

CA Client Automation

Asset Management 管理者ガイド

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 Asset Management へようこそ 15

概要および機能.....	16
Asset Management を使用する利点.....	20

第 2 章： アーキテクチャ 21

エンタープライズ マネージャ	22
エンタープライズ マネージャ コンポーネント	23
エンタープライズ DSM エクスプローラからのアクセス.....	24
エンタープライズ エンジン	24
ドメイン マネージャ	25
ドメイン マネージャ コンポーネント	26
BDSM -- ストレージエリア	27
エンジン.....	27
スケーラビリティ サーバ.....	28
エージェント.....	29
エージェントのタイプ.....	29
Asset Management エージェントの起動方法.....	31
ユーザ作業ディレクトリ	32
DSM エクスプローラ	33
DSM エクスプローラの Asset Management オブジェクト	34
Asset Management セキュリティ オブジェクト クラス	35
Common Application Framework (CAF).....	37
CA メッセージ キューイング (CAM)	37
Comstore.xml	38

第 3 章： 実装 39

サーバの選択.....	39
選択基準.....	40
ネットワーク パフォーマンスへの影響.....	40
エンジン.....	40
エージェント.....	40

ストレージエリア	41
インストール前の実際的な注意事項	43
インストールの計画	43
最良のメイン サイトの選択	43
スケーラビリティ サーバの数	44
シナリオ	45

第 4 章 : Asset Management の設定 47

アセットのグループ化	48
ユーザ指定スキャン	48
インストール後のユーザ指定スキャンの設定	49

第 5 章 : カスタム ソフトウェア シグネチャの作成方法 51

シグネチャのタイプについて	52
製品の作成	54
スイート、リリース、またはパッチの作成	55
分類によるソフトウェア定義の整理	59
カスタム シグネチャ定義の確認	61
ソフトウェア シグネチャ XML リファレンス情報	62
Intellisig	77
Intellisig -- スクリプトによるソフトウェア検出	77
Intellisig -- 概要	78
Intellisig とは	79
Intellisig を使用したソフトウェアの検出	80
マネージャ間での Intellisig の移動	85
カスタム Intellisig の作成	89
カスタム Intellisig の変更	121
Intellisig データと別の CA 製品との調整	124
Intellisig の複製	125
DMScript の拡張	129
Intellisig に対する追加情報	135
仮想アプリケーション イメージ	141
VMware ThinApp を使用したアプリケーションの配信	143
検出方法	143
コンテンツ ユーティリティ	148
コンテンツ ユーティリティの実行	148
コンテンツ ユーティリティの設定	149

コンテンツ ユーティリティ ログ ファイル	151
収集モジュール	152
インベントリ 検出 モジュール	152
インベントリ テンプレート モジュール	155
デバイス コンプライアンス スキャナ (DCS)	165
ファイル収集	183
DSM エクスプローラの [ファイル収集] フォルダへのアクセス	184
バックアップ用に設定されたファイルの表示	185
バックアップ用ファイルの設定	185
新しいファイル収集定義の追加	186
ファイル収集定義の変更	186
設定ファイルのバックアップ バージョンおよびプッシュバックの表示	187
設定ファイルのバックアップが管理される方法	187
イベント ポリシーの定義	188
収集タスク	189
DSM エクスプローラの [収集タスク] フォルダへのアクセス	190
エンジン収集タスク	192
ハードウェア インベントリ	193
ソフトウェアの検出	203
ファイルのスキャン	212
テンプレート インベントリ	217
ソフトウェア使用状況	219
仮想ホストインベントリ	234
既存の収集タスクのリンク	243
アセットから収集タスクのリンクを解除	244
収集タスクのステータスの確認	244
収集タスクの無効化	245
収集タスクの削除	246
コンテンツ配信を制御する収集タスクの設定	246
プラットフォーム仮想化	248
グリーン IT レメディエーション	265
GreenIT レメディエーションの実装	265

第 6 章 : Asset Management のカスタマイズ 273

管理情報フォーマット (.MIF) ファイル	274
Asset Management での MIF ファイルの使用方法	274
ジョブ	278
アセット ジョブ	279
ジョブのスケジューリング	288

ジョブの再初期化.....	289
ジョブ ステータスの表示.....	290
ジョブの有効化または無効化.....	290
クエリ.....	291
新規クエリの作成.....	292
クエリ デザイナ.....	293
クエリの実行.....	295
クエリ プレビュー.....	296
クエリ結果の保存.....	296
クエリの削除.....	297
クエリ定義のインポートまたはエクスポート.....	297
ポリシー.....	298
ポリシー定義.....	298
ポリシーへのアクションの追加.....	301
ポリシー評価.....	305
事前定義ポリシー.....	305
ポリシーの重要度.....	307
イベント ログ.....	308
例：重複するネットワーク アドレスの処理.....	308
例：エージェント コンピュータへのアプリケーションのインストールおよびアンインストールの追跡.....	311
CA Service Desk Manager を使用した統合.....	312
重複チケット ポリシー.....	319
ポリシーの有効化または無効化.....	320
ポリシーの削除.....	320
Asset Collector.....	321
前提条件.....	322
Asset Collector の動作の仕組み.....	323
インベントリ ファイルの種類.....	324
差分操作.....	325
発行元と信頼レベル.....	326
発行元と信頼レベルのスキーマの変更.....	327
調整.....	328
ホスト キー.....	328
ユーザ URI.....	329
Asset Collector の設定.....	329
テナンシー収集.....	334
セキュリティ.....	350
発行元および信頼レベルを表示する.....	357
インベントリ ファイルの作成.....	362

制限事項.....	377
Client Automation に CA Mobile Device Management を統合する方法.....	377
CA Mobile Device Management アセット情報用の CA Client Automation 統合	377
MDM 用の Client Automation 統合の設定	387
既知の問題およびトラブルシューティング	392
エージェントブリッジ.....	393
エージェントブリッジの UUID 生成.....	394
制限事項.....	394
既知の問題.....	395
エージェント登録.....	396
移行に関する注意事項.....	398
AM エージェントブリッジ	398
SD エージェントブリッジ.....	402
Intel AMT と CA ITCM を統合する	403
Intel AMT アセットの設定	403
Intel AMT のステータス	406
Intel AMT アセットのステータスを表示する	407
Intel AMT アセットを参照する	408
Intel AMT アセットを隔離する	410
AMT コマンドポリシー アクションを使用する.....	411
仮想ホスト.....	412
サポートされている仮想化サーバプラットフォーム	412
CA Web サイトのコンテンツの更新	413
Solaris SPARC.....	414
HP-UX	422
AIX	430
VMware ESX.....	437
仮想ホスト インベントリの表示.....	441
Windows リモート エージェント ホスト上での Plink の設定.....	444
非常駐インベントリ	446
要件	447
NRI 選択的インベントリの起動	448
NRI Web サービスの設定.....	456
NRI エージェント	460
NRI プライマ	466
NRI エージェント用の追加インベントリ モジュールの設定.....	470
DSM レポータ	487
機能	488
DSM レポータの開始	489
Reporter 環境設定の指定	490

Reporter の操作	491
CA Asset Converter for Microsoft SCCM	496
CA Asset Converter for Microsoft SCCM エンジン タスクを作成する	498
タスク プロパティ	499

第 7 章：システム エンジンの使用 509

エンジン インスタンスの作成	511
エンジンの設定	512
エンジン ログ	513
エンジンの停止および起動	514
ジョブのパフォーマンス	514
定義済みエンジン タスク	515
エンジン タスク	516
複製ジョブ	518

第 8 章：診断およびトラブルシューティング 519

ログ ファイル収集ツール dsminfo	519
レポートされたエラーのトラブルシューティング	520
MDB がダウンすると AM マネージャがクラッシュ	520
Asset Collector によって作成される重複エントリ	521
ログインに記録されたエラー イベント	521
Citrix XenServer 仮想マシンでインベントリ属性ホスト名に正しくない値が示される	522
Microsoft Hyper-V クローン用の新しいホスト UUID が存在しない	522
Asset Management が Citrix XenServer の VM 上でインベントリ データを収集しない	523
DSM エクスプローラで vDisk レコードが見つからない	523
プロセッサ スロットルが Client Automation に別の値を表示する	524
Citrix XenServer ゲスト仮想マシンが仮想インベントリに表示されない	524
アセットが新しいテナントに移動するとき、テナント ID が更新されない	524
コンテンツ ダウンロードが失敗する	525
アンインストール ジョブの後のソフトウェア ジョブ履歴動作	526
CAM サーバ間の不安定な通信	527
ファイル転送のタイムアウト	529
Asset Management エージェントを Windows XP SP2 コンピュータに展開できない	530
再作成されたグループに対する既存のクエリが失敗する	531
ソフトウェア コンテンツのダウンロード ジョブが失敗する	531
プロキシ サーバの詳細の欠落	532
evmUpdate1_0 を実行しようとしたときに不明なエラーが発生しました。 .RC : -6	532

Unicenter Patch Management インストール	533
VM ホストまたはシステム コントローラが DSM Explorer に表示されない	533
関連するコンピュータが仮想ホストに表示されない	533
検出されたソフトウェアの欠落	534
Dual-Core HP-UX コンピュータで報告されたプロセッサの数	534
SUN E4800/4900/6800/6900 システム コントローラで報告されたプロセッサの数	534
インストールされている amVMAgent と、表示されている amVMAgent のバージョンが異なります。	535
[概要] ページにプラットフォームが「未分類」と表示される	535
仮想ホストとそのゲストの関係が表示されない	536
インベントリ ファイルにエラー タグが表示される	536
ロード配信	536
エラーの検出	537
Asset Collector が処理できるインベントリ ファイル数の制限	537
[信頼レベル] フィールドと [発行元] フィールドが DSM エクスプローラで表示されない	538
DSM エクスプローラの [信頼レベル] フィールドと [発行元] フィールドが、他のドメインに接 続しているときに表示されない	538
バックアップ	539
フロッピー ドライブからのアセット収集	539
ネットワーク ドライブからの収集	540
未処理ファイル	541
アプリケーション イベント ログの大量のエラー	542
SCCM Converter エンジン タスク エラー	542
インベントリ情報が見つからない	543
どうすればエージェントブリッジが稼動中であることがわかりますか?	543
自分のレガシー エージェントを登録できない	544
自分の PDA で USD エージェントが UAM エージェントに上書きされる	544
なぜエージェント名が重複するのですか?	545
エージェントブリッジログ ファイルはどのようにすれば表示できますか?	546
ログ ファイルが見つからない	546
ハードウェア モジュール 1 つだけが実行される	547
Solaris の非大域ゾーン、リソース プール、およびプロセッサセットのインベントリが見つからな い	547
Intellisig におけるスクリプト コンパイル エラー	548
収集タスクの実行が成功した場合でも、Intellisig の実行に失敗する	548
Intellisig の実行の確認	549
ターゲット コンピュータ上での Intellisig 実行のタイムアウト	550
エージェント上で実行する Intellisig スクリプトの確認	551
ドメイン マネージャによる Intellisig 定義のエクスポートの確認	552
エンジンによって管理されるポリシー パラメータを変更しても、その動作が変化しない	553

複製された Intellisig が、手動による削除の後に複製されない	554

付録 A: 管理情報フォーマット (.MIF) ファイルのリファレンス 555

語の規則.....	556
コメント.....	556
キーワード.....	556
データ タイプ	557
カウンタ.....	557
ゲージ.....	557
文字列.....	558
日付	558
定数	558
リテラル.....	559
ブロック スコープ.....	560
language 文	562
一般の文.....	563
name 文	563
description 文	563
ID ステートメント	564
コンポーネント定義.....	564
パス定義.....	565
列挙定義.....	566
グループ定義.....	567
class 文	569
key 文	570
属性定義.....	571
type 文	572
access 文	572
storage 文	573
value 文	574
テーブルの作成.....	576
ComponentID グループ	577
.MIF ファイルの例.....	579
Asset Management 圧縮テキスト ファイル.....	582

付録 B: インベントリ マトリックス 583

レポートされるインベントリ項目のリスト	583

付録 C: インベントリ ファイル プロパティ 607

Status (グループ)	607
Status/Input Files (テーブル)	608
Status/Output Files (テーブル)	608
General (グループ)	609
General Identity (オプション グループ)	609
Target (グループ)	610
Target/Facts (オプション テーブル)	610
Set Values (テーブル)	611
Rule Results/<rule id> (グループ)	611
Rule Results/<rule id>/Idents (オプション テーブル)	612
Scores (テーブル)	612

付録 D: プラットフォーム名および ID 613

付録 E: SCAP 設定パラメータ 645

付録 F: CA Asset Converter for Microsoft SCCM Inventory Mapping 649

Client Automation Asset Management ハードウェア インベントリへの Microsoft SCCM ハードウェア アセット インベントリのマップ	649
Client Automation Asset Management ソフトウェア インベントリへの Microsoft SCCM ソフトウェア アセット インベントリのマップ	654

付録 G: SCAP 標準の実装 655

SCAP	655
CVE	656
CCE	657
CPE	658
CVSS.....	658
XCCDF	659
OVAL.....	659

用語集 661

第 1 章 : Client Automation Asset Management へようこそ

CA Client Automation は、特に異機種混在環境を管理するよう設計されている高度な IT アセット管理を実現します。この製品を使用すると、IT 部門では、ハードウェアおよびソフトウェアのアセットの設定に標準およびポリシーを適用することによって、サービス コストを削減できます。

このマニュアルでは、管理者が以下のタスクを実行するための技術的なサポートについて説明します。

- アセット管理固有の設定の共通の設定ポリシーの設定
- ソフトウェア シグネチャの作成、ソフトウェア シグネチャのエクスポート、およびソフトウェア シグネチャのインポート
- ジョブのスケジュール作成およびタスクの収集
- クエリの作成
- ポリシーの定義
- 収集モジュールの作成および設定
- 収集用ファイルの設定
- さまざまなソースからインベントリ データを収集するための Asset Collector、エージェントブリッジ、および Asset Converter の設定
- Intel AMT と Client Automation との統合
- 仮想ホスト上でインベントリを実行し、インベントリ情報を収集します（仮想ホストインベントリ収集タスクがその仮想ホストに対して設定され、有効である場合）。

概要および機能

アセット管理では、以下のシステム管理機能を提供しており、これは非常に複雑な IT 環境でのアセット管理で役立ちます。強固な管理データベース (MDB) では、エージェントを確認し、組み込み展開ウィザードを使用してネットワーク環境のすべての IT アセットに展開できます。

エージェントが展開されると、コンピュータ アセットで以下のタスクを実行できます。

ハードウェア インベントリ

シリアル番号、CPU 情報、RAM、内部ディスク ドライブおよび周辺ディスク ドライブ、OS バージョンおよびサービス パック、ネットワーク設定、電源設定などの詳細なインベントリ情報を検出およびレポートします。

ハードウェア インベントリは、エージェントに設定されたインベントリ検出モジュールに基づいて収集されます。

これらのモジュールを使用すると、以下の操作を実行できます。

- デフォルトでシステム管理 BIOS (SMBIOS) インベントリを収集します。
- アセットに関する特定のハードウェアおよびネットワーク情報を検出するための新しいモジュールを作成およびカスタマイズします。
- FDCC チェックリストに準拠していることを確認するためにターゲットコンピュータをスキャンします。
- インベントリおよび設定情報を収集するための Windows Management Instrumentation (WMI) 標準をサポートします。
- アセットへの変更を追跡し、変更の日時および過去と現在の値を含む履歴を保持します。

ソフトウェア インベントリ

管理対象アセットにインストールされているソフトウェア アプリケーション（非仮想または仮想）を検出し、詳細で正確な情報をレポートします。アセット管理では、以下の方法のうちの 1 つを使用してソフトウェア インベントリを収集できます。

ソフトウェア シグネチャ

シグネチャ データベースを使用して、エージェント コンピュータをスキャンします。アセット管理に付属している、事前定義済みシグネチャがあるシグネチャ データベースでは、インストール直後から、インストールされているアプリケーションとその場所の概要が（IT 管理者に）迅速に表示されます。また、業務特有のソフトウェアのソフトウェア シグネチャを作成したり、新規および更新されたシグネチャをインターネットで CA が一括管理しているデータベースからダウンロードすることもできます。デフォルトでは、これらの更新されたシグネチャは、デフォルト ソフトウェア コンテンツ ダウンロード ジョブによって 1 日に 1 回自動的にダウンロードされます。

Intellisig

Intellisig は、エージェント コンピュータにインストールされたソフトウェアを検出するスクリプトです。Intellisig は、ヒューリスティック スキャンおよびソフトウェア シグネチャ スキャンと比較して、ソフトウェアを検出する最も柔軟で正確な方法を提供します。Intellisig は、ソフトウェア メーカーが提供する定義済みソースからソフトウェア定義情報を抽出します。そのソースとして、テキスト ファイル、データベース、レジストリ、またはバイナリ ファイルを使用できます。たとえば、`dsmver -f<output file>` は、CA ITCM に関するバージョン情報を出力するコマンドです。製造元が、バージョン情報を製品に格納する方法を変更しない場合、Intellisig は、製品の今後のバージョンも検出できます。

ヒューリスティック スキャン

Windows の [プログラムの追加と削除] データベース、MSI データベース、デスクトップのショートカットおよびスタート メニューをスキャンして、インストール済みアプリケーションを検出します。Linux/UNIX エージェントでは、ヒューリスティック スキャンは PIF、PKG、および RPM データベース上で実行されます。

ユーザ指定スキャン

シグネチャ スキャンおよびアセット管理エージェントのプロセス優先度を指定します。これは、シグネチャ スキャン中のハード ドライブの負荷を最小化するのに役立ちます。

注：ユーザ指定スキャンは、Linux または UNIX システムでのみ設定できます。Windows エージェントでは、デフォルトでユーザ指定スキャンは最適化されており、実行速度は最大、および CPU 時間は最小となるため影響は最小限となります。

ソフトウェア使用状況の監視

ソフトウェア使用状況の監視では、特定のアプリケーションの使用状況を制御できます。ソフトウェア使用状況エージェントでは、以下のことが可能になります。

- 使用パターンを監視して未使用のソフトウェアの再割り当てを行い、ライセンスを必要としているユーザは新しいライセンスを購入する必要がなくなります。
- アプリケーションをスイートに分類して正確なライセンス追跡を可能にします。
- 使用状況情報をローカルに記録して、アセットがオフラインの場合にもアプリケーションを管理します。
- ライセンス数が指定されているライセンス数を超えた場合に、アプリケーションへのユーザ アクセスを抑制します。
- ライセンスの数が超過した場合は、ユーザをキューに入れ、ユーザがアプリケーションを閉じたときにアクセスを許可します。

ネットワーク インベントリ

一般インベントリ モジュールでも、管理対象アセットの TCP/IPv4、TCP/IPv6、WINS、および DNS 設定などのネットワーク設定がスキャンされます。

注：IPv6 インベントリには、Windows XP および Windows 2003 Server でのゲートウェイに関する情報は含まれていません。Windows Vista 以降の Windows のバージョンでのゲートウェイ情報のみが含まれます。

クエリ

必要とする特定の情報を取得するためにデータベースをクエリできます。ジョブまたは収集タスク ステータスのクエリ、およびインベントリまたはアセットの検索ができます。また、クエリに基づいたポリシーを作成できます。

ポリシーベースの管理

アセット管理は、特定のポリシーを適用して接続されたアセットを管理します。これらのポリシーを使用すると、特定のしきい値が超過した場合に重要なデータに焦点を当てることができます。ポリシーに違反があったか、またはイベントが発生した場合は、クエリベースおよびイベントベースのポリシーを作成して、実行する必要があるアクションを指定できます。事前定義されたイベントベースのポリシーも利用できます。

レガシー エージェント サポート

AM エージェント ブリッジは、Unicenter Asset Management 4.0 のすべてのレガシー エージェントをサポートします。

Asset Collector

Asset Collector は、適切に構成されたインベントリ ファイルから、ハードウェアおよびソフトウェアのインベントリ情報を収集します。このインベントリの発行元と信頼性をトラッキングすることもできます。Asset Collector を使用して、CA Client Automation、メインフレーム コンピュータなどで現在サポートされていない特殊なデバイスのように様々なソースのインベントリ情報を作成できます。

CA Asset Converter for Microsoft SCCM

CA Asset Converter for Microsoft® SCCM は、Microsoft System Center Configuration Manager (SCCM) に接続し、ハードウェア インベントリやソフトウェア インベントリなどのデータベースに格納されているコンピュータの情報を抽出するコンポーネントです。

仮想ホストインベントリ

仮想ホスト インベントリ機能では、リモート マシン上の Client Automation エージェントから仮想ホスト上のインベントリ データを収集し、レポートします。

非常駐インベントリ

非常駐インベントリ (NRI) ソリューションは、システムのインベントリ (一覧) 作成を、Client Automation エージェントを配備することなく簡単に行う方法を提供します。

強力なレポート

アセット管理では、さまざまなアセット関連のレポートを作成するために **DSM** レポーターを使用します。これらのレポートは、管理決定を行う場合に役立ちます。クエリ デザイナを使用すると、データを評価し、レポートで表示するフィールドを指定できます。これらのレポートは印刷したり、**CSV** ファイルや **HTML** ファイルなどの別のアプリケーションにエクスポートできます。

レポートは手動でいつでも生成できます。また、**DSM** レポーター **GUI** を使用して、特定の時間に生成されるようにスケジュールすることもできます。システム エンジンでは、スケジュールされたレポートが指定した時間に生成されます。

Asset Management を使用する利点

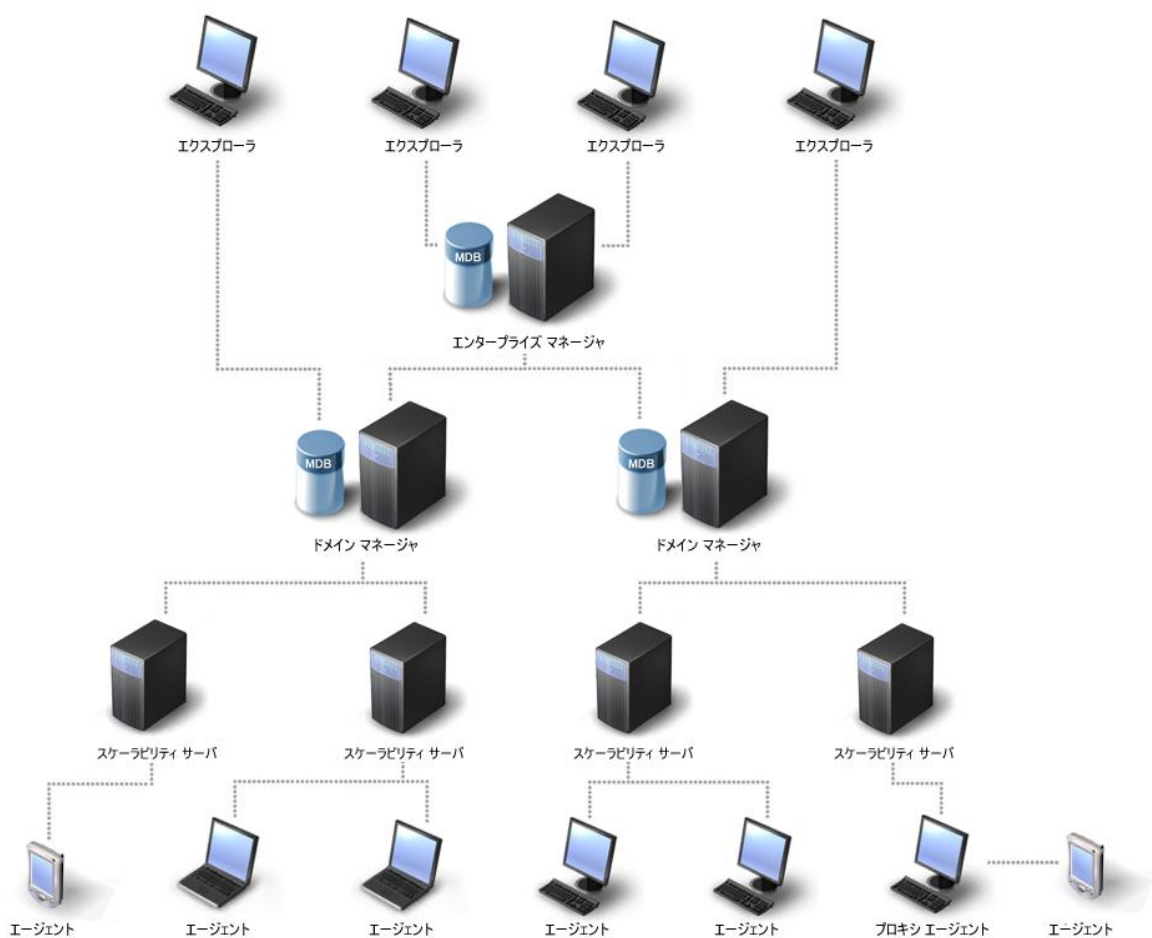
アセット管理では、さまざまな管理ツールが提供されています。これらの管理ツールを使用すると、さまざまな方法でシステム管理機能の監視、自動化、およびメンテナンスを行い、コストを削減できます。また、これらのツールでは配置されたアセットの情報を即時的に取得することができ、また自動ディスカバリ、ハードウェアやソフトウェアのインベントリ、環境設定管理、ソフトウェアの使用状況の監視、ソフトウェア ライセンス管理、および詳細なクロスプラットフォーム レポートにより広範なアセット トラッキング機能が提供されます。

第 2 章：アーキテクチャ

本章では、各種コンポーネントおよび一部の機能の簡単な説明など、アセット管理のアーキテクチャの概要について説明します。

以下の図に、DSM のアーキテクチャを示します。

DSM アーキテクチャ



Client Automation のスケーラブルな多層アーキテクチャは、大小にかかわらずあらゆる規模の組織に適応できます。すべてのアセット情報がドメイン マネージャごとに管理されるため、このアーキテクチャは強固です。アセット情報がエンタープライズ マネージャに複製された場合、標準の複製ルールに従って、エンタープライズ マネージャからアセットを管理することもできます。

このセクションには、以下のトピックが含まれています。

[エンタープライズ マネージャ](#) (P. 22)

[ドメイン マネージャ](#) (P. 25)

[エージェント](#) (P. 29)

[DSM エクスプローラ](#) (P. 33)

[Common Application Framework \(CAF\)](#) (P. 37)

[CA メッセージ キューイング \(CAM\)](#) (P. 37)

[Comstore.xml](#) (P. 38)

エンタープライズ マネージャ

エンタープライズ マネージャを使用すると、接続したすべてのドメインからのデータの同期化および絞り込みを行うことができます。分散インストールでは、エンタープライズ マネージャを使用して、本社で子会社の概要を保持できます。エンタープライズ マネージャは、以下のタスクの実行に役立ちます。

- エンタープライズ マネージャから複数のドメインおよびそのデータへのアクセス。たとえば、接続したすべてのドメインのインベントリ、ユーザ情報、ジョブ、およびアラーム定義にアクセスできます。
- 選択したドメイン、またはすべての接続済みドメインに対して適用される統合アクションの実行。たとえば、選択したドメインまたはすべてのドメインに適用するポリシーを設定できます。
- エンタープライズ マネージャに接続済みのドメイン マネージャからのデータを含むレポートの準備。

注：環境内で保持できるエンタープライズ マネージャは 1 つのみです。

エンタープライズ マネージャ コンポーネント

エンタープライズ マネージャには、アセット管理で使用するデータを管理、制御、収集、配布、処理、および保持するコンポーネントがあります。エンタープライズ マネージャの基本コンポーネントは、以下のとおりです。

エンタープライズ DSM エクスプローラ

リクエストやアクションのスケジュール、クエリの実行、およびポリシー確立のためのエンタープライズ管理インターフェースを提供します。

Enterprise DSM レポータ

複製されたデータまたはターゲットのドメインを使用してレポートを作成するレポート ツールを提供します。

エンタープライズ エンジン

コンテンツ ダウンロード ジョブを実行し、エンタープライズ レベルでのクエリベースのグループやポリシーを保持するエンタープライズ エンジンを含みます。

エンタープライズ データベース

エンジンによって接続済みドメインから収集され、エンタープライズ DSM エクスプローラで表示できるアセット（コンピュータおよびユーザ）に関する情報を格納するためのデータベースが含まれます。

エンタープライズ DSM エクスプローラからのアクセス

エンタープライズ エクスプローラから、すべてのドメイン マネージャにアクセスできます。

- 概要のウィンドウから、エンタープライズ マネージャおよびすべてのドメイン マネージャにアクセスできます。
- エンタープライズ エクスプローラでは、特定のドメイン マネージャで作業するためのウィンドウを開くことができます。ドメイン マネージャおよびエンタープライズ マネージャ間でオブジェクトをドラッグアンドドロップできます。
- エンタープライズ マネージャは、複数のドメイン マネージャと同時に開くことができます。DSM エクスプローラで特定のワーク セッション用に一度マネージャを開くと、再度開く必要はありません。
- [エンタープライズ エクスプローラのセットアップ] ウィンドウを使用すると、各ドメイン データベースおよびエンタープライズ マネージャへの接続方法を設定できます。

アセット管理に接続されているすべてのエージェントおよびユーザは、以下のいずれかの方法で制御されます。

- ドメイン DSM エクスプローラによる直接制御
- エンタープライズ DSM エクスプローラによる間接制御

エンタープライズ エンジン

エンタープライズ エンジンでは、以下の機能が実行されます。

- コンテンツ ダウンロード ジョブの実行
- エンタープライズ レベルでのクエリ ベースのグループまたはポリシーの保持
- DSM エクスプローラへのクエリ結果の送信
- レポート テンプレートのスケジューリング

注：エンジンは DSM エクスプローラと同じコンピュータで実行できます。ただし、複数のドメインで更新されたインベントリ データをクエリして処理する場合は、応答時間を短縮するためにエンジンを別のコンピュータで実行することをお勧めします。

ドメイン マネージャ

ドメイン マネージャは、ネットワークのサーバクラスのコンピュータで動作し、以下のタスクを実行します。

- ドメイン内の管理対象アセットの設定情報を保持します。
- ドメイン マネージャに接続できるアセット管理ユーザのセキュリティ、および各オブジェクトでの権限の範囲を設定します。
- スケーラビリティ サーバと通信して、アセットにスケジュールされたジョブをプッシュし、タスクを収集します。
- 各エージェント コンピュータから収集されたハードウェア インベントリおよびソフトウェア インベントリを保存します。
- ソフトウェア使用状況情報を保持します。
- エンジンをつリガしてスケーラビリティ サーバに格納されているデータを収集します。
- データベースにクエリし、ポリシーを適用します。
- 強力なレポート ツールを提供します。
- システムにエージェントをインストールしなくても簡単にシステムのインベントリを作成できます（非常駐インベントリ）。

ドメイン マネージャ コンポーネント

アセット管理ドメインは、ドメイン マネージャの情報を構成および管理するために使用される以下のコンポーネントで構成されています。

グループ

主に設定およびスケジューリング用に、集まりとして定義されているアセットを示します。管理対象アセットは、**1** つ以上のグループに属する場合があります。

動的グループ

ドメイン データベースのクエリを実行して、定義された条件を満たし、動的に検出されるアセットを含めます。クエリには、**DSM** エクスプローラから **1** つ以上の動的グループを直接定義できます。

スケーラビリティ セクタ

システム トランザクションのドメイン領域を表示します。各ネットワークのオペレーティング システム、プロトコル、トポロジ、またはセグメントにこのサーバを作成できます。

アセット

最小のコンポーネントを示します。**1** 台のコンピュータまたは **1** 名のユーザです。

BDSM -- ストレージ エリア

デフォルトで、アセット管理は 2 つのストレージエリアを使用してインベントリデータを保存します。これらのエリアはドメイン データベースおよびスケーラビリティ サーバです。

ドメイン データベース

アセット管理エージェントが収集したデータを保存します。エンジンがスケーラビリティ サーバからデータを取得し、ドメイン データベースを更新します。DSM エクスプローラでは、アセットのインベントリデータおよび設定データの格納と収集にドメイン データベースが使用されます。データベースは、ローカルまたはリモート システムに置くことができます。

スケーラビリティ サーバ

アセット管理エージェントが収集したデータを一時的にハード ドライブに保存します。これは、ドメイン データベースおよびエージェントにリンクした一時的なストレージエリアです。コンピュータやユーザにスケジュールされた管理トランザクションを格納するために使用されます。また、エージェントによって実行されたトランザクション結果のステータス データを保持するためにも使用されます。ネットワークの要件を満たすために、ネットワークのオペレーティング システム、転送プロトコル、または企業の地理的位置に基づいたスケーラビリティ サーバを持つことができます。

エンジン

ドメイン マネージャのエンジンでは、以下のタスクが実行されます。

- ドメイン マネージャのデータ処理タスクの実行。たとえば、エンジンでは、アクションのステータスでドメイン データベースを更新したり、ドメイン データベースにクエリを実行してデータを検出できます。
- ソフトウェア定義のコンテンツ ダウンロード ジョブの実行。
- エンジンがサービスを提供するドメインとエンタープライズの間でのオブジェクトの複製（プルおよびプッシュ）の実行。これは、ドメインがエンタープライズのメンバである場合に適用できます。

エンジンは CAF プラグインであり、起動時に自動的に起動されます。通常、エンジンは常に実行するようにスケジュールされています。

スケーラビリティ サーバ

スケーラビリティ サーバによって、エンド システム (エージェント) と マネージャ 間のバッファ ポイントおよび回復力が提供され、以下の機能が実行されます。

- ドメイン マネージャと通信して、管理対象アセットにスケジュールされたジョブおよびタスクを取得します。
- アセットにジョブおよびスケジューリング設定を提供します。
- エージェントから収集されたインベントリ情報を格納します。

管理するエージェントが多数あり、1つのマネージャには多すぎて処理できないことがあります。また、データベースにデータを格納するのにエージェントごとにデータベース クライアントが必要になるため、費用がかかる場合もあります。分散環境では、地理的に分散した大量のエージェントを処理するためにスケーラビリティ サーバが挿入されます。これにより、サーバが仲介の役割を果たしマネージャ間の情報を中継するため、マネージャ間のトラフィックによるネットワークのオーバーロードが回避されます。

スケーラビリティ サーバには、セクタと呼ばれるディレクトリおよびファイルの集まりがあり、エージェントのデータ ファイルはここに格納されます。エージェントがデータを収集する場合、データは、**DSM** エンジンによる処理のためにスケーラビリティ サーバに格納されます。エンジンがスケーラビリティ サーバから情報を収集し、ドメイン データベースを更新します。

分散環境では、地理的に分散した大量のエージェントを処理するためにスケーラビリティ サーバが挿入され、マネージャ間のトラフィックによるネットワークのオーバーロードが回避されます。

エージェント

エージェントは管理対象アセットに配置され、コンピュータまたはユーザにスケジュールされたタスクを実行します。エージェントでは、ハードウェアおよびソフトウェア インベントリ スキャン、ソフトウェア配信ジョブ、およびリモート コントロール アクティビティなど、数多くのタスクが実行されます。

エージェントでは、主に以下の機能が実行されます。

- スケーラビリティ サーバのジョブをチェックし、エージェントが常駐するコンピュータにスケジュールされたタスクを収集します。
- ジョブを実行し、タスクを収集します。
- 収集したデータをスケーラビリティ サーバの収集エリアに保存します。

製品のインストール ウィザード (DVD または共有から) の実行、または展開ウィザードによってエージェントを展開できます。エージェントはアセット管理システムで管理する必要があるコンピュータに展開する必要があります。展開ウィザードを使用すると、以下のいずれかの条件に基づいてエージェントを展開できます。

- ドメイン内のコンピュータ
- IP アドレス範囲内のコンピュータ
- 特定のコンピュータ
- LDAP ディレクトリ (アクティブ ディレクトリを含む) 内のコンピュータ

エージェントを展開すると、アセットが管理対象アセットのリストに表示されます。このリストのコンピュータは、アセットジョブおよび収集タスクを実行できます。収集された情報は、管理情報フォーマット (MIF) を使用して拡張できます。

エージェントのタイプ

アセット管理エージェントには、以下の 4 つのタイプがあります。

- Windows エージェント
- Linux エージェント
- Solaris、HP-UX、AIX、および MAC OS X エージェント
- Palm デバイスおよび Windows CE デバイス用 Docked Device プロキシエージェント

Windows Asset Management エージェント

Windows エージェントには、さまざまなオペレーティングシステムで実行されるコンピュータの制御プログラムが含まれます。サポートされるオペレーションシステムについては、[認定マトリックス](#)を参照してください。

注：制御プログラムは、管理対象アセットを起動するかまたはアセットへログオンするたびに起動します。

エージェントソフトウェアには、管理対象コンピュータでネットワーク オペレーティングシステムが起動されたときにシステム関連データを取得するために起動する部分、およびユーザがネットワークにログオンしたときにユーザ関連データを取得するために起動する部分の 2 つの部分があります。

注：サポート対象プラットフォームの最新のリストについては、「*CA Client Automation Readme*」を参照してください。

Linux/UNIX エージェント

Linux/UNIX エージェントには、**Linux** および **UNIX** オペレーティングシステムで実行するコンピュータ用の制御プログラムが含まれています。

注：制御プログラムは、管理対象アセットを起動するかまたはアセットへログオンするたびに起動します。

エージェントソフトウェアには、管理対象コンピュータでネットワーク オペレーティングシステムが起動されたときにシステム関連データを取得するために起動する部分、およびユーザがネットワークにログオンしたときにユーザ関連データを取得するために起動する部分の 2 つの部分があります。

Palm デバイスおよび Windows CE デバイス用 Docked Device プロキシ エージェント

CA ITCM アセット管理では、モバイル デバイスを使用して、インベントリの実行、ソフトウェアの配信、およびさまざまなタスクのスケジュールを行うことができます。これらのジョブは、モバイル デバイス ユーザが一時的にそのユーザのコンピュータに戻って、モバイル デバイスとコンピュータ間で情報を交換および同期化するときに実行されます。通常、モバイル デバイスは、コンピュータのシリアルポートに接続された「クレードル」を使用して接続します。

アセット管理エージェントソフトウェアによってサポートされているプラットフォームは、Windows CE オペレーティング システム上で稼働する Microsoft Windows CE/Pocket PC シリーズのデバイスです。

注： 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前に、Microsoft Activesync コンポーネントをインストールしておく必要があります。また、Microsoft Activesync コンポーネントでは、Client Automation のインストール時の PATH 環境変数の変更を認識しておく必要があります。Client Automation のインストール後、必要な環境変数を設定するには、いったんログオフして再度ログインする必要があります。Activesync および Palmsync の統合およびサポートされるバージョンの詳細については、「実装ガイド」を参照してください。

Asset Management エージェントの起動方法

アセット管理エージェントを起動すると、エージェント コンピュータに設定された収集タスクおよびアセット ジョブが実行されます。

以下のいずれかの方法で Asset Management エージェントを起動できます。

- 自動 - 簡易インストールでは、エージェントは 1 日に 1 回、午前 12 時に実行するように設定されます。カスタム インストールを実行して間隔またはエージェントを実行する特定の時間を指定すると、この間隔を変更できます。
- 手動 - 以下のいずれかの方法を使用します。
 - DSM エクスプローラでコンピュータ アセットを右クリックし、[アセット ジョブ] - [ジョブ確認のアクティブ化] を選択します。
 - 適切な権限がある場合は「caf start amagent」をローカル コンピュータで実行します。

注： Asset Management エージェントは、スケジュールした時間にスキャンを開始し、ローカル システム アカウント (Windows) または root (Linux/UNIX) を使用して情報を収集します。ユーザがログオンすると、エージェントはネットワーク接続、ユーザ テンプレート インベントリなどのユーザ関連のデータの収集を開始します。

ユーザ作業ディレクトリ

Windows コンピュータでは、エージェントの作業ディレクトリは以下のパスで使用できます。

- ...¥Agent¥units¥00000001 フォルダには、エージェントによってローカル システム アカウントを使用して収集されたデータが格納されています。
- ...¥Agent¥units¥00000003（およびすべての奇数増分）フォルダには、エージェントによってユーザのログインから収集されたデータが格納されています。アセット管理によって、コンピュータにユーザごとにフォルダが作成されます。
- ...¥Agent¥units¥00000002 およびすべての偶数番号のフォルダはソフトウェア配信によって使用されます

Linux および UNIX コンピュータでは、「/opt/CA/DSM/Agent/AM/data/transfer」フォルダにエージェントの作業ディレクトリがあります。ただし、インストールパスがカスタマイズされている場合があります。

DSM エクスプローラ

DSM エクスプローラは、オブジェクトを適切な分類にまとめ、ツリー構造で表示するアセット管理のグラフィカルユーザインターフェース (GUI) です。DSM エクスプローラから、以下のアクションを実行することができます。

- データベース内の情報の表示および管理
- データベースへのクエリ
- 以下のような、コンピュータ、ユーザ、コンピュータのグループまたはユーザのグループで実行されるジョブのスケジュールおよび表示
 - ハードウェアおよびソフトウェア インベントリ
 - ソフトウェア使用状況および設定制御
 - メッセージ表示
 - 強制プログラム実行
 - ソアアップグレード
- ポリシーの設定
- 監査機能の実行
- コンピュータ、ユーザ、およびエージェントの制御
- ソフトウェア定義の作成

DSM エクスプローラには、さまざまな手順を説明したオンライン チュートリアルも組み込まれています。

DSM エクスプローラの Asset Management オブジェクト

[DSM エクスプローラ] ウィンドウのさまざまな場所からアセット管理オブジェクトを表示および設定することができます。

アセット管理を使用すると、以下のレベルでオブジェクトを作成および設定することができます。

グループ レベル

グループ レベルで作成されたオブジェクトは、自動的にメンバアセットにリンクされます。グループ レベルでオブジェクトを有効化または無効化すると、すべてのメンバアセットに対しても有効化または無効化されます。グループ レベルで無効化されたオブジェクトは、グループ レベルでのみ有効化することができます。

コンピュータ レベル

コンピュータ レベルで作成されたオブジェクトは、それぞれのコンピュータにリンクされます。

ユーザ レベル

ユーザ レベルで作成されたオブジェクトは、それぞれのユーザにリンクされます。

ドメイン レベル

ドメイン レベルで作成されたオブジェクトは、いずれのアセットまたはグループにもリンクできます。ドメイン レベルでは、グループおよびアセット レベルにあるオブジェクトも含むドメインで作成されたすべてのオブジェクトを表示することができます。

Asset Management セキュリティ オブジェクト クラス

アセット管理セキュリティ オブジェクト クラスでは、アセット管理オブジェクトへのアクセス権を取り扱います。すべてのアセット管理ユーザは、ログインして DSM エクスプローラの各種の機能を実行するには、以下のオブジェクトクラスへの適切なアクセス権が必要です。

- アセット グループ
- コンピュータ
- ヘルス監視アラート
- セキュリティ プロファイル
- クラスのアクセス権
- セキュリティ エリア
- データベース クレデンシャル
- ユーザ アカウント
- ユーザ プロファイル
- 外部アセット
- ソフトウェアの分類
- ソフトウェア定義
- ソフトウェア グループ
- ソフトウェア パッケージ
- プロシージャ グループ
- プロシージャ
- OS インストール イメージ
- ソフトウェア ジョブ コンテナ
- ソフトウェア ジョブ
- アセット ジョブ
- 共通クエリ
- クエリ ベースのポリシー
- イベント ベースのポリシー
- コントロール パネル アクセス
- エンジン

- エンジン タスク
- インベントリ タスク
- ソフトウェア検出タスク
- ソフトウェアの使用方法タスク
- テンプレート タスク
- 仮想ホスト インベントリ タスク
- 展開ジョブ
- ドメイン グループ
- ドメイン
- スケーラビリティ サーバ グループ
- スケーラビリティ サーバ
- マネージャ
- レポート テンプレート
- レポート スケジューリング
- 設定コンピュータのポリシー
- ソフトウェア ベースのポリシー
- 設定されたディレクトリ

注：共通セキュリティおよびオブジェクト クラスの詳細については、「DSM エクスプローラ ヘルプ」および「実装ガイド」を参照してください。

Common Application Framework (CAF)

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」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。

注： CAF および CAF のプラグインの詳細については、「実装ガイド」を参照してください。

CA メッセージ キューイング (CAM)

CA メッセージ キューイング (CAM) は、高性能でありながらリソース使用率が低く抑えられた、信頼性の高いスケーラブルなアプリケーション間メッセージングを実現する軽負荷メッセージ サービスとして CA 製品で使用されるコンポーネントです。アセット管理エージェントでは、スケーラビリティ サーバとの通信に CAM が使用されます。CAM では、デフォルトで通信に UDP ポート 4104 が使用されます。

Comstore.xml

comstore.xml ファイルには、すべての Client Automation コンポーネントの設定データがすべて格納されます。インストール後、各エージェントには、それぞれの設定データと共にこのファイルのコピーがあります。

共通設定ポリシー設定を使用して、これらの設定を変更できます。更新後、comstore.xml は comstore.enc に変換されます。この後の CCNF 操作では comstore.enc のみを更新します。

comstore を復号化するには、以下のコマンドを使用します。

```
ccnfcmda -cmd GetConfigStore -fi filename.xml
```

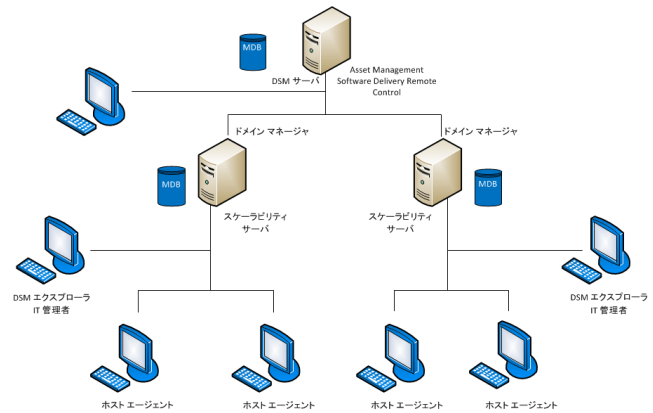
重要： comstore.xml に誤った値を入力すると、Client Automation コンポーネントの機能に悪影響を与えます。

第 3 章：実装

この章では、大規模な組織でアセット管理をインストールする前に、実装および実際の注意事項について説明します。この場合、大規模な組織とは、500 台以上のコンピュータを備えたサイトとします。アセット管理を使用すると、ストレージを分散し、異なるコンポーネントとサーバでデータを処理することによって、大規模なコンピュータ ネットワークを管理できます。

Client Automation には、すべてのプラグイン (アセット管理、ソフトウェア配信、およびリモート コントロール) に共通のアーキテクチャがあります。本章では、このアーキテクチャのアセット管理特有の実装の注意事項について説明します。

以下の図に、CA Client Automation のアーキテクチャを示します。



注：インストールの前提条件のおよびインストール手順の詳細については、「実装ガイド」を参照してください。

サーバの選択

アセット管理ではソフトウェアおよびデータベース コンポーネントを複数のサーバに分散できるため、インプリメンテーションで使用するのに適したネットワーク内のサーバを選択する必要があります。

注：サーバ設定の詳細については、Readme を参照してください。

選択基準

アセット管理実装用のサーバの選択基準には、以下の 2 つがあります。

- パフォーマンスを大幅に低下させることなしに、多数のユーザを同時にサポートすることができる必要があります。
- また、アセット管理特有のファイルおよびデータベース情報のストレージ用に、十分なディスク領域がある必要があります。

ネットワーク パフォーマンスへの影響

複数のスケーラビリティ サーバを使用してアセット管理システムを設定し、各エージェントから見て、ローカル LAN セグメントで常に少なくとも 1 台のスケーラビリティ サーバを使用可能にしておくことによって、混合 LAN/WAN 環境で WAN セグメントをトラバースする必要があるアセット管理トラフィックを最小限に抑えることができます。

エンジン

アセット管理システムに複数のエンジンを導入すると、多数のスケーラビリティ サーバからデータを収集し、ドメインデータベースへ出力することが容易にできるようになります。ドメインデータベースに最新のデータを保持するための正確なニーズに適応するように、エンジンごとに異なる設定を行うことができます。

エージェント

アセット管理エージェントは、以下のいずれかの方法でインストールできます。

- [Client Automation エージェントの展開] またはスケーラビリティ サーバウィザードの使用
- Client Automation インストール DVD の使用

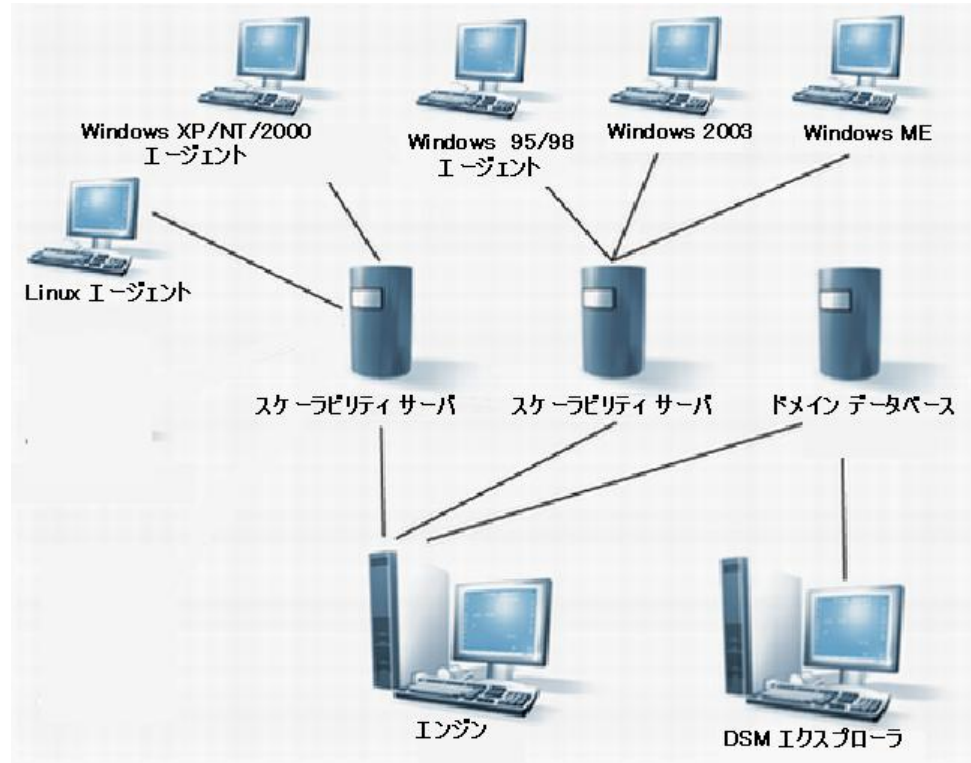
各エージェントを関連するスケーラビリティ サーバに接続するように設定する必要があります。 エージェントによって、エージェントの作業ディレクトリにデータがローカルに格納されます。検出されたコンピュータまたはユーザデータがローカルに格納された以前のスキャン結果と比較され、差異のみがスケーラビリティ サーバに転送されます（通常 20 KB 以下）。

ストレージ エリア

エージェントからドメイン データベースへデータを直接送信することによって、不要なボトルネックが発生する可能性があり、それを回避するために、ストレージを 2 つの異なるエリアに分割することができます。

各管理対象アセットは、ドメイン データベースに接続する代わりにスケーラビリティ サーバに接続し、圧縮 ASCII テキスト形式でデータをスケーラビリティ サーバにコピーします。 エンジンではスケーラビリティ サーバの収集エリアから ASCII テキスト ファイルを取得し、ドメイン データベースのデータベース構造に格納できるように処理します。

以下の図は、DSM エクスプローラ、エンジン、およびエージェントがスケーラビリティサーバおよびドメインデータベースにどのように関連付けられているかを示したものです。



上記の図は、エージェントおよびエンジンとスケーラビリティサーバとの接続を示しています。

- エージェントはスケーラビリティサーバに接続し、管理トランザクションへのアクセス、ハードウェアとソフトウェアのデータおよびステータス情報のレポートを行います。
- エンジンはスケーラビリティサーバに接続し、ドメインデータベース間のデータの更新、スケジュールされたアクションおよび完了したアクションのステータス情報の取得を行います。

インストール前の実際的な注意事項

複数サイトまたは大規模サイト環境におけるアセット管理システムのインストール、使用、およびメンテナンスに関する実際的な注意事項についての以下の情報を読む前に、これまでのセクションをよく理解しておく必要があります。このセクションには、以下の新しい用語があります。

メイン サイト - エンタープライズ データベースおよびドメイン データベースがあるサイトです。

サイト - WAN リンクでメイン サイトに接続されたリモート サイトです。

インストールの計画

アセット管理をインストールする前に、以下の質問について検討してください。

- サイトはいくつありますか？
- リモートおよびメインのサーバ名とタイプは何ですか？
- 異なる WAN リンクの速度はどれだけですか？
- WAN リンクではどのプロトコルが伝送されますか？
- 営業時間中に、エンド ユーザが使用できる帯域幅は充分ですか？ または夜間のみ、WAN リンクを使用するようにアセット管理を設定する必要がありますか？
- DSM エクスプローラ ユーザをどこに配置しますか？ メイン サイトのみですか、それともリモート サイトにも配置しますか？

最良のメイン サイトの選択

大規模な組織のメイン サイトとして最適なのは、大部分の **Client Automation** エクスプローラ ユーザが配置されるサイトです。ドメイン データベースは、この場所に常駐する必要があります。

大部分のサポートおよび管理アクティビティが実行されるサイトを選択します。多くの場合、これはほとんどのアセット管理エージェントがあるサイトでもあります。このことをお勧めする理由は、ほとんどのデータベース アクセスは、**DSM** エクスプローラからドメイン データベースへ、およびエンジンからドメイン データベースへ行われるためです。（通常、エンジンは、**IS** 部門に近く、技術装置用に設計された部屋に置かれます。）

スケーラビリティ サーバの数

スケーラビリティ サーバの数を決定する前に、以下のことを考慮しておく必要があります。

- スケーラビリティ サーバあたりのコンピュータおよびユーザ（アセット）の数
- サイトの数
- サーバが処理できるディレクトリあたりのファイルの数（ネットワーク オペレーティング システムに依存）
- サーバでライセンス供与が行われる方法（ネットワーク オペレーティング システムに依存）

スケーラビリティ サーバあたりのコンピュータ台数

スケーラビリティ サーバあたり **1000** 台のコンピュータを容易に操作できます（アセット管理のみを使用している場合）。アセット管理エージェントは **CA** メッセージ キューイング (CAM) を使用して、スケーラビリティ サーバと通信します。

サイトあたりのスケーラビリティ サーバ台数

エージェントは **WAN** リンク経由で接続できないため、サイトあたりに少なくとも **1** 台のスケーラビリティ サーバが必要です。 エージェントが **WAN** リンク経由で接続された場合、エージェントの実行時に不必要な遅延が生じます。

ディレクトリあたりのファイル数

一部のネットワーク オペレーティング システムでは、ディレクトリ内のファイルが特定の数を超えなければ、サーバは高い性能を実現することができます。

1 つのディレクトリ内のファイルの数は、所定のサーバのコンピュータおよびユーザの数以上になることはありません。唯一の例外は収集ディレクトリですが、ディレクトリ内のファイルの数は一時的なものであるため、問題とはなりません。

サーバのライセンス供与

一部のサーバは接続でライセンス供与されます。 この種の環境では、ログオンサーバあたり **1** 台のスケーラビリティ サーバを配置して、常にどのサーバのライセンス数も超過しないようにすることができます。

シナリオ

従業員数が数百人で、北アメリカに 4 つの主要な事業所を持つ中規模の生鮮食品の製造者です。事業所の 3 つは米国（ボストン、ニューヨーク、およびオレゴン州ポートランド）にあり、1 つはカナダのバンクーバーにあります。各事業所には 75 - 100 人の従業員が働いています。また、この会社には、最近買収によって取得した小規模な出張所がテキサス州オースチンにあります。オースチンの出張所では、20 - 30 人が働いています。

中心的な事業所はニューヨークにあり、この事業所は本社の役割も果たしています。エンタープライズマネージャはここに配置されており、業務のすべての側面の集中管理およびすべての事業所の監視を可能にしています。

4 つの事業所は地理的に離れていますが、2 つの異なる地域に分類されます。ボストンおよびニューヨークの事業所は、どちらも北米の北東部にあり、ポートランドおよびバンクーバーの事業所はどちらも北西部にあります。このため、各地域にスケーラビリティ サーバとドメインマネージャを 1 台ずつ配置することが決定されました。2 台のスケーラビリティ サーバとドメインマネージャが、それぞれの階層に属する毎日のタスクを管理します。

各地域には独自のドメイン管理者がおり、ネットワーク内のコンピュータへのアセット管理エージェントの展開、セキュリティ プロファイルの作成、DSM エクスプローラにアクセスできるユーザおよびアクセス範囲の指定、IT アセットの効率的な使用の監視を行います。管理者は、地域のドメインマネージャ上で **Client Automation** エクスプローラを使用して問題のトラブルシューティングも行います。

管理者または適切な権限を持つ他のいずれかのユーザは、ビジネス要件に合うように以下のアセット管理固有の設定を行います。

- 収集モジュールを作成および設定し、追加のハードウェア インベントリを収集します。
- アセット管理によって検出される追加のソフトウェア シグネチャを作成します。
- 接続されているすべてのエージェントにポリシーを適用し、エージェントを完全に制御します。たとえば、管理者はポリシーを作成してすべてのエージェント上の正常なジョブの実行を確認し、電子メールまたは **CA Service Desk Manager** チケットによって障害を報告することができます。

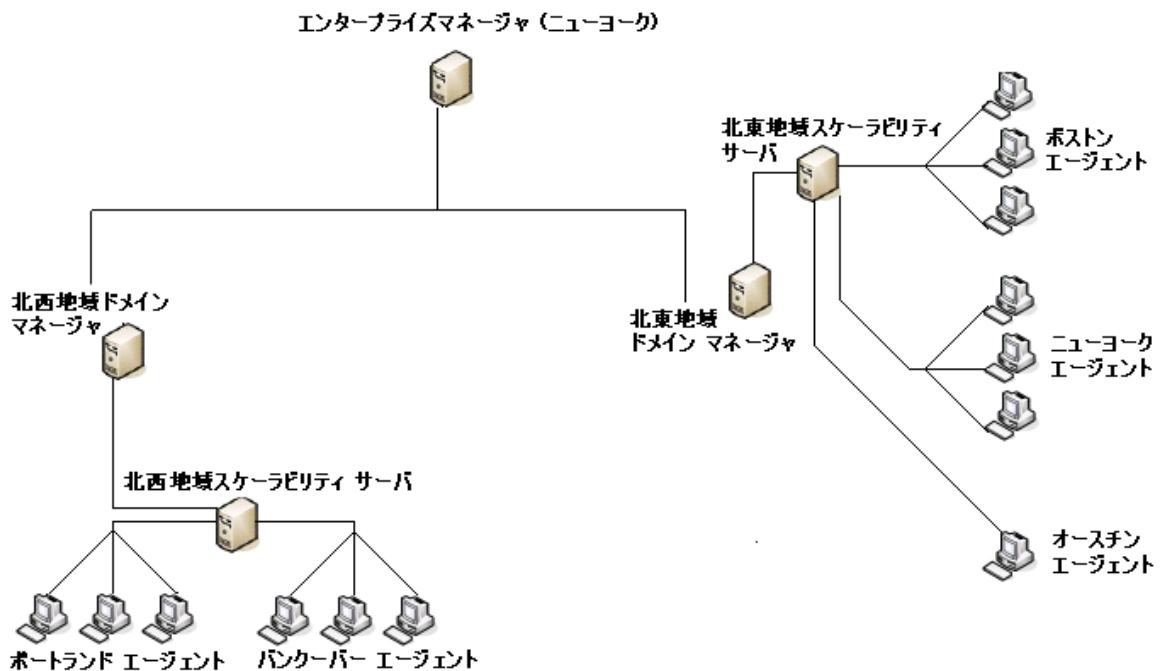
残りの唯一の問題は、オースチンに関してはどうするかということです。オースチンはいずれの地域にも分類されません。従業員は西海岸と東海岸のどちらのスケーラビリティ サーバを使用すればよいのでしょうか。またはオースチンに独自のスケーラビリティ サーバ、ドメインマネージャ、およびドメイン管理者が必要でしょうか。

決定的要素は、スケーラビリティ サーバに接続するユーザの数です。オースチンの出張所には 30 人の従業員しかいないため、ほとんどの場合、独自のスケーラビリティ サーバを持つ必要はありません。その代わりに、オースチンの従業員はユーザ数が最も少ないスケーラビリティ サーバにデータを送信することができます。

従業員のニーズが増えた場合は、オースチン、または 2 箇所の主要地域のいずれかに、別のスケーラビリティ サーバを追加することができます。Client Automation は完全にスケーラブルであるため、必要に応じて、スケーラビリティ サーバとドメイン マネージャを追加することができます。Client Automation のスケーラブルな多層アーキテクチャは、大小にかかわらずあらゆる規模の組織に適応できます。すべてのアセット インベントリ情報が各ドメイン マネージャの場所で管理されるため、このアーキテクチャは堅牢です。

アーキテクチャ全体は、ドメイン マネージャ間のデータを複製するエンタープライズ マネージャによって制御されます。ドメイン内のすべてのコンピュータで必ず実行する必要があるジョブおよびポリシーをプッシュできます。

以下の図は、アセット管理アーキテクチャを生鮮食品製造会社を導入する方法を示したものです。



注：アセット管理導入の詳細については、「実装ガイド」を参照してください。

第 4 章 : Asset Management の設定

アセット管理に各種の設定を行い、アセット管理エージェントのパフォーマンスを最適化し向上させることができます。これらの設定は、[DSM エクスプローラ] ウィンドウを使用して設定できるドメイン マネージャによって保持および制御されます。

本章では、ビジネス要件に応じて設定してエージェントの機能を強化できるさまざまなアセット管理オブジェクトについて説明します。

- アセットのグループ化
- アセット管理固有の設定の共通設定ポリシーの設定
 - 電子メール システムへの統合の設定
 - Service Desk への統合の設定
- 収集モジュール
 - インベントリ検出モジュール
 - インベントリ テンプレート モジュール
- カスタム ソフトウェア シグネチャの作成
- バックアップ用ファイルの設定
- 収集タスクの設定およびスケジュール

このセクションには、以下のトピックが含まれています。

[アセットのグループ化](#) (P. 48)

[ユーザ指定スキャン](#) (P. 48)

[カスタム ソフトウェア シグネチャの作成方法](#) (P. 51)

[Intellisig](#) (P. 77)

[仮想アプリケーション イメージ](#) (P. 141)

[コンテンツ ユーティリティ](#) (P. 148)

[収集モジュール](#) (P. 152)

[ファイル収集](#) (P. 183)

[収集タスク](#) (P. 189)

[グリーン IT レメディエーション](#) (P. 265)

アセットのグループ化

アセットグループを使用すると、コンピュータおよびユーザを論理的にグループに分類することができます。[すべてのコンピュータ]、[すべてのユーザアカウント]、[すべてのユーザプロファイル]は、コンピュータ、ユーザ、およびユーザプロファイルのデフォルトグループになります。アセットをアセットグループに分類することにより、以下のことが可能になります。

- グループのメンバのクエリ
- グループに固有のジョブまたはタスクのプッシュ
- ポリシーに違反したグループ内コンピュータの表示
- グループレベル権限の指定。たとえば、組織にさまざまな部門がある場合、部門コードに基づいてアセットを分類し、グループの部門マネージャに完全な権限を付与することができます。

アセットグループは、以下のいずれかになります。

静的グループ

手動でグループに追加または削除されたメンバが含まれています。

動的グループ

クエリ結果に基づいて動的に追加または削除されたメンバが含まれています。動的グループは、クエリに基づいています。

ユーザ指定スキャン

ユーザ指定スキャンを使用すると、ソフトウェアスキャンおよびアセット管理エージェントのプロセス優先度を設定できます。ユーザ指定スキャンではファイルスキャン中のハードドライブの負荷が最小化されるため、ソフトウェアスキャナによって消費される I/O 時間が減少します。

Windows エージェントでは、最適なパフォーマンスを得るためにユーザ指定スキャンが実装されています。

Linux/UNIX エージェントの場合、ユーザ指定スキャンの設定は、「インストール後のユーザ指定スキャンの設定」で説明されているように、インストール中に行うことも、インストール後に `comstore.xml` ファイルを変更することで行うこともできます。

注：エディタを使用して `comstore.xml` ファイルを変更しないでください。

インストール後のユーザ指定スキャンの設定

シグネチャスキャンおよびアセット管理エージェントの優先度を指定する場合は、ユーザ指定スキャンを設定する必要があります。これは、インストール中またはインストール後に行うことができます。設定された優先度に基づいて、エージェントをいずれの優先度レベルでも実行することができます。

注：ユーザ指定スキャンは、UNIX/Linux エージェントに対してのみ設定できます。

インストール後にユーザ指定スキャンを設定する方法

1. 以下のコマンドを実行します。

```
caf stop
```

caf プロセスが停止します。

2. 以下のコマンドを使用してエージェントの優先度レベルを指定します。

```
ccnfcmda -cmd SetParameterValue -ps /itrm/uam/prio_value -pn Client -v Value
```

使用できる値は、-20 から 19 までです。

-20

エージェントが高い優先度で実行されることを示します。

19

エージェントが低い優先度で実行されることを示します。

0

エージェントがデフォルトまたは通常の優先度で実行されることを示します。

3. 以下のコマンドを使用して caf プロセスを開始します。

```
caf start
```

エージェントが、設定した優先度に基づいて実行されます。

第 5 章：カスタム ソフトウェア シグネチャの作成方法

このシナリオでは、管理者がカスタム ソフトウェア シグネチャを作成する方法について説明します。ソフトウェア シグネチャ定義は、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、変更日などの属性を使用してソフトウェア アプリケーションを識別するために役立ちます。たとえば、所属する企業でのみ使用されるソフトウェアなど、事前定義されたシグネチャが使用できないソフトウェアでも、カスタム シグネチャを作成できます。

この機能は、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するために役立ちます。また、既存の製品に新しいソフトウェア リリースおよびパッチを追加することもできます。以下の図に、カスタム ソフトウェア シグネチャ作成の手順を示します。

カスタム ソフトウェア シグネチャの作成方法



このセクションには、以下のトピックが含まれています。

[シグネチャのタイプについて](#) (P. 52)

[製品の作成](#) (P. 54)

[スイート、リリース、またはパッチの作成](#) (P. 55)

[分類によるソフトウェア定義の整理](#) (P. 59)

[カスタム シグネチャ定義の確認](#) (P. 61)

[ソフトウェアシグネチャ XML リファレンス情報](#) (P. 62)

シグネチャのタイプについて

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。

注： 事前定義されたシグネチャおよび CA から提供されたシグネチャは、変更できません。

使用するライセンスソフトウェアを検出するための新しいソフトウェアシグネチャを作成したり、既存の製品定義に新しいリリースやパッチを追加することもできます。ドメインレベルでソフトウェア定義を作成した場合、検出されたソフトウェア情報はドメインレベルのみで表示されます。ただし、エンタープライズレベルでソフトウェア定義を作成した場合は、検出されたソフトウェア情報をドメインレベルおよびエンタープライズレベルの両方で表示および使用できます。

手動でユーザインターフェースからソフトウェア認識パラメータを指定したり、XML ファイルをインポートすることで、スイート、リリース、およびパッチを作成できます。

- [ユーザインターフェースからのソフトウェア認識パラメータの指定](#) (P. 55)
- [XML ファイルからのソフトウェア認識パラメータのインポート](#) (P. 57)

以下の種類の定義を作成できます。

製品

ソフトウェア定義の基礎となる定義です。このコンテナ コンポーネントには、リリースおよびスイートが含まれます。製品には以下のコンポーネントが必要です。たとえば、**Microsoft Outlook 2000** は製品です。製品定義には、バージョン情報のみがあります。

リリース

ソフトウェアの特定のリリースが含まれています。リリース定義は、製品に対してのみ作成されます。たとえば、**Microsoft Outlook 2000 SP2** はリリースです。

パッチ

リリースへの修正が含まれています。パッチはリリースに対してのみ作成されます。たとえば、**Q303833** は **Microsoft Outlook 2000 SP2** リリースのパッチです。

スイート

さまざまな個々の製品および統合された製品で構成されるソフトウェア群が含まれています。たとえば、**Microsoft Office** などです。スイート定義は、製品に対してのみ作成されます。

スイート コンポーネント

Microsoft Word などのスイートの個々の製品が含まれています。スイート コンポーネントは、スイートに対してのみ作成されます。

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ソフトウェア定義のベースを定義します。**CA** はコンテンツ ダウンロード サービスで仮想アプリケーションイメージを認識するソフトウェア定義を提供できませんので、**DSM** 管理者はこれらの仮想アプリケーションイメージ定義を作成する必要があります。

エージェントがコンピュータにソフトウェア シグネチャ指定があるかどうかスキャンする際に、すべての指定が満たされていることを確認してください。ソフトウェアは認識されます。

製品の作成

製品は、定義の基礎です。リリースまたはスイートを追加する前に製品を作成する必要があります。

新しい製品を作成する方法

1. DSM エクスプローラで [ドメイン] - [ソフトウェア] - [定義] - [分類] フォルダに移動します。

ドメインの既存の分類が表示されます。

2. 既存の分類を選択するか、[タスク] セクションで [新規分類] をクリックして、新しい分類を作成します。

分類の既存の定義が表示されます。

3. 分類を右クリックして、[新規製品] を選択します。

[製品の新規作成] ダイアログ ボックスが表示されます。

4. 製品名およびバージョンを入力し、[OK] をクリックします。

製品のリリースを作成するかどうかを確認するメッセージが表示されます。

- a. [はい] をクリックします。

[リリースの新規作成] ダイアログ ボックスが表示され、新しいリリースの詳細を指定できます。

- b. [いいえ] をクリックします。

製品が分類に追加されます。

注：製品自体に機能はありません。リリースまたはパッチを作成して、シグネチャを指定する必要があります。

関連項目：

[シグネチャのタイプについて](#) (P. 52)

スイート、リリース、またはパッチの作成

手動でユーザ インターフェースからソフトウェア認識パラメータを指定したり、XML ファイルをインポートすることで、スイート、リリース、およびパッチを作成できます。

- [ユーザ インターフェースからのソフトウェア認識パラメータの指定](#) (P. 55)
- [XML ファイルからのソフトウェア認識パラメータのインポート](#) (P. 57)

ユーザ インターフェースからのソフトウェア認識パラメータの指定

以下の手順で示されるように、ユーザ インターフェースからリリース、パッチ、またはスイートを作成できます。

- [リリースの作成](#) (P. 56)
- [パッチの作成](#) (P. 56)
- [スイートの作成](#) (P. 55)

スイートの作成

スイートには、スイート定義が含まれています。シグネチャ スキャナでエージェント コンピュータがスキャンされると、スイートおよびスイート コンポーネント インベントリの両方が返されます。たとえば、ドメインの **Microsoft Office** のインストール数を参照できますが、同様に **Microsoft Word** のインストール数も参照できます。

新しいスイートを作成する方法

1. **DSM** エクスプローラで [ドメイン] - [ソフトウェア] - [定義] - [分類] フォルダに移動します。
ドメインの既存の分類が表示されます。
2. 既存の分類を選択するか、[タスク] セクションで [新規分類] をクリックして、新しい分類を作成します。
分類の既存の定義が表示されます。
3. スイートを追加する製品を右クリックし、[新規スイート] を選択します。
[スイートの新規作成] ダイアログ ボックスが表示されます。
4. 新しいスイートの詳細を [一般]、[識別]、[除外] の各オプション タブで設定し、[OK] をクリックします。
該当の製品で新しいスイートが作成されます。

関連項目：

[シグネチャのタイプについて \(P. 52\)](#)

リリースの作成

リリースには、ソフトウェア定義が含まれています。ここでは、リリースを一意に識別するパラメータが定義されます。リリース定義は、エージェント コンピュータのスキャン中にシグネチャ スキャナによって使用されます。

新しいリリースを作成する方法

1. **DSM** エクスプローラで [ドメイン] - [ソフトウェア] - [定義] - [分類] フォルダに移動します。
ドメインの既存の分類が表示されます。
2. 既存の分類を選択するか、[タスク] セクションで [新規分類] をクリックして、新しい分類を作成します。
分類の既存の定義が表示されます。
3. リリースを追加する製品を右クリックし、[新規リリース] を選択します。
[リリースの新規作成] ダイアログ ボックスが表示されます。
4. 新しいリリースの詳細を [一般]、[識別]、[除外] の各オプション タブで設定し、[OK] をクリックします。
該当の製品で新しいリリースが作成されます。

パッチの作成

パッチ レベルのインベントリ データをトラッキングするには、パッチを作成する必要があります。

新しいパッチを作成する方法

1. **DSM** エクスプローラで [ドメイン] - [ソフトウェア] - [定義] - [分類] フォルダに移動します。
ドメインの既存の分類が表示されます。
2. 既存の分類を選択するか、[タスク] セクションで [新規分類] をクリックして、新しい分類を作成します。
分類の既存の定義が表示されます。

3. 製品をダブルクリックします。
製品の既存のリリースおよびスイートが表示されます。
4. パッチを追加するリリースを右クリックし、[新規パッチ] を選択します。
[パッチの新規作成] ダイアログ ボックスが表示されます。
5. 新しいパッチの詳細を [一般]、[識別]、[除外] の各オプション タブで設定し、[OK] をクリックします。
該当のリリースで新しいパッチが作成されます。

関連項目：

[シグネチャのタイプについて](#) (P. 52)

XML ファイルからのソフトウェア認識パラメータのインポート

XML ファイルからシグネチャ定義をインポートできるようになりました。このインポート機能では、複雑なシグネチャの作成をサポートしています。この XML ファイルを使用して、1 つのシグネチャに対し複数のレジストリおよびパッケージ情報を指定できます。

この新しい方法を使用すると、以下ことができます。

- 複雑なカスタム シグネチャ作成処理を簡略化できます。
- カスタム シグネチャを追加する時間を削減し、柔軟に対応できます。
- シグネチャでパッケージ、レジストリ、またはファイル XML タグを使用し、ネストされたグループを追加できます。
- CA 提供のシグネチャ定義を参照用として使用し、カスタム シグネチャを作成できます。
- XML 内のシグネチャ定義を表示し、DSM エクスプローラの [識別] タブで特定の CA 提供シグネチャ リリース、パッチ、またはスイートを確認できます。

次の手順に従ってください：

1. **DSM** エクスプローラで [ドメイン] - [ソフトウェア] - [定義] - [分類] フォルダに移動します。
ドメインの既存の分類が表示されます。
2. 既存の分類を選択するか、[タスク] セクションで [新規分類] をクリックして、新しい分類を作成します。
分類の既存の定義が表示されます。
3. 新しいソフトウェア定義（リリース、スイート、パッチなど）を作成するか、または既存の定義を右クリックします。
新しいスイート、リリース、またはパッチ ダイアログ ボックスが表示されます。
4. [識別] タブに移動し、認識パラメータを **XML** テキストとして指定するチェック ボックスをオンにします。
5. 以下のいずれかの方法で、**XML** ファイル テキストを追加します。

参照

XML ファイルをインポートします。

XML テキスト領域

XML コンテンツを **XML** テキスト領域にコピーおよび貼り付けします。

6. （オプション）XML コンテンツをプレビューし、[OK] をクリックしてカスタム シグネチャを完成させます。
リリースおよびシグネチャは作成され、製品に関連付けられます。

注： CA 提供のソフトウェア定義のいくつかに複数のシグネチャがある場合、**Windows** シグネチャ パラメータのみが表示されます。入力シグネチャ **XML** が有効な **XML** 形式であることを確認してください。

XML タグ、キー属性、およびサンプル シグネチャの詳細については、「[ソフトウェア シグネチャ XML リファレンス情報 \(P. 62\)](#)」を参照してください。

分類によるソフトウェア定義の整理

ソフトウェア定義を分類および整理すると、定義のタイプ、メーカー、および分類に従って容易に検索できるようになります。

次の手順に従ってください：

1. ドメインマネージャで [ソフトウェア] - [定義] - [分類] に移動します。
右側のペインに既存の分類が表示されます。
2. [タスク] セクションで [新規分類] をクリックします。
[新しいソフトウェアの分類] ダイアログ ボックスが表示されます。
注： 既存の分類を使用することもできます。
3. このダイアログ ボックスで分類の名前およびそのほかの詳細を指定し、
[OK] をクリックします。
新しい分類が追加されます。
4. 分類を右クリックして、[分類の整理] を選択します。
[分類の整理] ダイアログ ボックスが表示されます。
5. 条件を指定してソフトウェア定義をフィルタし、[選択した定義] に追加して [OK] をクリックします。
選択された定義が分類に追加されます。

製品コンポーネントの追加

以下の関連コンポーネントを追加することによって製品を整理できます。

- スイートおよびリリースを製品に追加
- パッチをリリースに追加
- スイート コンポーネントをスイートに追加

親定義に基づいて作成されたコンポーネントは、自動的に親定義に追加されます。これらのコンポーネントもほかの定義に追加する場合、製品コンポーネントもそれに合わせて追加できます。

製品コンポーネントを追加する方法

1. 製品、リリース、またはスイートを右クリックし、[製品の整理] を選択します。
[製品の整理] ダイアログ ボックスが表示されます。
2. ソフトウェア定義に追加する関連コンポーネントをフィルタし、[選択した定義] に追加して [OK] をクリックします。
選択されたコンポーネントが定義に従って整理されます。

定義のスキャンの有効化または無効化

デフォルトでは、すべてのソフトウェア定義のシグネチャ スキャンが有効になっています。ある定義で、シグネチャ スキャナでリリースまたはパッチのスキャンを行わない場合は、その定義のスキャンを無効化できます。

定義のスキャンを有効化または無効化する方法

方法 1

1. [ドメイン] - [ソフトウェア] - [定義] - [分類] - [すべての定義] に移動し、必要な定義を選択します。
選択された定義の詳細が表示されます。
2. [検出の有効化] 列を確認します。この列には、以下のいずれかの値を設定できます。

はい

この定義のスキャンが有効であることを示します。

いいえ

この定義のスキャンが無効であることを示します。

3. 定義を右クリックし、状況に応じて「スキャンの有効化」または「スキャンの無効化」を選択します。

確認メッセージが表示されます。

- a. 「はい」をクリックします。

これで、リンクされているすべての定義のスキャンが有効化または無効化されます。たとえば、製品の場合、「はい」をクリックすると、リンクされているリリース、スイートおよびパッチのスキャンが無効化または有効化されます。

- b. 「いいえ」をクリックします。

これで、選択された定義のスキャンのみが有効化または無効化されます。

方法 2

1. 「ドメイン」 - 「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 - 「ソフトウェア」 - 「検出」に移動します。

選択したコンピュータで検出されたソフトウェアが表示されます。

2. もうスキャンしないソフトウェアを右クリックし、「スキャンの無効化」を選択します。

選択したソフトウェアが、検出されたソフトウェアのリストからすぐに削除され、「検出の有効化」列の「すべての定義」フォルダが「いいえ」に設定されます。

注：方法 2 では、1 つの定義のスキャンのみを無効化することがすることができます。スキャンを有効化するには、方法 1 の手順に従います。

カスタム シグネチャ 定義の確認

シグネチャ スキャンが正常に完了した後、「ドメイン」、「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」、「ソフトウェア」、検出セクションの順に移動し、検出されたソフトウェア リストにあるカスタム ソフトウェア シグネチャ 定義を確認します。

カスタム ソフトウェア シグネチャ が完成しました。

ソフトウェア シグネチャ XML リファレンス情報

ソフトウェア シグネチャは、IT Client Automation サーバに登録されているエージェント上にインストールされたソフトウェアを識別するために役立ちます。シグネチャは、一般システム情報、ファイル コンテンツ、プロパティ、およびインストールされたソフトウェアのレジストリ コンテンツ（Windows の場合）またはパッケージ情報（UNIX の場合）が含まれる XML テンプレートです。

この付録では、シグネチャ XML タグ、キー属性、およびサンプル シグネチャに関する以下の概念情報の理解に役立つ情報を提供します。

- [シグネチャ XML タグ](#) (P. 63)
- [キー属性およびネスト](#) (P. 67)
- [サンプル シグネチャ](#) (P. 73)

シグネチャ XML タグ

ソフトウェアシグネチャでは、XML 形式にあるシグネチャデータを収集するために以下の XML タグが使用されます。

レジストリ タグ

Windows レジストリ キー/値を解析する機能を提供します。例：

```
<group type="and">
  <registry
    name="HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Trust
    Antivirus\CurrentVersion\Version" match=" 7.1" />
  <registry
    name="HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Trust
    Antivirus\CurrentVersion\Build" match="501" /> </group>
```

ファイル タグ

ファイル名、バージョン、サイズ、変更日、パスを解析する機能、およびファイルのコンテンツをスキャンする機能も提供します。

path

Windows の %systemroot% および %windir% などの値を使用して、ファイルの存在を確認します。ワイルドカード * を使用すると、ファイルシステム全体が検索されます。以下に例を示します。

```
<file name="named.conf" path="*" />
```

ファイルシステム全体を確認します。

```
<file name="Reader\acord32.exe" path="*" />
```

パスの一部に Reader がある acord32.exe ファイルを確認します。

```
<file name="openssl" path="/bin:/usr/bin:/usr/local/bin" />
```

絶対値のパスを確認します。

match

ファイルのコンテンツを解析します。一致条件の定義にあるものと同じデータがファイルに含まれている場合、true を返します。例：<file name="Ouactrl.ocx" match="2¥.0¥.0¥.0" path="*" />

minversion および maxversion

ファイルバージョン情報を確認します (Windows のみ)。UNIX では常に false を返します。

ファイルバージョン番号が指定値以上である場合、`minversion` 属性は `true` を返します。

ファイルバージョン番号が指定値以下である場合、`maxversion` 属性は `true` を返します。

注：バージョン番号は `W.X.Y.Z` の形式です。`W`、`X`、`Y`、および `Z` は 16 ビットの数値です。`minversion` および `maxversion` を組み合わせると、非常に柔軟にバージョン範囲を確認できます。例：

```
<file name="QuickTimePlayer.exe" minversion="5.0.2.15"
maxversion="5.0.2.15" path="*" />
```

```
<file name="InoRT.exe" minversion=" 7.1.192.0" maxversion="
7.1.500.0" path="*" />
```

`minmodified` および `maxmodified`

ファイルの変更日を確認します。例：`<file name="ErwDSM.exe" minmodified="2004-10-28T00:00:00Z" maxmodified="2004-10-28T23:59:59Z" path="*" />`

`minfilesize` および `maxfilesize`

ファイルのサイズを確認します。例：`<file name="BPSyncER.exe" minfilesize="151603" maxfilesize="151603" path="*" />`

システム情報タグ

以下のオペレーティング システム情報を解析する機能を提供します。

`osname`

UNIX では、`uname -s` の出力から取得される名前です。

Windows バージョンでは、`osname` は常に `Windows` です。

例：`<sysinfo osname="HP-UX" />`

`osversion`

UNIX では、照合される情報は `uname -v` の出力と同等です。

Windows では、この情報は Microsoft 提供のサービス パック 文字列（例： *Service Pack 3*）です。

例：`<sysinfo osversion=". *Version 6¥.3.*" />`

`osrelease`

UNIX では、この情報は `uname -r` の出力と同等です。

Windows では、この情報は、「NT 4.0」、「2000」、または「XP」です。

例：<sysinfo osrelease="2¥.4¥.*"/>

platform

UNIX では、照合される情報は `uname -m` の出力と同等です。

Windows では、照合される文字列は常に「x86」です。

例：<sysinfo platform="sun4.*"/>

processor

Solaris では、照合される情報は `uname -p` の出力と同等です。

HP-UX では、プロセッサは `pa-riscX.Y` または不明として識別されます。ここで、`X.Y` は 1.0、1.1、1.2、2.0 のいずれかです。

Windows では、照合される文字列は常に不明です。

AIX では、プロセッサは RS1、RSC、RS2、601、603、604、620、630、A35、RS64II、RS64III、POWER4、mpc7450、POWER5、または不明のいずれかとして識別されます。

Linux では、プロセッサは常に不明として識別されます。

例：<sysinfo processor="sparc"/>

パッケージ タグ

インストールされたプログラム データベースからパッケージ情報をクエリすることを可能にします。

Windows

この情報は、以下のアンインストール レジストリ セクション内にあります。

`HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall`

注：`DisplayName` はパッケージ タグの値名で、`DisplayVersion` はパッケージ タグのバージョン値です。

Linux

この情報は、RPM データベース内にあります。

- `rpm -qa` を使用すると、コンピュータにインストールされたパッケージがリスト表示されます。SuSe 上のパッケージ詳細をリスト表示するには、パッケージ名 `rpm -qi` を使用できます。

HP-UX

この情報は、システム パッケージ データベース内にあります。

- `swlist` を使用すると、コンピュータにインストールされたパッケージがリスト表示されます。

IBM AIX

この情報は、システム パッケージ データベース内にあります。

`lspp -l` を使用すると、コンピュータにインストールされたパッケージがリスト表示されます。

Sun Solaris

この情報は、システム パッケージ データベース内にあります。

`pkginfo -l` を使用すると、コンピュータにインストールされたパッケージがリスト表示されます。以下に例を示します。

```
<package name="ca-unicenter-servicedesk"/> <package  
name="ca-unicenter-servicedesk" version="11.2.0.0"/>
```

バージョンおよびリリースが指定された場合、両方が一致する必要があります。

キー属性およびネスト

インストールされたソフトウェアのシグネチャデータを収集するためのキー属性を以下に示します。

レジストリ (Windows のみ)

レジストリ データは、どのレジストリ ハイブからでも収集できますが、ほとんどの場合 HKLM\Software が通常使用されます。以下に例を示します。

- iGateway のシグネチャには以下のレジストリ識別子が含まれています：

```
<registry
name="HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\iGateway\Version" match="4.0.060220" />
```



注：以下のいずれかのレジストリの場所に、プログラムの追加と削除エントリがすべて見つかります。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

- VLC Media Player 2.1.3 がインストールされている場合、プログラムの追加と削除内の対応情報は以下のレジストリの場所にマップされています。
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\VLC media player

VLC Media Player 2.1.3 のシグネチャには、以下のようなレジストリ識別子が含まれています。



- ```
<package name=" VLC media player 2.1.3" version="2.1.3"/>
```

### 一意のファイルおよびその属性

インストールによってドロップされたソフトウェア ファイルを以下の属性を使用して一意に識別します。

### ファイル バージョン

.exe ファイルのプロパティ ウィンドウで表示されるものと同じです。例：

```
<file name="igateway.exe" path="*" minversion="4.0.60220.0"
maxversion="4.0.60220.0"/>
```



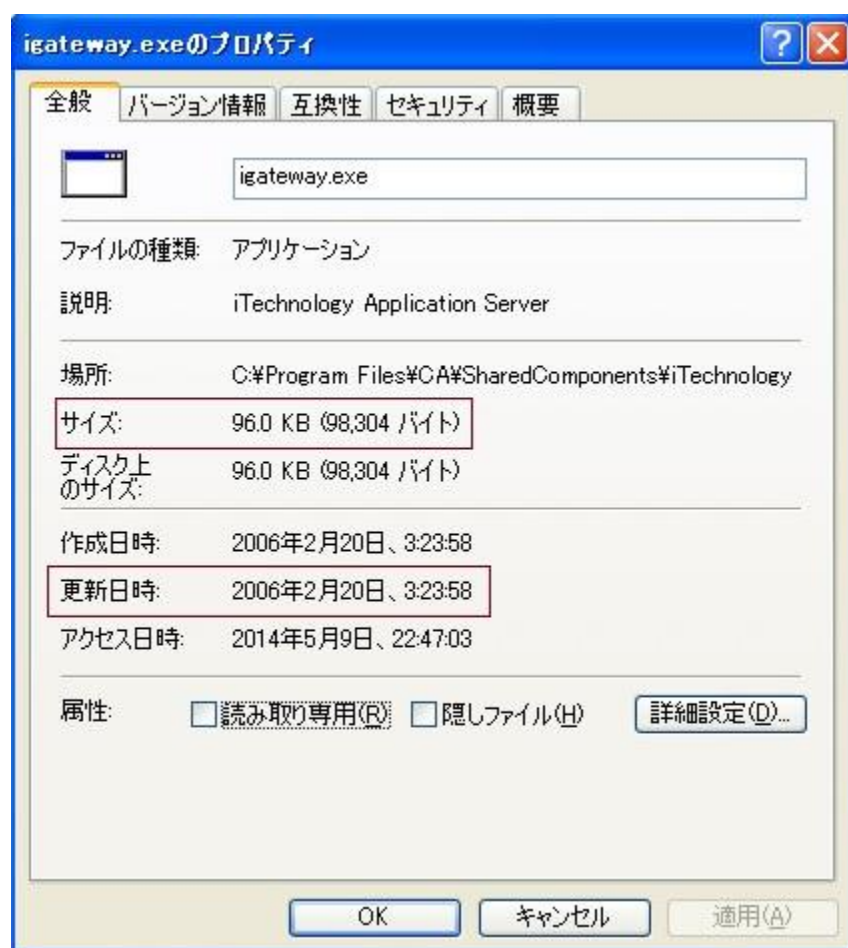
## ファイル日付

.exe ファイルのプロパティ ウィンドウの「更新日時」に表示されるものと同じです。

## ファイル サイズ

.exe ファイルのプロパティ ウィンドウで表示されるものと同じです。 例：

```
<file name="igateway.exe" path="*" minfilesize="98304"
maxfilesize="98304" minmodified="2006-02-20T00:00:00Z"
maxmodified="2006-02-20T23:59:59Z"/>
```



## 設定ファイル

パーサが読み取ることができるバージョン情報が含まれています。パーサはファイルのコンテンツを読み取り、一致条件に指定されているデータを検索します。例：<file name="igateway.conf" path="\*" match="4.0.060220" />



注：ファイルバージョンおよびレジストリがない場合に UNIX シグネチャを作成するには、設定ファイルを使用する方が便利です。

#### XML での arch="64" タグの使用方法

HKLM¥SOFTWARE¥Wow6432Node キーは、64 ビット Windows OS 上で 32 ビット アプリケーションによって使用されます。このキーは「HKLM¥SOFTWARE」と同等ですが、独立しています。通常、64 ビットのバイナリ ファイルは、自分自身を HKLM¥SOFTWARE に登録します。他方、32 ビットのバイナリ ファイルは、自分自身の情報を HKLM¥SOFTWARE¥Wow6432Node 下に入力します。同様に、32 ビット アプリケーションは %SystemRoot%¥Syswow64 を %SystemRoot%¥System32 と見なします。2 つの [Program Files] ディレクトリがあり、いずれも 32 ビットおよび 64 ビット アプリケーションの両方から見ることは可能です。2 つのディレクトリを区別するために 32 ビットのファイルが格納されているディレクトリは [Program Files (x86)] という名前になっており、他方 64 ビットの方は追加の修飾子のない従来の [Program Files] という名前を保持しています。

**重要：**デフォルトでは、arch="64" タグがない場合、CA Client Automation エージェントはレジストリ/ファイルパスを 32 ビットとして処理します。arch="64" タグは、レジストリおよびファイルの名前タグにのみ適用されることに注意してください。したがって、アプリケーションのアーキテクチャに従い適切なレジストリ キーを使用するように注意します。

例：<registry name="HKEY\_LOCAL\_MACHINE¥SOFTWARE¥JavaSoft¥Java Runtime Environment¥1.6.0" arch="64" /> Or <file name="bin¥java.exe" match="1.6.0-b105" path="\*" arch="64" />

## ネスト/グループ化

複数のレジストリ キー値およびファイル属性をグループ化します。**group** タグを使用した以下の論理条件を使用し、必要なインストール済みソフトウェアの存在を確認するために複数のデータ項目/タグをグループ化できます。

### AND を使用したネスト

AND グループ下のすべての項目およびグループを評価し、TRUE にします。

例：

```
<group type="and">
 <registry
 name="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
 Version\Uninstall\Mozilla Firefox (2.0.0.3)"/>
 <file name="firefox.exe" minversion="1.8.20070.30919"
 maxversion="1.8.20070.30919" path="*" />
</group>
```

### OR を使用したネスト

OR グループ下の少なくとも 1 つの項目またはグループを評価し、TRUE にします。

例：

```
<group type="or">
 <group type="and">
 <file name="sw3eng.exe" path="*" minversion="3.0.1.73"/>
 <file name="EngineApplet.exe" path="*"
 minversion="3.0.1.73"/>
 </group>
 <group type="and">
 <file name="LGClient.exe" path="*" minversion="3.0.1.73"/>
 <file name="LGWorkspace.exe" path="*" minversion="3.01.73"/>
 </group>
</group>
```

### NOT を使用したネスト

下位の項目またはグループが TRUE に評価されている場合、目的のグループを FALSE に評価します。

例：

```
<group type="and" >
<sysinfo osname="AIX" />
<file name="LDS-em-client.jar" minfilesize="183308"
maxfilesize="183308" path="*" />
<group type="not" >
<file name="LDS-descriptions.jar" path="*" />
</group>
</group>
```



## サンプル シグネチャ

カスタム シグネチャを作成するには、以下のサンプル シグネチャを参照します。

### ファイル バージョンの読み取り

```
Assignment Wizard Exe 1.0
<file name="ABTRep¥BIN¥assgnwiz.exe" path="*"
minversion="1.0" maxversion="1.0" />
```

### package name タグを使用した情報の読み取り

```
IBM Java 2 Runtime Environment v1.4.1 x86 32
<package name = "IBM 32-bit Runtime Environment for Java 2,
v1.4.1" />
```

### レジストリ キーの存在の確認

```
InCtrl5
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Current
Version¥Uninstall¥InCtrl5" />
```

### file name および package name 名タグを使用した AND 条件のある 1 つのグループ内のシグネチャ

```
Quest Software Toad for Oracle 10.6
<group type="and">
<package name = "Toad for Oracle 10.6" />
<file name="TOAD.exe" minversion="10.6" maxversion="10.6"
path="*" />
</group>
```

### package name および sysinfo osname タグを使用した 1 つの AND グループのあるシグネチャ

```
IBM Directory Client SDK 4.1 [AIX]
<group type="and">
<sysinfo osname="AIX" />
<package name="ldap.client.adt" version="4.1.0.0" />
</group>
```

### ファイル日付属性と共に file name タグを使用したシグネチャ

```
Project Bridge Modeler 4.03.21
```

```
<file name="ABTRep¥BIN¥Pbm.exe"
minmodified="1998-10-11T00:00:00Z"
maxmodified="1998-10-13T23:59:59Z" path="*" />
```

**registry name および package name タグを使用した 1 つの AND グループのあるシグネチャ**

```
FedEx Ship Manager API 8.50.002
<group type="and">
<package name="FedEx Ship Manager API" />
<registry name="HKEY_LOCAL_MACHINE¥SOFTWARE¥FedEx¥FedEx Ship
Manager API¥8.50.002" />
</group>
```

**registry name、file name( ファイル バージョンの読み取り )、および package name タグを使用した 1 つの AND グループのあるシグネチャ**

```
SAPIEN Technologies PrimalScript 2011
<group type="and">
<package name="PrimalScript 2011" version="6.0.*" />
<registry name="HKEY_LOCAL_MACHINE¥SOFTWARE¥SAPIEN
Technologies, Inc.¥PrimalScript¥2011¥" />
<file name="PrimalScript 2011¥PrimalScript.exe" path="*"
minversion="6.0" maxversion="6.0" />
</group>
```

**registry name、file name ( ファイルの存在の確認 )、および package name タグを使用した 1 つの AND グループのあるシグネチャ**

```
X1 Desktop Search Professional 6.7
<group type="and">
<package name="X1 Professional Client" version="6.7" />
<registry name="HKEY_LOCAL_MACHINE¥SOFTWARE¥X1 Desktop
Search" />
<file name="X1.exe" path="*" />
</group>
```

**sysinfo osname、file name ( ファイルの存在の確認 )、および package name タグを使用した 1 つの AND グループのあるシグネチャ**

```
RHEL4-iproute 2.6.9-4.el4 x86 32
<group type="and">
<sysinfo osname="Linux" />
<package name = "iproute" version="2.6.9" release="4.el4" />
<file name="/etc/redhat-release"/>
</group>
```

package name ( ワイルドカードを使用 )、registry name、および file name ( ファイルバージョンの読み取り/ファイルの存在の確認/ファイル コンテンツの読み取り ) を使用するネストされたグループ ( AND 内の OR および NOT 条件 ) のあるシグネチャ

```
IBM Lotus Notes Client 8.5.1
<group type="and">
<group type="or">
<package name = "Lotus Notes 8.5.1" version="8.51.*" />
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Lotus¥Notes¥Version"
match="080501" />
</group>
<file name="notes.exe" minversion="8.5.10"
maxversion="8.5.10" path="*" />
<group type="not">
<file name="notes.ini" match="FaultRecovery_Build=Release
8.5.1 FP1" path="*" />
</group>
</group>
```

registry name および file name ( パスの一部指定によるファイルの存在の確認/ファイル コンテンツの読み取り ) を使用した 1 つの AND グループのあるシグネチャ

```
IBM Lotus Workforce Management 6.1
<group type="and">
<registry name =
"HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersi
on¥Uninstall¥IBM Lotus Workforce Management" />
<file name="Web-App_6.1.0¥Packages¥lwm.builders.base.pkg"
path="*" />
<file name=".com.zerog.registry.xml" path="*"
match="Web-App_6.1.0¥¥Packages¥¥lwm.builders.checklist.pkg"
/>
</group>
```

sysinfo platform タグ、およびファイル サイズ属性と共に file name タグを使用した 1 つの AND グループのあるシグネチャ

```
Adobe Reader 7.0.9 PowerPC
<group type="and">
<sysinfo platform="Power Macintosh" />
<file name="MacOS/Adobe Reader" minfilesize="9140"
maxfilesize="9140" path="*" />
</group>
```

**package name タグ、およびファイル サイズ/ファイル日付属性と共に file name タグを使用した 1 つの AND グループのあるシグネチャ**

```
CA AllFusion Erwin Data Modeler r7
<group type="and">
<package name="CA AllFusion ERwin Data Modeler r7" />
<file name="ERwin.exe" minfilesize="3883008"
maxfilesize="3883008" path="*" />
<file name="ERwin.exe" minmodified="2007-05-21T00:00:00Z"
maxmodified="2007-05-21T23:59:59Z" path="*" />
</group>
```

**ワイルドカードを含む registry name および file name ( ファイル バージョンの読み取り ) を使用するネストされたグループ ( AND 内の 2 つの OR 条件 ) のあるシグネチャ**

```
Microsoft Office Project 2007 Standard Edition x86 32 EN
<group type="and">
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Office¥12.0¥Project" />
<group type="or">
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Current
Version¥Uninstall¥{90120000-00B4-0409-0000-00000000FF1CE}" />
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Current
Version¥Uninstall¥{91120000-00B4-0409-0000-00000000FF1CE}" />
</group>
<group type="or">
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Current
Version¥Uninstall¥{90120000-003A-0000-0000-00000000FF1CE}¥Di
splayVersion" match="12.0.4518.*" />
<registry
name="HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥Current
Version¥Uninstall¥{91120000-003A-0000-0000-00000000FF1CE}¥Di
splayVersion" match="12.0.4518.*" />
</group>
<file name="OFFICE12¥WINPROJ.EXE" minversion="12.0"
maxversion="12.0" path="*" />
</group>
```

# Intellisig

## Intellisig -- スクリプトによるソフトウェア検出

*Intellisig* は、エージェント コンピュータにインストールされたソフトウェアを検出するスクリプトです。 *Intellisig* は、ヒューリスティック スキャンおよびソフトウェア シグネチャ スキャンと比較して、ソフトウェアを検出する最も柔軟で正確な方法を提供します。 *Intellisig* は、ソフトウェア メーカーが提供する定義済みソースからソフトウェア定義情報を抽出します。 そのソースとして、テキストファイル、データベース、レジストリ、またはバイナリ ファイルを使用できます。たとえば、`dsmver -f<output file>` は、**Client Automation** に関するバージョン情報を出力するコマンドです。 製造元が、バージョン情報を製品に格納する方法を変更しない場合、*Intellisig* は、製品の今後のバージョンも検出できます。 ソフトウェア シグネチャ スキャンでは、製品、リリース、およびパッチのすべてのバージョンのシグネチャが必要ですが、単一の *Intellisig* は、複数のソフトウェア製品のリリースおよびパッチを検出できます。たとえば、過去と将来のバージョンを含めて、**Microsoft Office** 製品のすべてのバージョンを検出する *Intellisig* を作成できます。

注： *Intellisig* を使用して、さまざまなプラットフォーム上のソフトウェアを検出できます。

以下の *Intellisig* タイプを使用できます。

### CA Intellisig

CA が提供する *Intellisig* を含みます。 CA が提供するソフトウェア シグネチャと同様に、CA が提供する *Intellisig* は、コンテンツのダウンロードジョブの一部としてダウンロードされます。

### カスタム Intellisig

ユーザの要件に基づいて、作成された *Intellisig* を含みます。 これらの *Intellisig* を作成し、DSM エクスプローラを使用してインポートします。

注： *Intellisig* は、オフラインとオンラインの両方でソフトウェア使用状況（測定）をサポートしません。

DSM レポータは、*Intellisig* レポートをサポートしません。

## Intellisig -- 概要

従来のシグネチャは、リリースまたはパッチの一部である特定バージョンおよびサイズの特定のファイルのみ検索します。それは、検出対象のソフトウェアの変化に順応できない、固定されたルールです。必要なインテリジェンスと柔軟性を実現できるように、Intellisig はコードで実装されています。このインテリジェンスと柔軟性により、Intellisig は、単一のシグネチャで可能なよりも、さらに多くの項目を検出できます。たとえば、Microsoft Office 内に存在する可能性がある各項目に対してシグネチャが 1 つ対応するシグネチャの大きなセットとは対照的に、単一の Intellisig で、すべてのバージョンのすべての Microsoft Office 製品を検出できます。

dmscript は、Client Automation で提供される移植可能なスクリプト言語およびプロセッサです。dmscript 言語の機能が拡張され、標準的なシンプル フォーマットで出力できるようになりました。

Intellisig を書き込むには、以下のタスクを実行します。

1. ソフトウェア識別情報の分析
2. Intellisig のコード化。
3. Intellisig のテスト。
4. 実稼働使用のための Intellisig のリリース。

以下に、Intellisig の出力を示します。

- 多数の製品定義（たとえば Microsoft Windows）。製品を認識できるようにするために、MDB で製品を作成する必要はありません。Intellisig は、実行時に定義を作成します。この機能により、新製品を検出できます。
- 製品（たとえば Windows 7 Ultimate 32 ビット ENU）の多くのリリース定義。
- リリースに適用される多くのパッチ定義。これらの修正が発行され、インストールに適用されます。たとえば、「KB123456」と指定します。
- インストールされたリリースまたはパッチの 1 つ以上のインスタンス。

この出力が、DSM エクスプローラで [検出されたソフトウェア] および [ソフトウェア定義] ノード下に表示されます。

## Intellisig とは

Intellisig は、以下のコンポーネントで構成されています。

- dmscript で記述されたスクリプト
- データ、シェル スクリプトなどのオペレーティング システム依存スクリプト、または別の dmscripts が含まれる任意の数の補助ファイル
- Intellisig、名前、バージョン、タイムアウト、およびトリガを記述するメタデータ

これらのコンポーネントは MDB に格納され、スケーラビリティ サーバとエージェントに配信されます。Intellisig は、ソフトウェア スキャナによって起動される dmscript の制御下で実行されます。スキャナは、次に CA Asset Management エージェントによって起動されます。

スクリプトの出力は、<Intellisig-uuid>.xml と呼ばれる XML ファイルです。このファイルの形式は、ソフトウェア ID タグの ISO19970-2 標準に従います。これは、ソフトウェア製品が、それ自身に関する情報を格納する手段を提供する国際標準です。その後、この情報は Client Automation などの製品によって読み取られ、ソフトウェア スキャナによって標準 CA Asset Management インベントリ形式に変換されます。

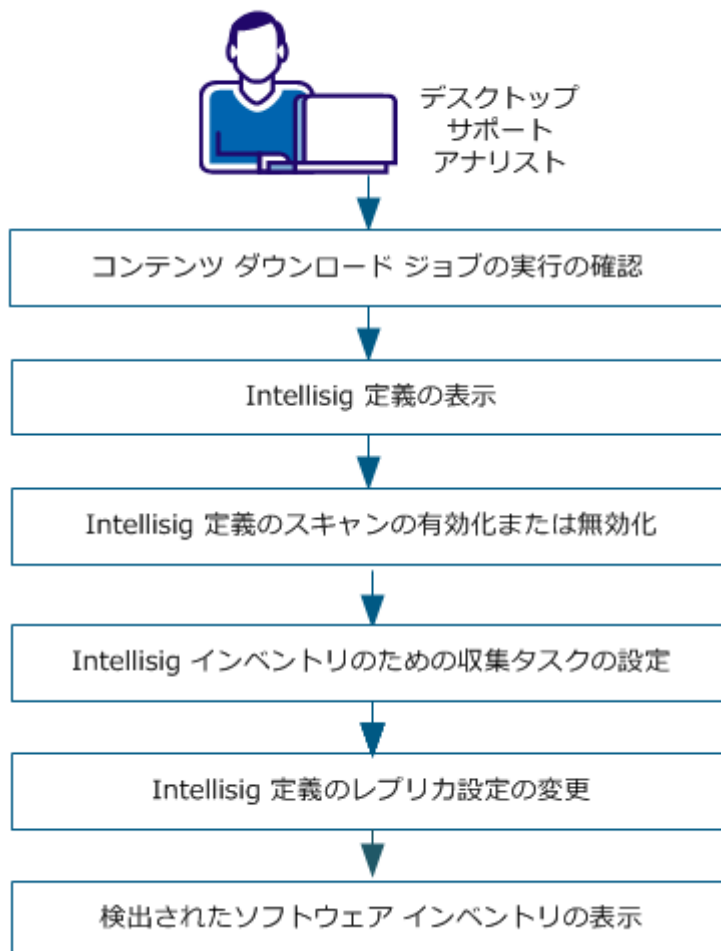
ドメイン マネージャは、ソフトウェア Intellisig の現在のセットをスケーラビリティ サーバに送信します。それは、次に、エージェントに送信されます。CA Asset Management エージェントは、実行時にソフトウェア収集タスクが設定されているかどうかを確認します。設定されている場合、ソフトウェア スキャナを開始し、次に利用可能な各 Intellisig を実行します。各 Intellisig について、利用可能なすべてのトリガを評価して、スクリプトを実行する必要があるかどうかを確認します。トリガが true の場合、dmscript が適切な引数で実行されます。完了すると、エージェントは、出力 XML ファイルを収集し、それをインベントリ形式に変換し、サーバにアップロードしてドメイン マネージャに返します。MDB に格納した後、DSM エクスプローラで結果を利用できます。従来のシグネチャ スキャンおよびヒューリスティック スキャンを実行するように設定されている場合、エージェントはその処理も実行します。

動作する Intellisig を参照するには、DSM エクスプローラを使用して、CA によって提供され、コンテンツ サーバからダウンロードされた標準 Intellisig のコンテンツを表示します。これらの Intellisig は、独自の Intellisig を開発するためのモデルとして使用できます。

## Intellisig を使用したソフトウェアの検出

デスクトップ サポート アナリストとして、ターゲット コンピュータ上のソフトウェアを検出して、ターゲット コンピュータ上にソフトウェアのインベントリをインストールできるようにします。

### Intellisig を使用したソフトウェアの検出





## コンテンツ ダウンロード ジョブの実行の確認

デフォルトのソフトウェア コンテンツ ダウンロード ジョブは、CA Web サイトから CA によって提供される Intellisig をダウンロードします。このリリースをインストールした後、少なくとも 1 回は、このジョブが実行されたことを確認します。ジョブが正しく完了すると、CA が提供する Intellisig が、ユーザのドメイン マネージャにダウンロードされることが確認されます。

以下の手順に従います。

1. [コントロール パネル] - [エンジン] - [すべてのエンジン] - [システム エンジン] フォルダに移動します。

右ペインに、エンジン ログとタスク リストが表示されます。

2. デフォルトのソフトウェア コンテンツ ダウンロード ジョブの [ステータス] に [OK] が表示されること、およびこのリリースをインストールした後の最終実行であることを確認します。

これらの条件のいずれかが false の場合、ジョブをただちに実行するか、またはジョブが次にスケジュールされた時間まで待機することができます。両方の条件が満たされる場合、ダウンロードされた Intellisig 定義を表示できます。

注：カスタム Intellisig を作成して使用する場合、「[カスタム Intellisig の作成](#) (P. 89)」を参照してください。

## Intellisig 定義の表示

Intellisig には、マスタ定義およびいくつかの検出された定義が含まれます。マスタ定義は、名前、作成詳細、ターゲット プラットフォーム、スクリプト詳細などの Intellisig 詳細を含む第 1 レベルのオブジェクトです。検出された定義には、Intellisig がターゲット コンピュータ上で検出した後にのみ作成される製品、リリース、およびパッチ定義が含まれます。Intellisig をダウンロードした後、マスタ Intellisig 定義およびそれらの詳細のみ表示できます。検出された定義は、Intellisig 収集タスクが、ターゲット コンピュータ上でソフトウェアを検出した後でのみ利用可能です。Intellisig 定義を表示するには、DSM エクスプローラで [ソフトウェア] - [定義] - [Intellisig] をクリックします。

## Intellisig 定義のスキヤンの有効化または無効化

デフォルトでは、ソフトウェア スキャンに対してすべての Intellisig が有効になっています。ソフトウェア スキャナがある Intellisig を一時的にスキャンしないようにする場合、その Intellisig のスキャンを無効にできます。スキャナが再度それを検出するようにする場合には、それらを後で有効にできます。

注：製品、リリース、またはパッチ定義レベルではなく Intellisig レベルでのみ無効にできます。

以下の手順に従います。

1. [ソフトウェア] - [定義] - [Intellisig] に移動します。

右側のペインにすべての Intellisig が表示されます。

2. 無効にする Intellisig を右クリックし、[スキヤンの無効化]を選択します。[はい] をクリックして、確認します。

収集タスクを次回実行するとき、無効化された Intellisig はエージェントに送信されません。収集タスクが実行された後、以前のスキヤンで検出されたレコードが存在する場合、それらのレコードは、[すべてのコンピュータ] - [コンピュータ名] - [ソフトウェア] - [検出] に表示されなくなります。ただし、検出された製品、リリース、またはパッチ定義は、[ソフトウェア] - [定義] - [Intellisig] から削除されません。

## ソフトウェア インベントリのための収集タスクの設定

Intellisig を使用してソフトウェア インベントリを収集するには、Intellisig スキャンを含むように収集タスクを設定する必要があります。

以下の手順に従います。

1. [すべてのコンピュータ] - グループ名またはコンピュータ名 - [設定] に移動します。

注：グループ レベルで設定された収集タスクは、グループ内のすべてのコンピュータに適用可能です。

2. [収集タスク] を右クリックし、[新規] を選択します。
3. [新しい収集タスク タイプの選択] ダイアログ ボックスで [ソフトウェアの検出] を選択し、[OK] をクリックします。
4. 収集タスクの名前を指定し、[方法] タブをクリックします。
5. [方法] に [シグネチャのスキャン] を選択し、[スキャナの設定] をクリックします。
6. [Intellisig スキャン] を選択して [OK] をクリックします。

注：同じ収集タスクの一部として、シグネチャのスキャンと Intellisig スキャンの両方を選択できます。いくつかの定義がシグネチャであり、いくつかは Intellisig の場合、そのような選択を適用できます。同じソフトウェアが両方のスキャナで検出された場合、そのソフトウェアは、検出されたソフトウェア リストに 2 回一覧表示されます。ただし、リストには、ソフトウェアがシグネチャ スキャンと Intellisig スキャンのどちらで収集されたかを指定する検出ソースが提供されます。

収集タスクが設定されます。収集タスクを次回実行するときに、エージェントは、Intellisig スクリプトを実行して Intellisig インベントリを収集します。

**重要：** CA Patch Manager では、シグネチャ スキャンを有効にする必要があります。CA Patch Manager を使用してターゲット コンピュータにセキュリティ パッチを適用している場合、ターゲット コンピュータに対してもシグネチャ スキャンを設定したことを確認してください。Intellisig のみ設定すると、パッチ管理が正しく動作しなくなります。

## 検出されたソフトウェアの表示

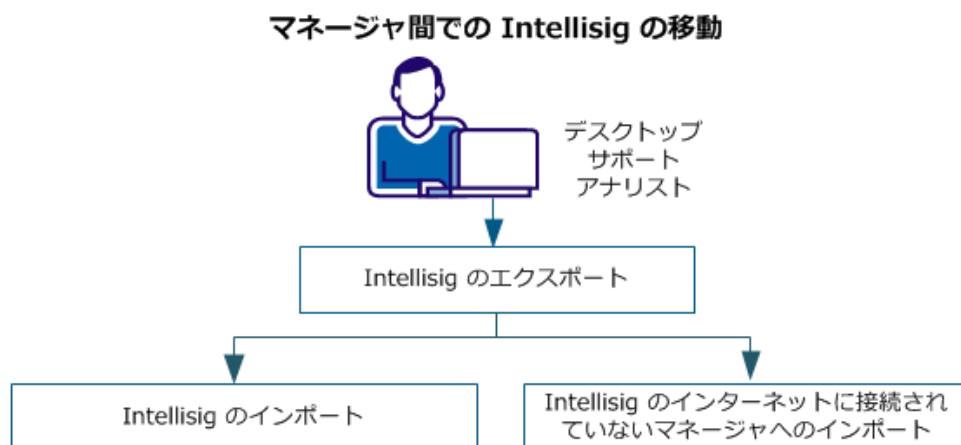
検出されたソフトウェアを表示して、エージェント コンピュータ上で Intellisig によって検出されたソフトウェアを確認できます。検出された Intellisig は、DSM エクスプローラ内の以下の場所から利用できます。

- [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 - [ソフトウェア] - [検出]
- [ソフトウェア] - [定義] - [Intellisig] - *Intellisig 名-検出された製品- 検出されたリリース* - [検出されたインストール]
- [ソフトウェア] - [定義] - [Intellisig] - *Intellisig 名-検出された製品-検出されたリリース- 検出されたパッチ* - [検出されたインストール]
- [ソフトウェア] - [定義] - [カテゴリ] - *検出された製品- 検出されたリリース* - [検出されたインストール]
- [ソフトウェア] - [定義] - [カテゴリ] - *検出された製品- 検出されたリリース- 検出されたパッチ* - [検出されたインストール]
- [ソフトウェア] - [定義] - [製造元] - *検出された製品- 検出されたリリース* - [検出されたインストール]
- [ソフトウェア] - [定義] - [製造元] - *検出された製品- 検出されたリリース- 検出されたパッチ* - [検出されたインストール]

注：ソフトウェア定義、カテゴリ、および製造の詳細については、DSM エクスプローラのオンラインヘルプを参照してください。

## マネージャ間での Intellisig の移動

デスクトップ サポート アナリストとして、マネージャ間で Intellisig を移動して、各マネージャが手動で作成する必要があるようにすることができます。ソース マネージャから Intellisig をエクスポートして、ターゲット マネージャにインポートできます。



## Intellisig のエクスポート

Intellisig をエクスポートして Intellisig を変更するか、またはドメイン マネージャからエンタープライズ マネージャ、または別のドメイン マネージャに移動します。すべての Intellisig、特定の Intellisig、または Intellisig の特定バージョンをエクスポートできます。また、Intellisig のエクスポートに CLI を使用できます。CLI の詳細については、「[intelligcmd export -- Intellisig のエクスポート \(P. 138\)](#)」を参照してください。

**注：** 製品、リリース、またはパッチ定義レベルではなく、Intellisig レベルでのみエクスポートできます。

次の手順に従ってください：

1. [ソフトウェア] - [定義] に移動し、すべての Intellisig、特定の Intellisig、または Intellisig の特定バージョンをエクスポートするかどうかに応じて、以下のいずれかを実行します。

### すべての Intellisig

- [Intellisig] ノードを右クリックして、[プロパティ] を選択します。

### 特定の Intellisig

- [Intellisig] ノードをクリックして、右ペインでエクスポートする Intellisig を選択します。選択対象を右クリックし、[更新] を選択します。

### Intellisig の特定バージョン

- [Intellisig] ノードをクリックし、Intellisig を右クリックして、[プロパティ] を選択します。[バージョン] タブをクリックし、エクスポートするバージョンを選択して、[Intellisig プロパティ] ダイアログ ボックスで [エクスポート] をクリックします。

[Intellisig エクスポート] ダイアログ ボックスに、選択した Intellisig が一覧表示されます。

2. Intellisig を圧縮ファイルとしてエクスポートするか、または圧縮されていないフォルダとしてエクスポートするかを指定し、必要な場合には [参照] をクリックして場所を変更します。

**注：** Intellisig の変更中は圧縮されていない形式、管理者間での Intellisig の移動時には圧縮形式の使用をお勧めします。

3. [OK] をクリックします。

選択された Intellisig は、指定した場所にエクスポートされ配置されます。

関連項目：

[カスタム Intellisig の変更 \(P. 121\)](#)

[マネージャ間での Intellisig の移動 \(P. 85\)](#)

## Intellisig のインポート

Intellisig をインポートして、変更後に Intellisig を更新するか、また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、または別のドメイン マネージャに移動します。また、Intellisig のエクスポートに CLI を使用できます。CLI の詳細については、「[intellisigcmd import -- Intellisig のインポート \(P. 139\)](#)」を参照してください。

次の手順に従ってください：

1. [ソフトウェア] - [定義] に移動し、[Intellisig] ノードを右クリックして [インポート] を選択します。  
[Intellisig インポート] ダイアログ ボックスが開きます。
2. [参照] をクリックし、インポートする Intellisig の ZIP ファイルまたは XML ファイルを選択します。
3. [インポート モード] を選択して、既存の定義を置換するか、新しい変更のみマージするか、またはすべての変更をマージするかを指定します。
4. (オプション) アクティブな Intellisig バージョンを変更しない場合は、[インポート中にアクティブな Intellisig バージョンを更新する] オプション中をクリアします。[OK] をクリックします。  
リストア処理が開始します。

注：（Intellisig のみのエクスポート ZIP オプションから）対応する ZIP によって ZIP 形式で Intellisig をエクスポートする必要があります。任意のサードパーティ圧縮（ZIP）ユーティリティを使用しないでください。

## インターネットに接続されないマネージャへの Intellisig のインポート

CA コンテンツ サーバから Intellisig をダウンロードする場所で、インターネットに接続されているマネージャが 1 台存在する場合、インターネットに接続されていないマネージャにも Intellisig をインポートできます。

詳細については、Intellisig 機能の「[コンテンツ ユーティリティ \(P. 148\)](#)」を参照してください。

次の手順に従ってください：

1. コマンドライン ツール contentutility.exe を実行します。

注：.xml パラメータ ファイルを提供するか、またはコマンドライン上で直接パラメータを指定することによってツールを実行できます。パラメータなしでツールを実行すると、CA¥DSM¥bin ディレクトリ内に content\_utility.xml という名前の XML ファイルが作成されます。CA 提供のパラメータ、カスタム作成パラメータ、ca\_intellisig パラメータ、および custom\_intellisig パラメータの組み合わせを指定することにより、どのソフトウェア定義をエクスポートまたはインポートするか判断できます。

2. 以下のパラメータに値を指定します。

### ca\_intellisig

エクスポートまたはインポートに CA 定義の Intellisig を含めるかどうかを指定します。

### custom\_intellisig

エクスポートまたはインポートにカスタム定義の Intellisig を含めるかどうかを指定します。

### intellisig\_detail

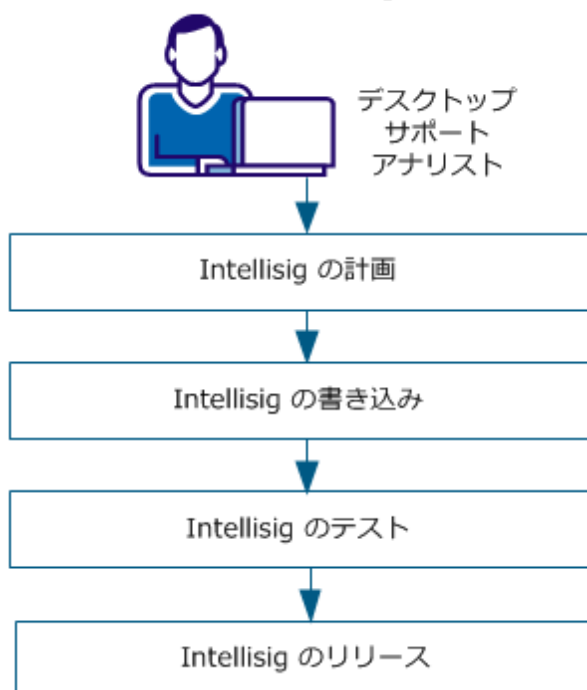
エクスポートまたはインポート中に Intellisig と関連付けられるスクリプトおよびトリガを含めるかどうかを指定します。[いいえ]に設定すると、マスタ定義はエクスポートまたはインポートされますが、詳細は省略されます。



## カスタム Intellisig の作成

CA が提供する Intellisig が利用できない任意のソフトウェアに対して、開発者は、カスタム Intellisig を作成できます。

### カスタム Intellisig の作成



## 独自の Intellisig の計画

### Intellisig の設計に関する考慮事項

- Intellisig は、現在および将来の製品リリースを検出するためのメカニズムを提供します。スクリプトの作者は、記述したスクリプトが将来の使用に耐えられる方法でシステムを検査するよう注意する必要があります。
- Intellisig 定義の数を少なくして、各定義で複数の製品を網羅することをお勧めします。各ベンダーに対して 1 つの Intellisig を作成すること、また大きなベンダーに対しては、ベンダーごとおよびソフトウェア カテゴリごとに Intellisig を作成することをお勧めします。例：IBM - Database Software、Microsoft - Database Software、Microsoft - Office Software、Apache - Office Software、および CA - Management Software。操作性の観点から、すべての Intellisig に対してカテゴリ名が同期していることを確認します。
- Intellisig にはメイン スクリプトが含まれています。また、それ自身がスクリプトであるファイルを含めて、多数のデータ ファイルを含むことができます。データ ファイルを製品検出のためのスクリプト として使用することにより、ベンダーまたはカテゴリ レベルで設計をクリーンかつ動作可能に保つことができます。ベンダーに固有のメイン スクリプトは、その他のすべての(データ) スクリプトを呼び出します。これらのスクリプトは、次に個別の製品を検出します。Intellisig の機能を拡張するには、新しい完全な Intellisig を追加するのではなく、ベンダーに固有の Intellisig バージョンを作成して、新しいスクリプトまたは更新済みの既存スクリプトを追加します。バージョンは、単一の Intellisig 内に埋め込まれたチェーンです。したがって、ユーザインターフェースに影響しません。トップレベルの Intellisig のリストを、可能な限り短く維持します。

- ヒューリスティックに検出されるか、または従来のシグネチャを使用して検出されるソフトウェアは、ソフトウェア製品とリリースの間に 1 対 1 の関係を使用します。Intellisig では、検出される製品とリリースの両方を作成するため、この動作を制御できます。ベストプラクティスは、以下の 3 つの理由で、検出される製品とリリースの間に 1 対多数の関係を作成することです。
  1. 製品は、複数のリリースを持つことができます。
  2. 1 対 1 の関係を使用するとき必要なデータの量は、1 対多数の場合と比較して大きくなります。
  3. 最も重要なことには、CA DSM が、検出情報を CA Software Compliance Manager (SCM) に提供することです。SCM は、リリースではなく DSM 製品に対処します。これを考慮に入れて、どのようにライセンスされるかに基づいて検出される製品を作成します。この方法では、SCM ライセンス対象製品が単一の DSM 検出製品に一致することを確認できます。さらに、リリース（およびパッチ）レベルで詳細な検出を行い、製品レベルで意味のある検出を達成することができます。
- Intellisig で作成された製品、リリースおよびパッチ（検出されるソフトウェア定義）は、名前とバージョン ラベルだけでなく、Intellisig の検出階層内の位置によって識別されます。空のバージョン ラベルが許可されており、個別のバージョン（空のバージョン）として扱われます。Intellisig に検出されたソフトウェア定義は、同じ名前とバージョンを持つ場合であっても、CA が提供したソフトウェア定義、カスタム ソフトウェア定義、およびヒューリスティック ソフトウェア定義とは個別のものです。さらに、別の Intellisig は、同じ名前とバージョンで別の定義を作成できます。
- DMscript 機能を使用し、各々に対してソフトウェア名とバージョンを指定します。
- 検出された定義を作成するとき、製造元を指定できます。この情報は、UUID または名前によって提供できます。製造元 UUID は、既存の製造元のものである必要があります。存在しない場合、検出された定義の製造元が空になります。製造元名は、既存の製造元または新しい製造元のいずれかにすることができます。後者については、製造元が作成され、検出された定義が割り当てられます。既存の製造元は、CA から提供されたもの、カスタム作成されたもの、またはヒューリスティック ソフトウェア ディスカバリによって作成されたものの、いずれかにすることができます。
- 検出された定義も、カテゴリに割り当てることができます。この情報は、UUID または名前によって提供できます。UUID によって提供される場合、カテゴリが存在する必要があります。名前によって提供される場合、カテゴリは、存在しない場合には作成されます。既存のカテゴリは、CA 提供、またはカスタム作成にすることができます。

以下に、Microsoft Windows、Microsoft Office および Microsoft SQL Server の 3 つの異なる製品を使用して、Intellisig 動作のベスト プラクティスを示します。

## 製品のネーミング

製品がライセンス可能なエンティティを反映していることを確認します。ネーミングのためのベストプラクティスは、以下のとおり（角かっこ内のオプション）です。

- **Name:** "<Manufacturer> <Product> [<Edition>] [<Architecture>] [<Language>]" - 該当する場合は、エディションを追加します。ライセンスがアーキテクチャまたは言語に依存する場合は、名前にそれを含めます。作成する製品の数をも最小にするため、必要な場合にのみこの情報を含めることを確認します。
- **Version Label:** "<major>[.<minor>]" - バージョンと別のバージョンを区別します

### 例：

- **Name:** "Microsoft Windows 7 Ultimate"  
**Version Label:** "6.1"  
メジャーバージョンとマイナーバージョンの両方を使用して、**Windows Vista**（6.0）と **Windows 8**（6.2）を区別します。必要な場合には、名前から **7** を削除します。
- **Name:** "Microsoft Office 2010 Professional Plus"  
**Version Label:** "14"  
**Office** の 2 つのリリースが区別されるため、メジャーバージョンのみを使用します。必要な場合には、名前から **2010** を削除します。
- **Name:** "Microsoft SQL Server 2008 R2 Enterprise"  
**Version Label:** "10.5"  
メジャーバージョンとマイナーバージョンの両方を使用して、あるバージョンを別のバージョンと区別します。必要な場合には、名前から **2008 R2** を削除します。

利用可能な場合には、データベース内の専用列に挿入される次のオプションのプロパティを指定します：**VersionNumber**、**Language**、**Bitness**、**Architecture**、**Manufacturer**、**Category** および **Description**。

## リリースのネーミング

リリースが、検出されたソフトウェアに関する情報を可能な限りキャプチャすること、およびそれが製品にリンクされることを確認します。ネーミングのためのベストプラクティスは、以下のとおり（角かっこ内のオプション）です。

- 名前 : "<Manufacturer> <Product>[ <Edition>] [<Architecture>] [<Language>]"
- バージョン ラベル : "<major>.<minor>.<minor'>.<minor'>" [<release/service pack>]" – 可能な限り多くの詳細を含めます。Architecture と Language にはそれぞれ個別のリリース レコードがありますが、すべて同じ製品にリンクされます。

### 例 :

- Name: "Microsoft Windows 7 Ultimate x64 en-us"  
Version Label: "6.1.7601 Service Pack 1 Build 7601"
- Name: "Microsoft Office 2010 Professional Plus x64 en-us"  
Version Label: "14.0.6112.5000 Service Pack 1"
- Name: "Microsoft SQL Server 2008 R2 Enterprise x64 en-us"  
Version Label: "10.50.1617.0 Service Pack 1"

利用可能な場合には、データベース内の専用列に挿入される次のオプションのプロパティを指定します : VersionNumber、Language、Bitness、Architecture、Manufacturer、Category および Description。

## リリースのインスタンのネーミング

リリース インスタンスは、リリースをソフトウェア インベントリのコンピュータ およびフォームの部分にリンクする実際の検出レコードです。コンピュータには、同じリリースの複数インスタンスをインストールできます。インストールには、インスタンスに固有の追加のプロパティを指定できます。

**例：**

- Microsoft Windows 7 Ultimate インスタンス :  
InstallPath: C:\Windows  
Origin=Forward Inc  
TrustLevel=5
- Microsoft Office 2010 Professional Plus インスタンス :  
InstallPath: C:\Program Files\Office  
ProductGUID: FBD367D1-642F-47CF-B79B-9BE48FB34007  
CustomData: Product-ID=02257-210-8656854-49625  
Origin=Forward Inc  
TrustLevel=5
- Microsoft SQL Server 2008 R2 Enterprise インスタンス 1 :  
InstallPath: C:\Program Files\Microsoft SQL Server\MSSQL10\_50.MSSQLSERVER  
Label: MSSQLSERVER  
CustomData: CPU=2/8/16;RAM=32GB;  
Origin=Forward Inc  
TrustLevel=5
- Microsoft SQL Server 2008 R2 Enterprise インスタンス 2 :  
InstallPath: C:\Program Files\Microsoft SQL Server\MSSQL10\_50.SQLEXPRESS  
Label: EXPRESS  
CustomData: CPU=2/8/16;RAM=32GB;  
Origin=Forward Inc  
TrustLevel=5

利用可能な場合には、データベース内の専用列に挿入される次のオプションのプロパティを指定します: Label、InstallPath、SerialNumber、ProductGUID、LastAccessed、Origin、TrustLevel、および CustomData。

CustomData プロパティは、ライセンスに影響するインスタンス固有の情報を収集するために使用されます。そのサイズは 255 文字に制限されています。このプロパティは、プロセッサ、コア、またはスレッドの数、およびメモリに関する情報を保持できます。収集されたカスタム データは、Client Automation では使用されませんが、現場で開発されたソリューションで使用できます。

## パッチのネーミング

パッチが、検出されたソフトウェアに関する情報を可能な限りキャプチャすること、およびそれがリリースにリンクされることを確認します。Intellisig を使用して検出されるパッチは、DSM Patch Manager では使用されません。

### 例：

Name: "KB971033 x64 en-us"  
Version label: ""

利用可能な場合には、データベースで専用列に挿入される以下のオプションのプロパティを指定します。

- VersionNumber Language
- Bitness
- Architecture
- Manufacturer
- Category および
- Description

## パッチのインスタンスのネーミング

パッチ インスタンスは、パッチをソフトウェア インベントリのコンピュータおよびフォームの部分にリンクする実際の検出レコードです。コンピュータには、同じリリースの複数インスタンスをインストールできます。それらの各リリース インスタンスには、パッチをインストールすることも、しないことも可能です。したがって、各リリース インスタンスに 1 つのパッチ インスタンスを作成します。パッチには、インスタンスに固有の追加のプロパティを指定できます。

利用可能な場合には、データベース内の専用列に挿入される次のオプションのプロパティを指定します: Label、InstallPath、SerialNumber、ProductGUID、LastAccessed、Origin、TrustLevel、および CustomData。

### 例：

KB971033 x64 en-us instance:

Origin=Forward Inc  
TrustLevel=5

## Intellisig およびフォルダ構造の例

2 つの Intellisig のサンプルが、*DSM path¥Intellisigs* フォルダに提供されています。

- Windows の場合：00000000-A0A0-AAAA-0000-AAAA0000AAAA
- UNIX の場合：00000000-B0B0-BBBB-0000-BBBB0000BBBB

Sample.xml には、ユーザの MDB にこれらのサンプルをインポートするためのメタデータが含まれます。Intellisig ディレクトリで、以下のコマンドを実行します。

```
intellisigcmd import file=sample.xml
```

サンプル Intellisig は、それぞれ以下のフォルダ構造を持ちます。

```
uuid of intellisig¥version id¥scriptfile.dms
```

注：同じ場所に、任意の追加の Intellisig データ ファイルを配置します。

## ソフトウェア識別情報の分析

従来のシグネチャの場合と同様に、スクリプトとその出力を反映するため、製品構成を決定します。以下を決定します。

- 製品のネーミング。たとえば **Microsoft Office**
- 製品のリリースがどのように構造化され、ネーミングされるかを決定します。
  - 32 ビットと 64 ビットリリースが存在するかどうかを確認します。
  - 複数の言語が存在するかどうかを確認します。
  - たとえば Windows 用の Office や Mac 用の Office など、異なるプラットフォーム用に異なるリリースが存在するかどうかを確認します。
- パッチが個別のバイナリか、または OS に登録されたインストール可能なパッケージかどうかを確認します。
- 必要な情報を提供するために、読み取り可能な ISO19770-2 SWID ファイルが、製品によって提供されるかどうかを確認します。



製品構成と命名規則を決定した後に、Intellisig の精度を決めます。これは、製品を網羅するのに必要な個別の Intellisig 数を決定することを意味します。たとえば Microsoft Office など、製品が大きい場合があります。各製品を検出するのに必要なスクリプトが大きい場合は、1つのサブ製品に対して複数のスクリプトを計画します。これらのスクリプトは、すべてのタスクを実行する大規模なスクリプトよりも保守が簡単です。たとえば 7-Zip など、製品が小さい場合には単一のスクリプトで十分です。

最後に、検出方法を決定します。Intellisig は、何がインストールされているか検出するために、システム上のリソースを検査する必要があります。これは、特定のファイル、レジストリ キー、設定ファイル、および設定を検索することを意味します。Intellisig は、必要に応じてインテリジェントになることができます。1つのレベルで、従来のシグネチャをエミュレートすること、および特定の情報を検索することができます。別のレベルでは、Intellisig が製品を認識していない場合であっても、コンピュータを分析して、すべての製造元から可能性のあるすべての製品を検出できます（ヒューリスティック スキャンに類似）。Intellisig は、これらの 2つのレベル間で動作できることが理想的です。少なくとも、過去と将来を含めて、製品のすべてのバージョンおよび構成を検出できることを確認します（特定の既存のバージョンではなく）。

## ユーザの Intellisig の書き込み

カスタム Intellisig は、メタデータ ファイルおよびスクリプトを必要とします。ファイルは、特定のフォルダ構造に存在する必要があります。サンプル Intellisig スクリプトおよびフォルダ構造については、「[Intellisig およびフォルダ構造の例 \(P. 96\)](#)」を参照してください。

## メタデータ ファイルの書き込み

メタデータ ファイルは、Intellisig に関する情報を含む .xml ファイルです。ドメイン マネージャおよびソフトウェア スキャン エージェントは、このファイルを使用して 1 単位としてそれを管理します。また、このファイルには、トリガの定義が含まれます。エージェントは、これらのルールを評価して、エージェントのランタイムを最小化するためにスクリプトを実行するかどうかを決定します。

**例：**

```
<eso_fingerprints version="1.0.0">
 <preferences>
 <ignore dllcache="true" />
 <ignore spuninstall="true" />
 <ignore internetcache="true" />
 <ignore cookies="true" />
 <ignore nortontrash="true" />
 <ignore sysbackup="true" />
 <ignore SDLib="true" />
 </preferences>
 <technologies dateupdateint="1320340565" dateupdate="05/12/11 11:28:05" >
 <technology id="11111111-B1B1-BBBB-1111-BBBB11110000"
 name="Trigger Test Unix Single File And" version="1.0.0"
 descr="Intellisig only run if file trigger detected
(trigger_file.txt)"
 swtype="17" srctype="6" iscript="intellisig-trigger-test.dms"
os="Unix">
 <additional_files>
 <data name="Trigger_Test_Unix.txt"/>
 <data name="Trigger_Test2_Unix.txt"/>
 </additional_files>
 <group type="and">
 <file name="trigger_file.txt" path="*" />
 </group>

 </technology>
 </technologies>
</eso_fingerprints>
```

**ID**

Intellisig の UUID を指定します。この ID は、Intellisig コマンドライン ツール (intellisigcmd.exe genuuid) を使用して生成できます。

**iscript**

Intellisig スクリプト ファイルの名前を指定します。

**Additional\_files**

スクリプトが必要とするオプションのファイルのリストを指定します。

**Group**

オプションのトリガを定義します。

## スクリプトの記述

Intellisig スクリプトを記述するためには、`dmscript` を使用してプログラムを記述する方法を基本的に理解していることが前提条件となります。

注： `dmscript` 言語の詳細については、*ITCM\_DMSScriptingLanguage\_Ref\_ENU.pdf* を参照してください。

Intellisig スクリプトは以下タスクを実行します。

- 引数を初期化し、収集し、確認。
- 出力ファイルを作成。
- 意図されている製品、リリース、パッチを検索し、インスタンスをインストールし、各々に関する必要な情報項目を収集。
- 適切な `dmscript` 機能呼び出し、この情報を出力ファイルに正しい順序でコピー。
- すべてのエラーを報告
- クリーンアップと終了

Windows では、`dmsedit` ユーティリティを使用してスクリプトを開発できます。このユーティリティは、スクリプトを開発し実行するための統合エディタおよびデバッガです。この方法により、ブレークポイント、コードのステップ実行、変数の検査など、すべての標準デバッグ機能が提供されます。

**重要：** スクリプトは対話式ではないので、Windows 上で印刷ステートメントを使用しないでください。Windows では、結果は、スクロール不可能なダイアログ ボックスに 10 秒間のみ表示されます。UNIX では、出力は `stdout` です。

スクリプトの開発には、テキストエディタとコマンドライン ウィンドウを使用します。 `dmstrace` 機能を使用して、トレース ログに診断情報を出力できます。

## 複数の製品を検出するスクリプトの記述

`dmscript` 言語は、機能を実行するスクリプトを組み込む `#include` ディレクティブをサポートします。 **Intellisig** を作成するためのベスト プラクティスに従って、以下の方法でスクリプトを記述することを推奨します。

1. 検出する各製品に対するスクリプトを記述し、各スクリプトを補助ファイルとして **Intellisig** 定義に追加します。これらのスクリプトは、検出を実行し、また検出された製品、リリース、パッチ、および検出されたインスタンスの登録を実行します。これらのスクリプトが **Intellisig** の初期化または終了コードを実行しないことを確認します。
2. **Intellisig** の開始と終了を実行するメイン スクリプトを記述して、**Intellisig** 定義に追加します。メイン スクリプトで `#include` ディレクティブを使用して補助ファイルをインクルードし、記述されている検出機能をメイン スクリプトの実行の一部として実行します。

### 例：

補助ファイル `windows.dms` は、関数 `DetectWindows(...)` を定義します。

補助ファイル `office.dms` は、関数 `DetectOffice(...)` を定義します。

補助ファイル `sql.dms` は、関数 `DetectSql(...)` を定義します。

メイン スクリプト `main.dms` は、以下のように表示されます。

```
#include windows.dms
#include office.dms
#include sql.dms
```

`DoInitialization(...)`

`args` の解析と `OpenDetectedSoftwareOutputFiles` の呼び出しを実行し、別の初期化タスクを実行する、`main.dms` に定義されている `REM` 関数を指定します。

`DetectWindows(...)`

`windows.dms` に定義されている `REM` 関数を指定します。

`DetectOffice(...)`

`office.dms` に定義されている `REM` 関数を指定します。

`DetectSql(...)`

`sql.dms` に定義されている `REM` 関数を指定します。

`DoFinalization(...)`

`CloseDetectedSoftwareOutputFiles` の呼び出しを実行し、別のクリーンアップタスクを実行する、`main.dms` に定義されている `REM` 関数を指定します。

## カスタム Intellisig のヘルプの記述

作成する Intellisig のヘルプを記述し、個別の Web ページに詳細を追加できます。詳細なヘルプにより、Intellisig ユーザは、Intellisig をさらに深く理解できます。ヘルプは、DSM エクスプローラ内の Intellisig プロパティ ページに表示されます。

次の手順に従ってください：

1. CA が提供する Intellisig の 1 つに関するヘルプ ファイルを表示します。
  - a. DSM エクスプローラを開き、[ソフトウェア] - [定義] に移動します。
  - b. CA が提供する Intellisig を右クリックし、[プロパティ] をクリックします。
  - c. [Intellisig プロパティ] ダイアログ ボックスで [詳細] タブをクリックします。
  - d. [?] ボタンをクリックします。

Web ページに、Intellisig に関する追加情報が表示されます。

2. CA が提供する Intellisig に基づいて、カスタム Intellisig の .html ヘルプ ファイルを作成します。
3. ファイル名として Intellisig 名を持つヘルプ ファイルを保存します。
4. Web サーバ上でヘルプ ファイルをホストします。

ヘルプ ファイルをホストした後、デフォルト設定ポリシー内に URL を設定します。
5. [コントロール パネル] - [設定] - [設定ポリシー] に移動します。デフォルト ポリシーを封印解除します。
6. [DSM] - [管理コンソール] に移動します。
7. [customIntellisigsURL] パラメータをダブルクリックし、[プロパティの設定] ダイアログ ボックスで値に「c:¥webinfo¥%name%.html」を指定します。

ヘルプ ファイルは、HTML ファイル名、および設定した URL に基づいて対応する Intellisig と関連付けられます。Intellisig のテスト時にヘルプもテストできます。

注：caIntellisigsURL パラメータは、CA が提供する Intellisig に関するヘルプ ファイルの詳細を指定します。

8. カスタム Intellisig に対して手順 1 を繰り返し、対応するヘルプ ファイルを表示します。

## 初期化

スキャナは、以下の引数で、スクリプトファイルと同じディレクトリ内の `dmscript` を起動します。

```
dmscript <scriptfile> -I <uuid of Intellisig> -v <version of Intellisig> -n <name of Intellisig> -t <trigger_info>
```

`trigger_info`

Intellisig を実行するトリガに関する情報を含むオプションの文字列を指定します。必要な場合、スクリプトは、その検出プロセスでヒントとしてこの文字列を使用できます。

スクリプトは、これらの引数を収集して存在することを確認し、欠落している場合には、エラーを報告して終了します。引数の値は `argv` 関数から使用可能です。

例：

```
dim sUuid as string
dim sISVersion as String
dim sISName as String
dim X as Integer
for X=0 to argc()
 if (argv(X)="-i") then
 sUuid = argv(X+1)
 endif
 if (argv(X)="-v") then
 sISVersion=argv(X+1)
 endif
 if (argv(X)="-n") then
 sISName = argv(X+1)
 endif
next X
if sUuid = "" then
 LogDetectedSoftwareError ("00404","Param1=missing argument uuid to script ")
 exit
endif
```

## トレースとレポートのエラー

`dmscript` は、ログ ファイル `TRC_DMSCRIPTINTERPRETER_0.log` にトレース情報を出力する手段を提供します。ログ ファイルは、Intellisig の開発中のデバッグとリリース後のトラブルシューティングに役立ちます。

`LogDetectedSoftwareError` 関数を使用して、管理者にエラーをレポートします。この関数は、`<uuid>.err` という名前のファイルに、標準形式でエラーを書き込みます。このファイルは、ドメインマネージャに自動的にアップロードされます。エラーもトレース ログ ファイルにコピーされます。DSM エクスプローラは、メッセージをローカル言語に変換した後、ジョブ ステータス ダイアログ ボックスに表示します。

**注：** この機能に従うと、英語テキストを直接指定することになりますが、ローカライズされたエラー メッセージを使用してください。必要な場合には、マネージャまたはエクスプローラ上で `statmod.<lang>` ファイルを編集して、自分のメッセージを追加します。

## 出力ファイルの作成

`OpenDetectedSoftwareOutputFiles` 関数を使用して、出力ファイルを開きます。

**例：**

```
if OpenDetectedSoftwareOutputFiles (sUuid,sISVersion,sISName) <> CASWDETECT_OK then
 exit
endif
```

この関数は、`<uuid>.xml` という名前のファイルを作成して結果を格納します。

## アイテムの検索

項目の検索は、製品の詳細に左右されます。以下の関数を使用できます。



## ファイルとディレクトリの検出

ファイルが存在するかどうか検出するには、**ExistFile** 関数を使用します。ディレクトリを検出するには、**ExistDirectory** 関数を使用します。

例：

```
ProgramFiles = EnvGetString("ProgramFiles")
if ExistDirectory (ProgramFiles + "¥Microsoft Office") then
...found MS Office...
if ExistFile (ProgramFiles + "¥Microsoft Office¥Office14¥EXCEL.EXE") then
... found excel...
```

## レジストリの読み取り

以下の関数を使用します。

**RegOpenKey**

レジストリを読み取ります

**RegQueryValue**

値を読み取ります

**RegEnumKeys**

キーを列挙します

**RegEnumVariable**

変数を列挙します

**RegCloseKey**

キーを閉じます

注：dmscript は 32 ビットのプログラムです。したがって、Windows は、**HKLM¥SOFTWARE** などの特定キーにレジストリのリダイレクトを適用します。64 ビットプログラム用に予約されたレジストリの一部を読み取るには、**setmode64(1)** を呼び出します。このアクションにより、リダイレクトがオフになります。また、この関数は、**¥windows¥system32** など、ファイルシステムの特定部分に適用されます。

## 環境を読み取り

Windows または UNIX 上の環境変数の内容を読み取るには、`EnvGetString` 関数を使用します。

例：

```
path = EnvGetString("PATH")
...now search the path for a target directory..
```

また、`EnvGetFirst` 関数と `EnvGetNext` 関数を使用して、環境変数をすべて列挙できます。

## 設定ファイルの読み取り

以下の関数を使用します。

- `.ini` スタイル ファイルを読み取るには、`ReadIniEntry` 関数を使用します。
- プレーン テキスト ファイルを読み取るには、`OpenFile` 関数を使用して開き、`ReadFile` 関数を使用して読み取ります。新しい `GetToken` 関数を使用して、テキスト行を解析できます。
- XML ファイルまたはバイナリ ファイルを読み取るには、カスタム DLL または外部プログラムを記述してスクリプトから呼び出します。`OpenFile` 関数を使用して、プログラムの出力を読み取ることができます。

注：カスタム バイナリは、Intellisig 定義に含めることができません。

## プログラムの実行

`dmscript` は、いくつかのタスクを実行できない場合があります。また、タスクによっては、既存のシェル スクリプトや外部プログラムを実行する方が単純な場合があります。そのような場合には、`Execute` 関数を使用します。

例：

Windows 上のシステム バージョンを取得するには、以下のコマンドを使用します。

```
Execute ("cmd.exe /c ver > dms.tmp", True, 0)
```

出力は `dms.tmp` で利用可能です。

## インストールされたプログラム リストの読み取り

Windows で、Microsoft (SysInternals) から、以下のいずれかのコマンドを実行します。

```
wmic product
psinfo -accepteula -s
```

ファイルへの出力をリダイレクトし、次にそれを読み取ります。

## 実行中のプログラムの検出

dmscript は、実行中のプログラムを直接検出できませんが、これらのプログラムを検出するシステム コマンドを発行して、次にそれらの出力を読み取ることができます。

### 例：

```
(Unix)
execute ("ps -ef | grep myprogram > /tmp/dms.tmp")
(Windows)
execute ("cmd.exe /c tasklist /nh /fi ""imagename eq powerpnt.exe"" > dms.tmp",true,0)
...now read the contents of dms.tmp...
```

## 出力の作成

スクリプト内では、製品、リリース、パッチ、およびインスタンスが存在する階層に従う必要があります。

- 製品には、複数のリリースがあります。
- リリースには、複数のパッチがあります。
- リリースには、複数のインスタンス（またはインストールされたソフトウェアのコピー）があります。
- パッチには、複数のインスタンス（またはインストールされたパッチのコピーを）があります。

これは、最初に製品を指定し、続いてそのリリース、パッチ、およびインスタンスを指定する必要があることを意味します。子の項目を作成するときには、親の名前とバージョンも指定する必要があります。 **dmscript** は、作成されている階層を記憶し、項目の親が存在し有効であることを確認します。それ以外の場合には、エラーが返されます。製品を作成するために、複数の特定の関数が存在します。これらの関数は、以下の一般的な形式を持ちます。

```
CreateDetectedSoftwareXXXX (name, version, [parentname, parentversion,...]
OptionalProperties)
```

## 製品の作成

製品を作成するには、以下のコードを使用します。

```
CreateDetectedSoftwareProduct (ProductName as String,

 ProductVersionLabel as String,

 OptionalProperties as String) as integer
```

**例：**

```
CreateDetectedSoftwareProduct("Microsoft Windows 7 Ultimate", "6.1",
"VersionNumber=6.1 | Language=en-us | Bitness=64 | Architecture=x64 |
Manufacturer=Microsoft Corporation | Category=Operating Systems | Description=The
Microsoft Windows 7 Product | ")
```

この例では、値は定義されています。しかし、実際のスクリプトで、それらは検出プロセスの一部として決定されます。

## リリースの作成

製品のリリースを作成するには、以下のコードを使用します。

```
CreateDetectedSoftwareRelease (ProductName as String,
 ProductVersionLabel as String,
 ReleaseName as String,
 ReleaseVersionLabel as String,
 OptionalProperties as String) as integer
```

例：

```
CreateDetectedSoftwareRelease("Microsoft Windows 7 Ultimate", "6.1", "Microsoft
Windows 7 Ultimate x64 64 en-us", "6.1.7600", "VersionNumber=6.1.7600 | Language=en-us
| Bitness=64 | Architecture=x64 | Manufacturer=Microsoft Corporation |
Category=Operating Systems | Description=The Microsoft Windows 7 Release | ")
```

## パッチの作成

パッチを作成するには、以下のコードを使用します。

```
CreateDetectedSoftwarePatch (ProductName as String,
 ProductVersionLabel as String,
 ReleaseName as String,
 ReleaseVersionLabel as String,
 PatchName as String,
 PatchVersionLabel as String,
 OptionalProperties as String) as integer
```

例：

```
CreateDetectedSoftwarePatch("Microsoft Windows 7 Ultimate", "6.1", "Microsoft
Windows 7 Ultimate x64 64 en-us", "6.1.7600", "KB971033 x64 64 en-us", "Language=en-us
| Bitness=64 | Architecture=x64 | Manufacturer=Microsoft Corporation |
Category=Operating Systems | Description=The Microsoft Windows 7 Activation Checker
Update | ")
```

## インスタンスの作成

インストールされたリリースのインスタンスを作成するには、以下のコードを使用します。

```
CreateDetectedSoftwareReleaseInstance (ProductName as String,
 ProductVersionLabel as String,
 ReleaseName as String,
 ReleaseVersionLabel as String,
 OptionalProperties as String) as integer
```

インストールされたパッチのインスタンスを作成するには、以下のコードを使用します。

```
CreateDetectedSoftwarePatchInstance (ProductName as String,
 ProductVersionLabel as String,
 ReleaseName as String,
 ReleaseVersionLabel as String,
 PatchName as String,
 PatchVersionLabel as String,
 OptionalProperties as String) as integer
```

### 例：

```
CreateDetectedSoftwareReleaseInstance("Microsoft Windows 7 Ultimate", "6.1",
 "Microsoft Windows 7 Ultimate x64 64 en-us", "6.1.7600", "Origin=Forward Inc |
TrustLevel=5 | InstallPath=C:\Windows | SerialNumber=1234-567-890414-86668 |
LastAccessed=2011-11-29T12:30 | ")

CreateDetectedSoftwarePatchInstance("Microsoft Windows 7 Ultimate", "6.1",
 "Microsoft Windows 7 Ultimate x64 64 en-us", "6.1.7600", "KB971033 x64 64 en-us", "",
 "Origin=Forward Inc | TrustLevel=5 | ")
```

注：ユーザの組織名を反映するために Origin パラメータ内の値を置換します。

## 出力ファイルのクローズ

スクリプトで使用しているリソースを解放した後、  
`CloseDetectedSoftwareOutputFiles` を呼び出します。

## Intellisig のテスト

リリースする前に、少数のコンピュータ上でスクリプトをオフラインでテストします。テストすることにより、組織内のすべてのコンピュータ上で適用する前に、スクリプトを修正できます。コマンドラインからスクリプトを実行し、次に結果として以下のファイルを検査します。

- コンパイルエラーは、存在する場合にはトレース ログ ファイル内に生成されます。また、Unix 上の `dmsedit` および `stdout` でこれらのエラーを表示できます。
- スクリプトによって上げられるすべてのエラーが `<uuid>.err` に格納され、またトレース ログ ファイルにも格納されます。
- 検出されたソフトウェアの結果は、`<uuid>.xml` に格納されます。

テストでは、コマンドラインに **UUID** を指定する必要はありません。出力ファイルに名前を付ける場合、任意の文字列が有効であり、使用できます。**UUID** は、エージェントにのみ必要であり、この文字列を使用して名前を付けられたファイルを検索します。**UUID** の使用が推奨されています。

検出対象のコンピュータ、オペレーティングシステム、およびソフトウェアがインストールされており、利用可能であることを確認します。それ以外の場合には、通常存在する適切なファイル、レジストリ、および設定エントリを作成することにより、インストールされているソフトウェアをシミュレートします。ベンダーからの体験版を取得できます。

すべてのターゲット オペレーティングシステム上のスクリプトをテストすることを確認します。

2 番目のテスト レベルでは、予備のコンピュータまたは仮想マシンを使用して、小さな **DSM** の環境を作成します。これらのコンピュータのうち、1 台のコンピュータ上に **MDB**、ドメイン マネージャ、およびスケラビリティ サーバが存在する必要があるため、また **Asset Management** エージェントがターゲット オペレーティングシステムの 1 つにインストールされている必要があります。**DSM** エクスプローラを使用して **Intellisig** をインポートし、**Intellisig** ベースのソフトウェア検出タスクを実行します。予期された結果が表示されることを確認します。

## Intellisig のリリース

**Client Automation** が作成する **Intellisig** は、コンテンツ ダウンロード ジョブを使用して顧客に配信されます。カスタム作成された **Intellisig** の場合は、**DSM** エクスプローラを使用してテスト マネージャからエクスポートし、次に実稼働企業またはドメイン マネージャにインポートします。

関連項目：

[Intellisig のエクスポート](#) (P. 86)

[Intellisig のインポート](#) (P. 87)

## Intellisig トリガ

特定の条件またはトリガが満たされる場合に限り、Intellisig スクリプトが実行されるように制限できます。この制限により、効率的な Intellisig を設計できます。各 Intellisig は、特定のファイルに関してファイルシステムを検索する必要はありません。特定のファイル、レジストリ エントリ、サービス、またはインストールされたパッケージをスキャンするようにスキャナに指示し、またこれらの条件が満たされた場合に Intellisig スクリプトを実行するよう指示できます。スキャナは、指定されたファイル基準の数に関係なく、ファイルシステム検索を 1 回のみ実行します。

注：これらのトリガは、従来のシグネチャ定義と同じ方法で定義されています。これらの基準を使用して従来のシグネチャを作成した経験を持つことが前提条件となります。



## トリガ基準タイプ

以下に、Intellisig と関連付けることができるトリガのタイプを示します。

### ファイル

ファイルの存在のチェックをサポートし、また検索パスの基準、ファイル名コンテンツ パターン、ファイルの作成および変更日付範囲、ファイルサイズ範囲、MD5 ハッシュ値、および許可の指定をサポートします。

### レジストリ

特定のキーに対するレジストリ エントリのチェック、値のパターン マッチング、および 32 ビットと 64 ビット ハイブの確認をサポートします。

### パッケージ

バージョンとリリースを指定して、インストールされたパッケージをチェックします。Windows では、このオプションは [プログラムの追加と削除] データベースを確認します。UNIX では、プラットフォームのインストール データベースを確認します。

### サービス

インストールされたサービスまたはデーモンを検索します。

### システム情報

プラットフォーム、プロセッサ、OS リリース、OS 名、および OS バージョンなど属性のチェックをサポートします。

## トリガの論理的な階層

Intellisig に対して、複数のトリガ基準を指定できます。また、トリガは、論理 AND、OR、および NOT 演算子でグループ化できます。論理演算子は、タイプを持つグループとして定義されます。タイプは、*and*、*or*、または *not* であり、グループに含まれている項目の結果を組み合わせる方法を定義します。グループ (*not* グループを除く) は、より多くのグループを含めて、任意の数の追加トリガ基準を含むことができます。*not* タイプのグループは、単一項目のみ含むことができますが、この単一項目は別のグループとすることができます。

## 除外されるディレクトリ

Intellisig トリガを定義する場合、ディレクトリを除外するように指定できます。除外ディレクトリにリストされたディレクトリは、シグネチャ スキャナがファイル システムを検索して、ファイル トリガ基準で指定されたファイルを探すときに除外されます。

## XML 形式

トリガを記述するときに、XML を使用して基準を指定します。

各トリガにトップレベルのグループを含めます。各グループにはタイプが含まれます。タイプは、*and*、*or*、または *not* のいずれかです。タイプは、グループに含まれる基準に適用される論理演算を定義します。

```
<group type="and">
...<other criteria>...
</group>
```

## ファイル基準

ファイル基準は **<file>** タグで定義されます。**file** タグは、以下の属性をサポートしています。

### name

検索するファイルを指定します

### path

検索するパスを指定します

### match

指定されたパターンに一致するか、指定されたファイルをスキャンします

### md5

ファイルの **MD5** ハッシュを指定された値と比較します

### minversion

指定されたファイルのバージョンを提供された値と比較します

### maxversion

指定されたファイルのバージョンを提供された値と比較します

### mincreation

指定されたファイルのファイル作成日を提供された値と比較します

### maxcreation

指定されたファイルのファイル作成日を提供された値と比較します

**minmodified**

指定されたファイルのファイル変更日付を提供された値と比較します

**maxmodified**

指定されたファイルのファイル変更日付を提供された値と比較します

**minfilesize**

指定されたファイルのファイル サイズを指定されたサイズ値と比較します

**maxfilesize**

指定されたファイルのファイル サイズを指定されたサイズ値と比較します

**permsmustexclude**

許可を除外します

**permsmustinclude**

許可を包含します

**rootowner**

ファイルのルート所有者を指定します

**daclallow**

ACL を許可します

**dacldeny**

ACL を拒否します

**arch**

Windows プラットフォーム上のバイナリ ファイルのアーキテクチャを指定します

**例 :**

```
<group type="and">
<file name="msword.exe" path="*" />
</group>
```

## レジストリ基準

レジストリ基準は <registry> タグで指定されます。registry タグは、以下の属性をサポートしています。

### name

検索するレジストリ キーを指定します

### match

一致対象のパターンを指定します

### daclallow

ACL を許可します

### dacldeny

ACL を拒否します

### arch

64 ビット マシン上の動作を指定します。サポートされる値は 32、または 64、および any です。64 ビット Windows コンピュータでは、64 を指定すると、指定されたキーに関して 64 ビット ハイブのみ検索します。32 を指定すると、64 ビット コンピュータ上で 32 ビット ハイブのみ検索します。この値は、32 ビット コンピュータ上では無視されます。アーキテクチャを指定しないと、32 の動作がデフォルトの動作となります。

### 例：

```
<group type="and">
<registry name="HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Adobe Acrobat\6.0\Language\UI"
match="ENU" />
</group>
```

## パッケージ基準

パッケージ基準は `<package>` タグで指定されます。 `package` タグは、以下の属性をサポートしています。

### name

検索するインストールされた製品の名前を指定します

### version

検索するインストールされた製品のバージョンを指定します

### 例：

```
<group type="and">
<package name="DmWare Mini Remote Control" version="6.0.*" />
```

## サービス基準

サービス基準は `<service>` タグで指定されます。 `service` タグは、以下の属性をサポートしています。

### name

検索するインストールされたサービスの名前を指定します

### path

インストールされたサービスへの（UNIX のみ）パスを指定します

### 例：

```
<group type="and">
<service name="SNMP"/>
</group>
```

## システム情報基準

システム情報基準は `<sysinfo>` タグで指定されます。`<sysinfo>` タグは、以下の属性をサポートしています。

### platform

プラットフォームが Windows 上の x86 または x64 かどうかを指定します

### processor

プロセッサを識別します

### osrelease

OS リリースを識別します

### osname

OS 名を識別します

### osversion

OS バージョンを識別します

### 例：

```
<group type="and">
<sysinfo osname="Windows" />
</group>
```

## Intellisig を起動する場合のトリガ パラメータ

トリガが満足され、Intellisig スクリプトが実行されると、Intellisig のトリガに寄与する基準を定義するスクリプトに文字列が渡されます。トリガは `-t` フラグを使用して、Intellisig スクリプトに渡されます。スクリプトに渡されるトリガ文字列の形式は、トリガ定義で使用する基準タイプによって異なります。以下の表に、異なるトリガ基準タイプを使用するトリガ文字列の例を示します。複数のトリガが Intellisig スクリプトの実行に寄与する場合には、個別の基準を区切り文字 `|` を使用して指定します。Intellisig スクリプトは、トリガ文字列を解析して、トリガ評価で実行された処理を活用する必要があります。

| ファイル     | トリガの例                                                                                                                                                                                                                                               | -t パラメータの例                                                                                                                                                           |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| file     | <pre>&lt;group type="and"&gt;   &lt;file name="file1.test" path="*" /&gt; &lt;/group&gt; &lt;group type="not"&gt;   &lt;file name="file1.test" path="*" /&gt; &lt;/group&gt;</pre>                                                                  | <p>肯定的なトリガ :</p> <pre>-t "file:c:¥file1.test"</pre> <p>NOT トリガ :</p> <pre>-t "!file:file1.test"</pre> <p>NOT トリガについては、完全パスは提供できません。</p>                              |
| registry | <pre>&lt;group type="and"&gt; &lt;registry name="HKEY_LOCAL_MACHINE¥SOFTWARE¥iSigTest¥T1" match="V1"/&gt; &lt;/group&gt;  &lt;group type="not"&gt; &lt;registry name="HKEY_LOCAL_MACHINE¥SOFTWARE¥iSigTest¥T1" match="V1"/&gt; &lt;/group&gt;</pre> | <p>肯定的なトリガ :</p> <pre>-t "registry:HKEY_LOCAL_MACHINE¥SOFTWARE¥iSigTest¥T1"</pre> <p>NOT トリガ :</p> <pre>-t "!registry:HKEY_LOCAL_MACHINE¥SOFTWARE¥iSigTest¥T1"</pre> |
| service  | <pre>&lt;group type="and"&gt; &lt;service name="DNS Client"/&gt; &lt;/group&gt;  &lt;group type="not"&gt; &lt;service name="DNS Client"/&gt; &lt;/group&gt;</pre>                                                                                   | <p>肯定的なトリガ :</p> <pre>-t "service:DNS Client"</pre> <p>NOT トリガ</p> <pre>-t "!service:DNS"</pre>                                                                      |



| ファイル    | トリガの例                                                                                                                                                                                         | -t パラメータの例                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| sysinfo | <pre>&lt;group type="and"&gt; &lt;sysinfo osname="windows" platform="x86"/&gt; &lt;/group&gt;  &lt;group type="not"&gt; &lt;sysinfo osname="windows" platform="x86"/&gt; &lt;/group&gt;</pre> | <p>肯定的なトリガ :</p> <pre>-t "sysinfo:osname=Windows;platform=x86"</pre> <p>NOT トリガ :</p> <pre>-t "!sysinfo:osname=Linux;platform=x86"</pre> |
| package | <pre>&lt;group type="and"&gt; &lt;package name="CA DSM Explorer"/&gt; &lt;/group&gt;  &lt;group type="not"&gt; &lt;package name="CA DSM Explorer"/&gt; &lt;/group&gt;</pre>                   | <p>肯定的なトリガ :</p> <pre>-t "package:CA DSM Explorer"</pre> <p>NOT トリガ :</p> <pre>-t "!package:CA DSM Explorer EXTRA123"</pre>              |

## カスタム Intellisig の変更

Intellisig の開発者として、カスタム Intellisig を変更して、Intellisig 内のスクリプト、トリガ、またはデータ ファイルを更新できます。



## Intellisig のエクスポート

Intellisig をエクスポートして Intellisig を変更するか、またはドメイン マネージャからエンタープライズ マネージャ、または別のドメイン マネージャに移動します。すべての Intellisig、特定の Intellisig、または Intellisig の特定バージョンをエクスポートできます。また、Intellisig のエクスポートに CLI を使用できます。CLI の詳細については、「[intellisigcmd export -- Intellisig のエクスポート \(P. 138\)](#)」を参照してください。

**注：** 製品、リリース、またはパッチ定義レベルではなく、Intellisig レベルでのみエクスポートできます。

次の手順に従ってください：

1. [ソフトウェア] - [定義] に移動し、すべての Intellisig、特定の Intellisig、または Intellisig の特定バージョンをエクスポートするかどうかに応じて、以下のいずれかを実行します。

### すべての Intellisig

- [Intellisig] ノードを右クリックして、[プロパティ] を選択します。

### 特定の Intellisig

- [Intellisig] ノードをクリックして、右ペインでエクスポートする Intellisig を選択します。選択対象を右クリックし、[更新] を選択します。

### Intellisig の特定バージョン

- [Intellisig] ノードをクリックし、Intellisig を右クリックして、[プロパティ] を選択します。[バージョン] タブをクリックし、エクスポートするバージョンを選択して、[Intellisig プロパティ] ダイアログ ボックスで [エクスポート] をクリックします。

[Intellisig エクスポート] ダイアログ ボックスに、選択した Intellisig が一覧表示されます。

2. Intellisig を圧縮ファイルとしてエクスポートするか、または圧縮されていないフォルダとしてエクスポートするかを指定し、必要な場合には [参照] をクリックして場所を変更します。

**注：** Intellisig の変更中は圧縮されていない形式、管理者間での Intellisig の移動時には圧縮形式の使用をお勧めします。

3. [OK] をクリックします。

選択された Intellisig は、指定した場所にエクスポートされ配置されます。

関連項目：

[カスタム Intellisig の変更](#) (P. 121)

[マネージャ間での Intellisig の移動](#) (P. 85)

## カスタム Intellisig の変更

Intellisig を変更して、スクリプト、トリガ、またはデータ ファイルを更新できます。

次の手順に従ってください：

1. Intellisig をエクスポートしたことを確認します。
2. エクスポートされた Intellisig アーカイブ ファイルまたはフォルダを開き、要件ごとにファイルを更新します。Intellisig のカスタマイズの詳細については、「[カスタム Intellisig の作成](#) (P. 89)」を参照してください。
3. 変更したファイルを保存し、ZIP ファイルとしてインポートする場合は、それらを圧縮します。

## Intellisig のインポート

Intellisig をインポートして、変更後に Intellisig を更新するか、またはドメイン マネージャからエンタープライズ マネージャ、または別のドメイン マネージャに移動します。また、Intellisig のエクスポートに CLI を使用できます。CLI の詳細については、「[intellisigcmd import -- Intellisig のインポート \(P. 139\)](#)」を参照してください。

次の手順に従ってください：

1. [ソフトウェア] - [定義] に移動し、[Intellisig] ノードを右クリックして [インポート] を選択します。  
[Intellisig インポート] ダイアログ ボックスが開きます。
2. [参照] をクリックし、インポートする Intellisig の ZIP ファイルまたは XML ファイルを選択します。
3. [インポート モード] を選択して、既存の定義を置換するか、新しい変更のみマージするか、またはすべての変更をマージするかを指定します。
4. (オプション) アクティブな Intellisig バージョンを変更しない場合は、[インポート中にアクティブな Intellisig バージョンを更新する] オプション中をクリアします。[OK] をクリックします。

リストア処理が開始します。

注：(Intellisig のみのエクスポート ZIP オプションから) 対応する ZIP によって ZIP 形式で Intellisig をエクスポートする必要があります。任意のサードパーティ圧縮 (ZIP) ユーティリティを使用しないでください。

## Intellisig データと別の CA 製品との調整

検出された Intellisig ソフトウェア定義および検出されたそのソフトウェア インスタンスは、Client Automation ソース MDB からターゲット MDB に同期され、別の CA 製品との統合が可能になります。

## Intellisig 定義とリモート データベースの同期

ターゲット MDB が Intellisig をサポートする場合、同期タスクが作成されるとき、検出された Intellisig ソフトウェア定義および検出されたそのソフトウェア インスタンスが同期設定に追加されます。同期タスクがすでに存在する場合、次回にタスクが実行されるときに設定が更新されます。

これは、CA が提供する Intellisig とカスタム Intellisig の両方に適用できます。

検出されたソフトウェア定義のマスタ Intellisig 定義は、コンテンツ ユーティリティを実行するときに、同期の最初の段階で作成されます。

検出されたソフトウェア定義は、ターゲット（別の MDB ソースから送信された）で任意のすべての定義と比較されます。

製造元とカテゴリへの検出されたソフトウェア定義のリンクは、製造元とカテゴリ付き（必要な場合には作成）ターゲット MDB にレプリケートされます。Intellisig によって作成された以前のすべてのカテゴリ メンバシップが削除されます。しかし、手動で作成された任意のカテゴリ メンバシップは保持されます。

同期ジョブの削除およびクリーンアップの選択時に、ソース MDB から開始された検出されたソフトウェアが削除されます。これが最後のソース MDB である場合、検出されたソフトウェア定義および詳細のないマスタ Intellisig も削除されます。

## Intellisig の複製

エンタープライズ マネージャ上でカスタム Intellisig 定義を作成して、それらの定義を複製できます。複製により、各ドメイン マネージャ上で定義を別々に定義する必要がなくなります。

### ( オプション ) Intellisig 定義に関する複製設定の変更

複製タスクで定義されているデフォルトの複製設定を変更できます。

次の手順に従ってください：

1. DSM エクスプローラーを開きます。 [コントロールパネル] - [設定] - [設定ポリシー] - [ポリシー名] に移動し、ポリシーを右クリックして [封印解除] を選択します。
2. 設定ポリシーの下の [マネージャ] - [エンジン] に移動します。

3. 以下の設定ポリシー パラメータの値を指定します。

#### 複製された Intellisig がローカルに定義されている場合は無視する

Intellisig 定義が、以前にドメイン マネージャによってローカルに作成された場合、複製の動作を制御します。このパラメータを [はい] に設定すると、エンタープライズ マネージャからのマスタ定義と詳細は複製されません。それ以外の場合、ドメイン マネージャで、マスタ定義がエンタープライズ マネージャからの定義によって更新されます。その `domain_uuid` は、ソースのものに変更されます。ドメイン マネージャで既存の定義が更新されます。ドメイン マネージャで、マスタのすべての既存の詳細が削除されます。エンタープライズ マネージャからの Intellisig の詳細が、ドメイン マネージャに複製されます。

デフォルト： いいえ

#### 複製された Intellisig をリンク解除時に変換する

リンク解除時に、ドメイン マネージャで複製されたマスタ Intellisig 定義およびその詳細をすべて削除するデフォルト動作を無効にします。このパラメータを [はい] に設定すると、リンク解除時に、ドメイン マネージャで複製されたすべてのマスタ Intellisig 定義と詳細が、ドメイン マネージャに属するものとして変換されます。つまり、それらの `domain_uuid` が、エンタープライズ マネージャのものからドメイン マネージャのものに変更されます。

デフォルト： いいえ

#### 複製されたソフトウェア定義を残す

複製されたヒューリスティックおよび Intellisig で検出されたソフトウェア定義がドメイン マネージャによって削除された場合、それらをエンタープライズ マネージャで保持する必要があるかどうかを指定します。[いいえ] に設定すると、最後のドメイン マネージャでそれらが削除されたことがレポートされたときに、それらはエンタープライズ マネージャで削除されます。

デフォルト： いいえ

#### コレクション上の非参照ソフトウェア定義を残す

ヒューリスティック ソフトウェア定義の最後に検出されたソフトウェア インスタンスが削除された場合、エンジン収集で、ドメイン マネージャがそれらの定義を削除しないで残す必要があるかどうかを指定します。

デフォルト：いいえ

4. ポリシーを保存して封印します。DSM エンジン（レプリケーション タスクを実行）をホストするコンピュータ上でポリシーを適用します。

関連項目：

[エンタープライズ マネージャ セットアップで Intellisig を使用するための考慮事項 \(P. 127\)](#)

## エンタープライズ マネージャ セットアップで Intellisig を使用するための考慮事項

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、エンタープライズ マネージャは、検出されたソフトウェア定義および検出されたソフトウェア レコードを複製します。レプリケーション処理の後、1つの場所から情報の表示、問い合わせ、レポート、および同期を行うことができます。

エンタープライズ マネージャのセットアップで Intellisig を使用するとき、以下の考慮事項が適用されます。

- カスタム作成された Intellisig 定義およびそれらの詳細が、エンタープライズ マネージャからドメイン マネージャに複製されます。
- CA で定義された Intellisig 定義およびそれらの詳細は、エンタープライズ マネージャからドメイン マネージャに複製されません。
- Intellisig によって検出された製品、リリース、およびパッチは、ドメイン マネージャからエンタープライズ マネージャに複製されます。
- Intellisig 定義は、エンタープライズ マネージャに存在しない場合には作成されます。

- Intellisig によって検出される定義の製造元およびカテゴリは、以下のように作成されます。
  - 検出されたソフトウェア定義に関して、Intellisig スクリプトは、その定義の製造元を検出し、カテゴリにリンクします。これらの関係は、ドメインの MDB で収集され、エンタープライズ マネージャに複製されます。レプリケーションによって、ドメイン マネージャでのものと同じ UUID を持つエンタープライズ マネージャ内に一致する製造元またはカテゴリが見つかった場合、この処理は単純です。
  - 同じ UUID の製造元またはカテゴリがエンタープライズ マネージャに存在しない場合、およびドメイン マネージャで製造元またはカテゴリが CA によって提供される場合には、同じ名前および UUID の製造元またはカテゴリが、ソース タイプとして CA を持つエンタープライズ マネージャで作成されます。
  - 同じ UUID の製造元またはカテゴリがエンタープライズ マネージャに存在しない場合、およびドメイン マネージャで製造元またはカテゴリが CA によって提供されない場合には、レプリケーションによって、同じ名前のカテゴリの製造元が検索されます。
  - エンタープライズ マネージャで、同じ名前の製造元またはカテゴリがこのように見つかる場合、それを使用して検出された定義とリンクされます。
  - 同じ名前の製造元またはカテゴリが見つからない場合、新しい製造元またはカテゴリが作成され、検出された定義とのリンクに使用されます。
  - 新しい製造元またはカテゴリのソース タイプは、Intellisig のソース タイプに応じて、CA Intellisig またはカスタム Intellisig のいずれかになります。それらは、いずれのドメインにも複製されません。
  - 以前に Intellisig によってレポートされた検出済みのソフトウェア定義のカテゴリおよび製造元が変更された場合、それらは、ドメイン マネージャ上の検出されたソフトウェア定義からリンク解除されます。手動でリンクされるカテゴリと製造元は変更されません。
- Intellisig によって検出された検出済みソフトウェア リリースおよびパッチは、ドメイン マネージャからエンタープライズ マネージャに複製されます。
- [複製されたソフトウェア定義を残す] 設定ポリシーが false 設定されている場合、検出されたソフトウェア レコードがエンタープライズ マネージャまたはドメイン マネージャにリンクされていない場合には、ヒューリスティックおよび検出済み Intellisig 定義が削除されます。ポリシーの詳細については、「[Modify Replication of Intellisig Definitions from Enterprise Manager \(P. 125\)](#)」を参照してください。
- ソフトウェアがドメイン マネージャで存在する場合、任意のソフトウェア定義カテゴリ メンバシップがエンタープライズ マネージャからドメイン マネージャに複製されます。



## DMScript の拡張

### ソフトウェア定義および検出レコードの作成

カスタム Intellisig を作成するときには、エージェント コンピュータ上で検出されるソフトウェア レコードをレポートするために Intellisig スクリプト内で **DMScript** 関数を呼び出します。**DMScript** は、検出されたソフトウェア レコードを出力ファイルに書き込む組み込み関数を提供します。

注：DMScript は、エージェントでコマンドを実行するための共通手段を提供するスクリプト言語です。DMScript の詳細については、**CA Client Automation マニュアル** 選択メニューから「*Desktop Management* スクリプト言語」ガイドを参照してください。

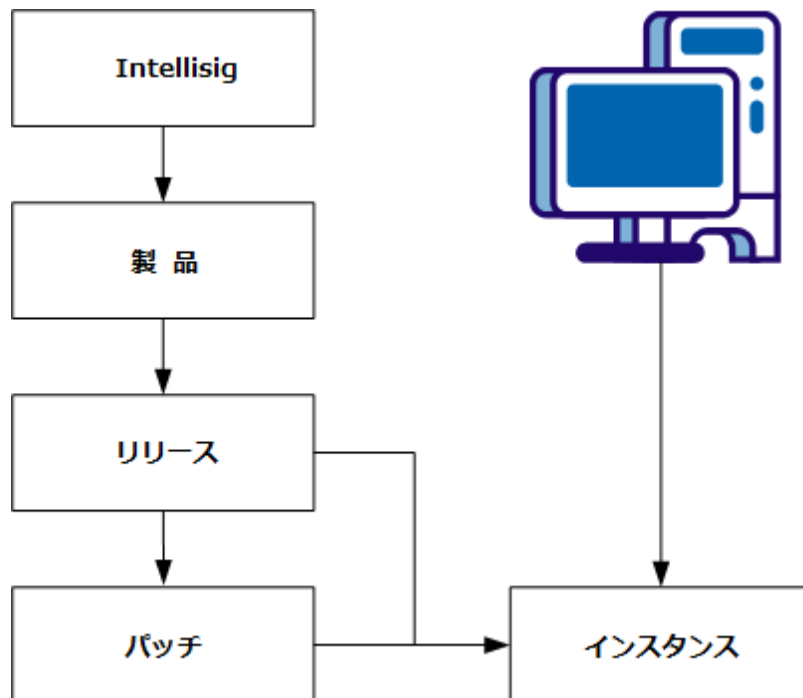
Intellisig スクリプトは、以下の順序で関数を呼び出す必要があります。

1. OpenDetectedSoftwareOutputFiles
2. CreateDetectedSoftwareProduct
3. CreateDetectedSoftwareRelease
4. CreateDetectedSoftwarePatch
5. CreateDetectedSoftwareReleaseInstance
6. CloseDetectedSoftwareOutputFiles

Intellisig 関数の詳細については、「Desktop Management スクリプト言語」ガイドを参照してください。

## Intellisig オブジェクトの階層

カスタム Intellisig を作成する場合、Intellisig オブジェクトの階層の理解することが重要です。オブジェクトは、特定の階層で存在する必要があります。各オブジェクトには親があり、前もって作成されている必要があります。階層は、以下のようになります。



- Intellisig には、多くの製品を検出するための情報が含まれます。
- たとえば Microsoft Office の製品には、Office 2003、Office 2010 などの多数のリリースがあります。
- リリースには、修正が含まれるパッチが複数あります。
- コンピュータには、リリースの複数のインスタンス、またはパッチがインストールされています。
- 製品、リリース、およびパッチはソフトウェア定義として作成され、インスタンスは検出されるソフトウェアとして作成されます。
- オブジェクトの作成時に、DMscript は、親オブジェクトの可用性をチェックします。たとえば、リリースを作成する場合、DMScript は、親製品が存在するかどうかを確認します。この確認により、関連する製品、リリース、パッチ、およびインスタンスの間に適切な関係が作成されることが保証されます。

## 固定パラメータと可変パラメータ

検出されたソフトウェア出力ファイルを作成する関数を使用して、固定パラメータおよび可変パラメータを受け入れることにより、将来の拡張用に対する方法が提供されます。修正されたパラメータは必須ですが、可変パラメータはオプションです。可変パラメータには、通常 **Intellisig** と関連付けられ、追加のプロパティを追加するための手段となるプロパティが含まれます。関数は、将来、既存のスクリプトに影響を与えることなく、可変パラメータを追加して拡張できます。

固定パラメータと可変パラメータの指定および使用には、以下のガイドラインが適用されます。

- 固定パラメータは必須であり、値が明示的に要求されます。
- 可変パラメータはオプションであり、**OptionalProperties** パラメータで指定されます。**OptionalProperties** パラメータは文字列であり、以下の形式を使用して、任意の数のプロパティ名と値のペアを含むことができます。  
`property=value | property=value |...`
- `|` 文字を使用して、プロパティ名と値のペアを分離します。`|` 文字の前後のスペースは、重要な意味を持ちません。
- **OptionalProperties** 内に不明のプロパティが存在する場合、警告が生成されますが、スクリプトは停止しません。この動作により、各種リリースのエージェントは、ドメインマネージャから送られた **Intellisig** スクリプトを処理できます。スクリプトで、特定のバージョンの **DMScript** では認識できないプロパティが使用された場合、そのプロパティは無視されますが、**DMScript** トレースログに警告が書き込まれます。
- オプションパラメータ内の不明な値により、警告が生成されます。ただし、値はエンジンに渡され、解釈または無視されます。たとえば、**bitness** パラメータの値には、**32** または **64** のみ使用できますが、**16** を渡してもスクリプトは失敗しません。

## サポートされるアーキテクチャ

以下に、ソフトウェア検出力ファイルに検出されたレコードを書き込む DMscript 関数へ渡すことができるアーキテクチャ名のリストを示します。

- AMD64
- ARM
- Alpha
- Big Endian MIPS
- HP Precision
- IA64
- IBM S/390
- Little Endian MIPS
- Motorola 680x0
- PA\_RISC
- PowerPC
- SPARC
- s390x
- x64
- x86

## エラー コードおよびオプション プロパティ

LogDetectedSoftwareError メソッドは、特定の形式でエラー メッセージを受け入れます。エラー メッセージは、エージェントに Intellisig 実行エラーがあるとき生成されるローカライズ可能な文字列です。次に、エラー メッセージは、ドメインマネージャに送信され、DSM エクスプローラ内のソフトウェア インベントリ収集タスクに対するステータス コメントとして表示されます。

### 例 : LogDetectedSoftwareError

```
LogDetectedSoftwareError("ISE:00400","PARAM5=Microsoft Windows 7
Ultimate x64 64 en-us|PARAM6=VersionNumber=6.1.7600
|VersionLabel=6.1.7600 |Language=en-us |Bitness=64
|Architecture=x64 |Manufacturer=Microsoft
Corporation|Category=Operating Systems |Description=The Microsoft
Windows 7 Product|PARAM7=SWDETECT_BADARGS");
```

Intellisig スキャナは、自動的に以下のエラー メッセージを生成して、Intellisig の起動に関連する問題を報告します。

| エラー コード   | エラー テキスト                                                                                                                                                                   |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISE:00302 | The intellisig named %1\$t, version %2\$t, UUID %3\$t, is missing the mandatory parameter %4\$t.                                                                           |
| ISE:00303 | Intellisig named %1\$t, version %2\$t, UUID %3\$t, script file %4\$t did not produce an output file.                                                                       |
| ISE:00304 | The execution of Intellisig named %1\$t, version %2\$t, UUID %3\$t, script file %4\$t has exceeded the allowable timeout (%5\$t seconds).                                  |
| ISE:00305 | Intellisig named %1\$t, version %2\$t, UUID %3\$t, script file %4\$t could not be found.                                                                                   |
| ISE:00306 | Intellisig named %1\$t, version %2\$t, uuid %3\$t, script file %4\$t, caused an internal error while attempting to start an intellisig                                     |
| ISE:00307 | The dmscript interpreter reported an error parsing the Intellisig named %1\$t, version %2\$t, uuid %3\$t, script file %4\$t                                                |
| ISE:00405 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, %5\$t was called to create "%6\$t" with an unknown parent "%7\$t".                                               |
| ISE:00406 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, %5\$t was called to create "%6\$t" with a parent "%7\$t" of the wrong type.                                      |
| ISE:00407 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, %5\$t was called to create an instance with a parent "%6\$t" of the wrong type.                                  |
| ISE:00411 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, %5\$t was called with mandatory property "%6\$t" set to blank.                                                   |
| ISE:00412 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, the lastaccessed property was specified with an invalid value: %5\$t: should be in the format: yyyy-mm-dd:hh:mm. |

以下のエラーメッセージを生成して、Intellisig の作成に関連する問題を処理できます。

| エラー コード   | エラー テキスト                                                                                                                                                                                                         | 関数の構文                                                                                                                       |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| ISE:00400 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, Failed to create software product. The parameters were ProductName:%5\$t OptionalProperties : %6\$t. Return Code : %7\$t                               | LogDetectedSoftwareError ("ISE:00400", "PARAM5=ProductName PARAM6=OptionalProperties PARAM7=ReturnCode")                    |
| ISE:00401 | Intellisig %1\$t version %2\$t, UUID %1\$t, script %4\$t, Failed to create Software Release. The parameters were ProductName:%5\$t ReleaseNameProductRelease:%6\$t OptionalProperties %7\$t. Return Code : %8\$t | LogDetectedSoftwareError ("ISE:00401", "PARAM5=ProductName PARAM6=ReleaseName PARAM7=OptionalProperties PARAM8=ReturnCode") |
| ISE:00402 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, Failed to create Software Patch. The parameters were ReleaseName:%5\$t PatchName:%6\$t OptionalProperties %7\$t. Return Code: %8\$t                    | LogDetectedSoftwareError ("ISE:00402", "PARAM5=ReleaseName PARAM6=PatchName PARAM7=OptionalProperties PARAM8=ReturnCode")   |
| ISE:00403 | Intellisig %1\$t version %2\$t, UUID %3\$t, script %4\$t, Failed to create Software Instance. The parameters were PatchName:%5\$t OptionalProperties: %6\$t. Return Code : %7\$t                                 | LogDetectedSoftwareError ("ISE:00403", "PARAM5=PatchName PARAM6=OptionalProperties PARAM7=ReturnCode")                      |

| エラー コード   | エラー テキスト                                                                                                                                                   | 関数の構文                                                                                    |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| ISE:00404 | Intellisig %1\$t version %2\$t,<br>UUID %3\$t, script %4\$t,<br>produced the following<br>error : %5\$t<br><br>注：PARAM5 に、任意のカス<br>タム エラー テキストを指定<br>できます。 | LogDetectedSoftwareError<br>("ISE:00404", "PARAM5="An<br>unexpected error has occurred") |

## Intellisig に対する追加情報

### Intellisig の整合性を確認に使用される証明書

Client Automation は、データベース内の各スクリプトと暗号化されたハッシュを関連付けることにより、Intellisig の整合性を維持します。エージェントは、ハッシュを確認した後、各 Intellisig を実行します。ハッシュの検証が失敗すると、エージェントは、Intellisig の実行を拒否し、GUI にメッセージを送信して、この検証エラー、および整合性の確認に失敗した特定の Intellisig の詳細を示します。

注：ハッシュは、ManagerSigner のタグ付き証明書 x509cert://dsm r11/cn=manager signer,o=computer associates, c=us を使用して暗号化されます。カスタム x509 証明書を使用すると、Intellisig は、暗号化に対して自動的にカスタム証明書を使用します。

## 32 ビットおよび 64 ビット レジストリの両方を使用した 64 ビット OS 上のソフトウェアの検出

レジストリおよびファイルエントリの両方に関して、DSM エクスプローラで従来のカスタム シグネチャを作成する場合、レジストリのアーキテクチャ値を指定できます。指定された値は、指定された Windows アーキテクチャに対してバイナリが構築されていることを確認します。

次の手順に従ってください：

1. [DSM エクスプローラ] - [ソフトウェア] - [定義] - [ソフトウェア カテゴリ] - [ソフトウェア カテゴリのリリース] - [プロパティ] - [識別] - [詳細設定] - [レジストリ] に移動します。
2. 64 ビット OS の [アーキテクチャ] ドロップダウン ボックスで、以下のいずれかの値を選択します。

32

32 ビット レジストリ ハイブ内の検索をトリガします。

64

64 ビット レジストリ ハイブ内の検索をトリガします。

注：OS グループ タイプを UNIX に変更すると、[アーキテクチャ] ドロップダウン ボックスが無効になります。

## Intellisig に対するデフォルト タイムアウトの設定

Intellisig のデフォルト タイムアウトにより、不正な Intellisig がコンピュータ上で無期限に実行されないことが保証されます。コンピュータ上で実行されるすべての Intellisig スクリプト、または特定の Intellisig に対して、デフォルト タイムアウト値を定義できます。たとえばデータベース サーバなど負荷が大きい場合、および Intellisig の完了に余分な時間が必要な場合には、エージェントにより長いデフォルト時間を適用できます。デスクトップ コンピュータでは、負荷が小さい場合、より短いタイムアウト値を設定できます。



次の手順に従ってください：

1. [DSM] - [エージェント] - [Asset Management] に移動します。
2. 以下のパラメータに対する値を定義します。

#### IntellisigDefaultExecutionTimeout

デフォルト タイムアウト値を分単位で指定します。

デフォルト：5

注：Intellisig を作成するときには、そのタイムアウト値をデフォルトに設定します。このアクションにより、エージェントが、設定されたデフォルト タイムアウトを適用することが保証されます。Intellisig に 0 より大きいタイムアウト値がある場合、Intellisig の実行時に、指定された値が適用されます。

## intellisigcmd - コマンドライン ツール

intellisigcmd は、Intellisig のコマンドライン ツールです。このツールの形式は、以下のとおりです。

```
intellisigcmd <cmd> param1=value1 param2=value2 ... [<DB_Credentials>]
```

cmd

import、export、または genuuid コマンドを指定します。

#### DB\_Credentials

MDB のデータベース クレデンシャルを指定します。デフォルトでは、クレデンシャルは comstore から取得されます。

DB クレデンシャルの指定では、以下のサンプル形式を使用します。

例：SQLServer DB クレデンシャル

```
dbvendor=mssql dbhost=myhost dbname=mdb dbuser=ca_itrm dbpassword=mypwd
dbinstance=inst
```

例：Oracle DB クレデンシャル

```
dbvendor=oracle dbhost=myhost dbname=orcl dbuser=ca_itrm dbpassword=mypwd
dbinstance=1521
```

## intellisigcmd export -- Intellisig のエクスポート

intellisigcmd export コマンドでは、Intellisig をエクスポートできます。DSM エクスプローラまたはコマンドを使用して Intellisig をエクスポートできます。

コマンドの形式

```
intellisigcmd export file=<export name> [type=xml|zip] [platform=all|windows|unix]
```

**export name**

エクスポートする Intellisig XML または ZIP ファイルの名前を指定します。ファイル拡張子を指定せず、タイプが xml の場合、このコマンドは指定された名前でフォルダを作成します。

**type**

XML または ZIP ファイルをエクスポートするかどうかを指定します。type パラメータが含まれない場合、このコマンドは、エクスポートファイル拡張子に応じてエクスポートタイプを想定します。

**有効な値：** xml、zip

**platform**

どの Intellisig がエクスポートされるかを決定するために、プラットフォームを指定します。

**有効な値：** all、windows、unix

**デフォルト：** all

## intellisigcmd import -- Intellisig のインポート

intellisigcmd import コマンドでは、Intellisig をインポートできます。DSM エクスプローラまたはコマンドを使用できます。

コマンドの形式

```
intellisigcmd import [file=<import source>] [type=xml|zip]
[mode=replace|mergenew|mergeall] [updateactive=yes|no] [delete=yes|no]
```

import source

Intellisig をインポートする XML または ZIP ファイルの名前を指定します。ファイル拡張子を指定しない場合、このコマンドは、タイプに応じてファイル拡張子を想定します。

注：XML ファイルにインポートする場合、サポートするディレクトリが XML ファイルと同じフォルダに存在することを確認します。

type

XML または ZIP ファイルをインポートするかどうかを指定します。このパラメータが含まれない場合、このコマンドは、インポートファイル拡張子に応じてインポートタイプを想定します。

有効な値：xml、zip

#### mode

インポート モードを指定します。以下のインポート モードがサポートされています。

**デフォルト :** mergenew

#### replace

インポートされた定義で既存の定義を置換します。既存の定義が失われます。

#### mergenew

マネージャ上の定義に、新しい Intellisig バージョンを追加します。既存の定義は変更されません。

#### mergeall

新しい Intellisig バージョンを追加して、インポート ファイルに含まれている既存の定義を更新します。インポート ファイルで定義されていない Intellisig バージョンは変更されません。

#### updateactive

インポート中に、アクティブな Intellisig バージョンが更新可能かどうかを指定します。

**有効な値 :** Yes、Y、true、1 または No、N、false、0

**デフォルト :** Yes

#### delete

インポートの前に Intellisig を削除するかどうかを指定します。delete スイッチを指定しない場合、いずれの Intellisig もインポートの前に削除されません。

**デフォルト :** No

## intellisigcmd genuuid -- UUID の生成

intellisigcmd genuuid コマンドでは、カスタム Intellisig の作成時に使用可能な一意の UUID を生成できます。

コマンドの形式

```
intellisigcmd genuuid [num=<count>]
```

num

生成する UUID の数を指定します。このパラメータを指定しない場合、単一の UUID が生成されます。それ以外の場合、<count> 数の UUID が生成されます。

有効な値：1 ～ 1000

## 仮想アプリケーション イメージ

Client Automation のこのリリースでは、Asset Management は、Microsoft App-V（以前の SoftGrid）および VMware ThinApp で仮想化されたアプリケーションの検出およびインベントリをサポートします。

アプリケーションは、Microsoft App-V Sequencer または VMware ThinApp Setup Capture アプリケーションを使用し、アプリケーション データをキャプチャすることによって仮想化されます。アプリケーションは**仮想アプリケーションイメージ**にまとめられます。密接に統合されたスイート製品またはアプリケーションの場合は、複数のアプリケーションを同じイメージに仮想化できます。

**注：** 検出する仮想アプリケーション イメージ用に Client Automation スケーラビリティ サーバによって配信された新しいソフトウェア シグネチャは、レガシー エージェントに無視されるように特別にタグが付けられています。そのため、エージェントはこれらのソフトウェア シグネチャおよびインベントリ仮想アプリケーションを適切に処理します。

非仮想アプリケーション（通常、ローカルにインストールされるアプリケーション）と異なり、**仮想アプリケーション**は複数の方法でインストールされます。

### ストリーム配信

このモードでは、仮想アプリケーションイメージはエンド ユーザのコンピュータにコピーされません。イメージ内の仮想アプリケーションは、たとえば、ユーザの [スタート] メニューまたはデスクトップ上でユーザに通知されます。ユーザがストリーム配信仮想アプリケーションを開くと、必要なアプリケーション データがネットワークを経由してオンデマンドで配信されます。

### スタンドアロン

このモードでは、仮想アプリケーションイメージは、ユーザのハードディスク上でローカルにステージングされます。イメージ内の仮想アプリケーションはユーザに通知されます。ユーザがスタンドアロン仮想アプリケーションを開くと、必要なアプリケーション データがローカル ハード ディスクから直接配信されます。

### ステージ済み

このモードでは、仮想アプリケーションイメージは、ユーザのハードディスクにローカルにインストールされます。ただし、イメージ内の仮想アプリケーションはエンドユーザに通知されません。このインストールタイプは、他のストリーム配信インストール用のサーバで見られます。仮想アプリケーションイメージ内のアプリケーションは、コンピュータのローカルユーザが利用することはできません。

**Asset management** は 3 つのタイプの仮想アプリケーションのインストールをすべて検出し、インベントリを作成できます。さらに、仮想アプリケーションイメージ自体がレポートされます。仮想アプリケーションイメージをストリーム配信するか、ステージングすることができます。

仮想アプリケーションが **CA ITCM** ソフトウェア配信機能、プロプライエタリ ストリーミング ソリューションまたはアドホック配信のうち、どの方法を使用して展開したかにかかわらず、**Asset Management** は仮想アプリケーションを検出できます。

**注：**仮想アプリケーションイメージの作成、パッケージ、および展開の詳細については、「ソフトウェア配信管理者ガイド」および「ソフトウェア配信ヘルプ」を参照してください。

## VMware ThinApp を使用したアプリケーションの配信

VMware ThinApp は、仮想アプリケーションをネットワーク配信するために専用のストリーミング サーバを使用しません。代わりに、アドホック ベースでネットワーク共有場所からアプリケーションを開くと、アプリケーションがストリーム配信されます。

ユーザのデスクトップまたは [スタート] メニュー上に共有場所のアプリケーションへのショートカットが存在する場合のみ、Asset Management は ThinApp 仮想アプリケーションがストリーム配信されたと判断します。特定のコンピュータからアクセス可能な共有場所に ThinApp 仮想アプリケーションを配置しただけでは、ストリーム配信されたアプリケーションの検出は有効になりません。

ストリーム配信された ThinApp アプリケーションの検出サポートはデフォルトでは有効ではありません。DSM エクスプローラの [コントロール パネル] の下から [収集タスク] セクションにあるシグネチャ スキャナの設定を使用すると、このサポートを有効にすることができます。

## 非ドメイン環境での ThinApp パッケージの検出

非ドメイン環境でのストリーム ThinApp パッケージの検出は断続的です。ユーザがサーバの共有フォルダのアクセス認証を持つ場合、ユーザ毎のスキャンを一度に実行しないのであれば、スキャンはその共有のコンテンツを検出できません。

一般的に、スキャンの実行はログオン直後に実施され（この場合、ユーザはスクラビリティ サーバへの認証をまだ持っていない可能性がある）、またフル シグネチャ スキャンが実行されている場合には常に実施されます。フル チグネチャ スキャンは低い頻度でしか発生せず、またユーザのログオン時には発生しません。

そのため CA は、ストリーム ThinApp アプリケーションへのドメイン/アクティブ ディレクトリの使用と、ThinApp 仮想アプリケーション パッケージの展開を強くお勧めします。

## 検出方法

非仮想アプリケーションのインベントリと同様に、Asset Management には仮想アプリケーションの検出および一覧作成を行うための 2 つの方法があります。これは、シグネチャ スキャナとヒューリスティック スキャナです。

詳細情報：

[ソフトウェアの検出](#) (P. 203)

## 仮想アプリケーションのシグネチャ スキャン

シグネチャ スキャナは、ThinApp 実行可能ファイル、App-V.sft ファイルなどのエージェント マシンで利用可能な仮想アプリケーションを検出することによって、アプリケーション仮想化をサポートします。

MDB では、仮想アプリケーション イメージがそのイメージに含まれていると認識されているソフトウェア リリースおよびパッチと関連付けられます。この情報は、仮想アプリケーション イメージとそのイメージに含まれる仮想アプリケーションのすべてのインベントリを提供するために使用されます。

仮想アプリケーション イメージの作成はエンドユーザによって実行されるので、CA コンテンツ チームが仮想アプリケーション イメージを認識するソフトウェア定義を提供することはできません。そのため、DSM 管理者はこれらの仮想アプリケーション イメージ定義を作成する必要があります。仮想アプリケーション パッケージがソフトウェア配信ライブラリに登録されている場合、このプロセスは自動的に行われます。カスタム定義を手動で作成する場合、仮想アプリケーション イメージ定義の識別情報も自動的に検出できます。

仮想アプリケーション イメージとそのコンテンツの関連付けは重要なタスクであり、手動で実行する必要があります。仮想アプリケーション イメージ定義が作成されると、[封印解除済み] 状態に設定されます。また、イメージのコンテンツは定義されていません。DSM 管理者は、CA が提供した既存のソフトウェア定義またはカスタムで作成したソフトウェア定義からコピーおよび貼り付けを実行することによって、そのイメージとイメージに含まれると認識されている非仮想リリースを関連付ける必要があります。可能な場合には、CA が提供したソフトウェア定義を使用してください。このソフトウェア定義では、インストールタイプに関係なく特定のアプリケーションのインスタンスをクエリすることができます。

既知のソフトウェアが仮想アプリケーション イメージと関連付けられると、イメージ定義を封印できます。このアクションは、すぐにソフトウェア インベントリを更新し、イメージとリリースの間の新しい関連付けを反映させます。イメージのインスタンスが検出されたコンピュータには、そのインベントリ内に検出された仮想リリースが表示されます。

内容を変更する必要がある場合、仮想アプリケーション イメージ定義を再度封印解除できます。封印解除されると、イメージ定義が再度封印されるか、変更が破棄されるまで、イメージとリリースの間の既存の関連付けはアクティブなままです。



### 例 - ThinApp を使用して仮想アプリケーション イメージおよびソフトウェア定義を作成する

DSM 管理者は、Microsoft Office の仮想アプリケーション イメージを作成するために ThinApp を使用します。

CA ITCM Software Delivery 機能を使用して仮想アプリケーションを展開する場合、仮想アプリケーション パッケージ登録ウィザードが使用されます。（このウィザードの詳細については、「DSM エクスプローラ ヘルプ」の「ソフトウェア配信」を参照してください。）

登録の後、仮想アプリケーション イメージ定義を作成するように管理者にメッセージが表示されます。ソフトウェア配信ライブラリを使用しない場合、管理者は [仮想アプリケーション イメージ定義の新規作成] ダイアログ ボックスを使用して仮想アプリケーション イメージを登録することができます。（このダイアログの詳細については、「DSM エクスプローラ ヘルプ」の「ソフトウェア定義」を参照してください。）

DSM 管理者は、「Microsoft-TA」などのイメージ定義にふさわしい名前を選択します。

次に、管理者は [ソフトウェア定義] ツリーを参照し、Microsoft Word、Microsoft Excel 用に CA が提供した定義を検索します コピー および 貼り付けを実行すると、これらの既存のリリース定義は新しく作成された仮想アプリケーション イメージ定義と関連付けられます。すべての既知のコンテンツを仮想アプリケーション イメージ定義と関連付けた後、DSM 管理者がイメージを封印します。

プロビジョニング済みのパッケージのあるマシンのソフトウェア インベントリには、「Microsoft-TA」のステージ済み仮想アプリケーション イメージ、および Microsoft Word、Microsoft Excel などのスタンドアロンの仮想リリースが含まれます。仮想リリースは、同じアプリケーションの通常インスタンス共にクエリおよびレポートされる、既存リリースの特別なインスタンスです。

## ThinApp パッチおよびアップグレードのスキャン

ThinApp パッチおよびアップグレードは、元の **.exe** を置換するのではなく、新しいメイン コンテナを追加することによって実行されます。元のファイルが実行中の場合、新しいコンテナを検索し、現在のコンテンツを無視して、最新のコンテンツを代わりに使用します。

たとえば、以下のような ThinApp パッケージについて考えてみましょう。

- **winrar.exe** （元の ThinApp パッケージ）
- **winrar.001** （アップグレード ThinApp パッケージ）  
このファイルが存在する場合、**winrar.exe** の実行中にはこのファイルが代わりに実行されます。
- **winrar.002** （別のアップグレード ThinApp パッケージ）  
**winrar.exe** および **winrar.001** などよりも、このファイルが優先して選択されます。

元の ThinApp パッケージは、（アップグレード パッケージがディレクトリから削除されていない場合）常に最新のアップグレードを実行するので、シグネチャ スキャンでは、ThinApp パッケージの最新のバージョンのみが検出されます。

## 不明な仮想アプリケーション イメージの検出

仮想アプリケーションはエンドユーザーによってパッケージ化されるので、DSM 管理者は環境に存在する仮想アプリケーションの大部分を 把握する必要があります。把握することによって、適切なソフトウェア定義を作成できます。ただし、イメージが不足していたり、イメージを外部ソースから取得する場合があります。

シグネチャ スキャナは、検出されたにもかかわらず、ソフトウェア定義に一致しない仮想アプリケーション イメージをレポートすることができます。この機能はデフォルトでは無効に設定されているため、シグネチャ スキャナの設定で機能を有効にする必要があります。この設定には、DSM エクスプローラの [収集タスク] ノードからアクセスできます。

不明な仮想アプリケーション イメージは、DSM エクスプローラにリスト表示された各コンピュータの下の [エージェント] - [ソフトウェア] - [不明] サブノードにレポートされます。パッケージの仮想化テクノロジーがレポートされます。検出された不明な仮想アプリケーション イメージが DSM 管理者によって認識されていると判明した場合、そのイメージの仮想アプリケーション イメージ定義を自動的に作成できます。認識されていない場合、DSM 管理者は修正処理を開始し、不明なパッケージを詳しく調べることができます。

注: 不明な仮想アプリケーション イメージおよびそれらのソフトウェア定義の作成方法の詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

## 仮想アプリケーションのヒューリスティック スキャン

ヒューリスティック スキャナでは、仮想アプリケーション イメージ、およびそのイメージに含まれている仮想アプリケーションを特定するように設定できます。ヒューリスティック スキャナは、仮想アプリケーションとそのアプリケーションを含む仮想アプリケーション イメージを自動的に関連付けます。

[ヒューリスティック スキャナ] 設定ダイアログで、検出する仮想アプリケーション テクノロジーを選択できます。Microsoft App-V アプリケーションがインストールされている場合、クエリを実行することによって App-V Client が検出されます。ThinApp 仮想アプリケーションは、[スタート] メニューおよびデスクトップをスキャン中に検出されます。そのため、ThinApp のヒューリスティック検出が有効である場合、[スタート] メニューおよびデスクトップのスキャンが有効に設定されている必要があります。

## ヒューリスティック スキャナの制限事項

ヒューリスティック スキャナは、検出したとおりにソフトウェアを取得し、結果をレポートします。そのため、仮想アプリケーション イメージの外観を意図的に変更することによって、スキャナの検出動作を変更することができます。

ヒューリスティック スキャナは、検出するソフトウェアに対して新しいソフトウェア定義を作成します。ソフトウェアのこれらのインスタンスは、レポートまたはクエリ内でソフトウェア標準インスタンスと関連付けることはできません。

ヒューリスティック スキャナは、ストリーム配信仮想アプリケーションを検出できません。

そのため、企業内でソフトウェア インベントリのプライマリ ソースとしてヒューリスティック スキャナを使用していない場合、シグネチャ スキャナを使用して仮想アプリケーション イメージのインベントリを作成することをお勧めします。

## コンテンツ ユーティリティ

コンテンツ ユーティリティ ツールを使用すると、関連のない **Client Automation** インストール間でソフトウェア定義を共有できます。**CA Technologies** が提供する新規および更新されたソフトウェア定義は、インターネットにアクセス可能なオンライン ドメイン（またはエンタープライズ）マネージャへダウンロードした後、すべてのオフライン ドメイン（またはエンタープライズ）マネージャにインポートすることができます。

エクスポートされた定義はテキスト ファイルとして保存されます。また、このファイルは、同じネットワークの一部ではないインストールや、オフライン環境で稼働しているインストールと共有できます。

また、ソフトウェア定義は、共有ネットワーク ロケーションにあるファイルまたは **USB** デバイスなどのポータブル メディアにエクスポートした後、オフラインのインストールにインポートすることができます。

ユーティリティは **CA Technologies** 提供のソフトウェア定義およびカスタムのソフトウェア定義と共に機能し、コマンドライン ユーティリティとして利用できます。

## コンテンツ ユーティリティの実行

コンテンツ ユーティリティは、設定ファイル **content\_utility.xml** に記述されたアクションを実行するコマンドライン ツールです。

コンテンツ ユーティリティを実行するには、コマンドプロンプトで以下のコマンドを指定します。

**Contentutility.exe**

## コンテンツ ユーティリティの設定

コンテンツ ユーティリティを初めて実行すると、`content_utility.xml` という名前の設定ファイルが「インストールパス¥CA¥DSM¥bin フォルダ」に生成されます。以下のパラメータを設定するには、このファイルを設定する必要があります。

- エクスポート、インポート、またはその両方を行うかどうかを指定します。両方を行うことを選択した場合、エクスポートが完了した後にのみインポートが開始されます。
- エクスポートまたはインポートに `ca_intellisig`、`custom_intellisig`、および `intellisig_detail` を含むかどうかを指定します。
- CA から提供された定義、カスタム定義、またはその両方を処理するかどうかを指定します。
- エクスポート サーバ名およびインポート サーバ名を指定します。

初めて実行した後の `content_utility.xml` は、以下のようになります。

```
<contentutility_configuration>
 <general>
 <datadirectory>default</datadirectory>
 </general>
 <export>
 <manager>
 <hostname>machine001.ca.com</hostname>
 <enabled>yes</enabled>
 <ca_provided>no</ca_provided>
 <custom_created>yes</custom_created>
 <ca_intellisig>no</ca_intellisig>
 <custom_intellisig>yes</custom_intellisig>
 <intellisig_detail>yes</intellisig_detail>
 </manager>
 </export>
 <import>
 <manager>
 <hostname>machine101.ca.com</hostname>
 <enabled>yes</enabled>
 <ca_provided>no</ca_provided>
 <custom_created>yes</custom_created>
 <ca_intellisig>no</ca_intellisig>
 <custom_intellisig>yes</custom_intellisig>
 <intellisig_detail>yes</intellisig_detail>
 </manager>
 </import>
</contentutility_configuration>
```

## general セクション

このセクションには、以下のタグがあります。

### datadirectory

エクスポート ファイルおよびインポート ファイルの場所を定義します。デフォルトのパスは、**C:¥Documents and Settings¥All Users¥Application Data¥CA¥software\_definitions** です。

## Export セクション

このセクションでは、ファイルをエクスポートするための以下のパラメータを指定できます。

### hostname

エクスポートするファイルがある **DSM** マネージャの名前を定義します。

### ca\_provided

**CA** から提供された定義をエクスポートする必要があるかどうかを定義します。

### custom\_created

カスタム ソフトウェア定義をエクスポートする必要があるかどうかを定義します。

### enabled

ファイルをエクスポートするかどうかを指定します。

### ca\_intellisig

**ca\_intellisig** をエクスポートするかどうかを指定します。

### custom\_intellisig

**ca\_intellisig** をエクスポートするかどうかを指定します。

### intellisig\_detail

**ca\_intellisig** をエクスポートするかどうかを指定します。

## Import セクション

このセクションでは、ファイルをインポートするための以下のパラメータを指定できます。

### hostname

インポートするファイルがある DSM マネージャの名前を定義します。

### ca\_provided

CA から提供された定義をインポートする必要があるかどうかを定義します。

### custom\_created

カスタム ソフトウェア定義をインポートする必要があるかどうかを定義します。

### enabled

ファイルをインポートするかどうかを指定します。

### ca\_intellisig

Intellisigs をインポートするかどうかを指定します。

## コンテンツ ユーティリティ ログ ファイル

コンテンツ ユーティリティによって、エクスポートまたはインポートのステータスまたは結果を判別できるログ ファイルのセットが生成されます。以下のログ ファイルが「...¥DSM¥logs」の下に配置されます。

### ContentUtility.log

コンテンツ ユーティリティが起動された以降にユーティリティによって生成された情報が含まれます。

### ContentUtility[hostname].log

ホスト システムで実行されたアクションが含まれます。

### .out および .err ファイル

インポート中に生成された情報が含まれます。最後のインポート データで上書きされます。これらのファイルは、各プロセス テーブルのデータ ディレクトリで利用できます。

## 収集モジュール

アセット管理には、インベントリ検出モジュールとインベントリ テンプレート モジュールの 2 種類の収集モジュールが付属しています。

インベントリ検出モジュールには、ハードウェア インベントリ情報を収集するための指定が含まれています。インベントリ テンプレート モジュールでは、.MIF ファイルから収集する情報が定義されます。

これらのモジュールは、DSM エクスプローラの [コントロール パネル] - [設定] - [収集モジュール] で使用することができます。

**注：** ユーザ用にスケジュールされたテンプレートは、そのユーザがアセットにログインし、コンピュータ用にスケジュールされたテンプレートがそのスケジュール設定に応じてローカル システム アカウント (Windows) または root (Linux/UNIX) で実行されたときに実行されます。

## インベントリ検出モジュール

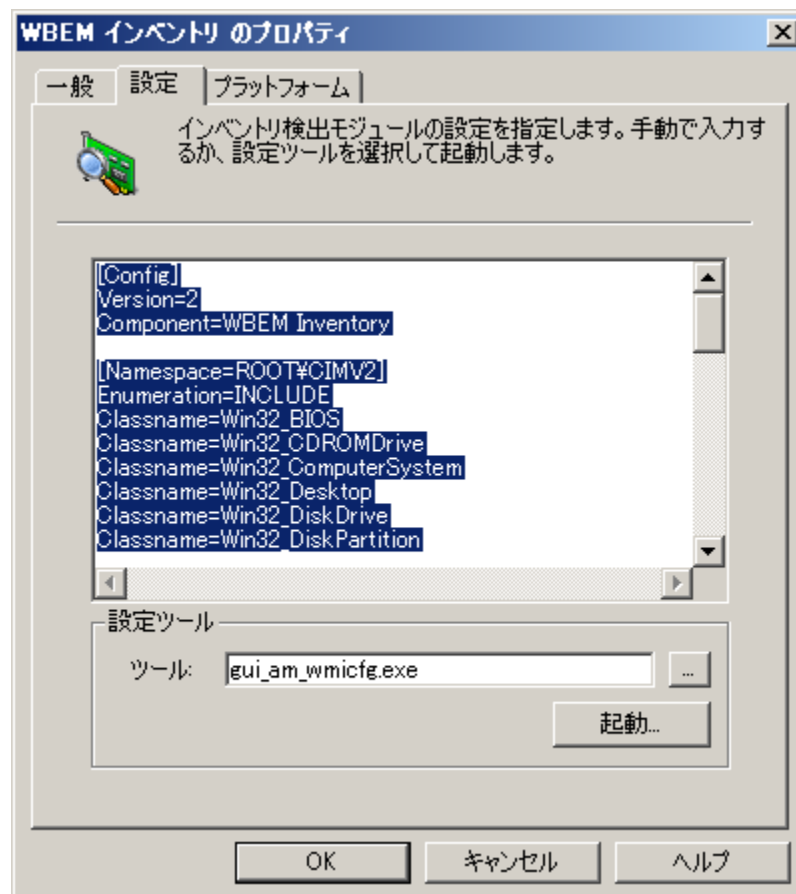
Asset Management エージェントには、一般、パフォーマンス、プリンタ、WBEM、ユーザ アカウント、ユーザ環境インベントリなど、基本および詳細なインベントリ情報を収集する定義済み検出モジュールのセットが備わっています。

インベントリ情報を収集するための指定は、以下のいずれかになります。

- 値を収集するためのコードが含まれている実行可能ファイル。このファイルは、エージェントのオペレーティングシステムによって異なる場合があります。アセットのオペレーティングシステムに基づいて、アセット管理によって適切なファイルが呼び出されます。
- インベントリを行う項目を起動および選択できる設定ツール。
- 設定情報を手動で入力します。



以下の図では、インベントリ検出モジュールのサンプル設定情報を示します。



注：新しいインベントリ検出モジュールの作成の詳細については、「DSM エクスプローラ ヘルプ」を参照してください。

関連項目：

[ハードウェア インベントリ](#) (P. 193)

## インベントリ検出モジュールの設定

既存のインベントリ検出モジュールを設定することにより、追加のインベントリ情報を収集することができます。最もよい例として、WBEM インベントリ モジュールの設定を上げることができます。このモジュールによって、Windows アセットからハードウェア インベントリ情報が収集されます。このモジュールに基づいて新しいモジュールを設定または作成し、追加のインベントリ情報を収集することができます。

**重要：**追加のインベントリ データを使用可能にするときには、注意が必要です。大量の情報を設定すると、膨大なデータが収集、転送、およびインポートされる可能性があります。このため、アセットに大きな負荷がかかり、ネットワーク パフォーマンスが大幅に低下する場合があります。

### WBEM インベントリ モジュールを設定する方法

1. WBEM インベントリ モジュールをダブルクリックします。  
[WBEM インベントリのプロパティ] ダイアログ ボックスが表示されます。
2. [設定] タブで [起動] をクリックします。  
[WMI 設定] ウィンドウが開きます。
3. モジュールに追加するインベントリ項目を選択し、[OK]をクリックします。  
インベントリ検出モジュールは、追加のインベントリ項目で設定されます。  
WBEM モジュールを収集タスクのいずれかに追加すると、収集タスクを実行しているアセットから追加のインベントリ項目を返すことができます。

### 関連項目：

[ハードウェア インベントリ収集タスクの作成、設定およびスケジュール \(P. 195\)](#)

## インベントリ検出モジュールの表示または変更

デフォルトで、検知モジュールにはインベントリ情報を収集する必要がある実行可能ファイルが定義されます。このようなインベントリを収集するためのソースがある場合、検知モジュールに関連付けられた実行可能ファイルの名前を変更できます。また、設定ツールを起動して、追加のインベントリ情報を収集したり、モジュールの実行をサポートしているプラットフォームを指定できます。

インベントリ検出モジュールを参照、または変更するには、モジュールをダブルクリックします。[検知モジュール] ダイアログ ボックスのプロパティが表示されます。必要に応じて、このダイアログ ボックスの設定を変更します。

注：このダイアログ ボックスの詳細については、「DSM エクスプローラ ヘルプ」を参照してください。

## インベントリ テンプレート モジュール

インベントリ テンプレート モジュールでは、MIF ファイルから収集する特定のインベントリ情報が定義されます。これらのモジュールを設定して、ログインしているユーザに入力を求めるプロンプトを表示できます。情報はエージェントによって MIF ファイルに書き込まれます。

アセット管理には、デフォルトのテンプレートであるユーザ テンプレートが用意されています。このテンプレートによって、会社およびユーザ情報が収集されます。ユーザ テンプレートは、[すべてのユーザ アカウント] グループ内にいるすべてのユーザにリンクしています。デフォルトでは、このテンプレートによってユーザに入力が要求されることはありません。入力を要求するには、テンプレート モジュールを設定する必要があります。

このテンプレートでは NCUSER.MIF ファイルを使用して会社およびユーザの情報を格納し、取得します。このファイルは、`C:\Program Files\CA\DSM\Agent\units\00000003\um` フォルダにあります。

新しいテンプレートを作成して、プリンタ、端末、ブリッジ、ルータなどの特定のデバイスに関する情報を収集することもできます。属性を収集するようスケジューリングされた時間になると、ユーザはテンプレートによって入力を要求されます。標準装備のテンプレート エディタを使用してテンプレートを作成し、必要なユーザおよびコンピュータに設定できます。

注：ユーザが設定したテンプレートは、そのユーザが（ドメイン内のいずれかの場所から）ログインし、コンピュータに設定されたテンプレートが Local System アカウントを使用して実行されたときに実行されます。テンプレートは、Windows エージェントでのみ使用できます。

関連項目：

[テンプレートインベントリの作成、設定およびスケジュール](#) (P. 217)

## ユーザ テンプレート インベントリの設定

ユーザ テンプレート インベントリ モジュールまたは他の任意のユーザ定義のモジュールを設定して、収集する属性およびユーザへの入力の要求タイミングを指定できます。

### ユーザ テンプレート インベントリ モジュールを設定する方法

1. [収集モジュール] - [インベントリ テンプレート モジュール] へ移動します。  
ドメインの既存のテンプレートが表示されます。
2. ユーザ テンプレート モジュールを右クリックし、[プロパティ] をクリックします。  
[ユーザ テンプレートのプロパティ] ダイアログ ボックスが表示されます。
3. [テンプレート エディタ] をクリックします。  
ツリー構造に収集された属性を表示した、[テンプレート エディタ] ダイアログ ボックスが表示されます。  
  
**注：** これらの属性の値が収集されると、ツリー構造はインベントリの下の、追加フォルダに複製されます。
4. 任意の属性を選択し、[属性の編集] をクリックします。  
[属性の編集] ダイアログ ボックスが表示されます。
5. [アクセス権] フィールドで [エンドユーザにプロンプト] または [エンドユーザにプロンプトして回答を必須とする] を選択し、[OK] をクリックします。
6. 値を要求する属性ごとに、手順 4 と 5 を繰り返します。  
次回エージェントを実行するときに、ユーザに入力を要求するプロンプトが表示されます。

**注：** テンプレート モジュールの作成、表示、変更の詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

## 新しいテンプレートの作成

テンプレートを作成して、ユーザ定義のインベントリ情報を収集することができます。

### 新しいテンプレートを作成する方法

1. [コントロール パネル] - [設定] - [収集モジュール] - [インベントリ テンプレート モジュール] フォルダに移動します。

右側のペインに既存のテンプレート モジュールが表示されます。

2. [タスク] セクションで [新規] をクリックします。

[テンプレートの新規作成] ダイアログ ボックスが表示されます。

3. モジュールの名前を入力し、[テンプレート エディタ] をクリックします。

[テンプレートの作成] ダイアログ ボックスが表示されます。

4. テンプレートの名前を入力し、ユーザに入力を要求する頻度を指定してから [OK] をクリックします。

[テンプレート エディタ] ダイアログ ボックスが表示されます。

5. グループを追加して、グループごとに属性を作成します。

**注：** 各属性の [アクセス権] フィールドに適切な値が選択されていることを確認してください。

表示されたこれらのグループおよび属性は、エージェント コンピュータから収集された場合と同じ構造を持ちます。

6. [OK] をクリックします。

指定した仕様の新しいテンプレートが作成されます。

新しいテンプレートは、いずれかの既存のテンプレート インベントリ収集タスクまたは新規収集タスクの作成で有効にすることができます。

**注：** 収集が済むと、このモジュールに入力されたデータは、[コンピュータおよびユーザ グループ] - [すべてのコンピュータ] - [コンピュータ] - [インベントリ] - [追加] - [テンプレート] フォルダから使用できます。

## 新しいテンプレートの作成： [ 一般 ] タブ

[一般] タブを使用して、テンプレートに関する一般情報を指定します。

このタブには以下のフィールドが含まれます。

### 名前

新しいテンプレートの名前を定義します。

### 説明

テンプレートについて簡単に説明します。

### テンプレート エディタ

ユーザに入力を要求するかどうかを指定する [\[テンプレートの作成\] ダイアログ ボックス](#) (P. 159)を開きます。

## 新しいテンプレートの作成： [ 詳細設定 ] タブ

[詳細設定] タブを使用して、テンプレート ファイル名を指定します。

注：通常はデフォルト値で十分です。変更する必要はありません。

このタブには、以下のフィールドが含まれています。

### ファイル名

収集されたテンプレート情報の保存先となる、テンプレート ファイルの名前を指定します。テンプレート ファイルでは、コンポーネントの管理属性が .MIF ファイル形式で記述されます。このファイルは、アセット管理エージェント ソフトウェアがエージェント コンピュータで実行された後、ローカルアセット管理エージェントディレクトリ（通常は、C:\Program Files\CA\DSM\Agent\units\000000001 または 000000003）に置かれます。

## [ テンプレートの作成 ] ダイアログ ボックス

[テンプレートの作成] ダイアログ ボックスを使用すると、ユーザが情報を更新する頻度を指定することができます。

このダイアログ ボックスには以下のフィールドが含まれます。

### 名前

コンポーネント名を表示します。プリンタ、ネットワーク コンポーネント、または全く異なるもの（たとえば、レンタルした機器やオフィス用品）の場合があります。

注：コンポーネント名はテンプレート エディタのグループ ヘッダです。

テンプレートが実行された後、このフィールドに入力した名前は関連するコンピュータのインベントリ/追加フォルダの下に表示されます。

### 説明

ヘッダ コンポーネントについて説明します。

### 属性の変更

ユーザに情報を要求するすべての属性をスケジュールします。

### プロンプト質問

この情報がユーザによって更新される頻度を指定します。

デフォルト：なし

使用できるオプションは、以下のとおりです。

#### なし

テキスト メッセージなしで、入力ボックスが表示されます。テキスト メッセージを表示しない場合は、このオプションを選択します。

#### 1 回

テンプレート収集タスクが実行された初回時にのみ、入力ボックスとテキスト メッセージが表示されます。

### 月に 1 回

月の指定した日に、入力ボックスとテキストメッセージが表示されます。

注：テンプレートの収集タスクは、その日について有効化されている必要があります。

### 定期的

入力ボックスとテキストメッセージが、スケジュールされたとおりに表示されます。経過後にモジュールが情報を収集する日数を指定することができます。

注：テンプレートの収集タスクは、その日について有効化されている必要があります。

### 常時

テンプレート収集タスクが実行されるたびに、入力ボックスとテキストメッセージが表示されます。

### プロンプトする前にテキストを表示

ユーザに対して情報を更新するようプロンプトで要求する前に、表示されるテキストを定義します。

### OK

テンプレートの構造を作成できる[テンプレートエディタ](#) (P. 161)を開きます。



## [ テンプレート エディタ ] ダイアログ ボックス

[テンプレート エディタ] ダイアログ ボックスを使用すると、作成しているテンプレートのグループおよび属性を追加することができます。グループ名をアセット番号や属性名にすることができます。グループはコンピュータ、モニタ、プリンタ、テーブル、およびチェアにすることができます。エンドユーザがこれらの属性に入力する値は、コンピュータ、モニタ、テーブルなどのそれぞれのアセット番号です。

このダイアログ ボックスには以下のフィールドが含まれます。

### 新規グループ

[新規グループの作成] ダイアログ ボックスが表示されます。新規グループの名前および簡単な説明を指定し、入力が完了したら [OK] をクリックします。指定した名前のグループが作成されます。このボタンをクリックして、任意の数のグループとサブグループを作成します。

テンプレートが実行された後に、ここに入力した名前がインベントリ/追加/テンプレート名/グループ名の下に表示されます。

### グループの削除

既存のグループを削除します。グループを選択して、[グループの削除] をクリックします。プロンプトが表示されたら、削除を確認します。

### グループの編集

[グループの編集] ダイアログ ボックスが開きます。グループのプロパティを編集します。

### 新規属性

新しい属性をテンプレートに追加します。左ペインのツリー構造でグループを選択し、属性を適切なグループに置きます。[新しい属性の作成](#) (P. 162)を参照してください。

### 属性を削除

既存の属性を削除します。属性を選択し、[属性を削除] をクリックします。プロンプトが表示されたら、削除を確認します。

### 属性を編集

属性の情報を編集できる [属性の編集] ウィンドウが開きます。

## [ 新規属性の作成 ] ダイアログ ボックス

[新規属性の作成] ダイアログ ボックスを使用して、テンプレート グループに追加する新しい属性を作成します。

このダイアログ ボックスには以下のフィールドが含まれます。

### 属性名

属性の名前を定義します。

テンプレートが実行された後、このフィールドに入力した名前が、インベントリ/追加/テンプレート名/グループ名/属性名 (右ペインのみ) の下に表示されます。この属性に入力した値も表示されます。

### 説明

テンプレートについて簡単に説明します。

### タイプ

このフィールドに入力するデータに合わせて、データ タイプを指定します。

#### 整数

64 ビットなどの整数のデータ タイプを指定します。

#### 文字列

256 文字 (最大長) などの文字列のデータ タイプを指定します。

#### ユーザ定義

[ユーザ定義タイプ] セクションで、属性のユーザ定義値の数を定義することができます。エージェント コンピュータで値を要求するプロンプトが表示された場合、このフィールドに指定した値がドロップダウン リストに表示されます。

## アクセス権

「エンドユーザにプロンプト」や「使用可能にする」などの、新しい属性のアクセス タイプを指定します。

### 読み取り専用

値が読み取り専用であることを指定します。この値は、属性の作成時に事前定義されます。値を要求するプロンプトは表示されません。これは、テンプレート ファイル属性に対する標準の DMI 仕様アクセス タイプです。

### 使用可能にする

値を編集可能にします。

### エンド ユーザにプロンプト

エージェント コンピュータのユーザにプロンプトを表示し、属性の値を入力できるようにします。

### エンド ユーザにプロンプトして回答を必須とする

ユーザに値を要求するプロンプトを表示し、強制的に解答の入力を促します。このアクセス タイプを選択すると、属性の値を入力することができ、値を入力した場合にのみ先に進む入力ボックスがアセット管理エージェントに表示されます。

## ユーザ定義タイプ

「タイプ」フィールドで「ユーザ定義」を選択した場合、このセクションの「追加」および「削除」ボタンが起動されます。

## 値

ユーザ定義データ タイプの値のリストを指定します。「追加」または「削除」ボタンをクリックして、値を追加、削除します。値の入力を要求するプロンプトが表示された場合は、ドロップダウンリストに表示される値から選択します。「値」フィールドの横にある「ソート」ボタンをクリックすると、値を昇順または降順でソートすることができます。

タイプとして「整数」または「文字列」を選択した場合は、このフィールドにデフォルト値を指定することができます。プロンプトが表示されたら、デフォルト値を保存するか、変更することができます。たとえば、すべての新しいコンポーネントを1つのグループに保持する場合、このグループをデフォルト値として入力することができます。入力すると、このグループは自動的にテンプレート ファイルに表示されます。

## 既存のインベントリ テンプレートの表示または変更

テンプレートを変更して、グループおよび属性を追加、編集、削除できます。

### テンプレートを表示または変更する方法

1. 「コントロール パネル」 - 「設定」 - 「収集モジュール」 - 「インベントリ テンプレート モジュール」 フォルダに移動します。  
右側のペインに既存のテンプレートが表示されます。
2. 表示または編集するコマンドをダブルクリックします。  
選択したテンプレートの「プロパティ」ダイアログ ボックスが表示されます。
3. 「テンプレート エディタ」 をクリックします。  
テンプレートで定義されたグループおよび属性が表示された [「テンプレート エディタ」ダイアログ ボックス \(P. 161\)](#)が表示されます。
4. 「グループの編集」 または 「属性の編集」 をクリックして、それぞれのテンプレートのグループまたは属性を変更し、「OK」 をクリックします。  
テンプレート モジュールの変更内容が保存されます。

## アセットへのテンプレートの設定

テンプレート インベントリで設定されたインベントリを収集するには、アセットにインベントリを設定する必要があります。以下のいずれかの方法を使用します。

### 方法 1

1. [コントロール パネル] - [設定] - [収集モジュール] に移動し、[インベントリ テンプレート モジュール] をクリックします。

右側のペインに、すべての使用可能なテンプレートが表示されます。

2. 必要なテンプレート モジュールを、情報の収集元となるアセットまたはグループにドラッグしてリンクします。

選択されたテンプレート モジュールは、アセット上で設定されます。設定されたテンプレートは、[コンピュータ/ユーザ グループ] - [すべてのコンピュータ] - アセット名 - [設定] - [収集タスク] フォルダに置かれます。

### 方法 2

1. 必要なアセットに移動し、[設定] フォルダをクリックします。
2. [収集タスク] を右クリックし、コンテキスト メニューから [新規] をクリックします。

[新しい収集タスク タイプの選択] ダイアログ ボックスが表示されます。

3. [テンプレート インベントリ] を選択し、[OK] をクリックします。
4. [テンプレート] タブをクリックし、アセット上で実行する必要がある単一のテンプレートまたは複数のテンプレートを選択し、[OK] をクリックします。

選択されたテンプレート モジュールは、アセット上で設定されます。

## デバイス コンプライアンス スキャナ ( DCS )

デバイス コンプライアンス スキャナ (DCS) は、SCAP (Secure Content Automation Protocol) を使用して NIST (National Institute for Standards and Technology、国立標準技術研究所) が作成した チェックリストに基づいてターゲット コンピュータを自動的に評価します。

この製品のリリース時に NIST によって公表された FDCC チェックリストは、DCS をインストールする時にデフォルトでインストールされます。スキャナは、古いまたは新しい FDCC チェックリストを含め、有効な SCAP データ ストリームに対してコンプライアンス チェックを実行します。追加またはカスタムのチェックリストを使用して、スキャナがコンプライアンス チェックを実行するように設定できます。

## 本リリースにバンドルされた FDCC チェックリスト

以下のチェックリストが本リリースにバンドルされています。

- Windows XP チェックリスト
- Windows Vista チェックリスト
- Windows XP ファイアウォール チェックリスト
- Windows Vista ファイアウォール チェックリスト
- IE7 チェックリスト

上記チェックリストの詳細については、<http://nvd.nist.gov/fdcc/index.cfm> にアクセスしてください。

注：チェックリストが有効な SCAP データ ストリームであれば、スキャナはさらに追加のチェックリストを処理可能です。

## チェックリストの配布方法

DCS スキャンがエージェント コンピュータをスキャンする場合、エージェント コンピュータ用の **SCAP** チェックリストが必要です。以下のプロセスは、チェックリストをエージェント コンピュータに自動的に配布する方法、およびチェックリストの自動的な配布に必要なアクションを説明しています。

1. DCS がドメイン マネージャにインストールされる場合、**Client Automation** インストーラは、バンドルされている **FDCC** チェックリストをドメイン マネージャの **ITCM\_installpath¥SCAP\_Checklists** ディレクトリにコピーします。

注：カスタム チェックリストまたは更新したチェックリストがある場合は、それらを「**SCAP\_Checklists**」ディレクトリの下の新規ディレクトリに手動でコピーします。

2. **DSM** エンジンがデフォルトの **SCAP** チェックリストプロセス ジョブを実行して、以下のタスクを実行します。
  - ドメイン マネージャの **SCAP\_Checklists** ディレクトリを監視して、チェックリスト（新規またはアップデート）の更新を調べます。
  - 新規またはアップデートされたチェックリストを圧縮アーカイブ ファイルにパッケージ化し、それらにデジタル処理で署名して、データが改ざんされるのを防ぎ、**¥Documents and Settings¥All Users¥Application Data¥CA¥scap\_checklists** ディレクトリの下に保存します。
  - 新規およびアップデートされたチェックリストのリストを使用して **MDB** を更新します。
  - 新規およびアップデートされた各チェックリストのインベントリ検出モジュールを作成または更新します。

3. DSM エンジンがエンジン収集タスクを実行して、新規またはアップデートされたチェックリストの圧縮アーカイブ ファイルをスケーラビリティ サーバにプッシュします。
4. チェックリストをスキャンするように設定されているハードウェア インベントリ収集タスクをエージェントが実行する場合、エージェントはスケーラビリティ サーバから必要となる新規またはアップデートされたチェックリストの圧縮アーカイブ ファイルをプルし、エージェント コンピュータに保存します。
5. エージェントは、圧縮アーカイブ ファイルの署名を確認します。 書名の確認ができない場合、長いエントリが **TRC\_AMAGENT\*.log** ファイルに追加されます。

DSM 基本ホスト ID 証明書の変更のために署名の確認が失敗した場合、チェックリスト ファイルを再配布してください。

注： チェックリスト ファイルをスケーラビリティ サーバに配布するには、[スケーラビリティ サーバへの SCAP チェックリストの配布] 設定ポリシーをはいに設定する必要があります。 このポリシー（デフォルトでは「いいえ」に設定）は、DSM エクスプローラ ツリーの [設定ポリシー] - [デフォルト コンピュータ ポリシー] - [DSM] - [マネージャ] - [エンジン] にあります。

## 圧縮済みチェックリストの署名用の基本ホスト ID 証明書

圧縮されたチェックリスト ファイルのデジタル署名は、DSM 基本ホスト ID 証明書（**dsmcommon** と呼ばれる）を使用して作成されます。 生成された署名は、圧縮されたチェックリスト ファイルとともにスケーラビリティ サーバに送られます。 DCS スキャン実行時に、この場所から **Asset Management** エージェントがチェックリストを取得します。 エージェントは、圧縮されたチェックリスト ファイルの署名を確認し、署名が正常に確認された場合のみスキャンを続行します。



## 証明書変更時のチェックリストの再配布

チェックリストが署名され配布された後に基本ホスト ID 証明書が変更された場合、エージェントでの署名の確認は失敗し、設定された DCS インベントリ モジュールは実行しません。この問題を解決するには、チェックリストのバージョンを変更して、新しく生成された署名とともに、スケーラビリティ サーバおよび Asset Management エージェント コンピュータに再配布します。

### 証明書変更時にチェックリストを再配布する方法

1. ドメインマネージャで `checklist_xccdf.xml` ファイルを開き、`<version>` タグを見つけます。
2. バージョン番号を変更して、チェックリストの再配布を有効にします。

注：新しいチェックリストがリリースされたときに、バージョン番号の競合が発生しにくいように、以前のバージョン番号を指定することをお勧めします。

3. XCCDF ファイルを保存します。
4. [DSM エクスプローラ] を表示し、変更されたチェックリストが圧縮され署名されるように、デフォルトの SCAP チェックリストプロセス ジョブを実行します。

これで、チェックリストはスケーラビリティ サーバに再配布する準備ができました。

## DCS の仕組み

DCS は Asset Management インベントリ検出モジュールとして実装されます。このインベントリ検出モジュールをハードウェア インベントリ収集タスクの一部として設定することができます。以下の手順は、スキャナの動作の仕組み、およびスキャナの動作に対して必要なアクションを理解するのに役立ちます。

1. Client Automation では、「*ITCM\_Installpath¥SCAP\_Checklists*」フォルダの下に配置されたすべてのチェックリストに対して、インベントリ検出モジュールを自動的に作成します。
2. 1つ以上のハードウェア インベントリ収集タスクを設定し、スキャンおよび FDCC インベントリ検出モジュールからの結果の収集をスケジュールします。新しい収集タスクを作成するか、またはスキャンをスケジュールする既存の収集タスクを変更できます。
3. 収集タスクがエージェント コンピュータで実行されると、エージェント コンピュータで使用可能なチェックリストに基づいて、スキャナがスキャンを開始します。各チェックリストには、SCAP データ ストリームがあります。SCAP データ ストリームは、以下のファイルから構成されます。
  - ルール セットを定義する XCCDF (eXtensible Configuration Checklist Description Format) ファイル
  - XCCDF ファイルで定義されたルールを使用して、コンプライアンスのチェック方法を指定する 1つ以上の OVAL (Open Vulnerability and Assessment Language) ファイル
  - (オプション) CPE (Common Platform Enumeration) ディクショナリ ファイル。ターゲット システムに必要なオペレーティング システムまたはアプリケーションが存在するかどうかをチェックする方法を指定します。たとえば、Windows XP 用のチェックリストの場合、CPE ディクショナリ ファイルは、ターゲット システムに Windows XP が存在するかどうかをチェックする方法を指定します。

4. スキャナは、XCCDF ファイル内のルールを解析し、OVAL インタープリタを起動して、SCAP データ ストリームで参照されている OVAL 定義を評価します。
5. インタープリタは、各 OVAL 定義の値を含む OVAL 結果ファイルを作成します。
6. スキャナは、結果ファイルを読み込み、チェックリスト内の各ルールについてコンプライアンス チェックの結果を判別し、以下の ファイルを作成します。

- XCCDF コンプライアンス テスト 結果ファイル (XML 形式)
- Asset Management インベントリ ファイル

注：すべての結果ファイルは、Asset Management エージェントの作業ディレクトリ以下のサブディレクトリに保存されます。

7. インベントリ ファイルの情報は、MDB (management database、管理データベース) に保存されます。スキャンの結果は、DSM エクスプローラおよび Web コンソールに表示されます。他の任意のインベントリ データで行うのと同様に、このインベントリ情報に基づいて、クエリとレポートを作成できます。

## エージェント コンピュータからの結果ファイルの収集

スキャナは、XCCDF および OVAL 結果ファイルを、デフォルトで、エージェント コンピュータに保存します。FDCC インベントリ 検出モジュールを設定して、エージェント コンピュータの結果ファイルをスケーラビリティ サーバに集めることを有効にすることができます。エンジンが次回収集タスクを実行する際には、スケーラビリティ サーバから結果ファイルを収集して、それらをドメインマネージャに保存します。結果ファイルをドメインマネージャに保存すると、それらを集中的に管理し、必要なときに迅速にファイルを取り出すことが容易にできます。

注：結果ファイルは、エージェントとマネージャ間でデータが改ざんされるのを防ぐために、デジタル署名を使って署名されています。マネージャが署名を確認できない場合、イベントが発生し、デフォルトのイベントログに記録されます。

関連項目：

[結果ファイルの場所の変更 \(P. 174\)](#)

## スキャナの設定

以下のセクションでは、インベントリ用のスキャナを設定する手順について記述します。

## Windows ファイアウォール設定の変更

Client Automation が正しく機能することを確認するために、FDCC 準拠の Windows XP および Windows 7 コンピュータ上のある特定のファイアウォール設定を変更する必要があります。

以下の手順に従います。

1. [スタート] - [ファイル名を指定して実行] をクリックし、[名前] プロンプトで「gpedit.msc」と入力します。
2. [ローカル グループ ポリシー エディター] ウィンドウで、[コンピュータの構成]-[管理用テンプレート]-[ネットワーク]-[ネットワーク接続]-[Windows ファイアウォール] - [標準プロファイル] パスのポリシーを検索します。
3. [Windows ファイアウォール: 例外を許可しない] ポリシー設定を [無効] に変更します。
  - [Windows ファイアウォール: ローカル ポートの例外を許可する] ポリシー設定を [有効] に変更します。ファイアウォールで例外ポートに、以下のポートを追加します。
    - TCP ポート 4105
    - UDP ポート 4104
    - TCP ポート 4728

Client Automation 製品の内部通信メカニズムは、ここで説明するポートを使用します。これらのポートにアクセスできない場合、Client Automation は動作できません。アクセスなしでは、エージェントは、そのマネージャやレポート インベントリまたはステータスに問い合わせることができません。また、マネージャからエージェントに制御メッセージを渡すことができません。これらのポート上の通信は、Client Automation 製品によって確実に暗号化され管理されます。Client Automation リリース 12.9 は、FIPS 準拠の暗号化を使用します。

## テスト結果ファイル収集の設定

通常、FDCC インベントリ検出モジュールは、テスト結果ファイルの収集設定以外は、詳細な設定を必要としません。XCCDF および OVAL テスト結果ファイルは、Asset Management エージェントの作業ディレクトリの下のサブディレクトリに保存されます。スキャン後にこれらのファイルを収集し、ドメイン マネージャに集中管理して保存するには、DCS インベントリ検出モジュールを構成して、結果ファイルの自動収集を有効にします。

注：インベントリ検出モジュールに別のパラメータを設定する場合、「追加チェックリスト用にインベントリ検出モジュールを作成する」で各パラメータの説明を参照してください。

### テスト結果ファイル収集の設定方法

1. [コントロール パネル] - [設定] - [インベントリ検出モジュール] に移動します。

新しい DCS インベントリ検出モジュールが、他のインベントリ検出モジュールとともに表示されました。

2. 設定する [インベントリ検出モジュール] をダブルクリックします。  
[モジュール名] 用のプロパティ ダイアログ ボックスが表示されます。
3. [設定] タブの [起動] ボタンをクリックします。  
[SCAP 設定] ダイアログ ボックスが既存の設定で表示されます。
4. [一般] タブで以下のチェックボックスを選択します。

- XCCDF 結果ファイルの収集
- OVAL 結果ファイルの収集

注：通常の場合、OVAL テスト結果ファイルは約 10 MB です。それらをドメイン マネージャに保存する特別な理由がない場合、XCCDF 結果ファイルのみを収集します。

5. [OK] をクリックします。

収集タスクをもう一度実行すると、エンジンはテスト結果ファイルを収集し、それをドメイン マネージャに保存します。

注：結果ファイルは、エージェントとマネージャ間でデータが改ざんされるのを防ぐために、デジタル署名を使って署名されています。マネージャが署名を確認できない場合、イベントが発生し、デフォルトのイベントログに記録されます。

関連項目：

[結果ファイルの場所の変更 \(P. 174\)](#)

## 結果ファイルの場所の変更

エージェントからの収集した **SCAP** 結果ファイルを設定する場合、デフォルトでは結果ファイルの保存先は、ドメインマネージャの **ITCM\_installpath¥SCAP\_Result\_Files** ディレクトリとなります。結果ファイルの場所は、必要に応じて変更できます。

結果ファイルの場所を変更するには、[デフォルトのコンピュータ ポリシー] - [DSM] - [マネージャ] - [アセット管理] にある、[**SCAP 結果ファイルの場所**] を設定する設定ポリシーを変更します。収集タスクが次回実行される際に、エンジンはテスト結果ファイルを収集し、それを指定したディレクトリに保存します。

## ハードウェア インベントリ収集タスクの収集 DCS インベントリへの設定

FDCC チェックリスト スキャンのスケジュールおよびテスト結果の収集を行うには、ハードウェア インベントリ収集タスクを設定します。

注：複数のハードウェア インベントリ収集タスクがある場合、チェックリスト スキャンのスケジュールをそれらすべてについて行うのか、または選択したいくつかのみに行うのかを決定します。たとえば、すべての **Windows Vista** コンピュータをグループ化し、そのグループ用の特定の収集タスクを作成する場合、収集タスクを **WinVista**、**VistaFirewall**、および **IE7** チェックリストに対して設定することができます。ただし、すべてのコンピュータにチェックリストを設定したとしても、スキャナは **OS** 要件に適合したコンピュータのみをスキャンします。

### ハードウェア インベントリ収集タスクを設定する方法

1. **DSM** エクスプローラで、[コントロール パネル] - [設定] - [収集タスク] - [ハードウェア インベントリ] に移動します。  
既存のハードウェア インベントリ収集タスクが表示されます。
2. 設定する収集タスクを右クリックして、[プロパティ] を選択します。  
収集タスクのプロパティのダイアログ ボックスが表示されます。
3. [検出モジュール] タブをクリックして、**DCS** [インベントリ検出モジュール] を選択し、[OK] をクリックします。  
変更内容が保存されます。収集タスクが次回実行される際に、設定したチェック リストでスキャン結果が収集されます。

## ( オプション ) SCAP インベントリ用のインベントリ検出モジュールの作成

Client Automation では、「SCAP\_Checklists」フォルダの下に配置されたすべての FDCC チェックリストに対して、インベントリ検出モジュールを自動的に作成します。既存のチェックリストの新バージョンを「SCAP\_Checklists」フォルダの下の新規フォルダにコピーすると、チェックリストの既存のインベントリ検出モジュールは最新のバージョンの情報で更新されます。スキャン用に別のバージョンのチェックリストを使用することが必要な場合があります。この場合、現在使用するように設定されていないバージョンのインベントリ検出モジュールを手動で作成する必要があります。たとえば、インベントリ検出モジュールが常に最新バージョンをスキャンするように設定されている場合、同じバージョンをスキャンに使用する場合には、任意の古いチェックリストバージョンのインベントリ検出モジュールを作成できます。

### インベントリ検出モジュールを作成する方法

1. [DSM エクスプローラ] で、[コントロール パネル] - [設定] - [収集モジュール] - [インベントリ] - [検出モジュール] に移動します。

右ペインに既存の検出モジュールが表示されます。

2. [インベントリ検出モジュール] フォルダを右クリックして、コンテキストメニューから [新規] をクリックします。

[インベントリ モジュールの新規作成] ダイアログ ボックスが表示されます。

3. [一般] タブで、インベントリ モジュール名を指定します。チェックリスト名を示す名前を指定します。
4. [設定] タブで、SCAP インベントリ検出用の設定を指定します。FDCC IE7 チェックリスト用のサンプル設定を以下に示します。

```
[SCAP]
SCAPPath=FDCC-Major-Version-1.2.1.0¥ie7
XCCDFFile=fdcc-ie7-xccdf.xml
XCCDFID=fdcc-ie-7
XCCDFVersion=v1.2.1.0
XCCDFVersionOptions=v1.2.1.0Profileoptions=v1.2.1.0;Federal Desktop Core
Configuration version 1.2.1.0; CPEDictionary=fdcc-ie7-cpe-dictionary.xml
CollectXCCDFResultFile=false
CollectOVALResultFiles=false
OvaldiPath=ovaldi-ca
InvComponent=$SCAP$FDCC IE7
```

注：パラメータおよびその説明の詳細については、付録の「SCAP 設定パラメータ」を参照してください。

5. [プラットフォーム] タブで、[Windows 32 ビット] を選択し、[Win32 一般] をクリックしてから、オプション ボタンに隣接するテキスト フィールドに「**amiscap.exe**」in を入力します。
6. [OK] をクリックします。

設定されたチェックリストのインベントリ検出モジュールが作成され、[インベントリ検出モジュール] フォルダの下に表示されます。1 つまたは複数のハードウェア インベントリ 収集タスクを設定して、新しいインベントリ検出モジュールを含めます。

## 追加の SCAP データ ストリーム

このリリースにバンドルされたチェックリストに加えて、スキャナはすべての有効な SCAP データ ストリームをスキャンします。追加の SCAP データ ストリームには、新規、またはアップデートした FDCC チェックリスト、カスタム チェックリスト、またはすべてのソースからの SCAP データが追加できます。

## 追加の SCAP データ ストリームの設定方法

Client Automation は、追加の SCAP データ ストリームをターゲット エージェント コンピュータに自動的に配布できます。追加の SCAP データ ストリームを自動配布に設定すると、以下のタスクが必要になります。

1. SCAP データ ストリームをドメイン マネージャにコピーする
2. [ハードウェア インベントリ収集タスクの設定](#) (P. 174)

## SCAP データ ストリームのドメイン マネージャへのコピー

DCS のスキャンで使用するチェックリスト ファイル (SCAP データ ストリーム) は、ドメイン マネージャの特定のディレクトリで使用可能である必要があります。デフォルトの SCAP チェックリスト処理ジョブを実行する場合には、DSM エンジンがこのディレクトリでチェックリストが新規に作成されたかまたはアップデートされたかをチェックします。

SCAP データ ストリームをドメイン マネージャの

「*ITCM\_installpath*¥SCAP\_Checklists」ディレクトリの下の新規ディレクトリにコピーします。

**注:** SCAP データ ストリームまたはそのディレクトリのチェックリストに属するすべてのファイルを SCAP\_Checklists ディレクトリに配置する必要があります。



## SCAP 設定のエクスポート

[SCAP 設定] ダイアログ ボックスから設定情報の設定を .CFG ファイルにエクスポートできます。カスタム、または追加の SCAP データ ストリーム用のインベントリ検出モジュールを作成する場合に、このファイルを使用して [SCAP 設定] ダイアログ ボックスで環境設定情報をインポートすることができます。

### SCAP 設定をエクスポートする方法

1. エクスポートする SCAP 設定の DCS インベントリ検出モジュールをダブルクリックします。  
[モジュール名] 用のプロパティ ダイアログ ボックスが表示されます。
2. [設定] タブで、gui\_am\_scapcfg.exe 設定ツールを使用することを確認します。
3. [起動] をクリックします。  
[SCAP 設定] ダイアログ ボックスが既存の設定で表示されます。
4. ダイアログ ボックスの左上隅のシステム メニュー アイコンから、[設定のエクスポート] を選択します。  
[Save As] ダイアログ ボックスが表示されます。
5. ファイル名を指定して、[保存] をクリックします。  
これで、設定は指定した場所のファイルにエクスポートされます。

## SCAP 設定のインポート

インベントリ検出モジュールを作成する場合、SCAP 設定ファイルから [SCAP 設定] ダイアログ ボックスに情報をインポートできます。SCAP 設定をインポートすると、[SCAP 設定] ダイアログ ボックスのそれぞれのフィールドに設定の詳細が入力されます。

### SCAP 設定をインポートする方法

1. 新規インベントリ モジュールの [SCAP 設定] ダイアログ ボックスで、左上隅のシステム メニュー アイコンから [設定のインポート] を選択します。  
[インポートするファイルを選択] ダイアログ ボックスが表示されます。
2. 有効な SCAP 設定ファイルを選択し、[開く] をクリックします。

設定情報が [SCAP 設定] ダイアログ ボックスのそれぞれのフィールドにインポートされます。

以下に、サンプルの SCAP 設定ファイルの内容を示します。

```
[SCAP]
SCAPPath=FDCC-Major-Version-1.2.1.0¥ie7
XCCDFFile=fdcc-ie7-xccdf.xml
XCCDFID=fdcc-ie-7
CPEDictionary=fdcc-ie7-cpe-dictionary.xml
InvComponent=$SCAP$FDCC IE7
CollectXCCDFResultFile=false
CollectOVALResultFiles=false
OvaldiPath=ovaldi-ca
```

## スキャン結果の処理

以下のセクションでは、スキャン結果を使用して何を実行できるかについて説明します。

## スキャナによりレポートされた結果

コンプライアンス チェック後、スキャナは XCCDF ファイル内の各ルールに対する以下の結果をレポートします。

### 合格

選択したルールに対して、コンピュータがコンプライアンス チェックに合格したことを示します。

### 不合格

選択したルールに対して、コンピュータがコンプライアンス チェックに不合格となったことを示します。

### エラー

選択したルールに対して、コンプライアンス チェックを実行時にエラーが発生したことを示します。

### 未確認

ルールに定義されたチェックが含まれていないため、スキャナがコンプライアンス チェックを実行できないことを示します。

### 不明

評価する特性が見つからないか、または特性が見つかったが、収集されたオブジェクト フラグが「収集不可」であることを示します。

### 適用不可

ルールが、エージェント コンピュータにインストールされたオペレーティング 環境に適用できないことを示します。

## スキャン結果の表示

スキャン結果を表示して、エージェント コンピュータがコンプライアンス チェックに合格か不合格かを確認します。結果は、**XCCDF** ファイルの各ルールと照合して示されます。**DSM** エクスプローラおよび **Web** コンソールは、スキャン結果を読み取りやすい形式で表示します。**XCCDF** および **OVAL** テスト結果ファイルを開いて、スキャン結果を表示することもできます。

### 結果ファイルからスキャン結果を表示する方法

以下のディレクトリに移動して、**XCCDF** および **OVAL** テスト結果ファイルを表示します。

- エージェント コンピュータの エージェント作業ディレクトリ  
¥SCAP\_Result\_Files
- テスト結果ファイルのコレクションを設定している場合、ドメイン マネージャの *ITCM\_installpath¥SCAP\_Result\_Files*

注： 前述のパスはテスト結果ファイルのデフォルトの場所です。

### GUI からスキャン結果を表示する方法

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] - [SCAP] - [インベントリ コンポーネント名] に移動します。

注： [インベントリ コンポーネント名] は、インベントリ検出モジュールを作成したときに、[SCAP 設定] ダイアログの [インベントリ ノード名] フィールドで指定した値です。

選択したインベントリ コンポーネントのスキャン結果は、さまざまなサブノードに表示されます。スキャン結果の詳細については、「**DSM** エクスプローラ ヘルプ」を参照してください。

## クエリおよびレポート

他のインベントリ データで行うのと同様に、**DCS** によって作成された結果に基づいて、クエリまたはレポートを作成できます。クエリおよびレポートの詳細については、「**DSM** エクスプローラ」オンライン ヘルプおよび「**DSM** レポータ」オンライン ヘルプを参照してください。

## 定義済みレポート テンプレート

DSM レポートは、以下に示す DCS スキャン結果用 Client Automation リリース 12.9 事前定義済みレポート テンプレートを提供します:

### SCAP スキャン サマリ

ドメインマネージャの各コンピュータにスキャン結果のサマリをレポートします。

### フラット スコア

ドメインマネージャの各コンピュータにフラット スコア結果をレポートします。

### ルール結果の概要

特定のコンピュータ用のチェックリストにおけるルールすべてのスキャン結果をレポートします。このレポート機能は、ルール結果の概要を表示するコンピュータを絞り込む、ランタイム クエリを起動します。

### パッチ結果の概要

特定のコンピュータ用のチェックリストにおけるパッチすべてのスキャン結果をレポートします。このレポート機能は、パッチ結果の概要を表示するコンピュータを絞り込む、ランタイム クエリを起動します。

### SCAP 入力ファイル情報

特定のコンピュータで DCS スキャンに使用される入力ファイル (SCAP データ ストリーム) の詳細をレポートします。このレポート機能は、入力ファイル情報を表示するコンピュータを絞り込む、ランタイム クエリを起動します。

### SCAP 出力ファイル情報

特定のコンピュータで DCS スキャンによって作成される結果ファイルの詳細をレポートします。このレポート機能は、出力ファイル情報を表示するコンピュータを絞り込む、ランタイム クエリを起動します。

## DCS ログ ファイル

DCS ログは、エージェント コンピュータで以下のログ ファイルに追加されます。

### TRC\_UAM\_\*.log

これには、チェックリスト ファイルの圧縮および解凍、チェックリスト ファイルの署名の作成と確認、および実際のチェックリスト プロセスに関連するログが含まれます。

### TRC\_AMAGENT\*.log

これには、チェックリスト ファイルの圧縮および解凍、チェックリスト ファイルの署名の作成と確認、および実際のチェックリスト プロセスに関連するログが含まれます。

### TRC\_AMRAPI\*.log

これには、チェックリスト ファイルの転送、および結果ファイルのエージェントへの転送およびエージェントからの転送に関連するログが含まれます。

マネージャの場合、DCS スキャナ ログは以下のファイルに追加されます。

### TRC\_AMSCAP\_FTPLUGIN\*.log

これには、XCCDF 結果ファイルの転送、OVAL 結果ファイルの転送、および圧縮チェックリスト ファイルの DSM エンジンへの転送および DSM エンジンからの転送に関連するログが含まれます。

ログ ファイルは、*ITCM\_installpath¥logs* ディレクトリ以下にあります。これらのログ ファイルとは別に、スキャナは各 OVAL ファイル用の OVAL インタープリタの実行結果を、エージェント コンピュータのチェックリスト出力ディレクトリ下の *ovalfilename-ovaldi-stdout.txt* ファイルにも保存します。

## ファイル収集

アセット管理を使用すると、ネットワーク上のシステム設定ファイルを一元的に管理することができます。管理対象アセット上の設定グループをバックアップし、データベース内の設定ファイルの各種のバージョンを保持することができます。これは、ファイルの以前のバージョンをプッシュ バックするのに役立ちます。

注：ファイル収集は、Windows エージェントでのみ使用できます。

AUTOEXEC.BAT、CONFIG.SYS、WIN.INI、SYSTEM.INI、または NET.CFG などの設定ファイルのバックアップ コピーの名前および番号を設定することができます。また、特定のバックアップ ファイルのセットをグループ レベルで定義して、ユーザ単位でのバックアップの設定に多くの時間を費やすことなく、さまざまなネットワーク グループやユーザのニーズを満たすことができます。アセット管理エージェントの実行中は、常に設定ファイルが変更されたかどうかチェックされます。変更された場合は、DSM エクスプローラが以前および現在のファイル内容で更新されます。

以下の理由により、ファイル収集は、ユーザ レベルで設定するよりもコンピュータ レベルで設定するほうが効率的です。

- エージェントでは、ファイルの収集にローカル システム アカウントのクレデンシャルが使用されます。これらのユーザ アカウントにはすべてのファイルへの完全なアクセス権があります。反対に、ユーザ レベルで設定した場合には、ファイルの収集にユーザのクレデンシャルが使用されます。ユーザにファイルへのアクセス権がない場合、ファイル収集は失敗します。
- ファイル システムはコンピュータによって保持され、各ユーザのファイルのコピーは存在しないため、ファイル収集をユーザ レベルで設定するのはあまり有益ではありません。
- ファイル収集をユーザ レベルで設定した場合、同じファイルの複数のコピーが各ユーザに作成されます。このことは、データベースのパフォーマンスに深刻な影響を与える可能性があります。

注：設定ファイルの数およびバックアップする最大リビジョンは、データベースおよびアセットとドメイン マネージャのパフォーマンスに影響を与えるため、設定ファイルの数およびバックアップする最大リビジョンには注意する必要があります。

関連項目：

[DSM エクスプローラの \[ファイル収集\] フォルダへのアクセス \(P. 184\)](#)

## DSM エクスプローラの [ ファイル収集 ] フォルダへのアクセス

ファイル収集フォルダにアクセスして、バックアップ ファイルの設定、およびバックアップされたファイルのリビジョンを表示できます

### DSM エクスプローラで [ ファイル収集 ] フォルダにアクセスする方法

1. ファイル収集を表示または設定するレベルに従って、DSM エクスプローラで以下のパスに移動します。

#### グループ レベル

##### コンピュータ グループ

ドメイン、コンピュータおよびユーザ、すべてのコンピュータ、グループ詳細

##### ユーザ アカウント グループ

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、グループ詳細

##### ユーザ作成グループ

ドメイン、コンピュータおよびユーザ、グループ、グループ詳細

注：特定のアセットにこの設定を適用しない場合は、アセット レベルで無効することがにできます。

#### コンピュータ レベル

ドメイン、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。

#### ユーザ レベル

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、ユーザ アカウント

#### ドメイン レベル

ドメイン、コントロール パネル、設定、ファイル収集

2. ドメイン レベル以外で [ソフトウェア] - [ファイル収集] フォルダに移動します。



右ペインにバックアップ用に設定されたファイルが表示されます。グループレベルで設定されたファイルは、自動的にメンバアセットでのバックアップ用に設定されます。ただし、特定のアセットから収集をしない場合は、これらのファイル収集を無効化できます。

注：ファイルはコンピュータレベルで保持され、各ユーザのファイルのコピーは存在しないため、ファイル収集をユーザレベルで設定することは、あまり有用ではありません。

## バックアップ用に設定されたファイルの表示

アセットの設定ファイル情報には、以下の情報が表示されます。

- バックアップ用に設定されたファイル
- ファイルが最後に更新された日時
- データベースで使用できるリビジョンの数
- リビジョンの最大数。リビジョン 1 は、現在のバージョンを示します。

バックアップ用に設定されたファイルを表示するには、グループレベルまたはアセットレベルで「ファイル収集」フォルダに移動します。使用できるバックアップリビジョンを表示するには、設定ファイルをダブルクリックします。

## バックアップ用ファイルの設定

エージェント コンピュータ上でファイルをバックアップするには、まずファイルをドメインマネージャで設定する必要があります。設定後にファイルを変更すると、そのたびに **Asset Management** エージェントによってバックアップされます。

注：ファイル スキャンでは、ユーザ アクセスが拒否されているファイルをディレクトリから取得できません。

### バックアップ用ファイルを設定する方法

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 - [ソフトウェア] - [ファイル収集] に移動します。

右ペインにバックアップ用に設定されたファイルが表示されます。

2. [タスク] セクションで [設定] をクリックします。  
[収集するファイルを選択] ダイアログ ボックスが表示されます。
3. 設定するファイルを選択し、[OK] をクリックします。  
選択したファイルにバックアップのマークが付けられ、右ペインに表示されます。

注：Windows エージェント コンピュータでネットワーク ドライブをファイル スキャンするようエージェントが設定されている場合、そのエージェントは、ネットワーク ドライブをマップするユーザーと同じユーザー アカウントでインストールして実行する必要があります。

関連項目：

[新しいファイル収集定義の追加](#) (P. 186)

## 新しいファイル収集定義の追加

バックアップまたは収集するファイルがバックアップ用に定義されたファイルのリストで使用できない場合は、新しいファイル収集定義を追加することができます。

### バックアップする新しいファイルを追加する方法

1. [コントロール パネル] - [設定] - [ファイル収集] に移動します。  
既存のファイル収集定義が表示されます。
2. [タスク] セクションで [新規] をクリックします。  
[ファイル収集定義を追加します] ダイアログ ボックスが開きます。
3. 必要な情報を入力し、[OK] をクリックします。  
ファイルのリストに、選択したファイルが追加されます。

## ファイル収集定義の変更

ファイル収集定義を修正して、その設定のいずれかを変更できます。ファイル収集定義を変更するには、設定ファイルを右クリックして [プロパティ] を選択します。[設定ファイルのプロパティ] が表示されます。必要な設定を変更して、[OK] をクリックします。

## 設定ファイルのバックアップ バージョンおよびプッシュバックの表示

アセット管理エージェントでは、設定ファイルがエージェントの前回の実行時から変更された場合、アセットから設定ファイルを収集し、**DSM** エクスプローラにリビジョンとして記録します。任意のリビジョンをプッシュバックして、以前のバージョンに戻すことができます。

### 設定ファイルのバックアップ バージョンを表示する方法

1. アセット レベルで [ファイル収集] に移動します。  
右ペインにバックアップ用に設定されたファイルが表示されます。
2. 設定ファイルをダブルクリックします。  
右ペインにファイルの使用可能なバックアップ リビジョンが表示されます。  
リビジョン番号 **1** は、ファイルの現在のバージョンを示します。
3. リビジョンを右クリックして、[編集およびプッシュバック] を選択します。  
[コンテンツを編集してエージェントにプッシュバックします] ウィンドウが表示され、必要に応じて内容を変更することができます。
4. [OK] をクリックします。  
選択したリビジョンがアセットにプッシュされます。

## 設定ファイルのバックアップが管理される方法

アセット管理では、以下のプロセスによって設定ファイルのバックアップを管理します。

1. ファイルが最初にバックアップ用に設定されたとき、エージェントではそのファイルの内容を収集し、アセット上のエージェントの作業ディレクトリに保存します。
2. コンピュータまたはユーザがネットワークにログインするたびに、エージェントでは前回保存されたファイルとファイルの現在のバージョン間の変更をチェックします。このチェックはアセット上でローカルに実行されるため、高速です。
3. 変更があった場合、エージェントでは手順 **1** が繰り返されます。

## イベント ポリシーの定義

イベント ベースのポリシーを定義することにより、設定ファイルに加えられた変更をトラッキングすることができます。このポリシーを設定すると、たとえば、ユーザにメッセージを表示したり、ユーザが設定ファイルを変更しようとした場合に、権限を与えられたユーザに電子メールを送信できます。

### イベント ポリシーを定義する方法

#### 方法 1

1. [コントロール パネル] - [設定] - [[ファイル収集](#) (P. 184)] に移動します。  
右ペインに、バックアップ用に設定されたすべてのファイルが表示されます。
2. 右ペインで設定ファイルを右クリックして、[イベント ポリシーの定義] を選択します。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
3. 「ファイル収集」セクションで監視する対象のファイルを選択し、ファイルの変更時に実行されるようにするアクションを追加して、[OK] をクリックします。

選択された設定ファイルをユーザが変更したとき、指定されたアクションが実行されます。

#### 方法 2

1. [ポリシー] - [イベント ベース] - [アセット ファイルの収集] に移動します。  
右ペインにアセット ファイル収集の分類ポリシーが表示されます。
2. [アセット ファイルの収集] を右クリックし、[新規] を選択します。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
3. 「ファイル収集」セクションで監視する対象のファイルを選択し、ファイルの変更時に実行されるようにするアクションを追加して、[OK] をクリックします。

選択された設定ファイルをユーザが変更したとき、指定されたアクションが実行されます。

注：[ポリシー デザイナ] ダイアログ ボックスに関する詳細については、「DSM エクスプローラ ヘルプ」を参照してください。

## 収集タスク

収集タスクではアセットのデータが収集されます。収集タスクは、アセットレベル、グループレベル、およびドメインレベルで作成することができます。アセットレベルで作成されたタスクはそれぞれのアセットにリンクされ、グループレベルで作成されたタスクはグループのすべてのメンバアセットにリンクされます。ドメインレベルでは、ドメイン内のすべてのタスクの表示、新しいタスクの作成、および任意のグループまたはアセットへタスクをリンクすることができます。任意の数の収集タスクを作成して、特定のアセットまたはグループにリンクすることができます。

アセット管理には、すべてのコンピュータグループおよびそのすべてのメンバアセットにリンクされた以下の定義済み収集タスクがあります。

### インベントリ設定

アセットからハードウェアインベントリ情報を収集します。デフォルトでは、一般、Microsoft ライセンス、および保護のモジュールで指定された情報が収集され、DSM エクスプローラでアセットの [インベントリ] フォルダの下に表示されます。

### ソフトウェアインベントリ設定

アセットからソフトウェアインベントリ情報を収集します。デフォルトでは、すべてのアセット上でシグネチャスキャンが実行され、DSM エクスプローラのアセットの [ソフトウェア] - [検出済み] フォルダの下に表示されます。アセット管理エージェントは、Client Automation のインストール後に、定義済みソフトウェアシグネチャに基づいて、アセット上のソフトウェアインベントリ情報の収集を開始できます。

### ユーザテンプレート設定

会社およびユーザ固有の情報を収集します。このタスクは、すべてのコンピュータグループのすべてのアセットに自動的に設定されます。デフォルトでは、ユーザテンプレートモジュールで指定された情報が収集され、DSM エクスプローラのアセットの [インベントリ] フォルダの下に表示されます。

これらの定義済み収集タスクとは別に、以下のタイプの収集タスクを新たに作成することができます。

- ファイルのスキャン
- ハードウェア インベントリ
- ソフトウェアの検出
- ソフトウェア使用状況
- テンプレート インベントリ
- 仮想ホストインベントリ

注：これらの各収集タスクの詳細については、「**DSM エクスプローラ ヘルプ**」の「**Asset Management**」を参照してください。

## DSM エクスプローラの [ 収集タスク ] フォルダへのアクセス

[収集タスク] フォルダでは、収集タスクの作成、設定、リンク、無効化、ステータスチェック、およびスケジュールが行えます。

### [ 収集タスク ] フォルダにアクセスする方法

1. アセット ジョブを表示または設定するレベルに従って、**DSM エクスプローラ**で以下のパスに移動します。

#### グループ レベル

##### コンピュータ グループ

ドメイン、コンピュータおよびユーザ、すべてのコンピュータ、グループ詳細

##### ユーザ アカウント グループ

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、グループ詳細

##### ユーザ作成グループ

ドメイン、コンピュータおよびユーザ、グループ、グループ詳細

## コンピュータ レベル

ドメイン、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

## ユーザ レベル

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、ユーザ アカウント

## ドメイン レベル

ドメイン、コントロール パネル

2. 上記のパスから、[設定] - [収集タスク] フォルダに移動します。

グループ レベルで作成された収集タスクは、グループのメンバアセットに自動的にリンクされます。ただし、アセット レベルでこれらのタスクの実行を無効にできます。タスクがリンクされているメンバアセットおよびそれぞれのタスク ステータスを表示するには、収集タスクをダブルクリックします。

**注：**仮想ホスト インベントリ 収集タスクを除いて、これらのすべてのレベルのタスクを管理対象アセットまたはグループにリンクすることができます。仮想ホスト インベントリ 収集タスクは、リモート エージェント（AMRemoteAgent）がインストールされた アセットまたはエージェントのみに対して作成できます。また、そのタスクは、同じ OS クラスの他のエージェントにのみリンクできます。たとえば、Windows エージェント用に作成された仮想ホスト インベントリ 収集タスクは、他の Windows エージェントにのみリンクすることができます。

**関連項目：**

[収集タスク](#) (P. 189)

## エンジン収集タスク

エンジン収集タスクでは、スケーラビリティ サーバから情報を収集し、データベースを更新します。エンジン収集タスクは、[コントロール パネル] - [エンジン] - [エンジン タスク] - [収集タスク] フォルダの下で使用できます。エンジン収集タスクを設定して、以下の情報を収集することができます。

### 監査

監査を有効にしたソフトウェア使用状況収集タスクで生成された監査データを収集します。

### バックアップ

ファイル収集で設定されたファイルを収集します。

### コンテンツ配信

ターゲット コンピュータがコンテンツを取得できるように、ドメイン マネージャからスケーラビリティ サーバに新しいコンテンツを配信します。

### ハードウェア インベントリ

ハードウェア インベントリ収集タスクおよびテンプレート インベントリ収集タスクで生成されたインベントリ情報を収集します。

### ソフトウェアの検出

ソフトウェア検出収集タスクおよびファイル スキャン収集タスクで生成されたインベントリ情報を収集します。

### ソフトウェア使用状況

ソフトウェア使用状況収集タスクで生成された情報を収集します。

### ステータス

アセット ジョブおよび収集タスクからステータス タイム スタンプを収集します。



## ハードウェア インベントリ

ハードウェア インベントリ収集タスクでは、エンタープライズ内の各コンピュータ上に展開されたハードウェアに関する情報が収集されます。アセットを効率的に管理することは、機器コストを抑制することや、ユーザが必要な機器にアクセスできるように重要であるだけでなく、LAN および WAN のトラブルシューティングの実施にも役立ちます。

ハードウェア インベントリ収集タスクでは、ハードディスクや RAM などの物理データと、ハードディスク内のパーティションなどの論理データの両方を収集できます。アセット管理には、さまざまなソースからハードウェア インベントリを収集する事前定義済みのインベントリ検出モジュールが用意されています。これらのモジュールを変更すると、追加のインベントリ情報を収集したり、新しいモジュールを作成できます。

注：インベントリ検出モジュールの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

関連項目：

[インベントリ検出モジュール](#) (P. 152)

### Asset Management エージェントによりハードウェア インベントリが収集される方法

ハードウェア インベントリの設定およびスケジュールを行うには、エージェントコンピュータからインベントリを収集するためにアセット管理エージェントが実行するアクションをまず理解する必要があります。このプロセスを理解すると、インベントリ収集プロセスのトラブルシューティングのほか、インベントリを収集する頻度およびその間隔でインベントリを収集する影響に基づくハードウェア インベントリのスケジュールにも役立ちます。

エージェントにより以下のアクションが実行され、ハードウェア インベントリが収集されます。

- スケジュールされた時間には、アセットに設定された各収集タスクがエージェントによって実行されます。
- 各検知モジュールから情報を収集するための適切な実行可能ファイルを実行し、特定のファイルに保存します。たとえば、一般インベントリ情報はエージェントで `ig40.inv` として格納されます。

- フルスキャンファイルを保存して、これらのファイルを前のファイルと比較します。そして、差分値をスケーラビリティ サーバへ送信します。差分値はローカルで保存されません。スケーラビリティ サーバへ送信された情報は `i##` ファイルとして保管され、前の差分値が収集されていない場合、このファイルのバージョン番号は `i01`、`i02` のように増分されます。差分値がどのように収集されるかの詳細は、この後の「[差分値の収集](#) (P. 201)」セクションを参照してください。
- エージェントは最初にこのファイルを[エージェント作業ディレクトリ](#) (P. 32)に保存し、次にスケーラビリティ サーバの収集エリア (`...¥ServerDB¥Sector¥Collect or .../Server/Sector/COLLECT in case of Linux/UNIX platforms`) に置きます。エージェントは、データを収集するたびにこのステップを繰り返します。

**注：** エンジンによりデータが収集される前にエージェントが 2 回以上実行された場合、実行のたびにインベントリ ファイルが作成されます。たとえば、一般インベントリ情報は、`i01`、`i02` のように順に拡張子が付けられて収集されます。したがって、`i00` から `i23` までの 24 個のファイルが作成されます。

- エンジンは、エンジン収集タスクをトリガすると、スケーラビリティ サーバからすべてのファイルを収集し、ファイルを処理して内容をデータベースに格納します。処理が完了すると、エンジンはスケーラビリティ サーバの収集エリアからファイルを削除します。
- スケジューリング設定を含む新規または変更されたインベントリ モジュール設定は、スケーラビリティ サーバ上で収集タスクによって更新されます。エージェントは、新規または更新されたインベントリ情報を受け取ります。

このプロセスには、エージェント、収集タスク、およびエンジン収集タスクという 3 つのオブジェクトが関与しています。これらのオブジェクトにはそれぞれ、個別のスケジューリングオプションが備わっています。これらのオブジェクトのスケジューリングに違いがある場合は、以下の点を考慮する必要があります。

- 収集タスクの実行は、エージェントの実行に依存します。
- 収集タスクにはそれぞれ独自のスケジューリング オプションが備わっています。デフォルトでは、タスクは常に実行されるようにスケジュールされます。
- データベースの更新は、エンジン収集タスクのスケジューリングに依存します。

以下の例で、このシナリオについて説明します。3 つのオブジェクトに、以下のスケジューリングオプションが指定されているとします。

- エージェント - 1 時間ごと
- インベントリ収集タスク - 常にジョブを実行
- エンジン収集タスク - 1 日に一度

この場合、エージェントは1時間に1回実行され、収集タスクがただちに実行されます。ただし、エンジンは1日に1回しか情報を収集できません。したがって、エージェントは1日に24回情報を収集するのに、データベースは1回しか更新されません。このようなシナリオは望ましくありません。最適な実装にするために、収集タスクとエンジン収集タスクが同時に実行されるようにスケジュールすることができます。これにより、データベース内のすべての収集済みデータが確実に更新されます。

## ハードウェア インベントリ収集タスクの作成、設定およびスケジュール

デフォルトのインベントリ設定収集タスクでは、一般およびパフォーマンス インベントリが収集されます。追加のインベントリを収集するか、または特定のグループまたはアセットのデフォルトの収集タスクによって収集されたインベントリを制限する場合は、アセットまたはグループに新しい収集タスクを作成し、必要なモジュールを設定してタスクをスケジュールできます。

### ハードウェア インベントリ収集タスクを作成、設定、スケジュールする方法

1. アセットまたはグループ レベルで [収集タスク] フォルダに移動し、[新規] をクリックします。

[新しい収集タスク タイプの選択] ダイアログ ボックスが表示されます。

2. 収集タスクのタイプを選択し、[OK] をクリックします。

[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。

3. 収集タスクの一意的な名前を入力し、[スケジューリングの設定] をクリックします。

[スケジューリング オプション] ダイアログ ボックスが表示されます。

4. スケジューリング オプションを指定して [OK] をクリックします。

[スケジューリング オプション] ダイアログ ボックスが閉じ、[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。

5. [検知モジュール] タブをクリックし、必要なインベントリ検出モジュールを選択します。

収集タスクが、選択されたモジュールで設定されます。

注：各インベントリ検出モジュールの収集対象の詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

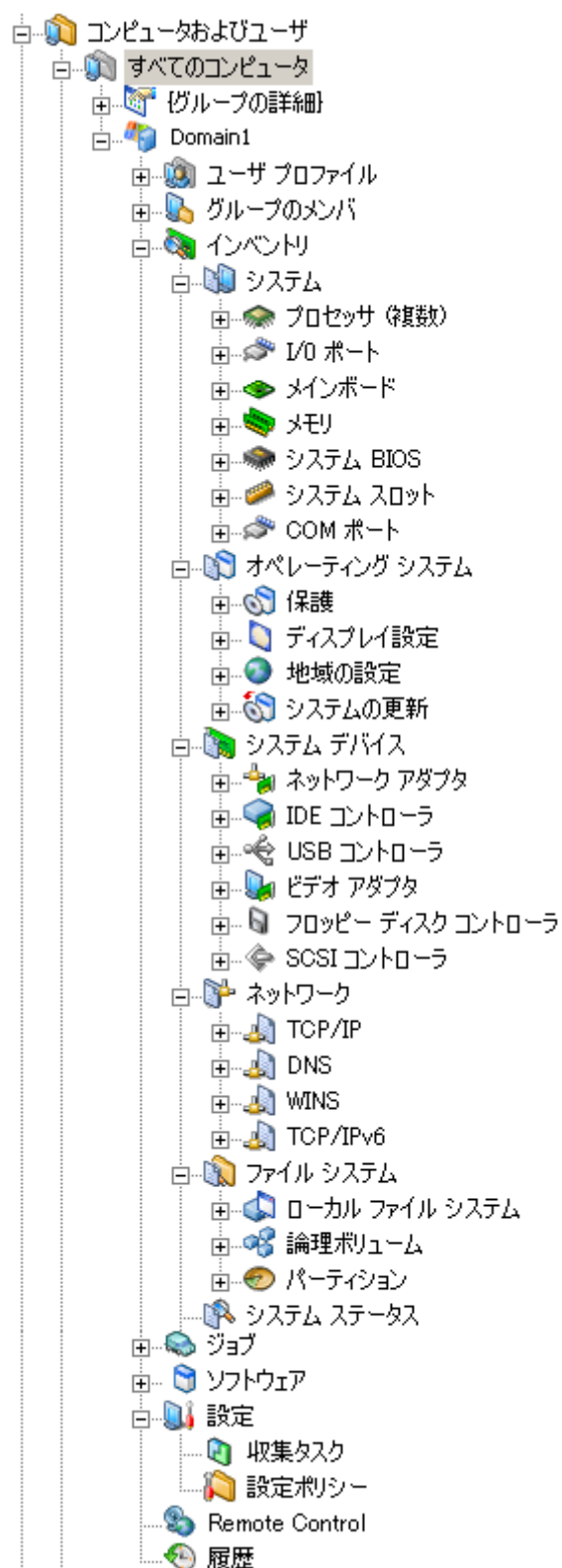
## コンピュータ インベントリ

ハードウェア インベントリ収集タスクでは、ハードウェア インベントリ情報が取得され、その情報は **DSM** エクスプローラの [インベントリ] フォルダ (たとえば、システム、オペレーティング システム、システム デバイス、ネットワーク、ファイル システム、外部デバイスなど) の下に表示されます。 [インベントリ] フォルダに表示される情報の量は、**Asset Management** がインストールされているかどうかによって異なります。 このため、ハードウェア インベントリ情報の構造は、情報を収集するのに使用されるモジュールに依存しています。これらのモジュールに基づいて、収集された情報を以下のカテゴリに分類することができます。

### 基本ハードウェア インベントリ

共通エージェントによって収集された基本ハードウェア インベントリが含まれます。この場合、基本ハードウェア インベントリのみが使用されるので、情報のサブセットのみが収集され表示されます。共通エージェントは、**DSM** ドメイン内のコンピュータに自動的に展開されます。このインベントリは、アセット管理がインストールされているかどうかにかかわらず収集されます。

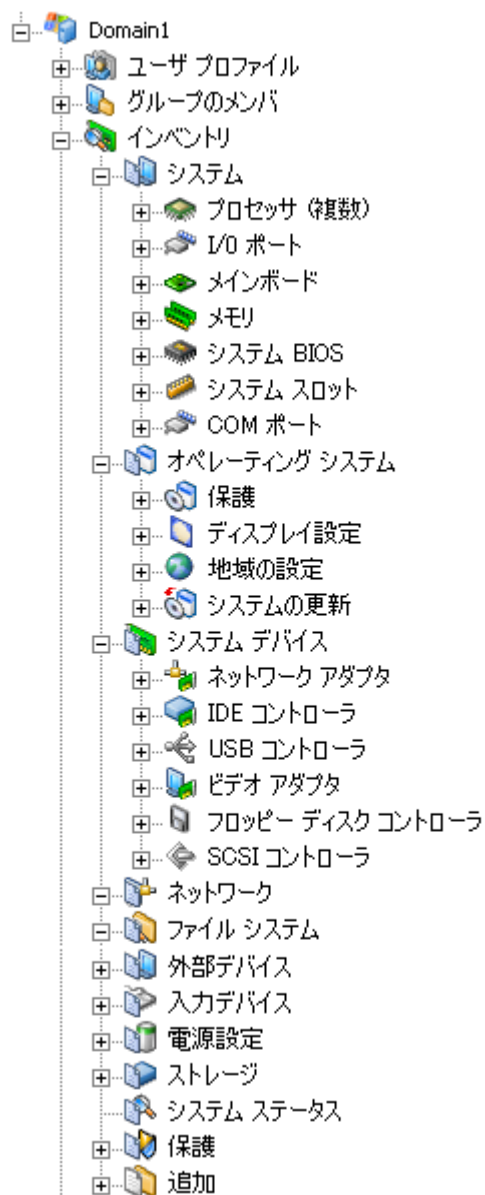
たとえば、以下のスクリーンショットには、基本ハードウェア インベントリ モジュールを使用する場合に利用できる情報が表示されています。



## 検知モジュール インベントリ

設定された検知モジュールに基づいて収集されたインベントリ 情報が含まれます。これらのインベントリは、**Asset Management** をインストールした場合のみ収集されます。デフォルトでは、一般インベントリ、**Microsoft** ライセンス情報、パフォーマンス インベントリ、および保護インベントリのオプションが選択されます。

たとえば、以下のスクリーンショットには、**Asset Management** インベントリを使用する場合に利用できる情報が表示されています。



## 追加インベントリ

一般インベントリ モジュールを除く、さまざまなモジュールを使用して収集された情報が含まれます。また、このフォルダには、システムパフォーマンスおよびテンプレートインベントリが含まれます。これらのインベントリは、**Asset Management** をインストールした場合のみ収集されます。

たとえば、以下のスクリーンショットには、ほかのオプションモジュールで利用できる追加インベントリ情報が表示されています。



関連項目：

[ハードウェア インベントリ情報の表示 \(P. 202\)](#)



## データ値の収集

コンピュータからハードウェアおよびソフトウェアのインベントリ情報を収集する場合、アセット管理エージェントでは、以前のスキャン結果と現在のスキャン結果の計算によってディファレンシャル（差分）値のみが報告されます。エージェントでは、最初にインベントリ全体を収集し、その結果が以前のスキャン結果 (**bak** ディレクトリで利用可能な) と比較されます。エージェントでは、**DIF** ファイルが作成され、差異が保存されます。この **DIF** ファイルはスケラビリティ サーバの収集エリアに置かれ、データベースを更新するためにエンジンによって処理されます。これにより、ネットワーク上を移動し、エンジンによって処理されるレコードが少なくなるため、ネットワーク トラフィックが減少し、エンジンのパフォーマンスが向上します。

デフォルトでは、エージェントは差分値のみを送信します。ただし、収集したすべての値をスケラビリティ サーバに送信するようにエージェントに指示することができます。これはインベントリの再収集と呼ばれます。

注：シグネチャ スキャンの場合、エージェントは差分値を送信しません。

## インベントリの再収集

デルタ値ではなく完全インベントリが送信されるよう、エージェントを設定できます。エージェントのこのデフォルト動作を変更するには、以下の方法に従います。

### 方法 1

#### ドメイン マネージャからこの作業を行う方法

1. [ドメイン] - [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。

右側のペインに、ドメインに接続されているすべてのコンピュータが表示されます。

2. インベントリを再収集するコンピュータを右クリックし、[アセット ジョブ] - [ジョブ確認のアクティブ化] を選択します。

[アセット ジョブ確認] ダイアログ ボックスが表示されます。

3. ほかの再スキャン オプションのいずれか一方または両方を指定して [再収集] オプションを選択し、[OK] をクリックします。

エージェントがターゲット コンピュータで実行され、すべてのインベントリ情報が収集されます。

## 方法 2

### エージェントからこの作業を行う方法

1. コマンドラインで以下のコマンドを指定します。

```
caf start amagent args /RESCAN_SOFTWARE /RESCAN_INVENTORY /COLLECT
```

エージェントがターゲット コンピュータ上で実行されます。エージェントにより、ソフトウェア インベントリおよびハードウェア インベントリの情報が収集されて、スケーラビリティ サーバの収集エリアに保存されます。

**注:** ソフトウェア インベントリとハードウェア インベントリのいずれか一方のみを収集する場合は、再収集しないインベントリの再スキャン引数を削除します。たとえば、ソフトウェア インベントリのみを再収集する場合は、以下のコマンドを指定します。

```
caf start amagent args /RESCAN_SOFTWARE /COLLECT
```

## ハードウェア インベントリ情報の表示

ハードウェア インベントリ情報を使用すると、どのようなハードウェア リソースを所有しているか、およびそれらのリソースが組織内のどこにあるのかを知ることができます。

### ハードウェア インベントリ情報を表示する方法

1. 情報を表示するレベルに従って、以下のフォルダに移動します。

#### コンピュータ レベル

ドメイン、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

#### ユーザ レベル

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、ユーザ アカウント

2. [インベントリ] フォルダに移動します。

コンピュータ レベルでは、CPU や RAM などのコンピュータ関連のインベントリを表示できます。また、ユーザ レベルでは、テンプレート データなど、ユーザから収集された情報を表示できます。

## ソフトウェアの検出

ソフトウェア検出収集タスクでは、アセット上にインストールされているソフトウェアが収集されます。これにより、ライセンスのないソフトウェア インストールをトラッキングし、修正処置を行うことができます。また、このタスクでは、ファイル システムをスキャンしてソフトウェア シグネチャを比較したり、オペレーティング システム固有のパッケージ登録情報をクエリすることにより、Linux ベースおよび Windows ベースの両方のアセット上でソフトウェア パッケージを検出できます。

ソフトウェア検出収集タスクでは、以下のいずれかの方法を使用してソフトウェア情報を収集できます。

- ヒューリスティック スキャン
- ソフトウェア シグネチャ (デフォルト)

### ヒューリスティック スキャン

エージェント コンピュータ上のレジストリや MSI などのローカル ソフトウェア データベースがスキャンされます。また、デスクトップおよびスタート メニューにあるアプリケーションのショートカットをスキャンすることも選択できます。

注：デスクトップやスタート メニューのショートカットのスキャンを選択すると、多くの容量と時間が必要になります。また、製品をアンインストールした後もデスクトップおよびスタート メニューにショートカットが残っている可能性があるため、結果が正確でないことがあります。

Linux/UNIX システムでは、ヒューリスティック スキャンの設定は不要です。デフォルトでは、Linux/UNIX プラットフォーム上でヒューリスティック スキャンを実行すると、RPM、PKG、および PIF データベースがスキャンされます。

注：デフォルトでは、ヒューリスティック スキャンの結果は、エンタープライズ マネージャには複製されません。ただし、DSM エクスプローラを使用してこれらを設定できます。複製を有効または無効にするには、[ソフトウェア]-[検出済み] ノードに移動し、[検出済み] ノードのコンテキスト メニューから [ヒューリスティックをエンタープライズに複製] 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適用されます。詳細については、「実装ガイド」を参照してください。

## ソフトウェアシグネチャ

エージェント コンピュータのハードディスク内で実行可能ファイルがスキャンされ、データベース内の使用可能なシグネチャを持つファイルと照合されます。DSM エクスプローラでは、ソフトウェアシグネチャはソフトウェア定義として指定されます。[エンジン タスク] からデフォルトのソフトウェア コンテンツのダウンロードジョブを選択すると、CA Online Content Service から 1 日に 1 回、最新のシグネチャがダウンロードされます。さらに、新しいソフトウェア定義を作成し、スキャン用に使用可能にすることもできます。ドメインレベルでソフトウェア定義を作成した場合、検出されたソフトウェア情報はドメインレベルのみで表示されます。しかし、エンタープライズレベルでソフトウェア定義を作成した場合、検出されたソフトウェア情報はドメインレベルでもエンタープライズレベルでも表示されます。

### Intellisig

ソフトウェア メーカーが提供する定義済みソースからソフトウェア定義情報を抽出します。そのソースとして、テキストファイル、データベース、レジストリ、またはバイナリ ファイルを使用できます。たとえば、`dsmver -f<output file>` は、CA ITCM に関するバージョン情報を出力するコマンドです。製造元が、バージョン情報を製品に格納する方法を変更しない場合、Intellisig は、製品の今後のバージョンも検出できます。

## Asset Management エージェントによりソフトウェア インベントリが収集される方法

ソフトウェア インベントリ情報を収集するためにアセット管理エージェントで使用されるプロセスは、スキャンの方法によって異なります。このプロセスを理解すると、ソフトウェア インベントリ収集プロセスのトラブルシューティングのほか、ソフトウェア インベントリを組織に最も適した間隔でスケジュールおよび設定するのに役立ちます。

### ヒューリスティック スキャン

- スケジュールされた時間になると、アセット管理エージェントにより、選択したソース内で、Windows エージェント上にインストールされているソフトウェアがスキャンされます。Linux/UNIX では、RPM、PKG、および PIF データベースが検索されます。

### シグネチャのスキャン

- スケジュールされた時間になると、アセット管理エージェントにより、アセットのハードディスク内で実行可能ファイルがスキャンされ、データベース内の使用可能なシグネチャを持つファイルと照合されます。

どちらの方法を使用した場合も、エージェントにより、インストール済みソフトウェア情報の収集後に以下のアクションが実行されます。

- ソフトウェア インベントリ ヒューリスティック スキャンを使用する場合は、**amapp.dat** ファイルを作成します。このファイルには、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が含まれます。しかし、ソフトウェア シグネチャ スキャンを使用する場合は、**amsoft.xml** ファイルを作成します。このファイルには、シグネチャ スキャンにより検出されたソフトウェアが含まれます。
- 両方のスキャンで収集された結果を前のスキャン結果と比較し、差分値をスケーラビリティ サーバへ送信します。スケーラビリティ サーバでは差分値が **w##** ファイルに保管されます。
- エンジン は、エンジン収集タスクをトリガすると、スケーラビリティ サーバからすべてのファイルを収集し、ファイルを処理して内容をデータベースに格納します。処理が完了すると、エンジンはスケーラビリティ サーバの収集エリアからファイルを削除します。

このプロセスには、エージェント、インベントリ収集タスク、およびエンジン収集タスクという 3 つのオブジェクトが関与しています。これらのオブジェクトにはそれぞれ、個別のスケジューリング オプションが備わっています。これらのオブジェクトのスケジューリングに違いがある場合は、以下の点を考慮する必要があります。

- インベントリ収集タスクの実行は、エージェントの実行に依存します。
- インベントリ収集タスクにはそれぞれ独自のスケジューリング オプションが備わっています。デフォルトでは、タスクは常に実行されるようにスケジュールされます。
- データベースの更新は、エンジン収集タスクのスケジューリングに依存します。逆に、エンジン収集タスクは、データベースからスケーラビリティ サーバまでの情報（新規または変更されたエージェント収集モジュール設定およびジョブ スケジューリング オプション）も更新します。ソフトウェア シグネチャ スキャン用のソフトウェア シグネチャもエンジン収集タスクによって更新されます。

以下の例で、このシナリオについて説明します。3つのオブジェクトに、以下のスケジューリングオプションが指定されているとします。

- エージェント - 1時間ごと
- インベントリ収集タスク - 常にジョブを実行
- エンジン収集タスク - 1日に一度

この場合、エージェントは1時間に1回実行され、収集タスクがただちに実行されます。ただし、エンジンは1日に1回しか情報を収集できません。したがって、エージェントは1日に24回情報を収集するのに、データベースは1回しか更新されません。このようなシナリオは望ましくありません。最適な実装にするために、収集タスクとエンジン収集タスクが同時に実行されるようにスケジュールすることができます。これにより、データベース内のすべての収集済みデータが確実に更新されます。

## ソフトウェア検出収集タスクの作成、設定およびスケジュール

デフォルトのソフトウェアインベントリ設定収集タスクでは、シグネチャスキャンを実行するよう設定されています。特定のグループまたはアセットで、ヒューリスティックスキャンの結果または不明なソフトウェアの情報を収集する場合は、アセットまたはグループに新しい収集タスクを作成し、そのタスクを設定してスケジュールできます。

### ソフトウェア検出収集タスクを作成、設定およびスケジュールする方法

1. アセットまたはグループレベルで [収集タスク] フォルダに移動し、[新規] をクリックします。  
[新しい収集タスク タイプの選択] ダイアログボックスが表示されます。
2. 収集タスクのタイプを選択し、[OK] をクリックします。  
[新規収集タスクのスケジュール] ダイアログボックスが表示されます。
3. 収集タスクの一意的な名前を入力し、[スケジューリングの設定] をクリックします。  
[スケジューリング オプション] ダイアログボックスが表示されます。
4. スケジューリング オプションを指定して [OK] をクリックします。  
[スケジューリング オプション] ダイアログボックスが閉じ、[新規収集タスクのスケジュール] ダイアログボックスが表示されます。

5. [方法] タブで、以下のいずれかを選択します。

### ヒューリスティック スキャン

ヒューリスティック スキャンを有効にします。スキャン対象のソースを含めるまたは除外するには、[スキャナの設定] をクリックします。有効なオプションは、以下のとおりです。

- [プログラムの追加と削除] データベース
- MSI (Microsoft Software Installer)
- ショートカット - デスクトップ
- ショートカット - [スタート] メニュー
- VMware ThinApp 仮想アプリケーション イメージ
- Microsoft App-V 仮想アプリケーション イメージ

### シグネチャのスキャン

シグネチャ スキャンを有効にします。スキャン対象のソースを含めるまたは除外するには、[スキャナの設定] をクリックします。有効なオプションは、以下のとおりです。

- Intellisig スキャン
- シグネチャ スキャン
  - 不明な実行ファイルをレポート
  - 不明な仮想アプリケーション イメージをレポート
  - ストリーム配信された VMware ThinApp 仮想アプリケーションをレポート

この 2 つの方法では、アセット管理エージェントにより、情報を収集するために異なるアクションが実行されます。

## 検出済みソフトウェア情報のエクスポート

「検出されたソフトウェア」レポートでは、インストールパスやインストール数など、さらに詳細な情報が表示されます。このレポートを **csv** ファイルにエクスポートしてハードディスクに保存することができます。

### 検出されたソフトウェア情報を参照してエクスポートする方法

1. **DSM** エクスプローラで「検出済み」フォルダに移動します。

右側のペインに検出されたソフトウェアが表示されます。この情報は、ソフトウェア インベントリ収集タスクが正常に実行された場合のみ使用可能です。

2. レポートを表示する検出済みソフトウェアを選択し、選択したソフトウェアを右クリックします。

コンテキストメニューが表示されます。

3. 「詳細」をクリックします。

「コンピュータ」ダイアログ ボックスの「ソフトウェア レポート」が表示されます。

4. 「エクスポート」をクリックします。

5. 「出力ファイルを入力します」ダイアログ ボックスで **csv** ファイルの名前およびパスを指定し、「OK」をクリックします。

レポートが **csv** ファイルにエクスポートされます。



## 検出されたソフトウェアの表示

ソフトウェア インベントリ情報を使用すると、アセットにインストールされたソフトウェアを確認できます。

### ソフトウェア インベントリ情報を参照する方法

1. 情報を表示するレベルに従って、以下のフォルダに移動します。

#### グループ レベル

##### コンピュータ グループ

ドメイン、コンピュータおよびユーザ、すべてのコンピュータ、グループ詳細

##### ユーザ アカウント グループ

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、グループ詳細

##### ユーザ作成グループ

ドメイン、コンピュータおよびユーザ、グループ、グループ詳細

#### コンピュータ レベル

ドメイン、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。

#### ユーザ レベル

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、ユーザ アカウント

2. [ソフトウェア] - [検出済み] フォルダに移動します。

右側のペインに検出されたソフトウェアが表示されます。

関連項目：

[ソフトウェアの検出](#) (P. 203)

### 不明なソフトウェアの収集

デフォルトでは、ソフトウェア検出収集タスクによりシグネチャ スキャンが実行され、登録済みのアプリケーション（シグネチャに一致するソフトウェア）のみが取得されます。ただし、非仮想および仮想アプリケーションから不明なアプリケーション（シグネチャに一致しないソフトウェア情報）を収集するように設定することもできます。

Asset Management エージェントは、アセットのハードディスク上にある実行可能ファイル、または（有効に設定されている場合）ソフトウェア定義に一致しないすべての仮想パッケージのどちらかを収集し、以下のフォルダに正しく表示します。

- すべての登録済みアプリケーションは、[ドメイン] - [コンピュータおよびユーザ] - [すべてのコンピュータ] - [グループの詳細] - [コンピュータ] - [ソフトウェア] - [検出済み] を選択すると表示されます。
- 不明な非仮想および仮想アプリケーションは、[ドメイン] - [コンピュータおよびユーザ] - [すべてのコンピュータ] - [グループの詳細] - [コンピュータ] - [ソフトウェア] - [不明] を選択すると表示されます。

注：不明なソフトウェア情報の収集は、シグネチャ スキャンの場合のみサポートされます。

### 不明なアプリケーションの登録

不明なアプリケーションを登録すると、アセット上のライセンスのない不正なソフトウェア インストールをトラッキングできます。また、エージェントの次の実行時に登録済みアプリケーションとして検出されるように正当なソフトウェアを登録できます。

#### 不明なアプリケーションを登録する方法

1. DSM エクスプローラで [不明] フォルダに移動します。
2. 登録するアプリケーションを右クリックし、[登録] を選択します。  
[リリースの新規作成] ダイアログ ボックスが表示されます。
3. [一般] - [識別] - [オプションの除外] タブで詳細を確認し、[OK] をクリックします。

アプリケーションがソフトウェア シグネチャとして登録されます。[ドメイン] - [ソフトウェア] - [定義] - [分類] - [すべての定義] フォルダを選択すると、このアプリケーションが一覧表示されます。

## エージェント インベントリの日付の収集

Asset Management エージェントによって収集される情報には、Asset Management ソフトウェア スキャナによって使用されるソフトウェア シグネチャ ファイルの「配信日」と「作成日」が含まれます。[システム ステータス] ペインには、アセットに対するこれらのインベントリ項目が表示されます。項目名は以下のとおりです。

### ソフトウェア シグネチャ ファイル作成日

エンジンによってシグネチャ ファイルが作成され、スケーラビリティ サーバへの配信準備ができた日時を特定します。

### ソフトウェア シグネチャ ファイル配信日

シグネチャ ファイルがターゲット コンピュータに配信された日時を特定します。

これらのインベントリ項目を Client Automation のクエリ定義の一部として含めることができます。

**注：**エンジンがエージェントによってダウンロードされたシグネチャを作成するまで、シグネチャ作成日は使用できません。収集タスクでコンテンツ配信が無効に設定されている場合、このアクションは発生しません。

## ヒューリスティック ソフトウェア定義および検出されたインベントリの削除

また、ヒューリスティック ソフトウェア定義および対応する検出されたインベントリを削除できます。

### ヒューリスティック ソフトウェア定義および検出されたインベントリを削除する方法

1. **DSM** エクスプローラ内の各ドメイン マネージャに対する以下のフォルダに移動します: [ソフトウェア] - [定義] - [カテゴリ] - [すべての定義] (または他のカテゴリ ノード)。

右側のペインにすべてのソフトウェア定義が表示されます。

2. 削除する定義を選択した後、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。

3. [削除] をクリックします。

**CA ITCM** は定義および関連するインベントリ項目を削除します。

**注:** また、ヒューリスティック ソフトウェア データを必要としなくなった場合は、すべてのヒューリスティック スキャンを無効化できます。これを行うには、エンタープライズおよびドメイン マネージャ上のヒューリスティック スキャン収集タスクを無効化します。 **注:** ヒューリスティック スキャン収集タスクの無効化する方法の詳細については、「収集タスクの無効化」、「アセットから収集タスクのリンクを解除」、「収集タスクの削除」の手順を参照してください。

## ファイルのスキャン

ファイルのスキャン収集タスクでは、アセットのハードディスク上の個々のファイルおよびディレクトリ構造が収集され、**Client Automation** エクスプローラのファイル エクスプローラに表示されます。

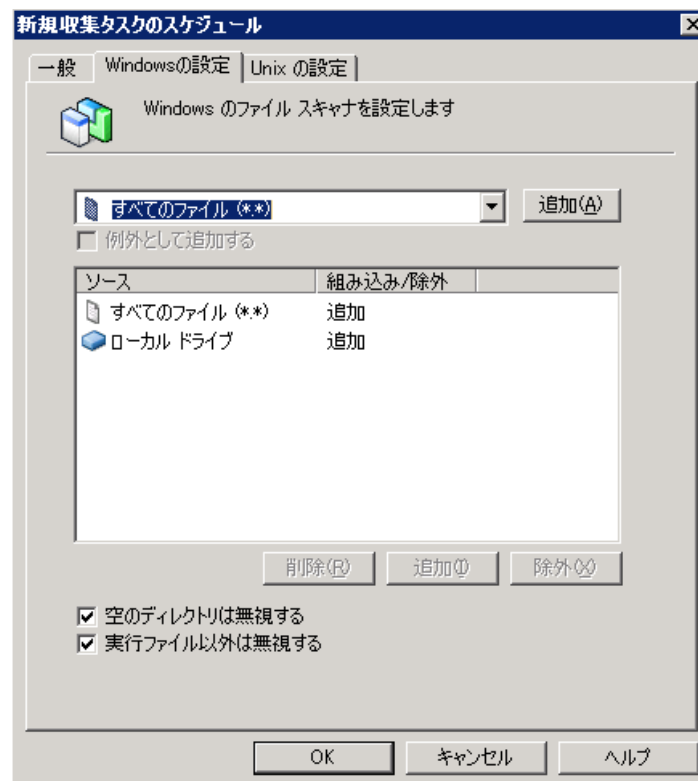
## ファイル スキャンの作成、設定およびスケジュール

ファイル スキャン収集タスクでは、エージェント コンピュータのハードディスクからフォルダおよびドライブ情報が収集され、ファイル エクスプローラに表示されます。

### ファイル スキャンを作成、設定、スケジュールする方法

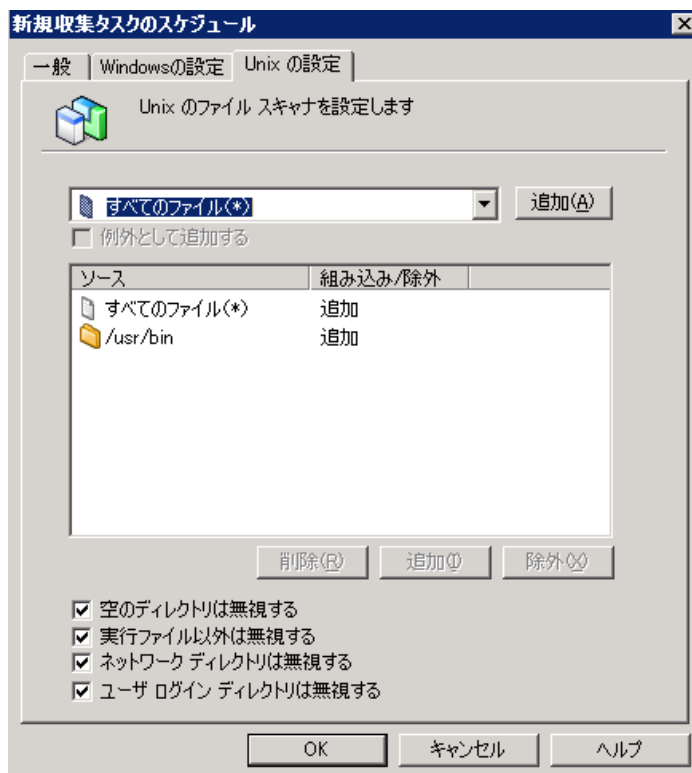
1. アセットまたはグループ レベルで [収集タスク] フォルダに移動し、[新規] をクリックします。  
[新しい収集タスク タイプの選択] ダイアログ ボックスが表示されます。
2. 収集タスクのタイプを選択し、[OK] をクリックします。  
[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。
3. 収集タスクの一意な名前を入力し、[スケジューリングの設定] をクリックします。  
[スケジューリング オプション] ダイアログ ボックスが表示されます。
4. スケジューリング オプションを指定して [OK] をクリックします。  
[スケジューリング オプション] ダイアログ ボックスが閉じ、[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。
5. [Windows 設定] タブを選択し、Windows エージェント上でスキャンするファイル タイプ、フォルダ、またはドライブを選択します。

以下の図のタスクの設定では、ドライブ C のすべての実行可能ファイル（.exe、.dll、.bat）が収集され、空のディレクトリは無視されます。



6. [Unix の設定] タブを選択し、Unix/Linux エージェント上でスキャンするファイルタイプ、フォルダ、またはドライブを選択して [OK] をクリックします。

以下の図のタスクの設定では、すべての実行可能ファイルが収集され、空のネットワーク ディレクトリおよびユーザ ログインディレクトリは無視されます。



注：ファイル スキャンでは、ユーザ アクセスが拒否されているファイルをディレクトリから取得できません。Windows で、アセット管理エージェントがネットワーク ドライブをファイル スキャンするように設定されている場合、そのエージェントは、ネットワーク ドライブをマップするユーザと同じユーザ アカウントでインストールして実行する必要があります。

関連項目：

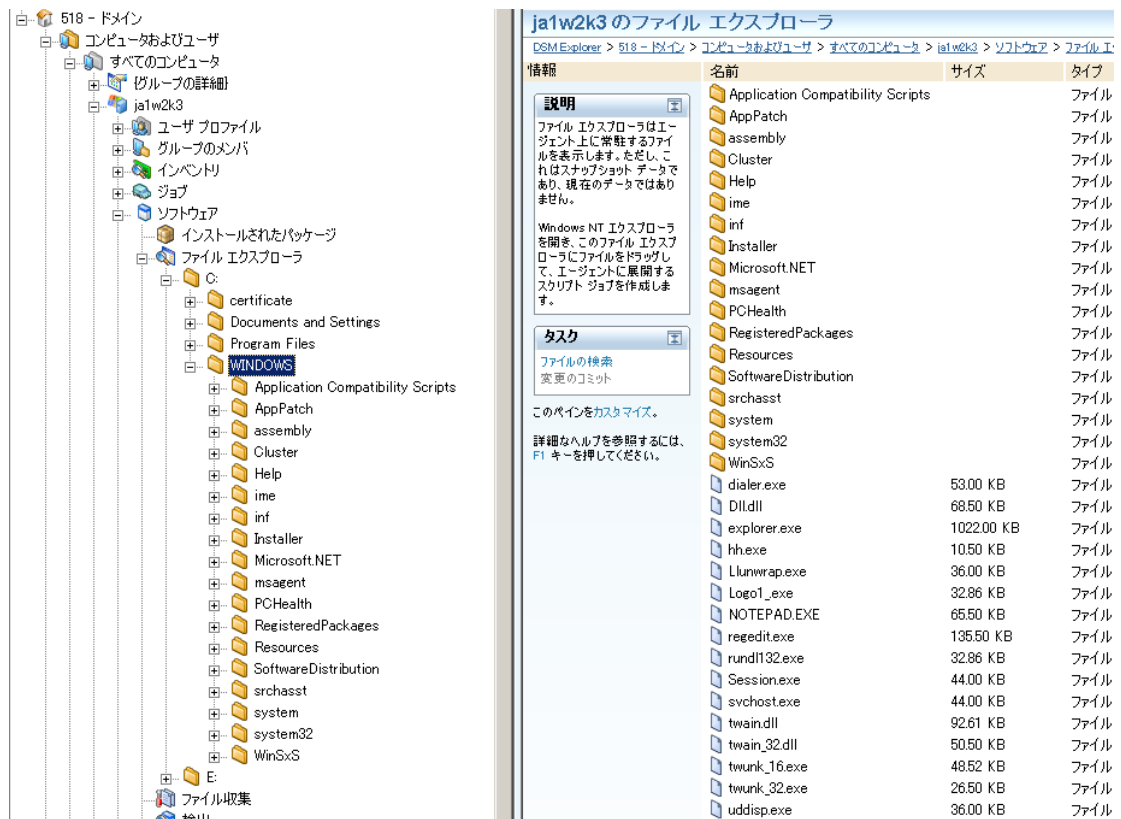
[収集タスクのステータスの確認](#) (P. 244)

## ファイル エクスプローラ

ファイル エクスプローラでは、ファイル スキャン収集タスクにより収集されたすべてのファイルおよびディレクトリが表示されます。ファイル エクスプローラのルック アンド フィールは、**Windows** エクスプローラに似ています。 ファイルとディレクトリの作成、ドメイン コンピュータ上のネットワーク共有場所からアセットのファイル エクスプローラへのファイルのコピー、およびファイルとディレクトリの削除を行うことができます。これらのアクションは、アセット上ですぐには実行されず、自動スクリプト ジョブが作成されます。アクションが実行されるのは、エージェントが次回実行されるときです。

ファイル エクスプローラでは、ファイル名、ディレクトリ、サイズ、日付、および属性のみが表示され、リモート コンピュータ上のファイルの内容は表示されません。

以下の図は、エージェント コンピュータ用のファイル エクスプローラを示します。



注：これはスナップショット データであり、ライブ データではありません。アセットでの変更内容は、アセット管理エージェントが次に実行されたときに有効になります。



## テンプレート インベントリ

テンプレート インベントリ 収集タスクでは、インベントリ テンプレート モジュール内に設定されているデータが収集されます。テンプレートは、ハードウェア インベントリまたはソフトウェア インベントリの一部ではない情報を収集する場合に使用されます。テンプレートを作成および変更するには、[コントロール パネル] - [設定] - [収集モジュール] - [インベントリ テンプレート モジュール] フォルダを選択します。

スケジュールされた時間に、エージェントによってユーザに入力を求めるプロンプトが表示され、データがスケーラビリティ サーバに転送されます。エンジンによって、スケーラビリティ サーバからデータベースにデータがインポートされます。この情報を表示するには、[すべてのユーザ アカウント] - [ユーザ] - [インベントリ] - [追加] フォルダを選択します。

デフォルトのユーザ テンプレート モジュールは、[すべてのコンピュータ] グループにリンクしています。ただし、このモジュールではユーザに入力を求めるプロンプトは表示されません。ユーザに入力を求めるプロンプトが表示されるように、モジュールを設定する必要があります。

注：インベントリ テンプレート モジュールの作成および設定の詳細については、「DSM エクスプローラ ヘルプ」を参照してください。

## テンプレート インベントリの作成、設定およびスケジュール

選択したテンプレート 検知モジュール内で設定されているインベントリ情報が収集されるように、テンプレート インベントリ 収集タスクを作成および設定することができます。

### テンプレート インベントリ 収集タスクを作成および設定する方法

1. アセットまたはグループ レベルで [収集タスク] フォルダに移動し、[新規] をクリックします。

[新しい収集タスク タイプの選択] ダイアログ ボックスが表示されます。

2. 収集タスクのタイプを選択し、[OK] をクリックします。

[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。

3. 収集タスクの一意な名前を入力し、[スケジューリングの設定] をクリックします。

[スケジューリング オプション] ダイアログ ボックスが表示されます。

4. スケジューリング オプションを指定して **[OK]** をクリックします。  
[スケジューリング オプション] ダイアログ ボックスが閉じ、[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。
5. [テンプレート モジュール] タブを選択し、収集するインベントリが含まれるテンプレート モジュールを選択して **[OK]** をクリックします。  
テンプレート インベントリ収集タスクは、上記の設定で保存されます。

## ソフトウェア使用状況

ソフトウェア使用状況収集タスクには、ソフトウェア ライセンス管理機能が備わっています。この機能を使用して、以下の作業を行うことができます。

- 組織内にインストールされているソフトウェア パッケージおよびアプリケーションのうち、どれがどのアセットで使用されているかを監視します。
- サーバまたはローカル ディスクから実行されるアプリケーションの使用頻度を測定します。
- エンタープライズ内のコンピュータ上で実行されているソフトウェア製品のコピー数を監視して、使用許諾契約に準拠しているかどうかを調べ、ユーザーを識別しやすいようにアップグレードを新しいソフトウェアに保存します。
- コンピュータ上で起動および停止されたアプリケーションを検出します（ソフトウェア監査）。
- ユーザーが自分でソフトウェアをインストールできないようにし、承認されたライセンス数しか会社で使用されないようにするなど、認可されていないソフトウェアの使用を未然に防ぎます。
- システム管理者は、使用できないソフトウェアを定義するのではなく、許可されるアプリケーションを定義することができます。その他のアプリケーションはデスクトップで実行不可能になります。

**重要：** ユーザーは指定されたアプリケーション以外を実行できなくなるため、この設定は非常に慎重に行う必要があります。ライブ環境で設定を適用する前に、テスト環境で設定をテストする必要があります。

監視するアプリケーションを選択し、各アプリケーションの使用可能ライセンス数を指定してから、指定した数を超えた場合に実行するアクションを指定できます。以下のアクションを指定できます。

- アクションなし（監視のみ）
- 警告を表示
- アプリケーションの起動を回避

サイト全体、特定のアセット グループ、または 1 つのアセットを監視できます。ローカル ドライブにインストールされたソフトウェア パッケージとネットワーク ドライブにインストールされたソフトウェア パッケージを区別できるように、ソフトウェア使用状況収集タスクを設定できます。

ソフトウェア使用状況収集タスクはコンピュータ レベルおよびユーザー レベルの両方で設定できますが、コンピュータ レベルで設定した場合は、ローカル システム アカウントを使用してソフトウェア使用状況エージェントを実行できます。これにより、どのユーザーがログインしているかに関係なく、エージェントは常に実行されます。

注：ソフトウェア使用状況機能は、データベース内で定義されているすべてのソフトウェアシグネチャ定義に対して使用できます。ただし、仮想アプリケーションでは、ソフトウェアの使用と監査はサポートされていません。

### 使用状況の監視の有効化

DSM ドメイン内のコンピュータに割り当てられたソフトウェア ライセンスおよび使用中のソフトウェア ライセンスをトラッキングするには、使用状況の監視をオンにする必要があります。デフォルトでは、使用状況の監視はオフになっています。

ソフトウェア使用状況の監視をオンにするには、以下の 2 つの方法があります。

- ソフトウェア定義をソフトウェア使用状況収集タスクに追加
- [検出されたソフトウェア] ペインで、検出されたソフトウェアのソフトウェア使用状況の監視を有効化

[検出されたソフトウェア] ペインでソフトウェア使用状況の監視をオンにするには、アセットまたはグループの [検出されたソフトウェア] ペインで、監視するソフトウェアを右クリックし、[使用状況の監視の有効化] を選択します。新しいソフトウェア使用状況収集タスクが作成され、アセットまたはグループにリンクされます。この場合、デフォルトで [オンライン使用状況] がオフになります。ソフトウェア使用状況収集タスクがすでに存在する場合、新しい定義は同じタスクに追加されます。

## ソフトウェア使用状況のコンポーネント

ソフトウェア使用状況機能では、以下のコンポーネントが使用されます。

### ソフトウェア使用状況サーバ

ソフトウェア使用状況サーバは、スケーラビリティ サーバ上に常駐します。ソフトウェア使用状況サーバでは、以下の機能が実行されます。

- 監視対象アプリケーションのオンライン使用状況データを追跡および保存します。
- アプリケーションごとに監査情報および使用可能なライセンスをトラッキングします。
- エージェントがアプリケーションへのアクセスを要求すると、サーバは要求されたアプリケーションの使用可能ライセンスを確認します。使用可能なライセンスがある場合は、アクセスを許可し、使用可能ライセンスの数を 1 つ減らします。使用可能なライセンスがない場合は、ソフトウェア使用状況収集タスクで指定されたアクションを実行するようにエージェントに指示します。
- キューを保持します。ライセンス数を超えた場合は、サーバが追加のリクエストをキューに格納し、既存のユーザがアプリケーションを閉じたときにライセンスを解放することにより、このキューを管理します。

注：ソフトウェア使用状況サーバでは、同じアプリケーションの異なるバージョン（たとえば、Microsoft Word 97 と Microsoft Word 2000）を区別できます。

## ソフトウェア使用状況エージェント

ソフトウェア使用状況エージェントは、アセット管理により管理されるすべてのアセット上に常駐し、アセット管理エージェントが起動されるたびに起動されます。

- オンラインのソフトウェア使用状況では、エージェントにより以下の機能が実行されます。

**注：** UNIX/Linux エージェントでは、オンライン ソフトウェア使用状況はサポートされていません。UNIX ソフトウェア使用状況エージェントの誤動作を防ぐには、UNIX/Linux ソフトウェア使用状況タスクに対してオンラインメータリングのオプションを無効にする必要があります。これは DSM エクスプローラのユーザインターフェースを使用して検証、調整することができます。[コンピュータおよびユーザ] - [すべてのコンピュータ] - [グループの詳細] - [設定] - [収集タスク] - [ソフトウェア使用状況] の順に選択します。ソフトウェア使用状況タスクの [プロパティ] ダイアログ ボックスを開き、[オンライン] タブで [オンライン ソフトウェア使用状況を有効にする] チェック ボックスがオフになっていることを確認します。

- アプリケーションの使用と監視対象のアプリケーションの開始、停止時間、ならびにアプリケーションが正常に起動および停止されたかを監視します。エージェントは 1 台のコンピュータ上の複数のインスタンスを無視します。
- ユーザがソフトウェア使用状況に対して有効になっているアプリケーションを開こうとすると、ソフトウェア使用状況エージェントはリクエストをソフトウェア使用状況サーバに送信します。
- 使用可能なライセンスがある場合、サーバはエージェントに通知し、エージェントはユーザがアプリケーションで作業することを許可します。使用可能なライセンスがない場合は、警告メッセージが表示されるか、またはユーザはアプリケーションにアクセスできません。
- ライセンス数が最大数に達していない場合は、以前にアクセスを禁止されたユーザにアプリケーションが使用可能であることが通知されます。

- オフラインのソフトウェア使用状況では、エージェントにより以下の機能が実行されます。
  - アプリケーションの使用と監視対象のアプリケーションの開始、停止時間、ならびにアプリケーションが正常に起動および停止されたかを監視します。エージェントは1台のコンピュータ上の複数のインスタンスを無視します。
  - ほかの収集済みデータと同様に、データをアセット管理エージェントの作業ディレクトリに保存します。

注：ソフトウェア定義は一意である必要があります。同じソフトウェア定義を2つ以上作成し、それを監視するようにソフトウェア使用状況エージェントを設定した場合、最初にソフトウェア使用状況収集タスクに追加された定義のみが起動された定義としてレポートされます。

## 完全な使用状況データ

DSM エクスプローラから、ソフトウェア使用状況データに対するクエリを作成できます。オンラインおよびオフラインのいずれのソフトウェアの使用状況データをクエリすることもできます。このデータに基づいて、使用状況の統計やしきい値のアラームなど、拡張的なクエリ、レポート、またはグラフを作成できます。

## オフラインでの使用状況

オフラインでの使用状況の場合、監視対象のアプリケーションの起動と停止が、コンピュータアセット上のエージェントの作業ディレクトリにローカルに記録されます。アセット管理エージェントが次に実行されたときに、エンジンによってデータベース内のこの情報が更新されます。アプリケーションのリストは、[オフラインの使用状況ビュー] ウィンドウに表示されます。

また、オフラインでの使用状況データに基づいてレポートを作成することもできます。

注：オフラインでの使用状況データが DSM エクスプローラに表示されない場合は、実行中のアプリケーションを停止してからアセット管理エージェントを開始します。

関連項目：

[エンジンの停止および起動 \(P. 514\)](#)

## オンライン使用率

オンラインでの使用状況の場合、ソフトウェア使用状況エージェントが引き続きアプリケーションの起動または停止を監視し、スケーラビリティ サーバに常駐するソフトウェア使用状況サーバにこの情報を送信します。このため、[オンラインでの使用状況] ウィンドウで表形式およびグラフ形式により、使用されているライセンスの実際の数をもいつでも確認できます。この情報は、スケーラビリティサーバのファイル システムに最長 3 日間保管されますが、データベースには格納されません。データはデータベースにインポートできます。ソフトウェア使用状況エージェントは、ソフトウェア使用状況サーバと直接通信して、要求されたアプリケーションに対してライセンスが使用可能かどうかを判別します。

**注：** オンライン使用状況では、対象ドメインにわたるライセンス数が数えられます。エージェント上にある同じリリースの複数のインスタンスは無視されます。1 マシン当たりのカウント数は常に 0 または 1 です。

オンラインでの使用状況は、ライセンス数を超えたときにアプリケーションの使用を禁止し、アプリケーションにアクセスしようとするユーザに通知する場合に役立ちます。オンラインでの使用状況は、以下のオプションを使用して設定できます。

### アクションなし ( 監視のみ )

使用の開始および停止のエントリのみを生成します。

### 警告メッセージを表示

使用の開始および停止のエントリの生成、使用中のライセンスの確認を行い、ライセンス数を超えた場合には警告メッセージを表示します。

### 実行を回避して、回避メッセージを表示

使用の開始および停止のエントリの生成、使用中のライセンスの確認を行い、ライセンス数を超えた場合にはアプリケーションの実行を回避します。これらのユーザをキューに格納し、ライセンスが使用可能になったときにアクセスを許可することができます。

**注：** オンラインでの使用状況は、Windows エージェントでのみサポートされます。



## データベースへのオンラインでの使用状況データのインポート

オンラインでの使用状況データは、スケーラビリティ サーバのファイル システムに最長 3 日間のみ保管されます。このデータが将来のレポートに必要な場合、データをスケーラビリティ サーバからインポートして、データベースにエクスポートできます。

### オンラインでの使用状況データをデータベースにインポートする方法

1. 使用状況データをインポートするアセットまたはグループを右クリックし、  
[表示] を選択します。  
[オフラインでの使用状況] ウィンドウが表示されます。
2. [データ] メニューをクリックして [オンラインでの使用状況] を選択します。  
[オンラインでの使用状況] ウィンドウが表示されます。
3. [データ] メニューをクリックして [DB へのインポート] を選択します。

**注：** [DB へのインポート] オプションは、[オンラインでの使用状況] ウィンドウが表示されているときのみ使用可能です。

スケーラビリティ サーバのオンラインでの使用状況データがデータベースにインポートされ、保存されます。

## キュー

アプリケーションの使用可能ライセンスがすべて使用中の場合、キューで待機することを選択できます。このキューは **FIFO** (先入れ先出し) の原則で動作します。つまり、キュー内の最初のユーザが次に使用可能になったライセンスを取得します。このオプションは、[実行を回避して、回避メッセージを表示] オプションを選択した場合にのみ有効になります。

キューに入れられたユーザは、アプリケーションのライセンスが使用可能になると、通知を受け取ります。ユーザがその時点でアプリケーションを使用するように選択する場合は、ダイアログ ボックスで [はい] をクリックすると、アプリケーションが起動されます。制限時間内にユーザが応答しなかった場合、ライセンスが解放され、キュー内の次のユーザに付与されます。

### 非活動時間の検出

定義された一定時間非活動状態であったアプリケーションを閉じて使用中のライセンスが解放されるように、ソフトウェア使用状況エージェントを設定できます。これは、ソフトウェア使用状況収集タスクで設定できます。

**注：**アプリケーションの非活動状態を監視してよいのは、オンライン ソフトウェアの使用状況をトラッキングする場合と、ユーザのためのソフトウェア使用状況を設定する場合のみです。アプリケーションの非活動を監視できるのはユーザのソフトウェア使用状況のみですが、それはアプリケーションとソフトウェア使用状況エージェントが同じアカウントで実行されている場合のみです。コンピュータのためのソフトウェア使用状況では、アプリケーションの非活動状態を監視できません。

**関連項目：**

[ソフトウェア使用状況収集タスクの作成、設定およびスケジュール \(P. 232\)](#)

### 監査

監査を行うと、監視対象のアプリケーションを指定しなくても、コンピュータ上で起動および停止されたアプリケーションが登録されます。ソフトウェア使用状況機能には、実行可能ファイル、DLL ファイル、および Windows サービスを監査する機能が含まれます。

**注：**UNIX エージェントでは、実行可能ファイルに対する監査のみがサポートされます。

監査機能は、ソフトウェア使用状況エージェントと共に実行されるように設計されています。アプリケーションを 1 つ追加してから、ソフトウェア使用状況収集タスク内の「監査」をオンにする必要があります。

**注：**すべてのコンピュータに対して「監査」をオンにすると、大量のネットワークおよびデータベース トラフィックが発生します。この機能は主に、単一のアセットまたはアセット グループで新規または不正なアプリケーションを検出する目的で使用する必要があります。

## タイムスタンプの同期

ネットワーク オペレーティング システムに関係なく、ソフトウェア使用状況エージェントには、受信データのタイムスタンプの正確さを高めるための日時の同期スキームが組み込まれています。この機能は、オンラインでの使用状況を使用している場合のみ使用可能です。同期では、ソフトウェア使用状況サーバの時間が使用されます。

## 使用状況情報の表示

DSM エクスプローラでは、さまざまな形式で使用状況情報が表示され、データの簡単な分析に役立ちます。

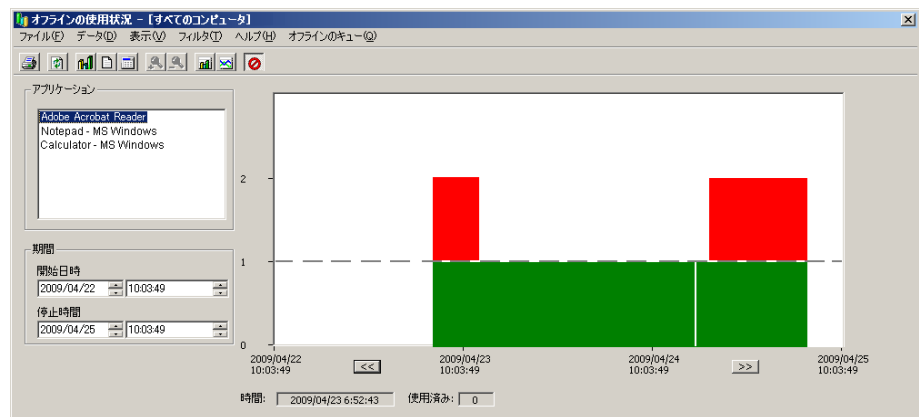
### 使用状況情報を参照する方法

1. [ドメイン] - [コンピュータおよびユーザ] - [すべてのコンピュータ] / [すべてのユーザ アカウント] - [コンピュータ/ユーザ アカウント] - [ソフトウェア] - [使用方法] フォルダに移動します。

右側のペインに、ソフトウェア使用状況の監視用に設定されているすべてのアプリケーションが表示されます。

2. 右側のペインでアプリケーションを選択し、[タスク] セクションで [表示] をクリックします。

[オンラインでの使用状況] / [オフラインでの使用状況] ウィンドウが表示されます。



上の図では、以下の点に注目してください。

- 水平方向の点線は、承認されている（設定可能な）ライセンス数を超えていることを示しています。
- 起動するビューを見つけるには、メニュー バーから [データ] を選択します。ビューは、[グラフ]、[統計]、および [詳細] です。
- [統計] には、指定された時間内に選択されたアプリケーションを使用していたアセットに関する詳細情報が表示されます。
- グラフで選択された期間における、指定したアプリケーションに関するレポートが一覧に表示されます。

## [ グラフ ] ビューの X 軸上の間隔のマーク方法

[ グラフ ] ビューでは、特定の時間におけるデータを表示して、より詳しく調べることができます。

1. 特定の時間におけるデータを表示するには、左マウス ボタンでグラフ エリア内の特定のポイントを選択します。これにより、X 軸（垂直線）が表示されます。
2. 選択したポイントにおける特定のデータを表示するには、マウスの左ボタンを押したままカーソルをドラッグして間隔をマークしてからマウス ボタンを放します。
3. [ ズーム ] アイコンをクリックして、マークした間隔内のデータを表示します。

## ソフトウェア使用状況の制限

Windows の場合、ソフトウェア使用状況には以下の制限があります。

- DOS ベースのアプリケーションには、使用状況情報はありません。
- Unicode はサポートされていません。
- ソフトウェア使用状況は、端末サーバ コンソール セッションではサポートされていますが、端末サービス セッションではサポートされていません。アプリケーションの複数のインスタンスが同時に実行されている場合、ソフトウェア使用状況は、アプリケーションの最初のインスタンスのみをカウントします。
- 端末サーバ上でソフトウェア使用状況を実行する場合、端末サービスのサービスが実行されている必要があります。

## ネットワーク時間

ほとんどのネットワークには、コンピュータの時間をネットワーク（ファイルサーバ）の時間に設定できるユーティリティ プログラムがあります。ログイン スクリプトでこのユーティリティを実行すると効果的な場合もあります。ネットワーク（ファイルサーバ）の時間が正確であれば、これによってすべてのコンピュータの時間が正確に設定されます。

## ソフトウェア使用状況サーバ

ソフトウェア使用状況サーバでは、以下のアクションが実行されます。

- すべてのソフトウェア使用状況エージェントがサーバの管理下に置かれるように、ライセンス情報を管理します。
- キューに格納されたユーザを管理し、使用可能になったライセンスをユーザに割り当てます。
- オンラインのソフトウェア使用状況の監視用に設定されているアプリケーションに関するライセンス キュー情報を保持します。
- リクエストに応じて、ライセンス情報を **DSM** エクスプローラにレポートします。

このサーバはスケーラビリティ サーバをサポートするあらゆるプラットフォームでサービスとして実行できます。

**注：**ソフトウェア使用状況の設定が変更された場合、ソフトウェア使用状況サーバは新しい設定で更新されます。次に、サーバは、現在使用されているライセンスおよびキューに関する情報をリセットします。その結果、エージェントが次にアプリケーションを要求したときは、ライセンス カウントが **1** として表示されます。

## ソフトウェア使用状況およびライセンスにおけるアクセス レベル

アセットのアクセス レベルでは、無償ライセンスの割り当てに関して、その権限が定義されます。

### パワー ユニット

常にアプリケーションを起動できるアセットが含まれています。

### VIP ユニット

無償ライセンスの割り当てで常に優先されるアセットが含まれています。

### 通常ユーザ

無償ライセンスの割り当てに関して、優先順位が最も低いアセットが含まれています。パワー ユニットまたは **VIP** ユニットとして追加されていないアセットは、通常のアクセス権を持ちます。

## アセットへのアクセス レベルの割り当て

ソフトウェア使用状況サーバでは、アセットのアクセス レベルに基づいてライセンスを割り当てます。設定した優先順位に基づいて、コンピュータおよびユーザーに適切なアクセス レベルを割り当てることができます。たとえば、アプリケーションへのアクセスが非常にクリティカルなコンピュータまたはユーザーには、パワー ユニット アクセスを割り当てられます。異なるアプリケーションに対して、異なるアクセス レベルを割り当てることができます。

### アセットにアクセス レベルを割り当てる方法

1. アクセス レベルを割り当てるコンピュータまたはユーザーを右クリックして、[ソフトウェアの権限] を選択します。  
[アセット] ダイアログ ボックスの [ソフトウェアの権限] が表示されます。
2. 権限を割り当てるアプリケーションを指定し、アセットに割り当てるアクセス レベルを選択して [追加] をクリックします。  
指定されたアクセス レベルで、アプリケーションがアセット名の下に追加されます。
3. 複数のアプリケーションにアクセス レベルを割り当てるには手順 2 を繰り返し、[OK] をクリックします。  
アセットにアクセス レベルが割り当てられます。

## エンタープライズ全体でライセンス情報が共有される方法

オフラインでの使用状況を使用すると、エンタープライズ内の複数のソフトウェア使用状況サーバがライセンス情報を共有することができます。ソフトウェア使用状況収集タスクを設定してこの機能を有効にするには、これらのサーバ間でライセンス情報がどのように共有されるかを理解しておく必要があります。

1. スケーラビリティ サーバには、ファイル システム内の接続されているすべてのアセットに関するオフラインでの使用状況データが存在します。
2. このファイルは、各ドメイン複製ジョブによって複製されます。
3. エンジン収集ジョブによって、データベース上の使用方法情報が更新されます。
4. アセットがアプリケーションへのアクセスを要求するたびに、ソフトウェア使用状況エージェントがデータベースを確認して使用可能なライセンスがあるか調べ、それに応じてアプリケーションへのアクセスを許可します。

## ソフトウェア使用状況収集タスクの作成、設定およびスケジュール

ソフトウェア使用状況収集タスクでは、エージェント コンピュータからソフトウェア使用状況情報が収集されます。ソフトウェア使用状況収集タスクを設定して、利用可能なライセンスに基づいたソフトウェア使用状況の制限、監査の有効化、非活動時間パラメータの設定、警告メッセージおよび回避メッセージの指定を行うことができます。

### ソフトウェア使用状況収集タスクを作成、設定、スケジュールする方法

1. アセットまたはグループ レベルで [収集タスク] フォルダに移動し、[新規] をクリックします。  
[新しい収集タスク タイプの選択] ダイアログ ボックスが表示されます。
2. 収集タスクのタイプを選択し、[OK] をクリックします。  
[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。
3. 収集タスクの一意な名前を入力し、[スケジューリングの設定] をクリックします。  
[スケジューリング オプション] ダイアログ ボックスが表示されます。
4. スケジューリング オプションを指定して [OK] をクリックします。  
[スケジューリング オプション] ダイアログ ボックスが閉じ、[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。
5. [アプリケーション] タブを選択して [追加] をクリックします。  
[監視するアプリケーションの追加] ダイアログ ボックスが表示されます。
6. 監視するアプリケーションを選択し、使用可能ライセンス数を指定してから非活動時間を定義します。指定したライセンス数を超えた場合に実行するアクションを選択し、[OK] をクリックします。  
[監視するアプリケーションの追加] ダイアログ ボックスが閉じ、[新規収集タスクのスケジュール] ダイアログ ボックスが表示されます。
7. [オンライン] タブで、オンラインでのソフトウェア使用状況をオンまたはオフにします。[プラットフォーム] タブで、エージェントを実行するオペレーティング システムを選択します。[監査] タブで、監査をオンまたはオフにします。[詳細] タブで、回避メッセージおよび警告メッセージをします。[OK] をクリックします。  
指定された設定およびスケジューリング オプションで、ソフトウェア使用状況収集タスクが作成されます。



関連項目：

[非活動時間の検出](#) (P. 226)

## ソフトウェア使用状況情報の表示

ソフトウェアの使用状況では、アセットで使用されていた監視対象アプリケーションの一覧およびその起動時間と停止時間が表示されます。

### ソフトウェア使用状況情報を表示する方法

1. 情報を表示するレベルに従って、DSM エクスプローラで以下のパスに移動します。

#### グループレベル

##### コンピュータ グループ

ドメイン、コンピュータおよびユーザ、すべてのコンピュータ、グループ詳細

##### ユーザ アカウント グループ

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、グループ詳細

##### ユーザ作成グループ

ドメイン、コンピュータおよびユーザ、グループ、グループ詳細

#### コンピュータ レベル

ドメイン、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

#### ユーザ レベル

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、ユーザ アカウント

2. [ソフトウェア] - [使用状況] フォルダに移動します。

選択されたグループ、コンピュータ、またはユーザで使用可能なソフトウェア使用状況情報が、右側のペインに表示されます。

関連項目：

[ソフトウェア使用状況](#) (P. 219)

## 仮想ホストインベントリ

Client Automation は、プラットフォーム仮想化をサポートします。これは、コンピュータまたはオペレーティング システムのカプセル化で、そこでは、その物理特性がユーザから隠され、実行時にコンピュータ プラットフォームがエミュレートされます。

このドキュメントでは、仮想ホスト インベントリのサポートを説明するために以下の用語を使用します。

- ゲストとは、VMware VM、Solaris ドメインおよび [非グローバル] ゾーン、AIX 論理パーティション、HP-UX nPar および仮想パーティションなどの仮想マシンを表す一般的な用語です。
- 1 つ以上のゲストが、仮想ホスト (アプリケーションまたはハイパーバイザ形式のソフトウェア) によって処理されます。この例は、ESX Server および Sun System Controller になります。
- リモート エージェントとは、別のコンピュータから仮想ホストにアクセスする Client Automation Asset Management エージェントの追加部分です。仮想ホストに Client Automation ソフトウェアをインストールできないので、通常リモート エージェントが実行されます。

仮想ホスト インベントリ収集タスクは、AM リモート エージェントがインストールされた Windows、Linux、UNIX コンピュータおよびエージェントに対して、DSM エクスプローラで設定可能で、Asset Management を使用して企業内に存在する仮想ホストに関する情報を収集できるようになります。仮想ホストの機能によっては、この収集タスクでホスト タイプ、仮想マシンの名前、シリアル番号およびメモリ サイズなどのデータを収集できます。

注：仮想ホスト インベントリ収集タスクは特定のアセットのみに作成できます。他のタイプの収集タスクとは異なり、仮想ホスト インベントリ収集タスクは、ユーザ アカウント用に作成したり、ユーザ アカウントにリンクさせることはできません。この収集タスクを作成するには、関連するアセットに移動します。

関連項目：

[仮想ホスト](#) (P. 412)

## 仮想ホスト インベントリ収集タスクを作成する方法

1 つ以上の仮想ホストに関する詳細情報を仮想サーバから検出および収集するために、仮想ホスト インベントリ収集タスクを作成および設定できます。

新しい仮想ホスト インベントリ収集タスクを作成するには、DSM 管理者が新しい収集タスク タイプの選択ダイアログ ボックスを使用して以下の手順を実行します。

1. 新しい収集タスクを作成し、[仮想ホスト インベントリ] オプションを選択して、そのスケジュール オプションを設定します。
2. [リモート インベントリ収集を設定](#) (P. 235) します。
3. [仮想サーバ](#) (P. 236) を追加します。

## リモート インベントリ収集の設定

リモート インベントリ収集用に設定する仮想ホストのプロパティの追加、削除、表示を行うには、[仮想サーバ] タブ ページを使用します。

### 仮想サーバを収集タスクに追加する方法

1. [仮想サーバ] タブ ページで [追加] をクリックします。  
設定する仮想サーバの追加ダイアログ ボックスが表示されます。
2. 仮想サーバ タイプを選択し、詳細情報を入力します。(詳細については、「仮想サーバの追加」を参照してください。)

**注:** 1 つの収集タスクにつき、仮想サーバを 5 つまで追加できます。同じエージェントで 6 つ以上の仮想化サーバからデータを収集する必要がある場合、同じエージェントに対して追加の収集タスクを定義できます。

1 つの収集タスク当たり 5 つを超える仮想化サーバを追加する場合は、これらの手順に従います。

1. DSM エクスプローラを閉じます。
2. 以下のコマンドを実行します。  

```
ccnfcmda -cmd SetParameterValue -ps itrm/ammanager/hosttypesconfig -pn maxhostcountpertask -v <MAX number of hosts per task> -manager
```
3. DSM エクスプローラを実行して、設定を完了します。
3. [OK] をクリックします。  
[仮想サーバ] タブ ページに戻ります。

4. リストビューの情報が正しい場合は、[OK] をクリックします。  
新しい収集タスク タイプの選択ダイアログ ボックスに戻ります。
5. [OK] をクリックします。  
RVI 設定情報がスケジュールされている次回の実行時に指定されたエージェント コンピュータに転送されます。

## 仮想化サーバの追加

設定する仮想サーバの追加ダイアログ ボックスを使用して、仮想サーバのタイプを選択した後、1 つ以上の仮想サーバを追加します。

以下の手順に従います。

1. [タイプ] ドロップダウン リストからサーバタイプを選択します。有効なタイプは以下のとおりです。
  - HP
  - IBM
  - Sun
  - VMware vSphere Hypervisor (ESX/ESXi)
  - VMware vCenter Server
  - Citrix XenServer
  - Microsoft Hyper-V
2. [ホスト名] フィールドに仮想化サーバ名または IP アドレスを入力します。
3. [ユーザ名] フィールドに、Web サービス ユーザ名を入力します。
4. 指定された仮想化サーバタイプおよびエージェント コンピュータの OS タイプに基づいて、以下の情報を入力します。

注： この手順に続く表に、必須フィールドを一覧表示します。

### パスワード

指定したユーザの Web サービス パスワードを指定します。

注： パスワードおよび SSH キーに関しては、どちらかが認証に必要です。プレーン テキストのパスワードより安全なので、SSH キーを使用することをお勧めします。

### ホストのシリアル番号

(IBM HMC) ホストのシリアル番号を指定します。

## Web サービス URL

Web サービスの URL を指定します。

VMware vSphere Hypervisor( ESX/ESXi )および VMware vCenter Server  
URL の形式は以下のとおりです。

`https://ESXHostFQDNservername/sdk`

## Citrix XenServer

URL の形式は以下のとおりです。

`https://XenMasterFQDNservername`

各インストール内の変数は、サーバの完全修飾ホスト名です。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。

このフィールドのデフォルト動作では、RVI Edit URL 設定ポリシーが変更されていない場合、自動入力されます。このポリシーの詳細については、Asset Management（管理コンソール）ポリシーグループを参照してください。

## SSH キーの場所

SSH（Secure Shell）の秘密鍵の場所を指定します。キーがデフォルトの場所がない場合、Linux/UNIX ホストにのみ SSH キーの場所を提供してください。

注：SSH キーの生成時には、空のパスフレーズが必要です。

5. [リモート インベントリ収集が有効] オプションが選択されていること（デフォルト設定）を確認します。
6. (VMware vCenter Server および Citrix XenServer) 次の手順に進む前に、[フィルタ] タブをクリックしてフィルタリング オプションを指定します。
7. [OK] をクリックします。  
[仮想サーバ] タブ ページに戻ります。
8. [OK] をクリックします。

新しい仮想ホスト インベントリ収集タスクが、Collect Tasks フォルダに追加されます。

## 関連項目：

[Asset Management（管理コンソール）ポリシーグループ \(P. 258\)](#)

以下の表に、指定した仮想サーバタイプおよびエージェント マシンの OS タイプに基づいて必要なフィールドを示します。

| ターゲット/リモート エージェント                     | Windows エージェント ホスト               | Linux/UNIX エージェント ホスト           |
|---------------------------------------|----------------------------------|---------------------------------|
| HP Integrity Virtual Host             | パスワードまたは SSH キーの場所               | (オプション) SSH キーの場所               |
| IBM Hardware Management Console (HMC) | ホストのシリアル番号<br>パスワードまたは SSH キーの場所 | ホストのシリアル番号<br>(オプション) SSH キーの場所 |
| Sun システム コントローラ                       | パスワードまたは SSH キーの場所               | パスワードまたは SSH キーの場所              |
| VMware vSphere Hypervisor (ESX、ESXi)  | パスワード<br>Web サービス URL            | パスワード<br>Web サービス URL           |
| VMware vCenter Server                 | パスワード<br>Web サービス URL            | パスワード<br>Web サービス URL           |
| Citrix XenServer                      | パスワード<br>Web サービス URL            | パスワード<br>Web サービス URL           |
| Microsoft Hyper-V                     | パスワード                            | ホスト名                            |

関連項目：

[Windows リモートエージェント ホスト上での Plink の設定](#) (P. 444)

[VMware ESX セキュリティおよび認証](#) (P. 439)

[環境設定](#) (P. 440)

## リモート エージェントおよび仮想ホストの表示

仮想インベントリは、DSM エクスプローラの [すべてのコンピュータ] ノードの下に表示されます。以下の新規または更新されたノードが表示されます。

| リリース 12.5 ノード  | リリース 12.8 ノード                       |
|----------------|-------------------------------------|
| 設定             | 仮想化/VMware ESX 設定                   |
| サポートされている機能    | 仮想化/VMware ESX 設定/サポートされている機能       |
| 仮想化/データストア     | 仮想化/VMware ESX データストア               |
| 仮想化/サービス コンソール | 仮想化/VMware ESX サービス コンソール           |
|                | 注：このノードは ESXi ではなく ESX でのみ使用できます。   |
| N/A            | 仮想化/VMware 仮想マシン                    |
| N/A            | 仮想化/Citrix XenServer 設定             |
| N/A            | 仮想化/Citrix XenServer 仮想マシン          |
| N/A            | 仮想化/Citrix XenServer ストレージ リポジトリ    |
| N/A            | Virtualization/Microsoft Hyper-V 設定 |
| N/A            | 仮想化/Microsoft Hyper-V 仮想マシン         |

CA Client Automation では、仮想サーバ、仮想ホスト、およびエージェント用のインベントリを収集するすべての検出された AM リモート エージェントを検索および表示できます。クエリ デザイナを使用すると、クエリ結果は、収集に使用するエージェントを設定する [すべてのコンピュータ] の下に表示されます。

関連項目：

[仮想ホストとゲストの関係 \(P. 443\)](#)

[仮想ホストインベントリの表示 \(P. 441\)](#)

## すべてのリモート エージェントの表示

Client Automation にリモート エージェントがインストールされると、このエージェントは **AM リモート エージェント** という名前の新しいエージェント コンポーネントとして登録されます。これは、収集エンティティを表わします。コンピュータのエージェント プロパティを表示すると、**AM リモート エージェント** はエージェント コンポーネント リストに表示されます。

**注：** **AM 仮想エージェント (AMVirtualAgent)** は、このリリースでは収集されたエンティティを表わします。**AM 仮想エージェント**は、実際のエージェントは含まないが、仮想エージェントのみを含む仮想ホストを示します。

リモート エージェントをすべて表示するために、エージェント コンポーネントに基づいたカスタム コンピュータ クエリを作成できます。クエリ結果には、**AM リモート エージェント**がインストールされているすべてのエージェントがリスト表示されます。

以下の手順に従います。

1. **DSM** エクスプローラで [クエリ] を右クリックし、コンテキスト メニューから [新規] を選択します。  
[ターゲットを選択] ダイアログ ボックスが表示されます。
2. [コンピュータ] を選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが表示されます。
3. [一般情報] - [コンピュータ] をクリックします。  
[フィールドを選択] ダイアログ ボックスが開きます。
4. リスト ビューから [エージェント コンポーネント] を選択した後、[引数] グループにある [コンポーネント] ドロップダウン リストから **AMRemoteAgent** を選択します。
5. (オプション) [バージョン] オプションを選択した後、対応するドロップダウン リストからバージョン番号を選択します。
6. [OK] をクリックします。  
クエリ デザイナに戻ります。
7. (オプション) クエリを実行するには、[プレビュー] をクリックします。  
[クエリ プレビュー] ペインに結果が表示されます。
8. [閉じる] をクリックします。  
クエリ デザイナに戻ります。



9. [OK] をクリックします。  
[クエリを保存] ダイアログ ボックスが表示されます。
10. クエリの名前を入力した後、[OK] をクリックして名前を保存します。  
指定した名前のクエリが作成され、[クエリ] - [コンピュータ] に追加されます。
11. (オプション) [クエリ] ペインで検出されたエージェントを右クリックし、コンテキスト メニューから [移動] を選択します。  
[すべてのコンピュータ] の下のエージェント ノードに移動します。このノートで、リモート仮想ホスト インベントリ収集用のエージェントを設定できます。

## すべての仮想ホストの表示

仮想ホストは、他のすべてのコンピュータと共に [すべてのコンピュータ] の下に標準ノードとして表示されます。

仮想ホストのみを表示する場合、コンピュータのクラス ID に基づいたカスタムコンピュータ クエリを作成できます。

### 仮想ホストのみを表示する方法

1. DSM エクスプローラで [クエリ] を右クリックし、コンテキスト メニューから [新規] を選択します。  
[ターゲットを選択] ダイアログ ボックスが表示されます。
2. [コンピュータ] を選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが表示されます。
3. [一般情報] - [コンピュータ] をクリックします。  
[フィールドを選択] ダイアログ ボックスが開きます。
4. リスト ビューから [分類] - [クラスまたはサブクラス] を選択します。
5. 引数グループ ボックスにある [分類] ドロップダウン リストから適切なクラスを選択します。関連するオプションは以下のとおりです。

#### クラス

未分類

#### サブクラス

RTOS

Sun RTOS

クラス

仮想ホスト マシン

ハイパーバイザ

サブクラス

HP Chassis

IBM Server

VMware ESX

VMware ESX Server 3.5

VMware ESX Server 4.0

Sun eXtended System Control Facility (XSCF)

6. [OK] をクリックします。  
クエリ デザイナに戻ります。
7. [OK] をクリックします。  
[クエリを保存] ダイアログ ボックスが表示されます。
8. クエリの名前を入力した後、[OK] をクリックして名前を保存します。
9. 指定した名前のクエリが作成され、[クエリ] - [コンピュータ] に追加されます。
10. [タスク] ポートレットから [クエリの実行] を選択します。  
[すべてのコンピュータ] ペインの下に結果が表示されます。

注: 仮想ホスト用にインストールされたエージェント コンポーネントがないので、仮想ホストにジョブや設定を適用することはできません。そのため、[アセット] コンテキスト メニューは無効になります。

## 関連するコンピュータ/関連ホスト コンピュータ ビュー

仮想化プラットフォーム間の関係を含め、コンピュータの関係を表示できます。サーバ（たとえば、VMware ESX サーバ）を選択すると、管理対象ゲストマシンが「すべてのコンピュータ」の下に「関連するコンピュータ」ペインに関連するコンピュータとして表示されます。

同様に、管理対象ゲスト（たとえば、VMware ゲスト コンピュータ）を選択すると、関連するホストサーバが「すべてのコンピュータ」の下に「関連ホスト コンピュータ」ペインに表示されます。

**注：**DSM エージェントがインストールされた管理対象ゲストにのみ、「すべてのコンピュータ」の下にノードが表示されます。管理対象外ゲストは、「関連するコンピュータ」ペインに表示されません。

## 既存の収集タスクのリンク

さまざまなアセットに対して同じ収集タスクを実行する場合、一度だけ収集タスクを作成して、それをほかのすべてのアセットにリンクすることができます。ドメイン レベル、グループ レベル、およびアセット レベルで作成された収集タスクをリンクできます。

**注：**ドメイン レベルで作成された収集タスクは、ターゲットのアセットにドラッグアンドドロップすることができます。

### 既存の収集タスクをアセットにリンクする方法

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」 - 「ジョブ」 - 「アセット ジョブ」 に移動します。

コンピュータにリンクされている収集タスクがすべて表示されます。

2. 「タスク」 セクションで「既存の収集タスクのリンク」をクリックします。  
「収集タスクの選択」 ダイアログ ボックスが表示されます。

3. リンクする収集タスクを選択し、[OK] をクリックします。  
選択された収集タスクがアセットにリンクされます。

**注：** 仮想ホスト インベントリ 収集タスクは、リモート エージェント (AMRemoteAgent) がインストールされた アセットまたはエージェントのみに作成できます。また、そのタスクは、同じ OS クラスの他のエージェントにのみリンクできます。たとえば、Windows エージェント用に作成された仮想ホスト インベントリ 収集タスクは、他の Windows エージェントにのみリンクすることができます。

## アセットから収集タスクのリンクを解除

アセットまたはアセット グループに対して実行しなくなった収集タスクのリンクを解除できます。

収集タスクのリンクを解除するには、収集タスクを右クリックし、コンテキストメニューから [リンク解除] を選択します。

**注：** アセットから収集タスクのリンクを解除しても、ドメインから収集タスクが削除されるわけではありません。

## 収集タスクのステータスの確認

DSM エクスプローラに表示されるインベントリ情報は、収集タスクが正常に実行されたかどうかによって異なります。

### アセット レベルで収集タスクのステータスを確認する方法

1. [収集タスク] フォルダに移動します。
2. 収集タスクを右クリックし、[ステータス] を選択します。  
[モジュール ステータス] ダイアログ ボックスに収集タスクのステータス詳細が表示されます。

**注：** ステータスおよびステータス コメントの詳細については、F1 キーを押してください。

### 関連項目

[DSM エクスプローラの \[収集タスク\] フォルダへのアクセス \(P. 190\)](#)

## 収集タスクの無効化

収集タスクを作成すると、スキャンが自動的に有効になります。収集タスクを無効にすることによって、エージェント、グループおよびユーザー アカウント上でのスキャンを無効にできます。

### 収集タスクを無効にする方法

1. DSM エクスプローラの [コンピュータおよびユーザー] - [すべてのコンピュータ] に移動します。
2. ドメイン上のすべてのエージェントで収集タスクを無効にするには、[グループの詳細] フォルダを開きます。また、特定のエージェントの収集タスクを無効にするには、[エージェント] フォルダを開きます。
3. [設定] フォルダを開き、[収集タスク] をクリックします。

右ペインには、グループまたはエージェントに適用される収集タスクが表示されます。

4. 収集タスクを 1 つ選択して、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。
5. [無効] を選択します。

個別のエージェント（エージェントを 1 つ選択した場合）、またはすべてのエージェント（[グループの詳細] を選択した場合）に対して収集タスクが無効になります。

## 収集タスクの削除

使用しなくなった収集タスクを削除できます。

### 収集タスクを削除する方法

1. [コントロール パネル] - [設定] - [収集タスク] に移動します。  
右側のペインに、さまざまな収集タスク タイプが表示されます。
2. タスクの収集タスク タイプをダブルクリックします。  
そのタイプで使用可能な収集タスクがすべて表示されます。
3. 削除するタスクを右クリックし、[削除] を選択します。  
[削除の確認] メッセージが表示されます。
4. [はい] をクリックします。  
すべてのリンクしたアセットおよびグループからタスクのリンクが解除され、データベースから削除されます。

## コンテンツ配信を制御する収集タスクの設定

いつコンテンツをドメイン マネージャからスケーラビリティ サーバおよび管理対象エージェントに配信するかを制御できます。エンジン収集タスクがこのコンテンツ配信を実行します。この収集タスクを設定すると、ドメイン サーバ上で新しいサーバが検出された場合に、コンテンツを自動的にスケーラビリティ サーバに配信することができます。また、エンジン収集タスクを設定し、自動コンテンツ配信を除外することもできます。

## エンジン収集タスクの設定による自動配信の除外

Client AutomationDSM エクスプローラ GUI から収集タスクが実行する機能を設定できます。

### エンジン収集タスクを設定し、自動配信を除外する方法

1. DSM エクスプローラを起動した後、以下のパスに示す [エンジン タスク] の正しいノードに移動します。

[ドメイン] - [コントロール パネル] - [エンジン] - [エンジン タスク] - [収集]

選択したドメイン マネージャ上で設定した収集タスクが表示されます。

2. 設定する収集タスクを右クリックして、[プロパティ] オプションを選択します。

[プロパティ] ダイアログ ボックスには、収集タスクのプロパティが表示されます。

3. [収集] タブをクリックします。

4. [選択したタスク] リスト内で [コンテンツ配信] を選択し、左矢印ボタンをクリックします。

[コンテンツ配信] は [使用できるタスク] リストに移動し、収集タスクから除外されます。

5. (オプション) タスクを選択して右矢印ボタンをクリックすると、タスクが [使用できるタスク] リストから [選択したタスク] リストに移動します。

[選択したタスク] リストには、収集タスクに含まれている機能が表示されます。

6. (オプション) タスクを選択して左矢印ボタンをクリックすると、タスクが [選択したタスク] リストから [使用できるタスク] リストに移動します。

[使用できるタスク] リストには、収集タスクから除外されているタスクが表示されます。

7. [OK] をクリックして、変更を確定します。

8. このタスクにリンクされているすべてのエンジンのステータスを再初期化するようにメッセージが表示される場合は、[はい] を選択します。

収集タスクが設定され、コンテンツ配信機能は含まれません。

## オンデマンドによるコンテンツ配信

コンテンツ配信を除外するようにエンジン収集タスクを設定している場合でも、エンジンからスケーラビリティ サーバに現在のコンテンツを配信することが必要な場合があります。この配信を可能にするために、**CADSMCMD** コマンドラインユーティリティを使用して **MDB** からスケーラビリティ サーバにコンテンツを配信するように要求することができます。

コンテンツのオンデマンド配信を実行するには、以下の **CADSMCMD** コマンドオプションを使用します。

```
cadsmcmd scalabilityServer action=collectSector name=<サーバ名> CONTENTDISTRIBUTION
```

このコマンドでは、収集ジョブのデフォルト設定に関係なく、**MDB** から指定したスケーラビリティ サーバへのコンテンツ配信を強制的に実行します。

注：詳細については、「**CLI コマンドリファレンス**」を参照してください。

## プラットフォーム仮想化

### リモート仮想化インベントリ ( RVI )

AM リモート エージェントは、仮想ホストから以下の **RVI** データを収集します。

- 仮想マシンをホストするか、またはそのようなシステムを管理する仮想化サーバのハードウェア インベントリ
- 仮想化サーバのためのソフトウェア パッチ情報（利用可能な場合）
- データ センター、クラスタ、およびリソース プールなどの仮想化情報
- ゲスト名、UUID、電源状態など、各仮想マシン（**VM**）のハードウェア情報

この情報は、電源がオン、一時停止、電源がオフなど、その状態にかかわらず **VM** に関して収集されます。ただし、**VM** の電源がオンで、仮想化ツールがインストールされている場合にのみ、特定の情報を利用できます。

注：RVI エージェントは、Microsoft Hyper-V および XenServer サーバ上で実行されている Linux 仮想マシンからは、特定の BIOS インベントリ属性を収集できません。さらに、SCVMM（Microsoft System Center Virtual Machine Manager）からのインベントリ収集のサポートはありません。



関連項目：

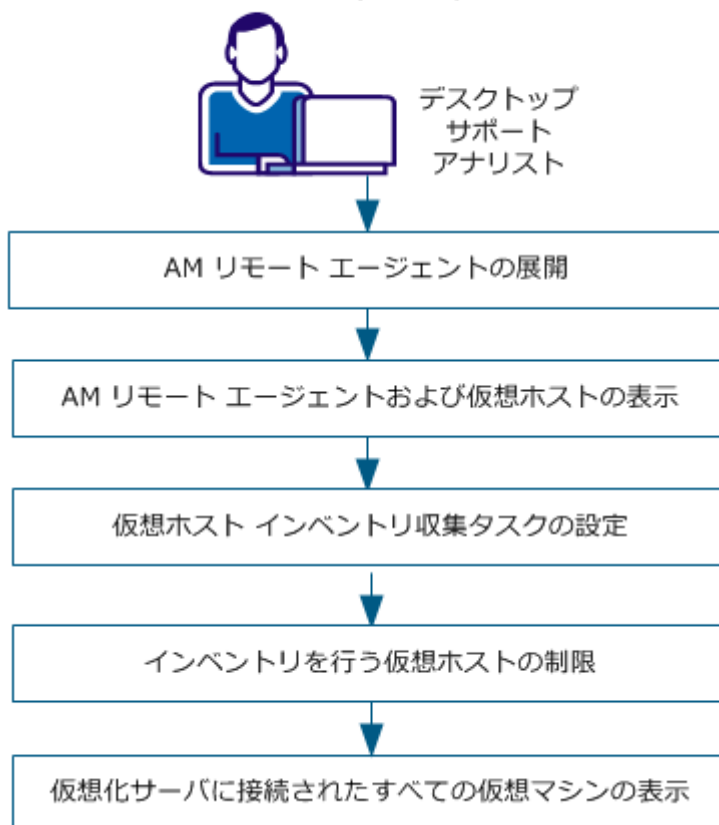
[仮想ホスト インベントリ収集タスクの設定](#) (P. 253)

## 仮想化サーバからの仮想ホスト インベントリの収集

デスクトップ サポート アナリストとして、複数の仮想ホストから RVI (Remote Virtualization Inventory) データを収集できます。仮想ホストは、複数の仮想マシンをホストする仮想化サーバです。仮想ホスト上のインベントリを収集することにより、仮想ホストおよび関連する仮想マシンの関係を識別します。仮想マシンの登録時には、ドメインマネージャは、それを仮想マシンとして識別しません。

インベントリ収集プロセスで、コンピュータに追加のプロパティを追加することにより、仮想マシンが仮想として識別されます。さらに、RVI データには、サーバに関するハードウェアおよびソフトウェア パッチ情報が含まれます。また、データには、各仮想マシンの仮想化情報およびハードウェア情報が含まれます。

### 仮想化サーバからの仮想ホスト インベントリの収集



## AM リモート エージェントの展開

仮想ホストから RVI データを収集するには、物理コンピュータまたは仮想コンピュータ上に AM リモート エージェントを展開します。管理するホストおよび仮想マシンの数に応じて、複数のコンピュータ上に AM リモート エージェントを展開できます。

次の手順に従ってください：

1. DSM エクスプローラを開き、[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エージェントを展開し、CA DSM エージェント AM RVI プラグイン パッケージの 1 つを選択します。
3. ウィザードを完了して展開を開始します。  
ターゲット コンピュータ上で展開が始まります。
4. [コントロール パネル] - [展開] - [展開ジョブのステータス] をクリックします。  
展開ジョブのステータスが表示されます。

## RVI インベントリ収集 DLL のダウンロード

XenServer 用の AM Remote エージェントから RVI インベントリを収集するには、サードパーティの FTP ダウンロード サイトからインベントリ収集 DLL を手動でダウンロードする必要があります。

次の手順に従ってください：

1. [http://opensrcd.ca.com/ips/07400\\_4](http://opensrcd.ca.com/ips/07400_4) を開き、AM リモート エージェント プラットフォームに応じて以下のいずれかを実行します。

### Windows の場合

AM リモート エージェント コンピュータ上の `DSM_install_path¥bin` に  
¥WindowsProductFiles\_x86¥libxenserver.dll をコピーします。

### Linux の場合

AM リモート エージェント コンピュータ上の  
`target/opt/CA/SharedComponents/lib` に ¥LinuxProductFiles\_x86¥libxenserver.so/  
をコピーします。

AM リモート エージェントは、RVI インベントリを収集するように設定されます。

## AM リモート エージェントおよび仮想ホストの表示

AM リモート エージェントだけが仮想ホスト インベントリ データを収集できます。自分の環境内の AM リモート エージェントおよび仮想ホストを理解して、各 AM リモート エージェントに割り当てる仮想ホストを決定できるようにする必要があります。たとえば、9 つの仮想ホストがあり、AM リモート エージェントごとに 3 つのホストを割り当てたい場合があります。利用可能なすべての AM リモート エージェントとホストを表示して、各 AM リモート エージェントに割り当てるホストを決定できます。

次の手順に従ってください：

1. DSM エクスプローラで [クエリ] ノードを右クリックして、[新規] を選択します。  
[ターゲットの選択] ダイアログ ボックスが表示されます。
2. [コンピュータ] を選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが開きます。
3. [クエリ] から [引数の挿入] - [一般情報] に移動して、[コンピュータ] を選択します。  
[フィールドの選択] ダイアログ ボックスが表示されます。
4. リモート エージェントまたは仮想ホストを表示するかどうかに応じて、以下の手順に従います。

■ すべてのリモート エージェントの表示

- a. リスト ビューから [エージェント コンポーネント] を選択した後、[引数] グループにある [コンポーネント] ドロップダウン リストから **AMRemoteAgent** を選択します。
- b. (オプション) [バージョン] ドロップダウン リストからバージョン番号を選択します。

注：あるいは、AM リモート エージェント コンポーネント クエリを持つ Assets を使用して、すべてのリモート AM エージェントを表示できます。

■ すべての仮想ホストの表示

- a. リスト ビューから、[分類] - [クラスまたはサブクラス] に移動します。
- b. [引数] グループ内の [分類] ドロップダウン リストから適切なサーバ名を選択します。

注：リスト内にサーバ名が見つからない場合、リストの末尾で [<続く...>] をクリックします。それでも [指定可能な値の検索] ダイアログ ボックスにサーバ名が見つからない場合は、[結果の制限] をより大きな数にします。

5. [OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスに戻ります。
6. [プレビュー] をクリックします。

クエリは、ユーザの基準に基づいて、リモート エージェントまたは仮想ホストのリストを返します。

## 仮想ホスト インベントリ収集タスクの設定

仮想ホスト インベントリ収集タスクを設定して、仮想化サーバから RVI データを収集できます。

**注：** 完全なゲスト オペレーティング システム インベントリを収集するためには、ハイパーバイザにツールをインストールする必要があります。また、Microsoft Hyper-V サーバ上で実行されている Linux 仮想マシンからは、RVI データを収集できないことに注意してください。

次の手順に従ってください：

1. DSM エクスプローラを開き、[コンピュータおよびユーザ] - [すべてのコンピュータ] - [AM リモート エージェント] - [設定] - [収集タスク] に移動します。
2. [収集タスク] を右クリックし、[新規] を選択します。  
[新しい収集タスク タイプの選択] ダイアログ ボックスが開きます。
3. [仮想ホスト インベントリ] を選択して [OK] をクリックします。

**注：** [仮想ホスト インベントリ] タイプは、AMRemoteAgent がインストールされているアセットにのみ利用可能です。

[新規収集タスクのスケジュール] ダイアログ ボックスが開きます。

4. [一般] タブで収集タスクの名前を入力し、[スケジューリングの設定] をクリックします。収集タスク用のスケジュール オプションを指定して [OK] をクリックします。
5. [仮想化サーバ] タブから [追加] をクリックします。  
[設定する仮想ホストの追加] ダイアログ ボックスが開きます。

**注：** 収集タスクには、5 つの仮想化サーバのみ追加できます。同じエージェントで 6 つ以上の仮想化サーバからデータを収集する必要がある場合、同じエージェントに対して追加の収集タスクを定義できます。

6. 仮想化サーバタイプを選択し、選択した仮想化サーバタイプに対して以下のフィールドに必要な情報を入力して、[OK] をクリックします。

注：選択されたサーバタイプに対して情報が適用可能でない場合、フィールドの一部は無効です。

### ホスト名

インベントリを行う仮想ホストの FQDN を指定します。

### ユーザ名

仮想ホスト上で任意のユーザのユーザ名を指定します。AM リモートエージェントは、このクレデンシャルを使用してシステムにログインし、インベントリを収集します。

### パスワード

指定したユーザのパスワードを入力します。

注：認証には、パスワードまたは SSH キーを使用できます。プレーンテキストのパスワードより安全なので、SSH キーを使用することをお勧めします。

### ホストのシリアル番号

(IBM HMC) ホストのシリアル番号を指定します。

### Web サービス URL

Web サービスの URL を指定します。

URL は、VMware vSphere Hypervisor (ESX/ESXi) および VMware vCenter Server に対して以下の形式になります。

`https://ESXHostFQDNservername/sdk`

URL は、以下の形式の Citrix XenServer となります

`https://XenMasterFQDNservername`

各インストール内の変数は、サーバの完全修飾ホスト名です。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。

デフォルトでは、RVI Edit URL 設定ポリシーが変更されていない場合、このフィールドは自動入力されます。このポリシーの詳細については、Asset Management (管理コンソール) ポリシーグループを参照してください。

### SSH キーの場所

SSH (Secure Shell) の秘密鍵の場所を指定します。キーがデフォルトの場所がない場合、Linux/UNIX ホストにのみ SSH キーの場所を提供してください。

注：SSH キーの生成時には、空のパスフレーズを指定します。

### リモート インベントリ収集が有効

リモート インベントリ収集が有効かどうかを指定します。このオプションが選択されていることを確認します。

7. (オプション) [フィルタ] タブをクリックして、特定のデータ センターまたはクラスターに属するホストを選択します。インベントリが収集されるホストを制限するときに限り、この手順を実行します。詳細については、「[インベントリを行う仮想ホストの制限](#) (P. 255)」を参照してください。

注：[フィルタ] タブは、VMware vCenter Server および Citrix XenServer に対してのみ表示されます。

フィルタは収集タスクに追加されます。

8. [OK] をクリックします。

収集タスクは、次にスケジュールされたランタイムにエージェント コンピュータで実行され、選択されたサーバから RVI データを収集します。

注：仮想ホスト インベントリ収集タスクは、同じ OS クラスの別のエージェントに対してのみリンクできます。たとえば、Windows エージェント用に作成された仮想ホスト インベントリ収集タスクは、別の Windows エージェントにのみリンクできます。

関連項目：

[リモート仮想化インベントリ \(RVI\)](#) (P. 248)

## インベントリを行う仮想ホストの制限

デフォルトでは、収集タスクは、選択された仮想化サーバのすべての仮想ホストをインベントリ処理します。ただし、すべてのホストをインベントリ処理するのではない場合、インベントリ収集をより少数の仮想ホストに制限できます。収集タスクの作成中、または後で既存の収集タスクを変更することにより、フィルタを設定できます。

注：VMware vCenter Server および Citrix XenServer に対してのみフィルタを設定できます。

次の手順に従ってください：

1. DSM エクスプローラを開き、[コンピュータおよびユーザ] - [すべてのコンピュータ] - [AM リモート エージェント] - [設定] - [収集タスク] に移動します。

設定およびスケジュールされたインベントリ収集タスクのリストが表示されます。

2. フィルタを設定するタスクを右クリックして、[プロパティ]を選択します。  
[プロパティ] ダイアログ ボックスが開きます。
3. [仮想化サーバ] タブからホストを選択し、[プロパティ] をクリックします。

[仮想ホスト設定の更新] ダイアログ ボックスが開きます。

4. [フィルタ] タブをクリックし、VMware vCenter Server のデータ センター、クラスタ、およびホスト レベルでフィルタを指定します。Citrix XenServer のホスト レベルでのみフィルタを指定できます。

注：フィルタ内で使用されるすべての名前に対して、アスタリスク (\*) およびパーセント (%) ワイルドカード文字を使用できます。

5. [OK] をクリックします。

フィルタは収集タスクに設定されます。収集タスクは選択したホストからのみ RVI データを収集します。

## 仮想化サーバに接続されたすべての仮想マシンの表示

AM リモート エージェントがインベントリを収集した後、ホストと仮想マシンの関係を表示できます。[すべてのコンピュータ] 下の仮想化サーバを選択します。右ペインの [ホームページ] タブには、[環境] ポートレット下の [関連するコンピュータ] ビューに管理対象ゲストが表示されます。

たとえば、[VMware ESX - 790-1g2-i2duo] ノードを選択した場合、[関連するコンピュータ] ビューに VMware 管理対象ゲストが表示されます。

同様に、[すべてのコンピュータ] 下で同じ管理対象 VMware ゲストを選択すると、アセットのホームページ上の [関連するコンピュータ] ビューに、それに関連するホストサーバ (VMware ESX - 790-1g2-i2duo) が表示されます。

注：[関連するコンピュータ] ビューには、管理対象ゲストのみ、つまりその上に DSM エージェントがインストールされているゲストのみ表示されます。



## 設定ポリシー

### Asset Management ( エージェント ) ポリシー グループ

リモート仮想インベントリ用の **Agent** ポリシー グループ下およびレガシー **VMware ESX** 仮想化インベントリの表示下に、新しいポリシー サブグループ (**Asset Management**) が追加されています。

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。

**Asset Management** 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。

#### RVI レガシー インベントリ

**DSM** エクスプローラ内で、**VMware ESX** 仮想化インベントリが [すべてのコンピュータ] 下のレガシー リリース **12.9** の位置および新しい位置に表示されるかどうかを指定します。

[はい] に設定すると、レガシー **VMware ESX** 仮想化インベントリは、**DSM** エクスプローラ ツリー内で両方の場所に表示されます。 [いいえ] に設定すると、レガシー **VMware ESX** 仮想化インベントリは新しいリリース **12.9** の場所にもみ表示されます。

以下の表に、**VMware ESX** インベントリのレガシーおよび現在の位置を示します。

| リリース 12.5 ノード                                                   | 現在のノード                        |
|-----------------------------------------------------------------|-------------------------------|
| 設定                                                              | 仮想化/VMware ESX 設定             |
| サポートされている機能                                                     | 仮想化/VMware ESX 設定/サポートされている機能 |
| 仮想化/データストア                                                      | 仮想化/VMware ESX データストア         |
| 仮想化/サービス コンソール                                                  | 仮想化/VMware ESX サービス コンソール     |
| 注： このノードは <b>VMware ESXi</b> ではなく、 <b>VMware ESX</b> でのみ利用可能です。 |                               |

デフォルト： いいえ、<ローカル管理>

### Asset Management ( 管理コンソール ) ポリシー グループ

仮想ホスト インベントリ収集タスクを作成するときに、**Web サービス URL** を指定するため、新規ポリシー サブグループ (Asset Management) が管理コンソール ポリシー グループ下に追加されます。

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。

Asset Management 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。

#### RVI 編集 URL

仮想ホスト インベントリ収集タスクで、**Web サービス URL** を手動で入力または編集できるかどうかを指定します。**Web サービス URL** フィールドは、収集タスクで自動的に入力されます。これは、このポリシーで設定された値にかかわらず、ホスト名に基づきます。

**True** の場合、**Web サービス URL** フィールドは有効であり、**URL** を編集できます。

注：その後、[ホスト名] フィールドを変更する場合には、**Web サービス URL** フィールドを更新してください。

**False** の場合、**Web サービス URL** を編集できず、またこのフィールドは無効です。

デフォルト：False、<ローカル管理>

関連項目：

[仮想化サーバの追加](#) (P. 236)

## クエリおよびレポート

### クエリ

クエリ デザイナでクエリを作成するときには、現在、仮想化サーバおよび仮想ホストについてレポートするための追加の引数を使用できます。また、以下の事前定義済みクエリを使用できます。

- アセットは仮想マシンです - Citrix XenServer
- アセットは仮想マシンです - Microsoft Hyper-V
- アセットは仮想マシンです - VMware ESX

## レポート

拡張されたプラットフォーム仮想化サポートのため、DSM レポーターに以下のレポートが追加されます。

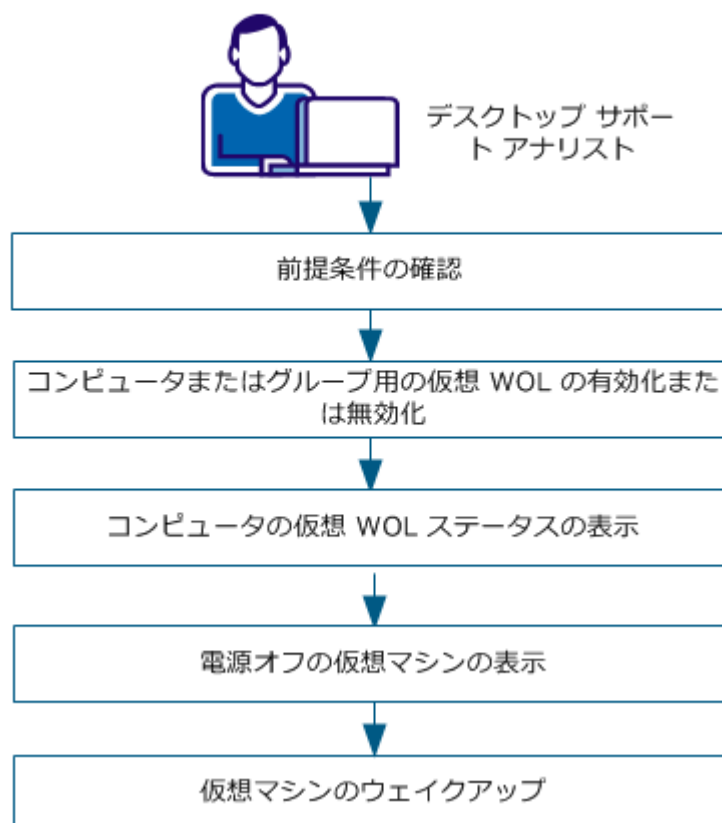
- すべての XenServer ホストおよび XenServer 仮想マシン
- すべての Hyper-V ホストおよび Hyper-V 仮想マシン

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、仮想化サーバおよびそれに対応する仮想マシンがすべてリスト表示されます。

## 仮想マシンのウェイクアップ ( 仮想 WOL )

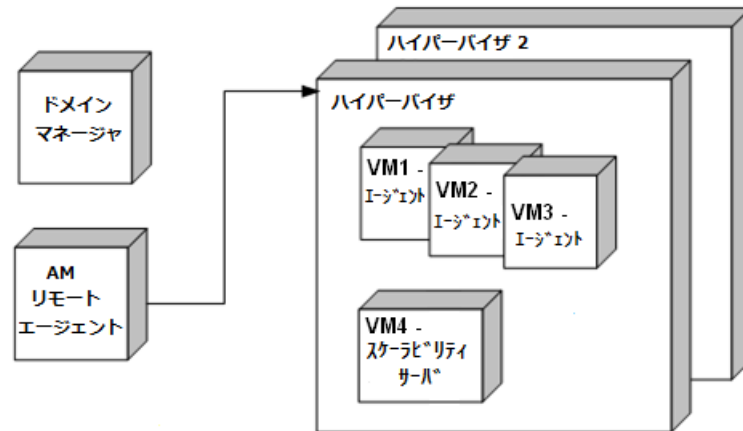
デスクトップ サポート アナリストとして、一時停止またはスリープ モードの単一またはグループの仮想マシンを、リモート コンピュータから起動できます。Client Automation は、仮想マシンをウェイクアップするために、仮想 WOL (vWOL) をサポートしています。

### 仮想マシンのウェイクアップ ( 仮想 WOL )



## 仮想環境シナリオ

典型的な仮想環境には、ドメイン マネージャ、AM リモート エージェント コンピュータ、および以下の図で表示されるような DSM エージェントやスケーラビリティ仮想マシンを含めて、さまざまな仮想化サーバ タイプが含まれます。



DSM ドメイン マネージャは、すべてのコンピュータを管理します。また、AM リモート エージェント コンピュータは、RVI および仮想 WOL の両操作のための VM に関する詳細を収集します。

このシナリオでは、以下の方法を使用して、仮想 WOL を実行できます。

- 仮想マシンに **Software Delivery** ジョブを送信

ジョブ コンテナは、該当するスケーラビリティ サーバに送信されます。それにより、CAF API の WOL 機能を使用して VM がウェイクアップされます。

- ドメイン マネージャで DSM エクスプローラを使用し特定の VM をウェイクアップ

詳細については、「[DSM エクスプローラを使用した仮想マシンのウェイクアップ](#) (P. 265)」を参照してください。

- リモート コントロールを使用して、まず VM をウェイクアップすることにより接続

- [接続設定] - [詳細] タブで [電源オン] をクリックすると、リモート コントロールが VM をウェイクアップします。また、スリープモード VM に接続できます。ウェイクアップして VM に接続するかどうかを確認するメッセージが表示されます。

- OS インストール ジョブの一部として仮想マシンをウェイクアップするために OSIM ブート サーバにリクエストを送信

OS インストールの起動中に、[OS インストールのセットアップ] ダイアログ ボックスで Wake-On-LAN オプションを設定できます。

## Client Automation が仮想マシンをウェイクアップする方法

仮想マシンをウェイクアップする方法は、物理コンピュータのウェイクアップに使用する方法とは異なります。各プラットフォーム仮想化ベンダーは、WOL 操作に対してそれぞれ独自の SDK を提供しています。AM リモート エージェントは、すでにこれらの SDK を使用してインベントリを収集しているので、エージェントは新しい一般的な SendWOL メソッドを使用して仮想 WOL を実行できます。Client Automation は、以下処理を使用して仮想マシンをウェイクアップします。

- 仮想マシンを DSM ドメイン マネージャに登録する時点では、ドメイン マネージャは、最初はそれが仮想マシンであることを認識しません。次回に AM リモート エージェントが実行され、仮想マシンとそのホスト間で必要な関係情報を送信する時点でのみ、WOL プロトコルタイプが「nw」から「vm」に変更されます。また、このアクションは、仮想マシン（仮想マシンに対するデフォルト設定）上の WOL を無効にします。
- AM リモート エージェントは、仮想化サーバから VM に関する以下のインベントリ情報を収集し、DSM ドメイン マネージャと MDB にこの情報をレポートします。

注：RVI エージェントは、Microsoft Hyper-V および XenServer サーバ上で実行されている Linux 仮想マシンからの特定の BIOS インベントリ属性を収集できません。仮想 WOL は、そのような Linux 仮想マシン上ではサポートされていません。

- ウェイクアップのための VM の親仮想化サーバの FQDN。
- プラットフォーム仮想化タイプ（VMware ESXi、Microsoft Hyper-V など）
- 仮想化サーバのためのログイン クレデンシヤル
- VM のためのベンダーに固有の識別文字列

注：通常、文字列は仮想 GUID ですが、システム ID またはシリアル番号の場合もあります。

- AM リモート エージェントは、`CA\DSM\Agent\units\00000001\am\rvi` フォルダ下の `rvidb.txt` という名前の単純なフラット ファイルにこの情報を格納します。その URL が指定された場合、このファイルにアクセスして、仮想化サーバに関する情報を追加および取得することができます。このファイルが無制限に大きくなるのを回避するため、古くなったすべての仮想化サーバ、およびそれぞれの VM のリストは、1 年後に自動的に削除されます。
- ドメイン マネージャは、vWOL リクエストを受信すると、スケーラビリティサーバにリクエストを委任します。スケーラビリティサーバは、次に、それを AM リモート エージェント コンピュータに委任します。その後、AM リモート エージェント コンピュータは仮想マシンをウェイクアップします。

## 前提条件の確認

仮想 WOL の動作には、以下の前提条件が必要です。

- 物理コンピュータまたは仮想マシンに、AM リモート エージェント（RVI 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。仮想 WOL は、常に AM リモート エージェントを実行するコンピュータから実行されます。

注： RVI エージェントは、Microsoft Hyper-V および XenServer サーバ上で実行されている Linux 仮想マシンからの特定の BIOS インベントリ属性を収集できません。仮想 WOL は、そのような Linux 仮想マシン上ではサポートされていません。

- スケーラビリティ サーバが AM リモート エージェント コンピュータと通信できることを確認します。仮想 WOL リクエストは、スケーラビリティ サーバから AM リモート エージェントにルーティングされます。
- AM リモート エージェントが、ユーザがウェイクアップした VM からの仮想化データを検出し収集したことを確認します。AM リモート エージェントは、インベントリ収集タスクを通じて仮想化データを収集します。インベントリ収集が実行されるまで、WOL 操作は、ターゲット コンピュータは物理コンピュータであり、仮想コンピュータではないと仮定します。インベントリ収集には、検出および登録される VM の数に応じた時間がかかります。

注：無料バージョンではホストへの API アクセスが制限されるので、仮想 WOL は、無料バージョンの VMware ESXi 上で実行されるゲストではサポートされていません。

## コンピュータまたはグループ用の仮想 WOL の有効化または無効化

仮想 WOL は、デフォルトではすべての仮想マシン上で有効です。仮想化サーバが多数の VM をホストする場合で、それらを同時に実行するリソースが不足している場合には、その VM 上で仮想 WOL を無効にできます。リモートからコンピュータの電源をオンにする場合、それを有効に戻すことができます。

次の手順に従ってください：

1. コンピュータまたはグループを右クリックし、[電源オン] - [無効] を選択します。

仮想 WOL は、コンピュータ上で無効になります。コンピュータまたはグループは、「ウェイクアップなし」グループに追加されます。

2. コンピュータまたはグループを右クリックし、[電源オン] - [電源オン] がグレー表示されていることを確認します。

このアクションにより、仮想 WOL が無効であることが確認されます。

## コンピュータの仮想 WOL ステータスの表示

コンピュータの仮想 WOL ステータスを表示して、Client Automation を使用して電源をオンにできるかどうかを知ることができます。DSM エクスプローラで、以下のいずれかのノード内でステータスを表示できます。

- 仮想マシンのホーム ページ タブ上の [エージェント ステータス] ポートレット下で有効になっている電源オン
- [コンピュータ プロパティ] ダイアログ ボックス上の [電源をオンにできません] オプション

注：このオプションは、ソフトウェア配信や DTS など、一括ウェイクアップを実行できる DSM コンポーネントでのみ利用可能です。[電源をオンにできません] オプションは、リモート コントロールには適用できません。

- コンピュータ ベース クエリ用クエリ デザイナの [引数の追加] ダイアログ ボックス内の [コンピュータ] - [一般] - [コンピュータ] 下の [電源オン] オプション

## 電源オフの仮想マシンの表示

仮想マシンをウェイクアップする前に、電源がオンかオフかを知る必要があります。電源がオフのもののみウェイクアップします。特定の仮想化サーバ上の仮想マシンの電源オン ステータスを表示するには、[すべてのコンピュータ] - [仮想化サーバ] - [インベントリ] - [仮想化] - [サーバ仮想マシン] に移動します。右ペインで [状態] 列を表示します。

## CLI を使用した仮想マシンのウェイクアップ

CLI を使用して、仮想マシンをウェイクアップすることができます。たとえば、バッチ スクリプトを使用して、複数の仮想マシンをウェイクアップしたい場合があります。以下のコマンドで、仮想マシンをウェイクアップします。

```
caf sendwol [user username password password] vm vGUID guid vsvr url rviagent fqdn
username および password
```

AM リモート エージェント コンピュータ上の管理者ユーザのクレデンシアルを指定します。CLI を実行しているのと同じコンピュータ クレデンシアルを使用する場合、このパラメータをスキップできます。

**vm**

仮想 WOL を実行する必要があることを指定します。

**vGUID**

ホストが認識している仮想マシンの ID を指定します。ID は、プラットフォーム仮想化サーバタイプに応じて、仮想 GUID、システム ID、またはシリアル番号にすることができます。

**vsvr**

現在の仮想マシンの仮想サーバ ホストの URL を指定します。

**rviagent**

仮想マシンを検出した AM リモート エージェントの FQDN を指定します。

### 仮想 WOL の例

この例では、仮想マシン上で仮想 WOL を実行します。

```
caf sendwol user root password secret vm vsvr https://virt.acme.com/sdk vguid 123456
rviagent rvi3.acme.com
```

注：CAF コマンドの詳細情報については、「caf <command> /?」と、コマンドプロンプトで入力してください。



## DSM エクスプローラを使用した仮想マシンのウェイクアップ

DSM エクスプローラから仮想マシンをウェイクアップすることができます。ウェイクアップする仮想マシンを右クリックし、[電源オン] オプションを選択します。このアクションは、コンピュータの仮想 WOL リクエストを送信します。仮想マシンに接続して、仮想マシンがウェイクアップされているかどうか確認します。

# グリーン IT レメディエーション

## GreenIT レメディエーションの実装

デスクトップ サポート アナリストは、最適な電力消費量を保証するために組織内の電源設定および電力スキームを設定できます。 **Client Automation** を使用して、指定された時間（たとえば業務終了後、週末、休日など）に自動的に電源を落とすように、コンピュータの設定ポリシーを定義およびプッシュします。また、現在の電源スキームを監視し、組織にわたって標準的な **Windows** 電源スキーム実装を定義できます。

GreenIT レメディエーションを実装するには、以下のタスクを実行します。

前提条件の確認

コンピュータの自動的な省電力の設定

グリーン IT レメディエーションに対するインベントリの更新

Software Delivery への GreenIT レメディエーションの影響

### 前提条件の確認

グリーン IT レメディエーションを実装する前に、以下の前提条件を確認します。

- ターゲット コンピュータに DSM のエージェントがインストールされることを確認します。 **Client Automation**、**CA IT Inventory** マネージャ、または **ecoDesktop** の一部として DSM エージェントをインストールできます。

## コンピュータの自動的な省電力の設定

特定のコンピュータまたはコンピュータのグループに対して自動的な省電力を設定できます。自動的な省電力では、業務終了後、週末、休日など、指定された時間に自動的にコンピュータの電源を落とすことにより、エネルギーを節約できます。

次の手順に従ってください：

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] に移動します。

### 設定ポリシー名

自動的な省電力設定を定義しているコンピュータまたはグループに適用されるポリシーの名前を指定します。

2. 設定ポリシーを右クリックし、[封印解除] をクリックします。
3. [DSM] - [共通コンポーネント] - [CAF] - [GreenIT 省電力] に移動します。
4. [GreenIT: 省電力] を有効にします。
5. [DSM] - [共通コンポーネント] - [CAF] - [シャットダウン] - [電源管理カレンダー] - [時間範囲] に移動します。

[電源管理カレンダー] ダイアログ ボックスが開きます。

- 指定されたパラメータに対して必要な値を指定します。

#### 時間

自動的な省電力アクションの時間を指定します。 **Software Delivery** シャットダウン機能とは異なり、自動的な省電力では、時間範囲の開始時刻のみ使用して省電力ジョブをスケジュールします。これは、時間範囲の開始時刻が、自動的な省電力アクションがトリガされる時間であることを意味します。時間範囲の終了時刻を指定しても、**GreenIT** の自動的な省電力機能に影響しません。

[タイプ] フィールドで、以下のいずれかの値を選択します。

#### 標準の曜日

省電力アクションが実行される平日を指定します。

#### 特別な日付

yyyy-mm-dd 形式で日付を指定します。日付がゼロの場合、毎年、毎月、または毎日、設定が適用されることを示します。

##### 例

指定された日付が **2012-00-08** の場合、ジョブは、**2012** 年の毎月 **8** 日に実行されます。指定された日付が **00-08-00** の場合、ジョブは、毎年 **8** 月のすべての日に実行されます。

#### 日付範囲

開始日と終了日の間の各日を含みます。

##### 例

指定された日付範囲が **2012-05-01 ~ 2012-05-11** の場合、ジョブは、**2012** 年 **5** 月 **1** 日から **11** 日まで、すべての日に実行されます。

自動的な省電力アクションの条件が定義されます。

- ターゲット コンピュータまたはコンピュータ グループに、この設定ポリシーをコピーします。

スケジュールされた時間に、**Client Automation** は、自動シャットダウン、休止状態、スリープ、電源オフのための開始タイマ メッセージを表示します。ユーザアクション（今すぐシャットダウン、今すぐハイバネート、今すぐスリープ、今すぐディスプレイをオフ、延期、またはキャンセル）に基づいて、コンピュータの電源がオフになります。ユーザからの応答がない場合、カウントダウンの終了のタイムアウトで、スケジュールされたアクションが自動的に実行されます。

**例：**

毎日、午後 6 時から午前 9 時まで自動的な省電力時間を指定するとします。コンピュータにログオンしているユーザは、コンピュータに対してスケジュールされた電源オフに関して午後 6 時にアラートを受け取ります。以下のいずれかのオプションをクリックできます。

**今すぐシャットダウン、今すぐハイバネート、今すぐスリープ、今すぐディスプレイの電源オフ。**

省電力アクションをただちに適用します。省電力状態（シャットダウン、ハイバネート、ディスプレイの電源オフ、スリープなど）からコンピュータを再開した場合、次に定義されている省電力スケジュールに従って省電力が再び開始されます。

**延期**

省電力アクションをしばらく延期します。延期する時間、および省電力アクションを適用するまでに「延期」をクリックできる最大回数を指定できます。

**キャンセル**

省電力アクションをキャンセルします。タイマおよびポップアップダイアログボックスがキャンセルされます。省電力は、次に定義された省電力スケジュールに従って再度開始されます。

カウントダウン タイムアウトの最後にユーザからの応答がない場合、省電力アクションが自動的に適用されます。

## グリーン IT レメディエーションに対するインベントリの更新

以下の表は、インベントリの別のノードに追加された新しいフィールドのリストを示しています。

| インベントリ ノード                 | フィールド                                | 説明                                                                                                                                                                                             |
|----------------------------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [一般インベントリ]、[電源設定]、[電源ポリシー] | AC - プロセッサ スロットル<br>DC - プロセッサ スロットル | CPU スロットリングまたはプロセッサ スロットリングは、CPU が過熱による損傷を防止するための処理です。CPU 温度が指定された限度を超えると、システムは、冷却のために CPU を減速します。この処理は、コンピュータがアイドルの場合、または重要なタスクが実行されない場合に実行されます。CPU は、低周波数に切り替えてエネルギー消費を最適化し、またファンの騒音を最小化します。 |

## Software Delivery への GreenIT レメディエーションの影響

Software Delivery の [電源管理カレンダー] により、指定されたハードウェアを電源オフに設定するときに、管理者が時間範囲を定義できるようになります。GreenIT 省電力では、省電力設定の定義に使用するのと同じカレンダーを使用します。両方の機能が有効な場合、1 つの機能に対して設定される時間スケジュールが、別の機能にも適用されます。

一時停止やシャットダウンなどの **GreenIT** 省電力アクションが開始された場合、ユーザに対して省電力ダイアログ ボックスが表示されていると、**Software Delivery** エージェントは実行されません。省電力が完了した後、**Software Delivery** エージェントは、**WOL** 機能を使用してコンピュータを起動し、**Software Delivery** ジョブを実行します。

**注:** [今すぐディスプレイの電源オフ]ダイアログ ボックスが表示されている間、またはディスプレイのオフ操作の進行中に、ソフトウェア配信が実行されます。

ソフトウェア配信中にグリーン IT 省電力ジョブが開始されると、自動省電力アクションは、ソフトウェア配信が完了するまで、またはタイムアウトが終了するまで待機します。この動作は、省電力アクション [今すぐディスプレイの電源オフ] には適用されません。

以下の設定パラメータを使用して、**Client Automation** が開始する省電力アクション、またはユーザが開始する電源アクションが、**Software Delivery** ジョブの進行中に許可されるかどうかを指定します。

### CAF: 省電力アクションを許可

**Software Delivery** ジョブ中に、**Client Automation** が開始する任意の省電力アクション（ディスプレイの電源オフは除く）を許可するかどうかを指定します。このパラメータは、[スタート] メニューから開始されるアクションを制御しません。また、このパラメータは、**Software Delivery** ジョブ中に、**Windows** 電源スキームによって開始されるスリープアクション、またはハイバネートアクションを防止するかどうかを指定します。

### 再起動：アプリケーションによるログオフおよび再起動を許可

**Software Delivery** ジョブの進行中に、ログオフ、再起動、またはシャットダウンアクション（ユーザが開始したアクションを含むが、スリープ、ハイバネート、ディスプレイのオフの各アクションは除く）を許可するかどうかを指定します。

両方のパラメータは、デフォルトでは [はい] に設定されています。この状態で **Software Delivery** ジョブが進行中の場合、**Client Automation** が開始した省電力アクション（シャットダウン、ハイバネート、またはスリープ）とユーザが開始したシャットダウンアクションの両方を許可しません。一貫した動作を保証するため、両方のパラメータを同じ値に設定することをお勧めします。両方のパラメータを [はい] に設定できます。その場合、進行中、またはユーザからの入力を待機中の **Software Delivery** ジョブが中止され、再起動、ログオフ、またはシャットダウンが実行されます。

[DSM] - [共通コンポーネント] - [CAF] - [一般] で利用可能な以下の設定パラメータの使用することにより、**Client Automation** が開始する省電力アクションに対して、延期タイムアウトを設定できます。

#### CAF: 最大電源アクション延期タイムアウト

省電力アクションを実施する前に、CAF がプラグインの完了を待機する最大時間値を指定します。

デフォルト値は **7200** 秒に設定されています。**0** に設定すると、延期タイムアウトは許可されません。

または、**Software Delivery** ジョブの進行中は、**Client Automation** が開始する省電力アクションを延期できます。

次の手順に従ってください：

1. [DSM] - [共通コンポーネント] - [CAF] - [一般] - [CAF 電源アクションの延期] に移動します。
2. [CAF プラグイン: **Software Delivery** エージェント] パラメータを [有効] に設定します。

注：Asset Management については、[CAF プラグイン: Asset Management エージェント] パラメータを有効に設定します。このパラメータを有効にすると、Asset Management ジョブの進行中は、**Client Automation** が開始する省電力アクションが延期されます。





# 第 6 章 : Asset Management のカスタマイズ

---

ビジネスのニーズに合わせてたり環境をより制御するために、アセット ジョブ、クエリ、ポリシーなどをカスタマイズできます。

このセクションには、以下のトピックが含まれています。

[管理情報フォーマット \(.MIF\) ファイル](#) (P. 274)

[ジョブ](#) (P. 278)

[クエリ](#) (P. 291)

[ポリシー](#) (P. 298)

[Asset Collector](#) (P. 321)

[Client Automation に CA Mobile Device Management を統合する方法](#) (P. 377)

[エージェントブリッジ](#) (P. 393)

[Intel AMT と CA ITCM を統合する](#) (P. 403)

[仮想ホスト](#) (P. 412)

[Windows リモートエージェント ホスト上での Plink の設定](#) (P. 444)

[非常駐インベントリ](#) (P. 446)

[DSM レポーター](#) (P. 487)

[CA Asset Converter for Microsoft SCCM](#) (P. 496)

## 管理情報フォーマット ( .MIF ) ファイル

管理情報フォーマット ( .MIF ) ファイルは、ハードウェアまたはソフトウェアのコンポーネントデータの記述に使用されます。MIF ファイルは、アセット管理システムによりシステム設定情報をレポートする場合に使用されます。アセット管理では、スケジュールされたインベントリ、テンプレート、設定ファイル、および外部アセット定義はそれぞれ mif ファイルで構成されます。

.MIF ファイルはテキスト ファイルであり、サービス レイヤにインストールされ、MIF データベースに追加できるように表示されます。.MIF ファイルはテキストエディタで変更できますが、このプロセスを自動化できるコンポーネントプロバイダを使用することをお勧めします。Distributed Management Task Force (DMTF) により、Desktop Management Interface (DMI) 仕様における .MIF ファイルの仕様が策定されました。

アセット管理では、.MIF ファイルを使用して、[エージェント作業ディレクトリ](#) (P. 32) にローカルに情報を登録および格納します。

### Asset Management での MIF ファイルの使用方法

アセット管理では、.MIF ファイルを使用してエージェント作業ディレクトリに情報を登録および格納します。これらの .MIF ファイルは、DMI 仕様に従って作成されます。アセット管理では、ユーザにこれらの .MIF ファイルの情報の入力要求できる .MIF ファイルの特定の拡張機能が使用可能になっています。ユーザに特定の値を選択させる機能が、この一例です。ローカル コンピュータおよびローカル ユーザ ディレクトリに置かれた各 .MIF ファイルは、エージェントによって処理されます。これらすべての .MIF ファイル内の情報は、スケーラビリティ サーバに送信されます（また、エンジンによってドメイン データベースに送信されます）。

アセット管理では、以下の場合に MIF ファイルが使用されます。

- テンプレート インベントリの収集（Windows エージェントのみ）
- 外部アセット情報の収集（外部アセット認識）

関連項目：

[ユーザ作業ディレクトリ](#) (P. 32)

## テンプレート インベントリで MIF ファイルが使用される方法

テンプレート インベントリ モジュールを使用すると、MIF ファイルからカスタマイズ済みのインベントリ情報を収集できます。これは、どのインベントリ検出モジュールによっても収集されない情報です。アセット管理では、以下のプロセスを使用して、情報を MIF ファイルに格納し、また MIF ファイルから情報を取得します。これらのアクションを理解することにより、MIF ファイルを要件に合わせて最適に設定する方法を選択できます。

- アセット管理エージェントは、テンプレート インベントリ収集タスクの実行時にテンプレート インベントリごとに MIF ファイルを作成して、収集済みのインベントリ情報を格納します。
- エージェント ソフトウェアにより、ローカル コンピュータまたはユーザディレクトリ内に置かれた各 MIF ファイルが処理されます。アセット管理では、圧縮アルゴリズムを使用してこれらの .MIF ファイルのサイズを縮小し、ファイル転送時間を短縮しています。圧縮されたファイルの名前は MIF ファイルと同じですが、拡張子は .MNV になり、コンピュータまたはユーザの BAK ディレクトリに格納されます。

**注：** エージェントでは、DMI 仕様に準拠する .MIF ファイルのみが処理されます。

- エージェントが初めて実行される場合、または BAK ディレクトリが削除されている場合は、エージェントによって全インベントリがスケーラビリティ サーバに送信されます。全インベントリを収集するために、手動で通知を送信することもできます。それ以外の場合は、差分値のみが送信されます。BAK ディレクトリには、エージェントで現在のインベントリ値と以前のスキャン値の比較に使用される情報が含まれています。
- 現在のインベントリ値と以前に収集されたインベントリ値の差分がスケーラビリティ サーバに送信されます。このデータは、...¥ServerDB¥SECTOR¥COLLECT で使用可能になります。
- エンジンにより収集エリアからこの情報が収集され、それに応じてドメインデータベースが更新されます。

## 外部アセット認識で MIF ファイルが使用される方法

アセット管理では、外部アセットを認識するために以下のオブジェクトが必要になります。

- 外部アセット定義
- アセット情報が含まれた MIF ファイル

アセット管理では、エンタープライズ内の外部アセットを認識できます。外部アセットとは、コンピュータとユーザ以外のアセット（たとえば、プリンタなど）です。このプロセスを理解しておくと、外部アセットを認識できるように MIF ファイルを設定する際に役立ちます。

- 外部アセット定義には、スケーラビリティ サーバの収集エリアに存在する適切な MIF ファイルを識別する認識項目が含まれています。
- エンジンにより、収集エリア（Windows では `...¥ServerDB¥SECTOR¥COLLECT`、Linux では `/ServerDB/SECTOR/COLLECT`）内の各 MIF ファイルが収集されます。
- 外部アセット定義内の認識項目が MIF ファイル内の値と一致しているかどうかを確認されます。
  - 一致が見つかり、エンジンにより、外部アセット定義内に設定されている情報が収集され、指定した名前新しい外部アセットが作成されて、収集エリアからファイルが削除されます。
  - 一致が見つからない場合、エンジンによって MIF ファイルが削除されるだけです。

注：Linux または UNIX スケーラビリティ サーバでは、MIF ファイルのファイル拡張子は、たとえば `my_printer.MIF` のように大文字である必要があります。そうしないと、MIF ファイルは処理されません。

- [すべての外部アセット] ノードが存在しない場合は作成され、その下に新しい外部アセット エントリが作成されます。

## 外部アセット定義の作成

外部アセット定義では、外部アセットの識別方法を定義します。定義が済むと、エンジンがアセットを認識して、そのアセットからインベントリを収集できます。

### 外部アセットを設定する方法

1. [ドメイン] - [コントロール パネル] - [設定] - [外部アセットの認識] フォルダに移動します。

既存の外部アセット定義が表示されます。

2. [新規] をクリックします。

[外部アセット クラス定義の新規作成] ダイアログ ボックスが表示されます。

注：このダイアログ ボックス内のフィールドの詳細については、F1 キーを押してください。

3. [MIF ブラウザを開く] をクリックします。

[MIF 項目の選択] ダイアログ ボックスが表示され、選択した MIF ファイル内の項目が示されます。

4. 関連する項目を [外部アセット クラス定義の新規作成] ダイアログ ボックスにドラッグし、[OK] をクリックします。

[外部アセットの認識] フォルダの下に外部アセット定義が作成されます。

5. 外部アセット情報が含まれる MIF ファイルを収集エリア（Windows では ...¥ServerDB¥SECTOR¥COLLECT または Linux では / ServerDB/SECTOR/COLLECT）にコピーします。

注：Linux または UNIX スケーラビリティ サーバでは、MIF ファイルのファイル拡張子は、たとえば my\_printer.MIF のように大文字である必要があります。そうしないと、MIF ファイルは処理されません。

エンジンにより、このファイルが収集され、処理されます。エンジンは MIF ファイル内に認識項目を見つけると、新しい外部アセットを作成して [すべての外部アセット] フォルダの下に挿入します。

## ジョブ

ジョブは、エージェントまたはエンジンに特定のアクションを実行するように指示します。ジョブを使用すると、たとえば、コマンドまたはスクリプトの実行、インベントリ情報の収集やアセット上でのメッセージのポップアップなどを行うことができます。これらのジョブを特定の時間に実行するようにスケジュールすることができます。アセット管理では、ジョブは以下の分類に分けられます。

- **アセット ジョブ**：エージェントによりアセット上で実行されるジョブ。このため、アセット ジョブは、アセットにリンクされている場合のみ実行されます。
- **エンジン タスク**：エンジンにより実行されるジョブ。このため、エンジン ジョブは、エンジンにリンクされている場合のみ実行されます。

## アセット ジョブ

アセット ジョブは、特定のコンピュータでまたはユーザがログインしたときに特定のアクションを実行するようエージェントに指示します。たとえば、アセット ジョブを使用してスクリプトまたはコマンドを実行し、メッセージを表示するよう指示できます。

ジョブは、アセット レベル、グループ レベル、およびドメイン レベルで作成できます。アセット レベルで作成したジョブは個々のアセットにリンクされ、グループ レベルで作成したジョブはグループ内のすべてのメンバアセットにリンクされます。ドメイン レベルでは、ドメイン内のすべてのジョブの表示、新しいジョブの作成、任意のグループまたはアセットへのジョブのリンクを行うことができます。特定のアセットまたはグループに対して、いくつでもジョブを作成およびリンクできます。

DSM エクスプローラのウィンドウのアドレス バーで、ドメイン名に次のパスを追加します。以下のパスで説明します。

- 「コンピュータ」は、ドメイン内のコンピュータ名を参照します。
- 「ユーザ」は、ドメイン内のユーザ名を参照します。

### アセット/ユーザ レベル

アセット - ドメイン/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/ジョブ/アセット ジョブ

ユーザ - ドメイン/コンピュータおよびユーザ/すべてのユーザ アカウント/ユーザ/ジョブ/アセット ジョブ

### グループ レベル

すべてのコンピュータ グループ - ドメイン/コンピュータおよびユーザ/すべてのコンピュータ/{グループの詳細}/ジョブ/アセット ジョブ  
すべてのユーザ グループ - ドメイン/コンピュータおよびユーザ/すべてのユーザ アカウント/{グループの詳細}/ジョブ/アセット ジョブ  
ユーザ定義グループ - ドメイン/コンピュータおよびユーザ/グループ名/{グループの詳細}/ジョブ/アセット ジョブ

### ドメイン レベル

ドメイン/ジョブ

既存のジョブは、任意のグループまたはコンピュータにリンクすることができます。したがって、ジョブが作成されるフォルダとは無関係です。

使用可能なジョブおよびそれらのスケジューリング オプションを表示するには、  
[アセット ジョブ] フォルダに移動します。

注：ジョブ タイプおよびジョブの作成や編集の詳細については、「DSM エクス  
プローラ ヘルプ」の「Asset Management」を参照してください。

関連項目：

[DSM エクスプローラの \[アセット ジョブ\] フォルダへのアクセス \(P. 281\)](#)



## DSM エクスプローラの [ アセット ジョブ ] フォルダへのアクセス

[アセット ジョブ] フォルダでは、アセット ジョブを作成、設定、リンク、およびスケジュールできます。

### DSM エクスプローラの [ アセット ジョブ ] フォルダにアクセスする方法

1. アセット ジョブを表示または設定するレベルに従って、DSM エクスプローラで以下のパスに移動します。

#### グループ レベル

##### コンピュータ グループ

ドメイン、コンピュータおよびユーザ、すべてのコンピュータ、グループ詳細

##### ユーザ アカウント グループ

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、グループ詳細

##### ユーザ作成グループ

ドメイン、コンピュータおよびユーザ、グループ、グループ詳細

#### コンピュータ レベル

ドメイン、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

#### ユーザ レベル

ドメイン、コンピュータおよびユーザ、すべてのユーザ アカウント、ユーザ アカウント

#### ドメイン レベル

ドメイン

2. 上記のパスから、[ジョブ] - [アセット ジョブ] フォルダに移動します。

グループ レベルで作成されたジョブは、グループのメンバアセットに自動的にリンクされます。ただし、アセット レベルでこれらのジョブの実行を無効にできます。ユーザにリンクしたジョブは、そのユーザのログイン時に実行されます。

**注：**これらのすべてのレベルで作成されたアセット ジョブは、任意の管理対象アセットまたはグループにリンクすることができます。

### ジョブ タイプ

新しいジョブを作成する場合、ジョブ タイプを選択する必要があります。ジョブ タイプによって、ジョブを実行するためのパラメータが異なります。以下のアセットジョブを使用できます。

- メッセージジョブ (Windows のみ)
- コマンドジョブ
- 同期処理ジョブ (Windows のみ)
- 外部ユーティリティジョブ
- セキュア構成ファイルの保護ジョブ (Windows のみ)
- スクリプトジョブ

### メッセージジョブ

メッセージジョブでは、アセット上にまたはユーザのログイン時にメッセージを表示できます。ジョブステータスを表示すると、メッセージがいつ表示されたかがわかります。

ユーザにメッセージジョブが割り当てられていて、同じユーザが複数のセッションにログオンした場合は、いずれか1つのユーザセッションにメッセージジョブを表示できます。

注：このジョブは Windows エージェントにのみ適用可能です。

関連項目：

[ジョブステータスの表示](#) (P. 290)

### コマンドジョブ

コマンドジョブを使用すると、選択したアセットまたはグループに対してコマンドファイル（たとえば、バッチファイルや UNIX シェル スクリプトなど）を実行できます。このファイル内では、通常のネイティブ コマンド言語のあらゆるコマンドを使用できます。

## 同期ジョブ

ディレクトリ同期ジョブを使用すると、アセット上の2つのディレクトリが同期されます。同期では、ターゲットディレクトリとソースディレクトリの内容が比較され、ターゲットディレクトリの内容がソースディレクトリの内容と同じになります。

**注：**このジョブは、コンピュータアセットにのみリンクでき、Windows エージェントにのみ適用されます。

新規ジョブウィザードの手順3で、以下のディレクトリを指定します。

### ソース

比較の基準となるディレクトリを指定します（イメージ）。

### ターゲット

違いを調べるディレクトリを指定します（イメージの反射）

**注：**UNCパスの使用がサポートされています。構文は、`\\servername\sharename`です。

新規ジョブウィザードの手順4で、以下のことを指定します。

- サブディレクトリについても違いを調べるかどうか。
- ソースに存在しないターゲット上のファイルを削除するかどうか。
- ターゲットファイルの属性がソースファイルの属性と同じにならないように、比較時に属性を無視するかどうか。
- コピー時に属性を無視するかどうか。無視した場合、ジョブは書き込み保護されたターゲットファイルを上書きしようとします。
- 2つのディレクトリのサイズの差異が指定されたサイズ (KB) を超えた場合、ジョブをキャンセルするかどうか。このパラメータは、ネットワーク上の大きなサイズが誤ってコピーされることを防ぐために提供されています。

### 例：プリンタファイルの同期

これは、ユーザのローカルハードディスクに存在するユーザのプリンタ ファイルを更新する方法の例です。更新を簡単にするには、最新のプリンタ ファイル（たとえば、`N:¥PRINTERS`）のみを更新する必要があります。次に、ディレクトリ同期を使用して、ディレクトリ `C:¥WINDOWS¥PRINTERS` と `N:¥PRINTERS` を同じ内容にします。これで、ハードディスク上に存在するプリンタ ファイルが、ネットワーク ドライブ `N` 上のプリンタ ファイルと同じ内容になります。これ以降は、ネットワーク上でコンピュータが起動されるたびに、ディレクトリの差異が調べられます。

ソース： `N:¥PRINTERS`

ターゲット： `C:¥WINDOWS¥PRINTERS`

選択するオプション： [サブディレクトリを含める]、[不明なファイルを削除する]、[比較時にファイルの属性を無視する]、[コピー時にファイルの属性を無視する]

### 例：ポータブル コンピュータ ファイルの更新

ネットワーク上にポータブル コンピュータが存在する場合、ポータブル コンピュータのハードディスク上のサブディレクトリをサーバ上の個人用ネットワーク ドライブと同期させることができます。これにより、ポータブル コンピュータがネットワークに接続されていないときに作成されたポータブル コンピュータ ファイルをネットワークに自動的に転送することができます。

ディレクトリ同期ジョブを実行すると、2つのディレクトリは完全に一致します。また、属性も等しくなります。ソース上に見つからないターゲット上のファイルは削除されます（削除するように指定されている場合）。ターゲット上に見つからないディレクトリは、作成されます。

場合によっては、ディレクトリ内のファイルおよびサブディレクトリの一部を同期処理から除外する必要があります（たとえば、**Agent Software** ディレクトリでは、**PROTOCOL.INI** ファイルおよび **HOST** ファイルをネットワーク全体で同じにすることは好ましくありません）。このような場合は、同期処理から除外するファイルおよびディレクトリを指定する必要があります。

### 例：ファイルの除外

これは、ファイルを同期処理から除外する例です。たとえば、ローカルの `C:¥PW` ディレクトリをデフォルトのネットワーク ディレクトリ `F:¥PWDEFAULT` と同期化するとします。そのディレクトリの **PROTOCOL.ini** ファイルおよびすべての **\*.TPL** ファイルには各コンピュータに固有の値が含まれているため、システム管理者は、これらのファイルを同期処理から除外する必要があることがわかっています（ディレクトリ **BAK** も除外します）。

ソース： `F:¥PWDEFAULT`

ターゲット： `C:¥PW`

選択するオプション： [サブディレクトリを含める]、 [ソースで不明なファイルをターゲットから削除]

指定する項目： 同期処理から除外するファイル： \*.TPL、PROTOCOL.INI、 (DIR) BAK

## 外部ユーティリティ ジョブ

外部ユーティリティ ジョブは、外部ユーティリティを実行します。このタイプのジョブは、アセット管理以外の管理ツール用に作成されたスクリプトを実行する場合に使用できます。

## スクリプト ジョブ

スクリプト ジョブでは、アセット上でスクリプトを実行できます。スクリプトを直接記述することも、ファイルから保存済みのスクリプトを開くこともできます。

## セキュア構成ファイルの保護ジョブ

セキュア構成ファイルの保護ジョブを使用すると、指定したシステムまたは設定ファイルは常に、このジョブで指定されている内容（セキュア ファイル）と同じになります。

エージェントは、実行されている間、設定ファイルが変更されたかどうかを確認します。設定ファイルが変更された場合、エージェントはセキュア ファイルをアセットにコピーし、変更済みのファイルを上書きします。

**注：** このジョブは Windows エージェントにのみ適用可能です。UNIX または Linux では、DSM スクリプトを作成して共有領域にファイルをコピーできます。

### ジョブ実行順序の変更

ジョブは、作成された順序で実行されます。ただし、あるジョブが他のジョブの実行に依存している場合は、この順序を変更できます。

注：この作業は、グループ レベルおよびアセット レベルでのみ実行できます。

#### ジョブの実行順序を変更する方法

1. [アセット ジョブ] フォルダに移動します。
2. 順序を変更するジョブを右クリックして順序を変更し、[順序の変更] を選択します。  
サブメニューが表示されます。
3. 以下のいずれかのメニュー項目を選択します。

##### 上に移動

ジョブを 1 レベル上に移動します。複数のジョブを越えて上に移動する場合は、目的の位置になるまでこのメニュー項目をクリックします。

##### 下に移動

ジョブを 1 レベル下に移動します。複数のジョブを越えて下に移動する場合は、目的の位置になるまでこのメニュー項目をクリックします。

##### 先頭に移動

ジョブを先頭位置に移動します。

##### 最後

ジョブを最後の位置に移動します。

##### 位置の設定

ジョブを指定した位置に移動します。たとえば、5 個のジョブを越えて上または下に移動する場合などは、このオプションを使用できます。

### ジョブの順序のクリア

ジョブの既存の順序をクリアし、アルファベット順に並べ替えます。

選択したメニュー項目に基づいて、ジョブの順序が変更されます。

## ジョブのスケジューリング

ジョブは、1回、指定した回数、または継続的に実行されるようにスケジュールすることができます。ジョブを設定するときは、たとえば、以下のようなさまざまな方法でアクションが実行されるようにスケジュールできます。

- 繰り返し実行
- 特定の日時に、または一定時間経過後に実行
- 曜日の依存関係に基づいて実行
- 別のジョブの実行、ファイルの存在、またはアクションを今すぐ実行するか後で実行するかのエンドユーザの決定に基づいて実行

デフォルトでは、ジョブは常に実行されるようにスケジュールされます。つまり、アセット上でアセット管理エージェントが起動されるたびにジョブが実行されます。言い換えると、アセットジョブの実行はエージェントの実行に依存しています。たとえば、アセット管理エージェントが1日に1回実行されるようにスケジュールされており、アセットジョブが木曜日のみに実行されるようにスケジュールされている場合、木曜日にエージェントが起動されたときにジョブが実行されます。

スケジューリング オプションは、以下のいずれかの方法で指定できます。

- ジョブの作成時、新規ジョブ ウィザードに、スケジューリング オプションを指定できる [スケジューリングの設定] ボタンがあります。
- ジョブの作成後は、ジョブを右クリックし、コンテキスト メニューから [スケジューリング] を選択できます。

どちらの場合も、以下の項目を定義できる [スケジューリング オプション] ダイアログ ボックスが表示されます。

### スケジューリング

ジョブの実行頻度を指定します。

#### 条件

ジョブのさまざまな条件を指定します。一定範囲の日時に実行されるように、または特定の曜日に実行されるようにジョブをスケジュールできます。

#### 依存関係



あるジョブの実行を別のジョブの正常な完了または別のファイルの存在に依存させることを指定します。スケーラビリティ サーバ当たりのアクションの最大同時実行数を指定することにより、同時ジョブの制限を使用して一定期間内のネットワーク負荷を分散することができます。

### ジョブ実行前

ジョブの実行前にチェックする必要がある条件を指定します。

- エンドユーザがジョブの実行のキャンセルを選択できるようなプロンプトを有効にします。
- 実行が特定の数に達した後、強制実行を有効にします。
- ネットワーク ドライブをマップします。これがジョブの実行に必要な場合があります。

### ジョブ実行後

ジョブの完了後に実行するアクションを指定します。完了後にコンピュータを再起動したり、ジョブを自動的に削除するようにスケジュールできます。

### その他

ユーザ操作なしでジョブを実行できるように指定します。

注：[スケジューリング]および[スケジューリング オプション] ダイアログボックスの詳細については、「*DSM エクスプローラ ヘルプ*」を参照してください。

## ジョブの再初期化

ジョブに変更を加えた後は、[ジョブの再初期化] メッセージボックスが表示されます。以下のいずれかを選択して、ジョブのステータスを[待機中]に再初期化できます。

### はい

ジョブに接続されているすべてのアセット上のジョブのステータスを再初期化します。

### いいえ

選択したアセットまたはグループ上のジョブのステータスを再初期化します。

## ジョブ ステータスの表示

ジョブ ステータスにより、ジョブが正常に完了したか、待機中であるか、またはエラーで完了したかがわかります。

### ジョブ ステータスを表示する方法

1. [\[アセットジョブ\]](#) (P. 281) に移動します。

右側のペインに、選択されたアセットまたはグループにリンクするアセットジョブがすべて表示されます。

2. ジョブを右クリックし、**[ステータス]** を選択します。

**[アクション ステータス]** ダイアログ ボックスが表示され、ステータス テキスト、ジョブが最後に実行された日時など、ステータスに関する詳細が表示されます。

## ジョブの有効化または無効化

アセットまたはグループに対して実行しないジョブを一時的に無効化することができます。グループ レベルで無効化されたジョブは、グループ レベルでのみ有効化できます。同様に、アセット レベルで無効化されたジョブは、アセット レベルでのみ有効化できます。

### ジョブを有効化または無効化する方法

1. [\[アセットジョブ\]](#) (P. 281) に移動します。

右側のペインに、選択されたアセットまたはグループにリンクするアセットジョブがすべて表示されます。

2. ジョブを右クリックし、**[無効]** または **[有効]** を選択します。

ジョブが無効化または有効化され、それに応じてステータスが変更されます。

## クエリ

クエリは、データベースを使用する場合の大きなメリットです。データベースをクエリすると、指定した基準に合致するアセットを検索できます。動的グループを作成するためにクエリを使用できます。動的グループのメンバは、クエリの結果に従って変わります。クエリに基づいてポリシーを作成し、結果オブジェクトにそのポリシーを適用することもできます。**Asset Management** では、データベースに対して基本的なクエリまたは詳細なクエリを実行する事前定義クエリが提供されています。[クエリ デザイナ] ツールを使用すると、複雑なクエリを簡単に作成できます。

## 新規クエリの作成

基準に合致するアセットのリストを取得する必要がある場合、クエリを作成できます。これらのクエリを使用して、動的グループおよびクエリ ベースのポリシーを作成できます。

### 新しいクエリを作成する方法

1. **DSM** エクスプローラで [クエリ] を右クリックし、コンテキスト メニューから [新規] を選択します。  
[ターゲットを選択] ダイアログ ボックスが表示されます。
2. クエリを作成するオブジェクトを選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが表示されます。
3. 新しいクエリの作成に必要な引数を挿入し、[OK] をクリックします。  
指定した名前でクエリが作成され、[クエリ] フォルダ内の適切なフォルダの下に表示されます。
4. [クエリ] を右クリックし、コンテキスト メニューから [新規] を選択します。  
[ターゲットを選択] ダイアログ ボックスが表示されます。
5. [コンピュータ] を選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが表示されます。
6. [ジョブ] - [アセット ジョブ] をクリックします。  
[フィールドを選択] ダイアログ ボックスが開きます。
7. [ジョブ ステータス] - [現在のステータス] を選択します。
8. [ジョブ] フィールドで [CA eTrust ウイルス スキャナ - シグネチャの更新を強制実行] を選択し、[ステータス] フィールドで [OK] をクリックします。
9. [OK] をクリックし、クエリに一意の名前を入力します。  
新しいクエリが [クエリ] - [コンピュータ] フォルダの下に作成されます。
10. クエリを選択し、[クイック プレビュー] をクリックします。  
[CA eTrust ウイルス スキャナ - シグネチャの更新を強制実行] ジョブが正常に完了したすべてのアセットが表示されます。

## クエリ デザイナ

クエリ デザイナを使用すると、簡単にデータベースをクエリできます。このツールを使用するときに、データベース フィールドについての知識は必要はありません。

クエリ デザイナ ツールを使用すると、クエリを作成または変更できます。このツールを使用して、コンピュータおよびユーザ、ジョブ、ポリシー、ソフトウェア、インベントリ、および外部ディレクトリに関する情報をクエリできます。また、データベース フィールドをクエリしたり、詳細クエリを作成することもできます。[クエリ デザイナ] ダイアログ ボックスの左側のペインには、すべての使用可能な引数が含まれた[引数の挿入]、[ブール演算子]、[引数の削除]、プレビュー機能、および SQL 文を表示するオプションが一覧表示されます。

**注：**現在、ユーザは **Asset Collector** への登録が可能であり関連する信頼レベルと発行元を持っていますが、クエリ デザイナではその条件の信頼レベルと発行元でユーザ クエリを作成できません。

新しいクエリに引数を追加すると、[クエリ デザイナ] ダイアログ ボックスの右側のペインにその引数が表示されます。

### 引数の挿入

#### 一般情報

検出されたハードウェアおよびソフトウェアのプロパティを一覧表示します。

#### インベントリ

検出されたインベントリを一覧表示します。

#### ソフトウェア

ソフトウェア パッケージ、検出されたソフトウェア使用状況、およびファイルの内容をクエリします。

#### ジョブ

アセット ジョブおよび収集タスクをクエリします。

#### ポリシー

クエリ ベースおよびイベント ベースのポリシーをクエリします。

### ディレクトリ クエリ

メンバをクエリするための組織アセットを参照したり、直属の部下をクエリするためのユーザを選択します。

注: ディレクトリ クエリを作成するには、[コントロール パネル]-[ディレクトリの統合] - [設定済みディレクトリ] フォルダの下にディレクトリ オブジェクトが使用可能になっている必要があります。

### 詳細な引数

限定的なクエリを実行するために、データベース内のアセット管理テーブルをクエリします。[詳細な引数の追加] ダイアログ ソックスで引数を選択します。

### クエリのリンク

[クエリの選択] ダイアログ ソックスを開くと、既存クエリのリンクおよび引数としてクエリの追加ができます。

### ブール演算子

以下の演算子を指定します。クエリ デザイナによって、この演算子を使用して一部の条件の有効性がテストされ、TRUE または FALSE のブール値が返されます。

#### および

2 つのブール式を結合し、両方の式が TRUE の場合は TRUE を返します。

#### OR

2 つの条件を結合し、どちらか一方の式が TRUE の場合は TRUE を返します。1 つの式で複数の論理演算子を使用した場合、OR 演算子が AND 演算子の後に評価されます。

#### NOT

ブール式の値を逆にします。

#### ()

評価の順序を変更します。

### 引数を削除

右側のペインで選択されている引数をクエリ デザイナから削除します。

## プレビュー

クエリを実行し、[クエリ プレビュー] ダイアログ ソックスを開いてクエリ結果を表示します。

## SQL の表示

[SQL ビュー] ダイアログ ボックスに SQL クエリ文を表示します。このダイアログ ボックスに表示された SQL 文は変更できません。

## クエリの実行

クエリを設計した後は、クエリを実行して結果を表示できます。

### クエリを実行する方法

1. 実行するクエリを選択します。
2. [タスク] セクションで [クエリの実行] をクリックします。

クエリが実行され、[クエリ プレビュー] ダイアログ ボックスに結果が表示されます。

**注：** クエリの実行は 5 分ごとにタイムアウトし、クエリの実行を継続するか、またはキャンセルするかを選択するメッセージが表示されます。実行中はいつでも、Esc キーを押すと実行をキャンセルできます。

**注：** エンジンに発行されたクエリは、自動的に実行されます。

### クエリ プレビュー

「クエリ デザイナ」ダイアログ ボックスでクエリを設計中であっても、クエリの結果をプレビューできます。これは、クエリによって期待する出力が得られるかどうかを確認するのに役立ちます。また、「SQL の表示」アイコンをクリックすると、クエリの SQL バージョンが表示されます。

「クエリ デザイナ」ダイアログ ボックスでクエリの結果をプレビューするには、「クエリ デザイナ」ダイアログ ボックスで新しいクエリを作成し、左側のペインで「プレビュー」をクリックします。「クエリ プレビュー」ダイアログ ボックスが表示され、クエリの結果が示されます。

**注：**クエリの実行は 5 分ごとにタイムアウトし、クエリの実行を継続するか、またはキャンセルするかを選択するメッセージが表示されます。実行中はいつでも、Esc キーを押すと実行をキャンセルできます。

動的グループまたはポリシーに適用されたクエリの結果を表示する場合や、ドメインをクエリして最新の情報を確認する場合、以下のことが前提条件となります。

- エンジンにクエリをサブミットします。
- エンジンがクエリの処理を完了していることを確認します。

**重要：**クエリ デザイナを使用すると、柔軟かつ確実に操作を行うことができます。クエリに間違いがあると、エンジンがクラッシュします。クエリを動的グループまたはポリシーに適用する前には必ず、「プレビュー」オプションを使用してクエリをテストしてください。

### クエリ結果の保存

将来参照できるように、クエリの結果の記録を保存することができます。

#### クエリの結果を保存する方法

1. クエリを右クリックして、「クエリの実行」を選択します。  
「クエリ プレビュー」ダイアログ ボックスが表示され、結果が示されます。
2. 「保存」をクリックし、クエリ結果の名前を指定します。  
指定した名前でクエリ結果が保存され、選択したクエリの下に表示されます。



## クエリの削除

使用しなくなったクエリを削除できます。

### 既存のクエリを削除する方法

1. クエリを右クリックし、コンテキストメニューから [削除] を選択します。  
確認ダイアログボックスが開きます。
2. [はい] をクリックします。  
削除が確認され、データベースからクエリが削除されます。

## クエリ定義のインポートまたはエクスポート

保存済みのクエリをインポートし、DSM エクスプローラで実行できます。`.cmsobj` ファイルにクエリを保存する必要があります。クエリ定義をインポートするには、[クエリ] フォルダに移動し、フォルダを右クリックして [インポート定義] を選択します。

DSM エクスプローラで作成したクエリを `.cmsobj` ファイルにエクスポートするには、[クエリ] フォルダに移動し、エクスポートするクエリを右クリックして [定義のエクスポート] を選択します。

注：`.qry` 形式でのクエリのエクスポートは、Client Automation r12.5 以降では有効なオプションではありません。ただし、古い `.qry` 形式でのクエリ定義のインポートはサポートされます。`.qry` から `.cmsobj` 形式への変換する方法の 1 つとして、古い形式でインポートしてから、それらを `.cmsobj` 形式でエクスポートする方法があります。変換するクエリ定義の数が多い場合は、バッチ スクリプトが役立ちます。

## ポリシー

ポリシーを使用すると、管理者は、特定のしきい値を超えた場合やイベントが発生した場合のクリティカルデータに重点を置くことができます。ポリシーを使用して、アラームまたは警告を設定したり、ポリシーの違反が発生した場合に実行する処理を指定することができます。たとえば、ドメイン内に重複するネットワークアドレスが見つかったときにアラームを発生させるようなポリシーを作成できます。

Asset Management のポリシー システムは、ユーザ定義のクエリおよび定義済みのイベントに基づいています。

### クエリ ベースのポリシー

ポリシーを起動するために満たす必要のある基準を指定するクエリに基づいたポリシーが含まれます。このクエリではエージェントにより送信されたデルタ値のみがチェックされるため、データベースを継続的にクエリする必要はありません。クエリ ベースのポリシーは、[ポリシー] - [クエリ ベース] フォルダの下で使用できます。

### イベント ベースのポリシー

特定のイベントがトリガされたときに起動されるポリシーが含まれます。アセット管理では、定義済みのイベント ベースのポリシー分類のセットが用意されています。これらの分類のポリシーを作成または削除することはできません。ただし、これらのポリシーを変更することはできます（たとえば、アクションを追加するなど）。イベント ベースのポリシーは、[ポリシー] - [イベント ベース] フォルダの下で使用できます。

## ポリシー定義

[ポリシー デザイナ] ダイアログ ボックスでポリシーを定義できます。ポリシーを定義するときは、以下の要因について考慮してください。

- リンクするクエリ
- 実行するアクション
- ポリシーを起動するイベント
- ポリシーのヘッダおよび説明

## クエリ ベースのポリシーの作成

クエリ ベースのポリシーは、関連するクエリが実行されるたびに評価されます。

### クエリ ベースのポリシーを作成する方法

1. [ポリシー] フォルダに移動します。
2. [タスク] セクションで [新規] をクリックします。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
3. 以下のセクションで必要な詳細を指定します。

#### 一般

名前、重要度、依存クエリなど、ポリシーに関する一般情報を指定します。

#### 評価

ポリシーを評価するためのオプションを指定します。収集タスクの処理が完了した時点でポリシーを評価することも、エンジンを指定して特定の間隔でポリシーを評価することもできます。

#### Service Desk

CA Service Desk Manager の統合を有効にします。ポリシー違反が発生した場合は随時、問題のタイプを選択し、サービス チケットの発行を選択できます。

注：このセクションは Service Desk の統合を True に設定している場合にのみ有効化されます。デフォルトでは、False に設定されています。

#### アクションの追加

ポリシーによってトリガされるアクション タイプを指定します。

注：[ポリシー デザイナ] ダイアログ ボックスに関する詳細については、「[DSM エクスプローラ ヘルプ](#)」を参照してください。

関連項目：

[Service Desk への統合の設定](#) (P. 313)

## イベント ベースのポリシーの作成

以下の分類で新しいイベント ベースのポリシーを定義できます。

- アセット ファイルの収集
- アセット インベントリ
- アセット ソフトウェア
- アセット ソフトウェアの使用状況

注: これらのカテゴリの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」にある「イベント ベースのポリシー」を参照してください。

### イベント ベースのポリシーを作成する方法

1. [ポリシー] - [イベント ベース] フォルダに移動します。
2. 上記の一覧で指定されたフォルダのいずれかを右クリックし、[新規] を選択します。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
3. 以下のセクションで詳細を指定します。

#### 一般

名前の指定、重要度の割り当て、ポリシーの履歴トラッキングの有効化を行います。

#### Service Desk

CA Service Desk Manager の統合を有効にします。ポリシー違反が発生した場合は随時、問題のタイプを選択し、サービス チケットの発行を選択できます。

注: このセクションは Service Desk の統合を True に設定している場合にのみ有効化されます。デフォルトでは、False に設定されています。

#### アクションの追加

ポリシーによってトリガされるアクション タイプを指定します。

選択されたイベント分類に基づいて、このダイアログ ボックスには以下のセクションが表示されます。

#### アセット ファイルの収集: ファイル収集

監視するファイルを指定します。この分類のポリシーは、選択したファイルが変更されるとトリガされます。

### アセット インベントリ： インベントリ項目

ポリシーにより監視するインベントリ項目を指定します。この分類のポリシーは、選択したインベントリ項目の値が変更されるとトリガされます。

### アセット ソフトウェア： アプリケーション

ポリシーにより監視するソフトウェア アプリケーションおよびトラッキングするイベントを指定します。このタイプのポリシーは、選択したアプリケーションで選択したイベントが発生するとトリガされます。

### アセット ソフトウェアの使用状況： アプリケーション

ソフトウェア使用状況を監視するアプリケーションを指定します。実行できなかった、正常に開始された、異常終了したなど、トラッキングするさまざまな使用方法イベントを選択できます。このタイプのポリシーは、選択したアプリケーションで選択した使用方法イベントが発生するとトリガされます。

指定した仕様のポリシーが作成されます。

注： [ポリシー デザイナ] ダイアログ ボックスに関する詳細については、「DSM エクスプローラ ヘルプ」を参照してください。

関連項目：

[イベント ポリシーの定義 \(P. 188\)](#)

## ポリシーへのアクションの追加

ポリシー アクションでは、ポリシー違反が発生した場合に使用されるアクションが定義されます。たとえば、記憶域で特定のしきい値に達したときに、ユーザーに対してメッセージを送信します。また、アセットのポリシー違反がなくなった時点でポリシー アクションを実行できます。

注： ポリシー アクションの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

## 通知

DSM エクスプローラにアラームを表示します。メッセージテキストは、イベント ログのメッセージテキスト同様に作成できます。

## メッセージ

エージェント上に表示メッセージを作成します。メッセージテキストは、イベント ログのメッセージテキスト同様に作成できます。

## ジョブのスケジュール

指定されたジョブが違反の発生したアセット上で実行されるようにスケジュールします。ジョブは、次にエージェントが実行されたときに実行されます。

## アプリケーションの起動

アセットがポリシーをトリガすると、選択されたアプリケーションをエンジン上で実行します。

## グループに追加

指定されたドメイン グループにアセットを追加します。

## テキスト ファイルの生成

ポリシーの発生時にエンジンにより生成されたメッセージ テキストを含むテキスト ファイルにテキストを追加します。メッセージ テキストは、イベント ログのメッセージ テキスト同様に作成できます。

## メールの送信

指定された受信者に MAPI 電子メールを送信します。メッセージ テキストは、イベント ログのメッセージ テキスト同様に作成できます。

注：電子メール ポリシーが機能するためには、メール クライアントが実行されている必要があります。

## アセットの削除

システムからアセットを削除します。

## システム イベント ログ

システム イベント ログにポリシー通知を記録します。ポリシー通知に表示されるメッセージテキストを構成できます。たとえば、`$NAME$::$TYPE$` を指定した場合、データベース内で見つかった特定のアセット名およびアセットタイプがメッセージテキストで表示されます。このテキストは、ポリシーが発生したときにエンジンによってトリガされる通知のテキスト ファイルに含まれます。

## Unicenter イベント ログ

Unicenter イベント コンソールにポリシー通知を記録します。イベント コンソールには、DSM エクスプローラの [ツール] - [Unicenter] - [イベント コンソール] メニューからアクセスすることができます。

注：エンジンによってインストール先のコンピュータにログ エントリが生成されます。

## AMT コマンド

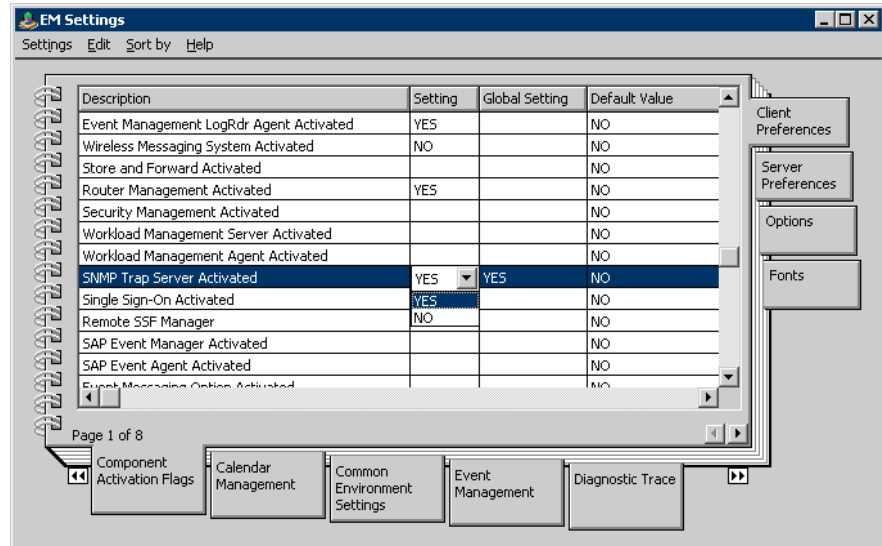
Intel AMT リモート コマンドを Intel AMT アセット上で、ポリシーに違反したとき実行します。これらのコマンドを使用して、Intel AMT アセットを制御できます。

## SNMP トラップ

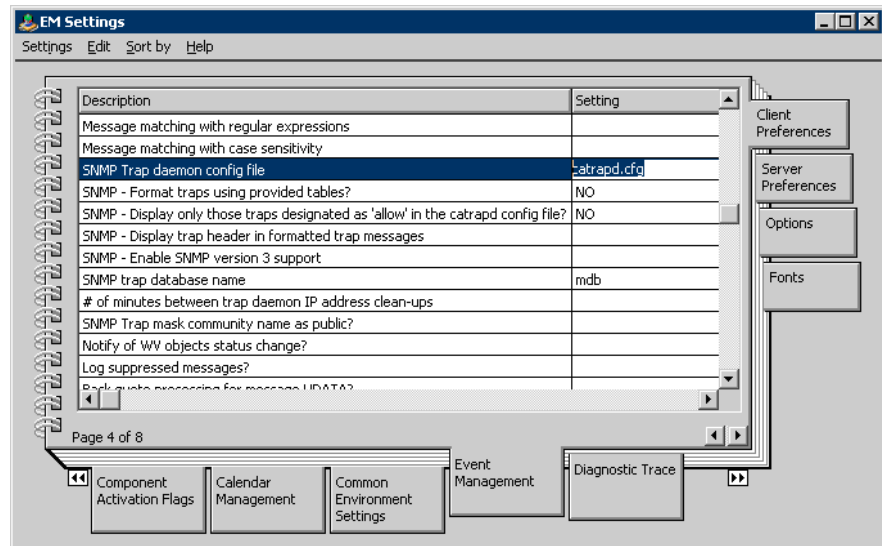
SNMP トラップをトリガします。メッセージテキストは、イベント ログのメッセージテキスト同様に作成できます。SNMP トラップを Unicenter エンタープライズ管理と組み合わせて使用すると、CA 製品間の統合が可能になります。

注：SNMP 機能をアセットでインストールしておく必要があります。このアセットは、通常は Windows コンポーネントです。さらに、CCS イベント管理（または Unicenter NSM）の以下の設定を有効にする必要があります。

- 以下の図で示すように、Unicenter エンタープライズ管理で [SNMP トラップ アクティブ] を有効にしていることを確認してください。この処理を正常に動作させるには、コンピュータを再起動します。



- 以下の図で示すように、設定ファイルを使用している場合は、かならず イベント マネージャを有効にして指定したファイルを使用してください。



- 設定ファイルで、かならず CAITCM SNMPTRAP.EXE ユーティリティが使用する OID を有効にしてください。

#### # CAITCM SNMP traps

\*:\*:\*:\*:1.3.6.1.4.1.791.\*

allow

# Enable AM

Policy traps



## ポリシー評価

ポリシー評価により、ポリシーがトリガされる条件および方法が決まります。

以下の場合、クエリ ベースのポリシーが評価されます。

- 手動 - ポリシーを右クリックして [今すぐ評価] を選択できます。
- 自動 - [ポリシー デザイナ] ダイアログ ボックスの [評価] セクションで評価オプションを指定できます。収集タスクの処理が完了した時点でポリシーを評価することも、エンジンを指定して特定の間隔でポリシーを評価することもできます。

イベント ベースのポリシーは、指定したイベントが発生するたびに評価されます。

注： [ポリシー デザイナ] ダイアログ ボックスの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

## 事前定義ポリシー

アセット管理には、以下のような定義済みのクエリ ベースのポリシーが用意されています。デフォルトでは、これらのポリシーにアクションは関連付けられていません。アセットがポリシーに違反したとき、またはポリシーの違反がなくなったときに実行するアクションを定義できます。

### 定義が封印解除される仮想アプリケーション イメージがあるアセット

定義が封印解除される仮想アプリケーション イメージが検出されたコンピュータを評価します。

### リソース不足のアセット ( パフォーマンス使用率 75% )

日中のシステム パフォーマンスが 75% を超えるコンピュータを評価します。

### AM ジョブのステータスが「エラー」のユーザ

ユーザ ログイン時に [エラー] ステータスでアセット ジョブが失敗するたびに評価されます。

### AM ジョブ ステータスが「エラー」のアセット

コンピュータ上でアセット ジョブが [エラー] ステータスで失敗するたびに評価されます。

### 減少しているメモリ

アセットのメモリが以前のスキャン値から減少するたびに評価されます。

イベント ベースのポリシー用の定義済みポリシーは、以下の分類から使用可能です。 クエリ ベースのポリシーと同様に、これらのイベント ベースのポリシーにもアクションを定義できます。

注：これらの分類のポリシーを作成または削除することはできません。

### アセット ジョブのリンク

アセットがジョブにリンクするたび、またはアセットとジョブのリンクが解除されるたびに評価されます。

### アセット ジョブ

アセット ジョブが作成、変更、または削除されるたびに評価します。

### アセット

アセットの作成や変更、ファイル ID、セクタ、アセット DNA の変更、または関係の登録が行われるたびに評価されます。

### 収集タスク

収集タスクが作成、変更、または削除されるたびに評価します。

### ファイル収集定義

ファイル収集が作成、変更、または削除されるたびに評価します。

### インベントリ検出モジュール

インベントリ検出モジュールが作成、変更、または削除されるたびに評価されます。

### インベントリ テンプレート モジュール

インベントリ テンプレート モジュールが作成、変更、または削除されるたびに評価します。

### ポリシー

ポリシーが作成、変更、または削除されるたびに評価します。

### クエリ

クエリが作成、変更、または削除されるたびに評価します。

### クエリ結果

クエリ結果が作成または削除されるたびに評価します。

### ソフトウェア定義

ソフトウェア定義が作成、変更、または削除されるたびに評価します。

## ポリシーの重要度

ポリシーのタイプは、ポリシーの重要度を示します。ポリシーの重大度または重要度に基づいて、[ポリシー デザイナ] ダイアログ ボックスの [一般] セクションで重要度を割り当てることができます。コンピュータがポリシーに違反している場合、DSM エクスプローラでコンピュータの左側のアイコンが、ポリシーの重要度に応じて変更されます。

### アラーム

クリティカルな状況を示し、ただちにアクションが必要です。コンピュータがこの重要度でポリシーに違反している場合、コンピュータのアイコンが赤色に変わります。

### 警告：

潜在的な問題を示します。このタイプのポリシーは、詳細通知の場合も同じです。コンピュータがこの重要度でポリシーに違反している場合、コンピュータのアイコンが黄色に変わります。

### メッセージ

情報目的のみであることを示します。これはデフォルトタイプです。コンピュータがこの重要度でポリシーに違反している場合、コンピュータのアイコンが青色に変わります。

## イベント ログ

イベント ログにより、ポリシー通知が記録されます。組み込み変数を使用して、ポリシー通知に表示されるメッセージテキストを構成できます。

たとえば、`$NAME$` と `$TYPE$` を指定すると、ポリシーおよびポリシー タイプに違反しているアセットの名前が表示されます。

このテキストは、ポリシーが発生したときにエンジンによってトリガされる通知のテキスト ファイルに含まれます。

**注：**通知アクションの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

## 例：重複するネットワーク アドレスの処理

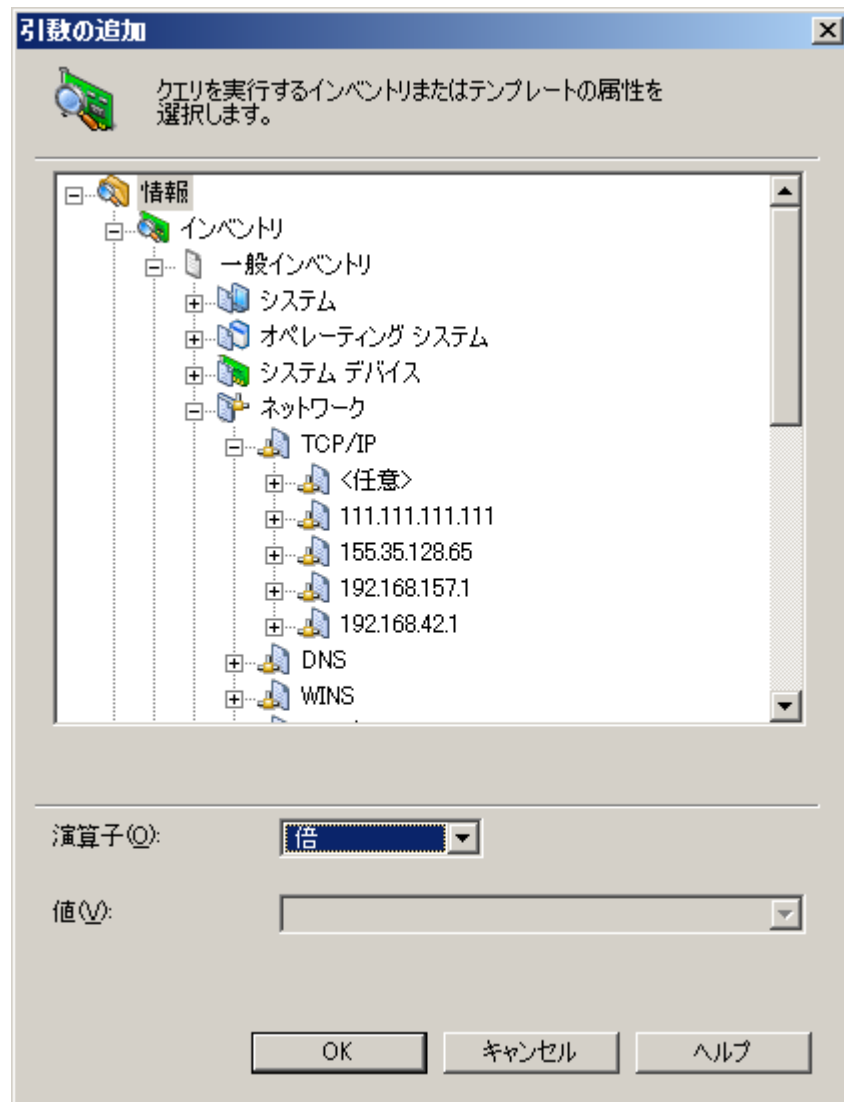
重複するネットワーク アドレスによって発生するポリシーは、2つの段階で作成します。

- 一意でないネットワーク アドレスを捕捉するクエリの設定
- そのクエリに基づいて機能するポリシーの設定

### クエリを設定する方法

1. [クエリ] に移動します。
2. [クエリ] フォルダを右クリックし、[新規] を選択します。  
[ターゲットを選択] ダイアログ ボックスが表示されます。

3. [コンピュータ] を選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが表示されます。
4. [インベントリ] - [検出されたインベントリ] を選択します。  
[引数の追加] ダイアログ ボックスが表示されます。
5. 下図のようにツリー ビュー内を移動し、[OK] をクリックします。



6. [クエリ] に名前を入力し、[OK] をクリックします。  
上記のクエリに基づいてポリシーを作成する必要があります。

### ポリシーを設定する方法

1. ポリシーに移動します。
2. [クエリ ベースのポリシー] フォルダを右クリックし、[新規] を選択します。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
3. クエリのリストから、上記のクエリを選択します。
4. 必要なアクションをポリシーに追加し、[OK] をクリックします。

このポリシーは、ユーザがネットワーク内で重複する IP アドレスを指定しようとするたびにトリガされ、指定したアクションが実行されます。

## 例：エージェント コンピュータへのアプリケーションのインストールおよびアンインストールの追跡

アセット管理エージェント コンピュータでアプリケーションがインストールまたはアンインストールされると、何らかのアクションをトリガするイベントベースのポリシーを作成できます。

**注：** インストールとアンインストールのいずれも追跡する場合は、2 種類のポリシーを作成する必要があります。

**注：** ソフトウェア ジョブを使用してソフトウェアがインストールまたはアンインストールされたときで、しかも **Client Automation** にそのソフトウェアに関連するソフトウェア定義があった場合にのみ、アセット ソフトウェア ポリシーがトリガされます。

### アプリケーションのインストールまたはアンインストールを追跡する方法

1. [ポリシー] - [イベント ベース] - [アセット ソフトウェア] フォルダに移動します。
2. [タスク] セクションで [新規] をクリックします。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
3. [アプリケーション] をクリックします。  
[ソフトウェア] ペインが表示されます。
4. アクションを実行する必要があるイベント（インストールまたはアンインストール）を選択します。
5. 以下のいずれかのオプションを選択します。

### すべてのアプリケーションのトラッキング

すべてのアプリケーションのインストールまたはアンインストールを追跡します。

### 特定のアプリケーションのトラッキング

特定のアプリケーションのインストールまたはアンインストールを追跡します。 ドロップダウン リストから追跡するアプリケーションを選択できます。

6. ポリシーがトリガされたときに実行するアクションを追加します。
7. [OK] をクリックします。  
ポリシーが保存されます。

## CA Service Desk Manager を使用した統合

アセット管理を CA Service Desk Manager と統合すると、ポリシー違反の発生時に自動的に Service Desk チケットが発生します。また、管理対象コンピュータ アセットに関連して、一時的な Service Desk チケットを作成することもできます。DSM 管理者は、ソフトウェア ポリシーに関連付けられたチケットをただちに表示できるよう CA Service Desk Manager Web ブラウザを起動できます。同様に、Service Desk アナリストは、ポリシー違反を見つけるために DSM エクスプローラおよび Web コンソールを起動することができます。

統合を有効にするための前提条件として、一般設定ポリシー内で Service Desk 統合を有効にしておく必要があります。

以下の機能が実装されます。

### 問題タイプ

アセット管理では、問題タイプが CA Service Desk Manager データベースから取り込まれて [ポリシー デザイナ] ダイアログボックスの [Service Desk] セクションに表示されます。ポリシーを作成するときは、これらの問題タイプから選択できます。CA Service Desk Manager でチケットを作成するとき、アセット管理によってこの問題タイプが割り当てられます。

### 重複チケット処理

CA Service Desk Manager には重複チケット処理ポリシーがあり、これにより、ポリシー違反が発生するたびに新しい案件を開くか、または単に同じ問題のアクティビティ ログに追加するかが決定されます。また、この両方を組み合わせて、たとえば新規案件を毎日開くように設定することもできます。

### チケットのクローズ

アセット管理では、サービス デスク チケットの自動クローズをサポートしていません。Service Desk の GUI からチケットをクローズする必要があります。

注： CA Service Desk Manager 統合の詳細については、「実装ガイド」を参照してください。



## Service Desk への統合の設定

アセットによるポリシー違反が発生した場合、自動的にサービス チケットを発行するために、アセット管理を **CA Service Desk Manager** に統合します。この統合を **Service Desk** に設定するには、以下の手順に従います。

1. [ドメイン] - [コントロール パネル] - [設定] - [設定ポリシー] - [デフォルト設定ポリシー] - [DSM] - [Service Desk インテグレーション] - [デフォルト] へ移動します。

**Service Desk** 統合に関連するポリシー設定が、右側のペインに表示されます。

2. 以下のポリシー設定をダブルクリックして、値を変更します。

注：ポリシーを右クリックし、[封印解除] を選択して [デフォルト設定ポリシー] を封印解除した場合にのみ、これらの設定を変更することができます。

### 有効

**CA Service Desk Manager** 統合が可能であるかどうかを示します。

デフォルト： いいえ (False)

### 識別子フィールド

指定されたアセットまたはソフトウェア配信によって作成される、すべてのチケットに対するクエリ用に、**MDB** にフィールドを定義します。

注：デフォルトの代わりに、string# フィールドの 1 つを予約できます (**CA Service Desk Manager** がユーザ専用 to 提供します)。

デフォルト： summary

### ログオン パスワード

**CA Service Desk Manager Web** サービスのログオン パスワードを指定します。

### ログオン サービス アウェア ポリシー

[Service Desk へのログオンのタイプ] が [管理対象外] に設定されている場合にログインするポリシーの名前を指定します。空白の場合、デフォルトの **Service Desk** ポリシーが使用されます。

注：PKCS#12 証明書には、この値を常に上書きするポリシー記述が含まれます。

デフォルト： MANAGED\_ASSET\_EVENTS

## ログオン ユーザ名

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。

デフォルト : System\_MA\_User

## Service Desk エンドポイント

CA Service Desk Manager Web サービスの URL を指定します。  
*myhost* を実際のインストール環境に合わせて、適切なサーバアドレスに置き換えます。ポート 8080 がデフォルトポートであることに注意してください。

デフォルト : `http//myhost:8080/axis/services/USD_R11_WebService`

## スロットリング

CPU のスロットリングが有効かどうかを示します。

デフォルト : いいえ (False)

## タイムアウト

CA Service Desk Manager Web サービス呼び出しのタイムアウト間隔を指定します。有効な値は、0 = 無限、正の整数 = 秒、および負の整数 = ミリ秒です。

例 : 値 200 の場合、200 秒後に呼び出しがタイムアウトになり、値 -200 の場合、200 ミリ秒後に呼び出しがタイムアウトになります。

デフォルト : 120

## Service Desk へのログオンのタイプ

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。有効な値は、[管理対象] (PKCS#12 証明書による) および [管理対象外] (ユーザ アカウントおよびパスワードによる) です。

デフォルト : managed

Service Desk への統合は、上記のフィールドで指定した設定のとおり設定されます。

注 : 統合を有効にするには、DSM エクスプローラ GUI を再起動する必要があります。

**重要：**このセクションは、管理者のみを対象としています。無効な情報を入力すると、製品が正常に動作しないことがあります。このため、ポリシーを新規作成し、それを変更することをお勧めします。

## ポリシーに関する Service Desk 統合の設定

アセット管理では、管理対象アセットがポリシーに違反した場合に自動的に CA Service Desk Manager チケットを発生させることができます。ポリシー違反が発生した場合、CA Service Desk Manager により以下のいずれかの処理を行うことができます。

- ポリシー違反に対する新しいチケットを作成します。
- 同じポリシー違反に対してすでにチケットが作成されている場合は、アクティビティ ログに追加します。

**注：**CA Service Desk Manager では、重複チケット処理ポリシーに基づいて決定が行われます。ポリシーの違反が発生するたびに新しいチケットを作成する場合は、CA Service Desk Manager 管理者に連絡してください。

### ポリシーに関して Service Desk 統合を設定する方法

1. ポリシーを右クリックし、[プロパティ] を選択します。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
2. 左側のペインで [Service Desk] をクリックします。  
[Service Desk] セクションが表示されます。

**注：**[Service Desk のチケットの作成] オプションは、[CA Service Desk の統合] を有効にした場合にのみ使用可能になります。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」で Service Desk 統合ポリシー グループを参照してください。

3. [Service Desk の統合を有効にする] チェック ボックスをオンにし、CA Service Desk Manager でポリシー違反に対して割り当てる問題タイプを選択します。Service Desk 案件に説明として含めるコメントを指定し、[OK] をクリックします。

ポリシーが保存されます。管理対象アセットがポリシーに違反したり、アクティビティ ログに追加されると、このポリシーによってチケットが作成されます。

## Service Desk チケットの作成

DSM エクスプローラで、コンピュータ アセットのコンテキスト内で Service Desk チケットを手動で作成できます。たとえば、ポリシーに違反しているコンピュータ、または失敗したジョブが存在するコンピュータに対して Service Desk チケットを作成できます。

### Service Desk チケットを作成する方法

1. コンピュータ アセットを右クリックして、コンテキスト メニューから [Service Desk チケットの作成] を選択します。

CA Service Desk の [新規チケットの作成] ウィンドウが表示され、選択したアセット名が [アセット] フィールドに表示されます。

注： [Service Desk のチケットの作成] オプションは、 [CA Service Desk の統合] を有効にした場合にのみ使用可能になります。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」で Service Desk 統合ポリシー グループを参照してください。

2. CA Service Desk 内のほかの必須フィールドを指定し、 [OK] をクリックします。

Service Desk チケットが発生します。

注： CA Service Desk でのチケット作成の詳細については、*CA Service Desk 実装ガイド* を参照してください。

## 失敗したジョブに対する Service Desk チケットの作成

アセット管理は、ポリシーを介してのみ CA Service Desk Manager と統合されます。このため、失敗したジョブに対してチケットを自動的に発生させる場合は、以下のことを行う必要があります。

- 失敗したジョブを取得するクエリを作成します。
- そのクエリに基づいてポリシーを作成します。失敗したジョブに対してチケットが作成されるようにこのポリシーを設定することができます。

### 失敗したジョブを取得するクエリを作成する方法

1. [クエリ] フォルダを右クリックし、[新規] を選択します。  
[ターゲットを選択] ダイアログ ボックスが表示されます。
2. [コンピュータ] を選択し、[OK] をクリックします。  
[クエリ デザイナ] ダイアログ ボックスが表示されます。
3. [引数の挿入] セクションで、[ジョブ] - [アセット ジョブ] を選択します。  
[フィールドを選択] ダイアログ ボックスが開きます。
4. ツリーを展開し、[ジョブ ステータス] を選択します。
5. [ジョブ] フィールドでクエリするジョブを選択し、[ステータス - エラー] を選択して [OK] をクリックします。  
[フィールドを選択] ダイアログ ボックスが閉じます。

6. [クエリ デザイナ] ダイアログ ボックスで [OK] をクリックします。  
[クエリを保存] ダイアログ ボックスが表示されます。
7. クエリの名前を入力し、[OK] をクリックします。  
指定した名前でクエリが保存され、[クエリ] - [コンピュータ] フォルダの下に表示されます。

### 上記のクエリに基づいてポリシーを作成する方法

1. [ポリシー] - [クエリ ベース] フォルダを右クリックし、[新規] を選択します。  
[ポリシー デザイナ] ダイアログ ボックスが表示されます。
2. ポリシー名およびポリシー重要度を指定し、[一般] セクションのクエリ リストから上記のクエリを選択します。
3. [Service Desk] セクションをクリックし、**Service Desk 統合**を有効にします。次に問題タイプを選択し、説明またはコメントを指定して [OK] をクリックします。

ポリシーが保存されます。このポリシーによって、選択したジョブが管理対象コンピュータ上で失敗したかどうかを確認されます。ジョブが失敗した場合は、ポリシー違反に対する **Service Desk チケット**が作成されます。

## 重複チケット ポリシー

CA Service Desk Manager では、各チケットに関連付けられたポリシーに基づいた重複処理が実装されています。CA Service Desk Manager 管理者は、問題タイプに基づいて以下の動作を設定できます。

### 重複チケットを無視

同じポリシーに対して複数のチケットが作成された場合、重複するチケットを無視して破棄します。

### 新しいチケットを作成

ポリシーの違反が発生するたびに新しいチケットを作成します。

### 既存のチケットにログ コメントを追加

最初のチケットに 2 番目のチケットの説明のログ コメントを追加します。最初にポリシー違反時に、CA Service Desk Manager によってポリシー違反のチケットが作成され、以降の違反発生時には最初のチケットにログ コメントが単に追加されていきます。

### 子チケットを作成

ポリシー違反に対するチケットがすでに使用可能な場合は、子チケットを作成します。

**注：**管理対象アセットがポリシーに違反した場合、または違反がなくなった場合、そのアセットに対する Service Desk チケットが作成されます。ただし、ポリシーが再評価されたがアセットの違反状態が変更されていない場合、新しいチケットは作成されません。

## ポリシーの有効化または無効化

しばらくポリシーがトリガされないようにする場合はポリシーを無効化し、再びポリシーを適用する場合はポリシーを有効化することができます。

### ポリシーを無効化または有効化する方法

1. [ポリシー] フォルダに移動します。
2. 該当するフォルダを選択し、その下の[クエリ ベース]または[イベント ベース]を選択します。

カテゴリで使用可能な定義が表示されます。

3. 無効化または有効化するポリシーを右クリックし、[無効]または[有効]をクリックします。

選択に応じてポリシーが無効化または有効化されます。

## ポリシーの削除

ポリシーのトリガを中止する場合は、データベースからポリシーを削除できます。

### ポリシーを削除する方法

1. [ポリシー] フォルダに移動します。
2. 該当するフォルダを選択し、その下の[クエリ ベース]または[イベント ベース]を選択します。

この分類において利用可能なすべてのポリシーのリストが表示されます。

3. 削除するポリシーを右クリックし、[削除]を選択します。

確認メッセージが表示されます。

4. [OK] をクリックします。

ポリシーがデータベースから削除されます。



## Asset Collector

Asset Collector を使用すると、たとえば以下のようなソースについてもインベントリ情報を作成できます。

- 現在 CA Client Automation ではサポートされていない特殊なデバイス
- メインフレーム コンピュータ
- 現在 CA Client Automation ではサポートされていないオペレーティング システムを搭載したコンピュータ
- エージェントをインストールしていないコンピュータ
- ユーザ

Asset Collector を使用することによって、現在の DSM インフラストラクチャでは実現できなかったアセット、ユーザ、およびユーザに関連するインベントリの詳細を把握することができます。また、このインベントリの発行元と信頼性をトラッキングできるので、アセットをより綿密に制御および管理することが可能になります。

従来は、デバイスからインベントリ データを収集する方法として、対象のハードウェア上で実行されるカスタムの DSM エージェントを作成していました。そして、CA の DSM エージェントが、従来のソースからアセット情報を収集していました。Asset Collector は、適切に構成されたインベントリ ファイルから、ハードウェアおよびソフトウェアのインベントリ情報を収集するコンポーネントです。Asset Collector のシンプルかつ柔軟なアーキテクチャにより、あらゆるデバイスやユーザについてのインベントリ情報を作成することができます。これにより、コストが大幅に削減されます。

注： Client Automation リリース 12.9 では、Asset Collector が機能拡張されて、さまざまなテナントまたは組織からアセットおよびインベントリ処理を行えるようになりました。詳細については、CA support site (<http://ca.com/support>)で Asset Collector Release Notes を参照ください。

## 前提条件

Asset Collector CAF プラグインは、自動的に Windows プラットフォームのスケールビリティ サーバにインストールされます。

しかし Asset Collector プラグインは、デフォルトでは無効か、または実行されていません。

プラグインを有効にするには、以下のコマンドを実行する必要があります。

```
caf enable assetcollector
```

これにより、プラグインは caf ステータスに表示されます。

以下のコマンドで Asset Collector プラグインを開始します。

```
caf start assetcollector
```

## Asset Collector の動作の仕組み

以下は、インベントリ ファイルからインベントリ情報を収集する手順を示しています。

1. すべてのインベントリ ファイルを特定のフォルダに格納し、関連する共通設定ポリシーを使用してフォルダの場所を指定します。

共通設定ポリシーを使用して指定しない場合は、以下のフォルダが作成されます。

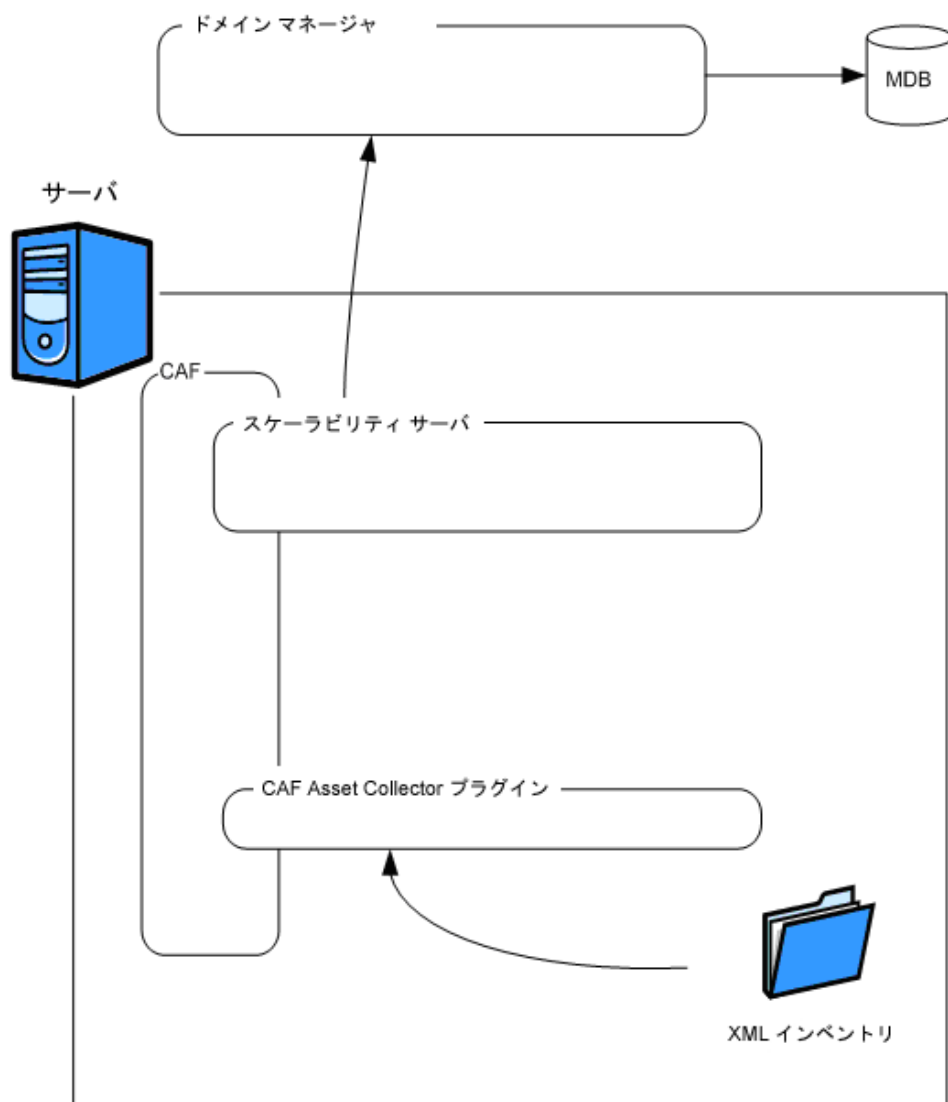
- 収集フォルダの作成場所： *DSM* インストールパス¥AssetCollectorCollect
- 出力フォルダの作成場所： *DSM* インストールパス¥AssetCollectorOutput
- 差分作業フォルダの作成場所： *DSM* インストールパス¥AssetCollectorBAK

注：これらのフォルダは、オペレーティングシステムのセキュリティ機能を利用して確実に保護しておくことをお勧めします。適切な権限のあるユーザのみがインベントリ ファイルを作成、修正、削除できるようにしてください。

2. **Asset Collector** では、共通設定ポリシーで指定したフォルダを監視して、新しいインベントリ ファイルがないかどうかを確認します。
3. 新しいインベントリ ファイルが検出されたら、ファイルが解析され、アセットやユーザのインベントリ情報が抽出されます。
4. インベントリ情報がすでに処理されている場合、**Asset Collector** は、処理済の情報と新しい情報を比較し、差分のインベントリのみをスケーラビリティサーバに送ります。それ以外の場合は、完全なインベントリが送られます。

スケーラビリティサーバでは、受け取った情報を処理して **DSM** マネージャに転送します。応報は、そこで管理データベース（**MDB**）に格納されます。

以下の図は、Asset Collector がどのような仕組みで機能するかを示しています。



## インベントリ ファイルの種類

Asset Collector では、以下の拡張子のファイルが処理されます。

.xiu = xml インベントリ ファイル (署名なし)

.xis = xml インベントリ ファイル (署名あり)

これらのファイル タイプは、XML を含む通常のテキスト ファイルです。

関連項目：

[invSign - インベントリ ファイルの署名、検証、または署名解除 \(P. 356\)](#)

## 差分操作

Asset Collector の差分操作とは、同じファイルの異なるバージョン間で、差分を検出することです。

インベントリ ファイルが提供されると（差分操作が有効になっている場合）、そのファイルの処理済みの前回のバージョンと、現在のバージョンが比較されます。差分のみがスケーラビリティ サーバに送られます。これにより、MDB で実行されるデータ変更を最適化することができます。

## 発行元と信頼レベル

発行元と信頼レベルは、**Asset Collector** で新たに導入されたフィールドです。これらのフィールドを使用して、アセットの発行元および信頼性を定義することができます。これらのフィールドは、インベントリ ファイルまたは **Asset Collector** の設定で定義します。GUI には新しい列として表示されます。

### 発行元

収集されたアセット/ユーザのソースを定義します。この情報は **DSM** エクスプローラに表示されます。ソースは、**Client Automation** エージェントまたは **Asset Collector** である場合があります。**Asset Collector** では、収集されたアセット/ユーザの発行元を、インベントリ ファイルまたは **Asset Collector** の設定ポリシーのいずれかに指定できます。通常、発行元の値として **User Keyed**、**SMS Extract**、**Legacy** があります。**Client Automation** エージェントによって収集されたアセットの発行元は **CA** になります。

### 信頼レベル

アセット/ユーザの信頼性を定義します。この情報は、**DSM** エクスプローラに表示されます。信頼レベルは、1 から 5 までの星の数で示されます。5 が最も信頼性が高いことを示しています。**Asset Collector** では、信頼レベルをインベントリ ファイルまたは **Asset Collector** の設定ポリシーで指定できます。**Asset Collector** によって収集されたインベントリ情報は、手動プロセスによって集められたものであるため、情報の信頼性は低くなります。そのため、**Asset Collector** によって収集された情報には、信頼レベルにデフォルトで 3 が設定されます。**Client Automation** エージェントによって収集された情報には 5 が設定されます。

## 発行元と信頼レベルのスキーマの変更

アセット/ユーザの発行元と信頼レベルの情報を保存するには、以下のスキーマの変更をアセット テーブルに加える必要があります。

| テーブル名                  | 列名                | 列のデータ型       | 列の<br>NULL<br>オブ<br>ション | 列のコメント                                        |
|------------------------|-------------------|--------------|-------------------------|-----------------------------------------------|
| inv_root_map           | trustlevel        | integer      | not null                | アセット/ユーザで検出されたコンポーネントの信頼レベルを定義します。<br>デフォルト：5 |
| inv_root_map           | origin            | nvarchar(64) | not null                | アセット/ユーザで検出されたコンポーネントの発行元を定義します。              |
| ca_agent               | trustlevel        | integer      | not null                | アセット/ユーザの信頼レベルを定義します。<br>デフォルト：5              |
| ca_agent               | origin            | nvarchar(64) | not null                | アセット/ユーザの発行元を定義します。                           |
| ca_discovered_hardware | external_host_key | nvarchar(64) | not null                | Asset Collector によって生成または渡されたキーを定義します。        |
| ca_discovered_software | trustlevel        | integer      |                         | アセット/ユーザの検出されたソフトウェアの信頼レベルを定義します。<br>デフォルト：5  |
| ca_discovered_software | origin            | nvarchar(64) | not null                | アセット/ユーザーの検出されたソフトウェアの発行元を定義します。              |

## 調整

Asset Collector を通じて報告されたアセットにエージェントがインストールされている場合、「調整」というプロセスが適用されます。これにより、Asset Collector からの情報は、エージェントからの情報で上書きされます。それ以降の Asset Collector からのインベントリ情報は無視されます。

Asset Collector を使用して、すでに報告済みのアセットにインベントリ情報を追加することはできません。

**注：** 調整プロセスが正しく実行されるようにするには、Asset Collector によって登録されたアセットが、コンピュータと同じ MAC（Media Access Control）アドレスとホスト名を使用している必要があります。

調整は、Asset Collector を使用して作成しているユーザ オブジェクトにも行われます。ユーザは、ユーザのキーとして URI を使用して登録されます。同じ URI のユーザが DSM エージェントを経由して登録されると、収集された情報は上書きされて、その後続くこの URI の Asset Collector インベントリは無視されます。

## ホスト キー

エージェントが MDB にアセットを登録する前に、UUID が必要になります。UUID は、通常エージェント コンピュータで作成され、将来使用するためにエージェント コンピュータに保存されます。

ただし、インベントリ ファイルはサーバで提供されるため、Asset Collector では UUID の代わりに固有のホスト キー (*host\_key*) を使用します。このキーは、インベントリ ファイル (*host\_key*) で定義されるか、指定されていない場合は、そのアセットに対して自動的に作成されます。調整プロセスを容易にするため、エージェントがアセットにインストールされている場合、収集されたアセット データには、少なくとも登録するアセットの MAC アドレスおよびホスト名が含まれている必要があります。

Asset Collector によってアセットのホスト キーが生成されると、アセットのインベントリ ファイルにもこのキーが書き込まれます。また、Asset Collector によって、ホスト名と MAC アドレスの組み合わせ、関連するホスト キーのリストが管理されます。これにより、そのインベントリ ファイルが次にホスト キーなしで提供されても同じキーを使用することができます。

ホスト キーのリストは、ストレージに書き込まれるので、次回 Asset Collector が起動したときに使用できます。指定可能な間隔で、設定ポリシーを使用して、このリストから古くなったエントリを消去することができます。データ消去までの期間を設定することもできます。



## ユーザ URI

ユーザ オブジェクトには、一意の識別子もあります。ユーザの一意の識別子は **URI** フィールドで、これはインベントリ ファイルで指定されています。つまりインベントリ ファイル内の **URI** が変更されてインベントリ ファイルが **Asset Collector** に再サブミットされると、新しいユーザ オブジェクトが作成されます。元のユーザ オブジェクトの手動での削除が必要になります。

## Asset Collector の設定

**Asset Collector** を、設定ポリシーを使用して設定できます。新しい **Asset Collector** サブノードおよびポリシー グループ フォルダが、**DSM** エクスプローラ ツリーの [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] - [スケーラビリティ サーバ] の下に追加されています。

注： **Asset Collector** 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」を参照してください。

注： **Asset Collector** の収集フォルダ、出力フォルダ、差分作業フォルダは、同じフォルダを参照しないよう設定してください。サーバの起動時に、これらのフォルダが同じフォルダを参照していると、**Asset Collector** サービスが終了し、システム イベントが発生します。

## Asset Collector の設定

ご使用の環境に合わせて **Asset Collector** をカスタマイズ、または設定することができます。

### Asset Collector を設定する方法

1. **DSM** エクスプローラから、[コントロール パネル] - [設定] - [設定ポリシー] ノードへ移動します。
2. [設定ポリシー] ノードを右クリックし、[新規ポリシー] をクリックします。  
[新規設定ポリシー] ダイアログ ボックスが表示されます。
3. [名前] および [説明] を入力してから [OK] をクリックします。  
ツリー ビューに [新規設定ポリシー] が表示されます。
4. 作成した新規設定ポリシー ノードをクリックして、展開します。
5. [DSM] - [スケーラビリティ サーバ] - [Asset Collector] をクリックします。  
すべての **Asset Collector** ポリシーが、[Asset Collector] ペインに表示されます。
6. 該当する設定（[収集フォルダ] など）をダブルクリックします。  
[プロパティの設定] ダイアログ ボックスが表示されます。
7. 設定の値を指定します。
8. 必要に応じて手順 3 と手順 4 を繰り返します。
9. [OK] をクリックします。
10. ポリシー ノードを右クリックして、メニューから [封印] を選択します。
11. [すべてのコンピュータ] フォルダの [スケーラビリティ サーバ] に、ポリシーをドラッグ アンド ドロップします。  
このポリシーを設定するスケーラビリティ サーバにポリシーが適用されます。

**Asset Collector** が、ご使用の環境に設定されます。

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。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。

関連項目：

[発行元と信頼レベル](#) (P. 326)

## 設定手順

以下は、手動で作成されたインベントリ ファイルからインベントリを生成する一般的な手順です。以下のような設定オプションがあります。

- 収集フォルダを定義する。
- 発行元および信頼レベルを指定する。
- 作業フォルダおよび出力フォルダを定義する。
- 収集フォルダのサブフォルダに含まれる、新しいインベントリ ファイルをスキャンするかどうかを指定する。
- サーバ名を指定する。
- デジタル署名付きのファイルのみを処理するかどうかを指定する。

## 一般的な環境における Asset Collector の設定

以下の手順を使用して、一般的な環境に Asset Collector を設定します。

### 一般的な環境に Asset Collector を設定する方法

1. [コントロール パネル] - [設定] - [設定ポリシー] ノードへ移動します。
2. [設定ポリシー] ノードを右クリックし、[新規ポリシー] をクリックします。  
[新規設定ポリシー] ダイアログ ボックスが表示されます。
3. [名前] および [説明] を入力してから [OK] をクリックします。  
ツリー ビューに [新規設定ポリシー] が表示されます。
4. [DSM] - [スケーラビリティ サーバ] - [Asset Collector] をクリックします。  
すべての Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
5. 手順 4 ～ 11 については、関連ポリシーをダブルクリックし、指定されているとおりに、対応する [プロパティの設定] ダイアログ ボックスでデフォルト値を変更またはそのまま適用します。次に、[OK] をクリックします。
6. 収集フォルダのポリシーの値は空白のままにします。  
デフォルトでは、[AssetCollectorCollect] 収集フォルダが、DSM インストール ディレクトリに作成されます。
7. [デフォルトの発行元] ポリシーに、デフォルト値の [XML ファイル] をそのまま適用します。

この値は、インベントリが、手動で作成されたインベントリ ファイルから生成される場合は変更されません。

**注：**ただし、インベントリ ファイルを自動で作成するタスクを使用していた場合は、この値を変更して反映することができます。例えば、社内でインベントリ ファイルを作成するツールが、ハンドヘルドデバイスに基づいたものであったとします。このツールを使用して、出力先である

[AssetCollectorCollect] 収集フォルダにインベントリ ファイルを配信する場合は、デフォルトの発行元を「Handheld Inventory Collector」に指定することができます。デフォルトの発行元および信頼レベルは、インベントリ ファイルに発行元と信頼レベルが含まれていない場合にのみ使用されます。

8. デフォルトの信頼レベル ポリシーには、デフォルト値 3 を適用します。

インベントリのソースは手動で作成されたインベントリ ファイルなので、入力されたインベントリはすぐに古くなります。信頼レベル 5 は上記の理由（日付が無効になる）により使用されません。

**注：**どの信頼レベルを使用するかは、DSM 管理者が決定します。

9. [差分作業フォルダ] のポリシーの値は空白のままにします。

デフォルトでは、[AssetCollectorBAK] 作業フォルダが、DSM インストールディレクトリに作成されます。

10. [出力フォルダ] のポリシーの値は空白のままにします。

デフォルトでは、[AssetCollectorOutput] 出力フォルダが、DSM インストールディレクトリに作成されます。

11. [再帰] ポリシーを [はい] に設定します。

[はい] に設定すると、選択した収集フォルダがスキャンされ、新しいインベントリ ファイルが格納されたサブフォルダがないかどうかチェックされます。

注： この設定は、収集フォルダにサブフォルダがない場合は無効です。

12. [サーバ名] ポリシーに、デフォルトのサーバ名「*localhost*」をそのまま使用します。

このポリシーでは、インベントリ ファイルがアップロードおよび登録されたサーバの名前を指定します。ほとんどの場合、Asset Collector はスケーラビリティ サーバにインストールされるため、インベントリはローカル マシンに配信されます。

13. [署名付きファイルのみ] ポリシーを [いいえ] に設定します。

[いいえ] に設定すると、デジタル署名の有無に関わらず、すべてのファイルが処理されます。[はい] に設定すると、Asset Collector により、有効で信頼できるデジタル署名付きのファイルのみが処理されます。

14. ポリシー ノードを右クリックして、メニューから [封印] を選択します。

注： ポリシーの封印/封印解除の詳細については、「DSM エクスプローラ ヘルプ」の「設定ポリシー」を参照してください。

15. [すべてのコンピュータ] フォルダ内にあるターゲット コンピュータに、ポリシーをドラッグアンドドロップします。

このポリシーで設定するターゲット コンピュータにポリシーが適用されます。

この手順で Asset Collector が設定されます。

## テナンシー収集

テナンシーでは、同じ MDB の内のさまざまなソースから収集されたアセット情報を管理できます。収集されたアセット情報は、同じ MDB 内でアセットのテナンシーメンバシップが保守および管理されるのと同じ方法で MDB にインポートされます。

CA ITCM は、マルチテナント対応ではありません。ただし、CA ITCM は、外部インベントリ ファイルを収集し、別のマルチテナント対応 CA 製品で使用可能なすべてのテナント情報を格納できます。

Asset Collector は、収集フォルダを使用してインベントリ ファイルを受信します。収集フォルダを設定して、テナントを個別の収集フォルダに関連付けることができます。

テナンシーは、*ca\_tenant* MDB テーブルで定義されています。収集フォルダ上でテナンシーを定義すると、エンジンは、MDB 内の *ca\_asset* テーブル上に *tenant\_id* という名前の新しい列を入力します。*ca\_tenant* テーブルからの列 *tenant\_number* は、Asset Collector の設定に使用されます。

注：CA Service Desk Manager や CA IT Asset マネージャなど、別の CA 製品は *ca\_tenant* テーブルに入力できますが、Client Automation は入力できません。したがって、CA Service Desk Manager または別のいくつかの CA 製品でテナントを定義する場合、各テナントのテナンシー番号を指定します。Asset Collector は、テナントを区別するためにこのテナンシー番号を使用します。

## テナンシー収集用のデータベースの有効化

デフォルトでは、**Client Automation** データベースは、テナンシー収集を実行するように設定されていません。**MDB** がデータベース内のテナンシー列を保守するために、いくつかのデータベース トリガを有効にする必要があります。

以下のステートメントを実行して、トリガを有効にします。

### **Oracle データベースに対して：**

```
execute sp_enableTenantTriggers(1);

commit;
```

注：Oracle 上で、**ca\_itrm** ユーザとしてではなく、**mdbadmin** としてコマンドを実行する必要があります。

### **Microsoft SQL Server データベースに対して：**

```
exec sp_enableTenantTriggers 1
```

注：MDB ネームスペース内でコマンドを実行する必要があります。

以下のコマンドを実行することにより、MDB ネームスペースにセッションを変更できます。

```
use mdb;
```

## テナンシー収集の設定

Asset Collector 設定フォルダを設定することにより、同じ MDB 内のさまざまなソースから収集されたアセット情報を管理できます。

以下のように指定することにより、Asset Collector 設定フォルダを設定できます。

- 各収集フォルダのテナンシー
- テナントの指定のない収集フォルダ
- 単一のテナントのための複数の収集フォルダ

注：複数のテナントに対して 1 つの収集フォルダを設定することはできません。

### テナンシー収集のために収集フォルダを設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。  
Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
4. [収集フォルダ] をダブルクリックします。  
[設定の変更] ダイアログ ボックスが表示されます。
5. 各行に対して、収集フォルダを定義し [OK] をクリックします。

注：テナンシー番号列はオプションです。この列に指定された値は、MDB 内の `ca_tenancy` テーブルの `ca_tenancy` 列内にあるエン트리と一致する必要があります。

6. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
7. [すべてのコンピュータ] フォルダのスケーラビリティ サーバに、ポリシーをドラッグアンドドロップします。  
ポリシーがスケーラビリティ サーバに適用されます。



## インベントリ ファイルを処理するためのルール

複数のテナントから収集されたインベントリ ファイルを処理するためのルールを指定できます。ルールは、インベントリ ファイルの 2 つの属性（信頼レベルと収集時間）の 1 つに基づくことができます。

2 つの操作モードがあります。

### Trust Enabled Mode ( TRUE )

信頼レベルに基づいてインベントリ ファイルを処理します。

以前のインベントリ ファイルの信頼レベル以上の信頼レベルを持つインベントリ ファイルは、スケーラビリティ サーバに伝達されます。

### Trust Disabled Mode ( FALSE )

収集時間に基づいてインベントリ ファイルを処理します。

以前のインベントリ ファイルの収集時間より大きい収集時間を持つインベントリ ファイルは、スケーラビリティ サーバに伝達されます。

同じ日付に得られたインベントリ レコードの再提出を防止するには、*同一日付範囲*設定を秒単位で定義して、同一日付範囲内に収集時間を持つインベントリ ファイルが処理されないようにします。

同一日付範囲をゼロに設定するとチェックが実行されず、以降の収集時間を持つすべてのインベントリが処理されます。

**注：**すべてのテナントに対する処理ルールを定義するのではない場合、以下の設定に関するデフォルトの処理ルールを定義できます。

- いずれのルールも設定されていないすべてのテナント
- 収集フォルダ内のテナンシー番号のないインベントリ ファイル

## インベントリ ファイルを処理するためのルールの設定

複数のテナントから収集されたインベントリ ファイルを処理するためのルールを指定できます。インベントリ ファイルを受け入れるか、または拒否するには、信頼レベルまたは収集時間に基づいてルールを設定します。

### インベントリ ファイルを処理するためのルールを設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。  
Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
4. [処理ルール] をダブルクリックします。  
[設定の変更] ダイアログ ボックスが表示されます。
5. ダイアログ ボックス内のフィールドに値を入力します。  
以下のフィールドについて説明します。

### テナント番号

テナント番号を指定します。

このテナント番号は、収集フォルダ テーブル内で定義されたテナント番号、つまり `ca_tenant` テーブル内の `tenant_number` 列に一致する必要があります。

### 信頼モード

インベントリ ファイルを処理するために信頼モードまたは収集日時を使用するかどうかを指定します。インベントリ ファイルを処理するために信頼レベルを使用するには [はい] に設定し、収集時間を使用するには [いいえ] に設定します。

### 同一日付範囲

収集時間の範囲を秒単位で指定します。同じ時間範囲内に収集日時が設定されているインベントリ ファイルは処理されません。

同一日付範囲を無効にするには、値をゼロに設定します。

注：各テナントには、処理ルールのセットを 1 つだけ定義する必要があります。

[OK] をクリックします。

6. ポリシー ノードを右クリックして、メニューから [封印] を選択します。

ポリシーが封印されます。

7. [すべてのコンピュータ] フォルダのスケラビリティ サーバに、ポリシーをドラッグアンドドロップします。

ポリシーがスケラビリティ サーバに適用されます。

**注：** 各テナントに対して処理ルールを定義するのではない場合、またはテナント番号のない設定フォルダが存在する場合、**Asset Collector** 設定セクションで以下の処理ルールを定義します。

- 処理ルール: デフォルト信頼モード
- 処理ルール: デフォルト同一日付範囲

デフォルトルールを定義すると、テナント処理ルールと同じ動作が実行されます。ただし、指定されたテナントにルールが定義されていない場合、またはサブミットされたアセットにテナントが関連付けられていない場合に適用されます。

## 発行元信頼レベル マッピング

発行元信頼レベル マッピングを使用すると、特定の発行元からのアセットに対する信頼レベルを定義できます。信頼レベルの定義は、複数の発行元からインベントリ情報を収集する場合に役立ちます。収集されたアセット ファイルに信頼レベルが定義されていない場合、マッピングが使用されます。

### 発行元信頼レベル マッピングを設定する方法

1. **DSM** エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。  
Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
4. [発行元信頼レベルマッピング] をダブルクリックします。  
[設定の変更] ダイアログ ボックスが表示されます。
5. 各発行元について、信頼レベルを定義します。

注：同じ発行元に対して、複数の信頼レベルを定義しないでください。ただし、同じ信頼レベルを複数の発行元に対して使用できます。

[OK] をクリックします。

6. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
7. [すべてのコンピュータ] フォルダのスケーラビリティ サーバに、ポリシーをドラッグアンドドロップします。  
ポリシーがスケーラビリティ サーバに適用されます。

## テナント番号の設定

Client Automation エージェントのテナント分類を必要とする CA Service Desk Manager のような別の CA 製品が存在する場合、テナント番号を指定できます。スケーラビリティ サーバの設定ポリシーでテナント番号を指定することにより、Client Automation エージェントとテナントを関連付けることができます。

スケーラビリティ サーバは、単一のテナントのみをサポートできます。別のテナントのエージェントを収集する場合、各テナントに対して別のスケーラビリティ サーバを使用する必要があります。

テナント番号は、CA Service Desk Manager または CA IT Asset マネージャによって `ca_tenant` テーブルで定義されています。

スケーラビリティ サーバによって登録されるアセットで使用され、テナント番号が Asset Collector によって指定されない場合に限り適用されるテナント番号を設定する必要があります。

### スケーラビリティ サーバ上でテナント番号を設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [共通サーバ] に移動します。  
[共通サーバ] ペインに共通サーバ ポリシーが表示されます。
4. [テナント番号] をダブルクリックします。  
[プロパティの設定] ダイアログ ボックスが表示されます。
5. テナント番号を入力し [OK] をクリックします。

**注：**適用されるテナント番号は、`ca_tenant` テーブル内のテナント番号に一致する必要があります。

6. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
7. [すべてのコンピュータ] フォルダのスケーラビリティ サーバに、ポリシーをドラッグアンドドロップします。  
ポリシーがスケーラビリティ サーバに適用されます。

## 未来の収集時間を持つインベントリ ファイルの拒否

*xml* インベントリ無署名のファイル (*.xiu*) 内で有効なタイムスタンプを持つインベントリ ファイルのみ受け入れ、未来の収集時間を持つインベントリ ファイルを拒否するように **Asset Collector** を設定できます。未来の日付を定義するように同一日付許容範囲を設定して、別のタイムゾーンからのインベントリ ファイルの処理を支援できます。

### 未来の収集時間を持つインベントリ ファイルを拒否するよう設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。  
Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
4. 以下の設定パラメータを変更します。

#### 収集日時: 収集日時のないインベントリを許可

収集日時が指定されていないインベントリ ファイルを許可するかどうかを指定します。

XML に収集日時が存在しないインベントリ ファイルを許可するには、[はい] に設定します。

#### 収集日時: 未来の日時の許容範囲

現在の日時に適用される許容範囲を秒単位で指定して、未来の日時を定義します。

収集日時が未来になっているインベントリ ファイルは、未来の日時と照合されます。

#### 収集日時: 未来の日時のファイルを拒否

収集日時が未来の日時を超えるインベントリ ファイルを拒否します。

収集時間が未来の日時の許容範囲を超えるファイルを拒否するには、この値を [はい] に設定します。

5. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。

6. [すべてのコンピュータ] フォルダのスケールビリティ サーバに、ポリシーをドラッグアンドドロップします。

ポリシーがスケールビリティ サーバに適用されます。

## 後処理アクションの設定

Asset Collector プロセスでインベントリ ファイルを処理する場合、以下の結果となる可能性があります。

- インベントリ ファイルが受け入れられる
- インベントリ ファイルが拒否される
- インベントリ ファイルにエラーが含まれる

Asset Collector では、上記のイベントに対して後処理アクションを定義できます。

インベントリ ファイルが拒否される場合、またはエラーが含まれる場合には、ファイルを削除するか、ファイルを出力フォルダにコピーするか、または拡張子 .error を付けてファイル名を変更するように Asset Collector を設定できます。

インベントリ ファイルが受け入れられる場合、ファイルを削除するか、またはファイルを出力フォルダにコピーするように Asset Collector を設定できます。

### 後処理アクションを設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。

Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。

4. 以下の設定パラメータを変更します。

### 拒否されたインベントリ ファイル

拒否されたインベントリ ファイルに対するアクションを指定します。

ファイルを削除するにはパラメータ値を **0** に、ファイルを出力フォルダに移動するには **1** に、拡張子 .error を使用してファイル名を変更するには **2** にそれぞれ設定します。

### インベントリ ファイル処理

処理されたインベントリ ファイルに対するアクションを指定します。



ファイルを削除するにはパラメータ値を **0** に設定し、ファイルを出力フォルダに移動するには **1** にそれぞれ設定します。

### インベントリ ファイル エラー

エラーを含んでいるインベントリ ファイルに対するアクションを指定します。

ファイルを削除するにはパラメータ値を **0** に、ファイルを出力フォルダに移動するには **1** に、拡張子 **.error** を使用してファイル名を変更するには **2** にそれぞれ設定します。

5. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
6. [すべてのコンピュータ] フォルダのスケラビリティ サーバに、ポリシーをドラッグアンドドロップします。  
ポリシーがスケラビリティ サーバに適用されます。

## Asset Collector MDB 監査の設定

MDB 内で監査情報を生成して、トレーサビリティとレポート機能を強化できます。

監査レコードを生成するように **Asset Collector** を設定できます。これらのレコードは、MDB で **CA\_AC\_AUDIT\_LOG** テーブルに書き込まれます。

## Asset Collector 監査の設定

Asset Collector は、監査イベントの内部キャッシュを維持し、サイズまたは経過期間に関してしきい値に到達すると、それらをスケーラビリティ サーバに送信します。

ユーザの環境に対応するように、しきい値をカスタマイズできます。

Asset Collector 監査を設定するには、以下の手順に従います。

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印解除済みポリシーを展開します。  
ポリシーが展開されます。
4. [DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。  
Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
5. ユーザの環境に対応して、以下の設定パラメータを変更します。

### 監査ログ：最大経過時間

MDB に格納するためにスケーラビリティ サーバに送信される監査ログのキューの最大経過時間を指定します。

### 監査ログ：待機時間

ポーリング期間を秒単位で指定します。ポーリング期間は、監査コンポーネントが監査ログのキューと経過期間を確認するために使用されます。

### 監査ログ：最大キュー サイズ

MDB に格納するためにスケーラビリティ サーバに送信される監査ログのキューの最大項目数を指定します。

6. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
7. [すべてのコンピュータ] フォルダのスケーラビリティ サーバに、ポリシーをドラッグアンドドロップします。  
ポリシーがスケーラビリティ サーバに適用されます。

## Asset Collector 監査イベントの設定

Asset Collector の設定セクションから、監査レコードを生成するイベントを設定できます。

### Asset Collector 監査イベントを設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印解除済みポリシーを展開します。  
ポリシーが展開されます。
4. [DSM] - [スケーラビリティ サーバ] - [Asset Collector] - [イベント] に移動します。  
設定可能な監査イベントが表示されます。
5. 以下のように、ユーザの要件に一致する監査イベントを設定します。

### 受け入れたアセットの監査

正常に処理された各インベントリ ファイルに対して監査レコードを作成するかどうかを指定します。

### 未来の収集日時による拒否を監査

インベントリ ファイルに指定されている収集日時が未来の日時であるためそのファイルを拒否するときに監査レコードを作成するかどうかを指定します。

### 古い収集日時による拒否を監査

インベントリ ファイルに指定されている収集日時が同じアセットの前のサブミットより古いいためそのインベントリ ファイルを拒否するときに監査レコードを作成するかどうかを指定します。

### 同一収集日による拒否を監査

インベントリ ファイルの収集日時が前回処理されたアセットの同一日付範囲に含まれるためそのインベントリ ファイルを拒否するときに監査レコードを作成するかどうかを指定します。

### 必須値の不足による拒否を監査

インベントリ ファイル内にキー値が見つからないためそのファイルを拒否するときに監査レコードを作成するかどうかを指定します。

6. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
7. [すべてのコンピュータ] フォルダのスケラビリティ サーバに、ポリシーをドラッグアンドドロップします。  
ポリシーがスケラビリティ サーバに適用されます。

## Asset Collector 収集監査テーブル

Asset Collector 収集監査項目は、CA\_AC\_AUDIT\_LOG テーブルに書き込まれます。このテーブルには、以下の列があります。

| 名前          | 説明                                        |
|-------------|-------------------------------------------|
| アセット名       | アセットのホスト名を定義します。                          |
| MAC アドレス    | 利用可能な場合、MAC アドレスを定義します。                   |
| スケラビリティ サーバ | Asset Collector がレポートするスケラビリティ サーバを定義します。 |
| 発行元         | アセットの発行元を定義します。                           |
| テナント番号      | アセットのテナント ID を指定します。                      |
| 状態          | アセットが受け入れられた (0) か、または拒否された (1) かを指定します。  |
| イベント コード    | アセットの拒否に関するイベント コードを指定します。                |
| 詳細          | アセットを拒否する理由を示します。                         |

CA\_AC\_AUDIT\_LOG テーブルの [イベント コード] 列には、以下のイベント コードが表示される可能性があります。

| イベント<br>コード | 原因 | 説明                                                   |
|-------------|----|------------------------------------------------------|
| 0           | なし | アセットが受け入れられることを指定します。アセットが受け入れるイベントに対して、値がゼロに設定されます。 |

| イベント<br>コード | 原因         | 説明                                                                              |
|-------------|------------|---------------------------------------------------------------------------------|
| 1           | 古い収集日時     | 同じアセットに関して、最後に受け入れられたインベントリ ファイルよりも収集時間の値が小さいため、アセットが拒否されることを指定します。             |
| 2           | より低い信頼レベル  | 信頼レベルが有効になっている同じアセットに関して、最後に受け入れられたインベントリ ファイルよりも信頼レベルが低い場合、アセットが拒否されることを指定します。 |
| 3           | 最後の送信と同じ日付 | 同じアセットに関して、最後に受け入れられたインベントリ ファイルと同じ日付許容範囲に収集時間が入るため、アセットが拒否されることを指定します。         |
| 4           | 未来の収集時間    | 収集時間が未来の時間を表しているため、アセットが拒否されることを指定します。                                          |
| 5           | 値が欠落       | いくつかのキー データ フィールドが欠落しているため、アセットが拒否されることを指定します。                                  |

## 監査テーブル管理

古いレコードをパージすることにより、CA\_AC\_AUDIT\_LOG テーブルのサイズを管理できます。Asset Collector の設定セクション内で値を設定することにより、古いレコードをパージできます。

### 古いレコードのパージを設定する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [設定] - [設定ポリシー] ノードに移動します。
2. 封印済みポリシーを右クリックし、[封印解除] を選択します。  
ポリシーが封印解除されます。
3. 封印されていないポリシーを展開し、[DSM] - [スケーラビリティ サーバ] - [Asset Collector] に移動します。  
Asset Collector ポリシーが、[Asset Collector] ペインに表示されます。
4. 以下のパラメータを変更します。

### 監査パージ間隔

監査レコードがパージされるまで時間を、日数で指定します。

パージを防止するには、値をゼロに設定します。

### 監査パージ最大経過時間

監査レコードをパージするまでの経過期間を、日数で指定します。

5. ポリシー ノードを右クリックして、メニューから [封印] を選択します。  
ポリシーが封印されます。
6. [すべてのコンピュータ] フォルダ内にあるドメイン マネージャに、ポリシーをドラッグ アンド ドロップします。  
ポリシーがドメイン マネージャに適用されます。

## セキュリティ

このセクションでは、Asset Collector の使用に際して、考慮する必要があるセキュリティ関連の項目について説明します。

## 収集フォルダの保護

Asset Collector は、収集フォルダのポリシーで設定されたフォルダから、インベントリ ファイルを収集します。これらのフォルダについては、オペレーティング システムのセキュリティ機能を使用して、権限を持つユーザのみがフォルダからファイルを作成、変更、または削除できるようにすることをお勧めします。

## デジタル署名付きのインベントリ ファイル

Asset Collector では、パブリック キー インフラストラクチャ (PKI) の署名プロセスを使用して、ファイルの作成者の信頼性を確認できます。

関連項目：

[一般的な環境における Asset Collector の設定](#) (P. 332)

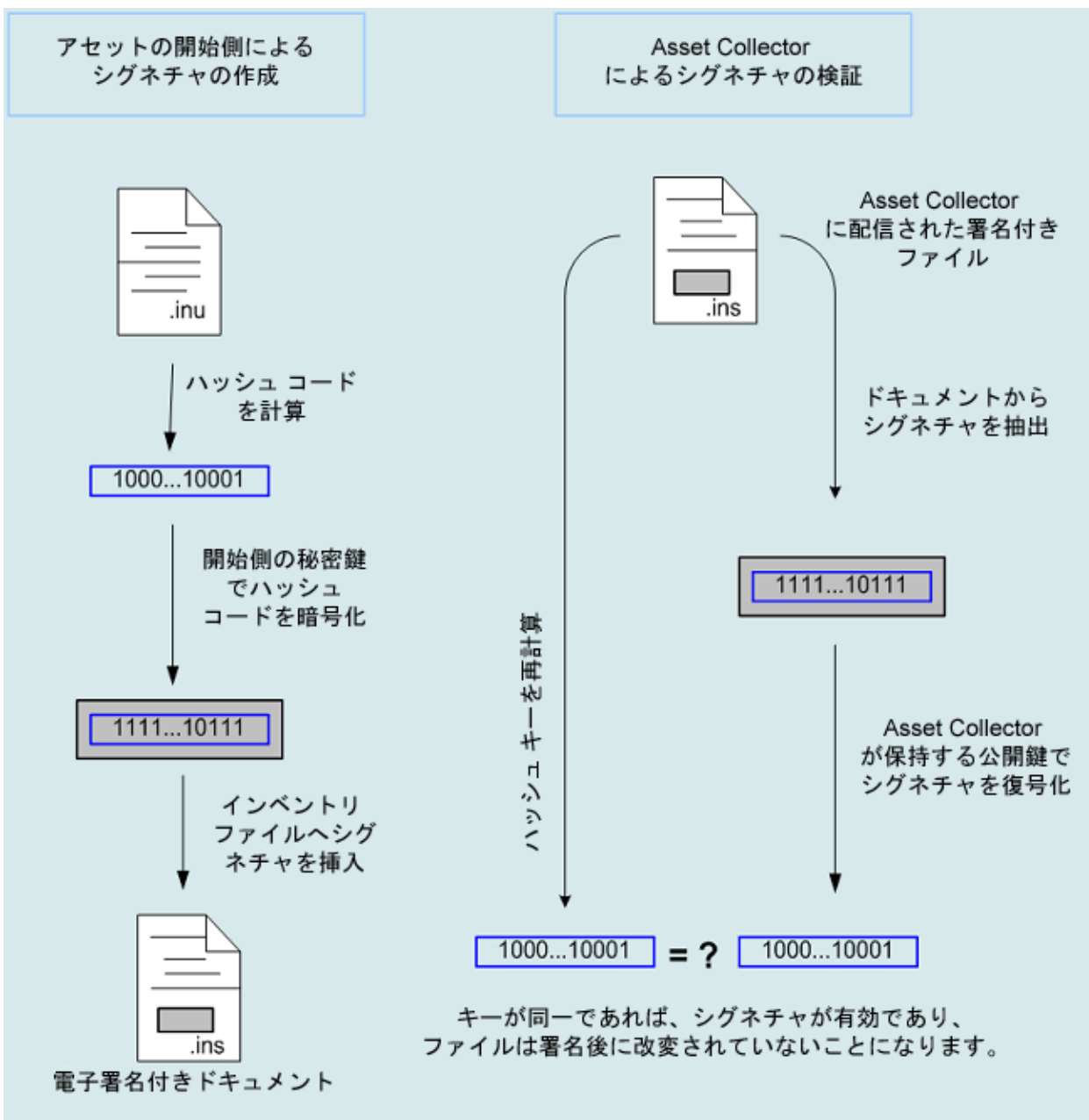
## デジタル署名付きのインベントリ ファイルの確認方法

以下では、デジタル署名付きインベントリ ファイルの処理方法について説明します。

1. 管理者は証明書を作成し、インベントリ ファイルに署名するマシンに証明書をインストールします。さらに、署名を検証する Asset Collector に公開鍵をインストールします。
2. インベントリ ファイルは `invsign.exe` ツールを使用して署名されます。  
詳細は、「[invSign - インベントリ ファイルの署名、検証、または署名解除](#) (P. 356)」を参照してください。
3. インベントリ ファイルは、Asset Collector 収集フォルダに配信されます。ここで、以前インストールした公開鍵を使用して、署名が認証されます。

**重要：** 署名を構成するバイナリ情報が破損するため、署名ファイルは変更しないでください。

以下の図に、この手順を示します。





## cacertutil create — 証明書の作成

cacertutil create コマンドで証明書を作成します。

このコマンドのフォーマットは、以下のとおりです。

```
cacertutil create -o:filename -op:passphrase -s:subject -od:filename
```

**-o:filename**

証明書の出力ファイル名を指定します。

**-op:passphrase**

証明書を暗号化するパスフレーズを指定します。

**-s:subject**

証明書の発行先をサブジェクト名に指定します。

**-od:filename**

公開証明書のみを使用して、DER でエンコードされたファイルを作成します。

### 例：証明書の作成

以下の例では、AssetCollectorCert.p12 および AssetCollectorCert.der の 2 つのファイルを作成します。.der ファイルには証明書の公開部分のみが含まれます。.der ファイルは、署名を検証する Asset Collector コンピュータにコピーする必要があります。

```
cacertutil create -o:c:\AssetCollectorCert.p12 -op:password
-s:"CN=AssetCollector,O=Computer Associates,c=US" -od:c:\AssetCollectorCert.der
```

注：cacertutil コマンドの詳細については、「コマンドライン リファレンス ガイド」を参照してください。

## cacertutil import — 証明書インポート

`cacertutil import` コマンドで、証明書を Client Automation comstore にインポートします。

**重要：** この操作は、管理者がインベントリ ファイルの署名を行う予定のコンピュータで実行する必要があります。また、署名前に行う必要があります。

このコマンドのフォーマットは、以下のとおりです。

**注：** `cacertutil` コマンドの詳細については、「コマンドライン リファレンス ガイド」を参照してください。

```
cacertutil import -i:filename -ip:passphrase -t: tag
```

**-i:filename**

インポートする証明書のファイル名を指定します。

以下が重要なパラメータです。

**-ip:passphrase**

パスフレーズを指定し、暗号化して **comstore** に格納します。

**-t:tag**

タグ名を指定します。

**注：** インベントリ ファイルの検証および署名を実行するコンピュータでは、**-t** パラメータで指定されたのと同じタグ名を使用する必要があります。

### 例：証明書のインポート

```
cacertutil import -i:C:\AssetCollectorCert.p12 -ip:password -t:AssetCollector
```

## cacertutil import—公開鍵のインポート

cacertutil import コマンドで、Asset Collector サーバの公開鍵を Client Automation comstore にインポートします。

このコマンドのフォーマットは、以下のとおりです。

```
cacertutil import -i :filename -t:tag -it:certificatetype
```

**-i:filename**

インポートする証明書のファイル名を指定します。

以下が重要なパラメータです。

**-it:type**

インポートする証明書のタイプを指定します。有効なオプションは、X509V3 または PKCS#12 です。

デフォルトは PKCS#12 です。

**-t:tag**

タグ名を指定します。

注：cacertutil コマンドの詳細については、「コマンドライン リファレンス ガイド」を参照してください。

### 例：公開鍵のインポート

```
cacertutil import -i:C:\AssetCollectorCert.der -t:AssetCollector -it:x509v3
```

## invSign - インベントリ ファイルの署名、検証、または署名解除

`invsign` コマンドは、インベントリ ファイルの署名、検証、または署名解除に使用します。

**重要：** `invsign` コマンドの対象は、次の拡張子を持つファイルです。`.xiu` ファイル（署名用）、`.xis` ファイル（署名解除用）。`.xiu` ファイルは、署名に成功すると `.xis` ファイルに変更されます。`.xis` ファイルは、署名解除に成功すると `.xiu` ファイルに変更されます。

このコマンドのフォーマットは、以下のとおりです。

```
invsign command xiu or xis file [certificate tag]
```

### command

以下のコマンドのいずれかを含みます。

#### Sign

指定された証明書のタグを使用して、インベントリ ファイルに署名します。署名には、インベントリ ファイルの最後に追加されるバイナリ データ ストリームが含まれます。

**重要：** 署名付きインベントリ ファイルを開くと、ファイルの最後に予期しない文字が追加されてしまいます。したがって、署名付きインベントリ ファイルを開いたり、変更を加えようとししないでください。それが原因で、署名が無効になったり、ファイルが **Asset Collector** に拒否されることがあります。

**注：** 秘密鍵は、`sign` コマンドで指定されるタグ名を使用して、すでに証明書ストアにインポートされている必要があります。また、インベントリ ファイルに署名するには、署名に使用するコンピュータの `comstore` に証明書をインストールする必要があります。

#### Verify

インベントリ ファイルの署名を確認します。

**注：** 公開鍵は、署名プロセスの際に付与されたのと同じタグ名で使用する必要があります。

#### Unsign

インベントリ ファイルから署名を削除します。

### Inventory File

署名、検証、または署名解除するインベントリ ファイル名を定義します。

### Certificate Tag

(`sign` コマンドでは必須です)。インベントリ ファイルの署名中に割り当てる証明書タグを定義します。

注：証明書タグは、一意の証明書識別子です。各証明書には、1つの証明書タグが割り当てられます。

証明書タグは、`sign` コマンドを使用する場合のみ必須です。

### 例：invSign コマンド

```
invsign sign Server1.xiu AssetCollector
```

```
invSign verify Server1.xis
```

```
invSign unsign Server1.xis
```

`invsign` コマンドラインを使用して、署名、署名解除、および検証を実行する複数のファイルを指定できます。

複数ファイルの `sign` の形式は、以下のとおりです。

```
Invsign sign file1.xiu file2.xiu file3.xiu [certificate tag]
```

以下のようにワイルドカードを使用することもできます。

```
Invsign sign f*.xiu [certificate tag]
```

または、以下のように組み合わせて使用することができます。

```
Invsign sign f*.xiu newComputer.xiu [certificate tag]
```

**重要：** `unsign` および `verify` コマンドでも、複数ファイルとワイルドカードを指定することができます。これらのコマンドに、*CertificateName* は指定しないでください。

関連項目：

[インベントリ ファイルの種類](#) (P. 324)

## 発行元および信頼レベルを表示する

アセット、ソフトウェア インベントリとハードウェア インベントリ、およびユーザの発行元および信頼レベルを表示できます。

## アセットの発行元と信頼レベル

アセットの発行元と信頼レベルは、DSM エクスプローラのアセットのホーム ページから表示できます。

- アセットのホーム ページ。信頼レベルと発行元は、以下の図に示されているように [ステータス] ペインに表示されます。

DSM Explorer > ITOMTest - ドメイン > コンピュータおよびユーザ > すべてのコンピュータ > MACHINE\_NAME

ホームページ インベントリ ソフトウェア インスタント診断 詳細

**概要**

**インベントリ**

|          |                                  |
|----------|----------------------------------|
| 名前       | MACHINE_NAME                     |
| タイプ      |                                  |
| シリアル番号   |                                  |
| プラットフォーム | Windows NT Server 4.0 Enterprise |
| バージョン    |                                  |
| サービス パック |                                  |
| モデル      |                                  |
| ベンダー     |                                  |
| メモリの合計   |                                  |
| 前回の実行    | 2009/04/11 16:02:49              |

**設定**

|          |     |
|----------|-----|
| PXE 管理対象 | いいえ |
|----------|-----|

**ステータス**

違反したポリシー (0)

なし

失敗したジョブ (0)

なし

実行が回避されたアプリケーション (0)

なし

**エージェント ステータス (0)**

|           |               |
|-----------|---------------|
| AMT ステータス | 不明            |
| AM ステータス  | インストールされていません |
| RO ステータス  | インストールされていません |
| SD ステータス  | インストールされていません |
| 保護ステータス   | インストールされていません |
| エージェント制限  | なし            |
| 信頼レベル     | ...           |
| 発行元       | XML File      |

- [コンピュータ グループ] ペイン

DSM Explorer > ITOMTest - ドメイン > コンピュータおよびユーザ > すべてのコンピュータ

情報 名前 OS 信頼レベル 発行元 AM ステータス

| 名前                    | OS                | 信頼レベル | 発行元      | AM ステータス     |
|-----------------------|-------------------|-------|----------|--------------|
| Domain                | Windows Server... | ***** | CA       | 操作可能         |
| assetcollected.ca.com | Windows NT Ser... | ...   | XML File | インストールされて... |
| tableData             | Windows NT Ser... | ...   | XML File | インストールされて... |

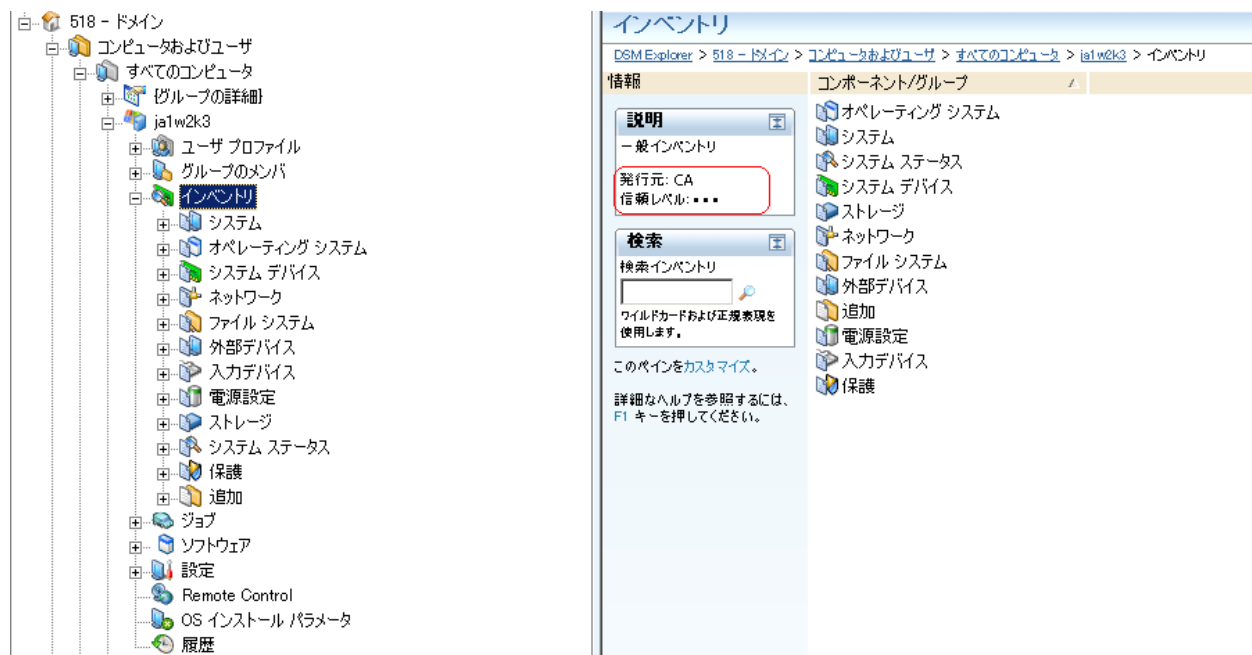
**説明**

【すべてのコンピュータ】フォルダには、ネットワーク上にあるコンピュータのうち、ドメインと接続している DSM エージェントのあるコンピュータがすべて一覧表示されます。

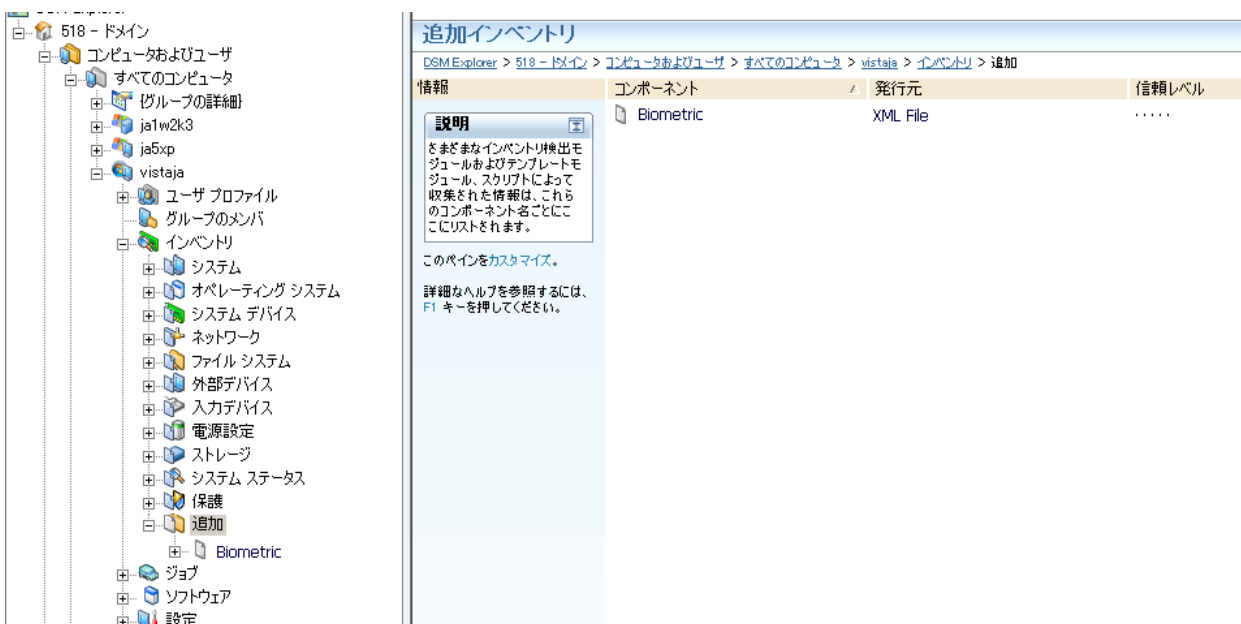
## ハードウェア インベントリの発行元と信頼レベル

アセットの発行元と信頼レベルは、DSM エクスプローラの以下の場所から表示できます。

- [インベントリ] フォルダの [情報] ペイン。以下の図で示すように、いずれかのインベントリ項目を選択すると、[情報] ペインに発行元と信頼レベルが表示されます。



- [追加インベントリ] フォルダの右ペインの [発行元] および [信頼レベル] 列。これらの列は、デフォルトで非表示になっています。以下の図で示すように、該当する列のヘッダを右クリックして、[発行元] および [信頼レベル] を選択すると、これらの列を表示できます。



## ソフトウェア インベントリの発行元と信頼レベル

「検出されたソフトウェア」ペインでソフトウェアを右クリックし、「詳細」を選択すると、ソフトウェア インベントリの発行元と信頼レベルを表示できます。これにより、以下の図で示すように、選択したソフトウェアの発行元と信頼レベルが記述されたソフトウェア レポートが表示されます。



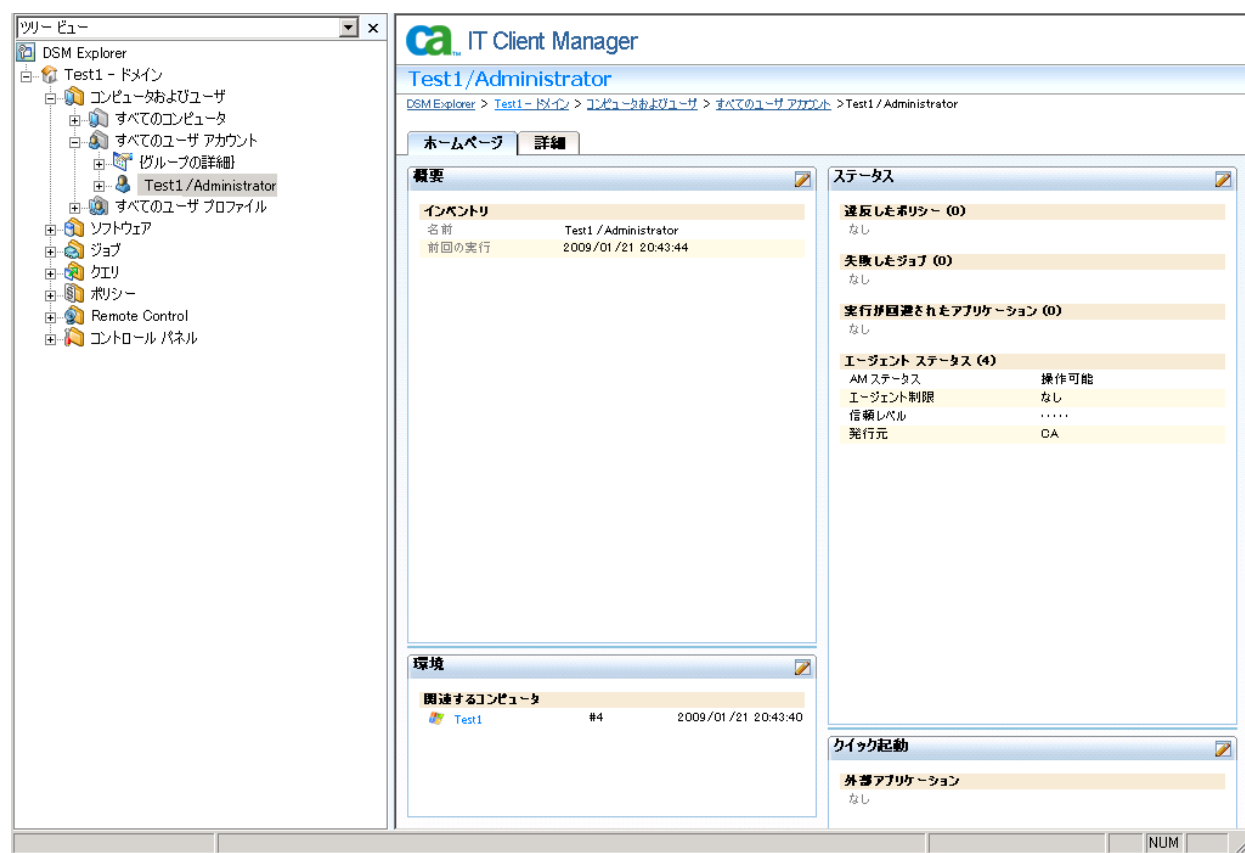
注：「検出されたソフトウェア」ペインでソフトウェア アイテムを複数選択することもできます。



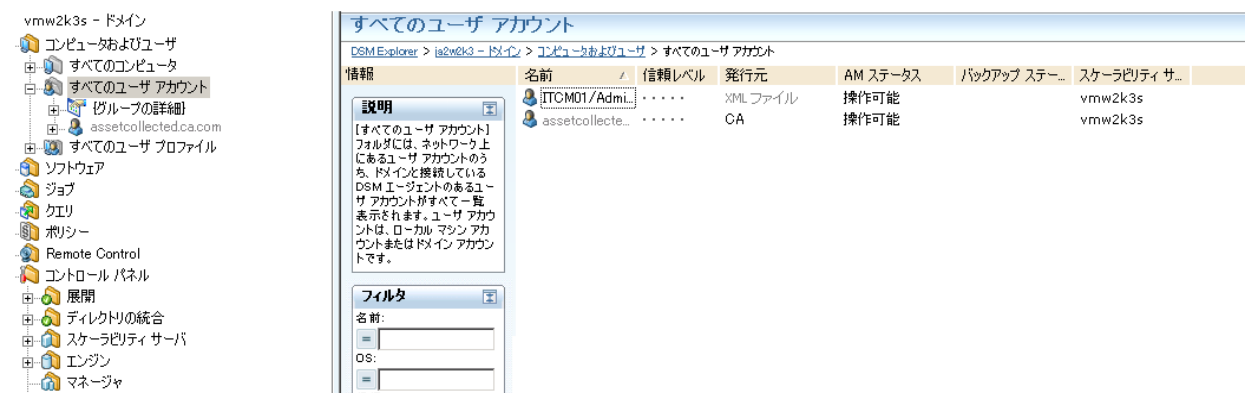
## ユーザの発行元と信頼レベル

ユーザの発行元と信頼レベルは、DSM エクスプローラのアセットのホーム ページから表示できます。

- ユーザのホーム ページ。信頼レベルと発行元は、以下の図に示されているように [ステータス] ペインに表示されます。



- [すべてのユーザ アカウント] ペイン



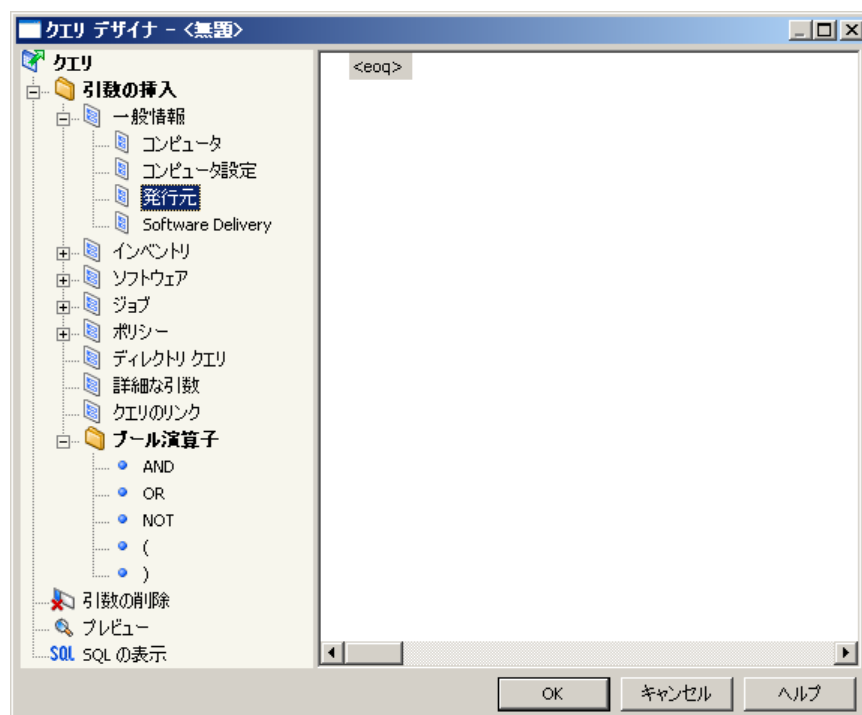
## [ クエリ デザイナ ] ダイアログ ボックス

[ クエリ デザイナ ] ダイアログ ボックスでは、アセットの発行元と信頼レベルを照会できます。

[ 発行元 ] をクリックすると [ フィールドを選択 ] ダイアログ ボックスが開きます。そこで照会する発行元と信頼レベルのパラメータを指定します。

注：このリリースでは、ユーザ信頼レベルと発行元を持つクエリを作成できません。

以下の図は、[ 引数の挿入 ] - [ 一般情報 ] の下の [ 発行元 ] カテゴリを示しています。



## インベントリ ファイルの作成

Asset Collector で処理するインベントリ ファイルを作成できます。

## インベントリ ファイル形式

Asset Collector では、拡張子が `.xiu` および `.xis` のすべてのファイルの処理を試行します。

- `.xiu` = xml インベントリ ファイル（署名なし）
- `.xis` = xml インベントリ ファイル（署名あり）

**重要：** これらのファイルは、まだ `xml` を含むテキスト ファイルのままです。

`invsign` ツールでも、`.xiu` ファイル（署名用）、および `.xis` ファイル（署名解除用）のみ使用します。

インベントリ ファイルには、以下の例のように、一般的な `header` セクション、`hardware` セクション、および `software` セクションがあります。

```
<asset translator="ACBsFmt" version="1_0">
<asset>
 <general> </general>
 <hardware> </hardware>
 <software> </software>
 <user>
 <general> </general>
 <hardware> </hardware>
 <software> </software>
 </user>
</asset>
```

このレイアウトで示すように、`xiu` ファイルの中にオプションの `<user>` セクションを入れ、この `<user>` セクションにハードウェア セクションとソフトウェア セクションを入れることもできます。

**重要：** 最初の行は、Asset Collector でこのファイルをどのように解析するかを示しているなので、省略することはできません。

## general セクション

**general** セクションにはインベントリ項目のエントリが含まれます。**header** セクションで許可される項目は、記述されている項目のタイプによって決まります。いくつかの **header** 項目は **<asset> <general>** セクションのみで指定しますが、別の項目は **<user> <general>** セクションのみで指定する必要があります。ユーザー一般セクションとアセット一般セクションのどちらでも指定できる属性もあります。

ユーザは単独で配信することも、コンピュータとともに配信することもできます。ユーザをコンピュータと配信すると、ユーザはそのコンピュータにリンクされます。この関連は、**DSM** エクスプローラで表示されます。

以下の表に、**general** セクションのタグを示します。

| 名前                      | 説明                                                                            | ヘッダ   |
|-------------------------|-------------------------------------------------------------------------------|-------|
| <i>vendor</i>           | 文字列（オプション）                                                                    | asset |
| <i>serial_number</i>    | 文字列（オプション）                                                                    | asset |
| <i>asset_tag</i>        | 文字列（オプション）                                                                    | asset |
| <i>host_name</i>        | 完全修飾名ではない（必須）                                                                 | asset |
| <i>host_key</i>         | 指定されていない場合は、キー文字列が生成されます（オプション）                                               | asset |
| <i>class_id</i>         | 文字列または数字のプラットフォーム名<br><br>注：プラットフォーム名の詳細リストについては、付録の「プラットフォーム名および ID」を参照ください。 | asset |
| <i>Network_id</i>       | オプション<br><br>注：XIU ファイルの登録セクションで複数のネットワーク インターフェースをサポートします。                   | asset |
| <i>default_address</i>  | 必須                                                                            | asset |
| <i>default_mac</i>      | 必須                                                                            | asset |
| <i>default_hostname</i> | 必須                                                                            | asset |

| 名前                         | 説明                 | ヘッダ    |
|----------------------------|--------------------|--------|
| <i>default_subnet_mask</i> | オプション              | asset  |
| <i>collect_time</i>        | 秒数（オプション）          | asset  |
| <i>trustlevel</i>          | 1 ～ 5 までの整数（オプション） | asset  |
| <i>origin</i>              | 文字列（オプション）         | asset  |
| <i>fileid</i>              | 最大長 36             | user   |
| <i>URI</i>                 | 必須                 | user   |
| <i>user_name</i>           | 必須                 | user   |
| <i>domain_name</i>         | N/A                | user   |
| <i>previous_uri</i>        | N/A                | user   |
| <i>r_usage_list</i>        | N/A                | user   |
| <i>r_name</i>              | N/A                | user   |
| <i>r_proc_os_id</i>        | N/A                | user   |
| <i>r_ip_address</i>        | N/A                | user   |
| <i>user_item_1</i>         | N/A                | common |
| <i>user_item_2</i>         | N/A                | common |
| <i>user_item_3</i>         | N/A                | common |
| <i>user_item_4</i>         | N/A                | common |
| <i>r_computer</i>          | N/A                | common |
| <i>collect_time</i>        | N/A                | common |
| <i>trustlevel</i>          | 1 から 5 の整数         | common |
| <i>origin</i>              | 最大 64 文字の文字列       | common |

注：MAC アドレスが無効の場合は、アセットの UUID を指定することができます。

### 例：ユーザのみ

ファイル内でユーザのみの場合の形式は、次のようになります。

```
<asset>
 <user>
 <general> </general>
 <hardware> </hardware>
 <software> </software>
 </user>
</asset>
```

hardware セクションと software セクションは、ファイルの asset セクションと user セクションの両方で任意です。

### 例：ユーザおよびアセット

アセットとともに配信されるユーザの形式は、次のようになります。

```
<asset>
 <general> </general>
 <hardware> </hardware>
 <software> </software>
 <user>
 <general> </general>
 <hardware></hardware>
 <software> </software>
 </user>
</asset>
```

### 例：general セクション

以下は、general セクションのコード例です。

```
<?xml version="1.0" encoding="utf-8" ?>
<asset translator="ACBsFmt" version="1_0">
 <general>
 <host_name>machine1</host_name>
 <default_hostname>machine1.domain.com</default_hostname>
 <default_address>150.120.13.119</default_address>
 <default_mac>00:0D:56:CB:C1:ED</default_mac>
 <class_id>21</class_id>
 <network_id>
 <mac_address>mac</mac_address>
 <ip_address>ip</ip_address>
 <dns_name>name</dns_name>
 <subnet_mask></subnet_mask>
 </network_id>
 <host_key>70669be2-1fed-4201-9777-d7137486dcab</host_key>
 <origin>User Keyed</origin>
 </general>
</asset>
```

注：Default\_hostname、default\_address、default\_subnet\_mask は、必須エントリです。network\_id セクションは任意です。複数の network\_id セクションを含めることができます。default\_hostname、default\_subnet\_mask、default\_mac は、common\_asset\_report の default\_XXX フィールドで使用されます。追加の network\_id セクションは、登録メッセージに読み込まれます。

以下の図は、**general** セクション インベントリが **DSM** エクスプローラでどのように表示されるかを示します。

すべてのコンピュータ

DSM Explorer > is1w2k3 - ドメイン > コンピュータおよびユーザ > すべてのコンピュータ

| 情報                                                                                                | 名前       | OS                 | 信頼レベル | 発行元        | AM ステータス | SD ステータス      |
|---------------------------------------------------------------------------------------------------|----------|--------------------|-------|------------|----------|---------------|
| <b>説明</b><br>[すべてのコンピュータ] フォルダには、ネットワーク上にあるコンピュータのうち、ドメインと接続している DSM エージェントのあるコンピュータがすべて一覧表示されます。 | ドメイン     | Windows Server ... | ..... | CA         |          | 操作可能          |
|                                                                                                   | machine1 | Windows NT Ser...  | ...   | User Keyed |          | インストールされていません |

上の図では、以下の点に注目してください。

- **Machine1** は、**Asset Collector** を通じて、完全に有効なエージェントではないとレポートされたため使用できません。
- 上の例のインベントリ ファイルには、**trustlevel** タグが含まれていなかったため、デフォルトの信頼レベル 3 が **Machine1** に割り当てられます。
- **Machine1** の[発生元]列には、上の例の XML ファイルで指定された **User Keyed** が表示されます。

## hardware セクション

**hardware** セクションには、一般インベントリおよび追加インベントリのエントリが含まれます。**General Inventory** セクションには、**Client Automation** エージェントに収集されたインベントリ グループおよびインベントリ属性のみを設定できます。ユーザ定義のグループおよび属性を追加する場合は、**GeneralInventory group** タグの外側で作成する必要があります。ユーザ定義のグループおよび属性は、**DSM** エクスプローラの [追加] フォルダの下の [インベントリ] に表示されます。

**hardware** セクションには以下のタグがあります。

### group name

グループ名を定義します。この下に、インベントリ項目が作成されます。

### attribute name

インベントリ項目の名前、タイプ、およびサブタイプを定義します。



### 例：hardware セクション ( 属性および値 )

以下は、hardware セクションのコード例です。

```
<hardware>
<group name="GeneralInventory">
 <group name="System">
 <attribute name="Total Memory" type="int64"
 subtype="byte">2147483648</attribute>
 <attribute name="Model" type="string">OptiPlex GX270</attribute>
 <attribute name="Type" type="string">Desktop</attribute>
 <attribute name="No of Processors" type="int32"
 subtype="normal">1</attribute>
 <attribute name="No of COM ports" type="int32"
 subtype="normal">2</attribute>
 <attribute name="No of Printer ports" type="int32"
 subtype="normal">1</attribute>
 <attribute name="No of USB ports" type="int32"
 subtype="normal">2</attribute>
 <attribute name="No of Video ports" type="int32"
 subtype="normal">1</attribute>
 <attribute name="Vendor" type="string">Dell Computer
 Corporation</attribute>
 <attribute name="Serial Number" type="string">50ZQ21J</attribute>
 <attribute name="Asset Tag" type="string">N/A</attribute>
 <attribute name="System ID"
 type="string">44454C4C-3000-105A-8051-B5C04F32314A</attribute>
 </group>
</group>
</hardware>
```

以下の図は、上記コードの GUI 結果を示します。



## 例：ハードウェア インベントリ ファイル ( 表形式 )

以下は、ハードウェア インベントリ ファイルのコード例です。

```
<hardware>
 <group name="GeneralInventory">
 <group name="FileSystem">
 <group name="LocalFileSystem" tableid="0001">
 <attribute name="Device" type="string">%Device%HarddiskVolume1</attribute>
 <attribute name="FileSystem" type="string">FAT32</attribute>
 <attribute name="Free" type="int64" subtype="G">2230124544</attribute>
 <attribute name="Mount Point" type="string">C:¥</attribute>
 <attribute name="Name" type="string">C:¥</attribute>
 <attribute name="Serial Number" type="string">5872-D416</attribute>
 <attribute name="Size" type="int64" subtype="G">3784294400</attribute>
 <attribute name="Type" type="string">Fixed</attribute>
 <attribute name="Used" type="int64" subtype="G">1554169856</attribute>
 <attribute name="Used %" type="int32">20</attribute>
 <attribute name="Volume Label" type="string">C</attribute>
 </group>

 <group name="LocalFileSystem" tableid="0002">
 <attribute name="Device" type="string">%Device%HarddiskVolume2</attribute>
 <attribute name="FileSystem" type="string">FAT32</attribute>
 <attribute name="Free" type="int64" subtype="G">2230124544</attribute>
 <attribute name="Mount Point" type="string">D:¥</attribute>
 <attribute name="Name" type="string">D:¥</attribute>
 <attribute name="Serial Number" type="string">5872-D423</attribute>
 <attribute name="Size" type="int64" subtype="G">43784794400</attribute>
 <attribute name="Type" type="string">Fixed</attribute>
 <attribute name="Used" type="int64" subtype="G">41554269856</attribute>
 <attribute name="Used %" type="int32">89</attribute>
 <attribute name="Volume Label" type="string">D</attribute>
 </group>
 </group>
</group>
</group>
</hardware>
```

以下の図は、上記コードの GUI 結果を示します。



## 一般インベントリ グループおよび属性

アセット インベントリ内では、インベントリ ファイルの各グループは、**group** タグで表されます。最上位のグループ名は、**GeneralInventory** または **AdditionalInformation** のいずれかになります。**GeneralInventory** グループの下に特別なインベントリ グループを配置する場合は、以下のリストに指定されているグループ名を使用する必要があります。**GeneralInventory** グループの外で作成されたグループは、追加ノードの下に追加され、**DSM** エクスプローラではどのアイコンにも関連付けられません。ユーザ インベントリはグループ名にあらゆる文字列を使用できますが、ユーザ インベントリ グループはすべて同じアイコンで表示されるので注意してください。

以下は、アセット インベントリの **GeneralInventory** グループの下で使用するための有効なグループ名の一覧です。

- GeneralInventory
- System
- Mainboard
- Processors
- OperatingSystem
- Memory
- Keyboard
- SoundAdapters
- Monitor
- DisplayAdapter
- NetworkAdapters
- Network
- SystemBios
- IOPorts
- Country
- Identification
- TCPIP
- Controllers
- Disk
- HostInformation
- CronQueue
- Status

- FileSystems
- FixedDrives
- SwapDevices
- LocalFileSystem
- SystemSlots
- SystemDevices
- FloppyControllers
- DisplaySettings
- Installation
- RegionalSettings
- SystemUpdates
- Network
- IDEControllers
- USBControllers
- SCSIControllers
- IOPorts
- VideoAdapters
- SystemBios
- DNS
- WINS
- Storage
- FixedDrives
- FloppyDrives
- CDROMDrives
- Partitions
- LogicalVolumes
- InputDevices
- PointingDevices
- PowerSettings
- PowerPolicy
- ACAdapter
- SystemStatus

## ユーザ定義グループ

このセクションでは、マシン インベントリの [追加] フォルダの下に、さまざまな属性を持つユーザ定義グループを作成する方法について説明します。

### 例：ユーザ定義グループ

以下は、ユーザ定義グループのコード例です。

```
<hardware>

 <group name="Biometrics">

 <group name="Retina Scanner">
 <attribute name="Manufacturer" type="string">Eye Ball UK
 Inc.</attribute>
 <attribute name="Model" type="string">EyeReader 1.0</attribute>
 </group>
 </group>
</hardware>
```

以下の図は、ユーザ定義のハードウェア インベントリ ファイル セクションが DSM エクスプローラでどのように表示されるかを示します。



## タイプとサブタイプ

以下の表には、属性として指定することができる有効なタイプとサブタイプが含まれます。

注：サブタイプにより、値がどのように GUI に表示されるかが決定されます。

| タイプ                      | サブタイプ                | 説明                                   |
|--------------------------|----------------------|--------------------------------------|
| <b>Boolean</b>           |                      | Boolean 値は、以下のサブタイプに基づいて表示することができます。 |
|                          | TrueFalse            | True または False                       |
|                          | YesNo                | はい または いいえ                           |
|                          | OnOff                | ON または OFF                           |
|                          | SupportedUnsupported | サポートまたは未サポート                         |
|                          | ActiveNotactive      | 有効または無効                              |
|                          | OkError              | OK またはエラー                            |
|                          | PresentNotpresent    | あり または なし                            |
| <b>int32 &amp; int64</b> |                      | 数値は、以下のサブタイプに基づき表示することができます。         |
|                          | separation           | 3 桁区切り（例：1,000,000）                  |
|                          | normal               | 区切りなし                                |
|                          | K                    | 1024 で割った数字を表示                       |
|                          | M                    | 1024 の 2 乗で割った数字を表示                  |
|                          | G                    | 1024 の 3 乗で割った数字を表示                  |
|                          | T                    | 1024 の 4 乗で割った数字を表示                  |
|                          | kilo                 | 1000 で割った値を表示                        |
|                          | mega                 | 1e6 で割った値を表示                         |
|                          | giga                 | 1e9 で割った値を表示                         |
|                          | milli                | 1e3 を掛けた値を表示                         |
|                          | micro                | 1e6 を掛けた値を表示                         |

| タイプ          | サブタイプ        | 説明                                |
|--------------|--------------|-----------------------------------|
|              | nano         | 1e9 を掛けた値を表示                      |
|              | hex          | 16 進数で表示                          |
|              | time         | 日付で表示                             |
|              | timeInterval | 継続時間で表示                           |
|              | bytes        | GUI で KB、MB、GB、または TB で表示         |
| <b>Float</b> |              | 浮動小数点値は、以下のサブタイプに基づいて表示することができます。 |
|              | Auto         | 自動フォーマット                          |
|              | placesXX     | 小数点以下 XX で表示                      |
| 文字列          |              | 文字列にはサブタイプはありません                  |

## 新規グループの追加

hardware セクション内にある、GeneralInventory タグと AdditionalInventory タグの下にグループを追加し、関連するインベントリ属性をグループ化できます。

グループおよび属性を作成する構文は以下になります。

```
<group name="user defined name">
 <attribute name="attribute name"
 type="type"
 subtype="subtype">
 値
 </attribute>
</group>
```

注: 1 つのグループには、複数の属性と複数のグループを含めることができます。

## Software セクション

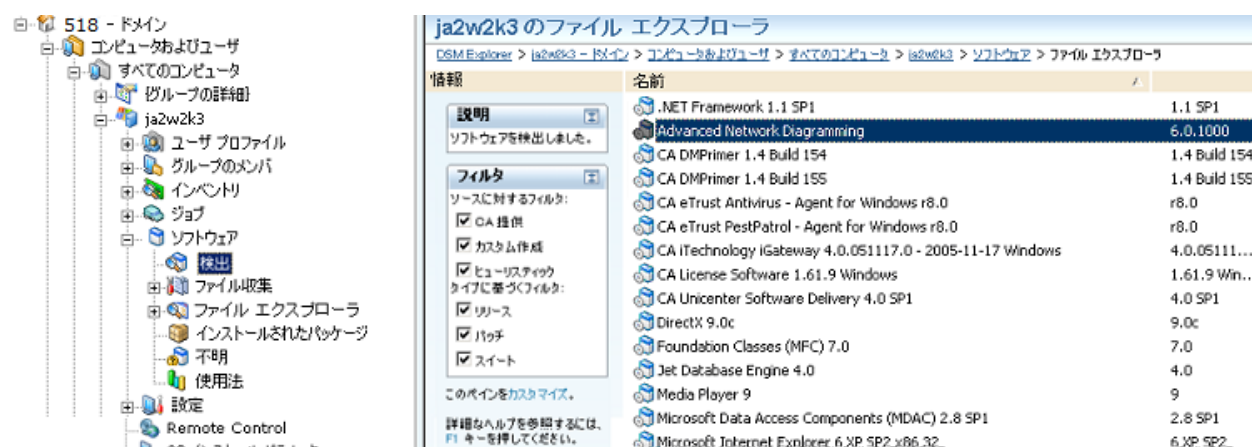
Software セクションには、ソフトウェア インベントリのエントリが含まれます。

ソフトウェア インベントリ ファイルは、より単純な形式に従っているため、グループは必要ありません。

注：GUID、Path、および Filename 値は必須ではありません。

```
<software>
 <package name="Advanced Network Diagramming">
 <attribute name="Ver">6.0.1000</attribute>
 <attribute name="Pub">Visio Corporation</attribute>
 <attribute name="Method">msi</attribute>
 <attribute name="GUID">{325C4969-4808-4A87-9547-F58620C444CA}</attribute>
 <attribute name="Path">C:\Program Files\ANP</attribute>
 <attribute name="Filename">ANP.exe</attribute>
 </package>
</software>
```

以下の図は、ソフトウェア インベントリ ファイル セクションが DSM エクスプローラでどのように表示されるかを示します。



## サンプル XIU ファイル

Asset Collector には、有効なグループおよび属性タグを持つサンプル XIU ファイルが含まれます。この XIU ファイルを変更してインベントリ値に使用できます。

サンプル XIU ファイルである SampleInventoryFile.xiu は、インストールパス¥bin フォルダにあります。



## 制限事項

このセクションでは、Asset Collector の制限事項について説明します。

### サポートされるプラットフォーム

Asset Collector は、Client Automation リリース 12.9 スケーラビリティ サーバがサポートされるすべてのプラットフォームでサポートされます (Linux と UNIX は除く)。

### WAC

ユーザ信頼レベルと発行元を使用したクエリと検索は実行できません。

## Client Automation に CA Mobile Device Management を統合する方法

### CA Mobile Device Management アセット情報用の CA Client Automation 統合

CA Client Automation はシームレスに CA Mobile Device Management (CA MDM) を統合し、そのデータベースに格納されたモバイルデバイスに関する情報を抽出します。MDM との統合により、IT 管理者にとって、あらゆるエンドポイント、およびエンタープライズ システムとサービスへのアクセスに使用されるアプリケーションの包括的な表示と収集が強化されます。統合では Android、BlackBerry、iOS、Windows Phone および従来型の Win 32 (ラップトップ/デスクトップ/サーバ) デバイスがサポートされます。

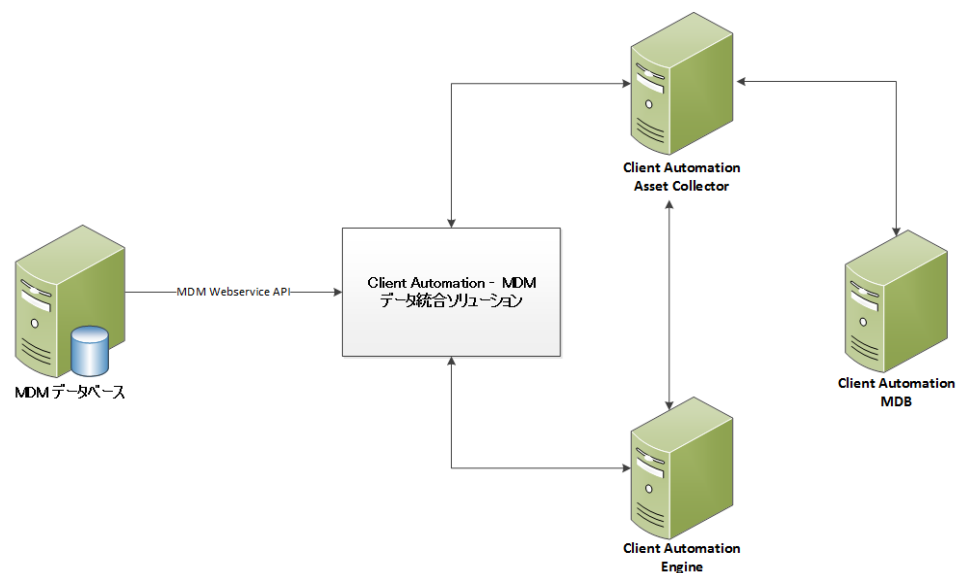
MDM 用の Client Automation 統合により、Client Automation が統合するその他の製品が MDM データにアクセスすることもできます。たとえば、CA Client Automation では、CA Service Desk Manager、CA IT Asset Management の製品が統合され、デフォルトでこれらの製品が MDM データにアクセスします。

セキュリティ制限により、MDM サーバでは、Software as a Service (SAAS) で有効になっている認証はサポートされません。このソリューションは、MDM サーバおよび Client Automation が両方とも同じネットワークにあるという前提でのみ使用できます。

## MDM 用の Client Automation 統合のしくみ

MDM 用の CA Client Automation 統合では、MDM サーバからアセット情報が収集されて、複数の XML ファイルへ変換されます。これらのファイルが CA Client Automation によって処理されると、MDM データベースからのアセットは、ネイティブ DSM エージェントによって検出されたアセットと共に検出されたハードウェアアセットとして CA MDB に表示されます。Client Automation は収集されたソフトウェアインベントリをヒューリスティックソフトウェアとして扱います。

以下の図は、MDM 用の Client Automation 統合がどのように動作するかを示しています。



MDM 用の Client Automation 統合に含まれるコンポーネントを以下に示します。

#### MDM サーバ

これは、CA Client Automation によって収集される MDM アセット情報が含まれる CA MDM サーバです。

#### MDM 用の Client Automation 統合

これは、MDM サーバに接続して、XML ファイルへの変換のためにアセットデータを収集する統合ソリューションです。

#### Client Automation Asset Collector

Asset Collector はインベントリ情報を抽出し、それをエンジンへ渡すために XML ファイルを処理します。

#### Client Automation エンジン

これは、MDM ソリューション用の Client Automation 統合を呼び出す Client Automation エンジンです。また、このエンジンは、Asset Collector から収集されたインベントリ情報を処理して、Client Automation MDB に挿入します。

#### Client Automation MDB

ネイティブ DSM エージェントによって収集されたインベントリ情報と共に、MDM アセット情報が含まれています。

## 前提条件および推奨事項

統合環境の設定のための前提条件を以下に示します。

1. エンジンがインストールされているコンピュータに **.Net Framework 4.5** 以上がインストールされていること。
2. **Asset Collector** が有効で実行中であることを検証して、確認します。 **Asset Collector** を有効にして起動するには、以下のコマンドを実行します。
  - a. `caf enable assetcollector`
  - b. `caf start assetcollector`
3. MDM サーバ名およびユーザ クレデンシャルを書き留めます。 **CA MDM** アセット統合エンジン タスクの作成中に指定されたユーザは、**MDM** サーバにアクセスできる必要があります。 **CA MDM** アセット統合エンジン タスクを作成します。
4. 生成されたアセット **XIU** ファイルに使用される出力フォルダまたはパスは、アセット ファイルを直接取り込む **Asset Collector** 用のパスとして設定できます。または、**Asset Collector** 用の既存のコレクタ フォルダに対して指定された出力パス値を設定できます。 リモートの **Asset Collector** が使用されている場合には、それはネットワーク パス（**UNC** パス）である可能性があります。詳細については、「**XIU\_Config\_Settings** ファイルのカスタマイズ」セクションを参照してください。
5. 高いディスク容量使用率、メモリの使用率、および **CPU** サイクルによるパフォーマンス低下およびその他のタスクへの影響を考慮して、**[CA MDM Asset Integration Engine のスケジューリングを常に実行]** タスクを使用しないことが推奨されます。

## CA MDM アセット統合エンジン タスクを作成する

CA MDM Asset 統合用に CA Client Automation を設定するには、まずエンジン タスクを作成する必要があります。

次の手順に従ってください：

1. DSM エクスプローラを開き、[コントロール パネル] - [エンジン] - [エンジン タスク] を選択します。
2. [情報] ペインの [タスク] エリアから [新規] を選択します。  
エンジン タスクの [新規タスク ウィザード] が表示されます。
3. [タスク タイプ] ドロップダウン リストから [CA MDM Asset 統合] を選択し、[次へ] をクリックします。
4. 現在のタスクに対して名前および説明を指定し、[次へ] をクリックします。  
注：名前は一意であることが必要で、空にすることはできません。説明はオプションです。
5. MDM アセット情報の抽出に使用される以下の MDM サーバの詳細を指定し、[次へ] をクリックします。

### サーバ

情報の抽出元の MDM サーバのホスト名またはアドレスを入力します。

### ユーザ名

MDM サーバに接続するユーザ名を入力します。

注：

CA MDM では、認証用に Active Directory やドメイン ユーザ クレデンシャルはサポートされていません。

### パスワード

MDM サーバへの接続時に使用するパスワードを入力します。

### テナント リストの取得

MDM サーバから使用可能なテナントのリストを取得します。

### テナント名

ドロップダウン リストからテナント名を選択します。有効なオプションには以下のものが含まれます。

### <テナント名>

対応するテナントの名前を指定します。

### すべて

リストのテナントをすべて指定します。

### テスト接続

現在指定されたサーバ詳細で MDM サーバへの接続確立が可能かどうかを判断します。

6. [スケジューリング] 画面で [スケジュールを設定します] をクリックして、スケジュール オプションを編集し、さらに指定された時間でタスクを実行します。

**デフォルト：** 日に 1 回実行

**重要：** 高いディスク容量使用率、メモリの使用率、および CPU サイクルによるパフォーマンス低下およびその他のタスクへの影響を考慮して、[常に実行] を使用しないことが推奨されます。

7. [完了] をクリックします。

作成されたタスクは、[すべてのエンジン タスク] ノード下でリスト表示されます。

## CA MDM アセット統合タスクをエンジンにリンクする

CA MDM Asset 統合タスクが作成されると、次に、実行されるためにエンジンまたはエンジン インスタンスにリンクする必要があります。

次の手順に従ってください：

タスクをエンジンにリンクするにはいくつかの方法があります。以下のいずれかを実行します。

- CA MDM アセット統合タスクを、DSM エクスプローラのツリー ビュー内の適切なエンジンにドラッグアンドドロップします。
- ツリー ビュー内でエンジンを選択し、[情報] ペインで [既存のタスクのリンク] をクリックします。次に、表示されるダイアログ ボックスで [CA MDM アセット統合] タスクを選択します。
- ツリー ビュー内でエンジンを選択し、[新規タスクの追加] をクリックします。[新規タスクの作成] ウィザードが表示されます。このウィザードでは、タスクの作成、設定、および関連付けのすべてを 1 ステップで実行することができます。

リンクされると、エンジンがタスクを実行し、次回にタスク リストに表示され、スケジューリング設定により実行が可能になります。

## CA MDM アセット統合タスクを表示して監視する

タスクのステータスは、エンジンのタスク リストに表示されます。指定可能な値は以下のとおりです。

### 待機中

エンジンはまだタスクを実行していません。

### アクティブ

タスクは現在実行中です。

### OK

タスクは実行されていて、「OK」ステータスが返されました。

### ERROR ( エラー )

タスクは実行されていて、「エラー」ステータスが返されました。

タスク リストには、タスクが最後に実行された時刻も表示されます。

MDM タスクの実行中、エンジン コンソールには対応するタスクのサマリが表示されます。MDM タスク サマリの例を以下に示します。

```
11/25/2014 2:45:12 AM
```

```
#=====
```

```
11/25/2014 2:45:12 AM Total MDM Assets Processed Failure : 0
```

```
11/25/2014 2:45:12 AM Total MDM Assets Processed Successfully: 15
```

```
11/25/2014 2:45:12 AM Total MDM Assets Processed: 15
```

```
11/25/2014 2:45:12 AM Total MDM Assets Found: 15
```

```
11/25/2014 2:45:12 AM Time taken in the process completion for XIU file
generation (in Seconds): 14
```

```
11/25/2014 2:45:12 AM Exits processing of MDM Assets, End Time:
```

```
11/25/2014 2:45:12 AM
```

```
11/25/2014 2:45:12 AM Start processing of MDM Assets, Start Time:
```

```
11/25/2014 2:44:57 AM
```

```
11/25/2014 2:45:12 AM #===== Summary Report
```

```
=====
```

```
11/25/2014 2:45:12 AM MDM Integration Task Executed Successfully
```

```
11/25/2014 2:44:57 AM Performing Job:MDM-Integration-Engine-Task1
```



CA MDB 内の CA MDM アセット情報

一旦 MDM アセット統合ソリューション用に Client Automation によって作成された XIU ファイルが CA Client Automation によって取り込まれると、それが表すコンピュータが、その他の検出されたハードウェア アセットと共に DSM エクスプローラの GUI に表示されます。

以下の図は、[エージェント ステータス] セクションに、デバイスにインストールされている DSM Asset Management エージェントがなく、デバイスの発行元が CA MDMであることを示しています。



## 診断と追跡

通常の DSM 追跡システムは、MDM アセット統合タスクの CA Client Automation 統合実行時の詳細情報を記録するのに使用します。使用されるトレース ファイルを以下に示します。

### TRC\_<エンジン名>

CA MDM アセット統合エンジン タスクに関連する、トレースする情報を含んでいます。ログ設定の詳細については、「[Client Automation general tracing and logging](#)」を参照してください。

### TRC\_MDM\_MDMDataln

MDM アセット情報ソリューション用の CA Client Automation 統合に関連するトレース情報を含んでいます。MDM 統合ソリューション ログ設定の詳細については、トピック「[Configuring Log File for CA MDM Asset Integration for Client Automation](#)」を参照してください。

アセットが DSM エクスプローラで使用可能ではないことが判明した場合は、その問題を識別するために以下のログ ファイルを参照します。

### TRC\_MDM\_MDMDataln

接続認証、デバイスアセットデータの収集、および XIU ファイル生成用の CA MDM 統合ソリューションに関連するトレース情報を含んでいます。

### TRC\_<linked task\_engine name>.log

CA MDM アセット統合エンジン タスクの実行に関連するトレース情報を含んでいます。

### TRC\_ASSETCOLLECTOR\_0.log

Asset Collector による処理用に生成された XIU ファイルに関連するトレース情報を含んでいます。

### TRC\_SYSTEMENGINE\_0.log

Asset Collector から収集されて MDB に挿入されるインベントリ情報を処理するシステム エンジンに関連するトレース情報を含んでいます。

## MDM 用の Client Automation 統合の設定

CA MDM アセット統合ソリューションには、CA MDM アセット統合エンジン タスクによって呼び出される MDM Asset Data をインポートするユーティリティが含まれています。このユーティリティは MDM Web サービス API を使用し、HTTP/HTTPS を使用して接続します。それは、MDM サーバからアセット データを取得し、Asset Collector 互換の XIU ファイルを生成して、設定された場所に置きます。デフォルトでは、設定ファイルは以下のパスで使用可能です。

CA¥DSM¥Bin¥resources¥config

MDM 用の Client Automation Integration は詳細に設定可能で、拡張可能です。新しいデバイス、スキーマ変更、インベントリ フィールドの追加と削除、ノード、テーブルおよびインベントリ マッピングの変更に対応するために、必要に応じて XML ファイルを設定し拡張できます。

アセット インベントリの生成に対して、MDM 用の Client Automation アセット統合が使用する XML ファイルのタイプを以下に示します。

### XIU\_Config\_Settings\_<Device>

各サポート対象デバイス タイプに対して、アセット XIU ファイルを処理し生成するための設定を含んでいます。

### MDM\_Config\_Settings

サポート対象 MDM デバイス、およびその他の設定ファイルに対する入力パスに関連する設定を含んでいます。

### <Device>\_DataKeySet

各サポート対象デバイス タイプに対して、MDM データベース スキーマに基づくデータ セット キー情報を含んでいます。

### XIU\_Schema\_<Device>

各サポート対象デバイス タイプに対して、MDM インベントリ項目および Client Automation インベントリ項目間のデータ マッピング情報を含んでいます。

**重要：** MDM\_Config\_Settings、<Device>\_DataKeySet、XIU\_Schema\_<Device> のファイルを変更するには、CA Client Automation および CA Mobile Device Management のデータ アーキテクチャの前提知識が必要です。これらのファイルを変更するのに必要な任意の追加のヘルプについては、CA サービスにお問い合わせください。

## MDM\_Config\_Settings ファイルをカスタマイズする

[MDM サーバ] からアセット収集用のデバイス タイプを設定するために MDM\_Config\_Settings ファイルを変更できます。

次の手順に従ってください：

デバイス タイプそれぞれの以下のコード行を検索し、パラメータ「enabled」を必要に応じて「true」または「false」に設定します。

```
<device type="<device number>" name="<device type>"
datakeyfilename="<device type>_DataKeySet.xml"
xiumappingfilename="XIU_Schema_<device type>.xml"
xiuconfigfilename="XIU_Config_Settings_<device type>.xml"
enabled="<true>"/>
```

```
enabled="<true>"
```

対応するデバイス用アセット インベントリのインポートを有効にします。

```
enabled="<false>"
```

対応するデバイス用アセット インベントリのインポートを無効にします。

## DataKeySet ファイルをカスタマイズする

サポート対象デバイスに基づいて、以下の DataKeySet ファイルを検出できます。

- Android\_DataKeySet
- BlackBerry\_DataKeySet
- ios\_DataKeySet
- Win32\_DataKeySet
- WinPhone\_DataKeySet

## XIU\_Schema ファイルをカスタマイズする

サポート対象デバイスに基づいて、次の XIU Schema マッピング ファイルを検出できます： XIU\_Schema\_Android

- XIU\_Schema\_BlackBerry
- XIU\_Schema\_ios
- XIU\_Schema\_Win32
- XIU\_Schema\_WinPhone

## XIU\_Config\_Settings ファイルをカスタマイズする

ユーザの環境設定に基づいたインベントリ収集のカスタマイズに推奨される一般設定を設定するために、各デバイス タイプに対して XIU\_Config\_Setting ファイルを変更できます。サポート対象デバイスに基づいて、以下の XIU Configuration Settings ファイルを検出できます。

- XIU\_Config\_Settings
- XIU\_Config\_Settings\_Android
- XIU\_Config\_Settings\_BlackBerry
- XIU\_Config\_Settings\_Ios
- XIU\_Config\_Settings\_Win32
- XIU\_Config\_Settings\_WinPhone

各デバイス タイプに対して、以下の設定を必要に応じて設定できます。

### <output-settings>

生成されたアセット XIU ファイル用の出力設定を含んでいます。

#### output-path value

生成されたアセット XIU ファイルに使用される出力フォルダまたはパスを指定します

**デフォルト：** C:¥Import¥MDM¥Data¥

アセット ファイルを直接取り込む Asset Collector 用のパスを設定できます。または、Asset Collector 用の既存のコレクタ フォルダに対する出力パス値を設定できます。

**注：** Windows ネットワーク パス（UNC パス）もサポートします。たとえば、¥¥<hostname or IP>¥Import¥MDM¥Data¥

#### output-filename value

生成されたアセット XIU ファイルの名前を指定します。ファイルに名前を付けるためにデフォルト値を任意の値に置換できます。

**デフォルト：** Asset

#### output-filename host\_key

生成された XIU ファイル名に対して、付加する値を指定します。True は指定された値を付加することを示し、False はどんな値も追加しないことを示します。

**デフォルト：** True

例：

- この値が「True」に設定される場合、ファイル名は Asset\_<host\_key>.xiu にでき、ここで <host\_key> は対応するデバイスの一意の識別子です。
- この値が「False」に設定される場合、ファイル名は Asset.xiu にできます。

#### multi-tenant-support enabled

マルチテナントサポートが有効かどうかを指定します。「True」は有効であることを示し、「False」は無効であることを示します。

デフォルト： オフ

この値を「True」に設定すると、生成されたアセット XIU ファイルは、出力パス値で設定されるテナントの特定のフォルダに配置されます。テナントフォルダが存在しない場合、新しいフォルダが作成されます。

例：

- テナントが ABC で、値が「True」に設定され、出力パスが C:¥Import¥MDM¥Data¥ である場合、新しいフォルダ ABC が作成され、アセット XIU ファイルはパス C:¥Import¥MDM¥Data¥ABC 下の ABC フォルダに配置されます。
- テナントが ABC で、値が「True」に設定され、出力パスが C:¥Import¥MDM¥Data¥XXX である場合、アセット XIU ファイルは XXX フォルダに配置されます。

#### <processing-info>

生成されたアセット XIU ファイル用の処理設定を含んでいます。

#### origin value

収集されたアセットの発行元を指定します。

デフォルト： CA MDM

#### trust-level

アセットの信頼レベルを指定します。信頼レベルは、1 から 5 までの範囲で示され、5 が最も信頼性が高いことを示しています。

デフォルト： 4

## MDM 用の Client Automation 統合用ログ ファイルの設定

MDM 用の Client Automation 統合は Apache log4net をログ記録機能に使用します。ログ レベル、ログ ファイル バックアップの最大数、最大ファイル サイズなど共通のログ ファイル生成設定用の MDMDatIn\_Log4net.config ファイルを設定できます。

- MDMDatIn\_Log4net.config ファイル用のデフォルト パスは CA¥DSM¥Bin です。
- デフォルトでは、生成されるログ ファイル名は、パス CA¥DSM¥logs¥TRC\_MDM\_MDMDatIn.log 下の TRC\_MDM\_MDMDatIn.log です
- 複数のログ ファイルがある場合、ファイル名に増分の数が付加されます。  
たとえば TRC\_MDM\_MDMDatIn.log、TRC\_MDM\_MDMDatIn.log.1、TRC\_MDM\_MDMDatIn.log.2 など。

MDMDatIn\_Log4net.config ファイルの例を以下に示します。

```
<?xml version="1.0" encoding="utf-8" ?>
<log4net>
<root>
<!--
OFF - 何もログ記録されない (コールできない)
 FATAL (致命的)
 ERROR (エラー)
 WARN (警告)
 INFO (情報)
 DEBUG (デバッグ)
 ALL - すべてがログ記録される (コールできない)
-->
<level value="Error" />
<appender-ref ref="LogFileAppender" />
</root>
<appender name="LogFileAppender" type="log4net.Appender.RollingFileAppender" >
 <file value="../logs/TRC_MDM_MDMDatIn.log"/>
 <appendToFile value="true" />
 <rollingStyle value="Size" />
 <maxSizeRollBackups value="10" />
 <maximumFileSize value="5MB" />
 <staticLogFileName value="true" />
 <layout type="log4net.Layout.PatternLayout">
 <conversionPattern value="%date [%thread] %level %logger
- %message%newline%exception" />
 </layout>
</appender>
</log4net>
```

## 既知の問題およびトラブルシューティング

### CA MDM アセット統合エンジン タスクはステータスをエラーとして表示します

#### 症状

CA MDM アセット統合エンジン タスクを実行すると、エンジン タスクはステータスをエラーとして表示し、アセット情報は収集されません。

#### 解決方法

MDM サーバおよびエンジン実行中のサーバ間の時間差が 5 分を超えている場合、これが発生する可能性があります。2 台のコンピュータ間の時間差が 5 分未満であることを確認します。



## エージェントブリッジ

エージェントブリッジは、**Client Automation** の現在のバージョンに基づいて、拡張エージェントおよびレガシー エージェントの下位互換性を提供する **Client Automation** の機能拡張です。モバイル エージェントから取得した情報を収集して、ジョブ、モジュール、テンプレート、および設定をそれらのエージェントに配信することができます。

**注：** エージェントブリッジは、**Microsoft Windows** のみでサポートされています。

**注：** 本リリースでエージェントブリッジによってサポートされるエージェントプラットフォームは、**Windows Mobile 6.1**（ARM ベース、**StrongARM**、**XScale** を含む）、**Windows Mobile 6**（**Classic**、**Standard**、**Professional**）（ARM ベース、**StrongARM**、**XScale**、**TI OMAP** を含む）、**Windows Mobile 5**（ARM ベース、**StrongARM**、**XScale** を含む）です。

### 主要なコンポーネント

エージェントブリッジは、以下のコンポーネントで構成されています。

- **共通レガシー サーバ コンポーネントとそのプロセス コンポーネント**  
エージェントブリッジ用の通信、設定、およびエージェント登録を扱います。
- **Asset Management コンポーネント**  
アセット管理の拡張エージェントおよびレガシー エージェントのサーバサポートを提供します。
- **Software Delivery コンポーネント**  
ソフトウェア配信の拡張エージェントおよびレガシー エージェントのサーバサポートを提供します。

**注：** 同じマシンにインストールされた **Asset Management** エージェントおよび **Software Delivery** のレガシー エージェントは、エージェントブリッジを有効にした同じ **Client Automation** リリース 12.9 スケーラビリティ サーバに向ける必要があります。

## エージェントブリッジの UUID 生成

UUID がレポートされていない場合、UUID 生成では、エージェントブリッジでレガシーエージェントのエージェント UUID を生成することができます。さらに、UUID 生成動作を制御するために新しい設定ポリシーが追加されました。

注：常にご使用の動作環境に可能な最新のエージェントを使用してください。レガシーエージェントの認定ステータスを確認するには、「CA Support Online」Web サイト (<http://support.ca.com>) にある適切な互換性マトリックスを参照してください。

## 制限事項

CA Client Automation の現在のリリースは新型のアセット管理、ソフトウェア配信、およびリモート制御です。そのため、これらのコンポーネントの旧バージョンに存在しない新しい機能のいくつかは、レガシーエージェントでは機能しません。エージェントブリッジのサポート対象には、以下の Client Automation リリース 12.9 DSM 機能は含まれません。

- アセット ジョブ確認
- パフォーマンス モジュール抽出
- 設定ポリシー

注：[設定ポリシー] ツリー ノードはレガシーエージェントでは非表示になっており、[ジョブ確認のアクティブ化] オプションもレガシーエージェントでは無効になっています。

- インスタント診断
- DMDeploy 機能
- シグネチャに基づくソフトウェア ファイル スキャン

このリリースの Client Automation における技術の変更により、既存の Unicenter Asset Management 4.0 および Unicenter Software Delivery 4.0 の機能のいくつかは、エージェントブリッジを使用した Client Automation のこのリリースのレガシーエージェントではサポートされていません。このようなサポートされていない機能を以下に示します。

- アセット管理レガシーエージェント用のオンライン メータリング

注：ただし、オフライン メータリングはサポートされています。

- アプリケーション定義に基づくソフトウェア ファイル スキャン

- Unicenter Asset Management 4.0 および Unicenter Software Delivery 4.0 レガシー エージェントに基づくドッキング デバイス
- ソフトウェア配信レガシー エージェント用のソフトウェア カタログ
- ソフトウェア配信レガシー エージェントの自動インストール

Windows Mobile エージェントをサポートしているため、エージェントブリッジは書式設定済みレガシー データ ファイルを読み取り、**DSM** エンジンにより収集される **Client Automation** リリース **12.9** の書式設定済みデータ インベントリ ファイルへ変換します。このコンポーネントでは、できるだけ多くのデータが変換されます。その結果、一般インベントリのような複製サブノードの一部は、多様な動作環境と、レガシー エージェントの異なるバージョン間でかすかな違いがあるために、**DSM** エクスプローラに表示される場合があります。また、「シリアル番号」、「アセット タグ」、「ディスクのシリアル番号」のような一部のプロパティは、一部のコンピュータの「コンピュータ プロパティ」ノードの下では空になります。これは、これらのアセットがレガシー システムでは収集されないためです。

## 既知の問題

現在は、エージェントブリッジでは以下の問題が確認されています。

### ジョブ確認のアクティブ化

**Software Delivery** レガシー エージェントでのジョブ確認のアクティブ化は、以下の状況で失敗することがあります。

1. パッケージの展開中に、[スケーラビリティ サーバでジョブをトリガする] オプションが選択されていない。
2. ジョブ コンテナが作成されて「アクティブ」状態になったとき、[ジョブ確認のアクティブ化] オプションを **DSM** エクスプローラで選択するか、**sdacmd jobcheck** をエージェント マシンで実行する。

結果は、ジョブのステータスが「アクティブ」状態のままになります。

この問題を回避するには、**Unicenter Software Delivery 4.0** エージェント マシンで **sdjexec.exe** を実行します。ジョブのステータスは、**DSM** エクスプローラで成功として表示されます。

### Windows Mobile 5.0 デバイス

エージェントブリッジをポイントしている Windows Mobile 5.0 デバイスで Unicenter Asset Management 4.0 SP1 C2 エージェントを最初にインストールして、その後に Unicenter Software Delivery 4.0 SP1 C3 エージェントをインストールすると、DSM エクスプローラに表示される Unicenter Asset Management エージェントのバージョン番号が正しくない場合があります。

また、エージェントブリッジをポイントしている Windows Mobile 5.0 デバイスで Unicenter Software Delivery 4.0 SP1 C3 エージェントを最初にインストールし、その後に Unicenter Asset Management 4.0 SP1 C2 エージェントをインストールすると、Unicenter Asset Management 4.0 SP1 C2 エージェントがレポートされない場合があります。

注：診断ヒントの詳細は、「トラブルシューティング」の章を参照してください。

## エージェント登録

Client Automation エージェントは、次の情報を指定して MDB に登録します。

- ホスト名
- UUID (Host Universal Unique Identifier)
- オペレーティング システム クラス ID
- IP アドレス
- MAC アドレス
- 使用法リスト文字列

エージェントブリッジにより、ホスト UUID がレガシー エージェントにより指定され、レガシー エージェントはエージェントブリッジを使用して Client Automation システムに登録されます。Client Automation およびエージェントブリッジが使用するエージェント登録方法は、レガシー情報を Client Automation のレガシー情報とマップします。たとえば、アセット管理 8 バイト ファイル ID は、Client Automation の書式設定済 32 バイトの英数字ホスト UUID にマップされます。レガシー エージェントに生成されるホスト UUID は、アセット管理とアセット管理エージェントの両方で共通であり、共通の使用法ファイルに保管されます。

レガシー エージェントが一意的ホスト UUID を指定せず、UUID 生成が有効でない場合、このエージェントはエージェントブリッジにより登録されず、無効なエージェントとして扱われます。

UUID 生成が有効な場合、アセット管理およびソフトウェア配信レガシー エージェントを登録するための正しい手順は次のようになります。

レガシー エージェントを登録するために、これらのエージェントのいくつかは自身の UUID をレポートしない場合がある

- アセット管理エージェントとソフトウェア配信エージェントの両方がホスト UUID をレポートしない場合、アセット管理エージェントとソフトウェア配信エージェントを任意の順序で登録できます。しかし、2つのエージェントの登録と登録の間に、通常それぞれ5分以上待つ必要があります。
- アセット管理エージェントがホスト UUID をレポートしないのに、ソフトウェア配信エージェントがレポートする場合は、常にソフトウェア配信エージェントを先に登録する必要があります。それから、5分後にアセット管理エージェントを登録します。
- ソフトウェア配信エージェントがホスト UUID をレポートしないのにアセット管理エージェントがレポートする場合は、常にアセット管理エージェントを先に登録する必要があります。それから5分後に、ソフトウェア配信エージェントを登録します。

一般に、大部分の Unicenter Asset Management 4.0 エージェントおよび Unicenter Software Delivery 4.0 エージェントは、サーバに登録するときにホスト UUID をレポートします。

#### **Asset Management エージェント**

すべてのレガシーな Unicenter Asset Management 4.0 エージェントの登録は、Client Automation のエージェントブリッジによりサポートされています。

モバイル PDA エージェントでは、エージェントブリッジと連動する前にパッチ (T434066) の適用が必要になります。このパッチも、CA オンラインサポート (<http://ca.com/support>) で入手できます。

#### **Software Delivery エージェント**

レガシーの Unicenter Software Delivery 4.0 エージェントの登録は、Client Automation およびエージェントブリッジが使用するエージェント登録方法でサポートされています。

### 移行に関する注意事項

エージェントブリッジを使用してレガシー エージェントを現在のリリースの **Client Automation** に移行する場合、以下の制限事項に留意してください。

- 移行したエージェントが「クラッシュ後の再インストール」(RAC)を実行した後で、同じエージェントの新しい移行によって、既存のエージェントが更新されるのではなく新しいユニットが作成されます。
- 移行した **Software Delivery** レガシー エージェントがすでに **Client Automation** リリース 12.9 環境内にある場合、**Unicenter Asset Management 4.0** レガシー エージェントまたは **Client Automation** リリース 12.9 **Asset Management** エージェントをインストールすることにより、移行した **Software Delivery** レガシー エージェントのステータスが上書きされます。SD ステータスは「移行操作によりロック」から「未インストール」に変わります。そのため、この方法を使用してレガシー エージェント データを移行および登録しないでください。代わりに、**DSM** 移行ツールを使用してください。

注：DSM 移行ツールの詳細については、「**実装ガイド**」を参照してください。

### AM エージェントブリッジ

**Asset Management** エージェント (AM エージェントブリッジ) 用のエージェントブリッジ レガシー セクタ サーバのサポートは自己完結型モジュール **amLrss.exe** であり、**Client Automation Asset Management** スケーラビリティ サーバの一部です。ポリシーで設定可能であり、**Client Automation Common Application Framework** (CAF) サービスの一部として開始および停止することができます。

AM エージェントブリッジには、アセット管理スケーラビリティ サーバの一部である次のモジュールも含まれています。

- モバイル セクタ サーバ (amss.exe)  
レガシー セクタ サーバとモバイル PDA エージェント間の通信を管理します。このプロセスは **amLrss** レガシー セクタ サーバの起動時に開始し、**amLrss** が停止すると停止します。
- ブリッジ変換モジュール (amBridge.exe)  
レガシー セクタ サーバデータベースと **Client Automation** リリース 12.9 セクタ データベースの間でデータを変換します。このプロセスはスケジュールされた間隔で **amLrss** により開始されます。この間隔はポリシー別に設定可能です。

## サポートされている動作環境と Asset Management エージェント

Client Automation メディアには、Windows Mobile 5.0、6.0 および 6.1 用のエージェントが含まれます。このエージェントでは、レガシーエージェントブリッジを使用する必要があります。その他のエージェントでは、レガシーエージェントブリッジはサポートされていません。

注：常にご使用の動作環境で可能な最新のアセット管理エージェントを使用してください。最新のバージョンがあるか確認するには、CA サポート オンライン Web サイト (<http://support.ca.com>) にあるアセット管理の互換性マトリックスを参照してください。

## ローカルおよびドメイン ユーザ

「レガシー ユーザ サポートを有効にする」設定ポリシーが有効の場合、エージェントブリッジは Unicenter Asset Management 4.0 での操作と同じようにレガシー ユーザ アカウントを操作します。つまり、ローカル ユーザとドメイン ユーザに違いはなく、ユーザのアカウントに関するドメイン情報は Client Automation リリース 12.8 に渡されません。ただし、接頭辞 LEGACY\_USER\_ACCOUNT が、すべてのアセット管理レガシー ユーザのアカウントのドメイン名として使用されます。

## 設定

設定ポリシーを使用して AM エージェントブリッジをレガシー エージェント用に設定できます。アセット管理ポリシー グループ フォルダおよびポリシーは、[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] - [スケーラビリティ サーバ] サブノードの下にあります。

さらに、下位互換性フォルダとポリシーは、[設定ポリシー] - [デフォルトのコンピュータ ポリシー] - [DSM] - [スケーラビリティ サーバ] 共通サーバ サブノードにあります。

注：AM エージェントブリッジ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」を参照してください。

### AM エージェントブリッジのイベントメッセージ

以下は、AM エージェントブリッジ イベントメッセージです。

- 「AM エージェントブリッジの設定が変わりました。」

注：設定ポリシーがユーザにより変更されると、イベントメッセージが OS イベントログと DSM イベントログの両方に送信されます。

- 「AM エージェントブリッジは正常に起動しました。」
- 「AM エージェントブリッジが正常に停止しました。」
- 「AM エージェントブリッジが起動に失敗しました。」
- 「AM エージェントブリッジが停止に失敗しました。」

### レガシーデータの収集方法

ソフトウェアおよびハードウェアのインベントリデータは、インベントリ モジュールと収集タスクを使用して収集されます。

以下に示すのは、関連するレガシー エージェントのインベントリ データを収集する方法です。

- **Unicenter Asset Management 4.0 拡張エージェントとレガシー エージェント**  
Unicenter Asset Management 4.0 拡張エージェントとレガシー エージェントの場合、DSM エクスプローラ内の既存の **Client Automation** インベントリ モジュールを使用できます。

### インベントリ検出モジュール

既存の **Client Automation** リリース 12.9 エンジン インベントリ検出モジュールを使用し、レガシー エージェント インベントリ ファイルの内容を収集できます。結果は、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] - [追加] の下に表示されます。「追加ノード」は動的であり、登録されているレガシー エージェントのタイプに応じて、一般インベントリ、ハードウェア、シリアル番号およびモデル (WMI)、サービス、ソフトウェア インベントリ、**Software Delivery** 情報、ユーザ インベントリ、ユーザ情報、ユーザ テンプレート、および **WBEM** インベントリのサブノードのいずれかまたはすべてを含むことがあります。

エージェントブリッジは **Unicenter Asset Management 4.0** の書式設定済データ ファイルを読み取り、DSM エンジンにより収集される **Client Automation** リリース 12.9 の書式設定済データ インベントリへ変換します。



## 既存のインベントリ モジュールを使用する

Client Automation リリース 12.9 システムと Unicenter Asset Management 4.0 システムの検出モジュールを以下の表に示します。Client Automation リリース 12.9 モジュール名は、エージェントブリッジ変換モジュールを使用して Unicenter Asset Management 4.0 モジュール名に変換されます。

| インベントリ モジュール名                    | 目的 | OS 名             | Client Automation リリース 12.8 名 | UAM 4.0 名   |
|----------------------------------|----|------------------|-------------------------------|-------------|
| General Inventory Advanced (4.0) |    | Windows 95/98/Me | amadvinv9x.exe                | IG40W95.EXE |
|                                  |    | Windows CE       | N/A                           | IG40WCE.EXE |

デフォルトでは、Client Automation リリース 12.8 の一般インベントリ モジュールは、Unicenter Asset Management 4.0 フォーマットに変換されます。

## インベントリ モジュールを作成する

Unicenter Asset Management 4.0 レガシー エージェント用のインベントリ検出モジュールを DSM エクスプローラを使用して作成し、レガシー エージェントに配信することができます。

以下の表にあるインベントリ モジュールはレガシー エージェントのみに固有のものであり、Client Automation リリース 12.8 DSM エージェントには適用されません。

| インベントリ モジュール名                  | 目的    | OS 名             | UAM 4.0/3.2 名 |
|--------------------------------|-------|------------------|---------------|
| General Inventory (3.2 エージェント) | OS 固有 | Windows 95/98/Me | IGENW95.EXE   |
|                                |       | Windows CE       | IGENWCE.EXE   |

### オフライン メータリング

オフライン メータリング (Client Automation リリース 12.8 での名前はオフラインのソフトウェア使用状況) は、レガシーエージェントの場合のみエージェントブリッジでレポートできます。この機能により Client Automation は、既存のソフトウェア パッケージおよびアプリケーション、またはユーザ定義ソフトウェアを使用して、アプリケーションを監視しできます。

ユーザ定義ソフトウェアの場合、オフライン メータリング機能は Unicenter Asset Management 4.0 の場合と同じです。バージョンおよびモジュール情報を含む新しいソフトウェア パッケージを定義し、使用方法是監視されるレガシー エージェントに渡されます。メータリング インベントリ ファイルはエージェントブリッジにより収集され、ユーザ定義ソフトウェアの使用状況は DSM エクスプローラで見ることができます。

Client Automation リリース 12.8 のシグネチャ スキャン情報に基づく既存のソフトウェア パッケージおよびアプリケーションでは、レガシー エージェントはバージョン情報を一致させずにソフトウェアを監視します。これは、DSM エクスプローラのソフトウェア リストから特定のバージョン番号のソフトウェア パッケージを選択すると、レガシー エージェントにより検出されたソフトウェア使用状況は、選択した「ソフトウェア使用状況」モジュールにより定義されたバージョンと正確に一致しないことを意味します。

たとえば、Adobe Acrobat 5.0 x86 32 EN をオフライン ソフトウェア使用状況監視に選択すると、レガシー エージェントは、指定されたバージョン番号に関わらず、任意のバージョンの Adobe Acrobat の使用状況データを返します。この理由は、レガシー エージェントにバージョン検出機能がないためです。

### SD エージェントブリッジ

ソフトウェア配信エージェント (SD エージェントブリッジ) については、*「Software Delivery 管理者ガイド」* を参照してください。

## Intel AMT と CA ITCM を統合する

CA ITCM 用の Intel® Active Management Technology (Intel AMT) 機能により、Intel AMT 対応のアセットを DSM Explorer ユーザ インターフェースから管理できます。この機能は、DSM エクスプローラでの Intel AMT アセットの統合と使用状況に対応します。この機能を使用して、以下のタスクを実行することができます。

- DSM エクスプローラ ユーザ インターフェースで統合ポイントを作成することにより、Intel AMT アセットへのアクセスを可能にします
- Intel AMT アセットのポリシーベースの管理を提供します。
- 様々な Intel AMT コマンドを使用して、Intel AMT アセットで様々なアクションを制御および実行します。

## Intel AMT アセットの設定

Intel AMT アセットで Intel AMT コマンドを実行する前に、Intel AMT アセットを設定する必要があります。Intel AMT アセットを設定するには、Intel AMT コマンドをアセットが実行する準備が整うように、DSM ドメイン マネージャから Intel AMT アセットをプロビジョニングする必要があります。

注：DSM ドメイン マネージャからアセットをプロビジョニングしないと、アセットは Intel AMT コマンドを実行しません。

DSM ドメイン マネージャを使用すると、C:\Program Files\CA\SC\ConstantAccess\caprovision.exe にプロビジョニング ツールキットがインストールされます。Intel AMT アセットをプロビジョニングするには、ドメイン マネージャから caprovision.exe ファイルを使用します。

## caprovision.exe の実行

Intel AMT アセットで何らかのアクションを実行する前に、caprovision.exe (caprovision provision *hostname adminusername adminpasswd userid userpasswd*) を実行します。

caprovision.exe ファイルを実行するには、以下のコマンドを実行します。

```
caprovision -c command -h hostname -os hostOSName -u adminUser -p adminPassword
[-usern userName] [-userP userPassword] [-certn certificateName] [-certP
certificatePassword] [-i]
```

### -c *command*

実行される Intel AMT アセットの動作を定義します。サポートされている動作/コマンドは、**provision**、**unprovision**、**getprovisioneddata**、**isdeviceprovisioned** です。-i オプションが使用されていない場合のみ、必須です。**provision** オプションにより、デバイスでさまざまなコマンドを使用することができるようになります。つまり、AMT デバイスメモリのユーザ、パスワード、およびタグが設定されます。**unprovision** オプションは、デバイスのプロビジョニング状態を解除します。つまり、ユーザ、パスワード、およびタグをデバイスメモリから削除します。**getprovisioneddata** オプションにより、指定したデバイスのプロビジョニングデータが一覧表示されます。**isdeviceprovisioned** オプションは、指定したデバイスがプロビジョニングされた場合に、それについて通知します。

### -h *hostname*

Intel AMT アセットのホスト名を定義します。-i オプションが使用されていない場合のみ、必須です。

### -u *adminUser*

管理者のユーザ名を定義します。-i オプションが使用されていない場合のみ、必須です。

### -p *adminPassword*

管理者のパスワードを定義します。-i オプションが使用されていない場合のみ、必須です。

**-os *hostOSName***

Intel AMT アセットのオペレーティング システムの名前を定義します。  
-i オプションが使用されていない場合のみ、必須です。

**-usern *userName***

新規ユーザの名前を定義します。このオプションが使用されておらず、  
-i オプションが指定されていない場合、ユーザ名はランダムに生成されます。

**-userp *userPassword***

新規ユーザのパスワードを定義します。このオプションが使用されておらず、  
-i オプションが指定されていない場合、ランダムなパスワードが自動的に生成されます。

**-i**

インタラクティブ モードを定義します。また、コマンドラインで指定されなかったパラメータをユーザに要求します。

## Intel AMT アセット設定の検証

Intel AMT アセットを設定した後に、アセットが適切に設定されたかどうかを確認できます。

### Intel AMT アセット設定を検証する方法

1. 以下の URL を使用して、ポート番号 16992 で Intel AMT アセットを参照します。

`http://<hostname>:16992`

ログイン ページが表示されます。

2. 有効なユーザ クレデンシャルを入力します。

ユーザ クレデンシャルが有効で、アセットが適切に設定されると、Intel AMT アセットの詳細を含む [インデックス] ページが表示されます。

これで、DSM エクスプローラを使用して、Intel AMT アセットでさまざまな操作を実行できるようになりました。

## Intel AMT のステータス

CA ITCM では、Intel AMT のステータスは Intel AMT アセットの様々な状態で表されます。次の表では、Intel AMT のステータスに有効なすべてのオプションを記載しています。

| 状態          | 説明                                                                                  |
|-------------|-------------------------------------------------------------------------------------|
| 不明          | CA ITCM は、現在このアセットの Intel AMT ステータスを把握していません。リフレッシュアイコンをクリックして、実際の状態を問い合わせる必要があります。 |
| サポートされていません | アセットには Intel AMT チップセットがなく、Intel AMT もサポートしていません。                                   |
| 未プロビジョニング   | アセットには Intel AMT チップセットがありますが、現在は Intel AMT により管理されるようにプロビジョニングされていません。             |
| 無効          | アセットには Intel AMT チップセットがありますが、Intel AMT による管理は有効ではありません。                            |
| 有効          | アセットには Intel AMT チップセットがあり、Intel AMT による管理が有効です。                                    |
| 隔離済み        | アセットには Intel AMT チップセットがあり、現在隔離されています。DSM を除くすべてのネットワーク トラフィックはブロックされます。            |

## Intel AMT アセットのステータスを表示する

Intel AMT アセットのステータスを、ステータス ポートレットの下の [エージェント ステータス] セクションで表示します。アセットのステータスを解析した後で適切な措置をとることができます。

### Intel AMT アセットのステータスを表示する方法

1. [ドメイン] - [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] に移動します。  
[ホームページ] タブが表示されます。
2. ステータス ポートレットの下の [エージェント ステータス] セクションに移動します。
3. 以下の図に示すように、AMT ステータスの値を見て、Intel AMT アセットのステータスを確認します。

| ステータス                       |                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------|
| <b>違反したポリシー (0)</b>         |                                                                                           |
| なし                          |                                                                                           |
| <b>失敗したジョブ (0)</b>          |                                                                                           |
| なし                          |                                                                                           |
| <b>実行が回避されたアプリケーション (0)</b> |                                                                                           |
| なし                          |                                                                                           |
| <b>エージェント ステータス (8)</b>     |                                                                                           |
| AMT ステータス                   | 隔離済み  |
| AM ステータス                    | 操作可能                                                                                      |
| エージェント制限                    | なし                                                                                        |
| 信頼レベル                       | .....                                                                                     |
| 発行元                         | CA                                                                                        |

注：デフォルトでは、ステータスは「不明」です。「AMT ステータス」値の横のリフレッシュアイコンをクリックして、Intel AMT アセットの現在のステータスを表示してください。

## Intel AMT アセットを参照する

Intel AMT アセットを参照してインベントリ情報を見ることができます。ただし、アセットのリモート（読み取り専用）ステータスのみが有効です。

### Intel AMT アセットを参照する方法

1. [コンピュータおよびユーザ] - [すべてのコンピュータ] - コンピュータに移動します。

[ホームページ] タブが表示されます。

2. [AMT ブラウザ] タブをクリックします。

注：このタブを選択できるのは、Intel AMT がアセット上で有効な場合のみです。

[ログ オン] ページが表示されます。

3. [ログ オン] ボタンをクリックして、ユーザ クレデンシャルを入力します。

[システム ステータス] ページが表示されて、IP アドレス、システム ID などの情報が表示されます。





注：左ペインのリンクをクリックすると、それに対応する情報が表示されます。

## Intel AMT アセットを隔離する

Intel AMT 対応アセットが隔離モードに入ると、Intel AMT アセット上の着信および発信ネットワーク トラフィックにポリシーを強制するフィルタが適用されます。隔離モードに入る Intel AMT アセットは、AMT ポートと DSM ポートだけがオープンになるため、あらゆるユーザ、アプリケーション、インターネット アプリケーションでネットワーク アクセスが禁止されます。ただし、DSM 管理者はエージェントを遂行して、Intel AMT アセットの DSM 関連の管理を実行できます。

### Intel AMT アセットを隔離する方法

1. [ドメイン] - [コンピュータおよびユーザ] - [すべてのコンピュータ] - コンピュータに移動します。

[ホームページ] タブが表示されます。

2. クイック起動ポートレットに移動します。

3. [アクション] セクションの下に [アセットの隔離] リンクをクリックします。

注：[アセットの隔離] リンクを選択できるのは、Intel AMT がアセット上で有効な場合のみです。

確認メッセージが表示されます。

4. [はい] をクリックします。

以下の図に示すように、Intel AMT アセットが正常に隔離されます。

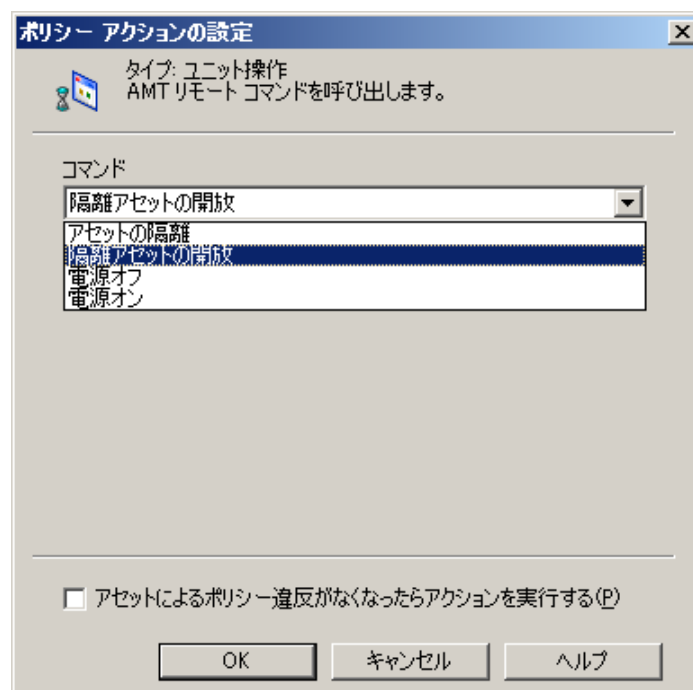


Intel AMT アセットが正常に隔離された後で、[アセットの隔離] リンクが [隔離アセットの開放] リンクに変わります。Intel AMT アセットを隔離から開放したい場合は、[隔離アセットの開放] リンクをクリックします。

## AMT コマンド ポリシー アクションを使用する

Intel AMT アセットを管理するためのポリシーを作成できます。ポリシーを作成している間、AMT コマンド ポリシー アクションを使用して、Intel AMT コマンドを Intel AMT アセット上で実行します。このポリシーに違反すると、指定されたコマンドが Intel AMT アセット上で実行されます。

以下の図は、利用可能な Intel AMT リモート コマンドを示します。



注：AMT コマンド ポリシー アクションの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

## 仮想ホスト

**Client Automation** は、プラットフォーム仮想化をサポートします。これは、コンピュータまたはオペレーティング システムのカプセル化で、そこでは、その物理特性がユーザから隠され、実行時にコンピュータ プラットフォームがエミュレートされます。

以前のリリースでは、パーティション化された **UNIX** サーバエージェントによってサポートが提供されました。このリリースでは、パーティション化された **UNIX** サーバエージェントの機能が新しい **AM** リモート エージェントに完全に統合されました。また、このエージェントは、**DSM** エクスプローラからのみ仮想ホストの情報を収集するように設定できます。

**AM** リモート エージェントは、仮想ホスト コンピュータおよびプラットフォーム上で稼働し、以下のタスクを実行します。

- 仮想ホスト インベントリ収集タスクの実行 この収集タスクは、**DSM** エクスプローラのインベントリ ツリーを生成するインベントリ ファイルを作成します。
- 仮想ホスト コンピュータをアセット管理ユニットとして登録
- それぞれの仮想ホスト コンピュータとそのホストに含まれるすべての管理対象ゲスト コンピュータとの関係を保持します。

収集された情報は、**DSM** エクスプローラのインベントリ ツリーに表示され、仮想ホストの特定のプロパティを反映します。 **HP**、**IBM**、**Sun**、および **VMware ESX** のサーバは、コンピュータ ユニットとして表示されます。それぞれの管理対象ゲスト コンピュータに対するコンピュータ ユニットが表示されます。

仮想ホストとその仮想ホストに関連する管理対象ゲスト コンピュータは、関連するコンピュータとして報告され、双方の間を簡単に移動できます。

追加の **AM** リモート エージェントは、**AIX**、**HP**、**Linux**、**Solaris SPARC** および **x86**、および **Windows** エージェント マシン上にインストールできます。

それぞれの管理対象ゲスト マシンは、**DSM** エクスプローラ ツリー ビューで個別のコンピュータとして表示されます。

## サポートされている仮想化サーバ プラットフォーム

仮想ホスト上のインベントリ用のサポート対象プラットフォーム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。

## CA Web サイトのコンテンツの更新

AM リモート エージェントを実装するには、CA Web サイトから MDB データベースの最新のコンテンツを入手する必要があります。コンテンツをダウンロードするには、DSM ドメイン マネージャおよび DSM エクスプローラが装備されているコンピュータがインターネットにアクセスする必要があります。DSM エクスプローラから、ソフトウェアのコンテンツのダウンロード設定ポリシー（[ドメイン]-[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]-[ソフトウェアのコンテンツのダウンロード]）を設定します。コンテンツ ダウンロード ポート ポリシーは 443（新規インストール）または 5250（アップグレード）に設定されます。

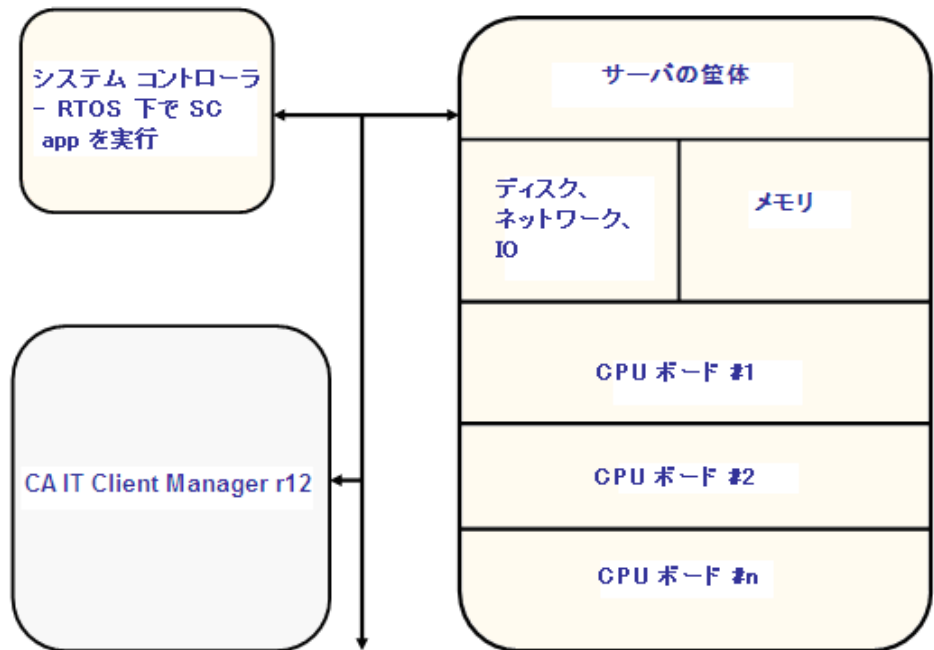
注：詳細については、DSM エクスプローラ ヘルプの「ソフトウェアのコンテンツのダウンロードポリシー グループ」を参照してください。または、ContentUtility.exe というユーティリティを使用して、コンテンツをダウンロードできます。このユーティリティの詳細については、このマニュアルの「Asset Management の設定」の章を参照してください。

## Solaris SPARC

Solaris SPARC では、モジュールは、ドメインをサポートしている Sun Enterprise/Sun Fire システムに関するパーティション情報を生成します。

ドメインは、通常は CPU ボード、メモリ、ディスクアレイ、およびその他の使用可能なリソースの組み合わせを使用した、いくつかの固有のコンピュータからなる大きなハードウェアの設定の一部です。つまり、ドメインは、固有のコンピュータとして動作する、別個のカプセル化された環境と見なすことができます。システムコントローラ (SC) および eXtended System Controller Facility (XSCF) は、各ドメインのハードウェアリソースの割り当てを管理します。また、Sun サーバラックでホストされているドメインの設定とステータスも記録および保持されます。

以下の図は、AM リモート エージェントが Sun ドメイン用にサポートしている、ハードウェアの配置を示しています。



## システム コントローラごとに収集された情報

以下の表には、システム コントローラごとに収集された情報が含まれます。

| ホストしているドメインの情報         | 制御しているホスト サーバの情報  | システム コントローラ自体の情報            |
|------------------------|-------------------|-----------------------------|
| 各ドメインのホスト名             | インストールされているメモリの容量 | システム コントローラのホスト名および IP アドレス |
| 各ドメインの IP アドレス         |                   | それが利用できるメモリの容量              |
| 各ドメインの状態（アクティブ、非アクティブ） |                   | オペレーティング システムのリビジョン レベル     |
| MAC アドレス（XSCF を除く）     |                   |                             |
| ホスト UUID               |                   |                             |

## インストール

AM リモート エージェントは、パーティション化できる UNIX サーバ上での Asset Management エージェントのインストールに追加された部分です。

このエージェントは、Solaris ドメインにインストールし、SSH を使用してシステム コントローラにダイレクトする必要があります。

**重要：** ほかの CA Client Automation インストールと同じネットワーク上にシステム コントローラを設定します。

## M3000/M4000/M5000/M8000/M9000 システム監視機構へのアクセスの前提条件

システム監視機構（XSCF）上の SSH サービスはデフォルトでは無効に設定されています。XSCF にアクセスするには、以下の前提条件を実行する必要があります。

- XSCF ユーザ アカウントの追加
- XSCF ユーザのパスワードの作成
- XSCF ユーザへの権限の割り当て
- SSH の有効化
- XSCF の再起動
- SSH サービス用のホスト公開鍵の生成
- SSH userpublic キーのインストール

### XSCF ユーザ アカウントの追加

#### XSCF ユーザ アカウントを追加する方法

1. useradm 権限を使用して、XSCF コンソールにログインします。
2. 「adduser username」コマンドを使用し、ユーザを追加します。  

```
XSCF> adduser uamuser
```
3. 「uamuser」が追加されたことを確認するには、「showuser」コマンドを使用します。

### XSCF ユーザのパスワードの作成

#### パスワード ポリシーを作成する方法

1. useradm 権限を使用して、XSCF コンソールにログインします。
2. 「password username」コマンドを使用し、ユーザのパスワードを設定します。  

```
XSCF> password uamuser
```
3. メッセージが表示されたらパスワードを入力し、もう一度パスワードを入力します。



## XSCF ユーザへの権限の割り当て

### 権限を割り当てる方法

1. useradm 権限を使用して、XSCF コンソールにログインします。
2. 「setprivileges ユーザ権限」コマンドを使用し、ユーザに権限を割り当てます。

```
XSCF> setprivileges uamuser platadm
```

3. 「uamuser」の権限を確認するには、「showuser -p」コマンドを使用します。

注：インストールされている XSCF ファームウェア のバージョンを表示するには、platadm 権限が必要です。

## SSH の有効化

SSH を有効にするには、platadm 権限を使用して XSCF コンソールにログインし、「setssh」コマンドを使用します。

```
XSCF> setssh -c enable
```

## XSCF の再起動

上記の SSH 設定の変更を有効にするには、XSCF を再起動する必要があります。

XSCF を再起動するには、XSCF コンソールから以下のコマンドを入力します。

```
XSCF> rebootxscf
```

## SSH サービス用のホスト公開鍵の生成

SSH サービスには、ホスト公開鍵が必要です。

### ホスト公開鍵を生成する方法

1. platadm 権限を使用し、XSCF コンソールにログインします。
2. setssh コマンドを以下のように入力します。

```
XSCF> setssh -c genhostkey
```

3. XSCF をリセットすることによって、ホスト キーを生成します。（「XSCF の再起動」を参照してください。）

## SSH ユーザ公開鍵のインストール

SSH キーは AM リモート エージェント システム上で生成され、XSCF にインストールされる必要があります。XSCF にアクセスするには、以下の前提条件を実行する必要があります。

1. `ssh-keygen` コマンドを使用して、AM リモート エージェント マシン上に SSH キーをセットアップします。SSH キーが設定されると、エージェントは SSH を使用して XSCF ホストにアクセスし、関連するインベントリ情報を収集します。

注：SSH パッケージは、Solaris 8 以降にはデフォルトではインストールされていません。<http://www.openssh.org/> サイトからダウンロードできます。

2. `root` ユーザを使用して、エージェント マシン上で `ssh-keygen` を実行します。  
これによって、秘密鍵と公開鍵の 2 つの鍵が作成されます。これらの鍵は、`~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub` に保存されます。
3. `setssh` を使用し、公開鍵ファイルの中身 (`~/.ssh/id_rsa.pub`) を XSCF 上の対象となる Asset Management ユーザ「`uamuser`」に追加します。次に、手順 2 で作成したユーザの公開鍵をコピーして貼り付けます。Enter キーを押した後、「Ctrl」と「D」キーを押してインストールを完了します。

```
XSCF> setssh -c addpubkey -u uamuser
```

4. `showssh` コマンドを使用し、`uamuser` 公開鍵が XSCF にインストールされたことを確認します。

```
XSCF> showssh -c pubkey -u uamuser
```

これで、SSH を使用して、パスワードを要求されることなくシステム コントローラにログインできます。

## E4800/4900/6800/6900 システム コントローラへのアクセスの前提条件

システム コントローラ上の SSH サービスは、デフォルトで無効になっています。システム コントローラにアクセスするには、以下の前提条件を実行する必要があります。

- SSH の有効化
- システム コントローラへのリモート アクセスの有効化
- システム コントローラの再起動
- すべての変更の確認

## システムコントローラへのリモート アクセスの有効化

システム コントローラへのリモート アクセスを有効化するには、以下のように「ssh」を選択します。

接続タイプ (ssh、telnet、なし) [なし] : ssh

### SSH の有効化

「setupplatform -p network」コマンドを使用して、以下のようにプラットフォーム シェルから SSH を有効化します。

```
schostname:SC> setupplatform -p network
```

ネットワークの設定

システム コントローラはネットワーク上にありますか? [はい] :

DHCP または静的ネットワーク設定のいずれを使用しますか? [静的] :

ホスト名 [schostname] :

IP アドレス [xx.x.xx.xx] :

ネットマスク [xxx.xxx.xxx.x] :

ゲートウェイ [xx.x.xx.x] :

DNS ドメイン [xxxx.xxx.xxx]

プライマリ DNS サーバ [xxx.xxx.xxx.xx] :

セカンダリ DNS サーバ [xxx.xxx.xx.x] :

### システムコントローラの再起動

上記のネットワーク設定が有効になるには、システム コントローラを再起動する必要があります。

アイドル接続タイムアウト (分で指定、0 はタイムアウトなしの意味) [0] :

システム コントローラを再起動するには、プラットフォーム シェルから以下のコマンドを入力します。

```
schostname:SC> reboot -y
```

### すべての変更の確認

システム コントローラを再起動した後に、「showplatform」コマンドを使用して、すべての変更が実装されたことを確認します。

## E10K/12K/15K システム コントローラへのアクセスの前提条件

システム コントローラとそのドメインの両方で SSH キーが生成されている必要があります。システム コントローラにアクセスするには、以下の前提条件を実行する必要があります。

1. 「ssh-keygen」コマンドを使用して、システム コントローラとそのドメイン システム上で SSH キーを設定します。SSH キーを設定すると、エージェントは SSH を使用してシステム コントローラにアクセスし、関連するインベントリ情報を収集します。

注：SSH パッケージは、Solaris 8 以降にはデフォルトではインストールされていません。<http://www.openssh.org/> サイトからダウンロードできます。

2. root ユーザで、ドメイン上で ssh-keygen を実行します。

これによって、秘密鍵と公開鍵の 2 つの鍵が作成されます。これらの鍵は、`~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub` に保存されます。

3. 公開鍵ファイルの中身 (`~/.ssh/id_rsa.pub`) をシステム コントローラ上の対象となる Asset Management ユーザ (`~/.ssh/authorized_keys`) に追加します。

これで、SSH を使用して、パスワードを要求されることなくシステム コントローラにログインできます。

## システム コントローラへのアクセス

システム コントローラでは、サードパーティ製のソフトウェアをインストールすることはできません。そのため、システム コントローラにリモートからアクセスし、システム コントローラが管理しているドメイン、ドメインの設定、または現在の状態を調べる必要があります。システム コントローラへリモートアクセスできるようにするには、システム コントローラ上で SSH を有効にする必要があります。Asset Management エージェントは、SSH を使用してシステム コントローラにアクセスし、インベントリ情報を収集します。

## 仮想ホスト インベントリの手動テスト

仮想ホスト インベントリを手動でテストし、正しい情報が収集されたことを確認できます。

**注：**手動でインベントリ収集モジュールを実行するのは、テストまたは診断を行う場合です。診断メッセージが画面に表示される場合がありますが、これはインベントリの収集には影響しません。

### 仮想ホスト インベントリを手動でテストする方法

1. DSM エクスプローラを使用して、仮想ホスト インベントリ収集タスクを作成します。
2. Asset Management エージェントがインストールされている Solaris ドメインで、以下のコマンドを入力します。

```
caf start amagent
```

**注：**amagent を起動すると、AM リモート エージェントおよびその登録プロセスが自動的に開始されます。

次の場所に、システム コントローラ インベントリが書き込まれます。

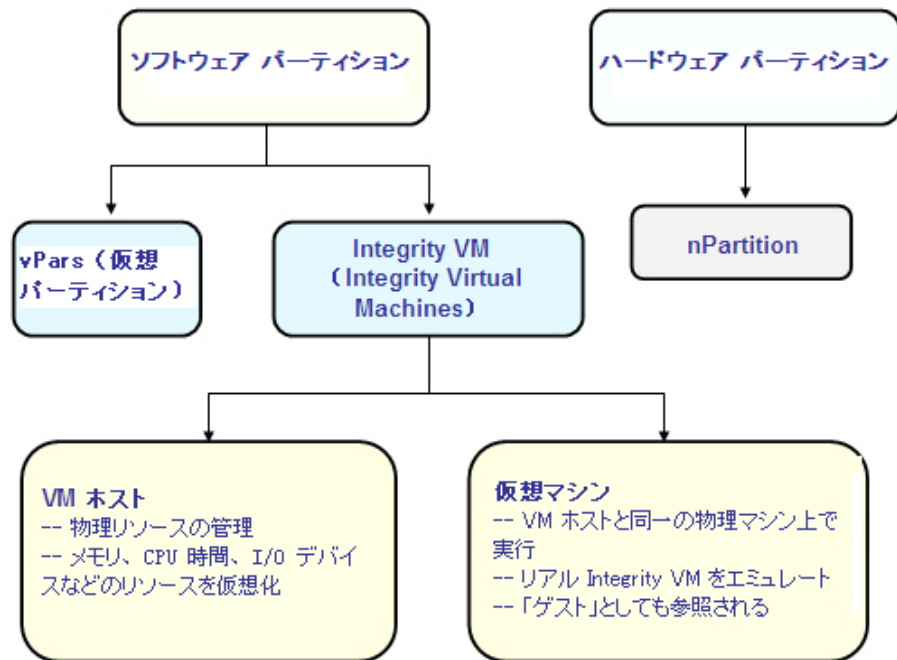
```
$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm/12amvminvux.inv
```

3. システム コントローラ固有のさまざまなコマンドからの出力とインベントリ ファイルの情報を確認します。

**注：**詳細については、「Sun Fire Midrange System Controller Command Reference Manual」 (<http://docs.sun.com/source/>) および「Sun SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Administration Guide」 (<http://dlc.sun.com/pdf>) を参照してください。

## HP-UX

HP システムでは、ソフトウェア パーティションおよびハードウェア パーティションの 2 つの主要なカテゴリが対象になります。以下の図は、ソフトウェアパーティションおよびハードウェア パーティションによるパーティションを示しています。



- ハードのパーティション化である nPartitions (nPars) を使用すると、ユーザはハードウェア レベルでパーティションを作成できます。各 nPartition ではその独自の OS イメージが実行されており、あるパーティションで実行されているアプリケーションは、他のハードパーティションで実行されているアプリケーションからは完全に孤立しています。つまり、各パーティションは別個の物理サーバのように動作します。
- ソフトパーティション化である仮想パーティション (vPars) を使用すると、ユーザは 1 つのサーバまたは nPartition 内に複数の仮想システムを作成できます。各仮想システムはその他の仮想システムから孤立しており、その独自の OS インスタンス、リソース、アプリケーション、およびユーザを持っています。
- ソフトパーティション化である Integrity Virtual Machines (Integrity VM) は、HP Itanium サーバまたは nPartition 上に複数の仮想マシンを作成するための機能を提供します。各仮想マシンでは、完全に孤立した環境で、その独自の別個の「ゲスト」オペレーティングシステムインスタンス、アプリケーション、およびユーザが実行されます。Itanium サーバは、必要に応じてホストするさまざまな仮想マシンに、その物理リソースを割り当てます。

## HP Integrity 仮想マシン

AM リモート エージェントは、HP-UX 11i v2（2005 年 5 月）以降を実行している HP Itanium サーバの情報を収集し、レポートします。仮想マシン機能は、アプリケーション レベルのソフトウェアによって提供され、各仮想マシンは、HP-UX 11i v2、HP-UX 11i v3、Windows Server 2003、および Red Hat 4 バージョン 3.0 などのような異なるオペレーティングシステムを使用してゲストを実行できます。HP Itanium サーバ用に以下の情報が収集されます。

- ホストしている仮想マシン。次のものが含まれます。
  - 各仮想マシンのホスト名。
  - 各仮想マシンの IP アドレス。
  - 各仮想マシンにインストールされているオペレーティングシステム。
  - 各仮想マシンの状態（アクティブ、非アクティブ）。
  - 仮想マシンのゲストのシリアル番号と UUID。
- オペレーティングシステムのリリースレベル。
- CD、DVD など取り付けられている物理デバイス。
- 使用可能なメモリの容量。
- 利用可能な合計量を超えて使用されているディスク領域。
- ホストのホスト名および IP アドレス。
- ネットワーク ハードウェア（カードタイプおよび設定、MAC アドレス）。

## インストール

標準の Asset Management エージェントに加えて、AM リモート エージェントがインストールされます。

HP Integrity Virtual Machines については、このエージェントをエージェント マシン（AIX、HP、Linux、Solais または Windows）上にインストールした後、SSH を使用して VM Host にダイレクトします。

## Integrity VM ホストへのアクセスの前提条件 (BAR)

SSH キーは、VM ホストと VM ゲストのシステムの両方で生成される必要があります。VM ホストにアクセスするには、以下の前提条件を実行する必要があります。

- HP-UX DSAU（Distributed Systems Administration Utilities）ツールを使用して、VM ホストと VM ゲストのシステムで SSH キーを設定できます。これは、デフォルトで HP-UX 11.23（0512 リリース）以降にインストールされています。

- 「/opt/dsau/bin/csshsetup \$VMHostName」というコマンドを使用して、VM ホストと VM ゲストのシステム間に SSH キーを設定できます。SSH キーを設定すると、エージェントは SSH を使用して VM ホストにアクセスし、関連するインベントリ情報を収集します。

### Integrity VM ホストへのアクセス

VM ホストには、アプリケーションをインストールしないことをお勧めします。VM ホストにリモートからアクセスし、それが管理している仮想マシン、仮想マシンの設定、または現在の状態を調べる必要があります。VM ホストへのリモートアクセスを可能にするには、VM ホストと VM ゲストのシステムの両方で SSH キーを生成する必要があります。Asset Management エージェントは、SSH を使用して VM ホストにアクセスし、関連するインベントリ情報を収集します。

### 設定

Integrity VM ホストを設定するには、DSM エクスプローラを使用して仮想ホストインベントリ収集タスクを作成します。



## 仮想ホスト インベントリの手動テスト

仮想ホスト インベントリを手動でテストし、正しい情報が収集されたことを確認できます。

**注：**手動でインベントリ収集モジュールを実行するのは、テストまたは診断を行う場合です。診断メッセージが画面に表示される場合がありますが、これはインベントリの収集には影響しません。

### 仮想ホスト インベントリを手動でテストする方法

1. DSM エクスプローラを使用して、仮想ホスト インベントリ収集タスクを作成します。
2. Asset Management エージェントがインストールされている VM Guest システムで、以下のコマンドを入力します。

```
caf start amagent
```

**注：**amagent を起動すると、AM リモート エージェントおよびその登録プロセスが自動的に開始されます。

VM ホスト インベントリが以下の場所書き込まれます。

```
$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm/12amvminvux.inv
```

3. VM ホスト 固有のさまざまなコマンドからの出力とインベントリ ファイルの情報を確認します。

**注：**詳細については、「HP Integrity Virtual Machines: Installation, Configuration, and Administration」 (<http://docs.hp.com/>) を参照してください。

## HP nPartition および仮想パーティション

AM リモート エージェントは、HP-UX 11i 以降を実行している HP サーバ上に nPar および vPar の詳細を生成します。エージェントは、nPar および vPar システムにアクセスし、それらのインベントリ情報を取得し登録できます。

## HP Chassis および nPartitions 用に収集される情報

Chassis および その nPartitions では、HP Chassis および nPartitions 用に次の情報が収集されます。

- サーバ名
- サーバのシリアル番号
- サーバのモデル名
- サーバのベンダー
- ハードまたはソフトのパーティション情報
- 使用可能なメモリ容量
- サーバのプロセッサの合計

Chassis およびその nPartitions 用に、次の情報は収集されません。

- サーバの MAC アドレス
- サーバの IP アドレス
- プロセッサの詳細情報
- サーバのストレージ情報

## nPar システム と vPar システムの関係

HP-UX nPar システムでは、複数の nPar を持つことができます。それぞれの nPar は、他の nPar をパーティション ID およびパーティション名で識別します。これらの nPar のすべては、同じシリアル番号を共有します。

nPar は、以下の情報は持っていません。

- 他の nPar のホスト名
- 所有する vPar システム

注：1 つの nPar システムは、複数の vPar を持つことができます。

同様に、vPar システムでは、それぞれの vPar はほかの vPar をパーティション名で識別します。これらの vPars のすべては、それらの親の nPar を持つ同じシリアル番号を共有します。

vPar は、以下を認識します。

- 属している nPar
- この nPar が所有する 別の vPar、およびそのパーティション名

ただし、vPar は、ほかの vPar のホスト名に関する情報を持っていません。ほかの vPar システムは、自身をパーティション名で識別します。

## DSM エクスプローラ GUI における nPar と vPar の関係の表示

DSM エクスプローラのユーザ インターフェースでは、nPar と vPar の関係は通常「関連するコンピュータ」として表示されます。「関連するコンピュータ」として関係を表示するため、親子のパターンが無視され、関係を簡単に表すことができます。

## インストール

インベントリ情報を収集およびレポートするには、すべての nPar と vPar に AM リモート エージェントをインストールする必要があります。このインストールでは、仮想ホスト インベントリ収集タスクを設定する必要はありません。

**注：** nPar システムと vPar システムに十分なリソースがある場合のみ、すべての nPar と vPar にエージェントをインストールすることをお勧めします。

## Chassis インベントリ モジュールの手動テスト

Chassis インベントリ モジュールを手動でテストし、正しい情報が収集されたことを確認できます。

**注：**手動でインベントリ収集モジュールを実行するのは、テストまたは診断を行う場合です。診断メッセージが画面に表示される場合がありますが、これはインベントリの収集には影響しません。

### Chassis インベントリ モジュールを手動でテストする方法

1. Asset Management エージェントがインストールされている nPar （または vPar）システムで、以下のコマンドを入力します。

```
cd $CA_ITRM_BASEDIR/Agent/AM/plugin
```

```
./amvminvhp 0
```

次の場所に、Chassis インベントリが書き込まれます。

```
$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm/amvminvux.inv
```

2. nPar および vPar 固有のさまざまなコマンドからの出力とインベントリ ファイルの情報を確認します。

Chassis インベントリ ファイルの作成後、以下の方法のいずれかを使用して、AM リモート エージェントを手動で実行できます。

#### ■ 方法 1

```
cd $CA_ITRM_BASEDIR/Agent/AM/plugin
```

```
./amVMAgent register
```

#### ■ 方法 2

```
caf start amagent
```

**注：**amagent を起動すると、AM リモート エージェントおよびその登録プロセスが自動的に開始されます。

## nPar インベントリ モジュールの手動テスト

nPar インベントリ モジュールを手動でテストし、正しい情報が収集されたことを確認できます。

注：手動でインベントリ収集モジュールを実行するのは、テストまたは診断を行う場合です。診断メッセージが画面に表示される場合がありますが、これはインベントリの収集には影響しません。

### nPar インベントリ モジュールを手動でテストする方法

1. Asset Management エージェントがインストールされている nPar（または vPar）システムで、以下のコマンドを入力します。

```
cd $CA_ITRM_BASEDIR/Agent/AM/plugin
```

```
./amvminvhp 1
```

次の場所に、nPar インベントリが書き込まれます。

```
$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm/amvminvux.inv
```

2. nPar および vPar 固有のさまざまなコマンドからの出力とインベントリ ファイルの情報を確認します。

nPar インベントリ ファイルの作成後、以下のいずれかの方法を使用して、AM リモートエージェントを手動で実行できます。

#### ■ 方法 1

```
cd $CA_ITRM_BASEDIR/Agent/AM/plugin
```

```
./amVMAgent register
```

#### ■ 方法 2

```
caf start amagent
```

注：amagent を起動すると、AM リモートエージェントおよびその登録プロセスが自動的に開始されます。

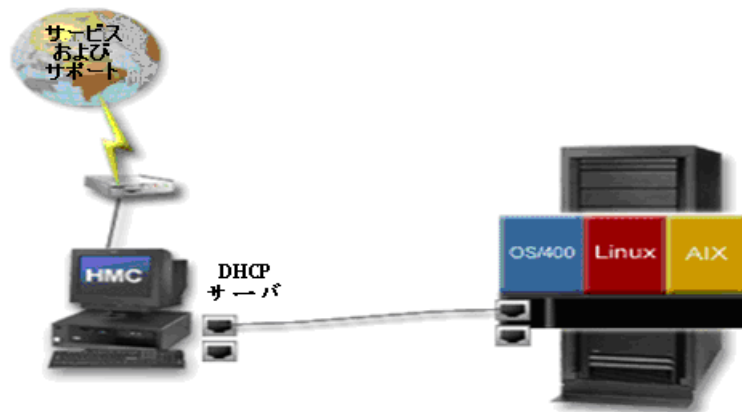
注：Chassis インベントリの収集によって、  
\$CA\_ITRM\_BASEDIR/Agent/AM/data/transfer\_vm/amvminvux.inv の Chassis 情報が上書きされた後に、nPar インベントリが収集されます。

## AIX

AIX では、LPAR およびサーバ システムを設定および管理するために IBM HMC (Hardware Management Console) が使用されている、IBM eServer pSeries システムおよび IBM System p5 システム上で AIX 5.3 以降が実行されている論理パーティション (LPAR) 情報をモジュールが生成します。

論理パーティションとは、一連のリソースがその独自のオペレーティング システム インスタンスおよびアプリケーションで独立して動作できるように、コンピュータのプロセッサ、メモリ、およびストレージを複数のリソースに分割したものです。作成できる論理パーティションの数は、システムのプロセッサ モデルおよび使用可能なリソースによって異なります。

HMC (Hardware Management Console) は、IBM eServer pSeries システムおよび IBM System p5 システム上の論理パーティションを設定、管理、および監視するための標準的なユーザ インターフェースを提供します。これは、DVD-RAM ドライブで AIX または Linux が実行されている 32 ビット版の Intel ベースのデスクトップ PC で構成されています。以下の図は、LPAR、そのサーバ、および HMC の関係を示しています。



注：AM リモート エージェントによってサポートされる HMC のバージョンは、v2.0 から v7.0 です。

## 各 IBM サーバ用に収集された情報

IBM サーバ用に次の情報が収集されます。

- ホストしている論理パーティション。次のものが含まれます。
  - 各論理パーティションのパーティション名
  - 各論理パーティションのパーティション ID
  - 各論理パーティションの状態（アクティブ、非アクティブ）
  - 論理パーティションがあるサーバ名
- IO デバイスの数
- プロセッサの数
- 使用可能なメモリ容量
- シリアル番号
- サーバ名
- サーバのモデル名
- サーバのベンダー

IBM サーバでは、次の情報が収集されません。

- サーバの MAC アドレス
- サーバの IP アドレス
- サーバのプロセッサの詳細情報
- サーバのストレージ情報

## インストール

IBM のサーバについては、Asset Management エージェントに加えて、AM リモートエージェントがインストールされます。

このエージェントをエージェントマシン（AIX、HP、Linux、Solais または Windows）上にインストールした後、SSH（Secure Shell）を使用して HMC に向けます。

## IBM HMC ( Hardware Management Console ) の設定スクリプト

エージェントは信頼済みの SSH キー関係および特定の「uamuser」ユーザアカウントを使用して IBM HMC に接続します。これにより、HMC 管理者のパスワードをエージェントに公表する必要はありません。

UNIX および Linux エージェントについては、UAMhmcConfig と呼ばれるシェルスクリプトがあり、これによってエージェントのセットアップ手順を進めます。Windows エージェントから IBM HMC にアクセスしようとしている場合に実行すべき設定ステップについては、このセクションで後ほど説明します。

### 前提条件

HMC 上でリモート コマンドを実行するために UAMhmcConfig スクリプトおよび Asset Management エージェントを有効化するには、2 つの前提条件を満たす必要があります。

- HMC 上で、[リモート コマンドの実行の有効化/無効化] オプションを有効化する必要があります。これをチェックするには、HMC システム管理環境を使用し、[HMC のメンテナンス]、[システムの設定] にある設定を調べます。
- スクリプトを実行するエージェント マシン上に SSH がインストールされている必要があります。

注：SSH は、AIX オペレーティング システムで提供されていますが、デフォルトではインストールされていません。

注：Windows エージェントについては、Plink (PuTTY Link) ユーティリティがエージェントと共にインストールされており、SSH コマンドライン インターフェイスを使用できます。詳細については、「[Windows リモート エージェント ホスト上での Plink の設定 \(P. 444\)](#)」セクションを参照してください。このセクションで後ほど説明する、Windows エージェントの設定に使用するコマンドは、すでにお持ちの他の SSH コマンド ツールと併用する場合もあります。



## Linux および UNIX エージェントの設定

HMC にリモートでアクセスするためにインベントリ処理に必要な要件が、UAMhmcConfig スクリプトによって設定されます。HMC で Asset Management ユーザアカウント (uamuser) が作成され、エージェントはこのアカウントを使用してインベントリ情報を収集します。またこのスクリプトによって、パスワードを要求しない、HMC へのリモート コマンドアクセスを有効にするための SSH キーが作成されます。

UAMhmcConfig スクリプトは、デフォルトのインストールディレクトリ (通常は /opt/CA/DSM/Agent/AM/scripts) にあります。これは、Asset Management エージェントが実行される前に、ルート ユーザアカウントで実行する必要があります。HMC がエージェントにアクセスできるようにするには、AM リモートエージェントがインストールされている 1 つのエージェントマシンでスクリプトを 1 度だけ実行する必要があります。ただし、複数のエージェントマシンで UAMhmcConfig スクリプトを実行すると、スクリプトが実行されたエージェントマシンが突然使用できなくなった場合でも、サーバインベントリ全体が生成される可能性が高くなります。

Asset Management エージェントを呼び出す前に UAMhmcConfig スクリプトを実行しない場合、エージェントは、サーバ上のリソース使用率の合計や使用可能な空きリソースなどの全体的なサーバインベントリについてレポートすることができません。

スクリプトを開始すると、以下の情報を入力するように求められます。

- サーバを管理するために使用される HMC のホスト名。
- uamuser アカウントを作成するときに使用できる、HMC 上の既存のユーザアカウントの名前とパスワード。この既存のアカウントは、少なくとも「User Administrator」の役割を持っている必要があります。
- uamuser アカウントのパスワードが作成されます。

uamuser アカウントが HMC にすでに存在しているかどうかをスクリプトが確認し、必要な場合のみ作成されます。この確認中に、HMC の信頼性が確立できないことを示すメッセージが表示され、接続を続行するかどうか確認される場合があります。通常これは、入力した HMC のホスト名が \$HOME/.ssh/known\_hosts ファイルにエントリを持たないことを意味します。この質問に「はい」と答えると、known\_hosts ファイルが自動的に更新され、今後はこのメッセージは表示されなくなります。

uamuser アカウントが使用可能になると、Asset Management エージェントのパブリック キー/プライベート キーのペアが作成されます。キー ファイルは \$HOME/.ssh にあり、プライベート キーおよびパブリック キーのそれぞれに uamkey および uamkey.pub という名前が付きます。HMC 上で uamuser アカウントを使用して Asset Management エージェントがリモート コマンドを実行できるようにするには、パブリック キーを uamuser authorized\_keys2 ファイルに配置する必要があります。UAMhmcConfig スクリプトは、uamuser authorized\_keys2 ファイルを選択し、Asset Management エージェントのパブリック キーをファイルに書き込み、authorized\_keys2 ファイルを元の場所にコピーし直します。この操作中、アカウント作成フェーズで入力した uamuser パスワードの入力が要求されます。

注：仮想ホスト インベントリ収集タスクを設定する場合、「仮想ホストの追加」手順で (236P. )IBM HMC の [SSH キーの場所] フィールドに「\$ROOT\_HOME/.ssh/uamkey」と入力する必要があります。

## アンインストール

Asset Management エージェントをアンインストールする前に、UAMhmcDeconfig スクリプト（通常、\$CA\_ITRM\_BASEDIR/Agent/AM/scripts パスの下にある）を呼び出し、HMC の設定を取り消す必要があります。アンインストール前にこれを行わないと、「uamuser」ユーザが HMC コンピュータに残ります。エージェント コンピュータでは、この uamuser の SSH キーが \$ROOT\_HOME/.ssh/uamkey に残ります。

## Windows エージェントの設定

IBM HMC 上での Windows エージェントを設定するには、以下の手順の実行が必要です。

- HMC 上で uamuser アカウントを作成します。
- uamuser アカウントを使用して、Windows エージェントと HMC との間に信頼済みキー関係を確立します。

信頼済みキー関係の作成には、HMC ファイルを Windows エージェント ホスト上で編集しての変更が必要です。ホスト間でのファイルの転送には、SCP ユーティリティが必要です。この作業に適したユーティリティは PSCP クライアントで、これは PuTTY/Plink からのユーティリティの一つです。PSCP は PuTTY/Plink Web サイトの [www.chiark.greenend.org.uk](http://www.chiark.greenend.org.uk) から取得可能です。

### 「uamuser」アカウントを作成する方法

1. HMC に管理者としてログインします（または、管理ユーザとして SSH コマンドを使用）。
2. 以下のいずれかのコマンドを使用して、「uamuser」というユーザを HMC に追加します。

HMC バージョン 4 以上については、以下を入力します。

```
mkhmcusr -u uamuser -a hmcoperator -d UAM user
```

それより以前の HMC バージョンについては、以下を入力します。

```
mkhmcusr -u uamuser -a sysadmin -d UAM user
```

Plink を使ってこの手順を実行するには以下を入力します。

```
"C:¥Program Files¥CA¥DSM¥Agent¥units¥00000001¥uam¥plink" -ssh
hmc-admin-user@hmc-host mkhmcusr -u uamuser -a hmcoperator -d UAM user
```

*hmc-admin-user* 変数は、新規ユーザの作成権限を持つ HMC の管理ユーザ名を表し、*hmc-host* は Windows エージェントのアクセス対象となる HCM のホスト名または IP アドレスを表します。

### Windows エージェントおよび HMC との間での信頼済みキー関係の確立

1. SSH キーの公開鍵/秘密鍵ペアを、たとえば、PuTTYgen または他の SSH ツールを使用して生成します。
2. 秘密鍵には、空のパスフレーズを使用します。
3. 公開鍵を、HMC 上の uamuser に対する、authorized key ファイルにインストールします。この設定を行う方法
  - a. HMC サーバから Windows アセット管理エージェント ホストに鍵をコピーし、SCP クライアントを使用して編集します。例えば、PSCP を使用すると以下のようなコマンドラインになります。

```
pscp -scp uamuser@hmc-host:/home/uamuser/.ssh/authorized_keys2
C:¥Temp¥authorized_keys2
```

- b. C:¥Temp¥authorized\_keys2 ファイルを編集します。（例に続く）このファイルの末尾に、上記で作成された公開鍵を含む行を追加します。

**重要：** ファイルは **Unix 形式** で保存し、**DOS 形式** に変換しないでください。

- c. 変更されたファイルを、たとえば以下のコマンドを使用して HMC サーバにアップロードします。

```
pscp -scp C:¥Temp¥authorized_keys2
uamuser@hmc-host:/home/uamuser/.ssh/authorized_keys2
```

4. 秘密鍵を安全な場所に保存します（たとえば、“C:¥Program Files¥CA¥DSM¥Agent¥uamkey.txt”）。
5. この鍵ファイルは、[SSH キーの場所] を入力する、収集タスク ダイアログボックスで指定します。

## アンインストール

Windows エージェントを削除する前に、または Windows エージェントと IBM HMC との間の信頼済み関係を取り消す場合は、以下の手順を実行します。

- Windows エージェントと IBM HMC との間の信頼済み関係を取り消します。
- IBM HMC 上で uamuser ユーザ アカウントを削除します。

### 信頼済み関係の取り消し

1. 管理ユーザとして HMC にログインします。
2. /home/uamuser/.ssh/authorized\_keys2 ファイルを編集します。設定時に挿入された公開鍵を削除します。
3. ファイルを保存します。
4. 以前に説明した設定手順で作成した秘密鍵を、保存先の Windows エージェント コンピュータから削除します。

### uamuser ユーザ アカウントの削除

1. 管理ユーザとして HMC にログインします。
2. 以下のコマンドを実行します。

```
rmhmcusr -u uamuser
```

Plink を使用して Windows コンピュータからこのコマンドを実行するには、以下のコマンドを実行します。

```
"C:¥Program Files¥CA¥DSM¥Agent¥units¥000000001¥uam¥plink" -ssh
hmc-admin-user@hmc-host rmhmcusr -u uamuser
```

## 仮想ホスト インベントリの手動テスト

仮想ホスト インベントリを手動でテストし、正しい情報が収集されたことを確認できます。

**注：**手動でインベントリ収集モジュールを実行するのは、テストまたは診断を行う場合です。診断メッセージが画面に表示される場合がありますが、これはインベントリの収集には影響しません。

### 仮想ホスト インベントリを手動でテストする方法

1. DSM エクスプローラを使用して、仮想ホスト インベントリ収集タスクを作成します。
2. Asset Management エージェントがインストールされているエージェント マシンで以下のコマンドを入力します。

```
caf start amagent
```

**注：**amagent を起動すると、AM リモート エージェントおよびその登録プロセスが自動的に開始されます。

次の場所に、HMC インベントリが書き込まれます。

```
$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm/12amvminvux.inv
```

3. HMC 固有のさまざまなコマンドからの出力とインベントリ ファイルの情報を確認します。

## VMware ESX

VMware ESX は、データ センター仮想化プラットフォームです。VMware ESX サーバは、サードパーティ オペレーティング システムの上では実行されませんが、vmkernel と呼ばれる独自のカーネルが含まれています。1 つの VMware ESX サーバ上で複数の仮想マシンを実行できます。仮想マシンは、非常に孤立したソフトウェア コンテナであるため、物理コンピュータのようにオペレーティング システムおよびアプリケーションを起動できます。仮想マシンは、物理コンピュータのように動作し、仮想（すなわち、ソフトウェア ベースの）CPU、RAM、ハードディスクおよびネットワーク インターフェース カード（NIC）が含まれます。

VMware ESX Server 3.5 および 4.0 は AM リモート エージェントによってサポートされています。

## VMware ESX サーバからのインベントリの収集

Client Automation は、VMware ESX サーバからインベントリを収集する 2 つの方法を提供します。

- 1 つ目の方法では、VMware ESX サービス コンソール上で Asset Management エージェントをインストールします。

VMware ESX 3.5 では、追加 CD 上にある特別な VMware ESX エージェントをインストールする必要があります。

VMware ESX 4.0 では、リリース 12.9 エージェントがインストールされる場合があります。

このエージェントが、VMware サービス コンソールのプロパティを収集します。収集されるディスク、メモリおよびその他のシステム プロパティは、VMware サービス コンソールと割り当てられたリソースの状態を示しています。ただし、これはマシン全体のリソースの小さなサブセットであることに注意してください。下位互換性として、このエージェントでは VMware サービス コンソールによってレポートされたホスト名を使用して、インベントリをレポートします。

- 2 つ目の方法では、Asset Management エージェントに Asset Management リモート仮想インベントリのアドオンのインストールと設定を行います。これは、Client Automation リリース 12.9 の新機能で、コンピュータ全体のプロパティを収集します。このエージェントによってレポートされるディスク、メモリ、およびその他のシステム プロパティは、コンピュータのハードウェア全体の状態を示しています。このインベントリと VMware サービス コンソール上にインストールされたエージェントが返すデータを区別するために、先頭に「VMware ESX -」と付いたサービス コンソールのホスト名を使用してインベントリをレポートします。

同じコンピュータに対して両方のインベントリ収集方法が使用された場合、DSM エクスプローラでは、[関連するコンピュータ] ペインを使用して VMware サービス コンソール用に収集したインベントリとマシン全体用に収集したインベントリを表示します。

## VMware ESX サーバ用に収集された情報

AM リモート エージェントによって収集された情報は、ローカル エージェントによって収集された情報に似ています。ただし、AM リモート エージェントによって収集できる情報のタイプに違いがあります。また、これは VMware プログラミング インターフェースの機能に依存します。

AM リモート エージェントは、設定情報と共に VMware ESX でサポートされている機能もレポートします。この情報は、ローカル エージェントではレポートされません。ただし、AM リモート エージェント インベントリ 収集では、ホスト入力 デバイスのような情報はレポートされません。

注： AM リモート エージェントの収集した一部の仮想マシン プロパティでは、VMware ツールが仮想マシン上にインストールされて実行されていることを必要とするものがあります。VMware ツールのステータスは、仮想マシン プロパティのツール ステータス列で判断できます。VMware ツールで必要なプロパティは、ホスト名、IP アドレス、ツールのバージョン、ゲスト ファミリ、ディスク領域の合計、ディスク空き領域の合計、および ラベルです。

## 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。

### 環境設定

VMware ESX ホストのインベントリ収集を設定するには、DSM エクスプローラを使用して、仮想ホスト インベントリ収集タスクを作成します。

### VMware ESX パラメータ

VMware ESX Web サービスにアクセスするには、ESX ホスト マシン用のログオン クレデンシアルを指定する必要があります。クレデンシアルは、Administrator または Read-only の VMware システム ロールがある VMware ESX ホストのユーザ用である必要があります。

#### ホスト名

Asset Management インベントリを収集する 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

Administrator または Read-only の VMware システム ロールを持つ VMware ESX ユーザの名前を指定します。

#### Web サービス パスワード

指定した Web サービス ユーザ名 に対応するパスワードが必要です。

#### Web サービス URL

Web サービス URL を示します。以下の形式を使用します。

`https://ESXHostFQDNservername/sdk`

*ESXHostFQDNservername* は、ESX サーバの完全修飾ホスト名を表わします。また、ホスト名の代わりに IP アドレスを指定できます。

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、HTTPS 上で SSL を使用してアクセスできる安全な Web サービスとして、ポート 443 上で Web サービスを実行します。

### インストール

AM リモート エージェントは、追加パッケージとして Asset Management エージェントにインストールされます。AM リモート エージェント パッケージは Windows または Linux で使用できます。



## 仮想ホスト インベントリの手動テスト

仮想ホスト インベントリを手動でテストし、正しい情報が収集されたことを確認できます。

**注：**手動でインベントリ収集モジュールを実行するのは、テストまたは診断を行う場合です。診断メッセージが画面に表示される場合がありますが、これはインベントリの収集には影響しません。

### 仮想ホスト インベントリを手動でテストする方法

1. DSM エクスプローラを使用して、仮想ホスト インベントリ収集タスクを作成します。
2. AM リモート エージェントがインストールされている Windows または Linux コンピュータで以下のコマンドを入力します。

```
caf start amagent
```

**注：**amagent を起動すると、AM リモート エージェントおよびその登録プロセスが自動的に開始されます。

ESX ホスト インベントリが以下の場所書き込まれます。

```
$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm/12amvminvux.inv
```

3. インベントリ ファイル内の情報と VMware Virtual Infrastructure Client または Managed Object Browser 内の情報を照合します。

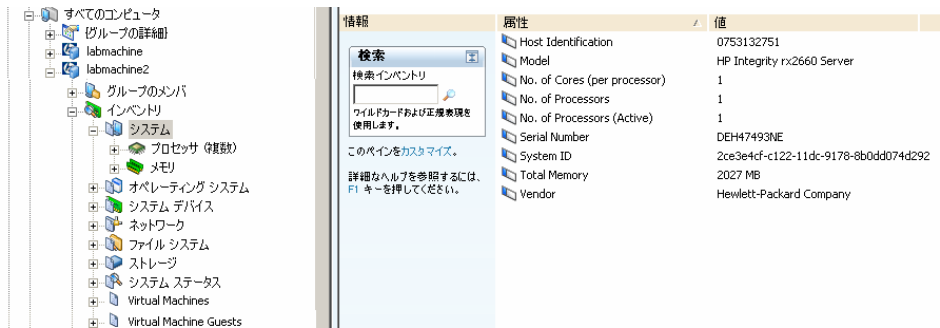
## 仮想ホスト インベントリの表示

仮想ホスト用に収集されたインベントリ情報は、他のインベントリ情報と同様に DSM エクスプローラのツリー ビューに表示されます。

インベントリには仮想ホストの特定のプロパティが反映され、Sun、IBM、および HP および VMware ESX のサーバがコンピュータ ユニットとして表示されます。

コンピュータ ユニットは、それぞれの管理対象ゲスト コンピュータに表示されます。仮想ホストおよびそのホストに関連付けられているゲストは、関連するコンピュータとしてレポートされ、双方の間を簡単に移動できます。

以下の図は、仮想ホストのインベントリ情報を示しています。



注：システム コントローラ コンピュータのインベントリ データに対して DSM エクスプローラ（インベントリ、システム、プロセッサ ノードの下）に表示されるプロセッサの数は、起動されているプロセッサのみが含まれています。この場合、電源が入っていないプロセッサはカウントされません。

関連項目：

[リモート エージェントおよび仮想ホストの表示 \(P. 239\)](#)

## 仮想ホストとゲストの関係

仮想ホストとゲスト コンピュータはアセット管理ユニットとして登録され、DSM エクスプローラのツリー ビューに表示されます。以下の図では、仮想ホストと仮想ホストの管理対象ゲスト コンピュータの関係を示しています。



[ホームページ] タブで、[関連するコンピュータ] の下の使用可能なユニットのハイパーリンクをクリックすると、仮想ホストとそのホストに關係する管理対象ゲストが表示されます。

## 仮想ホストとそのゲストの關係の作成

仮想ホストがドメイン マネージャに登録されると、仮想ホストとそのゲストとの關係が作成されます。ドメイン マネージャによって、仮想ホストとそのすべての既知のゲスト (HP-UX nPars と vPars、IBM LPAR、および Sun ドメインなど) との關係がドメインで作成されます。仮想ホストの登録後に登録されたゲストとの關係は、仮想ホストの次の登録プロセスまで作成されません。

注： HP-UX nPar、HP-UX vPar、および IBM LPAR では、仮想ホストとそのゲスト システムとの間に親子關係はありません。

## コンピュータ プロパティ ダイアログ ボックスでの AM リモート エージェントの表示

AM リモート エージェントは HMC、システム コントローラ、および VM ホスト システムに実際にはインストールされていないので、通常の [Asset Management エージェント] ではなく、[Asset Management 仮想エージェント] として [コンピュータ プロパティ] ダイアログ ボックスの [エージェント] タブに表示されます。[エージェント] タブには、エージェント名や登録といったその他のエージェント関連情報も表示されます。

### エージェント情報を表示する方法

1. コンピュータを右クリックし、[プロパティ] を選択します。  
[コンピュータ プロパティ] ダイアログ ボックスが開きます。
2. [エージェント] タブをクリックします。

AM リモート エージェントについては、エージェントの説明として [コンポーネント] 列に「Asset Management 仮想エージェント」と表示されます。

## Windows リモート エージェント ホスト上での Plink の設定

Client AutomationAM リモート エージェントは、多くの種類のリモート ホストと通信するために、SSH クライアントとして Plink (PuTTY Link) をインストールして使用します。ただし、指定したユーザを使用し、Plink が新しいターゲットに初めて接続する場合、セキュリティ対策としてホスト キーを表示し、ホストが適切かどうかを対話的に確認します。AM リモート エージェントでは、そのようなユーザとの対話機能がサポートされていないため、インベントリを収集する前に Plink を再度確認する必要があります。

Plink ではリモート ホストのキーをレジストリに保存するので、便利なログイン ユーザ用にそのようなレジストリ エントリを生成した後、Asset Management エージェントが実行時に使用する LocalSystem アカウンの下に同じキーを保存することができます。

### レジストリ エントリを生成し、ホスト キーを LocalSystem アカウントの下に保存する方法

1. まだ実行していない場合、PuTTYgen を使用して公開 SSH キーと秘密 SSH キーのペアを生成し、公開鍵をターゲットにインストールします。
2. 通常のログイン ユーザを使用し、インベントリを収集するリモート ホストに対してコマンド ウィンドウからコマンドを実行します。以下のコマンドを使用します。

```
"C:\Program Files\CA\DSM\Agent\units\00000001\um\plink" -ssh -i
"private_key_file" root@target ls
```

変数 *private\_key\_file* はファイルの絶対パスで、*target* はリモート ホスト名です。Client Automation が別の場所にインストールされている場合は、Plink パスを調整します。

3. PuTTY からサーバのホスト キーがレジストリにキャッシュされていないため、キーを追加するかどうかを確認するメッセージが表示された場合、キーを追加することを選択します。コマンド (この例では ls) が正常に実行されます。実行されない場合、SSH キー ファイルを確認し、必要な場合には繰り返します。
4. regedit または他のレジストリ エディタを使用して、レジストリにキャッシュされたキーを検索します。  
HKEY\_CURRENT\_USER\Software\SimonTatham\putty\SshHostKeys の下を確認します。このキーを一時ファイルにエクスポートします。
5. HKEY\_CURRENT\_USER のすべての出現箇所を LocalSystem SID である HKEY\_USERS\S-1-5-18 で置換してエクスポート ファイルを編集します。編集したファイルを保存します。

6. regedit で、編集したファイルをインポートします。
7. 「HKEY\_USERS\S-1-5-18\Software\SimonTatham\putty\SshHostKeys」 キーにリモートホストのエントリが含まれていることを確認します。

Plink は、AM リモート エージェントでインベントリを収集する各ホストに設定する必要があります。そのため、ホスト キーを生成するためにすべてのリモートホストに接続し、上記のエクスポートとインポート手順を一度実行します。

Plink が LocalSystem アカウントに対して正しく設定されていないと思われる場合は、アセット管理エージェントを実行 (“caf start amagent”) して、すべての IAM プロセスが終わるのを待ち、そのあとでトレース ファイル

TRC\_UAM\_amvminvux\_\*.log を確認してください。「サーバのホスト キーはレジストリにキャッシュされていません。」というメッセージを検索します。そのようなエラーが見つかった場合、Plink は正しく設定されていません。さらに、「アクセスが拒否されました」というエラーがトレース ファイルにあれば、これは通常リモートホストへのアクセスに使用した認証情報に問題があったことを意味します。たとえば、誤ったパスワードや SSH キーなどです。

注：Plink の詳細情報については、以下の Web サイトで PuTTY/Plink マニュアルを参照してください：<http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html>

## 非常駐インベントリ

非常駐インベントリ (NRI) ソリューションは、Windows、Linux、UNIX コンピュータシステムのインベントリ (一覧) 作成を、CA Client Automation エージェント (DSM エージェント) を展開せずに簡単に行う方法を提供します。

NRI ソリューションは既存の Client Automation インベントリ コンポーネントをベースにしており、インストールしたエージェントベースの検出が提供するのと同じ強固な検出機能を提供しますが、インベントリ スキャンを実行する前または後の CA ソフトウェアがインストールされていないコンピュータシステム上で機能します。

3 つの異なるレベルの検出機能が提供されており、各々のレベルはインストールした NRI Web サイトからアクセス可能です。このサイトは、システムの一覧を作成するためにアクセスする必要があります。ただし NRI エージェントは、ログインスクリプトを介して実行することもできます。

NRI ソリューションはカスタマイズ可能であり、ニーズに合わせた独自のレベルまたはパッケージを作成可能になります。

## 要件

非常駐インベントリでは、次のコンポーネントがすでにインストールされている必要があります。

- WAC (Web Administration Console)
- DSM Web サービス
- スケーラビリティ サーバ
- CA Asset Collector

## NRI 選択的インベントリの起動

NRI 選択的インベントリ Web ページは、ホスト Web サーバへのアクセス権を持つすべてのユーザからすぐにアクセスできるようになります。

**重要：**受信インベントリ フォルダと Asset Collector フォルダは、ユーザが手動で設定する Internet Guest Account で完全アクセス可能でなければなりません。変更するフォルダの詳細については、「[NRI Web サービスの設定](#)」を参照してください。

NRI Web ページに移動するには、サポートされている Web ブラウザに以下の URL を入力します。サポートされている Web ブラウザの詳細については、[認定マトリックス](#)を参照してください。

`http://webserver-hostname/wac/jsp/ei/ei.jsp`

以下の図に示すように、NRI Web ページは Client Automation WAC システムをベースにしており、定義されているインベントリ レベルやパッケージの概略が表示されます。

### 選択的インベントリ

#### 指示

- お使いのコンピュータに対して、ハードウェア/ソフトウェア インベントリのスキャンを実行してください。
- 完了したら、コンピュータが管理データベースに登録され、関連するインベントリデータがアップロードされます。
- 最初に以下のオプションのいずれかを選択し、メッセージが表示されたら [実行] をクリックしてインベントリ スキャンを開始してください。
- この操作の間は、コンピュータにソフトウェアはインストールされません。
- 注: Firefox ブラウザを使用している場合、[実行] ボタンは表示されない可能性があります。その場合、実行ファイルを既知の場所に保存し、ブラウザを使用しないで実行してください。インベントリ スキャンの完了後は実行ファイルを手動で削除できます。

#### クイック スタート

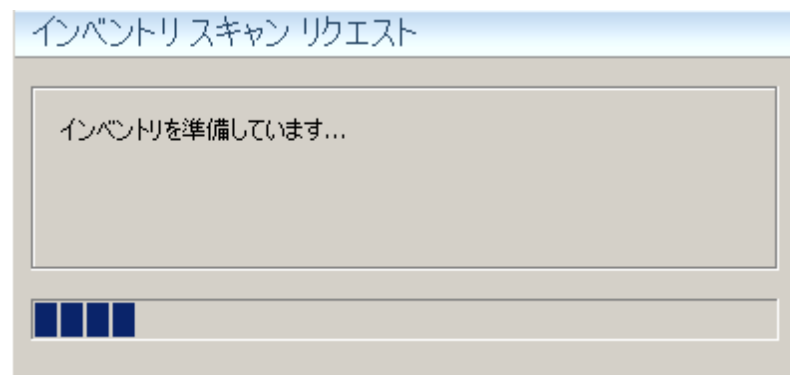
|                                                                                     |                                                                        |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------|
|  | <b>基本スキャン</b><br>コンピュータ上のハードウェアおよびソフトウェアの高速スキャンを実行する場合に選択します。          |
|  | <b>インベントリ詳細スキャン</b><br>コンピュータ上のハードウェアおよびソフトウェアの広範なインベントリを実行する場合に選択します。 |
|  | <b>アセット登録</b><br>インベントリを収集および配布することなしにコンピュータを迅速に登録します。                 |

インベントリを起動するには、[クイック スタート] ポートレットの中のパッケージの 1 つを、イメージをクリックして選択します。（各パッケージの収集内容と実行内容の詳細は、[NRI エージェント パッケージ](#)を参照してください。）



各リンクは、指定バージョンの **NRI Primer** 実行ファイルを指しています。ファイルを「実行」するのか「保存」するのかを **Web** ブラウザでたずねられたら、「実行」を選択してください。 **NRI Primer** がダウンロードされて実行されます。

以下の図は、インベントリ スキャン要求の進行状況を示します。



必要な検出モジュールをダウンロードして実際のインベントリを実行するのに要する時間は、**NRI** ホスト **Web** サーバの現在の負荷によって異なります。特に[インベントリ詳細スキャン] オプションの場合、インストールしたハードディスク上のファイル数がこの時間に影響を及ぼすことがあります。

スキャンは、完了するのに最短 **1** 分から、最大で **30** 分以上かかることもあります。スキャン プロセスではコンピュータ リソースのかかなりの部分を利用しますが、通常はスキャン全体で使用可能です。

メッセージ ダイアログに、スキャンがいつ終了するかが表示されます。

## Linux または UNIX コンピュータからの NRI の起動

Linux または UNIX では、NRI Web サイトから NRI を起動できません。これらのオペレーティング システム上で、NRI は最小要件で実行されるように設計されています。NRI エージェントの配布および収集された結果の分析は、手動で行われます。

### Linux または UNIX コンピュータから NRI を起動する方法

1. コマンド シェルから、以下を実行します。

```
<dvd_root>/ProductFiles_x86/nriagent/nriagent.tar
```

注：nriagent.tar ファイルは、プラットフォーム固有のフォルダの下にあります。これを任意の共有のロケーションにコピーして、NRI を起動することもできます。

2. 以下のコマンドを使用して、任意のロケーションにファイルを抽出します。

```
tar -xf nriagent.tar
```

ファイルは、フォルダ「*nriagent*」に抽出されます。

3. コンピュータを登録するには、以下のスクリプトを実行します。

```
./cmnriagent --script register.ini
```

インベントリ ファイルが作成され、コンピュータが登録されます。

4. NRI は以下の 2 種類のインベントリを実行できます。

- 基本的なハードウェア インベントリとヒューリスティック ソフトウェア スキャン
- 完全なハードウェア インベントリとソフトウェア シグネチャ スキャン。

基本的なハードウェア インベントリおよびヒューリスティック ソフトウェア スキャンを実行するには、以下のスクリプトを実行します。

```
./cmnriagent --script basic.ini
```

完全なハードウェア インベントリおよびソフトウェア シグネチャ スキャンを実行するには、以下のスクリプトを実行します。

```
./cmnriagent --script adv.ini
```

注：別のインベントリ モジュールを使用するには、.ini ファイルをカスタマイズして、「nriagent」フォルダにコピーします。

インベントリのスキャンが開始され、インベントリ レポートが「nriagent」フォルダに作成されます。nriagent フォルダの実際の名前は、この名前の前に、たとえば、「12FDBEBA-572D-4408-BFC8-E7922AD4A998.xiu」というような、コンピュータで生成されたホスト UUID が付きます。

5. インベントリ レポートを、実行中の **Asset Collector** に属する「**AssetCollectorCollect**」フォルダの 1 つにコピーします。

**Asset Collector** は新しいインベントリ ファイルを検出し、アセット インベントリ情報を抽出します。

## NRI エージェント パッケージ

スキャンが要求されたときに、定義済みの **NRI エージェント パッケージ** のセットが作成されます。パッケージは、**NRI エージェント実行ファイル**、必要なライブラリ、そしてインベントリ検出モジュールとそれらに必要なライブラリからなります。すべてのファイルは 1 つのフォルダに置かれており、様々なパッケージが共通のライブラリを共有することを意味しています。デフォルトのパッケージの場所は、...¥DSM¥Web Console¥webapps¥wac¥jsp¥ei¥wl¥windows¥packages です。たとえば、C:¥Program Files¥CA¥DSM¥Web Console¥webapps¥wac¥jsp¥ei¥wl¥windows¥packages などです。

以下の 3 つのパッケージが作成されます。

- 基本スキャン

基本インベントリ スキャナとヒューリスティック スキャナを実行します。

- 拡張スキャン

一般インベントリ スキャナとソフトウェア シグネチャ スキャナを実行します。

- アセット登録

アセットを、簡単かつすばやく登録します。ハードウェア インベントリもソフトウェア情報も報告されません。

## 報告される情報

NRI エージェントは標準の DSM エージェント コンポーネントを使用しますが、NRI エージェントが報告するインベントリが DSM エージェントが報告するよりも少なくなる可能性があります。この理由は、上で説明した使用事例のいくつかでは、NRI エージェントが標準のドメイン ユーザ アカウントを持つユーザによって実行される可能性があり、この場合一般に、通常の DSM エージェントが実行されるローカル システム アカウント（または管理者アカウント）よりも権限が少なくなってしまう。NRI エージェントは、実行されるときの権限に基づいて、可能な限り多くの情報を収集します。

NRI エージェントは、次の 3 つの手法を使用してハードウェア インベントリ情報を取得します。

- 標準の Windows API 機能呼び出す
- レジストリ キーを読み取る
- SMBIOS インベントリ データを収集するデバイス ドライバをインストールして実行する。最も詳細なハードウェア インベントリ情報は、この SMBIOS メカニズムによって収集されます。SMBIOS データが収集されると、デバイス ドライバは削除されるため、一覧作成されたシステムの設定に影響が残るということはありません。デバイス ドライバのインストールでは権限が必要であるため、NRI エージェントが特権ユーザとして実行されない限り、詳細な SMBIOS データは収集できません。
- NRI エージェントは、3 つの異なるメモリ値を収集します。
  - OS がレポートするメモリ  
この値は、オペレーティング システムによりレポートされる、ビデオアダプタなどのデバイスが使用する量を引いた後で残っているメモリ量になります。
  - 物理メモリ使用率  
この値は、メイン ボードに搭載されているメモリになります。
  - メモリ合計  
この値は、上の 2 つの値のうち大きいほうの値です。

注：物理メモリは、NRI エージェントを制限ユーザのコンテキストで実行している場合はレポートされません。

NRI エージェントをリモート デスクトップ 接続を介して実行している場合、いくつかの値は実際の値と異なってレポートされる可能性があります。

ヒューリスティック ベースのソフトウェアスキャンの場合、NRI エージェントはインストールされているソフトウェアの詳細を、以下を調べることで取得します。

- Windows MSI データベースを調べて、インストールされている MSI パッケージの詳細を取得します
- Windows の「ソフトウェアの追加/削除」リストを調べます

シグネチャベースのソフトウェア スキャンの場合、インストールされたソフトウェアの検出は、NRI エージェントに有効なソフトウェア コンテンツ シグネチャに依存します。NRI エージェントには最新のコンテンツ シグネチャが付属していますが、DSM 管理者は、シグネチャ コンテンツ ファイルを 1 つ置き換えるだけで、このシグネチャを新しいコンテンツ定義で更新できます。

NRI エージェントを制限ユーザが実行していると、レポートされるソフトウェア インベントリの量は、管理権限を持つユーザによりレポートされる量と異なることがあります。ヒューリスティック ソフトウェアの場合、ユーザが使用できるアプリケーションのみがレポートされます。シグネチャ スキャンの場合、いくつかのシグネチャについては、ファイル アクセス制限のために、アプリケーションがインストールされているかの確認が禁じられる可能性があります。

ユーザが管理者である場合、デフォルト パッケージは信頼レベル 5 を返します。ユーザが制限ユーザの場合、信頼レベルとして 3 が返されます。収集インベントリでのレポート中は、レポートされる信頼レベルについて注意することが重要です。

いずれかのアセットが以前にフル DSM エージェントによってインベントリ処理されている場合、そのインベントリが管理者によって収集されているのであれば（信頼レベル 5）、NRI インベントリがそのインベントリを上書きします。管理者でないユーザの生成した NRI インベントリは、DSM エージェントによって収集されたインベントリを上書きしません。

レポートされることが予想されるインベントリ情報の一覧については、[「レポートされるインベントリ項目のリスト」](#) (P. 583)を参照してください。

## シグネチャ データベースの更新

拡張スキャン パッケージでは、Client Automation ソフトウェア シグネチャ スキャナによるソフトウェア検出が可能です。シグネチャ スキャナは、シグネチャ データベースを使用してインストールされたソフトウェアを認識します。非常駐インベントリ ソリューションのインストール中、シグネチャ データベース ファイルのバージョンもインストールされます。

Client Automation システムは、Client Automation コア システムに新しいシグネチャを自動的にダウンロードして、実際の Client Automation エージェントと一緒に使用します。また、作成されたカスタム シグネチャを追加することもあります。しかし、非常駐インベントリ ソリューションはこれらの自動更新には含まれないため、これらの更新は手動で実行する必要があります。

### 拡張スキャン パッケージが使用するシグネチャ データベースを手動で更新する方法

1. 非常駐インベントリ ソリューションのホスト サーバでファイル エクスプローラを開きます。
2. ...DSM¥ServerDB¥SECTOR¥SSFW フォルダへ移動します。  
このフォルダには、W0000xxx.zml ファイルの一覧が入っています。
3. 一番大きな番号の .ZML ファイル、たとえば W0000084.zml を見つけてください。
4. このファイルを Web Console¥webapps¥wac¥jsp¥ei¥wl¥windows¥packages にコピーします。
5. Web Console¥webapps¥wac¥jsp¥ei¥wl¥windows¥packages に移動します。
6. w0000001.zml という名前のファイルを削除します。
7. コピーしたファイルの名前を w0000001.zml に変更します。

## プライマ スクリプトの数の制限

「選択的インベントリ」Web ページからパッケージの数を制限するための 2 つのオプションがあります。Web ページは、利用可能なプライマ スクリプトに基づいて動的に作成されています。

プライマ スクリプトは、NRI ソリューションをホストする Web サーバ上にある ...DSM¥Web Console¥webapps¥wac¥jsp¥ei¥wl¥scripts フォルダに配置されています。ファイル名によって、各スクリプトの目的がわかります。

注：詳細については、「NRI プライマ スクリプト ファイル」を参照してください。

### Web ページからオプションを削除する方法

1. スクリプト フォルダからファイルを削除するか、ファイルの拡張子を “.wlscr” 以外の拡張子に変更します。
2. ファイルを削除や名前変更した後で、Client Automation Tomcat サービスをコマンドプロンプトから再起動して、次のコマンドを入力します。

```
caf stop tomcat
```

```
caf start tomcat
```

**重要：** Web 管理コンソールや NRI Web ページはアクセス不可能になり、現在ログオンしているユーザのセッションは Tomcat サービスが停止している間に失効します。

また、リストされるスクリプトを 1 つのスクリプトだけに限定することもでき、そのためにはスクリプト ファイルの名前を、たとえば次のように URL の一部として指定します。

```
http://webserver-hostname/wac/jsp/ei/ei.jsp?script=2adv
```

この例では、リストを拡張インベントリ スキャン パッケージのみに限定します。

## Web ページのカスタマイズ

「NRI 選択的インベントリ」 Web サイトを、組織の標準を順守するようにカスタマイズできます。

NRI ソリューションのメイン ページは “ei.jsp” であり、...¥DSM¥Web Console¥webapps¥wac¥jsp¥ei フォルダにあります。

**重要：** ファイル内のサーバ側スクリプト タグを変更や上書きしないでください。サーバ側のコードは、“<%” starting tag, and a “%>” エンコード タグでカプセル化されています。

Web ページが現在使用しているイメージは、...¥DSM¥Web Console¥webapps¥wac¥jsp¥ei¥images フォルダにあります。 CA ログファイルは “circleca.png” という名前で、組織と一致するロゴと置き換えることができます。また、このフォルダに新しいロゴファイルを置くこともできます。“ei.jsp” ファイルの中の参照を、新しいロゴを指すように変更する必要があります。

ページに表示されるラベルは、...¥DSM¥Web Console¥webapps¥wac¥WEB-INF¥classes¥com¥ca¥wac¥ei¥i18n フォルダにある “i18n\_ei.properties” という名前のファイルに具体化されます。

各々の変更を有効にするには、Tomcat サービスの再起動が必要です。次のコマンドを実行して、Tomcat サービスを再起動します。

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

注： Web サイトに変更を加える前に、ファイルをバックアップしてください。

## NRI Web サービスの設定

NRI Primer は、新しい NRI Web サービスを使用してホスト Web サーバのファイルをダウンロードしたりアップロードします。NRI Web サービスは、DSM エクスプローラから変更および適用が可能な Client Automation 共通設定ポリシーを介して設定できます。（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」を参照してください。）

NRI Web サービス固有のポリシーは、DSM エクスプローラ ツリーの [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] - [Web サービス] - [非常駐インベントリ] にあります。



## 非常駐インベントリ ポリシー グループ

非常駐インベントリ ポリシー グループでは、NRI Web サービスの動作を制御する既存の設定ポリシー パラメータの表示と編集ができます。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。

### ファイルを Asset Collector にコピーする

NRI Web サービスが受信したインベントリ レポートをローカルの Asset Collector にコピーするかどうかを指定します。有効な場合、ファイルは Asset Collector の最初に設定した収集フォルダに置かれます。有効な値は、1 (= 有効) と 0 (= 無効) です。

デフォルト : 1

**重要：** 収集フォルダがデフォルトの収集フォルダと異なる場合（つまり、DSMROOT フォルダである `c:\program files\ca\dsm` に対する `AssetCollectorCollect`）、このフォルダは、ユーザが手動で設定する Internet Guest Account で完全アクセス可能である必要があります。

### Asset Collector へのコピーの後でファイルを削除する

NRI Web サービスがファイルを Asset Collector フォルダにコピーした後で、受信したインベントリ フォルダから削除するかどうかを指定します。このポリシーは、「Asset Collector へファイルをコピー」ポリシーが 1 に設定されている場合にのみ承認されます。有効な値は、1 (= 有効) と 0 (= 無効) です。

デフォルト : 0

### 有効

NRI Web サービスがファイルのダウンロードまたはインベントリのアップロードリクエストを受け入れるかどうかを示します。有効な値は、1 (= 有効) と 0 (= 無効) です。

デフォルト : 1

### 受信したファイルが保存されるフォルダ

NRI Web サービスが受信したインベントリ レポートをどこに置くかを指定します。このフォルダを完全修飾しない限り、DSMROOT フォルダの相対位置、たとえば `c:\program files\ca\dsm` に置かれます。

デフォルト : NRIReceivedReports

**重要：** デフォルト値が異なるフォルダに変更される場合、このフォルダは、ユーザが手動で設定する **Internet Guest Account** で完全アクセス可能である必要があります。

## ログイン スクリプトからの NRI エージェントの実行

「選択的インベントリ」Web ページを使用する方法に代わる方法として、たとえばログインスクリプトや USB メモリ スティックを使用して、NRI エージェントを直接実行することができます。

NRI エージェントの実行ファイル `cmNriAgent.exe` は、`...¥DSM¥Web Console¥webapps¥wac¥jsp¥ei¥wl¥windows` フォルダに、必要なすべてのインベントリ モジュールおよびサポート ライブラリと一緒に入っています。

このフォルダには、3 つのプライマ スクリプトに対応した 3 つのスクリプト ファイルと「選択的インベントリ」ページにあるオプションもあります。スクリプトの 1 つを使用して NRI エージェントを実行するには、次のコマンドをコマンドプロンプトから実行します。

```
cmNriAgent.exe -script .¥basic.ini
```

このコマンドは NRI エージェントを実行し、コンピュータ上の生成されたホスト UUID の名前を取ってインベントリ レポート（たとえば `12FDBEBA-572D-4408-BFC8-E7922AD4A998.xiu`）を作成します

このファイルは、実行中の Asset Collector に属している収集フォルダの 1 つにいつでも手動でコピーできます。

注： 詳細については、CA Asset Collector のセクションを参照してください。

NRI エージェントは、コマンドラインで“-o” 引数を使用すると、出力ディレクトリを Asset Collector フォルダへ向けるように設定することもできます。NRI エージェントの機能の詳細は、次のセクションをお読みください。

USB メモリ スティックを使用して NRI エージェントを実行することも簡単にできます。`...¥DSM¥Web Console¥webapps¥wac¥jsp¥ei¥wl¥windows` のすべてのファイルを USB スティックにコピーするだけです。次に NRI エージェントを、次のようにして呼び出します。出力がメモリ スティックのサブフォルダに送信されるように指定することをお勧めします。

```
cmNriAgent.exe -script .¥basic.ini -o .¥reports
```

注： NRI エージェントは出力フォルダが存在することを想定しているため、存在しなければ失敗します。

## NRI エージェント

非常駐インベントリ ソリューションのコア コンポーネントは、新しい **NRI エージェント** です。このエージェントは既存の **Client Automation** インベントリ検出モジュールの内部作業を知っており、これらのモジュールの出力を **Asset Collector** が認識する **XML** ファイルに変換できます。

**NRI エージェント** は手動で実行され、コマンドラインまたはスクリプト ファイルから、あるいはこれらの組合せから制御されます。

## コマンドライン

以下の表に、**NRI エージェント** が認識するコマンドライン スイッチを示します。

| コマンド                     | 説明                                                                                        |
|--------------------------|-------------------------------------------------------------------------------------------|
| -o "<output path>"       | エージェントがインベントリ <b>XML</b> ファイルを置く場所を指定します。                                                 |
| -origin "wished origin"  | アセットの発行元を指定します。発行元の詳細は、 <b>Asset Collector</b> のマニュアルを参照してください。                           |
| -trustlevel <trustlevel> | アセットの信頼レベルを指定します。信頼レベルは、1 から 5 までの数値です。信頼レベルの詳細は、 <b>Asset Collector</b> のマニュアルを参照してください。 |
| -file "<file name>"      | 出力ファイルは、デフォルトでは、生成されたホスト <b>UUID</b> を使用して命名されます。これは、このパラメータによって上書きできます。                  |
| -nohw                    | ハードウェア インベントリを収集しません。                                                                     |
| -nosw                    | ソフトウェア インベントリを収集しません。                                                                     |
| -script <script file>    | スクリプト ファイルの場所。                                                                            |

## スクリプト ファイル

エージェントは、スクリプト ファイルを通じて実行したり何をするかを指示します。スクリプトには、コマンドラインで提供されるオプションのいくつかが明記されています。オプションがコマンドラインだけでなくスクリプト ファイルでも指定されている場合、コマンドラインの指定が優先されます。

注：デフォルトの設定スクリプト ファイルを変更する場合、ファイルは `...¥DSM¥Web Console¥webapps¥wac¥jsp¥ei¥wl¥scripts` フォルダにあります。それぞれのファイル名は、`1basic.wlscr`、`2adv.wlscr`、および `3register.wlscr` です。

スクリプト ファイルには、必ず **General** セクションが必要です。

```
[General]
OutputFolder=.¥
OutputFile=
Origin=CA Elective Inventory
Trustlevel=5
TrustlevelRestrictedUser=3
KeepHostkey=Yes
ProcessPriority=0-3
```

以下の表には、**[General]** セクションで使用可能なパラメータが含まれます。

| パラメータ                    | 説明                                                                                                                                                  |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| OutputFolder             | エージェントがインベントリ XML ファイルを置く場所を指定します。                                                                                                                  |
| OutputFile               | 出力ファイルを指定します。デフォルトでは、出力ファイルは生成されたホスト UUID を使用して命名されます。これは、このパラメータによって上書きできます。                                                                       |
| Origin                   | アセットの発行元を指定します。発行元の詳細は、 <b>Asset Collector</b> のマニュアルを参照してください。                                                                                     |
| Trustlevel               | アセットの信頼レベルを指定します。信頼レベルは、1 から 5 までの数値です。信頼レベルの詳細は、 <b>Asset Collector</b> のマニュアルを参照してください。                                                           |
| TrustLevelRestrictedUser | NRI エージェントが制限ユーザによって実行されている場合に、そのユーザの信頼レベルを指定します。制限ユーザには管理者と同じ情報へのアクセス権がないため、レポートされる情報を信頼できるとみなすことはできません。<br>この項目が指定されていない場合、“trustlevel” 値が使用されます。 |

| パラメータ                   | 説明                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KeepHostkey<br>(オプション)  | <p>このパラメータが指定されて値が「はい」の場合、エージェントは生成されたホストキーをレジストリに残します。値が「いいえ」の場合、このキーは削除されます。デフォルトは「はい」です。実際の <b>Client Automation</b> エージェントを後でプッシュする予定であれば、ホストキーを残しておいてください。 <b>Client Automation</b> エージェントはホストキーを再使用するため、このホストキーを選択的にスキャンしたエージェントと結合するのが容易になります。</p>                                                                                                |
| ProcessPriority (オプション) | <p><b>Client Automation</b> エージェントが起動したサブプロセスの優先度を制御するために使用します。デフォルト値は <b>0</b> (アイドル) であり、サブプロセスは他のプロセスが使用していない <b>CPU</b> のみを使用することを意味します。</p> <p>設定可能な値は以下のとおりです。</p> <ul style="list-style-type: none"><li><b>0</b> = アイドル (デフォルト)</li><li><b>1</b> = 低</li><li><b>2</b> = 通常</li><li><b>3</b> = 高</li></ul> <p>注：実際の優先順位は <b>OS</b> によって制御されます。</p> |

## スクリプト ファイル：Inventory セクション

どのインベントリ検出モジュールを実行するかを指定するには、「Inventory」セクションをスクリプト ファイルに追加する必要があります。このセクションを省略すると、エージェントは基本インベントリ スキャナをデフォルトで実行します。

### 例：Inventory セクション

```
[Inventory]
Method=0/1/2

ScanRestrictedUser=0/1
AdditionalModules=1
Module1Binary=vistainv.exe
Module1Commandline=-o inv.out
Module1Outputfile=inv.out
Module1Cleanup=inv.out,tmp.bak
TemplateModules=1
Template1=user_information.tpl
```

以下の表には、[Inventory] セクションで使用可能なパラメータが含まれます。

| パラメータ              | 説明                                                                                                                                                                        |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Method             | デフォルト インベントリ モジュールの 1 つを指定します。値は、以下のいずれかになります。<br>0 = どのデフォルト モジュールも実行されません。<br>1 = 基本インベントリ モジュールを実行します。約 4KB の情報を作成します。<br>2 = 一般インベントリ モジュール全体を実行します。約 30KB の情報を作成します。 |
| ScanRestrictedUser | 制限ユーザに対してハードウェア インベントリ スキャンを実行するべきかどうかを示します。<br>0 = いいえ。制限ユーザはスキャンされません。<br>1 = はい（デフォルト）                                                                                 |
| AdditionalModules  | 実行する追加モジュールの数を指定します。エージェントは 1 から指定されたモジュール数までを反復し、ModuleXBinary 項目、ModuleXCommandLine 項目、ModuleXOutputfile 項目、および ModuleXCleanup 項目からモジュール情報を読み取ります。                      |
| ModuleXBinary      | インベントリ モジュールを格納するファイルの名前を指定します。                                                                                                                                           |

| パラメータ              | 説明                                                                                                                                                                                                                      |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ModuleXCommandline | インベントリ モジュールの実行に使用するコマンドラインを指定します。                                                                                                                                                                                      |
| ModuleXOutputfile  | インベントリ モジュールが保管する情報の保管場所であるファイルの名前を指定します。                                                                                                                                                                               |
| ModuleXCleanup     | エージェントがモジュール実行の後で削除するファイルのカンマ区切りリストを指定します。ファイルは、パスで指定できます。                                                                                                                                                              |
| TemplateModules    | <p>ユーザに要求するインベントリ テンプレート モジュールの数を指定します。</p> <p><b>注：</b> NRI 選択的インベントリを通じてテンプレート インベントリを実行するために、以下のファイルを <b>NRI</b> プライマ スクリプト ファイルのダウンロードセクションに追加する必要があります。</p> <p><b>amtplw32.exe、amtext.enu および amm2iw32.exe</b></p> |
| TemplateX          | テンプレート ファイルのファイル名を指定します。 テンプレート ファイルは <b>MIF</b> 形式であり、 <b>DSM</b> エクスプローラを使用するか、 <b>gui_am_tpledit.exe</b> を <b>Client Automation</b> インストールから手動で起動することにより作成できます。                                                      |



## スクリプト ファイル：Software セクション

ソフトウェア インベントリ スキャンの制御は、スクリプト ファイルの「Software」セクションで行われます。

### 例：Software セクション

```
[Software]
Method=0/1/2

ScanRestrictedUser=0/1
```

以下の表には、[Software] セクションで使用可能なパラメータが含まれます。

| パラメータ              | 説明                                                                                                                                                                                 |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Method             | 使用するソフトウェア スキャン方法を指定します。値は、以下のいずれかになります。<br>0 = ソフトウェア スキャンを実行しません。<br>1 = MSI とデータベース追加/削除をスキャンするヒューリスティック スキャナを実行します。<br>2 = CA 提供のシグネチャ データベースを使用してソフトウェアを認識するシグネチャ スキャナを実行します。 |
| ScanRestrictedUser | 制限ユーザに対してソフトウェア インベントリ スキャンを実行するべきかどうかを示します。<br>0 = いいえ。制限ユーザはスキャンされません。<br>1 = はい（デフォルト）                                                                                          |

## NRI プライマ

NRI プライマは、NRI ソリューションのホストである「Web コンソール」Web ページ間でリンクされているバイナリです。ただし、必要であれば Web Launcher をディスクまたはネットワーク共有から直接実行することができます。

NRI Primer のサポートされているオペレーティング システムについては、[認定マトリックス](#)を参照してください。

NRI ソリューションの主な役割は、NRI エージェントを実行することと、一覧作成されたコンピュータと Client Automation ドメインマネージャ間のイントラネットまたはインターネット上での通信方法を促進することです。通信は、新しい Web サービス方法のセットを使用して行われます。

## スクリプト ファイル

Web Launcher は、スクリプト ファイルによって制御されます。スクリプト ファイルには、どのファイルをダウンロードして実行するかに関する情報や、ファイルをダウンロードやアップロードする方法やどのサーバにアップロードするかについての情報が含まれています。スクリプト ファイルは INI ファイル形式であり、「General」、「Advanced」、「Platforms」の 3 つのセクションが含まれます。

### スクリプト ファイル：General セクション

「General」セクションは、Web コンソールがリンクを形成したりスクリプトにホスト Web ブラウザのオペレーティング システムのサポートを含むかどうかを決定するために使用する情報からなります。

#### 例：General セクション

```
[General]
Title=Basic Inventory Scan
Description=Select this to perform a basic and fast inventory of your computer.
Image=nri_basic_scan.gif
```

以下の表には、[General] セクションで使用可能なパラメータが含まれます。

| パラメータ       | 説明                                 |
|-------------|------------------------------------|
| Title       | 表示目的のためだけに使用され、WAC でのリンクの作成に使用します。 |
| Description | 一般的な説明です。                          |

| パラメータ | 説明                                                                                                                     |
|-------|------------------------------------------------------------------------------------------------------------------------|
| Image | 「Web コンソール」ページで使用するイメージのファイル名を指定します。イメージは、Web コンソールインストールの共通の「イメージ」フォルダから選択されます。イメージが指定されていない場合、nricustom.gif が使用されます。 |

## スクリプト ファイル：Advanced セクション

「Advanced」セクションは、現在は次の項目のみからなります。

### 例：Advanced セクション

```
[Advanced]
KeepWorkArea=0/1
```

以下の表には、[Advanced] セクションで使用可能なパラメータが含まれます。

| パラメータ        | 説明                                                                                  |
|--------------|-------------------------------------------------------------------------------------|
| KeepWorkArea | デフォルト値は 0 です。値を 1 に設定すると、NRI プライマはダウンロードしたすべてのファイルを削除しません。生成されたインベントリ ファイルも削除されません。 |

## スクリプト ファイル：Platforms セクション

「Platforms」セクションには、スクリプトがサポートするプラットフォームがリストされます。現在は、以下のように 4 つの主なプラットフォームが定義されています。値が「はい」の場合、スクリプトはその言語にサポートされています。値が「いいえ」の場合、またはプラットフォームがリストされていない場合は、プラットフォームはサポートされていません。

### 例：Platforms セクション

```
[Platforms]
Windows=Yes
Linux=Yes
Unix=No
Mac=No
```

## スクリプト ファイル：プライマ <Platform> セクションのダウンロード

サポートされるプラットフォームごとに、スクリプト ファイルには「プライマ <Platform> のダウンロード」セクションが含まれることがあります。このセクションには、プライマが機能するためにダウンロードしなければならないプライマ固有ファイルがいくつかリストされています。

### 例：プライマ <Platform> のダウンロード セクション

```
[Download_Primer_Windows]
Files=2
File1=def_inf.exe
File2=zlib1.dll
```

以下の表には、[プライマ <Platform> のダウンロード] セクションで使用可能なパラメータが含まれます。

| パラメータ | 説明                     |
|-------|------------------------|
| Files | ダウンロードするファイル数を指定します。   |
| FileX | ダウンロードするファイルの名前を指定します。 |

注：上の例でリストされているファイルは、圧縮されているファイルを解凍するために必要なファイルです。

## スクリプト ファイル：<Platform> のダウンロード セクション

サポートされるプラットフォームごとに、スクリプト ファイルには「<Platform> のダウンロード」セクションが含まれています。このセクションでは、**Web Launcher** について、指定されたプラットフォームに何のファイルをどのようにダウンロードするかを説明しています。以下は、**Windows** プラットフォームの例です。

### 例：<Platform> のダウンロード セクション

```
[Download_Windows]
Method=webservice
Executable=cmNriAgent.exe
CommandLine=-script .%adv.ini
Files=2
File1=basic_heuristic.exe
File2=w00000001.zml,w00000001.xml
```

以下の表には、[<Platform> のダウンロード] セクションで使用可能なパラメータが含まれます。

| パラメータ       | 説明                                                                                                   |
|-------------|------------------------------------------------------------------------------------------------------|
| Method      | ファイルのダウンロードに使用する方法を定義します。現在は、"webservice" のみがサポートされています。                                             |
| Executable  | すべてのファイルをダウンロードするときプライマが実行する必要がある実行ファイルの名前を定義します。                                                    |
| CommandLine | 実行ファイルの実行時に使用するコマンドラインを指定します。                                                                        |
| Files       | ダウンロードするファイルの数を指定します。                                                                                |
| FileX       | ダウンロードするファイルの名前を指定します。カンマの後の未圧縮名を指定してください。<br><br>注：(470P.) 詳細については、「ダウンロードのためのファイルの圧縮と解凍」を参照してください。 |

## ダウンロードのためのファイルの圧縮と解凍

いくつかのファイルは非常に大きく、ダウンロードするのにかなり時間がかかることがあります。このため、ファイルを圧縮および解凍することが可能です。ファイルを圧縮するには、**def\_inf.exe** ツールを使用する必要があります。NRI プライマにダウンロード後のファイルを解凍させるには、圧縮した名前と解凍された名前の両方が "FileX" 行で、カンマで区切って指定されている必要があります。

### 例

```
File2=w0000001.zml,w0000001.xml
```

この例では、ファイル "w0000001.zml" が NRI プライマによってダウンロードされて、"w0000001.xml" という名前のファイルに展開されます。ファイルは両方とも作業領域の消去時に削除されます。

## NRI エージェント用の追加インベントリ モジュールの設定

このセクションでは、独自の NRI インベントリ収集モジュールを設定する方法について説明します。

### 前提条件

NRI インベントリ収集モジュールの設定を始める前に、以下のタスクを必ず終了してください。

- 非常駐インベントリに関連するスクリプト ファイルの構造および使用方法を理解します。

注：詳細については、「スクリプト ファイル」を参照してください。

- NRI エージェント用のインベントリ収集モジュールの作成に使用するバイナリを準備します。これらのモジュールによって生成されたインベントリ ファイルの出力形式は、**Asset Management** 対応である必要があります。

完全な手順が、別の例によって説明されています。最初の例では、NRI エージェント用のテンプレート インベントリ収集モジュールの設定方法を説明し、2 番目の例では、NRI エージェント用のユーザ情報収集モジュールの設定方法を説明し、3 番目の例では、ローカライズされた言語を含む **.wlscr** ファイルの設定方法を説明しています。それぞれの例は、各タスクを達成する方法に関する情報を提供します。

## テンプレート インベントリ収集モジュールの作成

NRI エージェント用のテンプレート インベントリ収集モジュールを作成できます。このプロセスに含まれる手順は以下のとおりです。

1. NRI エージェント用のテンプレート ファイルを作成します。
2. INI ファイルを作成します。
3. .wlsr script ファイルを作成します。
4. ファイルを適切なフォルダにコピーします。
5. Tomcat サービスを再起動します。
6. NRI Web ページへアクセスします。
7. 新しいモジュールを実行します。

## NRI エージェント用のテンプレート ファイルの作成

NRI エージェント内で使用されるテンプレート ファイルを作成します。この例として、**Asset Management** からテンプレート ファイルの内容を抜粋しています。ファイルのフォーマットは、**AM** テンプレート ファイルと同じです。この例でのテンプレート ファイルの名前は、**template.tpl** です。

template.tpl ファイルは、以下の内容で作成されています。

```
//
// Asset Management システムを使用して作成された MIF ファイル
//
Start Component

Name = "User Template"

UpdateType = "Never"

UpdateMsg = ""

LastUpdated = ""

Description = "Basic Template for Users"

Start Group

Name = "User Information"

Id = 1

Class = "NETCON|User Information|1.0"
```

```
Description = ""

Start Attribute

 Name = "User Name"

 Id = 1

 Storage = Specific

 Type = String(32)

 Access = Write-Only

End Attribute

Start Attribute

 Name = "First Name"

 Id = 2

 Storage = Specific

 Type = String(64)

 Access = Write-Only

End Attribute

Start Attribute

 Name = "Last Name"

 Id = 3

 Storage = Specific

 Type = String(64)

 Access = Write-Only

End Attribute

Start Attribute

 Name = "Address"

 Id = 4

 Storage = Specific

 Type = String(128)

 Access = Write-Only
```



```
End Attribute

Start Attribute

 Name = "ZipCode"

 Id = 5

 Storage = Specific

 Type = String(32)

 Access = Write-Only

End Attribute

Start Attribute

 Name = "City"

 Id = 6

 Storage = Specific

 Type = String(128)

 Access = Write-Only

End Attribute

Start Attribute

 Name = "Country"

 Id = 7

 Storage = Specific

 Type = String(64)

 Access = Write-Only

End Attribute

Start Attribute

 Name = "Home Phone"

 Id = 8

 Storage = Specific

 Type = String(32)

 Access = Write-Only
```

```
End Attribute

End Group

Start Group

Name = "Company Information"

Id = 2

Class = "NETCON|Company Information|1.0"

Description = ""

Start Attribute

Name = "Department"

Id = 1

Storage = Specific

Type = String(64)

Access = Write-Only

End Attribute

Start Attribute

Name = "Phone"

Id = 2

Storage = Specific

Type = String(32)

Access = Write-Only

End Attribute

End Group

Start Group

Name = "Additional Information"

Id = 3

Class = "NETCON|Additional Information|1.0"

Description = ""

Start Attribute
```

```
Name = "Additional Text"

Id = 1

Storage = Specific

Type = String(256)

Access = Write-Only

End Attribute

Start Attribute

Name = "Default Workstation"

Id = 2

Storage = Specific

Type = String(64)

Access = Write-Only

End Attribute

End Group

End Component
```

## INI ファイルの作成

この例では、`basic.ini` ファイルの内容をコピーして INI ファイル (`tpl.ini`) が作成されています。`basic.ini` は、`..¥DSM¥WebConsole¥webapps¥wac¥jsp¥ei¥wl¥windows¥packages` フォルダにあります。

`tpl.ini` ファイルの内容は以下のとおりです。

```
[General]

OutputFolder=.¥

OutputFile=
```

```
Origin=CA NRI (Tpl Scan)

Trustlevel=5

TrustlevelRestrictedUser=3

KeepHostkey=Yes

[Inventory]

Method=1

ScanRestrictedUser=1

AdditionalModules=0

TemplateModules=1

Template1=template.tpl

[Software]

Method=1

ScanRestrictedUser=1
```

[TemplateModules] オプションの値が **1** に変更されています（この値は、basic.ini ファイルの中では **0** でした）。値 **1** は、テンプレート ファイルが **1** つのみ存在することを示します。

[TemplateModules] オプションには、[Template1] オプションが続きます。このオプションは、テンプレート ファイルの名前を表します。つまり、以下のような行があります。

```
Template1=template.tpl
```

追加するテンプレートが複数ある場合、INI ファイルの中身には以下のように追加オプションを含めます。

```
TemplateModules=3

Template1=template.tpl

Template2=mytemplate2.tpl

Template3=mytemplate3.tpl
```

## .wlscr スクリプト ファイルの作成

tpl.ini ファイルの作成後、このテンプレート インベントリ収集モジュール用に .wlscr スクリプト ファイルを作成します。この例の .wlscr ファイルの名前は、tpl.wlscr です。

以下の tpl.wlscr ファイルの内容を参照し、独自の要件に基づいて以下のオプションを変更する必要があることに注意してください。

- タイトル
- 説明
- -origin description 付きの CommandLine パラメータ
- ダウンロードされるファイルの数
- ファイル名リスト：プライマがどのファイルをターゲット コンピュータにダウンロードするか把握できるように、このスクリプト ファイルに含めるバイナリ名のリストを持つ必要があります。この例では、5つの新規ファイルが追加されています。
  - tpl.ini
  - template.tpl
  - amm2iw32.exe
  - amtplw32.exe
  - amtext.enu

**重要：** このプロセスで面倒なのは、このタスクを実行するのに使用できるバイナリの数およびこのモジュールを実行するのに使用されるコマンドラインを取得することです。これには、どのモジュールがどのインベントリ データを生成するかを定義するための **Asset Management** エージェント機能を理解しているユーザーの専門知識が必要になります。上記のバイナリは、**Asset Management** エージェントのインストールで配信されます。

.wlscr ファイルの内容は以下のとおりです。

[General]

Title=Template Test

Description=コンピュータ上のハードウェアおよびソフトウェアの高速スキャンを実行するには、これを選択します。

Image=nri\_basic\_scan.gif

[Advanced]

KeepWorkArea=0

```
[Platforms]

Windows=Yes

Linux=No

Unix=No

Mac=No

[Download_Windows]

Method=webservice

Executable=cmNriAgent.exe

CommandLine=-script .¥tpl.ini -origin "CA Elective Inventory (Basic Scan+Template)"

Files=20

File1=cmNriAgent.exe

File2=tpl.ini

File3=cainf.dll

File4=cawinexf.dll

File5=cfUtilities.dll

File6=msvcp71.dll

File7=msvcr71.dll

File8=cfTrace.dll

File9=cfTrace.ini

File10=amappw32.exe

File11=cfbasichwnt.exe

File12=cfXMLParser.dll

File13=cfOSServices.dll

File14=cfig40wnt.sys

File15=cfigw32.sys
```

```
File16=cfigw64.sys
```

```
File17=template.tpl
```

```
File18=amm2iw32.exe
```

```
File19=amtplw32.exe
```

```
File20=amtext.enu
```

すべてのファイルが作成されたら、..`¥DSM¥Web`

`Console¥webapps¥wac¥jsp¥ei¥wl¥scripts` フォルダに移動します。そのフォルダに含まれる既存のスクリプトファイルを数え、カウントを 1 ずつ増やします。この新しい数を `tpl.wlscr` ファイルの名前に含めます。たとえば、フォルダに 3 つのスクリプトが含まれている場合は、次のファイルを `4tpl.wlsc` という名前にする必要があります。

## 適切なフォルダへのファイルのコピー

その他のファイルを..`¥DSM¥Web`

`Console¥webapps¥wac¥jsp¥ei¥wl¥windows¥packages` フォルダにコピーします。

この例では、以下のファイルをフォルダにコピーする必要があります。

- `tpl.ini`
- `template.tpl`
- `amm2iw32.exe`
- `amtplw32.exe`
- `amtext.enu`

## Tomcat サービスの再起動

以下のコマンドを使用して Tomcat サービスを再起動します。

```
caf stop tomcat
```

```
caf start tomcat
```

## NRI Web ページへのアクセス

NRI Web ページに移動するには、以下の URL を入力します。

```
http://<webserver-hostname>/wac/jsp/ei/ei.jsp
```

新しいインベントリ収集モジュールがリストに追加されたのが分かります。

## 新しいモジュールの実行

新しいモジュールをクリックして実行します。テンプレート情報が収集され、インベントリ データ セットに追加されます。

## 追加のインベントリ収集モジュールの作成

この例では、NRI エージェント用にユーザ アカウント インベントリ収集モジュールが作成されます。

追加のインベントリ収集モジュールを作成する手順は、テンプレート インベントリ収集モジュールの作成に非常に似ています。

**重要：** 開始する前に、このインベントリ モジュールで使用するすべての必須バイナリを取得しているかを確認してください。また、コマンドプロンプトからモジュールを実行する場合は、これらのモジュールのコマンドラインの実行を調査する必要があります。渡すパラメータ、生成される出力ファイルなどを把握する必要もあります。

このプロセスに含まれる手順は以下のとおりです。

1. INI ファイルの作成
2. .wlscr ファイルの作成
3. 「テンプレート インベントリ収集モジュールの作成」セクションで説明されている手順 4 ～ 7 に従います。



## INI ファイルの作成

バイナリ「**amusernt.exe**」が追加の **DLL** と共に使用されます。この追加バイナリと共に基本インベントリ ファイル リストを使用することで、このインベントリ バイナリが機能します。このバイナリを呼び出すコマンドラインは以下のとおりです。

```
amusernt.ext invdata.inv
```

上記の情報に基づいて、この追加インベントリ収集モジュールの **ini** ファイルが作成されます。この例では、ファイルは **addmod.ini** と名付けられます。

以下のファイルの内容を参照し、独自の要件に基づいて **ini** ファイル内の以下のオプションを変更する必要があることに注意してください。

- 発行元
- **AdditionalModules** : 値に **1** を入力します。これは、実行する追加モジュールが **1** つあることを意味します。追加するモジュールが複数ある場合は、適切な番号を入力します。
- **[AdditionalModules]** フィールドにゼロでない値が入力されている場合は、**basic.ini** ファイルに基づいて以下のフィールドを追加する必要があります。
  - **Module1Bianry=**
  - **Module1Commandline=**
  - **Module1Outputfile=**
  - **Module1cleanup=**

注： [AdditionalModules] フィールドの値が 2 の場合は、モジュール情報の 2 番目のセットは以下のようになります。

- Module2Binary=xxxx.exe
- Module2Commonline=.%xxxx xxxxx
- Module2Outputfile=.%xxxx.txt
- Module2Cleanup=.%xxxx.txt

ファイルの内容は以下のとおりです。

[General]

OutputFolder=.%

OutputFile=

Origin=CA NRI (ユーザ アカウント スキャン)

Trustlevel=5

TrustlevelRestrictedUser=3

KeepHostkey=Yes

[Inventory]

Method=1

ScanRestrictedUser=1

AdditionalModules=1

Module1Binary=amusersnt.exe

Module1Commandline=.%users.inv

Module1Outputfile=.%users.inv

Module1cleanup=.%users.inv

TemplateModules=0

[Software]

Method=1

ScanRestrictedUser=1

## .wlscr ファイルの作成

以下は、この例で使用する .wlscr ファイルの例です。ファイルには、**5addmod.wlscr** という名前が付けてあります。以下の手順で、ファイルの [タイトル] および [説明] を変更できます。さらに、強調表示されたフィールドを調べ、それらのフィールドを変更する必要があるかどうかを確認する必要があります。

[General]

Title= 追加のモジュール テスト

Description= コンピュータ上のハードウェアおよびソフトウェアに加えて**ユーザ アカウント** インベントリの高速スキャンを実行するには、これを選択します。

Image=nri\_basic\_scan.gif

[Platforms]

Windows=Yes

Linux=No

Unix=No

Mac=No

[Download\_Windows]

Method=webservice

Executable=cmNriAgent.exe

CommandLine=-script .\b**5addmod.ini** -origin "CA Elective Inventory (Basic Scan+**User module**)"

Files=17

File1=cmNriAgent.exe

File2=**addmod.ini**

File3=cainf.dll

File4=cawinexf.dll

File5=cfUtilities.dll

File6=msvc71.dll

File7=msvcr71.dll

File8=cfTrace.dll

File9=cfTrace.ini

File10=amappw32.exe

File11=cfbasichwwnt.exe

File12=cfXMLParser.dll

File13=cfOSServices.dll

File14=cfig40wnt.sys

File15=cfigw32.sys

File16=cfigw64.sys

File17=**amusersnt.exe**

手順 4 ～ 7 （すでに上記のセクションで説明済み）に従って、プロセスを完了させます。

## ローカライズされた .wlscr ファイルの設定

独自のバージョンの .wlscr ファイルを変更し、ローカライズされた言語をファイルに含めることができます。これ以降、NRI リンクにアクセスすると、NRI インベントリ オプションはローカライズされた言語で表示されます。

### ローカライズされた .wlscr ファイルを設定する方法

1. たとえば、5addmod.wlscr などの .wlscr ファイルを開きます。

ファイルが開きます。

2. このファイルの中の [General] セクションを変更し、独自の言語を追加します。たとえば、5addmod.wlscr ファイルの中にドイツ語の名前と説明が以下のように追加されています。

[General]

Title= 追加のモジュール テスト

Description= コンピュータ上のハードウェアおよびソフトウェアに加えてユーザ アカウント インベントリの高速スキャンを実行するには、これを選択します。

Image=nri\_basic\_scan.gif

Title\_DE=xxxxxx

Description\_DE=xxxxx.....

ドイツ語のオペレーティング システムで動作するコンピュータ上に DSM サーバをインストールした場合は、情報が表示されます。

注：以下は、ローカライズされたほかの言語に使用される言語トークンです。

- \_ENU：（デフォルト）トークン必要なし
- \_DE：ドイツ語

- `_FR` : フランス語
  - `_JPN` : 日本語
  - `_ES` : スペイン語
  - `_IT` : イタリア語
  - `_KOR` : 韓国語
  - `_PT` : ポルトガル語
3. ファイルを保存してそれを閉じます。  
すべての設定が保存されます。
  4. 以下のコマンドを使用して **Tomcat** サービスを再起動します。  
  
`Caf stop tomcat`  
  
`Caf start tomcat`  
  
Tomcat サービスが開始されます。
  5. **NRI Web** ページにアクセスするための **URL** を入力します。  
  
NRI インベントリ オプション用にローカライズされた言語の独自のバージョンが表示されます。

## DSM レポーター

DSM レポーター ツールでは、データベースからインベントリ情報が抽出されます。クエリ デザイナを使用すると、ユーザはこのデータを評価し、レポートに表示するフィールドを指定することができます。抽出された情報は GUI でフィルタリング、ソート、および要約し、ただちに表示することができます。また、この情報を利用してレポートを印刷したり、ほかのアプリケーション（たとえば、CSV ファイルや HTML ファイルなど）にエクスポートすることもできます。レポートは、エクスプローラと同様のツリー ビューで階層表示されます。また、レポートごとに自動履歴として多数の定義済み結果セットを保持できます。使用しなくなった結果セットが削除されないように、ユーザはその結果セットを選択して保存することができます。

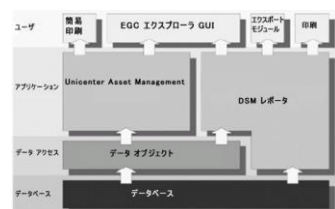
レポート生成は、ユーザが開始することも、スケジュールすることもできます。レポートのスケジュールは、レポーターの GUI で行います。すると、エンジンにより、スケジュールリングプロパティに従ってレポート生成そのものが開始されます。

**注：** インストール後にはじめて DSM レポーターを起動する際には、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 レポーターを再度起動してください。

以下の図は、DSM レポーターがアセット管理環境にどのように埋め込まれているかを示します。



**注：** 定義済みレポートおよび DSM レポーターの詳細については、「DSM レポーター ヘルプ」を参照してください。

## 機能

レポータを使用すると、以下の分類に基づいてレポートを作成できます。

### コンピュータ

メーカー情報、サービス レベル、サマリ、ユーザ関係、仮想マシン レポートなど、コンピュータに固有の情報に関するレポートが含まれています。

### DSM インフラストラクチャ

エンジン情報、およびドメイン内のすべての管理アセットの情報に関するレポートが含まれています。

### ハードウェア

ハードウェア情報に関するレポートが含まれています。

### ネットワーク

ネットワーク情報に関するレポートが含まれています。

### ポリシー

ポリシー関連の情報に関するレポートが含まれています。

### 非管理対象のアセット

非管理対象アセットに関するレポートが含まれています。

### ユーザ

ユーザに固有の情報に関するレポートが含まれています。

これらのデータ タイプを使用すると、高度なレポートを簡単に作成することができます。たとえばソフトウェア インベントリのみに関連するレポートを作成したり、7 種類すべてのデータを混在させることができます。このため、たとえば、**Netscape Navigator** プログラムがインストールされているすべてのコンピュータを検索してから、これらのコンピュータを使用しているユーザの名前をレポートに表示することなどができます。**Reporter** では、ドメイン内の各コンピュータからエージェントにより収集されたさまざまなデータについてデータベースをクエリできます。

**Reporter** には、たとえば以下の機能があります。

- エクスプローラと同様にレポート テンプレートおよび結果の処理が統合され、フォルダおよびテンプレートの構造は無制限にユーザが定義できます。



- 結果は、ただちに GUI で表示できます。
- 結果は、さまざまな形式でファイルにエクスポートできます。
- 一般的なアセット プロパティ、ソフトウェア プロパティ、および実行済みジョブとモジュールのプロパティに関するレポートを生成できます。
- 現在のインベントリ値、および以前に収集された最新の値に関するレポートを生成できます。
- すべてのプロセッサおよびすべてのローカル ドライブなど、固有でない論理インベントリ グループに関するレポートを生成できます。
- 構文が色で強調表示されたポイント アンドクリック フィルタ エディタが備わっています。レポート テンプレートのデフォルト フィルタ、および結果セットごとの個別フィルタリングが備わっています。
- レポートを実行するための SQL スクリプトを作成できます。
- カスタマイズ可能な HTML レポートを印刷できます。

## DSM レポータの開始

DSM レポータは、以下のいずれかの方法で起動できます。

- Windows で、[スタート] - [プログラム] - [CA] - [IT Client Manager] - [DSM レポータ] を選択します。
- DSM エクスプローラのメニュー バーから [ツール] - [DSM レポータ] を選択します。

[レポータ] ウィンドウを使用すると、レポートを表示したり、レポート テンプレートおよびスケジュール レポートを参照したり、新しいレポート テンプレートを作成することができます。右側のペインの [情報] ウィンドウでいずれかの項目をクリックするか、または該当する [内容] 項目を展開します。

ツリー ビューでノードを選択すると、対応する情報またはサブ項目が [Reporter] ペイン内に表示されます。プロパティ シートを使用して、新しい項目を追加したり、既存の項目を編集することができます。一方、必要な情報はすべて DSM エクスプローラで直接表示されるため、通常はデータを表示するためにプロパティ シートまたはダイアログ ボックスを開く必要はありません。HTML ビューでは、ユーザは複雑なレポート定義についてもすばやく概要を把握できます。

## Reporter 環境設定の指定

Reporter 環境設定では、管理者およびすべてのユーザに対する設定が定義されています。レポーター環境設定をカスタマイズして、希望の方法でレポートを表示できます。

### レポーター環境設定を指定する方法

1. メニューバーから [ツール] - [環境設定] をクリックします。  
[環境設定] ウィンドウが表示されます。
2. [管理者] タブをクリックし、管理者の設定を指定します。

#### [ 情報 ] セクション

レポートの情報ペインにヒントを表示するか、または古いスタイルのメッセージボックスを使用するかを定義します。 ヒントには、黄色い電球アイコンのマークが付きます。

#### [ レポートの実行 ] セクション

ユーザ個人の環境設定で、レポートの実行後に行う適切なアクションについて定義します。

#### [ 結果 ] セクション

レポート表示設定を定義します。

3. [グローバル設定] タブをクリックし、管理者のみが変更できる、DSM レポーターのすべてのユーザに影響する設定を指定します。

#### [ 自動結果 ] セクション

[内容] ツリー内の [結果] の下に保持する自動履歴結果セットの数を指定します。 より古い結果をデータベースから完全に削除します。 ユーザ インターフェースに関連して、管理者は、ファイルが含まれるフォルダを削除するように選択することもできます。

#### [ デフォルトで保持するスケジュール済み結果 ] セクション

デフォルトで保持するスケジュール済み結果の数を指定します。

### [ 制限 ] セクション

管理者のみが統計をリセットでき、管理者のみがスケジュールの結果カウントを編集できることを指定します。

### [ ユーザ インターフェース ] セクション

空でないフォルダの削除、整合性確認のパフォーマンスなどを許可します。

### [ エンタープライズ ] セクション

エンタープライズ マネージャでのレポータの実行時に、インポートされた新しいテンプレートにドメイン名を含めることができます。

注：「環境設定」ダイアログ ボックスの詳細については、「DSM レポータ ヘルプ」を参照してください。

## Reporter の操作

DSM レポータの基本ツリー構造は、主にフォルダおよびレポート テンプレートで構成されます。この構造はファイル構造と似ています。フォルダとレポート テンプレートは、ニーズに合わせて作成および編成できます。また、構造には、レポート テンプレートとスケジュール済みレポートのプライマリ プロパティを表す項目、および既存の結果セットを表す項目が含まれます。

## 新しいレポート テンプレートの作成

レポート テンプレートには、レポートの定義が含まれます。レポート テンプレートを作成した後は、これらのレポートを実行することも、特定の時間に実行するようにスケジュールすることもできます。

### 新しいレポート テンプレートを作成する方法

1. [レポート テンプレート] フォルダの下適切なフォルダを右クリックし、[新規レポート テンプレート] を選択します。

[レポート テンプレート タイプ] ダイアログ ボックスが表示されます。

2. レポート テンプレートのタイプを選択し、[OK] をクリックします。

選択したレポート タイプに基づいて、新規レポート タイプダイアログ ボックスが表示されます。

注：[レポート テンプレート タイプ] ダイアログ ボックスおよび新規 レポート タイプダイアログ ボックスの詳細については、「DSM レポータ ヘルプ」を参照してください。

## レポートの実行

今すぐレポートを実行し、レポートの結果セットに追加するには、レポートを右クリックし、[レポートの実行] を選択します。

## レポート テンプレートのエクスポート

エンタープライズ内のあるドメインからほかのドメインにレポート テンプレートをエクスポートし、レポート テンプレートを再利用することもできます。

### 選択したフォルダ (サブフォルダを含む) からレポートをエクスポートする方法

1. [レポート テンプレート] フォルダの下任意のフォルダを右クリックし、[すべてのレポート テンプレートをエクスポート] を選択します。

[レポート テンプレートのエクスポート] ダイアログ ボックスが表示されます。

2. 宛先フォルダを指定し、[サブフォルダから再帰的にテンプレートをエクスポート] チェック ボックスをオンにして [OK] をクリックします。

選択したフォルダおよびそのすべてのサブフォルダ内の使用可能なレポート テンプレートが、宛先フォルダにエクスポートされます。

注：レポートを右クリックして [エクスポート] - [レポート定義] を選択することにより、特定のレポートをファイルにエクスポートすることもできます。

## レポート テンプレートのインポート

ドメイン内で作成されたレポート テンプレートをエクスポートおよびインポートすることによって、そのテンプレートをほかのドメインで再利用できます。

### レポート テンプレートをインポートする方法

1. [レポート テンプレート] フォルダを右クリックし、[レポート テンプレートのインポート] を選択します。  
検索ダイアログ ボックスが開きます。
2. 適切なレポート定義ファイル (.rep) を参照し、[開く] をクリックします。  
テンプレート レポートが[レポート テンプレート] フォルダの下にすぐに表示され、同様に情報ペインにも表示されます。

## レポートのスケジュール

特定の時間に実行されるようにレポートをスケジュールできます。

### レポートのスケジュールを設定する方法

1. レポートを右クリックし、[レポートのスケジュール] を選択します。  
レポートの [プロパティ] ダイアログ ボックスが表示されます。
2. [スケジューリング] タブで、[スケジューリングの設定] をクリックします。  
[スケジューリング プロパティ] ダイアログ ボックスが表示されます。
3. スケジューリング オプションを指定して [OK] をクリックします。  
レポートは、指定した時間に実行されるようにスケジュールされます。

## SQL スクリプトのエクスポート

Reporter では、エクスポート用に SQL スクリプトが生成されます。このオプションは、レポート テンプレートのすべてのフィールドおよびオプションでサポートされている場合にのみ使用可能になります。ローカルな処理が必要なフィールドは SQL で表現できないため、このようなフィールドを含むテンプレートは SQL スクリプトとしてエクスポートできません。

SQL スクリプトはクリップボードまたはファイルにエクスポートできます。レポートを右クリックし、[エクスポート] - [SQL スクリプトをクリップボードにエクスポート] または [SQL スクリプトをファイルにエクスポート] を選択します。

## レポート出力オプション

レポータの結果セットの基本形式は、データベース内の 2 つのテーブルで構成されます。一方のテーブルには、オブジェクトの行（アセットや、レポートに含まれるフィールドに対応する列など）が含まれます。もう一方のテーブルには、結果セットのメタ データ（含まれているインベントリ項目のフル ネームなど）が表示されます。後者のテーブルは「マップ テーブル」と呼ばれ、前者のテーブルが実際の結果テーブルと見なされます。

## GUI での結果の表示

すべての結果セットは、ツリー ビューから選択するだけで GUI で完全に表示できます。[情報] ペインに、レポート定義の基準に合致するすべてのアセットが表示されます。[情報] 列に一般的な結果情報が表示され、結果をフィルタリングしたり（オンとオフを切り替えて、完全な結果セットとフィルタにより定義されたサブセットを比較できます）、フィールドの凡例を表示することができます。

## 結果のプレビューおよび印刷

結果セットは **HTML** ビューでプレビューできます。また、印刷することもできます。印刷結果は **HTML** 生成に基づいており、ユーザがカスタマイズすることができます。カスタマイズには、テーブル生成プロパティやソートなどが含まれます。さらに、ユーザはカスケードスタイルシートへのアクセスおよびこの変更を行うこともできます。カスケードスタイルシートでは、**HTML** 生成のためのほとんどのデフォルトフォーマットオプションが定義されます。

**注：** レポート結果をプレビューまたは印刷するには、レポートを実行する必要があります。

結果をプレビューおよび印刷するには、結果を右クリックして [印刷] を選択します。別個のウィンドウに、**HTML** レポートのプレビューが表示されます。このウィンドウには、以下のボタンがあります。

### 印刷

Microsoft Windows の [印刷] ダイアログ ボックスを開きます。

### ページ設定

ページプロパティを指定するための Microsoft Windows の [ページ設定] ダイアログ ボックスを開きます。

### オプション

結果に使用可能なレイアウトおよびカスタマイズ オプションにアクセスできます。

### 閉じる

現在のウィンドウを閉じます。

## 結果のエクスポート

さまざまな **CSV** および **HTML** 形式用の組み込みエクスポート モジュールを使用すると、結果を外部ツールで使用するためにエクスポートすることが簡単になります。すべてのエクスポートは **GUI** からカスタマイズできます。個々のカスタマイズはそれぞれのスケジュール済みレポートと共に保存されるため、スケジュール済みレポートを非常に柔軟に発行することができます。結果をエクスポートするには、結果を右クリックして [エクスポート] を選択し、必要なエクスポート形式を選択します。

## CA Asset Converter for Microsoft SCCM

CA Asset Converter for Microsoft® SCCM は、Microsoft System Center Configuration Manager (SCCM) に接続し、ハードウェア インベントリやソフトウェア インベントリなどのデータベースに格納されているコンピュータの情報を抽出するコンポーネントです。

CA Asset Converter は、この情報を、ネイティブの DSM Asset Management エージェントが収集する情報とできる限り類似した形式に変換します。この情報は、次に CA Asset Collector で必要とされる形式で一連の XML ファイルに書き込まれます。CA Asset Collector がこれらのファイルを選択すると、Microsoft SCCM データベースに登録されているコンピュータは、ネイティブの DSM エージェントが検出したコンピュータと共に、検出されたハードウェア アセットとして CA MDB に表示されます。関連するハードウェアおよびソフトウェアのインベントリ情報も、同じ方法で格納され構成されます。

ハードウェアまたはソフトウェアのいずれかのインベントリ情報のみを収集するように CA Asset Converter を設定できます。または、インベントリ情報を一切収集しないように設定することもできます。最後の例では、コンピュータ名およびいくつかの基本属性のみが抽出されます。

CA Asset Converter for Microsoft SCCM エンジン タスクは Windows でのみ利用でき、Microsoft System Center Configuration Manager (SCCM) で認定されています。

このエンジン 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。

**重要：** ライセンス情報 CA Asset Converter for Microsoft SCCM は別途ライセンスされるコンポーネントです。このコンポーネントを使用する前に必要なライセンスを購入する場合、CA の担当者にお問い合わせください。ライセンスをすぐに取得しなくても、未ライセンス製品のコンポーネントを 30 日間試用することができます。この期間が過ぎても継続して使用するにはライセンスを購入する必要があります。適切なライセンスを購入しない場合は、ライセンス契約に違反することになります。

**注：** CA Asset Converter for Microsoft SCCM は、Windows システムに DSM エンジンをインストールするとその一部としてインストールされます。ただし、インストール先のシステムではない Asset Collector のインスタンスに出力を配信するように設定することができます。



関連項目：

[Client Automation Asset Management ハードウェア インベントリへの Microsoft SCCM ハードウェア アセット インベントリのマップ \(P. 649\)](#)

[Client Automation Asset Management ソフトウェア インベントリへの Microsoft SCCM ソフトウェア アセット インベントリのマップ \(P. 654\)](#)

## CA Asset Converter for Microsoft SCCM エンジン タスクを作成する

CA Asset Converter for Microsoft SCCM を設定するには、最初にエンジン タスクを作成する必要があります。

注：CA Asset Converter for Microsoft SCCM エンジンのタスクは、データを抽出しようとしている Microsoft SCCM サイト サーバと同じコンピュータ上で実行中のエンジンには割り当てられません。

### CA Asset Converter for Microsoft SCCM エンジン タスクを作成する方法

1. DSM エクスプローラを開き、[コントロール パネル] - [エンジン] - [エンジン タスク] を選択します。

2. [情報] ペインの [タスク] エリアから [新規] を選択します。

エンジン タスクの [新規タスク ウィザード] が表示されます。

3. 以下の図に示すように、[タスク タイプ] ドロップダウン リストから [CA Asset Converter for Microsoft SCCM] を選択します。

**新規タスク ウィザード**

**新規タスクの作成**  
作成するタスクのタイプを選択します

このウィザードでは、新しいタスクを作成する手順が順番を追って説明されます。リストされているタスクのタイプを1つ選択し、[次へ] を押して続行します。

タスク タイプ(B): CA Asset Converter for Microsoft SMS/SCCM

**タスク タイプの説明**

Microsoft SMS/SCCM が収集したアセット情報を DSM MDB にフィードするため、Microsoft SMS/SCCM インストールから情報を抽出し、CA ITCM Asset Collector にフィードします。

< 戻る(B)    次へ(N) >    キャンセル    ヘルプ

4. [次へ] をクリックします。

残りの画面は、既存の CA Asset Converter for Microsoft SCCM タスクの [プロパティ] ダイアログ ボックスと同じです。次のセクションで説明します。

## タスク プロパティ

CA Asset Converter for Microsoft SCCM タスクの設定は、[新規タスク] ウィザードでの作成時か、または既存のタスクの場合は [プロパティ] ダイアログ ボックスで行います。いずれの場合でも、設定 GUI はほとんど同じです。違いは、ページ間では [次へ] と [戻る] ボタンを使用するのに対して、[プロパティ] ダイアログ ボックスではタブを使用することのみです。

## 説明

最初のページは任意のタイプのすべてのエンジン タスクで共通で、現在のタスクの名前と説明を指定することができます。名前は、空白ではない一意のものである必要があります。説明はオプションです。

## SCCM サーバ オプションの設定

SCCM Server タブは、抽出の対象となる SCCM サイト サーバに関する情報を参照するために使用します。

以下の手順を使用して SCCM Server オプションを設定します。

### SCCM サーバ オプションを設定する方法

1. [サーバ] フィールドに、情報の抽出元である SCCM サイト サーバのホスト名またはアドレスを入力します。
2. [サイト ID] フィールドに、接続する SCCM インストールのサイト ID を入力します。

各 SCCM サイト インストールには 3 文字のサイト ID があります。サイト ID が異なっていれば、同じサーバに複数の SCCM サイトをインストールすることができます。そのような場合は、このフィールドを使用して Asset Converter タスクの接続先サイトを指定する必要があります。

SCCM サイトがサーバ上に 1 つしか存在しない場合は、このフィールドの左側は空白にして、Asset Converter が自動的に有効なサイト ID のみを選択できるようにする必要があります。

3. [ユーザ名] フィールドに、**SCCM** サイトサーバとの接続時に使用するドメイン名とユーザ名を入力します。左側が空白の場合は、現在タスクを実行しているエンジンのユーザ情報が使用されます。
4. [パスワード] フィールドに、**SCCM** サイトサーバとの接続時に使用するパスワードを入力します。左側が空白の場合は、現在タスクを実行しているエンジンのユーザ情報が使用されます。

指定されたユーザは、サーバマシン上の **SCCM WMI** クラスにリモートでアクセスできる必要があります。

5. [テスト接続] ボタンをクリックし、現在入力されたサーバ情報で **SCCM** サイトと接続を確立できるかどうかを確認します。
6. [次へ] をクリックします。

ここでの結果が成功だったとしても、今後、異なるマシンおよび異なるユーザ情報で起動しているエンジンでタスクを実行した場合に、同じ結果になるとは限りません。[新規タスクの作成] ダイアログ ボックスの [テスト接続] ボタンをクリックして行うテストは、**GUI** を起動しているマシン上、かつその **GUI** を起動している状況下で実行されます。実際の **SCCM Converter** タスクが実行される場合、その実施はエンジンマシン上、かつそのエンジンで使用するユーザアカウント下（デフォルトではローカルシステム アカウント）で行われます。このため、テスト接続に成功した場合でも、実際のタスク実行時に接続が成功するとは限りません。環境設定の [ユーザ名] フィールドに、必ずドメイン名（ドメイン名\ユーザ名の形式で）が含まれるようにすれば、このような相違の可能性を取り除くことができます。含まれていない場合は、現在のユーザのドメインがデフォルトとして設定され、デフォルトのエンジンにとってはそのエンジンマシンのローカルユーザが設定されることとなります。また可能であれば、変換を実行するエンジンマシンとまったく同様に **SCCM** インストールにアクセスする任意のマシン上でもテストを実行してください。

## 収集オプションの設定

「収集オプション」タブには、ハードウェア情報、ソフトウェア情報の収集を有効または無効にする、それぞれ別個のオプションがあります。

### 収集オプションを設定する方法

- たとえば、「インベントリ情報の収集」、「ソフトウェア情報の収集」、および「収集範囲の指定」のいずれかのオプションを選択します。

- 「次へ」をクリックします。

デフォルトでは、この情報は **SCCM** クライアントがインストールされた **SCCM** インストールにあるすべてのコンピュータから収集されます。

抽出範囲を、**SCCM** サイトの 1 つの特定のコンピュータ グループに限定することが可能です。これを実行するには、「収集範囲の指定」チェックボックスを有効にし、「収集」フィールドに抽出する **SCCM** 収集の名前を入力します。

## 配信場所の設定

〔配信場所〕タブでは、CA Asset Converter for Microsoft SCCM タスクによって生成された XML ファイルの格納場所を指定します。通常は、Asset Collector インストールの収集フォルダになります。

以下の手順を使用して〔配信場所〕を設定します。

### 配信場所を設定する方法

1. 以下のオプションから選択します。

#### ローカルの Asset Collector を使用する

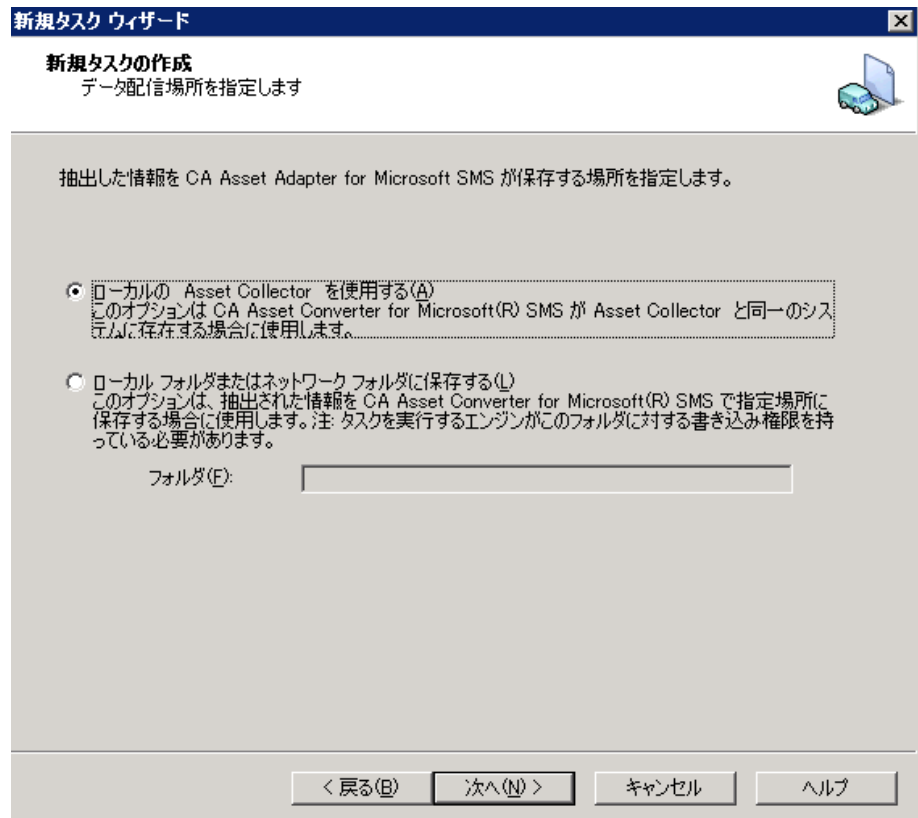
選択すると、CA Asset Converter for Microsoft SCCM タスクと同じコンピュータ上で実行されている Asset Collector の収集フォルダにファイルが書き込まれるようになります。これはデフォルトの設定です。

注：コンピュータに Asset Collector がインストールされていない場合、CA Asset Converter for Microsoft SCCM タスクは失敗します。

## ローカルフォルダまたはネットワークフォルダに保存する

選択すると、指定したローカルまたはネットワークのフォルダにファイルが格納されるようになります。

たとえば、以下の図では、[ローカルの Asset Collector を使用する] オプションが選択されています。



2. [次へ] をクリックします。

## スケジューリング

CA Asset Converter for Microsoft SCCM タスクは、他のすべてのエンジン タスクと同じスケジュール ダイアログを使用します。SCCM データを完全に抽出するには、時間がかかる上に SCCM データベース サーバに負荷をかける場合があります。サーバが使用されていない可能性が最も高い時間帯に、タスクをスケジュールすることをお勧めします。

## タスク管理

CA Asset Converter for Microsoft SCCM タスクを実行して、そのステータスを確認できます。

## タスクの実行

タスクを作成して設定した場合、実行するには 1 つのエンジンに関連付ける必要があります。

### CA Asset Converter for Microsoft SCCM タスクを実行する方法

これを行う方法はいくつかあります。

- SCCM タスクを、DSM エクスプローラのツリー ビュー内の適切なエンジンにドラッグアンドドロップします。
- ツリー ビュー内でエンジンを選択し、[情報] ペインで [既存のタスクのリンク] をクリックします。次に、CA Asset Converter for Microsoft SCCM タスクを、表示されるダイアログで選択します。
- ツリー ビュー内でエンジンを選択し、[新規タスクの追加] をクリックします。[新規タスクの作成] ウィザードが表示されます。このウィザードでは、タスクの作成、設定、および関連付けのすべてを 1 ステップで実行することができます。

関連付けされると、次回タスクリストに表示され、スケジューリング設定で実行が許可されたときに、エンジンはそのタスクを実行します。

## タスク ステータス

タスクのステータスは、エンジンのタスク リストに表示されます。指定可能な値は以下のとおりです。

### 待機中

エンジンはまだタスクを実行していません。

### アクティブ

タスクは現在実行中です。

### OK

タスクは実行されていて、「OK」ステータスが返されました。

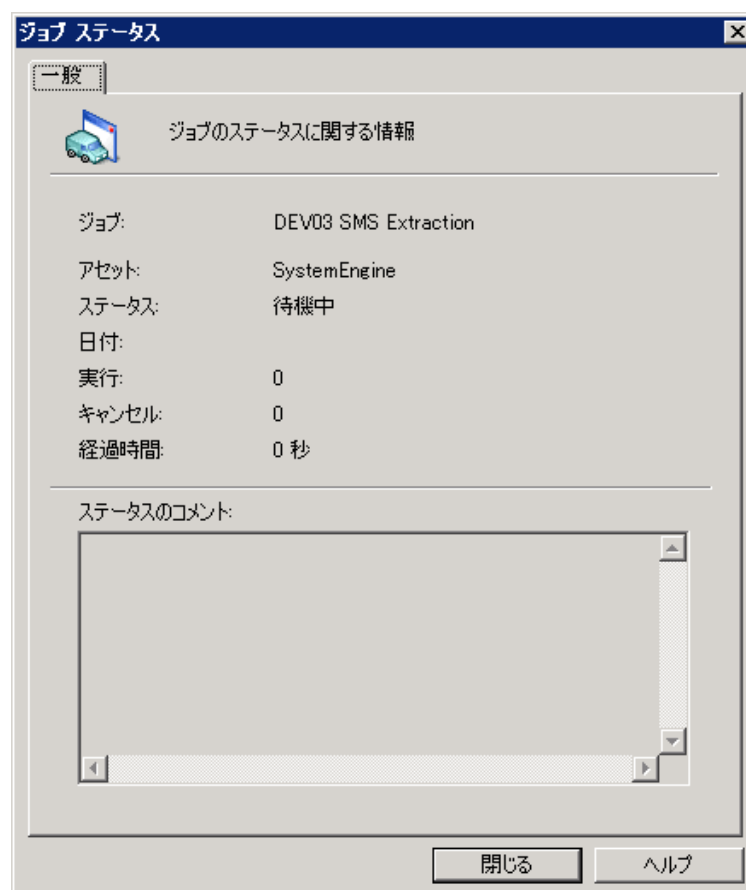


## エラー

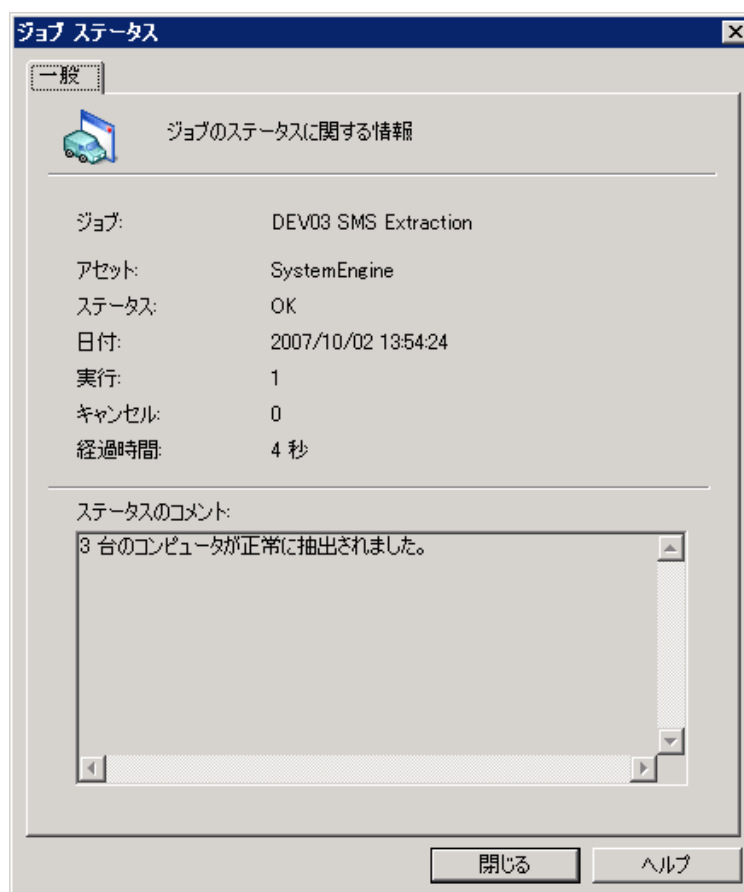
タスクは実行されていて、「エラー」ステータスが返されました。

タスク リストには、タスクが最後に実行された時間も表示されます。

### 待機中ステータスの CA Asset Converter for Microsoft SCCM タスクの例



### OK ステータスの CA Asset Converter for Microsoft SCCM タスクの例



## CA MDB の SCCM 変換済みデータ

CA Asset Converter for Microsoft SCCM が生成した XML ファイルが Asset Collector に取得されると、そのコンピュータは、検出されたほかのハードウェア アセットと共に DSM GUI に表示されます。

以下の図は、[エージェント ステータス] セクションに、コンピュータにインストールされている DSM Asset Management エージェントがなく、コンピュータの発行元が Microsoft SCCMであることを示しています。



## 診断と追跡

通常の DSM 追跡システムは、CA Asset Converter for Microsoft SCCM タスク実行実行時の詳細情報を記録するのに使用します。適切な設定手順が実行された場合、使用される追跡ファイルは、TRC\_SMSEX.log です。それ以外の場合は、他の DSM コンポーネントからの情報と共に TRC\_UAM.log ファイルに出力されます。

## am\_sms\_ex.exe コマンドライン ユーティリティ

実際に SCCM 抽出作業を行う実行可能ファイルは *am\_sms\_ex.exe* で、テストまたはデバッグ用に手動で起動されることがあります。

有効なコマンドライン引数は以下のとおりです。

*/s:<servername>*

抽出元の SCCM サイト サーバ名およびアドレスを指定します。指定されない場合のデフォルトは **localhost** です。

*/u:<username>*

サーバへの接続時に使用するユーザ名を指定します。デフォルトは現在のユーザです。

*/pp:<password>*

使用するパスワード（平文テキスト形式）を指定します。ユーザ名が指定されている場合のみ使用します。

*/c:<site id>*

接続先の SCCM インストールのサイト ID です。サーバに SCCM インストールが複数含まれる場合にのみ必要です。

*/d:<output directory>*

生成された XML ファイルを格納するディレクトリです。

*/collect\_sw*

ソフトウェア情報を抽出します。

*/collect\_hw*

ハードウェア情報を抽出します。

*/collect\_users*

関連アセットである各コンピュータで最後にログオンしたユーザを抽出します。

## 第 7 章：システム エンジンの使用

---

システム エンジンは、アーキテクチャの主要コンポーネントであり、サーバとデータベース間の主要な通信ポイントとなります。システム エンジンは以下の 2 つのレベルで使用可能です。各レベルでのシステム エンジンの機能は異なります。

### システム エンジン - エンタープライズ マネージャ

エンタープライズ マネージャにおけるシステム エンジンは、データ処理を実行します。エンジンでは、以下の操作が行われます。

- エンタープライズ データベースまたはドメイン データベースからデータを取得するためのレポート テンプレートのスケジューリング
- クエリ、SQL スクリプト、および外部ユーティリティの実行
- ソフトウェア コンテンツのダウンロード ジョブ（デフォルト）を実行して、エンタープライズ マネージャのソフトウェア定義リストを更新します。

### システム エンジン - ドメイン マネージャ

ドメイン マネージャのシステム エンジンでは、以下のタスクが実行されます。

- ドメイン データベースからデータを取得するためのレポート テンプレートのスケジューリング
- データ収集
- データ配信
- エンタープライズ マネージャとの間のデータの複製
- クエリ、SQL スクリプト、および外部ユーティリティの実行
- ソフトウェア コンテンツのダウンロード ジョブ（デフォルト）を実行して、ドメイン マネージャのソフトウェア定義リストを更新します。
- デフォルト ディレクトリの同期処理ジョブの実行

このエンジンは、専用の Windows コンピュータ上で動作するのが普通です。ただし、エンジンはドメイン マネージャ上でも動作できます。専用コンピュータ上でエンジンを実行した場合、クエリの作成時、および多数のコンピュータから更新されたインベントリが処理されるときドメイン マネージャの応答時間が向上します。

**注：** GUI を手動でリフレッシュするか、またはレジストリ キーを設定して、ステータスをリアルタイムのエンジンのステータスに更新します。

このセクションには、以下のトピックが含まれています。

[エンジン インスタンスの作成](#) (P. 511)

[エンジンの設定](#) (P. 512)

[エンジン ログ](#) (P. 513)

[エンジンの停止および起動](#) (P. 514)

[ジョブのパフォーマンス](#) (P. 514)

[定義済みエンジン タスク](#) (P. 515)

[エンジン タスク](#) (P. 516)

## エンジン インスタンスの作成

同じコンピュータでエンジンのインスタンスを複数作成できます。ドメイン マネージャ コンピュータでは、メインエンジンは **SystemEngine** と呼ばれますが、リモート インストールされたシステムでは、**computername\_Engine** と呼ばれます。これらのエンジンを右クリックして、そのインスタンスを新規作成できます。新しいインスタンスは、同じコンピュータ上に常駐します。

以下のようなケースでは、エンジン インスタンスを追加すると役に立ちます。

- つまり、スケジュールされたエンジン タスクの数が原因で、タスクの再スケジュールの間隔が長すぎるというケースです。
- この場合、タスクの終了までに時間がかかって、ほかのタスクが妥当な時間内に処理されなくなってしまう。

次の手順に従ってください：

1. [コントロール パネル] フォルダの [システム エンジン] を右クリックして [新規インスタンスの作成] を選択し、エンジンの一意の名前をテキスト フィールドに入力して [OK] をクリックします。

新しく作成したエンジンは [すべてのエンジン] フォルダに表示されます。

**注：** 新しいインスタンスは、選択したエンジンと同じコンピュータ上で実行されます。エンジンを別のコンピュータ上に分散するには、選択したコンピュータ上で新しいエンジンを **Client Automation** インストーラを使用してインストールする必要があります。

## エンジンの設定

エンジンを設定すると、エンジンの使用状況を最適にし、パフォーマンスを向上させることができます。

### エンジンを設定する方法

1. [コントロール パネル] - [エンジン] - [すべてのエンジン] フォルダに移動します。

ドメイン内の既存のエンジンがフォルダの下に表示されます。

2. エンジンを右クリックし、[プロパティ] を選択します。

[Engine\_Name のプロパティ] ダイアログ ボックスが表示されます。

3. [詳細設定] タブをクリックし、以下の設定を指定します。

#### 1 回の収集サイクルでエンジンが収集するファイル数

1 回の収集サイクルでエンジンが収集するファイル数を指定します。デフォルトでは、この数値は **10000** に設定されます。この場合、エンジンは 1 回の収集サイクルで **10000** ファイルを収集し、次のサイクルを開始する前にキュー内のエンジン タスクの実行を許可します。次の収集サイクルは、下のフィールドで指定した周期の経過後に開始されます。

デフォルト : 10000

#### エンジンのタスクの間隔 ( 秒 )

エンジン タスクの実行間隔の周期を秒数で指定します。デフォルトでは、この周期は **60** 秒に設定されます。この場合、エンジンは 1 分ごとにスケーラビリティ サーバからデータを収集します。長時間実行されるエンジン タスクがある場合は、この周期をエンジン タスクの実行に適した値に変更します。

デフォルト : 60



## エンジン ログ

エンジンまたはエンジン インスタンスは、すべてのアクションをログ ファイルに記録します。このログ ファイルを表示すると、エンジンがスケーラビリティ サーバからいつデータを収集したかを調べたり、エンジンに関連する問題のトラブルシューティングを行うことができます。[SystemEngine] ペインに、このログの簡単な概要が表示されます。

エンジン SystemEngine

DSM Explorer > 518 - ドメイン > コントロール パネル > エンジン > すべてのエンジン > SystemEngine

**説明**

次のタスクは、現在、このエンジンで実行するようスケジューリングされています。

**タスク**

- エンジンの停止
- エンジンのアクティブ化
- 新規タスクの追加
- 既存のタスクのリンク

**詳細**

開始時間: 2008/11/04 6:05:55  
動作時間: 06:22:39

このペインをカスタマイズ。  
詳細なヘルプを参照するには、F1 キーを押してください。

エンジンがアイドル状態です。  
2008/11/04 12:28:05 ジョブを実行しています isat m2k3 収集

| タスク                             | ステータス | 最終の実行               | アクション   |
|---------------------------------|-------|---------------------|---------|
| ソフトウェア コンテンツのダウンロード ジョブ (デフォルト) | OK    | 2008/11/04 0:00:37  | ✖ ➡ ⬆   |
| デレクティブ ジョブ (デフォルト)              | OK    | 2008/11/02 0:01:27  | ✖ ➡ ⬆ ⬆ |
| isat m2k3 収集                    | OK    | 2008/11/04 12:28:21 | ✖ ➡ ⬆ ⬆ |

すべてのエンジン ログは、システム エンジンに関しては C:\Program Files\CA\DSM\Logs\SystemEngine.log に、その他のエンジンに関しては、各 <エンジン名>.log に含まれています。

デフォルトでは、自動リフレッシュは無効になっています。自動リフレッシュを有効にする場合、適切な値（秒単位）を設定して UI をリフレッシュします。

[HKEY\_CURRENT\_USER\Software\ComputerAssociates\EGC3.0\RefreshRates\cDispEngine]

## エンジンの停止および起動

エンジンは、ドメイン マネージャによって起動時間に自動的に実行されます。ただし、特定の時間にエンジンを停止してから起動して、タスク リスト内のすべてのタスクを再度実行することもできます。

### エンジンを停止して起動する方法

1. [コントロール パネル] - [エンジン] - [すべてのエンジン] - [SystemEngine] フォルダに移動します。

右側のペインに、エンジン ステータスおよびタスク リストが表示されます。

2. [タスク] セクションで [エンジンの停止] をクリックします。

エンジンが停止されます。エンジンがこの時点でタスクを実行している場合は、タスクの完了後にエンジンが停止されます。

3. [タスク] セクションで [エンジンの開始] をクリックします。

エンジンが起動し、タスク リスト内のタスクを実行します。

**注：** リモートからエンジンを起動または停止できるのは、エンジンを実行しているコンピュータに対する管理権限を持つユーザのみです。

## ジョブのパフォーマンス

システム エンジンは、ドメイン マネージャ上で以下のジョブを実行します。

- 定義済みタスク
- エンジン タスク

## 定義済みエンジン タスク

定義済みタスクはエンジンにリンクされており、エンジンの起動直後に実行されます。使用可能な定義済みエンジン タスクは、以下のとおりです。

### ソフトウェア コンテンツのダウンロード ジョブ ( デフォルト )

CA Online Content Service から新しいソフトウェア シグネチャをデータベースにダウンロードします。ソフトウェアのコンテンツ ダウンロードが終了したら、**DSM** エクスプローラおよび **AM** マネージャをそれぞれ必ず再起動するようにしてください。そうしないと、ダウンロードしたソフトウェアが **DSM** エクスプローラ **GUI** に反映されません。

**AM** マネージャを再起動するには、以下のコマンドを実行します。

```
caf stop ammanager
caf start ammanager
```

**重要:** ソフトウェア シグネチャのダウンロード中に **CAF** による停止を実行しないでください。ダウンロードプロセスでは、整合する必要があるデータベース内の多数の重要なテーブルが更新されます。このため、プロセスを中止すると、データが整合しなくなる可能性があります。ダウンロードプロセスは **java** 実行可能ファイルであるため、プロセス リスト内の **java.exe** を確認し、[コントロール パネル] で [システム エンジン] に移動することにより、ソフトウェア コンテンツのダウンロード ジョブ ( デフォルト ) が実行されていないことを確認してください。

### デフォルト ディレクトリの同期処理ジョブ

[コントロールパネル] - [ディレクトリの統合] - [ディレクトリの同期] フォルダの下に設定されているディレクトリの同期処理ジョブを実行します。

### デフォルトの SCAP チェックリスト処理ジョブ

*ITCM\_installpath¥SCAP\_Checklists* フォルダにある SCAP チェックリストを処理します。新規または更新されたチェックリストが存在する場合、このジョブはチェックリストファイルの圧縮アーカイブを作成し、新規または更新されたチェックリスト用のインベントリ検出モジュールを作成または更新します。

### エンジン収集タスク

ハードウェア、ソフトウェア、使用状況などのインベントリ情報を収集するエンジン収集タスクを実行します。

注：定義済みエンジン タスクを変更、リンク解除、または削除すると、Client Automation システムの機能の一部が影響を受けることがあります。

関連項目：

[エンジン収集タスク](#) (P. 192)

## エンジン タスク

エンジン タスクはエンジンにリンクできます。リンクされた後、エンジンはそのタスクをタスク リストに追加し、順番にタスクを実行します。

使用可能なエンジン タスクは以下のとおりです。

### 収集タスク

スケーラビリティ サーバからインベントリ情報を収集するようにエンジンに指示します。

### クエリ タスク

クエリを実行して結果を DSM エクスプローラに返すようにエンジンに指示します。

### SQL スクリプト タスク

SQL スクリプトを実行するようにエンジンに指示します。

### 外部ユーティリティ タスク

外部ユーティリティを実行するようにエンジンに指示します。

注： 外部ユーティリティがユーザからの入力待ちなどで応答を停止しないようにしてください。 停止するような状況が発生すると、エンジンは、それにリンクされている他のすべてのタスクの処理を停止してしまいます。

### データベース同期タスク

エンジンに、DSM ドメインまたはエンタープライズ マネージャの Microsoft SQL Server (Windows) に収集された Client Automation アセットとインベントリ データを、リモートの SQL Server (Windows) または Oracle DBMS (Solaris) の一致データと同期化するように指示します。

### CA Asset Converter for Microsoft SCCM タスク

エンジンに指示して、System Center Configuration Manager に接続して、そのデータベースに保管されているコンピュータについてのハードウェアおよびソフトウェア インベントリを含む情報を抽出するようにします。

### CA リポジトリ抽出

リポジトリからパッケージ メタデータを抽出すると、DSM Web コンソールに Debian パッケージの詳細を表示できます。 詳細については、「Software Delivery 管理ガイド」の「リポジトリからパッケージメタデータを抽出する」を参照してください。

### スケジュール済みレポート タスク

スケジュール済みレポートを実行するようにエンジンに指示します。

注： 各エンジン タスクの詳細については、「DSM エクスプローラ ヘルプ」の「Asset Management」を参照してください。

### 複製ジョブ

ドメイン マネージャがエンタープライズ マネージャに接続されている場合、ITCM はアップロード複製タスクおよびダウンロード複製タスクを自動的に作成します。ITCM は 2 つの複製タスクをドメイン マネージャ内のシステム エンジンにリンクします。エンジンは、ダウンロード複製ジョブをすぐに実行し、続いてアップロード複製ジョブを実行して、ドメイン マネージャとエンタープライズ マネージャ間の両方の方向でデータが複製されるようにします。アップロード複製タスクは次の 2 段階で発生します。

- エンタープライズ マネージャからデータを削除します（アップロード削除ステージ）。
- エンタープライズ マネージャにデータを更新します（アップロード更新ステージ）。

同様に、ダウンロード複製タスクにより、ドメイン マネージャからデータを削除し（ダウンロード削除ステージ）、ドメイン マネージャにデータを更新します（ダウンロード更新ステージ）。

これらのタスクにはデフォルトで以下の名前が付いています。

- <ホスト名> アップロード複製
- <ホスト名> ダウンロード複製

注：

- 複製タスクはドメイン マネージャのみに作成されます。
- 複製ジョブを実行する前に、ドメイン マネージャおよびエンタープライズ マネージャが同じパッチ レベルになっていることを確認してください。

デフォルトでは、複製ジョブは常に実行されるようにスケジュールされています。ジョブ プロパティを変更して別のスケジュールを設定できます。

注：ドメインデータがエンタープライズ マネージャ上で複製されない場合、ドメイン マネージャのエンジン収集タスクおよび複製タスクのステータスを確認します。両方のジョブのステータスが OK である場合、ドメイン マネージャで以下のコマンドを実行します。

```
caf stop engine
caf start engine
```

# 第 8 章：診断およびトラブルシューティング

---

以下のセクションでは、アセット管理の使用中的問題解決に役立つさまざまなトラブルシューティングアクションについて説明します。

## ログ ファイル収集ツール dsminfo

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。

## レポートされたエラーのトラブルシューティング

以下に、スキャンによってレポートされたエラーを解決する方法を示します。

- DSM エクスプローラで、<コンピュータ名>-[インベントリ]-[SCAP]-<チェックリスト名>-[ステータス]で移動します。右ペインのステータス属性には、スキャンがエラーに終わった理由が表示されます。この属性では、ベンチマークがプラットフォームに対して実行できない、XCCDF ファイルまたは OVAL ファイルにエラーがあるなどのエラーを明示します。
- インタープリタからの出力を調査することによって、ルールエラーを調査することができます。これには、チェックリストで使用する各 OVAL 定義の結果が含まれています。ルールエラーを調査するには、以下のうち 1 つを行います。
  - エージェントの作業ディレクトリ¥SCAP\_Result\_Files ディレクトリの下の *MachineName-fdcc-checklistname-oval-ovaldi-stdout.txt* ファイルを表示します。
  - OVAL テスト結果ファイルのコレクションを設定している場合、ドメインマネージャ上の *ITCM\_installpath¥SCAP\_Result\_Files¥checklistname¥version\_number* ディレクトリの下の *MachineName-fdcc-checklistname-oval-ovaldi-stdout.txt* ファイルを表示します。
- 以下のコマンドを使用してトレースレベルを「詳細」に設定し、スキャンによって生成されたすべてのエラーについて、Asset Management ログファイルを調査することができます。

```
cftrace -c set -f UAM -l DETAIL
```

詳細については、スキャナによって生成されたログファイルをチェックしてください。

## MDB がダウンすると AM マネージャがクラッシュ

データベースまたはデータベース リスナがアクティブでない場合、AM マネージャがクラッシュすることがあります。



## Asset Collector によって作成される重複エントリ

### 症状

別の MAC アドレスと同じアセットを再ロードすると、Asset Collector は、エージェントに対して重複したエントリを作成します。同じ動作は、NRI アセットにも当てはまります。

### 解決方法

データは `external_host_key` と `host_uuid` に基づいて処理されるため、重複エントリが作成されます。重複エントリが作成されないよう保証するため、シリアル番号に関して新しい検証が提供されています。

以下の手順に従います。

以下のコマンドを実行してパラメータを作成し、パラメータ値に `1` を設定します。

```
ccnfcmda -cmd setparametervalue -ps /itrm/manager/engine -pn
AssetMatchOnUniqueSerialNumber -v 1
```

この変更により、`hostuuid`（ホスト名と MAC）に関する既存の検索に加えて、シリアル番号の一意の検索が可能になります。

## ログインに記録されたエラー イベント

### 症状：

OSIM イメージの作成と登録は正常に動作しますが、`sdmpcworker` が、イベント「ファイルが見つかりません」をログに記録します。

### 解決方法：

このログ エントリは、無視してもかまいません。Microsoft ロードは、必要がない場合にもフォントのロードを試みます。その後、Microsoft ロードは、このフォントファイルなしで動作しますが、ブート サーバは、`tftp` でファイルを読み取る試行をログに記録します。

## Citrix XenServer 仮想マシンでインベントリ属性ホスト名に正しくない値が表示される

### 症状

RVI エージェント プラグインを使用して Citrix XenServer プラットフォームの仮想化インベントリを収集する場合、ノード [仮想化] の下のインベントリ属性ホスト名に、Citrix XenServer 仮想マシンが、いくつかのゲスト仮想マシンに対して正しくない値を表示します。

### 解決方法

DNS テーブル内の逆の IP ルックアップが正しくないホスト名値を返すか、または値を返さない場合に、この問題が発生します。正しいインベントリ データを取得するには、IP とホスト名が DNS サーバで正しく更新されていることを確認します。

## Microsoft Hyper-V クローン用の新しいホスト UUID が存在しない

Microsoft Hyper-V で VM を使用して VM クローン作成を行う場合、DSM エージェントは、クローン作成されたことを識別できません。したがって、新しいホスト UUID を生成できません。その理由は、UUID ソースが BIOS (Client Automation のデフォルトのソース) ではなく、Microsoft WMI (Windows Management Instrumentation) であることによります。Microsoft Hyper-V では、UUID は、ゲストからではなく、ハイパーバイザー WMI からのみアクセス可能です。

注：テンプレートからクローンを作成する場合、この問題は発生しません。

クローンが新しい仮想マシンとして表されることを確認するには、以下の手順に従います。

1. CAF を停止します。
2. レジストリから HOSTUUID キー  
HKLM¥SOFTWARE¥ComputerAssociates¥HostUUID を削除します。
3. ホスト名を変更して再起動します。

## Asset Management が Citrix XenServer の VM 上でインベントリ データを収集しない

エージェントが Citrix XenServer の仮想マシン上で実行される場合、Asset Management エージェントが、以下のサブインベントリ ノードのインベントリ データを収集しません。

- インベントリ、システム、メモリ
- インベントリ、システム、I/O ポート
- インベントリ、システム、システム スロット
- インベントリ、システム、COM ポート
- インベントリ、電源設定、AC アダプタ
- インベントリ、電源設定、バッテリー

## DSM エクスプローラで vDisk レコードが見つからない

以下の理由により、DSM エクスプローラで vDisk レコードが見つかりません。

- プロビジョニング サーバへの接続で、vDisk 情報の取得に失敗しました。
- vDisk 上とプロビジョニング サーバ上のシステム時刻が同期していません。
- プロキシを介したプロビジョニング サーバへの接続はサポートされていません。

すべての場合に、CAF がシャット ダウンします。

修正するには、以下の手順に従います。

次の手順に従ってください：

1. 管理者権限で vDisk にログインします。
2. 個人データ プロビジョニング サービス情報を確認します。
3. プロビジョニング サーバへの接続をトラブルシューティングします。

成功すると CAF が開始し、vDisk 登録が実行されます。

## プロセッサ スロットルが Client Automation に別の値を表示する

powercfg.exe ユーティリティの出力と比較した場合、インベントリ項目プロセッサ スロットルが Client Automation に別の値を表示します。この値は powerprof.dll の 64 ビットのバージョンを使用して読み取られます。

この値は、Windows プラットフォーム上の `..¥windows¥SysWOW64` フォルダに存在する powercfg.exe ユーティリティの出力と一致します。同じ powercfg.exe ユーティリティの 32 ビットのバージョンは以下のフォルダに存在します。  
`..¥ windows¥system32`。このバージョンの出力は、64 ビットバージョンとは異なります。

## Citrix XenServer ゲスト仮想マシンが仮想インベントリに表示されない

### 症状

RVI エージェント プラグインを使用して Citrix XenServer プラットフォーム用の仮想化インベントリを収集する場合、一部のゲスト仮想マシンが [インベントリ] - [仮想化] - [Citrix XenServer 仮想マシン] の下に表示されません。

### 解決方法

この問題に対する解決方法は開発中です。解決方法が公開されているかについては、[support.ca.com](https://support.ca.com) を参照してください。

## アセットが新しいテナントに移動するとき、テナント ID が更新されない

アセットが新しいテナントに移動するとき、テナント ID が更新されません。回避策は、まずアセットを削除し、次に新しいテナントに再度登録することです。

## コンテンツ ダウンロードが失敗する

### 症状

CIC プロセスがバックグラウンドで実行されているときで、別のインスタンスがエンジンによって起動されるときにコンテンツをダウンロードすると、CIC インスタンスの接続解除が発生します。

### 解決方法

以下の手順に従います。

1. wrapper.exe プロセスを終了します。
2. CIC によって使用されている java.exe を終了します。
3. アンカー ファイルおよび loc ファイルが存在する場合、それらを C:\Program Files (x86)\CA\SC\CIC\bin から削除します。
4. エンジン タスクから、コンテンツ ダウンロード ジョブを再度開始します。

## アンインストール ジョブの後のソフトウェア ジョブ履歴動作

ジョブ履歴のクリーンアップ時間設定で指定された期間が経過すると、エージェントのソフトウェア ジョブ履歴がクリーンアップされます。クリーンアップタスクは、設定ポリシーの「開始時間」で指定された時間に毎日実行されます。クリーンアップタスクは、ジョブ履歴のクリーンアップ時間設定に基づいて、設定ポリシーで指定された時間数より古いインストールジョブを毎日確認します。デフォルト期間は **4320 時間**または **180 日**です。

クリーンアップタスクは、パッケージのすべてのプロシージャと一緒に削除しようとしています。これは、このタスクでは、インストールジョブ履歴を削除する前に、パッケージのアンインストールジョブ履歴を検索することを意味しています。したがって、インストールジョブ履歴が **180 日**を超えるものであっても、アンインストールジョブ履歴が利用可能になるまで、タスクは、ジョブ履歴を削除できません。アンインストールプロシージャを展開した後は、ソフトウェアジョブ履歴にアンインストールジョブも含まれます。クリーンアップタスクは、次にスケジュールされた時間に実行されるときに、設定ポリシーで指定された時間より古く、履歴内に対応するアンインストールジョブが存在するインストールジョブを探します。一致するものが見つかり、パッケージの完全なジョブ履歴（インストール、起動、アンインストールプロシージャを含む）が、エージェントのソフトウェアジョブ履歴から削除されます。これにより、アンインストールの直後に履歴が除去されます。

リリース **12.9** では、アンインストールジョブが設定ポリシーで指定された時間を超えると、ソフトウェアジョブ履歴が削除されるように、**comstore** 設定が変更されています。たとえば、ジョブ履歴クリーンアップ時間パラメータを **10 日**に設定している場合、コンピュータにアンインストールプロシージャがインストールされた時間から、最大で **10 日**分のパッケージの完全なジョブ履歴が削除されます。

## CAM サーバ間の不安定な通信

### 症状

アセット管理環境においてデータの配信や収集に関連する問題が断続的または継続的に発生します。影響を受けるコンポーネントがアクティブになっていて、互いに通信できることは確認されています。この問題の一例として、アセット管理エージェントが正常に動作せず、インベントリ情報を返していないことが考えられます。

### 解決方法

製品コンポーネントがアクティブで正常に動作していると判断し、双方向通信が可能であることが確認できた場合、**camping** コマンドを使用し、現在の環境のネットワーク プロトコル サポートのレベルが原因でこの通信問題が発生しているかどうかを判断してください。

常に **User Datagram Protocol (UDP)** を優先/デフォルトの接続プロトコルとして使用してください。ただし、以下のいずれかに該当する場合にはこの原則は適用されません。

- ネットワーク内に **UDP** の使用に関する制限がある場合。
- ネットワーク内に **UDP** パケットの最大サイズに関する制限があり、**CAM** でこのサイズを超えるメッセージを送信できなくなる場合。パケットサイズの制限があるかどうかを判断するには、**camping -s** オプションを使用し、実際に制限があるかないかを判断できるまで、**UDP** パケットに徐々に大きな値を指定します。

以下に例を示します。

```
camping -s 64 <remote_machine_ip_address>
camping -s 128 <remote_machine_ip_address>
camping -s 256 <remote_machine_ip_address>
camping -s 512 <remote_machine_ip_address>
camping -s 1024 <remote_machine_ip_address>
camping -s 2048 <remote_machine_ip_address>
camping -s 4096 <remote_machine_ip_address>
camping -s 8192 <remote_machine_ip_address>
```

サイズ制限が存在すると判断した場合は、より小さい増分量を指定することで、サポートできる正確な最大サイズを見つけてください。

次に、実際に CAM でその最大サイズに達しているかどうかを判断します。これを判断するには、通常の転送（または一連の転送）に対する CAM トレース ログを調べます。CAM トレース ログ内で以下のような行を探してください。

```
send_message(10.1.1.14) called
```

```
Seq 41, Fd (Sec 0), from uxkul01/CAIFTRANS, to NTA0C04/CAIFTRANS, len 8198, data ><,
created 43434, life 60, notify: yes, src 10.7.1.1, dst 10.1.1.14
```

この例では、2 行目の len 8198 が、CAM が送信しようとしているメッセージパケットのサイズを表しています（この場合は 8198 バイト）。次に、CAM により送信されたすべてのメッセージ内でこのフィールドを検索すると、CAM で発生した最大パケットサイズを判断できます。このサイズが（上記の手順で camping -s スイッチを使用して指定した）最大 UDP パケットサイズより大きい場合は、UDP パケットサイズの制限値を大きくするか、または制限値を削除することを検討してください。

アセット管理インベントリ収集が失敗した場合、そのインベントリ収集のサイズ（最初の収集では大きくなることもある）がネットワーク内の UDP パケットの最大サイズを超えている可能性があります。

中間ルータの MTU サイズ制限が送信元ポイントまたは送信先ポイントよりも小さい場合があります。その中間ルータが適切な ICMP 応答を送信側ホストに送信できない場合は、そのような状況であることを示しており、このルータはブラックホールルータと呼ばれます。サイズが同じぐらいのパケットが破棄されるという問題が発生する場合は、問題がある可能性があります。

以下のトピックの詳細については、Microsoft のナレッジベースを調べてください。

- ブラックホールルータ問題に関するトラブルシューティングを実行する方法 ([159211](#))
- さまざまなネットワーク トポロジのデフォルトの MTU サイズ ([140375](#))



## ファイル転送のタイムアウト

### 症状

最適なネットワーク プロトコルを選択した後も、その転送がタイムアウトになります。

### 解決方法

転送がタイムアウトになる場合、以下の 2 つの理由が考えられます。

- 転送先のリモート マシンがビジーであり、転送に割り当てられた時間内にすべての着信接続を処理することができません。この場合は、割り当てられた時間内にリモート マシンがすべての接続を処理できるように、別の時間にリモート マシンへの転送することを検討してください。
- 接続帯域幅の大きさが充分でなく、転送に割り当てられた時間内にファイル/データの転送を完了できません。この問題が原因かどうかを調べるには、CAM トレース ログで CAM が 1 秒間にリモート マシンに送信できるメッセージ数を調べます。以前に判断したパケット サイズと 1 秒間に処理されるメッセージ数を使用して、これを外挿することにより、CAM が割り当てられた時間内に送信できる適切な最大ファイル/データ サイズを判断することができます。許容された時間内で、このサイズが、送信する必要のあるファイル/データ サイズより小さい場合、帯域幅が充分ではありません。このような場合、接続の帯域幅を改善するか、または転送を開始したアプリケーションのサポート担当者に連絡して、転送時間を拡大できるかどうか、およびその方法を決定する必要があります。

## Asset Management エージェントを Windows XP SP2 コンピュータに展開できない

### 症状

アセット管理エージェントを Windows XP SP2 コンピュータに展開すると、配信に失敗し、プライマ トランスポートがないというステータスが表示されます。

### 解決方法

Windows XP SP2 コンピュータのローカルセキュリティ ポリシーおよびファイアウォールにより、システムへのアクセスが禁止されています。アセット管理エージェントを展開する前に、ローカルセキュリティ ポリシーを変更し、ファイアウォール設定を指定する必要があります。

#### ローカル セキュリティ ポリシーを変更する方法

1. 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] を開きます。  
[ローカル セキュリティ設定] ウィンドウが表示されます。
2. [ローカル ポリシー] - [セキュリティ オプション] に移動し、[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] をダブルクリックします。セキュリティ設定を [クラシック - ローカル ユーザーがローカル ユーザーとして認証する] に変更し、[OK] をクリックします。  
ローカル セキュリティ ポリシーが変更されます。

ファイアウォール設定を変更することにより、CAM 通信用の UDP ポートを開く必要があります。

#### ファイアウォール設定を変更する方法

1. Windows の [コントロール パネル] を開いて [Windows ファイアウォール] を選択します。  
[Windows ファイアウォール] ダイアログ ボックスが表示されます。
2. [例外] タブで [ファイルとプリンタの共有] を選択し、4104 用に 1 つの UDP ポートを、7 用に 1 つの UDP/TCP ポートを追加して [OK] をクリックします。

## 再作成されたグループに対する既存のクエリが失敗する

### 症状

グループを削除してから同じ名前でグループを再作成した後、そのグループに依存するクエリを実行すると、結果が生成されません。

### 解決方法

グループを作成すると、そのグループに新しい UUID が割り当てられます。クエリ デザインは（グループ名ではなく）この UUID を使用してデータベースをクエリします。このため、グループを削除してから同じ名前でグループを再作成した場合は、両方のグループの UUID が異なるため、クエリが失敗します。クエリを編集し、グループ名を再度選択すると、正確な結果が表示されます。

注：リンクされているアセットについてスケーラビリティ サーバをクエリする場合にも、同様の症状が発生します。サーバを削除してから再び登録すると、そのサーバに依存しているクエリを実行しても結果が生成されません。同様の解決方法に従ってください。

## ソフトウェア コンテンツのダウンロード ジョブが失敗する

デフォルトのソフトウェア コンテンツのダウンロード ジョブは、以下の状況で失敗することがあります。

- [プロキシ サーバの詳細の欠落](#) (P. 532)
- [ネットワークの問題 - evmUpdate1 0 を実行しようとしたときに不明なエラーが発生しました。RC : -6](#) (P. 532)
- [Unicenter Patch Management インストール](#) (P. 533)

## プロキシ サーバの詳細の欠落

### 症状

DSM インストールがプロキシ サーバの背後に常駐する場合、プロキシ カスタマイズ内容が存在しないために自動のソフトウェア コンテンツのダウンロード ジョブが失敗する可能性があります。

### 解決方法

ソフトウェア コンテンツのダウンロード ジョブがサーバに接続される前に、共通設定ポリシーでプロキシ サーバの詳細を更新する必要があります。

1. 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] に移動します。

既存の設定ポリシーが表示されます。

2. 変更するポリシーを選択し、[DSM] - [マネージャ] - [ソフトウェア コンテンツのダウンロード] に移動します。

[ソフトウェア コンテンツのダウンロード] の設定が表示されます。

3. サーバ名、ポート、ユーザ、パスワードなどのプロキシ詳細を追加します。
4. 設定を封印します。

コンテンツのダウンロードでは、プロキシ サーバを介して接続し、ソフトウェア ダウンロードを完了できます。

## evmUpdate1\_0 を実行しようとしたときに不明なエラーが発生しました。RC : -6

### 症状

デフォルトのソフトウェア コンテンツのダウンロード ジョブは、ネットワークの問題が原因で失敗することがあります。この失敗が発生した場合は、「evmUpdate1\_0 を実行しようとしたときに cic.log ファイルで不明なエラーが発生しました。RC : -6」というエントリが表示されます。

注：cic.log ファイルは、CIC のログ ディレクトリ（Program Files¥CA¥SC¥CIC¥logs）にあります。

### 解決方法

以後のダウンロードは正常に行われ、エラーなしで完了します。

## Unicenter Patch Management インストール

### 兆候

ソフトウェア コンテンツのダウンロード ジョブが失敗します。

### 解決策

Client Automation をインストールする前に、すでに Unicenter Patch Management がインストールされていないことを確認してください。

## VM ホストまたはシステム コントローラが DSM Explorer に表示されない

### 症状

amagent の完了後、\$CA\_ITRM\_BASEDIR/Agent/AM/data/transfer\_vm ディレクトリ (UNIX) に 12amvminvux.inv ファイルが見つかりません。(関連する Windows ディレクトリは、..¥Agent¥units¥00000001¥uam¥transfer\_vm です。)

### 解決方法

仮想ホスト インベントリ収集タスクの特定の仮想ホストを有効にする必要があります。

## 関連するコンピュータが仮想ホストに表示されない

### 症状

amagent は正常に完了しましたが、関連するコンピュータが仮想ホストに表示されません。

### 解決方法

最新のインベントリを DSM マネージャにアップロードするには、amagent を再度実行する必要があります。

## 検出されたソフトウェアの欠落

All Users¥Application Data¥CA¥eso\_fingerprints 下にサイズがゼロの Windows シグネチャ ファイルが生成されると、シグネチャ スキャンが失敗する場合があります。そのようなゼロサイズのファイルは、同時プロセスの競合による可能性があります。回避策は、ゼロサイズのファイルを削除するか、または新しいソフトウェア定義を追加することにより、シグネチャ ファイルを再生成することです。

## Dual-Core HP-UX コンピュータで報告されたプロセッサの数

### 症状

[インベントリ]-[システム]で報告されたプロセッサの数が、HP-UX SAM (System Administration Manager) によって報告された数と異なります。

### 解決方法

Dual-Core プロセッサを使用してコンピュータが実行されている場合、SAM は各物理プロセッサに対して 2 つのプロセッサを表示します。このような場合、[インベントリ] - [システム] の下にある「コアの数 (プロセッサごと)」の属性を考慮する必要があります。

## SUN E4800/4900/6800/6900 システム コントローラで報告されたプロセッサの数

### 症状

[インベントリ] - [システム] で報告されたプロセッサの数が、「showboards -p cpu」コマンドによって報告された数と異なります。

### 解決方法

システム ボードの「説明」が「No board power」である場合、このボードのプロセッサの数はカウントされません。

## インストールされている amVMAgent と、表示されている amVMAgent のバージョンが異なります。

### 症状

インストールされている amVMAgent のバージョンと、DSM エクスプローラ ユーザ インターフェースに表示されている amVMAgent のバージョンを比較すると、バージョンが異なっています。

### 解決方法

（異なるバージョンの） amVMAgent を使用して、インベントリ ファイル `amvminvux.inv` を `$CA_ITRM_BASEDIR/Agent/AM/data/transfer_vm` フォルダに配置することによって登録を手動で行った場合、この方法を使用して登録された仮想エージェントのバージョン番号は、コンピュータ上の amVMAgent と同じになります。

## [ 概要 ] ページにプラットフォームが「未分類」と表示される

### 症状

[概要] ページにプラットフォームが「未分類」と表示されます。

### 解決方法

DSM エクスプローラ GUI で、デフォルトのエンジン ジョブである「デフォルト ソフトウェアのコンテンツのダウンロードジョブ」を有効にし（[コントロール パネル] - [エンジン] - [システム エンジン]）、このジョブが有効になっていてエラーが発生していないことを確認します。ジョブの実行でエラーが表示されている場合、このシステムがインターネットに接続されていて、CA Web サイトから更新をダウンロードできることを確認してください。

## 仮想ホストとそのゲストの関係が表示されない

### 症状

仮想ホストを登録し、その後に新しいゲストシステム（HP-UX vPar など）を登録しました。ゲストシステムの登録後、このゲストシステムと関連する仮想ホストとの関係が表示されません。何が起こったのでしょうか。

### 解決方法

デフォルトでは、仮想ホストとそのゲスト システムの関係は、仮想ホストの登録時にのみ作成されます。後でゲスト システムが登録された場合、関係が確立されません。

仮想ホスト インベントリ収集タスクが設定されたエージェント マシン上で Asset Management エージェントを起動するか、次にスケジュールされた Asset Management エージェント プロセスまで待つことができます。

## インベントリ ファイルにエラー タグが表示される

### 症状

インベントリ ファイルの 1 つにエラー タグが表示されます。

### 解決方法

インベントリ ファイルの処理に問題がある場合、ファイル名が変更され、ファイル名の最後に「.error」が付加されます。エラー原因の詳細については、アプリケーション イベント ログを参照する必要があります。

## ロード配信

### 症状

ロードの配信方法がわかりません。

### 解決方法

Asset Collector がインストールされた複数のスケーラビリティ サーバがある場合は、有効な Asset Collector 間で、インベントリ ファイルを均等に配分してロードを配信できます。



## エラーの検出

### 症状

どこでエラーを参照するのがわかりません。

### 解決方法

インベントリ ファイル内でエラーが検出された場合、そのファイルの名前には `.error` という拡張子が付加されます。アプリケーション イベント コンソールで検出されたエラー内容を確認できます。

以下にエラーの例を示します。

- 無効な形式の `xml` です
- 文字列値が長すぎます
- 整数値に文字列が含まれています
- 整数値が設定された制限値の範囲外です

## Asset Collector が処理できるインベントリ ファイル数の制限

### 症状

Asset Collector が処理できるインベントリ ファイル数がわかりません。

### 解決方法

処理できるファイル数は、使用可能なディスク容量によってのみ制限されます。`hostuuid` キャッシュは、新規アセットが作成されるたびに増加します。ストレージ容量が、唯一の制限要因です。

## [ 信頼レベル ] フィールドと [ 発行元 ] フィールドが DSM エクスプローラで表示されない

### 症状

DSM エクスプローラで [ 信頼レベル ] フィールドと [ 発行元 ] フィールドを参照できません。

### 解決方法

これには、以下 3 つの理由が考えられます。

- DSM エクスプローラが、Asset Collector の変更がインストールされていないマネージャに接続されている。この場合、DSM エクスプローラにはこれらの列が表示されません。
- DSM エクスプローラが更新されておらず、Asset Collector の変更が含まれていない。
- 上記の両方

## DSM エクスプローラの [ 信頼レベル ] フィールドと [ 発行元 ] フィールドが、他のドメインに接続しているときに表示されない

### 症状

DSM エクスプローラの [ 信頼レベル ] フィールドと [ 発行元 ] フィールドが、1 つのドメインに接続しているときにだけ参照でき、他のドメインに接続しているときには参照できません。

### 解決方法

これは恐らく、Asset Collector の変更を適用したドメインの 1 つに問題があるためです。MDB の変更とコンポーネントの変更（インストール）は、別々に適用する必要があることに注意してください。

## バックアップ

### 症状

惨事復旧用にバックアップを行いたい。

### 解決方法

Host UUID ¥ Mac Address キャッシュ ファイルを、現在の惨事復旧計画に追加します。このファイルの名前は、有効な設定ポリシーに指定されます。デフォルト名は machostcache.xml です。

## フロッピー ドライブからのアセット収集

### 症状

フロッピー ドライブを Asset Collector の収集ポイントとして指定したいのですが、フロッピー ディスクを挿入すると、ファイル変更通知メカニズムが動作してしまいます。

### 解決方法

Asset Collector を強制的にフロッピー ディスクから再収集させるには、以下のコマンドを使用して Asset Collector CAF プラグインを停止し、再開します。

```
caf stop assetcollector
caf start assetcollector
```

## ネットワーク ドライブからの収集

### 症状

ネットワーク ドライブから収集することができません。

### 解決方法

デフォルトでは、Asset Collector はローカル システム アカウント ユーザとして起動します。ご使用のコンピュータのネットワーク ドライブへのアクセス権限はありません。Asset collector CAF プラグインを設定し、別のユーザとして起動する必要があります。

### Asset Collector でネットワーク ドライブからの収集を行う方法

1. AssetCollector を設定し、別のユーザとして起動します。  
`caf setprop assetcollector setcreds 1`
2. 使用するクレデンシャルを指定します。  
`caf setcreds assetcollector user <username> password <password>`
3. Asset Collector を停止/再開して、新規ユーザの使用を開始します。  
`caf stop assetcollector`  
`caf start assetcollector`

この設定を元に戻すには、以下のコマンドを使用します。

```
caf setcreds assetcollector user "" password ""
```

## 未処理ファイル

### 症状

収集フォルダのファイルが処理されません。予想していたようにファイルが出力フォルダに移動しません。

### 解決方法

**Asset collector** が起動していることを確認します。 `caf status`、または `caf status assetcollector` コマンドを実行することで確認できます。

**Asset Collector** が起動していない場合は、`caf start assetcollector` で起動します。

**Asset Collector** で監視している収集フォルダが、ファイルを格納しているフォルダであることを確認します。 **DSM** エクスプローラで、コンピュータからの設定レポートをリクエストし、使用中の設定ポリシーを参照できます。

**Asset Collector** と接続して、インベントリを登録およびアップロードするサービスが起動していない可能性があります。 **Asset Collector** は、登録には共通サーバプラグインに依存し、インベントリのアップロードにはアセット管理サーバに依存します。登録またはアップロードに失敗した場合は、イベント ログでメッセージを参照する必要があります。サービスが再開すると、**Asset Collector** は再度インベントリのアップロードを試行する必要があります。これには、依存するサービスが開始されてから 5 分ほどかかります。

**Asset Collector** で、無効なスケーラビリティ サーバにインベントリをレポートするよう設定されていることがあります。有効な設定であることを確認してください。

## アプリケーション イベント ログの大量のエラー

### 症状

Asset Collector でインベントリ データを登録またはアップロードできない場合に、大量のエラー イベントがアプリケーション イベント ログに書き込まれます。

### 解決方法

Asset Collector がインベントリ ファイルを登録またはアップロードできない場合、ファイルはキューに格納されて再試行されます。Asset Collector は 5 秒後に登録を再試行します。登録できない場合は、遅延時間が 10 秒、20 秒と増えていきます。これは最大遅延時間が 5 分になるまで繰り返されます。イベントは、これらの試行が失敗するたびに発生します。そのため、Asset Collector が依存する caf プラグインがサービスを再開した場合、その 5 分後にすべてのインベントリ ファイルが Asset Collector で処理されます。

## SCCM Converter エンジン タスク エラー

### 症状

SCCM Converter エンジン タスクが、[新規タスクの作成] ダイアログ ボックスのテスト接続に成功したにも関わらず、「SCCM サイトに接続できませんでした」というメッセージが表示されて失敗します。

### 解決方法

[新規タスクの作成] ダイアログ ボックスの [テスト接続] ボタンをクリックして行うテストは、GUI を起動しているマシン上、かつその GUI を起動している状況下で実行されます。実際の SCCM Converter タスクが実行される場合、その実施はエンジンマシン上、かつそのエンジンで使用するユーザ アカウント下（デフォルトではローカルシステム アカウント）で行われます。このため、テスト接続に成功した場合でも、実際のタスク実行時に接続が成功するとは限りません。環境設定の [ユーザ名] フィールドに、必ずドメイン名（ドメイン名¥ユーザ名の形式で）が含まれるようにすれば、このような相違の可能性を取り除くことができます。

含まれていない場合は、現在のユーザのドメインがデフォルトとして設定され、デフォルトのエンジンにとってはそのエンジン マシンのローカル ユーザが設定されることになります。また可能であれば、変換を実行するエンジン マシンとまったく同様に SCCM インストールにアクセスする任意のマシン上でもテストを実行してください。

## インベントリ情報が見つからない

### 症状

コンピュータ グループのアセットは表示されていますが、詳細なインベントリ情報が見つかりません。

### 解決方法

Asset Collector でインベントリの送信先として設定されたスケーラビリティ サーバに、アセット管理サーバがインストールされていない場合、登録されたアセットのインベントリ情報は使用できません。コンピュータ グループのアセットは表示されますが、詳細なインベントリ情報はありません。使用可能で、且つ動作しているアセット管理サーバプラグインがインストールされたスケーラビリティサーバだけを使用してください。

## どうすればエージェントブリッジが稼動中であることがわかりますか？

### 症状

エージェントブリッジが実際に稼動中であることを確認したいのですが。どうすればよいでしょうか。

### 解決方法

AM エージェントブリッジが稼動中であることを確認するには、Windows のタスク マネージャを開いて、[プロセス] タブで `amLrss.exe` と `amss.exe` の 2 つのプロセスを確認します。この 2 つがリストされている場合、AM エージェントブリッジは有効であり稼動しています。

SD Agent Bridge の場合、このブリッジはソフトウェア配信スケーラビリティサーバと完全統合されているので、ソフトウェア配信スケーラビリティサーバが稼動していれば、SD Agent Bridge は稼動しています。

## 自分のレガシー エージェントを登録できない

### 症状

エージェントブリッジを有効にした後で、自分のレガシー エージェントを **Client Automation** に登録できません。

### 解決方法

エージェントブリッジ設定ポリシーを有効にした後で、数分間待たないとレガシー エージェントを登録することはできません。

## 自分の PDA で USD エージェントが UAM エージェントに上書きされる

### 症状

USD 4.0 エージェントをインストールしてエージェントブリッジをポイントしている PDA デバイスを持っています。Unicenter DSM に正常に登録できました。その後、そのデバイスに UAM 4.0 エージェントもインストールして、同じエージェントブリッジをポイントして、登録しました。ところが、私の USD エージェントが、別の名前を持つ UAM エージェントによって上書きされてしまいました。私の USD エージェントはどうなったのでしょうか？

### 解決方法

既存の UAM および USD 4.0 PDA デバイスのエージェントには、UAM および USD PDA デバイス エージェント ソフトウェアのインストール中に、特定のエージェント名を付けることができます。この名前は、PDA デバイスの登録に使用されます。UAM エージェントに USD 名と異なる名前が付けられると、これが原因で UAM エージェントと USD PDA エージェントは登録プロセス中に互いをそれぞれの名前で上書きします。

この問題を解決するためには、デバイス上でのエージェント ソフトウェアのインストール中に UAM エージェントと USD エージェントの両方に同じ名前を付けて、UAM エージェントと USD エージェントの両方が Unicenter DSM システムで同じ名前を共有するようにする必要があります。



## なぜエージェント名が重複するのですか?

### 症状

最初に Unicenter Asset Management 3.2 エージェントを登録し、その後すぐに Unicenter Software Delivery 4.0 エージェントを登録しました。数分後、Unicenter Asset Management と Unicenter Software Delivery の 2 つのエージェントが DSM エクスプローラで同じ名前が表示されています。

### 解決方法

UUID 生成を有効にしていると、Unicenter Asset Management エージェントは Agent Bridge を介してホスト UUID を生成しましたが、Unicenter Software Delivery エージェントはホスト UUID をエージェント コンピュータ自身から受信しました。両方のエージェントが非常に短い時間内で登録されると、一方は Unicenter Asset Management 用でもう一方は Unicenter Software Delivery 用の重複したエージェント名が生成される可能性があります。

この場合は、Unicenter Asset Management エージェントを DSM エクスプローラから手動で削除する必要があります。この問題が再発しないようにするには、以下の登録ルールに従ってください。

レガシー エージェントを登録するために、これらのエージェントのいくつかは自身の UUID をレポートしない場合がある

- Unicenter Asset Management エージェントと Unicenter Software Delivery エージェントの両方がホスト UUID をレポートしない場合、Unicenter Asset Management エージェントと Unicenter Software Delivery エージェントを任意の順序で登録できます。しかし、2 つのエージェントの登録と登録の間で、通常それぞれ 5 分以上待つ必要があります。
- Unicenter アセット管理エージェントがホスト UUID をレポートしないのに Unicenter Software Delivery エージェントがレポートする場合は、常に Unicenter Software Delivery エージェントを先に登録する必要があります。それから 5 分後に、Unicenter Asset Management エージェントを登録します。
- Unicenter Software Delivery エージェントがホスト UUID をレポートしないのに Unicenter Asset Management エージェントがレポートする場合は、常に Unicenter Asset Management エージェントを先に登録する必要があります。それから 5 分後に、Unicenter Software Delivery エージェントを登録します。

一般に、大部分の Unicenter Asset Management 4.0 エージェントおよび Unicenter Software Delivery 4.0 エージェントは、サーバに登録するときにホスト UUID をレポートします。

## エージェントブリッジ ログ ファイルはどのようにすれば表示できますか?

### 症状

エージェントブリッジコンポーネントのログファイルが `..DSM¥logs` ディレクトリで見つかりません。これらのログファイルはどのようにすれば表示できますか?

### 解決方法

コマンドラインスクリプト `AgentBridge.dms` を実行した後で、CAF サービスを再起動してすべてのトレースファイルのエントリが正しくシステムに登録されるようにしてください。CAF を起動した後で、エージェントブリッジのログファイルが見つからない場合は、CA サポートオンライン (<http://support.ca.com>) にお問い合わせください。

## ログファイルが見つからない

### 症状

`amss.log` ファイルを探しているのですが、見つかりません。このログファイルはどこにありますか。

### 解決方法

AM エージェントブリッジモバイルセクタサーバモジュール `amss.exe` のログファイルの名前は、`amss.log` ではなく、`TRC_AMSS.LOG` です。このファイルは `..DSM¥logs` ディレクトリにあります。

AM エージェントブリッジには、他に 2 つの新しいログファイルがあるので注意してください。

#### ■ `TRC_AMBRIDGE.LOG`

AM エージェントブリッジ変換モジュール `amBridge.exe` のログファイル。

#### ■ `TRC_AMLRSS.LOG`

AM エージェントブリッジセクタサーバモジュール `amLrss.exe` のログファイル。

## ハードウェア モジュール 1 つだけが実行される

### 症状

ハードウェア インベントリ モジュールのうち 1 つだけしか実行されていません。他のすべては「待機」状態を示しています。エージェントブリッジのどこがおかしいですか？

### 解決方法

Microsoft Windows では、最初のハードウェア インベントリ モジュールのみがエージェントによって実行され、残りは無視されます。これは、Unicenter Asset Management 4.0 エージェントでの意図的な動作です。この制限を回避するには、すべてのハードウェア インベントリ収集タスクを 1 つのモジュールの中に入れて、このモジュールをコンピュータに割り当てます。この場合、すべてのインベントリ タスクがエージェントにより実行されます。

## Solaris の非大域ゾーン、リソース プール、およびプロセッサ セットのインベントリが見つからない

### 症状

Solaris の非大域ゾーンに関連するインベントリが見つからない。

### 解決方法

大域ゾーンに Asset Management エージェントをインストールする必要があります。仮想ホストインベントリ収集タスクを設定する必要はありません。これは、非大域ゾーン、リソース プール、およびプロセッサ セットについての情報はデフォルトでエージェントによって収集されるためです。

非大域ゾーン インベントリは、DSM エクスプローラの [仮想化] - [ゾーン] でレポートされます。リソース プール インベントリは、[仮想化] - [リソース プール] - [リソース プール] でレポートされ、プロセッサ セットの情報は [仮想化] - [リソース プール] - [プロセッサ セット] でレポートされます。

## Intellisig におけるスクリプト コンパイル エラー

### 症状

特定の Intellisig では、常にスクリプト コンパイル エラーが表示されます。

### 解決方法

ターゲット コンピュータ上の `dmscript.exe` のバージョンが **R12.5.1010** 未満ではないことを確認します。Intellisig スクリプトは、**R12.5.1010** より前は利用可能ではなかった `dmscript` の新機能を使用するため、更新バージョンが必要です。

## 収集タスクの実行が成功した場合でも、Intellisig の実行に失敗する

### 症状

収集タスクが正常に実行される場合であっても、特定の Intellisig が実行されません。

### 解決方法

以下の手順に従います。

1. [ソフトウェア] - [定義] - [Intellisig] に移動します。
2. 実行する Intellisig で [Discovery の有効化] が [はい] に設定されていることを確認します。それ以外の場合、右クリックして [スキャンの有効化] を選択します。
3. Intellisig を右クリックして [プロパティ] を選択し、[バージョン] タブを表示します。正しい Intellisig バージョンで [アクティブ] が [はい] に設定されていることを確認します。アクティブなバージョンが存在しない場合、Intellisig は実行されません。

## Intellisig の実行の確認

### 症状

自分の Intellisig が正しく実行しているか確認します。

### 解決方法

ソフトウェア インベントリの実行中に何らかのエラーが発生した場合、そのエラーを DSM エクスプローラのメイン ページの [システム ステータス] ポータルに表示できます。

以下の手順に従います。

1. [コンピュータ] - [設定] - [収集タスク] に移動します。

そのアセットに対してソフトウェア インベントリが設定されている場合、[ソフトウェア インベントリ設定]が収集タスクの 1 つとして表示されます。

2. タスクを右クリックし、[ステータス] を選択してソフトウェア インベントリの実行に関する詳細なエラー情報を確認します。

個々のコンピュータ上で、ソフトウェア インベントリの実行状態を表示できます。

## ターゲット コンピュータ上での Intellisig 実行のタイムアウト

### 症状

いくつかのターゲット コンピュータ上では、いくつかの Intellisig の実行が常にタイムアウトになります。

### 解決方法

スクリプトの実行時にターゲット コンピュータのパフォーマンスへの影響を最小にするため、Intellisig は、バックグラウンドプロセスとして実行するように設計されています。この理由のため、負荷の大きいコンピュータ上で長時間実行されるスクリプトは、実行にさらに長い時間がかかる可能性があります。そのような場合、Intellisig は、利用可能な実行タイムアウトを超過します。

設定ポリシーを使用して、利用可能な実行タイムアウトを制御できます。以下の場所で、デフォルトの Intellisig 実行タイムアウト値を制御する設定ポリシー値を検索できます。

[コントロール パネル] - [設定] - [設定ポリシー] - ポリシー名 - [DSM] - [エージェント] - [Asset Management] - [Intellisig デフォルト実行タイムアウト]。

Client Automation 設定ポリシーでは、別のポリシーに対してタイムアウト値を異なる期間として定義できます。異なるポリシーを別のコンピュータ、またはコンピュータのグループに適用できます。この方法では、Intellisig タイムアウトが検出されるコンピュータ上でアクティブなポリシーに対してのみ、設定値を変更できます。

## エージェント上で実行する Intellisig スクリプトの確認

### 症状

エージェント上で実行する Intellisig スクリプトを確認します。

### 解決方法

次の手順に従ってください：

1. DSM エクスプローラ - [ソフトウェア] - [定義] - [Intellisig] に移動します。
2. 確認する Intellisig を右クリックします。
3. [バージョン] タブをクリックし、次に確認する Intellisig バージョンを選択します。

注：Intellisig は、複数のバージョンを持つことができますが、一度にアクティブにできるバージョンは 1 つのみです。ユーザのエージェント コンピュータ上で実行されるのは、アクティブなバージョンです。

4. 確認するバージョンを選択して、[プロパティ] ボタンをクリックします。  
ダイアログ ボックスに、Intellisig の詳細情報が表示されます。
5. [スクリプト] タブをクリックして、Intellisig スクリプトの名前を表示します。
6. [プレビュー] ボタンをクリックして、ファイルのコンテンツを表示します。

## ドメイン マネージャによる Intellisig 定義のエクスポートの確認

### 症状

マネージャによって、最新の Intellisig 定義がエクスポートされたことを確認します。

### 解決方法

Intellisig 定義は、Client Automation エンジンによって %ALLUSERSPROFILE%\Application Data\CA\eso\_fingerprints フォルダ内の XML ファイルおよび DAT ファイルにエクスポートされます。Intellisig 定義は、Windows については Xnnnnnnnn.xml ファイルと Xnnnnnnnn.dat ファイル、UNIX については Mnnnnnnnn.xml と Mnnnnnnnn.dat に提供されます。ここで、nnnnnnnn は、定義が変更されるたび増分される番号です。

XML ファイルには、Intellisig 定義、メイン スクリプト ファイルの名前、および任意のトリガおよび追加ファイルのリストが含まれています。

DAT ファイルには、メイン スクリプトおよび任意の追加ファイルが含まれます。このファイルは圧縮形式であり、たとえば 7-Zip を使用して圧縮解除できます。XML ファイルと DAT ファイルの内容を、DSM エクスプローラに表示される Intellisig 定義で比較できます。



## エンジンによって管理されるポリシー パラメータを変更しても、その動作が変化しない

### 症状

エンジンによって管理されるポリシー パラメータを変更しましたが、動作が変化しません。

### 解決方法

エンジンが実行されているマシンが、更新された設定ポリシーを受信したことを確認します。これは、**DSM** エクスプローラから、[すべてのコンピュータ] -<コンピュータ>- [設定ポリシー] - [設定レポートのリクエスト] - [設定レポートの表示] に移動することにより実行できます。ポリシー パラメータに必要な値があることを確認します。

コンピュータ上でポリシー パラメータが変更されると、そのコンピュータ上の **Client Automation** エンジンに変更が通知され、再度パラメータを読み取ります。**CONFIGURATION\_CHANGED** を検索することにより、詳細なエンジン ログでこれを確認できます。エンジンプロセスを再起動することにより、新しい設定が取得されたことを確認できます。

**注：** 操作が開始されるコンピュータ上で [複製された **Intellisig** をリンク解除時に変換する] パラメータが有効であることを確認します。このコンピュータは通常、エンタープライズ マネージャです。

## 複製された Intellisig が、手動による削除の後に複製されない

### 症状

ドメイン マネージャ上で、複製された Intellisig 定義を手動で削除しました。  
Intellisig 定義は、エンタープライズ マネージャから再度複製されませんでした。

### 解決方法

レプリケーションは、MDB で作成、更新、または削除された内容に応じて、デルタ メカニズムで動作します。複製されたオブジェクト（たとえば、ドメイン マネージャで複製された Intellisig 定義）を手動で削除すると、エンタープライズ マネージャで変更がない限り、再度複製されません。

# 付録 A: 管理情報フォーマット( .MIF )ファイルのリファレンス

---

以下の各セクションでは、.MIF ファイルの使用に関するさまざまな規則、定義、および規定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。

- [語の規則](#) (P. 556)
- [language 文](#) (P. 562)
- [一般の文](#) (P. 563)
- [コンポーネント定義](#) (P. 564)
- [パス定義](#) (P. 565)
- [列挙定義](#) (P. 566)
- [グループ定義](#) (P. 567)
- [属性定義](#) (P. 571)
- [テーブルの作成](#) (P. 576)
- [ComponentID グループ](#) (P. 577)
- [.MIF ファイルの例](#) (P. 579)

## 語の規則

MIF では文字セットとして、国際標準化機構文書 (ISO 8859-1 (Latin Alphabet No. 1)) または Unicode 1.1 を使用します。Unicode の MIF が提供されている場合、.MIF ファイルの最初のオクテットは 0xFE (16 進数) で、2 番目のオクテットは 0xFF である必要があります。そうでない場合、サービス レイヤはこのファイルを ISO8859-1 MIF として処理します。

トークンには、キーワード、整定数、文字列 (リテラル)、およびセパレータの 4 つのクラスがあります。「start」と「end」の 2 つのキーワードがスコープ キーワードであり、その後にほかのキーワードが続く場合のみ有効になります。以下に説明するブランク、タブ、改行、キャリッジリターン、およびコメント (総じて「空白」と呼ばれる) は、個別のトークンとして機能する場合を除いて、無視されます。隣接するキーワードおよび定数を区切る場合は、空白が必要です。

MIF では大文字と小文字が区別されません。ただし、リテラル文字列の場合は例外で、二重引用符で囲まれた文字は大文字と小文字が区別されます。

空白で区切られたリテラル文字列は結合され、1 つのリテラル文字列として格納されます。

## コメント

コメントはファイルのどこにでも挿入可能で、無視されます。コメントの開始は、連続する 2 つのスラッシュ (//) で示します。コメントは行の最後まで続きます。

## キーワード

.MIF ファイル構造では以下のキーワードが使用されます。

Component、Group、Attribute、Table、Path、enum、Name、Description、ID、Type、Class、Key、Value、Access、Storage、Language、Start、End、Unsupported、Counter、Counter64、Gauge、Octetstring、Displaystring、String、Integer、Int、Date、Integer64、Int64、Win16、Win32、DOS、Macros、Os2、UNIX、Read-only、Readwrite、Write-only、Direct-interface、Common、Specific

## データ タイプ

データ タイプは、ストレージ要件およびいくつかのセマンティクスを記述します。以下の表に、MIF でサポートしているデータ タイプを示します。

| データ タイプ                         | 説明                             |
|---------------------------------|--------------------------------|
| integer (int)                   | 32 ビット符号付き整数。既知のセマンティクスはありません。 |
| integer64 (int64)               | 符号付き整数。既知のセマンティクスはありません。       |
| gauge 32-bit                    | 増減可能な符号なし整数。                   |
| counter 32-bit                  | 減少しない符号なし整数。                   |
| counter64                       | 減少しない 64 ビット符号なし整数。            |
| string (n) または displaystring(n) | n オクテットの表示可能文字列。               |
| octetstring(n)                  | n オクテットの文字列。必ずしも表示可能ではありません。   |
| date                            | 28 オクテットの表示可能な文字列。             |

## カウンタ

カウンタは、その最大値 (232-1 または 264-1) まで増加し、最大値に達するとロールオーバーします。自動車のオドメータなどは、カウンタの一例です。

## ゲージ

ゲージは増加または減少できますが、その最大値 (232-1) に達すると、値が最大値を下回るまで最大値をレポートし続けます。自動車のスピードメータなどは、ゲージの一例です。

## 文字列

`string` タイプでは、値 `n` が `string` 内の最大オクテット数を表します。実際に使用されているオクテット数は、この最大値よりも少ない可能性があります。`string` は、実際の値のほかに、最初の 4 オクテット (`n` にはカウントされない) に値の長さ情報が格納されます。`C/C++` プログラミング言語のように 0 で終了する必要はありません。`string` の長さは、文字数ではなく `string` 内のオクテット数を表します。

## 日付

MIF ファイルにおける `Date` の形式は以下のとおりです。

```
yyyymmddHHMMSS.ffffff+ooo
```

この場合、各項目の意味は以下のとおりです。

`yyyy` は年、`mm` は月、`dd` は日、`HHMMSS` はそれぞれ時間、分、および秒を表します。`ffffff` はマイクロ秒であり、`+ooo` は UTC からのオフセット (分) です。UTC より東の場合は、数値の前にプラス (+) 記号が付きます。西の場合は、マイナス (-) 記号が付きます。これは 25 オクテットのみですが、日付はメモリ配置の理由から 28 オクテットフィールドとして格納され、最後の 3 オクテットはゼロ (「¥0」) です。

たとえば、2004 年 2 月 6 日金曜日の午後 1 時 30 分 15 秒 EDT は、「20040206133015.000000-300」と表されます。

必要に応じて、値にゼロを埋め込みます (たとえば、上記の例では 06)。フィールドに値を指定しない場合、フィールドの内の各文字をアスタリスク (\*) 文字で置き換える必要があります。

## 定数

整数値は、`C/C++` 言語と同じように指定できます。以下の表に、構文とベースに関する情報を示します。

| 構文              | ベース   |
|-----------------|-------|
| Nnn             | 10 進数 |
| Onnn            | 8 進数  |
| Oxnnn または OXnnn | 16 進数 |

`n` は真の基底における桁です。

注： MIF では浮動小数点値はサポートされません。

## リテラル

リテラル（文字列）は、二重引用符で囲まれた一連の文字です。（空白をはさんだ）連続する二重引用符文字は、複数部分からなるリテラルを示します。このリテラルは 1 つの文字列として扱われます。

以下に例を示します。

"This is an example"      " of a multi-part" " literal string."

リテラルのエスケープ文字は円記号（¥）です。これは、C/C++ プログラミング言語と同じように、以下の表に示す文字を入力する場合に使用されます。

| シーケンス | 文字                |
|-------|-------------------|
| ¥a    | アラート（ターミナルベルを鳴らす） |
| ¥b    | バックスペース           |
| ¥f    | 改ページ              |
| ¥n    | 改行                |
| ¥r    | キャリッジリターン         |
| ¥t    | 水平タブ              |
| ¥v    | 垂直タブ              |
| ¥¥    | 円記号               |
| ¥"    | 二重引用符             |
| ¥xhh  | ビットパターン、16 進数     |
| ¥ooo  | ビットパターン、8 進数      |

円記号に続く文字が上記のいずれでもない場合、円記号は無視されます。

8 進数のビットパターンの場合、MIF が ISO8859-1 形式で指定されているときは、ooo は 1 桁、2 桁、または 3 桁の 8 進数 (¥0 から ¥377 まで) になります。MIF が Unicode 形式で指定されているときは、1 から 6 桁の 8 進数 (¥0 から ¥177777 まで) になります。

16 進数のビットパターンの場合、MIF が ISO8859-1 形式で指定されているときは、hh は 1 桁または 2 桁の 16 進数 (¥x0 から ¥xff まで) になります。MIF が Unicode 形式で指定されているときは、1 から 4 桁の 16 進数 (¥x0 から ¥ffff まで) になります。

## ブロック スコープ

キーワード「start」および「end」は、定義ブロックのスコープを区切ります。start と end の後には、関連付けられたキーワードが続きます。以下の表に、キーワードとそのスコープを示します。

| ブロック    | 含まれる場所    | 説明                                                                                                      |
|---------|-----------|---------------------------------------------------------------------------------------------------------|
| コンポーネント | .MIF ファイル | コンポーネントを定義します。ほかのすべてのブロックは、このスコープ内に存在します。各 .MIF ファイルにつきコンポーネント定義は 1 つだけです。                              |
| パス      | コンポーネント   | 記号文字列を、オペレーティング システムに固有のパス名に関連付けます。MIF 内には 0 個以上のパス定義が存在します。通常は、ファイルの先頭のグループの前にあります。                    |
| グループ    | コンポーネント   | 属性の集まりを定義します。テーブルのテンプレート行として使用されることもあります。各 .MIF ファイルにつき少なくとも 1 つのグループ (以下で定義する ComponentID グループ) が必要です。 |
| 属性      | グループ      | 管理対象データのユニットを定義します。すべての属性は、グループ定義のスコープ内に「存在」します。各グループに少なくとも 1 つの属性が含まれている必要があります。                       |
| テーブル    | コンポーネント   | 以前に定義されたグループを使用して、グループのインスタンスを 1 つまたは複数定義します。オプション。                                                     |



---

|    |              |                                                                                                                                    |
|----|--------------|------------------------------------------------------------------------------------------------------------------------------------|
| 列举 | コンポーネントまたは属性 | 整数から文字列へのマッピングのリストを定義します。名前付き列举はコンポーネントレベルで定義でき、名前なし列举は属性定義の範囲内で定義できます。これはオプションですが、コンポーネントレベルでは多数の列举を定義できるのに対し、各属性に定義できる列举は1つだけです。 |
|----|--------------|------------------------------------------------------------------------------------------------------------------------------------|

---

.MIF ファイル構造の例を以下に示します。わかりやすくするために、各ブロックにつき 1 つだけ示しています。読みやすいように各レベルをインデントしています。

```
start component
 start path
 end path
 start enum
 end enum
 start group
 start attribute
 start enum
 end enum
 end attribute
 end group
 start table
 end table
end component
```

## language 文

**language** 文は、.MIF ファイルのネイティブ（人間の）言語を記述します。このオプションの文は、指定する場合、**start component** 文の前に置きます。構文は以下のとおりです。言語、地域としての方言、および文字列エンコーディングを識別するテキスト文字列としての言語文字列を指定します。

```
language = "language string"
```

言語文字列の書式は以下のとおりです。**language-code** は ISO 639 で定義されている 2 文字コードの 1 つであり、**territory-code** は ISO 3166 で定義されている 2 文字コードの 1 つであり、**encoding** は ISO8859-1 または Unicode です。

```
language-code|territory-code|encoding
```

たとえば、以下の言語文字列は、ISO8859-1（8 ビット）エンコーディングを使用するフランス語（カナダ）を示します。

```
"fr|CA|iso8859-1"
```

いずれかのフィールドを指定しない場合、それらのフィールドは省略されますが、文字列内に 2 本の縦棒を表示する必要があります。デフォルトの言語文字列は以下のとおりです。

```
"en|US|iso8859-1".
```

エンコーディングは .MIF ファイルの最初の 2 バイトにより決定されるため、.MIF ファイル内の **encoding** フィールドは無視されます。ただし、.MIF ファイルを介して通信する場合には **encoding** フィールドが使用されます。

ユーザは .MIF ファイルを編集してリテラル文字列を別の言語に翻訳できるため、言語文字列も同様に変更できます。**language** 文は、各 .MIF ファイルにつき 1 回のみ指定できます。

本章の最後に、2 つの ISO 標準で定義されたコードの例を記載しています。

**注：**ローカライズ（翻訳）された .MIF ファイルでは、リテラル文字列のみが翻訳されている必要があります。たとえば、名前、記述、列挙リテラル、および MIF 内のコメントなどです。クラス文字列または言語名はローカライズしないでください。キーワードはローカライズしないでください。

## 一般の文

以下の 3 つの文は、注記されているように、ほとんどの定義の範囲内で使用できます。定義を記述する際は、その定義に固有の文を記述します。

### name 文

**name** 文により、比較的短い文字列を定義に割り当てます。この名前はユーザに表示されるもので、255 文字以下にする必要があります。以下に、構文の例を示します。

```
name = "name string"
```

**name** 文では、.MIF ファイルの提供者が名前文字列を定義します。ただし、ユーザは .MIF ファイルを編集し、名前を変更することができます。**name** 文は、各定義につき 1 回のみ指定できます。名前は一意でなくてもかまいませんが、列挙およびパスの名前は例外で、コンポーネント内のほかの列挙（およびパス）の名前の中で一意である必要があります。

### description 文

オプションの **description** 文では、定義する要素に関する詳細情報を提供します。**description** 文は要素の記述を提供し、それをユーザに表示します。以下に、構文の例を示します。

```
description = "description string"
```

**description** 文では、.MIF ファイルの提供者が記述文字列を定義します。ただし、ユーザは .MIF ファイルを編集し、記述を変更することができます。**description** 文は、コンポーネント、グループ、および属性定義内で使用されます。**description** 文は、各定義につき 1 回のみ指定できます。

### ID ステートメント

ID 文により、定義に一意の数値識別子を割り当てます。ID を持つ必要のある各定義タイプは、そのスコープ内に一意の ID を持つ必要があります。ID は、API レベルでの項目の名前指定、およびネットワーク管理プロトコルへのマッピングに使用されます。構文は以下のとおりです。

```
id = n
```

ID 文では、.MIF ファイルの提供者が *n* を定義します。*n* の値は 0 以外の 32 ビット符号なし整数で、包含する定義のスコープ内で一意である必要があります。たとえば、グループ内の属性はすべて異なる ID を持つ必要がありますが、全部のグループにわたって属性 ID が一意である必要はありません。コンポーネントおよび管理アプリケーションにより通信時にこれらの ID が使用されるため、ユーザがこれらの ID を変更することはできません。

属性およびテーブル定義内では、ID 文は必須です。グループ定義内では、ID 文はオプションです。コンポーネント、パス、および列挙の定義では ID 文は使用されません。インストール時にサービス レイヤにより ID がコンポーネントに割り当てられます。ID 文は、各定義につき 1 回のみ指定できます。

## コンポーネント定義

コンポーネント定義の構文は以下のとおりです。

```
start component

 name = "component name"

 [description = "description string"]

 (ここにコンポーネント定義が入ります)

end component
```

コンポーネント定義は、.MIF ファイル内に 1 つのみ指定できます。

## パス定義

パス定義により、コンポーネントのアクティブな管理に使用するファイルの位置を変更します。

パス定義では、以下の文を順序どおりに指定します。

- `start path`
  - 記号名を定義する `name` 文
- 注：記号名には、呼び出し可能な関数を呼び出すことにより取得または設定するかどうかを示す値を、属性定義内で後で割り当てることができます。
- オペレーティングシステム識別子と呼び出し可能プログラムのパスが等記号で結ばれた複数の行
  - `end path`

オペレーティングシステム識別子は、DOS、MacOS、OS2、UNIX、win16、および win32 です。この識別子では、大文字と小文字は区別されません。コードによりサービスレイヤ（SL）に接続するコンポーネント計測が提供されている場合は、キーワード `direct-interface` を使用します。これに対し、要求時に SL によりコードが起動される場合は、呼び出し可能プログラムのパス名を指定します。

### 例：パス定義

`start path`

```
name = "Performance Info Instrumentation Code"

win16 = "C:¥¥someplace¥¥wincode.dll"

os2 = direct-interface

dos = "C:¥¥someplace¥¥doscode.com"

unix = "/someplace/unixcode"
```

`end path`

コンポーネント定義内では、1つの呼び出し可能関数に対して1つずつ、多数のパス定義を使用できます。パス名は、コンポーネント定義内のほかのすべてのパス名の間で一意である必要があります。

（本章の最後の）サンプル MIF で、パス定義内に定義された記号の使用例を参照してください。

## 列挙定義

列挙リストでは、文字列を符号付き 32 ビット整数と関連付けることができます。列挙は、コンポーネント スコープまたは個々の属性のスコープ内に定義します。コンポーネント計測では、これらの列挙を使用して **DMI** を介して整数を渡すため、管理アプリケーションでは対応するテキスト文字列をユーザの母国語で表示することができます。

列挙リストの構文は以下のとおりです。

```
start enum

 name = "enum name"

 vvv = "string literal for vvv"

 [xxx = "string literal for xxx"]

end enum

enum name
```

このコンポーネント内の一意の列挙リスト名を指定します。

### 整数値 vvv および xxx

最小値および最大値を指定します。これは、任意の順序でリストできます。最小値と最大値の間のすべての数値をリストする必要はありません。ただし、列挙定義内では各値は一意である必要があります。

コンポーネント定義内では、1 つの列挙リストに対して 1 つずつ、多数の列挙定義を使用できます。列挙では **ID** も **description** 文も使用しません。

## グループ定義

グループは、1つまたは複数の属性の集まりです。グループを使用すると、コンポーネント提供者は属性を論理セットに編成することができます。また、グループを使用して属性の配列（テーブル）を表すこともできます。グループを使用すると、コンポーネント内の論理サブセットをベンダー間で標準化することができます。

グループ定義の構文は以下のとおりです。

```
start group

 name = "group name"

 class = "class string"

 [id = nnn]

 [description = "description string"]

 [key = nnn[,mm]...]

 (属性定義がここに入ります)
```

end group

ID 文（提供された場合）は、コンポーネント内のほかのグループ全体で一意の値を持つ必要があります。キーなしでグループ ID を指定した場合、このグループ定義によりグループが定義されます。ID とキーを両方指定した場合、グループ定義はコンポーネント計測コードにより管理されるテーブルを表します。（以下に定義するような）コンポーネント定義内の後続のテーブル定義は、このグループ定義をテンプレートとして使用できません。

key 文を指定して ID 文を指定しない場合、グループ定義は、定義されるテーブル内のテンプレート行を表します。（以下に定義するような）value 文は行内のデフォルト値を表します。テンプレートに基づいてテーブルを作成するためのテーブル定義がこの後に続く場合もあります。詳細については、テーブル定義に関するセクションを参照してください。文の指定の組み合わせとその結果は、以下の表のとおりです。

| キーの指定 | ID の指定 | 結果                                    |
|-------|--------|---------------------------------------|
| いいえ   | いいえ    | エラー                                   |
| いいえ   | はい     | スカラ グループ。テーブルではありません。id はグループの ID です。 |

|    |     |                                         |
|----|-----|-----------------------------------------|
| はい | いいえ | テンプレート。テーブル定義が後に続くこともあります。              |
| はい | はい  | テーブル。Id はテーブルの ID です。後でテンプレートとして使用できます。 |

コンポーネント内には多数のグループを定義できます。



## class 文

必須の **class** 文は、グループのソースおよびグループ バージョンを識別します。同じクラス文字列を使用するすべてのグループは、属性タイプ、アクセス、（以下に定義する）ストレージ、ID など、グループ内の同じ属性定義を共有する必要があります。ただし、属性名、記述、および値は異なることがあります。**class** 文は、管理アプリケーションでグループの属性のセマンティクスを決定する際に役立ちます。

**class** 文の構文は以下のとおりです。

```
class = "class string"
```

通常、**class** 文字列は以下のようにエンコードされます。

```
"defining body|specific name|version"
```

### defining body

グループを定義する組織の名前を指定します。たとえば、「DMTF」、「IEEE」、「Acme Computer」などです。

### specific name

グループの内容を指定します。たとえば、「Server Stats」、「Toaster Controls」などです。

### version

グループ定義のバージョンを指定します。たとえば、「1」、「A」、「FIRST ONE EVER」などです。

基本的に **class** 文字列はあいまいな文字列であり、任意の規則を使用できます。ただし、**List Component** コマンドから情報を取得する際にアプリケーションおよびサービス レイヤがこの規則に基づいている可能性があるため、コンポーネントの提供者はこの規則を使用することをお勧めします。

グループ定義が異なる 2 つのグループに対して同じクラス文字列を指定するのは誤りです。管理アプリケーションは、クラス文字列が同じグループ定義を同一と見なします。

**注：** 縦棒の前後にスペースのない「DMTF|Sample|1.0」と、縦棒の前後にスペースのある「DMTF | Sample | 1.0」は、同じではありません。

クラスにより定義された属性のサブセットを指定した場合、実装では、サポートされていない属性の定義は省略されるだけです。サポートされていないキーワードは属性定義内に使用するほうが良い方法です（以下に定義）。管理アプリケーションは、クラスのサブセットを処理できる堅牢性を十分に備えている必要があります。

各グループにつき **class** 文は 1 つのみ許可されます。

### key 文

**key** 文では、テーブルのインデックスとして使用される属性 ID を定義します。グループ内の属性がテーブル内の行を定義する場合、グループ定義に **key** 文が含まれている必要があります。キーとして使用する属性は、どのデータタイプでもかまいません。キーは常に、グループのインスタンス（テーブルの行）を 1 つしか識別しません。

**key** 文の構文は以下のとおりです。

**key** = n[,m]

**n**

このテーブルのキーとなる属性 ID を指定します。テーブルのインデックス作成に複数の属性を使用する場合、それらの属性をカンマで区切った整数で指定する必要があります。管理アプリケーションによるリクエストの送信時、またはコンポーネント計測による結果の送信時、キーの値は **key** 文でリストされている順序どおりに送信される必要があります。

各グループにつき **key** 文は 1 つのみ許可されます。

## 属性定義

属性は、コンポーネントに関連付けられたデータの項目です。属性は、グループの範囲内で定義します。属性定義の構文は以下のとおりです。

```
start attribute

 name = "attribute name"

 id = nnn

 [description = "description string"]

 type = datatype

 [access = method]

 [storage = storagetype]

 [value = [v | * "name" | "enum string"]]

end attribute
```

必須の `id` 文は、グループ内のほかのすべての属性全体で一意的な値を持つ必要があります。グループは、少なくとも 1 つの属性定義を持つ必要があります。グループ定義内には多数の属性定義を指定できます。

## type 文

属性定義内の必須の **type** 文では、定義するストレージおよびセマンティクスの特徴を記述します。構文は以下のとおりです。

```
type = datatype
```

**datatype** は、通常、すでに定義されているデータ タイプの 1 つです。

データ タイプは列挙にすることもできます。この場合、符号付き 32 ビット整数として格納され、処理されます。（コンポーネント レベルで）すでに定義されている列挙は、1 つのタイプとして、名前によって参照できます（たとえば、**type = "Color"**）。また、列挙を「インライン」で構成することもできます。

```
type = start enum
 (enum definition
 end enum
```

この場合、列挙はこの属性定義のスコープ外では参照されないため、列挙の名前は必要ありません。指定した名前はすべて無視されます。

属性定義内には **type** 文は 1 つのみ指定できます。

## access 文

オプションの **access** 文では、属性値の読み取りまたは書き込みを可能にするかどうかを指定します。

構文は以下のとおりです。

```
access = method
```

```
method
```

アクセスを読み取り専用、読み書き可能、書き込み専用のいずれにするかを指定します。**access** 文を指定しない場合、デフォルトのアクセスは読み取り専用になります。キーとしてマークされた属性は、書き込み専用にはできません。属性定義内には **access** 文は 1 つのみ指定できます。

## storage 文

オプションの **storage** 文では、ストレージ要件を最適化するためのヒントを管理アプリケーションに提供します。

構文は以下のとおりです。

**storage** = where

**where**

ストレージエリアを指定します。共通ストレージにも、特定ストレージにもできます。共通ストレージは、この属性に使用できる値が非常に限定されていることを表します。**CPU** のクロック速度などは、共通ストレージの一例です。特定ストレージは、多くの異なる値が使用可能であるため、この属性の値が最適化するために最も適した値ではない可能性があることを表します。コンポーネントのシリアル番号などは、特定属性の一例です。

**storage** 文を指定しない場合、デフォルトのストレージは特定ストレージになります。属性定義内には **storage** 文は 1 つのみ指定できます。

## value 文

**value** 文は、値または値アクセスのメカニズムを提供します。

構文は以下のとおりです。

```
value = v
```

```
value = "enumeration value"
```

```
value = * "Name"
```

```
value = unsupported
```

**v**

属性が読み取り専用で、変更されないことを指定します。たとえば、コンポーネントの製造者などです。これに対してコンポーネント計測などでは、サービス レイヤが処理できるように読み書き属性を指定します。書き込み専用属性に対して **v** を指定することは禁止されています。値 **v** は、属性の適切なデータ タイプで指定する必要があります。たとえば、日付およびリテラル文字列は二重引用符で囲んで指定する必要があります。

**"enumeration value"**

値が列挙文字列であることを指定します。この値はサービス レイヤにより整数にマッピングされます。この値は二重引用符で囲みます。マッピングは、このコンポーネント定義または属性定義内の **enum** 定義ですでに定義されているものである必要があります。また、属性のタイプは列挙である必要があります。書き込み専用属性に対して列挙値を指定することは禁止されています。

注：列挙に対して整数を指定することは許容されています。

**\* "Name"**

実行時に属性の読み取りまたは書き込みを行うために起動するコンポーネント計測コードの記号名を指定します。記号名は、このコンポーネント定義内のパス定義ですでに定義されているものである必要があります。値 **\* "Name"** では、名前の前にアスタリスク (\*) を付け、名前を二重引用符で囲みます。

サポートされない値 (予約済みキーワード) を挿入して、この属性がこのコンポーネントでサポートされないことをサービス レイヤに指示することができます。

**value** 文は必須です。ただし、テーブルテンプレートが定義されている場合はオプションです。テンプレート内に値が指定されている場合は、その値がテーブルの作成時のデフォルト値になります。値を指定しない場合、デフォルト値はありません。

### 例：2つの属性を持つグループの例

Start Group

Name = "Software Template"

Class = "DMTF|Software Example|1"

Key = 1 // key on Product Name

Start Attribute

ID = 1

Name = "Product Name"

Description = "The name of the product"

Storage = Common

Type = String(64)

End Attribute

Start Attribute

ID = 2

Name = "Product Version"

Description = "The product's version number"

Type = String(32)

Value = ""

End Attribute

End Group

この例では、グループ ID はありませんが、キーが指定されているため、グループはテンプレートとして機能します。バージョンのデフォルト値は空の文字列です。製品名のデフォルトはありません。

## テーブルの作成

テーブルは、グループ インスタンスの配列で構成されます。インスタンスはテーブルの行です。各行の属性の値はコンポーネントによって提供されるため、多くの場合、テーブルを定義するには、キーと共にグループを定義するだけです。ただし、.MIF ファイルそのものにテーブルの値を指定して、属性定義内で値を定義すると効果的な場合もあります。

テーブル作成メカニズムにより、グループの定義がグループ内のデータから切り離されます。このメカニズムでは、すでに定義されているグループをテンプレートとして使用して MIF データベースに値を格納します。

テーブルを作成するための構文は、以下のとおりです。

```
start table

 name = "table name"

 id = nnn

 class = "class string"

 { v1[,v2 ...] }

 [{ vn[,vm ...] }]

end table
```

**name** 文でこのテーブルを記述する必要があります。必須の **id** 文では、このコンポーネント内のほかのすべてのグループおよびテーブル全体で一意的な整数値を指定します。必須の **class** 文では、テンプレートとして使用される定義済みのグループを指定します。

テーブル行では、上記のように値を指定し、カンマで区切って波カッコ「{」と「}」で囲みます。値のリストは属性 ID の順に（最も小さい ID を持つ属性の値を最初に）左から右に指定します。リスト内の値を省略した場合、それに対応する属性値（テンプレート内に定義されている場合）が「デフォルト」値として使用されます。テンプレート内にデフォルト値が指定されていない場合に属性値を省略することは、禁止されています。カンマの数が足りない行は、必要な数の後続カンマがある行として扱われます。このため、テンプレートで指定された値が、行内のその他の属性に対しても使用されます。

### 例：すでに定義されているグループを使用したテーブルの作成

```
start table

 Name = "Software Table"
```



```

Class = "DMTF|Software Example|1"

Id = 42

{"Circus", "4.0a"}

{"Disk Blaster", "2.0c"}

{"Oleo", "3.0"}

{"Presenter", "1.2"}

end table

```

この例では、4 行のテーブルが生成されます。行が取り込まれるとき、グループ定義内の **value** 文が、行そのものとしてでなくデフォルト値として使用されます。

キーを構成する属性の組み合わせに対して一意の値が指定されていない場合に、行を取り込むことは不適切です。サービス レイヤは、行の取り込み中に、一意のキーが指定されていない **MIF** を拒否する必要があります。

テーブル定義は、その参照先のグループ定義の後に指定する必要があります。グループは、ID 文でなく **key** 文を使用して指定されたグループである必要があります。1 つのテンプレートから複数のテーブルを作成できますが、各テーブルはそれぞれ異なる ID を持つ必要があります。

## ComponentID グループ

どの .MIF ファイルにも、ID 1 の標準グループが含まれている必要があります。このグループにより、コンポーネントのベース レベルでの認識が可能になり、ベンダーが提供する必要がある最小限の情報がわかります。属性がサポートされていないか、または当該コンポーネントに対して無効である場合は、値としてキーワード **unsupported** を指定する必要があります。

ComponentID. "DMTF|ComponentID|1.0" はクラス文字列です。グループの属性はすべて読み取り専用です。以下の表に、それらの定義を示します。

| Integer 名       | ID | タイプ        | ストレージ | 説明                 |
|-----------------|----|------------|-------|--------------------|
| "Manufacturer"  | 1  | String(64) | 共通    | このコンポーネントを作成した組織   |
| "Product"       | 2  | String(64) | 共通    | このコンポーネントまたは製品の名前  |
| "Version"       | 3  | String(64) | 詳細    | このコンポーネントのバージョン文字列 |
| "Serial Number" | 4  | String(64) | 詳細    | このコンポーネントのシリアル番号   |

|                |   |    |    |                              |
|----------------|---|----|----|------------------------------|
| "Installation" | 5 | 日付 | 詳細 | このシステムにコンポーネントを最後にインストールした日時 |
| "Verify"       | 6 | 整数 | 共通 | このコンポーネントの検証レベル              |

「Verify」属性値を問い合わせると、コンポーネントがシステム内にあるかどうか、およびコンポーネントが適切に機能しているかどうかを検証するためにコンポーネント計測が実行されます。以下の表に示す値の中からいずれか1つが返されます。

| 値 | 意味                             |
|---|--------------------------------|
| 0 | エラーが発生しました。ステータス コードを確認してください。 |
| 1 | コンポーネントは存在しません。                |
| 2 | 検証はサポートされていません。                |
| 4 | コンポーネントが存在します。機能はテストされていません。   |
| 5 | コンポーネントが存在します。機能は不明です。         |
| 6 | コンポーネントが存在します。機能は正常ではありません。    |
| 7 | コンポーネントが存在します。機能は正常です。         |

## .MIF ファイルの例

.MIF ファイルの例を以下に示します。

Start Component

```
// A double slash indicates that the line contains comments,
```

```
// and should be ignored...
```

```
// First we name and describe the component...
```

```
 Name = "AM Windows 95 PC information"
```

```
 Description = "This MIF file contains basic hardware inventory for a AM Windows 95
Computer"
```

```
// Then we list the groups...
```

Start Group

```
 // First we name the group....
```

```
 // Every group within the component must be
```

```
 // assigned a unique ID and a class...
```

```
 // and optionally a description
```

```
 Name = "Processors"
```

```
 Id = 1
```

```
 Class = "AM|Processors|001"
```

```
 Description = "Describes the processors present in the system"
```

```
// Then we list the groups attributes...
```

Start Attribute

```
 // First we name the attribute....
```

```
 // Every attribute within the group must be
```

```
 // assigned a unique ID and optionally a description
```

```
 Name = "Main processor type"
```

```
 Id = 1
```

```
 Description = "The type of processor currently in the system"
```

```
 // Specify the attribute type (A string)...
```

```
 Type = String(64)

 // ...and the attribute value...

 Value = "Pentium"

 // End of attribute...

End Attribute

// Describe a new attribute within the group...

Start Attribute

 Name = "Main processor speed"

 Id = 2

 Description = "Maximum speed (in MHz) of this processor"

 Type = Integer

 Value = 90

End Attribute

Start Attribute

 Name = "Main processor vendor ID"

 Id = 3

 Description = "This is the Vendor ID returned by the
processor in response to the CPUID instruction"

 Type = String(64)

 Value = "GenuineIntel"

End Attribute

// Continue until no more attributes in the group...

// End of group...

End Group

// Describe a new group within the component...

Start Group

 Name = "Operating system"

 Id = 2

 Class = "AM|OSsystem|001"
```

```
Description = "Describes the operating system running on this system"

Start Attribute

 Name = "Operating system"

 Id = 1

 Description = "Specifies the operating system"

 Type = String(64)

 Value = "Windows 95"

End Attribute

Start Attribute

 Name = "Operating system Major version"

 Id = 2

 Description = "Specifies the major version of the operating system"

 Type = Integer

 Value = 4

End Attribute

Start Attribute

 Name = "Operating system Minor version"

 Id = 3

 Description = "Specifies the minor version of the operating system"

 Type = Integer

 Value = 0

End Attribute

End Group

// Continue until no more groups in component..

// End of Component...

End Component
```

## Asset Management 圧縮テキスト ファイル

上記の .MIF ファイルに対するアセット管理圧縮テキスト ファイルを以下に示します。

000101[Asset Management Windows 95 PC information]

000201[Asset Management Windows 95 PC information|Processors]

00010500Main processor type|Pentium

00020201Main processor speed|90

00030500Main processor vendor ID|GenuineIntel

000301[Asset Management Windows 95 PC information|Operating system]

00010500Operating system|Windows 95

00020201Operating system Major version|4

00030201Operating system Minor version|0

# 付録 B: インベントリ マトリックス

このセクションには、以下のトピックが含まれています。

[レポートされるインベントリ項目のリスト \(P. 583\)](#)

## レポートされるインベントリ項目のリスト

基本スキャンでは拡張スキャンによってレポートされるインベントリのサブセットがレポートされ、拡張スキャンでは最低でも以下の表に示した項目が論理的に分類されて報告されることが予想されます。

NRI エージェントが制限ユーザにより実行される場合は、以下の説明を考慮する必要があります。

\* 制限ユーザによりレポートされない項目。

\*\* 管理者ユーザによりレポートされる場合、より複雑か有益になる項目。

\*\*\* リモート デスクトップ接続を通じて影響を受ける可能性がある値を持つ項目。

| インベントリ項目      | 基本スキャン | 拡張スキャン |
|---------------|--------|--------|
| ¥System       | X      | X      |
| 合計メモリ**       | X      | X      |
| 物理メモリ*        | X      | X      |
| OS がレポートするメモリ | X      | X      |
| モデル*          | X      | X      |
| タイプ*          | X      | X      |
| プロセッサ数        | X      | X      |
| COM ポート数*     |        | X      |
| プリンタ ポート数     |        | X      |
| USB ポート数*     |        | X      |
| ビデオ ポート数*     |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                | 基本スキャン | 拡張スキャン |
|-------------------------|--------|--------|
| ウェイクアップ タイプ*            |        | X      |
| ベンダ*                    | X      | X      |
| シリアル番号*                 | X      | X      |
| アセット タグ                 | X      | X      |
| システム ID*                | X      | X      |
|                         |        |        |
| ¥ System ¥ System Bios* |        | X      |
| ベンダ                     |        | X      |
| SM BIOS バージョン           |        | X      |
| バージョン                   |        | X      |
| ROM サイズ                 |        | X      |
| 日付                      |        | X      |
|                         |        |        |
| ¥System ¥ I/O Ports*    |        | X      |
| 内部指定子                   |        | X      |
| 内部コネクタ タイプ              |        | X      |
| 外部指定子                   |        | X      |
| 外部コネクタ タイプ              |        | X      |
| 外部ポート タイプ               |        | X      |
|                         |        |        |
| ¥ System ¥ Processors   | X      | X      |
| ベンダ ID                  | X      | X      |
| ベンダ                     | X      | X      |
| モデル                     | X      | X      |
| 速度                      | X      | X      |
| 最大 速度*                  |        | X      |
| タイプ                     |        | X      |



| インベントリ項目                | 基本スキャン | 拡張スキャン |
|-------------------------|--------|--------|
| シリアル番号                  |        | X      |
| アセット タグ*                |        | X      |
| ソケット指示子*                |        | X      |
| L2 キャッシュ*               |        | X      |
| ハイパースレッド                |        | X      |
| 64 ビット サポート             |        | X      |
| コア数                     | X      | X      |
|                         |        |        |
| ¥ System ¥ System Slots |        | X      |
| 名前                      |        | X      |
| バスのタイプ                  |        | X      |
| 現在の使用状況                 |        | X      |
| 速度                      |        | X      |
| バス幅                     |        | X      |
| 特徴                      |        | X      |
|                         |        |        |
| ¥System ¥ COM Ports     |        | X      |
| モデル                     |        | X      |
| ベンダ                     |        | X      |
| ドライバプロバイダ               |        | X      |
| ドライバ                    |        | X      |
| ドライババージョン               |        | X      |
| ロケーション                  |        | X      |
| ステータス テキスト              |        | X      |
| ステータス                   |        | X      |
|                         |        |        |
| ¥ System ¥ Memory       |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目             | 基本スキャン | 拡張スキャン |
|----------------------|--------|--------|
| メモリ バンク              |        | x      |
| サイズ                  |        | x      |
| タイプ                  |        | x      |
| シリアル番号               |        | x      |
| ロケーション               |        | x      |
| メモリ形式                |        | x      |
| 用途                   |        | x      |
| 動作周波数                |        | x      |
|                      |        |        |
| ¥ System ¥ Mainboard |        | x      |
| ベンダ                  |        | x      |
| バージョン                |        | x      |
| メモリ バンク数             |        | x      |
| 使用しているメモリ バンクの数      |        | x      |
| 空いているメモリ バンクの数       |        | x      |
| BIOS ROM サイズ         |        | x      |
| CPU ソケットの数           |        | x      |
| 使用している CPU ソケットの数    |        | x      |
| モデル                  |        | x      |
| 空いている CPU ソケットの数     |        | x      |
| シリアル番号               |        | x      |
|                      |        |        |
| ¥ System Devices     | x      | x      |
| サウンドアダプタ数            |        | x      |
| ビデオアダプタ数             |        | x      |
| ネットワーク アダプタ数         | x      | x      |
| IDE コントローラ数          |        | x      |

| インベントリ項目                                 | 基本スキャン | 拡張スキャン |
|------------------------------------------|--------|--------|
| USB コントローラ数                              |        | X      |
| フロッピー ディスク コントローラ数                       |        | X      |
| SCSI コントローラ数                             |        | X      |
| PCI コントローラ数                              |        | X      |
| <b>¥ System Devices ¥ Sound Adapters</b> |        | X      |
| モデル                                      |        | X      |
| ベンダ                                      |        | X      |
| ドライバプロバイダ                                |        | X      |
| ドライバ                                     |        | X      |
| ドライババージョン                                |        | X      |
| ロケーション                                   |        | X      |
| ステータス テキスト                               |        | X      |
| ステータス                                    |        | X      |
| <b>¥ System Devices ¥ Video Adaptors</b> |        | X      |
| モデル                                      | X      | X      |
| ベンダ                                      | X      | X      |
| ドライバプロバイダ                                |        | X      |
| ドライバ                                     |        | X      |
| ドライババージョン                                |        | X      |
| ロケーション                                   |        | X      |
| ステータス テキスト                               |        | X      |
| ステータス                                    |        | X      |
| チップ タイプ                                  |        | X      |
| BIOS 文字列                                 |        | X      |
| メモリ サイズ                                  |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                            | 基本スキャン | 拡張スキャン |
|-------------------------------------|--------|--------|
| X 解像度                               |        | X      |
| Y 解像度                               |        | X      |
| リフレッシュ周波数***                        |        | X      |
| Color 深度                            |        | X      |
|                                     |        |        |
| ¥ System Devices ¥ Network Adapters | X      | X      |
| モデル                                 | X      | X      |
| ベンダ                                 |        | X      |
| ドライバプロバイダ                           |        | X      |
| ドライバ                                |        | X      |
| ドライババージョン                           |        | X      |
| ロケーション                              |        | X      |
| ステータス テキスト                          |        | X      |
| ステータス                               |        | X      |
| MAC アドレス                            | X      | X      |
| 速度                                  |        | X      |
| 説明                                  | X      | X      |
| アダプタ タイプ                            |        | X      |
| デバイス名                               |        | X      |
|                                     |        |        |
| ¥ System Devices ¥ IDE Controllers  |        | X      |
| モデル                                 |        | X      |
| ベンダ                                 |        | X      |
| ドライバプロバイダ                           |        | X      |
| ドライバ                                |        | X      |
| ドライババージョン                           |        | X      |
| ロケーション                              |        | X      |

| インベントリ項目                                     | 基本スキャン | 拡張スキャン |
|----------------------------------------------|--------|--------|
| ステータス テキスト                                   |        | x      |
| ステータス                                        |        | x      |
|                                              |        |        |
| <b>¥ System Devices ¥ USB Controllers</b>    |        | x      |
| モデル                                          |        | x      |
| ベンダ                                          |        | x      |
| ドライバプロバイダ                                    |        | x      |
| ドライバ                                         |        | x      |
| ドライババージョン                                    |        | x      |
| ロケーション                                       |        | x      |
| ステータス テキスト                                   |        | x      |
| ステータス                                        |        | x      |
|                                              |        |        |
| <b>¥ System Devices ¥ Floppy Controllers</b> |        | x      |
| モデル                                          |        | x      |
| ベンダ                                          |        | x      |
| ドライバプロバイダ                                    |        | x      |
| ドライバ                                         |        | x      |
| ドライババージョン                                    |        | x      |
| ロケーション                                       |        | x      |
| ステータス テキスト                                   |        | x      |
| ステータス                                        |        | x      |
|                                              |        |        |
| <b>¥ System Devices ¥ SCSI Controllers</b>   |        | x      |
| モデル                                          |        | x      |
| ベンダ                                          |        | x      |
| ドライバプロバイダ                                    |        | x      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                      | 基本スキャン | 拡張スキャン |
|-----------------------------------------------|--------|--------|
| ドライバ                                          |        | x      |
| ドライババージョン                                     |        | x      |
| ロケーション                                        |        | x      |
| ステータス テキスト                                    |        | x      |
| ステータス                                         |        | x      |
| <b>¥ System Devices ¥ PCI Controllers</b>     |        | x      |
| ベンダ                                           |        | x      |
| モデル                                           |        | x      |
| リビジョン                                         |        | x      |
| <b>¥ Operating System</b>                     |        | x      |
| バージョン                                         | x      | x      |
| ベンダ                                           |        |        |
| リリース                                          |        |        |
| サービス パック                                      | x      | x      |
| オペレーティング システム                                 | x      | x      |
| 言語                                            | x      | x      |
| ローカル言語                                        |        | x      |
| 仮想マシン                                         | x      | x      |
| Windows アップデート数                               |        | x      |
| プラットフォーム タイプ                                  |        | x      |
| <b>¥ Operating System ¥ Regional Settings</b> |        | x      |
| 国コード                                          |        | x      |
| 国名                                            |        | x      |
| 通貨スタイル                                        |        | x      |

| インベントリ項目                                     | 基本スキャン | 拡張スキャン |
|----------------------------------------------|--------|--------|
| 通貨記号                                         |        | X      |
| データの区切り記号                                    |        | X      |
| 日付の形式                                        |        | X      |
| 日付の区切り記号                                     |        | X      |
| 小数点の記号                                       |        | X      |
| 言語                                           |        | X      |
| 単位システム                                       |        | X      |
| 通貨の有効桁数                                      |        | X      |
| 3 桁区切り記号                                     |        | X      |
| 時刻の形式                                        |        | X      |
| 時刻の区切り記号                                     |        | X      |
| <b>¥ Operating System ¥ Display Settings</b> |        | X      |
| アダプタ名                                        |        | X      |
| 解決方法                                         |        | X      |
| 水平解像度                                        |        | X      |
| 垂直解像度                                        |        | X      |
| 表示周波数***                                     |        | X      |
| Color 深度                                     |        | X      |
| <b>¥ Operating System ¥ Installation</b>     |        | X      |
| バージョン                                        |        | X      |
| メジャーバージョン                                    |        | X      |
| マイナーバージョン                                    |        | X      |
| サービス パック                                     |        | X      |
| ビルド番号                                        |        | X      |
| 名前                                           |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                   | 基本スキャン | 拡張スキャン |
|--------------------------------------------|--------|--------|
| ベンダ                                        |        | X      |
| 製品 ID                                      |        | X      |
| プロダクト キー                                   |        | X      |
| 組織                                         |        | X      |
| ライセンス                                      |        | X      |
| システム パス                                    |        | X      |
| インストール日                                    |        | X      |
| 言語                                         |        | X      |
| Hyper V 有効                                 |        | X      |
| Hyper V 対応                                 |        | X      |
| <b>¥ Operating System ¥ System Updates</b> |        | X      |
| 更新                                         |        | X      |
| 説明                                         |        | X      |
| インストール ユーザ名                                |        | X      |
| インストール日付                                   |        | X      |
| タイプ                                        |        | X      |
| アンインストール プログラム                             |        | X      |
| <b>¥ Operating System ¥ Cron Queue</b>     |        | X      |
| ユーザ名                                       |        | X      |
| 索引の入力                                      |        | X      |
| 分                                          |        | X      |
| 時間                                         |        | X      |
| 日付                                         |        | X      |
| 月                                          |        | X      |
| 曜日                                         |        | X      |



| インベントリ項目                                      | 基本スキャン | 拡張スキャン |
|-----------------------------------------------|--------|--------|
| コマンド                                          |        | x      |
| <b>¥ Operating System ¥ Installed Patches</b> |        | x      |
| 名前                                            |        | x      |
| <b>¥ Operating System ¥ Swap Devices</b>      |        | x      |
| サイズ                                           |        | x      |
| 空き                                            |        | x      |
| デバイス                                          |        | x      |
| <b>¥ Network</b>                              |        |        |
| コンピュータ名                                       | x      | x      |
| コンピュータの説明                                     |        | x      |
| IP アドレス                                       | x      | x      |
| ホスト名                                          | x      | x      |
| ドメイン名                                         | x      | x      |
| IPv4 対応                                       | x      | x      |
| IPv6 対応                                       | x      | x      |
| <b>¥ Network ¥ TCP/IP</b>                     | x      | x      |
| IP アドレス                                       | x      | x      |
| サブネット マスク                                     |        | x      |
| MAC アドレス                                      |        | x      |
| ドメイン ネーム サーバ                                  |        | x      |
| ネットワーク アダプタ                                   | x      | x      |
| ドライバ                                          |        | x      |
| ドライババージョン                                     |        | x      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                    | 基本スキャン | 拡張スキャン |
|---------------------------------------------|--------|--------|
| ドライバプロバイダ                                   |        | X      |
| ホスト名                                        | X      | X      |
| ドメイン                                        | X      | X      |
| デフォルト ゲートウェイ                                |        | X      |
| DHCP                                        |        | X      |
| DHCP サーバ                                    |        | X      |
| リース取得日                                      |        | X      |
| リース有効期限                                     |        | X      |
| WINS*                                       |        | X      |
| プライマリ WINS サーバ*                             |        | X      |
| セカンダリ WINS サーバ*                             |        | X      |
| デバイス名                                       |        | X      |
| <b>¥ Network ¥ DNS</b>                      |        | X      |
| サーバ                                         |        | X      |
| シーケンス                                       |        | X      |
| ドメイン                                        |        | X      |
| サーバ名                                        |        | X      |
| ホスト                                         |        | X      |
| <b>¥ Network ¥ WINS</b>                     |        | X      |
| ネットワーク アダプタ                                 |        | X      |
| セカンダリ WINS サーバ                              |        | X      |
| プライマリ WINS サーバ                              |        | X      |
| <b>¥ Network ¥TCP/IPv6 ¥ IPv6 Addresses</b> |        | X      |
| IPv6 アドレス                                   | X      | X      |

| インベントリ項目                        | 基本スキャン | 拡張スキャン |
|---------------------------------|--------|--------|
| ゾーン ID                          |        | X      |
| MAC アドレス                        |        | X      |
| ドメイン                            | X      | X      |
| DHCP                            |        | X      |
| デバイス名                           |        | X      |
| プレフィックス発行元                      |        | X      |
| サフィックス発行元                       |        | X      |
| 有効な存続時間                         |        | X      |
| 優先存続時間                          |        | X      |
| リース存続時間                         |        | X      |
| DAD 状態                          |        | X      |
| タイプ                             |        | X      |
| ネットワーク アダプタ                     | X      | X      |
| プライマリ DNS サーバ                   |        | X      |
| DHCPv6 サーバ                      |        | X      |
| トンネル タイプ                        |        | X      |
| デフォルト ゲートウェイ                    |        | X      |
| WINS サーバ                        |        | X      |
| ホスト名                            |        | X      |
| プレフィックス長                        |        | X      |
| ¥ Network ¥ TCP/IPv6 ¥ DNS      |        | X      |
| サーバ                             |        | X      |
| ゾーン ID                          |        | X      |
| シーケンス                           |        | X      |
| ¥ Network ¥ TCP/IPv6 ¥ Gateways |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                                                                                                       | 基本スキャン | 拡張スキャン |
|--------------------------------------------------------------------------------------------------------------------------------|--------|--------|
| 住所                                                                                                                             |        | X      |
| ゾーン ID                                                                                                                         |        | X      |
| 注：IPv6 インベントリには、Windows XP および Windows 2003 Server でのゲートウェイに関する情報は含まれていません。Windows Vista 以降の Windows のバージョンでのゲートウェイ情報のみが含まれます。 |        |        |
| ¥ Storage                                                                                                                      | X      | X      |
| 固定ドライブ数                                                                                                                        | X      | X      |
| フロッピー ドライブ数                                                                                                                    |        | X      |
| CD-ROM ドライブ数                                                                                                                   |        | X      |
| ディスク領域の合計                                                                                                                      |        | X      |
| ¥ Storage ¥ Fixed Drives                                                                                                       |        | X      |
| モデル                                                                                                                            |        | X      |
| ベンダ                                                                                                                            |        | X      |
| ドライバプロバイダ                                                                                                                      |        | X      |
| ドライバ                                                                                                                           |        | X      |
| ドライババージョン                                                                                                                      |        |        |
| 場所**                                                                                                                           |        | X      |
| ステータス テキスト                                                                                                                     |        | X      |
| ステータス                                                                                                                          |        | X      |
| シリアル番号*                                                                                                                        |        | X      |
| ファームウェア バージョン*                                                                                                                 |        | X      |
| ターゲット ID*                                                                                                                      |        | X      |
| インターフェース                                                                                                                       |        | X      |
| デバイス                                                                                                                           |        | X      |
| サイズ*                                                                                                                           |        | X      |

| インベントリ項目                         | 基本スキャン | 拡張スキャン |
|----------------------------------|--------|--------|
| キャッシュ サイズ*                       |        | X      |
| シリンダ*                            |        | X      |
| シリンダあたりのトラック数*                   |        | X      |
| トラックあたりのセクタ数*                    |        | X      |
| セクタあたりのバイト数*                     |        | X      |
| <b>¥ Storage ¥ Floppy Drives</b> |        | X      |
| モデル                              |        | X      |
| ベンダ                              |        | X      |
| ドライバプロバイダ                        |        | X      |
| ドライバ                             |        | X      |
| ドライババージョン                        |        | X      |
| ロケーション                           |        | X      |
| ステータス テキスト                       |        | X      |
| ステータス                            |        | X      |
| デバイス                             |        | X      |
| <b>¥ Storage ¥ CD-ROM Drives</b> |        | X      |
| モデル                              |        | X      |
| ベンダ**                            |        | X      |
| ドライバプロバイダ                        |        | X      |
| ドライバ                             |        | X      |
| ドライババージョン                        |        | X      |
| ロケーション                           |        | X      |
| ステータス テキスト                       |        | X      |
| ステータス                            |        | X      |
| シリアル番号*                          |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                            | 基本スキャン | 拡張スキャン |
|-------------------------------------|--------|--------|
| ファームウェア リビジョン*                      |        | X      |
| ターゲット ID*                           |        | X      |
| インターフェース                            |        | X      |
| デバイス                                |        | X      |
| DVD ドライブ*                           |        | X      |
|                                     |        |        |
| ¥ File System                       | X      | X      |
| 論理ボリューム数                            |        | X      |
| ローカル ファイル システム数                     |        | X      |
| パーティション数                            |        | X      |
|                                     |        |        |
| ¥ File Systems ¥ Local File Systems | X      | X      |
| 名前                                  | X      | X      |
| サイズ                                 | X      | X      |
| 使用中                                 | X      | X      |
| 空き                                  | X      | X      |
| 使用率                                 | X      | X      |
| タイプ                                 | X      | X      |
| ファイル システム                           |        | X      |
| ボリューム ラベル                           |        | X      |
| マウント ポイント                           |        | X      |
| デバイス                                |        | X      |
| シリアル番号                              |        | X      |
|                                     |        |        |
| ¥ File Systems ¥ Logical Volumes    |        | X      |
| 名前                                  |        | X      |
| ボリューム サイズ                           |        | X      |

| インベントリ項目                   | 基本スキャン | 拡張スキャン |
|----------------------------|--------|--------|
| 使用済みボリューム サイズ              |        | x      |
| 空きボリューム サイズ                |        | x      |
| 使用ボリューム率                   |        | x      |
| ファイル システム                  |        | x      |
| ドライブ モデル                   |        | x      |
| ドライブ デバイス                  |        | x      |
| ボリューム デバイス                 |        | x      |
|                            |        |        |
| ¥ File System ¥ Partitions |        | x      |
| ブート可能デバイス                  |        | x      |
| ドライブ デバイス                  |        | x      |
| ファイル システム                  |        | x      |
| パーティション数                   |        | x      |
| パーティション タイプ                |        | x      |
| 認識されたパーティション               |        | x      |
| サイズ                        |        | x      |
| 始動オフセット (バイト)              |        | x      |
| ボリューム デバイス                 |        | x      |
|                            |        |        |
| ¥ Input Devices            |        |        |
| キーボード                      |        | x      |
| ポインティング デバイス               |        | x      |
|                            |        |        |
| ¥ Input Devices ¥ Keyboard |        | x      |
| モデル                        |        | x      |
| ベンダ                        |        | x      |
| ドライバプロバイダ                  |        | x      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                  | 基本スキャン | 拡張スキャン |
|-------------------------------------------|--------|--------|
| ドライバ                                      |        | X      |
| ドライババージョン                                 |        | X      |
| ロケーション                                    |        | X      |
| ステータス テキスト                                |        | X      |
| ステータス                                     |        | X      |
| <b>¥ Input Devices ¥ Pointing Devices</b> |        | X      |
| モデル                                       |        | X      |
| ベンダ                                       |        | X      |
| ドライバプロバイダ                                 |        | X      |
| ドライバ                                      |        | X      |
| ドライババージョン                                 |        | X      |
| ロケーション                                    |        | X      |
| ステータス テキスト                                |        | X      |
| ステータス                                     |        | X      |
| ボタン数                                      |        | X      |
| 左利き                                       |        | X      |
| タイプ                                       |        | X      |
| ホイール***                                   |        | X      |
| ボタンの切り替え                                  |        | X      |
| <b>¥ External Devices</b>                 |        | X      |
| モニタ数                                      |        | X      |
| プリンタ数                                     |        | X      |
| デフォルト プリンタ                                |        | X      |
| <b>¥ External Devices ¥ Monitor</b>       |        | X      |



| インベントリ項目                                  | 基本スキャン | 拡張スキャン |
|-------------------------------------------|--------|--------|
| モデル                                       |        | X      |
| ベンダ                                       |        | X      |
| ドライバプロバイダ                                 |        | X      |
| ドライバ                                      |        | X      |
| ドライババージョン                                 |        | X      |
| ロケーション                                    |        | X      |
| ステータス テキスト                                |        | X      |
| ステータス                                     |        | X      |
| 最大 解決方法                                   |        | X      |
| シリアル番号                                    |        | X      |
| 製造年                                       |        | X      |
| 製造週                                       |        | X      |
| <b>¥ External Devices ¥ Local Printer</b> |        | X      |
| モデル                                       |        | X      |
| ロケーション                                    |        | X      |
| コメント                                      |        | X      |
| デフォルト プリンタ                                |        | X      |
| ポート                                       |        | X      |
| <b>¥ Power Settings</b>                   |        | X      |
| ハイバネーションのサポート                             |        | X      |
| UPS あり                                    |        | X      |
| <b>¥ Power Settings ¥AC Adapter</b>       |        | X      |
| AC 電源                                     |        | X      |
| ドライバ                                      |        | X      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                           | 基本スキャン | 拡張スキャン |
|----------------------------------------------------|--------|--------|
| ドライバプロバイダ                                          |        | x      |
| ドライババージョン                                          |        | x      |
| ロケーション                                             |        | x      |
| モデル                                                |        | x      |
| ステータス                                              |        | x      |
| ステータス テキスト                                         |        | x      |
| ベンダ                                                |        | x      |
| <b>¥ Power Settings ¥ Power Policy</b>             |        | x      |
| AC – ハードディスク タイムアウト                                |        | x      |
| AC – ハイバネート タイムアウト                                 |        | x      |
| AC – モニタ タイムアウト                                    |        | x      |
| AC – スリープ タイムアウト                                   |        | x      |
| 電源スキーム名                                            |        | x      |
| ハイバネーションのサポート                                      |        | x      |
| <b>¥ Power Settings ¥ Power Policy ¥ AC Policy</b> |        | x      |
| 表示の暗転                                              |        | x      |
| 動的スロットル                                            |        | x      |
| ファン スロットル許容範囲 %                                    |        | x      |
| 強制スロットル %                                          |        | x      |
| ハードディスク スピンドアウン タイムアウト                             |        | x      |
| アイドル感度 %                                           |        | x      |
| アイドル タイムアウト                                        |        | x      |
| 最大スリープ                                             |        | x      |
| 最小スリープ                                             |        | x      |
| 最小スロットル %                                          |        | x      |

| インベントリ項目                                                                                                                                                                                                                                                                               | 基本スキャン | 拡張スキャン |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------|
| 電源用の最適化                                                                                                                                                                                                                                                                                |        | x      |
| 待機スリープ時間削減                                                                                                                                                                                                                                                                             |        | x      |
| 一時停止（休止タイムアウト）                                                                                                                                                                                                                                                                         |        | x      |
| ビデオ タイムアウト                                                                                                                                                                                                                                                                             |        | x      |
| Win ログオン フラグ                                                                                                                                                                                                                                                                           |        | x      |
| ブロードキャスト容量精度（バッテリーが存在する場合にのみ表示）                                                                                                                                                                                                                                                        |        | x      |
| LID - 閉（ラップトップなど LID が存在する場合のみ表示）                                                                                                                                                                                                                                                      |        | x      |
| LID - 開（LID が存在する場合のみ表示）                                                                                                                                                                                                                                                               |        | x      |
| <b>¥ Power Settings ¥ Power Policy ¥ AC Policy ¥ Power Button Pressed</b><br>（また、¥ Power Settings ¥ Power Policy ¥ AC Policy ¥ Sleep Button Pressed、¥ Power Settings ¥ Power Policy ¥ AC Policy ¥ On Enter Idle State、および¥ Power Settings ¥ Power Policy ¥ AC Policy ¥ Over Throttled） |        | x      |
| アクション                                                                                                                                                                                                                                                                                  |        | x      |
| イベント コード: ユーザの電源ボタンの押下をクリア                                                                                                                                                                                                                                                             |        | x      |
| イベント コード: ユーザの電源ボタンの押下に対する応答                                                                                                                                                                                                                                                           |        | x      |
| イベント コード: シャットダウン/オフ                                                                                                                                                                                                                                                                   |        | x      |
| イベント コード: 実行するプログラムを指定                                                                                                                                                                                                                                                                 |        | x      |
| イベント コード: 音でユーザに通知                                                                                                                                                                                                                                                                     |        | x      |
| イベント コード : UI でユーザに通知                                                                                                                                                                                                                                                                  |        | x      |
| フラグ: すべての起動イベントを無効化                                                                                                                                                                                                                                                                    |        | x      |
| フラグ: クリティカルな強制一時停止                                                                                                                                                                                                                                                                     |        | x      |
| フラグ: 最も明るいものが最初                                                                                                                                                                                                                                                                        |        | x      |
| フラグ: コンソールをロック                                                                                                                                                                                                                                                                         |        | x      |
| フラグ: アプリケーション上書き                                                                                                                                                                                                                                                                       |        | x      |

## レポートされるインベントリ項目のリスト

| インベントリ項目                                           | 基本スキャン | 拡張スキャン |
|----------------------------------------------------|--------|--------|
| フラグ: クエリ許可                                         |        | X      |
| フラグ: UI 許可                                         |        | X      |
|                                                    |        |        |
| ¥ System Status                                    | X      | X      |
| ブート時間                                              |        | X      |
| ハードウェア スキャン                                        | X      | X      |
| 動作時間                                               |        | X      |
| DSM エージェント ユーザ アカウント                               | X      | X      |
| DSM エージェント ユーザ特権                                   | X      | X      |
| 現在のユーザ数                                            |        | X      |
| FIPS モード                                           | X      |        |
| ソフトウェア シグネチャ ファイル作成日                               |        | X      |
| ソフトウェア シグネチャ ファイル配信日                               |        | X      |
|                                                    |        |        |
| ¥ System Status¥ Agent Software                    |        | X      |
| DSM エージェント ユーザ特権                                   |        | X      |
| DSM エージェント ユーザ アカウント                               |        | X      |
| ベンダ                                                |        | X      |
| バージョン                                              |        | X      |
| ビルド                                                |        | X      |
| Basedir                                            |        | X      |
|                                                    |        |        |
| ¥ System Status¥ Agent Software ¥ Inventory Module |        | X      |
| 説明                                                 |        | X      |
| ファイル サイズ                                           |        | X      |
| バージョン                                              |        | X      |
| ファイル日付                                             |        | X      |

| インベントリ項目                         | 基本スキャン | 拡張スキャン |
|----------------------------------|--------|--------|
| ビルド                              |        | x      |
| ファイル                             |        | x      |
|                                  |        |        |
| ¥ System Status¥ Logged in users |        | x      |
| ユーザ識別                            |        | x      |
| ログイン                             |        | x      |
| ログインに使用する項目                      |        | x      |
| ユーザ名                             |        | x      |
|                                  |        |        |



# 付録 C: インベントリ ファイル プロパティ

DCS は、エージェント コンピュータにリンクされた収集タスクで設定した各インベントリ検出モジュールに 1 つのインベントリ ファイルを作成します。インベントリ ファイルは、エージェントの作業ディレクトリで使用できます。それには、1 つのコンポーネント（トップレベル グループ）が含まれており、その名前はそのインベントリ検出モジュール設定から取り込まれます。

以下のセクションでは、インベントリ ファイルのテーブル、グループ、および属性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。

- [Status \(グループ\)](#) (P. 607)
- [Status/Input Files \(テーブル\)](#) (P. 608)
- [Status/Output Files \(テーブル\)](#) (P. 608)
- [General \(グループ\)](#) (P. 609)
- [General/Identity \(オプション グループ\)](#) (P. 609)
- [Target \(グループ\)](#) (P. 610)
- [Target/Facts \(オプション テーブル\)](#) (P. 610)
- [Set Values \(テーブル\)](#) (P. 611)
- [Rule Results/<rule id> \(グループ\)](#) (P. 611)
- [Rule Results/<rule id>/Idents \(オプション テーブル\)](#) (P. 612)
- [Scores \(テーブル\)](#) (P. 612)

## Status (グループ)

Status グループには、コンプライアンス チェックの全体のステータスに関する以下の情報が含まれます。

| 属性    | タイプ  | 説明                       |
|-------|------|--------------------------|
| 確認完了  | ブール値 | 完了したチェックが成功したかどうかを示します。  |
| ステータス | 文字列  | チェックが完了できなかった場合、理由を示します。 |

## Status/Input Files ( テーブル )

Status/Input Files テーブルには、処理される SCAP データ ストリーム ファイルに関する以下の情報が含まれます。

| 属性      | タイプ    | 説明                                   |
|---------|--------|--------------------------------------|
| 名前      | string | 入力 SCAP データ ストリームのファイル名を示します。        |
| タイプ     | string | 入力ファイルが XCCDF ファイルか OVAL ファイルかを示します。 |
| ロケーション  | string | 入力ファイルの場所を示します。                      |
| タイムスタンプ | string | 入力ファイルが作成された日時を示します。                 |
| サイズ     | int64  | 入力ファイルのサイズをバイト単位で示します。               |

## Status/Output Files ( テーブル )

Status/Output Files には、スキャナが作成する出力ファイルに関する以下の情報が含まれます。

注：このテーブルにはインベントリ ファイルは含まれません。

| 属性      | タイプ    | 説明                                   |
|---------|--------|--------------------------------------|
| 名前      | string | 出力ファイル名を示します。                        |
| タイプ     | string | 出力ファイルが XCCDF ファイルか OVAL ファイルかを示します。 |
| ロケーション  | string | 出力ファイルの場所を示します。                      |
| タイムスタンプ | string | 出力ファイルが作成された日時を示します。                 |
| サイズ     | int64  | 出力ファイルのサイズをバイト単位で示します。               |



## General (グループ)

General グループにはベンチマークおよびそのテストに関する以下の情報が含まれます。

| 属性                                   | タイプ    | 説明                                                     |
|--------------------------------------|--------|--------------------------------------------------------|
| ID                                   | string | 特定のインベントリ ファイルでレポートされるテスト結果の一意の ID を示します。              |
| プロファイル                               | string | オプション。ベンチマークの実行時に、適用されるプロファイルの ID を示します。               |
| 開始時間                                 | string | ベンチマークの実行またはコンプライアンス チェックの開始時間を示します。                   |
| 終了時間                                 | string | チェックの終了時間を示します。開始および終了時間は、XCCDF ファイルで使用する形式の文字列で示されます。 |
| ベンチマーク 参照                            | int64  | 使用した XCCDF ファイルへの参照(ファイル名またはリンク) を示します。                |
| タイトル                                 | string | オプション                                                  |
| コメント                                 | string | オプション                                                  |
| 組織                                   | string | オプション。結果に関連している組織を示します。                                |
| Organization_2、<br>Organization_3... | string | オプション。追加の組織を示します。追加の組織に階層構造がある場合は、上位の組織から順番に表示されます。    |

## GeneralIdentity (オプション グループ)

General/Identity オプション グループ には、テストに使用されるユーザ アカウントに関する以下の情報が含まれます。

| 属性 | タイプ    | 説明                            |
|----|--------|-------------------------------|
| 名前 | string | ベンチマークの識別名 (ユーザ アカウント) を示します。 |

| 属性   | タイプ  | 説明                     |
|------|------|------------------------|
| 特権   | bool | ID が特権（管理者）であることを示します。 |
| 認証済み | bool | ID が認証済みであることを示します。    |

## Target (グループ)

Target グループには、スキャナがベンチマーク テストを実行したターゲット システムに関する、以下の情報が含まれます。

| 属性         | タイプ    | 説明                                 |
|------------|--------|------------------------------------|
| 名前         | string | ベンチマークテストが実行されたターゲット システムの名前を示します。 |
| 住所         | string | オプション。ターゲット システムのネットワーク アドレスを示します。 |
| 住所 2、3、... | string | オプション。追加のネットワーク アドレスを示します。         |

## Target/Facts (オプション テーブル)

Target/Facts オプション テーブルには、ターゲット システムに関する、以下の情報が含まれます。

| 属性  | タイプ    | 説明                         |
|-----|--------|----------------------------|
| 名前  | string | ファクトの名前を示します (URL)。        |
| タイプ | string | 「数値」、「文字列」または「ブール値」を指定します。 |
| 値   | string | 値を示します。                    |

## Set Values ( テーブル )

Set Values テーブルには、テスト中に値オブジェクトに使用した値に関する以下の情報が含まれます。

| 属性 | タイプ    | 説明               |
|----|--------|------------------|
| ID | string | 使用した値の ID を示します。 |
| 値  | string | 使用した値を示します。      |

## Rule Results/<rule id> ( グループ )

Rule Results/*rule id* グループには、テスト中に選択した各ルールに作成されたグループに関する以下の情報が含まれます。

| 属性    | タイプ    | 説明                                              |
|-------|--------|-------------------------------------------------|
| Idref | string | ファクトの名前を示します (URL) 。                            |
| ルール   | string |                                                 |
| 時間    | string | 結果が生成された時刻を示します。                                |
| 重大度   | string |                                                 |
| バージョン | string |                                                 |
| 加重    | double | 加重スコアリング モデルの結果の重さを示します。                        |
| 結果    | string | 「合格」、「不合格」、「エラー」、「不明」、「未確認」または「適用不可」などの結果を示します。 |

## Rule Results/<rule id>/Idents ( オプション テーブル )

Rule Results/*rule id*/Idents オプション テーブルには、グローバルに意味のある以下の情報を持つ CCE ID などのルール ID のテーブルが含まれます。

| 属性   | タイプ    | 説明                     |
|------|--------|------------------------|
| システム | string | 命名システムを識別する URL を示します。 |
| 名前   | string | 命名システムの ID の名前を示します。   |

## Scores ( テーブル )

Scores テーブルには、ベンチマークで指定したモデルに応じたテスト スコアに関する以下の情報が含まれます。

| 属性  | タイプ    | 説明                  |
|-----|--------|---------------------|
| モデル | string | スコア モデルの URL を示します。 |
| スコア | double | 達成したスコアを示します。       |
| 最大  | double | 可能な最大スコアを示します。      |

## 付録 D: プラットフォーム名および ID

---

以下の表には、インベントリ ファイルの *general* セクションにある *class\_id* タグに指定できるプラットフォームが含まれます。クラス ID は、数値または文字列値として指定できます。

注：サポート対象のオペレーティング システムのリストについては、「[認定マトリックス](#)」を参照してください。

| クラス ID ( プラット<br>フォーム ID ) | プラットフォーム名                              |
|----------------------------|----------------------------------------|
| 0                          | 未分類                                    |
| 2                          | Windows                                |
| 3                          | Windows Server 2003                    |
| 4                          | Windows Server 2003 Web Edition        |
| 5                          | Windows Server 2003 Enterprise Edition |
| 6                          | Windows Server 2003 Datacenter Edition |
| 7                          | Windows 2000                           |
| 8                          | Windows 2000 Professional              |
| 9                          | Windows 2000 Advanced Server           |
| 10                         | Windows 2000 DC Server                 |
| 11                         | Windows 2000 Server                    |
| 12                         | Windows 9x                             |
| 13                         | Windows 95                             |
| 14                         | Windows 98                             |
| 15                         | Windows 98 SE                          |
| 16                         | Windows ME                             |
| 17                         | Windows NT                             |
| 18                         | Windows NT Workstation 3.51            |
| 19                         | Windows NT workstation 4.0             |

|    |                                     |
|----|-------------------------------------|
| 20 | Windows NT Server 4.0               |
| 21 | Windows NT Server 4.0 Enterprise    |
| 22 | Windows XP                          |
| 23 | Windows XP Home                     |
| 24 | Windows XP Professional             |
| 25 | Windows XP Media Center Edition     |
| 26 | Windows XP Tablet PC Edition        |
| 27 | Windows XP Professional x64 Edition |
| 28 | Windows 3x                          |
| 29 | Windows 3.0                         |
| 30 | Windows 3.1                         |
| 31 | Windows 3.11                        |
| 32 | Windows CE                          |
| 33 | Windows CE 2.00                     |
| 34 | Windows CE 2.01                     |
| 35 | Windows CE 2.11                     |
| 36 | Windows CE 3.00                     |
| 37 | Windows Mobile 2003                 |
| 38 | Palm OS                             |
| 39 | Symbian                             |
| 40 | Unix                                |
| 41 | DG_UX                               |
| 42 | Tru64                               |
| 43 | HP Tru64 4                          |
| 44 | DEC 3.0                             |
| 45 | DEC 3.2                             |
| 46 | DEC 4.0                             |
| 47 | HP Tru64 5                          |
| 48 | FUJIUxp                             |

|    |                    |
|----|--------------------|
| 49 | HPUnix             |
| 50 | HPUX 9             |
| 51 | HPUX 10            |
| 52 | HPUX 11            |
| 53 | ICLUnix            |
| 54 | Linux              |
| 74 | NCRUnix            |
| 75 | NCR SV             |
| 76 | NCR SV 2x          |
| 77 | NCR SV 3x          |
| 78 | NCR SST            |
| 79 | NCR SST S4         |
| 80 | NCR SST S4I        |
| 81 | AIX                |
| 82 | AIX 3.2            |
| 83 | AIX 4.1            |
| 84 | AIX 4.2            |
| 85 | AIX 4.3            |
| 86 | AIX 5.0            |
| 87 | AIX 5.1            |
| 88 | AIX 5.2            |
| 89 | Unixware           |
| 90 | Unixware 2.0       |
| 91 | Unixware 2.1       |
| 92 | Unixware 7.x       |
| 93 | SCO OpenServer 3.2 |
| 94 | SCO OpenServer 5.2 |
| 95 | Sinix              |
| 96 | Sinix 5.42         |

|     |                |
|-----|----------------|
| 97  | Sinix 5.43     |
| 98  | Sinix 5.44     |
| 99  | Sinix 5.45     |
| 100 | Irix           |
| 101 | Irix 6.2       |
| 102 | Irix 6.3       |
| 103 | Irix 6.4       |
| 104 | Irix 6.5       |
| 105 | Dynix          |
| 106 | Dynix 4.2.x    |
| 107 | Dynix 4.4.x    |
| 108 | Solaris        |
| 109 | Solaris 2.3    |
| 110 | Solaris 2.4    |
| 111 | Solaris 2.5    |
| 112 | Solaris 2.6    |
| 113 | Solaris 7      |
| 114 | Solaris 8      |
| 115 | Solaris 9      |
| 116 | SunOS 4.1.4    |
| 117 | OS/2           |
| 118 | AS400          |
| 119 | OS390          |
| 120 | DOS            |
| 121 | Macintosh      |
| 122 | Macintosh 10.0 |
| 123 | Macintosh 10.1 |
| 124 | Macintosh 10.2 |
| 125 | Macintosh 10.3 |



|     |                                                        |
|-----|--------------------------------------------------------|
| 126 | Macintosh 10.4                                         |
| 127 | Netware                                                |
| 128 | OpenVMS                                                |
| 129 | OpenVMS 5.5                                            |
| 130 | OpenVMS 6.0                                            |
| 131 | OpenVMS 6.1                                            |
| 132 | OpenVMS 6.2                                            |
| 133 | OpenVMS 7.0                                            |
| 134 | OpenVMS 7.1                                            |
| 135 | OpenVMS 7.2                                            |
| 136 | Windows NT Server 3.51                                 |
| 137 | Windows XP Embedded                                    |
| 138 | Windows Server 2003 Standard Edition                   |
| 139 | Windows Small Business Server 2003                     |
| 140 | Windows Server 2003 Enterprise x64 Edition             |
| 141 | Windows Server 2003 Enterprise 64 ビット版 Itanium Edition |
| 201 | Caldera/SCO Linux                                      |
| 202 | Caldera Linux 3.0                                      |
| 203 | Caldera Linux 3.1                                      |
| 204 | SCO Linux 4.0                                          |
| 205 | Connectiva                                             |
| 206 | Connectiva Linux 8                                     |
| 207 | Connectiva Linux 9                                     |
| 208 | Connectiva Linux 10                                    |
| 209 | Debian GNU/Linux                                       |
| 210 | Debian GNU/Linux 2.0                                   |
| 211 | Debian GNU/Linux 2.1                                   |
| 212 | Debian GNU/Linux 2.2                                   |
| 213 | Debian GNU/Linux 3.0                                   |

|     |                                 |
|-----|---------------------------------|
| 214 | Fedora                          |
| 215 | Fedora Core 1                   |
| 216 | Fedora Core 2                   |
| 217 | Miracle Linux                   |
| 218 | Miracle Linux 2.1               |
| 219 | Miracle Linux 3.0               |
| 220 | Red Flag Linux                  |
| 221 | Red Flag Linux 3.0              |
| 222 | Red Flag Linux 3.2              |
| 223 | Red Flag Linux 4.0              |
| 224 | Red Flag Linux 4.1              |
| 225 | RedHat Linux                    |
| 226 | Red Hat Linux 7.0               |
| 227 | Red Hat Linux 7.1               |
| 228 | Red Hat Linux 7.2               |
| 229 | Red Hat Linux 7.3               |
| 230 | Red Hat Linux 8.0               |
| 231 | Red Hat Enterprise Linux ES 2.1 |
| 232 | Red Hat Enterprise Linux AS 2.1 |
| 233 | Red Hat Enterprise Linux WS 2.1 |
| 234 | Red Hat Enterprise Linux ES 3   |
| 235 | Red Hat Enterprise Linux AS 3   |
| 236 | Red Hat Enterprise Linux WS 3   |
| 237 | Red Hat Enterprise Linux ES 4.0 |
| 238 | Red Hat Enterprise Linux AS 4.0 |
| 239 | Red Hat Enterprise Linux WS 4.0 |
| 240 | Red Hat Desktop                 |
| 241 | Sun Java Desktop System         |
| 242 | Sun Java Desktop System 2003    |

|     |                                |
|-----|--------------------------------|
| 243 | Sun Java Desktop System 2      |
| 244 | SuSE Linux                     |
| 245 | SuSE Linux 7.0                 |
| 246 | SuSE Linux 7.1                 |
| 247 | SuSE Linux 7.3                 |
| 248 | SuSE Linux 8.0                 |
| 249 | SuSE Linux 8.1                 |
| 250 | SuSE Linux 8.2                 |
| 251 | SuSE Linux Professional 9      |
| 252 | SuSE Linux Professional 9.1    |
| 253 | SuSE Linux Personal 9          |
| 254 | SuSE Linux Personal 9.1        |
| 255 | SuSE Linux Enterprise Server 7 |
| 256 | SuSE Linux Enterprise Server 8 |
| 257 | SuSE Linux Enterprise Server 9 |
| 258 | SuSE Standard Server 8         |
| 259 | SuSE Desktop 1                 |
| 260 | SuSE Desktop 2                 |
| 261 | Turbo Linux                    |
| 262 | TurboLinux Server 8            |
| 263 | TurboLinux Workstation 8       |
| 264 | TurboLinux Enterprise 8        |
| 265 | TurboLinux 10                  |
| 266 | Xandros Desktop OS             |
| 267 | Xandros Desktop 1.0            |
| 268 | Xandros Desktop 1.1            |
| 269 | Xandros Desktop 2.0            |
| 270 | OpenVMS 7.3                    |
| 271 | Unixware 7.1.4                 |

|     |                            |
|-----|----------------------------|
| 272 | SCO OpenServer             |
| 273 | SCO OpenServer 5.7         |
| 274 | SCO Unix                   |
| 275 | Nokia AdminSuite           |
| 276 | Nokia AdminSuite 1.0       |
| 277 | OpenVMS 8.0                |
| 278 | OpenVMS 8.2                |
| 279 | Solaris 10                 |
| 280 | AIX 5.3                    |
| 281 | NCR MP-RAS 3.02            |
| 282 | HPUX 11.10                 |
| 283 | HPUX 11.22                 |
| 284 | HPUX 11.23                 |
| 285 | HPUX 11.00                 |
| 286 | HP Tru64 5.1               |
| 287 | HP Tru64 5.0               |
| 288 | HP Tru64 4.0F              |
| 289 | HP Tru64 4.0G              |
| 290 | HPUX 10.00                 |
| 291 | HPUX 10.10                 |
| 292 | HPUX 10.20                 |
| 293 | HPUX 10.30                 |
| 294 | HPUX 11.20                 |
| 296 | AIX 5                      |
| 297 | Windows Vista              |
| 298 | Windows Vista Business     |
| 299 | Windows Vista Enterprise   |
| 300 | Windows Vista Home Premium |
| 301 | Windows Vista Home Basic   |

|      |                                        |
|------|----------------------------------------|
| 302  | Windows Vista Ultimate                 |
| 303  | Windows Vista Business x64 Edition     |
| 304  | Windows Vista Enterprise x64 Edition   |
| 305  | Windows Vista Home Premium x64 Edition |
| 306  | Windows Vista Home Basic x64 Edition   |
| 307  | Windows Vista Ultimate x64 Edition     |
| 308  | Windows Mobile                         |
| 309  | Windows Mobile 5.0                     |
| 2001 | _3COM                                  |
| 2002 | Acer                                   |
| 2003 | Adaptec                                |
| 2004 | Alcatel                                |
| 2005 | Altos                                  |
| 2006 | Apple                                  |
| 2007 | Asante                                 |
| 2008 | ATT                                    |
| 2009 | Avaya                                  |
| 2010 | Banyan                                 |
| 2011 | Bay                                    |
| 2012 | Belkin                                 |
| 2013 | Breeze                                 |
| 2014 | Brocade                                |
| 2015 | Cabletron                              |
| 2016 | Chaparral                              |
| 2017 | Ciprico                                |
| 2018 | Crossroads                             |
| 2019 | Chipcom                                |
| 2020 | Cisco                                  |
| 2021 | Compaq                                 |

|      |            |
|------|------------|
| 2022 | DEC        |
| 2023 | Dell       |
| 2024 | Digital    |
| 2025 | EMC        |
| 2026 | Emulex     |
| 2027 | Epson      |
| 2028 | Ericcson   |
| 2029 | EthAirNet  |
| 2030 | Exabyte    |
| 2031 | Extreme    |
| 2032 | Fore       |
| 2033 | Foundry    |
| 2034 | Fujitsu    |
| 2035 | Gadzoox    |
| 2036 | Gateway    |
| 2037 | Gator      |
| 2038 | Hitachi    |
| 2039 | ICL        |
| 2040 | Intel      |
| 2041 | Intergraph |
| 2042 | IPX        |
| 2043 | HP         |
| 2044 | IBM        |
| 2045 | JNI        |
| 2046 | KarlNet    |
| 2047 | LSILogic   |
| 2048 | Linksys    |
| 2049 | McDATA     |
| 2050 | Micom      |

|      |                  |
|------|------------------|
| 2051 | Motorola         |
| 2052 | MultiNet         |
| 2053 | NBase            |
| 2054 | NCD              |
| 2055 | NCR              |
| 2056 | NEC              |
| 2057 | NetApps          |
| 2058 | NetBotz          |
| 2059 | NetGear          |
| 2060 | NetJet           |
| 2061 | NetQue           |
| 2062 | NetWorth         |
| 2063 | Nokia            |
| 2064 | Nortel           |
| 2065 | Novell           |
| 2066 | Orinoco          |
| 2067 | Palm             |
| 2068 | Pathlight        |
| 2069 | Qlogic           |
| 2070 | RoamAbout        |
| 2071 | SCO              |
| 2072 | Samsung          |
| 2073 | Siemens          |
| 2074 | Silicon Graphics |
| 2075 | SMC              |
| 2076 | StorageTek       |
| 2077 | Sun              |
| 2078 | Symbol           |
| 2079 | SynOptics        |

|      |                      |
|------|----------------------|
| 2080 | Tandberg             |
| 2081 | Tandem               |
| 2082 | Tektronix            |
| 2083 | Telebit              |
| 2084 | Toshiba              |
| 2085 | Troika               |
| 2086 | Unisys               |
| 2087 | Vitalink             |
| 2088 | Vixel                |
| 2089 | Xerox                |
| 2090 | Xiotech              |
| 2091 | Xircom               |
| 2092 | Xylan                |
| 2093 | Xylogics             |
| 2094 | Xyplex               |
| 2095 | Wellfleet            |
| 2096 | Brocade 2400         |
| 2097 | Brocade 3200         |
| 2098 | Brocade 3500         |
| 2099 | Brocade 12000        |
| 2100 | Dell Axim            |
| 2101 | Dell Latitude        |
| 2102 | Dell Optiplex        |
| 2103 | EMC Clariion         |
| 2104 | EMC Symmetrix        |
| 2105 | Siemens optiPoint    |
| 2106 | Dell Optiplex GL110  |
| 2107 | Dell Optiplex GLX270 |
| 2108 | Bay Bridge           |



|      |                     |
|------|---------------------|
| 2109 | Bay Hub             |
| 2110 | Bay Switch          |
| 2111 | HP Printer          |
| 2112 | HP スイッチ             |
| 2113 | HP Bridge           |
| 2114 | HP Computer         |
| 2115 | HP サーバ              |
| 2116 | _3COM Switch        |
| 2117 | HP PC               |
| 2118 | Brocade Switch      |
| 2119 | Alcatel IP Phone    |
| 2120 | Dell Switch         |
| 2121 | Cisco Router        |
| 2122 | Cisco Switch        |
| 2123 | Enterasys           |
| 2124 | Enterasys Router    |
| 2125 | Enterasys Switch    |
| 2126 | IBM Router          |
| 2127 | IBM スイッチ            |
| 2128 | IBM MSS             |
| 2129 | IBM 8265            |
| 2130 | IBM 8271            |
| 2131 | IBM 8371            |
| 2132 | Foundry Switch      |
| 2133 | Dell Computer       |
| 2134 | Cisco Fabric Switch |
| 2135 | Adaptec HBA         |
| 2136 | AMCC                |
| 2137 | AMCC HBA            |

|      |                        |
|------|------------------------|
| 2138 | Chaparral Bridge       |
| 2139 | CNT                    |
| 2140 | CNT スイッチ               |
| 2141 | Crossroads Bridge      |
| 2142 | Emulex HBA             |
| 2143 | Emulex Hub             |
| 2144 | Gadzoox Switch         |
| 2145 | Gadzoox Hub            |
| 2146 | HP HBA                 |
| 2147 | IBM HBA                |
| 2148 | LSILogic HBA           |
| 2149 | McDATA Director        |
| 2150 | McDATA スイッチ            |
| 2151 | McDATA EFC Manager     |
| 2152 | Pathlight Bridge       |
| 2153 | Qlogic HBA             |
| 2154 | Qlogic Switch          |
| 2155 | Vixel Switch           |
| 2156 | Vixel Hub              |
| 2157 | Cisco Access Point     |
| 2158 | Intel Access Point     |
| 2159 | Symbol Access Point    |
| 2160 | Compaq Access Point    |
| 2161 | Belkin Access Point    |
| 2162 | NetGear Access Point   |
| 2163 | Linksys Access Point   |
| 2164 | RoamAbout Access Point |
| 2165 | KarlNet Access Point   |
| 2166 | SMC Access Point       |

|      |                        |
|------|------------------------|
| 2167 | Orinoco Access Point   |
| 2168 | BreezeCOM Access Point |
| 2169 | EthAirNet Access Point |
| 2170 | Avaya Access Point     |
| 2171 | Ericcson Access Point  |
| 2172 | _3COM Access Point     |
| 2173 | Nortel Access Point    |
| 2174 | Ascend                 |
| 2175 | Kyocera                |
| 2176 | Lexmark                |
| 2177 | Sato                   |
| 2178 | Ascend Router          |
| 2179 | Epson Printer          |
| 2180 | Kyocera Printer        |
| 2181 | Lexmark Printer        |
| 2182 | Sato Printer           |
| 3001 | コンピュータ                 |
| 3002 | ネットワーキング デバイス          |
| 3003 | プリンタ                   |
| 3004 | ストレージデバイス              |
| 3005 | テレコム デバイス              |
| 3006 | デスクトップ                 |
| 3007 | ラップトップ                 |
| 3008 | メインフレーム                |
| 3009 | ミニコンピュータ               |
| 3010 | サーバ                    |
| 3011 | Bridge (ブリッジ)          |
| 3012 | Hub (ハブ)               |
| 3013 | ネットワーク アダプタ            |

|      |                     |
|------|---------------------|
| 3014 | モデム                 |
| 3015 | Router (ルータ)        |
| 3016 | Switch (スイッチ)       |
| 3017 | バブル ジェット プリンタ       |
| 3018 | ドット マトリックス プリンタ     |
| 3019 | レーザ プリンタ            |
| 3020 | ライン プリンタ            |
| 3021 | マイクロフィッシュ           |
| 3022 | プロッタ                |
| 3023 | テープ サブシステム          |
| 3024 | ディスク サブシステム         |
| 3025 | 電話                  |
| 3026 | Telco Hub           |
| 3027 | Telco Circuit       |
| 3028 | Telco Router        |
| 3029 | ネットワーク インターフェース カード |
| 3030 | ホスト バス アダプタ         |
| 3031 | iSCSI アダプタ          |
| 3032 | ワイヤレス ネットワーク カード    |
| 3033 | SAN スイッチ            |
| 3034 | イーサネット スイッチ         |
| 3035 | インクジェット             |
| 3036 | テープ ドライブ            |
| 3037 | テープ エンクロージャ         |
| 3038 | ディスク ドライブ           |
| 3039 | ディスク エンクロージャ        |
| 3040 | IP 電話               |
| 3041 | 光ディスク サブシステム        |

|      |                               |
|------|-------------------------------|
| 3042 | WORM エンクロージャ                  |
| 3044 | テープ                           |
| 3045 | テープ サブシステム コンポーネント            |
| 3046 | ディスク サブシステム コンポーネント           |
| 3047 | 光ディスク サブシステム コンポーネント          |
| 3048 | ロボット アーム                      |
| 3049 | 光ディスク                         |
| 3050 | CD-ROM ドライブ                   |
| 3051 | DVD ドライブ                      |
| 4001 | 仮想マシン                         |
| 4002 | 仮想ノード                         |
| 4003 | VMware セッション                  |
| 4004 | MS Virtual Server             |
| 4005 | クラスタ ノード                      |
| 4006 | 論理パーティション                     |
| 4007 | HP ハードパーティション                 |
| 5001 | x86                           |
| 5002 | Itanium (64 ビット)              |
| 5003 | Windows サーバ                   |
| 5004 | Windows ワークステーション             |
| 5005 | モバイル                          |
| 5006 | Windows Server 64 ビット         |
| 5007 | Windows NT Server 3.x         |
| 5008 | Windows NT Server 4.0 以降      |
| 5009 | Windows 9x エディション             |
| 5010 | Windows NT Workstation 4.0 以降 |
| 5011 | Windows CE 以降                 |
| 5013 | Windows Server 2003 64 ビット以降  |

|      |                                   |
|------|-----------------------------------|
| 5014 | Windows NT Server 4.0 エディション      |
| 5015 | Windows 2000 Server 以降            |
| 5016 | Windows NT Workstation 4.0 エディション |
| 5017 | Windows 2000 Workstation 以降       |
| 5018 | Windows CE 2x                     |
| 5019 | Windows CE 3x                     |
| 5020 | Windows Server 2003 64 ビット        |
| 5021 | Windows 2000 Server エディション        |
| 5022 | Windows Server 2003 以降            |
| 5023 | Windows 2000 Workstation エディション   |
| 5024 | Windows XP 以降                     |
| 5025 | Windows Server 2003 エディション        |
| 5026 | Windows Server 2003 (x64)         |
| 5027 | Windows XP エディション                 |
| 5028 | Windows XP (64 ビット)               |
| 5029 | Macintosh 10.x 以上                 |
| 5030 | HP Tru64 DEC                      |
| 5031 | HP Tru64 4.0x 以降                  |
| 5032 | HP Tru64 4.0x                     |
| 5033 | HP Tru64 5.0 以降                   |
| 5034 | HP Tru64 5.0x                     |
| 5035 | HP Tru64 5.1 以降                   |
| 5036 | HP Tru64 5.1x                     |
| 5037 | HPUX 10.x 以降                      |
| 5038 | HPUX 10.x                         |
| 5039 | HPUX 11.x 以降                      |
| 5040 | HPUX 11.x                         |
| 5042 | AIX 5.x 以降                        |

|      |                                   |
|------|-----------------------------------|
| 5043 | AIX 5.x                           |
| 5044 | NCR SST S4 以降                     |
| 5045 | NCR SST S4x                       |
| 5046 | NCR MP-RAS 3.x 以降                 |
| 5047 | NCR MP-RAS 3.x                    |
| 5048 | Netware 5.1 SP1                   |
| 5049 | Netware 6.5 SP3                   |
| 5050 | Netware 5.1 SP3                   |
| 5051 | Netware 6.5                       |
| 5052 | Netware 5.1                       |
| 5053 | Netware 5.1 SP7                   |
| 5054 | Netware 5.1 SP6                   |
| 5055 | Netware 6.5 SP1.1                 |
| 5056 | Netware 6.5 SP2                   |
| 5057 | Netware 5.1 SP2                   |
| 5058 | Netware 5.1 SP4                   |
| 5059 | Netware 5.1 SP8                   |
| 5060 | Netware 5.1 SP5                   |
| 5061 | Red Hat Linux 9.0                 |
| 5062 | ONS                               |
| 5063 | IOS                               |
| 5064 | OSF/1                             |
| 5065 | Netware 6.5 SP4                   |
| 5066 | Netware 6.5 SP5                   |
| 5067 | z/OS                              |
| 5068 | Windows Vista エディション              |
| 5069 | Windows Vista (64 ビット)            |
| 5082 | SuSE Linux Enterprise Server 10   |
| 5083 | SuSE Linux Enterprise Server 10.1 |

|      |                                                 |
|------|-------------------------------------------------|
| 5084 | SuSE Linux Enterprise Desktop 10                |
| 5085 | SuSE Linux Enterprise Desktop 10.1              |
| 5088 | Windows Server 2003 Standard x64 Edition        |
| 5089 | Windows Server 2003 Datacenter x64 Edition      |
| 5090 | Unixware 7.1.3                                  |
| 5091 | Macintosh 10.5                                  |
| 5092 | Red Hat Enterprise Linux Server 5               |
| 5093 | Red Hat Enterprise Linux Desktop 5              |
| 5094 | Red Hat Enterprise Linux 5 Advanced Platform    |
| 5095 | Solaris ドメイン パーティション                            |
| 5096 | Sun サーバ                                         |
| 5097 | Sun Fire E25K                                   |
| 5098 | Sun Fire E20K                                   |
| 5099 | Sun Fire 15K                                    |
| 5100 | Sun Fire 12K                                    |
| 5101 | Sun Enterprise 10000                            |
| 5102 | Sun Enterprise 6500                             |
| 5103 | Sun Enterprise 5500                             |
| 5104 | Sun Enterprise 4500                             |
| 5105 | Sun Enterprise 3500                             |
| 5106 | Windows Embedded POS                            |
| 5107 | Windows Embedded for Point of Service Version 1 |
| 5108 | Windows Embedded                                |
| 5109 | Windows Embedded for Point of Service           |
| 5110 | Windows Embedded for Point of Service 1.0       |
| 5111 | HPUX 11.11                                      |
| 5112 | HPUX 11.31                                      |
| 5114 | RTOS                                            |
| 5115 | Sun RTOS                                        |



|      |                                                |
|------|------------------------------------------------|
| 5116 | Red Hat Enterprise Linux Server 5.1            |
| 5117 | Red Hat Enterprise Linux Desktop 5.1           |
| 5118 | Red Hat Enterprise Linux 5.1 Advanced Platform |
| 5119 | Windows Server 2008                            |
| 5120 | Windows Server 2008 Standard Edition           |
| 5121 | Windows Server 2008 Standard x64 Edition       |
| 5122 | Windows Server 2008 Enterprise Edition         |
| 5123 | Windows Server 2008 Enterprise x64 Edition     |
| 5124 | Windows Server 2008 Datacenter Edition         |
| 5125 | Windows Server 2008 Datacenter x64 Edition     |
| 5126 | Windows Web Server 2008                        |
| 5127 | Windows Web Server 2008 x64 Edition            |
| 5128 | Windows Storage Server 2008                    |
| 5129 | Windows Storage Server 2008 x64 Edition        |
| 5130 | Windows Small Business Server 2008             |
| 5131 | Windows Essential Business Server 2008         |
| 5132 | Windows Server 2008 IA-64 Edition              |
| 5133 | Windows Server 2008 IA-64 以上                   |
| 5134 | Windows Server 2008 以上                         |
| 5135 | Windows Server 2008 Editions (32 ビット)          |
| 5136 | Windows Server 2008 (x64)                      |
| 5137 | Windows Mobile 6.0                             |
| 5138 | AIX 6                                          |
| 5139 | AIX 6.1                                        |
| 5140 | AIX 6.x 以降                                     |
| 5141 | AIX 6.x                                        |
| 5142 | RIM                                            |
| 5143 | RIM OS                                         |
| 5144 | ハイパーバイザ                                        |

|      |                                                  |
|------|--------------------------------------------------|
| 5145 | Microsoft Hyper-V                                |
| 5146 | VMware ESX                                       |
| 5147 | VMware ESXi                                      |
| 5148 | Windows Server 2008 Hyper-V                      |
| 5149 | VMware ESX Server 3.5                            |
| 5150 | VMWare ESXi 3.5                                  |
| 5153 | 仮想ホスト マシン                                        |
| 5154 | HP Chassis                                       |
| 5155 | IBM Server                                       |
| 5156 | Windows 7                                        |
| 5157 | Windows 7 Enterprise                             |
| 5158 | Windows 7 Enterprise x64 Edition                 |
| 5159 | Windows 7 Home Premium                           |
| 5160 | Windows 7 Home Premium x64 Edition               |
| 5161 | Windows 7 Professional                           |
| 5162 | Windows 7 Professional x64 Edition               |
| 5163 | Windows 7 Starter                                |
| 5164 | Windows 7 Home Basic                             |
| 5165 | Windows 7 Home Basic x64 Edition                 |
| 5166 | Windows 7 Ultimate                               |
| 5167 | Windows 7 Ultimate x64 Edition                   |
| 5168 | Macintosh 10.6                                   |
| 5169 | SUSE Linux Enterprise Server 11                  |
| 5188 | Windows Server 2008 R2                           |
| 5189 | Windows Server 2008 R2 Datacenter x64 Edition    |
| 5190 | Windows Server 2008 R2 Enterprise x64 Edition    |
| 5191 | Windows Server 2008 R2 IA-64 Edition             |
| 5192 | Windows Server 2008 R2 Standard x64 Edition      |
| 5193 | Windows Server 2008 Server Core Standard Edition |

|      |                                                           |
|------|-----------------------------------------------------------|
| 5194 | Windows Server 2008 Server Core Standard x64 Edition      |
| 5195 | Windows Server 2008 R2 Server Core Standard x64 Edition   |
| 5196 | Windows Server 2008 Server Core Enterprise Edition        |
| 5197 | Windows Server 2008 Server Core Enterprise x64 Edition    |
| 5198 | Windows Server 2008 R2 Server Core Enterprise x64 Edition |
| 5199 | Windows Server 2008 Server Core Datacenter Edition        |
| 5200 | Windows Server 2008 Server Core Datacenter x64 Edition    |
| 5201 | Windows Server 2008 R2 Server Core Datacenter x64 Edition |
| 5202 | Windows Web Server 2008 R2 x64 Edition                    |
| 5203 | Windows Web Server 2008 Server Core Edition               |
| 5204 | Windows Web Server 2008 Server Core x64 Edition           |
| 5205 | SuSE Linux Enterprise Desktop 11                          |
| 5206 | Windows Web Server 2008 R2 Server Core x64 Edition        |
| 5210 | Windows Server 2008 Server Core Installation              |
| 5211 | Windows Server 2008 (x64) Server Core Installation        |
| 5212 | Windows Server 2008 R2 以上                                 |
| 5213 | Windows Server 2008 R2 Server Core Installation           |
| 5214 | Windows Vista 以上                                          |
| 5215 | Windows Server 7 以上                                       |
| 5216 | Windows 7 Editions                                        |
| 5217 | Windows Vista (x64) 以上                                    |
| 5218 | Windows 7 (x64) 以上                                        |
| 5219 | Windows 7 (64 ビット)                                        |
| 5220 | openSUSE                                                  |
| 5221 | openSUSE 11.0                                             |
| 5222 | openSUSE 11.1                                             |
| 5223 | Sun eXtended System Control Facility (XSCF)               |
| 5224 | Windows Mobile 6.1                                        |
| 5226 | VMWare ESX Server 4.0                                     |

|      |                                                    |
|------|----------------------------------------------------|
| 5229 | Windows Embedded POSReady 2009                     |
| 5230 | Windows Storage Server 2008 Standard Edition       |
| 5231 | Windows Storage Server 2008 Basic Edition          |
| 5232 | Windows Storage Server 2008 Enterprise Edition     |
| 5233 | Windows Storage Server 2008 Workgroup Edition      |
| 5234 | Windows Storage Server 2008 Standard X64 Edition   |
| 5235 | Windows Storage Server 2008 Basic X64 Edition      |
| 5236 | Windows Storage Server 2008 Enterprise X64 Edition |
| 5237 | Windows Storage Server 2008 Workgroup X64 Edition  |
| 5238 | VMWare ESX Server 4.1                              |
| 5239 | Windows Mobile 6.5                                 |
| 5240 | VMware ESXi 4.0                                    |
| 5241 | VMware ESXi 4.1                                    |
| 5242 | Citrix XenServer                                   |
| 5243 | Citrix XenServer 4.0                               |
| 5244 | Citrix XenServer 4.1                               |
| 5245 | Citrix XenServer 5.0                               |
| 5246 | Citrix XenServer 5.5                               |
| 5247 | Citrix XenServer 5.6                               |
| 5248 | Windows Server 2008 R2 Hyper-V                     |
| 5249 | Hyper-V Server 2008                                |
| 5250 | Hyper-V Server 2008 R2                             |
| 5251 | Red Hat Enterprise Linux 5.4 Advanced Platform     |
| 5252 | Red Hat Enterprise Linux Desktop 5.4               |
| 5253 | Red Hat Enterprise Linux Server 5.4                |
| 5254 | Windows Embedded Standard 7 Edition                |
| 5255 | Windows Embedded Standard 7 X64 Edition            |
| 5256 | AIX 7                                              |
| 5257 | AIX 7.1                                            |

|      |                                            |
|------|--------------------------------------------|
| 5258 | Red Hat Enterprise Linux Server 6.0 x86    |
| 5259 | Red Hat Enterprise Linux Server 6.0 x86_64 |
| 5260 | Debian GNU/Linux 5.0                       |
| 5261 | Debian GNU/Linux 6.0                       |
| 5262 | Debian GNU/Linux 7.0                       |
| 5263 | Ubuntu Linux                               |
| 5264 | Ubuntu Linux 10.04                         |
| 5265 | Ubuntu Linux 10.10                         |
| 5266 | Ubuntu Linux 11.04                         |
| 5267 | Ubuntu Linux 11.10                         |
| 5268 | Ubuntu Linux 12.04                         |
| 5269 | Macintosh 10.7                             |
| 5270 | Red Hat Enterprise Linux Server 6.1 x86    |
| 5271 | Red Hat Enterprise Linux Server 6.1 x86_64 |
| 5272 | openSUSE 11.2 x86                          |
| 5273 | openSUSE 11.2 x86_64                       |
| 5274 | openSUSE 11.3 x86                          |
| 5275 | openSUSE 11.3 x86_64                       |
| 5276 | openSUSE 11.4 x86                          |
| 5277 | openSUSE 11.4 x86_64                       |
| 5278 | Red Hat Enterprise Linux Server 6.2 x86    |
| 5279 | Red Hat Enterprise Linux Server 6.2 x86_64 |
| 5280 | Debian GNU/Linux 1.1                       |
| 5281 | Debian GNU/Linux 1.2                       |
| 5282 | Debian GNU/Linux 1.3                       |
| 5283 | Debian GNU/Linux 3.1                       |
| 5284 | Debian GNU/Linux 4.0                       |
| 5285 | Ubuntu Linux 4.10                          |
| 5286 | Ubuntu Linux 5.04                          |

|      |                                                       |
|------|-------------------------------------------------------|
| 5287 | Ubuntu Linux 5.10                                     |
| 5288 | Ubuntu Linux 6.06                                     |
| 5289 | Ubuntu Linux 6.10                                     |
| 5290 | Ubuntu Linux 7.04                                     |
| 5291 | Ubuntu Linux 7.10                                     |
| 5292 | Ubuntu Linux 8.04                                     |
| 5293 | Ubuntu Linux 8.10                                     |
| 5294 | Ubuntu Linux 9.04                                     |
| 5295 | Ubuntu Linux 9.10                                     |
| 5296 | Windows CE 6.00                                       |
| 5297 | Windows CE 5.00                                       |
| 5298 | Windows CE .NET 4.0                                   |
| 5299 | Windows CE .NET 4.1                                   |
| 5300 | Windows CE .NET 4.2                                   |
| 5301 | Oracle Linux                                          |
| 5302 | Oracle Enterprise Linux Server 5 x86                  |
| 5303 | Oracle Enterprise Linux Server 5 x86_64               |
| 5304 | Oracle Linux Server 6 x86                             |
| 5305 | Oracle Linux Server 6 x86_64                          |
| 5307 | Windows Storage Server 2008 R2                        |
| 5308 | Windows Storage Server 2008 R2 Essentials x64 Edition |
| 5309 | Red Hat Enterprise Linux Server 6.3 x86               |
| 5310 | Red Hat Enterprise Linux Server 6.3 x86_64            |
| 5311 | Windows Embedded POSReady 7                           |
| 5312 | Windows 8                                             |
| 5313 | Windows 8 Pro x86                                     |
| 5314 | Windows 8 Pro x64                                     |
| 5315 | Windows 8 Enterprise x86                              |
| 5316 | Windows 8 Enterprise x64                              |

|      |                                                |
|------|------------------------------------------------|
| 5317 | Windows Embedded standard 8 x86                |
| 5318 | Windows Embedded standard 8 x64                |
| 5319 | Windows 8 x86                                  |
| 5320 | Windows 8 x64                                  |
| 5321 | Windows Server 2012                            |
| 5322 | Windows Server 2012 Foundation x64             |
| 5323 | Windows Server 2012 Essentials x64             |
| 5324 | Windows Server 2012 Standard x64               |
| 5325 | Windows Server 2012 Datacenter x64             |
| 5326 | Windows 8 以降                                   |
| 5327 | Windows 8 のエディション                              |
| 5328 | Windows 8 (x64) 以降                             |
| 5329 | Windows 8 (64 ビット)                             |
| 5330 | Windows Server 2012 以降                         |
| 5331 | Windows Storage Server 2012                    |
| 5332 | Windows Storage Server 2012 Workgroup x64      |
| 5333 | Windows Storage Server 2012 Standard x64       |
| 5334 | Solaris 11                                     |
| 5335 | AIX 7.x 以降                                     |
| 5336 | AIX 7.x                                        |
| 5337 | Macintosh 10.8                                 |
| 5338 | VMware ESXi 5.1                                |
| 5339 | Red Hat Enterprise Linux 5.5 Advanced Platform |
| 5340 | Red Hat Enterprise Linux 5.6 Advanced Platform |
| 5341 | Red Hat Enterprise Linux 5.7 Advanced Platform |
| 5342 | Red Hat Enterprise Linux 5.8 Advanced Platform |
| 5343 | Red Hat Enterprise Linux 5.9 Advanced Platform |
| 5344 | Red Hat Enterprise Linux Desktop 5.5           |
| 5345 | Red Hat Enterprise Linux Desktop 5.6           |

|      |                                            |
|------|--------------------------------------------|
| 5346 | Red Hat Enterprise Linux Desktop 5.7       |
| 5347 | Red Hat Enterprise Linux Desktop 5.8       |
| 5348 | Red Hat Enterprise Linux Desktop 5.9       |
| 5349 | Red Hat Enterprise Linux Server 5.5        |
| 5350 | Red Hat Enterprise Linux Server 5.6        |
| 5351 | Red Hat Enterprise Linux Server 5.7        |
| 5352 | Red Hat Enterprise Linux Server 5.8        |
| 5353 | Red Hat Enterprise Linux Server 5.9        |
| 5354 | Red Hat Enterprise Linux Server 6.4 x86    |
| 5355 | Red Hat Enterprise Linux Server 6.4 x86_64 |
| 5356 | Hyper-V Server 2012                        |
| 5357 | Windows Server 2012 Hyper-V                |
| 5358 | Android                                    |
| 5359 | Android 2.2                                |
| 5360 | Android 2.3                                |
| 5361 | Android 3.0                                |
| 5362 | Android 4.0                                |
| 5363 | iOS 6.1.1                                  |
| 5364 | iOS 6.1.3                                  |
| 5365 | iOS 6.1                                    |
| 5366 | iOS 6.0.1                                  |
| 5367 | iOS 6.0.2                                  |
| 5368 | iOS 5.1                                    |
| 5369 | iOS 5                                      |
| 5370 | BlackBerry OS                              |
| 5371 | BlackBerry OS 7.0                          |
| 5372 | BlackBerry OS 6.0                          |
| 5373 | BlackBerry OS 5.0                          |
| 5374 | Windows Phone                              |



|      |                                       |
|------|---------------------------------------|
| 5375 | Windows Phone 8.0                     |
| 5376 | Android 4.1                           |
| 5377 | Android 4.2                           |
| 5378 | BlackBerry 10.0                       |
| 5379 | BlackBerry 10.1                       |
| 5380 | iOS 6.0                               |
| 5381 | iOS 6.1.2                             |
| 5382 | iOS 6.1.4                             |
| 5383 | Macintosh 10.9                        |
| 5384 | Windows 8.1                           |
| 5385 | Windows 8.1 Enterprise x64            |
| 5386 | Windows 8.1 Enterprise x86            |
| 5387 | Windows 8.1 Pro x64                   |
| 5388 | Windows 8.1 Pro x86                   |
| 5389 | Windows 8.1 x64                       |
| 5390 | Windows 8.1 x86                       |
| 5391 | Windows Embedded 8.1 Standard x64     |
| 5392 | Windows Embedded 8.1 Standard x86     |
| 5393 | Windows Server 2012 R2                |
| 5394 | Windows Server 2012 R2 Datacenter x64 |
| 5395 | Windows Server 2012 R2 Essentials x64 |
| 5396 | Windows Server 2012 R2 Standard x64   |
| 5397 | openSUSE 12.1 x86                     |
| 5398 | openSUSE 12.1 x86_64                  |
| 5399 | openSUSE 12.2 x86                     |
| 5400 | openSUSE 12.2 x86_64                  |
| 5401 | openSUSE 12.3 x86                     |
| 5402 | openSUSE 12.3 x86_64                  |
| 5403 | Citrix XenServer 6.0                  |

|      |                                                   |
|------|---------------------------------------------------|
| 5404 | Citrix XenServer 6.1                              |
| 5405 | Windows Server 2012 R2 Foundation x64             |
| 5406 | Windows Server 2012 Server Core Datacenter x64    |
| 5407 | Windows Server 2012 Server Core Standard x64      |
| 5408 | Windows Server 2012 R2 Server Core Datacenter x64 |
| 5409 | Windows Server 2012 R2 Server Core Standard x64   |
| 5410 | Hyper-V Server 2012 R2                            |
| 5411 | Windows Server 2012 R2 Hyper-V                    |
| 5412 | Windows Storage Server 2012 R2                    |
| 5413 | Windows Storage Server 2012 R2 Standard x64       |
| 5414 | Windows Storage Server 2012 R2 Workgroup x64      |
| 5415 | Windows Server 2012 R2 以降                         |
| 5416 | Windows Server 2012 R2 Server Core Installation   |
| 5417 | Windows Storage Server 2012 R2 以降                 |
| 5418 | Windows 8.1 以降                                    |
| 5419 | Windows 8.1 のエディション                               |
| 5420 | Windows 8.1 (x64) 以降                              |
| 5421 | Windows 8.1 (64 ビット)                              |
| 5422 | Windows Server 2012 Server Core Installation      |
| 5423 | Red Hat Enterprise Linux Server 6.5 x86           |
| 5424 | Red Hat Enterprise Linux Server 6.5 x86_64        |
| 5425 | openSUSE 13.1 x86                                 |
| 5426 | openSUSE 13.1 x86_64                              |
| 5427 | VMware ESXi 5.5                                   |
| 5428 | Red Hat Enterprise Linux Server 7.0 x86_64        |
| 5429 | Windows Embedded POSReady 7 x64                   |
| 5430 | Oracle Linux Server 7 x86_64                      |
| 5431 | Android 4.3                                       |
| 5432 | Android 4.4                                       |

|      |                                             |
|------|---------------------------------------------|
| 5433 | iOS 5.0.1                                   |
| 5434 | iOS 5.1.1                                   |
| 5435 | iOS 6.1.5                                   |
| 5436 | iOS 6.1.6                                   |
| 5437 | iOS 7.0                                     |
| 5438 | iOS 7.0.1                                   |
| 5439 | iOS 7.0.2                                   |
| 5440 | iOS 7.0.3                                   |
| 5441 | iOS 7.0.4                                   |
| 5442 | iOS 7.0.5                                   |
| 5443 | iOS 7.0.6                                   |
| 5444 | iOS 7.1                                     |
| 5445 | iOS 7.1.1                                   |
| 5446 | iOS 7.1.2                                   |
| 5447 | iOS 8.0                                     |
| 5448 | Windows Embedded Compact 7.0                |
| 5449 | Windows Embedded Compact 2013               |
| 5450 | Windows Phone 8.1                           |
| 5451 | Macintosh 10.10                             |
| 5452 | Red Hat Enterprise Linux Server 5.10 x86    |
| 5453 | Red Hat Enterprise Linux Server 5.11 x86    |
| 5456 | Red Hat Enterprise Linux Server 5.10 x86_64 |
| 5457 | Red Hat Enterprise Linux Server 5.11 x86_64 |



# 付録 E: SCAP 設定パラメータ

---

このセクションでは、FDCC インベントリ検出モジュールを設定時に指定する必要がある、SCAP 設定パラメータについて説明します。 [インベントリ モジュールの新規作成] ダイアログ ボックスの [設定] タブに表示されるテキスト フィールドに以下のパラメータを指定できます。

## SCAPPath

エージェント コンピュータ上の SCAP データ ストリーム ディレクトリへのパスを指定します。このパスは、ドメイン マネージャの SCAP データ ストリーム ディレクトリに一致する必要があります。たとえば、IE7 チェックリストの場合、FDCC-Major-Version-1.2.1.0ie7 を指定します。チェックリストがエージェント コンピュータに配布された場合、エージェント コンピュータの `ITCM_installpath¥Agent¥units¥00000001¥UAM¥ SCAP_Content` ディレクトリの下に同様のディレクトリ構造が作成されます。

## XCCDFFile

コンプライアンス ベンチマークを調査する SCAP データ ストリームの XCCDF ファイルの名前を指定します。

注：このファイルは、SCAPPath パラメータに指定された場所に存在する必要があります。

### XCCDFID

XCCDF ファイルのベンチマーク タグに対して与えられた ID を指定します。たとえば、Windows XP チェックリストのベンチマーク ID は、FDCC-Windows-XP です。

### XCCDF バージョン

(オプション) 同じ XCCDFID を持つ複数のバージョンがある場合、使用するチェックリストのバージョンを指定します。

### XCCDFVersionOptions

現在配信可能なチェックリストのバージョンをリスト表示します。DSM エンジン は、このパラメータを使用して [SCAP 設定] ダイアログボックスの [XCCDF バージョン] フィールドにデータを表示します。このパラメータは、DSM エンジンが作成するすべての SCAP インベントリ モジュールで利用可能です。

**重要:** チェックリスト用のインベントリ モジュールを手動で作成している場合、このパラメータを含めないでください。このパラメータを追加または変更すると、環境設定が無効になり、チェックリストのスキャン結果が空になることがあります。

### ProfileOptions

現在配信可能なチェックリストの各バージョンに対して、有効なプロファイルをリスト表示します。DSM エンジン は、このパラメータを使用して [SCAP 設定] ダイアログボックスの [XCCDF プロファイル] フィールドにデータを表示します。このパラメータは、DSM エンジンが作成するすべての SCAP インベントリ モジュールで利用可能です。ただし、チェックリスト用のインベントリ モジュールを作成する場合、[SCAP 設定] ダイアログ ボックスに無効なプロファイル名が表示されるため、このパラメータを含めないでください。

**重要:** チェックリスト用のインベントリ モジュールを手動で作成している場合、このパラメータを含めないでください。このパラメータを追加または変更すると、環境設定が無効になり、チェックリストのスキャン結果が空になることがあります。

### CPEDictionary

(オプション) CPE ディクショナリ ファイルの名前を指定します。SCAP データ ストリームがディクショナリ ファイルを含む場合、このパラメータに対してファイル名を指定します。それ以外の場合、このパラメータは省略できます。

注：このファイルは、SCAPPath パラメータに指定された場所に存在する必要があります。

### InvComponent

スキャナによって作成されたインベントリ ファイルで使用するコンポーネント名を指定します。この値はインベントリ ファイルでトップレベルのグループ名として使用されます。したがって [DSM エクスプローラ] で [SCAP] カテゴリ - [インベントリ] の下にインベントリ コンポーネント名としても表示されます。

### CollectXCCDFResultFile

チェックリスト用の XCCDF 結果ファイルの収集を設定します。このオプションを選択すると、チェックリストをスキャンした後、スキャナを使用して XCCDF 結果ファイルを Asset Management エージェントの作業ディレクトリからドメインマネージャに安全にコピーすることができます。

デフォルト：オフ

### CollectOVALResultFiles

チェックリストの OVAL 結果ファイルの収集を Asset Management エージェントの作業ディレクトリにするか、ドメインマネージャにするかを設定します。

デフォルト：オフ

### XCCDFProfile

XCCDF プロファイルのタイトルをコンプライアンス チェックに適用できるように指定します。このパラメータの値を「空」にしておくと、プロファイルは適用されず、XCCDF ファイル内のすべての設定内容が使用されます。

### OutputPath

OVAL および XCCDF 結果ファイルが置かれるディレクトリを定義します。絶対パスか、Asset Management エージェントの作業ディレクトリの下にある SCAP\_Result\_Files ディレクトリへの相対パスのいずれかを指定できます。このフィールドを「空」にすると、ファイルはデフォルトのパスの下に保存されます。このパスのデフォルトは次のとおりです。エージェントの作業ディレクトリ¥SCAP\_Result\_Files¥データ ストリーム パス。

注：スキャンを実行するユーザアカウントは、このフィールドで指定したディレクトリへの書き込みアクセス権を持つ必要があります。

### OvaldiPath

**Ovaldi** インタープリタを含む、エージェント コンピュータ上のディレクトリを指定します。絶対パスか、エージェントのインストールディレクトリの **bin** ディレクトリへの相対パスのいずれかを指定できます。**Client Automation** の本リリースに同梱された **OVAL** インタープリタは、**ITCM\_installpath¥bin¥ovaldi-CA** ディレクトリ以下にインストールされます。**SCAP** データ ストリームが、このリリースに同梱したもの以外の **OVAL** インタープリタを必要とした場合、**OVAL** インタープリタをすべてのエージェント コンピュータに配布し、このフィールドにそのパスを指定していることを確認します。

デフォルト: **ITCM\_installpath¥ovaldi-CA**

### 組織

(オプション) **XCCDF** 結果ファイルの **<organization>** タグに含めたい組織の名前を指定します。組織名を指定して、[リストに追加] をクリックします。

注： 任意の数の組織を追加し、お好みの順序に移動することができます。値は、最高レベルが最初に表示される階層構造です。

**重要:** チェックリスト用のインベントリ モジュールを手動で作成している場合、このパラメータを含めないでください。このパラメータを追加または変更すると、環境設定が無効になり、チェックリストのスキャン結果が空になることがあります。



# 付録 F: CA Asset Converter for Microsoft SCCM Inventory Mapping

このセクションには、以下のトピックが含まれています。

[Client Automation Asset Management ハードウェア インベントリへの Microsoft SCCM ハードウェア アセット インベントリのマップ \(P. 649\)](#)

[Client Automation Asset Management ソフトウェア インベントリへの Microsoft SCCM ソフトウェア アセット インベントリのマップ \(P. 654\)](#)

## Client Automation Asset Management ハードウェア インベントリへの Microsoft SCCM ハードウェア アセット インベントリのマップ

次の表は、CA Asset Converter for Microsoft® SCCM によって収集されたハードウェア インベントリ データ、および Client Automation Asset Management でマップされた対応するその属性を示しています。

| AM インベントリグループ | AM インベントリの属性      | SCCM インベントリの属性                                       |
|---------------|-------------------|------------------------------------------------------|
| \$System\$    | モデル               | SMS_G_System_COMPUTER_SYSTEM.Model                   |
|               | メモリ合計             | SMS_G_System_X86_PC_MEMORY.TotalPhysicalMemory       |
|               | ベンダ               | SMS_G_System_COMPUTER_SYSTEM.Manufacturer            |
|               | タイプ               | SMS_System_COMPUTER_SYSTEM.SystemRole                |
|               | アセット タグ           | SMS_System_COMPUTER_SYSTEM.SMBIOSAssetTag            |
|               | ドメイン              | SMS_System_COMPUTER_SYSTEM.ResourceDomainORWorkgroup |
|               | 最後にログオンしたユーザ ドメイン | SMS_System_COMPUTER_SYSTEM.LastLogonUserName         |

| AM インベントリ<br>グループ             | AM インベントリの属<br>性  | SCCM インベントリの属性                                                  |
|-------------------------------|-------------------|-----------------------------------------------------------------|
|                               | 最後にログオンした<br>ユーザ名 | SMS_System_COMPUTER_SYSTEM.LastLogonUserNa<br>me                |
|                               | 元の SMS サイト サーバ    | ジョブ エンジンの設定から                                                   |
|                               | シリアル番号            | SMS_G_System_SYSTEM_ENCLOSURE.SerialNumber                      |
| \$System\$ \$System<br>Bios\$ | バージョン             | バージョン SMS_G_System_PC_BIOS.Version                              |
|                               | ベンダ               | SMS_G_System_PC_BIOS.Manufacturer                               |
| \$System\$ \$Processo<br>rs\$ | ベンダ ID            | SMS_G_System_PROCESSOR.Manufacturer                             |
|                               | モデル               | SMS_G_System_PROCESSOR.ProcessorId (に基づ<br>く)                   |
|                               | 速度                | SMS_G_System_PROCESSOR.CurrentClockSpeed                        |
|                               | 最大速度              | SMS_G_System_PROCESSOR.MaxClockSpeed                            |
|                               | ソケットの指定           | SMS_G_System_PROCESSOR.SocketDesignation                        |
| \$Network\$                   | コンピュータ名           | SMS_R_System.Name                                               |
|                               | ドメイン名             | SMS_R_System.ResourceDomainORWorkgroup                          |
|                               | IP アドレス           | SMS_G_System_NETWORK_ADAPTER_CONFIGURATI<br>ON.IPAddress        |
| \$Network\$ \$TCP/IP<br>\$    | IP アドレス           | SMS_G_System_NETWORK_ADAPTER_CONFIGURATI<br>ON.IPAddress        |
|                               | サブネット マスク         | SMS_G_System_NETWORK_ADAPTER_CONFIGURATI<br>ON.IPSubnet         |
|                               | デフォルト ゲートウェ<br>イ  | SMS_G_System_NETWORK_ADAPTER_CONFIGURATI<br>ON.DefaultIPGateway |
|                               | DHCP              | SMS_G_System_NETWORK_ADAPTER_CONFIGURATI<br>ON.DHCPEnabled      |
|                               | DHCP Server       | SMS_G_System_NETWORK_ADAPTER_CONFIGURATI<br>ON.DHCPServer       |

| AM インベントリ<br>グループ                          | AM インベントリの属<br>性 | SCCM インベントリの属性                                            |
|--------------------------------------------|------------------|-----------------------------------------------------------|
| \$System<br>Devices\$ Sound<br>Adapter\$   | モデル              | SMS_G_System_SOUND_DEVICE.Name                            |
|                                            | ベンダ              | SMS_G_System_SOUND_DEVICE.Manufacturer                    |
|                                            | ステータス            | SMS_G_System_SOUND_DEVICE.Status                          |
| \$System<br>Devices\$ Video<br>Adapters\$  | モデル              | SMS_G_System_VIDEO_CONTROLLER.Name                        |
|                                            | ドライバ             | SMS_G_System_VIDEO_CONTROLLER.InstalledDisplayDrivers     |
|                                            | ドライババージョン        | SMS_G_System_VIDEO_CONTROLLER.DriverVersion               |
|                                            | チップ タイプ          | SMS_G_System_VIDEO_CONTROLLER.VideoProcessor              |
|                                            | X 解像度            | SMS_G_System_VIDEO_CONTROLLER.CurrentHorizontalResolution |
|                                            | Y 解像度            | SMS_G_System_VIDEO_CONTROLLER.CurrentVerticalResolution   |
|                                            | リフレッシュ周波数        | SMS_G_System_VIDEO_CONTROLLER.CurrentRefreshRate          |
|                                            | メモリ サイズ          | SMS_G_System_VIDEO_CONTROLLER.AdapterRAM                  |
|                                            |                  |                                                           |
| \$System<br>Devices\$Network<br>Adapters\$ | モデル              | SMS_G_System_NETWORK_ADAPTER.Name                         |
|                                            | ベンダ              | SMS_G_System_NETWORK_ADAPTER.Manufacturer                 |
|                                            | MAC アドレス         | SMS_G_System_NETWORK_ADAPTER.MACAddress                   |
|                                            | 説明               | SMS_G_System_NETWORK_ADAPTER.Description                  |
|                                            | アダプタ タイプ         | SMS_G_System_NETWORK_ADAPTER.AdapterType                  |
| \$System<br>Devices\$ IDE<br>Controllers\$ | モデル              | SMS_G_System_IDE_CONTROLLER.Name                          |
|                                            | ベンダ              | SMS_G_System_IDE_CONTROLLER.Manufacturer                  |

| AM インベントリ<br>グループ                           | AM インベントリの属<br>性  | SCCM インベントリの属性                                     |
|---------------------------------------------|-------------------|----------------------------------------------------|
|                                             | ステータス             | SMS_G_System_IDE_CONTROLLER.Status                 |
| \$System<br>Devices\$ USB<br>Controllers\$  | モデル               | SMS_G_System_USB_CONTROLLER.Name                   |
| \$Operating System\$                        | オペレーティング シス<br>テム | SMS_G_System_OPERATING_SYSTEM.Caption              |
|                                             | サービス パック          | SMS_G_System_OPERATING_SYSTEM.CSDVersion           |
|                                             | バージョン             | SMS_G_System_OPERATING_SYSTEM.Version (に基<br>づく)   |
| \$Operating<br>System\$ Installation\$      | 名前                | SMS_G_System_OPERATING_SYSTEM.Caption              |
|                                             | ベンダ               | SMS_G_System_OPERATING_SYSTEM.Manufacturer         |
|                                             | システム パス           | SMS_G_System_OPERATING_SYSTEM.WindowsDirec<br>tory |
|                                             | インストール日           | SMS_G_System_OPERATING_SYSTEM.InstallDate          |
|                                             | バージョン             | SMS_G_System_OPERATING_SYSTEM.Version (に基<br>づく)   |
|                                             | メジャー バージョン        | SMS_G_System_OPERATING_SYSTEM.Version (に基<br>づく)   |
|                                             | マイナー バージョン        | SMS_G_System_OPERATING_SYSTEM.Version (に基<br>づく)   |
|                                             | ビルド番号             | SMS_G_System_OPERATING_SYSTEM.Version (に基<br>づく)   |
| \$File<br>Systems\$ Local File<br>Systems\$ | 名前                | SMS_G_System_LOGICAL_DISK.Name                     |
|                                             | サイズ               | SMS_G_System_LOGICAL_DISK.Size                     |
|                                             | 使用中               | サイズおよび空き領域からの計算                                    |
|                                             | 空き                | SMS_G_System_LOGICAL_DISK.FreeSpace                |

| AM インベントリ<br>グループ               | AM インベントリの属<br>性 | SCCM インベントリの属性                           |
|---------------------------------|------------------|------------------------------------------|
|                                 | 使用率              | サイズおよび空き領域からの計算                          |
|                                 | タイプ              | SMS_G_System_LOGICAL_DISK.DriveType      |
|                                 | ファイル システム        | SMS_G_System_LOGICAL_DISK.FileSystem     |
|                                 | ボリューム ラベル        | SMS_G_System_LOGICAL_DISK.VolumeName     |
|                                 | マウント ポイント        | SMS_G_System_LOGICAL_DISK.Name           |
| \$Storage\$                     | ディスク領域の合計        | 固定ドライブ (SMS_G_SYSTEM_DISK) のサイズか<br>らの計算 |
| \$Storage\$ \$Fixed<br>Drives\$ | デバイス             | SMS_G_System_DISK.DeviceID               |
|                                 | サイズ              | SMS_G_System_DISK.Size                   |

関連項目：

[CA Asset Converter for Microsoft SCCM](#) (P. 496)

## Client Automation Asset Management ソフトウェア インベ ントリへの Microsoft SCCM ソフトウェア アセット インベ ントリのマップ

次の表は、CA Asset Converter for Microsoft® SCCM によって収集されたソフトウェア  
インベントリ データ、および Client Automation Asset Management でマップされ  
た対応するその属性を示しています。

| AM インベントリ<br>グループ | AM インベントリの属<br>性 | SCCM インベントリの属性                                                                  |
|-------------------|------------------|---------------------------------------------------------------------------------|
|                   |                  | すべてのソフトウェア情報は、WMI クラスの<br>SMS_G_System_ADD_REMOVE_PROGRAMS のインス<br>タンスに基づいています。 |
| 検出されたソフト<br>ウェア   | 名前               | SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName                                    |
|                   | バージョン            | SMS_G_System_ADD_REMOVE_PROGRAMS.Version                                        |
|                   | 発行者              | SMS_G_System_ADD_REMOVE_PROGRAMS.Publisher                                      |

関連項目：

[CA Asset Converter for Microsoft SCCM](#) (P. 496)

# 付録 G: SCAP 標準の実装

---

Client Automation 内の DCS (Device Compliance Scanner) は、FDCC チェックリストへの準拠に関してターゲット コンピュータをスキャンします。この章では、SCAP 標準の実装について説明します。

## SCAP

DCS は、セキュリティ設定共通化手順 (SCAP) を中心に構築されます。SCAP は、ソフトウェアの欠陥、セキュリティ関連の設定問題、および製品名を列挙する、選択されたオープンスタンダードのスイートです。また、このスイートは、システムを測定して脆弱性の存在を判断するとともに、これらの測定結果をランク (スコア) 付けて、検出されたセキュリティの問題に対する影響度を評価するメカニズムを提供します

Client Automation は、SCAP 標準 (XCCDF、CCE、CVE、CPE、CVSS、および OVAL) で利用される XML 形式で記述された SCAP 1.1 データ ストリームのコンプライアンスチェックを実装しています。DCS は、アセット管理インベントリ モジュールとして実装されます。DCS は、すべてのエージェントに配布され、スケジュール時刻にコンプライアンスチェックを実行し、仕様によって必要とされる出力ファイルを作成します。DCS スキャナは、XCCDF および OVAL 評価プロトコルを使用して、どの項目をチェックし、どのようにチェックするかを決定します。また、スキャナは、CPE、CCE、CVSS、および CVE 参照プロトコルを使用して、すべてのルールが正確に、適切にシステムに反映されていることを確認します。DCS スキャナは、検査、レポート作成、およびクエリのその結果を中央管理データベースにレポートします。結果ファイルは、入力 SCAP データ ストリームの各ファイルに生成されます。また、検証用にエージェント コンピュータおよびドメインマネージャ (設定されている場合) に保存されます。

## CVE

共通脆弱性識別子 (CVE) 標準は、公に広く知られた情報セキュリティの脆弱性およびソフトウェアの欠陥に対して標準 ID を提供するリストまたはディクショナリです。Client Automation によって作成されたコンプライアンス チェック結果には、チェックリストの定義自体に CVE ID 参照が含まれていれば、チェックされたすべてのルール出力に関連する CVE ID 参照が含まれます。CVE 情報は、スキャナによって生成されたパッチ結果 XML ファイルに保存され、検査と検証に関するエージェントの作業ディレクトリで使用可能です。

SCAP データ ストリームで、アプリケーション、パッチ、または脆弱性の検出用である OVAL コンテンツには、CVE ID 参照が含まれ、CVE リストの正確なエレメントを識別できます。Windows XP および IE7 用の FDCC チェックリストには、この目的のために設けられている個別の OVAL ファイルが含まれ、また、CVE ID が追加されています。

これらの SCAP データ ストリームを処理する場合は、生成された OVAL 結果ファイルに、各 OVAL 定義の CVE ID 参照も追加されます。また、DSM エクスプローラでターゲットシステムに対して表示されたインベントリ データには、詳細パッチの結果グループが含まれます。ここでパッチまたは脆弱性を検出するための OVAL 定義は、いずれもそれ自体のサブグループを持っています。OVAL 定義が SCAP データ ストリームで定義された CVE 参照を持つ場合は常に、このサブグループには CVE 参照テーブルが含まれます。各 CVE 参照には、CVE URL および NVD URL が含まれています。DSM エクスプローラ を使用すると、これらの URL を直接参照できます。



## CCE

CCE (Common Configuration Enumeration) は、システム設定問題に対して一意の ID を提供します。この ID を使用すると、複数の情報ソースおよびツールにわたっての設定データの相関を迅速に正確に把握できます。たとえば、CCE ID は、設定の評価ツールのチェックと設定のベストプラクティス ドキュメントの記述を関連付けるために使用できます。

CCE ID を参照する SCAP データ ストリームでは、CCE ID は、XCCDF ファイルと OVAL ファイルのどちらにあってもかまいません。XCCDF ファイルでは、CCE 参照は `<ident>` タグの形式を取ります。このタグにはリスト内の各ルールに関連付けられている CCE ID をリストします。CCE ID が XCCDF ファイルに存在する場合、DCS はそれらの参照を各ルール結果に含めます。この情報は、作成された XCCDF 結果ファイルとデータベースに送られるインベントリ データの両方で使用可能です。DSM エクスプローラでは、CCE 参照情報は、[インベントリ] - [SCAP] - <チェックリスト名> - [Rule Results] - <ルール名> - [Idents] 以下に表示されます。

OVAL ファイルは、各 OVAL 定義に関連付けられ、`<reference>` タグに含まれる CCE ID を含むことができます。このような参照が存在する場合、CCE ID は、OVAL 定義が処理されて作成された OVAL 結果ファイルに含められます。

また、CCE 参照と結果は、`<machine>-<checklist>-xccdf-CCE-result.txt` という名前で、結果ファイルのセットで利用可能です。

Client Automation とともにパッケージ化されたすべての FDCC チェックリストには、CCE ID 参照が XCCDF ファイルと OVAL ファイルの両方に含まれます。出力ファイルの名前および場所は、DSM エクスプローラで、[インベントリ] - [SCAP] - <チェックリスト インベントリ コンポーネント> - [Status] グループ以下に表示されます。

## CPE

CPE (Common Platform Enumeration) は、情報テクノロジーシステム、プラットフォーム、およびパッケージの命名スキームです。CPE には、URI (Uniform Resource Identifiers) の一般的な構文に基づいて、フォーマル名フォーマット、複雑なプラットフォームを記述する言語、システムに対して名前をチェックする方法、およびテキストとテストを名前にバインドする記述フォーマットが含まれます。

SCAP データストリームには、CPE 名を OVAL 定義にマップする CPE ディクショナリを含めるオプションがあります。この OVAL 定義を使用して、CPE 名で識別される OS またはアプリケーションの存在をテストします。DCS は、データストリームからの XCCDF ファイルに `<platform>` タグが含まれるときに、このディクショナリを使用します。このタグは、XCCDF ファイルが指定した CPE 名の存在を要求していることを示しています。すべてのパッケージ化された FDCC チェックリストには、CPE ディクショナリ ファイルおよび XCCDF ファイルで指定されたそれらの参照が含まれます。XCCDF 結果ファイルに `<platform>` タグの CPE 名が含まれると、プラットフォームテストがチェックリスト全体で成功したことを示します。出力ファイルの名前および場所は、DSM エクスプローラで、[インベントリ] - [SCAP] - <チェックリスト インベントリ コンポーネント> - [Status] グループ以下に表示されます。

## CVSS

共通脆弱性評価システム (CVSS) 標準は、IT 脆弱性の特性と影響を伝えるオープンフレームワークを提供します。この計量モデルは、繰り返し可能で正確な計測を確保する一方で、スコアを生成するために使用した潜在的な脆弱性の特性を確認することができます。したがって、CVSS は、正確で一貫性のある脆弱性の影響のスコアを必要とする、産業、組織、および政府にとって標準の計測システムとして適しています。CVSS の 2 つの一般的な用途は、脆弱性の改善のための活動のプライオリティの表示と、システムで検出された脆弱性の重大度の算出です。NVD (National Vulnerability Database) は、ほとんど知る限りの脆弱性の CVSS スコアを提供します。

すべてのパッチまたは脆弱性ごとに、CVE ID 参照が DSM エクスプローラで提供されています。DSM エクスプローラは、CVE URL および NVD URL を含む詳細なパッチ結果も提供します。この URL を使用して、NIST (National Institute of Standards and Technology) の Web ページで、NVD 内の対応する CVE ID のエントリを参照できます。このデータベース エントリには、脆弱性に関する CVSS スコアおよび追加の情報が含まれています。CVE 参照の詳細は、[インベントリ] - [SCAP] - <チェックリスト インベントリ コンポーネント> - [Detailed patch results] グループ以下に表示されます。

## XCCDF

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 システムのある集合のセキュリティ設定ルール の構造化されたコレクションを示します。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。

DCS は、XCCDF ファイルを読み込み、XCCDF ファイルで指定されたルールに基づいてターゲット コンピュータをスキャンできます。スキャナは、XCCDF ファイル内の各ルールに関する結果が含まれるインベントリ ファイルを生成します。XCCDF 出力ファイルは、各エージェント コンピュータのエージェントの作業ディレクトリに保存されます。ルールの結果および最終的なスコアは、DSM エクスプローラの、[インベントリ] - [SCAP] - <チェックリスト インベントリ コンポーネント> - [Rule Results] 以下に表示されます。

XCCDF ファイル、および処理済みの結果ファイルの名前と場所は、DSM エクスプローラの、[インベントリ] - [SCAP] - <チェックリスト インベントリ コンポーネント> - [Status] グループ以下に表示されます。

## OVAL

Client Automation は、セキュリティ検査言語 (OVAL) 標準を実装します。OVAL は、オープンで公に利用可能なセキュリティ コンテンツの促進に使用される国際的な情報セキュリティ、コミュニティ標準です。その目標は、セキュリティ ツールとサービスの全範囲にわたって、この情報の転送を標準化することです。

XCCDF ファイル内のチェックリスト ルール定義は通常、ターゲット コンピュータのルール準拠性をどのようにチェックするかを示す方法として OVAL ファイルの OVAL 定義を参照します。同様に、CPE ディクショナリにリストされる CPE 名も、名前によって示されるソフトウェアの一部の存在をどのようにチェックするかを指定する方法として OVAL 定義を参照します。これらの目的のために、バンドルされた DCS SCAP データ ストリームには、すべて、1 つ以上の OVAL ファイルが含まれています。

各評価済み OVAL ファイルの場合、OVAL インタープリタは、エージェントの作業ディレクトリに OVAL 結果ファイルを作成します。すべての OVAL ファイル、および処理済みの結果ファイルの名前と場所は、DSM エクスプローラの、[インベントリ] - [SCAP] - <チェックリスト インベントリ コンポーネント> - [Status] グループ以下に表示されます。



# 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 ファイルを無償で提供し、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のあるセキュリティ要件が規定されています。