

CA ControlMinder

実装ガイド

12.8



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

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

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

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

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

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2013 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

サードパーティに関する通知

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

© Copyright IBM Corporation 1999, 2002

All Rights Reserved

サンプル スクリプトおよびサンプル SDK コード

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

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

CA Technologies 製品リファレンス

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

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

ドキュメントの表記規則

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

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

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

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

例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

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

ファイル ロケーションに関する規則

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

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

CA への連絡先

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

マニュアルの変更点

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

- イベントの電子メール通知
- CA Business Intelligence への接続を設定します。
- UNIX エンドポイントのインストールおよびカスタマイズ - 以下の更新を含めるために章が更新されました。
 - UNIX インストール パラメータ ファイル - UNIX インストールのカスタマイズ
 - CA ControlMinder RPM パッケージのカスタマイズ
 - CA ControlMinder を Debian または Ubuntu Linux にインストールする方法
 - customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ
 - bff ネイティブ パッケージ ファイルのカスタマイズ
 - AIX ネイティブ パッケージのインストール
 - customize_eac_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ
 - CA ControlMinder を Solaris ゾーンにインストールする方法
- CA ControlMinder RPM パッケージのカスタマイズ
- Veritas Cluster Server を使用した Linux 上の CA ControlMinder ハイ アベイラビリティの実装
- キーストアへのユーザ ディレクトリ 証明書の追加
- エンタープライズ管理サーバ SSL 通信
- ac_entm_pers のパスワードの変更

目次

第 1 章: 本書の内容	19
第 2 章: エンタープライズ実装の計画	21
セキュリティ システムの計画	21
実装計画の準備	22
システム管理部門との連携	23
保護方法の決定	24
スタッフの教育とトレーニング	25
CA ControlMinder エンタープライズ管理 の実装方法	27
エンタープライズ管理サーバの実装	28
ディザスタ リカバリのための CA ControlMinder の実装	29
CA ControlMinder エンタープライズ管理 展開アーキテクチャ	30
デフォルトのエンタープライズ展開アーキテクチャ	31
負荷分散デプロイメント アーキテクチャ	32
ハイアベイラビリティ展開アーキテクチャ	33
ディザスタ リカバリ アーキテクチャ	34
CA ControlMinder エンタープライズ管理 のコンポーネント	34
エンタープライズ管理サーバ	35
配布サーバ	35
Web ベースのアプリケーション	38
CA ControlMinder エンタープライズ管理	39
デプロイ マップ サーバ (DMS)	40
レポート ポータル	40
セントラル RDBMS	41
エンドポイント	41
CA User Activity Reporting Module コンポーネント	42
ユーザ ストア	42
実装のサイジング	43
CA ControlMinder データベース サイズの制限	44

第 3 章: サイジングとパフォーマンス	45

第 4 章: エンタープライズ管理サーバのインストール	57

環境アーキテクチャ	57
エンタープライズ管理サーバの準備方法	59
Windows でのエンタープライズ管理サーバの準備	59
Linux でのエンタープライズ管理サーバの準備	61
エンタープライズ管理のための中央データベースの準備	64
必須ソフトウェア インストール ユーティリティの実行	69
エンタープライズ管理サーバ コンポーネントのインストール方法	70
Windows での CA ControlMinder エンタープライズ管理 のインストール	72
Linux での CA ControlMinder エンタープライズ管理 のインストール	78

第 5 章: SUN ONE および CA Directory 用のエンタープライズ管理サーバの 設定	87

コネクタ サーバへの接続設定	98
CA ControlMinder エンタープライズ管理 を起動します。	101
CA ControlMinder エンタープライズ管理 を開く	102
詳細な環境設定	103
Windows での CA ControlMinder エンタープライズ管理 のアンインストール	119
Linux での CA ControlMinder エンタープライズ管理 のアンインストール	120
エンタープライズ管理サーバからの追加コンポーネントの削除	121
配布サーバの実装	122
配布サーバのインストール	122

第 6 章: エンタープライズ レポート機能の実装	125

エンタープライズ レポート機能	125
レポート サービスのアーキテクチャ	126
レポート サービス サーバコンポーネントの設定方法	128
レポート ポータル コンピュータのセットアップ方法	129
CA Business Intelligence のインストール用の Linux の準備	133
レポート パッケージのデプロイ	135
大規模デプロイに対する BusinessObjects の設定	139
CA Business Intelligence への接続を設定します。	141
スナップショット定義の作成	142
CA ControlMinder r12.0 でインストールしたレポート ポータルへのレポート パッケージのデプ ロイ	155

第 7 章: エンドポイントの実装の準備 159

保護するポリシー オブジェクトの決定	159
ユーザ	159
グループ	162
権限属性	164
グローバル権限属性	165
グループ権限属性	165
警告期間の使用方法	166
CA ControlMinder バックドア	167
実装に関するヒント	168
セキュリティの種類	168
アクセサ	169
リソース	169

第 8 章: Windows エンドポイントのインストールおよびカスタマイズ 173

はじめに	173
インストール方法	174
ファイアウォール設定	174
新規インストール	175
アップグレードおよび再インストール	176
その他の製品との共存	178
Product Explorer によるインストール	178
Product Explorer を使用したインストール	179
インストール ワークシート	180
コマンドラインによるインストール	188
インストール プログラムに対するカスタム デフォルトの設定	189
サイレント モードでのインストール	190
setup コマンド - CA ControlMinder for Windows のインストール	191
Windows エンドポイントのアップグレード	201
CA ControlMinder の起動および停止	202
CA ControlMinder の停止	203
CA ControlMinder の手動での起動	204
インストールの確認	205
ログイン保護画面の表示	205
エンドポイントへの拡張ポリシー管理の設定	206
レポート作成のための Windows エンドポイントの設定	206
CA ControlMinder のクラスタ環境用へのカスタマイズ	207
アンインストールの方法	208

CA ControlMinder をアンインストールします。	209
サイレント モードでの CA ControlMinder のアンインストール	210
第 9 章: UNIX エンドポイントのインストールおよびカスタマイズ	211
はじめに.....	211
オペレーティング システムのサポートおよび要件	211
管理端末.....	212
インストール上の注意事項.....	213
UNIX インストール パラメータ ファイル -- UNIX インストールのカスタマイズ	220
Linux s390 エンドポイントのインストールの考慮事項	236
ネイティブ インストール	238
ネイティブ パッケージ.....	239
ネイティブ インストールの際に考慮するその他の事項	239
RPM Package Manager のインストール.....	244
CA ControlMinder を Debian または Ubuntu Linux にインストールする方法	254
Solaris ネイティブ パッケージングのインストール.....	261
HP-UX ネイティブ パッケージのインストール	274
AIX ネイティブ パッケージのインストール	280
AIX Workload Partition (WPAR) の実装.....	288
通常のスクリプト インストール	294
install_base スクリプトを使用したインストール	295
install_base コマンド - インストール スクリプトの実行	297
install_base スクリプトのしくみ.....	304
インストール後の設定	308
CA ControlMinder の起動.....	309
エンドポイントへの拡張ポリシー管理の設定	311
レポート作成のための UNIX エンドポイントの設定	312
CA ControlMinder のカスタマイズ.....	313
trusted プログラム	313
初期設定ファイル.....	317
拡張ポリシー管理.....	320
sesu および sepass ユーティリティ	321
メンテナンス モードの保護 (サイレント モード)	323
Solaris ゾーンへのインストール方法.....	325
Solaris ネイティブ パッケージを使用したインストール	328
Install_Base スクリプトを使用したインストール.....	340
zlogin を使用した管理者アクセスの許可.....	345
リソースを保護するためのルール の定義.....	345
CA ControlMinder のアンインストール.....	347

CA ControlMinder の自動起動.....	347
サービス マネジメント機能による CA ControlMinder の管理	348

第 10 章: UNAB ホストのインストールとカスタマイズ 351

UNAB ホスト	351
UNAB の実装方法	352
はじめに.....	353
インストール モード.....	353
Active Directory サイト サポート	354
64 ビット Linux ホストのインストールの考慮事項.....	355
SSH PAM 設定	356
Linux s390 エンドポイントのインストールの考慮事項	360
Kerberos と SSO の考慮事項	362
システム適合性の確認.....	367
UNIX コンピュータ名が正しく解決されることの確認	370
UNAB インストール パラメータ ファイル - UNAB インストールのカスタマイズ.....	371
CA ControlMinder エンタープライズ管理 を使用した UNAB の管理.....	377
CA ControlMinder との統合.....	379
RSA SecurID との統合	381
RPM Package Manager のインストール.....	384
UNAB RPM パッケージのインストール	385
UNAB RPM パッケージのカスタマイズ.....	386
customize_uxauth_rpm コマンド - UNAB RPM パッケージをカスタマイズします	389
インストールが正常に完了したことを確認する	391
UNAB RPM パッケージのアップグレード.....	391
UNAB RPM パッケージのアンインストール	392
Solaris ネイティブ パッケージングのインストール.....	393
Solaris ネイティブ パッケージのカスタマイズ.....	393
customize_uxauth_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ.....	395
UNAB Solaris ネイティブ パッケージのインストール	397
選択したゾーンへの UNAB Solaris ネイティブ パッケージのインストール	400
Solaris 上の UNAB のアップグレード	401
UNAB Solaris ネイティブ パッケージのアンインストール	402
HP-UX ネイティブ パッケージのインストール.....	403
UNAB SD-UX 形式パッケージのカスタマイズ	403
customize_uxauth_depot コマンド - SD-UX 形式パッケージのカスタマイズ.....	406
UNAB HP-UX ネイティブ パッケージのインストール	408
HP-UX パッケージのアンインストール.....	409
AIX ネイティブ パッケージのインストール	410

AIX 上のプラグ可能な認証モジュール (PAM)	410
bff ネイティブ パッケージ ファイルのカスタマイズ	413
customize_uxauth_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ (UNAB)	415
UNAB AIX ネイティブ パッケージのインストール	417
AIX パッケージのアンインストール	419
AIX ワークロードパーティション (WPAR) ネイティブ パッケージのインストール	420
共有モードでの UNAB AIX 7.1 WPAR ネイティブ パッケージのインストール	421
分離モードでの UNAB AIX 7.1 WPAR ネイティブ パッケージのインストール	422
UNAB AIX 7.1 WPAR パッケージのアンインストール	423
インストール後のタスク	423
Active Directory での UNIX ホストの登録	423
UNAB の設定	426
レポート作成のための UNAB の設定	427
UNAB の開始	427
UNAB のアクティブ化	428
完全統合モードでの実装方法	429
UNAB と Active Directory との統合	430
CA ControlMinder UNIX Attributes プラグインのインストール	431
ユーザとグループの移行	434
UNIX ユーザおよびグループの属性に対する管理権限の UNIX 管理者への委任	437
Active Directory ユーザ用の UNIX 属性の設定	439
信頼済みドメイン環境での UNAB の実装	440
一方向の信頼関係にあるドメイン環境で UNIX ホストを登録する方法	443
Windows エージェントレス エンドポイントの作成	447
特権アカウントの検出	449
パスワード コンシューマの作成	452
CA ControlMinder RPM パッケージのインストール	456
CA ControlMinder の起動	459
Active Directory での UNIX ホストの登録	460
UNAB のアクティブ化	463
UNAB の開始	464

第 11 章: エンドポイント管理のインストール 465

エンドポイント管理サーバの準備方法	465
Windows での CA ControlMinder エンドポイント管理 のインストール	466
Solaris または Linux 上での CA ControlMinder エンドポイント管理 のインストール	467
Windows での CA ControlMinder エンドポイント管理 のアンインストール	468
Solaris または Linux 上での CA ControlMinder エンドポイント管理 のアンインストール	470
CA ControlMinder エンドポイント管理 の起動	471

CA ControlMinder エンドポイント管理 を開く	472

第 12 章: ハイアベイラビリティ展開のインストール 475

ハイアベイラビリティ	475
ハイアベイラビリティ展開の利点および制限	476
ハイアベイラビリティ展開アーキテクチャ	477
ハイアベイラビリティ環境アーキテクチャの配布サーバ	478
ハイアベイラビリティ環境のコンポーネント	479
共用ストレージ	480
クラスタ ソフトウェア	480
障害が発生した場合の動作	481
ハイアベイラビリティ環境の CA ControlMinder エンタープライズ管理 を設定する方法	482
プライマリ エンタープライズ管理サーバの設定	484
セカンダリ エンタープライズ管理サーバの設定	487
高可用性用の負荷分散エンタープライズ管理サーバの設定	490
フェールオーバー用の Active Directory の設定	491
ローカル DMS での CA ControlMinder エンタープライズ管理 の設定	492
ハイアベイラビリティ環境の配布サーバを設定する方法	493
プライマリ配布サーバの設定	494
セカンダリ配布サーバの設定	496
ハイアベイラビリティ環境のエンドポイントの設定	497
ハイアベイラビリティ用の Oracle RAC の設定	498
Veritas Cluster Server を使用した Linux 上の CA ControlMinder ハイアベイラビリティの実装	501
前提条件の確認	504
プライマリ エンタープライズ管理サーバの設定	505
セカンダリ エンタープライズ管理サーバの設定	515
ハイアベイラビリティ設定の確認	518

付録 A: トラブルシューティング 521

第 13 章: Disaster Recovery Deployment のインストール 523

ディザスタ リカバリの概要	523
ディザスタ リカバリ	523
ディザスタ リカバリ アーキテクチャ	525
ディザスタ リカバリのコンポーネント	526
エンドポイント上のディザスタ リカバリの展開の仕組み	527
ディザスタ リカバリ展開をインストールする方法	529
運用環境 CA ControlMinder エンタープライズ管理 のセットアップ	530

ディザスタ リカバリ CA ControlMinder エンタープライズ管理 のセットアップ	532
DMS サブスクリプションの設定	534
エンドポイントのセットアップ	535
ディザスタ リカバリ展開をインストールするための追加情報	536
ディザスタ リカバリ プロセス	542
リストアできるデータ	543
DMS をリストアする場合	544
DH をリストアする場合	544
DMS のリストア方法	545
DH のリストア方法	546
障害からの復旧方法	547
sempd を使用した DMS のバックアップ	549
selang を使用した DMS のバックアップ	550
DH のリストア	552
運用環境の DMS のリストア	553
ディザスタ リカバリ DMS のリストア	554
メッセージキュー サーバのデータ ファイルのバックアップ	555
メッセージキュー サーバのデータ ファイルのリストア	556
メッセージキュー サーバデータ ファイルを同期する方法	556

付録 B: 通信の暗号方式の変更 559

通信の暗号化	559
対称暗号化	560
sechkey による対称暗号化の設定方法	561
対称暗号化鍵の変更	561
対称暗号化方式の変更	563
エンタープライズ展開での複数の対称暗号化方法	564
SSL、認証、および証明書	565
証明書の内容	565
証明書が証明すること	567
ルート証明書とサーバ証明書	567
SSL 暗号化の有効化	569
エンタープライズ管理サーバ SSL 通信	575
メッセージキュー サーバの SSL ポート番号	583
同一の暗号化鍵を使用するためのサーバの設定	584
CA ControlMinder Web サービスの URL の変更	586
Microsoft SQL Server データベース接続設定の変更	588
レポート ポータル用の Windows 認証設定	590
Windows 認証で動作するようにレポート ポータルを設定する方法	591

付録 C: CA ControlMinder サービス アカウント設定の変更 599

CA ControlMinder サービス アカウントと CA ControlMinder コンポーネントとの関係	600
サービス アカウント パスワード	602
RDBMS_service_user のパスワードの変更	602
reportserver のパスワードの変更	604
+reportagent のパスワードの変更	608
+policyfetcher パスワードの変更	610
+devcalc のパスワードの変更	611
ac_entm_pers のパスワードの変更	612
ADS_LDAP_bind_user のパスワードの変更	613
JNDI 接続アカウントの変更	614
メッセージキュー ユーザの作成	614
tibco-jms-ds.xml ファイルでのアカウントの変更	616
メッセージキューの通信設定の変更	618
メッセージキュー管理者パスワードの変更	619
メッセージキューのサーバ証明書の変更	620
メッセージキュー SSL キーストアのパスワードの変更	621
New Topic (320)	624
パスワード変更手順	625
selang を使用したパスワードの変更	625
sechkey を使用したメッセージキュー パスワードの変更	626
メッセージキューのパスワードの設定	628
クリアテキストパスワードの暗号化	630
properties-service.xml ファイルでのパスワードの変更	631
login-config.xml ファイルでのパスワードの変更	632
CA IdentityMinder 管理コンソールでのユーザディレクトリのパスワードの変更	635

第 1 章：本書の内容

本書では、CA ControlMinder のさまざまなコンポーネントを計画し、インストールし、さらにカスタマイズする方法について説明します。対象となるコンポーネントは、Windows および UNIX 用の CA ControlMinder サーバおよびエンドポイント、CA ControlMinder エンドポイント管理 コンポーネントなどです。エンタープライズ管理およびレポートのインストールに関する章は、CA ControlMinder にのみ該当します。

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

第 2 章: エンタープライズ実装の計画

このセクションには、以下のトピックが含まれています。

[セキュリティ システムの計画](#) (P. 21)

[実装計画の準備](#) (P. 22)

[システム管理部門との連携](#) (P. 23)

[保護方法の決定](#) (P. 24)

[スタッフの教育とトレーニング](#) (P. 25)

[CA ControlMinder エンタープライズ管理 の実装方法](#) (P. 27)

[CA ControlMinder エンタープライズ管理 展開アーキテクチャ](#) (P. 30)

[CA ControlMinder エンタープライズ管理 のコンポーネント](#) (P. 34)

[実装のサイジング](#) (P. 43)

セキュリティ システムの計画

セキュリティ システムの第一の目標は、組織の情報資産を保護することです。効果的なセキュリティを実装するには、サイトに存在する脅威を認識する必要があります。さらに、そのような脅威から最も的確にサイトを保護する方法を決定する必要があります。

コンピュータ リソースの不正使用を防止するには、以下の 2 つの基本的な方法があります。

- 権限のないユーザによるシステムへのアクセスをブロックする
- アクセス権を持つユーザに対して特定の機密情報へのアクセスをブロックする

CA ControlMinder には、この両方の方法でシステムを保護するツールが用意されています。CA ControlMinder には、ユーザのアクティビティをトレースして、コンピュータ システムの不正使用の試みを追跡する監査ツールもあります。

セキュリティ プロジェクトの目標を決定すれば、セキュリティ ポリシー ステートメントを作成して、実装チームを編成できます。この実装チームは、セキュリティで保護する必要があるデータ、アプリケーション、およびユーザの決定に役立つ優先順位を確立する必要があります。

実装計画の準備

実装計画の作成時に、計画の目標がセキュリティ ポリシーに沿っていることを繰り返し確認します。新しいセキュリティ コントロールは、ユーザに適応期間を与えるために、段階的に導入する必要があります。

- セキュリティ計画に基づいた特定の目標の定義

セキュリティ 計画の実行に役立つ目標を定義します。

- **CA ControlMinder** を実装するために、プロトタイプとしてユーザのパイロット グループを定義します。

このパイロット グループでの **CA ControlMinder** のすべての機能をテストしてから、グループ以外のエンティティを保護します。パイロットグループでのテストは、他の組織を保護する方法を理解するのに役立ちます。

- 保護対象の決定

CA ControlMinder は、パイロット グループのビジネス データ、ジョブ、およびユーザを保護します。

- セキュリティ制御の展開方法の定義

現在の業務パターンの中断を最小限に抑えつつ、新しいセキュリティ制御を段階的に導入する方法について考慮します。さまざまなリソースやクラスに対する、監査のみのアクセス、および制限なしのアクセスの期間を考慮します。この監査期間に作成される監査レコードによって、どのユーザがどのリソースにアクセスする必要があるか、傾向を確認できます。

注: 警告モード（監査専用モード）の詳細については、「**UNIX** エンドポイント管理ガイド」および「**Windows** エンドポイント管理ガイド」を参照してください。

システム管理部門との連携

システム管理部門が **CA ControlMinder** の導入を決定しただけでは、サイトにおけるセキュリティが十分とは言えません。セキュリティプロジェクトの成功には、システム管理部門の積極的な関与が不可欠です。システム管理部門は、セキュリティ ポリシー、手続き、セキュリティ機能に割り当てるリソース、およびコンピュータ システムのユーザの責任を決定する必要があります。このようなシステム管理部門の支援がない場合、セキュリティの手続きは正しく使用されなくなり、単に管理上のわずらわしい作業となってセキュリティの効力が減少します。このような状況は、セキュリティに関する誤解を生み、重大なセキュリティの脅威にさらされる危険を引き起こす原因となります。

セキュリティ管理者はシステム管理部門の協力を得て、明確で包括的なセキュリティ ポリシー ステートメントを準備する必要があります。このステートメントには、以下の内容を含める必要があります。

- 正社員、パート タイム従業員、契約社員、およびコンサルタントに関する企業ポリシー
- システムを利用する外部ユーザに関する企業ポリシー
- システムを利用するすべてのユーザが求める動作
- 物理的な保護に関する考慮事項
- ユーザの各部門でのセキュリティ要件
- 監査上の要件

このような内容のセキュリティ ポリシーを作成することによって、**CA ControlMinder** の実装計画を、導入先のセキュリティ ポリシーに沿った現実的なものにすることができます。

保護方法の決定

CA ControlMinder をインストールする前に、使用する機能を決定します。

CA ControlMinder は、以下の保護方式を提供します。

- CA ControlMinder エンドポイント管理 を使用してすでによく知られているセキュリティ機能を実装するネイティブ セキュリティ。
- より巧妙な攻撃から守る高度なネイティブ セキュリティ。CA ControlMinder により、以下のことができます。
 - 特権アカウントの権限を制限する
 - 特別なユーザのユーザ パスワードを変更する機能など、特別な権限を一般ユーザに割り当てる
 - NTFS、FAT、および CDFS などの複数のファイル システムをサポートする
 - Windows および UNIX の両システムを含む異機種環境でセキュリティ ポリシーと監査を一元化する
- 組織向けに作成する複数ルール ポリシー（スクリプト ファイル）を展開する拡張ポリシー管理。このポリシー ベースの方法により、バージョン制御ポリシーの作成、エンタープライズ環境のホスト グループへのポリシーの割り当ておよび割り当て解除、デプロイ済みポリシーの直接デプロイおよび削除（デプロイ解除）、デプロイ ステータスおよびデプロイの偏差の確認などが可能になります。
- セキュリティ データベース、およびユーザ、グループ、アクセスルールを一連のサブスクリバに伝達する、Policy Model データベース（PMDB）。PMDB は、受け取ったすべての更新情報を定期的にサブスクリバに伝達します。このメカニズムによって、システム管理者の負担が大幅に軽減されます。
- 特権ユーザ パスワード管理（PUPM）により、中央ロケーションからターゲット エンドポイント上の特権アカウント用に、ロールベースのアクセス管理が提供されます。また、特権アカウントおよびアプリケーション ID パスワードを安全に保管できるようにし、ポリシーに基づいて特権アカウントおよびパスワードへのアクセスを制御します。
- UNIX Authentication Broker (UNAB) により、Active Directory に対してローカルの UNIX ユーザおよびグループのクレデンシャルを検証できます。すべてのユーザに対して単一のリポジトリを使用できるため、ユーザは同じユーザ名とパスワードですべてのプラットフォームにログインすることができます。

スタッフの教育とトレーニング

セキュリティ管理者には、CA ControlMinder のインストール時に混乱なく作業を進めるために必要な知識をシステム ユーザに伝える役割もあります。

各ユーザが CA ControlMinder に関してどの程度詳しく理解する必要があるかは、そのユーザに使用を許可する機能によって異なります。様々なタイプのシステム ユーザが必要とする情報には、以下のようなものがあります。

- SAM ユーザ

特権アカウントパスワードのチェックアウトおよびチェックアウト方法、および特権アカウントへのアクセスをリクエストするタイミング、および break glass を行うタイミングの理解。

- CA ControlMinder エンドポイント データベースに定義されているすべてのユーザ

- ユーザ名とパスワードでシステムに対して認証を行い、パスワードを変更する方法。システム セキュリティに対するパスワードの重要性を認識していることも必要です。
- パスワード ポリシー検証を実行する場合、パスワード マネージャに精通していること。
- 同時ログインを無効および有効にする *secons -d-* および *secons -d+* コマンドの使用方法。同時ログインとは、1 人のユーザが複数の端末から同時に 1 つのシステムにログインして開始した複数のセッションのことです。
- *sesudo* コマンドに精通している必要があります。このコマンドを使用すると、事前定義されたアクセス ルール（パスワードチェックが含まれるかどうかは場合による）に基づいて代理ユーザになることができます。

- 技術サポート担当

移行の考慮事項、および CA ControlMinder のインストールや再インストールを行う必須手順に精通している必要があります。データベースのメンテナンスを行うユーザは、データベース ユーティリティをよく理解しておく必要があります

■ 監査担当者

AUDITOR 属性が割り当てられたユーザは、監査ツール（CA ControlMinder エンドポイント管理 および seaudit ユーティリティ）をよく理解しておく必要があります。

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

■ 未承認アプリケーションを作成するプログラマ

プログラマは、作成するアプリケーションで CA ControlMinder* 関数ライブラリを使用して、保護されているリソースへのアクセスの制御（SEOSROUTE_RequestAuth 関数を使用）など、セキュリティに関連するサービスを要求できます。また、このインストールでは、インストール定義のリソース クラスを作成できます。導入先でこれらのリソース クラスのレコードを作成した場合、アプリケーションで SEOSROUTE_RequestAuth コマンドを発行して、アクションを完了するための十分な権限がユーザにあるかどうかをチェックできます。特定のユーザ アクションに必要な権限のレベルは、そのアプリケーションが SEOSROUTE_RequestAuth 関数を呼び出す方法に従って決定されます。

注: CA ControlMinder API の詳細については、「SDK 開発者ガイド」を参照してください。

■ 承認済みアプリケーションを作成するプログラマ

承認済みアプリケーション（SERVER 属性で実行するプログラム）を作成するプログラマは、CA ControlMinder* 関数ライブラリを使用して、セキュリティに関連する以下のサービスを要求できます。

- ユーザの識別と検証
- ユーザ ログアウト サービス
- ユーザ認証要求

CA ControlMinder エンタープライズ管理 の実装方法

組織に CA ControlMinder エンタープライズ管理 を実装する前に、インストールするコンポーネント、インストールの順序、インストール先について理解しておく必要があります。CA ControlMinder エンタープライズ管理 を組織に展開する際は、以下のガイドラインに従ってください。

- 実装プロセスは、上位から下位へと進めてください。エンタープライズ管理サーバのインストールから始め、追加の配布サーバをインストールし、Enterprise Reporting を実装してから、CA ControlMinder エンドポイントをインストールします。
- 実装を開始する前に、使用するコンピュータで必要な仕様が満たされていて、前提条件となるソフトウェアがすべてインストールされていることを確認してください。

注: 必須ハードウェアとソフトウェアの仕様書詳細については、[CA Support](#) の CA ControlMinder 製品ページから利用可能な CA ControlMinder Compatibility Matrix を参照してください。

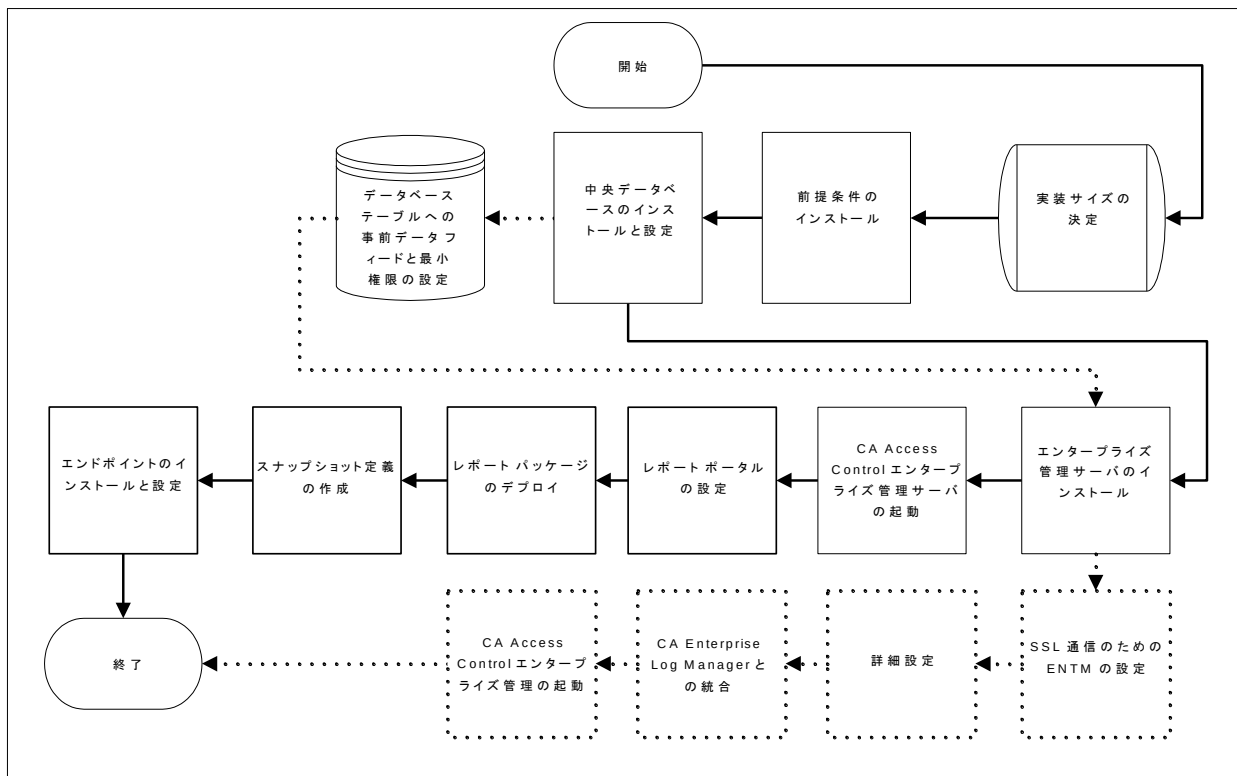
以下のプロセスを使用して、CA ControlMinder エンタープライズ管理 を実装します。

1. 使用する展開アーキテクチャを決定します
2. 中央データベースとしてサポートされている RDBMS をインストールします
3. (オプション) サポートされているユーザストアをインストールします
4. エンタープライズ管理サーバをインストールします
5. Enterprise Reporting を実装します
6. (オプション) CA User Activity Reporting Module と統合します
7. エンドポイントをインストールします

以下の図は、CA ControlMinder エンタープライズ管理 の実装プロセスを示しています。

エンタープライズ管理サーバの実装

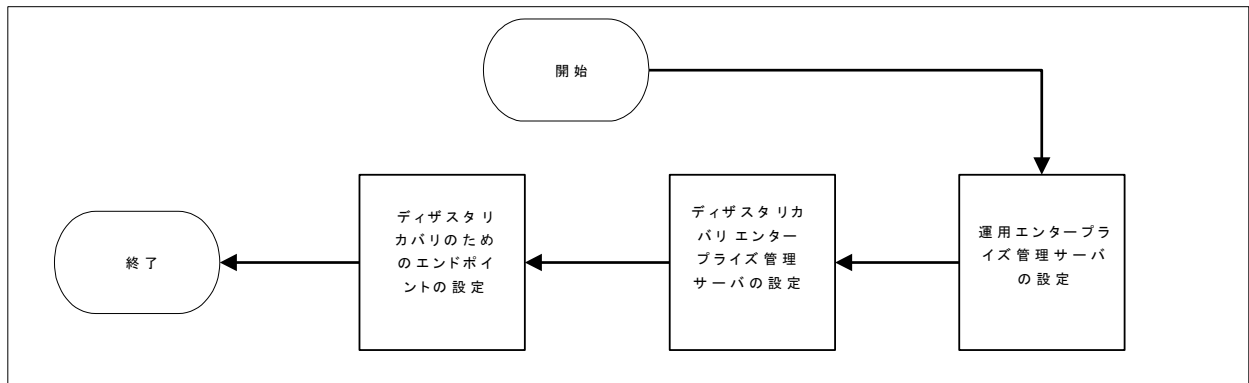
エンタープライズ管理サーバの実装の補助に、この図を使用してください。



注: 点線はオプションの手順を表しています。

ディザスタリカバリのための CA ControlMinder の実装

ディザスタリカバリ用の CA ControlMinder の実装の補助に、以下の図を使用します。



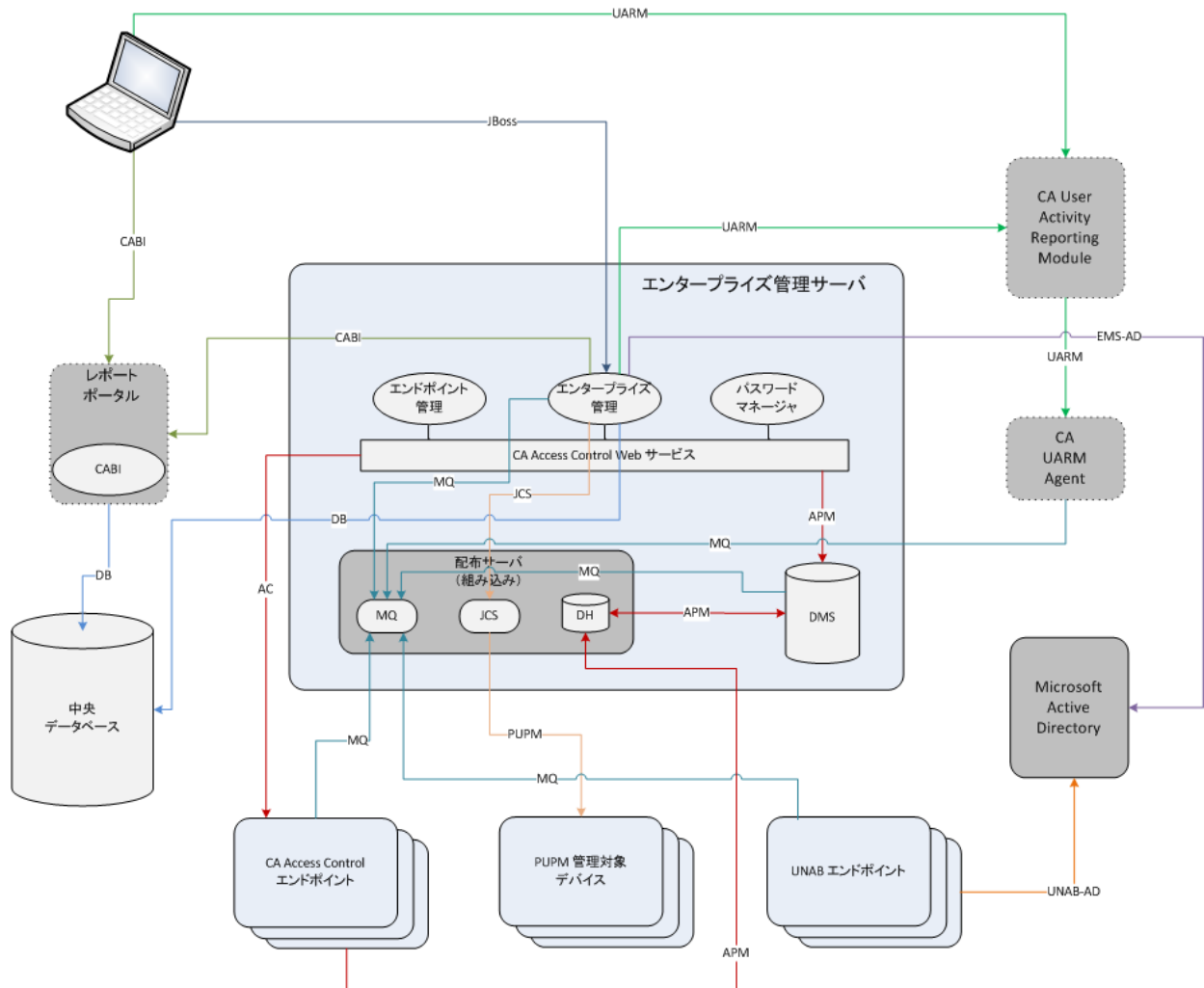
CA ControlMinder エンタープライズ管理 展開アーキテクチャ

CA ControlMinder エンタープライズ管理 の実装を開始する前に、以下の実装アーキテクチャのいずれを使用するか決定する必要があります。

- デフォルト -- デフォルト展開では、CA ControlMinder エンタープライズ管理 のすべてのコンポーネントを単一のサーバ上にインストールします。デフォルトアーキテクチャの実装はCA ControlMinder エンタープライズ管理 を実装する最も速い方法です。デフォルト実装アーキテクチャでは、ハイアベイラビリティおよびディザスタ リカバリ機能はサポートされません。
- 負荷分散 -- 負荷分散デプロイメント アーキテクチャによって、共通のユーザおよびデータ ストアを使用して、エンタープライズ管理サーバ間の作業負荷を分散することができます。負荷分散デプロイメントでは、プライマリおよび複数の負荷分散エンタープライズ管理サーバをデプロイします。
- ハイアベイラビリティ -- ハイアベイラビリティ展開アーキテクチャによって、フェールオーバーと冗長性が提供されるように CA ControlMinder エンタープライズ管理 を実装できます。ハイアベイラビリティ実装では、CA ControlMinder エンタープライズ管理 を複数のサーバ上に展開するため、サーバ障害時にエンドポイントからの継続的なアクセスが保障されます。
- ディザスタ リカバリ -- ディザスタ リカバリ展開アーキテクチャによって、ディザスタ リカバリが提供されるように CA ControlMinder エンタープライズ管理 を実装できます。ディザスタ リカバリ展開では、CA ControlMinder エンタープライズ管理 を複数のサーバ上に展開するため、ディザスタ リカバリが保障されます。

デフォルトのエンタープライズ展開アーキテクチャ

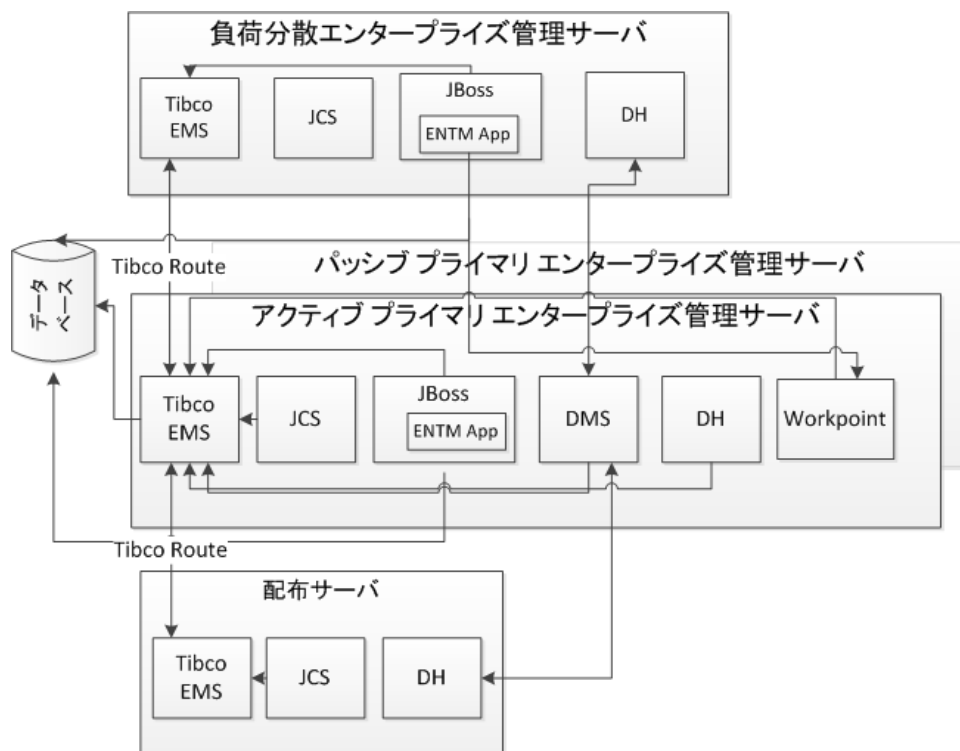
以下の図は、企業での CA ControlMinder の展開方法について示したものです。



注: 点線はオプション コンポーネントを示しています。

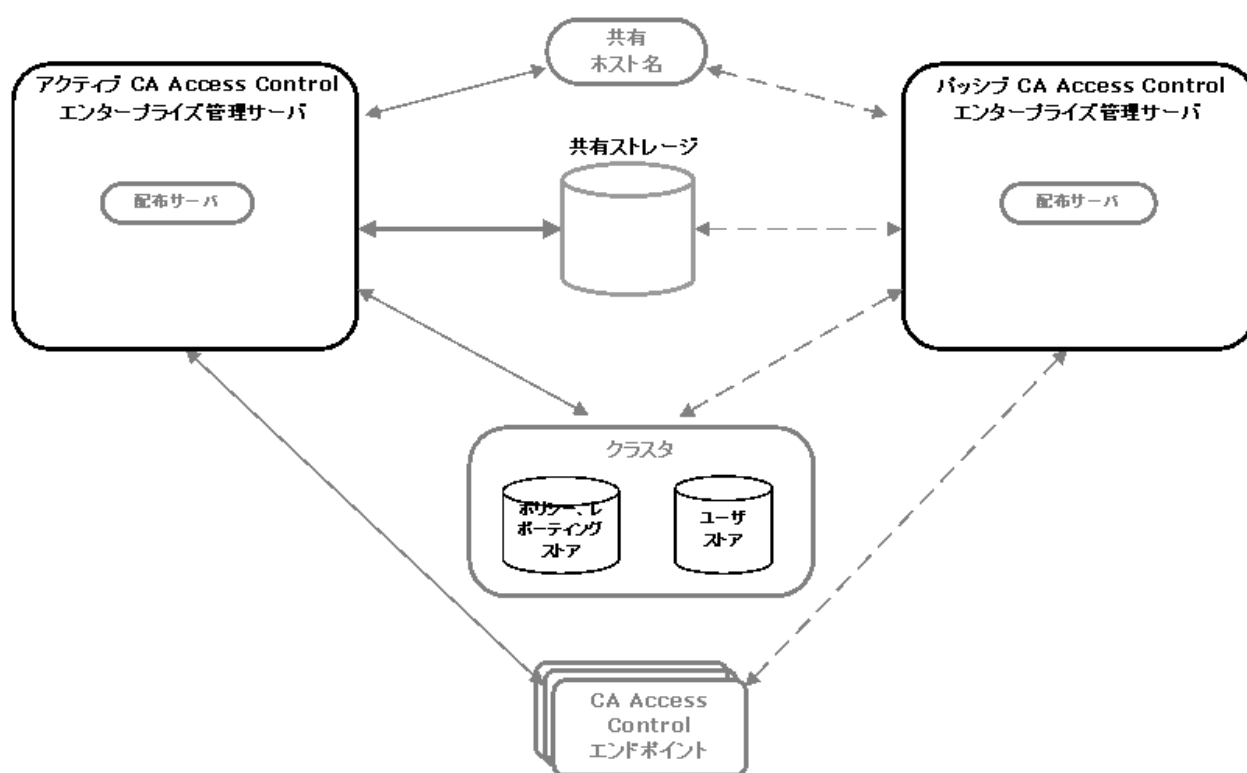
負荷分散デプロイメント アーキテクチャ

以下の図は、ユーザの組織で負荷分散エンタープライズ管理サーバをどのようにデプロイできるかを示します。



ハイアベイラビリティ展開アーキテクチャ

以下の図は、ハイアベイラビリティ環境における CA ControlMinder エンタープライズ管理 を示しています。

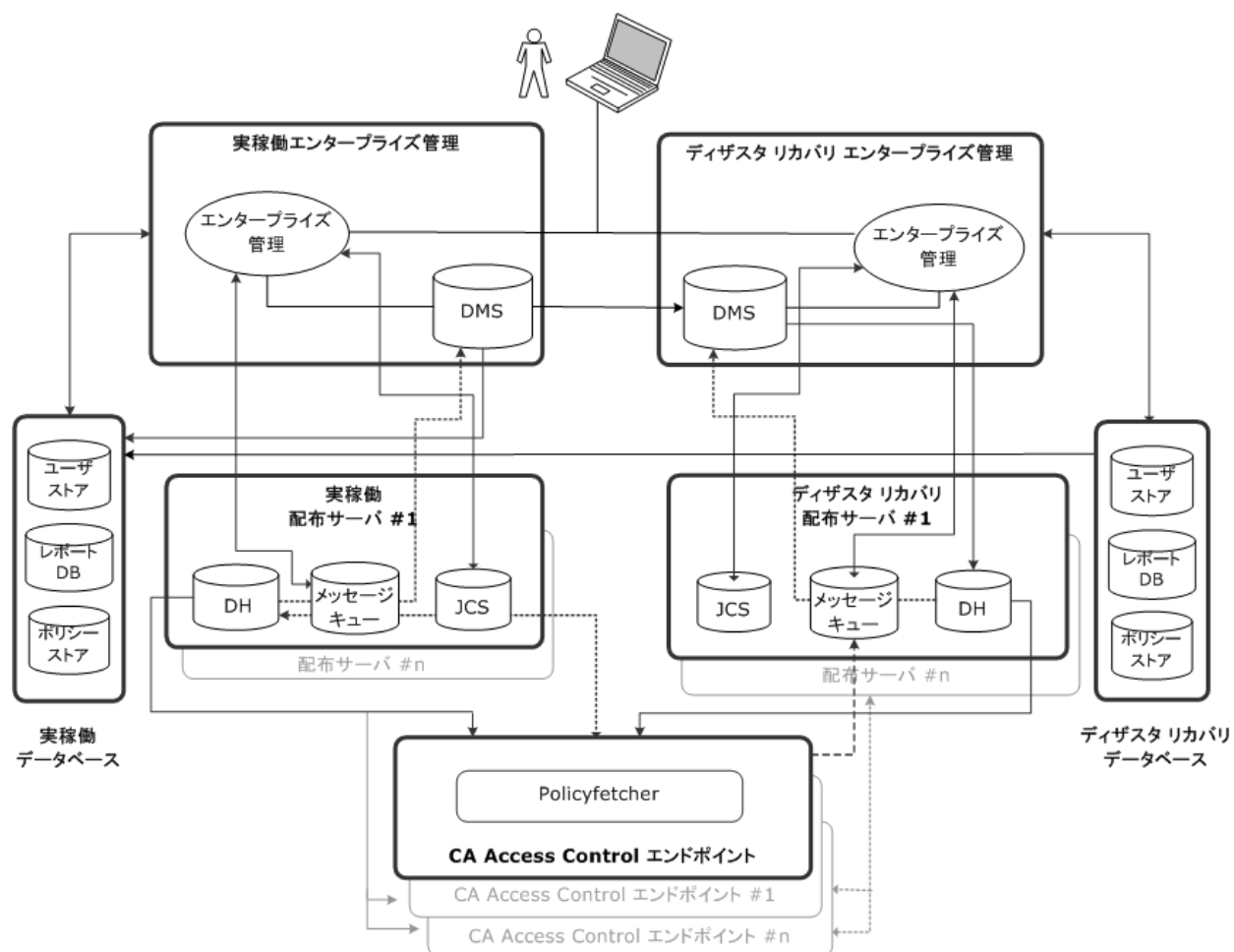


この図に示されるように、ハイアベイラビリティ展開には以下のコンポーネントがあります。

- プライマリ エンタープライズ管理サーバと、少なくとも 1 つのセカンダリ エンタープライズ管理サーバ
- ポリシーおよびレポートストアのクラスタ化されたインストール、およびユーザストア
- プライマリおよびセカンダリ CA ControlMinder エンタープライズ管理サーバからアクセス可能な共有ストレージ
- 共有ホスト名
- プライマリおよびセカンダリの両方のエンタープライズ管理サーバにアクセス可能な CA ControlMinder エンドポイント

ディザスタリカバリ アーキテクチャ

以下の図は、ディザスタリカバリ構成で、CA ControlMinder をどのように展開するかを示しています。



CA ControlMinder エンタープライズ管理 のコンポーネント

CA ControlMinder エンタープライズ管理 は以下のコンポーネントで構成されるか、以下のコンポーネントを使用します。

エンタープライズ管理サーバ

エンタープライズ管理サーバは集中管理サーバで、エンドポイントへのポリシーのデプロイ、特権アカウントの管理、リソース、アクセサ、およびアクセスレベルの定義を行うためのコンポーネントやツールが含まれています。エンタープライズ管理サーバには、エンタープライズ管理サーバ、エンドポイント、他のコンポーネント間の通信を管理するコンポーネントも含まれています。

エンタープライズ管理サーバをインストールすると、CA ControlMinder がサイレントインストールされます。CA ControlMinder は、エンタープライズ管理サーバを保護し、エンタープライズ管理サーバ上のアプリケーションをサポートするコア機能を提供します。

配布サーバ

配布サーバは、アプリケーションサーバとエンドポイント間の通信を処理します。配布サーバには次のコンポーネントが含まれています。

- 配布ホスト (DH)
- メッセージキュー (MQ)
- Java 接続サーバ (JCS)

注: フェイルオーバーのため、企業内で複数の配布サーバをインストールしたり、複数のコンピュータに配布サーバコンポーネントをインストールしたりすることができます。配布サーバはデフォルトではエンタープライズ管理サーバ上にインストールされます。

配布ホスト(DH)

DH は、DMS で設定されたポリシー デプロイをエンドポイントに配布します。また、エンドポイントからデプロイ ステータスを受信して、DMS に送信します。このタスクを達成するために、DH は 2 つの Policy Model データベースを使用します。

- **DH Writer** - エンドポイントから受信したデータを DMS に書き込みます。

この PMDB の名前は、*DHNameWRITER* です。ここで、*DHName* は DH の名前であり、デフォルトでは **DH__** となります。

- **DH Reader** - DMS からデータを読み取り、エンドポイントがそのデータを取得できるようにします。

この PMDB の名前は、*DHName* です。ここで、*DHName* は DH の名前であり、デフォルトでは **DH__** となります。

デフォルトでは、DH は 配布サーバと同じコンピュータにインストールされます。ただし、複数の DH ノードをインストールし、各 DH に企業の 1 部門を管理させて、負荷を分散させることもできます。

メッセージ キュー

メッセージ キューは、エンタープライズ管理サーバと他のコンポーネント間で送受信されるメッセージを管理します。メッセージ キューには、エンタープライズ管理サーバと通信する各クライアント コンポーネント専用の以下のキューがあります。

- レポート キュー - エンドポイント データベースのスケジュールされたスナップショットを受信します。
レポート サービスは、スナップショットを使用して **CA ControlMinder** レポートを生成します。
- 監査キュー - エンドポイント上で発生した監査イベントを受信します。
監査イベントを収集し、レポートするように **CA Enterprise Log Manager** を設定できます。
- サーバ - エンドポイント キュー - エンドポイントが収集した **DMS** からのデータを受信します。
たとえば、**UNAB** 設定ポリシーをデプロイする場合、**DMS** は設定ポリシーをこのキューに送信します。**UNAB** エージェントは、このキューからポリシーを収集し、**UNAB** エンドポイントにポリシーをデプロイします。
- エンドポイント - サーバ キュー - **DMS** が収集したエンドポイントの情報を受信します。
たとえば、**UNAB** エンドポイントはハートビート通知をこのキューに送信します。**DMS** は、このキューからハートビート通知を収集し、データベース内のエンドポイントのステータスを更新します。

Java 接続サーバ(JCS)

Java コネクタ サーバ (**JCS**) は、**Windows** オペレーティング システムや **SQL** サーバのように、**Java** がサポートする管理デバイスと通信し、**SAM** エンドポイントの特権アカウントを管理します。

Web ベースのアプリケーション

CA ControlMinder のエンタープライズ インストールを管理するために Web ベースのアプリケーションを使用します。 Web ベースのアプリケーションはアプリケーション サーバにインストールします。 アプリケーション サーバは、デフォルトではエンタープライズ管理サーバ上にインストールされます。

アプリケーション サーバには次の Web ベース アプリケーションが含まれています。

- CA ControlMinder エンタープライズ管理 -- 企業のネットワーク全体でポリシーを管理し、エンドポイントを設定できます。また、CA ControlMinder エンタープライズ管理 に含まれている特権ユーザパスワード管理 (SAM) は、企業のネットワーク全体で特権アカウントを管理し、特権アカウントのパスワードボールドとして機能します。
- CA ControlMinder エンドポイント管理 - 各 CA ControlMinder エンドポイントを中央の管理サーバから管理および設定します。
- CA ControlMinder パスワード マネージャ - CA ControlMinder のユーザパスワードを管理します。 CA ControlMinder ユーザのパスワードを変更したり、次回ログイン時にユーザに強制的にパスワードを変更させたりすることができます。

CA ControlMinder エンタープライズ管理

CA ControlMinder エンタープライズ管理 はエンタープライズを管理するユーザ インターフェースです。CA ControlMinder エンタープライズ管理 および CA ControlMinder エンドポイントの初期インストールを完了した後、ユーザ インターフェースに習熟することをお勧めします。

CA ControlMinder エンタープライズ管理 を運用するのを助けるために、問題特定のタスクがタブの下でグループ化されます。これらの結果を使用して、以下のことができます。

- エンタープライズの全体にわたる CA ControlMinder 実装の表示
- ホストとホスト グループを設定と、CA ControlMinder と UNAB エンドポイントへのポリシーの割り当て
- 特権アカウント パスワードをチェックアウトおよびチェックインします。
- 特権アカウント、エンドポイント、パスワード ポリシーおよびパスワード コンシューマの設定
- レポートの表示、スナップショット定義の管理およびスナップショット データのキャプチャ
- ユーザ、グループ、ロールおよびタスクの管理
- システム全体の接続設定の管理
- 監査レコードの表示

注: CA ControlMinder エンタープライズ管理 でのタスクの完了の詳細については、[オンライン ヘルプ](#)を参照してください

デプロイ マップ サーバ(DMS)

DMS は、拡張ポリシー管理の中核となります。DMS は、ポリシーに関する最新情報（ポリシーのバージョンおよびスクリプト）と、各コンピュータ上でのポリシー デプロイ ステータスを保持することを目的としています。DMS には、ポリシーのバージョンが格納され、後から必要に応じてこれらのバージョンの割り当て、割り当て解除、デプロイ、およびデプロイ解除を行うことができます。

DMS は Policy Model ノードであり、データ リポジトリとして PMDB を使用します。DMS は、これが設定された各エンドポイントからの通知から受信したデータを収集し、これらのエンドポイントの各々のデプロイ情報を格納します。

レポート ポータル

レポート ポータルは CA ControlMinder レポートを表示します。

CA ControlMinder レポートは、各エンドポイントにある CA ControlMinder データベース内のデータに関する情報を提供します。データに関する情報とは、エンドポイントにデプロイしたルールやポリシー、およびそれらのルールやポリシーからの偏差です。CA ControlMinder レポートは、CA Business Intelligence または CA ControlMinder エンタープライズ管理 で参照します。

中央の RDBMS には、CA ControlMinder レポートで使用されるエンドポイント データが格納されています。

セントラル RDBMS

セントラル RDBMS には以下が格納されています。

- CA ControlMinder レポートで使用するエンドポイント データ
- 特権アカウントのパスワード
- Web ベース アプリケーションのセッション データ
- Web ベース アプリケーションのユーザ データ (ユーザ ストアとして Active Directory または Sun ONE を使用しない場合)

注: Web ベースのアプリケーションは、CA ControlMinder エンタープライズ管理、CA ControlMinder エンドポイント管理、および CA ControlMinder パスワードマネージャです。

エンドポイント

CA ControlMinder を企業内で展開する場合、3 つのタイプのエンドポイントがあります。

- CA ControlMinder エンドポイント - CA ControlMinder をインストールしたエンドポイント。
CA ControlMinder エンドポイントは、オプションで、SAM エンドポイントとして設定することも可能です。
- UNAB エンドポイント - UNIX 認証ブローカ (UNAB) をインストールした UNIX エンドポイント。
- SAM エンドポイント - Privileged User Password Management (PUPM) で管理するエンドポイント。

CA User Activity Reporting Module コンポーネント

CA ControlMinder 監査イベントは、各エンドポイントから、そして、エンタープライズ管理サーバから CA User Activity Reporting Module に送信して、収集およびレポートに利用できます。以下のコンポーネントは、CA ControlMinder と CA User Activity Reporting Module の統合をサポートしています。

- CA User Activity Reporting Module エージェント - 配布サーバ上の監査キューから監査イベントを収集し、CA User Activity Reporting Module サーバに処理用に送信します。
- CA User Activity Reporting Module サーバ - 監査イベントを受信し、場合によっては抑制および集約ルールを適用後に、イベントを格納します。

注: CA User Activity Reporting Module コンポーネントの詳細については、CA User Activity Reporting Module のマニュアルを参照してください。

ユーザストア

Active Directory または Sun One で定義されているグループとユーザを使用するように CA ControlMinder と CA ControlMinder の Web ベース アプリケーションを設定できます。これは、単一のデータストアをすべてのユーザに対して使用できることを意味します。

注: Web ベースのアプリケーションは、CA ControlMinder エンタープライズ管理、CA ControlMinder エンドポイント管理、および CA ControlMinder パスワードマネージャです。

実装のサイジング

CA ControlMinder の実装を開始できるようになる前には、実装のサイズを見積もって、それに応じてリソースを割り当てる必要があります。実装の見積もり評価のために、以下の情報を使用します。

CA ControlMinder のエンドポイント 3000 ごとに配布サーバを 1 台インストールすることをお勧めします。

以下の表では、エンタープライズ管理サーバおよびレポート ポータル コンピュータ上でさまざまなコンポーネント用に割り当てる必要があるデータベースサイズの合計について説明します。

コンポーネント	基準	ゲージ	割り当て量
エンタープライズ管理サーバ	ユーザストアとしての Active Directory	1000 Active Directory アカウントごと	20 MB
CA ControlMinder	スナップショットのレポート	1000 CA ControlMinder エンドポイントごと	スナップショットごとに 5GB
SAM	エンドポイント タイプの定義	1000 PUPM エンドポイントごと	2 MB
SAM	特権アカウント	1000 特権アカウントごと	75 MB
SAM	特権アカウント パスワード操作	1000 PUPM 特権アカウント パスワード操作ごと	250 MB
CA Business Intelligence	CMS および監査データベース	基本的なインストール	300 MB

注: システム要件の詳細については、「リリースノート」を参照してください。

CA ControlMinder データベース サイズの制限

CA ControlMinder データベースでは、オブジェクト数が 100 万 (1,000,000) 個に制限されています。大規模な環境で拡張ポリシー管理を使用している場合のみ、このサイズ制限がデプロイメントに影響を及ぼす可能性があります。

企業内の CA ControlMinder データベースで 1,000,000 個のオブジェクトを保持する可能性がある場合、使用されていない古いデプロイメント オブジェクトを削除する必要があります。

例: CA ControlMinder データベース内のオブジェクト数の算出

以下の例では、DMS - セントラル CA ControlMinder 管理データベース内に保持されるオブジェクト数の算出方法を示しています。

この例では、CA ControlMinder エンタープライズ デプロイメントが 5000 個のエンドポイント上に存在し、各エンドポイントでアサインされたポリシーを 50 個保持しています。その結果、以下に示すように、DMS には少なくとも 250,000 個のオブジェクトが含まれていることになります。

$5,000 \text{ エンドポイント} \times 50 \text{ ポリシー} = 250,000 \text{ デプロイメント オブジェクト}$

各ポリシーの 4 つのバージョンを作成し、そのポリシーを 5000 個のエンドポイントにそれぞれアサインすると、DMS のオブジェクト数は以下のよう に オブジェクト数の制限値である 1,000,000 個に達します。

$5,000 \text{ エンドポイント} \times 50 \text{ ポリシー} \times 4 \text{ バージョン} = 1,000,000 \text{ デプロイメント オブジェクト}$

第 3 章：サイジングとパフォーマンス

このセクションには、以下のトピックが含まれています。

[サイジングとパフォーマンスのデータ](#) (P. 45)

[パフォーマンス結果](#) (P. 52)

サイジングとパフォーマンスのデータ

環境への CA ControlMinder の実装を開始する前に、サイジングとパフォーマンスのデータを確認することをお勧めします。この情報を使用して、リソースプランを作成し、それにしたがってリソースを割り当てます。

注: データは、小、中、大規模の CA ControlMinder 環境でパフォーマンスのテストを行った後に、収集されます。

テストされた機能

CA ControlMinder の以下のパフォーマンス機能が、小規模（100 アカUNT）、中規模（1000 アカUNT）、および大規模（100,000 アカUNT）な CA ControlMinder 環境上でテストされました。

- アカUNT パスワードチェックアウトおよびチェックイン
- パスワードポリシーによるパスワードリセット
- スナップショットのキャプチャ

データ設定

コンポーネントおよび機能は、以下のデータ設定でテストされました。

テストされた機能	小規模な環境	中規模な環境	大規模な環境
管理対象アカUNT	100	1000	100,000
SAM ユーザ	10	100	1000
チェックアウトおよび チェックイン(1 日あたり、 1 ユーザあたり)	5	5	5

テストされた機能	小規模な環境	中規模な環境	大規模な環境
パスワードの一括変更の頻度	90 日	90 日	90 日
エンタープライズ管理サーバの数	1	2 (1つのプライマリ、1つのロードバランシング)	2 (1つのプライマリ、1つのロードバランシング)

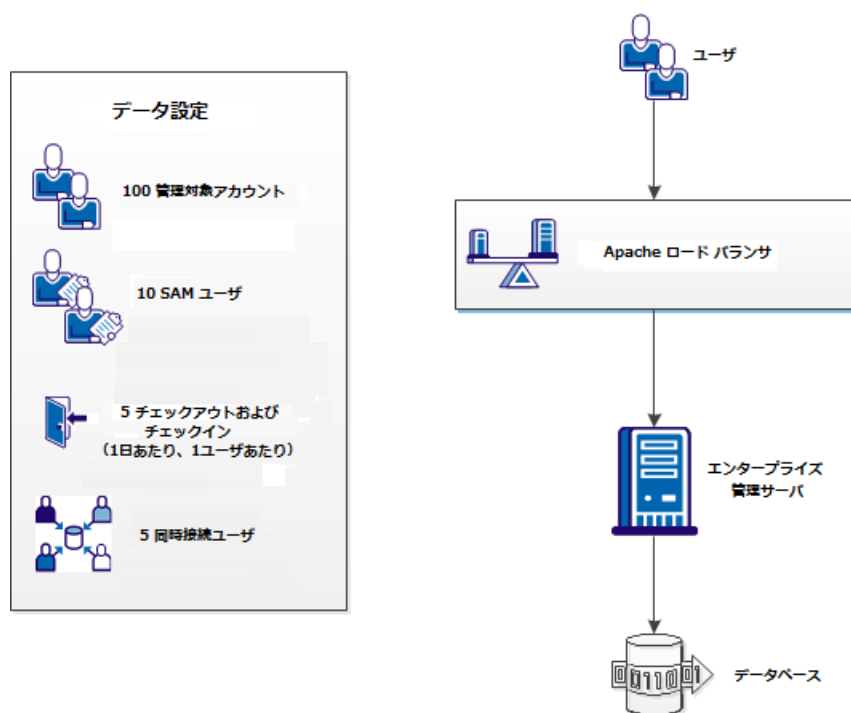
展開アーキテクチャ

このセクションでは、小、中、大規模環境用の展開アーキテクチャの詳細について説明します。

小規模環境(100 の管理対象アカウント)用の展開アーキテクチャ

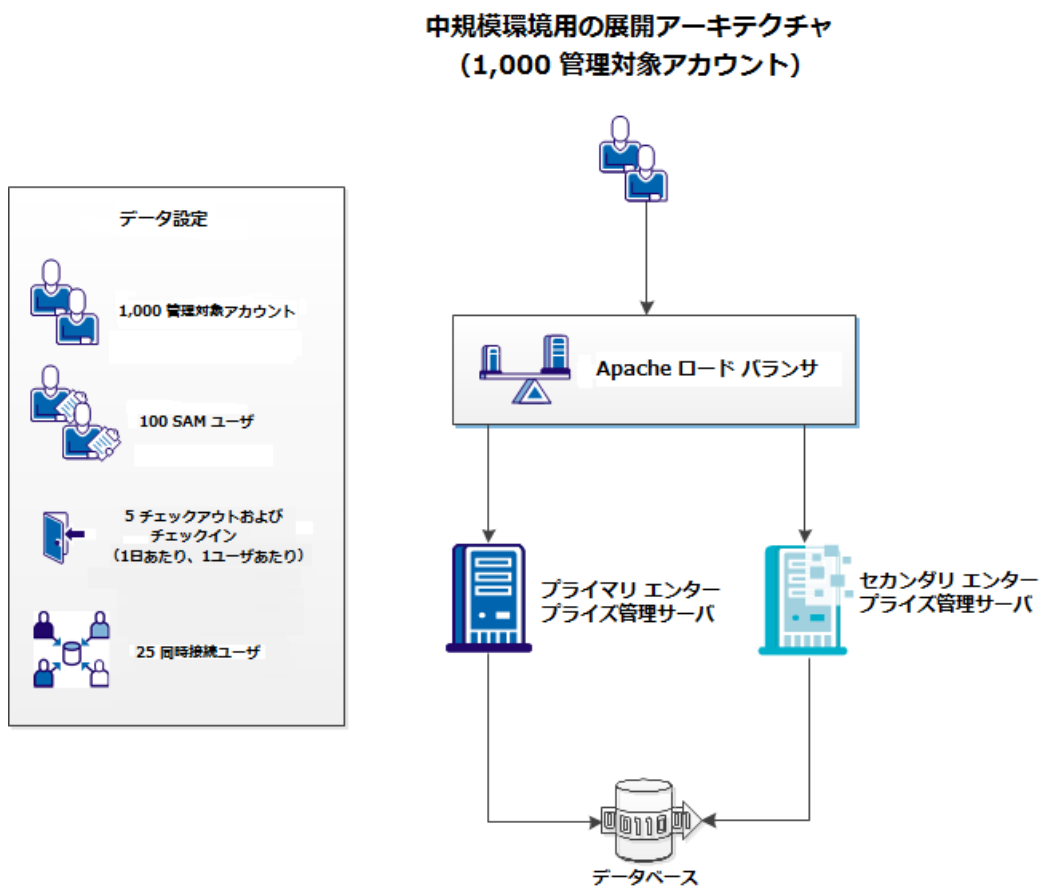
以下の図は、小規模環境用のテスト済み展開アーキテクチャを示しています。

小規模環境用の展開アーキテクチャ
(100 管理対象アカウント)



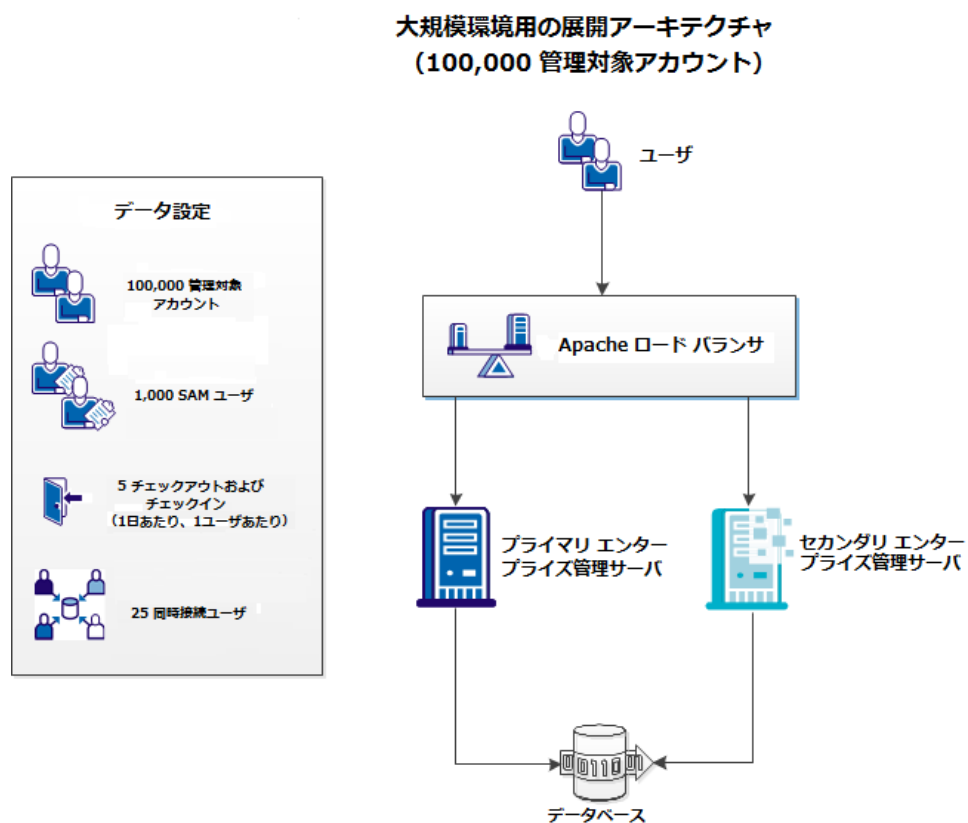
中規模環境(1000 の管理対象アカウント)用の展開アーキテクチャ

以下の図は、中規模環境用のテスト済み展開アーキテクチャを示しています。



大規模環境(100,000 の管理対象アカウント)用の展開アーキテクチャ

以下の図は、大規模環境用のテスト済み展開アーキテクチャを示しています。



ハードウェアとソフトウェアの設定

このセクションでは、製品のパフォーマンス テスト中にテストされ、プロファイルされた設定の詳細について説明します。

小規模環境用ハードウェアおよびソフトウェア設定

パフォーマンス データを収集するために、以下のテスト環境が使用されました:

コンポーネント	詳細	仕様
エンタープライズ管理サーバ	オペレーティングシステム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1

コンポーネント	詳細	仕様
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	8,192 MB
	オブジェクト/ユーザ ストア	SQL 2008/Active Directory
	サードパーティの詳細	Jboss-4.2.3.GA Java バージョン 1.6.0_30 Java (TM) SE ランタイム環境 (ビルド 1.6.0_30-b12) Java HotSpot (TM) 64 ビットのサーバ VM (ビルド 20.5-b03、混合モード)
データベース	オペレーティングシステム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	8,192 MB
	データベース	Microsoft SQL Server 2008
Active Directory	オペレーティングシステム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	4,096 MB
	AD ユーザ/グループの数	1000 ユーザおよび 100 グループ (グループにはそれぞれ 10 人のユーザが含まれます)
ロード バランサ (Apache サーバ)	オペレーティングシステム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	2,048 MB
	Apache バージョン	Apache HTTP サーバ バージョン 2.2

中規模環境用ハードウェアおよびソフトウェア設定

パフォーマンス データを収集するために、以下のテスト環境が使用されました:

コンポーネント	詳細	仕様
エンタープライズ管理 サーバ	オペレーティング システム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	8,192 MB
	オブジェクト/ユー ザ ストア	SQL 2008/Active Directory
	サードパーティの 詳細	Jboss-4.2.3.GA Java バージョン 1.6.0_30 Java (TM) SE ランタイム環境 (ビルド 1.6.0_30-b12) Java HotSpot (TM) 64 ビットのサーバ VM (ビル ド 20.5-b03、混合モード)
データベース	オペレーティング システム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	4
	物理メモリ (RAM)	8,192 MB
	データベース	Microsoft SQL Server 2008
Active Directory	オペレーティング システム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	4,096 MB
	AD ユーザ/グルー プの数	10,000 ユーザおよび 500 グループ (グループには それぞれ 100 ユーザが含まれます)

コンポーネント	詳細	仕様
ロード バランサ (Apache サーバ)	オペレーティング システム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	2,048 MB
	Apache バージョン	Apache HTTP サーバ バージョン 2.2

大規模環境用ハードウェアおよびソフトウェア設定

パフォーマンス データを収集するために、以下のテスト環境が使用されました:

コンポーネント	詳細	仕様
エンタープライズ管理 サーバ	オペレーティング システム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	8,192 MB
	オブジェクト/ユー ザストア	SQL 2008/Active Directory
	サードパーティの 詳細	Jboss-4.2.3.GA Java バージョン 1.6.0_30 Java (TM) SE ランタイム環境 (ビルド 1.6.0_30-b12) Java HotSpot (TM) 64 ビットのサーバ VM (ビルド 20.5-b03、混合モード)
データベース	オペレーティング システム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	4
	物理メモリ (RAM)	8,192 MB
	データベース	Microsoft SQL Server 2008

コンポーネント	詳細	仕様
Active Directory	オペレーティングシステム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	4,096 MB
	AD ユーザ/グループの数	100,000 ユーザおよび 10,000 グループ (グループにはそれぞれ 1,000 ユーザが含まれます)
ロード バランサ (Apache サーバ)	オペレーティングシステム	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
	システム タイプ	x64 ベースのコンピュータ
	プロセッサ数	2
	物理メモリ (RAM)	2,048 MB
	Apache バージョン	Apache HTTP サーババージョン 2.2

パフォーマンス結果

このセクションでは、製品のパフォーマンス テスト中にテストされ、プロファイルされたパフォーマンスの結果の詳細について説明します。

小規模環境用のパフォーマンス結果

以下のセクションでは、小規模環境用のテスト中のパフォーマンス結果の詳細について説明します。

データベース アクティビティ サマリ(小規模環境)

以下のテーブルでは、小規模環境用のパフォーマンス テスト中のデータベース アクティビティの詳細について説明します。

アクティビティ	データベースの成長
エンタープライズ管理サーバの新規インストール時のデータベース サイズ	15.06 MB

アクティビティ	データベースの成長
エンタープライズ管理サーバの新規インストールで 100 アカウントを作成した後のデータベース サイズ	21.06 MB
特権アカウント チェックアウトおよびチェックイン中のデータベースの成長	3 MB
パスワード ポリシーによるパスワード リセット中のデータベースの成長	0.039 MB
スナップショットのキャプチャ中のデータベースの成長	3 MB
アクティビティがレポートされない日の 1 日あたりのデータベースの成長	3 MB

中規模環境用のパフォーマンス結果

以下のセクションでは、中規模環境用のテスト中のパフォーマンス結果の詳細について説明します。

データベース アクティビティ サマリ(中規模環境)

以下のテーブルでは、中規模環境用のパフォーマンス テスト中のデータベース アクティビティの詳細について説明します。

アクティビティ	データベースの成長
エンタープライズ管理サーバの新規インストール時のデータベース サイズ	15.06 MB
エンタープライズ管理サーバの新規インストールで 1000 アカウントを作成した後のデータベース サイズ	69.56 MB
特権アカウント チェックアウトおよびチェックイン中のデータベースの成長	56 MB
パスワード ポリシーによるパスワード リセット中のデータベースの成長	1 MB
スナップショットのキャプチャ中のデータベースの成長	31.63 MB
アクティビティがレポートされない日の 1 日あたりのデータベースの成長	3 MB

大規模環境用のパフォーマンス結果

以下のセクションでは、大規模環境用のテスト中のパフォーマンス結果の詳細について説明します。

データベース アクティビティ サマリ(大規模環境)

以下のテーブルでは、大規模環境用のパフォーマンス テスト中のデータベース アクティビティの詳細について説明します。

アクティビティ	データベースの成長
エンタープライズ管理サーバの新規インストール時のデータベース サイズ	15.06 MB
エンタープライズ管理サーバの新規インストールで 100,000 アカウントを作成した後のデータベース サイズ	1045.19 MB
特権アカウント チェックアウトおよびチェックイン中のデータベースの成長	556 MB
パスワード ポリシーによるパスワードリセット中のデータベースの成長	138 MB
スナップショットのキャプチャ中のデータベースの成長	705 MB
アクティビティがレポートされない日の 1 日あたりのデータベースの成長	3 MB

統合されたデータベース メトリック

以下のテーブルでは、小、中、大規模環境用の統合されたデータベース アクティビティの詳細について説明します。

イベント	小規模な環境	中規模な環境	大規模な環境
エンタープライズ管理サーバの新規インストール時のデータベース サイズ	15.06 MB	15.06 MB	15.06 MB
エンタープライズ管理サーバの新規インストールで管理対象アカウントを作成した後のデータベースの成長	6 MB	54.5 MB	1030.13 MB

イベント	小規模な環境	中規模な環境	大規模な環境
特権アカウント チェックアウト およびチェックイン中のデータ ベースの成長	3 MB	56 MB	556 MB
パスワード ポリシーによるパス ワードリセット中のデータベー スの成長	0.039 MB	1 MB	138 MB
スナップショットのキャプチャ 中のデータベースの成長	3 MB	31.63 MB	705 MB
アクティビティがレポートされ ない1日あたりの のデータベー スの成長	3 MB	3 MB	3 MB

第 4 章: エンタープライズ管理サーバのインストール

このセクションには、以下のトピックが含まれています。

[環境アーキテクチャ \(P. 57\)](#)

[エンタープライズ管理サーバの準備方法 \(P. 59\)](#)

[必須ソフトウェア インストール ユーティリティの実行 \(P. 69\)](#)

[エンタープライズ管理サーバ コンポーネントのインストール方法 \(P. 70\)](#)

[配布サーバの実装 \(P. 122\)](#)

環境アーキテクチャ

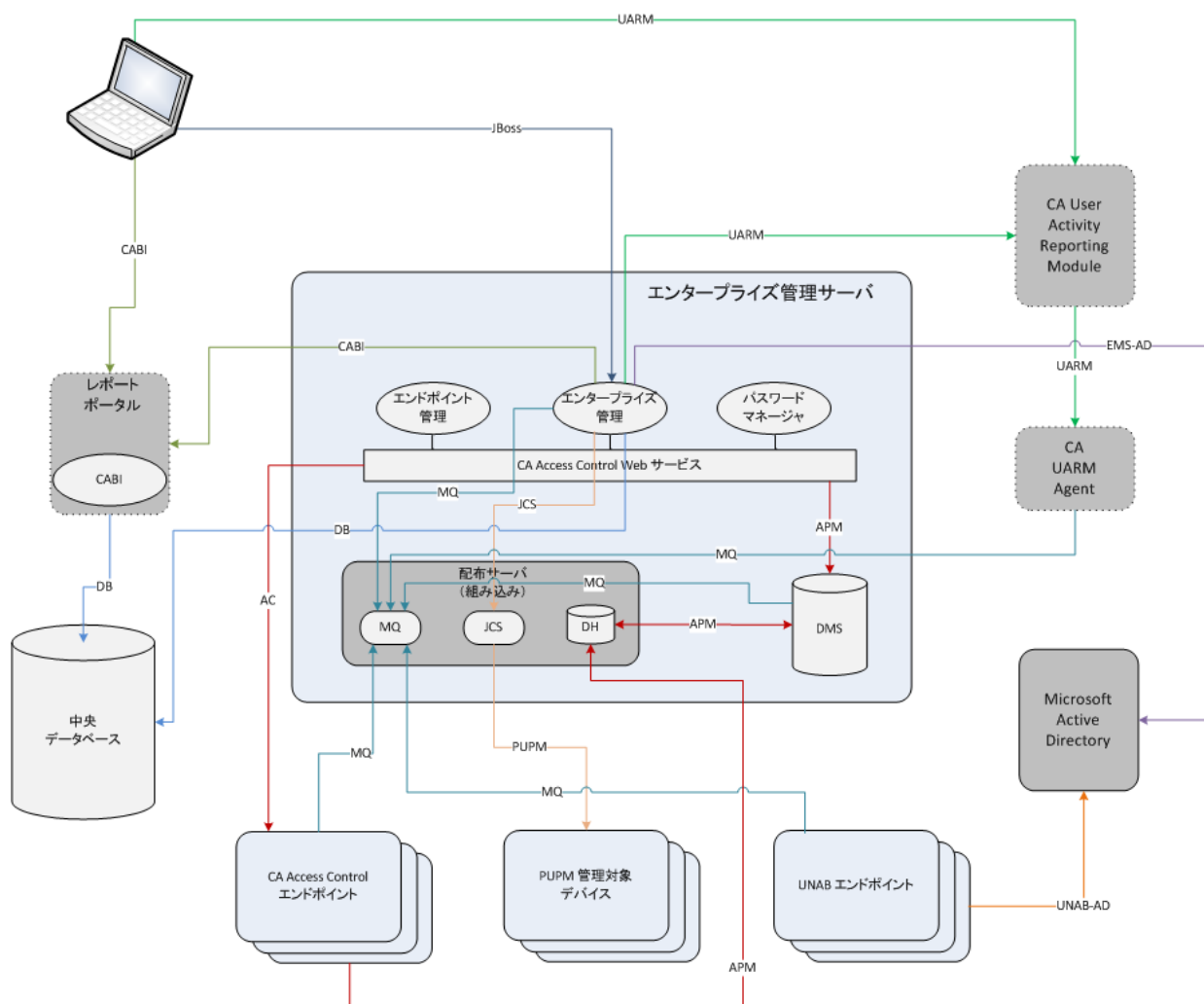
CA ControlMinder のエンタープライズインストールでは、ポリシー、特権アカウント、および CA ControlMinder エンドポイントの集中管理、各エンドポイントのポリシー情報の表示、およびエンドポイントのセキュリティステータスのレポートが可能です。これらの機能は、Web ベース インターフェース、またはユーティリティによって管理できます。

CA ControlMinder のエンタープライズインストールを管理するには、中央コンピュータにエンタープライズ管理サーバをインストールし、組織に合わせて設定する必要があります。

エンタープライズ管理サーバをインストールすると、CA ControlMinder がサイレントインストールされます。CA ControlMinder は、エンタープライズ管理サーバを保護し、エンタープライズ管理サーバ上のアプリケーションをサポートするコア機能を提供します。

エンタープライズ管理サーバをインストールしたら、CA ControlMinder および UNAB エンドポイントをインストールして設定します。既存の CA ControlMinder エンドポイントがある場合、拡張ポリシー管理およびレポート用に、各エンドポイントを設定する必要があります。

次の図に、エンタープライズ管理サーバのアーキテクチャを示します。



上の図は、以下のことを示します。

- エンタープライズ管理サーバでは以下のポートを使用します。
 - 対称暗号化にポート 8891、および CA ControlMinder エンドポイントとの SSL 通信にポート 5249
 - RDBMS との通信にポート 1433 (MS SQL) または 1521 (Oracle)
 - Active Directory との暗号化通信にポート 389 または 686
 - Java コネクタ サーバ (JCS) との暗号化通信にポート 20411
 - メッセージキューとの暗号化通信にポート 7243

- SAM は、エンドポイント タイプ（Windows Agentless、SSH デバイスなど）に基づいてエンドポイントと通信します。
- エンタープライズ管理サーバは、ポート 8080 を使用して CA Business Intelligence と通信します。
- エンタープライズ管理サーバは、暗号化通信用にポート 5250 を使用して CA User Activity Reporting Module と通信します。
- UNAB は、ポート 53、88、123、289、445、464、3268 を使用して Active Directory と通信します。

エンタープライズ管理サーバの準備方法

Windows でのエンタープライズ管理サーバの準備

Windows で該当

エンタープライズ管理サーバをインストールする前に、サーバを準備します。r12.5 以降のインストールをアップグレードしている場合は、エンタープライズ管理サーバに関する準備は整っています。再度これらの手順を行う必要はありません。

注: エンタープライズ管理サーバのインストール時に、CA ControlMinder エンドポイント管理 がまだインストールされていない場合、インストールプログラムにより、そのインストールも行われます。CA ControlMinder エンドポイント管理 をインストール済みの場合は、これらの手順を繰り返さないでください。

以下の手順に従います。

1. エンタープライズ管理用の中央データベースの準備

RDBMS ネイティブ管理ツールを使用して、手動で中央データベースを作成および設定することによってデータベースを準備することもできます。

2. 以下の方法のいずれかを使用して、必須のソフトウェアをインストールします。

■ [前提条件インストールユーティリティを実行します \(P. 69\)](#)。

CA ControlMinder は、Java Development Kit (JDK) および JBoss アプリケーションサーバをインストールするユーティリティを提供します。これらのソフトウェアをすでにインストール済みである場合は、この手順をスキップできます。

■ 既存のソフトウェアを使用するか、または以下のとおり必須のソフトウェアを手動でインストールします。

注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA ControlMinder Third Party Components DVD に格納されています。サポートされている JBoss バージョンの詳細については、「リリースノート」を参照してください。

- a. サポートされているバージョンの Java Development Kit (JDK) をインストールします。
- b. サポートされている JBoss バージョンをインストールします。JBoss をサービスとして実行することをお勧めします。

注: すでに JBoss がインストールされている場合、オープンポートの問題を解決するために CA ControlMinder エンタープライズ管理 をインストールする前に、JBoss を一度だけ実行することをお勧めします。CA ControlMinder エンタープライズ管理 インストールプログラムはデフォルト JBoss ポートを使用しません。たとえば、インストールプログラムは、HTTP 接続用のポート番号 8080 ではなくポート番号 18080 を使用します。エンタープライズ管理サーバインストール中に JBoss が使用するポートを指定していることを確認します。

これで、CA ControlMinder エンタープライズ管理 をエンタープライズ管理サーバにインストールする準備ができました。

Linux でのエンタープライズ管理サーバの準備

Linux で該当

エンタープライズ管理サーバをインストールする前に、サーバを準備します。r12.5 以降のインストールをアップグレードしている場合は、エンタープライズ管理サーバに関する準備は整っています。再度これらの手順を行う必要はありません。

エンタープライズ管理サーバのインストール時に、CA ControlMinder エンドポイント管理 がまだインストールされていない場合、インストール プログラムによって、そのインストールも行われます。CA ControlMinder エンドポイント管理 をインストール済みの場合は、これらの手順を繰り返さないでください。

以下の手順に従います。

1. エンタープライズ管理用の中央データベースの準備

注: データベース管理者が CA ControlMinder がデータベースに対して行う変更を確認および制御する場合は、RDBMS ネイティブ管理ツールを使用して中央データベースを作成および設定して、データベースを手動で準備できます。

2. Java Development Kit (JDK) のサポートされているバージョンをインストールするか、または既存のソフトウェアを使用します。

注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA ControlMinderThird Party Components DVD に格納されています。サポートされている JBoss バージョンの詳細については、「リリースノート」を参照してください。

- a. サーバ アーキテクチャが 32 ビットか 64 ビットか判断するために、システム情報を出力します。

```
uname -m
```

コマンドが「i386」または「i686」を返す場合、アーキテクチャは 32 ビットです。「x86_64」を返す場合、アーキテクチャは 64 ビットです。

- b. インストール メディア上で "x86" ディレクトリ (32 ビット用) または "x64" ディレクトリ (それぞれ 64 ビット用) に移動し、インストーラを実行します。例:

```
chmod 750 jdk-7u21-linux-x64.rpm.bin
./jdk-7u21-linux-x64.rpm.bin
```

- c. JDK/bin パスをシステム パスへ追加します。

たとえば、`bash` シェルを使用して、パス「`/usr/java/jdk1.7.0_21/`」を設定するには、以下のコマンドを入力します。

```
export PATH=/usr/java/jdk1.7.0_21/bin:$PATH
```

注: パスを恒久的に設定するには、以下のコマンドをユーザのシェル スタートアップ ファイルに追加します。

3. サポートされている JBoss バージョンをインストールするか、既存のソフトウェアを使用します。JBoss をデーモンとして実行することをお勧めします。

注: すでに JBoss がインストールされている場合、オープン ポートの問題を解決するために CA ControlMinder エンタープライズ管理 をインストールする前に、JBoss を一度だけ実行することをお勧めします。CA ControlMinder エンタープライズ管理 インストール プログラムはデフォルト JBoss ポートを使用しません。たとえば、HTTP 接続用に、デフォルトのポート番号 8080 ではなく、ポート番号 18080 が使用されます。

- a. JBoss アーカイブを抽出し、それをインストールします。

```
cp jboss-4.2.3.GA.zip /opt/  
jboss-4.2.3.GA.zip を解凍します。
```

- b. `server.xml` で、ポート番号を 8080 から 18080 に変更し、リダイレクト ポートを 8443 から 18443 に変更します。

```
vi  
/opt/jboss-4.2.3.GA/server/default/deploy/jboss-web.deploye  
r/server.xml  
<Connector URIEncoding="UTF-8" acceptCount="150"  
address="${jboss.bind.address}" connectionTimeout="20000"  
disableUploadTimeout="true" emptySessionPath="true"  
enableLookups="false" maxHttpHeaderSize="8192"  
maxThreads="250" port="18080" protocol="HTTP/1.1"  
redirectPort="18443"/>  
<Connector SSLEnabled="true" URIEncoding="UTF-8"  
clientAuth="false" keyAlias="entm"  
keystoreFile="/opt/jboss-4.2.3.GA/server/default/deploy/Ide  
ntityMinder.ear/custom/ppm/truststore/ssl.keystore"  
keystorePass="secret" maxThreads="150" port="18443"  
protocol="HTTP/1.1" scheme="https" secure="true"  
sslProtocol="TLS"/>  
<Connector address="${jboss.bind.address}"  
emptySessionPath="true" enableLookups="false" port="8009"  
protocol="AJP/1.3" redirectPort="18443"/>
```

- c. jboss-minimal.xml で、ネーミング ポートを 1099 から 11099 に変更します。

```
vi /opt/jboss-4.2.3.GA/server/default/conf/jboss-minimal.xml
<mbean code="org.jboss.naming.NamingService"
      name="jboss:service=Naming"
      xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
  <attribute name="CallByValue">false</attribute>
  <attribute name="Port">11099</attribute>
```

- d. jboss-service.xml で、ネーミング ポートを 1099 から 11099 に変更します。

```
vi /opt/jboss-4.2.3.GA/server/default/conf/jboss-service.xml
<mbean code="org.jboss.naming.NamingService"
      name="jboss:service=Naming"
      xmbean-dd="resource:xmdesc/NamingService-xmbean.xml">
  <attribute name="CallByValue">false</attribute>
  <attribute name="Port">11099</attribute>
```

- e. デーモンとして開始するように JBoss を設定します。詳細については、<https://community.jboss.org/wiki/startjbossbootwithlinux> を参照してください。

4. インストール中のエラーを回避するために、オープン ファイルの最大数を変更します。

```
ulimit -n 10000
```

5. Linux ディストリビューションから rpmbuild パッケージがインストールされていることを確認します。

エンタープライズ管理サーバでは、拡張ポリシー管理オプションをサーバにインストールするには rpmbuild パッケージが必要です。

これで、CA ControlMinder エンタープライズ管理 をエンタープライズ管理サーバにインストールする準備ができました。

エンタープライズ管理のための中央データベースの準備

CA ControlMinder エンタープライズ管理 には、リレーショナル データベース システム (RDBMS) が必要です。CA ControlMinder エンタープライズ管理 をインストールする前に、RDBMS をセットアップします。

CA ControlMinder エンタープライズ管理 で使用するデータベースのセットアップには以下の 2 つのオプションがあります。

- CA ControlMinder が提供するデプロイメント スクリプトを使用して、中央データベースに事前にデータを読み込みます。
このオプションを使用した場合、データベースの準備と CA ControlMinder エンタープライズ管理 のインストールは別々に行われます。データベース管理者は、CA ControlMinder によるデータベース への変更を確認および制御できます。
- CA ControlMinder エンタープライズ管理 によって、インストール時に、中央データベースが自動的に準備されます。
このオプションを使用した場合、CA ControlMinder エンタープライズ管理 のインストール処理の一部としてデータベースにデータが読み込まれます。

次の手順に従ってください:

1. まだ存在しない場合は、サポート対象の RDBMS を中央データベースとしてインストールします。

注: サポート対象の RDBMS ソフトウェアの詳細については、「リリースノート」を参照してください。

2. CA ControlMinder エンタープライズ管理 への RDBMS の設定:

データベースにローカルで、またリモート クライアントからアクセス可能であることを確認します。

- Oracle では、以下の手順に従います。

- a. 中央データベースに対するユーザを作成します。このユーザには、以下の権限および設定が必要です。

- システム権限、ADMINISTER DATABASE TRIGGER、ALTER SESSION、CREATE CLUSTER、CREATE DATABASE LINK、CREATE SEQUENCE、CREATE SESSION、CREATE SYNONYM、CREATE TABLE、CREATE VIEW、CREATE ANY INDEXTYPE、CREATE OPERATOR、CREATE PROCEDURE、CREATE TRIGGER、CREATE TYPE、EXECUTE ON SYS.DBMS_CRYPTO、SELECT ANY DICTIONARY、UNLIMITED TABLESPACE

- b. 以下のコマンドを入力して、データベースへの接続数を増やします。

```
ALTER SYSTEM SET transactions=275 SCOPE=SPFILE
```

```
ALTER SYSTEM SET sessions=250 SCOPE=SPFILE
```

```
ALTER SYSTEM SET processes=200 SCOPE=SPFILE
```

- SQL Server の場合:

- a. 大文字小文字を区別しない、新しいデータベースを作成します。

このデータベースには、並べ替え順序として SQL_Latin1_General_CP1_CI_AS が必要です。

- b. 新規ログインを作成し、新規データベースをログインのデフォルト データベースにします。
- c. ログインをデータベース所有者として設定します。

3. (オプション) CA ControlMinder が提供するデプロイメント スクリプトを使用して、中央データベースに事前にデータを読み込みます。
 - a. お使いのオペレーティング システム用の適切な CA ControlMinder サーバ コンポーネント DVD を光ディスク ドライブに挿入します。
 - b. RDBMS のデプロイメント スクリプトを一時ローカル フォルダにコピーします。

デフォルトでは、データベース デプロイメント スクリプトは光学メディアの以下の場所にあります。

- Oracle : /Schema/oracle_database_deployment_script.sql
- SQL Server : /Schema/mssql_database_deployment_script.sql

- c. [デプロイメント スクリプトを展開します](#) (P. 67)。
- d. CA ControlMinder エンタープライズ管理 のインストールに使用するデータベース ユーザを設定します。
 - Oracle の場合、作成したユーザに対して ALTER SESSION、CREATE SESSION、EXECUTE ON SYS.DBMS_CRYPTO および SELECT ANY DICTIONARY システム権限を維持します。
 - SQL Server の場合、ユーザを作成し、作成済みのデータベースをデフォルトとして選択し、ユーザをデータベースにマップして、次の権限を設定します。CONNECT、SELECT、INSERT、DELETE、UPDATE、EXECUTE。
- e. 事前定義済みユーザ アカウント パスワードをリセットします。以下の手順に従います。
 - a. 管理権限を持つユーザとして CA ControlMinder エンタープライズ管理 にログインします。
 - b. [ユーザおよびグループ] - [ユーザ] - [ユーザ パスワードのリセット] を選択します。
[ユーザ パスワードのリセット] 画面が表示されます。
 - c. 検索クエリを入力して、利用可能なユーザをすべて表示し、[検索] を選択します。

CA ControlMinder エンタープライズ管理 は、以下のユーザ アカウントを表示します。[デフォルト ユーザ]、superadmin、neteautoadmin、selfreguser

- d. 各アカウントに対して、以下を実行します。

ユーザアカウントを選択し、[選択] をクリックします。

[パスワードのリセット] ウィンドウが開きます。

[パスワードの確認] フィールドにアカウント パスワードを入力します。

(オプション) [パスワードの変更が必要] オプションを選択し、[サブミット] をクリックします。

CA ControlMinder エンタープライズ管理 はアカウント パスワードをリセットします。

中央データベース スクリプト デプロイメントの例

スクリプトのデプロイによって、中央データベースにデータが取り込まれ、中央データベースで CA ControlMinder エンタープライズ管理 インストールの準備ができます。スクリプトのデプロイは、ネイティブ データベース ツールを使用して行います。

例: Oracle Database 10g 上での CA ControlMinderOracle デプロイメントスクリプトのデプロイ

この例は、CA ControlMinder Oracle デプロイメント スクリプトを Oracle Database 10g 上にデプロイする方法を示しています。

1. [スタート] - [すべてのプログラム] - [Oracle - ORACLE_HOME] - [Application Development] - [SQL Plus] をクリックします。
[Oracle SQL*PLUS] ウィンドウが開きます。
2. 以前に作成したユーザを使用して、Oracle データベースに接続します。
3. @ 記号の前に、スクリプト ファイルの完全パス名を入力します。以下に例を示します。

```
@C:\temp_directory\oracle_database_deployment_script.sql
```

Oracle はスクリプトをデータベースにデプロイします。

例: SQL Server 2005 上への CA ControlMinder Microsoft SQL Server デプロイメントスクリプトのデプロイ

この例は、CA ControlMinder Microsoft SQL Server デプロイメント スクリプトを SQL Server 2005 上にデプロイする方法を示しています。

1. [スタート] - [すべてのプログラム] - [Microsoft SQL Server 2005] - [SQL Server Management Studio] をクリックします。
[ログイン] ウィンドウが開きます。
2. システム管理者としてログインします。
Microsoft SQL Server Management Studio が開きます。
3. [ファイル] - [開く] - [ファイル] をクリックします。
[ファイルを開く] ダイアログ ボックスが表示されます。
4. CA ControlMinder Microsoft SQL Server デプロイメント スクリプトを参照して選択し、[開く] をクリックします。
5. [利用可能なデータベース] ドロップダウン リストから、以前作成したデータベースをスクリプトのデプロイ先として選択します。
6. [実行] をクリックして、スクリプトをデプロイします。
Microsoft SQL Server はスクリプトをデータベースにデプロイします。

必須ソフトウェア インストール ユーティリティの実行

Windows で有効

CA ControlMinder エンタープライズ管理 では、Java Development Kit (JDK) および JBoss アプリケーション サーバが実行されている必要があります。この事前インストールが必要なサードパーティ ソフトウェアの正しいバージョンは、CA ControlMinder Third Party Components DVD で提供されます。また、この DVD には、以下のような、事前インストール ソフトウェアをインストールするユーティリティもあります。

- JDK および JBoss を設定して、CA ControlMinder エンタープライズ管理 に適切な設定でインストールするようにします。
- JBoss をサービスとしてインストールします。
- あらかじめ設定された事前インストール ソフトウェアの設定で、CA ControlMinder エンタープライズ管理 のインストールを開始します。

これらのソフトウェアがすでにインストールされていれば、この手順をスキップできます。インストールされていない場合は、提供されているユーティリティを使用して、この手順に従ってインストールすることをお勧めします。

すでに JBoss がインストールされている場合、オープン ポートの問題を解決するために CA ControlMinder エンタープライズ管理 をインストールする前に、JBoss を一度だけ実行することをお勧めします。

以下の手順に従います。

1. 光ディスク ドライブに CA ControlMinder Third-Party Components DVD for Windows を挿入します。
2. 光ディスクドライブ上の PrereqInstaller ディレクトリに移動し、**install_PRK.exe** を実行します。
InstallAnywhere ウィザードが開きます。
3. 必要に応じてウィザードを完了します。

注: 追加の JBoss ポート番号を設定するには、[JBoss ポート設定] ページの [詳細設定] を選択します。ユーザがビジーな JBoss ポートを指定した場合、インストーラによって異なるポート番号の指定を促すメッセージが表示されます。

4. サマリ レポートで詳細を確認し、[インストール]をクリックします。
事前インストール ソフトウェアがインストールされます。この処理には時間がかかる場合があります。
 5. 以下のいずれかの操作を実行します。
 - 必須のソフトウェアをインストールした後、CA ControlMinder エンタープライズ管理 のインストールを開始する場合は、プロンプトが表示されたら光ディスクドライブにご使用のオペレーティングシステム用の **CA ControlMinder Server Components DVD** を挿入し、[完了] を選択します。Product Explorer ウィンドウが表示されたら、閉じます。
 - 高可用性または障害復旧のために追加のエンタープライズ管理サーバをインストールする場合は、CA ControlMinder エンタープライズ管理 をインストールするカスタム FIPS キーを指定します。メッセージが表示されたら [完了] をクリックし、続いて [完了] をクリックして表示されたダイアログ ボックスを閉じます。
 - 必須のソフトウェアをインストールした後に CA ControlMinder エンタープライズ管理 のインストールを開始しない場合は、プロンプトが表示されたら [完了] をクリックし、[終了] をクリックして表示されたダイアログ ボックスを閉じます。
- 必須のソフトウェアのインストールプロセスが完了しました。

エンタープライズ管理サーバコンポーネントのインストール方法

エンタープライズ管理サーバコンポーネントによって、CA ControlMinder の企業への展開を一元的に管理できます。エンタープライズ管理サーバコンポーネントのインストール後、レポート サービスおよび、CA ControlMinder と UNAB のエンドポイントをインストールします。

実装を開始する前に、使用しているコンピュータが必要なハードウェアおよびソフトウェア要件を満たしていることを確認します。

注: 必須ハードウェアとソフトウェアの仕様書詳細については、[CA Support](#) の CA ControlMinder 製品ページから利用可能な CA ControlMinder Compatibility Matrix を参照してください。

エンタープライズ管理サーバ コンポーネントをインストールするには、以下の手順を実行します。

1. エンタープライズ管理サーバを準備します。

エンタープライズ管理サーバをインストールする前に、前提条件のインストールおよび設定によりコンピュータを準備します。

注: エンタープライズ管理サーバをインストールする前に、ユーザのシステム用の最新のソフトウェア更新とパッチをインストールすることをお勧めします。

2. マスタ CA ControlMinder エンタープライズ管理 をインストールします。

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA ControlMinder がインストールされます。

3. (オプション) 負荷分散エンタープライズ管理サーバをインストールします。

4. (オプション) Sun ONE ディレクトリまたは CA Directory ユーザストアを使用するように、エンタープライズ管理サーバを設定します。

Active Directory またはリレーショナルデータベース ユーザストアの代わりに Sun ONE または CA Directory ユーザストアを使用するように、CA ControlMinder エンタープライズ管理 を定義できます。

5. (オプション) SSL 通信用にエンタープライズ管理サーバを以下のように設定します。

a. (オプション) SSL 通信用に JBoss を設定します。

b. (Active Directory) SSL 通信用のエンタープライズ管理サーバを設定します。

6. (オプション) 詳細設定を指定します。

CA IdentityMinder 管理コンソールを使用して、詳細な環境設定タスクを実行できます。こうしたタスクには、カスタム レポートを生成するための中央データベースのプロパティの変更、特定のイベント発生時に電子メール通知を送信するための CA ControlMinder エンタープライズ管理 の設定などがあります。

7. (オプション) エンタープライズ レポート機能の実装

エンタープライズ管理サーバは CA Business Intelligence 共通レポートサーバ (CA ControlMinder レポート ポータル) を使用して、レポート機能を提供します。

8. (オプション) CA User Activity Reporting Module と統合します。

エンタープライズ管理サーバがインストールされました。これで、エンドポイントをインストールし設定できます。

詳細情報:

[レポート サービス サーバコンポーネントの設定方法 \(P. 128\)](#)

Windows での CA ControlMinder エンタープライズ管理 のインストール

CA ControlMinder エンタープライズ管理 をインストールすると、エンタープライズ管理のサーバコンポーネントがすべてインストールされます。CA ControlMinder エンタープライズ管理 をインストールする前に、エンタープライズ管理サーバを準備します。

前提条件キットを使用して、CA ControlMinder エンタープライズ管理 のインストールを開始することをお勧めします。Install_PRK.exe は必要なサードパーティ ソフトウェアをインストールし、次に、CA ControlMinder エンタープライズ管理 のインストールを開始します。

注: ネットワーク インストールによって CA ControlMinder エンタープライズ管理 をインストールすることはできません。CA ControlMinder Server Components DVD の Disk 1 ディレクトリの内容をすべてインストール ディレクトリにコピーするか、代わりにドライブを DVD にマッピングします。

重要: CA ControlMinder エンタープライズ管理 をインストールしてハイアベイラビリティを実現する場合、プライマリおよびセカンダリのエンタープライズ管理サーバ上に同じ FIPS キーを指定します。CA ControlMinder エンタープライズ管理 をインストールして FIPS サポートによるハイアベイラビリティを実現する場合、カスタム FIPS キーを指定します。

次の手順に従ってください:

1. JBoss アプリケーション サーバが実行中の場合は、これを終了させます。
2. CA ControlMinder がすでにインストールされているコンピュータに CA ControlMinder エンタープライズ管理 をインストールする場合は、CA ControlMinder サービスを停止します。

3. 光ディスク ドライブに CA ControlMinder Server Components DVD for Windows を挿入します。
4. Product Explorer で [Components] フォルダを展開し、CA ControlMinder エンタープライズ管理 を選択し、[インストール] をクリックします。
5. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

インストール モードの選択

エンタープライズ管理サーバのインストール モードを定義します。

- プライマリ エンタープライズ管理サーバ - プライマリ エンタープライズ管理サーバをインストールするために選択します。
- 負荷分散エンタープライズ管理サーバ - 負荷分散エンタープライズ管理サーバをインストールするために選択します。

重要: インストール モードは新しいインストールのみに適用されます。

インストール フォルダの選択

インストール フォルダの完全パスを定義します。

デフォルト : %ProgramFiles%CA%AccessControlServer%

注: 64 ビットのオペレーティング システムでのデフォルトのインストール フォルダは、以下のとおりです。

%Program Files(x86)%CA%AccessControlServer%

Java Development Kit (JDK)

既存の JDK の場所を定義します。

注: CA ControlMinder Third Party Component DVD を使用して必須ソフトウェアをインストールした直後に、CA ControlMinder エンタープライズ管理 のインストールを開始した場合、このウィザードは表示されません。インストールユーティリティは、必須のソフトウェア インストールプロセスの際に指定した値を基に、このページのインストール設定を行います。

JBoss アプリケーション サーバ情報

アプリケーションをインストールする JBoss インスタンスを定義します。

これを行うには、以下を定義します。

- JBoss フォルダ (JBoss をインストールしているトップディレクトリ)。
たとえば、Windows の場合は `C:\jboss-4.2.3.GA`、Solaris の場合は `/opt/jboss-4.2.3.GA` です。
- URL (インストール先のコンピュータの IP アドレスまたはホスト名)。
- JBoss が使用するポート。
- JBoss が安全な通信のために使用するポート (HTTPS)。
- ネーミング ポート番号。

注: CA ControlMinder Third Party Component DVD を使用して必須ソフトウェアをインストールした直後に、CA ControlMinder エンタープライズ管理のインストールを開始した場合、このウィザードは表示されません。インストールユーティリティは、必須のソフトウェアインストールプロセスの際に指定した値を基に、このページのインストール設定を行います。

通信パスワード

(プライマリ エンタープライズ管理サーバのみ) CA ControlMinder エンタープライズ管理サーバのコンポーネント間通信に使用されるパスワードを定義します。

注: CA ControlMinder エンタープライズ管理 は通信パスワードを使用して Message Queue キーストアおよび管理者アカウントを管理し、CA ControlMinder エンタープライズ管理 とエンドポイントの間の通信を処理し、Java 接続サーバを管理します。

プライマリ エンタープライズ管理サーバ情報

(負荷分散エンタープライズ管理サーバのみ) プライマリ エンタープライズ管理サーバのホスト名または IP アドレス、および FIPS キーへのフルパス名を定義します。

注: デフォルトでは、FIPS キーは以下のパスにあります。

`JBoss_HOME` は JBoss をインストールしたディレクトリです。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys`

データベース情報

RDBMS への接続の詳細を定義します。

- **データベース タイプ** - サポートされている RDBMS を指定します。
- **ホスト名** - RDBMS をインストールしているホストの名前を定義します。
- **ポート番号** - 指定した RDBMS によって使用されるポートを定義します。インストールプログラムでは、RDBMS のデフォルトポートが指定されます。
- **サービス名** - (Oracle) システムの RDBMS を識別する名前を定義します。たとえば、Oracle Database 10g の場合はデフォルトで *orcl* になります。
- **データベース名** - (MS SQL) 作成したデータベースの名前を定義します。
- **ユーザ名** - データベースを準備した際に作成したユーザの名前を定義します。

注: このユーザには、データベースを準備した際に適切なデータベース許可が与えられています。

- **パスワード** - データベースを準備した際に作成した RDBMS パスワードを定義します。

インストールプログラムは、続行する前にデータベースへの接続を確認します。

Active Directory の設定

Active Directory ユーザ ストアの設定を定義します。

- **ホスト** -- Active Directory のドメイン コントローラ ホスト名を定義します。
- **ポート** -- Active Directory に対する LDAP クエリにデフォルトで使用されるポートを定義します (たとえば 389) 。

- **検索ルート** - 検索ルートを、「ou=DomainName, DC=com」のように定義します。

注: [検索ルート] には、ディレクトリツリーにおいて、[ユーザ DN] および [システムユーザ] として指定したユーザの識別名 (DN) よりも高いノードを少なくとも 1 つ設定します。そうしないと、エンタープライズ管理がタブをまったく表示せずに起動する場合があります。

- **ユーザ DN** -- CA ControlMinder エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウント名を定義します。例: CN=Administrator, cn=Users, DC=DomainName, DC=Com

注: このユーザは、Active Directory に対する LDAP クエリを発行します。このパラメータ用の読み取り専用権限を持ったユーザを定義してもかまいません。ただし、読み取り専用権限を持ったユーザを定義する場合、CA ControlMinder エンタープライズ管理 内のユーザに管理ロールまたは特権アクセス ロールを割り当てることはできません。代わりに、Active Directory グループを指すように各ロールのメンバ ポリシーを変更します。

- **パスワード** -- CA ControlMinder エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウントのパスワードを定義します。

インストールプログラムは、続行前に Active Directory への接続を確認します。

注: ディレクトリ照会ユーティリティ **DSQUERY** を使用して、ユーザの識別名 (ユーザ DN) を検出することができます。このクエリは、Active Directory サーバ上で実行する必要があります。以下に例を示します。

```
dsquery user -name administrator  
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

システム ユーザ

(Active Directory のみ) CA ControlMinder エンタープライズ管理 で System Manager 管理ロールが割り当てられている Active Directory ユーザの DN を定義します。

例 : CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

注: デフォルトでは、System Manager 管理ロールを持ったユーザは、CA ControlMinder エンタープライズ管理 内のタスクをすべて実行、作成、および管理できます。システム マネージャ管理ロールの詳細については、「エンタープライズ管理ガイド」をご覧ください。

管理者パスワード

(組み込みユーザ ストアのみ) CA ControlMinder エンタープライズ管理 管理者である superadmin のパスワードを定義します。インストール完了時に CA ControlMinder エンタープライズ管理 にログインできるように、パスワードをメモしておきます。

注: この手順で、組み込みユーザ ストアの superadmin ユーザを作成します。superadmin ユーザには、CA ControlMinder エンタープライズ管理 のシステム マネージャ管理ロールが割り当てられます。CA ControlMinder エンタープライズ管理 への初回ログイン時には、superadmin としてログインします。システム マネージャ管理ロールの詳細については、「エンタープライズ管理ガイド」をご覧ください。

FIPS キーの場所

元の FIPSkey.dat のコピーへのパスを定義します。FIPS キー ファイルによって、暗号化されたデータベースが移行の後に読み取り可能であることが確実になります。

ウィザードの完了後に、エンタープライズ管理サーバがインストールされます。インストールを完了するために、コンピュータを再起動します。

6. [はい] を選択し、システムを再起動し、[完了] をクリックします。コンピュータが再起動します。これで、ご自分の環境に合わせて CA ControlMinder エンタープライズ管理 を設定できるようになりました。

詳細情報:

[メッセージキュー管理者パスワードの変更 \(P. 619\)](#)

Linux での CA ControlMinder エンタープライズ管理 のインストール

CA ControlMinder エンタープライズ管理 をインストールすると、エンタープライズ管理のサーバコンポーネントがすべてインストールされます。CA ControlMinder エンタープライズ管理 をインストールする前に、エンタープライズ管理サーバを準備します。

Linux コンピュータに CA ControlMinder エンタープライズ管理 をインストールするには、コンソールインストールを使用します。

以下の手順に従います。

1. JBoss アプリケーション サーバが実行されている場合はシャットダウンします。
2. CA ControlMinder がすでにインストールされているコンピュータに CA ControlMinder エンタープライズ管理 をインストールする場合は、CA ControlMinder サービスを停止します。以下の手順に従います。
 - a. 以下のコマンドを入力して、CA ControlMinder サービスを停止します。

```
/opt/CA/AccessControl/bin/secons -sk
```

CA ControlMinder が停止されます。

- b. 以下のコマンドを入力して、CA ControlMinder をアンロードします。

```
/opt/CA/AccessControl/bin/SEOS_load -u
```

CA ControlMinder が停止されます。コンピュータはインストールの準備ができました。

3. 以下の手順を実行します。
 - a. お使いのオペレーティング システム用の適切な CA ControlMinder サーバコンポーネント DVD を光ディスク ドライブに挿入します。
 - b. 光ディスク ドライブをマウントします。noexec オプションは指定しません。noexec オプションを指定すると、インストールは失敗します。

注: Linux の一部のリリースでは、noexec オプションを指定すると、オペレーティング システムが光ディスク ドライブを自動マウントします。

- c. 端末ウィンドウを開いて、作業ディレクトリとして書き込み可能な一時ディレクトリを設定します。

注: インストーラは作業ディレクトリにインストール ファイルをアンパックします。光学メディア上の作業ディレクトリを指定すると、インストーラがファイルをアンパックすることができないので、インストールは失敗します。

- d. インストーラへのフルパスをコマンドに指定して、インストーラを実行します。たとえば、光ディスク ドライブを **/media** ディレクトリ内にマウントする場合は、以下のコマンドを入力します。

```
/media/EnterpriseMgmt/Disk1/InstData/NoVM/install_EntM.bin -i console
```

重要: CA ControlMinder エンタープライズ管理 をインストールしてハイ アベイラビリティを実現する場合、プライマリおよびセカンダリのエンタープライズ管理サーバ上に同じ **FIPS** キーを指定します。CA ControlMinder エンタープライズ管理 をインストールして **FIPS** サポートによるハイ アベイラビリティを実現する場合、カスタム **FIPS** キーを指定します。

InstallAnywhere コンソールが表示されます。

4. 必要に応じてプロンプトを完了します。以下のインストール入力には、説明が必要です。

インストール モードの選択

エンタープライズ管理サーバのインストール モードを定義します。

- プライマリ エンタープライズ管理サーバ - プライマリ エンタープライズ管理サーバをインストールするために選択します。
- 負荷分散エンタープライズ管理サーバ - 負荷分散エンタープライズ管理サーバをインストールするために選択します。

重要: インストール モードは新しいインストールのみに適用されます。

Java Development Kit (JDK)

既存の **JDK** の場所を定義します。

JBoss アプリケーション サーバ情報

アプリケーションをインストールする JBoss インスタンスを定義します。

以下を実行する必要があります。

- JBoss をインストールしているトップディレクトリの JBoss フォルダの定義。

例: /opt/jboss-4.2.3.GA

- JBoss が使用するポートの定義。
- JBoss が安全な通信のために使用するポートの定義 (HTTPS)。
- ネーミング ポート番号の定義。

注: CA ControlMinder エンタープライズ管理 インストール プログラムはデフォルト JBoss ポートを使用しません。その代り、デフォルト JBoss ポート番号に 10000 を加えます。たとえば、インストール プログラムは、HTTP 接続用のポート番号 8080 ではなくポート番号 18080 を使用します。JBoss が使用するポートを指定していることを確認します。

通信パスワード

(プライマリ エンタープライズ管理サーバのみ) CA ControlMinder エンタープライズ管理サーバのコンポーネント間通信に使用されるパスワードを定義します。

注: CA ControlMinder エンタープライズ管理 は通信パスワードを使用して Message Queue キーストアおよび管理者アカウントを管理し、CA ControlMinder エンタープライズ管理 とエンドポイントの間の通信を処理し、Java 接続サーバを管理します。

プライマリ エンタープライズ管理サーバ情報

(負荷分散エンタープライズ管理サーバのみ) プライマリ エンタープライズ管理サーバのホスト名または IP アドレス、および FIPS キーへのフルパス名を定義します。

注: デフォルトでは、FIPS キーは以下のパスにあります。

`JBoss_HOME` は JBoss をインストールしたディレクトリです。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netscape/certmgr/certs`

データベース情報

RDBMS への接続の詳細を定義します。

- **データベース タイプ** - サポートされている RDBMS を指定します。
- **ホスト名** - RDBMS をインストールしているホストの名前を定義します。
- **ポート番号** - 指定した RDBMS によって使用されるポートを定義します。インストールプログラムでは、RDBMS のデフォルトポートが指定されます。
- **サービス名** - (Oracle) システムの RDBMS を識別する名前を定義します。たとえば、Oracle Database 10g の場合はデフォルトで *orcl* になります。
- **データベース名** - (MS SQL) 作成したデータベースの名前を定義します。
- **ユーザ名** - データベースを準備した際に作成したユーザの名前を定義します。

注: このユーザには、データベースを準備した際に適切なデータベース許可が与えられています。

- **パスワード** - データベースを準備した際に作成した RDBMS パスワードを定義します。

インストールプログラムは、続行する前にデータベースへの接続を確認します。

ユーザストアタイプ

CA ControlMinder エンタープライズ管理 が使用するユーザ ストアタイプを定義します。以下のいずれかを選択します。

- **組み込みユーザ ストア** -- CA ControlMinder エンタープライズ管理 は RDBMS にユーザ情報を格納します。
- **Active Directory** -- 次の 画面に接続情報の詳細を指定します。
- **他のユーザ ストア** -- CA ControlMinder エンタープライズ管理 のインストール完了後に、ユーザ ストアの構成情報を指定します。

注: UNAB にログイン許可ポリシーをデプロイするには、ユーザストアとして [Active Directory] または [他のユーザストア] を選択する必要があります。ユーザストアとして [Active Directory] または [他のユーザストア] を選択した場合、CA ControlMinder エンタープライズ管理 でユーザおよびグループを作成または削除できません。UNAB および Active Directory の制限事項の詳細については、「エンタープライズ管理ガイド」をご覧ください。

Active Directory の設定

Active Directory ユーザストアの設定を定義します。

- **ホスト** -- Active Directory のドメインコントローラホスト名を定義します。
- **ポート** -- Active Directory に対する LDAP クエリにデフォルトで使用されるポートを定義します (たとえば 389)。
- **検索ルート** - 検索ルートを、「ou=DomainName, DC=com」のように定義します。

注: [検索ルート] には、ディレクトリツリーにおいて、[ユーザ DN] および [システムユーザ] として指定したユーザの識別名 (DN) よりも高いノードを少なくとも 1 つ設定します。そうしないと、エンタープライズ管理がタブをまったく表示せずに起動する場合があります。

- **ユーザ DN** -- CA ControlMinder エンタープライズ管理 を管理するために使用される Active Directory ユーザアカウント名を定義します。例: CN=Administrator、cn=Users、DC=DomainName、DC=Com

注: このユーザは、Active Directory に対する LDAP クエリを発行します。このパラメータ用の読み取り専用権限を持ったユーザを定義してもかまいません。ただし、読み取り専用権限を持ったユーザを定義する場合、CA ControlMinder エンタープライズ管理 内のユーザに管理ロールまたは特権アクセスロールを割り当てることはできません。代わりに、Active Directory グループを指すように各ロールのメンバポリシーを変更します。

- パスワード -- CA ControlMinder エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウントのパスワードを定義します。

インストール プログラムは、続行前に Active Directory への接続を確認します。

注: ディレクトリ照会ユーティリティ **DSQUERY** を使用して、ユーザの識別名 (ユーザ DN) を検出することができます。このクエリは、Active Directory サーバ上で実行する必要があります。以下に例を示します。

```
dsquery user -name administrator  
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

システム ユーザ

(Active Directory のみ) CA ControlMinder エンタープライズ管理 で System Manager 管理ロールが割り当てられている Active Directory ユーザの DN を定義します。

例 : CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

注: デフォルトでは、System Manager 管理ロールを持ったユーザは、CA ControlMinder エンタープライズ管理 内のタスクをすべて実行、作成、および管理できます。システム マネージャ管理ロールの詳細については、「エンタープライズ管理ガイド」をご覧ください。

管理者パスワード

(組み込みユーザ ストアのみ) CA ControlMinder エンタープライズ管理 管理者である **superadmin** のパスワードを定義します。インストール完了時に CA ControlMinder エンタープライズ管理 にログインできるように、パスワードをメモしておきます。

注: この手順で、組み込みユーザ ストアの **superadmin** ユーザを作成します。**superadmin** ユーザには、CA ControlMinder エンタープライズ管理 のシステム マネージャ管理ロールが割り当てられます。CA ControlMinder エンタープライズ管理 への初回ログイン時には、**superadmin** としてログインします。システム マネージャ管理ロールの詳細については、「エンタープライズ管理ガイド」をご覧ください。

5. インストール前の概要情報を確認します。情報が正しければ、Enter キーを押します。
CA ControlMinder エンタープライズ管理 がインストールされます。
6. Enter キーを押します。
インストーラが閉じます。
7. 必要に応じて、コンピュータを再起動します。
所属する組織のための CA ControlMinder エンタープライズ管理 の設定を開始します。

エンタープライズ管理サーバ上での HTTP アクセスのブロック

症状:

インストール後、HTTP および HTTPS のポートはデフォルトで開いています。HTTP ポートを無効にする必要があります。

解決方法:

HTTP ポートを無効にするには、JBoss 設定内の HTTP コネクタをコメントアウトします。

次の手順に従ってください:

1. `JBoss_HOME/server/default/deploy/jboss-web.deployer` ファイルを参照し、`server.xml` ファイルを編集します。
2. HTTP コネクタのデフォルト ポートを定義する以下の文字列を検索します。
`port="18080"`
注: インストール ウィザードの別のポートを設定している場合、ポート番号は異なる可能性があります。
このポート属性は `<Connector>` 要素の一部です。
3. コメント タグ (`<!--` および `-->`) で要素を囲んで、この `<Connector>` 要素をコメントアウトします。
HTTP コネクタが無効になります。
4. JBoss サービスを再起動します。

例

```
<!-- <Connector port="18080" address="{jboss.bind.address}"  
      connectionTimeout="20000" /> -->
```

負荷分散エンタープライズ管理サーバと配布サーバのインストール後に、サブスクライバを作成します

複数のエンタープライズ管理サーバをインストールする場合、CA ControlMinder エンタープライズ管理を開始する前にサブスクライバを作成する必要があります。プライマリ エンタープライズ管理サーバで、以下の手順を完了します。

重要: 負荷分散エンタープライズ管理サーバおよび配布サーバをインストールする場合は、この手順を完了します。

以下の手順に従います。

1. コマンドプロンプト ウィンドウを開きます。
2. サブスクライバを作成するには、以下のコマンドを入力します。

```
sepmc -n DMS__DH__@<LB_entm>
```

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

第 5 章: SUN ONE および CA Directory 用のエンタープライズ管理サーバの設定

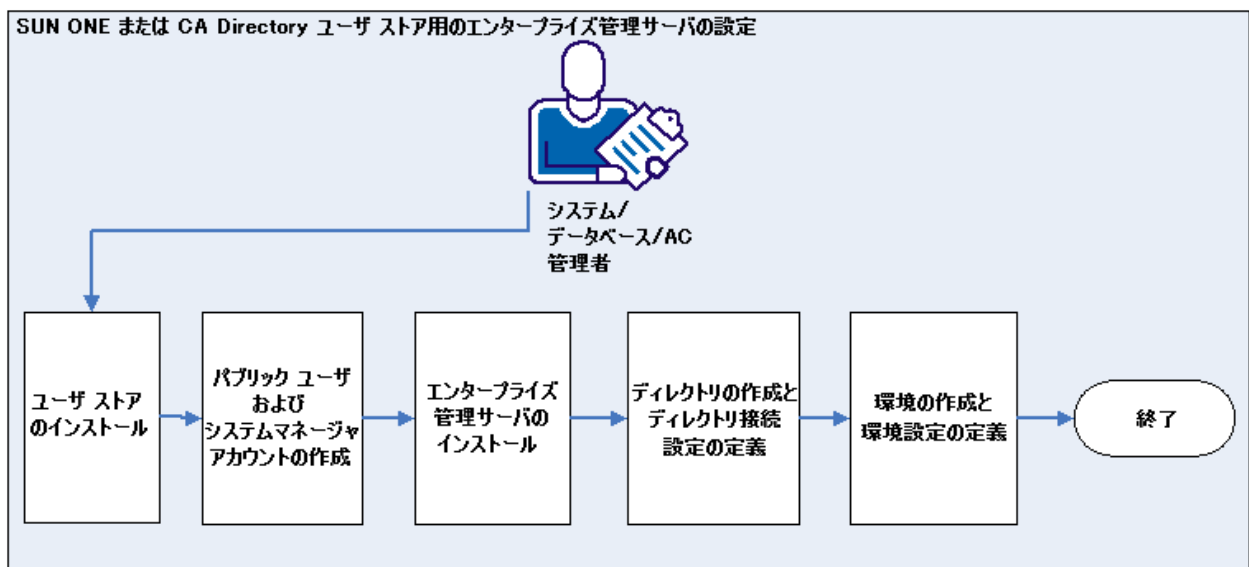
このシナリオでは、SUN ONE または CA Directory 用のエンタープライズ管理サーバをどのように設定するかを説明します。ユーザストアとして SUN ONE または CA Directory を使用している場合、CA ControlMinder エンタープライズ管理のインストール後に、ユーザストアを設定します。CA IdentityMinder 管理コンソールを使用して、ディレクトリと環境を設定します。

重要: ユーザストアとして SUN ONE ディレクトリまたは CA Directory を使用するには、CA ControlMinder エンタープライズ管理 インストール ウィザードの [ユーザストアタイプの選択] 画面で [他のユーザストア] オプションを選択します。

このシナリオは次のユーザを対象にしています。

- システム管理者
- データベース管理者
- CA ControlMinder 管理者

以下の図は、SUN ONE または CA Directory ユーザストア用のエンタープライズ管理サーバの設定を完了する手順を示します。



次の手順に従ってください:

1. ユーザストアディレクトリをインストールします。

注: SUN ONE の場合、SUN ONE Directory Suite および Administration Services をインストールしていることを確認してください。CA Directory の詳細については、「CA Directory インストールガイド」を参照してください。

2. パブリック ユーザおよびシステム管理者アカウントを作成します。
環境作成時に、ユーザクレデンシャルを指定します。

3. エンタープライズ管理サーバをインストールします。

注: インストール中にユーザストアを指定しないでください。エンタープライズ管理サーバインストールの詳細については、「実装ガイド」を参照してください。

4. ディレクトリを作成し、接続設定を定義します。

- [SUN ONE](#) (P. 89)
- [CA Directory](#) (P. 93)

5. 環境を作成し、環境設定を定義します。

- [SUN ONE](#) (P. 90)
- [CA Directory](#) (P. 96)

注: ディレクトリと環境を設定および定義するために CA IdentityMinder 管理コンソールを使用します。

6. `secons -s` コマンドを使用して、CA ControlMinder サービスを停止します。
7. `seosd -start` コマンドを使用して、CA ControlMinder サービスを開始します。

SUN ONE ユーザ ストア用のディレクトリの作成

ディレクトリによって、エンタープライズ管理サーバが管理するユーザディレクトリに関する情報が提供されます。エンタープライズ管理サーバのインストール後、SUN ONE ディレクトリを設定します。

次の手順に従ってください:

1. 以下のディレクトリに移動します。ここで、*JBoss_HOME* は JBoss をインストールしたディレクトリです。

```
JBoss_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/  
/
```

2. *SAM_iPlanet_directory.xml* ファイルを見つけて、一時ディレクトリにコピーします。

3. 以下のようにして、CA IdentityMinder 管理コンソールを開きます。

```
http://enterprise_host:port/idmmanage
```

4. [ディレクトリ] - [新規] を選択します。

新規ディレクトリのウィンドウが開きます。

5. [参照] を選択し、*SAM_iPlanet_directory.xml* ファイルを見つけます。
[次へ] をクリックします。

6. 以下の情報を入力します。

- **名前** -- ディレクトリの論理名を定義します
- **説明** -- (オプション) ディレクトリの説明を指定します
- **オブジェクト接続名** -- ユーザストア名を指定します
- **ホスト** -- ディレクトリのホスト名または IP アドレスを定義します
- **ポート** -- ディレクトリのポート番号を定義します

例 : 389

- **検索ルート** -- 組織の検索ルートを定義します ディレクトリ検索は、ルート レベルから開始します
- **ユーザ DN** -- ディレクトリへのログイン権限を持つユーザ アカウントを定義します

例 : cn=Username, ou=Administration, ou=Corporate, o=Democorp, c=AU

- **パスワード** -- ユーザ アカウント パスワードを定義します
- **パスワードの確認** -- パスワードを確認するユーザ アカウント パスワードを入力します
- **セキュア接続** -- ディレクトリへの接続がセキュリティで保護されていることを示します

7. [次へ] および [完了] をクリックします。

新規ディレクトリが作成されます。ここで、環境を作成する必要があります。

SUN ONE ユーザストア用の環境の作成

Windows で該当

SUN ONE ディレクトリ用のディレクトリ設定の作成および設定後、環境を作成します。「環境」とはユーザストアのビューです。環境では、ユーザ、グループ、組織、タスク、およびロールを管理します。

注: JBoss アプリケーション サーバサービスは、Windows スタートアップ中に自動的に開始されます。また、環境が存在しない場合は、1つ作成されます。自動的なサービス スタートアップを無効にすることをお勧めします。環境がすでに存在する場合は、それを削除してから、SUN ONE ユーザストア用の環境を作成します。

環境を作成する前に、Sun ONE ユーザディレクトリ内にシステム マネージャ アカウントを定義する必要があります。

重要: システム マネージャ アカウントを検索ルート 組織単位 (OU) の下に直接ではなく、検索ルートの下にある組織単位の下に定義することを確認します。たとえば、定義した検索ルートが **dc=company, dc=com** である場合、以下のように、ユーザ **OU** の下にシステム マネージャ アカウントを作成します。**uid=Sysmanager,ou=Users,dc=company,dc=com**

次の手順に従ってください:

1. 以下のディレクトリに移動します。ここで、**JBOSS_HOME** は JBoss をインストールしたディレクトリです。

`JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/`

- a. 以下のファイルを見つけて、一時ディレクトリにコピーします。

`ac-RoleDefinitions_Iplanet_EN.xml`

`ac-environmentSettings.xml`

- b. `ac-environment.properties` ファイルが存在していれば、削除します。

2. CA IdentityMinder 管理コンソールを開き、[環境]、次に [新規] を選択します。

新規環境の画面が表示されます。

3. 環境名として **ac-env** を入力し、説明を提供し、パブリック URL エイリアスとして **ac** を入力します。[次へ] をクリックします。

利用可能なディレクトリを一覧する画面が表示されます。

4. この環境に関連付けるために定義した **SUN ONE** ディレクトリを選択してから、[次へ] をクリックします。

- a. (オプション) この環境のプロビジョニングディレクトリとして使用するディレクトリを選択してから、[次へ] をクリックします。

- b. (オプション) 匿名の接続を認証するユーザ アカウントを指定してから、[検証] を選択します。

CA IdentityMinder 管理コンソールはユーザ アカウントを検証します。

5. [次へ] をクリックして続行します。

6. [ファイルからのロールのインポート] を選択し、[参照] を使用してファイル `ac-RoleDefinitions_iPlanet_EN.xml` を見つけ、[次へ] をクリックします。
7. ユーザ マネージャ アカウントを指定し、[追加] を選択してから [次へ] を選択します。
サマリ画面が開きます。

重要: ユーザ マネージャ アカウントがディレクトリに存在することを確認します。

8. サマリを確認して [完了] をクリックします。
CA IdentityMinder 管理コンソールは環境を作成します。
9. [環境] - [ac-env] - [詳細設定] を選択してから、[インポート] をクリックします。
[インポート設定] ウィンドウが開きます。

- a. `ac-environmentSettings.xml` ファイルを保存したディレクトリを参照し、それを選択してから、[完了] をクリックします。

CA IdentityMinder 管理コンソールは環境を作成します。

10. [続行]、次に [開始] を選択します。
環境が開始されます。

11. [環境] - [ac-env] - [詳細設定] - [ワークフロー] を選択します。
ワークフローの [プロパティ] ウィンドウが開きます。

- a. [有効プロパティ] の横のボックスをオンにしてワークフローを有効にしてから、[保存] をクリックします。

CA IdentityMinder 管理コンソールは、変更を環境に適用します。

12. [環境] - [ac-env] - [システム マネージャ] を選択します。
[システム マネージャ] ウィンドウが開きます。

- a. システム マネージャのユーザ アカウントを指定してから、[検証] を選択します。

CA IdentityMinder 管理コンソールは、システム マネージャのアカウント プロパティを表示します。

- b. [次へ]、[完了] を選択します。

CA IdentityMinder 管理コンソールはシステム マネージャの設定出力を表示し、エラーを指定します（識別される場合）。

- c. [続行] を選択します。

13. [ステータス] フィールドで [再起動] を選択します。

CA IdentityMinder 管理コンソールは環境を再起動します。

14. JBoss アプリケーション サーバを再起動します。

15. コマンドプロンプト ウィンドウを開いて、bin ディレクトリに移動します。

16. 以下のコマンドを実行して、ComponentRegistration を実行します。

```
ComponentRegistration -comp jcs -register -userDN cn=root,dc=etasa -serverDN
dc=im,dc=etasa -pwd <communication_password> -port 20411 -ssl yes -file
C:\temp\output.txt -verbose
```

例 : ComponentRegistration -comp jcs -register -userDN cn=root,dc=etasa
-serverDN dc=im,dc=etasa -pwd password -port 20411 -ssl yes -file
C:\temp\output.txt -verbose

SUN ONE ディレクトリを CA ControlMinder エンタープライズ管理用のユーザストアとして定義しました。これで、CA ControlMinder エンタープライズ管理にログインできるようになりました。

CA Directory 用のディレクトリの作成

ディレクトリによって、CA ControlMinder エンタープライズ管理が管理するユーザディレクトリに関する情報が提供されます。CA ControlMinder エンタープライズ管理のインストール後、CA Directory を設定します。

重要: ディレクトリの UID 属性に値が含まれていない場合、ディレクトリを作成する前に、SAM_CA_Directory.xml ファイルを編集する必要があります。例 :

```
<ImManagedObjectAttr physicalname="uid" displayname="User ID" description="User
ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%"
maxlength="0" permission="WRITEONCE"/>
```

注: UID 属性には一意のユーザ定義データが必要です。CA Directory の各属性は、CA Directory XML ファイル内の CA ControlMinder エンタープライズ管理属性に 1 回マップされます。

次の手順に従ってください:

1. 以下のディレクトリに移動します。ここで、JBoss_HOME は JBoss をインストールしたディレクトリを示しています。

```
JBoss_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/  
/
```

2. 以下のファイルを一時ディレクトリにコピーします。
 - a. SAM_CA_Directory.xml
 - b. ac-RoleDefinitions_CADir_EN.xml
 - c. ac-environmentSettings.xml
3. ac-environment.properties ファイルが存在している場合は削除します。
4. JBoss アプリケーション サーバを起動します。
5. 以下のようにして、CA IdentityMinder 管理コンソールを開きます。

```
http://enterprise_host:port/idmmanage
```

CA IdentityMinder 管理コンソールが開きます。

6. [ディレクトリ] - [新規] を選択します。
新規ディレクトリのウィンドウが開きます。
7. [参照] を選択し、SAM_CA_Directory.xml ファイルを選択します。[次へ] をクリックします。

8. 以下の詳細を入力します。

- **名前** -- ディレクトリの論理名を定義します
- **説明** -- (オプション) ディレクトリの説明を指定します
- **オブジェクト接続名** -- ユーザストア名を指定します
- **ホスト** -- ディレクトリのホスト名または IP アドレスを定義します
- **ポート** -- ディレクトリのポート番号を定義します

例 : 389

- **検索ルート** -- 組織の検索ルートを定義します ディレクトリ検索は、ルート レベルから開始します

注: 複数のドメインを使用する場合、このフィールドは空白のままにします。

- **ユーザ DN** -- ディレクトリへのログイン権限を持つユーザ アカウントを定義します

例 : cn=Username, ou=Administration, ou=Corporate, o=Democorp, c=AU

- **パスワード** -- ユーザ アカウント パスワードを定義します
- **パスワードの確認** -- パスワードを確認するユーザ アカウント パスワードを入力します
- **セキュア接続** -- ディレクトリへの接続がセキュリティで保護されていることを示します

9. [次へ] および [完了] をクリックします。

新規ディレクトリが作成されます。ここで、環境を作成する必要があります。

CA Directory 用の環境の作成

Windows で該当

CA Directory 用のディレクトリ設定を作成して設定したら、環境を作成します。「環境」とはユーザストアのビューです。環境では、ユーザ、グループ、組織、タスク、およびロールを管理します。

注: JBoss アプリケーション サーバ サービスは、Windows スタートアップ中に自動的に開始されます。また、環境が存在しない場合は、1つ作成されます。自動的なサービス スタートアップを無効にすることをお勧めします。環境が存在する場合は、それを削除してから CA Directory 用の環境を作成します。

環境を作成する前に、CA Directory でシステム マネージャ アカウントを定義します。

重要: システム マネージャ アカウントを検索ルート 組織単位 (OU) の下に直接ではなく、検索ルートの下にある組織単位の下に定義することを確認します。たとえば、定義した検索ルートが `dc=company, dc=com` である場合、以下のように、ユーザ OU の下にシステム マネージャ アカウントを作成します。`uid=Sysmanager,ou=Users,dc=company,dc=com`

注: 複数の `domDN.ins` をサポートする場合は、ユーザの完全な DN を定義します。

次の手順に従ってください:

1. CA IdentityMinder 管理コンソールを開き、[環境]、次に [新規] を選択します。
新規環境の画面が表示されます。
2. 環境名として **ac-env** を入力し、説明を提供し、パブリック URL エイリアスとして **ac** を入力します。[次へ] をクリックします。
利用可能なディレクトリを一覧する画面が表示されます。
3. この環境に関連付ける CA Directory を選択し、[次へ] をクリックします。
 - a. (オプション) この環境のプロビジョニング ディレクトリとして使用するディレクトリを選択してから、[次へ] をクリックします。

- b. (オプション) 匿名の接続を認証するユーザ アカウントを指定してから、[検証] を選択します。

CA IdentityMinder 管理コンソールはユーザ アカウントを検証します。

4. [次へ] をクリックして続行します。
5. [ファイルからのロールのインポート] を選択し、[参照] を使用してファイル `ac-RoleDefinitions_CADir_EN.xml` を選択して、[次へ] をクリックします。
6. ユーザ マネージャ アカウントを指定し、[追加] を選択してから [次へ] を選択します。

注: 複数のドメインをサポートする場合は、ユーザの完全な DN を指定します。

サマリ画面が開きます。

重要: ユーザ マネージャ アカウントがディレクトリに存在することを確認します。

7. サマリを確認して [完了] をクリックします。

CA IdentityMinder 管理コンソールは環境を作成します。

8. [環境] - [ac-env] - [詳細設定] を選択してから、[インポート] をクリックします。

[インポート設定] ウィンドウが開きます。

- a. `ac-environmentSettings.xml` ファイルを保存したディレクトリを参照し、それを選択してから、[完了] をクリックします。

CA IdentityMinder 管理コンソールは環境を作成します。

9. [続行]、次に [開始] を選択します。

環境が開始されます。

10. [環境] - [ac-env] - [詳細設定] - [ワークフロー] を選択します。

ワークフローの [プロパティ] ウィンドウが開きます。

- a. [有効プロパティ] の横のボックスをオンにしてワークフローを有効にしてから、[保存] をクリックします。

CA IdentityMinder 管理コンソールは、変更を環境に適用します。

11. [環境] - [ac-env] - [システム マネージャ] を選択します。

[システム マネージャ] ウィンドウが開きます。

- a. システム マネージャのユーザアカウントを指定してから、[検証] を選択します。

CA IdentityMinder 管理コンソールは、システム マネージャのアカウント プロパティを表示します。

- b. [次へ]、[完了] を選択します。

CA IdentityMinder 管理コンソールはシステム マネージャの設定出力を表示し、エラーを指定します（識別される場合）。

- c. [続行] を選択します。

12. [ステータス] フィールドで [再起動] を選択します。

CA IdentityMinder 管理コンソールは環境を再起動します。

13. JBoss アプリケーション サーバを再起動します。

14. CA ControlMinder サービスを再起動します。

CA Directory を使用するよう CA ControlMinder エンタープライズ管理 が定義されました。これで、CA ControlMinder エンタープライズ管理 にログインできるようになりました。

コネクタ サーバへの接続設定

CA ControlMinder エンタープライズ管理 は、管理デバイス上で特権アカウントを検索し、管理するために、コネクタ サーバと通信します。デフォルトでは、CA ControlMinder エンタープライズ管理 は、CA ControlMinder エンタープライズ管理 コンピュータに適用されている環境設定で、コネクタ サーバにインストールされます。必要に応じて、コネクタ サーバをさらに追加できます。

次の手順に従ってください:

1. CA ControlMinder エンタープライズ管理 で、[システム] - [接続管理] - [コネクタ サーバ] - [コネクタ サーバの作成] をクリックします。

[コネクタ サーバの作成: コネクタ サーバの選択] タスク ページが表示されます。

2. (オプション) 既存のコネクタ サーバを選択し、そのコピーとしてコネクタ サーバを以下のように作成します。
 - a. [オブジェクト タイプ:"コネクタ サーバ" のコピーの作成] を選択します。
 - b. 検索する属性を選択してフィルタ値を入力し、[検索] をクリックします。
フィルタ条件に一致するコネクタ サーバのリストが表示されます。
 - c. 新しいコネクタ サーバのベースとして使用するオブジェクトを選択します。
3. [OK] をクリックします。
[コネクタ サーバの作成] タスク ページが表示されます。既存のオブジェクトからコネクタ サーバを作成した場合、ダイアログ ボックスのフィールドには既存オブジェクトの値がすでに入力されています。
4. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドについて説明します。

名前

接続名を定義します。

説明

(オプション) 接続の説明を定義します。

ホスト

CA ControlMinder エンタープライズ管理 の動作対象となるコネクタ サーバの名前を定義します。

例 : host1.comp.com

ポート

コネクタ サーバが通信に使用するポートを定義します。

例 : 20411

セキュリティで保護

CA ControlMinder エンタープライズ管理 とコネクタ サーバ間の接続をセキュリティで保護するかどうかを指定します。

ユーザ名

管理権限を持つユーザのユーザ名を定義します。

例 : cn=root, dc=etasa

パスワード

管理権限を持つユーザ アカウントのパスワードを定義します。

プライマリ

この接続が、ユーザのログインの際に **CA ControlMinder エンタープライズ管理** がデフォルトで使用する接続かどうかを指定します。

注: プライマリ接続を指定する場合、接続を確立する前に一度ログアウトして再ログインします。

プロビジョニングドメイン名

CA IdentityMinder が管理するプロビジョニング ドメインの名前を定義します。

注: ドメイン名では大文字と小文字が区別されます。

タイプ

コネクタ サーバのタイプを指定します。

5. [サブミット] をクリックします。

CA ControlMinder エンタープライズ管理 は、ユーザが指定した情報を使用してコネクタ サーバへのログインを試行します。情報が正しい場合、接続が設定され、これで **CA ControlMinder エンタープライズ管理** を使用して、特権アカウントを管理できるようになります。情報が正しくなく、**CA ControlMinder エンタープライズ管理** がコネクタ サーバに接続できない場合、エラー メッセージが表示され、接続が確立できなかった理由が示されます。

CA ControlMinder エンタープライズ管理 を起動します。

CA ControlMinder エンタープライズ管理 をインストールした後は、CA ControlMinder および Web アプリケーション サーバを起動する必要があります。

以下の手順に従います。

1. CA ControlMinder サービスが開始されていることを確認します。

CA ControlMinder エンタープライズ管理 を使用するには、CA ControlMinder が実行中である必要があります。

2. JBoss アプリケーション サーバ サービスが開始されていることを確認します。JBoss アプリケーション サーバ サービスが開始されていない場合は、以下の操作の 1 つを実行します。

- (Windows) [スタート] - [プログラム] - [CA] - [ControlMinder] - [タスク エンジンの開始] をクリックします。

注: タスク エンジン は、初回のロード時に多少時間がかかる場合があります。

- (Windows) [サービス] パネルから JBoss アプリケーション サーバ サービスを開始します。
- (Linux) 「./JBOSS_DIR/bin/run.sh -b 0.0.0.0」と入力します。

JBoss Application Server のロードが終了すると、CA ControlMinder エンタープライズ管理 の Web ベース インターフェースにログインできます。

CA ControlMinder エンタープライズ管理 を開く

CA ControlMinder エンタープライズ管理 をインストールして起動すると、CA ControlMinder エンタープライズ管理 の URL を使用してリモート コンピュータから Web ベースのインターフェースを起動することができます。

CA ControlMinder エンタープライズ管理 を開く方法

1. Web ブラウザを開き、ホストに以下のいずれかの URL を入力します。

- SSL 接続を使用しない場合は、以下の URL を入力します。

`http://enterprise_host:port/iam/ac`

- SSL 接続を使用する場合は、以下の URL を入力します。

`https://enterprise_host:HTTPSport/iam/ac`

2. 自分のクレデンシャルを使用して、ログインします。

CA ControlMinder エンタープライズ管理 のホームページが表示されます。

注: CA ControlMinder エンタープライズ管理 がインストールされている Windows コンピュータから CA ControlMinder エンタープライズ管理 を開くこともできます。それには、[スタート] - [プログラム] - [CA] - [Access Control] - [Enterprise Management] をクリックします。

例: CA ControlMinder エンタープライズ管理 を開く

Web ブラウザに次の URL を入力して、ネットワーク上の任意のコンピュータから CA ControlMinder エンタープライズ管理 を開きます。

`http://appserver123:18080/iam/ac`

この URL から、CA ControlMinder エンタープライズ管理 が `appserver123` という名前のホストにインストールされ、デフォルトの CA ControlMinder エンタープライズ管理 ポート `18080` を使用しているのがわかります。

例: SSL を使用して CA ControlMinder エンタープライズ管理 を開く

Web ブラウザに以下の URL を入力し、ネットワーク上の任意のコンピュータから SSL を使用して CA ControlMinder エンタープライズ管理 を開きます。

`https://appserver123:18443/iam/ac`

この URL から、CA ControlMinder エンタープライズ管理 が `appserver123` という名前のホストにインストールされ、デフォルトの CA ControlMinder エンタープライズ管理 ポート `18443` を使用しているのがわかります。

詳細な環境設定

CA IdentityMinder 管理コンソールを使用して、詳細な環境設定タスクを実行できます。こうしたタスクには、レポート データベースのプロパティの変更によるカスタム レポートの生成や、特定のイベント発生時の CA ControlMinder エンタープライズ管理 の設定による電子メール通知の送信などがあります。

CA IdentityMinder 管理コンソールによって、ディレクトリの管理およびグラフィカル表示を制御する環境を作成および管理できます。

注: 詳細については、*CA IdentityMinder 管理* コンソールのオンライン ヘルプをご覧ください。オンライン ヘルプは、アプリケーションからアクセスできます。

詳細情報:

[CA IdentityMinder 管理コンソールの有効化](#) (P. 104)

[CA IdentityMinder 管理コンソールの起動](#) (P. 105)

[イベントに対する電子メール通知のセットアップ](#) (P. 105)

CA IdentityMinder 管理コンソールの有効化

エンタープライズ管理サーバの初回のインストール時には、CA IdentityMinder 管理コンソール オプションは無効になっています。CA IdentityMinder 管理コンソールを有効にするには、デフォルト設定を変更します。

重要: インストール時に **Active Directory** または組み込みユーザ ストアの使用を選択した場合のみ、以下のプロシージャを完了します。

CA IdentityMinder 管理コンソールの有効化

1. JBoss が実行されている場合は、停止します。以下のいずれかの操作を実行します。
 - JBoss ジョブ ウィンドウから、プロセスを中断します (Ctrl+C)。
 - [サービス] パネルから JBoss アプリケーション サーバ サービスを停止します。
2. 以下のディレクトリに移動します。ここで、*JBoss_HOME* は JBoss をインストールしたディレクトリです。

```
JBoss_HOME/server/default/deploy/  
IdentityMinder.ear/management_console.war/WEB-INF
```

3. 編集可能な形式で *web.xml* ファイルを開きます。
4. 以下のセクションを探します。

```
AccessFilter
```
5. <param-value> フィールドで、値を [True] に変更します。
6. ファイルを保存して閉じます。
7. JBoss を起動します。

CA IdentityMinder 管理コンソールが有効になります。

CA IdentityMinder 管理コンソールの起動

CA IdentityMinder 管理コンソールには Web ベースのインターフェースがあります。CA IdentityMinder 管理コンソールを有効化して CA ControlMinder エンタープライズ管理 を起動すると、お使いのネットワーク上の任意のコンピュータから CA IdentityMinder 管理コンソールを開くことができます。

CA IdentityMinder 管理コンソールを開くには、ホストで Web ブラウザを起動し、次の URL 入力します。

`http://enterprise_host:port/idmanage`

CA IdentityMinder 管理コンソールが開きます。

例: CA IdentityMinder 管理コンソールの起動

ネットワーク上の任意のコンピュータから CA IdentityMinder 管理コンソールを開くには、Web ブラウザに次の URL を入力します。

`http://appserver123:18080/idmanage`

この URL から、CA IdentityMinder 管理コンソールが appserver123 という名前のホストにインストールされ、デフォルトの ACPMI ポート 18080 を使用しているのがわかります。

イベントに対する電子メール通知のセットアップ

このシナリオは、システム管理者が、ユーザが共有アカウント パスワードをリクエストした場合、またはアカウント パスワードをチェックアウトした場合などのイベントに対する電子メール通知を設定する方法を説明します。

電子メール通知

電子メール通知は電子メール テンプレートから生成され、CA ControlMinder エンタープライズ管理 ユーザにシステムのイベントを通知します。承認ワークフローに関連するイベント用の電子メール通知を有効にするのがベスト プラクティスです。

電子メール通知を有効にすると、以下のいずれかのイベントの発生時に、エンタープライズ管理サーバは電子メール通知を生成します。

- 承認または拒否を必要とするイベントが保留中の場合。
- 承認者がイベントを承認した場合。
- 承認者がイベントを拒否した場合。
- イベントが開始、失敗、または完了した場合。
- CA ControlMinder エンタープライズ管理 ユーザが作成または変更された場合。

注: 電子メール通知の設定方法の詳細については、「実装ガイド」を参照してください。

電子メール通知のしくみ

電子メール通知は、システムのイベントを CA ControlMinder エンタープライズ管理 ユーザに通知します。

1. イベントが発生すると、CA ControlMinder エンタープライズ管理 はイベントに対して電子メール通知が有効になっているかどうかを確認します。
2. 電子メール通知が有効な場合、CA ControlMinder エンタープライズ管理 は適切なサブディレクトリ内のイベント タイプを検索します。
たとえば、電子メールが特権アカウント要求を承認するために送信される場合、CA ControlMinder エンタープライズ管理 は **Approved** サブディレクトリの中を検索します。
3. CA ControlMinder エンタープライズ管理 のサブディレクトリにイベントと同じ名前の電子メール テンプレートが存在するかを確認します。次に、以下を実行します。
 - イベントと同じ名前の電子メール テンプレートが存在する場合、CA ControlMinder エンタープライズ管理 は電子メール テンプレートを受信者に送信します。
 - イベントと同じ名前の電子メール テンプレートが存在しない場合、CA ControlMinder エンタープライズ管理 は、**defaultEvent.tmpl** 電子メール テンプレートを受信者に送信します。

例

以下のユースケースは、イベント、およびイベントに対して送信される通知の例です。

1. ユーザが、次の火曜日にアカウントを使用することを要求するとします。電子メールが承認者のもとに送信され、承認者のワークリストに要求が存在することを知らせます。

CreatePrivilegedAccountExceptionNotStartedEvent 通知は「保留中」フォルダに送信されます。

2. 承認者は要求を承認します。ユーザは、要求が承認されたことを伝える電子メールを受信します。

CreatePrivilegedAccountExceptionNotStartedEvent 通知は「承認」フォルダに送信されます。

3. 火曜日に、アカウントはユーザに対して使用可能になります。ユーザは、アカウント使用して作業を開始できることを伝える電子メールを受信します。

CreatePrivilegedAccountExceptionEvent 通知は「完了」フォルダに送信されます。

4. 火曜日が終わり、アカウントが使用可能ではなくなりました。ユーザは、アカウントに対するアクセス権がなくなったことを伝える電子メールを受信します。

DeletePrivilegedAccountExceptionEvent は「完了」フォルダに送信されます。

最も一般的に使用されるイベントは以下のとおりです。

BreakGlassCheckOutAccountEvent

特権アカウントが **Break Glass** アクションを実行する場合に承認者に通知を送信します。

CheckOutAccountPasswordEvent

パスワードがチェックアウトされるたびに承認者に通知を送信します。

CreatePrivilegedAccountExceptionEvent

アカウントが使用可能な場合、要求者に通知を送信します。このイベント用の通知を有効にするには、「完了」フォルダ内のテンプレートを編集します。

CreatePrivilegedAccountExceptionNotStartedEvent

特権アカウントに対するアクセス権の要求が、承認者のワーク リストで処理待ちであることを伝える通知を承認者に送信します。要求が承認、拒否、または完了した場合、要求者に通知を送信します。

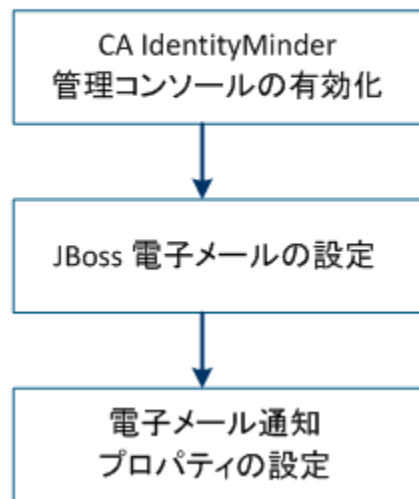
イベントに対して電子メール通知をセットアップする方法

CA IdentityMinder 管理コンソールを使用して、電子メール通知オプションを設定し、環境でレポートするデータベース設定を定義します。

CA IdentityMinder 管理コンソールを開くと、「環境」で作業することになります。「環境」では、ディレクトリが視覚的に表され、ディレクトリの管理を制御します。たとえば、環境において、電子メール通知オプションを設定し、レポートするデータベース設定を定義することができます。SAM イベントには電子メール通知のみを有効にすることをお勧めします。

重要: 環境に対する変更は、CA ControlMinder エンタープライズ管理の安定性に影響を与える場合があります。詳細については、CA サポート (<http://ca.com/jp/support>) にお問い合わせください。

CA ControlMinder のイベントに 電子メール通知をセットアップする方法



次の手順に従ってください:

1. [CA IdentityMinder 管理コンソールの有効化](#) (P. 104)
2. [JBoss 電子メールの設定](#) (P. 111)
3. [電子メール通知プロパティの設定](#) (P. 114)

JBoss 電子メールの設定

電子メール通知を送信するには、JBoss インストール環境で `mail-service.xml` および `email.properties` ファイルを設定し、既存の **CA ControlMinder** 電子メール テンプレートをそれに応じて変更します。

次の手順に従ってください:

1. エンタープライズ管理マシンに接続し、JBoss が実行中の場合は停止します。以下のいずれかの操作を実行します。
 - JBoss がサービスとしてインストールされていない場合は、JBoss アプリケーション サーバ ウィンドウを中断します (Ctrl+C)。
 - JBoss がサービスとしてインストールされている場合は、サービス画面から JBoss サービスを停止します。
2. `mail-service.xml` ファイルを編集するために開きます。デフォルトでは、このファイルは JBoss インストール ディレクトリのサブディレクトリに位置します。

`JBASS_HOME/server/default/deploy/mail-service.xml`

3. mail-service.xml 内の "mail.smtp.host" エントリを確認します。SMTP ホストのデフォルト値を、送信電子メールサーバ (SMTP サーバ) のフル DNS ドメイン名に変更します。

```
<property name="mail.smtp.host" value="mail.ca.com" />
```

注:エンタープライズ管理サーバ上の hosts ファイルは、このプロパティに指定するフル DNS ドメイン名を SMTP サーバの IP アドレスに対して解決できる必要があります。

4. 通知送信者の電子メールアドレスを指定します。

```
<property name="mail.from" value="sendername@ca.com" />
```

5. (オプション) SMTP 認証および TLS セキュリティを有効にします。そのためには、SMTP ユーザ名とパスワードを指定し、SMTP 設定プロパティを追加します。

```
<attribute name="User">MySMTPUser</attribute>
<attribute name="Password">MySMTPPassword</attribute>
<attribute name="Configuration">
  <configuration>
    <property name="mail.smtp.auth" value="true"/>
    <property name="mail.smtp.starttls.enable" value="true"/>
  </configuration>
</attribute>
```

注: 認証を必要としない SMTP サービスを使用している場合は、この手順をスキップできます。

電子メール通知を設定するイベントごとに以下を実行します。

次の手順に従ってください:

1. イベントに対応する電子メール テンプレートを開きます。

例 :

- a. 特権アカウント パスワード要求が承認されたことを受信者に知らせる電子メール通知を設定するには、以下のディレクトリで `CreatePrivilegedAccountExceptionEvent.tmpl` ファイルを開きます。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/approved`

- b. 保留中のエンドポイント ステータスについて受信者に知らせる電子メール通知を設定するには、次のディレクトリで `EndpointStatusEvent.tmpl` ファイルを開きます。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailtemplates/default/pending`

2. テンプレート ホスト名およびポートを `'http://localhost:8080/iam/ac'` からエンタープライズ管理サーバのホスト名およびポートに変更します (例: `"https://computer.com:18443/iam/ac"`) 。
3. ファイルを保存して閉じます。

`email.properties` ファイルを設定します。

次の手順に従ってください:

1. 以下のディレクトリを参照し、`email.properties` ファイルを開きます。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/`

2. `mail-service.xml` ファイルと同じように送信者電子メール アドレスを以下の形式で指定します。

`admin.email.address=sendername@ca.com`

3. `email.properties` ファイルを保存して閉じます。
4. JBoss を再起動します。

電子メール通知プロパティの設定

環境で電子メール通知プロパティを設定するために CA IdentityMinder 管理コンソールを開きます。

注: 環境の詳細については、コンソールから参照できる CA IdentityMinder 管理コンソール オンライン ヘルプを参照してください。

重要: 環境に対する変更は、CA ControlMinder エンタープライズ管理 の安定性に影響を与える場合があります。詳細については、CA サポート (<http://ca.com/jp/support>) にお問い合わせください。

次の手順に従ってください:

1. [環境] をクリックします。設定する環境をクリックし、次に [詳細設定]、[電子メール] をクリックします。

電子メールのプロパティ ウィンドウが表示されます。

2. 組織に該当するオプションを設定します。以下のオプションがあります。

イベント電子メール有効化

SAM イベントを含む CA ControlMinder エンタープライズ管理 イベントの電子メール通知を有効にします。

タスク電子メール有効化

SAM タスクの電子メール通知を有効にします。CA ControlMinder エンタープライズ管理 はタスク用の電子メールテンプレートを提供しないため、タスク用の電子メール通知を有効にしないことをお勧めします。

テンプレート ディレクトリ

CA IdentityMinder で電子メール メッセージの作成に使用する電子メールテンプレートの場所を指定します。この値を "default" に設定します。

注: 電子メールテンプレートは、以下のディレクトリにあります。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/`

3. 電子メール通知を送信したいイベントを指定します。

電子メール テンプレートが提供されている **SAM** イベントのみを指定することをお勧めします。以下の手順を実行します。

a. イベントごとにチェックボックスをオンにします。ただし、以下の **SAM** イベントは除きます。

- CreatePrivilegedAccountExceptionNotStartedEvent
- CreatePrivilegedAccountExceptionEvent
- BreakGlassCheckOutAccountEvent
- CheckOutAccountPasswordEvent

b. [削除] をクリックします。

上記の **SAM** イベント以外のすべてのイベントが削除されます。これらの **SAM** イベントについて電子メール通知を送信するよう **CA ControlMinder** エンタープライズ管理 が設定されました。

4. [保存] をクリックします。

電子メール通知プロパティは保存され、[環境プロパティ] ウィンドウに戻ります。

5. [再起動] をクリックします。

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

注: 電子メール通知の詳細については、「エンタープライズ管理ガイド」を参照してください。

電子メール テンプレート

CA ControlMinder エンタープライズ管理 は、電子メール テンプレートから電子メール通知を生成します。各電子メール テンプレートには、以下の情報が含まれています。

- **配信情報** - 電子メールの受信者リスト。
- **件名** - 電子メールの件名で使用するテキスト。
- **コンテンツ** - 電子メール本文。本文には通常、静的テキストと変数の両方が含まれています。CA ControlMinder エンタープライズ管理 は、電子メールをトリガするタスクまたはイベントに基づいてこれらを解決します。

電子メール テンプレートは以下のディレクトリにあります。*JBoss_home* は、JBoss をインストールしたディレクトリです。

JBoss_home/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default

emailTemplates ディレクトリには、5つのサブディレクトリが含まれます。各フォルダはイベント状態と関連付けられます。以下の表では、各サブディレクトリにある電子メールテンプレートの目的をリストします。

サブディレクトリ	内容
承認済み	■ CertifyRoleEvent.tmpl - 使用されなくなりました。 ■ CheckOutAccountPasswordEvent.tmpl - 特権アカウント パスワード要求が承認されたことを受信者に通知します。 ■ CreatePrivilegedAccountExceptionEvent.tmpl - 特権アカウント パスワード要求が指定した期間承認されたことを受信者に知らせます。（このテンプレートは特権アカウント要求タスクに該当します）。 ■ defaultEvent.tmpl - イベントが承認されたことを受信者に知らせます。 ■ defaultTask.tmpl - タスクが承認されたことを受信者に知らせます。 ■ ForgottenPasswordEvent.tmpl - 使用されなくなりました。 ■ SelfRegisterUserEvent.tmpl - 使用されなくなりました。

サブディレクトリ 内容

完了

- AccumulatedProvisioningRolesEvent.tmpl - 使用されなくなりました。
- CertificationNonCertifiedActionCompletedNotificationEvent.tmpl - 使用されなくなりました。
- CertificationNonCertifiedActionPendingNotificationEvent.tmpl - 使用されなくなりました。
- CertificationRequiredFinalReminderNotificationEvent.tmpl - 使用されなくなりました。
- CertificationRequiredNotificationEvent.tmpl - 使用されなくなりました。
- CertificationRequiredReminderNotificationEvent.tmpl - 使用されなくなりました。
- CheckOutAccountPasswordEvent.tmpl -- チェックアウトした特権アカウントのパスワードを受信者に通知します。
- CreateProvisioningUserNotificationEvent.tmpl - 使用されなくなりました。
- CreatePrivilegedAccountExceptionEvent -- 要求されたアカウントが使用可能であることを受信者に伝えます。
- CreatePrivilegedAccountExceptionNotStartedEvent.tmpl -- 特権アカウントへのアクセスのリクエストがワーク リスト内で保留中であることを受信者に伝えます。
- defaultEvent.tmpl - CA ControlMinder エンタープライズ管理 がイベントを完了したことを受信者に知らせます。
- defaultTask.tmpl - CA ControlMinder エンタープライズ管理 がタスクを完了したことを受信者に知らせます。
- ForgottenPassword.tmpl - 使用されなくなりました。
- ForgottenUserID.tmpl - 使用されなくなりました。
- Self Registration.tmpl - 使用されなくなりました。

無効

- AssignProvisioningRoleEvent.tmpl - 使用されなくなりました。
 - DefaultEvent.tmpl - イベントが失敗したことを受信者に知らせます。
 - DefaultTask.tmpl - タスクが失敗したことを受信者に知らせます。
-

サブディレクトリ	内容
保留中	■ BreakGlassCheckOutAccountEvent.templ - Break Glass チェックアウトが実行されたこと承認者に知らせます。 ■ CertifyRoleEvent.templ - 使用されなくなりました。 ■ CheckOutAccountPassswordEvent.templ -- 特権アカウントのチェックアウトに対応する必要があることを承認者に知らせます。 ■ defaultEvent.templ - ワーク リスト項目に対応する必要があることを承認者に知らせます。 ■ defaultTask.templ -- タスクに対応する必要があることを承認者に通知します。 ■ ModifyUserEvent.templ - 使用されなくなりました。
拒否	■ CertifyRoleEvent.templ - 使用されなくなりました。 ■ CheckOutPasswordEvent.templ - 特権アカウント パスワード要求が拒否されたことを受信者に通知します。 ■ CreatePrivilegedAccountExceptionEvent.templ - 指定した期間の特権アカウントへのアクセス要求が拒否されたことを受信者に通知します（このテンプレートは、特権アカウント要求タスクに対応します）。 ■ defaultEvent.templ - イベントが拒否されたことを受信者に通知します。 ■ defaultTask.templ - タスクが拒否されたことを受信者に通知します。 ■ ForgottenPasswordEvent.templ - 使用されなくなりました。 ■ SelfRegisterUserEvent - 使用されなくなりました。

Windows での CA ControlMinder エンタープライズ管理 のアンインストール

Windows で該当

Windows で CA ControlMinder エンタープライズ管理 をアンインストールするには、Windows 管理者権限を持つユーザ（Windows 管理者または Windows Administrators グループのメンバ）として Windows システムにログインする必要があります。

注: この手順は、必須のソフトウェアをアンインストールしません。必須のソフトウェアをアンインストールするには、JDK をアンインストールする前に JBoss をアンインストールする必要があります。必須ソフトウェアのアンインストールの詳細については、対象の製品のドキュメントを参照してください。

Windows での CA ControlMinder エンタープライズ管理 のアンインストール方法

1. JBoss が実行されている場合は、停止します。
2. [スタート] - [コントロール パネル] - [プログラムの追加と削除] を選択します。
[プログラムの追加と削除] ダイアログ ボックスが表示されます。
3. プログラム リストをスクロールして CA ControlMinder エンタープライズ管理 を選択します。
4. [変更と削除] をクリックします。
CA ControlMinder エンタープライズ管理 のアンインストール ウィザードが表示されます。
5. ウィザードの手順に従って、CA ControlMinder エンタープライズ管理 をアンインストールします。
アンインストールが完了し、コンピュータから CA ControlMinder エンタープライズ管理 が削除されます。
6. ウィザードを終了するには、[完了] をクリックしてください。

Linux での CA ControlMinder エンタープライズ管理 のアンインストール

コンピュータから CA ControlMinder エンタープライズ管理 を削除するには、CA ControlMinder エンタープライズ管理 が提供するアンインストールプログラムを使用する必要があります。

以下の手順に従います。

1. 以下のいずれかを実行して JBoss を停止します。

- JBoss ジョブ ウィンドウから、プロセスを中断します (Ctrl+C)。
- 別のウィンドウで、以下のように入力します。

```
./JBoss_path/bin/shutdown -S
```

2. 以下のコマンドを入力します。

```
"/ACPMInstallDir/Uninstall_EnterpriseManagement/Uninstall_CA_Access_Control_Enterprise_Management"
```

ACPMInstallDir

CA ControlMinder エンタープライズ管理 のインストール ディレクトリを定義します。デフォルトでは、このパスは次のとおりです。

```
/opt/CA/AccessControlServer/
```

InstallAnywhere がアンインストール ウィザードまたはコンソールをロードします。

3. プロンプトに従って、CA ControlMinder エンタープライズ管理 をアンインストールします。

アンインストールが完了し、コンピュータから CA ControlMinder エンタープライズ管理 が削除されます。

エンタープライズ管理サーバからの追加コンポーネントの削除

CA ControlMinder エンタープライズ管理 を完全にアンインストールするには、アンインストールプログラムを実行した後、コンピュータから追加のコンポーネントを削除します。

ビジネス データの損失を防ぐため、アンインストールプログラムは以下のリソースを削除しません。

- CA ControlMinder エンドポイント管理 フィルタ (場所 :
JBoss_Dir/server/default/conf/accesscontrol)
- メッセージキュー データ ファイル (場所 :
ACServerDir/MessageQueue/tibco/ems/data)

エンタープライズ管理サーバから追加コンポーネントを削除する方法

1. 以下のディレクトリを削除します。
 - *JBoss_Dir/server/default/deploy/IdentityMinder.ear*
 - *JBoss_Dir/server/default/deploy/SiteMinderAgent.ear*
2. CA ControlMinder をアンインストールします。
3. (Windows) 以下のレジストリ キーを削除します。
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall\CA Access Control Advanced Policy Management Server
4. 以下のとおり JCS を削除します。
 - a. (Windows) [プログラムの追加と削除] ダイアログ ボックスを使用して CA IdentityMinder コネクタ サーバをアンインストールします。
 - b. *jcs.exe* プロセスを終了します。
 - c. CA IdentityMinder - コネクタ サーバ(Java) サービスを削除します。
5. エンタープライズ管理サーバをインストールしたディレクトリを削除します。
たとえば、*C:\Program Files\CA\AccessControlServer* を削除します。
すべての CA ControlMinder エンタープライズ管理 コンポーネントがコンピュータから削除されました。

詳細情報:

[アンインストールの方法](#) (P. 208)

配布サーバの実装

配布サーバは、アプリケーションサーバとエンドポイント間の通信を処理します。配布サーバはデフォルトではエンタープライズ管理サーバ上にインストールされます。フェールオーバーとハイ アベイラビリティを実現するために、企業内に複数の配布サーバをインストールすることができます。

配布サーバのインストール

CA ControlMinder デプロイメントの拡張を計画している場合は、配布サーバを別々のコンピュータにインストールし、それらの間でファイルを配布するように、配布サーバを設定します。

以下の手順に従います。

1. お使いのオペレーティング システム用の適切な CA ControlMinder サーバ コンポーネント DVD を光ディスク ドライブに挿入します。
2. 以下の手順を実行します。
 - Windows の場合

autorun が有効になっている場合は、Product Explorer が自動的に表示されます。以下の手順に従います。

 - a. Product Explorer が表示されない場合は、光ディスク ドライブのディレクトリに移動し、ProductExplorerrx86.EXE ファイルをダブルクリックします。
 - b. Product Explorer で [コンポーネント] フォルダを展開し、CA ControlMinder 配布サーバを選択して、[インストール] をクリックします。

- Linux の場合

- a. 光ディスク ドライブをマウントします。
- b. ターミナル ウィンドウを開き、光ディスク ドライブ上の以下のディレクトリに移動します。

`/DistServer/Disk1/InstData/NoVM`

- c. 以下のコマンドを実行します。

```
./install_DistServer.bin -i console
```

3. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

メッセージ キュー設定

メッセージ キュー サーバの管理者パスワード（通信パスワード）を定義します。

制限：最低 6 文字

Java コネクタ サーバ - プロビジョニング ディレクトリ情報

Java コネクタ サーバ用のパスワードを定義します。

注：Java コネクタ サーバは、CA ControlMinder エンタープライズ管理に特権アカウント管理機能を提供します。

CA ControlMinder 配布サーバのインストールが完了します。

重要：エンタープライズ管理サーバをインストールした際に定義したのと同じ通信パスワードを指定することを確認します。エンタープライズ管理サーバは、通信パスワードを使用してメッセージ キュー キーストア、管理者アカウントを管理し、CA Access Control エンタープライズ管理とエンドポイントの間の通信を処理し、Java Connection Server を管理します。

注：ディザスタ リカバリの実装の一部として配布サーバをインストールする場合は、追加の手順を完了する必要があります。

4. エンタープライズ管理サーバ上で、配布サーバをインストールした後、sepmid ユーティリティを使用して、外部配布ホストを配布マップ サーバに手動でサブスクライブします。

注：この手順なしでは、配布サーバはポリシーを受信できません。

詳細情報:

[運用環境配布サーバのセットアップ](#) (P. 538)

[ディザスタリカバリ配布サーバのセットアップ](#) (P. 540)

第 6 章：エンタープライズ レポート機能の実装

このセクションには、以下のトピックが含まれています。

[エンタープライズ レポート機能 \(P. 125\)](#)

[レポート サービスのアーキテクチャ \(P. 126\)](#)

[レポート サービス サーバ コンポーネントの設定方法 \(P. 128\)](#)

エンタープライズ レポート機能

CA ControlMinder エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ (CA ControlMinder レポート ポータル) を使用して、レポート機能を提供します。エンタープライズ レポート機能を使用すると、各エンドポイント (ユーザ、グループ、リソース) のセキュリティ ステータスを 1 つの場所で確認できます。CA ControlMinder レポートは、各エンドポイントについて、誰が何を実行できるかを定義するルールおよびポリシーを記述し、ポリシーの例外があれば示します。

設定が終了すると、CA ControlMinder エンタープライズ レポート機能は単独で機能して、手動操作の必要なく継続的に各エンドポイントからデータを収集し、情報を中央サーバに格納します。各エンドポイントからのデータの収集は、スケジュールで設定することも、オンデマンドで行うこともできます。各エンドポイントに接続しなくても、誰がどのリソースへのアクセスを許可されているかを確認することができます。収集サーバが稼働しているかダウンしているかに関係なく、各エンドポイントは自身のステータスについてレポートします。

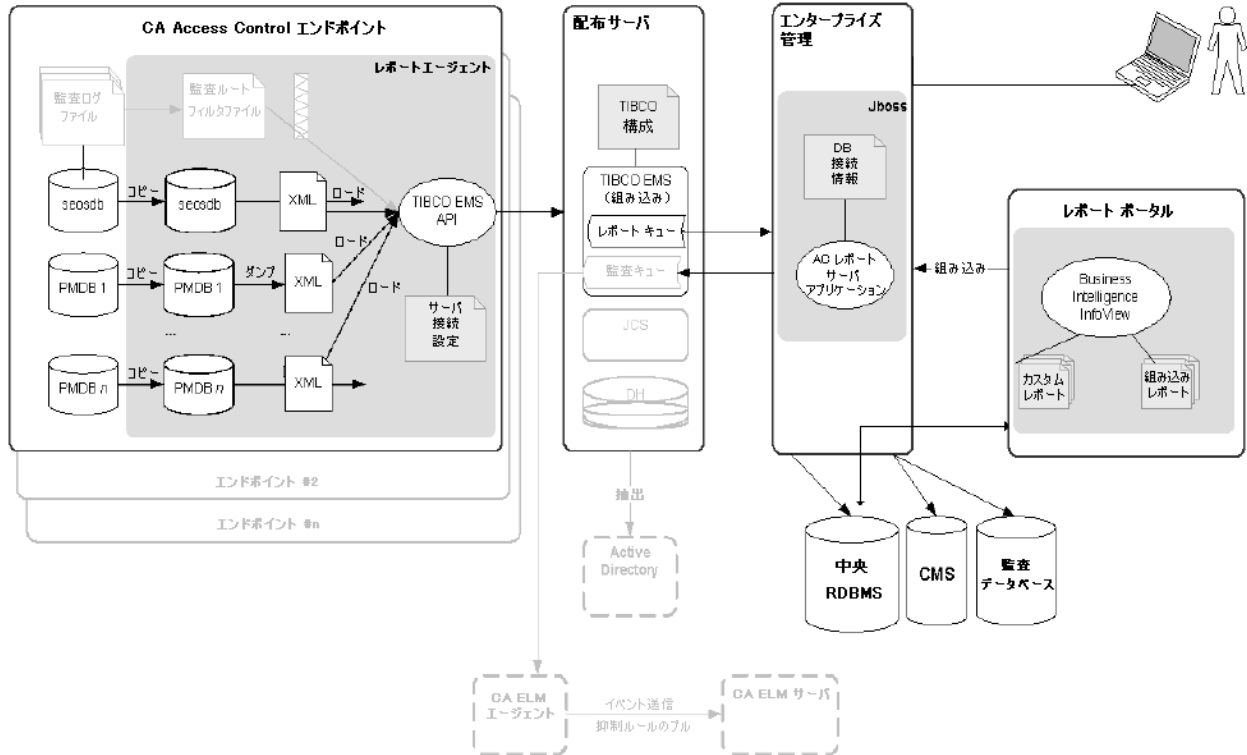
レポート サービスのアーキテクチャ

CA ControlMinder レポート サービスは、CA ControlMinder エンタープライズ レポートの作成に対応するサーバベースのプラットフォームを提供します。このプラットフォームを使用して、すべての CA ControlMinder エンドポイントから取得したデータを含むレポートを作成できます。作成したレポートは、Web 対応のアプリケーション上で表示および管理できます。

レポート サービスでは、既存の CA ControlMinder インフラストラクチャ上にレポート環境を構築できます。

注: エンタープライズ レポートの詳細については、「エンタープライズ管理ガイド」を参照してください。

以下の図に、レポート サービス コンポーネントのアーキテクチャを示します。この図では、コンポーネント間でのデータの流れについても示します。



上の図は、以下のことを示します。

- CA ControlMinder データベース (seosdb) および任意の数の Policy Model (PMDB) が含まれる各エンドポイントには、レポート エージェント コンポーネントがインストールされています。
- レポート エージェントはエンドポイントからデータを収集し、配布サーバに処理のため送信します。
- シンプルなエンタープライズ モデルでは、1つの配布サーバがすべてのエンドポイント データを処理し、処理したデータを中央データベースに格納のため送信します。配布サーバ コンポーネントを複製することで、大規模な企業環境においてフォルト トレランスおよび高速処理を実現する設計が可能です。
- 中央データベース (RDBMS) はエンドポイント データを格納します。
- レポート ポータルを利用すると、中央データベース内のデータにアクセスして組み込み型のレポートを作成すること、またはデータについて問い合わせを行いカスタム レポートを作成することができます。

レポート サービス サーバコンポーネントの設定方法

エンタープライズ レポートを使用するには、CA ControlMinder レポーティング サービスのサーバコンポーネントをインストールして設定します。サーバコンポーネントをインストールして設定してから、各エンドポイントでレポート エージェントを設定します。

注: レポート エージェントのインストールと設定は、CA ControlMinder および UNAB エンドポイントのインストールの一環として行われるものであり、この手順では取り扱いません。

レポート サービス サーバコンポーネントをセットアップするには、以下の手順に従います。

1. まだ行っていない場合は、エンタープライズ管理サーバをインストールして設定します。
2. レポート ポータル コンピュータ (CA Business Intelligence) をセットアップします。

CA Business Intelligence インストール ファイルは、CA サポートの Web サイトにあります。

3. レポート ポータルで CA ControlMinder レポート パッケージをデプロイします。
4. CA Business Intelligence への接続を設定します。
5. スナップショット定義を作成します。

ここで、CA Business Intelligence と CA ControlMinder エンタープライズ管理 でレポートを作成して表示できます。

注: レポートの作成と表示の詳細については、「エンタープライズ管理ガイド」を参照してください。

詳細情報:

[レポート作成のための Windows エンドポイントの設定](#) (P. 206)

[レポート作成のための UNIX エンドポイントの設定](#) (P. 312)

[レポート作成のための UNAB の設定](#) (P. 427)

レポート ポータル コンピュータのセットアップ方法

レポート ポータルを使用すると、CA ControlMinder エンタープライズ管理が中央データベースに格納するエンドポイント データにアクセスして、組み込みレポートの作成、またはデータを問い合わせ、カスタム レポートの作成を行うことができます。 レポート ポータルは、CA Business Intelligence を使用します。

注: レポート ポータルの旧バージョン、または CA Business Intelligence または BusinessObjects EnterpriseXI がスタンドアロンでインストールされている場合、アップグレードの必要はなく、既存のインストールを代わりに使用できます。

レポート ポータルをセットアップするには、以下の手順に従います。

1. Oracle データベースを使用する場合は、レポート ポータル コンピュータに完全な Oracle クライアントをインストールします。
2. Microsoft SQL Server を使用する場合は、レポート ポータル コンピュータに Microsoft SQL Server Native Client をインストールします。
3. まだ実行していない場合は、中央データベースおよび配布サーバをセットアップします。

注: エンタープライズ管理サーバのインストール時に、中央データベースおよび配布サーバをセットアップします。

4. (UNIX) レポート ポータル コンピュータが Solaris または Linux のコンピュータである場合は、CA Business Intelligence インストール用に UNIX コンピュータを準備します。
5. レポート ポータル コンピュータおよびエンタープライズ管理サーバのシステム時刻を同期します。

システム時刻を同期しない場合、CA ControlMinder エンタープライズ管理が生成するレポートのステータスが保留または循環のままになります。

6. ご使用のオペレーティングシステムに対応する CA Business Intelligence をインストールします。

CA Business Intelligence インストール ファイルは、CA サポートの Web サイトにあります。

注: Windows 用のレポート ポータルでは、デフォルトで Microsoft SQL Server 認証を使用して、接続が認証されます。認証にドメイン ユーザアカウント設定を使用する場合、[Windows 認証で動作 \(P. 591\)](#)するようにレポート ポータルを設定できます。

レポート ポータルがセットアップされ、これで CA ControlMinder レポート パッケージをデプロイできるようになりました。

注: CA Business Intelligence の詳細については、[CA Technologies サポート](#)から入手可能な「CA Business Intelligence インストール ガイド」を参照してください。

例: Windows への CA Business Intelligence のインストール

以下の手順は、Windows への CA Business Intelligence のインストール手順を示しています。

注: インストールは、完了まで約 1 時間かかる場合があります。

1. CA Business Intelligence for Windows DVD をご使用の光ディスク ドライブに挿入します。
2. ¥Disk1¥InstData¥VM フォルダに移動し、install.exe をダブルクリックします。

CA Business Intelligence のインストール ウィザードが起動します。

3. 以下の表を使用して、インストール ウィザードを完了します。

情報	アクション
インストール言語	使用するサポート対象インストール言語を選択し、[OK] をクリックします。 注: 英語以外のサポート対象言語のいずれかにインストールする場合、ローカライズされたオペレーティングシステムが必要です。
使用許諾契約書	[使用許諾契約書の条項に同意します] を選択し、[次へ] をクリックします。
インストール タイプ	[標準] を選択して、[次へ] をクリックします。
root 以外のクレデンシャル	root 以外のユーザ名とパスワードを入力します。
BusinessObjects XI 管理者パスワード	「P@ssw0rd」と 2 回入力して、パスワードを設定、確認し、[次へ] をクリックします。 注: パスワードルールについては、「CA Business Intelligence インストール ガイド」をご覧ください。これは、CA ControlMinder のマニュアル選択メニューからご利用いただけます。
Web サーバ設定	[次へ] をクリックして、デフォルト設定をそのまま使用します。

情報	アクション
CMS データベース設定	以下の情報を入力して、[次へ] をクリックします。 ■ MySQL root パスワード : P@ssw0rd ■ ユーザ名 : cadbusr ■ パスワード : C0nf1dent1al ■ データベース名 : MySQL1 注: CA Business Intelligence Central Management Server (CMS) は内部管理目的のみに使用されます。
監査の有効化	[次へ] をクリックして、デフォルト設定をそのまま使用します。
監査データベース設定	以下の情報を入力して、[次へ] をクリックします。 ■ ユーザ名 : cadbusr ■ パスワード : C0nf1dent1al ■ データベース名 : MySQL1
設定の確認	設定を確認し、[インストール] をクリックして、インストールを完了します。

インストールが開始されます。完了まで約 1 時間かかる場合もあります。

重要: CA Business Intelligence Central Management Server (CMS) は内部管理目的のみに使用され、レポートの生成と表示に使用されるレポートデータは含まれていません。CA ControlMinder エンタープライズ管理 をインストールした際に定義したレポートデータベースには、レポートエージェントが配布サーバにアップロードするデータが含まれています。CMS の詳細については、「CA Business Intelligence インストール ガイド」を参照してください。

CA Business Intelligence のインストール用の Linux の準備

CA Business Intelligence を Linux にインストールするには、コンピュータを事前に準備しておく必要があります。CA Business Intelligence インストール用に root 以外のユーザを作成し、Oracle RDBMS が CA Business Intelligence のインストールで認識されることを確認し、環境変数を設定します。

以下の手順に従います。

1. root ユーザとしてログインします。
2. root 以外のユーザを作成します。CA Business Intelligence インストールでは root 以外のユーザが必要になります。

たとえば、以下のコマンドを入力し、グループ「other」に属する bouser という名前のユーザを作成します。

```
groupadd other
useradd -d /home/bouser -g other -m -s /bin/bash -c bouser bouser
passwd bouser
```

プロンプトが表示されたら、定義済みのユーザのパスワードを入力して確認します。

3. LANG 環境変数が以下のように設定されることを確認します。

```
LANG=en_US.utf8
```

4. 作成した root 以外のユーザとしてログインします。
5. 以下のコマンドを入力して、ORACLE_HOME および TNS_ADMIN 環境変数が正しく設定されていることを確認します。

```
echo $ORACLE_HOME
echo $TNS_ADMIN
```

出力が空でなければ、これらの環境変数が有効であることがわかります。以下に例を示します。

```
/opt/oracle/app/oracle/product/10.2.0/client_1
/opt/oracle/app/oracle/product/10.2.0/client_1/admin/network
```

コマンドで空の出力を受信した場合は、root でないユーザとして作成したユーザ用に変数が設定されていることを確認します。たとえば、/home/bouser/.profile を次のように編集します。

```
ORACLE_HOME=/opt/oracle/app/oracle/product/10.2.0/client_1
export ORACLE_HOME
TNS_ADMIN=$ORACLE_HOME/network/admin
export TNS_ADMIN
```

6. `root` でないユーザに対する `LD_LIBRARY_PATH` に以下のパスが含まれていることを確認します。

```
$ORACLE_HOME/lib:$ORACLE_HOME/lib32
```

たとえば、次のコマンドを入力し、出力を検索してこれらのパスを探します。

```
echo $LD_LIBRARY_PATH
```

これらのパスが見つからない場合は、`LD_LIBRARY_PATH` に追加します。たとえば、`/home/bouser/.profile` を次のように編集します。

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/lib32
export LD_LIBRARY_PATH
```

7. `LD_LIBRARY_PATH` および `TNS_ADMIN` 内のフォルダがアクセス可能であることを次のように確認します。

```
ls -l $ORACLE_HOME
ls -l $TNS_ADMIN/tnsnames.ora
```

これらのコマンドから「アクセス許可が拒否されました」というエラーが返されなければ問題ありません。もし返された場合は、適切なアクセス許可を付与する必要があります。たとえば、`root/oracle` ユーザは、次のコマンドを実行する必要があります。

```
chmod -R +xr $ORACLE_HOME
```

8. `TNS Ping` ユーティリティを以下のように使用して、`Oracle` 接続が有効であることを確認します。

```
$ORACLE_HOME/bin/tnsping service_name
```

`TNS Ping` からの出力は、以下の例のようになります。

```
TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008
09:17:02
Copyright (c) 1997, 2005, Oracle. All rights reserved.
使用されるパラメータ ファイル
/opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlnet.ora
別名を解決するために使用される TNSNAMES アダプタ
問合わせ中 (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST =
172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = service_name)))
OK (30 msec)
```

これで `CA Business Intelligence` を `Linux` にインストールできます。

レポート パッケージのデプロイ

レポート パッケージは、BIAR ファイルで、これによって CA ControlMinder の標準レポートがデプロイされます。 レポート パッケージには、レポート ポータル上でのデプロイに使用するアーティファクトおよびディスクリプタの集合体が含まれています。 これらの標準レポートを使用するには、レポート パッケージ ファイルを BusinessObjects InfoView にインポートする必要があります。

注: このパッケージは、レポート ポータルの旧バージョンと下位互換性があります。 最新のレポート パッケージを利用するためにレポート ポータルをアップグレードする必要はありません。 また、ローカライズされたレポート パッケージをデプロイできます。 これは、横に並んだ、別々の .biar ファイルとして提供されます。

レポート ポータルでのレポート パッケージのデプロイ

標準の CA ControlMinder レポートを使用するには、レポート パッケージ ファイルを BusinessObjects InfoView にインポートします。

注: この手順では、レポート ポータル上に、同じパッケージの旧バージョンがすでにデプロイされていない場合に、レポート パッケージをデプロイする方法について説明します。

以下の手順に従います。

1. 中央データベース、配布サーバ、レポート ポータルが設定されていることを確認します。

注: JAVA_HOME 変数がレポート ポータル コンピュータ上でセットアップされていることを確認します。

2. CA Business Intelligence for Windows DVD を光ディスク ドライブに挿入し、¥Disk1¥cabi¥biconfig フォルダに移動します。
3. biconfig ディレクトリの中身を一時ディレクトリにコピーします。
4. お使いのオペレーティング システム用の適切な CA ControlMinder サーバコンポーネント DVD を光ディスク ドライブに挿入し、¥ReportPackages フォルダにアクセスします。

5. 以下のファイルを、光ディスク ドライブから同一一時ディレクトリにコピーします。

- `¥ReportPackages¥RDBMS¥import_biar_config.xml`
- `¥ReportPackages¥RDBMS¥AC_BIAR_File.biar`

RDBMS

CA ControlMinder レポートで使用される RDBMS のタイプを定義します。

値：Oracle、MSSQL2005

import_biar_config.xml

使用する RDBMS のインポート構成ファイル (.xml) の名前を定義します。

値：import_biar_config_oracle10g.xml、
import_biar_config_oracle11g.xml、import_biar_config_mssql_2005.xml

注：中央データベースとして MS SQL Server 2008 を使用する場合は、import_biar_config_mssql_2005.xml ファイルを設定します。

AC_BIAR_File.biar

使用する言語と RDBMS の CA ControlMinder レポート ファイル (.biar) の名前を定義します。

注：使用する RDBMS 用のインポート設定ファイルの <biar-file name> プロパティは、このファイルを指します。デフォルトでは、RDBMS の英語バージョンの名前に設定されます。

6. `import_biar_config.xml` ファイルのコピーを編集します。以下の XML プロパティを定義します。

<biar-file name>

CA ControlMinder レポート ファイル (.biar) への完全なパス名を定義します。ファイルは前の手順でコピーしました。

<networklayer>

使用する RDBMS でサポートされているネットワーク層を定義します。

値 (Windows)：

- OLE DB -- MS SQL Server 認証モードの場合
- Oracle OCI
- ODBC -- Windows 認証モードの場合

<rdms>

CA ControlMinder レポートで使用される RDBMS のタイプを定義します。

値 (Oracle OCI) : Oracle 10 または Oracle 11

値 (ODBC) : 一般的な ODBC データソース

値 (OLE DB) : MS SQL Server 2005、MS SQL Server 2008、または Oracle 10 か Oracle 11 以外の任意の値

注: このプロパティに指定できる値の詳細については、CA Business Intelligence のドキュメントを参照してください。

<username>

エンタープライズ管理用に中央データベースを準備した際に作成した RDBMS 管理者ユーザのユーザ名を定義します。

<password>

エンタープライズ管理用に中央データベースを準備した際に作成した RDBMS 管理者ユーザのパスワードを定義します。

<datasource>

以下のいずれかを定義します。

- (Oracle) データベースの名前
- (SQL Server 2005 または 2008) 作成したデータベース
- (ODBC) 作成した DSN

重要: CA Business Intelligence CMS ではなく、CA ControlMinder によってレポート用に使用されるデータベースの名前を指定します。

<server>

SQL Server 2005 または 2008 コンピュータの名前を定義します。
Oracle Database 10g、11g、および ODBC では、この値を空のままにします。

7. 以下を実行します。

- コマンドプロンプトを開き、以下のコマンドを入力します。

```
System_Drive:¥B0¥biconfig.bat -h host_name -u user_name -p password -f  
ac_biar_config.xml
```

host_name

レポート ポータルのホスト名を定義します。

user_name

レポート ポータルをインストールした時に設定したレポート ポータル管理者を定義します。

パスワード

レポート ポータル管理者のパスワードを定義します。

以下に例を示します。

```
biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f  
C:\¥B0¥import_biar_config_oracle11g.xml
```

- (UNIX) 以下のとおり、スクリプト ファイル `biconfig.sh` に実行許可を設定し、実行します。

```
temp_dir/biconfig.sh -h host_name -u user_name -p password -f  
ac_biar_config.xml
```

以下に例を示します。

```
biconfig.sh -h reportportal.comp.com -u Administrator -p P@ssw0rd -f  
/tmp/rp/import_biar_config_orcl.xml
```

バッチ ファイルによって **CA ControlMinder** レポートが **InfoView** にインポートされます。インポートは、完了するまで数分かかる場合があります。バッチ ファイルと同じフォルダにログ ファイル (`biconfig.log`) が作成され、インポートが成功したかどうかを示します。

例: Oracle Database 11g インポート設定ファイルのサンプル

以下のコードは、Oracle Database 11g 用に編集されたインポート設定ファイル (`import_biar_config_oracle11g.xml`) の例です。

```
<?xml version="1.0"?>  
<biconfig version="1.0">  
  <<step priority="1">  
    <<<add>  
      <<<<<biar-file name="c:\¥temp¥AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">  
        <<<<<<networklayer>Oracle OCI</networklayer>  
        <<<<<<rdms>Oracle 11</rdms>  
        <<<<<<username>root</username>  
        <<<<<<password>P@ssw0rd</password>  
        <<<<<<datasource>orcl</datasource>  
        <<<<<<server></server>  
      <<<<<</biar-file>  
    <<<</add>  
  <<</step>  
</biconfig>
```

例: Microsoft SQL Server 2005 インポート設定ファイルのサンプル

以下のコードは、MS SQL Server 2005 用に編集されたインポート設定ファイル (import_biar_config_mssql2005.xml) の例です。

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:\temp\AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
        <networklayer>OLE DB</networklayer>
        <rdms>MS SQL Server 2005</rdms>
        <username>dbAdmin</username>
        <password>P@ssw0rd</password>
        <datasource>r125db</datasource>
        <server>rdbms.org</server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

詳細情報:

[レポート作成のための Windows エンドポイントの設定 \(P. 206\)](#)

[レポート作成のための UNIX エンドポイントの設定 \(P. 312\)](#)

大規模デプロイに対する BusinessObjects の設定

大規模デプロイで CA ControlMinder レポートを実行するには、BusinessObjects のデフォルト設定を変更する必要があります。BusinessObjects ページサーバで作成できる同時接続の最大数を変更します (デフォルトは 20,000)。また、入力パラメータ選択リストに表示される値の最大数も変更します。

大規模デプロイに対して BusinessObjects を設定する方法

1. BusinessObjects ページサーバで作成可能な同時接続数を変更します。
 - a. レポート ポータルのコンピュータ上で、[スタート] - [プログラム] - [Crystal Enterprise] - [Crystal Configuration Manager (CCM)] をクリックします。

BusinessObjects Configuration Manager が開きます。
 - b. [Crystal Page Server] を右クリックし、[停止] を選択します。

- c. [Crystal Page Server] を右クリックし、[プロパティ] を選択します。
 - d. 実行ファイルへのパスを示すフィールドで、**-restart** の後ろに以下のテキストが表示されていることを確認します。

```
-maxDBResultRecords 0
```
 - e. BusinessObjects ページサーバを再起動します。
2. レポート用の入力パラメータ選択リストに表示される値の最大数を変更します。
- a. Windows レジストリ エディタを開きます。
 - b. 以下のレジストリ キーに移動します。

```
HKEY_CURRENT_USER\Software\Business Objects\Suite  
12.0\CrystalReports\DatabaseOptions
```
 - c. [編集] - [新規] - [DWORD 値] をクリックします。
REG_DWORD タイプの新しいレジストリ エントリが表示されます。
 - d. このエントリの名前を「**QPMMaxLOVSize**」に変更します。
 - e. エントリをダブルクリックして、値データを「**1000**」に変更します。
新しいレジストリ エントリが設定されます。
 - f. BusinessObjects Central Management Console (CMC) を開きます。
 - g. [Servers management area] 領域に移動します。
 - h. 設定を変更する Web Intelligence Report Server へのリンクをクリックします。
[Property] タブ内で [Web Intelligence Report Server] ページが開きます。
 - i. 以下の値を 1000 を超える値に、または必要数に変更します。
 - [List of Values Batch Size]
 - [Maximum Size of List of Values for Custom Sorting][Apply] をクリックして変更をサブミットし、変更がただちに有効になるようにサーバを再起動します。

CA Business Intelligence への接続を設定します。

CA ControlMinder エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ (CA ControlMinder レポート ポータル) を使用して、レポート機能を提供します。 レポート ポータルをインストールし、レポートを展開した後に、CA ControlMinder エンタープライズ管理 から CA Business Intelligence への接続を設定する必要があります。この接続を設定するには CA IdentityMinder 管理コンソールを使用します。

CA Business Intelligence への接続の設定方法

1. [CA IdentityMinder 管理コンソールを有効にします](#) (P. 104)。
2. [CA IdentityMinder 管理コンソールを開きます](#) (P. 105)。
3. [環境] - [ac-env] - [詳細設定] - [レポート] をクリックします。
[レポート プロパティ] ウィンドウが表示されます。
4. データベースおよび Business Objects のプロパティを入力します。

重要: CA Business Intelligence Central Management Server (CMS) は内部管理目的のみに使用され、レポートの生成と表示に使用されるレポートデータは含まれていません。CMS の詳細については、「*CA Business Intelligence インストールガイド*」を参照してください。

注: 詳細については、CA IdentityMinder 管理コンソールのオンラインヘルプをご覧ください。オンラインヘルプは、アプリケーションからアクセスできます。

重要: Business Objects のポート フィールドで、レポート ポータルが使用するポート番号を入力します。デフォルトのポートは **8080** です。
Business Objects レポート フォルダ フィールドで、「CA ControlMinderr12」と入力します。

5. [Save] をクリックします。

CA Business Intelligence 設定が保存されます。

注: CA Business Intelligence の詳細については、[CA Technologies サポート](#) から入手可能な「*CA Business Intelligence インストールガイド*」を参照してください。

スナップショット定義の作成

レポートは、CA ControlMinder および UNAB エンドポイントから収集されて中央データベースに格納されるデータ スナップショット、CA ControlMinder エンタープライズ管理 からの SAM データ、ユーザ ストアからデータに基づいて生成されます。

CA ControlMinder レポートを実行および表示するには、スナップショット定義を作成し、スナップショット データをキャプチャする必要があります。スナップショット定義には、CA ControlMinder が収集するレポート データおよびデータ収集のスケジュールを指定します。

スナップショット パラメータ XML ファイルは、CA ControlMinder が収集するレポート データを指定します。デフォルトでは、このファイルで、すべての CA ControlMinder および UNAB エンドポイント、SAM データ、およびユーザ ストアからのデータをレポート スナップショットに含めるように指定します。スナップショット パラメータ XML ファイルをカスタマイズして、レポート スナップショットの範囲を制限できます。

レポートに常に最新のデータが含まれるようにするには、エンドポイントのスナップショットより頻繁にスナップショットが実行されることのないようにスケジュールを設定します。たとえば、エンドポイントで毎週スナップショットが送信されるように設定し、CA ControlMinder エンタープライズ管理 で毎日スナップショットがキャプチャされるように設定した場合、レポート データはエンドポイントから週に一度収集されますが、SAM およびユーザ ストアからは毎日取得されるため、古いエンドポイント データがレポートに含まれることになります。

重要: 複数のスナップショット定義を有効にしないでください。複数のスナップショット定義が有効に設定されている場合、CA ControlMinder エンタープライズ管理 ではすべてのレポートを正常に実行できません。

注: デフォルトでは、スナップショット定義を作成するには「システム マネージャ」ロールが必要です。

以下の手順に従います。

1. CA ControlMinder エンタープライズ管理 で、以下の手順を実行します。
 - a. [レポート] をクリックします。
 - b. [タスク] サブタブをクリックします。
 - c. 左側のタスク メニューで [スナップショット定義の管理] ツリーを展開します。
[スナップショット定義の作成] タスクが使用可能なタスク リストに表示されます。
2. [スナップショット定義の作成] をクリックします。
[スナップショット定義の作成：スナップショット定義の選択] ページが表示されます。
3. [OK] をクリックします。
[スナップショット定義の作成] ページが表示されます。
4. [プロファイル] タブで以下のフィールドに入力します。

スナップショット定義名

スナップショット定義の名前を定義します。

スナップショット定義の説明

スナップショット定義を説明する追加情報を指定します。

有効

CA ControlMinder エンタープライズ管理 がスナップショット定義を有効にするかどうかを指定します。

注: このチェック ボックスを選択しない場合、CA ControlMinder エンタープライズ管理 でスナップショットはキャプチャされず、レポートを表示できません。一度に有効にできるスナップショットは1つのみです。

識別子

レポート スナップショットの範囲を定義するスナップショットパラメータ XML ファイルを指定します。

オプション：

- HOST_PROTECTION.XML -- CA ControlMinder エンドポイントからレポートデータを収集します。
- HOST_PROTECTION_SAM_LDAP.XML -- LDAP ユーザストアを使用する CA ControlMinder および SAM エンドポイントからレポートデータを収集します。
- HOST_PROTECTION_SAM_RDB.XML -- CA ControlMinder および SAM エンドポイントからレポートデータを収集します。
- HOST_PROTECTION_SAM_UNAB_LDAP.XML -- LDAP ユーザストアを使用する CA ControlMinder、UNAB、および SAM エンドポイントからレポートデータを収集します。
- HOST_PROTECTION_UNAB_LDAP.XML -- UNAB エンドポイントからレポートデータを収集します。
- SAM_LDAP.XML -- LDAP ユーザストアを使用する SAM エンドポイントからレポートデータを収集します。
- SAM_RDB.XML -- SAM エンドポイントからレポートデータを収集します。

過去の保存件数

中央データベースに格納される正常なスナップショットの数を指定します。データベース内のスナップショットの数が指定した数に達すると、CA ControlMinder は古いスナップショットを削除します。

注：スナップショットの数は 0 より大きい数値にする必要があります。このフィールドの値を指定しない場合、CA ControlMinder に格納されるスナップショットの数に制限はありません。最大 3 つの正常なスナップショットを格納するよう設定することをお勧めします。

5. [繰り返し] タブをクリックし、[スケジュール] を選択します。
スケジュール オプションが表示されます。

6. スナップショットの実行時間および繰り返しのパターンを指定し、
[サブミット] をクリックします。

注: スナップショットの実行頻度は、CA ControlMinder および UNAB スナップショットの実行頻度より低くスケジュールすることをお勧めします。

スケジュールされた時間および頻度でスナップショットがキャプチャされるよう CA ControlMinder が設定されます。

注: スナップショット定義を作成した後に、オンデマンドでスナップショットをキャプチャするか、スケジュールされた時間と頻度でスナップショットをキャプチャするか選択できます。スナップショットデータのキャプチャの詳細については、「エンタープライズ管理ガイド」を参照してください。

レポート スナップショットのスコープの制限

CA ControlMinder エンタープライズ管理 がレポート スナップショットをキャプチャする場合、CA ControlMinder および UNAB エンドポイントのスナップショットからデータを収集します。また、CA ControlMinder エンタープライズ管理 から SAM データ、ユーザ ストアからデータを収集します。CA ControlMinder エンタープライズ管理 はレポート データを収集した後で、中央データベースにデータを格納します。

スナップショット パラメータ XML ファイルは、CA ControlMinder エンタープライズ管理 が収集するレポート データを指定します。スナップショット パラメータ XML ファイルのカスタマイズによりレポート スナップショットのスコープを制限できます。

たとえば、ユーザ ストアとして Active Directory を使用する場合、CA ControlMinder エンタープライズ管理 はレポート スナップショットをキャプチャするとき、各 Active Directory ユーザのデータを収集します。この処理には時間がかかる場合があります。スナップショットのキャプチャに要する時間を削減するため、スナップショット パラメータ XML ファイルのカスタマイズにより Active Directory スナップショットのスコープを制限できます。

レポート スナップショットのスコープを制限する方法

1. 以下のディレクトリに移動します。ここで *JBoss_HOME* は、JBoss をインストールしたディレクトリです。

```
JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/  
config/imreexport/sample
```

2. PPM_ALL.xml ファイルをコピーして名前を変更し、同じディレクトリに保存します。

これで、新しいスナップショット パラメータ XML ファイルが作成されます。

3. 編集可能な形式で新しいスナップショット パラメータ XML ファイルを開きます。
4. <!--IM COLLECTORS--> セクションのエントリを編集し、ユーザストアから CA ControlMinder エンタープライズ管理 が収集するデータのスコープを指定します。
5. <!--PUPM COLLECTORS--> セクション内で、レポート スナップショットに含めない CA ControlMinder エンタープライズ管理 コンポーネントに該当するエントリを、(!--) および (--) でコメントアウトします。
6. (オプション) Active Directory スナップショットのスコープを制限します。
 - a. 「[LDAP クエリでレポート スナップショットを制限するしくみ \(P. 153\)](#)」および「[LDAP 構文の考慮事項 \(P. 154\)](#)」のトピックを確認します。

これらのトピックの情報は、LDAP クエリを以下の手順で正確に定義する際に役立ちます。

- b. <!--PUPM COLLECTORS--> セクションで、以下のエレメントを検索します。

```
<export object="com.ca.ppm.export.ADUsersCollector">  
</export>
```

このエレメントは、スナップショットに含める Active Directory ユーザ データを指定します。

- c. エlementを以下のように編集します。*ldap_query* は、データを収集するユーザを定義する LDAP クエリを指定します。

```
<export object="com.ca.ppm.export.ADUsersCollector">
  <where attr="%USER" satisfy="ANY">
    <value op="EQUALS">(ldap_query)</value>
  </where>
</export>
```

- d. <!--PUPM COLLECTORS--> セクションで、以下のElementを検索します。

```
<export object="com.ca.ppm.export.ADGroupsCollector">
</export>
```

- e. Elementを以下のように編集します。*ldap_query* は、データを収集するグループを定義する LDAP クエリを指定します。

```
<export object="com.ca.ppm.export.ADGroupsCollector">
  <where attr="%USER" satisfy="ANY">
    <value op="EQUALS">(ldap_query)</value>
  </where>
</export>
```

Active Directory スナップショットのスコープが制限されました。

7. 新しいスナップショットパラメータ XML ファイルを保存し、閉じます。
8. 新しいスナップショットパラメータ XML ファイルを使用するために、CA ControlMinder エンタープライズ管理 のスナップショット定義を変更します。

キャプチャ スナップショット タスクを実行すると、スナップショットパラメータ XML ファイルで指定したデータのみ収集します。

例: レポート スナップショットのスコープを CA ControlMinder エンドポイントに制限

SAM および UNAB を使用しない場合、CA ControlMinder エンドポイントからのみデータを収集するよう、レポート スナップショットのスコープを制限できます。データ収集のスコープを CA ControlMinder エンドポイントに制限するには、`<!-- PUPM COLLECTORS -->` セクション内の `ReportIdMarkerCollector` エントリ 以外のすべてのエントリに `(!-- )` および `(--)` をコメントします。

以下は、`PPM_ALL.xml` ファイルのスニペットです。 `ReportIdMarkerCollector` エントリを除く、`<!-- PUPM COLLECTORS -->` セクションのすべてのエントリがコメントに変更されています。

```
<!-- PUPM COLLECTORS -->
  <!-- export object="com.ca.ppm.export.AccountPasswordCollector">
    </export -->

  <!-- export object="com.ca.ppm.export.PPMRolesCollector">
    <exportattr attr="|rolemembers|" />
  </export -->

  <!-- export object="com.ca.ppm.export.
    PrivilegedAccountExceptionCollector">
  </export -->

  <!-- export object="com.ca.ppm.export.PPMPasswordPolicyCollector">
  </export -->

  <!-- export object="com.ca.ppm.export.ADUsersCollector">
  </export -->

  <export object="com.ca.ppm.export.PPMAccountUserAccessCollector">
  </export -- !>

  <!-- export object="com.ca.ppm.export.ADGroupsCollector">
    <exportattr attr="|groupmembers|" />
  </export -->

  <export object="com.ca.ppm.export.ReportIdMarkerCollector">
  </export>
```

スナップショット パラメータ XML ファイル構文 -- レポート スナップショットの制限

スナップショット パラメータ XML ファイルは、CA ControlMinder エンタープライズ管理 が収集するレポート データを指定します。スナップショット パラメータ XML ファイルを編集して、レポート スナップショットの範囲を制限できます。

CA ControlMinder エンタープライズ管理 が収集するレポート データは、ユーザがスナップショット パラメータ XML ファイルで定義する条件を満たしたオブジェクトのもののみです。ファイル内の各コレクタによって、CA ControlMinder エンタープライズ管理 が収集するオブジェクトセットを定義します。

各コレクタの構造は以下のようになっています。

```
<export object=" ">
  <where attr=" " satisfy=" ">
    <value> </value>
  </where>
  <exportattr attr=" " />
</export>
```

注: <where>、<value>、<exportattr> エレメントはオプションです。

各コレクタには、以下のエレメントが含まれています。

<export>

CA ControlMinder エンタープライズ管理 が収集するオブジェクト データを示します。たとえば、<export> エレメントは、CA ControlMinder エンタープライズ管理 がユーザ データを収集することを指定する場合があります。

<export> エレメントには 1 つ以上の <exportattr> および <where> エレメントを含めることができます。これによって、一定の条件を満たすデータのみを収集できます。<exportattr> または <where> エレメントをまったく指定しない場合、CA ControlMinder エンタープライズ管理 はオブジェクトのすべてのデータを収集します。

<export> エレメントには object パラメータしかありません。

<where>

<value> エレメントで定義された条件に基づいて、収集されたデータをフィルタします。 <where> エレメントには 1 つ以上の <value> エレメントが必要です。また、複数の <where> エレメントを指定して、フィルタを絞り込むことができます（エレメントは OR エレメントとして機能します）。

以下の表では、<where> エレメントのパラメータについて説明します。

パラメータ	説明
attr	フィルタに使用する属性を示します。
satisfy	収集するオブジェクトまたは属性について、値の評価の一部または全部を満たす必要があるかどうかを示します。 ■ ALL - 属性またはオブジェクトは値の評価のすべてを満たす必要があります。 ■ ANY - 属性またはオブジェクトは 1 つ以上の値の評価を満たす必要があります。

<value>

<where> エレメントで、収集される属性またはオブジェクトが満たす必要がある条件を定義します。 <value> エレメントには operator (op) パラメータが必要です。operator には EQUALS または CONTAINS を指定します。

注: スナップショット パラメータ XML ファイルの <!--PUPM COLLECTORS--> セクションで、<value> エレメントに LDAP 構文を使用できます。LDAP 構文によって、CA ControlMinder エンタープライズ管理が Active Directory から収集する ユーザおよびグループのデータを指定できます。

<exportattr>

収集する特定の属性を示します。 <exportattr> エレメントを使用して、収集するオブジェクトの属性のサブセットを収集します。たとえば、ユーザの ID のみを収集する場合、<exportattr> エレメントを使用できます。

<exportattr> エレメントには attr パラメータがあります。

以下の表は、<where> エlementまたは<exportattr> Elementで使用できる属性を、オブジェクトごとに示しています。

オブジェクト	<where> Elementで使用できる属性	<exportattr> Elementで使用できる属性
role	name 属性を使ってフィルタリングできます。 name - フィルタ基準を満たす名前が付けられたロール	以下の属性のいずれかを収集できます。 ■ tasks - ロールに関連付けられているすべてのタスク ■ rules - ロールに適用されるすべてのメンバ、管理、所有者、およびスコープルール ■ users - ロールのすべてのメンバ、管理者、および所有者 ■ rolemembers - すべてのロールメンバ ■ roleadmins - すべてのロール管理者 ■ roleowners - すべてのロール所有者
ユーザ	汎用属性またはフィジカルアトリビュート、および以下の属性のいずれか。 ■ groups - グループのメンバ ■ roles - ロールのメンバ ■ orgs - フィルタ基準を満たす組織にプロファイルが存在するユーザ	以下の属性のいずれかを収集できます。 ■ all_attributes - すべての使用可能なユーザ属性 ■ groups - ユーザがメンバまたは管理者であるすべてのグループ ■ roles - ユーザがメンバ、管理者、または所有者であるすべてのロール

オブジェクト	<where> エlementで使用できる属性	<exportattr> Elementで使用できる属性
group	汎用属性またはフィジカルアトリビュート、あるいは以下の属性。 groups - フィルタ基準を満たすグループ内の、ネストされたグループのリスト	汎用属性または物理属性、あるいは以下の属性のいずれかを収集できます。 ■ all_attributes - ディレクトリ設定ファイル (directory.xml) で Group オブジェクトに定義されたすべての属性 ■ groups - グループ内のすべてのネストされたグループ ■ users - グループのすべてのメンバ ■ groupadmins - 指定したグループの管理者であるすべてのユーザ ■ groupmembers - 指定したグループのメンバであるすべてのユーザ ■ users - すべてのグループ管理者とグループメンバ
organization	汎用属性またはフィジカルアトリビュート	汎用属性または物理属性、あるいは以下の属性のいずれかを収集できます。 ■ all_attributes - ディレクトリ設定ファイル (directory.xml) で Organization オブジェクトに定義されたすべての属性 ■ orgs - 組織内のすべてのネストされた組織 ■ groups - 組織内のすべてのグループ ■ users - 組織内のすべてのユーザ

レポート スナップショットで LDAP クエリがユーザおよびグループ データを制限する仕組み

Active Directory をユーザ ストアとして使用する場合、レポート スナップショットでキャプチャされたユーザおよびグループ データを指定できます。

ユーザ別またはグループ別に Active Directory データをフィルタリングするスナップショット パラメータ XML ファイルで LDAP クエリを使用できます。ただし、ロール メンバシップ別に Active Directory データをフィルタリングする LDAP クエリは使用できません。LDAP クエリを使用できるのは、スナップショット パラメータ XML ファイルの <!--PUPM COLLECTORS--> のみです。

以下のプロセスでは、スナップショット パラメータ XML ファイル内の LDAP クエリが、CA ControlMinder エンタープライズ管理 が収集する Active Directory データをどのように制限するかについて説明します。この情報によって、レポート スナップショットを制限する、適切な LDAP クエリを記述できます。

CA ControlMinder エンタープライズ管理 が Active Directory レポート スナップショットをキャプチャする際に、以下を行います。

1. 以下のエレメント内の LDAP クエリで指定されている Active Directory ユーザのみのデータを収集します。

```
<export object="com.ca.ppm.export.ADUsersCollector">
```

エレメントに LDAP クエリが含まれていない場合、CA ControlMinder エンタープライズ管理 はすべての Active Directory ユーザのデータをスナップショットに含めます。

2. 以下のエレメント内の LDAP クエリで指定されている Active Directory グループのみのデータを収集します。

```
<export object="com.ca.ppm.export.ADGroupsCollector">
```

エレメントに LDAP クエリが含まれていない場合、CA ControlMinder エンタープライズ管理 はすべての Active Directory グループのデータをスナップショットに含めます。

注: CA ControlMinder エンタープライズ管理 は、ステップ 1 でクエリによって返されなかったユーザのデータは収集しません。ユーザがステップ 2 でクエリによって返されるグループのメンバであるが、ユーザがステップ 1 のクエリによって返されない場合、CA ControlMinder エンタープライズ管理 はそのユーザのデータを Active Directory スナップショットに含めません。

LDAP 構文の考慮事項

Active Directory スナップショットのスコープを制限する LDAP クエリを記述する際に、以下を考慮します。

- LDAP クエリで以下の論理演算子を使用できます。
 - EQUAL TO (=)
 - OR (|)
 - AND (&)
注: 一部の制限は、アンパサンド (&) 文字の使用に適用されます。
 - NOT (!)
 - ワイルドカード (*)
- アンパサンド文字 (&) と左山形かっこ (<) は、以下の状況でのみ使用できます。
 - マークアップ区切り文字として
 - コメント内で
 - 処理命令内で
 - CDATA セクション内で

他の状況でアンパサンド文字を表すには、文字列「&」または Unicode 文字参照を使用します。他の状況で左山形かっこ文字を表すには、文字列「<」または Unicode 文字参照を使用します。

- 右山形かっこ文字 (>) は、CDATA セクションの終わりを示す文字列 (]] >) でのみ使用できます。

他の状況で右山形かっこ文字を表すには、文字列「>」または Unicode 文字参照を使用します。

例: アンパサンド文字

以下のスナップショットパラメータ XML ファイルの一部では、レポートスナップショットに **Active Directory** ユーザデータをすべて含めるように指定しています。この LDAP クエリの一部では、アンパサンドを表すために `&` 文字列を使用しています。

```
<export object ="com.ca.ppm.export.ADUsersCollector">
  <where attr="%USER%" satisfy="ANY">
    <value op="EQUALS">(&(objectClass=user))</value>
  </where>
</export>
```

CA ControlMinder r12.0 でインストールしたレポートポータルへのレポートパッケージのデプロイ

Windows で有効

標準の CA ControlMinder レポートを使用するには、BusinessObjects InfoView にレポートパッケージファイルをインポートする必要があります。

この手順では、レポートパッケージを、CA ControlMinder r12.0 でインストールした既存の CA Business Intelligence 上にデプロイする方法について説明しています。

以下の手順に従います。

1. お使いのオペレーティングシステム用の適切な CA ControlMinder サーバコンポーネント DVD を光ディスクドライブに挿入し、`/ReportPackages` ディレクトリに移動します。
2. インストールファイル用に一時フォルダを作成します。
 - Windows の場合は、`C:¥` ドライブのルートの下に `BO` という名前のフォルダを作成します。

注: このフォルダ内にはおよそ 2GB のメモリが必要となります。
 - Linux の場合は、`directory /work/bo` を作成します。

3. 光ディスクドライブから同じ一時ディレクトリに、以下のファイルをコピーします：

- /ReportPackages/RDBMS/import_biar_config.xml
- /ReportPackages/RDBMS/AC_BIAR_File.biar

RDBMS

使用している RDBMS のタイプを定義します。

値：Oracle、MSSQL2005

import_biar_config.xml

使用する RDBMS のインポート構成ファイル (.xml) の名前を定義します。

値：import_biar_config_oracle10g.xml、
import_biar_config_oracle11g.xml、import_biar_config_mssql_2005.xml

注：中央データベースとして MS SQL Server 2008 を使用する場合は、import_biar_config_mssql_2005.xml ファイルを設定します。

AC_BIAR_File.biar

使用する言語と RDBMS の CA ControlMinder レポート ファイル (.biar) の名前を定義します。

注：使用する RDBMS 用のインポート設定ファイルの <biar-file name> プロパティは、このファイルを指します。デフォルトでは、RDBMS の英語バージョンの名前に設定されます。

4. 使用するプラットフォーム用の CA ControlMinder r12.0 Server Components DVD を光ディスク ドライブに挿入し、/ReportPortal ディレクトリに移動します。

注：この DVD は r12.0 に付属しているメディアの一部です。

5. 以下のいずれかの操作を実行します。
 - Windows の場合、DVD の ¥ReportPortal¥BO ディレクトリの内容を、作成した C:¥BO フォルダにコピーします。
 - Linux の場合、/ReportPortal/bo_install.tar.gz を、作成した /work/bo フォルダに解凍します。
6. DVD の ¥ReportPortal¥BO ディレクトリの内容を、作成した C:¥BO フォルダにコピーします。

7. ターゲットディレクトリを開き、*BO_files/biek-sdk* にアクセスします。
8. *biekInstall.properties* ファイルのコピーを以下のように編集します。

```
BIEK_CONNECT_LAYER=networklayer
BIEK_CONNECT_DB=rdms
BIEK_CONNECT_USER=rdms_adminUserName
BIEK_CONNECT_PASSWORD=rdms_adminUserPass
BIEK_CONNECT_SOURCE=rdms_Datasource
BIEK_CONNECT_SERVER=rdms_hostName
BIEK_BO_USER=InfoView_adminUserName
BIEK_BO_PASSWORD=InfoView_adminUserPass
BIEK_BIAR_FILE=AC_BIAR_File.biar
```

networklayer

使用する RDBMS でサポートされているネットワーク層を定義します。

制限： 大文字と小文字を区別します。

rdms

使用している RDBMS のタイプを定義します。

制限： 大文字と小文字を区別します。

rdms_adminUserName

作成済みの RDBMS 管理ユーザのユーザ名を定義します。

rdms_adminUserPass

作成済みの RDBMS 管理ユーザのパスワードを定義します。

rdms_Datasource

Oracle データベースの Transparent Network Substrate (TNS) の名前を定義します。

rdms_hostName

RDBMS サーバのホスト名を定義します。

InfoView_adminUserName

InfoView 管理ユーザのユーザ名を定義します。デフォルトでは、このユーザは **Administrator** となります。

InfoView_adminUserPass

InfoView 管理ユーザのパスワードを定義します。デフォルトでは、このユーザにパスワードは付与されていません（空のままにします）。

AC_BIAR_File.biar

CA ControlMinder レポート ファイル (.biar) への完全なパス名を定義します。これは以前にコピーしたファイルです。

9. バッチファイル *BO_Files/biek-sdk/importBiarFile.bat* を実行します。

CA ControlMinder レポートが InfoView にインポートされます。インポートは、完了するまで数分かかる場合があります。

第 7 章: エンドポイントの実装の準備

このセクションには、以下のトピックが含まれています。

[保護するポリシー オブジェクトの決定](#) (P. 159)

[権限属性](#) (P. 164)

[警告期間の使用方法](#) (P. 166)

[実装に関するヒント](#) (P. 168)

保護するポリシー オブジェクトの決定

以下のセクションでは、企業のアプリケーションおよびデータへのアクセスを許可するセキュリティ ポリシーによって使用される重要なオブジェクトについて説明します。

ユーザ

CA ControlMinder には、複数のユーザ タイプがあります。ユーザ タイプごとに一定レベルの権限と一定の制限が設定されます。組織のセキュリティ ポリシーを作成する作業には、特別な権限とそれを与えるユーザを決定する作業が含まれます。

CA ControlMinder では、ユーザがログオンできる回数や実行される監査の種類など、ユーザに関する情報を格納します。ユーザに関する情報は、データベース レコードのプロパティに格納されます。

注: ユーザの詳細については、「[エンドポイント管理ガイド](#)」を参照してください。

ユーザ タイプ

CA ControlMinder では以下のタイプのユーザがサポートされ、CA ControlMinder データベース内のリソース管理に使用されます。

一般ユーザ

組織の-社内エンド ユーザ - 組織のビジネスを遂行する人たち。システムに対する一般ユーザのアクセス権は、ネイティブ OS および CA ControlMinder の両方で制限できます。

特別な権限を持つユーザ(サブ管理者)

1 つ以上の特定の管理タスクを実行する権限が与えられた一般ユーザ。一般ユーザに対して特定の管理機能の実行を許可すると、管理者の負荷を軽減できます。CA ControlMinder では、これを「タスクの委任」といいます。

管理者

ネイティブ OS および CA ControlMinder 内で最上位の権限を持つユーザ。管理者は、ユーザの追加、削除、および更新のほか、ほとんどの管理タスクを実行できます。CA ControlMinder では、ネイティブ スーパーユーザの権限を制限できます。そのアカウントが自動的に認識されない特定のユーザに管理タスクを割り当てることができます。これは、どのユーザが管理タスクを実行するかが、侵入者にはただちに明らかにはならないことを意味します。

グループ管理者

ある特定のグループ内で、ユーザの追加、削除、更新など、ほとんどの管理者機能を実行できるユーザ。制限された特定の権限を持つこのユーザ タイプは、ネイティブ Windows にはありません。

パスワード管理者

他のユーザのパスワード設定を変更する権限を持つユーザ。パスワード管理者は、他のユーザの属性は変更できません。このユーザ タイプは、ネイティブ OS にはありません。

グループ パスワード管理者

ある特定のグループ内で、他のユーザのパスワード設定を変更する権限を持つユーザ。グループ パスワード管理者は、グループ内のユーザの、その他の設定を変更することはできません。このユーザ タイプは、ネイティブ OS にはありません。

監査担当者

監査ログの読み取り権限を持つユーザ。ログインやリソースへのアクセスが試みられたときに実行する監査の種類を決定する権限もあります。このユーザタイプは、ネイティブ OS にはありません。

グループ監査担当者

グループに関連する監査ログの読み取り権限を持つユーザ。ある特定のグループ内で行う監査の種類を決定する権限もあります。このユーザタイプは、ネイティブ OS にはありません。

オペレータ

データベース内のすべての情報の表示（読み取り）、CA ControlMinder トレースの管理など、secons ユーティリティを使用したタスクの実行、および実行時統計情報の表示が可能なユーザ。このユーザタイプは、ネイティブ OS にはありません。

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

グループオペレータ

データベースの、自分が定義されているグループに関するすべての情報を表示できるユーザ。このユーザタイプは、ネイティブ OS にはありません。

Server

実際にはプロセスである特別なタイプのユーザ。他のユーザの権限をリクエストすることが許可されています。

セキュリティ ポリシーとユーザ

実装を準備する際に、決定する必要のある項目。

- 定義済みユーザに付与する特殊な権限（存在する場合）
- 定義済みユーザに許可する、グローバル権限属性およびグループ権限属性

たとえば、システム管理者、パスワード管理者、グループ パスワード管理者、監査担当者、オペレータとして定義するユーザを決定する必要があります。

グループ

グループは、通常、同一のアクセス権限を共有するユーザの集合です。管理者は、グループへのユーザの追加、グループからのユーザの削除、およびシステム リソースへのアクセスをグループ単位で許可または拒否することができます。このタイプのグループは、ネイティブ OS および CA ControlMinder の両方に存在します。

グループ レコードには、グループに関する情報が格納されます。グループ レコードに格納される最も重要な情報は、グループのメンバであるユーザのリストです。

重要: グループ レコードのアクセス権限ルールは、グループの階層内の各ユーザに繰り返し適用されます。

たとえば、グループ A には、ユーザ X とグループ B という 2 つのメンバがあります。ユーザ Y はグループ B のメンバです。ユーザがグループ A の権限ルールを変更する場合、CA Access Control は変更された権限ルールをグループ A 階層内のすべてのユーザおよびグループ、すなわち、ユーザ X、グループ B、ユーザ Y に適用します。

グループ レコードの情報はプロパティに格納されます。

CA ControlMinder では、グループ管理者は、グループ管理者が定義されている特定のグループのグループ機能を管理できます。グループ パスワード管理者は、グループ メンバのパスワードを変更できます。

セキュリティポリシーとグループ

組織のセキュリティ ポリシーを作成する際は、以下のことを決定する必要があります。

- セキュリティ管理を目的として作成するグループ
- 各グループに追加するユーザ
- グループ管理者とグループ パスワード管理者を定義するかどうか、定義する場合はこれらの管理者の役割を割り当てるユーザ

事前定義されたユーザのグループ

CA ControlMinder には事前定義されたグループがあり、そのグループにユーザを追加することができます。このようなグループの 1 つが、`_restricted` グループです。`_restricted` グループのユーザのファイルとレジストリ キーは、すべて CA ControlMinder によって保護されます。ファイルまたはレジストリ キーのアクセス ルールが明示的に定義されていない場合は、そのクラス (FILE または REGKEY) の `_default` レコードがアクセス権に適用されます。

`_restricted` グループを使用する場合は、注意が必要です。`_restricted` グループ内のユーザは、業務の遂行に必要な十分な権限を与えられていない場合があります。このため、ユーザを `_restricted` グループに追加する場合は、最初に警告モードの使用を検討してください。Warning モードでは、ユーザが業務を遂行するために必要なファイルおよびレジストリ キーを監査ログによって知ることができます。監査ログの確認後、適切な権限を付与し、Warning モードをオフに切り替えます。

リソース アクセス用に事前定義されたグループ

CA ControlMinder に事前定義されている他のタイプのグループは、特定のリソースに対するアクセスの許可または禁止を定義します。以下のグループが事前定義されています。

■ `_network`

(Windows のみ) `_network` グループでは、ネットワークから特定のリソースへのアクセスが定義されます。すべてのユーザは、このグループのメンバとして扱われます。つまり、ユーザをこのグループに明示的に追加する必要はありません。

たとえば、特定のリソースの読み込みをネットワークからのみに限定できます。`selang` のコマンドを使用して、以下のように新規リソースを定義します。

```
newres FILE c:¥temp¥readonly defaccess(none)
```

次に、ネットワークから可能なアクセスを指定します。

```
authorize FILE c:¥temp¥readonly gid(_network) access(read)
```

この指定は、CA ControlMinder エンドポイント管理 を使用して行うこともできます。

これで、ネットワークから `c:¥temp¥readonly` にアクセスする際に、ユーザはネットワークからのみファイルを読み取れます。

- **_interactive**

_interactive グループは、特定のリソースが存在するコンピュータから、そのリソースに対するアクセス許可を定義します。たとえば、ファイルに対する読み取りアクセス権を与える場合、このリソースに対してネットワークからのアクセスが許可されていない場合でも、ファイルが定義されているコンピュータからのアクセス権を与えることができます。

以下の点に注意してください。

- **CA ControlMinder** では、**_network** グループと **_interactive** グループの間に関係はありません。これは、ネットワークから特定のリソースへのアクセスを定義するルールが、**_network** グループに存在し、同時に、**_interactive** グループ内の他のルールで、同じリソースに対するアクセスを定義できる、ということを意味します。
- **_network** グループと **_interactive** グループにユーザを追加する必要はありません。
- これらのグループによって、データベースに定義されているすべての **Windows** リソースを保護できます。

権限属性

権限属性は、データベース内のユーザレコードに設定するプロパティです。権限属性によって、一般ユーザが実行できない操作をユーザに許可します。権限属性には、**グローバル**と**グループ**の2種類があります。各グローバル権限属性によって、ユーザはデータベース内のレコードに対して特定の種類の機能を実行できます。グループ権限属性によって、ユーザは指定した1つのグループ内で、特定の種類の機能を実行できます。グローバル権限属性とグループ権限属性の機能と制限については、以下のセクションで説明します。

グローバル権限属性

自分のユーザ レコードにグローバル権限属性が設定されているユーザは、データベース内の関連するレコードに対して特別な機能を実行できます。グローバル権限属性は、以下のとおりです。

- ADMIN
- AUDITOR
- OPERATOR
- PWMANAGER
- SERVER
- IGN_HOL

注: グローバル認証属性の詳細については、「[エンドポイント管理ガイド](#)」を参照してください。

グループ権限属性

自分のユーザ レコードに *グループ権限属性*が設定されているユーザは、指定されたグループ内で特別な機能を実行できます。グループ権限属性は、以下のとおりです。

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

注: グループ認証属性の詳細については、「[エンドポイント管理ガイド](#)」を参照してください。

警告期間の使用方法

実装チームは、保護する対象を決定するほか、新しいセキュリティ コントロールを導入する方法を考える必要があります。現在進行中の業務への影響を最小限に抑えるには、アクセス制約を適用するのではなく、リソースアクセスの監視のみを行う初期期間の実施を考慮する必要があります。

アクセスを監視するには、リソースを警告モードに設定します。リソースまたはクラスに対する警告モードが有効になっていて、ユーザアクセスがアクセス制約に違反したとき、**CA ControlMinder** では監査ログに警告メッセージが記録され、ユーザにリソースへのアクセスが許可されます。

注: 警告モードを使用する場合は、監査ログの最大サイズを増やすことを検討してください。警告モードの詳細については、「**エンドポイント管理ガイド**」を参照してください。

CA ControlMinder バックドア

たとえば、評価展開で初めて CA ControlMinder をインストールする際に、CA ControlMinder データベース内でのルール定義が正しくない場合があります。不正なルールを定義すると、ユーザがログインできなくなったり、コマンドを実行できなくなる場合があります。たとえば、システムディレクトリや Windows レジストリの非常に重要な部分へのアクセスを拒否するルールを誤って定義する場合があります。

CA ControlMinder を停止して、これらの間違いを修正するのは難しいため、CA ControlMinder にはバックドアが用意されていて、これによってこの種の問題を修正できます。バックドアは不正に使用することもできるため、CA ControlMinder では、システムがセットアップされ、安定すると、バックドアを無効にすることもできます。

このバックドアにアクセスするには、コンピュータの起動時に起動メニューから [Windows セーフモード] または [セーフモードとネットワーク] を選択します。これらのオプションのいずれかを選択すると、CA ControlMinder サービスを自動的に開始せずに、システムが開始されます。

このバックドアを無効にするには、レジストリ キー `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\AccessControl` の下にデータ型 `reg_dword` のレジストリ値「LockEE」を定義し、「1」に設定します。

注: このレジストリ値は、デフォルトでは存在しません。

LockEE を「1」に設定して、システムを起動する場合

- セーフモードでは、CA ControlMinder エンジンおよび CA ControlMinder Watchdog のみがロードされます。

CA ControlMinder エージェント（および Policy Model）は、ネットワークサービスに依存するため、ロードされません。

- [セーフモードとネットワーク] では、CA ControlMinder は正常に起動します。

UNIX では、単一ユーザモードで CA ControlMinder を使用することができます。単一ユーザモードを使用する場合は、以下の制限が適用されます。

- `selang` はローカルモード (`selang -l`) のみでサポートされます。
- ネットワーク クラスはサポートされません。
- PMDB 機能は (`selang env pmd` の使用を含め) 動作しません

実装に関するヒント

このセクションでは、CA ControlMinder のインストール後に考慮すべき、実装に関するその他の情報を示します。

セキュリティの種類

サイトのセキュリティは、以下のアプローチのいずれかに従って処理できます。

- 明示的に許可されていないものはすべて禁止する。これは理想的なアプローチですが、実装時に使用することは不可能です。システムで行われることを許可するルールがないため、システムでは、アクセスルールを定義しようとするすべての試みがブロックされます。これは、イグニッションにキーを入れたまま、車から締め出されたような状態です。
- 明示的に禁止されていないものはすべて許可する。このアプローチでは、セキュリティが低下する場合がありますが、セキュリティシステムを実装する上で、実用的な方法です。

CA ControlMinder では、第 2 のアプローチで開始し、アクセスルールが定義された後に、第 1 のアプローチに切り替えます。デフォルトアクセス (defaccess) ルールおよびユニバーサルアクセス (_default) ルールを使用すると、アプローチを定義し、いつでも保護ポリシーを切り替えることができます。

重要: 保護ポリシーを切り替える際に、すべてのユーザを `_restricted` グループに追加する必要がある場合があります。複数の保護ポリシー間での切り替えの際に、パフォーマンスに著しい影響が及ぶ可能性があります。

アクセサ

アクセサとは、リソースにアクセスできるエンティティのことです。最も一般的なアクセサタイプはユーザまたはグループです。つまり、アクセス権限の割り当ておよびチェックの対象となるユーザです。プログラムがリソースにアクセスする際には、プログラムの所有者（ユーザまたはグループ）が「アクセサ」となります。アクセサは、以下の3つのカテゴリに分類されます。

- 特定のユーザ名に関連付けられた要員
- アクセスする権限を持つグループのメンバである要員
- 特定のユーザ ID に関連付けられた運用プロセス

最も一般的なアクセサタイプはユーザです。つまり、ログインを実行でき、アクセス権限の割り当ておよびアクセス権限のチェックを受ける要員です。CA ControlMinder の最も重要な機能の1つは、アカウントビリティです。個々のアクションまたはアクセスの試みは、要求に対して責任を持つユーザの代わりに実行されます。

CA ControlMinder では、ユーザのグループを定義できます。通常、ユーザは、プロジェクト、部、または課別にグループ化されます。ユーザをグループ化することによって、セキュリティ管理に必要な作業量を大幅に削減することができます。

CA ControlMinder エンドポイント管理 または `selang` コマンドを使用して、ユーザやグループの新規定義、および既存のユーザやグループの変更を行うことができます。

リソース

セキュリティ ポリシーで最も重要なことは、保護を必要とするシステムリソースを決定し、リソースに設定する保護の種類を定義することです。

リソース クラスとアクセス ルール

CA ControlMinder は、インストールされた直後に、システム イベントのインターセプト、およびリソースにアクセスするユーザ権限のチェックを開始します。システム リソースに対するアクセスの制限方法と制限対象のリソースを CA ControlMinder に指示するまで、すべての権限チェックはアクセスを許可することになります。

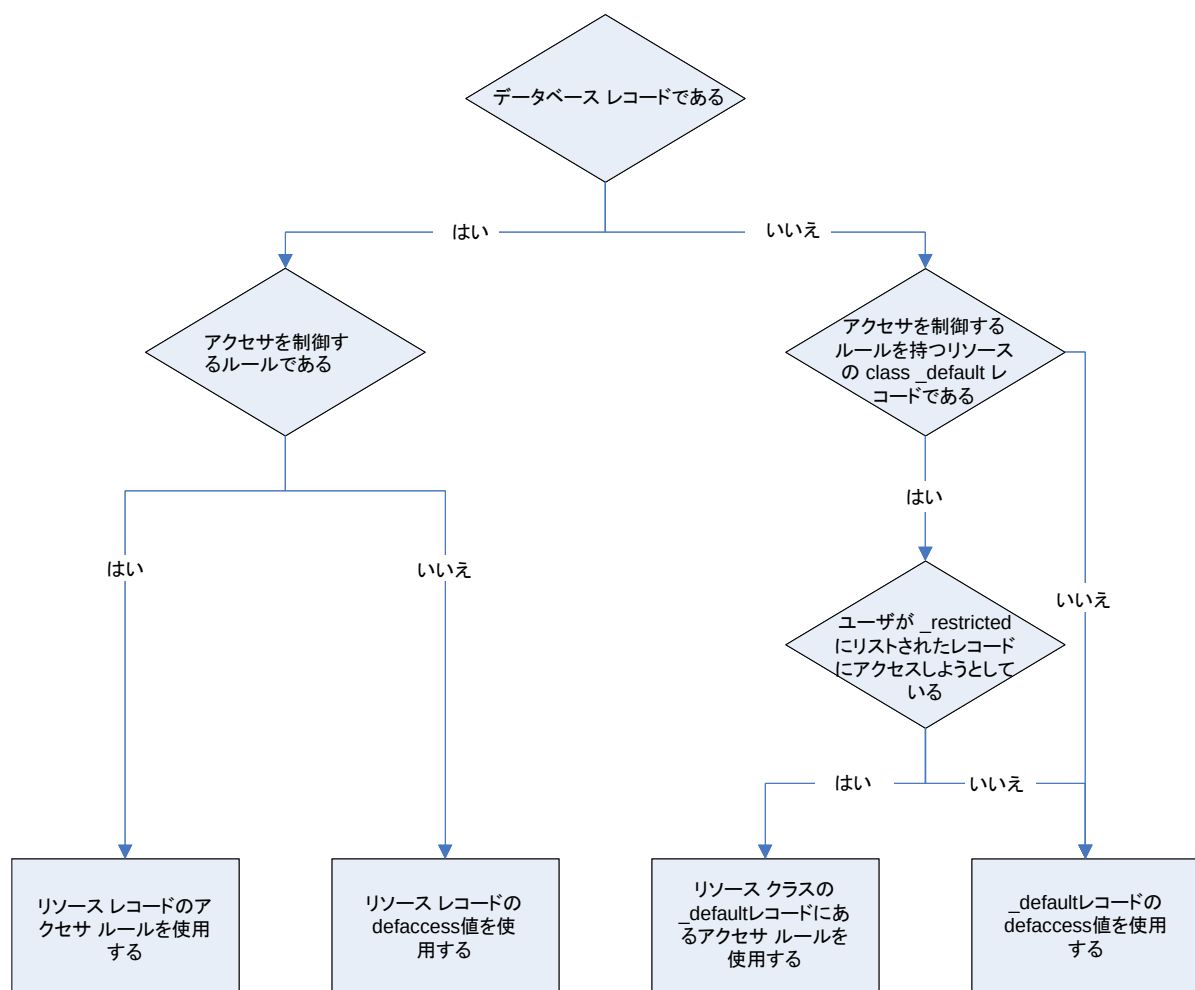
保護対象のリソースのプロパティはリソース レコードに格納され、リソース レコードはクラスに分類されます。リソース レコード内で最も重要な情報は、アクセス ルールです。アクセス ルールは、1 つ以上のリソースを操作する 1 つ以上のアクセサの権限を制御します。アクセス ルールを定義するには、以下のいくつかの方法があります。

- **Access Control List** (リソースへのアクセス権を持つアクセサと、アクセサに実際に与えられるアクセス権を明示したリスト)。 **ACL** ともいいます。
- **Negative Access Control List** (リソースへのアクセスが拒否されるアクセサを明示したリスト)。 **NACL** ともいいます。
- リソースに対するデフォルト アクセス。 **ACL** で明示的に定義されていないアクセサに対してアクセス ルールを指定します。
- ユニバーサル アクセス (クラスの **_default** レコード)。そのクラスの、特定のリソース レコードをまだ持たないリソースに対するアクセス権を指定します。
- プログラム アクセス制御リスト (**PACL**)。特定のプログラムを使用して、特定のアクセサに対するアクセス権を定義します。
- 条件付きアクセス制御リスト (**CACL**)。ある条件に基づいてアクセス権を与えます。たとえば、**TCP** レコードでは、特定のアクセサからの特定のリモート ホストに対するアクセス権を定義できます。
- **Inet ACL**。特定のポート経由の受信ネットワーク アクティビティに対するアクセス権を定義します。

defaccess と _default の使用方法

リソースへのアクセスが要求されると、その要求の処理方法を決定するために、以下の順序でデータベースが検索され、検出された最初のアクセスルールが **CA ControlMinder** によって使用されます。デフォルト アクセス (**defaccess**) と **_default** の違いに注意してください。

1. データベースにリソースのレコードがあり、そのレコードにアクセサを制御するルールが指定されている場合、**CA ControlMinder** はそのルールを使用します
2. データベースにレコードがあり、そのレコードにアクセサを制御するルールが指定されていない場合は、そのレコードのデフォルト アクセスルール (**defaccess** 値) がアクセサに適用されます。
3. レコードが存在せず、リソース クラスの **_default** レコードにアクセサを制御するルールが指定されている場合、**CA ControlMinder** はそのルールを使用します。
4. レコードが存在せず、リソース クラスの **_default** レコードにアクセサを制御するルールが指定されていない場合、**_default** レコードのデフォルト アクセスルール (**defaccess** 値) がアクセサに適用されます。ファイルおよびレジストリ キーについては、この方法を [restricted ユーザ](#) (P. 163) のみに適用します。



注: リソース クラスおよびアクセス ルールの詳細については、「*selang* リファレンス ガイド」を参照してください。

第 8 章: Windows エンドポイントのインストールおよびカスタマイズ

このセクションには、以下のトピックが含まれています。

[はじめに](#) (P. 173)

[Product Explorer によるインストール](#) (P. 178)

[コマンドラインによるインストール](#) (P. 188)

[Windows エンドポイントのアップグレード](#) (P. 201)

[CA ControlMinder の起動および停止](#) (P. 202)

[インストールの確認](#) (P. 205)

[ログイン保護画面の表示](#) (P. 205)

[エンドポイントへの拡張ポリシー管理の設定](#) (P. 206)

[レポート作成のための Windows エンドポイントの設定](#) (P. 206)

[CA ControlMinder のクラスタ環境用へのカスタマイズ](#) (P. 207)

[アンインストールの方法](#) (P. 208)

はじめに

CA ControlMinder をインストールするには、事前に準備要件を満たし、必要な情報を揃えておく必要があります。

インストール方法

以下の方法で、CA ControlMinder Endpoint Components for Windows DVD を使用して CA ControlMinder for Windows をインストールできます。

- **Product Explorer - CA ControlMinder** をインストールするのに最も簡単な方法は、Product Explorer を使用することです。Product Explorer は、グラフィカルなインストールプログラムで、CA ControlMinder の異なるアーキテクチャでのインストールと、ランタイム SDK のインストールが可能です。Product Explorer では、インストールのプロセスが段階的に実行され、各段階で必要な情報を入力するように要求されます。
- **コマンドライン-インストールプログラム**に対するコマンドラインインターフェースを使用すれば、以下のことができます。

- グラフィカルインストールプログラムを実行するためのカスタムデフォルトの設定

コマンドラインからグラフィカルインストールプログラムにデフォルト値を渡すことができます。この方法を使用すれば、希望する事前設定済のデフォルトでインストールプログラムを開くだけでなく、インストールごとにオプションをカスタマイズすることも可能なバッチファイルを作成できます。

- サイレントインストールの実行

コマンドラインでは、グラフィカルインストールプログラムにデフォルト値を単に渡すだけでなく、サイレントモードで CA ControlMinder をインストールすることも可能です。リモートコンピュータにインストールする場合に、この方法を使用します。

- **Unicenter ソフトウェア配信 - Unicenter ソフトウェア配信**を使用して CA ControlMinder を配布するためのパッケージを作成することができます。

ファイアウォール設定

Windows Server 2003 または Windows Server 2008 に CA ControlMinder をインストールする場合、CA ControlMinder は SSL 以外の TCP 接続用にポート 8891 を開きます。また、SSL TCP 接続用にポート 5249 を開きます。このポートが、CA ControlMinder のエージェントとクライアント間の接続のデフォルトのポートとなります。

注: Windows 上で CA ControlMinder が使用するポートの詳細については、「リファレンスガイド」を参照してください。

新規インストール

CA ControlMinder の新しいインスタンスをインストールするときは、以下の点に注意してください。

- 「リリースノート」をお読みください。

このドキュメントでは、サポートされるプラットフォームに関する情報、既知の問題点、考慮事項、および CA ControlMinder をインストールする前に把握しておく必要のあるその他の重要な情報について説明しています。

- CA ControlMinder は、Windows の Administrator または Administrators グループのメンバがインストールする必要があります。
- CA ControlMinder は、ほかの製品のインストールディレクトリとは別の固有のディレクトリにインストールします。
- Microsoft Internet Explorer 6.x または 7.x をインストールしておく必要があります。
- CA ControlMinder では、製品のインストールを完了するのに、Microsoft Visual C++ 2005 Redistributable Package が必要です。

このパッケージが見つからない場合、インストールプログラムはこのパッケージをまずインストールします。

- CA Technologies のライセンス許可の使用

CA Technologies のすべての製品およびオプションを使用するには、CA Technologies ソフトウェアが稼動するネットワーク内の各コンピュータでライセンスファイルの CA.OLF が必要となります。CA ControlMinder の購入時に、この製品を正常にインストールおよび使用するために必要な情報が含まれるライセンス証明書を受け取ります。

エンタープライズライセンスファイルをインストールするには、CA.OLF ファイルを（CA ControlMinder という行を追加して）CA_license ディレクトリ（C:\Program Files\CA\SharedComponents\CA_LIC など）にコピーします。

アップグレードおよび再インストール

CA ControlMinder をアップグレードする場合は、以下の点に注意が必要です。

- 「リリース ノート」をお読みください。

このドキュメントでは、サポートされるプラットフォームに関する情報、新しいリリースへのアップグレードが可能な CA ControlMinder のバージョン、既知の問題点、考慮事項、および CA ControlMinder をインストールする前に把握しておく必要のあるその他の重要な情報について説明しています。

- 実環境をアップグレードする前に、新しいリリースについて簡易的な内部テストを実施することをお勧めします。

- CA ControlMinder のアップグレード時には、インストールを完了させるために、コンピュータを再起動する必要がある場合があります。将来的にパッチによって再起動が必要でなくなる可能性があります。

注: アップグレード時に、CA ControlMinder のどのリリースで再起動が必要となるかについては、「リリース ノート」を参照ください。

- 対象となる環境が PMDB 階層で設定されている場合、またはそのような環境を設定する場合は、以下の作業を行うことをお勧めします。

- 階層内の各コンピュータのインストールまたは各コンピュータのアップグレードを下から上の順（サブスクライバが最初）で行います。

PMDB のアップグレード時に、旧バージョンを利用しているサブスクライバが存在する場合、誤ったコマンドが送信される場合があります。この問題は、旧バージョンの PMDB に存在しないクラスやプロパティが新しい PMDB に含まれることが原因で発生します。

注: 単一のコンピュータ上で動作する PMDB 階層については、同時にアップグレードすることができます。

- PMDB またはポリシーの更新中にアップグレードを行わないでください。
- サブスクライバおよび PMDB ポリシーをバックアップします。

注: 旧バージョンの PMDB は、新しいバージョンのサブスクライバを保持できます。しかし、これと逆の状況は許可されていません。旧バージョンのコマンドは最新バージョンでもサポートされているため、現在の CA ControlMinder のサブスクライバへの古い PMDB の伝播が可能です。

- アップグレードする前に使っていたのと同じ暗号化鍵を使用する必要があります。
- インストールプログラムは、前のインストールのレジストリ設定を自動的に保存およびアップグレードします。旧バージョンのレジストリキーが再配置された場合、アップグレードプロセスでは以前の設定が新しい場所にコピーされます。

CA ControlMinder のレジストリ設定は、以下の場所に格納されています。

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl

- 完全監査は、CA ControlMinder のアップグレード時に、デフォルトで有効になります。

重要: データベースに保存されているルールによりませんが、この機能の結果として、CA ControlMinder がログ ファイルに記録する監査イベントの数が大幅に増える可能性があります。そのような場合、監査ログ ファイルのサイズとバックアップ設定を見直すことをお勧めします。

注: 完全監査および監査ログ バックアップ用のレジストリ設定の使用および構成の詳細については、「*Windows エンドポイント管理ガイド*」を参照してください。

その他の製品との共存

CA ControlMinder をインストールする場合は、CA ControlMinder とその他のプログラムをコンピュータ上で共存させる場合の問題について検討してください。

CA ControlMinder は、たとえば、CA Antivirus などの他のプログラムと並行した環境で実行します。これは、CA ControlMinder とローカル コンピュータ上で実行しているプログラムとの衝突を引き起こす可能性があります。このため、共存ユーティリティ (eACoexist.exe) を CA ControlMinder のインストール中に実行して、衝突を引き起こす可能性のあるローカル コンピュータのプログラムを検出します。ユーティリティは、CA ControlMinder がサポートする各共存プログラムにプラグイン (バイナリ モジュール) を使用します。CA ControlMinder が検出するプログラムが **trusted** の場合は、CA ControlMinder は SPECIALPGM ルールを作成することによってプログラムを登録します。この SPECIALPGM ルールはこのプログラムへのアクセスを決定し、アクセスを付与するときに CA ControlMinder がそれを確実に無視するようにします。

注: eACoexist ユーティリティおよびサポートされているプラグインに関する詳細については、「リファレンス ガイド」を参照してください。

例: Dr Watson の trusted プログラム ルール

この例では、共存ユーティリティが CA ControlMinder と同じコンピュータ上で Dr Watson アプリケーションを発見した場合に、作成できる **trusted** プログラム ルールを示します。これらのルールはデフォルトの Windows 2000 Server がインストールされているコンピュータに従います。

```
editres SPECIALPGM ('C:\WINNT\system32\DRWTSN32.EXE') pgmtype(DCM)
editres PROGRAM ('C:\WINNT\system32\DRWTSN32.EXE') owner(nobody) defacc(x) trust
```

Product Explorer によるインストール

CA ControlMinder Product Explorer では、CA ControlMinder の異なるアーキテクチャでのインストールと、ランタイム SDK のインストールが可能です。さらに、インストール コンポーネントのシステム要件を表示できます。

注: autorun が有効になっている場合、CA ControlMinder Endpoint Components for Windows DVD を光ディスク ドライブに挿入すると、Product Explorer が自動的に表示されます。

Product Explorer を使用したインストール

CA ControlMinder Product Explorer では、CA ControlMinder の異なるアーキテクチャでのインストールと、ランタイム SDK のインストールが可能です。Product Explorer は、グラフィカルインターフェースを使用して CA Access Control のアンインストールを実行し、ユーザに対し、対話的にフィードバックを行います。

Product Explorer を使用したインストール方法

1. Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログインします。
2. 実行中のアプリケーションがあれば、すべて終了します。
3. CA ControlMinder Endpoint Components for Windows DVD を光ディスクドライブに挿入します。

autorun が有効になっている場合は、Product Explorer が自動的に表示されます。autorun が有効になっていない場合は、光ディスクドライブのディレクトリに移動し、PRODUCTEXPLORERX86.EXE ファイルをダブルクリックします。

4. Product Explorer のメインメニューから、Components フォルダを展開し、CA ControlMinder for Windows (*my_architecture*) を選択し、[インストール] をクリックします。

インストール先のコンピュータのアーキテクチャに適合するインストールオプションを選択する必要があります（32 ビット、64 ビット x 64、または 64 ビット Itanium）。

[セットアップ言語の選択] ウィンドウが表示されます。

5. CA ControlMinder をインストールする言語を選択し、[OK] をクリックします。

CA ControlMinder インストールプログラムがローディングを開始し、しばらくして、概要画面が表示されます。

注: CA ControlMinder の既存のインストールがインストールプログラムによって検出された場合、CA ControlMinder のアップグレードを実行するかどうかを選択するように促されます。

6. インストール画面の指示に従います。

インストール中、ユーザは情報を入力するよう求められます。CA ControlMinder のインストール時にユーザが必要となる情報については、[インストールワークシート \(P. 180\)](#) を参照してください。

インストールプログラムによって CA ControlMinder がインストールされます。インストールが完了したら、Windows をすぐに再起動するか、または後で再起動するかを選択します。

7. [はい、今すぐコンピュータを再起動します] を選択して [OK] をクリックします。

システムの再起動後に、[CA ControlMinder が正しくインストールされたことを確認 \(P. 205\)](#) できます。

注: コンピュータを後で再起動するように選択した場合、コンピュータが再起動されるまでインストールが完了しないことを示す警告メッセージが表示されます。ログオンインターセプトなどの CA ControlMinder の一部の機能は、コンピュータを再起動するまで機能しません。

インストール ワークシート

インストールプログラムはユーザに CA ControlMinder の初期設定に必要な情報を入力するよう求めます。以下のセクションでは、提供することが必要な情報を説明し、推奨事項を示します。

機能の選択

インストールプログラムの [機能の選択] 画面では、CA ControlMinder をインストールする場所と、コンピュータにインストールする機能を定義することができます。以下の機能が使用可能です。

機能	説明	推奨
タスクの委任	管理タスクを実行するのに必要な権限を一般ユーザに与えることができます。 注: デフォルトで選択されています。	この機能は、サブ管理権限をユーザに付与する場合に選択します。インストール後に設定することもできます。

機能	説明	推奨
SDK	SDK と呼ばれるサブディレクトリを作成します。このサブディレクトリには、CA ControlMinder SDK および API サンプルを使用するのに必要なライブラリおよびファイルが含まれています。	この機能は、CA ControlMinder のセキュリティ機能を使用して社内アプリケーションを開発する場合に選択します。
Stack Overflow Protection (STOP)	CA ControlMinder スタック オーバーフロー保護機能を有効にします。	この機能は、プログラムが不正に利用されるのを防ぐために選択します。
メインフレームのパスワード同期	ユーザ パスワードをメインフレーム コンピュータと同期させることができます。	この機能は、メインフレーム コンピュータとの同期を維持する場合に選択します。
Unicenter 統合	Unicenter NSM と CA ControlMinder を統合し、Unicenter NSM のデータを移行することができます。CA ControlMinder により、Unicenter NSM の環境設定パラメータで指定されたホストまたは選択されたホストに監査データが送信されます。 注: この機能は、該当するコンピュータに Unicenter NSM がインストールされている場合にのみ利用できます。	

機能	説明	推奨
拡張ポリシー管理 クライアント	ローカル コンピュータに拡張 ポリシー管理を設定します。	この機能は、拡張ポリシー管理を使用した ポリシーのデプロイ先とするすべてのエン ドポイントに対して選択してください。 注: 拡張ポリシー管理の詳細については、 「エンタープライズ管理ガイド」を参照し てください。
Policy Model サブ スクライバ	親 PMDB から更新情報を受信 するためにローカル コン ピュータを設定します。	この機能は、親 PMDB からの更新対象とす るすべてのエンドポイントに対して選択し てください。 注: Policy Model サービスの詳細について は、「Windows エンドポイント管理ガイド」 を参照してください。
SAM の統合	SAM 統合により、ローカル コ ンピュータは Shared Accounts Management (SAM) 用に設定 されます。これにより、その コンピュータ上の特権アカウ ントとアプリケーションの検 出と管理ができるようになります。 ます。	この機能は、SAM を使用して管理する共有 アカウントがあるすべてのエンドポイント に対して選択してください。 注: SAM の詳細については、「エンタープラ イズ管理ガイド」を参照してください。
レポート エー ジェント	データベースのスケジュール されたスナップショットを配 布サーバに送信するように、 コンピュータを設定するこ とができます。 さらに、監査レコードを配布 サーバに送信するように選択 することができます。	レポート エージェント機能は、このエンド ポイントをエンタープライズ レポートに含 める場合に選択します。CA Enterprise Log Manager を使用してエンタープライズ監査 ログを管理する場合は、監査ルーティング サブ機能を選択します。

管理者とホストの情報

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	説明	推奨される手順
管理者	CA ControlMinder データベースへの管理アクセス権限を有するユーザを定義することができます。	
管理端末	管理者が CA ControlMinder データベースを管理するために使用できるコンピュータを定義できます。	管理者が CA ControlMinder エンドポイント管理を使用して CA ControlMinder を管理する場合は、CA ControlMinder エンドポイント管理がインストールされているコンピュータのみを定義する必要があります。管理者によってブラウザが開かれるコンピュータを定義する必要はありません。
DNS ドメイン名	CA ControlMinder がホスト名に追加するネットワークのドメイン名を入力できます。	CA ControlMinder がホスト名に追加するドメイン名のうち少なくとも 1 つを入力する必要があります。

ユーザおよびグループ

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	説明	推奨される手順
プライマリ ストアからのユーザおよびグループのサポート	既存のエンタープライズ ユーザ ストアを使用できます。このため、CA ControlMinder データベース内でこれらのユーザを重複させる必要はありません。	CA ControlMinder で、エンタープライズ ユーザ ストアをサポートするためにプライマリ ストアのサポートを設定することをお勧めします。エンタープライズ ストアをサポートしない場合、保護対象のアクセサが CA ControlMinder データベース内で重複することになります。

情報	説明	推奨される手順
Windows ユーザおよびグループのデータのインポート	保護対象のアクセサを作成するよう指定した場合は、既存の Windows ユーザおよびグループがデータベース内に自動的に作成されます。	Windows ユーザおよびグループをインポートするよう指定した場合は、以下のオプションのうちの 1 つ以上を選択します。 ■ ユーザのインポート - Windows ユーザをデータベースにインポートします。 ■ グループのインポート - Windows グループをデータベースにインポートします。 ■ ユーザのデフォルト グループへの接続 - インポートするユーザを、データベース内の適切なインポート済みグループに自動的に追加します。 ■ インポートされたデータの所有者の変更 - インポートするデータの所有者として自分以外のユーザを定義します。デフォルトでは、これらのレコードの所有者はインストール作業を実行している管理者に設定されます。 ■ ドメインからのインポート - 指定されたドメインからアクセサ データをインポートします。

Unicenter Integration

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	説明	推奨される手順
CA ControlMinder と Unicenter TNG の統合	Unicenter TNG の環境設定パラメータで指定されたホストまたは選択されたホストに監査データが送信されるように、CA ControlMinder を設定できます。	統合するには、監査データが Unicenter NSM に送信されるように指定し、CA ControlMinder が監査データを送信するホストを選択します。

情報	説明	推奨される手順
CA ControlMinder と Unicenter カレンダの統合	Unicenter NSM カレンダとユーザおよびアクセス権限の統合がサポートされるよう設定できます。	デフォルトの設定 10 分前後の間隔で、Unicenter NSM カレンダから更新情報を取得するように CA ControlMinder を設定します。
Unicenter セキュリティのデータの移行	Unicenter セキュリティデータを CA ControlMinder に移行することができます。	このオプションを選択しない場合、Unicenter セキュリティから CA ControlMinder への移行は行われません。また、CA ControlMinder でのユーザ名は完全修飾されて表示されます (DOMAINNAME¥USERNAME)。移行では、ユーザ名は修飾されません (USERNAME)。

コンポーネント間通信の暗号化

以下の表では、必要となる情報について説明し、推奨事項を示します。

画面	説明	推奨される手順
SSL 通信	コンポーネント間の通信に Secure Socket Layer (SSL) を使用するかどうかを指定できます。SSL および対称鍵暗号化の両方を使用できます。	SSL (公開鍵を使用) および対称鍵暗号化を両方とも使用することをお勧めします。
証明書の設定	SSL を使用する場合は、使用する証明書を指定できます。	確かな認証局 (CA) が発行した証明書の使用をお勧めします。
証明書の生成	ルート証明書として使用する、自己証明書と鍵のペアを作成できます。	自己証明書の使用も可能ですが、この方法はお勧めしません。 自己証明書を使用する場合は、自己証明書の使用をすべてのホストで許可する必要があります。
証明書の設定の変更	証明書の設定を変更できます。	証明書および鍵のペアの設定をデフォルト設定から変更することを強くお勧めします。 サーバ証明書の秘密鍵を保護するためにパスワードを指定することもできます。

画面	説明	推奨される手順
既存の証明書	インストールした証明書に関する情報を提供します。	
暗号化の設定	暗号化の方法および対称暗号化の鍵を設定できます。	暗号化鍵の設定をデフォルト設定から変更することを強くお勧めします。

詳細情報:

[対称暗号化](#) (P. 560)

[SSL、認証、および証明書](#) (P. 565)

Policy Model のサブスクライバの設定

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	Description	推奨される手順
親 Policy Model データベースの指定	このデータベースがサブスクライブする 1 つ以上の親 PMDB を定義します。ローカルデータベースは、このリストで指定されていない PMDB からの更新情報を受け入れません。親 PMDB は、 <i>pmdb@hostname.com</i> の形式で定義します。	インストールの完了後、このデータベースを親 PMDB 上でサブスクライバとして定義する必要があります。 注: <i>_NO_MASTER_</i> を親 PMDB として指定し、任意の PMDB から伝達される更新をローカルデータベースが受け入れることを示します。
パスワード Policy Model	パスワードの変更を伝達する、親パスワード Policy Model を定義します。パスワード PMDB は、 <i>pmdb@hostname.com</i> の形式で定義します。	インストールの完了後、このデータベースをパスワード PMDB 上でサブスクライバとして定義する必要があります。

拡張ポリシー管理クライアント

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	Description	推奨される手順
拡張ポリシー管理サーバのホスト名の指定	拡張ポリシー管理サーバのホスト名がインストールされているサーバの名前を定義します。	「dhName@hostName」という形式で、ホスト名を定義します。 注: 拡張ポリシー管理およびレポートの詳細については、「エンタープライズ管理ガイド」を参照してください。

レポートエージェントの設定

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	説明	推奨される手順
レポートスケジュールの選択	レポートエージェントが、いつ配布サーバにデータベースのスナップショットを送信するかを指定します。	システムリソースの消費が激しいときにレポートエージェントによってスナップショットが送信されることのないように設定することをお勧めします。
監査ルーティングの環境設定	監査ログファイルのタイムスタンプされたバックアップを保持するかどうかを指定します。 注: このオプションは、[機能の選択] ページで、監査ルーティングのインストールを選択している場合にのみ表示されます。	監査ログファイルのタイムスタンプされたバックアップを保持するように選択していることを確認してください。これはデフォルトの設定で、すべての監査レコードがレポートエージェントによって確実に読み取ることができるようにするのに必要です。 CA ControlMinder は、50 ファイルに達すると、監査ログファイルを上書きします。この数が企業に適さない場合は、logmgr レジストリ サブキーの audit_max_files トークンを適切な値に編集する必要があります。

配布サーバの設定

以下の表では、必要となる情報について説明し、推奨事項を示します。

情報	説明	推奨される手順
サーバ名	配布サーバがインストールされているホストの名前を定義します。	配布サーバがインストールされているホストの完全修飾ホスト名を指定する必要があります。
セキュア接続の使用	配布サーバとレポートエージェント間および配布サーバと SAM 間の通信に SSL を使用するかどうかを指定します。	SSL を使用することをお勧めします。 SSL を使用しない場合、配布サーバは、レポートエージェントおよび SAM エージェントとの通信に TCP を使用します。
サーバポート	配布サーバとレポートエージェント間、および配布サーバと SAM エージェント間の通信に使用するポート番号を定義します。	SSL 通信を使用する場合、デフォルトのサーバポートは 7243 です。 SSL 通信を使用しない場合、デフォルトのサーバポートは 7222 です。
通信キー	配布サーバとレポートエージェント間、および配布サーバと SAM エージェント間の通信を認証するキーを新規に定義します。	配布サーバをインストールする場合は、必ず同じキーを使用してください。 注: SSL 通信を使用する場合、通信キーを指定する必要があります。SSL 通信を使用しない場合、通信キーを指定しないことを選択できます。

コマンドラインによるインストール

コマンドラインを使用すると、以下のことが可能です。

- グラフィカルインストールプログラムにデフォルト設定を渡します。
- CA ControlMinder をサイレントモードでインストールします。

インストール プログラムに対するカスタム デフォルトの設定

企業で使用するデフォルトを使用して CA ControlMinder インストール プログラムを設定するには、コマンドラインを使用します。グラフィカル インストール プログラムは、コマンドラインから入力を受け取り、事前に選択されているオプションを確認します。

インストール プログラムに対してカスタム デフォルトを設定する方法

1. Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログインします。
2. 実行中のアプリケーションがあれば、すべて終了します。
3. CA ControlMinder Endpoint Components for Windows DVD を光ディスク ドライブに挿入します。

autorun が有効になっている場合、CA ControlMinder Product Explorer が表示されます。

4. CA ControlMinder Product Explorer が表示されたら、これを閉じます。
5. コマンドラインを開き、光ディスク ドライブの以下のディレクトリに移動します。

`%architecture`

`architecture`

オペレーティング システムのアーキテクチャの省略形を定義します。

X86、**X64**、および **IA64** のいずれかとなります。

6. 以下のコマンドを入力します。

```
setup [/s] /v"<insert_params_here>"
```

`<insert_params_here>` 変数では、インストール プログラムに渡すインストール設定を指定します。

インストール プログラムが表示されます。インストール プログラムの画面には、プログラムに渡すように選択しているデフォルト オプションが表示されます。これらのオプションを変更して CA ControlMinder をインストールできます。

サイレントモードでのインストール

対話形式のフィードバックなしで CA ControlMinder をインストールするには、コマンドラインを使用して CA ControlMinder をサイレントモードでインストールすることができます。

CA ControlMinder をサイレントモードでインストールする方法

1. Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログインします。
2. 実行中のアプリケーションがあれば、すべて終了します。
3. CA ControlMinder Endpoint Components for Windows DVD を光ディスクドライブに挿入します。

autorun が有効になっている場合、CA ControlMinder Product Explorer が表示されます。

4. CA ControlMinder Product Explorer が表示されたら、これを閉じます。
5. コマンドラインを開き、光ディスクドライブの以下のディレクトリに移動します。

`%architecture`

`architecture`

オペレーティングシステムのアーキテクチャの省略形を定義します。

X86、**X64**、および **IA64** のいずれかとなります。

6. 以下のコマンドを入力します。

```
setup /s /v"/qn COMMAND=keyword <insert_params_here>"
```

`<insert_params_here>` 変数では、インストールプログラムに渡すインストール設定を指定します。

注: サイレントインストールを実行するには、エンドユーザ使用許諾契約に同意する必要があります。エンドユーザ使用許諾契約への同意およびサイレントモードでの CA ControlMinder のインストールに必要な **keyword** は、インストールプログラムを実行したときに表示されるエンドユーザ使用許諾契約の下部にあります。

setup コマンド - CA ControlMinder for Windows のインストール

[事前に設定されたカスタム デフォルト \(P. 189\)](#)を使用して CA ControlMinder for Windows をインストールする場合、または[サイレントインストール \(P. 190\)](#)を実行する場合は、**setup** コマンドを使用します。

注: コマンドラインの構文の詳細については、Microsoft Developer Network ライブラリで入手できる Windows インストーラ SDK を参照してください。

このコマンドの形式は以下のようになります。

```
setup [/s] [/L] [/v"<insert_params_here>"]
```

/s

setup の最初のダイアログ ボックスを非表示にします。

/L

CA ControlMinder インストール言語を定義します。

注: このリリースでサポートされている CA ControlMinder のインストール言語の詳細については、リリース ノートを参照してください。

```
/v "<insert_params_here>"
```

インストールプログラムに渡すパラメータを定義します。

注: パラメータはすべて二重引用符 ("") で囲みます。

以下のパラメータは、**/v** パラメータを介してインストールプログラムに渡されます。

/l[*mask*] *log_file*

インストール ログ ファイルの完全パスと名前を定義します。利用可能な情報をすべてログに記録するには、マスク ***v** を使用します。

/forcerestart

インストーラが再起動を必要とする場合は、インストールが完了した後でコンピュータが再起動するように指定します。

/norestart

インストールが完了した後でコンピュータが再起動されないよう指定します。

/qn

/s オプションと共に、サイレント インストールを指定します。

重要: サイレント インストールを実行するには、**COMMAND** パラメータを使用します。

AC_API={1 | 0}

SDK ライブラリとサンプルをインストールする (1) かどうかを指定します。

デフォルト : 0 (インストールしない)

ADMIN_USERS_LIST=¥"users¥"

CA ControlMinder データベースに対する管理アクセス権限を持つユーザのスペース区切りリストを定義します。

デフォルト : インストールを実行するユーザ

重要: リストで NT Authority¥System ユーザを定義しないでください。ローカル管理ユーザ アカウントを定義します。

ADV_POLICY_MNGT_CLIENT={1 | 0}

ローカル コンピュータに拡張ポリシー管理を設定する (1) かどうかを指定します。

デフォルト : 1

このオプションが 1 に設定されている場合は、以下を指定します。

- **APMS_HOST_NAME=¥"name¥"**

拡張ポリシー管理コンポーネントがインストールされているサーバの名前を定義します。

COMMAND=keyword

エンドユーザ使用許諾契約への同意およびサイレント モードでの CA ControlMinder のインストールに必要なコマンドを定義します。実際の **keyword** は、グラフィカルインストールプログラムを実行したときに表示されるエンドユーザ使用許諾契約の下部にあります。

デフォルト : none

DIST_SERVER_NAME=¥"name¥"

SAM エージェントおよびレポート エージェントが通信する配布サーバホストの完全修飾名を定義します（たとえば test.company.com）。

デフォルト： none

DIST_SERVER_PORT=¥"port¥"

SAM エージェントおよびレポート エージェントが配布サーバとの通信に使用するポート番号を定義します。

デフォルト： 7243

DOMAIN_LIST=¥"domains¥"

ホスト名に追加する、CA ControlMinder 用のネットワーク DNS ドメインの名前のスペース区切りリストを定義します。

デフォルト： none

ENABLE_STOP={1 | 0}

スタック オーバーフロー保護（STOP）機能を有効にする（1）かどうかを指定します。

デフォルト： 0（無効）

注： STOP のサポートは、x86 と x64 のインストールにのみ適用できます。

HOSTS_LIST=¥"hosts¥"

管理者が CA ControlMinder データベースの管理に使用するコンピュータ（CA ControlMinder 端末）のスペース区切りリストを定義します。

デフォルト： 現在のコンピュータ

IMPORT_NT={Y | N}

プライマリ（エンタープライズ）ユーザストアをサポートするかどうかを指定します。Nを指定した場合、プライマリユーザストアがサポートされます。Yを指定すると、プライマリユーザストアはサポートされません。以下のオプションを1つ以上指定して、Windows ユーザと Windows グループを CA ControlMinder データベースにインポートできます。

- **IMPORT_USERS={1 | 0}**

Windows ユーザをデータベースにインポートするかどうかを選択します。

- **IMPORT_GROUPS={1 | 0}**

Windows グループをデータベースにインポートするかどうかを選択します。

- **IMPORT_CONNECT_USERS={1 | 0}**

インポートしたユーザをデータベース内の対応するインポートしたグループに追加するかどうかを指定します。

- **IMPORT_CHANGE_OWNER={1 | 0} NEW_OWNER_NAME=name**

インポートしたデータの所有者として、自分以外のユーザを指定します。

- **IMPORT_FROM_DOMAIN={1 | 0} IMPORT_DOMAIN_NAME=name**

定義したドメインからアクセサデータをインポートするかどうかを指定します。

注: デフォルトでは、これらのオプションのいずれも指定されていません（値 0 に相当する）。

INSTALLDIR=¥"location¥"

CA ControlMinder がインストールされる場所を定義します。

デフォルト : C:¥Program Files¥CA¥AccessControl

MAINFRAME_PWD_SYNC={1 | 0}

メインフレームのパスワード同期機能をインストールする (1) かどうかを指定します。

デフォルト : 0 (インストールしない)

NEW_KEY=¥"name¥"

配布サーバと、SAM エージェントおよびレポート エージェントとの通信を認証する SSL キーを定義します。

PMDB_CLIENT={1 | 0}

ローカル CA ControlMinder データベースを親 Policy Model データベースにサブスクライブするかどうかを指定します。

デフォルト : 0 (設定しない)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションを指定します。

- **PMDB_PARENTS_STR=¥"parents¥"**

ローカルの CA ControlMinder データベースがサブスクライブされる、親ポリシー モデル データベースのリストをカンマ区切りリストで定義します。 任意の PMDB から伝達される更新をローカルデータベースが受け入れるようにするには、**_NO_MASTER_** を親 PMDB として指定します。

デフォルト : none

- **PWD_POLICY_NAME=¥"name¥"**

パスワード Policy Model の名前を定義します。

デフォルト : none

PMDB_PARENT={1 | 0}

Policy Model 親データベースを作成するかどうかを指定します。このオプションを指定し、値を 1 に設定した場合は、以下のオプションを指定します。

- **PMDB_NAME=¥"name¥"**

作成する PMDB の名前を定義します。

デフォルト : pmdb

- **PMDB_SUBSCRIBERS_STR=¥"subs¥"**

PMDB_NAME オプションで指定された PMDB が変更内容を伝達するサブスクライバデータベースのスペース区切りリストを定義します。これらは基本的にインストール済み親 PMDB のサブスクライバデータベースです。

PUPM_INTEGRATION={1 | 0}

SAM エージェントをインストールする (1) かどうかを指定します。

デフォルト : 0 (インストールしない)

このオプションを指定し、値を 1 に設定した場合は、
DIST_SERVER_NAME、DIST_SERVER_PORT、USE_SECURE_COMM を指定します。

REPORT_AGENT={1 | 0}

レポート エージェントをインストールする (1) かどうかを指定します。

デフォルト : 0 (インストールしない)

このオプションを指定し、値を 1 に設定した場合は、
DIST_SERVER_NAME、DIST_SERVER_PORT、USE_SECURE_COMM および以下のパラメータを指定します。

- **AUDIT_ROUTING={1 | 0}**

監査ルーティング機能をインストールする (1) かどうかを指定します。

デフォルト : 0 (インストールしない)

- **REPORT_DAYS_SCHEDULE=days**

レポート エージェントが動作する曜日のカンマ区切りリストを定義します。

値 : Sun、Mon、Tue、Wed、Thu、Fri、Sat

デフォルト : none

- **REPORT_TIME_SCHEDULE={hh:mm}**

レポート エージェントが、指定された日に動作する時刻を定義します (たとえば、14:30)。

制限 : hh は 0~23 の範囲の数字で、mm は 0~59 の範囲の数字です。

デフォルト : none

TASK_DELEGATION={1 | 0}

タスクの委任機能を有効にするかどうかを指定します。

デフォルト : 1 (有効)

UNICENTER_INTEGRATION={1 | 0}

Unicenter の統合機能を有効にする (1) かどうかを指定します。この機能は、該当するコンピュータに Unicenter NSM がインストールされている場合にのみ利用できます。

デフォルト : 0 (無効)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションを指定します。

- SEND_DATA_TO_TNG={1 | 0}

監査データを Unicenter NSM に送信する (1) かどうかを指定します。

デフォルト : 1 (データを送信)

- OTHER_TNG_HOST_NAME=¥"name¥"

監査データが送信されるホストを定義します。

デフォルト : Unicenter NSM で指定されたホスト名

- SUPPORT_TNG_CALENDAR= {1 | 0}

Unicenter NSM カレンダをサポートする (1) かどうかを指定します。

デフォルト : 1 (サポートする)

- TNG_REFRESH_INTERVAL=¥"mm¥"

更新間隔を分単位で定義します。SUPPORT_TNG_CALENDAR=1 も設定したことを確認してください。

デフォルト : 10

- UNICENTER_MIGRATION={1 | 0}

Unicenter セキュリティ データを CA ControlMinder に移行する (1) かどうかを指定します。

デフォルト : 1 (移行する)

USE_SECURE_COMM={1 | 0}

SAM エージェントおよびレポート エージェントがセキュアな通信を使用する (1) かどうかを指定します。

デフォルト : 0 (設定しない)

このオプションを指定し、値を 1 に設定した場合は、次に NEW_KEY の SSL キーの値を指定します。

USE_SSL={1 | 0}

通信の暗号化として SSL を設定するかどうかを指定します。

デフォルト : 0 (設定しない)

このオプションを指定し、値を 1 に設定した場合は、次に以下のオプションを指定します。

- **CERT_OPTION={1 | 2}**

使用する認証オプションを指定します。

値 : 1 - CA ControlMinder 証明書を生成します。2 - インストールされた既存の証明書を使用します。

デフォルト : 1

- **GENERATE_OPTION={1 | 2}**

CA ControlMinder 証明書の生成方法を指定します。

CERT_OPTION=1 を設定したことを確認してください。

値 : 1 - デフォルトのルート証明書を使用します。2 - ルート証明書を指定します。

- **SERVER_PRIV_KEY_PWD=¥"password¥"**

生成された CA ControlMinder 証明書用の秘密鍵のパスワードを定義します。CERT_OPTION=1 を設定したことを確認してください。

- **GEN_ROOT_CERT=¥"file¥"**

ルート証明書ファイル (.pem) の完全修飾ファイル名を定義します。CERT_OPTION=1 および GENERATE_OPTION=2 を設定したことを確認してください。

- **GEN_ROOT_PRIVATE=¥"file¥"**

ルート秘密鍵ファイル (.key) の完全修飾ファイル名を定義します。CERT_OPTION=1 および GENERATE_OPTION=2 を設定したことを確認してください。

- **ROOT_PRIV_KEY_PWD=¥"password¥"**

ルート秘密鍵用のパスワードを定義します。CERT_OPTION=1 および GENERATE_OPTION=2 を設定したことを確認してください。

- **EXIST_ROOT_CERT=¥"file¥"**

ルート証明書ファイル (.pem) の完全修飾ファイル名を定義します。CERT_OPTION=2 を設定したことを確認してください。

- **EXIST_SERVER_CERT=¥"file¥"**

サーバ証明書ファイル (.pem) の完全修飾ファイル名を定義します。CERT_OPTION=2 を設定したことを確認してください。

- **EXIST_PRIVATE_KEY=¥"file¥"**

サーバ秘密鍵ファイル (.key) の完全修飾ファイル名を定義します。CERT_OPTION=2 を設定したことを確認してください。

- **EXIST_PRIV_KEY_PWD=¥"password¥"**

サーバ秘密鍵用のパスワードを定義します。CERT_OPTION=2 を設定したことを確認してください。

USE_SYMT_KEY={1 | 0}

通信に対して対称鍵暗号化を設定するかどうかを指定します。USE_SSL=0 の場合、このパラメータは 1 に設定されます。

デフォルト : 1

このオプションを指定し、値を 1 に設定した場合は、次に以下のオプションも指定します。

- **ENCRYPTION_METHOD={Default | DES | 3DES | 256AES | 192AES | 128AES}**

通信において使用する暗号化の方法を指定します。

デフォルト : 256 AES

- **CHANGE_ENC_KEY={1 | 0}**

デフォルトの暗号化キーを変更する (1) かどうかを指定します。

デフォルト : 1 (変更する)

- **NEW_ENCRYPT_KEY=¥"key¥"**

デフォルトの暗号化キーの変更を選択した場合に、暗号化キーを定義します。CHANGE_ENC_KEY=1 も設定してください。

例: setup コマンドを使用してインストール時のデフォルトを設定する

以下の例では、インストールディレクトリを設定し、CA ControlMinder インストールのためにインストール ログ ファイルのデフォルトを定義し、グラフィカルインストールプログラムを開きます。

```
setup.exe /s /v"INSTALLDIR="C:¥Program Files¥CA¥AccessControl"
/L*v %SystemRoot%¥eACInstall.log"
```

例: setup コマンドを使用して暗号化設定を指定する

以下の例では、さまざまな暗号化設定を使用して、CA ControlMinder をサイレントモードでインストールします。それぞれの例で、コマンドによって CA ControlMinder のインストール、デフォルトのレポート エージェントおよびタスク委任機能のインストール、SSL の有効化、インストール ログファイルのパスおよび名前の定義が実行されます。

- この例は、デフォルトの CA ControlMinder ルート証明書からサーバ証明書を生成し、サーバ秘密鍵用のパスワードを定義します。

```
setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=1 GENERATE_OPTION=1  
SERVER_PRIV_KEY_PWD=%"P@ssw0rd%" /l*v C:%AC_silent.log"
```

- この例は、サードパーティのルート証明書からサーバ証明書を生成します。ルート秘密鍵はパスワード保護されています。

```
setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=1 GENERATE_OPTION=2  
GEN_ROOT_CERT=%"C:%Crypto%example.pem%"  
GEN_ROOT_PRIVATE=%"C:%Crypto%example.key%" ROOT_PRIV_KEY_PWD=%"P@ssw0rd%" /l*v  
C:%AC_silent.log"
```

- この例は、CA ControlMinder でサードパーティのルート証明書およびサーバ証明書を使用するよう指定します。サーバ秘密鍵はパスワード保護されています。

```
setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=2  
EXIST_ROOT_CERT=%"C:%Crypto%example.pem%"  
EXIST_SERVER_CERT=%"C:%Crypto%server.pem%"  
EXIST_PRIVATE_KEY=%"C:%Crypto%server.key%" EXIST_PRIV_KEY_PWD=%"P@ssw0rd%"  
/l*v C:%AC_silent.log"
```

詳細情報:

[通信の暗号化](#) (P. 559)

Windows エンドポイントのアップグレード

いずれかのエンドポイントをアップグレードする場合、CA ControlMinder インストール プログラムは CA ControlMinder の主要機能、およびそのエンドポイントにすでにインストールされているすべての機能をアップグレードします。CA ControlMinder の主要機能をアップグレードした後に、新機能をインストールできます。

注: インストール完了後に、コンピュータの再起動が必要な場合があります。アップグレード時に、CA ControlMinder のどのリリースで再起動が必要となるかについては、「リリース ノート」を参照ください。

エンドポイントのアップグレード方法

1. Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログインします。
2. 実行中のアプリケーションがあれば、すべて終了します。
3. CA ControlMinder Endpoint Components for Windows DVD を光ディスクドライブに挿入します。

autorun が有効になっている場合は、Product Explorer が自動的に表示されます。autorun が有効になっていない場合は、光ディスク ドライブのディレクトリに移動し、PRODUCTEXPLORERX86.EXE ファイルをダブルクリックします。

4. Product Explorer のメイン メニューから、Components フォルダを展開し、CA Access Control for Windows (*my_architecture*) を選択し、[インストール] をクリックします。

注: コンピュータのアーキテクチャと一致するインストール オプションは強調表示され、このコンピュータ上に CA ControlMinder がすでにインストールされていることがわかります。

CA ControlMinder のアップグレードを実行するかどうか尋ねるダイアログ ボックスが表示されます。

5. [はい] をクリックします。

CA ControlMinder インストール プログラムがローディングを開始し、しばらくして、概要画面が表示されます。

6. インストール画面の指示に従います。

インストールプログラムによって CA ControlMinder がアップグレードされます。アップグレードが完了すると、Windows をすぐに再起動するか、または後で再起動するかを選択します。

7. (オプション) 「はい」を選択すると、コンピュータがすぐに再起動します。

コンピュータが再起動して、アップグレードが完了します。

8. (オプション) 以下のように 追加の CA ControlMinder 機能をインストールします。

- a. [スタート] - [コントロール パネル] - [プログラムの追加と削除] を選択します。

- b. プログラム リストをスクロールして CA ControlMinder を選択し、[変更] をクリックします。

CA ControlMinder インストールプログラムのローディングが開始され、しばらくして、プログラムのメンテナンス画面が表示されます。

- c. [変更] を選択し、インストール画面の指示に従って、各機能をインストールします。

インストール中、ユーザは情報を入力するよう求められます。各機能のインストールに必要な情報については、[インストールワークシート](#) (P. 180)を参照してください。インストール完了後に、コンピュータの再起動が必要な場合があります。

CA ControlMinder の起動および停止

デフォルトでは、Windows を開始する場合は常に、CA ControlMinder サービスが自動的に開始します。

CA ControlMinder の停止

`secons` ユーティリティを使用して、ローカル コンピュータおよびリモート コンピュータ上の **CA ControlMinder** を停止します。**CA ControlMinder** の停止には特定の **Windows** 権限を必要としませんが、**CA ControlMinder** の **ADMIN** または **OPERATOR** 属性を持っている必要があります。

注: **CA ControlMinder** が **Windows** サービス マネージャから実行されている間は、その **CA ControlMinder** を停止できません。`secons` ユーティリティを使用して **CA ControlMinder** を停止してから、**Windows** サービス マネージャ内で **CA ControlMinder** サービスを変更してください。

CA ControlMinder の停止方法

1. コマンドプロンプト ウィンドウを開き、**CA ControlMinder** バイナリがあるディレクトリに移動します。

デフォルトでは、**CA ControlMinder** バイナリは **C:\Program Files\CA\AccessControl\bin** にあります。

2. 以下のコマンドを入力します。

```
secons -s [hosts | ghosts]
```

```
-s [hosts | ghosts]
```

スペース区切りで定義された複数のリモート ホスト上の **CA ControlMinder** サービスを停止します。ホストを指定しない場合、**CA ControlMinder** はローカル ホスト上のサービスを停止します。

ghost レコードの名前を入力することで、ホスト グループを定義できます。このオプションをリモート端末から使用する場合は、ユーティリティによってパスワードの検証が要求されます。また、リモート コンピュータとローカル コンピュータの管理者権限、およびローカル コンピュータでのリモート ホスト データベースに対する書き込み権限も必要です。

ユーザがローカル コンピュータ上の **CA ControlMinder** を停止する場合、以下のメッセージが表示されます。

CA ControlMinder は現在停止中です。

リモート ホスト上の **CA ControlMinder** を停止すると、リモート ホスト上の **CA ControlMinder** の停止が正常に行われたかどうかを報告するメッセージが表示されます。1 台のリモート ホスト上の **AC** を正常に停止できなかった場合でも、そのホストの後に指定されているリモート ホスト上の **AC** の停止操作は続行されます。

CA ControlMinder の手動での起動

通常、Windows を起動することで、CA ControlMinder を起動します。

CA ControlMinder を停止した場合は、コマンドプロンプトからコマンドを発行することにより、CA ControlMinder を手動で再起動することができます。

CA ControlMinder を手動で起動するには、以下の手順に従います。

1. Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログオンしていることを確認してください。
2. [コマンドプロンプト] ウィンドウで、CA ControlMinder のバイナリファイルがインストールされているディレクトリに移動します（デフォルトでは、バイナリ ファイルは、システム ディレクトリの C:\Program Files\CA\AccessControl\bin にインストールされています）。
3. 以下のコマンドを入力して、CA ControlMinder を起動します。

```
seosd -start
```

インストールの確認

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

- 以下の Windows レジストリに新しいキーが追加されています。

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl
```

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

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

ログイン保護画面の表示

デフォルトでは、CA ControlMinder をインストールすると、サービスが実行されている場合に、ユーザが対話形式 (GINA) でログインすると、常にログイン保護画面が表示され、このコンピュータが CA ControlMinder により保護されていることをユーザに通知します。

スプラッシュ画面が 4 秒間表示され、自動的に閉じます。

この保護メッセージを無効にするには、

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SplashEnable レジストリ キーの値を 1 から 0 に変更する必要があります。

エンドポイントへの拡張ポリシー管理の設定

拡張ポリシー管理サーバコンポーネントをインストールしたら、拡張ポリシー管理を行うために企業内の各コンピュータを設定する必要があります。その際、サーバコンポーネントとの間で情報の送信先および受信元として機能するエンドポイントを設定します。

注: この手順では、拡張ポリシー管理を行うために **CA ControlMinder** の既存のインストールを設定する方法を示します。エンドポイント上に **CA ControlMinder** をインストールした時にこの情報を指定している場合は、再びエンドポイントを設定する必要はありません。

エンドポイントを設定して拡張ポリシー管理を実行できるようにするには、コマンドウィンドウを開き、次のコマンドを入力します。

```
dmsmgr -config -dhname dhName
```

dhName

エンドポイントが対応する分散ホスト (DH) 名のカンマ区切り形式のリストを定義します。

例: DH__@centralhost.org.com

このコマンドでは、拡張ポリシー管理を行うためにエンドポイントが設定されます。また、定義された DH と動作するようにエンドポイントが設定されます。

注: 詳細については、「リファレンス ガイド」の「dmsmgr -config」コマンドの説明を参照してください。

レポート作成のための Windows エンドポイントの設定

CA ControlMinder エンドポイント管理 およびレポート ポータルのインストールおよび設定の完了後、配布サーバにデータを送信して処理するようにエンドポイントを設定できます。そのためには、レポート エージェントを有効にして設定します。

注: **CA ControlMinder** をインストールすると、レポート作成のためにエンドポイントを設定することが可能になります。この手順では、インストール時にこのオプションを設定しなかった場合、レポートを送信するための既存のエンドポイントを設定する方法について説明します。

レポート作成のための Windows エンドポイントの設定方法

1. [スタート] - [コントロールパネル] - [プログラムの追加と削除] を選択します。
[プログラムの追加と削除] ダイアログ ボックスが表示されます。
2. プログラム リストをスクロールして CA ControlMinder を選択します。
3. [変更] をクリックします。
CA ControlMinder のインストール ウィザードが表示されます。
4. ウィザードのプロンプトに従って CA ControlMinder インストールを変更し、レポート エージェント機能を有効にします。

注: レポート エージェントを有効にしたら、CA ControlMinder 構成設定を変更してパフォーマンス関連の設定を変更できます。 レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

CA ControlMinder のクラスタ環境用へのカスタマイズ

クラスタ環境で CA ControlMinder を使用するには、クラスタの各ノードに CA ControlMinder をインストールする必要があります。各ノードの共通リソース用に一連の同じルール（クォーラム ディスク、またはネットワーク インターセプトを使用している場合はネットワーク）を定義します。

CA ControlMinder では、CA ControlMinder がクラスタ環境で実行されているかどうかを検出できます。CA ControlMinder により、クラスタに別のクラスタの内部通信用ネットワーク アダプタがあることが検出された場合、これらのネットワーク アダプタのネットワーク インターセプトは無効になります。クラスタを企業内の他のネットワークに接続するネットワーク インターフェースについては、ネットワーク インターセプトは通常どおり機能します。

注: クラスタで、クラスタ内部通信用およびネットワークの他の部分との通信用の両方に同じネットワーク インターフェースが使用されている場合、この機能は有効になりません。

例

2つのノードがあると仮定します。

- NODE1 は以下の 2 つの IP アドレスを保持しています。
 - 10.0.0.1 は、内部クラスタ ネットワーク IP アドレスです。
 - 192.168.0.1 は、外部ネットワーク接続用の IP アドレスです。
- NODE2 は以下の 2 つの IP アドレスを保持しています。
 - 10.0.0.2 は、内部クラスタ ネットワーク IP アドレスです。
 - 192.168.0.2 は、外部ネットワーク接続用の IP アドレスです。

クラスタ自体は、これら以外の IP アドレス **192.168.0.3** を保持しています。

NODE1 と NODE2 の間の通信はクラスタ内部ネットワーク用の IP アドレスを使用して行われるため、ネットワーク インターセプトは、これらのノード間で接続が行われることを妨げません。

NODE1 または NODE2 で外部ネットワーク IP アドレスを使用して接続が行われる場合、ネットワーク インターセプトは **CA ControlMinder** のルールで定義したとおりに機能します。

さらに、クラスタの IP アドレス「**192.168.0.3**」に対して接続が行われた場合、ネットワーク インターセプトは **CA ControlMinder** で定義したとおりに機能します。

アンインストールの方法

以下の方法で **Windows** エンドポイントから **CA ControlMinder** をアンインストールすることができます。

- 標準アンインストール - この方法では、グラフィカル インターフェースを使用して **CA ControlMinder** のアンインストールを実行し、ユーザに対し、対話的にフィードバックを行います。
- サイレント アンインストール - この方法では、コマンドラインを使用して、対話形式のフィードバックなしで **CA ControlMinder** をアンインストールします。

CA ControlMinder をアンインストールします。

Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログオンしていることを確認してください。

CA ControlMinder のアンインストール方法

1. （オプション）[CA ControlMinder のシャットダウン](#)（P. 203）を実行します。

注：この操作をユーザが手動で実行しない場合、インストールプログラムが代わりに CA ControlMinder をシャットダウンします。

2. [スタート] - [設定] - [コントロール パネル] を選択します。

Windows の [コントロール パネル] が表示されます。

3. [プログラムの追加と削除] をダブルクリックします。

[プログラムの追加と削除] ダイアログ ボックスが表示されます。

4. インストールされているプログラムのリストから CA ControlMinder を選択し、[追加と削除] をクリックします。
5. CA ControlMinder の削除を確認するメッセージ ボックスで [はい] をクリックします。
6. アンインストールの完了後、[OK] をクリックします。
7. コンピュータを再起動すると、すべての CA ControlMinder コンポーネントが削除されます。

サイレントモードでの CA ControlMinder のアンインストール

対話形式のフィードバックなしで CA ControlMinder をアンインストールするには、コマンドラインを使用して CA ControlMinder をサイレントモードでアンインストールすることができます。Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログオンしていることを確認してください。

CA ControlMinder r12.5 をサイレントモードでアンインストールするには、以下のコマンドを入力します。

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn insert_params_here
```

<insert_params_here> 変数では、インストールプログラムに渡すインストール設定を指定します。たとえば、このコマンドは CA ControlMinder をアンインストールして、c:\¥ac_uninst.log に以下のアンインストールログを作成します。

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn /l*v c:\¥ac_uninst.log
```

注: この操作をユーザが手動で実行しない場合、インストールプログラムが代わりに CA ControlMinder をシャットダウンします。

第 9 章: UNIX エンドポイントのインストール およびカスタマイズ

この章では、CA ControlMinder UNIX エンドポイントのインストールプロセスについて説明します。この章の手順に従って CA ControlMinder のインストールを完了すると、CA ControlMinder エンドポイント ソフトウェアと CA ControlMinder の基本データベースがシステムにインストールされます。次に、CA ControlMinder の起動方法、および関連するコマンドの使用方法について説明します。起動後にデータベースを編集することにより、システムを保護するアクセス ルールを定義できます。

このセクションには、以下のトピックが含まれています。

- [はじめに \(P. 211\)](#)
- [ネイティブ インストール \(P. 238\)](#)
- [通常のスクリプト インストール \(P. 294\)](#)
- [インストール後の設定 \(P. 308\)](#)
- [CA ControlMinder の起動 \(P. 309\)](#)
- [エンドポイントへの拡張ポリシー管理の設定 \(P. 311\)](#)
- [レポート作成のための UNIX エンドポイントの設定 \(P. 312\)](#)
- [CA ControlMinder のカスタマイズ \(P. 313\)](#)
- [メンテナンス モードの保護 \(サイレント モード\) \(P. 323\)](#)
- [Solaris ゾーンへのインストール方法 \(P. 325\)](#)
- [CA ControlMinder の自動起動 \(P. 347\)](#)
- [サービス マネジメント機能による CA ControlMinder の管理 \(P. 348\)](#)

はじめに

CA ControlMinder をインストールするには、事前に準備要件を満たし必要な情報をすべて揃えておく必要があります。

オペレーティング システムのサポートおよび要件

サポートされている UNIX オペレーティング システムのいずれか 1 つに CA ControlMinder をインストールすることができます。

注: 詳細については、「リリース ノート」を参照してください。

管理端末

CA ControlMinder ポリシーを管理するには、CA ControlMinder エンドポイント管理 および CA ControlMinder エンタープライズ管理 を使用して中央から管理するか、コマンドライン (**selang**) を使用してコンピュータに接続し、コンピュータのアクセス ルールを直接更新します。

コンピュータのアクセス ルールを直接更新するには、管理用端末での書き込みアクセス権と、CA ControlMinder データベース内のコンピュータ ポリシーにおける **admin** 属性が必要です。

デフォルトでは、CA ControlMinder をインストールすると、ローカル コンピュータ端末に対してのみ端末許可が設定されます。この設定は変更できます。それには、ローカル端末からこのオプションを無効にするか、リモートで管理可能な端末を追加します。

端末 **my_terminal** の管理オプションを、ユーザ **my_user** を使用してコンピュータ **my_machine** に追加するには、以下の **selang** ルールを作成します。

```
er terminal my_terminal owner(nobody) defaccess(r)
auth terminal my_terminal xuid(my_user) access(all)
```

これらのルールでは、すべてのユーザがこの端末にログインでき (CA ControlMinder 管理ではなく、通常のログイン)、企業ユーザ **my_uid** はコンピュータにログインし CA ControlMinder 管理ツール (**selang** や CA ControlMinder エンドポイント管理 など) を使用できます。

注: 管理者が CA ControlMinder エンドポイント管理 を使用して CA ControlMinder を管理する場合は、CA ControlMinder エンドポイント管理 がインストールされているコンピュータを定義するだけで済みます。管理者によってブラウザが開かれるコンピュータを定義する必要はありません。

インストール上の注意事項

CA ControlMinder をインストール（初回か、アップグレードの一環かに関わらず）する際には、以下の点に注意してください。

- 「リリースノート」をお読みください。

このドキュメントでは、サポートされているプラットフォーム、既知の問題、考慮事項およびその他の重要な情報について説明します。CA ControlMinder をインストールする前に、「リリースノート」をお読みください。

- 対象となる環境が PMDB 階層で設定されている場合、またはそのような環境を設定する場合は、以下の作業を行うことをお勧めします。

- Deployment Map Server (DMS) コンピュータをインストールまたはアップグレードします。

これは拡張ポリシーベース管理を使用する場合にのみ必要な作業です。この作業により、各 Policy Model ノードおよびそのサブスクライバが DMS に確実に登録されます。

- 階層内の各コンピュータのインストールまたは各コンピュータのアップグレードを下から上の順（サブスクライバが最初）で行います。

PMDB のアップグレード時に、旧バージョンを利用しているサブスクライバが存在する場合、誤ったコマンドが送信される場合があります。この問題は、旧バージョンの PMDB に存在しないクラスやプロパティが新しい PMDB に含まれることが原因で発生します。

注: 単一のコンピュータ上で動作する PMDB 階層については、同時にアップグレードすることができます。

- PMDB またはポリシーの更新中にアップグレードを行わないでください。
- サブスクライバおよび PMDB ポリシーをバックアップします。

注: 旧バージョンの PMDB は、新しいバージョンのサブスクライバを保持できます。旧バージョンのコマンドは最新バージョンでもサポートされているため、CA ControlMinder r12.0 のサブスクライバへの古い PMDB の伝播が可能です。

- r12.0 より前のバージョンからアップグレードする場合：
 - STOP によるバイパスが必要なプログラムは、データベース ルールとして定義されるようになります (*stop* タイプの SPECIALPGM レコード)。
 - SURROGATE によるバイパスが必要なプログラムは、データベース ルールとして定義されるようになりました (*surrogate* タイプの SPECIALPGM レコード)。

注: アップグレードプロセスでは、ファイル内に保存されている古い定義が新しいデータベース ルールに変換されます。これらの新しいルールを既存の *selang* スクリプトに追加します。

- 既存の *seos.ini* ファイルおよび *pmd.ini* ファイルをアップグレードすることも、これらのファイルを新規作成することもできます。

いずれの場合も、インストール スクリプトにより、古い *seos.ini* ファイルのコピーが *seos_ini.back* として保存され、各 *pmd.ini* ファイルのコピーが *pmd_ini.back* として保存されます。保存先は、該当する Policy Model ディレクトリです。

- アップグレード中には、CA ControlMinder によって、*serevu.cfg*、*audit.cfg*、*trcfilter.init*、および *sereport.cfg* という既存のファイルがバックアップされます。

これらのファイルの変更内容を保持したい場合は、バックアップ ファイルを使用する必要があります。

- 既存のデータベースをアップグレードする場合は、以下の作業を行うことをお勧めします。
 - まず、データベースをバックアップします。
データベースをバックアップするには、*dbmgr -b* を使用します。
 - *sync* モードのサブスクリイバが存在していないことを確認します。
サブスクリイバのステータスを確認するには、*sepm -L* を使用します。
- Unicenter セキュリティの統合および移行は、AIX、HP-UX PA-RISC、Solaris SPARC、および Linux x86 のプラットフォームでのみサポートされています。

- Unicenter TNG および CA ControlMinder for UNIX

Unicenter NSM 3.0 より古いバージョンの Unicenter TNG がインストールされている場合は、以下の Unicenter TNG 修正プログラムをインストールして、CA ControlMinder でプロセス情報を取得できるようにしてください。

- Unicenter TNG 2.4 運用の HP-UX ユーザの場合：修正プログラム QO01182
- Unicenter TNG 2.4 運用の Linux ユーザの場合：修正プログラム PTF LO91335
- Unicenter TNG 2.4 運用の Sun ユーザの場合：修正プログラム QO00890

注：Unicenter NSM 3.0 運用の AIX 5.x ユーザは、弊社 Unicenter テクニカルサポートにお問い合わせの上、互換性パッチを入手してください。CA ControlMinder をホストにインストールする前に、この互換性パッチをインストールします。

- Linux s390 に Unicenter の関連オプション (install_base オプション: -uni または -mfsd) をインストールするには、CA ControlMinder をインストールする前に、korn シェル (ksh) をインストールしておく必要があります。

CCI Standalone (CCISA) のセットアップスクリプトで ksh を使用しますが、これはデフォルトでは Linux にインストールされません。

- CA ControlMinder32 ビットバイナリを Linux x86 64 ビット上にインストールする場合は、_LINUX_xxx.tar.Z または CAeAC-xxxx-y.y.iii.i386.rpm のいずれかのインストールパッケージを使用することをお勧めします。これらのインストールパッケージは、32 ビットの CA ControlMinder バイナリを 64 ビットの Linux x86 システムにインストールします。アップグレードの場合、これらのパッケージは以前の 32 ビット CA ControlMinder のインストールとの互換性を維持しています。CA ControlMinder をインストールする前に、以下のオペレーティングシステムの 32 ビットライブラリがインストールされていることを確認します。

- ld-linux.so.2
- libICE.so.6
- libSM.so.6
- libX11.so.6
- libXext.so.6
- libXp.so.6
- libXt.so.6
- libc.so.6
- libcrypt.so.1
- libdl.so.2
- libgcc_s.so.1
- libm.so.6
- libncurses.so.5
- libnsl.so.1
- libpam.so.0
- libpthread.so.0
- libresolv.so.2
- libstdc++.so.5
- libaudit.so.0 (RHEL5 および OEL 5)
- libaudit.so.1 (RHEL6 および OEL6 以降のみ)

以下に、必要な関連 RPM パッケージを示します。

- SLES 10: compat-libstdc++, glibc-32bit, libgcc, ncurses-32bit, pam-32bit, xorg-x11-libs-32bit
- SLES 9: glibc-32bit, libgcc, libstdc++, ncurses-32bit, pam-32bit, XFree86-libs-32bit
- RHEL 6: ksh, dos2unix, libgcc_s.so.1, libpthread.so.0, libstdc++.so.6
- RHEL 5 および OEL 5: audit-libs, compat-libstdc++, glibc, libgcc, libICE, libSM, libXext, libXp, libXt, ncurses, pam
- RHEL 4 および OEL 4: compat-libstdc++, glibc, libgcc, ncurses, pam, xorg-x11-deprecated-libs, xorg-x11-libs
- RHEL 3: glibc, libgcc, libstdc++, ncurses, pam, XFree86-libs

- CA ControlMinder 64 ビット バイナリを Linux x86 64 上にインストールするには、`_LINUX_X64_xxx.tar.Z` または `CAeAC-xxxx-y.y.iii.x86_64.rpm` のいずれかのインストールパッケージを使用します。これらのインストールパッケージを使用している場合は、その他に RPM パッケージをインストールする必要はありません。

64 ビットの CA ControlMinder バイナリを 64 ビットの Linux x86 にインストールまたはアップグレードする前に、以下の点に注意が必要です。

- 64 ビットのインストールパッケージは、`selock` や `selogo` などの CA ControlMinder GUI ユーティリティをサポートしていません。
- `install_base` スクリプトが 32 ビットと 64 ビットの両方の `tar` ファイルにアクセスできる場合、`install_base` スクリプトはデフォルトで 32 ビットの `tar` ファイルを使用します。この動作を変更するには、`install_base` コマンドの実行時に使用する `tar` ファイルを指定します。64 ビットの RPM パッケージをインストールする場合は、64 ビットのバイナリとライブラリのみがインストールされます。例：

```
./install_base_LINUX_X64_125.tar.Z
```
- 構築されて API にリンクされているアプリケーションは、64 ビットのインストール用に再構築する必要があります。64 ビットの API サンプルを構築するには、`LINUX64` 系のターゲットを使用します。このターゲットは、`D64BIT` および `-D64BITALL` (`-m32` を削除) を使用します。ライブラリを構築するには、`-m elf_x86_64` が必要です。
- `install_base` スクリプトを使用して 32 ビットの CA ControlMinder インストールから 64 ビットの CA ControlMinder インストールにアップグレードするには、インストールの前に `-force_install` フラグを設定する必要があります。このフラグを設定していない場合、インストールは失敗します。
- CA ControlMinder をアンインストールしてから `cawin` を完全にアンインストールするには、アンインストールプロセスで 32 ビットと 64 ビットの両バージョンの `cawin` が削除されるように `rpm -e --allmatches` を使用してください。

- CA ControlMinder を 64 ビットの Linux s390x にインストールする場合は、以下のオペレーティングシステムの 32 ビット ライブラリがインストールされていることを確認します。
 - ld.so.1
 - libcrypt.so.1
 - libc.so.6
 - libdl.so.2
 - libICE.so.6
 - liblaus.so.1 (SLES 8, RHEL 3)
 - libaudit.so.0 (RHEL 4, RHEL 5)
 - ibm.so.6l
 - ibnsl.so.1
 - libpam.so.0
 - libresolv.so.2
 - libSM.so.6
 - libX11.so.6
 - libXext.so.6
 - libXp.so.6
 - libXt.so.6

以下の RPM パッケージが必要です。

- SLES 10 : glibc-32bit、pam-32bit、xorg-x11-libs-32bit
- SLES 9 : XFree86-libs-32bit、glibc-32bit、pam-32bit
- RHEL 5 : audit-libs、libXp、glibc、libICE、libSM、libX11、libXext、libXt、pam

- RHEL 4 : audit-libs、glibc、pam、xorg-x11-deprecated-libs、xorg-x11-libs
- RHEL 3 : glibc、laus-libs、pam
- Linux s390x 上で、install_base スクリプト CA ControlMinder を使用してインストールを使用する場合は、ca-lic-01.90.04-00.s390x.rpm パッケージの使用を指定して、CA_LIC をインストールします。
- -all オプションを使用して、CA ControlMinder を Linux および Linux-IA64 プラットフォームにインストールする場合、mfsd はインストールされません。
- CA ControlMinder を Solaris にインストールする場合は、SUNWlibc (Sun Workshop Compilers Bundled libC) パッケージをインストールします。
- CA ControlMinder は、Solaris SMF サービスを自動的に使用するためにインストールされています。
- 32 ビットまたは 64 ビットの Linux コンピュータに CA ControlMinder 32 ビット バイナリをインストールする前に、libstdc++.so.5 32 ビット ライブラリがインストールされていることを確認します。このライブラリをインストールしないと、CA ControlMinder のインストール後に ReportAgent デーモンが開始されません。
- CA ControlMinder を Linux にインストールする前に、環境でホーム ディレクトリを指定します。
- Solaris 8 に CA ControlMinder をインストールする前に、libCstd ライブラリ レベルが 1.2 以降であることを確認します。
- エンタープライズ管理サーバをインストールする前に、CA ControlMinder エンドポイント カーネルがアンロードされ、システム内にないことを確認します。

UNIX インストール パラメータ ファイル -- UNIX インストールのカスタマイズ

UNIX パラメータ ファイルには、要件に応じてカスタマイズできるインストールパラメータが含まれています。パラメータ ファイルには、**CA Control Minder** パッケージの特定の領域用のカスタマイズ可能なパラメータが含まれています。特定のパラメータが有効になるには、対応するシェルス変数が設定される必要があります。

パラメータ ファイルはシェル構文に一致し、~~鍵=~~値ペアが含まれる必要があります。インストールするパッケージのパラメータ ファイルを使用します。

このファイルの形式は以下のとおりです。

ADMIN_USERS

ユーザをセキュリティ管理者として定義します。

注: セキュリティ管理者は、認定ユーザへのアクセス権限の割り当て、特権ユーザパスワードの管理、ユーザ アクティビティに関するレポートを実行できます。

値: ユーザ ID のスペース区切りリスト、**none**

デフォルト: **none** (**root** のみがセキュリティ管理者として定義されます)

API_INSTALL

API パッケージをインストールするかどうかを指定します。

値: **yes**、**no**

デフォルト: **no**

APMS_ADMIN_USERS

ローカル ホスト以外の拡張ポリシー管理サーバ コンポーネントの管理者を定義します。

値: ユーザのスペース区切りリスト、**none**

デフォルト: **none**

APMS_DESKTOP

ローカル ホスト以外の拡張ポリシー管理サーバ コンポーネントの管理コンピュータを定義します。

値: コンピュータのスペース区切りリスト、**none**

デフォルト: **none**

APMS_DIST_MODE

拡張ポリシー管理サーバが配布モードで実行されるかどうかを定義します。

値： yes、no

デフォルト： no

AUDIT_BK

監査ファイルのタイムスタンプ付きバックアップを保存するかどうかを指定します。

注：

- 監査データをレポートサーバに送信するには、「yes」を指定します。
- 指定されたサイズ制限に達すると、CA Control Minder は監査ファイルをバックアップします。

値： yes、no

デフォルト： no

AUDIT_GROUP

CA Control Minder 監査ファイルを読み取るグループの名前を指定します。

値： 任意の既存のグループ名、none。

デフォルト： none（root のみが監査ファイルを読み取れます）

注： CA Control Minder アクセスルールを使用してアクセスを拒否しない限り、root ユーザは監査ファイルを読み取ることができます。

CLIENT_INSTALL

クライアントパッケージをインストールするかどうかを指定します。

値： yes、no

デフォルト： yes

DH_NAME

エンドポイント拡張ポリシー管理サーバコンポーネントホスト上の配布ホスト（DH）の名前を定義します。

値： *dh1@host1 dh2@host1* という形式のスペース区切りの DH リスト、none

デフォルト： none

DIST_SRV_HOST

メッセージキュー ホスト名を定義します。

値：有効なホスト名のカンマ区切りリスト、none

デフォルト：none

DIST_SRV_PORT

メッセージキューのポートを定義します。

値：7243 (ssl プロトコルの場合)、7222 (ssl 以外のプロトコルの場合)

デフォルト：7243

DIST_SRV_PROTOCOL

メッセージキューの通信プロトコルを定義します。

値: ssl、tcp

デフォルト：ssl

DRDH_NAME

エンドポイントディザスタリカバリ配布ホスト (DR DH) の名前を定義します。

値: *dr_dh1@drhost dr_dh2@drhost* 形式の DR DH のカンマ区切りリスト、none

デフォルト：none

ENABLE_ELM

CA Control Minder がレポート サーバにエンドポイント監査データを送信するかどうかを指定します。

注：「yes」を指定すると、CA Control Minder は監査バックアップを保持するように設定されます (AUDIT_BK=yes)。

値：yes、no

デフォルト：no

ENABLE_KBL

CA Control Minder が KBL 監査レコードマネージャを有効にするかどうかを指定します。

値：yes、no

デフォルト：no

ENCRYPTION_METHOD_SET

対称暗号化、非対称暗号化（公開鍵）またはその両方を使用するかどうかを定義します。

値： 1（対称鍵）、2（公開鍵）、3（公開鍵および対称鍵）

デフォルト： 1

注：

- 公開鍵暗号化については、ルート証明書が必要です。
- 対称暗号化については、暗号化方式（TRIPLEDES、DES または AES）を選択します。
- FIPS のみの暗号化を設定する場合は、FIPS_ONLY パラメータを「yes」に設定します。

重要: 暗号化方式は、すべての CA Control Minder ホスト上で同じである必要があります。CA Control Minder の旧リリースでは、デフォルトで単純な対称暗号化方式が設定されました。

ETC_SEOS_SYMLINK

CA Control Minder インストールディレクトリを参照するリンクが /etc ディレクトリ内に作成されるかどうかを定義します。

値： yes、no

デフォルト： yes

FIPS_ONLY

CA Control Minder が FIPS 専用モードで動作するかどうかを指定します。

注: このモードでは、FIPS 以外の機能はすべて無効になり、暗号化方法は FIPS のみに設定されます。

値： yes、no

デフォルト： no

FORCE_ENCRYPT

デフォルトではない暗号化鍵の使用について、ユーザに対して警告するかどうかを指定します。

注: アップグレードが完了すると、暗号化鍵はデフォルトに設定されます。

値： yes、no

デフォルト： no

FORCE_INSTALL

同じ CA Control Minder バージョンの既存のインストールに対する上書きインストールを強制的に行うかどうかを指定します。

FORCE_INSTALL は、インストールディレクトリが新規 CA Control Minder パッケージで設定されたインストールディレクトリと異なるかどうかを指定します。

値： yes、no

デフォルト： no

FORCE_KERNEL

古いカーネル モジュールをアンロードできない場合に、ユーザに対して警告するかどうかを指定します。

注：「no」を指定した場合、アップグレードの完了後に、システムが再起動されます。

値： yes、no

デフォルト： no

INST_PHASE1

ベースライン セキュリティ パックをインストールするかどうかを指定します。

注：

- ベースライン セキュリティ パックは、オペレーティング システムを保護する基本的なルールを定義します。
- インストール後に、*install_baseline.sh* ユーティリティを使用して、ベースライン セキュリティ パックをインストールできます。
- インストール試験期間（推奨）の後にルール保護をアクティブにするには、警告モードを無効にします。

値： yes、no

デフォルト： no

INSTALL_ACCOUNT_MNG

エンドポイント JCS 管理を設定するかどうかを指定します。

注：アカウント マネージャを設定するには、[配布サーバ] パラメータを設定します。

値： yes、no

デフォルト： no

INSTALL_APMC

拡張ポリシー管理用のエンドポイントを設定するかどうかを指定します。

注: 拡張ポリシー管理サーバ コンポーネントから更新を受信するように、各 CA Control Minder エンドポイントを設定する必要があります。

値: yes、no

デフォルト: yes

INSTALL_APMS

管理対象ポリシー デプロイメントを一元管理するために、拡張ポリシー管理サーバ コンポーネントをインストールするかどうかを指定します。

注: 拡張ポリシー管理サーバ コンポーネントを中央コンピュータにインストールすることをお勧めします。

値: yes、no

デフォルト: no

INSTALL_PUPM

PUPM エージェントを設定するかどうかを指定します。

値: yes、no

デフォルト: no

INSTALL_RA

エンドポイント メッセージ キューを設定するかどうかを指定します。

値: yes、no

デフォルト: no

JAVA_HOME

インストールされている Java 環境のパスを定義します。

注: Java 環境パスは、バージョンとプラットフォームに依存します。たとえば Linux390 上にインストールされている IBM J2SE バージョン 5.0 では、`JAVA_HOME=/opt/ibm/java2-s390-50/jre` です。

値: インストールされている Java 環境のパス

デフォルト: java_home (accommon.ini 内の値はインストール中に設定されます)

JCS_SERVER_DN

JCS サーバの識別名 (DN) を指定します。

値：有効な DN 形式文字列

デフォルト：dc=im、dc=etasa

JCS_SERVER_PORT

JCS ポートを指定します。

値：ポート番号

デフォルト：20411

JCS_SSL

JCS 通信プロトコルを定義します。

値：yes (SSL 接続の場合)、no

デフォルト：yes

JCS_USER_DN

JCS 管理ユーザの識別名 (DN) を指定します。

値：有効な DN 形式文字列

デフォルト：cn=root,dc=etasa

JCS_USER_PSSWD

JCS 管理ユーザ パスワードを指定します。

注: インストール後に、JCS_USER_PSSWD はワイルドカード (*) に置換されます。

値：有効な DN 形式文字列

デフォルト：デフォルト値なし

LANG

CA Control Minder インストール言語を定義します。

例：日本語の EUC サポート付きで CA Control Minder をインストールするには、`LANG=ja_JP` を指定します。サポートされている全言語のリストについては、コマンド `locale -a` を入力します。

注：

- ローカライズされている HP-UX パッケージをインストールするには、このトークンを設定します。
- このパラメータを指定すると、インストーラの LANG 環境変数は無視されます。

値： サポートされている言語文字列

デフォルト： English

LIB_ENCRYPTION

<eCA> プログラムと CA Control Minder がインストールされているホストとの間の通信を保護するために使用される暗号化方法を定義します。

注：

- この暗号化方法は、相互に通信するすべての CA Control Minder ホスト上で同じである必要があります。
- このオプションでは、SET_SYMMETRIC が「yes」に設定される必要があります。

値： 99 (AES2526) 、 1 (SCRAMBLE) 、 2 (DES) 、 3 (TRIPLEDES) 、 4 (AES128) 、 5 (AES192)

デフォルト： 99

LIC_CMD

使用許諾契約を承認するコマンドを定義します。

注：

- このコマンドは、使用許諾契約内で角かっこで囲まれています。
- 使用許諾契約ファイルは「eACLlicenseAgreementUNIX_japanese_cp1252.txt」です。

重要： LIC_CMD コマンドは、CA Control Minder のインストールに必要です。

LIC_INSTALL_DIR

CA ライセンスのインストール場所を定義します。

値： 任意の絶対パス名。

デフォルト： /opt/CA/SharedComponents (lic98 のデフォルトと同じ)

LOG_FILE_NAME

\$SEOSDIR で作成されるインストール ログ ファイル名を定義します。

値： 任意の有効なファイル名。

デフォルト： AccessControl_install.log

MFSD_INSTALL

メインフレーム同期サポート デーモンをインストールするかどうかを指定します。

値： yes、no

デフォルト： no

NO_TNG_INT

selogrd/TNG 統合をセットアップするかどうかを指定します。

値： yes (selogrd/TNG 統合セットアップの試行)、no (selogrd/TNG 統合は発生しません)

デフォルト： no

OS_USERS

OS データベース管理者を指定します。

値： ユーザのスペース区切りリスト、none

デフォルト： none

PARENT_PMD

このコンピュータが更新を受け取る **Policy Model** データベース (PMDB) のカンマ区切りリストを定義します。

注: ローカルの **CA Control Minder** データベースは、このリストに指定されていない PMDB からの更新情報を拒否します。

値: `_NO_MASTER_` (ローカル データベースは任意の PMDB から更新を受け取ります)、`pmd1@host1`、`pmdb2@host1` 形式の PMDB のカンマ区切りリスト、PMDB の行区切りリストが含まれるファイルのパス、`none` (ローカル データベースは任意の PMDB からの更新を受け取りません)。

デフォルト: `none`

PASSWD_PMD

`sepass` がパスワード更新を送信する、**Policy Model** データベース (PMDB) を指定します。

値: `pmd_name@hostname` 形式の PMDB、`none`

デフォルト: `none`

注:

- パスワード更新は、パスワード履歴の確認をサポートします。
- `PASSWD_PMD` を設定しない場合、`PARENT_PMD` の値が継承されます。
- `PARENT_PMD` トークンと `PASSWORD_PMD` トークンに同じ値を指定できます。
- `PARENT_PMD` と `PASSWORD_PMD` の値が同じでない場合、`PARENT_PMD` データベースは `PASSWORD_PMD` データベースの子 (サブスクライバ) である必要があります。

POSTEXIT

ポスト インストール スクリプトの実行後に実行される、プログラムまたはスクリプトの完全パス名を定義します。

値: `yes`、パス名

デフォルト: `no`

PREINSTALL

ポスト インストール スクリプトの実行前に実行される、プログラムまたはスクリプトの完全パス名を定義します。

値： yes、パス名

デフォルト： no

PRIMARY_ENTM_NAME

プライマリ エンタープライズ管理サーバのホスト名を定義します。

値： 文字列、none

デフォルト： none

PROVIDE_OR_GEN_CERT

ユーザが所有者証明書および鍵を生成するか、既存の所有者証明書および鍵を指定するかどうかを指定します。

注：

- SSL をセットアップするには、所有者証明書、鍵、およびルート証明書を指定します。
- SSL 通信を使用するすべてのコンピュータで、ルート証明書は共通である必要があります。
- デフォルト証明書、または指定する証明書から所有者証明書およびキーを自動的に生成できます。 または、**CA Control Minder** が既存の証明書を参照するように設定することもできます。

値： 1（所有者証明書および鍵を生成します）、2（既存の証明書および鍵を指定します）

デフォルト： 1

PWFORCE

PMDB 更新実行中の、アップグレード動作を定義します。

注:

- CA Control Minder をアップグレードする場合は、また Policy Model 更新ファイルもアップグレードします。
- `sepmc -n` コマンドの実行中は、パッケージのインストールが異常終了し、`sempd` が処理を終了します。このパラメータを「yes」に設定して、強制的にインストールできますが、実行中の `sepmc` が正常に完了しない場合があります。

値: yes、no

デフォルト: no

REPORT_SHARED_SECRET

メッセージキュー SSL 認証用の共有秘密鍵を定義します。

注: インストール後に、共有秘密鍵はワイルドカード (*) に置換されます。

値: 任意の文字列

デフォルト: 空の値

REPORT_SRV_QNAME

レポート送信時の、キューの名前を定義します。

制限: キュー名を表す文字列

デフォルト: queue/snapshots

REPORT_SRV_SCHEDULE

レポートが生成され、レポート サーバに送信される日時を定義します。

値: 「時刻@日付,曜日」という形式の、日付と時刻を表す文字列

例: 19:22@Sun, Mon。 (この例では、毎週日曜日と月曜日の 19 時 22 分にレポートを生成します)。

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

ROOT_CERT_KEY

所有者キーの生成に使用される公開鍵を指定します。

値: 所有者証明書の完全パス名。デフォルト。

デフォルト: デフォルト (インストールパッケージで提供される鍵)

ROOT_CERT_PATH

所有者証明書の生成に使用されるルート証明書を指定します。

値：所有者証明書の完全パス名。デフォルト。

デフォルト：デフォルト（インストールパッケージで提供されるルート証明書）

SELINUX_POLICY

UNIX 認証ブローカ がインストール中に SELinux ポリシーをアクティブにするかどうかを指定します。

値： yes、no

デフォルト： no

SEOS_GROUP

CA Control Minder ファイルを所有するグループの名前を定義します。

値： 任意の既存のグループ名。

デフォルト： root

SERIAL_NUM

所有者証明書のシリアル番号を定義します。

注：所有者証明書のシリアル番号を定義するには、CA Control Minder でデフォルト値を使用するか、ユーザの入力を使用します。

値： 有効なシリアル番号、0003ba39cc23

制限： 3 から 247 文字

デフォルト： 0003ba39cc23

SERVER_INSTALL

サーバパッケージをインストールするかどうかを指定します。

値： no、yes

デフォルト： yes

SET_SYMMETRIC

デフォルトの対称暗号化方式を変更するかどうかを指定します。

注:

- 暗号化は、CA Control Minder プログラムと CA Control Minder のインストール済みホストの間の通信を保護します。
- 推奨される（デフォルトの）暗号化方式は、公開鍵と対称メソッドの組み合わせです。
- 対称暗号化を設定するには、LIB ENCRYPTION を設定します。

値: yes、no

デフォルト: yes

SUBJECT_CERT_KEY_PATH

公開鍵の場所を指定します。

値: 所有者証明書ファイルの完全パス名。

デフォルト: SEOSDIR>/data/crypto/sub.key

SUBJECT_CERT_PATH

所有者証明書の場所を指定します。

注: 所有者証明書を生成するには、ファイルの場所を指定します。

値: 所有者証明書ファイルの完全パス名。

デフォルト: SEOSDIR>/data/crypto/sub.pem

SUBJECT_EXP_DATE

所有者証明書の有効期限を定義します。

注: 所有者証明書の有効期限を定義するには、CA Control Minder でデフォルト値を使用するか、ユーザの入力を使用します。

値: *mm/dd/yy* 形式の日付

デフォルト: 12/31/35

SUBJECT_NAME

所有者証明書の名前を定義します。

注: 所有者証明書の名前を定義するには、CA Control Minder でデフォルト値を使用するか、ユーザの入力を使用します。

値: LDAP 形式の名前。cn=any.string

制限: 3 から 63 文字

デフォルト: c=any.string

TNG_INSTALL

Unicenter 統合および移行パッケージをインストールするかどうかを指定します。

注: このパッケージは、CAUTIL、Workload Management および Unicenter のイベント管理コンポーネントとの CA Control Minder 統合および移行をサポートします。

値: yes、no

デフォルト: no

UPDATE_ENCRYPT

CA Control Minder プログラムと CA Control Minder のインストール済みホストとの間の通信を保護するデフォルトの暗号化方式を変更するかどうかを指定します。

値: yes、no

デフォルト: yes

UPDATE_PROFILE

CA_LIC がファイル */etc/profile* を *profile.ca* のロードで更新するかどうかを定義します。

値: yes、no

デフォルト: yes

UPGRADE_KERNEL_UNLOAD

別のバージョンをインストールする場合に、インストーラが CA Control Minder の既存バージョンの停止およびアンロードを試行するかどうかを指定します。

値: yes、no

デフォルト: yes

USE_OSUSER

OS ユーザのサポートを有効にします。

注: OS ユーザは、CA Control Minder データベースではなく OS リポジトリで定義されています。OS ユーザサポートを有効にすると、CA Control Minder データベースで定義されていないユーザを参照できます。

値 : yes、no

デフォルト : yes

USE_STOP

CA Control Minder の STOP (Stack Overflow Protection) 機能を有効にするかどうかを指定します。

値 : yes、no

デフォルト : no

USE_UXIMPORT

CA Control Minder がネイティブ ユーザとグループをデータベースへインポートするかどうかを指定します。

値 : yes、no

デフォルト : no

注: インポート プロセスはローカル ホスト ファイルを使用します。または、ローカル NIS は情報源としてマップされます。ユーザおよびグループのインポートに必要な時間は、定義されているユーザ、グループおよびホストの数に応じて異なります。また、UxImport ユーティリティを使用して、インストール後に、このデータを CA Control Minder データベースへインポートできます。

UserBrandZone

(Solaris 10 のみ) ブランドゾーンに CA Control Minder がインストールされること、または CA Control Minder がインストールされたブランドゾーンが設定されることを指定します。

注: この値を **yes** に設定すると、インストールによってカーネル通信モードが **sysscall** ではなく **iotcl** を使用するように変更されます。

値: yes、no

デフォルト: no

WITH_DNS

インストール中に、ホスト ルックアサイド データベースを作成するために DNS を使用するかどうかを指定します。

値: yes、no

デフォルト: yes

Linux s390 エンドポイントのインストールの考慮事項

CA ControlMinder Linux s390 で UNAB をリモート管理し、Linux IA64 上でレポート機能を使用するためにメッセージキュー機能を使用する場合、J2SE バージョン 5.0 以降をエンドポイントにインストールします。

メッセージキュー機能を使用すると、CA ControlMinder エンドポイントからレポート ポータルおよび CA Enterprise Log Manager に、それぞれレポートおよび監査データを送信することができます。 リモート管理では、CA ControlMinder エンタープライズ管理を使用して UNAB エンドポイントを管理できます。

エンドポイントに CA ControlMinder や UNAB をインストールする前または後に、J2SE をインストールできます。 CA ControlMinder または UNAB をインストールした後に J2SE をインストールする場合、エンドポイント上に Java の場所も設定する必要があります。

インストール時の Java の設定

Linux s390、Linux s390x および Linux IA64 で有効

UNAB Linux s390 エンドポイントをリモート管理し、Linux IA64 でレポート機能を使用するためにメッセージキュー機能を使用する場合、サポートされている Java のバージョンをエンドポイントにインストールします。

Linux s390 または Linux IA64 エンドポイントに CA ControlMinder または UNAB をインストールすると、以下が実行されます。

1. 有効な Java 環境へのパスを以下の順序で確認します。
 - a. インストール時の入力データの `JAVA_HOME` パラメータ。
インストール時の入力データには、対話型の CA ControlMinder インストールで入力された UNAB インストール パラメータ ファイル、UNIX CA ControlMinder インストール パラメータ ファイル、ネイティブ インストール用のカスタマイズされたパッケージ、およびユーザ入力データがあります。
 - b. `JAVA_HOME` 環境変数。
 - c. (Linux s390 および Linux s390x) デフォルトのインストール パス、`/opt/ibm/java2-s390-50/jre`
2. `accommon.ini` ファイルのグローバル設定で `java_home` 設定の値を以下のいずれかの値に設定します。
 - 有効な Java 環境へのパスがインストール時に見つかった場合、値はこのパスに設定されます。
 - 有効な Java 環境へのパスがインストール時に見つからなかった場合、値は `ACSharedDir/JavaStubs` に設定されます。デフォルトでは、`ACSharedDir` は `/opt/CA/AccessControlShared` です。

Linux s390 および Linux s390x エンドポイント上で Java の場所を設定します。

Linux s390 および Linux s390x に該当

メッセージ キュー機能を使用し、UNAB Linux s390 エンドポイントをリモートで管理するには、エンドポイントに J2SE バージョン 5.0 以降をインストールする必要があります。CA ControlMinder または UNAB をインストールした後に J2SE をインストールする場合、追加の設定手順を実行する必要があります。

Linux s390 および Linux s390x エンドポイント上で Java の場所を設定する方法

1. CA ControlMinder および UNAB が実行されている場合は停止します。
2. accommon.ini ファイルのグローバルセクション内の java_home 設定の値を、Java のインストールパスに変更します。

例 : java_home=/opt/ibm/java2-s390-50/jre

3. CA ControlMinder および UNAB を開始します。
Java の場所が設定されます。

ネイティブ インストール

CA ControlMinder に用意されているネイティブ パッケージ形式を使用すると、サポートされているオペレーティング システム上で、CA ControlMinder をネイティブにインストールおよび管理できます。ネイティブ パッケージでは、ネイティブ パッケージ管理ツールを使用して、インストールされた CA ControlMinder を管理できます。

ネイティブ パッケージ

CA ControlMinder には、サポートする各ネイティブ インストール形式について、ネイティブ パッケージがあります。これらのパッケージでは、ネイティブ パッケージ機能を使用して、CA ControlMinder コンポーネントのインストール、更新、および削除を管理できます。ネイティブ パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

以下は、パッケージとその説明です。

ca-lic

(Linux のみ) 他のすべてのパッケージの前提条件となる CA Technologies ライセンス プログラムをインストールします。

注: Linux の場合は RPM 形式でのみ提供されます。

CAeAC

中心となる CA ControlMinder コンポーネントをインストールします。これは、メインの CA ControlMinder インストールパッケージです。サーバ、クライアント、ドキュメント、TNG 統合、API、および mfsd の各パッケージの組み合わせです。これらのパッケージは、従来は別々に提供されていました。

注: UNAB パッケージでは、CAWIN 共有コンポーネントもインストールされます。

一部のネイティブ コマンド (RPM でのパッケージの削除など) を実行するには、パッケージの名前を知る必要があります。パッケージファイルを使用してパッケージの名前を確認するには、適切なネイティブ パッケージ コマンドを入力します。たとえば、RPM パッケージの場合は、以下のように入力します。

```
rpm -q -p RPMPackage_filename
```

ネイティブ インストールの際に考慮するその他の事項

ネイティブ パッケージングを使用して CA ControlMinder をインストールするときは、以下の点に注意してください。

- CA ControlMinder RPM パッケージをインストールするには、ライセンス プログラムパッケージ ca-lic-01.0080 以上が必要です。

- `/etc/profile.CA` が環境にロードされないようにするには、`CA_LIC` パッケージをインストールする前に、以下の環境変数を設定します。

```
setenv Update_Profile0
```

- カスタム `CA ControlMinder RPM` ネイティブ インストールパッケージ (`customize_eac_rpm`) を作成するには、ご使用のコンピュータで `rpmbuild` ユーティリティが使用可能である必要があります。
- カスタム `CA ControlMinder AIX` ネイティブ インストールパッケージ (`customize_eac_bff`) を作成するには、コンピュータに `bos.adt.insttools` をインストールする必要があります。

AIX 5.2 の場合、`bos.adt.insttools` のバージョンは 5.2.0.75 以降である必要があります。

- AIX ネイティブ パッケージは、`bos.rte.install 5.2.0.75` で作成されます。したがって、ネイティブ パッケージングをエラーなしに操作するには、`bos.rte.install 5.2.0.75` 以降を使用することをお勧めします。
- HP-UX ネイティブ パッケージは、インストール時に Perl を使用します。
- Solaris ネイティブ パッケージは、グループおよび全員に対する読み取りアクセス権が設定された公開場所 (`/var/spool/pkg` など) に配置される必要があります。
- Solaris ネイティブ パッケージ コマンド `pkgadd -R` は、`CA ControlMinder` パッケージではサポートされていません。

インストールディレクトリを変更するには、`CA ControlMinder` パッケージカスタマイズスクリプトを使用します (`customize_eac_pkg -i install_loc`)。

- HP-UX ネイティブ パッケージのローカライズされたバージョンをインストールする場合は、必ず、カスタマイズされたパッケージに使用するパラメータ ファイル内の **LANG** 設定の値を設定してください。

注: パラメータ ファイルには、すでに **LANG** 設定が含まれています。設定するには、先頭のコメント文字 (`#`) およびスペースを削除し、値を入力します。 `locale -a` コマンドを使用すると、OS がサポートしているエンコーディング値を見ることができます。

CA ControlMinder でパスワード保護されたルート証明書を使用するよう指定する方法

CA ControlMinder をインストールする際は、パスワード保護されたサードパーティのルート証明書を使用するように設定することができます。

CA ControlMinder をインストールした後、ルート証明書を使用して CA ControlMinder サーバ証明書を作成します。サーバ証明書は、CA ControlMinder コンポーネント間の通信を暗号化および認証します。

パスワード保護されたサードパーティのルート証明書を使用するよう CA ControlMinder を設定するには、ネイティブ パッケージを使用して CA ControlMinder をインストールする際に、いくつかの手順を以下のとおり追加で実行する必要があります。

1. ネイティブ パッケージ インストールの一部として `params` ファイルをカスタマイズする際に、ファイル内の以下のパラメータを指定します。
 - `ENCRYPTION_METHOD_SET=2`
 - `ROOT_CERT_PATH=root_cert_path`
 - `ROOT_CERT_KEY=root_key_path`
2. CA ControlMinder をインストールした後、以下を実行します。
 - a. ルート証明書から CA ControlMinder サーバ証明書を以下のとおり作成します。`ACInstalldir` は、CA ControlMinder がインストールされたディレクトリです。

```
ACInstalldir/bin/sechkey -e -sub -in
/opt/CA/AccessControl/crypto/sub_cert_info -priv root_key_path -capwd
password [-subpwd password]
-priv root_key_path
```

ルート証明書の秘密鍵を保持するファイルを指定します。

```
-ca password
```

ルート証明書の秘密鍵用のパスワードを指定します。

```
-subpwd password
```

サーバ証明書の秘密鍵用のパスワードを指定します。

- b. サーバ鍵のパスワードを指定した場合は、CA ControlMinder で保存されたパスワードを使用して鍵を開くことができることを確認します。

```
ACInstalldir/bin/sechkey -g -verify
```

- c. **crypto** セクション内の **communication_mode** 設定の値を以下のいずれかに変更します。

all_modes

対称鍵暗号化および **SSL** 暗号化の両方を有効にする場合は、この値を指定します。この値を指定すると、すべての **CA ControlMinder** コンポーネントとコンピュータが通信できるようになります。

use_ssl

SSL 暗号化のみを有効にする場合は、この値を指定します。この値を指定すると、**SSL** 暗号化を使用する **CA ControlMinder** コンポーネントのみとコンピュータが通信するようになります。

- d. **CA ControlMinder** を起動します。

CA ControlMinder が起動し、**CA ControlMinder** サーバ証明書を使用して通信を暗号化および認証します。

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

CA ControlMinder でパスワード保護されたサードパーティのサーバ証明書を使用するよう指定する方法

パスワード保護されたサードパーティのサーバ証明書を使用して、**CA ControlMinder** コンポーネント間の通信を暗号化および認証することができます。

パスワード保護されたサードパーティのサーバ証明書を使用するよう **CA ControlMinder** を設定するには、ネイティブ パッケージを使用して **CA ControlMinder** をインストールする際に、以下のとおりいくつかの手順を追加で実行する必要があります。

1. ネイティブ パッケージ インストールの一部として **params** ファイルをカスタマイズする際に、ファイル内の以下のパラメータを指定します。
 - **ENCRYPTION_METHOD_SET=2**
 - **ROOT_CERT_PATH=root_cert_path**
 - **ROOT_CERT_KEY=root_key_path**
 - **PROVIDE_OR_GEN_CERT=2**

- SUBJECT_CERT_PATH=*server_cert_path*
- SUBJECT_KEY_PATH=*subject_key_path*

2. CA ControlMinder をインストールした後、以下を実行します。

- a. 秘密鍵のパスワードをコンピュータに以下のとおり保存します。
ACInstallDir は CA ControlMinder をインストールしたディレクトリです。

```
ACInstallDir/bin/sechkey -g -subpwd password
-subpwd password
```

サーバ証明書の秘密鍵用のパスワードを指定します。

- b. CA ControlMinder で、保存されたパスワードを使用して鍵を開くことができることを確認します。

```
ACInstallDir/bin/sechkey -g -verify
```

- c. **crypto** セクション内の **communication_mode** 設定の値を以下のいずれかに変更します。

all_modes

対称鍵暗号化および SSL 暗号化の両方を有効にする場合は、この値を指定します。この値を指定すると、すべての CA ControlMinder コンポーネントとコンピュータが通信できるようになります。

use_ssl

SSL 暗号化のみを有効にする場合は、この値を指定します。この値を指定すると、SSL 暗号化を使用する CA ControlMinder コンポーネントのみとコンピュータが通信するようになります。

- d. CA ControlMinder を起動します。

CA ControlMinder が起動し、パスワード保護されたサードパーティのサーバ証明書を使用して、通信を暗号化および認証します。

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

RPM Package Manager のインストール

RPM Package Manager (RPM) は、個々のソフトウェア パッケージを作成、インストール、クエリ、確認、更新、および消去することができるコマンドラインユーティリティです。RPM は、Fedora、Red Hat Enterprise Linux、CentOS などの Linux プラットフォームで使用されます。

注: 詳細については、RPM Package Manager の Web サイト (<http://www.rpm.org>) および RPM に関する UNIX のマニュアル ページを参照してください。

通常のインストールの代わりに、CA ControlMinder に用意されている RPM パッケージを使用することができます。これにより、インストールした CA ControlMinder を、RPM を使用してインストールされた他のソフトウェアと同様に管理できます。

RPM データベースからの既存の RPM パッケージの削除

自分で作成した CA ControlMinder RPM パッケージがすでにインストールされている場合は、そのパッケージを RPM データベースから削除する必要があります。これにより、新たにインストールされたパッケージがデータベースに反映されます。既存のパッケージを削除することなく新しいパッケージをインストールした場合、RPM データベースでは古いパッケージと新しいパッケージの両方がインストールされていると示されますが、ファイル システムでは、既存のファイルが新しいパッケージのファイルによって上書きされます。RPM でパッケージをアップグレードする場合、パッケージの名前は現在インストールされているパッケージと同じ名前にする必要があります。

注: パッケージを削除しても CA ControlMinder ファイルは削除されません。ネイティブ パッケージをインストールすると、アップグレードされます。

RPM データベースからパッケージを削除するには、以下のコマンドを使用します。

```
rpm -e --justdb your_ACPackageName
```

CA ControlMinder RPM パッケージのカスタマイズ

ネイティブ パッケージを使用して **CA ControlMinder** をインストールする前に、**CA ControlMinder** パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストールパラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、**CA ControlMinder** パッケージをカスタマイズしてください。

サポートされた各 Linux オペレーティングシステムに対する RPM パッケージは、**CA ControlMinder Endpoint Components for UNIX DVD** の **NativePackages/RPMPackages** ディレクトリにあります。

次の手順に従ってください:

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所にコピーします。

OS は、オペレーティングシステム上の適切なサブディレクトリ名です。

ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

2. **customize_eac_rpm** スクリプト ファイルおよび **pre.tar** ファイルをファイル システム上の一時的な保存場所にコピーします。

pre.tar ファイルは、圧縮された **tar** ファイルであり、インストール メッセージおよび **CA ControlMinder** のエンド ユーザ使用許諾契約が含まれています。

注: **customize_eac_rpm** スクリプト ファイルと **pre.tar** ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

```
customize_eac_rpm -a [-d pkg_location] pkg_filename
```

4. 使用許諾契約の最後に表示される、角かっこで囲まれているキーワードをメモします。

次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA ControlMinder パッケージをカスタマイズします。

```
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
```

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

6. (オプション) インストールパラメータ ファイルの言語を設定します。

```
customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename
```

7. (オプション) eTrust Access Control r8 SP1 パッケージからアップグレードします。

```
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
```

8. (オプション) デフォルトの暗号化ファイルを変更します。

```
customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename
```

9. (オプション) インストールパラメータ ファイルを取得します。

```
customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename
```

10. (オプション) インストール要件に合わせて、インストールパラメータ ファイルを編集します。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。たとえば、POSTEXIT 設定（前の # 文字を削除します）をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション) カスタマイズしたパッケージのインストールパラメータを設定します。

```
customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA ControlMinder をインストールできるようになりました。

注: 実際に使用するコマンドは、アップグレードなのか初回インストールなのか、またはデフォルトのディレクトリへのインストールなのかなど、さまざまな要因によって異なります。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。以下の例では、CA ControlMinder Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント) にある x86 CA ControlMinder RPM パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、CA ControlMinder をインストールできるようになりました。

詳細情報:

[customize_eac_rpm コマンド - RPM パッケージのカスタマイズ \(P. 251\)](#)

CA ControlMinder RPM パッケージのインストール

インストールした CA ControlMinder を、インストールされた他のソフトウェアと同様に管理するには、CA ControlMinder RPM パッケージをカスタマイズしてインストールします。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

注: 実際に使用するコマンドは、アップグレードなのか初回インストールなのか、またはデフォルトのディレクトリへのインストールなのかなど、さまざまな要因によって異なります。 コマンドの例は、このトピックに記述されています。

CA ControlMinder RPM パッケージをインストールする方法

1. rpm コマンドを使用して、ca-lic パッケージをインストールします。
ライセンス プログラムがインストールされます。

2. [CAeAC パッケージのカスタマイズ](#) (P. 245)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

注: CA ControlMinder をアップグレードしている場合は、使用許諾契約への同意を指定するためにパッケージをカスタマイズする必要はありません。

3. rpm コマンドを使用して、CAeAC パッケージをインストールします。
CA ControlMinder がインストールされます。

注: UNAB パッケージでは、CAWIN 共有コンポーネントもインストールされます。

重要: 既存の CA ControlMinder パッケージをアップグレードする場合は、SEOS syscall をアンロードしてから、新しいパッケージのインストールを試みます。そうしない場合は、インストールに失敗します。

例: Red Hat Linux に CA ControlMinder をインストールする、または Red Hat Linux 上の CA ControlMinder をアップグレードする

以下の例では、CA ControlMinder Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント) にある CA ControlMinder パッケージを Red Hat Linux x86 ES 4.0 コンピュータにインストールする方法を示します。この方法により、CA ControlMinder の新規インストールを行ったり、現在インストールされている CA ControlMinder RPM パッケージのアップグレード (インストールされているパッケージを最初に削除する必要はなし) を行ったりすることが可能です。そのためには、ライセンス プログラム パッケージをインストールし、以下のように CA ControlMinder パッケージをカスタマイズし、使用許諾契約に同意してインストールするようにします。

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX
rpm -U ca-lic*i386.rpm ca-cs-cawin*i386.rpm
cp CAeAC*i386.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*i386.rpm
rpm -U /tmp/CAeAC*i386.rpm
```


例: eTrust Access Control r8 SP1 パッケージのインストールからのアップグレード

/opt/CA/eTrustAccessControl にインストールされている eTrust Access Control r8 SP1 パッケージを、Linux s390 SLES 9 コンピュータの CA ControlMinder Endpoint Components for UNIX DVD (/mnt/AC_DVD に搭載) にある CA ControlMinder パッケージにアップグレードする方法について、以下に例を示します。これを行うには、以下の手順を使用して、ライセンス プログラム パッケージ、CAWIN パッケージ、およびカスタマイズされた CA ControlMinder パッケージをこの順番でインストールします。

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390
rpm -U ca-lic*rpm ca-cs-cawin*rpm
cp -R CAeAC*s390.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /opt/CA -d /tmp CAeAC*s390.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*s390.rpm
rpm -U /tmp/CAeAC*s390.rpm
```

例: カスタム ディレクトリに CA ControlMinder および必須パッケージをインストールする

以下の例では、CA ControlMinder Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント) にあるデフォルトの CA ControlMinder および必須パッケージを、Red Hat Linux Itanium IA64 ES 4.0 のカスタム ディレクトリにインストールする方法を示します。これを行うには、以下のコマンドを使用します。

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX_IA64
rpm -U --prefix /usr/CA/shared ca-lic*ia64.rpm
cp -R CAeAC*ia64.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*ia64.rpm
../customize_eac_rpm -u /usr/CA -d /tmp CAeAC*ia64.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*ia64.rpm
rpm -U --prefix /usr/CA /tmp/CAeAC*ia64.rpm
```

CA ControlMinder は、指定したカスタム ディレクトリと製品の名前 (Access Control) を連結した /usr/CA/AccessControl のカスタム ディレクトリにインストールされます。

注: ご使用の環境に \$CASHCOMP 変数が定義されていない場合 (/etc/profile.CA に定義可能)、ライセンス プログラムは指定されたディレクトリにのみインストールされます。定義されている場合、ライセンス プログラムは \$CASHCOMP にインストールされます。\$CASHCOMP が定義されていない場合に、-lic_dir を指定しないと、ライセンス プログラムは /opt/CA/SharedComponents ディレクトリにインストールされます。

詳細情報:

[ネイティブ インストールの際に考慮するその他の事項](#) (P. 239)

[CA ControlMinder RPM パッケージのカスタマイズ](#) (P. 245)

[customize_eac rpm コマンド - RPM パッケージのカスタマイズ](#) (P. 251)

customize_eac_rpm コマンド - RPM パッケージのカスタマイズ

customize_eac_rpm コマンドは、CA ControlMinder RPM パッケージのカスタマイズスクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、CA ControlMinder RPM パッケージでのみ機能します。

注: このスクリプトは、ライセンス プログラム パッケージで使用するためのものではありません。

- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_rpm -h [-l]
customize_eac_rpm -a [-d pkg_location] pkg_filename
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
customize_eac_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_rpm -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
pkg_filename
customize_eac_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
customize_eac_rpm -t tmp_dir [-d pkg_location] pkg_filename
pkg_filename
```

カスタマイズする CA ControlMinder パッケージのファイル名を定義します。

注: -d オプションを指定しない場合は、パッケージ ファイルの完全パス名を定義する必要があります。

-a

使用許諾契約を表示します。

-c certfile

ルート of 証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d *pkg_location*

(オプション) ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはパッケージ ファイルへの完全パス名が *pkg_filename* であるとみなします。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (stdout) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。**-i** オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-k *keyfile*

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、**CAeAC** パッケージにのみ利用できます。

-l *lang*

インストール パラメータ ファイルの言語を *lang* に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、**-h** オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、**-f** オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t tmp_dir

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは /tmp です。

-u install_prefix

eTrust Access Control r8 SP1 パッケージをインストールしている場所のプレフィックスを定義します。実際のインストール場所は、このプレフィックスと製品の名前を連結したものになります。r8 SP1 パッケージは製品の名前に eTrust があるため、eTrustAccessControl サブディレクトリにインストールされました。新しいバージョンは、AccessControl サブディレクトリにインストールされます。

たとえば、r8 SP1 が /opt/CA/eTrustAccessControl にインストールされており、r12.0 SP1 にアップグレードする場合は、rpm コマンドを使ってパッケージをインストールする前に以下を入力します。

```
./customize_eac_rpm -u /opt/CA -d . CAeAC-1200-0.1106.i386.rpm
```

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、-a オプションを使用します。

RPM パッケージのアンインストール

インストールされている CA ControlMinder RPM パッケージをアンインストールするには、インストール時とは逆の手順で、CA ControlMinder パッケージをアンインストールする必要があります。

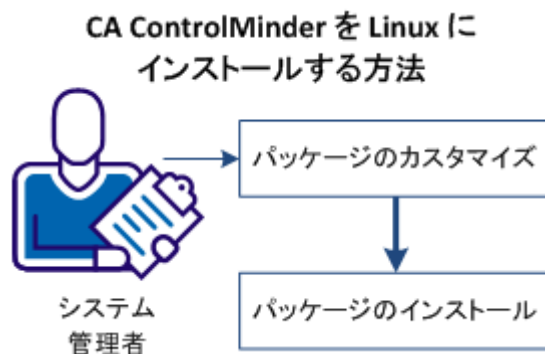
RPM パッケージをアンインストールするには、以下のコマンドを実行します。

```
rpm -e CAeACPackage_name
```

CA ControlMinder を Debian または Ubuntu Linux にインストールする方法

Debian Package Manager (dpkg) は、ソフトウェア パッケージをインストール、クエリ、確認、更新、および削除することができるコマンドラインユーティリティです。Debian および Ubuntu の Linux プラットフォームで使用されます。

Debian または Ubuntu Linux に CA ControlMinder をインストールする標準的な方法は、CA ControlMinder が提供するネイティブ .deb パッケージを使用することです。これにより、インストールした CA ControlMinder を、dpkg を使用してインストールされた他のソフトウェアと同様に管理できます。



次の手順に従ってください:

1. [パッケージをカスタマイズします。](#) (P. 254)
2. [以下のようにパッケージをインストールします。](#) (P. 259)

CA ControlMinder .deb パッケージのカスタマイズ

ネイティブ パッケージを使用して CA ControlMinder をインストールする前に、CA ControlMinder パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、CA ControlMinder パッケージをカスタマイズしてください。

次の手順に従ってください:

1. CA ControlMinder Endpoint Components for UNIX DVD の NativePackages ディレクトリで .deb パッケージを見つけます。
2. ファイル システム (*pkg_location*) 上の一時読み取り/書き込み可能な場所に .deb パッケージをコピーします。同じ場所に *customize_eac_deb* ファイルおよび *pre.tar* ファイルをコピーします。
pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA ControlMinder の使用許諾契約が含まれています。
3. 使用許諾契約を表示します。
`customize_eac_deb -a [-d pkg_location] pkg_filename`
4. 使用許諾契約の最後に表示される、角かっこで囲まれている キーワードをメモします。
次の手順でこのキーワードを指定します。
5. 使用許諾契約に同意することを示すために、CA ControlMinder パッケージをカスタマイズします。
`customize_eac_deb -w keyword [-d pkg_location] pkg_filename`
6. (オプション) インストール パラメータ ファイルの言語を指定します。
`customize_eac_deb -r -l lang [-d pkg_location] pkg_filename`
7. (オプション) eTrust Access Control r8 SP1 パッケージからアップグレードします。
`customize_eac_deb -u install_prefix [-d pkg_location] pkg_filename`
8. (オプション) デフォルトの暗号化ファイルを変更します。
`customize_eac_deb -s -c certfile -k keyfile [-d pkg_location] pkg_filename`
9. (オプション) ターゲット インストール ディレクトリを *target_location* に変更します。
`customize_eac_deb -i target_location [-d pkg_location] pkg_filename`
デフォルトのインストール場所は /opt/CA/ です。

10. (オプション) パッケージ用の他のカスタム デフォルトを設定します。インストール パラメータ ファイルを取得し、*tmp_params* として保存します。

```
customize_eac_deb -g -f tmp_params [-d pkg_location] pkg_filename
```

- a. インストール要件に合わせて、インストール パラメータ ファイル *tmp_params* を編集します。たとえば、POSTEXIT 設定 (前の # 文字を削除します) をアクティブにして、実行するインストール後スクリプトをポイントするようにします。
- b. カスタマイズされたパッケージにカスタマイズされたインストール パラメータを割り当てます。

```
customize_eac_deb -s -f tmp_params [-d pkg_location]  
pkg_filename
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA ControlMinder をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。以下の例は、使用許諾契約を受理するように 64 ビットの CA ControlMinder deb パッケージをカスタマイズする方法を示しています。この例では /mnt/AC_DVD にマウントされる UNIX DVD に対する CA ControlMinder Endpoint Components 上でパッケージを検索します。

```
cp /mnt/AC_DVD/NativePackages/_LINUX_X64_DEB_PKG_128.tar.Z /tmp  
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp  
cd /tmp  
zcat _LINUX_X64_DEB_PKG_128.tar.Z | tar -xvf -  
chmod 777 caeac*.deb  
/mnt/AC_DVD/NativePackages/customize_eac_deb -w keyword  
-d /tmp 128sp1-123_amd64.deb
```

カスタマイズされたパッケージを使用して、CA ControlMinder をインストールできるようになりました。

customize_eac_deb Command—Customize .deb Package

customize_eac_deb コマンドを使用して、CA ControlMinder を Debian または Ubuntu Linux にインストールする前に CA ControlMinder Debian パッケージ カスタマイズ スクリプトを実行します。

- このスクリプトは、CA ControlMinder Debian パッケージでのみ機能します。

注: このスクリプトは、ライセンス プログラム パッケージで使用するためのものではありません。

- ファイル システム上の読み取り/書き込みディレクトリにパッケージを移動させます。

このコマンドの形式は以下のようになります。

```
customize_eac_deb -h [-l lang]
customize_eac_deb -a [-d pkg_location] pkg_filename
customize_eac_deb -i target_location [-d pkg_location] pkg_filename
customize_eac_deb -w keyword [-d pkg_location] pkg_filename
customize_eac_deb -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_deb -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
pkg_filename
customize_eac_deb -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_deb -t tmp_dir [-d pkg_location] pkg_filename
pkg_filename
```

カスタマイズする CA ControlMinder パッケージのファイル名を定義します。

注: -d オプションを指定しない場合は、パッケージ ファイルの完全パス名を定義する必要があります。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション) ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはパッケージ ファイルへの完全パス名が *pkg_filename* であるとみなします。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (**stdout**) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。**-i** オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *target_location*

パッケージのカスタム ターゲット インストール ディレクトリを定義します。

例: **/opt/CA/**

-k *keyfile*

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、**CAeAC** パッケージにのみ利用できます。

-l *lang*

インストール パラメータ ファイルの言語を **lang** に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、**-h** オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、**-f** オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t tmp_dir

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは /tmp です。

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、**-a** オプションを使用します。

CA ControlMinder .deb パッケージのインストール

CA ControlMinder.deb パッケージを Linux プラットフォームにインストールするには、**dpkg -i** コマンドを使用します。パッケージファイル名にはバージョン番号が含まれており、**.deb** というサフィックスがついています。たとえば、「**caeac-128sp0-246_amd64.deb**」ファイルは、64 ビットバージョンの CA ControlMinder 12.8、サービスパック 0、ビルド 246 をインストールします。

次の手順に従ってください:

1. root ユーザとしてログインします。
2. 次の CA ControlMinder パッケージをインストールします。
dpkg -i caeac-xxxspx-xxx_amd64.deb
このパッケージはデフォルトで /opt/CA/ ディレクトリにインストールされます。
3. パッケージステータスが「OK installed」であることを確認します。
dpkg -s caeac-xxxspx-xxx

詳細情報:

[customize_eac_deb Command—Customize .deb Package \(P. 257\)](#)

CA ControlMinder .deb パッケージのアンインストール

Debian または Ubuntu の Linux システムから CA ControlMinder パッケージを削除するには、`dpkg -r` および `-P` コマンドを使用します。

次の手順に従ってください:

1. アンインストールする CA ControlMinder パッケージのフル ネームを検索します。

```
dpkg -l | grep caeac
```


パッケージ名の形式は `caeac-xxxsp-xxx` です。
2. CA ControlMinder パッケージ `caeac-xxxsp-xxx` を削除およびパーシします。

```
dpkg -r caeac-xxxsp-xxx  
dpkg -P caeac-xxxsp-xxx
```
3. CA ControlMinder ディレクトリがインストールディレクトリから削除されたことを確認します。

```
ls /opt/CA/
```

Linux または UNIX への CA ControlMinder のインストールを確認します

(オプション) CA ControlMinder の基本機能が動作することを確認することで、インストールを確認できます。 インストールログは、インストールディレクトリ内の `AccessControl/AccessControl_install.log` にあります。

次の手順に従ってください:

1. root ユーザとしてログインします。
2. テストファイルを作成し、全ユーザに読み取り許可を与えます。

```
echo "## This is my test file ##" > /tempfile  
chmod 666 /tempfile
```
3. CA ControlMinder bin ディレクトリに移動します。まだ実行されていない場合は CA ControlMinder をロードします。

```
cd /opt/CA/AccessControl_128SP0_211/bin/  
./seload
```

4. `selang` を実行し、`testuser` を作成し、テスト ファイルにアクセスする排他的権限を与えます。

```
./selang
AC> eu testuser password(1)
AC> ef /testfile owner(nobody)
AC> auth FILE /testfile uid(testuser) acc(A)
AC> exit
```

5. `root` ユーザがファイルにアクセスできないことを確認します（「`permission denied`」）。
6. ユーザ `testuser` としてシステムにログインします。
7. `testuser` が予測どおりにファイルにアクセスできることを確認します。

```
cat /testfile
```

```
ssh localhost -l testuser
```

```
cat /testfile
```

CA ControlMinder インストールが完了しました。

Solaris ネイティブ パッケージングのインストール

Solaris のネイティブ パッケージングは、コマンドラインユーティリティとして提供されます。このため、各パッケージを個別に作成、インストール、削除、およびレポートすることができます。

注: Solaris ネイティブ パッケージングの詳細については、[Sun Microsystems の Web サイト](#)ならびに `pkgadd`、`pkgrm`、`pkginfo`、および `pkgchk` に関するマニュアル ページを参照してください。

通常のインストールの代わりに、CA ControlMinder に用意されている Solaris ネイティブ パッケージを使用することができます。このため、インストールした CA ControlMinder を、Solaris ネイティブ パッケージングを使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、CA ControlMinder をアンインストールするには、`pkgrm` コマンドを使用する必要があります。 `uninstall_AC` スクリプトは使用しないでください。

Solaris ネイティブ パッケージのカスタマイズ

ネイティブ パッケージを使用して **CA ControlMinder** をインストールする前に、**CA ControlMinder** パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、**CA ControlMinder** パッケージをカスタマイズしてください。

サポートされている各 Solaris オペレーティング システムに対する Solaris ネイティブ パッケージは、**CA ControlMinder Endpoint Components for UNIX DVD** の **NativePackages** ディレクトリにあります。

Solaris ネイティブ パッケージのカスタマイズ方法

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

ファイル システムの読み取り/書き込み可能な領域で、必要に応じてパッケージをカスタマイズできます。

重要: パッケージを抽出する際には、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認します。そうしないと、Solaris ネイティブ パッケージング ツールはそのパッケージを破損したものとみなします。

2. **customize_eac_pkg** スクリプト ファイルおよび **pre.tar** ファイルをファイル システム上の一時的な保存場所にコピーします。

pre.tar ファイルは、圧縮された **tar** ファイルであり、インストール メッセージおよび **CA ControlMinder** のエンド ユーザ使用許諾契約が含まれています。

注: **customize_eac_pkg** スクリプト ファイルと **pre.tar** ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

```
customize_eac_pkg -a [-d pkg_location] pkg_name
```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA ControlMinder パッケージをカスタマイズします。

```
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
```

6. (オプション) インストールパラメータ ファイルの言語を指定します。

```
customize_eac_pkg -r -l lang [-d pkg_location] [pkg_name]
```

7. (オプション) インストールディレクトリを変更します。

```
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
```

8. (オプション) デフォルトの暗号化ファイルを変更します。

```
customize_eac_pkg -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
```

9. (オプション) インストールパラメータ ファイルを取得します。

```
customize_eac_pkg -g -f tmp_params [-d pkg_location] [pkg_name]
```

10. (オプション) インストール要件に合わせて、インストールパラメータ ファイルを編集します。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。たとえば、POSTEXIT 設定（前の # 文字を削除します）をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション) カスタマイズしたパッケージのインストールパラメータを設定します。

```
customize_eac_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA ControlMinder をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。以下の例では、CA ControlMinder Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント) にある x86 CA ControlMinder Solaris パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/_SOLARIS_X86_PKG*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _SOLARIS_X86_PKG*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_pkg -w keyword -d /tmp CAeAC
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、CA ControlMinder をインストールできるようになりました。

詳細情報:

[customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ \(P. 331\)](#)

Solaris ネイティブ パッケージのインストール

インストールした CA ControlMinder を、インストールされたほかのソフトウェアと同様に管理するには、CA ControlMinder Solaris ネイティブ パッケージをカスタマイズしてインストールします。CA ControlMinder Solaris のネイティブ パッケージを使用すると、Solaris 上で CA ControlMinder を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

CA ControlMinder Solaris ネイティブ パッケージのインストール方法

1. (オプション) Solaris ネイティブ インストール時のデフォルトを設定します。

- a. インストール管理ファイルを現在の場所にコピーします。

```
convert_eac_pkg -p
```

インストール管理ファイルを現在の場所に *myadmin* という名前でコピーします。

インストール管理ファイルを編集して、*pkgadd* のインストール時のデフォルトを変更できます。*pkgadd -a* オプションを使用すれば、CA ControlMinder など、特定のインストール用に変更されたファイルを使用できます。ただし、このファイルは CA ControlMinder に固有のものではありません。

重要: インストールされている既存の Solaris パッケージを以前の CA ControlMinder リリースからアップグレードするには、この手順を実行する必要があります。

- b. インストール管理ファイル (*myadmin*) を必要に応じて編集し、そのファイルを保存します。

これで、他のインストールに影響を及ぼすことなく、変更したインストール設定を CA ControlMinder ネイティブ インストールのために使用できます。

注: Solaris ネイティブ パッケージングでは、デフォルトで、ユーザによる操作を必要とする場合があります。インストール管理ファイルおよびこのファイルの使い方の詳細については、*pkgadd* (1M) および *admin* (4) に関する Solaris のマニュアル ページを参照してください。

2. [CAeAC パッケージのカスタマイズ](#) (P. 262)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のようにパッケージをインストールします。

```
pkgadd [-a dir/myadmin] -d pkg_location CAeAC
```

-a *dir/myadmin*

手順 1 で作成した **myadmin** インストール管理ファイルの場所を定義します。

このオプションを指定しない場合、**pkgadd** ではデフォルトのインストール管理ファイルが使用されます。

pkg_location

CA ControlMinder パッケージ (CAeAC) が配置されている場所を定義します。

重要: パッケージは、公開場所 (つまり、グループおよび全員に対する読み取りアクセス権が設定された場所) に配置する必要があります。たとえば、**/var/spool/pkg** です。

注: Solaris ネイティブ パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の **NativePackages** ディレクトリにあります。

これで、CA ControlMinder のインストールは完了しましたが、まだ起動されていません。

詳細情報:

[ネイティブ インストールの際に考慮するその他の事項 \(P. 239\)](#)

[Solaris ネイティブ パッケージのカスタマイズ \(P. 262\)](#)

[customize eac pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ \(P. 331\)](#)

[選択したゾーンへの Solaris ネイティブ パッケージのインストール \(P. 267\)](#)

[convert eac pkg - Solaris ネイティブ インストールの設定 \(P. 271\)](#)

[customize eac pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ \(P. 268\)](#)

選択したゾーンへの Solaris ネイティブ パッケージのインストール

Solaris のネイティブ パッケージングを使用し、選択したゾーンに CA ControlMinder をインストールすることができます。それには、CA ControlMinder をグローバル ゾーンにインストールする必要があります。

注: Solaris ネイティブ パッケージを使用して、CA ControlMinder をすべてのゾーンにインストールすることをお勧めします。

選択したゾーンに CA ControlMinder をインストールする方法

重要: すべてのゾーンで必ず同じ CA ControlMinder バージョンを使用するようにしてください。

1. グローバル ゾーンから以下のコマンドを発行して、CA ControlMinder をインストールします。

```
pkgadd -G -d pkg_location CAeAC  
pkg_location
```

カスタマイズした CA ControlMinder パッケージ (CAeAC) が配置されている場所を定義します。

重要: パッケージは、公開場所 (つまり、グループおよび全員に対する読み取りアクセス権が設定された場所) に配置する必要があります。たとえば、`/var/spool/pkg` です。

このコマンドによって、CA ControlMinder がグローバルゾーンにのみインストールされます。

2. グローバルゾーン内で `SEOS_load` コマンドを入力して、CA ControlMinder カーネル モジュールをロードします。

注: CA ControlMinder カーネルはロードされますが、CA ControlMinder はグローバルゾーン内のイベントをインターセプトしません。

3. **CA ControlMinder** をインストールするそれぞれの非グローバル ゾーンで以下の操作を行います。
 - a. 非グローバル ゾーンの一時的な保存場所に **CAeAC** パッケージをコピーします。
 - b. 非グローバル ゾーンから以下のコマンドを発行します。

```
pkgadd -G -d pkg_location CAeAC
```

このコマンドは、作業元である非グローバル ゾーンに **CA ControlMinder** をインストールします（前の手順でコピーしたパッケージを使用）。

これで、内部ゾーンで **CA ControlMinder** を開始できるようになります。

注： **CA ControlMinder** をグローバル ゾーンから削除する前に、すべての非グローバル ゾーンからアンインストールする必要があります。

customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ

customize_eac_pkg コマンドは、**CA ControlMinder Solaris** ネイティブ パッケージのカスタマイズスクリプトを実行します。

- このスクリプトは、利用可能な **CA ControlMinder Solaris** ネイティブ パッケージのいずれでも機能します。
- ファイル システム上の読み取り/書き込みディレクトリにパッケージを移動させます。
- ローカライズされたスクリプト メッセージを使用するには、**pre.tar** ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_pkg -g -f tmp_params -d pkg_location pkg_name
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(オプション) カスタマイズする CA ControlMinder パッケージの名前です。パッケージを指定しない場合、スクリプトはデフォルトでメインの CA ControlMinder パッケージ (CAeAC) を選択します。

-a

使用許諾契約を表示します。

-c certfile

ルート of 証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション) ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで `/var/spool/pkg` を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: `-g` オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (stdout) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを `-f` オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 `-l` オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストール ディレクトリを *install_loc/AccessControl* に設定します。

-k *keyfile*

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-l *lang*

インストールパラメータ ファイルの言語を *lang* に設定します。言語の設定は、-r オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。デフォルトでは、インストールパラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t *tmp_dir*

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは /tmp です。

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、-a オプションを使用します。このオプションは、新規インストールおよびアップグレードに必要です。

convert_eac_pkg - Solaris ネイティブ インストールの設定

Solaris `pkgadd` のデフォルト動作は、インストール管理ファイルによって決定されます。デフォルトの設定を変更するには、インストール管理ファイル（デフォルトでは、`/var/sadm/install/admin/default`）を変更する必要があります。たとえば、**CA ControlMinder** パッケージによって `setuid` 実行可能ファイルがインストールされたら、必要に応じて、インストール後スクリプト（`root` として実行）を実行できます。デフォルトの Solaris `pkgadd` 動作では、これらの操作の確認がユーザに求められます。

注： インストール管理ファイルを編集して、`pkgadd` のインストール時のデフォルトを変更できます。`pkgadd -a` オプションを使用すれば、**CA ControlMinder** など、特定のインストール用に変更されたファイルを使用できます。ただし、このファイルは **CA ControlMinder** に固有のものではありません。

このコマンドの形式は以下のようになります。

```
convert_eac_pkg -c [-d pkg_location] [pkg_name]
```

```
convert_eac_pkg -p [-f file]
```

-c

古い形式のパッケージを新しい形式のパッケージに変換します。

注: 古い形式のパッケージは、CA ControlMinder r8 SP1 で使用されてきました。アップグレードを行う前に、これらを変換する必要があります。

インストールされた CA ControlMinder パッケージまたはスプールされたパッケージの情報は、変換できます。スプールされたパッケージについては、**-d** オプションを使用してパッケージがどこに配置されているかを示します。

-d *pkg_location*

ファイル システム上でパッケージを配置するディレクトリを定義します。

pkg_name

パッケージの名前を定義します（デフォルトでは CAeAC）。

-p

名前が付けられたカスタム パッケージ構成ファイルを用意します。

-f *file*

CA ControlMinder インストール管理ファイルを作成する場所を定義します。

これを指定しないと、現在のディレクトリに[「*myadmin*」という名前のファイルが作成されます。

例: サイレント インストールを行うために Solaris ネイティブ インストールを設定する

以下の手順では、**setuid** 実行可能ファイルのインストールについての確認、またはインストール後スクリプトの実行についての確認をユーザが求められないように Solaris ネイティブ インストールを設定する方法について説明します。

1. インストール管理ファイルを現在の場所にコピーします。

```
convert_eac_pkg -p
```

これによって、他のインストールに影響することなく、**CA ControlMinder** ネイティブ インストールの構成設定を変更できます。

2. パッケージ構成ファイル (**myadmin**) 内の以下の設定を、以下のよう
に編集します。

```
setuid=nocheck  
action=nocheck
```

ファイルを保存します。

3. パッケージをカスタマイズします。

最小要件として、使用許諾契約への同意を指定する必要があります。

4. 以下のコマンドを実行して、カスタマイズされた **CA ControlMinder**
パッケージをサイレント インストールします。

```
pkgadd -n -a config_path%myadmin -d pkg_path CAeAC
```

例: 古い形式を使用する Solaris ネイティブ インストールをアップグレードする

以下の手順では、既存の **CA ControlMinder** ネイティブ パッケージインストールを新しいリリースにアップグレードする前にその変換を行う方法について説明します。 これを行うには、以下のコマンドを実行します。

```
convert_eac_pkg -c CAeAC
```

HP-UX ネイティブ パッケージのインストール

HP-UX のネイティブ パッケージは、GUI とコマンドライン ユーティリティのセットとして提供されます。これにより、個々のソフトウェア パッケージの作成、インストール、削除、およびレポート作成を行うことができます。HP-UX ネイティブ パッケージでは、リモート コンピュータにソフトウェア パッケージをインストールすることもできます。

注: HP-UX のネイティブ パッケージである、Software Distributor-UX (SD-UX) の詳細については、HP の Web サイト (<http://www.hp.com>) を参照してください。swreg、swinstall、swpackage、および swverify については、man ページも参照できます。

通常のインストールの代わりに、CA ControlMinder に用意されている SD-UX ネイティブ パッケージを使用することができます。これにより、インストールした CA ControlMinder を、SD-UX を使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、CA ControlMinder をアンインストールするには、**swremove** コマンドを使用する必要があります。uninstall_AC スクリプトは、使用しないでください。

SD-UX 形式パッケージのカスタマイズ

ネイティブ パッケージを使用して CA ControlMinder をインストールする前に、CA ControlMinder パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、CA ControlMinder パッケージをカスタマイズしてください。

サポートされた各 HP-UX オペレーティング システムに対する Software Distributor-UX (SD-UX) 形式パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の NativePackages ディレクトリに格納されています。

SD-UX 形式パッケージのカスタマイズ

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

重要: パッケージを展開するときは、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうでないと、HP-UX ネイティブ パッケージング ツールによってパッケージが破損していると見なされます。

2. `customize_eac_depot` スクリプト ファイルおよび `pre.tar` ファイルをファイル システム上の一時的な保存場所にコピーします。

`pre.tar` ファイルは、圧縮された `tar` ファイルであり、インストール メッセージおよび CA ControlMinder のエンド ユーザ使用許諾契約が含まれています。

注: `customize_eac_depot` スクリプト ファイルと `pre.tar` ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

```
customize_eac_depot -a [-d pkg_location] pkg_name
```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA ControlMinder パッケージをカスタマイズします。

```
customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
```

6. (オプション) インストールパラメータ ファイルの言語を指定します。

```
customize_eac_depot -r -l lang [-d pkg_location] [pkg_name]
```

7. (オプション) インストールディレクトリを変更します。

```
customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
```

8. (オプション) デフォルトの暗号化ファイルを変更します。

```
customize_eac_depot -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
```

9. (オプション) インストールパラメータ ファイルを取得します。

```
customize_eac_depot -g -f tmp_params [-d pkg_location] [pkg_name]
```

10. (オプション) インストール要件に合わせて、インストール パラメータ ファイルを編集します。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。たとえば、**POSTEXIT** 設定（前の **#** 文字を削除します）をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション) カスタマイズしたパッケージのインストール パラメータを設定します。

```
customize_eac_depot -s -f tmp_params [-d pkg_location] [pkg_name]
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で **CA ControlMinder** をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。以下の例では、**CA ControlMinder Endpoint Components for UNIX DVD**（**/mnt/AC_DVD** にマウント）にある **x86 CA ControlMinder SD-UX** パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/_HPUX11_PKG_*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _HPUX11_PKG_*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_depot -w keyword -d /tmp CAeAC
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、**CA ControlMinder** をインストールできるようになりました。

詳細情報:

[customize_eac_depot コマンド - SD-UX 形式パッケージのカスタマイズ \(P. 278\)](#)

HP-UX ネイティブ パッケージのインストール

インストールした CA ControlMinder を、インストールされたほかのソフトウェアと同様に管理するには、CA ControlMinder SD-UX 形式パッケージをカスタマイズしてインストールします。CA ControlMinder SD-UX 形式パッケージを使用すると、HP-UX に CA ControlMinder を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

CA ControlMinder HP-UX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

HP-UX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. [CAeAC パッケージのカスタマイズ](#) (P. 274)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のコマンドを使用して、カスタマイズされたパッケージを SD-UX に登録します。

```
swreg -l depot pkg_location
```

```
pkg_location
```

CA ControlMinder パッケージ (CAeAC) が配置されている場所を定義します。

4. 以下のコマンドを使用して、CA ControlMinder パッケージをインストールします。

```
swinstall -s pkg_location CAeAC
```

SD-UX は、*pkg_location* ディレクトリから、CAeAC パッケージのインストールを開始します。

これで、CA ControlMinder のインストールは完了しましたが、まだ起動されていません。

詳細情報:

[ネイティブ インストールの際に考慮するその他の事項](#) (P. 239)

[SD-UX 形式パッケージのカスタマイズ](#) (P. 274)

customize_eac_depot コマンド - SD-UX 形式パッケージのカスタマイズ

customize_eac_depot コマンドは、SD-UX 形式パッケージ用の CA ControlMinder ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な CA ControlMinder Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_depot -h [-l]
customize_eac_depot -a [-d pkg_location] [pkg_name]
customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
customize_eac_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
customize_eac_depot -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location] [pkg_name]
customize_eac_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

(オプション) カスタマイズする CA ControlMinder パッケージの名前です。パッケージを指定しない場合、スクリプトはデフォルトでメインの CA ControlMinder パッケージ (CAeAC) を選択します。

-a

使用許諾契約を表示します。

-c certfile

ルート of 証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d *pkg_location*

(オプション) ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで `/var/spool/pkg` を指定します。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: `-g` オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (`stdout`) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを `-f` オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。`-i` オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストール ディレクトリを `install_loc/AccessControl` に設定します。

-k *keyfile*

ルート の秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、`CAeAC` パッケージにのみ利用できます。

-l *lang*

インストール パラメータ ファイルの言語を *lang* に設定します。言語の設定は、`-r` オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、`-h` オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、-a オプションを使用します。

HP-UX パッケージのアンインストール

インストールされている CA ControlMinder HP-UX パッケージをアンインストールするには、インストール時とは逆の手順で、CA ControlMinder パッケージをアンインストールする必要があります。

CA ControlMinder パッケージをアンインストールするには、メインの CA ControlMinder パッケージをアンインストールします。

```
swremove CAeAC
```

AIX ネイティブ パッケージのインストール

AIX ネイティブ パッケージは、GUI およびコマンドライン ユーティリティのセットとして提供されます。これを使用して、個別のソフトウェアパッケージを管理できます。通常のインストールの代わりに、CA ControlMinder に用意されている AIX ネイティブ パッケージを使用することができます。これにより、インストールした CA ControlMinder を、AIX installp を使用してインストールされた他のソフトウェアと同様に管理できます。

注: 一部の AIX バージョンはいくつかのパッケージ形式（installp、SysV、RPM）をサポートしていますが、CA ControlMinder では AIX のネイティブ パッケージ形式（installp）のみが提供されます。

重要: パッケージのインストール後、CA ControlMinder をアンインストールするには、installp コマンドを使用する必要があります。uninstall_AC スクリプトは、使用しないでください。

bff ネイティブ パッケージ ファイルのカスタマイズ

ネイティブ パッケージを使用して CA ControlMinder をインストールする前に、CA ControlMinder パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、CA ControlMinder パッケージをカスタマイズしてください。

UNIX DVD の CA ControlMinder Endpoint Components の NativePackages ディレクトリ内に installp 形式のネイティブ パッケージング (AIX bff ファイル) を見つけることができます。

次の手順に従ってください:

1. root ユーザとしてログインします。
2. パッケージをファイル システム上の一時的な場所に展開します。

ファイル システムの読み取り/書き込み可能な領域で、パッケージ (bff ファイル) を必要に応じてカスタマイズできます。

重要: パッケージのサイズの少なくとも 2 倍のディスク領域があり、一時再パッケージ ファイルを保存できることを確認します。

3. customize_eac_bff スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA ControlMinder のエンド ユーザ使用許諾契約が含まれています。

注: customize_eac_bff スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

4. 使用許諾契約を表示します。

```
customize_eac_bff -a [-d pkg_location] pkg_name
```

5. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

6. 使用許諾契約に同意することを示すために、CA ControlMinder パッケージをカスタマイズします。

```
customize_eac_bff -w keyword [-d pkg_location] pkg_name
```

7. (オプション) インストールパラメータ ファイルの言語を設定します。

```
customize_eac_bff -r -l lang [-d pkg_location] pkg_name
```

8. (オプション) インストールディレクトリを変更します。

```
customize_eac_bff -i install_loc [-d pkg_location] [pkg_name]
```

注: WPAR (Workload Partitions : 作業負荷パーティティション) へのインストールに対して CA ControlMinder パッケージをセットアップしている場合は、-i オプションを使用して、非共有ファイルシステムにインストール場所を変更します。デフォルトでは、/opt および /usr は共有ファイルシステムで、CA ControlMinder の WPAR インストールには使用できません。

9. (オプション) デフォルトの暗号化ファイルを変更します。

```
customize_eac_bff -s -c certfile -k keyfile [-d pkg_location] pkg_name
```

10. インストールパラメータ ファイルを取得します。

```
customize_eac_bff -g -f tmp_params [-d pkg_location] pkg_name
```

11. (オプション) インストール要件に合わせて、インストールパラメータ ファイルを編集します。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。たとえば、POSTEXIT 設定 (前の # 文字を削除します) をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

12. (オプション) カスタマイズしたパッケージのインストールパラメータを設定します。

```
customize_eac_bff -s -f tmp_params [-d pkg_location] pkg_name
```

カスタマイズされたパッケージを使用して、CA ControlMinder をインストールできるようになりました。

AIX ネイティブ パッケージのインストール

インストールした CA ControlMinder を、インストールされたほかのソフトウェアと同様に管理するには、CA ControlMinder AIX ネイティブ パッケージをカスタマイズしてインストールします。CA ControlMinder AIX のネイティブ パッケージ (bff ファイル) を使用すると、AIX に CA ControlMinder を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

次の手順に従ってください:

1. root ユーザとしてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. [CAeAC パッケージのカスタマイズ](#) (P. 281)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. (オプション) インストールするパッケージのレベル (バージョン) を記録します。

```
installp -l -d pkg_location
```

pkg_location

CA ControlMinder パッケージ (CAeAC) が配置されている場所を定義します。

pkg_location 内の各パッケージについて、AIX ではパッケージ レベルの一覧が作成されます。

注: AIX ネイティブ パッケージのインストール オプションの詳細については、installp の man ページを参照してください。

4. 以下のコマンドを使用して、CA ControlMinder パッケージをインストールします。

```
installp -ac -d pkg_location CAeAC [pkg_level]
```

pkg_level

前に記録したパッケージのレベル番号を定義します。

重要: WPAR にインストールしている場合は、インストールする非共有ファイル システムを指定し、グローバル環境にインストールします。

AIX は、*pkg_location* ディレクトリから、CAeAC パッケージのインストールを開始します。これで、CA ControlMinder のインストールは完了しましたが、まだ起動されていません。

5. (オプション) 特定の WPAR *wparname* にインストールします。(すべてのシステム WPAR にインストールする場合は、-A を使用します)。
 - グローバル環境から、次のコマンドを実行します。

```
syncwpar wpar_name
```
 - または WPAR から、次のコマンドを実行します。

```
syncroot
```

詳細情報:

[ネイティブ インストールの際に考慮するその他の事項](#) (P. 239)

customize_eac_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ

customize_eac_bff コマンドによって、bff ネイティブ パッケージ ファイル用の、CA ControlMinder ネイティブ パッケージ カスタマイズ スクリプトが実行されます。

このパッケージは、AIX で使用可能な CA ControlMinder ネイティブ パッケージのいずれでも機能します。パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

重要: パッケージの抽出場所には、再パッケージの中間ファイルを保存するために、少なくともパッケージの 2 倍のサイズが必要です。

注: ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_bff -h [-l lang]
customize_eac_bff -a [-d pkg_location] pkg_name
customize_eac_bff -w keyword [-d pkg_location] pkg_name
customize_eac_bff -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_bff -i install_loc [-d pkg_location] [pkg_name]
customize_eac_bff -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
pkg_name
customize_eac_bff -g [-f tmp_params] [-d pkg_location] pkg_name
customize_eac_bff -t temp_dir [-d pkg_location] [pkg_name]
```

pkg_name

カスタマイズする CA ControlMinder パッケージ (bff ファイル) の名前です。

-a

使用許諾契約を表示します。

-c certfile

ルート of 証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d *pkg_location*

(オプション) ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで `/var/spool/pkg` を指定します。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (`stdout`) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。**-i** オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストール ディレクトリを `install_loc/AccessControl` に設定します。

-k *keyfile*

ルート の秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、**CAeAC** パッケージにのみ利用できます。

-l *lang*

インストール パラメータ ファイルの言語を *lang* に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、**-h** オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t *tmp_dir*

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは /tmp です。

-w **キーワード**

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、-a オプションを使用します。

AIX パッケージのアンインストール

インストールされている CA ControlMinder AIX パッケージをアンインストールするには、インストール時とは逆の手順で、CA ControlMinder パッケージをアンインストールする必要があります。

CA ControlMinder パッケージをアンインストールするには、メインの CA ControlMinder パッケージをアンインストールします。

```
installp -u CAeAC
```

AIX Workload Partition (WPAR) の実装

AIX は、ワークロードパーティション (WPAR) と呼ばれる AIX の単一インスタンス内の仮想化されたオペレーティング システム環境を提供します。ワークロードパーティションは、AIX オペレーティング システムの単一インスタンスのリソースから作成され、それを共有するソフトウェアパーティションです。AIX には、「グローバル環境」と呼ばれるマスタパーティションと、それと並行して実行されるワークロードパーティションがあります。

CA ControlMinder を使用して、環境内の各パーティションを保護できます。これにより、パーティションごとに異なるルールおよびポリシーを定義し、パーティションごとに異なるアクセス制約を定義できます。

CA ControlMinder を AIX WPAR にインストールする前に、以下の考慮事項および制限事項を確認します。

- CA ControlMinder をインストールできるのは、AIX 7.1 以降のみです。
- 標準スクリプト インストール (install_base) はサポートされていません。CA ControlMinder を AIX WPAR にインストールするために、ネイティブ パッケージ インストールを使用します。
- 共有モード (/opt および /usr ディレクトリがすべてのパーティションによって共有される) での AIX WPAR の使用を選択する場合は、プライベート インストール ディレクトリを使用します。例：CA ControlMinder を、/opt/CA/AccessControl ではなく、/CA/AccessControl/ ディレクトリにインストールするように指定します。
- AIX WPAR ライブ移行はサポートされていません。
- ワークロードパーティション上で、キー ロガーを使用するには、CA ControlMinder が実行されており、キーボード ロガーがグローバル環境および各ワークロードパーティション上で有効であることを確認します。
- ワークロードパーティションに適用される CA ControlMinder ファイル保護ルールでは、グローバル環境からのユーザアクセスから保護されません。グローバル環境を保護するには、グローバル環境にファイル保護ルールを適用します。
- CA ControlMinder を AIX WPAR 5.2 上へにインストールし実行する前に、CA ControlMinder インストール パッケージをカスタマイズする必要があります。CA ControlMinder を AIX WPAR 7.1 以降にインストールするためにカスタマイズするインストール パッケージを使用できません。

- ユーザのログイン試行（たとえば: `segrace`、`serevu` および監査ログ レコード）を識別する CA ControlMinder PAM 機能は、AIX WPAR 5.2 ではサポートされていません。

共有モードでの CA ControlMinder AIX WPAR ネイティブ パッケージのインストール

CA ControlMinder の AIX WPAR のデフォルト パーティションへのインストールは、デフォルトではないインストールディレクトリを使用することを除けば、標準インストールに類似しています。共有モードでは、`/opt` および `/usr` ディレクトリはすべてのワークロード パーティションで共有されています。

以下の手順に従います。

1. グローバル環境に `root` としてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、`root` アカウントに関連した権限が必要です。

2. [CAeAC パッケージのカスタマイズ](#) (P. 281)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズします。また、パッケージをカスタマイズしてカスタムインストールを指定することも可能です。

重要: インストールディレクトリを変更して、プライベートディレクトリを指定します。以下に例を示します。

```
customize_eac_bff -i /CA/AccessControl -d pwd CaeAC.12.6.1.*.bff
```

3. 以下のコマンドを使用して、CA ControlMinder パッケージをインストールします。

```
installp -d pkg_location CAeAC
```

AIX は、`pkg_location` ディレクトリから、CAeAC パッケージのインストールを開始します。

これで、CA ControlMinder のインストールは完了しましたが、まだ起動されていません。

4. 以下のコマンドを使用して、CA ControlMinder を AIX ワークロードパーティションと同期します。

```
synchwpar <wpar_name>
```

`wpar_name`

AIX ワークロードパーティションの名前を指定します。

注: CA ControlMinder をすべてのパーティションにインストールするには、`synchwpar -A` コマンドを使用します。

CA ControlMinder は指定された AIX ワークロードパーティションにインストールされます。

分離モードでの CA ControlMinder AIX 7.1 WPAR ネイティブ パッケージのインストール

CA ControlMinder の AIX ワークロード パーティションへのインストールは、標準インストールに類似しています。分離モードでは、ワークロードパーティションはそれぞれ、`/opt` および `/usr` ディレクトリのローカルコピーを使用します。

以下の手順に従います。

1. グローバル環境に `root` としてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、`root` アカウントに関連した権限が必要です。

2. [CAeAC パッケージのカスタマイズ](#) (P. 281)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズします。また、パッケージをカスタマイズしてカスタムインストールを指定することも可能です。

3. 以下のコマンドを実行して、CA ControlMinder をインストールします。

```
installp -d pkg_location CAeAC
```

AIX は、`pkg_location` ディレクトリから、CAeAC パッケージのインストールを開始します。

これで、CA ControlMinder のインストールは完了しましたが、まだ起動されていません。

4. 分離されている各ワークロードパーティションに、インストールパッケージをコピーします。
5. `root` としての各ワークロードパーティションにログインおよび CA ControlMinder のインストール

CA ControlMinder は AIX ワークロードパーティションにインストールされます。

AIX 5.2 への AIX WPAR ネイティブ パッケージのインストール

AIX 5.2 オペレーティング システムが 1 つ以上のワークロード パーティションに対してインストールされる場合、グローバル環境に **CA ControlMinder** をインストールした後に、**CA ControlMinder** をワークロードパーティションにインストールできます。

重要: **CA ControlMinder** の **AIX 7.1 WPAR** グローバル環境へのインストールおよび実行のみ可能です。

以下の手順に従います。

1. グローバル環境に **root** としてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、**root** アカウントに関連した権限が必要です。

2. [CAeAC パッケージのカスタマイズ](#) (P. 281)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズします。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のコマンドを実行して、**CA ControlMinder** をインストールします。

```
installp -d pkg_location CAeAC
```

AIX は、*pkg_location* ディレクトリから、**CAeAC** パッケージのインストールを開始します。

これで、**CA ControlMinder** のインストールは完了しましたが、まだ起動されていません。

4. 元の **CA ControlMinder** インストール パッケージを各ワークロードパーティションにコピーします。
5. ワークロードパーティションに **root** としてログインします。
6. **CAeAC** パッケージを **AIX 5.2 WPAR** 用にカスタマイズします。

重要: **CA ControlMinder** インストール パッケージを **AIX 7.1** 環境用と **AIX 5.2** 環境用に別々にカスタマイズして、各オペレーティング システム上の **installp** プログラムとの互換性を保証します。

7. **CA ControlMinder** をワークロードパーティションにインストールします。

CA ControlMinder は指定された AIX ワークロードパーティションにインストールされます。

CA ControlMinder AIX 7.1 WPAR パッケージのアンインストール

まず CA ControlMinder をグローバル環境から削除し、次に各ワークロードパーティションから削除して、AIX 7.1 WPAR パッケージをアンインストールします。

以下の手順に従います。

1. 以下のコマンドを使用して、グローバル環境、および各ワークロードパーティション上の CA ControlMinder デーモンをすべて停止します。

```
secons -sk
```

2. グローバル環境に root としてログインします。

3. 以下のコマンドを使用して、CAeAC パッケージを削除します。

```
installp -u CAeAC
```

4. 以下のコマンドを使用して、ワークロードパーティションを同期します。

```
synchwpar <wpar_name>
```

注: 離れているパーティションおよび AIX 5.2 を実行しているワークロードパーティションから CA ControlMinder をアンインストールするには、各パーティションに対して uninstall コマンドを実行して、インストールパッケージを削除します。

CA ControlMinder はグローバル環境および各ワークロードパーティションから削除されます。

通常のスクリプト インストール

CA ControlMinder では、UNIX 上に CA ControlMinder を対話形式またはサイレント モードでインストールする `install_base` スクリプトを提供しています。

通常のスクリプト インストール（ネイティブ インストールでなく）を使用する場合は、CA ControlMinder インストール メディアに含まれる 3 つのファイルが必要になります。

- **install_base - tar** ファイルから CA ControlMinder をインストールするスクリプトです。
- **_opSystemVersion_ACVersion.tar.Z** - すべての CA ControlMinder ファイルが含まれている圧縮 tar ファイルです。たとえば、CA ControlMinder r12.0 を IBM AIX バージョン 5 にインストールする場合、使用する tar ファイルは **_AIX5_120.tar.Z** となります。
- **pre.tar** - 圧縮された tar ファイルであり、インストールに関するメッセージおよびエンドユーザ使用許諾契約が含まれています。

エンドユーザ使用許諾契約を読んだ後、インストールを続行するには、そのファイルの最後で検出されるコマンドを入力します。

- サイレント インストール (`install_base -autocfg` を使用) を実行する場合は、`-command` オプションと、エンドユーザ使用許諾契約ファイルの最後で検出されるコマンドを使用します。
- 応答ファイル (`-autocfg file_name`) を使用する場合、`-command` オプションは必要ありません。

ライセンス ファイルの名前と場所を取得するには、`install_base -h` を実行します。間違ったコマンドを入力した場合も、ファイルの名前と場所が得られます。

これらのファイルは、CA ControlMinder Endpoint Components for UNIX DVD の `/Unix/Access-Control` ディレクトリにあります。

install_base スクリプトを使用したインストール

サポートされている OS には `install_base` スクリプトを使用して **CA ControlMinder** をインストールすることができます。これは対話形式のスクリプトですが、サイレント モードでの実行も可能です。

注: `install_base` スクリプトを実行する前に、インストールする機能を必ず決定し、[install base コマンド](#) (P. 297)を確認します。これにより、決定した機能のインストールを開始する方法を把握することができます。また、[install base スクリプトのしくみ](#) (P. 304)を最初に学習することもできます。

CA ControlMinder のインストール方法

1. **CA ControlMinder** がすでにインストールされていて実行中である場合は、管理者としてログインし、以下のコマンドを入力して、**CA ControlMinder** を停止します。

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

2. **root** ユーザとしてログインします。

CA ControlMinder をインストールするには、ルート権限が必要です。

3. 光ディスク ドライブに **CA ControlMinder Endpoint Components for UNIX DVD** をセットします。

重要: 光ディスク ドライブから **HP** にインストールする場合は、**DVD** からファイル名が正しく読み込まれていることを確認する必要があります。ファイル名が強制的にすべて大文字の短い名前に変更されるのを防ぐために、`pfs_mountd &` および `pfsd &` コマンドを入力し、`pfs_mountd`、`pfsd.rpc`、`pfs_mountd.rpc`、および `pfsd` の 4 つのデーモンが呼び出されることを確認します。詳細については、該当する `pfs*` デーモンおよびコマンドのマニュアルページを参照してください。

4. エンドユーザ使用許諾契約の内容を読みます。

`install_base` スクリプトを実行するには、エンドユーザ使用許諾契約に同意する必要があります。エンドユーザ使用許諾契約を読んだ後、インストールを続行するには、そのファイルの最後に記述されたコマンドを入力します。ライセンスファイルの名前と場所を取得するには、`install_base -h` を実行します。

5. `install_base` スクリプトを実行します。

`install_base` スクリプトが開始されると、選択内容に基づいて、インストールに関して該当する質問に答えるよう指示されます。

注: インストールスクリプトによって適切な圧縮 `tar` ファイルが検出されるため、ご使用のプラットフォームに対する `tar` ファイル名の入力は省略できます。

これで **CA ControlMinder** のインストールは完了しましたが、**CA ControlMinder** はまだ実行されていません。

例: クライアントおよびサーバ パッケージおよびデフォルト機能をインストールする

以下のコマンドでは、対話形式の `install_base` スクリプトを開始し、すべてのデフォルト **CA ControlMinder** 機能でのクライアント パッケージおよびサーバパッケージをインストールする方法を説明します。インストール中には、**CA ControlMinder** のクライアントおよびサーバパッケージのインストールに関する質問に答えるように求められます。

```
/dvdrom/Unix/Access-Control/install_base
```

注: インストールするパッケージを指定していないので、`install_base` コマンドではクライアント パッケージとサーバパッケージの両方がインストールされます。

例: STOP を有効にした状態でクライアント パッケージをカスタム ディレクトリにインストールする

以下のコマンドでは、対話形式の `install_base` スクリプトを開始してクライアント パッケージを `/opt/CA/AC` ディレクトリにインストールし、スタック オーバフロー防止機能オプションを有効にする方法を示します。

```
/dvdrom/Unix/Access-Control/install_base -client -stop -d /opt/CA/AC
```


install_base コマンド - インストール スクリプトの実行

`install_base` コマンドでは、インストール スクリプトを実行し、1 つ以上のインストール オプションが選択された 1 つ以上の **CA ControlMinder** パッケージをインストールします。

このコマンドの形式は以下のようになります。

```
install_base [tar_file] [packages] [options]
```

tar_file

(オプション) ご使用のプラットフォームに対応する **CA ControlMinder** インストール ファイルが含まれている **tar** ファイルの名前を定義します。インストール スクリプトによって適切な圧縮 **tar** ファイルが検出されるため、**tar** ファイル名の入力は省略できます。

packages

(オプション) インストールする **CA ControlMinder** パッケージを定義します。パッケージを何も指定しない場合は、インストール スクリプトによりクライアント パッケージとサーバ パッケージの両方がインストールされます。ただし、**CA ControlMinder** のアップグレードしている場合は例外で、すでにインストールされているパッケージと同じパッケージがインストールされます。

注: クライアント パッケージについては、その他のパッケージをインストールする前に、インストールする必要があります。ただし、クライアント パッケージと一緒に他のパッケージもインストールするように指定することは可能です。

インストールできる **CA ControlMinder** パッケージを以下に示します。

-all

すべての **CA ControlMinder** パッケージをインストールします。クライアント パッケージ、サーバ パッケージ、API パッケージ、MFSD パッケージがあります。また **STOP** (**-stop** オプション) が有効になります。

-api

API ライブラリおよびサンプル プログラムが含まれている API パッケージをインストールします。

-client

CA ControlMinder コア機能が含まれているクライアント パッケージをスタンドアロン コンピュータにインストールします。

-mfsd

メインフレーム同期デーモンが含まれている MFSD パッケージをインストールします。

注: MFSD パッケージをインストールするには、事前にサーバパッケージをインストールしておく必要があります。

-server

サーバパッケージをインストールします。サーバパッケージには、より多くのバイナリおよびスクリプト (**selogrcd**、**sepmdd**、**sepmdd**、**sepmddadm**、**secrepsw**) が含まれています。これらは、クライアントパッケージを補完するものです。たとえば、**sepmdd** では、コンピュータに **Policy Model** を設定できます。

-uni

Unicenter セキュリティ統合および移行パッケージをインストールします。このパッケージは、**CA ControlMinder** と、Unicenter の **CAUTIL**、負荷管理、およびイベント管理の各コンポーネント、ならびに **Unicenter EMSec API** との統合をサポートします。

options

(オプション) 追加で設定するインストール オプションを定義します。

注: CA ControlMinder の機能に影響するインストール オプション (たとえば、**-stop**) を指定できるのは、クライアント パッケージをインストールするときのみです。インストール プロセスに影響するインストール オプション (たとえば、**-verbose**) は、どのパッケージでも指定できます。

指定できるオプションを以下に示します。

-autocfg [response_file]

インストールをサイレント モード (対話モードをオフ) で実行します。応答ファイルが指定されている場合、インストールではそのファイル内に格納された環境設定を使用して、対話形式のインストール プロセスに自動的に応答します。応答ファイルが指定されていない場合、または応答ファイルにオプションが指定されていない場合、インストールでは事前設定済のデフォルトが使用されます。

応答ファイルの作成方法

- **-savecfg** オプションを使用します。
- **parameters.tar** にあるインストール パラメータ ファイルを編集します。

重要: 応答ファイルを指定しない場合は、**-autocfg** オプションを使用するときに、**-command** オプションを使用する必要があります。

サイレント インストールを実行する場合は、以下の点に留意してください。

- 暗号化鍵は変更できません。
- デフォルトでは、クライアント パッケージとサーバ パッケージのみがインストールされます。

他のパッケージまたは機能をインストールするには、通常のインストールの場合と同様に適切なオプションを指定する必要があります。

- `install_base` コマンドでは、インストールに関する詳細がインストール中に画面に出力されません。

インストール中にインストールに関するメッセージを画面に表示させるには、**-verbose** オプションを使用します。

- セキュリティ上の理由により、レポート エージェントと配布サーバ間の **SSL 通信** を保護する共有秘密鍵をサイレント インストールで指定することはできません。共有秘密鍵を指定するには、インストール後にレポート エージェント ユーザ (**+reportagent**) を設定する必要があります。

-command *keyword*

エンド ユーザ使用許諾契約にユーザが同意していることを指定するコマンドを定義します。このコマンドは使用許諾契約（角かっこ [] 内）の最後にあり、**-autocfg** オプションを使用する際は、このコマンドを使用する必要があります。エンド ユーザ使用許諾契約ファイルの場所を特定するには、**install_base -h** を実行します。

注: エンド ユーザ使用許諾契約が利用できるのは、ヘルプが表示されている間だけです。ヘルプを読み終えると、エンド ユーザ使用許諾契約は削除されます。

-d *target_dir*

カスタム インストール ディレクトリを定義します。デフォルトのインストール ディレクトリは、**/opt/CA/AccessControl/** です。

重要: マウントしたネットワーク ファイル システム（**NFS**）に **CA ControlMinder** データベースを配置することはできません。

-dns | -nodns

DNS ホストの有無に関係なく、**lookaside** データベースを作成します。**-nodns** オプションは、インストール中に **CA ControlMinder** が DNS 内の任意のホストで **nslookup** を実行しないことを指定します。

-fips

FIPS 専用の公開鍵(非対称)の暗号化を有効にするよう指定します。

-force

インストール時に、新たにアクティブになったサブスクリバ更新 (*sepmc -n* および *subs <pmdb> newsubs(sub_name)*) を無視して、インストールを続行するようにします。デフォルトでは、インストールが停止し、サブスクリバの更新をまず終了させるよう求められます。

注: このオプションを使用した場合、新しいサブスクリバ更新は失敗します。

-force_encrypt

インストール時に、警告を表示せずにデフォルト以外の暗号化鍵を使用するようにします。

重要: アップグレードが完了すると、暗号化鍵はデフォルトに設定されます。

注: CA ControlMinder には、SSL、AES (128 ビット、192 ビット、および 256 ビット)、DES、および 3 DES も用意されており、この中から選択できます。

--force_install

すでにインストールされているバージョンを強制的に上書きインストールします。同じバージョンを上書きインストールする場合、このオプションを使用します。

-force_kernel

古いカーネルのアンロードが不可能なことを警告することなく、インストールが続行されるようにします。

注: インストール完了後に、コンピュータの再起動が必要な場合があります。

-g *groupname*

CA ControlMinder ファイルのグループ所有者の名前を定義します。デフォルト値は 0 です。

-h | -help

このコマンドのヘルプを表示します。

-ignore_dep

アンインストール手順で、他の製品との依存関係をチェックしないように指定します。

-key *encryption_key*

アップグレード時に暗号化鍵を復元します。

注: アップグレード時には、アップグレードの前に使用していたのと同じ暗号化鍵を使用する必要があります。

-lang *lang*

CA ControlMinder をどの言語でインストールするかを定義します。サポート対象の言語および文字セットについては、ヘルプを表示 (install_base -h) する際にこのオプションの説明を確認してください。

-lic_dir *license_dir*

ライセンス プログラムがまだインストールされていない場合、ライセンス プログラムのインストール ディレクトリを定義します。

注: コンピュータ環境に `$CASHCOMP` 変数が定義されていない場合 (/etc/profile.CA に定義可能)、ライセンス プログラムは指定されたディレクトリにのみインストールされます。定義されている場合、ライセンス プログラムは `$CASHCOMP` にインストールされます。`$CASHCOMP` が定義されていない場合に、`-lic_dir` を指定しないと、ライセンス プログラムは `/opt/CA/SharedComponents` ディレクトリにインストールされます。`CAWIN` は、ライセンス パッケージの場合と同じディレクトリにインストールされます。

-nolink

CA ControlMinder をデフォルトパス (`/opt/CA/AccessControl/`) にインストールする際に `/etc` ディレクトリ内の `seos.ini` へのリンクが作成されないように指定します。

デフォルト以外のディレクトリに CA ControlMinder をインストールすると、CA ControlMinder により `/etc` ディレクトリ内の `seos.ini` へのリンクが作成されます。これにより、CA ControlMinder はインストール場所を「検出」できます。デフォルトパスにインストールしており、(セキュリティ上の要件により) `/etc` ディレクトリを更新しない場合は、このオプションを使用します。

-nolog

インストールプロセスに対してログが保持されないように指定します。デフォルトでは、インストールプロセスに関連付けられたすべてのトランザクションが *ACInstallDir/AccessControl_install.log* に格納されます（ここで、*ACInstallDir* は、CA ControlMinder のインストールディレクトリです）。

-no_tng_int

インストール時に *selogrd* と *Unicenter* イベント管理との統合が設定されないよう指定します。

このオプションを指定しない場合、インストールスクリプトにより *Unicenter* イベント管理がインストールされているかどうかチェックされます。インストールスクリプトは、*Unicenter* イベント管理がインストールされているとみなすと、*selogrd.cfg* に以下の行を追加して *selogrd* と *Unicenter* イベント管理との統合を設定します。

```
uni hostname
```

-noprofile

/etc/profile.CA がユーザ環境にロードされないように指定します。

-post program_name

インストールが完了した後で実行するプログラムを指定します。

-pre program_name

インストールの開始前に実行するプログラムを指定します。

-rcert certificate.pem

ルートの証明書ファイルへの完全パス名を指定します。

注: このオプションを使用すると、スクリプトでは *tar* ファイルを抽出し、このファイルをユーザにより提供されたファイルと再パッケージ化し、デフォルト ファイル (*def_root.pem*) と置き換えます。

-rkey certificate.key

ルートの鍵ファイルへの完全パス名を指定します。

注: このオプションを使用すると、スクリプトでは *tar* ファイルを抽出し、このファイルをユーザにより提供されたファイルと再パッケージ化し、デフォルト ファイル (*def_root.key*) と置き換えます。

-rootprop

sepass による root のパスワードの変更が Policy Model に送信されるように指定します。

注: インストールの完了後は、seos.ini ファイルの AllowRootProp トークンを使用してこのオプションを設定できます。seos.ini 初期化ファイルの詳細については、「リファレンス ガイド」を参照してください。

-savecfg <response_file>

対話式のインストールで入力した応答を後で --autocfg オプションでできるように保存します。

-stop

STOP (スタック オーバーフロー保護) 機能を使用できるようにします。

-system_resolve

システム関数の使用を指定します。この関数は、システム上のネットワーク キャッシュの省略を定義します。

注: このオプションを IBM AIX プラットフォームで使用することはできません。

-v

CA ControlMinder パッケージのバージョンを表示します。

-verbose

インストール時にインストールに関するメッセージが画面に表示されるように指定します。対話形式のインストールではデフォルトになっています。-autocfg オプションを使用するときは、これらのメッセージを確認したい場合にのみ、このオプションを設定します。

install_base スクリプトのしくみ

install_base スクリプトで実行される内容は以下のとおりです。

1. デフォルト インストール ディレクトリを変更するかどうかを確認するメッセージが表示されます。
2. 指定したインストール オプションが表示され、インストールを続行するかどうかを確認するメッセージが表示されます。

3. tar.Z ファイルからインストール場所にデータが抽出されます（デフォルトの場所または `target_dir` で指定された場所）。
4. プラットフォームが異なると、実行されるアクションも異なります。
 - Sun Solaris の場合、CA ControlMinder の `syscall` スクリプトが `/etc/name_to_sysnum` ファイルに追加されます。元のファイルは `/etc/name_to_sysnum.bak` として保存されます。ブートシーケンスの一部となる `/etc/rc2.d/S68SEOS` ファイルが作成されます。
 - IBM AIX の場合、`SEOS_syscall` スクリプトがロードされます。
5. CA ControlMinder データベースの割り当て、初期設定、およびフォーマットが実行され、`seos.ini` ファイルが作成されます。データベースファイルは、`ACInstallDir/seosdb` ディレクトリに配置されます（`ACInstallDir` は CA ControlMinder のインストールディレクトリです）。
6. マシンが NIS+ であるかどうか判断されます。
 - マシンが NIS+ であると判断された場合は、`[passwd]` セクションの `nis_env` トークンが `nisplus` に設定されます。
 - それ以外の場合、マシンが NIS であれば、`nis_env` トークンが `nis` に設定されます。

さらに、`rpc.nisd` が実行中の場合は、`[passwd]` セクションの `NisPlus_server` トークンが `yes` に設定されます。
7. サポートされている 32 ビットプラットフォーム Sun Solaris、IBM AIX、HP-UX、および Linux では、NIS または DNS でマシンが実行されているかどうか、このスクリプトによって判断されます（キャッシュを使用）。NIS または DNS でマシンが実行されていると判断された場合は、自動的に `lookaside` データベースが作成され、`seos.ini` ファイルの `[seosd]` セクションにある 2 つのトークン（`under_NIS_server` および `use_lookaside`）が `yes` に設定されます。

注: 他のプラットフォームの場合は、`lookaside` データベースをインストールするかどうかを確認するメッセージ、およびインストール先ディレクトリを指定するように指示するメッセージが表示されます。
8. 以下の追加情報を入力するよう促されます（これらの設定は、インストールの終了後いつでも変更できます）。
 - 監査ファイルの読み取りができる監査者グループの名前。
 - すべての UNIX ユーザ、ユーザグループ、およびホストを CA ControlMinder データベースに追加するかどうか。

- データベースを PMDB にサブスクライブするかどうか。サブスクライブする場合は、そのデータベース名。

この質問に回答しても、データベースを PMDB に実際にサブスクライブしたことにはなりません。サブスクリプションを後で作成した場合に、指定された PMDB がこのデータベースに更新情報を提供するだけです。

この質問に対しては、以下のように指定すれば問題ありません。

目的のアクション	指定方法
特定の PMDB にデータベースをサブスクライブする	PMDB の名前。形式は <i>pmd_name@hostname</i>
(少なくとも後から指定するまで) どの PMDB にもデータベースをサブスクライブしない	Enter キー

上記のいずれも指定しないで「_NO_MASTER_」と入力すると、データベースを任意の PMDB にサブスクライブできます。ただし、このように指定すると PMDB の選択ができなくなるため、問題が発生する可能性があります。

- パスワード Policy Model 名。
- CA ControlMinder のセキュリティ管理者となるユーザ。
- CA ControlMinder で企業ユーザをサポートするかどうか。サポートする場合、任意のユーザをセキュリティ管理者として定義するかどうか。
- FIPS 専用インストールを選択した場合、暗号化に関する FIPS 専用オプションを指定するかどうか。
- FIPS 専用の暗号化を選択しなかった場合、デフォルトの暗号化方式を変更するかどうか。

CA ControlMinder では、対称鍵、公開鍵、およびこの 2 つの組み合わせを、選択可能な暗号化オプションとして用意しています。

- 公開鍵暗号化を選択した場合、CA ControlMinder では、サブジェクトの証明書とルート of 証明書を提供する方法を指定できます。

選択内容に応じて、CA ControlMinder では SSL を容易に設定できます。

- 対称暗号化を選択した場合、新しい暗号化鍵を設定するかどうか。

注: 暗号化の詳細については、「リファレンス ガイド」の「*sechkey*」を参照してください。

- ベースライン セキュリティ ルールをインストールするかどうか。

ベースライン セキュリティ ルールをインストールすることで、管理者はシステム、パスワードおよびログ ファイルの保護を強化するための 2 つのルールセットを含むパッケージをインストールできます。このうちの 1 つのルールセットは、すべてのプラットフォームに適用され、CA ControlMinder ファイルを保護します。もう 1 つのルールセットは UNIX ファイルを保護し、Sun Solaris、HP-UX および IBM AIX の各プラットフォームに固有のルールセットです。この 2 つのルールセットは、いずれか一方のみをインストールすることはできません。ベースライン セキュリティ ルールは警告モードでインストールされます。情報は提供されますが、実際に保護は適用されません。したがって、ルールを理解した後に警告モードを解除することをお勧めします。

- リモート ホストから CA ControlMinder を起動できるようにするかどうか。
- レポート エージェントを有効にするかどうか。有効にする場合は、CA Enterprise Log Manager を有効にするかどうか。

レポート エージェントは、データベースのスケジュール済みスナップショットをメッセージ キューに送信します。レポート エージェントを有効にする場合は、配布サーバのホスト名、使用するポート、キューの名前を定義する必要があります。CA Enterprise Log Manager を有効にする場合は、さらに監査ログ ファイルのタイムスタンプされたバックアップを保持するように指定することもできます。

- SAM エージェントを有効にするかどうか。

SAM エージェントは、ローカル コンピュータを SAM 用に設定し、このコンピュータから特権アカウントのパスワードを取得できるようにします。SAM エージェントを有効にする場合は、配布サーバのホスト名、使用するポート、キューの名前を定義する必要があります。

- このエンドポイントを、拡張ポリシー管理のために設定するかどうか。設定する場合は、偏差計算結果の送信先である配布ホスト (DH) 名。

`dhName@hostName` という形式で DH ホスト名を定義します。たとえば、`host123.comp.com` という名前のホストに配布サーバをインストールした場合は、`DH__@host123.comp.com` を使用する必要があります。

インストール後の設定

インストールが完了したら、CA ControlMinder を環境に合わせて設定する必要があります。

以下の手順に従います。

1. PATH 環境変数に `ACInstallDir/bin` ディレクトリを追加します。

デフォルトでは、インストールディレクトリは `/opt/CA/AccessControl/` です。

2. [seos.ini](#) (P. 318) ファイル トークンをチェックして、設定が要件を満たしていることを確認します。

必要に応じて設定を変更します。

3. CA ControlMinder のマニュアル ページにアクセスできるようにするには、自分の MANPATH に `ACInstallDir/man` ディレクトリを追加します。

たとえば、`csh` シェルを現在のセッションで使用している場合は、次のコマンドを入力します。

```
setenv MANPATH $MANPATH:/opt/CA/AccessControl//man
```

今後のセッションのため、`.login`、`.profile`、または `.cshrc` ファイルに同様の行を追加します。

CA ControlMinder の起動

X Window 環境で作業している場合は、CA ControlMinder を起動し、それがシステムに適切にインストールされていることを確認します。重要なシステム保護を開始するには、以下の手順に従ってください。

1. **root** (スーパーユーザ) 権限でログインし、2 つのウィンドウを開きます。
2. いずれかのウィンドウで以下のコマンドを入力します。

```
seload
```

seload コマンドで 3 つのデーモン (エンジン、エージェント、および Watchdog) が起動されるまで待機します。

3. 3 つのデーモンを起動した後、もう一方のウィンドウに移動して以下のコマンドを入力します。

```
secons -t+ -tv
```

CA ControlMinder によって、オペレーティング システムのイベントを報告するメッセージがファイルに記録されます。**secons -tv** コマンドを入力すると、メッセージが画面上にも表示されます。

4. **seload** コマンドを指定した最初のウィンドウで、以下のコマンドを入力します。

```
who
```

CA ControlMinder のトレース メッセージが書き込まれる 2 番目のウィンドウに注意して、CA ControlMinder が **who** コマンドの実行をインターセプトし、そのことについて報告するかどうかを確認します。**who** コマンドのインターセプトが報告された場合、CA ControlMinder はシステムに適切にインストールされています。

5. 必要な場合は、さらにコマンドを入力して **CA ControlMinder** の反応を確認します。

データベースには、アクセスの試行を禁止するためのルールがまだ準備されていません。この場合でも、**CA ControlMinder** はシステムを監視しているため、**CA ControlMinder** がインストールされ実行されているシステムの動作を確認し、**CA ControlMinder** がインターセプトするイベントを確認することができます。

6. 以下のコマンドを入力して、**seosd** デーモンを停止します。

```
secons -s
```

以下のメッセージが画面に表示されます。

CA ControlMinder は現在停止中です。

エンドポイントへの拡張ポリシー管理の設定

拡張ポリシー管理サーバコンポーネントをインストールしたら、拡張ポリシー管理を行うために企業内の各コンピュータを設定する必要があります。その際、サーバコンポーネントとの間で情報の送信先および受信元として機能するエンドポイントを設定します。

注: この手順では、拡張ポリシー管理を行うために **CA ControlMinder** の既存のインストールを設定する方法を示します。エンドポイント上に **CA ControlMinder** をインストールした時にこの情報を指定している場合は、再びエンドポイントを設定する必要はありません。

エンドポイントを設定して拡張ポリシー管理を実行できるようにするには、コマンドウィンドウを開き、次のコマンドを入力します。

```
dmsmgr -config -dhname dhName
```

dhName

エンドポイントが対応する分散ホスト（DH）名のカンマ区切り形式のリストを定義します。

例: DH__@centralhost.org.com

このコマンドでは、拡張ポリシー管理を行うためにエンドポイントが設定されます。また、定義された DH と動作するようにエンドポイントが設定されます。

注: 詳細については、「リファレンス ガイド」の「dmsmgr -config」コマンドの説明を参照してください。

レポート作成のための UNIX エンドポイントの設定

CA ControlMinder エンドポイント管理 およびレポート ポータルのインストールおよび設定の完了後、配布サーバにデータを送信して処理するようにエンドポイントを設定できます。そのためには、レポート エージェントを有効にして設定します。

注: CA ControlMinder をインストールすると、レポート作成のためにエンドポイントを設定することが可能になります。この手順では、インストール時にこのオプションを設定しなかった場合、レポートを送信するための既存のエンドポイントを設定する方法について説明します。

レポート作成のための UNIX エンドポイントの設定方法

1. `ACSharedDir/lbin/report_agent.sh` を実行します。

```
report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number  
[-rqueue queue_name]]
```

設定オプションを省略すると、デフォルト設定が使用されます。

注: `report_agent.sh` スクリプトの詳細については、「リファレンス ガイド」を参照してください。

2. データベース内に `+reportagent` ユーザを作成します。

このユーザは、ADMIN 属性および AUDITOR 属性、ならびローカル端末への書き込みアクセス権を有する必要があります。また、`epassword` をレポート エージェント共有秘密キー（配布サーバのインストール時に定義）に設定する必要があります。

3. レポート エージェント プロセス用に `SPECIALPGM` を作成します。

`SPECIALPGM` は、`root` ユーザを `+reportagent` ユーザにマップします。

注: レポート エージェントを有効にしたら、CA ControlMinder 構成設定を変更してパフォーマンス関連の設定を変更できます。レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

例: selang を使用してレポート作成に UNIX Endpoint を設定する

次の `selang` コマンドは、レポート エージェントを有効にして設定した場合に、どのように必要なレポート エージェント ユーザを作成し、レポート エージェント プロセスの特別なセキュリティ権限を指定するかを示します。

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) ¥
Nativeuid(root) pgmtype(none)
```

CA ControlMinder のカスタマイズ

CA ControlMinder を使用して本格的にセキュリティを実装するには、適用するセキュリティ ポリシーを定義する必要があります。ポリシーの定義に要する時間は、サイトの規模および選択したセキュリティの管理方法によって異なります。

たとえば大学の場合、通常は CA ControlMinder に学生を定義せず、`resource_default` の設定のみに基づいてアクセスを規制することになるでしょう。一方、銀行の場合は、すべてのユーザを CA ControlMinder に定義し、特定のリソースには特定のユーザのみがアクセスできるように、すべてのリソースのアクセス リストを設定することが考えられます。したがって、ユーザ数が同じであっても、CA ControlMinder の実装にかかる時間は銀行よりも大学の方が短くなります。

セキュリティ管理者は、プロジェクトの目的を定義する必要があります。サイトのポリシーに関する決定は慎重に行う必要があります。CA ControlMinder には、各サイトでセキュリティ ポリシーを実装する際に便利な複数のカスタマイズ可能なファイルが含まれています。

trusted プログラム

trusted プログラムとは、プログラムが変更されていない場合のみ、実行できるプログラムです。通常、これは `setuid/setgid` プログラムです。CA ControlMinder では、通常のプログラムも trusted として指定できます。プログラムが改ざんされていないことが確実な場合は、そのプログラムを PROGRAM クラスに登録します。このクラスは、CA ControlMinder によってその整合性が保護されます。

trusted プログラムは、*program pathing* と併用できます。これにより、ユーザは trusted プログラムによって特定のタスクのみを実行できます。

注: プログラム パスの詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

CA ControlMinder には、ユーザがすべての **setuid** プログラムと **setgid** プログラムを trusted として登録するためのスクリプトが用意されています。

1. **setuid** プログラムと **setgid** プログラムをすべて記憶する手間を省くために、以下に示すように **seuidpgm** プログラムを使用します。このプログラムはファイルシステムを検索して、**setuid** プログラムと **setgid** プログラムをすべて検出し、検出されたすべてのプログラムを **PROGRAM** クラスで登録するために **selang** のコマンドのスクリプトを作成します。

以下のコマンドを発行します。

```
seuidpgm -q -l -f / > /opt/CA/AccessControl//seuid.txt
```

このようにして実行された **seuidpgm** プログラムは、以下の処理を行います。

- (/ から始めて) ファイル システム全体を検索します。
- メッセージを表示しません (-q オプションを指定すると、「cannot chdir」メッセージは表示されません)。
- シンボリック リンクをすべて無視します (-l)。
- **FILE** クラスと **PROGRAM** クラスの両方にプログラムを登録します (-f)。
- ファイル **/opt/CA/AccessControl//seuid.txt** にコマンドを出力します。

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

2. テキスト エディタを使用して **seuid.txt** ファイルをチェックし、trusted として登録するすべての **setgid/setuid** プログラムがこのファイルに含まれていること、およびそれ以外のプログラムが含まれていないことを確認します。必要に応じてファイルを編集します。
3. **selang** を使用して、編集したコマンドファイルを実行します。 **seosd** デーモンが実行中でない場合は、-l スイッチを指定します。

```
selang [-l] -f /opt/CA/AccessControl//seuid.txt
```

selang の実行が完了するまで数分かかる場合があります。

4. **seosd** デーモンがまだ実行されていない場合は、**seosd** デーモンを再起動します。次に、システムが所定の動作を実行しているかどうか、**setuid** プログラムが起動できるかどうかを確認します。
5. セキュリティ管理者が知らない間に、**trusted** ではない新しい **setuid** プログラムまたは **setgid** プログラムが追加されて実行されるのを防ぐために、**PROGRAM** クラスのデフォルトのアクセス権を **NONE** に設定しておくことをお勧めします。

以下の **selang** コマンドを入力して、このデフォルトのアクセス値を設定します。

```
chres PROGRAM _default defaccess(none)
```

注: CA ControlMinder を長く使用しているユーザは、この接続に **UACC** クラスを使用することを思い付くかもしれません。 **UACC** クラスはこのバージョンでも存在するので、リソースのデフォルトアクセス権の指定に使用できます。ただし、使いやすさを考慮した場合、クラスのデフォルトアクセス権を指定するには、そのクラスの **_default** レコードを使用することをお勧めします。 **_default** を使用した指定は、同じクラスの **UACC** を使用した指定より優先されます。

登録した **setuid** プログラム、**setgid** プログラム、および通常プログラムを表す **PROGRAM** クラスのレコードには、実行可能ファイルの以下の属性が格納されます。

- デバイス番号
- i-node
- 所有者
- グループ
- サイズ
- 作成日
- 作成時刻
- 最終変更日
- 最終変更時刻
- MD5 シグネチャ

- SHA1 シグネチャ
- チェックサム CRC（巡回冗長チェック）

登録する各プログラムの最も重要な属性は、そのプログラムが **trusted** であることです。これは、そのプログラムが実行しても安全であることを意味します。すでに記載された属性に変化があると、プログラムの **trusted** ステータスは失われます。その場合、CA ControlMinder は、そのプログラムが実行されないようにすることができます。

未登録プログラムの使用の監視

データベースに適切なプログラムをすべて登録できたかどうかわからない場合は、以下のコマンドを使用して、未登録のプログラムの有無を調べることができます。

```
chres PROGRAM _default warning
```

この **warning** プロパティにより、**PROGRAM** クラスに警告モードが設定されます。つまり、未登録の **setuid** プログラムまたは **setgid** プログラムが使用されるたびに、特別な監査レコードが警告として表示されます。ただし、未登録プログラムの使用は妨げられません。

監査ログの確認

監査ログで **untrusted** レコードを手動で検索することができます。または、特定のプログラムが **untrusted** プログラムになったときに通知されるように、特別な通知方法を設定することができます。特別な通知方法を設定すると、ユーザは **untrusted** になったプログラムを使用することを、管理者に連絡する必要がなくなるので便利です。管理者は、ファイルが **untrusted** プログラムになったという通知を受け取ったらすぐにファイルをチェックします。

注: 特別な監査通知を設定する方法については、「[エンドポイント管理ガイド](#)」を参照してください。

保護

trusted ではない **setuid** コマンドおよび **setgid** コマンドの実行を阻止するには、以下のコマンドを発行します。

注: データベースには、自動的にユーザ「**nobody**」が含まれます。

```
newres PROGRAM _default defaccess(none) ¥
owner(nobody) audit(all)
```

CA ControlMinder では、新規プログラムまたは変更されたプログラムを実行する前に管理者の承認を要求することにより、バックドアまたはトロイの木馬から保護します。

たとえば、新しく有用な **setuid** プログラムを受け取ったとします。このプログラムがトロイの木馬でないことが確実で、すべてのユーザがこのプログラムを実行できるようにしたいとします。このプログラムを **trusted** プログラムとして登録するには、以下のコマンドを発行します。

```
newres PROGRAM program-pathname ¥ defaccess(EXEC)
```

untrusted プログラムから trusted プログラムへの再変換

プログラムのサイズや変更日時、またはその他の監視対象プロパティの変更により、このプログラムが **untrusted** 状態になった場合、管理者がそのプログラムを再度 **trusted** 状態にして、データベースにその承認を再度登録するまで、このプログラムを再び実行することはできません。プログラムを再度 **trusted** 状態にするには、以下のコマンドを入力します。

```
editres PROGRAM program_name trust
```

注: **seretrust** ユーティリティを使用して、プログラムを再度 **trusted** 状態にすることもできます。このユーティリティおよびそのオプションの詳細については、「リファレンスガイド」を参照してください。

初期設定ファイル

このセクションでは、CA ControlMinder によって初期設定時に読み込まれるさまざまなファイルについて説明します。デフォルトでは、初期設定ファイルは、**seos.ini** ファイルがあるディレクトリ（CA ControlMinder のインストールディレクトリ）に作成されます。

seos.ini

seos.ini ファイルでは、グローバルパラメータを設定します。

注: ファイルおよびサポート対象のトークンの構造の詳細については、「リファレンスガイド」を参照してください。

seos.ini ファイルは、インストール時の初期状態では保護されており、CA ControlMinder の実行中は更新できません。ただし、すべてのユーザは READ 権限でいつでも seos.ini ファイルにアクセスできます。CA ControlMinder が実行中であっても権限のあるユーザが seos.ini ファイルを更新できるようにするために、以下のコマンドを入力します。

```
newres FILE ACInstallDir/seos.ini owner(authUser) defacc(read)
```

ACInstallDir は CA ControlMinder のインストールディレクトリであり、デフォルトでは /opt/CA/AccessControl/ です。

このコマンドにより、ファイルのデフォルトのアクセス権は「読み取り」に設定されます。ただし、ファイルの所有者である *authUser* のみに、ファイルの更新権限が与えられます。

注: 多数のユーティリティがその実行中に seos.ini ファイルにアクセスするので、このファイルのデフォルトのアクセス権を「読み取り」に設定しておくことが重要です。ファイルを読み込めない場合、ユーティリティの実行は失敗します。

トレース フィルタ ファイル

このオプションのファイルには、あらゆる種類の **CA ControlMinder** トレース メッセージを除外するためのフィルタ マスクを指定するエントリが保存されています。

トレース フィルタ ファイルでは、フィルタ処理で除外するトレース メッセージ（つまり、トレース ファイルに表示しないトレース メッセージ）を指定します。表示を抑止するメッセージのグループを識別するマスクを各行に指定します。たとえば、以下のファイルでは、**WATCHDOG** または **INFO** で始まるすべてのメッセージ、および **BYPASS** で終わるすべてのメッセージを表示しません。

```
WATCHDOG*  
*BYPASS  
INFO*
```

デフォルトでは、**trcfilter.init** という名前のトレース フィルタ ファイルが使用されます。**seos.ini** ファイルの **[seosd]** セクションで **trace_filter** トークンの値を編集して、トレース フィルタ ファイルの名前および場所を変更できます。

トレース レコードをフィルタするには、必要に応じてファイルを編集します。ファイルに注釈（コメント行）を追加するには、行の先頭にセミコロン（;）を入力します。

trcfilter.init ファイルは、ユーザ トレースによって生成された監査レコードをフィルタしません。これらの監査レコードをフィルタするためには、**audit.cfg** ファイルを編集します。

注: 詳細については、「リファレンス ガイド」にある「**seosd** ユーティリティ」を参照してください。

拡張ポリシー管理

作成した複数ルールポリシー (selang コマンド) は、格納し、指定の方法で企業にデプロイすることができます。このポリシー ベースの方法を使用すれば、ポリシー バージョンを格納した上で、それらをホストまたはグループ ホストに割り当てることができます。ポリシーは割り当てられると、デプロイのためにキューに登録されます。あるいは、ホストまたはホスト グループに対するポリシー バージョンのデプロイおよびデプロイ解除を直接行うこともできます。

注: 拡張ポリシー管理の詳細については、「エンタープライズ管理ガイド」を参照してください。

拡張ポリシー管理の設定

拡張ポリシー ベースの管理を使用するように企業内の設定をするには、DMS および DH を中央の 1 つの場所にインストールし、[拡張ポリシー管理を行うために各エンドポイントを設定します](#) (P. 320)。

インストール後に、拡張ポリシー管理を行うために階層を設定するには、dmsmgr ユーティリティを使用します。

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

エンドポイントのポリシー偏差計算の設定

各エンドポイントは、ポリシー偏差計算が可能なように設定する必要があります。通常、この設定はインストール中に行います。この手順は、そうではなく、インストール後にその設定を実行することを目的にしています。

エンドポイントにポリシー偏差計算を設定するには、以下の selang コマンドを入力します。

```
so dms+(DMS@host)
DMS@host
```

上記の形式で指定された DMS の名前を定義します。

sesu および sepass ユーティリティ

オペレーティング システムの `passwd` コマンドの代わりに `sepass` を使用し、`su` の代わりに `sesu` を使用することをお勧めします。そのためには、元のシステム バイナリを保存し、`sepass` および `sesu` へのシンボリック リンクとそれぞれ置き換える必要があります。この処理が終了したら、これらのユーティリティが常に使用できることを確認します。

ほとんどのオペレーティング システムでは、CA ControlMinder がロードされていなくても、`sepass` および `sesu` ユーティリティが動作します。ただし、一部のオペレーティング システム（たとえば、AIX）では、CA ControlMinder がロードされていないと、これらのユーティリティは動作しません。このようなオペレーティング システムのために、CA ControlMinder ではラッパー スクリプトを用意しています。

sesu および sepass ラッパー スクリプト

`sesu` および `sepass` ラッパー スクリプトは、以下のディレクトリにあります。

`ACInstallDir/samples/wrappers`

このファイルには、以下のファイルが含まれています。

ファイル	説明
<code>sesu_wrap.sh</code>	<code>sesu</code> のラッパー スクリプト
<code>sepass_wrap.sh</code>	<code>sepass</code> のラッパー スクリプト
README	これらのラッパーの用途および概念に関する情報が含まれるテキスト ファイル

ラッパー スクリプトを使用した `sesu` の実行

CA ControlMinder がロードされていないときに `sesu` ユーティリティがオペレーティング システムで動作しない場合は、ラッパー スクリプトを使用して `sesu` ユーティリティを実行します。

注: CA ControlMinder がロードされていないとき `sesu` ユーティリティが動作しない場合は、この手順のみを実行する必要があります。

ラッパー スクリプトを使用して `sesu` を実行する方法

1. テキスト エディタを使用して、`sesu_wrap.sh` スクリプトを開きます。
テキスト エディタにラッパー スクリプトが表示されます。
2. 必要ならば、以下の 2 つの変数を変更します。

SEOSDIR

CA ControlMinder インストール ディレクトリを定義します。デフォルトでは、デフォルトのインストール ディレクトリに設定されています。

```
/opt/CA/AccessControl/
```

SYSSU

交換対象の元の `su` システム バイナリの名前を定義します。デフォルトでは、以下のディレクトリに設定されます。

```
/usr/bin/su.orig
```

3. `sesu` ユーティリティを指す `su` シンボリック リンクではなく、`sesu_wrap.sh` ラッパー スクリプトを指す `su` シンボリック リンクを代わりに使用します。

`su` を実行するたびに、`sesu` ラッパー スクリプトが `sesu` ユーティリティを実行します。

ラッパー スクリプトを使用した `sepass` の実行

CA ControlMinder がロードされていないとき、`sepass` ユーティリティがオペレーティング システムで動作しない場合は、ラッパー スクリプトを使用して `sepass` ユーティリティを実行します。

注: CA ControlMinder がロードされていないとき `sepass` ユーティリティが動作しない場合は、この手順のみを実行する必要があります。

ラッパー スクリプトを使用して `sepass` を実行する方法

1. テキスト エディタを使用して、`sepass_wrap.sh` スクリプトを開きます。
テキスト エディタにラッパー スクリプトが表示されます。

- 必要ならば、以下の 2 つの変数を変更します。

SEOSDIR

CA ControlMinder インストールディレクトリを定義します。デフォルトでは、デフォルトのインストールディレクトリに設定されています。

`/opt/CA/AccessControl/`

SYSPASSWD

交換対象の元の `sepass` システム バイナリの名前を定義します。デフォルトでは、以下のディレクトリに設定されます。

`/usr/bin/passwd.orig`

- `sesu` ユーティリティを指す `su` シンボリック リンクではなく、`sesu_wrap.sh` ラッパー スクリプトを指す `su` シンボリック リンクを代わりに使用します。

`passwd` を実行するたびに、`sepass` ラッパー スクリプトが `sepass` ユーティリティを実行します。

メンテナンス モードの保護(サイレント モード)

CA ControlMinder には、メンテナンス モード (サイレント モードとも呼ばれる) が実装されています。CA ControlMinder デーモンがメンテナンスのために停止した場合は、このモードにより保護されます。メンテナンス モードでは、これらのデーモンが停止している間、CA ControlMinder ではイベントが拒否されます。

CA ControlMinder は、稼動している場合には、セキュリティを脅かすイベントをインターセプトして、イベントを許可するかどうかをチェックします。メンテナンス モードをアクティブにしないと、CA ControlMinder サービスが停止している間、すべてのイベントが許可されます。メンテナンス モードをアクティブにした場合は、CA ControlMinder デーモンが停止すると、イベントは拒否されます。このため、システムのメンテナンスが行われている間、ユーザの活動は停止されます。

メンテナンス モードは調整することができます。デフォルトでは、無効です。

CA ControlMinder セキュリティ サービスが停止している間は、以下のような状態になります。

- メンテナンス モードがアクティブである場合、セキュリティを脅かすイベントはすべて拒否されます（ただし、特別な場合、およびメンテナンス ユーザによって実行されるイベントは除きます）。
- メンテナンス モードが無効である場合、CA ControlMinder は介入せず、実行はオペレーティング システムに渡されます。

メンテナンス モードがアクティブでセキュリティが停止しているときに拒否されたイベントは、監査ログ ファイルに記録されません。

メンテナンス モードを有効にするには、以下の手順に従います。

重要: root がメンテナンス ユーザでない場合、メンテナンス ユーザ用に開いているセッションがあることを確認します。そのようなセッションがない場合、ログインすることはできません。

1. CA ControlMinder デーモンが停止していることを確認します。
2. seini ユーティリティを使用して、トークン `silent_deny` の値を `yes` に変更します。

トークンは、SEOS_syscall セクションにあります。

```
seini -s SEOS_syscall.silent_deny yes
```

3. トークン `silent_admin` の値を数値の UNIX UID に変更し、CA ControlMinder デーモンが停止している間、この UNIX UID がコンピュータにアクセスできるようにします。

```
seini -s SEOS_syscall.silent_admin <maintenance_UID>
```

注: root は、デフォルトのメンテナンス モード ユーザ (UID 0) です。

重要: メンテナンス ユーザが root でない場合は、メンテナンス モードで CA ControlMinder を起動できるように CA ControlMinder 認証デーモン `setuid` を root ユーザに設定します。この変更を行うには、以下のコマンドを入力します。

```
chmod 6111 seosd
```

4. `seload` コマンドを使用して、CA ControlMinder デーモンを起動します。

注: メンテナンス モード ユーザが root でない場合は、`seosd` コマンドを使用して CA ControlMinder デーモンを起動します。

Solaris ゾーンへのインストール方法

Solaris 10 ゾーンへの CA ControlMinder のインストールは標準インストールと同様です。Solaris 10 への CA ControlMinder のインストールに推奨されているのは Solaris ネイティブ パッケージング (pkgadd および pkgrm) コマンドを使用する方法です。

重要: CA ControlMinder が非グローバル ゾーンで動作するためには、まずグローバル ゾーンにインストールする必要があります。

CA ControlMinder をすべてのゾーン、または選択されたゾーンのみにインストールするかどうかに応じて、以下のいずれかのメソッドを使用します。

- [Solaris ネイティブ パッケージを使用した CA ControlMinder のインストール \(P. 328\)](#)

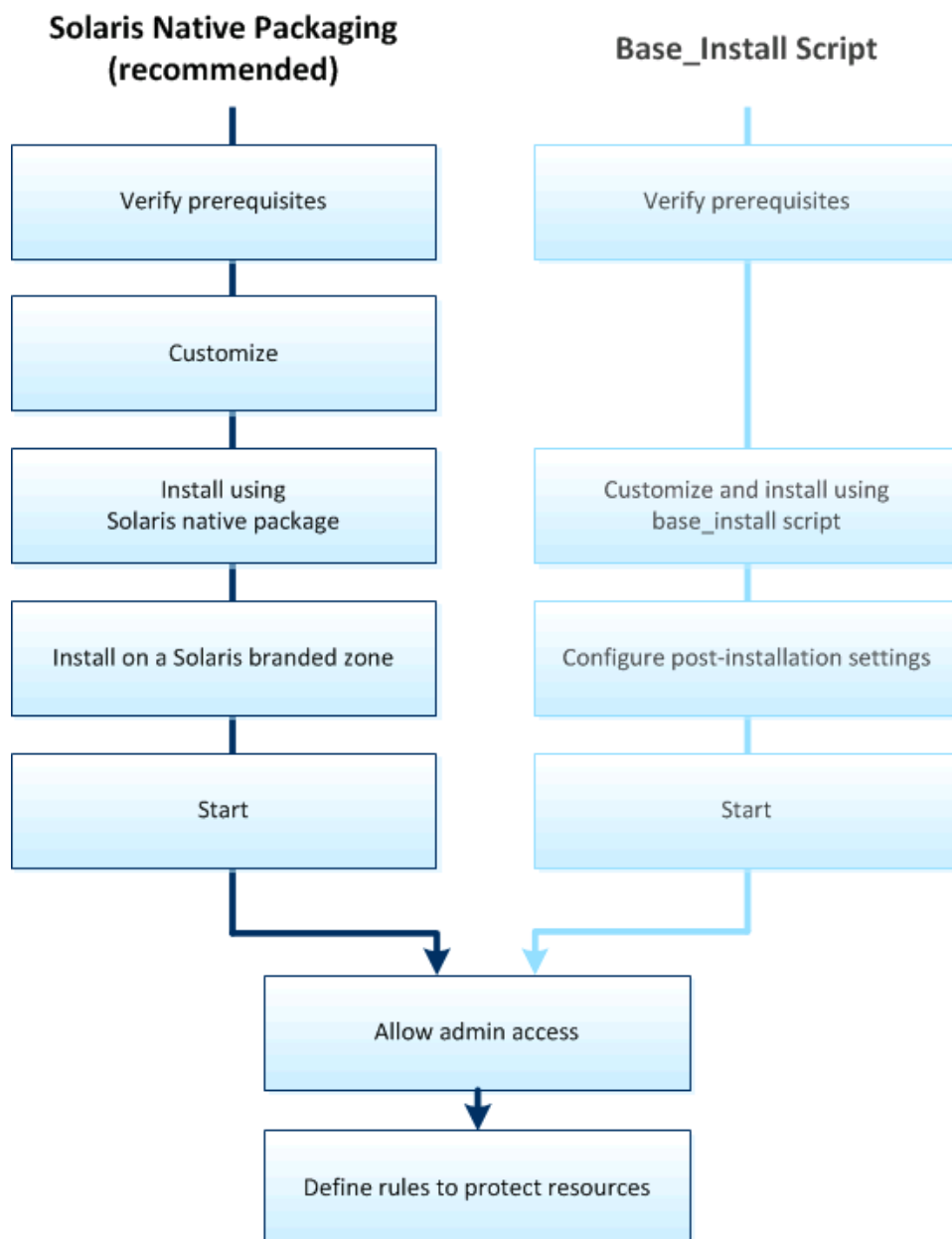
Solaris ネイティブ パッケージ インストールを使用することをお勧めします。次のいずれかを実行できます。

- [すべてのゾーンへの CA ControlMinder のインストール \(P. 261\)](#)
- [グローバル ゾーンおよび選択されたゾーンに CA ControlMinder をインストールします。 \(P. 267\)](#)

- [install_base スクリプトを使用した CA ControlMinder の選択されたゾーンへのインストール \(P. 340\)](#)

install_base スクリプトを使用すると、このスクリプトを実行したゾーンに CA ControlMinder がインストールされます。まずグローバルゾーンに CA ControlMinder をインストールします。

How to Install on Solaris Zones



次の手順に従ってください:

1. 以下のいずれか 1 つの方法を使用して CA ControlMinder をインストールします。
 - [Solaris ネイティブ パッケージを使用した CA ControlMinder のインストール \(P. 328\)](#) (推奨)
 - a. [前提条件の確認 \(P. 329\)](#)
 - b. [Solaris ネイティブ パッケージのカスタマイズ \(P. 330\)](#)
 - c. [Solaris ネイティブ パッケージのインストール \(P. 334\)](#)
 - d. [Solaris ブランド ゾーンへのインストール \(P. 335\)](#)
 - e. [通信での ioctl の使用 \(P. 337\)](#)
 - f. [CA ControlMinder の起動 \(P. 338\)](#)
 - [install base スクリプトを使用した各ゾーンへの CA ControlMinder のインストール \(P. 340\)](#)
 - a. [前提条件の確認 \(P. 340\)](#)
 - b. [install base スクリプトを使用したカスタマイズおよびインストール \(P. 341\)](#)
 - c. [インストール後の設定 \(P. 308\)](#)
 - d. [CA ControlMinder の起動 \(P. 309\)](#)
2. [zlogin を使用した管理者アクセスの許可 \(P. 345\)](#)
3. [リソースを保護するためのルールの定義 \(P. 345\)](#)

注: Solaris 11 の制限事項のため、CA ControlMinder パッケージはインストール中に非グローバル ゾーンに適用されません。Solaris ネイティブ パッケージ ツール (pkgadd) を使用して、各ゾーンに個別に CA ControlMinder をインストールすることをお勧めします。

Solaris ネイティブ パッケージを使用したインストール

Solaris のネイティブ パッケージングは、コマンドライン ユーティリティとして提供されます。このため、各パッケージを個別に作成、インストール、削除、およびレポートすることができます。

注: Solaris ネイティブ パッケージングの詳細については、[Sun Microsystems の Web サイト](#)ならびに `pkgadd`、`pkgrm`、`pkginfo`、および `pkgchk` に関するマニュアルページを参照してください。

通常のインストールの代わりに、CA ControlMinder に用意されている Solaris ネイティブ パッケージを使用することができます。このため、インストールした CA ControlMinder を、Solaris ネイティブ パッケージングを使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、CA ControlMinder をアンインストールするには、`pkgrm` コマンドを使用する必要があります。 `uninstall_AC` スクリプトは使用しないでください。

Solaris ネイティブ パッケージを使用してすべてのゾーンに CA ControlMinder をインストールする場合、初めてのインストールの後に作成したゾーンにも CA ControlMinder が自動的にインストールされます。ただし、インストール後の CA ControlMinder 手順スクリプトは、非グローバルゾーンから、新しいゾーンに対して実行する必要がありますが、これらのスクリプトは新しいゾーンの設定が完了した後でないと実行できません。特に、「`zlogin -C zonename`」コマンドを実行する必要があります (名前サービス、`root` パスワードなどの設定を完了させる必要があります)。

重要: 「`zlogin -C zonename`」コマンドを実行しなかった場合、または新しいゾーンのブートおよびログインを早急に行った場合、CA ControlMinder のインストールは不完全なものとなります。これは、インストール後スクリプトが実行されていないからです。

注: 新しいゾーンの正しい設定方法の詳細については、Sun の「*System Administration Guide: Solaris Containers--Resource Management and Solaris Zones*」を参照してください。このドキュメントは [Sun Microsystems Documentation の Web サイト](#)にあります。

前提条件の確認

サポートされている各 Solaris オペレーティング システムに対する Solaris ネイティブ パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

- pre.tar
- _Solaris_PKG*.tar.Z
- convert_eac_pkg
- customize_eac_pkg

_Solaris_PKG*.tar は Solaris 用のネイティブ パッケージです。pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA ControlMinder の使用許諾契約が含まれています。

次の手順に従ってください:

1. メディアから一時ディレクトリ `$PACKAGE_DIR` (グループおよび全員に読み取り可能) にインストール ファイルをコピーします。たとえば `/tmp` などです。

```
cp /mnt/AC_DVD/NativePackages/_Solaris_PKG*.tar.Z $PACKAGE_DIR
cp /mnt/AC_DVD/NativePackages/pre.tar             $PACKAGE_DIR
cp /mnt/AC_DVD/NativePackages/*_eac_pkg           $PACKAGE_DIR
```

2. `$PACKAGE_DIR` 内の tar アーカイブをアンパックします。

```
cd $PACKAGE_DIR
zcat _Solaris_PKG*.tar.Z | tar -xvf -
```

重要: パッケージを抽出する際には、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認します。そうしないと、Solaris ネイティブ パッケージング ツールはそのパッケージを破損したものとみなします。

3. システムが C++ ライブラリの正しいバージョンをサポートしていることを確認します。

```
pvs -d /usr/lib/libCstd.so.1
libCstd.so.1;
SUNW_1.1.1;
SUNW_1.1;
SUNW_1.2;
SUNW_1.3;
SUNW_1.3.1;
```

Solaris ネイティブ パッケージのカスタマイズ

ネイティブ パッケージを使用して **CA ControlMinder** をインストールする前に、**CA ControlMinder** パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストールパラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、**CA ControlMinder** パッケージをカスタマイズしてください。

次の手順に従ってください:

1. 使用許諾契約を表示します。

```
customize_eac_pkg -a -d $PACKAGE_DIR CAeAC
```

2. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

3. 使用許諾契約への同意を示すキーワードを提供します。

```
customize_eac_pkg -w keyword -d $PACKAGE_DIR CAeAC
```

4. (オプション) インストールパラメータ ファイルの言語を *lang* に変更します。デフォルトでは、インストールパラメータ ファイルは英語で記述されています。

```
customize_eac_pkg -r -l lang -d $PACKAGE_DIR CAeAC
```

5. (オプション) デフォルトの暗号化ファイルを変更します。

```
customize_eac_pkg -s -c certfile -k keyfile -d $PACKAGE_DIR CAeAC
```

6. /tmp からカスタムパス (たとえば /opt/CA/) にインストール先ディレクトリを変更します。

```
customize_eac_pkg -i /opt/CA -d $PACKAGE_DIR CAeAC
```

7. デフォルト値を使用して応答ファイル「**paramtemplate**」を作成します。

```
customize_eac_pkg -g -f $PACKAGE_DIR/paramtemplate -d  
$PACKAGE_DIR CAeAC
```

8. **paramtemplate** ファイル内のデフォルト値を、自分の環境に固有のデータで変更します。

paramtemplate ファイルでは、パッケージに対するインストールデフォルトを設定できます。たとえば、**POSTEXIT** 設定（前の **#** 文字を削除します）をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ

customize_eac_pkg コマンドは、CA ControlMinder Solaris ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な CA ControlMinder Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、**pre.tar** ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_pkg -g -f tmp_params -d pkg_location pkg_name
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(オプション) カスタマイズする CA ControlMinder パッケージの名前です。パッケージを指定しない場合、スクリプトはデフォルトでメインの CA ControlMinder パッケージ (CAeAC) を選択します。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション) ファイルシステム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで `/var/spool/pkg` を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: `-g` オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (stdout) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを `-f` オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 `-l` オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストールディレクトリを *install_loc*/AccessControl に設定します。

-k *keyfile*

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-l *lang*

インストールパラメータファイルの言語を *lang* に設定します。言語の設定は、-r オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。デフォルトでは、インストールパラメータファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストールパラメータファイルからの入力を使用するようにします。

-t *tmp_dir*

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは /tmp です。

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、-a オプションを使用します。

注: DH の暗号のオプション用のパラメータが、*install_base* がインストールされている環境のものと同じであることを確認します。

Solaris ネイティブ パッケージのインストール

インストールした **CA ControlMinder** を、インストールされたほかのソフトウェアと同様に管理するには、**CA ControlMinder Solaris** ネイティブ パッケージをカスタマイズしてインストールします。すべてのゾーンで必ず同じ **CA ControlMinder** バージョンを使用するようにしてください。

Solaris ネイティブ パッケージングでは、デフォルトで、ユーザによる操作を必要とする場合があります。また、サイレントモードでインストールを実行するためには、以下のように設定することをお勧めします。

注: インストール管理ファイル (**myadmin**) およびその使い方の詳細については、**pkgadd (1M)** および **admin (4)** に関する **Solaris** のマニュアルページを参照してください。

次の手順に従ってください:

1. サイレントインストールを有効化するために **\$CONFIG_DIR** 内にインストール管理ファイルを生成します。

```
convert_eac_pkg -p
```

ファイル「**myadmin**」は一般的なテンプレートから作成されます。

2. **myadmin** ファイルを編集し、以下の設定を変更します。

```
setuid = nocheck  
action = nocheck
```

サイレントモードで実行するようにインストール管理ファイルを設定しました。

3. `-n` オプションを使用して、カスタマイズされた CA ControlMinder パッケージをサイレント インストールします。

以下のいずれかの操作を実行します。

- すべてのゾーンにインストールするには、グローバル ゾーンから以下のコマンドを実行します。

```
pkgadd -n -a $CONFIG_DIR/myadmin -d $PACKAGE_DIR CAeAC
```

- 選択したゾーンへインストールする場合は、以下の操作を行います。

グローバル ゾーンから以下のコマンドを実行します。

```
pkgadd -G -n -a $CONFIG_DIR/myadmin -d $PACKAGE_DIR CAeAC
```

選択された各非グローバル ゾーンで以下のコマンドを実行します。

```
pkgadd -n -a $CONFIG_DIR/myadmin -d $PACKAGE_DIR CAeAC
```

インストールが完了します。これで CA ControlMinder を開始できます。

Solaris ブランド ゾーンへのインストール

Solaris の `pkgadd` は、Solaris 10 のグローバル ゾーンにインストールされているアプリケーションのブランド ゾーンへのプロパゲートをサポートしません。CA ControlMinder は、`syscall` ではなく `ioctl` を使用してカーネル モジュールとの通信を行う必要があります。

注: グローバル ゾーンにインストールすると、インストール パラメータ ファイルによって、ブランドのゾーンも自動的にインストールできるようになります。

次の手順に従ってください:

1. `$PACKAGE_DIR/paramtemplate` ファイルを編集し、以下の設定を変更します。

```
UseBrandZone = "yes"
```

2. `seos.ini` ファイルを編集し、以下の行を変更します。

```
SEOS_use_ioctl = 1
```

CA ControlMinder は `ioctl` を使用するよう設定されます。

3. `pkgadd` を使用して、CA ControlMinder を Solaris 10 ブランド ゾーンにインストールします。

```
customize_eac_pkg -s -f $PACKAGE_DIR/paramtemplate -d $PACKAGE_DIR CAeAC  
pkgadd -G -a $PACKAGE_DIR/myadmin -d $PACKAGE_DIR CAeAC
```

4. `pkgadd` を使用して、CA ControlMinder を Solaris 8 および 9 ブランド ゾーンにインストールします。

```
customize_eac_pkg -s -f $PACKAGE_DIR/paramtemplate -d $PACKAGE_DIR CAeAC  
pkgadd -n -a $PACKAGE_DIR/myadmin -d $PACKAGE_DIR CAeAC
```

警告を無視し、確認を求められたら「y」を入力します。

インストールが完了します。これで、ブランドゾーンで CA ControlMinder を開始できるようになります。

重要: `SEOS_use_ioctl` が 0 に設定されている場合は、すべてのゾーンにおける通信に `ioctl` を使用するよう **CA ControlMinder** を変更する必要があります。この変更を行い、すべてのゾーンを再起動すると、インストールは完了します。

通信での ioctl の使用

CA ControlMinder を Solaris ブランド ゾーンにインストールする場合は、`syscall` ではなく `ioctl` を使用してカーネル モジュールと通信する必要があります。

次の手順に従ってください:

1. グローバル ゾーンおよびそれ以外のすべてのゾーンで、CA ControlMinder を停止します。

最後のゾーンを停止します。イベント インターセプトが無効になり、カーネル モジュールをアンロードするための準備が開始されます。

```
zlogin -z zone_name /opt/CA/AccessControl/bin/secons -sk
```

2. グローバル ゾーンで CA ControlMinder カーネル モジュールをアンロードします。

```
SEOS_load -u
```

注: `SEOS_load -u` コマンドを実行すると、CA ControlMinder のアンロードの前に、CA ControlMinder が非グローバル ゾーンで実行されることは決してありません。

3. CA ControlMinder がインストールされている各ゾーン（グローバル、非グローバル、およびブランド ゾーン）で、`seos.ini` エントリを 1 に設定します（デフォルトでは、0 に設定されています）。

```
SEOS_use_ioctl = 1
```

4. カーネル モジュールをグローバル ゾーンにロードします。

```
SEOS_load
```

これによって、擬似デバイスがインストールされ、CA ControlMinder が `ioctl` によってカーネル モジュールと通信し、`ioctl` を使用できるようになるために再起動が必要なゾーンを識別できるようになります。

5. CA ControlMinder がインストールされている各非グローバル ゾーンおよびブランドゾーンを再起動します。

ゾーン内での CA ControlMinder の起動および停止

Solaris 10 ゾーン内での CA ControlMinder の起動および停止は、通常、Solaris コンピュータでの CA ControlMinder の起動および停止の場合と同じ方法で実行されます。

ゾーンでの CA ControlMinder の起動には、以下の例外が適用されます。

- CA ControlMinder カーネル モジュール (SEOS_load) は、グローバル ゾーンからしかロードできません。
- 非グローバルゾーンで CA ControlMinder を起動するには、事前にグローバルゾーンに CA ControlMinder カーネル モジュールをロードする必要があります。

CA ControlMinder カーネル モジュールがグローバルゾーンにロードされたら、任意のグローバルゾーンで、任意の順序で CA ControlMinder を起動および停止することができます。

ゾーンでの CA ControlMinder の停止には、以下の例外が適用されます。

- 1 つ以上のゾーンで [メンテナンス モード](#) (P. 323) が有効になっている場合、CA ControlMinder カーネル モジュールをアンロードすることはできません。
- すべてのゾーンで CA ControlMinder を任意の順序で停止するには、各ゾーンで `secons -s` コマンドを実行します。
- すべてのゾーンで CA ControlMinder を同時に停止するには、GHOST レコードにすべてのゾーンを追加し、グローバルゾーンから `secons -s ghost_name` コマンドを発行します。

この方法は、すべてのゾーンで CA ControlMinder をアップグレードするときに有用です。

- 最後のゾーンは `secons -sk` を使用して停止します。これにより、イベント インターセプトが無効にされ、CA ControlMinder カーネル モジュールをアンロードするための準備が行われます。
- CA ControlMinder カーネル モジュール (SEOS_load -u) は、グローバルゾーンからしかアンロードできません。

注: SEOS_load -u コマンドを実行すると、CA ControlMinder のアンロードの前に、CA ControlMinder が非グローバルゾーンで実行されることは決してありません。

非グローバル ゾーン内での CA ControlMinder の起動

通常の場合と同様に非グローバル ゾーンから CA ControlMinder を起動することができますが、それにはまずグローバル ゾーンで CA ControlMinder カーネル モジュールをロードする必要があります。

非グローバル ゾーン内で CA ControlMinder を起動する方法

1. グローバル ゾーン内で `SEOS_load` コマンドを入力して、CA ControlMinder カーネル モジュールをロードします。

CA ControlMinder カーネルがロードされると、任意のゾーンで CA ControlMinder を起動できるようになります。

注: CA ControlMinder カーネルはロードされますが、CA ControlMinder はグローバル ゾーン内のイベントをインターセプトしません。

2. 非グローバル ゾーンでは、`seload` コマンドを入力して CA ControlMinder を起動します。

非グローバル ゾーンは、CA ControlMinder によって保護されます。

注: 非グローバル ゾーンでは、CA ControlMinder をリモートで起動することもできます。詳細については、「リファレンス ガイド」の「`seload`」コマンドの説明を参照してください。

Install_Base スクリプトを使用したインストール

前提条件の確認 (Install_Base)

CA ControlMinder では、UNIX 上に CA ControlMinder を対話形式またはサイレント モードでインストールする `install_base` スクリプトを提供しています。

通常のスクリプト インストール（ネイティブ インストールでなく）を使用する場合は、CA ControlMinder インストール メディアに含まれる 3 つのファイルが必要になります。

- **install_base - tar** ファイルから CA ControlMinder をインストールするスクリプトです。
- **_opSystemVersion_ACVersion.tar.Z** - すべての CA ControlMinder ファイルが含まれている圧縮 tar ファイルです。たとえば、CA ControlMinder r12.0 を IBM AIX バージョン 5 にインストールする場合、使用する tar ファイルは **_AIX5_120.tar.Z** となります。
- **pre.tar** - 圧縮された tar ファイルであり、インストールに関するメッセージおよびエンドユーザ使用許諾契約が含まれています。

エンドユーザ使用許諾契約を読んだ後、インストールを続行するには、そのファイルの最後で検出されるコマンドを入力します。

- サイレント インストール (`install_base -autocfg` を使用) を実行する場合は、**-command** オプションと、エンドユーザ使用許諾契約ファイルの最後で検出されるコマンドを使用します。
- 応答ファイル (`-autocfg file_name`) を使用する場合、**-command** オプションは必要ありません。

ライセンス ファイルの名前と場所を取得するには、`install_base -h` を実行します。間違ったコマンドを入力した場合も、ファイルの名前と場所が得られます。

これらのファイルは、CA ControlMinder Endpoint Components for UNIX DVD の `/Unix/Access-Control` ディレクトリにあります。

Install_Base スクリプトを使用したカスタマイズおよびインストール

`install_base` スクリプトを使用して、CA ControlMinder をインストールできます。これは対話形式のスクリプトですが、サイレントモードでの実行も可能です。

CA ControlMinder のインストール方法

1. CA ControlMinder がすでにインストールされていて実行中である場合は、管理者としてログインし、以下のコマンドを入力して、CA ControlMinder を停止します。
`ACInstallDir/bin/secons -sk`
`ACInstallDir/bin/SEOS_load -u`
2. `root` ユーザとしてログインします。

CA ControlMinder をインストールするには、ルート権限が必要です。
3. 光ディスク ドライブに CA ControlMinder Endpoint Components for UNIX DVD をセットします。

4. エンド ユーザ使用許諾契約の内容を読みます。

`install_base` スクリプトを実行するには、エンド ユーザ使用許諾契約に同意する必要があります。エンド ユーザ使用許諾契約を読んだ後、インストールを続行するには、そのファイルの最後に記述されたコマンドを入力します。ライセンス ファイルの名前と場所を取得するには、`install_base -h` を実行します。

5. (オプション) インストールをカスタマイズします。

注: どのオプション機能をインストールするか決定するには、「[CA ControlMinder 実装ガイド](#)」で [install_base コマンド](#) (P. 297)のオプションを確認します。

例: 以下のカスタマイズされたコマンドでは、対話形式の `install_base` スクリプトを開始してクライアント パッケージを `/opt/CA/AC` ディレクトリにインストールし、スタック オーバフロー防止機能オプションを有効にする方法を示します。

```
/dvdrom/Unix/Access-Control/install_base -client -stop -d
/opt/CA/AC
```

6. クライアントおよびサーバパッケージをインストールします。

例: 以下のコマンドは、対話形式の `install_base` スクリプトを開始し、すべてのデフォルト **CA ControlMinder** 機能でのクライアント パッケージおよびサーバパッケージをインストールします。

```
/dvdrom/Unix/Access-Control/install_base
```

`install_base` スクリプトが開始されます。インストール中には、**CA ControlMinder** のクライアントおよびサーバパッケージのインストールに関する質問に答えるように求められます。この例ではインストールするパッケージを指定していないので、`install_base` コマンドではクライアント パッケージとサーバパッケージの両方がインストールされます。

これで **CA ControlMinder** のインストールは完了しましたが、まだ実行されていません。

インストール後の設定

インストールが完了したら、CA ControlMinder を環境に合わせて設定する必要があります。

以下の手順に従います。

1. PATH 環境変数に *ACInstallDir/bin* ディレクトリを追加します。
デフォルトでは、インストールディレクトリは */opt/CA/AccessControl/* です。
2. [seos.ini](#) (P. 318) ファイル トークンをチェックして、設定が要件を満たしていることを確認します。
必要に応じて設定を変更します。
3. CA ControlMinder のマニュアル ページにアクセスできるようにするには、自分の MANPATH に *ACInstallDir/man* ディレクトリを追加します。
たとえば、*csh* シェルを現在のセッションで使用している場合は、次のコマンドを入力します。

```
setenv MANPATH $MANPATH:/opt/CA/AccessControl//man
```

今後のセッションのため、*.login*、*.profile*、または *.cshrc* ファイルに同様の行を追加します。

CA ControlMinder の起動

X Window 環境で作業している場合は、CA ControlMinder を起動し、それがシステムに適切にインストールされていることを確認します。重要なシステム保護を開始するには、以下の手順に従ってください。

1. *root* (スーパーユーザ) 権限でログインし、2 つのウィンドウを開きます。
2. いずれかのウィンドウで以下のコマンドを入力します。

```
seload
```

seload コマンドで 3 つのデーモン (エンジン、エージェント、および Watchdog) が起動されるまで待機します。

3. 3つのデーモンを起動した後、もう一方のウィンドウに移動して以下のコマンドを入力します。

```
secons -t+ -tv
```

CA ControlMinder によって、オペレーティング システムのイベントを報告するメッセージがファイルに記録されます。**secons -tv** コマンドを入力すると、メッセージが画面上にも表示されます。

4. **seload** コマンドを指定した最初のウィンドウで、以下のコマンドを入力します。

```
who
```

CA ControlMinder のトレース メッセージが書き込まれる 2 番目のウィンドウに注意して、CA ControlMinder が **who** コマンドの実行をインターセプトし、そのことについて報告するかどうかを確認します。**who** コマンドのインターセプトが報告された場合、CA ControlMinder はシステムに適切にインストールされています。

5. 必要な場合は、さらにコマンドを入力して CA ControlMinder の反応を確認します。

データベースには、アクセスの試行を禁止するためのルールがまだ準備されていません。この場合でも、CA ControlMinder はシステムを監視しているため、CA ControlMinder がインストールされ実行されているシステムの動作を確認し、CA ControlMinder がインターセプトするイベントを確認することができます。

6. 以下のコマンドを入力して、**seosd** デーモンを停止します。

```
secons -s
```

以下のメッセージが画面に表示されます。

CA ControlMinder は現在停止中です。

zlogin を使用した管理者アクセスの許可

zlogin ユーティリティを使用することで、管理者はゾーンに入ることができます。非グローバルゾーンにログインできるユーザを制御するには、このユーティリティに対して **LOGINAPPL** リソースを追加する必要があります。

zlogin ユーティリティを保護するために、**CA ControlMinder** には事前に定義された **LOGINAPPL** リソースがあります。

リソースを保護するためのルールの定義

CA ControlMinder では、任意のコンピュータを保護する場合と同じ方法で **Solaris 10** ゾーンを保護します。各ゾーンはそれぞれ、他のゾーンと分離して保護され、**CA ControlMinder** で定義する各ルールは該当するゾーンで作業しているユーザにのみ適用されます。グローバルゾーンに適用するルールは、非グローバルゾーンで認識可能なリソースをカバーするルールであっても、グローバルゾーンからそれらのリソースにアクセスするユーザにのみ適用されます。

注: 必要に応じて非グローバルゾーンのリソースを、非グローバルゾーンおよびグローバルゾーンの両方で確実に保護してください。

例: グローバルゾーンのルールおよび非グローバルゾーンのルール

以下の例では、非グローバルゾーン（myZone1）ファイルを保護するルールを定義します。システムファイルはすべて、グローバルゾーンから常に認識可能です。

保護するファイルは、/myZone1/root/bin/kill（グローバルゾーンからのパス）。このファイルを保護するには、以下の CA ControlMinder ルールを定義します。

■ グローバルゾーンでは：

```
nu admin_pers owner(nobody)
nr FILE /myZone1/root/bin/kill defaccess(none) owner(nobody)
authorize FILE /myZone1/root/bin/kill uid(admin_pers) access(all)
```

■ myZone1（非グローバルゾーン）では：

```
nu admin_pers owner(nobody)
nr FILE /bin/kill defaccess(none) owner(nobody)
authorize FILE /bin/kill uid(admin_pers) access(all)
```

グローバルゾーンと非グローバルゾーンの両方でこれらのルールを使用することで、ユーザ（admin_pers）を定義し、保護すべきリソースとしてファイルを定義し、そのファイルにアクセスする権限をユーザに付与しました。このような処理を両方のゾーンで行わなければ、リソースはリスクを伴います。

CA ControlMinder のアンインストール

Solaris ゾーンから CA ControlMinder をアンインストールする前に、以下の要件を考慮します。

- CA ControlMinder をグローバルゾーンから削除する前に、まずすべての非グローバルゾーンからアンインストールします。
- Solaris ネイティブ パッケージを使用してインストールしてある場合、すべてのゾーンから CA ControlMinder をアンインストールするにはネイティブ パッケージ コマンド `pkgrm` を使用します。

重要: この場合 `uninstall_AC` スクリプトを使用しないでください。

- `install_base` スクリプトを使用して CA ControlMinder をインストールした場合は、個々の非グローバルゾーンからその CA ControlMinder をアンインストールできます。ただし、CA ControlMinder カーネルは、CA ControlMinder がすべてのゾーンで停止された後で、グローバルゾーンからのみアンインストール可能です。

重要: `install_base` を使用してグローバルゾーンから CA ControlMinder をアンインストールし、その後すべてのゾーンからアンインストールする場合、ユーザはゾーンからロックアウトされる場合があります。Solaris ゾーンでの CA ControlMinder のインストールおよびアンインストールには、Solaris ネイティブ パッケージを使用することをお勧めします。

CA ControlMinder の自動起動

CA ControlMinder をテストして、その機能に問題がない場合は、CA ControlMinder の保護機能を実装することができます。

システムの起動時に `seosd` デーモンが自動的に起動して、リソースがすぐに保護されるように設定するには、`ACInstallDir/samples/system.init/sub-dir` ディレクトリを使用します。ここで、`sub-dir` はオペレーティングシステム用のディレクトリです。各サブディレクトリには、`README` ファイルと、それぞれのオペレーティングシステムでこのタスクを実行するための手順が含まれています。

サービス マネジメント機能による CA ControlMinder の管理

Solaris 10 で有効

Solaris サービス管理ファシリティ (SMF) ユーティリティを使用すると、CA ControlMinder デーモンを管理できます。SMF ユーティリティを使用して、Watchdog デーモン (seoswd) を管理する認可デーモン (seosd) および seagent デーモンをコントロールします。seload および secons コマンドの代わりに SMF 固有コマンドを使用します。

注: Solaris 10 に CA ControlMinder をインストールした直後から、サービス管理ファシリティ ユーティリティを使用すると CA ControlMinder を管理できます。

注: seload および secons コマンドの詳細については、「リファレンス ガイド」を参照してください。

SMF コマンドは以下の形式で指定します。

```
#svcadm enable daemon
#svcadm disable daemon
#svcadm restart daemon
#svcadm refresh daemon
#svcs daemon
#svcs -l daemon
#svcadm clear daemon
```

例: seosd デーモンを起動します。

以下の例は、seosd デーモンを開始する方法を示します。

```
#svcadm enable seosd
```

注: このコマンドは seload コマンドの使用と同等です。

例: seosd デーモンを停止します。

以下の例は、seosd デーモンを停止する方法を示します。

```
#svcadm disable seosd
```

注: このコマンドは secons -sk コマンドの使用と同等です。

例: seosd デーモンを再起動します。

以下の例は、seosd デーモンを再起動する方法を示します。

```
#svcadm restart seosd
```

例: seosd 設定を再ロードします。

以下の例は、seosd デーモン設定を再ロードする方法を示します。

```
#svcadm refresh seosd
```

注: このコマンドは secons -rl コマンドの使用と同等です。

例: seosd デーモンのステータスを表示します。

以下の例は、seosd デーモンのステータスを一覧表示する方法を示します。

```
#svcs -l seosd
```

例: seosd デーモンのメンテナンス状態をクリアします。

以下の例は、seosd デーモンのメンテナンス状態をクリアする方法を示します。

```
#svcadm clear seosd
```


第 10 章: UNAB ホストのインストールとカスタマイズ

このセクションには、以下のトピックが含まれています。

[UNAB ホスト \(P. 351\)](#)

[UNAB の実装方法 \(P. 352\)](#)

[はじめに \(P. 353\)](#)

[RPM Package Manager のインストール \(P. 384\)](#)

[Solaris ネイティブ パッケージングのインストール \(P. 393\)](#)

[HP-UX ネイティブ パッケージのインストール \(P. 403\)](#)

[AIX ネイティブ パッケージのインストール \(P. 410\)](#)

[AIX ワークロード パーティション \(WPAR\) ネイティブ パッケージのインストール \(P. 420\)](#)

[インストール後のタスク \(P. 423\)](#)

[完全統合モードでの実装方法 \(P. 429\)](#)

[信頼済みドメイン環境での UNAB の実装 \(P. 440\)](#)

[一方向の信頼関係にあるドメイン環境で UNIX ホストを登録する方法 \(P. 443\)](#)

UNAB ホスト

UNIX 認証ブローカ (UNAB) を使用すると、Active Directory データ ストアを使用して UNIX コンピュータにログインできます。これは、すべてのユーザに対して単一のリポジトリを使用できることを意味します。ユーザは同じユーザ名とパスワードですべてのプラットフォームにログインできます。

UNIX アカウントと Active Directory の統合により、UNIX のユーザおよびグループの基本的なプロパティが Active Directory に転送され、厳密な認証およびパスワードのポリシーが実現されます。これにより、UNIX のユーザとグループを Windows のユーザとグループを管理しているのと同じ場所で管理できます。

注: インストール時に、UNAB はどの既存の PAM モジュールも置換しません。UNABPAM は既存の PAM スタックに挿入されます。

UNAB の実装方法

UNAB を実装する前に、組織内の UNAB のカスタマイズ、インストール、設定を実行する上で必要な手順を見直すことをお勧めします。

1. [UNIX コンピュータ名が正しく解決されることを確認します](#) (P. 370)。
2. [システムの適合性を確認します](#) (P. 367)。

uxpreinstall ユーティリティは、システムが UNAB 要件と互換性があることを確認します

3. [UNAB インストールパッケージをカスタマイズします](#) (P. 371)。

注: UNAB のインストール先に予定しているすべての UNIX ホストについて UNAB インストールパッケージをカスタマイズする必要はありません。各オペレーティングシステムに合わせてインストールパッケージを一度カスタマイズし、それを使用して、UNAB を組織内でインストールします。

4. [CA ControlMinder エンタープライズ管理 と連動するように UNAB を設定します](#) (P. 377)。

CA ControlMinder エンタープライズ管理 サーバユーザ インターフェースを使用して、UNAB エンドポイントを管理します。

5. UNAB パッケージを UNIX ホストへインストールします。

注: システム要件およびオペレーティングシステム サポートの詳細については、「リリースノート」をご覧ください。

6. [Active Directory に UNIX ホストを登録します](#) (P. 423)。
7. [UNAB を開始します](#) (P. 427)。

これにより、UNAB デーモン (uxauthd) が開始されます。

8. CA ControlMinder エンタープライズ管理 でログイン許可ポリシーを作成し、ポリシーを UNAB エンドポイントへ割り当てます。

ログインポリシーによって、UNIX ホストへのアクセスを許可または拒否されるエンタープライズユーザを定義します。

注: ログインポリシーの詳細については、「エンタープライズ管理ガイド」を参照してください。

9. [UNIX ホスト上の UNAB をアクティブにします](#) (P. 428)。

UNAB をアクティブにすると、エンタープライズユーザが UNIX ホストにログインします。

10. (オプション) [完全統合モードで UNAB を実装します](#) (P. 429)。

完全統合モードの場合、UNAB は、Active Directory を使用してユーザの認証および許可を行います。

はじめに

UNAB をインストールするには、事前に準備要件を満たし、必要な情報をそろえておく必要があります。UNAB の実装および事前検証の実行を完了するために必要な手順を見直すことをお勧めします。

インストール モード

UNAB では 2 つのインストール モードがサポートされています。

- **完全統合** - 完全統合モードでは、UNIX ホストは、ユーザの認証および権限付与の両方を Active Directory サーバに依存します。
- **部分統合** - 部分統合モードでは、UNIX ホストは、ユーザの認証のみを Active Directory に依存し、権限付与に関しては、UNIX ベースのユーザストアを使用します。部分統合モードは、UNIX ユーザストアを保守する場合に使用します。

Active Directory サイト サポート

UNAB をインストールする前に、UNAB で Active Directory サイト サポートがどのように実装されるか理解する必要があります。Active Directory サイト サポートは、ネットワーク トラフィックの最適化、接続速度の向上、応答時間の短縮に貢献します。

Active Directory に UNAB エンドポイントを登録すると、デフォルトでは、`uxconsole` ユーティリティによって以下が実行されます。

- エンドポイントの物理的な場所に最も近い Active Directory サイトを検出します。
- `uxauth.ini` ファイル内の `ad` セクションで `ad_site` 設定に Active Directory サイトの名前を書き込みます。

登録が終わると、UNAB エンドポイントは検出された Active Directory サイトのドメイン コントローラ (DC) とのみ通信します。エンドポイントがこのサイトの DC と通信できない場合、UNAB エンドポイントのステータスはオフラインに変わります。

デフォルトの設定は変更しないことをお勧めします。ただし、UNAB インストールパッケージをカスタマイズする場合は、UNAB エンドポイントが通信する DC のリスト、および UNAB エンドポイントが無視する DC のリストを指定できます (それぞれ `lookup_dc_list` および `ignore_dc_list` パラメータ)。これらのリストで指定された DC は、以下の方法で Active Directory サイト サポートと対話します。

- `lookup_dc_list` -- UNAB エンドポイントは、この設定のリストに含まれている DC と通信し、Active Directory サイト サポートまたは DNS クエリによって検出された DC とは通信しません。
- `ignore_dc_list` -- UNAB エンドポイントは、Active Directory サイト サポートまたは DNS クエリによって検出され、この設定のリストに含まれていないすべての DC と通信します。

注: インストールの後、`uxconsole -register` ユーティリティを使用して、UNAB エンドポイントが通信する Active Directory サイトを手動で設定することができます。`uxconsole` ユーティリティの詳細については、「リファレンス ガイド」を参照してください

64 ビット Linux ホストのインストールの考慮事項

UNAB を Linux 64 ビット コンピュータにインストールする前に、以下のオペレーティングシステムの 32 ビット ライブラリがインストールされていることを確認します。

ld-linux.so.2、libICE.so.6、libcrypt.so.1、libdl.so.2、libgcc_s.so.1、libm.so.6、libnsl.so.1、libpam.so.0、libpthread.so.0、libresolv.so.2、libstdc++.so.5（およびカーネル v2.6 上の libstdc++.so.6）、libaudit.so.0（RHEL5 および OEL 5 のみ）。

以下に、必要な関連 RPM パッケージを示します。

- SLE 10 : compat-libstdc++, glibc-32bit、libgcc、pam-32bit
- SLES 9 : glibc-32bit、libgcc、libstdc++、pam-32bit
- RHEL 5 および OEL 5 : audit-libs、compat-libstdc++、glibc、libgcc、pam
- RHEL 4 および OEL 4 : compat-libstdc++、glibc、libgcc、pam
- RHEL 3 : glibc、libgcc、libstdc++、pam

UNAB を Linux s390x 64 ビット コンピュータにインストールする前に、以下のオペレーティングシステムの 32 ビット ライブラリがインストールされていることを確認します。

ld.so.1、libcrypt.so.1、libc.so.6、libdl.so.2、liblaus.so.1（RHEL 3）、libaudit.so.0（RHEL 4、RHEL 5）、libm.so.6、libnsl.so.1、libpam.so.0、libresolv.so.2

以下に、必要な関連 RPM パッケージを示します。

- SLES 10 : compat-libstdc++、glibc-32bit、pam-32bit
- SLES 9 : glibc-32bit、libstdc++、pam-32bit
- RHEL 5 : audit-libs、compat-libstdc++、glibc、pam
- RHEL 4 : audit-libs、compat-libstdc++、glibc、pam
- RHEL 3 : glibc、laus-libs、libstdc++、pam

SSH PAM 設定

UNAB をインストールする前に、オペレーティング システムが PAM 設定の有効化に必要な以下の SSH サーバおよびステートメントをサポートしていることを確認します。

注: SSH 設定ファイルの場所は、特定のカスタムインストールに応じて変わる場合があります。

AIX 用の SSH サーバおよび PAM 設定

SSH サーバ設定ファイルは、以下のディレクトリにあります。

`/etc/ssh/`

OpenSSH 3.6 以前のバージョンを使用するには、`/etc/ssh/sshd_config` 内の以下のエントリを変更します。

`PAM_AuthenticationViaKbdint yes`

OpenSSH 3.7 移行のバージョンを使用するには、`/etc/ssh/sshd_config` 内の以下のエントリを変更します。

`ChallengeResponseAuthentication yes`

`UsePAM yes`

例: AIX 上の OpenSSH 用の pam.conf エントリ

以下の例は、AIX 上で OpenSSH サーバをサポートするための関連エントリが含まれる `pam.conf` の抜粋です。

```
# Entries for OpenSSH
sshd auth optional /usr/lib/security/pam_seos.o
sshd auth optional /usr/lib/security/pam_aix
sshd auth sufficient /usr/lib/security/pam_uxauth.o
sshd auth required /usr/lib/security/pam_aix try_first_pass
sshd account sufficient /usr/lib/security/pam_uxauth.o
sshd account requisite /usr/lib/security/pam_uxauth.o
sshd account required pam_aix
sshd password sufficient /usr/lib/security/pam_seos.o
sshd password sufficient /usr/lib/security/pam_uxauth.o
sshd password required pam_aix
sshd session sufficient /usr/lib/security/pam_uxauth.o
create_homedir
sshd session required pam_aix
```

Tectia SSH Server 4.x 設定ファイル `sshd2_config` は以下のファイル:ディレクトリにあります。

`/etc/ssh2/`

Tectia Server 4.x を使用するには、`/etc/ssh2/ssh2d_config` 内の以下のエントリを変更します。

`AllowedAuthentications ,publickey,keyboard-interactive,password`

`AuthKbdint.Optional pam`

例: AIX 上の Tectia SSH Server 4.x の `pam.conf` エントリ。

以下の例は、AIX 上で Tectia SSH サーバをサポートするための関連エントリが含まれる `pam.conf` の抜粋です。

```
# Entries for tectia (sshd2)
sshd2 auth optional /usr/lib/security/pam_seos.o
sshd2 auth optional /usr/lib/security/pam_aix
sshd2 auth sufficient /usr/lib/security/pam_uxauth.o
sshd2 auth required /usr/lib/security/pam_aix try_first_pass
sshd2 account sufficient /usr/lib/security/pam_uxauth.o
sshd2 account requisite /usr/lib/security/pam_uxauth.o
sshd2 account required pam_aix
sshd2 password sufficient /usr/lib/security/pam_seos.o
sshd2 password sufficient /usr/lib/security/pam_uxauth.o
sshd2 password required pam_aix
sshd2 session sufficient /usr/lib/security/pam_uxauth.o
create_homedir
sshd2 session required pam_aix
```

The Tectia SSH Server 6.x SSH configurations file `sshd-server-config.xml` is located in the following directory:

`/etc/ssh2/`

Tectia SSH Server 6.x を使用するには、`/etc/ssh2/ssh-server-config.xml` ファイルで以下を変更します。

```
<settings windows-logon-type="interactive"
pam-account-checking-only="yes" />
...
<pluggable-authentication-modules service-name="ssh-server-g3"
pam-calls-with-commands="no" />
...
<authentication name="authentication" action="allow">
...
<auth-publickey />
<auth-password />
<auth-keyboard-interactive >
    <submethod-pam />
</auth-keyboard-interactive>
</authentication>
</authentication-methods>
```

例: AIX 上の Tectia SSH Server 6.x の `pam.conf` エントリ。

以下の例は、AIX 上で Tectia SSH サーバをサポートするための関連エントリが含まれる `pam.conf` の抜粋です。

```
# Entries for Tectia (Tectia 6.x)
ssh-server-g3 auth optional      /usr/lib/security/pam_seos.o
ssh-server-g3 auth optional      /usr/lib/security/pam_aix
ssh-server-g3 auth sufficient    /usr/lib/security/pam_uxauth.o
ssh-server-g3 auth required      /usr/lib/security/pam_aix
try_first_pass
ssh-server-g3 account sufficient /usr/lib/security/pam_uxauth.o
ssh-server-g3 account requisite /usr/lib/security/pam_uxauth.o
ssh-server-g3 account required   pam_aix
ssh-server-g3 password sufficient /usr/lib/security/pam_seos.o
ssh-server-g3 password sufficient /usr/lib/security/pam_uxauth.o
ssh-server-g3 password required  pam_aix
ssh-server-g3 session sufficient /usr/lib/security/pam_uxauth.o
create_homedir
ssh-server-g3 session required    pam_aix
```

Solaris 用の SSH サーバおよび PAM 設定

SSH サーバ設定ファイル `sshd_config` は、以下のディレクトリにあります。

```
/usr/local/etc/ssh/
/etc/ssh
```

Open SSH 3.9 以降を使用するには、`sshd_config` ファイル内で以下を変更します。

```
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation no
```

SunSSH 1.1 および SunSSH 1.1.3 を使用するには、`sshd_config` ファイル内で以下を変更します。

```
PAMAuthenticationViaKBDInt yes
```

SunSSH 1.1.1 を使用するには、`sshd_config` ファイル内で以下を変更します。

```
ChallengeResponseAuthentication yes
UsePAM yes
```

Linux 用の SSH サーバおよび PAM の設定

Tectia SSH Server 6.x SSH 設定ファイル `sshd-server-config.xml` は、以下のディレクトリにあります。

```
/etc/ssh2/
```

設定ファイル内の以下のエントリを変更します。

```
<settings windows-logon-type="interactive"
pam-account-checking-only="yes" />
<auth-keyboard-interactive>
  <submethod-pam />
</auth-keyboard-interactive>
```

`/etc/pam.d/ssh-server-g3` ファイルで以下を変更します。

```
auth      include    system-auth
account   required    pam_nologin.so
account   include     system-auth
password  include     system-auth
session   optional    pam_keyinit.so force revoke
session   include     system-auth
session   required    pam_loginuid.so
```

Linux s390 エンドポイントのインストールの考慮事項

CA ControlMinder Linux s390 で UNAB をリモート管理し、Linux IA64 上でレポート機能を使用するためにメッセージキュー機能を使用する場合、J2SE バージョン 5.0 以降をエンドポイントにインストールします。

メッセージキュー機能を使用すると、CA ControlMinder エンドポイントからレポート ポータルおよび CA Enterprise Log Manager に、それぞれレポートおよび監査データを送信することができます。リモート管理では、CA ControlMinder エンタープライズ管理 を使用して UNAB エンドポイントを管理できます。

エンドポイントに CA ControlMinder や UNAB をインストールする前または後に、J2SE をインストールできます。CA ControlMinder または UNAB をインストールした後に J2SE をインストールする場合、エンドポイント上に Java の場所も設定する必要があります。

インストール時の Java の設定

Linux s390、Linux s390x および Linux IA64 で有効

UNAB Linux s390 エンドポイントをリモート管理し、Linux IA64 でレポート機能を使用するためにメッセージキュー機能を使用する場合、サポートされている Java のバージョンをエンドポイントにインストールします。

Linux s390 または Linux IA64 エンドポイントに CA ControlMinder または UNAB をインストールすると、以下が実行されます。

1. 有効な Java 環境へのパスを以下の順序で確認します。
 - a. インストール時の入力データの JAVA_HOME パラメータ。
インストール時の入力データには、対話型の CA ControlMinder インストールで入力された UNAB インストール パラメータ ファイル、UNIX CA ControlMinder インストール パラメータ ファイル、ネイティブ インストール用のカスタマイズされたパッケージ、およびユーザ入力データがあります。
 - b. JAVA_HOME 環境変数。
 - c. (Linux s390 および Linux s390x) デフォルトのインストール パス、
/opt/ibm/java2-s390-50/jre

2. accommon.ini ファイルのグローバル設定で `java_home` 設定の値を以下のいずれかの値に設定します。
 - 有効な Java 環境へのパスがインストール時に見つかった場合、値はこのパスに設定されます。
 - 有効な Java 環境へのパスがインストール時に見つからなかった場合、値は `ACSharedDir/JavaStubs` に設定されます。デフォルトでは、`ACSharedDir` は `/opt/CA/AccessControlShared` です。

Linux s390 および Linux s390x エンドポイント上で Java の場所を設定します。

Linux s390 および Linux s390x に該当

メッセージキュー機能を使用し、UNAB Linux s390 エンドポイントをリモートで管理するには、エンドポイントに J2SE バージョン 5.0 以降をインストールする必要があります。CA ControlMinder または UNAB をインストールした後に J2SE をインストールする場合、追加の設定手順を実行する必要があります。

Linux s390 および Linux s390x エンドポイント上で Java の場所を設定する方法

1. CA ControlMinder および UNAB が実行されている場合は停止します。
2. accommon.ini ファイルのグローバルセクション内の `java_home` 設定の値を、Java のインストールパスに変更します。

例 : `java_home=/opt/ibm/java2-s390-50/jre`

3. CA ControlMinder および UNAB を開始します。

Java の場所が設定されます。

Linux IA64 エンドポイント上での Java の場所の設定

Linux IA64 に該当

CA ControlMinder Linux IA 64 エンドポイント上でメッセージキュー機能およびレポート機能を使用するには、エンドポイントに J2SE バージョン 6.0 以降をインストールします。CA ControlMinder をインストールした後に J2SE をインストールする場合、追加の設定手順を実行します。

Linux IA64 エンドポイント上で Java の場所を設定する方法

1. 実行する場合、CA ControlMinder を停止します。
2. accommon.ini ファイルのグローバルセクション内の `java_home` 設定の値を、Java のインストールパスに変更します。
例： `java_home=/usr/share/java016.0/jre`
3. CA ControlMinder を起動します。
Java の場所が設定されます。

Kerberos と SSO の考慮事項

Kerberos が有効なエンドポイントに UNAB をインストールして登録すると、Kerberos シングルサインオン (SSO) サービスを活用でき、これにより認証が可能となり、同じユーザクレデンシャルで複数のエンドポイントへログインできます。設定されていない場合は、Kerberized ネットワーク サービスおよびアプリケーションのインストールと設定により、エンドポイント上の SSO 機能を有効にします。

設定はシステムにより異なるので、エンドポイント上で Kerberos と SSO を有効にする前に、以下の手順を実行するように強くお勧めします。

- 特に以下に関して、システム マネージャ ページおよび SSO で使用する予定のネイティブ アプリケーション サービス バイナリのリリース特定のオプションを読んでください。
 - sshd(1M)
 - telnetd
 - in.telnetd
 - inetd
 - pam.conf
 - inetd.sec
- Kerberos をサポートするバージョンのネットワーク アプリケーションの PATH 変数を確認します。たとえば、ほとんどの Linux システムでは、Kerberos ツールは `/usr/Kerberos` ディレクトリの下に位置します。

- 以降の Kerberos をサポートするアプリケーションが以下のように設定されていることを確認します。
 - SSH -- クレデンシャル委任をサポートします。たとえば、GSSAPIDelegateCredentials トークンを yes に設定します。
 - SSHD -- GSSAPIAuthentication トークンをサポートし有効にします。
 - Telnet -- Solaris では、PAM スタックが設定され、Kerberos 設定および keytab ファイルが利用可能になっています。シンボリック リンクまたは環境変数 KRB5_CONFIG および KRB5_KTNAME を作成して、keytab ファイルを利用可能にします
 - rlogin -- Kerberos をサポートするバージョンのアプリケーションをインストールします。

注: さらにシステム特定の Kerberos と SSO の設定については、システム ドキュメントを参照します。

例: Solaris 上での Kerberos の設定

以下の例は Solaris 上で Kerberos を設定するのに必要な設定を示しています。この例では、Solaris パッケージをインストールして設定し、Kerberos を有効にします。

重要: 使用しているシステムを Kerberos 用に設定するためには、追加のパッケージをインストールして設定する必要がある場合があります。

- SUNWcry パッケージをインストールして、強力な暗号化を有効にします
- Solaris 10 では、GSSAPIDelegateCredentials が SSH でサポートされていません。
- `svc:/network/shell:kshell`、`svc:/network/login:klogin`、`svc:/network/telnet:default` を有効にして、`rsh`、`rlogin`、および `telnet` のサービスを使用します。
- Kerberos 認証を処理するように、`/etc/pam.conf` ファイルを変更します。

以下は `/etc/pam.conf` ファイルからの断片で、`rlogin`、`rsh` および `telnet` 用に Kerberos 認証を有効にする追加されたセクションを示しています。

```
# Kerberized rlogin サービス
#
krlogin auth required          pam_unix_cred.so.1
krlogin auth required          pam_krb5.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh      auth sufficient        pam_rhosts_auth.so.1
rsh      auth required          pam_unix_cred.so.1
#
# Kerberized rsh service
#
krsh      auth required          pam_unix_cred.so.1
krsh      auth required          pam_krb5.so.1
#
# Kerberized telnet service
#
ktelnet auth required          pam_unix_cred.so.1
ktelnet auth required          pam_krb5.so.1
```

Kerberos が有効な環境では、UNAB 登録はどのように動作するか

ユーザが Active Directory にホストを登録する際に、UNAB によりネイティブ Kerberos と同じ場所内にユーザ チケットが作成されます。その後、ユーザは、Ticket Granting Ticket (TGT) を手動で取得する必要なく、kerberized アプリケーションの使用に透過的に進めます。

Kerberos が有効なホストでの UNAB 登録処理は以下のとおりです。

1. `uxconsole -register` コマンドを実行し、`-sso` 引数を指定して、UNAB を Active Directory に登録します。

`-sso` 引数により、`uxconsole` は `uxauth.ini` ファイルではなく、ホストの Kerberos ファイルを使用することになります。
2. `uxconsole` により、設定の目的で UNAB がホストの Kerberos ファイルを使用できることが確認されます。以下のいずれかのイベントが発生します。
 - a. `uxconsole` により、UNAB を登録するための必須ドメイン情報がそのファイルに含まれることが識別されます。
 - b. `uxconsole` により、登録に必要な情報がそのファイルに含まれないことが識別されます。
3. そのファイルに情報が含まれていない場合、UNAB によりオリジナルファイルのバックアップが作成され、`kerberos_configuration` トークンが内部に設定されます。

注: `uxconsole -deregister` コマンドを使用して Active Directory から UNAB を削除しても、Kerberos 設定ファイルは変更されず、バックアップファイルは削除されません。

4. そのファイルに必要な情報が含まれている場合、`uxconsole` により `kerberos_configuration` トークンが標準に設定されます。
5. `uxconsole` では登録処理が続行されます。

注: `uxconsole -register` コマンドおよび `seos.ini` の `kerberos_configuration` トークンの詳細については、「リファレンス ガイド」を参照してください。

重要: ホスト上の Kerberos ファイルに UNAB を登録するために必要な情報が含まれていない場合、登録は失敗します。

SSO 用の UNAB ホストの有効化

UNAB ホストを SSO 用に設定して、1 つの UNAB ホストにログインしている Active Directory ユーザがそのユーザ名を使用して他の UNAB ホストにログインするようにできます。SSO が有効なモードで、UNAB はそれが UNIX リポジトリで生成したキーを保持します。ユーザが他のホストへログインする際に、Kerberos が有効なアプリケーションは、キーを使用してユーザを認証します。

重要: SSO モードで UNAB を有効にしているホストで Kerberos が有効になっていることを確認します。この手順を開始する前に、`uxpreinstall` ユーティリティを使用して、システムの適合性を確認します。

SSO 用に UNAB ホストを有効化する方法

1. UNIX ホストに root 権限でログインします。
2. SSO モードで、UNAB を Active Directory に登録します。以下のコマンドを実行します。

```
./uxconsole -register -d<active_directory_domain> -sso
```

注: UNAB を SSO モードで登録する前に、UNAB を登録解除する必要はありません。

3. UNAB をアクティブにして、ユーザが UNIX ホストにログインできるようにします。以下のコマンドを実行します。

```
./uxconsole -activate
```

4. `-status -detail` 引数を使用して、Kerberos モードが [標準] に設定されていることを確認します。例：

```
./uxconsole -status -detail | grep Kerberos
```

```
Kerberos configuration - standard
```

これで、SSO 用に UNAB ホストを設定しました。

システム適合性の確認

uxpreinstall ユーティリティは、UNIX コンピュータが UNAB システム要件に適合しているかどうかを確認します。UNAB を開始し、アクティブにする前に、uxpreinstall を使用してシステムの適合性を確認し、ユーティリティが検出したエラーまたは競合を解決しておくことを強くお勧めします。これらのエラーの解決は、UNAB の動作上の問題を防ぐために役立ちます。

重要: uxpinstall ユーティリティは、実在または潜在的な問題を報告しますが、その修正は行いません。このユーティリティを使用して、オペレーティングシステムまたは UNAB を設定することはできません。

uxpreinstall の使用は、UNAB のインストール前でもインストール後でも構いません。uxpreinstall は、エンドポイントや UNAB のインストールを変更しませんが、起こりうる問題を診断し、問題に対する解決方法を提案します。uxpreinstall が検出する問題は、エンドポイントの問題であり、uxpreinstall に関する問題ではありません。

注: UNAB をインストールする前に uxpinstall を実行する場合は、UNAB がインストールされている別のエンドポイントからユーティリティをコピーします。uxpreinstall ユーティリティの詳細については、「リファレンスガイド」を参照してください

システム適合性の確認方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. 詳細レベル 0 で uxpinstall を実行します。

uxpreinstall はチェックを実行し、そのチェックと、検出したエラーまたは競合のサマリを表示します。

3. エラーまたは競合が検出されると、uxpreinstall は詳細レベル 2 以上で再度自動的に実行されます。

uxpreinstall は、検出したエラーおよび競合についてさらに詳細な情報を表示します。

4. エラーと競合を解決します。
5. uxpinstall がエラーまたは競合を検出しなくなるまで、手順 2 ～ 4 を繰り返します。

uxpreinstall の出力にエラーまたは競合が表示されなければ、コンピュータは UNAB 要件に適合しています。この時点で、UNAB を開始し、アクティブにする準備が整っています。

例: uxpreinstall ユーティリティの実行

この例では、Active Directory ドメイン domain.com に対して、管理者ユーザのクレデンシャルで、詳細レベル 3 で uxpreinstall ユーティリティを実行します。

```
./uxpreinstall -a administrator -w admin -d domain.com -v 3
```

Uxconsole および Microsoft ユーティリティを使用した Active Directory のトラブルシューティング

実装プロセスで、登録や有効化の問題など、Active Directory に関してさまざまな問題が発生する可能性があります。uxpreinstall ユーティリティは、問題に関係するすべての要因を収集、特定、および評価するのに役立ちます。Active Directory のトラブルシューティングを強化するため、Microsoft の dcdiag（ドメイン コントローラ診断）ユーティリティおよび netdiag（ネットワーク診断）ユーティリティを使用することもできます。

重要: Windows Server 2003 を使用している場合、dcdiag.exe と netdiag.exe のユーティリティは Support Tools ソフトウェア パンドルに含まれています。詳細については、Microsoft Knowledge Base の記事 KB247811、KB265706、KB321708 を参照してください。

Active Directory のトラブルシューティングを行うには、以下の手順に従います。

1. 詳細レベル 0 で uxpreinstall を実行します。

uxpreinstall はチェックを実行し、そのチェックと、検出したエラーまたは競合のサマリを表示します。

2. エラーまたは競合が検出されると、**uxpreinstall** は詳細レベル 2 以上で再度自動的に実行されます。

uxpreinstall は、検出したエラーおよび競合についてさらに詳細な情報を表示します。

注: **-l** (システム ロガー チェック) および **-k** (シングルサインオン対応チェック) 引数を使用する場合は、出力が大量になるため、慎重に行ってください。

3. **uxpreinstall** 出力をログ記録するには、**uxpreinstall -f** を実行します。
4. **Microsoft dcdiag** ユーティリティの出力をログ記録するには、**dcdiag /f** を実行します。

注: **netdiag** ユーティリティは、ログ ファイル **NetDiag.log** を自動的に作成します。

5. 失敗、エラー メッセージ、警告が発生した場合は、ログ ファイルを確認してください。必要に応じて、**uxpreinstall** および **dcdiag** ユーティリティを実行し、さらに詳細を取得します。
6. ログ ファイルを参照して、正常に完了しなかったアクションおよび警告メッセージを確認します。

エラーは、ユーザ設定によってエラー メッセージではなく警告としてログ記録される場合があります。

7. **dcdiag /test:DNS /v /e** を実行し、ドメイン コントローラ パラメータのトラブルシューティングを行います。
8. ログ ファイルの最後から始めて、出力を確認します。
9. すべての警告およびエラー メッセージを解決するまで、トラブルシューティングを続行します。

例: **dsquery** を使用したユーザとグループのクエリ

以下の例では、ユーザとグループをクエリするために **dsquery** ユーティリティを使用する方法を示します。

```
dsquery user -name user1
dsquery group -name grp1
dsquery * "CN=Users,DC=example,DC=com" -scope base -attr *
```

例: dnscmd ユーティリティを使用した DNS 設定の取得

以下の例では、DNS 設定を取得するために dnscmd を使用方法を示します。

```
dnscmd /enumzones
dnscmd /zoneprint <zonename>
```

例: dsquery ユーティリティを使用した Active Directory サイトの検出

以下の例では、Active Directory サイトを検出するために dsquery ユーティリティを使用する方法を示します。

```
dsquery subnet -name 192.168.*
dsquery site -o dn
dsquery subnet -o rdn -site <mysite>
nltest /DSGETSITECOV
```

UNIX コンピュータ名が正しく解決されることの確認

UNAB が機能するには、UNIX コンピュータおよび Active Directory コンピュータの両方が、UNIX コンピュータの IP アドレスを、ドメイン名を含む同じコンピュータ名に名前解決する必要があります。

UNIX コンピュータ名が正しく解決されることを確認するには、uxpreinstall ユーティリティを実行してください。

例: uxpinstall ユーティリティを使用して、UNIX コンピュータ名が正しく解決されることを確認する

この例では、computer.caom と名付けられた Windows Active Directory サーバと UNIX コンピュータの両方に対して、Linux 上で詳細レベル 3 で uxpinstall を実行した結果が示されています。

```
Locating Active Directory services in domain <DOMAIN.COM>
Locating '_ldap._tcp.DOMAIN.COM.' records in DNS ...
computer.com:389 [100:0] (_ldap)
computer.com:389 [100:0] (_ldap)
Found LDAP services:
  computer:389
Performing name resolution on <computer.com>
Running command "host computer.com" ...
  DNS server reply:
    computer.com has address 192.168.1.1
Name <computer.com> was resolved to IP address <192.168.1.1>
```

例: nslookup コマンドを使用して、UNIX コンピュータ名が正しく解決されることを確認する

この例では、acctdept と名付けられた Windows Active Directory サーバと UNIX コンピュータの両方に対して Linux で正引きの nslookup 名前解決コマンドを実行した結果が示されています。

```
# nslookup acctdept
Server:          172.24.789.0
Address:         172.24.789.0#53

Name:   acctdept.parallel.com
Address: 172.24.123.110
```

UNAB インストール パラメータ ファイル - UNAB インストールのカスタマイズ

UNAB パラメータ ファイルには、必要に応じてカスタマイズできるインストールパラメータが含まれています。

このファイルの形式は以下のとおりです。

AUDIT_BK

監査ファイルのタイムスタンプ付きバックアップを保存するかどうかを指定します。

注: 監査データを配布サーバに送る場合は、この値を「yes」に設定します。この値を「yes」に設定した場合、CA ControlMinder は、監査ファイルが audit_size 設定で指定したサイズ制限に達すると、そのファイルをバックアップし、タイムスタンプを付けます。これによって、すべての監査データがレポート エージェントで使用可能になります。

制限: yes、no

デフォルト: no

COMPUTERS_CONTAINER

UNIX コンピュータが登録される、Active Directory 内のコンテナ名を定義します。

デフォルト: cn=Computers

DIST_SRV_HOST

配布サーバのホスト名を指定します。

制限： 任意の有効なホスト名

デフォルト： none

DIST_SRV_PORT

配布サーバのポート番号を指定します。

制限： SSL: 7243、TCP: 7222

デフォルト： 7243

DIST_SRV_PROTOCOL

配布サーバの通信プロトコルを指定します。

制限： tcp、ssl

デフォルト： ssl

ENABLE_ELM

レポート エージェントが配布サーバにエンドポイント監査データを送信するかどうかを指定します。これによって、CA Enterprise Log Manager と統合されます。

注： この値を「yes」に設定する場合、監査のバックアップを保存するように CA ControlMinder を設定してください（AUDIT_BK=yes）。

制限： yes、no

デフォルト： no

GROUP_CONTAINER

UNIX グループの定義を含む Active Directory コンテナのコンテナ名を定義します。

IGNORE_DC_LIST

LDAP 接続の確立時に UNAB が無視する Active Directory ドメイン コントローラを指定します。

注： 現在のドメインおよび信頼済みドメインの両方からドメイン コントローラを指定できます。

制限： none、カンマ区切りリスト

デフォルト： none

IGNORE_DOMAIN_LIST

ユーザおよびグループの照会時に UNAB が無視する Active Directory ドメインを指定します。

制限： none、UNAB は現在のドメインまたすべての信頼済みドメインを照会、UNAB は現在のドメインのみを照会、無視するドメインのカンマ区切りリスト

デフォルト： none

IGNORE_USER_CONTAINER

Active Directory を検索する際に無視するユーザ コンテナを指定します。

コンテナはセミコロンで区切られたそれぞれの識別名 (DN) により定義されます。コンテナの DN にドメイン名が含まれていない場合、それはクエリ対象のドメインすべてに適用されます。

制限： セミコロンによって区切られたコンテナの DN のリスト、none

デフォルト： none

IGNORE_GROUP_CONTAINER

Active Directory を検索する際に無視するグループ コンテナを指定します。

コンテナはセミコロンで区切られたそれぞれの識別名 (DN) により定義されます。コンテナの DN にドメイン名が含まれていない場合、それはクエリ対象のドメインすべてに適用されます。

制限： セミコロンによって区切られたコンテナの DN のリスト、none

デフォルト： none

INTEGRATION_MODE

UNAB の統合モードを指定します。

制限： 1 - 部分統合、2 - 完全統合

デフォルト： 2

JAVA_HOME

(Linux s390) インストールされた Java 環境のフルパス名を指定します (Java バージョンおよびオペレーティング システムによって異なる)。

Java 環境がデフォルトの場所にインストールされていない場合のみ、このパラメータを指定します。Java 環境がデフォルトの場所にインストールされている場合、インストール プログラムはこのパラメータの値を設定します。

LANG

インストール言語を指定します。

LIC_CMD

ライセンス同意コマンドを指定します。

LOCAL_POLICY

ログイン ポリシー使用オプションを指定します。

制限: yes、UNAB ポリシーおよびローカル ログイン ファイルを使用、no、UNAB ログイン ポリシーのみを使用

デフォルト: no

LOOKUP_DC_LIST

LDAP 接続を確立する Active Directory ドメイン コントローラ (DC) を指定します。

注: 現在のドメインおよび信頼済みドメインの両方から DC を指定できます。使用する DC を指定すると、UNAB は Active Directory から DC のリストを取得します。使用する DC を指定しない場合、UNAB はエンドポイントの物理的な場所に最も近い Active Directory サイトを検出し、そのサイトの DC と通信します。

制限: none、カンマ区切りリスト

デフォルト: none

NTP_SRV

NTP (Network Time Protocol) サーバの名前または IP アドレスを定義します。

REPORT_SHARED_SECRET

レポート エージェントが配布サーバへの認証に使用する、共有秘密鍵を指定します。

制限： 任意の有効な文字列

デフォルト： none

注： 配布サーバをインストールした際と同じ共有秘密鍵を指定する必要があります。

REPORT_SRV_QNAME

スナップショットの送信先のキューの名前を指定します。

制限： キュー名を表す文字列。

デフォルト： queue/snapshots

REPORT_SRV_SCHEDULE

レポート エージェントがレポートを生成し、配布サーバに送信する時間を定義します。

このトークンは次の形式を使用します： 時間@曜日 [,曜日 2] [...]

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

RENAME_KRB_TKT

ユーザ ログイン中に生成された Kerberos チケットの名前を変更するかどうかを指定します。

注： ユーザの Kerberos チケット名がランダム文字列で構成される場合、このオプションを使用して SSO ログインをサポートします。このトークンが有効なとき、スクリプト `/etc/profile.d/uxauth_rename_krb_tkt.sh` によってユーザのチケット名が変更され、該当の値が環境変数 `KRB5CCNAME` に設定されます。

制限： yes、no

デフォルト： no

SSO

UNAB で Kerberos ベースのシングル サインオン (SSO) がサポートされるかどうかを指定します。

制限： yes、no

デフォルト： no

TIME_SYNC

UNAB がシステム時間を NTP (Network Time Protocol) サーバと同期するかどうかを指定します。

注: この値を「yes」に設定すると、NTP_SRV トークンの値を指定する必要があります。この値を「no」に設定すると、UNAB は、/etc/ntp.conf で定義されたシステム時間に対して、UNIX メカニズムを使用します。

制限: yes、no

デフォルト: no

USER_CONTAINER

UNIX ユーザの定義を保持する Active Directory コンテナ名を定義します。

UXACT_ADMINISTRATOR

Active Directory の管理者のユーザ名を定義します。

UXACT_ADMIN_PASSWORD

Active Directory の管理者のアカウント パスワードを定義します。

UXACT_DOMAIN

UNIX コンピュータが所属するドメインを定義します。

UXACT_RUN

インストール中に uxconsole -register コマンドを実行するかどうかを指定します。

制限: yes、no

デフォルト: no

注: uxconsole -register コマンドは、Active Directory サーバの Computers コンテナに UNIX コンピュータを登録します。

UXACT_RUN_AGENT

インストールプロセスの終了時に UNAB デーモンを起動するかどうかを指定します。

制限: yes、no

デフォルト: yes

UXACT_SERVER

Active Directory サーバの名前を定義します。

UXACT_VERB_LEVEL

詳細レベルを定義します。

制限：0 ～ 7

CA ControlMinder エンタープライズ管理を使用した UNAB の管理

CA ControlMinder エンタープライズ管理 を使用して、UNAB エンドポイントを管理できます。ここでは、ワールドビューからの UNAB エンドポイントの表示、ログイン ポリシーおよび設定ポリシーの作成および割り当て、また移行処理中に検出された競合の解決が可能です。CA ControlMinder エンタープライズ管理 で UNAB エンドポイントを管理できるように、CA ControlMinder エンタープライズ管理 に UNAB を登録します。UNAB インストールパッケージをカスタマイズして、パッケージ パラメータを変更します。

注: この手順を完了してから、UNAB をインストールします。

CA ControlMinder エンタープライズ管理を使用した UNAB の管理

1. UNAB パッケージからインストール パラメータを抽出して、一時ファイルに保存します。
2. テキストエディタで一時ファイルを開きます。
3. ユーザの組織に合わせて、以下のパラメータを変更します。

DISTRIBUTION_SRV_HOST

配布サーバのホスト名を指定します。

制限：任意の有効なホスト名

デフォルト：none

DISTRIBUTION_SRV_PROTOCOL

配布サーバの通信プロトコルを指定します。

制限：tcp、ssl

デフォルト：ssl

DISTRIBUTION_SRV_PORT

配布サーバのポート番号を指定します。

制限：ssl: 7243、tcp: 7222

デフォルト：7243

4. カスタマイズしたパッケージにインストールパラメータを設定します。
5. カスタマイズしたパッケージを使用して、**UNAB** をインストールします。

UNAB はカスタマイズされた設定でインストールされます。

6. **acuxchkey** ユーティリティを使用して、**UNAB** ホストへのエンタープライズ管理サーバのインストール中に指定したメッセージキューパスワードを設定します。以下に例を示します。

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

インストールが完了していて、**UNAB** ホスト上でメッセージキューパスワードを設定した後、**UNAB** エンドポイントを管理するために **CA ControlMinder** エンタープライズ管理を使用します。

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

CA ControlMinder との統合

UNAB と CA ControlMinder を同じエンドポイントにインストールする場合、UNAB 機能の一部を活用して、CA ControlMinder 内の UNAB 特定の情報を表示できます。たとえば、監査レコード内の UNIX アカウント名の代わりにエンタープライズユーザ名を表示できます。seos.ini 設定ファイルには、UNAB を CA ControlMinder と統合する際に有効にするトークンが含まれています。

重要: UNAB を CA ControlMinder と統合する前に、エンドポイントに CA ControlMinder バージョン r12.5 以降がインストールされていることを確認します。

[seosd] セクションの以下のトークンは、UNAB と CA ControlMinder の統合を制御します。

use_unab_db

seosd が UNAB データベースを使用してユーザとグループの名前を解決するように指定します。CA ControlMinder は、このトークンによって新規ユーザ ログインなどの UNAB の変化を検出できます。

use_mapped_user_name

seosd が監査レコード内にユーザ企業名を使用するかどうかを指定します。有効な場合、seaudit ユーティリティは UNIX アカウント名ではなく企業ユーザ名を表示します。

[OS_User] セクションの以下のトークンは、UNAB と CA ControlMinder の統合を制御します。

nonunix_unabgroup_enabled

CA ControlMinder が UNAB データベースで非 UNIX ユーザ グループをサポートするかどうかを指定します。有効な場合、CA ControlMinder は UNIX 以外のグループのユーザをサポートします。

osuser_enabled

エンタープライズ ユーザおよびエンタープライズ グループを有効にするかどうかを指定します。

[seos] セクションの以下のトークンは、UNAB と CA ControlMinder の統合を制御します。

auth_login

ログイン権限方法を決定します。このトークンにより、パスワードチェックによるユーザ認証が有効化されます(例: `sesudo`、`sesu`、`sepass`)。

pam_enabled

LDAP データベースでの認証およびパスワード変更のために、ローカルホストで PAM を使用できるようにするかどうかを指定します。

[passwd] セクションの以下のトークンは、UNAB と CA ControlMinder の統合を制御します。

nis_env

ローカルホストが NIS クライアントまたは NIS+ クライアントかどうかを指定します。

change_pam

LDAP データベースにおけるパスワードの認証および変更に、ローカルホストが PAM を使用するかどうかを指定します。このトークンを使用して、`sepass` が外部 `pam` ストア（たとえば UNAB）で動作することを有効にします。

[pam_seos] セクションの以下のトークンは、UNAB と CA ControlMinder の統合を制御します。

PamPassUserInfo

`pam_seos` がユーザ情報を `seosd` に送信するかどうかを指定します。

pam_login_events_enabled

`pam_seos` がログイン イベントを `seosd` に送信するかどうかを指定します。

pam_surrogate_events_enabled

`pam_seos` が代理イベントを `seosd` に送信するかどうかを指定します。

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

RSA SecurID との統合

ユーザの組織で RSA SecurID を使用してユーザの認証を行っている場合、RSA SecurID の機能を使用して UNAB エンドポイントへのユーザ ログインを認証できます。RSA SecurID クライアントがインストールされているホストに UNAB をインストールして、Active Directory でユーザ ログイン ポリシーを管理できます。

RSA SecurID がインストールされているホスト上で UNAB が実行されている場合、UNAB はユーザ ログインを認証しません。UNAB は、ユーザ認証がサードパーティ プログラムによって実行されることを検出します。UNAB はエンドポイント上のユーザ アクティビティを管理します。たとえば、ローカルおよびエンタープライズセキュリティ ポリシーの適用や監査メッセージの生成を行うことができます。

UNAB と RSA SecurID との統合の仕組み

UNAB は PAM スタック機能の活用により RSA SecurID と統合します。PAM スタック機能では、ログインプロセスでのユーザ認証に使用する認証プログラムや認証の実行順序を設定できます。

以下の手順では、UNAB を RSA SecurID と統合する方法を説明します。

1. RSA SecurID がインストールされているエンドポイントに UNAB をインストールします。
2. ユーザ認証の実行順に PAM スタックを設定します。たとえば、ユーザパスワードおよび PIN 番号の認証用に RSA SecurID を呼び出し、それに失敗した場合は UNAB を使用してユーザの Active Directory クレデンシアルを認証するように PAM スタックを設定します。
3. ユーザが UNAB ホストへのログインを試行すると、以下の処理が発生します。

RSA SecurID 認証および UNAB 認証を使用します。

- a. RSA SecurID は、パスワードと PIN 番号を指定するよう、ユーザにメッセージを表示します。
- b. ユーザはパスワードと PIN 番号を入力します。
- c. RSA SecurID は、ユーザのパスワードと PIN 番号の認証を試行します。以下のように処理されます。
 - RSA SecurID はユーザのパスワードと PIN 番号を検証し、ユーザによるログインを許可します。認証プロセスが終了し、ユーザアカウントの管理プロセスが開始されます。
 - RSA SecurID はユーザのパスワードと PIN 番号を拒否します。
 - UNAB は、Active Directory ユーザアカウントまたはローカルアカウントのクレデンシアルを指定するよう、ユーザにメッセージを表示します。
 - UNAB は、ユーザクレデンシアルの認証を試行し、認証に成功した場合、認証プロセスは終了し、ユーザアカウントの管理プロセスが開始されます。

例: Red Hat Advanced Server 5.3 での RSA SecurID 認証の使用

/etc/pam.d/system-auth ファイルの以下のスニペットは、Red Hat Linux Advanced Server 5.3 でのユーザ認証が RSA SecurID のみによって実行されることを示します。

```
auth required pam_securid.so
```

例: Red Hat Linux Advanced Server 5.3 での RSA SecurID、ローカル UNIX、および UNAB 認証の使用

/etc/pam.d/system-auth ファイルの以下のスニペットは、Red Hat Linux Advanced Server 5.3 でのユーザ認証が RSA SecurID、ローカル UNIX、および UNAB によって実行されることを示します。

```
auth sufficient pam_securid.so
auth sufficient pam_unix.so
auth sufficient pam_uxauth.so
```

この例の /etc/pam.d/system-auth ファイルは、RSA SecurID (pam_securid.so) モジュールを呼び出してユーザ クレデンシャルの認証を試行するように設定されています。失敗した場合、ローカル UNIX PAM モジュール

(pam_unix.so) がユーザ クレデンシャルの認証を試行します。失敗した場合、UNAB PAM スタック モジュール (pam_uxauth.so) がユーザ クレデンシャルの認証を試行します。この例では、UNAB PAM モジュールがユーザ クレデンシャルの認証を試行した場合、UNAB はユーザにパスワードの入力を求めません。ローカル UNIX PAM モジュールが UNAB PAM スタック モジュールにパスワードを提供します。

注: 認証プロセスはいずれかの PAM スタック モジュールで完了する場合があります。

例: Red Hat Advanced Server 5.3 での UNAB 認証および RSA SecurID 認証の使用

/etc/pam.d/system-auth ファイルの以下のスニペットは、Red Hat Advanced Server 5.3 でのユーザ認証が UNAB 認証および RSA SecurID 認証を使用して完了することを示しています。

```
auth optional      pam_unix.so
auth sufficient    pam_uxauth.so
auth sufficient    pam_securid.so
```

この例では、RSA SecurID PAM スタック (pam_securid.so) を使用してユーザのパスコードを認証する前に、UNAB PAM スタック (pam_uxauthd.so) を使用してユーザの Active Directory クレデンシャルの認証を試行するように、/etc/pam.d/system-auth ファイルが設定されています。ローカル UNIX PAM スタック モジュール (pam_unix.so) はオプションとして設定されています。これは、ローカル UNIX PAM スタックはユーザを認証せずにユーザにパスワードの入力を求め、そのパスワードを PAM スタックに転送することを示しています。

注: この例の認証プロセスは、RSA SecurID または UNAB モジュールの認証成功で完了します。ローカルの UNIX 認証は使用しません。

RPM Package Manager のインストール

RPM Package Manager (RPM) は、個々のソフトウェアパッケージを作成、インストール、クエリ、確認、更新、および消去することができるコマンドラインユーティリティです。RPM は、UNIX プラットフォームで使用するためのものです。

注: 詳細については、RPM Package Manager の Web サイト (<http://www.rpm.org>) および RPM に関する UNIX のマニュアル ページを参照してください。

CA ControlMinder に用意されている RPM パッケージを使用して、インストールした UNAB を、RPM を使用してインストールされたその他すべてのソフトウェアと同様に管理できます。

UNAB RPM パッケージのインストール

Active Directory ユーザアカウントを使用して、UNIX コンピュータにログインするには、アクセスする各 UNIX コンピュータに UNAB をインストールする必要があります。UNABRPM パッケージを使用すると、Linux コンピュータに UNAB をインストールできます。

UNAB RPM パッケージをインストールする方法

1. Linux コンピュータに root としてログインします。
2. CA ControlMinder Endpoint Components for UNIX DVD の /UNAB ディレクトリにある、該当するサーバプラットフォーム用圧縮 tar ファイルをユーザのファイルシステムの一時的な保存場所にコピーします。

ファイルシステムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。圧縮 tar ファイルには UNAB パッケージおよびインストール ファイルが含まれます。

3. 一時ディレクトリに移動し、圧縮 tar ファイルを解凍し、内容を展開します。たとえば、以下は、_LINUX_Ux_PKG_125.tar.Z という名前のファイルを解凍し、内容を展開するコマンドです。

```
gunzip _LINUX_Ux_PKG_125.tar.Z
tar xvf _LINUX_Ux_PKG_125.tar
```

4. rpm コマンドを使用して、ca-lic パッケージをインストールします。ca-lic は、他すべてのパッケージの前提となる、CA Technologies のライセンス プログラムです。例：

```
rpm -U ca-lic-0.0080-04.i386.rpm
```

ca-lic パッケージがインストールされます。

5. [UNAB パッケージをカスタマイズします \(P. 386\)](#)。

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

6. rpm コマンドを使用して、UNAB パッケージをインストールします。
例：

```
rpm -U uxauth-125-3.0.1517.i386.rpm
```

インストールプロセスが開始します。

インストールプロセスが正常に完了したことを通知するメッセージが表示されます。

注: UNAB パッケージでは、CAWIN 共有コンポーネントもインストールされます。

7. インストールログファイル (uxauth_install.log) を参照して、インストールプロセスに関する情報を確認します。

このログファイルは、UNAB のインストールディレクトリにあります。デフォルトでは以下の場所です。

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

8. [インストールが正常に完了したことを確認します](#) (P. 391)。

UNAB RPM パッケージのカスタマイズ

UNAB をインストールするには、RPM パッケージをカスタマイズして、使用許諾契約への同意を示す必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージを手動で変更することはお勧めしません。代わりに、以下の説明に従って、customize_uxauth_rpm スクリプトを使用してください。カスタム UNAB RPM インストールパッケージを作成するには、ご使用のコンピュータで rpmbuild ユーティリティが使用可能である必要があります。

UNAB パッケージのカスタマイズ

1. まだ実行していない場合は、以下の手順に従います。

- a. CA ControlMinder Endpoint Components for UNIX DVD の /UNAB ディレクトリにある、該当するサーバプラットフォーム用圧縮 tar ファイルをユーザのファイルシステムの一時的な保存場所にコピーします。

ファイルシステムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

- b. 一時ディレクトリに移動し、圧縮 tar ファイルを解凍し、内容を展開します。

圧縮 tar ファイルには UNAB のインストール ファイルが含まれます。

2. インストールパッケージから `uxpreinstall` ユーティリティを抽出する以下のコマンドを入力します。

```
customize_uxauth_rpm -e uxpinstall -f tmp_params [-d pkg_location]
pkg_filename
```

UNAB をインストールする前に、`uxpreinstall` ユーティリティを使用して、システムの適合性を確認してください。

3. (オプション) 以下のコマンドを入力して、インストールパラメータファイルの言語を設定します。

```
customize_uxauth_rpm -r -l lang [-d pkg_location] pkg_filename
```

4. 以下のコマンドを入力して、使用許諾契約を表示します。

```
customize_uxauth_rpm -a [-d pkg_location] pkg_filename
```

5. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

6. 以下のコマンドを入力します。

```
customize_uxauth_rpm -w keyword [-d pkg_location] pkg_filename
```

このコマンドは、ユーザが使用許諾契約に同意したことを指定します。

7. 以下のコマンドを入力して、インストールパラメータ ファイルを取得します。

```
customize_uxauth_rpm -g -f tmp_params [-d pkg_location] pkg_filename
```

8. [インストール要件に合わせて、インストール パラメータ ファイルを編集します \(P. 371\)](#)。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

9. 以下のコマンドを入力します。

```
customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename
```

このコマンドは、カスタマイズしたパッケージにインストール パラメータを設定します。

これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

例: UNAB RPM パッケージのカスタマイズ

以下の例では、uxauth-125-3.0.1517.i386.rpm という名前の UNAB RPM パッケージをカスタマイズする方法が示されます。このパッケージは、/unab_tmp ディレクトリにあります。

- この例では、使用許諾契約とキーワードが表示されます。

```
./customize_uxauth_rpm -a /unab_tmp/uxauth-125-3.0.1517.i386.rpm
```

- この例では、使用許諾契約に同意します。この例では、キーワードは「agreemen」です。

```
./customize_uxauth_rpm -w agreement /unab_tmp/uxauth-125-3.0.1517.i386.rpm
```

- この例ではインストール パラメータ ファイルを取得し、parameters.txt ファイルを同じディレクトリに配置します。

```
./customize_uxauth_rpm -g -f parameters.txt  
/unab_tmp/uxauth-125-3.0.1517.i386.rpm
```

- この例では parameters.txt ファイル内のパラメータでインストール パラメータを設定します。

```
./customize_uxauth_rpm -s -f parameters.txt  
/unab_tmp/uxauth-125-3.0.1517.i386.rpm
```

customize_uxauth_rpm コマンド - UNAB RPM パッケージをカスタマイズします

`customize_eac_rpm` コマンドは、UNAB RPM パッケージのカスタマイズ スクリプトを実行します。

注: パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_rpm -h [-l]
customize_uxauth_rpm -a [-d pkg_location] pkg_filename
customize_uxauth_rpm -w keyword [-d pkg_location] pkg_filename
customize_uxauth_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename
customize_uxauth_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_uxauth_rpm -e uxpreinstall [-d pkgdir] [pgn_name]
customize_uxauth_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

カスタマイズする UNAB パッケージのファイル名を定義します。

注: `-d` オプションを指定しない場合は、パッケージ ファイルの完全パス名を定義する必要があります。

`-a`

使用許諾契約を表示します。

`-e uxpreinstall`

指定すると、インストール パッケージから `uxpreinstall` ユーティリティを抽出します。

`-w キーワード`

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角カッコ [] 内）。使用許諾契約ファイルを検索するには、`-a` オプションを使用します。

`-d pkg_location`

（オプション）ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはパッケージファイルへの完全パス名が *pkg_filename* に含まれているものとみなします。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (**stdout**) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。**-l** オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-l *lang*

インストール パラメータ ファイルの言語を **lang** に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: 指定可能なサポート対象言語の一覧については、**customize_eac_rpm -l -h** を実行してください。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、**-f** オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t *tmp_dir*

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは **/tmp** です。

インストールが正常に完了したことを確認する

UNAB のインストールの完了後、インストールが正常に完了したことを確認する必要があります。

インストールが正常に完了したことを確認するには、以下のコマンドを入力します。

```
rpm -q unab_package_name  
unab_package_name
```

UNAB ネイティブ パッケージの名前を定義します。

UNAB が正常にインストールされた場合、このパッケージがインストールされていることを通知するメッセージが表示されます。

例: インストールが正常に完了したことを確認する

以下の例では、**uxauth** という名前の UNAB ネイティブ パッケージのインストールが正常に完了したことを確認します。

```
rpm -q uxauth
```

UNAB RPM パッケージのアップグレード

UNAB の既存のバージョンがすでにインストールされていて、新規バージョンをインストールする場合、インストール済みのバージョンを削除せずに、UNAB の既存のバージョンをアップグレードできます。UNABRPM パッケージを使用すると、Linux コンピュータ上で UNAB をアップグレードできます。

注: **ca-lic** を手動でアップグレードする必要はありません。

UNAB RPM パッケージのアップグレード方法

1. Linux コンピュータに **root** としてログインします。
2. CA ControlMinder Endpoint Components for UNIX DVD の **/UNAB** ディレクトリにある、該当するサーバプラットフォーム用圧縮 **tar** ファイルをユーザのファイルシステムの一時的な保存場所にコピーします。

圧縮 **tar** ファイルにはインストール ファイルとアップグレードファイルが含まれます。

3. 一時ディレクトリに移動し、圧縮 tar ファイルを解凍し、内容を展開します。たとえば、以下は、`_LINUX_Ux_PKG_125.tar.Z` という名前のファイルを解凍するコマンドです。

```
unzip _LINUX_Ux_PKG_125.tar.Z
tar xvf _LINUX_Ux_PKG_125.tar
```

圧縮パッケージには、UNAB のインストール ファイルとアップグレード ファイルが含まれます。

4. rpm コマンドを使用して UNAB をアップグレードします。例：

```
rpm -U uxauth-125-3.0.1517.i386.rpm --verbose
```

アップグレードプロセスが開始します。

アップグレードプロセスが正常に完了したことを通知するメッセージが表示されます。

UNAB RPM パッケージのアンインストール

UNAB をアンインストールする場合、インストールした UNIX コンピュータから RPM パッケージを削除する必要があります。

UNAB をアンインストールするには、root としてログインし、以下のコマンドを入力します。

```
rpm -e unab_package_name
unab_package_name
```

UNAB ネイティブ パッケージの名前を定義します。

アンインストール プロセスが開始されます。

プロセスが正常に完了したことを通知するメッセージが表示されます。

Solaris ネイティブ パッケージングのインストール

Solaris のネイティブ パッケージングは、コマンドライン ユーティリティとして提供されます。このため、各パッケージを個別に作成、インストール、削除、およびレポートすることができます。

注: Solaris ネイティブ パッケージングの詳細については、[Sun Microsystems の Web サイト](#)ならびに `pkgadd`、`pkgrm`、`pkginfo`、および `pkgchk` に関するマニュアルページを参照してください。

重要: パッケージのインストール後、UNAB をアンインストールするには、`pkgrm` コマンドを使用する必要があります。

Solaris ネイティブ パッケージのカスタマイズ

Solaris ネイティブ パッケージングを使用して UNAB をインストールする前に、インストールパッケージをカスタマイズして、使用許諾契約への同意を指定します。また、パッケージをカスタマイズする際に、カスタムインストール設定を指定することもできます。

以下の手順に従って、UNAB パッケージをカスタマイズします。パッケージを手動で変更することはお勧めしません。代わりに、以下の説明に従って、`customize_uxauth_pkg` スクリプトを使用してください。

Solaris ネイティブ パッケージのカスタマイズ方法

1. カスタマイズするパッケージを、CA ControlMinder Endpoint Components for UNIX DVD の /UNAB ディレクトリからファイルシステムの一時的な保存場所に展開します。

ファイルシステムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

重要: パッケージを抽出する際には、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうしないと、Solaris ネイティブ パッケージング ツールはそのパッケージを破損したものとみなします。

2. (オプション) `customize_uxauth_pkg` スクリプト ファイルおよび `pre.tar` ファイルをファイル システム上の一時的な保存場所にコピーします。

スクリプト ファイルと同じディレクトリ内に `pre.tar` ファイルを配置して、すべての言語でスクリプト メッセージを受信します。 `pre.tar` ファイルは、圧縮された `tar` ファイルであり、インストール メッセージおよび UNAB のエンドユーザ使用許諾契約が含まれています。

注: `customize_uxauth_pkg` スクリプト ファイルと `pre.tar` ファイルは、ネイティブ パッケージの抽出先と同じ場所に格納されています。

3. インストール パッケージから `uxpreinstall` ユーティリティを抽出する以下のコマンドを入力します。

```
customize_uxauth_pkg -e uxpinstall -f tmp_params [-d pkg_location] [pkg_name]
```

UNAB をインストールする前に、`uxpreinstall` を使用して、システムの適合性を確認してください。

4. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_pkg -r -l lang [-d pkg_location] [pkg_name]
```

インストール パラメータ ファイルの言語を設定します。

5. 以下のコマンドを入力します。

```
customize_uxauth_pkg -a [-d pkg_location] pkg_name
```

このコマンドは使用許諾契約を表示します。

6. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

7. 以下のコマンドを入力します。

```
customize_uxauth_pkg -w keyword [-d pkg_location] [pkg_name]
```

このコマンドは、ユーザが使用許諾契約に同意したことを指定します。

8. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]
```

このコマンドはインストール ディレクトリを変更します。

9. 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

```
customize_uxauth_pkg -g -f tmp_params [-d pkg_location] [pkg_name]
```

10. [インストール要件に合わせて、インストール パラメータ ファイルを編集します。](#) (P. 371)

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

11. 以下のコマンドを入力して、カスタマイズされたパッケージのインストール パラメータを設定します。

```
customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

customize_uxauth_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ

customize_uxauth_pkg コマンドは、UNAB Solaris ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な UNAB Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_pkg -h [-l]
customize_uxauth_pkg -a [-d pkg_location] [pkg_name]
customize_uxauth_pkg -w command [-d pkg_location] [pkg_name]
customize_uxauth_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
customize_uxauth_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_uxauth_pkg -e uxpreinstall [-d pkg_location] [pkg_name]
customize_uxauth_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(オプション) カスタマイズする UNAB パッケージの名前です。パッケージを指定しない場合、スクリプトはデフォルトでメインの UNAB パッケージ (uxauth) を選択します。

-a

使用許諾契約を表示します。

-e uxpreinstall

指定すると、インストール パッケージから **uxpreinstall** ユーティリティを抽出します。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、**-a** オプションを使用します。

-l lang

インストール パラメータ ファイルの言語を **lang** に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、**-h** オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-d pkg_location

(オプション) ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで **/var/spool/pkg** を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (**stdout**) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。**-l** オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストール ディレクトリを *install_loc/uxauth* に設定します。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、**-f** オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t *tmp_dir*

インストール操作の一時ディレクトリを設定します。

注: デフォルトの一時ディレクトリは */tmp* です。

UNAB Solaris ネイティブ パッケージのインストール

UNAB Solaris のネイティブ パッケージを使用すると、Solaris 上で UNAB を簡単にインストールできます。

注: 以下の手順では、UNAB がデフォルトの設定でインストールされます。UNAB パッケージは、インストールする前にカスタマイズできます。

UNAB Solaris ネイティブ パッケージのインストール方法

1. (オプション) Solaris ネイティブ インストール時のデフォルトを設定します。

- a. 以下のコマンドを入力します。

```
convert_uxauth_pkg -p
```

インストール管理ファイルを現在の場所に *myadmin* という名前でコピーします。

インストール管理ファイルを編集して、**pkgadd** のインストール時のデフォルトを変更できます。**pkgadd -a** オプションを使用すれば、**UNAB** など、特定のインストール用に変更されたファイルを使用できます。ただし、このファイルは **UNAB** に固有のものではありません。

- b. インストール管理ファイル (*myadmin*) を必要に応じて編集し、そのファイルを保存します。

これで、他のインストールに影響を及ぼすことなく、変更したインストール設定を **CA ControlMinder** ネイティブ インストールのために使用できます。

注: Solaris ネイティブ パッケージングでは、デフォルトで、ユーザによる操作を必要とする場合があります。インストール管理ファイルおよびこのファイルの使い方の詳細については、**pkgadd (1M)** および **admin (4)** に関する Solaris のマニュアル ページを参照してください。

2. 以下のコマンドを入力します。

```
pkgadd [-a dir/myadmin] -d pkg_location uxauth
```

-a dir/myadmin

手順 1 で作成した **myadmin** インストール管理ファイルの場所を定義します。

このオプションを指定しない場合、**pkgadd** ではデフォルトのインストール管理ファイルが使用されます。

pkg_location

UNAB パッケージ (**uxauth**) が格納されているディレクトリを定義します。

重要: パッケージは、公開場所（つまり、グループおよび全員に対する読み取りアクセス権が設定された場所）に配置する必要があります。たとえば、**/var/spool/pkg** です。

注: Solaris ネイティブ パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の UNAB ディレクトリにあります。

これで、UNAB のインストールは完了しましたが、まだ起動されていません。

選択したゾーンへの UNAB Solaris ネイティブ パッケージのインストール

Solaris のネイティブ パッケージングを使用し、選択したゾーンに **UNAB** をインストールすることができます。ただし、**UNAB** をグローバル ゾーンにもインストールする必要があります。

注: Solaris ネイティブ パッケージを使用して、**UNAB** をすべてのゾーンにインストールすることをお勧めします。

選択したゾーンに UNAB をインストールする方法

重要: すべてのゾーンで必ず同じ **UNAB** バージョンを使用するようにしてください。

1. グローバル ゾーンから、以下のコマンドを入力します。

```
pkgadd -G -d pkg_location uxauth  
pkg_location
```

UNAB パッケージ (uxauth) が格納されているディレクトリを定義します。

重要: パッケージは、公開場所 (つまり、グループおよび全員に対する読み取りアクセス権が設定された場所) に配置する必要があります。たとえば、`/var/spool/pkg` です。

このコマンドによって、**UNAB** がグローバルゾーンにのみインストールされます。

2. **UNAB** をインストールする非グローバル ゾーンごとに、以下を行います。
 - a. 非グローバル ゾーンの一時的な保存場所に **uxauth** パッケージをコピーします。
 - b. 非グローバルゾーンから以下のコマンドを入力します。

```
pkgadd -G -d pkg_location uxauth
```

このコマンドは、作業元である非グローバルゾーンに **UNAB** をインストールします (前の手順 1 でコピーしたパッケージを使用)。

これで、内部ゾーンで **UNAB** を開始できるようになります。

注: **UNAB** をグローバルゾーンから削除する前に、すべての非グローバルゾーンからアンインストールする必要があります。

Solaris 上の UNAB のアップグレード

UNAB Solaris ネイティブ パッケージによって、Solaris 上の既存バージョンの UNAB を新規バージョンにアップグレードできます。

Solaris 上の UNAB のアップグレード方法

1. UNAB デーモンをすべて停止します。
2. (オプション) Solaris ネイティブ インストール時のデフォルトを設定します。

- a. 以下のコマンドを入力します。

```
convert_uxauth_pkg -p
```

インストール管理ファイルを現在の場所に *myadmin* という名前でコピーします。

インストール管理ファイルを編集して、*pkgadd* のインストール時のデフォルトを変更できます。*pkgadd -a* オプションを使用すれば、UNAB など、特定のインストール用に変更されたファイルを使用できます。ただし、このファイルは UNAB に固有のものではありません。

- b. インストール管理ファイル (*myadmin*) を必要に応じて編集し、そのファイルを保存します。

これで、他のインストールに影響を及ぼすことなく、変更したインストール設定を CA ControlMinder ネイティブ インストールのために使用できます。

注: Solaris ネイティブ パッケージングでは、デフォルトで、ユーザによる操作を必要とする場合があります。インストール管理ファイルおよびこのファイルの使い方の詳細については、*pkgadd* (1M) および *admin* (4) に関する Solaris のマニュアル ページを参照してください。

3. 以下のコマンドを入力します。

```
pkgadd [-a dir/myadmin] -v -d . UNAB
```

```
-a dir/myadmin
```

手順 1 で作成した *myadmin* インストール管理ファイルの場所を定義します。

このオプションを指定しない場合、*pkgadd* ではデフォルトのインストール管理ファイルが使用されます。

UNAB

UNAB ネイティブ パッケージの名前を定義します。

注: デフォルトディレクトリでないディレクトリに UNAB の旧バージョンをインストールしている場合は、以下のコマンドを実行して UNAB ディレクトリの完全パスを指定します。

```
./customize_eac_pkg -i previous-path -d ./ CAeAC  
-i Previous-path
```

既存の UNAB ディレクトリの完全パスを定義します。

注: 完全パス名の末尾にスラッシュ (/) が含まれていないことを確認します。

これで、UNAB の新バージョンがインストールされましたが、まだ開始されていません。

UNAB Solaris ネイティブ パッケージのアンインストール

UNAB Solaris パッケージインストールをアンインストールするには、UNAB パッケージをアンインストールします。

メインの UNAB パッケージをアンインストールするには、以下のコマンドを入力します。

```
pkgrm unab_package_name  
unab_package_name
```

UNAB ネイティブ パッケージの名前を定義します。

UNAB はコンピュータから削除されます。

HP-UX ネイティブ パッケージのインストール

HP-UX のネイティブ パッケージは、GUI とコマンドライン ユーティリティのセットとして提供されます。これにより、個々のソフトウェア パッケージの作成、インストール、削除、およびレポート作成を行うことができます。HP-UX ネイティブ パッケージでは、リモート コンピュータにソフトウェア パッケージをインストールすることもできます。

注: HP-UX のネイティブ パッケージである、Software Distributor-UX (SD-UX) の詳細については、HP の Web サイト (<http://www.hp.com>) を参照してください。swreg、swinstall、swpackage、および swverify については、man ページも参照できます。

重要: パッケージのインストール後、UNAB をアンインストールするには、*swremove* コマンドを使用する必要があります。

UNAB SD-UX 形式パッケージのカスタマイズ

ネイティブ パッケージを使用して UNAB をインストールする前に、UNAB パッケージをカスタマイズして、使用許諾契約への同意を示す必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、UNAB パッケージをカスタマイズしてください。

サポートされた各 HP-UX オペレーティング システムに対する Software Distributor-UX (SD-UX) 形式パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の UNAB ディレクトリに格納されています。

SD-UX 形式パッケージのカスタマイズ

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

重要: パッケージを展開するときは、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうでないと、HP-UX ネイティブ パッケージング ツールによってパッケージが破損していると見なされます。

2. `customize_uxauth_depot` スクリプト ファイルおよび `pre.tar` ファイルをファイル システム上の一時的な保存場所にコピーします。

`pre.tar` ファイルは、圧縮された `tar` ファイルであり、インストール メッセージおよび UNAB のエンド ユーザ使用許諾契約が含まれています。

注: `customize_uxauth_depot` スクリプト ファイルおよび `pre.tar` ファイルは以下のディレクトリにあります。

```
/uxauth/FILESET/opt/CA/uxauth/lbin
```

3. インストール パッケージから `uxpreinstall` ユーティリティを抽出する以下のコマンドを入力します。

```
customize_uxauth_depot -e uxpinstall -f tmp_params [-d pkg_location] [pkg_name]
```

UNAB をインストールする前に、`uxpreinstall` を使用して、システムの適合性を確認してください。

4. 以下のコマンドを入力します。

```
customize_uxauth_depot -a [-d pkg_location] [pkg_name]
```

このコマンドは使用許諾契約を表示します。

5. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

6. 以下のコマンドを入力します。

```
customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
```

このコマンドは、ユーザが使用許諾契約に同意したことを指定します。

7. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_depot -r -l lang [-d pkg_location] [pkg_name]
```

このコマンドは、インストール パラメータ ファイルの言語を設定します。

8. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]
```

このコマンドはインストールディレクトリを変更します。

9. (オプション) 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

```
customize_uxauth_depot -g -f tmp_params [-d pkg_location] [pkg_name]
```

10. (オプション) [インストール要件に合わせて、インストールパラメータ ファイルを編集します \(P. 371\)](#)。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

11. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]
```

このコマンドは、カスタマイズしたパッケージにインストール パラメータを設定します。

これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。以下の例は、パッケージファイルの抽出先のディレクトリ上にある x86 UNAB SD-UX パッケージをカスタマイズして、使用許諾契約への同意を示す方法を説明しています。

```
cp /mnt/AC_DVD/UNAB/_HPUX11_Ux_PKG_1*.tar.Z /tmp
cd /tmp
zcat _HPUX11_Ux_PKG_1*.tar.Z | tar -xvf -
/uxauth/FILESET/opt/CA/uxauth/lbin/customize_eac_depot -w keyword -d /tmp uxauth
```

これで、/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、UNAB をインストールできるようになりました。

詳細情報:

[customize_eac_depot コマンド - SD-UX 形式パッケージのカスタマイズ \(P. 278\)](#)

customize_uxauth_depot コマンド - SD-UX 形式パッケージのカスタマイズ

customize_uxauth_depot コマンドは、SD-UX 形式パッケージ用の UNAB ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な UNAB HP-UX ネイティブ パッケージのすべてで機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_depot -h [-l]
customize_uxauth_depot -a [-d pkg_location] pkg_name
customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
customize_uxauth_depot -r -l lang [-d pkg_location] [pkg_name]
customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]
customize_uxauth_depot -e uxpreinstall [-d pkg_location] [pkg_name]
customize_uxauth_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

(オプション) カスタマイズする UNAB パッケージの名前です。パッケージを指定しない場合、スクリプトはデフォルトでメインの UNAB パッケージ (uxauth) を選択します。

-a

使用許諾契約を表示します。

-e uxpreinstall

指定すると、インストール パッケージから uxpreinstall ユーティリティを抽出します。

-d *pkg_location*

(オプション) ファイルシステム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで `/var/spool/pkg` を指定します。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (`stdout`) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。**-i** オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストール ディレクトリを *install_loc*/uxauth に設定します。

-l *lang*

インストール パラメータ ファイルの言語を *lang* に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、**-h** オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、-a オプションを使用します。

UNAB HP-UX ネイティブ パッケージのインストール

インストールした UNAB を、インストールされたほかのソフトウェアと同様に管理するには、カスタマイズされた UNAB SD-UX 形式パッケージをインストールします。UNAB SD-UX 形式パッケージを使用すると、HP-UX に UNAB を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

UNAB HP-UX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

HP-UX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. [UNAB パッケージをカスタマイズします](#) (P. 403)。

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のコマンドを使用して、カスタマイズされたパッケージを SD-UX に登録します。

```
swreg -l depot pkg_location
```

```
pkg_location
```

UNAB パッケージが格納されるディレクトリを定義します。

4. 以下のコマンドを使用して、UNAB パッケージをインストールします。

```
swinstall -s pkg_location uxauth
```

SD-UX は、*pkg_location* ディレクトリから、パッケージのインストールを開始します。

これで、UNAB のインストールは完了しましたが、まだ起動されていません。

詳細情報:

[ネイティブ インストールの際に考慮するその他の事項](#) (P. 239)

[SD-UX 形式パッケージのカスタマイズ](#) (P. 274)

HP-UX パッケージのアンインストール

インストールされている UNAB HP-UX パッケージをアンインストールするには、インストール時とは逆の手順で、UNAB パッケージをアンインストールする必要があります。

CA ControlMinder パッケージをアンインストールするには、メインの UNAB パッケージをアンインストールします。

```
swremove unab_package_name
```

```
unab_package_name
```

UNAB ネイティブ パッケージの名前を定義します。

AIX ネイティブ パッケージのインストール

AIX ネイティブ パッケージは、GUI およびコマンドライン ユーティリティのセットとして提供されます。これを使用して、個別のソフトウェア パッケージを管理できます。

注: 一部の AIX バージョンはいくつかのパッケージ形式 (installp、SysV、RPM) をサポートしていますが、UNAB では AIX のネイティブ パッケージ形式 (installp) のみが提供されます。

重要:

- パッケージのインストール後、UNAB をアンインストールするには、*installp* コマンドを使用する必要があります。
- UNAB では、ユーザの認証に AIX Loadable Authentication Module (LAM) ではなく Pluggable Authentication Mode (PAM) を使用します。UNAB をインストールする前に、AIX システムを設定して PAM を有効にする必要があります。
- アプリケーションの失敗を防ぐには、ユーザ ID とプライマリ グループ ID が異なるユーザ ストアから来ていないことを確認します。たとえば、ユーザ ID が */etc/passwd* からのもので、プライマリ グループが Active Directory からのものでないかを確認します。

AIX 上のプラグ可能な認証モジュール(PAM)

デフォルトでは、AIX は識別と認証に Loadable Authentication Module (LAM) を使用します。UNAB がシステムにアクセスするユーザを認証できるようにするには、AIX で PAM を使用するように設定する必要があります。UNAB をカスタマイズしインストールする前に、PAM を使用するように AIX システムを設定します。

注: PAM を有効にできるのは、AIX バージョン 5.3 以降です。

例: PAM を使用するための AIX の設定

以下の例は、PAM を使用するために AIX バージョン 5.3 以降を設定する方法を示しています。PAM は、UNAB が認証のために使用します。

1. PAM 設定ファイルを作成します。

AIX ではデフォルトの `/etc/pam.conf` ファイルは提供されません。

2. `pam.conf` ファイルを開き、基本的なモジュール スタックを含め、ファイルを保存します。以下に例を示します。

```
#
# Authentication
#
ftp      auth      required      /usr/lib/security/pam_aix
imap     auth      required      /usr/lib/security/pam_aix
login    auth      required      /usr/lib/security/pam_aix
rexec    auth      required      /usr/lib/security/pam_aix
rlogin   auth      required      /usr/lib/security/pam_aix
snapp    auth      required      /usr/lib/security/pam_aix
su        auth      required      /usr/lib/security/pam_aix
telnet   auth      required      /usr/lib/security/pam_aix
OTHER    auth      required      /usr/lib/security/pam_aix
#
# Account Management
#
ftp      account    required      /usr/lib/security/pam_aix
login    account    required      /usr/lib/security/pam_aix
rexec    account    required      /usr/lib/security/pam_aix
rlogin   account    required      /usr/lib/security/pam_aix
rsh       account    required      /usr/lib/security/pam_aix
su        account    required      /usr/lib/security/pam_aix
telnet   account    required      /usr/lib/security/pam_aix
OTHER    account    required      /usr/lib/security/pam_aix
#
# Password Management
#
login    password    required      /usr/lib/security/pam_aix
rlogin   password    required      /usr/lib/security/pam_aix
su        password    required      /usr/lib/security/pam_aix
telnet   password    required      /usr/lib/security/pam_aix
OTHER    password    required      /usr/lib/security/pam_aix
#
# Session Management
#
ftp      session     required      /usr/lib/security/pam_aix
imap     session     required      /usr/lib/security/pam_aix
login    session     required      /usr/lib/security/pam_aix
rexec    session     required      /usr/lib/security/pam_aix
```

rlogin	session required	/usr/lib/security/pam_aix
rsh	session required	/usr/lib/security/pam_aix
snapp	session required	/usr/lib/security/pam_aix
su	session required	/usr/lib/security/pam_aix
telnet	session required	/usr/lib/security/pam_aix
OTHER	session required	/usr/lib/security/pam_aix

3. /lib/security に移動し、methods.cfg ファイルを開いて編集します。
4. 以下の行を追加して PAM 認証を有効にし、ファイルを保存します。

```
PAM:  
    program = /usr/lib/security/PAM  
PAMfiles:  
    options = auth=PAM,db=BUILTIN
```

5. /etc/security に移動し、login.cfg ファイルを開いて編集します。
6. PAM への認証タイプを設定し、ファイル auth_type=PAM_AUTH を保存します。

以下に例を示します。

```
chsec -f /etc/security/login.cfg -s usw -a auth_type=PAM_AUTH
```

7. /etc/ssh/ に移動し、sshd_config ファイルを開いて編集します。
8. 以下のパラメータを追加して SSH PAM 認証を有効にし、ファイルを保存します。

```
UsePAM yes
```

注: PAM がサポートされているバージョンの OpenSSH (バージョン 3.9p1 以降) を使用していることを確認します。バージョンを確認するには、以下のコマンドを使用します。

```
ls-lpp -i openssh.base.server
```

9. /etc に移動し、pam.conf ファイルを開いて編集します。

10. 以下の行を追加して SSH PAM 認証を追加し、ファイルを保存します。

sshd	auth	required	/usr/lib/security/pam_aix
OTHER	auth	required	/usr/lib/security/pam_aix
sshd	account	required	/usr/lib/security/pam_aix
OTHER	account	required	/usr/lib/security/pam_aix
sshd	password	required	/usr/lib/security/pam_aix
OTHER	password	required	/usr/lib/security/pam_aix
sshd	session	required	/usr/lib/security/pam_aix
OTHER	session	required	/usr/lib/security/pam_aix

11. コンピュータを再起動します。

AIX は認証に PAM を使用するよう設定されます。これで AIX ネイティブ パッケージをカスタマイズし、UNAB をインストールできるようになりました。

bff ネイティブ パッケージ ファイルのカスタマイズ

ネイティブ パッケージを使用して UNAB をインストールする前に、UNAB パッケージをカスタマイズして、使用許諾契約への同意を示す必要があります。また、パッケージをカスタマイズする際に、カスタムインストール設定を指定することもできます。

パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、UNAB パッケージをカスタマイズしてください。

サポートされた各 AIX オペレーティング システムに対する installp 形式ネイティブ パッケージ (bff ファイル) は、CA ControlMinder Endpoint Components for UNIX DVD の UNAB ディレクトリにあります。

重要: UNAB をインストールする前に、認証に PAM を使用するよう AIX を設定したことを確認します。

bff ネイティブ パッケージ ファイルのカスタマイズ方法

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

ファイル システムの読み取り/書き込み可能な領域で、パッケージ (bff ファイル) を必要に応じてカスタマイズできます。

重要: この領域のディスク容量は、再パッケージングの一時的なファイルを格納できるように、少なくともパッケージの 2 倍のサイズである必要があります。

2. `customize_uxauth_bff` スクリプト ファイルおよび `pre.tar` ファイルをファイル システム上の一時的な保存場所にコピーします。

`pre.tar` ファイルは、圧縮された `tar` ファイルであり、インストール メッセージおよび `UNAB` のエンド ユーザ使用許諾契約が含まれています。

注: `customize_uxauth_bff` スクリプト ファイルおよび `pre.tar` ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. インストール パッケージから `uxpreinstall` ユーティリティを抽出する以下のコマンドを入力します。

```
customize_uxauth_bff -e uxpinstall -f tmp_params [-d pkg_location] pkg_name
```

`UNAB` をインストールする前に、`uxpreinstall` を使用して、システムの適合性を確認してください。

4. 以下のコマンドを入力します。

```
customize_uxauth_bff -a [-d pkg_location] pkg_name
```

このコマンドは使用許諾契約を表示します。

5. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

次の手順でこのキーワードを指定します。

6. 以下のコマンドを入力します。

```
customize_uxauth_bff -w keyword [-d pkg_location] pkg_name
```

このコマンドは、ユーザが使用許諾契約に同意したことを指定します。

7. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_bff -r -l lang [-d pkg_location] pkg_name
```

このコマンドは、インストール パラメータ ファイルの言語を設定します。

8. (オプション) 以下のコマンドを入力します。

```
customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
```

このコマンドはインストール ディレクトリを変更します。

9. 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

```
customize_uxauth_bff -g -f tmp_params [-d pkg_location] pkg_name
```

10. (オプション) [インストール要件に合わせて、インストール パラメータ ファイルを編集します \(P. 371\)](#)。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

11. (オプション) 以下のコマンドを入力して、カスタマイズされたパッケージのインストール パラメータを設定します。

```
customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

customize_uxauth_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ (UNAB)

customize_uxauth_bff コマンドによって、bff ネイティブ パッケージ ファイル用の、<uxauth> ネイティブ パッケージ カスタマイズ スクリプトが実行されます。

このスクリプトは、AIX で使用可能な <uxauth> ネイティブ パッケージのいずれでも機能します。パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

重要: パッケージの抽出場所には、再パッケージの中間ファイルを保存するために、少なくともパッケージの 2 倍のサイズが必要です。

注: ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_bff -h [-l]
customize_uxauth_bff -a [-d pkg_location] pkg_name
customize_uxauth_bff -w keyword [-d pkg_location] pkg_name
customize_uxauth_bff -r [-d pkg_location] [-l lang] pkg_name
customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name
customize_uxauth_bff -e uxpreinstall [-d pkg_location] pkg_filename
customize_uxauth_bff -g [-f tmp_params] [-d pkg_location] pkg_name
```

pkg_name

カスタマイズする UNAB パッケージ (bff ファイル) の名前です。

-a

使用許諾契約を表示します。

-e uxpreinstall

指定すると、インストールパッケージから *uxpreinstall* ユーティリティを抽出します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d *pkg_location*

(オプション) ファイルシステム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで */var/spool/pkg* を指定します。

-f *tmp_params*

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: **-g** オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力 (*stdout*) に出力されます。

--g

インストール パラメータ ファイルを取得し、それを **-f** オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。-l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i *install_loc*

パッケージのインストール ディレクトリを *install_loc/uxauth* に設定します。

-l *lang*

インストール パラメータ ファイルの言語を *lang* に設定します。言語の設定は、**-r** オプションを使用した場合のみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、**-h** オプションと組み合わせて実行します。デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、**-f** オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンドユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [] 内）。使用許諾契約ファイルを検索するには、**-a** オプションを使用します。

UNAB AIX ネイティブ パッケージのインストール

インストールした UNAB を、インストールされたほかのソフトウェアと同様に管理するには、UNAB AIX ネイティブ パッケージをカスタマイズしてインストールします。UNAB AIX のネイティブ パッケージ（**bff** ファイル）を使用すると、AIX に UNAB を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。**CA ControlMinder** エンタープライズ管理 を使用して UNAB エンドポイントを管理する場合は、UNAB をインストールする *前*に、UNAB エンドポイントを **CA ControlMinder** エンタープライズ管理 に登録する必要があります。

UNAB AIX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. [UNAB パッケージをカスタマイズします \(P. 413\)](#)。

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. (オプション) インストールするパッケージのレベル (バージョン) を記録します。

```
installp -l -d pkg_location
```

pkg_location

UNAB パッケージ (uxauth) が格納されているディレクトリを定義します。

pkg_location 内の各パッケージについて、AIX ではパッケージ レベルの一覧が作成されます。

注: AIX ネイティブ パッケージのインストール オプションの詳細については、installp の man ページを参照してください。

4. 以下のコマンドを使用して、UNAB パッケージをインストールします。

```
installp -ac -d pkg_location uxauth[pkg_level]
```

pkg_level

前に記録したパッケージのレベル番号を定義します。

AIX は、*pkg_location* ディレクトリから、UNAB パッケージのインストールを開始します。

これで、UNAB のインストールは完了しましたが、まだ起動されていません。

詳細情報:

[ネイティブ インストールの際に考慮するその他の事項 \(P. 239\)](#)

AIX パッケージのアンインストール

インストールされている **UNAB AIX** パッケージをアンインストールするには、インストール時とは逆の手順で、**UNAB** パッケージをアンインストールする必要があります。

UNAB パッケージをアンインストールするには、メインの **UNAB** パッケージをアンインストールします。

```
installp -u unab_package_name
```

```
unab_package_name
```

UNAB ネイティブ パッケージの名前を定義します。

AIX ワークロード パーティション(WPAR)ネイティブ パッケージのインストール

AIX は、ワークロード パーティション (WPAR) と呼ばれる AIX の単一インスタンス内の仮想化されたオペレーティング システム環境を提供します。ワークロード パーティションは、AIX オペレーティング システムの単一インスタンスのリソースから作成され、それを共有するソフトウェア パーティションです。AIX には、「グローバル環境」と呼ばれるマスタ パーティションと、それと並行して実行されるワークロード パーティションがあります。

UNAB を AIX WPAR にインストールする前に、以下の考慮事項および制限事項を確認します。

- UNAB をインストールできるのは、AIX 7.1 WPAR 以降のみです。
- 共有モード (/opt および /usr ディレクトリがすべてのパーティションによって共有される) での AIX WPAR の使用を選択する場合は、プライベートインストールディレクトリを使用します。例: UNAB を /opt/CA/uxauth ディレクトリではなく、/CA/uxauth/ ディレクトリにインストールするように指定します。
- AIX WPAR ライブ移行はサポートされていません。
- UNAB は AIX 5.2 WPAR にインストールできません。
- AIX グローバル環境上のみで、use_time_sych オプションを有効にします ('yes' に設定)。UNAB のワークロードパーティションインスタンス上で、このオプションを無効にします ('no' に設定)。

共有モードでの UNAB AIX 7.1 WPAR ネイティブ パッケージのインストール

UNAB の AIX WPAR のデフォルト パーティションへのインストールは、デフォルトではないインストール ディレクトリを指定することを除けば、標準インストールに類似しています。共有モードでは、`/opt` および `/usr` ディレクトリはすべてのワークロード パーティションで共有されています。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

以下の手順に従います。

1. グローバル環境に `root` としてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、`root` アカウントに関連した権限が必要です。

2. [UNAB パッケージをカスタマイズします \(P. 413\)](#)。

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

重要: インストール ディレクトリを変更して、プライベート ディレクトリを指定します。以下に例を示します。

```
customize_eac_bff -i /CA/uxauth -d pwd uxauth.12.6.1.*.bff
```

3. 以下のコマンドを実行して、UNAB をインストールします。

```
installp -d 'pwd' -a uxauth
```

AIX は UNAB パッケージのインストールを開始します。

これで、UNAB のインストールは完了しましたが、まだ起動されていません。

4. 以下のコマンドを使用して、UNAB を AIX ワークロード パーティションと同期します。

```
synchwpar <wpar_name>
```

`wpar_name`

AIX ワークロード パーティションの名前を指定します。

注: UNAB をすべてのパーティションにインストールするには、`synchwpar -A` コマンドを使用します。

UNAB は指定された AIX ワークロード パーティションにインストールされます。UNAB をグローバル環境、および各ワークロードパーティションで別々に管理できるようになりました。

分離モードでの UNAB AIX 7.1 WPAR ネイティブ パッケージのインストール

UNAB の AIX ワークロード パーティションへのインストールは、標準インストールに類似しています。分離モードでは、ワークロードパーティションはそれぞれ、`/opt` および `/usr` ディレクトリのローカルコピーを使用します。

以下の手順に従います。

1. グローバル環境に `root` としてログインします。

AIX ネイティブ パッケージを登録し、インストールするには、`root` アカウントに関連した権限が必要です。

2. [UNAB パッケージをカスタマイズします \(P. 413\)](#)。

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のコマンドを実行して、UNAB をインストールします。

```
installp -d 'pwd' -a uxauth
```

AIX は、`pkg_location` ディレクトリから、`uxauth` パッケージのインストールを開始します。

これで、UNAB のインストールは完了しましたが、まだ起動されていません。

4. 分離されている各ワークロードパーティションに、インストールパッケージをコピーします。
5. `root` としての各ワークロードパーティションへのログインおよび UNAB のインストール

UNAB は AIX ワークロードパーティションにインストールされます。

UNAB AIX 7.1 WPAR パッケージのアンインストール

まず UNAB をグローバル環境から削除し、次に各ワークロードパーティションから削除して、AIX 7.1 WPAR パッケージをアンインストールします。

以下の手順に従います。

1. グローバル環境に root としてログインします。
2. 以下のコマンドを使用して、uxauth パッケージを削除します。
`installp -u uxauth`
3. 以下のコマンドを使用して、ワークロードパーティションを同期します。

`synchwpar <wpar_name>`

注: 分離パーティション内の UNAB をアンインストールするには、各パーティションで `uninstall` コマンドを実行して、インストールパッケージを削除します。

CA ControlMinder は、グローバル環境および各ワークロードパーティションから削除されます。

インストール後のタスク

以下のトピックは、UNAB エンドポイントを設定し、UNAB をアクティブにするために実行する必要があるインストール後のタスクについて説明します。

Active Directory での UNIX ホストの登録

Active Directory に定義されたユーザが UNIX コンピュータにログインできるようにするには、UNAB をインストールした各 UNIX コンピュータを Active Directory サーバに登録する必要があります。

注: UNAB インストールパラメータ ファイルを設定して、UNAB のインストール中にインストールプロセスによって UNIX エンドポイントが Active Directory に登録されるよう指定することができます。

Active Directory での UNIX ホストの登録方法

1. UNIX ホストおよび Active Directory サーバの時間が同期されていることを確認します。

2. UNIX コンピュータにスーパーユーザとしてログインします。

注: Active Directory ユーザが UNIX コンピュータにログオンできるようにするには、UNAB をアクティブにする必要があります。

3. Microsoft Services for UNIX (SFU) を使用する場合、uxauth.ini ファイルのマップセクションに属性名を指定します。

uxauth.ini ファイルに属性名を指定しない場合、SFU でのみ定義されているユーザは UNAB ホストにログインすることができません。

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

4. UNAB bin ディレクトリに移動します。デフォルトのディレクトリは、以下の通りです。

`/opt/CA/uxauth/bin`

5. `uxconsole -register` ユーティリティを実行します。

UNAB は UNIX コンピュータを Active Directory に登録し、`uxauthd` デモンを開始します。

注: `uxconsole -register` の詳細については、「リファレンス ガイド」を参照してください。

例: Active Directory での UNIX ホストの登録方法

この例では、UNIX コンピュータを Active Directory に登録する方法を示します。ユーザ名 (`-a administrator`) およびパスワード (`-w admin`) を入力し、Active Directory のホスト名 (`-d Active_Directory_Host`) を定義し、詳細レベル (`-v 3`) を設定し、インストール完了時に UNAB エージェントが実行されないよう指定 (`-n`) します。さらに、Active Directory のコンテナの名前を定義します (`-o OU=COMPUTERS`)。コンテナは、UNIX コンピュータを Active Directory に登録する前に存在する必要があります。

```
./uxconsole -register -a administrator -w admin -d Active_Directory_Host -v 3 -n -o  
OU=COMPUTERS
```


例: UNIX ホストを登録する権限を Active Directory ユーザへ委任する

`uxconsole -register` コマンドを実行するときに、管理者ユーザ名およびパスワードを指定しない場合、UNIX ホストを **Active Directory** に登録するための権限を委任されたユーザのユーザ名およびパスワードを指定できます。以下の例は、UNIX ホストを **Active Directory** に登録するための権限を **Active Directory** ユーザに委任する方法について示しています。

1. **Active Directory** コンピュータで、[スタート] - [プログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] をクリックします。
[Active Directory ユーザーとコンピュータ] ウィンドウが開きます。
2. **Computers** フォルダを右クリックし、[制御の委任] を選択します。
[制御の委任] ウィザードが開きます。
3. [Next] をクリックします。
ウィザードが開始します。
4. 以下の表を使用して、インストール ウィザードを完了し、[完了] をクリックします。

情報	アクション
ユーザおよびグループ	制御を委任するユーザを指定します。 [追加] を選択し、制御を委任するユーザを検索します。
委任するタスク	選択したユーザまたはグループに委任するタスクを定義します。 [委任するカスタム タスクを作成する] を選択します。
Active Directory オブジェクトの種類	委任するタスクのスコープを定義します。 以下の手順を実行します。 ■ [このフォルダ、このフォルダ内の既存のオブジェクト、およびこのフォルダ内の新しいオブジェクトの作成] を選択します。 ■ リストから [コンピュータ オブジェクトの作成] のアクセス許可を選択します。

情報	アクション
アクセス権	ユーザに委任するアクセス権を定義します。 [特定の子オブジェクトの作成または削除]を選択します。

ウィザードが閉じます。Active Directory にコンピュータ オブジェクトを作成する権限が、指定したユーザに委任されました。このユーザには、Active Directory で UNIX ホストを登録するための十分な権限が付与されています。

UNAB の設定

uxauth.ini ファイルでは、起動時と実行時の UNAB のアクションを指定します。uxauth.ini ファイルには、必要に応じて変更できるデフォルトの値のセットが含まれています。

UNAB の設定方法

1. UNAB を実行している UNIX ホストにログインします。
2. デフォルトでは、以下のディレクトリに格納されている uxauth.ini ファイルを開きます。

/opt/CA/uxauth

3. 設定を確認し、必要に応じて変更します。

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

注: CA ControlMinder エンタープライズ管理 を使用して、uxauth.ini ファイルを設定できます。

レポート作成のための UNAB の設定

UNAB のインストールおよび設定すると、データを配布サーバに送信して処理するように設定することができます。これを行うには、レポート エージェントを有効にして設定します。UNAB のインストール時にレポート エージェントを設定しなかった場合は、レポート エージェントを有効化する際に設定してください。

注: 下の手順は、レポートを送信できるように既存の UNAB エンドポイントを設定する方法を示しています。CA ControlMinder と UNAB を同じコンピュータ上にインストールしている場合、レポート エージェントの設定は 1 回で済みます。

レポート作成用に UNAB を設定するには、`ACSharedDir/lbin/report_agent.sh` を実行します。

```
report_agent config {-server hostname [-proto {ssl|tcp}] [-port port_number] [-rqueue queue_name] -schedule <time@day> [,day2][...] > [-audit] | [-silent] }
```

環境設定オプションのいずれかを省略すると、スクリプトによってそのオプションのデフォルト値が設定されます。

注: `report_agent.sh` スクリプトおよび レポート エージェント設定の詳細については、「リファレンス ガイド」を参照してください。

UNAB の開始

ユーザが Active Directory から UNIX コンピュータへログインするには、UNAB を起動する必要があります。

UNAB の開始方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB lbin ディレクトリを見つけます。
3. 以下のコマンドを入力します。

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

UNAB デーモンが開始されます。

UNAB のアクティブ化

Active Directory で UNIX ホストを登録した後、UNAB をアクティブにする必要があります。アクティブ化は、UNAB の実装プロセスの最終ステップです。一旦 UNAB がアクティブ化されれば、UNAB は Active Directory のパスワードに基づいてユーザを認証します。

UNAB をアクティブにする方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB bin ディレクトリに移動します。デフォルトのディレクトリは、以下の通りです。

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

3. 以下のコマンドを実行します。

```
./uxconsole -activate  
-activate
```

Active Directory ユーザのログインがアクティブ化されることを指定します。

UNAB がアクティブにされます。

注: UNAB をアクティブにすると、Active Directory アカウントを持っているローカルユーザが、UNIX ホストに継続してログインできるようになります。

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

例: アクティブ化後の UNAB へのログイン

以下の例は、UNAB の部分モードでのインストールおよび登録後、Active Directory アカウントを使用して、UNIX コンピュータにログインする方法を示しています。

1. ターミナル ウィンドウを開きます。
2. UNIX ホストへの接続

```
telnet computer.com
```

ユーザは UNIX コンピュータに接続され、UNIX シェルが開きます。
3. Active Directory アカウントのユーザ名およびパスワードを入力します。
ログインが成功した場合、前回の路銀の詳細を通知するメッセージが表示されます。

完全統合モードでの実装方法

完全統合モードの場合、UNAB エンドポイントはユーザの認証および認可を Active Directory サーバに任せます。

完全統合モードでの UNAB の実装

1. UNAB を実装します。
これにより、UNIX エンドポイントに UNAB がインストールされアクティブになります。
2. Active Directory ユーザの UNIX 属性を管理するためのツールをインストールします。

Active Directory ユーザおよびコンピュータ管理では、UNIX 属性にアクセスできないので、これらの属性を表示および変更するために追加のツールをインストールする必要があります。たとえば、CA ControlMinder UNIX Attributes プラグイン、Microsoft Identity Management for UNIX、ADSI Edit、LDAP クライアントなどを使用して、UNIX 属性を表示および変更できます。

3. UNAB エンドポイント上のユーザおよびグループの属性を **Active Directory** に移行します。以下のいずれかの操作を実行します。
 - UNAB 移行ツールを使用して、UNAB エンドポイントのユーザおよびグループのプロパティを **Active Directory** にコピーします。
 - 手順 2 でインストールしたツールを使用して、UNAB エンドポイントのユーザおよびグループの属性を **Active Directory** に手動で設定します。

これにより、**Active Directory** を使用して、エンドポイントへのアクセスを制御できるようになります。UNAB は完全統合モードで実装されました。

4. (オプション) **Active Directory** 上で UNAB ユーザおよびグループの権限を管理する許可を **UNIX** 管理者に委任します。
5. 手順 2 でインストールしたツールを使用して、必要に応じて **Active Directory** の **UNIX** 属性を更新します。

たとえば、管理者はこのツールを使用してユーザのデフォルトのログイン シェルを更新します。

UNAB と Active Directory との統合

完全統合モードの場合、以下の **UNIX** ユーザおよびグループの属性が **Active Directory** に格納されます。

- UID
- GID
- ホーム ディレクトリ
- ログイン シェル
- GECOS

UNAB は、これらの属性を格納するために **Windows 2003 R2** スキーマを使用します。通常、UNAB はこれらの属性を読み取りますが、属性に書き込むことはしません。UNAB では、`uxconsole -migrate` ユーティリティを使用して **UNIX** ユーザおよびグループを **Active Directory** に移行する場合のみ、**Active Directory** への書き込みを行います。

UNAB は、**Active Directory** スキーマを拡張することはありません。

CA ControlMinder UNIX Attributes プラグインのインストール

CA ControlMinder UNIX Attributes プラグインを使用すると、Active Directory 上で UNAB ユーザの UNIX 属性を管理することができます。このプラグインによって NIS サーバがインストールされることはありません。UNAB ユーザの UNIX 属性を管理するために使用できるツールには、ほかに Microsoft Identity Management for UNIX、ADSI Edit、または単純な LDAP クライアントがあります。

デフォルトでは、プラグインは、Active Directory データの読み書きに Active Directory 2003 R2 スキーマを使用します。R2 スキーマが存在しない場合、別の属性を使用するようにプラグインを設定できます。

注: インストール中に、Active Directory の管理者パスワードを指定します。Active Directory スキーマが変更されるので、このパスワードが必要です。CA ControlMinder は Active Directory の管理者パスワードを保存しません。

プラグインは、ユーザが Active Directory の管理に使用するサーバにインストールしますが、Active Directory ドメイン コントローラ (DC) にインストールする必要はありません。

次の手順に従ってください:

1. サーバ上の光ディスクドライブに CA ControlMinder Endpoint Components for UNIX の DVD を挿入します。
2. 以下のディレクトリに移動します。

ADTools¥UnixADTabExt

3. 使用しているオペレーティング システムに適合するディレクトリを選択します。
4. **setup.exe** ファイルをダブルクリックします。
CA ControlMinder UNIX 属性プラグイン インストール ウィザードが起動します。
5. CA ControlMinder UNIX 属性プラグインをインストールするには、以下の手順に従います。
Active Directory ホスト上に CA ControlMinder UNIX 属性プラグインがインストールされます。
6. (オプション) プラグインが使用する Active Directory 属性を設定します。
Active Directory スキーマが Windows 2003 R2 でない場合は、この手順を完了します。

プラグインが使用する属性の設定

CA ControlMinder UNIX Attributes プラグインでは、Active Directory データの読み書きに Active Directory 2003 R2 スキーマを使用します。お使いの Active Directory サーバで 2003 R2 スキーマを使用していない場合、別のスキーマの属性を使用するようプラグインを設定できます。

別のスキーマの属性を使用するようプラグインを設定した場合、UNAB エンドポイントでも同じ属性を使用するよう設定する必要があります。UNAB エンドポイントが使用する属性を設定するには、**uxauth.ini** ファイルの **map** セクションを使用します。

プラグインが使用する属性を設定するには、以下のレジストリ エントリの値を変更します。このエントリは、以下のレジストリ キーに存在します。

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth

エントリ	Default Value	プラグインのフィールド名
user_uid_attr_name	uidNumber	UID
user_loginshell_attr_name	loginShell	Login Shell
user_homedir_attr_name	unixHomeDirectory	ホーム ディレクトリ
user_gecos_attr_name	gecos	GECOS

エントリ	Default Value	プラグインのフィールド名
user_gid_attr_name	gidNumber	Primary Group Name/GID
group_gid_attr_name	gidNumber	GID (Group ID)

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

CA ControlMinder UNIX Attributes プラグインのアンインストール

CA ControlMinder UNIX Attributes プラグインを使用すると、Active Directory のユーザおよびグループの UNIX 属性を管理することができます。

CA ControlMinder UNIX Attributes プラグインをアンインストールする方法

1. [スタート] - [コントロール パネル] - [プログラムの追加と削除] を選択します。

[プログラムの追加と削除] ダイアログ ボックスが表示されます。

注: Windows Server 2008 で、[スタート] - [コントロール パネル] - [プログラムと機能] をクリックします。

2. プログラム リストをスクロールし、[CA Access Control UNIX 属性スナップイン] を選択します。
3. 使用するオペレーティング システムに応じて、[変更¥削除] または [アンインストール] をクリックします。

アンインストール プロセスによって、CA ControlMinder UNIX 属性 プラグインがシステムから削除されます。

4. 以下のレジストリ キーを削除します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥uxauth

5. コンピュータから ACUnixAttributesShellExt.dll ファイルを削除します。

CA ControlMinder UNIX Attributes プラグインがアンインストールされます。

例: ACUnixAttributesShellExt.dll のアンインストール

以下の例は、ディレクトリ C:¥WINDOWS¥system32 から CA ControlMinder UNIX Attributes プラグインをアンインストールします。

```
regsvr32 /u %WINDIR%¥system32¥ACUnixAttributesShellExt.dll
```

ユーザとグループの移行

ユーザを UNIX ホストから Active Directory に移行すると、管理タスクを単一の管理アプリケーションに統合できるため、UNIX ホスト上でのユーザおよびグループの管理が容易になります。UNIX ユーザを Active Directory に移行すると、UNIX ホストへのアクセスを制御するだけですみ、各 UNIX ホスト上でパスワードや shadow ファイルを管理する必要はなくなります。

ユーザとグループを UNIX ホストから Active Directory へ（完全統合モードで）移行すると、Active Directory がユーザの認証と権限付与を実行します。

詳細情報:

[移行のしくみ](#) (P. 435)

[Active Directory への UNIX ユーザおよびグループの移行](#) (P. 436)

移行のしくみ

UNIX ホスト上で移行プロセスを開始すると、UNAB は以下のタスクを実行します。

1. ローカル ユーザおよび NIS/NIS+ ユーザのリストを取得します。

Active Directory で、リスト上の各ユーザ名を検証して、各ユーザに対して以下のいずれかを行います。

- ユーザが Active Directory に存在し、ユーザの UNIX 属性が UNIX ホストに表示される属性と同じ場合、ユーザ アカウントは移行されます。
- ユーザが Active Directory に存在し、ユーザの UNIX 属性のいくつかが不足している場合、UNAB はユーザを移行せず、不足しているプロパティをログに記録します。
- ユーザが Active Directory に存在し、ユーザが UNIX 属性を持っていない場合、UNAB はユーザを移行し、不足している属性を追加します。
- ユーザが Active Directory 内に存在しない場合、UNAB では Active Directory 内にユーザ アカウントは作成されません。

2. ローカル グループおよび NIS/NIS+ グループのリストを取得します。

Active Directory で、グループ名、および各グループが以下のいずれかを行っているかどうかを検証します。

- グループが Active Directory に存在し、そのグループの UNIX 属性が UNIX ホストの属性と同じ場合、そのグループは移行されます。
- グループが Active Directory に存在し、そのグループの ID が UNIX ホスト上の ID と異なる場合、UNAB では、そのメンバを含むグループは Active Directory に移行されません。
- グループが Active Directory に存在し、そのグループ ID が同一であっても、一部の UNIX 属性が不足している場合、UNAB では、そのグループが Active Directory に移行され、不足している属性が補完されます。
- グループが Active Directory 内に存在しない場合、UNAB では、グループが作成され、それらのグループが Active Directory に移行されます。

注: Active Directory に同じ名前のユーザまたはグループが存在する場合、ユーザまたはグループを移行することはできません。たとえば、g1 という名前のグループを移行しようとしている場合、Active Directory に g1 という名前のユーザが存在すると、UNAB はそのグループを移行することはできません。

注: root ユーザを Active Directory に移行するように選択すると、その root アカウントはログイン時にローカルに認証されて、Active Directory に置かれます。その結果、認証プロセスに時間がかかる場合があります。

Active Directory への UNIX ユーザおよびグループの移行

1 つの場所からのホストへのアクセスを管理するために、ローカル UNIX ホストから Active Directory へユーザを移行します。

UNIX ユーザおよびグループの Active Directory への 移行

1. root ユーザとして UNIX コンピュータにログインします。
2. UNAB インストール bin ディレクトリに移動します。このディレクトリのデフォルトのパスは、以下になります。

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

3. `-uxconsole -migrate` ユーティリティを実行します。

`uxconsole` プログラムは、UNIX ユーザおよびグループを Active Directory へ移行します。操作が正常に完了したことを通知するメッセージが表示されます。

注: 移行における競合の解決の詳細については、「エンタープライズ管理ガイド」を参照してください。`uxconsole` ユーティリティの詳細については、「リファレンスガイド」を参照してください

UNIX ユーザおよびグループの属性に対する管理権限の UNIX 管理者への委任

UNIX 管理者が Active Directory の UNIX ユーザおよびグループの属性を管理できるようにするため、特定の管理権限を UNIX 管理者に委任できます。管理権限を委任することにより、UNIX ユーザおよびグループの属性が Active Directory に移行された後も、UNIX 管理者が引き続きそれらの属性を管理することができるようになります。

管理権限を委任する前に、Active Directory ユーザの UNIX 属性を管理するためのツールがインストールされていることを確認します。管理権限は、個別のユーザにではなくグループに対して委任することをお勧めします。

例: UNIX ユーザおよびグループの属性に対する管理権限を UNIX 管理者に委任する

以下の例は、Active Directory 内の UNIX ユーザおよびグループを管理するための権限を UNIX 管理者のグループに委任する方法を示しています。

1. Active Directory コンピュータで、[スタート] - [プログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] をクリックします。

[Active Directory ユーザーとコンピュータ] ウィンドウが開きます。

2. [組織単位 (OU)] を右クリックし、[プロパティ] を選択します。
組織単位のプロパティ ウィンドウが表示されます。

3. [セキュリティ] タブを選択します。

注: [セキュリティ] タブが表示されない場合は、[表示] タブで [詳細設定] が強調表示されていることを確認します。

4. [詳細] をクリックし、次に [追加] ボタンをクリックします。

[ユーザー、コンピュータ、またはグループの選択] ウィンドウが開きます。

5. 管理権限を委任するグループまたはユーザの名前を入力します。[OK] をクリックします。

[アクセス許可のエントリ] ウィンドウが表示されます。

6. [プロパティ] タブをクリックします。

このウィンドウでグループまたはユーザに許可を割り当てます。

7. [適用先] メニューから [グループ オブジェクト] を選択します。
8. [許可] 列で「gidNumber の読み取り」および「gidNumber の書き込み」のオプションを選択します。
9. [OK] をクリックします。

UNIX グループに対する属性管理権限が UNIX 管理者グループに委任されました。
10. UNIX ユーザに管理権限を委任するには、手順 1 から 6 までを繰り返します。
11. [適用先] メニューから [ユーザ オブジェクト] を選択します。
12. [許可] 列で以下の属性を選択します。
 - Gecos の読み取り
 - Gecos の書き込み
 - gidNumber の読み取り
 - gidNumber の書き込み
 - uid の読み取り
 - uid の書き込み
 - uidNumber の読み取り
 - uidNumber の書き込み
 - unixHomeDirectory の読み取り
 - unixHomeDirectory の書き込み
 - loginShell の読み取り
 - LoginShell の書き込み
13. [OK] をクリックします。

UNIX ユーザに対する属性管理権限が UNIX 管理者グループに委任されました。

Active Directory ユーザ用の UNIX 属性の設定

以下の手順は、CA ControlMinder UNIX Attributes プラグインを使用して Active Directory 上の UNIX ユーザの属性を管理する方法を示しています。ほかのツールを使用して Active Directory 上の UNIX 属性を管理することもできます。たとえば、Microsoft Identity Management for UNIX、ADSI Edit、または単純な LDAP クライアントなどを使用できます。

注: ユーザ アカウント プロパティを定義する際は、このユーザがログオン可能なコンピュータを指定する必要はありません。これらの設定は、UNIX ホストには適用されません。

Active Directory ユーザの UNIX 属性の設定

1. [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] をクリックします。
[Active Directory ユーザーとコンピュータ] ウィンドウが開きます。
2. ユーザ アカウントをダブルクリックします。
ユーザ アカウント プロパティが表示されます。
3. [CA ControlMinder UNIX 属性] タブをクリックします。
[CA ControlMinder UNIX 属性] タブが表示されます。
4. 以下のフィールドに値を入力します。

UNIX 属性の有効化

ユーザ アカウントに対して UNIX 属性が有効かどうかを指定します。ユーザの UNIX 属性を有効にするにはこのチェック ボックスを選択する必要があります。

UID

UNIX コンピュータ上のユーザ ID 番号を定義します。次の使用可能な UID を見つけるには [生成] をクリックします。

ホーム ディレクトリ

UNIX コンピュータ上のユーザのホーム ディレクトリを定義します。

例: /home/user

重要: ユーザ ホーム ディレクトリを設定する前に、ホーム ディレクトリの親ディレクトリが存在することを確認します。

Login Shell

ユーザ アカウントのログイン シェルを定義します。

例： /bin/sh

GECOS

ユーザの GECOS 情報を指定します。

Primary Group Name/GID

ユーザが所属するプライマリ グループ名または GID を定義します。

例： UNIXUsers

重要：ユーザ アカウントを定義する際は、有効なグループ名/GID を割り当てる必要があります。

5. [OK] をクリックします。

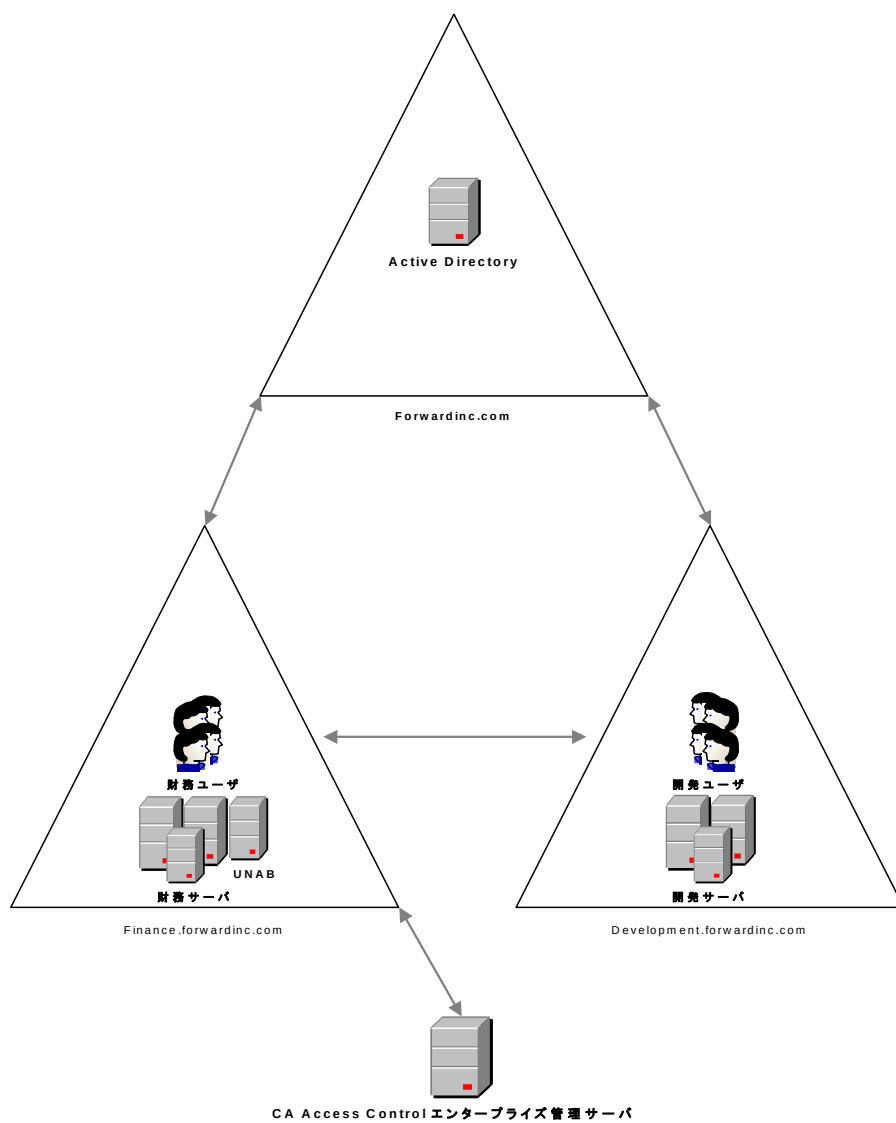
ユーザの UNIX 属性が設定されます。

信頼済みドメイン環境での UNAB の実装

UNAB をインストールする際に、UNAB が登録されるドメインのパラメータを指定します。UNAB をインストール、登録、アクティブ化した後に、ユーザとグループをドメインに移行します。

指定したドメインに他のドメインとの信頼関係がある場合、それらのドメインのユーザは UNAB がメンバになっているドメイン内のコンピュータにアクセスできます。

この図は trusted ドメイン環境における UNAB の実装を示します。



前の図では、UNAB は、他のドメインとの信頼関係が確立されたドメインにインストールされています。この環境では、信頼済みドメインのユーザは、もう一方のドメインのメンバでなくても、そのドメインにアクセスできます。

信頼済みドメイン環境に UNAB をインストールする前に、以下の点を考慮する必要があります。

- UNAB ログイン ポリシーでは、ユーザ名に基づいてドメイン内コンピュータへのアクセスが制御されます。複数のユーザが同一のユーザ名を持っており、複数のドメインで定義されている場合、UNAB はユーザの所属元のドメインを識別できず、ドメインへのアクセスを許可することができません。
- レポートの生成は、UNAB がメンバであるドメインについてのみ可能です。信頼済みドメイン用にレポートを生成することはできません。
- UNAB がメンバであるドメインに定義されているユーザは、Active Directory に移行することができます。

信頼済みドメインから許可されていないユーザがアクセスするのを防ぐため、ユーザ名およびグループ名は一意であるようにすることをお勧めします。

一方向の信頼関係にあるドメイン環境で UNIX ホストを登録する方法

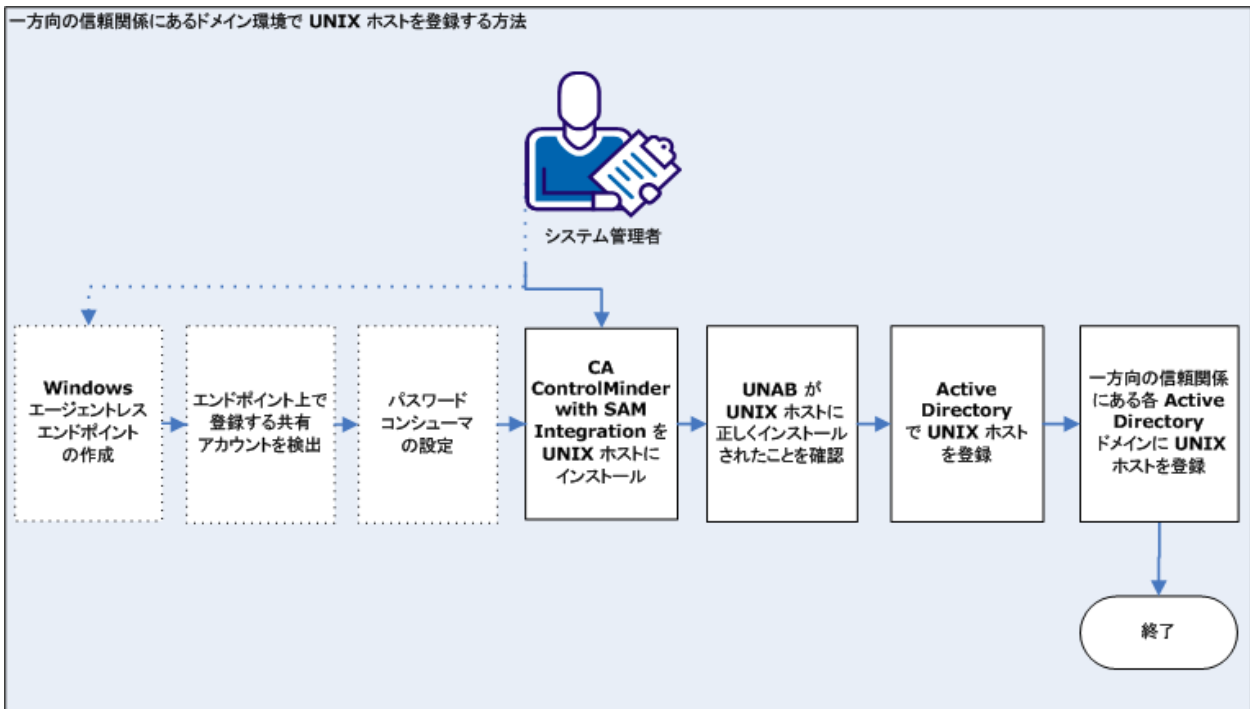
Active Directory で UNIX ホストを登録する場合、ユーザおよびグループ詳細を取得する権限のあるユーザ アカウントを **Active Directory** で使用します。双方向の信頼関係にあるドメイン環境で UNIX ホストを登録する場合、単一ユーザ アカウントを使用して、すべての **Active Directory** ドメインからユーザおよびグループを取得できます。

一方向の信頼関係にあるドメイン環境の場合、UNIX ホストの登録に使用する **Active Directory** アカウントでは他の **Active Directory** ドメインからデータを取得できません。一方向の信頼関係にあるドメイン環境では、一般ユーザ アカウントで各 **Active Directory** ドメインから UNIX ホストを登録します。

さらに、**Active Directory** 共有アカウントで UNIX ホストを登録し、**SAM** を使用してアカウントを管理できます。ユーザ アカウントには、すべての **Active Directory** ドメインからユーザおよびグループの属性を取得するため、十分な権限が必要です。

ドメイン アカウントを使用して UNIX を登録するには、**SAM** 統合を使用します。**SAM** との統合によって、登録するユーザ アカウントを管理できます。たとえば、ドメインセキュリティ ポリシーの適用、アカウントパスワードの自動変更などを行うことができます。

以下の図は、一方向の信頼関係であるドメイン環境で UNIX ホストを登録する方法を示しています。



注: 点線はオプションの手順を示します。

以下の手順に従います。

1. (オプション) UNIX ホストの登録に共有アカウントを使用するには、以下の手順に従います。

- a. [Windows エージェントレス エンドポイントを作成します](#) (P. 447)。

各 UNIX ホストの登録に使用する Active Directory ドメインの接続詳細を指定します。

- b. [エンドポイント上で登録する共有アカウントを検出します](#) (P. 449)。

作成した Windows エージェントレス エンドポイント上で、アカウント検出ウィザードを実行します。

- c. [パスワード コンシューマを定義します](#) (P. 452)。

SDK パスワード コンシューマとして UNAB エンドポイントを指定して、登録するユーザアカウント パスワードをエンドポイントが取得できるようにします。

2. [UNAB がインストールされている各 UNIX ホストに、SAM 統合で CA ControlMinder をインストールします](#) (P. 456)。

SAM 統合で、Shared Accounts Management (SAM) のためにローカル コンピュータを設定します。SAM をエンドポイントにインストールするために INSTALL_PUPM オプションを yes に設定します。SAM の詳細については、「エンタープライズ管理ガイド」を参照してください。

3. UNAB のインストールが正常に完了したことを確認します。以下の手順を実行します。
 - a. accommon.ini ファイルを見つけます。デフォルトでは、ファイルは以下のディレクトリにあります。
`/opt/CA/AccessControlShared`
 - b. 通信セクションで Distribution_Server トークンを見つけます。
 - c. 配信サーバの URL を定義します。以下に例を示します。
`tcp://ds_dr.comp.com:7222`
注: accommon.ini ファイルの詳細については、「リファレンス ガイド」を参照してください。
 - d. sechkey ユーティリティを使用して、通信パスワードを設定します。
 - e. selang コマンドプロンプト ウィンドウを開いて、以下のコマンドを入力します。
`er ACVAR unab value("/opt/CA/uxauth/bin/uxauthd")`
`er ACVAR unab value+("/opt/CA/uxauth/bin/uxconsole")`
4. 以下のいずれかの操作を実行します。
 - 通常アカウントを使用して UNIX ホストを登録するには、以下の手順に従います。
 - a. CA ControlMinder を起動します。
 - b. [各 Active Directory ドメインで UNIX ホストを登録します](#) (P. 460)。
 - c. [UNAB をアクティブにします](#) (P. 463)。
 - d. `uxconsole -register -ows` コマンドを使用して、一方向の信頼関係にあるドメイン環境にある各 Active Directory で UNIX ホストを登録します。
 - e. [UNAB を開始します](#) (P. 464)。

- 共有アカウントを使用して UNIX ホストを登録するには、以下の手順に従います。
 - a. CA ControlMinder を起動します。
 - b. [Active Directory に UNIX ホストを登録します](#) (P. 460)。
 - c. [UNAB をアクティブにします](#) (P. 463)。
 - d. `uxconsole -register -ows` コマンドを使用して、一方向の信頼関係であるドメイン環境にある各 Active Directory で UNIX ホストを登録します。
 - e. [UNAB を開始します](#) (P. 464)。

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

Windows エージェントレス エンドポイントの作成

SAM で Active Directory 上のドメイン ユーザを管理できます。Active Directory アカウントを管理するには、Windows エージェントレス エンドポイントを定義し、以下の情報を提供します。

ユーザ ログイン

エンドポイントを管理する管理ユーザの名前を定義します。SAM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

このフィールドにはユーザ名を指定します。コンピュータ名/ユーザ名形式またはドメイン名/ユーザ名形式は使用しません。

例：Administrator

注：[詳細] オプションを指定すると、SAM は管理タスクの実行に[ユーザ ログイン] アカウントを使用しません。代わりに、SAM は[詳細] オプションで指定されたアカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

注：[詳細] オプションを使用する場合は、パスワードは指定しません。

ホスト

Active Directory DNS ドメイン名を定義します。

例：company.com

注：SAM は、ドメイン名から Active Directory ドメイン コントローラの解決を試行します。SAM によりこの名前が解決されない場合は、Active Directory ドメイン コントローラ (DC) DNS 名または IP アドレスを指定します。

ホストドメイン

ドメイン名 (NETBIOS 名) を指定します。

例：domain1

注：DNS 名 (domain1.ca.com) は使用せず、NETBIOS 名 (domain1) を使用します。

Active Directory

このオプションを選択して **Active Directory** を指定します。

ユーザドメイン

〔ユーザ ログイン〕フィールドまたは〔詳細〕フィールド（〔詳細〕が使用された場合）で指定されたユーザのドメイン名（**NETBIOS** ドメイン名）を指定します。

例：domain1

注：DNS 名（domain1.ca.com）は使用せず、**NETBIOS** 名（domain1）を使用します。

詳細

事前に定義された特権管理アカウントを使用して、エンドポイントに対する管理タスクを実行するかどうかを指定します。たとえば、**SAM** は〔ユーザ ログイン〕フィールドで指定されたアカウントを使用する代わりに、〔詳細〕フィールドで定義されたアカウントを使用して、このエンドポイントを管理します。このオプションは、同じ特権アカウントを使用して複数のエンドポイントを管理する場合に役立ちます。

注：このオプションを指定すると、**SAM** は管理タスクの実行に〔ユーザ ログイン〕アカウントを使用しません。

排他的セッションの無効化

このオプションでは、このエンドポイントに対して排他的セッションチェックを無効にするかどうかを指定します。選択すると、**SAM** はエンドポイントのオープンセッションをチェックしません。

特権アカウントの検出

一定の間隔で特権アカウント検出プロセスを実行して、エンドポイント上に新規特権アカウントがないかどうかスキャンすることをお勧めします。特権アカウントの検出によって、複数の特権アカウントを同時に作成できます。**CA ControlMinder** エンタープライズ管理によって検出されたアカウントがテーブルで示されます。そのため、すでに **SAM** で管理しているアカウントを容易に識別します。

エンドポイントタイプ上で特権アカウントを初めて検出すると、**CA ControlMinder** エンタープライズ管理は、そのエンドポイントタイプ上で特権アカウントを使用するために、エンドポイント特権アクセスロールを自動的に作成します。たとえば、**Windows** エージェントレスエンドポイント上で初めて特権アカウントを検出した場合、**CA ControlMinder** エンタープライズ管理は **Windows** エージェントレス接続エンドポイント特権アクセスロールを自動的に作成します。

以下の手順に従います。

1. **CA ControlMinder** エンタープライズ管理で、[特権アカウント] - [アカウント] - [特権アカウント検出ウィザード] をクリックします。
[特権アカウント検出ウィザード：特権アカウントの選択] ページが表示されます。
2. リストから [エンドポイントタイプ] を選択します。
3. 検索属性を選択し、フィルタ値を入力し、[検索] をクリックします。
フィルタ条件に一致するエンドポイントのリストが表示されます。
4. 管理する特権アカウントを選択します。

以下のテーブル列見出しには説明が必要です。

検出されたアカウント

アカウントが **CA ControlMinder** エンタープライズ管理にすでに認識されているかどうかを示します。既知のアカウントには、**CA ControlMinder** エンタープライズ管理がすでに管理しているアカウント、および、**CA ControlMinder** エンタープライズ管理がエンドポイントを管理するために使用する管理者アカウントなどがあります。

エンドポイント管理者

CA ControlMinder エンタープライズ管理 がエンドポイントを管理するために、このアカウントを使用するかどうかを指定します。

重要: エンドポイント管理者アカウントを選択する際には注意が必要です。CA ControlMinder エンタープライズ管理 は、管理する特権アカウントのパスワードを自動的に変更します。エンドポイント管理者アカウントを選択すると、エンドポイント上の特権アカウントにログインして管理する機能が失われます。

[次へ] をクリックします。

[特権アカウント検出ウィザード: 全般アカウントの詳細] ページが表示されます。

5. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドについて説明します。

接続解除システム

アカウントの場所を接続解除システムにするかどうかを指定します。

このオプションを選択すると、SAM はアカウントを管理しません。代わりに、SAM は、接続解除システムの特権アカウントのパスワード ボールトとしてのみ機能します。パスワードを変更するたびに、管理対象エンドポイント上のアカウント パスワードも手動で変更する必要があります。

パスワード ポリシー

特権またはサービス アカウントに適用するパスワード ポリシーを指定します。

チェックアウト期限

チェックアウト アカウントが失効するまでの期間を分単位で指定します。

専用アカウント

単一ユーザだけがいつでもアカウントを使用することができるかどうかを指定します。専用アカウントは、アカウントの使用を 1 回に 1 ユーザに制限する、特権アカウントの制限事項です。

排他的セッションは、エンドポイント上で現在実行されているオープンセッションがない場合に、単一ユーザのみがアカウントを使用できることを指定します。

チェックアウト時にパスワードを変更

特権アカウントがチェックアウトされるたびに、**CA ControlMinder エンタープライズ管理** でそのパスワードを変更するかどうかを指定します。

注: このオプションはサービス アカウントに適用されません。

チェックイン時にパスワードを変更

ユーザまたはプログラムによって特権アカウントがチェックインされるたび、またはチェックアウト期間の失効時に、**CA ControlMinder エンタープライズ管理** でそのパスワードを変更するかどうかを指定します。

注: アカウントが専用ではない場合、すべてのユーザがアカウントをチェックインしている場合のみ、**CA ControlMinder エンタープライズ管理** は新規特権アカウント パスワードを生成します。

注: このオプションはサービス アカウントに適用されません。

サービス アカウント

検出されたアカウントがサービス アカウントかどうかを指定します。

注: さらに、サービス アカウント検出ウィザードを使用して、サービス アカウントを検出できます。

[完了] をクリックします。

エラーがない場合、**CA ControlMinder エンタープライズ管理** はタスクをサブミットし、選択された特権アカウントを作成します。

パスワード コンシューマの作成

パスワード コンシューマはアプリケーション、Windows サービスおよび Windows スケジュール タスクであり、特権アカウントおよびサービス アカウントを使用して、スクリプトの実行、データベースへの接続、あるいは Windows サービス、スケジュール タスク、RunAs コマンドを管理します。

パスワード コンシューマには 2 つのグループがあります。

- オンデマンドでパスワードを取得するパスワード コンシューマ -- Software Development Kit、データベース、Windows 実行ユーザ
注: オンデマンドでパスワードを取得するパスワード コンシューマを使用するには、SAM 統合機能を有効にした SAM エンドポイント上に CA ControlMinder をインストールする必要があります。
- パスワード変更時にパスワードを取得するパスワード コンシューマ -- Windows スケジュール タスク、Windows サービス

各グループからパスワード コンシューマを作成するには、異なる情報を提供します。デフォルトでは、パスワード コンシューマを作成するには、「システム マネージャ」ロールが必要です。

注: Software Development Kit、データベース、および Windows 実行ユーザタイプのパスワード コンシューマを作成する場合は、このタスクを完了します。サービス アカウント検出ウィザードを使用して、Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを作成することをお勧めします。

以下の手順に従います。

1. CA ControlMinder エンタープライズ管理 で、[特権アカウント] - [パスワード コンシューマ] - [パスワード コンシューマの作成] をクリックします。

[パスワード コンシューマの作成：パスワード コンシューマ検索] 画面ページが表示されます。

2. (オプション) 既存のパスワード コンシューマを選択して、以下のようにして、そのコピーとしてパスワード コンシューマを作成します。

- a. [パスワード コンシューマ タイプのオブジェクトのコピーの作成] を選択します。
- b. 検索属性を選択し、フィルタ値を入力し、[検索] をクリックします。

フィルタ条件に一致するパスワード コンシューマのリストが表示されます。

- c. 新規パスワード コンシューマのベースとして使用するオブジェクトを選択します。

3. [OK] をクリックします。

[パスワード コンシューマの作成] タスク ページが表示されます。パスワード コンシューマを既存のオブジェクトから作成した場合、ダイアログ ボックスのフィールドには、既存オブジェクトの値がすでにロードされています。

4. [全般] タブで以下のフィールドに入力します。

名前

このパスワード コンシューマの参照に使用する名前を定義します。

説明

(オプション) パスワード コンシューマに関して、記録する情報を定義します (書式自由)。

コンシューマ タイプ

パスワード コンシューマのタイプを指定します。

アプリケーション パス

(Software Development Kit、データベース、Windows 実行ユーザ、Windows スケジュール タスク) エンドポイント上のパスワード コンシューマの完全パス名を定義します。

- Software Development Kit パスワード コンシューマについては、パスワード リクエストを実行するアプリケーションのパス名を指定します。
- データベース パスワード コンシューマについては、データベースに接続するアプリケーションのパス名を指定します。
- Windows 実行ユーザ パスワード コンシューマについては、ユーザが実行するアプリケーションのパス名を指定します。
- Windows スケジュール タスク パスワード コンシューマについては、スケジュール タスクのパス名を指定します。

注: パラメータで、ワイルドカード (*) および CA ControlMinder 変数を使用します。たとえば、「<!AC_ROOT_PATH>%bin%acpwd.exe」のようになります。

サービス名

(Windows サービス) Windows サービスのパス名を定義します。
[Windows サービス] プロパティ ページに表示される通りに、パス名を正確に指定します。

有効

パスワード コンシューマの有効化、つまり、SAM がこのコンシューマからのリクエストを受け取るか、このコンシューマにパスワードの変更を強制するように指定します。

[Status]

(Windows スケジュール タスクまたは Windows サービス) 前回のパスワード変更が成功したか失敗したかを示します。

最終同期日

(Windows スケジュール タスクまたは Windows サービス) 前回の成功したパスワード同期を表示します。

再起動

(Windows サービス) パスワード変更後に、Windows サービスを再起動するかどうかを指定します。

5. [特権アカウント] タブをクリックして、パスワード コンシューマに関連付けられている特権アカウントを指定します。

Software Development Kit、データベースまたは Windows 実行ユーザ パスワード コンシューマを作成する場合、パスワード コンシューマは指定する特権アカウントのパスワードを取得できます。

Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを作成する場合、これらの特権アカウントのパスワード変更時に、SAM はパスワード コンシューマのパスワード変更を強要します。

6. パスワード コンシューマを使用できるエンティティを指定します。以下のいずれかの操作を実行します。

- Software Development Kit、データベースまたは Windows 実行ユーザ パスワード コンシューマを作成するには、以下の手順に従います。

- a. [ホスト] タブをクリックし、[すべてのホスト] を選択して、すべてのホストまたはホスト グループに特権アカウント パスワードへのアクセスを許可します。

注: [名前] フィールドにホストまたはホスト グループ名を入力するか、「...」をクリックして CA ControlMinder ホストまたはホスト グループ (HNODE または GHNODE オブジェクト) を検索します。

- b. [ユーザ] タブをクリックして特権アカウント パスワードをリクエストできるユーザまたはユーザ グループを指定するか、[すべてのユーザ] を選択して各ユーザが特権アカウント パスワードを要求することを許可します。

ユーザまたはグループの名前をエンドポイントに表示されているように指定します。たとえば、「DOMAIN¥user1」のように指定します。CA ControlMinder エンタープライズ管理 ユーザまたはグループは指定しません。

- Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを作成するには、[エンドポイント] タブをクリックし、パスワード コンシューマを作成するエンドポイントを指定します。

7. [サブミット] をクリックします。

CA ControlMinder エンタープライズ管理 によってパスワード コンシューマが作成されます。

CA ControlMinder RPM パッケージのインストール

インストールした CA ControlMinder を、インストールされた他のソフトウェアと同様に管理するには、CA ControlMinder RPM パッケージをカスタマイズしてインストールします。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

注: 実際に使用するコマンドは、アップグレードなのか初回インストールなのか、またはデフォルトのディレクトリへのインストールなのかなど、さまざまな要因によって異なります。 コマンドの例は、このトピックに記述されています。

以下の手順に従います。

1. rpm コマンドを使用して、ca-lic パッケージをインストールします。

ライセンス プログラムがインストールされます。

2. [CAeAC パッケージのカスタマイズ](#) (P. 245)

使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

注: CA ControlMinder をアップグレードしている場合は、使用許諾契約への同意を指定するためにパッケージをカスタマイズする必要はありません。

3. rpm コマンドを使用して、CAeAC パッケージをインストールします。

CA ControlMinder がインストールされます。

注: UNAB パッケージでは、CAWIN 共有コンポーネントもインストールされます。

重要: 既存の CA ControlMinder パッケージをアップグレードする場合は、SEOS syscall をアンロードしてから、新しいパッケージのインストールを試みます。 そうしない場合は、インストールに失敗します。

CA ControlMinder RPM パッケージのカスタマイズ

ネイティブ パッケージを使用して CA ControlMinder をインストールする前に、CA ControlMinder パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。パラメータ ファイルを変更しなくても済むように、カスタマイズスクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。代わりに、以下の手順に記載されているスクリプトを使用して、CA ControlMinder パッケージをカスタマイズしてください。

サポートされた各 Linux オペレーティング システムに対する RPM パッケージは、CA ControlMinder Endpoint Components for UNIX DVD の NativePackages/RPMPackages ディレクトリにあります。

次の手順に従ってください:

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所にコピーします。

OS は、オペレーティング システム上の適切なサブディレクトリ名です。

ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

2. customize_eac_rpm スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA ControlMinder のエンド ユーザ使用許諾契約が含まれています。

注: customize_eac_rpm スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

```
customize_eac_rpm -a [-d pkg_location] pkg_filename
```

4. 使用許諾契約の最後に表示される、角かっこで囲まれているキーワードをメモします。

次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA ControlMinder パッケージをカスタマイズします。

```
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
```

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

6. (オプション) インストールパラメータ ファイルの言語を設定します。

```
customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename
```

7. (オプション) eTrust Access Control r8 SP1 パッケージからアップグレードします。

```
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
```

8. (オプション) デフォルトの暗号化ファイルを変更します。

```
customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename
```

9. (オプション) インストールパラメータ ファイルを取得します。

```
customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename
```

10. (オプション) インストール要件に合わせて、インストールパラメータ ファイルを編集します。

このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。たとえば、POSTEXIT 設定 (前の # 文字を削除します) をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション) カスタマイズしたパッケージのインストールパラメータを設定します。

```
customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
```

これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA ControlMinder をインストールできるようになりました。

注: 実際に使用するコマンドは、アップグレードなのか初回インストールなのか、またはデフォルトのディレクトリへのインストールなのかなど、さまざまな要因によって異なります。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。以下の例では、CA ControlMinder Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント) にある x86 CA ControlMinder RPM パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、CA ControlMinder をインストールできるようになりました。

詳細情報:

[customize_eac_rpm コマンド - RPM パッケージのカスタマイズ \(P. 251\)](#)

CA ControlMinder の起動

X Window 環境で作業している場合は、CA ControlMinder を起動し、それがシステムに適切にインストールされていることを確認します。重要なシステム保護を開始するには、以下の手順に従ってください。

1. root (スーパーユーザ) 権限でログインし、2 つのウィンドウを開きます。
2. いずれかのウィンドウで以下のコマンドを入力します。

```
seload
```

seload コマンドで 3 つのデーモン（エンジン、エージェント、および Watchdog）が起動されるまで待機します。

3. 3つのデーモンを起動した後、もう一方のウィンドウに移動して以下のコマンドを入力します。

```
secons -t+ -tv
```

CA ControlMinder によって、オペレーティング システムのイベントを報告するメッセージがファイルに記録されます。**secons -tv** コマンドを入力すると、メッセージが画面上にも表示されます。

4. **seload** コマンドを指定した最初のウィンドウで、以下のコマンドを入力します。

```
who
```

CA ControlMinder のトレース メッセージが書き込まれる 2 番目のウィンドウに注意して、CA ControlMinder が **who** コマンドの実行をインターセプトし、そのことについて報告するかどうかを確認します。**who** コマンドのインターセプトが報告された場合、CA ControlMinder はシステムに適切にインストールされています。

5. 必要な場合は、さらにコマンドを入力して CA ControlMinder の反応を確認します。

データベースには、アクセスの試行を禁止するためのルールがまだ準備されていません。この場合でも、CA ControlMinder はシステムを監視しているため、CA ControlMinder がインストールされ実行されているシステムの動作を確認し、CA ControlMinder がインターセプトするイベントを確認することができます。

6. 以下のコマンドを入力して、**seosd** デーモンを停止します。

```
secons -s
```

以下のメッセージが画面に表示されます。

CA ControlMinder は現在停止中です。

Active Directory での UNIX ホストの登録

Active Directory に定義されたユーザが UNIX コンピュータにログインできるようにするには、UNAB をインストールした各 UNIX コンピュータを Active Directory サーバに登録する必要があります。

注: UNAB インストールパラメータ ファイルを設定して、UNAB のインストール中にインストールプロセスによって UNIX エンドポイントが Active Directory に登録されるよう指定することができます。

以下の手順に従います。

1. UNIX ホストおよび Active Directory サーバの時間が同期されていることを確認します。

2. UNIX コンピュータにスーパーユーザとしてログインします。

注: Active Directory ユーザが UNIX コンピュータにログオンできるようにするには、UNAB をアクティブにする必要があります。

3. Microsoft Services for UNIX (SFU) を使用する場合、uxauth.ini ファイルのマップセクションに属性名を指定します。

uxauth.ini ファイルに属性名を指定しない場合、SFU でのみ定義されているユーザは UNAB ホストにログインすることができません。

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

4. UNAB bin ディレクトリに移動します。デフォルトのディレクトリは、以下の通りです。

`/opt/CA/uxauth/bin`

5. `uxconsole -register` ユーティリティを実行します。

UNAB は UNIX コンピュータを Active Directory に登録し、`uxauthd` デモンを開始します。

注: `uxconsole -register` の詳細については、「リファレンス ガイド」を参照してください。

例: Active Directory での UNIX ホストの登録方法

この例では、UNIX コンピュータを Active Directory に登録する方法を示します。ユーザ名 (`-a administrator`) およびパスワード (`-w admin`) を入力し、Active Directory のホスト名 (`-d Active_Directory_Host`) を定義し、詳細レベル (`-v 3`) を設定し、インストール完了時に UNAB エージェントが実行されないよう指定 (`-n`) します。さらに、Active Directory のコンテナの名前を定義します (`-o OU=COMPUTERS`)。コンテナは、UNIX コンピュータを Active Directory に登録する前に存在する必要があります。

```
./uxconsole -register -a administrator -w admin -d Active_Directory_Host -v 3 -n -o OU=COMPUTERS
```

例: UNIX ホストを登録する権限を Active Directory ユーザへ委任する

`uxconsole -register` コマンドを実行するときに、管理者ユーザ名およびパスワードを指定しない場合、UNIX ホストを Active Directory に登録するための権限を委任されたユーザのユーザ名およびパスワードを指定できます。以下の例は、UNIX ホストを Active Directory に登録するための権限を Active Directory ユーザに委任する方法について示しています。

1. Active Directory コンピュータで、[スタート] - [プログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] をクリックします。
[Active Directory ユーザーとコンピュータ] ウィンドウが開きます。
2. Computers フォルダを右クリックし、[制御の委任] を選択します。
[制御の委任] ウィザードが開きます。
3. [次へ] をクリックします。
ウィザードが開始します。
4. 以下の表を使用して、インストール ウィザードを完了し、[完了] をクリックします。

情報	アクション
ユーザおよびグループ	制御を委任するユーザを指定します。 [追加] を選択し、制御を委任するユーザを検索します。
委任するタスク	選択したユーザまたはグループに委任するタスクを定義します。 [委任するカスタム タスクを作成する] を選択します。
Active Directory オブジェクトの種類	委任するタスクのスコープを定義します。 以下の手順を実行します。 ■ [このフォルダ、このフォルダ内の既存のオブジェクト、およびこのフォルダ内の新しいオブジェクトの作成] を選択します。 ■ リストから [コンピュータ オブジェクトの作成] のアクセス許可を選択します。

情報	アクション
権限	ユーザに委任するアクセス権を定義します。 [特定の子オブジェクトの作成または削除]を選択します。

ウィザードが閉じます。Active Directory にコンピュータ オブジェクトを作成する権限が、指定したユーザに委任されました。このユーザには、Active Directory で UNIX ホストを登録するための十分な権限が付与されています。

UNAB のアクティブ化

Active Directory で UNIX ホストを登録した後、UNAB をアクティブにする必要があります。アクティブ化は、UNAB の実装プロセスの最終ステップです。一旦 UNAB がアクティブ化されれば、UNAB は Active Directory のパスワードに基づいてユーザを認証します。

以下の手順に従います。

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB bin ディレクトリに移動します。デフォルトのディレクトリは、以下の通りです。

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

3. 以下のコマンドを実行します。

```
./uxconsole -activate
-activate
```

Active Directory ユーザのログインがアクティブ化されることを指定します。

UNAB がアクティブにされます。

注: UNAB をアクティブにすると、Active Directory アカウントを持っているローカルユーザが、UNIX ホストに継続してログインできるようになります。

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

例: アクティブ化後の UNAB へのログイン

以下の例は、UNAB の部分モードでのインストールおよび登録後、Active Directory アカウントを使用して、UNIX コンピュータにログインする方法を示しています。

1. ターミナル ウィンドウを開きます。
2. UNIX ホストへの接続

```
telnet computer.com
```

ユーザは UNIX コンピュータに接続され、UNIX シェルが開きます。
3. Active Directory アカウントのユーザ名およびパスワードを入力します。
ログインが成功した場合、前回の路銀の詳細を通知するメッセージが表示されます。

UNAB の開始

ユーザが Active Directory から UNIX コンピュータへログインするには、UNAB を起動する必要があります。

以下の手順に従います。

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB lbin ディレクトリを見つけます。
3. 以下のコマンドを入力します。

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

UNAB デーモンが開始されます。

第 11 章: エンドポイント管理のインストール

このセクションには、以下のトピックが含まれています。

[エンドポイント管理サーバの準備方法 \(P. 465\)](#)

[Windows での CA ControlMinder エンドポイント管理 のインストール \(P. 466\)](#)

[Solaris または Linux 上での CA ControlMinder エンドポイント管理 のインストール \(P. 467\)](#)

[Windows での CA ControlMinder エンドポイント管理 のアンインストール \(P. 468\)](#)

[Solaris または Linux 上での CA ControlMinder エンドポイント管理 のアンインストール \(P. 470\)](#)

[CA ControlMinder エンドポイント管理 の起動 \(P. 471\)](#)

[CA ControlMinder エンドポイント管理 を開く \(P. 472\)](#)

エンドポイント管理サーバの準備方法

CA ControlMinder エンドポイント管理 をインストールする前に、サーバを準備する必要があります。

重要: 同じコンピュータに CA ControlMinder エンタープライズ管理 をインストールする場合は、以下の手順を実行する必要はありません。インストールプログラムは、CA ControlMinder エンタープライズ管理 インストールの一環として CA ControlMinder エンドポイント管理 のインストールを行います。

エンドポイント管理サーバを準備するには、以下の手順を実行します。

1. サポートされている Java Development Kit (JDK) をインストールします。

注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA ControlMinder Third Party Components DVD に格納されています。サポートされている JBoss バージョンの詳細については、「リリースノート」を参照してください。

2. サポートされている JBoss バージョンをインストールします。

JBoss をサービス（UNIX ではデーモン）として実行することをお勧めします。

注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA ControlMinderThird Party Components DVD に格納されています。サポートされている JBoss バージョンの詳細については、「リリースノート」を参照してください。

3. CA ControlMinder をインストールします。

注: CA ControlMinder のエンドポイントのインストールに関する手順に従ってください。

4. （Windows のみ）コンピュータを再起動します。

5. CA ControlMinder サービスを停止します（secons -s）。

これで、サーバの準備が整いましたので、CA ControlMinder エンドポイント管理 をインストールできます。

Windows での CA ControlMinder エンドポイント管理 のインストール

Windows で有効

グラフィカル インストールでは、ウィザードを使用して Windows コンピュータへの CA ControlMinder エンドポイント管理 のインストールをサポートおよびガイドします。

Windows での CA ControlMinder エンドポイント管理 のインストール方法

1. [サーバが適切に準備されていること](#) (P. 465)を確認します。
2. 光ディスク ドライブに CA ControlMinder Server Components for Windows DVD を挿入します。
3. CA ControlMinder Product Explorer (ProductExplorerrx86.EXE) を開きます。
CA ControlMinder の Product Explorer が表示されます。
4. Components フォルダを展開し、CA ControlMinder エンドポイント管理を選択し、[インストール] をクリックします。
InstallAnywhere ウィザードがロードを開始します。

5. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

JBoss フォルダ

JBoss アプリケーション サーバがインストールされる場所を定義します。

用意されている JBoss バージョンを使用する場合、これは、JBoss zip ファイルの内容を展開した場所になります。

Web サービス情報

CA ControlMinder Web サービスをインストールする **場所**と、このサービスに使用する **ポート**（デフォルトは **5248**）を指定します。

フル コンピュータ名

アプリケーション サーバ（ローカル コンピュータ）の名前を定義します。この名前は、このアプリケーションにアクセスする際、URL 内で使用する必要があります。

これでインストールは終了です。

Solaris または Linux 上での CA ControlMinder エンドポイント管理 のインストール

Solaris または Linux コンピュータに CA ControlMinder エンドポイント管理をインストールするには、コンソール インストールを使用する必要があります。

Solaris または Linux 上での CA ControlMinder エンドポイント管理 のインストール方法

1. [サーバが適切に準備されていること](#) (P. 465)を確認します。
2. 光ディスク ドライブに CA ControlMinder Server Components for Solaris または Server Component for Linux の DVD を挿入します。
3. 光ディスク ドライブをマウントします。
4. ターミナル ウィンドウを開き、光ディスク ドライブの EndPointMgmt ディレクトリに移動します。

5. 以下のコマンドを入力します。

```
install_EM_r125.bin -i console
```

InstallAnywhere コンソールが表示されます。

6. 必要に応じてプロンプトを完了します。以下のインストール入力には、説明が必要です。

数字によるロケールの選択

インストールしたいロケールを表わす数を定義します。

注: 英語以外のサポート対象言語のいずれかにインストールする場合、ローカライズされたオペレーティングシステムが必要です。

JBoss フォルダ

JBoss アプリケーション サーバがインストールされる場所を定義します。

用意されている JBoss バージョンを使用する場合、これは、JBoss zip ファイルの内容を展開した場所になります。

Web サービス情報

CA ControlMinder Web サービスをインストールする *場所*と、このサービスに使用する *ポート* (デフォルトは **5248**) を指定します。

フル コンピュータ名

アプリケーション サーバ (ローカル コンピュータ) の名前を定義します。この名前は、このアプリケーションにアクセスする際、URL 内で使用する必要があります。

これでインストールは終了です。

Windows での CA ControlMinder エンドポイント管理 のアンインストール

Windows の管理者権限を持つユーザ (すなわち、Windows Administrator または Windows Administrators グループのメンバ) として Windows システムにログオンしていることを確認してください。

Windows での CA ControlMinder エンドポイント管理 のアンインストール方法

1. JBoss が実行されている場合は、停止します。
2. [スタート] - [コントロール パネル] - [プログラムの追加と削除] を選択します。
[プログラムの追加と削除] ダイアログ ボックスが表示されます。
3. プログラム リストをスクロールして **CA ControlMinder エンドポイント管理** を選択します。
4. [変更と削除] をクリックします。
CA ControlMinder エンドポイント管理 のアンインストール ウィザード が表示されます。
5. ウィザードの手順に従って、**CA ControlMinder エンドポイント管理** をアンインストールします。
アンインストールが完了し、コンピュータから **CA ControlMinder エンドポイント管理** が削除されます。
6. ウィザードを終了するには、[完了] をクリックしてください。

Solaris または Linux 上での CA ControlMinder エンドポイント管理 のアンインストール

コンピュータから CA ControlMinder エンドポイント管理 を削除するには、CA ControlMinder エンドポイント管理 が提供するアンインストール プログラムを使用する必要があります。

Solaris または Linux 上での CA ControlMinder エンドポイント管理 のアンインストール方法

1. 以下のいずれかを実行して JBoss を停止します。
 - JBoss ジョブ ウィンドウから、プロセスを中断します (Ctrl+C)。
 - 別のウィンドウで、以下のように入力します。

```
./JBoss_path/bin/shutdown -S
```

2. 以下のコマンドを入力します。

```
"/ACEMInstallDir/Uninstall_EndpointManagement/Uninstall_CA_Access_Control_Endpoint_Management"
```

ACEMInstallDir

CA ControlMinder エンドポイント管理 のインストール ディレクトリを定義します。デフォルトでは、このパスは次のとおりです。

```
/opt/CA/AccessControlServer/EndpointManagement/
```

InstallAnywhere がアンインストール コンソールをロードします。

3. プロンプトに従って、CA ControlMinder エンドポイント管理 をアンインストールします。

アンインストールが完了し、コンピュータから CA ControlMinder エンドポイント管理 が削除されます。

CA ControlMinder エンドポイント管理 の起動

CA ControlMinder エンドポイント管理 をインストールしたら、CA ControlMinder および Web アプリケーション サーバを起動する必要があります。

CA ControlMinder エンドポイント管理 を開始する方法

1. CA ControlMinder サービスを開始します。

CA ControlMinder エンドポイント管理 を使用するには、CA ControlMinder が実行中である必要があります。

2. (Windows のみ) 以下を行います。
 - a. 以下に示す追加サービスを開始します。これらのサービスは、`seosd -start` を実行してもロードされません。
 - CA ControlMinder Web サービス
 - CA ControlMinder メッセージキュー (存在する場合)
 - b. 以下のいずれかの方法で、JBoss アプリケーション サーバを起動します。

- [スタート] - [プログラム] - [CA] - [Access Control] - [タスク エンジンの開始] をクリックします。

注: タスク エンジンは、初回のロード時に多少時間がかかる場合があります。

- [サービス] パネルから JBoss アプリケーション サーバサービスを開始します。

JBoss アプリケーション サーバのロードが完了すると、CA ControlMinder エンドポイント管理 の Web ベース インターフェースにログインできます。

3. (UNIX のみ) 「`./JBoss_HOME/bin/run.sh -b 0.0.0.0`」と入力します。

注: JBoss アプリケーション サーバは、初回のロード時に多少時間がかかる場合があります。

JBoss アプリケーション サーバのロードが完了すると、CA ControlMinder エンドポイント管理 の Web ベース インターフェースにログインできます。

CA ControlMinder エンドポイント管理 を開く

CA ControlMinder エンドポイント管理 をインストールして起動すると、CA ControlMinder エンドポイント管理 用の URL を使用してリモート コンピュータから Web ベースのインターフェースを開くことができます。

CA ControlMinder エンドポイント管理 を開く方法

1. Web ブラウザを開き、使用しているホストに合わせて URL を入力します。

`http://enterprise_host:port/acem`

2. 以下の情報を入力します。

ユーザ名

CA ControlMinder の管理タスクを実行する権限を有するユーザの名前を定義します。

注: ログインに使用するユーザ名にはコンピュータ名が含まれている必要があります (たとえば、Windows の場合は `myComputer¥Administrator`、UNIX の場合は `root`)。

パスワード

CA ControlMinder ユーザのパスワードを定義します。

ホスト名

管理タスクを実行するエンドポイントの名前を定義します。これに相当するのはホストまたは PMDB であり、次の形式で指定します。 `PMDB_name@host_name`

注: CA ControlMinder エンドポイント管理 がインストールされているコンピュータからエンドポイントを管理する (TERMINAL リソースを使用して) 権限が必要になります。

[Log In] をクリックします。

[ダッシュボード] タブ上で CA ControlMinder エンドポイント管理 が開きます。

注: CA ControlMinder エンドポイント管理 をインストールした Windows コンピュータから CA ControlMinder エンドポイント管理 を開くこともできます。それには、[スタート] - [プログラム] - [CA] - [Access Control] - [エンドポイント管理] をクリックします。

例: CA ControlMinder エンドポイント管理 を開く

ネットワーク上の任意のコンピュータから CA ControlMinder エンドポイント管理 を開くには、Web ブラウザに次の URL を入力します。

`http://appserver123:18080/acem`

この URL からは、CA ControlMinder エンドポイント管理 が `appserver123` という名前のホストにインストールされ、デフォルトの JBoss ポート `18080` を使用しているのがわかります。

第 12 章: ハイ アベイラビリティ展開のインストール

このセクションには、以下のトピックが含まれています。

[ハイ アベイラビリティ \(P. 475\)](#)

[ハイ アベイラビリティ環境のコンポーネント \(P. 479\)](#)

[ハイ アベイラビリティ環境の CA ControlMinder エンタープライズ管理を設定する方法 \(P. 482\)](#)

[ハイ アベイラビリティ環境の配布サーバを設定する方法 \(P. 493\)](#)

[ハイ アベイラビリティ環境のエンドポイントの設定 \(P. 497\)](#)

[ハイ アベイラビリティ用の Oracle RAC の設定 \(P. 498\)](#)

[Veritas Cluster Server を使用した Linux 上の CA ControlMinder ハイ アベイラビリティの実装 \(P. 501\)](#)

ハイ アベイラビリティ

CA Access Control エンタープライズ管理は、ハイ アベイラビリティ展開を提供するためにミラーリングされたサイトを使用します。ミラーリングされたサイトは、すべてのリアルタイム情報がミラーリングされた完全な冗長機能で、あらゆる技術的側面においてプライマリ サイトと同一です。データは、プライマリ サイトとミラーリングされたサイトで同時に処理されます。

ミラーリングされたサイトでは、フェールオーバーに関してアクティブ/パッシブ展開が使用されます。アクティブ/パッシブ展開には 2 つ以上のデータ センターが含まれます。1 つがアクティブにリクエストを処理し、もう 1 つはアクティブな方に障害が発生した場合にリクエストを処理するために待機します。選択するクラスタ化ソリューション ソフトウェアは、アクティブ サーバとパッシブ サーバの管理、および障害発生時の両者の切り替えを行います。

アクティブ/パッシブ展開では、アクティブなサーバはプライマリ サーバと呼ばれ、パッシブ サーバはセカンダリ サーバと呼ばれます。

ハイ アベイラビリティ展開の利点および制限

ハイ アベイラビリティ展開によって、1 つ以上のコンポーネントまたはサーバが失敗した場合に、お使いの **CA ControlMinder** エンタープライズ管理コンポーネントが継続してリクエストに対応できるようサポートされます。エンドポイントがプライマリ環境に接続できない場合、プライマリ環境がリストアされるまで、エンドポイントはセカンダリサーバに接続します。

ハイ アベイラビリティ展開には、以下の利点があります。

- プライマリ エンタープライズ管理サーバが失敗した場合に、特権アカウント、**DMS** データソース ファイル、エンドポイント定義が失われるのを防ぎます。
- 運用が中断されることのないようサポートします。

ハイ アベイラビリティ展開を計画する際は、以下の制限を考慮します。

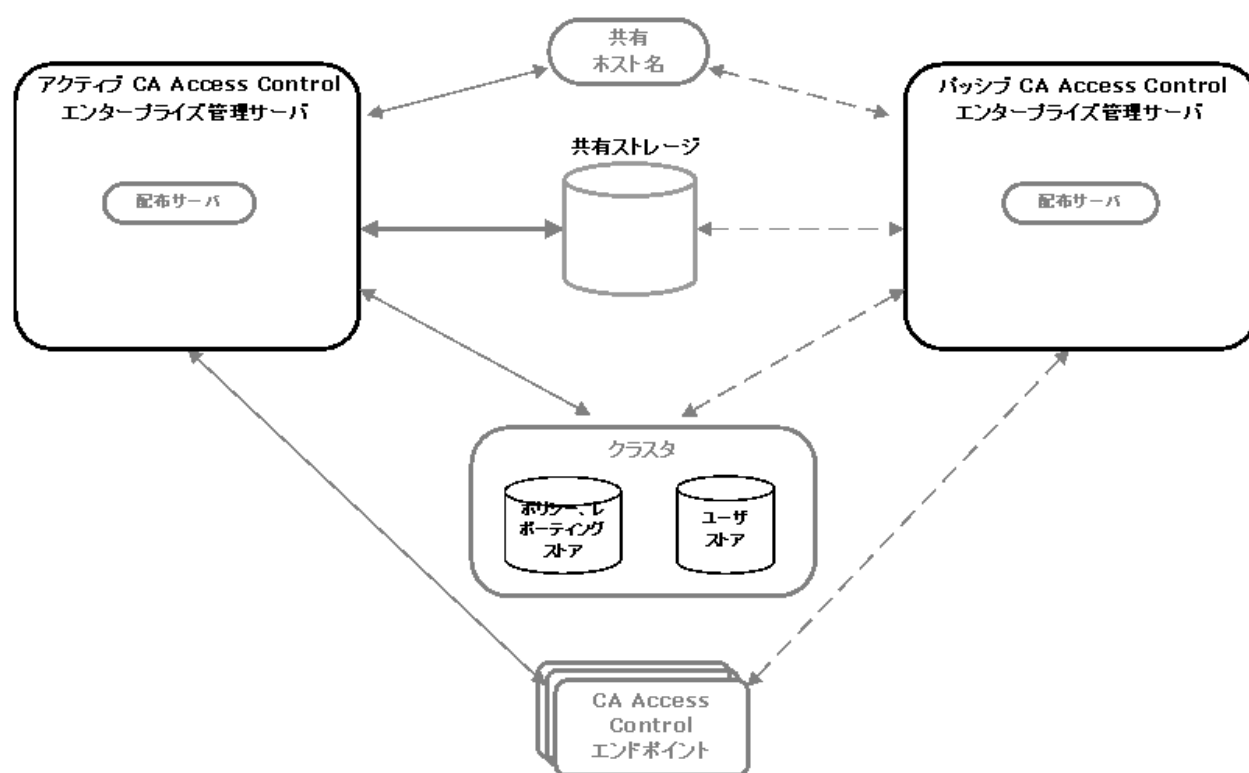
- エンタープライズ管理サーバは、失敗時のセッション継続性をサポートしません。アクティブなサーバが応答しない場合、ユーザセッションは終了します。ログインしていたユーザは再度ログインする必要があります。
- 1 つのアクティブな **DMS** のみがサポートされています。
- プライマリおよびセカンダリのエンタープライズ管理サーバをインストールする場合、同じ通信パスワードが使用されます。
- プライマリサーバおよびセカンダリサーバ上の **Java Connector Sever (JCS)** は、同じ名前を持つ必要があります。

注: クラスタ化ソフトウェア ソリューションによって制御される仮想 **DNS** 名を使用して、障害の発生時にサーバ間でのシームレスな移行が実現するようにすることをお勧めします。

たとえば、ユーザセッションが開いているときにプライマリ エンタープライズ管理サーバに障害が発生した場合、ユーザはセカンダリ エンタープライズ管理サーバの **URL** を入力するか、仮想 **DNS** またはロードバランサを使用して、同じ **URL** で作業を続行できます。

ハイアベイラビリティ展開アーキテクチャ

以下の図は、ハイアベイラビリティ環境における CA ControlMinder エンタープライズ管理 を示しています。



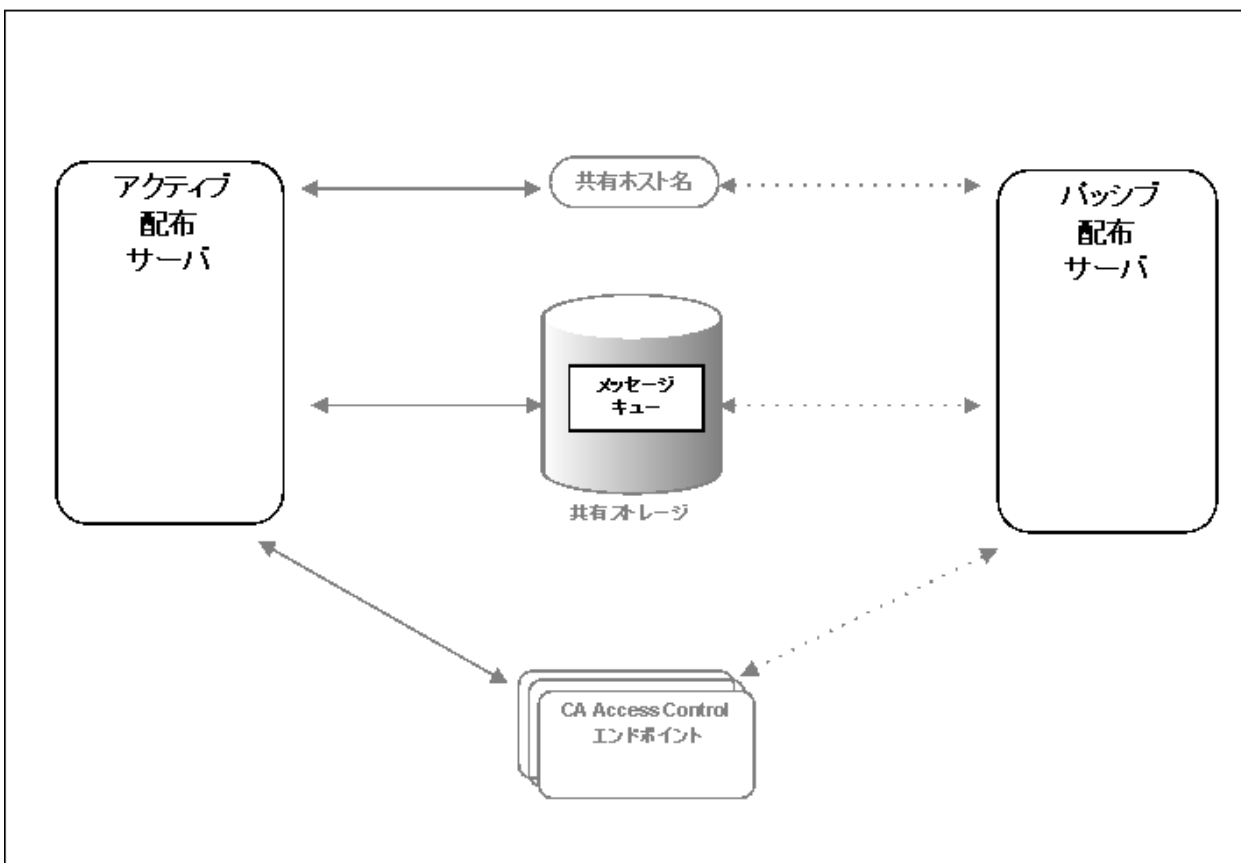
この図に示されるように、ハイアベイラビリティ展開には以下のコンポーネントがあります。

- プライマリ エンタープライズ管理サーバと、少なくとも 1 つのセカンダリ エンタープライズ管理サーバ
- ポリシーおよびレポートストアのクラスタ化されたインストール、およびユーザストア
- プライマリおよびセカンダリ CA ControlMinder エンタープライズ管理サーバからアクセス可能な共有ストレージ
- 共有ホスト名
- プライマリおよびセカンダリの両方のエンタープライズ管理サーバにアクセス可能な CA ControlMinder エンドポイント

ハイ アベイラビリティ環境アーキテクチャの配布サーバ

配布サーバでの障害発生時に、エンドポイントから収集された監査イベントの損失を防止するために、ハイ アベイラビリティを目的に追加の配布サーバを展開できます。

以下の図は、ハイ アベイラビリティ環境に実装されたプライマリおよびセカンダリの配布サーバを表しています。



この図で示されるように、配布サーバのハイ アベイラビリティの実装には以下が必要になります。

- プライマリ配布サーバと、少なくとも 1 つのセカンダリ配布サーバ。
- メッセージキューのデータ ファイルを保持し、プライマリおよびセカンダリの両方の配布サーバからアクセス可能な共有ストレージ。

メッセージキューのデータ ファイルを共有ストレージに配置して、配布サーバの障害発生時に、エンドポイントから届いた監査イベントメッセージが失われていないことを確認します。

- 共有ホスト名
- プライマリおよびセカンダリの両方の配布サーバと連携可能な CA ControlMinder エンドポイント

ハイ アベイラビリティ環境のコンポーネント

ハイ アベイラビリティ環境で CA ControlMinder を展開するには、以下が必要になります。

- プライマリ サーバ
 - エンタープライズ管理サーバ
- セカンダリ サーバ
 - エンタープライズ管理サーバ
- ユーザ リポジトリ
- ポリシーおよびレポーティング データベース
- 共有ストレージ ソリューション
 - クラスタ ソフトウェア
 - 共有ストレージ

共用ストレージ

共用ストレージデバイスを使用して共用ストレージ ソリューションを実装することをお勧めします。共用ストレージは、アクティブ サーバとパッシブ サーバの両方からアクセス可能である必要があります。使用する共用ストレージ ソリューションが以下の条件を満たすことを確認します。

- 書き込み順序 -- バッファでの発生順と同じ順序で共用ストレージにデータ ブロックが書き込まれる必要があります。
- 同期書き込み永続性 -- 同期書き込みコールからのリターン時に、ストレージ ソリューションはすべてのデータが永続ストレージに書き込まれたことを保証します。

以下は、ソフトウェア ベースの共用ストレージ ソリューションの例です。

- デュアル ポート SCSI デバイス
- Storage Area Network (SAN)

デュアル ポート SCSI および SAN ソリューションは、書き込み順序および同期書き込み永続性の要件を満たしています。

クラスタソフトウェア

クラスタ ソフトウェアによって、ネットワーク内のサーバがコンピュータ クラスタ内で協調して動作し、アプリケーションのハイ アベイラビリティを提供します。

重要: この章で説明されている手順は、**Microsoft クラスタ ソフトウェア** および **Active Directory** のみに適用されます。

ハイ アベイラビリティ展開では、クラスタ ソフトウェアは以下のタスクを実行します。

- プライマリおよびセカンダリのエンタープライズ管理サーバのステータスを監視します。
- 1つのインスタンス（プライマリ サーバまたはセカンダリ サーバのいずれか）のみが一度にアクティブであることを確認します。
- エンタープライズ管理サーバ上の CA ControlMinder サービスを管理します。
- エンドポイントをアクティブなサーバにポイントする、共有ホスト名を管理します。

障害が発生した場合の動作

高可用環境では、クラスタ化ソリューション ソフトウェアが、一定の間隔でプライマリ サーバの可用性を確認します。プライマリ サーバが事前に定義された期間内に応答しない場合、クラスタ化ソリューション ソフトウェアおよび **CA ControlMinder** では以下を実行します。

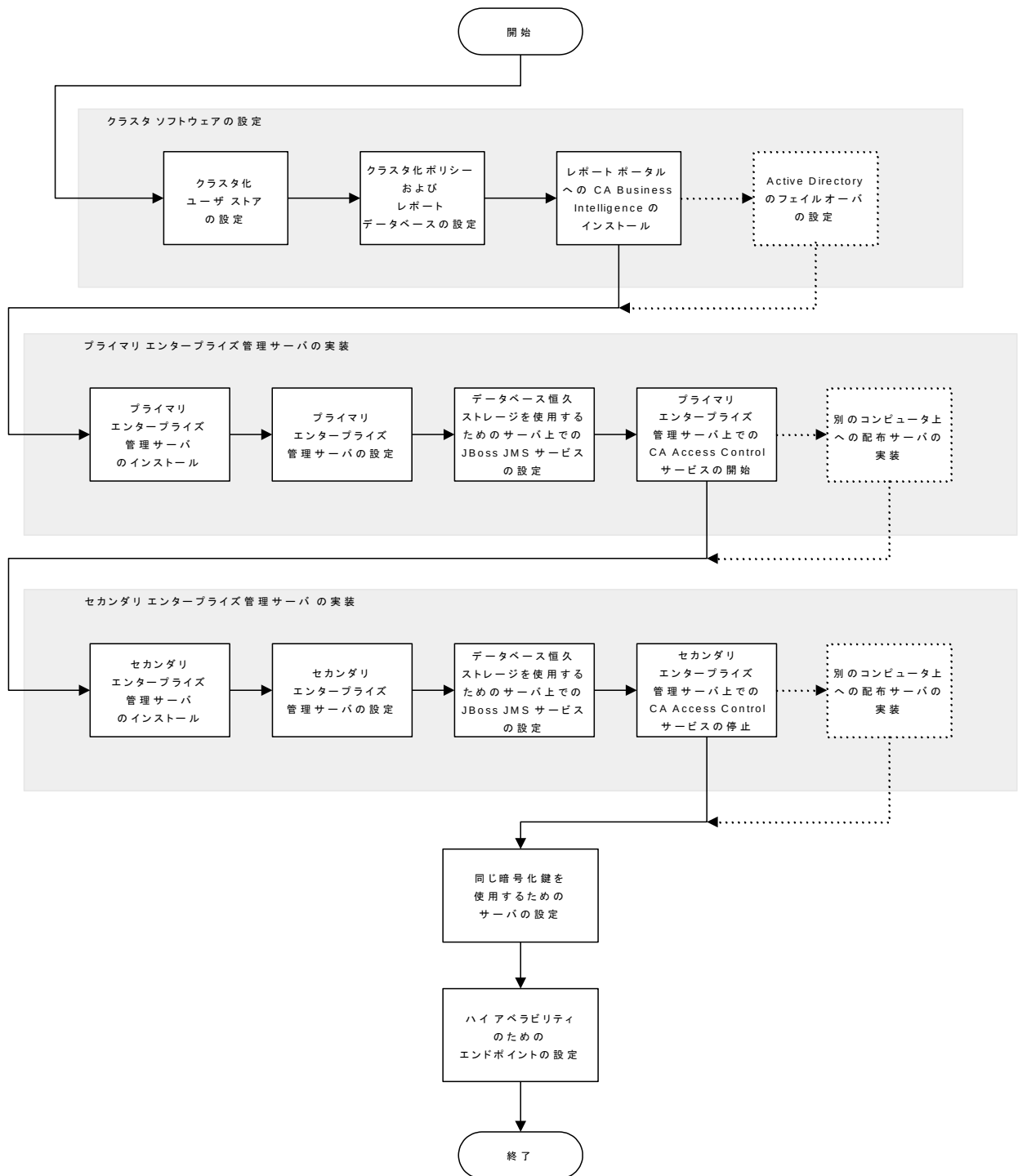
1. クラスタ化ソリューション ソフトウェアは、プライマリ サーバ上で実行されているすべてのエンタープライズ管理サーバサービスを停止します。
2. クラスタ化ソリューション ソフトウェアは、セカンダリ サーバ上ですべてのエンタープライズ管理サーバサービスを開始します。
3. **CA ControlMinder** エンドポイントは、セカンダリ サーバに接続して作業を続行することを試行します。
4. クラスタ化ソフトウェア ソリューションがプライマリ サーバ上のエンタープライズ管理サーバサービスを停止した場合、アプリケーションにログインしていたすべてのユーザはログアウトされます。アプリケーションの使用を続行するには、再度 **CA ControlMinder** エンタープライズ管理 にログインする必要があります。

ハイ アベイラビリティ環境の CA ControlMinder エンタープライズ管理 を設定する方法

ハイ アベイラビリティ展開を正しく設定するには、プライマリおよびセカンダリのエンタープライズ管理サーバを正しい順序でセットアップする必要があります。

以下の図は、ハイ アベイラビリティ環境に複数のエンタープライズ管理サーバを実装するために必要な手順を示しています。

注: 任意の手順として、フェールオーバー用に **Active Directory** を設定すること、および配布サーバを別のコンピュータに実装することがあります。



詳細情報:

[エンタープライズ管理サーバコンポーネントのインストール方法 \(P. 70\)](#)

[レポート サービス サーバコンポーネントの設定方法 \(P. 128\)](#)

プライマリ エンタープライズ管理サーバの設定

プライマリ エンタープライズ管理サーバは集中管理サーバで、エンドポイントへのポリシーのデプロイ、特権アカウントの管理、リソース、アクセス、およびアクセス レベルの定義を行うためのコンポーネントやツールが含まれています。

以下の手順に従います。

1. まだの場合は、プライマリ サーバに **CA ControlMinder エンタープライズ管理** をインストールします。

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA ControlMinder がインストールされます。

2. すべての CA ControlMinder サービスを停止します。
3. サービスが自動的にではなく手動で開始されるように変更します。
4. 以下のとおり、共用ストレージに **DMS** と **DH** をコピーします。
 - a. **DMS** ディレクトリにアクセスし、共用ストレージにコピーします。このディレクトリは、以下の場所にあります。

`ACServerInstallDir/APMS/AccessControl/data/DMS__`

`ACServerInstallDir`

エンタープライズ管理サーバがインストールされているディレクトリの名前を定義します。

- b. **DH** ディレクトリにアクセスし、共用ストレージにコピーします。このディレクトリは、以下の場所にあります。

`ACServerInstallDir/APMS/AccessControl/Data/DH__`

- c. **DH__WRITER** ディレクトリにアクセスし、共用ストレージにコピーします。デフォルトでは、このディレクトリは以下の場所にあります。

ACServerInstallDir/APMS/AccessControl/Data/DH__WRITER

- d. `_pmd directory_` レジストリ キーを設定し、DMS および DH のコピー先の共有ストレージ ディレクトリの完全パス名を設定します。
例: `Z:\PMD`

プライマリ サーバは、共有ストレージ上の DMS と DH を使用するよう
に設定されます。

- 5. 以下の手順に従って、共有ストレージを使用するようメッセージ
キューを設定します。

- a. 以下のファイルを共有ストレージに移動します。 `routes.conf`、
`groups.conf`、`queues.conf`、`users.conf`

これらのファイルは、以下のディレクトリにあります。

ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

- b. メッセージ キューのデータストア ファイルを共有ストレージに
移動します。これらのファイルは、以下のディレクトリにあります。

ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/data
store

- c. `tibemsd.conf` ファイルを編集できる形で開きます。このファイルは、
デフォルトで以下のディレクトリにあります。

ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

- a. `routes.conf`、`user.conf`、`groups.conf` および `queues.conf` の場所を
共有ストレージに設定します。 例: `Z:/Tibco/users.conf`
- b. "store" トークンの値を、データ ストア ファイルがコピーされ
た共有ストレージ上のディレクトリを指すように設定します。
例: `Z:\PMD\DATASTORE`
- c. "server" トークンの値を、サフィックスのない大文字で、クラ
スタ論理名に設定します。 例: `server=ENTMCLUSTER`.
- d. ファイルを保存して閉じます。
- d. `queues.conf` ファイルを編集できる形で開きます。
 - a. 各キュー定義行の行末に、カンマと `"store=$sys.fail-safe"` という
単語を追加します。
 - b. ファイルを保存して閉じます。

6. プライマリ エンタープライズ管理サーバが運用を再開した場合に CA ControlMinder サービスをすべて開始するバッチ ファイルを以下のように作成します。

```
seosd -start
net start acrpmtq
net start "CA Access Control Web Service"
net start im_jcs
net start JBAS50SVC
```

7. プライマリ エンタープライズ管理サーバが失敗した場合にすべての CA ControlMinder サービスを停止するバッチ ファイルを以下のように作成します。

```
secons -s

net stop acrpmtq
net stop "CA Access Control Web Service"
net stop im_jcs
net stop JBAS50SVC
```

8. 失敗時にスクリプトを実行するためのクラスタ ソフトウェアを設定します。
9. すべての CA ControlMinder サービスを開始します。

例: queues.conf ファイルの編集

queues.conf ファイルの以下のスニペットは、共有ストレージを使用するようメッセージキューを設定するために、ファイルを変更する方法について例を示しています。

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

セカンダリ エンタープライズ管理サーバの設定

セカンダリ エンタープライズ管理サーバは、プライマリ サーバに障害が発生した場合にエンドポイントのリクエストを処理します。

以下の手順に従います。

1. 必要に応じて、プライマリ エンタープライズ管理サーバから一時ディレクトリに **FIPS** キーをコピーします。このファイルは以下のディレクトリにあります。

```
JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys
```

JBoss_HOME

JBoss がインストールされているディレクトリの名前を定義します。

2. コマンドプロンプト ウィンドウからエンタープライズ管理サーバをセカンダリ サーバにインストールし、プライマリ エンタープライズ管理サーバ上の **FIPS** キーの完全パス名を指定します。

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA ControlMinder がインストールされます。

3. すべての CA ControlMinder サービスを停止します。
4. サービスが自動的にではなく手動で開始されるように変更します。
5. **_pmd directory_** レジストリ キーを設定し、DMS および DH のコピー先の共有ストレージ ディレクトリの完全パス名を設定します。例：

Z:\PMD

セカンダリ サーバは、共用ストレージ上の DMS と DH を使用するよう設定されます。

6. 共用ストレージを使用するようにメッセージ キューを設定します。以下の手順を実行します。
 - a. **tibemsd.conf** ファイルを編集できる形で開きます。このファイルは、デフォルトで以下のディレクトリにあります。

```
ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
```

ACServerInstallDir

エンタープライズ管理サーバがインストールされているディレクトリの名前を定義します。

- a. `routes.conf`、`user.conf`、`groups.conf` および `queues.conf` の場所を共有ストレージに設定します。例：`Z:/Tibco/users.conf`
- b. "server" トークンの値を、サフィックスのない大文字で、クラスタ論理名に設定します。例：`server=ENTMCLUSTER`。
- c. ファイル、`routes.conf`、`groups.conf`、`queues.conf`、`users.conf` を以下のディレクトリから削除します。

ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

- d. "store" トークンの値を、データストアファイルがコピーされた共有ストレージ上のディレクトリを指すように設定します（例：`Z:¥PMD`）。
 - e. ファイルを保存して閉じます。
- b. `queues.conf` ファイルを編集できる形で開きます。
 - c. キュー定義の行ごとに、行末にカンマと "`store=$sys.fail-safe`" という単語を追加し、ファイルを保存して閉じます。

7. CA ControlMinder サービスが実行されていないことを確認します。
8. セカンダリ エンタープライズ管理サーバを許可するよう DMS を以下のとおり設定します。

- a. プライマリ エンタープライズ管理サーバで、JCS、JBoss アプリケーションサーバ、CA ControlMinder およびメッセージキュー サービスを開始します。
- b. `selang` コマンドプロンプト ウィンドウを開いて、以下のコマンドを入力します。

```
host DMS__@
```

ローカル ホストに接続されたことを通知するメッセージが表示されます。

- c. 以下のコマンドを入力し、許可された端末のリストを表示します。

```
sr TERMINAL *
```

CA ControlMinder は、許可された端末の詳細を表示します。

- d. 以下のコマンドを入力し、セカンダリ エンタープライズ管理サーバを許可された端末リストに追加します。

```
newres TERMINAL
<secondary_enterprise_management_server_full_DN> audit (f)
owner(nobody)defacc(r)
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(+reportagent) access(write)
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(DOMAIN¥Administrator) access(write,read)
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(ac_entm_pers) access(write,read)
```

9. プライマリ エンタープライズ管理サーバに障害が発生した場合に CA ControlMinder サービスをすべて開始するバッチ ファイルを以下のよう

```
seosd -start
net start acrptmq
net start "CA Access Control Web Service"
net start im_jcs
net start JBAS50SVC
```

10. プライマリ エンタープライズ管理サーバが運用を再開した場合に CA ControlMinder サービスをすべて停止するバッチ ファイルを以下のよう
に作成します。

```
secons -s
net stop acrptmq
net stop "CA Access Control Web Service"
net stop im_jcs
net stop JBAS50SVC
```

11. 失敗時にスクリプトを実行するための Microsoft クラスタ ソフトウェアを設定します。

セカンダリ エンタープライズ管理サーバが設定されました。

高可用性用の負荷分散エンタープライズ管理サーバの設定

高可用性用にプライマリおよびセカンダリ エンタープライズ管理サーバを設定した後、高可用性用に負荷分散エンタープライズ管理サーバをインストールし設定できます。

注: 負荷分散エンタープライズ管理サーバをインストールする前に、クラスタの完全修飾 DNS 名を解決できることを確認します。

負荷分散エンタープライズ管理サーバをインストールするには、プライマリ エンタープライズ管理サーバのインストール手順に従います。

重要: インストール ウィザードによってプロンプトが表示されたら、[負荷分散エンタープライズ管理サーバ] を選択します。プライマリ エンタープライズ管理サーバ情報に関するプロンプトが表示されたら、クラスタ論理名を指定する必要があります。IP アドレスは指定しません。

フェールオーバー用の Active Directory の設定

ユーザストアとして Active Directory を使用する場合、複数のドメインコントローラと連携するようエンタープライズ管理サーバを設定できます。プライマリドメインコントローラに障害が発生した場合は、別のドメインコントローラが引き継いでクライアント要求に対応します。

以下の手順に従います。

1. [CA IdentityMinder 管理コンソールを有効にします](#) (P. 104)。

CA Identity Manager 管理コンソールを使用して、環境内のドメインコントローラのリストを設定します。

2. [CA IdentityMinder 管理コンソールを開きます](#) (P. 105)。

3. [ディレクトリ] をクリックし、ac-dir 環境を選択します。

ディレクトリのプロパティウィンドウが表示されます。

4. [エクスポート] をクリックし、XML ファイルを保存します。

5. XML ファイルを編集できる形で開きます。<Connection host=host_name> タグを見つけて、以下に例を示します。

```
<Connection host="primaryDir.com" port="389">
```

6. 行の終りに文字列 "failover" を追加し、ドメインコントローラのホスト名およびポート番号をスペース区切りのリストで指定して、ファイルを保存します。以下に例を示します。

```
<Connection host="ADserver1" port="389"
failover="ADserver2:389"/>
```

7. 管理コンソールで、[更新] をクリックします。

ディレクトリの更新ウィンドウが表示されます。

8. 編集した XML ファイルの完全パス名を入力するか、ファイルを検索して選択し、[完了] をクリックします。

ディレクトリ設定出力フィールドにステータス情報が表示されます。

9. [続行] をクリックし、環境を再起動します。

エンタープライズ管理サーバがプライマリおよびセカンダリのドメインコントローラと連携できるようになりました。

ローカル DMS での CA ControlMinder エンタープライズ管理 の設定

完全修飾ドメイン名ではなく「localhost」を使用して、DMS に接続するように、エンタープライズ管理サーバ上で DMS を設定します。

ローカル DMS で CA ControlMinder エンタープライズ管理 を設定する方法

1. CA ControlMinder エンタープライズ管理 にログインし、[システム] - [DMS] - [接続の変更] を選択します。

[接続の変更： 接続の検索] ウィンドウが表示されます。

2. デフォルトの DMS 接続を検索し、[選択] をクリックします。

[接続の変更：<接続名>] ウィンドウが表示されます。

3. 以下のようにホスト名を LocalHost に変更します。

DMS__@localhost

4. [サブミット] をクリックします。

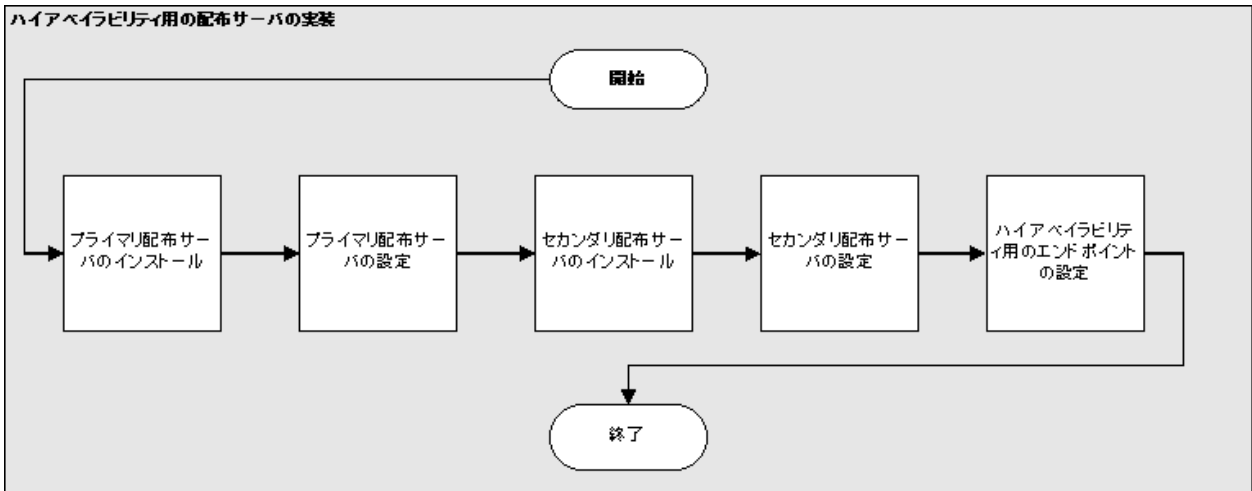
セカンダリおよびプライマリの配布ホストで、DMS コンピュータを共有できるようになりました。

ハイ アベイラビリティ環境の配布サーバを設定する方法

ハイ アベイラビリティ環境で複数の配布サーバを適切に設定するには、プライマリおよびセカンダリの配布サーバを正しい順序でセットアップする必要があります。

以下の図は、1つのエンタープライズ管理サーバと連携するように複数の配布サーバをセットアップするために必要な手順を示しています。

重要： CA ControlMinder エンタープライズ管理 を CA Enterprise Log Manager と統合する場合のみ、以下の手順を完了します。障害が発生した配布サーバが収集したが、エンタープライズ管理サーバおよび CA Enterprise Log Manager に送信しなかったすべてのイベントが失われないように、ハイ アベイラビリティ用に配布サーバを設定します。



詳細情報：

[配布サーバのインストール](#) (P. 536)

プライマリ配布サーバの設定

配布サーバは、アプリケーションサーバとエンドポイント間の通信を処理します。

スタンドアロン配布サーバのみをインストールする場合は、この手順を完了する必要があります。

以下の手順に従います。

1. [サービス] ウィンドウから、JCS、CA ControlMinder およびメッセージキューサーバサービスを停止します。
2. サービスが自動的にではなく手動で開始されるように変更します。
3. 共有ストレージに **PMD** ディレクトリを作成します。
4. 以下の手順に従って、共有ストレージを使用するよう配布ホストを設定します。

- a. 共有ストレージに **DH** ディレクトリをコピーします。このディレクトリは、以下の場所にあります。

DistServerInstallDir/APMS/AccessControl/Data/DH__

DistServerInstallDir

配布サーバをインストールしたディレクトリの名前を定義します。

- b. 共有ストレージに **DH__WRITER** ディレクトリをコピーします。このディレクトリは、以下の場所にあります。

DistServerInstallDir/APMS/AccessControl/Data/DH__WRITER

- c. 共有ストレージに **DMS__directory** をコピーします。このディレクトリは、以下の場所にあります。

DistServerInstallDir/APMS/AccessControl/Data/DMS__

- d. **¥ComputerAssociates¥AccessControl¥PMD** の下で、**_pmd_directory_** レジストリキーを、**DMS** と **DH** がコピーされた共有ストレージディレクトリの完全パス名に設定します。例：**Z:¥PMD**

プライマリサーバは、共有ストレージ上の **DMS** と **DH** を使用するように設定されます。

5. 以下の手順に従って、共有ストレージを使用するようメッセージキューを設定します。
 - a. 共有ストレージ上にディレクトリを作成します。例：
`Z¥MessageQueue`
 - b. メッセージキューのデータストア フォルダを共有ストレージにコピーします。これらのファイルは、以下のディレクトリにあります。

`DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`
 - c. `tibemsd.conf` ファイルを編集できる形で開きます。このファイルは、以下のディレクトリにあります。

`DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`
 - d. "`store`" トークンの値を、データ ストア ファイルがコピーされた共有ストレージ上のディレクトリを指すように設定します。例：
`F:¥MessageQueue`
 - e. ファイルを保存して閉じます。
 - f. `queues.conf` ファイルを編集できる形で開きます。
 - g. キュー定義の行ごとに、行末にカンマと "`store=$sys.fail-safe`" という単語を追加し、ファイルを保存します。
6. CA ControlMinder サービスを開始します。

例: `queues.conf` ファイルの編集

`queues.conf` ファイルの以下のスニペットは、共有ストレージを使用するようメッセージキューを設定するためにファイルを変更する方法を示しています。

```
queue/snapshots secure,store=$sys.fail-safe
queue/audit secure,store=$sys.fail-safe
ac_endpoint_to_server secure,store=$sys.fail-safe
ac_server_to_endpoint secure,store=$sys.fail-safe
```

セカンダリ配布サーバの設定

アクティブな配布サーバが事前に定義された期間内に応答しなかった場合、セカンダリ配布サーバが、アプリケーションサーバとエンドポイントの間の通信を処理します。

以下の手順に従います。

1. JCS、CA ControlMinder およびメッセージキューサーバサービスを停止します。
2. サービスが自動的にではなく手動で開始されるように変更します。
3. ¥ComputerAssociates¥AccessControl¥PMD の下で、_pmd_directory_ レジストリキーを、DMS と DH がコピーされた共用ストレージディレクトリの完全パス名に設定します。例：Z:¥PMD

セカンダリ配布サーバは、共用ストレージ上の DMS と DH のファイルにアクセスできるようになりました。共有ストレージを使用できるように配布ホストが設定されました。

4. 以下の手順に従って、共用ストレージを使用するようメッセージキューを設定します。
 - a. tibemsd.conf ファイルを編集できる形で開きます。このファイルは、以下のディレクトリにあります。

DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

DistServerInstallDir

配布サーバをインストールしたディレクトリの名前を定義します。

- b. "store" トークンの値を、データストアファイルがコピーされた共有ストレージ上のディレクトリを指すように設定します（例：Z:¥Datastore）。
 - c. ファイルを保存して閉じます。
 - d. queues.conf ファイルを編集できる形で開きます。
 - e. キュー定義の行ごとに、行末にカンマと "store=\$sys.fail-safe" という単語を追加し、ファイルを保存します。
5. セカンダリサーバ上の CA ControlMinder サービスが停止されていることを確認します。

ハイ アベイラビリティ環境のエンドポイントの設定

プライマリおよびセカンダリ エンタープライズ管理サーバをインストールして設定したら、ハイ アベイラビリティ環境で動作する CA ControlMinder エンドポイントをセットアップします。

ハイ アベイラビリティ環境のエンドポイントを設定する方法

1. 拡張ポリシー管理クライアント機能を有効にした状態で、CA ControlMinder をエンドポイントにインストールします。
CA ControlMinder エンドポイントがインストールされます。
2. エンドポイント上でコマンド プロンプト ウィンドウを開いて、以下のコマンドを入力します。

```
dmsmgr -config -dhname names
```

このコマンドは、カンマ区切り リストで指定した配布ホストと通信するようエンドポイントを設定します。

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

3. *Distribution_Server* 設定に配布サーバのリストをカンマ区切りで設定します。

```
ssl://ds1.sample.com:7243, ssl://ds2.sample.com:7243
```

4. 設定を保存します。

エンドポイントが通信可能な配布ホストおよび配布サーバのリストが設定されました。エンドポイントがハイ アベイラビリティ環境で動作するようになりました。

例: 配布サーバのリストの設定

以下の例は、ハイアベイラビリティ環境で使用する配布サーバのリストを設定する方法を示しています。

エンドポイントのインストール時に、エンドポイントが通信する配布サーバのパラメータを入力するよう求められます。デフォルトでは、これはエンタープライズ管理サーバになります。ハイアベイラビリティ環境を実現するには、プライマリ配布サーバに障害が発生した場合にセカンダリ配布サーバが使用されるようエンドポイントを設定します。

1. プライマリおよびセカンダリの配布サーバの名前を入力します。

```
dmsmgr -config -dhname DH__@node1.computer.com,DH__@node2.computer.com
```

アクションが正常に実行されたことを確認するメッセージが表示されます。

2. プライマリおよびセカンダリの配布サーバの URL のリストを指定します。

- UNIX : `accommon.ini` ファイルの [通信] セクション内の `Distribution_Server` パラメータを変更します。
- Windows : Windows レジストリで `Distribution_Server` 値を変更します。このパラメータは以下にあります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication
```

詳細情報:

[UNIX エンドポイントのインストールおよびカスタマイズ \(P. 211\)](#)

[Windows エンドポイントのインストールおよびカスタマイズ \(P. 173\)](#)

ハイアベイラビリティ用の Oracle RAC の設定

ポリシーおよびレポート データベースとして Oracle を使用している場合、Oracle RAC を使用してハイアベイラビリティ用に Oracle を設定できます。Oracle Real Applications Cluster (RAC) は共有ディスク アーキテクチャをベースとするクラスタ データベースで、Oracle データベースにハイアベイラビリティを提供します。

例: Oracle RAC を使用した、ハイ アベイラビリティ用の CA ControlMinder エンタープライズ管理 の設定

以下の例では、ハイ アベイラビリティ用に Oracle RAC を使用するための、CA ControlMinder エンタープライズ管理 の設定方法について説明します。

1. エンタープライズ管理用の Oracle データベースの準備

Oracle RAC サーバ上にユーザ アカウントを作成し、CA ControlMinder エンタープライズ管理 をインストールするためのユーザ権限を割り当てます。

2. ハイ アベイラビリティ用の CA ControlMinder エンタープライズ管理 の実装

プライマリおよびセカンダリのエンタープライズ管理サーバをインストールおよび設定します。

注: [ホスト名] フィールドに Oracle RAC の論理名を、[サービス名] フィールドに共有サービス名をそれぞれ指定します。

3. Oracle RAC ホスト名が正しく解決されることを確認します。

ホストの IP アドレスを Oracle RAC の論理名にマップします。例:

```
11.11.111.11  Node1MachineName
11.11.111.12  Node2MachineName
11.11.111.11  Node1LogicalMachineName
11.11.111.12  Node2LogicalMachineName
```

4. Oracle RAC を使用するために、プライマリおよびセカンダリのエンタープライズ管理サーバ設定を変更します。以下の手順を実行します。

- a. JBoss アプリケーション サーバを停止します。
- b. 以下のディレクトリに移動します。ここで、JBoss_HOME は JBoss をインストールしたディレクトリです。

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

5. 以下のファイルを編集できる形で開きます。

```
imauditdb-ds.xml
imtaskpersistencedb-ds.xml
imworkflowdb-ds.xml
objectstore-ds.xml
reportsnapshot-ds.xml
```

6. 各ファイルで、<connection-url> タグを見つけ、ホスト名とサービス名を以下のように指定します。

```
<connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)
)(ADDRESS_LIST=(ADDRESS=(protocol=tcp)(host=Node1LogicalMachineName)(port=1521))
(ADDRESS=(protocol=tcp)(host=Node2LogicalMachineName)(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=SharedService)))</connection-url>
```

7. 各ファイルで、以下の行を追加します。

```
<check-valid-connection-sql>select 1 from dual</check-valid-connection-sql>
```

8. ファイルを保存して閉じます。
9. JBoss アプリケーション サーバを始動します。

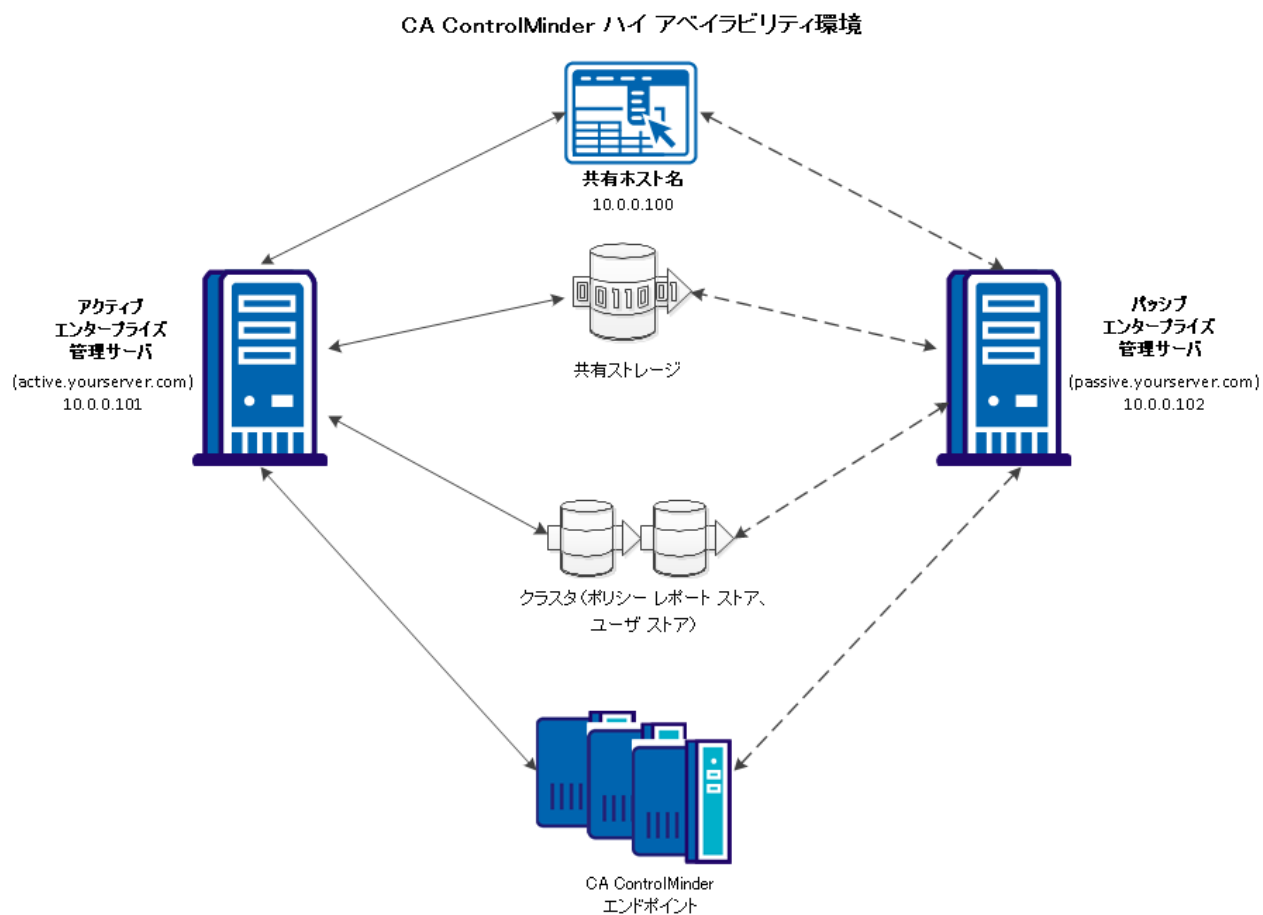
これで、プライマリおよびセカンダリのエンタープライズ管理サーバを設定しました。

Veritas Cluster Server を使用した Linux 上の CA ControlMinder ハイ アベイラビリティの実装

ハイ アベイラビリティ展開によって、1 つ以上のコンポーネントまたはサーバに障害が発生した場合に、使用する **CA ControlMinder** エンタープライズ管理コンポーネントが継続してリクエストに対応できるようサポートされます。エンドポイントがプライマリ環境に接続できない場合、プライマリ環境がリストアされるまで、エンドポイントはセカンダリサーバに接続します。

プライマリおよびセカンダリ **CA ControlMinder** エンタープライズ管理サーバは共有されたホスト名にアクセスする同じデータセンターに位置します。プライマリ環境に障害が発生した場合、**Veritas Cluster** ソフトウェアはサービスの切り替えを有効にし、セカンダリ環境が制御を開始します。

以下の図は、ハイ アベイラビリティ環境における **CA ControlMinder** エンタープライズ管理を示しています。

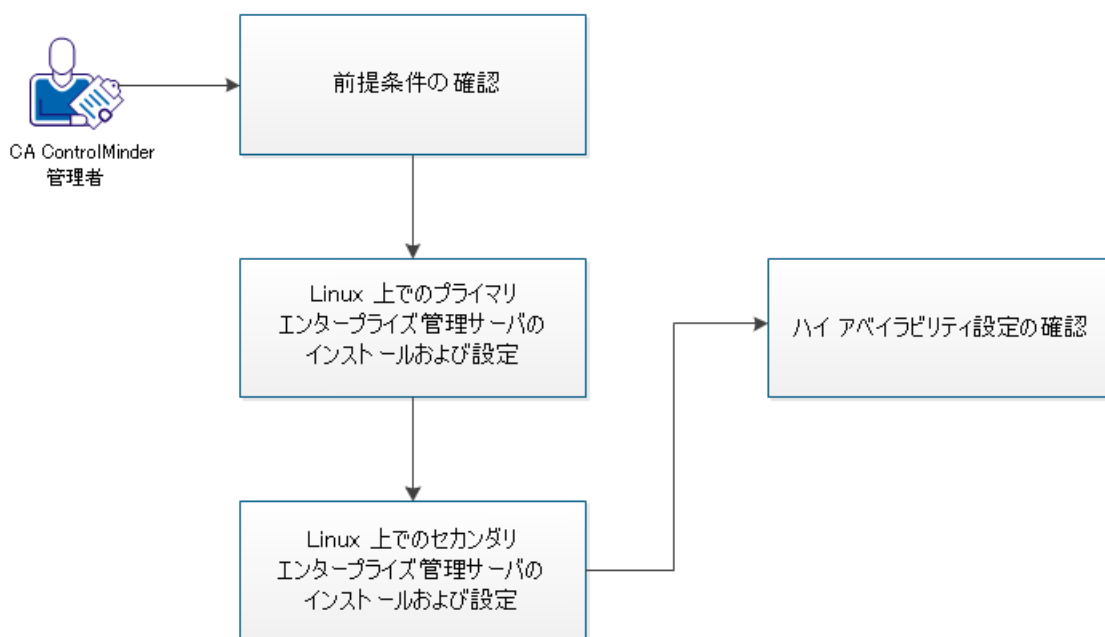


この図に示されるように、ハイ アベイラビリティ展開には以下のコンポーネントがあります。

- プライマリ（アクティブ）エンタープライズ管理サーバと、少なくとも1つのセカンダリ（パッシブ）エンタープライズ管理サーバ。
- ポリシーおよびレポートストアのクラスタ化されたインストール、およびユーザストア。
- プライマリおよびセカンダリ CA ControlMinder エンタープライズ管理サーバの両方からアクセス可能な共有ストレージ。
- 共有ホスト名
- プライマリおよびセカンダリ エンタープライズ管理サーバの両方にアクセス可能な CA ControlMinder エンドポイント。

以下の図は、Veritas Cluster Server を使用して Linux 上に CA ControlMinder ハイ アベイラビリティを設定する方法を示しています。

**Veritas Cluster Server を使用した
Linux 上の CA ControlMinder ハイ アベイラビリティの実装**



以下の手順に従います。

1. [前提条件を確認します](#) (P. 504)。
2. [Linux 上でプライマリ エンタープライズ管理サーバを設定します](#) (P. 505)。
3. [Linux 上でセカンダリ エンタープライズ管理サーバを設定します](#) (P. 515)。
4. [ハイ アベイラビリティ設定を確認します](#) (P. 518)。

前提条件の確認

Veritas Cluster Server を使用して、Linux 上で CA ControlMinder ハイ アベイラビリティを実装する前に以下の前提条件を確認します。

1. サポートされた OS バージョンおよび 2 つの NIC（ネットワーク インターフェース コントローラ）を持つ 2 つの同様のノードが使用可能です。
2. プライマリおよびセカンダリ CA ControlMinder エンタープライズ管理サーバがインストールされていることを確認します。
注: エンタープライズ管理サーバを Linux にインストールする詳細については、「実装ガイド」を参照してください。
3. 共有ストレージが各ノードによってアクセス可能であることを確認します。4 ～ 5 のディスクまたは LUN（論理装置番号）が 2 つのノードで共有されることをお勧めします。
4. Linux Veritas Cluster Server がインストールされ、スクリプトに自動スイッチ オーバーの準備ができていることを確認します。

注: Veritas Cluster Server をインストールする詳細については、[Symantec](#) Web サイト上の「Linux 5.1 Veritas Cluster Server インストールガイド」を参照してください。

プライマリ エンタープライズ管理サーバの設定

プライマリ エンタープライズ管理サーバは集中管理サーバで、エンドポイントへのポリシーのデプロイ、特権アカウントの管理、リソース、アクセス、およびアクセス レベルの定義を行うためのコンポーネントやツールが含まれています。

注: この手順は、ユーザがプライマリ エンタープライズ管理サーバおよびすべての Web ベース アプリケーション、配布サーバ、および DMS をインストールしたことを前提としています。

次の手順に従ってください:

1. CA ControlMinder サービスが開始されていることを確認します。

CA ControlMinder エンタープライズ管理 を使用するには、CA ControlMinder が実行中である必要があります。

2. JBoss アプリケーション サーバ サービスが開始されていることを確認します。JBoss アプリケーション サーバ サービスが開始されていない場合は、以下のコマンドを実行します。

```
./JBOSS_DIR/bin/run.sh -b 0.0.0.0
```

JBoss Application Server のロードが終了すると、CA ControlMinder エンタープライズ管理 の Web ベース インターフェースにログインできます。

3. セカンダリ エンタープライズ管理サーバを許可するよう DMS を以下のとおり設定します。
 - a. プライマリ エンタープライズ管理サーバで、JCS、JBoss アプリケーション サーバ、CA ControlMinder およびメッセージ キュー デーモンを開始します。
 - b. `selang` コマンドプロンプト ウィンドウを開いて、以下のコマンドを入力します。

```
host DMS__@
```

ローカル ホストに接続されたことを通知するメッセージが表示されます。

- c. 以下のコマンドを入力し、許可された端末のリストを表示します。

```
sr TERMINAL *
```

CA ControlMinder は、許可された端末の詳細を表示します。

- d. 以下のコマンドを入力し、セカンダリ エンタープライズ管理サーバを許可された端末リストに追加します。

```
newres TERMINAL
<secondary_enterprise_management_server_full_DN> audit (f)
owner(nobody)defacc(r)
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(+reportagent) access(write)
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(DOMAIN¥Administrator) access(write,read)
authorize TERMINAL
<secondary_enterprise_management_server_full_DN>
uid(ac_entm_pers) access(write,read)
```

4. 以下のコマンドを実行して、ポリシーを配布するために CA ControlMinder が使用するホスト名を変更します。

```
sepmd -u DH__WRITER DMS__@<node1 host name>
sepmd -s DH__WRITER DMS__@<cluster shared DNS NAME>
sepmd -u DMS__ DH__@<node1 host name>
sepmd -s DMS__ DH__@<cluster shared DNS NAME>
```

5. すべての CA ControlMinder デーモンを停止します。
6. [サービスが自動的にではなく手動で開始されるように変更](#) (P. 510) します。
7. 以下のとおり、共用ストレージに DMS と DH をコピーします。
- a. たとえば /shared/AccessControlServer/ のような共有ストレージに DMS ディレクトリをコピーします。このディレクトリは、以下の場所にあります。

```
ACServerInstallDir/APMS/AccessControl/policies/DMS__
ACServerInstallDir
```

エンタープライズ管理サーバをインストールしたディレクトリの名前を定義します。

- b. 共有ストレージに DH ディレクトリをコピーします。このディレクトリは、以下の場所にあります。

```
ACServerInstallDir/APMS/AccessControl/policies/DH__
```

- c. 共有ストレージに DH__WRITER ディレクトリをコピーします。このディレクトリは、以下の場所にあります。

```
ACServerInstallDir/APMS/AccessControl/policies/DH__WRITER
```

- d. `seos.ini` ファイルを開いて、編集します。このファイルは以下の場所にあります。

```
ACServerInstallDir/APMS/AccessControl
```

- e. `_pmd directory_` トークン設定の値を、DMS と DH がコピーされた共有ストレージディレクトリの完全パス名に設定します。例：
`/shared/AccessControlServer/`

プライマリ サーバは、共有ストレージ上の DMS と DH を使用するように設定されます。

- 8. 以下の手順に従って、共有ストレージを使用するようメッセージキューを設定します。

- a. メッセージキューのデータストア ファイルを共有ストレージに移動します。これらのファイルは、以下のディレクトリにあります。

```
ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore
```

メッセージキュー データ ストア ファイルをコピーする例を以下に示します。

```
# cp -r  
/opt/CA/AccessControlServer/MessageQueue/tibco/cfgmgmt/ems/  
data /shared/MessageQueue/data/
```

- b. `tibemsd.conf` ファイルを開いて、編集します。このファイルは、デフォルトで以下のディレクトリにあります。

```
ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
```

- a. `routes.conf`、`user.conf`、`groups.conf` および `queues.conf` の場所を共有ストレージに設定します。例：
`/shared/MessageQueue/data/users.conf`

- b. `store` トークンの値を、データ ストア ファイルがコピーされた共有ストレージ上のディレクトリを指すように設定します。
例：`/shared/MessageQueue/data/datastore`。

- c. `server` トークンの値を、サフィックスのない大文字のクラスタ論理名に設定します。例：`server=ENTMCLUSTER`。

- d. ファイルを保存して閉じます。

- c. `queues.conf` ファイルを開いて、編集します。
 - a. 各キュー定義行の行末に、カンマと `store=$sys.failsafe` という単語を追加します。
 - b. ファイルを保存して閉じます。
- d. `routes.conf` ファイルを開いて編集し、以下をコメントにします。

```
# vi shared/MessageQueue/data/routes.conf
```

```
#[EMS-SERVER2]
```

```
# url=tcp://7022
```

- e. Tibco ユーザが読み取りおよび書き込みアクセスを持つように Tibco フォルダを変更します。
 - a. `gid 65534` で Tibco グループを作成します。Tibco フォルダを作成する例を以下に示します。

```
# groupadd -g 65534 tibco
```
 - b. `uid 65534` で Tibco ユーザを作成します。Tibco ユーザを作成する例を以下に示します。

```
# useradd -g 65534 -u 65534 tibco
```
 - c. `MessageQueue` ディレクトリおよびすべてのサブディレクトリの所有権を変更します。 `MessageQueue` ディレクトリおよびすべてのサブディレクトリの所有権を変更する例を以下に示します。

```
#chown -R tibco /shared/MessageQueue
```
 - d. `MessageQueue` ディレクトリおよびすべてのサブディレクトリで権限を変更します。 `MessageQueue` ディレクトリおよびすべてのサブディレクトリの権限を変更する例を以下に示します。

```
#chmod -R u=rwx,go= /shared/MessageQueue
```

- e. デフォルトの Tibco ディレクトリ権限を変更して Tibco ユーザにのみ **rwX** アクセスを許可します。ディレクトリ権限を変更して Tibco ユーザにのみ **rwX** アクセスを許可する例を以下に示します。

```
#chown -R tibco /opt/CA/AccessControlServer/MessageQueue/  
#chmod -R u=rwX,go= /opt/CA/AccessControlServer/MessageQueue/
```

9. [CA Identity Minder 管理コンソールのクラスタ名にベース URL を変更します](#) (P. 511)。
10. プライマリ エンタープライズ管理サーバが失敗した場合に[すべての CA ControlMinder サービスを停止するバッチ ファイルを作成します](#) (P. 512)。
11. プライマリ エンタープライズ管理サーバが運用を再開した場合に[すべての CA ControlMinder サービスを開始するバッチ ファイルを作成します](#) (P. 513)。
12. [CA ControlMinder サービスのステータスを確認するバッチ ファイルを作成します](#) (P. 514)。
13. 失敗時にスクリプトを実行するためのクラスタ ソフトウェアを設定します。
14. すべての CA ControlMinder サービスを開始します。

プライマリ エンタープライズ管理サーバが設定されました。セカンダリ エンタープライズ管理サーバの設定に進んでください。

手動で開始するようにサービスを変更

プライマリおよびセカンダリ エンタープライズ管理サーバで `chkconfig` コマンドを使用することで、手動で開始するようにサービスを変更します。以下のスニペットは `chkconfig` スクリプトの例です。

```
# chkconfig --list im_jcs
im_jcs          0:off  1:off  2:on   3:on   4:on   5:on   6:off
# chkconfig im_jcs off
# chkconfig --list im_jcs
im_jcs          0:off  1:off  2:off  3:off  4:off  5:off  6:off
# chkconfig --list ca-acrptmq
ca-acrptmq      0:off  1:off  2:on   3:on   4:on   5:on   6:off
# chkconfig ca-acrptmq off
# chkconfig --list ca-acrptmq
ca-acrptmq      0:off  1:off  2:off  3:off  4:off  5:off  6:off
--list name
```

このオプションは、`chkconfig` が認識するすべてのサービス、および各実行レベルで停止または開始されるかどうかをリストします。 *name* を指定すると、サービス名情報が表示されます。

ベース URL の変更

ベース URL を CA Identity Minder 管理コンソールのクラスタ名に変更します。

次の手順に従ってください:

1. CA Identity Minder 管理コンソールが有効化されたことを確認します。
注: CA Identity Minder 管理コンソールの有効化の詳細については、「実装ガイド」のトピック「CA Identity Minder 管理コンソールの有効化」を参照してください。
2. CA Identity Minder 管理コンソールを開き、ホストで Web ブラウザを起動し、次の URL を入力します。
`http://enterprise_host:port/idmanage`
CA Identity Minder 管理コンソールが開きます。
3. [環境] をクリックします。
[環境] ページは、Identity Manager 環境のリストを示しています。
4. 環境を選択します。
[環境プロパティ] ページが表示されます。
5. ベース URL をクラスタ名に変更します。たとえば
`https://clusterentm.ca.com` にします。
[保存] をクリックします。

CA ControlMinder サービスを停止するバッチ ファイルの作成

プライマリおよびセカンダリ エンタープライズ管理サーバ上の CA ControlMinder サービス をすべて停止するバッチ ファイルを作成します。以下の例はメッセージキュー、Java Connector Service (JCS) および JBoss を停止します。

```
#!/bin/sh
#To Stop the AccessControl Services
/opt/CA/AccessControlServer/APMS/AccessControl/bin/secons -sk

#To Stop the CA ControlMinder Message Queue
#/etc/init.d/ca-acrptmq stop
su - tibco -c "/etc/init.d/ca-acrptmq stop"

#To Stop the Web Services
/opt/CA/AccessControlServer/APMS/AccessControl/bin/secons -S
"eacws"

#To Stop Java Connector Service JCS
/etc/init.d/im_jcs stop

#To Stop JBOSS
cd /opt/jboss-4.2.3.GA/bin/
/opt/jboss-4.2.3.GA/bin/shutdown.sh -S &
sleep 60
```


CA ControlMinder サービスを開始するバッチ ファイルの作成

プライマリおよびセカンダリ エンタープライズ管理サーバ上の CA ControlMinder サービス をすべて開始するバッチ ファイルを作成します。以下の例はメッセージキュー、Java Connector Service (JCS) および JBoss を開始します。

```
#!/bin/sh
#To Start the AccessControl Services
/opt/CA/AccessControlServer/APMS/AccessControl/bin/seload

#To Start the CA ControlMinder Message Queue
#/etc/init.d/ca-acrptmq start
su - tibco -c "/etc/init.d/ca-acrptmq start" &
sleep 10

#To Start Java Connector Service JCS
/etc/init.d/im_jcs start

#To Start JBOSS
cd /opt/jboss-4.2.3.GA/bin/
/opt/jboss-4.2.3.GA/bin/run.sh -b 0.0.0.0 &
sleep 9
```

CA ControlMinder サービスのステータスを確認するバッチ ファイルの作成

プライマリおよびセカンダリ エンタープライズ管理サーバ上のすべての CA ControlMinder サービスのステータスを確認するバッチ ファイルを作成します。

注: 要件に基づいてスクリプトをカスタマイズします。例で使用する終了コードは Veritas セットアップに基づいています。コードの詳細については、[Symantec サポート Web サイト](#)を参照してください。

すべての CA ControlMinder Services に対してステータスを確認する例を以下に示します。

```
#!/bin/sh

a=1;
b=1;
c=1;
d=1;
#CA Control Minder Status check using the Process SE0SD status
ps -ef | grep -v grep| grep seosd >/dev/null 2>&1;
a=$?;

#JCS running status check
b=`/etc/init.d/im_jcs status`;
if [ "$b" == "jcs is running" ];
then
b=0;
else
b=1;
fi

#CA ControlMinder Message Queue status check
c=`/etc/init.d/ca-acrptmq status`;
if [ "$c" = "CA ControlMinder Message Queue is running" ];
then
c=0;
else
c=1;
fi

#JB0SS running status check
ps -ef | grep -v grep| grep run.sh >/dev/null 2>&1;
d=$?

#echo "$a $b $c $d" #To Check the Individual process Status All Zeros
Means All Services are up and running and All Ones Means All Services
are down
```

```
#Script status will return '110' when all the services are up and
running, will return '100' when all services are down and will return
'1' when anyone of the service is down
if [ "$a$b$c$d" = "0000" ];
then
exit 110

elif [ "$a$b$c$d" = "1111" ];
then
exit 100

else
exit 1
fi
```

セカンダリ エンタープライズ管理サーバの設定

セカンダリ エンタープライズ管理サーバは、プライマリ サーバに障害が発生した場合にエンドポイントのリクエストを処理します。

次の手順に従ってください:

1. プライマリ エンタープライズ管理サーバから一時ディレクトリに FIPS キーをコピーします。このファイルは以下のディレクトリにあります。

```
JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/
netegrity/config/keys
```

JBOSS_HOME

JBoss がインストールされているディレクトリの名前を定義します。

2. コマンドプロンプトウィンドウからエンタープライズ管理サーバをセカンダリ サーバにインストールし、プライマリ エンタープライズ管理サーバ上の FIPS キーの完全パス名を指定します。

注: 同じデータベースおよび通信パスワードの詳細がプライマリ エンタープライズ管理サーバに使用されるのと同じ物であることを確認します。

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA ControlMinder がインストールされます。

3. すべての CA ControlMinder デーモンを停止します。
4. [サービスが自動的にではなく手動で開始されるように変更](#) (P. 510) します。

5. `_pmd directory_` トークン設定の値を、DMS と DH がコピーされた共有ストレージディレクトリの完全パス名に設定します。例：
`/shared/AccessControlServer/`

セカンダリ サーバは、共有ストレージ上の DMS と DH を使用するよう
に設定されます。

6. 共有ストレージを使用するようにメッセージキューを設定します。以下の手順を実行します。
 - a. `tibemsd.conf` ファイルを開いて、編集します。このファイルは、デフォルトで以下のディレクトリにあります。

`ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`
`ACServerInstallDir`

エンタープライズ管理サーバをインストールしたディレクトリ
の名前を定義します。

メッセージキュー データ ストア ファイルをコピーする例を以下
に示します。

```
# cp -r  
/opt/CA/AccessControlServer/MessageQueue/tibco/cfgmgmt/ems/  
data /shared/MessageQueue/data/
```

- a. `routes.conf`、`user.conf`、`groups.conf` および `queues.conf` の場所を共有ストレージに設定します。例：
`/shared/MessageQueue/data/users.conf`
- b. `server` トークンの値を、サフィックスのない大文字のクラスタ論理名に設定します。例：`server=ENTMCLUSTER`。

注: インストールは元の値としてコンピュータ名を書き込みます。
値は大文字で、ドメイン名を持たないクラスタのショートネーム
に変更される必要があります。クラスタ DNS 名が
「`entmcluster.ca.com`」である場合は、`ENTMCLUSTER` を指定します。

- c. ファイル、`routes.conf`、`groups.conf`、`queues.conf`、`users.conf` を以下のディレクトリから削除します。

`ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`

- d. *store* トークンの値を、データ ストア ファイルがコピーされた共有ストレージ上のディレクトリを指すように設定します (例: `/shared/MessageQueue/datastore`) 。
- e. ファイルを保存して閉じます。
- b. Tibco ユーザが読み取りおよび書き込みアクセスを持つように Tibco フォルダを変更します。
 - a. `gid 65534` で Tibco グループを作成します。Tibco フォルダを作成する例を以下に示します。

```
# groupadd -g 65534 tibco
```
 - b. `uid 65534` で Tibco ユーザを作成します。Tibco ユーザを作成する例を以下に示します。

```
# useradd -g 65534 -u 65534 tibco
```
 - c. デフォルトの Tibco ディレクトリ権限を変更して Tibco ユーザにのみ `rwX` アクセスを許可します。ディレクトリ権限を変更して Tibco ユーザにのみ `rwX` アクセスを許可する例を以下に示します。

```
#chown -R tibco /opt/CA/AccessControlServer/MessageQueue/  
#chmod -R u=rwX,go= /opt/CA/AccessControlServer/MessageQueue/
```
- 7. CA ControlMinder デーモンが実行されていないことを確認します。
- 8. プライマリ エンタープライズ管理サーバに障害が発生した場合に[すべての CA ControlMinder サービスを開始するバッチ ファイルを作成します](#) (P. 513)。
- 9. プライマリ エンタープライズ管理サーバが運用を再開した場合に[すべての CA ControlMinder サービスを停止するバッチ ファイルを作成します](#) (P. 512)。
- 10. [CA ControlMinder サービスのステータスを確認するバッチ ファイルを作成します](#) (P. 514)。
- 11. 失敗時にスクリプトを実行するためのクラスタ ソフトウェアを設定します。
セカンダリ エンタープライズ管理サーバが設定されました。

ハイ アベイラビリティ設定の確認

CA ControlMinder ハイ アベイラビリティ設定が正しく機能していることを確認します。

次の手順に従ってください:

1. プライマリ エンタープライズ管理サーバにログインし、以下の手順に従います。

- a. CA ControlMinder、JBoss およびメッセージ キュー サービスが開始され実行されていることを確認します。
- b. DMS および Tibco のリソースがプライマリ エンタープライズ管理サーバと共有されていることを確認します。
- c. `server.log` ファイルを開き、エラーが存在するかどうかを確認します。

`JBossInstallDir/server/default/log/server.log`

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

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

- d. CA ControlMinder、JBoss およびメッセージ キュー サービスを停止してプライマリ エンタープライズ管理サーバをシャットダウンします。
2. セカンダリ エンタープライズ管理サーバにログインし以下の手順に従います。

- a. 共有リソースがセカンダリ エンタープライズ管理サーバと共有されていることを確認します。
- b. CA ControlMinder、JBoss およびメッセージ キュー デーモンを開始します。
- c. `server.log` ファイルを開き、エラーが存在するかどうかを確認します。

`JBossInstallDir/server/default/log/server.log`

3. CA ControlMinder エンタープライズ管理にログインし以下の手順に従います。
- a. プライマリおよびセカンダリ エンタープライズ管理サーバが [ワールド ビュー]、[ホスト] セクションに表示されていることを確認します。

- b. プライマリおよびセカンダリ エンタープライズ管理サーバが [特権アカウント]、[エンドポイントの表示] セクションに表示されていることを確認します。
 - c. プライマリおよびセカンダリ エンタープライズ管理サーバが [システム]、[コネクタ サーバ]、[コネクタ サーバの表示] セクション内に表示されていることを確認します。
4. セカンダリ エンタープライズ管理サーバでさまざまなアクションを実行し、プライマリ エンタープライズ管理サーバ内のイベントを確認します。

エラーが発生しない場合は、CA ControlMinder ハイ アベイラビリティは正常に設定されています。

付録 A: トラブルシューティング

このセクションには、以下のトピックが含まれています。

[Tibco ユーザが Tibco サービスを開始できない \(P. 521\)](#)

[JCS がホストに接続できません \(P. 521\)](#)

[queues.conf ファイルの JBoss エラー \(P. 522\)](#)

Tibco ユーザが Tibco サービスを開始できない

症状:

Tibco ユーザは Tibco サービスを開始できません。

解決方法:

以下の状態を確認します。

- Tibco ユーザはプライマリおよびセカンダリ エンタープライズ管理サーバ上に存在します。
- Tibco ユーザには、/shared/MessageQueue フォルダおよび /opt/CA/AccessControlServer/MessageQueue フォルダに対する rwx 権限があります。
- tibemsd.conf 内のストア値は、/shared/MessageQueue/data/datastore フォルダ内のデータ ストアにマップされます。
- ユーザ、グループ、トピック、キューおよびルートは /shared/MessageQueue/data フォルダにマップされます。

JCS がホストに接続できません

症状:

セカンダリ エンタープライズ管理サーバ上の JCS がホストに接続できません。

解決方法:

セカンダリ エンタープライズ管理サーバ上のインストールの後に JBoss を開始しないとこの問題が発生します。JCS 登録メッセージは期限切れになり、コネクタサーバは表示されません。

この問題を解決するには、プライマリ エンタープライズ管理サーバからコネクタサーバをコピーし、ホスト詳細を変更します。

queues.conf ファイルの JBoss エラー

症状:

queues.conf ファイルは以下のいずれかの JBoss エラー メッセージを表示します。

再接続に失敗しました

`javax.naming.NameNotFoundException`

解決方法:

これらのエラーが発生するのは、**queues.conf** ファイルが正しく設定されていない場合です。この問題を解決するには、**queues.conf** ファイルがプライマリおよびセカンダリ エンタープライズ管理サーバから共有されていることを確認します。

第 13 章: Disaster Recovery Deployment のインストール

このセクションには、以下のトピックが含まれています。

[ディザスタ リカバリの概要 \(P. 523\)](#)

[ディザスタ リカバリ展開をインストールする方法 \(P. 529\)](#)

[ディザスタ リカバリ プロセス \(P. 542\)](#)

[障害からの復旧方法 \(P. 547\)](#)

[メッセージキュー サーバ データ ファイルを同期する方法 \(P. 556\)](#)

ディザスタ リカバリの概要

サブシステムのクラッシュまたはその他の障害発生時に、ディザスタ リカバリによってユーザのシステムをリストアします。

ディザスタ リカバリの目的は、可能な限り多くのデータをリストアし、バックアップおよびリストアで必要なリソースを制限することです。

詳細情報:

[ディザスタ リカバリ \(P. 523\)](#)

[ディザスタ リカバリ アーキテクチャ \(P. 525\)](#)

[ディザスタ リカバリのコンポーネント \(P. 526\)](#)

[エンドポイント上のディザスタ リカバリの展開の仕組み \(P. 527\)](#)

ディザスタ リカバリ

ディザスタ リカバリ展開によって、壊滅的なシステム障害発生時に、エンタープライズ管理サーバのリストアをより容易に行うことができます。CA ControlMinder および SAM のエンドポイントが運用環境に接続できない場合、運用環境がリストアされるまで、エンドポイントはディザスタ リカバリ環境に接続します。

ディザスタリカバリの展開には、以下の利点があります。

- ディザスタリカバリ DMS のデータベースは運用環境 DMS のデータベースの複製です。これは、運用環境 DMS データベースが破損した場合に、ポリシーのコピーがあることを意味します。
- エンドポイントは運用環境またはディザスタリカバリ環境に接続できます。運用環境が停止した場合でも、エンドポイントはデータをディザスタリカバリ環境に送信するので、重大なシステム障害が発生した場合でも、ポリシーのステータスおよび偏差に関する情報は失われません。
- 障害復旧後、再度各エンドポイントをサブスクライブする必要はありません。

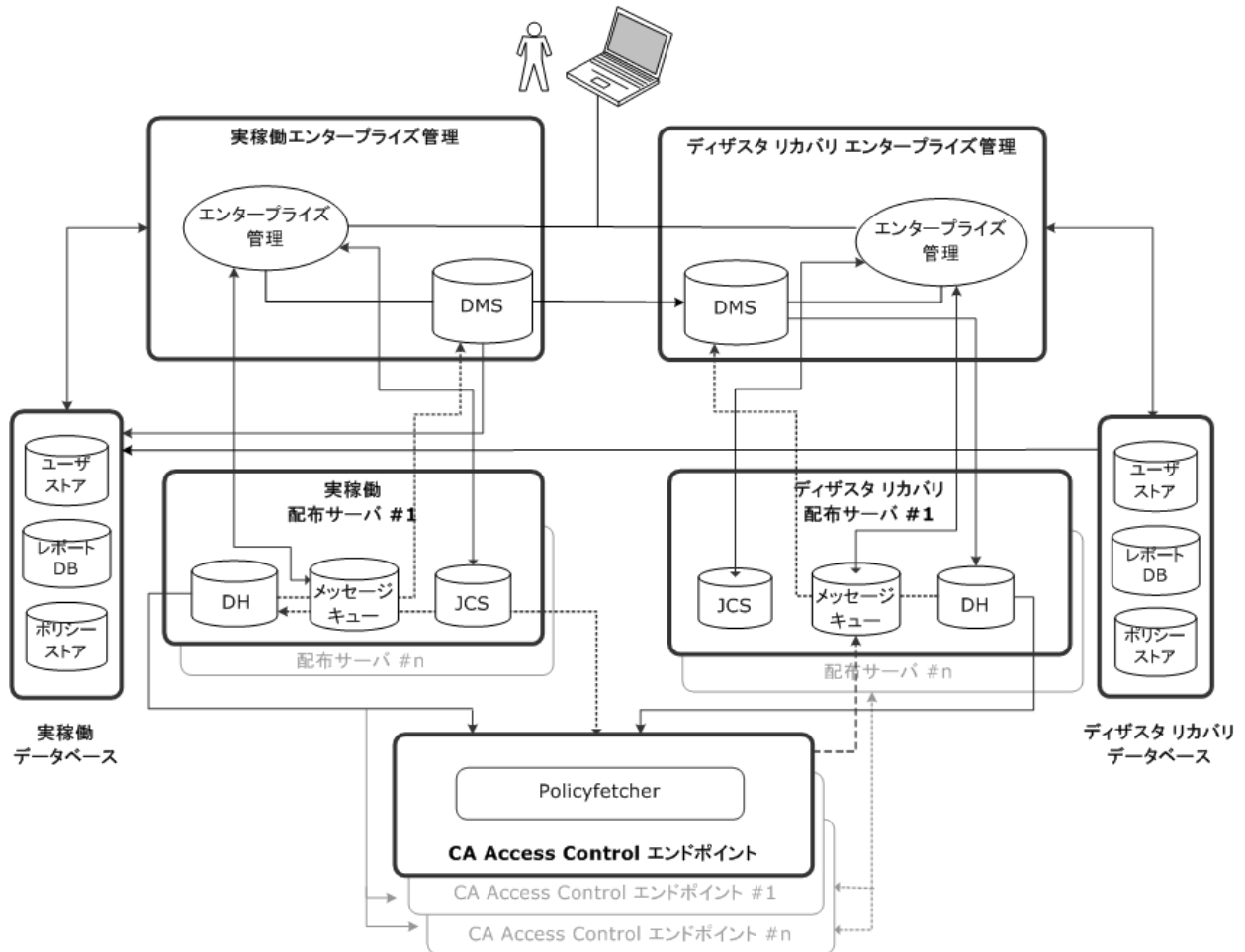
以下の CA ControlMinder コンポーネントは、ディザスタリカバリプロセス中にバックアップまたはリストアされません。これらのコンポーネントを別々にバックアップします。

- パスワードポリシー モデル
- PMDB
- RDBMS
- CA ControlMinder エンドポイント管理
- CA ControlMinder エンタープライズ管理
- エンドポイント上のデータ
- CA ControlMinder 監査ファイル
- CA ControlMinder エンドポイント
- レポート
- メッセージキュー
- CA Business Intelligence

注: DMS がバックアップされると、DMS 監査ファイルが保存されます。

ディザスタリカバリ アーキテクチャ

以下の図は、ディザスタリカバリ構成で、CA ControlMinder をどのように展開するかを示しています。



ディザスタリカバリのコンポーネント

ディザスタリカバリ構成に CA ControlMinder を展開するには、以下のコンポーネントが必要です。

- 運用環境の場合：
 - エンタープライズ管理サーバの 1 つのインストール
 - 中央データベース (RDBMS)
 - 配布サーバの 1 つ以上のインストール
- ディザスタリカバリ環境の場合：
 - エンタープライズ管理サーバの 1 つのインストール
 - 中央データベース (RDBMS)
 - 配布サーバの 1 つ以上のインストール

ディザスタリカバリの展開を計画する場合は、以下の点も考慮する必要があります。

- DMS はプラットフォーム、オペレーティング システム、CA ControlMinder のバージョンが同じ状態で保存されたバックアップ ファイルからでないとはリストアできません。たとえば、CA ControlMinder r12.0 SP1 を使用した DMS のバックアップ ファイルから CA ControlMinder r12.5 を使用して DMS をリストアすることはできません。
- お使いの RDBMS に対して、クラスタリングまたはその他のフェールオーバーソリューションをセットアップできます。
- 運用サーバとディザスタリカバリサーバの間で、RDBMS 内のデータを同期する必要があります。
- 運用サーバとディザスタリカバリサーバの間で、メッセージキュー データ ストアを同期する必要があります。

エンドポイント上のディザスタリカバリの展開の仕組み

ディザスタリカバリを展開すると、運用環境配布サーバデータベースの複製が作成され、エンドポイントから送信されたデータがシステム障害で失われないようになり、障害発生後の運用環境のリストアが容易になります。

以下のプロセスでは、エンドポイント上へのディザスタリカバリの展開の仕組みについて説明します。

1. 運用環境とディザスタリカバリの配布サーバのリストと照合して、作業するエンドポイントを設定します。
2. 指定された時間に、エンドポイントは運用環境内のエンタープライズ管理サーバへの接続を試行します。
 - a. エンドポイントは、リストの最初の運用環境配布サーバへの接続を試行します。接続できなかった場合、エンドポイントは、その配布サーバへの接続を指定された回数試行します。以下のいずれかのイベントが発生します。
 - エンドポイントは運用環境配布サーバに接続します。このステップで、プロセスが終了します。
 - エンドポイントは運用環境配布サーバに接続できません。プロセスは、ステップ b に移動します。

注: エンドポイントが配布サーバへの接続を試行する回数および接続先の配布サーバは、**communication** セクションの **Distribution_Server** 環境設定および **policyfetcher** セクションの **max_dh_command_retry** 環境設定で定義されます。

- b. エンドポイントは、リストの 2 番目の運用環境配布サーバへの接続を試行します。このように、リストに掲載されているサーバに順に（必要に応じて、定義されているのと同じ回数）接続を試行します。以下のいずれかのイベントが発生します。
 - エンドポイントは運用環境配布サーバに接続します。このステップで、プロセスが終了します。
 - エンドポイントはどの運用環境配布サーバにも接続できず、サイクルが終了します。プロセスは、ステップ 3 に移動します。

3. エンドポイントは、指定されたサイクル数、ステップ 2 を繰り返します。以下のいずれかのイベントが発生します。

- エンドポイントは運用環境配布サーバに接続します。このステップで、プロセスが終了します。
- エンドポイントは運用環境配布サーバに接続しません。プロセスは次のステップに移動します。

注: エンドポイントが配布サーバへの接続を試行する回数および接続先の配布サーバは、**communication** セクションの

Distribution_Server 環境設定および **policyfetcher** セクションの **max_dh_command_retry** 環境設定で定義されます。

4. エンドポイントは、リストの最初のディザスタリカバリ配布サーバへの接続を試行します。エンドポイントがこの配布サーバに接続できなかった場合、エンドポイントはリストの 2 番目のディザスタリカバリ配布サーバへの接続を試行します。エンドポイントがディザスタリカバリ配布サーバに接続するまで、それ以降、リストに掲載されているサーバに順に接続を試行します。

注: エンドポイントが運用環境またはディザスタリカバリの配布サーバに接続できない場合、エンドポイントは **DMS** にハートビートを送信しません。エンドポイントがオンラインかオフラインかどうかを決定するには、最後のハートビート通知が **DMS** にいつ送信されたかを確認します。

5. ディザスタリカバリ配布サーバに接続された後、エンドポイントでは継続して、運用環境配布サーバへの接続が試行されます。以下のいずれかのイベントが発生します。

- エンドポイントは運用環境配布サーバに接続し、運用環境に戻ります。
- エンドポイントは運用環境配布サーバに接続しません。エンドポイントはディザスタリカバリ環境に残り、ステップ 4 を繰り返します。

注: **policyfetcher** および通信セクションの詳細については、「リファレンスガイド」を参照してください。

ディザスタリカバリ展開をインストールする方法

ディザスタリカバリコンポーネントを相互に適切にサブスクライブしていることを確認するには、運用環境とディザスタリカバリのコンポーネントを、以下のプロセスで指定されている順番で設定する必要があります。

ディザスタリカバリを設定しておけば、重大なシステム障害発生時に、エンタープライズ管理サーバコンポーネントのリストアが容易になります。たとえば、中央データベース（RDBMS）など、他の CA ControlMinder コンポーネントを別々にバックアップする必要があるかもしれません。

重要: CA ControlMinder の別の運用環境またはバージョンを使用するバックアップファイルから、DMS をリストアできません。CA ControlMinder の同一のプラットフォーム、オペレーティングシステムおよびバージョン上に、運用環境とディザスタリカバリの環境が展開されていることを確認します。

注: このプロセスは、DMS と DH を別々のホストにインストールしたと想定しています。

以下のプロセスでは、ディザスタリカバリ展開をインストールする方法について説明します。

1. [運用環境エンタープライズ管理サーバのセットアップ](#) (P. 530)
2. [ディザスタリカバリ エンタープライズ管理サーバのセットアップ](#) (P. 532)
3. 運用サーバとディザスタリカバリサーバ間のデータベースレプリケーションの設定
4. [DMS サブスクリプションの設定](#) (P. 534)
5. [メッセージキューサーバデータファイルの同期](#) (P. 556)
6. [エンドポイントをセットアップします](#) (P. 535)。

注: RDBMS は、クラスタ、またはサイト間のデータ同期を許可する何らかの仕組み上にインストールすることをお勧めします。

運用環境 CA ControlMinder エンタープライズ管理 のセットアップ

運用環境エンタープライズ管理サーバには **DMS** が含まれています。 **DMS** は、各エンドポイントのポリシーバージョン、ポリシー スクリプトおよびポリシー デプロイメント ステータスに関する最新情報を格納します。運用環境 **DMS** を使用して、組織のポリシーをデプロイおよび管理します。

運用環境 **DHS** とディザスタリカバリ **DMS** は運用環境 **DMS** にサブスクライブしているので、他のディザスタリカバリ コンポーネントをセットアップする前に、運用環境 **DMS** をセットアップしてください。これによって、後にインストールプロセスで、サブスクリプションが正常に設定されるようになります。

運用環境エンタープライズ管理サーバのセットアップ方法

1. エンタープライズ管理サーバを実装します。

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA Access Control がインストールされます。

2. (オプション) [配布サーバを実装します](#) (P. 536)。

メッセージキューと Java 接続サーバがインストールされています。

3. (オプション) エンタープライズ管理サーバからローカル DH を削除し、配布サーバ上の DH を使用する場合、管理サーバと配布サーバの分離を維持するために、運用環境エンタープライズ管理サーバ上で以下のコマンドを実行します。

```
dmsmgr -remove -dh name  
-dh name
```

ローカル ホストで名前を指定した DH を削除します。

例: `dmsmgr -remove -dh DH`

上記の例では、DH という名の DH をホストから削除します。

運用環境 DMS はサブスクライバなしで作成されます。

4. フェールセーフ モードで動作するようにメッセージ キューを設定します。 以下の手順を実行します。
 - a. 以下のディレクトリに移動します。ここで、`ACServerInstallDir` は、エンタープライズ管理サーバをインストールしたディレクトリです。

```
ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
```

- b. `queues.conf` ファイルを編集できる形で開きます。
- c. 各キュー定義行の末尾に「**failsafe**」という単語を追加し、ファイルを保存して閉じます。

5. [ローカル DMS で CA ControlMinder エンタープライズ管理 を設定します](#) (P. 492)。

運用環境エンタープライズ管理サーバをインストールし設定しています。これで、ディザスタリカバリ エンタープライズ管理サーバを設定できるようになりました。

例: queues.conf ファイルの編集

queues.conf ファイルの以下のスニペットは、共有ストレージを使用するようメッセージキューを設定するために、ファイルを変更する方法について例を示しています。

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

ディザスタリカバリ CA ControlMinder エンタープライズ管理 のセットアップ

ディザスタリカバリのエンタープライズ管理サーバでは、破滅的なシステム障害の場合にユーザの企業ポリシーがデプロイされ管理されます。ディザスタリカバリのエンタープライズ管理サーバは運用環境エンタープライズ管理サーバのサブスクリバであるため、そのデータベースには、運用環境エンタープライズ管理サーバと同じ、ポリシーバージョン、ポリシースクリプト、およびエンドポイントデプロイメントステータスに関する情報が含まれています。

注: ディザスタリカバリのエンタープライズ管理サーバをセットアップする前に、運用環境エンタープライズ管理サーバを設定します。

ディザスタリカバリのエンタープライズ管理サーバのセットアップ方法

1. FIPsKey.dat ファイルを運用環境エンタープライズ管理サーバからディザスタリカバリサーバにコピーします。このファイルは以下のディレクトリ内にあります。ここで、JBoss_HOME は JBoss をインストールしたディレクトリを示します。

```
JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys
```

2. ディザスタリカバリサーバ上にエンタープライズ管理サーバを実装します。

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA Access Control がインストールされます。

重要: インストールプロセスの開始時に、運用環境エンタープライズ管理サーバからコピーした FIPsKey.dat ファイルを指定します。例:

```
E:%EnterpriseMgmt%Disk1%InstData%NoVM%install_EntM_r125.exe
-DFIPS_KEY=C:%tmp%FIPskey.dat
```

3. (オプション) [ディザスタリカバリ配布サーバを実装します \(P. 540\)](#)。
メッセージキューと Java 接続サーバがインストールされています。

4. (オプション) ローカル DH を削除し、配布サーバ上の DH を使用する
場合、管理サーバと配布サーバの分離を維持するために、ディザスタ
リカバリ エンタープライズ管理サーバ上で以下のコマンドを実行し
ます。

```
dmsmgr -remove -dh name
```

```
-dh name
```

ローカル ホストで名前を指定した DH を削除します。

例: `dmsmgr -remove -dh DH`

ディザスタリカバリ DMS はサブスクライバなしで作成されます。

5. フェールセーフ モードで動作するようにメッセージキューを設定し
ます。以下の手順を実行します。

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

```
ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
```

- b. `queues.conf` ファイルを編集できる形で開きます。

- c. 各キュー定義行の末尾に「**failsafe**」という単語を追加し、ファ
イルを保存して閉じます。

6. [ローカル DMS で CA ControlMinder エンタープライズ管理を設定しま
す \(P. 492\)](#)。

ディザスタリカバリ エンタープライズ管理サーバをインストールし設定
しています。

例: `queues.conf` ファイルの編集

`queues.conf` ファイルの以下のスニペットは、共有ストレージを使用する
ようメッセージキューを設定するために、ファイルを変更する方法につ
いて例を示しています。

```
queue/snapshots secure,store=$sys.failsafe
queue/audit secure,store=$sys.failsafe
ac_endpoint_to_server secure,store=$sys.failsafe
ac_server_to_endpoint secure,store=$sys.failsafe
```

DMS サブスクリプションの設定

ディザスタリカバリ エンタープライズ管理サーバは、運用環境エンタープライズ管理サーバのサブスクリバです。そのため、そのデータベースには、運用環境エンタープライズ管理サーバと同じポリシーバージョン、ポリシースクリプトおよびエンドポイント展開ステータスに関する情報が含まれています。

2つのデータベースを同期するために、ディザスタリカバリ エンタープライズ管理サーバのデータベースを運用環境エンタープライズ管理サーバのサブスクリバとして設定します。

DMS サブスクリプションの設定方法

1. ディザスタリカバリ エンタープライズ管理サーバに移動します。
2. 運用環境エンタープライズ管理サーバをディザスタリカバリ エンタープライズ管理サーバの親として定義します。以下のコマンドを実行します。

```
env pmd  
subs drpmd_name parentpmd(<pr_dms_pmdname>@pr_host)  
drpmd_name
```

ディザスタリカバリ PMDB の名前を定義します。

3. 運用環境エンタープライズ管理サーバに移動します。
4. 以下のコマンドを実行します。

```
sepmc -n prDMS_name drDMS_name  
prDMS_name
```

運用環境 DMS の名前を定義します。

```
drDMS_name
```

ディザスタリカバリ DMS の名前を定義します。ディザスタリカバリ DMS は、「*drDMS_name@hostname*」形式で指定します。

ディザスタリカバリのエンタープライズ管理サーバは運用環境エンタープライズ管理サーバにサブスクライブされ、同期されます。

エンドポイントのセットアップ

エンタープライズ管理サーバを運用環境とディザスタリカバリ環境にインストールすると、運用環境サーバとディザスタリカバリサーバのコンポーネントを操作するために、エンタープライズネットワーク内の各エンドポイントを設定する必要があります。その際、サーバコンポーネントとの間で情報の送信先および受信元として機能するエンドポイントを設定します。

注: インストールプロセスの一部として、拡張ポリシー管理サーバコンポーネントのホスト名を指定します。以下の形式で、運用環境 DH の名前を入力します。 `prDH_name@hostname[, prDH_name@hostname..]`

エンドポイントのセットアップ方法

1. 拡張ポリシー管理クライアントコンポーネントを有効にした状態で、CA ControlMinder エンドポイント機能をエンドポイントホストにインストールします。

CA ControlMinder エンドポイント機能性はホストにインストールされます。また、エンドポイントは運用環境 DH にサブスクライブします。

2. エンドポイントで **selang** コマンド ウィンドウを開きます。
3. 以下のコマンドを入力します。

```
so dh_dr+(drDH_name[, drDH_name...])
```

drDH_name

ディザスタリカバリ DH の名前を定義します。形式：
drDH_name@hostname。

エンドポイントはディザスタリカバリ DH にサブスクライブします。

4. 運用環境とディザスタリカバリの配布サーバの URL のリストを指定します。

- UNIX : **accommon.ini** ファイルの [通信] セクション内の **Distribution_Server** パラメータを変更します。
- Windows : Windows レジストリで **Distribution_Server** 値を変更します。このパラメータは以下にあります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication
```

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

注: または、指定された **selang** コマンドでポリシーを作成し、それをエンドポイントにデプロイして、エンドポイントをディザスタリカバリ DH にサブスクライブできます。ポリシーの作成とデプロイの詳細については、「エンタープライズ管理ガイド」を参照してください。

ディザスタリカバリ展開をインストールするための追加情報

以下のトピックでは、ディザスタリカバリ展開をインストールするために実行する必要がある場合がある追加の設定手順について説明します。

配布サーバのインストール

ディザスタリカバリ環境またはハイアベイラビリティ環境で動作するように **CA ControlMinder** を設定する場合、配布サーバを別々のコンピュータにインストールし、その間でファイルが伝達されるように配布サーバを設定します。

配布サーバのインストール方法

1. お使いのオペレーティング システム用の適切な CA ControlMinder サーバ コンポーネント DVD を光ディスク ドライブに挿入します。
2. 以下のいずれかの操作を行います。

- Windows の場合

autorun が有効になっている場合は、Product Explorer が自動的に表示されます。以下の手順を実行します。

- a. Product Explorer が表示されない場合は、光ディスク ドライブのディレクトリに移動し、ProductExplorerox86.EXE ファイルをダブルクリックします。
- b. Product Explorer で [Components] フォルダを展開し、CA ControlMinder 配布サーバを選択して、[インストール] をクリックします。

InstallAnywhere インストール プログラムが起動します。

- UNIX の場合

- a. 光ディスク ドライブをマウントします。
- b. ターミナル ウィンドウを開き、光ディスク ドライブ上の以下のディレクトリに移動します。

`/DistServer/Disk1/InstData/NoVM`

- c. 以下のコマンドを実行します。

```
./install_DistServer.bin -i console
```

InstallAnywhere インストール プログラムが起動します。

3. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

メッセージ キュー設定

メッセージ キュー サーバの管理者パスワード（通信パスワード）を定義します。

制限：最低 6 文字

Java コネクタ サーバ - プロビジョニング ディレクトリ情報

Java コネクタ サーバ用のパスワードを定義します。

注: Java コネクタ サーバは、CA ControlMinder エンタープライズ管理に特権アカウント管理機能を提供します。

CA ControlMinder 配布サーバのインストールが完了します。

注: ディザスタ リカバリの実装の一部として配布サーバをインストールする場合は、追加の手順を完了する必要があります。

詳細情報:

[運用環境配布サーバのセットアップ](#) (P. 538)

[ディザスタ リカバリ配布サーバのセットアップ](#) (P. 540)

運用環境配布サーバのセットアップ

運用環境配布サーバには、DH が含まれています。DH は、運用環境 DMS で作成されたポリシー デプロイメントをエンドポイントに配布し、デプロイメント ステータスの更新をエンドポイントから受け取って、運用環境 DMS に送ります。

運用環境 DHS とディザスタ リカバリ DMS は運用環境 DMS にサブスクライブしているので、他のディザスタ リカバリ コンポーネントをセットアップする前に、運用環境 DMS をセットアップしてください。これによって、後にインストール プロセスで、サブスクリプションが正常に設定されるようになります。

運用環境配布サーバのセットアップ方法

1. [配布サーバを運用環境配布サーバ コンピュータにインストールします](#) (P. 536)。
2. 運用環境配布サーバ上で以下のコマンドを実行して、DH を設定します。

```
dmsmgr -remove -auto
```

```
dmsmgr -create -dh name -parent name%  
[-admin user[,user...]] [-desktop host[,host...]]
```

-dh name

ローカル ホストに指定した名前で DH を作成します。

-parent name

DH がエンドポイント通知を送る先の運用環境 DMS を定義します。
運用環境 DMS を「*DMS_name@hostname*」の形式で指定します。

-admin user[,user...]

(オプション) 作成される DH の管理者として、内部ユーザを定義します。

-desktop host[,host...]

(オプション) 作成された DH があるコンピュータに対して
TERMINAL アクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、常に作成された DH に対する管理権限が与えられます。

これで、運用環境 DH が作成および設定されました。

3. 以下のコマンドを実行します。

```
sepmc -n prDMS_name prDH_name
```

prDMS_name

運用環境 DMS の名前を定義します。

prDH_name

運用環境 DHs の名前を定義します。名前は、
「*DMS_name@hostname*」という形式で指定します。

例: *DH__@prdh.com*

DH は運用環境 DMS にサブスクライブし、同期されます。

4. 配布サーバと運用環境 DMS の間をルーティングするメッセージキューをセットアップします。
5. 各運用環境配布サーバについて、ステップ 1-4 を繰り返します。

ディザスタリカバリ配布サーバのセットアップ

ディザスタリカバリ配布サーバは運用環境配布サーバのサブスクライバであるため、そのデータベースには、運用環境配布サーバと同じ、ポリシーバージョン、ポリシースクリプト、およびエンドポイントデプロイメントステータスに関する情報が含まれています。

注: ディザスタリカバリ配布サーバをセットアップする前に、運用環境配布サーバをセットアップする必要があります。

ディザスタリカバリ配布サーバのセットアップ方法

1. [配布サーバ](#) (P. 536) をディザスタリカバリ配布サーバコンピュータにインストールします。
2. ディザスタリカバリ配布サーバ上で以下のコマンドを実行して、DHを設定します。

```
dmsmgr -remove -auto
```

```
dmsmgr -create -dh name -parent name%  
[-admin user[,user...]] [-admin user[,user...]]
```

-dh name

ローカルホストに指定した名前でDHを作成します。

-parent name

DHがエンドポイント通知を送る先のディザスタリカバリDMSを定義します。ディザスタリカバリDMSは、「drDMS_name@hostname」形式で指定します。

-admin user [,user...]

(オプション) 作成されるDHの管理者として、内部ユーザを定義します。

-desktop host[,host...]

(オプション) 作成されたDHがあるコンピュータに対してTERMINALアクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、常に作成されたDHに対する管理権限が与えられます。

これで、ディザスタリカバリDHが作成および設定されました。

3. ディザスタリカバリ配布サーバ上で、以下のコマンドを実行します。

```
sepmc -n drDMS_name drDH_name
```

drDMS_name

ディザスタリカバリDMSの名前を定義します。

drDH_name

ディザスタリカバリDHの名前を定義します。名前は、「drDH_name@hostname」という形式で指定します。

例: DH__@drdh.com

DHはディザスタリカバリDMSにサブスクライブし、同期されます。

4. 配布サーバとディザスタリカバリ DMS の間をルーティングするメッセージキューをセットアップします。
5. 各ディザスタリカバリ配布サーバについて、ステップ 1-4 を繰り返します。

ディザスタリカバリプロセス

ディザスタリカバリプロセスには、「バックアップ」と「リストア」の 2 つの段階があります。バックアップ段階では、DMS データベース内のデータは別のディレクトリにコピーされます。リストア段階では、dmsgmr ユーティリティは、バックアップ DMS ファイルを使用して既存の DMS をリストアするか、または DMS を作成します。

注: ディザスタリカバリ設定を使用すると、重大なシステム障害の発生時に拡張ポリシー管理コンポーネントをより容易に復元できます。他の CA ControlMinder コンポーネントの個別バックアップが必要な場合もあります。

詳細情報:

[リストアできるデータ](#) (P. 543)

[DMS をリストアする場合](#) (P. 544)

[DH をリストアする場合](#) (P. 544)

[DMS のリストア方法](#) (P. 545)

[DH のリストア方法](#) (P. 546)

リストアできるデータ

DMS をリストアする場合、dmsmgr は、別の DMS のバックアップ ファイルを使用して新しい DMS を作成します。DH をリストアする場合、dmsmgr は DMS バックアップ ファイルのデータを DH リーダ ディレクトリにコピーします。いずれの場合も、同じデータをリストアします。

リストアするデータは DMS データベース内のデータの複製で、その内容は以下のとおりです。

- ユーザの組織のポリシー、バージョンおよび割り当てに関する情報
- デプロイメントおよびポリシー ステータス、デプロイメント偏差およびデプロイメント階層に関する情報
- ホストとホスト グループの定義
- 設定
- updates.dat ファイル
- レジストリ エントリ
- DMS 監査ファイル

注: DH__Writer は一時的なデータベースであるため、リストアする必要はありません。

DMS をリストアする場合

DMS をリストアする場合、`dmsmgr` は、別の DMS のバックアップ ファイルを使用して新しい DMS を作成します。以下のシナリオは、運用環境 DMS をリストアする場合です。

- 運用環境システムに致命的な障害が発生している。
- 運用環境 DMS データベースが破損している。
- 新しい運用環境 DMS を別のホストにセットアップする必要がある。

以下のシナリオは、ディザスタ リカバリ DMS をリストアする場合です。

- ディザスタ リカバリ DMS が運用環境 DMS と同期していない。
- ディザスタ リカバリ DMS データベースが破損している。
- 新しいディザスタ リカバリ DMS を別のホストにセットアップする必要がある。

注: DMS は、既存の DMS 上に、または DMS が存在しない新規ディレクトリにリストアできます。

DH をリストアする場合

DH をリストアする場合、`dmsmgr` は DMS バックアップ ファイルのデータを DH リーダ ディレクトリにコピーします。以下のシナリオは、DH をリストアする場合です。

- 運用環境システムに致命的な障害が発生している。
- DH データベースが壊れている。
- DH が DMS と同期していない。
- 新しい DH を異なるホストにセットアップする必要がある。

注: DH ライタは一時的なデータベースであるため、リストアする必要はありません。DH をリストアする前に、DH ライタが既存の DH ファイル構造に存在していることを確認してください。

DMS のリストア方法

`dmsmgr` ユーティリティがどのように **DMS** をリストアするか理解することは、リストア プロセスで発生する可能性がある問題の診断に役立ちます。

以下のプロセスでは、`dmsmgr` で **DMS** をリストアする方法について説明します。

1. `dmsmgr` は既存の **DMS** を削除します。
2. `dmsmgr` は、**DMS** のバックアップ ファイルを、指定した場所から **DMS** ディレクトリにコピーします。
3. `dmsmgr` は、**DMS** のすべてのサブスクライバを削除します。
4. 以下のいずれかのイベントが発生します。
 - 運用環境 **DMS** をリストアすると、`dmsmgr` は、バックアップ ファイルに格納されている最後のグローバル オフセットと同じオフセット値で、ディザスタリカバリ **DMS** を、その最初のサブスクライバとして、運用環境 **DMS** に追加します。
 - 惨事復旧 **DMS** をリストアすると、`dmsmgr` は、バックアップ ファイルに格納されている最後のグローバル オフセットと同じオフセット値で、ディザスタリカバリ **DMS** を運用環境 **DMS** に再サブスクライブします。
5. `dmsmgr` は各 **DH** を **DMS** にサブスクライブします。各 **DH** は、オフセット値 0 および非同期ステータスを持っています。

注: 同期してない場合、**DH** は **DMS** から更新を受け取れません。非同期ステータスから **DH** を解放するには、**DH** をリストアします。

DH のリストア方法

dmsmgr ユーティリティがどのように DH をリストアするか理解することは、リストアプロセスで発生する可能性がある問題の診断に役立ちます。

以下のプロセスでは、dmsmgr で DH をリストアする方法について説明します。

1. dmsmgr は既存の DH を削除します。
2. dmsmgr は、DH のバックアップ ファイルを、指定した場所から DH ディレクトリにコピーします。
3. dmsmgr は、バックアップ ファイルに格納された最後のグローバル オフセットと等しいオフセット値を持つ DMS に DH をサブスクライブします。
4. dmsmgr は、DH 上の非同期フラグをクリアします。

オフセット値

updates.dat ファイルには、DMS がデプロイする各コマンドが格納されます。新しいサブスクライバを作成するときに、Policy Model は updates.dat ファイル内のコマンドをサブスクライバに送信します。各コマンドには、オフセット値という増分番号がインデックス付けされます。

DMS にサブスクライバを追加するときには、以下のオフセットを指定できます。

- **0** - Policy Model はすべてのコマンドをサブスクライバに送信します。
- **最後のオフセット** - Policy Model はコマンドをサブスクライバに送信しません。
- **0 と最後のオフセットの間の整数 X** - Policy Model は X から最後のオフセットまでのすべてのコマンドをサブスクライバに送信します。

非同期サブスクリバ

非同期サブスクリバとは、`updates.dat` ファイルが前回切り捨てられてから、更新を一切受け取っていないサブスクリバです。サブスクリバに非同期フラグを立てると、CA ControlMinder はそのサブスクリバを無視し、そのサブスクリバにコマンドが一切送られなくなります。

非同期サブスクリバは、その親 DMS または Policy Model から、更新を一切受け取りません。非同期フラグをクリアし、サブスクリバが更新を受け取るようにするには、サブスクリバをその親に再サブスクリブする必要があります。

親 DMS または Policy Model のサブスクリバがすべて非同期の場合、親には実質的にサブスクリバがないことになります。

障害からの復旧方法

運用システムに障害が発生した場合、エンドポイントはディザスタ リカバリ環境に対して機能します。障害から復旧する際、ディザスタ リカバリ環境からリストアした運用環境に操作を戻します。

以下のプロセスは、障害から復旧する方法について説明します。

1. 運用環境のエンタープライズ管理サーバと運用環境の配布サーバで CA ControlMinder を停止します。
2. ディザスタ リカバリ DMS に対するすべての管理作業を停止します。つまり、CA ControlMinder エンタープライズ管理 と `policydeploy` ユーティリティを停止します。
3. (オプション) `updates.dat` ファイルの自動切り捨てを実行します。
4. ディザスタ リカバリ DMS をバックアップします。DMS は、以下のいずれかの方法でバックアップできます。
 - [ローカルバックアップ](#) (P. 549)
 - [リモートバックアップ](#) (P. 550)
5. 運用環境のデータベース (RDBMS) のリストア
6. ディザスタ リカバリ DMS のバックアップファイルから [運用環境の DMS をリストアします](#) (P. 553)。
7. 運用環境の DMS で CA ControlMinder を開始します。

8. 運用環境の DMS をバックアップできます。DMS のバックアップは、以下のいずれかの方法で行うことができます。
 - [ローカルバックアップ](#) (P. 549)
 - [リモートバックアップ](#) (P. 550)
9. 運用環境の DMS のバックアップファイルから[各運用環境の DH をリストアします](#) (P. 552)。
10. 各運用環境の配布サーバ上で CA ControlMinder を開始します。
11. すべての管理作業を運用環境の DMS に移動します。つまり、運用環境の CA ControlMinder エンタープライズ管理 で、CA ControlMinder エンタープライズ管理 と policydeploy ユーティリティを開始します。
12. (オプション) ディザスタ リカバリ DMS が運用環境の DMS と同期していない場合は、以下の手順を完了します。
 - a. 運用環境の DMS のバックアップファイルから[ディザスタ リカバリ DMS をリストアします](#) (P. 554)。
 - b. ディザスタ リカバリ DMS をバックアップできます。DMS のバックアップは、以下のいずれかの方法で行うことができます。
 - [sepmid ユーティリティ](#) (P. 549)
 - [selang のコマンド](#) (P. 550)
 - c. ディザスタ リカバリ DMS のバックアップファイルから[各ディザスタ リカバリ DH をリストア](#) (P. 552)します。

sempd を使用した DMS のバックアップ

DMS をバックアップして、エンドポイントにデプロイしたポリシー、およびエンタープライズ管理サーバがエンドポイントから受け取ったレポートスナップショットを保存します。

DMS のバックアップでは、DMS データベースのデータを指定したディレクトリにコピーします。

sempd ユーティリティは、ローカル ホストにのみ DMS をバックアップします。DMS のバックアップ ファイルは、安全な場所、できれば CA ControlMinder アクセス ルールで保護された場所に保存してください。DMS をバックアップする前に、updates.dat ファイルの自動切り捨てを実行することが推奨されます。

注: DMS は selang コマンドを使ってローカル ホストまたはリモート ホストにバックアップすることもできます。

sempd を使用して DMS をバックアップする方法

1. 以下のコマンドを使用して、DMS をロックします。

```
sempd -bl dms_name
```

DMS はロックされるため、サブスクライバにコマンドを送信できなくなります。

2. 以下のコマンドを使用して、DMS データベースをバックアップします。

```
sepmc -bd dms_name [destination_directory]
```

dms_name

ローカル ホストにバックアップする DMS の名前を定義します。

destination_directory

DMS のバックアップ先ディレクトリを定義します。

デフォルト: (UNIX) *ACInstallDir/data/policies_backup/dmsName*

デフォルト: (Windows)

ACInstallDir\data\policies_backup\dmsName

DMS データベースを宛先ディレクトリにバックアップします。

3. 以下のコマンドを使って、DMS のロックを解除します。

```
sepmc -ul dms_name
```

DMS はロックが解除されるため、サブスクライバにコマンドを送信できるようになります。

selang を使用した DMS のバックアップ

DMS のバックアップでは、データを DMS データベースから指定したディレクトリにコピーします。

DMS は *selang* コマンドを使ってローカル ホスト、またはリモート ホストにバックアップできます。DMS のバックアップ ファイルは、安全な場所、できれば CA ControlMinder アクセスルールで保護された場所に保存してください。DMS をバックアップする前に、*updates.dat* ファイルの自動切り捨てを実行することが推奨されます。

注: ローカル ホストに DMS をバックアップする場合は、*sepmc* ユーティリティも使用できます。

selang を使用して DMS をバックアップする方法

1. (オプション) *selang* を使用してリモート ホストから DMS に接続している場合は、以下のコマンドを使って DMS ホストに接続します。

```
host dms_host_name
```

2. 以下のコマンドを使用して、PMD 環境に移動します。

```
env pmc
```

3. 以下のコマンドを使用して、DMS をロックします。

```
pmd dms_name lock
```

DMS はロックされるため、サブスクリバにコマンドを送信できなくなります。

4. 以下のコマンドを使用して、DMS データベースをバックアップします。

```
backuppmd dms_name [destination(destination_directory)]
```

dms_name

ローカル ホストにバックアップする DMS の名前を定義します。

destination(*destination_directory*)

DMS のバックアップ先ディレクトリを定義します。

デフォルト: (UNIX) *ACInstallDir/data/policies_backup/dmsName*

デフォルト: (Windows)

ACInstallDir¥data¥policies_backup¥dmsName

DMS データベースを宛先ディレクトリにバックアップします。

5. 以下のコマンドを使って、DMS のロックを解除します。

```
pmd dms_name unlock
```

DMS はロックが解除されるため、サブスクリバにコマンドを送信できるようになります。

DH のリストア

dmsmgr ユーティリティを使用して、データを **DMS** バックアップ ファイルから **DH_Reader** ディレクトリにコピーして、**DH** をリストアします。**DH** ライタをリストアする必要はありません。これは、そのデータベースが一時的なものであるためです。**DH** をリストアする前に、**DH** ライタが既存の **DH** ファイル構造に存在していることを確認してください。

注: **DH** ライタが既存の **DH** ファイル構造にない場合、または新しい **DH** をセットアップする場合は、**DH** をリストアする前に、**dmsmgr-create** 機能を使用して新しい **DH** を作成します。

注: **dmsmgr** ユーティリティを使用するには、オペレーティング システムへの完全な管理アクセス権が必要です。

DH をリストアするには、**DH** ホストで以下のコマンドを実行します。

```
dmsmgr -restore -dh name -source path -parent name%  
[-admin user[,user...]] [-xadmin user[,user...]] [-desktop host[, host...]]
```

-admin user[,user...]

(UNIX) リストアされる **DMS** または **DH** の管理者として内部ユーザを指定します。

-desktop host[, host...]

(オプション) リストアする **DH** があるコンピュータに対して **TERMINAL** アクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、リストアする **DH** に対する管理権限が常に与えられます。

-dh name

ローカル ホストにリストアする **DH** の名前を定義します。

-parent name

リストアされた **DH** がサブスクライブする親 **DMS** の名前を定義します。親 **DMS** は「**DMS_name@hostname**」という形式で指定します。

-source path

リストアするバックアップ ファイルが存在するディレクトリを定義します。

`-xadmin user[,user...]`

(UNIX) リストアされる DMS または DH の管理者としてエンタープライズ ユーザを定義します。

DH がリストアされて、DMS にサブスクライブされます。

運用環境の DMS のリストア

運用環境の DMS のリストア時、`dmsmgr` はディザスタ リカバリ DMS バックアップ ファイルから運用環境の DMS にデータをコピーします。

注: `dmsmgr` ユーティリティを使用するには、オペレーティング システムへの完全な管理アクセス権が必要です。

運用環境の DMS をリストアするには、運用環境の DMS ホストで以下のコマンドを実行します。

```
dmsmgr -restore -dms name -source path -replica name¥  
[-subscriber dhname[,dhname...]] [-admin user[,user...]]¥  
[-xadmin user[,user...]]
```

`-admin user[,user...]`

(UNIX) リストアされる DMS または DH の管理者として内部ユーザを指定します。

`-dms name`

ローカル ホストにリストアする DMS の名前を定義します。

`-replica name`

運用環境の DMS にサブスクライブするディザスタ リカバリ DMS の名前を定義します。ディザスタ リカバリ DMS は「**DMS 名@ホスト名**」形式で指定します。

`-subscriber dh_name[, dh_name...]`

(オプション) リストアされる DMS がポリシーの更新を送信する DH のリストをカンマ区切りで定義します。各 DH は **DH_name@hostname** という形式で指定します。

-source path

リストアするバックアップファイルが存在するディレクトリを定義します。

-xadmin user[,user...]

(UNIX) リストアされる DMS または DH の管理者としてエンタープライズ ユーザを定義します。

運用環境の DMS がリストアされます。

注: 運用環境の DMS をリストアした後は、運用環境の DMS をバックアップし、そのバックアップファイルから運用環境の DH をリストアする必要があります。これにより、運用環境の DMS と DH が同期されます。

ディザスタリカバリ DMS のリストア

ディザスタリカバリ DMS のリストア時、**dmsmgr** はバックアップファイルのデータをディザスタリカバリ DMS ディレクトリにコピーします。

注: **dmsmgr** ユーティリティを使用するには、オペレーティングシステムへの完全な管理アクセス権が必要です。

ディザスタリカバリ DMS をリストアするには、ディザスタリカバリ DMS ホストで以下のコマンドを実行します。

```
dmsmgr -restore -dms name -source path -parent name%  
[-subscriber dhname[,dhname...]] [-admin user[,user...]]%  
[-xadmin user[,user...]]
```

-admin user[,user...]

(UNIX) リストアされる DMS または DH の管理者として内部ユーザを指定します。

-dms name

ローカルホストにリストアする DMS の名前を定義します。

-parent name

リストアされたディザスタリカバリ DMS がサブスクライブする運用環境の DMS の名前を定義します。運用環境の DMS は **DMS_name@hostname** のフォーマットで指定します。

-source *path*

リストアするバックアップファイルが存在するディレクトリを定義します。

-subscriber *dh_name*[, *dh_name*...]

(オプション) リストアされる DMS がポリシーの更新を送信する DH のリストをカンマ区切りで定義します。各 DH は *DH_name@hostname* という形式で指定します。

-xadmin *user*[,*user*...]

(UNIX) リストアされる DMS または DH の管理者としてエンタープライズユーザを定義します。

ディザスタリカバリ DMS がリストアされて、運用環境の DMS にサブスクライブされます。

注: ディザスタリカバリ DMS をリストアした後は、ディザスタリカバリ DMS をバックアップし、そのバックアップファイルからディザスタリカバリ DH をリストアする必要があります。これにより、ディザスタリカバリ DMS と DH が確実に同期されます。

メッセージキューサーバのデータファイルのバックアップ

メッセージキューサーバのデータファイルをバックアップして、データを運用メッセージキューサーバからディザスタリカバリメッセージキューサーバにコピーします。

メッセージキューサーバのデータファイルをバックアップするには、メッセージキューサーバのデータファイルを運用配布サーバからディザスタリカバリ配布サーバにコピーします。デフォルトで、データファイルは以下のディレクトリにあります。ここで、「*ACServerInstallDir*」はメッセージキューサーバのインストール先ディレクトリです。

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

メッセージ キュー サーバのデータ ファイルのリストア

メッセージ キュー サーバのデータ ファイルをリストアして、データをディザスタ リカバリ メッセージ キュー サーバから運用メッセージ キュー サーバにコピーします。

メッセージ キュー サーバのデータ ファイルをリストアするには、メッセージ キュー サーバ データ ファイルをディザスタ リカバリ 配布サーバから運用配布サーバにコピーします。デフォルトで、データ ファイルは以下のディレクトリにあります。ここで、「*ACServerInstallDir*」はメッセージ キュー サーバのインストール先ディレクトリです。

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

メッセージ キュー サーバ データ ファイルを同期する方法

ディザスタ リカバリ環境で作業を行う場合、運用メッセージ キュー サーバとディザスタ リカバリ メッセージ キュー サーバを同期することが非常に重要になります。サーバを同期することによって、運用およびディザスタ リカバリの両方のメッセージ キュー サーバ上のデータが更新されることを容易に確認でき、運用サーバが停止した場合、ディザスタ リカバリ サーバが中断なく継続してデータを提供できます。

注: この同期ソリューションは、サードパーティーのレプリケーションツールをベースにしています。ストレージソリューションによって、データブロックがデータ バッファに書き込まれたのと同じ順番で共有ストレージに書き込まれることを確認します。同期書き込みコールへの返答を受け取るとすぐに、ストレージソリューションによってすべてのデータが耐久性のある、持続的なストレージに書き込まれるのを確認します。

メッセージ キュー サーバのデータ ファイルを同期するには、以下を実行します。

1. 運用環境配布サーバ上で、メッセージ キュー サーバとエンタープライズ管理サーバにインストールされているすべてのメッセージ キュー サーバの間でメッセージルーティング設定をセットアップします。
2. ディザスタ リカバリ配布サーバ上のメッセージ キュー サーバとディザスタ リカバリのエンタープライズ管理サーバの間で、メッセージルーティング設定をセットアップします。

3. エンタープライズ管理サーバ上のディザスタリカバリおよび運用環境のメッセージキューサーバの両方で `queues.conf` ファイルを変更し、「fail-safe」行を追加します。

以下に例を示します。

```
queue/snapshots secure,failsafe
queue/audit secure, failsafe
ac_endpoint_to_server secure, failsafe
ac_server_to_endpoint secure,failsafe
```

デフォルトで、このファイルは以下のディレクトリにあります。ここで、「`ACServerInstallDir`」はエンタープライズ管理サーバのインストール先ディレクトリです。

`ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data`

4. サードパーティのレプリケーション ツールを使用して、エンタープライズ管理サーバ上の運用環境メッセージキューサーバの **EMS** データ ファイルを、ディザスタリカバリのエンタープライズ管理サーバ上のメッセージキューサーバに複製します。

デフォルトで、メッセージキューサーバの **EMS** データ ファイルは、以下のディレクトリにあります。ここで、「`ACServerInstallDir`」はエンタープライズ管理サーバのインストール先ディレクトリです。

`ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore`

メッセージキューサーバの **EMS** データ ファイル同期設定を設定しました。

付録 B: 通信の暗号方式の変更

このセクションには、以下のトピックが含まれています。

[通信の暗号化](#) (P. 559)

[対称暗号化](#) (P. 560)

[SSL、認証、および証明書](#) (P. 565)

[レポート ポータル用の Windows 認証設定](#) (P. 590)

通信の暗号化

CA ControlMinder コンポーネント間の通信の暗号化、および CA ControlMinder クライアント/サーバ通信の暗号化には、以下の方法を使用できます。

- 対称暗号化
- SSL

注: Windows では、暗号化モードを変更したときに（たとえば、FIPS 専用モードに変更）、パスワード PMDB からパスワードを送信する必要がある場合は、CA ControlMinder サービスを再起動します。

対称暗号化

CA ControlMinder は、暗号化ライブラリを使用して対称（標準）暗号化を実装します。CA ControlMinder コンポーネント間の通信の暗号化には以下の方法を使用できます。

- デフォルト（専用）暗号化
- AES128
- AES192
- AES256
- DES
- 3DES

注：「デフォルト」という名前の暗号方式は、CA ControlMinder のデフォルトの暗号化方式ではありません。デフォルトの暗号化方式は AES256 です。

CA ControlMinder をインストールすると、インストーラは暗号化ライブラリを以下のディレクトリに格納します。ACInstallDir は CA ControlMinder をインストールしたディレクトリです。

- （Windows） ACInstallDir¥bin
- （UNIX） ACInstallDir/lib

Windows の場合、CA ControlMinder は、対称暗号化に使用する暗号化ライブラリの完全パスを以下の設定で格納します。

HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥Encryption Package

対称暗号化鍵および対称暗号化方式を変更するには sechkey ユーティリティを使用します。

詳細情報：

[対称暗号化鍵の変更](#) (P. 561)

[対称暗号化方式の変更](#) (P. 563)

sechkey による対称暗号化の設定方法

対称暗号化鍵の長さは、55 文字です。sechkey によって、鍵がこれより長すぎる場合は切り捨てられ、短すぎる場合は文字が埋め込まれます。

sechkey を使用して暗号化鍵を変更すると、sechkey によって CA ControlMinder データベース内のすべてのプログラムの暗号化鍵が同時に変更されます。sechkey が対称鍵または対称暗号化方式を変更すると、以下を復号化および再暗号化します。

- コンピュータにインストールされたすべての Policy Model の暗号化されたレコード
- CA ControlMinder メッセージキューのパスワードを含む、CA ControlMinder データベース内のすべての暗号化されたパスワード (CA ControlMinder が双方向パスワード (ユーザパスワード) を使用している場合)
- サーバ秘密鍵 (鍵がパスワード保護されていない場合)
- サーバ秘密鍵用のパスワード (鍵がパスワード保護されている場合)

さらに、CA ControlMinder と通信するプログラムを作成するために CA ControlMinderAPI を使用する場合は常に、新しいプログラム用の通信が同じ鍵で暗号化されます。

対称暗号化鍵の変更

対称暗号化鍵は、CA ControlMinder コンポーネント間の通信を保護します。対称暗号化鍵を変更するには sechkey ユーティリティを使用します。sechkey は、対話モードまたは非対話モードのどちらでも使用できます。

対称暗号化鍵を変更する際は、以下の制限に注意します。

- パスワードの長さは 1 文字から 55 文字までに限られます。
- パスワードに拡張 ASCII 文字を含めることはできません。
- パスワードに二重引用符 (") を含めることはできません。

sechkey パラメータを使用するには ADMIN 属性が必要です。

重要: 通信の問題を回避するには、CA ControlMinder コンポーネントを実行するすべてのコンピュータ上で同じ暗号化鍵を使用します。

対象暗号化鍵を変更する方法

1. CA ControlMinder を停止します。

CA ControlMinder エンタープライズ管理サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも停止します。

2. sechkey ユーティリティを対話モードで実行します。

```
sechkey
```

ユーティリティによって、既存の鍵と新しい鍵の入力が求められ、対称暗号化鍵が変更されます。

3. CA ControlMinder を起動します。

CA ControlMinder エンタープライズ管理サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも起動します。

CA ControlMinder が起動し、新しい暗号化鍵を使用して通信を暗号化します。

例: 対称暗号化鍵を非対話モードで変更

以下の例は、デフォルトの CA ControlMinder 対称鍵を、newkey という値で新しい鍵に変更します。

```
sechkey -d newkey
```

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

対称暗号化方式の変更

CA ControlMinder コンポーネント間の通信を保護する対称暗号化は、暗号化ライブラリによって実装されます。暗号化ライブラリの変更によって対称暗号方式を変更するには、**sechkey** ユーティリティを使用します。

sechkey パラメータを使用するには **ADMIN** 属性が必要です。

注: CA ControlMinder が FIPS 専用モードで実行されている場合、対称暗号化方式を変更することはできません。**crypto** セクションの **fips_only** 構成トークンの値が **1** の場合、CA ControlMinder は FIPS のみのモードで動作します。この制限によって、暗号化方式が FIPS 準拠でない暗号化方式に変更されるのを防ぐことができます。

重要: 通信の問題を回避するには、**CA ControlMinder** コンポーネントを実行するすべてのコンピュータ上で同じ暗号方式を使用します。

対象暗号方式を変更する方法

1. CA ControlMinder を停止します。

CA ControlMinder エンタープライズ管理サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも停止します。

2. **sechkey** ユーティリティを使用して、対称暗号方式を変更します。
3. CA ControlMinder を起動します。

CA ControlMinder エンタープライズ管理サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも起動します。

CA ControlMinder が起動し、新しい暗号方式を使用して通信を暗号化します。

例: 対称暗号方式を 3DES に変更

以下のコマンドは、対称暗号方式を 3DES に変更します。

```
sechkey -m -sym tripledes
```

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

エンタープライズ展開での複数の対称暗号化方法

エンドポイントは、暗号化方式が異なる他の CA ControlMinder コンポーネントと通信できます。[crypto] セクションの [encryption_methods] 設定で、エンドポイントが受け取る対称暗号化方式を指定します。

デフォルトでは、この設定には順番に以下の暗号化方法がリスト表示されています。

- AES256
- AES192
- AES128
- DES
- 3DES

CA ControlMinder エージェントが別のコンポーネントからの受信通信を復号化する際に、エージェントはリストの各方法を順番に試行します。これは、復号化が成功するまで続きます。エージェントは、そのコンポーネントへの送信通信の暗号化に同じ暗号化方式を使用します。

同様に、CA ControlMinder Web Service がエンドポイントに接続する際に、エージェントはリストの各方法を順番に試行します。これは、エンドポイントとの通信が成功するまで続きます。

複数の暗号化方法によって、企業の CA ControlMinder 展開を容易にアップグレードできます。たとえば、DES 暗号化を使用する r12.5 展開があるとします。r12.5 SP4 への段階的なアップグレードを実行し、アップグレードされたコンポーネントの暗号化方法を AES256 に変更します。エンタープライズ管理サーバを r12.5 SP4 にアップグレードします。これで、サーバはデフォルトで AES256 暗号化を使用するようになります。ただし、r12.5 SP4 サーバは DES 暗号化を使用する CA ControlMinder コンポーネントと通信できるので、エンタープライズ管理サーバは継続して r12.5 エンドポイントを管理できます。

SSL、認証、および証明書

TLS などの Secure Sockets Layer (SSL) では、コンピュータ プログラム間の通信を実現できます。SSL は、通信に以下のプロパティが含まれていることを確認するのに役立ちます。

- 通信の参加者は認証されます。つまり、通信の参加者は身元が確認されたプログラムまたはユーザです。
- データは安全に暗号化され、そのデータを読み取ることができるのは参加者だけです。

参加者は、X.509 証明書を使用して互いに認証します。X.509 証明書は、証明書の所有者のアドレスを公開鍵とリンクさせる電子文書です。この証明書は偽造することは不可能です。

SSL はクライアント/サーバ モデルで機能し、PKI (public key infrastructure) を使用します。クライアントがサーバから X.509 証明書を受け取ると、その証明書が有効かどうかをチェックします。証明書が有効である場合、クライアントでは、サーバの正体がそれ自身が主張するプログラムまたはユーザであることを認識するので、サーバは認証されます。また、クライアントが証明書の公開鍵を使用してデータを暗号化した場合、サーバはそのデータしか復号化できません。したがって、データの安全性が守られます。サーバ側では、クライアントから受信する X.509 を同様に使用します。

証明書の内容

プログラムは X.509 証明書を送信して、その ID が公開鍵にバインドされていることを証明します。これにより、他のプログラムは、証明書の所有者のみ暗号化されたメッセージを復号化できることを認識して、メッセージを暗号化します。

X.509 証明書の内容は以下のとおりです。

- **証明書データ** - 最も重要な証明書データ フィールドには以下のものがあります。
 - 証明書の所有者の公開識別子（たとえば **Web** アドレス）
 - 証明書の有効期間（開始日および終了日）
- **証明書を証明する認証局（CA）の名前** - シグネチャが有効な場合、証明書のリーダに対して、公開鍵が所有者に関連付けられていることを認証局が保証します。つまり、証明書のリーダが **CA** を信頼している場合、公開鍵を使用して暗号化されたデータが所有者によってのみ読み取り可能であることを信用できます。
- **所有者の公開鍵** - 証明書のリーダは、公開鍵を使用してデータを暗号化し、それを証明書の所有者に送信します。
- **デジタル署名** - デジタル署名は、証明書の他のすべてのデータがハッシュおよびカプセル化されたもので、**CA** の秘密鍵を使用して暗号化されます。（送信者が公開鍵を使用してデータを暗号化するという暗号化の場合とは逆です。）**CA** の公開鍵へのアクセス権を有する人は誰でも、シグネチャを読み取り、このシグネチャが証明書内の他のデータと一致するかどうかをチェックすることができます。証明書内のいずれかのテキストが変更されている場合、シグネチャは証明書のテキストとは一致しなくなります。

所有者の秘密鍵は証明書と関連付けられていますが、個別に管理され、安全性が保たれています。所有者は秘密鍵を使用して、プログラムが公開鍵を使用して暗号化したメッセージを復号化します。

証明書が証明すること

リーダは、認証局（CA）の公開鍵を使用して証明書シグネチャを検証することができます。復号化されたシグネチャが証明書の残りの内容と一致し、かつリーダが CA を信頼している場合、リーダは以下のことが当てはまることを認識しています。

- リーダが公開鍵を使用してデータを暗号化すると、そのデータを復号化し、読み取ることができるのは秘密鍵の所有者だけです。
- 証明書の秘密鍵の所有者は、証明書内で指定された所有者です。

証明書が有効であることを確信するために、リーダは CA を信頼し、さらに CA の公開鍵にアクセスする必要があります。ほとんどの場合、CA はよく知られた会社であり、プログラム（およびすべての一般的な Web ブラウザ）は CA 公開鍵のコピーを保持しているので、リーダはオンラインで CA が本当に証明書を検証したかどうかをチェックする必要はありません。

発行者がまた所有者である場合、証明書は自己署名証明書と呼ばれます。この発行者を信頼することには、問題があります。

証明書を送信したプログラムが証明書の所有者であることを確認するには、リーダは他の方法を使用する必要があります。通常、リーダは、証明書の送信者を探すのに使用したアドレスが証明書内にあるアドレスと同じであることをチェックします。

ルート証明書とサーバ証明書

ルート（CA）証明書は、認証局（CA）によって検証された信頼済み X.509 証明書です。この信頼済み証明書を使用して、サーバ（所有者）証明書という追加の X.509 証明書を作成します。各サーバ証明書は、ルート証明書の秘密鍵によって署名されます。リーダがルート証明書を信頼する場合、そのルート証明書から作成されたすべてのサーバ証明書を信頼できることとなります。

ルート証明書は、サーバ証明書を生成および認証します。CA ControlMinder では、以下のタイプのルート証明書を使用できます。

- デフォルトの CA ControlMinder ルート証明書
- サードパーティのルート証明書（パスワード保護された証明書を含む）

サーバ証明書は、CA ControlMinder クライアント/サーバ通信および CA ControlMinder コンポーネント間の通信を暗号化し、認証します。CA ControlMinder では、以下のタイプのサーバ証明書を使用できます。

- デフォルトの CA ControlMinder サーバ証明書
- サードパーティのサーバ証明書 (パスワード保護された証明書を含む)
- サードパーティのルート証明書から作成された CA ControlMinder サーバ証明書

SSL 暗号化の有効化

CA ControlMinder をインストールする際は、暗号化を設定します。インストールの後には、**sechkey** ユーティリティを使用して SSL 暗号化を変更できます。設定の値も変更する必要がある場合があります。

重要: 通信の問題を回避するには、**CA ControlMinder** コンポーネントを実行するすべてのコンピュータ上で同じ暗号方式を使用します。

SSL 暗号化を有効にする方法

1. CA ControlMinder を停止します。

CA ControlMinder エンタープライズ管理 サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも停止します。

2. **crypto** セクション内の **communication_mode** 設定の値を以下のいずれかに変更します。

all_modes

対称鍵暗号化および SSL 暗号化の両方を有効にする場合は、この値を指定します。この値を指定すると、すべての CA ControlMinder コンポーネントとコンピュータが通信できるようになります。

注: この値を指定した場合、CA ControlMinder では、別の CA ControlMinder コンポーネントとの通信を試行する際に常に SSL 暗号化を使用します。SSL が失敗した場合は対称暗号化を使用します。この値によって、対称暗号化環境から SSL 暗号化環境に CA ControlMinder デプロイメントを移行することができます。

use_ssl

SSL 暗号化のみを有効にする場合は、この値を指定します。この値を指定すると、SSL 暗号化を使用する CA ControlMinder コンポーネントのみとコンピュータが通信できるようになります。

注: (Windows) CA ControlMinderSDK を使用するサードパーティ プログラムを使用している場合、**crypto** セクションは、インストール時に定義した CA ControlMinderSDK レジストリ パスにあります。

3. (推奨) SSL 通信を以下のいずれかに設定します。
 - [サードパーティのルート証明書およびサーバ証明書を使用 \(P. 570\)](#)。
 - [サードパーティのルート証明書から生成したサーバ証明書を使用 \(P. 573\)](#)。

注: SSL 暗号化をさらに設定しない場合、CA ControlMinder コンポーネント間の通信を暗号化および認証するためにデフォルトの CA ControlMinderX.509 証明書を使用できます。ただし、デフォルト証明書は変更することをお勧めします。

4. CA ControlMinder を起動します。

- CA ControlMinder エンタープライズ管理 サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも起動します。
- CA ControlMinder SDK を使用するサードパーティのプログラムを使用している場合、CA ControlMinder SDK を使用するプロセスを再起動します。

SSL 暗号化が有効になります。

サードパーティのルート証明書およびサーバ証明書の使用

SSL 暗号化を使用する場合、サードパーティのルート証明書とサーバ証明書を使用して、CA ControlMinder コンポーネント間の通信を暗号化および認証できます。

サードパーティのルート証明書およびサーバ証明書を使用するには以下のファイルが必要です。

- **root.pem** - ルート証明書
- **server.pem** - サーバ証明書
- **server.key** - サーバ証明書の秘密鍵

OU パスワード保護されたサーバ証明書を使用する場合、サーバ証明書の秘密鍵のパスワードも必要になります。

注: サーバ証明書がすでに作成されているので、ルート証明書の秘密鍵は必要ではありません。

サードパーティのルート証明書およびサーバ証明書を使用する方法。

1. CA ControlMinder サービスが停止され、SSL が有効であることを確認します。
2. ルート証明書を置き換えます。以下のいずれかの操作を実行します。

- `crypto` セクションの `ca_certificate` 設定で指定された場所に新しいルート証明書をコピーします。
- `crypto` セクションの `ca_certificate` 設定の値を編集し、新しいルート証明書への完全パスを指定します。

注: 新規ディレクトリにルート証明書をインストールした場合は、新規ディレクトリを保護する CA ControlMinder ファイル ルールを作成する必要があります。

3. サーバ証明書を置き換えます。以下のいずれかの操作を実行します。

- `crypto` セクションの `subject_certificate` 設定で指定された場所に新しいサーバ証明書をコピーします。
- `crypto` セクションの `subject_certificate` 設定の値を編集し、新しいサーバ証明書への完全パスを指定します。

注: 新規ディレクトリにサーバ証明書をインストールした場合は、新規ディレクトリを保護する CA ControlMinder ファイル ルールを作成する必要があります。

4. サーバ鍵を置き換えます。以下のいずれかの操作を実行します。

- `crypto` セクションの `private_key` 設定で指定された場所に新しいサーバ鍵をコピーします。
- `crypto` セクションの `private_key` 設定の値を編集し、新しいサーバ鍵への完全パスを指定します。

注: 新規ディレクトリにサーバ鍵をインストールした場合は、新規ディレクトリを保護するために CA ControlMinder ファイル ルールを作成する必要があります。

5. OU パスワード保護された証明書を使用する場合は、以下を実行します。

- a. `crypto` セクションの `fips_only` 設定の値が `0` であることを確認します。

注: CA ControlMinder が FIPS 専用モードで動作している場合、パスワード保護された証明書を使用することはできません。

- b. サーバ証明書の秘密鍵用のパスワードを以下のようにコンピュータに格納します。

```
sechkey -g -subpwd private_key_password
```

注: `sechkey` を使用するには ADMIN 属性が必要です。

- c. CA ControlMinder で、保存されたパスワードを使用して秘密鍵を開くことができることを確認します。

```
sechkey -g -verify
```

CA ControlMinder で鍵を開けない場合は、手順 **b** を繰り返し、正しいパスワードを指定します。

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

6. CA ControlMinder を起動します。

- CA ControlMinder エンタープライズ管理 サーバ上の暗号化設定を変更している場合は、CA ControlMinder Web サービスも起動します。
- CA ControlMinder SDK を使用するサードパーティのプログラムを使用している場合、CA ControlMinder SDK を使用するプロセスを再起動します。

SSL 暗号化が有効になります。

サードパーティのルート証明書から生成したサーバ証明書の使用

SSL 暗号化を使用する場合、サードパーティのルート証明書からサーバ証明書を作成できます。作成した証明書を使用して、CA ControlMinder コンポーネント間の通信を暗号化および認証します。

パスワード保護されたサーバ証明書を作成できます。その場合、CA ControlMinder では、指定されたパスワードを使用してサーバ証明書の秘密鍵を保護します。

サードパーティのルート証明書からサーバ証明書を作成するには以下のファイルが必要です。

- **root.pem** - ルート証明書
- **root.key** - ルート証明書の秘密鍵

サードパーティのルート証明書から生成したサーバ証明書を使用する方法。

1. CA ControlMinder サービスが停止され、SSL が有効であることを確認します。
2. OU パスワード保護された証明書を使用する場合、**crypto** セクションの **fips_only** 設定の値が 0 であることを確認します。

注: CA ControlMinder が FIPS 専用モードで動作している場合、パスワード保護された証明書を使用することはできません。

3. 以下のディレクトリの **sub_cert_info** 以外のすべてのファイルを削除します。**ACInstallDir** は、CA ControlMinder をインストールしたディレクトリです。

ACInstallDir/data/crypto

重要: **sub_cert_info** ファイルは削除しないでください。

デフォルトのサーバ証明書およびサーバ証明書のデフォルトの鍵が削除されます。

4. ルート証明書を置き換えます。以下のいずれかの操作を実行します。

- `crypto` セクションの `ca_certificate` 設定で指定された場所に新しいルート証明書をコピーします。
- `crypto` セクションの `ca_certificate` 設定の値を編集し、新しいルート証明書への完全パスを指定します。

注: 新規ディレクトリにルート証明書をインストールした場合は、そのディレクトリを保護するため **CA ControlMinder** ファイルルールを作成する必要があります。

5. `sechkey` ユーティリティを使用してサーバ証明書を生成します。

注: `sechkey` ユーティリティの詳細については「リファレンスガイド」を参照してください。 `sechkey` パラメータを使用するには **ADMIN** 属性が必要です。 **CA ControlMinder SDK** を使用するサードパーティのプログラムを使用している場合は、`sechkey` を実行するときに、`sechkey` コマンドに `-s` オプションを追加します。

6. (オプション) ルート証明書の秘密鍵を削除します。

ルート証明書からの別のサーバ証明書を作成しない場合、ルート証明書の秘密鍵を削除できます。

7. **CA ControlMinder** を起動します。

- **CA ControlMinder** エンタープライズ管理 サーバ上の暗号化設定を変更している場合は、**CA ControlMinder Web** サービスも起動します。
- **CA ControlMinder SDK** を使用するサードパーティのプログラムを使用している場合、**CA ControlMinder SDK** を使用するプロセスを再起動します。

SSL 暗号化が有効になります。

例: `sechkey` を使用してサーバ証明書を作成

この例では、サードパーティのルート証明書からサーバ証明書を作成します。この例は、デフォルトの **CA ControlMinder** 証明書情報ファイルを使用します。ルート証明書の秘密鍵は `custom_root.key` という名前で、`/opt/CA/AccessControl/data/crypto` にあります。

```
sechkey -e -sub -in "/opt/CA/AccessControl/data/crypto/sub_cert_info" -priv  
/opt/CA/AccessControl/data/crypto/custom_root.key
```

パスワード保護されたサーバ証明書

CA ControlMinder がパスワード保護されたサーバ証明書を使用するように設定することができます。その場合、CA ControlMinder では、指定されたパスワードを使用してサーバ証明書の秘密鍵を保護します。CA ControlMinder は、*ACInstallDir/Data/crypto* ディレクトリ内の *crypto.dat* ファイルにパスワードを保存します。*ACInstallDir* は、CA ControlMinder がインストールされたディレクトリです。*crypto.dat* ファイルは非表示かつ暗号化され、読み取り専用で CA ControlMinder によって保護されます。CA ControlMinder が停止されている場合、スーパーユーザのみがパスワードにアクセスできます。

パスワード保護されているサーバ証明書を作成する場合、*sechkey* は証明書を暗号化しません。パスワード保護されていないサーバ証明書を作成する場合、*sechkey* は AES256 および CA ControlMinder 暗号化鍵を使用して証明書を暗号化します。

エンタープライズ管理サーバ SSL 通信

12.7 以降、エンタープライズ管理サーバ コンポーネントは通信に SSL を使用するようになりました。以下のコンポーネントの SSL 通信設定を変更できます。

- JBoss アプリケーション サーバ

デフォルトでは、JBoss のインストールで SSL はサポートされません。

- メッセージキュー

ウェルノウン ポートへの不正なアクセスを防ぐために、メッセージキューのデフォルト SSL ポートを変更できます。

- CA ControlMinder エンタープライズ管理

- (オプション) Java コネクタ サーバ

デフォルト証明書を使用した場合のみ、CA ControlMinder 12.5 SP3 にアップグレードした後に、新しい SSL 証明書をインポートします。

JBoss の SSL 通信

JBoss アプリケーション サーバは、12.7 以降では SSL サポートでインストールされます。JBoss SSL 通信設定は変更できます。

注: JBoss 用に SSL を設定する方法の詳細については、JBoss 製品のドキュメントを参照してください。

例: Windows で SSL 通信用に JBoss を変更する

この例では、安全に通信を行うために SSL を使用する JBoss アプリケーション サーバを設定する方法を示します。

重要: この手順では、JBoss バージョン 4.2.3 および JDK バージョン 1.5.0 を使用して、安全な通信を行うために SSL の使用するように JBoss アプリケーション サーバを設定する方法を説明します。

次の手順に従ってください:

1. JBoss が実行されている場合は、停止します。
2. コマンドプロンプト ウィンドウを開き、以下のディレクトリに移動します。

```
JBoss_HOME\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore
```


3. 以下のコマンドを入力して、デフォルトの `ssl`、キーストア パスワードを変更します。

```
keytool -storepasswd -new <password> -keystore ssl.keystore -storepass secret  
-storepasswd
```

キーストア パスワードを変更するように指定します。パスワードは 6 文字以上である必要があります。

`-keystore`

証明書を追加するキーストア名を指定します。

`-keystore`

キーストアの名前を指定します。

`-storepass`

キーストアの保護に使用されるパスワードを定義します。

4. 以下のコマンドを入力して、エンタープライズ管理サーバのキーを作成します。

```
keytool -genkey -alias entm -keystore ssl.keystore -keyalg RSA
```

`-genkey`

コマンドによる鍵ペア（公開鍵と秘密鍵）の作成を指定します。

`-alias`

エントリをキーストアに追加するために、エイリアスを定義します。

`-keyalg`

鍵ペアの生成に使用するアルゴリズムを指定します。

`keytool` ユーティリティが起動します。

5. 「`secret`」というパスワードを入力します。
6. 必要に応じてプロンプトを完了し、**Enter** キーを押して、入力したパラメータを確認します。

証明書がキーストアに追加されます。

注: キーストアおよびキー エイリアスには、同一のパスワードを使用する必要があります。

7. ファイルへのキーストア パスワードの暗号化を行う、以下のコマンドを入力します。

```
java -cp C:/jboss-4.2.3.GA/server/default/lib/jbosssx.jar
org.jboss.security.plugins.FilePassword welcometoboss 13 <password>
keystore.password
```

注: Salt と IterationCount は暗号化されたパスワードの強度を定義する変数です。この例では、"welcometoboss" は Salt です。また、13 は IterationCount です。

8. 以下のディレクトリで server.xml という名のファイルを検索し、編集可能な形式でそれを開きます。

```
JBossInstallDir¥server¥default¥deploy¥jboss-web.deployer
```

9. 以下のセクションで <Connector Port> タグを探します。

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
      This connector uses the JSSE configuration, when using APR, the
      connector should be using the OpenSSL style configuration
      described in the APR documentation -->
<!--
<Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" />
```

注: コネクタ ポート番号は、必須ソフトウェアまたは CA ControlMinder エンタープライズ管理 のインストール時に指定した JBoss HTTPS ポート番号に対応します。

10. "<!--" above the <Connector port> タグのコメントを解除します。

これで、このタグを編集できるようになりました。

11. <Connector port> タグへ以下のプロパティを追加します。

```
securityDomain="java:/jaas/encrypt-keystore-password"
SSLImplementation="org.jboss.net.ssl.JBossImplementation"
```

12. server.xml ファイルを保存して閉じます。

13. jboss-service.xml ファイルを見つけるために、以下のディレクトリに移動します。

JBoss_HOME/server/default/deploy/jboss-web.deployer/META-INF

14. <server> と </server> タグの間に、以下の mbean を追加します。

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="jboss.security:service=PBESecurityDomain">
  <constructor>
    <arg type="java.lang.String" value="encrypt-keystore-password"></arg>
  </constructor>
  <attribute
name="KeyStoreURL">${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/
ppm/truststore/ssl.keystore</attribute>
  <attribute
name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:${jboss.se
rver.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keystore.passw
ord</attribute>
  <attribute name="Salt">welcometojboss</attribute>
  <attribute name="IterationCount">13</attribute>
</mbean>
```

注:: 前の例で、welcometojboss は Salt、13 は IterationCount です。

15. jboss-service.xml を保存し閉じます。

16. CA ControlMinder エンタープライズ管理 を起動して開きます。

注: この手順を終えた後、JBoss および CA ControlMinder エンタープライズ管理 への接続には、SSL モードまたは SSL 以外のモードのいずれかを選択できます。

SSL 通信用に CA ControlMinder エンタープライズ管理 を設定する方法

Active Directory または CA Directory と連携する場合に SSL を使用するよう、エンタープライズ管理サーバを設定できます。

以下の手順を実行します。

1. DER、CRT または CERT 形式のユーザディレクトリ証明書を取得します。
2. 証明書をキーストアに追加します。
3. SSL 通信を使用するように CA ControlMinder エンタープライズ管理 を設定します。

詳細情報:

[キーストアへのユーザディレクトリ証明書の追加 \(P. 580\)](#)

[SSL 通信用の CA ControlMinder エンタープライズ管理 の設定 \(P. 581\)](#)

キーストアへのユーザディレクトリ証明書の追加

SSL 通信を使用するよう CA ControlMinder エンタープライズ管理 を設定する前に、ユーザディレクトリ証明書をキーストアに追加する必要があります。

注: Active Directory または CA Directory に SSL を設定する方法の詳細については、Active Directory および CA Directory のドキュメントを参照してください。

例: キーストアへの Active Directory 証明書の追加

重要: この例では、JBoss バージョン 4.2.3 および JDK バージョン 1.5.0 を使用して、Active Directory との安全な通信を行うために SSL の使用するよう に CA ControlMinder エンタープライズ管理 を設定する方法について説明します。この手順を開始する前に、DER、CER または CERT にエンコードされたバイナリ形式の Active Directory 証明書を取得する必要があります。

1. JBoss が実行されている場合は、停止します。以下のいずれかの手順を実行します。
 - JBoss ジョブ ウィンドウから、プロセスを中断します (Ctrl+C)。
 - [サービス] パネルから JBoss アプリケーション サーバサービスを停止します。
2. エンタープライズ管理サーバで、コマンドプロンプト ウィンドウを開き、以下のディレクトリに移動します。

```
jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore
```

3. 以下のコマンドを入力します。

```
keytool -import -keystore ssl.keystore -alias ad -file <activedirectory.cert>
```

パスワードの入力を促すメッセージが表示されます。

-import

ユーティリティが証明書を読み取り、それをキーストアに格納するように指定します。

-alias

キーストアへのエントリの追加で使用するエイリアスを指定します。

-file

Active Directory 証明書ファイルの完全パス名を指定します。

4. 「secret」というパスワードを入力します。
5. JBoss bin ディレクトリへ移動します。デフォルトでは、このディレクトリは以下にあります。

```
JbossInstallDir/bin
```

6. run.bat ファイルを開いて、trusted ユーザ ストア データで java_ops パラメータを設定します。例：

```
set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m  
-Djavax.net.ssl.trustStore=C:\%jboss-4.2.3.GA\server\default\deploy\IdentityMi  
nder.ear\custom\ppm\truststore\ssl.keystore
```

7. ファイルを保存して、JBoss を起動します。

詳細情報：

[SSL 通信用の CA ControlMinder エンタープライズ管理 の設定 \(P. 581\)](#)

SSL 通信用の CA ControlMinder エンタープライズ管理 の設定

ユーザ ディレクトリ証明書をキーストアへ追加したら、SSL 通信を使用するように CA ControlMinder エンタープライズ管理 を設定できます。

注：SSL 接続用に CA ControlMinder エンタープライズ管理 を設定するには、CA IdentityMinder 管理コンソールを有効にする必要があります。CA IdentityMinder 管理コンソールの詳細については、*CA IdentityMinder 管理コンソールのオンラインヘルプ*をご覧ください。

SSL 通信用の JBoss の設定方法

1. CA IdentityMinderManagement Console で、[ディレクトリ] をクリックします。
2. ac-dir ディレクトリをクリックします。
[ディレクトリのプロパティ] ウィンドウが表示されます。
3. プロパティ ウィンドウの一番下で、[エクスポート] をクリックします。
4. プロンプトが表示されたら、XML ファイルを保存します。
5. XML ファイルを編集できる形で開きます。
6. `<Provider userdirectory="ac-dir" type="LDAP">` タグを探します。
7. `secure` パラメータを `true` に変更します。例：

```
<LDAP searchroot="DC=abc,DC=company,DC=com" secure="true">
```
8. `<Connection host="COMPUTER.abc.company.com" port=" ">` タグを探し、ポート番号を `636` に変更します。例：

```
<Connection host="COMPUTER.abc.company.com" port="636">
```
9. `<Container objectclass="top,organizationalUnit" attribute="ou"/>` タグをすべて検索して、各行の最後に `value` パラメータを入力します。例：

```
<Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
```
10. ファイルを保存します。
11. CA IdentityMinder 管理コンソールで、ディレクトリのプロパティ ページから [更新] をクリックします。
ディレクトリの更新ウィンドウが表示されます。
12. Identity Manager ディレクトリを更新するための XML ファイルのパスとファイル名を入力するか、ファイルを参照して選択し、[完了] をクリックします。
ディレクトリ設定出力フィールドにステータス情報が表示されます。
13. [続行] をクリックし、環境を再起動します。
CA ControlMinder エンタープライズ管理が SSL を使用してユーザ ディレクトリと通信できるようになりました。

詳細情報:

[CA IdentityMinder 管理コンソールの有効化](#) (P. 104)

[CA IdentityMinder 管理コンソールの起動](#) (P. 105)

メッセージ キュー サーバの SSL ポート番号

CA ControlMinder エンタープライズ管理 のインストール時に、メッセージ キュー サーバはデフォルトの SSL 通信ポート番号で設定されます。たとえば、ウェルノウンポートからの不正なアクセスを防止するために、CA ControlMinder エンタープライズ管理 のインストール後に、ポート番号を変更できます。

例: メッセージ キュー サーバの SSL ポート番号の変更

以下の例では、メッセージ キュー サーバの SSL ポート番号のデフォルトポート番号からの変更方法について説明します。

メッセージ キュー サーバの SSL ポート番号の変更方法

注: メッセージ キュー サーバの設定を変更する前に、CA ControlMinder のサービスまたはデーモンをすべて停止します。

1. CA ControlMinder エンタープライズ管理 サーバ上で、以下のディレクトリに移動します。

```
ACServer_InstallDir/AccessControlServer/MessageQueue/tibco/ems/bin
```

2. routes.conf ファイルを開いて、編集します。
3. エントリ [PR_DMS_SERVER] を見つけて、[url] フィールドでポート番号値を変更します。以下に例を示します。

```
url = ssl://PR_DMS_SERVER:7777
```

4. tibemsd.conf ファイルを編集できる形で開きます。
5. エントリ リスニング ポートを見つけて、ポート番号を変更します。以下に例を示します。

```
listen = ssl://7777
```

6. tibcoems-service.xml ファイルを開いて、編集します。

7. セクション `<!-- The JMS provider loader -->` を見つけて、`java.naming.provider.url` 行でポート番号を変更します。以下に例を示します。

```
java.naming.provider.url=tibjmsnaming://localhost:7777
```

8. `factories.conf` ファイルを開いて、編集します。
9. セクション `[SSLQueueConnectionFactory]`、`[SSLTopicConnectionFactory]`、`[SSLXAQueueConnectionFactory]` を見つけて、`[url]` フィールドでポート番号を変更します。以下に例を示します。

```
[SSLQueueConnectionFactory]
type                        = queue
url                        = ssl://7777
ssl_verify_host            = disabled

[SSLTopicConnectionFactory]
type                        = topic
url                        = ssl://7777
ssl_verify_host            = disabled

[SSLXAQueueConnectionFactory]
type                        = xaqueue
url                        = ssl://7777
ssl_verify_host            = disabled
```

10. エントリ `org.jboss.naming.NamingAlias` を見つけて、ポート番号を変更します。以下に例を示します。

```
tibjmsnaming://localhost:7777
```

11. CA ControlMinder サービスを開始します。

これで、メッセージキュー サーバの SSL ポート番号がリクエストどうりに変更されました。

同一の暗号化鍵を使用するためのサーバの設定

複数のエンタープライズ管理サーバをインストールした場合、各サーバは独自の暗号化鍵を使用して、中央データベース内のデータの暗号化および復号化を行います。お使いの環境で、複数のエンタープライズ管理サーバが 1 つの中央データベースに対してデータの読み書きを行っている場合、すべてのサーバで同一の暗号化鍵を使用する必要があります。

重要: `-DFIPS_KEY` オプションを使用してセカンダリ管理サーバをインストールした際に、プライマリ エンタープライズ管理サーバが使用する FIPS キーを指定しなかった場合のみ、以下の手順を完了します。

同一の暗号化鍵を使用するようサーバを設定する方法

1. JBoss が実行されている場合は、停止します。以下のいずれかの操作を実行します。
 - JBoss アプリケーション サーバ ウィンドウを中断します (Ctrl + C)。
 - [サービス] パネルから JBoss サービスを停止します。
2. 同一の暗号化鍵を使用するようエンタープライズ管理サーバを設定します。以下を実行します。
 - a. プライマリ エンタープライズ管理サーバから以下のディレクトリに、FIPSSKey.dat ファイルをコピーします。

`JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys`
 - b. 各セカンダリ エンタープライズ管理サーバ上で、コピーした FIPSSKey.dat ファイルをこのディレクトリに貼り付けます。

この名前のファイルが存在することを通知するメッセージが表示されます。
 - c. 新規ファイルで既存ファイルを上書きすることを選択します。

新規ファイルがディレクトリに格納されます。各エンタープライズ管理サーバで同一の暗号化鍵を使用するようになりました。
3. 各セカンダリ エンタープライズ管理サーバ上で、新しい暗号化鍵を使用して AES パスワードを更新します。以下を実行します。
 - a. [クリア テキスト パスワードを暗号化](#) (P. 630) します。
 - b. 各セカンダリ エンタープライズ管理サーバで、以下のファイルにアクセスします。

`JBoss_HOME/server/default/conf/login-config.xml`
`JBoss_HOME/server/default/deploy/properties-service.xml`
 - c. ファイル内の各 AES パスワードを新しく暗号化されたパスワードで置き換えます。
4. JBoss を起動します。

プライマリおよびセカンダリのエンタープライズ管理サーバで、データの暗号化および復号化に同一の暗号化鍵が使用されるようになりました。

例: 暗号化された AES パスワード

login-config.xml ファイル内の以下のスニペットは、暗号化された AES パスワードを表しています。

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
      code="com.netegrity.jboss.datasources.PasswordEncryptedLogin"
      flag="required">
      <module-option name="userName">user1</module-option>
      <module-option name="password">
        {AES}:/LxnvWwAEcYhSmOu3YT3ow==</module-option>
      <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
      </login-module>
    </authentication>
  </application-policy>
```

CA ControlMinder Web サービスの URL の変更

CA ControlMinder エンタープライズ管理 および CA ControlMinder エンドポイント管理 へのアクセスには CA ControlMinder Web サービスを使用します。CA ControlMinder Web サービスの URL は、`HTTP:hostname:port;` の形式になっています。たとえば `example, http://entmserver:5248` などです。デフォルトでは、`hostname` はエンタープライズ管理サーバの名前です。

CA ControlMinder Web サービスの URL を変更する場合、Web サービスがリスンする IP アドレスおよびポートを変更します。セキュリティを強化するため、ホスト名を `localhost` に変更できます（たとえば `http://127.0.0.1:5248`）。`localhost` を使用すると、ローカル ホスト環境の外部からのスキャナによって Web サービスが検出されるのを防ぐことができます。そのため、Web サービスの露出を抑えることができます。

以下の手順に従います。

1. JBoss および CA ControlMinder サービスが実行されている場合は停止します。
2. URL 内のホスト名を以下のように変更します。
 - (Windows) WebService レジストリ キーの **machineName** レジストリ値の値を新しいホスト名に変更します。
 - (Linux) **seos.ini** ファイル内の **WebService** セクションの **machineName** 設定の値を新しいホスト名に変更します。
3. (オプション) URL 内のポート番号を以下のように変更します。
 - (Windows) WebService レジストリ キーの **portNumber** レジストリ値の値を新しいポート番号に変更します。
 - (Linux) **seos.ini** ファイル内の **WebService** セクションの **portNumber** 設定の値を新しいポート番号に変更します。
4. 以下のファイルを開きます (*JBoss_home* は、JBoss をインストールしたディレクトリです)。
JBoss_home/server/default/conf/webservice.properties
5. **webservice.url** プロパティの値を新規ホスト名とポートに変更します。以下に例を示します。
webservice.url=http://127.0.0.1:5248
6. ファイルを保存して閉じます。
7. CA ControlMinder Web Service を含む CA ControlMinder サービスを再起動します。
8. JBoss を再起動します。
CA ControlMinder Web Service URL が変更されました。

Microsoft SQL Server データベース接続設定の変更

Microsoft SQL Server にエンタープライズ管理サーバをインストールした場合、認証モードは SQL Server 認証に設定されます。インストールが完了した後、データベース認証モードを Windows 認証モードに変更することができます。

SQL Server が Windows 認証モードで動作している場合、エンタープライズ管理サーバは JBoss サービス アカウントを使用して SQL Server 上の中央データベースを管理します。別の JBoss サービス アカウントを使用する場合、SQL Server データベース インスタンス上のアカウントを変更する必要があります。

重要: Windows 認証モードで動作するように SQL Server を設定するには、SQL Server JDBC 2.0 ドライバをインストールする必要があります。

重要: Microsoft SQL Server で指定したユーザにデータベース ロール dbowner が割り当てられていることを確認してください。

SQL Server データベース接続設定の変更方法

1. まだの場合は、SQL Server JDBC 2.0 ドライバ ファイルを一時ディレクトリにダウンロードおよび解凍してください。
2. JBoss が実行されている場合は、停止します。以下のいずれかの操作を行います。
 - JBoss アプリケーション サーバ ウィンドウを中断します (Ctrl + C)。
 - [サービス] パネルから JBoss サービスを停止します。
3. JBoss lib ディレクトリへ移動します。ディレクトリは以下にあります。

`JBossInstallDir/server/default/lib`

4. ファイル `sqljdbc.jar` を一時ディレクトリから JBoss lib ディレクトリにコピーします。

この名前のファイルが存在することを通知するメッセージが表示されます。

5. 新規ファイルで既存ファイルを上書きすることを選択します。
新規ファイルがディレクトリに格納されます。

- JBoss bin ディレクトリへ移動します。デフォルトでは、このディレクトリは以下にあります。

JBossInstallDir/bin

- ファイル `sqljdbc_auth.dll` を一時ディレクトリから JBoss bin ディレクトリにコピーします。

新規ファイルがディレクトリに格納されます。

- JBoss の `deploy` ディレクトリへ移動します。デフォルトでは、このディレクトリは以下にあります。

JBoss-directory/server/default/deploy

- 以下のファイルを開きます。

- `imauditdb-ds.xml`
- `imtaskpersistencedb-ds.xml`
- `imworkflowdb-ds.xml`
- `objectstore-ds.xml`
- `reportsnapshot-ds.xml`

- 各ファイルで `<connection-url>` タグを見つけて、`DatabaseName=` パラメータの後ろに以下を追加します。

`;integratedSecurity=true`

- 各ファイルから、`<security-domain>` タグを削除します。

- ファイルを保存して、JBoss を再起動します。

これで、CA ControlMinder エンタープライズ管理 が Windows 認証モードで SQL サーバと連動するようになります。

例: JBoss 環境設定ファイルの変更による Windows 認証モードの有効化

以下の例は、SQL 認証モードから Windows 認証モードに切り替える JBoss 環境設定ファイルの 1 つを変更する方法を示します。この例では、管理者はファイル `objectstore-ds.xml` を変更し、接続モードを Windows 認証

(`;integratedSecurity=true`) に指定します。次に、管理者はファイルから `<security-domain>` タグを削除します。このタグが削除されるのは、その適用対象が SQL 認証モードのみであるためです。

以下の抜粋は、管理者が接続設定を変更した後の `objectsstore-ds.xml` ファイルを示しています。

```
<connection-url>jdbc:sqlserver://example.comp.com:1433;  
selectMethod=cursor;DatabaseName=ACDB;  
integratedSecurity=true</connection-url>
```

レポート ポータル用の Windows 認証設定

Windows で有効

レポート ポータル (CA Business Intelligence) をインストールし、CMS データベースとして Microsoft SQL Server を使用することを選択すると、認証モードは SQL Server 認証に設定されます。Microsoft SQL Server 認証では、データベース接続を認証するために SQL ユーザ アカウントが使用されます。

ユーザの組織で Active Directory が使用される場合には、認証方式を Windows 認証に変更できます。Windows 認証では、CMS データベースへの接続はローカル ユーザ アカウントではなく Domain ユーザ アカウントを使用して認証されます。

Windows 認証による接続の認証では、すべてのレポート ポータル コンポーネント間にセキュリティで保護された伝達方法が提供されます。ユーザ クレデンシャルが格納されたデータベースへの ODBC 接続を設定することにより、レポート ポータル上でデプロイするレポート パッケージからクリア テキストのパスワードを排除できます。

重要: Windows 認証では、Internet Information Server (IIS) と Microsoft SQL Server の両方を使用する必要があります。

Windows 認証で動作するようにレポート ポータルを設定する方法

レポート ポータルのデータベース接続認証モードを変更するために実行する手順を理解すると、Windows 認証でレポート ポータルを実装する際に役に立ちます。

レポート ポータルを Windows 認証用に設定するには、以下の手順を実行します。

1. Microsoft SQL Server 2005 のデータベースを準備して、CMS データベースとして使用します。
2. デフォルトのユーザと照合を使用して、CA Business IntelligenceCMS データベースを準備します。
3. System DSN を作成して、SQL Server 認証を使用するように指定します。
System DSN はレポート ポータルの CMS データベースに接続するために使用されます。
4. Active Directory ユーザをローカル Administrators グループに追加します。
このユーザを指定して、レポート ポータルを設定する際に Windows 認証で動作するように認証します。
5. ASP.NET Web Service Extension to Allowed を設定します。
6. [レポート ポータル CA Business Intelligence をインストールします \(P. 129\)](#)。インストール中に以下の手順を実行します。
 - a. CA Business Intelligence のカスタム モードでのインストールを選択します。
 - b. データベースとして Microsoft SQL Server 2005 を指定します。
 - c. Web サーバとして IIS を指定します。
7. レポート ポータルを Windows 認証用に設定します。
Active Directory ユーザ アカウントを使用して Windows 認証で認証するように CA Business Intelligence サービスを設定します。
8. Windows 認証を使用して、CA ControlMinder のレポート データベース用の System DSN を作成します。
System DSN は CA ControlMinder のレポート ポータルへ接続するために使用されます。
9. レポート ポータルでレポート パッケージをデプロイします。

Windows 認証用のレポート ポータルの設定

レポート ポータルをインストールしたら、Windows 認証で動作するようにレポート ポータルを設定できます。Active Directory のユーザ アカウントを使用するようにレポート ポータルを設定し、さらに System DSN 接続パラメータを変更します。

Windows 認証用にレポート ポータルを設定する方法

1. オペレーティング システムの管理者としてレポート ポータルのホストにログインします。
2. Windows NT 認証に対するレポート ポータル CMS 用に System DSN を変更します。
3. [スタート] - [プログラム] - [BusinessObjects XI Release 2] - [BusinessObjects Enterprise] - [Central Configuration Manager] の順に選択します。

Central Configuration Manager が開かれて、CA Business Intelligence サービスが表示されます。

4. すべての CA Business Intelligence サービスを停止します。
5. サービスの Log On As 設定を Active Directory のユーザ クレデンシャルに変更します。すべての CA Business Intelligence サービスに対して、これを実行します。

重要: WinHTTP Web Proxy Auto-Discovery と World Wide Web Publishing サービスの設定は変更しないでください。

6. すべての CA Business Intelligence サービスを開始します。

これで、レポート ポータルは Windows 認証で認証を行うように設定されています。

注: Microsoft SQL Server Activity Monitor から、レポート対象のデータベースへの接続で Active Directory のユーザ アカウントが使用されることが確認できます。

例：CA Business Intelligence サービスの Log On As 接続設定の変更

以下の例では、CA Business Intelligence Connection Server サービスの Log On As クレデンシャルをシステム アカウントから Active Directory アカウントに変更する方法が示されています。

1. リストで **Connection Server** サービスを右クリックし、**[プロパティ]** を選択します
Connection Server サービス プロパティ ウィンドウが表示されます。
2. **Log On As** セクションで、**System Account** オプションからマークを削除します。
接続設定フィールドは有効です。
3. **Active Directory** ユーザ名とパスワードを入力し、パスワードを確認します。

例：Domain/username

[OK] をクリックします。サービス接続設定が変更されます。

4. **Central Configuration Manager** を終了します。

System DSN 接続設定の例

System DSN 接続設定では、データベースに接続するために必要とされるパラメータが定義されます。以下の例では、インストールされている場合、レポート ポータルでは SQL 認証のサポートだけが行われるので、SQL Server 認証でのユーザ接続を認証する System DSN を作成します。CA Business Intelligence をインストールする前に、CMS データベースの System DSN を設定します。

以下の例では、レポート ポータルの CMS データベース用の System DSN を作成します。

1. **[スタート] - [設定] - [コントロールパネル] - [管理ツール] - [データ ソース (ODBC)]** の順に選択します。
ODBC データ ソース アドミニストレータが表示されます。
2. **[システム DSN]** タブで、**[作成]** を選択します。
[Select a New Data Source] ウィンドウが開きます。
3. 下へスクロールして、**[SQL Server]** を選択してから、**[完了]** をクリックします。
[Create a New Data Source to SQL Server] ウィザードが表示されます。

4. 接続名、説明および SQL サーバ名を入力します。 [次へ] をクリックします。
5. SQL Server 認証を使用するように選択します。
6. 管理者ユーザのクレデンシャルを入力して、SQL サーバに接続します。 [次へ] をクリックします。
7. [Change the default database to option] を選択して、リストからレポート ポータルの CMS データベースを選択します。 [次へ] をクリックします。
8. [完了] をクリックします。接続のテストを選択してから、[OK] をクリックします。

System DSN が作成されます。

Windows 認証で動作するレポート ポータル上でのレポート パッケージのデプロイ

Windows で有効

標準の CA ControlMinder レポートを使用するには、BusinessObjects InfoView にレポート パッケージ ファイルをインポートする必要があります。

注: この手順では、レポート ポータル上に、同じパッケージの旧バージョンがすでにデプロイされていない場合に、レポート パッケージをデプロイする方法について説明します。

レポート ポータルでレポート パッケージをデプロイする方法

1. 中央データベース、配布サーバ、レポート ポータルが設定されていることを確認します。

注: JAVA_HOME 変数がレポート ポータル コンピュータ上でセットアップされていることを確認します。

2. CA ControlMinder のレポート対象データベース用の System DSN を作成して、Windows NT 認証を使用するように指定します。

作成する System DSN は CA ControlMinder のレポート対象データベースに接続するために使用されます。System DSN はレポート パッケージを設定する際に指定します。

3. CA Business Intelligence for Windows DVD を光ディスク ドライブに挿入し、¥Disk1¥cabi¥biconfig フォルダに移動します。

4. biconfig ディレクトリの中身を一時ディレクトリにコピーします。
5. お使いのオペレーティング システム用の適切な CA ControlMinder サーバ コンポーネント DVD を光ディスク ドライブに挿入し、
¥ReportPackages フォルダにアクセスします。
6. 以下のファイルを、光ディスクから同じ一時ディレクトリにコピーします。
 - ¥ReportPackages¥RDBMS¥import_biar_config.xml
 - ¥ReportPackages¥RDBMS¥AC_BIAR_File.biar

RDBMS

CA ControlMinder レポートで使用する RDBMS のタイプを定義します。

値： MSSQL2005

import_biar_config.xml

使用する RDBMS のインポート構成ファイル (.xml) の名前を定義します。

値： import_biar_config_mssql_2005.xml

注： 中央データベースとして MS SQL Server 2008 を使用する場合は、import_biar_config_mssql_2005.xml ファイルを設定します。

AC_BIAR_File.biar

使用する言語と RDBMS の CA ControlMinder レポート ファイル (.biar) の名前を定義します。

注： 使用する RDBMS 用のインポート設定ファイルの <biar-file name> プロパティは、このファイルを指します。デフォルトでは、RDBMS の英語バージョンの名前に設定されます。

7. *import_biar_config.xml* ファイルのコピーを編集します。以下の XML プロパティを定義します。

重要: ファイルからユーザ名、パスワードおよびサーバのフィールドを削除します。

<biar-file name>

CA ControlMinder レポート ファイル (.biar) への完全なパス名を定義します。これは前の手順でコピーしたファイルです。

<networklayer>

使用する RDBMS でサポートされているネットワーク層を定義します。

値: ODBC

<rdms>

CA ControlMinder レポートで使用される RDBMS のタイプを定義します。

値: 汎用 ODBC データ ソース

<datasource>

作成した DSN を定義します。

重要: CA Business Intelligence CMS ではなく、CA ControlMinder によってレポート用に使用されるデータベースの名前を指定します。

8. コマンドプロンプト ウィンドウを開いて、以下のコマンドを入力します。

```
System_Drive:¥B0¥biconfig.bat -h host_name -u user_name -p password -f  
ac_biar_config.xml
```

host_name

レポートポータルのホスト名を定義します。

user_name

レポートポータルをインストールした時に設定したレポートポータル管理者を定義します。

password

レポートポータル管理者のパスワードを定義します。

例:

```
biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f  
C:¥B0¥import_biar_config_mssql_2005.xml
```

例: Windows 認証を使用するように設定された Microsoft SQL Server 2005 Import Configuration ファイル

以下のコード断片が、Windows 認証で動作するレポート ポータル上でデプロイする MS SQL Server 2005 用に編集されたインポート設定ファイル (import_biar_config_mssql2005.xml) の例です。

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:\temp\biconfig\
AccessControl_R12.5_EN_JP_KR_SQL_6_DEC_2009.biar">
        <networklayer>ODBC</networklayer>
        <rdms>Generic ODBC datasource</rdms>
        <datasource>acdb</datasource>
      </biar-file>
    </add>
  </step>
</biconfig>
```

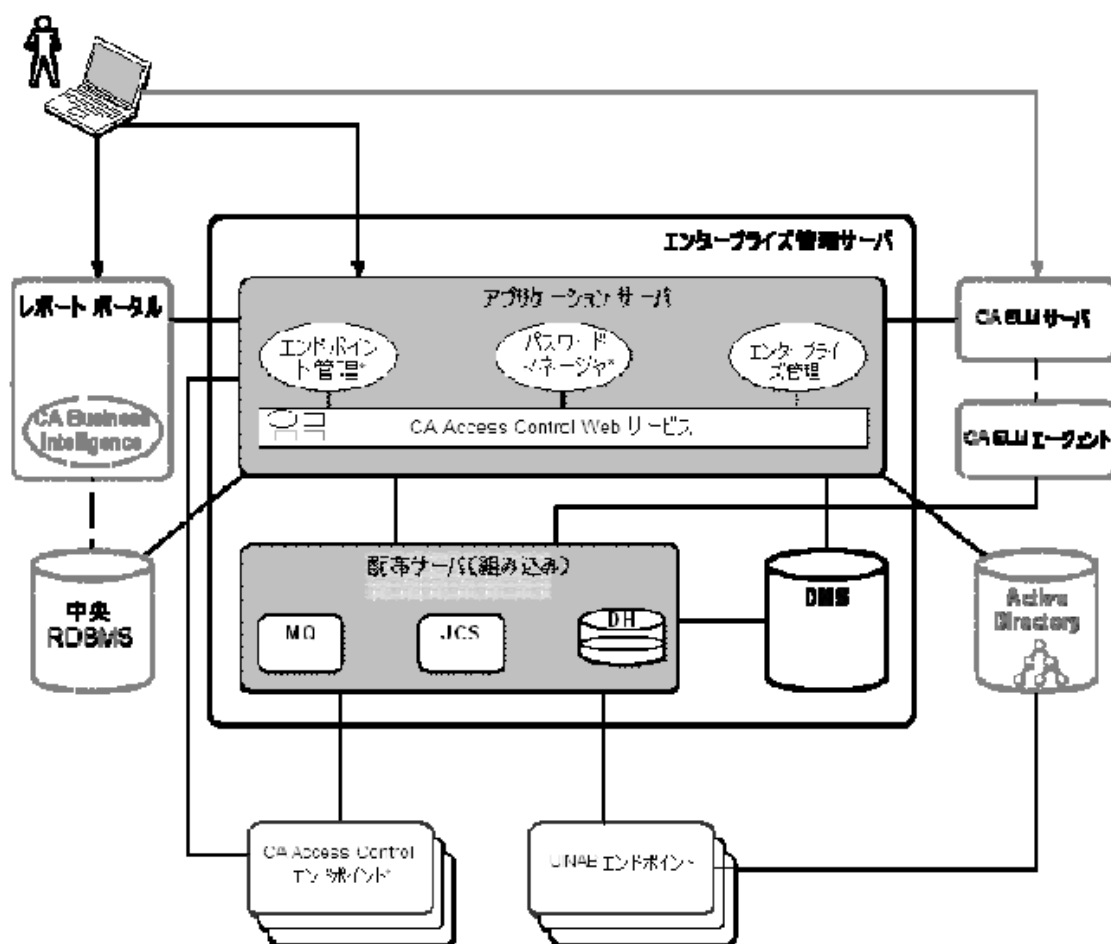

付録 C: CA ControlMinder サービス アカウント設定の変更

このセクションには、以下のトピックが含まれています。

[CA ControlMinder サービス アカウントと CA ControlMinder コンポーネントとの関係 \(P. 600\)](#)
[サービス アカウント パスワード \(P. 602\)](#)
[JNDI 接続アカウントの変更 \(P. 614\)](#)
[メッセージ キューの通信設定の変更 \(P. 618\)](#)
[パスワード変更手順 \(P. 625\)](#)

CA ControlMinder サービス アカウントと CA ControlMinder コンポーネントとの関係

以下の図は、サービス アカウントがさまざまな CA ControlMinder コンポーネントとどのように関わっているかを示しています。



図の中の番号は、以下のサービス アカウントに対応しています。

1. RDBMS_service_user

このアカウントは、エンタープライズ管理サーバと RDBMS の間の通信を認証します。

注: このアカウントの名前は RDBMS_service_user ではありません。CA ControlMinder エンタープライズ管理用にデータベースを準備するためにユーザを作成する際に、このアカウントの名前を指定します。

2. **guest**

このアカウントは、メッセージキューサーバ内のメッセージキューを特定する JNDI 接続アカウントです。

注: インストール後に JNDI 接続アカウントを変更できます。

3. **reportserver**

このアカウントによって、DMS と CA ControlMinder エンタープライズ管理がメッセージキューにログインします。

4. **+reportagent**

このアカウントによって、エンドポイントがメッセージキューにログインします。

5. **+policyfetcher**

このアカウントは、エンドポイント上で **policyfetcher** デーモンまたはサービスを実行します。

6. **+devcalc**

このアカウントは、エンドポイントのポリシー偏差計算を実行します。

7. **ac_entm_pers**

このアカウントは、エンタープライズ管理サーバと DMS の間の通信を認証します。

8. **ADS_LDAP_bind_user**

このアカウントによって、CA ControlMinder エンタープライズ管理が Active Directory に対して LDAP クエリを実行します。

注: このアカウントの名前は **ADS_LDAP_bind_user** ではありません。このアカウントの名前は、CA ControlMinder エンタープライズ管理をインストールするときに Active Directory 設定ウィザードページで指定するユーザ DN になります。

サービス アカウント パスワード

ほとんどの場合、CA ControlMinder サービス アカウントのパスワードは、CA ControlMinder エンタープライズ管理 をインストールする時に設定します。ただし、インストール後にそれらのアカウントのパスワードを変更する必要がある場合があります。たとえば、組織のセキュリティ ポリシーまたはパスワード ポリシーに対応するため、毎年パスワードを変更する必要がある場合があります。

サービス アカウントが 2 つの CA ControlMinder コンポーネントと対話する場合、各コンポーネント上でアカウントのパスワードを変更する必要があります。1 つのコンポーネントのみでパスワードを変更した場合、そのサービス アカウントはもう一方のコンポーネントにログインできません。

RDBMS_service_user のパスワードの変更

RDBMS_service_user アカウントは、エンタープライズ管理サーバと RDBMS の間の通信を認証します。このアカウントの名前は RDBMS_service_user ではありません。このアカウントは、CA ControlMinder エンタープライズ管理 用にデータベースを準備する際に作成します。また、CA ControlMinder エンタープライズ管理 のインストール時に、他のデータベース情報と併せて、アカウント名とパスワードを提供します。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、RDBMS_service_user のパスワードを定期的に変更する必要がある場合があります。パスワードの変更は、エンタープライズ管理サーバおよび RDBMS の両方で行う必要があります。

このアカウントのパスワードを変更する際は、以下の点に注意します。

- このアカウントのデフォルトのパスワードは、ユーザを作成したときに指定したパスワードです。
- パスワードには以下の制限があります。
 - 長さは 1 文字から 50 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - 二重引用符 (") を含むことはできません。
 - RDBMS のパスワードルールを厳守している必要があります。
- パスワードは以下の XML ファイルに格納されます。JBoss_home は、JBoss をインストールしたディレクトリです。

JBoss_home/server/default/conf/login-config.xml

RDBMS_service_user のパスワードを変更する方法

1. 適切なデータベース ツールを使用して、パスワードを変更します。

注: パスワードを変更する方法の詳細については、MS SQL または Oracle のドキュメントを参照してください。

2. エンタープライズ管理サーバのパスワードを変更します。

- a. JBoss アプリケーション サーバを停止します。
- b. [クリア テキスト パスワードを暗号化](#) (P. 630) します。
- c. [login-config.xml ファイル内でパスワードを変更](#) (P. 632) します。
- d. JBoss アプリケーション サーバを再起動します。
- e. CA ControlMinder エンタープライズ管理 にログインできることを確認します。

JBoss が正常に開始され、エンタープライズ管理サーバでパスワードが変更されます。

RDBMS_service_user パスワードはすべての場所で変更されます。

例: login-config.xml ファイルでパスワードを変更

login-config.xml ファイルの以下のスニペットは、RDMBS_service_user の変更されたパスワードの 1 つのインスタンスを示しています。ユーザの名前は caidb01 です。パスワードは次のように暗号化されています: }>8:Jt^+%INK&i^v:

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
      code="com.netegrity.jboss.datasources.PasswordEncryptedLogin"
      flag="required">
      <module-option name="userName">caidb01</module-option>
      <module-option name="password">
        {AES}:}>8:Jt^+%INK&i^v==</module-option>
      <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
      </login-module>
    </authentication>
  </application-policy>
```

reportserver のパスワードの変更

CA ControlMinder エンタープライズ管理 および DMS は、メッセージキューへの接続に reportserver アカウントを使用します。

CA ControlMinder エンタープライズ管理 は、reportserver を使用して以下を実行します。

- CA Enterprise Log Manager へレポート データを送信
- UNAB リモート移行コマンドを送信
- SAM エンドポイント上の SAM エージェントに特権アカウント パスワードを提供
- CA ControlMinder エンドポイントからレポート データを受信

DMS は、**reportserver** アカウントを使用して以下を実行します。

- UNAB エンドポイントに UNAB ポリシーを送信
- UNAB エンドポイントから送信されたポリシー展開ステータス情報を受信

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、**reportserver** のパスワードを定期的に変更する必要がある場合があります。パスワードの変更は、配布サーバ、エンタープライズ管理サーバ、DMS 上で行う必要があります。

reportserver のパスワードを変更する際は、以下の点に注意します。

- このアカウントのデフォルトのパスワードは、**CA ControlMinder** エンタープライズ管理 をインストールするときに指定した通信用パスワードです。
- パスワードには以下の制限があります。
 - 長さは 1 文字から 240 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - 二重引用符 (") を含むことはできません。
- パスワードは、メッセージ キューおよび以下の XML ファイルに格納されます。*JBoss_home* は、JBoss をインストールしたディレクトリです。
 - *JBoss_home*/server/default/deploy/properties-service.xml
 - *JBoss_home*/server/default/conf/login-config.xml

重要: 企業で複数の配布サーバを持っている場合は、まずエンタープライズ管理サーバにインストールされた配布サーバ上でパスワードを変更し、次に、他の配布サーバ上でパスワードを変更します。

reportserver のパスワードを変更する方法

1. 配布サーバで、[reportserver ユーザ用のメッセージキュー パスワードを設定](#) (P. 628) します。

配布サーバで reportserver のパスワードが変更されました。

2. エンタープライズ管理サーバで、以下のとおりパスワードを変更します。
 - a. JBoss アプリケーション サーバを停止します。
 - b. [クリア テキスト パスワードを暗号化](#) (P. 630) します。
 - c. [properties-service.xml ファイル内でパスワードを変更](#) (P. 631) します。
 - d. [login-config.xml ファイル内でパスワードを変更](#) (P. 632) します。
 - e. JBoss アプリケーション サーバを再起動します。
 - f. CA ControlMinder エンタープライズ管理 にログインできることを確認します。

JBoss が正常に開始され、エンタープライズ管理サーバでパスワードが変更されます。

3. [sechkey を使用して DMS 上で reportserver のパスワードを変更](#) (P. 626) します。

reportserver パスワードはすべての場所に変更されます。

例: reportserver ユーザ用のメッセージ キュー パスワードを設定

この Tibco EMS 管理ツール コマンドは、reportserver ユーザ用にメッセージキュー パスワードを設定します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
ssl://localhost:7243> set password reportserver "secret"  
Password of user 'reportserver' has been modified  
ssl://localhost:7243>
```

例: properties-service.xml ファイルでパスワードを変更

properties-service.xml ファイルの以下のスニペットは、reportserver の変更されたパスワードを示しています。パスワードは次のように暗号化されています: }>8:Jt^+%INK&i^v:

```
<attribute name="Properties">
    SamMDB.mdb-user=reportserver
    <!-- encoded tibco password -->
    SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

例: login-config.xml ファイルでパスワードを変更

login-config.xml ファイルの以下のスニペットは、reportserver の変更されたパスワードを示しています。パスワードは次のように暗号化されています: }>8:Jt^+%INK&i^v:

```
<application-policy name="JmsXATibcoRealm">
    <authentication>
        <login-module
            code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
            <module-option name="userName">reportserver</module-option>
            <module-option
                name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
            <module-option name="managedConnectionFactoryName">
                jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
            </login-module>
        </authentication>
    </application-policy>
```

例: sechkey を使用して DMS 上でメッセージキューのパスワードを変更

以下のコマンドは、DMS 上でメッセージキューのパスワードを変更します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
sechkey -t -server -pwd "secret"
```

+reportagent のパスワードの変更

+reportagent アカウントは、エンドポイントでメッセージキューへのログインに使用されます。各エンドポイントでは、UNAB エージェント、SAM エージェント、およびレポート エージェントが、このアカウントを使用してメッセージキューと通信します。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、+reportagent のパスワードを定期的に変更する必要がある場合があります。パスワードの変更は、メッセージキューおよびエンドポイントの両方で行う必要があります。

+reportagent のパスワードを変更する際は、以下の点に注意します。

- デフォルトのパスワードは、CA ControlMinder エンタープライズ管理をインストールするときに指定した通信用パスワードです。
- パスワードには以下の制限があります。
 - 長さは 1 文字から 240 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - 二重引用符 (") を含むことはできません。
- パスワードは、エンドポイント (seosdb) 上の CA ControlMinder データベースおよびメッセージキューに格納されます。

重要: 企業で複数の配布サーバを持っている場合は、まずエンタープライズ管理サーバにインストールされた配布サーバ上でパスワードを変更し、次に、他の配布サーバ上でパスワードを変更します。メッセージキューは、配布サーバの一部です。

+reportagent のパスワードを変更する方法

1. 配布サーバで、[+reportagent ユーザ用のメッセージ キュー パスワードを設定](#) (P. 628) します。

メッセージ キューで +reportagent のパスワードが変更されます。

2. エンドポイントでメッセージ キューに接続するために、レポート エージェントが使用する[パスワードを sechkey を使用して変更](#) (P. 626) します。

+reportagent のパスワードの変更は、エンドポイントに継承されます。

注: selang を使用して、エンドポイント上で +reportagent パスワードを変更することもできます。ただし、ユーザ パスワードを設定するために拡張ポリシー管理を使用できないので、ポリシーを使用して selang コマンドを継承させることはできません。

例: +reportagent ユーザ用のメッセージ キュー パスワードを設定

この Tibco EMS 管理ツール コマンドは、+reportagent ユーザ用にメッセージ キュー パスワードを設定します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
ssl://localhost:7243> set password +reportagent "secret"  
Password of user '+reportagent' has been modified  
ssl://localhost:7243>
```

例: sechkey を使用してエンドポイント上でメッセージ キューのパスワードを変更

以下のコマンドは、+reportagent ユーザのメッセージ キュー パスワードを、配布サーバにサブスクライブされるエンドポイントに継承させます。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
sechkey -t -pwd "secret"
```

+policyfetcher パスワードの変更

+policyfetcher アカウントは、policyfetcher デーモン（サービス）を実行します。このデーモンは、DH 上の展開タスクを検索し、ローカルの CA ControlMinder データベース (seosdb) にポリシー更新を適用し、DH にハートビートを定期的に送信します。CA ControlMinder では、SPECIALPGM ルールを使用して +policyfetcher をシステム ユーザとして定義します。+policyfetcher は、Windows で NT Authority¥System ユーザとして実行されます。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、+policyfetcher のパスワードを定期的に変更する必要がある場合があります。

+policyfetcher のパスワードを変更する際は、以下の点に注意します。

- このアカウントのデフォルトのパスワードはありません。CA ControlMinder では、インストール中に +policyfetcher 用のパスワードを設定しません。
- パスワードには以下の制限があります。
 - 長さは 1 文字から 240 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - 二重引用符 (") を含むことはできません。
- パスワードはローカルの CA ControlMinder データベース (seosdb) に格納されます。

重要: このユーザが CA ControlMinder データベースにログインするのを妨ぐため、このユーザにはパスワードを設定しないことをお勧めします。

+policyfetcher のパスワードを変更する場合は、[selang を使用してパスワードを変更](#) (P. 625) します。

例: +policyfetcher のパスワードを変更

以下のコマンドは、+policyfetcher ユーザのパスワードを変更します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
Successfully updated USER +policyfetcher
```

+devcalc のパスワードの変更

+devcalc アカウントは、ポリシー偏差計算を実行します。つまり、ポリシー展開の結果としてエンドポイントに展開される予定のアクセス ルールと、同じエンドポイントにすでに展開された実際のルールとの差異を計算します。CA ControlMinder では、SPECIALPGM ルールを使用して +devcalc をシステム ユーザとして定義します。+devcalc は、Windows で NT Authority¥System ユーザとして実行されます。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、+devcalc のパスワードを定期的に変更する必要がある場合があります。

+devcalc のパスワードを変更する際は、以下の点に注意します。

- このアカウントのデフォルトのパスワードはありません。CA ControlMinder では、インストール中に +devcalc 用のパスワードを設定しません。
- パスワードには以下の制限があります。
 - 長さは 1 文字から 240 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - 二重引用符 (") を含むことはできません。
- パスワードはローカルの CA ControlMinder データベース (seosdb) に格納されます。

重要: このユーザが CA ControlMinder データベースにログインするのを妨ぐため、このユーザにはパスワードを設定しないことをお勧めします。

+devcalc のパスワードを変更する場合は、[selang を使用してパスワードを変更](#) (P. 625) します。

例: +devcalc のパスワードを変更

以下のコマンドは、+devcalc ユーザのパスワードを変更します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
AC> cu +devcalc password("secret") grace- nonative
(localhost)
Successfully updated USER +devcalc
```

ac_entm_pers のパスワードの変更

ac_entm_pers アカウントは、DMS とエンタープライズ管理サーバの間の通信を認証します。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、ac_entm_pers のパスワードを定期的に変更する必要がある場合があります。パスワードの変更は、RDBMS と DMS の両方で行う必要があります。

ac_entm_pers パスワードを変更する際は、以下の点に注意します。

- デフォルトのパスワードは、インストール中に CA ControlMinder によってランダムに生成されるパスワードです。
- パスワードには以下の制限があります。
 - 長さは 1 文字から 48 文字までに限られます。
 - 二重引用符 (") を含めることはできません。
 - 拡張 ASCII 文字を含めることはできません。
- パスワードは RDBMS と DMS 内に格納されます。

ac_entm_pers のパスワードを変更する方法

1. [selang を使用して DMS で ac_entm_pers のパスワードを変更](#) (P. 625) します。
2. CA ControlMinder エンタープライズ管理 では、DMS への接続を設定し、新しいパスワードを指定します。

ac_entm_pers パスワードはすべての場所を変更されます。

注: DMS への接続の設定の詳細については、*CA ControlMinder エンタープライズ管理* のオンライン ヘルプを参照してください。

例: selang を使用して ac_entm_pers のパスワードを変更

以下のコマンドは、DMS に接続して ac_entm_pers ユーザのパスワードを変更します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
AC> eu ac_entm_pers admin auditor nonative password(secret) logical nonative grace-
```

ADS_LDAP_bind_user のパスワードの変更

ADS_LDAP_bind_user アカウントは、CA ControlMinder エンタープライズ管理で Active Directory に対する LDAP クエリの実行に使用します。このアカウントの名前は ADS_LDAP_bind_user ではありません。このアカウントの名前は、CA ControlMinder エンタープライズ管理をインストールするときに Active Directory 設定ウィザード ページで指定する ユーザ DN になります。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、ADS_LDAP_bind_user のパスワードを定期的に変更する必要がある場合があります。パスワードの変更は、Active Directory と RDBMS の両方で行う必要があります。

ADS_LDAP_bind_user のパスワードを変更する際は、以下の点に注意します。

- デフォルトのパスワードは、CA ControlMinder エンタープライズ管理をインストールするときに Active Directory 設定ウィザード ページで指定したパスワードです。
- パスワードには以下の制限があります。
 - 長さは 7 文字から 120 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - コロン (:) を含めることはできません。
 - Active Directory パスワードルールを厳守する必要があります。
- パスワードは Active Directory と RDBMS に格納されます。

ADS_LDAP_bind_user のパスワードを変更する方法

1. Active Directory ツールを使用して、Active Directory でパスワードを変更します。

注: パスワードを変更する方法の詳細については、Active Directory のドキュメントを参照してください。

2. [CA IdentityMinder 管理コンソールでユーザ ディレクトリのパスワードを変更](#) (P. 635) します。

ADS_LDAP_bind_user パスワードはすべての場所に変更されます。

JNDI 接続アカウントの変更

JNDI 接続アカウントは、**guest** という名前が付けられ、メッセージキューサーバ内のメッセージキューを特定します。デフォルトでは、このアカウントにはパスワードがありません。

メッセージキューサーバ内でメッセージキューを特定するために JNDI が使用するアカウントは変更できます。このアカウントの名前は、メッセージキューおよび以下の XML ファイルに格納されます。**JBoss_home** は、JBoss をインストールしたディレクトリです。

```
JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml
```

JNDI 接続アカウントを変更する方法

1. メッセージキューのユーザを作成します。
2. JNDI 接続アカウントを以下の手順で変更します。
 - a. JBoss アプリケーションサーバを停止します。
 - b. **tibco-jms-ds.xml** ファイル内のアカウント名を、作成したメッセージキューユーザの名前で置換します。
 - c. JBoss アプリケーションサーバを再起動します。
 - d. CA ControlMinder エンタープライズ管理 にログインできることを確認します。

JBoss が正常に開始され、JNDI 接続アカウントが変更されます。

メッセージキューユーザの作成

JNDI 接続アカウントを変更する際は、メッセージキューユーザを作成します。

メッセージキューユーザを作成する方法

1. 以下のディレクトリに移動します（**DistServer** は配布サーバをインストールしたディレクトリです）。

```
DistServer/MessageQueue/tibco/ems/5.1/bin
```

2. (UNIX) 以下のコマンドを入力します。

```
tibemsadmin
```

Tibco EMS 管理ツールが起動します。

3. (Windows) 以下のコマンドを入力します。

```
tibemsadmin.exe
```

Tibco EMS 管理ツールが起動します。

4. 以下のいずれかのコマンドを使用して、現在の環境に接続します。

- 配布サーバがポート **7222** (デフォルト ポート) でレポート エージェントをリスニングする場合は、以下のコマンドを使用します。

```
connect
```

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

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

5. ユーザ名およびパスワードを入力します。

注: デフォルトのユーザ名は **admin** で、パスワードは **CA ControlMinder** エンタープライズ管理 のインストール時に指定した通信用パスワードです。

メッセージキューに接続します。

6. 以下のコマンドを入力します。

```
create user username
```

username

新しいメッセージ キュー ユーザの名前を指定します。

新しいユーザが作成されます。

例: メッセージ キュー ユーザを作成

以下の Tibco EMS 管理ツール コマンドは、**example** という名前のメッセージ キュー ユーザを作成します。

```
> connect SSL://7243
Login name (admin): admin
Password:
Connected to: ssl://localhost:7243
ssl://localhost:7243> create user example
User 'example' has been created
ssl://localhost:7243>
```

tibco-jms-ds.xml ファイルでのアカウントの変更

JNDI 接続アカウントを変更する際は、tibco-jms-ds.xml ファイル内のアカウントを変更します。

tibco-jms-ds.xml ファイルでアカウントを変更する方法

1. JBoss アプリケーション サーバが停止していない場合は、停止します。
2. 以下のディレクトリに移動します (*JBoss_home* は、JBoss をインストールしたディレクトリです)。

JBoss_home/server/default/deploy/jms

3. tibco-jms-ds.xml ファイルをテキスト エディタで開きます。
4. 以下のパラメータの終わりでアカウント名を変更します。

`java.naming.security.principal=`

5. ファイルを保存して閉じます。

例: tibco-jms-ds.xml ファイルでアカウント名を変更

tibco-jms-ds.xml ファイルの以下のスニペットは、変更された JNDI 接続アカウントを示します。アカウントの名前は **example** になります。

```
<!-- The JMS provider loader -->
  <mbean code="org.jboss.jms.jndi.JMSProviderLoader"
    name=":service=JMSProviderLoader,name=TibjmsProvider">
    <attribute name="ProviderName">TIBCOJMSProvider</attribute>
    <attribute name="ProviderAdapterClass">
      org.jboss.jms.jndi.JNDIProviderAdapter</attribute>
    <attribute
name="FactoryRef">SSLXAQueueConnectionFactory</attribute>
    <attribute
name="QueueFactoryRef">SSLXAQueueConnectionFactory</attribute>
    <attribute
name="TopicFactoryRef">SSLXATopicConnectionFactory</attribute>
    <attribute name="Properties">
      java.naming.security.principal=example

      java.naming.factory.initial=com.tibco.tibjms.naming.TibjmsInitialContextF
actory

      java.naming.provider.url=tibjmsnaming://localhost:7243
      java.naming.factory.url.pkgs=com.tibco.tibjms.naming
      com.tibco.tibjms.naming.security_protocol=ssl
      com.tibco.tibjms.naming.ssl_enable_verify_host=false

    </attribute>
  </mbean>
```

メッセージ キューの通信設定の変更

メッセージ キューの以下の通信設定は変更することができます。

- メッセージ キュー管理者のパスワード
- メッセージ キューのサーバ証明書
- メッセージ キューの URL
- メッセージ キューの SSL キーストア用のパスワード
- メッセージ キューに接続するためにエンドポイントが使用するパスワード

注: エンドポイントでは、+reportagent サービス アカウントを使用してメッセージ キューに接続します。

- メッセージ キューに接続するために CA ControlMinder エンタープライズ管理 と DMS が使用するパスワード

注: CA ControlMinder エンタープライズ管理 および DMS では、reportserver サービス アカウントを使用してメッセージ キューに接続します。

詳細情報:

[+reportagent のパスワードの変更](#) (P. 608)

[reportserver のパスワードの変更](#) (P. 604)

メッセージ キュー管理者パスワードの変更

メッセージ キューの管理者アカウントは **admin** という名前で、メッセージ キューで管理タスクを実行できます。

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、**admin** のパスワードを定期的に変更する必要がある場合があります。

メッセージ キュー管理者パスワードを変更する際は、以下の点に注意します。

- このアカウントのデフォルトのパスワードは、**CA ControlMinder エンタープライズ管理** をインストールするときに指定した通信用パスワードです。
- パスワードには以下の制限があります。
 - 長さは **1 文字から 240 文字**までに限られます。
 - 拡張 **ASCII 文字**を含むことはできません。
 - 二重引用符 (") を含むことはできません。
- パスワードはメッセージ キューに格納されます。

重要: 企業で複数の配布サーバを持っている場合は、まずエンタープライズ管理サーバにインストールされた配布サーバ上でパスワードを変更し、次に、他の配布サーバ上でパスワードを変更します。メッセージ キューは、配布サーバの一部です。

メッセージ キュー管理者パスワードを変更するには、[admin ユーザ用のメッセージ キュー パスワードを設定](#) (P. 628) します。

例: admin ユーザ用のメッセージ キュー パスワードを設定

以下の Tibco EMS 管理ツール コマンドは、**admin ユーザ**用にメッセージ キュー パスワードを設定します。パスワードは **"secret"** です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
ssl://localhost:7243> set password admin "secret"
Password of user 'admin' has been modified
ssl://localhost:7243>
```

メッセージ キューのサーバ証明書の変更

メッセージ キューは、メッセージ キューとそのクライアントの間に、SSL 通信用のサーバ証明書を使用します。メッセージ キュー クライアントは、CA ControlMinder エンドポイントおよび CA ControlMinder エンタープライズ管理 です。

メッセージ キューのサーバ証明書を変更する方法

1. CA ControlMinder メッセージ キューを停止します。

2. X.509 サーバ証明書を作成します。

.p12 形式の証明書を作成することをお勧めします。

3. 以下のディレクトリに移動します (*DistServer* は配布サーバをインストールしたディレクトリです) 。

DistServer/MessageQueue/tibco/bin/ems

4. 以下のコマンドを入力します。

```
tibemsadmin -mangle password  
password
```

サーバ証明書のパスワードを指定します。

サーバ証明書のパスワードが暗号化されます。

5. *tibemsd.conf* ファイルをテキスト エディタで開きます。 このファイルは以下のディレクトリにあります。

DistServer/MessageQueue/tibco/bin/ems

6. 以下のパラメータの値を変更します。

ssl_server_identity

サーバ証明書の完全パスを指定します。

ssl_server_key

サーバ証明書鍵の完全パスを指定します。

注: .p12 証明書を使用する場合は、このパラメータを空白のままにします。

ssl_password

サーバ証明書の暗号化されたパスワードを指定します。

7. ファイルを保存して閉じます。
メッセージ キューのサーバ証明書が変更されます。
8. CA ControlMinder メッセージ キュー サービスを再起動します。

例: tibemds.conf ファイル

以下は、.p12 サーバ証明書用の tibemds.conf ファイル内のメッセージ キュー サーバパラメータの例です。パスワードは「}>8:Jt^+%lNK&i^v」に暗号化され、ssl_server_key パラメータには値がありません。

```
ssl_server_identity    = "C:%Program
Files%CA%AccessControlServer%MessageQueue%conf%keystore.p12"
ssl_server_key         =
ssl_password           = }>8:Jt^+%lNK&i^v
```

メッセージ キュー SSL キーストアのパスワードの変更

メッセージ キューの SSL キーストアには、メッセージ キューが SSL 通信で使用するサーバ証明書が格納されます。メッセージ キュー SSL キーストア用のパスワードを変更する際は、サーバ証明書を署名する公開鍵/秘密鍵のペアを更新します。

組織のセキュリティ ポリシーおよびパスワード ポリシーに対応するため、メッセージ キュー SSL キーストアのパスワードを定期的に変更する必要がある場合があります。

メッセージ キュー SSL キーストアのパスワードを変更する際は、以下の点に注意します。

- デフォルトのパスワードは、CA ControlMinder エンタープライズ管理をインストールするときに指定した通信用パスワードです。
- パスワードには以下の制限があります。
 - 長さは 6 文字から 50 文字までに限られます。
 - 拡張 ASCII 文字を含むことはできません。
 - 二重引用符 (") を含むことはできません。
- パスワードは以下のファイルに格納されます。ACServer は、CA ControlMinder エンタープライズ管理をインストールしたディレクトリです。

ACServer/MessageQueue/conf/keystore.p12

重要: 企業で複数の配布サーバを持っている場合は、まずエンタープライズ管理サーバにインストールされた配布サーバ上でパスワードを変更し、次に、他の配布サーバ上でパスワードを変更します。メッセージ キューは、配布サーバの一部です。

メッセージ キュー SSL キーストアのパスワードを変更する方法

1. CA ControlMinder メッセージ キュー サービスを停止します。
2. コマンドプロンプト ウィンドウを開き、以下のディレクトリに移動します (*JDK* は Java Development Kit をインストールしたディレクトリです)。

JDK/bin

3. 以下のコマンドを実行します。

```
keytool -genkey -keyalg RSA -keysize 1024 -keystore "keystore.p12" -storetype PKCS12 -dname "cn=acmq" -alias acmq -storepass "password" -keypass "password"
```

コマンドによって鍵のペア（公開鍵と秘密鍵）を作成することを指定します。

-keyalg RSA

鍵のペアの生成に **RSA** アルゴリズムを使用することを指定します。

-keysize 1024

生成される鍵のサイズが **1024** ビットであることを指定します。

-storetype PKCS12

生成される鍵が **PKCS12** ファイル形式であることを指定します。

-dname "cn=acmq"

生成される証明書の **X.500** 識別名が **acmq** であることを指定します。この名前は、証明書の発行者と所有者のフィールドで使用されます。

-alias acmq

acmq という名前のキーストア エントリを更新することを指定します。

-storepass "password"

メッセージ キュー SSL キーストアを保護するパスワードを指定します。このパスワードは、**-keypass** パラメータに指定したパスワードと同一である必要があります。

-keypass "password"

新しい鍵のペアの秘密鍵を保護するパスワードを指定します。このパスワードは、**-storepass** パラメータに指定したパスワードと同一である必要があります。

keytool ユーティリティは、メッセージ キュー SSL キーストア用のパスワードを変更します。

4. 以下のディレクトリに移動します (*DistServer* は配布サーバをインストールしたディレクトリです)。

DistServer/MessageQueue/tibco/bin/ems

5. 以下のコマンドを実行します。

```
tibemsadmin -mangle password
```

SSL キーストア用のパスワードが暗号化されます。

New Topic (320)

メッセージ キューではローカルホストが **URL** として使用されます。
tibco-jms-ds.xml ファイルを変更することで、**URL** を変更して、ホストの完全修飾識別名 (**FQDN**) を使用できます。

URL 情報は、以下の **XML** ファイルのメッセージ キューに格納されます。
JBoss_HOME は、JBoss がインストールされたディレクトリです。

`JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml`

次の手順に従ってください:

1. JBoss アプリケーション サーバ、CA ControlMinder メッセージ キュー サービス、およびすべての CA ControlMinder サービスを停止します。

2. 以下の場所にある **tibco-jms-ds.xml** ファイルをバックアップします。

`JBoss_home¥server¥default¥deploy¥jms`

3. **tibco-jms-ds.xml** ファイルを開き、以下の手順に従います。

- a. **localhost** を見つけます。
- b. **localhost** を **FQDN** に置換します。
- c. **localhost** のすべてのインスタンスに対して、手順 **a** および **b** を実行します。
- d. ファイルを保存して閉じます。

4. 以下の場所を参照して、通信キーを変更します。

`HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Common¥communication`

5. キー値 **Distribution_Server** を見つけます。

デフォルト値は `ssl://localhost:7243` です。

6. `ssl://localhost:7243` 値を `ssl://<FQDN>:7243` に置換します。

7. CA ControlMinder メッセージ キュー サービスを含む、すべての CA ControlMinder サービスを開始します。

8. JBoss サービスを開始します。

CA ControlMinder メッセージ キュー **URL** が変更されます。

パスワード変更手順

以下の手順では、CA ControlMinder パスワードを変更するためのさまざまな方法について説明します。

selang を使用したパスワードの変更

selang を使用して、以下のサービス アカウントのパスワードを変更できます。

- +policyfetcher
- +devcalc
- ac_entm_pers

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、これらのアカウントのパスワードを定期的に変更する必要がある場合があります。

selang を使用してパスワードを変更する際は、以下の点に注意します。

- パスワードは二重引用符で囲む必要があります。
- 拡張ポリシー管理を使用して、パスワード変更コマンドを継承させることはできません。

注: サービス アカウントが対話するすべてのコンポーネント上でパスワードを変更するために複数の方式を使用する必要がある場合があります。

selang を使用してパスワードを変更するには、以下のコマンドを実行します。

```
cu user password("password") grace- nonative
```

ユーザ

パスワードが変更されるユーザの名前を指定します。

password

新しいパスワードを指定します。

注: パスワードをコマンドにカット アンド ペーストする場合は、パスワードに CR（キャリッジリターン）または LF（ラインフィード）が含まれていないことを確認します。

例: +policyfetcher のパスワードを変更

以下のコマンドは、+policyfetcher ユーザのパスワードを変更します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
Successfully updated USER +policyfetcher
```

詳細情報:

[+policyfetcher パスワードの変更](#) (P. 610)

[+devcalc のパスワードの変更](#) (P. 611)

sechkey を使用したメッセージ キュー パスワードの変更

sechkey を使用して、以下のサービス アカウントのパスワードを変更できます。

- reportserver
- +reportagent

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、これらのアカウントのパスワードを定期的に変更する必要がある場合があります。 sechkey を使用してパスワードを変更する場合は、パスワードを二重引用符で囲む必要があります。

注: サービス アカウントが対話するすべてのコンポーネント上でパスワードを変更するために複数の方式を使用する必要がある場合があります。

`sechkey` を使用してメッセージ キューのパスワードを変更するには、配布サーバで以下のコマンドを実行します。

```
{sechkey | acuxchkey} -t [-server] -pwd "password"
```

`sechkey`

CA ControlMinder エンドポイント上でパスワードを変更することを指定します。

`acuxchkey`

UNAB エンドポイント上でパスワードを変更することを指定します。

`-server`

DMS 上でパスワードを変更することを指定します。

注: このパラメータは `sechkey` パラメータでのみ有効です。

`password`

新しいパスワードを指定します。

注: パスワードをコマンドにカット アンド ペーストする場合は、パスワードに CR (キャリッジリターン) または LF (ラインフィード) が含まれていないことを確認します。

例: UNAB エンドポイント上でメッセージ キューのパスワードを変更

以下のコマンドは、配布サーバと通信するすべての UNAB エンドポイントへメッセージ キューのパスワードを継承させます。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
acuxchkey -t -pwd "secret"
```

例: DMS 上でメッセージ キューのパスワードを変更

以下のコマンドは、DMS 上でメッセージ キューのパスワードを変更します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
sechkey -t -server -pwd "secret"
```

詳細情報:

[+reportagent のパスワードの変更](#) (P. 608)

[reportserver のパスワードの変更](#) (P. 604)

メッセージ キューのパスワードの設定

メッセージ キューのパスワードを設定して、以下のサービス アカウントのパスワードを変更できます。

- reportserver
- +reportagent

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、これらのアカウントのパスワードを定期的に変更する必要がある場合があります。メッセージ キューのパスワードを設定する際は、パスワードを二重引用符で囲む必要があります。

注: サービス アカウントが対話するすべてのコンポーネント上でパスワードを変更するために複数の方式を使用する必要がある場合があります。

メッセージ キューのパスワードを設定する方法

1. 以下のディレクトリに移動します (*DistServer* は配布サーバをインストールしたディレクトリです)。

```
DistServer/MessageQueue/tibco/ems/5.1/bin
```

2. (UNIX) 以下のコマンドを入力します。

```
tibemsadmin
```

Tibco EMS 管理ツールが起動します。

3. (Windows) 以下のコマンドを入力します。

```
tibemsadmin.exe
```

Tibco EMS 管理ツールが起動します。

4. 以下のいずれかのコマンドを使用して、現在の環境に接続します。

- 配布サーバがポート **7222** (デフォルトポート) でレポートエージェントをリスニングする場合は、以下のコマンドを使用します。

```
connect
```

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

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

5. ユーザ名およびパスワードを入力します。

注: デフォルトのユーザ名は **admin** で、パスワードは **CA ControlMinder** エンタープライズ管理 のインストール時に指定した通信用パスワードです。

メッセージキューに接続します。

6. 以下のコマンドを実行します。

```
set password user "password"
```

ユーザ

パスワードが変更されるユーザの名前を指定します。

"password"

新しいパスワードを指定します。

ユーザのパスワードがメッセージキューで変更されます。

注: パスワードをコマンドにカットアンドペーストする場合は、パスワードに **CR** (キャリッジリターン) または **LF** (ラインフィード) が含まれていないことを確認します。

例: reportserver ユーザ用のメッセージキューパスワードを設定

この Tibco EMS 管理ツール コマンドは、reportserver ユーザ用にメッセージキューパスワードを設定します。パスワードは "secret" です。このパスワードはクリアテキストで指定し、二重引用符で囲む必要があります。

```
> connect SSL://7243
Login name (admin): admin
Password:
Connected to: ssl://localhost:7243
ssl://localhost:7243> set password reportserver "secret"
Password of user 'reportserver' has been modified
ssl://localhost:7243>
```

詳細情報:

[+reportagent のパスワードの変更](#) (P. 608)

[reportserver のパスワードの変更](#) (P. 604)

クリア テキスト パスワードの暗号化

以下のサービス アカウント用にクリア テキスト パスワードを暗号化します。

- RDBMS_service_user
- reportserver

パスワードは JBoss ディレクトリ内のクリア テキスト XML ファイルに格納されるため、暗号化します。クリア テキスト パスワードを暗号化するためには **pwdtools** ユーティリティを使用します。

暗号化されたパスワードで改行記号が誤って選択されないようにするため、暗号化されたパスワード（ユーティリティの出力）はテキスト ファイルに出力することをお勧めします。 そうしないと、暗号化されたパスワードが 1 行に収まらない場合に改行が挿入される可能性があります。

pwdtools を使用してクリア テキスト パスワードを暗号化する際は、パスワードを二重引用符で囲む必要があります。

クリア テキスト パスワードを暗号化する方法

1. コマンドプロンプト ウィンドウを開きます。
2. 以下のディレクトリに移動します（**ACServerInstallDir** は **CA ControlMinder エンタープライズ管理** をインストールしたディレクトリです）。

ACServerInstallDir/IAM Suite/Access Control/tools/PasswordTool

3. 以下のコマンドを実行します。

```
pwdtools -FIPS -p "password" -k [filename]
```

password

クリア テキスト パスワードを指定します。

filename

暗号化されたパスワードが **pwdtools** によって出力されるファイル名を指定します。

pwdtools がパスワードを暗号化します。

例: クリア テキスト パスワードの暗号化

以下のコマンドは、クリア テキスト パスワードを暗号化し、暗号化されたパスワードを **pw.txt** ファイルに出力します。クリア テキスト パスワードは "secret" で、二重引用符で囲まれている必要があります。

```
C:\Program Files\CA\AccessControlServer\IAM Suite\Access  
Control\tools>PasswordTool>  
pwdtools.bat -FIPS -p "secret" -key  
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegrity\c  
onfig\keys\FIPSkey.dat"
```

詳細情報:

[reportserver のパスワードの変更 \(P. 604\)](#)

[RDBMS_service_user のパスワードの変更 \(P. 602\)](#)

properties-service.xml ファイルでのパスワードの変更

reportserver アカウントのパスワードを変更するには、**properties-service.xml** ファイル内のパスワードを変更します。組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、このアカウントのパスワードを定期的に変更する必要がある場合があります。

注: サービス アカウントが対話するすべてのコンポーネント上でパスワードを変更するために複数の方式を使用する必要がある場合があります。

properties-service.xml ファイルでパスワードを変更する方法

1. JBoss アプリケーション サーバを停止します。
2. 以下のディレクトリに移動します (*JBoss_home* は、JBoss をインストールしたディレクトリです)。

JBoss_home/server/default/deploy
3. **properties-service.xml** ファイルをテキスト エディタで開きます。
4. **SamMDB.mdb-passwd** パラメータ内のパスワードを変更します。
5. ファイルを保存して閉じます。

例: properties-service.xml ファイルでパスワードを変更

properties-service.xml ファイルの以下のスニペットは、reportserver の変更されたパスワードを示しています。パスワードは次のように暗号化されています: }>8:Jt^+%INK&i^v:

```
<attribute name="Properties">
    SamMDB.mdb-user=reportserver
    <!-- encoded tibco password -->
    SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

詳細情報:

[reportserver のパスワードの変更](#) (P. 604)

login-config.xml ファイルでのパスワードの変更

以下のサービス アカウント用のパスワードを変更するには、login-config.xml ファイル内のパスワードを変更します。

- RDBMS_service_user
- reportserver

組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、これらのアカウントのパスワードを定期的に変更する必要がある場合があります。

注: サービス アカウントが対話するすべてのコンポーネント上でパスワードを変更するために複数の方式を使用する必要がある場合があります。パスワードがクリア テキスト パスワードである場合は、login-config.xml ファイルでパスワードを変更する前に、pwdtools ユーティリティを使用してパスワードを暗号化します。

login-config.xml ファイルでパスワードを変更する方法

1. JBoss アプリケーション サーバを停止します。
2. 以下のディレクトリに移動します (JBoss_home は、JBoss をインストールしたディレクトリです)。

JBoss_home/server/default/conf

3. login-config.xml ファイルをテキスト エディタで開きます。

4. RDBMS_service_user のパスワードを以下の手順で変更します。

- a. ファイル内で RDBMS_service_user アカウントの名前の各インスタンスを特定します。

ファイル内には 6 つのインスタンスがあります。このアカウントの名前は、CA ControlMinder エンタープライズ管理用にデータベースを準備するためにユーザを作成する際に指定します。

- b. 名前の各インスタンスの直後にあるパラメータ内でパスワードを変更します。

パラメータは `<module-option name="password">` タグおよび `</module-option>` タグで囲まれています。

RDBMS_service_user のパスワードが変更されます。

5. reportserver のパスワードを以下の手順で変更します。

- a. ファイル内で次のエントリを確認します。

```
<module-option name="userName">reportserver</module-option>
```

- b. このパラメータの直後にあるパラメータ内のパスワードを変更します。

パラメータは `<module-option name="password">` タグおよび `</module-option>` タグで囲まれています。

reportserver のパスワードが変更されます。

6. ファイルを保存して閉じます。

例: login-config.xml ファイルで RDBMS_service_user のパスワードを変更

login-config.xml ファイルの以下のスニペットは、RDBMS_service_user の変更されたパスワードの 1 つのインスタンスを示しています。ユーザの名前は caidb01 です。パスワードは次のように暗号化されています: }>8:Jt^+%INK&i^v:

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
      code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
      flag="required">
      <module-option name="userName">caidb01</module-option>
      <module-option
        name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
      <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
      </login-module>
    </authentication>
  </application-policy>
```

例: login-config.xml ファイルで reportserver のパスワードを変更

login-config.xml ファイルの以下のスニペットは、reportserver の変更されたパスワードを示しています。パスワードは次のように暗号化されています: }>8:Jt^+%INK&i^v:

```
<application-policy name="JmsXATibcoRealm">
  <authentication>
    <login-module
      code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">reportserver</module-option>
      <module-option
        name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
      <module-option name="managedConnectionFactoryName">
        jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
      </login-module>
    </authentication>
  </application-policy>
```

詳細情報:

[reportserver のパスワードの変更](#) (P. 604)

[RDBMS_service_user のパスワードの変更](#) (P. 602)

CA IdentityMinder 管理コンソールでのユーザ ディレクトリのパスワードの変更

ADS_LDAP_bind_user のパスワードを変更する場合は、CA IdentityMinder 管理コンソールでユーザ ディレクトリのパスワードを変更します。組織のセキュリティ ポリシーおよびパスワード ポリシーに準拠するため、このアカウントのパスワードを定期的に変更する必要がある場合があります。

注: サービス アカウントが対話するすべてのコンポーネント上でパスワードを変更するために複数の方式を使用する必要がある場合があります。

CA IdentityMinder 管理コンソールでユーザ ディレクトリのパスワードを変更する方法

1. [クリア テキスト パスワードを暗号化](#) (P. 630) します。
2. [CA IdentityMinder 管理コンソールを開きます](#) (P. 105)。
3. [ディレクトリ] をクリックします。
[ディレクトリ] ページが表示されます。
4. ac-dir をクリックします。
ディレクトリのプロパティ ページが表示されます。
5. [エクスポート] をクリックします。
ac-dir.xml ファイルがエクスポートされます。
6. エクスポートされたファイルを テキスト エディタで開きます。
7. 以下のパラメータを確認します。
`<Credentials user=`
8. 暗号化されたパスワードを以下のフィールドに入力します。このフィールドは、`<credentials>` パラメータの後ろにあります。
`{PBES}=`
9. ファイルを保存して閉じます。
10. CA IdentityMinder 管理コンソールで、ディレクトリのプロパティ ページから [更新] をクリックします。
ディレクトリの更新ウィンドウが表示されます。

11. 編集した XML ファイルのパスおよびファイル名を入力するか、ファイルを参照して選択し、[完了] をクリックします。

ディレクトリ設定出力フィールドにステータス情報が表示されます。

12. [続行] をクリックし、環境を再起動します。

CA IdentityMinder 管理コンソールでユーザ ディレクトリのパスワードが変更されました。

例: ユーザ ディレクトリのパスワードを変更

エクスポートされた ac-dir.xml ファイルの以下のスニペットは、ユーザ ディレクトリの変更されたパスワードを示しています。ユーザの名前は Administrator です。パスワードは次のように暗号化されています:

す: }>8:Jt^+%INK&i^v:

```
<Credentials user="CN=Administrator,cn=Users,DC=unixauthdemo,DC=co,DC=il">
{PBES}:}>8:Jt^+%INK&i^v==</Credentials>
```

詳細情報:

[CA IdentityMinder 管理コンソールの有効化](#) (P. 104)

[CA IdentityMinder 管理コンソールの起動](#) (P. 105)

[ADS LDAP bind user のパスワードの変更](#) (P. 613)