パスワードを入力します。
 - エクスポートしたファイルを指定したパスワードで暗号化する場合は **isEncrypted=True** を設定し、暗号化しない場合は **isEncrypted=False** を設定します（この場合、パスワードおよびその他の機密情報はエクスポートされません）。
4. **[Invoke]** をクリックしてエクスポートします。

エクスポート・プロセスが正常に完了すると、ファイルは次の場所に保存されます。

c:\hp\UCMDB\UCMDBServer\conf\discovery\<顧客のディレクトリ>。

UCMDB サーバから資格情報をインポートするには、次の手順を実行します。

1. UCMDB サーバで、Web ブラウザを起動して次のアドレスを入力します。
http://localhost:8080/jmx-console
ユーザ名とパスワードを使用してログインする必要がある場合もあります。
2. **UCMDB:service=DiscoveryManager** をクリックして、[JMX MBEAN View] ページを開きます。
3. **importCredentialsAndRangesInformation** 操作を見つけます。
4. 顧客 ID を入力します（標準設定は1）。
5. インポートするファイルの名前を入力します。このファイルは
c:\hp\UCMDB\UCMDBServer\conf\discovery\<顧客のディレクトリ> にあります。
6. パスワードを入力します。ファイルのエクスポート時に使用したパスワードを入力する必要があります。
7. **[Invoke]** をクリックして資格情報をインポートします。

資格情報マネージャ・クライアントのログ・ファイル・メッセージ・レベルの変更

Probe には、機密マネージャ・サーバと機密マネージャ・クライアント間の機密マネージャ関連通信についての情報を含む2つのログ・ファイルがあります。ファイルは次のとおりです。

- 「[機密マネージャ・クライアント・ログ・ファイル](#)」(62ページ)
- 「[LW-SSO ログ・ファイル](#)」(62ページ)

機密マネージャ・クライアント・ログ・ファイル

security.cm.log ファイルは `c:\hp\UCMDB\DataFlowProbe\runtime\log` フォルダにあります。

ログには、機密マネージャ・サーバと機密マネージャ・クライアント間でやり取りされた情報メッセージが含まれます。標準設定では、これらのメッセージのログ・レベルは INFO に設定されています。

メッセージのログ・レベルを **DEBUG** レベルに変更するには、次の手順を実行します。

1. Data Flow Probe Manager サーバで `c:\hp\UCMDB\DataFlowProbe\conf\log` に移動します。
2. **security.properties** ファイルをテキスト・エディタで開きます。
3. 次の行
`loglevel.cm=INFO`
を次に変えます。
`loglevel.cm=DEBUG`
4. ファイルを保存します。

LW-SSO ログ・ファイル

security.lwssso.log ファイルは `c:\hp\UCMDB\DataFlowProbe\runtime\log` フォルダにあります。

このログには、LW-SSO に関する情報メッセージが含まれます。標準設定では、これらのメッセージのログ・レベルは INFO に設定されています。

メッセージのログ・レベルを **DEBUG** レベルに変更するには、次の手順を実行します。

1. Data Flow Probe Manager サーバで `c:\hp\UCMDB\DataFlowProbe\conf\log` に移動します。
2. **security.properties** ファイルをテキスト・エディタで開きます。
3. 次の行
`loglevel.lwssso=INFO`
を次に変えます。
`loglevel.lwssso=DEBUG`
4. ファイルを保存します。

暗号鍵の生成または更新

UCMDB サーバと Data Flow Probe 間の機密マネージャ通信および認証設定の暗号化または復号化に使用する暗号鍵を、生成または更新できます。生成または更新のいずれの場合も、UCMDB サーバは指定したパラメータ（鍵の長さ、追加 PBE サイクル、JCE プロバイダなど）に基づいて新しい暗号鍵を作成し、プローブに配布します。

generateEncryptionKey メソッドを実行すると、暗号鍵が新しく生成されます。この暗号鍵は安全なストレージにのみ保存され、名前などの詳細は認識されません。既存の Data Flow Probe を再インストールまたは新しいプローブを UCMDB サーバに接続する場合、新たに生成されたこの暗号鍵は新しいプローブには認識されません。このような場合、**changeEncryptionKey** メソッドを使用して暗号鍵を変更することをお勧めします。このようにすることで、Probe を再インストールまたは新しい Probe をインストールするときに、Probe JMX コンソールで **importEncryptionKey** メソッドを実行して（名前と場所を知っている）既存の鍵をインポートできます。

注:

- 鍵の作成に使用するメソッド（**generateEncryptionKey**）と鍵の更新に使用するメソッド（**changeEncryptionKey**）の違いは、**generateEncryptionKey** は新しいランダム暗号鍵を作成し、**changeEncryptionKey** は指定した名前の暗号鍵をインポートするという点です。
- インストールされた Probe の数に関わらず、システムで使用できる暗号鍵は1つのみです。

本項の内容

- [「新規暗号鍵の生成」 \(63ページ\)](#)
- [「UCMDB サーバでの暗号鍵の更新」 \(64ページ\)](#)
- [「プローブでの暗号鍵の更新」 \(65ページ\)](#)
- [「Probe Manager とプローブ・ゲートウェイが別々のマシンにインストールされている場合における暗号鍵の手動による変更」 \(66ページ\)](#)
- [「複数の JCE プロバイダの定義」 \(66ページ\)](#)

新規暗号鍵の生成

UCMDB サーバと Data Flow Probe で暗号化または復号化に使用される新しい鍵を生成できます。UCMDB サーバは、古い鍵を新しく生成した鍵と置き換え、この鍵をプローブに配布します。

JMX コンソールを使用して新しい暗号鍵を生成するには、次の手順を実行します。

1. UCMDB サーバで、Web ブラウザを起動して次のアドレスを入力します。
http://localhost:8080/jmx-console
ユーザ名とパスワードを使用してログインする必要がある場合もあります。
2. **UCMDB:service=DiscoveryManager** をクリックして、[JMX MBEAN View] ページを開きます。

3. generateEncryptionKey 操作を見つけます。
 - a. **[customerID]** パラメータ・ボックスに1 (標準設定) を入力します。
 - b. **keySize** に、暗号鍵の長さを指定します。有効な値は 128, 192, 256 です。
 - c. **usePBE** に、**True** または **False** を指定します。
 - **True にすると**、追加 PBE ハッシュ・サイクルを使用します。
 - **False にすると**、追加 PBE ハッシュ・サイクルを使用しません。
 - d. **jceVendor** には、標準設定でない JCE プロバイダの使用を選択できます。このボックスが空のときは、標準設定のプロバイダが使用されます。
 - e. **autoUpdateProbe** に、**True** または **False** を指定します。
 - **True の場合** :サーバは新しい鍵を自動的に Probe に配布します。
 - **False の場合** :新しい鍵を手動で Probe に配置してください。
 - f. **exportEncryptionKey** に、**True** または **False** を指定します。
 - **True の場合** :新しいパスワードを作成して安全なストレージに保存するほかに、サーバは新しいパスワードをファイル・システム (`c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin`) にエクスポートします。このオプションにより、新しいパスワードを使用して Probe を手動で更新できます。
 - **False の場合** :新しいパスワードはファイル・システムにエクスポートされません。Probe を手動で更新するには、**autoUpdateProbe** を **False** に設定し、**exportEncryptionKey** を **True** に設定します。

注: Probe が稼動していて、サーバに接続されていることを確認してください。Probe が停止している場合、鍵は Probe に接続できません。プローブが停止する前に鍵を変更した場合は、プローブが再起動するとそのプローブに鍵が再送信されます。ただし、Probe が停止する前に鍵を複数回変更した場合は、JMX コンソールを通して手動でその鍵を変更する必要があります (**exportEncryptionKey** に **False** を選択します)。

4. **[Invoke]** をクリックして、暗号鍵を生成します。

UCMDB サーバでの暗号鍵の更新

changeEncryptionKey メソッドを使用して独自の暗号鍵を UCMDB サーバにインポートし、すべてのプローブに配布します。

JMX コンソールを通して暗号鍵を更新するには、次の手順を実行します。

1. 「**新規暗号鍵の生成**」(63ページ) で生成した key.bin ファイルを `C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1` ディレクトリにコピーして、key.bin ファイルの名前を変更します。たとえば、key_1.bin などです。

注: 必ず key.bin ファイルの名前を変更するようにしてください。

2. UCMDB サーバで、Web ブラウザを起動して次のアドレスを入力します。
http://localhost:8080/jmx-console ユーザ名とパスワードを使用してログインする必要がある場合もあります。
3. **UCMDB:service=DiscoveryManager** をクリックして、[JMX MBEAN View] ページを開きます。
4. **changeEncryptionKey** 操作を見つけます。
 - a. **[customerID]** パラメータ・ボックスに **1** (標準設定) を入力します。
 - b. **newKeyFileName** に、新しい鍵の名前を入力します。
 - c. **keySizeInBits** に、暗号鍵の長さを指定します。有効な値は 128, 192, 256 です。
 - d. **usePBE** に、**True** または **False** を指定します。
 - **True の場合** :追加 PBE ハッシュ・サイクルを使用します。
 - **False の場合** :追加 PBE ハッシュ・サイクルを使用しません。
 - e. **jceVendor** には、標準設定でない JCE プロバイダの使用を選択できます。このボックスが空のときは、標準設定のプロバイダが使用されます。
 - f. **autoUpdateProbe** に、**True** または **False** を指定します。
 - **True の場合** :サーバは新しい鍵を自動的に Probe に配布します。
 - **False の場合** :プローブ JMX コンソールを使用して、新しい鍵を手動で配布する必要があります。

注: Probe が稼動していて、サーバに接続されていることを確認してください。Probe が停止している場合、鍵は Probe に接続できません。プローブが停止する前に鍵を変更した場合は、プローブが再起動するとそのプローブに鍵が再送信されます。ただし、Probe が停止する前に鍵を複数回変更した場合は、JMX コンソールを通して手動でその鍵を変更する必要があります (**autoUpdateProbe** に **False** を選択します)。

5. **[Invoke]** をクリックして、暗号鍵を生成および更新します。

プローブでの暗号鍵の更新

セキュリティを考慮して、暗号鍵を UCMDB サーバからすべてのプローブに自動配布しない場合、新しい暗号鍵をすべてのプローブにダウンロードし、プローブで **importEncryptionKey** メソッドを実行する必要があります。

1. 暗号鍵ファイルを **C:\hp\UCMDB\DataFlowProbe\conf\security** ディレクトリに置きます。
2. プローブ・マシンで Web ブラウザを起動し、次のアドレスを入力します。**http://localhost:1977** ユーザ名とパスワードを使用してログインする必要がある場合もあります。

注: Probe Manager とプローブ・ゲートウェイが個別のプロセスとして実行されている場合は、Probe Manager が実行されているマシンでアドレスを入力する必要があります。

```
http://localhost:1978
```

3. プローブのドメイン上で **type=SecurityManagerService** をクリックします。
4. **importEncryptionKey** メソッドを見つけます。
5. **C:\hp\UCMDB\DataFlowProbe\conf\security** に置かれる暗号鍵ファイルの名前を入力します。このファイルには、インポートされる鍵が含まれています。
6. [**importEncryptionKey**] ボタンをクリックします。
7. プローブの再起動を実行します。

Probe Manager とプローブ・ゲートウェイが別々のマシンにインストールされている場合における暗号鍵の手動による変更

1. Probe Manager マシンで、Probe Manager サービスを起動します（【スタート】 > 【プログラム】 > 【HP UCMDB】 > 【プローブ マネージャ】 を選択します）。
2. Probe Manager JMX を使用して、サーバから鍵をインポートします。詳細については、「[新規暗号鍵の生成](#)」(63ページ) を参照してください。
3. 暗号鍵のインポートが完了したら、Probe Manager およびプローブ・ゲートウェイのサービスを再起動します。

複数の JCE プロバイダの定義

JMX コンソールを使用して暗号鍵を生成する場合、**changeEncryptionKey** と **generateEncryptionKey** メソッドを使用して複数の JCE プロバイダを定義できます。

標準設定の JCE プロバイダを変更するには、次の手順を実行します。

1. **\$JRE_HOME/lib/ext** の JCE プロバイダ jar ファイルを登録します。
2. jar ファイルを **\$JRE_HOME** フォルダにコピーします。
 - UCMDB サーバの場合 :**\$JRE_HOME** へコピーします。 **c:\hp\UCMDB\UCMDBServer\bin\jre**
 - Data Flow Probe の場合 :**\$JRE_HOME** へコピーします。 **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. **\$JRE_HOME\lib\security\java.security** ファイルのプロバイダ・リストの最後にプロバイダ・クラスを追加します。
4. 無制限 JCE ポリシーを含めるように、**local_policy.jar** と **US_export_policy.jar** ファイルを更新します。これらの jar ファイルは Sun の Web サイトからダウンロードできます。
5. UCMDB サーバと Data Flow Probe を再起動します。

6. **changeEncryptionKey** または **generateEncryptionKey** メソッド用の JCE ベンダ・フィールドを見つけて、JCE プロバイダの名前を追加します。

資格情報マネージャの暗号化設定

次の表に、さまざまな JMX メソッドを使用して変更可能な暗号化設定を示します。これらの暗号化設定は、Confidential Manager のクライアントと Confidential Manager のサーバ間の通信の暗号化、および Confidential Manager のクライアントのキャッシュの暗号化に使用されます。

Confidential Manager Setting Name	プローブ資格情報マネージャの設定名	設定の詳細	利用可能な値	標準設定値
cryptoSource	暗号化ライブラリ名	この設定では、使用する暗号化ライブラリを指定します。	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBE Compatibility Mode	軽量暗号化方式の以前のバージョンのサポート	この設定では、軽量暗号化方式の以前のバージョンをサポートするかどうかを指定します。	true, false	true
engineName	エンジン名	暗号化メカニズム名	AES, DES, 3DES, Blowfish	AES
keySize	鍵サイズ	暗号鍵の長さ (ビット)	AES の場合 : 128, 192, 256。 DES の場合 : 64。 3DES の場合 : 192。 Blowfish の場合 : 32 から 448 までの任意の数値	256
algorithm Padding Name	アルゴリズム・パディング名	パディングの標準	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	PBE カウント	パスワード (初期化文字列) から鍵を作成するためにハッシュを実行す	任意の正数	20

Confidential Manager Setting Name	プローブ資格情報マネージャの設定名	設定の詳細	利用可能な値	標準設定値
		る回数		
pbeDigest Algorithm	PBE ダイジェスト・アルゴリズム	ハッシュ・タイプ	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	暗号化方式で MAC を使用	暗号化方式で MAC を使用するかどうかを指定	true, false	false
macKeySize	MAC 鍵サイズ	MAC アルゴリズムによって異なる	256	256

トラブルシューティングおよび制限事項

UCMDB サーバ上のデフォルトのドメイン名を変更する場合、まず Data Flow Probe が実行されていないことを確認する必要があります。デフォルトのドメイン名を適用した後は、Data Flow Probe 側で **DataFlowProbe\tools\clearProbeData.bat** スクリプトを実行する必要があります。

注: clearProbeData.bat スクリプトを実行すると、プローブがアップされたときにプローブ側でディスカバリ・サイクルが生じます。

第5章: Data Flow Probe の強化

本章の内容

• PostgreSQL データベースの暗号化パスワードの変更	69
• clearProbeData スクリプト: 使用法	71
• JMX コンソールに暗号化パスワードを設定	71
• UploadScanFile のパスワード設定	72
• PostgreSQL サーバへのリモート・アクセス	73
• UCMDB サーバと Data Flow Probe 間の SSL の有効化	73
• 概要	74
• キー・ストアとトラスト・ストア	74
• サーバ認証（一方向）での SSL の有効化	75
• サーバ証明書認証（双方向）の有効化	77
• エージェントまたはスキャナに対する aioptionrc ファイルの権限の変更方法	84
• Data Flow Probe のキー・ストアの作成	84
• プロブのキー・ストアとトラスト・ストアのパスワードを暗号化	85
• サーバと Data Flow Probe のデフォルトのキー・ストアとトラスト・ストア	85
• UCMDB サーバ	86
• Data Flow Probe	86
• エージェントまたはスキャナに対する aioptionrc ファイルの権限の変更方法	86

PostgreSQL データベースの暗号化パスワードの変更

本項では、PostgreSQL データベース・ユーザの暗号化されたパスワードの修正方法について説明します。

1. パスワードの暗号化形式（AES，192 ビット鍵）を作成します。
 - a. Data Flow Probe JMX コンソールにアクセスします。Web ブラウザを起動し、アドレスに「**http://<Data Flow Probe のマシン名または IP アドレス>:1977**」と入力します。Data Flow Probe をローカルで実行している場合は、**http://localhost:1977** と入力します。
ユーザ名とパスワードを使用してログインする必要がある場合もあります。

注: ユーザを作成していない場合は、標準設定のユーザ名 `sysadmin` とパスワード `sysadmin` を使用してログインします。

- b. **Type=MainProbe** サービスを見つけ、リンクをクリックして [操作] ページを開きます。
- c. **getEncryptedDBPassword** 操作を見つけます。
- d. **[DB パスワード]** フィールドに、暗号化するパスワードを入力します。
- e. **[getEncryptedDBPassword]** ボタンをクリックして操作を呼び出します。
この呼び出しの結果は、次のような暗号化されたパスワード文字列となります。

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

2. Data Flow Probe を停止します。

[スタート] > [すべてのプログラム] > [HP UCMDB] > [Data Flow Probe の停止] を選択します。

3. `set_dbuser_password.cmd` スクリプトを実行します。

このスクリプトは、次のフォルダにあります。 `C:\hp\UCMDB\DataFlowProbe\tools\dbscripts`

新しいパスワードを第1引数、PostgreSQL ルート・アカウントのパスワードを第2引数として `set_dbuser_password.cmd` スクリプトを実行します。

例:

```
set_dbuser_password <ユーザのパスワード><ルート・パスワード>
```

パスワードは、暗号化していない形式（平文）で入力する必要があります。

4. Data Flow Probe の構成ファイルにあるパスワードを更新します。

- a. 構成ファイルに書き込むパスワードは暗号化する必要があります。暗号化された形式のパスワードを取得するには、ステップ1の説明に従って `getEncryptedDBPassword JMX` メソッドを使用します。
- b. 暗号化されたパスワードを、 `C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties` ファイルの次のプロパティに追加します。

- `appilog.agent.probe.jdbc.pwd`

例:

```
appilog.agent.probe.jdbc.user = mamprobe
```

```
appilog.agent.probe.jdbc.pwd =
```

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
```

- `appilog.agent.local.jdbc.pwd`

- `appilog.agent.normalization.jdbc.pwd`

5. Data Flow Probe を起動します。

[スタート] > [すべてのプログラム] > [HP UCMDB] > [Data Flow Probe を開始] の順に選択します。

clearProbeData スクリプト: 使用法

現在のパスワードを変更せずにデータベース・ユーザを再作成するには、Windows では **clearProbeData.bat** スクリプトを実行し、Linux では **clearProbeData.sh** スクリプトを実行します。

スクリプトの実行後:

- 以下のファイルでerrorを確認してください:
C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log (Windows の場合) ,
/opt/hp/UCMDB/DataFlowProbe/runtime/log/probe_setup.log (Linux の場合)。
- データベースのパスワードが含まれているため、ファイルを削除します。

注: HP ソフトウェア・サポート によって指示を受けた場合を除いて、このスクリプトを実行しないでください。

JMX コンソールに暗号化パスワードを設定

本項では、JMX ユーザのパスワードの暗号化方法について説明します。暗号化されたパスワードは DataFlowProbe.properties ファイルに保存されます。JMX コンソールにアクセスするには、ログインする必要があります。

1. パスワードの暗号化形式 (AES, 192 ビット鍵) を作成します。
 - a. Data Flow Probe JMX コンソールにアクセスします。Web ブラウザを起動し、アドレスに **「http://<Data Flow Probe のマシン名または IP アドレス>:1977」** と入力します。Data Flow Probe をローカルで実行している場合は、**http://localhost:1977** と入力します。
ユーザ名とパスワードを使用してログインする必要がある場合もあります。

注: ユーザを作成していない場合は、標準設定のユーザ名 sysadmin とパスワード sysadmin を使用してログインします。

- b. **Type=MainProbe** サービスを見つけ、リンクをクリックして [操作] ページを開きます。
 - c. **getEncryptedKeyPassword** 操作を見つけます。
 - d. **[Key Password]** フィールドに、暗号化するパスワードを入力します。
 - e. **[getEncryptedKeyPassword]** ボタンをクリックして操作を呼び出します。
この呼び出しの結果は、次のような暗号化されたパスワード文字列となります。
85,-9,-61,11,105,-93,-81,118
2. Data Flow Probe を停止します。
[スタート] > [すべてのプログラム] > [HP UCMDB] > [Data Flow Probe の停止] を選択します。

3. 暗号化されたパスワードを,

暗号化されたパスワードを, **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** ファイルの次のプロパティに追加します。

appilog.agent.Probe.JMX.BasicAuth.Pwd

例:

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
```

```
appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,38,80,-111,-99,-64,-5,35,-122
```

注: 認証を無効にするには, これらのフィールドを空白のままにします。認証を無効にすると, ユーザは認証情報を入力せずにプローブの JMX コンソールのメイン・ページを開くことができます。

4. Data Flow Probe を起動します。

[スタート] > [すべてのプログラム] > [HP UCMDB] > [Data Flow Probe の起動] を選択します。

Web ブラウザで結果をテストします。

UploadScanFile のパスワード設定

本項では, オフサイト・スキャン保存に使用する **UpLoadScanFile** のパスワード設定方法について説明します。暗号化されたパスワードは **DataFlowProbe.properties** ファイルに保存されます。JMX コンソールにアクセスするには, ログインする必要があります。

1. パスワードの暗号化形式 (AES, 192 ビット鍵) を作成します。

- Data Flow Probe JMX コンソールにアクセスします。Web ブラウザを起動し, アドレスに **「http://<Data Flow Probe のマシン名または IP アドレス>:1977」** と入力します。Data Flow Probe をローカルで実行している場合は, **http://localhost:1977** と入力します。
ユーザ名とパスワードを使用してログインする必要がある場合もあります。

注: ユーザを作成していない場合は, 標準設定のユーザ名 **sysadmin** とパスワード **sysadmin** を使用してログインします。

- Type=MainProbe** サービスを見つけ, リンクをクリックして [操作] ページを開きます。
- getEncryptedKeyPassword** 操作を見つけます。
- [**Key Password**] フィールドに, 暗号化するパスワードを入力します。
- [**getEncryptedKeyPassword**] ボタンをクリックして操作を呼び出します。
この呼び出しの結果は, 次のような暗号化されたパスワード文字列となります。

```
85,-9,-61,11,105,-93,-81,118
```

2. Data Flow Probe を停止します。

【スタート】 > 【すべてのプログラム】 > 【HP UCMDB】 > 【Data Flow Probe の停止】 を選択します。

3. 暗号化されたパスワードを、

暗号化されたパスワードを、 `C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties` ファイルの次のプロパティに追加します。

com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd

例:

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
```

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,77,-108,14,127,4,-89,101,-33,-31,116,53
```

4. Data Flow Probe を起動します。

【スタート】 > 【すべてのプログラム】 > 【HP UCMDB】 > 【Data Flow Probe の起動】 を選択します。

Web ブラウザで結果をテストします。

PostgreSQL サーバへのリモート・アクセス

本項では、リモートのマシンからの PostgreSQL Data Flow Probe アカウントへのアクセスを許可 / 制限する方法について説明します。

注:

- 標準設定では、アクセスは制限されています。
- リモートのマシンから PostgreSQL ルート・アカウントにはアクセスできません。

PostgreSQL アクセスを許可するには、次の手順を実行します。

- コマンド・プロンプト・ウィンドウで次のスクリプトを実行します。

```
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd
```

PostgreSQL アクセスを制限するには、次の手順を実行します。

- コマンド・プロンプト・ウィンドウで次のスクリプトを実行します。

```
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd
```

UCMDB サーバと Data Flow Probe 間の SSL の有効化

Data Flow Probe と UCMDB サーバの両方で、証明書による認証を設定できます。設定すると、接続を確立する前に各コンポーネントの証明書が送信されて認証されます。

注: Data Flow Probe で SSL を有効化する方法は、最も安全で推奨される通信モードです。この方法は基本認証の手順に代わるものです。

本項の内容

- [「概要」 \(74ページ\)](#)
- [「キー・ストアとトラスト・ストア」 \(74ページ\)](#)
- [「サーバ認証 \(一方向\) での SSL の有効化」 \(75ページ\)](#)
- [「サーバ証明書認証 \(双方向\) の有効化」 \(77ページ\)](#)

概要

UCMDB は、UCMDB サーバと Data Flow Probe の間の通信で次のモードをサポートしています。

- **サーバ認証:** このモードでは、SSL を使用し、プローブは UCMDB サーバの証明書を認証します。詳細については、[「サーバ認証 \(一方向\) での SSL の有効化」 \(75ページ\)](#)を参照してください。
- **相互認証:** このモードでは、SSL を使用し、プローブによるサーバ認証とサーバによるクライアント認証の両方を実行できます。詳細については、[「サーバ証明書認証 \(双方向\) の有効化」 \(77ページ\)](#)を参照してください。
- **標準 HTTP:** SSL 通信は行われません。これは標準設定モードで、UCMDB の Data Flow Probe コンポーネントに証明書は必要ありません。Data Flow Probe は標準 HTTP プロトコルを使用してサーバと通信します。

注: SSL での作業時にはディスカバリは証明書チェーンを使用できません。そのため、証明書チェーンを使用している場合、UCMDB サーバとの通信を行うには Data Flow Probe 用のセルフ署名証明書を生成する必要があります。

キー・ストアとトラスト・ストア

UCMDB サーバと Data Flow Probe は、キー・ストアとトラスト・ストアを使用して動作します。

- **キー・ストア:** キー・エントリ (証明書および一致する秘密鍵) を保持するファイル。
- **トラスト・ストア:** リモート・ホストを検証するために使用する証明書を保持するファイル (たとえば、サーバ認証で使用する場合、Data Flow Probe のトラスト・ストアには UCMDB サーバの証明書が含まれている必要があります)。

相互認証の制限事項

C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties で定義した Data Flow Probe キー・ストアには、キー・エントリが1つだけ含まれている必要があります。

サーバ認証（一方向）での SSL の有効化

ここでは SSL を使用し、プローブはサーバの証明書を認証します。

本項の内容

- 「前提条件」(75ページ)
- 「UCMDB サーバの構成」(75ページ)
- 「Data Flow Probe 設定」(76ページ)
- 「マシンの再起動」(77ページ)

前提条件

1. UCMDB と Data Flow Probe の両方が実行されていることを確認します。

注: プローブが別々のモードでインストールされている場合、これらの手順は Probe Gateway のことを指します。

2. UCMDB または Data Flow Probe が標準設定フォルダにインストールされていない場合、正しい場所を確認してコマンドを適宜変更します。

UCMDB サーバの構成

1. UCMDB 証明書のエクスポート

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <keystore alias> -keystore <キーストアのファイル・パス> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

詳細:

- **keystore alias** はキーストアに与えられた名前です。
- **キーストアのファイル・パス**はキーストア・ファイルの場所のフル・パスです。

たとえば、定義済みの server.keystore の場合は次のコマンドを使用します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore  
C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file  
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

- b. キーストアのパスワードを入力します。たとえば、定義済みのキーストア・パスワードは **hppass** です。
- c. 証明書が次のディレクトリに作成されていることを確認します。

C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

2. UCMDB の Data Flow Probe コネクタのセキュリティ強化

- a. UCMDB JMX コンソールにアクセスします。Web ブラウザで次の URL を入力します:**http://<UCMDB マシンの名前または IP アドレス>:8080/jmx-console**。ユーザ名とパス

- ワードを使用してログインする必要がある場合もあります。
- b. 次のサービスを選択します:**Ports Management Services**。
 - c. **PortsDetails** メソッドを呼び出し、HTTPS のポート番号を確認します。(標準設定 :8443) [有効] カラムの値が [True] であることを確認します。
 - d. [**Ports Management Services**] に戻ります。
 - e. Data Flow Probe コネクタをサーバ認証モードにマップするには、次のパラメータを指定して **mapComponentToConnectors** メソッドを呼び出します。
 - o **componentName**:mam-collectors
 - o **isHTTPS**:true
 - o **ほかのすべてのフラグ** : false

次のメッセージが表示されます。

```
Operation succeeded.mam-collectors コンポーネントは、現在次のポートにマップされています:HTTPS ports
```

- f. [**Ports Management Services**] に戻ります。
- g. 資格情報マネージャ・コネクタをサーバ認証モードにマップするには、次のパラメータを指定して **mapComponentToConnectors** メソッドを呼び出します。
 - o **componentName**:cm
 - o **isHTTPS**:true
 - o **ほかのすべてのフラグ** : false

次のメッセージが表示されます。

```
Operation succeeded.cm コンポーネントは、現在次のポートにマップされています:HTTPS ports
```

3. UCMDB 証明書を各プローブ・マシンにコピー

UCMDB サーバ・マシンの証明書ファイル **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** を各 Data Flow Probe マシン上の次のフォルダにコピーします
C:\HP\UCMDB\DataFlowProbe\conf\security

Data Flow Probe 設定

注: 各 Data Flow Probe マシンに設定を行う必要があります。

1. 「**UCMDB 証明書のエクスポート**」(75ページ) で作成された **server.cert** ファイルをプローブのラスト・ストアにインポートします。
 - a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore  
C:\HP\UCMDB\DataFlowProbe\conf\security\hprobeTrustStore.jks -file  
C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
```

- b. キーストアのパスワード, logomania を入力します。
- c. **[Trust this certificate?]** と表示された場合は, **[y]** を押して **Enter** キーを押します。
次のメッセージが表示されます。

証明書がキーストアに追加されました。

2. 次の場所にある **DataFlowProbe.properties** ファイルを開きます:
C:\HP\UCMDB\DataFlowProbe\conf
 - a. **appilog.agent.probe.protocol** プロパティを **HTTPS** に更新します。
 - b. **serverPortHttps** プロパティを, ポート番号に更新します。(「[UCMDB サーバの構成](#)」(75 ページ)のステップ 2c のポート番号を使用します。)

マシンの再起動

UCMDB サーバとプローブ・マシンを両方再起動します。

サーバ証明書認証（双方向）の有効化

このモードでは, SSL を使用し, プローブによるサーバ認証とサーバによるクライアント認証の両方を実行できます。サーバとプローブの両方が, 認証のために証明書をほかのエンティティに送信します。

注: 証明書チェーンを使用して相互証明書認証を有効化することが可能です。証明書チェーンの生成の詳細については, 「[\(任意指定\) UCMDB 証明書チェーンの生成](#)」(81 ページ)を参照してください。

本項の内容

- [「前提条件」](#) (77 ページ)
- [「UCMDB サーバの初期設定」](#) (78 ページ)
- [「Data Flow Probe 設定」](#) (79 ページ)
- [「追加の UCMDB サーバの構成」](#) (81 ページ)
- [「マシンの再起動」](#) (81 ページ)

前提条件

1. UCMDB と Data Flow Probe の両方が実行されていることを確認します。

注: プローブが別々のモードでインストールされている場合, これらの手順は Probe Gateway のことを指します。

2. UCMDB または Data Flow Probe が標準設定フォルダにインストールされていない場合, 正しい場所を確認してコマンドを適宜変更します。

UCMDB サーバの初期設定

1. UCMDB 証明書のエクスポート

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <keystore alias> -keystore <キー  
ストアのファイル・パス> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

詳細:

- **keystore alias** はキーストアに与えられた名前です。
- **キーストアのファイル・パス**はキーストア・ファイルの場所のフル・パスです。

たとえば、定義済みの server.keystore の場合は次のコマンドを使用します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore  
C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file  
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

- b. キーストアのパスワードを入力します。たとえば、定義済みのキーストア・パスワードは **hppass** です。
- c. 証明書が次のディレクトリに作成されていることを確認します。
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

2. UCMDB の Data Flow Probe コネクタのセキュリティ強化

- a. UCMDB JMX コンソールにアクセスします。Web ブラウザで次の URL を入力します:**http://<UCMDB マシンの名前または IP アドレス>:8080/jmx-console**。ユーザ名とパスワードを使用してログインする必要がある場合もあります。
- b. 次のサービスを選択します:**Ports Management Services**。
- c. **PortsDetails** メソッドを呼び出し、クライアント認証で HTTPS のポート番号を確認します。(標準設定 :8444) **[有効]** カラムの値が **[True]** であることを確認します。
- d. **[Ports Management Services]** に戻ります。
- e. Data Flow Probe コネクタを相互認証モードにマップするには、次のパラメータを指定して **mapComponentToConnectors** メソッドを呼び出します。

- **componentName**:mam-collectors
- **isHTTPSWithClientAuth**: true
- **ほかのすべてのフラグ**: false

次のメッセージが表示されます。

操作は正常に完了しました。mam-collectors コンポーネントは、現在次のポートにマップされています:HTTPS_CLIENT_AUTH ポート。

- f. **[Ports Management Services]** に戻ります。
- g. 資格情報マネージャ・コネクタを相互認証モードにマップするには、次のパラメータを指定して **mapComponentToConnectors** メソッドを呼び出します。

- **componentName:cm**
- **isHTTPSWithClientAuth: true**
- **ほかのすべてのフラグ : false**

次のメッセージが表示されます。

操作は正常に完了しました。cm コンポーネントは、現在次のポートにマップされています:HTTPS_CLIENT_AUTH ポート。

3. UCMDB 証明書を各プローブ・マシンにコピー

UCMDB サーバ・マシンの証明書ファイル `C:\HP\UCMDB\UCMDBServer\conf\security\server.cert` を各 Data Flow Probe マシン上の次のフォルダにコピーします。

`C:\HP\UCMDB\DataFlowProbe\conf\security\`

Data Flow Probe 設定

注: 各 Data Flow Probe マシンに設定を行う必要があります。

1. 「UCMDB 証明書のエクスポート」(78ページ) で作成された `server.cert` ファイルをプローブのラスト・ストアにインポートします。

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore  
C:\HP\UCMDB\DataFlowProbe\conf\security\hprobeTrustStore.jks -file  
C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
```

- b. キーストアのパスワード, `logomania` を入力します。
- c. **[Trust this certificate?]** と表示された場合は, **[y]** を押して **Enter** キーを押します。

次のメッセージが表示されます。

証明書がキーストアに追加されました。

2. `client.keystore` ファイルの新規作成

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool -genkey -alias <プローブ名> -keyalg RSA -  
sigalg SHA256withRSA -keysize 2048 -keystore  
c:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
```

ここでは, **ProbeName** は Data Flow Probe の一意のエイリアスを示します。

注: このエイリアスが一意であることを確認するには, プローブ定義時にプローブに付与されたプローブ名識別子を使用します。

- b. キーストアのパスワードを6文字以上で入力し, その文字をメモしておきます。
- c. 確認のために再度パスワードを入力します。
- d. 次の各質問に回答し, **Enter** を押します。

あなたの氏名を教えてください。[不明]:

あなたの部署名を教えてください。[不明]:

あなたの組織を教えてください。[不明]:

あなたの住所（市以下）を教えてください。[不明]:

あなたの住所（都道府県）を教えてください。[不明]:

このユニットの 2 文字の国コードを教えてください。[不明]:

- e. 「CN=不明, OU=不明, O=不明, L=不明, ST=不明, C=不明でよろしいですか?」と表示されたらはいと入力します。
- f. 次の質問に回答して, **Enter** を押します。
<probekey> のキー・パスワードを入力します (キーストア・パスワードと同じ場合は戻る)。
- g. ファイルが次のフォルダに作成されており, そのファイル・サイズが 0 以上であることを確認します。 **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. 新しいクライアント証明書のエクスポート

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias <ProbeName> -keystore  
C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file  
C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert
```

- b. 求められたらキーストアのパスワードを入力します。(上記[ステップ 2b](#)のパスワード。)
次のメッセージが表示されます。

<C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert> のファイルに保存されている証明書

4. 次の場所にある DataFlowProbe.properties ファイルを開きます:

C:\HP\UCMDB\DataFlowProbe\conf

- a. **appilog.agent.probe.protocol** プロパティを **HTTPS** に更新します。
- b. **serverPortHttps** プロパティを, ポート番号に更新します。(「[UCMDB サーバの初期設定 \(78 ページ\)](#)」の [ステップ 2c](#) のポート番号を使用します。)

5. 次の場所にある ssl.properties ファイルを開きます:C:\HP\UCMDB\DataFlowProbe\conf\security\

- a. **javax.net.ssl.keyStore** プロパティを **client.keystore** に更新します。
- b. 上記[ステップ 2b](#)のパスワードを暗号化します。
 - i. Data Flow Probe を起動するか, すでに実行されていることを確認します。
 - ii. Probe JMX にアクセスします。次の場所を参照します。 **http://<probe_hostname>:1977**

たとえば, プロブをローカルで実行している場合は次の場所を参照します。
http://localhost:1977

- iii. **type=MainProbe** のリンクをクリックします。
- iv. **getEncryptedKeyPassword** の操作まで下にスクロールします。
- v. **[Key Password]** フィールドにパスワードを入力します。
- vi. **[getEncryptedKeyPassword]** ボタンを押します。

- c. 暗号化したパスワードをコピーおよび貼り付けして **javax.net.ssl.keyStorePassword** プロパティを更新します。

注: 数字はカンマで区切ります。例: -20,50,34,-40,-50.)

6. プローブ証明書を UCMDB マシンにコピー

C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert のファイルを Data Flow Probe マシンから **C:\HP\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert** の UCMDB マシンにコピーします。

追加の UCMDB サーバの構成

1. 各プローブ証明書の UCMDB トラスト・ストアへの追加

注: 各プローブ証明書ごとに次のステップを実施する必要があります。

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.truststore -file  
C:\hp\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert -alias <ProbeName>
```
- b. キーストアのパスワードを入力します。たとえば、定義済みのキーストア・パスワードは **hppass** です。
- c. **[Trust this certificate?]** と表示された場合は、**[y]** を押して **Enter** キーを押します。
次のメッセージが表示されます。

証明書がキーストアに追加されました

マシンの再起動

UCMDB サーバとプローブ・マシンを両方再起動します。

(任意指定) UCMDB 証明書チェーンの生成

1. キーストアの生成

次の手順を開始する前に、**C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore** にある古い **server.keystore** ディレクトリを削除してください。

- a. コマンド・プロンプトを開いて次のコマンドを実行します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool -genkey -alias <keystore alias> -keyalg RSA -sigalg  
SHA256withRSA -keysize 2048 -keystore <Keystore file path>
```

説明:

- **keystore alias** はキーストアに与えられた名前です。
 - **Keystore file path** はキーストア・ファイルの場所のフル・パスです。
- b. キーストアのパスワードを6文字以上で入力し、その文字をメモしておきます。
キーストアのパスワードを入力します。

- パスワードが変更された場合は、**UCMDB:service=Security Services** で JMX 操作 **changeKeystorePassword** を実行します。
 - パスワードが変更されていない場合、標準設定のパスワード **hpasswd** を使用します。
- c. 確認のために再度パスワードを入力します。
- d. 次の各質問に回答し、**Enter** を押します。

- **あなたの氏名を教えてください。**

[不明]: [共通名 (CN)]

CN は正しく入力される必要があります。CN は完全修飾ドメイン名 (FQDN) である必要があります。「sitename」のような単語の短縮名や IP アドレスは受け入れられません。

有効な FQDN の例は次のとおりです。

www.sitename.com

sitename.com

sitename.hp.com

sitename.eds.com

- **あなたの部署名を教えてください。**

[不明]: [組織単位 (OU)]

注: このフィールドはあらゆる形式の会社名 (HP, Hewlett-Packard, Google など) を参照しないようにします。所属する組織の CSR が、(HP が推奨しているように) このフィールドを空白にすることを認めていない場合は、ある種の部署 (オンライン、経理、財務など) を参照するようにします。このフィールドが正しく入力されていない場合、登録が失敗する原因になります。

- **あなたの組織を教えてください。**

[不明]: [組織 (O)]

組織の名前を入力します。たとえば、**Hewlett-Packard** です。

- **あなたの住所 (市以下) を教えてください。**

[不明]: [市区町村 (L)]

SSL 証明書が存在するサーバの市区町村を入力します。このフィールドは空白にできません。

- **あなたの住所 (都道府県) を教えてください。**

[不明]: [都道府県 (S)]

SSL 証明書が存在するサーバの都道府県を入力します。都道府県はすべての文字を入力し (3 文字以上)、短縮することはできません。(たとえば、**CO** ではなく **Colorado** と入力します)。このフィールドは空白にできません。

- **このユニットの 2 文字の国コードを教えてください。**

[不明]: [国 (C)]

SSL 証明書が存在するサーバの国を入力します。2 文字の ISO 3166 国番号を入力する必要があります。このフィールドは空白にできません。

- e. **Is CN=[XXX], OU=[XXXX], O=[XXXX], L=[XXXX], ST=[XXXX], C=[XXX] correct?** と表示された場合は **y** を入力します。
- f. 次の質問に回答して、**Enter** を押します。
<serverkey> のキー・パスワードを入力します（キーストア・パスワードと同じ場合は戻る）。
新しいパスワードを再入力します。
- g. ファイルが次のフォルダに作成されており、そのファイル・サイズが 0 以上であることを確認します。 **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**

2. CSR の生成

次のコマンドを実行して CSR を生成します。

```
c:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool -certreq -alias server -file  
c:\HP\UCMDB\UCMDBServer\conf\security\certreq.csr -keystore  
c:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -sigalg SHA256withRSA
```

3. サーバのプライベート証明書の取得

- a. CA ルート証明書を最初にダウンロードし、それを信頼されたルート証明書機関としてインストールします。
- b. サフィックスを **.cer** または **.crt** に変更します。
- c. 証明書ファイルを次のディレクトリに置きます。
C:\HP\UCMDB\UCMDBServer\conf\security\serverserver.cer

4. 証明書チェーンの生成

- a. 次のコマンドを使用してルート証明書をキーストアにインポートします。

```
c:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool -import -v -trustcacerts -alias root -keystore  
c:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -file  
c:\HP\UCMDB\UCMDBServer\conf\security\server.cer
```

- b. 次のコマンドを使用してサーバ証明書をキーストアにインポートします。

```
c:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool -import -v -trustcacerts -alias server -keystore  
c:\HP\UCMDB\UCMDBServer\conf\security\server.keystore -file  
c:\HP\UCMDB\UCMDBServer\conf\security\server.cer
```

注: このエイリアス名はキーストア生成時のエイリアス名に等しくなくてはなりません。また、インポートの順序は変更できません。

- c. 証明書チェーンが生成されます。

次のコマンドを使用してキーストアの詳細を表示します。

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -list -v -keystore  
C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
```

注: プローブ証明書チェーンを生成するには、上記の手順を繰り返します。異なる点は、エイリアス名を「client」にすることと、**client.keystore**および**client.cer**ファイルを生成することのみです。

エージェントまたはスキャナに対する aioptionrc ファイルの権限の変更方法

/.discagent/aioptionrc ファイルは、World-writable でその標準設定の権限は 666 に設定されています。ユーザが **-home** オプション（エージェントのインストールおよびスキャナ用）を使用して、**aioptionrc** ファイル・パスを特定の固定ディレクトリに設定する場合は、このファイルの標準設定の権限で異なるユーザがインベントリ・ジョブを自動的に実行（**sudo** 設定済み）またはスキャナを手動で実行することを許可します。

エージェントまたはスキャナに対する **aioptionrc** ファイルの権限を変更するには、次の手順を実行します。

1. スキャン後スクリプト・エディタを開きます。
スキャン後スクリプト・エディタにアクセスする方法の詳細については、『HP Universal CMDB データ・フロー管理ガイド』のPre/Post-Scan Script Editorを参照してください。
2. **chmod o-w ./aioptionrc** コマンドを、UNIX オペレーティング・システム用のスキャナのポスト・スクリプトに追加します。
スキャン後スクリプトを編集する方法の詳細については、『HP Universal CMDB データ・フロー管理ガイド』のHow to Edit Pre-/Post-Scan Scriptsを参照してください。
3. 結果
ファイルの権限が変更され、エージェントをインストールするかスキャナを実行する最初のユーザが唯一のユーザになります。

注: 同じグループ内の所有者とユーザは、ファイルに対して同じ書き込み権限を持ちます。

Data Flow Probe のキー・ストアの作成

1. プローブ・マシンで、次のコマンドを実行します。

```
c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool -genkey -alias <プローブ名> -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -keystore c:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
```
2. 新しいキー・ストアのパスワードを入力します。
3. 必要に応じて情報を入力します。
4. **[Is CN=... C=... Correct?]** と表示された場合は、**[はい]** と入力して **Enter** キーを押します。

5. もう一度 **Enter** キーを押して、そのキー・ストア・パスワードをキー・パスワードとして受け入れます。
6. **client.keystore** が次のディレクトリに作成されていることを確認します。
C:\HP\UCMDB\DataFlowProbe\conf\security

プローブのキー・ストアとトラスト・ストアのパスワードを暗号化

プローブのキー・ストアとトラスト・ストアのパスワードは、暗号化されて **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties** に保存されます。次の手順では、パスワードの暗号化方法について説明します。

1. Data Flow Probe を起動するか、すでに実行されていることを確認します。
2. Data Flow Probe JMX コンソールへのアクセス: Web ブラウザを起動し、アドレスに `http://<Data Flow Probe のマシン名または IP アドレス>:1977` と入力します。ローカルで Data Flow Probe を実行している場合は、`http://localhost:1977` と入力します。

注: ユーザ名とパスワードを使用してログインする必要がある場合もあります。ユーザを作成していない場合は、標準設定のユーザ名 `sysadmin` とパスワード `sysadmin` を使用してログインします。

3. **Type=MainProbe** サービスを見つけ、リンクをクリックして [操作] ページを開きます。
4. **getEncryptedKeyPassword** 操作を見つけます。
5. [キー パスワード] フィールドにキー・ストアまたはトラスト・ストアのパスワードを入力し、[**getEncryptedKeyPassword**] をクリックして操作を呼び出します。
6. この呼び出しの結果は、次のような暗号化されたパスワード文字列となります。
`66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61`
7. 暗号化したパスワードをコピーし、次のファイルのキー・ストアまたはトラスト・ストアの関連する行に貼り付けます。 **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**

サーバと Data Flow Probe のデフォルトのキー・ストアとトラスト・ストア

本項の内容

- [「UCMDB サーバ」 \(86ページ\)](#)
- [「Data Flow Probe」 \(86ページ\)](#)

UCMDB サーバ

ファイルは次のディレクトリにあります。 **C:\HP\UCMDB\UCMDBServer\conf\security**

エンティティ	ファイル名 / 用語	パスワード / 語句	エイリアス
サーバのキー・ストア	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
サーバのトラスト・ストア	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	hpcert (標準設定の信頼されるエントリ)
クライアントのキー・ストア	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

ファイルは次のディレクトリにあります。 **C:\HP\UCMDB\DataFlowProbe\conf\security**

エンティティ	ファイル名 / 用語	パスワード / 語句	エイリアス
プローブのキー・ストア	hprobeKeyStore.jks (pKeyStoreFile)	logomania (pKeyStorePass)	hprobe
相互認証手順で Data Flow Probe は、 cKeyStoreFile キー・ストアを標準設定キー・ストアとして使用します。これは UCMDB インストールの一部であるクライアント・キー・ストアです。			
プローブのトラスト・ストア	hprobeTrustStore.jks (pTrustStoreFile)	logomania (pTrustStorePass)	hprobe (標準設定の信頼されるエントリ)
cKeyStorePass パスワードは cKeyStoreFile の標準設定のパスワードです。			

エージェントまたはスキャナに対する aioptionrc ファイルの権限の変更方法

./discagent/aioptionrc ファイルは、World-writable でその標準設定の権限は 666 に設定されています。ユーザが **-home** オプション (エージェントのインストールおよびスキャナ用) を使用して、**aioptionrc** ファイル・パスを特定の固定ディレクトリに設定する場合は、このファイルの標準設定の

権限で異なるユーザがインベントリ・ジョブを自動的に実行 (**sudo** 設定済み) またはスキャナを手動で実行することを許可します。

エージェントまたはスキャナに対する **aioptionrc** ファイルの権限を変更するには、次の手順を実行します。

1. スキャン後スクリプト・エディタを開きます。

スキャン後スクリプト・エディタにアクセスする方法の詳細については、『HP Universal CMDB データ・フロー管理ガイド』のPre/Post-Scan Script Editorを参照してください。

2. **chmod o-w ./aioptionrc** コマンドを、UNIX オペレーティング・システム用のスキャナのポスト・スクリプトに追加します。

スキャン後スクリプトを編集する方法の詳細については、『HP Universal CMDB データ・フロー管理ガイド』のHow to Edit Pre-/Post-Scan Scriptsを参照してください。

3. 結果

ファイルの権限が変更され、エージェントをインストールするかスキャナを実行する最初のユーザが唯一のユーザになります。

注: 同じグループ内の所有者とユーザは、ファイルに対して同じ書き込み権限を持ちます。

第6章: Lightweight シングル・サインオン (LW-SSO) 認証

本章の内容

- LW-SSO 認証の概要 88
- LW-SSO のシステム要件 89
- LW-SSO のセキュリティに関する警告 90
- トラブルシューティングおよび制限事項 91
 - 既知の問題 91
 - 制限事項 92

LW-SSO 認証の概要

LW-SSO とは、一度ログオンしたユーザであれば、再びログオンせずに複数のソフトウェア・システムのリソースにアクセスできるようにするアクセス制御方法の1つです。設定されたソフトウェア・システムのグループに属するアプリケーションは、認証されていることを信用しているため、アプリケーションから別のアプリケーションに移動するときにさらに認証処理を行う必要がありません。

このセクションの情報は、LW-SSO バージョン 2.2 および 2.3 に適用されます。

• LW-SSO トークンの期限

LW-SSO トークンの期限の数値により、アプリケーションのセッションの有効性が判断されます。そのため、期限の数値は、アプリケーションのセッション期限の数値と同じか、またはそれよりも大きな値にする必要があります。

• LW-SSO トークンの期限の推奨設定

LW-SSO を使用するアプリケーションごとに、トークンの期限を設定する必要があります。推奨値は 60 分です。高度なセキュリティを必要としないアプリケーションの場合、値を 300 分に設定できます。

• GMT 時間

LW-SSO に統合されているアプリケーションでは、すべて同じ GMT 時間を使用し、最大誤差を 15 分に抑える必要があります。

• マルチドメイン機能

マルチドメイン機能では、LW-SSO 統合を行うアプリケーションを、異なる DNS ドメインのアプリケーションと統合する必要がある場合、それらすべてのアプリケーションで trustedHosts 設定

(または **protectedDomains** 設定) を行う必要があります。さらに、設定の **lwso** 要素に正しいドメインを追加する必要があります。

- **URL 機能での SecurityToken の取得**

ほかのアプリケーションから **URL に対する SecurityToken** として送信された情報を取得するには、ホスト・アプリケーション設定の **lwso** 要素で、正しいドメインを設定する必要があります。

LW-SSO のシステム要件

アプリケーション	バージョン	コメント
Java	1.5 以降	
HTTP サーブレット API	2.1 以降	
Internet Explorer	6.0 以降	ブラウザで、HTTP セッション cookie と HTTP 302 リダイレクト機能を有効にする必要あり。
Firefox	2.0 以降	ブラウザで、HTTP セッション cookie と HTTP 302 リダイレクト機能を有効にする必要あり。
JBoss 認証	JBoss 4.0.3 JBoss 4.3.0	
Tomcat 認証	スタンドアロン Tomcat 5.0.28 スタンドアロン Tomcat 5.5.20	
Acegi 認証	Acegi 0.9.0 Acegi 1.0.4	
Web サービス・エンジン	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

LW-SSO のセキュリティに関する警告

本項では、LW-SSO 設定に関するセキュリティの警告について説明します。

- **LW-SSO の `initString` 機密パラメータ** : LW-SSO では、対称暗号化方式を使用して LW-SSO トークンを検証および作成します。設定内にある `initString` パラメータは、秘密鍵の初期化に使用します。アプリケーションでトークンが作成され、同じ `initString` パラメータを使用するアプリケーションにより、トークンが検証されます。

注意:

- **`initString` パラメータの設定を行わずに LW-SSO を使用することはできません。**
 - **`initString` パラメータは機密情報なので、公開、転送、永続性などの点で慎重に扱う必要があります。**
 - **`initString` パラメータは、LW-SSO を使用して相互に統合されたアプリケーション間でのみ共有する必要があります。**
 - **`initString` パラメータは、12 文字以上の長さである必要があります。**
-
- **必要な場合のみ LW-SSO を有効化** : 特に必要な場合を除き、LW-SSO を無効にする必要があります。
 - **認証セキュリティのレベル** : 最も弱いタイプの認証フレームワークを使用し、他の統合アプリケーションで信頼されている LW-SSO トークンを発行するアプリケーションにより、アプリケーション全体の認証セキュリティ・レベルが決まります。
強力で安全な認証フレームワークを使用するアプリケーションの場合のみ、LW-SSO トークンを発行することをお勧めします。
 - **対称暗号化方式の影響** : LW-SSO では、対称暗号化方式を使用して LW-SSO トークンを発行および検証します。そのため、LW-SSO を使用するアプリケーションから、同じ `initString` パラメータを共有する、その他すべてのアプリケーションに信頼されたトークンを発行できます。これにより、`initString` を共有するアプリケーションが、信頼できない場所に置かれているか、またはそのような場所からアクセスできる場合、リスクが発生する場合があります。
 - **ユーザ・マッピング (同期)** : LW-SSO フレームワークでは、統合アプリケーション間のユーザ・マッピングが保証されていません。そのため、統合アプリケーションでユーザ・マッピングを監視する必要があります。すべての統合アプリケーションで、同じユーザ・レジストリ (LDAP/AD など) を共有することをお勧めします。
ユーザのマッピングに失敗すると、セキュリティ違反が発生し、アプリケーションの動作不良が起こる場合があります。たとえば、さまざまなアプリケーションで複数の実際のユーザに同じユーザ名が割り当てられることがあります。
さらに、ユーザのマッピングに失敗した場合、ユーザがあるアプリケーション (AppA) にログオンしてから、コンテナ認証またはアプリケーション認証を使用する別のアプリケーション

(AppB) にアクセスすると、そのユーザが手動で AppB にログオンしてユーザ名を入力することになります。ユーザが AppA へのログオンに使用していたのは別のユーザ名を入力した場合、次のような動作が発生する場合があります。その後ユーザが AppA または AppB から第 3 のアプリケーション (AppC) にアクセスすると、AppA または AppB へのログオンに使用していたユーザ名で、AppC にアクセスしてしまいます。

- **ID マネージャ**: 認証のために使用します。ID マネージャ内の保護されていないリソースはすべて、LW-SSO 構成ファイル内で **nonsecureURLs** に設定する必要があります。
- **LW-SSO のデモ・モード**:
 - デモ・モードは、デモ目的にのみ使用してください。
 - デモ・モードは、保護されていないネットワークでのみ使用してください。
 - デモ・モードは、実運用で使用しないでください。実運用モードとデモ・モードは、どのような形でも併用しないでください。

トラブルシューティングおよび制限事項

本項では、LW-SSO 認証作業時の既知の問題および制限について説明します。

既知の問題

本項では、LW-SSO 認証の既知の問題について説明します。

- **セキュリティ・コンテキスト**: LW-SSO のセキュリティ・コンテキストでは、1つの属性名につき1つの属性値のみがサポートされています。
そのため、SAML2 トークンから、同じ属性名の値が複数送信されても、LW-SSO フレームワークで許可される値は1つのみです。
同様に、同じ属性名に対して値を複数送信するように IdM トークンが設定されていても、LW-SSO フレームワークで許可される値は1つのみです。
- **Internet Explorer 7 を使用したマルチドメインのログアウト機能**: マルチドメインのログアウト機能は、次の条件下で失敗することがあります。
 - ブラウザに Internet Explorer 7 を使用していて、アプリケーションのログアウト手順で HTTP 302 リダイレクトの動作が3回を超え連続して呼び出されたとき

この場合、Internet Explorer 7 で HTTP 302 リダイレクトの応答が正しく処理されず、**[Internet Explorer ではこのページは表示できません]** というエラー・ページが表示される場合があります。

回避策としては、アプリケーションのログアウト手順で、できるだけリダイレクト・コマンドの数を少なくすることを推奨します。

制限事項

LW-SSO 認証を行う際、次の制限に注意してください。

• アプリケーションへのクライアント・アクセス:

ドメインが LW-SSO 設定で定義されている場合:

- アプリケーションのクライアントは、ログイン URL に FQDN (完全修飾ドメイン名) を使用してアプリケーションにアクセスする必要があります (http://myserver. **企業ドメイン名** .com/WebApp など)。

注: FQDN の長さはインフラストラクチャ設定マネージャの [ドメイン拡張子の最大長] 設定の値よりも長くなることはできません。標準設定値は 8 です。

- LW-SSO では、IP アドレスを使用した URL はサポートされていません (http://192.168.12.13/WebApp など)。
- LW-SSO では、ドメインのない URL はサポートされていません (http://myserver/WebApp など)。

ドメインが LW-SSO 設定で定義されていない場合: クライアントは、ログイン URL で FQDN を持たないアプリケーションにアクセスできます。この場合、LW-SSO のセッション cookie は、一切のドメイン情報を持たない単一のマシン専用で作成されます。そのため、この cookie がほかのブラウザに委譲されたり、同じ DNS ドメインにある別のコンピュータに渡されることはありません。つまり、LW-SSO は同じドメインで機能しないことを意味します。

- **LW-SSO フレームワークの統合:** アプリケーションで LW-SSO の機能を活用できるのは、あらかじめ LW-SSO フレームワーク内に統合されている場合のみです。

• マルチドメインのサポート:

- マルチドメイン機能は、HTTP リファラに基づいています。そのため LW-SSO では、アプリケーション間のリンクはサポートされていますが、2つのアプリケーションが同じドメインにある場合を除き、ブラウザ・ウィンドウへの URL の入力にはサポートされていません。

- **HTTP POST** を使用したドメイン間のリンクはサポートされていません。

最初のクロス・ドメイン・リンクに **HTTP POST** を使用することはサポートされていません。(HTTP GET 要求のみサポートされています)。たとえば、最初のアプリケーションから 2 番目のアプリケーションへの HTTP リンクがある場合、**HTTP GET** 要求はサポートされていますが、**HTTP FORM** 要求はサポートされていません。2 回目以降の要求は、すべて **HTTP POST** か **HTTP GET** のいずれかです。

- LW-SSO トークンのサイズ:

LW-SSO が、あるドメインのアプリケーションから別のドメインのアプリケーションに転送できる情報は、15 グループ/ロール/属性までに制限されています (各項目は平均 15 文字長)。

- マルチドメイン・シナリオでの、保護されたページ (HTTPS) から保護されていないページ (HTTP) へのリンク:

保護されたページ (HTTPS) から保護されていないページ (HTTP) にリンクする場合、マルチドメインは機能しません。これはブラウザの制限事項の1つです。この場合、保護されたりソースから保護されていないリソースにリンクするときに、リファラ・ヘッダが送信されません。具体例については、<http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP> を参照してください。

- サードパーティ cookie の Internet Explorer での動作:

Microsoft Internet Explorer 6 には、「P3P (Platform for Privacy Preferences) プロジェクト」をサポートするモジュールが含まれています。そのため、サードパーティ・ドメインの cookie は、[インターネット] セキュリティ・ゾーンの標準設定でブロックされています。IE では、セッションの cookie もサードパーティ cookie とみなされるため、セッションの cookie もブロックされてしまい、LW-SSO が機能しません。詳細については、次を参照してください:<http://support.microsoft.com/kb/323752/en-us>。

この問題を解決するには、起動したアプリケーション (または *.mydomain.com などの DNS ドメイン・サブセット) を、コンピュータの [イントラネット] または [信頼済みサイト] ゾーンに追加します (Microsoft Internet Explorer で、メニュー > [ツール] > [インターネット オプション] > [セキュリティ] > [ローカル イントラネット] > [サイト] > [詳細] を選択します)。こうすることで、cookie が許可されます。

注意: LW-SSO のセッション cookie は、ブロックされているサードパーティ・アプリケーションで使用する cookie の1つにすぎません

• SAML2 トークン

- SAML2 トークンを使用する場合、ログアウト機能がサポートされません。

そのため、SAML2 トークンを使用して2番目のアプリケーションにアクセスすると、最初のアプリケーションからログアウトするユーザが、2番目のアプリケーションからログアウトされません。

- SAML2 トークンの期限切れは、アプリケーションのセッション管理に反映されません。

そのため、SAML2 トークンを使用して2番目のアプリケーションにアクセスする場合、各アプリケーションのセッション管理が個別に処理されます。

- JAAS Realm : Tomcat の JAAS Realm はサポートされていません。

- Tomcat ディレクトリでのスペースの使用 : Tomcat のスペースの使用はサポートされていません。

Tomcat のインストール・パス (フォルダ) にスペースが含まれており (「Program Files」など)、かつ LW-SSO 構成ファイルが Tomcat の **common\classes** フォルダに置かれている場合は、LW-SSO を使用できません。

- ロード・バランサの設定 : LW-SSO によりデプロイされたロード・バランサは、セッション維持を使用するよう設定する必要があります。

- **デモ・モード**: デモ・モードでは、LW-SSO ではアプリケーション間のリンクはサポートされませんが、この場合は HTTP リファラ・ヘッダが存在しないため、ブラウザ・ウィンドウへの URL 入力はサポートされません。

第7章: HP Universal CMDB ログイン認証

本章の内容

- 認証メソッドの設定 95
- HP Universal CMDB への LW-SSO によるログインを有効化 96
- SSL (Secure Sockets Layer) プロトコルによるセキュア接続の設定 96
- JMX コンソールを使用した LDAP 接続のテスト 98
- LDAP 認証メソッドを有効化および定義する方法 98
- JMX コンソールを使用して LDAP 認証メソッドを有効化および定義する方法 100
- LDAP 認証設定 - 例 101
- 分散化環境における現在の LW-SSO 設定の取得 102

認証メソッドの設定

認証は次の方法で行うことができます。

- **内部 HP Universal CMDB サービスに対して。**
- **Lightweight Directory Access Protocol (LDAP)** を使用 : 内部 HP Universal CMDB サービスを使用する代わりに、専用の外部 LDAP サーバを使用して認証情報を格納できます。LDAP サーバは、すべての HP Universal CMDB サーバと同じサブネット上になければなりません。
LDAP の詳細については、『HP Universal CMDB 管理ガイド』の LDAP マッピングに関する項を参照してください。
標準設定の認証メソッドは内部 HP Universal CMDB サービスを使用します。標準設定のメソッドを使用する場合には、システムに変更を加える必要はありません。
これらのオプションは、ユーザインタフェースを介してだけでなく、Web サービスを介して実行されたログインにも適用されます。
- **LW-SSO を使用** : HP Universal CMDB には LW-SSO を設定します。HP Universal CMDB にログインをすることで、同じドメインで実行されているほかの設定済みのアプリケーションにログインしなくても自動的にアクセスできるようになっています。
LW-SSO 認証サポートを有効にする場合 (標準設定は無効)、シングル・サインオン環境のほかのアプリケーションも LW-SSO が有効になっており、同じ `initString` パラメータで機能することを確認してください。

HP Universal CMDB への LW-SSO によるログインを有効化

1. Web ブラウザのアドレスに `http://<サーバ名>:8080/jmx-console` と入力します。<サーバ名>には HP Universal CMDB がインストールされているマシンの名前が入ります。
2. **UCMDB-UI** の下で、**name=LW-SSO Configuration** をクリックして [操作] ページを開きます。
3. **setInitString** メソッドを使用して初期化文字列を設定します。
4. **setDomain** メソッドを使用して、UCMDB をインストールするマシンのドメイン名を設定します。
5. パラメータを「True」に設定して **setEnabledForUI** メソッドを呼び出します。
6. **任意指定**: 複数ドメイン機能を使用して作業する場合、**addTrustedDomains** メソッドを選択してドメイン値を入力し、[Invoke] をクリックします。
7. **任意指定**: リバース・プロキシを使用して作業する場合は、**updateReverseProxy** メソッドを選択し、[Is reverse proxy enabled] パラメータを [True] に設定して [Reverse proxy full server URL] パラメータの URL を入力して [Invoke] をクリックします。UCMDB への直接アクセス、および、リバース・プロキシを使用してのアクセスのどちらも行いたい場合は、次の追加構成を設定してください。**setReverseProxyIPs** メソッドを選択し、リバース・プロキシ ip/s パラメータの IP アドレスを入力して [Invoke] をクリックします。
8. **任意指定**: 外部認証ポイントを使用して UCMDB にアクセスする場合は、**setValidationPointHandlerEnable** メソッドを選択して [Is validation point handler enabled] パラメータを [True] に設定し、[Authentication point server] パラメータの認証ポイントの URL を入力して [Invoke] をクリックします。
9. 設定メカニズムに保存されているとおりに LW-SSO 設定を表示するには、**retrieveConfigurationFromSettings** メソッドを呼び出します。
10. 実際ロードされた LW-SSO 設定を表示するには、**retrieveConfiguration** メソッドを呼び出します。

注: ユーザ・インターフェースから LW-SSO を有効化することはできません。

SSL (Secure Sockets Layer) プロトコルによるセキュア接続の設定

ログイン処理では、HP Universal CMDB と LDAP サーバの間で機密情報がやり取りされるため、その内容に対して一定のレベルのセキュリティを適用するとよいでしょう。それには、LDAP サーバ上で SSL 通信を有効にして、SSL を使用できるように HP Universal CMDB を設定します。

HP Universal CMDB では、信頼できる認証局 (CA) から発行された証明書を使用する SSL をサポートしています。

Active Directory を含む大半の LDAP サーバは、SSL ベースの接続を対象とするセキュリティ保護されたポートを公開できます。プライベート CA を利用する Active Directory を使用している場合、当該 CA を JRE の信頼できる CA に追加する必要があります。

SSL 通信をサポートするように HP Universal CMDB プラットフォームを設定する方法の詳細については、「[Secure Sockets Layer \(SSL\) 通信の有効化](#)」(17ページ)を参照してください。

SSL ベースの接続を対象とするセキュリティ保護されたポートを公開するために、信頼できる CA に CA を追加するには、次の手順を実行します。

1. CA から証明書をエクスポートし、次の手順に従って、HP Universal CMDB で使用される JVM にインポートしてください。
 - a. UCMDB サーバ・マシンで、**UCMDBServer\bin\JRE\bin** フォルダにアクセスします。
 - b. 次のコマンドを実行します。

```
Keytool -import -file <自分の証明書ファイル> -keystore  
C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
```

例:

```
Keytool -import -file c:\ca2ss_ie.cer -keystore  
C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
```

2. **[管理] > [インフラストラクチャ設定] > [LDAP 全般]** カテゴリを選択します。

注: JMX コンソールを使用してこれらを設定することも可能です。詳細については、「[JMX コンソールを使用して LDAP 認証メソッドを有効化および定義する方法](#)」(100ページ)を参照してください。

3. **[LDAP サーバ URL]** を見つけ、次の形式で値を入力します。

```
ldaps://<ldapHost>[:<port>]/[<baseDN>][??scope]
```

例:

```
ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

ldaps の **s** に注意してください。

4. 新しい値を保存するには **[保存]** を、エントリを標準設定値 (空白の URL) で置き換えるには **[標準設定に戻す]** をクリックします。

JMX コンソールを使用した LDAP 接続のテスト

本項では、JMX コンソールを使用して LDAP 認証設定をテストする方法について説明します。

1. Web ブラウザを起動して、次のアドレスを入力します。 **http://<サーバ名>:8080/jmx-console**。
<サーバ名> には HP Universal CMDB がインストールされているマシンの名前が入ります。
ユーザ名およびパスワードでのログインが必要な場合もあります。
2. **UCMDB** で、 **UCMDB:service=LDAP Services** をクリックして [操作] ページを開きます。
3. **testLDAPConnection** を見つけます。
4. [顧客 ID] パラメータの [値] ボックスに、顧客 ID を入力します。
5. [Invoke] をクリックします。

LDAP 接続が成功したかどうか JMX MBEAN 操作結果ページに示されます。接続が成功した場合は、LDAP ルート・グループもこのページに表示されます。

LDAP 認証メソッドを有効化および定義する方法

HP Universal CMDB システムを対象に LDAP 認証メソッドの有効化と定義を行うことができます。

注:

- JMX コンソールで LDAP 認証設定を行うこともできます。詳細については、[「JMX コンソールを使用して LDAP 認証メソッドを有効化および定義する方法」\(100ページ\)](#)を参照してください。
- LDAP 認証設定の例については、[「LDAP 認証設定 - 例」\(101ページ\)](#)を参照してください。

UCMDB のユーザ・インタフェースで LDAP 認証メソッドを有効化および定義するには、次の手順を実行します。

1. [管理] > [インフラストラクチャ設定] > [LDAP 全般] カテゴリを選択します。
2. [LDAP サーバ URL] を選択して、次の形式で LDAP URL の値を入力します。

```
ldap://<ldapHost>[:<port>]/[<baseDN>][?scope]
```

例:

```
ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

3. **【LDAP グループ定義】** カテゴリを選択し, **【グループのベース DN】** で, 一般グループの識別名を入力します。
4. **【ルート グループのベース DN】** に, ルート・グループの識別名を入力します。
5. **【LDAP 全般】** カテゴリを選択し, **【ユーザ権限の同期化を有効化】** で, 値が **【True】** に設定されていることを確認します。
6. **【LDAP 一般認証】** カテゴリを選択して, **【検索権限のあるユーザのパスワード】** を見つけ, パスワードを入力します。
7. **【クラスと属性のための LDAP オプション】** カテゴリを選択し, **【グループ クラス オブジェクト】** を見つけ, オブジェクト・クラス名を入力します (Microsoft Active Directory の場合は **group**, Oracle Directory Server の場合は **groupOfUniqueNames**) 。
8. **【グループのメンバ属性】** を見つけて, 属性名を入力します (Microsoft Active Directory の場合は **member**, Oracle Directory Server の場合は **uniqueMember**) 。
9. **【ユーザのオブジェクト クラス】** を見つけて, オブジェクト・クラス名を入力します (Microsoft Active Directory の場合は **user**, Oracle Directory Server の場合は **inetOrgPerson**) 。
10. **【UUID 属性】** を見つけ, 使用しているディレクトリ・サーバのユーザの一意の識別属性を入力します。必ず使用しているディレクトリ・サーバ内で一意の属性を選択してください。たとえば, SunOne/Oracle ディレクトリ・サーバを使用する場合は UID 属性は一意ではありません。このような場合, 電子メール・アドレス属性と識別名のいずれかを使用してください。一意ではない属性を UCMDDB の一意の識別属性として使用すると, ログイン時に不整合な動作が起こる場合があります。
11. 新しい値を保存します。エントリを標準設定値で置き換えるには, **【標準設定に戻す】** をクリックします。
12. **【LDAP 全般】** のインフラストラクチャ設定 **【LDAP による認証の際に大文字と小文字を区別】** が **【True】** に設定されている場合, 認証は大文字と小文字を区別します。

注意: このインフラストラクチャ設定の値が変更されると, すべての外部ユーザを UCMDDB 管理者によって手動で削除する必要があります。

13. LDAP ユーザ・グループを UCMDDB ユーザ・グループにマッピングします。詳細については, [「HP Universal CMDB ログイン認証」\(95ページ\)](#)を参照してください。
14. グループ・マッピングのない LDAP グループのユーザに一連の標準権限を定義する場合, **【LDAP 全般】** カテゴリを選択し, **【自動的に割り当てられたユーザ グループ】** を見つけてグループ名を入力します。
15. **重要 :**高可用性環境で LDAP を設定している場合, 変更内容を有効にするにはクラスタを再起動する必要があります。

注: すべての LDAP ユーザの氏名および電子メールアドレスはローカル・リポジトリに保存されます。LDAP サーバに保存されているこれらのパラメータ値のいずれかがローカル・リポジトリのものとは異なる場合, ログイン時に LDAP サーバ値でローカル値が上書きされます。

JMX コンソールを使用して LDAP 認証メソッドを有効化および定義する方法

本タスクでは、JMX コンソールを使用して LDAP 認証を設定する方法について説明します。

注:

- 高可用性環境では、必ず Writer サーバの JMX コンソールにログインします。
- UCMDB で LDAP 認証設定を行うこともできます。詳細については、[「LDAP 認証メソッドを有効化および定義する方法」\(98ページ\)](#)を参照してください。
- LDAP 認証設定の例については、[「LDAP 認証設定 - 例」\(101ページ\)](#)を参照してください。

LDAP 認証設定を行うには、次の手順を実行します。

1. Web ブラウザを起動して、次のアドレスを入力します。 **http://<サーバ名>:8080/jmx-console**。
<サーバ名> には HP Universal CMDB がインストールされているマシンの名前が入ります。
ユーザ名およびパスワードでのログインが必要な場合もあります。
2. UCMDB で、 **UCMDB:service=LDAP Services** をクリックして [操作] ページを開きます。
3. 現在の LDAP 認証設定を表示するには、 **getLDAPSettings** メソッドを見つけます。 [Invoke] をクリックします。表に、すべての LDAP 設定とその値が表示されます。
4. LDAP 認証設定の値を変更するには、 **configureLDAP** メソッドを見つけます。関連する設定の値を入力して、 [Invoke] をクリックします。LDAP 認証設定の更新が成功したかどうか [JMX MBEAN Operation Result] ページに示されます。

注: 設定に値を入力しない場合は、現在の値が保持されます。

5. LDAP 設定を行った後、LDAP ユーザの資格情報を確認できます。
 - a. **verifyLDAPCredentials** メソッドを見つけます。
 - b. 顧客 ID、ユーザ名、およびパスワードを入力します。
 - c. [Invoke] をクリックします。
LDAP 認証が渡されたかどうか [JMX MBEAN Operation Result] ページに示されます。
6. **重要** :高可用性環境で LDAP を設定している場合、変更内容を有効にするにはクラスタを再起動する必要があります。

注: すべての LDAP ユーザの氏名および電子メールアドレスはローカル・リポジトリに保存されます。LDAP サーバに保存されているこれらのパラメータ値のいずれかがローカル・リポジトリのものと異なる場合、ログイン時に LDAP サーバ値でローカル値が上書きされます。

LDAP 認証設定 - 例

次の表に、LDAP 認証の設定値の例を示します。

設定	値
ユーザのオブジェクト・クラス	user
LDAP による認証の際に大文字と小文字を区別	false
グループのメンバ属性	member
識別名 (DN) 解決	true
ルート・グループ・フィルタ	(objectCategory=group)
LDAP 接続文字列	ldap://myldap.example.com:389/OU=Users,OU=Dept,OU=US,DC=example,DC=com??sub
LDAP 検索ユーザ	CN=John Doe,OU=Users,OU=Dept,OU=US,DC=example,DC=com
グループ・クラス・オブジェクト	group
親グループを見つけるためにボトムアップ・アルゴリズムを使用	true
UUID 属性	sAMAccountName
グループ名の属性	cn
グループ・ベース・フィルタ	(objectclass=group)
ユーザ・フィルタ	(&(sAMAccountName=*)(objectclass=user))
検索再試行数	3
グループの表示名の属性	cn
ルート・グループ・スコープ	sub
ユーザの表示名の属性	cn
グループ検索のスコープ	sub

設定	値
LDAP 認証の有効化	false
LDAP 同期の有効化	true
ルート・グループ	OU=Users,OU=Security Groups,DC=example,DC=com
グループ・ベース	OU=AMRND,OU=Security Groups,DC=example,DC=com
標準設定のグループ	AdminsGroup
グループの説明の属性	詳細

分散化環境における現在の LW-SSO 設定の取得

UCMDB が分散環境に組み込まれている場合（BSM デプロイメントの場合など）、次の手順を実行して処理マシン上の現在の LW-SSO 設定を取得します。

現在の LW-SSO 設定を取得するには、次の手順を実行します。

1. Web ブラウザを起動し、アドレスに `http://localhost.<domain_name>:8080/jmx-console` を入力します。
ユーザ名とパスワードの入力を求められる場合もあります。
2. **UCMDB:service=Security Services** を見つけ、リンクをクリックして [操作] ページを開きます。
3. **retrieveLWSSOConfiguration** 操作を見つけてみます。
4. **[Invoke]** をクリックして設定を取得します。

第8章: 機密マネージャ

本章の内容

- [機密マネージャの概要](#) 103
- [セキュリティの考慮事項](#) 103
- [HP Universal CMDB Server の設定](#) 104
- [定義](#) 105
- [暗号化プロパティ](#) 105

機密マネージャの概要

機密マネージャ・フレームワークは、HP Universal CMDB やほかの HP ソフトウェア製品の機密データの管理および配布に関する問題を解決します。

機密マネージャは、次に示す2つのメイン・コンポーネントで構成されています:クライアントおよびサーバ。これらの2つのコンポーネントは、データを安全に転送する役割を担います。

- 機密マネージャ・クライアントは、機密データにアクセスするためにアプリケーションによって使用されるライブラリです。
- 機密マネージャ・サーバは、機密マネージャ・クライアントまたはサードパーティのクライアントから要求を受信し、必要なタスクを実行します。機密マネージャ・サーバは、データを安全に保存する役割を担います。

機密マネージャは、転送、クライアント・キャッシュ、永続的な保存場所、メモリの資格情報を暗号化します。機密マネージャは、対称暗号化方式を使用して機密マネージャ・クライアントと機密マネージャ・サーバ間で資格情報を転送します。この転送には共有秘密鍵が使用されます。機密マネージャは、設定に応じてキャッシュ、永続的な保存場所、転送の暗号化にさまざまな秘密鍵を使用します。

Data Flow Probe で資格情報の暗号化を管理するためのガイドラインの詳細については、「[データ・フロー資格情報管理](#)」(49ページ)を参照してください。

セキュリティの考慮事項

- セキュリティ・アルゴリズムに使用できる鍵のサイズは、次のとおりです:128, 192, 256 ビット。鍵が小さいほどアルゴリズムの実行速度は速くなりますが、セキュリティは弱くなります。通常、128 ビットのサイズで十分なセキュリティを確保できます。

- システムをより安全にするには、次のように設定して MAC を使用します:**useMacWithCrypto** を **true** に設定。詳細については、「[暗号化プロパティ](#)」(105ページ)を参照してください。
- 強力な顧客セキュリティ・プロバイダを活用するには、JCE モードを使用できます。

HP Universal CMDB Server の設定

HP Universal CMDB で作業する場合、次の JMX メソッドを使用して暗号化の秘密鍵と暗号化プロパティを設定する必要があります。

1. HP Universal CMDB サーバ・マシンで Web ブラウザを起動し、次のサーバ・アドレスを入力します。**http://<UCMDB サーバのホスト名または IP>:8080/jmx-console**
ユーザ名とパスワードを使用してログインする必要がある場合もあります。
2. UCMDB で、**UCMDB:service=Security Services** をクリックして [操作] ページを開きます。
3. 現在の設定を取得するには、**CMGetConfiguration** 操作を見つけます。

[Invoke] をクリックして、機密マネージャ・サーバ設定の XML ファイルを表示します。

4. 設定を変更するには、前の手順で起動した XML をテキスト・エディタにコピーします。「[暗号化プロパティ](#)」(105ページ)の表に従って変更します。

CMSetConfiguration 操作を見つけます。更新された設定を [値] ボックスにコピーし、[Invoke] をクリックします。新しい設定が UCMDB サーバに書き込まれます。

5. 認証およびレプリケーションを行うためにユーザを機密マネージャに追加するには、**CMAddUser** 操作を見つけます。このプロセスは、レプリケーション・プロセスでも有効です。レプリケーションでは、スレーブ・サーバは権限のあるユーザを使用してマスタ・サーバと通信する必要があります。

- **ユーザ名**: ユーザ名です。
- **顧客**: 標準設定は ALL_CUSTOMERS です。
- **リソース**: リソース名です。標準設定は ROOT_FOLDER です。
- **権限**: ALL_PERMISSIONS, CREATE, READ, UPDATE, DELETE のいずれかを選択します。標準設定は ALL_PERMISSIONS です。

[Invoke] をクリックします。

6. 必要に応じて、HP Universal CMDB を再起動します。
通常、サーバを再起動する必要はありません。次のいずれかのリソースを変更した場合にサーバの再起動が必要になることがあります。
- ストレージ・タイプ
 - データベースのテーブル名またはカラム名
 - データベース接続の作成者

- データベースの接続プロパティ (URL, ユーザ, パスワード, ドライバ・クラス名)
- データベース・タイプ

注:

- UCMDB サーバとそのクライアントで転送用暗号化プロパティを同じにすることが重要です。これらのプロパティがUCMDB サーバで変更されている場合、すべてのクライアントで変更する必要があります。(これはData Flow Probeには関係ありません。UCMDB サーバと同じプロセスで実行されるからです。つまり、転送用の暗号化設定は必要ありません)。
- 機密マネージャ・レプリケーションは標準設定では設定されていませんが、必要に応じて設定できます。
- 機密マネージャ・レプリケーションが有効になっている場合、マスタの転送用の **initString** またはほかの暗号化プロパティが変更されると、すべてのスレーブでその変更が採用されます。

定義

ストレージ用暗号化プロパティ : サーバでデータ (暗号化プロパティで暗号化または復号化が必須のデータベースやファイルのデータなど) を保持および暗号化する方法, 資格情報を安全に保存する方法, 暗号化の処理方法, 準拠する設定を定義する設定です。

転送用暗号化プロパティ : 転送用の設定では, サーバとクライアント間の転送を暗号化する方法, 使用する設定, 安全に資格情報を転送する方法, 暗号化の処理方法, 準拠する設定を定義します。サーバとクライアントの両方で転送の暗号化と復号化に同じ暗号化プロパティを使用する必要があります。

レプリケーションおよびレプリケーション用暗号化プロパティ : 機密マネージャで安全に保持されているデータが複数のサーバ間で安全に複製されます。これらのプロパティでは, スレーブ・サーバとマスタ・サーバ間でどのようにデータを転送するのかを定義します。

注:

- 機密マネージャ・サーバの設定を保持しているデータベース・テーブルの名前は **CM_CONFIGURATION** です。
- Configuration Manager サーバの標準設定の構成ファイルは, **defaultCMServerConfig.xml** という名前で app-infra.jar にあります。

暗号化プロパティ

次の表に, 暗号化プロパティを示します。これらのパラメータの使用の詳細については, [「HP Universal CMDB Server の設定」\(104ページ\)](#)を参照してください。

パラメータ	詳細	推奨値
encryptTransportMode	転送データの暗号化: true false	true
encryptDecryptInitString	暗号化のパスワード	9文字以上
cryptoSource	使用する暗号化実装ライブラリ <ul style="list-style-type: none"> • lw • jce • windowsDPAPI • lwJCECompatible 	lw
lwJCEPBECompatibilityMode	軽量暗号化方式の以前のバージョンのサポート: <ul style="list-style-type: none"> • true • false 	true
cipherType	機密マネージャで使用する暗号化のタイプ。機密マネージャでサポートされる値は1つだけです。 symmetricBlockCipher	symmetricBlockCipher
engineName	<ul style="list-style-type: none"> • AES • Blowfish • DES • 3DES • Null (暗号化しない) 	AES
algorithmModeName	ブロック暗号化アルゴリズムのモード: <ul style="list-style-type: none"> • CBC 	CBC
algorithmPaddingName	パディングの標準: <ul style="list-style-type: none"> • PKCS7Padding • PKCS5Padding 	PKCS7Padding
keySize	アルゴリズムによって異なる (どの engineName をサポートするのかによる)	256
pbeCount	encryptDecryptInitString から鍵を作成するためにハッシュを実行する回数。 任意の正数。	1000

パラメータ	詳細	推奨値
pbeDigestAlgorithm	ハッシュ・タイプ: <ul style="list-style-type: none"> • SHA1 • SHA256 • MD5 	SHA256
encodingMode	暗号化するオブジェクトの ASCII 表現: <ul style="list-style-type: none"> • Base64 • Base64Url 	Base64Url
useMacWithCrypto	暗号化方式で MAC が使用されるかどうかの定義: <ul style="list-style-type: none"> • true • false 	false
macType	メッセージ認証コード (MAC) のタイプ: <ul style="list-style-type: none"> • hmac 	hmac
macKeySize SHA256	Mac アルゴリズムによって異なる	256
macHashName	ハッシュ用の Mac アルゴリズム: <ul style="list-style-type: none"> • SHA256 	SHA256

第9章: 可用性の高い強化

本章の内容

- クラスタ認証 108
- クラスタ・メッセージの暗号化 109
 - トラブルシューティング 110
- key.bin の鍵の変更 110

クラスタ認証

クラスタ認証を有効にするには、次の手順を実行します。

1. UCMDB で【管理】 > 【インフラストラクチャ設定マネージャ】に移動します。
2. 【ハイアベイラビリティ クラスタの結合時に認証を有効化】を見つけて、**true** に設定します。
3. JKS 形式で単一サーバ認証のキーストア（証明書と秘密および公開鍵）を用意します。このキーストアはすべてのサーバ上に配置され、ハイアベイラビリティ・クラスタへの接続時に認証に使用されます。

キー・ストアを次の場所に配置します。<UCMDB のインストール・フォルダ>\conf\security。名前は **cluster.authentication.keystore** にします。

注: UCMDB には、このキーストアが事前設定され、定義済み状態で用意されています。このキーストアは、すべての UCMDB のクリーン・インストールで同じものが使用されます。このため、安全ではありません。結合要求を安全に認証するには、このファイルを削除して、新しいファイルを作成します。

4. 次のとおり、クラスタ認証キー・ストアを生成します。
 - a. C:\hp\UCMDB\UCMDBServer\bin\jre\bin から次のコマンドを実行します。

```
keytool -genkey -alias hpcert -keystore <UCMDB のインストール・フォルダ>\conf\security\cluster.authentication.keystore -keyalg RSA
```

コンソールのダイアログ・ボックスが開き、新しいキーストアのパスワードを入力するように求められます。
 - b. 標準設定ではパスワードは **hppass** です。異なるパスワードを使用する場合、次の JMX メソッドを実行してサーバを更新します。 **UCMDB:service=High Availability Services:changeClusterAuthenticationKeystorePassword**
 - c. コンソールのダイアログ・ボックスで、**What is your first and last name?** と質問されるので、クラスタ名を入力します。

- d. 所属する組織の条件に合わせて、その他のパラメータを入力します。
 - e. キーのパスワードを入力します。キーのパスワードは、キー・ストアのパスワードと一致する必要があります。
JKS キーストアが **<UCMDB のインストール・フォルダ>\conf\security\cluster.authentication.keystore** に作成されます。
5. クラスタ内にあるすべてのサーバの古い **<UCMDB のインストール・フォルダ>\conf\security\cluster.authentication.keystore** を、この新しいキー・ストアで置き換えます。
 6. クラスタ内のサーバをすべて再起動します。

クラスタ・メッセージの暗号化

クラスタ・メッセージの暗号化を使用して、クラスタ内のすべてのメッセージを暗号化します。

クラスタ・メッセージの暗号化を有効にするには、次の手順を実行します。

1. UCMDB で **【管理】 > 【インフラストラクチャ設定マネージャ】** に移動します。
2. **【ハイアベイラビリティ クラスタ通信暗号化を有効化】** を見つけて、**true** に設定します。
3. 対称暗号化用の秘密鍵をすべてのサーバに配置します。この鍵は、タイプ JCEKS のキー・ストア (**<UCMDB のインストール・フォルダ>\conf\security\cluster.encryption.keystore**) にあります。

注: UCMDB には、このキー・ストアが事前設定され、定義済みの状態で用意されています。このキーストアは、すべての UCMDB のクリーン・インストールで同じものが使用されます。このため、安全ではありません。クラスタ・メッセージを安全に暗号化するには、このファイルを削除して、次の手順を実行して新しいファイルを作成してください。

4. **<UCMDB のインストール・フォルダ>\bin\jre\bin** から、次のコマンドを実行します。
Keytool -genseckey -alias hpcert -keystore <UCMDB のインストール・フォルダ>\conf\security\cluster.encryption.keystore -storetype JCEKS
5. 新しいキー・ストアのパスワードを入力するよう求められます。標準設定のパスワードは "hppass" です。異なるパスワードを使用する場合、次の JMX メソッドを実行してサーバを更新する必要があります。
UCMDB:service=High Availability Services:changeClusterEncryptionKeystorePassword
6. クラスタ内にあるすべてのサーバの古い **<UCMDB のインストール・フォルダ>\conf\security\cluster.encryption.keystore** を、この新しいキー・ストアで置き換えます。
7. サーバを再起動します。

トラブルシューティング

サーバを起動するたびに、サーバはテスト・メッセージをクラスタに送信して、サーバがクラスタに正常に接続しているかどうかを確認します。接続に問題がある場合、メッセージが失敗します。また、クラスタ全体が応答しなくなることを回避するためにサーバが停止します。

クラスタの暗号化設定の誤った例を、次に示します。

- 暗号化を無効にしているノードと有効にしているノードがある。
- `cluster.encryption.keystore` が誤っているが見つからない
- キー・ストアの鍵が誤っているが見つからない

設定の問題によってサーバが応答しなくなった場合、次のエラー・メッセージが表示されます。

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - ##### Server failed to connect properly to the cluster and its service is stopped!Please fix the problem and start it again #####
```

```
2012-09-11 17:48:23,586 [Thread-14] FATAL - Potential problems can be:wrong security configuration (wrong or missing cluster.encryption.keystore, wrong key, disabled encryption in a cluster with enabled encryption)
```

key.bin の鍵の変更

複数のサーバが存在する高可用性環境では、次のとおり **key.bin** の **key** を変更します。

1. JMX のライター・マシンに移動します。クラスタ内の任意のマシンを選択して、各ページの上部にある **[writer]** リンクをクリックできます。
2. コンソールの UCMDB セクションで、**UCMDB:service=Discovery Manager** をクリックします。
3. 次のいずれかの方法で key を変更します。
 - **[changeEncryptionKey]** をクリック（これによって、既存の暗号鍵がインポートされます）
 - **[generateEncryptionKey]** をクリック（これによって、ランダム暗号鍵が生成されます）
4. ライター・マシン上でファイル・システムに移動し、次の場所で **key.bin** を見つけます。
C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin
5. **key.bin** を、ライター・マシンの場所からクラスタ内にあるその他の各マシン（次の場所）にコピーします。**C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1**。対象ファイルの名前を変更します（例：**key_new.bin**）。
6. その他の各サーバ（リーダー）について、次の手順を実行します。
 - a. リーダをライターに切り替え、変更されるまで待ちます（切り替えはハイアベイラビリティ JMX からのみ行えます）。
 - b. 現在のライターの JMX に接続して、**[UCMDB:service=Discovery Manager]** をクリックしま

す。

- c. **[changeEncryptionKey]** をクリックして呼び出し、手順 3 と同じ入力内容で設定します (**newKeyFileName** には、手順 5 で割り当てた新しい名前を設定します)。
- d. 次のメッセージが表示されることを確認します。 **Key was created successfully**

ドキュメントに関するフィードバックの送信

このドキュメントに関するコメントについては、電子メールで[ドキュメント・チーム](#)までご連絡ください。ご使用のシステムに電子メール・クライアントが設定されている場合は、上記のリンクをクリックすると電子メールウィンドウが開き、以下の情報が件名の行に表示されます。

強化ガイド (Universal CMDB および Configuration Manager 10.20) に関するフィードバック

電子メールにフィードバックを記入して、送信ボタンをクリックしてください。

使用できる電子メール・クライアントがない場合は、上記の情報を Web メール・クライアントの新しいメッセージにコピーして、フィードバックを cms-doc@hp.com に送信してください。

お客様からのご意見をお待ちしております。