

CA Client Automation

実装ガイド

12.9



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 © 2014 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。

CA Technologies 製品リファレンス

このマニュアルセットで参照されている CA 製品は、以下のとおりです。

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA APM (CA Asset Portfolio Management)
- CA Business Intelligence
- CA Common Services™
- CA DMM (CA Desktop Migration Manager)
- CA Embedded Entitlements Manager (CA EEM)
- CA MDM (CA Mobile Device Management)
- CA NSM (CA Network and Systems Management)
- CA Patch Manager
- CA Process Automation
- CA Service Desk Manager
- CA WorldView™

CA への連絡先

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

目次

第 1 章: Client Automation について	23
DSM アーキテクチャ	23
DSM エクスプローラ	26
マネージャ	27
エンタープライズおよびドメインの概念	27
エンタープライズおよびドメイン コンポーネント	28
エンタープライズおよびドメインの概念での管理データベース	29
エンジンの概念	31
スケーラビリティ サーバ	39
基本的なスケーラビリティ サーバのサブコンポーネント	39
基本的なスケーラビリティ サーバのタスク	40
スケーラビリティ サーバおよび仮想アプリケーションの展開	41
OS インストール管理ブート サーバのインストールについて	42
エージェント	43
エージェント パッケージの概念	44
エージェントの設定	45
Remote Control ビューア	46
ソフトウェア カタログ	47
AM リモート エージェント	48
Web コンソール	48
Web コンソール アクセス	49
Web コンソールの機能	49
サポートされる Web ブラウザおよび Web サーバ	50
DSM レポーター	51
Common Application Framework	52
アプリケーション フレームワーク ユーザ インターフェース	52
システム トレイ	53
ログ	55
共通設定	57
設定パラメータ	58
設定ポリシー	59
エージェントからの設定レポート	60
エンタープライズ マネージャのエージェントの設定	60
ロケーション認識を有効化および設定する方法	61
サポートされているオペレーティング環境	77

ハードウェアの仕様および要件	77
エンタープライズ マネージャの仕様	77
ドメイン マネージャの仕様	78
スケーラビリティ サーバの仕様	79
エージェントの仕様	79
DSM エクスプローラの仕様	79
Windows 版 SQL Server MDB の仕様	80
Oracle MDB の仕様	80
デバイスのインベントリおよび管理	81
基本インベントリ コンポーネント	81
非常駐インベントリ サポート	82
NRI の制限事項	82

第 2 章: インフラストラクチャ インプリメンテーションの計画 83

IPv6 サポート	83
IPv6 サポート関連での制限事項	84
IPv6 サポート関連の設定に関する考慮事項	86
FIPS 140-2 のサポート	90
FIPS 140-2 プラットフォームのサポート	91
サポートされている FIPS モード	92
フェールオーバー サポートおよびハードウェアの置き換え	92
フェールオーバー サポート	93
マネージャ ハードウェアの置換	96
Client Automation インストール用の CA HIPS の設定	97
インフラストラクチャ コンポーネントに関する考慮事項	98
インフラストラクチャのインストール手順	99
インフラストラクチャのサイジング キー ファクタ	99
Client Automation でのコンピュータの識別	101
ドメイン間でのコンピュータのローミング	105
ログオフまたは再起動パナーのカスタマイズ	106
カスタム再起動プログラムの使用	106
ターミナル サーバ上の再起動とログオフのダイアログ ボックス	107
Web サービスのドキュメントおよび WSDL ファイルの場所	108
Web コンソール および Web サービスに関する注意事項	108
内部の依存関係	113
Windows でのその他の製品との依存関係	115
Windows に前提条件を手動でインストールする方法	117
Linux および UNIX でのその他の製品との依存関係	118
Linux での Apache の再起動	118

第 3 章: Client Automation のインストール

119

インストール処理の概要	120
インストーラの概要	121
前提条件および制限事項	122
インストール方法	122
インストールに関する注意事項	123
インストールに関するその他の考慮事項	124
FIPS に関連するインストールの考慮事項	124
インストール中の FIPS モードの選択	125
自動マイグレーションのインストール	126
インストールの前提条件	126
インストールに関する注意事項	127
自動マイグレーションの設定	127
多言語インストール	131
エージェント言語パッケージの作成およびインストールについて	132
エージェントインストールの特別なシナリオ	133
必要なハードウェア設定	133
管理データベース (MDB)	134
MDB PIF パッケージ	135
スタンドアロン MDB インストール	135
PIF インストール レコード	135
CCS の注意事項	136
CCS インストール エラー メッセージ	137
DSM マネージャのインストールの前提条件	141
マネージャおよび MDB インストールにおけるディスク領域についての注意事項	141
混合データベース環境でのスタンドアロン マネージャ	142
応答ファイルを使用した MDB の自動インストール	142
Microsoft SQL Server MDB の使用準備	144
Oracle MDB の使用準備	148
Oracle MDB のインストールおよび設定上の注意事項	155
ユーザ ca_DSM のデフォルトのパスワードの変更	156
MDB インストール ログ ファイル	158
MDB のアップグレード	158
アンインストール	159
Client Automation インストールに関する特記事項	159
セキュリティ ポリシー設定	160
CAM および SSA PMUX の再起動	160
ソフトウェア インベントリの使用可能性	160
IPv6 上での DSM マネージャとリモート SQL Server MDB のインストール	160

名前付きインスタンスを持つリモート SQL Server MDB を使用したドメイン マネージャのインストール.....	161
Remote Control スタンドアロン エージェントのインストール.....	161
Solaris Intel へのインストール.....	162
Solaris Intel 用の PATH 環境変数.....	163
VMware ESX Web サービスへのアクセス.....	163
Linux での Remote Control コンポーネントのインストール.....	164
Apple Mac OS X での Remote Control コンポーネントのインストール.....	164
ブート サーバの共有アクセス.....	165
CCS のインストール時のドメイン コントローラ接続.....	165
エージェントおよびスケーラビリティ サーバの移動操作.....	165
ドメイン コントローラ上の CCS WorldView マネージャまたは MDB インストールを含む CCS を使用した DSM マネージャ.....	166
Linux へのスケーラビリティ サーバのインストール.....	167
UNIX と Mac OS X コンポーネントのインストールと登録.....	167
UNIX エージェントに関する考慮事項.....	167
DTS (Data Transport Service) のインストールに関する注意事項.....	169
マネージャ コンピュータとスケーラビリティ サーバ コンピュータの名前の変更.....	170
完全修飾ドメイン名としてのシステム名.....	170
Unicenter NSM r11 がプリインストールされている場合の Client Automation のインストール.....	171
インストール時の Web コンソールのポート番号の指定.....	171
[インストールの変更] 方式を使用して Web コンソールを追加する際の注意事項.....	172
インストールおよびアンインストール中のウイルス保護の無効化.....	172
インストール中のリモート セクタ サーバ サービスの無効化.....	172
Windows XP ネットワーク アクセス - ローカル アカウントの共有とセキュリティ モデル.....	172
Windows Server 2003 の注意事項.....	173
Windows Server 2008 のコア オペレーティング環境.....	175
ファイアウォールおよびポートに関する注意事項.....	176
Linux の Compatibility Library.....	176
インストーラの MSI 前提条件.....	177
CA Service Desk Manager と Client Automation 間での MDB の共有.....	178
Windows への管理者によるインストール.....	178
Windows でのインストール ディレクトリ.....	178
Linux および UNIX でのインストール ディレクトリ.....	179
Alert Collector のインストール.....	181
コンピュータ名、ユーザ名、およびディレクトリ名の制限事項.....	182
コンピュータ名の制限事項.....	182
ユーザ名の制限事項.....	183
ディレクトリ名の制限事項.....	183
インストール ウィザードを使用したインタラクティブ インストール.....	184

インストール前のディスク領域の確認.....	185
各コンポーネントのインタラクティブ インストール	185
インストール サマリ	186
インストールのロールバック	186
インストール パッケージのコピー	187
CCS に関する考慮事項.....	187
Windows での CA Client Automation のインタラクティブ インストール	188
Linux および UNIX での対話式インストール.....	189
コマンドラインを使用した Client Automation のインストール (Windows)	190
Windows 用のパッケージのインストール	191
setup.exe を使用した CA Client Automation のインストール.....	193
インストール ツール msixec.....	193
Linux または UNIX でコマンドラインを使用した Client Automation のインストール.....	216
Linux または UNIX への Client Automation の installdsm スクリプト インストール	217
Linux および UNIX での応答ファイルの設定.....	218
インストール プロパティ値の変更.....	218
インストール ログ ファイル	232
インストール ログ ファイル (Windows)	233
インストール ログ ファイル (Linux および UNIX)	233
インストールされている DSM コンポーネントに関するバージョン情報.....	234

第 4 章: ポストインストール タスク 235

インストール後の製品言語の変更	235
MDB の管理.....	236
Microsoft SQL Server MDB のメンテナンス	236
Oracle MDB のメンテナンス	239
ターゲット MDB と同期されたオブジェクト	239
マネージャおよび MDB のアンインストール	244
SQL Bridge のインストール	248
Microsoft SQL Server MDB 1.0.4 を使用したターゲット側のアップグレード	249
Microsoft SQL Server MDB 1.5 を使用したターゲット側のアップグレード	249
Oracle Bridge のインストール	249
Solaris 上の Oracle MDB 1.5 を使用したターゲット側のアップグレード.....	250
Windows でドッキング デバイスを有効にする方法	251
Windows でソースからエージェントを実行する方法	252
Windows でユーザ アカウントで Client Automation サービスを実行する方法.....	254
管理者として Client Automation サービスを実行.....	254
独自の X.509 証明書をインストール イメージに取り込む方法.....	255
デフォルトの証明書 (Windows)	256

Linux および UNIX のデフォルトの証明書.....	256
cfcert.ini を使用した X.509 証明書のカスタマイズ.....	257
インストールの変更および修復.....	259
インストールの変更.....	260
インストールを修復する方法.....	261
インストールのアップグレード.....	261
Client Automation のアンインストール.....	262
Windows での Client Automation のアンインストール.....	263
Linux および UNIX 上の Client Automation のアンインストール.....	265
エージェントのアンインストールに関する一般注意事項.....	266

第 5 章: インフラストラクチャ展開 269

インフラストラクチャ展開の概要.....	270
通常の Client Automation インフラストラクチャ展開フェーズ.....	270
展開管理の概念.....	271
展開管理プロセス.....	275
DSM エクスプローラを使用した展開.....	285
コマンドラインを使用した展開.....	286
継続ディスカバリによってトリガされる展開.....	287
展開パッケージ.....	288
dsmpush ツール.....	290
Client Automation インフラストラクチャを自動展開するための前提条件.....	291
インフラストラクチャ展開で使用する FTP サーバの変更の詳細.....	294
エージェントの展開を有効にする Windows XP の設定.....	295

第 6 章: アップグレードと移行に関する考慮事項 297

サポートされているアップグレードパス.....	298
一般的な注意事項.....	298
Client Automation コンポーネントのアップグレードに関する考慮事項.....	298
MDB に関する考慮事項.....	299
アップグレードにおける注意事項.....	299
アップグレード情報.....	300
FIPS に関する考慮事項.....	300
OSIM のアップグレードに関する考慮事項.....	301
アップグレードプロセス.....	302
アップグレードに関する重要事項.....	303
フェーズ 1: DSM エンタープライズ マネージャのアップグレード.....	304
フェーズ 2: DSM ドメイン マネージャのアップグレード.....	305

フェーズ 3 : DSM スケーラビリティ サーバのアップグレード	307
フェーズ 4 : DSM エージェントのアップグレード	309
インストール DVD を使用したエージェントのアップグレード	310
インフラストラクチャ展開と「AM、RC、SD プラグイン」 (すべてのエージェント プラグイン) パッケージを使用した Windows エージェントのアップグレード	310
インフラストラクチャ展開および個々のプラグインを使用した Windows エージェントのアップグレード	311
インフラストラクチャ展開と「AM、RC、SD プラグイン」 (すべてのエージェント プラグイン) パッケージを使用した Linux または MacIntel エージェントのアップグレード	313
インフラストラクチャ展開および個々のプラグインパッケージを使用した Linux または MacIntel エージェントのアップグレード	313
Software Delivery と「AM、RC、SD プラグイン」 (すべてのエージェント プラグイン) パッケージを使用した Linux または MacIntel エージェントのアップグレード	314
Software Delivery および個々のエージェント プラグイン パッケージを使用した Linux または MacIntel エージェントのアップグレード	314
インフラストラクチャ展開と「AM、SD プラグイン」 (すべてのエージェント プラグイン) パッケージを使用した UNIX エージェントのアップグレード	315
インフラストラクチャ展開および個々のエージェント プラグイン パッケージを使用した UNIX エージェントのアップグレード	315
Software Delivery と「AM、RC、SD プラグイン」 (すべてのエージェント プラグイン) パッケージを使用した Windows エージェントのアップグレード	316
Software Delivery および個々のエージェント プラグイン パッケージを使用した Windows エージェントのアップグレード	316
Software Delivery と「AM、SD プラグイン」 (すべてのエージェント プラグイン) パッケージを使用した UNIX エージェントのアップグレード	317
Software Delivery および個々のエージェント プラグイン パッケージを使用した UNIX エージェントのアップグレード	318

第 7 章: CA Catalyst 用の CA ITCM コネクタ 319

第 8 章: デスクトップ仮想化 321

ゴールデン テンプレートの準備	322
前提条件の確認	324
ゴールデン テンプレート上での DSM エージェントの展開	325
CA DSM エージェント VDI サポート アドオン パッケージのインストール	327
ゴールデン テンプレート上での実稼働ソフトウェア パッケージの展開	328
ソフトウェア再インストールの設定	328
(オプション) 仮想デスクトップへのスケーラビリティ サーバの割り当て	340
ソフトウェア再インストールに対するインベントリ収集の設定	342
テンプレートのタグ付けとスナップショットまたは vDisk の作成	342

ゴールデンテンプレートの割り当ての確認	343
デスクトップ仮想化のサポートに対する設定ポリシー	343
ゴールデンテンプレートの更新	353
前提条件の確認.....	354
ゴールデンテンプレート上でのソフトウェアの展開または削除	354
(Xendesktop PVS に対して) vDisk ターゲット デバイス個人データの設定	355
vDisk インベントリの表示	357
更新後のテンプレートのタグ付け	358
仮想デスクトップ グループまたはプールの更新	359
仮想デスクトップのソフトウェア更新の確認	360
vDisk および vDisk クローンの管理	360
vDisk クローンを処理する方法	360
ゴールデンテンプレート、マスタ vDisk、およびクローン間の関係の表示	362
Client Automation からの仮想デスクトップの管理.....	364
仮想デスクトップ用の実装ガイドライン	364
仮想デスクトップ上でのセキュリティ パッチの適用	369
VDI インベントリの表示	373
クエリおよびレポート	374
クエリ デザインの変更点.....	375
DSM Reporter の変更点.....	375
廃止アセット ウィザードによるゴールデン イメージの除外	375

第 9 章: Client Automation インフラストラクチャの正常性を設定および監視 する方法

377

前提条件の確認.....	379
HM アーキテクチャおよび基本の理解	380
アラートおよびアラート テンプレート	381
ヘルス監視コンポーネント	382
外部プロセス マネージャ (CAF プラグイン)	384
アラート レメディエーション	385
アラートおよびアラート テンプレートの設定	385
アラートの設定.....	386
アラート テンプレートの設定	392
Alert Collector の設定	396
Alert Collector のプロパティの設定.....	397
アラート アクションの設定	399
アラート転送の詳細の指定	402
ヘルス監視エージェントの設定	404
アラート アップロードの設定	407

Alert Collector サーバの設定	408
プロキシ設定を設定する	409
WAC からのアラート ステータスの管理およびトラッキング	410
アラート複製	412

第 10 章: 外部ディレクトリを設定および認証する方法 413

サポートされている外部ディレクトリ	415
前提条件の確認	415
リポジトリへのディレクトリの追加	415
ディレクトリ サーバの詳細の指定	416
ディレクトリ バインド情報の指定	417
ベース ディレクトリ ノード詳細の指定	417
スキーマ マッピング属性の選択	418
スキーマ マッピングの調整/定義の詳細	418
設定オプションのレビューおよびディレクトリの追加	419
(オプション) 証明書のインポート (LDAPS のみ)	420
設定したディレクトリの確認	421
(オプション) ディレクトリの更新	421
ディレクトリの更新: [設定] タブ	422
ディレクトリの更新: [セキュリティ] タブ	424
ディレクトリの更新: [スキーマ] タブ	424
設定したディレクトリを使用した認証	425
セキュリティ プロファイルの追加	425
ディレクトリ認証の確認	428
ポリシーの変更による別のユーザ名形式の使用	430
スキーマ マッピング属性について	430
CA Client Automation のディレクトリ統合	438

第 11 章: Client Automation セキュリティ機能 439

認証	440
サポートされているユーザ名のフォーマット	441
X.509 証明書ベースの認証	442
オブジェクト レベルのセキュリティおよび証明書	442
ルート証明書	443
証明書の保管	443
基本ホスト ID の証明書	443
証明書の配信	444
新しい証明書の作成	445

新しいルート証明書の生成.....	445
アプリケーション固有の証明書の生成.....	446
基本ホスト ID の証明書の生成.....	447
新規証明書のインストール.....	448
新しいルート証明書のインストール.....	448
アプリケーション固有の証明書のインストール.....	449
基本ホスト ID の証明書のインストール.....	449
証明書の置換.....	450
証明書の削除.....	451
VMware ESX セキュリティおよび認証.....	451
認可.....	452
セキュリティ プロファイル.....	453
権限の概要.....	454
複製.....	469
制限事項.....	470
セキュリティ シナリオ - Software Delivery.....	471
共通セキュリティの設定.....	473
セキュリティの設定方法.....	474
セキュリティ プロファイルの追加.....	475
定義済みのアクセス タイプ.....	477
クラスのアクセス権を指定します。.....	478
オブジェクトのアクセス権を指定します。.....	479
グループのアクセス権を指定します。.....	480
累積アクセス権.....	480
セキュリティ エリアのサポート.....	481
セキュリティ エリアのグローバル設定.....	482
セキュリティ プロファイルのセキュリティ エリア設定の有効化.....	482
セキュリティ エリアの作成.....	483
セキュリティ エリアの削除.....	483
セキュリティ プロファイルへのセキュリティ エリアのリンクまたはリンク解除.....	484
セキュリティ エリアの保護されたオブジェクトへのリンクまたはリンク解除.....	485
暗号化の設定.....	485
通信用暗号化アルゴリズム.....	486
一致する暗号化アルゴリズムの選択.....	487
トップ シークレット環境での暗号化.....	488
古いバージョンとの通信（互換性ポリシー）.....	488
FIPS 準拠の暗号方式.....	489
FIPS モードを切り替える前に.....	489
FIPS のみモードに切り替える方法.....	491
FIPS 推奨モードに切り替える方法.....	492

変換ユーティリティの実行.....	493
FIPS モードを変更する設定ポリシーの変更	494
DSM コンポーネントの FIPS モードの検証.....	497
FIPS モードの事前定義済みクエリおよびレポート	497
DSM Web コンポーネント用の FIPS 準拠の設定	498
r12 コンポーネントに接続している FIPS のみエージェントの修復	499
FIPS ポリシーの変更が有効にならない場合のシナリオ.....	500

第 12 章: 拡張ネットワーク接続(ENC) 503

拡張ネットワーク接続へようこそ	503
ENC コンポーネント	505
サポートされるプラットフォーム	506
ENC ゲートウェイ接続プロセス	506
ENC ゲートウェイ セキュリティ.....	507
認証.....	507
ENC ゲートウェイ認可ルール	508
一般用語.....	508
ENC および Uniform Resource Identifier	510
認可ルールの設定.....	511
イベント.....	513
接続シーケンス.....	518
ENC 仮想接続.....	519
ルール設定の例.....	520
その他の質問およびその解決方法.....	526
イベントの監査.....	527
ENC ゲートウェイ コンポーネントのインストールおよび設定	527
ENC および SSA の設定.....	528
ENC クライアントを有効化する方法.....	528
ENC 環境における展開	529
ENC 展開シナリオ	530
ENC 展開シナリオ - パイロット スキーム	530
ENC 展開シナリオ - ブランチ オフィス	535
ENC 展開シナリオ - アウトソース クライアント会社（小規模）	539
ENC 展開シナリオ - アウトソース クライアント会社（中規模）	540
ENC 展開シナリオ - アウトソース クライアント会社（大規模）	541
スタンドアロン ENC ゲートウェイ ルータ.....	543
スタンドアロン ENC ゲートウェイ サーバ.....	543
インターネット プロキシのサポート	544
ENC ゲートウェイ経由で Client Automation を使用することに関する制限事項.....	545

encUtilCmd ユーティリティの使用	547
証明書の管理.....	548
X.509 証明書.....	549
PKI インフラストラクチャを使用した証明書の管理	549
証明書の要件.....	550
CA Technologies-プライベート認証オブジェクト ID.....	551

第 13 章: CA Service Desk Manager との統合 553

サービス アウェア ポリシー	554
チケットの処理.....	555
検出されたアセットと所有アセットとの関連付け	556
Client Automation と CA Service Desk Manager の間のコンテキスト起動.....	556
Client Automation から CA Service Desk Manager へのコンテキスト起動.....	556
管理対象アセットのコンテキストでのチケット作成（一時）	559
CA Service Desk Manager から Client Automation へのコンテキスト起動.....	559
CA Service Desk Manager および Client Automation のセットアップ	560
CA Service Desk Manager のコンテキスト内起動の前提条件	560
複数のエンジンと CA Service Desk Manager 統合するための前提条件	561
エンタープライズ マネージャと CA Service Desk Manager 統合するための前提条件.....	561
Client Automation と CA Service Desk Manager との統合について.....	561
Service Desk が有効なエンタープライズ マネージャからの Software Delivery ジョブ	562
CA Service Desk Manager Web サービスへのセキュア ログオン.....	562
セキュア ログオンの設定方法.....	563
ユーザ名とパスワードによる方式（非管理）	564
証明書または eTrust PKI 方式（管理）	564
設定ポリシー内の設定	566

第 14 章: トラブルシューティング 569

CIC 接続の解放エラー.....	569
Oracle MDB でのコンテンツ ダウンロードが失敗します.....	569
データベースが停止されると DSM エンジンがクラッシュする	570
Windows 8 および 8.1 での SXP パッケージ用前提条件.....	570
エクスポートされたレポートを開く	570
Alert Collector が指定されたマネージャの接続に失敗する	571
Alert Collector がデータベースへの接続に失敗する	571
ミーティング モード接続で DSM エクスプローラにプロンプト ウィンドウが表示されない.....	572
クラスタ セットアップでブート サーバ設定を tftp から共有アクセス モードに変更した場合の問題.....	572

プログラムの追加/削除での ITCM および CIC コンポーネントのサイズ詳細に関する問題	573
テクニカル サポートへの接続におけるエラーおよび遅延	573
Client Automation コンポーネントの SE-Linux によるサポート	574
日本語版のインストーラの UI に意味のない文字が表示されます。	574
コマンドプロンプトの文字列に関する問題	575
新しい 64 ビット版 Linux OS での共有ライブラリのロード時に発生するエラー	576
Solaris 上でエージェントをインストールするとエラーが発生して失敗する	577
Windows 8 および 8.1 のセキュア モードでのリモート制御	577
MDB に接続できない	578
CAM のアップグレードの後、DSM マネージャが起動に失敗する	578
一時フォルダ内のログが削除される	579
ORACLE_HOME 変数または ca_itrm パスワードが誤って設定されている場合、MDB インストーラが ハングアップする	579
名前付きインスタンスおよびポート ID によるインストール エラー	580
応答ファイルに未使用のエントリが含まれている	580
SQL MDB から Oracle MDB ターゲットへの同期エラー	580
Oracle 上のターゲット MDB での同期エラー	581
スタンドアロン WAC 上で Web コンソールからの統合ログオンが失敗する	582
DSM マネージャのアップグレードの後の高い CPU 使用率	583
Windows 2012 仮想マシンが含まれている場合はインフラストラクチャ展開に失敗する	583
Oracle 12.1.0.1 32bit Windows Client を使用したハードウェア インベントリの収集ができません	584

付録 A: 自動化サービス設定ファイル 585

付録 B: CA Client Automation で使用されるポート 593

ポート使用に関する一般的な考慮事項	594
エンタープライズ マネージャで使用されるポート	595
ドメイン マネージャで使用されるポート	596
インフラストラクチャ展開で使用されるポート	599
スケーラビリティ サーバで使用されるポート	601
ブート サーバで使用されるポート	603
エンジンで使用されるポート	604
エージェントで使用されるポート	605
パッケージャで使用されるポート	607
DSM エクスプローラおよび Reporter で使用されるポート	608
ENC ゲートウェイが使用するポート	609
AMT アセットの隔離が使用するポート	610
MDB ポートの使用状況	611

付録 C: インストールの Software Delivery プロシージャ 613

アンインストールに関する重要事項	614
CA DSM エージェント + AM、RC、SD プラグイン Linux (Intel) ENU.....	614
CA DSM エージェント + Asset Management プラグイン Linux (intel) ENU.....	614
CA DSM エージェント + 基本インベントリ プラグイン Linux (intel) ENU	615
CA DMPPrimer Linux (Intel) ENU	615
SMPackager (Linux)	615
CA DSM レガシー エージェントの削除 Linux (intel) ENU	615
CA DSM エージェント + Remote Control プラグイン Linux (intel) ENU	616
CA DSM エージェント + Software Delivery プラグイン Linux (intel) ENU	616
CA DSM スケーラビリティ サーバ Linux (Intel) ENU.....	617
CA DSM Agent + AM、RC、SD プラグイン Win32	617
CA DMS エージェント + Asset Management プラグイン	618
CA DMS エージェント + 基本インベントリ プラグイン	618
CA DMS エージェント + Data Transport プラグイン	618
CA DMS エージェント + Remote Control プラグイン	619
CA DMS エージェント + Software Delivery プラグイン	620
CA DSM Constant Access (Intel AMT)	621
CA DSM エクスプローラ	621
CA DSM マネージャ	622
CA DMS スケーラビリティ サーバ	622
CA DSM 安全なソケット アダプタ	623
CA DSM レガシー エージェントの削除 Win32.....	623

付録 D: CA Client Automation が提供する現在の証明書 625

共通の証明書	625
デフォルトの DSM ルート証明書	625
デフォルトの基本ホスト ID 証明書.....	626
アプリケーション固有の証明書	626
ディレクトリの同期の証明書	627
共通サーバ登録の証明書	627
設定およびステータス管理の証明書	628
Software Delivery エージェント ムーバの証明書	628
Software Delivery カタログ証明書	629
エンタープライズアクセスの証明書	630
ドメインアクセスの証明書	630
レポータ アクセスの証明書	631

付録 E: セキュリティ エリアのサポートのユース ケース 633

セキュリティ プロファイル用のセキュリティ エリア サポート	634
ユース ケース : Client Automation のインストール	635
ユース ケース : 既存のインストールのアップグレード	636
ユース ケース : セキュリティ プロファイル	636
ユース ケース : セキュリティ プロファイルの作成	637
ユース ケース : セキュリティ プロファイルに対するエリア設定の変更	637
ユース ケース : セキュリティ プロファイルの削除	638
ユース ケース : コンピュータ	638
ユース ケース : コンピュータ オブジェクトの手動による作成	639
ユース ケース : 新しく検出された DSM エージェント	639
ユース ケース : アセット グループ	640
ユース ケース : アセット グループの作成	640
ユース ケース : アセット グループへのコンピュータの追加	641
ユース ケース : アセット グループからのコンピュータの削除	642
ユース ケース : アセット グループのエリアの権限の変更	643
ユース ケース : 継承の無効化および復帰	643
ユース ケース : クエリ	644
ユース ケース : クエリの作成	644
ユース ケース : クエリの実行	645
ユース ケース : Software Delivery のコンテキストでのクエリの実行	646
ユース ケース : ソフトウェア パッケージ	646
ユース ケース : ソフトウェア パッケージの作成	647
ユース ケース : ソフトウェア プロシージャ	647
ユース ケース : ソフトウェア プロシージャの作成	647
ユース ケース : ソフトウェア グループ	648
ユース ケース : ソフトウェア グループの作成	648
ユース ケース : ソフトウェア ポリシー	648
ユース ケース : ソフトウェア ポリシーの作成	649
ユース ケース : ソフトウェア ジョブ	649
ユース ケース : ソフトウェア ジョブの作成	650
ユース ケース : アセット ジョブ	650
ユース ケース : アセット ジョブの作成	651
ユース ケース : エンジン タスク	651
ユース ケース : エンジン タスクの作成	652
ユース ケース : エリアの管理	652
ユース ケース : 最初のエリア コードのサポートの有効化	653
ユース ケース : エリア コードのサポートの無効化	654
ユース ケース : エリア コードのサポートの再有効化	654

ユース ケース：デフォルトのエリアの権限の変更	655
ユース ケース：新しいエリアの追加	655
ユース ケース：エリアの削除	656
ユース ケース：所有権の取得	656

付録 F: CAF でスケジュールされたジョブ 657

CAF 標準ジョブおよびパラメータ	657
CAF でスケジュールされたジョブの例	660

付録 G: FIPS 140-2 準拠 661

FIPS PUB 140-2	661
参照	662
サポートされている FIPS モード	662
暗号化モジュール - RSA Crypto	663
暗号化セキュリティ機能	663
コンポーネント固有の暗号化の使用	665
Client Automation 以外の FIPS 準拠コンポーネント	666
Windows 動作環境	667
SQL Server	667
その他のコンポーネント	667
認定されていないセキュリティ機能の使用	668

付録 H: アクセシビリティ機能	669
付録 I: 製品の機能拡張	671
付録 J: Remote Control ビューで文字列が切り捨てられる	675
付録 K: リンク リストの内容がフォーカスによって変化する	677
付録 L: Remote Control ビューアおよびリプレイヤーでの JAWS スクリーン リーダの使用	679
付録 M: リモート セッションの制限	681
付録 N: 高コントラスト モードの機能	683
用語集	685

第 1 章: Client Automation について

CA Client Automation は、クロスプラットフォームの IT リソース管理ソリューションで、シームレスに統合された最先端の Asset Management、Software Delivery、および Remote Control 機能をあらゆる企業に対して提供します。

このセクションには、以下のトピックが含まれています。

[DSM アーキテクチャ](#) (P. 23)

[DSM エクスプローラ](#) (P. 26)

[マネージャ](#) (P. 27)

[スケーラビリティ サーバ](#) (P. 39)

[エージェント](#) (P. 43)

[Web コンソール](#) (P. 48)

[DSM レポーター](#) (P. 51)

[Common Application Framework](#) (P. 52)

[共通設定](#) (P. 57)

[サポートされているオペレーティング環境](#) (P. 77)

[ハードウェアの仕様および要件](#) (P. 77)

[デバイスのインベントリおよび管理](#) (P. 81)

DSM アーキテクチャ

CA Client Automation では Asset Management、Software Delivery、および Remote Control の機能 (DSM アーキテクチャ) の共通インターフェースおよびアーキテクチャが提供されていますが、管理ユーザ インターフェース以外の点も統合されています。

インフラストラクチャの中心部が、Asset Management、Software Delivery、および Remote Control の機能とコンポーネントによって共有されます。たとえば、いずれか 2 つまたはすべての機能をインストールする場合、管理データベース、通信、プロセス制御、ロギング、イベント管理などがすべて同じになります。これにより、有用な機能とすべての製品における用語、アーキテクチャ、インターフェース、およびデータの整合性をインストールされた機能間で実現することが可能になりました。

さらに、このアーキテクチャには、**Asset Management**、**Software Delivery**、および **Remote Control** の機能間で共有される、一連の整合性のある共通の概念があります。具体的には、以下の共有コンポーネントが含まれています。

- グラフィカル ユーザ インターフェース (GUI)
- マネージャ
- スケーラビリティ サーバ
- エージェント

DSM アーキテクチャは、以下の階層で構成されます。

DSM エクスプローラ/Web コンソール

Client Automation およびそのコンポーネント プラグインを管理統制できます。**DSM エクスプローラ**は、**Windows** 用のグラフィカル ユーザ インターフェースで、**Web コンソール**は、**Windows** および **Linux** 両方で使用できるブラウザベースの GUI です。

エンタープライズ マネージャ

複数のドメインを一括管理することができます。

ドメイン マネージャ

低位階層およびエージェントに管理サービスが提供されます。

スケーラビリティ サーバ

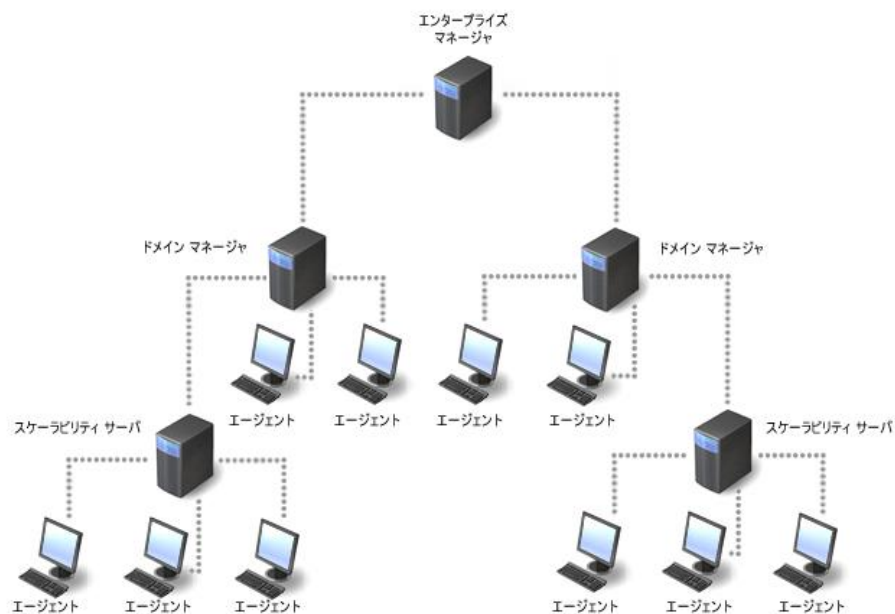
ソフトウェア配信および配布アクティビティの配布ポイントおよびアセット インベントリの収集ポイントの役割を果たします。

エージェント

サポートされているホスト上でリモート コントロール、ソフトウェア配信、およびアセット インベントリの各サービスが提供されます。

各マネージャ階層では、管理データベース (MDB) のインスタンスがホストされます。

以下の図に、多層アーキテクチャの例を示します。この例では、直接接続されているエージェントとダウンストリームのスケーラビリティ サーバをそれぞれ管理する 2 つのドメイン マネージャに対して、エンタープライズ マネージャが管理ポイントの役割を果たしています。スケーラビリティ マネージャは、エージェントとドメイン マネージャの層の間のタスクを管理します。



DSM エクスプローラ

DSM エクスプローラは **Client Automation** の主要な管理インターフェースで、**Windows** 動作環境で利用することができます。

左側の **DSM エクスプローラ** バーでは、ツリー ビュー、履歴、ブックマーク、および検索の 4 種類のビューが提供されます。 ツリー ビューはデフォルトの表示モードで、このモードを使用すると、**DSM エクスプローラ**のさまざまな機能にアクセスすることができます。

多数のツリー ノードでは、ツリー ビューで選択すると右側のビューにリストが表示されます。

また、多数のツリー ノードでは、グラフィカルな **Web** ベースの表示機能も提供されます。この機能の例の 1 つに、メイン ポータルが挙げられます。メイン ポータルでは、システム全体の **Client Automation** の概要が、以下の 4 つのポートレットを利用して提供されます。

主な機能

DSM エクスプローラの [コンピュータおよびユーザ]、[ソフトウェア]、[ジョブ]などの主要なエリアにアクセスすることができます。

使用頻度の高いもの

使用頻度が最も高いツリー ノードにアクセスすることができます。

システム ステータス

統計、失敗、違反、および進行中のタスクなどの接続されたドメインに関する情報が表示されます。

クイック スタート

よく使用される機能にすばやくアクセスすることができます。

システム ステータスおよびクイック スタート ポートレットは、ユーザのニーズに合わせてカスタマイズすることができます。

チュートリアルは、**DSM エクスプローラ**の右側のウィンドウから利用することができます。チュートリアルには、**DSM エクスプローラ**へのナビゲーション、およびほとんどの共通タスクの概要に関する情報が含まれます。チュートリアルは、**DSM エクスプローラ**の機能の [表示] - [チュートリアル バー] を使用して、有効または無効にすることができます。

コンテキスト依存ヘルプの詳細については、「**DSM エクスプローラ ヘルプ**」を参照してください。

マネージャ

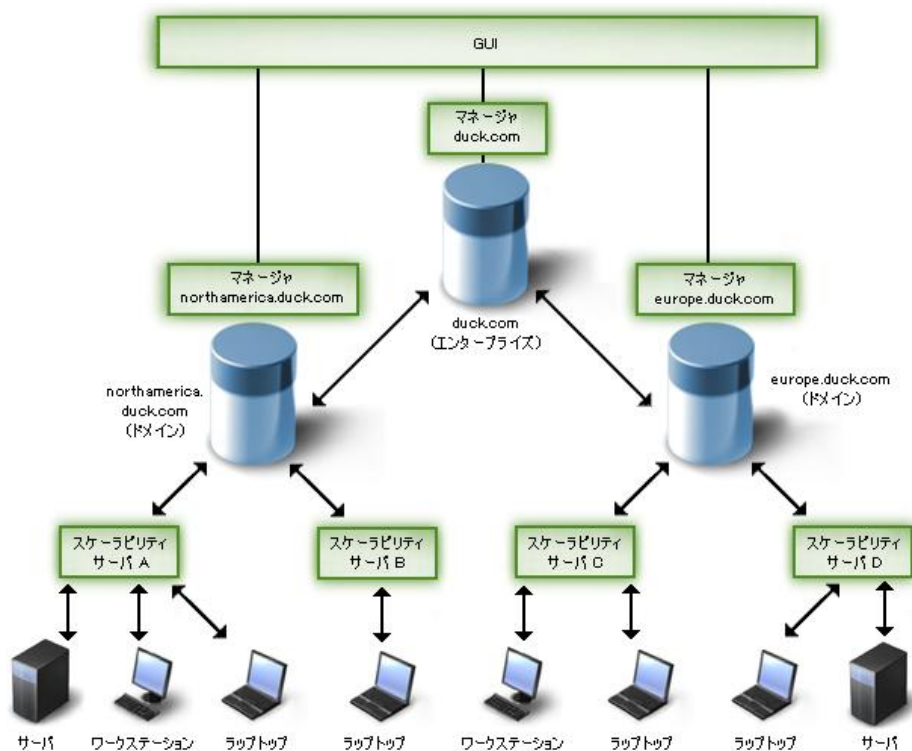
Client Automation のマネージャ ロールの以下の点について考慮します。

- [エンタープライズおよびドメインの概念](#) (P. 27)
- [エンタープライズおよびドメイン コンポーネント](#) (P. 28)
- [エンジンの概念](#) (P. 31)

エンタープライズおよびドメインの概念

Client Automation には、ドメインおよびエンタープライズの 2 つの管理層が存在し、両方の層には管理データベースが含まれています。複数のドメインが組織内で展開されている場合、エンタープライズを展開して、単一の管理ポイントを提供することができます。

以下の図は、会社のエンタープライズマネージャと 2 つのドメインマネージャで構成される 2 層アーキテクチャの例を示しています。各ドメインマネージャには、スケーラビリティサーバが接続されています。



これらは、**duck.com** と呼ばれるエンタープライズ マネージャ、および 2 つのドメインマネージャ (1 つは北アメリカ エリアにあるタスクおよびデバイスを管理するためのもの (**northamerica.duck.com**) で、もう 1 つはヨーロッパエリアにあるタスクおよびデバイスを管理するためのもの (**europe.duck.com**)) です。ラップトップやワークステーション、その他のサーバなどのエンドユーザ デバイスを管理することで、ドメインマネージャの作業負荷を削減するために、2 つのスケラビリティ サーバが各ドメイン マネージャに接続されています。

エンタープライズおよびドメイン コンポーネント

以下のリストに、**CA Client Automation** のエンタープライズおよびドメインの概念の理解に関連する用語および定義を示します。

エンタープライズ マネージャ

DSM エンタープライズ マネージャは、**CA Client Automation** のオプションのトップの管理層です。エンタープライズ マネージャでは、**DSM** ドメインのグループに単一の管理ポイントが提供され、またこれにより、複数のドメインに配置されているオブジェクトのグループの設定およびポリシーを設定することもできます。**DSM** 環境に存在できるエンタープライズ マネージャは、1 つのみです。

ドメイン マネージャ

DSM ドメイン マネージャはスケラビリティ サーバおよびエージェントを含む、ほかの **DSM** コンポーネントの集中管理ポイントです。

スケラビリティ サーバ

DSM スケラビリティ サーバは、エージェントのプライマリ インターフェースである配信処理です。スケラビリティ サーバは、多数のホストへの **DSM** のワークロードの配信を目的としています。

エンジン

DSM エンジンによって、スケラビリティ サーバとその親の **DSM** ドメインおよびエンタープライズ マネージャとの間の通信サービスが提供されます。

エンタープライズおよびドメインの概念での管理データベース

CA Technologies の製品スイートは、共通のエンタープライズデータ リポジトリである管理データベース (MDB) を利用して統合されています。MDB では、すべての CA Technologies 製品からの管理データのストレージの統合的な構造が提供されます。MDB によって、すべての IT 基準および CA Technologies 製品の管理データが統合されます。顧客およびサードパーティのパートナーは MDB を拡張すると、CA Technologies ソフトウェア製品およびツール以外の IT 管理データを追加することができます。

CA IT Client Manager は、MDB r1.5 SP1 に基づいており、デフォルトでは共通アセットと DSM スキーマしかインストールしません。CA ITCM によって作成される MDB を使用する予定があり、しかも MDB r1.5 をサポートするという CA 製品が他にもある場合、それらの製品は、自分のスキーマを既存 MDB の上にインストールする必要があります。

ただし、CA 製品が MDB r1.0.4 のみをサポートする場合は、インストールは失敗します。そのような場合は、「互換性モード」オプションをオンにして MDB をインストールしてください。CA ITCM では、最初に最新の MDB r1.0.4 パッチをインストールし、その後で、MDB が MDB r1.5 にアップグレードされます。そのため、すべてのスキーマ定義が存在し、共通アセット用のスキーマ定義と DSM のみが MDB r1.5 に関して同レベルに存在します。詳細については、「[Microsoft SQL Server MDB の使用準備 \(P. 144\)](#)」または「[Oracle MDB の使用準備 \(P. 148\)](#)」を参照してください。

展開および管理を含む MDB の一般的な情報については、オンライン CA Client Automation ドキュメントセット (ブックシェルフ) の一部に含まれる「[MDB の概要](#)」を参照してください。

多層アーキテクチャ内部では、管理データベース (MDB) はエンタープライズ層およびドメインマネージャ層で実装できます。両方の層で、Microsoft SQL Server および Oracle MDB がサポートされます。たとえば、ドメインマネージャに SQL Server を選択し、エンタープライズマネージャに Oracle を選択するといった、個別の層に異なるデータベース プロバイダの MDB を実装できます。.

SQL Server ベースの MDB を使用するドメインマネージャと Oracle ベースの MDB を使用するエンタープライズマネージャなどの混合構成では、マネージャ上に適切なデータベース クライアントが必要です。ここでの例では、ドメインマネージャ上に Oracle クライアント、およびエンタープライズマネージャ上に SQL クライアントが必要です。

現在、Oracle ベースの MDB は、Sun Solaris の動作環境で実行中のコンピュータ上のリモートデータベースとしてのみサポートされています。サポートされる最新のデータベース バージョンおよび動作環境については、CA Client Automation ドキュメントセット (ブックシェルフ) の一部に含まれる「[CA Client Automation リリースノート](#)」を参照してください。

サポートされるデータベース シナリオは、以下のとおりです。

ローカル SQL Server MDB

同じコンピュータ上にある MDB および SQL Server に基づく MDB を使用する Windows 上の DSM ドメインまたはエンタープライズ マネージャ

リモート SQL Server MDB

Windows で動作しているリモート サーバ コンピュータ上にある MDB および SQL Server に基づく MDB を使用する Windows 上の DSM ドメインまたはエンタープライズ マネージャ

リモート Oracle MDB

Solaris で動作しているリモート サーバ コンピュータ上にある MDB および Oracle に基づく MDB を使用する Windows 上の DSM ドメインまたはエンタープライズ マネージャ

エンタープライズおよびドメイン構造内のすべての MDB は同じスキーマを持っています。ドメインデータベースには、エンタープライズ マネージャへの接続方法に関する情報が含まれています。エンタープライズ データベースには、「リンク」されているすべてのドメインに接続する方法に関する情報、および利用できるマネージャとその場所に関する情報があります。

Client Automation では、ドメイン マネージャまたはエンタープライズ マネージャにある Microsoft SQL Server MDB で収集されたデータをリモートの SQL Server MDB または Oracle MDB のデータと同期できる機能が提供されます。このデータベース同期の機能では、たとえば、SQL Server または Oracle MDB を使用する CA Technologies Service Desk Manager および Asset Portfolio Management 製品の既存のインストールなどがサポートされます。同期機能の詳細については、「[MDB から別のターゲット MDB へのデータの同期](#) (P. 35)」を参照してください。

注: Unicenter Asset Portfolio Management 製品の統合を完全にサポートするには、RO02252 パッチをインストールする必要があります。インストールの手順については、Unicenter Asset Portfolio Management の Readme、RO02252 を参照してください。Unicenter Asset Portfolio Management および CA Service Desk Manager の詳細については、それぞれのマニュアルを参照してください。

MDB のインストール

管理データベース (MDB) は、スケーラビリティおよびパフォーマンスに関する要件に応じて、マネージャまたは別のコンピュータでローカルにインストールできます。DSM インストールキットでは、Windows および Solaris への MDB のインストールをサポートしています。

MDB のインストールの全体的な詳細については、「Client Automation のインストール」の章の「[管理データベース \(MDB\)](#) (P. 134)」を参照してください。

MDB の管理

データベース管理は、管理データベース (MDB) の正常度およびパフォーマンスを維持するのに不可欠です。このタスク用として、CA Technologies では CA Client Automation インストールメディア (DVD) の中に MDB メンテナンス スクリプトを提供しています。

MDB メンテナンス スクリプトの詳細については、「Client Automation のインストール」の章の「[管理データベース \(MDB\)](#) (P. 134)」を参照してください。設定およびメンテナンスに関する MDB 管理の特定の要件については、オンライン Client Automation ドキュメントセット (ブックシェルフ) の「*MDB Overview*」を参照してください。

エンジンの概念

エンジンはによって、スケーラビリティ サーバとドメイン マネージャおよび管理データベースとの間の通信サービスが提供されます。

エンジンの機能は、以下のとおりです。

- スケーラビリティ サーバからのコンピュータのインベントリの収集
- 設定データのスケラビリティ サーバへの書き込み
- エンタープライズとドメイン データベースとの間のデータのコピー (複製)
- 動的クエリ グループの評価の実行
- クエリ グループの評価に関連するアクションの実行
- スケジュール済みレポートの実行
- インベントリ ジョブ ステータスの通信

エンジンの管理面

エンジン タスクのステータスは、**DSM** エクスプローラで確認することができます。ここから、エンジン タスクを追加、変更、または削除することができます。

ドメイン マネージャおよびエンタープライズ マネージャの各インスタンスには、システム エンジンと呼ばれるデフォルトのエンジンが含まれています。

追加のエンジンをインストールして、デフォルトのエンジンのワークロードを解決することができます。

新しいスケーラビリティ サーバが展開されるごとに、エンジン収集タスクが自動的に作成され、デフォルトのシステム エンジンに対してスケジュールが設定されます。スケーラビリティ サーバのインストール処理中にこのタスクを処理するために、別のエンジンを指定することができます。

ドメイン マネージャがエンタープライズ マネージャにリンクされるたびごとに、エンジン複製タスクが自動的に作成され、デフォルトのシステム エンジンにリンクされます。

情報収集

エンジンの主なタスクは、アセット情報をスケーラビリティ サーバから収集することです。

DSM エージェントがスケーラビリティ サーバに初めて接続する場合に、作成されるリクエストを実行し、初期インベントリおよびシステム情報を保存します。

エンジンがスケーラビリティ サーバに接続すると、以下のタスクを実行します。

1. スケーラビリティ サーバの整合性を確認します。
2. エージェントが初めてそのサーバに接続しているかどうかを決定します。
3. アセットがシステム全体で新しいアセットである場合、データベースにアセットを作成します。
4. 既存のエージェントが提供するすべてのインベントリ情報を処理します。

収集された情報は、以下の形式になります。

- インベントリ（ハードウェアまたはテンプレート情報）
- ソフトウェア インベントリ（ヒューリスティックまたはシグネチャベース）
- 設定ファイル（`autoexec.bat` またはバックアップされるよう設定されたすべての `ini` ファイル）
- ジョブ ステータス
- モジュール ステータス
- エージェントの最終実行日時
- ソフトウェア使用状況の監視データ
- 関係情報（コンピュータ、ユーザ、およびデバイス間）

エンタープライズとドメインとの間のデータの複製

もう 1 つのエンジン タスクは、ドメインとエンタープライズ データベースとの間のデータの複製を処理することです。ドメイン マネージャ上の管理データベースからエンタープライズ データベース上の管理データベースへの複製は、複製ジョブによって実行されます。このジョブは、ドメイン マネージャのエンジン処理を利用して実行されます。

複製が開始されると、エンジンではドメインからエンタープライズ マネージャにプッシュされる必要がある情報、およびエンタープライズからドメイン マネージャにプルされる必要がある情報が決定されます。

通常、インベントリの属性などのホスト特有の情報は上方向に複製され、アセット グループなどの設定情報は下方向に複製されます。

各ドメイン マネージャと共に、デフォルトのエンジンがインストールされます。ドメイン マネージャがエンタープライズ マネージャにリンクされると、ドメインからエンタープライズへの複製タスクを実行するよう、そのエンジンが設定されます。

複製されるデータベース オブジェクト

以下の表に、エンタープライズからドメイン マネージャ（ダウン）、およびドメインからエンタープライズ マネージャ（アップ）に複製されるデータベース オブジェクトのリストを示します。

オブジェクト	複製の方向
検出されたコンピュータ	アップ

オブジェクト	複製の方向
検出されたユーザ	アップ
検出されたコンピュータ ユーザ (コンピュータとユーザとの関係)	アップ
Remote Control アドレス帳コンピュータ	ダウン
外部アセット定義	ダウン
外部アセット	アップ
コンピュータの一般インベントリ	アップ
追加インベントリ コンポーネント	アップ
注: デフォルトでは、これらのオブジェクトは複製されません。 エージェントの有効化/無効化の切り替えは、エージェントの [インベントリ] - [追加] <i>-<name-of-the module></i> ノードを右クリックし、 [ヒューリスティックをエンタープライズに複製] オプションを選択します。 変更された設定は、このグループ内のすべてのコンピュータに対して有効になります。	
外部アセット インベントリ	アップ
クエリ定義	ダウン
グループ定義	ダウン
グループ メンバシップ	ダウン
カスタムのソフトウェア定義	ダウン
カスタムに定義された製造者	ダウン
エンタープライズ マネージャのプロパティ	ダウン
ドメイン マネージャのプロパティ	アップ
コンピュータのソフトウェア インベントリ (シグネチャ スキャンに基づいて検出)	アップ
ヒューリスティック スキャンにより検出されたソフトウェア インベントリ	アップ
注: デフォルトでは、このオブジェクトは複製されません。複製は、 エージェントの [ソフトウェア] - [検出済み] ノードを右クリックし、 [ヒューリスティックをエンタープライズに複製] オプションを選択して、有効/無効を切り替えられます。 変更された設定は、 このグループ内のすべてのコンピュータに対して有効になります。	
Asset Management ジョブ	ダウン

オブジェクト	複製の方向
Asset Management ジョブのステータス	アップ
Asset Management モジュール	ダウン
Asset Management モジュールのステータス	アップ
Asset Management 設定ファイル定義	ダウン
Asset Management 設定ファイル	アップ
注: これらのファイルは、この情報を収集するリクエストがエンタープライズ マネージャで定義されている場合、エンタープライズ マネージャに対してのみ複製されます。ドメイン マネージャでこのリクエストが定義されている場合、データは上方向へは複製されません。	
Asset Management テンプレート定義	ダウン
Asset Management ポリシー定義	ダウン
ヘルス監視アラート	アップ

MDB から別のターゲット MDB へのデータの同期

お客様の実装によっては、Service Desk および Asset Portfolio Management などの CA Technologies 製品で、DSM マネージャが使用するデータベースとは別または異なる管理データベース（MDB）を使用する場合があります。

ただし、アセット管理タスクのさまざまな状況において、これらの CA Technologies 製品は Client Automation データに依存します。

そのため、Client Automation では、Client Automation が検出したデータをサポートし、Microsoft SQL Server（SQL Bridge）または Oracle（Oracle Bridge）に基づく別の MDB とのデータの同期をサポートするマネージャ機能を提供しています。同期の機能は、Client Automation アセットと DSM ドメインの SQL Server MDB または Windows 上のエンタープライズ マネージャに収集されたインベントリ データを、ターゲットの SQL Server または Oracle MDB で一致するデータと同期化します。

同期化は、スケジュールされた時間に実行されるエンジン タスクによって起動されます。このエンジン タスクを作成し、タスクのスケジュールを定義するには、DSM エクスプローラ GUI からエンジン タスク ウィザードを使用します。リモート コンピュータで個別のエンジンを使用して同期を実行することもできます。

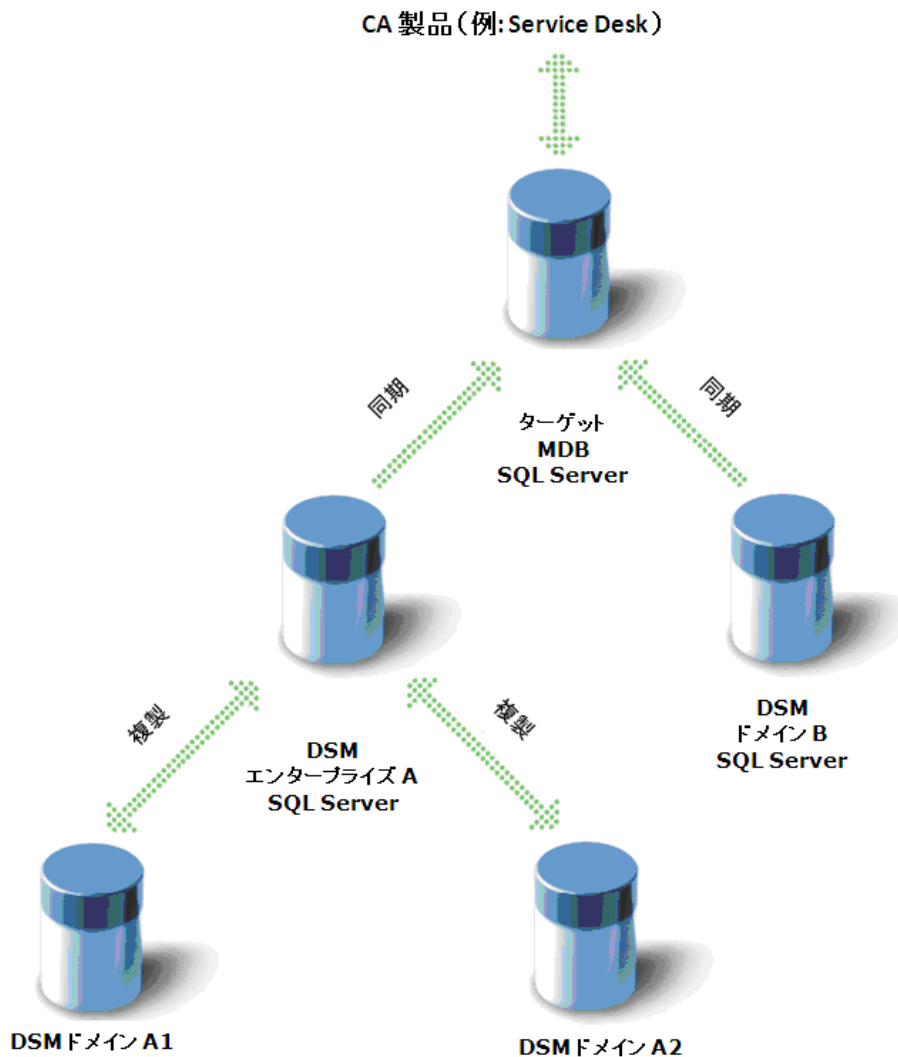
詳細については、「Client Automation のインストール」の章の「[管理データベース \(MDB\)](#) (P. 134)」を参照してください。

同期メカニズムのアーキテクチャ

同期メカニズムは、DSM ドメインマネージャとエンタープライズ マネージャ間で使用される複製メカニズムに似ています。

同期は、マネージャからターゲット MDB へ一方向に実行されます。これは、ターゲット MDB 上で同期されたデータがほかのプロセスによって変更されると、次回、同期メソッドがその特定のデータセットをマネージャの MDB からターゲット MDB に移動すると、同期されたデータが上書きされることを意味します。

以下の図は、それぞれが MDB を Microsoft SQL Server 上にホストしているエンタープライズ マネージャとドメイン マネージャから 1 つの SQL Server ターゲット MDB に同期が実行される特別なシナリオを示しています。



別のシナリオでは、MDB が Oracle ベースの可能性があります。エンタープライズ マネージャまたはドメイン マネージャ上の 1 つの SQL Server MDB を 2 つの異なるターゲット MDB に同期することも可能です。

サポートされるデータベース シナリオ

SQL ブリッジと Oracle ブリッジ同期機能のサポートについては、[互換性マトリックス](#)を参照してください。

SQL および Oracle Bridge でサポートされるデータベース シナリオ

SQL Bridge または Oracle Bridge に基づいて MDB に CA Service Desk Manager または CA IT Asset Manager をインストールした場合は、それらによってデータが入力されたテナント情報を Client Automation データベースに同期できます。

- SQL ブリッジおよび Oracle ブリッジの同期機能がサポートするデータベース シナリオについては、[互換性マトリックス](#)を参照してください。

CA Technologies 製品のサポート

SQL Server と Oracle ベースの MDB をサポートする CA Technologies 製品、CA Service Desk Manager および Unicenter Asset Portfolio Management の SQL Bridge および Oracle Bridge の同期機能については、[互換性マトリックス](#)を参照してください。

- **SQL Bridge :**

SQL Bridge を最大限活用するためには、Windows 用のテスト修正 T5D6008 を、CA Service Desk Manager r11.2 および Unicenter Asset Portfolio Management r11.3 がインストールされているマシンに適用する必要があります。テスト修正は、CA サポート オンラインから入手できます。テスト修正をダウンロードし、付属する Readme に記載されている詳細なインストール手順に従ってください。

- **Oracle Bridge :**

SQL Bridge を最大限活用するためには、新しいパラメータである dsm_oracle_ddl を AMS.Properties ファイルに追加し、CA Service Desk Manager が Oracle Bridge を有効化できるようにします。

```
dsm_oracle_ddl=1
```

ご使用のアプリケーション環境に SQL Bridge および Oracle Bridge をインストールする詳細については、「[SQL Bridge のインストール](#)」(P. 248)および「[Oracle Bridge のインストール](#)」(P. 249)を参照してください。

スケーラビリティ サーバ

Client Automation ではスケーラビリティ サーバによって、**Client Automation** エージェントとそのドメイン マネージャとの間のインターフェースを使用することができます。

スケーラビリティ サーバでは、最も基本的なレベルで、個々のエージェントが複数のホスト間で配信されるよう管理するワークロードを可能にします。すべてのエージェントが単一マネージャと直接通信するのではなく、複数のスケーラビリティ サーバ間でロードを共有することができます。たとえば、ソフトウェアパッケージは、エンド システムにダウンロードする前にスケーラビリティ サーバにステージングされ、インベントリは、マネージャにアップロードする前にスケーラビリティ サーバに保存することができます。

仮想アプリケーションに関して、スケーラビリティ サーバは仮想アプリケーション パッケージのストリーミング サーバとしても機能します。仮想アプリケーション パッケージは、**Windows** オペレーティング システムが稼働するターゲット コンピュータへストリーミングされます。

スケーラビリティ サーバは、ユーザ インターフェースを表示せず、バックグラウンドで実行される多数のシステム プロセスで構成されています。

基本的なスケーラビリティ サーバのサブコンポーネント

基本的なスケーラビリティ サーバのインストールは、以下のサブコンポーネントで構成されています。

- アプリケーション フレームワーク（登録関数付き）
- 共通サーバ機能

スケーラビリティ サーバによって、登録リクエストおよび基本インベントリ情報をエージェントから受信することができます。また、さまざまな管理情報および通知をマネージャに登録してマネージャ間で送受信することができます。

- ファイル ストア データベース

ファイル ストア データベースは、スケーラビリティ サーバで使用されるローカル リポジトリであり、エージェントを使用するために必要な情報が保管されます。最小限のスケーラビリティ サーバインストールでは、ファイル データベースは、登録済みエージェントのディクショナリとそれらエージェントによってレポートされる基本インベントリで構成されています。

基本的なスケーラビリティ サーバのタスク

基本的なスケーラビリティ サーバのインストールでは、以下のタスクを実行することができます。

- エージェントへの接続のための登録メカニズムを提供します。
- エージェントによってプッシュされる基本インベントリを受信します。
- スケーラビリティ サーバをマネージャに登録します。
- マネージャによってプッシュされるスケーラビリティ サーバの設定を受信します。
- マネージャによって要求されるエージェントの登録および基本インベントリ情報を転送します。
- マネージャからプッシュされたエージェント設定を転送します。

また、**Asset Management**、**Remote Control**、および **Software Delivery**（OS のインストール管理機能を含む）機能で製品固有のタスクを有効にすることができます。

注: スケーラビリティ サーバの **Software Delivery**（SD）機能を適切に運用するには、SD エージェントを各スケーラビリティ サーバにインストールします。スケーラビリティ サーバの誤作動を回避するには、SD エージェントをスケーラビリティ サーバから除去しないでください。

この場合、スケーラビリティ サーバのエージェントがそのスケーラビリティ サーバに登録されており、その他のスケーラビリティ サーバには登録されていない必要があります。これを検証するために、スケーラビリティ サーバ上で「**caf setserveraddress**」を実行すると、結果は「localhost」か、またはローカルホストを指す同等のアドレスになります。返されたアドレスが別のスケーラビリティ サーバを指している場合は、目的のスケーラビリティ サーバ上でコマンド「**caf setserveraddress localhost**」を実行して修正できます。

スケーラビリティ サーバおよび仮想アプリケーションの展開

仮想アプリケーション パッケージ登録ウィザード(仮想アプリケーション イメージのインポートおよびソフトウェア パッケージ ライブラリ内でのパッケージ作成に使用)は、各仮想アプリケーション イメージに対して以下のソフトウェア パッケージを作成します。

- ステージング - このパッケージは、パッケージ配信のスタンドアロンおよびストリーミング の両方のモード用の仮想アプリケーションへのアクセスを提供します。このパッケージには、仮想アプリケーション イメージが含まれています。
- スタンドアロン - このパッケージは、仮想アプリケーションをターゲット コンピュータにローカル インストールし実行するために使用されます。
- ストリーミング - このパッケージは、ストリーミング サーバから仮想アプリケーションをダウンストリームし、ローカル コンピュータ上で実行するために使用されます。

仮想アプリケーション ステージング パッケージをスケーラビリティ サーバに展開します。スケーラビリティ サーバは、仮想アプリケーションのストリーミング サーバとしても機能します。そのため、ステージング パッケージは、仮想アプリケーションをターゲット コンピュータにストリーム配信するためのスケーラビリティ サーバに展開します。

Microsoft App-V ストリーミング サーバは、ストリーミング通信用に 2 つのプロトコル、RTSP (セキュリティ保護なし) および RTSPS (セキュリティ保護あり) を使用します。Microsoft App-V ストリーミング サーバのデフォルトのプロトコルおよびポートは、RTSP とポート 554 です。セキュリティ保護された RTSPS プロトコルとポート 332 を使用する場合、ストリーミング サーバを設定する必要があります。Microsoft App-V ストリーミング サーバの設定の詳細については、Microsoft の製品ドキュメントを参照してください。

スタンドアロン パッケージおよびストリーミング パッケージをドメイン マネージャからターゲット コンピュータに展開します。また、ターゲット コンピュータへの展開の前に、パッケージをスケーラビリティ サーバにステージングすることができます。標準的な Software Delivery 展開メソッドを使用して、仮想アプリケーション パッケージをターゲット コンピュータに展開できます。

注: 仮想アプリケーション パッケージングおよび展開の詳細については、「Software Delivery 管理ガイド」を参照してください。

OS インストール管理ブート サーバのインストールについて

OS インストール管理（OSIM）ブート サーバは、スケーラビリティ サーバの一部としてインストールされます。ブート サーバのインストールでは、**TFTP** サーバ（アクセス権の制限付き）および **PXE** サーバが自動的に提供されます。

この機能を使用しない場合、以下の **CAF** コマンドを発行して、スケーラビリティ サーバのインストール中またはその後にブート サーバ サービスを無効にすることができます。

```
caf stop sdmpcserver
```

```
caf disable sdmpcserver
```

ブート サーバ サービスを再び有効にするには、以下の **CAF** コマンドを入力します。

```
caf enable sdmpcserver
```

```
caf start sdmpcserver
```

エージェント

エージェントはサポートされているすべての動作環境上のすべての管理対象エンドシステムに存在し、各エージェントが個々のタスクを実行します。

エージェントが ITCM マネージャに登録されている場合、ホスト **UUID** は、コンピュータを **MDB** 内の既存のコンピュータ レコードに照合するために使用される主な属性です。ホスト **UUID** に一致がない場合、ホスト名および **MAC** アドレスがコンピュータの照合に使用されます。

ホスト名および **MAC** アドレスの一致が見つかった場合は、コンピュータのホスト **UUID** が変更されたことを意味します。たとえば、**OS** の再インストールでは、それぞれのコンピュータのホスト **UUID** が変更されます。コンピュータ レコードは新しいホスト **UUID** で更新され、[クラッシュ後の再インストール] (**RAC**) **Software Delivery** ジョブ コンテナが作成されます。

ホスト名および **MAC** アドレスの一致が見つからない場合、新しいコンピュータが作成され、[クラッシュ後の再インストール] ジョブ コンテナは作成されません。

場合によっては、既存レコードに照合する代わりに、重複するコンピュータが作成されることがあります。このような場合に対応するため、ホスト名および **MAC** アドレスの一致アルゴリズムが改善されました。以前は、プライマリ **MAC** アドレスのみを使用して既存の **MAC** アドレスとの照合が行われていました。現在は、すべての標準 **MAC** アドレスのセットを使用して照合が行われます。誤った一致を避けるため、標準 **MAC** アドレスには、**VPN** からのアドレスなどの一時的な **MAC** アドレスは含まれません。

以下の表は、ホスト **UUID**、ホスト名、または **MAC** アドレスのいずれかが変更された場合に、新しいコンピュータが作成されるケース、および既存のコンピュータに照合されるケースについて簡単に示しています。

注: ハイフン (-) が記載されている場合は、システムが変更の検出を無視することを示します。

ホスト UUID の変更	ホスト名の変 更	標準 MAC の全変 更	プライマリ MAC の変更	新規アセットの 作成	RAC
N	-	-	-	N	N
Y	N	N	-	N	Y
Y	N	-	N	N	Y
Y	N	Y	Y	Y	N
Y	Y	-	-	Y	N

注: 仮想マシンのある環境（例：XenServer、Hyper-V、ESX）の場合、管理者は、ドメイン スペース内の各仮想マシンが一意の MAC アドレスを持っていることを確認する必要があります。

注: コンピュータがあらかじめ登録されている場合、管理者は、標準 MAC アドレスが入力されていることを確認する必要があります。

エージェント パッケージの概念

Client Automation の中のエージェント パッケージ（DSM エージェント）の概念によって、実際のエージェント機能が個別の言語リソースから区別されます。この概念は、エージェントの展開およびインストールに関して、以下の利点を提供します。

- 言語固有のエージェントのみの言語パッケージ

エージェント パッケージの概念により、個別に言語パッケージをインストールできます。言語パッケージには、エージェントのインストールに必要なすべての言語リソースが単一の言語に含まれています。

- 必要なコンポーネントのみを含む単一のインストールパッケージを作成することが可能

dsmPush スクリプトによって、たとえば、6 個の言語パッケージを持つ Asset Management および Software Delivery の機能を含む単一のパッケージなど、カスタマイズされた単一のパッケージを作成できます。

エージェント パッケージのフォーマットは、エージェントの機能に 0 個以上の言語パッケージを組み合わせたものです。言語パッケージを指定しないと、ENU（米英語）がデフォルトで使用されます。ENU リソースは、エージェント機能の一部として常に含まれるので、個別の言語パッケージとしては含まれていません。ただし、エージェントに対して、スタンドアロンの言語パッケージを展開することもできます。

注: 言語パッケージの詳細については、「Client Automation のインストール」の章の「インストール後の製品言語の変更」を参照してください。

DSM エージェントは、以下のプラグインを使用できます。

- CA DSM エージェント + Software Delivery プラグイン (SD エージェント)
- CA DMS エージェント + Remote Control プラグイン (RC エージェント)
- CA DMS エージェント + Asset Management プラグイン (AM エージェント)
- CA DMS エージェント + 基本インベントリ プラグイン (BHI エージェント)
- Software Delivery カタログ (SD カタログ)
- Remote Control ビューア (RC ビューア)
- たとえば、DTS (Data Transport Service) などの、エージェント側のすべてのコンポーネント

エージェントの設定

エージェントはドメイン マネージャによって集中管理されて設定されます。これらのタスクは、**DSM** エクスプローラを使用して実行されます。

Remote Control ビューア

Remote Control ビューア (RC ビューア) は、リモート コントロール サービスへのアクセスを提供するユーザ インターフェースです。インストールされると、RC ビューアに DSM エクスプローラ ツリーまたはコマンド ラインからアクセスすることができます。

Remote Control 機能では、Win32 または Web ブラウザ クライアントがサポートされます。ブラウザ クライアントでは、Microsoft Internet Explorer 6.0 がインストールされている必要があります。

この RC ビューアには、以下の機能が含まれます。

Remote Control

制御しているコンピュータが目の前にあるように操作することができます。

ファイル転送

ビューアとホスト コンピュータとの間でファイルを転送します。

チャット

リモート コントロールセッションの間に、インタラクティブなチャットセッションをユーザとの間で確立します。

セッションの記録

リモート コントロールセッションの記録を開始および停止します。

ソフトウェア カタログ

ソフトウェア カタログ（Software Delivery カタログまたは SD カタログとも呼ばれる）は、「セルフ サービス」を可能にするエージェントプラグインです。ソフトウェア カタログのウィザードベースのインターフェースを使用すると、管理者に提供されたライブラリからソフトウェアをコンピュータにインストールまたは除去することができます。

以下のスクリーンショットは、ソフトウェアの追加ウィザードの「はじめに」ページを示します。

ソフトウェアの追加:はじめに
戻る 次へ 完了 キャンセル

ソフトウェア カタログ > ソフトウェアの追加

1 はじめに
2 注文するソフトウェアを選択
3 インストール タイプの選択
4 注文の確認

コンピュータにソフトウェアを追加するには、ソフトウェア カタログを使用して「注文」する必要があります。ソフトウェア カタログで注文が受信され、処理されると、ご使用のコンピュータにソフトウェアが配信され、ほとんど操作することなく、自動的に使用可能となります。

このウィザードでは、4 つの簡単な手順でソフトウェア カタログのソフトウェアを注文する処理を示します。ソフトウェアは、ステージ 4 で注文を確認するまで配信されません。

注文できるソフトウェアのリストを参照するには、【次へ】ボタンをクリックします。

☒ このウィザードは常にステージ 2 で開始してください。今後変更が発生した場合は、ステージ 2 からここに戻り、このオプションを変更します。

ヘルプ
戻る 次へ 完了 キャンセル

以下のスクリーンショットは、ソフトウェアの追加ウィザードの「注文するソフトウェアの選択」ページの例を示します。

ソフトウェアの追加: 注文するソフトウェアを選択
戻る 次へ 完了 キャンセル

ソフトウェア カタログ > ソフトウェアの追加

1 はじめに
2 注文するソフトウェアを選択
3 インストール タイプの選択
4 注文の確認

このコンピュータで使用可能なソフトウェア

注文するソフトウェアを選択してください

ソフトウェア	コメント
☐ CA - Configurator 5.5	
☐ CA - MS Internet Explorer 6.0 SP1	
☐ Electronic Forms Designer 1.1	Fixes problems opening forms on Windows 98, NT, 2000 and XP
☐ Office XP Service Pack 2	
☐ Office XP SP1	
☐ Winzip 8.0 GA	This is the CA licensed version of Winzip

ヘルプ
戻る 次へ 完了 キャンセル

AM リモート エージェント

Client Automation は、以下の仮想化 UNIX 環境を含むプラットフォーム仮想化をサポートします。

- HP nPartition および仮想パーティション
- HP Integrity 仮想マシン
- IBM の論理パーティション
- SUN の動的システム ドメイン
- サン SPARC Enterprise M シリーズ サーバ上の SUN 動的システム ドメイン
- VMware ESXi 下で実行される仮想マシン。
- Citrix XenServer 下で実行される仮想マシン。

AM リモート エージェントが r12 Partitioned UNIX Server エージェントに取って代わります。その機能は AM リモート エージェントに完全に統合されます。このエージェントは、仮想ホストの情報を収集するために、DSM エクスプローラでのみ設定されます。

注: AM リモート エージェントの詳細については、「*Asset Management 管理ガイド*」を参照します。サポートされているプラットフォームの最新のリストについては、「[Compatibility Matrix](#)」を参照してください。

Web コンソール

Web コンソールは、ブラウザ ベースの CA Client Automation へのユーザ インターフェイスで、Windows および Linux の動作環境にインストールすることができます。

Web コンソールは、マネージャと同じコンピュータ上または別のコンピュータ（リモート Web コンソール）上にインストールできます。

Web コンソール アクセス

Web コンソールにアクセスするには、ブラウザを開き、アドレス バーに以下の URL を入力します。

`http://MyManager/wac`

MyManager は、Web コンソールがインストールされているコンピュータの DNS 名、ホスト名、または IP アドレスです。Web コンソールでは、コンピュータへログインするためにユーザが提供したクレデンシャルをベースに、ユーザのログインは自動的に行われます。Web コンソールのログインページにはドロップダウンがあり、それを使用して別のマネージャを指定できます。

Web コンソールの機能

Web コンソールを使用すると、簡単でありながら高機能な [検索] パネルを使用して、DSM オブジェクトにアクセスできます。オブジェクトが検索された後、タブ、ポートレット、ページセクション、およびナビゲーションリンクによって、豊富なブラウザ ベースのインターフェースが提供されます。

Web コンソールでは、DSM の情報に関する包括的なビューがユーザに提供されます。インストールされている製品およびコンポーネントに応じて、以下の項目が含まれます。

- コンピュータ
- グループ
- ユーザ
- ソフトウェア パッケージ
- ソフトウェア定義
- ジョブ
- ポリシー
- クエリ
- アラート

Web コンソールでは、以下のアクティビティを実行することもできます（適切な製品およびコンポーネントがインストールされている場合）。

- コンピュータの作成と削除
- グループの作成、変更、削除
- OS インストールジョブ
- ソフトウェアのインストール
- ソフトウェアのアンインストール
- ソフトウェアのインストール ジョブの設定
- ヘルス監視アラートの監視と追跡記録

Web コンソールは、URL を使用して、適切なオブジェクトの UUID へのアクセス権を持つほかのアプリケーションから、ジョブまたはポリシーのコンテキストで起動できます。

また、Web コンソールでは、CA Service Desk Manager アプリケーションも、ポリシー違反またはソフトウェアのジョブの失敗の結果引き起こされるチケット（発行）のコンテキストで起動することができます。

サポートされる Web ブラウザおよび Web サーバ

Web サーバおよびブラウザのサポートについては、「Compatibility Matrix」を参照してください。

DSM レポータ

DSM レポータは、情報をデータベースから抽出する場合に使用するクエリ ツールです。

レポートは、一時的またはスケジュールに基づいて生成することができます。DSM レポータでは、**Client Automation** データの値を分類、フィルタ、および表示することによって拡張します。また、DSM レポータでは、データを **.CSV** (*.csv) または **.HTML** (*.html) ファイルにエクスポートするオプションもあります。これらのファイルは、後でスプレッドシート、予算ツールなどにインポートすることができます。

DSM レポータ の見た目は、DSM エクスプローラと似ています。**Client Automation** ユニットおよびグループを印刷する、およびクエリに基づいた新しいレポートを作成するためのドラッグアンドドロップのオプションによって、DSM エクスプローラの拡張機能のように DSM レポータを使用することができます。

注: インストール後にはじめて DSM レポータを起動する際には、データベースにすべてのレポートテンプレートをインポートできるように十分な時間をとってください。ただし、レポートテンプレートのインポート中に何か問題が発生した場合、回避策としてレジストリ エディタを開いて

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥Unicenter

ITRM¥Reporter¥Library のサブキー を削除してください。サブキーの削除後、DSM レポータを再度起動してください。

Common Application Framework

DSM の各コンポーネントでは、CAF (Common Application Framework) が使用されます。CAF は、すべての DSM コンポーネントを 1 箇所で制御できるクロスプラットフォーム サービス コントローラです。

CAF では拡張性に優れたプラグイン モデルを使用して、必要に応じて DSM サービスを動的に提供します。各 CAF プラグインは、エージェント、スケーラビリティ サーバ、またはマネージャの機能を提供するプログラムです。CAF プラグインは、CAF 自体の拡張機能となることもあり、スケーラビリティ サーバへの登録やシステム イベントの検出などいくつかの共通サービスを提供します。

通常、CAF はブート時にすべてのプラグインを自動的に起動します。CAF はプラグインの起動および停止をコマンドラインから要求に応じて、特定の時間に行うことも、スケジューラを使用して定期的に行うこともできます。CAF を実行するスケジュールされたジョブを指定する方法については、付録の「[CAF スケジュール済みジョブ](#)」(P. 657)を参照してください。

CAF はプラグインに、ステータス情報および他のプラグインから送信されるルート メッセージのクエリを行うこともできます。

重要: Windows では、CAF はデフォルトでローカルシステム アカウントとしてログオンするようにインストールされます。セキュリティ上の理由から Net ログオン プロパティを変更する必要がある場合は、インストールの後、Windows の「コントロールパネル」から「管理ツール」、[サービス] を使用して変更する必要があります。ただし、権限が縮小されたアカウントに変更することによって、予期しない動作が発生したり、CA Client Automation の機能が低下する場合があります。

アプリケーション フレームワーク ユーザ インターフェース

アプリケーション フレームワーク (CAF) はバックグラウンドのサービスとして実行されるため、通常は操作を行う必要はありません。ただし、CAF にはコマンドライン インターフェース (caf コマンド) があります。管理者はこのコマンドライン インターフェースを使用して、以下の例にあるように CAF 機能にローカルおよびリモート アクセスを行うことができます。

- すべての CAF プラグインの現在のステータスに関する問い合わせ
- CAF と関連するすべてのプラグインおよびプロセスの起動および停止
- 個々のプラグインの起動、停止、およびステータスに関する問い合わせ
- プラグインの有効化および無効化

CAF のコマンドライン インターフェースでは、ほとんどの場合、コマンドの実行を指示するメッセージが CAF に送信されます。例外は、CAF サービスまたはデーモン自体を起動および停止するコマンドといくつかの設定コマンドです。

注: Windows Vista では、ほとんどの CAF コマンドで完全な管理者権限が必要とされます。Administrators グループに属しているユーザでも、管理者以外のユーザとしてログインしている場合は、ログイン ユーザの権限に基づいてコマンドライン ウィンドウが実行されます。CAF コマンドを実行する際は、関連するアイコンをクリックして、[管理者として実行] を選択してください。

システムトレイ

システムトレイは、CAF (Common Application Framework) などのシステム サービスにユーザがアクセスできるようにするツールです。

システムトレイは、UNIX 以外のオペレーティング システムのデスクトップのタスクバーにアイコンとして表示されます。アイコンを右クリックすると、ポップアップメニューから利用できるサービスの 1 つを選択することができます。必要に応じて、サービスの開始前にユーザ操作がシステムトレイ機能によってさらに要求される場合があります。

システムトレイを利用して使用できるサービス、およびシステムトレイアイコンがタスクバーに表示されるかどうかは、設定ポリシーによって決定されます。

Client Automation の実行時に、システムトレイおよびアイコンをコマンドラインから以下のコマンドを使用して制御することができます。

cfSysTray

システムトレイのステータスが設定ポリシーで [表示] に設定されている場合、システムトレイを開始します。アイコンがタスクバーに表示されます。

cfSysTray show

システムトレイが開始されていない場合は開始し、ステータスを設定ポリシーで [表示] に設定します。アイコンがタスクバーに表示されます。

cfSysTray stop

システムトレイを停止します。システムトレイアイコンがタスクバーに表示されなくなります。

cfSysTray hide

システムトレイを停止し、ステータスを設定ポリシーで [非表示] に設定します。システムトレイアイコンがタスクバーに表示されなくなります。

Linux で **Client Automation** システムトレイが機能するようにするには、**GIMP Toolkit GTK+ 1.2** (最小バージョン) をインストールする必要があります。GTK は、**Client Automation** には同梱されていません。必要なバージョンを www.gtk.org からダウンロードしてください。

ログ

共通コンポーネントライブラリ（CCL）では包括的なトレースがサポートされており、致命的エラーの診断に役立つクラッシュハンドラがあります。これらのサービスは、ほとんどのプラグインコンポーネントで利用および活用することができます。

CAF (Common Application Framework) サービスでは、アクティビティがログファイルに記録されます。詳細さはトレースレベルによって異なり、カスタマイズすることができます。ログファイルは、問題の分析に役立ちます。

トレースレベルは、デフォルトで **ERROR** に設定されています。より多くのトレース情報を取得する必要がある場合、以下の **cftrace** コマンドのいずれかを実行して、ソフトウェア配信機能または **Data Transport Service** のトレースレベルを **DETAIL** に変更できます。

```
cftrace -c set -f USD -l DETAIL -s 30000
```

```
cftrace -c set -f DTS -l DETAIL -s 30000
```

-s オプションでは、ログファイルのサイズを **30,000 KB** に設定します。デフォルトのサイズは **2,000 KB** ですが、**DETAIL** トレースレベルには小さすぎる可能性があります。（トレースファイルは設定済みトレースファイルのサイズおよび数が制限に到達した場合、上書きされます。）

Windows では、すべての CAF サービスのログファイルは、**install_dir¥logs**（デフォルト： **c:¥Program Files¥CA¥DSM¥logs**）にあります。

CA Client Automation のインストール中に作成されたログファイルは、ユーザの一時フォルダの下に置かれます。通常、環境変数 **%temp%** はこのフォルダを指します。

Linux では、すべての CAF サービスのログファイルは、**\$CA_DSM_BASEDIR/logs** にあります。

CA Client Automation のインストール中に作成されたログファイルは、**/opt/CA/installer/log** の下に置かれます。

トレース ログ ファイル

Client Automation コンポーネントは、実行中に、そのシステム アクティビティのトレース ログ ファイルを生成します。これらのログ ファイルを使用して、発生する可能性がある問題を分析し、そのトラブルシューティングを行うことができます。

各 **Client Automation** プロセスは、それ自身のトレース ログ ファイルに書き込まれます。 **comstore** にプロセスのトレース設定が含まれている場合、プロセスはトレース情報を定義済みファイルに書き込みます。 **comstore** にプロセスのトレース設定が含まれていない場合、プロセスはプロセス名前に基づいて命名されたファイルにそのトレース情報を書き込みます。同じプロセスの複数のインスタンスがある場合、各インスタンスを設定して、それ自身の一意の名前が付けられたファイルに書き込むようにできます。ただし、多数のトレース ファイルが作成されるのを防ぐために、この機能はデフォルトでは無効になっています。システムのトラブルシューティングを行う場合、この機能を有効にできます（共通設定を使用）。

プロセスのトレース レベルが **ERROR** に設定され、**ERROR** レベル トレースが開始された場合、**Client Automation** は追加の **INFO** レベル トレース情報をトレース ログ ファイルに書きこみます。この追加の **INFO** レベル情報は、エラーにつながったより低いレベルのトレースを提供することにより、エラーの内容について詳細な情報を提供します。

cnfcmda コマンドラインを使用して、トレース機能を制御するパラメータを設定できます。

注: **ccnfcmda** エージェント設定コマンドの詳細については、「<command>/?」と入力してください（コマンドプロンプトで実行）。

dsminfo 診断ツール

CA Technologies は、Client Automation がインストールされているシステムから、診断情報を収集する **dsminfo** ツールを提供しています。収集されたデータは、ログファイル、システム情報、ディレクトリ構造、レジストリおよび環境情報を含む単一のファイルに圧縮されます。この診断ツールは、**Client Automation** 製品インストールメディアの「**DiagnosticTools**」フォルダの下にあります。

Client Automation の問題が再現可能である場合は、以下のコマンドを実行してトレースレベルを **DETAIL** に変更してください。

```
cftrace -c set -l DETAIL
```

問題を再現し、**dsminfo** ツールを使って診断情報を収集してください。

注:

このツールの詳細については、製品インストールメディアの「**DiagnosticTools**」フォルダの下にある **DSMInfoReadMe.txt** ファイルを参照してください。

dsminfo ツールは、デフォルトでは「.7z」ファイルを作成します。これらのファイルは ZIP ファイルより高い圧縮を実行できます。そのため、CA へのアップロードが容易です。

共通設定

Client Automation は共通の設定コンポーネントを介して集中的に設定されます。共通の設定コンポーネントには、**Client Automation** の設定データへのアクセス、格納、および管理を行う機能があります。

設定パラメータ

設定の最小単位はパラメータです。パラメータは、コンピュータまたはコンピュータ グループに割り当てることができる設定ポリシーで分類することができます。

設定モデルでは、以下のオブジェクトが定義されます。

パラメータ

設定データが含まれています。パラメータには名前があり、少なくとも 1 つの値が含まれています。

パラメータ情報

パラメータに関する追加の情報が含まれています。

パラメータ セクション

論理的にグループを成すパラメータの集合です。たとえば、特定の関連機能を設定します。パラメータ セクションを使用して、パラメータ セットの階層構造が確立されます。

設定ポリシー

グループ固有またはコンピュータ固有のパラメータの集合です。

環境設定

設定の状態を表し、コンピュータまたはコンピュータ グループに割り当てられます。設定の値には、予定済み、スケジュール済み、アクティブ、またはエラーがあります。

設定パラメータの管理

マネージャにあるデフォルト ポリシー、つまり、デフォルト パラメータ セットには、リモート管理用のパラメータがあります。デフォルト ポリシーには、ローカルコンピュータで実行されているローカル アプリケーションのみに重要なパラメータは含まれていません。

デフォルト ポリシーのパラメータには、ローカル管理と集中管理の 2 種類の管理モードがあります。パラメータの管理モードはマネージャのみで変更することができます。

- ローカルに管理されるパラメータは、ローカル コンピュータで実行されるアプリケーションによって制御されます。
- 集中管理されるパラメータは、マネージャのポリシーによって制御され、ローカル アプリケーションにとっては読み取り専用です。集中管理されるパラメータは、ローカルに管理されるパラメータよりも優先されます。

Remote Control など、アプリケーションによってはスタンドアロン モードでインストールできるものもあります。スタンドアロン インストールを行った場合、設定パラメータはマネージャのデフォルト ポリシーでは制御されなくなり、パラメータ値はマネージャに報告されません。スタンドアロン モードはローカル管理および集中管理モードよりも優先されます。スタンドアロン モードは、アプリケーション (Remote Control など) のインストール中に設定します。

設定ポリシー

管理目的の場合、パラメータを設定ポリシーにグループ化することができます。これらのポリシーは、コンピュータまたはコンピュータのグループに割り当てることができます。

また、単一のコンピュータまたはグループを、複数の設定ポリシーに従わせることもできます。この場合、1 つのポリシーで定義されたパラメータ設定が、別のポリシーで定義されたパラメータと重複する場合があります。競合を解決するには、設定ポリシーが重複する場合に、以下のルールに準拠する必要があります。

- グループに割り当てられたポリシーは、グループの子に継承されます。子はグループまたはコンピュータの可能性がありえます。
- 階層では、子レベルに割り当てられたポリシーは、親レベルのポリシーを無効にします。つまり、親レベルで定義されたすべてのパラメータは、子に対しても定義されます。ただし、子のポリシーが親のポリシーを無効にする場合、子のポリシーが優先されます。

エージェントからの設定レポート

エージェントのパラメータ設定が変更されるごとに、その変更がマネージャに報告されます。マネージャでは、これらの設定が「設定レポート」として **DSM** エクスプローラで表示されます。

エンタープライズ マネージャのエージェントの設定

CA Client Automation のインフラストラクチャでは、共通設定アーキテクチャおよび手法が使用されています。管理者は **DSM** エクスプローラ インターフェースを使用して、設定ポリシーを変更します。これらの変更は、管理データベース (**MDB**) のドメインマネージャに保存されます。次に、変更は適用対象のエージェントに伝送されます。

1つの例外を除いたすべての場合において、これは簡単なソリューションです。エンタープライズ マネージャが存在する場合、設定管理アーキテクチャは、若干直感的でなくなります。

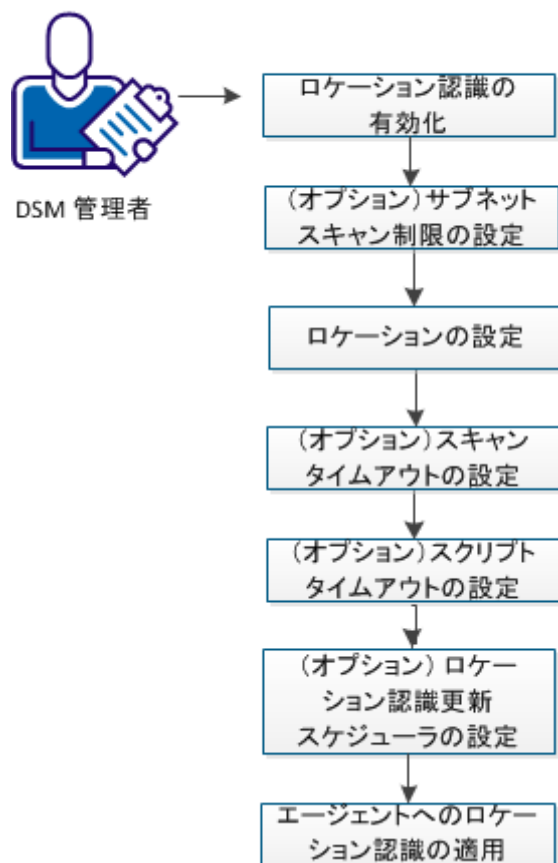
管理対象設定をサポートするには、エンタープライズ マネージャ自身が管理される必要があります。これには、エージェントのインストールが必要です。エージェントはスケーラビリティ サーバと通信し、次にスケーラビリティ サーバはドメインマネージャと通信します。このため、エンタープライズ マネージャのコンピュータを管理するスケーラビリティ サーバおよびドメイン マネージャを決定する必要があります。

ほとんどの組織で展開されるエンタープライズ マネージャは、1つのみです。

ロケーション認識を有効化および設定する方法

管理者は、ロケーション認識ポリシーを作成する必要があります。ロケーションの変更が検出された場合にコンピュータが適切なスケーラビリティ サーバにレポートするよう設定できます。DSM エージェント上でロケーション認識機能をポリシーに適用すると、コンピュータがロケーション認識ルールを評価できるようになります。

DSM エージェントのロケーション認識の有効化および設定方法



以下の手順に従います。

1. [ロケーション認識を有効にします](#) (P. 63)。
2. [\(オプション\) サブネット スキャンの制限を設定します](#) (P. 64)。
3. [場所を設定します](#) (P. 65)。
4. [\(オプション\) スキャンタイムアウトを設定します](#) (P. 72)。
5. [\(オプション\) スクリプトタイムアウトを設定します](#) (P. 72)。
6. [\(オプション\) ロケーション認識の更新スケジュールを設定します](#) (P. 73)。
7. [ロケーション認識をエージェントに適用します](#) (P. 76)。

ロケーション認識の有効化

ロケーション認識機能は、新規インストールまたはアップグレードのいずれかに対してはデフォルトで有効にされません。ロケーション認識ポリシーを有効にすることによって、エージェントの地理的な場所の変更を検出できます。変更が検出されると、エージェントはルールを評価し、次に、適切なスケーラビリティサーバに接続します。

重要: ロケーション認識機能を有効にする前に、ITCM 環境に存在する他のロケーション認識ソリューションを無効にしてください。

次の手順に従ってください:

1. [DSM] - [エージェント] - [共通エージェント] - [共通] - [ロケーション認識] の順に移動します。

以下のロケーション認識パラメータが表示されます。

- 有効
- サブネット スキャンの制限
- 場所
- スキャン タイムアウト
- スクリプト タイムアウト

2. [有効] を選択し、[タスク] ポートレットで [プロパティの設定] をクリックします。

[プロパティの設定] ダイアログ ボックスが開きます。

3. [値] フィールドから **True** (はい) を選択し、[OK] をクリックします。

ポリシー内で機能が有効になります。ポリシーは、封印してエージェントに適用するまでアクティブになりません。

注:

- エージェントがスケーラビリティサーバと同じコンピュータで実行されている場合、ロケーション認識ポリシーは常に無効になります。
- エージェント スケーラビリティサーバが一元管理として設定されている場合、エージェントのロケーション認識機能は、ルール評価後の値を変更できません。

(オプション)サブネット スキャンの制限の設定

サブネット スキャンの制限により、他のドメイン内のスケーラビリティ サーバを検出するためのサブネットのスキャンを可能にするかどうかを設定します。

次の手順に従ってください:

1. ロケーション認識設定ポリシーに移動します。
ロケーション認識パラメータが右ペインに表示されます。
2. [サブネット スキャンの制限] をダブルクリックします。
3. [タスク] ポートレットの [プロパティの設定] をクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
4. [値] フィールドで、お使いの環境に適切な値に変更します。
デフォルト: はい (True)
5. [OK] をクリックします。
[サブネット スキャンの制限] パラメータが設定されます。

場所の設定

ロケーションルールを定義することにより、地理的な場所の変更をサポートし、エージェントが適切なスケーラビリティ サーバに接続できるようにします。エージェントは、どのスケーラビリティ サーバに接続するかを判断するために作成されたルールを評価します。

次の手順に従ってください:

1. [場所] を選択し、[タスク] ポートレットで [プロパティの設定] をクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. ルールを設定するために [行の追加] をクリックします。
以下のパラメータを持つ行が、現在のテーブル構造に追加されます。
 - 場所の名前
 - 優先度
 - アドレス範囲
 - スケーラビリティ サーバ
 - サブネット スキャン
 - スクリプト
3. 各パラメータを設定し、[OK] をクリックします。
場所パラメータ設定が設定されました。

重要: この機能では、アドレス範囲、サーバ名、サブネット スキャン、スクリプトの値を完全には確認または検証しません。これらのパラメータは注意して設定してください。

ロケーション ルールの優先度の設定

どのロケーションルールを処理するかを選択する優先度を指定できます。エージェントはルールを評価し、指定された優先度を使用して適用するルールを判断します。

たとえば、2つのルール（ルール A とルール B）を作成したとします。ルール A には優先度 1 を指定し、ルール B には優先度 2 を指定したと仮定します。ルール A とルール B の他のすべてのパラメータに同じ値を設定した場合、エージェントでは 2 つの一致が検出されます。しかし、ルール A の優先度の方が高いので、ルール A が適用されます。

次の手順に従ってください:

1. [優先度] の下の新しい値をダブルクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. [値] フィールドでロケーション ルールに対する優先度を指定し、[OK] をクリックします。

最高優先度： 0

最低優先度： 99999

ロケーション ルールの優先度が設定されました。

ロケーション ルールのアドレス範囲の設定

エージェントアドレスが IP アドレス範囲の条件に一致する場合、ロケーションルールは選択に含まれます。ロケーション認識機能は、IPv4 および IPv6 の両方のアドレスをサポートします。エージェントが複数のルールに一致する場合、ルールの優先度の値を使用して、使用するサーバを判断します。

次の手順に従ってください:

1. アドレス範囲列の新しい値をダブルクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. [値] フィールドにアドレス範囲を入力し、[OK] をクリックします。

制限: 最小値は 1 です。

IPv4 を使用する場合、アドレス範囲列に IP アドレス、IP ワイルドカード、または IP 範囲を指定できます。以下に例を示します。

- IP アドレス形式: 192.168.1.1
- IP ワイルドカード形式: 192.168.1.*
- IP 範囲形式: 192.168.2.1-192.168.2.100

IPv6 を使用する場合、アドレス範囲列にさまざまな IPv6 アドレス プレフィックスを指定できます。以下に例を示します。

2001:DB8::/48

組織、サイト、サブサイト、サブネットを特定します。48 はプレフィックスの長さ (ビット) で、許可される最大ビット数は 64 です。

特別なアドレス プレフィックス:

FE80::/64

リンク ローカル プレフィックスとの照合に使用します (ローカル サブネット)。

FEC0::/64

サイト ローカル プレフィックスとの照合に使用します。

::/0

すべての IPv6 アドレスとの照合に使用します。

マルチキャスト グループ アドレス:

FF02::1

ローカル ネットワーク セグメントの全ノードとの照合に使用します (リンク ローカル)。

FF05::1

サイト ネットワーク上の全ノードとの照合に使用します（サイトローカル）。

FF08::1

組織ネットワーク上の全ノードとの照合に使用します（組織ローカル）。

ロケーション ルールに対するアドレス範囲が設定されました。

ロケーション ルールのスケーラビリティ サーバの設定

[スケーラビリティ サーバ] 列の値を指定して、エージェントが接続するスケーラビリティ サーバの IP アドレス **FQDN**（完全修飾ドメイン名）を定義します。

次の手順に従ってください:

1. [スケーラビリティ サーバ] の下の新しい値をダブルクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. アドレス範囲内に存在するエージェントが接続するスケーラビリティ サーバの IP アドレスまたは **FQDN** を入力します。

ロケーション ルールに対するスケーラビリティ サーバが設定されました。

注: スケーラビリティ サーバを指定する場合は、[サブネット スキャン] 列および [スクリプト] 列を空にしておきます。スケーラビリティ サーバを使用していない場合は、[スケーラビリティ サーバ] 列を空にしておきます。

ロケーション ルールに対するサブネット スキャンの設定

サブネット スキャン設定は、指定されたサブネットのスキャンに対してルールを定義し、そのサブネット上のアクティブなスケーラビリティ サーバをすべて検出します。エージェントは、他のルールと、アクティブなサーバの予測応答数を評価し、最適なサーバを選択します。ロケーション認識機能は、IPv4 および IPv6 の両方のアドレスをサポートします。

次の手順に従ってください:

1. サブネット スキャン列の新しい値をダブルクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. [値] フィールドにサブネット スキャンを入力し、[OK] をクリックします。
IPv4 を使用する場合、サブネット スキャン列に IP アドレス、IP ワイルドカード、または IP 範囲を指定できます。
IPv6 を使用する場合、サブネット スキャン列にさまざまな IPv6 アドレスプレフィックスを指定できます。
ロケーション ルールに対するサブネット スキャンが設定されました。

注: サブネット スキャンを指定する場合は、[スケーラビリティ サーバ] と [スクリプト] 列を空にしておきます。サブネット スキャンを使用していない場合は、[サブネット スキャン] 列を空にしておきます。

ロケーション ルールのスクリプトの設定

エージェントで実行されるスクリプトを追加し、使用するスケーラビリティ サーバを決定することができます。追加したスクリプトは、エージェント コンピュータに配布する必要があります。

次の手順に従ってください:

1. [スクリプト] 列の新しい値をダブルクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. [値] フィールドで、DM スクリプトの名前を指定し、[OK] をクリックします。

注: スクリプトの場所は、絶対パスまたは相対パスで指定できます。相対パスは、ITCM インストール ディレクトリ (通常は以下のいずれか) に対する相対パスになります。

Windows の場合

C:\Program Files(x86)\CA\DSM

UNIX/Linux の場合

/opt/CA/DSM

この機能では、以下のパラメータがサーバ選択スクリプトへ渡されます。

-o <出力ファイル名>

特定するスケーラビリティ サーバの名前をスクリプトが書き込むファイルの名前を指定します。

-x <エラー ファイル名>

生成されたエラー情報をスクリプトが書き込むファイルの名前を指定します。

-a <照合アドレス>

このアドレスに一致すると、このスクリプトを実行することになります。

DM スクリプトがロケーションルールに対して設定されました。

注: スクリプトを指定する場合は、[スケーラビリティ サーバ] と [サブネット スキャン] の列を空にしておきます。サブネット スキャンを使用していない場合は、[サブネット スキャン] 列を空にしておきます。

例:

```
rem -----  
rem Simple location aware server identification script  
rem This script writes a hard coded server name to the output file
```

```
rem -----  
  
dim sMatchingAddress as string  
dim sOutputFileName as string  
dim sErrorFileName as string  
  
dim X as Integer  
FOR X=0 to argc()  
  
    rem Read the output file from the provided parameters  
  
    if ( argv(X)="-o") THEN  
        sOutputFileName = argv(X+1)  
    ENDIF  
  
    rem read the matching address from the provided parameters  
  
    if ( argv(X)="-a") THEN  
        sMatchingAddress = argv(X+1)  
    ENDIF  
  
    rem read the matching address from the provided parameters  
  
    if ( argv(X)="-x") THEN  
        sErrorFileName = argv(X+1)  
    ENDIF  
  
NEXT X  
  
Dim fHandle as integer  
  
fHandle = OpenFile(sOutputFileName,0_WRITE)  
IF NOT(EOF(fHandle)) Then  
    WriteFile(fHandle,"sampleserver.ca.com")  
    CloseFile(fHandle)  
    exit  
ENDIF  
exit
```

(オプション)スキャン タイムアウトの設定

サブネット スキャンを使用する場合、スキャン タイムアウト設定により、スキャンでスケーラビリティ サーバからの応答を待機する最大の間隔を決定します。

次の手順に従ってください:

1. [スキャン タイムアウト] をダブルクリックし、[タスク] ポートレット内の [プロパティの設定] をクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. [値] フィールドで、お使いの環境に適切な値に変更して、[OK] をクリックします。

デフォルト : 30

スキャン タイムアウト パラメータが設定されました。

(オプション)スクリプト タイムアウトの設定

スクリプト タイムアウト設定は、スクリプトを実行する時間の最大の間隔を決定します。指定された間隔が経過すると、スクリプトは実行を停止します。

次の手順に従ってください:

1. [スクリプト タイムアウト] を選択し、[タスク] ポートレットで [プロパティの設定] をクリックします。
[プロパティの設定] ダイアログ ボックスが開きます。
2. [値] フィールドで、お使いの環境に適切な値に変更して、[OK] をクリックします。

値 :

- 0 : 無限タイムアウト
- >0 : タイムアウトするまでスクリプトを実行する秒数
- 許可される最大タイムアウト値 : 600 秒 (10 分)

デフォルト : 300

スクリプト タイムアウト パラメータが設定されました。

(オプション)ロケーション認識の更新スケジュールの設定

[ロケーション認識の更新] ポリシー グループ フォルダには、CAF を定期的にサーバに登録するジョブが含まれています。ポリシー パラメータ値を変更するには、ポリシーをダブルクリックして [プロパティの設定] ダイアログ ボックスを表示します。

CAF スケジューラ: コマンドライン

このジョブを実行する CAF コマンドを定義します。

デフォルト: location aware

CAF スケジューラ: 除外する日

スケジュールから除外する日 (曜日) を指定します。月、火、水、木、金、土、日を自由に組み合わせた値を指定します。複数の値はスペースで区切ります。

デフォルト: 空

CAF スケジューラ: 有効

登録更新ジョブを有効にするかどうかを指定します。

デフォルト: はい (True)

CAF スケジューラ: 時間

日単位のスケジュールの場合は、ジョブを実行する時間を定義します。このポリシーは、時間単位および分単位のスケジュールには使用しません。

デフォルト: 12

CAF スケジューラ: 除外する時間

スケジュールから除外する時間を指定します。24 時間の単位で時間を指定します。複数の値はスペースで区切ります。

デフォルト: 空

CAF スケジューラ: 分

日単位のスケジュールの場合は、ジョブを実行する時間に続いて分を定義します。このポリシーは、分単位のジョブには使用されません。

デフォルト: 0

CAF スケジューラ: ランダムな分

random_minute ジョブに追加する分数を定義します。ジョブは、指定された時間にランダムな分数（指定された値を最大とする）を追加した時間に実行されます。エージェントの接続時間を厳密に指定しないことにより、ポリシーではジョブを「あいまいな」間隔で定期的に行い、サーバの負荷を分散します。

デフォルト： 90

CAF スケジューラ: ランダムな現在時間

random_now ジョブが開始されるまでの最大時間を秒数で定義します。ジョブは、指定されたランダムな秒数が経過するまでに実行されます。このポリシーにより、同時に起動されたコンピュータがそれぞれのジョブを同時に開始しないようになります。

デフォルト: 0

CAF スケジューラ: 繰り返し

ジョブを繰り返す間隔を定義します。この値はジョブタイプによって異なります。たとえば、タイプが日単位 (**day**) の場合、この値はジョブが実行される間隔の日数を表します。

デフォルト: 1

CAF スケジューラ: ジョブのタイプ

スケジュール間隔のタイプを指定します。有効な値は、日 (**day**)、時間 (**hour**)、分 (**minute**) です。また、必要に応じて以下の修飾子を追加できます。

random

指定したジョブの時間から、[ランダムな分] の値を最長として、ランダムな時間の経過後にジョブを実行します。

random_hour

1 日のうちランダムな時間に実行します。

random_minute

1 時間のうちランダムな分に実行します。

now

指定された時間になったらジョブをすぐに起動します。

複数の値はスペースで区切ります。

例:

毎日午後 2:30 に **amagent** ジョブを実行する場合。

```
type="day", repeat=1, hour=14, minute=30, cmd="start amagent"
```

CAF が開始したときに、毎日 (週末を除く) 午前 1:00 から午前 2:30 の間でランダムに **amagent** ジョブを実行する場合。

```
type="day now random", hour=1, minute=0, randomminutes=90,  
excludedays="Saturday Sunday", cmd="start amagent"
```

エージェントへのロケーション認識の適用

ポリシーを作成して封印したら、アセット（コンピュータまたはグループ）に適用します。

次の手順に従ってください: (アセットに対して)

1. ツリー ビューの [コントロール パネル] ノードの下に [設定ポリシー] フォルダに移動します。
2. 適用するポリシーを右クリックし、コンテキスト メニューから [コピー] を選択します。
3. ツリー ビューで、アセットを選択して右クリックし、コンテキスト メニューから [貼り付け] を選択します。

ポリシーがアセットに適用されます。

次の手順に従ってください: (複数のアセットまたはグループに対して)

1. ツリー ビューで、アセットまたはグループを選択します。
2. 強調表示したターゲットを右クリックし、コンテキスト メニューから [貼り付け] を選択します。

別のコンテキスト メニューが表示されます。

3. [設定ポリシー] をクリックします。
[ポリシーのスケジュール] ダイアログ ボックスが開きます。
4. ポリシーをアクティブ化するためにスケジュールを設定します。

注: 1つのアセットまたはグループにポリシーを適用すると、[カスタマイズ およびプレビュー] ボタンが有効になります。複数のアセットまたはグループにポリシーを貼り付ける場合は、このボタンが無効になります。

5. [OK] をクリックして、複数のアセットまたはグループにポリシーを適用します。

DSM エージェントに対してロケーション認識機能が正常に有効化され設定されました。

サポートされているオペレーティング環境

CA Client Automation (Client Automation) では、主な動作環境がすべてサポートされています。サポートされているオペレーティング システムの最新のリストについては、互換性マトリックスを参照してください。

注: このドキュメントでは、UNIX という用語は UNIX の派生物である AIX、HP-UX、Solaris、Mac OS X を意味します。このリリースのシステム コンポーネントまたはソフトウェア機能が一部の UNIX 派生物に適用されない場合、コンポーネントまたは機能の説明で明記されます。

ハードウェアの仕様および要件

以下の表では、このリリースに対して推奨されるハードウェアの仕様および要件の最小値を示します。

実際のハードウェア要件は、システムの負荷（頻度、収集および転送されるデータの量、および操作数など）に依存します。

エンタープライズ マネージャの仕様

DSM エンタープライズ マネージャの最小ハードウェア構成要件は以下の通りです。

コンポーネント	速度/サイズ
DVD-ROM ドライブ	任意
CPU	1 つまたは 2 つの CPU、2GHz。 注: MDB が DSM エンタープライズ マネージャと同じコンピュータでホストされる場合、2 つの CPU が必要です。
メモリ	最小 2 GB。 注: MDB が DSM エンタープライズ マネージャと同じコンピュータでホストされる場合、4 GB 以上の RAM が必要です。

コンポーネント	速度/サイズ
空きディスク領域	最小 30 GB 注: MDB が DSM エンタープライズ マネージャと同じコンピュータでホストされる場合、100 GB 以上必要です。 重要: 必要な MDB ディスク容量は MDB と同じディスクパーティションに存在する必要があります。 ソフトウェア パッケージ ライブラリ用の追加領域を確保してください。必要な総領域は、格納されるパッケージの数とサイズによって異なります。
NIC	100 Mbps

ドメイン マネージャの仕様

DSM ドメイン マネージャの最小ハードウェア構成要件は以下の通りです。

コンポーネント	速度/サイズ
DVD-ROM ドライブ	任意
CPU	1 つまたは 2 つの CPU、2GHz 注: MDB が DSM ドメイン マネージャと同じコンピュータでホストされる場合、2 つの CPU が必要です。
メモリ	最小 2 GB。 注: MDB が DSM ドメイン マネージャと同じコンピュータでホストされる場合、4 GB 以上の RAM が必要です。
空きディスク領域	最小 30 GB 注: MDB が DSM ドメイン マネージャと同じコンピュータでホストされる場合、100 GB 以上必要です。 重要: 必要な MDB ディスク容量は MDB と同じディスクパーティションに存在する必要があります。 ソフトウェア パッケージ ライブラリ用の追加領域を確保してください。必要な総領域は、格納されるパッケージの数とサイズによって異なります。
NIC	100 Mbps

スケーラビリティ サーバの仕様

DSM スケーラビリティ サーバの最小ハードウェア構成要件は以下の通りです。

注: これらの最小要件はサポート対象のすべての Windows、RedHat および SuSE オペレーティング環境に当てはまります。

コンポーネント	速度/サイズ
CPU	1 CPU、2 GHz
メモリ	2 GB
空きディスク領域	30 GB
NIC	100 Mbps

エージェントの仕様

DSM エージェントの最小ハードウェア構成要件は以下の通りです。

注: これらの最小要件はサポート対象のすべてのエージェント環境に当てはまります。

コンポーネント	速度/サイズ
CPU	1 CPU、2 GHz
メモリ	256 MB
空きディスク領域	300 MB
NIC	10 Mbps

DSM エクスプローラの仕様

DSM エクスプローラの最小ハードウェア構成要件は以下の通りです。

注: これらの最小要件はサポート対象の Windows オペレーティング環境にのみ当てはまります。

コンポーネント	速度/サイズ
DVD-ROM ドライブ	任意
CPU	1 CPU、2 GHz

コンポーネント	速度/サイズ
メモリ	2 GB
空きディスク領域	30 GB
NIC	100 Mbps
ディスプレイ アダプタ	1024x768 の解像度

Windows 版 SQL Server MDB の仕様

Windows 上の Microsoft SQL Server 管理データベース (MDB) の最小ハードウェア構成要件は以下の通りです。

コンポーネント	速度/サイズ
DVD-ROM ドライブ	任意
CPU	2 CPU、2GHz
メモリ	4 GB
空きディスク領域	100 GB
NIC	100 Mbps

Oracle MDB の仕様

複数の Oracle MDB インスタンスをインストール場合の最小ハードウェア構成要件は以下の通りです。

コンポーネント	速度/サイズ
DVD-ROM ドライブ	任意
CPU	2 CPU、1.5GHz
メモリ	設定された Oracle データベース インスタンスごとに、最低 3.2 GB (SGA : 2.7 GB、PGA : 0.5 GB) のメインメモリが必要です。 これは、最大で 10,000 台のコンピュータ アセットをインストールする場合の推奨値です。
空きディスク領域	100 GB
NIC	100 Mbps

デバイスのインベントリおよび管理

CA Client Automation (Client Automation) のアセット管理機能は、ディスカバリおよびエージェント展開のプロセスを通じて、エンタープライズ ネットワーク上のデバイスのインベントリおよび管理を行うための簡単な自動化されたメカニズムを管理者に提供します。検出されたデバイスに対するインストールされたエージェントのプロビジョンが、継続的なデバイスの集中管理および制御を可能にします。

このセクションでは、以下のアセット管理機能に関する情報を提供します。

- [基本インベントリ コンポーネント](#) (P. 81)
- [非常駐インベントリ サポート](#) (P. 82)

アセット管理機能、コンポーネント、および要件の詳細については、CA Client Automation ドキュメントセットの一部である「*Asset Management Administration Guide*」を参照してください。

基本インベントリ コンポーネント

基本インベントリ コンポーネントでは、ローカル コンピュータに関する、ハードウェア情報の動的サブセットが検出され、この情報がほかの DSM コンポーネントで利用できるようになります。インベントリ情報の詳細は、ハードウェア環境とそれが実行されているプラットフォームに依存します。

基本インベントリ情報には、以下のようなハードウェア情報が含まれます。

- システム (たとえば、アセット タグ、モデル、プロセッサ、またはメモリ)
- オペレーティング システム (たとえば、言語、オペレーティング システム、サービス パック、またはバージョン)
- システム デバイス (たとえば、ネットワークまたはビデオ アダプタ)
- ネットワーク (たとえば、コンピュータおよびドメイン名、IP アドレス/ IPv6、または TCP/IP)
- ファイル システム (たとえば、ローカル ファイル システムまたはパーティション)
- システム ステータス (たとえば、ハードウェアの最後のスキャン)

注: CA Client Automation で実行中の言語にかかわらず、このインベントリ情報は常に英語で使用可能です。

非常駐インベントリ サポート

アセット管理の非常駐インベントリ サポート機能によって、エンタープライズ管理者がインベントリされたデバイスに永続的な影響を与えることなく、ネットワークをインベントリできるようになり、このことによってインベントリ機能が補完されます。NRI では、エンドユーザが Web ページに誘導され、システムのインベントリを収集する選択的なソリューションや、エンタープライズ管理者がたとえばログオン スクリプトによってインベントリ収集を開始する管理ソリューションが提供されます。

NRI サポートでは、Asset Collector および Web コンソールとともに 一般的な DSM エージェントのコンポーネントが使用されます。

NRI を使用するには、少なくとも 1 つの Web コンソール（および関連する Web サービス）と 1 つの Asset Collector が、非常駐インベントリが収集され保存されるドメインマネージャごとにインストールされている必要があります。最も単純なシナリオでは、各ドメインマネージャが単一の Web コンソールと Asset Collector を共同でホストする場合があります。より大規模で拡張可能なシナリオでは、多くのスケーラビリティ サーバが Web コンソール と Asset Collector を共同でホストする場合があります。

NRI は、CA Client Automation の設定プログラムを通じて、アセット管理機能の一部としてインストールされます。NRI の設定は、簡単な設定ファイル（スクリプト ファイル）によって行うことができます。

NRI は Windows、Linux および UNIX ターゲット コンピュータ上でのインベントリ処理をサポートしています。また、NRI の管理コンポーネントも、Windows で動作するマネージャおよびスケーラビリティ サーバでのみサポートされています。

NRI の制限事項

「root」ユーザ（UNIX および Linux の場合）、または管理者アカウント（Windows の場合）に比べて限られた権限を持つ標準的なドメイン ユーザ アカウントを使用して NRI を実行する場合、通常の Client Automation エージェントに比べて NRI エージェントによってレポートされるインベントリはより小さくなります。

NRI の実行に使用される特権に基づいて、NRI エージェントは可能な限り多くの情報を収集します。

注: NRI の詳細については、「Asset Management 管理ガイド」を参照してください。

第 2 章: インフラストラクチャ インプリメンテーションの計画

本章では、CA Client Automation の要件およびスケーラビリティに関する重要な情報について説明します。ここで取り上げられている情報は、DSM コンポーネントの導入前に熟読し、理解する必要があります。

このセクションには、以下のトピックが含まれています。

[IPv6 サポート \(P. 83\)](#)

[FIPS 140-2 のサポート \(P. 90\)](#)

[フェールオーバーサポートおよびハードウェアの置き換え \(P. 92\)](#)

[Client Automation インストール用の CA HIPS の設定 \(P. 97\)](#)

[インフラストラクチャ コンポーネントに関する考慮事項 \(P. 98\)](#)

[内部の依存関係 \(P. 113\)](#)

[Windows でのその他の製品との依存関係 \(P. 115\)](#)

[Linux および UNIX でのその他の製品との依存関係 \(P. 118\)](#)

IPv6 サポート

IPv6 (Internet Protocol version 6) は、IPv4 の後継となるインターネットプロトコルの次期バージョンとして、一般的な用途に正式に採用されています。IPv6 は、ネットワークでつながったデバイスにより多くのアドレスをに提供する（たとえば、携帯電話やモバイル電子デバイス）がアドレスをそれぞれ持てる）ことを目的としています。

IPv6 は、128 ビットアドレスをベースにして動作するようになっているので、ばく大なアドレス空間を提供します。この巨大なアドレス空間により、特定のドメインで無限とも言えるアドレスの階層および割り当てが可能となります。またこのプロトコルによって、自動設定、セキュリティ、簡易ルーティングなどのサービスをより向上させることもできます。

Client Automation は、IPv6 に準拠しており、純粋な IPv4 環境、純粋な IPv6 環境、および IPv4/IPv6 が混在した環境で機能します。

IPv6 を使用すれば、ネットワーク アダプタに IPv6 アドレスを複数個持たせたり、IPv4 アドレスと IPv6 アドレスを両方持たせたりすることができます。マネージャやスケーラビリティ サーバなどを識別するには、完全修飾ドメイン名 (FQDN) を使用することを強くお勧めします。

IPv6 サポート関連での制限事項

以下の制限が、CA Client Automation（Client Automation）における IPv6 サポートとの関連で適用されます。

- comstore にあるプロトコルの優先順位パラメータを「ipv6,ipv4」に設定して Oracle MDB を使用すると、製品の動作が遅くなる傾向があります。これは、Oracle データベースに対して最初に IPv4 アドレスではなく IPv6 アドレスを使って接続しようとするからです。つまり、IPv6 アドレスによる接続が失敗して、その後に IPv4 アドレスでデータベースに接続するので、その分、時間がかかるからです。このようなパフォーマンスの低下を防ぎながら製品のほかの部分では IPv6 アドレスを優先的に使用し続けるには、レジストリの中に HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥Unicenter ITRM¥ UseIPv4ForDB という DWORD を作成してその値を 1 に設定してください。
- OS インストール管理（OSIM）は、IPv4 をサポートするネットワークでのみ利用できます。これは、OSIM が、IPv4 に依存する PXE に依存しているためです。
- Client Automation では、以下の 2 つの場合を除いて、インフラストラクチャ コンポーネントにアドレス指定する場合に、リンク ローカルアドレスがサポートされません。
 - Remote Control ビューアから Remote Control ホストへ接続する場合は、リンク ローカルアドレスを Remote Control ビューアに入力することができます。
 - ローカル ネットワークを参照するのに Remote Control を使用する場合は、リンク ローカルアドレスが表示され、選択できます。

注: リンク ローカルアドレスは、インベントリ収集および表示の一部として収集され表示されます。

- Software Delivery（SD）ジョブ用の NOS ダウンロード方法は、以下の条件下では、純粋な IPv6 上ではサポートされません。
 - すべてのプラットフォーム上のエージェントは、Samba または NFS を使用しています。
 - エージェントは、Windows Vista よりも古い Windows プラットフォームで Microsoft NOS を使用しています。

ただし、Windows プラットフォームが Windows Server 2003 の場合は、以下の手順を実行して NOS ダウンロードを有効にできます。

1. エージェント コンピュータ上で、以下のレジストリ キーを 1 に設定する必要があります。

HKLM¥System¥CurrentControlSet¥Services¥smb¥Parameters¥IPv6EnableOutboundGlobal (REG_DWORD)

2. DSM スケーラビリティ サーバライブラリ共有をマウントするすべてのエージェント コンピュータに対して、以下にリストされている 2 つのホットフィックス更新を適用する必要があります。

<http://support.microsoft.com/kb/947369/en-us>

<http://support.microsoft.com/kb/950092/en-us>

3. スケーラビリティ サーバコンピュータのホスト名は、グローバル IPv6 アドレスに解決される必要があります。
4. スケーラビリティ サーバライブラリ共有（スケーラビリティ サーバの comstore に保存されている）は、ホスト名を使用する必要があります（IP アドレスは不可）。IP アドレスが使用されているかどうかを確認するには、以下のコマンドを実行します。

```
ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn exportarchive
ccnfcmda -cmd GetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
```

いずれかのコマンドが IP アドレスを含む値を返す場合は、以下のコマンドを使用して、IP アドレスをホスト名に置き換えます。

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn exportarchive
-v IP_replaced_with_hostname

ccnfcmda -cmd SetParameterValue -ps itrm/usd/shared -pn msiadminpathunc
-v IP_replaced_with_hostname
```

たとえば、msiadminpathunc の GetParameterValue が ¥¥2001:db9:1:2:f045:c89:5c2:bdf5¥SDMSILIB を返した場合は、新しい値は ¥¥foobar.testarea.ca.com¥SDMSILIB になります。

注: ccnfcmda エージェント設定コマンドの詳細については、「<command> /?」と入力してください（コマンドプロンプトで実行）。

実際には、NOS ダウンロード方法が失敗した場合、Software Delivery は、NOS なしダウンロード方法の使用にフォールバックします。ただし、デフォルトポリシーの変更によって、フォールバックが無効になっている場合は、SD ジョブはこれらの条件下で失敗します。

- DTS (Data Transport Service) WorldView 動的コンテナ メンバシップは、IPv4 アドレス範囲のみをサポートします。

- インフラストラクチャ展開および継続ディスカバリでは、IPv4 アドレス範囲のみサポートされます。
- 非管理対象コンピュータを排除するのに使用される 1 つ以上のサブセットをユーザが入力できる非管理対象コンピュータ ウィザードでは、IPv4 サブセットのみがサポートされます。
- CAF サービス ロケータは、ローカル サブセットでのみ機能することができるので、ローカル サブセットのみでマネージャを検出するパッケージに影響を及ぼす可能性があります。（これは、ルータが範囲マルチキャストを許可するかどうかに依存します。）
- DTS PPP プロトコルは、IPv6 をサポートしません。
- Client Automation は、Windows Server 2003 と Windows XP での IPv4 の無効化をサポートしません。これは、これらの Windows プラットフォームでの IPv4 の無効化が一般的にサポートされていないためです。
- Windows Vista および Windows Server 2008 では、Client Automation が 純粋な IPv6 をサポートしています。これらのプラットフォーム上では、以下のコマンドをコマンドプロンプトから実行して IPv4 を削除する必要があります。
`netsh interface ipv4 uninstall`
再起動が必要な場合は、メッセージが表示されます。

IPv6 サポート関連の設定に関する考慮事項

CA Client Automation（Client Automation）における IPv6 サポートとの関連で、以下の設定に関する注意事項および側面に注意する必要があります。

- DSM エクスプローラ内の設定パラメータ（ポリシー エントリ）が IPv6 および IPv4 の接続を制御します。

DNS ルックアップの優先度を定義

DNS クエリを直接実行する場合、つまり、一般的な機能を使用しない場合に、DNS クエリの優先順位を定義します。Windows Vista より前の動作環境では、DNS は IPv4 経由でのみサポートされています。

デフォルト：ipv4,ipv6

名前解決の優先度を定義

名前解決機能の優先順位を定義します。環境によっては、WINS および NETBIOS の名前解決が DNS よりも信頼できる場合があります。そのような場合には、NETBIOS による解決が DNS ルックアップより優先して使用されるように指定できます。

このパラメータが設定されると、「NETBIOS ショートネーム フォールバックの使用」設定パラメータが無視され、名前解決では、DNS およびその他の方法にフォールバックする前に、FQDN をショートネームに省略することで、最初に NETBIOS をクエリします。このポリシーが原因でショートネームのルックアップがすでに実行されている場合は、ショートネームのフォールバックはスキップされます（有効な場合）。このパラメータは、NETBIOS ルックアップをサポートしている Client Automation でのみサポートされています。

注：このパラメータは現在使用されていません。

デフォルト： dns,netbios

解決済みアドレスの優先度を定義

複数の IP アドレスファミリが使用される場合に、IP アドレスファミリ（IPv6 または IPv4）の優先順位を定義します。

アドレスを解決する際には、この集中管理されているパラメータによって、アドレスファミリごとにどの優先順位を提供する必要があるかが指定されます。デフォルトでは、相互運用性を最大限に保つために、IPv6 アドレスの前に IPv4 アドレスが優先されます。

デフォルト： ipv4,ipv6

IPv4 解決を有効化

IPv4 のアドレス解決のサポートを有効にします。このパラメータは、現バージョンのソフトウェアではプレースホルダの機能のみであるため、エンドノードはその設定を無視して、常に IPv4 解決をサポートします。

デフォルト： True

IPv6 解決を有効化

IPv6 のアドレス解決のサポートを有効にし、IPv6 アドレスが返されるようにします。無効 (False) になっている場合、リゾルバによって名前解決の結果から IPv6 アドレスが削除されます。

注: このパラメータは、ミラー IPv4 制御とは対照的に、エンド ノードにより保持されます。

デフォルト : True

名前解決のフォールバックにデータベースを使用

名前がアドレス ロケーション サービス (DNS) または NETBIOS を通じて解決できない場合に、マネージャの MDB データベースまたはサーバのデータベースのいずれかに保存されている IP アドレスにフォールバックするように指定します。

注: デフォルトのフォールバック オプションはたいいてい場合はそのままにしておきますが、CA テクニカル サポート 担当者が求める場合のみ変更する必要があります。

有効な値は以下のとおりです。

1 = すべてのフォールバック モードが有効

2 = サーバ データベース フォールバックの使用

4 = MDB フォールバックの使用

デフォルト : 1

NETBIOS ショートネーム フォールバックの使用

完全修飾名 (FQN) ルックアップが失敗した場合に、NETBIOS のショートネームをフォールバックとして使用するかどうかを示します。

デフォルト : True

注: これらの設定パラメータは、[設定ポリシー] - [デフォルトのコンピュータ ポリシー] - [DSM] - [共通コンポーネント] - [ネットワーク] - [一般] ペインにあります。詳細については、「*DSM* エクスプローラ ヘルプ」の「設定ポリシー」にある一般ポリシー グループ (ネットワーク) のトピックを参照してください。

- IPv4 のみのコンピュータに Client Automation がインストールされており、後ほど IPv6 が有効化された場合は、コンピュータを再起動し、CAF サービスを再度開始させる必要があります。

- ご使用のネットワークで IPv6 のみがサポートされる場合（つまり、IPv4 ルーティングが無効か停止した場合）、または主に IPv6 接続を使用している場合は、「解決済みアドレスの優先度を定義」設定パラメータの値を `ipv6,ipv4` に変更することをお勧めします。この設定は、エンタープライズドメインにある異なるコンピュータ間の通信のパフォーマンスを向上させます。
- リモート MDB を使用するマネージャがあり、そのマネージャとリモート MDB 間に IPv6 ルーティングのみが存在する場合は、「解決済みアドレスの優先度を定義」設定パラメータの値がデフォルトで初期値として `ipv4,ipv6` に設定されるので、初めて DSM エクスプローラを開くのにかなり時間がかかってしまいます。この場合、名前がまず IPv4 アドレスに解決され、データベース接続がタイムアウト後に失敗し、その後、IPv6 アドレスが試行され、それが成功します。設定ポリシーは、DSM エクスプローラが開くまで変更できません。
- ご使用のネットワーク内にかなりの数の Windows 2003 および Windows XP コンピュータが存在する場合は、これらのプラットフォーム上では、DNS メッセージが IPv4 接続経由でのみ送信されるので、「DNS ルックアップの優先度を定義」設定パラメータを `ipv4,ipv6` のままにする必要があります。

DSM コンポーネントをホストしているコンピュータの DNS 名前解決

エンタープライズマネージャ、ドメインマネージャ、スケーラビリティサーバ、エージェントなどの DSM コンポーネントをホストしているすべてのコンピュータは、前方と逆引きの両方の DNS ルックアップをサポートする必要があります。DSM コンポーネント間の通信が正しく機能していることを確認します。

ループバック IP へのホスト名の割り当て

Client Automation では、ホスト名が内部と外部の通信に対して常に解決可能である必要があります。インタラクティブ インストーラには、以前のオプションを設定できる [Assigned hostname to the loopback IP] オプションが含まれています。

自動インストールの場合は、以下のように、`autoinst.xml` のネットワークまたは DNS セクションで `write_hostname` エントリを `True` に設定します。

```
<networking>
  <dns>
    <dhcp_hostname config:type="boolean" >false</dhcp_hostname>
    <dhcp_resolv config:type="boolean" >true</dhcp_resolv>
    <hostname>$HostName$</hostname>
    <write_hostname config:type=boolean>true</write_hostname>
  </dns>
</networking>
```

`autoinst.xml` ファイルは、以下の場所で見つけることができます。

```
DSM_Install_Folder¥server¥SDBS¥var¥managedpc¥images¥IMAGE_NAME¥IMAGE_NAME¥suse
```

FIPS 140-2 のサポート

FIPS（連邦情報処理標準）パブリケーション 140-2（FIPS PUB 140-2）は、暗号のモジュールの認証に使用される米国政府のコンピュータ セキュリティ標準です。この標準は、NIST（国立標準技術研究所）によって発行され、メンテナンスされています。

FIPS 140-2 認証を受けた暗号モジュールを FIPS 認証を受けたモードで使用しているコンピュータ製品は、FIPS によって認証されたセキュリティ機能（AES（Advanced Encryption Standard）、SHA-1（Secure Hash Algorithm）など）、および FIPS 140-2 標準および実装ガイドで明示的に許可された上位プロトコル（TLS v1.0 など）のみを使用できます。

Client Automation の暗号機能は、以下の側面を処理します。

- パスワードのストレージおよび検証
- CA 製品コンポーネント間、および CA 製品とサードパーティ製品間のすべての機密データの通信

FIPS 140-2 は、取り扱い注意ではあるが機密扱いではないデータを保護するセキュリティ システムの中で暗号アルゴリズムを使用するための要件を規定しています。

Client Automation は、FIPS 準拠の暗号技術をサポートしています。Client Automation には、RSA BSafe および Crypto-C ME v2.1 暗号ライブラリが組み込まれています。これらは、FIPS 140-2 の暗号モジュールセキュリティ要件を満たしていることが確認されています。

FIPS 140-2 プラットフォームのサポート

FIPS 140-2 に準拠するには、FIPS 140-2 認定暗号化モジュールを認定されたモードおよび設定で使用する必要があります。認定 RSA 暗号化モジュールは、Client Automation が利用可能なすべてのプラットフォームでは使用できません。認定モジュールが利用可能ではないが、ドメイン ポリシーで FIPS 140-2 のみの暗号化を指定しているプラットフォームの場合、これらのプラットフォーム上の暗号化サポートでは FIPS に承認されたアルゴリズムおよび機能のみを使用します。ただし、それらは承認されていない暗号化モジュール（CA OpenSSL）によって提供されます。

以下のプラットフォームは、FIPS のみのモードで実行中の場合に FIPS 140-2 に準拠します。

- Windows NT x86
- Linux
- Solaris SPARC/32

現在、その他のすべてのプラットフォームは FIPS 140-2 に準拠していません。これらのプラットフォームが FIPS のみのモードで実行するように設定されている場合、FIPS 承認のアルゴリズムおよび機能を使用しますが、認定された暗号化プロバイダは使用しません。

サポートされている FIPS モード

Client Automation は、「FIPS 推奨」および「FIPS のみ」の 2 つのモードの、FIPS に準拠する暗号化をサポートしています。この 2 つのモードは、パスワードのストレージおよび検証、および CA 製品コンポーネント間、および CA 製品とサードパーティ製品間のすべての機密データの通信用に適用できます。

FIPS 推奨モード

Client Automation の前のリリースと後方互換性のあるモードを指します。このモードでは、リリース 12.9 コンポーネントは、他のリリース 12.9 コンポーネントとの通信に FIPS- 準拠の暗号化を使用します。ただし、前のリリースのコンポーネントと通信する場合、それらのコンポーネントは後方互換性を保つために、FIPS に準拠しないセキュリティ機能を使用する場合があります。FIPS 推奨は新規インストールのデフォルトモードである一方で、それはアップグレードに関してサポートされている *唯一* のモードです。

注: 環境内の DSM コンポーネントをすべてアップグレードした後に、FIPS のみモードに切り替えることができます。

FIPS のみモード

暗号化に FIPS 準拠の技術のみを使用しているモードを指します。Client Automation の *新規* インストールには、このオプションを使用します。このモードでは Client Automation の前のリリースとの後方互換性はありません。

注: FIPS のみモードに切り替えた後に、コンポーネントでレガシーな暗号化を使用することはできません。必要ならば、再度 FIPS 推奨モードに切り替えることができます。

フェールオーバー サポートおよびハードウェアの置き換え

CA Client Automation では、クラスタ環境でのフェールオーバーがサポートされており、また、ハードウェア障害またはハードウェア アップグレード時のマネージャハードウェアの置き換えもサポートされています。

詳細については、以下のセクションを参照してください。

- [フェールオーバー サポート](#) (P. 93)
- [マネージャ ハードウェアの置換](#) (P. 96)

フェールオーバー サポート

フェールオーバー サポートは、Windows 動作環境および Microsoft SQL Server データベースでのみ利用可能です。

フェールオーバー サポートにより、Microsoft クラスタを実行している 2 つの異なるコンピュータにマネージャ コンポーネントがインストールされます。システムにはマネージャの機能を実行中にアクティブ ノードである必要があるものもありますが、多くのシステムでは、マネージャ ソフトウェアがインストールされていても起動されていない場合、待機中はパッシブ ノードとなります。

クラスタへのインストール

Client Automation には、システム障害を検出し、システム障害の場合にアクティブなノードからパッシブなノードへ自動的に切り替える機能はありません。

Client Automation は、アクティブ ITCM Manager またはパッシブ ITCM Manager のいずれかの 2 つのモードでインストールできます。「アクティブ」および「パッシブ」という用語は、DSM マネージャがアクティブかパッシブかということを指し、クラスタ ノード（それ自身、アクティブまたはパッシブになり得る）に言及しているわけではありません。

クラスタに Client Automation をインストールする場合、DSM マネージャの 1 つのインスタンスがアクティブ ITCM Manager としてインストールされ、もう一方のインスタンスがパッシブ ITCM Manager としてインストールされます。

アクティブ ITCM Manager のインストール方法

1. クラスタのアクティブ ノードで、通常の方法で Client Automation インストーラを起動し、カスタム インストールを実行します。
2. マネージャ コンポーネントおよびインストールの一部となるその他のコンポーネントを選択します。
3. [マネージャの設定] ダイアログ ボックスで、管理データベース サーバの名前を入力します。
4. [回復] ボタンをクリックする。
5. 表示されるダイアログ ボックスで、[回復サポートの有効化] および [アクティブ] オプションを選択します。
6. クラスタ名および共有ドライブの場所を入力します。

注: DSM ドメイン マネージャとローカル Microsoft SQL Server を Microsoft Cluster 環境にインストールする場合は、Microsoft SQL Server 仮想名を使用して、Client Automation を Microsoft SQL Server Cluster Group にインストールする必要があります。

7. [インストール先の場所の選択] ダイアログ ボックスが表示されるまで、インストールを続行します。このダイアログ ボックスでは、インストール先のフォルダを設定します。

インストール先のフォルダには、コンピュータのローカル ディスク上（共有 クラスタ ディスクではない）の場所を指定してください。

設定データの場所は、クラスタの共有ディスクをポイントしている必要があります。これは、[フェールオーバー] ダイアログ ボックスに入力した情報に基づいて自動で行われます。ただし、[詳細設定] ボタンをクリックしてこれらの場所を確認できます。共有コンポーネントの場所もコンピュータのローカル ディスク上にある必要があります。この場所は、同じ [詳細設定] ボタンを使用して設定されます。

8. [次へ] をクリックし、インストールが開始するまでインストーラのダイアログ ボックスを続行します。

クラスタ コンピュータ上での CCS とマネージャのインストールは、スタンドアロンの非クラスタ コンピュータ上でのインストールとは少し異なります。通常は CCS のインストールはサイレントで行われます。ただし、クラスタ上では、Client Automation によって CCS の対話式インストールが起動されます。

重要: Client Automation によって適切な値が入力されているので、これらのダイアログ ボックスの情報のいずれも変更しないでください。CCS インストールが開始されるまで、続けて [次へ] をクリックします。

パッシブ ITCM Manager のインストール方法

1. クラスタ内の別のコンピュータ（1 つまたは複数）にインストールする前に、クラスタ グループが利用可能であり、共有リソースが動作していることを確認します。または、コンピュータをクラスタ内のアクティブ ノードにします。
2. 通常の方法で Client Automation インストーラを起動し、カスタム インストールを実行します。
3. アクティブ ITCM Manager インストールで選択されたのと同じコンポーネントを選択します。
4. [マネージャの設定] ダイアログ ボックスで、管理データベース サーバの名前を入力します。
5. [回復] ボタンをクリックする。
6. 表示されたダイアログ ボックスで、[リカバリ サポートの有効化] および [パッシブ] オプションを選択します。
7. 次に、インストーラによって DSMRecovery.ini ファイルの場所が要求されます。これは、クラスタの共有ディスク上の Client Automation 設定データ ディレクトリの中にあります。実際の場所は、アクティブ ITCM Manager のインストール時に定義されています。

8. [次へ] をクリックし、インストーラのダイアログ ボックスを続行し、インストールを開始します。

アクティブ ITCM Manager のインストールと同様に、CCS は対話式に実行されます。

重要: 繰り返しになりますが、**Client Automation** によって適切な値が入力されているので、これらのダイアログ ボックスの情報のいずれも変更しないでください。CCS インストールが開始されるまで、続けて [次へ] をクリックします。

インストールが完了すると、クラスタのリソースをクラスタのアクティブ ノードに戻すことができます。

以後、クラスタ内のコンピュータ間でアクティブ クラスタ ノードが切り替わる場合、パッシブ ITCM Manager に通知する必要があります。通知するには、**ActivateManagerNode.bat** ファイルを実行します。このファイルは、DSM マネージャのインストール先の bin ディレクトリにあります。または、クラスタ管理システムを使用する場合は、**ActivateManagerNode.bat** ファイルの内容を実行するようにクラスタ マネージャを設定することもできます。

注:

- クラスタのセットアップの詳細については、<http://ca.com/greenbooks> にある「Client Automation/CA Unicenter Desktop & Server Management」という名前のグリーン ペーパーを参照してください。
- デフォルトでない名前付き SQL インスタンスにインストールする場合は、そのインスタンスの TCP/IP ポート番号がクラスタの全ノードで同じであることを確認してください。同じでないものが 1 つでもある場合は、そのポート番号を修正してください。SQL Server ブラウザが実行されていることも確認してください。
- 現在、ブート サーバはクラスタではサポートされていません。
- Windows 2008（および Windows Vista）では、すべての管理者権限を持つアカウントを使用して **ActivateManagerNode.bat** コマンドファイルを実行する必要があります。管理者ユーザとしてログインしている場合、ユーザはデフォルトで自動的にすべての権限を持っています。ただし、Administrators グループの他のユーザを使用してログインしている場合、このユーザには通常の権限しかなく、このコマンドを正常に実行することができないため、Windows で問題を調整します。この状態を変更するには、**ActivateManagerNode.bat** コマンドファイルを権限を昇格したユーザとして実行する必要があります。たとえば、権限を昇格した状態でコマンドライン ウィンドウを開くには、コマンドプロンプトのアイコンを右クリックし、[管理者として実行] を選択します。このウィンドウからコマンド ファイルを実行できます。

マネージャ ハードウェアの置換

システム エラーの場合や、オリジナル **MDB** および設定をこのまま使用方法でハードウェアをアップグレードする場合、マネージャ システムのハードウェアを置き換えることができます。

元の設定が使用できるので、**MDB** を再インストールしたり、**Software Delivery** ライブラリまたは **Remote Control** のアドレス帳を再設定したりする必要はありません。

マネージャ システムの置き換えが必要な場合に備えて準備するには、インストール ウィザードで設定を実行する必要があります。[マネージャの設定] ダイアログ ボックスで、[リカバリ] ボタンでフェールオーバー ダイアログ ボックスを表示します。フェールオーバー ダイアログ ボックスで、[システムの置換] および [置換の有効化] オプションを選択します。インストール ディレクトリを設定するダイアログ ボックスで、マネージャ データ (**MDB** および設定データ) のディレクトリを、定期的なバックアップが必要なパスに設定します。インストール時、さまざまなダイアログ ボックスからのすべての入力は **DSMRecovery.ini** というファイルに格納され、指定した設定データの保存場所に保存されます。このファイルを使用して、クラッシュの場合にハードウェアを置き換えることが可能です。

ハードウェア置換後にマネージャを再インストールする必要がある場合は、[リカバリ] ダイアログ ボックスを再度実行して [置換の有効化] を選択し、[システムの置換] オプションを選択します。

最初に保存された **DSMRecovery.ini** をインストーラで検索できるように、ダイアログ ボックスの下部に設定データのインストール パスを入力する必要があります。インストーラはすべてのインストール パラメータを読み込み、元のマネージャのインストールと同じ **MDB** やソフトウェア ライブラリなどを使用します。

設定データの相対パスは、アクティブ マネージャの場合と同じである必要があります。

マネージャ システムの置き換えでは、古いマネージャのハードウェアと新しいマネージャのハードウェアで同じシステム名を使用する必要があります。

注: コンピュータ ハードウェア障害の場合、データの一貫性は保証されません。

Client Automation インストール用の CA HIPS の設定

CA Host-based Intrusion Prevention System (CA HIPS) クライアントがインストールされているマシンに Client Automation をインストールする場合、クライアントマシンに Client Automation をインストールするには、まず CA HIPS サーバを設定する必要があります。

Client Automation インストール用に CA HIPS を設定する方法

1. CA HIPS サーバマシン上で、CA HIPS コンソールにログオンします。
2. [ポリシー管理] - [定義] - [アプリケーション リポジトリ] の順にクリックします。
3. グループ リストに **SafeApps** グループが含まれない場合は、**SafeApps** と呼ばれるグループを作成し、以下の手順に従います。
 - a. [ポリシー管理] - [定義] - [共通設定] - [OS システム セキュリティ グローバル] の順にクリックします。
 - b. [ユーザ モードフックをバイパスするためのアプリケーション グループ] ドロップダウン リストから **SafeApps** を選択し、[OK] をクリックします。
 - c. [ポリシー管理] - [定義] - [アプリケーション リポジトリ] の順にクリックします。
4. **SafeApps** グループを選択します。
5. [新規追加] をクリックし、以下の詳細を入力して **setup.exe** を定義します。

フィールド	値
メンバタイプ	アプリケーション
メンバ名	setup.exe
識別基準	FileName
パス	setup.exe
グループ	SafeApps

6. [OK] をクリックします。
7. [新規追加] をクリックし、以下の詳細を入力して **CACMS.MSI** を定義します。

フィールド	値

フィールド	値
メンバタイプ	アプリケーション
メンバ名	CACMS.MSI
識別基準	FileName
パス	CACMS.MSI
グループ	SafeApps

8. [OK] をクリックします。
9. [ポリシー管理] - [展開] の順にクリックします。
10. [配置] をクリックします。
11. バージョン番号を指定し、[OK] をクリックします。
12. ポリシーが CA HIPS クライアント マシン上で有効になるまで待機します。

これで、CA HIPS クライアント マシンが Client Automation インストール用に準備が整いました。

インフラストラクチャ コンポーネントに関する考慮事項

Client Automation の各種コンポーネント間の関係は、以下のとおりです。

- エージェントには、スケーラビリティ サーバとの間に多対 1 の関係があります。各エージェントは唯一のスケーラビリティ サーバにレポートする必要があります。
- スケーラビリティ サーバには、ドメイン マネージャとの間に多対 1 の関係があります。各スケーラビリティ サーバは、唯一のドメイン マネージャにレポートする必要があります。
- ドメイン マネージャには、エンタープライズ マネージャとの間にオプションの多対 1 の関係があります。各ドメインは、唯一のエンタープライズ マネージャにレポートする必要があります。

インフラストラクチャのインストール手順

インフラストラクチャを正常にインストールするには、以下の上位レベルの手順に従います。

- 適切なコンポーネントの配置を決定します。

これには、ネットワーク帯域幅、既存システムの負荷、およびその他の側面などの考慮すべき事項に基づいて、各マシンが果たす役割の決定が含まれます。
- ネットワークの設定が正しいかどうかを確認します。

DNS 設定は、Client Automation 階層の垂直接続（エンタープライズ マネージャとドメイン マネージャ、ドメイン マネージャとスケーラビリティ サーバ、スケーラビリティ サーバとエージェント、ドメイン マネージャとエージェント）間で、「nslookup *IP_address*」を正常に実行できるようになっている必要があります。
- エンタープライズ マネージャおよびドメイン マネージャをインストールします。
- スケーラビリティ サーバをインストールします。
- エージェントをインストールします。
- DSM エクスプローラ管理コンソールをインストールします。

インフラストラクチャのサイジング キー ファクタ

インフラストラクチャのサイジングやシステム パフォーマンスに大きな影響を与えるキー ファクタは数多くあります。

アセット管理タスクにかかる負荷

インフラストラクチャ サイズは、以下の Asset Management のタスクにかかる負荷の影響を受けます。

- 収集されるインベントリ属性の数
- インベントリ収集の間隔

ソフトウェア配布タスクにかかる負荷

インフラストラクチャ サイズは、以下の **Software Delivery** のタスクにかかる負荷の影響を受けます。

- 配信するソフトウェア パッケージのサイズ
- 配信するソフトウェア パッケージの数量
- ネットワーク帯域幅の管理
- ソフトウェア パッケージの配信の間隔（日単位、週単位、月単位など）

Client Automation でのコンピュータの識別

Client Automation は、各管理対象コンピュータに CA Technologies 固有のユニバーサルユニーク識別子 (UUID) を割り当てます。これは、各コンピュータの以下の場所に保存されます。

Windows レジストリ

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\HostUUID

Linux/UNIX

/etc/cadmuuid

CA ITCM アプリケーション フレームワーク (CAF) は、CA Technologies 固有の UUID の場所を定期的に確認します。UUID が検出された場合、CAF はこのアセットがすでにデータベースに登録されているとみなします。UUID が検出されない場合、CAF によって新しい UUID が作成され、このアセットがデータベースに登録されます。

別のコンピュータにインストールする、またはバックアップとして使用するためにインストールをコピーする場合（たとえば、GHOST などのイメージング ツールを使用したハードディスクの物理ダンプ、または VMware などのツールを使用した仮想マシンのイメージファイルなど）、コピーされたインストールには元のコンピュータの CA 固有の UUID が含まれます。コピーされたインストールを元のコンピュータ以外で起動する場合、CA 固有の UUID が 2 つ現れます。

CA 固有の UUID の重複を防ぐために、Client Automation は以下のアクションを実行します。

1. CAF が開始される場合、または「caf register」コマンドが発行される場合、ターゲット コンピュータが元のコンピュータか別のコンピュータかを検証するアルゴリズムが実行されます。
2. ターゲット コンピュータが元のコンピュータの場合、元のコンピュータの CA 固有 UUID が使用されます。元のコンピュータではない場合、新しい CA 固有 UUID が作成されます。

CA 固有 UUID が必要かどうかを検出するために、CA ITCM ではデフォルト アルゴリズム（推奨）またはレガシー アルゴリズムのいずれかを使用できます。アルゴリズムは、ターゲット コンピュータの以下の特性をデータベース内の値と比較して確認します。

仮想マシン

アルゴリズムによって確認される特性は、システム ID（システム BIOS 属性）のみです。

物理コンピュータ

- MAC アドレスの整合性

MAC アドレスの 1 つがターゲットの元の MAC アドレスの 1 つに一致している場合、この条件は満たされたことになります。

- ハードディスク シリアル番号の整合性

ハードディスク シリアル番号の 1 つがターゲットの元のハードディスク シリアル番号の 1 つに一致している場合、この条件は満たされたことになります。

- システム ID の整合性

システム ID がターゲット マシンの元のシステム ID と一致する場合、この条件が満たされたことになります。

上記で説明した特性の値が変更された場合でも、必ずしも CA 固有の UUID を変更する必要はありません。CA 固有の UUID の変更に関する考慮事項は以下になります。

- 特性の元の値がデータベースに存在し、新しい値が元の値とは異なる場合のみ値の変更が発生します。

たとえば、比較に使用する MAC アドレスの古いリストがデータベースに存在しない場合、CA 固有の UUID の変更は開始されません。

- MAC アドレスまたはディスク シリアル番号の新しい値がデータベース内の既存の値と一致する場合のみ変更が発生します。

ホスト UUID のロック

ハードウェアを変更すると、通常はホスト UUID が変更されます。ホスト UUID を変更する必要がない場合、ホスト UUID をロックすることができます。

- Windows 上でホスト UUID をロックするには、レジストリ キー「HKLM¥Software¥ComputerAssociates¥HostUUID」の下に文字列値「LockHostUUID」を作成し、値を「1」に設定する必要があります。
- Linux または UNIX 上でホスト UUID をロックするには、「/etc/calockuuid」という名前のファイルを作成します。

デフォルト アルゴリズム (推奨)

デフォルト アルゴリズムは IDE と SCSI の両方のディスクを検出します (レガシー アルゴリズムは IDE ディスクのみを検出)。また、レガシー アルゴリズムと比較するとホストの変化を正確に特定します。

アルゴリズムでターゲット コンピュータの特性を確認した後、以下のシナリオの場合に CA 固有の UUID が生成されます。

- ハードディスク シリアル番号が変わり、かつ MAC アドレスまたはシステム ID が変わった場合。
- ハードディスク シリアル番号が検出されず、システム ID および MAC アドレスの両方が変わった場合。

注: 仮想マシンでは、システム ID が変わると新しいホスト UUID が生成されます。

レガシー アルゴリズム

Client Automation でコンピュータの識別にレガシー アルゴリズムを使用するには、レガシー アルゴリズムを有効にする必要があります。

重要: アップグレードまたは新規インストールを開始する前に、レガシー アルゴリズムを有効にする必要があります。アップグレードまたはインストール後にレガシー アルゴリズムに変更した場合、レガシー アルゴリズムは不正な CA 固有の UUID を生成します。

レガシー アルゴリズムを有効にするには、Windows、Linux または UNIX 上で以下の方法のいずれかを使用します。

- Windows 上でレガシー アルゴリズムを有効にするには、レジストリ キー「HKLM¥Software¥ComputerAssociates¥HostUUID」の下に文字列値「LegacyHostUUID」を作成し、値を「1」に設定する必要があります。
- Linux または UNIX 上でレガシー アルゴリズムを有効にするには、「/etc/calegacyuuid」という名前のファイルを作成します。

注: CA ITCM エージェントを実行する各コンピュータ上でレガシー アルゴリズムを有効にする必要があります。

物理コンピュータでは、アルゴリズムによって前の部分で説明した 3 つの特性が確認されます。これら 3 つの条件のうち少なくとも 2 つが満たされていない場合、ターゲットシステムは新しいコンピュータとみなされ、新しい CA 固有の UUID が生成されます。

重要: Unicenter® Software Delivery、Unicenter® Asset Management、Unicenter® Remote Control など、CA Technologies のデスクトップ管理ソフトウェアの以前のバージョンによって生成された UUID は、グローバルでは一意でない場合があります。

ドメイン間でのコンピュータのローミング

1 台のコンピュータから、いくつかの異なるドメイン マネージャにレポートを行うことができます。ローミング機能では、コンピュータが同じエンタープライズ マネージャにリンクされたドメイン間を移動する場合、エンタープライズ マネージャ上でエントリが重複するのを回避します。

異なるドメインにレポートするコンピュータでは、新しいドメイン マネージャに移動された情報（配信されたソフトウェア、インベントリ属性など）を保持します。

コンピュータは、ローミングしたドメインから削除されます。デフォルトでは、このタスクは **Software Delivery** 機能によって実行されます（インストールされている場合）。**Software Delivery** 機能がインストールされていないか、ジョブ履歴を保存しないように設定されている場合は、コンピュータの削除は複製ジョブによって実行されます。

例: ローミング コンピュータ

ドメイン マネージャ A および B は両方とも、同じエンタープライズ マネージャにリンクされています。コンピュータ X は、ドメイン マネージャ A に登録され、エンタープライズ マネージャに複製されます。その後、コンピュータ X はドメイン マネージャ B に登録されます。

コンピュータ X がエンタープライズ マネージャに複製される前に、ドメイン マネージャ B は同じ UUID（CA Technologies 固有 UUID または HostUUID）を持つコンピュータがエンタープライズ上にすでに存在するかどうかを確認します。コンピュータ X がドメイン A から検出され、コンピュータ X はドメイン マネージャ A からドメイン マネージャ B にローミングされたことが識別されます。**domain A/computer X** アカウントはドメイン マネージャ B の複製によってエンタープライズ マネージャから削除され、ローミング通知がエンタープライズ マネージャのデータベースに保存されます。**domain B/computer X** アカウントがエンタープライズ マネージャに複製されます。ドメイン マネージャ A は、変更または新しいコンピュータを複製する前に、ローミング通知があるかどうかを確認します。コンピュータ X のローミング通知が検出され、ドメイン マネージャ A から削除されます。（ローミング コンピュータに **Software Delivery** エージェントがインストールされている場合は、すぐには削除されません。）

これにより、コンピュータ X は正常にローミングされ、エンタープライズ マネージャの環境で **domain B/computer X** としてのみ存在します。

ログオフまたは再起動バナーのカスタマイズ

Software Delivery または Remote Control の機能でターゲット コンピュータのログオフまたは再起動が開始されると、CAF (Common Application Framework) にバナービットマップを示すダイアログが表示され、ユーザに現在の状態が通知されます。

サイズが 500x65 ピクセルのビットマップ イメージ ファイル (ファイル拡張子 .bmp) を作成して、独自のビットマップのいずれかをデフォルトのバナー ビットマップと置き換えることができます。このファイルをローカル ディスクまたはネットワーク共有に格納し、Common Components/CAF/General/CAF Dialog: bitmap filename 設定ポリシーをファイルのパス名に設定します。ダイアログ ボックスが表示されると、このファイルが読み込まれ、イメージが表示されます。

カスタム再起動プログラムの使用

CAF (Common Application Framework) では通常、システム再起動のリクエストをオペレーティング システムに転送して実際の再起動を実行します。特別な要件を考慮できるカスタム再起動プログラムを使用できます。

カスタム システム再起動プログラムの使用を有効化および設定する場合、...DSM/common/caf/general configuration policy group に含まれる以下の設定ポリシー設定を利用できます。

CAF: 再起動コマンド

オペレーティング システム API の代わりに使用するカスタム再起動プログラムの名前を指定します。再起動プログラムを指定しない場合は、オペレーティング システム API が使用されます。

CAF ダイアログ ボックス: [有効]ダイアログ ボックス

カウントダウン ダイアログ ボックスを表示するか (値 = True) 、またはカウントダウン ダイアログ ボックスを表示しないですぐに再起動するか (値 = False) を指定します。これは、ダイアログ ボックスからのユーザ操作が可能でないような特別なハードウェアの場合に便利です。

ターミナル サーバ上の再起動とログオフのダイアログ ボックス

再起動の実行中に、何がいつ行われるかを示すダイアログ ボックスが表示されます。このダイアログ ボックスには、プロセスの制御を可能にする以下のようなボタンが表示されています。

今すぐ再起動

指定されたタイムアウトのタイミングを待たずに今すぐ再起動します。

延期

しばらくの間再起動を延期します。その間に作業を完了または保存することができます。

キャンセル

再起動を中止します。

1 人のユーザのみが作業しているコンピュータでは、ほかに影響を受けるユーザがいないのでこれらの操作が可能です。ただし、ターミナル サーバでは、複数のユーザが同時に作業している可能性があるため、これは当てはまりません。その場合、これらのボタンはすべて無効になっています。いずれかの操作を選択すると、ほかのユーザが同意または認識しない状況で彼らに影響を及ぼす可能性があるからです。また、コンピュータはシステム管理者によって「所有」されているとみなされるので、管理者のみが再起動を制御する権限を持ちます。

ただし、ログオフの場合は、そのユーザのみに関係する操作なので、[今すぐログオフ] ボタンが有効になります。[延期] および [キャンセル] ボタンは無効のままです。

Web サービスのドキュメントおよび WSDL ファイルの場所

「Web サービス リファレンス ガイド」は、以下の場所から参照できます。

- 主要な CA Client Automation ドキュメント システム
- 場所は、以下のとおりです (Web サービスがインストールされている場合)。
`http://%machine_name%/UDSM_R11_WebService/help/index.htm` (Windows)
`http://%machine_name%/UDSM_R11_WebService/help` (Linux)

Web サービスがインストールされている場合、WSDL ファイルが以下の場所で見つかります。

- `http://%machine_name%/UDSM_R11_WebService/wsdl`

`%your_install_directory%\CA\DSM\webservices\wsdl`

Linux の場合、WSDL ファイルは以下の場所にあります。

- `%your_install_directory%/CA/DSM/webservices/wsdl`

Web コンソール および Web サービスに関する注意事項

以下は、Web コンソールおよび Web サービスに関連するインストールと統合に関する注意事項です。

Web コンソールで必要なパッケージのインストール

以下の表は、Web コンソールの前提条件であるサード パーティ製のパッケージおよび CA Technologies パッケージをリストしています。

パッケージ	オペレーティング システム	説明/コメント
AMS	Windows および Linux	Asset Maintenance System の CA Technologies コンポーネント AMS は、所有アセットおよびディスカバリされたアセットに関する情報を Web コンソールで表示するのに使用されます。

パッケージ	オペレーティング システム	説明/コメント
AMS	Windows および Linux	Asset Maintenance System の CA Technologies コンポーネント AMS は、所有アセットおよびディスカバリされたアセットに関する情報を Web コンソールで表示するのに使用されます。
Apache Web サーバ	Linux	Web コンソール アプリケーションをホストするコンポーネント。 Apache Web サーバの特定のバージョンを使用する場合は、CA Client Automation のインストールを開始する前に、CA_DSM_USE_APACHE_PROG 変数をバイナリの親ディレクトリではなく完全パスに設定する必要があります。以下に例を示します。 CA_DSM_USE_APACHE_PROG=/apache2.2.8/bin/httpd
Apache Tomcat	Windows および Linux	Web コンソール用のサーブレット コンテナ
ISAPI 用の Apache Tomcat コネクタ	Windows	Internet Information Services (IIS) および Tomcat 間のコネクタ
Apache 用の Apache Tomcat コネクタ (mod_jk)	Linux (32 ビット版、64 ビット版)	Apache Web サーバおよび Tomcat 間のコネクタ
Oracle JDBC ドライバ	Windows および Linux	Oracle データベースへの接続に使用される JDBC ドライバ。
Apache Axis	Windows および Linux	WebService ツールキット
CA CMDB	Windows および Linux	構成管理データベース
CA Service Desk	Windows および Linux	

パッケージ	オペレーティング システム	説明/コメント
AMS	Windows および Linux	Asset Maintenance System の CA Technologies コンポーネント AMS は、所有アセットおよびディスカバリされたアセットに関する情報を Web コンソールで表示するのに使用されます。
Microsoft IIS	Windows	Web コンソール アプリケーションをホストする Microsoft Internet Information Services コンポーネント
Log4j	Windows および Linux	ロギング ツールキット
Microsoft SQL Server JDBC ドライバ	Windows	SQL Server データベースに接続するのに使用される JDBC ドライバ。
Microsoft SQL Server JDBC ドライバ	Linux	SQL Server データベースに接続するのに使用される JDBC ドライバ。
Sun JRE	Windows および Linux	Sun Java Runtime Environment IPv6 を使用する場合、Web コンソールに必要です。

重要: `wacconfig.properties` ファイルに含まれる、データベース ポート番号を含むキー `SQLServer.PortNo` の変更はサポートされなくなりました。後で変更することができないため、インストール中に正しいポート番号を指定する必要があります。

64 ビット版 Linux マシンへの Web 管理コンソール(WAC)または Web サービスのインストール

Client Automation は、Linux マシンの 64 ビット版 Apache Web サーバをサポートしません。Client Automation Web コンソールまたは Client Automation Web サービスを 64 ビット版 Linux マシンにインストールする前に、すべての 64 ビット版 Apache Web サーバをアンインストールしてください。

Web コンソールによる Tomcat ポートの使用

Web コンソールでは、Apache Tomcat Web サーブレット エンジンが使用されます。デフォルトで使用する Tomcat ポート番号は、8090（開始）、8095（シャットダウン）、および 8020（AJP）です。

Tomcat ポート画面の情報は、インストール時に取得されます。インストール時に適切なポート番号を入力する必要があります。

Web コンソールによって使用される Tomcat ポートは、システム インストール パスの `server.xml` ファイルで見つかります。

Windows の場合、`server.xml` ファイルの場所は以下のとおりです。

```
[installpath]\Web Console\conf\server.xml
```

Linux の場合、`server.xml` ファイルの場所は以下のとおりです。

```
[install_path]/webconsole/conf/server.xml
```

Web コンソール用の Tomcat ポート設定

1 つまたはすべてのデフォルトの Tomcat ポートが、コンピュータにすでにインストールされているほかの CA Technologies アプリケーションによって、すでに使用されている場合があります。Web コンソールのインストーラでは、すでに使用中のポートが確認され、自動的に適切な新しいポート番号が割り当てられます。

同じポート番号を重複して使用するアプリケーションが検出されるためには、そのアプリケーションがインストール時に実行中である必要があります。実行中ではなかった場合は、ポート番号の衝突を解決するために、インストール後に手動で作業する必要があります。同じポート番号を使用しようとする別のアプリケーションは、開始できない場合があります。通常、最初のアプリケーションは正常に開始され、後のアプリケーションは開始することができません。

Web コンソールが使用するポート番号を変更するには、以下の手順に従います。

1. Tomcat の Web コンソール インスタンスが実行中の場合は、コマンド コンソールを開き、以下のように入力して停止します。
`caf stop tomcat`
2. テキスト エディタで、`server.xml` ファイルを開きます。
ファイルには、以下のようなエントリが含まれます。

```
<Server port="8095" shutdown="SHUTDOWN" debug="0">  
  
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"  
  port="8090" minProcessors="5" maxProcessors="75"  
  enableLookups="true" redirectPort="8443"  
  acceptCount="100" debug="0" connectionTimeout="20000"  
  useURIVValidationHack="false" disableUploadTimeout="true" />
```
3. `port="nnnn"` の割り当て（上の例にはこのうち 2 つがあります）のポート番号 `nnnn` を空きポートに変更します。
4. ファイルを保存し、テキスト エディタを終了します。
5. コマンド コンソールを開き、以下のように入力して Tomcat の Web コンソール インスタンスを開始します。
`caf start tomcat`

ほかのアプリケーションで使用中のポート番号が不確かな場合、すべてのポート番号を 1 ずつ大きくしてください。次に、アプリケーションを開始し、まだ問題が発生する場合は、上記の処理を繰り返します。

スタンドアロン Web コンソールの展開

DSM マネージャ コンピュータ上または別のコンピュータ上に Web コンソールを展開できます。最適なパフォーマンスを実現するために、スタンドアロン Web コンソールをホストするコンピュータおよび MDB とドメイン マネージャをホストするコンピュータを同じサブネット（地理的に同じ場所）に配置することをお勧めします。

Web コンソール: CMDB ビューア

設定管理データベース (CMDB) ビューア (Visualizer) は、Web ベースのユーザ インターフェイスであり、CMDB データベース内のさまざまな設定項目間の関係を表示します。2つの前提条件として、CMDB がドメイン マネージャと同じ MDB にインストールされる必要があり、Service Desk 統合の設定ポリシーが WAC がインストールされているコンピュータに適用される必要があります。

CMDB ビューアは、以下のホームページのクイック起動セクションから起動できます。

`computer/Homepage/Quick Launch/External Applications/CMDB Visualizer`

CMDB ビューアは別個にインストールし、Client Automation インストールの一部に含まれていないようにする必要があります。

内部の依存関係

一部の DSM コンポーネントには、ほかの DSM コンポーネントとの内部の依存関係があります。インストール時に、選択したコンポーネントの内部の依存関係が確認されます。選択したコンポーネントがほかの DSM コンポーネントに依存している場合、これらのコンポーネントも自動的にインストールされます。

たとえば、Software Delivery (SD) 機能の関連では、スケーラビリティ サーバの機能は同一システム上に SD エージェントを必要とします。このため、エージェントのインストールが選択されていない場合でも、スケーラビリティ サーバのインストールが選択されている場合は、SD エージェントは自動的にインストールされます。

以下は、DSM コンポーネントが追加で自動インストールされる依存関係を示しています。

マネージャ :

コンポーネント	以下が必要となります。
マネージャ (SD)	同一システム上のすべての DTS コンポーネント (マネージャおよびエージェント) ドメイン マネージャの場合は、スケーラビリティ サーバ。
マネージャ (エンタープライズまたはドメイン)	Asset Management マネージャ プラグイン。 エンジン
エンタープライズ マネージャ	DTS エージェント
Web コンソール	Web サービス

サーバ :

コンポーネント	以下が必要となります。
スケーラビリティ サーバ (SD)	同一システム上の SD エージェント DTS エージェント

エージェント :

コンポーネント	以下が必要となります。
カタログ (SD)	同一システム上の SD エージェント

Windows でのその他の製品との依存関係

一部の MSI インストールパッケージには、ほかのサードパーティ製品との依存関係があります。Client Automation インストーラによって自動的にインストールされる製品もありますが、お客様側で発注およびインストールする必要のある製品もあります。

Client Automation インストール パッケージ	サードパーティの前提条件	インストール イメージの一部かどうか	マスタ セットアップ インストール? (*)
エクスプローラ - レポート プラグイン	DB クライアント	いいえ	いいえ
マネージャ - すべてのプラグイン	MDB の場合 - DB クライアント またはローカル DB サーバ	いいえ	いいえ
マネージャ - Asset Management プラグイン	SUN Microsystems J2SE JRE (Java ランタイム環境)	はい	はい - JRE はマネージャ インストールの一部であり、カスタム インストール時に自動的に、または、MSI コマンドラインを使用してマネージャをインストールすると、インストールされます。
Web サービス	Microsoft Internet Information Server (IIS) 7.0 注: IIS 7.0 のデフォルトのインストールでは、Web コンソールで必要なコンポーネントがインストールされないため、Web コンソールをインストールする前に、ISAPI 拡張およびフィルタをインストールします。	いいえ	いいえ

Client Automation インストール パッケージ	サード パーティの前提条件	インストール イメージの一部かどうか	マスタ セットアップ インストール? (*)
Web コンソール	Apache Jakarta Tomcat 5.5.12	はい	はい - Tomcat はマネージャ インストールの一部であり、カスタムインストール時に自動的に、または、MSI コマンドラインを使用してマネージャをインストールすると、インストールされます。
	Oracle J2SE JRE 1.7.0_17 (Java Runtime Environment)	はい	はい - JRE はマネージャ インストールの一部であり、カスタムインストール時に自動的に、または、MSI コマンドラインを使用してマネージャをインストールすると、インストールされます。
	AMS 1.6.2	はい	カスタム インストール時にのみ [はい]

(*) 自動インストールに「はい」と指定されたパッケージの一部は、インタラクティブ インストール ウィザード使用時のみインストールされます。MSI パッケージを直接呼び出してインストールすることはできません。これは、Client Automation インストーラに提供されているパッケージに使用するテクノロジーおよびフォーマットに依存する動作です。

このため、Software Delivery 機能または展開ウィザードを使用してマネージャ コンポーネントを別のシステムに配信する場合は、コンポーネントパッケージをインストールする前に、まず前提条件を手動でインストールする必要があります。

Windows に前提条件を手動でインストールする方法

インストールパッケージの実行に当たっては、事前にインストールしておかなければならないものがありますが、そのインストールの参考となるコマンドの例と手順を、以下にいくつか示します。

■ CA Asset Maintenance Sytem（AMS）のインストール

```
WindowsProductFiles_x86¥AMS¥setupwin32console.exe -P
installLocation="c:¥Program Files¥CA¥DSM¥Web Console¥webapps¥AMS" -V
SERVERNAME="manager_system_name" -V WEBPORT="Tomcat_startup_port" -V
DASSERVERNAME="mdb_servername" -V INGRESLISTENER="db_instance_name" -silent
```

■ MSAARDK のインストール

```
WindowsProductFiles_x86¥MSAARDK¥MSAARDK.exe /R:N
```

コマンドラインまたはバッチ処理からインストールする必要がある場合は、以下の方法をお勧めします。インストールが必要なものは何か、また実行すべきコマンドラインは何かといったような事項を明確にする最も良い方法は、マネージャ機能の特定の組み合わせに合ったテンプレートをインストールすることです。インストーラは、%temp% ディレクトリに複数のログ ファイルを作成します。コマンドを検出するには、DSMSetup.log を開き、Launch ciCCSSetup を検索します。これにより、異なるコンポーネントをインストールするために実行されたコマンドのセクションへ移動します。

ここで、さらに「Launch」を検索することもできます。そうすれば、以下のものをインストールする msexec コマンドのシーケンスを表示できます。

- AMS
- エージェント
- スケーラビリティ サーバ
- DSM エクスプローラ
- マネージャ
- この後に同様の記述が続きます。

各コマンドラインにはコマンドの呼び出し時に使用するプロパティが表示され、自動化スクリプトにコピーされます。すべての関連するパラメータは、「[インストール ツール](#) (P. 193)」の msexec で説明されています。

マネージャのインストールの場合は、最初のパッケージに MDB をインストールおよび設定し、その後、それ以外のものをインストールする必要があります。

Linux および UNIX でのその他の製品との依存関係

Linux および UNIX バージョンの CA Client Automation では、Java Runtime Environment などのサードパーティ製のコンポーネントは PIF または RPM パッケージとして DVD イメージに組み込まれ、必要に応じて DSM パッケージのインストール時にインストールされます。通常は、単独で手動でインストールする必要はありません。

ただし、一部の Linux バージョンでは、DSM コンポーネントをインストールする前に、互換性のあるランタイム ライブラリをインストールする必要があります。詳細については、「Linux の 互換性ライブラリ」を参照してください。

Linux でシステムトレイが機能するようにするには、GIMP Toolkit GTK+ 1.2（厳密にこのバージョン）をインストールする必要があります。GTK は、CA Client Automation には同梱されていません。必要なバージョンを www.gtk.org からダウンロードしてください。

パッケージの選択の包括的な制御は、応答ファイルの設定をインストール コマンドのコマンドライン オプション /R と組み合わせて使用した Linux および UNIX のインストール時に使用可能です。使用可能なオプションの詳細は、[「Linux および UNIX でコマンドラインを使用した Client Automation のインストール \(P. 216\)」](#)で説明されています。

Linux での Apache の再起動

Apache を再起動する必要がある場合、Linux GUI では、CA Client Automation が要求する環境が選択されないためこの GUI を使用して Apache を再起動しないでください。その代わりに、たとえば、シェルに移動して、そこから以下のコマンドを使用して Apache を起動します。

```
dsm_restart_apache [-f]
```

-f オプションを指定すると、Apache を起動します（現在実行中でない場合）。

-f オプションを指定していない場合で、Apache が実行中でない場合、Apache は起動されません。Apache がすでに実行中の場合は、Apache が再起動されます。

第 3 章: Client Automation のインストール

次の章では、**Client Automation** のインストールの一般的な手順と要件について説明します。章の始めにあるいくつかのセクションには、**DSM** コンポーネントのインストールに関する具体的な注意事項と情報が記載されています。これらのセクションを省略して、インストーラの概要とインストール処理の説明を読んでもかまいません。その後、対話式インストールおよびコマンドラインを使用したインストールについての説明が続きます。

このセクションには、以下のトピックが含まれています。

[インストール処理の概要](#) (P. 120)

[インストーラの概要](#) (P. 121)

[前提条件および制限事項](#) (P. 122)

[インストール方法](#) (P. 122)

[インストールに関する注意事項](#) (P. 123)

[FIPS に関連するインストールの考慮事項](#) (P. 124)

[インストール中の FIPS モードの選択](#) (P. 125)

[自動マイグレーションのインストール](#) (P. 126)

[多言語インストール](#) (P. 131)

[エージェント言語パッケージの作成およびインストールについて](#) (P. 132)

[必要なハードウェア設定](#) (P. 133)

[管理データベース \(MDB\)](#) (P. 134)

[Client Automation インストールに関する特記事項](#) (P. 159)

[Windows への管理者によるインストール](#) (P. 178)

[Windows でのインストールディレクトリ](#) (P. 178)

[Linux および UNIX でのインストールディレクトリ](#) (P. 179)

[Alert Collector のインストール](#) (P. 181)

[コンピュータ名、ユーザ名、およびディレクトリ名の制限事項](#) (P. 182)

[インストール ウィザードを使用したインタラクティブインストール](#) (P. 184)

[コマンドラインを使用した Client Automation のインストール \(Windows\)](#) (P. 190)

[Linux または UNIX でコマンドラインを使用した Client Automation のインストール](#) (P. 216)

[インストール ログ ファイル](#) (P. 232)

[インストールされている DSM コンポーネントに関するバージョン情報](#) (P. 234)

インストール処理の概要

インストール処理は、主に以下の 3 つのステップで構成されます。

1. 準備フェーズ
2. インタビュー フェーズ
3. 実行フェーズ

準備フェーズでは、この章の最初のセクションで説明したように、製品オプションを調査し、インストールに必要なすべての情報を収集します。前提条件のソフトウェアが存在していることを確認して、欠落しているソフトウェアがある場合はインストールし、インストールメディアに付属しているその他の製品機能のインストールを選択して開始する必要があります。

インタビュー フェーズでは、インストール ウィザードの手順に従うか、応答ファイルを準備して、手順 1 で収集した情報を入力します。たとえば、インストールの言語およびインストールする製品、インストール タイプ（簡易インストールまたはカスタム インストール）、およびインストールしたコンポーネントを稼働させるための関連する構成設定を指定します。

最後に、手順 2 で入力した情報を使用して、インストールの指示を実行します。

インストール ウィザードを使用すると、インタラクティブに製品コンポーネントをインストールおよび削除することができます。また、コマンドライン インターフェイスを使用して、インストールと設定に関する数多くのパラメータおよびプロパティを指定することもできます。

インストーラの概要

Client Automation インストーラには、基本的な製品の機能をインストールし、必要に応じてさらに **CA Technologies** 製品をプラグインとしてインストールするインストールルーチンが用意されています。

簡易インストール オプションとカスタム インストール オプションが使用できます。簡易インストールでは、いくつかの管理機能をすばやく利用可能にできるのに対し、カスタム インストール オプションでは、より柔軟性および細分性の高い機能選択オプションを使用することができます。

購入した製品機能を選択し、簡易インストールまたはカスタム インストールのいずれかを実行することができます。ライセンスを購入していないユーザは、製品機能を選択するオプションを選択することができますが、この場合は 30 日間の試用期間になります。

Client Automation マスタ インストーラ カスタム インストールを使用して、リモートおよびローカル コンピュータに **MDB** および **DSM** マネージャの両方をインストールできます。このインストーラは **Microsoft** の **SQL Server** および **Oracle MDB** の両方に対して適用可能です。

インストールを実行する場合、インストーラはターゲット コンピュータに最新の **MDB** がインストールされているかどうかを確認します。**MDB** がインストール済みの場合、インストーラは **DSM** マネージャのインストールを続行します。**MDB** がインストールされていない場合、インストーラはまず **MDB** をインストールしてから、**DSM** マネージャのインストールを続行します。また、**DSM** マネージャのより新しいバージョンにアップグレードする場合にも、**MDB** インストールを確認するプロセスが行われます。

また、マスタ インストーラを使用して、**Microsoft SQL Server** および **Oracle** の両方にスタンドアロン **MDB** をインストールできます。ローカルおよびリモート コンピュータのどちらにもインストール可能です。ただし、今までどおり、まず **MDB** をインストールしてから、**DSM** マネージャをインストールすることにより、インストールの既存のプロセスに従うことができます。

注: **CCS** と **DSM** マネージャをリモート **MDB** にインストールする場合は、リモート コンピュータに **MDB** と **CCS** があらかじめインストールされている必要があります。**DSM** マネージャのアンインストールでは、リモート コンピュータから **CCS** を手動でアンインストールする必要があります。

前提条件および制限事項

Client Automation リリース 12.9 をインストールする際には、以下の前提条件および制限事項に注意してください。

- データベース プロバイダとして、Microsoft SQL Server または Oracle を使用する必要があります。
- Oracle の場合は、マネージャをインストールするときに、インストーラのインタビューで「sys」パスワードの入力が要求されます。SQL Server の場合は、[DB 管理者] および [DB 管理者パスワード] フィールドが非表示になっており、インストーラは信頼できる SQL Server 接続を使用して MDB をインストールし、DSM マネージャをセットアップします。

インストール方法

インストールする製品機能を選択した後、インストール方法を選択し、プロンプトに従って製品の配信と設定を開始することができます。

以下のインストール方法を使用できます。

簡易インストール

スケーラビリティ サーバ、エージェント、DSM エクスプローラを含むスタンドアロンのドメイン マネージャを Windows にインストールします。

簡易エージェント インストール

エンド システムの管理に必要なすべての機能をインストールします。このエンドシステムを管理するドメイン マネージャまたはスケーラビリティ サーバが、すでにネットワークにインストールしてあることが理想的です。

カスタム インストール

個々の製品コンポーネントを選択または選択解除したり、インストール設定を変更できます。MDB は、ローカルおよびリモート コンピュータの SQL Server および Oracle の両方に対してインストールできます。インストーラが、ターゲット コンピュータ（ローカルまたはリモート）上で ITCM の現在のバージョンに互換性のある MDB を識別すると、MDB のインストールはスキップされ、ITCM のインストールが進められます。

インストールに関する注意事項

Oracle 11g 上に MDB をインストールする場合は、以下の考慮事項が適用されます。

- 少なくとも、Oracle 11g クライアントをインストールする必要があります。
- DSM マネージャを Oracle MDB と共にインストールしているときに CCS コンポーネントのインストールを選択する場合は、C: ドライブが存在する必要がある、さらに CCS コンポーネントのデフォルトのインストールパスを変更しないままにする必要があります。
- Client Automation は、DSM マネージャから Oracle データベースへの接続として EZCONNECT メソッドのみをサポートします。EZCONNECT 接続メソッドの設定の詳細については、Oracle のマニュアルを参照してください。
- DSM マネージャは Oracle 11g 32 ビット Client を必要とするため、DSM マネージャを Oracle 11g 64 ビット Server または Client と同じコンピュータにインストールすることはできません。Oracle 11g 64 ビット Server に MDB がインストールされている場合、このサーバは DSM マネージャからのリモートである必要があります。
- DSM マネージャと MDB の間では、IPv4 と IPv6 の両方がサポートされています。
- System Global Area (SGA) と Program Global Area (PGA) の両方に、少なくとも 2 GB を推奨します。
- インストールログは、mdb-schema-setup.log という名前で一時ディレクトリ内に存在します。
- 再インストールまたはアップグレード中に、sys、mdbadmin、および ca_itrm の正しいパスワードを入力します。
- MDB PIF パッケージは、Windows および Linux/Solaris 上の応答ファイルからの自動インストールをサポートします。
- 基礎となるデータベースが Oracle である場合は、データソースに接続するために mdbadmin 認証情報を指定します。また、抽出を実行する前に mdbadmin に AIADMIN ロールを追加します。

関連項目：

[インストールの前提条件](#) (P. 126)

インストールに関するその他の考慮事項

Windows ターミナル サービスがアプリケーション サーバ モードに設定されている場合は、以下の設定が必要です。

- リモート アクセスからインストールを実行する場合は、**CONSOLE** モードを使用します。

例：

```
mstsc /v:HostName /console
```

- インストールの前に、ターミナル サーバの **USER** 設定を **INSTALL** に変更します。

例：

```
change user /install
```

- 以下のコマンドを実行して、ユーザ設定を確認します。

```
change user /query
```

注: Windows ターミナル サーバの **CHANGE USER** ユーティリティの詳細については、support.microsoft.com/kb/186504 を参照してください。

関連項目：

[インストールの前提条件](#) (P. 126)

FIPS に関連するインストールの考慮事項

Client Automation を **FIPS** モードのいずれかでインストールする場合、インストールに関する以下の考慮事項があります。

- コンピュータ上の **DSM** コンポーネントはすべて同じ **FIPS** モードを使用します。たとえば、すでにリリース **12.9 Software Delivery** エージェントがあるコンピュータにアセット管理エージェントをインストールする場合、前者は後者と同じ **FIPS** モードで作動します。
- エンジン、**Web** サービス、**Web** コンソール、レポートなど、マネージャ コンポーネントはすべて、マネージャが使用するのと同じ **FIPS** モードを使用する必要があります。
- クラスタ化された展開については、最初のノードに対してのみ **FIPS** モードを選択できます。他のノードはすべて最初のノードと同じモードで動作します。

インストール中の FIPS モードの選択

FIPS モードを選択できるのは、インストーラを使用して対話形式で、またはコマンドライン、`msiexec`、またはインフラストラクチャ展開（`DMDeploy`）を使用してサイレントモードで **Client Automation** をインストールする場合です。デフォルトのモードは「FIPS- 推奨」です。

注: **Client Automation** インストールをアップグレード、変更、または修復する場合は、FIPS モードを指定できません。インストールの後に **DSM** コンポーネントの FIPS モードを変更する場合は、必要なモードに切り替えます。特定の FIPS モードへの切り替えの詳細については、「セキュリティ機能」のセクションを参照してください。

このセクションは、さまざまなインストール方法およびオプションを使用する際に、FIPS モードを変更する方法について説明します。

対話型インストール

Client Automation インストーラには、製品のインストールする時に、**[FIPS 推奨]** セクションで FIPS モードを選択するオプションがあります。チェックボックスを選択して、インストールするコンポーネントの FIPS のみモードを有効にします。インストールの変更または修復の場合、インストーラにこのオプションはありません。

注: FIPS モードを選択できるのは、カスタムインストール時のみです。簡易インストールでは、常に「FIPS 推奨」モードで **Client Automation** がインストールされます。スタンドアロンの **Remote Control** エージェントのインストールでは、カスタムおよび簡易の両方のインストール時に、FIPS モードを指定できます。

コマンドライン、`msiexec`、または `DMDeploy` を使用したインストール

コマンドライン、`msiexec` または `DMDeploy` を使用して、サイレントインストールを実行する際に、FIPS モードの設定で以下のパラメータを指定できます。

Windows の場合

```
FIPS_MODE=1 // (FIPS 推奨)
FIPS_MODE=2 // (FIPS のみ)
```

Linux または UNIX :

```
/RITCM_FIPS_MODE=1 // (FIPS 推奨)
/RITCM_FIPS_MODE =2 // (FIPS のみ)
```

Software Delivery を使用したインストール

Software Delivery を使用して DSM コンポーネントをインストールまたはアップグレードする場合、FIPS モードを指定することはできません。FIPS モードは以下の要因に基づいて決定されます。

- ターゲットにすでに DSM コンポーネントがインストールされている場合、Software Delivery によるそれ以降のインストールでは既存のコンポーネントと同じ FIPS モードを使用します。それ以外の場合、FIPS モードは「FIPS 推奨」に設定されます。
- Client Automation インストールを変更または修正する場合は、FIPS モードを指定できません。

すべての場合、マネージャは FIPS モードを設定する設定ポリシーを適用して、FIPS モードを無効化できます。

自動マイグレーションのインストール

インストールの前提条件

インストールを開始する前に、社内で以下のインストール済み製品が使用可能であることを確認します。

- CA IT PAM バージョン 03.0.00 および Service Pack 03.0.01 または CA Process Automation 03.1.00 および Service Pack 03.1.01 または CA Process Automation 4.1 SP1

注: 必要に応じて、ID およびアクセス管理のために CA EEM をインストールできます。Windows 64 ビット環境に CA EEM をインストールする場合は、インストールの前に *EEM_Install_64.pdf* の指示に従います。

- Oracle MDB および CA IT PAM バージョン 03.0.00 を使用している場合は、CA IT PAM のインストールに CA IT PAM パッチ、ITPAM_3.0_11182010_OracleJar_HF_19813962 をインストールする必要があります。

重要: パッチを適用する前に、CA IT PAM Orchestrator サービスを停止してください。

インストールに関する注意事項

自動マイグレーションには、以下の考慮事項が適用されます。

- 自動マイグレーションは **DSM** ドメイン マネージャをサポートしているため、**DSM** エンタープライズ マネージャには適用できません。
- 自動マイグレーションは、**Web** コンソールにリンクされたデフォルトのドメイン マネージャにのみ適用されます。**Web** コンソールが複数のドメイン マネージャにリンクされている場合、自動マイグレーション機能は、デフォルトのドメイン マネージャに接続されている場合にのみ使用できます。
- 自動マイグレーションは、ドメイン マネージャあたり **1** つの **Web** コンソール インスタンスにのみインストールできます。複数の **Web** コンソール インスタンスに同じデフォルトのマネージャが割り当てられている場合は、自動マイグレーションをいずれかの **Web** コンソール コンピュータにのみインストールする必要があります。
- 自動マイグレーションは、**Windows** オペレーティング環境でのみサポートされています。
- 自動マイグレーションを変更またはアンインストールするときに、**WAC** マネージャがリモート コンピュータにインストールされている場合は、**CAF** が有効になっていることを確認します。

自動マイグレーションの設定

自動マイグレーションを使用する前に、以下のタスクを完了します。

1. **Client Automation** での **CA IT PAM** ユーザ アカウントの設定
2. **Web** コンソールおよび自動化 **Web** サービス用に **SSL** を有効化
3. (オプション) 自動化サービス設定ファイルの変更

Client Automation での CA IT PAM ユーザ アカウントの設定

自動マイグレーションは、CA IT PAM を使用して OS マイグレーション ワークフローを自動化します。CA IT PAM を有効にして Client Automation と対話するには、DSM ドメインマネージャで CA IT PAM ユーザ アカウントを設定してください。

注: 設定対象の CA IT PAM ユーザは、CA IT PAM での実行権限を持つ必要があります。

Client Automation の CA IT PAM ユーザ アカウントの設定方法

1. ドメインマネージャ コンピュータで、CA IT PAM ユーザのローカル WINNT ユーザ アカウントを作成します。CA IT PAM ユーザの LDAP ユーザ クレデンシャルを使用する場合は、この手順をスキップできます。

重要: 自動マイグレーションは、Sun ONE Directory Server をサポートしていません。LDAP として Sun ONE Directory Server を使用している場合は、CA IT PAM ユーザの WINNT ユーザ アカウントを使用してください。

2. CA IT PAM ユーザ アカウントを Client Automation セキュリティ プロファイルに追加し、以下のセキュリティ オブジェクト クラスに対するフル コントロールを許可します。
 - ソフトウェア ジョブ
 - コンピュータ
 - ソフトウェア ジョブ コンテナ
 - OS インストール イメージ
 - プロシージャ
 - アセット グループ
 - 共通クエリ
 - マネージャ
 - データベース クレデンシャル
 - ソフトウェア ベースのポリシー
 - ソフトウェア グループ
 - ソフトウェア パッケージ

CA IT PAM 管理者には、Client Automation にアクセスして必要な機能を実行する権限が与えられています。マイグレーション ジョブの作成時に、このユーザのクレデンシャルを指定します。

DMM 共有アクセスの設定

DMM ネットワーク共有を Windows Server 2008 以降で実行する場合、リストアフェーズ中に、DMM の適用プロシージャの実行が、いずれかのターゲットマシンのランタイムエラーで失敗する場合があります。

以下のいずれかの手順に従います。

- Windows Server 2003 SP2 で実行される DMM ネットワーク共有を使用します。
- SMB 2.0 を以下のように無効化し、Windows Server 2008 SP2 または Windows Server 2008 R2 で実行される DMM ネットワーク共有を使用します。
 1. regedit を開きます。
 2. HKLM、System、CurrentControlSet、Services、LanmanServer、Parameters に移動します。
 3. smb2 という名前の DWORD キーを追加し、値を 0 に設定します。
 4. サーバを再起動します。

Web コンソールおよび自動化 Web サービス用に SSL を有効化

Web コンソールおよび自動化 Web サービス用に SSL (Secure Socket Layer) を有効にすると、安全なチャネルを介して通信できるようになります。

以下の手順に従います。

1. Web コンソール ヘルプの「Web コンソールおよび Web サービス用に SSL を有効化」のトピックの指示に従います。
2. DSM Web コンソール ヘルプ内の「Web コンソールおよび Web サービス用に SSL を有効化」のトピックで指定されたパラメータに加えて、WACConfig.properties ファイル内の以下のパラメータ値を変更します。

WIN7SERVICE_URL:

自動化 Web サービスの URL を定義します。URL を変更し、http ではなく https で開始されるようにします。たとえば、
`https://testmachine.test.com/axis/services/automationService` のようにします。

ITCMEPR

Client Automation WebService URL を定義します。URL を変更し、http ではなく https で開始されるようにします。たとえば、
`https://testmachine.test.com/UDSM_R11_WebService/mod_gsoap.dll` のようにします。

3. 「Web コンソールおよび Web サービス用に SSL を有効化」のトピックの残りの手順を完了します。

(オプション) 自動化サービス設定ファイルの変更

自動化サービス設定ファイルには、自動マイグレーションがさまざまなタスクに使用する設定パラメータが含まれています。ほとんどの場合、デフォルト設定では、最適化されたパフォーマンスで自動マイグレーションが動作します。ただし、サーバが処理できる負荷など、環境に応じて特定の設定を変更し、ジョブのパフォーマンスを向上できます。

自動化サービス設定ファイルを変更する方法

1. `C:\Program Files\CA\DSM\Automation Service\bin` フォルダまたは `%autohome%\bin` フォルダを開きます。
2. テキストエディタで、`automation.config` ファイルを編集します。
3. 必要なパラメータの値を変更します。各パラメータの詳細については、「自動化サービス設定ファイル」を参照してください。

注: `automation.config` ファイル内の整数値には、スペースを含めることができません。また、整数値をスペースで囲むことができません。`automation.config` ファイルで整数値を指定する場合は、値内および値の周囲にスペースがないことを確認します。整数値内にスペースが含まれると、自動化サービスが誤動作する場合があります。

4. 以下のコマンドを使用して、ファイルを保存し、Tomcat を再起動します。

```
caf stop tomcat  
caf start tomcat
```

設定ファイルへの変更が有効になります。

多言語インストール

Client Automation インストールを開始すると、インストール時に使用する言語を選択するよう求めるダイアログ ボックスが表示されます。ご使用のローカル環境でいずれかのサポート言語が使用されている場合、この言語がデフォルト言語として事前に選択されます。別の言語を選択すると、インストーラはその言語で実行されます。

CA Client Automation の多言語インストールをサポートするために、インストールメディア (DVD) には、元の英語版以外に、他言語版の製品が含まれています。

インストーラの実行用に選択した言語は、製品が実行される言語である必要はありません。インストール中に、製品が実行される言語、および **Software Delivery** とインフラストラクチャ展開のソフトウェア ライブラリで製品用に使用できる言語を選択するように求められます。

Client Automation のインストールで選択した言語に関係なく、**CA Common Services (CCS)** は常に英語で表示されることに注意してください。

自動インストール中に言語が指定されなかった場合、システムのデフォルトのロケールが使用されます (そのような言語パッケージが利用可能な場合)。システムのデフォルト ロケールがサポートされていないロケールの場合は、インストーラが自動的に英語 (米国) を選択します。

重要: ローカライズされたホスト名、つまり米国英語以外 (非 **ENU**) の言語ロケールによるホスト名をサポートするには、基礎となるドメイン ネーム システム (**DNS**) インフラストラクチャが、**DNS** 内で **UTF-8** 文字エンコードをサポートしている必要があります。

関連項目:

[インストール後の製品言語の変更 \(P. 235\)](#)

エージェント言語パッケージの作成およびインストールについて

CA Client Automation は、基本ハードウェア インベントリ (BHI) エージェント、Asset Management (AM) エージェント、Remote Control (RC) エージェント、および Software Delivery (SD) エージェント用に、言語非依存の基本パッケージを提供します。言語非依存の基本パッケージには、英語 (ENU) 言語パッケージがあらかじめ含まれているので、別個の英語 (ENU) 言語パッケージはありません。

管理者は、**dsmPush** スクリプトを使用して、どのエージェントとどの言語を組み合わせるかを指定することで、独自のエージェント パッケージのセットを作成できます。これは、マネージャ コンピュータ上で、ディスク ドライブに DVD を挿入した状態で実行する必要があります。

dsmPush スクリプトは、エージェント ロール用の言語非依存の基本パッケージと目的の言語パッケージとを含むインストール可能なユニットを構築します。コマンドラインで指定すると、**dsmPush** はこれらのインストール可能なユニットを **Software Delivery** ライブラリまたはインフラストラクチャ展開のライブラリにインポートします。**dsmPush** を「-single」パラメータと使用することで、管理者は単一パッケージのみをライブラリにインポートするように強制することができます。

言語パッケージは、基本パッケージと同時に、または後続の別の手順でインストールすることができます。言語パッケージのインストールは、完全に自動で実行されます。

dsmPush スクリプトを使用して、言語パッケージを **Software Delivery** およびインフラストラクチャ展開に登録することをお勧めします。

注: **dsmPush** ツールの詳細については、「CLI リファレンス ガイド」を参照してください。

エージェントインストールでは、パッケージはインフラストラクチャ展開ライブラリにはインポートされず、エージェントおよび言語パッケージ (ENU インストールではない場合) がインストールされるだけです。ただし、すでにインストール済みの多言語エージェント パッケージがある場合、インストーラは言語パッケージをインストールせずに多言語エージェントをアップグレードします。

対話式インストールでは、異なる言語パッケージを選択してインストールし、その言語パッケージで製品を運用することができます。さらに、これらの言語パッケージは、**Software Delivery** とインフラストラクチャ展開のソフトウェア ライブラリにインポートされます。

エージェント インストールの特別なシナリオ

以下のリストでは、エージェントのインストールまたはアップグレードの特別なシナリオに関する関連情報が提供されます。

■ 複合パッケージ上のエージェント プロシージャ

dsmPush スクリプトを使用して、1 つ以上のエージェント基本パッケージや言語パッケージから構成される複合パッケージを作成する場合、ソフトウェアパッケージライブラリに含まれる複合パッケージが利用できるプロシージャ（DSM エクスプローラの [ドメイン] - [ソフトウェア] - [ソフトウェアパッケージライブラリ] - [ソフトウェア パッケージ] - [パッケージ] - [プロシージャ] に表示される）は、Linux 用のインストール、および Windows 用のインストールとアンインストールのみです。

たとえば、Software Delivery (SD) エージェントの SWD スキャン プロシージャなどの製品特有のアクションを実行する場合は、ソフトウェア パッケージライブラリに含まれる言語非依存の SD エージェント基本パッケージからプロシージャを実行します。

■ スタンドアロン Remote Control エージェントのインストール

スタンドアロン Remote Control (RC) エージェントは、SD 機能を使用してインストールすることはできません。これは、SD エージェントがエージェントホストにあらかじめ存在している必要があるからです。（さらに、スタンドアロン RC エージェントがスタンドアロンになる準備が整っている必要があります。これは、ほかのエージェント プラグインとは共存できません。）

スタンドアロン RC エージェントのインストールは、対話式に行うか、インフラストラクチャ展開ウィザードを使用して、追加パラメータ `/RITRM_RC_AGENT_STANDALONE=1` を指定して行うかの方法しかありません。そのため、「スタンドアロン エージェント」RC エージェント プロシージャは、ソフトウェア パッケージ ライブラリに含まれる複合パッケージには関係ありません。

必要なハードウェア設定

ハードウェアの仕様は、ネットワーク アーキテクチャ、使用可能な帯域幅、操作の頻度、操作のサイズ、およびエンドシステムの数など、さまざまなパラメータによって異なります。たとえば、Software Delivery マネージャをインストールする場合、必要なハードディスク領域の合計は、管理対象のソフトウェア パッケージおよび OSIM オペレーティング システム イメージのサイズと数に大きく依存します。

CA Client Automation を適切にインストールし実行するために満たす必要のあるハードウェアの要件に関しては、「CA Client Automation リリース ノート」の「ハードウェアの仕様および要件」を参照してください。

管理データベース(MDB)

DSM マネージャには管理データベース (MDB) が必要です。サポートされているプラットフォームの最新のリストについては、CA サポートの「[Compatibility Matrix](#)」を参照してください。

MDB は、以下の設定で表示できます。

- **ローカル設定** - マネージャおよびデータベースは、同一コンピュータ上で実行しています。

CA Client Automation では、Microsoft SQL Server に基づく MDB にのみこのことが適用されます。 マネージャおよび MDB の両方が Windows の動作環境にインストールされます。

- **リモート設定** - データベースはコンピュータ A 上にあり、マネージャはコンピュータ B にインストールされ、コンピュータ A のデータベースに接続しているクライアントを使用しています。

CA Client Automation では、Microsoft SQL Server および Oracle MDB の両方にこのことが適用されます。

Oracle MDB では、リモート設定が必須になります。 実際は、DSM マネージャは、Windows で動作しているコンピュータ上に存在し、OracleMDB は、サポート対象の Sun Solaris オペレーティングシステムで動作しているコンピュータ上にインストールされます。

多層アーキテクチャ内部では、管理データベース (MDB) はエンタープライズ層およびドメイン マネージャ層で実装できます。 両方の層で、Microsoft SQL Server および Oracle MDB がサポートされます。 たとえば、ドメイン マネージャに SQL Server を選択し、エンタープライズ マネージャに Oracle を選択するといった、個別の層に異なるデータベース プロバイダの MDB を実装できます。 .

SQL Server ベースの MDB を使用するドメイン マネージャと Oracle ベースの MDB を使用するエンタープライズ マネージャなどの混合構成では、マネージャ上に適切なデータベース クライアントが必要です。 ここでの例では、ドメイン マネージャ上に Oracle クライアント、およびエンタープライズ マネージャ上に SQL クライアントが必要です。

CA Client Automation のインストールが開始する前に、データベース サーバ（ローカル設定用）またはデータベース クライアント（リモート設定用）のいずれかをインストールする必要があります。

CA Client Automation のインストール中に、データベース タイプを選択します。

MDB PIF パッケージ

このパッケージをスタンドアロン MDB インストーラとして使用できます。

スタンドアロン MDB インストール

次の適切な MDB ディレクトリからセットアップ スクリプト (`setup.bat` または `setup.sh`) を実行することにより、スタンドアロン MDB インストーラとして MDB PIF パッケージを呼び出すことができます。

```
<DVR00T> %WindowsProductFiles_x86%mdb
```

```
<DVR00T> /LinuxProductFiles_x86/mdb
```

```
<DVR00T> /SolarisProductFiles_sparc/mdb
```

スタンドアロン インストーラとしての MDB PIF パッケージは MDB の新規インストール、再インストール、およびローカルまたはリモート ターゲット データベース サーバへのアップグレードをサポートします。

Oracle に対して、スタンドアロン MDB PIF パッケージは、Oracle Client が Oracle 11g Release 2 レベルかどうかをテストします。

PIF インストール レコード

MDB インストーラは、呼び出したソース コンピュータに PIF インストール レコードを残しません。そのため、ソース コンピュータを再利用して、別のターゲット リモート コンピュータに MDB をインストールすることができます。PIF インストール レコードは後者に残りません。

ただし、MDB インストーラは、メンテナンスを支援するため、`ca_settings` テーブルにそのバージョン番号を書き込みます。

リモート MDB コンピュータ上の古い PIF インストール レコードは、ローカルで実行されている場合でもリモートで実行されている場合でも、MDB のアップグレード時に削除されません。lsrm -e コマンドで Solaris にこれらの古いインストール レコードを手動で削除できます。

CCS の注意事項

CA Client Automation とともにインストールされる CA Common Services (CCS) には、Micro-CCS (英語のみ) として知られる簡易バージョン、および元々のフルバージョンの 2 種類があります。Micro-CCS (英語のみ) では、イベント管理およびカレンダーがサポートされますが、WorldView (DTS ネットワーク設定に使用される) またはディスカバリ (継続ディスカバリを含む) はサポートされません。CCS r11.2 (英語のみ) のフルバージョンは、Microsoft SQL Server MDB でのみ使用できます。

インストール時に、インストーラによって適切なバージョンが自動的に選択されます。これらの 2 種類のバージョンは、ネットワーク内の異なるホスト上には共存できますが、単一のホスト上には共存できないことに注意してください。また、Micro-CCS は、フル CCS にアップグレードできないことに注意してください。

以下の表は、さまざまな動作環境および MDB に対してどの CCS のバージョンをインストールできるかを要約したものです。

Linux の場合

インストール済みコンポーネント	CCS のバージョン
エージェント	なし
カレンダーなしのスケラビリティ サーバ	なし
カレンダーありのスケラビリティ サーバ	Micro-CCS、イベント エージェントのみ

注: CA Client Automation では、Linux 上でフル CCS が使用されることはありません。

Windows :

インストール済みコンポーネント	CCS のバージョン
エージェント	なし
カレンダーなしのスケラビリティ サーバ	なし
カレンダーありのスケラビリティ サーバ	Micro-CCS、イベント エージェントのみ
* ローカル SQL Server MDB を使用するマネージャ	フル CCS
* リモート SQL Server MDB を使用するマネージャ	MDB ホストにインストールする必要があるフル CCS、Client Automation ホスト上にもインストールする必要あり

リモート Oracle MDB を使用するマネージャ Micro-CCS（Client Automation 上のみ）、イベント エージェントとイベント マネージャ

* クラスタ化の使用の有無によって違いはありません。

UNIX :

CCS のバージョンがインストールされていません。

注: CCS と共にドメイン マネージャをインストールする場合は、SQL Server の名前付きインスタンスを使用すると、CCS をインストールできません。名前付き SQL インスタンスを使用して CCS を正常にインストールするには、SQL Server Browser サービスが動作している必要があります。SQL Server Browser サービスは SQL Server 構成マネージャから開始できます。

CCS インストール エラー メッセージ

CCS カレンダは、スケーラビリティ サーバへのインストールのみが信頼性があることに注意してください。DSM マネージャでフル CCS インストールが実行された場合は、以下のメッセージが表示される可能性があります。ここでの失敗のすべては、CCS と SQL Server ベースの MDB とのやりとりに関係します。

エラー テキスト (%TEMP%\ TRC_Inst2_ITRM.log 中)	条件	診断および解決策
MSSQLServer サービスが ¥¥local_host 上で実行されて いません。	MDB はリモートであ り、ローカルとリモ ートのホストが同じド メイン内にありませ ん。	リモート MDB ホストとは関係が確立され ようとはしていないため、このメッセージ は誤解を招く恐れがあります。 ローカル ホストをリモート ホストと同じ ドメインに追加します。

エラー テキスト (%TEMP%¥ TRC_Inst2_ITRM.log の中)	条件	診断および解決策
MSSQLServer サービスが ¥¥local_host 上で実行され ていません。	MDB はリモートであ り、ローカルとリモ ートのホストが同じド メイン内にありませ ん。	リモート MDB ホストとは関係が確立され ようとはしていないため、このメッセージ は誤解を招く恐れがあります。 ローカル ホストをリモート ホストと同じ ドメインに追加します。
ユーザ nsmadmin 用に指定 したパスワードが無効で す。		■ nsmadmin アカウントがすでに SQL Server 上に存在しており、DSM のインストール時に指定されたパスワードが異なっていました。(a) インストール前にすべての DSM/CCS ログインおよび DB ユーザを SQL Server から削除する、(b) DSM のインストール時に、一致するパスワードを指定する、または (c) DSM のインストール時に指定されるパスワードに一致するように、SQL Server の中で nsmadmin を変更する、のいずれかを行います。 ■ nsmadmin パスワードがシステムのパスワードの強度の条件を満たしません。パスワードの強度を上げます。
指定された MDB クレデン シャルが無効です。		nsmadmin アカウントがすでに SQL Server に対して定義されており、MDB 自体が存在しているかいないかのいずれかです。すでに SQL Server に存在するパスワードと、nsmadmin のパスワードが一致する場合であっても、このメッセージが表示されます。DSM/CCS ログインおよび DB ユーザを SQL Server から削除し、クリーンな状態にします。

エラー テキスト (%TEMP%\ TRC_Inst2_ITRM.log の中)	条件	診断および解決策
MSSQLServer サービスが %local_host 上で実行され ていません。	MDB はリモートであ り、ローカルとリモ ートのホストが同じド メイン内にありませ ん。	リモート MDB ホストとは関係が確立され ようとはしていないため、このメッセージ は誤解を招く恐れがあります。 ローカル ホストをリモート ホストと同じ ドメインに追加します。
この製品が使用する 1 つ 以上のデータベースに接 続しているアクティブな プロセスが存在します。 データの整合性およびシ ステムの安定性を保つた ために、インストールを開始 する前にこれらのプロセ スを正常にシャットダウ ンし、データベース接続を 閉じます。 [%TEMP%\ITRM.CCS#wizint. log また は %TEMP%\DSM_CCS_wizi nt.log の中。]		ほかのリモート Client Automation マネー ジャが以下の例のように MDB を共有して います。 11:36:50 ** Active DB Processes ** 11:36:50 DB Processes for 11:36:50 DB Name = mdb, Node = UNI6505L3-065, Process = CA IT Client Manager r12 11:36:50 DB Name = mdb, Node = CMQA158, Process = CA IT Client Manager r12 11:36:50 DB Processes for 11:36:50 ** End DB Processes ** 11:36:50 There are active processes connected ... これは、Client Automation システムが誤って 設定されているか、間違った順序で設定さ れている状態でない限り、実際に発生する 可能性は低いです。 一時的にリモートプロセスをシャットダウ ンします。ログファイルに、どのリモート ホストが関係するかが記載されています。

エラー テキスト (%TEMP%¥ TRC_Inst2_ITRM.log 中)	条件	診断および解決策
MSSQLServer サービスが ¥¥local_host 上で実行され ていません。	MDB はリモートであ り、ローカルとリモ ートのホストが同じド メイン内にありませ ん。	リモート MDB ホストとは関係が確立され ようとはしていないため、このメッセージ は誤解を招く恐れがあります。 ローカル ホストをリモート ホストと同じ ドメインに追加します。
依存関係チェック テスト が失敗しました。	Terminal Services がホ スト上で有効です。	CCS インストール時に Terminal Services を一時的に無効にしてください。 コンソール上でのインストールも動作可能になります。 また、「CCS/NSM 実装ガイド」では、「このリリースでは、アプリケーション サーバモードに設定されている場合でも、Windows ターミナル サービスからのインストールをサポートしています。」と記述されています。ただし、以下の設定が必要です。 ■ リモート アクセスからインストールを実行するには CONSOLE モードを使用する必要があります。 例： <pre>mstsc /v:HostName /console</pre> ■ インストール前に、ターミナル サーバの USER 設定を INSTALL に変更する必要があります。 例： <pre>change user /install</pre> ユーザ設定を確認するには、以下のコマンドを実行します。 <pre>change user /query</pre> Windows ターミナル サーバのユーザ変更ユーティリティの詳細については、 http://support.microsoft.com/kb/186504 http://support.microsoft.com/kb/186504 を参照してください。

DSM マネージャのインストールの前提条件

ほかの CA Technologies 製品が DSM マネージャ システムにインストールされ、マネージャ システムにはすでに MDB がインストールされているという場合があります。

DSM マネージャ インストールを開始する前に、MDB を使用中の製品がないことを確認してください。MDB を使用中の製品があると、インストール処理がハングアップする可能性があります。

Windows では、Unicenter Asset Portfolio Management の後に Client Automation をインストールする場合、corasmm.exe 処理が実行中であるかどうかを確認します。実行中の場合は、Unicenter Asset Portfolio Management 通知サーバおよび Unicenter Asset Portfolio Management キャッシュ サービスを手動に設定し、コンピュータを再起動してから Client Automation をインストールします。Client Automation インストールが完了したら、Unicenter Asset Portfolio Management 通知サーバおよび Unicenter Asset Portfolio Management キャッシュ サービスを再起動し、再度有効にする必要があります。これは、[コントロール パネル] - [管理ツール] - [サービス] にあるサービス コントロール マネージャで実行できます。

マネージャおよび MDB インストールにおけるディスク領域についての注意事項

12 GB 以上の空きディスク領域のパーティションに DSM マネージャをインストールします。約 7.7 GB のディスク領域がインストールに使用され、ログ ファイル用に追加領域を必要とします。同じパーティション上に MDB もインストールする場合は、データベース (SQL Server と Oracle の両方) および関連するオンラインチェック ポイントおよびジャーナル ファイル用に、追加で少なくとも 50 GB が必要となります。大きな SQL Server または Oracle データベースでは、最大 100 GB まで必要な場合があります。この数字は、配信するソフトウェア パッケージを保存するデータ ストレージ要件とは無関係です。詳細については、CA Client Automation ドキュメント セット (ブックシェルフ) の一部に含まれる「CA Client Automation リリース ノート」の「ハードウェアの仕様および要件」を参照してください。

通常、インストール後のシステムの再起動は必要ありませんが、再起動するとさらに多くのシステム リソースを使用可能にし、パフォーマンスが向上する場合があります。

ドメイン層とエンタープライズ層との間でデータの複製を行うには、tempdb データベースの最小サイズが必要です。したがって、tempdb ファイルおよびトランザクション ログに十分な領域が割り当てられるようにすることが重要です。tempdb 用の初期ファイル サイズをドメイン層では 80 MB に、エンタープライズ層では 2 GB にそれぞれ設定することをお勧めします。また、autogrowth プロパティが「unrestricted growth」に設定されていることを確認してください。

混合データベース環境でのスタンドアロン マネージャ

スタンドアロン ドメイン マネージャをインストールし、別の MDB データベース タイプを使用しているエンタープライズ マネージャにリンクする場合は、関連 データベース クライアントをドメイン マネージャに手動でインストールする必要があります。これは、ドメイン マネージャが複製を目的としてエンタープライズ マネージャに接続できるようにするためです。

たとえば、ドメイン マネージャが Microsoft SQL Server を使用しており、エンタープライズ マネージャが Oracle を使用している場合、ドメイン マネージャに Oracle データベース クライアントをインストールする必要があります。

応答ファイルを使用した MDB の自動インストール

MDB インストーラは、Windows の場合は `setup.bat -r response_file` コマンド、Linux/Solaris の場合は `setup.sh -r response_file` コマンドを使用した、応答ファイルからの自動インストールをサポートします。

MDB インストーラはまた、Windows の場合は `setup.bat -g response_file` コマンド、Linux/Solaris の場合は `setup.sh -g response_file` コマンドを使用した、応答ファイルの作成もサポートしています。

応答ファイルを生成する代わりに、応答ファイル テンプレート `install.rsp` を編集し、このテンプレートを使用して自動インストールを実行することができます。

応答ファイル内のパスワードの暗号化と復号化

デフォルトでは、MDB インストーラは MDB パッケージに含まれている Blowfish 暗号化および復号化ユーティリティ（Windows の場合は `blfs.exe`、Linux および Solaris の場合は `blfs`）を使用します。`-g` オプションを使用してセットアップを実行すると、アプリケーションは、自動的に Blowfish を使用して応答ファイル内のパスワードを暗号化します。

含まれているテンプレート `install.rsp` を編集することによって応答ファイルを作成した場合は、コマンドまたはシェル ウィンドウから Blowfish ユーティリティを実行してパスワードを暗号化します。次に、結果の文字列を応答ファイルにコピーします。

たとえば、Linux/Solaris 上で `blfs` の `validation_0101` コマンドから暗号化された文字列 `0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673` が返された場合は、この文字列を以下のように応答ファイルにコピーする必要があります。

```
# Password of Oracle MDB admin user
ITRM_MDBADMINPWD=0x530924b11654032a6e0e213281cd8565c3f9ec63b09dc673
```

どちらの場合も、`-r` オプションを使用してセットアップを実行すると、アプリケーションは、自動的に **Blowfish** ユーティリティを使用して応答ファイル内のパスワードを復号化します。

注: 暗号化されていないパスワードを `0x` (大文字と小文字が区別される) で始めることはできません。

Blowfish アルゴリズムは、**FIPS** に準拠していません。関連するプログラムを指す環境変数を設定することによって、暗号化または復号化のための **FIPS** 準拠のカスタム ユーティリティを指定できます。つまり、**MDB_ENC_PROG** を暗号化プログラムの完全パス名に、**MDB_DEC_PROG** を復号化プログラムの完全パス名に設定します。

例: Windows 上の暗号化または復号化プログラムの変更

```
set MDB_ENC_PROG=E:\tmp\my_encrypter.exe
```

```
set MDB_DEC_PROG=E:\tmp\my_decrypter.exe
```

Windows では、プログラムのファイル名に `.exe` 拡張子が含まれている必要があります。

例: Solaris または Linux 上の暗号化または復号化プログラムの変更

```
MDB_ENC_PROG=/tmp/my_encrypter  
export MDB_ENC_PROG
```

```
MDB_DEC_PROG=/tmp/my_decrypter  
export MDB_DEC_PROG
```

MDB_DEC_PROG を設定しない場合、またはそのプログラムが存在しない場合は、**MDB_DEC_PROG** が **MDB_ENC_PROG** と同じであると見なされます。
MDB_ENC_PROG を設定しない場合、またはそのプログラムが存在しない場合は、デフォルトの **Blowfish** 暗号化および復号化プログラムが使用されます。

Microsoft SQL Server MDB の使用準備

Microsoft SQL Server に基づく DSM マネージャをインストールする前に、Microsoft SQL Server を以下の設定でインストールしておく必要があります。

- 混合モード認証（つまり、Windows 認証および Microsoft SQL Server 認証）が必要です。
- TCP/IP ネットワーク プロトコルが有効になっており動作しています。ネットワーク プロトコルの選択および設定方法の詳細については、SQL Server のマニュアルを参照してください。
- 以下のルールは、Microsoft SQL Server インストール時に選択したサーバ照合順序に適用されます。

大文字小文字を区別しない照合がサポートされる照合名を選択する必要があります。

Client Automation インストール ウィザードを使用して、以下の説明に従って SQL Server MDB を設定します。

- ウィザードの [マネージャの設定] ページで、次のような、ターゲットデータベース システム用の必須の指定（接続パラメータ）を入力する必要があります。
 - 管理データベース プロバイダ（Microsoft SQL Server を選択）
 - 管理データベース サーバ
 - MDB パスワード

注：混合モード認証が使用されるので、このパスワードはシステム ログインパスワードのセキュリティ レベルに適合する必要があります。

- [Microsoft SQL Server MDB の設定] ページでは、以下の設定を入力できます。
 - 互換モード

注: 製品とともに出荷される新しい MDB 1.5 をインストールし、後から MDB 1.0.4 のみをサポートする CA Technologies 製品をインストールしようとする場合は、[互換モード] チェック ボックスを選択する必要があります。[互換モード] チェック ボックスを選択しないと、MDB 1.5 をサポートしない後続の製品のインストールが失敗します。

デフォルト: 互換モードは選択されていません。
 - MDB データベース名

デフォルト: mdb
 - MDB インターフェース名。

ドロップダウン リストからインスタンス名を選択します。

デフォルト: default
 - データベースのポート番号

デフォルト: 1433

インストール時、デフォルト以外のすべてのインスタンスに対して、Microsoft SQL Server インスタンスに関連付けられたポート番号を入力する必要があります。ポートは、SQL Server 設定管理を使用して、SQL Server TCP/IP 設定内で検索できます。

指定したインスタンスによって **Microsoft SQL Server** を設定すると、[TCP 動的ポート] オプションがポート番号付きで自動的に設定されます (動的ポート設定)。その後、システムの再起動などが原因で **MDB** システム上のポート番号が一時的に変更されるために、ドメインまたはエンタープライズマネージャがデータベースにアクセスできなくなることもあります。これらの失敗を避けるには、以下のようにポート設定を手動で静的ポート ID に変更することをお勧めします。

- **Windows** の [スタート] メニューから、[SQL Server 構成マネージャ] - [SQL Server ネットワークの構成] - [(インスタンス名) のプロトコル] - [TCP/IP] の順に選択します。
- **TCP/IP** を右クリックし、コンテキストメニューから [プロパティ] を選択します。
- [TCP/IP のプロパティ] ダイアログボックスで、[IP アドレス] タブを選択します。[IPAll] 領域で、[TCP 動的ポート] フィールドのポート値を切り取って [TCP ポート] フィールドに貼り付けます。

重要: デフォルト以外のポート番号を手動で割り当てる場合には、レジストリ内の **reservedPorts** リストを更新することをお勧めします。そうしないと、再起動後、**SQL Server** の前に **CAF** が開始されるようになり、**CAF** が動的ポート番号を要求すると、**SQL Server** 用に設定されたポート番号を **CAF** が取得してしまう可能性があります。その結果、**SQL Server** が起動時に失敗してしまいます。

DSM マネージャのインストール: Microsoft SQL Server MDB

Microsoft SQL Server MDB のインストールが完了したら、**DSM** エンタープライズまたはドメイン マネージャをインストールします。

以下の手順に従います。

1. **DSM** エンタープライズまたはドメイン マネージャをインストールするコンピュータに **Microsoft SQL** クライアントをインストールします。

注: **Microsoft SQL Server** がすでにコンピュータにインストールされている場合、この手順は必要ありません。

2. **Client Automation DSM** マネージャをインストールし、関連するダイアログボックスに **Microsoft SQL Server MDB** の詳細を入力します。
3. **CAF** を起動します。

Microsoft SQL Server のためのリモート MDB のインストール

リモート Microsoft SQL Server MDB を使用して DSM マネージャを実行することを予定している場合は、Windows 環境での実行時に、マネージャ コンピュータとリモート MDB コンピュータに信頼関係が必要です。

ドメインまたはエンタープライズ マネージャのインストール中に、ローカル ホストに MDB をインストールするか、または MDB の既存のリモートインスタンスを使用することができます。

リモート構成の場合は、[MDB のインストール] (CCS 機能なし) を選択することによって、リモート コンピュータにデータベースをインストールします。

Client Automation と共に CCS を使用する必要がある場合は、ローカルからリモートにかかわらず、MDB ホスト コンピュータに CCS をインストールする必要があります。最上位レベルの Client Automation インストール ダイアログ ボックスから、[CCS のインストール] オプションを使用します。次に、ドメインまたはエンタープライズ マネージャをインストールします。

リモート Microsoft SQL Server を使用する場合は、ドメインまたはエンタープライズ マネージャをインストールする前に、Microsoft SQL クライアント管理ツールをインストールします。Microsoft SQL クライアントのインストール中に、Microsoft SQL クライアント管理ツールが選択されていることを確認します。

Client Automation は、データベース レベルで作成された特定のユーザ `ca_itrm` を使用して MDB アクセスを認証されます。[MDB のインストール] および [Client Automation のインストール] ダイアログ ボックスでは、ユーザ `ca_itrm` に同じパスワードを指定する必要があります。ユーザ `ca_itrm` が自動的に作成されます。

リモート Microsoft SQL Server MDB と共に複数のドメイン マネージャをインストールする場合は、各データベース サーバインスタンス上に 1 つの MDB だけが存在することを確認します。この制限は、MDB と同じ数のデータベース サーバが存在する必要があることを示します。

注: リモート Microsoft SQL Server MDB では、ドメイン MDB をホストしているサーバの名前がドメイン マネージャの名前として使用されます。そのため、エンタープライズ マネージャ内の DSM エクスプローラには、そのデータベース サーバの名前と共にドメイン マネージャが表示されます。

Oracle MDB の使用準備

Client Automation インストール ウィザードを使用して、以下の説明に従ってマネージャが Oracle MDB と連携するように設定します。これらの設定手順の間に指定されたパラメータ値が、Oracle MDB のインストール中に入力されたパラメータ値と一致する必要があります。

- ウィザードの [マネージャの設定] ページで、次のような、ターゲットデータベース システム用の必須の指定（接続パラメータ）を入力する必要があります。
 - MDB プロバイダ（Oracle を選択）
 - MDB サーバ
 - MDB パスワード
 - データベース管理者（sys）
(詳細については、「[Oracle 上のデータベース管理者ユーザ \(P. 149\)](#)」を参照してください。)
 - データベース管理者のパスワード
- [マネージャの詳細設定] 領域の [データベース] ボタンをクリックし、別のウィザード ページを開き、カスタム MDB インストール用の詳細設定を指定します。
- [Oracle MDB の設定] ページでは、以下のような詳細設定を入力できます。
 - 互換モード
注: 製品とともに出荷される新しい MDB 1.5 をインストールし、後から MDB 1.0.4 のみをサポートする CA Technologies 製品をインストールしようとする場合は、[互換モード] チェック ボックスを選択する必要があります。[互換モード] チェック ボックスを選択しないと、MDB 1.5 をサポートしない後続の製品のインストールが失敗します。

デフォルト: 互換モードは選択されていません。
 - MDB データベース名
デフォルト: orcl
 - データベースのポート番号
デフォルト: 1521
 - MDB 管理者パスワード

前提条件

このセクションでは、Oracle 11g 上に MDB をインストールするための前提条件を示します。

- MDB をインストールまたはアップグレードすることを予定しているコンピュータに Oracle 11g サーバをインストールします。このリリースでは、Oracle 11g MDB 用に Windows、Solaris、および Linux サーバがサポートされます。
- Oracle Database Configuration Assistant を使用して Oracle インスタンスを作成します。インスタンスの作成中は、以下の要因を考慮してください。
 - データベース インスタンス名 (SID) は、Oracle サービス名 (グローバル名) と同じである必要があります。
 - Oracle Database Configuration Assistant の [Memory] タブにある [SGA size] および [PGA Size] フィールドに適切な値を入力する必要があります。
SGA には、少なくとも 2 GB を推奨します。
- CA ITCM DSM マネージャをインストールまたはアップグレードすることを予定しているコンピュータに Oracle 11g クライアントをインストールします。

注: インストール手順の詳細については、Oracle ドキュメント ライブラリに掲載されている適切な「インストール ガイド」を参照してください。

Oracle 上のデータベース管理者ユーザ

マネージャのインストールには、Oracle 管理者ユーザが必要です。Oracle ユーザ「SYS」を使用する場合、インストーラは「as sysdba」で接続します。ただし、ほかのユーザも使用することができます。その場合、そのユーザは、SYSDBA と同じ権限を持つユーザとして作成される必要があります。つまり、SYSDBA 権限がそのユーザに付与されていることを意味します。

Oracle に対する以下の操作を実行するには、ユーザは SYSDBA 権限を持つ必要があります。

- データベースの起動
- データベースのシャットダウン
- データベースのバックアップ
- データベースの回復
- データベースの作成

Oracle MDB をインストールする方法(スタンドアロン)

重要: インストール ウィザードの手順で入力した値およびパスワードは、後ほど DSM マネージャの設定時に必要になるのでメモするようにしてください。

インタラクティブモードで Oracle 11g 上に MDB をインストールするための基本的な手順は以下のとおりです。

1. まだ実行していない場合は Oracle Database Configuration Assistant を使用して Oracle インスタンスを作成し、以下の手順に従います。
 - データベース インスタンス名 (SID) が Oracle サービス名 (グローバル名) と同じであることを確認します。
 - Oracle Database Configuration Assistant の [Memory] タブにある [SGA size] および [PGA Size] フィールドに、インスタンスの適切な値を入力します。
2. MDB ディレクトリから、ターゲットデータベース サーバ上の適切なスクリプト ファイルを実行します。

Windows で有効

```
setup.bat
```

Solaris または Linux で有効

```
sh ./setup.sh
```

MDB インストーラが起動され、最初のウィザード ページである [セットアップ言語の選択] が表示されます。

3. セットアップ言語として英語を受け入れます。

注: このリリースで使用可能な言語は英語だけです。
4. エンド ユーザ使用許諾契約を受け入れます。
5. (Windows のみ) この手順では、データベース タイプとして Oracle サーバを選択します。
6. 有効な Oracle ランタイム環境を定義するために、[ORACLE_HOME] フィールドに、MDB のための Oracle インストールのパスを入力します。

リモート MDB のインストールの場合は、ローカル コンピュータの ORACLE_HOME 値を入力します。
7. Oracle データベース サーバ名および MDB サイズを指定します。
8. MDB ユーザおよびデータベース管理者の認証情報を指定します。

注: デフォルトの MDB ユーザ名は ca_itrm です。

9. Oracle サービス名、Oracle Transparent Network Substrate (TNS) 名、ポート番号、テーブル領域パス、MDB 管理者パスワードを含む、詳細な Oracle 構成設定を指定します。
10. データベース設定オプションを見直し、[インストール] ボタンをクリックしてインストールを確認します。

インストールが開始され、Oracle データベース内に MDB スキーマが作成されます。

注: Solaris 上の MDB インストーラでは、Oracle のバージョンや、オペレーティング環境の前提条件の確認を示すダイアログボックスが表示されます。新しい MDB インストーラでは、このダイアログボックスは前提条件のエラーがある場合にのみ表示され、それ以外の場合はインストールが続行されます。

11. Oracle MDB のインストールが完了したら、DSM マネージャをインストールします。

注: DSM マネージャは、Oracle MDB に接続するために EZCONNECT を使用します。

DSM マネージャのインストール: Oracle MDB

DSM エンタープライズまたはドメイン マネージャをインストールします。

以下の手順に従います。

1. DSM エンタープライズまたはドメイン マネージャをインストールするコンピュータに Oracle 11g クライアントをインストールします。
2. Client Automation DSM マネージャをインストールし、関連するダイアログボックスに Oracle MDB の詳細を入力します。

注: マネージャのインストールに MDB Oracle サーバの名前が必要なときは、マネージャと MDB が同じコンピュータ上に存在する場合にのみ IP アドレスを入力します。それ以外の場合は、ホストまたは DNS 名を入力します。

3. ウィザードの指示に従って、マネージャのインストールを完了します。
4. DSM マネージャが Windows Oracle MDB と同じコンピュータにインストールされる場合は、以下の追加の手順を実行します。

- a. mdbadmin として以下の SQL コマンドを実行します。

```
update ca_n_tier set
    label='<MDB Server host name>',
    db_host_name='<MDB Server host name>',
    db_server='<MDB Server DNS name>'
where domain_uuid in (select set_val_uuid from ca_settings where set_id=1)
```

- b. 更新がコミットされていることを確認します。自動コミットが無効になっている場合は、更新を手動でコミットします。
- c. コマンドプロンプトから以下のコマンドを実行します。

```
ccnfcmda -cmd setparametervalue -ps /itrm/database/default -pn dbmsserver -v
<MDB Server DNS name>
```

5. CAF を起動します。

リモート Oracle MDB のインストール

リモート Oracle MDB をインストールするには、まず Sun Solaris オペレーティングシステムで動作しているリモート コンピュータ上で、Oracle Database Configuration Assistant を使用して Oracle インスタンスを作成する必要があります。

Oracle MDB のインストール方法

1. 「root」ユーザで Solaris のホストにログオンし、
`DVD_mount/SolarisProductFiles_MDB/remotemdb` に移動します。
2. `sh ./setup.sh` を実行します。
3. [セットアップ言語の選択] オプションを選択します。
インストール ウィザードで使用する言語は、英語、フランス語、ドイツ語、および日本語です。
4. [新規インスタンス] を選択し、ウィザードの指示に従ってください。
重要: 以下の手順で入力した値およびパスワードは、後ほど DSM マネージャの設定時に必要になるのでメモするようにしてください。
5. インストール ウィザードを続行するには、エンドユーザ使用許諾契約を読んで承諾する必要があります。
6. ORACLE_HOME 環境変数には、MDB 用に使用する Oracle インストールのパスを入力します。
インストーラによって、ハードウェア プラットフォームおよび ORACLE の環境がチェックされます。失敗したテストがある場合は、インストールは行われません。すべてのテストが正常した場合のみ、ユーザはインストール ウィザードを続行できます。
7. 現在のインストール向けに「製品インスタンス名」を選択します。通常、これは ORACLE インスタンス (SID) と同じ名前です。
[製品名の選択] ドロップダウン リストには、すでに使用されている名前が表示されます。製品インスタンス名は、一意である必要があります。
8. MDB ユーザ名 (ca_itrm) 用のパスワードを入力します。
パスワードは、インストール時に設定され、確認するように要求されます。パスワードは覚えておいてください。
9. DB 管理者の名前 (デフォルト名「sys」) および DB 管理者のパスワードを入力します。DB 管理者は、Oracle インスタンス内で SYSDBA を付与された *username* です。

注: 詳細については、Client Automation ドキュメント セットの一部である「MDB の概要」を参照してください。

10. 互換モードをインストールするかどうかを指定します。

注: 製品とともに出荷される新しい **MDB 1.5** をインストールし、後から **MDB 1.0.4** のみをサポートする **CA Technologies** 製品をインストールしようとする場合は、[互換モード] チェック ボックスを選択する必要があります。[互換モード] チェック ボックスを選択しないと、**MDB 1.5** をサポートしない後続の製品のインストールが失敗します。

デフォルト: 互換モードは選択されていません。

11. [MDB データベース] フィールドに、MDB 用に使用する Oracle データベースインスタンスの **SID** を入力します。

このフィールドの値は、デフォルトでウィザードの以前のページで入力した製品インスタンス名になります。

12. データベースのポート番号を指定します。

デフォルト: 1521

重要: ここで入力するポート番号は、データベース作成時に使用されたポート番号によって異なります。データベース作成時にデフォルト以外のポート番号を使用した場合は、**MDB** をインストールする際に同じポート番号を入力してください。それ以外の場合は、デフォルトで表示されるデータベースのポート番号を変更しないでください。

13. Oracle がデータベース ファイルを作成するディレクトリとなる、テーブルスペースパスを入力します。このパスに含まれるすべてのディレクトリは、最後のものを除いてあらかじめ存在する必要があります。たとえば、ウィザードで事前に設定されたデフォルトパスの中で、「mdb」ディレクトリは存在できません。

デフォルト: /opt/CA/SharedComponents/oracle/mdb

14. [MDB 管理者パスワード] フィールドには、**MDBADMIN** ユーザのパスワードを入力する必要があります。

MDBADMIN データベース ユーザは、**MDB** スキーマを作成するのに使用され、このスキーマの所有者でもあります。

15. ウィザードプロセスの **MDB** のインストール ステージで、[インストール] ボタンをクリックしてインストールを確認する必要があります。

この確認が行われて初めて、**MDB** スキーマが **Oracle** データベース内に作成されます。

重要: リモート **Oracle MDB** を使用している場合、**Oracle 11g** クライアントがマネージャおよび **DSM** エンジンまたは **DSM** レポータが実行されているすべてのシステム上で利用できる必要があります。タイプが「管理者」である **Oracle 11g** クライアントを必ずインストールしてください。

関連項目:

[Oracle MDB のメンテナンス \(P. 239\)](#)

Oracle 用のリモート MDB インストール

注: Oracle データベースへのリモート MDB のインストールは、Windows からのみサポートされます。

リモートインストールの場合、ORACLE_HOME 環境変数は（Oracle クライアントのみが存在する可能性のある）ローカル コンピュータを参照します。

リモート Oracle MDB へのインストールおよびアップグレードの場合は、ローカル コンピュータ上の Oracle tnsnames.ora ファイル内にリモート コンピュータの TNS 名を定義します。これにより、リモート Oracle サーバをアドレス指定できます。

ローカル Oracle MDB のインストールの場合、MDB インストーラは、指定されたテーブル領域パス フォルダを作成します（まだ存在しない場合）。この手順は、リモートインストールには使用できません。そのため、MDB インストール中に選択しようとしているテーブル領域フォルダパスがリモート コンピュータ上に存在することを確認します。そのテーブル領域フォルダがリモート コンピュータ上に存在しない場合は、エラーが発生し、インストールの続行が妨げられます。

Oracle の CCS サポートに関する注意事項

CA Common Services (CCS) では現在、Oracle MDB をサポートしていません。

そのため Client Automation では、厳密に Client Automation のニーズ（主にイベント（カレンダー）および IPv6 サポート）に焦点を絞った、制限された機能セットを持つ CCS サブセットが利用可能です。

インストーラによって、ご使用の環境に適した CCS のバージョンが自動的に選択されます。

Oracle MDB のインストールおよび設定上の注意事項

以下のセクションでは、Oracle MDB のインストールおよび設定上の注意事項を示します。

Solaris 版 Oracle サーバのインストール

インストール手順の詳細については、Oracle ドキュメント ライブラリに掲載されている「インストール ガイド」を参照してください。

Oracle データベース インスタンスの削除および再作成

Oracle データベース インスタンスを削除および作成するには、Oracle Database Configuration Assistant ツールを使用します。このツールを使用して Oracle データベース インスタンスを作成する際、Oracle がそのインスタンス用に使用できるメモリ サイズを入力するようプロンプトが表示されます。[Memory] タブの [SGA size] および [PGA Size] フィールドに適切な値を入力します。

たとえば、[SGA Size] フィールドに「1198」、[PGA Size] フィールドに「399」と入力します。これらの推奨値は、データおよび制御情報 (SGA) 用に約 1.2 GB が、またプログラム領域 (PGA) 用に約 0.4 GB がそれぞれ使用できることを意味しています。これらは、コンピュータ アセットが最大 10,000 個までのシステムに対して推奨される最小値です。

Oracle サーバのインストールの確認

Oracle は、正しいバージョンとパッチ レベルがインストールされている必要があります。これらが誤っていると、DSM マネージャの処理が失敗する可能性があります。Oracle のバージョンおよびパッチ レベルを確認するには、以下のコマンドを実行します。

```
goto $ORACLE_HOME/OPatch
call ./opatch lsinventory
```

マルチバイト言語サポート用の Oracle MDB の設定

マルチバイト言語をサポートするには、Database Configuration Assistant ツールを使用して Oracle データベース インスタンスを作成する際に、[Character Sets] タブの [Use Unicode (AL32UTF8)] オプションを選択します。

ユーザ ca_DSM のデフォルトのパスワードの変更

マネージャのインストール中、または MDB のインストール中に、MDB へのアクセスで使ったユーザ ca_DSM のパスワードを変更することができます。

ca_DSM のパスワードを必要に応じて変更するには、データベース プロバイダのいずれかに応じていくつかの手順に従う必要があります。

- Microsoft SQL Server MDB
- Oracle MDB

Microsoft SQL Server を使用している場合のデフォルト パスワードの変更

データベース プロバイダとして **Microsoft SQL Server** を使用している場合に、ユーザ **ca_itrm** のデフォルト パスワードを任意のパスワードに変更するには、以下の手順に従います。

1. **Microsoft SQL Server** が実行されているシステムに移動します。
2. **Windows** の [スタート] - [プログラム] - [Microsoft SQL Server Management Studio] を開きます。
3. **Management Studio** の中でユーザ **ca_itrm user** を選択し、パスワードを変更します。
4. マネージャがインストールされているシステムに移動します。
5. `cadsmcmd setDBCredentials passwd=new_password` を実行します。
6. `caf stop` を実行します。
7. `caf start` を実行します。

Oracle を使用している場合のデフォルト パスワードの変更

データベース プロバイダとして **Oracle** を使用している場合に、ユーザ **ca_itrm** のデフォルト パスワードを任意のパスワードに変更するには、以下の手順に従います。

1. **Oracle** が実行されているシステムに移動します。
2. **Windows** の [スタート] - [プログラム] を開き、適切な **Oracle** データベース コントロールを起動します。
3. **Oracle** データベース コントロールの中のユーザ **ca_itrm** を選択し、パスワードを変更します。
4. マネージャがインストールされているシステムに移動します。
5. `cadsmcmd setDBCredentials passwd=new_password` を実行します。
6. `caf stop` を実行します。
7. `caf start` を実行します。

MDB インストール ログ ファイル

Microsoft SQL Server MDB を Windows で動作しているコンピュータ上にインストールする場合、以下の場所からログ ファイルを参照できます。

- %TEMP%\%ITRM%\database¥setup.log
- %TEMP%\%ITRM%\database¥mdb_install¥install_xxxx.log
- *Client Automation_installation_directory¥database¥setup.log*

Oracle MDB を Sun Solaris で動作しているコンピュータ上にインストールする場合、以下の場所からログ ファイルを参照できます。

- /tmp/CAInstaller.ca-cms-mdb-schema.install.log
- *Client Automation_installation_directory/database/setup.log*
- *Client Automation_installation_directory/database/mdb_install/install_xxxx.log*

Solaris では、以下の場所にもログ ファイルが保存されています。

- *Client Automation_installation_directory/log/mdbinstall.log*
- *Client Automation_installation_directory/log/mdbupgrade.log*

前にインストールに失敗した場合は、ログ ファイルが /tmp/mdbinstall.log に残っている可能性があります。

MDB のアップグレード

このリリースでは、以下の MDB のアップグレードがサポートされます。

- Microsoft SQL Server MDB がローカルまたはリモートでインストールされたリリース 12.5SP1 またはそれ以降の DSM マネージャ。
- Oracle 11g MDB が Solaris、Linux、または Windows 上にリモートでインストールされたリリース 12.5SP1 またはそれ以降の DSM マネージャ。
- Windows、Linux、および Solaris 上にローカルまたはリモートでインストールされた、パッチが適用された DSM マネージャおよび Oracle MDB。

注: まず Oracle 10g サーバを Oracle 11g R2 にアップグレードする必要があります。また、DSM マネージャ セットアップを起動する前に、DSM マネージャ上の Oracle クライアントを Oracle にアップグレードします。

データベース サーバがリモートである場合、MDB は、DSM マネージャの現在のリリースへのアップグレード中にアップグレードされます。Microsoft SQL Server の場合は、comstore からデータベースの詳細が取得されるため、ユーザ インタクションは必要ありません。Oracle の場合は、ORACLE_HOME 環境変数を設定し、Oracle サービス名、TNS 名、および mdbadmin と sys のパスワードを入力します。

アップグレード中に既存のデータベースセッションが見つかった場合は、各セッションが、データベースユーザの名前、プロセス ID、およびホストコンピュータと共に表示されます。データベースセッションは、ダイアログボックス内に 2 つのリストで表示されます。最初のリストは、アップグレードの続行が許可される前に閉じる必要のあるセッションを示します。このリストには、DSM スキーマによって作成されたロールのメンバであるデータベースユーザに属するセッションが含まれています。担当者のロールは、ams_group、ca_itrm_group、ca_itrm_group_ro (Oracle のみ)、ca_itrm_group_ams、upmuser_group、および mdbadmin (Oracle のみ) です。emadmin、emuser、uniadmin、uniuser、wvadmin、wvuser などの CCS ロール (Microsoft SQL Server の場合のみ) もまた、最初のリストに含まれています。(これらのロールは、DVD イメージ上の設定ファイルから読み取られます。)

2 番目のリストには、他のデータベースユーザに属する残りのセッションがすべて表示されます。これらのセッションも閉じることをお勧めしますが、この手順は必須ではありません。これらの未処理のセッションが開かれたままでも、アップグレードに進むことができます。

開かれたデータベースセッションを閉じたときにリストを更新するには、このダイアログボックスにある [更新] ボタンを使用します。[継続] ボタンは、データベースセッションの最初のリストが空の場合にのみ有効になります。

アンインストール

Client Automation では、MDB スキーマのアンインストールがサポートされていません。DSM マネージャのアンインストール中にデータ アンインストール スクリプトを使用して、MDB から選択されたデータを削除できます。また、Microsoft SQL Server と Oracle の機能を使用して、MDB インスタンスを削除および再作成することもできます。

Client Automation インストールに関する特記事項

以下は、特別なインストール シナリオの注意事項および推奨事項です。内容は上級ユーザ向けとなっています。

セキュリティ ポリシー設定

以下のセキュリティ ポリシーは、DSM マネージャまたは管理データベース (MDB) をインストールするために使用するユーザ ログオンに対して有効にする必要があります。

- ネットワークからこのコンピュータにアクセス
- オペレーティング システムの一部として動作します。
- ターミナル サービス経由のログオンを許可します。
- サービスとしてログオン

これらのポリシーは、Windows の [コントロール パネル] - [管理ツール] - [ローカル セキュリティ ポリシー] で有効にできます。

CAM および SSA PMUX の再起動

拡張ネットワーク接続 (ENC) をインストールするか否かにかかわらず、Client Automation インストーラは、内部的に CA メッセージ キューイング (CAM) および安全なソケット アダプタ ポート マルチプレクサ (SSA PMUX) インストーラを起動し、必要に応じて、CAM および SSA PMUX が再起動されます。

注: SSA PMUX の再起動は、Windows にのみ適用されます。

ENC については、「拡張ネットワーク接続 (ENC)」を参照してください。

ソフトウェア インベントリの使用可能性

ドメイン マネージャのインストール後、そのままソフトウェアのフル インベントリを使用することはできません。これは、デフォルトで夜の 12 時に実行されるようにスケジュールされているエンジン タスク経由で MDB にソフトウェア定義がインポートされるからです。

IPv6 上での DSM マネージャとリモート SQL Server MDB のインストール

IPv6 上で DSM マネージャ (ドメインまたはエンタープライズ) をリモート SQL Server MDB と共にインストールする場合は、インストールを開始する前に以下の手順に従います。

1. マネージャ マシンで以下のレジストリ キーの値を 1 に設定します。

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Services\Smb\Parameters\IPv6EnableOutboundGlobal (REG_DWORD)
```


2. 以下の点を確認します。
 - MDB マシンのホスト名がグローバル IPv6 アドレスに解決される。
 - IPv6 アドレスの逆引きルックアップが同じ MDB ホスト名に解決される。
 3. MDB マシンにアクセスするのに使用される DSM マネージャ マシン上で MDB マシンが到達可能な IPv6 アドレスにのみ解決されることを確認します。
- つまり、マネージャ マシンが使用する DNS サーバ上の MDB マシンの IPv4 DNS レコードや、マネージャ マシンが MDB マシンにアクセスできないようなアドレスを含む IPv6 DNS レコードは、すべて削除する必要があります。DSM マネージャ上の DNS キャッシュは、必要に応じて内容を消去する必要があります。そうしないと、JDBC が MDB への接続に失敗し、結果的に、CCS、CIC、および MDB Java コンポーネントのインストールに影響を及ぼします。

名前付きインスタンスを持つリモート SQL Server MDB を使用したドメイン マネージャのインストール

名前付きインスタンスを持つリモート SQL Server MDB を使用して、ドメイン マネージャを正常にインストールするには、SQL Server ブラウザがリモート MDB システム上で実行されていることを確認します。インストールを開始する前に、ドメイン マネージャがリモート MDB に接続できること、および Microsoft SQL ブラウザが正常に機能していることを、ドメイン マネージャ システム上で以下のコマンドを実行して、確認します。

```
sqlcmd -E -d mdb -S MDB server name [¥instance name] -q "select * from mdb"
```

Remote Control スタンドアロン エージェントのインストール

Client Automation のリモート コントロール (RC) 機能は、スタンドアロン モードで設定できます。このモードでは、RC エージェントは、セントラル ドメイン マネージャから送信されたポリシーではなく、ローカル セキュリティおよび設定ポリシーを使用します。

Client Automation インストール メディア (DVD) には、スタンドアロン RC エージェントをインストールする `setup_rc` という名前の別のインストール ウィザードが含まれています。

スタンドアロン RC エージェントのインストールでは、以下の CAF プラグインのみが有効になります。

- pmux
- rchost
- smsserver

Setup_rc は以下の場所にあります。

- WindowsProductFiles_x86¥AgentRC
- LinuxProductFiles_x86/rc_agent

Solaris Intel へのインストール

Solaris (Intel) プラットフォーム上への Client Automation のインストールを開始する前に、必ず SUNWlibc パッケージ用の以下のパッチをインストールします。

- 109148-07
- 108436-16

これらのパッチを適用することで、標準 C++ ランタイム ライブラリを確実に使用できるようにすることができます。

以下のコマンドを使用して、これらのパッチの存在を検証できます。

```
showrev -p | grep SUNWlibc
```

このコマンドを実行すると、以下のようなメッセージが出力されます。

```
Patch: 108436-16 Obsoletes: Requires: 109148-07 Incompatibles: Packages: SUNWlibc
```

注: Client Automation は CAPKI に依存します。CAPKI は Solaris Intel 上の libc++ に依存性しています。Solaris Intel 11 では、libc++ がデフォルトでインストールされない場合、インストールは失敗します。

libc++ を Solaris Intel 11 にインストールするには、以下の手順に従います。

1. パッケージを識別するために以下のコマンドを実行します。

```
pkg search -r /usr/ucblib/libc++.so.1
```
2. パッケージをインストールするために以下のコマンドを実行します。

```
pkg install <パッケージ名>
```

Solaris Intel 用の PATH 環境変数

シェルの起動により、起動スクリプトが呼び出されます。sh ベースのシェル (bash など) が、`/etc/profile` を呼び出し、その後に `~/.profile` を呼び出すことに注意してください。ただし、Solaris 11 Intel では、root ユーザの `~/.profile` が PATH 環境変数よりも優先されます。

PATH に CA パスが含まれていない場合は、必ず、以下の方法で起動スクリプトを実行してください。

- `./etc/profile.CA all` または
- `source /etc/csh_login.CA all`

VMware ESX Web サービスへのアクセス

VMware ESX Web サービスにアクセスするには、VMware ESX ホスト マシンのユーザ用に以下のログオン クレデンシャルを指定する必要があります。

ホスト名

アセット管理インベントリが収集される ESX ホストの名前を指定します。IP アドレスも指定できます。

Web サービス ユーザ名

VMware システム ロールが「管理者」または「読み取り専用」の VMware ESX ユーザの名前を指定します。

Web サービス パスワード

指定された VMware ESX ユーザのパスワードが必要です。

Web サービス URL

Web サービスの URL を、以下の形式で示します。

`https://ESXHostFQDNservername/sdk`

ESXHostFQDNservername は、ESX サーバの完全修飾ホスト名を表わします。ホスト名の代わりに IP アドレスを指定することもできます。

ESX インベントリ収集は、Web サービス (SOAP) エンジンを使用して実行されます。デフォルトでは、Web サービスは、ポート 443 で、SSL over HTTPS を使用してアクセス可能な、セキュリティ保護された Web サービスとして実行されます。

Linux での Remote Control コンポーネントのインストール

Client Automation のリモート コントロール (RC) 機能は、Linux をサポートします。このオペレーティング環境では、RC ホストのコンポーネントのみがサポートされています。

このオペレーティング環境でスタンドアロン RC エージェントが必要な場合は、LinuxProductFiles_x86/rc_agent ディレクトリからインストールする必要があります。

スタンドアロン エージェントは、Software Delivery の機能またはインタラクティブ インストーラを使用して展開することはできません。

Apple Mac OS X での Remote Control コンポーネントのインストール

Client Automation のリモート コントロール機能は、Apple Mac OS X をサポートします。このオペレーティング環境では、Remote Control ホストのコンポーネントのみがサポートされています。

セキュア コントロール モードはサポートされていません。その他すべてのコントロール モードはサポートされています（ステルス ビュー、ビュー、共有、クラスルーム、および排除）。

Linux と同様、ホストの壁紙やその他のユーザ エクスペリエンス機能を無効にするビューアのオプションは、効力を持ちません。

重要: Mac OS X プラットフォームで Remote Control エージェントのインストール、再インストール、修復、またはアップグレードを行ったら、システムから一旦ログアウトし、ログインし直すことをお勧めします。これにより、重要な DSM プロセスが、正しいユーザ コンテキストで確実に開始されます。この手順を省略すると、リモート コントロール接続の試行が、「ホストは現在のユーザのデスクトップを開けませんでした。」というメッセージで拒否されます。

ブート サーバの共有アクセス

ブート サーバは常にスケーラビリティ サーバの一部としてインストールされます。ブート サーバの詳細設定は、インストール ウィザードのスケーラビリティ サーバの設定ページで指定します。

TFTP (デフォルト) ではなく共有アクセスを設定する必要がある場合は、[スケーラビリティ サーバの設定] ページの [サーバの詳細設定] エリアにある [ブート サーバ] ボタンをクリックし、[Windows のネットワーク共有の使用を有効にします] オプションを選択します。インストーラにより、SMB プロトコルを介してアクセス可能な読み取り専用ネットワーク共有が作成されます。

TFTP から共有アクセスに切り替える方法、および PXE サーバを停止する方法の詳細については、「OS インストール管理 管理者ガイド」を参照してください。このガイドは、CA Client Automation のドキュメント セット (マニュアル選択メニュー) の一部として利用可能です。

CCS のインストール時のドメイン コントローラ接続

ドメイン管理者で CCS をインストールしている時にドメイン コントローラへの接続が失われ、インストールするユーザの権限が検証されようとする際に、1073741819 というリターン コードで CCS のインストールが失敗してしまうことがあります。

これを解決するには、ドメイン コントローラへの接続を再度確立するか、ローカル管理者でインストールを実行します。

エージェントおよびスケーラビリティ サーバの移動操作

エージェントは、ある特定の時点で 1 つのドメイン マネージャにのみ接続するように設定されています。ただし、エージェントは再設定可能です。エージェントの移動は、以下のコマンドを実行してトリガできます。

```
caf setserveraddress new_scalability_server
```

スケーラビリティ サーバの移動は、以下のコマンドを実行してトリガできます。

```
cserver config -h new_domain_manager  
cserver レジスタ
```

CA Common Services (CCS) サーバ (DSM マネージャ上にある) でカレンダーが更新された場合は、CCS エージェント (DSM スケーラビリティ サーバ上にある) を更新する必要があります。そのため、CCS エージェントがインストールされたダウンロードのすべてのスケーラビリティ サーバ上で、スケーラビリティ サーバ プロシージャ「CCS カレンダーの同期」を実行します。

コマンド `cserver config -h new_manager` を使用して、マネージャ間でスケーラビリティ サーバを移動する場合、CCS エージェント（スケーラビリティ サーバ上にある）は、新しいマネージャに接続するように、自動的に再設定されます。

注: サーバの再登録時に CCS 値が変更されないようにするには、"-h" ではなく "-i" オプションを指定して `cserver` コマンドを実行します。

ただし、ポリシーを使用してサーバを移動する場合は、手動で再設定する必要があります。そうしないと、エージェントは古い CCS サーバに接続し続けます。`new_manager` 上の CCS サーバに変更するには、スケーラビリティ サーバコンピュータ上で以下のコマンドを使用します。

```
cautenv setlocal CA_CALENDAR_NODE new_manager_address
cautenv setlocal CA_OPR_PROXY new_manager_address
unicntrl stop all
unicntrl start all
```

ドメイン コントローラ上の CCS WorldView マネージャまたは MDB インストールを含む CCS を使用した DSM マネージャ

ドメイン コントローラ上の CCS（CA Common Services）WorldView マネージャまたは「MDB を含む CCS」を使用した DSM マネージャのインストール シナリオでは、以下の CCS 制限が適用されます。

CCS WorldView マネージャは、ドメイン コントローラに指定されているサーバにインストールすることはできません。

このことは、CA 重要度継承 COM オブジェクトを開始するときに、IPSEC セキュリティが Microsoft COM サーバのユーザ権限を上書きすることが原因です。

この制限により、CA Client Automation は CCS WorldView マネージャをドメイン コントローラにインストールすることができません。DSM マネージャおよび「MDB を含む CCS」のインストールが関連しています。DSM マネージャを正しくインストールするために、ドメイン コントローラで以下のオプションを使用できます。

- CCS を無効にします（そうすると CCS 機能が使用できなくなります）。
- MDB および CCS をリモートでインストールします（そうすると CCS WorldView マネージャが MDB 側にインストールされます）。

Linux へのスケーラビリティ サーバのインストール

DMDeploy または Software Delivery を使用して、CA DSM スケーラビリティ サーバ Linux (インテル) ENU パッケージと共にスケーラビリティ サーバを Linux にインストールする場合、CA Common Services ソフトウェアはインストールされません。Linux 上でスケーラビリティ サーバに CCS が必要な場合、それを DVD から対話形式でインストールする必要があります。

UNIX と Mac OS X コンポーネントのインストールと登録

これらのコンポーネントは、ドメイン マネージャのインストール時に、Software Delivery ライブラリおよびインフラストラクチャ展開ライブラリに自動的に登録されません。

これらのパッケージをドメイン マネージャで使用可能にするには、dsmPush ツール (DVD のルートディレクトリにある dsmPush.dms ファイル) を使用して、該当する CD からマネージャのソフトウェア パッケージライブラリおよびインフラストラクチャ展開ペイロードエリアにインポートします。

以下のコマンドを実行します。

```
dmscript dsmPush.dms copy -I location_of_CD_image
```

ソフトウェア パッケージライブラリへのこれらのパッケージの登録は、該当する CD から DSM エクスプローラの [ソフトウェア ライブラリ] フォルダへ、パッケージをコピーアンドペーストしても実行できます。

UNIX エージェントに関する考慮事項

Client Automation の UNIX エージェントにより現在サポートされている UNIX 動作環境の一覧は、Client Automation ブックシェルフまたは CA サポートで利用できる互換性マトリックスを参照してください。そこに記載されているプラットフォームは、Linux および UNIX 用パッケージを実行できるプラットフォームでもあります。

Sun Solaris でのエージェント インストールの前提条件

adsm> UNIX エージェントを Sun Solaris コンピュータにインストールする前に、必要な最低限のカーネル設定パラメータが設定されていることを確認する必要があります。

Solaris 5.10 用のカーネル設定パラメータを設定または変更する方法

Solaris 5.10 では、`max-shm-memory` リソース制御設定パラメータを 5242880 またはそれ以上に設定する必要があります。

また、`max-sem-ids` パラメータを 256 またはそれ以上に設定する必要があります。

1. `prctl` コマンドを使用して、たとえば以下のようにしてこれらのパラメータの現在の値を問い合わせます。

```
prctl -P -n project.max-shm-memory -i project user.root
```

```
prctl -P -n project.max-sem-ids -i project user.root
```

2. リソース制御設定パラメータを更新する必要がある場合は、以下のコマンドの中から 1 つを使用します。

- `prctl` を使用して、たとえば以下のようにリソース制御設定パラメータを変更します。

```
prctl -n project.max-shm-memory -v 5242880 -r -i project user.root
```

```
prctl -n project.max-sem-ids -v 256 -r -i project user.root
```

注: `prctl` コマンドを使用して変更された設定パラメータは効力が永続的ではないので、システムが再起動したらコマンドを再度実行する必要があります。

- `projmod` を使用して、たとえば以下のようにリソース制御設定パラメータを変更します。

```
projmod -s -K "project.max-shm-memory=(priv,5242880,deny)" user.root
```

```
projmod -s -K "project.max-sem-ids=(priv,256,deny)" user.root
```

注: `projmod` コマンドを使用して変更された設定パラメータは、システムの再起動後も効力が持続します。

IBM AIX でのエージェント インストールの前提条件

AIX バージョン 5.3 以降が実行されている IBM AIX コンピュータに Client Automation UNIX エージェントをインストールする際に、最新の IBM のランタイム環境ライブラリがインストールされます。

Software Delivery のダウンロードと UNIX エージェント

Software Delivery ダウンロードメソッドが内部 NOS メソッドに設定されている場合、以下の注意事項が適用されます。

Sun Solaris カーネルは、現在 Samba 共有のマウントをサポートしていません。

スケーラビリティ サーバで NFS マウント ポイントのみが設定されている（つまり、Samba を使用しない）場合、Sun Solaris エージェントは自動的に NFS を使用します。

スケーラビリティ サーバに Samba の共有が設定されており、NOSLessSwitchAllowed パラメータが 1（True）の場合、Sun Solaris エージェントは内部 NOSless ダウンロードメソッドを使用します。

スケーラビリティサーバに Samba の共有が設定されており、NOSLessSwitchAllowed パラメータが 0（False）である場合、スケーラビリティサーバに NFS マウント ポイントが設定されていても、ダウンロードは失敗します。

NOSLessSwitchAllowed パラメータに設定されている値を確認するには、以下のコマンドを実行します。

```
ccnfcmda -cmd GetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed
```

以下のコマンドを実行すると NOSLessSwitchAllowed パラメータの値を 1 に設定できます。

```
ccnfcmda -cmd SetParameterValue -ps itrm/usd/agent -pn NOSLessSwitchAllowed -v 1
```

注: ccnfcmda エージェント設定コマンドの詳細については、「<command> /?」と入力してください（コマンドプロンプトで実行）。

DTS (Data Transport Service) のインストールに関する注意事項

Windows では、DTS (Data Transport Service) 機能は SD (Software Delivery) エージェントプラグインではなく、別個のインストールパッケージに含まれています。このため、たとえば特定のエージェントに対して DTS ダウンロード方法を使用するために DTS 機能が必要な場合、そのエージェントに対して別個の DTS インストールパッケージを展開する必要があります。

Linux または UNIX では、DTS (Data Transport Service) 機能は SD (Software Delivery) プラグインに含まれています。このため、DTS は SD エージェントインストールパッケージによりインストールされます。

マネージャ コンピュータとスケーラビリティ サーバ コンピュータの名前の変更

CA Client Automation (Client Automation) では、特定の [ドメイン プロパティ] または [エンタープライズ プロパティ] ダイアログ ボックスを使用して DSM エクスプローラによるエンタープライズ マネージャとドメイン マネージャの名前変更をサポートしています。[名前]、[連絡先情報]、および [説明] フィールドは編集でき、これらの値は、エンタープライズ マネージャとドメイン マネージャ間で複製されます。

Client Automation では、スケーラビリティ サーバ コンピュータの名前変更はサポートされていません。

完全修飾ドメイン名としてのシステム名

Client Automation インストーラによってシステム名の入力を求められた場合は必ず、ドメイン サフィックスを含む完全修飾ドメイン名 (FQDN) を入力することを強くお勧めします。これにより、転送リクエストが関連するすべての DNS 用に設定されていない場合でも、他のネットワーク ドメイン内のコンピュータ システムに接続することができます。

Unicenter NSM r11 がプリインストールされている場合の Client Automation のインストール

CA Client Automation の前に Unicenter NSM r11 がインストールされている場合、CA Client Automation のインストールが開始される前に Unicenter NSM によって以下の CCS コンポーネントがインストールされている必要があります。

Unicenter NSM コンポーネント：

- Management Database
 - Microsoft SQL Server の MDB
- WorldView
 - 管理クライアント
 - WorldView マネージャ
- エンタープライズ管理
 - 管理クライアント
 - イベント管理
 - イベント エージェント
 - イベント マネージャ
- 継続ディスカバリ
 - 継続ディスカバリ エージェント
 - 継続ディスカバリ マネージャ

Unicenter NSM のインストールを開始して、リストされているコンポーネントがすべてインストールされているかどうかを確認し、欠落しているコンポーネントをインストールします。

Unicenter NSM のインストールが完了したら、CA Client Automation のインストールを開始できます。

インストール時の Web コンソールのポート番号の指定

wacconfig.properties ファイルに含まれるデータベースのポート番号を使用した SQLServer.PortNo キーの変更は、Web コンソールの複数マネージャのサポートでは有効ではなくなりました。正しいポート番号はインストール中に設定する必要があり、後で変更することはできません。

[インストールの変更]方式を使用して Web コンソールを追加する際の注意事項

[インストールの変更]方式を使用して Web コンソールを追加する場合は、最低 8 GB のディスク領域が使用可能であることを確認する必要があります。

インストールおよびアンインストール中のウイルス保護の無効化

CA Client Automation のインストールまたはアンインストールを開始する前に、ウイルス保護を無効化しておくことをお勧めします。ウイルス保護ソフトウェアが有効になっている場合、インストールまたはアンインストール プロセス中に干渉が発生することがあります。

インストール中のリモート セクタ サーバ サービスの無効化

Client Automation のインストール先のコンピュータ上にインストールされている以前の Unicenter Asset Management リリースからのリモート セクタ サーバ (RSS) が存在する場合、RSS サービスを停止してから Client Automation インストールを開始する必要があります。RSS サービスを無効化しておく必要があるのは、自動的にこのサービスの再起動が試行されるためです。

サービス コントロール マネージャから Asset Management セクタ サーバ サービスを無効化します。インストール後にサービスを再び有効化します。

Windows XP ネットワーク アクセス - ローカル アカウントの共有とセキュリティ モデル

Windows XP のポリシーが [ゲストのみ] に設定されている場合、ローカル ユーザとしての認証を試行するユーザは、デフォルトで無効になっている Guest アカウントにマップされます。このため、認証は失敗します。

この問題を訂正するには、次のサイトで Microsoft のドキュメントを参照してください。

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/506.mspx

Windows Server 2003 の注意事項

Windows NT サーバおよび Windows 2000 サーバの場合、ネットワーク リソースへのアクセスに、デフォルトで匿名アクセス（NULL セッションとも呼ばれる）を使用することができます。ファイル システム 共有（NULL セッション共有と呼ばれる）は、NULL セッションを受け入れるように設定することができます。LocalSystem アカウントで実行されている Software Delivery（SD）エージェントがスケーラビリティ サーバ上のソフトウェア パッケージ ライブラリ（SDLIBRARY\$ 共有）にアクセスする場合は、常にこの方法が推奨されてきました。

Windows Server 2003 では、旧バージョンのサーバオペレーティング システムと比較してセキュリティ レベルが向上しています。デフォルトでは、匿名アクセスおよび NULL セッション共有は無効になっています。ドメインに属するコンピュータの場合は、Windows セキュリティ システムでマシン ドメイン アカウントを有効なセキュリティ プリンシパルにすることにより、匿名アクセスを行う必要はなくなりました。Windows 2000 ドメインおよび Windows Server 2003 ドメインでは、アクセス権限はユーザ アカウントだけでなくマシン アカウントに対しても付与することができます。

Windows Server 2003 の場合、これらのエージェントにソフトウェア パッケージ ライブラリへのアクセスを提供するために NULL セッション共有は使用されません。この場合、SD では、エージェントはマシンのドメイン アカウントを介してライブラリにアクセスすることを許可されます。このアプローチはセキュリティの度合が高く、Microsoft でも推奨されていますが、サポートされているすべての SD エージェント動作環境に対して完全なソリューションを提供するわけではありません。

Windows 動作環境での匿名アクセスの変遷については、Microsoft のサポートの Knowledge Base 文書 278259 をお読みください。

SDMSILIB を使用した、Windows Server 2003 への MSI 管理者によるインストール

MSI 管理者によるインストールを使用して SDMSILIB 共有に対してパッケージを展開する場合、その共有に接続するには「sd_ss cmd libraryaccess」メソッドだけでは不十分です。Software Delivery（SD）の機能を使用したインストールまたは環境設定が実行されていなくても、エージェントはこの共有にアクセスする必要があります。これは、たとえば修復や自己回復の実行時に、MSI インストールによって SDMSILIB 共有へのアクセス リクエストが要求される可能性があるためです。この場合、SD では、エージェントはマシンのドメイン アカウントを介して SDMSILIB 共有にアクセスすることを許可されます。

Windows 2003 SP1 MSI ライブラリ アクセス - 名前付きパイプおよび共有への匿名アクセスの制限

デフォルトでは、Windows 2003 Service Pack 1 でのネットワーク共有への匿名アクセスは拒否されます。

SDMSILIB 共有から MSI パッケージのネットワーク インストールを実行する場合や、Windows 2003 Service Pack 1 を実行しているコンピュータ上の SDLIBRARY\$ 共有に対する汎用匿名アクセスを行う場合は、以下の手順を実行する必要があります。

- [ローカル セキュリティ ポリシー] で、次のセキュリティ オプションを設定します。
[ネットワーク アクセス: 名前付きパイプおよび共有への匿名アクセスの制限] - [無効]
- システムを再起動して、変更を有効にします。

SD スケーラビリティ サーバに接続している SD エージェント

以下の記述は、Windows Server 2003 で実行されている Software Delivery (SD) スケーラビリティ サーバに SD エージェントが接続されており、かつマネージャまたはスケーラビリティ サーバ上で [ローカル セキュリティ ポリシー] の [ネットワーク アクセス: 名前付きパイプおよび共有への匿名アクセスの制限] が、[有効] に設定されていることを前提としたものです。

Windows XP または Windows Server 2003 を使用するコンピュータ上で実行されている SD エージェントで、どのドメインにも属していないもの、およびソフトウェア パッケージ ライブラリ 共有が存在する SD マネージャとは別の信頼されていないドメインに属しているもののいずれもが、同様にアクセスを拒否されます。

Windows XP または Windows Server 2003 上の SD エージェントのアクセス問題を解決するには、スケーラビリティ サーバ マシン上で専用ユーザ アカウントを手動で作成し、Everyone グループに追加します。これにより、SDLIBRARY\$ 共有への読み取り専用アクセスが許可されます。新しい Windows マネージャ プラットフォーム上で実行されるドメイン マネージャおよびスケーラビリティ サーバそれぞれの共通設定ストアに、ユーザ名とパスワードを入力する必要があります。

障害を未然に防ぐため、ライブラリへのアクセスが拒否された場合、SD エージェントは自動的に内部 NOS なしダウンロードにフォールバックします。設定ポリシー セクション itrm/usd/agent 内の NOSLessSwitchAllowed を False に設定することにより、オプションでこの動作を無効にすることができます。

Windows Server 2008 のコア オペレーティング環境

このセクションは、Windows Server 2008 のサーバのコア オペレーティング環境での、既知の問題、回避策およびソリューションについて記述します。

GUI (グラフィカル ユーザ インターフェース)での依存関係

Windows Server 2008 Server Core での GUI 機能には制限があります。GUI での依存関係のために、次の Client Automation エージェント オプションがサポートされていません。

- Remote Control チャット
- Remote Control ビューア
- Software Catalog
- Systray

IE での依存関係

Windows Server 2008 Server Core は IE の依存関係のために、HTML ベースのインストーラをサポートしません。

Client Automation エージェントをインストールするには、以下のいずれかを行います。

- インストール メディアで、WindowsProductFiles ディレクトリに移動し、`setup.exe` を実行します。
- DSM エクスプローラから、DMDeploy を使用してエージェント プラグインを展開します。

エージェントのアンインストール

Windows Server 2008 サーバ コアでは、「プログラムの追加と削除」はサポートされません。エージェントをアンインストールするには、コマンドラインから `msiexec` を実行します。

`msiexec` の使用の詳細については、「[インストール ツール msiexec \(P. 193\)](#)」のセクションを参照してください。

サポートされないオプション

Windows Server 2008 サーバ コアは以下をサポートしません。

- エージェントのオンライン ヘルプ
- ログオン シールドの「ジョブの実行前にユーザを強制的にログオフ」操作モード
- 「実行前のブート レベル」および「実行後のブート レベル」プロシージャ オプションでの、ログオフ オプション

ファイアウォールおよびポートに関する注意事項

Windows XP および Red Hat などの一部のオペレーティング システムには、リモート接続の確立を不可能にするファイアウォール機能が含まれています。これらのリモート接続には、他の DSM コンポーネント（スケーラビリティ サーバなど）からの接続が含まれます。CA Client Automation が正常に機能するためには、ファイアウォールを再設定する必要があることがあります。

CA Client Automation により現在使用されているポートおよびその各コンポーネントの概要は、付録「[CA Client Automation で使用されるポート](#) (P. 593)」を参照してください。

Linux の Compatibility Library

DSM インストーラは、特定の依存ライブラリが存在することを前提としています。これらのライブラリが存在しない場合、インストール済みのコンポーネントが正常に機能しないことがあります。

以下の表では、ソフトウェア ライブラリの前提条件の詳細を示します。DSM コンポーネントをインストールする場合、Linux ホスト上にこれらのライブラリが存在している必要があります。

Linux ディストリビューション/バージョン	必要な RPM パッケージ
Red Hat 5 Enterprise Linux	glibc 2.3.3-84 compat-libstdc++ 33-3.2.3-61 64 ビット バージョンの OS 用 : ncurses 5.4-1.3 (i386) または ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) または zlib-devel 1.2.1.2-1.2 (i386)

Linux ディストリビューション/バージョン	必要な RPM パッケージ
Red Hat 5 Enterprise Linux	glibc 2.3.3-84 compat-libstdc++ 33-3.2.3-61 64 ビット バージョンの OS 用 : ncurses 5.4-1.3 (i386) または ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) または zlib-devel 1.2.1.2-1.2 (i386)
SuSE Linux Enterprise Server 10	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38

注: 必須の **Compatibility Library** および追加のシステム パッケージの詳細については、Linux サプライヤのサポート Web サイトを参照してください。

インストーラの MSI 前提条件

すべての Windows 動作環境において、Client Automation インストーラは Microsoft Windows Installer (MSI) engine 2.0 を必要とします。このバージョンが使用可能でない場合、インストール ウィザードにより、インストール ステップの前に自動的にインストールされます。MSI 2.0 にアップグレードするには、システムを再起動する必要があります。

Windows 2003 システムでは、MSI 2.0 はオペレーティング システムの一部としてインストールされているはずなので、システムの再起動はまず必要ありません。

コンポーネント	インストール先の Windows プラットフォーム	期待される MSI バージョン	ターゲット コンピュータ上に期待される MSI バージョンが存在しない場合にインストーラにより実行されるアクション
GUI	すべて	2.0	バージョン 2.0 のインストール/バージョン 2.0 へのアップグレード
マネージャ	すべて	2.0	バージョン 2.0 のインストール/バージョン 2.0 へのアップグレード
サーバ	すべて	2.0	バージョン 2.0 のインストール/バージョン 2.0 へのアップグレード
エージェント	2003	2.0	バージョン 2.0 のインストール/バージョン 2.0 へのアップグレード

注: Software Delivery またはインフラストラクチャ展開機能を使用してエージェントをインストールする場合は、Microsoft Windows インストーラがターゲットコンピュータ上にインストールされていることを確認する必要があります。必要に応じて、Microsoft の Web サイト (www.microsoft.com) から Microsoft Windows インストーラをダウンロードすることができます。

CA Service Desk Manager と Client Automation 間での MDB の共有

CA Service Desk Manager と Client Automation の間で同じ MDB の共有を計画している場合は、まず CA Service Desk Manager をインストールし、次に Client Automation をインストールする必要があります。

Windows への管理者によるインストール

これは、Windows 動作環境のみに適用される手動のインストール オプションです。管理者によるインストールでは、Microsoft Windows インストーラ機能によりインストールイメージの内容が展開され、展開されたイメージがネットワーク共有にコピーされます。

Windows でのインストール ディレクトリ

Windows 環境におけるインストール ディレクトリの構造と、それに適用されるルールおよび制限事項について、以下に説明します。

デフォルトのベース パス

C:\Program Files\CA\DSM

プロンプトが表示されたら、デフォルトのベース パスを変更することができます。

共有コンポーネント パス

共有コンポーネントは、さまざまなディレクトリにインストールされています。デフォルトでは、Windows インストーラにより、各共有コンポーネントのディレクトリがベースパスの下に作成されます。

C:\Program Files\CA\SC

プロンプトが表示されたら、デフォルトのベースパスを変更することができます。

PATH 環境変数

インストール中、PATH 環境変数は、以下のパスを使用して拡張されます。

`basepath¥bin`

ただし、以下の場合は、インストール中に PATH 環境変数が自動的に更新されないことがあります。

ターミナル サーバセッションを介してインストールする場合、PATH 変数の変更は、以下のいずれかのアクションの完了後に初めて有効になります。

- システムからのログオフおよび再ログイン
- システムを再起動します

この動作は Microsoft オペレーティング システムに起因するもので、変更することができません。

この結果、一部の Windows システムでは、PATH 変数の変更が検出されるまでアプリケーション フレームワーク (CAF) コマンドライン インターフェイスを使用することができません。

PATH 変数の最大長は、使用している Windows 動作環境によって決まります。インストール中に、PATH 変数の実際の長さが確認されます。長さの制限によってディレクトリ名を追加できない場合、インストール処理は停止します。

Linux および UNIX でのインストール ディレクトリ

Linux および UNIX 環境における Client Automation のインストール ディレクトリの構造と、それに適用されるルールおよび制限事項について、以下に説明します。

デフォルトのベース パス

デフォルトの Client Automation インストール ディレクトリは以下のとおりです。

`/opt/CA/DSM`

Client Automation インストール ディレクトリは、環境変数 `$CA_DSM_BASEDIR` によっても参照されます。

プロンプトが表示されたら、デフォルトのベース パスを変更することができます。

共有コンポーネントパス

共有コンポーネントは、さまざまなディレクトリにインストールされています。デフォルトでは、**Windows** インストーラにより、各共有コンポーネントのディレクトリがベースパスの下に作成されます。

`/opt/CA/SharedComponents`

共通コンポーネントの場所は、環境変数 `$CASHCOMP` によっても参照されます。これはインストーラによって設定されます。

注: `$CASHCOMP` は、コンピュータ上のすべての **CA** 製品により共有されます。(以前に別の **CA** 製品をインストールしたことで) この値がすでに設定されている場合、**Client Automation** インストールで値を変更することはできません。インストーラでは既存の設定が保持されます。

PATH 環境変数

インストール終了時に、システム全体の **PATH** 環境変数を更新するかどうかを指定することができます。更新しないように指定した場合も、インストール後に、**Client Automation** の正常な動作に必要な他の環境変数と同様に、このパスを手動で設定することができます。

Bourne/Korn/bash シェルでこれを設定するには、以下のコマンドを実行します。

```
# . $CA_DSM_BASEDIR/scripts/dsmenv
```

C シェルで環境を設定するには、以下のコマンドを実行します。

```
# source $CA_DSM_BASEDIR/scripts/dsmenvcsh
```

Alert Collector のインストール

展開時に Alert Collector を実行する必要があるルールを設定できます。Alert Collector を以下のいずれかのルールに設定します。

MDB への永続アラート

MDB へのアラートを継続するように Alert Collector を設定します。

MDB への永続アラートおよび設定されたアクションの実行

MDB へのアラートを継続し、設定されたアクション（メールの送信、SNMP トラップの生成、Windows/CCS イベント ログへの書き込みなど）を実行するように Alert Collector を設定します。

Persist Alerts, Take Configured Actions, and Forward

アラートを MDB に継続して送信するように Alert Collector を設定し、設定済みアクションを実行し、アラートを別の Alert Collector へ転送します。

転送

別の Alert Collector にアラートを転送するように Alert Collector を設定します。

DM/EM 上のマネージャ MDB に接続する EM、DM、またはスタンドアロンマシンに Alert Collector をインストールします。また、[アラートの転送] ロールのスタンドアロンマシンにインストールすることもできます。

以下のセクションでは、設定に基づいて選択できるルールについて説明します。

エンタープライズ マネージャまたは EM に接続するスタンドアロン サーバの場合

[MDB への永続アラート] を選択します。EM については、他のルールはサポートされません。

ドメイン マネージャまたは DM に接続するスタンドアロン サーバの場合

[MDB への永続アラートおよび設定されたアクションの実行] または [MDB への永続アラート。設定済みアクションを実行し、それを転送] を選択します。アラートが EM に転送されるように DM が EM にリンクされている場合は、後者のルールを選択してください。MDB へのアラートの継続または EM 上の Alert Collector へのアラートの転送のみが必要な場合は、他のルールを選択します。

スタンドアロン サーバ(DM または EM に接続しない)

アラートを別の Alert Collector に送信するには、[転送] を選択します。たとえば、ENC 環境で、アラートが DM 上の Alert Collector に転送されるように、DMZ に存在する ENC サーバに Alert Collector をインストールします。

デフォルトでは、Alert Collector を DM、EM（存在する場合）またはマネージャ上の MDB に接続された個別のサーバ マシンに直接インストールできます。増加する負荷に対応するには、以下の手順に従います。

- 追加の Alert Collector サーバを導入し、各サーバが DM 上の Alert Collector に転送するようにします。
- IIS 上の DSM_WebService_HM アプリケーション プールのワーカ プロセスの数を増やします。

コンピュータ名、ユーザ名、およびディレクトリ名の制限事項

コンピュータ名、ディレクトリ名、およびユーザ名は、Client Automation がインストールされているオペレーティング システムに対して有効であり、また、以下のセクションで指定されている制限事項に準拠している必要があります。

- [コンピュータ名の制限事項](#) (P. 182)
- [ユーザ名の制限事項](#) (P. 183)
- [ディレクトリ名の制限事項](#) (P. 183)

コンピュータ名の制限事項

コンピュータ名には、以下の ASCII 文字のみを含める必要があります。

- 英数字
- ハイフン (-)

コンピュータ名は、ハイフンで始めることはできません。

重要: ローカライズされたホスト名、つまり米国英語以外（非 ENU）の言語ロケールによるホスト名をサポートするには、基礎となるドメイン ネーム システム（DNS）インフラストラクチャが、DNS 内で UTF-8 文字エンコードをサポートしている必要があります。

ユーザ名の制限事項

ユーザ名には、以下の ASCII 文字のみを含める必要があります。

- 英数字
- アット @
- ポンド #
- ドル \$
- アンダースコア _

ユーザ名を @、#、\$、または数字で始めることはできません。

ディレクトリ名の制限事項

ディレクトリ名は以下のいずれかで始まる必要があります。

- ASCII 文字 (a ~ z および A ~ Z)
- 数字 0 ~ 9
- アンダースコア _

続けて以下を指定できます。

- ASCII 文字
- 数字
- ハイフン (-)
- アンダースコア (_)
- ピリオド .
- チルダ ~

一般に、パス名では大文字小文字を区別しないことをお勧めします。

Windows に固有の注意事項

- 絶対ディレクトリ名は、ドライブ指定（ドライブ文字とその直後に続くコロン）で開始し、続いて円記号 ¥、相対ディレクトリ パスの順に指定します。UNC パスは許可されません。
- 丸かっこ (および) は、ディレクトリ名の最初の文字の後に使用できますが、マネージャインストール時には、丸かっこ (および) とハイフン - をディレクトリ名で使用することはできません。
- スペースは、ディレクトリ名の最初の文字の後に使用できます。
- 大文字と小文字は区別されません（たとえば、A は a と同じです）。
- Windows では、イメージの場所に UNC パス名を使用して、ローカルまたはリモートの MDB を使用するマネージャをインストールすることはできません。イメージの場所がリモートシステム上である場合は、その場所を Windows 共有としてアクセスできるようにする必要があります。また、パス名に @ を含めることはできません。

Linux および UNIX に固有の注意事項

- 絶対ディレクトリ パスはスラッシュ (/) で開始し、続けて相対ディレクトリ パスを指定します。相対ディレクトリ パスには、スラッシュで区切った複数のディレクトリ名を含めます。
- 大文字と小文字は区別されます（たとえば、A は a と同じではありません）。
- 空白文字（たとえば、スペース、タブ文字など）は、インストールディレクトリ パスには使用できません。

インストール ウィザードを使用したインタラクティブ インストール

Client Automation インストール ウィザードでは、すべてのソフトウェア コンポーネントおよび一部の前提条件のインストール全体が管理されます。欠落している前提条件がある場合、インストーラによりエラー メッセージが表示されます。

インストール前のディスク領域の確認

セットアッププログラムにより、選択したコンポーネントのインストールに必要なディスク領域が評価されます。インストールは、使用可能なディスク領域が充分にある場合のみ続行されます。

ただし、通常はデータ格納のために大量の追加ディスク領域が必要とされます。

各コンポーネントのインタラクティブ インストール

1 つまたは複数のコンポーネントを既存の Client Automation に個別にインストールするには、以下の手順に従います。

1. インストール ウィザードを実行し、[CA ITCM のインストール] オプションを選択します。

既存のインストールが検出された場合、[インストール オプションの選択] ダイアログ ボックスが表示されます。

[インストールの変更] オプションを選択し、インストール ウィザードの指示に従います。

2. すべての使用可能な機能が表示される [コンポーネントおよび機能の選択] ダイアログ ボックスで、インストールする機能を選択します。

注: すでにインストールされている機能は、選択状態になっています。既存の機能の選択を解除すると、この機能は削除されます。

3. インストール ウィザードの以降のダイアログ ボックスの指示に従って、インストールおよび設定に必要な情報を入力します。

インストール サマリ

インストール中、インストーラにより、セットアッププログラムの呼び出し後に実行されたすべてのステップに関する情報が収集されます。インストール サマリには、ユーザがインストールを選択したコンポーネントのリストが示されます。このサマリは、インストールの開始前にユーザに表示されます。

Windows では、インストールの完了後、インストール サマリは **DSMSummary.txt** という名前のテキスト ファイルとしても使用可能です。インストール サマリ テキスト ファイルは、**%temp%** 環境変数によって指定されたディレクトリの下に格納されます。

Linux および **UNIX** では、インストール サマリはメイン インストール ログ ファイル内に格納されます。デフォルトでは以下のファイルです。

`/opt/CA/installer/log/ca-dsm.install.log`

インストールのロールバック

セットアッププログラムにより呼び出されたいずれかのコンポーネントのインストールが失敗した場合、または完了できなかった場合、このパッケージと、インストール セッションの一部としてインストールされている他のパッケージに対してロールバックが実行され、システムが一貫性のある状態にリストアされます。

インストール パッケージのコピー

セットアッププログラムは、インストール メディア (DVD) からローカル システムまたはソフトウェア パッケージ ライブラリに、選択された機能に実際に必要なパッケージのみをコピーすることにより、ディスク領域の使用率を最適化します。以下の 2 つの場合を考えてください。

- インストールでインフラストラクチャ展開機能が選択されている場合は、エージェントおよびサーバのインストール パッケージがインストール メディアからローカル システムにコピーされます。
- **Software Delivery** マネージャ機能をインストールする場合は、**DSM** エクスプローラおよびマネージャを含むすべてのインストール パッケージがソフトウェア パッケージ ライブラリの **AUTOREG** フォルダにコピーされます。

この 2 つの場合は、選択した機能に必要なパッケージのみが、ローカル システムおよびソフトウェア パッケージ ライブラリにコピーされます。すべての機能が選択されている場合は、すべてのパッケージがコピーされます。ソフトウェア配布機能のみが選択されている場合は、ソフトウェア配布に必要なパッケージのみがコピーされます。

CCS に関する考慮事項

DSM マネージャ セットアップは、**CA Common Services (CCS)** の適切なバージョン (**Micro-CCS** またはフル **CCS** のどちらか) を自動的に選択します。アプリケーションは、その **MDB** が **Oracle** 上に存在する場合に **DSM** マネージャと共に **Micro-CCS** をインストールします。フル **CCS** は、**Microsoft SQL Server MDB** と共にインストールされます。

DSM マネージャをアップグレードすると、**DSM** マネージャ セットアップは、フル **CCS** または **Micro-CCS** のどちらかを適切にアップグレードしようとします。

〔**CCS** のインストール〕 オプションは、**Client Automation** インストール ウィザードの最上位レベルから引き続き使用できます。完全な **CCS** がローカル コンピュータにインストールされます。このオプションでは、**MDB** がプリインストールされた状態で **Microsoft SQL Server** が後者に必要です。

ただしこのリリースでは、**Client Automation** インストール ウィザードの最上位レベルから 〔**CCS** のインストール (**MDB** を含む)〕 オプションが削除されています。

Windows での CA Client Automation のインタラクティブ インストール

最初に「前提条件の確認」オプションを実行して、インストール開始前に、関連する前提条件ソフトウェアが存在していることを確認することをお勧めします。ここで「CCS の注意事項」を参照してください。

Client Automation をインタラクティブにインストールするには、以下の手順を実行する必要があります。

- 管理者としてシステムにログオンします。
- インストール DVD をマウントするか、セットアップ コマンドを実行するかして、インストール ウィザードを開きます。
- インストール ウィザードの指示に従って、インストールおよび設定に必要な情報を入力してください。インストール ウィザードでは、役に立つ説明とヒントがインストール画面に表示されます。
- インストール ウィザードの最初のダイアログ ボックスでは、インストール時に使用する言語が選択できます。

インストール ウィザードの[ようこそ]画面には、以下のオプションがあります。

Client Automation のインストール

使用許諾契約書に同意した上で、インストールする製品機能を選択することができます。

MDB のインストール

CCS (CA Common Services) コンポーネントなしで管理データベース (MDB) を専用ホストにインストールできます。この MDB は、それを必要とするすべてのコンポーネントによってリモートにアクセスされます。このインストール オプションは、マネージャが CCS 機能を使用できないようにします。

CCS のインストール

対話式の CCS インストールを起動します。

MDB を含む CCS のインストール

管理データベース (MDB) を含む CCS インストールを起動します。DSM マネージャを CCS 機能と共に使用する場合は、このオプションを選択する必要があります。

前提条件の確認

ホスト環境を確認して、製品インストールを正常に実行できるかどうかを判別します。欠落している外部の前提条件があるかどうかはアプリケーションによって通知されます。**Client Automation** インストールを続行する前に、必要なソフトウェアをインストールする必要があります。

ドキュメントの表示

PDF 形式で使用可能なドキュメント ファイルのリストが示されます。これらのファイルは、**Acrobat Reader** を使用して読み取ることができます。

お問い合わせ

CA Technologies の公式な住所、Web アドレス、電子メール アドレス、電話番号、および Fax 番号が表示されます。

Linux および UNIX での対話式インストール

Linux または UNIX に **CA Client Automation** をインタラクティブにインストールするための処理は、以下のとおりです。

1. Linux または UNIX コンピュータにユーザ **root** としてログオンします。
2. インストール DVD をマウントし、DVD のルートに移動して以下のスクリプトを実行します。

```
# sh ./setup.sh
```

インストール ウィザードが起動されます。コンポーネントのインストール先のディレクトリの詳細を指定したことを確認します。

3. インストール ウィザードの指示に従って、インストールおよび設定に必要な情報を入力してください。

最初のダイアログ ボックスでは、インストール時に使用する言語が選択できます。

後続の [ようこそ] ダイアログ ボックスでは、以下のオプションを使用できます。

DSM のインストール

使用許諾契約書に同意した上で、インストールする製品機能を選択することができます。

ドキュメントの表示

PDF 形式で使用可能なドキュメント ファイルのリストが示されます。これらのファイルは、**Acrobat Reader** を使用して読み取ることができます。

お問い合わせ

CA Technologies の公式な住所、Web アドレス、電子メール アドレス、電話番号、および Fax 番号が表示されます。

[DSM のインストール] オプションを選択すると、インストール ウィザードでは、最初に [エンド ユーザ使用許諾契約 (EULA)] ダイアログ ボックスに移動します。使用許諾契約に同意すると、以下の機能を任意に組み合わせて選択しインストールすることができます。

- Asset Management
- Remote Control
- Software Delivery

製品のライセンスを未購入であっても、任意またはすべての機能をインストールし、使用期間の間その機能を実行できます。

インストール ウィザードの後続のダイアログ ボックスでは、インストール方法を選択するように求められます。

注: デフォルトでは、Linux および UNIX でのインストール ウィザードは Java グラフィカル ユーザ インターフェイス (GUI) です。グラフィカル ユーザ インターフェイスを表示できない場合 (たとえば文字ベースのコンソールからインストールする場合など)、インストール ウィザードには VT100 形式の (キャラクターベースの) ユーザ インターフェイスが備わっています。

コマンドラインを使用した Client Automation のインストール (Windows)

以下のセクションでは、コマンドラインを使用して Windows への Client Automation インストールを実行および制御する場合に使用できる、ツール、インストール パッケージ、およびインストール オプションについて説明します。

Windows 用のパッケージのインストール

CA Client Automation は、ネットワークの配信とインストールを効率的に行い、エージェント展開の際のネットワーク トラフィックを低減できるように、MSI パッケージのセットとして構成されています。

マスタ セットアップにはすべてのインストーラ ダイアログ ボックスが含まれます。これにより、サイレント モードで他のパッケージを呼び出すために必要な情報が収集され、必要に応じてロールバックが管理されます。他のパッケージはすべて、特定のコンポーネントに必要なファイルおよびリソースをインストールします。

DSM コンポーネントの内部前提条件となっているサードパーティの製品は、別個の MSI パッケージから自動的にインストールされます。

MSI インストール パッケージは、以下の場所のインストール メディアに搭載されています (*component* は、マネージャやエクスプローラなどを表します)。

...¥WindowsProductFiles_x86¥*component*

Windows 用のパッケージのインストール

以下の表は、CA Client Automation に利用できるインストール パッケージの概要、それらのファイル名、および Windows のコントロール パネル内の [アプリケーションの追加と削除] アプレットによって表示される名前を示しています。

インストール パッケージは、CA Client Automation インストール DVD の WindowsProductFiles_x86 フォルダに含まれています。

パッケージ	ファイル名	Windows の[アプリケーションの追加と削除]リスト内の名前
マスタ セット アップ	setup.exe	CA Client Automation
エクスプローラ	Explorer.msi	CA DSM エクスプローラ
マネージャ	Manager.msi	CA DSM マネージャ
サーバ	Server.msi	CA DMS スケーラビリティ サーバ
Base Agent	AgtBHW.msi	CA DMS エージェント + 基本インベントリ プラグイン
AM エージェント	AgtAM.msi	CA DMS エージェント + Asset Management プラグイン
DTS エージェント	AgtDTS.msi	CA DMS エージェント + Data Transport プラグイン

パッケージ	ファイル名	Windows の[アプリケーションの追加と削除]リスト内の名前
RC エージェント	AgtRC.msi	CA DMS エージェント + Remote Control プラグイン
SD エージェント	AgtSD.msi	CA DMS エージェント + Software Delivery プラグイン
マニュアル	Documentation.msi	CA DSM ドキュメント
DMPPrimer	dmsetup.exe	CA DSM DMPPrimer
ENC サーバ	ServerENC.msi	CA ENC サーバ
RVI	RVI.msi	CA DSM リモート仮想化インベントリ

サードパーティのインストール パッケージ

以下の表は、個別の DSM コンポーネントが必要とするサードパーティ製のインストールパッケージの概要、それらのファイル名、およびそれらの目的の説明を示します。サードパーティ製品のバージョンとリリースの詳細については、Client Automation マニュアル選択メニューにある TPLA を参照してください。

パッケージ	ファイル名	説明
AMS 12.8	setupwin32.exe	Asset Maintenance System の CA コンポーネント。Web サービスで必須。
CCS r11.2	setup.exe	CA Common Services の CA Technologies コンポーネント。マネージャのインストールで必須。
MDAC	mdac_typ.exe	Microsoft Data Access パッケージ。マネージャのデータベースアクセスに必要。
Apache Tomcat 7.0.40		Apache Tomcat installation. Web コンソールで必須。
CA SSA 3.2.0	CA Secure Socket Adapter_NoEtpki.msi	CA 安全なソケットアダプタ。
CAPKI 4.3.0	Setup.exe	CA PKI ライブラリ

setup.exe を使用した CA Client Automation のインストール

コマンドラインから CA Client Automation をインストールまたは設定するには、インストールメディア (DVD) の `WindowsProductFiles_x86` ディレクトリから `setup.exe` を実行して、インストールを開始する必要があります。

`setup.exe` プログラムを実行する際は、以下のオプションを設定することができます。

`/a`

管理者によるインストールを開始します。これにより、すべての DSM コンポーネントおよびファイルがネットワーク共有に展開されます。

注: このパラメータは、製品ファイルディレクトリの下でセットアップを実行した場合のみ機能します。インストールメディアのルートディレクトリでセットアップを実行した場合には機能しません。

`/V"/! *v x:¥DSMSetupxxx.log"`

ログファイルパスを指定します。ログファイル名は静的であり、変更することができません。

インストール ツール `msiexec`

MSI インストールパッケージでは、コマンドラインインターフェースがサポートされています。コマンドラインインターフェースは、カスタム構築した DVD または CD など、別の方法で DSM 機能をリモートシステムに展開する場合、または Client Automation 機能をホスト展開イメージ内に構築する場合に使用することができます。

Microsoft Windows インストーラ (MSI) により、`.msi` というファイル拡張子を持つパッケージファイルからソフトウェアがインストールされます。

`msiexec.exe` は、コマンドラインから MSI パッケージをインストールする際に使用できる実行可能コマンドです。`msiexec` は、数多くのコマンドラインオプションを備えた非常に柔軟性の高いツールです。`msiexec` のオプションおよびパラメータの詳細については、Microsoft のオンラインヘルプを参照してください。

すべての MSI パッケージで、汎用オプションがサポートされています。また、一部の MSI パッケージでは、パッケージに固有のオプションがサポートされています。この 2 つのオプションセットを使用することで、特定のアプリケーションをインストールする詳細な方法を制御することができます。

汎用オプション (/i、-l*v、/qn) およびマネージャ パッケージに固有のインストール オプション ADDLOCAL を使用する msexec コマンドの例を、以下に示します。

```
msiexec /i "x:%WindowsProductFiles_x86%Manager%Manager.msi" -l*v  
"c:%DSMSetupMgr.log" ADDLOCAL=Manager,MgrDC,MgrAM ALLUSERS=1 /qn
```

汎用オプションおよびパッケージに固有のオプションの詳細については、[msiexec の汎用オプション](#) (P. 194)および[パッケージ固有の MSI プロパティ](#) (P. 196)を参照してください。

注: エージェント パッケージに固有のオプションは、インタラクティブな展開で使用されるインストールパラメータのオプションであり、展開ウィザードの [エージェントの設定] ページで [追加の Windows インストール オプション] を指定します。このページでは、複数のインストール オプションをスペースで区切って入力し、既存のオプションを上書きできます。

重要: MSI コマンドライン msiexec を使用して DSM コンポーネントを直接インストールする場合は、MSI インストールプロパティ ALLUSERS の値を 1 に設定して (つまり、すべてのユーザに対してインストールされるが、ユーザにはコンピュータの管理者としてのアクセス権限が必要)、DSM マネージャの Software Delivery または Software Deployment 機能を使用して後でアップグレード、アンインストール、または再インストールできるようにしておく必要があります。パラメータをこのように設定しなかったり、パラメータを空のままにした場合、コンポーネントは、それを最初にインストールする特定のユーザに対して登録されるため、マネージャ機能を使用して管理することができません。

システム名の指定に関する注意事項

Client Automation インストーラによってシステム名の入力を求められた場合は必ず、ドメインサフィックスを含む完全修飾ドメイン名 (FQDN) を入力することを強くお勧めします。これにより、転送リクエストが関連するすべての DNS 用に設定されていない場合でも、他のネットワーク ドメイン内のコンピュータ システムに接続することができます。

msiexec の一般オプション

すべての MSI パッケージでは、以下の一般オプションがサポートされています。

/i *msi install package*

Client Automation のインストールまたは設定

/q *n|b|r|f|+|?*

ユーザ インターフェース レベルを設定します。

オプション (組み合わせ)	ユーザ インターフェース レベル

オプション(組み合わせ)	ユーザ インターフェース レベル
q	ユーザ インターフェースなし。
qn	ユーザ インターフェースなし。
qb	標準ユーザ インターフェース。qb! を使用して、[キャンセル] ボタンを非表示にします。
qr	最小ユーザ インターフェース (インストールの最後にモーダル完了ダイアログ ボックスなし)
qf	完全ユーザ インターフェースおよび作成された FatalError、UserExit、または最後の終了モーダル ダイアログ ボックス。
qn+	最後に表示されるモーダル ダイアログ ボックスを除く、ユーザ インターフェースなし。
qb+	最後に表示されるモーダル ダイアログ ボックスありの標準ユーザ インターフェース。ユーザがインストールをキャンセルした場合は、モーダル ダイアログ ボックスは表示されません。qb+! または qb!+ を使用して、[キャンセル] ボタンを非表示にします。
qb-	標準ユーザ インターフェース(モーダル完了ダイアログ ボックスなし) /qb+? は、サポートされているユーザ インターフェース レベルでないことに注意してください。qb-! または qb!- を使用して、[キャンセル] ボタンを非表示にします。

注: ! オプションは Microsoft Windows Installer 2.0 で使用でき、標準ユーザ インターフェースでのみ機能します。完全ユーザ インターフェースと共に使用することはできません。

/! [i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] Logfile

指定されたパスでログ情報をログ ファイルに書き込みます。フラグによって、ログ記録する報を指定します。フラグを指定しなかった場合のデフォルトは、iwearmo です。

フラグ	ログ記録する情報
i	ステータス メッセージ
w	非致命的警告
e	すべてのエラー メッセージ
a	アクションの開始

フラグ	ログ記録する情報
r	アクション固有の記録
u	ユーザ リクエスト
c	初期ユーザ インターフェース パラメータ
m	メモリ不足または致命的な終了情報
o	ディスクの空き容量が不足しているメッセージ
p	端末のプロパティ
v	履歴の出力
x	デバッグの詳細情報 Windows Server 2003 でのみ使用可能
+	既存ファイルに追加
!	各行をログにフラッシュ
*	ワイルドカード。v および x オプションを除く、すべての情報のログ記録。v および x オプションを含めるには、/!*vx を指定します。

パッケージ固有の MSI プロパティ

以下の DSM コンポーネントの MSI インストール パッケージおよびプラグインでは、パッケージ固有のインストール プロパティがサポートされています。

- DSM エクスプローラ
- 基本インベントリ エージェント
- Asset Management エージェント
- Data Transport Service エージェント
- Remote Control エージェント
- Software Delivery エージェント
- スケーラビリティ サーバ
- マネージャ
- ENC ゲートウェイ サーバ

注: ソフトウェア ジョブでは、ユーザ パラメータとしてパッケージ固有の MSI プロパティを指定する必要があります。ユーザ パラメータの詳細については、「DSM エクスプローラ ヘルプ」の「Software Delivery」にある「ジョブ タブ」を参照してください。

MSI パッケージをインストールするための前提条件

MSI パッケージをインストールする前に、ETPKI ライブラリおよび CA 安全なソケットアダプタをインストールする必要があります。これらの前提条件で必要とされるバージョンについては、「[サードパーティのインストールパッケージ \(P. 192\)](#)」を参照してください。

■ CAPKI のインストール :

CAPKI のセットアップは、CA Client Automation のインストールメディア (CD/DVD) の WindowsProductFiles_x86¥CAPKI ディレクトリにあります。

CAPKI ライブラリをインストールするには、以下のコマンドラインを使用します。

```
setup install caller=CADSMCAPKI
```

■ CA 安全なソケットアダプタのインストール :

CA 安全なソケットアダプタは、CA Client Automation インストールメディア (CD/DVD) の WindowsProductFiles_x86¥SSA ディレクトリにある安全なソケットアダプタのインストーラを使用してインストールできます。

CA 安全なソケットアダプタをインストールするには、以下のコマンドラインを使用します。

```
msiexec.exe
/i"D:¥WindowsProductFiles_x86¥SSA¥CASockAdapterSetupWin32NoEtpki.msi" /l*v
"C:¥DOCUME~1¥ADMINI~1¥LOCALS~1¥Temp¥DSMSSetupSSA.log" /qb-!
```

エクスプローラ パッケージの MSI プロパティ

DSM エクスプローラ (Explorer.msi) の MSI インストールパッケージでは、以下のパッケージ固有のプロパティがサポートされています。

ADDLOCAL

個別にインストール可能な機能です。

値	説明
エクスプローラ	エクスプローラの共通コンポーネント (エクスプローラのインストールには必須です)
ExpAM	Asset Management プラグイン
ExpRC	Remote Control 共通プラグイン
ExpSD	Software Delivery 共通プラグイン

値	説明
ExpSDB	ブート マネージャ プラグイン
ExpSDM	Software Delivery マネージャ クライアント API
ExpRP	Reporter プラグイン
ALL	上記の機能をすべて選択。

ADMINCONSOLE_MANAGER

DSM エクスプローラの接続先のマネージャ システムです。

値：システム名または IP アドレス

基本インベントリ エージェント パッケージの MSI プロパティ

基本インベントリ エージェント プラグイン (AgtBHW.msi) および ENC クライアントの MSI インストール パッケージでは、以下のパッケージ固有のプロパティがサポートされています。

AGENT_SERVER

エージェントの接続先のスケーラビリティ サーバです。

値：システム名または IP アドレス

AGENT_DEFAULTGROUPS

エージェントが自動的に登録するマネージャで作成されるグループまたは管理グループのリストです。

値：グループ名のカンマ区切りのリスト

例：Grp1/subgroup1,Group2,...

ENC_CLIENT_ENABLED

基本ハードウェア インベントリがインストールされた際に、ENC クライアントを有効にするかどうかを指定します。デフォルトでは、クライアント ファイルはコンピュータにコピーされますが、実行はされていません。これにより、インストーラが簡素化され、必要に応じて後ほどクライアントを有効化する簡単な設定ジョブが利用できます。

値：0 (非アクティブのまま)、1 (アクティブ化)

注: 以下のパラメータは、ENC クライアントが有効でない場合は指定する必要はありません。

ENC_SVR_ADDR

このクライアントが接続する **NC** ゲートウェイ サーバ。

値: サーバの **FQN**。

ENC_SVR_TCP_PORT

ENC ゲートウェイ サーバ上の接続先となる **TCP** ポート。

デフォルト: 443

ENC_SVR_HTTP_PORT

ENC ゲートウェイ サーバ上の接続先となる **HTTP** ポート。

デフォルト: 80

ENC_HTTP_PROXY_ADDR

ローカル ネットワーク外で接続するために **ENC** クライアントが接続する必要のある **HTTP** インターネット プロキシのアドレス。

ENC_HTTP_PROXY_PORT

接続先となるプロキシ上のポート番号。

デフォルト: 8080

ENC_PROXY_ORDER

ENC クライアントが試行する接続タイプのセット。省略すると、デフォルトの順序が使用されます。

値: これは、**socket**、**socks4Anon**、**socks5Auth**、**socks5Anon**、**httpConnect**、**http**、および **httpProxy** のキーワードをゼロ以上並べた、スペース区切りのリストです。

ENC_SOCKS_ADDR

ローカル ネットワーク外で接続するために **ENC** クライアントが接続する必要のある **SOCKS** インターネット プロキシのアドレス。

値: サーバの **FQN** または **IP** アドレス

ENC_SOCKS_PORT

接続先となるプロキシ上のポート番号。

デフォルト: 1080

ENC SOCKS_USER

SOCKS サーバへの接続時に認証するユーザ名。

例: socksuser

ENC SOCKS_PW

ENC SOCKS_USER で指定したユーザの平文のパスワード。

ENC HTTP_PROXY_USER

HTTP サーバへの接続時に認証するユーザ名。

例: httpuser

ENC HTTP_PROXY_PW

ENC HTTP_PROXY_USER で指定したユーザの平文のパスワード。

注: ENC プロパティの詳細については、「*encUtilCmd* コマンドリファレンス」を参照してください。また、「*DSM* エクスプローラヘルプ」の「設定ポリシー」にある「ENC ゲートウェイ ポリシー グループ」のトピックを参照してください。

Asset Management エージェント パッケージの MSI プロパティ

Asset Management エージェント プラグイン (AgtAM.msi) の MSI インストールパッケージでは、以下のパッケージ固有のプロパティがサポートされています。

AGENT_SERVER

エージェントの接続先のスケーラビリティ サーバです。

値: システム名または IP アドレス

AGENT_DEFAULTGROUPS

エージェントが自動的に登録するマネージャで作成されるグループまたは管理グループのリストです。

値: グループ名のカンマ区切りのリスト

例: Grp1/subgroup1,Group2,...

Data Transport Service エージェント パッケージの MSI プロパティ

Data Transport Service (DTS) エージェント プラグイン (AgtDTS.msi) の MSI インストール パッケージでは、以下のパッケージ固有のプロパティがサポートされています。

SC_DSMPROP

[エージェント プロパティ] ダイアログ ボックスへのショートカット

値	説明
1	[エージェント プロパティ] ダイアログ ボックスへのショートカットは、[スタート] メニューに導入されます。
0	ショートカットは作成されません。

ADDLOCAL

個別にインストール可能な機能です。

値	説明
エージェント	エージェントの共通部分 (エージェントのインストールには必須です)
AgtDTS	Data Transport Service エージェントの共通部分 (DTS エージェントのインストールには必須です)
ALL	上記の機能をすべて選択。

AGENT_DEFAULTGROUPS

エージェントが自動的に登録するマネージャで作成されるグループまたは管理グループのリストです。

値：グループ名のカンマ区切りのリスト

例：Grp1/subgroup1,Group2,...

Remote Control エージェント パッケージの MSI プロパティ

Remote Control エージェント プラグイン (AgtRC.msi) の MSI インストール パッケージでは、以下のパッケージ固有のプロパティがサポートされています。

SC_DSMPROP

[エージェント プロパティ] ダイアログ ボックスへのショートカット

値	説明
1	[エージェント プロパティ] ダイアログ ボックスへのショートカットは、[スタート] メニューに導入されます。
0	ショートカットは作成されません。

ADDLOCAL

個別にインストール可能な機能です。

値	説明
エージェント	エージェントの共通部分 (エージェントのインストールには必須です)
AgtRC	Remote Control エージェントの共通部分 (Remote Control エージェントのインストールには必須です)
AgtRCA	Remote Control ホスト
AgtRCV	Remote Control ビューア
AgtRCP	Remote Control リプレイア
ALL	上記の機能をすべて選択。

AGENT_SERVER

エージェントの接続先のスケラビリティ サーバです。

値: システム名または IP アドレス

RC_AGENT_STANDALONE

値	説明

値	説明
0	Remote Control エージェントは集中管理されています。
1	Remote Control エージェントはスタンドアロンです。

AGENT_DEFAULTGROUPS

エージェントが自動的に登録するマネージャで作成されるグループまたは管理グループのリストです。

値：グループ名のカンマ区切りのリスト

例：Grp1/subgroup1,Group2,...

Software Delivery エージェント パッケージの MSI プロパティ

Software Delivery エージェント プラグイン (AgtSD.msi) の MSI インストールパッケージでは、以下のパッケージ固有のプロパティがサポートされています。

SC_DSMPROP

[エージェント プロパティ] ダイアログ ボックスへのショートカット

値	説明
1	[エージェント プロパティ] ダイアログ ボックスへのショートカットは、[スタート] メニューに導入されます。
0	ショートカットは作成されません。

ADDLOCAL

個別にインストール可能な機能です。

値	説明
エージェント	エージェントの共通コンポーネント (エージェントのインストールには必須です)
AgtSD	Software Delivery エージェントの共通コンポーネント (Software Delivery エージェントのインストールには必須です)
AgtSDA	Software Delivery コンポーネント (SD カタログには必須です)

値	説明
AgtSDC	Software Delivery カタログ コンポーネント
ALL	上記の機能をすべて選択。

AGENT_SERVER

エージェントの接続先のスケーラビリティ サーバです。

値：システム名または IP アドレス

AGENT_DEFAULTGROUPS

エージェントが自動的に登録するマネージャで作成されるグループまたは管理グループのリストです。

値：グループ名のカンマ区切りのリスト

例：Grp1/subgroup1,Group2,...

スケーラビリティ サーバ パッケージの MSI プロパティ

スケーラビリティ サーバ (Server.msi) の MSI インストールパッケージでは、以下のパッケージ固有のプロパティがサポートされています。

FIPS_MODE

Client Automation インストーラによって設定される FIPS モードを定義します。

値	説明
1	FIPS 推奨
2	FIPS のみ

ADDLOCAL

個別にインストール可能な機能です。

値	説明
サーバ	スケーラビリティ サーバの共通コンポーネント (サーバのインストールには必須です)

値	説明
SrvAM	Asset Management スケーラビリティ サーバプラグイン
SrvSD	Software Delivery スケーラビリティ サーバプラグイン
SrvRC	Remote Control スケーラビリティ サーバプラグイン
ALL	上記の機能をすべて選択。

SRV_SDBPATH

スケーラビリティ サーバ データベースをインストールするディレクトリ パスです。

SERVER_PATH

スケーラビリティ サーバ固有データをインストールするディレクトリ パスです。

SERVER_MANAGER

スケーラビリティ サーバの接続先のマネージャ システムです。

値： システム名または IP アドレス

SERVER_ENGINE

スケーラビリティ サーバの接続先のエンジン システムです。 このパラメータが指定されていない場合は、デフォルトでシステム エンジンが使用されます。

値： エンジン名

BS_OS_PATH

OS イメージおよびほかのブート サーバ固有データを格納するディレクトリ パスです。 パス名は、文字列「¥SDBS¥var」で終わる必要があります。

例： f:¥Program Files¥CA¥DSM¥Server¥SDBS¥var

CREATESDMSISHARE

Software Delivery マネージャに登録されている MSI パッケージにアクセスするための共有です。

値	説明
1	MSI パッケージにアクセスするための共有を作成します。
0	共有 SERVER_ENGINE を作成しません。

CREATESDLIBSHARE

ソフトウェアパッケージライブラリに登録されているパッケージにアクセスするための共有です。

値	説明
1	パッケージにアクセスするための共有を作成します。
0	共有を作成しません。

BOOTSERVER_ENABLED

ブート サーバ サービスを有効にするかどうかを決定します。

値	説明
0	ブート サーバ サービスを有効にしません。
1	ブート サーバ サービスを有効にします。

BOOTSERVER_DISABLESHARES

ブート サーバに登録されているパッケージにアクセスするための共有です。

値	説明
0	パッケージにアクセスするための共有を作成します。
1	共有を作成しません。

マネージャ パッケージのパッケージ固有の MSI プロパティ

マネージャ (Manager.msi) の MSI インストール パッケージでは、以下のパッケージ固有のプロパティがサポートされています。

ADDLOCAL

個別にインストール可能な機能です。

値	説明
マネージャ	マネージャの共通コンポーネント (マネージャのインストールには必須です)
MgrInf	マネージャの共通インフラストラクチャ (マネージャのインストールには必須です)
MgrDC	エンジン プラグイン (マネージャのインストールには必須です)
MgrAM	Asset Management マネージャ プラグイン
MgrRC	Remote Control マネージャ プラグイン
MgrSD	Software Delivery マネージャ プラグイン
MgrDTS	Data Transport Service プラグイン (Software Delivery マネージャのインストールには必須です)
MgrDM	展開マネージャ プラグイン
MgrIP	イメージ作成マネージャ プラグイン
ALL	上記の機能をすべて選択。

DMSOFTLIBDIR

DMDeploy のパッケージをインストールするディレクトリ パスです。

DMKEYLOCATION

展開マネージャ キー ファイルのディレクトリ パスです。

SDLIBRARY

ソフトウェア パッケージ ライブラリをインストールするディレクトリ パスです。

MANAGER_ROLE

マネージャのロールです。

値	説明
0 = エンタープライズ	マネージャはエンタープライズ マネージャとして機能します。
1 = ドメイン メンバ	マネージャはエンタープライズ内でドメイン マネージャとして機能します。
2 = スタンドアロン マネージャ	マネージャはスタンドアロン ドメイン マネージャとして機能します。

ENTERPRISE_NAME

ドメイン マネージャのロール (値 = 1) が定義されている場合の、ドメイン マネージャの接続先のエンタープライズ マネージャ システムです。定義されていない場合は、このプロパティは空です。

値：システム名または IP アドレス

WAC_MANAGER

スタンドアロン Web コンソール インストール用の Web コンソール マネージャ システム。

値：システム名または IP アドレス

ENGINE_MANAGER

スタンドアロン エンジン インストール用のエンジン マネージャ システム。

値：システム名または IP アドレス

DSM_TOMCAT_PORT

ハンドラがリクエストをリスンする TCP/IP ポート。

デフォルト：8090

DSM_TOMCAT_SHUT

ハンドラがシャットダウン リクエストをリスンする TCP/IP ポート。

デフォルト：8095

DSM_TOMCAT_AJP

リクエストをプロセス外のワーカに AJPv13 プロトコルを使用して転送するために、ワーカが AJP13 リクエストをリスンするポート。

デフォルト : 8020

DB

使用するデータベースのタイプです。

値 : SQLServer または Oracle

DBSERVER

データベースの常駐しているシステム名

値 : システム名または IP アドレス

DBUSERNAME

データベース アクセス用の Windows ユーザ名です。

DBPASSWORD

DBUSERNAME のパスワードです。

DBVUSER

データベースが Ingres で、リモート データベース システムが使用されている場合は、データベース システムの Vnode です。

DBVPWD

DBVUSER のパスワードです。

DBSW

ソフトウェア検出のためのソフトウェア シグネチャが管理データベースに挿入されるか（組み込まれる）、または挿入されない（除外される）場合は、フラグを立てます。

値	説明
excl_sw	ソフトウェア シグネチャを挿入しません。
incl_sw	ソフトウェア シグネチャを挿入します。

FAILOVER_ENABLED

リカバリ サポートが有効か無効のいずれであることを示すフラグです。

値	説明
0	リカバリ サポートは無効。
1	リカバリ サポートは有効。

FAILOVER_STATUS

このマネージャがクラスタ環境内でアクティブ ノードまたはパッシブ ノードのいずれであることを示すフラグです。

値	説明
0	このマネージャはパッシブ マネージャ。
1	このマネージャはアクティブ マネージャ。

FAILOVER_CLUSTER_NAME

マネージャのクラスタ名です。

ENC ゲートウェイ サーバ パッケージの MSI プロパティ

ENC ゲートウェイ サーバの MSI インストール パッケージでは、以下のパッケージ固有のプロパティがサポートされています。

AGENT_SERVER

エージェントの接続先のスケラビリティ サーバです。

値：システム名または IP アドレス

ENC_CLIENT_ENABLED

ENC ゲートウェイ サーバがインストールされた際に、ENC クライアントを有効にするかどうかを指定します。

値：0（非アクティブのまま）、1（アクティブ化）

ENC_SERVER_TYPE

ENC ゲートウェイ サーバのロールを指定します。これは、以下の表にリストされているスペースで区切られた 1 つ以上の値である必要があります。ENC ゲートウェイ サーバは、1 つ以上のロールで動作できます。マネージャが指定されている場合、サーバも自動的に設定されます。ENC クライアントも、このサーバに登録されるように自動的に設定されます。

1 つの ENC ゲートウェイ サーバのみが設定されている場合は、クライアントもこのサーバに登録されます。

上記の 2 つの場合では、クライアントに対する設定パラメータは ENC_CLIENT_ENABLED 以外はありません。

1 つのルータのみが設定されている場合は、クライアントとルータの両方が別の ENC ゲートウェイ サーバに登録される必要があります。これは、ENC_SVR_ADDR パラメータによって設定されます。

値	説明
ENC_SRS	ENC ゲートウェイ 登録サーバとして動作するように設定します。
ENC_ROUTER	ENC ゲートウェイ ルータとして動作するように設定します。
ENC_MRS	ENC ゲートウェイ 登録マネージャとして動作するように設定します。

ENC_SVR_ADDR

ENC ゲートウェイ ルータをインストールする場合は、これは 登録先となる ENC ゲートウェイ サーバにする必要があります。

ENC ゲートウェイ 登録サーバをインストールする場合は、これは 登録先となる ENC 登録マネージャにする必要があります。

値： 登録先の ENC ゲートウェイ サーバまたはマネージャの FQN。

注： ENC ゲートウェイ マネージャをインストールする場合は、これは自動的に設定されます。

ENC_SVR_TCP_PORT

ENC ゲートウェイ マネージャ上の接続先となる TCP ポート。

デフォルト : 443

注: ENC ゲートウェイ マネージャをインストールする場合は、これは自動的に設定されます。

ENC_SVR_HTTP_PORT

ENC ゲートウェイ 登録サーバまたはルータの接続先となる ENC ゲートウェイ マネージャ上の HTTP ポート。

デフォルト : 80

注: ENC ゲートウェイ 登録 マネージャをインストールする場合は、これは自動的に設定されます。これは、ゲートウェイ サーバまたはルータに対してのみ設定が必要です。

注: ENC プロパティの詳細については、「*encUtilCmd* コマンドリファレンス」を参照してください。また、「*DSM* エクスプローラ ヘルプ」の「設定ポリシー」にある「ENC ゲートウェイ ポリシー グループ」のトピックを参照してください。

msiexec の追加プロパティ

以下のプロパティは、CA Technologies が提供する MSI インストール パッケージのすべてに共通するものです。

CA

ターゲット システム上のインストール ディレクトリ

例 : C:\Program Files\CA

CONFIGDATA_LOCATION

設定ストア (comstore) などのパッケージの設定データのインストール ディレクトリ。

デフォルト : 製品のインストール ディレクトリ。

例 : C:\Program Files\CA\DSM

SHAREDCOMPONENTS

パッケージの共有コンポーネントのインストール ディレクトリ

例 : C:\Program Files\CA\SC

注: パッケージがいったんインストールされると、これらの共通プロパティの値は、後からインストールされるほかのパッケージに対して固定されます。

各 MSI インストールパッケージに対して、さらに以下のプロパティを使用することができます。

DSM_LANGUAGE

CA Client Automation インストールの言語を指定します。指定可能な値は、**enu**（米英語）、**deu**（独語）、**fra**（仏語）および **jpn**（日本語）です。

サポートされている CA Client Automation のすべての言語バージョン用のファイルがインストールされますが、実際のインストールの言語としては **DSM_LANGUAGE** で指定されている言語が使用されます。

デフォルト：空（NULL）。この場合、インストーラはシステムのデフォルト ロケールを使用します。システムのデフォルト ロケールがサポート対象外のロケールの場合は、**enu**（米英語）が使用されます。

注：DSM_LANGUAGE は、インストール ウィザードのダイアログ ボックスの言語を指定しません。

REBOOT

値	説明
REALLYSUPPRESS	再起動が必要な場合、このプロパティによって抑制されるため、手動で再起動を実行する必要があります。

ALLUSERS

値	説明
0	特定のユーザ用にインストールします。
1	すべてのユーザ用にインストールしますが、ユーザにはコンピュータの管理者としてのアクセス権限が必要です。
2	ユーザが管理者としてアクセス権限がある場合には、すべてのユーザ用にインストールしますが、それ以外の場合は、特定のユーザ用にインストールします。

注: MSI コマンドラインを使用して DSM コンポーネントを直接インストールしている場合は、ALLUSERS=1 を設定して、マネージャの Software Delivery または Software Deployment 機能を使用して後でアップグレード、アンインストール、または再インストールを行うことができるようにする必要があります。パラメータをこのように設定しなかったり、パラメータを空のままにしたりした場合、コンポーネントは、それを最初にインストールする特定のユーザに対して登録されるため、マネージャ機能を使用して管理することができません。

ARPSYSTEMCOMPONENT

このプロパティを設定すると、Windows の [コントロールパネル] の [プログラムの追加と削除] のリストにアプリケーションが表示されません。このプロパティは、Windows 2000 および Windows XP 以前のオペレーティング環境には影響を与えません。

CAF_INSTALL_SERVICE

値	説明
0 1	システムに最初にインストールする MSI パッケージは 1 にする必要があります。それ以外の場合は、0 を指定できます。

CAF_START_SERVICE

値	説明
0 1	システムに最後にインストールする MSI パッケージでは 1 にする必要があります。それ以外の場合は、0 にする必要があります。

FIPS_MODE

値	説明
1	-FIPS 推奨モード (デフォルト) で Client Automation をインストールします
2	-FIPS のみ モードで Client Automation をインストールします

msiexec の アンインストール、修復、および管理者によるインストールのオプション

MSI コマンドライン インターフェースを使用して、以下の製品のアンインストール、修復、または管理者によってインストール タスクを開始することもできます。

/x msi_install_package | productcode

製品をアンインストールします。

/f [p|o|e|d|c|a|u|m|s|v] msi_install_package | productcode

製品を修復します。このオプションでは、コマンドラインで入力されたプロパティ値は無視されます。このオプションのデフォルトの引数リストは「omus」です。このオプションは、REINSTALLMODE プロパティと同じ引数リストを共有します。

オプション	説明
p	ファイルがない場合にのみ再インストールします。
o	ファイルがないか、または古いバージョンがインストールされている場合に、再インストールします。
e	ファイルがないか、または同等か古いバージョンがインストールされている場合に、再インストールします。
d	ファイルがないか、または異なるバージョンがインストールされている場合に、再インストールします。
c	ファイルがないか、または格納されているチェックサムが計算された値と一致しない場合に、再インストールします。ファイルテーブルの [属性] 列に msidbFileAttributesChecksum があるファイルのみ修復します。
a	すべてのファイルの再インストールを強制します。
u	すべての必要なユーザ固有のレジストリ エントリを再書き込みします。
m	すべての必要なコンピュータ固有のレジストリ エントリを再書き込みします。
s	すべての既存のショートカットを上書きします。
v	ソースから実行し、ローカル パッケージを再キャッシュします。アプリケーションまたは機能の最初のインストールには、v 再インストール オプションを使用しないでください。

```
/a msi_install_package
```

管理者によるインストール オプション。ネットにインストールできる場所から、ネットワーク共有に製品をインストールします。

msiexec オプションとプロパティの組み合わせる例

以下に、msiexec オプションとプロパティを組み合わせる例を示します。

```
msiexec.exe
/i "N:¥DSM_11_2_9999_0_DVD¥WindowsProductFiles_x86¥Manager¥Manager.msi"
/l *v "G:¥DOCUME~1¥KSYST0~1.TAN¥LOCALS~1¥Temp¥DSMSetupManager.log"
ADDLOCAL=Manager,MgrAM,MgrRC,MgrSD,MgrDC,MgrDTS,MgrDM,MgrIP
REBOOT=REALLYSUPPRESS ALLUSERS=1
CA="G:¥Program Files¥CA¥DSM¥"
CAF_INSTALL_SERVICE="1" CAF_START_SERVICE="0"
/qb-! DMSOFTLIBDIR="G:¥Program Files¥CA¥DSM¥"
SDLIBRARY="G:¥Program Files¥CA¥DSM¥SD¥ASM¥LIBRARY"
ENTERPRISE_NAME="KSYST01U"
MANAGER_ROLE="2" DB="SQLServer"
DBSERVER="KSYST01U" DBUSERNAME="ca_dsm" DBPASSWORD=XXX DBSW="excl_sw"
```

Linux または UNIX でコマンドラインを使用した Client Automation のインストール

LinuxProductFiles_x86/component の下の配信ディレクトリにある installdsm スクリプトを使用して、Linux または UNIX に、Client Automation をインストールします。

注: CADSMCMD は、Linux のみに提供され、その他の UNIX の派生製品には提供されません。詳細については、「*CLI リファレンスガイド*」を参照してください。

利便性と Windows のインストールとの整合性のために、インストール DVD のルートディレクトリに setup.sh という名前のスクリプト ファイルが用意されています。このスクリプトは、/LinuxProductFiles_x86/manager/installdsm を呼び出します。

デフォルトでは、Linux および UNIX のインストーラがインタラクティブ モードで実行されます。Client Automation がシステムにすでにインストールされている場合は、インストーラによって、アップグレード/修復、変更、またはアンインストールのオプションが示されます。

インストール メディアにも、テンプレート応答ファイルの install.rsp が含まれています。このファイルは、自動インストールを作成する場合に使用できます。

Linux または UNIX への Client Automation の installdsm スクリプト インストール

installdsm スクリプトの形式は以下のとおりです。

```
installdsm [-f | -r responsefile [/Rname=value...]] | -g responsefile ]
```

-f

既存で古い製品バージョンの可能性があるバージョンをバックアップせずに、強制的にインストールします。

-r responsefile [/Rname=value ...]

応答ファイルで指定された値を使用して、自動インストールを実行します。-r オプションを指定すると、installdsm によって応答ファイルが空ではなく、ラベルと値のペアの有効なセットが含まれていることが確認されます。/R 指定は応答ファイルで指定されたパラメータよりも優先されます。たとえば、優位に立つ各パラメータに対して、個別の /R 指定を提供します。

```
installdsm -r rsp.txt ¥  
/RITRM_AUTOSTART_INSTALL=1 ¥  
/RITRM_AUTOSTART_REBOOT=1
```

パラメータ名または値が有効かどうか、または指定されたパラメータが応答ファイルにあるかどうかは確認されません。

パラメータ設定のデフォルトリストは、Linux および UNIX の各パッケージでサンプルの応答ファイル `install.rsp` として提供されます。

対話式インストールのインストーラを使用するたびに、または自動インストールの応答ファイルを生成するために、パラメータ値を編集することができます。インストールスクリプトによってオプションを入力するプロンプトが表示された後、インストーラによりファイルが所定の場所にコピーされ、設定アクションが実行されます。

-g responsefile

応答ファイルを作成します。スクリプトによって、インタラクティブインストール用としてダイアログボックスが表示されますが、ダイアログボックスシーケンスの最後に、指定した応答ファイルに指定するプロパティ値をすべて書き込みます。

Linux および UNIX での応答ファイルの設定

Client Automation の自動インストールは、応答ファイルによって起動されます。応答ファイルは、インストールと設定を制御するパラメータ値が含まれているテキストファイルです。手動または **-g** オプションと共に **installdsm** スクリプトを使用するいずれの場合にも、応答ファイルはインストールする前に生成されます。インストール中は、応答ファイルは読み取り専用になります。

Client Automation インストールには、自動インストールを実行する場合に使用できる標準応答ファイルが含まれています。各コンポーネントのフォルダには、**install.rsp** ファイルが含まれています。このサンプル応答ファイルでは、コンポーネントの完全インストールが提供されています。

インストール プロパティ値の変更

応答ファイルには、インストールおよび初期設定を制御するパラメータ値（プロパティ）が含まれています。

ほとんどの Client Automation パラメータには、プレフィックス **CA_DSM**、**DSM_**、またはコンポーネントを示すプレフィックスがあります。ほかのパラメータは、ほかの CA 製品によって使用される可能性があります。

/R 指定と共に **installdsm** を使用して、応答ファイルのパラメータ値を上書きできます。パラメータ値を変更することによって、インフラストラクチャ展開ウィザードまたは **Software Delivery** パッケージを使用して、リモートインストールを実行するときのデフォルトのインストールの動作を変更することもできます。

応答ファイルを手動で編集する場合は、通常はほかのプロパティ値（ほとんどの場合、ディレクトリおよびサブディレクトリのロケーション）から派生するプロパティ値に注意してください。派生関係が壊れることを避けるために、以前に別のプロパティ値から派生したプロパティ値をハードコードしないでください。

例

SDLIBRARY (Software Delivery ライブラリの場所) は、デフォルトで CA_DSM_CONFIGDATA (Client Automation 設定データの場所) から派生し、CA_DSM_CONFIGDATA 自体も CA_ITRM_BASEDIR (メインの Client Automation の場所) から派生します。これらの関係は、提供される `install.rsp` 応答ファイル内で管理されます。応答ファイル内で、CA_DSM_CONFIGDATA が `CA_DSM_CONFIGDATA=/data/CA/ConfigDataLocation` としてハードコードされており、SDLIBRARY が `SDLIBRARY=/data/CA/SDLibrary` としてハードコードされている場合、CA_DSM_BASEDIR、CA_DSM_CONFIGDATA、および SDLIBRARY 間の派生関係は壊れます。

注: エージェントパッケージに固有のオプションは、インタラクティブな展開で使用するオプションであり、インフラストラクチャ展開ウィザードの [エージェントの設定] ページで [追加の UNIX インストール オプション] を指定します。このページでは、複数のインストール オプションをスペースで区切って入力し、既存のオプションを上書きできます。

基本インストール プロパティ

CA_DSM_BASEDIR

製品のインストールディレクトリを指定します。DSM コンポーネントのみがこのディレクトリに格納され、ほかの CA Technologies 製品と共有されるコンポーネントは、`$CASHCOMP` 環境変数で指定されたディレクトリに格納されます。DSM コンポーネントはすべて、`$CA_ITRM_BASEDIR` に同じ値を使用する必要があります。したがって、ドメインマネージャからインフラストラクチャ展開ウィザードまたはコマンドラインを使用して DSM エージェントを展開する場合は、DMPrimer コンポーネントに対して必要な CA_DSM_BASEDIR の値を引数で指定する必要があります。このコンポーネントは、通常、コンピュータに最初にインストールされる DSM コンポーネントです。詳細については、「[DMPrimer インストールへ受け渡すオプション](#) (P. 277)」を参照してください。

デフォルト: `/opt/CA/DSM`

CA_DSM_CONFIGDATA

設定データをインストールするディレクトリを指定します。

デフォルト: `$CA_ITRM_BASEDIR`

CASHCOMP

共通コンポーネントおよびリンク ディレクトリの親ディレクトリを指定します。この変数が現在インストールされているほかのコンポーネントによって設定されている場合は、変更されません。**\$CALIB** および **\$CABIN** 環境変数は、**CASHCOMP** から派生します。すべての **CA Technologies** ソフトウェア コンポーネントは、任意のコンピュータ上で **\$CASHCOMP** に同じ値を使用する必要があります。したがって、ドメインマネージャからインフラストラクチャ展開ウィザードまたはコマンドラインを使用して **DSM** エージェントを展開する場合は、**DMPPrimer** インストールに対して必要な **CASHCOMP** の値を引数で指定する必要があります。このコンポーネントは、通常、コンピュータに最初にインストールされる **DSM** コンポーネントです。詳細については、「[DMPPrimer インストールへ受け渡すオプション](#) (P. 277)」を参照してください。

デフォルト : /opt/CA/SharedComponents

DSM_ALLOW_SOFT_PREREQS

ソフトウェアの前提条件の確認に失敗した場合でも、インストールを継続するかどうかを指定します。必要なソフトウェアの前提条件がない場合でも、強制的にインストールする場合は、「1」を指定します。

重要: 前提条件確認を無効にすると、**CA Client Automation** のインストールが機能しなくなる可能性があります。

デフォルト : 0 (いいえ)

DSM_LANGUAGE

インストールの言語を指定します。指定可能な値は、**enu** (米英語)、**deu** (独語)、**fra** (仏語) および **jpn** (日本語) です。プロパティ値が **enu** でない場合でも、指定した言語のファイルだけでなく、**enu** インストールのファイルも常にインストールされます。

デフォルト : 空 (NULL)。この場合、インストーラはシステムのデフォルト ロケールを使用します。システムのデフォルト ロケールがサポート対象外のロケールの場合は、**enu** (米英語) が使用されます。

注: **DSM_LANGUAGE** は、インストール ウィザードのダイアログ ボックスの言語を指定しません。

DSM_AUTOSTART_INSTALL

インストール後に、DSM デーモンを開始するかどうかを指定します。インストール後に、DSM デーモンを開始しない場合は、0 を指定します。

デフォルト：1 (はい)

DSM_AUTOSTART_REBOOT

ホストが再起動されたときに、DSM デーモンを開始するかどうかを指定します。DSM デーモンを自動開始しない場合は、「0」を指定します。

デフォルト：1 (はい)

ITRM_INST_CMDLINE

Software Delivery および自動展開(DMSweep) コマンドラインユーティリティをインストールするかどうかを指定します。これらのユーティリティをインストールしない場合は、「0」を指定します。

デフォルト：1 (はい)

DSM_SETUP_SYS_PROFILE

システムプロファイル (/etc/profile またはそれと同等のもの) を変更して、ログインユーザ全員の DSM 環境を設定するかどうかを指定します。システムプロファイルを変更しないままにしておく場合は、「0」を指定します。

デフォルト：1 (はい)

FIPS_MODE

Client Automation の FIPS モードを指定します。FIPS 推奨モードの場合は 1、FIPS のみモードの場合は 2 を指定します。

デフォルト： 1 (FIPS 推奨)

エージェントの一般プロパティ

DSM_INST_AGENT

DSM エージェントをインストールするかどうかを指定します。指定されていない場合は、ほかの機能が依存していない限り、エージェント機能はインストールすることができません。ほかの設定で必要とならない限り、エージェント機能を展開しない場合は **0** を指定します。

デフォルト： **1** (はい)

DSM_SERVER

DSM エージェントの接続先のスケーラビリティ サーバシステムの名前を入力します。このパラメータは、`$DSM_INST_AGENT` が **1** に設定されている場合にのみ使用されます。

デフォルト： ローカル ホスト名

DSM_AGENT_DEFAULTGROUPS

スペースなしのカンマ区切りのリストで、エージェントが結合する管理グループを指定します。

デフォルト： **null** (エージェントがグループと結合していないことを示します)

スケーラビリティ サーバの一般プロパティ (Linux のみ)

DSM_INST_SERVER

DSM スケーラビリティ サーバをインストールするかどうかを指定します。指定しない場合は、スケーラビリティ サーバ機能はインストールされません。エージェント専用パッケージの場合、このパラメータは無視されます。スケーラビリティ サーバをインストールしない場合は、**0** を指定します。

デフォルト： **1** (はい)

DSM_MANAGER

DSM スケーラビリティ サーバが報告するドメイン マネージャのホスト名を指定します。このパラメータは、`$DSM_INST_SERVER` が **1** に設定されている場合にのみ使用されます。

デフォルト： ローカル ホスト名

スケーラビリティ サーバのプロパティ(Linux のみ)

DSM_ENGINE

スケーラビリティ サーバが使用するエンジン名を指定します。空の値は、システム エンジン指定します。

デフォルト : Null

DSM_PATH_COMMON_SERVER_DB

スケーラビリティ サーバ データベースのディレクトリのパスを指定します。

デフォルト : \$CA_DSM_CONFIGDATA/Server/serverdb

Asset Management エージェントのプロパティ

DSM_INST_AM_AGENT

Asset Management エージェント (AM エージェント) をインストールするかどうかを指定します。このエージェントをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

DSM_AMAGENT_CMDFILE_USER

AM エージェントがコマンド ファイルを実行する ユーザ ID を指定します。

デフォルト : root

DSM_AMAGENT_EXTUTILITY_USER

AM エージェントがユーティリティを実行する ユーザ ID を指定します。

デフォルト : root

DSM_AMAGENT_DMSCRIPT_USER

AM エージェントが DMScript を実行する ユーザ ID を指定します。

デフォルト : root

DSM_AMAGENT_USER_INVENTORY

ユーザ インベントリ モジュールをインストールするかどうかを指定します。ユーザ インベントリ モジュールをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

DSM_AMAGENT_WITHCRONINFO

crontab 情報を表示するかどうかを指定します。情報を表示しない場合は、0 を指定します。

デフォルト : 1 (はい)

DSM_AMAGENT_WITHUSERINFO

ユーザ情報を表示するかどうかを指定します。情報を表示しない場合は、0 を指定します。

デフォルト : 1 (はい)

DSM_AMAGENT_PRIO_LEVEL

Asset Management プロセス優先度を増分します。優先度の範囲は -20 - 19 です。

デフォルト : 0

DSM_AMAGENT_EXACTINTERVAL

AM エージェントを、間隔において (値 = 1) または一定の時刻 (値 = 0) に実行するかどうかを指定します。

デフォルト : 1

DSM_AMAGENT_RANDOM

AM エージェントを、一定の間隔 (値 = 0) またはランダムに選択された間隔 (値 = 1) で実行するかどうかを指定します。このパラメータは、\$DSM_AMAGENT_EXACTINTERVAL=1 の場合にのみ重要となります。

デフォルト : 0

DSM_AMAGENT_WEEKLY

AM エージェントが毎週実行されるように指定します。このパラメータは、\$DSM_AMAGENT_EXACTINTERVAL=1 の場合にのみ重要となります。

デフォルト : 0

DSM_AMAGENT_DAILY

AM エージェントが n 日ごとに実行されるように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=1` の場合にのみ重要となります。

デフォルト : 1

DSM_AMAGENT_HOURLY

AM エージェントが n 時間ごとに実行されるように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=1` の場合にのみ重要となります。

デフォルト : 0

DSM_AMAGENT_EXMONDAY

値が 1 の場合、AM エージェントが月曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト : 0 (エージェントが月曜日に実行されます)

DSM_AMAGENT_EXTUESDAY

値が 1 の場合、AM エージェントが火曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト : 0 (エージェントが火曜日に実行されます)

DSM_AMAGENT_EXWEDNESDAY

値が 1 の場合、AM エージェントが水曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト : 0 (エージェントが水曜日に実行されます)

DSM_AMAGENT_EXTHURSDAY

値が 1 の場合、AM エージェントが木曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト : 0 (エージェントが木曜日に実行されます)

DSM_AMAGENT_EXFRIDAY

値が 1 の場合、AM エージェントが金曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト：0（エージェントが金曜日に実行されます）

DSM_AMAGENT_EXSATURDAY

値が 1 の場合、AM エージェントが土曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト：0（エージェントが土曜日に実行されます）

DSM_AMAGENT_EXSUNDAY

値が 1 の場合、AM エージェントが日曜日に実行されないように指定します。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト：0（エージェントが日曜日に実行されます）

DSM_AMAGENT_EXECUTETIME

AM エージェントが日中のこの時刻に実行を開始するように指定します。時刻形式は hh:mm（時間：分）です。このパラメータは、`$DSM_AMAGENT_EXACTINTERVAL=0` の場合にのみ重要となります。

デフォルト：00:00（午前 0 時）

Asset Management の一般プロパティ

DSM_INST_AM

Asset Management（AM）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。指定しない場合は、AM 機能はインストールされません。AM 機能をインストールしない場合は 0 を指定します。

デフォルト：1（はい）

Asset Management ソフトウェア使用状況スケーラビリティ サーバのプロパティ(Linux のみ)

DSM_INST_AM_METER_SERVER

Asset Management (AM) ソフトウェア使用状況スケーラビリティ サーバをインストールするかどうかを指定します。ソフトウェア使用状況スケーラビリティ サーバをインストールしない場合は、**0** を指定します。

デフォルト : 1 (はい)

Asset Management セクタ サーバのプロパティ(Linux のみ)

DSM_INST_AM_SECTOR_SERVER

Asset Management (AM) セクタ サーバをインストールするかどうかを指定します。セクタ サーバをインストールしない場合は、**0** を指定します。

デフォルト : 1 (はい)

DMPriemer プロパティ

DSM_INST_DMPRIMER

DMPriemer をインストールするかどうかを指定します。DMPriemer をインストールしない場合は、**0** を指定します。

デフォルト : 1 (はい)

Data Transport Service の一般プロパティ(Solaris のみ)

DTS_PPP_USER

(Solaris でのみ使用) PPP ユーザを作成するかどうかを指定します。プロトコルの **asppp** または **Solstice PPP** のいずれかが検出されない場合は、このパラメータは無視されます。PPP ユーザを作成する場合は **1** を指定します。

デフォルト : 0 (いいえ)

RC の一般プロパティ (Linux/Mac OS X のみ)

DSM_INST_RC

Remote Control 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。指定しない場合、Remote Control 機能はインストールされません。Remote Control コンポーネントをインストールしない場合は 0 を指定します。

デフォルト : 1 (はい)

Remote Control エージェントのプロパティ (Linux/Mac OS X のみ)

DSM_INST_RC_AGENT

Remote Control エージェントをインストールするかどうかを指定します。エージェントをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

DSM_RC_AGENT_STANDALONE

Remote Control エージェントを集中管理するか (値 = 0) 、またはスタンドアロン (値 = 1) にするかを指定します。

デフォルト : 0

DSM_RC_AGENT_IN_MGMT_GROUPS

集中管理するエージェントを管理グループに表示するかどうかを指定します。

デフォルト : 1 (はい)

Remote Control スケーラビリティ サーバのプロパティ (Linux のみ)

DSM_INST_RC_SERVER

Remote Control スケーラビリティ 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。Remote Control スケーラビリティ サーバをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

Software Delivery の一般プロパティ

DSM_INST_SD

Software Delivery 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。設定しない場合は、SD 機能はインストールされません。SD コンポーネントをインストールしない場合は 0 を指定します。

デフォルト : 1 (はい)

Software Delivery エージェントのプロパティ

DSM_INST_SD_AGENT

Software Delivery (SD) エージェントをインストールするかどうかを指定します。 エージェントをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

CA_DSM_REPLACE_PRE_R11_SD_AGENT

pre-r11 SD エージェントを置き換える（つまり、削除する）か、または共存させるかを指定します。 システムに pre-r11 SD エージェントがすでにインストールされている場合にのみ該当します。 古いエージェントを削除する場合は、1 を指定します。

デフォルト : 0 (共存)。

SD ブート サーバのプロパティ(Linux のみ)

FIPS_MODE

Client Automation インストーラによって設定される FIPS モードを定義します。 有効な値は 1 (FIPS 推奨) および 2 (FIPS のみ) です。

DSM_INST_SD_BOOTSERVER

Software Delivery (SD) ブート サーバ をインストールするかどうかを指定します。通常、スケーラビリティ サーバおよびブート サーバは、同じホストにインストールされます。ブート サーバをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

DSM_BOOTSERVER_OS_INSTALL_PATH

OSIM OS イメージ ライブラリの場所を指定します。

デフォルト : \$ITRM_PATH_COMMON_SERVER_DB/SDBS/var

BOOTSERVER_ENABLED

ブート サーバ サービスを有効にするかどうかを決定します。 サービスを無効にするには、0 を指定します。

デフォルト : 1 (はい)

BOOTSERVER_DISABLESHARES

SMB 共有を使用不可にするかどうかを指定します。SMB 共有を使用可能にする場合は、0 を指定します。

デフォルト : 1 (はい)

SD スケーラビリティ サーバのプロパティ(Linux のみ)

DSM_INST_SD_STAGSERVER

Software Delivery (SD) スケーラビリティ 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。通常、スケーラビリティ サーバおよびブート サーバは、同じホストにインストールされます。SD スケーラビリティ サーバをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

SDLIBRARY

ソフトウェア パッケージ ライブラリの場所を指定します。

デフォルト : \$CA_DSM_CONFIGDATA/sd/asm/library

DSM_SD_EXPORT_NFS_SHARE

\$SDLIBRARY を NFS 共有としてエクスポートするかどうかを指定します。\$SDLIBRARY をエクスポートする場合は、1 を指定します。

デフォルト : 0 (いいえ)

DSM_SD_EXPORT_SAMBA_SHARE

\$SDLIBRARY を SAMBA 共有としてエクスポートするかどうかを指定します。SDLIBRARY を Samba 共有としてエクスポートする場合は、1 を指定します。

デフォルト : 0 (いいえ)

DSM_SD_INSTALL_CCS_CALENDAR

CCS カレンダ (イベント管理) をインストールするかどうかを指定します。CCS 配信が使用可能か、またはすでにインストールされている場合にのみ使用可能です。CCS カレンダをインストールする場合は、1 を指定します。

デフォルト : 0 (いいえ)

Web コンソールのプロパティ (Linux のみ)**DSM_INST_WEBGUI**

Web コンソールをインストールするかどうかを指定します。Web コンソールをインストールする場合は、1 を指定します。

デフォルト : 0 (いいえ)

Web サービスのプロパティ (Linux のみ)**DSM_INST_WEBSERVICES**

Web サービスをインストールするかどうかを指定します。Web サービスをインストールする場合は、1 を指定します。

デフォルト : 0 (いいえ)

WAC_MANAGER

Web サービスの接続先になるマネージャを指定します。

デフォルト : ローカル ホスト名

DSM_TOMCAT_PORT

ハンドラがリクエストをリスンする TCP/IP ポートを指定します。

デフォルト : 8090

DSM_TOMCAT_SHUT

ハンドラがシャットダウン リクエストをリスンする TCP/IP ポートを指定します。

デフォルト : 8095

DSM_TOMCAT_AJP

リクエストをプロセス外のワーカに AJPv13 プロトコルを使用して転送するために、ワーカ プロセスが AJP13 リクエストをリスンするポートを指定します。

デフォルト : 8020

DSM_AMS_WEBPORT

Asset Maintenance System の Web ポートを指定します。

デフォルト : 8080

PIF パッケージのプロパティ

DSM_INST_PACKAGER

PIF 製品ソフトウェア開発キット (SDK) をインストールするかどうかを指定します。SDK は、それ独自に、すなわち Client Automation とは無関係にインストールすることができます。SDK をインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

ドキュメントのプロパティ (Linux のみ)

DSM_INST_DOC

ドキュメントをインストールするかどうかを指定します。ドキュメントセットをインストールしない場合は、0 を指定します。

デフォルト : 1 (はい)

インストール ログ ファイル

CA Client Automation のインストーラのすべてのアクティビティは、インストーラによって自動的に作成されるファイルに記録されます。

CA Technologies ではログ ファイル収集ツールの dsminfo を提供しています。このツールは、Client Automation で発生した問題を分析するのに必要な情報があればそれを収集する場合に役立ちます。

dsminfo ツールは、CA オンライン サポートから入手可能で、<http://support.ca.com> からダウンロードできます。

インストール ログ ファイル(Windows)

Windows では、以下のタイプのログ ファイルがインストーラによって作成されます。

DSMSetupxxx.log

Microsoft Windows Installer (MSI) によって作成され、`%temp%` 環境変数で指定されるディレクトリに保存されます。このログ ファイルは、マネージャ、スケーラビリティ サーバ、DSM エクスプローラ、およびエージェントを使用しているときに作成されます。各 MSI パッケージは、個別にログ ファイルを作成します。

TRC_xxx.log

内部プロセスによって作成され、`%temp%` 環境変数で指定されるディレクトリに保存されます。これらのファイルには、インストールされているコンポーネントの設定（たとえば、CAF、マネージャ、またはデータベースの設定）が文書化されています。

ログ ファイルの名前の文字列 `xxx` は、ログ情報が属するコンポーネントの名前で置き換えられます（たとえば、`DSMSetupManager.log`）。

インストール ログ ファイル(Linux および UNIX)

Linux および UNIX 上のインストールの初期のログ ファイルの名前は、`ca-dsm.install.log` です。インストールを変更した場合、このログ ファイルの名前は `ca-dsm.reinstall.log` になります。製品を削除すると、このログ ファイルは `ca-dsm.deinstall.log` になります。

Linux および UNIX 上のインストール ログ ファイルは、以下のディレクトリに保存されます。

- `/tmp`
- `/opt/CA/installer/log`

インストールされている DSM コンポーネントに関するバージョン情報

インストーラは、インストールされている **CA Client Automation** のコンポーネントおよび機能に関するバージョン情報を提供します。この情報には、**dsmver** コマンドを使用してアクセスすることもできます。

バージョン情報は、**M.m.b.r** という形式で表されます。ここで、**M** はメジャーリリース番号、**m** はマイナーリリース番号、**b** はビルド番号、そして **r** はリビジョン/パッチ番号です。たとえば、バージョン **12.0.01234.1** は、メジャーリリース **12**、マイナーリリース **0**、ビルド **1234**、そしてリビジョン **1** となります。

インストールされているコンポーネントと機能、およびそれぞれのバージョンを表示するには、コマンドラインで **dsmver** コマンドを入力します。

dsmver コマンドのフォーマットは以下のとおりです。

dsmver

バージョン情報の出力フォーマットは、以下の例に示したようになります。

Desktop and Server Management

```
-----  
Explorer - Asset Management      12.0.1234.1  
Explorer - Remote Control        12.0.1234.1  
Explorer - Software Delivery     12.0.1234.1  
Manager - Engine                 12.0.1234.1  
Manager - Asset Management       12.0.1234.1  
Manager - Data Transport         12.0.1234.1  
サーバ  
. . . . .
```

第 4 章: ポストインストール タスク

この章では、既存のインストールの変更、修復、アップグレード、およびアンインストールに関する情報について説明します。

このセクションには、以下のトピックが含まれています。

[インストール後の製品言語の変更](#) (P. 235)

[MDB の管理](#) (P. 236)

[SQL Bridge のインストール](#) (P. 248)

[Oracle Bridge のインストール](#) (P. 249)

[Windows でドッキング デバイスを有効にする方法](#) (P. 251)

[Windows でソースからエージェントを実行する方法](#) (P. 252)

[Windows でユーザ アカウントで Client Automation サービスを実行する方法](#) (P. 254)

[独自の X.509 証明書をインストール イメージに取り込む方法](#) (P. 255)

[インストールの変更および修復](#) (P. 259)

[インストールのアップグレード](#) (P. 261)

[Client Automation のアンインストール](#) (P. 262)

インストール後の製品言語の変更

以下のリストでは、インストール後に CA Client Automation の製品言語を変更する方法に関する関連情報が提供されます。

- インストール後に製品言語を変更するには、以下のような別の方法があります。

- すでにインストールされている DSM コンポーネントの言語を変更できるコンポーネントは、エクスプローラ、スケーラビリティ サーバ、およびエージェントです。エージェント ホスト上で、ccnfcmda コマンドを以下のとおり実行してください。

```
ccnfcmda -cmd SetParameterValue -ps itrm/common/localization  
-pn language -v lang
```

lang の値によって、目的の言語が指定されます。使用可能な値は、enu（米英語）、deu（ドイツ語）、fra（フランス語）、および jpn（日本語）で、エージェントにはさらに chs（簡体字中国語）、esn（スペイン語）、および kor（韓国語）が使用できます。

注: ccnfcmda エージェント設定コマンドの詳細については、「<command> /?」と入力してください（コマンドプロンプトで実行）。

- 上記の ccnfcmda コマンドを実行するためのクエリ ベースのポリシーを作成します。

- マネージャをインストールした後にマネージャの言語を変更することはできません。
- CA Client Automation の製品言語を設定する際には、指定した言語の言語パッケージが利用可能かどうかはチェックされないので、言語パッケージがインストールされていることを確認してください。指定した言語の言語パッケージがインストールされていない場合、CA Client Automation は英語（米国）に戻ります。
- 言語を再設定する場合、新しい値を引き継がせるために `caf stop` および `caf start` をそれぞれ利用して CA Client Automation の停止および再開を行う必要があります。

関連項目：

[多言語インストール](#) (P. 131)

MDB の管理

以下のタスクは、管理データベースの管理および同期に関する情報を提供します。

Microsoft SQL Server MDB のメンテナンス

Microsoft SQL Server（SQL Server）データベース テーブルは、データベースで大量のデータの更新があった場合、常に最適化する必要があります。

SQL Server 上の管理データベース（MDB）の管理に役立つものとして、Client Automation では、`DsmMSSqlOpt.bat` メンテナンス スクリプトを管理者が常時適用できるように提供しています。

`DsmMSSqlOpt.bat` スクリプトを使用すると、インデックスのデフラグや統計の更新などのメンテナンス タスクを実行することで、データベース テーブルを最適化することができます。CA Client Automation が所有するテーブルのみがスクリプトによって影響を受けます。

`DsmMSSqlOpt` メンテナンス スクリプトは、CA Client Automation のインストール時に以下の場所に自動的にインストールされます。

```
%Program Files%\CA\DSM\database\mdb_install\mssql\DsmMsSqlOpt.bat
```

`DsmMSSqlOpt` メンテナンス スクリプトは、CA Client Automation のインストールメディア（DVD）の以下の場所からも利用できます。

```
Maintenance\Windows\mssql\DsmMsSqlOpt.bat
```

DsmMSSqlOpt メンテナンス スクリプトは、以下のような特定のオプション付きで実行できます。

```
DsmMsSqlOpt.bat [-pagecount=n] [-maxfrag=m] [ -usereindex] [ {local | ServerName}  
[MDBName] ]
```

-pagecount

テーブルまたはインデックスの最大ページ数 *n* を指定します。指定したページ数よりも大きいテーブルやインデックスはデフラグされます。*n* は数値です。

デフォルト：1000

-maxfrag

断片化の程度 *m* を指定します。指定した断片化の程度であるテーブルはデフラグされます。*m* は数値です。

デフォルト：10

-usereindex

インデックスがデフラグではなく再構築されるように指定します。デフォルトでは、DsmMsSqlOpt スクリプトはインデックスのデフラグを実行します。

DSM エンタープライズ マネージャおよびドメイン マネージャがある場合は、メンテナンス スクリプトを両方の層のデータベースに対して実行する必要があることに注意してください。ドメイン データベースに最初の 1,000 のコンピュータ アセットが登録された後、少なくとも 1 回はスクリプトを実行することをお勧めします。以後、5,000 のコンピュータ アセットを追加で登録するたびに、このスクリプトを実行する必要があります。エンタープライズの場合、5,000 のコンピュータ アセットが関連するドメイン マネージャから複製されるたびに、メンテナンスを実行する必要があります。

DsmMsSqlOpt.bat スクリプトは、MDB がインストールされているコンピュータ上でローカルに実行する必要があります。このスクリプトには 2 つのオプションがあり、インデックスの再構築か、またはインデックスのデフラグに使用できます。[インデックス再構築] オプションでスクリプトを実行する前に、MDB にアクセスするすべてのマネージャ コンポーネントをシャットダウンすることをお勧めします。DSM コンポーネントは、スクリプトの終了後に再起動する必要があります。

スクリプトがインデックスをデフラグするオプションで呼び出された場合、DSM コンポーネントは保持されて続行されます。ただし、スクリプトによって開始された捜査はリソースを大量に消費し、パフォーマンスにネガティブな影響を与える可能性があります。また、データベースの大きさを考慮すると、インデックスのデフラグを完了するには数時間かかる可能性があります。

このため、MDB のワークロードが少ないか、またはないときに MDB のメンテナンス タスクをスケジュールします。たとえば、スクリプトを 1 週間に 1 度夜間に起動する、または週末に起動するようスケジュールできます。

SQL Server MDB メンテナンスに関する重要事項

Microsoft SQL Server MDB メンテナンスに関する注意事項は、以下のとおりです。

- %TEMP% 変数は DsmMsSqlOpt.bat スクリプトが起動される前に、適切な作業ディレクトリに設定される必要があります。
- インデックスの再構築はデフラグより速い速度で実行されるため、最初のメンテナンス手順として断片化の程度が 30% より大きいインデックスを再構築するのは効果的な方法です。このような再構築を実行するには、以下の例のように、オプション `-usereindex` および `-maxfrag=30` を使用して DsmMsSqlOpt スクリプトを起動する必要があります。

```
DsmMsSqlOpt.bat -maxfrag=30 -usereindex
```

- 最初の手順の後、断片化が 10% より大きいすべてのテーブルはデフラグされる必要があります。このようなデフラグは、以下の例のように、DsmMsSqlOpt スクリプトをオプション `-maxfrag=10` を使用して呼び出すことにより実行されます。

```
DsmMsSqlOpt.bat -maxfrag=10
```

Oracle MDB のメンテナンス

Oracle MDB のパフォーマンスの問題を解決するには、以下のいずれかを実行します。

- Solaris Oracle サーバ コンピュータ上の Oracle SQL ツールから、以下のコマンドを実行します。

```
EXEC DBMS_STATS.gather_schema_stats(ownname =>'MDBADMIN', cascade =>true,  
method_opt=>'FOR ALL COLUMNS SIZE AUTO');
```

- Oracle ユーザ クレデンシャルを使用して Solaris コンピュータへログインし、コマンド シェルから、以下の例に示されているようにコマンドを実行します。

```
echo "EXEC DBMS_STATS.gather_schema_stats (ownname => 'MDBADMIN', cascade =>true,  
method_opt=>'FOR ALL COLUMNS SIZE AUTO');"|sqlplus sys/<pwd>@<instance> as  
sysdba
```

この例では、*<pwd>* は現在の Oracle インスタンスのパスワードで、*<instance>* は現在の Oracle インスタンスの名前 (SID) です。

関連項目：

[リモート Oracle MDB のインストール](#) (P. 153)

ターゲット MDB と同期されたオブジェクト

SQL Server と Oracle ベースの両方のターゲット MDB に同期されたオブジェクトには、以下のタイプが含まれます。

- プライマリ アセットおよびユーザ情報
 - 検出されたコンピュータ
 - 検出されたユーザ
 - 検出されたコンピュータ ユーザ (コンピュータとユーザとの関係)
- ハードウェア インベントリ
 - コンピュータ、一般インベントリ
- ソフトウェア インベントリ
 - ソフトウェア シグネチャ
 - コンピュータ、ソフトウェア インベントリ (シグネチャ ベースおよびヒューリスティック ベースのソフトウェア インベントリの両方)

同期化タスクの作成

DSM アセットおよびインベントリ データと SQL Server または Oracle ベースのターゲット MDB との同期化は、スケジュールされた時間に実行されるエンジンタスクによって起動されます。このタスクを作成し、タスクのスケジュールを定義するには、DSM エクスプローラ GUI を使用します。

DSM アセットおよびインベントリ データと Microsoft SQL Server 上の既存の MDB との同期を実行するエンジンタスクは、既存の DSM エンジンタスクと同じ方法で作成、設定、割り当て、スケジュール、および実行されます。DSM マネージャの [コントロールパネル] - [エンジン] - [すべてのエンジン] に移動し、同期化タスクを実行するエンジンを右クリックし、コンテキストメニューから [新規タスクの追加] を選択します。新規タスクの作成ウィザードが開き、説明に従って同期化タスクを作成できます。

新規タスクの作成ウィザードでは、以下の主な手順を実行します。

- ウィザードの最初のページで、[タスクタイプ] ドロップダウンリストからデータベースの同期化タスクタイプを選択します。
- ウィザードの 2 番目のページで、タスクの目的およびタイプを反映するようなデータベース同期化タスクの適切な名前と説明を入力します。
- ウィザードの 3 番目のページで、「[同期化タスクの設定オプション](#) (P. 241)」で説明されているように、ターゲットデータベースタイプおよびターゲット MDB のクレデンシャルを指定します。[テスト接続] ボタンをクリックすると、今作成した設定をすぐにテストできます。このページを閉じる前に、ウィザードによって、ターゲット MDB が存在し、要求される条件を満たしているかがチェックされます。
- ウィザードの 4 番目のページで、同期化タスクの事前設定されたスケジュールリング（「通常は常に実行するようにスケジュールされています」）を変更する場合は、[スケジュールリングの設定] ボタンをクリックします。事前設定されたスケジュールリングを使用する場合は、[完了] をクリックし、ウィザードを終了します。

同期化タスクの設定オプション

同期化タスクの作成中、新規タスクの作成ウィザードのページの 1 つの中で、ターゲット MDB 用のクレデンシヤル（接続プロパティ）を指定する必要があります。

■ SQL Server ベースのターゲット MDB :

SQL Server ベースのターゲット MDB では、必須のクレデンシヤルに以下のものが含まれます。

- ターゲット MDB のサーバタイプ（値：MS SQL Server）
- ターゲット MDB をホストするコンピュータ名
- データベース サーバ インスタンス、ポート番号（デフォルト：<none>）
- データベース名を指定します。
- ターゲット MDB 上のユーザ名
ユーザ名は `ca_itrm` に固定され、変更できません。
- ターゲット MDB 上のパスワード

重要：ここでは、同期のために SQL Server MDB をアップグレードした時の Client Automation セットアップに含まれる `CA_ITRM` パスワードパラメータを使用して指定したパスワードを入力する必要があります。

■ **Oracle ベースのターゲット MDB :**

Oracle ベースのターゲット MDB では、必須のクレデンシャルに以下のものが含まれます。

- ターゲット MDB のサーバタイプ (値 : Oracle)
- ターゲット MDB をホストするコンピュータ名
- ターゲット MDB のサーバ ID (デフォルト : orcl)
- ターゲット Oracle MDB のポート番号 (デフォルト : 1521)
- ターゲット MDB 上のユーザ名
ユーザ名は `ca_itrm` に固定され、変更できません。
- ターゲット MDB 上のパスワード

重要: ここでは、同期のために Solaris 上の Oracle MDB をアップグレードした時の **Client Automation MDB** インストーラに含まれる `CA_ITRM` パスワードパラメータを使用して指定したパスワードを入力する必要があります。

同じウィザードページにある [テスト接続] ボタンをクリックすると、今作成した設定をすぐにテストできます。マネージャは、次にターゲット MDB との接続を試みます。このアクションの結果は [テスト接続] ボタンの横に表示されます (「接続に成功しました。」など)。

新規タスクの作成ウィザードの [スケジューリング] ページにある [スケジューリングの設定] ボタンをクリックすることで、同期化タスクのスケジューリングを設定できます。デフォルトの設定は、「通常は常に実行するようにスケジュールされています」です。

同期化のオプションおよび制限

同期化タスクを実行する場合、以下のオプションがあります。

- **DSM ドメイン マネージャ上の MDB からターゲット MDB へのデータの同期化。**
- **DSM エンタープライズ マネージャ上の MDB からターゲット MDB へのデータの同期化。** これには、エンタープライズ マネージャに報告するすべてのドメイン マネージャからのデータの同期化が含まれます。

同期化には、以下の制限があります。

- 関連するエンタープライズ マネージャがすでに同じターゲット MDB と同期化を行っている場合は、**DSM ドメイン マネージャ MDB** からはデータを同期化しないでください。同期化を行うと、ネットワーク上に不要なデータ ロードが発生させてしまいます。
- 関連するドメイン マネージャの 1 つがすでに同じターゲット MDB と同期化を行っている場合は、**DSM エンタープライズ マネージャ MDB** からはデータを同期化しないでください。同期化を行うと、ネットワーク上に不要なデータ ロードが発生させてしまいます。

同期の削除

Microsoft SQL Server ソース MDB とターゲット MDB との同期を削除する場合は、同期化タスクを削除する必要があります。

同期化タスクがエンジンにリンクされている状態の時に、**DSM エクスプローラ GUI** 上の [すべてのエンジン タスク] ディレクトリから、同期化タスクの削除を開始します。エンジン タスクを右クリックし、コンテキスト メニューから [削除] を選択します。選択した項目を削除するかの確認を求められます。

ただし、同期化タスクはすぐには削除されません。[タスクの削除] ダイアログ ボックスによって、同期化タスクを削除する前に、エンジンをもう 1 度実行する必要があることが通知されます。

[タスクの削除] ダイアログ ボックスでは、同期されたオブジェクトに関するターゲット MDB をエンジンにクリーンアップさせるように選択することもできます。このオプションを選択しないと、エンジンは、ソース MDB のみをクリーンアップします。このオプションを選択すると、同期化タスクのステータスが「エンジンによるデータベース クリーンアップの保留中」に変わります。エンジンによってクリーンアップ タスクが実行され、次回それがスケジュールされると、同期化タスクをエンジンがリンク解除して削除します。

マネージャおよび MDB のアンインストール

DSM マネージャをアンインストールする場合、MDB はアンインストールされず、システム上に残ります。

MDB は、それとともにローカルにインストールされた別の CA Technologies 製品によって使用されたり、リモートの製品から使用されたりします。これらの CA Technologies 製品のいずれかをアンインストールしても、必ずしも MDB が使用されなくなるわけではありません。

MDB および選択された MDB プロバイダのアンインストールは、ほかの CA Technologies 製品のローカルまたはリモートでの使用状況の影響すべてを慎重に考慮した後、権限が与えられた管理者のみが実行することをお勧めします。

Microsoft SQL Server MDB は、Microsoft SQL エンタープライズ マネージャを使用して削除することができます。エンタープライズ マネージャでは、MDB データベースを選択し、削除することができます。MS SQL Server MDB の削除に使用できる別のツールは、SQL Server Management Studio です。

Oracle MDB を削除するには、設定プログラムを使用し、「アンインストール」を選択して MDB スキーマの PIF 製品の部分を削除します。その後、「oracle」でログインして、Oracle dbca 管理ツールを使用して、データベースのテーブルを削除できます。最後に、../opt/CA/SharedComponents/oracle/mdb フォルダに残っているファイルを、「root」でログインして手動で削除できます。

注: Oracle MDB の削除の詳細については、Client Automation ドキュメントセット（マニュアル選択メニュー）の一部である「*MDB の概要*」、または適切な Oracle のドキュメントを参照してください。

DSM マネージャをアンインストールする場合、Microsoft SQL Server から ca_itrm ユーザ、および ca_itrm_ams アカウント（存在する場合）を手動で削除する必要があります。ca_dsm ユーザが Microsoft SQL Serverに残っていると、その SQL Server では Client Automation を新規にインストールできない場合があります。使用していた CCS もアンインストールした場合は、nsmadmin および hostname¥TNDUsers アカウントも SQL Server から手動で削除する必要があります。

DSM マネージャをアンインストールする場合、デフォルトでは MDB に含まれている付随データは削除されません。

Client Automation インストール ウィザードには、MDB からデータを削除する機能があります。

なんらかの理由により、MDB からデータを削除する方法としてこの方法を選択しない場合は、スクリプト [data_uninstall](#) (P. 246) を実行して MDB をクリーンアップする必要があります。このスクリプトは、Microsoft SQL Server および Oracle をサポートしています。スクリプトの適切なバージョンである `data_uninstall.bat` (SQL Server 用) および `data_uninstall.sh` (Oracle 用) は、Client Automation インストール DVD の以下の場所から利用できます。

- `dvdroot\Maintenance\Windows\mssql\`
- `dvdroot\Maintenance\Windows\oracle\`

各サブディレクトリからローカルのマネージャ システムにすべてのファイルをコピーし、適切なパラメータを指定した `data_uninstall` スクリプトをコマンドプロンプトから実行します。

以下は、`data_uninstall` スクリプトを使用するシナリオおよびビジネス事例です。

マネージャを完全に削除

Client Automation が唯一のアプリケーションの場合は、MDB を手動で削除することができます。

または、`data_uninstall` スクリプトを実行して、`-pdata d` および `-data d` のフラグを設定します。

マネージャをクリーンアップして最初からやり直し

Client Automation が唯一のアプリケーションの場合は、MDB を手動で削除することができます。

または、`data_uninstall` スクリプトを実行して、`-pdata d` および `-cdat d` のフラグを設定します。

登録済みアセットも削除する場合は、引数 `-asset d` を設定する必要があります。

マネージャを削除してすべてのデータを保持

この場合、少なくともファイル システム オブジェクトを参照する一部のデータを削除する必要があります。そのため、`data_uninstall` スクリプトを実行して、`-sdonly` フラグを設定します。これによって、オペレーティング システム インストール管理 (OSIM) およびブート情報を含む、関連する Software Delivery ファイル システム オブジェクトへの参照が削除されます。

data_uninstall コマンド - データベースからデータを削除

data_uninstall コマンドを使用して、データベースからデータを削除したり、登録されている製品およびドメインをデータベースで確認します。data_uninstall コマンドは Microsoft SQL Server および Oracle をサポートしています。

このコマンドには異なる複数のフォーマットがあります。

```
data_uninstall -server server_name
               -instance instance_name:port_number
               -database database_name
               -asset {k | d }
               -pdata {k | d }
               -cdata {k | d }
               -user
               -pwd
```

引数で指定された k または d フラグに応じて (k = データを保持、d = データを削除)、データベースからデータを削除します。(引数を指定しないでコマンドを実行すると、この使用方法が表示されます。)

```
data_uninstall -server server_name
               -instance instance_name:port_number
               -database database_name
               -check
```

MDB に登録されている製品の数およびデータベースに登録されているドメインの数を出力します。

```
data_uninstall -server server_name
               -instance instance_name:port_number
               -database database_name
               -sdonly
```

ファイル システム内のオブジェクトに応じて、Software Delivery データのみを削除します。また、このコマンドは、OSIM およびブートイメージへの MDB の参照も削除します。

-server server_name

ローカルの RDBMS システムの名前を指定します。

重要: データベース サーバ名とデータベース インスタンス名を合わせた長さは、最大 29 文字とする必要があります。

-instance *instance_name:port_number*

データベース インスタンスを識別します。たとえば、Microsoft SQL Server のインスタンス名です。Microsoft SQL Server デフォルト インスタンスの場合を除き、ポート番号の指定は必須です。Microsoft SQL Server デフォルト インスタンスの場合は、二重引用符を使用して、「-instance ""」のように空の名前を定義する必要があります。

-database *database_name*

SQL Server の場合は、たとえば **mdb** などのデータベース名を指定します。

Oracle の場合は、SID を指定します。

-asset {k|d}

アセットデータを登録解除する必要があるかどうかを指定します。アセットを保持するには **-asset k**、アセットを登録解除するには **-asset d** を使用します。

-pdata {k|d}

製品固有のデータを削除する必要があるかどうかを指定します。データを保持する場合は **-pdata k**、データを削除する場合は **-pdata d** を使用します。

-cdata {k|d}

Client Automation の共通データを削除する必要があるかどうかを指定します。データを保持する場合は **-cdata k**、データを削除する場合は **-cdata d** を使用します。

-user *user_name*

たとえば、**ca_itrm** など、データベースに接続するユーザ名を指定します。

-pwd *password*

-user で指定したユーザのパスワードを指定します。

-check

CA Technologies 製品が現在もデータベースに登録されているかどうかを確認し、どのドメインが登録されているかを確認します。

-sdonly

OSIM およびブート データを含む、ファイル システム内のオブジェクトに関連する Software Delivery データのみを削除します。

例: 製品およびドメインの確認

この例では、CA Technologies 製品が現在も MDB に登録されているかどうかを確認し、登録されているすべてのドメインを一覧表示します。

```
data_uninstall -server myMachine
                -instance ""
                -database mdb
                -check
```

例: アセット以外のデータを削除

この例では、MDB データベースからすべての Client Automation データを削除しますが、アセットの登録抹消は行いません。

```
data_uninstall -server myMachine
                -instance ""
                -database mdb
                -check
                -asset k
                -pdata d
                -cdata d
                -user ca_dsm
                -pwd myPassword
```

data_uninstall ログ ファイル

data_uninstall スクリプト実行後、以下のように、data_uninstall.log という名前のログファイルが Temporary フォルダに作成されています。

- Windows :
%TEMP%
- Linux の場合
/tmp

SQL Bridge のインストール

SQL Bridge の同期機能が DSM マネージャ インストールの一部としてアプリケーション環境にインストールされます。これは、SQL Bridge のソース側では、特別なインストール手順は必要ないということです。ただし、SQL Bridge のターゲット側では、適切な MDB に対するアップグレード手順をいくつか実行します。

Microsoft SQL Server MDB 1.0.4 を使用したターゲット側のアップグレード

Microsoft SQL Server MDB 1.0.4 は Windows に Unicenter Asset Portfolio Management r11.3 と共に使用されます。

ターゲット Microsoft SQL Server MDB のアップグレード方法

1. インストール DVD から [MDB のインストール] セットアップを実行します。
この手順では、まだターゲット MDB で利用できない MDB パッチが適用され、ca_itrm データベース ユーザが作成されます。
2. 同期機能を最大限活用するためには、CA サポート オンラインから入手可能な Windows 用のテスト修正 T5D6008 をダウンロードしてインストールする必要があります。テスト修正に付属する詳細なインストール手順に従います。
T5D6008 には、Windows の Unicenter Asset Portfolio Management r11.3 に適用される修正が含まれます。

Microsoft SQL Server MDB 1.5 を使用したターゲット側のアップグレード

Microsoft SQL Server MDB 1.5 は、CA Service Desk Manager r12 on Windows と共に使用されます。

ターゲット Microsoft SQL Server MDB をアップグレードするには、Client Automation インストール DVD から [MDB のインストール] セットアップを実行します。

この手順では、ターゲット MDB で最新の MDB スキーマ更新が適用され、ca_itrm データベース ユーザが作成されます。

Oracle Bridge のインストール

Oracle Bridge の同期機能が DSM マネージャ インストールの一部としてアプリケーション環境にインストールされます。これは、Oracle Bridge のソース側では、特別なインストール手順は必要ないということです。ただし、Oracle Bridge のターゲット側では、MDB に対するアップグレード手順をいくつか実行する必要があります。

Solaris 上の Oracle MDB 1.5 を使用したターゲット側のアップグレード

Oracle MDB 1.5 は、CA Service Desk Manager r12 on Windows と共に使用されます。

ターゲット Oracle MDB のアップグレード方法

1. [Solaris 上の Oracle MDB インストーラ] セットアップを実行します。これは、Client Automation リリース 12.9 インストール DVD から利用可能です。

この手順では、ターゲット MDB で最新の MDB スキーマ更新が適用され、ca_itrm データベース ユーザが作成されます。

2. CA Service Desk Manager 用の AMS.Properties ファイルの中に、以下のように新しい設定パラメータを追加します。

dsm_oracle_ddl=1

例

以下は、AMS.Properties ファイルの例です。

```
# ca_itrm_ams user password to connect to DSM Domain Database.
dsm_domain_db_password=
# Table Owner for DSM on-the-fly created tables.
# This property should never need to be set unless the tables
# were not created by ca_itrm.
dsm_downer=
# If we are running r11.2 or later and want to support
# Oracle Bridging, set the value of dsm_oracle_ddl to 1
dsm_oracle_ddl=1
```

Windows でドッキング デバイスを有効にする方法

モバイル デバイスのユーザは、モバイル デバイスとコンピュータ間で情報を交換または同期する必要がある場合があります。PDA（Personal Digital Assistant）などのモバイル デバイスは、通常、「クレードル」や「ドッキング デバイス」を使用して接続します。クレードルやドッキング デバイスは、コンピュータのシリアルポートまたは USB ポートに接続するか、または赤外線や Bluetooth インターフェースを使用してコンピュータに直接接続します。

ドッキング デバイスを使用したモバイル デバイスとコンピュータ間のデータ交換を使用可能にするには、以下のインストールと設定ステップを実行する必要があります。

- 同期ソフトウェアをインストールします。
 - Windows CE デバイスの場合（PocketPC および Windows Mobile）：
Microsoft ActiveSync（PocketPC または Windows Mobile デバイスに付属しています）をターゲット コンピュータにインストールし、デバイスをこのコンピュータに接続します。

注：Microsoft ActiveSync コンポーネントをインストールした後、ホスト PC でドッキング デバイスのサポートを有効にする必要があります。また、Microsoft ActiveSync コンポーネントでは、Client Automation のインストール時に行われる PATH 環境変数の変更が認識されている必要があります。このことは、Client Automation のインストールを行った後にログオフしてから再度ログオンすることによって行うことができます。
 - Palm OS デバイスの場合：
HotSync ソフトウェア（Palm OS デバイスに付属している Palm Desktop）をターゲット コンピュータにインストールし、Palm OS デバイスをこのコンピュータに接続します。
- Software Delivery または Asset Management エージェントをターゲット コンピュータにインストールします。
- 以下の手順に従って、マネージャで Client Automation のプロキシデバイスを起動します。
 - 新規の設定ポリシー（my_dockingdevice_policy など）を作成し、「DSM/common components/docking_devices」パラメータの値を True に設定します。
 - Software Delivery の場合は、追加で「DSM/Agent/Common agent/software delivery docking device」パラメータを Palm+WinCE に設定します。
 - ポリシーをターゲット コンピュータに適用します。

- Windows CE デバイスの場合は、モバイル デバイスをターゲット コンピュータに再接続します（切断してから再度接続します）。
Palm OS デバイスの場合は、Palm OS デバイスとそのホスト PC を同期します。
- ターゲット コンピュータで「caf register all」を実行するか、または自動登録が行われるまで最大 24 時間待機します。

Windows でソースからエージェントを実行する方法

Client Automation では、Windows Asset Management、Software Delivery、および Remote Control エージェントの各コンポーネントを、MSI 管理ネットワークの共有インストール ポイントから実行することができます。この固有の機能は、ソースからの実行と呼ばれます。エージェントがソースからの実行モードでインストールされた場合、プログラムの実行可能ファイルは、そのネットワーク管理共有インストール ポイントからロードされ、実行されます。設定ファイルやログ ファイルなどは、ローカル ディスクに保存されます。

共通の CAM および CAWIN コンポーネントは、現在、常にローカルにインストールする必要があります。

ソースからの実行モードでエージェントをインストールした後に、エージェント システムを再起動する必要があります。

ソースから実行モードでエージェントをインストールするように環境をセットアップする方法

1. MSI 管理インストール ポイントを作成します。

対話式インストール ウィザードを使用して WindowsProductFiles_x86 フォルダに移動し、**setup.exe /a** を実行します。これにより、完全な製品とそのすべてのコンポーネントのインストール ポイントが作成されます。

自動でエージェントのインストールを実行する場合、またはエージェント コンポーネントのみをインストールする場合は、WindowsProductFiles_x86 の下のエージェント フォルダの 1 つに移動し、以下のコマンドを実行します。

```
msiexec /a msipackagename /qn /v*! %temp%\YDSMAdminAgt.log"
```

注: いくつかのエージェント パッケージに msiexec コマンドを使用する場合は、すべてのエージェントに対して、必ず同じルート フォルダを使用してください。

2. ここで作成した管理インストール ポイントに、ネットワーク共有を作成します（まだ作成していない場合）。このネットワーク共有は、**null** セッション共有として設定する必要があります。

3. 管理ネットワーク共有インストール ポイントから、MSI パッケージをインストールします。

ソースからの実行モードでエージェントをインストールしようとしているターゲット コンピュータで、以下のコマンドを実行します。

```
msiexec /i %servernode%adminshare%msipackagename ADDSOURCE=ALL  
AGENT_SERVER=servername CAF_START_SERVICE=0 /qn /v*! %temp%DSMSetupRFS.log
```

これにより、エージェントが自動的にインストールされます。

インストール ウィザードでカスタム インストール オプションを使用して、ソースから実行モードでエージェントをインストールするように環境をセットアップすることもできます。UNC パス `%server node%MSI admin share%setup.exe` を使用してインストール ウィザードを開始し、カスタム インストールのダイアログボックスの指示に従って、ソースから実行する各エージェントを設定します。

注: 管理ネットワーク共有が Windows 2003 Server によってホスティングされている場合は、エージェントのマシン アカウントを Windows 2003 Server の管理者グループに追加する必要があることがあります。

Windows でユーザ アカウントで Client Automation サービスを実行する方法

アプリケーションフレームワーク (CAF) をローカル システム アカウントで実行しているときに、**Software Delivery** エージェントなどの **Client Automation** サービスを管理者アカウントで実行する必要が発生することがあります。このため、CAF では以下の **caf** コマンド オプションが提供されています。

setcreds

caf setcreds コマンドは、**Client Automation** サービスのクレデンシアルを設定します。**Asset Management** エージェントおよび **Software Delivery** エージェントのみがサポートされています。このコマンドは、多くのコンピュータに送信されるアセットまたはソフトウェア ジョブ内のコンソールで直接使用できます。ただし、ジョブ内に埋め込まれている平文のパスワードに注意してください。

savecreds、loadcreds

caf savecreds コマンドを使用すると、さまざまなコンピュータやサービスの一連のクレデンシアルを暗号化されたファイル内に保存できます。このファイルは、**caf loadcreds** コマンドを使用して多くのコンピュータに送信して適用することができます。このファイルの各エントリはコンピュータに固有であるため、このファイルを使用すると、コンピュータごとに異なる管理者パスワードを指定できます。**caf loadcreds** コマンドでは、このコマンドが実行されているローカル コンピュータのエントリのみが適用されます。

管理者として Client Automation サービスを実行

Windows では、CAF 機能により、**Client Automation** プラグインまたはサービスを特定ユーザのクレデンシアルで実行できます。ただし、管理者グループのユーザのみがサポートされており、ほかの種類ユーザでは動作しません。

たとえば、sdagent サービスなどのプラグインまたはサービスを実行する方法

1. コマンドプロンプト ウィンドウを開きます。
2. コマンドを使用して、**sdagent** にクレデンシアルを設定します。
`caf setcreds sdagent user administrator password xxx`
3. 以下のコマンドを発行し、それが機能するかどうかをテストします。
`caf start sdagent`

sdagent プログラム (**sd_jexec.exe**) が管理者として実行され、タスク マネージャに表示されます。

独自の X.509 証明書をインストール イメージに取り込む方法

CA Client Automation は、そのクライアント プロセスと、認証を要求するサービスとの間の認証用として X.509 証明書を利用します。たとえば、**Software Delivery** コンポーネントがその親のスケラビリティ サーバに接続するときには、X.509 が使用されます。

CA Client Automation インストールには、CA ルート証明書によって署名されたデフォルトの標準証明書のセットが付属しています。公開されているルート証明書は、エンタープライズ内のすべてのノードにインストールされています。

ルート証明書、基本ホスト ID (BHI) の証明書、およびアプリケーション固有の証明書をエンタープライズごとに独自に作成して、それらを導入されることを強くお勧めします。

エンド ユーザ固有の証明書の作成に関する詳細は、「[CA Client Automation セキュリティ機能 \(P. 439\)](#)」を参照してください。

cacertutil ツールを使用して新しい証明書を作成するには、少なくとも 1 つのコンポーネント (エクスプローラや **Asset Management** エージェントなど) をインストールする必要があります。cacertutil ツールは、DSM のインストールディレクトリの下に bin フォルダにあります。

独自の固有証明書を作成した後、DSM コンポーネントのインストールまたは展開を開始する前に、インストールイメージ内のデフォルトの標準証明書を新しい証明書で置き換えてください。

インストールイメージ内の証明書を置き換えると、通常どおりインストールまたは展開を開始することができます。

デフォルトの証明書 (Windows)

Windows のデフォルトの証明書は、以下のフォルダ内にあります。これらの各フォルダには、関連する証明書を含むサブフォルダ構造の **Program Files¥CA¥DSM¥bin** があります。

- AgentBHW
- AgentAM
- AgentRC
- AgentSD
- AllAgents
- サーバ
- マネージャ
- エクスプローラ

Linux および UNIX のデフォルトの証明書

Linux/UNIX のデフォルトの証明書は、以下のパッケージ ディレクトリの下、**certificates** というサブディレクトリにあります。

- エージェント
- am_agent
- basichwinv
- rc_agent (Linux のみ)
- sd_agent
- server (Linux のみ)

cfcert.ini を使用した X.509 証明書のカスタマイズ

cfcert.ini ファイルは、Client Automation によってインストールされた証明書を制御します。cfcert.ini ファイルには、インストール内の各アプリケーション グループに対応するいくつかのセクションがあります。デフォルトの cfcert.ini ファイルを以下に示します。

```
[CAF]
files=dsm_dsm_r11_root.der,basic_id.p12

[Configuration]
files=ccsm.p12

[Manager]
files=dsm_dsm_r11_cmdir_eng.p12

[Registration]
files=registration.p12

[USD.Agent]
files=dsm_dsm_r11_sd_catalog.p12

[USD.Manager]
files=dsm_dsm_r11_agent_mover.p12,dsm_dsm_r11_sd_catalog.p12


[Files]
dsm_dsm_r11_root.der=cacertutil import -i:dsm_dsm_r11_root.der -it:x509v3
basic_id.p12=cacertutil import -i:basic_id.p12
-ip:enc:uAa8VNL4DKZlUUtFk5INPnr2RCLGb4h0 -h -t:dsmcommon
ccsm.p12=cacertutil import -i:ccsm.p12 -t:csm
-ip:enc:IWhun2x3ys7y1FM8Byk2LMs56Rr8KmXQ
dsm_dsm_r11_cmdir_eng.p12=cacertutil import -i:dsm_dsm_r11_cmdir_eng.p12
-ip:enc:gYuzGzNcIYzWjHA6w542pw68E8FobJhv -t:dsm_cmdir_eng
dsm_dsm_r11_sd_catalog.p12=cacertutil import -i:dsm_dsm_r11_sd_catalog.p12
-ip:enc:wdyZd4DXpx6j5otwKY0jSa00VLLi0txQruDV0slG0lNIMZw96c85Cw -t:dsm_sdcatalog
dsm_dsm_r11_agent_mover.p12=cacertutil import -i:dsm_dsm_r11_agent_mover.p12
-ip:enc:syt0QtZteLopAt1CX0jIJJcpqBWr7G7VegY7F7udogc1c5kLIylw -t:dsm_agtmv
registration.p12=cacertutil import -i:registration.p12
-ip:enc:z5jLhmvfkaAF4DLMDp3TWu7nG8yh3dfvmN668thfrU -t:dsm_csvr_reg
babld.p12=cacertutil import -i:babld.p12 -ip:enc:TrdWglmuNCde0Afj2j3vMwywVbGnIvX
-t:babld_server
dsmpwchgnt.p12=cacertutil import -i:dsmpwchgnt.p12
-ip:enc:QWF8vknD5aZsU1j5RLzgt1NQgF5DcXj4v1vS4ewDz0A -t:ent_access
dsmpwchgdom.p12=cacertutil import -i:dsmpwchgdom.p12
-ip:enc:sqb9q02SGjbYqzIvwM7HEbx0M6UJk8Dc82EvUoDeJmE -t:dom_access
dsmpwchgrep.p12=cacertutil import -i:dsmpwchgrep.p12
-ip:enc:x90leho57IZ19zg6g97rQetHjA1461na7nhBmJl7mcc -t:rep_access
```

[Tags]

```
dsmcommon=x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US
dsm=x509cert://dsm r11/CN=Configuration and State Management,O=Computer
Associates,C=US
dsm_cmdir_eng=x509cert://dsm r11/cn=dsm directory synchronisation,o=computer
associates,c=us
dsmsdcat=x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer
Associates,C=US
dsmagtmv=x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US
dsm_csvr_reg=x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer
Associates,C=US
babld_server=x509cert://dsm r11/cn=babld server,o=computer associates,c=us
ent_access=x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US
dom_access=x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US
rep_access=x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US
```

cfcert.ini ファイルの各セクションでは、関連付けられているインストーラによってインストールする必要のある証明書が宣言されています。 インストーラは、cfcert.ini 内の関連するセクションから「files=」エントリを読み取り、cfcert.ini ファイルの [Files] セクションにあるコマンドを使用して、リストされている各証明書を順にインストールします。

たとえば、CAF (Common Application Framework) インストーラは、証明書 dsm_r11_dsm_root.der および basic_id.p12 をインストールする必要があることを検出します。 CAF インストーラは、[Files] セクションの最初の 2 行にこれらの証明書に関連付けられている cacertutil コマンドを見つけ、これらのコマンドを実行します。

[Tags] セクションを使用して、標準の証明書の URI を使用しない新しい証明書を作成することができます。 DSM マネージャ ノードをインストールする場合は、インストール コンポーネントがこのセクションを読み取って、指定された URI のセキュリティ プロファイルを設定アップします。 前にリストしたタグおよび URI は Client Automation のデフォルトで、cfcert.ini ファイルが存在しない場合に使用されます。

規約により、cfcert.ini の各セクションの「files=」エントリにリストされているファイル名は、基本の証明書ファイルの名前と同じです。 これにより、cfcert.ini 初期化ファイルの保守が簡単になります。

デフォルトの証明書を独自の証明書で置き換えるには、新しい証明署名およびパスワードを反映するよう、それぞれのセクションおよび「Files」セクションを変更します。

重要: 新しい証明書が正しいタグ名を使用してインポートされるようにしてください。タグは `-t:` スイッチで指定します。詳細および使用可能な証明書のリストについては、[「アプリケーション固有の証明書のインストール」](#) (P. 449) および [「現在の証明書」](#) (P. 625) を参照してください。

インストールの変更および修復

Client Automation の既存のインストールを変更または修復するには、セットアッププログラムを実行します。利用できるオプションは以下のとおりです。

変更

コンポーネントを追加または削除することができます。

注: 変更プロセスの終了状態を指定するようにしてください。マネージャをインストール済みで、DSM エクスプローラを追加する場合は、マネージャおよび DSM エクスプローラがチェック済みであることを確認してください。これが希望する最終状態になります。

修復

既存のインストールを修復することができます。修復機能では、ファイル、レジストリ キー、およびオリジナルのインストールのショートカットがチェックされ、それらが削除されていたり、破損している場合には、再インストールされます。

インストールの変更

既存の **Client Automation** のインストールを変更するということは、つまり、新しい機能をインストールしたり、現在インストールされている機能を削除したりすることを意味します。

インストールを変更する方法

1. 設定プログラムを実行し、[**Client Automation** のインストール] オプションを選択します。

インストーラによって、インストールがすでに存在しているかどうかを検出され、[インストール オプションの選択] ダイアログ ボックスが表示されます。

2. [変更] を選択します。

[製品の機能を選択します] ダイアログ ボックスが表示されます。

3. 選択を行い、[次へ] をクリックします。

[機能の選択] ダイアログ ボックスが表示され、使用可能なすべての機能が表示されます。インストール済みの機能が選択されています。

4. インストールする機能を選択し、削除する機能は選択を解除します。
5. インストール ウィザードの指示に従います。

操作が正常に終了すると、ただちに **CAF** サービスを再起動するか、または後で **CAF** サービスを再起動するよう指定することができます。

マネージャ ロールを変更する方法

[変更] 機能を使用して、**DSM** マネージャのロールを、ドメイン マネージャからエンタープライズ マネージャへ、またはエンタープライズ マネージャからドメイン マネージャへ変更することはできません。マネージャのロールを別のロールに変更するには、以下の手順に従います。

- [変更] 機能を使用して、マネージャをアンインストールします
- データベース プロバイダおよび管理データベース (MDB) をアンインストールします。

重要: データベース プロバイダをアンインストールする前に、「[マネージャおよび管理データベースのアンインストール \(P. 244\)](#)」を参照してください。

- [変更] 機能を使用して、新しいロールを持つマネージャをインストールします。

インストールを修復する方法

既存の **Client Automation** を修復すると、欠落しているファイルや破損しているファイル、ショートカット、および以前のセットアップのレジストリ エントリが修正されます。

インストールを修復するには、以下の手順に従います。

1. 設定プログラムを実行し、[**Client Automation** のインストール] オプションを選択します。

インストーラによって、インストールがすでに存在しているかどうかを検出され、[インストール オプションの選択] ダイアログ ボックスが表示されます。

2. [修復] を選択します。
3. インストール ウィザードの指示に従います。

Client Automation の使用中に作成されたファイル、または変更された設定は、[修復] 機能で置き換えることはできません。

インストールのアップグレード

インストールをアップグレードするとは、古いインストールをアンインストールせずに、機能またはコンポーネントを、上位のバージョンまたはビルド番号に再インストールすることです。現在の設定はすべて維持され、データベースは上書きされません。

アップグレードは、以下のいずれかを使用して実行できます。

インストール ウィザードを使用します。

セットアップ プログラムを実行すると、前のバージョンが検出されたことが通知され、アップグレードが完了します。

DSM エクスプローラおよびアップグレード用の配布パッケージを使用します。

DSM エクスプローラ内で、登録済みの **Software Delivery** パッケージを使用して、コンポーネントを配布することができます。ターゲット コンピュータに旧バージョンが存在している場合は、**Software Delivery** 機能が自動的にアップグレードを実行します。

展開ウィザードを使用します。

DSM エクスプローラ内でインフラストラクチャ展開ウィザードを使用して、ターゲット コンピュータにパッケージを配布し、インストールできます。ターゲット コンピュータにすでに以前のバージョンがインストールされている場合は、[展開: エージェントの設定] ウィザード ページからアップグレードを要求する必要があります。ターゲット コンピュータでのアップグレードを要求するためには、入力フィールド [追加の Windows インストール オプション] で、以下の設定を入力する必要があります。

```
REINSTALL=ALL REINSTALLMODE=vomus
```

MSI パッケージを直接呼び出します。

MSI パッケージを直接使用している場合は、コマンドラインに以下のパラメータを追加する必要があります。

```
REINSTALL=ALL, REINSTALLMODE=vomus
```

例

```
msiexec.exe /i"N:¥DSM_12_0_1234_1_DVD¥WindowsProductFiles_x86¥AgentSD¥agtsd.msi"
```

```
REINSTALL=ALL
```

```
REINSTALLMODE=vomus /l*v "%temp%¥ITRMupdateSDagent.log"
```

Client Automation のアンインストール

Client Automation または Client Automation のインストールのパーツをアンインストールする方法については、以下のセクションで説明しています。

- [Windows での Client Automation のアンインストール](#) (P. 263)
- [Linux および UNIX 上の Client Automation のアンインストール](#) (P. 265)

Windows での Client Automation のアンインストール

Client Automation またはその一部をアンインストールする場合、以下のオプションのいずれかを使用できます。

- Windows の [コントロール パネル] で [プログラムの追加と削除] の機能を選択します。

この機能を使用すると、Client Automation 全体、またはそのコンポーネントを 1 つ削除することができます。インストール済みのソフトウェアのリストから、該当する項目を選択し、[変更と削除] ボタンをクリックします。

- Client Automation インストール ウィザードを使用します。

setup.exe を実行します。インストール ウィザードが起動し、その指示に従ってインタラクティブにアンインストールを進めることができます。[Client Automation のインストール] を選択します。これ以降に表示されるダイアログ ボックスの 1 つで、[削除]、[変更]、[修復] のオプションが提示されます。

[削除] オプションを選択すると、setup.exe が実行されたシステムから Client Automation インストールが完全に削除されます。

[変更] オプションを選択すると、インストーラによって管理されているすべてのコンポーネントおよび機能のリストが表示されます。現在ローカルシステムにインストールされている機能には、チェック マークが付けられています。アンインストールするコンポーネントまたは機能のチェックをオフにします (チェックマークが消えます)。このダイアログ ボックスを終了すると、指定した機能はアンインストールされますが、Client Automation のインストールは削除されません。

- コマンドラインで、適切な製品コードを使用して、msiexec /x を実行します。

削除するコンポーネントは、その製品コード (P. 264) で指定します。msiexec コマンドでオプション /qn を使用すると、自動モードでのアンインストールを指定することができます。

Windows では、セットアッププログラムを使用してアンインストールを行うと、すべての Client Automation 製品と言語パッケージがアンインストールされます。Windows の [コントロール パネル] で [プログラムの追加と削除] または msiexec コマンドライン ツールを使用して単一の MSI パッケージをアンインストールすると、そのほかの MSI パッケージはアンインストールされません。

注: Windows でアンインストールを終了しても、いくつかのファイル、フォルダ、およびレジストリ キーは残されます。アンインストールが完了した後に、手動で DSM のディレクトリを削除してください。

Client Automation の製品コード

Client Automation のインストール可能なコンポーネントは、以下のように個別の製品コードによって識別されます。

基本インベントリ エージェント (ENU および多言語)

{501C99B9?1644?4FC2?833B?E675572F8929}

Asset Management Agent (ENU および多言語)

{624FA386-3A39-4EBF-9CB9-C2B484D78B29}

Data Transport Service エージェント (ENU および多言語)

{C0C44BF2?E5E0?4C02?B9D3?33C691F060EA}

Remote Control エージェント (ENU および多言語)

{84288555?A79E?4ABD?BA53?219C4D2CA20B}

Software Delivery エージェント (ENU および多言語)

{62ADA55C?1B98?431F?8618?CDF3CE4CFEEC}

エージェント言語パッケージ DEU:

{6B511A0E-4D3C-4128-91BE-77740420FD36}

エージェント言語パッケージ FRA:

{9DA41BF7-B1B1-46FD-9525-DEDCCACFE816}

エージェント言語パッケージ JPN:

{A4DA5EED-B13B-4A5E-A8A1-748DE46A2607}

エージェント言語パッケージ ESN:

{94163038-B65E-45BE-A70C-DC319C43CFF2}

エージェント言語パッケージ KOR:

{2C300042-2857-4E6B-BC05-920CA9953D2C}

エージェント言語パッケージ CHS:

{2D3B15F5-BBA3-4D9E-B7AB-DC2A8BD6EAD8}

ドキュメント:

{A56A74D1?E994?4447?A2C7?678C62457FA5}

エクスプローラ:

{42C0EC64?A6E7?4FBD?A5B6?1A6AD94A2D87}

マネージャ

```
{E981CCC3?7C44?4D04?BD38?C7A501469B37}
```

MasterSetup:

```
{C163EC47?55B6?4B06?9D03?2A720548BE86}
```

スケーラビリティ サーバ

```
{9654079C-BA1E-4628-8403-C7272FF1BD3E}
```

DMPprimer:

```
{A312C331-2E7A-42E1-9F31-902920C402EE}
```

msiexec および製品コードを使用したアンインストールの例

以下の例では、Asset Management エージェントが自動モードで削除され、ドライブ **c** の **logs** フォルダ内のログ ファイル **rmvamagt.log** に削除情報が書き込まれます。

```
msiexec /x {A302890B-3180-455B-A958-6DDFAE9F4B00} /!v "c:¥logs¥rmvamagt.log" /qn
```

Linux および UNIX 上の Client Automation のアンインストール

Linux または UNIX 上の Client Automation またはそのパーツは、以下のいずれかのオプションを使用してアンインストールすることができます。

./setup.sh

インストール DVD から **setup.sh** を実行し、セットアップ ダイアログ ボックスで [アンインストール] を選択します。

lsm -e *prodname* [-s]

この **lsm** のコマンド バージョンを Client Automation コマンドラインから実行します。lsm コマンドでは、製品またはコンポーネントは **prodname** で指定されます。オプション **-s** は、自動（サイレント）アンインストール モードを指定します。

以下の例では、Client Automation が自動（サイレント）モードで完全にアンインストールされます。

```
lsm -e ca-dsm -s
```

以下の例では、DMPprimer がアンインストールされます。

```
lsm -e ca-dsm-dmprimer-standalone
```

Linux/UNIX インストーラ (ism) コマンドで変数 *prodname* の値として使用できる製品またはコンポーネントの名前を以下の表に示します。

製品名/コンポーネント名	説明
ca-dsm	CA Client Automation
ca-dsm-dmprimer-standalone	DMPprimer (Client Automation のインフラストラクチャ展開コンポーネントを使用する場合にのみインストールされます)
ca-dsm-SMPackager	Linux および UNIX 対応のソフトウェア パッケージャ

エージェントのアンインストールに関する一般注意事項

任意のエージェントのエージェント基本パッケージをアンインストールすると、それに関連するすべての言語パッケージもアンインストールされます。

言語パッケージをアンインストールしても、エージェント基本パッケージには影響はないので、言語パッケージはいつでも削除できます。

スタンドアロンの言語パッケージをアンインストールし、設定ストア (comstore) 内の現在の言語がそのアンインストールした言語に設定されていた場合、comstore 内の設定パラメータの値 *itrm/common/localization/language* は *enu* に変わります。その他の場合は、パラメータ値は変更されません。

言語パッケージは、アンインストール時に **Software Delivery** とインフラストラクチャ展開から自身の登録を解除します。

Software Delivery を使用した Windows エージェント DSM パッケージのアンインストール

DSM パッケージは、ベース パッケージおよびカスタム パッケージの 2 つのクラスに分けられます。カスタム パッケージはベース パッケージを「含み」、ベース パッケージは「最小構成単位」となります。インストール時または検出時に、ベース パッケージが登録され、「インストール済みソフトウェア」としてリスト表示されます。カスタム パッケージが **Software Delivery** を使用して配布およびインストールされている場合は、カスタム パッケージのインストール記録が作成されます。ただし、このカスタム パッケージインストール記録は、手動インストールまたはインフラストラクチャ展開を使用したインストールでは作成されません。

Software Delivery を使用して DSM パッケージをアンインストールする場合は、ベース パッケージのみをアンインストールするようにしてください。ここでは、ベース パッケージのアンインストール順序が重要です。最初に、エージェント言語パッケージ、次に DCS アドオン、その後 **Asset Management** または **Remote Control**、あるいはそれら両方をアンインストールします。**Software Delivery** エージェントのアンインストールは最後に行う必要があります。これを実行する 1 つの方法は、各段階のジョブを設定した **Software Delivery** アンインストール ジョブ コンテナを作成することです。ベース パッケージがアンインストールされたら、**DSM** エクスプローラを使用してカスタム パッケージのインストール記録を消去してください。

Secure Socket Adapter および **DMPimer** のようなプラグインは消去されませんのでご注意ください。これらのプラグインを消去するには、ターゲット コンピュータ上に残っているすべての **Client Automation** コンポーネントを、[プログラムの追加と削除] を使用して手動でアンインストールします。

第 5 章：インフラストラクチャ展開

以下では、インフラストラクチャ展開フェーズ、展開管理の概念、およびコマンドラインによって、または継続ディスカバリをトリガして、インタラクティブに展開を実行する方法について説明します。さらに、いくつかの展開の特殊な側面、前提条件、およびツールについても考慮しています。

このセクションには、以下のトピックが含まれています。

[インフラストラクチャ展開の概要](#) (P. 270)

[DSM エクスプローラを使用した展開](#) (P. 285)

[コマンドラインを使用した展開](#) (P. 286)

[継続ディスカバリによってトリガされる展開](#) (P. 287)

[展開パッケージ](#) (P. 288)

[dsmpush ツール](#) (P. 290)

[Client Automation インフラストラクチャを自動展開するための前提条件](#) (P. 291)

[インフラストラクチャ展開で使用する FTP サーバの変更の詳細](#) (P. 294)

[エージェントの展開を有効にする Windows XP の設定](#) (P. 295)

インフラストラクチャ展開の概要

展開管理 (DM) は、CA Client Automation 内のインフラストラクチャ展開ソリューションです。DM を使用すると、異機種が混在しているエンタープライズ内の数多くのターゲット コンピュータに対して、ソフトウェア コンポーネントのインフラストラクチャ展開を簡単に行うことができます。そのため、管理者は、手動でログオンして、インストール イメージを転送し、インストール プロセスを実行して、そのインストールの結果を各ターゲット コンピュータで順に監視していく必要はありません。

DM の利点は、以下のとおりです。

- ターゲットのさまざまな動作環境へのインフラストラクチャの自動展開。
- 同期展開。つまり、展開を開始すると、展開済みコンポーネントは、それ以上ユーザがなくてもインストールされ、実行されます。同期展開が不可能な場合は、非同期展開が行われます。この場合、ユーザがログオンするか、または再起動して、インストールを完了する必要があります。
- 拡張ログおよびレポート機能。DM では展開の進捗状況が監視され、適切なステータス情報が表示されます。
- 現在のエンタープライズ インストールの要求を満たすセキュリティ機能。ネットワーク伝送中に第三者が機密データにアクセスできないようにするために、または機密データが永続ストレージに保存されないようにするために、適切な認証技術および暗号化技術が使用されます。
- 展開時の大量のワークロードを展開クライアント インターフェースから分離する展開マネージャ。必要に応じて、複数の展開マネージャを単一のターゲット コンピュータに展開することができます。
- 新しく検出されたシステムへの自動展開。管理者は、コンピュータが初めてネットワークに追加されたときに特定のシステムへ特定のソフトウェアを展開するルールを定義できます。

通常の Client Automation インフラストラクチャ展開フェーズ

インフラストラクチャ展開は、以下に示す主要フェーズで構成されます。

- 本社でのインタラクティブなマネージャのインストール
- 展開ウィザードを使用した、このマネージャに対するスケーラビリティ サーバの定義、およびスケーラビリティ サーバの展開
- 展開ウィザードを使用した、スケーラビリティ サーバに接続されているエージェントの展開
- 新しく検出されたシステムへの自動展開

展開管理の概念

展開操作が要求されると、展開マネージャは、最初に比較的小さな「プライマ」パッケージをターゲット コンピュータに送信します。

プライマ パッケージは、ターゲットのオペレーティング システムおよびインストールされているソフトウェアに応じて、さまざまな方式の内の 1 つを使用してプッシュされます。

プライマは、常にリモートでプッシュできるわけではありません。たとえば、ネットワーク セキュリティの設定でリモート プッシュを実行できないようになっている場合は、プッシュできません。ただし、そのような場合でも、ターゲット コンピュータにプライマを手動でインストールすることができます。

プライマをインストールすると、これにより、実際の展開パッケージ データがターゲット コンピュータに転送され、インストールが実行されます。それ以降、同じターゲット コンピュータに対して展開を実行する場合は、常に既存のプライマインストールを使用することができます。

展開マネージャは、すべての展開操作を制御し、ジョブ ステータスを処理します。

展開クライアント（展開ウィザードおよび `dmsweep` コマンドライン インターフェース）は、展開マネージャとの通信に API を使用します。これらは、DSM エクスプローラとともにインストールされるので、必要に応じてマネージャ以外のコンピュータ上で実行できます。

多数のエージェントを展開するときのネットワーク使用量を減らすために、スケーラビリティ サーバで展開パッケージを「ステージング」できます。

スケーラビリティ サーバを使用してパッケージを転送するプロトコル

DMDeploy は、スケーラビリティ サーバを使用した展開時に、以下のプロトコルを使用してパッケージをターゲット コンピュータに転送します。

Windows ネットワーク共有

スケーラビリティ サーバとターゲット コンピュータが Windows 上にある場合、このメカニズムを使用します。

SSH/SFTP

スケーラビリティ サーバかターゲット マシンのいずれかが Linux または UNIX 上にある場合、このメカニズムを使用します。

Telnet/FTP

スケーラビリティ サーバかターゲット マシンのいずれかが Linux または UNIX 上にある場合、このメカニズムを使用します。

これらの転送メカニズムの詳細については、「[Client Automation インフラストラクチャを自動展開するための前提条件](#) (P. 291)」を参照してください。

インフラストラクチャ展開のコンテキストでのスケーラビリティ サーバの使用

多数のエージェントを展開するときのネットワーク使用量を減らすために、スケーラビリティ サーバで展開パッケージを「ステージング」できます。スケーラビリティ サーバで展開ペイロードパッケージを使用可能にするには、[スケーラビリティ サーバにパッケージをステージング] オプションを指定して、ペイロードをスケーラビリティ サーバに展開します。スケーラビリティ サーバに保存されているパッケージを後で展開する場合は、展開ペイロードを選択するときに、[スケーラビリティ サーバからパッケージを転送] オプションを有効にします。

インフラストラクチャ展開とともにスケーラビリティ サーバを使用すると、ネットワーク設定に影響します。通常、スケーラビリティ サーバは、エンタープライズネットワークの「閉じた」場所にあるターゲット コンピュータにエージェントを展開するために使用されます。つまり、スケーラビリティ サーバとエージェント コンピュータ間では、ネットワーク スピードは比較的速くなります。

インフラストラクチャ展開でスケーラビリティ サーバを使用する場合、以下のよう
に、数多くの管理タスクを注意して実行する必要があります。

- Telnet/FTP 転送メカニズムによって、Linux スケーラビリティ サーバを使用して、Windows ターゲット コンピュータに展開するために、Windows ターゲット コンピュータで Telnet を有効にする必要があります。Windows 2003、Windows XP、またはそれ以降のオペレーティング システムが稼働しているコンピュータ上では、[コントロール パネル] - [管理ツール] - [サービス] ダイアログ ボックスを使用して Telnet サービスを有効にし、開始する必要があります。
- Telnet/FTP 転送メカニズムによって、スケーラビリティ サーバを使用して Linux または UNIX ターゲット コンピュータに展開する場合、スケーラビリティ サーバで FTP サーバが使用可能になっている必要があります。また、マネージャはターゲット コンピュータへの接続に Telnet を使用し、スケーラビリティ サーバへは FTP を使用してパッケージを取り出すため、ターゲット コンピュータでは Telnet サーバが必要になります。

上記に加えて、使用中のスケーラビリティ サーバを Windows マシン上で実行している場合は、以下の設定タスクをスケーラビリティ サーバ上で実行し、インフラストラクチャ展開で使用される代替の FTP サイトを設定する必要があります。Client Automation エージェント パッケージが保存されるステージング場所を共有する場合は、その他の FTP エリアとのセキュリティ上の問題を避けるために、別々の FTP サイトが必要です。

- [コントロール パネル] - [管理ツール] を開き、[Internet Information Services (IIS) マネージャ] を選択します。
- [FTP サイト] ノードを右クリックし、[新規] - [FTP サイト] を選択して、FTP サイト作成ウィザードを実行します。
- ウィザードを実行し、新しいサイトの説明として、「ITCM FTP サイト」と入力します。[FTP サイトのホーム ディレクトリ] ウィザード ページが表示されるまで、ウィザードで与えられるデフォルト値を選択します。このページでは、DMPrimer インストール場所のディレクトリを指定する必要があります (ITCM インフラストラクチャ展開エージェント パッケージがこのディレクトリにステージングされるため)。すでに DMPrimer をインストールしている場合は、[参照] ボタンを使用してディレクトリを参照します。デフォルトでは、DMPrimer は Program Files¥CA¥DSM¥DMPrimer にインストールされます。FTP サイトのディレクトリを選択したら、デフォルトのオプションを選択してウィザードを続行し、[完了] ボタンをクリックします。

Linux ターゲットを展開するのに Windows スケーラビリティ サーバを使用する場合、Client Automation FTP サイトが開始されている必要があることに注意します。デフォルトの FTP サイトなど、その他の FTP サイトが停止されているのを確認してください。そうしないと、展開が失敗します。

- スケーラビリティ サーバで FTP を使用する場合、接続のために必要なユーザ クレデンシャルの指定に注意する必要があります。スケーラビリティ サーバ /FTP サーバにパッケージをステージングする場合は、スケーラビリティ サーバへの書き込み権限があるユーザのクレデンシャルを指定する必要があります。スケーラビリティ サーバ/FTP サーバからパッケージを展開する場合には、通常、パッケージへアクセスするために匿名ユーザを使用します。
- Telnet/FTP を使用した展開が必要な場合は、マネージャのインストール時に FTP サーバの詳細が提供され、DMPrimer パッケージが指定したサーバにアップロードされます。FTP サーバは、通常、スケーラビリティ サーバと同じコンピュータに配置されます。

単一のインフラストラクチャ展開マネージャに対して複数の FTP サーバを使用する場合、たとえば、各コンピュータ上で FTP サーバが実行されている複数のスケーラビリティ サーバがある場合は、いくつかの手動設定ステップを行ってから、インストール時に設定されなかった代替 FTP サーバを展開で使用する必要があります。

FTP の詳細を変更するために、新規 FTP サーバの詳細を使用して 'dmdeploy ftpinfo' コマンドを実行して、プライマ パッケージおよび dmkeydat.cer ファイルを FTP サーバ上の対応する場所にコピーする必要があります。これにより、展開マネージャでは、Telnet/FTP を使用した展開に対してこの FTP サーバが使用されます。これらのステップについては、「[インフラストラクチャ展開で使用する FTP サーバの変更の詳細 \(P. 294\)](#)」で説明されています。

- インフラストラクチャ展開に Windows のスケーラビリティ サーバを使用している場合、Windows では同時接続に制限があることに注意してください。接続制限に到達した場合、一部のジョブが失敗する可能性があります。その場合、「現時点のパッケージの取得に失敗しました。スケーラビリティ サーバの接続限度に達しました。再試行してください」というメッセージが表示されます。設定パラメータ「展開スレッドの制限」を使用して、インフラストラクチャ展開マネージャによって実行される同時展開の数を制御します。設定パラメータのデフォルト値は 10 です。Windows で実行されているスケーラビリティ サーバで展開する場合、この値を変更できます。
- 使用される Telnet のバージョンが IPv6 プロトコルをサポートしていないと、純粋な IPv6 環境では展開が失敗します。
- 使用される FTP のバージョンが IPv6 プロトコルをサポートしていないと、純粋な IPv6 環境では Linux または UNIX ターゲット コンピュータへの展開が失敗します。

関連項目：

[スケーラビリティ サーバを使用してパッケージを転送するプロトコル \(P. 272\)](#)

スケーラビリティ サーバのインフラストラクチャ展開コンテンツの監査

インフラストラクチャ展開を使用すると、ユーザは展開コンテンツが含まれるネットワーク内のスケーラビリティ サーバを監査したり、各スケーラビリティ サーバに存在する展開パッケージのリストを取得したりできます。

展開ウィザードのナビゲーション中にスケーラビリティ サーバを選択すると、そのスケーラビリティ サーバで使用可能なインフラストラクチャ展開パッケージのリストが表示されます。「`dmsweep sspack`」コマンドを使用して、スケーラビリティ サーバのコンテンツも表示できます。

展開管理プロセス

展開管理 (DM) を実行する場合、展開プロセスの以下の主要な手順を実行します。

1. 管理者のコンピュータから、インフラストラクチャ展開クライアント コンポーネント (展開ウィザードまたは `dmsweep` コマンド) によって、複数のターゲット コンピュータのリストにエージェントをインストールする要求が DM マネージャ (DMDeploy) に対して出されます。展開マネージャは、クライアントに対してリモートのコンピュータ上で実行されている場合があります。ターゲットのリストは、明示的なマシン名または IPv4 アドレスから構成されるか、Windows ドメイン、LDAP ディレクトリ、または Client Automation クエリなどの「コンテナ」ソースから取得される場合があります。

各ターゲット コンピュータに継承される展開の場合、ターゲット名が明示的に入力されているかコンテナから取得されているかにかかわらず、展開マネージャ コンピュータで表示されるときに、ターゲットのアドレスで解決されるのに適切なターゲット名であることが重要です。たとえば、ディレクトリから取得されるターゲットのリストが完全修飾名 (ネットワーク ドメイン名を持つ) ではない場合、特定のネットワーク設定では展開を継続できないことがあります。

2. **DMPrimer** がターゲット コンピュータにインストール済みであるかどうかを確認されます。インストールされていない場合は、最初にターゲット コンピュータに **DMPrimer** がインストールされます。**DM** マネージャでは、**DMPrimer** インストールパッケージの配信が試行されます。どのような方法を使用して配信されるかは、ターゲットの動作環境、およびその環境で有効になっているセキュリティによって異なります。**DMPrimer** イメージがターゲット コンピュータにコピーされた後、インストールが開始されます。

一部のオペレーティング システムには **DMPrimer** インストールのリモート呼び出しの方法がないため、再起動などの重要なオペレーティング システムのイベントが発生したときに、インストーラがインストールされるようにする必要があります場合があります。インストールの完了を示すメッセージは、指定がされていない将来のある時点で非同期的に受信されるため、このようなインストールは非同期インストールと呼ばれています。この場合、**DMPrimer** インストールは手動で実行することもできます。

3. **DMPrimer** インストーラによって、インストーラ自体および **CA** メッセージ キューイング (**CAM**) コンポーネントがターゲット コンピュータにインストールされます。インストール中、ターゲット コンピュータ上の **DMPrimer** の **FIPS** モードはマネージャの **FIPS** モードに依存します。マネージャは、インストールパラメータとして **FIPS** モードを渡します。このパラメータも **dmprimer.cfg** ファイルで更新されます。このファイルは、**DMprimer** インストールの一部です。

ただし、起動時には、**DMPrimer** はターゲット コンピュータ上のエージェント設定ポリシーから **FIPS** モードを読み取ります。成功した場合、プライマはエージェントの **FIPS** モードで **dmprimer.cfg** ファイルを更新し、そのモードで初期化を行います。ターゲット上にインストールされているエージェントがない場合、**DMPrimer** は **dmprimer.cfg** ファイルで指定されたモードで初期化を実行します。

注: 多くのオペレーティング システムでは、**DMPrimer** インストールは高度な権限で実行される必要があります。

4. **DMPrimer** がインストールされ、**DMDeploy** がターゲット コンピュータから「インストール完了」シグナルを受信すると、パッケージ展開を開始することができます。**DMDeploy** マネージャによって以前に **DMPrimer** がインストールされており、その **DMPrimer** を使用して認証される場合、**DMDeploy** マネージャでは、ユーザ名またはパスワードを再度提供しなくてもパッケージを展開できます。このような展開は、パブリック キーとプライベート キーを使用した認証によって行われます。**DMPrimer** が存在する場合でも、展開マネージャで **DMPrimer** を再転送およびインストールする行うことができます。これには、**DSM** エクスプローラを使用して、「プライマを常に展開」設定ポリシーを設定します。

DSM エクスプローラからの展開マネージャの使用については、展開ウィザードのオンラインヘルプを参照してください。

柔軟性のある展開ターゲットの指定

展開ターゲットの指定に柔軟性を持たせるため、ターゲット クレデンシアル ファイルが導入されました。管理者は、ターゲット クレデンシアル ファイルを使用して、個別のターゲット システムのリストまたはターゲット システムのグループを接続クレデンシアルに基づいて作成したり保持することができます。

ターゲット クレデンシアル ファイルを使用すると、ユーザは実際の展開ジョブを開始する前に、展開を「オフライン」で計画できます。クレデンシアル ファイルのファミリー、たとえば、異なる企業部門に関連するファイルのファミリーを作成することによって、展開を異なるネットワークの「領域」に指定できます。

ターゲット クレデンシアル ファイルは、**dmsweep** コマンド (**/targetcred** オプションを使用) およびインフラストラクチャ展開ウィザードの両方で使用できます。

DMPriemer インストールへ受け渡すオプション

DMPriemer インストールのオプションを指定できます。この指定によって、たとえば、標準ではない場所へ DMPriemer をインストールできます。これは、対象のコンピュータで行う **Client Automation** コンポーネント以降のすべてのインストールでは、DMPriemer のインストールにより最初に設定された場所の設定を使用する必要があるため、共通の要件です。したがって、**Client Automation** ソフトウェアでデフォルトではないインストール場所を使用する必要がある場合、特定のターゲット コンピュータに最初に展開するときに、以下のオプションを使用して、DMPriemer インストール場所を設定する必要があります。

dmsweep コマンド行 (**/primerargs** オプションを使用) および展開ウィザード ([エージェントの設定] ページの「詳細オプションの表示」を使用) の両方を使用して、インストール オプションを入力できます。

DMPriemer を標準ではない場所にインストールするには、DMPriemer インストールに以下の引数を受け渡す必要があります。

■ Windows ターゲット コンピュータへの展開の場合

CA=x:¥NewProductPath

CASHCOMP=x:¥NewSharedArea

Linux または UNIX ターゲット コンピュータへの展開の場合

/RCA_DSM_BASEDIR=/opt/NewProductPath /RCASHCOMP=/opt/NewSharedArea

デフォルトでは、DMPrimer インストールはマネージャと同じ FIPS モードを使用します。以下のパラメータを使用して、デフォルト値を無効にできます。

Windows ターゲット コンピュータ :

```
FIPS_MODE=1 // (FIPS 推奨)
FIPS_MODE=2 // (FIPS のみ)
```

Linux または UNIX のターゲット コンピュータ :

```
/RITCM_FIPS_MODE=1 // (FIPS 推奨)
/RITCM_FIPS_MODE=2 // (FIPS のみ)
```

Windows インストール オプションの追加に関する注意事項

インフラストラクチャ展開ウィザードの [エージェントの設定] ページを使用して、1 つ以上のスペースが含まれた Windows の追加インストール オプションを展開ジョブに渡す場合、パラメータ値を引用符で囲む必要があります。追加する Windows インストール オプションごとに、値は二重引用符で囲む必要があります。たとえば、次のようになります。

```
CA="C:¥Program Files¥mydir" CASHCOMP="C:¥Program Files¥mydir¥sharedComps"
```

コマンドラインでは、以下の例のように dmsweep を使用して個別のパラメータをカンマで区切り、二重引用符で保護する必要があります。

```
/pri "CA=¥"C:¥Program Files¥CA¥test¥" CASHCOMP=¥"C:¥Program Files¥CA¥test¥""
```

IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項

IPv6 を使用して CA Client Automation を展開する場合は、以下の注意事項を熟読してください。

- IPv6 環境でインフラストラクチャ展開を使用するには、最初に以下の条件を満たす必要があります。
 1. DSM マネージャで、以下のレジストリ キーを 1 に設定する必要があります。

HKLM¥System¥CurrentControlSet¥Services¥smb¥Parameters¥IPv6EnableOutboundGlobal (REG_DWORD)
 2. スケーラビリティ サーバの 2 つのホット フィックス更新を適用します。
 - <http://support.microsoft.com/kb/947369/en-us>
 - <http://support.microsoft.com/kb/950092/en-us>
 3. ターゲット マシンのホスト名は、グローバル IPv6 アドレスに解決される必要があります。

また、IPv6 アドレスの逆引きルックアップが同じホスト名に解決されることを確認してください。
 4. インフラストラクチャ展開設定ポリシーのオプション [ホスト名の使用] を True に設定する必要があります。

注: IPv6 環境で、インフラストラクチャ展開を使用してスケーラビリティサーバ経由でソフトウェアを任意の Windows 2003 マシンに展開するには、上記の手順 1 ～ 3 を目的の Windows 2003 ターゲットで実行する必要もあります。

IPv6 のみのネットワークでこれらの条件が満たされていない場合は、DMPrimer パッケージを手動でインストールする必要があります。詳細については、「[インフラストラクチャ展開プライマ ソフトウェアの手動インストール \(P. 280\)](#)」を参照してください。

- インフラストラクチャ展開および継続ディスクバリでは、展開がサポートされるのは IPv4 アドレス範囲までです。

インフラストラクチャ展開プライマ ソフトウェアの手動インストール

何らかの理由でターゲット コンピュータへの自動展開が不可能な場合でも、プライマ ソフトウェアを手動でターゲット コンピュータにインストールして、インフラストラクチャ ソフトウェアを展開できます。この展開は、物理的にプライマ パッケージをインストールするか、またはログイン スクリプトを使用してインストールを実行するかのいずれかによって可能です。

プライマ ソフトウェア自体をインストールし、セキュリティ キーも一緒にインストールします。このキーは、インフラストラクチャをターゲット コンピュータに展開するために使用する展開マネージャによって生成されます。

DMprimer インストーラによって、プライマ用の FIPS モードを指定するオプションが提供されます。インストール後に FIPS モードを変更する場合は、dmprimer.cfg ファイル内の FIPS_MODE 設定を更新します。ただし、起動時には、DMPrimer はターゲット コンピュータ上のエージェント設定ポリシーから FIPS モードを読み取ります。成功した場合、プライマはエージェントの FIPS モードで dmprimer.cfg ファイルを更新し、そのモードで初期化を行います。ターゲット上にインストールされているエージェントがない場合、DMPrimer は dmprimer.cfg ファイルで指定されたモードで初期化を実行します。

Windows での展開プライマ インストール

Windows で動作しているターゲット コンピュータでの展開プライマのインストールには、以下のアクションが必要です。

- **Client Automation** インストール メディア (DVD) をターゲット コンピュータで利用できるようにするか、プライマ設定ファイルをターゲット コンピュータに手動でコピーします。

プライマ設定ファイルは、インストール メディアに以下のように保存されています。

¥WindowsProductFiles_x86¥DMPrimer¥dmsetup.exe

- ターゲット コンピュータ上で dmsetup.exe を実行して、プライマをインストールします。

Linux または UNIX での展開プライマ インストール

Linux または UNIX ターゲット コンピュータでの展開プライマのインストールには、以下のアクションが必要です。

- **Client Automation** インストール メディア (DVD) をターゲット コンピュータで利用できるようにするか、プライマ インストール イメージをターゲット コンピュータに手動でコピーします。

プライマ インストール イメージは、インストール メディアの以下のディレクトリに格納されています。

```
/LinuxProductFiles_x86/dmprimer
```

- ターゲット コンピュータ上のプライマ インストール イメージが含まれるディレクトリに移動して、以下のインストール コマンドを実行し、プライマをインストールします。

```
# sh installdmp
```

展開管理証明書のプライマ インストールへの提供

展開マネージャは、ターゲット コンピュータ上のプライマが展開パッケージを受け取る前にターゲット コンピュータに転送する必要がある証明書を生成します。展開証明書ファイルは「dmkeydat.cer」と呼ばれます。

証明書ファイルの場所は、インストール時に設定されます。証明書ファイルをより安全なエリア、またはフェールオーバー ソリューションを提供する 2 つのマネージャが共有する場所へ格納する場合は、別のファイルの保存場所を設定します。後者の場合、証明書を共有すると、展開マネージャがいずれかのマネージャから配信された DMPprimer コンポーネントと通信できるようになり、認証クレデンシャルを再度提供する必要もありません。

Windows では、展開証明書は以下のディレクトリに保存されています。

```
%Program Files%\CA\DSM\DMDeploy
```

この証明書は、ターゲット コンピュータのプライマ インストール フォルダにコピーする必要があります。このフォルダは、デフォルトでは以下の場所にあります。

```
%Program Files%\CA\DSM\DMPrimer
```

Linux および UNIX では、展開証明書は以下のディレクトリに保存されています。

```
/opt/CA/DSM/DMDeploy
```

この証明書は、ターゲット コンピュータのプライマ インストール フォルダにコピーする必要があります。このフォルダは、デフォルトでは以下の場所にあります。

```
/opt/CA/DSM/dmprimer/bin
```

エージェント パッケージの展開

Client Automation エージェントの展開中にネットワークを介して転送されるデータの量を低減するために、Client Automation では、英語のみをサポートするエージェント パッケージと、サポートされるすべての言語のエージェントが含まれるパッケージ（多言語エージェント パッケージ）が提供されています。

製品のインストール DVD の製品ファイル フォルダに、各エージェント パッケージが格納されています（例：WindowsProductFiles_x86）。

英語のみのパッケージには、「_ENU」というサフィックス が付けられています（例：AllAgents_ENU）。多言語パッケージには、特にサフィックスは付いていません。

ソフトウェア パッケージ ライブラリでは、ENU パッケージには「（英語のみのエディション）」のサフィックスが付加され、多言語エージェント パッケージには特別な識別子はありません。

インフラストラクチャ展開ウィザードでは、ENU パッケージには「（英語のみのエディション） ENU」というマークが付加され、多言語エージェント パッケージにはサフィックス NLS（ENU、DEU、FRA、JPN）が付加されます。

インストール時に、英語のみのパッケージ、多言語エージェント パッケージ、またはその両方を Software Delivery ライブラリとインフラストラクチャ展開パッケージ フォルダにインポートするかどうかを選択します。

いずれか一方のパッケージ（たとえば、英語のエージェント パッケージ）のみを選択し、後で多言語エージェント パッケージを追加する場合は、dsmPush コマンドを実行して、選択したエージェント パッケージを展開する必要があります。

ターゲット コンピュータへの多言語エージェント展開では、特に指定されている言語はありません。代わりに、インストールはターゲット コンピュータのシステム言語で実行されます。ターゲット コンピュータへの展開時に、インストール言語を明示的に指定するには、インフラストラクチャの展開ウィザードの「追加の ... インストール オプションを入力してください」というフィールドに DSM_LANGUAGE オプションを入力します。このオプションは、以下のように指定する必要があります（lang には、ターゲット コンピュータのインストール言語を指定します。有効な値は、enu、deu、fra、jpn、chs、esn、kor のいずれかです）。

DSM_LANGUAGE=lang （Windows の場合）

/RDSM_LANGUAGE=lang （Linux および UNIX の場合）

言語設定を指定しない場合は、システムのデフォルト ロケールが使用されます（そのような言語 パッケージが利用できる場合）。システムのデフォルト ロケールがサポートされていないロケールの場合は、インストーラが自動的に `enu`（英語（米国））を選択します。

また、`dmsweep` コマンドラインを使用してターゲット コンピュータにパッケージを展開するときに、言語パラメータを指定する場合があります。その場合は、`pparams` オプションを使用して、`Client Automation` の操作で使用される言語を指定します。

例：以下のコマンドラインを使用して、ドイツ語版の Windows エージェントを展開します。

この例では、ドイツ語版 Windows エージェントのパッケージ番号は 3 です。

```
dmsweep deploy /ip targetcomputer /pn 3 /pparams servername,/DSM_LANGUAGE=deu
```

注： `DSM_LANGUAGE` などの追加のインストール オプション（「プロパティ」とも言います）およびその値の詳細については、「`Client Automation` のインストール」の章の「コマンドラインを使用した `Client Automation` のインストール」を参照してください。

デフォルトでは、エージェント パッケージはすべてマネージャと同じ **FIPS** モードでインストールされます。以下のパラメータを使用して、デフォルト値を無効にできます。

Windows ターゲット コンピュータ：

```
FIPS_MODE=1 // (FIPS 推奨)
```

```
FIPS_MODE=2 // (FIPS のみ)
```

Linux または UNIX のターゲット コンピュータ：

```
/RITCM_FIPS_MODE=1 // (FIPS 推奨)
```

```
/RITCM_FIPS_MODE=2 // (FIPS のみ)
```

Windows Vista および Windows 2008 コンピュータへの展開

Windows Vista または Windows 2008 オペレーティングシステムが稼働するターゲット コンピュータのファイアウォールが無効（オフ）になっていて、そのコンピュータへの展開に失敗する場合は、値が 1 になるように、以下のレジストリ変数を作成または設定する必要があります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
```

これが必要なのは、Windows Vista または Windows 2008 におけるユーザ アカウント管理（UAC）が、ローカルユーザに対して管理権限を自動的に付与しないためです。これは、ローカルユーザが管理者グループのメンバであっても必要です。

注: この値を設定すると、結果的に UAC アクセス トークンのフィルタリングが無効化されます。

Windows Vista または Windows 2008 が稼働しているコンピュータに対してローカル管理者アカウントを持っている場合は、この値を設定する意味があります。ドメイン管理者は、これを変更しても影響を受けません。

Windows Vista または Windows 2008 が稼働しているターゲット コンピュータのファイアウォールが有効（オン）になっている場合は、そのコンピュータへの展開を有効にするために、ファイル共有ポートだけでなく以下のポートも開いている必要があります。

	■ UDP ポート :
4104	CAM
137、138	ファイル共有およびプリンタ共有など
	■ TCP ポート :
135	dmdeploy
139、445	ファイル共有およびプリンタ共有など

それでも展開に失敗する場合は、Windows Vista のファイアウォールの以下の「送信の規則」を完全に有効にする必要があります。

- リモート アシスタンス
- ネットワークの検出
- ファイルとプリンタの共有
- コア ネットワーク

ポートを開き、送信規則を有効にした後でも、展開スキャンによって「応答がありません」というエラーが返される場合は、[スキャン中にターゲットに対して ping を実行しない] 設定オプションを **True** に設定する必要があります。このオプションは、「マネージャ¥インフラストラクチャ展開」セクションの設定ポリシーの下にあります。これにより、スキャン時にターゲットが「マシンは応答しています」とマークされ、展開が続行されます。これは、展開の正常終了を保証するためのものではなく、ターゲット コンピュータに最初に接続する際に発生する可能性のある問題を回避するための単なる方法です。

DSM エクスプローラを使用した展開

管理者は、インフラストラクチャ展開ウィザードを使用して、エージェントまたはスケーラビリティ サーバをエンタープライズ内に展開することができます。

ウィザードの指示に従うと、順を追って展開ジョブを作成できます。2つのジョブタイプ [ソフトウェアをターゲット コンピュータに展開] または [スケーラビリティ サーバにパッケージをステージング] から選択できます。展開するパッケージをリストから選択し、ある IPv4 アドレスの範囲内またはあるディレクトリ内にある、特定のドメイン内の特定のコンピュータまたはすべてのコンピュータのいずれにそのパッケージを展開するのかを指定します。次に展開ウィザードは、ターゲット コンピュータをスキャンして、すべてのターゲットで展開を実行できるかどうか、および展開にクレデンシャルが必要であるかどうかを検出します。

展開ウィザードは、ステップごとに画面に説明を表示し、独立したヘルプ システムを提供します。

展開ジョブの開始後、[コントロールパネル] - [展開ジョブ ステータス] 機能を使用して、ジョブを監視および制御できます。詳細については、**DSM エクスプローラ** ヘルプの「エージェント展開ジョブのモニタおよび制御」を参照してください。

注: Solaris の非大域ゾーン コンピュータにエージェント プラグインをインストールする際、「SSH は dmprimer のインストールに失敗しました。」というステータス メッセージが [展開ジョブのステータス] ペインに表示されることがあります。この問題を解決するには、**hosts** ファイル (**/etc/hosts**) の中に定義されているエージェントの IP アドレスと名前を更新します。

コマンドラインを使用した展開

dmsweep ユーティリティを使用すると、展開アクティビティを自動化したり、**DSM** エクスプローラで実行できるのと同じ数多くのタスクをインタラクティブに実行したりできます。

dmsweep を使用して、Windows NT 環境に **DMPPrimer** エージェントをインストールするための権限は、次のようにして展開管理で与えられます。**dmsweep** ユーティリティが、標準のセキュリティメカニズムを使用して展開マネージャに接続されます。**dmsweep** のユーザとして、マネージャで展開を実行する権限がシステム管理者によって付与されている必要があります(オペレーティングシステムレベルの特権管理者には、デフォルトで展開権限が付与されています)。ターゲットコンピュータのクレデンシャルは、**/tu** (ユーザ名) および **/tp** (パスワード) 引数を使用して指定できます。

継続ディスカバリによってトリガされる展開

新しいシステムが検出されたときにソフトウェアを展開する機能は、**CA Common Services** 継続ディスカバリ機能に基づいています。**CA Common Services** 配信インテリジェンス エージェント (**DIA**) は、新しいシステムが検出されるごとにイベントを取得するために使用されます。マシンの **IPv4** アドレスおよびオペレーティングシステムに応じて、どのパッケージをどのターゲット コンピュータに展開するかを示すポリシーをユーザが少なくとも 1 つ作成した後に、継続ディスカバリ機能がオンにされます。ポリシーは、継続ディスカバリ展開ポリシー ウィザードで定義できます。このウィザードは、インフラストラクチャ展開ウィザードと類似しています。

ディスカバリ プロセスは、以下のとおりです。

- システムからネットワークへ初めて接続されます。
- 継続ディスカバリ サービスによって新しいハードウェアが検出され、ヒューリスティックスを使用して分類されて、**WorldView** リポジトリのシステムを表す管理対象オブジェクトが作成されます。
- データベースに到着した新しいデータに応じて、特殊な（専用の）イベント テーブルへのイベント登録がトリガされます。
- これらのイベント用にサブスクライブされる **Client Automation** ディスカバリ アプリケーションに通知されます。
- 検出されたシステムが新しいソフトウェアを受け取るターゲットになっており、展開インターフェース (**DMSweep** の機能方法と類似) を呼び出す場合、ディスカバリ アプリケーションでは継続ディスカバリ ポリシーが確認されます。

注: 継続ディスカバリ機能については、**MicrosoftSQL Server** でドメイン マネージャ上のデフォルト ポート **1433** を設定してください。

展開パッケージ

以下の種類の展開パッケージが提供されます。

- CA DMS エージェント + 基本インベントリ プラグイン
- CA DMS エージェント + Asset Management プラグイン
- CA DMS エージェント + Remote Control プラグイン
- CA DMS エージェント + Software Delivery プラグイン
- CA DSM エージェント + AM、RC、SD プラグイン

このパッケージは、基本インベントリ、Asset Management、Remote Control、および Software Delivery 用のエージェント プラグインを組み合わせたパッケージです。

Linux では、このパッケージには CA Data Transport エージェント プラグインがさらに含まれます。

- CA DMS スケーラビリティ サーバ

このパッケージは、スケーラビリティ サーバ、および基本インベントリ、Asset Management、Remote Control、Software Delivery、および CA Data Transport 用のエージェント プラグインを組み合わせたパッケージです。

注: CA DSM スケーラビリティ サーバ展開パッケージが DMDeploy を使用して展開されると、スケーラビリティ サーバのプラグインおよびすべてのエージェント プラグインがインストールされます。ただし、Software Delivery の機能を使用してこのパッケージが展開されると、スケーラビリティ サーバのプラグインおよび Software Delivery と CA Data Transport のエージェント プラグインのみがインストールされます。

注: CA DSM スケーラビリティ サーバ Linux (インテル) 展開パッケージの詳細については、「[Linux へのスケーラビリティ サーバのインストール \(P. 167\)](#)」を参照してください。

- デバイス コンプライアンス スキャナ (DCS) を展開するために、以下の展開パッケージが提供されます。

Windows

- CA DSM エージェント AM DCS プラグイン (英語のみのエディション)
- CA DSM エージェント AM DCS プラグイン
- リモート仮想化インベントリを展開するために、以下の展開パッケージが提供されます。

Windows

- CA DSM エージェント AM RVI プラグイン (英語のみのエディション)
- CA DSM エージェント AM RVI プラグイン

AIX

- CA DSM エージェント AM RVI プラグイン AIX (RS/6000) (ENU)

HP-UX

- CA DSM エージェント AM RVI プラグイン HP-UX (800) (ENU)

Linux

- CA DSM エージェント AM RVI プラグイン Linux (intel) (ENU)

Solaris Sparc

- CA DSM エージェント AM RVI プラグイン Solaris-Sparc (ENU)

注: Client Automation ドキュメントは、展開されたクライアントパッケージと共にインストールされません。

展開パッケージは、ローカル システムに展開のマネージャ機能がインストールされた (デフォルト) 場合にのみ、マネージャ コンピュータ上に存在します。

展開パッケージの設定済みの場所は、インストール プロセスのインタビュアー フェーズで変更することができます。

重要: 展開パッケージの Windows バージョンに対して追加の MSI コマンドライン プロパティを指定できますが「CA DSM Agent + AM、RC、SD プラグイン」および「CA DSM スケーラビリティ サーバ」の、Windows バージョンには、特別に配慮してください。これらの組み合わせられた MSI パッケージには、ADDLOCAL などのパッケージ固有の MSI 機能リスト プロパティを指定しないでください。そうしないと、パッケージの展開が失敗します。パッケージの特定の機能をリストする必要がある場合、問題の専用エージェント展開パッケージに対してリストすることをお勧めします。

dsmpush ツール

dsmpush ツールを使用すると、インストール パッケージをインストール DVD からドメイン マネージャにインポートまたは「プッシュ」できます。dsmpush ツールを使用して、インフラストラクチャ展開または **Software Delivery** 機能で使用するパッケージをインポートします。

通常、これらのパッケージは、セットアップ中にマネージャ コンピュータにプッシュされますが、プッシュするかどうかは任意です。パッケージを再プッシュしたり、さらにパッケージを追加したり、パッケージを更新する必要がある場合は、dsmpush ツールを使用します。

dsmpush ツールは、チェック機能およびコピー機能を提供します。チェック機能は、マネージャ内の既存の展開パッケージを検証し、リストします。コピー機能は、指定の製品および動作環境のパッケージセットをローカル システムのインフラストラクチャ展開ライブラリまたは **Software Delivery** ライブラリにインポートします。

dsmpush ツールを実行するたびに、ログ情報がログ ファイル `TRC_Inst_dsmPush.ddmmyyyhhmmss.log` に書き込まれます。`ddmmyyyhhmmss` は、特定のログ ファイルのタイム スタンプです。

dsmpush のチェックおよびコピー機能、およびそのパラメータの詳細については、「*CLI リファレンス ガイド*」を参照してください。

Client Automation インフラストラクチャを自動展開するための前提条件

インフラストラクチャ展開コンポーネントを使用すると、Client Automation ソフトウェアが実行されていないターゲット コンピュータに、エージェントとスケラビリティ サーバ ソフトウェアをリモート インストールできます。このインストールは、ソースおよびターゲットのコンピュータ上の基本オペレーティング システムで提供されている機能を使用している場合にのみ実現でき、エンタープライズ ネットワーク 設定によって課せられている制限を受けます。

インフラストラクチャ ソフトウェアを展開するときの最初のステップでは、ターゲット コンピュータに小さな「プライマ」アプリケーション **DMPrimer** をリモート インストールします。この **DMPrimer** ソフトウェアは、その後のインフラストラクチャ ソフトウェア コンポーネントのインストール イメージを転送したり、各イメージをインストールするために呼び出したりします。ターゲット コンピュータに **DMPrimer** を配信する場合、展開マネージャは、ターゲットで有効な ユーザ クレデンシャルを提供する必要があります。

DMPrimer は、以下のメカニズムのいずれかを使用して、ターゲット システムに転送されます。ターゲット コンピュータのオペレーティング システムを展開マネージャが認識している場合は、適切な転送メカニズムが選択されます。ターゲットのオペレーティング システムを判別できない場合は、以下の各メカニズムが順に試行されます。

■ ネットワーク共有を開く

展開マネージャは、ターゲット システムにある **Windows** ネットワーク 共有に接続します。デフォルトでは、使用される共有名は **ADMIN\$** ですが、「**defaultTargetShare**」設定ポリシーを使用して変更できます。このメカニズムは、**Windows** ベースのプラットフォームで実行している展開マネージャからしか使用できず、一部の **Windows** ターゲットに対してしか成功しません。**Windows XP Home** などの少し異なる **Windows** バージョンは、この展開のメカニズムをサポートしていません。

- **SSH プロトコルを使用してターゲット コンピュータとのネットワーク接続を開き、SFTP を使用してプライマインストール パッケージを転送する**

このメカニズムは、SSH サーバが稼働しているすべてのコンピュータに対して機能しますが、主に、Linux や UNIX コンピュータをターゲットにする場合に役立ちます。

注: Solaris システムに展開する場合は、SunSSH v1.1 以上または最新バージョンの OpenSSH を使用することをお勧めします。Solaris プラットフォームおよびバージョンに適用可能なパッチの詳細については、Web サイト：
<http://opensolaris.org/os/community/security/projects/SSH> を参照してください。

ターゲット コンピュータでファイアウォールが稼働している場合は、SSH ポート (22) が展開マネージャからの接続を許可できることを確認してください。また、ターゲット コンピュータ上の SSH サーバが、暗号化用に RSA キーおよび 3DES 暗号、および HMAC-SHA1 メッセージ認証コード (MAC) を使用するように設定されているかどうか確認する必要があります。ほとんどの SSH サーバは、デフォルトでこの設定をサポートしますが、サポートしていない場合は、SSH サーバのドキュメントを参照し、これを追加する方法の説明を確認してください。

重要: Solaris 11 では、sshd 用のデフォルト暗号は aes128-ctr、aes192-ctr、aes256-ctr、arcfour128、arcfour256、arcfour です。展開では 3DES が必要なため、「Ciphers 3des-cbc」を sshd 設定ファイルに追加し、sshd を再起動する必要があります。

UNIX または Linux エージェントに正常に展開するために、最近の SSH 実装の /etc/ssh/sshd_config 設定ファイルを以下のように設定する必要があります。

- PasswordAuthentication を Yes に設定
- PermitRootLogin を Yes に設定
- SFTP サブシステムが有効であることを確認

IPv4 および IPv6 スタックの両方を実行している IBM AIX システムへ、IPv6 アドレスを使用して展開する場合は、ターゲット コンピュータの SSH サーバが IPv4 向けのポート 22 のみをリスンしている可能性があります。これにより、展開が失敗します。これを修正するには、sshd_config 設定ファイルを編集し、ListenAddress を「::」に設定します。

Solaris 11 に展開する場合は、以下の手順に従います。

- 以下をコメントアウトします。

```
CONSOLE=/dev/console
```

- 以下の行：

```
/etc/default/login.
```

```
vi /etc/default/login
```

```
#CONSOLE=/dev/console
```

- `/etc/user_attr` のルート エントリから以下を削除します。

```
;type=role
```

または以下のコマンドを使用します。

```
rolemod -K type=normal root
```

- SSH サービスの再起動

注: 展開マネージャとターゲット コンピュータ間の SSH 通信が FIPS に準拠するには、展開マネージャ上での FIPS のみモードの設定とは別に、ターゲット上で稼働している SSH サーバも FIPS 準拠の暗号化モジュールを使用していることを確認する必要があります。

- Telnet プロトコルを使用してターゲット コンピュータとのネットワーク接続を開き、FTP を使用してプライマインストールを転送する

このメカニズムは、主に、ターゲットとする UNIX システムが SSH をサポートしていない場合に役立ちます。Telnet/FTP は、本来セキュリティに弱点があるプロトコルであるために、あまり使用されなくなっており、SSH/SFTP にとって代われつつあります。

この接続方法を使用する場合、マネージャ内にある FTP サーバから DMPrimer インストールイメージを取り出すターゲット コンピュータで Telnet コマンドが実行されます。

重要: 現在使用されているオペレーティング システムでは、ソフトウェアのリモートインストールが推奨されていません。また、明確に禁止されている場合もあります。これらのシステムに Client Automation ソフトウェアを展開しようとすると、通常、ステータスが「プライマ トランスポートがありません」になり、展開は失敗します。そのような場合には、たとえば DVD などの物理的な配布メディアを使用せずにインストールを行うなど、ほかの手段を使用して Client Automation ソフトウェア コンポーネントをインストールします。

または、DMPrimer ソフトウェアは、手動でインストールすることもできます。手動の場合には、基本オペレーティング システムが提供している機能に頼らなくても Client Automation インフラストラクチャを展開することができます。

ご使用の環境で自動展開が可能かどうかを判別するには、以下のような標準オペレーティングシステム操作を実行して確認します。

- Windows 共有を使用した DMPrimer イメージの配信の場合は、展開リクエストで提供されるターゲットユーザクレデンシアルを使用して、共有（デフォルト：ADMIN\$）を展開マネージャホストコンピュータから各展開ターゲットコンピュータにマップする必要があります。
- SSH を使用した DMPrimer イメージの配信の場合、SSH を使用して、展開マネージャから展開ターゲットコンピュータへ接続する必要があります。
- Telnet を使用した DMPrimer の配信の場合には、展開リクエストで提供されるルート/管理者クレデンシアルを使用し、Telnet クライアントを使用して展開ターゲットコンピュータに接続する必要があります。また、匿名ユーザとして FTP に接続して、マネージャターゲットコンピュータから FTP 抽出操作を実行することもできます。

インフラストラクチャ展開で使用する FTP サーバの変更の詳細

インフラストラクチャ展開パッケージを格納するために使用する FTP サーバに関するオプション詳細は、インストール完了後に変更できます。たとえば、異なるサーバに FTP パッケージを再配置する場合に変更できます。

Windows ターゲットコンピュータのオプションの詳細を変更するには、以下のコマンドを実行します。

```
¥Program Files¥CA¥DSM¥bin¥dmdeploy.exe ftpinfo FTP_server FTP_user FTP_password
```

FTP_server

FTP サーバをホストするコンピュータのアドレスを指定します。

FTP_user

FTP に接続するユーザを指定します。

FTP_password

FTP ユーザに関連付けられるパスワードを指定します。

エージェントの展開を有効にする Windows XP の設定

たとえば、Windows XP Professional SP2 の Windows Firewall などのファイアウォールソフトウェアを実行するターゲット コンピュータへのエージェントの展開を有効にするには、以下のアクションを手動で実行する必要があります。

1. セキュリティ ポリシー [ネットワーク アクセス：ローカルアカウントの共有とセキュリティ モデル] を [Guest のみ - ローカル ユーザが Guest として認証する] から [クラシック - ローカル ユーザがローカル ユーザとして認証する] に変更します (Windows XP に適用)。

クラシック モデルでは、リソースへのアクセスを微調整でき、通常は指定されたリソースへの「読み取り専用」アクセスのみが可能な、ローカルアカウントを使用するネットワーク ログインがゲストアカウントにマップされないようにできます。

詳細については、Windows 製品のドキュメントの Web ページ「ネットワーク アクセス：ローカルアカウントの共有とセキュリティ モデル」を参照してください。

2. 以下のファイアウォール設定を行います。
 - ファイルおよびプリンタの共有を許可
 - UDP ポート 4104 のオープン
 - TCP ポート 135 のオープン

第 6 章：アップグレードと移行に関する考慮事項

このセクションには、以下のトピックが含まれています。

[サポートされているアップグレードパス \(P. 298\)](#)

[一般的な注意事項 \(P. 298\)](#)

[アップグレードプロセス \(P. 302\)](#)

[アップグレードに関する重要事項 \(P. 303\)](#)

[フェーズ 1：DSM エンタープライズ マネージャのアップグレード \(P. 304\)](#)

[フェーズ 2：DSM ドメイン マネージャのアップグレード \(P. 305\)](#)

[フェーズ 3：DSM スケーラビリティ サーバのアップグレード \(P. 307\)](#)

[フェーズ 4：DSM エージェントのアップグレード \(P. 309\)](#)

[インストール DVD を使用したエージェントのアップグレード \(P. 310\)](#)

[インフラストラクチャ展開と「AM、RC、SD プラグイン」 \(すべてのエージェント プラグイン\) パッケージを使用した Windows エージェントのアップグレード \(P. 310\)](#)

[インフラストラクチャ展開および個々のプラグインを使用した Windows エージェントのアップグレード \(P. 311\)](#)

[インフラストラクチャ展開と「AM、RC、SD プラグイン」 \(すべてのエージェント プラグイン\) パッケージを使用した Linux または MacIntel エージェントのアップグレード \(P. 313\)](#)

[インフラストラクチャ展開および個々のプラグイン パッケージを使用した Linux または MacIntel エージェントのアップグレード \(P. 313\)](#)

[Software Delivery と「AM、RC、SD プラグイン」 \(すべてのエージェント プラグイン\) パッケージを使用した Linux または MacIntel エージェントのアップグレード \(P. 314\)](#)

[Software Delivery および個々のエージェント プラグイン パッケージを使用した Linux または MacIntel エージェントのアップグレード \(P. 314\)](#)

[インフラストラクチャ展開と「AM、SD プラグイン」 \(すべてのエージェント プラグイン\) パッケージを使用した UNIX エージェントのアップグレード \(P. 315\)](#)

[インフラストラクチャ展開および個々のエージェント プラグイン パッケージを使用した UNIX エージェントのアップグレード \(P. 315\)](#)

[Software Delivery と「AM、RC、SD プラグイン」 \(すべてのエージェント プラグイン\) パッケージを使用した Windows エージェントのアップグレード \(P. 316\)](#)

[Software Delivery および個々のエージェント プラグイン パッケージを使用した Windows エージェントのアップグレード \(P. 316\)](#)

[Software Delivery と「AM、SD プラグイン」 \(すべてのエージェント プラグイン\) パッケージを使用した UNIX エージェントのアップグレード \(P. 317\)](#)

[Software Delivery および個々のエージェント プラグイン パッケージを使用した UNIX エージェントのアップグレード \(P. 318\)](#)

サポートされているアップグレード パス

Client Automation リリース 12.9 は、以下の製品およびバージョンからのアップグレードをサポートします。

- マネージャ コンポーネントについては、以下の製品からのアップグレードがサポートされています。
 - Client Automation 12.5 SP1
 - Client Automation 12.5 SP1 C1
 - Client Automation 12.8
 - Client Automation 12.8.01 Feature Pack
- スケーラビリティ サーバとエージェント コンポーネントについては、以下のものからのアップグレードがサポートされています。
 - Client Automation 12.5 SP1
 - Client Automation 12.5 SP1 C1
 - Client Automation 12.8
 - Client Automation 12.8.01 Feature Pack

一般的な注意事項

すべてのアップグレードは既存の言語ベースで実行される必要があります。たとえば、フランス語版をフランス語版の Client Automation にアップグレードすることはできますが、英語版にはアップグレードできません。

Client Automation コンポーネントのアップグレードに関する考慮事項

Client Automation コンポーネントをアップグレードする場合、以下の点について考慮する必要があります。

- 仮想アプリケーション イメージを検出するために Client Automation リリース 12.9 スケーラビリティ サーバによってプッシュダウンされる新規シグネチャは、レガシー エージェントによって無視されるように、特殊なタグが付けられています。

MDB に関する考慮事項

MDB に関する考慮事項を以下に示します。

- **Client Automation** リリース 12.9 は MDB として **Microsoft SQL Server 2005** をサポートしていません。 **Client Automation** リリース 12.9 にアップグレードする前に、データベース管理システムを **Microsoft SQL Server 2008** 以降にアップグレードします。

アップグレードにおける注意事項

リリース 12.9 へのアップグレード時：

- **Client Automation** は、前のリリースでインストールされたコンポーネントだけをアップグレードします。現在のリリース コンポーネントまたは追加のコンポーネントをインストールするには、[変更] オプションを有効にしてインストーラを実行し、インストールするコンポーネントを選択します。たとえば自動マイグレーションや **Alert Collector** など。
- **SSL** と共に **WAC** が設定されている場合は、アップグレードが完了した後に **JRE 1.7** 証明書ストアに証明書をインポートしたことを確認します。詳細については、「**Web** コンソールヘルプ」にある「**Web** コンソールおよび **Web** サービス用に **SSL** を有効化」のトピックを参照してください。
- **Windows** 上の **CA Asset Management** または **CA Remote Control** エージェントが **Software Delivery** ジョブを通してアップグレードされる場合は、**Software Delivery** エージェントパッケージがこのジョブに自動的に追加されます。最初に **Software Delivery** エージェントがアップグレードされ、次に要求されたエージェントがアップグレードされます。
- **OSIM IPS** コンポーネントをアップグレードすると、最新の **template.ini** が **OSIM** インストールディレクトリに格納される前に、カスタマイズされた **template.ini** が確実にバックアップされます。**template.ini** のバックアップからカスタム変更をすべて抽出し、それらを新しい **template.ini** に適用します。将来のリリースでは、**Client Automation** に、**boiler template.ini** のカスタマイズをサポートするための拡張可能なツールの更新が含まれます。
- プラグインが正しく動作するには、**DSM** のプラグインをすべて現在のリリースにアップグレードします。

アップグレード情報

注: Client Automation r12.5 SP1 または r12.5 SP1 C1 からアップグレードする場合、CCS はアップグレードされません。現在のリリースには、Windows Server 2012 および SQL Server 2012 をサポートするために必要な追加の CCS パッチが含まれています。Manager マシンを Windows Server 2012 または SQL Server 2012 にアップグレードする場合、適用するパッチのリストについて CA テクニカル サポートにお問い合わせください。

R12.5 SP1 および R12.5 SP1C1 から Client Automation リリース 12.9 にアップグレードする場合、アップグレードの前には `caf kill all` を実行しないでください。必要な場合、`caf stop` を実行します。

FIPS に関する考慮事項

FIPS に関する考慮事項を以下に示します。

- FIPS モードを選択できるのは、カスタム インストール時のみです。簡易インストールでは、常に「FIPS 推奨」モードで Client Automation がインストールされます。スタンドアロンの Remote Control エージェントのインストールでは、カスタムおよび簡易の両方のインストール時に、FIPS モードを指定できます。
- ユーザが FIPS のみモードに切り替えるまで、アップグレードされたコンポーネントはすべて FIPS モードを使用します。FIPS のみのモードに切り替えることができるのは、Client Automation インフラストラクチャ内のコンポーネントをすべて最新のリリースにアップグレードした場合です。FIPS モードの切り替えの詳細については、「セキュリティ機能」のセクションを参照してください。
- ドメイン マネージャおよびイメージ作成システム (IPS) をアップグレードした後に、IPS を使用して既存の OS およびブート イメージをアップグレードし、FIPS 標準に準拠するようにできます。次に、移行したイメージをブート サーバに登録し、適用できます。OS イメージのアップグレード、登録、および適用の詳細については、「OS インストール管理 管理者ガイド」を参照してください。

関連項目:

[FIPS のみモードに切り替える方法 \(P. 491\)](#)

[FIPS 推奨モードに切り替える方法 \(P. 492\)](#)

OSIM のアップグレードに関する考慮事項

R12.5 SP1 FP1 CentOS パッチ (R055831) または R12.5 SP1 FP1 C1 から Client Automation リリース 12.9 に ITCM をアップグレードしている間、以下の手順に従います。

- 既存の Linux ベース (LinuxPE) のブートイメージを更新します。
- 既存の RHEL5.x および RHEL6.x の LinuxPE ベースの OS イメージを更新します。
- 現在、LinuxPE でサポートされている既存の OS イメージ (以前は WinPE および Dosx でサポートされていた) を更新します。既存の OS イメージを更新した後、InstallDrive ブート パラメータの値が `sda`、`sdb` であることを確認します。
- OS イメージでサポートされている値に手動で変更します。

注: OS インストール用のローカルディスクの使用に関する InstallDrive ブート パラメータを指定します。デフォルト値は空です。最初に使用可能なローカルディスクが OS インストールに使用されます。

以下の方法でディスクを追加できます。

- 4つを超えるディスクの場合、`sde`、`sdf` などの DSM エクスプローラからディスクを追加します。
- OSIM IPS (CA¥DSM¥osimips¥os-template¥camenu) フォルダ下の `OS.def` ファイルを変更します。

LinuxPE ベースの OS イメージ用の InstallDrive ブート パラメータについては、新しい定義を確認してください。

```
[InstallDrive]
Type=MapListExt
Trans=yes
MaxLength=128
Comment=sda、sdb、または sdc などの OS をインストールするディスク。
item=sda
item=sdb
item=sdс
item=sdd
```

詳細については、「OS インストール管理 管理者ガイド」を参照してください。

アップグレードプロセス

Client Automation のアップグレードは複雑で時間を要するプロセスであり、システムリソースの不足や停電など、多くの外的要素によって影響を受ける可能性があります。アップグレードを開始する前に（特にマネージャおよびスケラビリティサーバコンポーネントの場合）、データの損失を防ぐため、インストールされている既存のインストールのフルバックアップを行っておくことをお勧めします。

コンポーネントをアップグレードする場合、アップグレード順序が非常に重要になります。このリリースの **Client Automation** では、厳格なトップダウンのアップグレード方法がサポートされています。続行する前に、以下の各フェーズに含まれる手順をすべて確認してください。

- フェーズ 1：DSM エンタープライズ マネージャのアップグレード
- フェーズ 2：DSM ドメイン マネージャのアップグレード
- フェーズ 3：DSM スケラビリティ サーバのアップグレード
- フェーズ 4：DSM エージェントのアップグレード

各アップグレードフェーズの後では、それぞれの設定は完全に機能します。つまり、アップグレードされたコンポーネントは、まだアップグレードされていないコンポーネントと通信を行うことができます。

注：すでにコンピュータにインストールされている **Client Automation** ソフトウェアのアップグレードに **Client Automation** インストール DVD を使用する場合は、そのコンピュータにインストールされているすべての **Client Automation** コンポーネントがアップグレードされることに注意してください。

注：既存のインストールのアップグレードに、元々 **Unicenter DSM** をインストールした際に使用したソースやメディアとは異なるもの（DVD リーダなど）を使用した場合、アップグレードインストールが **MSI エラー コード 1602** で失敗する可能性があります。こうした失敗を防ぐために、元々のインストールに使用したのと同じソースまたはメディアを使用するように、インストールを設定することをお勧めします。

アップグレードに関する重要事項

- アップグレード時に、既存のインストールの言語を変更することはできません。別の言語識別子を、たとえば、自動アップグレードの応答ファイルで指定した場合、アップグレードは中止されます。

- DSM ドメイン マネージャをアップグレードした後、DSM エクスプローラで [コントロール パネル] - [設定] - [設定ポリシー] - [ポリシー名] - [DSM] - [マネージャ] - [インフラストラクチャ展開] に移動し、[プライマを常に展開] パラメータの値が「いいえ」に設定されていることを確認します。

パラメータの値が「いいえ」に設定されている場合、マネージャは DMprimer のバージョンがマネージャよりも低いターゲット コンピュータのみに対して DMprimer をアップグレードします。パラメータの値が「はい」に設定されている場合、マネージャは DMprimer のバージョンに関係なく、ターゲット コンピュータの DMprimer をアップグレードします。

- アップグレードプロセスでは証明書は更新されません。これは、コンピュータにすでに配置されている可能性がある既存のカスタム証明書を保護するためです。新規のカスタム証明書を使用するためにマスタ イメージが更新されている場合、この証明書はインストール中に「bin」フォルダにコピーされますが、証明書ストアには適用されません。

カスタム証明書は、初回インストール時に適用するか、またはアップグレードプロセスが完了した後に手動で適用する必要があります。新規の証明書をインポートする場合に必要なコマンドについては、「セキュリティ機能」の章の [「認証」](#) (P. 440) を参照してください。

フェーズ 1: DSM エンタープライズ マネージャのアップグレード

アップグレードプロセスのフェーズ 1 では、**DSM エンタープライズ マネージャ** をアップグレードします。通常、エンタープライズ マネージャは、大企業や非常に分散している会社でインストールされます。これまでに **DSM エンタープライズ マネージャ** をインストールしていない場合は、アップグレードフェーズ 2 に進んでください。

エンタープライズ マネージャをアップグレードするには、以下の手順に従います。

1. **DSM エンタープライズ MDB** に接続している可能性のあるサービスおよびアプリケーションをすべて終了します。

純粹な **Client Automation** 実装の場合、このサービスおよびアプリケーションには、**DSM エンタープライズ マネージャ** 自体、エンタープライズ マネージャとドメインマネージャ両方向けのリモート エンジン、**DSM レポータ**の実行中のインスタンスなどがあります。**MDB** を共有する他の **CA** アプリケーションまたはサードパーティ製品がネットワーク上にインストールされているため **MDB** への接続が確立されない場合は、それらのアプリケーションもシャットダウンする必要があります。

2. **DVD** を使用して **MDB** をアップグレードします（適宜）。

MDB が **DSM エンタープライズ マネージャ** とは別のコンピュータにインストールされている場合は、**Client Automation DVD** を使用して **MDB** をアップグレードします。[**MDB のインストール**] または [**MDB** を含む **CCS** のインストール] を選択します。

Client Automation 12.9 で、インストーラを使用して、シングルステップで **MDB** および **Manager** をアップグレードできます。インストーラは **MDB** マシンを識別し、**MDB** をまずアップグレードし、次に、**Manager** をアップグレードします。**MDB** オプションを含めて、[**CCS のインストール**] を使用して **MDB** がインストールされている場合、この機能はサポートされていません。

3. **DVD** を使用して **DSM エンタープライズ マネージャ** 自体をアップグレードします。
4. **DVD** を使用してリモートの **DSM エンタープライズ エンジン** をすべてアップグレードします（適宜）。

これまでにリモート コンピュータ上にエンタープライズ レベルのエンジンをインストールしてある場合は、**Client Automation DVD** を使用して、それらのエンジンをアップグレードします。

5. DVD または Software Delivery パッケージを使用して、リモートの DSM エクスプローラまたは DSM Reporter をアップグレードします（適宜）。

DSM エンタープライズ マネージャへの接続に使用され、先行する手順の結果としてアップグレードされなかった DSM エクスプローラ、Web サービス、または Web コンソールのスタンドアロン インスタンスがあれば、ここでアップグレードする必要があります。DSM スケーラビリティ サーバまたは DSM エージェントと併せてコンピュータにインストールされているインスタンスは、それぞれフェーズ 3 およびフェーズ 4 の後にアップグレードしてください。

注: Client Automation リリース 12.9 は、CA Asset Intelligence リリース 12.9 または CA Patch Manager リリース 12.9 とのみ互換性があります。Client Automation リリース 12.9 にアップグレードする場合、CA Asset Intelligence または CA Patch Manager も リリース 12.9 へアップグレードする必要があります。

注: Client Automation r12.5 SP1 または r12.5 SP1 C1 からアップグレードする場合、CCS はアップグレードされません。現在のリリースには、Windows Server 2012 および SQL Server 2012 をサポートするために必要な追加の CCS パッチが含まれています。Manager マシンを Windows Server 2012 または SQL Server 2012 にアップグレードする場合、適用するパッチのリストについて CA テクニカルサポートにお問い合わせください。

R12.5 SP1 および R12.5 SP1C1 から Client Automation リリース 12.9 にアップグレードする場合、アップグレードの前には caf kill all を実行しないでください。必要な場合、caf stop を実行します。

フェーズ 2: DSM ドメイン マネージャのアップグレード

Client Automation のアップグレードプロセスのフェーズ 2 では、DSM ドメイン マネージャをアップグレードします。

DSM ドメイン マネージャをアップグレードするには、以下の手順に従います。

1. DSM ドメイン MDB に接続している可能性のあるサービスおよびアプリケーションをすべて終了します。

純粋な Client Automation 実装の場合、ここでのサービスおよびアプリケーションには、DSM ドメイン マネージャ自体、エンタープライズ マネージャとドメイン マネージャの両方へのリモート エンジン、（このドメインに加え、その親のエンタープライズ マネージャの）DSM レポータの実行中のインスタンスなどがあります。MDB を共有する他の CA アプリケーションまたはサードパーティ製品がネットワーク上にインストールされているため MDB への接続が確立されない場合は、それらのアプリケーションもシャットダウンする必要があります。

2. Client Automation のインストール DVD を使用して MDB をアップグレードします（適宜）。

MDB が DSM ドメイン マネージャとは別のマシンにインストールされている場合は、インストール DVD を使用して MDB をアップグレードします。[MDB のインストール] または [MDB を含む CCS のインストール] を選択します。

Client Automation リリース 12.9 で、インストーラを使用して、シングルステップで MDB および Manager をアップグレードすることもできます。インストーラは MDB マシンを識別し、MDB をまずアップグレードし、次に、Manager をアップグレードします。MDB オプションを含めて、[CCS のインストール] を使用して MDB がインストールされている場合、この機能はサポートされていません。

3. インストール DVD を使用して DSM ドメイン マネージャ自体をアップグレードします。
4. インストール DVD を使用してリモートの DSM ドメイン エンジンすべてをアップグレードします（適宜）。

これまでにリモート コンピュータ上に DSM ドメイン レベルのエンジンをインストールしてある場合は、インストール DVD を使用して、それらのエンジンをアップグレードします。

5. インストール DVD または Software Delivery パッケージを使用して、リモートの DSM エクスプローラまたは DSM Reporter をアップグレードします (適宜)。

DSM ドメイン マネージャへの接続に使用され、先行する手順の結果としてアップグレードされなかった DSM エクスプローラ、DSM レポータ、Web サービス、または Web コンソールのスタンドアロンインスタンスがあれば、ここでアップグレードする必要があります。DSM スケーラビリティ サーバまたは DSM エージェントと併せてコンピュータにインストールされているインスタンスは、それぞれフェーズ 3 およびフェーズ 4 の後にアップグレードしてください。

注: Client Automation リリース 12.9 は、CA Asset Intelligence リリース 12.9 または CA Patch Manager リリース 12.9 とのみ互換性があります。Client Automation リリース 12.9 にアップグレードする場合、CA Asset Intelligence または CA Patch Manager も リリース 12.9 へアップグレードする必要があります。

注: Client Automation r12.5 SP1 または r12.5 SP1 C1 からアップグレードする場合、CCS はアップグレードされません。現在のリリースには、Windows Server 2012 および SQL Server 2012 をサポートするために必要な追加の CCS パッチが含まれています。Manager マシンを Windows Server 2012 または SQL Server 2012 にアップグレードする場合、適用するパッチのリストについて CA テクニカルサポートにお問い合わせください。

R12.5 SP1 および R12.5 SP1C1 から Client Automation リリース 12.9 にアップグレードする場合、アップグレードの前には caf kill all を実行しないでください。必要な場合、caf stop を実行します。

フェーズ 3: DSM スケーラビリティ サーバのアップグレード

DSM スケーラビリティ サーバは、以下の方法のいずれかでアップグレードできます。

- Client Automation インストール DVD を使用する方法
- スケーラビリティ サーバの Software Delivery パッケージを使用する方法
- スケーラビリティ サーバのインフラストラクチャ展開 (DMDeploy) を使用する方法

インストール DVD を使用してスケーラビリティ サーバをアップグレードするには、スケーラビリティ サーバ コンピュータに DVD を挿入し、対話式インストール ウィザードを使用します。

Software Delivery パッケージを使用してスケーラビリティ サーバをアップグレードするには、**DSM スケーラビリティ サーバ** パッケージを含む **Software Delivery** 展開ジョブを作成し、スケーラビリティ サーバ コンピュータ上で **Software Delivery** ジョブの実行をスケジュールします。

インフラストラクチャ展開 (DMDeploy) を使用して **Windows** スケーラビリティ サーバをアップグレードするには、新しいスケーラビリティ サーバ パッケージをスケーラビリティ サーバ コンピュータに展開します。これにより、スケーラビリティ サーバ自体、およびエージェントとすでにインストールされているすべてのエージェント プラグインがアップグレードされます。エージェント プラグインをアップグレードするようインストーラに指示するには、インフラストラクチャ展開ウィザードの [追加の **Windows** インストール オプション] フィールドで以下のパラメータを指定する必要があります。

REINSTALL=ALL REINSTALLMODE=vomus

インフラストラクチャ展開 (DMDeploy) を使用して **Linux** スケーラビリティ サーバをアップグレードするには、新しいスケーラビリティ サーバ パッケージをスケーラビリティ サーバ コンピュータに展開します。これにより、スケーラビリティ サーバ自体、およびエージェントとすでにインストールされているすべてのエージェント プラグインがアップグレードされます。

フェーズ 4: DSM エージェントのアップグレード

DSM エージェントは、以下の方法のうちのいずれかを使用してアップグレードできます。以下のリストに示すアップグレード方法を確認の上、最も適切な方法を選択してください。このリストに続いて、詳細なアップグレード手順の説明があります。

- **Windows、Linux、MacIntel、および UNIX コンピュータ用の Client Automation インストール DVD** を使用する方法。
- **Windows、Linux、および MacIntel エージェント コンピュータ用のインフラストラクチャ展開 (DMDeploy) と「AM、RC、SD プラグイン」** (すべてのエージェント プラグイン) パッケージを使用する方法。

エージェント コンピュータにエージェント プラグインのフルセットがすでにインストールされている場合は、「すべてのエージェント プラグイン」パッケージを使用して、このセットをアップグレードできます。プラグインのフルセットがインストールされていない場合でも「すべてのエージェント プラグイン」パッケージの使用はできますが、その場合は、まだインストールされていないプラグインもすべて **Windows** に追加されることに注意してください。

- **Unix エージェント コンピュータ用のインフラストラクチャ展開と「AM、SD プラグイン」** (すべてのエージェント プラグイン) パッケージを使用する方法。
- **Windows、Linux、MacIntel、および UNIX エージェント コンピュータ用のインフラストラクチャ展開および個々のエージェント プラグインパッケージ**を使用する方法。
- インフラストラクチャ展開を使用して、スタンドアロンの **RC** エージェントをアップグレードできます。
- **Windows、Linux、および MacIntel エージェント コンピュータ用の Software Delivery** および「AM、RC、SD プラグイン」 (すべてのエージェント プラグイン) パッケージまたは個別のエージェント プラグイン パッケージを使用する方法。

エージェント コンピュータにエージェント プラグインのフルセットがすでにインストールされている場合は、「すべてのエージェント プラグイン」パッケージを使用して、このセットをアップグレードできます。プラグインのフルセットがインストールされていない場合でも「すべてのエージェント プラグイン」パッケージの使用はできますが、その場合は、まだインストールされていないプラグインもすべて **Windows** に追加されることに注意してください。

- UNIX エージェント コンピュータ用の **Software Delivery** および「AM、SD プラグイン」（すべてのエージェント プラグイン）パッケージまたは個別のエージェント プラグイン パッケージを使用する方法。

注: DSM エージェントをアップグレードする場合、**Software Delivery** を使用してアップグレードする前に以下のパッチを適用する必要があります。

- AIX : RO01350
- HP : RO01319
- SUN : RO01315

インストール DVD を使用したエージェントのアップグレード

インストール DVD を使用して DSM エージェントをアップグレードするには、エージェント コンピュータに DVD を挿入し、対話式インストール ウィザードを使用します。

インフラストラクチャ展開と「AM、RC、SD プラグイン」(すべてのエージェント プラグイン)パッケージを使用した Windows エージェントのアップグレード

エージェント コンピュータにエージェント プラグインのフルセットがすでにインストールされている場合は、「すべてのエージェント プラグイン」パッケージを使用して、このセットをアップグレードできます。ただし、「すべてのエージェント プラグイン」パッケージは AM、RC、および SD プラグインをアップグレードしますが、DTS プラグインはアップグレードしません。DTS パッケージを使用して DTS プラグインをアップグレードします。

注: Windows で「すべてのエージェント プラグイン」パッケージを使用すると、DTS プラグイン以外でほかにインストールされていないプラグインがあればそれらもインストールされます。

Windows エージェント コンピュータ用のインフラストラクチャ展開および「すべてのエージェント プラグイン」パッケージを使用して DSM エージェントをアップグレードするには、「AM、RC、SD プラグイン」パッケージをエージェント コンピュータに展開します。

アップグレードするようインストーラに指示するには、インフラストラクチャ展開ウィザードの [追加の Windows インストール オプション] フィールドで以下のパラメータを指定する必要があります。

REINSTALL=ALL REINSTALLMODE=vomus

インフラストラクチャ展開および個々のプラグインを使用した Windows エージェントのアップグレード

Windows エージェント コンピュータ用のインフラストラクチャ展開および個々のエージェント プラグイン パッケージを使用して DSM エージェントをアップグレードするには、以下の手順に従います。

- エージェント コンピュータに DSM Remote Control エージェント プラグイン パッケージを展開します (適宜)。

以前のバージョンの Remote Control エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

エージェント プラグインをアップグレードするようインストーラに指示するには、インフラストラクチャ展開ウィザードの [追加の Windows インストール オプション] フィールドで以下のパラメータを指定する必要があります。

REINSTALL=ALL REINSTALLMODE=vomus

- エージェント コンピュータに **DSM Software Delivery** エージェント プラグイン パッケージを展開します（適宜）。

以前のバージョンの **Software Delivery** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

エージェント プラグインをアップグレードするようインストーラに指示するには、インフラストラクチャ展開ウィザードの「追加の **Windows** インストール オプション」フィールドで以下のパラメータを指定する必要があります。

REINSTALL=ALL REINSTALLMODE=vomus

- エージェント コンピュータに **DSM Asset Management** エージェント プラグイン パッケージを展開します（適宜）。

以前のバージョンの **Asset Management** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

エージェント プラグインをアップグレードするようインストーラに指示するには、インフラストラクチャ展開ウィザードの「追加の **Windows** インストール オプション」フィールドで以下のパラメータを指定する必要があります。

REINSTALL=ALL REINSTALLMODE=vomus

- エージェント コンピュータに **DSM 基本インベントリ** エージェント プラグイン パッケージを展開します（適宜）。

以前のバージョンの基本インベントリ エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

エージェント プラグインをアップグレードするようインストーラに指示するには、インフラストラクチャ展開ウィザードの「追加の **Windows** インストール オプション」フィールドで以下のパラメータを指定する必要があります。

REINSTALL=ALL REINSTALLMODE=vomus

インフラストラクチャ展開と「AM、RC、SD プラグイン」(すべてのエージェント プラグイン)パッケージを使用した Linux または MacIntel エージェントのアップグレード

Linux または MacIntel エージェント コンピュータ用のインフラストラクチャ展開および「すべてのエージェント プラグイン」パッケージを使用して DSM エージェントをアップグレードするには、「AM、RC、SD プラグイン」パッケージをエージェント コンピュータに展開します。

「すべてのエージェント プラグイン」パッケージは、デフォルトではインストール済みの以前のバージョンのエージェント プラグインをアップグレードします。新しいプラグインは追加されません。

インフラストラクチャ展開および個々のプラグイン パッケージを使用した Linux または MacIntel エージェントのアップグレード

Linux または MacIntel エージェント コンピュータ用のインフラストラクチャ展開および個々のエージェント プラグイン パッケージを使用して DSM エージェントをアップグレードするには、以下の手順に従います。

- エージェント コンピュータに **DSM Remote Control** エージェント プラグイン パッケージを展開します (適宜)。

以前のバージョンの **Remote Control** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

- エージェント コンピュータに **DSM Software Delivery** エージェント プラグイン パッケージを展開します (適宜)。

以前のバージョンの **Software Delivery** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

- エージェント コンピュータに **DSM Asset Management** エージェント プラグイン パッケージを展開します (適宜)。

以前のバージョンの **Asset Management** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

- エージェント コンピュータに **DSM 基本インベントリ エージェント プラグイン** パッケージを展開します (適宜)。

以前のバージョンの基本インベントリ エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

Software Delivery と「AM、RC、SD プラグイン」(すべてのエージェント プラグイン)パッケージを使用した Linux または MacIntel エージェントのアップグレード

Linux エージェント コンピュータ用または MacIntel 用の **Software Delivery** および「すべてのエージェント プラグイン」パッケージを使用して **DSM エージェント** をアップグレードするには、以下の手順を実行します。

- 「すべてのエージェント プラグイン」パッケージを含む **Software Delivery** 展開ジョブを作成します。
- エージェント コンピュータで実行する **Software Delivery** ジョブをスケジュールします。

「すべてのエージェント プラグイン」パッケージは、デフォルトではインストール済みの以前のバージョンのエージェント プラグインをアップグレードします。新しいプラグインは追加されません。

Software Delivery および個々のエージェント プラグイン パッケージを使用した Linux または MacIntel エージェントのアップグレード

Linux または MacIntel エージェント コンピュータ用の **Software Delivery**、および個々のエージェント プラグイン パッケージを使用して **DSM エージェント** をアップグレードするには、以下の手順に従います。

- 少なくとも **DSM エージェント** および **Software Delivery エージェント プラグイン** パッケージを含む **Software Delivery** 展開ジョブを作成します。

エージェント コンピュータに、ほかにも以前のバージョンの **DSM エージェント プラグイン** がインストールされている場合は、それらのプラグインも展開ジョブに含めます。

- エージェント コンピュータで実行する **Software Delivery** ジョブをスケジュールします。

インフラストラクチャ展開と「AM、SD プラグイン」(すべてのエージェント プラグイン)パッケージを使用した UNIX エージェントのアップグレード

UNIX エージェント コンピュータ用のインフラストラクチャ展開および「すべてのエージェント プラグイン」パッケージを使用して **DSM** エージェントをアップグレードするには、「AM、SD プラグイン」パッケージをエージェント コンピュータに展開します。

「すべてのエージェント プラグイン」パッケージは、デフォルトではインストール済みの以前のバージョンのエージェント プラグインをアップグレードします。新しいプラグインは追加されません。

インフラストラクチャ展開および個々のエージェント プラグインパッケージを使用した UNIX エージェントのアップグレード

UNIX エージェント コンピュータ用のインフラストラクチャ展開および個々のエージェント プラグインパッケージを使用して **DSM** エージェントをアップグレードするには、以下の手順に従います。

- エージェント コンピュータに **DSM Software Delivery** エージェント プラグインパッケージを展開します (適宜)。

以前のバージョンの **Software Delivery** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。
- エージェント コンピュータに **DSM Asset Management** エージェント プラグインパッケージを展開します (適宜)。

以前のバージョンの **Asset Management** エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。
- エージェント コンピュータに **DSM 基本インベントリ** エージェント プラグインパッケージを展開します (適宜)。

以前のバージョンの基本インベントリ エージェント プラグインがエージェント コンピュータにインストールされていた場合は、新しいバージョンのプラグインを展開します。

Software Delivery と「AM、RC、SD プラグイン」(すべてのエージェント プラグイン)パッケージを使用した Windows エージェントのアップグレード

エージェント コンピュータにエージェント プラグインのフルセットがすでにインストールされている場合は、「すべてのエージェント プラグイン」パッケージを使用して、このセットをアップグレードできます。プラグインのフルセットがインストールされていない場合でも「すべてのエージェント プラグイン」パッケージの使用はできますが、その場合は、まだインストールされていないプラグインもすべて **Windows** に追加されることに注意してください。

Windows エージェント コンピュータ用の **Software Delivery** および「すべてのエージェント プラグイン」パッケージを使用して **DSM** エージェントをアップグレードするには、以下の手順を実行します。

- 「すべてのエージェント プラグイン」パッケージを含む **Software Delivery** 展開ジョブを作成します。
- エージェント コンピュータで実行する **Software Delivery** ジョブをスケジュールします。

Software Delivery および個々のエージェント プラグイン パッケージを使用した Windows エージェントのアップグレード

Windows エージェント コンピュータ用の **Software Delivery** および個々のエージェント プラグイン パッケージを使用して **DSM** エージェントをアップグレードするには、以下の手順を実行します。

- 少なくとも **DSM** エージェントおよび **Software Delivery** エージェント プラグイン パッケージを含む **Software Delivery** 展開ジョブを作成します。

エージェント コンピュータに、ほかにも以前のバージョンの **DSM** エージェント プラグインがインストールされている場合は、それらのプラグインも展開ジョブに含めます。

- エージェント コンピュータで実行する **Software Delivery** ジョブをスケジュールします。

Software Delivery と「AM、SD プラグイン」(すべてのエージェントプラグイン)パッケージを使用した UNIX エージェントのアップグレード

注: r11.1 UNIX エージェントからアップグレードする場合は、**Software Delivery** を使用してアップグレードする前に、以下のパッチを適用します。

- AIX : RO01350
- HP : RO01319
- SUN : RO01315

UNIX エージェント コンピュータ用の **Software Delivery** およびすべてのエージェントプラグイン パッケージを使用して **DSM** エージェントをアップグレードするには、以下の手順を実行します。

- すべてのエージェント プラグイン パッケージを含む **Software Delivery** 展開ジョブを作成します。
- エージェント コンピュータで実行する **Software Delivery** ジョブをスケジュールします。

すべてのエージェント プラグイン パッケージは、デフォルトではインストール済みの以前のバージョンのエージェント プラグインをアップグレードします。新しいプラグインは追加されません。

Software Delivery および個々のエージェント プラグイン パッケージを使用した UNIX エージェントのアップグレード

注: r11.1 UNIX エージェントからアップグレードする場合は、**Software Delivery** を使用してアップグレードする前に、以下のパッチを適用します。

- AIX : RO01350
- HP : RO01319
- SUN : RO01315

UNIX エージェント コンピュータ用の **Software Delivery** および個々のエージェント プラグイン パッケージを使用して **DSM** エージェントをアップグレードするには、以下の手順を実行します。

- 少なくとも **DSM** エージェントおよび **Software Delivery** エージェント プラグイン パッケージを含む **Software Delivery** 展開ジョブを作成します。

エージェント コンピュータに、ほかにも以前のバージョンの **DSM** エージェント プラグインがインストールされている場合は、それらのプラグインも展開ジョブに含めます。

- エージェント コンピュータで実行する **Software Delivery** ジョブをスケジュールします。

第 7 章: CA Catalyst 用の CA ITCM コネクタ

CA Catalyst コネクタは、製品データを CA Spectrum Service Assurance および CA IT Process Automation Manager などの製品に公開して、さまざまなコンテキストで視覚化、分析、および管理を実行できるようにします。

注: Client Automation コネクタは、既存のドメインマネージャまたはスケーラビリティ サーバによって、Windows オペレーティング システムにのみインストールできます。

Client Automation コネクタは、SSA 3.2.0 をサポートします。Client Automation コネクタは、DSM ドメインマネージャ、またはドメインマネージャに登録されたスタンドアロンのスケーラビリティ サーバとのインターフェースとして機能し、CA Catalyst インフラストラクチャを活用する製品が使用できるように Client Automation データを公開します。Client Automation データとそれを使用する製品（CA Spectrum SA など）を統合することにより、既存の構成アイテム（CI）によるエンティティ プロパティの調整および相互関連付けが可能になります。また、この統合により、データを、別のより広いビジネス サービス コンテキストで評価できます。

注: CA ITCM コネクタ 3.2.0 は、SOI 3.2.0 上の Northbound だけをサポートします。

CA Catalyst コネクタの統合により、ドメインごとに 1 つの Client Automation コネクタが存在します。Client Automation コネクタは、以下の Client Automation コンポーネントまたは機能により、ドメインマネージャとのインターフェースとして機能します。

- ADSM Web サービス

Client Automation Web サービスは、CA Catalyst コネクタに発行される CI に関する情報を取得するために使用されます。

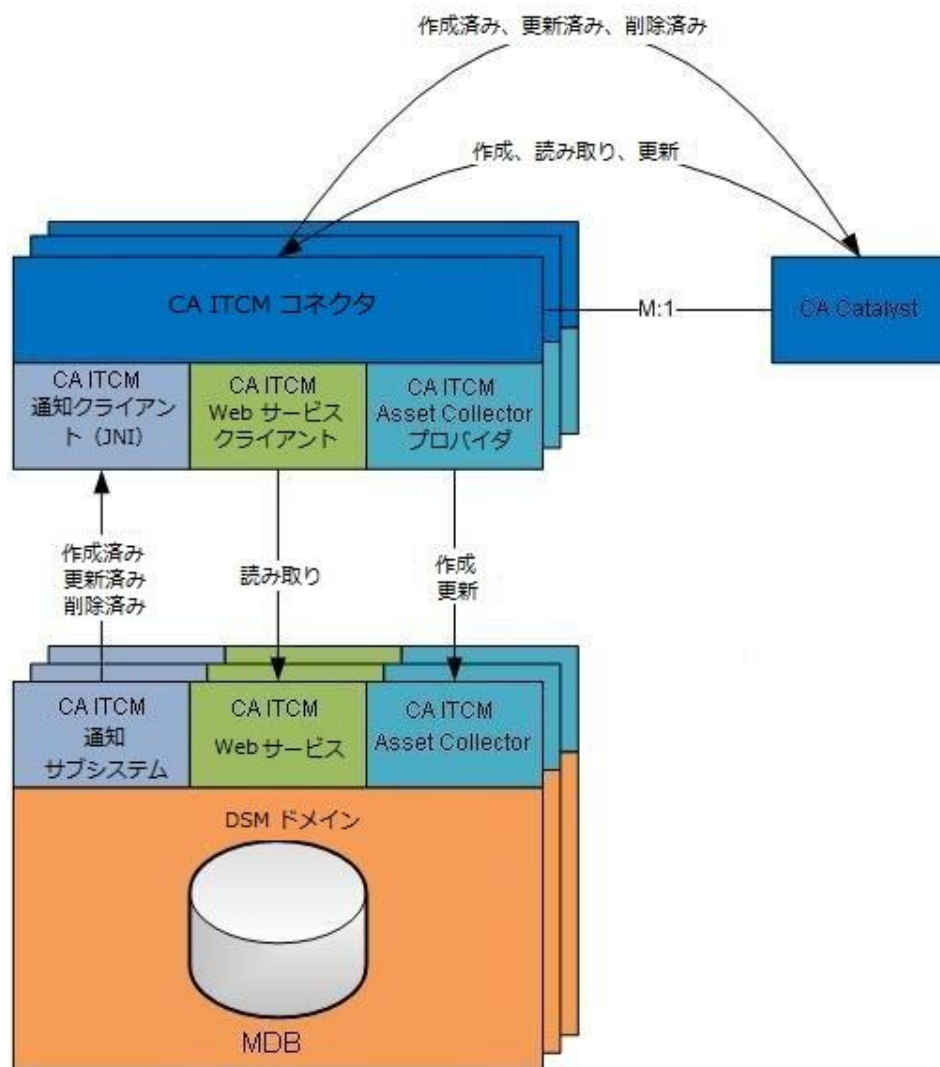
- Client Automation イベント通知サブシステム

発行された CI への更新に関するイベントは、Client Automation イベント通知サブシステムによって受信されます。

- Asset Collector

Asset Collector コンポーネントは、コンピュータ CI データに関する CA Spectrum SA サブスクリプション動作の実行時に使用されます。Asset Collector ファイルは、受信作成データおよび更新データのコンネクタから Client Automation MDB への移動に役立ちます。

以下の図は、Client Automation - CA Catalyst コネクタ統合を示しています。



注: CA Catalyst インフラストラクチャおよびそのコネクタに関するより一般的な情報、すべてのコネクタに適用される情報、およびカスタム コネクタ統合については、CA Spectrum SA に付属の「*Connector Guide*」を参照してください。Client Automation コネクタのインストール、設定、および使用の詳細については、CA Spectrum SA に付属の「*CA IT Client Manager Connector Guide*」を参照してください。

第 8 章: デスクトップ仮想化

このセクションには、デスクトップ仮想化サポート機能の使用に関するシナリオが含まれます。Client Automation を使用すると、VMware View および Citrix XenDesktop で仮想デスクトップ インフラストラクチャを管理できます。CA ITCM は、以下の手順の実行に役立ちます。

- ゴールデンテンプレート、vDisks、および仮想デスクトップを DSM エクスプローラから管理できます。
- 再起動または新しいバージョンのゴールデンテンプレートへのデスクトップ更新の後に行った変さらに影響を与えずに、仮想デスクトップにインストールされたソフトウェアの自動的な再インストールを設定できます。

たとえば、標準モードの vDisk ベースの仮想デスクトップにインストールされたソフトウェアは、ユーザがログオフした後、失われます。次回、これらのソフトウェアにログインしたときに自動的に再インストールされるように CA ITCM を設定できます。

- 新しい仮想デスクトップ識別および登録スキームを含み、アセット登録速度およびクエリおよびレポートが改善されました。

注: ユーザ プロファイル、ユーザ データ、ユーザの個人設定またはデスクトップ設定の管理は、このリリースではサポートされません。移動ユーザ プロファイルおよびフォルダ リダイレクトなどの Microsoft の手法により、これらのタスクに対処します。詳細については、Microsoft のドキュメントを参照してください。

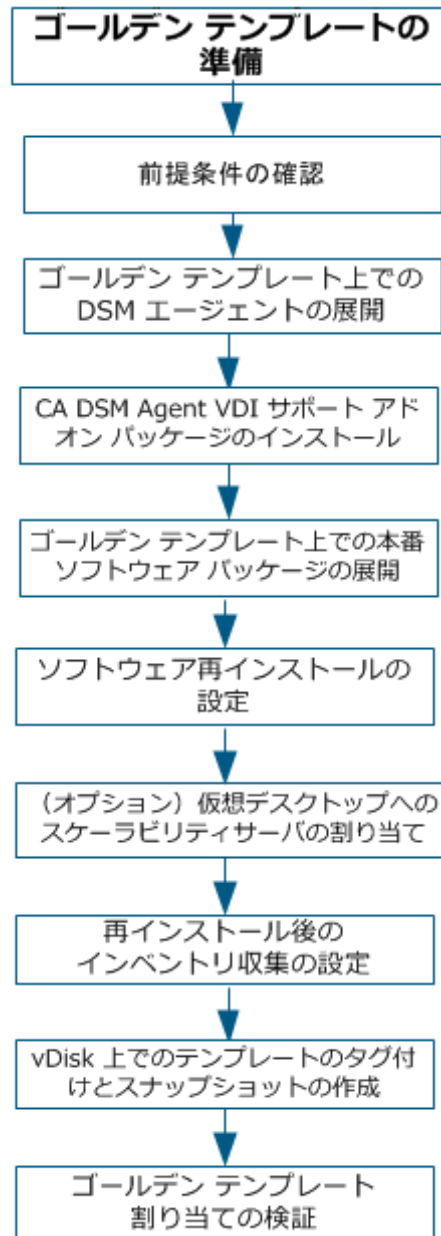
ゴールデン テンプレートの準備

デスクトップ サポート アナリストとして、**Client Automation** に仮想デスクトップ ソリューションを統合するためのゴールデン テンプレートを準備する必要があります。この統合により、**Client Automation** からゴールデン テンプレート、**VMware View Clone**、**Citrix PVS** ストリーム配信仮想デスクトップ、または **MCS** ベースの仮想デスクトップの管理が容易になります。

以下の図に、ゴールデン テンプレートを準備する手順を示します。



デスクトップ
サポート
アナリスト



ゴールデンテンプレート準備では、以下タスクを実行します。

1. [前提条件の確認](#) (P. 324)
2. [ゴールデンテンプレート上での DSM エージェントの展開](#) (P. 325)
3. [CA DSM エージェント VDI サポート アドオン パッケージのインストール](#) (P. 327)
4. [ゴールデンテンプレート上での実稼働ソフトウェア パッケージの展開](#) (P. 328)
5. [ソフトウェア再インストールの設定](#) (P. 328)
6. [テンプレートのタグ付けとスナップショットまたは vDisk の作成](#) (P. 342)
7. [\(オプション\) 仮想デスクトップへのスケーラビリティ サーバの割り当て](#) (P. 340)
8. [ソフトウェア再インストールに対するインベントリ収集の設定](#) (P. 342)
9. [ゴールデンテンプレートの割り当ての確認](#) (P. 343)

前提条件の確認

ゴールデンテンプレートを準備するには、以下の前提条件を確認します。

- ゴールデンテンプレート コンピュータに、仮想デスクトップ エージェントがインストールされていることを確認します。

注: Client Automation との統合を実装するには、VMware View や Citrix XenDesktop など、仮想デスクトップ ソリューションに関して、実際に役立つ適切な知識が必要です。

- Citrix vDisk ベースの仮想デスクトップを作成する場合、ゴールデンテンプレート コンピュータに Citrix PVS ターゲット デバイスがインストールされていることを確認します。
- (Citrix XenDesktop 7 のみ) .Net 3.5 が使用可能であることを確認します。

ゴールデン テンプレート上での DSM エージェントの展開

Client Automation は、必要な機能に応じて、別の DSM エージェント パッケージを提供します。少なくとも、DSM 共通エージェントおよび Software Delivery エージェント (CA DSM エージェント + Software Delivery プラグイン) が必要です。完全な機能が必要な場合は、CA DSM エージェント + AM、RC、SD プラグイン パッケージを展開します。

注: DSM エージェントは、DSM 共通エージェントおよび Software Delivery エージェント (CA DSM エージェント + Software Delivery プラグイン) を意味しており、示されているエージェント全体を意味していません。

ゴールデン テンプレート上で DSM エージェントを展開することにより、ゴールデン テンプレートから作成される仮想デスクトップ上で DSM エージェントが利用可能であることが保証されます。ゴールデン テンプレートおよびすべての仮想デスクトップは、管理対象コンピュータとして Client Automation に追加されます。

次の手順に従ってください:

1. DSM エクスプローラから、[コントロール パネル] - [展開] - [インフラストラクチャ展開ウィザード] に移動します。
2. ウィザードの指示に従って、以下タスクを実行します。
 - 必要な機能に応じて、エージェント パッケージを選択します。
 - ウィザードで、ターゲット コンピュータとしてゴールデン テンプレートを選択します。
 - 展開済みエージェントが登録されるスケーラビリティ サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
3. [完了] をクリックします。

展開ジョブは、[コントロール パネル] - [展開] - [展開ジョブのステータス] 下で作成されます。ジョブは、ゴールデン テンプレートにプッシュされます。

4. [コントロール パネル] - [展開] - [展開ジョブのステータス] ノードでジョブステータスを監視します。

展開が成功した後、エージェントは、自動的にスケーラビリティ サーバに登録されます。登録の後、ゴールデン テンプレートがドメイン マネージャに表示されます。

注: デフォルトでは、ゴールデン テンプレート、およびそれからプロビジョニングされる仮想デスクトップは、同じスケーラビリティ サーバにレポートします。仮想デスクトップの名前付けパターンに応じて、ある範囲の仮想デスクトップに別のスケーラビリティ サーバを割り当てることができます。「[\(オプション\) 仮想デスクトップへのスケーラビリティ サーバの割り当て \(P. 340\)](#)」を参照してください。

CA DSM エージェント VDI サポート アドオン パッケージのインストール

ゴールデンテンプレートに **CA DSM エージェント VDI サポート アドオン パッケージ**をインストールして、**Client Automation** と **VMware View** または **Citrix XenDesktop** 間でソフトウェアの再インストールおよび統合を有効にします。アドオンにより、**DSM エージェント**は、仮想デスクトップ環境を操作および管理できるようになります。

CA DSM エージェント VDI サポート アドオン パッケージは、以下のタスクを実行します。

- ソフトウェア状態データベースの使用を可能にし、必要な場合には、パスをセットアップします。
- エージェントをゴールデン テンプレート モードに設定します。
- ゴールデンテンプレートに、ソフトウェアの再インストール中に使用されるクローン作成スクリプトのセットをコピーします。

次の手順に従ってください:

1. **DSM エクスプローラ**でゴールデンテンプレートを右クリックし、**[ソフトウェア ジョブ]** - **[ソフトウェア パッケージの展開]** を選択します。
[ソフトウェア パッケージの展開] ウィザードが開きます。
2. ウィザードの指示に従います。ウィザードで以下のタスクを指定します。
 - **[DSM ソフトウェア パッケージ]** 下で **CA DSM エージェント VDI サポート アドオン Windows ENU パッケージ**を選択します。
注: このパッケージは、**VMware View** と **Citrix XenDesktop** の両方に共通の解決策を提供し、また **VMware View** 上で **Sysprep** 設定もサポートします。
 - 時間をスケジュールし、ジョブ コンテナ名を入力します。
3. **[完了]** をクリックします。
[ジョブのセットアップ] ダイアログ ボックスが表示されます。
4. **[OK]** をクリックします。
 パッケージはスケジュールされた時間に配信されます。
5. **DSM エクスプローラ**で、ゴールデンテンプレートを選択し、**[ジョブ]** - **[ソフトウェア ジョブ]** を選択してジョブ ステータスをモニタします。

ゴールデン テンプレート上での実稼働ソフトウェア パッケージの展開

Software Delivery を使用して、ゴールデン テンプレート上に実稼働ソフトウェア パッケージを展開できます。ゴールデン テンプレートにインストールされるソフトウェア アプリケーションは、ゴールデン テンプレートから作成される仮想デスクトップで自動的に利用可能です。

次の手順に従ってください:

1. **DSM** エクスプローラでゴールデンテンプレートを右クリックし、[ソフトウェア ジョブ] - [ソフトウェア パッケージの展開] を選択します。
[ソフトウェア パッケージの展開] ウィザードが開きます。
2. ウィザードの指示に従います。ウィザードで以下のアクションを指定します。
 - 展開するソフトウェア パッケージと手順を選択します。
 - ジョブ コンテナ名を入力します
3. ジョブの詳細設定ダイアログ ボックスを開き、[完了] をクリックします。
[ジョブのセットアップ] ダイアログ ボックスが表示されます。
4. [ジョブ] - [ジョブ オプション] - [スケーラビリティ サーバのステージング ライブラリにパッケージを格納する] オプションをクリックします。
5. [OK] をクリックします。

指定されたパッケージは、ゴールデン テンプレートのスケーラビリティ サーバ上でステージングされます。パッケージはスケジュールされた時間に配信されます。

ソフトウェア再インストールの設定

非永続的な仮想デスクトップにインストールされているソフトウェアは、再起動またはログオフの後、またはより新しいバージョンのゴールデン テンプレートによるデスクトップ更新で失われます。そのような場合、ソフトウェアを再インストールするように **Client Automation** を設定できます。**Client Automation** は、エージェントが仮想デスクトップ上で実行するすべてのソフトウェア ジョブの情報が含まれるインスタンス ソフトウェア状態データベースを使用します。仮想デスクトップには、インスタンス ソフトウェア状態データベースの詳細が含まれており、コンテキストを実行します。この情報は、ソフトウェアを再インストールする **Client Automation** にとって重要です。

デスクトップ仮想化ソリューションおよびデスクトップ プール/グループ設定に応じて、別の方法でソフトウェア再インストールを設定します。

VMware ビュー

- *quickprep* カスタマイズでのデスクトップ グループに対して、以下のいずれかの設定タスクを実行します。

- [設定ポリシーでのソフトウェア再インストール パラメータの設定](#) (P. 333)
- [仮想デスクトップ上で **Compose.bat** を実行するプール設定の設定](#) (P. 330)

注: ポリシー設定とプール設定の両方を設定すると、プール設定が優先されます。

- *sysprep* カスタマイズでのデスクトップ グループに対して、以下の設定タスクを実行します。

- [設定ポリシーでのソフトウェア再インストール パラメータの設定](#) (P. 333)

Citrix XenDesktop

- MCS から作成されたデスクトップについては、以下の設定タスクを実行します。

- [設定ポリシーでのソフトウェア再インストール パラメータの設定](#) (P. 333)

- vDisk ベースのデスクトップについては、以下のいずれかの設定タスクを実行します。

- [設定ポリシーでのソフトウェア再インストール パラメータの設定](#) (P. 333)
- [ターゲット デバイス上の個人データの設定](#) (P. 336)

注: ポリシー データと個人データの両方を設定すると、個人データが優先されます。

注: また、別の設定ポリシーを変更できます。これらのポリシーの詳細については、「[デスクトップ仮想化のサポートに対する設定ポリシー](#) (P. 343)」を参照してください。

仮想デスクトップ上で Compose.bat を実行するプール設定の設定

プールの作成時に、[Guest Customizations] 下のポスト同期スクリプトで、以下のコマンドを指定します。

Compose.bat [ISDBPath=<Path>] [Run=<Run>] [ISDBUser=<User> ISDBPassword=<Password>]

ISDBPATH

インスタンス ソフトウェア データベースが格納される場所へのパスを指定します。プールタイプに応じて、パスをローカルまたはネットワークにすることができます。非永続プール用のネットワーク パスと、永続プール用のローカルパスまたはネットワーク パスを指定します。パスの一部として、環境変数および、{SCALABILITY_SERVER} や {POOL_NAME}などの事前定義済みマクロが許可されています。

例：¥¥{SCALABILITY_SERVER}¥%COMPUTERNAME%

重要：Windows 7 上では、パス パラメータに %USERNAME% 環境変数が含まれる場合、コマンドラインパラメータとしてこのパラメータを Compose.bat に渡さないでください。代わりに、Compose.bat ファイル内にすべてのパラメータを含めます（VMware View のみ）。

{SCALABILITY_SERVER}

仮想デスクトップのレポート先であるスケーラビリティ サーバを返します。デフォルトでは、仮想デスクトップは、ゴールデン テンプレートがレポートするのと同じスケーラビリティ サーバにレポートします。[スケーラビリティ サーバ割り当てを明示的に変更 \(P. 340\)](#)した場合、マクロは、新しいスケーラビリティ サーバ名を返します。

{POOL_NAME}

仮想デスクトップのプール名を返します。このマクロは、VMware View に対してのみに適用できます。

永続的使用

%COMPUTERNAME% などの環境変数を、ISDB パスの一部として使用できます。

例：¥¥MachineName¥{POOL_NAME}¥%COMPUTERNAME%

このオプションを使用すると、（永続的な仮想デスクトップが常に同じユーザに割り当てられるため）ユーザに対して一意のパスが提供されます。

非永続的使用

ユーザ固有の環境変数 (%USERNAME% および %USERDOMAIN%) は、特定ユーザのソフトウェア状態データベースを一意に識別するために含めることができます。

例： ¥¥MachineName¥{POOL_NAME}¥%USERNAME%

注： 複数のデスクトップ プールが単一ユーザに割り当てられている際にネットワーク共有パスが使われている場合、場所を慎重に選択してください。 1つのプール内でユーザが使用する仮想デスクトップのソフトウェア状態が、別のプール内で同じユーザが使用する別の仮想デスクトップのデータを上書きしないようにする必要があります。たとえば、「User1」が非永続プール poolA と poolB を使用する権限を与えられているとします。両方のプールのパスが「//<マシン名>/<共有名>/Database/%USERNAME%」として指定される場合、ユーザがログオンし、両方のプールで両方の仮想デスクトップを使用すると、「User1」のソフトウェア状態が上書きされる可能性があります。このため、必ず別のパスを定義してください。

- 「</マシン名>/<共有名>/PoolA/%USERNAME%」
- 「</マシン名>/<共有名>/PoolB/%USERNAME%」

ISDBUSER

ネットワーク共有内のインスタンス ソフトウェア データベース パスに接続するユーザ名を指定します。ユーザ名は、sd_acmd encrypt コマンドを使用して暗号化する必要があります。

ISDBPASSWORD

ネットワーク共有内のインスタンス ソフトウェア データベース パスに接続するパスワードを指定します。パスワードは、sd_acmd encrypt コマンドを使用して暗号化する必要があります。

RUN

オフライン RAC プロセスを実行するタイミングを指定します。有効な値は **OnRecompose** および **OnLogon** です。

OnRecompose

更新または再構成後にデスクトップの開始後、オフライン RAC を開始するように指定します。このオプションは、永続的にリンクしたクローンなど、ユーザへのデスクトップ割り当てが固定されているデスクトップグループに使用します。

OnLogon

ユーザ ログオン時にオフライン RAC が開始されることを指定します。

このオプションは、非永続的デスクトップなど、ユーザへのデスクトップ割り当てが、セッションごとに変わるデスクトップグループに使用します。

例:

- 永続的使用 : `Compose.bat "ISDBPath=<Path>" "Run=OnRecompose"`
- 非永続的使用 : `Compose.bat "ISDBPath=<Path>" "Run=OnLogon"`

設定ポリシーでのソフトウェア再インストール パラメータの設定

次の手順に従ってください:

1. [コントロール パネル] - [設定ポリシー] - [デフォルト コンピュータ ポリシー] - [DSM] - [Software Delivery] - [エージェント] に移動します。
2. [RAC: 仮想マシン ソフトウェア再インストール設定] を選択して、以下の属性を表示します。

エージェントの名前付けパターン

仮想デスクトップのエージェントの名前付けパターンを指定します。VMware View については、名前付けパターンが、VMware プールで定義された名前付けパターンに一致する必要があります。XenDesktop については、名前付けパターンが **name##** である必要があります。このプレースホルダ (#) は、先頭に指定することはできません。また 2 回以上指定することもできません。

送信者

包含するデスクトップの開始範囲を指定します。範囲は数で指定できます。XenDesktop では、アルファベットも指定できます。開始は、名前付けパターンの開始を指定します。開始およびプレースホルダの長さは、等しくする必要があります。また、終了値は、プレースホルダの長さより大きくすることができます。

受信者

包含するデスクトップの終了範囲を指定します。範囲は数で指定できます。XenDesktop では、アルファベットも指定できます。

例: VMware View のエージェントの名前付けパターン

エージェントの名前付けパターン	送信者	受信者	可能なデスクトップ名
Name-{n}	1	100	Name-1、Name-2....Name-100

例: Citrix XenDesktop のエージェントの名前付けパターン

エージェントの名前付けパターン	送信者	受信者	可能なデスクトップ名
Name#	1	100	Name1、Name2、.....Name100
Name###	1	100	Name001、Name002...Name100
Name##	AA	AZ	NameAC、NameAE、...NameAZ

インスタンス ソフトウェア データベース パス

インスタンス ソフトウェア データベースが格納される場所へのパスを指定します。プールタイプに応じて、パスをローカルまたはネットワークにすることができます。非永続的なプールに対してネットワーク パスを指定するか、または永続的なプールに対してローカルパスまたはネットワーク パスを指定します (VMware View の場合は永続的にリンクしたクローン、およびデスクトップ割り当てが固定されている場合の XenDesktop では、異なるモードの vDisk ベースの仮想デスクトップ グループ)。後者の場合、仮想デスクトップに関連付けられた永続的なディスクが使用可能である場合は、ローカルパスのみ指定できます。パスの一部として、環境変数や、{SCALABILITY_SERVER}、{GROUP_NAME}、および {POOL_NAME} などの事前定義済みマクロが許可されています。

例：¥¥{SCALABILITY_SERVER}¥{GROUP_NAME}¥%COMPUTERNAME%
{GROUP_NAME}

仮想デスクトップのデスクトップ グループ名を返します。このマクロは、Citrix XenDesktop に対してのみ適用できます。

{POOL_NAME}

仮想デスクトップのプール名を返します。このマクロは、VMware View に対してのみに適用できます。

{SCALABILITY_SERVER}

仮想デスクトップのレポート先であるスケーラビリティ サーバを返します。デフォルトでは、仮想デスクトップは、ゴールデン テンプレートまたは vDisk がレポートするのと同じスケーラビリティ サーバにレポートします。[スケーラビリティサーバ割り当てを明示的に変更 \(P. 340\)](#)した場合、マクロは、新しいスケーラビリティ サーバ名を返します。

注: XenDesktop については、プールされた静的グループ内の単一のデスクトップに、複数のユーザを割り当てることができます。この場合、ユーザがインストールしたソフトウェアの再インストールをサポートするには、次の方法でインスタンス ソフトウェア データベース パスを指定します。

%%<server_name>%computername%%username%。また、実行コンテキストを *OnLogon* に設定します。

ユーザ名

ネットワーク共有内のインスタンス ソフトウェア データベース パスに接続するユーザ名を指定します。ユーザ名は、*sd_acmd encrypt* コマンドを使用して暗号化されます。

パスワード

ネットワーク共有内のインスタンス ソフトウェア データベース パスに接続するパスワードを指定します。パスワードは、*sd_acmd encrypt* コマンドを使用して暗号化されます。

実行

オフライン RAC プロセスを実行するタイミングを指定します。使用可能な値は *OnRecompose* と *OnLogon* です。

OnRecompose

リフレッシュまたは再構成 (VMware View)、デスクトップのリセットまたはスナップショット更新 (Citrix MCS)、および vDisk の更新またはデスクトップのリセット (ストリーム配信される仮想デスクトップ) 後にデスクトップが開始するときに、オフライン RAC が開始されるよう指定します。

このオプションは、永続的にリンクされたクローン、プールされた静的なデスクトップ、および異なるモードの vDisks に基づくデスクトップなど、ユーザへのデスクトップ割り当てが固定されている場合に、デスクトップ グループに対して使用します。

OnLogon

ユーザ ログオン時にオフライン RAC が開始されることを指定します。

このオプションは、非永続的なデスクトップ、プールされたランダム デスクトップ、および標準モードの vDisks に基づくプールされたデスクトップなど、ユーザへのデスクトップ割り当てがセッションごとに変化する場合に、プールされたデスクトップ グループに対して使用します。

3. ポリシーを保存して封印します。

ソフトウェア再インストール設定が、ゴールデン テンプレートに対して適用されます。

ターゲット デバイス上の個人データの設定

Citrix XenDesktop では、XenDesktop セットアップ ウィザードまたはストリーム配信 VM セットアップ ウィザードを使用してカタログを作成した後、およびマシンからデスクトップ グループが作成される前に、個人データを設定します。

次の手順に従ってください:

1. 仮想デスクトップに対して、Citrix Provisioning Services コンソールで [Target Device Properties] ダイアログ ボックスを開きます。
2. [Personality] タブをクリックし、以下のパラメータを追加します。

CA_DSM_ISDBPATH

インスタンス ソフトウェア データベースが格納される場所へのパスを指定します。プール タイプに応じて、パスをローカルまたはネットワークにすることができます。非永続的なプールに対してネットワーク パスを指定するか、または永続的なプールに対してローカルパスまたはネットワーク パスを指定します (デスクトップ割り当てが固定されている場合の XenDesktop では、異なるモードの vDisk ベースの仮想デスクトップ グループ)。

後者の場合、仮想デスクトップに関連付けられた永続的なディスクが使用可能である場合は、ローカルパスのみ指定できます。パスの一部として、環境変数や、{SCALABILITY_SERVER}、{GROUP_NAME}、および {GROUP_NAME} などの事前定義済みマクロが許可されています。

例: ¥¥{SCALABILITY_SERVER}¥{GROUP_NAME}¥%COMPUTERNAME%
{GROUP_NAME}

仮想デスクトップのデスクトップ グループ名を返します。このマクロは、Citrix XenDesktop に対してのみ適用できます。

{SCALABILITY_SERVER}

仮想デスクトップのレポート先であるスケーラビリティ サーバを返します。デフォルトでは、仮想デスクトップは、ゴールデン テンプレートまたは vDisk がレポートするのと同じスケーラビリティ サーバにレポートします。 [スケーラビリティ サーバ割り当てを明示的に変更 \(P. 340\)](#) した場合、マクロは、新しいスケーラビリティ サーバ名を返します。

CA_DSM_ISDBUSER

インスタンス ソフトウェア データベース ユーザの名前を、暗号化形式で指定します。 ユーザ名は、`sd_acmd encrypt` コマンドを使用して暗号化されます。

CA_DSM_ISDBPASSWORD

暗号化されたインスタンス ソフトウェア データベース パスワードを、暗号化形式で指定します。パスワードは、`sd_acmd encrypt` コマンドを使用して暗号化されます。

CA_DSM_RUN

オフライン RAC プロセスを実行するタイミングを指定します。 有効な値は `OnRecompose` および `OnLogon` です。

OnRecompose

デスクトップのリセットまたはスナップショットの更新後 (Citrix MCS の場合) および vDisk の更新またはリセット後 (ストリーミング配信される仮想デスクトップの場合)、デスクトップの開始時にオフライン RAC が開始されるように指定します。

このオプションは、プールされた静的なデスクトップ、および異なるモードの vDisks に基づくデスクトップなど、ユーザへのデスクトップ割り当てが固定されている場合に、デスクトップグループに対して使用します。

OnLogon

ユーザ ログオン時にオフライン RAC が開始されることを指定します。

このオプションは、プールされたランダム デスクトップや標準モードの vDisks に基づくプールされたデスクトップなど、ユーザへのデスクトップ割り当てがセッションごとに変化する場合に、プールされたデスクトップグループに対して使用します。

3. プロパティを保存します。

仮想デスクトップは、インスタンス ソフトウェア状態データベースの詳細を含むように設定されます。

4. 以下のいずれかの操作を実行します。

- すべての仮想デスクトップ上で手順 1 ～ 3 を実行します。
- デスクトップからすべての仮想デスクトップにパラメータをコピーします。

これで、ターゲット デバイス上に個人データが設定されました。

XenDesktop 5.5 での仮想デスクトップへの個人データのストリーミング

Citrix XenDesktop Virtual Desktop Agent 5.5 では、開始時に、仮想デスクトップに関する個人データが仮想デスクトップにストリーム配信されません。

設定ポリシーを通してではなく、個人データを使用してインスタンス ソフトウェア データベース設定が実行される場合、ソフトウェア再インストール機能が影響を受けます。

この問題を克服するために、Citrix 仮想デスクトップ エージェントの以下のホットフィックスを使用します。

- <http://support.citrix.com/article/CTX131268> (32 ビットバージョン)
- <http://support.citrix.com/article/CTX131269> (64 ビットバージョン)

ソフトウェアの再インストールでサポートされる仮想デスクトップ タイプ

Client Automation は、以下の仮想デスクトップ タイプ上でソフトウェアの再インストールをサポートします。

VMware View:

- リンク クローン

Citrix XenDesktop:

- プールされた静的デスクトップ
- プールされたランダム デスクトップ
- ストリーム配信デスクトップ
- 標準モードまたは異なるモードの vDisk 上の既存のカatalog ベース デスクトップ

注: ゴールデン テンプレートから以下のタイプを作成できますが、ソフトウェアの再インストールに対するサポートは必要ありません。開始時に、テンプレートソフトウェア レコードのみドメイン マネージャにレポートされます。通常の Client Automation エージェントとして、以下のタイプを独立して管理できます。

- プライベート モード vDisk デスクトップ
- 専用デスクトップ (MCS 経由)

重要: VMware View 内の浮動リンク クローンに関してユーザがログオフした場合に、再起動するように仮想デスクトップが設定されていることを確認します。複数のユーザに割り当てられたデスクトップでプールされた静的グループを作成する場合、ソフトウェア再インストールが想定通りに動作するために、この設定を手動で指定します。

(オプション)仮想デスクトップへのスケーラビリティ サーバの割り当て

すべての仮想デスクトップは、ゴールデン テンプレートまたは vDisk のエージェントとして同じスケーラビリティ サーバにレポートします。サーバ上で負荷を分散させるために、仮想デスクトップ上でエージェントに別のスケーラビリティ サーバを割り当てることができます。続行する前に、ゴールデン テンプレートから作成されるデスクトップに対する名前付けパターンを決定している必要があります。デスクトップの名前付けパターンに基づいて、デスクトップ上でエージェントに別のスケーラビリティ サーバを割り当てることができます。また、サーバに割り当てるデスクトップの数を設定できます。

次の手順に従ってください:

1. DSM エクスプローラで、ゴールデン テンプレートに適用する設定ポリシーを開きます。
2. [DSM] - [共通コンポーネント] - [登録] に移動します。
3. [スケーラビリティ サーバ] 設定ポリシーをダブルクリックします。

4. [行の追加] をクリックして、以下のフィールドで名前付けパターンと範囲を指定します。

エージェントの名前付けパターン

仮想デスクトップのエージェントの名前付けパターンを指定します。VMware View では、名前付けパターンは `name-{n}` であり、XenDesktop では `name##` のようにする必要があります。また、別の名前付けパターンを選ぶことができます。

スケーラビリティ サーバ

指定されたパターンと範囲に対して割り当てるスケーラビリティサーバを指定します。

開始

包含するデスクトップの開始範囲を指定します。範囲は数で指定できます。Citrix XenDesktop では、アルファベットも指定できます。開始およびプレースホルダの長さは、等しくする必要があります。また、終了値は、プレースホルダの長さより大きくすることができます。

終了

包含するデスクトップの終了範囲を指定します。範囲は数で指定できます。Citrix XenDesktop では、アルファベットも指定できます。

例: Citrix XenDesktop のエージェントの名前付けパターン

エージェントの名前付けパターン	開始	終了	可能なデスクトップ名
Name#	1	100	Name1、Name2、Name100
Name###	1	100	Name001、Name002、Name100
Name##	AB	BC	NameAC、NameAE、NameAZ

例: VMware View のエージェントの名前付けパターン

エージェントの名前付けパターン	開始	終了	可能なデスクトップ名
Name-{n}	1	100	Name-1、Name-2、Name-100

5. ポリシーを保存して封印します。

仮想デスクトップが作成されるときには、指定した設定に応じて、スケーラビリティサーバに自動的に割り当てられます。

ソフトウェア再インストールに対するインベントリ収集の設定

インベントリ収集を設定して、RAC の直後または RAC 後にユーザがログインしたときに、仮想デスクトップからインベントリを収集します。インベントリ収集は、ソフトウェア アプリケーションがすべて再インストールされるかどうかの確認を支援します。

次の手順に従ってください:

1. [コントロール パネル] - [設定] - [設定ポリシー] - [デフォルトのコンピュータ ポリシー] - [DSM] - [Software Delivery] - [エージェント] に移動します。
2. [RAC: 再インストール後のインベントリの収集] を選択し、値に以下のいずれかの属性を設定します。

いいえ

再インストール後にはインベントリが収集されず、RAC の前、または RAC の後に AM エージェントを通常に実行中は収集されるよう指定します。

即時

ソフトウェア再インストールの直後にインベントリが収集されるよう指定します。ユーザ ログオンの後にのみ、再インストールされたソフトウェアをソフトウェア インベントリの一部としてレポートし、IP、MAC アドレスおよびホスト名などのクライアントデバイス情報をレポートします。

ユーザ ログオン後

RAC 後にユーザがログインするときにのみ、インベントリが収集されるよう指定します。ユーザがログインした後、再インストールされたソフトウェアおよびクライアントデバイス情報がレポートされます。

RAC 後のインベントリ収集は、指定した設定に基づいて実行されます。

テンプレートのタグ付けとスナップショットまたは vDisk の作成

タグ付けにより、仮想デスクトップによって使用されるテンプレートのバージョンの追跡を支援します。テンプレートにタグ付けしてテンプレート タグを生成し、また仮想デスクトップをそれらの親のゴールデン テンプレートに関連付けます。

次の手順に従ってください:

1. **DSM** エクスプローラで、**CA DSM** エージェント アドオン **VDI** パッケージからゴールデン テンプレートにタグ テンプレート プロシージャをドラッグします。
 プロシージャを実行した後、プロシージャ ステータスが表示されます。
2. デスクトップ仮想化ソリューションに応じて、以下のいずれかのアクションを実行します。
 - (Citrix Provisioning Services を使用する **XenDesktop** の場合) **XenConvert** または別の適切なイメージング ツールを使用して **vDisk** を作成します。
 - (**VMware View** と **Citrix MCS** の場合) 仮想マシンをシャットダウンし、スナップショットを作成します。

このアクションにより、テンプレート タグにスナップショットまたは **vDisk** が関連付けられます。

スナップショットまたは **vDisk** が作成され、テンプレート タグを使用して、ゴールデン テンプレートに関連付けられます。

ゴールデン テンプレートの割り当ての確認

インベントリ、テンプレート設定から割り当てられたゴールデン テンプレートを確認できます。

次の手順に従ってください:

1. [コンピュータおよびユーザ] - [すべてのコンピュータ] - [コンピュータ名] - [インベントリ] に移動します。
2. [オペレーティング システム] タブ、[テンプレート設定] をクリックします。

割り当てられたテンプレートのリストが表示されます。

これで、仮想デスクトップの管理に対してゴールデン テンプレートが準備されます。

デスクトップ仮想化のサポートに対する設定ポリシー

CA DSM エージェント **VDI** サポート アドオン パッケージをインストールした後に、仮想デスクトップ用の **Client Automation** 設定ポリシーを設定します。これらのポリシーの一部は必須であり、**VMware View** によってプリセットされています。その他のポリシーはオプションであり、説明に従って入力する必要があります。

新しい登録ポリシー グループが追加されており、Citrix XenDesktop と VMware View によって提供される仮想デスクトップの管理をサポートするために、その他の設定ポリシー グループが拡張されています。

注: クローン作成された仮想デスクトップのエージェントおよびゴールデン テンプレートのエージェントに設定ポリシーを適用します。ゴールデン テンプレート スナップショットを保存する前に、クローン作成スクリプトによってプリセットされた必須のローカルに管理ポリシーを除いて、この処理を実行する必要があります。

ポリシーは、ゴールデン テンプレートからクローン作成された仮想デスクトップには自動的に継承されません。クローン作成された仮想デスクトップ値と中央管理されたポリシー値が異なる場合、その値は、管理者による登録の直後に上書きされます。

登録ポリシー グループ

仮想デスクトップに固有の識別のため、新しいポリシー サブグループ (登録) が、共通コンポーネント ポリシー グループの下に追加されました。登録ポリシー グループには、以下のポリシーが含まれています。

ホスト キー

クローン作成されたマシンを一意に識別するために使用される文字列を定義します。仮想デスクトップの各再構成により、MDB に新しい一意のコンピュータを登録する新しい仮想マシンが生成されるため、リンクされたクローンにはホスト キーが必要です。結果として、時間の経過に従って、ドメイン マネージャは、存在しなくなった多数のコンピュータを参照することになります。ホスト キーを使用すると、MDB 内の仮想デスクトップに対する既存コンピュータのレコードが、時間の経過とともに再利用されます。

ホスト キーには、プレーン テキストと任意の数のマクロが含まれます。登録時に、CAF はマクロを展開し、スケーラビリティ サーバに結果を送信します。次に、エンジンは、ホスト UUID/ホスト名/MAC アドレスではなく、ホスト キーを使用して MDB 内のアセットを識別します。この時点から、ホスト キーがエージェントを識別します。

注: 標準的なシナリオでは、MAC アドレスは、永続的にリンクされたクローンの再構成中に変更されません。ただし、永続的にリンクされたクローンの MAC アドレスが、再構成処理中に VMware によって変更される場合があります。したがって、通常は、非永続的、永続的にリンクされたクローン、および MCS ベースの仮想デスクトップの両方に対して、同様にホスト キーを使用する必要があります。

以下のマクロを使用します。

環境変数: `$env(name)`

例: `$env("COMPUTERNAME")-VDI`

レジストリ キー: `$reg(key,value)`

例: `$reg("HKLM¥SOFTWARE¥CA¥GuestID"," GuestUUID")-VDI`

INI ファイル値: `$ini(path,section,key)`

例: `$ini("c:¥id.ini","identity","uuid")-VDI`

また、これらのマクロは、同じ文字列内で組み合わせることもできます。

例:

`$env("COMPUTERNAME")-$reg("HKLM¥SOFTWARE¥CA¥GuestID","GuestUUID")-VDI`

注: デフォルトでは、`CAFPostInit.dms` スクリプトは、エージェント上で `$env("COMPUTERNAME")` でホスト キーを設定します。したがって、このポリシーを変更する必要はありません。ただし、別のマクロを使用する場合は、`CAFPostInit.dms` スクリプトで適切なホスト キー マクロ文字列を使用することにより、生成されたホスト キーがすべて一意であることを確認します。また、ホスト キーの長さが、64 文字以下であることを確認します。

デフォルト: 空、<ローカル管理>

スケーラビリティ サーバの設定

管理者が、デスクトップ プールおよび範囲に使用される仮想マシン名前付けパターンに基づいて、エージェント スケーラビリティ サーバを設定できるようにします。複数の範囲を適用できます。このポリシーはオプションであり、値が設定されない場合、すべてのクローンは、自分がクローン作成されたゴールデン テンプレートのエージェントと同じスケーラビリティ サーバにレポートします。詳細については、「スケーラビリティ サーバの設定」を参照してください。

エージェント (Software Delivery) ポリシー グループ

エージェント (Software Delivery) ポリシー グループは、VMware View 環境で Software Delivery エージェントを管理するために、以下の設定ポリシーを包含するように拡張されています。

注: エージェント ポリシー グループ内の RAC 設定ポリシーは、オフライン RAC にのみ適用されます。従来の RAC 機能は、[Software Delivery] - [マネージャ] ポリシー グループのポリシーによって設定されます。

ポリシーをダブルクリックして [プロパティの設定] ダイアログ ボックスを表示すると、そのポリシーのパラメータ値を変更できます。

RAC: 同じアクティビ化/設定プロシージャのエントリが複数ある場合の動作

重複するソフトウェア手順がオフライン RAC 中に除外されるかどうかを決定します。

Software Delivery では、インストール手順は 1 回のみ実行できますが、起動手順と設定手順は複数回実行できます。エージェントが、ソフトウェア パッケージに対して RAC コンテナを準備する場合、複数の起動手順と設定手順が含まれる可能性があります。このポリシーに対して設定する値により、単一のソフトウェア パッケージ内で重複する起動/設定手順がどのように処理されるかが決まります。有効な値は以下のとおりです。

重複しているアクティビ化/設定プロシージャをすべて再実行します。

データベースに記録されたすべての手順を実行するよう指定します。

重複しているアクティビ化/設定プロシージャの最初のプロシージャのみを再実行します

いずれかの起動/設定手順が 2 回以上含まれている場合、最初に重複した手順のみ実行するよう指定します。

重複しているアクティビ化/設定プロシージャの最後のプロシージャのみを再実行します

いずれかの起動/設定手順が 2 回以上含まれている場合、最後に重複した手順のみ実行するよう指定します。

デフォルト: 重複しているアクティビ化/設定プロシージャをすべて再実行します。

RAC: コンテナ タイプ

エージェントが、オフライン RAC コンテナ内のソフトウェア ジョブをバッチとして、またはリンクなしで実行するかどうかを指定します。有効な値は以下のとおりです。

バッチ

すべてのジョブが、各ターゲットに対して 1 単位のジョブとして順次実行されるよう指定します。シーケンス内のいずれかのジョブが失敗する場合、そのターゲットに対する残りのジョブは実行されません。

リンクなし

互いに独立して、順次実行されるジョブを指定します。

デフォルト： バッチ

RAC: ソフトウェア プロシージャが失敗した場合、ソフトウェア状態データベースから削除します

RAC コンテナ内の 1 つ以上のジョブが失敗する場合、ソフトウェア状態データベースが更新されるかどうかを制御します。[はい] に設定されている場合、失敗したジョブ エントリは、ソフトウェア状態データベースから削除されます。[いいえ] の場合、失敗したエントリが残ります。

デフォルト： はい

RAC: ユーザが閉じるまでジョブの確認 GUI を保持

対話型モードの再インストール中に RAC が失敗する場合、ユーザがダイアログ ボックスを閉じるのを [Software Delivery ジョブ確認] ダイアログ ボックスが待機するかどうかを制御します。たとえば、値が [はい] の場合、ユーザがコンピュータから離れているときに RAC 失敗が見落とされないことを保証します。

デフォルト： はい

RAC: インストール前ソフトウェア状態データベースの管理

仮想デスクトップにユーザが割り当てられない場合、プリインストール ソフトウェア状態データベースが保守されるかどうかを定義します。プリインストール ソフトウェア状態データベースは、プール内の仮想デスクトップが作成され、エージェントとして登録される場合で、まだいずれのユーザにも割り当てられていない場合に役立ちます。プリインストール データベースは、管理者が仮想デスクトップに必要なソフトウェア パッケージをプッシュするのに役立ちます。

「はい」に設定されている場合、プリインストール ソフトウェア状態 データベースは、ユーザが仮想デスクトップに割り当てられる前に、ローカル ファイル システム上で保守されます。プリインストール データベースは、ユーザが初めてログインするたびに、割り当てられたユーザ インスタンス ソフトウェア状態データベースにマージされます。

「いいえ」に設定されている場合、以下の条件が適用されます。

永続的なデスクトップ:

永続的なデスクトップでは、ログオン時にオフライン RAC が実行されるように設定されている場合、ソフトウェア ジョブ レコードがプリインストール データベースではなくインスタンス データベースに追加されるため、このポリシーを「いいえ」に設定すると、これらのソフトウェア パッケージが再インストールされます。

非永続的なデスクトップ:

非永続的なデスクトップでは、このポリシーを「いいえ」に設定すると、これらのソフトウェア パッケージに対して **Software Delivery** ジョブ レコードが維持されません。さらに、後で仮想デスクトップがリフレッシュされたときに、それらを再インストールできません。

デフォルト: はい

RAC: ソフトウェア状態データベースの管理

Software Delivery エージェントが、**VMware View** 機能に関係なく、データベースの状態を維持するかどうかを制御します。

注: このポリシーは必須であり、**VMware View** インテグレーション スクリプトによって「はい」にプリセットされています。手動で設定値を変更しないでください。

デフォルト: いいえ、<ローカル管理>

RAC: 再試行の最大秒数

1 つのジョブ確認中に、スケーラビリティ サーバへのアクセス試行間隔で、エージェントがスリープできる最大の秒数を定義します。このポリシーは、「RAC: オフライン RAC の再試行回数」ポリシーで動作します。これらのポリシーのいずれかによって指定された制限に到達するまで、再接続が試行されます。

デフォルト: 60

RAC: オフライン RAC の再試行回数

1 つのジョブ確認中に、エージェントがスケーラビリティ サーバに対して接続を試行できる最大回数を定義します。このポリシーは、
[RAC: 再試行の最大秒数] で動作します。これらのポリシーのいずれかによって指定された制限に到達するまで、再接続が試行されます。

デフォルト : 100

RAC: インスタンス ソフトウェア状態データベースにアクセスするためのパスワード

インスタンス ソフトウェア状態データベースへのアクセス許可を持つユーザのパスワードを指定します。パスワード文字列が暗号化されます。指定した場合、エージェントは、ネットワーク共有にアクセスするためにこれらのクレデンシャルを使用します。

パスワードは、「sd_acmd encrypt」コマンドを使用して暗号化することをお勧めします。次に、Compose.bat スクリプトの実行時にパラメータの 1 つとして暗号化されたパスワードを指定します。それにより、続いて設定パラメータが設定されます。

または、共有場所のパスワードが、特定のゴールデン テンプレート スナップショットから作成されるすべてのデスクトップ プールで同じ場合、設定ポリシーにパスワードを設定できます。次に、ゴールデン テンプレートおよびクローン作成された仮想デスクトップにポリシーを適用します。

デフォルト : 空、<ローカル管理>

RAC: インスタンス ソフトウェア状態データベースへのパス

インスタンス ソフトウェア状態データベースのインストール パスを指定します。指定されたパスには、埋め込み環境変数（たとえば「¥¥Fileserver1¥Share1¥%COMPUTERNAME%¥InstanceSoftwareDatabase」）を含めることができます。

注: このポリシーは必須ですが、Compose.bat スクリプトの実行時にパラメータの 1 つとしてパスを手動で入力してください。次に、このスクリプトにより設定パラメータが設定されます。

デフォルト : 空、<ローカル管理>

RAC: テンプレート ソフトウェア状態データベースへのパス

テンプレート ソフトウェア状態データベースのインストール パスを指定します。値が空の場合、エージェントは、適切な装置に固有のパス（すなわち「<ITCM InstallDir>%SD%ASM%DATABASE%Agent%TemplateSoftwareDatabase」）を使用します。

デフォルト： 空、<ローカル管理>

RAC: エージェントの RAC ポリシー設定

Software Delivery エージェントの [RAC ポリシー] 設定を制御します。[はい] に設定した場合、エージェントの [RAC ポリシー] がオフラインに設定されます。[いいえ] に設定した場合、[RAC ポリシー] はデフォルト RAC 設定に設定されます。

注: このポリシーは必須であり、VMware View インテグレーション スクリプトによって [はい] にプリセットされています。手動で設定値を変更しないでください。

この値セットは、デフォルトで [コンピュータ プロパティ] ダイアログ ボックスの [Software Delivery] タブになります。

デフォルト： いいえ、<ローカル管理>

RAC: SD エージェントをゴールデン テンプレート モードに設定します

エージェントが、ゴールデン テンプレートとクローン上のどちらで実行されるか区別できるようになります。[はい] の場合、エージェントはゴールデン テンプレート上で実行されます。

注: このポリシーは必須であり、VMware View インテグレーション スクリプトによってプリセットされます。

デフォルト： いいえ、<ローカル管理>

RAC: インスタンス ソフトウェア状態データベースにアクセスするためのユーザ名

インスタンス ソフトウェア状態データベースへのアクセス許可を持つユーザの名前を指定します。ユーザ名は、(*domainname* | *local¥*)「ユーザ」の形式にする必要があります。文字列が暗号化されます。指定した場合、エージェントは、ネットワーク共有にアクセスするためにこれらのクレデンシャルを使用します。

ユーザ名は、「sd_acmd encrypt」コマンドを使用して暗号化することをお勧めします。次に、**Compose.bat** スクリプトの実行時にパラメータの 1 つとして暗号化されたユーザ名を指定します。それにより、続いて設定パラメータが設定されます。

または、共有場所のユーザ名が、特定のゴールデン テンプレート スナップショットから作成されるすべてのデスクトップ プールで同じ場合、オプションで設定ポリシーにユーザ名を設定できます。次に、ゴールデン テンプレートおよびクローン作成された仮想デスクトップにポリシーを適用します。

注: デフォルトでは、フォルダが共有されている場合、その許可には、読み取りアクセス許可を持つ「Everyone」グループのみ含まれます。インスタンス ソフトウェア状態データベースがネットワークを通して保存されることを保証するには、ここで、ネットワーク共有に、[共有アクセス許可] タブ内で [フル コントロール] (WRITE) アクセス権を持つユーザを含める必要があります。

デフォルト: 空、<ローカル管理>

一般(CAF)ポリシー グループ

一般 (CAF) ポリシー グループに、は以下の設定ポリシーが含まれています。

CAF: 初期化前スクリプト

CAF が起動し、初期化が開始された場合に、実行するスクリプトを指定します。 UUID が確認される前、およびプラグインが開始される前に、このスクリプトが実行されます。

CAF: 初期化後スクリプト

CAF の初期化後に実行するスクリプトを指定します。 このスクリプトは、すべてのプラグインが起動してから、最初の登録が実行されるまでの間に実行されます。

CAF: 初期化前スクリプトのタイムアウト

初期化前スクリプトを終了するまでに、caf が待つ時間 (秒) を指定します。

CAF: 初期化後スクリプトのタイムアウト

初期化後スクリプトを終了するまでに、CAF が待機する時間 (秒) を指定します。

CAF: 起動時に登録を有効にする

ドメイン マネージャの起動時に、Common Application Framework (CAF) をただちに登録するかどうかを指定します。

デフォルト: はい(True)

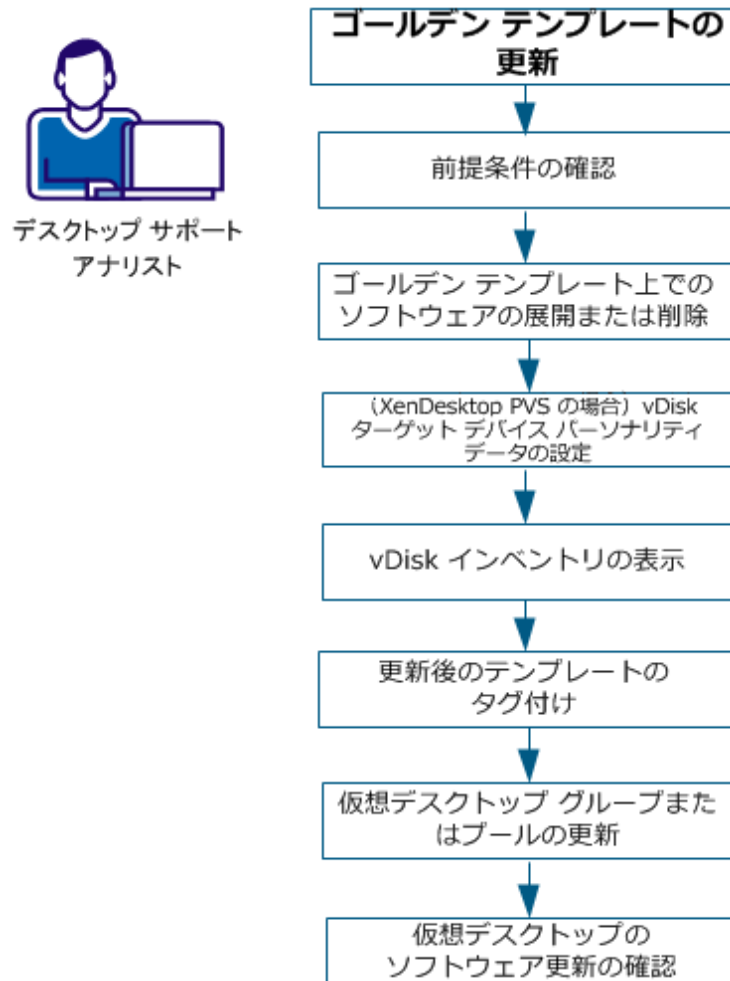
重要: CA DSM エージェント アドオン - VDI サポート - Windows ENU パッケージをインストールする前に、このポリシーをローカルで管理できるようにする必要があります。 ポリシーを右クリックして、コンテキスト メニューから [ローカル管理] を選択します。

注: CA DSM エージェント アドオン - VDI サポート - プレ R12.5Sp1 Feature pack1 の Windows ENU パッケージを使用した場合、このポリシーは VMware View ベースの仮想デスクトップにのみ適用可能です。

ゴールデン テンプレートの更新

ゴールデンテンプレートにソフトウェア パッケージを追加または削除する場合には、ユーザは、デスクトップ サポート アナリストとして、ゴールデンテンプレートの更新に責任を持つ必要があります。ゴールデンテンプレートの更新により、VMware View Clone、Citrix PVS ストリーム配信仮想デスクトップ、または MCS ベースの仮想デスクトップが更新されます。

以下の図に、ゴールデンテンプレートの更新で実行する手順を示します。



ゴールデンテンプレートの更新では、以下のタスクを実行します。

1. [前提条件の確認](#) (P. 354)
2. [ゴールデンテンプレートへのソフトウェアの展開](#) (P. 354)
3. [vDisk ターゲット デバイス個人データの設定](#) (P. 355)
4. [vDisk インベントリの表示](#) (P. 357)
5. [更新後のテンプレートのタグ付け](#) (P. 358)
6. [仮想デスクトップ グループまたはプールの更新](#) (P. 359)
7. [仮想デスクトップのソフトウェア更新の確認](#) (P. 360)

前提条件の確認

ゴールデンテンプレートを更新するには、以下の前提条件を確認します。

- 1 つ以上のゴールデン テンプレートを準備および展開したことを確認します。
- ゴールデンテンプレート コンピュータに、仮想デスクトップ エージェントがインストールされていることを確認します。

注: このシナリオには、VMware View や Citrix XenDesktop など、仮想デスクトップ ソリューションに関して実際に役立つ適切な知識が必要です。

- Citrix vDisk ベースの仮想デスクトップを作成する場合は、Citrix PVS ターゲット デバイスがインストールされていることを確認します。

ゴールデン テンプレート上でのソフトウェアの展開または削除

以下のいずれかの方法で、ゴールデンテンプレートにソフトウェア パッケージを展開または削除できます。

- ゴールデンテンプレート コンピュータ上で直接変更を行います。この方法は、スナップショット ベースの VMware View および Citrix MCS に適用できます。

- ゴールデン テンプレートから作成される vDisk を更新します。この方法は、Citrix Provisioning Services によってストリーム配信される Citrix XenDesktop 仮想デスクトップに適用できます。以下の考慮点が適用されます。
 - vDisk は、プライベート モードで、ゴールデン テンプレート コンピュータと同じ設定を持つコンピュータとして起動される必要があります。
 - Citrix Provisioning Server 内でプライベート モードでの vDisk の起動に使用されるターゲット デバイスは、テンプレート管理用に vDisk が起動されることを示す個人データが割り当てられます。個人データの詳細については、「[vDisk ターゲット デバイス個人データの設定](#) (P. 355)」を参照してください。
 - プライベート モードで初めて vDisk を起動する場合、Client Automation 内の管理対象エンティティとして vDisk が追加されます。その後、ソフトウェア配信を使用して、vDisk にパッケージを展開または削除できます。
 - vDisk は、DSM エクスプローラの [すべてのコンピュータ] 下に、以下の命名規則を持つコンピュータ レコードとして表示されます。
 <FarmName>-<StoreName>-<vDiskName>
 DSM エクスプローラにコンピュータ レコードが見つからない場合は、「DSM エクスプローラに vDisk レコードが見つからない」を参照してください。
 - 任意のコンピュータ上で、テンプレート管理のためにプライベート モードで vDisk を起動するときは、常に同じコンピュータ レコードが vDisk に使用されます。
 - プライベート モードで vDisk をホストするコンピュータが、すでに Client Automation 内の管理対象コンピュータの場合、ソフトウェア展開は、そのコンピュータ上ではなく、vDisk 上でのみ実行されます。
- 注: コンピュータが vDisk でプライベート モードで起動される場合、ローカル ドライブを持つコンピュータが起動されるまで、すべてのソフトウェア ジョブが待機します。

注: また、ゴールデン テンプレート自体を更新するか、それから vDisk を作成するか、または既存の vDisk を上書きして仮想デスクトップを更新できます。

(Xendesktop PVS に対して)vDisk ターゲット デバイス個人データの設定

Client Automation がプライベート モードで起動された vDisk をゴールデン テンプレートとして取り扱うことができるように、Provisioning Server コンソール内の vDisk ターゲット デバイス個人データを設定します。

次の手順に従ってください:

1. vDisk が割り当てられる Citrix Provisioning Services コンソール内でターゲット デバイスの [プロパティ] ダイアログ ボックスを開きます。
2. [Personality] タブをクリックし、以下のパラメータを追加します。

CA_DSM_GoldenTemplate

vDisk がゴールデン テンプレートか、またはプライベート モードの仮想デスクトップかを示します。パラメータの値を **True** に設定します。

ProvisioningServer

プロビジョニング サーバの IP アドレスまたはホスト名を指定します。

ProvisioningServicesUser

プロビジョニング サービス ファームへのアクセス権を持つユーザ名、またはプロビジョニング サーバ コンソールへの接続中に指定されるユーザを指定します。 **sd_acmd encrypt** コマンドを使用してユーザ名を暗号化し、暗号化された値を渡します。

ProvisioningServicesPassword

プロビジョニング サービス ユーザのパスワードを指定します。
sd_acmd encrypt コマンドを使用してパスワードを暗号化し、暗号化された値を渡します。

ProvisioningServerPort

SOAP サービスが実行されるプロビジョニング サーバのポートを指定します。デフォルト値は **54321** です。

注: [テンプレート インストール モード] のプッシュ中に、プロビジョニング サーバパラメータを、CA DSM エージェント VDI サポート アドオン パッケージ内のユーザ パラメータとしてゴールデン テンプレートに渡します。以下のフォーマットを使用します。

```
/pvsserver:<server IP/Name> /pvsuser:<encrypted username> /pvspwd:<encrypted  
pwd> /portno:<portno>
```

3. 変更を保存します。

vDisk ターゲット デバイス個人データは、ゴールデン テンプレートとして設定されます。

vDisk インベントリの表示

プライベート モードで vDisk を起動した後、Client Automation 内の管理対象エンティティとして追加されます。Citrix XenDesktop の例を以下に示します。

次の手順に従ってください: (DSM エクスプローラ内):

1. [コンピュータおよびユーザ] - [すべてのコンピュータ] - [vDisk_name] - [インベントリ] - [オペレーティング システム] ノードに移動します。

vDisk_name

FarmName-StoreName-vDisk.Name 形式で vDisk 名を指定します。

2. [テンプレート設定] サブフォルダを選択して、以下の属性に対する値を表示します。

IsGoldenTemplate

エージェントがゴールデン テンプレート (True) か、または仮想デスクトップ (False) かを示します。テンプレート管理のために、マスタ vDisk またはマスタ vDisk のクローンがプライベート モードで起動される場合、値は true に設定されます。

TemplateHostUUID

ゴールデン テンプレートのホスト UUID を指定します。マスタ vDisk について、hostuuid は、ゴールデン テンプレートおよびクローン作成された vDisk のマスタ vDisk です。

詳細については、「[vDisk の処理方法](#) (P. 360)」を参照してください。

TemplateName

ゴールデン テンプレートの名前を指定します。

TemplateTag

ゴールデン テンプレートが最後にタグ付けされた日時を示します。

3. [テンプレート履歴] ノードをクリックして、vDisk のテンプレート履歴を表示します。ゴールデン テンプレートに対する更新の履歴を参照できます。
4. [仮想化] - [Citrix XenvDisk] をクリックします。

vDisk のファーム、ストア、およびサイトが表示されます。

次の手順に従ってください: (Web コンソールで)

1. [コンピュータ] - [インベントリ] - [検出されたインベントリ] に移動し、[オペレーティング システム] をクリックします。
2. [詳細] タブ下の [テンプレート設定] をクリックして、[IsGoldenTemplate]、[TemplateName]、[TemplateTag]、および [TemplateHostUUID] 属性の値を表示します。
3. [詳細] タブ下の [テンプレート履歴] をクリックして、テンプレート履歴を表示します。

関係情報とテンプレート履歴を確認しました。

更新後のテンプレートのタグ付け

タグ付けにより、仮想デスクトップによって使用されるテンプレートのバージョンの追跡を支援します。テンプレートにタグ付けしてテンプレート タグを生成し、クローンをそれらの親のゴールデン テンプレートに関連付けます。

次の手順に従ってください:

1. DSM エクスプローラで、CA DSM エージェント アドオン VDI パッケージからゴールデンテンプレートにタグ テンプレート プロシージャをドラッグ アンド ドロップします。
2. 仮想デスクトップ ソリューションに応じて、以下のいずれかのアクションを実行します。
 - (Citrix PVS に基づく XenDesktop に対して) マシンをシャットダウンします。その結果、更新が vDisk に保存されます。
 - (VMware View と Citrix MCS の場合) 仮想マシンをシャットダウンし、スナップショットを作成します。

このアクションにより、テンプレート タグにスナップショットが関連付けられます。

仮想デスクトップ グループまたはプールの更新

更新したゴールデン テンプレートを使用する仮想デスクトップ グループまたはプールを更新します。仮想デスクトップ グループまたはプールの更新の詳細については、VMware View または Citrix XenDesktop のマニュアルを参照してください。仮想デスクトップ グループまたはプールが更新された後、ゴールデン テンプレート更新は、次の再起動時に仮想デスクトップに伝達されます。

更新された vDisk またはスナップショットを仮想デスクトップに割り当て、次の再起動時にゴールデン テンプレートの更新を伝達します。

次の手順に従ってください: (VMware ビューに対して)

1. ゴールデン テンプレートをシャットダウンします。
2. ゴールデン テンプレートのスナップショットを作成します。
3. 新しいスナップショットを使用して、プールの再構成操作を実行します。

次の手順に従ってください: (vDisk ベースの仮想デスクトップに対して)

1. vDisk コンピュータをシャットダウンします。
2. コンピュータから vDisk 割り当てを削除します。
3. vDisk モードを、標準または差分に変更します。
4. 仮想デスクトップに更新された vDisk を割り当てます。
5. 仮想デスクトップを再起動します。仮想デスクトップが次に再起動されるまで、変更は適用されません。

注: または、更新された vDisk は、自動的な、または Citrix Provisioning Services 増分 vDisk 更新機能を使用して、仮想デスクトップに割り当てることができます。

次の手順に従ってください: (MCS ベースの仮想デスクトップに対して)

1. ゴールデン テンプレートをシャットダウンします。
2. ゴールデン テンプレートのスナップショットを作成します。
3. プールされたカタログを新しいスナップショットで更新します。

仮想デスクトップのソフトウェア更新の確認

仮想デスクトップ ソフトウェアを表示して、ゴールデン テンプレートに対して行った更新が、仮想デスクトップ上で利用可能かどうかを確認します。

次の手順に従ってください:

1. [コンピュータおよびユーザ] - [すべてのコンピュータ] - [Virtual-Desktop] - [ソフトウェア] - [インストールされたパッケージ] ノードに移動します。

右ペインで、ゴールデン テンプレートまたは vDisk に加えた変更が、仮想デスクトップに反映されているかどうかを確認します。

ゴールデン テンプレートへの更新が完了しました。

vDisk および vDisk クローンの管理

デスクトップ サポート アナリストとして、Client Automation が vDisk とそのクローンの関係をどのように処理し管理するかを理解する必要があります。

このシナリオでは、Client Automation が vDisks とクローンを処理する方法について説明します。

vDisk クローンを処理する方法

仮想デスクトップをプロビジョニングするために、vDisks をコピーまたはクローン作成することができます。vDisk コピーまたはクローン、およびそれらの親 vDisk が、MDB に個別の管理レコードとして表示されます。プロビジョニング サーバファーム、ストア、サイト、vDisk 名の comstore 値によって、親 vDisk とクローンを作成された vDisk の親 vDisk が区別されます。

Client Automation は、以下のルールを使用して vDisk クローンを識別し、それらの個別の管理レコードを作成します。

- vDisk がテンプレート管理のためにプライベート モードで起動される場合、新しい管理レコードが Client Automation で作成され、エージェント名は *FarmName-StoreName-vDisk* 形式になります。
- vDisk クローンがテンプレート管理のためにプライベート モードで別のファームから起動される場合、クローンに対して新しい管理レコードが作成されます。
- クローンが同じファームかつ別のストアから起動される場合で、vDisk とその親名が異なる場合、vDisk コピーに対して新しい管理レコードが作成されます。
- vDisk コピーに対して、以下のルールで新しい管理レコードが作成されます。
 - クローン vDisk は、同じファームかつ別のストアから起動される
 - vDisk とその母体名は同じである
 - テンプレート管理のために vDisk が起動されるサイトとその親は異なる

注: サイトが親 vdisk と同じ場合、管理者は、MDB で管理レコードを作成するか、既存のものを再利用するかを確認するように促されます。
- 新しい管理レコードが、以下のルールで作成されます。
 - ファームとストアは同じ
 - vDisk 名を変更
 - 親 vDisk はストアの一部
 - vDisk はコピーとして起動される

注: 親 vdisk がストアの一部ではない場合、管理者は、MDB で管理レコードを作成するか、既存のものを再利用するかを確認するように促されます。
- vDisk、ファーム、およびストア名が同じ場合、既存の管理対象コンピュータレコードが再利用されます。

ゴールデン テンプレート、マスタ vDisk、およびクローン間の関係の表示

特定の vDisk が派生した vDisk を識別するために、Client Automation は、[テンプレート設定] およびテンプレート履歴下のインベントリを収集します。

このインベントリ情報を使用すると、特定の vDisk の直接的な親および vDisk に対して行われた変更の履歴を確認できます。関係は、以下のように識別されます。

- マスタ vDisk は、親としてゴールデン テンプレートを指します。
- プライベート モードでマスタ vDisk を起動した後、マスタ vDisk からクローンを作成する場合、クローンはその親としてマスタ vDisk を指します。
- プライベート モードでマスタ vDisk を起動する前にマスタ vDisk からクローンを作成した場合、クローンは、マスタ vDisk と同じであり、親としてゴールデン テンプレートを指します。そのようなマスタ vDisk の vDisk クローンからさらにクローンが作成される場合、すべてのクローンは、その親としてゴールデン テンプレートを指します。

次の手順に従ってください: (DSM エクスプローラで)

1. [コンピュータおよびユーザ] - [すべてのコンピュータ] - [vDisk_name] - [インベントリ] - [オペレーティング システム] フォルダに移動します。
2. [テンプレート設定] サブフォルダを選択して、以下の属性に対する値を表示します。

IsGoldenTemplate

問題のエージェントがゴールデン テンプレート (True) か、または仮想デスクトップ (False) かを示します。値は、マスタ vDisk とそのクローンについては true です。

TemplateHostUUID

ゴールデン テンプレートのホスト UUID を指定します。マスタ vDisk については、ゴールデン テンプレートのホスト UUID が表示されます。クローン作成された vDisks については、ホスト UUID が以下の要因に応じて異なります。

- マスタ vDisk がプライベート モードで起動された後にクローンが作成された場合、マスタ vDisk のホスト UUID が表示されます。
- マスタ vDisk がプライベート モードで起動される前にクローンが作成された場合、ゴールデン テンプレート システムのホスト UUID が表示されます。

TemplateName

ゴールデン テンプレートの名前を指定します。

TemplateTag

テンプレートがタグ付けされている場合にのみ、ゴールデン テンプレートまたは vDisk のテンプレートの日付とタイム スタンプを表示します。

3. テンプレートがタグ付けされている場合、[テンプレート履歴] サブフォルダを選択して、仮想デスクトップまたはテンプレートのテンプレート履歴を表示します。

次の手順に従ってください: (Web コンソールで)

1. [コンピュータ] - [インベントリ] - [検出されたインベントリ] ページに移動します。
2. [オペレーティング システム] タブをクリックして、[仮想マシン] 属性の値を表示します。
3. [詳細] タブ下の [テンプレート設定] をクリックして、[IsGoldenTemplate]、[TemplateName]、[TemplateTag]、および [TemplateHostUUID] 属性の値を表示します。
4. [詳細] タブ下の [テンプレート履歴] をクリックして、クローンのテンプレート履歴を表示します。

関係情報とテンプレート履歴を確認しました。

Client Automation からの仮想デスクトップの管理

デスクトップ サポート アナリストとしての責任には、Client Automation から仮想デスクトップを管理することが含まれます。仮想デスクトップの管理には、仮想デスクトップへのソフトウェアまたはパッチの展開、およびそれらからのインベントリの収集が含まれます。また、Client Automation がデスクトップ上にソフトウェアを再インストールする方法とタイミングを認識している必要もあります。

注: 仮想デスクトップでのソフトウェア パッケージの展開とインベントリの収集は、Client Automation 内での任意のコンピュータ上のソフトウェア展開およびインベントリ収集に類似しています

仮想デスクトップ用の実装ガイドライン

ゴールデンテンプレートにではなく、個別の仮想デスクトップにインストールされるソフトウェア パッケージについては、以下の制限およびガイドラインを考慮する必要があります。

- エージェントが登録されているスケーラビリティ サーバのソフトウェア ライブラリでステージされないパッケージは、再インストールされません。
- 再インストールは新しいファイルを使用する追加手順に対してはサポートされません。
- 再インストールは、ユーザ プロファイル エージェントに対してはサポートされません。コンピュータ エージェントに対してのみサポートされます。

- VMware View の [Offline Desktop] 機能を使用してチェックアウトされ、ロールバックされた場合（つまり、チェックアウトが破棄された）場合、ソフトウェア状態に対するどの変更もインスタンス ソフトウェア データベースに残ります。オフライン RAC を実行した場合、ソフトウェアが状態データベースに記録され、ロールバック中に削除されなかったため、ソフトウェアは再インストールされます。そのため、そのソフトウェアが必要でない場合、手動でアンインストールする必要があります。
- 再起動/ログオフ/シャットダウン オプションが有効にされた **Software Delivery** ジョブの送信は、非永続的な仮想デスクトップに対してはサポートされていません。非永続的なデスクトップは、ユーザがログオンしている間のみ、ユーザに関連付けられます。次回、ユーザがログオンする時に、ユーザは別のデスクトップに割り当てられる可能性があります。したがって、これらのオプションはこのケースにとって適切ではありません。
- ネットワークを介した転送に長時間かかるパッケージ、またはインストールに長時間かかるパッケージは、個別の仮想デスクトップではなく、ゴールデンテンプレートにインストールする必要があります。そうしないと、再インストールに時間がかかりすぎます。
- 仮想化アプリケーションは、ゴールデンテンプレートに事前にステージでき、後でスタンドアロンインストールを実行して個別の仮想デスクトップにプロビジョニングできます。このようにすると、再構成/リフレッシュ、および使用中のネットワーク帯域幅の使用量が最小化されます。
- 前の項目のような結果は、調査、または微調整を行った、SXP、PIF、および MSI などの管理対象パッケージ形式を使用して達成できます。たとえば、SXP は、パッケージがゴールデンテンプレートにインストールされることを可能にするユーザ フィルタを提供します。ただし、フィルタは、特定のローカルまたはアクティブ ディレクトリ ユーザ グループに属しているクローンのユーザに対してのみ使用可能になります。
- 仮想化アプリケーションを、ストリーミングモードの個別の仮想デスクトップにプロビジョニングする必要があります。このようにすると、再構成/リフレッシュ中のネットワーク帯域幅の使用量は最小化されますが、使用中は最小化されません。
- リダイレクトされたユーザ プロファイル/フォルダの外部に設定を格納するアプリケーションは、再インストールの後に自動的にそれらの設定を保持しません。インストールの一部として継承するのではなく、設定をリセットしたアプリケーションは、この問題に直面します。
- テンプレート ソフトウェア状態データベースおよびインスタンス ソフトウェア状態データベースの両方に、同じソフトウェアで、別のバージョンのレコードが含まれる場合、アップグレードまたはダウングレードは引き続き、オフライン RAC によって実行されます。管理者は適切にシステムを設定し、特にダウングレードのシナリオで、そのようなケースを防ぐ責任があります。

- DTS ダウンロード方式は、仮想デスクトップ エージェントに対してサポートされていません。
- 非永続的なデスクトップ プールについては、ユーザがログオンする場合にのみ、再インストールが実行されます。
- リンク クローンの仮想デスクトップの場合の、ソフトウェア配布機能用のユーザ プロファイル モードを無効にすることを推奨します。

ユーザおよび仮想デスクトップの間に 1 対 1 の関係があるので、ユーザ プロファイルはここでは必要ありません。ユーザ プロファイルの有効化によって、エージェントおよびスケーラビリティ サーバ間に追加の通信が発生し、全体のスケーラビリティに影響を与える可能性があります。

オフライン RAC

オフライン **RAC** は、マネージャではなくエージェントによって起動される、クラッシュ後の再インストール (**RAC**) タスクです。仮想デスクトップは頻繁に再構成されます。つまり、ゴールデンテンプレートが更新され、ディスクがリセットされた場合は常に、以前のリセット以降の仮想デスクトップへの変更がすべて実質的に無効になります。仮想デスクトップでは、マネージャではなくエージェントが **RAC** ジョブ コンテナの作成を担当します。ディスク リセットが発生すると、エージェントは、そのエージェントに展開されているソフトウェアをすべて復元するためにオフライン **RAC** を開始します。

オフライン **RAC** の場合、ソフトウェア配信エージェントにはファイル システムベースのソフトウェア状態データベースが含まれます。このデータベースには、インストールされた各ソフトウェア パッケージに関する以下の情報が含まれます。

- ソフトウェアのインストールに使用されるプロシージャ
- エージェントのみのコンピュータ ターゲット用のインストール後の有効化または設定プロシージャ。
- ユーザ パラメータなどのジョブ固有の情報。

このソフトウェア状態データベースは、ソフトウェア配信エージェントによって管理され、ソフトウェア ジョブが実行されるたびに更新されます。アンインストールが成功すると、そのソフトウェア パッケージ固有のレコードが削除されます。有効な場合、ソフトウェア状態データベースには常に、エージェントの現在のソフトウェア配信状態が反映されています。

ソフトウェア状態データベースは、仮想デスクトップの元になっているゴールデンテンプレートのインストール履歴も継承します。ソフトウェア状態データベースは2つの部分に分かれています。1つはゴールデンテンプレート用で、もう1つはクローンが作成されたインスタンス用です。ソフトウェア状態データベースのテンプレート部分は、ゴールデンテンプレートのシステムディスク上に格納されています。ゴールデンテンプレートをターゲットにする任意のソフトウェアジョブは、このデータベースのみを使用します。仮想デスクトップのクローンが作成される場合、そのエージェントはインスタンスソフトウェア状態データベースのみを使用して、その状態を追跡します。

クローンが作成された仮想デスクトップのシステムディスクは、再構成またはリフレッシュの操作中に破棄されるため、インスタンスソフトウェア状態データベースはシステムディスクに格納できません。このデータベースは、共通設定ポリシーによって管理されている別の場所に格納する必要があります。たとえば、クローンとリンクしている VMware View のユーザデータディスク、または仮想デスクトップからアクセス可能なファイルサーバなどです。

重要: 管理者は、標準的なソフトウェアジョブの管理中やオフラインインストールの実行中に、ソフトウェア状態データベースへ常にアクセスできるようにする必要があります。インスタンスソフトウェアデータベースがネットワーク共有上にある場合は注意が必要です。

関連項目:

[エージェント \(Software Delivery\) ポリシー グループ \(P. 346\)](#)

再インストールのステータス

再インストールプロセスの最後に、各ジョブが成功したか、失敗したかがドメインマネージャに報告されます。オフラインで再インストールを実行している場合は、エージェントの「ソフトウェア配信ジョブ確認」ダイアログボックスにもこのステータスが表示されます。

「RAC から除外」などの設定が原因でジョブが失敗するか、一部のジョブが実行できない場合、「ソフトウェア配信ジョブ確認」ダイアログボックスは、ユーザが明示的にダイアログボックスを閉じるまで、開かれたままになるように設定されます。このソフトウェア配信エージェント RAC ポリシーは設定可能で、オフにできます。また、無効なダウンロード方法や、レガシースケーラビリティサーバへの報告試行などが原因で、オフラインの再インストールを開始できなかった場合、この障害が「ソフトウェア配信ジョブ確認」ダイアログボックスで報告されます。さらに、スケーラビリティサーバがさまざまな理由によりアクセスできない場合、再インストールの再試行、延期、または中止を実行するオプションがエンドユーザに提供されます。

コンピュータプロパティ

エージェントポリシーの[RACポリシー]設定のデフォルト値は、[コンピュータプロパティ]ダイアログボックスの[ソフトウェア配信]タブで設定されます。
[エージェントポリシー]をTrueに設定すると、[RACポリシー]フィールドは無効になり、設定を変更できません。

DTSダウンロード方法は、オフライン RAC 中は、仮想デスクトップに対してサポートされていません。そのため、このオプションは[ダウンロード方法]ドロップダウンリストに表示されません。

仮想マシンのロック解除

エージェントがソフトウェアを再インストールした後、オフライン RAC 終了通知をスケーラビリティサーバに送信します。スケーラビリティサーバは次にその通知をマネージャに送信します。マネージャがこの通知を受信した後、仮想マシンはオフライン RAC からロック解除されます。

ただし、エージェントがソフトウェアを再インストールしたにもかかわらず、オフライン RAC 完了通知をスケーラビリティサーバに送信できなかった場合、仮想マシンを強制的にロック解除できます。たとえば、サーバがその瞬間に使用可能でなかったため、エージェントが通知を送信できない場合、仮想マシンをロック解除できます。

以下の手順に従います。

1. DSM エクスプローラで、[コンピュータおよびユーザ]-[すべてのコンピュータ]フォルダに移動します。
2. 対応する[すべてのコンピュータ]ペインで、関連するアセットを右クリックします。
3. 表示されたコンテキストメニューから[保留中 RAC ロックのクリア]コマンドを選択します。

注: 1 台または複数の仮想マシンが RAC によってロックされていることが[SD ステータス]列に示されている場合にのみ、この新しいコマンドが使用できます。それ以外の場合、コマンドは無効です。さらに、RAC 状態によってロックされた標準コンピュータに対して、このコマンドは使用できません。

選択されたアセットはロック解除されます。

DSM エクスプローラからの仮想マシンの削除

クローンを作成した後、ゴールデン テンプレートにあるドメイン マネージャから別のドメイン マネージャに移動すると、ゴールデン テンプレートは標準的な移動機能に従って移動されます。ただし、このゴールデン テンプレートから作成したクローンを再構成すると、クローンは自動的に新しいドメイン マネージャにレポートされます。そのため、オフライン RAC を使って、すべてのインストール履歴が再生成されるため、再構成されたクローンに対して移動を実行する必要はありません。

以前のドメイン マネージャへのレポートに使われた後、管理対象外となった使われなくなったクローンを削除するには、ゴールデン テンプレートのクローンを再構成した後、そのマネージャから移動したすべてのクローンを手動で削除します。

また、ネーミング パターンを変更してから、VMware View を使用して特定の仮想マシンを削除すると、新しい仮想マシンが新しい名前で作成されます。この場合、DSM エクスプローラから仮想マシンを手動で削除します。

ソフトウェア プロシージャ

ソフトウェア 配信システムは現在、ソフトウェア プロシージャごとに、RAC を有効にするか、無効にするか設定できます。項目プロシージャを RAC 処理の一部として実行しない場合は、実際のプロシージャの [プロパティ] ダイアログ ボックスで [RAC から除外する] オプションを選択します。このオプションを使うと、廃止されたパッケージやパッチを RAC から除外できます。

RAC から除外機能がオフライン RAC をサポートするように拡張されました。オフラインの再インストール時に、[プロパティ] ダイアログ ボックスの [RAC から除外する] 設定をソフトウェア プロシージャごとにオンにします。プロシージャを除外すると、そのプロシージャは実行されません。

再構成なしで仮想デスクトップに関連する重大なセキュリティ問題を解決するための個別パッチなどがその例です。ただし一度再構成すると、新しいバージョンのゴールデン テンプレートにはすべてのパッチが適用されるため、パッチの再インストールは不要になります。

仮想デスクトップ上でのセキュリティ パッチの適用

ユーザのログアウトまたは再起動後は変更が持続しない仮想デスクトップ上でソフトウェアの再インストールをトリガするために、Client Automation はオフライン RAC 処理を実行します。ユーザが仮想デスクトップに次回ログインするときに、オフライン RAC は、ログアウトまたは再起動の前にインストールしたソフトウェアとパッチを再インストールします。

(オプション)RAC 中、または再構成可能な仮想デスクトップ上でパッチ展開を処理するパッチマネージャの設定

パッチは、置き換えやロールアウトの順序を考慮せずに再展開されるため、デフォルトでは、RAC 中はパッチの展開が除外されます。この動作により、予期しない結果が発生する場合があります。同様に、ブラックリスト記載のターゲットも、パッチ展開中に除外されます。

再構成可能な仮想デスクトップは、デフォルトではブラックリスト記載のコンピュータの一部です。RAC から除外するため、およびブラックリスト記載のコンピュータを無視するためのデフォルト設定は、パッチ展開の処理に理想的です。設定を変更して、デフォルト動作を変更できます。

次の手順に従ってください:

1. CA Patch Manager にログインします。
2. [管理] - [設定] - [システム設定] - [DSM] - [オプション] に移動します。
設定オプションが表示されます。
3. 必要に応じて、以下のパラメータを変更します。

RAC から除外する

RAC 処理中のパッチ展開を除外します。RAC 中にパッチを展開するには、このオプションをクリアします。パッチは、置き換えやロールアウトの順序を考慮せずに再展開されるため、予期しない結果が発生する場合があります。

展開内のブラックリスト記載のコンピュータを無視する

パッチ展開中に、ブラックリスト記載のターゲットを選択されたターゲットリストに追加するときに、デフォルト オプションを指定します。パッチの展開で、選択されたブラックリスト記載のターゲットを含めるには、このオプションをクリアします。また、個別の展開で、このオプションを変更することもできます。指示されなかった場合に、ブラックリスト記載のターゲットを常に無視するには、このオプションを選択します。

ポリシー内のブラックリスト記載のコンピュータを無視する

ポリシーの評価中に、ブラックリスト記載のターゲットを無視する必要があることを指定します。このオプションを選択すると、UPM ブラックリストクエリが UPM ポリシークエリに追加されます。

ブラックリストクエリは、パッチ展開から除外されるコンピュータのリストを取得します。デフォルトでは、**blacklistQuery** パラメータは、**UPM – Blacklisted Computers** クエリに設定されています。このクエリは **Recomposable Computers** というクエリにリンクされ、インベントリ項目に基づく再構成可能なデスクトップを取得します。インベントリ項目 **IsRecomposable** は、[インベントリ] - [オペレーティングシステム] - [テンプレート設定] 下にあります。再構成可能なデスクトップに加えて、コンピュータを **UPM – Blacklisted Computers** に追加し、またはこのようなコンピュータを除外するクエリを作成できます。新しいクエリに、**Recomposable Computers** という名前のクエリが含まれていることを確認します。ブラックリスト記載のコンピュータのクエリを作成する場合、**Black List Query** パラメータでクエリの名前を指定します。

注: 既存の UPM ポリシーとパッケージを自動的に更新するには、それらをアップグレードしたことを確認します。アップグレードの詳細については、「Patch Manager パッケージおよびポリシーの更新」を参照してください。

4. 設定を保存します。

Patch Manager は、RAC、およびパッチ展開中にブラックリスト記載のコンピュータを処理するように設定されています。

vDisk またはゴールデン テンプレートへのパッチの適用

vDisk またはゴールデン テンプレートにセキュリティ パッチを適用することにより、仮想デスクトップに必要なすべてのセキュリティ パッチがインストールされることが保証されます。vDisk またはゴールデン テンプレートにパッチを適用するには、ゴールデン テンプレートの更新シナリオで指定されたプロセスに従います。

ブラックリスト記載のターゲットまたは再構成可能なデスクトップへのパッチの適用

デフォルトでは、再構成可能なデスクトップはブラックリスト記載のターゲットの一部であり、ブラックリスト記載のすべてのターゲットが、パッチの展開から除外されます。ただし、要件がある場合には、ブラックリスト記載のターゲットに対してパッチを適用できます。

次の手順に従ってください:

1. CA Patch Manager にログインし、ブラックリスト記載のターゲットで適用するパッチをクリックします。
2. [パッチの詳細] ページで [パッチを展開] をクリックします。
3. ブラックリスト記載のターゲットが含まれるグループを選択するか、またはブラックリスト記載の個別のターゲットを選択し、隣接する [選択したターゲット] ペインにそれらを追加します。

選択したグループ内のブラックリスト記載のターゲットのリスト、または個別のターゲットのリストが、[ブラックリスト記載のターゲット] ペインに表示されます。

4. [ブラックリスト記載のターゲット] ペインから、パッチを適用するターゲットを選択します。隣接する [選択したターゲット] ペインに、これらのターゲットを追加します。[次へ] をクリックします。
5. 展開スケジュールを指定します。[次へ] をクリックします。
6. [展開内のブラックリスト記載のコンピュータを無視する] オプションをクリアします。[完了] をクリックします。

選択されたターゲット上のパッチ展開が、スケジュールされた時間に開始します。

VDI インベントリの表示

インベントリ情報は、仮想デスクトップがテンプレートかクローンかを示す異なる値を使って、ゴールデン テンプレートと仮想デスクトップの両方に収集されます。

次の手順に従ってください:

1. [コンピュータおよびユーザ] - [すべてのコンピュータ] - [コンピュータ名] - [インベントリ] - DSM エクスプローラのオペレーティング システム ノードの順に移動します。

[オペレーティング システム] ペインを表示します。

2. [仮想マシン] 属性の値を確認します。

コンピュータが仮想マシンかどうかを指定します。

3. [テンプレート設定] を選択します。

以下の属性が表示されます。

IsGoldenTemplate

仮想マシンがゴールデン テンプレート (True) か、クローン (False) かを指定します。

Recomposable

仮想デスクトップが再構成できるかどうかを指定します。

TemplateHostUUID

(クローンのみ) ゴールデン テンプレートのホスト UUID を指定します。

TemplateName

(クローンのみ) ゴールデン テンプレートの名前を指定します。

TemplateTag

(クローンのみ) タグ付けされたテンプレート スナップショットの日時を指定します。

4. テンプレート履歴の選択

スナップショットがタグ付けされている場合、クローンのテンプレート履歴を表示します。

5. 収集した仮想化インベントリを表示するには、[コンピュータおよびユーザ] - [すべてのコンピュータ] - [コンピュータ名] - [インベントリ] - [仮想化ノード] の順に移動します。

コンピュータが使用するデスクトップ仮想化テクノロジーを表示します。

6. 仮想ノードを展開し、以下を選択します。

VM Ware View

プール名およびエージェント バージョンを表示します。

Citrix XenDesktop 設定

Citrix ファーム、グループ、ライセンスおよび製品情報を表示します。

注: その他の任意のインベントリ データと同様に、仮想化インベントリを使用してクエリとレポートを作成できます。

クエリおよびレポート

テンプレートに基づいた個別のデスクトップに加えて、テンプレート デスクトップでのクエリとレポートをサポートするため、基本ハードウェア インベントリが以下の属性および値で拡張されました。

ゴールデン テンプレート

ブール値

テンプレートの名前に基づく

文字列

テンプレートのバージョンに基づく

整数

テンプレートのホスト UUID に基づく

文字列

これらの属性は、DSM エクスプローラの [すべてのコンピュータ]、[コンピュータ名]、[インベントリ]、[オペレーティング システム] ペインに表示されます。

クエリ デザイナの変更点

クエリを作成するときに、ステータスがオフライン **RAC** のコンピュータについてレポートするための追加の引数を使用できるようになりました。さらに、事前定義済みのクエリが **VDI** サポートに対して追加されました。

- コンピュータ ベースのクエリの場合、クエリ デザイナの [フィールドの選択] ダイアログの [**RAC** ポリシー] ドロップダウン リストに値 [オフライン] が追加されました。
- 2 つの事前定義済み **VDI** サポート クエリ、[すべてのゴールデン テンプレート] および [ゴールデン テンプレートのすべてのクローン] が、**DSM** エクスプローラの [クエリ] ノードに追加されました。

DSM Reporter の変更点

VDI サポート用の以下の事前定義済みレポート テンプレートが **DSM Reporter** に追加されました。

- すべてのゴールデン テンプレート
- ゴールデン テンプレートのすべてのクローン

レポート テンプレートが実行され、インベントリが収集されると、これらのレポートに、検出されたゴールデン テンプレートおよびそれに対応する仮想デスクトップがすべてリスト表示されます。

廃止アセット ウィザードによるゴールデン イメージの除外

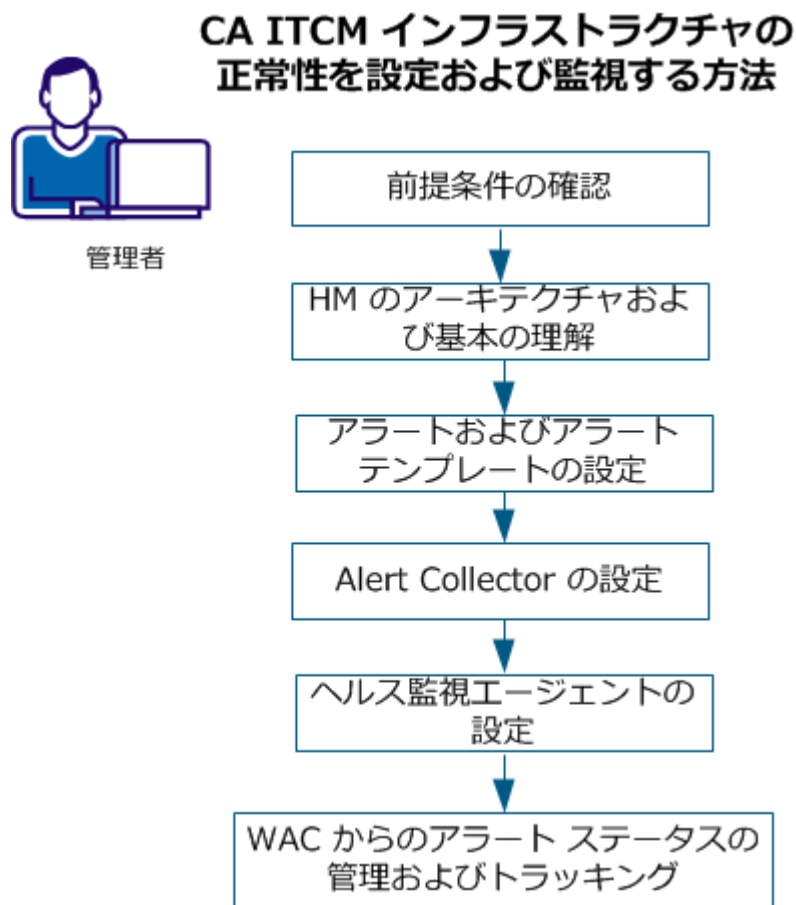
廃止アセット ウィザードは、古くなって使われなくなったコンピュータやユーザを追跡して、必要に応じて削除するのに役立ちます。ゴールデン テンプレートは標準のコンピュータおよびそのユーザと論理的に異なるため、ウィザードを生成する廃止資産クエリの結果セットから除外されていました。 **CA IT Client Manager** の前のリリースを使用して作成された廃止資産クエリは、ゴールデン テンプレートおよび関連ユーザを除外しません。そのため、既存の廃止資産クエリを置き換えて、ゴールデン テンプレートが結果セットから除外されることを確認します。

第 9 章: Client Automation インフラストラクチャの正常性を設定および監視する方法

Client Automation コンポーネントの正常性の管理は、管理者の担当範囲に含まれます。ヘルス監視（HM）機能は、以下のことを実行して正常性検査メカニズムを提供します。

- Client Automation 正常性条件を定義する
- インフラストラクチャを定期的に監視する
- 定義された条件が検出された場合にアラートを生成する
- 電子メールを送信し、SNMP トラップを生成し、Windows/CCS イベント ログに書き込むことにより、管理者に通知します。
- アラート レメディエーションの設定

Client Automation 可用性および回復力を改善するために HM 機能を使用します。
以下の図に HM のプロセスをまとめます。



以下のタスクを実行できます。

アラートの設定

使用可能なアラートを設定したり、新しいアラートを定義したりします。

アラートアクションの設定

電子メールの送信、SNMP トラップの生成、システムへの書き込み、CCS イベント ログへの書き込みなどのアラート アクションを設定します。

アラートの管理

アラートを WAC から表示、トラッキング、フォローアップ、およびクリアします。

このセクションには、以下のトピックが含まれています。

[前提条件の確認](#) (P. 379)

[HM アーキテクチャおよび基本の理解](#) (P. 380)

[アラートおよびアラート テンプレートの設定](#) (P. 385)

[Alert Collector の設定](#) (P. 396)

[ヘルス監視エージェントの設定](#) (P. 404)

[WAC からのアラート ステータスの管理およびトラッキング](#) (P. 410)

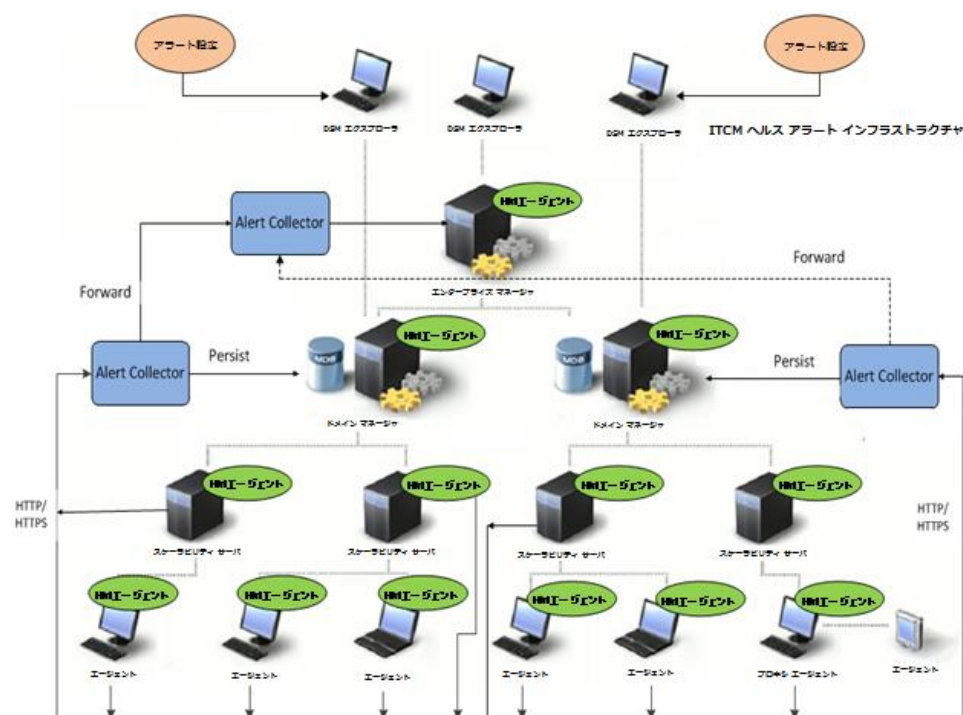
前提条件の確認

HM アラートを設定および監視する前に、以下の点について確認します。

- Client Automation インフラストラクチャに関する実務知識がある
- HM アーキテクチャおよび基本を理解している
- 既存のインフラストラクチャを Client Automation リリース 12.9 にアップグレードする
- Alert Collector をインストールする

HM アーキテクチャおよび基本の理解

以下の図は、HM 機能のコンポーネントと、Client Automation の正常性を監視するためのそれらのやりとりを示しています。



HM の基本についての詳細は、以下を参照してください。

- [アラートおよびアラート テンプレート](#) (P. 381)
- [ヘルス監視コンポーネント](#) (P. 382)
- [外部プロセス マネージャ \(CAF プラグイン\)](#) (P. 384)

アラートおよびアラート テンプレート

HM 機能は以下のアラート タイプを監視します。

パラメータ化されたアラート(アラート テンプレート)

追加パラメータをアラート定義の一部としてサポートします。それらのパラメータに対して指定される値に基づいて、監視の頻度、しきい値、重大度などのアラート プロパティをカスタマイズすることができます。パラメータ化されたアラートの定義および設定は、アラート テンプレートによって支援されます。

アラート テンプレートは、パラメータ化されたアラートのデフォルト定義とそのサポートされるパラメータのリストを提供します。テンプレートをベースとして使用し、異なるパラメータ値と関連する設定を使用して 1 つ以上のアラートを作成します。

パラメータ化されていないアラートまたはプレーン アラート(アラート)

追加パラメータはサポートされません。システムで定義されているアラート プロパティを使用します。

HM 機能は、すぐに使用できるアラート テンプレートとアラートを提供します。DM スクリプトに基づいて、カスタマイズされたテンプレートおよびアラートを作成することができます。アラートおよびアラート テンプレートのリストについては、ユーザ インターフェースを参照してください。

ヘルス監視コンポーネント

HM 機能により、以下のコンポーネントが導入されます。

HM エージェント

共通エージェントとともにインストールされ、**Client Automation** インフラストラクチャのすべての層に存在する、永続的なモジュールです。

- エージェント上のアラート設定を解釈し、アラート条件の発生を定期的に監視し、正常性条件の検出を管理者に通知します。

注: アラート モニタリングはデフォルトで無効です。ヘルス監視を有効にするには、設定ポリシーを適用します。

- 操作用の以下のコマンドライン オプションを入力します。

`hmagent start`

HM エージェントを起動します。

`hmagent stop`

HM エージェントを停止します。

`hmagent status`

エージェントが実行されているか、ヘルス監視が有効かどうかを表示します。

- HM エージェントは、Windows プラットフォーム上のサービスおよび Linux および Unix プラットフォーム上のデーモンです。

Alert Collector

Alert Collector は以下のモジュールから構成されます。

Web モジュール

HM エージェントからアラートを受信し、設定されたフォルダにそれらをコピーします。

永続的なモジュール

設定されたフォルダを監視し、設定された **Alert Collector** ロールに従って新しいアラートを処理します。詳細については、「[Alert Collector の設定](#) (P. 396)」を参照してください。

Alert Collector には以下の要件があります。

- Alert Collector は Windows のみでサポートされています。
- IIS のインストールは前提条件です。
- Application Development オプションがインストールされている状態で ISAPI 拡張機能および ISAPI フィルタが使用可能であることを確認します。
- Alert Collector がアラートを出し続ける DB タイプに応じて、32 ビット SQL または Oracle クライアントをインストールする必要があります。

Web モジュール アプリケーションは、IIS で HM Web サービスをホストします。この Web サービスは、既存の Client Automation Web サービス機能に依存せず、個別のアプリケーション プールで実行されます。

管理者は、サポートされているコマンドラインから Alert Collector プロセスを開始、停止し、プロセスのステータスを問い合わせることができます。Alert Collector は HM エージェントに類似したコマンドライン オプションをサポートします。

注: FIPS モードを変更する場合は常に、関連する [変更アクション] パラメータの値を確認してください。パラメータの値が [マシンを再起動します] 以外の場合は、CAF の再起動後、以下のコンポーネントの再起動も行っており、すべての Client Automation コンポーネントで FIPS モードが正常に切り替わるようにする必要があります。

マネージャまたはスタンドアロンの Alert Collector コンピュータの場合

- Alert Collector
- ヘルス監視エージェント

スケーラビリティ サーバまたはエージェント コンピュータの場合

- ヘルス監視エージェント

WAC 上のアラート

新しいアラートが生成されると、DSM エクスプローラによって通知が表示されます。通知には WAC を起動するためのハイパーリンクが含まれており、WAC への統合ログインが有効になっている場合は、アラート ページにアクセスできます。統合ログインが有効になっていない場合は、適切なユーザ クレデンシャルを入力してアラート ページに移動します。

外部プロセス マネージャ(CAF プラグイン)

このプラグイン (`cfProcessManager`) は、HM エージェントおよび `Alert Collector` などの外部プロセスを管理します。プラグイン機能は `CAF` に似ています。`CAF` は `Client Automation` 準拠のプラグインを管理しますが、プロセス マネージャは、`CAF` プラグインではない外部プロセスを管理します。

`cfProcessManager` が管理する外部プロセスは、*Maxinstances*、*Maxrestarts*、*Restartifdied*、*Enabled*、および *Maxrestarttime* などの通常の `CAF` プラグイン プロパティをサポートします。これらのプロパティの動作は `CAF` プラグインに似ています。

以下の追加のプロパティがサポートされます。

Startwithcaf

`CAF` の起動時に起動するプロセスを定義します。

デフォルト : `CAF` で起動しない。

Stopwithcaf

`CAF` の停止時に停止するプロセスを定義します。

デフォルト : `CAF` で停止しない。

Commandline

プロセスのコマンドラインを示します。

Startcmd

起動コマンドを定義します。デフォルト : `start`。

Stopcmd

停止コマンドを定義します。デフォルト : `stop`。

Statuscmd

ステータス コマンドを定義します。デフォルト : `status`。

注: 上記の設定を変更する場合、`cfProcessManager` を再起動します。

`CAF` の起動および停止コマンドで機能する新しい */EXT* オプションが導入されています。

Caf start /EXT

プラグイン、およびプロセス マネージャが管理する有効な外部プロセスをすべて起動します。

Caf stop /EXT

プラグイン、およびプロセス マネージャが管理する有効な外部プロセスをすべて停止します。

Caf status cfProcessManager コマンドは、外部プロセスのステータスを表示します。

アラートレメディエーション

特定のアラート状態の検出では、マシンでの問題を解決する修復アクションを関連付けることができます。以下のいずれかの修復アクションを指定します。

1. デフォルトアクション
2. スクリプト ベースのアクション

アラートおよびアラート テンプレートの設定

DM、EM、SS および Agent などの Client Automation コンポーネントの健全性を監視できます。重大度、しきい値、頻度の値を指定するアラートまたはアラートのテンプレートを作成します。

次の手順に従ってください:

1. [コントロール パネル] - [設定] - [設定ポリシー] - [DSM] - [ヘルス監視] - [アラート設定] に移動します。
2. 以下のエンティティを設定します。

アラート

事前定義されたアラートの頻度、しきい値、重大度などのアラート パラメータを設定したり、テンプレートに基づいてアラートを作成したり、DM スクリプトに基づいてアラートを作成したりします。

アラートテンプレート

事前定義されたアラート テンプレートのパラメータを設定したり、DM スクリプトに基づいてテンプレートを作成したりします。

アラートまたはアラート テンプレートが定義されます。

アラートの設定

次の手順に従ってください:

1. [コントロール パネル] - [設定] - [設定ポリシー] - [DSM] - [ヘルス監視] - [アラート設定] - [アラート] に移動します。
2. [追加] を選択して、テンプレートまたはスクリプトに基づくアラートを作成します。
3. 以下のフィールドに適切な値を指定します。

アラート名

アラートの名前を指定します。

テンプレート

アラートを生成するアラート テンプレートの名前を設定します。

注: テンプレート ベースのアラートを作成するには、ドロップダウン リストからテンプレートを選択します。たとえば、[アセット ジョブが更新されませんでした] を指定します。

スクリプト

スクリプト ベースのアラートのスクリプト名を指定します。

パラメータ

アラートに適したパラメータを指定します。

注: アラートがテンプレートから生成されると、テンプレート パラメータがテンプレートから引き継がれます。例:

```
GROUPS=ComputerGroups;RequiredPercentage=MINPERCENT;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%
```

注: スクリプト ベースのアラートのパラメータを指定することもできます。

メッセージ

アラート条件が検出された場合に評価されるアラート関連情報を定義します。この評価された情報は、HM エージェントによって生成されたアラートの一部として渡されます。例:

コンピュータ グループ *\$GROUPS* 内の *\$PERCENTAGE* 未満のコンピュータがアセット ジョブ結果をレポートしました

重大度

アラートの重大度をドロップダウン リストから設定します。

有効

アラートの状態を指定します。[True]に設定するとアラートが HM エージェントによって監視され、それ以外の場合は監視から除外されます。

検出層

アラートが検出される層を指定します。EM、DM、SS、エージェントなどを指定します。

注: 事前定義されたアラートについては、サポートされるリストから層を選択します。テンプレート ベースのアラートについては、テンプレートによってサポートされるリストから層を選択します。

動作周波数

アラートが監視される間隔を指定します。検出される各層について、頻度を分、時間、または日単位で指定できます。

しきい値

しきい値を指定します。この値は、アラートを生成させるアラート条件の存続期間（分/時間/日）またはアラート条件の発生回数を示します。

たとえば、エージェント層に頻度を 1 時間、しきい値を 6 時間と設定した [エージェントが SS と通信できない] を設定する場合、HM エージェントは 1 時間ごとにチェックし、エージェントがリモート スケーラビリティ サーバに通信できるかどうかを確認します。6 時間通信できない場合、アラートが生成されます。

レメディエーション

アラート用の修復方法を識別します。

hmStartCaf.dms

CAF サービスを起動します。

hmRepairWinAgent.dms

[パラメータ] 下で指定されるコンポーネントを修復します。エージェントのステージングをスケーラビリティ サーバ上で行う必要があります。（Windows でのみ有効です）。

パラメータ

レメディエーションが必要なコンポーネントを指定します。たとえば、`hmRepairAgent.dms` については、レメディエーションとして修復が必要となる **AM**、**SD**、**RC** および **ALL** を指定できます。

注: カンマ区切りリストで、**AM**、**SD**、**RC** および **ALL** の組み合わせを指定します。

4. (オプション) 値を確認するには [確認] をクリックします。
5. [適用] をクリックし、[OK] をクリックします。

これでアラートの設定が完了しました。

DM スクリプト ベースのアラートの作成

DM スクリプトに基づくカスタム アラートを作成できます。これらのアラートに関連する設定を適用する前のエージェント マシンで、スクリプト ディレクトリ（[設定ポリシー]-[*DSM*]-[ヘルス監視]-[ヘルス監視エージェント]-[*ScriptDir*] で設定される）にスクリプトを展開します。

次の手順に従ってください:

1. [コントロール パネル] - [設定] - [設定ポリシー] - [*DSM*] - [ヘルス監視] - [アラート設定] - [アラート] に移動します。
2. [追加] を選択して、スクリプトに基づくアラートを作成し、テンプレート名のフィールドを空のままにしておきます。
3. エージェント マシンに展開する **DM** スクリプト名を指定します。
4. [パラメータ] フィールドにパラメータを指定します。
5. メッセージフィールドに、アラートに関連するテキストを追加します（必要に応じて、パラメータを持つアラートに関して）。
6. その他のアラート パラメータを設定し、監視用のエージェントに適用します。

DM スクリプトアラートの例:

以下の DM スクリプトは、`hmAlertOPFormatter` を呼び出すことにより、アラート条件があるかないかを **HM** エージェントにレポートします。例:

```
'Do your alert condition checking here.
'...
' At bottom of your DM script, execute hmAlertOPFormatter
' to create the alert XML output.
dim ret as integer
ret = Exec("hmAlertOPFormatter.exe alertconditionexist=1 raisealertnow=1
""param1="" + argv(1) + ",param2="" + argv(2) + """" additionalinfo=this is some
additional text for script with Args", true)
print "hmAlertOPFormatter.exe: " + str(ret)
```

アラートを監視するために呼び出されたときに HM エージェントが処理する XML ファイルを作成するには、DM スクリプトで以下のコマンドを実行します。

hmAlertOPFormatter 実行可能ファイル

```
hmAlertOPFormatter.exe alertconditionexist=0|1 [raisealertnow=0|1]  
[PARAM1=data1,PARAM2=data2,...,PARAMX=datax] [additional info=Additional Info]  
alertconditionexist=0|1
```

DM スクリプトがアラート条件を決定していない場合は値 **0** を使用します。DM スクリプトがアラート条件を決定している場合は値 **1** を使用します。

raisealertnow=0|1

(オプション) デフォルト値は **0** です。アラートをすぐに生成する場合は値 **1** を使用します。

PARAM1=data1,PARAM2=data2 .. PARAMX=datax -

(オプション) これらのキー値のペアは、アラートメッセージ内のパラメータと値を示します。一連のキー値ペアはカンマ (,) によって区切り、キーと値は等号 (=) によって区切ります。

additionalinfo=<Additional Info>

(オプション) このパラメータは、コマンドラインの最後のパラメータです。等号 (=) より後ろの残りのコマンドラインはすべてまとめられ、生成されるアラート XML の 1 つのフィールドを形成します。

DM スクリプトを使用したレメディエーション スクリプトの作成

DM スクリプトに基づくカスタム レメディエーション スクリプトを作成できます。このレメディエーション スクリプトを使用するアラートを設定する前のエージェント マシンで、スクリプト ディレクトリ（[設定ポリシー] - [DSM] - [ヘルス監視] - [ヘルス監視エージェント] - [ScriptDir] で設定される）にスクリプトを展開します。

以下の手順に従います。

1. [コントロール パネル] - [設定] - [設定ポリシー] - [DSM] - [ヘルス監視] - [アラート設定] - [アラート] に移動します。
2. レメディエーション アクションを設定するあらゆるアラートを選択します。
3. アラートのレメディエーション セクションの下では、エージェント マシンに展開する DM スクリプト名を指定します。
4. [パラメータ] フィールドにパラメータを指定します。
5. メッセージフィールドに、アラートに関連するテキストを追加します（必要に応じて、パラメータを持つアラートに関して）。
6. その他のアラート パラメータを設定し、監視用のエージェントに適用します。

DM スクリプトレメディエーションの例:

以下の DM スクリプトは、hmAlertOPFormatter を呼び出すことにより、修復が成功したかどうかを HM エージェントにレポートします。例：

```
dim remediationStatus as string
dim validate as string
dim remediationInfo as string
dim ret as integer
dim commandline as string

'Do your remediation here.

'...

'Set the value of remediationStatus to either 0 or 1. 0 は成功したレメディエーションを、1 は失敗したレメディエーションを表します

'Set the value of remediationInfo to any string that you want to displayed in WAC for this remediation. IDS_REM_SUCCESS および IDS_REM_FAILURE はそれぞれ成功および失敗を表すために使用できる標準的な文字列 ID です。

'Set valudate to 1 if alert validation is required post remediation or 0 otherwise

' At bottom of your DM script, execute hmAlertOPFormatter

' to notify HM Agent about the status of remediation.
```

```
If left(osstring, 3) = "Win" Then
    commandline = "hmAlertOPFormatter.exe"
Else
    commandline = "hmAlertOPFormatter"
Endif

commandline = commandline + " statuscode=" + remediationStatus + " validate=" +
validate + " statusmsg=" + remediationInfo

ret = Exec(commandline, TRUE, 0)
```

レメディエーションのステータスに関してヘルス監視エージェントに通知するには、DM スクリプト内で以下のコマンドを実行します。

hmAlertOPFormatter 実行可能ファイル

```
hmAlertOPFormatter.exe statuscode=0|1 validate=0|1 statusmsg="<Any string>"
statuscode=0|1
```

レメディエーションが成功した場合は、値 **0** を使用します。レメディエーションが失敗した場合は、値 **1** を使用します。

Validate=0|1

レメディエーションにより実際にその問題が修正されたかどうかを確認するために検証を実行する必要がある場合、値 **0** を使用します。レメディエーションの後でもアラート条件が残っている場合に検証およびレメディエーション失敗メッセージのレポートを実行するようにヘルス監視エージェントに通知するには、**1** を使用します。

statusmsg

(オプション) レメディエーションのステータスを表す文字列メッセージ。

アラートテンプレートの設定

アラートテンプレートを設定できます。

次の手順に従ってください：

1. [コントロールパネル] - [設定] - [設定ポリシー] - [DSM] - [ヘルス監視] - [アラート設定] - [アラートテンプレート] に移動します。
2. [追加] を選択して、スクリプトベースのアラートテンプレートを作成します。
3. 以下のフィールドに適切な値を指定します。

アラート名

テンプレート名を指定します。

テンプレート

アラートを生成するアラートテンプレートの名前を設定します。

参照：

[アセットジョブが更新されませんでした \(P. 394\)](#)

[アセットインベントリはSSからの収集中に更新されませんでした \(P. 395\)](#)

スクリプト

スクリプト名を指定します。この名前が *ScriptDir* 内の HM エージェントに渡されたスクリプトファイル名と同じである必要があります。

パラメータ

テンプレートに適したパラメータを指定します。

注：複数のパラメータを指定するには、セミコロン (;) で区切られた名前と値のペアを使用し、1つのパラメータの複数の値を区切るにはカンマ (,) を使用します。例：

```
GROUPS=Group1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=TRUE;assetJobNames=%
```

メッセージ

アラート条件が検出された場合に評価されるアラート関連情報を定義します。例：

コンピュータグループ *\$GROUPS* 内の *\$PERCENTAGE* 未満のコンピュータがアセットジョブ結果をレポートしました

重大度

テンプレートアラートの重大度をドロップダウン リストから設定します。

検出層

アラートが検出される層を指定します。EM、DM、SS、エージェントなどを指定します。

既定の繰り返し回数

テンプレートのデフォルトの頻度を指定します。

デフォルトしきい値

テンプレートのデフォルトのしきい値を指定します。

4. (オプション) 値を確認するには [確認] をクリックします。
5. [適用] をクリックし、[OK] をクリックします。

これでアラート テンプレートの設定が完了しました。

事前定義済みアラートのテンプレート

Client Automation はすぐに使用できる以下のアラート テンプレートを提供します。

[アセット ジョブが更新されませんでした \(P. 394\)](#)

[アセット インベントリは SS からの収集中に更新されませんでした \(P. 395\)](#)

アセット ジョブが更新されませんでした

1 つ以上のコンピュータ グループのアセット ジョブの指定された割合が更新されていない場合、このテンプレートが検出してアラートを生成します。

パラメータ

このテンプレートは以下のパラメータをサポートします。

groups=<該当するグループのカンマ区切りのリスト>;

カンマによって区切られた 1 つ以上のコンピュータ グループ名を指定します。

requiredPercentage=<必要なパーセンテージ>;

アラートの生成を回避するために正常である必要がある、指定されたグループ内にある識別されたジョブの必要なパーセンテージを指定します。

IncludeLinkedGroupJobs=[TRUE] |[FALSE];

TRUE

検証に含める必要があるジョブの識別時にグループにリンクされるジョブを含めるには、値 **TRUE** を指定します。

FALSE

含める必要があるジョブの識別時にグループにリンクされるジョブを無視するには、値 **FALSE** を指定します。

IncludeLinkedAssetJobs=[TRUE] |[FALSE];

TRUE

検証に含める必要があるジョブの識別時にアセットにリンクされるジョブを含めるには、値 **TRUE** を指定します。

FALSE

含める必要があるジョブの識別時にアセットにリンクされるジョブを無視するには、値 **FALSE** を指定します。

注: パラメータ リストで *IncludeLinkedGroupJobs* または *IncludeLinkedAssetJobs* を指定しない場合、デフォルト動作にはそれぞれのジョブ リンク タイプが含まれます。

assetJobNames=<ジョブ名のカンマ区切りのリスト>

評価に必要なジョブ名を指定します。指定しない場合、指定されたグループのアセット ジョブはすべて評価の対象になります。

注: `assetJobNames` パラメータでカンマ区切り値を使用して複数のジョブ名を指定できます。以下のワイルドカード文字を使用します。

% (パーセント)

ゼロまたはより多くの文字の文字列を指定します。たとえば、`title LIKE %computer%` は、*computer* という語が使用されるすべての書名を検出します。

_ (アンダースコア)

単一の文字を指定します。たとえば、`_ean` は、*ean* で終わる全部で 4 文字の名前をすべて検出します。

[アセット ジョブが更新されませんでした]のパラメータの例:

```
GROUPS=Groups1,Group2;RequiredPercentage=80;IncludeLinkedAssetJobs=TRUE;IncludeLinkedGroupJobs=FALSE;assetJobNames=%
```

[アセット インベントリは SS からの収集中に更新されませんでした]

このテンプレートは、インベントリ更新が指定された時間で 1 台以上のスケーラビリティ サーバまたはスケーラビリティ サーバグループで成功しない場合、検出されてアラートが生成されます。

パラメータ

このテンプレートは以下のパラメータをサポートします。

Servers=<スケーラビリティ サーバのカンマ区切りのリスト>;

カンマによって区切られた 1 つ以上のサーバを指定します。

注: サーバパラメータは、FQDN ではなく DSM エクスプローラでリスト表示されるようなサーバ名が必要です。

ServerGroups=<スケーラビリティ サーバグループのカンマ区切りのリスト>;

カンマによって区切られた 1 つ以上のサーバグループを指定します。

注: サーバグループパラメータは、[すべてのコンピュータおよびユーザ] セクションからではなく、すべてのスケーラビリティ サーバ、DSM エクスプローラからのグループの名前を必要とします。

注: パラメータを指定しない場合、すべてのスケーラビリティ サーバが評価の対象になります。

[アセット インベントリは SS からの収集中に更新されませんでした]のパラメータの例:

```
Servers=Server1,Server2;ServerGroups=Group1,Group2
```

Alert Collector の設定

Alert Collector を以下のいずれかのロールに設定します。

MDB への永続アラート

MDB へのアラートを継続するように Alert Collector を設定します。

MDB への永続アラートおよび設定されたアクションの実行

MDB へのアラートを継続し、設定されたアクション（メールの送信、SNMP トラップの生成、Windows/CCS イベント ログへの書き込みなど）を実行するように Alert Collector を設定します。

Persist Alerts, Take Configured Actions, and Forward

アラートを MDB に継続して送信するように Alert Collector を設定し、設定済みアクションを実行し、アラートを別の Alert Collector へ転送します。

注：重大度または検出層に基づいて、転送されるアラートをフィルタリングできます。たとえば、DM で生成された重大度が「高」および「中」のアラートのみを転送します。

転送

別の Alert Collector にアラートを転送するように Alert Collector を設定します。

注：Alert Collector はクラスタ環境ではサポートされません。

Alert Collector のロールの詳細については、「[Alert Collector のインストール](#) (P. 181)」を参照してください。

Alert Collector のプロパティの設定

Alert Collector の設定には、Web モジュールと Alert Collector プロセスの両方の設定が含まれます。

Web モジュールの設定

次の手順に従ってください:

1. [コントロールパネル] - [設定] - [設定ポリシー] - [DSM] - [Web サービス] - [ヘルス監視] に移動します。
2. 以下のオプションに適切な値を指定します。

アラートアップロードフォルダ

アラート情報 XML ファイルがアップロードされる Alert Collector マシン上のフォルダを指定します。

デフォルト: *HMAAlertUploads* このフォルダは、Client Automation インストールフォルダを基準とします。

デフォルト以外の値を使用する場合は、Web モジュールを実行するユーザアカウントがそのフォルダの書き込み権限を持つ必要があります。

注: フォルダ位置のネットワークパスはサポートされません。

Alert Collector へファイルをコピー

アップロードされたファイルを Alert Collector の入力フォルダにコピーするには、値 **1** を指定します。

デフォルト: **1**

Alert Collector へのコピー後にファイルを削除

Alert Collector の入力フォルダへのコピー後にアラート情報 XML ファイルを削除するには、値 **1** を指定します。

デフォルト: **0**

これで Web モジュール の設定が完了しました。

Alert Collector プロセスの設定

次の手順に従ってください:

1. [コントロール パネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [ヘルス監視] - [Alert Collector] に移動します。
2. 以下のオプションに適切な値を指定します。

Alert Collector ロール(ローカル管理)

Alert Collector を実行する必要があるロールを指定します。この値は、インストール中に初期設定されます。インストール後に、以下のいずれかの方法で別のロールに変更します。

- ロール パラメータを集中管理に変更し、ロールの値を設定して、Alert Collector マシンに適用します。
- Alert Collector マシンでローカルに `ccnfcmda` CLI を使用して、この値を設定し、Alert Collector プロセスを再起動します。

アラート情報フォルダ

アラート情報 XML ファイルがアップロードされる Alert Collector マシン上のフォルダを指定します。

デフォルト: `AlertCollectorInput` このフォルダは、Client Automation インストール フォルダを基準とします。

デフォルト以外の値を使用する場合は、**Web** モジュールを実行するユーザ アカウントがそのフォルダの書き込み権限を持つ必要があります。

注: フォルダ位置のネットワーク パスはサポートされません。

マネージャ(ローカル管理)

Alert Collector が接続する必要があるマネージャを設定します。この値は、インストール中に初期設定されます。インストール後にマネージャを変更するには、「Alert Collector ロール (ローカル管理)」の手順に従います。

出力フォルダ

Alert Collector で処理された後にアラート情報 XML ファイルが配置されるフォルダを設定します。

デフォルト: AlertCollectorOutput このフォルダは、Client Automation インストールフォルダを基準とします。

アラート最大パージ時間

アラートをパージするまでの経過期間を、日数で指定します。

デフォルト: 60 日

アラートパージ間隔

アラート最大パージ時間値より古いアラートが削除される間隔を指定します。

デフォルト: 10 日

これで Alert Collector プロセスの設定が完了しました。

アラートアクションの設定

アラートアクションを設定し、以下のアクションを実行するように設定する Alert Collector に適用します。

次の手順に従ってください:

1. [コントロールパネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [ヘルス監視] - [Alert Collector] - [アラートアクション] - [アクション設定] に移動します。

アラートアクションダイアログボックスが表示されます。

2. [追加] を選択し、設定済みのいずれかのアラート用のアクションを作成します。

3. 以下の項目に適切な値を指定します。

アラート名

アラート名を定義します。

注: リストからアラートを選択できます。

可能なアクション

必要に応じて、以下のアクションを指定します。

電子メールの送信

[宛先アドレス] で指定されている電子メール アドレスにアラート情報を送信します。アドレスが指定されていない場合、メールは、SMTP 電子メール設定でグローバルに指定されている受信者アドレスに送信されます。

SNMPトラップの発行

SNMP サーバで指定されている IP アドレスに対して SNMP トラップを生成します。サーバが指定されていない場合、トラップは、[アラート アクション] でグローバルに指定されている SNMP サーバに対して生成されます。

Windows イベント ログへの書き込み

アラート情報を Windows のイベント ログに書き込みます。

CCS イベント ログへの書き込み

アラート情報を CCS のイベント ログに書き込みます。

宛先アドレス

アラート情報を送信する電子メール アドレスを設定します。複数のアドレスをセミコロンで区切って指定できます。

SNMP Server

SNMP トラップが生成される SNMP サーバを設定します。

4. [適用] をクリックし、[OK] をクリックします。

これでアラート アクションの設定が完了しました。

注: [アラート アクション] から、SMTP 電子メールおよび SNMP サーバのグローバル設定を指定できます。

SMTP 電子メール設定

SMTP 電子メールに関する以下の詳細設定を指定します。

送信者アドレス

メール ヘッダで送信するメール アドレスを定義します。例：

デフォルト： *HealthMonitoringSystem*

注: 送信者アドレスにはスペースを使用しないでください。

メール サーバ

SMTP メール サーバの DNS 名または IP アドレスを指定します。

宛先アドレス

受信者のメール アドレスを定義します。複数のアドレスをセミコロンで区切って指定できます。

件名

メールの件名を指定します。

デフォルト： *Health Monitoring Alert*

SNMP サーバに関する以下の詳細設定を指定します。

SNMP Server

SNMP トラップが生成される SNMP サーバを設定します。

アラート転送の詳細の指定

転送ロールで設定される Alert Collector に関するこれらの設定を適用します。

次の手順に従ってください：

1. [コントロール パネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [ヘルス監視] - [Alert Collector] - [アラート転送] に移動します。
2. 以下の項目に適切な値を指定します。

Alert Collector アドレス

アラートが転送される Alert Collector サーバのホスト名または IP アドレスを定義します。

アラート転送: アラート検出層

アラート転送時にフィルタとして使用される層を指定します。

デフォルト：DM

アラート転送: アラート重大度

アラート転送時にフィルタとして使用されるアラート重大度を指定します。

アラート転送: 保留中フォルダの転送

初回の転送に失敗したアラート情報 XML ファイルが配置されるフォルダを指定します。

アラート転送: 拒否フォルダの転送

転送されなくなったアラート情報 XML ファイルが配置されるフォルダを指定します。

再試行の間隔

保留中のアラートを再転送する間隔を分単位で指定します。

https の使用

サーバへの接続に https または通常の http を使用することを指定します。[True] に設定すると、https が使用されます。Https を介して接続する Alert Collector を設定するには、「[アラートアップロードの設定 \(P. 407\)](#)」を参照してください。

これでアラート転送の詳細の設定が完了しました。

転送コレクタの設定

アラートが転送される Alert Collector サーバへの接続および認証に使用される認証情報の詳細を設定します。

詳細については、「[Alert Collector サーバの設定 \(P. 408\)](#)」を参照してください。

プロキシ サーバの設定

アラート転送のために Alert Collector サーバへの接続に使用されるプロキシサーバの詳細を設定します。

詳細については、「[プロキシ設定を設定する \(P. 409\)](#)」を参照してください。

ヘルス監視エージェントの設定

ヘルス監視エージェントのプロパティを変更します。

次の手順に従ってください:

1. [コントロールパネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [ヘルス監視] - [ヘルス監視エージェント] に移動します。
2. [プロパティの設定] ダイアログ ボックスで、以下の項目に適切な値を指定します。

ヘルス監視の有効化

ヘルス監視の状態を指定します。デフォルト: いいえ (False)

True

ヘルス監視が有効になります。

False

ヘルス監視が無効になります。

スクリプト ディレクトリ

カスタム アラート スクリプトをコピーする必要があるフォルダを指定します。デフォルト: `scriptdir`

注: 絶対パスが指定されていない場合、このフォルダは DSM インストールディレクトリ下の HM フォルダからの相対パスと見なされます。ネットワーク パスはサポートされません。

スクリプト出力ディレクトリ

カスタム アラート スクリプトの出力がコピーされるフォルダの名前を定義します。デフォルト: `scriptoutputdir`

注: 絶対パスが指定されていない場合、このフォルダは DSM インストールディレクトリ下の HM フォルダからの相対パスと見なされます。ネットワーク パスはサポートされません。

スクリプト タイムアウト

スクリプト実行の完了をヘルス監視エージェントが待機する時間を秒単位で定義します。デフォルト: 120 秒

注: タイムアウト エラーによってスクリプトの実行が失敗する場合は、時間 (秒単位) を増やして再試行してください。

最大アップロード再試行数

アラート情報のアップロードが再試行される回数を定義します。デフォルト: 3

アップロード再試行間隔

アラート情報のアップロードが再試行される間隔を秒単位で定義します。デフォルト：5 秒。

アラートレメディエーションの有効化

アラートレメディエーションの状態を指定します。デフォルト：いいえ (False)

True

アラートレメディエーションを有効にします。

False

アラートレメディエーションを無効にします。

ユーザ名

共有パッケージライブラリへのアクセス権限のあるユーザを指定します。

パッケージライブラリ共有

共有パッケージライブラリの場所を指定します。ライブラリは共有の場所にある必要があります。

注：絶対パスが指定されていない場合、このフォルダは DSM インストールディレクトリ下の HM フォルダからの相対パスと見なされます。

レメディエーション スクリプト タイムアウト

レメディエーション スクリプトの実行の完了をヘルス監視エージェントが待機する時間を秒単位で定義します。デフォルト：120 秒

注：タイムアウトエラーによってスクリプトの実行が失敗する場合は、時間（秒単位）を増やして再試行してください。

パスワード

共有パッケージライブラリにアクセスするためのパスワードを指定します。

3. [OK] をクリックします。

これでヘルス監視エージェントが有効になりました。

また、HM イベント ログ記録用の追加パラメータを設定する必要があります。

次の手順に従ってください:

1. [設定ポリシー] - [デフォルトのコンピュータ ポリシー] - [DSM] - [共通コンポーネント] - [イベント ログ] - [ヘルス監視] イベントに移動します。
2. 以下のパラメータを設定します。

イベント ログの保存先フォルダ

DSM インストール フォルダを基準とした、イベント ログ ファイル用のフォルダの場所を定義します。 フォルダはエージェントに存在する必要があります。

デフォルト : HM

イベント ログ ファイル名

ヘルス監視イベントをログ記録するために使用するファイル名を定義します。

デフォルト : hmevents_list.xml

アラートアップロードの設定

Alert Collector サーバの詳細を設定し、エージェントに適用して、ヘルス監視エージェントが検出されたアラートをアップロードできるようにします。

次の手順に従ってください:

1. [コントロールパネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [Web サービス] - [クライアント] - [ヘルス監視] に移動します。
2. 以下のオプションに適切な値を指定します。

Alert Collector アドレス

アラートがアップロードされる Alert Collector サーバのホスト名または IP アドレスを指定します。

注: EM 上の HM エージェントについては、DM にインストールされている Alert Collector を設定します。

https の使用

http または https による Alert Collector サーバへの接続を指定します。

デフォルト: False (http を示す)。

Alert Collector が https 用に設定されている場合、エージェントマシンで以下の手順を実行します。

- Web サーバ (Alert Collector) マシンから CA Root Certificate を DER 形式でエクスポートします。
- エージェントに証明書をコピーし、以下のコマンドを使用してインポートします。

```
cacertutil import -i:<cert-file-path> -it:X509V3 -trust
```

HM エージェントがプロキシを介して Alert Collector に接続する必要があるため、Alert Collector サーバがクライアント リクエストを認証するように設定される場合は、以下のオプションを設定します。

Alert Collector サーバの設定

以下の方法で Alert Collector サーバの設定の詳細を指定します。

次の手順に従ってください:

1. [コントロールパネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [Web サービス] - [クライアント] - [ヘルス監視] - [Alert Collector サーバ設定] に移動します。
2. 以下の項目に適切な値を指定します。

認証方法

認証方法を決定する値を定義します。

HTTP 認証タイプ

http 認証のタイプを決定する値を定義します。

注: http では、基本、ダイジェスト、および NTLM 認証を使用できます。

ドメイン

サーバのドメイン名を指定します。

パスワード

プロキシによる認証のためのパスワードを定義します。

ユーザ名

サーバによる認証のためのユーザ名を定義します。

これで Alert Collector サーバの設定が完了しました。

プロキシ設定を設定する

以下の方法でプロキシ設定を指定します。

次の手順に従ってください：

1. [コントロールパネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [Web サービス] - [クライアント] - [ヘルス監視] - [プロキシサーバの設定] に移動します。
2. 以下の項目に適切な値を指定します。

プロキシ パスワード

プロキシによる認証のためのパスワードを定義します。

プロキシ ユーザ

サーバによる認証のためのユーザを定義します。

プロキシ サーバアドレス

プロキシサーバのアドレスを定義します。

プロキシ サーバポート

プロキシが接続リクエストを確認するポートを定義します。

プロキシ タイプ

プロキシのタイプを決定する値を定義します。値が [なし] の場合は、直接 http 接続を示します。

これで、プロキシの設定が完了しました。

注： HM エージェントは HTTP プロキシのみをサポートします。SOCKS プロキシサポートはこのリリースでは使用できません。

WAC からのアラート ステータスの管理およびトラッキング

アラート表示

新しいアラートが生成される場合、DSM エクスプローラ内のドメイン ノードのシステム ステータス ポートレットで通知を確認できます。この通知には WAC を起動するためのハイパーリンクがあり、統合ログインが有効になっている場合は、アラート ページにアクセスできます。ハイパーリンクとは別に、新しく生成されたアラートの数を確認します。その数は [新規] および [レメディエーションに失敗しました] の状態のアラートの合計です。

WAC 用の統合ログインを設定する方法：

次の手順に従ってください：

1. 'DSM¥Web Console¥webapps¥wac¥WEB-INF¥classes¥com¥ca¥wac¥config¥' の WAC Config.properties ファイルに移動します。
2. attemptUnifiedLogin の値を **true** に設定します。
3. Tomcat を再起動します。

```
Caf stop tomcat
```

```
Caf start tomcat
```

WAC 用の統合ログインが設定されました。

アラート表示用の WAC のリンクを設定できます。

次の手順に従ってください：

1. [コントロール パネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [ヘルス監視] - [アラート表示] - [WAC] に移動します。
2. WAC アラート ページへのリンクを設定します。

デフォルト： http://localhost/wac?context_launch_class=DSMHMAAlert

注：「localhost」は wac マシンのホスト名に置き換えてください。

WAC からのアラート ステータスの管理およびトラッキング

注を追加し、アラートの状態を「新規」、「フォローアップ」、または「クリア済み」に更新することによって、WAC からアラートを管理します。

次の手順に従ってください:

1. [アラート] に移動します。

アラート ページが表示されます。

2. 1 つまたは複数の アラートを選択し、[更新] または [削除] を選択します。

ダイアログ ボックスが表示されます。

- 更新するには、ドロップダウン オプションからのアラート ステータスを変更します。

新規

アラートを新規として指定します。

フォローアップ

アラートをフォローアップ用として指定します。

クリア済み

アラートの状態をクリア済みとして指定します。

- 削除するには、アラートを選択し、削除を確認します。

注: すべてのオプションの削除を選択して、すべてのアラートを削除できます。

3. アラートのステータスをトラッキングするために役立つ情報によって注を更新します。
4. [レメディエーション ステータス]、[レメディエーション スクリプト]、[レメディエーション スクリプト パラメータ]などのアラート レメディエーションの詳細を表示します。

これで、アラートの更新または削除が完了しました。

注: アラートはドメイン マネージャ レベルからのみトラッキング、更新、および削除することができます。エンタープライズ マネージャ上の HM アラートはすべて読み取り専用です。

アラート複製

「アラート複製」は、アラートの複製に役立ちます。

- **DM** のアラートに対する更新がエンジンによって **EM** に複製される場合、新しいアラートは複製の一部として作成されません。そのアラートは適切なフィルタを持った **DM** で、アラートの転送によってのみ、**EM** で作成されます。
- エンジンがアラートを **EM** に複製する前に、エンジンはアラートが存在するかどうかを確認します。アラートが見つからない場合、エンジンはアラート以上を複製しません。アラートが **DM** で削除される場合、**EM** の対応するアラートが削除されます。
- **DM** が **EM** からリンク解除される場合、以下の管理済み設定ポリシー パラメータにより、その **DM** の `domain_uuid` についてのすべてのアラートが **EM** にそのまま残るか、削除されるかどうかを制御します。そのように削除された場合、エンジンは、**DM** から **EM** に再度アラートを複製しません。**DM** が **EM** に再リンクされる場合、この動作が制限となります。

EM からドメインのリンクを解除する場合に特定のドメインのアラートの削除を制御するパラメータを編集するには、[コントロール パネル] - [設定] - [設定ポリシー] - [デフォルトのコンピュータ ポリシー] - [DSM] - [マネージャ] - [エンジン] - [リンク解除時にレプリケートされたアラームを削除] に移動します。また、**DM** のリンクを解除するときに値を **True** に設定すると、**DM** から複製されたアラートは、**EM** で削除されます。

第 10 章：外部ディレクトリを設定および認証する方法

デスクトップ サポート アナリストは、認証用として外部ディレクトリを使用できます。**DSM** エクスプローラで外部ディレクトリを使用すると、以下のタスクを実行できます。

- ユーザを認証する（ネイティブ モードの **Active Directory** ユーザを含む）。
- ディレクトリのエンティティにセキュリティ プロファイルをマッピングすることにより、ユーザを認証する。
- ディレクトリ内のコンテナに保持されているコンピュータまたはユーザと一致するターゲットで、クエリ グループを定義する。
- エージェントの展開をターゲットにする。

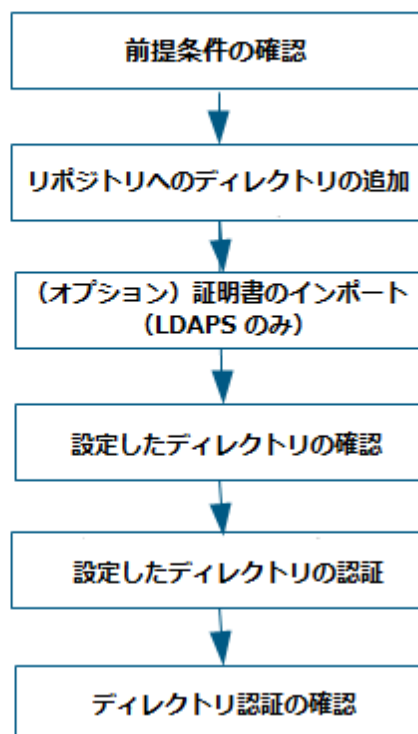
- ディレクトリから取得した階層を使用してレポートを生成する。

外部ディレクトリを使用して認証を行うには、以下の手順に従います。



デスクトップ サポート
アナリスト

外部ディレクトリを設定および 認証する方法



以下の手順に従います。

1. [リポジトリへのディレクトリの追加](#) (P. 415)
2. [\(オプション\) 証明書のインポート \(LDAPS のみ\)](#) (P. 420)
3. [設定したディレクトリの確認](#) (P. 421)
4. [設定したディレクトリの認証](#) (P. 425)
5. [ディレクトリ認証の確認](#) (P. 428)

サポートされている外部ディレクトリ

Client Automation は、以下のディレクトリをサポートしています。

- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory

サポートされているディレクトリ統合サービスの更新リストについては、[互換性マトリックス](#)を参照してください。

前提条件の確認

外部ディレクトリを使用して認証を行うには、以下の前提条件を確認します。

- 外部ディレクトリを設定するためのアクセス権があるかどうかを確認します。
- ディレクトリ統合機能に関する実務知識があることを確認します。

リポジトリへのディレクトリの追加

ユーザを認証して権限を付与するには、ディレクトリ内のエンティティにセキュリティプロファイルをマッピングし、外部ディレクトリをリポジトリに追加します。

次の手順に従ってください：

1. [コントロールパネル]、[ディレクトリ統合]、および[ディレクトリの追加]をクリックしてディレクトリの追加ウィザードにアクセスし、[次へ]をクリックします。

[はじめに/ディレクトリ名] ページが表示されます。

2. [ディレクトリ名] に、**Active Directory** に接続するときにディレクトリの識別に使用するディレクトリ名を指定します。
3. 以下の[ディレクトリ タイプ] オプションの **1** つを使用してディレクトリのタイプを選択します。以下のオプションを使用できます。

- Active Directory
- LDAP

デフォルト：Active Directory

4. [次へ] をクリックして [サーバの詳細] ページに進みます。

ディレクトリ サーバの詳細の指定

[サーバの詳細] ウィザード ページを使用して、追加するディレクトリと接続先のポート番号を保持するディレクトリ サーバの名前を指定します。

注: SSL (Secure Sockets Layer) を使用する外部ディレクトリでは、**Lightweight Directory Access Protocol (LDAP)** サーバが使用する証明書が有効であり、**Microsoft Windows** の認証局チェーンで認証可能である必要があります。以前のバージョンの **Windows** では、**LDAP** 開発者が証明書を検証するようになっていましたが、**Windows 2003** の **SSL** ではこの機能がさらに強化されました。

次の手順に従ってください:

1. [サーバ名] フィールドにディレクトリをサポートするサーバ名を入力します。
2. [ポート] フィールドにディレクトリ サービスのポート番号を入力します。

ディレクトリ クライアントは、常にここで指定したポートを使用し、ディレクトリに対して暗号化されたセキュアな接続を作成しようとします。一部のディレクトリでは、セキュアな通信やセキュリティ上の脆弱性がある通信に対してポート **389** がサポートされています。ポート **636** をセキュアのためのチャンネルとしてサポートするディレクトリもあります。どのポートを使用するかは、ディレクトリ管理者の指示を受けてください。

指定したポートに対してセキュアなチャンネルが使用可能な場合は、そのチャンネルを使用します。セキュアなチャンネルが使用可能ではなく、指定されたポートでセキュリティ上の脆弱性がある通信が許可されている場合は、その通信を使用します (セキュリティ上の脆弱性のある通信が許可されていない場合は、ディレクトリのインポートは拒否され、[完了] をクリックすると対応するエラー メッセージが表示されます)。

注: ディレクトリの共通設定ポリシー (特に、**LDAP 簡易認証を有効化**ポリシー) は、セキュリティ上の脆弱性のある通信チャンネルで認証が実行できるかどうかに影響を与えることがあります。

3. [次へ] をクリックして [ディレクトリのバインド] ページに進みます。

注: **LDAP** ディレクトリを追加した後、指定したアクセス ポートが変更される場合、元のセキュリティ権限が正しく削除されていないため、セキュリティ権限リストに無効なセキュリティ権限が含まれていることがあります。このことは、**Client Automation** に機能的な影響を与えませんが、元のセキュリティ権限がセキュリティ ダイアログ ボックスで有効として表示されます。関係のないセキュリティ権限の削除には、テクニカル サポートのツールが必要です。サポート担当者に連絡して、**cfspsetpass** ユーティリティを入手してください。

ディレクトリ バインド情報の指定

[ディレクトリのバインド] ウィザード ページを使用して、ディレクトリにアクセスするときに匿名で行うか、またはユーザのクレデンシャルを使用するかどうかを指定します。

次の手順に従ってください:

1. (オプション) [匿名バインドの使用] オプションを選択します。デフォルトでは、このオプションは選択されません (いいえ)。

注: 選択されている場合、ディレクトリへのアクセス権が制限されているか、またはアクセス権そのものがない場合があります。

2. 該当するフィールドにユーザ名とパスワードを入力します。

3. (オプション) [暗号化プロトコル (LDAPS) の使用] オプションを選択します。このオプションを選択した場合は、LDAP の代わりにセキュアな LDAPS プロトコルが使用されます。ただし、設定しているディレクトリで LDAPS がサポートされていることを確認してください。

注: このフィールドは、Active Directory または LDAP ディレクトリを設定している場合にのみ表示されます。

4. [次へ] をクリックして [ベース ディレクトリ ノード] ページに進みます。

ベース ディレクトリ ノード詳細の指定

[ベース ディレクトリ ノード] ウィザード ページを使用して、ディレクトリの参照を開始するルート ノードを指定します。

次の手順に従ってください:

1. [ベース ディレクトリ ノード] フィールドに、現在のディレクトリの参照用にルート オブジェクトの識別名 (DN) を入力します。

注: 検索を効率的にするために、ディレクトリ階層内の可能な限り深いベース DN を使用してください。利用できる最良の価値については、ディレクトリ管理者の指示を受けてください。

2. [次へ] をクリックして [スキーマ マッピングの選択] ページに進みます。

スキーマ マッピング属性の選択

[スキーマ マッピングの選択] ウィザード ページを使用して、ディレクトリ用のスキーマ マッピングを指定します。定義済み共通スキーマ マップを選択するか、または独自のマップを定義できます。

次の手順に従ってください:

1. (オプション) 自分のスキーマ マッピングを使用する場合、[新しいマッピングの定義] オプションを選択します。

このオプションでは、外部ディレクトリの (ユーザ、コンピュータ、グループなど) データ オブジェクトに関連した属性名と、対応する DSM オブジェクトによって使用される属性名とのマッピングを定義します。

2. [スキーマ マップ] オプションの 1 つを使用して事前定義したスキーマ マップを選択します。有効なオプションは、[Active Directory] および [eTrust Directory] です。

デフォルト: Active Directory

3. [次へ] をクリックして [スキーマ マッピングの調整/定義] ページに進みます。

スキーマ マッピングの調整/定義の詳細

[スキーマ マッピングの調整/定義] ウィザード ページでは、新しいスキーマ マップを定義し、指定したスキーマを修正できます。ディレクトリのスキーマは、属性の名前およびタイプを定義します。スキーマ マッピングでは、ディレクトリのスキーマで定義したディレクトリ オブジェクトの属性 (プロパティ) が、他の DSM ベースのアプリケーションで使用される共通スキーマに変換されます。

注: 最も一般的なスキーマに対する事前定義済みスキーマ マップがいくつか存在します。これには、WinNT および UnixL プロバイダ用のハードコードされたマップが含まれます。

次の手順に従ってください:

1. スキーマを新規作成する場合は、[スキーマ名] フィールドにスキーマ マップの一意の名前を入力します。入力しない場合、このフィールドには、選択した既存のスキーマ名が表示されます。

適切なマッピング テーブルが表示され、指定したディレクトリのスキーマにおける属性の名前とタイプが表示されます。

2. (オプション) DSM 属性のデフォルトの値を変更するには、マッピング テーブルでその属性をクリックします。

[属性マッピング] ダイアログ ボックスが表示されます。

3. (オプション) 1 つまたは複数の DSM 属性の値を変更し、[OK] をクリックします。

[属性マッピング] ダイアログ ボックスが閉じ、ウィザード ページに戻ります。

4. [次へ] をクリックして [完了] ページに進みます。

スキーマの詳細については、「[スキーマ マッピング \(P. 430\)](#)」を参照してください。

設定オプションのレビューおよびディレクトリの追加

[完了] ウィザード ページでは、ディレクトリに対して選択した設定とオプションの概要が表示されます。指定したディレクトリのリポジトリへの追加処理を完了する場合は [完了] をクリックします。または設定やオプションのいずれかを変更する場合は、[戻る] をクリックします。

外部ディレクトリが設定されました。

(オプション) 証明書のインポート (LDAPS のみ)

定義した LDAP または OpenLDAP ディレクトリへのアクセスを保護するために LDAPS を使用する場合、Windows サーバでは LDAPS サーバからの証明書が信頼できる必要があります。証明書が信頼できる認証局からのものでない場合は、新しいディレクトリの設定処理を完了するために証明書ストアに手動で証明書をインポートする必要があります。

注: 以下の手順に含まれるウィザードおよびダイアログ ボックスの詳細については、x.509 証明書に関する Microsoft のマニュアルを参照してください。

次の手順に従ってください:

1. `..¥CA¥DSM¥bin¥itrm¥r11_root.der` の場所を探し、このファイルをダブルクリックします。
[証明書のインポート] ダイアログ ボックスが表示されます。
2. [証明書のインストール] をクリックします。
証明書のインポート ウィザードが表示されます。
3. [次へ] をクリックします。
[証明書ストア] ウィザード ページが表示されます。
4. [証明書をすべて次のストアに配置する] オプションを選択します。
5. [参照] をクリックします。
[証明書ストアの選択] ダイアログ ボックスが表示されます。
6. [物理ストアを表示する] オプションを選択します。
7. 以下のいずれかの操作を実行します。
 - 証明書が自己署名される場合、[信頼されたルート証明機関] を拡張し、[ローカル コンピュータ] を選択します。
 - 証明書が自己署名されない場合、[サードパーティ ルート証明機関] を拡張し、[ローカル コンピュータ] を選択します。

重要: この手順は必須です。証明書は物理ストアに追加される必要があります。追加されない場合は、現在のユーザのストアが使用され、証明書は **Client Automation** によって使用されるローカルのシステム アカウントに利用できません。
8. [OK] をクリックします。
ダイアログ ボックスが閉じ、ウィザードに戻ります。
9. [次へ] をクリックして [完了] をクリックします。
インポートが成功したことを示すメッセージが表示されます。

10. [OK] をクリックします。

指定した証明書が証明書ストアに追加されました。

注: `encUtilCmd certimport` コマンドを使用して、同様の操作を実行することもできます。

設定したディレクトリの確認

ディレクトリを追加および設定したら、設定したディレクトリが **DSM** エクスプローラに追加されているかどうかを確認できます。

次の手順に従ってください:

1. [コントロール パネル] - [ディレクトリ統合] - [設定されたディレクトリ] ノードに移動します。

現在のドメインに定義されたすべての設定された外部ディレクトリの名前および説明が表示されます。このペインの説明列には、**Active Directory** でディレクトリを設定した場合、そのディレクトリごとに **LDAP** の URL が表示されます。

外部ディレクトリが設定されました。

(オプション)ディレクトリの更新

ディレクトリのプロパティを更新することもできます。

1. (オプション) 設定されたディレクトリのプロパティを使用して、設定されたディレクトリを更新します。

ディレクトリの更新ダイアログ ボックスに、以下のタブが表示されます。

- [設定](#) (P. 422)
- セキュリティ
- スキーマ (424P.)

ディレクトリの更新: [設定]タブ

[設定] タブには、ディレクトリのメイン設定オプションがあります。

このタブには以下のフィールドが含まれます。

ディレクトリ名

ディレクトリまたはディレクトリ サーバ名を以下のように指定します。

- **Active Directory** に接続するときは、ディレクトリの識別に使用する名前を指定します。これは、ディレクトリ サーバに対してディレクトリ自体が解決できる名前となります。
- **LDAP** を使用してスタンドアロンのディレクトリ（**Active Directory** のように分散されているディレクトリではないもの）に接続するときは、ディレクトリ サーバの名前を指定します。この名前は、ディレクトリのアクセスおよび認証に使用されるサーバのフル **DNS** 名となります。

例：Active Directory のドメイン **HQDirectory.com** は、マシン **FAKE_MACHINE** でホストされています。Active Directory が **FAKE_MACHINE** に対して **HQDirectory.com** を正常に解決できるため、このディレクトリを統合に設定するときに、このフィールドに **HQDirectory.com** を指定できます。

ディレクトリタイプ

ディレクトリのタイプを指定します。有効なオプションは、**[Active Directory]** および **[LDAP]** です。デフォルトでは、ディレクトリを追加したときに指定したディレクトリのタイプが選択されます。

ディレクトリ サーバ

ディレクトリをサポートするサーバ名を指定します。

ポート

ディレクトリ サービスのポート番号を指定します。ディレクトリ クライアントは、常にここで指定したポートを使用し、ディレクトリに対して暗号化されたセキュアな接続を作成しようとします。一部のディレクトリでは、セキュアな通信やセキュリティ上の脆弱性がある通信に対してポート 389 がサポートされています。ポート 636 をセキュアのためのチャンネルとしてサポートするディレクトリもあります。どのポートを使用するかは、ディレクトリ管理者の指示を受けてください。

指定したポートに対してセキュアなチャンネルが使用可能な場合は、そのチャンネルを使用します。セキュアなチャンネルが使用可能ではなく、指定されたポートでセキュリティ上の脆弱性がある通信が許可されている場合は、その通信を使用します（セキュリティ上の脆弱性のある通信が許可されていない場合は、ディレクトリのインポートは拒否され、[完了] をクリックすると対応するエラー メッセージが表示されます）。

注：ディレクトリの共通設定ポリシー（特に、LDAP 簡易認証を有効化ポリシー）は、セキュリティ上の脆弱性のある通信チャンネルで認証が実行できるかどうかに影響を与えることがあります。詳細については、「DSM エクスプローラ ヘルプ」の「設定ポリシー」を参照してください。

デフォルト： 389（LDAP ディレクトリの場合）

ベース DN

現行ディレクトリを参照するためのルート オブジェクトの識別名（DN）を指定します。利用できる最良の価値については、ディレクトリ管理者にお問い合わせください。

注：数多くのディレクトリ検索がこのベース ノードで実行される可能性があるため、実行される検索の効率と精度について慎重に考慮してください。ベース DN をディレクトリ階層内のできる限り深い場所を使用してください。これにより、検索がより効率的になります。

情報

オプションを選択するためのヒント、またはフィールドまたはダイアログ ボックスに情報を入力するためのヒントを表示します。

ディレクトリの更新: [セキュリティ]タブ

[セキュリティ] タブでは、ディレクトリに接続するためのセキュリティ オプションが提供されます。

このタブには以下のフィールドが含まれます。

匿名バインド

匿名バインドを使用するかどうかを指定します。 デフォルトでは、ディレクトリを追加したときに指定した値が選択されます。

ユーザ

[匿名バインド]が選択されていない場合は、ユーザ名を指定します。

パスワード

[匿名バインド] が選択されていない場合は、指定されたユーザのパスワードを指定します。

情報

オプションを選択するためのヒント、またはフィールドまたはダイアログ ボックスに情報を入力するためのヒントを表示します。

ディレクトリの更新: [スキーマ]タブ

[スキーマ] タブでは、ディレクトリ属性を **Client Automation** スキーマにマッピングする設定オプションが提供されています。

このタブには以下のフィールドが含まれます。

スキーマ

使用するスキーマを示します。最も一般的なスキーマに対する事前定義済みスキーママップがいくつか存在します。これには、WinNT および UnixL プロバイダ用のハードコードされたマップが含まれます。ドロップダウン リストからいずれか1つを選択します。

情報

オプションを選択するためのヒント、またはフィールドまたはダイアログ ボックスに情報を入力するためのヒントを表示します。

設定したディレクトリを使用した認証

認証は、提供されたクレデンシャルに基づいて、Trusted Computing Base のメンバーを識別します。外部ディレクトリを DSM セキュリティ認証操作のセキュリティ権限として追加します。Client Automation は、外部ディレクトリに対するセキュリティオブジェクトを認証して、認証済み ID またはグループメンバシップを以降の認証呼び出しに使用します。

セキュリティプロファイルの追加

セキュリティプロファイルの作成は、新しいセキュリティプロファイルを現在のセキュリティプロバイダによって提供されるユーザアカウントまたはグループのいずれかにマップすることを意味します。システムにアクセスするユーザまたはグループを選択して、セキュリティプロファイルに追加することができます。

次の手順に従ってください:

1. [セキュリティ]メニューから[セキュリティプロファイル]を選択します。
[セキュリティプロファイル] ダイアログボックスが表示されます。

注: このダイアログボックスを開くには、十分なアクセス権が必要です。権限がない場合には、セキュリティエラーメッセージが表示されます。管理者には、デフォルトでこれらのアクセス権があります。

2. [追加] をクリックします。
[セキュリティプロファイルの追加] ダイアログボックスが表示されます。

3. セキュリティ権限を[使用可能なディレクトリ] ツリーから選択し、必要なセキュリティプリンシパルを参照してクリックします。

選択されたセキュリティ権限およびプリンシパルが、[コンテナ識別子] および[名前] の各フィールドに表示されます。

4. ツリー内のプリンシパルをダブルクリックするか、または[リストへの追加] をクリックします。

[名前] フィールドに表示されたセキュリティプリンシパルが、セキュリティプロファイルのリストに追加されます。

プロファイルをさらに追加するには、[セキュリティプロファイルの追加] ダイアログボックスで最後の 2 ステップを繰り返します。

5. [OK] をクリックします。

選択されたユーザ アカウントまたはグループがセキュリティ プロファイルにマップされ、[クラスのアクセス権] ダイアログ ボックスが表示されます。

注: 1 つ以上のセキュリティ プリンシパルを追加した場合、[クラスのアクセス権] ダイアログ ボックスは表示されません。[セキュリティ プロファイル] ダイアログ ボックスでプロファイルを選択し、[クラスのアクセス権] をクリックする必要があります。

6. [クラスのアクセス権] ダイアログ ボックスでは、権限を割り当てるオブジェクト クラスを選択します。

注: 複数のオブジェクト クラスを選択して、それらすべてにクラスのアクセス権を指定することもできます。連続して選択するには、**Shift** キーを押してからオブジェクトをクリックします。任意に選択するには、**Ctrl** キーを押してからオブジェクトをクリックします。

7. [クラス アクセス] ドロップダウン リストから権限を選択して、[OK] をクリックします。

指定された権限が新しいセキュリティ プロファイルに割り当てられます。

[セキュリティ プロファイルの追加] ダイアログ ボックスには、次の利用可能なセキュリティ権限のリストが表示されます (**Windows NT** ドメイン、**UNIX** 認証ターゲット、**NDS** などの外部ディレクトリ、および **X.509** 証明書サブシステム)。

マネージャは、使用可能なセキュリティ権限のリストを格納します。 **Windows NT** ドメイン環境で実行中の場合、マネージャ ノードでは、利用可能なすべての明示的なドメインへの信頼が自動的に検証されます。利用可能なセキュリティ権限のリストは、[セキュリティ プロファイルの追加] ダイアログ ボックスから参照できます。

セキュリティ プロファイルの作成時に、暗黙的に信頼されたドメイン、つまり、直接検証されたリストにないドメインを使用する場合があります。

[セキュリティ プロファイル] ダイアログ ボックスを使用して、権限の追加および削除を実行できます。ただし、これは **Windows NT** ネームスペース (**winnt**) 内でのみ可能です。

- 暗黙的に信頼されたドメインを追加するには、[追加] をクリックして新しく表示されたダイアログ ボックスにドメイン名を入力します。
- 暗黙的に信頼されたドメインを削除するには、削除するドメインを強調表示して [削除] をクリックします。

注: 信頼の付与は、**Windows** オペレーティング システムによって実行されます。ドメインを追加して、マネージャがこのドメインを信頼するようにするには、基本オペレーティング システムでこのドメインがすでに信頼されている必要があります。

定義済みのアクセス タイプ

以下の例に、**Computer** オブジェクト クラスに対する各種アクセス権の効果を示します。

クラス アクセス	権限の効果
表示	[すべてのコンピュータ] フォルダの下すべてのコンピュータを表示します。
読み取り	コンピュータのプロパティを表示することができます。
マネジメント	コンピュータ にソフトウェア パッケージを展開する、またはコンピュータでジョブを実行することができます。
変更	新しいコンピュータを追加するか、またはコンピュータを削除することができます。
フル コントロール	コンピュータを完全制御することができます。

ディレクトリ認証の確認

ディレクトリ統合が成功したことを確認するには、**Client Automation** にログインすることによってディレクトリ認証を確認します。

次の手順に従ってください: (DSM エクスプローラで)

1. ユーザ名とパスワードを指定します。

ログインするユーザ名を定義します。

デフォルト: DN 形式。

重要: 認証用として **UID** または **SN** 形式を使用する場合、設定ポリシーの値を設定します。詳細については、「[ポリシーの変更による別のユーザ名形式の使用](#) (P. 430)」を参照してください。

2. 以下のリストからセキュリティ権限を選択します。

セキュリティプロバイダ

セキュリティプロバイダを指定します。**Client Automation** では、アクセス権の付与に外部ディレクトリ、オペレーティングシステムのユーザアカウントおよびグループが使用されているため、オペレーティングシステムがセキュリティプロバイダとして機能します。適切なセキュリティプロバイダを選択すると、対応する **Windows** ドメインまたはディレクトリが表示されます。

Windows ドメイン (Windows)/ディレクトリ (Idap)

ユーザアカウントを持つドメインまたはコンピュータを選択します。**Client Automation** にアクセスできる設定されたディレクトリがドロップダウンリストに表示されます。

3. [ログイン] をクリックします。

ログインクレデンシャルが正しい場合は、システムにログインできます。

次の手順に従ってください: (Web コンソール アクセスの場合)

1. Web コンソール ドロップダウンから [マネージャ名] を選択します。
2. ユーザ名とパスワードを指定します。

ログインするユーザ名を定義します。DN 形式を使用できます。

重要: 認証用として UID または SN 形式を使用する場合、設定ポリシーの値を設定します。詳細については、「[ポリシーの変更による別のユーザ名形式の使用](#) (P. 430)」を参照してください。

3. 以下のリストからセキュリティ権限を選択します。

セキュリティプロバイダ

セキュリティプロバイダを指定します。Client Automation では、アクセス権の付与に外部ディレクトリ、オペレーティングシステムのユーザアカウントおよびグループが使用されているため、オペレーティングシステムがセキュリティプロバイダとして機能します。適切なセキュリティプロバイダを選択すると、対応する Windows ドメインまたはディレクトリが表示されます。

Windows ドメイン (Windows) / ディレクトリ (Idap)

ユーザアカウントを持つドメインまたはコンピュータを選択します。Client Automation にアクセスできる設定されたディレクトリがドロップダウンリストに表示されます。

4. [ログイン] をクリックします。

ログインクレデンシャルが正しい場合は、システムにログインできます。

注: 設定されたディレクトリへのアクセス権は、ドメイン マネージャの管理者が付与します。

ポリシーの変更による別のユーザ名形式の使用

設定ポリシーの設定は、認証用に **DN** 形式を使用しない場合にのみ行います。[プロパティの設定] ダイアログ ボックスを使用して、特定の要件および環境に合わせて設定ポリシーを変更します。

注: ポリシーを変更する前に、封印を解除する必要があります。

次の手順に従ってください:

1. [設定] - [設定ポリシー] - [デフォルトのコンピュータ ポリシー] - [共通コンポーネント] - [セキュリティ] - [プロバイダ] - [コンポーネント] - [ldap] に移動します。

2. ペインの [Oracle LDAP: ショートネーム タイプ] を右クリックし、コンテキスト メニューから [プロパティの設定] を選択します。 または、 [タスク] ポートレットの [プロパティの設定] をクリックします。

[プロパティの設定] ダイアログ ボックスが開きます。

3. [値] フィールドで、ニーズに合わせて以下のいずれかの値を選択します。

sn

Oracle ldap の短縮名を指定します。

uid

Oracle ldap の一意の ID を指定します。

4. [OK] をクリックします。

新しい値は、認証用に提供されたユーザ名が **sn** であるか、または **uid** であるかを指定します。

注: **sn** は Active Directory ベースの ldap に対して一意である必要があります。

スキーマ マッピング属性について

スキーマ マップとは、外部ディレクトリにおいて使用されるユーザ、コンピュータ、グループなどのデータ オブジェクトに関連した属性名と、対応する **DSM** オブジェクトによって使用される属性名とのマッピングのことです。固定された標準的な **DSM** 属性名は、ディレクトリのクエリ、および複雑なクエリとレポートの構成に使用します。

Client Automation には、3 つの定義済みの共通スキーマ マッピングが提供されます。事前定義されているスキーマ セットに基づき、自分のカスタム スキーマを作成するオプションもあります。

DSM 属性名

以下の表に、DSM ベースのアプリケーションがディレクトリのクエリに使用する標準的な属性名のセットおよび簡単な説明を示します。

属性名	説明
objectClass	オブジェクトのクラス
dc	ドメイン コントローラ
o	組織
ou	組織単位
c	国
l	場所
userDn	ユーザの識別名
userCn	ユーザの共通名
userSn	ユーザの姓
givenName	ユーザの名
displayName	表示名
userName	ユーザ名
userID	ユーザ識別子
userPassword	ユーザ パスワード
memberOf	ユーザがメンバになっているグループの名前/識別名
directReports	このユーザに報告する人の名前/識別名
streetAddress	住所
postalCode	郵便番号
company	会社
department	部門
email	電子メール アドレス
telephoneNumber	電話番号
jobTitle	職位
userDescription	ユーザの説明

属性名	説明
assetDn	コンピュータの識別名
assetCn	コンピュータの共通名
assetName	コンピュータの名前
dnsHostName	DNS ホスト名
operatingSystem	オペレーティング システム
operatingSystemServicePack	OS サービス パック
operatingSystemVersion	OS バージョン
assetDescription	コンピュータの説明
groupDn	グループの識別名
groupCn	グループの共通名
groupName	グループの名前
groupMembers	このグループのメンバになっているユーザの名前/識別名
groupDescription	グループの説明

また、DSM スキーマ マップには、属性名でないフィールドが含まれています。これらは、DSM ベースのアプリケーションが使用するオブジェクト クラスの名前です。

- GUI では、**computerMap**、**groupMap**、および **userMap** を使用して、表示するノードのタイプが判別されます。
- ディレクトリ同期ジョブでは、**userMap** および **computerMap** が使用されます。

DSM スキーマ マップには、以下のフィールドが含まれています。

computerMap

設定されたディレクトリでコンピュータを表す **objectClass** 名にマッピングします。

groupMap

設定されたディレクトリでグループを表す **objectClass** 名にマッピングします。

userMap

設定されたディレクトリでユーザを表す **objectClass** 名にマッピングします。

containerMap

「コンテナ」のクラス名にマッピングします。

Active Directory スキーマ

以下の表に、DSM のスキーマにマップする Active Directory 属性名を示します。

DSM 属性名	Active Directory の属性名
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName

DSM 属性名	Active Directory の属性名
userID	name
userPassword	userPassword
memberOf	memberOf
directReports	directReports
streetAddress	streetAddress
postalCode	postalCode
company	company
department	department
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	dnsHostName
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	members
groupDescription	description
containerMap	container
groupMap	group
userMap	user
computerMap	computer
uniqueUserFields 1 – uniqueUserFields 5	–

DSM 属性名	Active Directory の属性名
uniqueComputerFields 1 - uniqueComputerFields 5	—
userDn*	distinguishedName
groupDn*	distinguishedName
assetDn*	distinguishedName
o*	o
ou*	ou

* 注: これらの属性のマッピングは固定されており、変更できません。ただし、クエリでは、これらの DSM 属性名を使用できます。

Oracle ディレクトリ スキーマ

以下の表に、DSM スキーマにマップする Oracle ディレクトリ 属性名を示します。

DSM 属性名	Oracle 属性名
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	Sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	—
directReports	—
streetAddress	streetAddress
postalCode	postalCode
company	company

DSM 属性名	Oracle 属性名
department	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	host
operatingSystem	operatingSystem
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	members
groupDescription	description
containerMap	container
groupMap	groupOfUniqueNames
userMap	inetOrgPerson
computerMap	computer
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–

* 注: これらの属性のマッピングは固定されており、変更できません。ただし、クエリでは、これらの DSM 属性名を使用できます。

eTrust Directory スキーマ

以下の表に、DSM のスキーマにマップする eTrust Directory 属性名を示します。

DSM 属性名	eTrust Directory の属性名
objectClass	objectClass
dc	dc
c	c
l	l
userCn	cn
userSn	sn
givenName	givenName
userName	name
displayName	displayName
userID	name
userPassword	userPassword
memberOf	—
directReports	—
streetAddress	streetAddress
postalCode	postalCode
company	company
department	departmentNumber
email	mail
telephoneNumber	telephoneNumber
jobTitle	title
userDescription	description
assetCn	cn
assetName	name
dnsHostName	host
operatingSystem	operatingSystem

DSM 属性名	eTrust Directory の属性名
operatingSystemServicePack	operatingSystemServicePack
operatingSystemVersion	operatingSystemVersion
assetDescription	description
groupCn	cn
groupName	name
groupMembers	members
groupDescription	description
containerMap	container
groupMap	groupOfNames
userMap	inetOrgPerson
computerMap	device
uniqueUserFields 1 – uniqueUserFields 5	–
uniqueComputerFields 1 – uniqueComputerFields 5	–
userDn*	dn
groupDn*	dn
assetDn*	dn
o*	o

* 注: これらの属性のマッピングは固定されており、変更できません。ただし、クエリでは、これらの **DSM** 属性名を使用できます。

CA Client Automation のディレクトリ統合

サポートされたディレクトリ サービスの詳細なリストについては、「[互換性マトリックス](#)」を参照してください。

第 11 章: Client Automation セキュリティ機能

Client Automation のセキュリティ機能では、2つのサブジェクトエリアがサポートされます。

認可

要求しているオブジェクトが名乗っている身元に信頼を与えます。

認証

保護されたオブジェクト上で操作を実行するために、アクセス権と権限の設定および検証が提供されています。

このセクションには、以下のトピックが含まれています。

[認証](#) (P. 440)

[認可](#) (P. 452)

[共通セキュリティの設定](#) (P. 473)

[セキュリティエリアのサポート](#) (P. 481)

[暗号化の設定](#) (P. 485)

[FIPS 準拠の暗号方式](#) (P. 489)

認証

認証は、提供されたクレデンシャルに基づいて、Trusted Computing Base のメンバを識別します。

Trusted Computing Base のメンバは、以下のとおりです。

ユーザ、および間接的なグループ メンバシップ

主に、これらは現在のオペレーティング システムからの同じ種類のセキュリティ プリンシパルです。これらは、たとえば Windows ユーザ (Active Directory、ドメイン、またはローカル)、UNIX (LDAP)、または UNIX のローカル ユーザなどの可能性があります。

マシン

Windows NT など、Trusted Computing Base の一部であるコンピュータは、識別して認証することが可能です。理論的には、UNIX コンピュータも、信頼関係を結ぶことができる Trusted Computing Base の一部であるので、識別することができます。

ユーザまたはマシンの認証に、以下のように別の情報が使用されます。

- Windows の動作環境の場合：
 - ユーザ名
 - パスワード
 - Windows ドメイン
 - セキュリティ プロバイダ
- Linux および UNIX 動作環境の場合：
 - マシン名
 - ユーザ名
 - パスワード
 - セキュリティ プロバイダ

アプリケーションが異なると、認証に別の要件が必要になります。可能な場合は、統合ログオンが使用されます。つまり、明示的な認証情報を使用するようユーザーが要求されるのではなく、ユーザーの現在の認証情報が暗黙的に使用されます。

ただし、場合によっては、これらの認証情報がアクセスしているリソースに対して有効でないか、または特別な操作によって再認証が必要とされる場合があります。統合ログオンが使用されないか、または認証情報が有効でない場合、必要に応じて GUI アプリケーションによって認証情報が要求されます。一方、バッチモードで実行しているコマンドラインアプリケーションではエラーが発生し、認証エラーが記録されます。

ログイン認証情報を指定しており、ディレクトリに対してユーザーの認証に LDAP セキュリティプロバイダを使用している場合、これらの認証情報がターゲットディレクトリに対して有効であり、完全に指定されていることを確認してください。Active Directory の場合は、以下のようなフル LDAP DN を使用する必要があります。

CN=user,OU=Users,OU=myOU,DC=mydomain,DC=com

外部汎用 LDAP ディレクトリを認証に使用している場合、グループメンバシップを直接評価することができないため、認証オブジェクトに直接アクセス権が付与されている必要があります。この条件は Active Directory には適用されません。

サポートされているユーザー名のフォーマット

Client Automation によってサポートされているユーザー名のフォーマットは、以下のとおりです。これらの名前のフォーマットは、たとえば、エクスプローラ GUI および Web サービスなど、ユーザー名が必要なすべての CA Technologies アプリケーションに対して適用されます。

Windows ネイティブ セキュリティまたは Linux/UNIX ローカル セキュリティ(ローカル ユーザーおよび信頼されたドメイン)

ユーザー名フォーマット: *username* (Windows NT のダウンレベル フォーマットまたは Linux ユーザー)

Active Directory と通信する LDAP (Windows および Linux/UNIX)

ユーザー名フォーマット: UPN または DN

(Active Directory を除く) 任意のディレクトリと通信する LDAP (Windows および Linux/UNIX)

ユーザー名フォーマット: DN

ユーザー名フォーマット: UID または SN (Oracle Idap の場合)

X.509 証明書ベースの認証

Client Automation クライアント処理が認証を必要とする CAF プラグインに通信する場合は、常にターゲット サービス セキュリティの要件に関連するセキュリティクレデンシャルをクライアント処理が渡す必要があります。クライアント処理を Windows NT サービスまたは UNIX デーモンなどの自立処理として実行している場合、クライアント処理はユーザ クレデンシャルがないときに X.509 V3 証明書を使用して認証する場合があります。

Client Automation 認証のための X.509 証明書は、非対称キーのペアのパブリックキーと共にパッケージ化された属性と値のペアのセットで構成されています。証明書はデジタルに署名され、ルート証明書によって封印されます。証明書には、証明書の発行先のサブジェクト名、発行した認証局の名前、および有効期限についての情報が記録されます。サブジェクト名を識別名 (DN) と呼ぶ場合があります。サブジェクト名は x509cert ネームスペースの Uniform Resource Identifier (URI) に、以下のようにマップされます。

```
x509cert://dsm r11/CN=Basic Host Identity,O=Computer Associates,C=US
```

現在の証明書の概要については、[共通の証明書](#) (P. 625)および[アプリケーション固有の証明書](#) (P. 626)を参照してください。

パブリック キーの暗号方式を使用して、クライアントはリクエスト時にスケーラビリティ サーバに対して自分自身を認証します。スケーラビリティ サーバは、証明された ID を使用して後続の認可を確認し、監査レコードをコミットすることができます。管理コンソールを使用すると、証明書の URI を Client Automation 管理データベース内のタスクまたはオブジェクトに割り当てられた権限にすることができます。

オブジェクトレベルのセキュリティおよび証明書

Client Automation 管理データベースでは、クラスおよびオブジェクトレベルのセキュリティ (OLS) が提供されます。データベースに割り当てられた権限は、オブジェクト URI によって表されるセキュリティ プロファイルに関連付けられます。証明書の URI をセキュリティ プロファイルに関連付け、Client Automation 管理データベースへのアクセスを規制する場合に使用できます。

たとえば、スケーラビリティ サーバがドメインマネージャに接続している場合、登録証明書を使用して、自分自身を認証します。登録証明書に関連付けられている URI には、スケーラビリティ サーバノードの登録を許可するのに十分なデータベースへの権限のみが付与されます。

ルート証明書

Client Automation では、信頼されたルート証明書が使用されて、認証に使用される証明書が検証されます。特定の認証局チェーンを管理したり、ある証明書チェーンから新しいチェーンへのマイグレーションを補助する場合には、複数のルート証明書を同時に使用できます。

2つのノードが正常に通信して、その後続けて認証するには、認証子ノード（応答側）が認証機関の証明書（開始側）に署名したルート証明書にアクセスする必要があります。証明書を利用できない、認識されない、または無効の場合、認証に失敗します。予定された証明書をマイグレーションする間、複数の信頼されたルート証明書を使用して認証子を更新し、クライアントを段階的にマイグレーションできます。開始側が異なるバージョンの証明書を使用している場合、応答側によって信頼されているルート証明書によって署名されている場合には、正常に認証されます。

証明書の保管

認証証明書は、各 Client Automation ノード上に安全に保存されます。証明書ファイルはパスワードで保護され、使用するパスワードは Client Automation 設定を使用して暗号化されます。

基本ホスト ID の証明書

各 Client Automation ノードには、デフォルトでインストールされた基本ホスト ID（BHI）を提供する証明書があります。特別な目的のためのほかの証明書は、その証明書を必要とするサービスと共にインストールされます（[現在の証明書](#) (P. 625)を参照）。CA Client Automation のインストールには、Client Automation ルート証明書によって署名されたデフォルトの標準証明書が付属します。この証明書はエンタープライズ内の各 Client Automation ノードにインストールされます。

エンドユーザ自身が自分のルート証明書、基本ホスト ID（BHI）の証明書、およびアプリケーション固有の証明書の作成を計画することをお勧めします。デフォルトの証明書をエンドユーザ固有の証明書で置き換える方法については、[X.509 証明書をインストールイメージへ導入する方法](#) (P. 255)を参照してください。

新しい BHI 証明書を作成する場合、3つの主要なパラダイムがあります。

- エンタープライズ内のすべての Client Automation ノードで使用される単一のホスト ID の証明書を作成します。固有のパッケージを作成するのにカスタムインストールイメージを 1 回だけ生成すればよい場合、これは最も簡単なソリューションです。

- DSM エンタープライズ内の各ノードに対して、一意のホスト ID の証明書を作成します。これは最も複雑なソリューションです。各ノードに割り当てられた DN が一意であり、ホストマシンの ID を反映している必要があります。通常、完全修飾ホスト名がこの目的に適しています。適切な証明書ファイルをターゲットマシンにインストールする場合は、カスタム インストールイメージが必要です。
- 上記 2 つのパラダイムを組み合わせます。Client Automation ノードの大半で使用する単一のホスト ID の証明書を作成します。DSM スケーラビリティサーバおよびマネージャ ノードで使用する固有の ID の証明書を作成します。固有の証明書の要件が識別された場合、新しい証明書を発行して指定されたノードにインストールします。これは最も柔軟なソリューションです。エンタープライズの重要なノードがより効率的に識別および保護されます。

証明書の配信

証明書の配信は、証明書の作成前に実行される必要があります。選択した証明書の作成方法に応じて、証明書の配信は非常に複雑になることがあります（[基本ホスト ID の証明書](#) (P. 443)の説明を参照）。

Client Automation では、証明書の自動配信テクノロジーはサポートされません。各 Client Automation ノードのデフォルトの証明書およびアプリケーション固有の証明書が配信されます。

デフォルトのインストール後、デフォルトの証明書をマイグレートするには、証明書を以下の（簡単な）方法で配信する必要があります。この方法により、通信時にダウンタイムが発生することなく、また信頼されたルートを同時使用する場合に必要な認証が実行されることなく、信頼できるマイグレーションが正常に実行されます。

1. 新しいルート証明書を作成します。ルート名 (DN) が既存の Client Automation ルート証明書の名前とは異なっていることを確認します。
2. DER でエンコードされた新しいルート証明書を Client Automation インフラストラクチャ内のすべてのノードに配信するスケジュールを設定します。これによって、ルートがすべての Client Automation ノードに対して信頼されたルート権限になることができます。
3. 新しいセキュリティ プロファイルを Client Automation 管理データベースに作成して、既存のアプリケーション固有の証明書プロファイルを置き換えます。ここではまだ古いプロファイルを削除しないでください。
4. 新しい証明書をすべての Client Automation ノードに配信するスケジュールを設定します。

5. 証明書の配信が正常に終了した後、古い **Client Automation** 証明書の削除をスケジュールします。
6. アプリケーション固有の証明書の古いセキュリティ プロファイルを削除します。

このリストは完全ではありません。大規模な証明書の配信および全面的な **PKI** 実装への置き換えについては、**CA Technologies** テクニカル サポートにお問い合わせください。

新しい証明書の作成

新しい証明書を作成するために、提供された **cacertutil** ツールを使用するか、または既存の **PKI** を使用して証明書を生成できます。外部 **PKI** システムの使用は、このドキュメントの範囲外ですが、証明書の要件は **cacertutil** での証明書の作成と同じです。

注: 外部 **PKI** では、**Client Automation** インフラストラクチャのために新しいルート証明書を作成する必要がありません。

新しいルート証明書の生成

新しいルート証明書を作成する場合、証明書は以下の 2 つの形式で作成する必要があります。

- **PKCS#12** エンコード ファイル。このファイルには、証明書のパブリック セクションとプライベート キーの両方が含まれます。
- **DER** エンコード ファイル。このファイルには、証明書の公開されてアクセスできる部分のみが含まれます。

証明書の両方の形式は、**Client Automation** ツールを使用して同時に生成されます。外部 **PKI** を使用している場合、ルート証明書を **DER** フォーマットでエクスポートできます。

新しいルート証明書は、**Client Automation** のセキュリティの中心となるため、偶発的また意図的な開示から保護される必要があります。**PKCS#12** 証明書ファイルは、複雑なパス フレーズで保護され、管理者による安全なデータ ストアに保存される必要があります。

PKCS#12 フォーマットの証明書は、ほかの証明書に署名する場合に使用されます。DER フォーマットの証明書は、これらの署名された証明書を検証する場合に使用されます。

新しいルート証明書を作成するためのコマンドのフォーマットは、以下のとおりです。

```
"cacertutil create -o:rootname.p12 -od:rootname.der -op:passphrase  
""-s:CN=YourRoot,O=YourOrg,C=Country"" -d:NumberOfDays -oe"
```

-o

PKCS#12 でパッケージ化された証明書の出力ファイル名を指定します。

-od

DER でエンコードされた証明書の出力ファイル名を指定します。

-op

PKCS#12 証明書ファイルを暗号化する場合に使用されるパスフレーズを指定します。

-s

証明書のサブジェクトを指定します。

-d

証明書の存続期間を日数で指定します（たとえば、730（2年））。

-oe

証明書のデコードに使用されるパスフレーズのランダムに暗号化されたバージョンを生成し、コンソールに出力します。暗号化されたパスフレーズは、平文のパスワードの代わりに証明書ツールに提供できます。

アプリケーション固有の証明書の生成

[「現在の証明書」](#) (P. 625)でリストされている各アプリケーションに対して、新しい証明書を作成します。付録の表でリストされているようには DN を使用しない場合、Client Automation セキュリティ ブラウザの証明書セキュリティ プロファイルに必要な権限を割り当てる必要もあります。

新しく作成した証明書が Client Automation セキュリティ ブラウザできちんと表示されるには、DER エンコード証明書をマネージャ ノードの Client Automation 証明書データベースにインポートする必要があります。

新しい証明書を作成するコマンドは、以下のとおりです。

```
"cacertutil create -o:certname.p12 -od:certname.der -op:passphrase ""-s:CertDN""  
-i:rootname.p12 -ip:rootpassphrase -d:730"
```

-o

PKCS#12 でパッケージ化された証明書の出力ファイル名を指定します。

-od

DER でエンコードされた証明書の出力ファイル名を指定します。

-op

PKCS#12 出力証明書を保護するパスフレーズを指定します。

-s

証明書の発行先となる DN を指定します。

-i

ルート PKCS#12 証明書のファイル名を指定します。

-ip

ルート PKCS#12 証明書を保護するパスフレーズを指定します。

-d

証明書の存続期間を日数で指定します（例では、2 年（730 日）が使用されています）。

基本ホスト ID の証明書の生成

基本ホスト ID（BHI）の証明書には、デフォルトのインストールでは **Client Automation** 管理データベースへの権限がなく、関連するセキュリティプロファイルもありません。このため、証明書のために新しい DN を選択しても、**Client Automation** セキュリティプロファイルおよび権限は追加されません。

BHI 証明書に割り当てられたデフォルトの DN は、以下のとおりです。

CN=Basic Host Identity,O=Computer Associates,C=US

新しい基本ホスト ID の証明書を作成するためのコマンドのフォーマットは、以下のとおりです。

```
"cacertutil create -o:certname.p12 -od:certname.der -op:passphrase ""-s:CertDN""  
-i:rootname.p12 -ip:rootpassphrase -d:730"
```

-o

PKCS#12 でパッケージ化された証明書の出力ファイル名を指定します。

-od

DER でエンコードされた証明書の出力ファイル名を指定します。

-op

PKCS#12 出力証明書を保護するパス フレーズを指定します。

-s

証明書の発行先となる DN を指定します。

-i

ルート PKCS#12 証明書のファイル名を指定します。

-ip

ルート PKCS#12 証明書を保護するパス フレーズを指定します。

-d

証明書の存続期間を日数で指定します（例では、2 年（730 日）が使用されています）。

新規証明書のインストール

新しい証明書を **Client Automation** ノードにインストールする場合、証明書をインストールする処理は、ローカルの管理者ユーザ、つまり、**Windows** では管理者グループのメンバとして実行する必要があります。

新しいルート証明書のインストール

新しいルート検証証明書を **Client Automation** ノードにインストールするには、DER エンコードファイルを使用します。この証明書をインストールするためのコマンドのフォーマットは、以下のとおりです。

```
cacertutil import -i:rootcert.der -ip:passphrase -it:X509V3
```

このコマンドによって、信頼されたルート証明書として公開されたアクセス可能な証明書情報が証明書データベースにインポートされます。

アプリケーション固有の証明書のインストール

CA Client Automation コードベースでは、アプリケーション固有の証明書は、証明書に割り当てられた DN ではなく、タグ名を使用して参照されます。関連するタグ名の詳細については、[「現在の証明書」](#) (P. 625)を参照してください。証明書は、DSM スケーラビリティ サーバまたはマネージャに対して認証する場合に証明書を必要とするノードにのみインストールする必要があります。

アプリケーション固有の証明書をインストールするためのコマンドのフォーマットは、以下のとおりです。

```
cacertutil import -i:certname.p12 -ip:passphrase -t:tagname
```

-i

インポートする PKCS#12 証明書ファイルの名前を指定します。

-ip

証明書を保護する場合に使用されるパス フレーズを指定します。

-t

証明書のタグ名を指定します。

証明書が DSM セキュリティ ブラウザで表示されるには、DER エンコード証明書をマネージャ ノードの証明書データベースにインポートする必要があります。DER エンコード証明書をインポートするためのコマンドのフォーマットは、以下のとおりです。

```
cacertutil import -i:certname.der -it:X509V3
```

-i

インポートする DER エンコード証明書の名前を指定します。

-it

インポートする証明書のタイプを指定します。X509V3 は DER エンコードを指定します。

基本ホスト ID の証明書のインストール

基本ホスト ID の証明書は、常にタグ名 `dsmcommon` を使用してインストールされます。BHI 証明書をインストールするためのコマンドのフォーマットは、以下のとおりです。

```
cacertutil import -i:certname.p12 -ip:passphrase -t:dsmcommon -h
```

-i

入力 PKCS#12 証明書のファイル名を指定します。

-ip

入力証明書を保護する場合に使用されるパス フレーズを指定します。

-t

証明書のタグ名を指定します。

-h

証明書がデフォルトのホスト ID を提供する場合に使用される必要があることを指定します。

証明書の置換

デフォルト **Client Automation** 証明書の置換では、新しい証明書でも、元の証明書の物理的ファイル名と同じ名前を使用する必要があります。証明書に割り当てられるサブジェクト名は、元の名前と同じにする必要はありません。これらの名前は、**cfcert.ini** インストール ファイルによって記録および制御され、このファイルの指示によって、インストール中にデータベースへ挿入されます。

以下の表に、ファイル名および関連のリストを示します。

ファイル名	Client Automation サブジェクトへの関連付け
dsm_dsm_r11_root.der	ルート証明書
basic_id.p12	基本ホスト ID の証明書
dsmpwchgent.p12	エンタープライズ アクセス
dsmpwchgdom.p12	ドメイン アクセス
dsmpwchgrep.p12	レポート アクセス
ccsm.p12	CSM アクセス
dsm_dsm_r11_cmdir_eng.p12	ディレクトリ同期アクセス
registration.p12	登録アクセス
dsm_dsm_r11_sd_catalog.p12	SD カタログ アクセス
dsm_dsm_r11_agent_mover.p12	SD エージェント ムーバアクセス

証明書の削除

証明書は、1 回に 1 つずつ、またはまとめてのいずれかで削除することができます。

証明書をそれぞれ削除するには、以下のコマンドを実行します。

```
cacertutil remove -s:subject_name [-t:tag_name] [-l:{local|global}]
```

-s

証明書を発行する相手へのサブジェクト名を指定します。

-t

一緒にインストールされている場合は、証明書のタグ名を指定します。

-l

証明書がグローバルまたはローカル共通ストアのどちらにインストールされたかを指定します。

証明書をまとめて削除するコマンドは、以下のとおりです。

```
cacertutil flush
```

重要: このコマンドを使用すると、すべての証明書エントリが現在のユーザおよびローカル マシンの両方の共通ストアから削除されます (現在のプロセス ユーザに十分な権限がある場合)。

VMware ESX セキュリティおよび認証

Client Automation AM リモート エージェントは、セキュリティで保護された HTTP モードで動作している VMware ESX サーバのみをサポートします。VMware では、セキュリティで保護された HTTP (デフォルト設定では HTTPS) を本番環境の展開に使用することを推奨しています。なぜなら、AM リモート エージェントが接続できるのは、デフォルト、つまりセキュリティで保護された HTTP を使用している推奨設定の ESX ホストのみだからです。

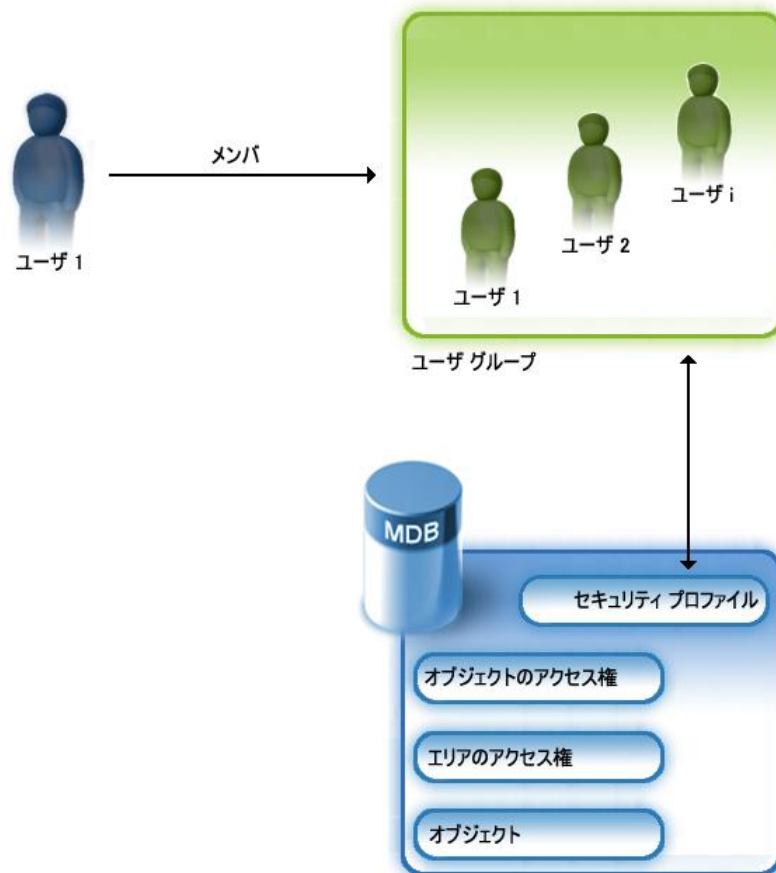
DSM エージェントと ESX ホスト マシン間の接続プロトコルとして、SSL (Secure Sockets Layer) が使用されます。ただし、ESX ホスト マシンの ID は事前にわからないため、DSM エージェントおよび ESX ホストの間の認証は行いません。ESX ホストの認証に証明書は使用されません。

認可

認可によって、認証されたエンティティ（通常はログイン ユーザ）に関連付けられたオブジェクトに対する権限が制御されます。認証されたエンティティは、セキュリティプロファイルで管理されます。つまり、ユーザまたはユーザグループはセキュリティプロファイルによって表され、すべてのアクセス権はセキュリティプロファイルに関連して管理されます。

Client Automation セキュリティ サブシステムでは、CA Client Automation 全体に対して堅牢かつ汎用的なセキュリティ オプションを提供することによって、認可が管理されます。セキュリティプロファイルで指定される認証されたエンティティに関連付けられたオブジェクトに対する権限は、このセキュリティ サブシステムによって制御されます。

以下の図に、認証を制御するセキュリティ サブシステムの概要を示します。



通常、システムにログオンするユーザは、複数のユーザ グループのメンバです。ユーザ グループは、セキュリティ プロファイルによって表されます。

つまり、**Client Automation** 管理者は、ユーザ グループのセキュリティ プロファイルまたは特定のユーザに対する個別のセキュリティ プロファイルを作成する必要があります。

Client Automation オブジェクトと共に、オブジェクトに対するセキュリティ プロファイルの権限も **MDB** に格納されます。

たとえば、セキュリティ プロファイルを作成して、**Client Automation** システムにアクセスできるオペレーティング システム依存のグループおよびユーザを決定できます。また、クラスのアクセス権、グループおよびオブジェクトのアクセス権を確立し、選択されたフォルダまたはオブジェクトへのユーザまたはユーザ グループのアクセス権を制限することもできます。

セキュリティ プロファイル

セキュリティ プロファイルは、ドメイン マネージャ（ローカル プロファイル）またはネットワーク ドメイン（ドメイン プロファイル）のオペレーティング システムのユーザ アカウントまたはグループです。

Client Automation のセキュリティ サブシステムでは、複数のセキュリティ プロファイルがサポートされています。セキュリティ プロファイルは組み込み（つまり、インストール時に作成される）か、またはユーザ定義のいずれかです。

ユーザ定義のセキュリティ プロファイルは、単一のユーザかまたはユーザ グループのいずれかを表わします。

インストール時に作成される重要なセキュリティ プロファイルは、以下のとおりです。

- 所有者（仮想アカウント）
- 全員（全員のためのデフォルトの仮想アカウント）

セキュリティ プロファイル以外に、プロファイルに関連付けられている一連のセキュリティ クラスもあります。各プロファイルには、一連の独自のセキュリティ クラスがあります。セキュリティ クラスによって、クラスのインスタンスの作成直後に割り当てられる権限を設定できます。

また、セキュリティ プロファイルを信頼されたドメインのユーザに対しても作成できます。各ユーザには、システムにログインするための有効なセキュリティ プロファイルが設定されている必要があります。新しいユーザが管理対象グループに追加された場合、グループに付与されたアクセス権を自動的に継承し、すぐにシステムにログインすることができます。

1人のユーザが複数のプロファイルを持つことができます。ただし、各プロファイルは、1つのユーザまたはグループにのみマップすることができます。たとえば、ユーザがグループのメンバである場合、プロファイルを2つ持つことができます。1つはユーザアカウントにマップされているもの、もう1つはグループにマップされているものです。この場合、ユーザの持つ権限は両プロファイルの和集合です。

ユーザが1つ以上のセキュリティプロファイルのメンバである場合、そのユーザに有効な権限とは、各セキュリティプロファイルで定義されている各権限の和集合です（すべての権限の OR 演算を適用するなど）。

各セキュリティプロファイルのユーザのアクセスを拒否する場合、そのユーザをセキュリティプロファイルから削除する必要があります。

システムには事前定義済みセキュリティプロファイルがあり、[セキュリティプロファイル] ダイアログボックスを使用して、プロファイルを必要に応じて作成することができます。

作成するプロファイルのうち少なくとも1つでは、システムへのアクセス権を[フルコントロール]に設定することをお勧めします。

権限の概要

認証には、以下の種類の権限があります。

- クラスのアクセス権
- オブジェクトのアクセス権
- エリアの権限

セキュリティサブシステムでは、すべての種類の権限が管理され、累積アプローチによって有効な権限が決定されます。

有効なエリアの権限を持っている場合、オブジェクトにアクセスするために、両方の種類の権限（オブジェクトのアクセス権およびエリアの権限）が確認されます。つまり、ユーザがオブジェクトを管理対象にするには、オブジェクトのアクセス権およびエリアの権限が必要となります。オブジェクトのアクセス権は、エリアのサポートが無効にされている場合にのみ確認されます。

クラスのアクセス権

クラスのアクセス権は、クラス レベルで指定するアクセス権です。つまり、クラス レベルのアクセス権は、そのクラスのインスタンスである各オブジェクトに対するデフォルトの権限となります。

セキュリティ プロファイルの作成時に、各セキュリティ プロファイルに対してクラスのアクセス権を指定する必要があります。すべてのセキュリティ クラスに対して、デフォルトでは「アクセス権なし」が設定されています。適切なクラスのアクセス権を持つセキュリティ プロファイルによって、システムへのアクセス権が付与されます。このアクセス権は、「クラスのアクセス権」ダイアログ ボックスで指定することができます。

クラスのアクセス権は、オブジェクト クラスのすべてのオブジェクトにグローバルに適用することができます。エクスプローラの特定のオブジェクトまたはフォルダのユーザを制限し、拡張アクセス権を付与する場合は、「オブジェクトのアクセス権」ダイアログ ボックスまたは「セキュリティ グループのアクセス権」ダイアログ ボックスをそれぞれ使用します。

セキュリティ クラスは、同一の種類オブジェクトをグループ化するために使用されます。**CA Client Automation** のセキュリティ サブシステムでは、以下のセキュリティ クラスがサポートされます。

- 検出されたハードウェア (コンピュータ)
- ユーザ
- コンピュータ ユーザ
- マネージャ
- サーバ
- アセット グループ
- サーバ グループ
- ドメイン グループ
- クエリ
- セキュリティ クラス
- セキュリティ プロファイル
- ソフトウェア パッケージ
- ソフトウェア プロシージャ
- プロシージャ グループ
- ジョブ コンテナ
- ソフトウェア ジョブ
- アセット ジョブ
- モジュール
- クエリ ベースのポリシー
- イベント ベース ポリシー
- OSIM ブート イメージ
- OSIM OS イメージ
- エンジン
- 設定ポリシー コンピュータ
- 設定ポリシー ユーザ
- 外部ディレクトリ アクセス
- レポート テンプレート
- インベントリ モジュール

以下のセキュリティ クラスは、クラス レベルでのみ使用されます。

- MDB アクセス
- コントロール パネルの有効化
- Remote Control の有効化

クラス レベルセキュリティとは、すべてのオブジェクトつまりクラスのインスタンスに、クラスで定義された権限がデフォルトで付与されることを意味します。

特定のアクションに必要なクラスのアクセス権の組み合わせ

一部のオブジェクト クラスの権限は、相互依存しています。したがって、以下のアクションを実行する場合には、複数のオブジェクト クラスに権限を付与する必要があります。

レポート テンプレート

レポート テンプレートをスケジュールする場合は、オブジェクト クラス「レポート スケジューリング」およびオブジェクト クラス「エンジン」に変更権限を付与する必要があります。

セキュリティ プロファイル

セキュリティ クラス「セキュリティ プロファイル」では、セキュリティ プロファイルの処理（削除など）が制御されます。セキュリティ プロファイルのオブジェクト クラスのアクセス権を変更する場合は、オブジェクト クラス「クラスのアクセス権」に対する特殊アクセス（VRP、「P」権限がある）を持っている必要があります。

エンジン

エンジン タスクをエンジンにリンクする場合、オブジェクト クラス「エンジン」に変更権限を付与し、オブジェクト クラス「エンジン タスク」に管理権限を付与する必要があります。

エンジンセキュリティにかかわらず、エンジン オブジェクトを開始、停止、または変更する場合には、セキュリティ プロファイルのクラス「エンジン」にフル コントロールを付与し、エンジンが実行されているコンピュータに NT 管理者権限または root 権限以上を付与する必要があります。

ソフトウェア ジョブ セキュリティ

/computer フォルダの下ソフトウェア ジョブを変更または削除する場合、ソフトウェアは /Jobs/Software Jobs へ配信されます。つまり、オブジェクト クラス「コンピュータ」および「ソフトウェア ジョブ」には、変更権限を付与する必要があります。

プロセスセキュリティ

プロセス オブジェクトを開始、停止、または変更する場合は、クラス「プロセス」に変更権限（VRWXD）を付与し、ファイル権限以上を管理者または root に付与する必要があります。

セキュリティエリアのサポート

セキュリティ エリアのサポートを有効化または無効化し、デフォルトのセキュリティ エリアを定義する場合は、オブジェクトクラス「セキュリティ エリア」のクラスのアクセス権を少なくとも特殊アクセス（VP）に設定する必要があります。

セキュリティ プロファイルをセキュリティ エリアにリンクする場合、オブジェクトクラス「セキュリティ エリア」には、表示（V）アクセス権があれば十分です。オブジェクトクラス「セキュリティ プロファイル」のクラスのアクセス権は、少なくとも特殊アクセス（VW）に設定する必要があります。

オブジェクトのアクセス権

オブジェクトのアクセス権を設定すると、特定のオブジェクトのアクセス権を制限する場合に役立ちます。すべてのオブジェクトは、オブジェクトクラスに設定された権限をデフォルトで継承します。

オブジェクトのアクセス権は、クラスおよびグループのアクセス権よりも優先されます。

オブジェクトのアクセス権は常に存在し、セキュリティ サブシステムによって管理されているため無効にすることはできません。オブジェクトのアクセス権を管理しない場合は、すべてのセキュリティ クラスのクラス レベルのアクセス権を [フル コントロール] に設定します。

認証は、アクセス制御エントリ（ACE）の概念に基づいています。ACE とは、以下の表に示すコード文字の任意の組み合わせ（たとえば VR）です。この ACE を使用して、オブジェクトを表示および読み取ることができます。その他のアクセスはすべて拒否されます。

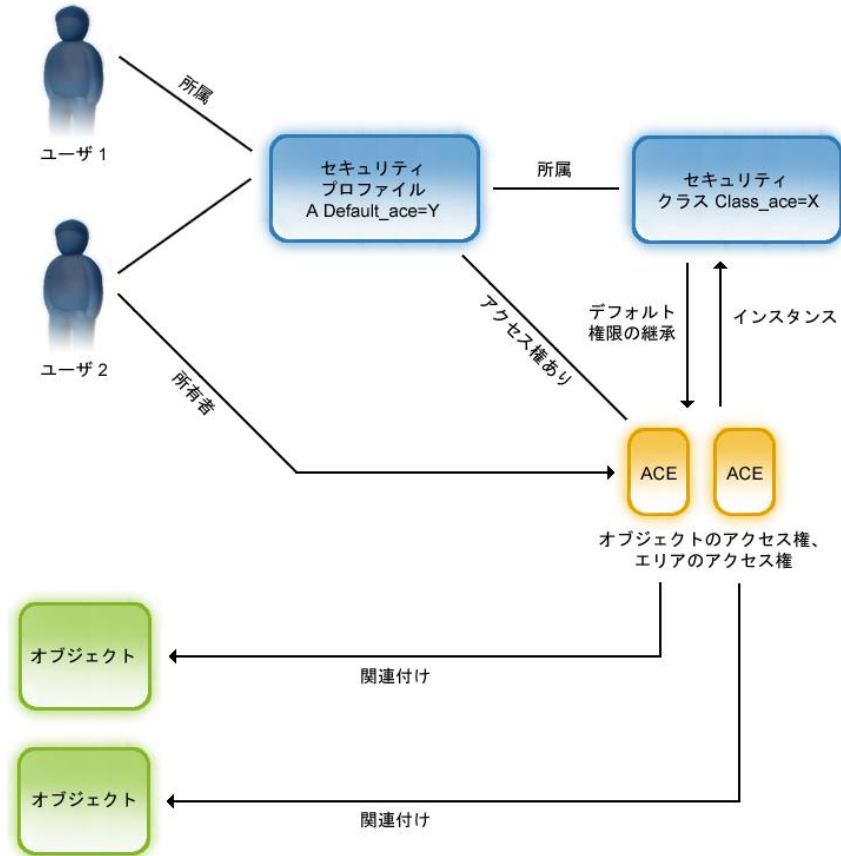
ACE が空（コード文字が含まれない）の場合、アクセス権はまったく付与されません。

以下の表に、オブジェクトのアクセス権の定義を示します。

コード文字 (ACE 内)	意味	付与される権限
V	ビュー	オブジェクトを表示することができます。
C	作成	オブジェクトを作成することができます。
R	読み取り	オブジェクトのサブオブジェクトを読み取ることができます。
W	書き込み	オブジェクトを変更することができます。
X	Execute	オブジェクト タイプに応じて実行することができます。
D	削除	オブジェクトを削除することができます。
P	権限	ACE 自身を変更することができます。
O	所有権	オブジェクトの所有権を取得することができます。

ユーザは、複数のセキュリティ プロファイルに属している場合があります。また、ユーザは、オブジェクトの所有者になることもできます。セキュリティ クラスのセットは、各セキュリティ プロファイルに割り当てられています。セキュリティ クラスのアクセス権では、クラスのインスタンスの作成時にオブジェクトに割り当てられるデフォルトのアクセス権が定義されます。

以下の図では、セキュリティプロファイル、セキュリティクラス、およびオブジェクトのアクセス権が相互に関連しており、オブジェクトはそれがインスタンスであるセキュリティクラスから権限を継承することを示しています。



この図では、ユーザ 1 はセキュリティプロファイル A に属し、ユーザ 2 はセキュリティプロファイル A に属し、かつ ACE で表されるオブジェクトの所有者でもあります。ユーザ 1 およびユーザ 2 は、セキュリティプロファイル A を介して、たとえば VR などの特定の ACE を持っています。ユーザ 2 は、オブジェクトの所有者として、たとえば VCRWD などの追加の ACE を持っています。

ユーザ 1 およびユーザ 2 のオブジェクトへのアクセス権をチェックするために、セキュリティシステムではユーザ固有の ACE および保護された特定のオブジェクトに関連付けられた ACE の（論理的な）結合が作成されます。たとえば、ユーザ 1 およびユーザ 2 はオブジェクトへの「参照」および「読み取り」のアクセス権を持っていますが、書き込みおよび削除のアクセス権を持っているのはユーザ 2 のみです。

セキュリティレベル

オブジェクトのアクセス権の取得方法に応じて、オブジェクトのセキュリティレベルのタイプが異なります。

クラスレベルのセキュリティ

オブジェクトのアクセス権がクラスレベルのアクセス権から（オブジェクトが属するクラスから）派生している場合、セキュリティレベルはクラスレベルに設定されます。保護されたオブジェクトが作成される場合のデフォルトです。

グループレベルのセキュリティ

保護されたオブジェクトが継承の許可されているグループのメンバーである場合、セキュリティレベルはグループレベルに設定されます。アクセス権は、オブジェクトがメンバーであるグループから派生します（グループレベルのアクセス権）。

オブジェクトレベルのセキュリティ

ユーザが特定の保護されたオブジェクトに対して手動でオブジェクトのアクセス権を設定する場合、セキュリティレベルはオブジェクトレベルに設定されます（アクセス権がオブジェクトに対して個別に設定されているため）。

グループからのアクセス権の継承

オブジェクトがグループのメンバーである場合、**Client Automation** のセキュリティサブシステムでは、以下のようにグループからメンバーへのアクセス権の動的な継承がサポートされています。

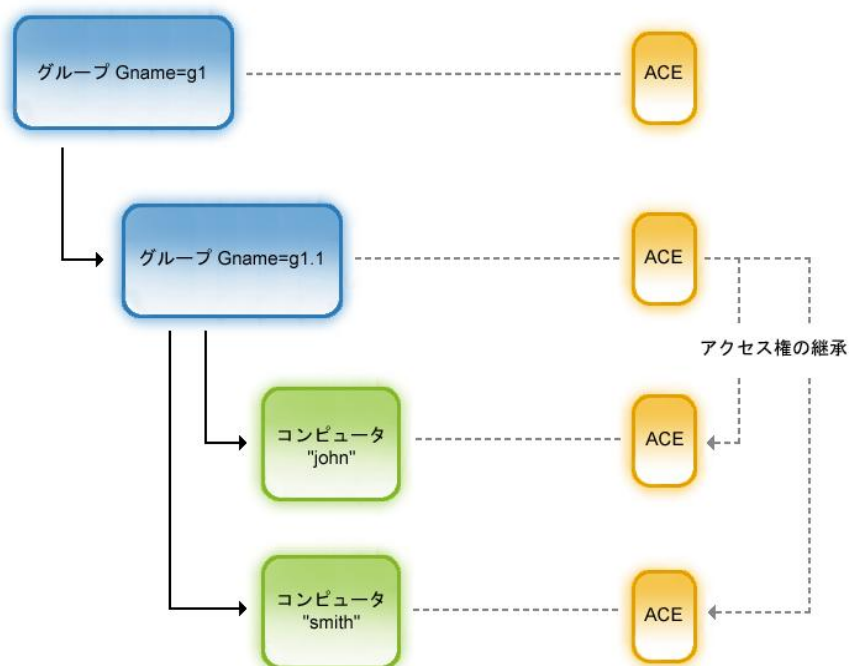
- フラグによって動的な継承のグループがマーキングされます。
- 指定されたメンバーの権限は、このグループのすべてのメンバーに継承されます。
- メンバーがグループに追加されている場合、自動的にグループの権限が継承されます。

グループセキュリティの設計、以下の決定事項に基づいて行われています。

- セキュリティの継承は、グループに対してオンまたはオフに設定できます。オンに設定すると、グループはセキュリティグループ（アプリケーションによって表示に使用されるアイコンが異なる場合があります）になります。
- このグループには、（ほかの保護されたオブジェクトと同様）グループ自体に対するアクセス権マスクと継承マスクという 2 つのアクセス権マスクがあります。
- グループが親グループからアクセス権を継承する場合、両方のマスクは親グループの継承マスクに変更されます。
- 1 つまたは複数のグループのメンバのアクセス権マスクは、メンバの親のすべてのアクセス権の「統合」として判断されます（すべてのアクセス権が OR 演算されます）。
- 親から子へと継承が行われるため、オブジェクトの再帰的な更新が発生する場合があります。
- 継承の深さに制限はありません。
- 優先順位は、オブジェクトのアクセス権、グループのアクセス、クラスのアクセス権となります。
- オブジェクトが少なくとも 1 つのセキュリティグループのメンバである場合、クラスのセキュリティの適用はモデルに違反しているため、そのオブジェクトに対して許可されている変更操作はオブジェクトセキュリティの適用のみです。クラスのセキュリティをアクティブにするには、オブジェクトをグループから削除するか、またはグループに対してセキュリティの継承をオフにする必要があります。

注: オブジェクトのセキュリティ レベルがオブジェクト レベルに設定された場合、グループからの継承はオフになります。

以下の図に、オブジェクトがグループのメンバであり、グループによってオブジェクトのアクセス権の継承が可能になっている場合の継承を示します。



グループ **g1.1** は、グループ **g1** のサブグループです。コンピュータ「john」および「smith」は、グループ **g1.1** のメンバです。

グループ **g1** ではアクセス権の継承が無効になっていますが、グループ **g1.1** では有効になっています。したがって、コンピュータ「john」および「smith」は、グループ **g1.1** のアクセス権からアクセス権を継承します。

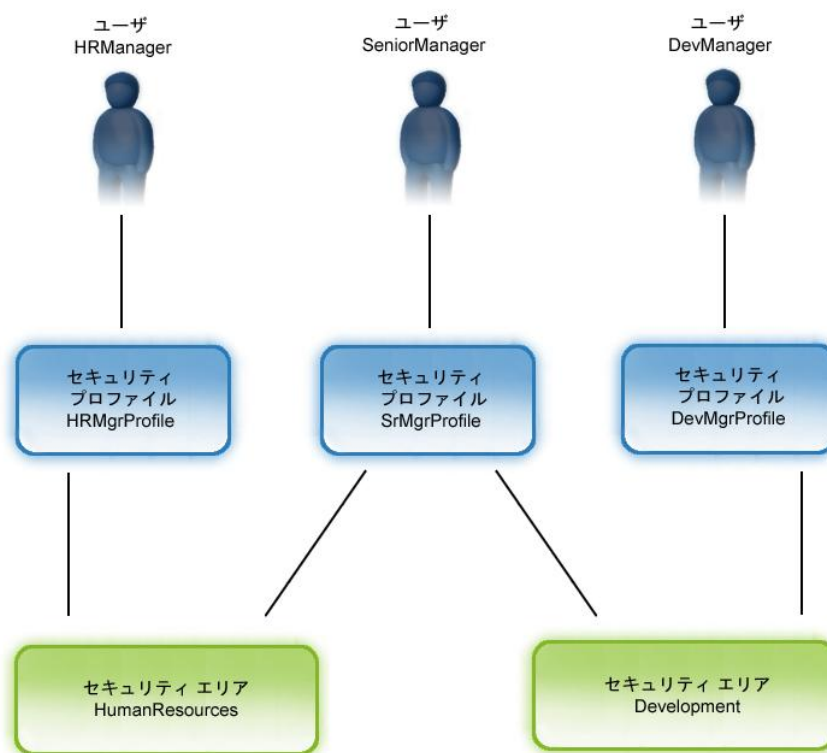
エリアの権限

セキュリティ エリアの概念によって、セキュリティ モデルが拡張されます。セキュリティ エリアは、さまざまなユーザが管理する何千ものオブジェクトが使用される大規模な実装に適したオプションの機能です。

セキュリティ エリアは、地理的、組織的、またはトポロジ上の区分です。セキュリティ エリアを定義しておく、ユーザのアクセス権をセキュリティ エリアにリンクされているオブジェクトにのみ制限する場合に役立ちます。セキュリティ エリアの概念では、セキュリティ プロファイルおよびオブジェクトによって示されるユーザがセキュリティ エリアにリンクされます。セキュリティ エリアは、複数のプロファイル、および複数のオブジェクトにリンクされている可能性があります。オブジェクトにリンクされている少なくとも 1 つのセキュリティ エリアが、ユーザの少なくとも 1 つのセキュリティ プロファイルにもリンクされている場合、ユーザはオブジェクトにアクセスできます。オブジェクトアクセス権が拒否された場合、ユーザに対してそのオブジェクトは表示されません。

例: 2つのセキュリティエリアおよび3人のユーザ

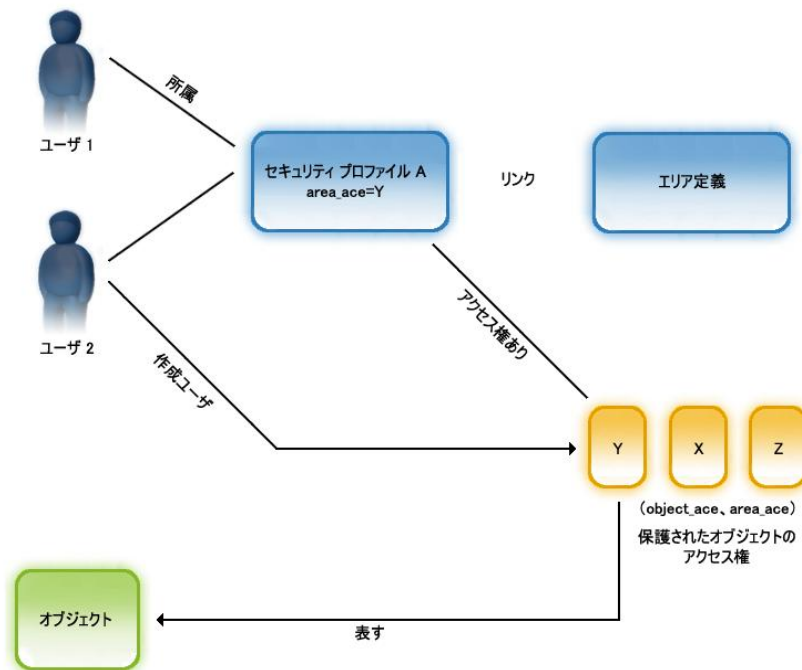
HRManager、SeniorManager、および DevManager の3人のユーザには、ユーザプロフィール HRMgrProfile、SrMgrProfile、および DevMgrProfile（すべてのアクセス権）が割り当てられます。HumanResources および Development という2つのセキュリティエリアが定義されています。プロフィール HRMgrProfile および SrMgrProfile は、セキュリティエリア HumanResources にリンクされています。プロフィール SrMgrProfile および DevMgrProfile は、セキュリティエリア Development にリンクされています。したがって、SrMgrProfile で示される SeniorManager は、HumanResources および Development の両方のセキュリティエリアへのアクセス権を持っています。HRManager はセキュリティエリア HumanResources へのアクセス権のみを持っていて、ユーザ DevManager はセキュリティエリア Development へのアクセス権のみを持っています。たとえば、HRManager が HumanResources エリア内の自分のコンソールでクエリを作成した場合、これはユーザ DevManager に対して非表示になります。すべてのユーザプロフィールに対しては、システムで作成されたオブジェクトのみが表示されます。



エリアのアクセス権を設定すると、1つ以上のプロファイルの特定のオブジェクトに対するアクセス権を制限できます。つまり、 $t1$ つのプロファイルに対して定義されている複数のクラス レベルのアクセス権が同じになります。オブジェクトをさまざまなエリアに割り当てまたはリンクするか、プロファイルのアクセスを特定のエリアにリンクされた オブジェクトのみの表示に制限できます。

オブジェクトのアクセス権は、基本的にセキュリティ クラスによって管理されています。また、セキュリティ サブシステムでは、最大 32 のエリアの作成が許可されています。

以下の図に、セキュリティ サブシステムのエリアのサポートの概要を示します。



ユーザ 1 および ユーザ 2 はセキュリティ プロファイル A に属しています。プロファイル A にリンクされているエリアの定義では、セキュリティ プロファイル A に属するユーザに対して表示するエリアが定義されます。

ユーザ 2 が作成したオブジェクトは、適切なエリアにリンクされているすべてのユーザに対して表示されます。

重要なユース ケース、およびこれらのユース ケースのコンテキストにおけるエリアのサポート内容については、[セキュリティ エリアのサポートのユース ケース \(P. 633\)](#)を参照してください。

エリアのオブジェクト アクセス権の前提条件

以下の条件を満たしてから、ユーザのエリアのアクセス権を評価します。

- ユーザは、そのオブジェクトへのオブジェクト アクセス権（表示または読み取り権限）を持っている必要があります。
- ドメイン マネージャ上でのセキュリティ エリア サポートを有効にする必要があります。
- ユーザがメンバになっているすべてのセキュリティ プロファイルで、セキュリティ エリアのサポートが有効になっている必要があります。

最初の条件が満たされていない場合、2 番目および 3 番目の条件を満たしていても、ユーザのオブジェクト アクセス権は拒否されます。2 番目または 3 番目の条件を満たしていない場合は、ユーザはエリアの権限に基づいて制限されることなくすべてのオブジェクトにアクセスできます。

注:

- ユーザはセキュリティ エリアが無効になっているセキュリティ プロファイルのメンバの場合、すべてのオブジェクトにアクセスできます。セキュリティ エリア サポートのために、すべてのセキュリティ プロファイルが有効になっていることを管理者が確認することをお勧めします。
- セキュリティ エリアのサポートは、DSM エンタープライズ マネージャでは使用できません。
- 「配信」プロファイルは、セキュリティ エリア サポートのために有効にできる唯一の組み込みプロファイルです。その他のすべての組み込みプロファイルは、セキュリティ エリア サポートに対して無効にします。
- 「プロシージャ」または「ソフトウェア ジョブ」セキュリティ クラスに属するオブジェクトは、DSM エクスプローラ内のセキュリティ エリアにリンクできません。これらのオブジェクトは、親コンテナ（「ソフトウェア パッケージ」および「ソフトウェア ジョブ コンテナ」）がリンクされているエリアに自動的にリンクされています。

取得されたエリアの権限

エリアのアクセス権は、以下の方法で設定および取得されます。

セキュリティプロファイルからのエリアのアクセス権

保護されたオブジェクトの作成時に作成ユーザが有効な場合、エリアのアクセス権は、そのオブジェクトを作成したユーザから取得されます。

(セキュリティ レベル：作成ユーザ)

グループからのエリアのアクセス権

このケースは保護されたオブジェクトがグループのメンバであり、継承が有効な場合にのみ適用されます。

(セキュリティ レベル：グループ)

手動で設定されたエリアのアクセス権

ユーザが特定のオブジェクトに手動でエリアのアクセス権を設定できます。

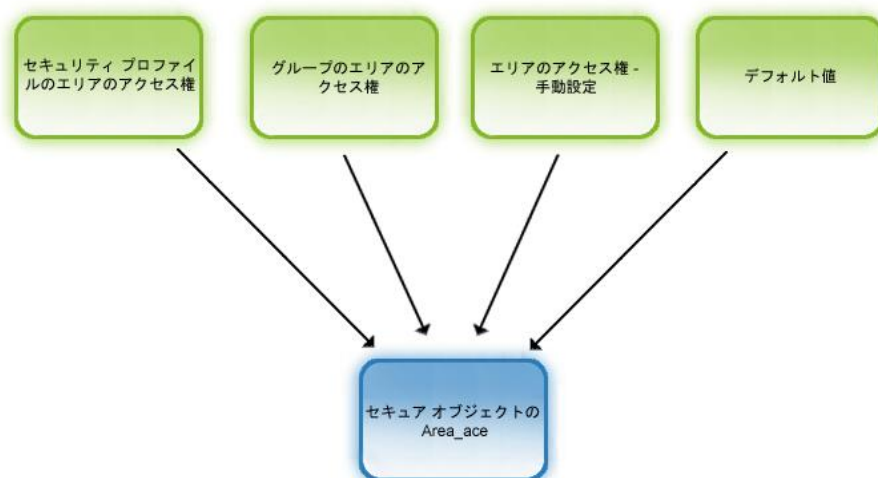
(セキュリティ レベル：オブジェクト)

デフォルトのエリアのアクセス権

保護されたオブジェクトが作成され、作成ユーザ設定されていないか、またはユーザリスト内に存在しない場合、エリアのアクセス権はグローバル設定(グローバル デフォルト アクセス権)から取得されます。

(セキュリティ レベル：グローバル設定)

以下の図に、オブジェクトのエリアのアクセス権を取得するさまざまな方法を示します。



複製

セキュリティ サブシステムでは、エンタープライズ層とドメイン層との間での複製から認可データが除外されます。アクセス権データを保持しているオブジェクトの数が多い場合は、複製に適していません。代わりに、セキュリティは、データベース間で移動されたオブジェクトに対して「リセット」されます。

つまり、複製された保護オブジェクトが作成されるとすぐに、アクセス権（オブジェクトおよびエリアのアクセス権）が再計算されます。これは、上下方向の複製に対して有効です。たとえば、エリア定義の複製は必要ありません。

■ **前提条件**

- ユーザ X がエンタープライズ レベルでクエリを作成します。
- ユーザ X は、エリア 1 および 2 にのみアクセスできます。
- また、ユーザ X はドメイン層で認識されており、エリア 5 にのみアクセスできます。

■ **アクション**

クエリが下方向に複製されます。

■ **事後条件**

- ドメイン層でクエリが作成されます。
- エリアのアクセス権は、作成ユーザ（この場合はユーザ X）が定義したとおりに設定されます。
- エリア 1 および 2 のエリアのアクセス権がないため、ドメイン層のユーザ X に対してはクエリが表示されません。

制限事項

- **Software Delivery** タスクは保護されていないため（オブジェクトおよびエリアのアクセス権も）、すべての管理者が、常に、コントロール パネルでこれらのタスクを確認できます。ただし、タスク リストは読み取り専用です。
- **Software Delivery** アプリケーション オブジェクトのアクセス権は、ターゲットオブジェクトから取得されます。
- エリア数は 32 に制限されています。

セキュリティシナリオ - Software Delivery

以下に、セキュリティの概念をより理解するためのシナリオを示します。

シナリオ

あるユーザにソフトウェアの作成を許可し、特定のコンピュータ グループに対してこのソフトウェアを編集および配布するための全権限を持たせるとします。同時に、ほかのユーザに対してこれらのアクセス権を拒否します。

複数のユーザ グループを作成して、独立した副管理者のグループを作成できます。

[セキュリティ プロファイル] ダイアログ ボックスを開きます。「全員」および「所有者/作成者」グループを変更しないでください。より全体的な権限を持つユーザに対して、「管理者」グループを予約できます。したがって、このシナリオの場合、新しいセキュリティ プロファイルをいくつか定義する必要があります。

上のシナリオを実施するには、以下の手順に従います。

1. 使用が制限された、新しいセキュリティ プロファイル **USER1**（ユーザ アカウント）を作成します。
2. 管理者グループを使用して、このプロファイルに以下の表に示すクラスのアクセス権を設定します。

オブジェクト クラス	クラスのアクセス権	コメント
ソフトウェア パッケージ	特殊アクセス (C)	ソフトウェア パッケージを作成します。ソフトウェア パッケージの作成者がその所有者になるため、これ以外の権限は必要ありません。
プロシージャ	特殊アクセス (C)	プロシージャを作成します。
ソフトウェア ジョブ	特殊アクセス (C)	ターゲット コンピュータでソフトウェア ジョブを作成します。

オブジェクト クラス	クラスのアクセス権	コメント
ソフトウェア パッケージ	特殊アクセス (C)	ソフトウェア パッケージを作成します。ソフトウェア パッケージの作成者がその所有者になるため、これ以外の権限は必要ありません。
ソフトウェア ジョブ コンテナ	特殊アクセス (CVRW)	ジョブ コンテナを作成、書き込み、および表示します。これは、[ジョブ] - [ソフトウェア ジョブ] - [すべてのソフトウェア ジョブ] フォルダの下にあります。
ジョブ コンテナの優先アクセス	アクセスなし	ジョブ コンテナ優先度の変更を制限します。 注: 高い優先度のジョブ コンテナは、優先度の低いジョブ コンテナの実行を遅らせるためにタスク マネージャに影響を与えます。
その他のすべてのオブジェクト クラス	アクセスなし	ユーザがほかのオブジェクトにアクセスできないように制限します。

- ソフトウェアを配布するアセット グループに移動し、以下のようにこのプロファイルにグループ アクセス権を設定します。

- オブジェクト アクセス : 管理 (VRX)
- メンバ アクセス : 管理 (VRX)

注: この特定のアセット グループは、メンバ継承アクセス権オプションを持つセキュリティ グループである必要があります。

- [オブジェクトのアクセス権] ダイアログ ボックスで、ドメイン (ノード)、コンピュータおよびユーザ、およびソフトウェア パッケージ ライブラリの各オブジェクトに対して、読み取り (VR) アクセス権を設定します。

このユーザが作成したジョブは、このユーザに対して表示されます。

同様の別のセキュリティ プロファイル **USER2** を設定します。 **USER2** は、 **USER1** のコンピュータ、ソフトウェア グループ、およびジョブにはアクセスできません。その逆も同様です。

USER1 が [特殊] 内のコンピュータ上のインストールを見た場合、注文されたインストールが表示されます。また、これらのコンピュータにインストールされている **Software Delivery** ソフトウェアは、ここでは **USER1** には表示されますが、それ以外の場所では表示されません。

共通セキュリティの設定

セキュリティの設定は、 **CA Client Automation** システムにゲートウェイを提供するため、インストール後に実行する不可欠なステップの 1 つです。組織にふさわしいセキュリティ モデルを決定し、それに応じてセキュリティ システムを設定することができます。セキュリティ モデルの決定は、以下の要因に基づいて実行できます。

- システムへのアクセス権が必要な個別のユーザおよびグループ（ローカルおよびドメインの両方）
- 各ユーザおよびグループによって必要とされる読み取り、書き込み、実行などのアクセス権のタイプ
- クラス、グループ、オブジェクト、またはエリア レベルのアクセス権などによって必要とされるアクセス権のレベル。

注: ユーザアカウントにマップされているプロファイルとグループにマップされているプロファイルの 2 つのプロファイルがユーザにある場合、その結果付与される権限は、両方のプロファイルを統合した権限です。また、ユーザがセキュリティ プロファイルとして定義される複数のグループのメンバである場合にも、このルールは有効です。

デフォルトでは、管理者グループのメンバには、完全なアクセス権のフル コントロールが付与されます。このため、 **CA Client Automation** のインストールが完了すると、管理者グループのメンバは、 **DSM** ドメインにログインして追加ユーザを作成し、アクセス権を付与することができます。

セキュリティの設定方法

セキュリティで制御されたシステムへのアクセス権の設定には、以下のタスクが含まれています。これらのタスクを理解すると、強力で効果的なセキュリティシステムを設定する場合に役立ちます。

- セキュリティ プロファイルをシステムに追加します。事前定義済みプロファイルがデフォルトでセキュリティ システムに追加され、削除することができません。
- [クラスのアクセス権] ダイアログ ボックスにリストされるオブジェクト クラスに対するクラスのアクセス権を指定します。

アクセス権をセキュリティ プロファイル、セキュリティ エリア、およびクラスのアクセス権のオブジェクト クラスに変更できないようプロファイルを制限するようにしてください。プロファイルを開き、これらの 3 つのオブジェクト クラスに対して、クラスのアクセス権のアクセス タイプをアクセス権なしに設定します。

ただし、セキュリティ システムのより詳細な設定を行うために、以下の処理を実行できます。

- 各フォルダのグループまたはオブジェクトにアクセス権を設定するか、またはオブジェクトをエクスプローラに表示させます。
- [特殊アクセス] を使用して、表示、読み取り、書き込み、削除、実行、アクセス権の変更、および所有権の取得のアクセス権限を組み合わせで選択します。

ドメイン マネージャ上で有効なアカウントを持つオペレーティング システムのユーザは、システムに接続できるようになります。つまり、ユーザは管理者である必要がなくなります。システムの機能へのアクセスは、内部セキュリティ メカニズムによって制御されています。デフォルトでは、管理者および所有者に完全なアクセス権があり、そのほかのユーザにはアクセス権なしが設定されています。ただし、インストール後に権限を更新することによって、アクセス権を変更できます。

注: エンタープライズ マネージャに接続している場合は、ダウストリーム ドメイン マネージャのセキュリティ機能にアクセスするために、十分なユーザ権限（またはユーザ グループ権限）があるアカウントを持っていることを確認してください。ドメイン マネージャに接続している場合、エンタープライズ マネージャのセキュリティ機能にアクセスするために、十分な権限があるアカウントを持っていることを確認してください。

セキュリティプロファイルの追加

セキュリティプロファイルの作成は、新しいセキュリティプロファイルを現在のセキュリティプロバイダによって提供されるユーザアカウントまたはグループのいずれかにマップすることを意味します。システムにアクセスするユーザまたはグループを選択して、セキュリティプロファイルに追加することができます。

セキュリティプロファイルを追加するには、以下の手順に従います。

1. [セキュリティ]メニューから[セキュリティプロファイル]を選択します。

[セキュリティプロファイル] ダイアログボックスが表示されます。

注: このダイアログボックスを開くには、十分なアクセス権が必要です。権限がない場合には、セキュリティエラーメッセージが表示されます。管理者には、デフォルトでこれらのアクセス権があります。

2. [追加] をクリックします。

[セキュリティプロファイルの追加] ダイアログボックスが表示されます。

3. セキュリティ権限を[使用可能なディレクトリ] ツリーから選択し、必要なセキュリティプリンシパルを参照してクリックします。

選択されたセキュリティ権限およびプリンシパルが、[コンテナ識別子] および[名前] の各フィールドに表示されます。

4. ツリー内のプリンシパルをダブルクリックするか、または[リストへの追加] をクリックします。

[名前] フィールドに表示されたセキュリティプリンシパルが、セキュリティプロファイルのリストに追加されます。

プロファイルをさらに追加するには、[セキュリティプロファイルの追加] ダイアログボックスで最後の 2 ステップを繰り返します。

5. [OK] をクリックします。

選択されたユーザアカウントまたはグループがセキュリティプロファイルにマップされ、[クラスのアクセス権] ダイアログボックスが表示されます。

注: 1 つ以上のセキュリティプリンシパルを追加した場合、[クラスのアクセス権] ダイアログボックスは表示されません。[セキュリティプロファイル] ダイアログボックスでプロファイルを選択し、[クラスのアクセス権] をクリックする必要があります。

6. [クラスのアクセス権] ダイアログボックスでは、権限を割り当てるオブジェクトクラスを選択します。

注: 複数のオブジェクトクラスを選択して、それらすべてにクラスのアクセス権を指定することもできます。連続して選択するには、Shift キーを押してからオブジェクトをクリックします。任意に選択するには、Ctrl キーを押してからオブジェクトをクリックします。

7. [クラス アクセス] ドロップダウン リストから権限を選択して、[OK] をクリックします。

指定された権限が新しいセキュリティ プロファイルに割り当てられます。

[セキュリティ プロファイルの追加] ダイアログ ボックスには、次の利用可能なセキュリティ権限のリストが表示されます。**Windows NT** ドメイン、**UNIX** 認証ターゲット、**NDS** や **LDAP** などの外部ディレクトリ、および **X.509** 証明書サブシステム。

利用可能なセキュリティ権限のリストは、マネージャに保存されています。**Windows NT** ドメイン環境で実行中の場合、マネージャ ノードでは、利用可能なすべての明示的なドメインへの信頼が自動的に検証されます。利用可能なセキュリティ権限のリストが [セキュリティ プロファイルの追加] ダイアログ ボックスによって要求されると、これらの信頼が返され、表示されます。

セキュリティ プロファイルの作成時に、暗黙的に信頼されたドメイン、つまり、直接検証されたリストにないドメインを使用する場合があります。このようなドメインの使用を有効にするために、[セキュリティ プロファイル] ダイアログ ボックスによって、権限の追加および削除を実行できます。ただし、このことは **Windows NT** ネームスペース (**winnt**) 内でのみ可能です。

暗黙的に信頼されたドメインを追加するには、[追加] をクリックして新しく表示されたダイアログ ボックスにドメイン名を入力します。[OK] をクリックすると、ドメインが利用可能な権限のリストに追加されます。暗黙的に信頼されたドメインを削除するには、削除するドメインを強調表示して [削除] をクリックします。

ドメインを権限のリストに追加しても、そのドメインに信頼を付与したことにはなりません。信頼の付与は、オペレーティング システムによって実行されます。ドメインをこのリストに追加して、マネージャがこのドメインを信頼するようにするには、基本オペレーティング システムでこのドメインがすでに信頼されている必要があります。

定義済みのアクセス タイプ

アクセス タイプは、オブジェクトまたはフォルダにアクセスするための権限を示します。アクセス タイプの値は以下のいずれかです。

表示

表示権限 (V)

読み取り

表示および読み取り権限 (VR)

マネジメント

表示、読み取り、および実行権限 (VRX)

変更

表示、読み取り、書き込み、実行、および削除権限 (VRWXD)

フル コントロール

権限の作成、表示、読み取り、書き込み、実行、削除、変更、および所有権の取得権限 (CVRWXDPO)

特殊アクセス

権限の別の組み合わせを付与する必要がある場合は、[特殊アクセス] を選択します。すべての権限が表示された [特殊アクセス] ダイアログ ボックスが表示されます。

アクセスなし

ユーザがオブジェクト クラス内のオブジェクトにアクセスできないようにします。

注: グループ「所有者/作成者」にはこの値を割り当てないでください。アプリケーションにまったくアクセスできなくなることがあります。

以下の例に、**Computer** オブジェクト クラスに対する各種アクセス権の効果を示します。

クラス アクセス	権限の効果
表示	[すべてのコンピュータ] フォルダの下すべてのコンピュータを表示します。
読み取り	コンピュータのプロパティを表示することができます。

クラス アクセス	権限の効果
マネジメント	コンピュータ にソフトウェア パッケージを展開する、またはコンピュータでジョブを実行することができます。
変更	新しいコンピュータを追加するか、またはコンピュータを削除することができます。
フル コントロール	コンピュータを完全制御することができます。

クラスのアクセス権を指定します。

セキュリティ プロファイルに割り当てられているクラスのアクセス権を変更することができます。

クラスのアクセス権の指定方法

1. [セキュリティ] メニューで [セキュリティ プロファイル] を選択します。
[セキュリティ プロファイル] ダイアログ ボックスが表示されます。
2. クラスのアクセス権を変更するセキュリティ プロファイルを選択し、[クラスのアクセス権] をクリックします。
[クラスのアクセス権] ダイアログ ボックスが表示されます。
3. 権限を割り当てるオブジェクト クラスを選択します。

注: 複数のオブジェクト クラスを選択して、それらすべてにクラスのアクセス権を指定することもできます。連続して選択するには、**Shift** キーを押してからオブジェクトをクリックします。任意に選択するには、**Ctrl** キーを押してからオブジェクトをクリックします。

4. [クラス アクセス] フィールドでクラスのアクセス権を選択し、[OK] をクリックします。

これにより、選択したセキュリティ プロファイルのメンバが、指定された範囲でオブジェクト クラスにアクセスできるようになります。

権限の異なる組み合わせを指定するには、オブジェクト アクセス権のドロップダウン リストから [特殊アクセス] を選択します。

オブジェクトのアクセス権を指定します。

たとえば、コンピュータ、ユーザ、ジョブなどのオブジェクトごとにオブジェクトのアクセス権を指定できます。デフォルトでは、オブジェクトはそのオブジェクトクラスからクラスのアクセス権を継承します。

注: オブジェクトのアクセス権は、クラスおよびグループのアクセス権よりも優先されます。

オブジェクトのアクセス権を指定するには、以下の手順に従います。

1. オブジェクトを選択し、以下のいずれかを実行します。
 - [セキュリティ] メニューから [アクセス権] を選択します。
 - オブジェクトを右クリックし、コンテキストメニューから [アクセス権] を選択します。

[オブジェクトのアクセス権] ダイアログ ボックスが表示されます。

注: 複数のオブジェクトクラスを選択して、それらすべてにクラスのアクセス権を指定することもできます。連続して選択するには、**Shift** キーを押してからオブジェクトをクリックします。任意に選択するには、**Ctrl** キーを押してからオブジェクトをクリックします。

2. [オブジェクト アクセス] ドロップダウン リストから必要なアクセス タイプを選択して、[OK] をクリックします。

プロファイルのメンバは、付与された権限を使用してオブジェクトにアクセスできます。

権限の異なる組み合わせを指定するには、オブジェクト アクセス権のドロップダウン リストから [特殊アクセス] を選択します。

グループのアクセス権を指定します。

任意のユーザ作成フォルダにグループのアクセス権を指定できます。

注: 優先順位は、オブジェクトのアクセス権、グループのアクセス権、クラスのアクセス権となります。これは、クラスのアクセス権を設定しても、個別に指定されたオブジェクトやグループ メンバのアクセス権が置き換えられないことを意味します。

グループのアクセス権を指定するには、以下の手順に従います。

1. フォルダを選択し、以下のいずれかを実行します。
 - [セキュリティ] メニューから [アクセス権] を選択します。
 - グループを右クリックし、コンテキスト メニューから [アクセス権] を選択します。

[セキュリティ グループのアクセス権] ダイアログ ボックスが表示されます。このダイアログ ボックスで、グループ レベルのアクセス権を設定できます。
2. プロファイルを選択し、オブジェクト アクセスおよびメンバ アクセスを指定します。

注: [デフォルト] を選択すると、メンバのアクセス権をクラスのアクセス権で上書きします。

これにより、プロファイルのメンバが、指定された範囲でフォルダまたはグループにアクセスできるようになります。

権限の異なる組み合わせを指定するには、オブジェクト アクセス権のドロップダウン リストから [特殊アクセス] を選択します。

累積アクセス権

以下で説明されているように、マップされているセキュリティ プロファイルに対するアクセス権は常に累積的です。

- ユーザが複数のセキュリティ グループのメンバになっている場合、各グループの権限が **OR** によりめとめられて、そのユーザのアクセス権限が決定されます。

たとえば、あるユーザが 2 つのグループのメンバになっており、それらのグループの内の一方がオブジェクトに対して書き込みアクセス権を持ち、もう一方が読み取りアクセス権を持っている場合、そのユーザは書き込みアクセス権を持ちます。
- オブジェクト レベルのアクセス権は、グループ レベルのアクセス権よりも優先され、グループ レベルのアクセス権は、クラス レベルのアクセス権よりも優先されます。

例:

- たとえば、グループ内のコンピュータをリストするためにフォルダを展開するには、そのフォルダに対する読み取り権限が必要です。
- オブジェクトを作成するには、そのオブジェクトに対する作成権限が必要です。
作成したオブジェクトをフォルダに配置する必要がある場合は、このフォルダに対する読み取り権限および書き込み権限も必要になります。
- （たとえば、ファイルおよびフォルダを貼り付けるときの）貼り付けおよびリンク操作には、現行フォルダまたはオブジェクトに対する書き込み権限が必要です。
- 移動操作には、2つのフォルダまたはオブジェクト（ソースおよび宛先の両方）に対する書き込み権限が必要です。

セキュリティ エリアのサポート

セキュリティ エリアは、地理的、組織的、またはトポロジ上の区分です。セキュリティ エリアは、複数のセキュリティ プロファイル、および複数のオブジェクトにリンクされている可能性があります。オブジェクトにリンクされている少なくとも1つのセキュリティ エリアが、ユーザの少なくとも1つのセキュリティ プロファイルにもリンクされている場合、ユーザはオブジェクトにアクセスできます。

重要なユース ケース、およびそれらのユース ケースのコンテキストにおけるエリア サポートの具体的な内容については、[「セキュリティ エリアのサポートのユース ケース」](#) (P. 633)を参照してください。

以下のセクションでは、セキュリティ エリアの使用方法について説明します。

セキュリティ エリアのグローバル設定

グローバル設定では、セキュリティ エリアのサポートのステータス、およびシステムが作成したオブジェクトをセキュリティ エリアで表示または非表示にするかどうかが定義されます。[セキュリティ] メニューから使用可能な[セキュリティ エリア] ダイアログ ボックスで、グローバル設定を変更できます。

ドメイン マネージャ上でのセキュリティ エリアのサポートは、デフォルトではオフになっています。エリアのサポートをオンにして、セキュリティ システムにセキュリティ エリア機能を実装する必要があります。ただし、このオプションをオンにしなくても、エリアを作成し、プロファイルおよびオブジェクトにリンクできます。ドメイン マネージャでセキュリティ エリアのサポートを有効にするには、[セキュリティ エリアのサポート] フィールドで[オン] オプション ボタンを選択します。

デフォルトでは、セキュリティ エリアはシステムで作成されたオブジェクトを表示するように設定されています。特定のセキュリティ エリアでシステムによって作成されたオブジェクトを非表示にする場合は、[セキュリティ エリア] ダイアログ ボックスでセキュリティ エリア名の横にあるチェック ボックスをオフにします。

セキュリティ プロファイルのセキュリティ エリア設定の有効化

セキュリティ エリアのサポートをそれぞれ適したセキュリティ プロファイルに対して有効にし、この機能をセキュリティ プロファイル レベルで実装する必要があります。

セキュリティ プロファイルのセキュリティ エリア設定を有効にするには

1. [セキュリティ] メニューから[セキュリティ プロファイル]を選択します。
[セキュリティ プロファイル] ダイアログ ボックスが表示されます。
2. セキュリティ エリア設定を有効にするセキュリティ プロファイルを選択して、[セキュリティ エリア] をクリックします。
[セキュリティ エリアの関連] ダイアログ ボックスが表示されます。
3. [このプロファイルのセキュリティ エリア サポートを有効化] チェック ボックスをオンにします。

このチェック ボックスの横のアイコンが緑色のチェックマークになり、セキュリティ エリアのサポートがオンになったことを示します。

セキュリティエリアの作成

地理的、トポロジ上、組織的な区分のエリア、または選択したそのほかのタイプのエリア管理を作成できます。

セキュリティエリアを作成するには

1. [セキュリティ] メニューから [セキュリティ エリア] を選択します。
[セキュリティ エリア] ダイアログ ボックスが表示されます。
2. [追加] をクリックします。
[新しいセキュリティ エリア] ダイアログ ボックスが表示されます。
3. 新しいエリアの名前と説明を入力して、[OK] をクリックします。

新しいエリアが [セキュリティ エリア] ダイアログ ボックスのセキュリティ エリアのリストに追加されます。[セキュリティ プロファイルの関連] ダイアログ ボックスが表示され、ここでセキュリティ プロファイルを新しいエリアにリンクできます。

セキュリティエリアの削除

セキュリティ エリアが不要になった場合には、そのエリアを削除できます。削除されたセキュリティ エリアはシステムから除去され、リンクされたすべてのプロファイルおよびオブジェクトから自動的にリンク解除されます。

セキュリティエリアを削除するには

1. [セキュリティ] メニューから [セキュリティ エリア] を選択します。
[セキュリティ エリア] ダイアログ ボックスが表示されます。
2. [削除] をクリックします。
確認メッセージが表示されます。
3. [はい] をクリックします。
セキュリティ エリアが削除されます。

セキュリティ プロファイルへのセキュリティ エリアのリンクまたはリンク解除

セキュリティ プロファイルをセキュリティ エリアにリンクすると、ユーザまたはグループがセキュリティ エリアにリンクされたオブジェクトにのみアクセスできるように制限できます。セキュリティ プロファイルは、1 つ以上の適切なセキュリティ エリアにリンクできます。複数のエリアの場合、ユーザは、ユーザが属しているすべてのセキュリティ エリアにリンクされているオブジェクトにアクセスできます。

ユーザがセキュリティ エリアに属さなくなった場合、そのエリアをリンク解除できます。

セキュリティ エリアをリンクまたはリンク解除するには

1. [セキュリティ] メニューで、[セキュリティ プロファイル] を選択します。
[セキュリティ プロファイル] ダイアログ ボックスが表示されます。
2. セキュリティ プロファイルを選択して、[セキュリティ エリア] をクリックします。
[セキュリティ エリアの関連] ダイアログ ボックスが表示され、選択したプロファイルの関連エリアがリストされます。
3. セキュリティ エリアを選択して、[リンク] または [リンク解除] をクリックします。
選択したセキュリティ プロファイルが、セキュリティ エリアにリンクまたはリンク解除されます。

セキュリティ エリアの保護されたオブジェクトへのリンクまたはリンク解除

保護されたオブジェクトをセキュリティ エリアにリンクすると、そのエリアに属するユーザのみがオブジェクトにアクセスできます。保護されたオブジェクトは、1 つ以上の適切なエリアにリンクできます。複数のエリアの場合、オブジェクトが属するすべてのセキュリティ エリアにリンクされているユーザが、そのオブジェクトにアクセスできます。

注: オブジェクトをグループにリンクまたはリンク解除する場合、そのオブジェクトのエリアのアクセス権が定義されているかどうかにかかわらず、オブジェクトによって自動的にグループのエリアのアクセス権が継承されます。オブジェクト レベルのエリアのアクセス権を保持する場合は、オブジェクトのリンクまたはリンク解除を実行した後で、エリアのアクセス権を確認および変更する必要があります。

セキュリティ エリアをリンクまたはリンク解除するには

1. エクスプローラでオブジェクトを選択して右クリックします。
コンテキストメニューが表示されます。
2. アクセス権を選択します。
[オブジェクトのアクセス権] ダイアログ ボックスが表示されます。
3. [セキュリティ エリア] をクリックします。
[セキュリティ エリアの関連] ダイアログ ボックスが表示され、選択したオブジェクトの関連エリアがリストされます。
4. セキュリティ エリアを選択して、[リンク] または [リンク解除] をクリックします。
選択した保護されたオブジェクトが、セキュリティ エリアにリンクまたはリンク解除されます。

暗号化の設定

Client Automation では、より強力な暗号化アルゴリズム、特に、セッション メッセージサブシステム、および直接関連のあるコンポーネント内の **Advanced Encryption Standard (AES)** がサポートされています。

暗号化ポリシーを使用して、ほかのパートナーとの通信で使用する暗号化アルゴリズムを設定できます。この設定は、セッション メッセージ、**Software Delivery** の保存および転送、**Remote Control** ビューア/ホスト間通信、**DTS** エージェント、および **NOS** なしファイル転送用 **Software Delivery** サーバを使用した通信で有効です。

利用可能な暗号化アルゴリズム、通信に最も適切なアルゴリズムの選択、および r11.2 以前のパートナーとの通信については、以下のセクションを参照してください。

- [通信用暗号化アルゴリズム](#) (P. 486)
- [一致する暗号化アルゴリズムの選択方法](#) (P. 487)
- [トップ シークレット環境での暗号化](#) (P. 488)
- [古いバージョンとの通信](#) (P. 488)

通信用暗号化アルゴリズム

通信に使用される暗号化アルゴリズムおよびその推奨されるオーダは、暗号の環境設定リストである暗号化ポリシーで定義されています。

通信の確立時に両方の通信パートナーの定義されたアルゴリズムが考慮され、最適なアルゴリズムの組み合わせが後続のセッションで選択されます。通信セッションを確立するには、両方の通信パートナーによって、共通のアルゴリズムが少なくとも 1 つ共有されている必要があります。

以下のリストに、利用できる暗号化アルゴリズムを強度の昇順で示します（つまり、AES-256 が最も強いアルゴリズムです）。

Triple-DES (Data Encryption Standard)

キー長が 168 ビットの Data Encryption Standard に従って、対称キーを示します。

AES-128 (Advanced Encryption Standard)

キー長が 128 ビットの Advanced Encryption Standard に従って、対称キーを示します。

AES-192

キー長が 192 ビットの Advanced Encryption Standard に従って、対称キーを示します。

AES-256

キー長が 256 ビットの Advanced Encryption Standard に従って、対称キーを示します。

一致する暗号化アルゴリズムの選択

各通信パートナーには暗号化ポリシーで定義された優先される暗号のリストがあり、リストの先頭に最優先の暗号が記されています。両方の通信パートナーのリストは以下のルールに従って比較され評価されます。

- 各リストについて、暗号が最初から最後まで参照され、もう一方のリストで一致する暗号について、一致が見つかるか、またはリストの最後に達するまで検索されます。
- 一致する暗号が 2 つある場合、より強力な暗号が以降のセッションで使用されます。
- 一致する暗号が 1 つの場合、この暗号が以降のセッションで使用されます。
- 一致する暗号が見つからない場合は、通信できません。

例:

パートナー A の暗号リストには、Triple-DES、AES-192、AES-128 が含まれます。パートナー B の暗号リストには、AES-256、AES-128、Triple-DES、AES-192 が含まれます。

システムは以下の手順を実行して、一致する暗号を識別します。

1. パートナー A の暗号リストを参照します。
最初のエン트리 (Triple-DES) がパートナー B のリストで検索されます。
一致が見つかります。Triple-DES が最初の一致する暗号です。
2. パートナー B の暗号リストを参照します。
最初のエン트리 (AES-256) がパートナー A のリストで検索されます。
一致は見つかりません。
2 番目のエン트리 (AES-128) がパートナー A のリストで検索されます。
一致が見つかります。AES-128 が 2 番目の一致する暗号です。
3. システムは AES-128 を Triple DES より強力であると見なし、このアルゴリズムを以降のセッションで使用します。

注: 最初の 2 つの一致のみが考慮されます。2 つの暗号リストでは、これ以上の検索と比較のアクションは実行されません。

トップ シークレット環境での暗号化

トップ シークレット環境で暗号化が必要な顧客は、最初にマネージャをインストールして、リストに **AES-256** のみを持つように暗号設定のポリシーを変更し、プロパティ **DSM/common components/encryption/compatibility/pre_11_2** を「False」に設定することをお勧めします。

マネージャ システムのエージェントでこの設定変更が行われた（つまり、設定ジョブが完了した）後、追加のスケラビリティ サーバを安全にインストールできるようになります。

スケラビリティ サーバ レベルで、以下のコマンドを入力して暗号リストが送られているかどうかを確認します。

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences  
-pncipher0
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences  
-pncipher1
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences  
-pncipher2
```

```
ccnfcmda -cmd GetParameterValue -psitrm/common/encryption/cipherpreferences  
-pncipher3
```

暗号 0 には **AES-256** が含まれており、その他の暗号は空である必要があります。暗号設定がすでに着信したかどうかを確認するために、このことはマネージャ レベルまたはエージェント レベルで行うことができます。

これで、そのサーバを示すエージェントを安全にインストールできるようになります。エージェントは、通信用に **AES-256** 暗号化を使用します。

共通設定がエージェントに送られると、エージェントは暗号リストに **AES-256** のみを持つことになるため、その他の暗号による通信は失敗します。

古いバージョンとの通信(互換性ポリシー)

pre-r11.2 パートナと通信を行う場合は、**pre_11_2** 互換性ポリシーが **True** に設定されている必要があります。

デフォルトの環境設定では、このポリシーの値は設定済みです。

環境全体で **r11.2** 以前のインストールが残っていない場合は、**pre_11_2** 互換性ポリシーを **False** に設定して、セッションの確立を改善する必要があります。

FIPS 準拠の暗号方式

Client Automation は、「FIPS 推奨」および「FIPS のみ」の 2 つのモードの、FIPS に準拠する暗号化をサポートしています。FIPS のみモードに切り替えることができるのは、インフラストラクチャ内のすべてのコンポーネントが FIPS- 推奨モードでアップグレードされたか、動作している場合のみです。必要ならば、再度 FIPS 推奨モードに切り替えることができます。

関連項目：

[FIPS 140-2 のサポート](#) (P. 90)

FIPS モードを切り替える前に

Client Automation インフラストラクチャの FIPS モードを切り替える前に、特定の FIPS モードでの稼働に関する実際の考慮事項を理解する必要があります。このセクションでは、FIPS モードを切り替える前に確認する必要がある考慮事項および前提条件を一覧します。

混合 FIPS モード

ユーザの Client Automation インフラストラクチャが混合 FIPS モード、つまり、一部は FIPS 推奨モードで、他は FIPS のみモードで実行されている場合、以下の制限事項が適用されます。

- 以下のコンポーネントが通信する場合、OSIM 機能の一部が正常に機能しない場合があります。
 - FIPS 推奨ドメイン マネージャから FIPS のみのスケーラビリティ サーバへ
 - FIPS 推奨エンタープライズ マネージャから FIPS のみのドメイン マネージャへ
- 以下のコンポーネント間の通信は失敗します。
 - Client Automation r12 コンポーネントから FIPS のみの DSM コンポーネントへ

ドメイン マネージャをエンタープライズ マネージャにリンクするときには、以下のことを考慮してください。

- FIPS のみモードのエンタープライズ マネージャにリンクできるのは、FIPS のみモードのドメイン マネージャだけです。
- ドメイン マネージャまたはエンタープライズ マネージャの FIPS モードが [FIPS 推奨 (FIPS のみモード準備済み)] または [FIPS-Preferred (Rerun conversion for FIPS-Only)] の場合は、リンク操作を実行できません。
- エンタープライズ マネージャが FIPS 推奨モードの場合は、FIPS 推奨モードまたはレガシーのドメイン マネージャをリンクできます。

FIPS 推奨モードから FIPS のみモードへ

FIPS 推奨から FIPS のみへモードを切り替えた後の、以下の機能の動作はサポートされていません。

- DTS 用の PLAIN および CACRYPT 暗号化フィルタ
- 信頼された転送および DTS ドメインの ADT 機能
- FIPS のみとレガシーの両方のモードで動作するコンピュータ グループへの、マルチキャストまたはブロードキャストを使用した DTS 転送
- パスワード暗号化 DNA ファイルの作成またはオープン
- まだアップグレードされていないレガシー OS およびブート イメージの使用。イメージのアップグレードの詳細については、「OS インストール管理 管理者ガイド」を参照してください。

前提条件

FIPS モードを切り替える前に、以下を実行したことを確認する必要があります。

- クラスタをアップグレードしている場合は、アップグレード前にクラスタのすべてのノード上に **Client Automation** の自動起動を無効にします。クラスタ内のノードがすべてアップグレードされた場合、サービスを有効にすることができます。
- 変換ユーティリティを実行している場合、**DSM** エクスプローラ（ローカルおよびリモート）、**Web** コンソールおよび **CLI** のセッションのインスタンスをすべて閉じます。変換ユーティリティの実行が完了するまで、これらの新規インスタンスを開かないでください。
- エンタープライズ マネージャとドメイン マネージャ上の設定ポリシーがすべて封印されていることを確認します。

FIPS のみモードに切り替える方法

Client Automation インフラストラクチャを FIPS のみモードに切り替えることで、単に FIPS 準拠の暗号化を使用できます。FIPS のみモードに切り替えた後、コンポーネントは r12 のコンポーネントと通信できません。

注: FIPS 準拠の暗号化のみを使用する準備ができるまで、FIPS 推奨モードを使用することをお勧めします。

以下のプロセスでは、Client Automation インフラストラクチャを FIPS のみモードに切り替える手順について説明します。

注: エンタープライズ マネージャに関連する手順が適用されるのは、環境内に Client Automation エンタープライズ マネージャがある場合のみです。

1. DSM コンポーネントがすべて リリース 12.9 にアップグレードされていることを確認します。
2. すべての OS およびブート イメージを FIPS 準拠の形式に更新します。イメージ更新の詳細については、「OS インストール管理 管理者ガイド」を参照してください。
3. エンタープライズ マネージャ上で変換ユーティリティを実行します。このユーティリティはグローバル OSIM 設定ポリシーを FIPS- 準拠の形式に変換し、すべてのドメイン マネージャに管理対象の値およびパラメータの定義を配布します。
4. エンタープライズ マネージャ上のイベント ログをチェックして、ポリシーがすべてのドメイン マネージャに正常にレプリケートされたことを確認します。
5. ドメイン マネージャ上で変換ユーティリティを実行します。このユーティリティはローカル OSIM 設定ポリシーを変換し、管理対象値を Client Automation インフラストラクチャ内のすべてのコンポーネントに配布します。
6. エンタープライズ マネージャ上のデフォルトの設定ポリシーを変更して、FIPS のみモードに切り替えます。

注: カスタム設定ポリシーを使用して FIPS モードを変更することはお勧めしません。

7. エンタープライズ マネージャ上のイベント ログをチェックして、ポリシーがすべてのドメイン マネージャに正常にレプリケートされたことを確認します。
8. エンタープライズ マネージャがない場合は、ドメイン マネージャ上のデフォルトの設定ポリシーを変更して、FIPS のみモードへ切り替えます。

注: FIPS モードが有効になるように、CAF を再起動します。

FIPS 推奨モードに切り替える方法

まれに、インフラストラクチャを FIPS のみモードに切り替えた後に、Client Automation が、レガシー エージェントなどの FIPS に準拠していないコンポーネントと通信する必要がある場合があります。FIPS のみモードには後方互換性がないので、再度 FIPS- 推奨モードへ切り換える必要があります。

以下のプロセスでは、インフラストラクチャを FIPS- 優先モードに切り替える手順について説明します。

注: エンタープライズ マネージャに関連する手順が適用されるのは、環境内に Client Automation エンタープライズ マネージャがある場合のみです。

1. エンタープライズ マネージャ上のデフォルトの設定ポリシーを変更して、FIPS 推奨モードに切り替えます。

注: カスタム設定ポリシーを使用して FIPS モードを変更することはお勧めしません。

2. エンタープライズ マネージャ上のイベント ログをチェックして、ポリシーがすべてのドメイン マネージャに正常にレプリケートされたことを確認します。
3. エンタープライズ マネージャがない場合は、すべてのドメイン マネージャ上のデフォルトの設定ポリシーを変更して、FIPS 推奨モードへ切り替えます。

注: FIPS モードが有効になるように、CAF を再起動します。CAF に対して変換ユーティリティを実行するには、少なくともその前に、エンタープライズまたはドメイン マネージャ上で CAF を再起動しておく必要があります。そうしないと、変換ユーティリティが失敗します。

4. エンタープライズ マネージャ上で変換ユーティリティを実行して、グローバル OSIM パラメータを後方互換の形式に変換します。
5. エンタープライズ マネージャ上のイベント ログをチェックして、ポリシーがすべてのドメイン マネージャに正常にレプリケートされたことを確認します。
6. ドメイン マネージャ上で変換ユーティリティを実行して、ローカル OSIM パラメータを後方互換の形式に変換します。

変換ユーティリティの実行

変換ユーティリティの実行によって、必要な FIPS モードを使用するように DSM コンポーネントを設定します。このユーティリティを、以下の順番で実行します。

- エンタープライズ マネージャ（ある場合）
- ドメイン マネージャ

変換ユーティリティを実行する方法

1. マネージャ上で設定ポリシーがすべて封印されていることを確認します。
2. コマンドライン ウィンドウを開いて、`ITCM_installpath\bin` フォルダに移動します。
3. 以下のコマンドを実行します。

```
dmscript dsm_fips_conv.dms FIPS_Mode
```

FIPS_Mode

切り替える先の FIPS モードを指定します。有効な値は FIPS-Only および FIPS-Preferred です。

このユーティリティの完了後、成功または失敗を通知するメッセージが返されます。FIPS-ONLY パラメータでユーティリティを実行していれば、ユーティリティ実行の成功または失敗に応じて、ユーティリティは対応するマネージャの FIPS モードを変更します。

4. マネージャ上で DSM エクスプローラを開き、ルート ノードをクリックし、FIPS-140 のシステム ステータス ポートレットを確認します。

FIPS-140 設定は、マネージャの FIPS モードを表示します。

- ユーティリティが正常に実行された場合、この設定は FIPS 推奨 (FIPS のみモード準備済み)を表示します。この場合、設定ポリシーの変更を続行して、FIPS モードを変更できます。
- ユーティリティが失敗した場合、設定は FIPS- 推奨 (dsm_fips_conv の実行中にエラーが発生しました)を表示します。変換ユーティリティがこのマネージャ上で正常に実行されるまで、マネージャはこのモードで継続して動作します。

注: マネージャが上記の 2 つのモードのいずれかで動作している場合、r12 のクライアント (DSM Explorer、CLI など) はマネージャに接続できません。

5. ユーティリティがエラーまたは警告で完了している場合は、以下の手順を実行します。
 - a. スクリプトがエラーまたは警告で完了した場合は、`ITCM_installpath\bin` フォルダにあるログ ファイル `osimfiputil.log` を表示します。さらに、イベント ログ内により多くの情報があります。
 - b. エラーを修正し、変換ユーティリティを再度実行します。DSM コンポーネントは必要な FIPS モードを使用するように設定されます。

例: FIPS のみモード用の変換ユーティリティを実行するためのコマンド:

```
dmscript dsm_fips_conv.dms FIPS_ONLY
```

FIPS モードを変更する設定ポリシーの変更

ユーザの **Client Automation** インフラストラクチャの FIPS モードを変更するには、デフォルト設定ポリシー内の **FIPS 関連ポリシー** を変更する必要があります。これらのポリシーは、切り替える先の FIPS モード、および FIPS モードを切り替える前に実行すべきアクションを決定します。

エンタープライズ マネージャがある場合は、エンタープライズ マネージャ上で以下の手順を実行します。ポリシー変更は、この場合、すべての関連するドメイン マネージャ、スケーラビリティ サーバおよびエージェントに自動的に伝達されます。エンタープライズ マネージャがない場合は、すべてのドメイン マネージャ上で以下の手順を実行します。

注: マネージャの FIPS モードが **FIPS 推奨 (FIPS -のみモード準備済み)** である場合のみ、このタスクを実行します。

FIPS モードを変更するポリシーの変更方法

1. [コントロール パネル] - [設定ポリシー] に移動し、[デフォルトの設定ポリシー] を右クリックして、[封印解除] をクリックします。

ポリシーが封印解除され、更新の準備ができます。

注: カスタム設定ポリシーを使用して FIPS モードを変更することはお勧めしません。

2. [DSM] - [共通コンポーネント] - [セキュリティ] - [FIPS 140 設定] に移動し、以下のポリシーを変更します。

FIPS 140 設定

FIPS 準拠レベルを定義します。切り替える先の FIPS モードを指定するために、この設定を変更します。

アクションの変更

FIPS 140 設定の変更時に実行するアクションを定義します。

注: これらの設定のポリシー値の詳細については、「**DDSM** エクスプローラ ヘルプ」を参照してください。

3. マネージャ上でポリシーを封印します。ポリシーの封印の詳細については、「**DSM** エクスプローラ ヘルプ」の設定ポリシー」セクションを参照してください。

ポリシー変更はすべての関連する DSM コンポーネントに伝達されます。このプロセスは、ユーザの **Client Automation** インフラストラクチャのサイズに応じて、少し時間がかかります。

4. ポリシー変更が以下のコンポーネントに自動的に伝達されないので、以下のコンポーネントの FIPS モードを手動で変更します。

- スタンドアロン Remote Control エージェント
- エンタープライズ マネージャ上の管理対象外 DSM エージェント

注: 管理対象外エージェントとは、どのドメイン マネージャにもリンクされていないエージェントです。後で、管理対象外エージェントをドメイン マネージャにリンクすると、エージェントの FIPS モードがドメイン マネージャの FIPS モードによって無効化されます。

FIPS モードを手動で変更するには、以下のコマンドを使用します。

```
ccnfcmda -cmd setparametervalue -ps /itrm/common/security/fips140 -pn  
installmode -v FIPS_MODE
```

FIPS_MODE

FIPS モードを指定します。FIPS 推奨モードの場合は 1、FIPS のみモードの場合は 2 を指定します。

コマンドが正常に実行される場合、指定された FIPS モードはエージェント上で設定されます。

注: スタンドアロン DSM エクスプローラおよび DSM レポータは特定の設定を必要としません。これは、DSM エージェントが常にこれらの 2 つのコンポーネントのスタンドアロンインストールと共にインストールされるためです。この場合、エージェントは、マネージャからのポリシー更新を自動的に受信します。

5. まだアクションの変更ポリシーのデフォルト設定を変更していないか、
[ITCM の次の再起動時に FIPS モードを切り替える] に設定している場合は、すべての DSM コンポーネントに対して以下のコマンドを実行します。

```
caf stop  
caf start
```

caf の再起動後、マネージャは新しい FIPS モードで動作します。

6. DSM エクスプローラ、DSM レポータおよび Web コンソールのインスタンスをすべて再起動します。

GUI で更新された FIPS モードが利用可能になります。

7. エージェントとマネージャの FIPS モードが要求された FIPS モードに変更されたことを確認します。

この検証によって、切り替えが成功します。

注: 変換ユーティリティが正常に実行されなかった場合、マネージャの FIPS モードは FIPS 推奨 (dsm_fips_conv の実行中にエラーが発生しました) のままになります。

DSM コンポーネントの FIPS モードの検証

DSM マネージャ、スケーラビリティ サーバおよびエージェントの FIPS モードを表示して、切り替え操作が成功したかどうか検証できます。FIPS モードはインベントリ データとして利用できます。

DSM コンポーネントの FIPS モードの表示方法

1. DSM エクスプローラ内のルート ノードをクリックします。
[システム ステータス] ポートレットに、マネージャの FIPS モードが表示されます。
2. [コンピュータおよびユーザ] - [すべてのコンピュータ] - *Computer_Name* - [インベントリ] - [システム ステータス] に移動します。
右ペイン内の FIPS モード属性は、選択されたコンピュータの FIPS モードを表示します。

注: FIPS 固有のクエリおよびレポートを実行して、複数のエージェント コンピュータおよびマネージャの FIPS モードを表示することもできます。

関連項目:

[FIPS モードの事前定義済みクエリおよびレポート \(P. 497\)](#)

FIPS モードの事前定義済みクエリおよびレポート

以下の事前定義済みクエリおよびレポートによって、インフラストラクチャ内の DSM コンポーネントの FIPS モードを表示することもできます。

クエリ

FIPS のみモードで実行中のアセット

FIPS 推奨モードで実行中のアセット

FIPS サポートなしで実行中のアセット

レポート

FIPS モードによるすべてのコンピュータ

注: リリース 12.9 マネージャ (FIPS 推奨モードで稼働) に接続している r11.x または r12 エージェント コンピュータの FIPS モードは「なし」とレポートされます。NRI エージェントの FIPS モードは「なし」とレポートされます。

DSM Web コンポーネント用の FIPS 準拠の設定

Web コンポーネントと他の DSM コンポーネント間の通信が FIPS に準拠するようにするために、Web コンソール、ブラウザ、および Web サーバを設定する必要があります。

Client Automation Web コンソール用に FIPS 準拠を設定する方法

1. 以下のコンポーネント間の SSL を設定します。
 - a. クライアントブラウザと Client Automation Web コンソール
 - b. Client Automation Web コンソールと Client AutomationWeb サービス
2. 通信に TLS 1.0 を使用するようにブラウザを設定します。詳細については、ブラウザのドキュメントを参照してください。
3. Web サーバ上で SSL を FIPS に準拠するように設定します。詳細については、Web サーバのドキュメントを参照してください。

4. *Install_Path¥Web*

Console¥webapps¥wac¥WEB-INF¥classes¥com¥ca¥wac¥config¥WACConfig.properties ファイル内の設定を以下のように変更します。

```
AMS_URL=https://hostname/AMS/login.do
WEBSERVICE_URL=https://hostname/UDSM_R11_WebService/mod_gsoap.dll (Windows 用)
WEBSERVICE_URL=https://hostname/UDSM_R11_WebService (Linux 用)
SSL_Enabled=True
TrustStoreFileFullPath=truststorepath
TrustStorePassword=password
```

Web コンソールはすべての通信で TLS を使用するように設定されます。

5. 以下のコマンドを使用して Tomcat を再起動します。

```
caf stop tomcat
caf start tomcat
```

更新された設定が有効になるのは、tomcat が正常に再起動された後です。

r12 コンポーネントに接続している FIPS のみエージェントの修復

FIPS のみエージェントが r12 のマネージャまたはスケーラビリティ サーバに接続している場合、それらのエージェントは、FIPS モードに互換性がないため、相互に通信できません。マネージャまたはスケーラビリティ サーバをアップグレードするか、エージェントの FIPS モードを「FIPS 推奨」に変更する必要があります。

エージェントの FIPS モードを FIPS 推奨に変更する方法

1. エージェントで、以下のコマンドを実行します。

```
ccnfcmda -cmd setparametervalue -ps /itrm/common/security/fips140 -pn  
installmode -v 1
```

コマンドが正常に実行された場合、エージェント上の FIPS モードは「FIPS 推奨」に設定されます。

2. 以下のコマンドを使用して caf を再起動します。

```
caf stop  
caf start
```

caf が正常に再起動した場合、エージェントは「FIPS 推奨」モードで動作します。

FIPS ポリシーの変更が有効にならない場合のシナリオ

設定ポリシーで **FIPS 140** の設定を変更し、ポリシーをマネージャに適用した後に、**Client Automation** は、アクションの変更ポリシーで設定された値を基に、アクションを実行します。以下のシナリオでは、**FIPS** ポリシー変更は有効にならず、アクションの変更ポリシーに基づく何のアクションも実行されません。

- ポリシーがまだターゲット コンピュータに届いていない - 以下のコマンドを使用して、ターゲット コンピュータ上の設定をチェックしてください。

```
ccnfcmda -cmd getparametervalue -ps /itrm/common/security/fips140 -pn policy
```

コマンドは **0**（レガシー）、**1**（FIPS 推奨）、または **2**（FIPS のみ）を返します。コマンドが新しい FIPS モード値を返せば、**Client Automation** が再起動し、新しい値を **installmode** パラメータにコピーすると、新しいモードが有効になります。コマンドが新しい FIPS モード値を返さない場合、それはポリシーがターゲット コンピュータにまだ到着していないことを示します。

ターゲット コンピュータ上で現在の FIPS モードを取得するには、以下のコマンドを使用します。

```
ccnfcmda -cmd getparametervalue -ps /itrm/common/security/fips140 -pn installmode
```

通常、**installmode** パラメータと **policy** パラメータは同じ値を含んでいる必要があります。ただし、ポリシー適用後に **Client Automation** が再起動されない場合は、ユーザが **Client Automation** を再起動するまで、**installmode** パラメータは前のポリシー値を保持し続けます。

注: **ccnfcmda** エージェント設定コマンドの詳細については、「<command> /?」と入力してください（コマンドプロンプトで実行）。

- **FIPS** のみポリシーは、変換ユーティリティを実行しなかったか、変換ユーティリティを実行したがエラーになった **DSM** マネージャに対して適用されます。**FIPS** のみモードでは変換ユーティリティが正常に実行される必要があるため、ユーザがマネージャ上で変換ユーティリティを正常に実行するまで、ポリシーの変更は有効になりません。

変換ユーティリティがマネージャ上で実行されたかどうかを表示するには、以下のコマンドを使用します。

```
ccnfcmda -cmd getparametervalue -ps /itrm/common/security/fips140 -pn ready_for_fips_only
```

コマンドが **1** を返す場合、それはユーティリティがマネージャ上で正常に実行されていることを示します。

注: **FIPS** 推奨モードから **FIPS** のみモードへ、または **FIPS** のみモードから **FIPS** 推奨モードへの切り替えを試行している場合は、変換ユーティリティが正常に実行されている必要があります。

- 新しい FIPS モードは現在の FIPS モードと同じです。ターゲット コンピュータが新しい FIPS モードと同じ FIPS モードですでに作動している場合、変更はターゲット コンピュータ上で有効になりません。
- アクションの変更ポリシーが [準備が完了した時に、ITCM を再起動するようユーザに促す] に設定されている場合、ポリシーがターゲット コンピュータに到達すると、ユーザに **Client Automation** の再起動を求めるダイアログ ボックスが表示されます。このダイアログ ボックスが表示されない場合は、以下のコマンドを使用して、ターゲット マシン上の `restartaction` パラメータを確認します。

```
ccnfcmda -cmd getparametervalue -ps /itrm/common/security/fips140 -pn  
restartaction
```

コマンドが 2 を返さない場合、それはポリシーがターゲット コンピュータに到達していないことを示します。

重要: ターミナルサーバ上で、[準備が完了した時に、ITCM を再起動するようユーザに促す] オプションを有効にしないでください。これは、このオプションがすべてのユーザに **Client Automation** の再起動を促すためです。

第 12 章：拡張ネットワーク接続 (ENC)

このセクションには、以下のトピックが含まれています。

[拡張ネットワーク接続へようこそ](#) (P. 503)
[ENC コンポーネント](#) (P. 505)
[サポートされるプラットフォーム](#) (P. 506)
[ENC ゲートウェイ接続プロセス](#) (P. 506)
[ENC ゲートウェイ セキュリティ](#) (P. 507)
[認証](#) (P. 507)
[ENC ゲートウェイ認可ルール](#) (P. 508)
[イベントの監査](#) (P. 527)
[ENC ゲートウェイ コンポーネントのインストールおよび設定](#) (P. 527)
[ENC および SSA の設定](#) (P. 528)
[ENC クライアントを有効化する方法](#) (P. 528)
[ENC 環境における展開](#) (P. 529)
[ENC 展開シナリオ](#) (P. 530)
[インターネットプロキシのサポート](#) (P. 544)
[ENC ゲートウェイ経由で Client Automation を使用することに関する制限事項](#) (P. 545)
[encUtilCmd ユーティリティの使用](#) (P. 547)
[証明書の管理](#) (P. 548)

拡張ネットワーク接続へようこそ

CA Client Automation (Client Automation) では、DSM コンポーネントおよびサービスが以下のエンドポイント間の接続を確立できる、拡張ネットワーク接続 (ENC) 機能がサポートされています。

- パーソナルまたはネットワーク ファイアウォール内
- 異なる IP アドレス空間内

ENC では、すべてが異なるファイアウォールまたは DMZ (非武装地帯) 内で動作している異なるコンポーネント間で接続を確立できる、仮想ネットワーク環境が提供されます。これには、エンタープライズ マネージャ、ドメイン マネージャ、GUI、スケーラビリティ サーバ、およびエージェントが含まれます。

重要: ENC は、非常に限定された目的です。すでに ENC 対応のアプリケーションがインストールされている特定のエンドポイントに、権限のある、認証を受けたアプリケーションのみが接続するのに使用できます。ENC では、ほかのアプリケーションが使用できる、ファイアウォールを介した一般チャネルは提供されません。

2つのコンピュータが、間にファイアウォールがあるために接続できないような場合には、ENCによって、2つのコンピュータ間のデータを中継する第3のコンピュータ（ENC ルータ）に2つのコンピュータが接続するように調整されます。

ENC ゲートウェイでは、以下を要求することによって、ファイアウォールを通じてセキュアな接続が提供されます。

- ENC ゲートウェイの仮想ネットワークを介するすべての接続は、証明書を使用して正常に認証される必要があります。
- すべての接続が正常に認可される必要があります。認可ルールは、ポリシーによって設定され、誰が誰に接続できるか、いつ何の操作のために接続できるかが設定されます。これは、公共ネットワークまたはインターネット経由で接続する場合に特に重要です。
- 接続の試行やその他の操作は、セキュリティおよびトラブルシューティングの目的ですべて監査することができます。

ENC コンポーネント

ENC は、CA Client Automation 環境において、以下を含む特定のコンポーネントを使用します。

ENC クライアント

すべての ENC ゲートウェイ対応のコンピュータ上で実行され、アプリケーションによって確立された ENC ゲートウェイ ネットワーク上のすべての接続を調整します。ENC クライアントは、ENC ゲートウェイ サーバへの接続を維持します。

ENC ゲートウェイ サーバ

ENC ゲートウェイに対して、ENC クライアントからの接続と登録を受け入れ、それらを ENC ゲートウェイ マネージャに渡すことにより、スケーラビリティ サーバとしての機能を果たします。ENC ネットワーク内では、複数のサーバを使用できます。

ENC ゲートウェイ マネージャ

エンドポイント間のすべての接続を調整します。ENC ゲートウェイ サーバ、クライアント、およびルータのコンポーネントは、開始時に登録されるので、ENC ゲートウェイ マネージャでは、それらのすべてが把握されています。1つの ENC ネットワーク内では、ENC ゲートウェイ マネージャが1つのみ許可されます。

ENC ゲートウェイ ルータ

エンドポイント間でデータを中継します。1つの ENC ネットワーク内で複数のルータを使用できます。

安全なソケット アダプタ

アプリケーションと ENC ネットワーク間のリンクを提供します。これは、低レベルのネットワーク コールを途中で捕捉し、それらを可能な場合は直接接続に、その他の場合は、ENC 接続にリダイレクトします。

注: ENC ゲートウェイは、マネージャ、サーバ、ルータ、またはそれらを任意に組み合わせたものとして動作できる単一のプログラムです。マネージャには常にサーバが含まれています。ロールは、設定ストア (comstore) 内の `itrm/common/enc/server - MRS、SRS、および Router` の設定によって制御されます。設定の値が 1 の場合は、サーバがそのロールを引き受けます。

サポートされるプラットフォーム

ENC が現在サポートしているオペレーティング システム プラットフォームは、オンライン **Client Automation** ドキュメント セット（ブックシェルフ）の一部に含まれる「**CA Client Automation リリース ノート**」の「サポートされている動作環境」にリストされています。

ENC ゲートウェイ接続プロセス

ENC ゲートウェイ機能では、**Client Automation** がファイアウォールで保護されているコンピュータと通信できます。2つのコンピュータが、間にファイアウォールがあるために接続できないような場合には、ENC ゲートウェイによって、2つのコンピュータ間のデータを中継する第3のコンピュータに2つのコンピュータが接続するように調整されます。

ENC ゲートウェイ ネットワーク内では、2つのエンド ポイント（コンピュータ）間の接続プロセスは以下のとおりです。

- エンド ポイント 1があるポートで接続をリスンしようとします。1つが本物、もう1つが仮想である2つのポートが開かれます。本物のポートでは直接接続が行われ、仮想ポートは、ENC クライアントによって維持され、ENC ゲートウェイ接続をリスンします。
- エンド ポイント 2が接続しようとします。ソケット アダプタによって、直接接続の確立が試行されます。これに成功すると（同じネットワーク内の可能性）、ENC ゲートウェイではそれ以上何も行われません。
- 失敗すると、ソケット アダプタが ENC ゲートウェイ マネージャに接続を調整するように求めます。
- ENC ゲートウェイ マネージャが、既知の ENC ゲートウェイ ルータのリストを両方のエンド ポイントに送信します。それぞれのエンド ポイントでは、ルータに ping を行い、その結果を返します。ENC ゲートウェイ マネージャは、両方のエンド ポイントが到達できるルータを選択し、それぞれのエンド ポイントにそのルータに接続するように通知します。
- それぞれのエンド ポイントが ENC ゲートウェイ ルータに接続し、そのルータがエンド ポイント間のデータを中継します。

このプロセスは、エンド ポイントがネットワークを介してファイアウォールの外にある ENC ゲートウェイ サーバおよび ENC ゲートウェイ ルータに接続できるかどうか依存します。内部向けの接続は行われませんので、内部向けのポートを開く必要はありません。

ENC ゲートウェイ セキュリティ

ENC ゲートウェイでは、以下のセキュリティ メカニズムを用いて、安全な方法でファイアウォールを超えた通信が可能になります。

■ 認証

すべての ENC ゲートウェイ ノード（クライアント、マネージャ、サーバ、およびルータ）は、SSL（Secure Sockets Layer）が更新されたバージョンである TLS（トランスポート レイヤ セキュリティ）を使用して、手動でお互いを認証する必要があります。この認証方法では、Microsoft PKI または同等のものを使用して証明書をインストールする必要があります。

■ 認証

すべての ENC ゲートウェイは、誰がいつ誰に何をできるかを定義するルール セットを使用して設定されています。これは、以下のような形式になります。

- ノードの領域メンバシップ（NT グループに類似するが、別のネットワークを使用）
- リスン中の IP アドレス。これは、ENC ゲートウェイ接続を設立する許可を受けた IP アドレスのリストです。
- ENC ゲートウェイごとの接続や登録などの操作用のルールを、領域メンバシップや時刻に基づいて許可したり拒否したりします。
- 時間範囲

インストール当初は、ENC ゲートウェイはロックされています。認証ルールを持たないため、すべての接続を拒否します。これらのサーバは、通常はインターネットに接続されているため、この動作は適切なものです。これにより、認証ルールを保持するのに Client Automation が使用され、ドメイン マネージャが ENC ゲートウェイを実行しているコンピュータからファイアウォールによって切断される可能性があるため、問題が発生してしまうことがあります。これを回避する手順は、「展開シナリオ」で説明されています。

認証

保護された接続の両方のエンドは、それぞれのピアの証明書を検証（認証）します（相互認証）。これには、認証局の発行も含まれます。

この目的を達成するために、両者がサードパーティの認証局を信頼している必要があります。ENC では、Microsoft SCHANNEL TLS プロバイダ、およびそれに続いて WinTrust ライブラリを使用して、証明書に信用を与えています。ルート信頼と（場合によっては）中間の証明書は、証明書ストアおよび API を使用してオペレーティング システムによって提供されます。

ENC ゲートウェイ認可ルール

ENC 仮想インフラストラクチャは、認証、認可、および監査によって保護されています。認証は、業界標準の TLS プロトコルを使用して提供され、「[認証 \(P. 440\)](#)」および「[ENC ゲートウェイ 認証 \(P. 507\)](#)」で説明されています。監査コンポーネントの詳細は、「[監査イベント \(P. 527\)](#)」でも説明されています。

このセクションでは、認可の使用法と使用場所について説明し、最後にわかりやすい例を示します。

一般用語

以下は、認可ルールに関して使用される用語のリストです。この中には、業界標準用語および ENC による使用に合わせて作成されたものが含まれます。

セキュリティプリンシパル

セキュリティプリンシパルとは、認証されたオブジェクト（常に ENC 内のコンピュータ）で、ゲートウェイ サーバによってその ID が認識されています。このオブジェクトは、常に URI（Uniform Resource Identifier）によって参照されます。このオブジェクトは、保護されたオブジェクトまたは操作にアクセスするためのリクエストを行うエンティティです。ENC では、セキュリティプリンシパルは、主に個別のコンピュータですが、コンピュータの領域（グループ）または URI に対するパターン照合によって定義されたコンピュータのサブグループを介して参照することもできます。

保護されたオブジェクト

保護されたオブジェクトは、アクセス リクエストまたは操作のターゲットです。保護されたオブジェクトは、常に URI によって名付けられたコンピュータですが、アクセス ルールは、単一のコンピュータ、パターン照合されたコンピュータのセット、または領域一式に適用できます。

レルム

領域とは、認可コンポーネントが一連のコンピュータに関して使用するコンピュータの論理グループです。アウトソースされたシナリオでは、通常、領域は、組織レベルまたは組織単位レベルにあるコンピュータを表します。セキュリティプリンシパルは、URI の完全一致または URI に対するパターン照合によって領域の中にマップされます。

パターン照合

ENC は、領域メンバシップを決定するのに、パターン照合を使用できます。パターン照合では、照合のアルゴリズムを実行するために正規表現が使用されます。

ENC は、パターン照合機能に PCRE (PERL Compatible Regular Expressions、<http://www.pcre.org/> を参照) を使用します。PCRE の構文全体については、<http://perldoc.perl.org/perlre.html> を参照してください。

TACE – 時間ベース アクセス制御エントリ

TACE とは、保護されたオブジェクトに対して、特定の時間にセキュリティ プリンシパルが特定の操作 (複数の場合あり) を実行できるかどうかを定義するルールです。ルールによって、アクセスを拒否したり許可したりします。拒否タイプの TACE は、許可タイプより優先されます。照合ルールを持たない操作は、すべて黙示的に拒否されます。

重要: アクセス制御エントリのアクティブ タイムは、常に操作のターゲットのローカル タイムです。エージェントが、別のタイムゾーンにある別のエージェントに接続しようとする場合、ENC ゲートウェイ マネージャ ノードは、ターゲットエージェントの枠内で時間範囲を検証します。

TACL – 時間ベース アクセス制御リスト

TACL とは、TACE ルールのリストです。

インフラストラクチャ ノード

この用語は、ENC 仮想ネットワーク インフラストラクチャ (マネージャ、サーバ、およびルータのノードを含むが、ENC エージェント自体は含まない) を提供する ENC ノードを指します。

URI – Uniform Resource Identifier

URI とは、リソースの名前を付けたり、リソースを識別したりするのに使用される文字列です。ENC は、URI を使用してすべての認証されたオブジェクトを表します。

ENC および Uniform Resource Identifier

ENC 認可では、内部データベース用に URI (Uniform Resource Identifier) が使用されます。ENC URI の形式は以下のとおりです。

```
x509cert://[TLS-SCHANNEL]/CN=forward,OU=computers,DC=forward,DC=com
```

x509cert

ネームスペースを示します。X509cert は、URI が x.509 証明書 ID を表すことを意味します。

[TLS-SCHANNEL]

URI に組み込まれている権限を指定します。この特別な権限名は、認証が TLS SCHANNEL セキュリティ プロバイダおよび WinTrust プロバイダに委譲されることを意味します。これらのプロバイダは、ENC のために証明書の信用を管理します。

CN=forward,OU=computers,DC=forward,DC=dom

x.500 サブジェクト名が証明書内に組み込まれるように定義します。この名前の実際の形式および内容は、プロバイダごとに異なります。上の例は、Microsoft Active Directory の統合認証サービスによって作成された証明書です。異なる PKI および手動による証明書作成では、異なる命名規則が使用されます。

コンピュータの URI をプログラムで調査する場合は、encUtilCmd ユーティリティを使用します。「encUtilCmd certv」を実行すると、マシンが ENC 認証に使用する証明書 ID (クライアントとして使用するか、該当する場合はクライアントおよびサーバの両方として使用) が表示されます。

例: encutilcmd certv コマンド

```
C:\>encutilcmd certv
```

```
INFO: Current process user is a member of local administrators group.
```

```
INFO: Created and validated client side TLS context OK.
```

```
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,0=enc
```

```
INFO: Created and validated server side TLS context OK.
```

```
URI: x509cert://[TLS-SCHANNEL]/CN=mach-02,CN=encserver,0=enc
```

認可ルールの設定

ENC ゲートウェイ サービス認証ルールは、DSM 設定ポリシー エディタから設定されます。他のポリシー セクションとは異なり、基礎的な認可テーブルに直接アクセスできず、設定はカスタム ビュー ダイアログ ボックスによって提供されます。このダイアログ ボックスは、テーブル間の依存関係进行处理し、指定したルールのコミット前評価を行います。

設定ビューは、設定ダイアログ ボックス内の 5 つのタブ形式のビューによって提供されます。タブおよびその内容は、以下のとおりです。

レールム

このビューでは、ENC 領域の表示または定義、および領域に関する簡潔な注意事項を追加することができます。

名前マッピング

このビューでは、認証されたオブジェクトとそれらの領域メンバシップ間のマッピングの確認や定義をすることができます。キー フィールドは、URI としての認証 ID です。URI から領域へのマッピングは、完全に一致する必要がある、完全に指定された URI、または複数の URI に一致する正規表現として指定されている URI 経由で行うことが可能です。

時間範囲

ENC 内のすべての認可アクセス制御は、時間の制限付きにすることができます。このタブ ビューでは、個別のアクセス制御エントリが使用する時間範囲を定義できます。エントリは、時間範囲が月曜から金曜までの 1 つ以上の曜日に適用される [標準の曜日] か、独立記念日などの [特別な日付] のいずれかにすることができます。

時間範囲が有効な時間は、24 時間全体の期間に対して、「00:00 - 00:00」などの 24 時間形式による開始期間および終了期間として指定されます。時間範囲の詳細度は、30 分なので、各エントリの分の値には 00 または 30 を使用する必要があります。

アクセス制御

このタブでは、時間ベース アクセス制御エントリへアクセスできます。各エントリを使用して、アクティビティを許可または拒否する名前付きのルールを指定できます（アクセスを拒否するように作成されたルールは、アクセスを許可するルールよりも優先されます）。TACE 名は、監査エントリ内に記録され、ルールセットをテストするためのアクセスをシミュレーションする際に、ユーティリティ コマンドでも表示されます。そのため、該当する場合は、各ルールに適度に説明的な名前を使用することをお勧めします。

アクセス制御エントリは、単一のイベントを制御するか、それらを集約し、単一のルール内の複数のイベントを制御することができます。各ルールには、保護されたリソース（保護されたオブジェクト）およびアクセスするオブジェクト（セキュリティ プリンシパル）があります。

IP アドレス

このタブでは、IP アドレスのホワイトリストの表が提供されます。各エントリは、単一の IP アドレスか、パターン照合式によって指定された IP アドレス範囲のいずれかです。インフラストラクチャ マシンは、指定したアドレスを持つマシンからの接続のみを受け付けます。

イベント

ENC インフラストラクチャは、認証チェックが必要な操作と同等の一連のイベントを定義します。これらのイベントのほとんどは、どのセキュリティ プリンシパルが何を誰に対していつ行うことができるかを制御するために、TACE の中で設定できます。ほとんどの場合、認証コンポーネントがアクセス リクエストを拒否すると、物理的な接続が切断されます。名前のルックアップおよびエージェントの接続のイベントは、このルールの例外です。

ここで、イベントごとに順番に、簡単に説明します。それぞれのイベントでは、「保護されたオブジェクト」エントリによって保護されたリソースが定義され、「セキュリティ プリンシパル」エントリによってリクエストを行うリソースが定義されます。

ネットワーク接続

保護されたオブジェクト： 接続を受け取る ENC ノード。

これは、TACE ルール内部で制御されない唯一のイベントなので、操作のターゲットは黙示的になります。インフラストラクチャへのアクセスはすべて、IP アドレス ホワイト リストによって制御されます。IP アドレス ホワイト リストの中にリストされているノードまたは IP 範囲のみが ENC インフラストラクチャ ノードに接続できます。このインスタンス内の保護されたオブジェクトは、常にターゲット ENC ノードです。ホワイト リストは、現在すべての ENC インフラストラクチャ ノードに適用されます。

認証接続

保護されたオブジェクト： 接続を許可する ENC ノード。

セキュリティ プリンシパル： 接続された ENC ノードの認証 ID。

すべてのノードは、パートナー ENC ノードへのネットワーク接続を確立した後は、認証を行う必要があります。このイベントは、認証シーケンスが正常に完了すると生成されます。許可する ENC ノードは、接続するノードの認証された URI を使用して認可 API を呼び出し、操作が許可されているかを確認します。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

サーバ登録

保護されたオブジェクト：ENC ゲートウェイ マネージャ ノード。

セキュリティプリンシパル：ENC ゲートウェイ サーバ ノードの認証 ID。

ENC ゲートウェイ サーバは、認証された接続をマネージャに対して正常に確立すると、サーバとして登録されるように要求する登録メッセージを送信します。その後、ENC ゲートウェイ マネージャは、認可コンポーネントを呼び出してサーバがこのマネージャに登録できるかを確認します。これは、ENC ゲートウェイ サーバが ENC 仮想ネットワークの中に配置されないようにします。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

ルータ登録

保護されたオブジェクト：リクエストを処理している ENC ゲートウェイ サーバ。

セキュリティプリンシパル：ENC ゲートウェイ ルータ ノードの認証 ID。

ルータは、認証された接続をサーバに対して正常に確立すると、ルータとして登録されるように要求する登録メッセージも送信します。ENC ゲートウェイ サーバは、ローカル認証チェックを実行し、この操作が許可されているかどうかを確認した後、さらなる認証のために ENC ゲートウェイ マネージャにリクエストを渡します。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

マネージャ ルータ登録

保護されたオブジェクト：ENC ゲートウェイ マネージャ ノード。

セキュリティ プリンシパル：ENC ゲートウェイ ルータ ノードの認証 ID。

このイベントは、サーバがルータ登録メッセージを転送するときに生成されます。ENC ゲートウェイ マネージャは、認可コンポーネントを呼び出してルータが ENC 仮想ネットワークに加わることができるかを確認します。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

サーバクライアント登録

保護されたオブジェクト：リクエストを処理している ENC ゲートウェイ サーバ。

セキュリティ プリンシパル：ENC クライアント ノードの認証 ID。

このイベントは、ENC クライアント ノードが ENC ゲートウェイ サーバ ノードに登録すると生成されます。サーバは、ローカル認証チェックを実行し、信頼できる答えを得るために ENC ゲートウェイ マネージャに登録リクエストを渡します。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

マネージャ クライアント登録

保護されたオブジェクト：ENC ゲートウェイ マネージャ ノード。

セキュリティ プリンシパル：ENC クライアント ノードの認証 ID。

このイベントは、ENC ゲートウェイ サーバ ノードが ENC クライアント登録メッセージを ENC ゲートウェイ マネージャに転送すると生成されます。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

ホストリスン

このイベントは、現在実装されていません。このイベントは、ENC エージェントがリスニング接続を作成できるかどうかを確認するためのエージェント ローカル認証チェックです。

ホスト接続

このイベントは、現在実装されていません。このイベントは、ENC エージェントが発信接続を作成できるかどうかを確認するためのエージェント ローカル認証チェックです。

エージェント接続

保護されたオブジェクト： ターゲット ENC ノードのセキュリティ ID。

セキュリティ プリンシパル： リクエストを行う ENC クライアント ノードの認証 ID。

このイベントは、ENC エージェントが別の ENC エージェント ノードに接続しようとするたびに、ENC ゲートウェイ マネージャ ノードで生成されます。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

ルータへのエージェント接続

保護されたオブジェクト： ENC ゲートウェイ ルータ ノードのセキュリティ ID。

セキュリティ プリンシパル： リクエストを行う ENC クライアント ノードの認証 ID。

このイベントは、ENC エージェントが別の ENC エージェント ノードに仮想接続を確立するためにルータに接続しようとする、ENC ゲートウェイ ルータ ノードで生成されます。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、コンピュータのサブグループにアドレス指定するためのパターン照合式、または領域名、のいずれかにターゲットを指定できます。

名前のルックアップ

保護されたオブジェクト： ターゲット ENC ノードのセキュリティ ID。

セキュリティプリンシパル： リクエストを行う ENC クライアントノードの認証 ID。

このイベントは、ENC ノードがシンボリック ホスト名から ENC プライベート アドレスに変換するために名前のルックアップ操作を実行しようとする、ENC ゲートウェイ マネージャ ノードで生成されます。

ENC ゲートウェイ マネージャは、最初にターゲット DNS の名前を名前のルックアップ リクエストから抽出し、これを 1 つ以上のクライアント レコードに変換します（これにより、領域の内部ではなく、領域にわたって重複したホスト名が許可されます）。これらのクライアント レコードは、名前のルックアップ リクエストを許可する（か否か）を決定するために認可コンポーネントへ渡されます。クライアント レコードは、既知の DNS 名およびオブジェクトの認証された ID で構成されます。

このイベントのアクセス制御エントリは、リテラルのコンピュータ ID（認証から）、領域名、またはコンピュータのサブグループや複数の領域にアドレス指定するためのパターン照合式のいずれかにターゲットを指定できます。

管理アクセス

保護されたオブジェクト： ターゲット ENC ノードのセキュリティ ID。

セキュリティプリンシパル： リクエストを行う ENC クライアントノードの認証 ID。

このイベントは、ENC クライアント接続がターゲット ENC ゲートウェイに管理情報を要求すると生成されます。

管理情報には、承認されたノードのみにアクセスを許可するために、ENC サーバがホストするすべての ENC 仮想接続に関するデータを含めることができます。

接続シーケンス

このセクションでは、すべての **ENC** ノードが、**ENC** 仮想インフラストラクチャに参加するために実行する必要がある共通機能について説明します。共通機能は、物理接続、認証、および認可という 3 つの異なるフェーズに分けられます。

物理接続

すべてのノードは、1 番目のインスタンス内のターゲット **ENC** ノードに接続が許可されるには、IP アドレス ホワイト リストのテーブルにリストされている必要があります。**ENC** ノードに対して確立されたそれぞれの接続上で、アクセスを許可または拒否する必要があるかどうかをチェックするために、認可コンポーネントが呼び出されます。アクセスが拒否される場合は、接続が即時に切断されます。

認証

ネットワーク トランスポート接続がいったん確立されると、通信を行う両方のピアは、**TLS** プロトコルを利用してお互いを認証し合い、信頼されるサードパーティの認証局経由で認証 ID が信頼できるか、および ID が現在有効かを検証します。

認可

認証フェーズに続いて、認証 ID は「認証接続」イベント チェック ボックスのために認可コンポーネントに渡されます。このイベントの保護されたオブジェクトは、ターゲット **ENC** ノードです。個別のコンピュータを保護されたオブジェクトとして使用するか、パターン照合式経由で指定されたコンピュータ名のグループを使用するか、領域メンバシップを介してこの操作を許可する（または拒否する）アクセスルールを指定できます。

適切なカテゴリまたはメッセージが有効化されている場合は、上記のシーケンスにおける失敗はすべて、セキュリティ監査サブシステムによって監査されます。監査コンポーネントは、成功したすべての操作を記録するようにも設定できます。

各 **ENC** ノードは、それがサーバ、ルータ、またはクライアント エージェントであるかにかかわらず、すべてが接続先となるノードへの登録を実行します。**ENC** ゲートウェイ サーバ ノードのみがサーバ登録操作の実行を許可され、**ENC** ゲートウェイ ルータのみがルータ登録の実行を許可される、というように、登録タイプごとに個別のイベントが定義されます。

インフラストラクチャに応じて、イベントごとに、または保護されたオブジェクトごとに（あるいはその両方）、個別のアクセス制御エントリを作成するか、より大まかなアクセス制御を行うために領域内のイベントおよびコンピュータをグループ化することができます。

ENC 仮想接続

すべての物理 **ENC** インフラストラクチャ ノードが正常に開くようになったので、**ENC** 仮想ネットワークの動作具合を考慮します。デフォルトの状態では、接続または名前のルックアップは、それを許可する明示的なアクセス制御エントリがない限り、ネットワーク上で許可されていません。領域マッピング内にも参加したコンピュータ同士でさえも、お互いを認識したり、接続したりする権限が自動的に与えられることはありません。

ENC エージェント ノードが別の **ENC** エージェント ノードと通信しようとする場合、通常最初に行われる操作は、名前のルックアップ イベントです。ほとんどの場合、この特定の名前を使用する登録済みのマシンは 1 つのみ存在し、通常は、リクエストを行うマシンと同じ領域内に存在するので、特定の領域内のすべての **ENC** ノードが、その領域内のメンバにコンタクトしルックアップを行えるようにする包括的なアクセス制御ルールによって処理されます。滅多にない場合ですが、同じ完全修飾名を持つ 2 つ以上のマシンが存在することがあります。このような場合は、リクエストを行うオブジェクトもメンバである領域内のコンピュータのみを修飾参照できるようにし、名前のルックアップの曖昧さを排除する必要があります。この仕組みは、アクセス ルールによって明示的に許可されない限り、領域間におけるデータのリークが発生しないようにするためのものです。

認可コンポーネントが名前のルックアップ リクエストを許可すると、仮想 **ENC** ホストの IP アドレスが **ENC** クライアント ターゲットに戻されます。**ENC** クライアントは、その後、エージェント接続リクエストを **ENC** ゲートウェイ サーバ/マネージャに対して発行します。さらに、**ENC** ゲートウェイ マネージャがこのリクエストに関連する保護された ID をルックアップし、操作を実行する許可を求めて認可システムを呼び出します。

接続許可が付与されると、両方のエージェント（仮想通信回路のピア）が **ENC** ゲートウェイ ルータに接続し、接続を完了させます。さらに、この接続が認証され、ルータへのアクセス権限が要求されます。

ルール設定の例

この例では、`encUtilCmd` のコマンドラインユーティリティファイル定義を使用して認可ルールを説明しますが、これは **DSM** エクスプローラでも似ており、ルールセットはほぼ同様のものです。

以下で説明するような、`encUtilCmd` ユーティリティおよびその `'create'` コマンドを使用して、簡単なルールセットを生成することができます。このユーティリティでは、ルールを実行するためのテストスクリプトも同時に生成できます。

この例では、以下の領域が使用されます。

infrastructure

これは、すべてのインフラストラクチャノード（マネージャ、サーバ、ルータなど）を含めるのに使用される領域です。**ENC** インフラストラクチャは、**Forward, Inc.** によって管理されています。ここでの例では、領域名を目立つようにかっこで囲んでいます。すべての領域名は等しく扱われるので、かっこで囲む必要はありません。すべてのインフラストラクチャコンピュータは、`DC=forwardinc,DC=com` という共通の **RDN**（Relative Distinguished Name）を使用した証明書名を持っています。

dsm

これは、**DSM** インフラストラクチャを構成するすべてのコンピュータを保持している領域の例です。領域同士をよりはっきりと描写するために、**ENC** インフラストラクチャと **DSM** インフラストラクチャは文脈上区別されます。すべての **DSM** コンピュータは、`DC=forward-dsm,DC=com` という **RDN** を使用した証明書名を持っています。

east

これは、'east' 会社のすべてのコンピュータを保持している領域の例です。すべての **east** コンピュータは、**DC=east,DC=com** という RDN を使用した証明書を持っています。

west

これは、'west' 会社のすべてのコンピュータを保持している領域の例です。すべての **west** コンピュータは、**DC=west,DC=com** という RDN を使用した証明書を持っています。

この例では、ENC ノード（最小限の DSM エージェントでもある）が、DSM ノードとは別のスタンドアロンデバイスとして扱われています。DSM ENC 環境では、DSM 領域ノードが個別領域内のすべてのノードを認識しそれらに接続でき、領域エージェントが DSM 領域内のノードに接続できるけれども、管理対象領域のメンバは別の管理対象領域のメンバを認識することや、それらに接続することができないことが通常の要件になります。

ここでは、インフラストラクチャに通信を許可し、領域コンピュータが仮想ネットワークに接続し、それを利用できるようにもするために、認可ルールの定義を開始する必要があります。最初のインスタンスでは、領域が使用され、相互参照されるように宣言する必要があります。

以下は、認可ルールファイルの領域セクションから抜粋したものです。上記の 4 つの領域について定義しています。

```
realm
{Name "[infrastructure]" Notes "ENC infrastructure realm"}
{Name "[dsm]" Notes "The DSM infrastructure realm"}
{Name "east" Notes "East Inc. Contact is admin@east.com"}
{Name "west" Notes "West Inc. Contact is admin@west.com"}
end
```

次の手順では、証明書 URI と領域自体とのマッピングを定義します。この例では、すべてのエントリに対するパターン照合を使用します。

```
URIMapping
{URI ".*,DC=forwardinc,DC=com" Enabled "1" Type "Pattern" Realm "[infrastructure]"}
{URI ".*,DC=forward-dsm,DC=com" Enabled "1" Type "Pattern" Realm "[dsm]"}
{URI ".*,DC=east,DC=com" Enabled "1" Type "Pattern" Realm "east"}
{URI ".*,DC=west,DC=com" Enabled "1" Type "Pattern" Realm "west"}
end
```

次に、IP アドレス ホワイト リストを扱います。この例では、2 つのパブリック IPv4 サブネットが ENC インフラストラクチャにアクセスできるようにします。

```
IPAddWhiteList
{IPAddress "130¥.119¥..+" enabled "1" Type "Pattern"}
{IPAddress "141¥.202¥..+" enabled "1" Type "Pattern"}
{IPAddress "131¥.119¥..+" enabled "1" Type "Pattern"}
end
```

個別のアクセス制御エントリに進む前に、アクティブな時間範囲を最後に作成します。ここでの例のために、時間範囲はすべての曜日に対してアクティブで、1 日のうちの 24 時間すべてをカバーするものとします。

```
TimeRange
{Name "all-days" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays "sunday -
saturday"}
end
```

これで、アクセス ルールに進むために必要な基本要素がそろったので、アクセス制御エントリ自体に集中できます。この例では、わかりやすくするために、主に個別のアクセス制御エントリを使用します。実際の現場では、いくつかのルールを単一のルールに組み込んだほうがよりシンプルで効率が良くなる場合があります。

以下は、例示としての目的のみで使用される単一のアクセス制御エントリ。ここで議論されるすべてのルールは、**TimeACL** および終了タグ間で定義されるか、または設定 UI で作成される必要があります。

AC-[infrastructure]-[infrastructure] という名前のこのルールは、インフラストラクチャ領域のすべてのメンバが、インフラストラクチャ領域の他のメンバにアクセスし、それに対して認証を行えるようにするエントリを定義します。このルールは、以前に定義した 'all-days' 時間範囲を参照するので、毎日、一日中アクティブになります。

```
TimeACL
{Name "AC-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "AuthenticatedConnection"}
...
end
```

別の領域にも似たようなルールを追加する必要があります。ここでは、'[dsm]'、'east'、および 'west' です。ルールは、上記のものと同一ですが、セキュリティプリンシパルは以下のような別の領域のものに変更されています。

```
{Name "AC-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "[infrastructure]"
Events "AuthenticatedConnection"}
{Name "AC-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[infrastructure]"
Events "AuthenticatedConnection"}
{Name "AC-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[infrastructure]"
Events "AuthenticatedConnection"}
```

インフラストラクチャ エントリをさらにいくつか定義します。これらのエントリには、目的を説明するコメントが含まれます。前述のように、[イベント] フィールドが「ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter ManagerRegisterAgent」に設定された単一のエントリに、これらのルールすべてを合理化することができます。ルールを分ける利点としては、ENC サブシステム内部の検証ツールおよび監査ロギングが、操作の許可または拒否の理由を記録する際に、独自のルール名を使用するということが挙げられます。

このエントリによって、すべてのインフラストラクチャ ノートがサーバをマネージャに登録できます。

```
{Name "MRS-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ManagerRegisterServer"}
```

;

このエントリによって、すべてのインフラストラクチャ ノートがルータをサーバに登録できます。

```
{Name "SRR-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ServerRegisterRouter"}
```

;

このエントリによって、すべてのインフラストラクチャ ノートがルータをマネージャに登録できます。

```
{Name "MRR-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ManagerRegisterRouter"}
```

;

このエントリによって、すべてのインフラストラクチャ ノートがクライアントをマネージャに登録できます。

```
{Name "MRA-[infrastructure]-[infrastructure]" enabled "1" RuleType "allow" TimeRange
"all-days" SecPrincType "realm" SecPrinc "[infrastructure]" SecObjType "realm"
SecObj "[infrastructure]" Events "ManagerRegisterAgent"}
```

ここで、DSM および管理対象領域用にインフラストラクチャ ノードに登録できるように宣言する必要があります。以下のエントリは、この設定を行います。

```
{Name "SRA-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "[infrastructure]"
Events "ServerRegisterAgent"}
```

```
{Name "SRA-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[infrastructure]"
Events "ServerRegisterAgent"}
```

```
{Name "SRA-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[infrastructure]"
Events "ServerRegisterAgent"}
```

また、ENC ゲートウェイ ルータには、接続先および中継先となるすべてのノードの認可設定も必要です。以下のエントリによって、このことを定義します。

これらのエントリは、すべての DSM ノードがインフラストラクチャ領域内のルータに接続できるようにします。

```
{Name "RAC-[dsm]-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "[infrastructure]"
Events "RouterAgentConnect"}
```

これらのエントリは、名前付き領域のすべてのエージェント ノードがインフラストラクチャ領域内のルータに接続できるようにします。

```
{Name "RAC-east-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[infrastructure]"
Events "RouterAgentConnect"}
```

```
{Name "RAC-west-[infrastructure]" enabled "1" RuleType "allow" TimeRange "all-days"
SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[infrastructure]"
Events "RouterAgentConnect"}
```

以上で、DSM および管理対象領域のすべての ENC ノードが ENC インフラストラクチャ内のすべてのノードに接続し、認証を行い、登録できるようにするための設定データが十分に準備できました。次の手順では、名前のルックアップおよびエージェント接続の機能を使用できるようにします。以下のエントリによって、このことを行います。

すべてのノードには、管理対象領域がすべての DSM ENC に接続されたコンピュータの名前をルックアップできるという、ミラー ルールがあります。さらに、DSM ENC に接続されたコンピュータは、管理対象領域のすべてのメンバを参照できます。ルールおよびミラー ルールは、以下に示すように明示的に指定する必要があります。

'east' が 'west' を参照できるようにするルール、およびその逆で 'west' が 'east' を参照できるようにするルールはないので、領域間の参照は不可能であることに注意してください。このネームスペースの分割は、仮想ネットワークが安全に動作するために欠かせないものです。

これらのエントリは、名前付き領域のすべてのエージェント ノードが DSM 領域内で ENC メンバのルックアップを実行できるようにします。

```
{Name "NL-east-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events "ManagerNameLookup"}
{Name "NL-west-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events "ManagerNameLookup"}
```

これらのエントリは、すべての DSM ノードが名前付きの領域内で ENC メンバのルックアップを実行できるようにします。

```
{Name "NL-[dsm]-east" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "east" Events "ManagerNameLookup"}
{Name "NL-[dsm]-west" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "west" Events "ManagerNameLookup"}
```

以下のエントリは、DSM および管理対象領域と、エージェント間で接続が行えるようにします。さらに、これらのエントリは、以前のルールセットと組み合わせることができましたが、分割することでルールのより詳細なロギングおよびトラブルシューティングが行えるようになります。

これらのエントリは、名前付き領域のすべてのエージェント ノードが DSM 領域内で ENC メンバに接続できるようにします。

```
{Name "ACN-east-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "east" SecObjType "realm" SecObj "[dsm]" Events "AgentConnect"}
{Name "ACN-west-[dsm]" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "west" SecObjType "realm" SecObj "[dsm]" Events "AgentConnect"}
```

これらのエントリは、すべての DSM ノードが名前付きの領域内で ENC メンバに接続できるようにします。

```
{Name "ACN-[dsm]-east" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "east" Events "AgentConnect"}
{Name "ACN-[dsm]-west" enabled "1" RuleType "allow" TimeRange "all-days" SecPrincType "realm" SecPrinc "[dsm]" SecObjType "realm" SecObj "west" Events "AgentConnect"}
```

これでルールセットの例は終わりです。

その他の質問およびその解決方法

このセクションでは、予想される質問を挙げ、それに対する解決な答えを提供します。

特殊なすべての領域メンバシップ(*)を使用していますが、時間範囲が遵守されていません。なぜですか。

*による一致は、コンピュータ オブジェクトをすべての領域のメンバとしてマークし、さらにこれが「スーパー ユーザ」であるとみなします。スーパー ユーザによるアクセスが可能なオブジェクトは、すべての操作を実行できるので、認可サブシステムは、時間制限またはアクセス制限にかかわらず常に指定された操作を許可します。スーパー ユーザ領域は、任意の接続、ルックアップなど、あらゆるものが可能です。スーパー ユーザタイプの使用は、システム アプリケーション ログの中に警告付きで監査されることに注意してください。

ルールを適用する前に、それを確認する方法はありますか。

はい、ENC ユーティリティ コマンド `encUtilCmd` および `'verify'` コマンドを使用します。これにより、前にリストしたすべてのイベントをシミュレーションできます。アプリケーションの使用方法に関する詳細な説明については、「`encUtilCmd` リファレンス ガイド」を参照してください。

作成するルールがたくさんあります。もっと簡単な方法はありませんか。

はい、ここでも ENC ユーティリティ コマンド `encUtilCmd` を使用します。'`create`' コマンドでは、複数の領域に対するルールセットを作成でき、このドキュメント セクションの方法を反映する基本ルールセットが定義されます。同時に、作成されたすべてのルールを、シミュレーションされた ID を使用して検証するテスト スクリプトを作成することもできます。生成されたルールを後から変更し、本物のセキュリティ ID を使用したり、特定の要件を満たすように他の領域をカスタマイズしたりできます。

イベントの監査

ENC ゲートウェイでは、ノード間の接続に関してイベントを内部的に監査し、オペレーティング システムのイベント ログに監査情報を生成します。オプションで、この情報をイベント管理システムやプレーンファイルに送信することもできます。監査イベントは、エラー、接続、セキュリティなどを対象とするカテゴリにグループ化されます。イベントは個別に、またはカテゴリごとに有効/無効を切り替えることができます。

デフォルトでは、カテゴリ内のメンバはすべて有効になっているのですが、エラー カテゴリを除くすべての監査カテゴリが無効になっています。これは、イベント ログが **ENC** イベントで一杯にならないようにするためです。管理者は、トラブルシューティングやシステムの動作を監視する際に、要求に応じてイベントを有効化する必要があります。

監査イベントは、対応するカテゴリを有効化するか、単一のパラメータを設定することですべて有効化できます。

また、監査設定データは、デフォルトですべてローカルで管理されていますが、**DSM** エクスプローラ内のポリシー エディタを使用して簡単に集中管理に切り替えることもできます。

イベント カテゴリの包括的なリストについては、「**DSM** エクスプローラ ヘルプ」の「設定ポリシー」にある「**ENC** ゲートウェイおよびクライアント監査ポリシー グループ」のトピックを参照してください。

ENC ゲートウェイ コンポーネントのインストールおよび設定

ENC ゲートウェイ機能のインストールは、**CA Client Automation** のインストーラを使用してサポートされています（現在は、**Windows** の動作環境のみ）。

ENC ゲートウェイ コンポーネントの設定は、パラメータを使用して行われ、管理対象設定ポリシーとしてプッシュされます。

ENC ゲートウェイ機能は、**CA Client Automation** インストールの大部分が会社ネットワーク内に存在し、インターネットや内部のファイアウォールを行き来する必要がないと想定されるので、デフォルトでは無効になっています。

注意： **IIS** または **Apache** などの **Web** サーバを **ENC** ゲートウェイ サーバと同じコンピュータ上で実行しようとする場合は、それらの **Web** サーバが同じポートを開こうとしないように設定する必要があります。デフォルトでは、**ENC** は、ポート **80** および **443** でリスンします。**IIS** および **Apache** もポート **80** でリスンします。**IISAdmin** もポート **443** でリスンします。ポートの競合が発生し、**ENC** がリスンできない場合、システム イベント ログに該当するイベントが通知されます。

ENC および SSA の設定

ENC コンポーネントの設定は共通設定パラメータを使用して行われ、管理対象の設定ポリシーを使用してプッシュされます。ENC または SSA の設定ポリシーが変更された場合は、SSA PMUX および CAM が再起動される可能性があります。ENC 設定ポリシーの詳細については、「DSM エクスプローラ ヘルプ」の「設定ポリシー」にある「ENC ゲートウェイ ポリシー グループ」を参照してください。

ENC クライアントを有効化する方法

デフォルトでは、DSM インストーラは、ENC クライアントのファイルをディスクにコピーしますが、有効にはしません。後ほど、クライアントを有効にしようとする場合は、さまざまな手順を実行する必要がありますが、それらは、encUtilCmd ユーティリティ プログラムによって簡単に処理できます。

クライアントを有効化するには、以下のコマンドを実行します。

```
//ネットワーク環境で必要な場合
encutilcmd client -proxy_http [proxy_socks] -proxy_host full_proxy_server_name
                -proxy_port proxy_port_number
                -user username -password password

encUtilCmd client -state enabled -server Name_of_Gateway_Server [-port n]
caf start
```

注: クライアントを有効にすると、CAM (CA メッセージ キューイング) および SSA PMUX (安全なソケット アダプタ ポート マルチプレクサ) が再起動されるという副作用があります。これは、ENC によってこれらのコンポーネントの両方が統合され、それらを「ENC 対応」にするために再起動が必要になるためです。

ENC 環境における展開

ENC 環境（つまり、間にファイアウォールが存在する環境）でソフトウェアを正常に展開するには、以下の前提条件を満たしている必要があります。

- **Client Automation** のインフラストラクチャ展開コンポーネントでは、**DMPprimer** および **dmkeydat.pmr** ファイル(展開証明書)の両方がターゲット コンピュータ上に存在する必要があります。

これを満たすための詳細については、「[インフラストラクチャ展開プライマソフトウェアの手動インストール \(P. 280\)](#)」および「[展開管理セキュリティキーのプライマインストールへの提供 \(P. 281\)](#)」を参照してください。

- **ENC** クライアント コンポーネントがターゲット コンピュータ上で実行され、操作可能である必要があります。**ENC** クライアント コンポーネントは、基本ハードウェア インベントリ コンポーネントとともにインストールされ、設定を行うことで操作可能になります。
- インフラストラクチャ展開ポリシー オプション[ホスト名の使用] および[スキャン中にターゲットに対して ping を実行しない] を **True** に設定する必要があります。
- インフラストラクチャ展開ポリシー オプション [プライマを常に展開] は、**False** に設定する必要があります。これは、**ENC** 環境では、ターゲット コンピュータにファイアウォールをインストールしている可能性があるため、通常の方法ではプライマを展開できず、代替方法を使用する必要があるためです。

ENC 展開シナリオ

このセクションで説明されているシナリオは、ENC ゲートウェイ機能が採用されている最も一般的なものであると考えられます。それらは、パイロット スキーム、ブランチ オフィス、および IT 委託者に基づいています。

委託者のシナリオでは、さまざまな規模の会社が、自社のデスクトップおよびサーバの管理を IT 管理の専門会社に出注しています。通常の技術的な管理タスクを実行するには **CA Client Automation** が採用されていますが、ファイアウォールおよびインターネット越しに作業を行うには、ENC ゲートウェイの機能が必要になります。もちろん、アウトソースを行う会社が同時に複数回、すべてのシナリオを処理している可能性もあります。

その他のシナリオももちろん考えられます。

各シナリオでは、システムのインストールおよび設定に必要な手順が説明され、結果が期待されています。

以下のセクションで考えられている ENC 展開シナリオは、以下のとおりです。

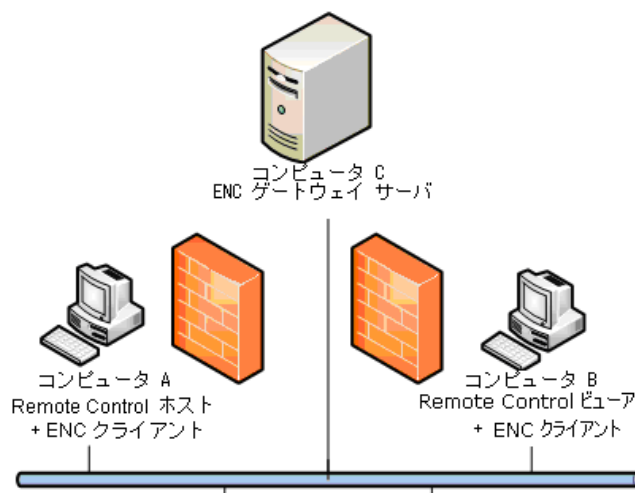
- [シナリオ 1：パイロット スキーム](#) (P. 530)
- [シナリオ 2：ブランチ オフィス](#) (P. 535)
- [シナリオ 3：アウトソース クライアント会社（小規模）](#) (P. 539)
- [シナリオ 4：アウトソース クライアント会社（中規模）](#) (P. 540)
- [シナリオ 5：アウトソース クライアント会社（大規模）](#) (P. 541)

ENC 展開シナリオ - パイロット スキーム

このシナリオは、組織が展開する最初のシナリオであると考えられ、システムがどのように働くかについて経験してもらうためのものです。また、ENC ゲートウェイの理解に役立つ簡単な例としての役割を果たします。

このシナリオは、単純に 3 つのコンピュータに基づいており、そのうちの 2 つは Windows のパーソナル ファイアウォール内にあるエージェント コンピュータで、3 つ目は接続を提供する ENC ゲートウェイ サーバです。

以下の図は、パイロット スキーム シナリオのレイアウトを示します。



このシナリオでは、コンピュータ A、B、および C がそれぞれ Remote Control ホスト、Remote Control ビューア、および ENC ゲートウェイ サーバを実行しています。コンピュータ B はファイアウォール内にあるので、コンピュータ A に接続できません。すべてのコンピュータ上では、コンピュータ C 上の ENC ゲートウェイ サーバに接続されている ENC クライアントが実行されています。コンピュータ B から A への接続を可能にしているのは、コンピュータ C です。このシナリオをできる限り単純なものにするために、設定はドメインマネージャの管理対象外です。

小規模の ENC ゲートウェイ ネットワークを設定するには、以下の手順に従います。

コンピュータ A 上での作業：

1. Windows ファイアウォールを有効化します。
2. Client Automation のカスタム インストールを開始します。 [Remote Control] および [エージェント] を選択します。
3. インストーラによってスケーラビリティ サーバのアドレスを求められたら、現在のデフォルト値を受け入れます。（サーバがないので）それでいいかどうかインストーラによって確認を求められたら、[はい] をクリックします。これにより、管理対象外のインストールを行うことができます。
4. [ENC クライアント] ボタンをクリックし、クライアントの設定を開始します。クライアントのサーバアドレスとして、コンピュータ C のアドレスをクリックします。
5. [Remote Control] ボタンをクリックし、[ホスト機能のインストール] のみを選択します。

6. インストールが完了したら、**Client Automation** を起動せずに以下のコマンドを実行します。

```
ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn centralizedsecurity -v 0
```

```
ccnfcmda -cmd setparametervalue -ps itrm/rc/host/managed -pn standalone -v 1
```

7. 「caf start」コマンドを使用して **Client Automation** を起動します。

コンピュータ B 上での作業：

1. Windows ファイアウォールを有効化します。
2. カスタム インストールを開始します。 [Remote Control] および [ビューア] を選択します。
3. スケーラビリティ サーバの指定はありません（コンピュータ A と同様に続行します）。
4. ENC クライアントをコンピュータ A で行ったのと同じ方法で設定します。
5. [Remote Control] ボタンをクリックし、[ビューア機能のインストール] のみを選択します。
6. インストールが完了したら、**Client Automation** を起動せずに以下のコマンドを実行します。

```
ccnfcmda -cmd setparametervalue -ps itrm/rc/viewer/managed -pn managedmode -v 0
```

7. 「caf start」コマンドを使用して **Client Automation** を起動します。

コンピュータ C 上での作業：

1. Windows ファイアウォールが無効になっていることを確認します。
2. カスタム インストールを開始します。製品の選択をすべてオフにします。カスタム インストールのダイアログ ボックスで、[ENC ゲートウェイ] および [エージェント] 以外のすべての選択をオフにします。
3. スケーラビリティ サーバの指定はありません（コンピュータ A と C と同様に続行します）。
4. ENC ゲートウェイを設定するためのダイアログ ボックスで、マネージャ、サーバ、およびルータの 3 つのロールすべてを選択します。
5. このコンピュータ上の **Client Automation** はまだ起動しないでください。ゲートウェイ サーバのセキュリティはまだ設定されていないので、クライアントからの接続はすべて拒否されます。ENC セキュリティを設定するには、すべての接続を許可するルールを含むテキスト ファイルを作成することができます。そのファイルは、その後、サーバが受信するための共通ストアにインポートされます。

重要: これは単なる例であることに注意してください。実際の本番環境では、オープン アクセスを許可するルールは決して使用しないでください。

- 以下のテキストを含む `defrules.txt` という名前のテキスト ファイルを作成します。

```
[authz]
RulesVersion=5

REALM
{Name "ENC" Notes "The default realm to which everyone belongs"}
end

TimeRange
{Name "all-days" enabled "1" Hours "00:00 - 00:00" Type "normal" Weekdays "sunday
- saturday"}
end

TimeACL
{Name "policy1" enabled "1" RuleType "allow" Events "AuthenticatedConnection
ManagerRegisterServer ServerRegisterRouter ManagerRegisterRouter
ServerRegisterAgent ManagerRegisterAgent ManagerNameLookup AgentConnect
RouterAgentConnect ManagementAccess" TimeRange "all-days" SecPrincType "realm"
SecPrinc "ENC" SecObj "ENC" SecObjType "realm"}
end

URIMapping
{URI "." enabled "1" Type "pattern" Realm "ENC"}
end

IPAddWhiteList
{IPAddress "." enabled "1" Type "pattern"}
end
```

- 以下のように、`encUtilCmd` コマンドを使用してこのルール ファイルをインポートします。

```
encUtilCmd import -i defrules.txt -fl
```

これで、ENC ゲートウェイ サーバがすべての接続を許可するルールを持つようになりました。

- 最後に、すべてのコンピュータに ENC 証明書をインストールします。詳細については、「[ENC ゲートウェイで使用するための証明書サービスの設定](#) (P. 548)」を参照してください。

シナリオをテストするには、以下の手順に従います。

- コンピュータ A および B 上で、「`caf start`」コマンドを使用して **Client Automation** を開始します。ENC ゲートウェイの機能をテストするので、コンピュータ C はまだ開始しないでください。
- ホスト設定ダイアログ ボックスをコンピュータ A のシステム トレイから選択して開始します。[ユーザ] タブを選択し、ローカル管理者がそのコンピュータ上の **Remote Control** のユーザであることを確認します。
- コンピュータ B で、ビューアを開始し、接続を試行します。これは、コンピュータ A 上のファイアウォールでブロックされるはずですが、

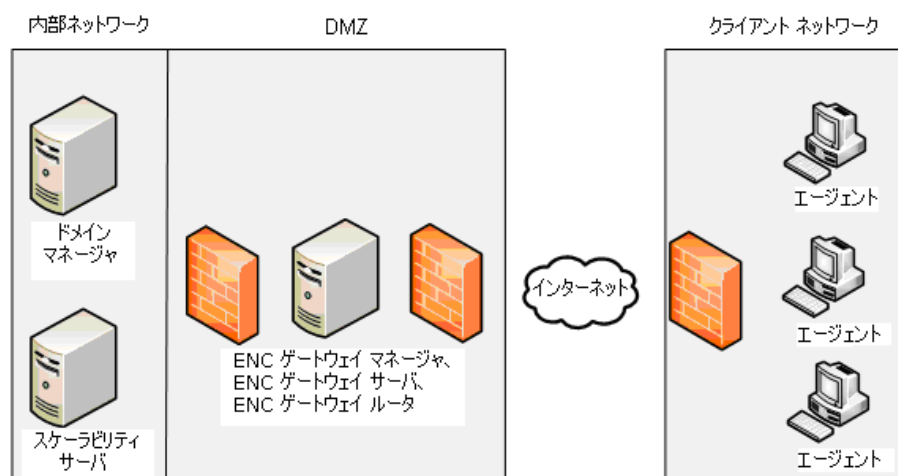
4. コンピュータ C 上の Client Automation を開始します。数分後、「**encclient status**」コマンドを使用して ENC クライアントが ENC ゲートウェイ サーバに登録されたことを確認します。これにより、クライアントが正常に登録され、準備が整ったことが報告されます。
5. 接続の試行を再実行します。今回はうまく行くはずですが、すべてのデータがコンピュータ C 経由で転送されます。「**encclient status**」コマンドによって、コンピュータ C 経由で接続が進行中であることが報告されます。
6. **defrules.txt** ファイルを変更し、再インポートすることでルールを調整できますが、**encUtilCmd** コマンドを **-o** オプション付きで使用すると、既存のルールに優先されます。これにより、異なる認可ルールを試すことができるので、システムの感触をつかむことができます。

(**encUtilCmd** ユーティリティ プログラムおよびそのすべてのオプションの詳細については、「**CA ブックシェルフ**」の「リファレンス ガイド」カテゴリにある「**EncUtilCmd コマンドリファレンス**」を参照してください。)

ENC 展開シナリオ - ブランチ オフィス

このシナリオでは、親会社がメイン オフィス ネットワーク（内部ネットワーク）上にドメイン マネージャおよびスケーラビリティ サーバを保持しています。ブランチ オフィスでは、コンピュータに **DSM エージェント**がインストールされた **LAN** を使用しています（クライアント ネットワーク）。両方のオフィスは、ファイアウォールで保護されており、インターネットに接続されています。

以下の図は、サンプルのブランチ オフィス展開シナリオにおけるネットワーク レイアウトを示します。



このシナリオでは、ENC ゲートウェイ サーバ コンピュータを含むネットワーク内のすべてのコンピュータに少なくとも **DMS エージェント**が1つインストールされていると想定されています。

DMZ（非武装地帯）によって、内部ネットワークから **DMZ** までの接続が可能になりますが、それを越えては接続できません。**DMZ** 内のコンピュータは、インターネットへは接続できますが、内部ネットワークへは接続できません。

このシナリオで必要な展開および設定の手順は、以下のとおりです。

- メイン オフィス（内部ネットワーク）で **ENC** インフラストラクチャを展開します
- **DSM エージェント**をブランチ オフィス（クライアント ネットワーク）へ展開します
- ブランチ オフィスのエージェントがメイン オフィスのスケーラビリティ サーバに報告するように設定します

メインオフィスのネットワークでは、以下のアクティビティが適用されます。

- まだ存在しない場合は、メインオフィスのネットワークで **DMZ** を作成します。これは、パブリックのインターネット経由での接続が想定されるブランチオフィスから **ENC** ゲートウェイ サーバが認識される必要があるために必要です。
- 親ネットワークにおける要求に従って、**DSM** ドメイン マネージャ、スケーラビリティ サーバ、エージェント、および **ENC** クライアントをインストールします
- **DSM** エージェント、**ENC** クライアント、マネージャ、サーバ、およびルータをメインオフィス ネットワークの **DMZ** 内にあるコンピュータ上にインストールします。内部ネットワークのスケーラビリティ サーバにエージェントが登録されるように設定します。
- 「[証明書](#)の管理 (P. 548)」の説明に従って、**ENC** ゲートウェイ対応のすべてのコンピュータ上に **ENC** 証明書をインストールします。これは、内部ネットワークおよび **DMZ** 内のコンピュータをカバーします。これらは、**ENC** ゲートウェイ認証に必要です。
- **DMZ** のコンピュータに **ENC** 証明書をインストールします。
- **ENC** ゲートウェイ サーバはまだ開始しないでください。この時点で、**ENC** ゲートウェイ サーバは認可ルールが設定されておらず、すべての接続が拒否されます。これはつまり、**DMZ** 内の **DSM** インフラストラクチャがメインオフィス ネットワーク内のドメイン マネージャに接続できず、認可ルールを含む設定ポリシーを受信することができないことを意味します。
- **DSM** エクスプローラを開き、**ENC** に必要なセキュリティ ポリシーを設定します。セキュリティ ポリシーを使用して **ENC** ゲートウェイを設定します。これは、メインオフィス ネットワーク内のコンピュータおよびブランチ オフィス内のコンピュータに対するアクセスをカバーする必要があります。ただし、現在のところ、コンピュータは、ドメイン マネージャに登録されるまでポリシーを受信できず、ドメイン マネージャに接続できるようにする認可ルールを定義するポリシーを受信するまでは登録できないという、矛盾した状況が存在するため、ドメイン マネージャから **ENC** ゲートウェイ サーバにこれを送信することはできません。

- この状況を修正するには、ENC ゲートウェイ サーバがドメイン マネージャへ接続するのに十分なルールを使用して、「ブートストラップ」される必要があります。いったん確立されると、ドメイン マネージャは本物のポリシーを送信してブートストラップ ポリシーを上書きできます。

まず、本物のポリシーをドメイン マネージャ上の設定ポリシーに入力する必要があります。これは、以下の 2 種類の方法のいずれかを使用して行うことができます。

1. 1 番目の方法は、DSM エクスプローラを開き、設定ポリシー エディタを使用して ENC に必要なセキュリティ ポリシーを設定します。GUI は、ルールの作成に役立つカスタム ダイアログ ボックスを提供します。
2. もう 1 つの方法は、デフォルトルールを使用してテキスト ファイルを作成し、encUtilCmd ユーティリティを使用してまとめてそれらをインポートします。（encUtilCmd およびそのすべてのオプションの詳細な説明については、「CA マニュアル選択メニュー」の「リファレンス ガイド」カテゴリにある「EncUtilCmd コマンドリファレンス」を参照してください）。encUtilCmd では、ルールを「ライブ」状態にする前に検証する方法も提供されます。

これらのルールは、最低でも メイン オフィス ネットワーク内の DSM インフラストラクチャが DMZ 内の ENC ゲートウェイ インフラストラクチャに接続し、登録できるようにする必要があります。

作成したルール ファイルは、ドメイン マネージャと ENC サーバ コンピュータの両方で使用できるので、2 番目の方法を使用してルールを作成することをお勧めします。GUI を使用して、将来ポリシーにさらなる変更を加えることができます。

「encUtilCmd importdb」コマンドを使用して、ドメイン マネージャにルールを適用します。これにより、DSM 設定データベースにルールが追加されます。データベースに追加されると、ENC サーバ コンピュータがいったん接続すると、通常のポリシー メカニズムを通じてポリシーを配信できます。

「encUtilCmd import」コマンドを使用して、これらのルールを DMZ 内の ENC ゲートウェイ サーバに適用します。これにより、認可ルールを使用してサーバがブートストラップされ、コンピュータがドメイン マネージャに接続し、登録可能になります。

ENC ゲートウェイ サーバが新しいルールを受け取り、ENC 接続の続行を許可するように、これらのサーバ上で CA Client Automation を開始します。

- デフォルトでは、ドメイン マネージャ内の設定ポリシーは、空のポリシーによって予想外に上書きされてしまうのを防ぐためにローカルで管理されるように設定されています。これを集中管理に設定します。CA Client Automation が正常に登録すると、最初のデフォルトルールがドメイン マネージャから送信されたポリシーによって上書きされます。

- 10 分待機してから、DMZ 内のコンピュータが登録され、GUI 上に表示されるようになったことを確認します。
- コンピュータが表示されない場合、デフォルトルールが不正確であるか、新しいポリシーのアクセスが切れているかのいずれかの可能性があります。この状況を診断するには、ENC ゲートウェイ サーバ上の NT アプリケーション イベント ログを調査します。

ブランチ オフィスでは、以下のアクティビティが適用されます。

- 必要な DSM エージェントをブランチ オフィス ネットワーク内の各コンピュータにインストールします。ENC ゲートウェイ機能は、デフォルトでインストールされますが、設定が必要です。メイン オフィスの DMZ ネットワークの ENC ゲートウェイ サーバにクライアントが登録されるように設定します。メイン オフィスとブランチ オフィス間では、ENC ゲートウェイがまだ機能していないので、DSM の展開は使用できません。その代わり、たとえば影響を受けるコンピュータ数などに依存する、以下のようなさまざまな方法を使用してインストールを実行できます。
- インストールするのが数台のコンピュータの場合の DVD からの手動インストール。
- NT ドメイン ログオン スクリプトを使用した、ユーザ ログオン時のパッケージのインストール。
- ブランチ オフィス ネットワークへのドメイン マネージャおよびスケラビリティ サーバの一時的なインストール。これは、ブランチに送信される本物または仮想のマシンを使用して実行できます。エージェント パッケージを送信するには、CA Client Automation の展開機能を使用します。いったん展開が完了し、すべてのエージェントがメイン オフィスのドメイン マネージャに登録されると、ブランチ オフィスの一時的なドメイン マネージャは削除されます。
- メイン オフィスの GUI の中で「すべてのコンピュータ」グループをチェックすることで、ブランチ オフィスのコンピュータが登録されているかを確認します。
- 組織で採用されている通常の検証テストを実行し、CA Client Automation が完全に機能するかを確認します。

ENC 展開シナリオ - アウトソース クライアント会社(小規模)

小規模な会社のシナリオは、セキュリティの強化が必要な点を除いて、ブランチオフィスのシナリオと似ています。アウトソースの委託者はさまざまな会社を担当している可能性があるため、それぞれの会社ネットワーク内のノード間で許可される接続に対して、コントロールを強化する必要があります。さらに、1つのアウトソース クライアントから別のクライアントへのアクセスは保護される必要があります。通常、あるクライアントは別のクライアント内のコンピュータを参照できないようになっています。これは、ENC ゲートウェイ認証の中の領域のサポートによって処理されます。

アウトソースを行う会社のコンピュータは、クライアントのコンピュータに接続できる必要があります。これには、委託者の ENC ゲートウェイ マネージャが以下を許可する認可ルールを使用して設定される必要があります。

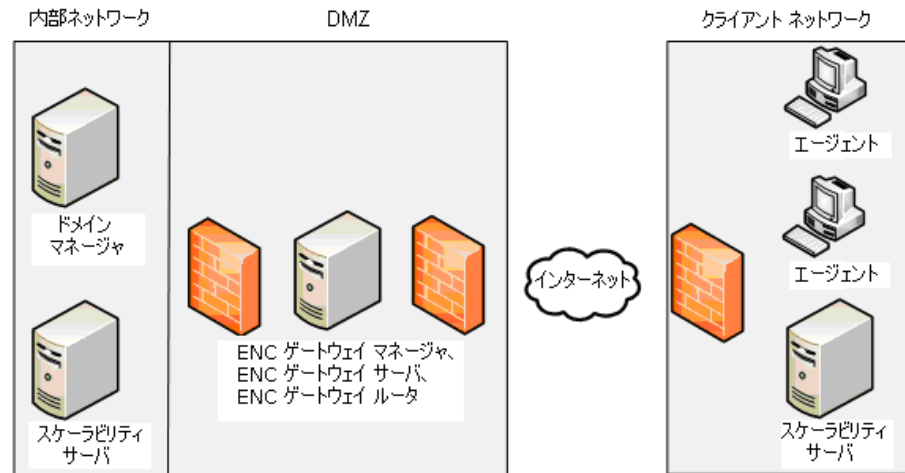
- クライアント ネットワーク内のコンピュータからの登録。
- クライアント ネットワーク内のコンピュータから委託者のネットワーク内のコンピュータへの接続（およびその逆）。
- 異なるクライアント領域間の接続は拒否されます。

Client Automation の構成および設定は似ていますが、セキュリティ エリア管理がセキュリティ要件を処理するようにも設定する必要があります（「[Client Automation セキュリティ機能](#)」(P. 439)の章を参照）。

ENC 展開シナリオ - アウトソース クライアント会社(中規模)

このシナリオでは、クライアントに独自のスケーラビリティ サーバを設置するのに十分な数のコンピュータが存在します。

以下の図は、サンプルの中規模アウトソース会社の展開シナリオにおけるネットワーク レイアウトを示します。



クライアント ネットワーク内のエージェントは、そのネットワーク内のスケーラビリティ サーバに登録されます。スケーラビリティ サーバは、委託者のネットワーク内のドメイン マネージャに ENC ゲートウェイ接続経由で接続します。展開の手順は、エージェントの設定を除いて、小規模会社のシナリオと非常に似ています。このシナリオでは、「社内」のスケーラビリティ サーバに登録されるように DSM エージェントが設定されます。

この中規模の委託者シナリオでは、通常、ENC は、エンドポイントのコンピュータ上に存在しません。これはつまり、このシナリオでは、ENC がエンドポイントのコンピュータ上で設定され実行されていない限り、直接接続が機能しないことを意味します。直接接続は、以下の通信に使用されます。

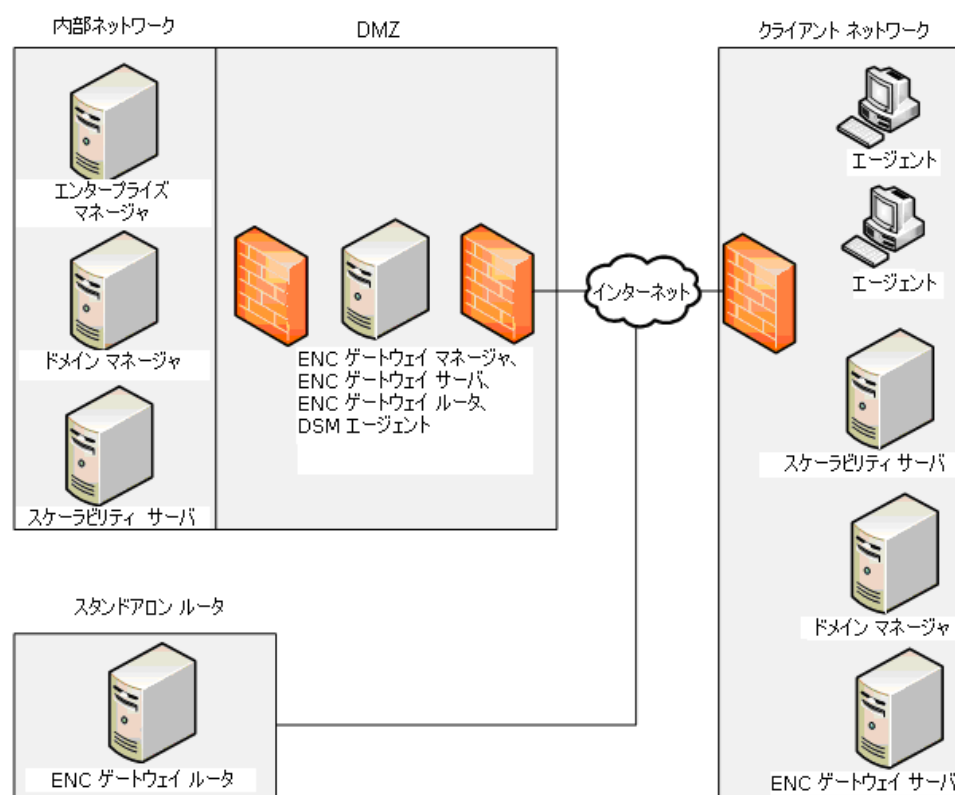
- Remote Control ホスト - ビューの接続
- DSM エクスプローラからエージェントへのインスタント診断
- エージェントからマネージャへのソフトウェア カタログ
- DTS 通知

ENC 展開シナリオ - アウトソース クライアント会社(大規模)

このシナリオでは、会社の規模が大きいので、独自のドメイン サーバに加え、複数のスケーラビリティ サーバと 1つの ENC ゲートウェイ サーバが存在します。

アウトソースを行う会社は、クライアントのドメイン マネージャにリンクされるエンタープライズ マネージャを保持しています。

以下の図は、大規模なアウトソース クライアント会社の ENC ゲートウェイの展開シナリオにおけるネットワーク レイアウトを示します。



クライアントのドメイン マネージャがインストールされると、通常どおりそれを使用して DSM エージェントをクライアント内で展開できます。

クライアントのドメイン マネージャを使用して、クライアントの ENC ゲートウェイ サーバがクライアント コンピュータから ENC 接続を受け入れることが可能になるようにポリシーをローカルで設定できます。

エンタープライズ マネージャは、データベース プロバイダ自身を使用して、データベースをドメイン マネージャに対して複製します。これは、ENC ゲートウェイ 接続経由では実行できません。これを可能にするには、Microsoft または Oracle が公開している既存のベストプラクティスで説明されているように、ファイアウォールを設定する必要があります。

アウトソースを行う会社のコンピュータは、クライアントのコンピュータに接続できる必要があります。これには、委託者の ENC ゲートウェイ マネージャが以下を許可する認可ルールを使用して設定される必要があります。

- クライアントの ENC ゲートウェイ サーバからの接続
- クライアント ネットワーク内のコンピュータからの登録
- クライアント ネットワーク内のコンピュータから委託者のネットワーク内のコンピュータへの接続（およびその逆）

スタンドアロン ENC ゲートウェイ ルータ

回復力または拡張性の目的で、追加の ENC ゲートウェイ ルータを展開することができます。これらの ENC ゲートウェイ ルータは、他の場所（インターネット上またはブランチ オフィス内）にインストールできます。

スタンドアロン ENC ゲートウェイ ルータを展開する手順は、以下のとおりです。

- DSM エージェントおよび ENC ゲートウェイ ルータをインストールし、委託者のオフィスの ENC ゲートウェイ サーバに登録されるように設定します。このルータは、別の適切な ENC ゲートウェイ サーバに登録されるようにももちろん設定できます。
- ドメイン マネージャで、スタンドアロン ルータ コンピュータ向けのポリシーに適切な認可ルールを追加します。このルールでは、ルータが存在する領域内で、ルータが接続および登録が許可されるようにする必要があります。
- ルータ コンピュータに適切な証明書をインストールします。
- ルータ コンピュータ上の **Client Automation** を開始します。ルータは、その後、ENC ゲートウェイ サーバに登録される必要があります。これには、イベントログを確認します。

注: これらのイベントを表示するには、設定パラメータ

`itrm/common/enc/audit/enabled` を 1 に設定する必要があります。設定ポリシーの中で、これは「すべて有効」というように表示されます。これにより、すべての ENC イベントの監査が有効になります。これにより、ENC システム内のアクティビティをより明確に確認できます。デフォルトでは、「エラー」カテゴリ内のイベントのきが有効になっています。監査を通常の状態に戻すには、設定パラメータを 2（「カテゴリ別に有効化」）に設定します。

- ルータ コンピュータ上の ENC クライアントが登録されると、**Client Automation** インフラストラクチャがポリシーを受け取るようになり、ルータの認可ルールをインストールできるようになります。ルータが認可ルールをいったん受け取ると、ENC ゲートウェイ ネットワーク内の他のコンピュータが接続するためのルータとしての役割を担うことができます。

スタンドアロン ENC ゲートウェイ サーバ

スタンドアロン ENC ゲートウェイ ルータに関して、同様の考慮事項がスタンドアロン ENC ゲートウェイ サーバにも適用されます。相違点としては、認可ルールがサーバ ロールに適したもの、つまり、ゲートウェイ ルータが実行できる操作とは対照的に、ゲートウェイ サーバが実行できる操作を可能にするものであるという点です。

インターネット プロキシのサポート

ENC ゲートウェイ サーバへの ENC クライアントのパスがインターネット プロキシによってブロックされる場合、そのプロキシ経由で接続できるように設定する必要があります。ENC ゲートウェイでは、**SOCKS4**、**SOCKS5**、および **HTTP** プロキシをサポートします。認証は、明示的なユーザ名およびパスワードか、ログオンユーザを別のユーザとして実行することで設定できます。クライアントは、現在の **Internet Explorer** の設定を使用して、プロキシを検索できます。

設定する必要があるプロパティは、ポリシー ノード '**common components/enc/client**' の中にあります。

SOCKS プロキシを設定するには、以下のようなパラメータを設定します。

- プロキシ コンピュータを識別するための **SocksProxyAddress** および **SocksProxyPort**
- 使用される認証のタイプ（基本またはセキュア）を定義するための **SocksProxyAuthType**
- クライアントがログオンユーザのクレデンシャルを使用できるようにする **SocksProxyImpersonate** これはもちろん、誰かがログオンしていないとクライアントが接続できないことを意味します。
- プロキシとの認証に明示的なクレデンシャルを使用する場合は、**SocksProxyUsername** および **SocksProxyPassword**
- ENC クライアントが IE の設定を使用して自動的にプロキシを検索するには、**SocksProxyDiscovery** この場合、通常は **SocksProxyImpersonate** を設定します

HTTP プロキシを設定するには、パラメータ名の中の「**Socks**」を「**HTTP**」に置き換える点を除いて、同じパラメータを設定します。

注: プロキシ設定は、**encUtilCmd** ユーティリティを使用しても設定できます。これは、問題のコンピュータがファイアウォールによって管理対象ポリシーから切断されているけれども、接続するためにポリシー設定が必要なことが明らかな場合に役立ちます。

ENC ゲートウェイ経由で Client Automation を使用することに関する制限事項

CA Client Automation (Client Automation) には、ENC ゲートウェイ接続経由で使用された場合に、機能に関するさまざまな制限事項があります。これらの制限事項には以下のものが含まれます。

- Wake-on-LAN (WOL) では UDP が使用されるのに対し、ENC ゲートウェイでは TCP 接続しかサポートされていないので、WOL が ENC ゲートウェイを経由できません。
- インスタント診断のいくつかの機能は、オペレーティングシステムによって提供される FTP などの ENC ゲートウェイ非対応のコンポーネントに依存しているため、機能しません。
- サービス ロケーションは、UDP を使用するので機能しません。
- レポータは、MDB に直接アクセスするので機能しません。
- ENC ゲートウェイを経由する Software Delivery (SD) のジョブは、トリガされるまでに最大 10 分かかる可能性があります。これは、SD が登録される際にターゲットの IP アドレスを使用しようとしませんが、IP アドレスが異なるネットワーク上では無効なために起こります。SD スケーラビリティ サーバは、ターゲットの FQN および IP を交互に使用して、10 分おきにジョブを再試行します。ENC ゲートウェイでは、ENC ゲートウェイ対応のコンピュータを一意に識別するために、その FQN が使用されるので、FQN が機能します。
- Client Automation 内部のコンポーネントの中には、SQL Server または Oracle クライアント側のコンポーネントを使用して、MDB (管理データベース) の直接接続を行うものもあります。これらの接続は ENC 対応ではないため、これらの接続がファイアウォールを通過する場合は、Microsoft または Oracle が推奨するファイアウォールの横断方法を使用する必要があります。

以下のリストでは、MDB の直接アクセスが行われ、さらに、SQL Server および Oracle で使用される特定のクライアント側のコンポーネントが指定されている場合のシナリオおよび DSM コンポーネントの詳細について説明します。

- エンタープライズ マネージャとやりとりを行うドメイン マネージャ
ドメイン マネージャとエンタープライズ マネージャ間の MDB の複製では、直接接続と大量コピーが使用されます。
クライアント側のコンポーネント：
SQL Server 用：SQL Native Client および bcp ユーティリティ
Oracle 用：OCI API および SQL*Loader

- **エンジンからドメイン マネージャおよびエンタープライズ マネージャ**
エンジンは、ドメイン マネージャおよびエンタープライズ マネージャと通信を行う場合は、直接データベース接続を使用します。
クライアント側のコンポーネント：
SQL Server 用： SQL Native Client および bcp ユーティリティ
Oracle 用： OCI API および SQL*Loader
- **レポーターからドメイン マネージャまたはエンタープライズ マネージャ**
レポーターは、レポートを生成するのに直接データベース接続を使用します。
クライアント側のコンポーネント：
SQL Server 用： SQL Native Client および bcp ユーティリティ
Oracle 用： OCI API および SQL*Loader
- **Web コンソールからドメイン マネージャまたはエンタープライズ マネージャ**
Web コンソールは、データベースに対して JDBC 接続を使用します。
クライアント側のコンポーネント：
SQL Server 用： JDBC
Oracle 用： JDBC
- **コンテンツのインポート/エクスポート ユーティリティ**
コンテンツのインポート/エクスポート ユーティリティは、リモートの Oracle または SQL Server MDB と DSM のデータの同期を行う場合は、直接データベース接続を使用します。
クライアント側のコンポーネント：
SQL Server 用： SQL Native Client および bcp ユーティリティ
Oracle 用： OCI API および SQL*Loader

encUtilCmd ユーティリティの使用

encUtilCmd ユーティリティとは、さまざまな ENC ゲートウェイ機能を実装するために設計されたプログラムです。ただし、このセクションでは、encUtilCmd の 1 つのユース ケースのみを扱います。

encUtilCmd コマンドおよびそのすべてのオプションの詳細な説明については、「CA ブックシェルフ」の「リファレンス ガイド」カテゴリにある「*EncUtilCmd* コマンドリファレンス」を参照してください。

ほかの機能に加えて encUtilCmd ユーティリティでは、ENC ゲートウェイ セキュリティの設定に関する問題が処理されます。

このユース ケースでは、スケーラビリティ サーバのインストール後に発生する問題（ロックされた状態）について考えます。ドメイン マネージャは、間にファイアウォールがあるために、スケーラビリティ サーバに直接接続できません。そのため、この方法を使用してスケーラビリティ サーバにポリシーを配布することはできません。スケーラビリティ サーバではすべての接続試行が拒否されるので、ドメイン マネージャは、ENC ゲートウェイを使用してスケーラビリティ サーバに接続できません。スケーラビリティ サーバに誰が接続できるかを定義するのは、このポリシーです。

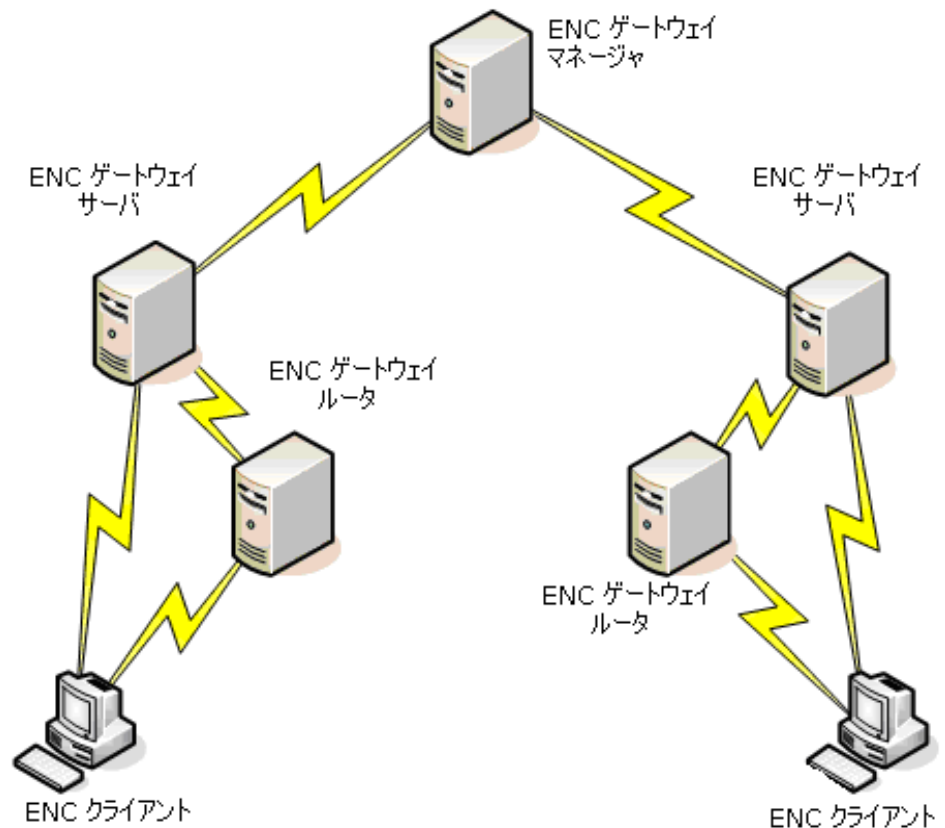
この問題を解決するには、テキスト ファイル内にいくつかのルールを定義し、ENC ゲートウェイ サーバ上で encUtilCmd コマンドを使用してこのファイルをインポートすることができます。

証明書の管理

ENC（拡張ネットワーク接続）インフラストラクチャでは、すべてのノード内通信は、標準の TLS（トランスポートレイヤセキュリティ）プロトコルを使用して保護されます。このプロトコルによって、機密性、整合性、および相互認証が提供されます。

TLS プロトコルの認証部分は、デジタル証明書およびパブリック/プライベート キーの暗号方式によって提供されます。機密性は、対称キーの暗号方式によって提供されます。

以下の図は、ENC インフラストラクチャ内の ENC コンポーネント間のノード内接続を示しています。



ENC インフラストラクチャ内のすべてのノード内接続は、TLS 認証によって保護されます。認証は常に相互的なものです。接続の開始側が応答側に対して認証され、応答側は開始側に対して認証されます。これにより、ENC インフラストラクチャは、それに接続するコンピュータを検証でき、さらに ENC クライアントは、接続先に対して保護されます。

X.509 証明書

ENC（拡張ネットワーク接続）は、認証用に X.509 バージョン 3 のデジタル証明書を使用します。使用される証明書プロファイルは、IETF PKIX 作業部会の RFC 3280 実装によるものです。

証明書とそれに関連するプライベート キーは、Microsoft 証明書ストアを通じて取得されます。証明書には、それを使用するアプリケーションに応じて、サーバ認証（1.3.6.1.5.5.7.3.1）またはクライアント認証（1.3.6.1.5.5.7.3.2）用にマークされた、拡張キー使用法の拡張が含まれる必要があります。

証明書ロケーション（1.3.6.1.4.1.791.2.10.8.3）を支援するために、拡張キー使用法の証明書拡張に対する Client Automation プライベート拡張を使用できます。この OID（オブジェクト ID）は、CA Technologies に対してはプライベートで、CA OID ツリーに対しては内部になります。

認証キー ペアに使用される RSA キーのサイズには、ENC の制限は課せられません。使用されるキーのサイズは、組織で独自に選択されるものですが、最低でも 1024 ビットのキーを推奨いたします。

PKI インフラストラクチャを使用した証明書の管理

証明書の作成および配布は、困難なプロセスになる場合があります。PKI（パブリック キー インフラストラクチャ）を使用してこのプロセスを自動化し補強することが非常に望ましいです。

証明書の要件

ENC ゲートウェイでは、標準の TLS 1.0 (SSL 3.1) セキュリティプロトコルが使用するために発行される X.509 v3 証明書を使用します。ENC ゲートウェイでは、標準の TLS 証明書を使用できますが、ENC サブシステムが主に ENC ゲートウェイによって使用される証明書を識別できるようにするための拡張キー使用法の拡張もサポートされています。

ENC ゲートウェイは、ID 用にロードするのに最適な証明書を検索します。最初の検索では、有効な証明書（および関連するプライベート キー）が検索され、CA ENC 使用法の拡張（以下の表の（1）を参照）に加えて、クライアント認証用の TLS 使用法の拡張（2）、またはサーバ認証（3）、個別（4）を使用してマークされます。

以下の表では、上記の項で（1）から（4）でマークされた用語に関する追加の詳細を示します。

マーカー	情報
(1)	CA Technologies では、拡張キー使用法の ID として、X.509 v3 証明書で使用するための OID（オブジェクト）が内部的に割り当てられています（RFC2459 のセクション 4.2.1.13 を参照）。この OID は、証明書が ENC セキュリティ サブシステムによって使用されることを示します。 ■ オブジェクト ID は、「1.3.6.1.4.1.791.2.10.8.3」です。 ■ オブジェクト ID タグは、「OID_PKIX_KP_CA_CMS_ENC_TLS_AUTH」です。 ■ 使用法の拡張は、重要または重要でないとマークできます。 ■ CA Technologies ベース OID は、「1.3.6.1.4.1.791」で、IANA 登録されています。
(2)	TLS クライアント認証の OID は、「1.3.6.1.5.5.7.3.2」です。
(3)	TLS サーバ認証の OID は、「1.3.6.1.5.5.7.3.1」です。
(4)	クライアントおよびサーバの両方として機能する ENC ゲートウェイ ノード（ルータおよびゲートウェイ サーバ）では、セキュリティ サブシステムは、クライアントに対してマークされた単一の証明書とサーバ認証、または、それぞれクライアント認証のみとマークされるかサーバ認証のみとマークされている個別の証明書のいずれかを使用できます。

ENC ゲートウェイが適切な証明書を見つけられなかった場合は、CA ENC 使用法の拡張の要件なしで検索が繰り返されます。

ENC ゲートウェイが使用する証明書を作成する場合は、CA 拡張キー使用法 OID を証明書に追加することをお勧めします。ただし、ENC ゲートウェイはこれなしで動作します。

CA Technologies-プライベート認証オブジェクト ID

証明書ロケーション（1.3.6.1.4.1.791.2.10.8.3）を支援するために、拡張キー使用法の証明書拡張に対する Client Automation プライベート拡張を使用できます。

この OID（オブジェクト ID）は、CA Technologies に対してはプライベートで、CA Technologies OID ツリーに対しては内部になります。

第 13 章: CA Service Desk Manager との統合

CA Client Automation と CA Service Desk Manager を統合すると、CA Client Automation がサービス アウェア アプリケーションになります。つまり、CA Client Automation は、その管理対象アセットのいくつかのイベントをトリガして、CA Service Desk Manager にチケットを作成できます。

CA Service Desk Manager でのチケットの作成とワークフローは、サービス アウェア ポリシーによって制御されます。このポリシーは、問題タイプを一覧表にします。CA Client Automation では、問題タイプを使用して問題を分類し、作成するチケットを特定します。

CA Client Automation および CA Service Desk Manager は、統合の観点から、状況に応じた相互起動を可能にするグラフィカル ユーザ インターフェースが備えられています。

本章では、システム、セキュリティ、および認証などの側面のセットアップおよび設定について説明します。設定に関する考慮事項は、DSM ドメインマネージャおよびエンタープライズマネージャに適用されます。

CA Service Desk Manager の詳細 (たとえば問題タイプ) については、CA Service Desk Manager のドキュメントセットを参照してください。

このセクションには、以下のトピックが含まれています。

[サービス アウェア ポリシー](#) (P. 554)

[チケットの処理](#) (P. 555)

[検出されたアセットと所有アセットとの関連付け](#) (P. 556)

[Client Automation と CA Service Desk Manager の間のコンテキスト起動](#) (P. 556)

[CA Service Desk Manager から Client Automation へのコンテキスト起動](#) (P. 559)

[CA Service Desk Manager および Client Automation のセットアップ](#) (P. 560)

[CA Service Desk Manager のコンテキスト内起動の前提条件](#) (P. 560)

[複数のエンジンと CA Service Desk Manager 統合するための前提条件](#) (P. 561)

[エンタープライズマネージャと CA Service Desk Manager 統合するための前提条件](#) (P. 561)

[Client Automation と CA Service Desk Manager との統合について](#) (P. 561)

[CA Service Desk Manager Web サービスへのセキュア ログオン](#) (P. 562)

[設定ポリシー内の設定](#) (P. 566)

サービス アウェア ポリシー

Client Automation と CA Service Desk Manager との統合に関しては、ManagedAssetEvents という名前のサービス アウェア ポリシーが定義されています。サービス アウェア ポリシーは、CA Service Desk Manager のインストール時に自動的にインストールされます。Client Automation は、チケットの作成時に、このポリシーで利用できる問題タイプを利用します。

以下に、サービス アウェア ポリシーの主要パラメータを示します。

表示名:

管理対象アセットのイベント

コード:

MANAGED_ASSET_EVENTS

説明:

このサービス アウェア ポリシーは、Web サービスを介して管理対象アセットによって発行されたチケットを処理する場合に使用されます。

CA Service Desk Manager のデフォルトの問題タイプ以外に、サービス アウェア ポリシーには、以下の表に一覧表示される問題タイプが含まれています。CA Service Desk Manager 管理者は、これらの問題タイプを変更するか、または自分自身の問題タイプを使用してこのリストを拡張することができます。

問題タイプの表示名	問題タイプのコード	問題タイプの説明	プライオリティ (5 が最上位です)
アセット イベントベースのポリシー - 高	ASSET_EVENT_POLICY_H	管理対象アセットによって、4 優先順位が高いイベントベース ポリシー違反が検出されました。	
アセット イベントベースのポリシー - 中	ASSET_EVENT_POLICY_M	管理対象アセットによって、3 優先順位が中位のイベントベース ポリシー違反が検出されました。	
アセット クエリベースのポリシー - 高	ASSET_QUERY_POLICY_H	管理対象アセットによって、4 優先順位が高いクエリベース ポリシー違反が検出されました。	

問題タイプの表示名	問題タイプのコード	問題タイプの説明	プライオリティ (5 が最上位です)
アセット クエリ ベースのポリ シー - 中	ASSET_QUERY_POLICY_M	管理対象アセットによって、 優先順位が中位のクエリ ベース ポリシー違反が検出 されました。	3
ソフトウェア配 信障害 - 高	SW_DISTR_FAIL_H	Software Delivery ジョブに よって、優先順位が高い障害 が検出されました。	4
ソフトウェア配 信障害 - 中	SW_DISTR_FAIL_M	Software Delivery ジョブに よって、優先順位が中位の障 害が検出されました。	3
ソフトウェア配 信障害 - 低	SW_DISTR_FAIL_L	Software Delivery ジョブに よって、優先順位が低い障害 が検出されました。	2

チケットの処理

チケットは、ドメイン、およびエンタープライズ レベルで作成できます。以下に、チケットが作成される可能性のあるイベントを示します。

- ポリシー違反が検出されました。
- Software Delivery ジョブが失敗しました。
- 管理者が、コンピュータのコンテキストでポップアップ メニューからチケットをインタラクティブに作成しました。

膨大な量のチケットが作成されないようにするには、以下のルールを使用して、新しいチケットの作成を制限します。

- チケットは、ポリシーごとに 1 つだけ作成されます。チケットは、最初のポリシー違反が検出されたときに新しく作成されます。その後と同じポリシー違反が発生した場合は、そのチケットにログが追加されます。
- チケットは、ソフトウェア ジョブごとに 1 つだけ作成されます。チケットは、ソフトウェア ジョブの最初の失敗が検出されたときに、新しく作成されます。その後と同じソフトウェア ジョブの失敗が発生した場合は、そのチケットにログが追加されます。

チケットの処理の詳細については、CA Service Desk Manager のドキュメントを参照してください。

検出されたアセットと所有アセットとの関連付け

Client Automation では、検出されたアセット（たとえば、コンピュータやユーザ）のコンテキストでチケットが作成されます。チケットが作成されると、検出されたアセットは、CA Service Desk Manager で認識されている所有アセットにマップされます。これにより、CA Service Desk Manager 管理者は、チケットと所有アセットの間を移動して、その間の関係を報告することができます。

Client Automation と CA Service Desk Manager の間のコンテキスト起動

以下の表に、DSM エクスプローラまたは DSM Web コンソール、CA Service Desk Manager Web GUI との間でサポートされているコンテキスト起動の概要を示します。

From	To	該当するコンテキスト	コンテキスト
エクスプローラ/Web コンソール	CA Service Desk Manager Web GUI	ソフトウェア ジョブ	ジョブ障害発生時に作成 されるチケット
エクスプローラ/Web コンソール	CA Service Desk Manager Web GUI	アセット ポリ シー	ポリシー違反の発生時に 作成されるチケット
CA Service Desk Manager Web GUI	エクスプローラ/Web コ ンソール	チケットの詳細	ソフトウェア ジョブ
CA Service Desk Manager Web GUI	エクスプローラ/Web コ ンソール	チケットの詳細	アセット ポリシー

Client Automation から CA Service Desk Manager へのコンテキスト起動

Client Automation には、以下のコンテキストで CA Service Desk Manager を起動することのできるユーザインターフェースがあります。

- [ソフトウェア ジョブ障害](#) (P. 557)
- [アセット ポリシー違反](#) (P. 558)

ソフトウェア ジョブ障害のコンテキストでのチケット詳細

失敗して CA Service Desk Manager チケットを発行したソフトウェア ジョブでは、失敗したソフトウェア ジョブを右クリックすると、コンテキスト メニュー エントリ [Service Desk のチケットを開く] が表示されます。 [Service Desk のチケットを開く] を選択すると、CA Service Desk Manager Web GUI が起動します。



アセット ポリシー違反のコンテキストでのチケット詳細

ポリシーが CA Service Desk Manager 対応の場合、DSM エクスプローラの情報列に追加のハイパーリンク「関連する Service Desk のチケットを開く」が表示されます。このハイパーリンクを選択すると、このポリシーに違反したときに最初に生成されたチケットの CA Service Desk Manager チケット詳細画面が表示されます。



ポリシー 'Test'

DSM Explorer > GOOSE-GXS001-ドメイン > ポリシー > クエリベース > Test

名前	説明
アクション	違反時に実行するアクション
違反者	現在のポリシー違反者

情報

説明

ポリシーはクエリ 'Test' で評価し、2007/01/31 17:57:05 に最後に評価されました。

情報

関連する Service Desk チケットを開きます

タスク

- 無効
- 評価
- プロパティ

管理対象アセットのコンテキストでのチケット作成(一時)

CA Service Desk Manager チケットは、クイック起動ポートレットで「Service Desk のチケットの作成」アクションをクリックするとただちに作成されます。



クイック起動ポートレットは「ホームページ」タブにあり、DSM エクスプローラで管理されたアセットを選択すると表示されます。

アセットのコンテキスト メニューでは、「チケットの作成」もコマンドとして使用できます。

CA Service Desk Manager から Client Automation へのコンテキスト起動

DSM エクスプローラおよび Web コンソールは、個々の URL を介して、CA Service Desk Manager Web GUI から起動されます。

DSM エクスプローラまたは DSM Web コンソールを起動するハイパーリンクが、CA Service Desk Manager チケットのサマリ情報の「説明」フィールドに表示されます。

▼ 概要情報			
概要			アクティビティ時間の合計
アセット イベント ベースのポリシー - 高			00:00:00
説明			
2005/04/12 10:06 - GOOSE-GXS001 :: goose-gxs001 違反したポリシー: 'Test'			
オープン日/時間	最終変更日	解決日/時間	クローズ日/時間
2005/04/12 10:06 am	2005/04/12 10:06 am		

注: DSM エクスプローラは、dsmgui.exe コマンドを使用して起動されるため、このエクスプローラは、CA Service Desk Manager Web GUI を実行している CA Service Desk Manager マシンにインストールする必要があります。

CA Service Desk Manager および Client Automation のセットアップ

CA Service Desk Manager のセットアップは、Client Automation のサービス アウェア ポリシー、およびチケット作成用として事前定義されている問題タイプを自動的にインストールします。サービス アウェア ポリシーの名前は、**ManagedAssetEvents** です。事前定義されている問題タイプは、いつでも CA Service Desk Manager 管理者によって変更または拡張できます。

また、CA Service Desk Manager は、定義済みの権限セットを使用して設定されている、Client Automation のプロキシ アカウント **System_MA_User** を作成し、それをサービス アウェア ポリシーに関連付けます。

Client Automation セットアップは、CA Service Desk Manager との統合のための設定ポリシーを自動的に作成します。この設定ポリシーは、以下に示したパス名の下での共通設定（CCNF）マネージャにインストールされます。

/Default Computer Policy/DSM/Service Desk Integration/default

統合を可能にするには、Client Automation 管理者が共通設定マネージャの GUI を使用して、設定ポリシーをセットアップする必要があります。

設定ポリシー パラメータには、以下のエリアがあります。

- CA Service Desk Manager 統合が可能であるかどうかを示すスイッチ
- CA Service Desk Manager Web サービスへのセキュア ログオン パラメータ
- CA Service Desk Manager Web サービスへの URL

CA Service Desk Manager のコンテキスト内起動の前提条件

CA Service Desk Manager 統合では、DSM エクスプローラから CA Service Desk Manager Web GUI へのコンテキスト依存起動がサポートされています。これらの起動では、適切なアクセス許可が CA Service Desk Manager で付与されている必要があります。したがって、DSM エクスプローラにログインするときのユーザ アカウント（ユーザ ID およびパスワード）を CA Service Desk Manager におけるコンタクトとして作成する必要もあります。

Client Automation ユーザ アカウントが CA Service Desk Manager で認識されていない場合は、CA Service Desk Manager Web GUI を起動しようとする、ログイン画面が表示されます。

複数のエンジンと CA Service Desk Manager 統合するための前提条件

複数のエンジンを使用してポリシーを評価する場合は、エンジンが実行されているすべてのシステムに対して、**CA Service Desk Manager** 統合を起動しておく必要があります。つまり、これらの各システムで、以下の前提条件を満たしておく必要があります。

- エージェントがインストールされ、実行されていること。
- **CA Service Desk Manager** の統合を有効にする設定ポリシーが、このエージェントにドラッグアンドドロップされていること。
- .p12 証明書ファイルがインポートされていること（managed メソッドが使用される場合）。

エンタープライズ マネージャと CA Service Desk Manager 統合するための前提条件

エンタープライズ マネージャで **CA Service Desk Manager** 統合を起動するには、そのエンタープライズ マネージャで以下の前提条件を満たしておく必要があります。

- エージェントがインストールおよび実行され、リンクされているドメイン マネージャの 1 つに接続されていること。
- **CA Service Desk Manager** の統合を有効にする設定ポリシーが、このエージェントにドラッグアンドドロップされていること。
- .p12 証明書ファイルがインポートされていること（managed メソッドが使用される場合）。

Client Automation と CA Service Desk Manager との統合について

以下の考慮事項は、**Client Automation** と **CA Service Desk Manager** との統合シナリオに影響を与える可能性があるため、十分に理解しておく必要があります。

- [Service Desk が有効なエンタープライズ マネージャからの Software Delivery ジョブ](#) (P. 562)

Service Desk が有効なエンタープライズ マネージャからの Software Delivery ジョブ

以下の項目は、Client Automation と CA Service Desk Manager との統合がエンタープライズ マネージャで実行された場合のシナリオに適用されます。

エンタープライズ マネージャから起動され、Service Desk が有効になっているソフトウェア配信ジョブでは、DTS プラグインがエンタープライズ マネージャまたはドメイン マネージャ上で停止しているために Service Desk のチケットの作成に失敗した場合、Service Desk のチケットは作成されません。

CA Service Desk Manager Web サービスへのセキュア ログオン

Client Automation 管理者は、CA Service Desk Manager Web サービスにセキュア ログオンするための方法として、ユーザ名とパスワードが要求される簡単なログオン方式（非管理方式）と公開鍵/秘密鍵および eTrust PKI 暗号化に基づいた管理ログイン方式のうちのいずれかを選択できます。

- ユーザ名とパスワードが要求される単純なログオン方式（非管理方式）
- 公開/秘密鍵および eTrust PKI 暗号化に基づいた管理ログイン方式

ユーザ名/パスワードおよび公開鍵/秘密鍵認証は、すぐに使用できるわけではありません。CA Service Desk Manager および Client Automation の両方が正常にインストールされた後に、個別の設定ステップが必要になります。

セキュア ログオン方式は、Client Automation 設定ポリシー（comstore）内の `sdlogonmanaged` パラメータを使用して指定されます。このパラメータのデフォルト値は、Managed です。つまり、eTrust PKI に基づく証明書と暗号化/復号化によってログオンが行われます。値が Notmanaged の場合は、ユーザはユーザ名とパスワードを使用してログインします。

セキュア ログオンの設定方法

セキュア ログオンを設定するには、**Client Automation** 管理者が以下の設定手順を実行する必要があります。

1. 認証方法を選択します。
2. 非管理方式を選択した場合は、以下の手順に従います。
 - **CA Service Desk Manager** に対し、個別のオペレーティング システム アカウントを作成します。
 - 作成したアカウントに応じて、設定ポリシーを使用して **Client Automation** を設定します。
3. 管理方式を選択した場合は、以下の手順に従います。
 - 秘密鍵を使用して **X.509** 証明書を作成し、それを **PKCS#12** ファイルを使用して公開します。管理者は、**CA Service Desk Manager** ユーティリティ **pdm_pki** をこの目的に使用するか、または自分自身の証明書を提供できます。
 - **Client Automation** ユーティリティ **cacertutil** を使用して、作成されたポリシー ファイルを **<adsm>** にインポートします。

ユーザ名とパスワードによる方式(非管理)

ユーザ名とパスワードには、それぞれ設定ポリシーのパラメータ `sdusr` と `sdpwd` が使用されます。

CA Service Desk Manager セットアップは、Client Automation が使用するコンタクト `System_MA_User` を自動的にロードして、これを Client Automation サービスウェア ポリシー `ManagedAssetEvents` に関連付けます。

すなわち、`sdusr` のデフォルト値は `System_MA_User` になります。

ログイン方式としてユーザ名とパスワードを有効にするには、CA Service Desk Manager 管理者が、以下のアクションを実行する必要があります。

- オペレーティングシステム ユーザを作成します。
- `System_MA_User` のコンタクトを編集し、オペレーティングシステム ユーザ名を [システム ログイン名] フィールドに挿入します。
(システム ログインは、デフォルトでは `System_MA_User` と同じになります。)

Client Automation 管理者は、Client Automation 設定ポリシーを、CA Service Desk Manager に作成された該当するコンタクト名およびパスワードに更新する必要があります。

管理者は、`System_MA_User` とは異なるコンタクトを作成して、それを使用することができます。したがって、管理者は、CA Service Desk Manager 内の設定および Client Automation 設定ポリシーを変更した場合は、それらを同期させる必要があります。

証明書または eTrust PKI 方式(管理)

CA Service Desk Manager セットアップは、Client Automation が使用するコンタクト `System_MA_User` を自動的にロードして、このコンタクトを Client Automation Service Aware ポリシー `ManagedAssetEvents` に関連付けます。

証明書 (eTrust PKI) をログイン方式として使用するには、CA Service Desk Manager 管理者が以下の 2 つのステップを実行する必要があります。

- [PKCS#12 ファイルを作成します](#) (P. 565)。
- [PKCS#12 ファイルを Client Automation 設定ファイルにインポートします](#) (P. 566)。

PKCS#12 ファイルの作成

管理者は、PKCS#12 ファイルを介して自分自身の鍵を提供できます。たとえば、管理者はサードパーティの認証局をこの目的に使用することができます。

PKCS#12 ファイルを作成するには、CA Service Desk Manager ユーティリティ（コマンド）`pdm_pki` を使用して、以下の手順を実行します。

1. 公開鍵と秘密鍵のペアを作成します。
2. 公開鍵を CA Service Desk Manager データベース内の Client Automation ポリシーに関連付けます。
3. 秘密鍵を使用して X.509 証明書を作成し、それを PKCS#12 ファイルを使用して公開します。

`pdm_pki` ユーティリティは、PKCS#12 ファイルを `MANAGED_ASSET_EVENTS.p12` というファイル名で、その作業ディレクトリ内に作成します。

`pdm_pki` コマンドのフォーマットは、以下のとおりです。

```
pdm_pki -p MANAGED_ASSET_EVENTS [-l certificate_file] [-f]
```

`-p`

ポリシー コードを定義します。この場合、値 `MANAGED_ASSETS_EVENTS` を使用する必要があります。

`-l`

証明書を新しく作成するのではなく、ファイルからロードします。

`-f`

既存の鍵を強制的に置き換えます。

Client Automation 設定ファイルへの PKCS#12 ファイルのインポート

PKCS#12 ファイルを Client Automation 設定ファイル（comstore）にインポートするには、以下の方法で示すように Client Automation ユーティリティ **cacertutil** を使用します。

PKCS#12 ファイルを Client Automation 設定ファイル（comstore）にインポートするための **cacertutil** コマンドのフォーマットは、以下のとおりです。

```
cacertutil import -i:certificate_file  
                  -ip:MANAGED_ASSET_EVENTS -t:MANAGED_ASSET_EVENTS  
                  -l:global
```

-i

証明書ファイルの名前を指定します。

-ip

パス フレーズを指定します。

-t

識別タグを指定します。

-l

ユーザを指定します。

設定ポリシー内の設定

CA Service Desk Manager 統合のための設定は、Client Automation 設定ファイル（comstore.xml）のパラメータ セクション **sdintegration** で指定されます。この設定ファイル内のパラメータは、共通設定（CCNF）ポリシーを使用して集中管理されるようにセットアップされます。

以下のパラメータが、CA Service Desk Manager 統合に使用されます。

SdlsEnabled

CA Service Desk Manager 統合が可能であるかどうかを示します。
SdlsEnabled の値が **True** の場合、CA Service Desk Manager 統合は可能です。この値が **False** の場合は、統合できません。

デフォルト：False

SdEnd

CA Service Desk Manager Web サービスへの URL を示します。

デフォルト : `http://myhost:8080/axis/services/USD_R11_WebService`

myhost は CA Service Desk Manager Web サービスの適切なサーバアドレスに置き換えてください。ポート 8080 が初期設定です。

SdLogonManaged

CA Service Desk Manager Web サービスへのログオンの制御方法を示します。この値が **Managed** の場合、ログオンは **PKCS#12** 証明書を介して制御されます。この値が **Notmanaged** の場合は、ログオンはユーザアカウントとパスワードを介して制御されます。

デフォルト : **Managed**

SdUsr

CA Service Desk Manager Web サービスにログオンするためのユーザアカウントを定義します。このパラメータは、**SdLogonManaged** が **Notmanaged** に設定されている場合にのみ使用されます。

デフォルト : **System_MA_User**

SdPwd

CA Service Desk Manager Web サービスにログオンするためのパスワードを定義します。このパラメータは、**SdLogonManaged** が **Notmanaged** に設定されている場合にのみ使用されます。

注: **SdUsr** アカウントに加えて、現在ログオンしているユーザのアカウントが重要です。管理対象アセットとの関係で、**DSM** エクスプローラ GUI から一時的チケットが作成された場合、このアカウントは **CA Service Desk Manager** 内でチケットの作成者として参照されます。チケットが **Asset Management** または **Software Delivery** との関連で作成された場合は、チケットの作成者は常に管理者になります。

デフォルト : 空

SdPolicy

ログイン先の **CA Service Desk Manager** サービス アウェア ポリシーの名前を示します。このパラメータは、**SdLogonManaged** が **Notmanaged** に設定されている場合にのみ使用されます。管理ログオンで使用される **PKCS#12** 証明書には、常にこの値よりも優先されるポリシーの記述がすでに含まれています。このパラメータを指定しなかった場合は、デフォルトの **CA Service Desk Manager** ポリシーが選択されます。

デフォルト : **MANAGED_ASSET_EVENTS**

SdThrottle

ネットワークおよび CPU のスロットリングが有効かどうかを指定します。この値が **True** の場合、スロットリングが有効です。この値が **False** の場合、スロットリングが無効です。

デフォルト : False

SdTimeout

CA Service Desk Manager Web サービスの呼び出しのタイムアウトを指定します。この値は、送信、受信、および接続時に強制的にタイムアウトになるように変更することができます。正の値は、タイムアウトになるまでの秒数を示します。たとえば、値が **20** の場合は、**20** 秒後にタイムアウトになることを指定します。負の値は、ミリ秒を示します。たとえば、値が **-200** の場合は、**200** ミリ秒後にタイムアウトになることを指定します。

デフォルト : 0 (無限)

第 14 章：トラブルシューティング

このセクションには、以下のトピックが含まれます。

CIC 接続の解放エラー

CA Content Import Client (CIC) が Oracle MDB への接続の解放に失敗し、CIC ログに以下のエラーが表示される場合があります。

```
[CCMain] WARN [com.ca.sccc.dbm.CCDBManager] - Failed to uninitialized MDB connection pool for domain 'xxx'
```

Oracle MDB でのコンテンツ ダウンロードが失敗します

症状

Oracle MDB でのコンテンツ ダウンロード ジョブが、ドメイン マネージャやエンタープライズ マネージャでの新規インストールの後で失敗し、CIC ログには次のエラーが記録されます。

ORA-00604 : 再帰 SQL レベルでエラーが発生しました

ORA-01000 : 最大オープン カーソル数を超過しました

解決方法

開いているカーソルの数が Oracle データベースで定義されている最大限度を超えている場合、コンテンツ インポート クライアントの実行中にこれが発生します。

開いているカーソルの上限をデフォルトの 50 よりも高い値に変更できます。

Oracle MDB で以下を実行します。

```
ALTER SYSTEM SET open_cursors = 1000 SCOPE=BOTH;
```

これにより、開いているカーソルの上限が 1000 に設定されます。

注: 上限により、カーソルを CIC の必要に応じて開き、終了後に閉じることができます。

データベースが停止されると DSM エンジンがクラッシュする

症状

メンテナンス（バックアップの取得など）のためにデータベースを停止すると、エンジンプロセスがクラッシュする場合があります。

解決方法

メンテナンスのためにデータベースを停止する前に、すべてのエンジン プロセスを停止したことを確認します。

注: データベースのメンテナンス中にエンジン プロセスがクラッシュした場合は、データベースを再起動した後にエンジン プロセスを再起動してください。

Windows 8 および 8.1 での SXP パッケージャ用前提条件

コンピュータ上で SXP パッケージャを使用してパッケージの作成を試みた場合は、以下の手順を使用して、.NET Framework 3.5 が Windows 8 または Windows Server 2012 コンピュータにインストールされ、有効になっていることを確認します。

Windows 8 および 8.1:

[コントロール パネル] - [プログラム] - [Windows 機能の有効化または無効化] をクリックします。詳細については、
<http://msdn.microsoft.com/en-us/library/hh506443.aspx> を参照してください。

Windows Server 2012 および Windows Server 2012 R2:

[役割と機能の追加] ウィザードを使用して .NET Framework 3.5 をインストールします。詳細については、
<http://technet.microsoft.com/en-us/library/hh83180.aspx> を参照してください。

エクスポートされたレポートを開く

エクスポート ファイルは、Unicode 形式です。Unicode をサポートしないアプリケーションでファイルを表示するには、ファイルを開く前に ANSI にエンコーディングを変更します。

Alert Collector が指定されたマネージャの接続に失敗する

症状:

Alert Collector のインストール中に、Alert Collector のステータス コマンドを実行する場合、Alert Collector は以下の内容のメッセージを表示します。

指定されたマネージャに接続できません。

解決方法:

EM または DM のいずれかに接続するように設定され、マネージャへの接続に失敗するスタンドアロン サーバに Alert Collector をインストールする場合。Alert Collector は、マネージャ タイプ (EM か DM か) を確認するため、初回はマネージャに接続します。無効なロールが指定されている場合、指定されたロールを検証し、デフォルトのロールに切り替えるためにマネージャ タイプが使用されます。

CAF がスタンドアロン サーバおよびマネージャで実行され、動作するかどうかを確認します。Alert Collector は必要な情報を取得し、正しく動作します。Alert Collector のマネージャが変更され、Alert Collector が再度起動される場合、このステータス メッセージが表示されます。問題を修正するために同じ手順が適用されます。

Alert Collector がデータベースへの接続に失敗する

症状:

Alert Collector にアラートをアップロードするとき、WAC にアップロードされたアラートが表示されません。AlertCollector ステータス コマンドを使用すると、以下のメッセージが表示されます。

データベースへの接続を確立できません。

解決方法:

データベース サーバの接続性を確認、または関連する 32 ビット DB クライアント ツール (SQL または Oracle クライアントなど) をマシンにインストールすることにより、スタンドアロン サーバ上の Alert Collector がデータベースに接続されることを確認します。

ミーティング モード接続で DSM エクスプローラにプロンプト ウィンドウが表示されない

症状

ドメイン マネージャで DSM エクスプローラを開き、エージェントを右クリックしてミーティング モード接続を確立しても、アプリケーションにプロンプト ウィンドウが表示されません。

解決方法

エージェントに libatk-1.0.so.0 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。

クラスタ セットアップでブート サーバ設定を tftp から共有アクセス モードに変更した場合の問題

症状

クラスタ セットアップで、ブート サーバ設定を tftp から共有アクセス モードに変更すると、以下の内容のエラーが発生します。

エラー: camenu 共有を作成しようとしていますエラー: sxpsetup 共有を作成しようとしています

解決方法

リモート スケーラビリティ サーバを設定することにより、Client Automation アプリケーション クラスタでブート サーバ設定として共有アクセス モードをエラーなしで設定できます。

プログラムの追加/削除での ITCM および CIC コンポーネントのサイズ詳細に関する問題

症状:

Client Automation リリース 12.9 をインストールまたはアップグレードした後、[コントロールパネル] の [プログラムの追加と削除] に、Client Automation、Content Import Client (CIC)、Patch Manager、その他の Client Automation コンポーネントの推定サイズが表示されません。

解決方法:

[コントロールパネル] の [プログラムの追加と削除] でサイズを取得して表示することは、InstallShield ではなく Windows OS の機能です。この動作は、Microsoft が Windows での推定サイズの計算方法を変更したために発生します。インストール済みの各コンポーネントの推定サイズは、OS アルゴリズムを使用して計算されます。このアルゴリズムは、Windows のバージョンごとに異なる可能性があるため、Client Automation の推定サイズの表示に影響があります。

推定サイズが表示されるようにするには、以下の手順に従います。

次の手順に従ってください:

Microsoft は、[プログラムの追加と削除] に推定サイズを表示するために EstimatedSize レジストリ キーを排他的に使用します。推定サイズを読み込むには、EstimatedSize レジストリ キー

(HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥{PRODUCT_CODE}) を手動で編集します。詳細については、Microsoft のドキュメントを参照してください。

テクニカル サポートへの接続におけるエラーおよび遅延

症状:

Client Automation のバージョン情報画面からテクニカル サポート ページにアクセスしようとすると、しばらくの遅延の後にスクリプト エラーが表示されます。

解決方法:

[はい] を押すと、しばらくの遅延の後にテクニカル サポート ページが表示されます。なお、この遅延は、Internet Explorer 7 固有のものです。

Client Automation コンポーネントの SE-Linux によるサポート

SE-Linux セキュリティ システムが有効になっている Linux システムには、以下の Client Automation コンポーネントに関する固有の SE-Linux 設定が必要です。

DSM Web サービスおよび Web コンソール

Client Automation Web サービスおよび Web コンソールのインストールは、SE-Linux が **enforcing** モードに設定されているシステムでも成功します。ただし、これらのコンポーネントを使用するには、以下の方法で **permissive** モードに切り替えてください。

次の手順に従ってください：

- テキスト エディタで、ファイル「/etc/selinux/config」を開きます。
- フラグ **SELINUX=enforcing** を **SELINUX=permissive** に変更します。
- システムを再起動します。

日本語版のインストーラの UI に意味のない文字が表示されます。

日本語版 Linux が該当

症状：

Linux 上で日本語でインストーラを起動すると、UI に意味のない文字が表示されます。

解決方法：

製品インストーラをコマンドライン モードで起動するか、応答ファイルによるサイレントインストールを実行してください。

コマンドプロンプトの文字列に関する問題

Windows および Linux が該当

症状:

ローカライズされた環境でコマンドを実行すると、コマンドプロンプトの文字列に関する問題が発生します。

解決方法:

コマンドプロンプトの文字列に関する問題を解決するには、以下の変更を実行します。

(Windows の場合)

この問題は、環境のデフォルト コード ページがサポートされていない場合に発生します。

たとえば、ドイツ語およびフランス語のデフォルト コード ページが **850** である場合、コマンドプロンプトの文字列が正常に表示されません。ドイツ語およびフランス語については、**Client Automation** がコード ページ **1252** をサポートすることに注意してください。以下のコマンドを実行することにより、環境設定のコード ページを設定しなおすことができます。

```
chcp 1252
```

(Linux の場合)

以下の方法で、言語パラメータを設定しなおすことができます。

1. `cd %etc%\sysconfig` フォルダに移動し、`i18n` を開きます。
2. 以下の方法で、`Lang` パラメータを変更します。

例:

(ドイツ語の場合) `Lang=de_DE.UTF-8`

(フランス語の場合) `Lang=fr_FR.UTF-8`

新しい 64 ビット版 Linux OS での共有ライブラリのロード時に発生するエラー

症状:

一部の DSM 機能（cfSysTray、リモート制御接続、DSM プロパティなど）が、新しい 64 ビット版 Linux オペレーティングシステムで正常に機能しません。たとえば、cfSysTray を実行すると、以下のエラーメッセージが表示されます。

```
[root@hostname]# cfsysTray show
cfSysTray: error while loading shared libraries: libgtk-x11-2.0.so.0: wrong ELF class: ELFCLASS64.
```

解決方法:

DSM は 32 ビット アプリケーションであり、32 ビットバージョンの OS ライブラリが必要です。64 ビット版 Linux オペレーティングシステムには 32 ビットバージョンの OS ライブラリが含まれないため、DSM コマンドは失敗します。デフォルトでは、これらのライブラリが、新しい 64 ビット版 Linux オペレーティングシステムにインストールされません。

必要なライブラリをインストールする方法については、[CA サポート](#)を参照するか、システム管理者にお問い合わせください。

Solaris 上でエージェントをインストールするとエラーが発生して失敗する

症状:

Solaris 10 でエージェントをインストールすると失敗し、ログ ファイルに以下のエラーが書き込まれます。

```
ld.so.1: setup: fatal: libCstd.so.1: version `SUNW_1.4.2' not found (required by file
/opt/CA/DSM/capki/setup)
ld.so.1: setup: fatal: libCstd.so.1: open failed: No such file or directory Killed
/opt/CA/DSM/capki/setup install caller=CAITCM verbose env=all failed with return code
= 137
11:43:58 !! Script executed with error: 137
Script or command "capki/pkiInst" failed with exit code 137.
Reason:The script or command encountered a problem.
Action: Find further details in the installation log file
/opt/CA/SharedComponents/installer/log/ca-dsm.log.
```

解決方法:

Solaris 10 でのエージェントのインストールは、libCstd ライブラリ バージョンに互換性がないために失敗します。この問題を解決するには、Solaris OS パッチ 119964-12 以降をインストールします。

Windows 8 および 8.1 のセキュア モードでのリモート制御

症状:

Windows 8、Windows 8.1、Windows Server 2012 および Windows Server 2012R2 上のリモート制御では、セキュア コントロール モード以外の接続モードがすべてサポートされます。

解決方法:

現在、解決方法を準備中であり、次回のメジャー リリースで実装される予定です。

MDB に接続できない

症状:

CIC のインストール中に以下のエラー メッセージが表示され、インストーラが停止します。

Unable to Connect to MDB. Please check MDB credentials.

解決方法:

MDB 認証情報がパスワード ポリシーに準拠していることを確認します。CIC では、MDB パスワードに英数字および以下の特殊文字を使用できます。

SQL

~!#\$*()_+ -{ } [] ? / @

Oracle

\$ _

- MDB パスワードをリセットすると、インストーラは正常に実行されます。

MS-SQL および Oracle データベースのパスワード ポリシーの詳細については、それぞれの会社の Web サイトを参照してください。

CAM のアップグレードの後、DSM マネージャが起動に失敗する

Client Automation をインストールする場合、CA Message Queuing (CAM) は通常、インストール処理中にアップグレードされます。CAM に接続できないために DSM マネージャが起動に失敗する場合は、現在実行されているバージョンの CAM を停止するか、または Client Automation のインストールの後に再起動します。

一時フォルダ内のログが削除される

症状

リモート デスクトップ サービスが設定されているコンピュータに **Client Automation** をインストールすると、ユーザがログオフした後か、またはマシンが再起動されたときに、一時フォルダ内のログが削除されます。

解決方法

以下の手順に従います。

- 対象のコンピュータの [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホスト] - [終了時に一時フォルダを削除しない] を選択します。
 - ステータスが [有効] に設定されている場合は、ユーザがセッションからログオフしたとき、ユーザのセッションごとの一時フォルダは保持されます。
 - ステータスが [無効] に設定されている場合は、管理者が **Remote Desktop Session Host Configuration** ツールで他の設定を指定している場合でも、ユーザがログオフすると一時フォルダは削除されます。
 - ステータスが [未設定] に設定されている場合は、サーバ管理者によって他の設定が指定されていない限り、リモート デスクトップ サービスはログオフ時にリモート コンピュータから一時フォルダを削除します。

注: リモート デスクトップ サービスのパスは、OS のバージョンによって異なります。

ORACLE_HOME 変数または ca_itrm パスワードが誤って設定されている場合、MDB インストーラがハングアップする

ORACLE_HOME 環境変数が誤って設定されている場合は、自動インストール、再インストール、またはアップグレード中に **MDB** インストーラがハングアップします。ORACLE_HOME 変数を正しく設定するか、またはこの環境変数の値を削除します。それにより、ORACLE_HOME の値が応答ファイルから取得されます。

再インストールまたはアップグレード（インタラクティブと自動の両方）中に正しくない **ca_itrm** パスワードを入力した場合は、**MDB** インストーラがハングアップします。正しい **ca_itrm** パスワードが入力されていることを確認します。

名前付きインスタンスおよびポート ID によるインストール エラー

名前付きインスタンスおよびポート ID プロパティのために、Microsoft SQL Server でインストールエラーが発生する場合があります。正しいポート ID を指定したことを確認します。

応答ファイルに未使用のエントリが含まれている

生成された応答ファイルと install.rsp テンプレートには、ITRM_DBSQLPORT=1433 および ITRM_SQLADMINUSER=sa の Microsoft SQL エントリが含まれています。これらのエントリは未使用であり、MDB インストーラによって無視されます。

SQL MDB から Oracle MDB ターゲットへの同期エラー

症状

SQL サーバ上の MDB を含むソースから Oracle 11g 上の MDB を含むターゲットへの同期を実行すると、ITCM R12.5 SP1 のエンジン ログに以下のエラーが表示されます。

```
Reclmpl_Ado |Reclmpl_Ado.cpp |001371|ERROR | FieldLng encounters an undefined VT type =5 for 14
```

```
Reclmpl_Ado |Reclmpl_Ado.cpp |001373|ERROR | FieldLng encounters an undefined VT type =0
```

解決方法

テスト修正 RO43621 を適用します。テスト修正の Readme の指示に従います。

Oracle 上のターゲット MDB での同期エラー

症状

Oracle 上のターゲット MDB との同期を実行すると、エンジン ログ ファイルに以下のエラー メッセージが表示されます。

```
ERROR | ERROR:OCISmtExecute() failed
```

解決方法

テスト修正 **RO43619** を適用します。テスト修正の **Readme** の指示に従います。

これを解決するには、パッチ番号 **RO43619** を適用する必要があります。パッチを適用する方法の詳細については、**CA** サポートサイトで **RO43619** のソリューション ドキュメントを参照してください。

スタンドアロン WAC 上で Web コンソールからの統合ログオンが失敗する

症状

Windows 2008 以降で、サポートされているブラウザから Web コンソールの統合ログオン機能にアクセスすると、ログインが失敗し、明示的なログオンを実行するよう求められます。

解決方法

以下の手順に従います。

- ドメイン コントローラが Windows 2008 以降で動作しており、以下のローカル ポリシー設定が指定されていることを確認します。
 - Network access: Sharing and security model for local accounts: Classic
 - Network access: LAN manager authentication level: Send LM and NTLM Responses
 - Network security: Verify that the minimum session security for NTLM SSP based (including secure RPC) clients is set to 'no minimum'
- ドメイン マネージャが Windows 2008 以降で動作していることを確認し、手順 1 で指定されているローカル ポリシーを設定します。
- ドメイン マネージャのレジストリが Windows 2008 以降で動作していることを確認し、ループバックのチェック ボックスを無効にします。

以下の手順に従います。

 - 「開始」 - 「実行」 をクリックします。
 - 「regedit」と入力します。 「OK」 をクリックします。
 - レジストリ エディタで、以下のレジストリ キーを見つけてクリックします。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
 - 「LSA」 を右クリックし、 「新規」 をポイントします。 「DWORD 値」 をクリックします。
 - 「DisableLoopbackCheck」と入力します。 Enter キーを押します。
 - 「DisableLoopbackCheck」 を右クリックします。 「修正」 をクリックします。
 - 「値のデータ」 ボックスに 「1」 と入力します。 「OK」 をクリックします。
- ユーザのボックスでブラウザ（IE または Firefox） の設定を確認します。

注: 統合ログオンのためのブラウザ設定の詳細については、「**Web** コンソールヘルプ」にある「統合ログオンのブラウザ設定」のトピックを参照してください。

5. ブラウザがサーバクラスのマシンで動作している場合は、手順 1 で指定されているローカルポリシー設定に従います。

DSM マネージャのアップグレードの後の高い CPU 使用率

症状:

DSM マネージャを現在のリリースにアップグレードした後、Tomcat 7 および JRE 1.7 で実行される古い暗号モジュールにより、CPU 使用率は高くなります。

解決方法:

DSM マネージャでのみ ITCM をアップグレードし、Patch Manager はアップグレードしていない場合、この問題が発生します。Patch Manager を現在の ITCM リリースにアップグレードします。

Windows 2012 仮想マシンが含まれている場合はインフラストラクチャ展開に失敗する

症状:

Windows 2012 仮想コンピュータ内に以下のいずれかが含まれている場合、インフラストラクチャ展開は失敗します。

- ドメイン マネージャ
- スケーラビリティ サーバ
- ターゲット コンピュータ

解決方法:

VMware ナレッジ ベースのエントリに従います: 「Possible data corruption after a Windows 2012 virtual machine network transfer (2058692)」 (英語)

Oracle 12.1.0.1 32bit Windows Client を使用したハードウェア インベントリの収集ができません

症状:

Oracle Server 12c で MDB と共に Client Automation がインストールされていて、Oracle 12.1.0.1 32bit Windows Client がデータベースへの接続に使用されていると、ハードウェアがドメイン マネージャで収集されないか、エンタープライズ マネージャで複製されません。

解決方法:

Oracle クライアントの場所で oraodm12.dll ファイルが使用できない場合にこれが発生します。

次の手順に従ってください:

1. Oracle サポート サイトからファイル oraodm12.dll をダウンロードします。
2. このファイルを以下の場所にコピーします。

<12.1_ORACLE_CLIENT_Location>%bin%

詳細については、Oracle サポート サイトの文書 ID 1593348.1 を参照してください。

付録 A: 自動化サービス設定ファイル

自動化サービス設定ファイルには、自動マイグレーションがさまざまなタスクに使用する設定パラメータが含まれています。このセクションではすべてのパラメータについて説明しますが、いくつかのパラメータは情報提供のみ行います。情報提供のみのパラメータを変更しないことをお勧めします。

注: `automation.config` ファイル内の整数値には、スペースを含めることができません。また、整数値をスペースで囲むことができません。`automation.config` ファイルで整数値を指定する場合は、値内および値の周囲にスペースがないことを確認します。整数値内にスペースが含まれると、自動化サービスが誤動作する場合があります。

AssessmentServiceEPR

評価サービスのエンドポイント URL を定義します。このパラメータは単なる通知用です。

ITCMEPR

CA ITCM Web サービスのエンドポイント URL を定義します。このパラメータは単なる通知用です。

ITPAMEPR

CA IT PAM Web サービスのエンドポイント URL を定義します。このパラメータは単なる通知用です。

AutomationServiceEPR

自動化サービスのエンドポイント URL を定義します。このパラメータは単なる通知用です。

JNI_BIN_PATH

`comstore` 値を取得するために JNI パスを定義します。このパラメータは単なる通知用です。

DEFAULT_MANAGER

Web コンソールおよび CA ITCM Web サービスのデフォルト マネージャの名前を定義します。このパラメータは単なる通知用です。

WipeAndReloadProcess

ワイプと再ロードマイグレーションの CA IT PAM プロセス定義へのパスを定義します。プロセス定義をカスタマイズしている場合のみ、このパラメータを変更します。

MachineReplacementProcess

マシン置換マイグレーション用の CA IT PAM プロセス定義へのパスを定義します。プロセス定義をカスタマイズしている場合のみ、このパラメータを変更します。

MaxNumberOfITPAMInstances

自動化サービスが同時に実行できる CA IT PAM インスタンスの最大数を定義します。CA IT PAM サーバが処理できる負荷に応じて、この値を変更します。

注: 自動化サービスは、マイグレーション ジョブのコンピュータごとに、1 つの CA IT PAM インスタンスを作成します。

ProcessLaunchInterval

CA IT PAM インスタンスの作成間の時間間隔（秒単位）を定義します。

TimeOutForOSIMJobs

コンピュータが OSIM ジョブを開始する必要がある期間である、タイムアウト期間（秒単位）を定義します。タイムアウト期間の後、OSIM ジョブがキャンセルされ、コンピュータの OS マイグレーション ジョブが失敗します。

WaitForBootServer

ブート サーバがターゲットを取得し、ドメイン マネージャに報告するまで、OS インストールの起動が待機することを指定します。

WaitForOSImage

割り当てられたブート サーバ上で必要な OS およびブート イメージが使用可能になるまで、OS インストールの起動が待機することを指定します。

WakeOnLAN

OS インストールの前に、ブート サーバがターゲット コンピュータを起動するかどうかを指定します。

Reboot

True に設定した場合に、インストールを起動する前にブート サーバがターゲット コンピュータに再起動を強制するかどうかを指定します。

ContainerPriority

マイグレーション ジョブ用に作成されたソフトウェア ジョブ コンテナの優先度を定義します。

DeliveryCalender

使用する配信カレンダーの名前を指定します。配信カレンダーを使用しない場合は、このパラメータを空白のままにしておきます。

IgnoreJobCalendarsOnTargetComputers

RAC コンテナの作成時に、ジョブ オプション [ターゲット コンピュータ上のジョブ カレンダーを無視する] を設定するかどうかを指定します。このポリシーを [いいえ] に設定すると、カレンダーはターゲット コンピュータで無視されません。[はい] に設定すると、カレンダーはターゲット コンピュータで無視されます。

JobsTriggerSS

スケジュールされた時間に、スケーラビリティ サーバがジョブを開始して実行するかどうかを指定します。

RemoveInstallationHistory

既存のインストール記録を削除して、インストール プロセスが起動される前にジョブが「インストール済み」のステータスで失敗するのを防止するかどうかを指定します。

RunFromSS

ジョブの実行中に、ターゲット コンピュータのジョブ確認プログラムがサーバとの通信をリリースするかどうかを指定します。ジョブが終了したとき、ジョブのステータスをレポートするために、エージェントとサーバが再接続されます。

TimesRelativeToEM

指定した起動時間をユニバーサル時間として解釈するかどうかを指定します。各ドメイン マネージャで設定された時間偏差は、受信した時間をローカル システム時間に変換するものと見なされます。

UseDeliveryCalender

配信カレンダーをジョブに使用するかどうかを指定します。

SoftwareBlackList

OS マイグレーション ジョブからコンピュータを除外するために使用される、ソフトウェア パッケージのリストを定義します。これらのいずれかのソフトウェア パッケージがインストールされているコンピュータは、OS マイグレーションから自動的に除外されます。

MaximumDelayOfJobContainer

コンテナを封印する前に、最初のコンピュータを追加した後、追加のコンピュータのためにジョブ コンテナが待機する時間を定義します。必要に応じて、追加のコンテナが自動的に作成されます。

MaxNumberOfTargetsPerJobContainer

ジョブ コンテナごとにターゲット コンピュータの最大数を定義します。ジョブ コンテナがこの制限に到達すると、コンテナが閉じられ、残りのコンピュータに対して新しいジョブ コンテナが作成されます。

LastTargetInContainerOptimization

マイグレーション ジョブにターゲットが残されていない場合、ジョブ コンテナをただちに起動するかどうかを指定します。コンテナは、コンテナ内のターゲット数が **MaxNumberOfTargetsPerJobContainer** で指定した数より少ない場合でも、**MaximumDelayOfJobContainer** の時間まで待機することなく、ただちに起動されます。このパラメータは単なる通知用です。

デフォルト： はい (True)

RenamePackageName

コンピュータの名前変更を使用される名前変更ソフトウェア パッケージを定義します。このパラメータは単なる通知用です。

RenamePackageVersion

コンピュータの名前変更を使用される名前変更ソフトウェア パッケージのバージョンを定義します。このパラメータは単なる通知用です。

RenameProcedure

コンピュータの名前変更を使用される名前変更ソフトウェア パッケージ プロシージャを定義します。このパラメータは単なる通知用です。

AutomationJobScheduleInterval

次の自動化ジョブをスケジュールする前に、自動化サービスが待機する遅延時間（秒単位）を定義します。

AutomationJobSchedulerBatchSize

スケジュールされたターゲットの **ITPAM** インスタンス ステータスを確認する前に、自動化サービスによってスケジュールされるターゲットの数を定義し、ステータスを「マイグレーションに成功しました」または「マイグレーションに失敗しました」に更新します。**CA IT PAM** サーバに対する負荷、およびターゲットのステータスを更新する頻度に応じて、この値を変更できます。

Log4j Properties

以下の log4j プロパティを定義します。

- log4j.rootLogger
- log4j.appender.A1

- `log4j.appender.A1.layout`
- `log4j.appender.A1.layout.ConversionPattern`
- `log4j.appender.A1.MaxFileSize`
- `log4j.appender.A1.MaxBackupIndex`

たとえば、以下のパラメータを変更して、ログ レベル、ファイル サイズ、または作成されるログ ファイル数を変更できます。

`log4j.rootLogger=ERROR, A1`

注: この値を `DEBUG` または `INFO` に変更し、それに応じてログ レベルを変更します。

`log4j.appender.A1.MaxFileSize=5000KB`

`log4j.appender.A1.MaxBackupIndex=1`

注: Log4j プロパティの詳細については、`org.apache.log4j.PropertyConfigurator` のドキュメントを参照してください。

付録 B: CA Client Automation で使用される ポート

以下の表に、各種 **DSM** コンポーネントのポート使用状況の詳細を示します。これらの表は包括的で、各コンポーネントの全体像を明らかにするため、重複があります。

このセクションには、以下のトピックが含まれています。

- [ポート使用に関する一般的な考慮事項](#) (P. 594)
- [エンタープライズ マネージャで使用されるポート](#) (P. 595)
- [ドメイン マネージャで使用されるポート](#) (P. 596)
- [インフラストラクチャ展開で使用されるポート](#) (P. 599)
- [スケーラビリティ サーバで使用されるポート](#) (P. 601)
- [ブート サーバで使用されるポート](#) (P. 603)
- [エンジンで使用されるポート](#) (P. 604)
- [エージェントで使用されるポート](#) (P. 605)
- [パッケージで使用されるポート](#) (P. 607)
- [DSM エクスプローラおよび Reporter で使用されるポート](#) (P. 608)
- [ENC ゲートウェイが使用するポート](#) (P. 609)
- [AMT アセットの隔離が使用するポート](#) (P. 610)
- [MDB ポートの使用状況](#) (P. 611)

ポート使用に関する一般的な考慮事項

通常、**Client Automation** では、大部分のネットワーク上のコンポーネント間通信で開いている必要があるポートは、特に、メッセージベースのトラフィック（通常は軽量）用の **UDP** ポート **4104** およびストリーム トラフィック（通常は大量）用の **TCP** ポート **4728** の 2 つのみです。

デフォルトで、**CA** メッセージキューイング（**CAM**）経由のリモート通信では、以下の表に示すように、ポート **4104** 上の **UDP** が使用されます。**CAM** でリモート通信に **TCP** を使用するように設定することができます（環境によってはこちらのほうが望ましい場合があります）。この場合、ソース ポートが **ANY** の **TCP** および **4105** のリスニング ポートが使用されます。ローカル マシンに **SSA** がインストールされていると、デフォルトでは、**CAM** **TCP** ポート通信は、すべての送信接続で **SSA** ポート **7163** にポート多重化されます。**TCP** 上の **CAM** 経由のリモート通信はこの表には示されていません。**CAM** は同じマシン上で実行されているコンポーネント間のローカル通信でも広く使用されます。この場合、ポート **4105** 上の **TCP** が使用されます。

Client Automation の特定の機能を設定して、ファイル共有を使用することができます。この場合、適切なファイル共有ポートを開く必要があります。特定のポート番号は、動作環境（プラットフォーム）および使用可能な設定されたメカニズムによって異なります。

通常のファイル共有ポートは以下のとおりです。

Windows

139/TCP（以前のスタイル）または 445/TCP（新しいスタイル）

Linux および UNIX

2049/TCP（NFS）

エンタープライズ マネージャで使用されるポート

以下の表は、エンタープライズ マネージャとの通信に使用されるポートの概要を示しています。

エンタープライズ マネージャからの通信

From	ポート	To	ポート	プロトコル	製品	説明
エンタープライズ マネージャ	すべて	エンタープライズ マネージャ	4105	TCP	すべて	CAM を介したローカル通信
エンタープライズ マネージャ	4104	ドメイン マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エンタープライズ マネージャ	すべて	ディレクトリ サーバ	389	TCP	すべて	LDAP ディレクトリ アクセス
エンタープライズ マネージャ	すべて	ディレクトリ サーバ	636	TCP	すべて	SSL ディレクトリ アクセス上の LDAP
エンタープライズ マネージャ	すべて	ドメイン マネージャ	4728	TCP	Software Delivery	DTS ファイル転送

エンタープライズ マネージャへの通信

From	ポート	To	ポート	プロトコル	製品	説明
エクスプローラ	4104	エンタープライズ マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
Web ブラウザ	すべて	エンタープライズ マネージャ	80	HTTP	すべて	Web コンソール アクセス
Web サービス クライアント	すべて	エンタープライズ マネージャ	80	HTTP	すべて	リモート クライアント アプリケーションからの Web サービス API へのアクセス

From	ポート	To	ポート	プロトコル	製品	説明
ドメイン マネージャ	すべて	エンタープライズ マネージャ	4728	TCP	Software Delivery	DTS ファイル転送
エクスプローラ	ファイル共有ポート	エンタープライズ マネージャ	ファイル共有ポート	UDP	Software Delivery	NOS ベースのファイル転送
エクスプローラ	すべて	エンタープライズ マネージャ	4728	TCP	Software Delivery	NOS を使用しないファイル転送
パッケージャ	4104	エンタープライズ マネージャ	4104	UDP	Software Delivery	CAM を介したネットワーク間の通信

注

- Web コンソールや Web サービス コンポーネントでセキュアな HTTP 通信を使用するように設定されている場合、ドメイン マネージャまたはエンタープライズ マネージャでのリスンにポート 443（デフォルト）が使用されます。
- Web コンソールでは Apache Tomcat が使用されます。デフォルトでは、Tomcat はポート 8090（起動）、8095（シャットダウン）、および 8020（ajp13）を使用するようにインストールし、設定します。ただし、通常、これらのポートはローカルにのみ使用されます。

ドメイン マネージャで使用されるポート

以下の表は、ドメイン マネージャとの通信に使用されるポートの概要を示しています。

ドメイン マネージャからの通信

From	ポート	To	ポート	プロトコル	製品	説明
ドメイン マネージャ	すべて	ドメイン マネージャ	4105	TCP	すべて	CAM を介したローカル通信

From	ポート	To	ポート	プロトコル	製品	説明
ドメイン マネージャ	4104	エンタープライズ マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
ドメイン マネージャ	4104	リモート ドメイン エンジン	4104	UDP	すべて	CAM を介したネットワーク間の通信
ドメイン マネージャ	4104	スケーラビリティ サーバ	4104	UDP	すべて	CAM を介したネットワーク間の通信
ドメイン マネージャ	すべて	ディレクトリ サーバ	389	TCP	すべて	LDAP ディレクトリ アクセス
ドメイン マネージャ	すべて	ディレクトリ サーバ	636	TCP	すべて	SSL ディレクトリ アクセス上の LDAP
ドメイン マネージャ	4104	エクスプローラ	4104	UDP	すべて	CAM を介したネットワーク間の通信
ドメイン マネージャ	すべて	エンタープライズ マネージャ	4728	TCP	Software Delivery	DTS ファイル転送：配信オーダー確認
ドメイン マネージャ	すべて	スケーラビリティ サーバ	4728	TCP	Software Delivery	DTS ファイル転送：パッケージ転送

ドメイン マネージャとの通信

From	ポート	To	ポート	プロトコル	製品	説明
エンタープライズ マネージャ	4104	ドメイン マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エクスプローラ	4104	ドメイン マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
スケーラビリティ サーバ	4104	ドメイン マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
Web ブラウザ	すべて	ドメイン マネージャ	80	HTTP	すべて	Web コンソール アクセス

From	ポート	To	ポート	プロトコル	製品	説明
Web サービス クライアント	すべて	ドメイン マ ネージャ	80	HTTP	すべて	リモート クライアン ト アプリケーション からの Web サービス API へのアクセス
リモート ドメ イン エンジン	4104	ドメイン マ ネージャ	4104	UDP	すべて	CAM を介したネット ワーク間の通信
エージェント	4104	ドメイン マ ネージャ	4104	UDP	Remote Control Software Delivery	CAM を介したネット ワーク間の通信 SD カタログ、 RC ホスト認証、 RC ビューア GAB
スケーラビリ ティ サーバ	すべて	ドメイン マ ネージャ	4728	TCP	Software Delivery	NOS を使用しないファ イル転送： ジョブ出力ファイル
エンタープライ ズ マネージャ	すべて	ドメイン マ ネージャ	4728	TCP	Software Delivery	DTS ファイル転送： パッケージ転送
エクスプローラ	ファイ ル共有 ポート	ドメイン マ ネージャ	ファイ ル共有 ポート	TCP/UDP	Software Delivery	NOS ベースのファイル 転送： パッケージ登録
エクスプローラ	すべて	ドメイン マ ネージャ	4728	TCP	Software Delivery	NOS を使用しないファ イル転送： パッケージ登録
パッケージャ	4104	ドメイン マ ネージャ	4104	UDP	Software Delivery	パッケージ登録制御 データ
パッケージャ	すべて	ドメイン マ ネージャ	4728	TCP	Software Delivery	NOS を使用しないファ イル転送： パッケージ登録

注

- Web コンソールや Web サービス コンポーネントでセキュアな HTTP 通信を使用するように設定されている場合、ドメイン マネージャまたはエンタープライズ マネージャでのリスンにポート 443（デフォルト）が使用されます。
- Web コンソールでは Apache Tomcat が使用されます。デフォルトでは、Tomcat はポート 8090（起動）、8095（シャットダウン）、および 8020（ajp13）を使用するようにインストールし、設定します。ただし、通常、これらのポートはローカルにのみ使用されます。

インフラストラクチャ展開で使用されるポート

密には、インフラストラクチャ展開はドメイン マネージャの一部です。そのポート使用については別のセクションで取り上げ、それらのポートはインフラストラクチャ展開が使用されている場合にのみ開いている必要があるということを説明します。

以下の表に示すポート（ポート 7 以外）は、インフラストラクチャ展開プライマをドメイン マネージャからプッシュするために使用されます。カスタマがプライマを手動でインストールする場合、またはインフラストラクチャ展開をまったく使用しない場合は、ポートが開かれる必要はありません。すべてのターゲットに対するすべてのポートを開く必要はありません。ポートは開いたままである必要はなく、展開中にのみ開いている必要があります。

さらに、カスタマでは、使用する通信メカニズムに応じて、MS Share/telnet および FTP/SSH ポートのサブセットを開くことができます。

ドメイン マネージャからの通信

送信者	ポート	受信者	ポート	プロトコル	製品	Description
ドメイン マネージャ	いずれか	ターゲット	7	TCP	すべて	エコー要求。ターゲット スキャン中に使用。このポートの使用は設定ポリシー内の適切な設定によって無効にできます

送信者	ポート	受信者	ポート	プロトコ ル	製品	Description
ドメインマ ネージャ	ファイ ル共有 ポート	ターゲット	ファイ ル共有 ポート	TCP UDP	すべて	プライマ パッケージ の Windows NOS ベー スのファイル転送。 ADMIN\$ の使用
ドメインマ ネージャ	いずれ か	ターゲット	135	TCP	すべて	プライマ インストー ルを開始する Windows RPC 呼び出し
ドメインマ ネージャ	いずれ か	ターゲット	21	TCP	すべて	プライマ パッケージ の FTP ベースのファイ ル転送
ドメインマ ネージャ	いずれ か	ターゲット	22	TCP	すべて	プライマ パッケージ の UNIX ssh / secure FTP ベースのファイル転 送。ドメインマネー ジャからのプッシュ。
ドメインマ ネージャ	いずれ か	ターゲット	23	TCP	すべて	ターゲットでのプライ マ パッケージの FTP ベースのファイル転送 の開始に使用される UNIX telnet 接続。
ドメインマ ネージャ	いずれ か	ターゲット	4104	UDP	すべて	CAM 優先の通信
ドメインマ ネージャ	いずれ か	ターゲット	4105 7163	TCP	すべて	CAM 優先の通信 7163 のポートは SSA によってポート多重化 に使用されます

ドメイン マネージャとの通信

送信者	ポート	受信者	ポート	プロトコ ル	製品	Description
ターゲット	いずれ か	ドメインマ ネージャ	20 21	TCP	すべて	プライマ パッケージ の FTP ベースのファイ ル転送

送信者	ポート	受信者	ポート	プロトコ ル	製品	Description
ターゲット	いずれ か	ドメインマ ネージャ	4104	UDP	すべて	CAM 優先の通信
ターゲット	いずれ か	ドメインマ ネージャ	4105 7163	TCP	すべて	CAM 優先の通信 7163 のポートは SSA によってポート多重化 に使用されます

スケーラビリティ サーバで使用されるポート

以下の表は、スケーラビリティ サーバとの通信に使用されるポートの概要を示しています。

スケーラビリティ サーバからの通信

From	ポート	To	ポート	プロトコ ル	製品	説明
スケーラビ リティ サーバ	すべて	スケーラビ リティ サー バ	4105	TCP	すべて	CAM を介したローカ ル通信
スケーラビ リティ サーバ	4104	ドメインマ ネージャ	4104	UDP	すべて	CAM を介したネット ワーク間の通信
スケーラビ リティ サーバ	4104	ドメインエ ンジン	4104	UDP	すべて	CAM を介したネット ワーク間の通信
スケーラビ リティ サーバ	4104	エージェン ト	4104	UDP	すべて	CAM を介したネット ワーク間の通信 構成、 SD トリガ ジョブ確 認、 AM トリガ ジョブ確 認
スケーラビ リティ サーバ	すべて	ドメインマ ネージャ	4728	TCP	Software Delivery	NOS を使用しない ファイル転送： ジョブ出力ファイル

From	ポート	To	ポート	プロトコル	製品	説明
スケーラビリティサーバ	すべて	エージェント	4728	TCP	Software Delivery	DTS ファイル転送 : パッケージ転送
スケーラビリティサーバ	554	エージェント	554	TCP	Software Delivery	App-V 仮想アプリケーション サービス用の RTSP (セキュリティ保護なし)
スケーラビリティサーバ	322	エージェント	322	TCP	Software Delivery	App-V 仮想アプリケーション サービス用の RTSPS (セキュリティ保護あり)

スケーラビリティサーバとの通信

From	ポート	To	ポート	プロトコル	製品	説明
ドメインマネージャ	4104	スケーラビリティサーバ	4104	UDP	すべて	CAM を介したネットワーク間の通信
ドメインエンジン	4104	スケーラビリティサーバ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エージェント	4104	スケーラビリティサーバ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エージェント	すべて	スケーラビリティサーバ	4728	TCP	すべて	NOS を使用しないファイル転送 バックアップデータ転送
エージェント	ファイル共有ポート	スケーラビリティサーバ	ファイル共有ポート	TCP	Software Delivery	NOS ベースのファイル転送
ドメインマネージャ	すべて	スケーラビリティサーバ	4728	TCP	Software Delivery	DTS ファイル転送 : パッケージ転送

From	ポート	To	ポート	プロトコル	製品	説明
エージェント	554	スケーラビリティサーバ	554	TCP	Software Delivery	App-V 仮想アプリケーション サービス用の RTSP（セキュリティ保護なし）
エージェント	322	スケーラビリティサーバ	322	TCP	Software Delivery	App-V 仮想アプリケーション サービス用の RTSPS（セキュリティ保護あり）

ブートサーバで使用されるポート

ブートサーバはスケーラビリティサーバの一部です。そのポート使用については別のセクションで取り上げ、それらのポートは OS インストール管理（OSIM）機能が使用されている場合にのみ開いている必要があるということを説明します。

スケーラビリティサーバとの通信

From	ポート	To	ポート	プロトコル	製品	説明
ターゲット	68	スケーラビリティサーバ	67	UDP	Software Delivery	ブートストラッププロトコルクライアント - bootpc
ターゲット	すべて	スケーラビリティサーバ	69	UDP	Software Delivery	Trivial File Transfer (TFTP)
PXE ターゲット	すべて	スケーラビリティサーバ	4011	UDP	Software Delivery	（オプション） 代替サービス ブート - altserviceboot.binl（PXE） ポート 4011 が使用できない場合は、代わりにポート 67 が使用されます。
ターゲット	ファイル共有ポート	スケーラビリティサーバ	ファイル共有ポート	TCP/UDP	Software Delivery	NOS ベースのファイル転送

エンジンで使用されるポート

以下の表は、エンジンとの通信に使用されるポートの概要を示しています。

エンジンからの通信

From	ポート	To	ポート	プロトコル	製品	説明
任意のエンジン	すべて	任意のエンジン	4105	TCP	すべて	CAM を介したローカル通信
任意のエンジン	すべて	コンテンツサーバ	443 または 5250	TCP	すべて	CA コンテンツ Web サイトからのソフトウェアシグネチャのダウンロード
任意のエンジン	すべて	ディレクトリサーバ	389	TCP	すべて	LDAP ディレクトリ アクセス： ディレクトリ同期、クエリ、レポート
任意のエンジン	すべて	ディレクトリサーバ	636	TCP	すべて	LDAP over SSL ディレクトリ アクセス： ディレクトリ同期、クエリ、レポート
任意のエンジン	すべて	SMTP サーバ	25	TCP/UDP	Asset Management	ポリシー違反時の電子メール送信
ドメインエンジン	4104	スケーラビリティサーバ	4104	UDP	すべて	CAM を介したネットワーク間の通信
リモートドメインエンジン	4104	ドメインマネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
リモートエンタープライズエンジン	4104	エンタープライズマネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信

エンジンへの通信

From	ポート	To	ポート	プロトコル	製品	説明
エンタープライズマネージャ	4104	リモートエンタープライズエンジン	4104	UDP	すべて	CAM を介したネットワーク間の通信
ドメインマネージャ	4104	リモートドメインエンジン	4104	UDP	すべて	CAM を介したネットワーク間の通信 一時的なクエリ評価などの通知
エクスプローラ	4104	任意のエンジン	4104	UDP	すべて	CAM を介したネットワーク間の通信
スケーラビリティサーバ	4104	ドメインエンジン	4104	UDP	すべて	CAM を介したネットワーク間の通信

エージェントで使用されるポート

以下の表は、エージェントとの通信に使用されるポートの概要を示しています。

エージェントからの通信

From	ポート	To	ポート	プロトコル	製品	説明
エージェント	すべて	エージェント	4105	TCP	すべて	CAM を介したローカル通信
エージェント	4104	スケーラビリティサーバ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エージェント	すべて	スケーラビリティサーバ	4728	TCP	すべて	NOS を使用しないファイル転送 バックアップ データ転送

From	ポート	To	ポート	プロトコル	製品	説明
エージェント	4104	ドメインマネージャ	4104	UDP	Remote Control Software Delivery	CAM を介したネットワーク間の通信 SD カタログ、 RC ホスト認証、 RC ビューア GAB
エージェント	ファイル共有ポート	スケーラビリティサーバ	ファイル共有ポート	TCP	Software Delivery	NOS ファイル転送
エージェント	554	スケーラビリティサーバ	554	TCP	Software Delivery	Microsoft App-V ストリーミング通信用の RTSP (セキュリティ保護なし)
エージェント	322	スケーラビリティサーバ	322	TCP	Software Delivery	Microsoft App-V ストリーミング通信用の RTSPS (セキュリティ保護あり)

エージェントとの通信

From	ポート	To	ポート	プロトコル	製品	説明
エクスプローラ	4104	エージェント	4104	UDP	すべて	即時診断 (DSM コンポーネント情報) SD トリガ ジョブ確認 AM トリガ ジョブ確認
スケーラビリティサーバ	4104	エージェント	4104	UDP	すべて	CAM を介したネットワーク間の通信 環境設定 SD トリガ ジョブ確認 AM トリガ ジョブ確認
スケーラビリティサーバ	すべて	エージェント	4728	TCP	Software Delivery	DTS ファイル転送 : パッケージ転送
パッケージジャ	すべて	エージェント	3001、3002	UDP	すべて	DSM サービス ロケータ
エクスプローラ	すべて	エージェント	4728 (*)	TCP	Remote Control	RC ビューアから RC ホスト

From	ポート	To	ポート	プロトコル	製品	説明
スケーラビリティ サーバ	554	エージェント	554	TCP	Software Delivery	Microsoft App-V ストリーミング通信用の RTSP（セキュリティ保護なし）
スケーラビリティ サーバ	322	エージェント	322	TCP	Software Delivery	Microsoft App-V ストリーミング通信用の RTSPS（セキュリティ保護あり）

注:

- 表の中の (*) は、レガシーの Remote Control ビューアが有効に設定されている場合、Remote Control ホストも TCP ポート 798 上でリスンすることを示しています。
- スケーラビリティ サーバはドメイン マネージャと同じコンピュータ上で実行される場合があります。

パッケージで使用されるポート

以下の表は、ソフトウェア管理パッケージとの通信に使用されるポートの概要を示しています。

パッケージからの通信

From	ポート	To	ポート	プロトコル	製品	説明
パッケージ	4104	エンタープライズ マネージャ	4104	UDP	Software Delivery	パッケージ登録制御データ
パッケージ	すべて	エンタープライズ マネージャ	4728	TCP	Software Delivery	NOS を使用しないファイル転送：パッケージ登録
パッケージ	4104	ドメイン マネージャ	4104	UDP	Software Delivery	パッケージ登録制御データ
パッケージ	すべて	ドメイン マネージャ	4728	TCP	Software Delivery	NOS を使用しないファイル転送：パッケージ登録

From	ポート	To	ポート	プロトコル	製品	説明
パッケージャ	すべて	エージェント	3001、 3002	UDP	すべて	Client Automation サービス ロケータ

DSM エクスプローラおよび Reporter で使用されるポート

以下の表は、DSM エクスプローラと DSM レポートからの通信、および DSM レポートへの通信に使用されるポートの概要を示しています。

エクスプローラおよびレポートからの通信

From	ポート	To	ポート	プロトコル	製品	説明
エクスプローラ	すべて	エクスプローラ	4105	TCP	すべて	CAM を介したローカル通信、通知メッセージ
エクスプローラ	4104	エンタープライズ マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エクスプローラ	4104	ドメイン マネージャ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エクスプローラ	4104	エージェント	4104	UDP	すべて	即時診断 (DSM コンポーネント情報) SD トリガ ジョブ確認 AM トリガ ジョブ確認
エクスプローラ	4104	任意のエンジン	4104	UDP	すべて	CAM を介したネットワーク間の通信
エクスプローラ	すべて	エージェント	4728	TCP	Remote Control	RC ビューアから RC ホスト
エクスプローラ	ファイル共有ポート	エンタープライズ マネージャ	ファイル共有ポート	UDP	Software Delivery	NOS ベースのファイル転送 : パッケージ登録
エクスプローラ	すべて	エンタープライズ マネージャ	4728	TCP	Software Delivery	NOS を使用しないファイル転送 : パッケージ登録

From	ポート	To	ポート	プロトコル	製品	説明
エクスプローラ	ファイル共有ポート	ドメインマネージャ	ファイル共有ポート	TCP UDP	Software Delivery	NOS ベースのファイル転送： パッケージ登録
エクスプローラ	すべて	ドメインマネージャ	4728	TCP	Software Delivery	NOS を使用しないファイル転送： パッケージ登録

エクスプローラとの通信

From	ポート	To	ポート	プロトコル	製品	説明
ドメインマネージャ	4104	エクスプローラ	4104	UDP	すべて	CAM を介したネットワーク間の通信
エンタープライズマネージャ	4104	エクスプローラ	4104	UDP	すべて	CAM を介したネットワーク間の通信

ENC ゲートウェイが使用するポート

以下の表は、ENC ゲートウェイ機能による通信に使用されるポートの概要を示しています。

From	ポート	To	ポート	プロトコル	製品	説明
ENC クライアント	すべて	ENC ゲートウェイサーバ	443	TCP	すべて	ENC クライアント登録、接続要求、リスン要求。
ENC クライアント	すべて	ENC ゲートウェイサーバ	80	TCP	すべて	CAM を介したネットワーク間の通信

From	ポート	To	ポート	プロトコル	製品	説明
ENC ゲートウェイ サーバ	すべて	ENC ゲートウェイ サーバ	443	TCP	すべて	ENC ゲートウェイ サーバ登録、ENC ゲートウェイ マネージャへのクライアント リクエストの中継、接続された ENC クライアント間でのデータの中継
ENC クライアント	すべて	インターネット プロキシ	1080	TCP	すべて	プロキシを介した通信
ENC クライアント	すべて	インターネット プロキシ	80	TCP	すべて	プロキシを介した通信

AMT アセットの隔離が使用するポート

CA Client Automation (Client Automation) は、AMT (Intel Advanced Management Technology) をサポートします。この関連では、AMT 隔離ポリシーが導入されます。これは、AMT デバイス上のインバウンドおよびアウトバウンドのネットワークトラフィックにフィルタを追加するブレーカー機能です。

隔離ポリシーは、AMT 対応アセットに対する新しい管理状態を提供します。Client Automation に対して高度な管理を実行している間、一時的にこのアセットをロックできます。隔離ポリシーは、AMT デバイスおよび Client Automation が通信のために使用するポートを除き、通常のインバウンドおよびアウトバウンドトラフィックすべてを閉鎖します。つまり、Intel AMT アセットの隔離は、Client Automation によって完全に管理できます。

隔離ポリシーは、以下のポートに影響を与えます。

- AMT コンピュータからの AMT 送信/受信 ARP トラフィック (ポート 67)
- AMT ポート上の AMT 送信/受信 データ トラフィック (ポート 16992 ~ 16995)
- Client Automation 送信/受信 (ポート 4104)
Client Automation 送信/受信 (ポート 4105)
Client Automation 送信/受信 (ポート 4728)
- DHCP サービス用のサポート ポート (ポート 53 が受信用に開いている)。
- DNS サービス用のサポート ポート (ポート 63 が送信/受信用に開いている)。

MDB ポートの使用状況

MDB 通信に使用されるデフォルト ポートは、以下のとおりです。

- Oracle : 1521
- Microsoft SQL Server : 1433

データベース管理者のみが、データベース サイトにおけるポート割り当てを変更できます。

付録 C: インストールの Software Delivery プロシージャ

CA Client Automation のインストーラには、インストール パッケージの定義済み Software Delivery (SD) プロシージャのセットが用意されています。

このセクションには、以下のトピックが含まれています。

[アンインストールに関する重要事項 \(P. 614\)](#)

[CA DSM エージェント + AM、RC、SD プラグイン Linux \(Intel\) ENU \(P. 614\)](#)

[CA DSM エージェント + Asset Management プラグイン Linux \(intel\) ENU \(P. 614\)](#)

[CA DSM エージェント + 基本インベントリ プラグイン Linux \(intel\) ENU \(P. 615\)](#)

[CA DMPrimer Linux \(Intel\) ENU \(P. 615\)](#)

[SMPackager \(Linux\) \(P. 615\)](#)

[CA DSM レガシー エージェントの削除 Linux \(intel\) ENU \(P. 615\)](#)

[CA DSM エージェント + Remote Control プラグイン Linux \(intel\) ENU \(P. 616\)](#)

[CA DSM エージェント + Software Delivery プラグイン Linux \(intel\) ENU \(P. 616\)](#)

[CA DSM スケーラビリティ サーバ Linux \(Intel\) ENU \(P. 617\)](#)

[CA DSM Agent + AM、RC、SD プラグイン Win32 \(P. 617\)](#)

[CA DMS エージェント + Asset Management プラグイン \(P. 618\)](#)

[CA DMS エージェント + 基本インベントリ プラグイン \(P. 618\)](#)

[CA DMS エージェント + Data Transport プラグイン \(P. 618\)](#)

[CA DMS エージェント + Remote Control プラグイン \(P. 619\)](#)

[CA DMS エージェント + Software Delivery プラグイン \(P. 620\)](#)

[CA DSM Constant Access \(Intel AMT\) \(P. 621\)](#)

[CA DSM エクスプローラ \(P. 621\)](#)

[CA DSM マネージャ \(P. 622\)](#)

[CA DMS スケーラビリティ サーバ \(P. 622\)](#)

[CA DSM 安全なソケット アダプタ \(P. 623\)](#)

[CA DSM レガシー エージェントの削除 Win32 \(P. 623\)](#)

アンインストールに関する重要事項

Software Delivery (SD) エージェントのアンインストール プロシージャを使用する前に、以下のことに注意してください。

- SD エージェント プラグインのアンインストール プロシージャは、パッケージのアンインストール ジョブを実行する SD エージェント プラグインであるため、ジョブ コンテナ内で最後のプロシージャとして配置する必要があります。
- Data Transport Service (DTS) エージェント プラグインは Windows の個別のパッケージであるため、SD エージェントをアンインストールしても DTS エージェントが暗黙的にアンインストールされることはありません。DTS エージェントは個別のジョブとしてアンインストールする必要がありますが、このジョブは同じジョブ コンテナ内に組み込むことができます。

CA DSM エージェント + AM、RC、SD プラグイン Linux (Intel) ENU

このインストール パッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- CA DSM のすべてのアンインストール

CA DSM エージェント + Asset Management プラグイン Linux (intel) ENU

このインストール パッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- CA DSM のすべてのアンインストール
- Asset Management プラグインのみのアンインストール

CA DSM エージェント + 基本インベントリ プラグイン Linux (intel) ENU

このインストール パッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- CA DSM のすべてのアンインストール

CA DMPrimer Linux (Intel) ENU

このインストール パッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- スタンドアロン Desktop Management Primer のアンインストール

SMPackager (Linux)

このインストール パッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- パッケージのインストール
- パッケージの再インストール
- パッケージのアンインストール

CA DSM レガシー エージェントの削除 Linux (intel) ENU

このインストール パッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- すべて削除
- AM の削除
- SD の削除

CA DSM エージェント + Remote Control プラグイン Linux (intel) ENU

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- 集中管理されたホストのみ
- スタンドアロン エージェント
- CA DSM のすべてのアンインストール
- Remote Control プラグインのみのアンインストール

CA DSM エージェント + Software Delivery プラグイン Linux (intel) ENU

このインストールパッケージには、Data Transport プラグインが含まれます。

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- SM インストーラのインストールのスキャン
- SWD のスキャン
- SWD のスキャン：Linux ソフトウェア
- SM インストーラ：トレースの無効化
- SM インストーラ：トレースの有効化
- SM インストーラ：すべてのトレースの取得
- SM インストーラ：最新トレースの取得
- CA DSM のすべてのアンインストール
- Software Delivery プラグインのみのアンインストール

CA DSM スケーラビリティ サーバ Linux (Intel) ENU

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- ブート サーバ共有の無効化
- MSILIB 共有の無効化
- NFS 共有の無効化
- Samba 共有の無効化
- SDLIB 共有の無効化
- ブート サーバ共有の有効化
- MSILIB 共有の有効化
- NFS 共有の有効化
- Samba 共有の有効化
- SDLIB 共有の有効化
- インストール
- CCS カレンダの同期
- ソフトウェア ジョブ レコードの同期
- ソフトウェア ステージング ライブラリの同期
- CA DSM のすべてのアンインストール
- スケーラビリティ サーバ+エージェントのみのアンインストール

CA DSM Agent + AM、RC、SD プラグイン Win32

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- アンインストール

CA DMS エージェント + Asset Management プラグイン

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- 検出
- インストール
- ローカルの修正
- アンインストール
- 確認

CA DMS エージェント + 基本インベントリ プラグイン

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- 検出
- インストール
- ローカルの修正
- アンインストール
- 確認

CA DMS エージェント + Data Transport プラグイン

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- 検出
- インストール
- ローカルの修正
- アンインストール
- 確認

CA DMS エージェント + Remote Control プラグイン

このインストールパッケージには、以下の定義済み **Software Delivery** プロシージャが含まれています。

- 完全一括管理エージェント
- 集中管理されたホストのみ
- 検出
- ローカルの修正
- スタンドアロン エージェント
- アンインストール
- 確認

CA DMS エージェント + Software Delivery プラグイン

このインストールパッケージには、**Data Transport** プラグインが含まれていません。

このインストールパッケージには、以下の定義済み **Software Delivery** プロシージャが含まれています。

- カタログ：追加
- カタログ：削除
- 検出
- 診断：設定およびバージョン情報（dsmdiag 情報）の取得
- インストール
- ローカルの修正
- MSI のスキャン（インストールされているパッケージについてローカル MSI データベースをスキャンします）
- SM インストーラのインストールのスキャン（エージェントにインストールされている SXP パッケージをスキャンします）
- SWD のスキャン（インストールされているパッケージについて SD プロプラエタリ エージェント db をスキャンします）
- SM インストーラ：トレースの無効化
- SM インストーラ：トレースの有効化
- SM インストーラ：すべてのトレースの取得
- SM インストーラ：履歴の取得
- SM インストーラ：最新トレースの取得
- SM インストーラ：ユーザ履歴の取得
- SM インストーラ：ユーザ トレースの取得
- アンインストール
- 確認

CA DSM Constant Access (Intel AMT)

このインストールパッケージには、以下の定義済み **Software Delivery** プロシージャが含まれています。

- インストール
- アンインストール

CA DSM エクスプローラ

このインストールパッケージには、以下の定義済み **Software Delivery** (SD) 関連プロシージャが含まれています。

- 検出
- インストール
- インストール (レポートを使用しない)
- AM のインストール
- AM のインストール (レポートを使用しない)
- AM + RC のインストール
- AM + RC のインストール (レポートを使用しない)
- AM + SD のインストール
- AM + SD のインストール (レポートを使用しない)
- RC のインストール
- RC のインストール (レポートを使用しない)
- SD のインストール
- SD のインストール (レポートを使用しない)
- SD + RC のインストール
- SD + RC のインストール (レポートを使用しない)
- ローカルの修正
- アンインストール
- 確認

CA DSM マネージャ

このインストールパッケージには、以下の定義済み **Software Delivery** プロシージャが含まれています。

- Detect

CA DMS スケーラビリティ サーバ

スケーラビリティ サーバインストールパッケージは、「CA DMS エージェント + Data Transport プラグイン」パッケージに依存しています。

スケーラビリティ サーバパッケージには、以下の定義済み **Software Delivery** プロシージャが含まれています。

- 検出
- ブート サーバ共有の無効化
- MSILIB 共有の無効化
- SDLIB 共有の無効化
- ブート サーバ共有の有効化
- MSILIB 共有の有効化
- SDLIB 共有の有効化
- インストール
- ローカルの修正
- CCS カレンダの同期
- ソフトウェア ジョブ レコードの同期
- ソフトウェア ステージング ライブラリの同期
- アンインストール
- Verify
- スケーラビリティ サーバ、**Software Delivery** のエージェント、**Remote Control**、**Asset Manager**、およびデータ トランスポート サービスのアンインストール

CA DSM 安全なソケット アダプタ

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- インストール
- アンインストール

CA DSM レガシー エージェントの削除 Win32

このインストールパッケージには、以下の定義済み Software Delivery プロシージャが含まれています。

- AM の削除
- RC の削除
- SD の削除
- すべて削除

付録 D: CA Client Automation が提供する現在の証明書

CA Client Automation には、以下のリストに示すように、共通およびアプリケーション固有の証明書があります。証明書の使用方法およびカスタマイズ方法の詳細については、「[X.509 証明書をインストールイメージへ導入する方法 \(P. 255\)](#)」および「[アプリケーション固有の証明書のインストール \(P. 449\)](#)」を参照してください。

このセクションには、以下のトピックが含まれています。

[共通の証明書 \(P. 625\)](#)

[アプリケーション固有の証明書 \(P. 626\)](#)

共通の証明書

共通の DSM 証明書は、以下のとおりです。

デフォルトの DSM ルート証明書

DN:

CN=DSM Root,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=DSM Root,O=Computer Associates,C=US

デフォルトの基本ホスト ID 証明書

DN:

CN=Generic Host Identity,O=Computer Associates,C=US

URI

x509cert://DSM r11/CN=Generic Host Identity,O=Computer Associates,C=US

タグ

dsmcommon

使用方法:

基本ホスト ID のプロビジョン。

構文要素:

エンタープライズのすべてのノード。

アプリケーション固有の証明書

管理データベース (MDB) のオブジェクトレベルのセキュリティ認証にアプリケーション固有の証明書が使用されます。デフォルト名を使用しない新しい証明書を作成する場合は、マネージャをインストールする前に新しい URI で `cfcert.ini` を更新するか、またはデフォルトのセキュリティ プロファイルに権利と権限を付加した新しいセキュリティ プロファイルを作成する必要があります。

[cfcert.ini ファイル](#) (P. 257) の [Tags] セクションの説明を参照してください。

ディレクトリの同期の証明書

DN:

CN=DSM Directory Synchronisation,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=DSM Directory Synchronisation,O=Computer Associates,C=US

タグ

dsm_cmdir_eng

使用方法:

ディレクトリの同期エンジンのジョブでマネージャを認証できるようにします。

共通サーバ登録の証明書

DN:

CN=DSM Common Server Registration,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=DSM Common Server Registration,O=Computer Associates,C=US

タグ

dsm_csvr_reg

使用方法:

スケーラビリティ サーバおよびマネージャの登録で、マネージャに対する認証を行います。

設定およびステータス管理の証明書

DN:

CN=Configuration and State Management,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=Configuration and State Management,O=Computer Associates,C=US

タグ

csm

使用方法:

CSM エージェント コントローラの認証。

Software Delivery エージェント ムーバの証明書

DN:

CN=DSM r11 Agent Mover,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=DSM r11 Agent Mover,O=Computer Associates,C=US

タグ

dsmagtmv

使用方法:

Unicenter Software Delivery エージェント ムーバ。

構文要素:

マネージャ ノード。

Software Delivery カタログ証明書

DN:

CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

URI:

x509cert://dsm r11/CN=DSM r11 Software Delivery Catalog,O=Computer Associates,C=US

タグ:

dsmsdcat

使用方法:

Software Delivery カタログ

各項目の説明:

マネージャ ノード、エージェント ノード (Windows のみ)。

注:

- Software Delivery カタログ証明書には、コンピュータおよびユーザ プロファイルに対して書き込み (W) 権限があります。証明書はすべてのドメイン マネージャおよびリモート エンジンに存在します。
- ドメイン マネージャまたはそのリモートエンジン上の証明書のコンピュータおよびユーザ プロファイルのクラス権限は変更しないでください。
- 同じ dsmsdcat タグを持つデフォルトまたはユーザ指定の Software Delivery カタログ証明書はどちらも削除しないでください。

エンタープライズ アクセスの証明書

DN:

CN=Enterprise Access,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=Enterprise Access,O=Computer Associates,C=US

タグ

ent_access

使用方法:

エンタープライズへのパスワード アクセス。

ドメイン アクセスの証明書

DN:

CN=Domain Access,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=Domain Access,O=Computer Associates,C=US

タグ

dom_access

使用方法:

ドメインへのパスワード アクセス。

レポータ アクセスの証明書

DN:

CN=Reporter Access,O=Computer Associates,C=US

URI

x509cert://dsm r11/CN=Reporter Access,O=Computer Associates,C=US

タグ

rep_access

使用方法:

レポータへのパスワードアクセス。

付録 E: セキュリティ エリアのサポートの ユース ケース

このセクションでは、ユーザの観点からのエリアのサポートでの最も重要なユース ケース、およびエリアのサポートの内容について説明します。

セキュリティ エリアのサポートおよびエリアのアクセス権に関する基本的な情報については、「[セキュリティ エリアのサポート \(P. 481\)](#)」および「[エリアの権限 \(P. 464\)](#)」セクションを参照してください。

ユース ケースの説明は、以下のようにすべて同じ構造を持っています。

シナリオ

ユーザのシナリオを簡単に説明します。ユーザがしようとすることを説明します。

前提条件:

ユーザが「アクション」で説明するアクションを実行する前に、どのようなオブジェクトが定義されるかを定義します。

アクション:

ユーザの行動を説明します。

事後条件:

ユーザが上記のアクションの実行後、シナリオに含まれるオブジェクトのプロパティを定義します。

このセクションには、以下のトピックが含まれています。

[セキュリティ プロファイル用のセキュリティ エリア サポート \(P. 634\)](#)

[ユース ケース: Client Automation のインストール \(P. 635\)](#)

[ユース ケース: 既存のインストールのアップグレード \(P. 636\)](#)

[ユース ケース：セキュリティプロファイル](#) (P. 636)
[ユース ケース：コンピュータ](#) (P. 638)
[ユース ケース：アセットグループ](#) (P. 640)
[ユース ケース：クエリ](#) (P. 644)
[ユース ケース：ソフトウェア パッケージ](#) (P. 646)
[ユース ケース：ソフトウェア プロシージャ](#) (P. 647)
[ユース ケース：ソフトウェア グループ](#) (P. 648)
[ユース ケース：ソフトウェア ポリシー](#) (P. 648)
[ユース ケース：ソフトウェア ジョブ](#) (P. 649)
[ユース ケース：アセット ジョブ](#) (P. 650)
[ユース ケース：エンジン タスク](#) (P. 651)
[ユース ケース：エリアの管理](#) (P. 652)
[ユース ケース：所有権の取得](#) (P. 656)

セキュリティプロファイル用のセキュリティ エリア サポート

セキュリティプロファイル用のセキュリティ エリア サポートは以下のルールに従います。

- [全員] プロファイルについては、エリア サポートの有効化または無効化は許可されません。いずれのエリアへのアクセスも拒否されます。
- [ディストリビュータ] プロファイルについては、エリア サポートの有効化または無効化を行うためには、エリア サポート セキュリティ クラスでの完全なアクセス権が必要です。

ユース ケース: Client Automation のインストール

シナリオ

ユーザが Client Automation をインストールします。

事前条件:

Client Automation の以前バージョンがコンピュータにインストールされていません。

アクション

ユーザが Client Automation をインストールします。

事後条件:

- デフォルトの組み込みプロファイルがインストールされています。
- エリアのサポートが無効になっています（グローバル設定）。
- デフォルトのエリアのアクセス権が、「全エリアの表示」に設定されています。
- 「全員」プロファイルに、エリアへのアクセス権がありません。
- 「管理者」プロファイルに、すべてのエリアへの完全なアクセス権があり、変更できません。
- あらかじめ定義されているエリア定義がインストールされていません。

ユース ケース: 既存のインストールのアップグレード

シナリオ

既存のインストールをアップグレードします。

事前条件:

Client Automation がインストールされています。

アクション:

MDB をアップグレードするための DSM MDB インストールを開始します。

事後条件:

- MDB Schema が変更されるか、アップグレードされます。
- エリア サポートはインストール後に無効になります。
- area_aces は、市外局番のデフォルト設定に基づき値が設定されるすべての既存の保護されたオブジェクトに対して作成されます。

注: アップグレード後、すべてのオブジェクトがすべての領域で表示されます。これはデフォルト設定です。

ユース ケース: セキュリティプロファイル

セキュリティ プロファイルに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [セキュリティプロファイルの作成](#) (P. 637)
- [セキュリティプロファイルのエリア設定の変更](#) (P. 637)
- [セキュリティプロファイルの削除](#) (P. 638)

ユース ケース: セキュリティ プロファイルの作成

シナリオ

管理者が新しいセキュリティ プロファイルを作成します。

事前条件:

セキュリティ プロファイルが存在しません。

アクション

管理者が 1 つ以上のエリア コードが割り当てられている新しいセキュリティ プロファイルを作成します。

事後条件:

- セキュリティ プロファイルが作成されています。
- すべてのセキュリティ クラス レベルのアクセス権が、新しいセキュリティ プロファイルに対して作成されています。
- オブジェクト レベルのアクセス権が、既存のすべての保護されたオブジェクトに対して計算されています。アクセス権が、(グループを含む) 既存の保護されたオブジェクトに対して計算されています。オブジェクトのアクセス権が、クラス レベルのアクセス権から取得されています。
- エリアのアクセス権が、セキュリティ プロファイルに割り当てられたエリアのアクセス権から作成および取得されています。

ユース ケース: セキュリティ プロファイルに対するエリア設定の変更

シナリオ

管理者は、セキュリティ プロファイルに割り当てられているエリア コードを変更します。

事前条件:

セキュリティ プロファイルが存在し、複数のエリアがプロファイルに割り当てられています。

アクション

管理者は、セキュリティ プロファイルに対してエリア コードを古いものから新しいものに変更します。

事後条件:

保護されたオブジェクトの `area_aces` は変更されません。

ユース ケース: セキュリティ プロファイルの削除

シナリオ

管理者がセキュリティ プロファイルを削除します。

事前条件:

セキュリティ プロファイルが存在し、複数のエリアがプロファイルに割り当てられています。

アクション

管理者がセキュリティ プロファイルを削除します。

事後条件:

- セキュリティ プロファイルが削除されています。
- 保護されたオブジェクト、および削除されたセキュリティ プロファイルに関するすべてのアクセス権の情報も削除されています。

ユース ケース: コンピュータ

コンピュータに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [コンピュータの手動による作成](#) (P. 639)
- [新しく検出された DSM エージェント](#) (P. 639)

ユース ケース: コンピュータ オブジェクトの手動による作成

シナリオ

ユーザが新しいコンピュータ オブジェクトを作成します。

事前条件:

ユーザは、複数のセキュリティ プロファイルのメンバです。

アクション

ユーザが **DSM** エクスプローラまたは **DSM** コマンド ライン ユーティリティを使用して、新しいコンピュータ オブジェクトを作成します。

事後条件:

- 新しいコンピュータ オブジェクトが作成されています。
- **area_ace** がセキュリティ プロファイルから派生し、コンピュータ オブジェクトに割り当てられています。ユーザが複数のセキュリティ プロファイルのメンバになっている場合、関連するすべてのセキュリティ プロファイルの **area_ace** が **OR** 演算され、保護されたオブジェクトに割り当てられています。

ユース ケース: 新しく検出された DSM エージェント

シナリオ

DSM エージェントが展開されており、初めて実行されます。

事前条件:

新しいアセットに対して **MDB** にオブジェクトが存在しません。

アクション

ユーザ アクションはありません。 **DSM** エンジンにより、新しいエージェントが検出され、アセット オブジェクトが作成されます (**ca_discovered_hardware** に挿入)。

事後条件:

- 新しい保護されたオブジェクトが作成されています。
- エリアのアクセス権が、グローバル レベルで定義されたように割り当てられています (グローバル設定パラメータ)。

ユース ケース: アセット グループ

アセット グループに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [アセット グループの作成](#) (P. 640)
- [アセット グループへのコンピュータの追加](#) (P. 641)
- [アセット グループからのコンピュータの削除](#) (P. 642)
- [アセット グループのエリアのアクセス権の変更](#) (P. 643)
- [継承の無効化および復帰](#) (P. 643)

ユース ケース: アセット グループの作成

シナリオ

ユーザが 1 つのセキュリティ プロファイルのみのメンバである場合に、新しいアセット グループを作成します。

事前条件:

同じ名前のグループがまだ存在していません。

アクション

ユーザが新しいアセット グループを作成します。

事後条件:

- 新しいグループが作成されています。
- `group_ace` がグループのクラス レベルのアクセス権に基づいて作成されています。
- `object_ace` がグループのクラス レベルのアクセス権に基づいて作成されています。
- `area_ace` が、作成ユーザが属するセキュリティ プロファイルから選択されています。作成ユーザが不明の場合、デフォルトの `area_ace` が割り当てられています。

注: スケーラビリティ サーバ グループおよびドメイン グループでも同じになります。

ユース ケース: アセット グループへのコンピュータの追加

シナリオ

ユーザが 1 つのセキュリティ プロファイルのみのメンバである場合に、コンピュータをグループに追加します。

前提条件:

- アセット グループが存在します。
- コンピュータが存在します。

アクション

ユーザがコンピュータをグループに追加します。グループに対して継承が有効です。

事後条件:

- コンピュータがグループにリンクされています。
- 継承グループでない場合は、何も実行されていません。継承グループの場合は、**object_ace** が親グループの **object_ace** に基づいて計算されています。
- エリア コードは、以下のように設定されています。
 - コンピュータが 1 つのアセット グループのみの唯一のメンバである場合、**area_ace** はアセット グループの **area_ace** と同じです。
 - コンピュータが複数のアセット グループのメンバである場合、親グループの **area_aces** は OR 演算され、保護されたオブジェクトに割り当てられています。

指定条件:

コンピュータのエリアのアクセス権が、グループに追加する前に **creation_user** レベル、またはグローバル デフォルト レベルに設定されている場合、エリアのアクセス権は、グループのエリアのアクセス権に設定されています。

コンピュータのエリアのアクセス権が、グループに追加する前に **object_level** に設定されている場合、エリアのアクセス権はグループ レベルに設定されません。ユーザは **REVERT** 関数を使用して、グループに適合するようにエリアのアクセス権を再計算する必要があります。

エリアのアクセス権は、アクセス権の継承が無効の場合、変更しないようにする必要があります。

注: 動的グループおよびグループの評価を実行しているエンジンでも、同じことが当てはまります。この場合、エンジンによりメンバがグループにリンクされます。

ユース ケース: アセット グループからのコンピュータの削除

シナリオ

ユーザが 1 つ以上のセキュリティ プロファイルのメンバである場合に、コンピュータをアセット グループから削除します。

前提条件:

- アセット グループが存在します。
- コンピュータが存在します。
- コンピュータは、1 つのアセット グループのみのメンバです。

アクション

ユーザがコンピュータをアセット グループからリンク解除します。グループに対して継承が有効です。

事後条件:

- コンピュータがグループからリンク解除されています。
- エリアのアクセス権は更新されません。
- セキュリティ レベルは、オブジェクト レベルに設定されています。

指定条件:

コンピュータが複数のアセット グループのメンバであり、セキュリティ レベルがグループ レベルに設定されている場合、エリアのアクセス権は（残っているグループ割り当てに基づいて）再計算および更新されています。

エリアのアクセス権がオブジェクト レベルに設定されている場合、エリアのアクセス権は更新されません。

注: コンピュータをアセット グループから削除した後で、ユーザは復帰機能を使用して、コンピュータのエリアのアクセス権を作成ユーザ レベルにすることができます。

ユース ケース: アセット グループのエリアの権限の変更

シナリオ

既存のアセット グループのエリアの権限を変更します。

前提条件:

- ユーザが 1 つ以上のセキュリティ プロファイルにリンクされています。
- アセット グループは権限継承が有効な場所に存在します。

アクション:

[アクセス権の変更] ダイアログ ボックスを使用し、既存グループを 1 つ以上のエリアにリンクするか、リンクを解除します。

事後条件:

- 既存グループの `area_ace` が変更されます。
- 継承グループの場合、メンバの `area_ace` が更新されます。

注: 権限継承の有効化または無効化によりエリアの権限が変更されることはありません。

ユース ケース: 継承の無効化および復帰

シナリオ

ユーザがアセット グループの継承を無効にして、アセット レベルで復帰を実行します。

前提条件:

- アセット グループが存在し、アクセス権の継承が有効です。
- コンピュータがアセット グループにリンクされ、エリアのアクセス権がリンク時にオブジェクト レベルに設定されています。

アクション

ユーザがアセット グループのアクセス権の継承を無効に設定し、コンピュータ オブジェクトの「復帰」を実行します。

事後条件:

コンピュータのオブジェクトのアクセス権が、作成ユーザに対して復帰されています。

注: 権限の継承の有効/無効を切り替えても、エリアの権限は変更されません。

ユース ケース: クエリ

クエリに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [クエリの作成](#) (P. 644)
- [クエリの実行](#) (P. 645)
- [Software Delivery のコンテキストでのクエリの実行](#) (P. 646)

ユース ケース: クエリの作成

シナリオ

ユーザが新しいクエリを作成します。

事前条件:

ユーザは、1つのセキュリティ プロファイルのみのメンバです。

アクション

ユーザが新しいクエリを作成します。

事後条件:

- 新しいクエリが作成されています。
- クエリの `area_ace` が、クエリの作成ユーザのプロファイルから取得されています。
- 新しいクエリには、「where」条件が追加され、作成ユーザに（クエリ自体に割り当てられた `area_ace` と同じ）アクセス権があるオブジェクトのみをクエリが返すことを確認します。
- `object_ace` が、クエリのセキュリティ クラスのクラス レベル `ace` に基づいて作成されています。

ユース ケース: クエリの実行

シナリオ

ユーザは動的なコンピュータ グループを作成します。グループはエンジンによって評価される必要があります。

事前条件:

なし

アクション

ユーザは動的グループを作成します。親グループは、「すべてのコンピュータ」です。

クエリを作成したユーザは、グループを作成するユーザとは異なります。

事後条件:

グループの評価は、以下のルールに基づいてエンジンによって実行されています。

- クエリが実行されています。
- グループを作成したユーザと同じエリアに当てはまるコンピュータのみをグループのメンバとして追加します。

つまり、グループ エリアのアクセス権は、グループのエリアのアクセス権よりも優先度が高くなります。

ユース ケース: Software Delivery のコンテキストでのクエリの実行

シナリオ

クエリは **Software Delivery** プロシージャの前提条件の一部として評価されます。評価は **Software Delivery** のタスク マネージャによって実行されます。

事前条件:

前提条件のあるプロシージャは、ターゲット コンピュータ上でのインストールで使用され、グローバル エリア設定がオンになります。

アクション:

タスク マネージャがクエリ評価 API を呼び出し、ユーザを **Software Delivery** アクティビティ オブジェクトから渡します。

事後条件:

クエリが **GUI** でジョブを作成したユーザと同じコンテキストで評価されています。つまり、ジョブを作成したユーザと同じエリアのオブジェクトのみがクエリによって返されています。ジョブがバックグラウンドプロセスによって作成されており、利用できるユーザ コンテキストがない場合、エリアのサポートが有効になっていなかったかのように、すべてのオブジェクトがクエリの評価によって返されています。

ユース ケース: ソフトウェア パッケージ

ソフトウェア パッケージに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [ソフトウェア パッケージの作成](#) (P. 647)

ユース ケース: ソフトウェア パッケージの作成

シナリオ

ユーザが新しいソフトウェア パッケージを作成します。

事前条件:

ソフトウェア パッケージが存在しませんでした。

アクション

ユーザが **Client Automation GUI** を使用してソフトウェア パッケージを作成します。

事後条件:

- ソフトウェア パッケージが作成されています。
- エリアのアクセス権が作成され、ソフトウェア パッケージがオブジェクトを作成したユーザと同じエリアにリンクされています。

ユース ケース: ソフトウェア プロシージャ

ソフトウェア プロシージャに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [ソフトウェア プロシージャの作成](#) (P. 647)

ユース ケース: ソフトウェア プロシージャの作成

シナリオ

ユーザが新しいソフトウェア プロシージャを作成します。

事前条件:

ソフトウェア プロシージャが存在しませんでした。

アクション

ユーザが **Client Automation GUI** を使用してソフトウェア プロシージャを作成します。

事後条件:

プロシージャは、プロシージャが含まれているソフトウェア パッケージと同じエリアのアクセス権を継承しています。

ユース ケース: ソフトウェア グループ

ソフトウェア グループに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [ソフトウェア グループの作成](#) (P. 648)

ユース ケース: ソフトウェア グループの作成

シナリオ

ユーザが新しいソフトウェア グループを作成します。

事前条件:

ユーザは、複数のセキュリティ プロファイルのメンバです。

アクション

ユーザが **DSM** エクスプローラを使用して、新しいソフトウェア グループを作成します (ソフトウェア パッケージ ライブラリの下の新しいノード)。

事後条件:

- 新しいソフトウェア グループが作成されています。
- ソフトウェア グループの **area_ace** が、クエリの作成ユーザのプロファイルから取得されています。
- **objects_ace** が、アセット ジョブのセキュリティ クラスのクラス レベル ACE に基づいて作成されます。
- また、**group_ace** も、セキュリティ プロファイルのクラス レベル **ace** に基づいて作成されています。

ユース ケース: ソフトウェア ポリシー

ソフトウェア ポリシーに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [ソフトウェア ポリシーの作成](#) (P. 649)

ユース ケース: ソフトウェア ポリシーの作成

シナリオ

ユーザが新しいソフトウェア ポリシーを作成します。

事前条件:

ユーザは、複数のセキュリティ プロファイルのメンバです。

アクション:

ユーザが **DSM** エクスプローラまたは **Client Automation** コマンド ラインを使用して、新しいソフトウェア ポリシーを作成します。

事後条件:

- 新しいソフトウェア ポリシーが作成されています。
- ソフトウェア ポリシーがアセット グループに割り当てられています。
- **object_ace** が、クラス **select ace** から取得されています。
- ソフトウェア ポリシーのエリアのアクセス権が、ポリシーの作成ユーザのプロファイルから取得されています。

ユース ケース: ソフトウェア ジョブ

ソフトウェア ジョブに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [ソフトウェア ジョブの作成](#) (P. 650)

ユース ケース: ソフトウェア ジョブの作成

シナリオ

ユーザが新しいソフトウェア ジョブを作成します。

事前条件:

ユーザは、複数のセキュリティ プロファイルのメンバです。

アクション:

ユーザが **DSM** エクスプローラまたは **DSM** コマンド ラインを使用して、新しいソフトウェア ジョブを作成します。

事後条件:

- 新しいソフトウェア ジョブが作成されています。
- オブジェクトのアクセス権が、クラス **select ace** から取得されています。
- ソフトウェア ジョブのエリアのアクセス権が、ジョブの作成ユーザのプロファイルから取得されています。

ユース ケース: アセット ジョブ

アセット ジョブに関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [アセット ジョブの作成](#) (P. 651)

ユース ケース: アセット ジョブの作成

シナリオ

ユーザが新しいアセット ジョブを作成します。

事前条件:

ユーザは、1つのみのセキュリティ プロファイルのメンバである。

アクション

ユーザが新しいアセット ジョブを作成します。アセット ジョブは、メッセージ、コマンドなど、任意のジョブ タイプにすることができます。

事後条件:

- 新しいアセット ジョブが作成されています。
- アセット ジョブの `area_ace` が、クエリの作成ユーザのプロファイルから取得されています。
- `objects_ace` が、アセット ジョブのセキュリティ クラスのクラス レベル ACE に基づいて作成されます。

ユース ケース: エンジン タスク

セキュリティ エリアのサポートのコンテキストで、エンジン タスクに関する以下の重要なユーザ シナリオを検討します。

- [エンジン タスクの作成](#) (P. 652)

ユース ケース: エンジン タスクの作成

シナリオ

ユーザが新しいエンジン タスクを作成する。

事前条件:

ユーザは、1つのみのセキュリティ プロファイルのメンバである。

アクション

ユーザが新しいエンジン タスクを作成する。

事後条件:

- 新しいエンジン タスクが作成される。
- エンジン タスクのエリアのアクセス権が、エンジン タスクの作成ユーザのプロファイルから取得されています。
- オブジェクトのアクセス権が、アセット ジョブのセキュリティ クラスのクラス レベルのアクセス権に基づいて作成されます。

ユース ケース: エリアの管理

エリアの管理に関する以下の重要なユーザ シナリオは、セキュリティ エリアのサポートのコンテキストで考慮されます。

- [最初のエリア コードのサポートの有効化](#) (P. 653)
- [エリア コードのサポートの無効化](#) (P. 654)
- [エリア コードのサポートの再有効化](#) (P. 654)
- [デフォルトのエリアのアクセス権の変更](#) (P. 655)
- [新しいエリアの追加](#) (P. 655)
- [エリアの削除](#) (P. 656)

ユース ケース: 最初のエリア コードのサポートの有効化

シナリオ

管理者がすべてのセキュリティ プロファイルに対して、過去に無効に設定されていたエリア コードを有効化します。

前提条件:

- エリア コードのサポートが無効になっており、**Client Automation** 製品がすでに使用されています。
- 保護されたオブジェクトおよびプロファイルが、エリアのサポートが無効になっている間に作成されました。

アクション

管理者は、エリア コードのサポートを有効にします。

事後条件:

- エリア コードのサポートが、**MDB** で有効になっています。
- すべてのプロファイルのエリア コードが、セキュリティ プロファイルの作成時に定義されたようにデフォルトのエリア コードに設定されています。
- 既存の保護されたオブジェクトのエリア コードが、セキュリティ プロファイルで定義されたエリア コードに設定されています。

注: このことは、管理者がエリア コードのサポートを初めて有効にした後で、1つ以上のエリア コードを明示的にセキュリティ プロファイルへ割り当てる必要があることを意味します。

ユース ケース: エリア コードのサポートの無効化

シナリオ

管理者がすべてのセキュリティ プロファイルに対してエリア コードを無効にします。

事前条件:

エリア コードが MDB で正しく設定されています。

アクション

管理者は、エリア コードのサポートを無効にします。

事後条件:

- MDB のフラグが、エリア コードを無効にするよう設定されています。
- エリア コード自体は、削除も変更もされていません。

ユース ケース: エリア コードのサポートの再有効化

シナリオ

管理者がすべてのセキュリティ プロファイルに対してエリア コードを再び有効にします。

事前条件:

エリア コードが MDB で正しく設定されていますが、エリア コードのサポートは無効に設定されています。

アクション

管理者は、エリア コードのサポートを有効にします。

事後条件:

- MDB のフラグが、エリア コードを有効にするよう設定されています。
- エリア コード自体は、エリア コードのサポートが無効になる前と同じです。

ユース ケース: デフォルトのエリアの権限の変更

シナリオ

デフォルトのエリアの権限を変更します。

事前条件:

Client Automation がインストールされています。

アクション:

デフォルトの権限を変更します。

事後条件:

- MDB に格納されているデフォルトのエリアの権限が変更されます。
- セキュリティ レベルが「デフォルト値」に設定されているエリアの権限もすべて変更されます。

ユース ケース: 新しいエリアの追加

シナリオ

ユーザが新しいエリア定義を作成します。

事前条件:

ユーザは、1つのセキュリティ プロファイルのメンバです。エリアのサポートを制御するセキュリティ クラス (SEC_CLSID_COM_CONTROL_AREA) で、少なくとも新しいエリアの作成が許可されています。

アクション

ユーザが新しいエリア定義を作成します。

事後条件:

新しいエリアが作成されています。

ユース ケース: エリアの削除

シナリオ

ユーザがエリア定義を削除します。

事前条件:

ユーザは、1つのセキュリティプロファイルのメンバです。エリアのサポートを制御するセキュリティクラス (SEC_CLSID_COM_CONTROL_AREA) で、少なくともエリアの削除が許可されています。

アクション

ユーザがエリア定義を手動で削除します。

事後条件:

- エリアが削除されます。
- エリアが存在しなくなったエリアのアクセス権が更新されます。

ユース ケース: 所有権の取得

所有権を取得しても、オブジェクトのエリアのアクセス権は変更されません。

付録 F: CAF でスケジュールされたジョブ

共通アプリケーション フレームワーク (CAF) で実行するスケジュール済みジョブを指定する完全なルールは、以下のとおりです。これらのジョブには、一定または任意の間隔での `caf` コマンドの実行が含まれています。たとえば、1 日に 1 回、Asset Management エージェントを実行する標準ジョブなどがあります。

このセクションには、以下のトピックが含まれています。

[CAF 標準ジョブおよびパラメータ \(P. 657\)](#)

[CAF でスケジュールされたジョブの例 \(P. 660\)](#)

CAF 標準ジョブおよびパラメータ

CAF は標準ジョブの集合と共にインストールされます（詳細については、*DSM* エクスプローラ ヘルプの「設定ポリシー」の「CAF ポリシー グループ」を参照してください）。

ジョブは、設定ストア (`comstore`) の以下のキーに格納されているパラメータのセットで記述されています。

`itrm/common/caf/scheduler/name_of_job`

スケジューラ自体は、上記のキーで「有効な」パラメータを設定して、有効化したり、無効化することができます。

ジョブのパラメータは、以下のとおりです。

desc

ジョブ記述を定義します。これはトレース ログに表示されます。

enabled

ジョブが有効かどうかを示します。有効値は次のとおりです。1= ジョブが有効です。0= ジョブが有効ではなく、実行されません。

type

ジョブのタイプを指定します。これにより、ジョブを繰り返す時間フレームが決定され、以下の値のいずれかになります。

day

数日おきに一定の時間および分単位でジョブを実行します。

hour

数時間おきに一定の分単位でジョブを実行します。

minute

数分おきにジョブを実行します。

以下の追加キーワードを指定することもできます。

now

今すぐおよびその後のスケジュールされた間隔でジョブを実行します。この場合、「今すぐ」とは、「cafの起動時」を意味します。

randomnowtime パラメータが設定されている場合、ジョブは最大 **randomnowtime** の値までの任意の秒数内で実行されます。これは、一緒に起動されるコンピュータが同時にそれぞれのジョブをすべて開始しないようにするために使用されます。

random

指定した期間および最大 **randomminutes** パラメータの値までの任意の分数でジョブを実行します。これはサーバへの接続を含むジョブの使用されます。こうすると、エージェントの接続時間がランダム化され、サーバの負荷を分散するのに役立ちます。

random_hour

その日付内の任意の時間にジョブを実行するよう指定します。日次スケジュールで使用されます。

random_minute

その時間内（任意の時間にすることも可能）の任意の分数にジョブを実行するよう指定します。日次および時間スケジュールで使用されます。

excludeDays

月曜日や火曜日など、スケジュールから除外する曜日の名前を指定します。各曜日はスペースで区切ります。たとえば、「**Monday Wednesday**」という設定では、月曜日および水曜日にはジョブが実行されません。

excludeHours

24 時間表示を使用してスケジュールから除外する時間数を指定します。各時間はスペースで区切ります。たとえば、「**1 15**」という設定では、**1:00 a.m.** および **3:00 p.m.** にはジョブが実行されません。

hour

24 時間表示を使用してジョブを開始する時間数を指定します。これは日次スケジュールでのみ使用されます。

minute

ジョブを開始する時間を分単位で指定します。これは日次および時間スケジュールで使用されます。

repeat

「**type**」プロパティにより定義された時間単位ごとに繰り返します。たとえば、ジョブタイプが「**hour**」の場合、「**repeat**」によりジョブ間の時間数が指定されます。

randomnowtime

秒数を指定します。CAF が起動したら、「**now**」と指定されたジョブがこの秒数内で任意の回数実行されます。

randomminutes

分数を指定します。指定した期間および最大このパラメータの値までの任意の回数、ジョブが実行されます。

cmd

このジョブを実行するための **caf** コマンドを指定します。これは、ホスト、ユーザ、およびパスワードオプションが使用できないことを除いて、コマンドラインと同じです。

CAF でスケジュールされたジョブの例

例: 毎正時に amagent プラグインが実行されます。

```
type="hour", repeat=1, minute=0, cmd="start amagent"
```

例: amagent が毎日 2:30 p.m に実行されます。

```
type="day", repeat=1, hour=14, minute=30, cmd="start amagent"
```

例: CAF の起動時、およびそれ以降は週末を除き毎日 1:00 a.m. から 2:30 a.m. までの間のランダムな時間に、amagent が実行されます。

```
type="day now random", hour=1, minute=0, randomminutes=90, excludedays="saturday  
sunday", cmd="start amagent"
```

付録 G: FIPS 140-2 準拠

この付録では、CA ITCM での暗号化の使用、特に FIPS 140-2 publication standard の準拠レベルについて説明します。

このセクションには、以下のトピックが含まれています。

[FIPS PUB 140-2](#) (P. 661)

[参照](#) (P. 662)

[サポートされている FIPS モード](#) (P. 662)

[暗号化モジュール - RSA Crypto](#) (P. 663)

[暗号化セキュリティ機能](#) (P. 663)

[コンポーネント固有の暗号化の使用](#) (P. 665)

[Client Automation 以外の FIPS 準拠コンポーネント](#) (P. 666)

[認定されていないセキュリティ機能の使用](#) (P. 668)

FIPS PUB 140-2

FIPS 140-2 は、セキュリティ システムで使用する暗号モジュールのセキュリティ要件を定めたセキュリティ規格です。これは NIST によって提唱された規格で、CMVP (Cryptographic Module Verification Program: 暗号モジュール評価プログラム) を通して暗号化モジュールの動作の評価や認証を行います。CMVP は NIST に認定された試験機関によって運営されており、暗号化モジュールのテストや評価を行います。FIPS 140-2 規格から生成したテスト要件に対してモジュールがテストされます。

FIPS 140-2 認定モードでの使用を評価および承認された各機能については、CAVP (Cryptographic Algorithm Validation Program : 暗号アルゴリズム評価プログラム) の元、モジュールの FIPS 140-2 認定書に機能が承認されたことが記録されます。認定書には、認定機能および非認定機能、FIPS 140-2 認定モードの操作で使用可能な機能の記述など、モジュールが提供するすべての機能がリストされています。

各認定モジュールは、関連するセキュリティ ポリシー ドキュメントを発行します。このドキュメントには、FIPS 140-2 規格に準拠するためにモジュールがどのように動作させる必要があるかが記述されています。

注: FIPS 140-2 に承認されたと認定されるのは、暗号化モジュールのみです。アプリケーションは認定された操作モードで FIPS 140-2 認定モジュールを使用できませんが、認定はされません。

参照

CMVP（暗号モジュール評価プログラム）の詳細については、NIST の Web サイトを参照してください。

<http://csrc.nist.gov/groups/STM/cmvp/>

以下の URL では、評価されたモジュールと関連するセキュリティ ポリシーへのリンクが表示されます。

<http://csrc.nist.gov/groups/STM/cmvp/validation.html>

この付録で説明されている認証番号に関する情報は上記の URL で確認できます。

サポートされている FIPS モード

Client Automation は、以下のいずれかのモードで動作します。

FIPS 推奨

FIPS 推奨モードでは、Client Automation は FIPS 140-2 認定セキュリティ機能を使用します。ただし、レガシー Client Automation コンポーネントと通信する際には、レガシーセキュリティ機能を使用します。このモードでは、MD5 のような非認定セキュリティ機能を使用する必要があるので、組み込み型暗号化モジュールは FIPS 140-2 認定モードでは動作しません。FIPS 推奨モードで操作する場合、Client Automation は以前のリリースの Client Automation との通信や操作を行うことができます。

FIPS のみ

FIPS のみのモードでは、Client Automation は FIPS 140-2 認定セキュリティ機能のみを使用します。このセクションの後で説明するように、非認定セキュリティ機能を暗号化せずに使用場合があります。ただし、FIPS 140-2 認定モードで操作する場合、これらは組み込み型暗号化モジュールでは提供されません。このモードでは、Client Automation は FIPS 推奨または FIPS のみのモードで、FIPS に準拠したコンポーネントとのみ通信できます。

注：この付録では特に Client Automation が FIPS のみのモードで操作する場合の暗号化の使用について説明します。

暗号化モジュール - RSA Crypto

Client Automation では、以下の暗号化モジュールを直接使用および実装します。

- RSA Crypto-C ME Version 2.1; CMVP certificate #828

以下は、この暗号化モジュールのセキュリティ ポリシーの抜粋です。

「This Cryptographic Module is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module must be tested upon a particular operating system and computer platform. The cryptographic boundary thus includes the Cryptographic Module running on selected platforms running selected operating systems while configured in "single user" mode. The Cryptographic Module was validated as meeting all FIPS 140-2 level 1 security requirements, including cryptographic key management and operating system requirements. The Cryptographic Module is packaged as a dynamically loaded module or shared library file which contains all the module's executable code. Additionally, the RSA BSAFE Crypto-C ME toolkit relies on the physical security provided by the host PC in which it runs.」

暗号化セキュリティ機能

以下の表では、Client Automation がさまざまなセキュリティ機能に使用する RSA Crypto-C モジュールの暗号化アルゴリズムを示します。

セキュリティ機能	暗号化アルゴリズム	認証証明書番号	コメント
非対称暗号化および複合化	RSA 暗号化および複合化	非認定	キー転送用に FIPS 140-2 モードで許可
対称暗号化および複合化	AES CBC	490	FIPS PUB 197 - 次世代暗号化規格
	Triple-DES	510	FIPS PUB 46-3 - データ暗号化規格 FIPS SP 800-67 - TDEA (Triple Data Encryption Algorithm) ブロック暗号に推奨 ANSI X9.52 - TDEA に承認された操作モード
ハッシュ関数	SHA-1	560	FIPS PUB 180-3 - セキュア ハッシュ規格

セキュリティ機能	暗号化アルゴリズム	認証証明書番号	コメント
	SHA-256	560	FIPS PUB 180-3 - セキュア ハッシュ規格
	SHA-512	560	FIPS PUB 180-3 - セキュア ハッシュ規格
乱数生成	PRNG	270	FIPS PUB 186-2 - デジタル署名規格 詳細については、「FIPS PUB 186-2 Digital Signature Standard」ドキュメントの「Appendix 3: Random Number Generation For The DSA」を参照してください。
非対称鍵の確立	TLS 1.0	適用不可	FIPS 認定暗号化スイートと共に「FIPS 140-2 Implementation Guidance」ドキュメントで許可
	SSH v2	適用不可	FIPS 認定暗号化スイートと共に「FIPS 140-2 Implementation Guidance」ドキュメントで許可

コンポーネント固有の暗号化の使用

このセクションでは、**Client Automation** が **FIPS** のみのモードで動作している場合のコンポーネント固有の暗号化の使用方法について説明します。

ノード間の通信[セッション メッセージング]

セッション メッセージング コンポーネントは、ノード間の通信に **TLS v1.0** プロトコルを使用します。選択された暗号化スイートは、通信するノード間のネゴシエーションによって選択されます。

いくつかのインスタンスでは、セッション メッセージ コンポーネントは **RFC3369** の **Cryptographic Message Syntax** バージョン 3（**CMS3**）で指定されているように **Key Transport Recipient Information** 構造を使用します。

ストリームベースのネットワーク

ストリームベースのネットワーク コンポーネントは、ノード間の通信に **TLS v1.0** プロトコルを使用します。選択された暗号化スイートは、通信するノード間のネゴシエーションによって選択されます。

Remote Control - ローカル アドレス帳

Remote Control - ローカル アドレス帳のエントリは乱数 **IV** を伴う **CBC** モードで **3DES** アルゴリズムによって保護されます。

Desktop Migration Manager [DMM]

DMM は、通信に **TLS v1.0** プロトコルを使用します。また、乱数 **IV** を伴う **CBC** モードで **192** ビット キーの **AES** アルゴリズムを使用します。

ENC

現在、Client Automation で ENC 機能が提供されるのは Windows のみであるため、Microsoft SCHANNEL プロバイダである Microsoft 認証ストア、およびその基礎となる Microsoft 暗号化サービス プロバイダ (RSAENH) と密接に統合されています。Microsoft 暗号化サービス プロバイダの FIPS ステータスの詳細については、「FIPS 認定 (667P.)Windows 動作環境」を参照してください。

OSIM および Software Delivery

OSIM および Software Delivery では、乱数 IV を伴う CBC モードの AES アルゴリズムによって提供された対称暗号化を使用します。また、RFC 3369 で指定されている Cryptographic Message Syntax バージョン 3 (CMS3) を使用して構成されます。

共通オブジェクト マネージャ、共通エンジン、SMS 抽出

共通オブジェクト マネージャ、共通エンジン、SMS 抽出コンポーネントは、乱数 IV を伴う CBC モードで 3TDES アルゴリズムを使用します。

プラットフォーム仮想化 - ESX モジュール

ESX モジュールは、リモート VMware ESX ノードとのコミュニケーションに TLS v1.0 プロトコルを使用します。

DTS

DTS プログラムでは、AES または 3TDES のアルゴリズムによって提供される対称暗号化を使用します。キー サイズは変化しますが、すべて乱数 IV を伴う CBC を使用します。

CCS

Client Automation は CA Common Services を利用できます。CA Common Services はオプションでインストールできます。CA Common Services の FIPS 準拠レベルの詳細については、CA マニュアル選択メニューから参照する「CA NSM 管理ガイド」の付録 B 「FIPS 140-2 暗号化」をご覧ください。

Client Automation 以外の FIPS 準拠コンポーネント

マシンには、Client Automation アプリケーション以外にも暗号化を使用するものが多く存在します。

Windows 動作環境

さまざまな Windows 動作環境にある Microsoft Enhanced Cryptographic Service Provider [RSAENH CSP] は FIPS-140 認定です。FIPS 認定動作環境のリストについては、「<http://technet.microsoft.com/en-us/library/cc750357.aspx>」を参照してください。また、このリンクでは FIPS 準拠の暗号化を使用するためにローカルセキュリティ ポリシーを有効にする方法について説明しています。ENC を FIPS 準拠にするには、ローカルセキュリティ ポリシー（システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う）を設定する必要があります。

注：FIPS のみのモードで操作する、つまり FIPS 準拠の暗号化のみを許可することによる影響を慎重に検討してください。詳細については、「[FIPS 140-2 のサポート \(P. 90\)](#)」を参照してください。

SQL Server

バージョン 2005 SP1 以降の Microsoft SQL Server は FIPS に準拠しています。FIPS 準拠モードで動作するように SQL Server を設定する方法の詳細については、「Microsoft サポート技術情報のエントリー 920995 (<http://support.microsoft.com/kb/920995/>)」を参照してください。

その他のコンポーネント

Client Automation は、ビジネス ソリューションを提供するアプリケーションおよびコンポーネント モジュールのスイートです。ソフトウェア パッケージとして、Client Automation は他の CA グループおよびサードパーティ プロバイダからのコンポーネントおよびサービスを利用します。言及されていない場合、これらのどのコンポーネントおよび（または）サービスでも Client Automation に暗号化機能を直接実装したり提供することはありません。そのため、これらが FIPS 140-2 認定暗号化モジュールに準拠しているかどうかは記述されていません。FIPS 140-2 関連の情報については、コンポーネント プロバイダのサポート ドキュメントを参照してください。

また、オペレーティング システムの暗号化操作は、オペレーティング システム ベンダーの権限事項です。準拠レベルおよび（または）サポートされる設定を含め、FIPS 140 および共通基準のサポートについては、FIPS 140-2 関連のドキュメントを参照してください。

注：Client Automation に付属する最新のコンポーネント リストについては、互換性マトリックスを参照してください。

認定されていないセキュリティ機能の使用

Client Automation では、FIPS 140-2 で許可されていないセキュリティ機能を使用する場合があります。これは、FIPS-のみのモードで実行されている Client Automation の通常の操作には影響を与えません。

Asset Management エージェント - ソフトウェア シグネチャ スキャナ

ソフトウェア シグネチャで <file> タグに属性値「md5」が含まれている場合、シグネチャ スキャナは MD5 コードをプライベートで実装します。このスキャナは、正の結果を返す前に、エージェント コンピュータ上で見つかった任意のファイルの MD5 ダイジェストが「md5」属性に一致するかどうかを確認します。ソフトウェア シグネチャ スキャナでは、MD5 は暗号化に使用されません。

インストール

Client Automation インストール中、PKCS#12 ベースのファイルは証明書およびキー インストールに使用できます。これらのファイルは、PKCS#5 v2.0 規格の PBKDF2 のようなパスワード ベースのキー派生機能 (PBKD) で生成したキーを使用して暗号化されます。インストール中、これらのファイルはパスワード ベース以外の技術を使用して抽出および保護されます。

注: パスワード ベースのキー派生 (パスワード ベースのキー確立) を非対称鍵共有に使用することは、「FIPS 140-2 Implementation Guidance」ドキュメントのセクション 7.1 に記述されているように明示的に許可されていません。

付録 H: アクセシビリティ機能

CA Technologies では、すべてのお客様が弊社の製品およびサポート ドキュメントを正しく使用して重要なビジネス業務を遂行できるよう、全力を尽くしています。このセクションでは、**Client Automation** に用意されているアクセシビリティ機能について説明します。

このセクションには、以下のトピックが含まれています。

[製品の機能拡張](#) (P. 671)

[Remote Control ビューで文字列が切り捨てられる](#) (P. 675)

[リンク リストの内容がフォーカスによって変化する](#) (P. 677)

[Remote Control ビューアおよびリプレイヤーでの JAWS スクリーン リーダの使用](#) (P. 679)

[リモート セッションの制限](#) (P. 681)

[高コントラスト モードの機能](#) (P. 683)

付録 I: 製品の機能拡張

Client Automation では、以下の領域でアクセシビリティが機能拡張されています。

- 表示形式
- 音声
- Keyboard
- マウス

注: 以下の情報は Windows ベースおよび Macintosh ベースのアプリケーションに適用されます。Java アプリケーションは多数のホストオペレーティングシステムで実行されており、これらのシステムの一部にはすでに Java アプリケーションで使用可能な支援テクノロジーがあります。これらの既存の支援テクノロジーで、JPL で記述されたプログラムへのアクセスを提供するには、ネイティブ環境における支援テクノロジー自体と、Java 仮想マシン (Java VM) 内から使用可能な Java Accessibility サポートとの間のブリッジが必要です。このブリッジは、両端が Java VM とネイティブプラットフォームであるため、ブリッジ先のプラットフォームごとに若干異なります。Sun では現在、このブリッジの JPL 側と Win32 側の両方を開発しています。

表示形式

コンピュータ画面の表示を見やすくするには、以下のオプションを調整します。

- フォントスタイル、色、およびアイテムのサイズ
フォントの色、サイズ、その他の表示の組み合わせを選択できます。
- 画面の解像度
ピクセル数を変更して、画面上でオブジェクトを拡大できます。

- カーソルの幅および点滅速度
カーソルを見つけやすくしたり、点滅速度を最小化したりできます。
- アイコンのサイズ
アイコンを大きくして見やすくしたり、アイコンを小さくして画面のスペースを増やしたりできます。
- 高コントラストの配色
見やすい色の組み合わせを選択できます。

注:

- 現在の GUI を使用する代わりに、Windows Vista より前のオペレーティングシステム用に別のユーザ インターフェースを有効にする必要がある場合は、[Software Delivery] - [エージェント] - [ログオン ユーザ用に常に GUI を表示する] 設定ポリシーを適用してください。
- Windows Vista より前のオペレーティングシステムで支援テクノロジー (AT) を有効にして SD ジョブ確認ウィンドウからテキストを読み込むには、[Software Delivery] - [エージェント] - [ログオン ユーザ用に常に GUI を表示する] 設定ポリシーをエージェントに適用してください。

音声

画像の代わりに音声を使用するか、またはコンピュータ サウンドを聞きやすくしたり区別しやすくしたりするには、以下のオプションを調整します。

- ボリューム
コンピュータ サウンドの音量を上げたり下げたりできます。
- 音声変換
音声で読み上げたコマンド オプションやテキストを聞くことができます。
- 警告
目に見える警告を表示できます。
- 通知
アクセシビリティ機能がオンまたはオフになったときに、聴覚的または視覚的な合図を出します。
- スキーム
コンピュータのサウンドと特定のシステム イベントを関連付けることができます。
- キャプション
スピーチおよびサウンドのキャプションを表示できます。

Keyboard

以下のようにキーボードを調節できます。

- 表示の間隔

キーを押したときにどのくらいの速度で文字を繰り返すかを設定できます。

- トーン

特定のキーを押したときに音が鳴るようにできます。

- スティッキー キー

片手または 1 本の指で入力するユーザは、別のキーボード レイアウトを選択できます。

キーボード ショートカット

以下の表に、**Client Automation** でサポートされているキーボード ショートカットを示します。

Keyboard	説明
Ctrl + X キー	切り取り
Ctrl + C キー	コピー
Ctrl + K キー	次を検索
Ctrl + F キー	検索置換
Ctrl + V キー	貼り付け
Ctrl + S キー	保存
Ctrl + Shift + S キー	すべて保存
Ctrl + D キー	行の削除
Ctrl + 右方向キー	次の語句
Ctrl + 下方向キー	下にスクロール
End	行の終わり

注: この機能パックでは、製品のアクセシビリティ機能を拡張するためにホットキー (F6) を追加しました。F6 キーを使用すると、**Software Delivery** カタログと **Remote Control** ビューアのペイン間をより簡単に移動できるようになります。

マウス

以下のオプションを使用して、マウスの動作を速くしたり使いやすくしたりできます。

- クリック速度

選択するときのマウス ボタンのクリック速度を選択できます。

- クリック ロック

マウス ボタンを押したままにしなくても強調表示したりドラッグしたりできます。

- アクションの入れ替え

マウスの左ボタンで制御される機能と右ボタンで制御される機能を入れ替えることができます。

- 点滅速度

カーソルの点滅速度を選択したり、点滅させるかどうかを選択したりできます。

- ポインタのオプション

以下の操作を実行できます。

- 入力中のポインタの非表示

- ポインタ位置の表示

- ポインタが画面を移動する速度の設定

- 視認性向上のためのポインタのサイズおよび色の選択

- ダイアログ ボックス内のデフォルト位置へのポインタの移動

付録 J: Remote Control ビューで文字列が切り捨てられる

Remote Control ビューアで表示設定をハイコントラストに変更すると、テキストの一部が切り捨てられることがあります。回避策として、代替 (ALT) テキストが提供されています。

付録 K: リンク リストの内容がフォーカスによって変化する

Remote Control ビューアでは、Insert+F7 キーでリンク リスト ウィンドウにすべてのリンクが表示されません。リンク リストの内容は、フォーカスによって変化することがあります。これは、Remote Control ビューア ページには 2 つの HTML ビューが存在するためです。

フォーカスがある HTML ビューのリンクがリンク リスト ウィンドウに表示されます。HTML ビューを切り替えるには、F6 ホット キーを押します。これは、スクリーン リーダで画面に表示される情報を読み上げる際に役立ちます。スクリーン リーダの動作は、HTML ビューのフォーカスによって変わるためです。Remote Control ビューア ページには 2 つの HTML ビューがあるため、スクリーン リーダはフォーカスがある HTML 表示を読み上げます。

付録 L: Remote Control ビューアおよびリプレイヤーでの JAWS スクリーンリーダーの使用

JAWS® スクリーンリーダーソフトウェアを使用する場合、複数の HTML ビューで構成されるウィンドウを読み上げる際に既知の問題が存在します。継続して使用していると、キーボードナビゲーションとリンクのアクティブ化で予期しない動作が発生する場合があります。

一貫性を向上させるために、[表示]-[現在]メニューを使用して、**Remote Control** ビューアまたはリプレイヤーの「**Web ページとして**」オプションを無効にすることをお勧めします。また、使用中でない場合はチュートリアルバーを非表示にしてください。

また、**JAWS+Z** キーを使用して仮想 PC カーソルを無効にすることによっても **Remote Control** ビューアの表示結果を向上させることができます。

付録 M: リモート セッションの制限

Remote Control ビューアでは、スクリーン リーダ、および表示設定の変更はリモート セッションに対しては機能しません。

付録 N: 高コントラスト モードの機能

高コントラスト モードでは、**Remote Control** ビューアは画面表示を自動的に変更して、ユーザ インターフェースの視認性を向上させます。**Remote Control** ビューアの使用中にハイコントラスト モードの有効/無効を切り替えた場合は、別のノードに切り替えるなどの操作を行って **GUI** をリフレッシュすることで、ハイコントラストの変更が表示されます。

注: **Remote Control** ビューア チュートリアル ページをリフレッシュするには、チュートリアル内の任意のリンクをクリックします。

用語集

CCE (Common Configuration Enumeration)

CCE (Common Configuration Enumeration) は、SCAP 標準の 1 つです。標準 ID、およびセキュリティに関連したシステム設定の問題用のディクショナリを含んでいます。SCAP データ ストリームのルール定義には、1 つ以上の CCE ID を含むことができます。ルールが特定の CCE 設定ガイダンス ステートメントまたは構成制御であることを示しています。詳細については、<http://cce.mitre.org/> にアクセスしてください。

CPE (Common Platform Enumeration)

CPE (Common Platform Enumeration) は、SCAP 標準の 1 つです。標準 ID、およびプラットフォーム/製品の命名用のディクショナリを含んでいます。たとえば、XCCDF ファイルのエレメントは、特定のプラットフォームのみに適用を制限できます。これは、CPE ID を使用して行います。詳細については、<http://cpe.mitre.org/> にアクセスしてください。

CVE (Common Vulnerabilities and Exposures)

CVE (Common Vulnerabilities and Exposures) は、公開されている情報セキュリティの脆弱性に関する共通名 (CVE 識別子) の辞書です。これらの識別子は、個別のネットワークセキュリティ データベースおよびツール同士で容易にデータを共有することが可能になります。CVE は SCAP で使用されるコンポーネントの 1 つです。詳細については、<http://cve.mitre.org/> を参照してください。

CVSS (Common Vulnerability Scoring System)

CVSS (Common Vulnerability Scoring System) は、SCAP 標準の 1 つです。脆弱性の影響の伝播、およびスコアリングするための標準を含んでいます。詳細については、<http://www.first.org/cvss/index.html> にアクセスしてください。

FIPS 準拠の暗号

*FIPS 準拠の暗号方式*とは、暗号方式に FIPS 140-2 認定モジュール、FIPS 承認および FIPS 許可技術およびアルゴリズムを使用していることを意味します。

FIPS 推奨

*FIPS 推奨*とは、Client Automation の操作モードの 1 つです。このモードでは、暗号化操作の大部分が FIPS に準拠しており、レガシー形式の暗号はほとんど残っていません。- このモードでは、Client Automation は以前のリリースの Client Automation と下位互換性があります。 -

FIPS 認定暗号化モジュール

*FIPS 認定暗号化モジュール*とは、RSA CryptoC BSAFE モジュールのことです。これは、FIPS 140-2 認定です。

FIPS のみ

*FIPS のみ*とは、**Client Automation** の操作モードの 1 つです。**FIPS** 準拠の暗号化のみが許可されます。このモードでは、**Client Automation** は前のリリースの **Client Automation** と下位互換性がありません。

MITRE

MITRE Corporation は、公共の利益のために設立された非営利組織です。**MITRE** は、インタープリタ、ソースコード、スキーマ、およびデータファイルが無償で提供し、個人および組織はそれらを発展、拡張させることが可能です。**Ovaldi** は、自由に使用できるそのようなインタープリタの 1 つです。

NIST (National Institute of Standards and Technology)

NIST (National Institute of Standards and Technology) は、米商務省内の非規制型連邦政府関係機関です。**NIST** の任務は、経済の安定を高め、生活の質を向上させるようなやり方で、計測学、標準、およびテクノロジーを進歩させることによって、米国の革新と産業競争力を促進することです。**NIST** によって運営されている「**The United States (U.S) National Vulnerability Database (NVD)**」は、**SCAP** 標準を利用できるコンテンツのリポジトリとデータフィードを提供しています。それは、特定の公式 **SCAP** 標準データのリポジトリでもあります。したがって、**NIST** は、**SCAP** コンテキスト内でオープンスタンダードを定義し、一連の **SCAP** 標準間のマッピングを定義しています。

OVAL (Open Vulnerability and Assessment Language)

OVAL (Open Vulnerability and Assessment Language) は、**SCAP** 標準の 1 つです。**OVAL** には、ソフトウェアの欠陥、設定の問題、およびパッチに関連するセキュリティをテストするプロシージャ用の標準 XML と、テスト結果のレポート用の標準 XML が含まれます。チェックリストでチェックするすべてのルールは、**SCAP** データストリームから **OVAL** ファイル内にある **OVAL** 定義への参照の形式を取ります。詳細については、<http://oval.mitre.org/> にアクセスしてください。

Ovaldi

Ovaldi は、**MITRE Corporation** によって開発された **OVAL** インタープリタです。これは、テストするコンピュータのプラットフォーム用の **OVAL** 定義を実行し評価するために、そのコンピュータからどのように情報が収集できるかを示すため、およびそのテスト結果をレポートするために作成された自由に使用できる参照目的の実装です。インタープリタは、**OVAL** 定義の有用性を実証し、正しい構文と **OVAL** スキーマの順守を確実にします。

SCAP (Security Content Automation Protocol)

SCAP (Security Content Automation Protocol) (「S Cap」と発音される)は、XCCDF、CCE、CVE、CVSS、CPE、および OVAL などの標準を使用する方式であり、自動化された脆弱性管理、測定、およびポリシー コンプライアンス評価 (例、FISMA コンプライアンス) を可能にします。特に、SCAP は、ソフトウェアの欠陥、セキュリティ関連の構成の問題、および製品名を列挙し、脆弱性の存在を調査するためにシステムを測定し、また検出されたセキュリティの問題の影響を評価するために、これらの測定結果をランク (スコア) 付けするメカニズムを提供する、選択されたオープンスタンダードのセットです。SCAP では、これらの標準をどのように組み合わせるかを定義します。National Vulnerability Database は、リポジトリおよび SCAP 標準を使用するコンテンツのデータ フィードを提供します。詳細については、<http://nvd.nist.gov/> にアクセスしてください。

SCAP データ ストリーム

SCAP データ ストリームは、自動化 XML 形式で表されるセキュリティ チェックリスト データ、脆弱性と製品名の列挙、および列挙間のマッピングから構成されます。SCAP データ ストリームは、XML の以下のファイルから構成されます。

- XCCDF ファイル
- 1つ以上の OVAL ファイル
- (オプション) CPE ディクショナリ ファイル

vDisk

Citrix XenDesktop では、vDisk (仮想ディスク) は基本的に、OS と必要なアプリケーション セットを含むイメージファイルです。

XCCDF (eXtensible Configuration Checklist Description Format)

XCCDF (eXtensible Configuration Checklist Description Format) は、セキュリティ チェックリスト、ベンチマーク、および関連するドキュメントを記述するための言語仕様です。XCCDF ドキュメントは、ターゲット システムのセットに対するセキュリティ設定ルールの集合を構造化して表示します。この仕様は情報交換、ドキュメント生成、組織および状況への適合、自動化されたコンプライアンス テスト、およびコンプライアンス スコアリングをサポートするように設計されています。詳細については、<http://nvd.nist.gov/xccdf.cfm> にアクセスしてください。

XCCDF プロファイル

XCCDF プロファイルは、ターゲット システムに適用するか、またはターゲット システムの設定と比較するポリシーです。各 SCAP データ ストリームの XCCDF ファイルは、サポートされているプロファイルのリストを定義します。XCCDF ファイルは、1つ以上の XCCDF プロファイルを持つ必要があり、特定のタイプのシステムをチェックするために使用するルールを指定します。システムが展開されている適用可能な各稼働環境の個別の XCCDF プロファイルを作成できます。

アプリケーション

アプリケーションとは、Microsoft Word などの 1つのソフトウェアです。

アプリケーション仮想化

アプリケーション仮想化とは、アプリケーションをカプセル化することです。アプリケーションが実行されている基になるオペレーティング システムからアプリケーションを分離します。実行時には、アプリケーションが元のオペレーティング システムおよびそれによって管理されているリソースと直接やりとりしているように見えますが、実際はそうではありません。

インスタンス ソフトウェア状態データベース

インスタンス ソフトウェア状態データベースは、ソフトウェア状態データベースの一部であり、非ゴールデン テンプレート システム（つまり、ゴールデン テンプレートのすべてのクローン）上で動作しているエージェントによって実行されたすべてのソフトウェア ジョブの履歴を含みます。

永続クローン

永続クローンは、ユーザがログオフされた後も更新または再構成されるまでそのまま残る、永続プールからの仮想デスクトップです。VMware View は、永続クローンを含むシステムおよびユーザ データのための標準装備の個別デバイスを提供します。ユーザ データ デバイスに格納された情報は更新または再構成アクションの後に残りますが、システム ディスクへの変更は失われます。

永続非リンク クローン仮想デスクトップ

永続非リンク クローン仮想デスクトップは、特定のユーザ専用の仮想マシンであり、カスタムのインストール済みアプリケーション、ユーザ設定、データなどと共に、各ログオン時にそのユーザに提供されます。

永続リンク クローン仮想デスクトップ

永続リンク クローン仮想デスクトップは、特定のユーザ専用の仮想マシンであり、ユーザは特定のソフトウェアの追加を要求したり、設定をカスタマイズしたりすることができます。各ログオン時に、ユーザのカスタマイズされた環境が復元されます。これは、仮想デスクトップが更新または再構成されるまで持続されます。その時点で、システム ドライブ上にインストールされたすべてのソフトウェア製品が失われます。

オフライン RAC

オフライン RAC は、マネージャではなくエージェントによって起動される、クラッシュ後の再インストール（RAC）タスクです。仮想デスクトップは頻繁に再構成されます。つまり、ゴールデン テンプレートが更新され、ディスクがリセットされた場合は常に、以前のリセット以降の仮想デスクトップへの変更がすべて実質的に無効になります。仮想デスクトップでは、マネージャではなくエージェントが RAC ジョブ コンテナの作成を担当します。ディスク リセットが発生すると、エージェントは、そのエージェントに展開されているソフトウェアをすべて復元するためにオフライン RAC を開始します。

オフラインパッチ

オフラインパッチでは、パッチ コンテンツおよびパッチ ファイルをリモートでエクスポートし、インターネットにアクセスせずに、CA Patch Manager を使用して Client Automation 環境にインポートできます。

仮想アプリケーション (VA)

仮想アプリケーションとは、仮想化されたソフトウェアです。

仮想アプリケーションイメージ

仮想アプリケーションイメージには、サポートするメタデータ ファイルセットと共に、1つのファイルに格納された1つ以上の仮想アプリケーションが含まれます。

仮想アプリケーションイメージ定義

仮想アプリケーションイメージ定義とは、仮想アプリケーションイメージを検出するための「足跡」を意味します。1つ以上の仮想アプリケーションが含まれる（内部に格納されている）イメージを検出するには、非仮想ソフトウェアのシグネチャが仮想アプリケーションイメージ定義に関連付けられている必要があります。

仮想アプリケーションスタンドアロンパッケージ

仮想アプリケーションスタンドアロンパッケージとは、スタンドアロン モードで仮想アプリケーションをプロビジョニングするために使用する仮想アプリケーションパッケージです。

仮想アプリケーションステージングパッケージ

仮想アプリケーションステージングパッケージとは、仮想アプリケーションイメージをステージングするために使用する仮想アプリケーションパッケージです。

仮想アプリケーションストリーミングパッケージ

仮想アプリケーションストリーミングパッケージとは、ストリーミング モードで仮想アプリケーションをプロビジョニングするために使用される仮想アプリケーションパッケージです。

仮想アプリケーションパッケージ (VAP)

1つ以上のソフトウェア配信パッケージにパッケージ化された仮想アプリケーションイメージを仮想アプリケーションパッケージといいます。これらのパッケージは、仮想アプリケーションを使用してコンピュータをプロビジョニングするために使用されます。

仮想イメージ

仮想イメージとは、ハードウェアの仕様および仮想ディスクなど、仮想マシンのすべての定義を含むファイルまたはセットです。ゲストのホスト ファイル システムを表わします。仮想イメージをキャプチャする仮想マシンの稼働状態によって、仮想イメージはオンラインまたはオフラインの場合があります。

仮想ディスク

仮想ディスクとは、ファイル システムを形成するファイルのセットです。このファイルセットは、ゲスト オペレーティング システムに対して物理ディスクとして表示されます。

仮想パッチ

仮想パッチとは、通常パッチの仮想版で、基本的に同じ意味を持ちます。この用語は、仮想アプリケーション（仮想アプリケーション イメージを除く）のソフトウェア インベントリをレポートする場合に使用されます。

仮想マシン (VM)

仮想マシンとは、物理マシンをシミュレートする孤立した仮想環境です。定義上、仮想マシンにゲスト オペレーティング システムは含まれません。

仮想リリース

仮想リリースとは、通常リリースの仮想版で、基本的に同じ意味を持ちます。この用語は、仮想アプリケーション（仮想アプリケーション イメージを除く）のソフトウェア インベントリをレポートする場合に使用されます。プロビジョニング済み仮想アプリケーションは、ステージ済み仮想アプリケーションまたはストリーム配信仮想アプリケーションをソースとして使用できることに注意してください。仮想アプリケーション イメージ内に含まれる仮想アプリケーションは、ステージングされているが、プロビジョニングされていないとみなされます。

ゲスト

一般的なプラットフォーム仮想化用語での **ゲスト**とは、仮想マシンおよびゲスト オペレーティング システムです。

ゲスト オペレーティング システム

ゲスト オペレーティング システムとは、仮想マシンの内部で動作しているオペレーティング システムです。

ゴールデン テンプレート

Client Automation の用語では、**ゴールデン テンプレート**は、仮想デスクトップのクローン生成の元になる仮想マシンです。

コネクタ

コネクタは、コネクタ データを消費する製品から外部製品またはドメイン マネージャへのリンクです。各コネクタは、そのドメイン マネージャから情報を取得し、その情報を視覚化や分析のためにコネクタ フレームワーク経由で消費している製品に送信します。コネクタはまた、ソース ドメイン マネージャ内のデータに対する受信操作（オブジェクト作成など）を実行することもできます。コネクタは、統合されたコネクタ フレームワークを使用して、消費している複数の製品との統合を可能にします。

サンドボックス

サンドボックスとは、アプリケーションのランタイム環境です。この環境では、アプリケーションをコンピュータのオペレーティング システムおよびリソースから、またコンピュータ上のその他のアプリケーションから分離します。分離の程度は、通常、アプリケーションにドキュメント フォルダのようなオペレーティング システム リソースへのアクセスを許可するように設定されています。

集中管理環境

集中管理環境では、Remote Control ドメイン マネージャが、コンピュータ ポリシー、グローバル アドレス帳 (GAB) 項目、ドメインのホスト エージェントのライセンス、およびユーザ権限を使用してホスト設定を制御します。この環境は、CA Client Automation のデフォルト設定となります。

集中管理ホスト環境

集中管理ホスト環境では、Remote Control のエンタープライズ マネージャまたはドメイン マネージャのいずれかが、ホストの設定およびビューア接続の認証の役割を担います。集中管理ホスト環境では、ユーザがホストの検索に使用するアドレス帳も管理します。

スキーマ マップ

スキーマ マップとは、外部ディレクトリにおいて使用されるユーザ、コンピュータ、グループなどのデータ オブジェクトに関連した属性名と、対応する Client Automation オブジェクトによって使用される属性名とのマッピングのことです。固定された標準的な DSM 属性名は、ディレクトリのクエリ、および複雑なクエリとレポートの構成に使用します。

スケーラビリティ サーバ

スケーラビリティ サーバは、種々の管理タスクに関して 地理的なスケーラビリティを実現可能な中央のサーバです。これはエージェントのプライマリ インターフェースである配信処理です。

スタンドアロン仮想アプリケーション

スタンドアロン仮想アプリケーションとは、プロビジョニングされたシステムに存在する仮想アプリケーション イメージをソースとして使用し、プロビジョニングされた仮想アプリケーションです。

スタンドアロン環境

スタンドアロン環境では、ホストおよびビューア コンピュータのユーザが、すべての設定、プロパティ、および Client Automation Remote Control コンポーネントのライセンスをローカルで管理します。これはスタンドアロン エージェント インストールによって設定されます。スタンドアロン エージェントを手動でインストールするには、RC エージェント セットアップを直接呼び出す必要があります。

ステージ済み仮想アプリケーション イメージ

ステージ済み仮想アプリケーション イメージとは、コンピュータのファイル システムで検出された仮想アプリケーション イメージです。

ストリーム配信仮想アプリケーション

ストリーム配信仮想アプリケーションとは、プロビジョニングされたシステムとは異なるリモートシステムに存在する仮想アプリケーションイメージをソースとして使用し、プロビジョニングされた仮想アプリケーションです。

ストリーム配信仮想アプリケーションイメージ

ストリーム配信仮想アプリケーションイメージとは、コンピュータからネットワーク経由でアクセス可能であることが検出された仮想アプリケーションイメージです。ストリーム配信仮想アプリケーションイメージの検出は、通常、イメージ内に存在する仮想アプリケーションがプロビジョニングされた場合のみ実行可能です。

設定ビュー

設定ビューは、特定のコンポーネントまたは機能に関連する設定ポリシーを編集できる、カスタマイズされた **Windows** のみのユーザインターフェースです。設定ビューは、これらのビューが階層および **DSM** エクスプローラ ツリーに実際に存在する場所から独立したコンポーネントまたは機能に関連するポリシーの概要を表示します。

ソフトウェア シグネチャ

ソフトウェア シグネチャでは、メイン実行可能ファイル名、その他の関連付けられたファイル、サイズ範囲、バージョン範囲、ソフトウェアの作成日、修正日などのソフトウェアの属性が定義されます。ソフトウェア シグネチャのこれらのすべての属性では、ソフトウェア アプリケーションが一意に識別されます。アセット管理のソフトウェア シグネチャは、ソフトウェア 定義として作成されます。製品、リリース、パッチ、スイート、またはスイート コンポーネント、仮想アプリケーションイメージに対してソフトウェア 定義を作成できます。デフォルトで、アセット管理では、IT 業界で広く使用されるソフトウェアを網羅する事前定義されたソフトウェア シグネチャを提供しています。

ソフトウェア タイプ

ソフトウェア タイプとは、ソフトウェア 定義のプロパティです。現在のタイプには、スイート、製品、リリース、パッチおよび仮想アプリケーションイメージが含まれます。

デスクトップ更新

デスクトップ更新は、仮想デスクトップを元の状態にリセットするプロセスです。リンク クローンは、そのクローンを含む仮想マシンへの変更を追跡します。クローンへのストレージ割り当てを制御するために、**VMware View** は、クローンをそのベースラインにリセットし、変更を追跡するために提供されるすべてのデルタを解放するための更新操作を提供します。つまり、クローンの作成や、その最後の更新または再構成の後にシステム ドライブに格納されたすべての情報が失われます。デスクトップ再構成とは異なり、更新操作の前と同じゴールデンテンプレートが引き続き使用されます。

デスクトップ再構成

デスクトップ再構成は、仮想デスクトップに新しいゴールデン テンプレートを割り当てるプロセスです。ホット フィックスやサービス パックによって解決される問題を修正するために、または新しいバージョンによる新機能を提供するために、オペレーティング システムやアプリケーションをその存続時間を通して維持する必要があります。リンク クローンの場合、これはマスタ イメージ（ゴールデンテンプレート）を更新する必要があることを示します。更新が完了すると、リンク クローンが再構成され、アクティブになります。再構成操作中、関連するリンク クローンはこの新しいゴールデンテンプレートにリンクされ、更新されません。

ネイティブ型仮想環境

ネイティブ型仮想環境とは、物理マシン上で直接実行する仮想化ソフトウェアです。ホスト オペレーティング システム（多くの場合最小）、つまり物理マシンおよびハイパーバイザとして動作します。同義語は「ベア メタル環境」です。

パーティション

パーティションとは、ホスト オペレーティング システムの分離されたインスタンスです。ホストのオペレーティング システムを共有するので、パーティションでは通常ゲスト オペレーティング システムを使用しません。

パーティション型仮想環境

パーティション型仮想環境とは、ホスト オペレーティング システムの複数のインスタンスを同じマシン上で分離して実行できる環境です。これは厳密には仮想化技術ではありませんが、同じタイプの問題を解決するために使用されます。

ハイパーバイザ

ハイパーバイザとは、ゲスト オペレーティング システムの代わりに物理ハードウェアをシミュレートする仮想化ソフトウェア レイヤです。この用語は 仮想マシンモニタ（VMM）と同義語です。

場所認識

場所認識では、コンピュータ上の DSM エージェントにコンピュータの場所を検出させます。

パッケージ形式

パッケージ形式とは、ソフトウェア パッケージのプロパティです。形式には、非仮想および仮想が含まれます。

パッケージ タイプ

パッケージタイプとは、ソフトウェア パッケージのプロパティです。現在のタイプには、一般、MSI、SXP、PIF および PKG が含まれます。パッケージタイプは使用されていないか、仮想アプリケーション パッケージをサポートするために変更されました。

非永続クローン

非永続クローンは、標準装備で一時的な、VMware View ユーザ データの非永続プールからの仮想デスクトップです。ユーザがログオフすると、クローンは更新され、システム ディスクにあるすべてのユーザ データが失われます。

非永続リンク クローン仮想デスクトップ

非永続リンク クローン仮想デスクトップは、ユーザがログオンするたびに更新または再構成される仮想マシンであり、カスタムのインストール済みアプリケーション、パーソナル化などの永続性はありません。

非仮想アプリケーション

非仮想アプリケーションとは、仮想化されていないアプリケーションです。従来の方法でアプリケーションをインストールしたり、実行できます。リリース、パッチおよびスイートについて説明する場合、非仮想アプリケーションであることを意味します。

非リンク クローン

VMware View では、非リンク クローン (フル クローン) は、マスタまたはゴールデンイメージのフル コピーです。クローンにはイメージのコピーが含まれ、ユーザ セッション中のシステムへのすべての変更がこのコピーに格納されます。

複製

複製は、ドメイン マネージャからエンタープライズ マネージャ、エンタープライズ マネージャからドメイン マネージャにデータ複製を実行するエンジン タスクです。

プラットフォーム仮想化

プラットフォーム仮想化とは、コンピュータまたはオペレーティング システムをカプセル化することです。これらの物理的特性をユーザから見えなくし、実行時にコンピュータ プラットフォームをエミュレートします。

プロビジョニング済みアプリケーション

プロビジョニング済みアプリケーションとは、ターゲット コンピュータ上で実行可能になったアプリケーション (非仮想または仮想) です。プロビジョニング済みとして扱うには、アプリケーションをローカルにインストールする必要はありません。

ヘルス監視

ヘルス監視 (HM) 機能では、アラートを設定し、しきい値を設定して、Client Automation インフラストラクチャの全体的な健全性をモニタできます。

ホスト

一般的なプラットフォーム仮想化用語でのホストとは、物理マシン、ホスト オペレーティング システムおよびハイパーバイザです。

ホストオペレーティングシステム

ホストオペレーティングシステムとは、物理マシン上で動作しているオペレーティングシステムです。

ホスト型仮想環境

ホスト型仮想環境とは、ホストオペレーティングシステム上、つまり、物理マシン、ホストOSおよびハイパーバイザで実行する仮想化ソフトウェアです。

ホストクラスタ

ホストクラスタとは、集約型コンピューティング、および同じネットワークやストレージの一部またはすべてを共有するホストグループのメモリリソースです。

マスタ vDisk

Citrix XenDesktop では、マスタ vDisk は、ゴールデンテンプレートマシンから生成される初期の vDisk です。

マスタターゲットデバイス

Citrix XenDesktop では、マスタターゲットデバイスは、vDisk を生成する元になる OS と必要なアプリケーションセットを含むベースデスクトップです。

リンククローン

VMware View では、マスタまたはゴールデンイメージのリンククローンはマスタまたはゴールデンイメージを参照するだけであり、それを含みません。ユーザーセッション中のシステムへの変更はマスタイメージには格納されず、クローンと共にデルタファイル内に保持されます。

連邦情報処理規格 (FIPS)

連邦情報処理規格 (FIPS) とは、NIST によって発行および承認が行われるセキュリティ規格です。機密性が高いが、アクセスが制限されていない情報を保護するセキュリティシステム内で使用する暗号モジュールが遵守する必要があるセキュリティ要件が規定されています。