

Dell EMC Avamar

バージョン 18.2

管理ガイド

302-005-101

REV 01

Copyright © 2001-2018 年 Dell Inc. その関連会社。All rights reserved. (不許複製・禁無断転載)

2018 年 12 月発行

掲載される情報は、発信現在で正確な情報であり、予告なく変更される場合があります。

本文書に記載される情報は、「現状有姿」の条件で提供されています。本文書に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示的保証はいたしません。この資料に記載される、いかなる Dell ソフトウェアの使用、複製、頒布も、当該ソフトウェアライセンスが必要です。

Dell、EMC、および Dell または EMC が提供する製品及びサービスにかかる商標は Dell Inc. またはその関連会社の商標又は登録商標です。その他の商標は、各社の商標又は登録商標です。Published in the USA.

EMC ジャパン株式会社
〒 151-0053 東京都渋谷区代々木 2-1-1 新宿メインズタワー
www.DellEMC.com/ja-jp/index.htm
お問い合わせは
www.DellEMC.com/ja-jp/index.htm

目次

図		13
表		15
序文		19
第 1 章	概要	23
	Avamar システムの概要.....	24
	Avamar サーバー.....	24
	Avamar クライアント.....	27
	ユーザー インターフェイス.....	29
	Data Domain システムのサポート.....	31
	データ重複排除.....	32
	セキュリティとネットワーク.....	32
	暗号化.....	32
	IPv4 および IPv6 のサポート.....	33
	TSL 1.2 暗号化プロトコルが必要.....	34
	SSH MAC アルゴリズム.....	34
第 2 章	Avamar Administrator	35
	Avamar Administrator の概要.....	36
	Avamar Administrator のインストール.....	36
	Microsoft Windows に Avamar Administrator をインストールする.....	36
	Linux に Avamar Administrator をインストールする.....	37
	Avamar Administrator のアップグレード.....	38
	Avamar Administrator のアンインストール.....	39
	Avamar Administrator クライアント プリファレンスの編集.....	39
	Avamar Administrator のセッション タイムアウトの設定.....	39
	Avamar Administrator の起動.....	40
	Avamar Administrator ダッシュボード.....	42
	起動リンク.....	42
	[System Information] パネル.....	43
	[Activities] パネル.....	45
	[Capacity] パネル.....	47
	[Critical Events] パネル.....	47
	Avamar Administrator ユーザー インターフェイスの構成要素.....	48
	ステータス バー.....	48
	ナビゲーション ツリーの機能.....	51
	マウスでの操作.....	52
第 3 章	Avamar Web ユーザー インターフェイス	53
	AUI の概要	54

	AUI へのアクセス.....	54
	AUI ナビゲーション ペイン.....	55
	基本管理タスク.....	56
	ナビゲーション ツリーの機能.....	57
	AUI ダッシュボード.....	57
	ダッシュボードでの資産の監視.....	58
	ダッシュボードでのシステム容量の監視.....	59
	ダッシュボードでのイベントの表示.....	60
	ダッシュボードでのバックアップ ジョブの監視.....	61
	ダッシュボードでのレプリケーション ジョブの監視.....	61
	クライアント情報の表示.....	61
	AUI アクティビティ モニター.....	62
	Activity Monitor の詳細.....	63
	バックアップの監視.....	65
	バックアップのキャンセル.....	65
	バックアップ ジョブの再開.....	66
	詳細なクライアント セッション ログの表示.....	66
	リストアの監視.....	66
	リストアのキャンセル.....	67
	AUI でのレプリケーションの監視.....	67
	レプリケーション タスクのキャンセル.....	68
第 4 章	クライアントの管理	69
	Avamar クライアントの概要.....	70
	クライアント ドメイン.....	70
	ドメインの作成.....	71
	ドメイン情報の編集.....	71
	ドメインの削除.....	72
	クライアント登録.....	72
	クライアント側登録.....	72
	クライアントの登録または追加.....	73
	クライアントのバッチ登録.....	73
	クライアントのアクティブ化.....	76
	クライアントの再アクティブ化.....	77
	クライアント ページング.....	77
	ページング可能クライアント.....	77
	ページング不可能なクライアント.....	78
	クライアント ページング設定の追加または変更.....	79
	クライアント情報の編集.....	79
	クライアント プロパティの表示.....	80
	クライアントの有効化/無効化.....	81
	クライアントを新規ドメインに移動.....	81
	クライアントの廃棄.....	82
	クライアントの削除.....	83
	統合クライアントの表示.....	83
	保護されていないクライアントの表示.....	84
第 5 章	ユーザー管理と認証	85
	Avamar ユーザー アカウントの概要.....	86
	ユーザー認証.....	86

	Avamar がユーザーを認証して役割を割り当てる方法.....	87
	Avamar 内部認証.....	88
	ディレクトリ サービスの認証.....	88
	LDAP ディレクトリ サービス認証.....	89
	OpenLDAP ディレクトリ サービス認証.....	96
	NIS ディレクトリ サービスの追加.....	101
	ディレクトリ サービスの構成中に表示されるエラー メッセージ.....	103
	LDAP マップの追加.....	103
	LDAP マップの役割の編集.....	104
	LDAP マップの削除.....	105
	ディレクトリ サービス プロセスの time-out 値の編集.....	105
	エンタープライズ認証での下位互換性の有効化.....	106
	ロール.....	107
	管理者ロール.....	107
	オペレーター ロール.....	108
	ユーザーの役割.....	109
	ロール ベースのアクセス制御と AUI.....	110
	ドメインへのユーザーの追加.....	112
	ユーザー情報の編集.....	113
	ユーザーの削除.....	114
第 6 章	バックアップ	115
	オン デマンド バックアップについて.....	116
	オン デマンド バックアップの実行.....	116
	[Policy] ウィザードを使用したバックアップのスケジュール設定.....	117
	データセット カタログ.....	118
	スケジュールの管理.....	124
	ルールの管理.....	129
	保存ポリシー.....	132
	バックアップ ポリシーについて.....	136
	バックアップ ポリシーの管理.....	137
	バックアップ ポリシーのオン デマンド バックアップの開始.....	145
	バックアップ ポリシーのスケジュール バックアップを有効にする.....	145
	バックアップのモニタリング.....	146
	バックアップのキャンセル.....	147
	完了したバックアップの管理.....	147
	完了した管理対象のバックアップの検索.....	147
	バックアップの有効期限日の変更.....	148
	バックアップの保存タイプの変更.....	149
	Avamar Administrator を使用したバックアップの検証.....	149
	バックアップ統計情報を表示.....	150
	バックアップの削除.....	151
第 7 章	リストアとリカバリ	153
	バックアップからのデータのリストア.....	154
	バックアップの検索.....	154
	元のクライアントへのリストア.....	155
	異なるクライアントへのリストア.....	156
	リストアの監視.....	157
	リストアのキャンセル.....	158

Windows クライアント システムのリカバリ.....	159
Red Hat および CentOS Linux システムのリカバリ.....	159
パーティション テーブルの再構築.....	159
ターゲット リカバリ クライアントの準備.....	160
Red Hat または CentOS Linux クライアントのシステム リカバリを実行する....	161
Red Hat または CentOS Linux クライアントのシステム リカバリに関するトラブ	
ルシューティング.....	165
SUSE Linux システムのリカバリ.....	166
パーティション テーブルの再構築.....	166
ターゲット リカバリ クライアントの準備.....	167
SUSE Linux クライアントのシステム リカバリを実行する.....	168
SUSE Linux クライアントのシステム リカバリをトラブルシューティングする....	171
Oracle Solaris システム リカバリ.....	173
Oracle Solaris システム リカバリのための準備.....	173
Oracle Solaris クライアントのシステム リカバリの実行.....	174

第 8 章

サーバー管理	177
サーバーのシャットダウンと再起動.....	178
Avamar サブシステムの管理.....	178
サーバの電源オフまたは再起動.....	180
サーバー アクティビティの一時停止と再開.....	182
バックアップとリストアの一時的停止と再開.....	182
スケジュールされた操作の一時的停止と再開.....	182
メンテナンス アクティビティの一時的停止と再開.....	183
クライアント セッションの管理.....	183
クライアント セッションのモニタリング.....	183
クライアント セッションの詳細ログの表示.....	184
Avamar サポート用の Zip ファイルの作成.....	185
クライアント セッションのキャンセル.....	185
クライアントのリセット.....	186
クライアント エージェントとプラグ インの管理.....	186
ビルド レコードの追加.....	187
バージョンまたはビルド レコードの編集.....	187
ビルド レコードの削除.....	187
クライアントが開始するすべてのアクティベーションを無効化する.....	188
クライアントが開始するすべてのバックアップを無効化する.....	188
バックアップ ウィンドウとメンテナンス ウィンドウ.....	188
バックアップ ウィンドウとメンテナンス ウィンドウの編集.....	190
チェックポイント.....	190
チェックポイントの作成.....	191
チェックポイントの削除.....	191
チェックポイントのロールバック.....	192
データの整合性アラートの消去.....	193
Avamar ソフトウェアのアクティブ化とサーバ ライセンスのインストール.....	193
Avamar ソフトウェアのアクティブ化.....	193
ライセンスのインストールとアクティブ化.....	194
サービスの管理.....	195
[Services Administration] タブの情報.....	195
サーバー パスワードと OpenSSH キーを変更する.....	196
MCS 構成設定.....	198

	MCS データのバックアップ.....	199
	MCS データのリストア.....	200
	デフォルトの MCS 構成設定に戻す.....	201
	NAT (ネットワーク アドレス変換) の使用.....	201
	NAT に関する一般的な問題のソリューション.....	202
	シングル ノード サーバーでネットワーク設定を編集する.....	203
	Web ブラウザからのログインにカスタムのセキュリティ通知を追加する.....	203
	サーバー担当者情報の表示と編集.....	203
	バックアップの移行.....	204
第 9 章	サーバーの監視	207
	毎日のサーバー監視の推奨.....	208
	アクティビティのモニタリング.....	208
	Activity Monitor の詳細.....	208
	サーバーのステータスと統計のモニタリング.....	211
	[Server Monitor] タブ.....	211
	[Server Management] タブ.....	214
	イベントの監視.....	226
	イベント通知.....	227
	イベント プロファイル.....	229
	[Event Monitor] でイベントを表示する.....	235
	イベント カタログの表示.....	236
	システム イベントの確認.....	237
	エラー イベントのカスタマイズ.....	237
	syslog を使用したサーバのモニタリング.....	237
	ローカル syslog の構成.....	238
	リモート syslog の構成.....	239
	SNMP を使用したサーバーのモニタリング.....	243
	SNMP を使用したサーバーのモニタリングの構成.....	244
	Avamar サーバ ログ ファイルの表示.....	246
	監査ログ.....	247
	監査ログの表示.....	248
	Avamar サポートへの自動通知.....	248
	使用状況インテリジェンス.....	249
	E メール ホーム.....	250
	ConnectEMC.....	251
	システムの整合性の検証.....	256
第 10 章	容量管理	259
	容量使用率の情報.....	260
	容量の制限と閾値.....	260
	容量フォーキャスト.....	261
	容量制限と動作のカスタマイズ.....	261
	Avamar Administrator の容量設定の編集.....	261
第 11 章	レプリケーション	265
	Avamar レプリケーションの概要.....	266
	レプリケーションのタイプ.....	266
	レプリケーションのスケジュール設定.....	266
	レプリケーション認証.....	267

ターゲット Avamar システムのレプリカの場合.....	268
Replicas at Source.....	268
レプリカの保存.....	270
Data Domain システムを使用したレプリケーション.....	271
Replicas at Source の有効化.....	272
ポリシー ベースのレプリケーションの構成.....	273
レプリケーション ターゲット.....	273
レプリケーション グループ.....	276
AUI でのオン デマンドレプリケーションの実行.....	282
[Policy] ウィンドウからオン デマンドレプリケーションを実行する.....	282
コマンドラインレプリケーションの実行.....	283
コマンド リファレンス.....	283
CLI の使用例.....	294
レプリケーションのモニタリング.....	295
AUI でのレプリケーションの監視.....	295
AUI でのレプリケーション タスクのキャンセル.....	295
ターゲット システム上のレプリカからバックアップをリストアする.....	296
Replicas at Source をサポートする MCS 構成パラメーター.....	297
Replicas at Source の構成の変更.....	299
Replicas at Source のリストア.....	300

第 12 章 **サーバー更新とホットフィックス** **301**

Avamar サーバ ソフトウェア アップデート プロセスの概要.....	302
Avamar Downloader Service.....	302
AvInstaller および Avamar インストール マネージャー.....	303
Avamar Downloader Service のインストールと構成.....	305
Avamar Downloader Service の構成.....	305
EMC リポジトリから新しいパッケージをダウンロードする.....	306
Avamar サーバでのパッケージのダウンロードおよびインストール.....	306
Avamar サーバ上のインストール パッケージのリストの表示.....	307
Avamar サーバへのインストール パッケージのアップロード.....	308
Repository タブの見出し.....	308
Avamar サーバからのパッケージの削除.....	309
インストール履歴の表示.....	310
インストール履歴情報.....	310
レガシー Avamar Downloader Service の使用.....	311
レガシー Avamar Downloader Service のインストール要件.....	312
レガシー Avamar Downloader Service ソフトウェアのダウンロード.....	312
レガシー Avamar Downloader Service ソフトウェアのインストール.....	313
HTTPS の有効化.....	313
レガシー Avamar Downloader Service の構成.....	314
レガシー Avamar Downloader Service ソフトウェアのアップデート.....	316
レガシー Avamar Downloader Service のアンインストール.....	316
EMC リポジトリから新しいパッケージをダウンロードする.....	316
ダウンロード可能なパッケージのリストを表示する.....	317
EMC リポジトリの接続性の表示.....	317
Avamar Downloader Service ステータスのモニタリング.....	318
Avamar Downloader Service モニターの停止と起動.....	319
Avamar Downloader Service に関する問題のトラブルシューティング.....	319

第 13 章	Avamar Client Manager	321
	Avamar Client Manager の概要.....	322
	接続セキュリティ.....	322
	Apache Web サーバー認証.....	322
	session time-out 時間の編集.....	322
	JavaScript time-out 時間の増加.....	323
	Avamar Client Manager の構成プロパティ.....	324
	Avamar Client Manager の起動.....	325
	ログイン ページ.....	326
	グローバル ツール.....	326
	Avamar サーバの追加.....	326
	Avamar サーバの削除.....	327
	Avamar サーバの設定の変更.....	327
	サーバーの選択.....	328
	フィルター.....	328
	詳細の表示.....	334
	データのエクスポート.....	335
	1 ページのエントリー数の制限の設定.....	335
	ツール チップの表示.....	335
	概要.....	336
	サーバ サマリー.....	336
	ダッシュボード.....	337
	クライアント.....	340
	クライアントおよびサーバー ツール.....	340
	[Add Clients]	346
	[Registered Clients]	351
	アクティブ化されたクライアント.....	352
	失敗したクライアント.....	354
	アイドル状態のクライアント.....	355
	クライアントのアップグレード.....	355
	ポリシー.....	358
	グループへのクライアントの追加.....	358
	グループからのクライアントの削除.....	359
	グループのデータセット ポリシーの表示.....	359
	グループの保存ポリシーの表示.....	360
	グループのスケジュール ポリシーの表示.....	360
	キュー.....	360
	タスクのキャンセル.....	361
	ログ.....	361
	Avamar クライアントのアップグレード後のクライアント ログの表示.....	362
	セクションのすべてのログ エントリーの消去.....	363
第 14 章	Avamar デスクトップ/ラップトップ	365
	Avamar デスクトップ/ラップトップの概要.....	366
	Avamar デスクトップ/ラップトップの要件.....	367
	クライアント コンピューターの要件.....	367
	Web ブラウザの要件.....	369
	ネットワークの条件.....	369
	Avamar クライアント ソフトウェアのインストール.....	370
	サポートされているシステム管理ツール.....	370
	Windows コンピューターへのプッシュ インストール.....	370

	Macintosh コンピューターでのプッシュ インストール.....	372
	ローカル クライアントのインストール.....	372
	Avamar クライアント ソフトウェアのアンインストール.....	373
Avamar	デスクトップ/ラップトップのユーザー 認証.....	373
	パススルー 認証.....	373
	LDAP 認証.....	374
	Avamar 認証.....	376
	混合認証.....	377
Avamar	デスクトップ/ラップトップ ユーザー インターフェイス.....	378
	クライアント ユーザー インターフェイス.....	378
	Web ユーザー インターフェイス.....	379
Avamar	デスクトップ/ラップトップを使用したバックアップ.....	384
	スケジュール設定されたバックアップ.....	385
	[Add data] オプション.....	386
	シングル クリック バックアップ.....	386
	インタラクティブなバックアップ.....	387
	オン デマンド バックアップの無効化.....	389
	オン デマンド バックアップの保存ポリシーを変更する.....	390
Avamar	デスクトップ/ラップトップを使用したリストア.....	390
	リストア対象のデータを見つける.....	390
	リストアのタイプ.....	391
	リストア要件.....	392
	リストアの制限.....	394
	レプリケートされたバックアップのリストア.....	394
	クライアントのバックアップおよびリストア アクティビティの履歴.....	395
Avamar	デスクトップ/ラップトップ パラメーターの編集.....	395
	Avamar デスクトップ/ラップトップパラメーター.....	395
	クライアント ログの場所.....	397

第 15 章	Data Domain システムの統合	399
	Data Domain システム統合の概要.....	400
	Avamar と Data Domain の統合.....	400
	Data Domain でのファイル システムのバックアップ.....	401
	Data Domain システムでのアプリケーションのバックアップ.....	401
	Data Domain Cloud Disaster Recovery.....	401
	VMware インスタント アクセス.....	402
	クラウド階層.....	402
	Data Domain システムでのチェックポイント.....	402
	Data Domain システム ストリーム.....	403
	Data Domain システムを使用したレプリケーション.....	403
	Data Domain システムのステータスの監視とレポート.....	404
	Data Domain システム統合のセキュリティ.....	404
	接続された Data Domain システムへのデータの移行.....	404
	Data Domain へのバックアップ適用.....	405
	Data Domain システムの追加の準備.....	405
	Data Domain システム統合のシステム要件.....	405
	DD Boost ユーザー アカウントの作成.....	408
	Data Domain システムの追加.....	409

付録 A	コマンド シェル サーバー ログイン	413
-------------	---------------------------	------------

	ユーザー アカウント.....	414
	コマンド シェル セッションの開始.....	414
	ユーザー ID の切り替え.....	414
	sudo の使用.....	415
	sudo によるコマンドのプレフィックス.....	415
付録 B	プラグ イン オプション	417
	プラグ イン オプションの設定方法.....	418
	バックアップ オプション.....	418
	リストア オプション.....	421
付録 C	Avamar Web Restore ページへのファイルの追加	425
	Avamar Web Restore の [Downloads] ページへのファイルの追加.....	426
	Avamar Web Restore の [Documentation] ページへのファイルの追加.....	427
用語集		429



1	Avamar サーバー ノード、ストライプ、オブジェクト.....	24
2	Avamar サーバーの機能ブロック図.....	26
3	Avamar クライアント エージェントとプラグ イン.....	28
4	データ重複排除.....	32
5	Avamar Administrator ダッシュボード.....	42
6	Avamar Administrator ステータス バー.....	48
7	ナビゲーション ツリーの機能.....	52
8	AUI ナビゲーション ペイン.....	55
9	AUI ダッシュボード.....	58
10	Avamar ドメインの例.....	70
11	Avamar ドメイン内のユーザー.....	86
12	開始時間、終了時間、継続期間のスケジュール設定.....	125
13	デフォルトのバックアップ ウィンドウとメンテナンス ウィンドウ.....	189
14	NAT を使用したマルチ ノード サーバー構成.....	202
15	レプリケーション ドメイン構造の例.....	268
16	CSV ファイルの例をアップロードした後のビュー.....	349
17	Avamar クライアント Web ユーザー インターフェイスの置き換え可能なグラフィック.....	382



表

1	表記規則.....	20
2	MCS 機能.....	26
3	サポートされるプラグ イン.....	28
4	Backup & Recovery Manager の Avamar システム管理機能.....	29
5	ダッシュボード起動リンク.....	42
6	Avamar Administrator ダッシュボード上の [System State] のフィールド.....	43
7	Avamar Administrator ダッシュボードの [Backup Jobs] フィールド.....	46
8	[Critical Events] パネルのシステム アラート.....	47
9	ステータス バーの起動ショートカット アイコン.....	48
10	スケジューラおよびバックアップ ディスパッチのステータス メッセージ.....	49
11	未確認イベントに対するステータス メッセージ.....	49
12	Avamar または Data Domain の動作ステータス メッセージ.....	50
13	AUI ナビゲーション ペイン.....	55
14	システム アラート.....	60
15	Activity Monitor で利用可能なセッションの詳細	63
16	Activity Monitor で利用可能なクライアントの詳細.....	63
17	Activity Monitor で利用可能なポリシーの詳細.....	64
18	クライアント定義ファイルの各エントリーの属性.....	74
19	クライアント サマリー情報.....	80
20	Avamar ユーザー アカウント情報.....	86
21	サポートされるディレクトリ サービス タイプ.....	88
22	必要なキー配布センター ポート.....	90
23	LDAP ベースの機能のパラメーター要件.....	94
24	LDAP ベースの機能のその他のパラメーター	95
25	OpenLDAP ディレクトリ サービス パラメーター.....	100
26	ディレクトリ サービスの構成中に表示されるエラー メッセージ.....	103
27	管理者ロール.....	107
28	オペレーター ロール.....	108
29	ユーザーの役割.....	110
30	管理者ユーザー ロールによってアクセスできる AUI 機能パネル.....	110
31	オペレーター ユーザー ロールによってアクセスできる AUI 機能パネル.....	111
32	Default Dataset バックアップから除外されるディレクトリ	118
33	UNIX Dataset バックアップから除外されるディレクトリ	119
34	Windows Dataset バックアップから除外されるディレクトリ	119
35	スケジュール タイプ.....	125
36	スケジュール カタログ.....	126
37	スケジュールの各タイプの設定.....	127
38	基本的な保存期間の設定.....	133
39	保存ポリシー カタログ.....	134
40	VMware groups.....	137
41	スケジュールの各タイプの設定.....	141
42	[Jobs Backups] パネル.....	150
43	[Backup Statistics] ダイアログ ボックスの情報.....	151
44	Oracle Solaris クライアントのシステム リカバリ バックアップのターゲット場所.....	173
45	[Session Monitor] タブのプロパティ.....	183
46	Avamar サーバのメンテナンス アクティビティ.....	189
47	チェックポイントの状態.....	191
48	[Services Administration] タブの情報.....	195
49	MCS 構成ファイルのデフォルトのライブ ファイル ディレクトリ.....	198

50	MCS バックアップのタイム スタンプ ファイル.....	199
51	NAT に関する一般的な問題のソリューション.....	203
52	View/Edit Contact Information ダイアログ ボックスの読み取り専用フィールド.....	204
53	View/Edit Contact Information ダイアログ ボックスの編集可能フィールド.....	204
54	システム監視ツールおよびタスク.....	208
55	Activity Monitor で利用可能なセッションの詳細	209
56	Activity Monitor で利用可能なクライアントの詳細.....	209
57	Activity Monitor で利用可能なポリシーの詳細.....	210
58	[Server Monitor] の [Avamar] タブに表示されるノードの詳細.....	212
59	[Server Monitor] の [Avamar] タブに表示される CPU の詳細.....	212
60	[Server Monitor] の [Avamar] タブに表示されるネットワークの詳細.....	212
61	[Server Monitor] の [Avamar] タブに表示されるディスクの詳細.....	213
62	[Server Monitor] の [Data Domain] タブに表示されるノードの詳細.....	213
63	[Server Monitor] の [Data Domain] タブに表示される CPU の詳細.....	214
64	[Server Monitor] の [Data Domain] タブに表示されるディスク (KB/S) の詳細.....	214
65	[Server Monitor] の [Data Domain] タブに表示されるネットワーク (KB/S) の詳細.....	214
66	[Server Management] タブでの選択項目に基づいたデータの表示.....	215
67	[Server Management] タブの [Bytes Protected Summary] プロパティ.....	215
68	[Server Management] タブに表示されるサーバーの詳細.....	215
69	[Server Management] タブに表示されるメンテナンス アクティビティの詳細.....	217
70	[Server Management] タブに表示されるガベージ コレクションの詳細.....	217
71	[Server Management] タブのモジュールのプロパティ	218
72	[Server Management] の [Node Information] 領域の [Status indicators]	218
73	[Server Management] の [Node Information] 領域に表示されるサーバーの詳細.....	219
74	[Server Management] の [Node Information] 領域に表示される OS の詳細.....	221
75	[Server Management] の [Node Information] 領域に表示されるハードウェアの詳細.....	221
76	[Server Management] の [Partition Information] 領域の [Status indicators]	221
77	[Server Management] の [Node Information] 領域に表示されるサーバーの詳細.....	222
78	[Server Management] タブの Data Domain システムのプロパティ.....	223
79	イベント情報.....	226
80	バッチ送信メールによる通知メッセージの例.....	227
81	syslog フィールドの Avamar イベント データへのマッピング.....	238
82	Avamar MIB 定義ファイルの場所.....	244
83	容量の制限と閾値	260
84	mcsserver.xml での容量設定.....	262
85	ソース Avamar サーバで使用できる Replicas at Source 機能.....	268
86	Replicas at Source と Avamar タスクの統合に関する説明.....	269
87	DD Boost を使用した Avamar レプリケーションのためのレプリケーション構成.....	271
88	Replicas at Source.....	276
89	avrepl コマンドのアカウント オプション.....	283
90	avrepl コマンドのログ オプション.....	285
91	avrepl コマンドのレプリケーション オプション.....	285
92	avrepl コマンドの Avamar 専用の高度なオプション.....	288
93	数値のプラグ イン ディスクリプター.....	291
94	avrepl コマンドに必要なオプション.....	294
95	Replicas at Source をサポートする MCS 構成パラメーター.....	298
96	Repository タブの情報.....	308
97	[History] タブにある情報.....	310
98	[History] タブの [Details]	311
99	レガシー Avamar Downloader Service のインストール要件.....	312
100	Avamar Downloader Service モニターのステータス メッセージ	318
101	Avamar Client Manager の構成プロパティ.....	324

102	検索文字列に使用できない文字.....	330
103	[Server Summary] セクションで使用される列.....	336
104	[Server] パネルのサーバー情報.....	338
105	[Client Details] の [Advanced] タブの設定.....	343
106	クライアント アクティベーション時の関係の状態.....	350
107	失敗したクライアントのフィルター.....	355
108	[Queues] ページでのタスク タイプ.....	360
109	[Logs] ページでのタスク タイプ.....	361
110	Avamar デスクトップ/ラップトップのハードウェア要件.....	368
111	Avamar デスクトップ/ラップトップでサポートされる Web ブラウザ.....	369
112	Avamar デスクトップ/ラップトップで Web ブラウザを起動するための環境変数.....	369
113	Avamar デスクトップ/ラップトップのネットワーク要件.....	369
114	プッシュ インストールの起動コマンドの引数.....	371
115	Avamar デスクトップ/ラップトップ クライアント ユーザー インターフェイスの機能.....	378
116	Avamar デスクトップ/ラップトップ Web ユーザー インターフェイスの機能.....	379
117	Avamar デスクトップ/ラップトップ クライアント バックアップを開始する方法の説明.....	385
118	シングル クリックによるオン デマンド バックアップのデータセット.....	386
119	restrictBackupsPerDay プロパティでサポートされる値.....	389
120	Avamar デスクトップ/ラップトップ データリストアのフィルター機能.....	392
121	Avamar デスクトップ/ラップトップで別のコンピューターからリストアを行う場合の要件.....	393
122	Avamar デスクトップ/ラップトップパラメーター.....	396
123	クライアントで使用可能なログ.....	397
124	Windows コンピューターでのログへのパス.....	398
125	Linux および Mac コンピューターでのログへのパス.....	398
126	DD Boost を使用した Avamar レプリケーションのためのレプリケーション構成.....	403
127	Data Domain システム要件.....	405
128	バックアップ プラグ イン オプション.....	418
129	SMS 認証 (NetWare のみ) 用のバックアップ プラグ イン オプション.....	419
130	ログ用のバックアップ プラグ イン オプション.....	419
131	ファイル システム スキャン用のバックアップ プラグ イン オプション.....	420
132	前処理スクリプト用のバックアップ プラグ イン オプション.....	420
133	後処理スクリプト用のバックアップ プラグ イン オプション.....	420
134	バックアップ プラグ イン クライアント キャッシュ オプション.....	420
135	バックアップ プラグ インの高度なオプション.....	421
136	バックアップあたりのクォータ制限.....	421
137	ファイル システム プラグ インのリストア オプション.....	422
138	(NetWare のみ) SMS 認証リストア プラグ イン オプション.....	422
139	リストア プラグ イン オプションのログ.....	422
140	前処理スクリプトリストア プラグ イン オプション.....	423
141	後処理スクリプトリストア プラグ イン オプション.....	423
142	クライアント キャッシュ リストア プラグ イン オプション.....	424
143	高度なリストア プラグ イン オプション.....	424

表

はじめに

製品ラインを改善するための努力の一環として、ソフトウェアおよびハードウェアのリビジョンを定期的にリリースしています。そのため、本書で説明されている機能の中には、現在お使いのソフトウェアまたはハードウェアのバージョンによっては、サポートされていないものもあります。製品のリリースノートには、製品の機能に関する最新情報が掲載されています。

製品が正常に機能しない、またはこのドキュメントの説明どおりに動作しない場合には、テクニカルサポート プロフェッショナルにお問い合わせください。

注

このマニュアルには、発行時点で正確だった情報が記載されています。このドキュメントの最新バージョンを確認するには、オンライン サポート (<https://support.EMC.com>) にアクセスしてください。

目的

このガイドでは、Avamar システムの構成、管理、監視、保守を行う方法について説明します。

対象読者

このガイドの情報は主に、ネットワーク上のサーバーとクライアントの管理を担当するシステム管理者、および日常的なバックアップやストレージ デバイスの監視を行うオペレーターを対象にしています。

リビジョン履歴

次の表に、このドキュメントのリビジョン履歴を示します。

リビジョン	日付	説明
01	2018 年 12 月 14 日	Avamar 18.2 の GA リリース。

関連ドキュメント

次に示す資料に補足情報が記載されています。

- <https://elabnavigator.emc.com/eln/modernHomeDataProtection> の「E-Lab Navigator」
- 「Avamar リリースノート」
- 「Avamar オペレーションのベスト プラクティス ガイド」
- 「Avamar および Data Domain システム統合ガイド」
- 「Avamar レポート ガイド」
- すべての Avamar クライアントおよびプラグインのユーザー ガイド

このマニュアルで使用される特記事項の表記規則

特別な注意を要する事項には次の表記法を使用します。

危険

回避しなかった場合に死亡または重傷を招く危険な状況を示します。

警告

回避しなかった場合に死亡または重傷を招く可能性がある危険な状況を示します。

注意

回避しなかった場合に軽度または中程度の傷害を招く可能性がある危険な状況を示します。

通知

負傷に関連しない作業を示します。

注

重要ではあるが、危険ではない情報を表します。

表記規則

このドキュメントではこれらのタイプの表記規則を使用します。

表 1 表記規則

[太字]	ウィンドウ名、ダイアログ ボックス、ボタン、フィールド、タブ名、キー名、メニュー バスなど、インタフェースの構成要素（ユーザーが明示的に選択またはクリックする対象）の名前に使用します。
「斜体」	本文内で参照される出版物の完全なタイトルを示す
Monospace	以下の場合に使用： <ul style="list-style-type: none">システム コードエラー メッセージやスクリプトなどのシステム出力バス名、ファイル名、プロンプト、構文コマンドおよびオプション
モノスペース斜体	変数に使用
モノスペース太字	ユーザーによる入力値を示す
[]	オプション値
	縦棒は、選択肢を示し、「または」を意味する
{ }	中括弧内は、ユーザーが指定する必要がある内容を示す（例：x、y、z）
...	省略記号は、例の中で省略される必須ではない情報を示す

問い合わせ先

Avamar サポート ページを利用すると、ライセンス情報、製品ドキュメント、アドバイザリ、ダウンロード、ハウツーおよびトラブルシューティングの情報にアクセスできます。カスタマー サポートに問い合わせる前に、この情報に基づいて、製品に関する問題を解決できる場合があります。

Avamar サポート ページにアクセスするには、次の手順を実行します。

1. <https://www.dell.com/support/home/us/en/19> に移動します。
2. **[Enter a Service Tag, Serial Number, Service Request, Model, or Keyword]** 検索ボックスに、製品名を入力します。
3. 表示されたリストから製品名を選択します。製品を選択すると、**[Product Support]** ページが自動的にロードされます。
4. (オプション) **[Product Support]** ページの右上隅の **[Add to My Saved Products]** をクリックして、製品を **[My Products]** リストに追加します。

ドキュメント

Avamar 製品ドキュメントには、包括的な機能概要、運用管理業務、テクニカルリファレンス情報が記載されています。製品管理ガイドおよびユーザー ガイドの補足情報については、次のドキュメントを確認してください。

- リリース ノートには、リリースに関する新機能の概要と既知の制限事項が記載されている。
- テクニカル ノートには、特定の製品機能に関する技術的詳細が記載されており、必要に応じて手順をステップごとに説明した内容も含まれている。
- ホワイト ペーパーには、重要なビジネス上の問題や要件に適用される、製品の技術的観点からの詳細な説明がある。

ナレッジベース

ナレッジベースには適用可能なソリューションが含まれており、ソリューション番号（たとえば、KB000xxxxxx）またはキーワードで検索することができます。

ナレッジベースを検索するには、以下の手順を実行します。

1. <https://www.dell.com/support/home/us/en/19> に移動します。
2. **[Support]** タブで、**[Knowledge Base]** をクリックします。
3. 検索ボックスにソリューション番号またはキーワードを入力します。(オプション) 検索ボックスに製品名を入力し、表示されたリストから製品を選択して、検索を特定の製品に限定することができます。

オンライン コミュニティ

製品サポートおよびソリューションに関して共通の関心を持つユーザーとの連絡、会話、製品サポートおよびソリューションの内容については、コミュニティ ネットワーク (<https://community.EMC.com>) にアクセスしてください。すべての製品について、対話形式により、カスタマー、パートナー、認定専門資格保持者とオンラインで対話します。

ライブ チャット

ライブ インタラクティブ チャットを使用してカスタマー サポートにアクセスするには、Avamar サポート ページの **[Service Center]** パネルの **[Join Live Chat]** をクリックします。

サービス リクエスト

カスタマー サポートからの詳細なヘルプが必要な場合は、Avamar サポート ページの **[Service Center]** パネルの **[Create Service Requests]** をクリックしてサービス リクエストを送信します。

注

サービス リクエストを利用するには、有効なサポート契約が結ばれている必要があります。有効なサポート契約の入手方法の詳細や、アカウントに関する質問については、担当営業にお問い合わせください。

未処理のサービス リクエストを確認する場合は、**[Service Center]** パネルで **[Service Center]** リンクをクリックして、**[View and manage service requests]** をクリックします。

サポート強化

すべての Avamar システムで、次のように ConnectEMC と Email Home を有効にすることを推奨します。

- ConnectEMC は、高い優先度を持つイベントに対するサービス リクエストを自動的に生成する。
- Email Home は、構成、容量、一般的なシステム情報をカスタマー サポートにメールで連絡します。

コメントと質問

ドキュメントの正確性、構成、品質を向上するため、お客様のご意見をお待ちしております。本書についてのご意見を DPAD.DOC.Feedback@emc.com にお送りください。

以下の情報を記載してください。

- 製品名とバージョン
- マニュアル名、パーツ番号、リビジョン（例：01）
- ページ番号
- その他、マニュアルの問題解決に役立つ情報

第1章

概要

本章は、次のトピックで構成されています。

- [Avamar システムの概要](#)..... 24
- [データ重複排除](#)..... 32
- [セキュリティとネットワーク](#)..... 32

Avamar システムの概要

Avamar システムは、クライアント/サーバ ネットワークでバックアップとリストアを行うソリューションです。

Avamar システムは、1 つまたは複数の Avamar サーバと、それらのサーバにデータをバックアップするネットワークサーバまたはデスクトップクライアントで構成されています。Avamar システムは、Avamar Administrator のグラフィカル管理コンソール ソフトウェア アプリケーションにより一元管理を提供します。

Avamar サーバー

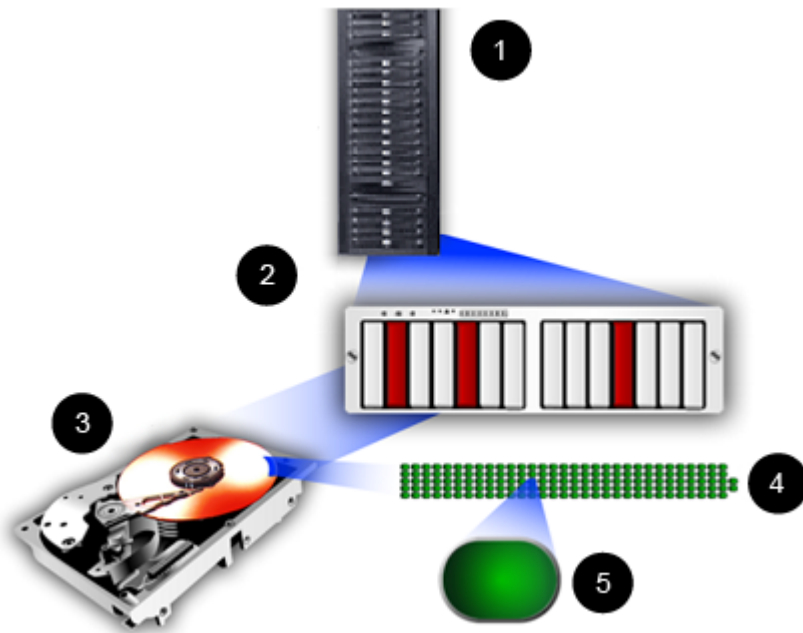
Avamar は、ハードディスク ベースの IP ネットワーク バックアップ/リストア ソリューションです。Avamar サーバーは、内部ハードディスクストレージを使用します。Avamar サーバーは、クライアントバックアップの保存と管理に使用するノードを論理的にグループ化したものです。

通常、ハードウェア メーカーではこのような装置をサーバーと呼んでいます（例：Dell PowerEdge 2950 サーバー）。Avamar システムの用語としては、これを [ノード] と呼びます。Avamar ノードは、自己完結型かつラックマウント型のネットワークアドレス対応コンピューターであり、Linux オペレーティングシステム上で Avamar サーバー ソフトウェアを実行します。

Avamar は、[ストライプ] と呼ばれる領域単位でディスクドライブ領域を管理して、エラー許容度を維持しています。

Avamar システムでは、[オブジェクト] とは、重複排除されたデータのシングル インスタンスを指します。それぞれの Avamar オブジェクトには、それぞれ一意な ID が割り当てられています。オブジェクトは、Avamar サーバーのストライプで保存、管理されます。

図 1 Avamar サーバー ノード、ストライプ、オブジェクト



1. Avamar サーバ
2. Avamar ノード
3. ノードのディスクドライブストレージ

4. ディスクドライブのストライプ
5. ストライプ上のオブジェクト

すべての Avamar サーバーは、クライアントのバックアップを格納し、クライアントへのアクセスとリモートシステム管理に不可欠なプロセスとサービスも提供します。

Avamar サーバーは、シングル ノードまたは拡張可能なマルチ ノード構成で導入できますが、ほとんどの場合、Avamar Administrator 管理コンソール ソフトウェアを使用すると、すべての Avamar サーバーは外観と動作が同じになります。Avamar サーバ構成では、サーバ モニタに表示されるノード数とディスクドライブ数のみが異なります。

Avamar サーバー ハードウェア構成の違いの具体的な内容については、本マニュアルには記載されていません。特定の構成における固有の制限事項やベスト プラクティスが明確になれば、その時点でお知らせいたします。ただし、これらのお知らせは一時的なものであり、確定的な情報ではありません。特定のハードウェアに関する詳細情報については、Avamar 担当営業、または Avamar 販売代理店にお問い合わせください。

ノード

Avamar サーバーの主な構成要素はノードです。個々のノードは、自己完結型かつラックマウント型のネットワーク アドレス対応コンピューターであり、Linux オペレーティング システム上で Avamar サーバー ソフトウェアを実行します。

ノードは、ハードディスクドライブという形で内部ストレージを持つこともできます。ノードが内部ストレージ構成になっている場合（つまり、シングル ノード サーバー）、このノードは、内部的にミラーリングされ、堅牢なフォルト トレランスを提供します。

次のような 3 種類のノードがあります。

ユーティリティ ノード

ユーティリティ ノードは、バックグラウンドの Avamar サーバー ジョブのスケジュール設定および管理専用です。拡張性に優れたマルチ ノード Avamar サーバーでは、単一のユーティリティ ノードによって次の基本内部サービスがサーバーに提供されます。

- MCS (Management Console Server)
- 外部認証
- NTP (ネットワーク タイム プロトコル)
- Web アクセス

ユーティリティ ノードは、マルチ ノード Avamar サーバー上でこれらの重要なサービスを実行するための専用ノードであるため、バックアップの保存には使用できません。シングル ノードの Avamar サーバーには、ユーティリティ ノードとストレージ ノードのすべての機能が 1 つのノードに統合されています。

ストレージ ノード

ストレージ ノードは、バックアップデータを保存するノードです。マルチ ストレージ ノードは、パフォーマンスおよび容量の要件に応じて、マルチ ノード Avamar サーバで構成されます。時間の経過に伴い、ストレージ ノードを Avamar サーバーに追加して、ダウンタイムを生じることなくパフォーマンスを拡張できます。

Avamar クライアントは、Avamar ストレージ ノードに直接接続されます。クライアント接続とデータのロード バランシングは、ストレージ ノードにわたって調整されます。

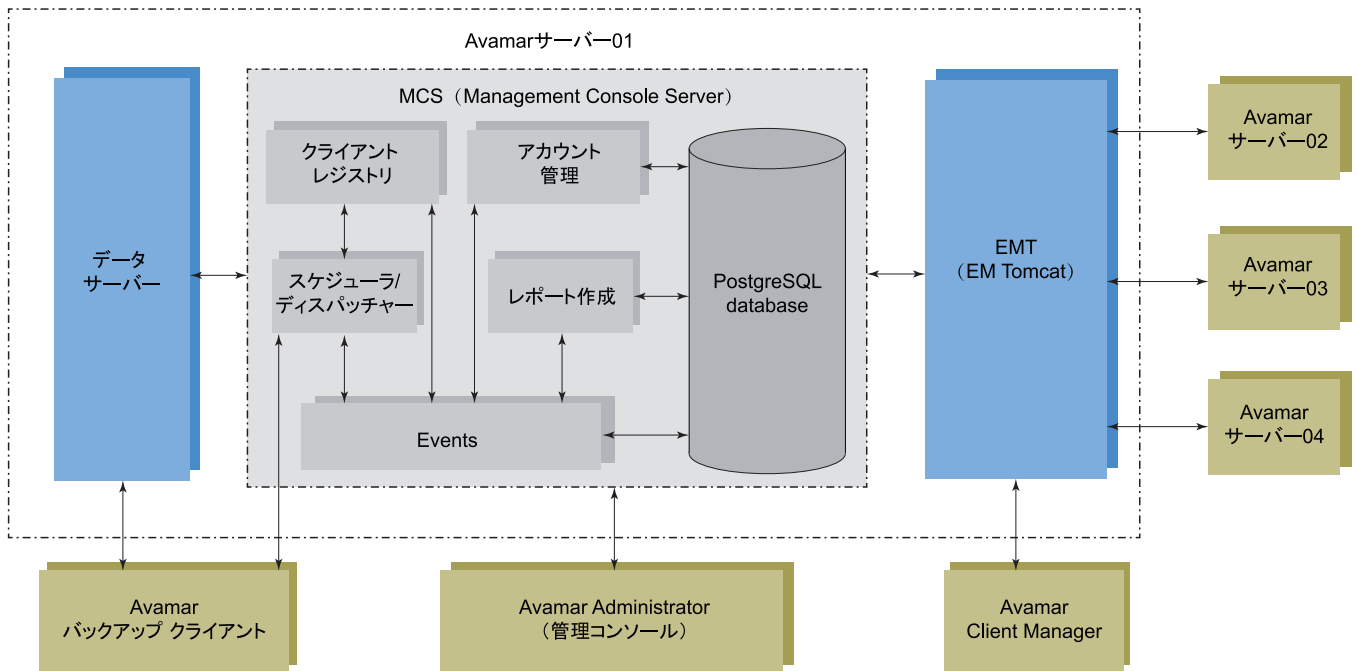
NDMP アクセラレーター

NDMP アクセラレーター ノードは、NDMP を使用して特定の NAS デバイス (EMC Celerra® IP ストレージ システムと Network Appliance ファイラー) のデータを保護する専用ノードです。

Avamar サーバーの機能ブロック

主な Avamar サーバーの機能ブロックには、データサーバー、MCS (Management Console Server)、EMT (EM Tomcat サーバー) が含まれます。次の図に、サーバー内のコンポーネントと他の Avamar コンポーネントの相関関係を示します。

図 2 Avamar サーバーの機能ブロック図



データサーバー

バックアップ、リストア、検証を実行する場合、Avamar バックアップ クライアントはデータサーバーと直接通信します。スケジュール設定バックアップは、すべて MCS スケジューラにより開始されます。

MCS (Management Console Server)

MCS (Management Console Server) により、Avamar サーバーを一元管理 (スケジュール設定、監視、管理) することができます。また MCS は、Avamar Administrator のグラフィカル管理コンソールが使用するサーバ側プロセスも実行します。

次の表では、MCS により提供される機能の詳細について説明しています。

表 2 MCS 機能

機能	説明
クライアントレジストリ	クライアント登録とアクティベーションを制御します。
アカウント管理	ドメイン、クライアント、ユーザー、グループの作成および管理に使用されます。
レポート作成	システムレポートの作成およびエクスポートに使用されます。詳細については、「Avamar レポート ガイド」を参照してください。
イベント	システム イベントおよびアクティビティを表示します。

表 2 MCS 機能 (続き)

機能	説明
スケジューラ/ディスパッチャー	バックアップおよびリストア処理が実行される時間、またはこれらの処理をキューに登録するかどうかを制御します。
PostgreSQL データベース	<p>Avamar サーバー データを保存します。</p> <p>PostgreSQL は、オープン アーキテクチャのデータベース管理システムです。MCS データベースの情報には、PostgreSQL 準拠の ODBC インターフェイス経由でアクセスが可能です。MCS データベースのファイル名は mcdb であり、/usr/local/avamar/var/mc/server_data/postgres ディレクトリのユーティリティ ノードに存在します。MCS データベースのコンテンツは、Avamar サーバに完全にバックアップされ、MCS の障害時にはリストアすることができます。</p> <p>通知</p> <p>MCS データベースは、レポート作成またはクエリーを目的とした、read-only アクセスを対象としたものです。Avamar サポートから指示を受けた場合を除いて、mcdb テーブルのデータは手動で変更しないでください。MCS の操作データを直接変更すると、参照整合性が失われ、回復不能なデータの消失を招く可能性があります。</p>

EMT (EM Tomcat サーバー)

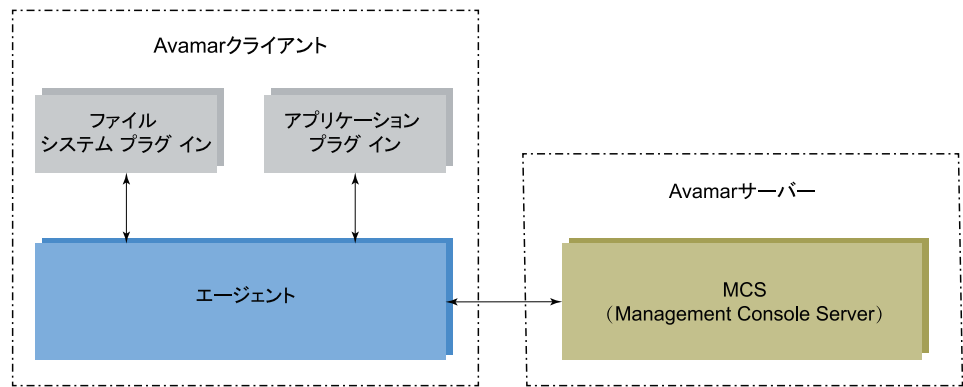
Avamar EMT (EM Tomcat サーバ) は、Avamar サーバ情報の表示や操作に必要とされる重要なサービスを提供します。

EMT は MCS と直接通信します。この通信は、すべての Avamar システムで必要とされる要素です。

Avamar クライアント

Avamar には、さまざまなコンピューティング プラットフォームに適したクライアント ソフトウェアが用意されています。各クライアントは、1つのクライアント エージェントと1つ以上のプラグ インで構成されます。

図 3 Avamar クライアントエージェントとプラグイン



エージェント

Avamar エージェントは、MCS（Management Console Server）およびクライアントにインストール済みのプラグインと通信するために、クライアントで実行されるプラットフォーム固有のソフトウェアプロセスです。

プラグイン

Avamar プラグインには、次の 2 つのタイプがあります。

- ファイルシステムプラグインは、特定のクライアントファイルシステムのファイル、またはディレクトリを参照、バックアップ、リストアする際に使用されます。
- アプリケーションプラグインは、データベースまたはその他の特定のアプリケーションのバックアップおよびリストアをサポートします。

次の表では、Avamar でサポートされるファイルシステムとアプリケーションプラグインを挙げています。

表 3 サポートされるプラグイン

プラグインのタイプ	サポートされるファイルシステムとアプリケーション
ファイルシステム	<ul style="list-style-type: none"> • FreeBSD • HP-UX • IBM AIX • Linux • Mac OS X[Mac OS X] • Microsoft Windows • Microsoft Windows VSS (Volume Shadow Copy Service) • SCO Open Server • SCO UnixWare • Oracle Solaris • VMware
アプリケーション	<ul style="list-style-type: none"> • IBM DB2 • Lotus Domino

表 3 サポートされるプラグ イン (続き)

プラグ インのタイプ	サポートされるファイル システムとアプリケーション
	<ul style="list-style-type: none"> • Microsoft Exchange • Microsoft Hyper-V • MOSS (Microsoft Office Sharepoint Server) • Microsoft SQL Server • NAS デバイス向け NDMP (EMC Celerra IP ストレージ システムと Network Appliance ファイラー) • Oracle • SAP with Oracle • Sybase ASE

クライアントの互換性要件、サポートされるオペレーティング システム、アプリケーションのバージョンの詳細については、<https://elabnavigator.emc.com/eln/modernHomeDataProtection> の「E-Lab Navigator」を参照してください。

ホストにインストールする Avamar ファイル システム クライアントとプラグ インは、同一のバージョン番号である必要があります。

ユーザー インターフェイス

Avamar システムでは、複数のユーザー インターフェイスが利用可能であり、管理とモニタリングを容易に実行できます。

Avamar Web ユーザー インターフェイス

Avamar Web ユーザー インターフェイス (AUI) は、Avamar サーバーの管理に使用される Web 管理アプリケーションです。

Avamar Administrator

Avamar Administrator は、サポートされている Windows クライアント コンピューターから Avamar システムを管理するグラフィカル管理コンソール ソフトウェア アプリケーションです。

Avamar Backup & Recovery Manager

Backup & Recovery Manager では企業内のすべての Avamar システムが管理されます。Backup & Recovery Manager では、企業内の NetWorker サーバーと Data Domain バックアップ ターゲットを管理するための統合されたユーザー インターフェイスも用意されています。

次の表は、Backup & Recovery Manager のエンタープライズ管理機能の一部を示します。この表には、NetWorker サーバーと Data Domain バックアップ ターゲットに固有な Backup & Recovery Manager のその他の機能は含まれていません。

表 4 Backup & Recovery Manager の Avamar システム管理機能

機能	Backup & Recovery Manager
ソフトウェア ホスト	VMware vSphere クライアント

表 4 Backup & Recovery Manager の Avamar システム管理機能（続き）

機能	Backup & Recovery Manager
概要ダッシュボード	Avamar システム、NetWorker サーバー、Data Domain システムの統合ステータスビューと個々のステータスビューを選択できる
Avamar システムに関する詳細なバックアップおよび容量情報	可
バックアップの監視	あり、[Activity Monitor] スクリーンを使用。 [Activity Monitor] スクリーンを使用して、バックアップおよびレプリケーションの詳細を表示し、タスクの開始、停止、再開を実行できる。
レプリケーション管理	可
他の管理アプリケーションの起動	<ul style="list-style-type: none"> • Avamar Administrator • Avamar Client Manager • Avamar インストール マネージャー • AvInstaller サービス
警告、エラー、システム アラートの表示	あり。素早く確認できるグラフィカル表示と、詳細なテキストによる表示。製品別、システム別、カテゴリ別にビューをフィルター。
レポート管理：選択、表示、エクスポート	<ul style="list-style-type: none"> • バックアップ • システム • 構成

ユーザー インターフェイスの詳細情報については、Backup & Recovery Manager 製品マニュアルを参照してください。

Avamar Client Manager

Avamar Client Manager は Web ベースの管理アプリケーションであり、大規模な事業や企業向けに Avamar クライアントの一元管理機能を提供します。Avamar Client Manager は、多数の Avamar クライアントの管理に役立ちます。

Avamar Client Manager は、サポートされているネイティブ オペレーティング システム上の Avamar クライアントおよび VMware 仮想マシンで実行されているサポート対象のオペレーティング システム上の Avamar クライアントと連携して機能します。Avamar Client Manager は、仮想センター、仮想マシン、仮想プロキシ構成を介して Avamar クライアントと連携できません。Avamar Client Manager ユーザー インターフェイスでは、サポートされている Avamar クライアントが表示され、サポートされていないクライアントはすべて表示されません。

Avamar デスクトップ/ラップトップ

Avamar デスクトップ/ラップトップは、企業のデスクトップとラップトップ コンピューターに拡張機能を追加する Avamar クライアント ソフトウェアのバージョンです。

Avamar デスクトップ/ラップトップの機能は、Windows および Macintosh のデスクトップとラップトップにおける Avamar クライアントの機能を向上させるために設計されています。ほとんどの機能は、認定された Linux コンピューターでもサポートされています。

Avamar デスクトップ/ラップトップの機能は、次の 2 種類のユーザー インターフェイスから利用可能です。

- クライアントユーザー インターフェイス（クライアントのローカルユーザー インターフェイス）は、Windows 用 Avamar クライアントまたは Mac OS X 用 Avamar クライアントのいずれかをインストールすると、クライアントコンピューターにインストールされます。クライアントユーザー インターフェイスを使用すると、Windows コンピューターでは通知領域（「システムトレイ」）に、Mac コンピューターではメニューバーに Avamar アイコンが表示されます。Windows でこのアイコンを右クリックするか、Mac でこのアイコンをクリックすると、クライアントメニューが開き、ここからバックアップ、リストア、プログラム設定、ログにアクセスできます。
- Web ユーザー インターフェイス（Web ブラウザー ユーザー インターフェイス）を使用すると、オンデマンド バックアップまたはリストアの開始や、クライアントコンピューターのバックアップおよびリストア アクティビティの表示、クライアントコンピューターの他のバックアップ設定の構成を実行できます。

Avamar インストール マネージャー

Avamar インストール マネージャーユーザー インターフェイスは、Avamar サーバソフトウェア インストールまたはアップグレード中に、カスタマー サポートによってユーティリティ ノードにインストールされる AvInstaller ソフトウェアの一部です。Avamar サーバーでは、Avamar インストール マネージャーを使用してソフトウェアのインストールとアップグレードを行います。

Avamar Downloader Service

Avamar Downloader Service では、Avamar サーバソフトウェア アップデートの確認およびダウンロードのプロセスを管理します。Avamar Downloader Service ソフトウェアは、インターネット上の Avamar サイトおよびサイトにあるすべての Avamar サーバへのネットワーク アクセスが許可されているスタンドアロンの Microsoft Windows サーバで稼働します。

Avamar Web Restore

Avamar Web Restore では、次の機能にアクセスできます。

- リストア対象のバックアップされたディレクトリおよびファイルの検索または参照。
- Avamar クライアントソフトウェアのダウンロード。
- Avamar サーバーに格納されている Avamar 製品マニュアルの表示。
- Avamar 管理者管理コンソール ソフトウェアを開きます。

Data Domain システムのサポート

バックアップは Avamar サーバーまたは Data Domain システムに保存することができます。バックアップメタデータは、Avamar サーバーに保存されます。

Data Domain システムにバックアップを保存するには、Avamar Administrator を使用して Data Domain システムを Avamar の構成に追加します。その後、オンデマンドのバックアップを実行する際、またはスケジュール設定されたバックアップのためのデータセットを作成する際は、プラグイン オプションで [Data Domain system] を選択します。また、CLI（コマンドライン インターフェイス）を使用して、Data Domain システムにバックアップを実行することも可能です。

バックアップをリストアするステップは、Avamar サーバーからのリストアであるか、Data Domain システムからのリストアであるかを問わず、同じです。リストア プロセスによって、バックアップの場所が決定され、バックアップが保存されます。

Data Domain Cloud Tier のサポートは、Avamar 7.4 から開始されました。DD Cloud Tier は、データを Data Domain からクラウドに移動します。Avamar Administrator で、クラウド階層を構成して Avamar バックアップを Data Domain からクラウドに移動でき、これらのバックアップのシームレスなリカバリを実行することができます。

Data Domain Cloud Tier のディザスタリカバリのサポートは Avamar 7.5 から開始されました。Data Domain が消失した場合はクラウドからバックアップをリカバリできます。また、クラウドから Avamar サーバをリカバリすることもできます。

Avamar 環境の Data Domain システムに関する詳細 (Data Domain システムを Avamar の構成に追加する詳しい手順など) については、「Avamar および Data Domain システム統合ガイド」を参照してください。

データ重複排除

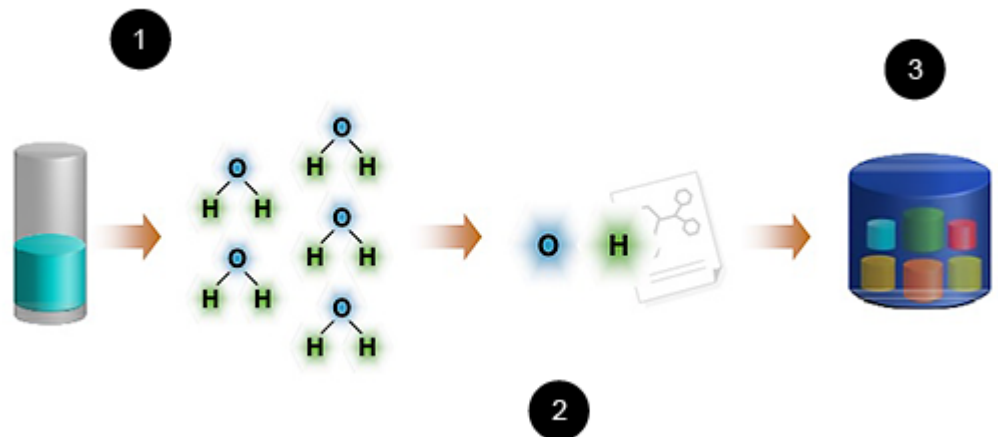
データ重複排除は、Avamar システムの重要な機能です。データ重複排除は、可変長のオブジェクトがサイトとサーバー全体でただ一度だけ保存されるようにするものです。

バックアップ中、Avamar クライアントソフトウェアは、クライアント ファイル システムを検査し、データ重複排除アルゴリズムで冗長データ シーケンスを識別します。まず、クライアントのファイル システムを可変長サブファイルのデータ セグメントに分割し、各データ セグメントに固有の ID (識別子) が振られます。

次に、クライアント ソフトウェアがこの固有 ID が Avamar サーバに保存済みかどうかを判断します。このオブジェクトが Avamar サーバにすでに保存されている場合、保存済みオブジェクトへのリンクはバックアップで参照されています。

一度オブジェクトがサーバー上に格納されると、そのオブジェクトがいずれかのクライアント上で何度出現したのかにかかわらずネットワーク上に再送信されることはありません。この機能により、ネットワークトラフィックを大幅に軽減でき、サーバー上のストレージ効率を大きく向上させることができます。

図 4 データ重複排除



1. データをアトム (ファイル データの可変長セグメント) に分割します。
2. 各アトムを 1 回のみ送信して格納します。
3. Avamar バックアップリポジトリの日次のデータは最大で 500 分の 1 まで削減されます。

セキュリティとネットワーク

次のセクションでは、Avamar の主なセキュリティおよびネットワーク機能の概要について説明します。製品セキュリティおよびネットワーク構成の包括的な詳細情報については、「Avamar 製品セキュリティガイド」を参照してください。

暗号化

セキュリティを機能拡張するには、Avamar では、クライアントとサーバ間で送信される「転送中」のすべてのデータを暗号化します。

暗号化レベルは、クライアント プロパティでクライアントごとに設定するか、グループ プロパティでクライアントのグループ全体に設定することができます。「転送中」暗号化を完全にオフにすることもできます。

Avamar サーバごとに、サーバに保存されているデータも「保存時」に暗号化するように構成することもできます。Avamar サーバに格納されるすべてのデータを暗号化するかどうかの決定は、通常、そのサーバをお客様サイトで初めて導入するときに 1 回だけ行います。

IPv4 および IPv6 のサポート

IP は、Avamar システム コンポーネントのようなアドレス可能なデバイスに、ネットワーク経由でトラフィックを経路指定するための一連の通信ルールです。Avamar システムでは、IPv4（インターネットプロトコルバージョン 4）および IPv6 の両方のアドレス表記をサポートします。

IPv4 表記

IPv4 表記は 4 個のオクテットで示されます。オクテットは 1～3 桁の 0～255 の範囲の 10 進数です。各オクテットは、ピリオドで区切られ、32 ビットのアドレス空間全体に対して 8 ビットのデータを示します。

サブネット マスクは、同じネットワーク上の IP アドレスの範囲（サブネット）を示します。Avamar の場合、サブネット マスクは /24 であり、255.255.255.0 ネットマスクを示します。

IPv4 アドレスとサブネット マスクの例は 10.99.99.99/24 です。

IPv4 表記の省略はできません。オクテットにゼロ (0) 値がある場合、そのオクテットで 0 を使用します。

IPv6 表記

IPv6 表記は 16 個のオクテットで示されます。オクテットは 00～FF の範囲内の 2 桁の 16 進数となります。IPv6 表記では、各オクテットをペアにして、コロンによって 8 個のグループに区切っています。各グループは、128 ビットのアドレス空間全体に対して 16 ビットを示します。

Avamar の場合、サブネット マスク（IPv6 の場合、プレフィックスと呼ばれる）は /64 です。

IPv6 アドレスとプレフィックスの例は 2001:0db8:85a3:0042:1000:8a2e:0370:7334/64 です。

ゼロ (0) の値を持つグループの場合、IPv6 表記では IPv4 表記と異なり、省略が可能です。例えば、次の表記は有効な IPv6 アドレスとプレフィックスです。2001:db8:abcd:0012::0/64。

Avamar IP の構成

Avamar ユーザー インターフェイスの場合、IPv4 または IPv6 表記で IP アドレスを表示できます。表示される値は、ハードウェアおよびソフトウェアのインストール時、該当のコンポーネントの構成方法によって決まります。

IPv4 と IPv6 は相互運用性はありません。それらは個別のスタック（つまり、並列の独立しているネットワーク）で動作します。

Avamar はデュアル スタック構成での設定が可能です。その場合、各 Avamar コンポーネントには、IPv4 アドレス、IPv6 アドレス、またはその両方（1つがプライマリで、もう1つがセカンダリ）が含まれている可能性があります。Avamar ユーザー インターフェイスでは、コンポーネントのプライマリ アドレスまたは両方のデュアル スタック アドレスを表示できます。例えば、特定のデバイスについて次の IP アドレスが表示された場合、それはデュアル スタックとして構成されていることを示します。

10.99.99.99/24, 2001:db8:abcd:0012::0/64。

TLS 1.2 暗号化プロトコルが必要

TLS 1.0 および TLS 1.1 プロトコルを使用して暗号化されたトラフィックは、現在サポートされていません。これらのプロトコルを必要とするブラウザ、クライアント、その他のコンポーネントはサーバに接続できません。TLS 1.2 暗号化のみがサポートされています。

SSH MAC アルゴリズム

SSH の構成が変更されて、SSH 接続に使用される脆弱な MAC アルゴリズムが削除されました。次の MAC アルゴリズムが SSH 接続に使用されます。

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-256
- umac-128-etm@openssh.com
- umac-128@openssh.com
- hmac-ripemd160-etm@openssh.com
- hmac-ripemd160

注

PuTTY や Plink などの以前のバージョンの SSH クライアントでは、SSH 接続の脆弱な MAC アルゴリズムを使用しているため、アップグレードする必要があります。PuTTY の最新リリースを表示するには、<http://www.putty.org/>を参照してください

第 2 章

Avamar Administrator

本章は、次のトピックで構成されています。

- [Avamar Administrator の概要](#)..... 36
- [Avamar Administrator のインストール](#)..... 36
- [Avamar Administrator のアップグレード](#)..... 38
- [Avamar Administrator のアンインストール](#)..... 39
- [Avamar Administrator クライアント プリファレンスの編集](#)..... 39
- [Avamar Administrator のセッション タイムアウトの設定](#)..... 39
- [Avamar Administrator の起動](#)..... 40
- [Avamar Administrator ダッシュボード](#)..... 42
- [Avamar Administrator ユーザー インターフェイスの構成要素](#)..... 48

Avamar Administrator の概要

Avamar Administrator はグラフィカル管理コンソール ソフトウェア アプリケーションであり、サポートされている Windows または Linux クライアント コンピューターから Avamar システムを管理するために使用されます。

サポートされるコンピューターに Avamar Administrator をインストールします。次に、デスクトップ アイコンまたはコマンド シェルからこのソフトウェアを起動するか、Web ブラウザーまたは Backup & Recovery Manager から Java Web Start バージョンのコンソール ソフトウェアを起動します。

Avamar Administrator は、Avamar システムの監視と構成に使用する主要なユーザー インターフェイスです。これを使用すると、バックアップ、リストア、システム メンテナンスといったアクティビティを監視できるほか、バックアップ ポリシーの構成、クライアントおよびユーザー アカウントの管理、他のシステム設定の構成を実行できます。

Avamar Administrator から管理できる Avamar システムは一度に 1 つのみです。

Avamar Administrator にログインすると、Avamar Administrator ダッシュボードが表示されます。このダッシュボードでは、Avamar システム ステータスの概要ビューが提供されるほか、メニューや起動リンクを使用して、すべての機能にアクセスすることができます。

Avamar Administrator のインストール

Avamar Administrator は、サポートされている Microsoft Windows および 64 ビット Linux プラットフォームにインストールできます。

特定のオペレーティング システム バージョンのサポートの詳細については、「E-Lab Navigator」を参照してください。

注

Avamar Administrator をインストールする前に、プラットフォームが手動ですでに Java 7 または 8 にアップグレードされていることを確認します。DNS 環境が、Administrator を実行するすべてのクライアントが hfsaddr (ハッシュ ファイル システム アドレス) の値を解決できるように構成されていることを確認します。

Microsoft Windows に Avamar Administrator をインストールする

手順

1. Avamar Administrator をインストールするコンピューターにログインします。
2. Web ブラウザーを開き、次の URL を入力します。

```
https://Avamar_server/dtlt/home.html
```

ここで、Avamar_server は Avamar サーバーの DNS 名または IP アドレスです。

[Avamar Web Restore] ページが表示されます。

3. [Downloads] をクリックします。
4. オペレーティング システムに応じて、次のいずれかを実行します。
 - 32 ビット Windows 上にソフトウェアをインストールする場合は、[Windows (32 bit)] フォルダーの横にある [+] をクリックします。
 - 64 ビット Windows 上にソフトウェアをインストールする場合は、[Windows (64 bit)] フォルダーの横にある [+] をクリックします。

5. オペレーティング システムに応じて、次のいずれかを実行します。
 - 32 ビット Windows 上にソフトウェアをインストールする場合は、**[Microsoft Windows Vista, 7, 8, 8.1, 10, Microsoft Windows Server 2008 (Console)]** フォルダーの横にある **[+]** をクリックします。
 - 64 ビット Windows 上にソフトウェアをインストールする場合は、**[Microsoft Windows Vista, 7, 8, 8.1, 10, Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2 (Console)]** フォルダーの横にある **[+]** をクリックします。
6. JRE (Java Runtime Environment) インストール パッケージを見つけます。通常は、フォルダーの最後のエントリーにあります。
7. クライアント コンピューター上の JRE が Avamar サーバーでホストされている JRE よりも古い場合は、次の手順で Avamar サーバーから新しい JRE をダウンロードし、インストールします。
 - a. `jre-version.exe` インストール パッケージをクリックします。ここで、`version` は JRE バージョンです。
 - b. インストール ファイルを開くか、またはファイルをダウンロードして保存した場所からそのファイルを開きます。
 - c. 画面の指示に従って JRE のインストールを完了します。
8. `AvamarConsoleMultiple-windows-version.exe` インストール パッケージをクリックします。ここで、`version` は Avamar Administrator ソフトウェアのバージョンです。
9. インストール ファイルを開くか、またはファイルをダウンロードして保存した場所からそのファイルを開きます。
10. 画面の指示に従って、Avamar Administrator ソフトウェアのインストールを完了します。

Linux に Avamar Administrator をインストールする

手順

1. Avamar Administrator をインストールするコンピューターにログインします。
2. Web ブラウザーを開き、次の URL を入力します。
`https://Avamar_server/dtlt/home.html`
 ここで、`Avamar_server` は Avamar サーバーの DNS 名または IP アドレスです。

[Avamar Web Restore] ページが表示されます。
3. **[Downloads]** をクリックします。
4. **[Linux for x86 (64 bit)]** フォルダーの横にある **[+]** をクリックします。
5. **[Red Hat Enterprise Linux 5 (Console)]** フォルダーの横にある **[+]** をクリックします。

注

サポートされているすべての Linux バージョンで Red Hat Enterprise Linux 5 インストール パッケージを使用します。

6. JRE RPM インストール パッケージを見つけます。通常、フォルダー内の最後のエントリーにあります。
7. クライアント コンピューターの JRE が Avamar サーバーにホストされている JRE よりも古い場合は、`/tmp` などの一時フォルダーにインストール パッケージをダウンロードします。

インストール パッケージのファイル名は `jre-version-platform.rpm` です。ここで、**version** は JRE バージョンであり、**platform** はコンピューティング プラットフォームです。

8. `AvamarConsole-linux-rhel5-x86_64-version.rpm` インストール パッケージを、`/tmp` などの一時インストール フォルダにダウンロードします。
9. コマンド シェルを開いて、ソフトウェアをインストールするコンピューターに `root` としてログインします。
10. インストール パッケージをダウンロードした一時フォルダにディレクトリを変更するには、`cd /tmp` のようなコマンドを入力します。
11. JRE をダウンロードしたら、`rpm -ivh jre-version-platform.rpm` と入力して、インストールします。
12. 画面の指示に従って JRE のインストールを完了します。
13. `rpm -ih AvamarConsole-linux-rhel5-x86_64-version.rpm` と入力して、Avamar Administrator をインストールします。

インストール プロセスにより、`avsetup_mcc` を実行して、Avamar Administrator を構成するようにプロンプトで指示されます。

14. `/usr/local/avamar/version/bin/avsetup_mcc` と入力して、Avamar Administrator を構成します。

構成プロセスにより、JRE インストールの場所を指定するようにプロンプトで指示されます。

15. **[Enter]** キーを押してデフォルトのインストールの場所を受け入れます。
構成プロセスにより、Avamar ソフトウェアのルート ディレクトリを指定するようにプロンプトで指示されます。
16. **[Enter]** キーを押してデフォルトのインストールの場所を受け入れます。
確認メッセージが表示されます。

Avamar Administrator のアップグレード

Avamar Administrator は、Microsoft Windows または Linux コンピューターのいずれかでアップグレードできます。

手順

- 同一の Microsoft Windows コンピューターに Avamar Administrator の複数のバージョンをインストールすることが可能です。すでに Avamar Administrator をインストール済みのコンピューターに、Avamar Administrator をインストールする場合は、インストール処理手順でインストール先フォルダを注意して選択してください。
 - 旧バージョンを残す場合は、別のインストール フォルダを選択してください。
 - Avamar Administrator インストールを直接アップグレードするには、同じインストール フォルダを選択します。2 種類のバージョンは、フル バージョン番号で識別されます。

注

Avamar Administrator をインストールまたはアップグレードする前に、プラットフォームが Java 7 または 8 に手動ですでにアップグレードされていることを確認します。

- Linux プラットフォームの Avamar Administrator ソフトウェアをアップグレードするには、古いバージョンのアンインストールを完了してから、新しいソフトウェアをインストールしてください。Linux ソフトウェア アップグレード コマンド (`rpm -Uh`) の使用はサポートされていません。

注

新しいバージョンの Avamar Administrator をインストールする前に、プラットフォームが Java 7 または 8 に手動ですでにアップグレードされていることを確認します。

Avamar Administrator のアンインストール

Microsoft Windows または Linux コンピューターから Avamar Administrator をアンインストールすることができます。

はじめに

開いている Avamar Administrator セッションをすべて閉じます。開いているセッションがあると、アンインストール プロセスが正常に完了しない場合があります、これによって、今後 Avamar Administrator をインストールする際に問題となる可能性があります。

手順

- Microsoft Windows コンピューターで、Windows の [Start] メニューを開き、[Programs] > [Avamar] > [Administrator] > [version] > [Uninstall] を順に選択して、確認メッセージで [OK] をクリックします。
- Linux コンピューターで次の手順を実行します。
 - a. コマンド シェルを開き、root としてログインします。
 - b. `rpm -qa | grep Av` と入力して、パッケージ名を確認します。
 - c. `rpm -e AvamarConsole-version` と入力します。ここで、AvamarConsole-version は Avamar Administrator インストール パッケージです。

Avamar Administrator クライアント プリファレンスの編集

Avamar Administrator で、Avamar Administrator クライアント プリファレンスの一部を直接編集できます。ただし、多数のプリファレンスは `mcclient.xml` クライアント プリファレンス ファイルでのみ編集可能です。

手順

1. Avamar Administrator を終了します。
2. `install_dir/var/mc/gui_data/prefs/mcclient.xml` をテキスト エディタで開きます。ここで、`install_dir` は Avamar Administrator インストール ディレクトリです。
3. プリファレンス設定の各要素を編集します。
4. ファイルを保存して閉じます。

変更は、次回 Avamar Administrator を起動する際に有効になります。

Avamar Administrator のセッション タイムアウトの設定

Avamar Administrator セッションは、ユーザーがメニューから [Exit] を選択してアプリケーションを閉じるまで、アクティブであり続けます。Avamar Administrator から利用できる資産を保護するために、`session time-out` 値を設定します。この値は、Avamar サーバに接続されたすべての Avamar Administrator セッションに適用されます。

`session time-out` 値を設定すると、Avamar Administrator によってユーザー インターフェイスのアクティビティが監視されます。time-out 値で設定した時間（分単位）の間、ユーザー インターフェイス

スでマウスまたはキーボードのアクティビティがないことが Avamar Administrator で検出されると、すべてのプロセスがシャットダウンされ、すべてのウィンドウが終了され、[Inactive] ダイアログ ボックスが表示されます。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、admin としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. admin としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、admin OpenSSH キーをロードします。
2. `dpnctl stop mcs` と入力して、mcs (Management Console Server) サービスを停止します。
3. `cd /usr/local/avamar/var/mc/server_data/prefs` と入力して、作業ディレクトリを `/usr/local/avamar/var/mc/server_data/prefs` に変更します。
4. 平文テキスト エディターで `mcserver.xml` を開きます。
5. `<node name="mon">` エントリーを見つけます。
6. `<node name="mon">` エントリー内の `<entry key="consoleInactiveMinutesToReport" value="n" />` エントリーの値を編集します。ここで n は、分単位の `session time-out` の値です。
7. 変更を保存して、テキスト エディターを閉じます。
8. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

```
dpnctl start mcs
dpnctl start sched
```

9. コマンド シェルを閉じます。

Avamar Administrator では、次回 Avamar Administrator を開いて、Avamar サーバに接続したときに、新しい `session time-out` 値を使用します。

Avamar Administrator の起動

ローカル コンピューターにインストールされたコンソール ソフトウェアを使用して Avamar Administrator を起動するか、Java Web Start バージョンのコンソール ソフトウェアを使用して Avamar Administrator を起動します。

はじめに

ローカル コンピューターに少なくとも 512 MB のシステム RAM が利用可能であることを確認します。これが不足すると、Avamar Administrator を起動する際に Java ヒープ エラーが発生する場合があります。

手順

1. 次のいずれかの方法で Avamar Administrator を起動します。

コンソール ソフトウェア のバージョン	方法
Microsoft Windows	Windows デスクトップの [Avamar Administrator] アイコンをダブルクリックします。
Linux	コマンド シェルを開いて、 <code>mcgui</code> と入力します。
Java Web Start	Web ブラウザの Web アドレス フィールドに <code>https://Avamar_server/mc-portal/mcgui</code> と入力します。ここで Avamar_server は Avamar サーバの IP アドレスまたは解決可能なホスト名です。
Backup & Recovery Manager の Java Web Start バージョン	Backup & Recovery Manager では、[Systems] ウィンドウで Avamar システムを選択して、[Launch Management Console] をクリックします。

[login] ウィンドウが表示されます。

- [Server] で、ログイン先の Avamar サーバの IP アドレスまたは DNS 名を入力します。

注

[Options] をクリックして [Default Administrator Server] にサーバ名、[Default Domain] にドメイン名を入力すると、[Server] ボックスと [Domain Name] ボックスには、自動的に Avamar サーバ名と Avamar ドメインが入力されます。

- [User Name] にユーザー名を入力します。

すべての Avamar Administrator 機能にアクセスするには、このユーザー名に関連づけられたアカウントに管理者の役割を割り当てる必要があります。その他の役割の場合、機能に制限があります。

内部認証システムを使用して認証するには、ユーザー名のみを入力します。エンタープライズ認証システム（非推奨）またはディレクトリ サービス認証を使用して認証するには、`username@server` を入力します。ここで、`username` はユーザー名であり、`server` は認証サーバの完全修飾ドメイン名です。

ユーザー名に `username@server` の形式を使用する場合、システムはエンタープライズ認証を使用してユーザーの認証を試みます。エンタープライズ認証を使用した認証に失敗すると、システムはディレクトリ サービス認証によってユーザーの認証を試みます。

- [Password] に、ユーザー アカウントのパスワードを入力します。
- [Domain Name] に、ログインする Avamar ドメインを入力します。
 - root ドメインでは、シングル スラッシュ (/) を入力するとデフォルトが使用されます。
 - 特定のドメインまたはサブドメインでは、構文 `/domain/subdomain1/subdomain2` を使用して、ドメイン パスを入力します。
- [ログイン] をクリックします。

これがこの Avamar サーバへの最初の接続の場合は、[Accept Server Certificate] ダイアログ ボックスが開きます。サーバ証明書の詳細を確認し、[Yes] をクリックします。

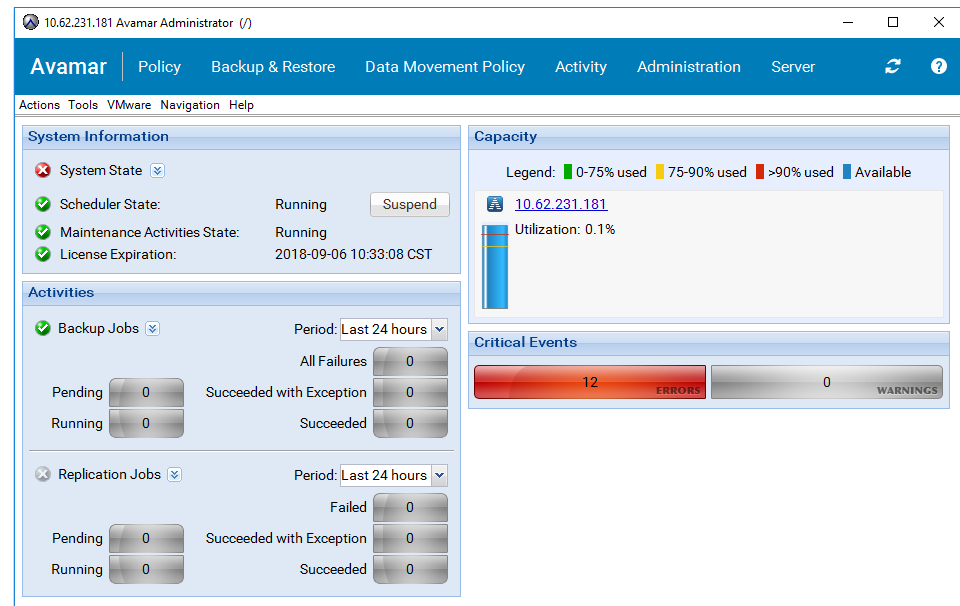
Avamar Administrator ダッシュボードが表示されます。

Avamar Administrator ダッシュボード

Avamar Administrator ダッシュボードでは、Avamar システム ステータスの概要ビューが提供されるほか、メニューや起動リンクを使用してすべての機能にアクセスすることができます。

Avamar Administrator にログインすると、ダッシュボードが表示されます。

図 5 Avamar Administrator ダッシュボード



起動リンク

ダッシュボードの起動リンクによって、永続的なウィンドウが起動され、Avamar Administrator のタスクを実行できます。

表 5 ダッシュボード起動リンク

ボタン	ウィンドウ	ウィンドウで使用できるタスク
Policy	Policy	グループ、データセット、スケジュール、保存ポリシーを作成および管理する。
Backup & Restore	Backup, Restore, and Manage	オン デマンド バックアップおよびリストアを実行し、完了したバックアップを管理する。
データ移動ポリシー	データ移動ポリシー	ポリシー ベースのレプリケーションおよびクラウド階層を構成する。
Activity	Activity	バックアップ、リストア、バックアップの検証、レプリケーション アクティビティを監視する。
Administration	Administration	ドメイン、クライアント、ユーザー、システム イベント、サービスを作成および管理する。
Server	Server	サーバー アクティビティとクライアント セッションを監視する。

[System Information] パネル

Avamar Administrator ダッシュボードにある **[System Information]** パネルでは、重要なシステム統計の概要が表示されます。

System State

[System State] アイコンは、全体的なシステムのステータスを示すステータス インジケータとして、次のように機能します。

- 緑色のチェックマークのアイコンは、システムがフル稼働していることを示します。
- 黄色の注意アイコンは、対応の必要な問題がシステムで発生していますが、バックアップは継続できることを示します。
- 赤色の x アイコンは、直ちに対応が必要な問題がシステムで発生していることを示します。この問題が解決されるまで、バックアップは実行できません。

システム状態の詳細情報が表示するには、**[System State]** フィールドの横にある矢印アイコンをクリックします。次の表は、ダッシュボードのシステム状態情報に関する詳細を提供します。

表 6 Avamar Administrator ダッシュボード上の **[System State]** のフィールド

フィールド	説明
[Avamar State]	<p>Avamar サーバの現在の動作状態を次のように要約します。</p> <ul style="list-style-type: none"> • 緑色のチェック マークは、Avamar サーバがフル稼働していることを示します。 • 黄色の注意アイコンは、対応の必要な 1 個以上の問題が Avamar サーバで発生していますが、バックアップは継続できることを示します。 • 赤色の x アイコンは、Avamar サーバが [Inactive]、[Offline]、[Degraded]、[Unknown] のいずれかの動作状態にあることを示します。
[Capacity State]	<p>システム容量の使用状況と稼働状態を次のように要約します。</p> <ul style="list-style-type: none"> • 緑色のチェック マークは、システムの使用率が合計ストレージ容量の 75%を超えていることを示します。 • 黄色の注意アイコンは、システムの使用量が合計ストレージ容量の 75%を超えているが 90%未満であることを示します。新しく容量を追加するか、過去のバックアップを削除することを検討してください。 • 赤色の x アイコンは、合計ストレージ容量の 90%超をシステムが使用していることを示します。容量を追加するか、古いバックアップを削除するまで、新しいバックアップは実行されません。
[Critical Events]	未確認のシステム イベントを次のように要約します。

表 6 Avamar Administrator ダッシュボード上の [System State] のフィールド (続き)

フィールド	説明
	<ul style="list-style-type: none"> • 緑色のチェック マークは、確認を必要とする重要なシステム イベントがないことを示します。 • 黄色の注意アイコンは、1 個以上の警告イベントについて、確認が必要であることを示します。 • 赤色の × アイコンは、1 個以上のシステム エラーイベントについて、確認が必要であることを示します。
[Last Checkpoint]	<p>前回のチェックポイントが実行されてからの経過時間を次のように示します。</p> <ul style="list-style-type: none"> • 緑色のチェック マークは、過去 24 時間以内に、この Avamar サーバでチェックポイントが正常に完了したことを示します。 • 黄色の注意アイコンは、24～48 時間前に、この Avamar サーバでチェックポイントが正常に完了したことを示します。 • 赤色の × アイコンは、この Avamar サーバでチェックポイントが正常に完了してから、48 時間超が経過したことを示します。
[Last Validated Checkpoint]	<p>前回のチェックポイントの検証が実行されてからの経過時間を次のように示します。</p> <ul style="list-style-type: none"> • 緑色のチェック マークは、過去 48 時間以内に、この Avamar サーバでチェックポイントの検証が正常に完了したことを示します。 • 黄色の注意アイコンは、48～72 時間前に、この Avamar サーバでチェックポイントの検証が正常に完了したことを示します。 • 赤色の × アイコンは、この Avamar サーバでチェックポイントの検証が正常に完了してから、72 時間超が経過したことを示します。
[Last Garbage Collection]	<p>前回のガベージ コレクションが実行されてからの経過時間を次のように示します。</p> <ul style="list-style-type: none"> • 緑色のチェック マークは、過去 30 時間以内に、この Avamar サーバでガベージ コレクションが正常に完了したことを示します。 • 黄色の注意アイコンは、過去 30 時間以内に、この Avamar サーバでガベージ コレクションが正常に完了していないことを示します。 • 赤色の × アイコンは、前回ガベージ コレクションを実行した際に、エラーが発生したことを示します。

表 6 Avamar Administrator ダッシュボード上の [System State] のフィールド (続き)

フィールド	説明
[Data Domain System(s) State]	<p>この Avamar サーバに追加されたすべての Data Domain システムの動作状態を、次のように要約します。</p> <ul style="list-style-type: none"> • 緑色のチェック マークは、すべての Data Domain システムがフル稼働していることを示します。 • 黄色の注意アイコンは、対応の必要な 1 個以上の問題が Data Domain システムで発生していることを示します。ただし、バックアップは継続できます。 • 赤色の × アイコンは、直ちに対応が必要な 1 個以上の問題が Data Domain システムで発生していることを示します。バックアップは、すべての問題が解決するまで実行されません。

Scheduler State

[Scheduler State] フィールドは、スケジュール設定されたアクティビティが実行中であるか、一時停止中であるかを示します。スケジュール設定されたアクティビティには、バックアップ、メール通知、レプリケーションが含まれます。スケジュール設定されたアクティビティが実行中の場合は、スケジュール設定された時間にアクティビティが実行されます。スケジュール設定されたアクティビティが一時停止中の場合は、このアクティビティを再開するまで、アクティビティは実行されません。

スケジュール設定されたアクティビティの一時停止または再開を実行するには、[Suspend] または [Resume] をクリックします。

Maintenance Activities State

[Maintenance Activities State] フィールドでは、メンテナンス アクティビティが実行中であるか、一時停止中であるかを示します。メンテナンス アクティビティには、チェックポイント、チェックポイントの検証、ガベージ コレクションなどが含まれます。メンテナンス アクティビティが実行中の場合は、スケジュール設定された時間にアクティビティが実行されます。メンテナンス アクティビティが一時停止中の場合は、[Server] ウィンドウでこのアクティビティを再開するまで、アクティビティは実行されません。

License Expiration

[License Expiration] フィールドでは、Avamar サーバのライセンスの有効期限が切れるカレンダー 1 日付を表示します。

[Activities] パネル

Avamar Administrator ダッシュボードにある [Activities] パネルでは、バックアップおよびレプリケーション ジョブのステータスと詳細情報が表示されます。

バックアップ ジョブ

[Activities] パネルのバックアップ ジョブに使用される主なステータス アイコンにより、スケジュール設定されたバックアップがスケジュールどおりの時間に実行されるかどうか、またスケジュール設定されたバックアップの実行を妨げる問題が発生していないかが分かります。

ステータスの詳細情報が表示するには、[Backup Jobs] フィールドの横にある矢印ボタンをクリックします。次の表では、バックアップ ジョブで使用されるステータス情報に関する詳細を説明します。

表 7 AvamarAdministrator ダッシュボードの [Backup Jobs] フィールド

フィールド	説明
[Scheduler State]	バックアップ、メール通知、レプリケーションなどのアクティビティに設定したスケジュールが実行中であるか、一時停止されているかを示します。
[Dispatcher State]	ディスパッチャーが実行中であるか、一時停止されているかを示します。ディスパッチャーが一時停止している場合は、Avamar サーバがヘルス チェック制限に達しており、バックアップを実行できません。詳細については、 容量の制限と閾値 (260 ページ) を参照してください。
[Backup Groups Enabled]	有効化されたバックアップ グループ数を示します。 [Policy] ウィンドウが開き、グループを管理するには、フィールドの右にあるウィンドウ アイコンをクリックします。

また、次の状態にあるバックアップ ジョブの合計数も確認できます。

- ペンディング中。
- 現在実行中。
- 指定した期間内で失敗。
- 指定した期間内に例外つきで成功。
- 指定した期間内で成功。

完了したバックアップの結果を示す期間を制御するには、[Period] リストで値を選択します。

[Activity Monitor] でバックアップ ジョブの詳細情報を表示するには、数を示すボタンをクリックします。

レプリケーション ジョブ

[Activities] パネルのレプリケーション ジョブに使用される主なステータス アイコンでは、レプリケーション ジョブが実行されるかどうかを、次のように示します。

- 緑色のチェック マークのアイコンは、スケジュール設定されたレプリケーション ジョブがスケジュールどおりの時間に実行されることを示します。
- 黄色の注意アイコンは、1 個以上のレプリケーション グループが無効化されていることを示します。
- 赤色の x アイコンは、スケジュール設定されたレプリケーション ジョブがブロックされることを示します。このブロックの原因としては、スケジューラが中断状態になっているか、すべてのレプリケーション グループが無効化されているか、またはシステムに関するその他の問題が発生していることが考えられます。

[Replication] ウィンドウでレプリケーション グループを構成するには、このアイコンの右にあるウィンドウ アイコンをクリックし、します。

また、次の状態にあるレプリケーション ジョブの合計数も確認できます。

- ペンディング中。
- 現在実行中。
- 指定した期間内で失敗。
- 指定した期間内に例外つきで成功。

- 指定した期間内で成功。

完了したレプリケーション ジョブの結果を示す期間を制御するには、**[Period]** リストで値を選択します。

[Replication Report] でレプリケーション ジョブの詳細情報を表示するには、数を示すボタンをクリックします。

[Capacity] パネル

Avamar Administrator ダッシュボードにある **[Capacity]** パネルでは、Avamar サーバおよび追加されたすべての Data Domain システムに関する、システム容量の使用状況が提供されます。

Avamar サーバの容量情報

Avamar サーバの容量の使用状況は、合計容量の割合 (%) に基づいて、使用レベルを示す色付きのインジケータとともに垂直バーとして表示されます。テキストフィールドには、使用済み容量の割合が一覧表示されます。

Avamar のシステム構成に Data Domain システムが含まれる場合は、Avamar サーバの容量計算に Data Domain システムのメタデータの使用状況も含まれます。

Avamar サーバ名のリンクをクリックすると、**[Server Monitor]** に詳細なシステム情報が表示され、該当する場合は Data Domain メタデータの使用率も表示されます。

Data Domain システムの容量情報

構成済みの各 Data Domain システムが、**[Capacity]** パネルに個別に表示されます。

Data Domain システムの容量の使用状況は、合計容量の割合 (%) に基づいて、使用レベルを示す色付きのインジケータとともに垂直バーとして表示されます。

テキストフィールドには、Data Domain システムの合計容量がギビバイト (GiB) 単位で表示されるほか、使用済み容量の割合 (%) と値 (GiB)、利用可能な合計容量 (GiB) を確認できます。

システムの Data Domain Enterprise Manager Web ページを表示するには、Data Domain システム名のリンクをクリックします。

[Critical Events] パネル

Avamar Administrator ダッシュボードにある **[Critical Events]** パネルでは、未確認の重大なシステム エラーおよび警告の発生数のほか、定義された特定のシステム アラートが表示されます。

これらの重大なシステム エラーおよび警告をクリアする (つまり、カウントを 0 にリセットする) には、明示的にこれらを確認する必要があります。詳細については、[システム イベントの確認](#) (237 ページ) を参照してください。

次の表では、**[Critical Events]** パネルに表示される可能性のあるシステム アラートを挙げています。

表 8 [Critical Events] パネルのシステム アラート

アラートのタイプ	説明
HFS チェックの失敗	前回のチェックポイントの検証が失敗した場合、データの整合性アラートが生成されます。できる限り早急に、この問題を調査し、対処してください。詳細については、 チェックポイントの作成 (191 ページ) を参照してください。

表 8 [Critical Events] パネルのシステム アラート (続き)

アラートのタイプ	説明
容量の警告	これらのアラートは、システムがクリティカルなシステムストレージ使用容量の閾値に近づいていることを警告します。
容量の使用状況の警告	これらのアラートは、システムがクリティカルなシステムストレージ容量予測の閾値に近づいていることを警告します。

Avamar Administrator ユーザー インターフェイスの構成要素

Avamar Administrator ユーザー インターフェイスのすべての主要なウィンドウで、ステータス バー、ナビゲーション ツリー機能、マウスでの操作をはじめとする、共通した複数の構成要素および機能が共有されています。

ステータス バー

各 Avamar Administrator の固定ウィンドウの下にあるステータス バーでは、ステータス情報が表示され、特定の機能へのシングル クリックによるショートカットを提供します。

図 6 Avamar Administrator ステータス バー



起動ショートカット

ステータス バーの左側に表示されているショートカット アイコンでは、Avamar Administrator の 6 つの主要ウィンドウへのショートカットが提供されます。

次の表では、ステータス バーで利用できるショートカット アイコンを挙げています。

表 9 ステータス バーの起動ショートカット アイコン

ボタン	ウィンドウ	ウィンドウで使用できるタスク
Policy	Policy	グループ、データセット、スケジュール、保存ポリシーを作成および管理する。
Backup & Restore	Backup, Restore, and Manage	オン デマンド バックアップおよびリストアを実行し、完了したバックアップを管理する。
データ移動ポリシー	データ移動ポリシー	ポリシー ベースのレプリケーションおよびクラウド階層を構成する。
Activity	Activity	バックアップ、リストア、バックアップの検証、レプリケーション アクティビティを監視する。
Administration	Administration	ドメイン、クライアント、ユーザー、システム イベント、サービスを作成および管理する。
Server	Server	サーバー アクティビティとクライアント セッションを監視する。

ステータス メッセージ

ステータス バーの右側には、スケジューラおよびバックアップ ディスパッチ、未確認イベント、Avamar サーバおよび Data Domain システムのステータス メッセージが表示されます。

スケジューラおよびバックアップ ディスパッチのステータス

スケジューラはスケジュール設定されたバックアップの実行をコントロールします。バックアップ ディスパッチ ステータスは、ヘルス チェック制限に到達したかどうかに基づいてバックアップが実行されるかどうかを示します。次の表は、使用可能なステータス メッセージを示しています。

表 10 スケジューラおよびバックアップ ディスパッチのステータス メッセージ

ステータス メッセージ	説明
Sch/Disp: Running/Running	バックアップはスケジュール設定された時間に実行します。スケジュール設定されたバックアップが有効になり、ヘルス チェック制限には到達していません。
Sch/Disp: Running/Suspended	スケジュール設定されたバックアップが有効になっていたとしても、ヘルス チェック制限に到達しているため、バックアップはスケジュール設定された時間に実行しません。システム容量問題を解決し、システム イベントを確認してバックアップを再開します。詳細は、 容量管理 (259 ページ) および システム イベントの確認 (237 ページ) を参照してください。
Sch/Disp: Suspended/Running	ヘルス チェック制限に到達していても、スケジュール設定されたバックアップが無効になっているため、バックアップはスケジュール設定された時間に実行しません。スケジュール設定された動作の再開時にバックアップを再開できます。
Sch/Disp: Suspended/Suspended	スケジュール設定されたバックアップが無効になっており、またヘルス チェック制限に到達しているため、バックアップはスケジュール設定された時間に実行しません。スケジューラを再度有効化する詳細については、 スケジュールされた操作の一時停止と再開 (182 ページ) スケジュールされた操作の一時停止と再開 (182 ページ) を参照してください。システム容量問題の解決と、システム イベントを確認してスケジュール設定バックアップを再開するための詳細については、 容量管理 (259 ページ) と システム イベントの確認 (237 ページ) を参照してください。

Unacknowledged Events

発生するたびに、Avamar サーバ管理者による確認応答を必要とする特定のシステム イベント。次の表は、使用可能なステータス メッセージを示しています。

表 11 未確認イベントに対するステータス メッセージ

ステータス メッセージ	説明
Have Unacknowledged Events	Unacknowledged Events リスト内に、Avamar サーバ管理者が明示的に確認する必要があるエントリが存在します。[Unacknowledged

表 11 未確認イベントに対するステータス メッセージ (続き)

ステータス メッセージ	説明
	Events ステータス アイコン、またはテキスト ラベルをクリックすると、 [Administration] ウィンドウの [Unacknowledged Events] パネル (タブ) が表示されます。詳細については、 システム イベントの確認 (237 ページ) を参照してください。
No Unacknowledged Events	Unacknowledged Events リスト内にエントリーは存在しません。

Avamar サーバおよび Data Domain システム ステータス

このアイコンは、Avamar サーバ、または構成済み Data Domain システムの動作ステータスを示します。次の表は、使用可能なステータス メッセージを示しています。

表 12 Avamar または Data Domain の動作ステータス メッセージ

ステータス メッセージ	説明
Server: Full Access	Avamar サーバの通常の動作状態。すべての操作が可能です。
Server: Admin	Avamar サーバが管理状態であり、Avamar サーバ ユーザーと root ユーザーがデータの読み取り/書き込みが可能です。他のユーザーは、データの読み取りのみ可能です。
Server: Admin Only	Avamar サーバが管理状態であり、Avamar サーバ ユーザーまたは root ユーザーがデータの読み取り/書き込みが可能です。他のユーザーは、アクセスすることができません。
Server: Admin Read Only	Avamar サーバが管理読み取り専用状態で、Avamar サーバ ユーザーまたは root ユーザーがデータの読み取りが可能です。他のユーザーは、アクセスすることができません。
Server: Degraded	Avamar サーバの 1 台、または複数のノードでディスク障害が発生しています。操作は可能ですが、すみやかに問題を修復する必要があります。
Server: Inactive	Avamar Administrator は、Avamar サーバと通信できませんでした。
Server: Node Offline	1 つ以上の Avamar サーバ ノードがオフライン状態です。
Server: Read Only	Avamar サーバが読み取り専用管理状態であり、すべてのユーザーはデータの読み取りが可能です。データの書き込みは許可されません。
Server: Suspended	Avamar Administrator と Avamar サーバは通信可能ですが、通常の操作は一時的に停止されています。

表 12 Avamar または Data Domain の動作ステータス メッセージ (続き)

ステータス メッセージ	説明
Server: Synchronizing	Avamar サーバは移行状態です。起動時や保守の際の短時間に、サーバがこの状態になるのは正常です。
Server: Unknown State	Avamar Administrator は、Avamar サーバの状態を判別できませんでした。
Data Domain System Unresponsive	Avamar は Data Domain システムに接続できますが、接続に関する問題が存在します。
DD System: Inactive	Avamar は、Data Domain システムに接続できません。

Avamar サーバのアクティビティを一時停止または再開するには、[**Server status**] アイコンまたはテキストラベルをクリックして、[**Avamar Server**] ウィンドウの [**Session Monitor**] タブを表示します。そこから、[**Actions**] > [**Resume Backups/Restores**] または [**Actions**] > [**Suspend Backups/Restores**] をそれぞれ選択して、サーバのアクティビティを再開または一時停止します。

Data Domain システムのステータスに関する追加の詳細を表示するには、[**Navigation**] > [**Server**] をクリックして、[**Server**] ウィンドウを開きます。[**Server Management**] タブを選択し、次にツリーで Data Domain システムを選択します。Data Domain システムの [**Monitoring Status**] が右のパネルに表示されます。表示される詳しいステータスメッセージの詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。

ナビゲーション ツリーの機能

[**Administration**]、[**Backup, Restore and Manage**]、[**Data Movement Policy**] の各ウィンドウのナビゲーション ツリーでは、1 つ以上のクライアントの場所を容易に見つけるためにいくつかのコントロールを提供します。

図 7 ナビゲーション ツリーの機能



上側のパネルは Avamar サーバのドメイン構造を表示します。下側のパネルは上側のパネルで選択されたドメインの内容を表示します。2つのパネルの間にあるフィルター フィールドの左側の分割パネル アイコンをクリックして、2つのパネルを水平方向ではなく、垂直方向に分割できます。

サブフォルダーのすべてのクライアントを表示するには、フィルター フィールドの左側にある、二重になったフォルダー アイコンをクリックします。

フィルター フィールドで1文字以上を入力すると、リストがフィルターされ、この文字を含む名前のクライアントのみが表示されます。

マウスでの操作

Avamar Administrator ユーザー インターフェイスでは、コンテキスト依存の左クリック、右クリック、ダブル クリックの操作をサポートしています。

右クリック

クリックで機能が実行されるすべての GUI 要素では、右クリックも使用できます。ただし、ナビゲーション機能だけを提供する GUI 要素の場合、右クリックは使用できません。例えば、[Policy] ウィンドウのクライアント ツリーでは右クリックでショートカット メニューが表示されます。これは、選択しているツリーのノードによって使用可能な機能が異なるためです。

ダブル クリック

プロパティ ダイアログ ボックスまたは編集ダイアログ ボックスを呼び出すことができるすべての表では、表の行をダブル クリックすると、プロパティ ダイアログ ボックスまたは編集ダイアログ ボックスが表示されます。また、リストを使用する場合は、そのリストの任意の要素をダブル クリックすると、編集ダイアログ ボックスが表示されます。

列見出しのソート

列をソートするには、テーブルの列見出しをクリックします。例えば、[Activity Monitor] の [State] 列をダブル クリックすると、[Activity Monitor] の表示内容が各バックアップの状態ですべてソートされます。

[Shift] キーを押しながら表の列見出しをクリックすると、表の列の値が逆ソートされます。

第3章

Avamar Web ユーザー インターフェイス

本章は、次のトピックで構成されています。

- [AUI の概要](#) 54
- [AUI へのアクセス](#)..... 54
- [AUI ナビゲーション ペイン](#)..... 55
- [基本管理タスク](#)..... 56
- [ナビゲーション ツリーの機能](#)..... 57
- [AUI ダッシュボード](#)..... 57
- [AUI アクティビティ モニター](#)..... 62

AUI の概要

Avamar Web ユーザー インターフェイスは、Avamar サーバーの管理に使用される Web 管理アプリケーションです。

AUI を使用して、Avamar サーバーを監視および構成できます。AUI を使用すると、バックアップ、リストア処理、システム メンテナンスといったアクティビティを監視できるほか、バックアップ ポリシーの構成、クライアントおよびユーザー アカウントの管理、他のシステム設定の構成を実行できます。

AUI から管理できる Avamar サーバーは一度に 1 つのみです。

Avamar にログインすると、AUI ダッシュボードが表示されます。ダッシュボードでは、Avamar システム ステータスの概要ビューが表示されます。ナビゲーション ペインでは、すべての機能にアクセスできます。

注

Avamar AUI は、スタンドアロン環境でのみサポートされます。

AUI へのアクセス

Web ブラウザーで Avamar Web ユーザー インターフェイスにアクセスします。

手順

1. Web ブラウザーを開き、次の URL を入力します。

```
https://Avamar_server/au
```

ここで、Avamar_server は Avamar サーバーの DNS 名または IP アドレスです。

注

お使いの環境が HTTPS 証明書の検証要件を満たしていない場合は、証明書の検証は失敗し、パッケージのダウンロードを続行するかどうかの確認を求めるエラー メッセージが表示されます。証明書の検証を無視すると、セキュリティの問題が発生する可能性があります。

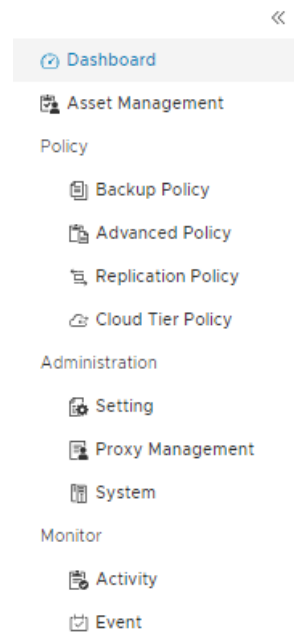
2. [**Avamar Username**] フィールドに、root または管理者権限を持つユーザー名を入力します。
3. [**Avamar Password**] フィールドに、この root または管理者ユーザーのパスワードを入力します。
4. [**Avamar Domain**] フィールドで、ログインする Avamar ドメインを入力します。
 - root ドメインでは、シングル スラッシュ (/) を入力するとデフォルトが使用されます。
 - 特定のドメインまたはサブドメインでは、構文/domain/subdomain1/subdomain2 を使用して、ドメイン パスを入力します。
5. [ログイン] をクリックします。
AUI ダッシュボードが表示されます。
6. UI の任意の場所からナビゲーション ペインを開くには、[>>] をクリックします。
ナビゲーション ペインが開き、使用可能なメニュー アイテムが表示されます。

AUI ナビゲーション ペイン

左側のナビゲーション ペインを使用して、UI のさまざまなパネルをすばやく参照できます。ナビゲーション ペインには、Avamar Web ユーザー インターフェイスのタスクを実行するための他のパネルを開くリンクが表示されます。

UI の任意の場所からナビゲーション ペインを開くには、[>>] をクリックします。ナビゲーション ペインが開き、次の図に示すように、使用可能なメニュー アイテムが表示されます。

図 8 AUI ナビゲーション ペイン











UI の別の場所を参照するには、ナビゲーション ペインのリンクをクリックします。このアクションにより、メイン ウィンドウでメニュー アイテムが開きます。

このリンクから、AUI の次の機能にアクセスできます。

表 13 AUI ナビゲーション ペイン

ナビゲーション リンク	アイコン	使用可能な機能
Dashboard		Avamar システム ステータスの概要ビューが表示されます。
Asset Management		Avamar ドメインおよびクライアント関連の操作を管理する機能を提供します。 <ul style="list-style-type: none"> Avamar ドメインの作成、編集、削除、更新。 Avamar サーバーのクライアントの追加、編集、削除、同期。 クライアントのバックアップおよびリストア。
Backup Policy		バックアップを自動化してユーザー コミュニティーのセグメント (グループ) 全体に一貫したルールとシステム動作を適用します。パッ


表 13 AUI ナビゲーション ペイン (続き)




ナビゲーションリンク	アイコン	使用可能な機能
		クアアップ ポリシーはデータセット、スケジュール、保存ポリシーで構成されます。バックアップ ポリシーは、そのバックアップ ポリシーのすべてのメンバーのバックアップ動作を制御します。
Advanced Policy		自動 SQL 検出、自動バックアップ グループ管理、自動クライアント SQL プラグ イン インストール/登録など、Cloud DR 対応バックアップとアプリケーション コンシステントな SQL 仮想マシンのバックアップを管理します。
Replication Policy		ソース Avamar システムから代替ターゲットにクライアント バックアップをコピーします。バックアップを代替ターゲットにレプリケーションすることにより、ソース Avamar システムに障害が発生した場合にデータロスから保護します。
Cloud Tier Policy		Avamar バックアップを Data Domain からクラウドに移動し、これらのバックアップのシームレスなリカバリを実行します。
Settings		管理者がシステムにアカウントを追加したり、スケジュール、データセット、保存ポリシー、ルールを作成および管理したりできるよう支援します。
Proxy Management		各 vCenter で導入する必要があるプロキシ数についての推奨事項と、プロキシごとに推奨される ESX ホストの場所を提供することにより、管理者が Avamar プロキシを導入および管理できるよう支援します。
System		管理者が vCenter から Avamar への認証の構成、vSphere Web Client 用の Avamar プラグ インの登録、Avamar への Data Domain システムの追加を行えるように支援します。
Activity		バックアップおよびレプリケーション ジョブについてのステータスと詳細な情報を提供します。
Event		動作ステータスとサーバー アクティビティを監視します。Avamar イベントの例としては、クライアントの登録や起動、バックアップの成功と失敗、ハード ディスクのステータスがあります。

基本管理タスク

Avamar Web ユーザー インターフェイスのログアウト、オンライン ヘルプへのアクセス、製品情報の表示、スケジュール設定されたアクティビティの一時停止または実行が可能です。

手順

1. AUI をログアウトするには、次のようにします。
 - a. AUI ヘッダー パネルで、 をクリックします。
確認のメッセージが表示されます。
 - b. [YES] をクリックします。
AUI からログアウトしました。


2. AUI オンライン ヘルプにアクセスするには、次のようにします。
 - a. AUI ヘッダー パネルで、 をクリックします。
 - b. **[Help]** をクリックします。
3. バージョンとビルドの詳細を表示するには、次のようにします。
 - a. AUI ヘッダー パネルで、 をクリックします。
 - b. **[About]** をクリックします。
4. スケジュール設定されたアクティビティを一時停止または実行するには、次のようにします。
 - a. AUI ヘッダー パネルで、 をクリックします。
 - b. **[Scheduler State]** スイッチを切り替えます。

[Scheduler State] は、スケジュール設定されたアクティビティが実行中であるか、一時停止中であるかを示します。スケジュール設定されたアクティビティには、バックアップ、メール通知、レプリケーションが含まれます。スケジュール設定されたアクティビティが実行中の場合は、スケジュール設定された時間にアクティビティが実行されます。スケジュール設定されたアクティビティが一時停止中の場合は、このアクティビティを再開するまで、アクティビティは実行されません。

ナビゲーション ツリーの機能

[Asset Management]、**[Backup Policy]**、**[Advanced Policy]**、**[Setting]** ウィンドウのナビゲーション ツリーには、1 つ以上のクライアントの場所を容易に見つけるためのコントロールが用意されています。

[Domain] パネルは Avamar サーバーのドメイン構造を表示します。

サブフォルダー内のすべてのクライアントを表示するには、ナビゲーションツリーで、 をクリックしてドメイン フォルダーを展開します。

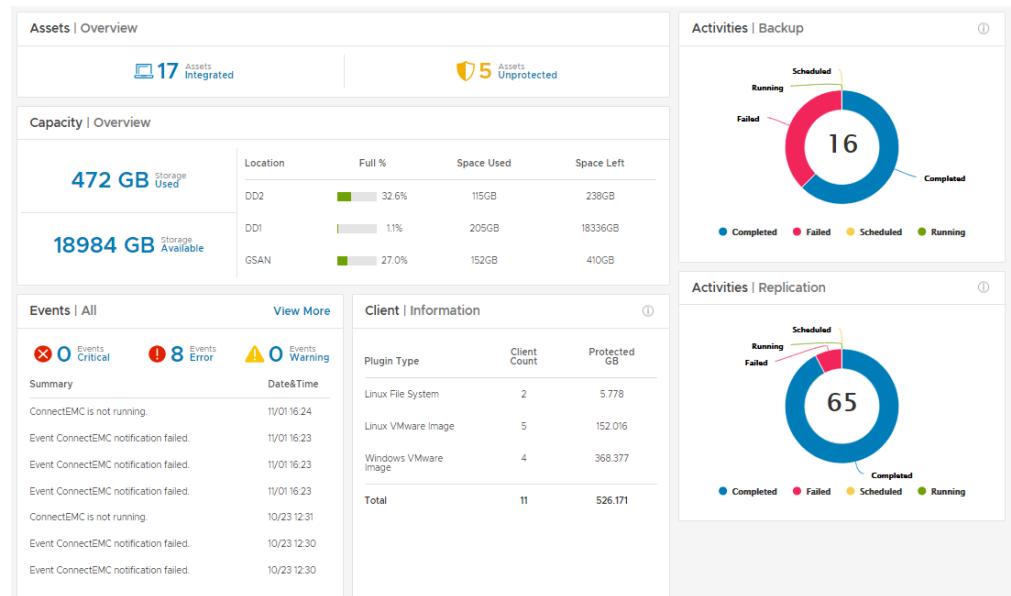
AUI ダッシュボード

Avamar Web ユーザー インターフェイスダッシュボードでは、Avamar システム ステータスの概要ビューが表示されます。

ダッシュボードは、AUI にログインしたときに表示され、サマリー情報を表示する各セクションに分かれています。

次の図に、ダッシュボード ビューを示します。

図 9 AUI ダッシュボード



AUI ダッシュボードには以下の情報が表示されます。

- Avamar サーバーの統合された資産と保護されていない資産
- Avamar サーバーまたは Data Domain システムのシステム容量使用量
- イベント
- クライアント情報
- バックアップ アクティビティのステータス
- レプリケーション アクティビティのステータス

ダッシュボードでの資産の監視

[**Assets | Overview**] パネルは、Avamar サーバーの統合された資産と保護されていない資産の数を示します。

- [Integrated] は、Avamar サーバーに統合されているクライアントの数を示します。
- [Unprotected] は、バックアップがないクライアントの数を示します。

注

クライアントのバックアップ ジョブを実行すると、Avamar サーバーによってこの値が更新されます。

ナビゲーション ペインで [**Asset Management**] を選択することで、AUI から資産を管理できます。

統合クライアントの表示

AUI ダッシュボードの [**Assets | Overview**] パネルには、Avamar サーバーに統合されているクライアントの数が表示されます。

手順

1. 統合されたクライアントに関する情報を表示するには、[**Integrated**] の横にあるアイコンをクリックします。




[**Asset Management**] パネルが表示されます。

- ドメイン ツリーでドメインまたはサブドメインを選択します。

中央のパネルに表示されるクライアントのリストは、ステータスなどのクライアント情報を示します。

結果

[**Asset Management**] ペインの上部には、次のようなクライアント ドメインに関する情報が表示されます。

アイコン	説明
 Clients	ドメイン内のクライアントの数を示します。
 Activities	ドメイン内のクライアントによって開始されたアクティビティ（バックアップ ジョブとレプリケーション ジョブ）の数を示します。
 Policies	ドメイン内のクライアントに適用されるポリシーの数を示します。

保護されていないクライアントの表示

AUI ダッシュボードの [**Assets | Overview**] パネルには、バックアップが存在しない、保護されていないクライアントの数が表示されます。

手順

- 保護されていないクライアントに関する情報を表示するには、[**Unprotected**] の横にあるアイコンをクリックします。

[**Clients with no backups**] ウィンドウが開き、各クライアントのサマリー情報が表示されます。

- クライアントのプロパティを確認します。

プロパティ	説明
Name	内容を説明するクライアント名。
Domain	クライアントの Avamar ドメイン。
Enabled	Avamar がクライアントのバックアップを実行できるかどうかを示します。この設定にかかわらず、以前のバックアップがシステム上に存在している限り、クライアントはファイルをリストアできます。
Activated	クライアントが Avamar サーバーでアクティブ化されるかどうかを示します。
Client type	クライアントのタイプ（通常、仮想マシン、イメージ プロキシ、VMware vCenter など）。

ダッシュボードでのシステム容量の監視

[**Capacity | Overview**] パネルは、Avamar サーバーおよび追加されたすべての Data Domain システムに関するシステム容量の使用状況が提供されます。

Avamar サーバの容量情報

[**Capacity | Overview**] パネルは、Avamar サーバで使用可能なストレージと使用済みストレージの容量をギガバイト (GB) で示します。また、横棒は使用済みストレージの合計の割合を示します。

Avamar のシステム構成に Data Domain システムが含まれる場合は、Avamar サーバの容量計算に Data Domain システムのメタデータの使用状況も含まれます。

Data Domain システムの容量情報

構成済みの各 Data Domain システムが、[**Capacity | Overview**] パネルに個別に表示されません。

[**Capacity | Overview**] パネルは、Data Domain システムで使用可能なストレージと使用済みストレージの容量を GB で示します。また、横棒は使用済みストレージの合計の割合を示します。

ダッシュボードでのイベントの表示

[**Events | All**] パネルは、発生した未確認の重大なシステム エラーと警告に加え、定義済みの特定のシステム アラートを表示します。

イベントは、名前、発生した日付と時刻とともにリストに表示されます。

重大度でイベントをフィルタリングするには、次のいずれかのオプションをクリックします。

- [**Critical**]
- [**Error**]
- [**Warning**]

[**Event Management**] パネルが表示され、選択した重大度に基づいて結果がフィルタリングされます。

すべてのイベントを表示するには、[**View More**] をクリックします。[**Event Management**] ペインに、すべてのイベントのリストが表示されます。

これらの重大なシステム エラーおよび警告をクリアする（つまり、カウントを 0 にリセットする）には、明示的にこれらを確認する必要があります。[**Event Management**] パネルからイベントを確認することができます。

次の表に、[**Events | All**] パネルに表示される可能性のあるシステム アラートを示します。

表 14 システム アラート

アラートのタイプ	説明
HFS チェックの失敗	前回のチェックポイントの検証が失敗した場合、データの整合性アラートが生成されます。できる限り早急に、この問題を調査し、対処してください。
容量の警告	これらのアラートは、システムがクリティカルなシステムストレージ使用容量の閾値に近づいていることを警告します。
容量の使用状況の警告	これらのアラートは、システムがクリティカルなシステムストレージ容量予測の閾値に近づいていることを警告します。

ダッシュボードでのバックアップ ジョブの監視

バックアップ ジョブは、オン デマンド バックアップまたは継続的に実行されるようにスケジュール設定されたバックアップです。バックアップ ポリシーは、Avamar Web ユーザー インターフェイスからナビゲーション ペインで **[Backup Policy]** を選択することで構成できます。

[Activities | Backup] パネルは、スケジュール設定されたバックアップがスケジュール設定された時間に行われるかどうか、またはバックアップが実行されない問題があるかを示します。

- 青色は、正常に完了したバックアップ ジョブを示します。
- 緑色は、進行中のスケジュール バックアップ ジョブを示します。
- 黄色は、スケジュール設定されているがまだ開始されていないバックアップ ジョブを示します。
- 赤色は、正常に完了しなかった、またはエラーありで完了したバックアップ ジョブを示します。

注

[Activities | Backup] パネルには過去 24 時間以内のバックアップのみが表示されます。Avamar MCS (Management Console Server) を再起動すると、この値はリセットされます。

ダッシュボードでのレプリケーション ジョブの監視

レプリケーション ジョブは、ソース Avamar システムから別のターゲット デスティネーション (Data Domain システムなど) にクライアント バックアップをコピーします。レプリケーションの目的は、ソース Avamar サーバーに障害が発生した場合にデータロスから保護することです。レプリケーション ジョブは、Avamar Web ユーザー インターフェイスからナビゲーション ペインで **[Replication Policy]** を選択することによって構成します。

[Activities | Replication] パネルは、レプリケーションを使用して構成されたグループの現在のバックアップ ステータスを示します。

- 青色は、正常に完了したレプリケーション ジョブを示します。
- 緑色は、進行中のスケジュール設定されたレプリケーション ジョブを示します。
- 黄色は、スケジュール設定されているがまだ開始されていないレプリケーション ジョブを示します。
- 赤色は、正常に完了しなかった、またはエラーありで完了したレプリケーション ジョブを示します。

注

[Activities | Replication] パネルには過去 24 時間以内のレプリケーション ジョブのみが表示されます。Avamar MCS (Management Console Server) を再起動すると、この値はリセットされます。

クライアント情報の表示


[Client | Information] パネルは、プラグ イン タイプ、合計クライアント数、合計保護容量 (GB) など、Avamar クライアントの詳細を表示します。

- プラグ イン タイプは、クライアントが使用する最も頻繁に使用されるプラグ インの上位 10 位を示します。
- 合計クライアント数は、特定のプラグ インを使用しているクライアントの数を示します。
- 合計保護容量 (GB) は、システムが各クライアントで保護するデータの合計量 (GB) を示します。

Avamar サーバーでは、このデータが 1 日 1 回更新されます。

注

Avamar クライアントの詳細を表示するには、スケジューラー サービスが実行されていることを確認します。

1. AUI ヘッダー パネルで、 をクリックします。
 2. **[Scheduler State]** スイッチを **[Running]** に切り替えます。
-

AUI アクティビティ モニター

Avamar Web ユーザー インターフェイスの **[Activity Monitor]** は、バックアップ、リストア、バックアップ検証、レプリケーションのアクティビティを監視するために使用します。クライアント セッションの詳細ログを表示して、解析またはトラブルシューティングを実行することができます。


[Activity Monitor] にアクセスするには、ナビゲーション ペインを開き、**[Activity]** をクリックします。**[Activity Monitor]** に、すべてのアクティビティのリストが表示されます。

注

AUI **[Activity Monitor]** ウィンドウは、1366 ピクセル以上の画面に合わせて最適化されています。小さな画面では、表示の問題が発生する可能性があります。AUI を正しく表示するには、ディスプレイの幅が 1366 ピクセル以上であることを確認します。

[Activity Monitor] には、表示される情報をフィルターするためのオプションが用意されています。

- アクティビティを期間別にフィルター：デフォルトでは、**[Activity Monitor]** には最新の 5000 クライアント アクティビティが表示されます。別の期間を選択するには、**[Filter activities by duration]** ドロップダウン リストで、**[Last 24 hours]** または **[Last 72 hours]** を選択します。
- ドメイン別にアクティビティをフィルター：デフォルトでは、**[Activity Monitor]** にはドメインに関係なくすべてのアクティビティが表示されます。特定のドメインのアクティビティのみを表示するには、**[Filter activities by domain]** ドロップダウン リストで、ドメインまたはサブドメインを選択します。
- ステータス別にアクティビティをフィルター：デフォルトでは、**[Activity Monitor]** にはステータスに関係なくすべてのアクティビティが表示されます。特定のステータスのアクティビティのみを表示するには、**[Activity Monitor]** の上部で、次のいずれかのオプションを選択します。
 - キャンセル済み
 - Completed
 - Completed with Exceptions (完了したが例外発生)
 - Failed
 - Running
 - Waiting

アクティビティをクライアント、開始時刻、プラグ イン、またはタイプ別にフィルターするには、それぞれの列で  をクリックします。

[Activity Monitor] には、アクティビティの開始日時と、アクティビティ中に検証された合計バイト数が表示されます。

アクティビティの詳細を表示するには、[<<<] をクリックして、[Details] パネルを展開します。

Activity Monitor の詳細

次の表では、Avamar Web ユーザー インターフェイス [Activity Monitor] で利用可能な情報を詳しく説明しています。

表 15 Activity Monitor で利用可能なセッションの詳細

フィールド	説明
Status	バックアップ、リストア、検証アクティビティのステータス。
Error Code	アクティビティが正常に完了しなかった場合、数値のエラー コードが表示されます。エラー コードをダブルクリックすると、詳細な説明が表示されます。
Start Time	このアクティビティが開始した実際の日付と時刻。括弧で括られたローカル タイムゾーンで表示します。DST (夏時間) の移行補正は自動的に行われます。
Elapsed Time	このアクティビティの経過時間。
End Time	このアクティビティが終了する日時。有効なタイムゾーン (かっこ内に表示) に調整されます。DST (夏時間) の移行補正は自動的に行われます。
Type	アクティビティのタイプ。各タイプの詳細については、Avamar Administrator のオンライン ヘルプを参照してください。
Server	アクティビティが発生した時点のサーバ。Avamar サーバまたは Data Domain システム。
Progress Bytes	このアクティビティ中に検証したバイト数の合計。
New Bytes	Avamar サーバまたは Data Domain システムにバックアップされた新しいバイト数のパーセンテージ。この値が低い場合は、重複排除のレベルが高いことを示します。

表 16 Activity Monitor で利用可能なクライアントの詳細

フィールド	説明
ID	Avamar クライアントの一意の識別子。
Client	Avamar クライアント名。
Domain	Avamar サーバ内のクライアントのフルの場所。
OS	クライアントのオペレーティング システム。
Client Release	Avamar クライアント ソフトウェア バージョン。このアクティビティが VMware イメージ バックアップまたはリストアの場合、この値はイメージ プロキシ クライアントで

表 16 Activity Monitor で利用可能なクライアントの詳細 (続き)

フィールド	説明
	実行中の Avamar クライアント ソフトウェアのバージョンになります。
Proxy	このアクティビティが VMware イメージ バックアップまたはリストアの場合、この値は仮想マシンの代わりにバックアップまたはリストアを実行するプロキシ クライアントの名前になります。その他すべてのアクティビティに対しては空白です。

表 17 Activity Monitor で利用可能なポリシーの詳細

フィールド	説明
Sched. Start Time	このアクティビティの開始をスケジュール設定した日付と時刻です。
Sched. End Time	このアクティビティの終了をスケジュール設定した日付と時刻です。
Elapsed Wait	このアクティビティがアクティビティ キューに存在した合計時間です。つまり、スケジュール設定した開始時間から実際の開始時間を差し引いた時間です。
Policy	このアクティビティを開始するグループ。以下のいずれかの値を指定します。 <ul style="list-style-type: none"> アクティビティがスケジュール設定バックアップの場合は、このスケジュール設定アクティビティが開始されたときにクライアントがメンバーだったグループです。 その他のバックアップ、リストア、および確認アクティビティに対して、[On-demand] が表示されます。 このアクティビティがスケジュール設定されたレプリケーションの場合、この値はレプリケーショングループになります。 オン デマンドレプリケーション アクティビティには [Admin On-Demand Group] と表示されます。
Plug-in	このアクティビティに使用するプラグ イン。
Retention	このバックアップに割り当てられている保存タイプ。次の値のうちの 1 つ、または複数になります。 <ul style="list-style-type: none"> [D] : 日単位 [W] : 週単位 [M] : 月単位 [Y] : 年単位 [N] : 特定の保存タイプはなし

表 17 Activity Monitor で利用可能なポリシーの詳細 (続き)

フィールド	説明
Schedule	アクティビティがスケジュール設定されたバックアップの場合、このアクティビティを開始したスケジュールが表示されます。Avamar Administrator またはクライアントで開始された他のすべてのアクティビティについて、[On-Demand] または [End User Request] がそれぞれ表示されます。
Dataset	バックアップ作成に使用されるデータセットの名前。アクティビティのタイプがレプリケーション ジョブである場合、この列には、レプリケーション先システム上でのレプリケーション元システム名、およびレプリケーション元システム上でのレプリケーション先名が表示されます。
WID	作業オーダー ID。このアクティビティのユニークな識別子。

バックアップの監視

バックアップを監視して、リストアが正常に完了したことを確認したり、問題をトラブルシューティングしたりすることができます。Avamar Web ユーザー インターフェイスの [Activity Monitor] により、バックアップに関するステータス情報を表示することができます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Activity] をクリックします。
[Activity Monitor] に、すべてのアクティビティのリストが表示されます。
2. 結果をフィルターしてバックアップ アクティビティのみを表示するには、次の手順を実行します。
 - a. [Type] 列の横にある▼をクリックします。
 - b. On-Demand Backup と入力します。
 - c. [Enter] キーを押します。

バックアップのキャンセル

バックアップは完了前であればいつでもキャンセルできます。キャンセルには、5 分以上かかる場合があります。バックアップがキャンセルよりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Activity] をクリックします。
[Activity Monitor] にアクティビティのリストが表示されます。
2. リストからバックアップを選択します。
3. [CANCEL] をクリックします。
確認ダイアログ ボックスが表示されます。
4. [YES] をクリックします。

バックアップ ジョブの再開

Avamar Web ユーザー インターフェイスの **[Activity Monitor]** で、完了または失敗したバックアップ ジョブを再開することができます。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Activity]** をクリックします。
[Activity Monitor] に、すべてのアクティビティのリストが表示されます。
2. リストからバックアップ ジョブを選択し、**[RESTART]** をクリックします。
確認ダイアログ ボックスが表示されます。
3. **[YES]** をクリックします。

詳細なクライアント セッション ログの表示

Avamar Web ユーザー インターフェイスの **[Activity Monitor]** では、クライアント セッションの詳細ログを表示して、解析またはトラブルシューティングを実行することができます。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Activity]** をクリックします。
[Activity Monitor] が開き、すべてのアクティビティのリストが表示されます。
2. リストからアクティビティを選択し、**[VIEW LOGS]** をクリックします。
[Log details] ウィンドウが表示されます。デフォルトでは、**[Activity Monitor]** に 72 時間以内のすべてのクライアント バックアップ アクティビティの詳細ログが表示されます。
3. 検索文字列に基づいてコンテンツをフィルタリングするには、**[Search]** フィールドに文字列を入力します。
4. ログ ファイルをダウンロードするには、**[Download]** をクリックします。

リストアの監視

[Activity Monitor] では、バックアップおよびリストア処理のステータス情報を監視および表示することができます。

[Activity Monitor] にアクセスするには、ナビゲーション ペインを開き、**[Activity]** をクリックします。**[Activity Monitor]** に、すべてのアクティビティのリストが表示されます。

注

AUI **[Activity Monitor]** ウィンドウは、1366 ピクセル以上の画面に合わせて最適化されています。小さな画面では、表示の問題が発生する可能性があります。AUI を正しく表示するには、ディスプレイの幅が 1366 ピクセル以上であることを確認します。

[Activity Monitor] には、表示される情報をフィルターするためのオプションが用意されています。

- アクティビティを期間別にフィルター：デフォルトでは、**[Activity Monitor]** には最新の 5000 クライアント アクティビティが表示されます。別の期間を選択するには、**[Filter activities by duration]** ドロップダウン リストで、**[Last 24 hours]** または **[Last 72 hours]** を選択します。
- ドメイン別にアクティビティをフィルター：デフォルトでは、**[Activity Monitor]** にはドメインに関係なくすべてのアクティビティが表示されます。特定のドメインのアクティビティのみを表示するに

は、[**Filter activities by domain**] ドロップダウン リストで、ドメインまたはサブドメインを選択します。

- ステータス別にアクティビティをフィルター：デフォルトでは、[**Activity Monitor**] にはステータスに関係なくすべてのアクティビティが表示されます。
特定のステータスのアクティビティのみを表示するには、[**Activity Monitor**] の上部で、次のいずれかのオプションを選択します。
 - キャンセル済み
 - Completed
 - Completed with Exceptions (完了したが例外発生)
 - Failed
 - Running
 - Waiting

アクティビティをクライアント、開始時刻、プラグ イン、またはタイプ別にフィルターするには、それぞれの列で [▼] をクリックします。

[**Activity Monitor**] には、アクティビティの開始日時と、アクティビティ中に検証された合計バイト数が表示されます。

アクティビティの詳細を表示するには、[◀◀] をクリックして、[**Details**] パネルを展開します。

リストアのキャンセル

リストアは完了前であれいつでもキャンセルできます。キャンセルには、5 分以上かかる場合があります。リストアがキャンセルの終了よりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Activity**] をクリックします。
[**Activity Monitor**] にアクティビティのリストが表示されます。
2. リストからリストアを選択します。
3. [**CANCEL**] をクリックします。
確認ダイアログ ボックスが表示されます。
4. [**YES**] をクリックします。

AUI でのレプリケーションの監視

AUI の [**Activity**] ウィンドウにより、オン デマンドレプリケーション アクティビティとスケジュール設定されたレプリケーション アクティビティに関するステータス情報を表示することができます。

手順

1. 左側の AUI ナビゲーション ペインで、>> をクリックし、[**Monitor**] > [**Activity**] に移動します。
[**Activity Monitor**] が開き、すべてのアクティビティのリストが表示されます。レプリケーション ジョブは、[**Type**] 列の [**Replication Source**] を示します。さらに、ビューをフィルタリングして、レプリケーション ジョブのみを表示することもできます。
2. 結果をフィルタリングしてレプリケーション アクティビティのみを表示するには、次のようにします。
 - a. [**Type**] 列の横にある ▼ をクリックします。

b. **Replication Source** と入力します。

レプリケーション タスクのキャンセル

ポリシー ベースのレプリケーション タスクは、完了前に **Activity Monitor** でいつでもキャンセルできます。キャンセルには、5 分以上かかる場合があります。レプリケーションがキャンセル処理よりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Activity**] をクリックします。
[**Activity Monitor**] にアクティビティのリストが表示されます。
2. リストからレプリケーション タスクを選択します。
3. [**CANCEL**] をクリックします。
確認ダイアログ ボックスが表示されます。
4. [**YES**] をクリックします。

第4章

クライアントの管理

本章は、次のトピックで構成されています。

• Avamar クライアントの概要	70
• クライアントドメイン	70
• クライアント登録	72
• クライアントのアクティブ化	76
• クライアントページング	77
• クライアント情報の編集	79
• クライアントプロパティの表示	80
• クライアントの有効化/無効化	81
• クライアントを新規ドメインに移動	81
• クライアントの廃棄	82
• クライアントの削除	83
• 統合クライアントの表示	83
• 保護されていないクライアントの表示	84

Avamar クライアントの概要

Avamar クライアントは、ネットワーク接続を介して、Avamar サーバにアクセスするネットワーク接続のコンピューターまたはワークステーションです。

Avamar ドメインを使用して、クライアントを整理および分類できます。ドメインによって、管理ユーザー アカウントをドメインごとに定義できるようになり、セキュリティを向上させることができます。

Avamar がクライアントでデータをバックアップ/リストアできるようにするには、まずそのクライアントを Avamar サーバに追加または [登録] して、アクティブ化する必要があります。

Avamar クライアントを可能な限り柔軟に導入するために、登録とアクティベーションは別のイベントとして非同期に実行されます。多くの場合、登録とアクティベーションはほぼ同時に実行されますが、数時間、数日、あるいは数週間のずれが生じる場合もあります。

Avamar Administrator では、クライアント名は常にクライアントのホスト名である必要があります。ホスト名が変更されたために Avamar Administrator でクライアント名を変更する必要がある場合、クライアントコンピューター上の Avamar ソフトウェアをシャットダウンします。クライアント情報を編集してクライアント名を変更し、Avamar クライアント ソフトウェアを再起動します。これは、クライアントが MCS (Management Console Server) データベースへの登録を確実に保持する唯一の方法であり、過去のバックアップが継続してクライアントと関連づけられることを確実にします。

クライアント ドメイン

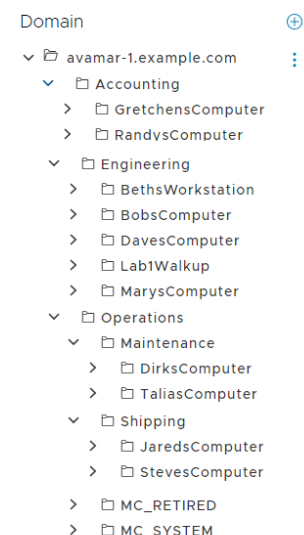
Avamar クライアント ドメインは、Avamar サーバ内でクライアントを整理および分類するための個別ゾーンです。管理ユーザー アカウントをドメインごとに定義できるようにすることで、サーバのセキュリティを高めることができます。

Avamar クライアント ドメインは、完全に Avamar サーバの内部的なものであり、インターネット ドメインとは何の関係もありません。

ドメインのネスト

ドメインをネストすることで、高度なツリー構造を作成できます。次のドメインの例を考えてみましょう。

図 10 Avamar ドメインの例



root ドメインである `avamar-1.example.com` には、次の 3 つの部門ドメインが含まれます。**Accounting**、**Engineering**、**Operations**。Operations ドメインには、**Maintenance** と **Shipping** の 2 つのサブドメインがあります。

ドメインとサブドメインの間には、機能的な違いはありません。[サブドメイン] は、上位の別のドメイン内にネストされるすべてのドメインを示す用語にすぎません。

階層的管理

ドメインの本当の強みは、クライアント ツリーの特定のレベルに管理者を追加できることにあります。こうしたドメイン レベルの管理者を追加することで、そのドメイン内のクライアントとポリシーを管理できます。

例えば、ルート ドメインに管理者を追加すると、その管理者はシステム全体のクライアントとポリシーを管理できます。ただし、ドメインに追加された管理者が管理できるのは、そのドメインと下位のサブドメインのクライアントとポリシーのみです。

このガイドの手順は、root ドメインにログインしていることを前提としています。下位のドメインにログインすると、そのドメイン外の特定のクライアント、データセット、グループ、イベント管理機能にはアクセスできない場合があります。

特殊ドメイン


MC_RETIRED および REPLICATE ドメインを削除することはできません。

MC_RETIRED ドメインには、廃棄されたクライアントが含まれます。このドメインの主な目的は、廃棄されたクライアント バックアップからのリストアを容易に実行することです。

REPLICATE ドメインには、他のサーバーからレプリケートされたデータが含まれます。

ドメインの作成

手順

1. 左側の AUI ナビゲーション ペインで、[>>>] をクリックしてから **[Asset Management]** をクリックします。
2. **[Asset Management]** パネルで、次の手順を実行します。
 - a. 階層 **[Domain]** ツリーで、ドメインを作成するツリー内の場所を選択します。
 - b.  をクリックします。

[Create domain] ダイアログ ボックスが表示されます。
3. **[Name]** フィールドに、ドメインの名前を入力します。
ドメイン名は 63 文字以内であることが必要であり、次に挙げる文字を使用することはできません。`=~!@#$%^&(){}[]|,`;'#\/:*?<>'\"&`
4. (オプション) 残りのフィールドで、ドメインの担当者について、名前、電話番号、メールアドレス、所在地を入力します。
5. **[OK]** をクリックします。
確認のメッセージが表示されます。

ドメイン情報の編集

ドメインの担当者と場所の情報を編集できます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>>] をクリックしてから **[Asset Management]** をクリックします。

2. 階層 **[Domain]** ツリーで、ドメインを選択します。
3. ドメイン情報を編集するには、次のいずれかの手順を実行します。
 - オーバーフローメニュー [⋮] をクリックして、**[Edit Domain]** を選択します。
 - **[DOMAIN ACTIONS]** パネルで、**[Edit Domain]** を選択します。**[Edit Domain]** ダイアログ ボックスが表示されます。
4. ドメインの担当者情報を編集します。
5. **[OK]** をクリックします。

ドメインの削除

ドメインを削除すると、そのドメイン内のクライアントもすべて削除されます。クライアントをシステム内にそのまま残すには、ドメインを削除する前にクライアントを新しいドメインに移動してください。

ディレクトリ サービス認証を使用する場合、Avamar はアクセスのためにそのドメインを使用する LDAP マップを削除します。一方、関連するディレクトリ サービス グループは削除の影響を受けません。

手順

1. 左側の AUI ナビゲーション ペインで、[>>>] をクリックしてから **[Asset Management]** をクリックします。
2. 階層 **[Domain]** ツリーで、削除するドメインを選択します。
3. ドメインを削除するには、次のいずれかの手順を実行します。
 - オーバーフローメニュー [⋮] をクリックして、**[Delete Domain]** を選択します。
 - **[DOMAIN ACTIONS]** パネルで、**[Delete Domain]** を選択します。**[Delete Domain]** ダイアログ ボックスが表示されます。
4. **[Yes]** をクリックします。

クライアント登録

クライアント登録は、Avamar サーバでの ID を確立するプロセスです。Avamar がクライアントを「認識」すると、固有 CID (クライアント ID) を割り当てます。この CID がアクティベーションの際にクライアントに送信されます。

クライアントを登録するには、次の 3 つの方法があります。

- クライアント側登録
- Avamar Administrator を使用して対話形式で行うサーバ側の登録
- クライアントのバッチ登録

注

別のサーバーにクライアントを登録する場合は、クライアントを元のサーバーから登録解除してから別のサーバーに登録します。

クライアント側登録

クライアント側登録は、オペレーティング システムによりプロセスが異なります。

サポートされている各オペレーティング システムのクライアント側登録については、「Avamar バックアップクライアント ユーザー ガイド」を参照してください。

また、クライアント側登録では、クライアントのアクティベーションが同時に行われます。ただし、クライアントはデフォルトグループに自動的に追加されるため、デフォルトのデータセット、スケジュール、保存ポリシーを使用する必要があります。結果として、この方法では十分に制御できないサイトもあります。

クライアントの登録または追加

AUI を使用して、ドメインとポリシーのシステムにクライアントを追加することができます。これにより高度なコントロールが可能となります。例えば、特定のデータセット、スケジュール、保存ポリシーを割り当てることができます。ただし、数多くのクライアントを追加するには、非常に時間がかかります。

クライアント登録は、Avamar サーバーでの ID を確立するプロセスです。Avamar がクライアントを「認識」すると、固有 CID (クライアント ID) を割り当てます。この CID がアクティベーションの際にクライアントに送信されます。

クライアントを追加して登録したら、ドメインとポリシーのシステムにクライアントを追加できます。これにより高度なコントロールが可能となります。例えば、特定のデータセットを割り当ててから、スケジュール、保存ポリシーを割り当てることができます。ただし、数多くのクライアントを追加するには、非常に時間がかかります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。
2. ドメイン ツリーで、クライアントのドメインまたはサブドメインを選択します。
3. [**ADD CLIENT**] をクリックします。

注

[VMware vCenter]、[Image Proxy]、[Virtual Machine] のクライアント タイプについては、「Avamar for VMware ユーザー ガイド」を参照してください。

[**New Client**] パネルが表示されます。

4. [**New Client Name**] フィールドに、アカウント名を入力して、[**NEXT**] をクリックします。

[**Optional Information**] パネルが表示されます。

5. (オプション) 連絡先名、電話番号、E メール、場所など、オプションの連絡先情報を入力し、[**NEXT**] をクリックします。

[**Summary**] パネルが表示されます。

6. クライアントのサマリー情報を確認して、[**ADD**] をクリックします。

[**Finish**] パネルが表示されます。

7. [**OK**] をクリックします。

クライアントのバッチ登録

クライアントを多数所有している大規模なサイトに対応するには、クライアントのバッチ登録機能が役立ちます。これにより、1 つのクライアント定義ファイルで複数のクライアントを定義することができます。このファイルは Avamar サーバで検証されインポートされます。

大規模なサイトでのクライアントのバッチ登録は、Avamar Administrator または AUI を使用して対話形式でクライアントを追加する場合と同程度の制御ができるうえ、非常に高速です。

クライアント定義ファイル

Avamar では、クライアントのバッチ登録に使用するクライアント定義ファイル用に XML (Extensible Markup Language) と CSV (Comma-Separated Values) の形式をサポートしています。

XML 形式

XML クライアント定義ファイルは、.xml 拡張子を使用し、次の構造と形式に準拠している必要があります。

```
<?xml version="1.0" encoding="UTF-8" ?>
  <registration_stream>
    <registrants>
      <entry
        host_name="MyClient.Example.com"
        mcs_domain="clients"
        mcs_group="MyGroup"
        dataset="MyDataset"
        retention_policy="MyRetentionPolicy"
        contact_address="192.168.31.5"
        contact_port="28002"
        access_list="user1@avamar:password, user2@LDAP"
        encryption="high"
        encryption_override="false"
      />
    </registrants>
  </registration_stream>
```

通知

このトピックで示すクライアント定義ファイルはあくまで参考用です。この例をコピーして、クライアント定義ファイルにペーストしないようにしてください。見えないフォーマット用の文字が含まれるため、正常に機能しません。

個別の<entry>エレメントを使用して、各クライアントを定義します。次の表では、各<entry>エレメントで利用可能な属性を説明しています。

表 18 クライアント定義ファイルの各エントリーの属性

属性	説明
host_name	このクライアントのネットワーク ホスト名または IP アドレス。
mcs_domain	このクライアントのオプションの Avamar ドメイン。この属性に値を指定すると、デフォルト clients ドメインをオーバーライドします。
mcs_group	このクライアントのオプションのデフォルト グループ。この属性に値を指定すると、デフォルト グループの割り当てをオーバーライドします。
dataset	バックアップ中に使用する、このクライアントのオプションのデフォルト データセット。この属性に値を指定すると、通常、グループから継承するデフォルトのデータセットをオーバーライドします。

表 18 クライアント定義ファイルの各エントリーの属性 (続き)

属性	説明
retention_policy	このクライアントで使用するオプションのデフォルトのバックアップ保存ポリシー。この属性に値を指定すると、通常、グループから継承するデフォルトの保存ポリシーをオーバーライドします。
contact_address	クライアントの IP アドレス (オプション)。
contact_port	contact_port をデフォルトの Avamar データ用ポートである 28002 に設定します。
access_list	このクライアントから Avamar サーバにアクセスできるユーザーのオプションリスト。 user@authentication:password のような形式で指定します。内部認証システムを使用する場合は、単語 password をコロンの後に配置します。このステップにより、ユーザーがシステムにアクセスしたとき、認証情報の入力を求められるようになります。外部認証システムを使用する場合は、:password を省略します。複数のユーザーを定義するには、各ユーザー エントリーをコンマ (,) で区切り、ユーザーのリスト全体を引用符 (" ") で囲みます。
encryption	クライアント/サーバー間のデータ転送に使用される暗号化方式 : <ul style="list-style-type: none"> • High • None <hr/> <p>注</p> <p>クライアント/サーバー間の接続における暗号化テクノロジーおよびビットの強度は、クライアントのプラットフォームおよび Avamar サーバのバージョンをはじめ、さまざまな要因によって異なります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。</p>
encryption_override	暗号化方式のオーバーライド (オプション)。TRUE に設定すると、このクライアントはグループの暗号化方式を使用しません。

CSV 形式

CSV 形式のクライアント定義ファイルでは、XML 形式のクライアント定義ファイルと同じエレメントおよび属性を使用します。ただし、次の例で示すように、各クライアントを 1 行で定義し、各属性の値をコンマで区切ります。

```
host_name,mcs_domain,mcs_group,dataset,retention_policy,
contact_address,contact_port,access_list,encryption,
encryption_override
```

クライアント定義ファイルの妥当性検査とインポート

手順

1. Avamar Administrator で、[**Administration**] 起動リンクをクリックします。
[**Administration**] ウィンドウが表示されます。
2. [**Account Management**] タブをクリックします。
3. [**Actions**] メニューから、[**Account Management**] > [**Import Clients from File**] を選択します。
[**Validate**] ダイアログ ボックスが表示されます。
4. 保存したクライアント定義ファイルを参照して選択します。
5. [**Validate**] をクリックします。
[**Validation Results**] ダイアログ ボックスが表示されます。
6. クライアント定義ファイルにエラーがない場合、[**Commit**] をクリックして、クライアントリストをインポートします。あるいは、クライアント定義ファイルにエラーがある場合、エラーを訂正し、ファイルを再度保存して、この手順を繰り返します。
[**Validation Results**] ダイアログ ボックスが閉じられ、[**Account Management**] ツリーに新規クライアントが表示されます。

クライアントのアクティブ化

クライアントのアクティベーションとは、CID（クライアント ID）をクライアントに送信するプロセスのことです。クライアントは受け取った CID を、クライアント ファイル システム上のファイルに格納します。

はじめに

- クライアントがネットワーク上に存在している必要があります。
- Avamar クライアントソフトウェアがクライアントにインストールされ、実行されている必要があります。
- Avamar サーバは、クライアントを登録するために使用したホスト名を解決できる必要があります。

クライアントのアクティベーションには、次の 2 つの方法があります。

- クライアントからアクティベーションを開始する。この方法は、「Avamar バックアップクライアント ユーザー ガイド」で説明されています。
- AUI を使用して、クライアントを招待し、サーバーでアクティブ化する。

通知

HP-UX、Linux、Solaris の各クライアントは、インストール中に、または Avamar Administrator を使用して、アクティブ化できます。これらのコンピューティング プラットフォームでは、クライアントのアクティベーションを開始するクライアント側のコマンドは用意されていません。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。

3. クライアントのリストで、アクティブ化するクライアントを選択します。

ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。

4. **[MORE ACTIONS]** > **[Invite Client]** をクリックします。

ステータス メッセージにより、サーバーでアクティブ化するためにクライアントに招待が送信されたことが示されます。

クライアントの再アクティブ化

クライアント コンピューターの交換など、特定の状況では、新たにインストールされたクライアント ソフトウェアでクライアントのアカウントを再度アクティブ化することが必要な場合があります。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Asset Management]** をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、再アクティブ化するクライアントを選択します。

ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。

4. **[MORE ACTIONS]** > **[Edit Client]** をクリックします。

[Edit Client] ウィンドウが表示されます。

5. **[Activated]** チェックボックスをオンにします。
6. **[UPDATE]** をクリックします。

必要条件

クライアントを非アクティブ化した後、特定プラグインのユーザー ガイドの指示に従いクライアントの登録を完了します。この処理手順により、クライアントが非アクティブになり再度アクティブ化できるようになります。

クライアント ページング

Avamar クライアントは、ページング可能である場合とページング不可能である場合があります。クライアントがページング可能の場合は、クライアントのページング設定を MCS で決定する方法を制御するために、設定を指定できます。ページング不可能なクライアントを使用する環境では、これによる制限事項への対処法を使用することが必要になる場合があります。

ページング可能クライアント

ページング可能クライアントでは、Avamar サーバにページ アドレスおよびポート番号を提供し、これによりオン デマンド バックアップおよびリストアを実行できます。また、Avamar Administrator のバックアップおよびリストア中に、Avamar Administrator によってクライアント ファイル システムを参照することも可能です。

次に挙げるクライアントのページング設定のいずれかを指定して、クライアントのページング設定を MCS が決定する方法を制御します。

- **[Automatic]** : デフォルト設定の自動ページングを使用すると、MCS はクライアントのページング設定を自動的に決定するように試みます。クライアントから更新されたページング情報を MCS が受け取ると、設定が自動的に更新されます。

- **[Manual]** : 手動ページングを使用する場合は、クライアント/MCS 間の通信で使用する IP アドレスとデータ用ポート番号を指定します。NAT (ネットワーク アドレス変換) を使用する場合は、手動ページングの使用が必要になることがあります。NAT を使用すると、MCS は適切なクライアント ページング設定を自動的に決定できなくなる場合があります。手動モードでは、MCS によってクライアントの IP アドレスやポート番号の設定が上書きされることはありません。

クライアント/MCS 間の通信に使用する IP アドレスまたはデータ用ポート番号を指定せずに、自動ページングを無効化することも可能です。自動ページングの無効化は、ラップトップコンピューターのように、長期間ネットワークに存在しないクライアントをサポートするために有効です。これらのクライアントでは、各自でオン デマンド バックアップを開始する必要があります。このため、可能な場合は必ずクライアント ページングを有効化します。

ページング不可能なクライアント

クライアントがページング不可能である場合、Avamar サーバ ユーティリティ ノードまたはシングル ノード サーバで実行される Avamar Administrator サーバは、Avamar クライアントのポート 28002 との TCP/IP 接続を確立できません。

クライアントがページング不可能である可能性がある場合

次の状況の場合、クライアントはページング不可能である可能性があります。

- 環境 (クライアントを含む) 内にクライアントとのポート 28002 での着信接続を妨げるファイアウォールのルールが存在している。
- クライアントは、Avamar サーバから開始される接続についてポート転送をサポートしないルータの背後にある。(このステップは、Managed サービス プロバイダーが VPN を使用せずに Avamar を導入した場合に発生する可能性がある一般的な状況です。)
- Avamar Administrator サーバは、Avamar Administrator サーバが使用するページング アドレスで Avamar クライアントと接続できない。1 つの例として、クライアントがマルチホームであり、クライアントとの接続のために Avamar Administrator サーバが使用するページング アドレスがページング アドレスに対する経路を持っていない場合が挙げられます。
- クライアントのポート 28002 でホスト間接続を確立するために認証が必要な環境であり、Avamar Administrator サーバ プロセスは必要な認証プロトコルをサポートすることができない。
- IPSec 環境 : Windows 環境では、Microsoft のベスト プラクティスにより、IPSec の有効化が推奨されているため、クライアントは IPSec 環境ではページ可能ではない。

MCS は、ページ可能ではないクライアントを自動的に検出し、設定を調整します。通常、MCS では手動による変更が必要ありません。AUI の **[Client Summary]** を参照することにより、クライアントがページング可能であるかどうかを判断できます。クライアントの **[Paging Enabled]** 列に **[No]** と表示されている場合は、MCS がクライアントの avagent プロセスに接続することができず、クライアントはページング不可能です。

ページング不可能なクライアントによる環境の制限事項

ページング不可能なクライアントを使用する環境では、Avamar Administrator を使用して、バックアップまたはリストアのほか、ポリシーの定義を実行することができます。場合によっては、明示的なパス名の入力が必要になります。

クライアントがページング不可能である場合、次の制限事項が適用されます。

- MCS がポート 28002 でクライアントをページングできない場合、Avamar は Avamar Administrator を使用して、クライアントを招待し、アクティブ化することができません。
- データセットを定義する場合、またはリストアのターゲットを選択するために参照する場合は、クライアント ファイル システムを参照できません。この制限事項に対処するには、クライアントを参

照せずに、バックアップ データセットを明示的に定義します。リストア中に、リストア ターゲットのパスを明示的に入力します。

- クライアント ログを表示することはできません。この制限事項に対処するには、クライアント コンピューターからログを取得します。
- クライアントを待機するワークオーダーが存在する場合、クライアントのページングはできません。この場合、クライアントは MCS に接続し、ワークオーダーの有無を確認するために、およそ 1 分に 1 回ポーリングを行います。
数百個を超えるページング不可能なクライアントをバックアップする際は、ポーリング間隔を増やすが必要になる場合があります。デフォルトのポーリング間隔は 60 秒です。MCS パフォーマンスが低下している場合、容認できるパフォーマンスが達成されるまでポーリング間隔を大きくします。

クライアント ページング設定の追加または変更

MCS では、クライアント ページング設定を自動的に決定できますが、任意のクライアント用に手動でページング設定を指定することも可能です。NAT を使用する場合は、手動でページング設定を指定することが必要になる可能性があります。

手順

1. 左側の AUI ナビゲーション ペインで [>>] をクリックしてから、[**Asset Management**] をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、編集するクライアントを選択します。
ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。
4. [**MORE ACTIONS**] > [**Edit Client**] をクリックします。
[**Edit Client**] ウィンドウが表示されます。
5. [**Paging**] タブをクリックします。
6. [**Automatic**] または [**Manual**] ページング モードのいずれかを選択します。
7. [**Manual**] を選択した場合は、次のようにクライアント/MCS 通信に使用するクライアント情報を指定します。
 - **Automatic** モードで、MCS がこのクライアントのホスト名を自動的に判別できない場合は、[**Address (IP or hostname)**] フィールドにクライアントの有効な (NAT ではない) IP アドレスを入力します。
 - [**Port Number (secure)**] フィールドで、データ用ポート番号を指定します。デフォルトのデータ用ポートは 30002 です。
 - [**Port Number (insecure)**] フィールドで、データ用ポート番号を指定します。デフォルトのデータ用ポートは 28002 です。
8. [**UPDATE**] をクリックします。

クライアント情報の編集

Avamar Administrator でクライアントの名前、担当者情報、所在地情報を編集できます。

Avamar Administrator では、クライアント名は常にクライアントのホスト名である必要があります。クライアントのホスト名が変更されたために Avamar Administrator でクライアント名を変更する必要がある場合、クライアント コンピューター上の Avamar ソフトウェアをシャットダウンします。この処理手順に従ってクライアント名を変更してから、Avamar クライアント ソフトウェアを再起動します。この

アクションは、クライアントが MCS (Management Console Server) データベースへの登録を確実に保持する唯一の方法であり、過去のバックアップが継続してクライアントと関連づけられることを確実にします。

手順

1. 左側の AUI ナビゲーション ペインで [>>] をクリックしてから、[Asset Management] をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、編集するクライアントを選択します。

ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。

4. [MORE ACTIONS] > [Edit Client] をクリックします。

[Edit Client] ウィンドウが表示されます。

5. クライアントの名前、担当者情報、所在地情報を編集します。
6. [UPDATE] をクリックします。

確認のメッセージが表示されます。

クライアントプロパティの表示

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Asset Management] をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、プロパティを表示するクライアントを選択します。

ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。

次の表で説明するクライアントの詳細は、ウィンドウの右パネルに表示されます。

表 19 クライアント サマリー情報

列	説明
Name	内容を説明するクライアント名。
Enabled	Avamar がクライアントのバックアップを実行できるかどうかを示します。この設定にかかわらず、以前のバックアップがシステム上に存在している限り、クライアントはファイルをリストアできます。
Activated	クライアントは Avamar サーバでアクティブ化されています。
アクティブ化時間	クライアントが Avamar サーバでアクティブ化された時刻。
Domain	クライアントの Avamar ドメイン。
Client OS	クライアントのオペレーティング システム。
Client Version	クライアント上の Avamar クライアント ソフトウェアのバージョン。
Client OS	クライアントのオペレーティング システム。

表 19 クライアント サマリー情報 (続き)

列	説明
Last Check-in	Avamar クライアント エージェントが最後に Avamar サーバにチェックインした日時。
Encryption	クライアント/サーバ間のデータ転送に使用される暗号化方式。
CID	Avamar サーバでのこのクライアントの固有識別子であるクライアント ID。CID は、クライアントのアクティベーション中に割り当てられます。
Client Paging	クライアントが Avamar サーバにページ アドレスとポート番号を提示したかどうかを示します。これにより、オン デマンド バックアップとリストアが実行可能となります。さらに Avamar Administrator では、Avamar Administrator によって開始されたバックアップおよびリストアの実行中に各自のファイル システムを参照できます。
Backup Statistics	クライアントのバックアップ ジョブのステータス情報。

クライアントの有効化/無効化

クライアントを無効にすることで、Avamar サーバでファイルをバックアップできないようにすることができます。通常、この操作は、システムがメンテナンス アクティビティを行える状態にしておくために実行します。クライアントが無効になっている場合は、クライアントがバックアップを再開できるように、事前にクライアントを再度有効化する必要があります。

手順

1. 左側の AUI ナビゲーション ペインで [>>] をクリックしてから、[**Asset Management**] をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、編集するクライアントを選択します。
ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。
4. [**MORE ACTIONS**] > [**Edit Client**] をクリックします。
[**Edit Client**] ウィンドウが表示されます。
5. クライアントを有効化するには、[**Basic**] タブで、[**Enabled**] チェックボックスをオンにします。
確認メッセージが表示されます。
6. クライアントを無効化するには、[**Basic**] タブで、[**Enabled**] チェックボックスをオフにします。
確認メッセージが表示されます。
7. [**UPDATE**] をクリックします。

クライアントを新規ドメインに移動

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。

2. 階層 **[Domain]** ツリーで、ドメインを選択します。
3. クライアントのリストで、移動するクライアントを選択します。
ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、**root** ドメインにログインします。
4. **[MORE ACTIONS]** > **[Move Client]** をクリックします。
[Move Client] ダイアログ ボックスが表示されます。
5. クライアントの新規ドメインを選択します。
6. **[OK]** をクリックします。

クライアントの廃棄

クライアントを廃棄すると、Avamar はクライアントのバックアップを停止します。Avamar は、廃棄されたクライアントの既存バックアップに指定された保存設定に基づいて、既存バックアップを保持する期間を判断します。また Avamar は、廃棄されたクライアントのバックアップの既存レプリカに指定された保存設定に基づいて、既存レプリカを保持する期間を判断します。

廃棄されたクライアントの既存バックアップまたはレプリカからデータをリストアするには、Avamar Administrator を使用します。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Asset Management]** をクリックします。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、破棄するクライアントを選択します。
ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、**root** ドメインにログインします。
4. **[MORE ACTIONS]** > **[Retire Client]** をクリックします。
[Retire Client] ウィンドウが表示されます。
5. **[Local Backups]** セクションで、クライアントのバックアップを保持する期間を選択します。
 - 既存の有効期限日までバックアップを保存する場合、**[Retain local backups with existing expiration date]** を選択します。
 - 既存の有効期限日にかかわらず無期限にバックアップを保存する場合、**[Retain all local backups indefinitely]** を選択します。
 - 新しい有効期限日までバックアップを保存する場合、**[New Expiration Date]** の **[Reset local backup expiration date]** を選択し、新しい日付を選択します。
6. レプリカがあるクライアントについては、**[Remote Backups]** セクションで、クライアントのレプリカを保持する期間を選択します。
 - 既存の有効期限日までレプリカを保存する場合、**[Retain remote backups with existing expiration date]** を選択します。
 - 既存の有効期限日にかかわらず無期限にレプリカを保存する場合、**[Retain all remote backups indefinitely]** を選択します。
 - 新しい有効期限日までレプリカを保持する場合、**[Reset remote backup expiration date]** を選択し、新しい日付を選択します。
7. 子 VMware クライアントを破棄するには、**[Force Retire]** セクションで、**[Ignore running activity and force retire child vm client]** を選択します。

8. **[Submit]** をクリックします。
確認メッセージが表示されます。

クライアントの削除

クライアントとクライアントのすべてのバックアップを削除します。必要に応じて、レプリケーション ターゲット システムに存在するすべてのレプリカの削除を選択できます。

クライアントを削除すると、Avamar はそのクライアントに格納されているバックアップをすべて完全に削除します。クライアントを削除するのは、そのクライアントのバックアップを保持する必要がないと確信している場合に限られます。確信がない場合は、代わりにクライアントを廃棄します。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Asset Management]** をクリックします。
2. 階層 **[Domain]** ツリーで、ドメインを選択します。
3. クライアントのリストで、削除するクライアントを選択します。
ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。
4. **[MORE ACTIONS]** > **[Delete Client]** をクリックします。
[Delete Client] ダイアログ ボックスが表示され、クライアントの既存バックアップの数が表示されます。
5. **[I understand this action is permanent and irreversible]** を選択します。
このフィールドは、クライアントとクライアントのバックアップを誤って削除しないようにする安全策です。
6. **[YES]** をクリックします。

統合クライアントの表示




AUI ダッシュボードの **[Assets | Overview]** パネルには、Avamar サーバーに統合されているクライアントの数が表示されます。

手順

1. 統合されたクライアントに関する情報を表示するには、**[Integrated]** の横にあるアイコンをクリックします。
[Asset Management] パネルが表示されます。
2. ドメイン ツリーでドメインまたはサブドメインを選択します。
中央のパネルに表示されるクライアントのリストは、ステータスなどのクライアント情報を示します。

結果

[Asset Management] ペインの上部には、次のようなクライアント ドメインに関する情報が表示されます。

アイコン	説明
 Clients	ドメイン内のクライアントの数を示します。
 Activities	ドメイン内のクライアントによって開始されたアクティビティ（バックアップ ジョブとレプリケーション ジョブ）の数を示します。
 Policies	ドメイン内のクライアントに適用されるポリシーの数を示します。

保護されていないクライアントの表示

AUI ダッシュボードの **[Assets | Overview]** パネルには、バックアップが存在しない、保護されていないクライアントの数が表示されます。

手順

1. 保護されていないクライアントに関する情報を表示するには、**[Unprotected]** の横にあるアイコンをクリックします。

[Clients with no backups] ウィンドウが開き、各クライアントのサマリー情報が表示されます。

2. クライアントのプロパティを確認します。

プロパティ	説明
Name	内容を説明するクライアント名。
Domain	クライアントの Avamar ドメイン。
Enabled	Avamar がクライアントのバックアップを実行できるかどうかを示します。この設定にかかわらず、以前のバックアップがシステム上に存在している限り、クライアントはファイルをリストアできます。
Activated	クライアントが Avamar サーバーでアクティブ化されるかどうかを示します。
Client type	クライアントのタイプ（通常、仮想マシン、イメージ プロキシ、VMware vCenter など）。

第 5 章

ユーザー管理と認証

本章は、次のトピックで構成されています。

• Avamar ユーザー アカウントの概要	86
• ユーザー認証	86
• Avamar 内部認証	88
• ディレクトリサービスの認証	88
• エンタープライズ認証での下位互換性の有効化	106
• ロール	107
• ドメインへのユーザーの追加	112
• ユーザー情報の編集	113
• ユーザーの削除	114

Avamar ユーザー アカウントの概要

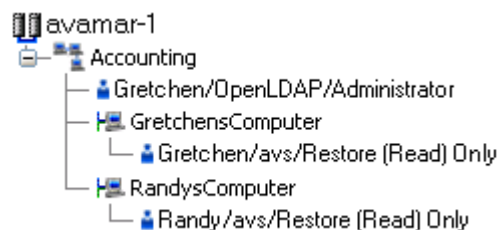
ユーザー アカウントにより、Avamar でドメインやクライアントを管理することができます。ユーザー アカウントでは、Avamar サーバへのユーザー アクセスを許可する際に使用する認証システムを定義します。また、ユーザーの役割も定義し、ユーザーが実行できる操作を制御します。

ユーザー アカウントをドメインや個々のクライアントに追加できます。ユーザー アカウントをドメインに追加すると、そのアカウントでドメインおよびそれに属するサブドメインを管理することができます。ユーザー アカウントを個々のクライアントに追加すると、そのアカウントでクライアントのバックアップとリストアを実行することができ、システム内のクライアントに属するバックアップにアクセスすることができます。

Avamar では、ユーザーはドメインまたはクライアントのアクセス リストのエントリーです。Avamar システムにユーザー アカウントを追加するときは、ドメインまたはクライアントのユーザー アクセス リストにエントリーを追加することになります。

次の例では、ユーザー「Gretchen」が、Accounting ドメインとそのユーザーのコンピューターに追加されています。ただし、認証システムと役割では、偶然同じユーザー名を持つことになった完全に異なるユーザー アカウントになります。

図 11 Avamar ドメイン内のユーザー



次の表では、Avamar ユーザー アカウントを構成する情報を説明しています。

表 20 Avamar ユーザー アカウント情報

情報	説明
ユーザー名	ユーザー名は認証システムにより異なるため、その認証システムが受け入れる形式でなければなりません。例えば、内部認証システムは、大文字と小文字を区別するユーザー名を使用しますが、Windows Active Directory のユーザー名は大文字と小文字を区別しません。ユーザー名は 31 文字以下にしてください。
認証システム	認証システムはユーザー名とパスワードのシステムであり、Avamar サーバへのユーザー アクセスを許可する際に使用されます。
ロール	ロールにより、各ユーザー アカウントに許可される操作が定義されます。

ユーザー認証

認証システムはユーザー名とパスワードのシステムであり、Avamar サーバへのユーザー アクセスを許可する際に使用されます。

Avamar は、次の認証システムをサポートしています。

- Avamar 内部認証。[Avamar 内部認証](#) (88 ページ) で説明しています。
- ディレクトリサービス認証。[ディレクトリサービスの認証](#) (88 ページ) で説明しています。

また Avamar は、非推奨の認証方法ですが、エンタープライズ認証をサポートします。[エンタープライズ認証での下位互換性の有効化](#) (106 ページ) では、エンタープライズ認証の継続的なサポートを有効化する方法について説明しています。

Avamar がユーザーを認証して役割を割り当てる方法

エンタープライズ認証との下位互換性を維持するため、また LDAP がマップされた複数のグループにユーザーが存在する可能性を確認するため、Avamar は各ログインの試行で、次の認証および役割の割り当てシーケンスを使用します。

1. ユーザー名が `user` の形式の場合 (ここで、`user` は `@server` が付かないユーザー名)、Avamar は内部の Avamar 認証データベースをチェックします。
ユーザー名、パスワード、ドメインが一致する場合、ログインは成功し、Avamar はそのユーザーに Avamar データベースでの役割を割り当てます。これらが一致しない場合、ログインは失敗します。
2. ユーザー名が `user@server` の形式の場合 (ここで、`user` はユーザー名、`server` は認証サーバの完全修飾ドメイン名)、Avamar はエンタープライズ認証を使用してログイン情報をチェックします。
ユーザー名、パスワード、ドメインが一致する場合、ログインは成功し、Avamar はそのユーザーに Avamar データベースでの役割を割り当てます。一致するものがない場合、評価は継続します。
3. ユーザー名が `user@server` の形式であり、エンタープライズ認証を使用した認証が失敗する場合、Avamar は LDAP マッピング システムをチェックします。
ログインの試行は、次の各識別子に一致するかどうかを、すべてのマップ済みグループに対してチェックされます。
 - ユーザー名 : [User Name] フィールドのエントリーの、@記号より前の部分。
 - パスワード : [Password] フィールドに入力されたエントリー。
 - Avamar ドメイン : [Domain Name] フィールドに入力されたエントリー。
 - ディレクトリサービスドメイン : [User Name] フィールドのエントリーの、@記号より後の部分。

識別子がすべて一致する場合、ログインは成功し、Avamar はそのユーザーにマップ済みグループからの役割を割り当てます。

ユーザーは、別のディレクトリサービスドメインでは、マップ済みグループのメンバーとなることができます。ログインの際に指定されたディレクトリサービスドメインに一致するマップ済みグループの役割は、そのセッションの間はそのユーザーに割り当てられます。

ユーザーが同じディレクトリサービスドメイン内の複数のマップ済みグループのメンバーである場合、最も強い権限を有する役割が割り当てられます。

4. ログイン情報が前述の手順のどの必要条件にも合わない場合、ログインは失敗し、失敗に関するメッセージが表示されます。

Avamar 内部認証

Avamar 内部認証では、Avamar ユーザー アカウントにユーザー名とパスワードを定義し、Avamar はその情報を格納します。ユーザー名は大文字と小文字が区別され、31 文字以下の必要があります。

内部 Avamar 認証を使用してユーザー アカウントを認証する場合、追加のステップは必要ありません。ユーザーを Avamar Administrator または AUI に追加する際に、各アカウントのユーザー名とパスワードを定義します。

ディレクトリ サービスの認証

ディレクトリ サービス認証を使用して認証を行い、既存のディレクトリ サービスの情報を使用して Avamar ユーザーに役割を割り当てます。ディレクトリ サービス認証は、特定の LDAP ディレクトリ サービスとともに機能し、OpenLDAP ディレクトリ サービスと併用する場合に追加機能を提供します。またディレクトリ サービス認証は、独自のディレクトリ サービス上の NIS (Network Information Service) またはサポートされる LDAP ディレクトリ サービスのいずれかでも機能します。

ディレクトリ サービス認証を使用する Avamar 製品

次の Avamar 製品では、ユーザーの認証と許可にディレクトリ サービス認証を使用できます。

- Avamar Administrator
- Avamar Web Restore
- Avamar クライアント Web ユーザー インターフェイス (Avamar Desktop/Laptop)

ディレクトリ サービス クライアントレコードを使用する Avamar 製品

Avamar Client Manager は、ユーザー ログインの認証と許可にディレクトリ サービス認証を使用しません。ただし、Avamar Client Manager は、ディレクトリ サービス メカニズムを使用して、Avamar クライアントになる可能性があるコンピューターについて情報を取得できます。Avamar Client Manager はディレクトリ サービスをクエリーして、クライアントに関する情報を入手します。さらに可能であれば、ディレクトリ ドメインなどのディレクトリ保守サービス体制ユニットやディレクトリ グループの情報も入手します。

ディレクトリ サービス タイプ

ディレクトリ サービス認証は、次のタイプのディレクトリ サービスをサポートします。

表 21 サポートされるディレクトリ サービス タイプ

タイプ	サポートされる実装
LDAP	<ul style="list-style-type: none"> • Windows Server 2003 Active Directory • Windows Server 2008 Active Directory ドメイン サービス • Windows Server 2012 Active Directory ドメイン サービス • Windows Server 2016 Active Directory ドメイン サービス • 389 Directory Server (バージョン 1.1.35)
OpenLDAP	SUSE OpenLDAP (バージョン 2.4)

表 21 サポートされるディレクトリ サービス タイプ (続き)

タイプ	サポートされる実装
NIS	Network Information Service

Avamar は、SSL/TLS を使用した暗号化された LDAP および OpenLDAP ディレクトリ サービス認証をサポートしています。デフォルトでは、LDAP または OpenLDAP サーバでサポートされている場合、Avamar は TLS 1.2 を使用します。サポートされていない場合、Avamar はサポートされているバージョンの SSL/TLS にフォールバックします。ただし、Avamar サーバはクライアント認証用の LDAP または OpenLDAP サーバに SSL/TLS 証明書を提供しません。

LDAP マップ

ディレクトリ サービス認証は、LDAP マップを使用して、ディレクトリ サービスの情報に基づいて Avamar ドメイン ユーザー グループを形成します。LDAP マップは、Avamar 許可レベルを、マップされたディレクトリ サービス ユーザー アカウントにリンクするために作成します。詳細については、「LDAP マップの追加」セクションを参照してください。

通知

Avamar ドメインを削除すると、その Avamar ドメインを使用してアクセスを行う LDAP マップが削除されます。ただし、LDAP マップを削除しても、削除されたマップに関連づけられているディレクトリ サービスグループまたはディレクトリ サービス ユーザー レコードには影響ありません。

LDAP ディレクトリ サービス認証

Avamar は、サポートされる LDAP ディレクトリ サービスで Avamar ユーザーに認証と許可の機能を提供します。

[LDAP ディレクトリ サービス認証を使用するための準備 \(90 ページ\)](#) では、LDAP ディレクトリ サービス認証の実装を準備する方法について説明します。

[サポートされる LDAP ディレクトリ サービスの情報を追加する \(91 ページ\)](#) では、LDAP ディレクトリ サービスに関して必要な情報を、Avamar システムに提供する方法について説明します。

[ディレクトリ サービス構成ファイルの編集 \(93 ページ\)](#) では、必要に応じて `ldap.properties` ファイルおよび `krb5.conf` ファイルを手動で編集する方法について説明します。

要件

Avamar ディレクトリ サービス認証は、以下の条件を満たした LDAP ディレクトリ サービスの利用をサポートします。

- LDAP サーバーが、以下の両方の形式でユーザー名のバインドを許可している。
 - `username`
 - `username@domain.com`
- LDAP サーバーが、ユーザー名を使用したグループ メンバーシップの検索を許可している。
- LDAP サーバーが、検索文字列を使用したグループの検索を許可している。
- LDAP マップの追加時に提供された LDAP サーバー アカウントが、ネストされた `ldapsearch` コマンドの実行権限を持っている。

Kerberos プロトコル

Avamar の LDAP ディレクトリ サービス認証では通常、キー配布センターとのすべての通信に Kerberos プロトコルを使用します。ユーザー名とパスワードは、キー配布センターのポート 88 に送信される前に、Avamar によって自動的に暗号化されます。

Simple バインドで、Kerberos プロトコルを使用せずに Avamar の LDAP ディレクトリ サービス認証を使用するには、`ldap.properties` ファイルを手動で編集します。

LDAP ディレクトリ サービス認証を使用するための準備

LDAP ディレクトリ サービス認証を使用するために準備するには、キー配布センターの特定のポートへのアクセスを Avamar に提供します。また、Avamar LDAP マップに関連づけられているディレクトリ サービス グループを作成します。

手順

- 次に挙げる KDC (キー配布センター) の認識されたポートに、Avamar がアクセスできることを確認します。

表 22 必要なキー配布センター ポート

ポート番号	説明
88	Kerberos 認証システム
389	LDAP (Lightweight Directory Access Protocol)
464	Kerberos Change/Set パスワード
636	LDAP over SSL/TLS

ポートは `krb5.conf` と `ldap.properties` で定義されます。

- (Avamar ではなく) ディレクトリ サービスにディレクトリ サービス グループを作成します。

グループ メンバーの数は 1 人からディレクトリ サービスが許容できる最大人数まで可能です。

できれば、Avamar LDAP マップで使用するための専用のディレクトリ サービス グループを作成してください。専用のディレクトリ サービス グループにより、許可されている Avamar アクセスのレベルに合わせて、グループ構成が検討されます。また、マッピング中に簡単に検索できるように、グループ名にはよく見られる文字パターンを使用しても構いません。例えば、各グループ名に、「av」で始まる文字を使用することもできます (「avAdministrators」など)。この文字パターンにより、ワイルドカード検索文字列に「av*」を使用することで、Avamar に関連したすべてのグループを検索することができるでしょう。

- コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。
 - マルチ ノード サーバーの場合、`admin` としてユーティリティ ノードにログインします。
- 次のコマンドを入力して、ユーザーを `root` に切り替えます。

```
su -
```

- 1 行に次のコマンドを入力して、キーストアをバックアップします。

```
cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/avamar/lib/rmi_ssl_keystore.bak
```

- 1 行に次のコマンドを入力して、キーストアに LDAP サーバ証明書をインポートします。

```
keytool -importcert -file <certfile>.crt -keystore /usr/local/avamar/lib/rmi_ssl_keystore -storepass changeme
```

ここで <certfile> は、パスを含む LDAP サーバ証明書の名前です。

7. 次のコマンドを入力して、MCS を再開します。

```
mcservers.sh --restart
```

必要条件

LDAP ディレクトリ サービスを使用するように、Avamar を構成します。

サポートされる LDAP ディレクトリ サービスの情報を追加する

ウィザードを使用して、Avamar ユーザーの認証と許可に使用するために、サポートされる LDAP ディレクトリ サービスの情報を追加します。

はじめに

ディレクトリ サービスが以下の要件を満たしていることを確認します。

- Kerberos を使用する SASL (Simple Authentication and Security Layer) BIND による認証を提供している。
- LDAP v.3 ベースの機能のみを使用している。
- 以下の両方の形式でユーザー名のバインドを許可している。
 - username
 - username@domain.com
- ユーザー名を使用したグループ メンバーシップの検索を許可している。
- 検索文字列を使用したグループの検索を許可している。
- 使用可能な LDAP サーバー アカウントがあり、ネストされた ldapsearch コマンドの実行権限を持っている。

通知

Simple バインド (平文) での認証を実行するディレクトリ サービスを追加するために、このウィザードを使用しないでください。代わりに[ディレクトリ サービス構成ファイルの編集 \(93 ページ\)](#) の説明に従って、手動で ldap.properties ファイルを編集してください。

手順

1. 管理者として Avamar Administrator の root ドメインにログインします。
 - a. Avamar Administrator を起動します。
 - b. [Server] で、ログイン先の Avamar サーバの IP アドレスまたは DNS 名を入力します。
 - c. [User Name] にユーザー名を入力します。

ユーザー名は、root ドメイン レベルの管理者役割が割り当てられているアカウントである必要があります。

Avamar がすでに、ディレクトリ サービスを使用するよう構成されている場合は、代わりに root ドメイン レベルの管理者許可を持つ LDAP アカウントを使用してログインすることができます。username@ldap-domain の形式を使用します。
 - d. [Password] に、ユーザー アカウントのパスワードを入力します。
 - e. [Domain Name] で、デフォルトのエントリーであるスラッシュ (/) の一文字を使用して、root ドメインを指定します。
 - f. [ログイン] をクリックします。

これがこの Avamar サーバへの最初の接続の場合は、**[Accept Server Certificate]** ダイアログ ボックスが開きます。サーバ証明書の詳細を確認し、**[Yes]** をクリックします。

Avamar Administrator ダッシュボードが表示されます。

2. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。

[Administration] ウィンドウが表示されます。

3. **[LDAP Management]** タブをクリックします。

4. **[Directory Service Management]** をクリックします。

[Directory Service Management] ダイアログ ボックスが表示されます。

5. ディレクトリ サービスを追加します。

- a. **[Add]** をクリックします。

[Adding a new Directory Service] セクションが表示されます。

- b. **[LDAP]** を選択します。

- c. **[Enter a fully qualified domain name]** に、ディレクトリ サーバーの完全修飾ドメイン名を入力します。

- d. (オプション) ディレクトリ サーバーが組織のデフォルトのディレクトリ サービス ドメインを示している場合は、**[Make this the default domain LDAP domain]** を選択します。

Avamar クライアント Web ユーザー インターフェイスで Macintosh コンピューターからのユーザーを認証できるようにするには、Macintosh ユーザーに割り当てられた LDAP サーバをデフォルト サーバとして構成する必要があります。

- e. **[Add]** をクリックします。

確認メッセージが表示されます。

- f. **[Yes]** をクリックします。

正常に実行されたことを示すメッセージが表示されます。代わりにエラー メッセージが表示される場合は、問題を解決してから、ディレクトリ サービスを再度追加してください。詳細については、[ディレクトリ サービスの構成中に表示されるエラー メッセージ](#) (103 ページ) を参照してください。

- g. **[OK]** をクリックします。

この変更は、mcs (Management Console Server) および emt (EM Tomcat) サービスに適用されます。

6. (オプション) 1 つ前のステップを繰り返して、他の認証ドメインを追加します。

7. 次の手順でディレクトリ サービス エントリーをテストします。

- a. **[Directory Service Management]** ダイアログ ボックスで、**[Configured Directory Services]** からエントリーの 1 つを選択します。

[Testing] セクションに表示されます。

- b. **[Username]** に、ディレクトリ サービス データベースの読み取り権限が与えられているアカウントのユーザー名を入力します。

- c. **[Password]** に、ユーザー名と関連づけられたパスワードを入力します。

- d. **[Run Test]** をクリックします。

エラーメッセージが表示される場合は、その問題を解決します。詳細については、[ディレクトリサービスの構成中に表示されるエラーメッセージ](#)（103 ページ）を参照してください。

e. **[Testing]** セクションを閉じるには、**[Close]** をクリックします。

8. **[Directory Service Management]** ダイアログ ボックスで **[Close]** をクリックします。

必要条件

ディレクトリ サービス グループを Avamar ユーザー情報と関連づけるには、LDAP マップを作成します。手順については、[LDAP マップの追加](#)（103 ページ）を参照してください。

ディレクトリ サービス構成ファイルの編集

LDAP 管理ツールでは、`ldap.properties` と `krb5.conf` のディレクトリ サービス構成ファイルを手動で編集できる機能が提供されます。標準以外の設定を構成したり、ディレクトリ サービスを使用するために Avamar を構成する際に発生した問題を解決したりするには、これらのファイルを手動で編集します。

はじめに

構成ファイルのキーと値に適切なフォーマットを決定します。

手順

1. 管理者として Avamar Administrator の root ドメインにログインします。
 - a. Avamar Administrator を起動します。
 - b. **[Server]** で、ログイン先の Avamar サーバの IP アドレスまたは DNS 名を入力します。
 - c. **[User Name]** にユーザー名を入力します。

ユーザー名は、root ドメインレベルの管理者役割が割り当てられているアカウントである必要があります。

Avamar がすでに、ディレクトリ サービスを使用するよう構成されている場合は、代わりに root ドメインレベルの管理者許可を持つ LDAP アカウントを使用してログインすることができます。`username@ldap-domain` の形式を使用します。

- d. **[Password]** に、ユーザー アカウントのパスワードを入力します。
- e. **[Domain Name]** で、デフォルトのエントリーであるスラッシュ (/) の一文字を使用して、root ドメインを指定します。
- f. **[ログイン]** をクリックします。

これがこの Avamar サーバへの最初の接続の場合は、**[Accept Server Certificate]** ダイアログ ボックスが開きます。サーバ証明書の詳細を確認し、**[Yes]** をクリックします。

Avamar Administrator ダッシュボードが表示されます。

2. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
3. **[LDAP Management]** タブをクリックします。
4. `ldap.properties` を編集するか、または `krb5.conf` を編集するために **[Edit KRB5 file]** を編集するには、**[Edit LDAP file]** をクリックします。
5. 追加および変更内容を **[Edit file]** ウィンドウに直接入力します。

6. [Save] をクリックしてから、[Close] をクリックします。

LDAP ベースの機能の形式要件と設定

Avamar Administrator の LDAP 管理ツールは、サポートされた LDAP ディレクトリ サービス向けに、適切な形式で `ldap.properties` ファイルを作成します。LDAP 管理ツールを使用してファイルを手動で編集する場合、指定形式は特定のパラメーターの要件に適合する必要があります。組織の認証要件を満たすため、`ldap.properties` に他の設定を手動で追加することができます。

LDAP ベースの機能のパラメーター要件

次の表に、LDAP ベースの機能のパラメーター要件を示します。

表 23 LDAP ベースの機能のパラメーター要件

ルール	説明	形式
各 LDAP サーバーにつき LDAP URL パラメーター 1 個	LDAP URL パラメーターは、特定のドメインコントローラーに LDAP サーバーを割り当てます。	<code>ldap.url.ds.example.abc.com=ldap://dchost.r1.example.abc.com:389</code> または <code>ldap.url.ds.example.abc.com=ldaps://dchost.r1.example.abc.com:636</code> ここで 、 <ul style="list-style-type: none"> • <code>ds.example.abc.com</code> は、LDAP サーバーの完全修飾ドメイン名です。 • <code>dchost.example.abc.com</code> は、LDAP サーバーで使用するドメインコントローラーの完全修飾ドメイン名です。 • <code>389</code> は LDAP サービスで使用するポートです。 • <code>636</code> は、SSL/TLS で暗号化されている場合に LDAP サービスで使用されるポートです。
正確なデフォルト サーバー パラメーター	デフォルト サーバー パラメーターは、特定のドメインにマッピングされていないクライアントのユーザーを認証する際に使用されます。例えば、ローカル ユーザーの他、AIX、FreeBSD、HP-UX、Linux、SCO、Solaris コンピューターからログインするユーザーです。	<code>ldap.qualified-name-default=dshost.example.abc.com</code> ここで、 <code>dshost.example.abc.com</code> はデフォルトの LDAP サーバの FQDN です。

その他のパラメーター

Avamar Administrator の LDAP 管理ツールを使用することで、他のパラメーターを `ldap.properties` に追加できます。次の表で、使用可能な設定を示します。

表 24 LDAP ベースの機能のその他のパラメーター

パラメーター	説明と値
<code>ldap.auth.domain.login-domain-suffix</code>	<p>LDAP を通して認証する際にユーザー名の値の一部として含まれるログインドメイン名のサフィックスを指定します。ここで、<code>login-domain-suffix</code> は、ログインドメイン名のサフィックスであり、値は認証ドメインです。例えば、ユーザーは <code>username@boston</code> または <code>username@boston.edu</code> を使用してログインできます。このパラメーターは次のように設定されます。</p> <pre>ldap.auth.domain.boston=boston.edu</pre> <p>このパラメーターを、パラメーター <code>ldap.query.domain</code> とともに使用すると、複数の認証ドメインが単一のログインドメイン名のサフィックスに割り当てられます。</p>
<code>ldap.query.domain.log-in-domain-suffix</code>	<p>追加の認証ドメインを単一のログインドメインのサフィックスに割り当てます。ここで、<code>ldap.auth.domain</code> パラメーターは <code>login-domain-suffix</code> を定義し、<code>ldap.query.domain</code> の値は組織のイントラネット内にある追加の認証ドメインです。たとえば、どちらの認証ドメインのユーザーも、<code>thusername@boston</code> の形式でログインします。この場合、2 個のパラメーターは次のように設定されます。</p> <pre>ldap.auth.domain.boston=boston.edu ldap.query.domain.boston=science.boston.edu,art.boston.edu</pre>
<code>ldap.entry.lookup.type.ldap-domain</code>	<p>ユーザー名の参照時に LDAP サーバーが使用する方法を定義します。この場合、<code>ldap-domain</code> は認証ドメインです。使用可能な値：</p> <ul style="list-style-type: none"> UN：ユーザー名。LDAP ディレクトリ サービスが通常使用する方法。(デフォルト) DN：識別名。OpenLDAP ディレクトリ サービスが通常使用する方法。
<code>user-login-module</code>	<p>認証メカニズムを制御します。次の値が利用可能です。</p> <ul style="list-style-type: none"> <code>kerberos</code>：Kerberos 暗号化付き LDAP 認証。この値はデフォルトです。 <code>ldap</code>：平文 LDAP 認証。またこのパラメーターでは、Windows ドメイン コンピューターでもユーザー ログインを強制するために、<code>ldap.auth.force.username.input=true</code> パラメーターが必要です。 <code>avamar</code>：Avamar 認証。 <code>mix</code>：kerberos と avamar の両方。
<code>ldap.auth.force.username.input</code>	<p>Kerberos パススルー認証が許可された Web アプリケーションのログイン画面でも、Avamar のユーザー ログインを要求するかどうかを制御します。使用可能な値：</p> <ul style="list-style-type: none"> <code>False</code>：ログインは不要です。この値はデフォルトです。

表 24 LDAP ベースの機能のその他のパラメーター (続き)

パラメーター	説明と値
	<ul style="list-style-type: none"> True : ログインが必要です。次のパラメーターで必要とされます。 user-login-module=ldap。
avamar-authentication-domains	次のパラメーターで必要とされます。user-login-module=mix。値は、ドメインのコンマ区切りリストです。Avamar 認証は、各リストのドメインのユーザーに適用されます。LDAP 認証はその他の全ユーザーに適用されます。
support-nis-authentication	NIS 認証サポートを有効化 (true) または無効化 (false) します。デフォルト値は false です。
nis.qualified-name-default	NIS ドメイン サーバーの完全修飾ドメイン名を指定します。
nis.url.nisdomainname	NIS ドメイン サーバーの IP アドレスを指定します。ここで、nisdomainname は nis.qualified-name-default の値です。

OpenLDAP ディレクトリ サービス認証

Avamar は、OpenLDAP ディレクトリ サービスを通じて、Avamar ユーザーの認証と許可をサポートします。

OpenLDAP ディレクトリ サービスの情報を Avamar に追加する方法については、[OpenLDAP ディレクトリ サービスの追加](#) (96 ページ) で説明します。

認証に OpenLDAP ディレクトリ サービスを使用するように Avamar を構成する場合、OpenLDAP のオプション パラメーターを使用できます。[OpenLDAP ディレクトリ サービス パラメーター](#) (100 ページ) では、OpenLDAP の必要なパラメーターとオプション パラメーターについて説明します。

OpenLDAP ディレクトリ サービスの追加

Avamar システムを構成して OpenLDAP ディレクトリ サービスを認証に使用するには、ldap.properties ファイルを編集します。

OpenLDAP ディレクトリ サービスを追加するには、Avamar サーバの ldap.properties ファイルを手動で編集して、必要なパラメーターを追加します。また Avamar システムが OpenLDAP ディレクトリ サービスと連携する方法を制御するために、オプションのパラメーターも追加できます。[OpenLDAP ディレクトリ サービス パラメーター](#) (100 ページ) では、必要なパラメーターとオプションパラメーターの詳細について説明します。

手順

1. 管理者として Avamar Administrator の root ドメインにログインします。
 - a. Avamar Administrator を起動します。
 - b. [Server] で、ログイン先の Avamar サーバの IP アドレスまたは DNS 名を入力します。
 - c. [User Name] にユーザー名を入力します。

ユーザー名は、root ドメイン レベルの管理者役割が割り当てられているアカウントである必要があります。

Avamar がすでに、ディレクトリ サービスを使用するよう構成されている場合は、代わりに root ドメイン レベルの管理者許可を持つ LDAP アカウントを使用してログインすることができます。username@ldap-domain の形式を使用します。

- d. **[Password]** に、ユーザー アカウントのパスワードを入力します。
- e. **[Domain Name]** で、デフォルトのエントリーであるスラッシュ (/) の一文字を使用して、root ドメインを指定します。
- f. **[ログイン]** をクリックします。

これがこの Avamar サーバへの最初の接続の場合は、**[Accept Server Certificate]** ダイアログ ボックスが開きます。サーバ証明書の詳細を確認し、**[Yes]** をクリックします。

Avamar Administrator ダッシュボードが表示されます。

2. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。

[Administration] ウィンドウが表示されます。

3. **[LDAP Management]** タブをクリックします。

4. ldap.properties を編集するには、**[Edit LDAP file]** をクリックします。

[Edit ldap.properties file] ダイアログ ボックスが表示されます。

5. テキスト入力領域で、新しい行に次のように入力します。

```
ldap.entry.lookup.type.ldap-domain=DN
ldap-domain は、OpenLDAP サーバのドメイン名です。
このパラメーターは必須です。
```

6. テキスト入力領域で、新しい行に次のように入力します。

```
ldap.userdn.ldap-domain=rdn-values
ここで、
```

- ldap-domain は、OpenLDAP サーバのドメイン名です
- rdn-values は、LDAP ツリーの root 識別名からの相対的なユーザー識別名ベースを、セミコロンで区切って指定したリストです。

コンマで区切られたリストの各エントリーは、逆階層の形式でユーザー グループの相対識別名ベースを表します。

ユーザーが root 識別名の直下に配置されている場合、または LDAP サーバが匿名の検索を許可している場合を除いて、このパラメーターが必要になります。

たとえば、ドメイン example.com のユーザーを、ツリー root にある Users、Employees、People に加えて、ツリー root にある Admins で検索できる場合、次のように入力します。

```
ldap.userdn.example.com=ou=Users,ou=Employees,ou=People;ou=Admins
```

7. テキスト入力領域で、新しい行に次のように入力します。

```
ldap.rootdn.ldap-domain=rootdn-format
ここで、
```

- ldap-domain は、OpenLDAP サーバのドメイン名です
- rootdn-format は、LDAP サーバで使用される root 識別名の形式です。

LDAP サーバで使用する root 識別名の形式が `dc=domain-segment,dc=domain-segment` になっていない限り、このパラメーターが必要になります。

たとえば、root 識別名を `dc=example, dc=com` として格納する LDAP サーバーでは、このパラメーターを `ldap.properties` 内で使用する必要はありません。

ただし、root 識別名を `u=example, o=com` として格納する LDAP サーバーでは、次のパラメーターを `ldap.properties` 内で使用する必要があります：

```
ldap.rootdn.exaple.com=u=example,o=com
```

8. テキスト入力領域で、オプションの OpenLDAP パラメーターを追加します。
各パラメーターは新しい行に入力します。
9. **[Save]** をクリックします。
10. 次の手順でディレクトリ サービス エントリーをテストします。
 - a. **[Directory Service Management]** ダイアログ ボックスで、**[Configured Directory Services]** からエントリーの 1 つを選択します。
[Testing] セクションに表示されます。
 - b. **[Username]** に、ディレクトリ サービス データベースの読み取り権限が与えられているアカウントのユーザー名を入力します。
 - c. **[Password]** に、ユーザー名と関連づけられたパスワードを入力します。
 - d. **[Run Test]** をクリックします。

エラー メッセージが表示される場合は、その問題を解決します。詳細については、[ディレクトリ サービスの構成中に表示されるエラー メッセージ](#) (103 ページ) を参照してください。
 - e. **[Testing]** セクションを閉じるには、**[Close]** をクリックします。
11. **[Directory Service Management]** ダイアログ ボックスで **[Close]** をクリックします。

結果

Avamar システムでは、OpenLDAP ディレクトリ サービスで認証することができます。

必要条件

ディレクトリ サービス グループを Avamar ユーザー情報と関連づけるには、LDAP マップを作成します。手順については、[LDAP マップの追加](#) (103 ページ) を参照してください。

OpenLDAP および Avamar 認証の有効化

Avamar 認証と OpenLDAP 認証を使用するよう Avamar システムを構成するには、`ldap.properties` ファイルを編集します。

はじめに

Avamar システムに OpenLDAP ディレクトリ サービスを追加します。

認証用に OpenLDAP ディレクトリ サービスを追加した後、一部の Avamar ドメインには Avamar 認証を使用するよう Avamar システムを構成します。

手順

1. 管理者として Avamar Administrator の root ドメインにログインします。
 - a. Avamar Administrator を起動します。

- b. **[Server]** で、ログイン先の Avamar サーバの IP アドレスまたは DNS 名を入力します。
- c. **[User Name]** にユーザー名を入力します。

ユーザー名は、root ドメイン レベルの管理者役割が割り当てられているアカウントである必要があります。

Avamar がすでに、ディレクトリ サービスを使用するよう構成されている場合は、代わりに root ドメイン レベルの管理者許可を持つ LDAP アカウントを使用してログインすることができます。username@ldap-domain の形式を使用します。

- d. **[Password]** に、ユーザー アカウントのパスワードを入力します。
- e. **[Domain Name]** で、デフォルトのエントリーであるスラッシュ (/) の一文字を使用して、root ドメインを指定します。
- f. **[ログイン]** をクリックします。

これがこの Avamar サーバへの最初の接続の場合は、**[Accept Server Certificate]** ダイアログ ボックスが開きます。サーバ証明書の詳細を確認し、**[Yes]** をクリックします。

Avamar Administrator ダッシュボードが表示されます。

- 2. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。

[Administration] ウィンドウが表示されます。

- 3. **[LDAP Management]** タブをクリックします。

- 4. ldap.properties を編集するには、**[Edit LDAP file]** をクリックします。

[Edit ldap.properties file] ダイアログ ボックスが表示されます。

- 5. テキスト入力領域で、新しい行に次のように入力します。

```
user-login-module=mix
```

Avamar 認証と OpenLDAP 認証を有効化するとき、このパラメーターが必要になります。

- 6. テキスト入力領域で、新しい行に次のように入力します。

```
user-login-module-mix-ldap=ldap
```

Avamar 認証と OpenLDAP 認証を有効化するとき、このパラメーターが必要になります。

- 7. テキスト入力領域で、新しい行に次のように入力します。

```
avamar-authentication-domains=av-domain-list
```

ここで、av-domain-list は Avamar ドメインのコンマ区切りリストです。

Avamar システムは、リストされた各ドメインからのユーザーのログイン認証に Avamar 認証を使用します。Avamar システムは、その他のすべてのユーザーには OpenLDAP 認証を使用します。

- 8. **[Save]** をクリックします。

- 9. **[Directory Service Management]** ダイアログ ボックスで **[Close]** をクリックします。

結果

Avamar システムでは、Avamar 認証と OpenLDAP 認証の指定された混在を有効化します。

OpenLDAP ディレクトリ サービス パラメーター

次の表では、表 23 (94 ページ) で指定した基本パラメーターに加え、OpenLDAP ディレクトリ サービスで使用するための `ldap.properties` ファイル パラメーターについて説明します。

表 25 OpenLDAP ディレクトリ サービス パラメーター

パラメーターと例	説明
<pre>ldap.entry.lookup.type.ldap-domain=DN</pre> <p>OpenLDAP を使用する LDAP ドメインの「xyz.com」:</p> <pre>ldap.entry.lookup.type.xyz.com=DN</pre>	<p>OpenLDAP を指定します。ldap-domain を LDAP サーバーのドメイン名に置き換えます。識別名の形式でのみユーザー ログインを受け入れる OpenLDAP サーバーに、このパラメーターを使用します。例えば、<code>uid=jsmith,dc=example,dc=com</code> です。このパラメーターは、この表に示したその他の OpenLDAP パラメーターを有効化します。</p>
<pre>ldap.userdn.ldap-domain=rdn-values</pre> <p>ユーザーを次の組織単位で分類する LDAP ドメイン"xyz.com"の場合:</p> <ul style="list-style-type: none"> Managers、ツリー root の下 Accountants、people の下、ツリー root の下 HRs、Employees の下、Users の下、ツリー root の下 Users、ツリー root の下 <pre>ldap.userdn.xyz.com=ou=Managers;ou=Accountants,ou=people;ou=HRs,ou=Employees,ou=Users;ou=Users</pre>	<p>相対識別名ベースを指定します。これは、ユーザーが含まれる組織単位に割り当てられます。ldap-domain を LDAP サーバーのドメイン名に置き換えます。また、rdn-values は、LDAP ツリーの root 識別名からの相対的なユーザー識別名ベースをセミコロンで区切って指定したリストに置き換えます。コマンドで区切られたリストの各エントリは、逆階層の形式でユーザー グループの相対識別名ベースを表します。</p>
<pre>ldap.rootdn.ldap-domain=rootdn-format</pre> <p>root 識別名を <code>u=xyz,o=com</code> の形式で格納する LDAP ドメイン「xyz.com」の場合:</p> <pre>ldap.rootdn.xyz.com=u=xyz,o=com</pre>	<p>LDAP サーバーの root 識別名の形式を指定します。root 識別名の形式が <code>dc=domain-segment,dc=domain-segment</code> になっていない限り、このパラメーターが必要になります。ldap-domain を LDAP サーバーのドメイン名に置き換えます。また rootdn-format は、LDAP サーバーで使用される root 識別名の形式に置き換えます。</p>
<pre>ldap.user.search.classes.ldap-domain=search-object</pre> <p>ユーザー検索でオブジェクト クラス タイプ"person"を使用する LDAP ドメイン"xyz.com"の場合:</p> <pre>ldap.user.search.classes.xyz.com=person</pre>	<p>ユーザー検索フィルターで使用されるオブジェクト クラス タイプを指定します。このパラメーターはオプションです。ldap-domain を LDAP サーバのドメイン名に置き換えます。また、search-object は、ユーザー検索フィルターで使用されるオブジェクト クラス タイプの指定に使用する値に置き換えます。コマンド区切り値を使用できます。デフォルト値は*です。</p>
<pre>ldap.user.search.attrs.ldap-domain=search-attribute</pre> <p>ユーザー検索でオブジェクト クラス属性"cn"を使用する LDAP ドメイン"xyz.com"の場合:</p> <pre>ldap.user.search.attrs.xyz.com=cn</pre>	<p>ユーザー検索フィルターで使用されるオブジェクト クラス属性を指定します。このパラメーターはオプションです。ldap-domain を LDAP サーバのドメイン名に置き換えます。また search-attribute は、ユーザー検索フィルターで使用される 1 個の属性に置き換えます。デフォルト値は uid です。</p>
<pre>ldap.group.search.byUpn.classes.ldap-domain=search-upn</pre> <p>User Principal Name オブジェクト クラス タイプ sambaGroupMapping および posixGroup をグループ検索に使用する LDAP ドメイン「xyz.com」の場合:</p> <pre>ldap.group.search.byUpn.classes.xyz.com=sambaGroupMapping, posixGroup</pre>	<p>グループ検索の User Principal Name フィルターで使用されるオブジェクト クラス タイプを指定します。このパラメーターはオプションです。ldap-domain を LDAP サーバのドメイン名に置き換えます。また、search-upn は、グループ検索の User Principal Name フィルターで使用されるオブジェクト クラス タイプを指定する値に置き換えます。コマンド区切り値を使用できます。デフォルト値は*です。</p>

表 25 OpenLDAP ディレクトリ サービス パラメーター (続き)

パラメーターと例	説明
<pre>ldap.group.search.byUpn.attrs.ldap-domain=upn-attributes</pre> <p>User Principal Name オブジェクト クラス属性 memberUid および uniqueMember をグループ検索に使用する LDAP ドメイン「xyz.com」の場合 :</p> <pre>ldap.group.search.byUpn.attrs.xyz.com=memberUid,uniqueMember</pre>	<p>グループ検索の User Principal Name フィルターで使用されるオブジェクト クラス属性を指定します。このパラメーターはオプションです。ldap-domain を LDAP サーバのドメイン名に置き換えます。また、upn-attributes は、グループ検索の User Principal Name フィルターで使用されるオブジェクト クラス属性を指定する値に置き換えます。コンマ区切り値を使用できます。デフォルト値は memberUid, uniqueMember です。</p>
<pre>ldap.unique.group.search.classes.ldap-domain=unique-type</pre> <p>Unique Groups グループ検索でオブジェクト クラス タイプ "posixGroup" を使用する LDAP ドメイン "xyz.com" の場合 :</p> <pre>ldap.unique.group.search.classes.xyz.com=posixGroup</pre>	<p>Unique Groups グループ検索フィルターで使用されるオブジェクト クラス タイプを指定します。このパラメーターはオプションです。ldap-domain を LDAP サーバのドメイン名に置き換えます。また、unique-type は、Unique Groups グループ検索フィルターで使用されるオブジェクト クラス タイプを指定する値に置き換えます。コンマ区切り値を使用できます。デフォルト値は sambaGroupMapping, posixGroup, groupOfUniqueNames です。</p>
<pre>ldap.unique.group.search.attrs.ldap-domain=unique-attributes</pre> <p>Unique Groups グループ検索でオブジェクト クラス属性 "cn" および "uid" を使用する LDAP ドメイン "xyz.com" の場合 :</p> <pre>ldap.unique.group.search.attrs.xyz.com=cn,uid</pre>	<p>Unique Groups グループ検索フィルターで使用されるオブジェクト クラス属性を指定します。このパラメーターはオプションです。ldap-domain を LDAP サーバのドメイン名に置き換えます。また、unique-attributes は、Unique Groups グループ検索フィルターで使用されるオブジェクト クラス属性を指定する値に置き換えます。コンマ区切り値を使用できます。デフォルト値は cn です。</p>
<pre>user-login-module=mix</pre>	<p>Avamar 認証と OpenLDAP 認証の混在モードで認証できるようにします。また構成には次を含める必要があります。user-login-module-mix-ldap=ldap と avamar-authentication-domains=av-domain-list。</p>
<pre>user-login-module-mix-ldap=ldap</pre>	<p>Avamar システムが Avamar 認証と OpenLDAP 認証を使用するよう指定します。また構成には次を含める必要があります。user-login-module=mix と avamar-authentication-domains=av-domain-list。</p>
<pre>avamar-authentication-domains=av-domain-list</pre> <p>ドメインに OpenLDAP 認証と Avamar 認証を使用する Avamar システムの場合 : /, /swclients, /adminclients :</p> <pre>avamar-authentication-domains=/, /swclients, /adminclients</pre>	<p>Avamar システムが Avamar 認証でチェックする内部 Avamar ドメインを指定します。av-domain-list を Avamar ドメインのコンマ区切りリストに置き換えます。また構成には次を含める必要があります。user-login-module=mix および user-login-module-mix-ldap=ldap。</p>

NIS ディレクトリ サービスの追加

NIS ディレクトリ サービスで Avamar ユーザーに認証と許可を提供します。

手順

1. 管理者として Avamar Administrator の root ドメインにログインします。
 - a. Avamar Administrator を起動します。
 - b. [Server] で、ログイン先の Avamar サーバの IP アドレスまたは DNS 名を入力します。

- c. **[User Name]** にユーザー名を入力します。

ユーザー名は、root ドメイン レベルの管理者役割が割り当てられているアカウントのユーザー名である必要があります。

ディレクトリ サービスをすでに構成している場合は、root ドメイン レベルの管理者ロールを持つ LDAP ユーザーのアカウントでログインすることができます。

- d. **[Password]** に、ユーザー アカウントのパスワードを入力します。

- e. **[Domain Name]** で、デフォルトのエントリーであるスラッシュ (/) の一文字を使用して、root ドメインを指定します。

- f. **[ログイン]** をクリックします。

これがこの Avamar サーバへの最初の接続の場合は、**[Accept Server Certificate]** ダイアログ ボックスが開きます。サーバ証明書の詳細を確認し、**[Yes]** をクリックします。

Avamar Administrator ダッシュボードが表示されます。

2. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。

[Administration] ウィンドウが表示されます。

3. **[LDAP Management]** タブをクリックします。

4. **[Directory Service Management]** をクリックします。

[Directory Service Management] ダイアログ ボックスが表示されます。

5. **[Directory Service Management]** ダイアログ ボックスで、**[Add]** をクリックします。

[Adding a new Directory Service] セクションが表示されます。

6. **[NIS]** を選択します。

7. **[Enter a fully qualified domain name]** で、NIS ドメイン名を入力します。

8. **[NIS Domain IP address]** に、NIS サーバーの IP アドレスを入力します。

9. **[Add]** をクリックします。

確認メッセージが表示されます。

10. **[Yes]** をクリックします。

エラー メッセージが表示される場合は、この問題を解決してこのタスクを再試行してください。詳細については、[ディレクトリ サービスの構成中に表示されるエラー メッセージ \(103 ページ\)](#) を参照してください。

正常に実行されたことを示すメッセージが表示されます。

11. **[OK]** をクリックします。

結果

この変更は、mcs (Management Console Server) および emt (EM Tomcat) サービスに適用されます。

必要条件

ディレクトリ サービス グループを Avamar ユーザー情報と関連づけるには、LDAP マップを作成します。手順については、[LDAP マップの追加 \(103 ページ\)](#) を参照してください。

ディレクトリサービスの構成中に表示されるエラー メッセージ

ディレクトリサービスの構成の追加またはテスト中に問題が発生すると、エラー メッセージが表示されます。

次の表で、表示される可能性がある一部のメッセージと、その原因の説明を示します。

表 26 ディレクトリサービスの構成中に表示されるエラー メッセージ

エラー メッセージ	説明
Cannot discover KDC	指定したドメイン情報を使用して、KDC（キー配布センター）を検出できません。
No URL is present	指定したドメインは <code>ldap.properties</code> ファイルにありません。
Parameters are not correct	<code>ldap.properties</code> ファイルにあるディレクトリサービスドメイン情報は無効です。
Client not found in Kerberos database	指定されたユーザー名は無効です。
Pre-authentication information was invalid	指定されたパスワードは正しくありません。
Query fails	指定されたユーザー アカウントは、ディレクトリサービス データベースを読み取るために十分な権限がありません。
Clock skew too great	Avamar サーバ ホストのクロックと、ディレクトリサービス ホストのクロックの差が大きすぎます。
Cannot open LDAP configuration file	<code>ldap.properties</code> ファイルが存在しないか、ファイル権限によりアクセスできません。
Cannot open Kerberos configuration file	<code>krb5.conf</code> ファイルが存在しないか、ファイル権限によりアクセスできません。
GSS initiate failed	認証情報の認証に失敗しました。通常、認証の失敗は逆引き DNS が適切に構成されていないことが理由です。KDC ホストを Avamar サーバの <code>/etc/hosts</code> に追加します。
Cannot get kdc for realm	<code>krb5.conf</code> ファイルで KDC が適切に構成されていません。
Domain <domain> exists in ldap.properties file	指定したドメインは、すでに <code>ldap.properties</code> ファイルに含まれています。

LDAP マップの追加

ディレクトリサービス グループを Avamar ユーザー情報と関連づけるには、LDAP マップを作成します。LDAP マップとは、ユーザーのグループを認証システム、ドメインまたはサブドメイン アクセス リスト、ロールと関連付けるデータベース構成体です。

はじめに

ディレクトリサービスドメインを Avamar の構成に追加します。

手順

1. Avamar Administrator で、[Administration] 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。

2. **[Account Management]** タブをクリックします。
3. **[LDAP Maps]** タブをクリックします。
4. 左パネルの階層ツリーで、ドメインまたはサブドメインを選択し、ディレクトリ サービス グループのアクセス レベルを指定します。
5. **[Actions]** > **[Account Management]** > **[New LDAP Map]** を追加します。
[New LDAP Group Map] ダイアログ ボックスが表示されます。
6. **[LDAP Domains]** リストから、マップするディレクトリ サービス ドメインを選択します。
7. **[Group Search]** ボックスで、マップされることになるグループに特有の検索文字列を入力します。
1文字以上の英数字を意味するワイルドカードとして、アスタリスク (*) を使用することができます。
8. **[Search]** をクリックします。
[Directory Service Authentication] ダイアログ ボックスが表示されます。
9. ディレクトリ サービスのクエリー処理に必要な認証情報を指定します。
認証は、マップされているドメイン以外の別のドメイン経由でも行えますが、これら 2 つのドメインの間に信頼関係がある場合に限られます。
 - a. **[Auth Domain]** リストから、認証に使用するドメインを選択します。
 - b. **[User Name]** ボックスに、ドメインの読み取り権限があるアカウントのユーザー名を入力します。
 - c. **[Password]** ボックスに、ユーザー名のパスワードを入力します。
 - d. **[OK]** をクリックします。

[Directory Service Authentication] ダイアログ ボックスが閉じて、検索が始まります。
[New LDAP Group Map] ダイアログ ボックスの **[Search]** ボタンが **[Stop]** に置き換えられます。

検索を終了させるには、**[Stop]** をクリックします。ディレクトリ サービスの検索には時間が長くかかる場合があります。

検索が完了すると、**[LDAP Groups]** リストにグループが表示されます。
10. **[LDAP Groups]** リストから、マップするグループを選択します。
11. **[Role]** リストから、グループの役割を選択します。
12. **[OK]** をクリックします。
グループはマップされ、**[New LDAP Group Map]** ダイアログ ボックスは閉じます。**[LDAP Maps]** タブでマッピングを確認するには、管理ノードを選択します。

LDAP マップの役割の編集

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[Account Management]** タブをクリックします。
3. **[LDAP Maps]** タブをクリックします。

4. 左パネルの階層ツリーで、ドメインまたはサブドメインを選択します。
ドメインまたはサブドメインのマップが、[LDAP Maps] 領域に表示されます。
5. 編集するマップを選択します。
6. [Actions] > [Account Management] > [Edit LDAP Map] を選択します。
[Edit LDAP Map] ダイアログ ボックスが表示されます。
7. [Role] で、マップに割り当てる新しい役割を選択します。
8. [OK] をクリックします。
マップに新しい役割が割り当てられます。これ以降のすべてのセッションでは、グループメンバーには新しい役割が割り当てられています。

LDAP マップの削除

手順

1. Avamar Administrator で、[Administration] 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. [Account Management] タブをクリックします。
3. [LDAP Maps] タブをクリックします。
4. 左パネルの階層ツリーで、ドメインまたはサブドメインを選択します。
ドメインまたはサブドメインのマップが、[LDAP Maps] 領域に表示されます。
5. 削除するマップを選択します。
6. [Actions] > [Account Management] > [Delete LDAP Map] を選択します。
[Delete LDAP Map] ダイアログ ボックスが表示されます。
7. [Yes] をクリックします。

ディレクトリ サービス プロセスの time-out 値の編集

ディレクトリ サービス プロセスは、ディレクトリ サービスからのレスポンスを最長 5 分待ちます。この後、その試行は破棄され、タイムアウト メッセージが表示されます。time-out 値は編集可能です。

time-out 値は、以下のディレクトリ サービス認証プロセスで使用されます。

- ディレクトリ サービスを通じた認証リクエスト
- Avamar の構成へのディレクトリ サービスの追加
- Avamar の構成でのディレクトリ サービスのテスト

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、admin としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. admin としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```
2. `dpnctl stop mcs` と入力して、mcs (Management Console Server) サービスを停止します。

3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```

4. テキストエディターで `mcserver.xml` を開きます。
5. `<node name="ldap">` ノードを見つけます。
6. `<entry key="ldap_services_timeout_seconds" value="n" />` の値を新しい `time-out` 値（秒単位）に変更します。ここで、`n` は新しい値です。
デフォルト値は 300 秒（5 分）です。
7. 変更を保存して、ファイルを閉じます。
8. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```

9. コマンド シェルを閉じます。

エンタープライズ認証での下位互換性の有効化

非推奨のエンタープライズ認証メカニズムでユーザーを引き続き認証するには、この機能を有効化します。

エンタープライズ認証では、Avamar はホストである Linux オペレーティング システムの PAM (Pluggable Authentication Module) ライブラリを使用して、外部認証データベースにアクセスします。「Avamar 製品セキュリティガイド」で説明されているエンタープライズ認証は非推奨であり、今後のリリースでは打ち切りになる予定です。ユーザーをドメインやクライアントに追加しても、デフォルトではエンタープライズ認証ドメインは選択できません。認証メカニズムとしてエンタープライズ認証を引き続き使用するには、`mcserver.xml` にある **Enterprise Authentication** の選択設定を変更して、ユーザーを追加するときに、エンタープライズ認証の選択を有効化するようにシステムを構成します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin` OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```
2. `dpnctl stop mcs` と入力して、MCS (Management Console Server) サービスを停止します。
3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```
4. テキストエディターで `mcserver.xml` を開きます。
5. `<node name="ldap">` ノードを見つけます。
6. `<entry key="enable_new_user_authentication_selection" value="false" />` の値を `false` から `true` に変更します。

7. 変更を保存して、ファイルを閉じます。
8. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```

9. コマンド シェルを閉じます。

ロール

ロールにより、各ユーザー アカウントに許可される操作が定義されます。

ロールには、次の 3 つのタイプがあります。

- 管理者ロール
- オペレーター ロール
- ユーザー ロール

管理者ロール

管理者はサーバーの管理を行います。

管理者ロールが割り当てられるのは、ドメイン レベルのユーザー アカウントのみです。ドメイン レベルには、最上位 (root) ドメイン、またはその他のドメイン/サブドメインが含まれます。クライアントレベルのユーザー アカウントには、管理者の役割を割り当てることができません。

最上位レベル (root) のドメインのユーザーか、特定のドメインまたはサブドメインに管理者ロールを割り当てることができます。

Avamar 18.2 では、vCenter 管理者という概念が導入されています。このロールは AUI に固有であり、Avamar Administrator には対応するロールはありません。

表 27 管理者ロール

管理者タイプ	説明
root 管理者	最上位 (root) ドメインの管理者は、システムをすべてコントロールする権限を持ちます。このような管理者は、「root 管理者」とも呼ばれます。
ドメイン管理者	root 以外のドメインの管理者は、通常、このガイドで説明するほとんどの機能にアクセス権を持っています。管理者は、通常、ドメインにあるオブジェクトの表示または操作のみを実行できます。ドメイン管理者はドメイン外部にデータを表示することが可能であると思われるかもしれませんが、そのようなアクティビティは禁止されています。グローバルなサーバー機能（例えば、スケジュール設定された操作を停止、または再開する、メンテナンス アクティビティのため、実行時間を変更するなど）へのアクセスは禁止されています。ドメイン管理者： <ul style="list-style-type: none"> • 他のサブドメイン管理者を追加または編集することはできません。 • 割り当て済みロールを変更することはできません。 • パスワードを変更することができます。 ドメイン管理者は、AUI ダッシュボードにアクセスできません。
vCenter 管理者	vCenter 管理者は、ドメイン管理者と同じ機能にアクセスできますが、さらに vCenter ドメイン内の AUI ダッシュボードおよびイベント管理領域にアクセスすることもできます。

オペレーター ロール

一般的にオペレーター ロールは、特定のユーザーにサーバーの特定の領域への制限付きアクセスを許可するために実装され、バックアップおよびリストアの実行、またはステータスの取得やレポートの実行が可能です。このロールによって、管理者以外のスタッフにバックアップ、リストア、レポートといったタスクを柔軟に割り当てることができます。

オペレーター ロールが割り当てられるのは、ドメインレベルのユーザー アカウントのみです。クライアントレベルのユーザー アカウントには、これらのロールを割り当てることができません。サブドメインにユーザー アカウントを追加するには、親ドメイン以上の管理者権限で実行する必要があります。

オペレーター ロールのユーザーは、すべての管理機能にアクセスすることはできません。ログインすると、使用が許可されている機能にアクセスできるインターフェイスが表示されます。

次の表では、4 種類のオペレーター ロールについて説明しています。

表 28 オペレーター ロール

オペレーター タイプ	説明
リストア専用オペレーター	<p>リストア専用オペレーターは、一般的にリストアの実行とアクティビティの監視のみ許可されており、リストアが完了し、エラーが発生していないかを判断します。最上位（ルート）ドメインのリストア専用オペレーターは、サーバー内のあらゆるクライアントのリストアを実行できます。ルート以外のドメインのリストア専用オペレーターは、そのドメイン内のクライアント以外のリストアは実行できません。リストア専用オペレーターは、割り当てられたドメインでバックアップ データのリストアとアクティビティの監視を実行できます。</p> <ul style="list-style-type: none"> デフォルトでは、リストア専用オペレーターは、別の場所へのリストアまたは複数の場所へのリストアを実行できません。このオプションを有効化するには、<code>mcserver.xml</code> ファイルで <code>restore_admin_can_direct_restores</code> 属性を <code>true</code> に設定する必要があります。 デフォルトでは、リストア専用オペレーターは、コマンドラインまたは Avamar Web Restore インターフェイスからバックアップを参照することができません。リストア専用オペレーターに対してこれらのアクティビティを有効化するには、次のような <code>avmgr chgv</code> コマンドを使用して <code>noticketrequired</code> 権限を追加します： <code>avmgr chgv --acnt=location --u=name --ud=auth \ --pv="enabled,read,mclogin,noticketrequired"</code>（ここで、<code>location</code> はオペレーターのサブドメイン、<code>name</code> はユーザーの Avamar ユーザー名、<code>auth</code> はユーザー認証に使用する外部認証システムです）。
バックアップ専用オペレーター	<p>バックアップ専用のオペレーターは一般的に、バックアップの実行と、バックアップが完了してエラーが発生していないかを判断するためのアクティビティの監視のみ許可されています。最上位（root）ドメインのバックアップ専用オペレーターは、サーバー内のあらゆるクライアントまたはグループのバックアップを実行できます。root 以外のドメインのバックアップ専用オペレーターは、そのドメイン内のクライアントまたはグループのバックアップのみ実行できます。バックアップ専用オペレーターは、割り当てられたドメインでクライアントまたはグループのオン デマンド バックアップを実行できるほか、アクティビティを監視できます。</p> <ul style="list-style-type: none"> デフォルトでは、バックアップ専用オペレーターは、別の場所へのリストアまたは複数の場所へのリストアを実行できません。このオプションを有効化するには、<code>mcserver.xml</code> ファイルで <code>restore_admin_can_direct_restores</code> 属性を <code>true</code> に設定する必要があります。 デフォルトでは、バックアップ専用オペレーターはコマンドラインでバックアップを実行できません。バックアップ専用オペレーターに対してコマンドライン バックアップを有効化するには、次のコマンドを使用して <code>noticketrequired</code> 権限を追加します。 <code>avmgr chgvavmgr chgv --acnt=location --u=name --ud=auth \ --pv="enabled,read,mclogin,backup,noticketrequired"</code>（ここで、<code>location</code> はオペレーターのサブドメイン、<code>name</code> はユーザーの Avamar ユーザー名、<code>auth</code> はユーザー認証に使用する外部認証システムです）。

表 28 オペレーター ロール (続き)

オペレーター タイプ	説明
バックアップ/リストア オペレーター	<p>バックアップ/リストアのオペレーターは、一般的にバックアップ、またはリストアの実行とアクティビティの監視のみ許可されており、バックアップ/リストアが完了し、エラーが発生していないかを判断します。他のドメイン ユーザー アカウントに割り当てられた役割と同様に、最上位 (root) ドメインのバックアップ/リストア オペレーターは、サーバー内のあらゆるクライアントまたはグループのバックアップとリストアを実行できます。root 以外のドメインのバックアップ/リストア オペレーターは、そのドメイン内のクライアントまたはグループのバックアップとリストアのみ実行できます。バックアップ/リストア オペレーターは、割り当てられたドメイン内で次のタスクを実行できます。</p> <ul style="list-style-type: none"> • クライアントまたはグループのオン デマンド バックアップの実行。 • リストアの実行。 • アクティビティの監視。 <p>デフォルトでは、バックアップ/リストア オペレーターは、コマンドラインでも、または Avamar Web Restore インターフェイスを使用しても、バックアップを参照できません。そして、コマンドラインでバックアップを実行することはできません。これらのアクティビティを有効化するには、次のような avmgr chgv コマンドを使用して noticketrequired 権限を追加します：<code>avmgr chgv --acnt=location --u=name --ud=auth \ --pv="enabled,read,mclogin,backup,noticketrequired"</code> (ここで、location はオペレーターのサブドメイン、name はユーザーの Avamar ユーザー名、auth はユーザー認証に使用する外部認証システムです)。</p>
アクティビティ オペレーター	<p>アクティビティ オペレーターは、一般的にバックアップとリストア アクティビティの監視とレポートの作成のみ許可されています。最上位 (ルート) ドメインのアクティビティ オペレーターは、すべてのドメインとサブドメインでのバックアップとリストア アクティビティを表示すること、またはレポートを作成することができます。ルート以外のドメインのアクティビティ オペレーターは、そのドメイン以外のバックアップとリストア アクティビティは表示することも、レポートを作成することもできません。アクティビティ オペレーターは、割り当てられたドメイン内で次のタスクを実行できます。</p> <ul style="list-style-type: none"> • アクティビティの監視。 • グループ ステータス サマリーの表示。 • Activity Report の表示。 • Replication Report の表示。

ユーザーの役割

ユーザーの役割により、ユーザー アカウントに許可される操作が特定のクライアントに制限されます。いずれかのユーザー ロールに割り当てられたユーザーは、Avamar Administrator、AUI、Avamar Client Manager、Avamar クライアント Web UI にログインできません。

注

Avamar Administrator では、クライアントにユーザー アカウントを追加できる機能を提供していません。ただし、Avamar Web ユーザー インターフェイス (AUI) からクライアントにユーザー アカウントを追加することはできません。

次の表では、4 種類のユーザー ロールについて説明しています。

表 29 ユーザーの役割

ユーザー タイプ	説明
バックアップ専用ユーザー	この役割を割り当てられたユーザーは、 <code>avtar</code> コマンドラインを使用して、クライアントから直接バックアップを開始できます。
リストア（読み取り）専用ユーザー	この役割を割り当てられたユーザーは、 <code>avtar</code> コマンドラインまたは MCS (Management Console Server) Web サービスを使用して、クライアントから直接リストアを開始できます。
バックアップ/リストア ユーザー	この役割を割り当てられたユーザーは、 <code>avtar</code> コマンドラインまたは MCS Web サービスを使用して、クライアントから直接バックアップおよびリストアを開始できます。
リストア（読み取り）専用/ファイル許可のスキップ	リストア時にオペレーティング システム ファイルの権限が無視される点を除いて、その他はリストア（読み取り）専用ユーザーの役割と同じです。このユーザーは、Avamar クライアントのために格納されたすべてのファイルをリストアできます。この役割は、Avamar 内部認証を使用してユーザーを認証する場合に限って使用できます。次の条件が両方とも正しい場合のみ、Windows クライアントのユーザー アカウントにはこの役割を割り当てます。これにより、リストアをトラブルなく確実に実行できます。 <ul style="list-style-type: none"> ユーザーは Avamar 内部認証を使用して認証される。 ユーザーは、Avamar クライアント Web UI にアクセスする必要はありません。

ロール ベースのアクセス制御と AUI

AUI は、Web ベースのインターフェイスにアクセスするユーザー向けにロール ベースのセキュリティを提供します。

ユーザーが AUI にログインするたびに、セキュリティ サブシステムによって、ユーザーと、割り当てられたすべてのロールおよびドメインがマッピングされます。Avamar では、この情報を使用して、ユーザーのアクセスレベルに対応する管理領域と URL のテーブルを構築します。

ログインした後、AUI はユーザーのロールのデフォルト ページを表示し、ユーザーのアクセスレベルに対応していないすべてのコントロールと領域を非表示にします。たとえば、バックアップ専用オペレーターには、ナビゲーション ペインの **[Asset Management]** および **[Activity]** 領域が表示されますが、サーバー管理領域は表示されません。

ユーザーがどのような方法であっても AUI 領域に移動するたびに、セキュリティ サブシステムによってアクセス テーブルに対する受信リクエストがチェックされ、それに応じてリクエストが許可または拒否されます。AUI は、不正な領域へのアクセス試行をすべて再ルーティングします。

次の表は、AUI 内の指定された各機能パネルにアクセスできるユーザーのロールを示しています。

表 30 管理者ユーザー ロールによってアクセスできる AUI 機能パネル

AUI 機能パネル	ルート管理者	ドメイン管理者	vCenter 管理者
[Dashboard]	可	不可	可
[Asset Management]	可	可 ^a	可 ^a
[Asset Management] Domain	可	可 ^a	可 ^a

表 30 管理者ユーザー ロールによってアクセスできる AUI 機能パネル (続き)

AUI 機能パネル	ルート管理者	ドメイン管理者	vCenter 管理者
[Asset Management] Backup	可	可 ^a	可 ^a
[Asset Management] Restore	可	可 ^a	可 ^a
[Backup Policy]	可	可 ^a	可 ^a
[Advanced Policy]	可	可 ^a	可 ^a
[Replication Policy]	可	不可	不可
[Cloud Tier Policy]	可	不可	不可
[Setting]	可	可 ^a	可 ^a
[Proxy Management]	可	可 ^a	可 ^a
[System]	可	可 ^a	可 ^a
[Activity]	可	可 ^a	可 ^a
[Event]	可	不可	可 ^a

a. (指定されたドメイン内)

表 31 オペレーター ユーザー ロールによってアクセスできる AUI 機能パネル

AUI 機能パネル	バックアップ/リストア オペレーター	バックアップ専用 オペレーター	リストア専用オペ レーター	アクティビティ オペ レーター
[Dashboard]	不可	不可	不可	不可
[Asset Management]	可	可	可	不可
[Asset Management] Domain	不可	不可	不可	不可
[Asset Management] Backup	可	可	不可	不可
[Asset Management] Restore	可	不可	可	不可

表 31 オペレーター ユーザー ロールによってアクセスできる AUI 機能パネル (続き)

AUI 機能パネル	バックアップ/リストア オペレーター	バックアップ専用オペレーター	リストア専用オペレーター	アクティビティ オペレーター
[Backup Policy]	不可	不可	不可	不可
[Advanced Policy]	不可	不可	不可	不可
[Replication Policy]	不可	不可	不可	不可
[Cloud Tier Policy]	不可	不可	不可	不可
[Setting]	不可	不可	不可	不可
[Proxy Management]	不可	不可	不可	不可
[System]	不可	不可	不可	不可
[Activity]	可	可	可	可
[Event]	不可	不可	不可	不可

ドメインへのユーザーの追加

ユーザー アカウントが、Avamar 内部認証または非推奨のエンタープライズ認証システムを使用して認証されている際に、ドメインにユーザー アカウントを追加することが可能です。

既存のディレクトリ サービスを使用して認証したユーザーを追加する際の詳細については、[LDAP ディレクトリ サービス認証を使用するための準備 \(90 ページ\)](#) を参照してください。

手順

1. [ロール \(107 ページ\)](#) をレビューして、このユーザーに正しい役割を割り当てることを確認します。
2. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから **[Setting]** をクリックします。
[Setting] パネルが表示されます。
3. **[User]** タブをクリックします。
4. 左パネルの **[Domain]** ツリーで、新しいユーザーのドメインを選択します。

注

MC_RETIRED ドメインにユーザー アカウントを追加することはできません。

5. **[Add]** をクリックします。
[User Management] ウィンドウが表示されます。
6. (オプション) **[Authentication System]** リストから、認証システムを選択します。

通常では、[**Axion Authentication System**]（内部システム）が選択済みとなっており、[**Authentication System**] リストはグレー表示されます。このステップは、エンタープライズ認証システムを選択する機能が現在有効になっていないことを示しています。

「Avamar 製品セキュリティ ガイド」で説明されているエンタープライズ認証システムは非推奨であり、今後のリリースで打ち切りになる予定です。ただし、このリリースでは使用することは可能です。エンタープライズ認証システムを選択する機能を有効にするには、[エンタープライズ認証での下位互換性の有効化](#)（106 ページ）で説明される手順を完了してください。

エンタープライズ認証よりも強固な選択肢については、[LDAP ディレクトリ サービス認証を使用するための準備](#)（90 ページ）で説明されている方法を使用してください。

7. [**User Name**] ボックスに、新しいユーザー名を入力します。

ユーザー名は、次の要件を満たしている必要があります。

- エンタープライズ認証を使用する場合、このオプションにはそのシステムで割り当てられたユーザー名を入力する必要があります。
- ユーザー名は 31 文字を超えることはできません。
- ユーザー名には、次の文字のいずれも含めることができません：~!@\$%^&(){}[]|,`;'#\/:*?<>'"&.

8. [**Role**] リストから、ユーザーのロールを選択します。

9. [**Password**] ボックスに、ユーザーのパスワードを入力します。

パスワードは大文字と小文字を区別し、次の要件を満たしている必要があります。

- パスワードは、6～31 文字の長さである必要があります。
- パスワードに使用できる文字は、英数字、ハイフン、ピリオド、アンダースコアのみです。
- パスワードには、少なくともアルファベット文字を 1 文字含める必要があります。

このフィールドはエンタープライズ認証では使用されません。

10. [**Confirm Password**] ボックスに、パスワードを再入力します。

このフィールドはエンタープライズ認証では使用されません。

11. [**OK**] をクリックします。


確認メッセージが表示されます。

ユーザー情報の編集

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Setting**] をクリックします。
[**Setting**] パネルが表示されます。
2. [**User**] タブをクリックします。
3. 左パネルの [**Domain**] ツリーで、ユーザーが所在しているドメインを選択します。
4. ユーザーを選択します。
5. (オプション) ユーザーのロールを変更します。
 - a. [**Edit**] をクリックします。

[**User Management**] ウィンドウが表示されます。

- b. **[Role]** リストから、ユーザーのロールを選択します。
- c. **[OK]** をクリックします。
確認メッセージが表示されます。
6. (オプション) ユーザーのパスワードを変更します。
 - a. オーバーフローメニュー () をクリックして、**[Edit]** します。
 - b. **[Edit Password]** をクリックします。
[User Management] ウィンドウが表示されます。
 - c. **[Password]** ボックスと **[Confirm Password]** ボックスの両方に、新しいパスワードを入力します。
 - d. **[OK]** をクリックします。
確認メッセージが表示されます。

ユーザーの削除

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Setting]** をクリックします。
[Setting] パネルが表示されます。
2. **[User]** タブをクリックします。
3. 左パネルの **[Domain]** ツリーで、ユーザーが所在しているドメインを選択します。
4. ユーザーを選択します。
5. **[Delete]** をクリックします。
確認メッセージが表示されます。
6. **[Yes]** をクリックします。
再度確認メッセージが表示されます。

第 6 章

バックアップ

本章は、次のトピックで構成されています。

- [オン デマンド バックアップについて](#) 116
- [オン デマンド バックアップの実行](#) 116
- [\[Policy\] ウィザードを使用したバックアップのスケジュール設定](#) 117
- [バックアップのモニタリング](#) 146
- [バックアップのキャンセル](#) 147
- [完了したバックアップの管理](#) 147

オン デマンド バックアップについて

各クライアントのオン デマンド バックアップ、つまりバックアップ ポリシーを実行できます。

オン デマンド バックアップとは、Avamar クライアント コンピューターのデータの 1 回限りのバックアップです。Avamar クライアント ソフトウェアをインストールした後すぐに、クライアントの最初のバックアップを作成するために、オン デマンド バックアップを実行することが必要になる場合があります。システム保守、ソフトウェアのインストール、ソフトウェア アップグレードを実行する前にも、オン デマンド バックアップを実行します。

Avamar サーバでバックエンドストレージに Data Domain を使用している場合、オン デマンド バックアップはデフォルトで Data Domain に書き込まれます。

オン デマンド バックアップの実行

既存のスケジュールとバックアップ ポリシーから独立しているクライアント バックアップを実行できます。

次のプラグ イン タイプに対して、AUI を使用してオン デマンド バックアップを実行することができます。

- VMware イメージ
- DB2
- Linux ファイル システム
- Microsoft SQL
- Microsoft Hyper-V
- Microsoft Exchange
- Microsoft Windows ファイル システム
- NDMP
- Oracle

このリストに含まれていないその他すべてのプラグ イン タイプについては、Avamar Administrator を使用します。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから **[Asset Management]** をクリックします。

[Asset Management] ウィンドウが表示されます。

2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストで、バックアップするクライアント コンピューターを選択します。

ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。

4. **[BACKUP]** をクリックします。

Backup ウィザードが表示されます。**[Plugin]** パネルで、クライアント上のプラグ インのリストが表示されます。

5. **[Plugins]** パネルで、プラグ インを選択してから、バックアップするデータの隣にあるチェックボックスをオンにします。
6. **[NEXT]** をクリックします。

[Basic Configuration] ウィンドウが表示されます。

7. バックアップの保存ポリシー設定を選択します。
 - ある特定の時間が経過した後に、Avamar サーバからこのバックアップを自動的に削除する場合は、[Retention period] を選択します。保存期間の日数、週数、月数、年数を指定します。
 - ある特定のカレンダー日付に、Avamar サーバからこのバックアップを自動的に削除する場合は、[End date] を選択し、カレンダーでその日付を探します。
 - このクライアントが Avamar サーバでアクティブである限り、このバックアップを保持する場合は、[No end date] を選択します。
8. [Avamar encryption method] リストから、バックアップ中にクライアントと Avamar サーバ間のデータ転送に使用する暗号化方式を選択します。

クライアント/サーバ間の接続における暗号化テクノロジーおよびビットの強度は、クライアントのオペレーティング システムおよび Avamar サーバのバージョンをはじめ、さまざまな要因によって異なります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。
9. [Optionally select a proxy to perform backup] リストで、プロキシを選択します。

デフォルト設定は [Automatic] であり、これにより Avamar サーバはこの操作に最適なプロキシを選択できます。
10. [NEXT] をクリックします。

[More Options] ウィンドウが表示されます。
11. プラグ イン オプションを設定します。各オプションの詳細については、各プラグ インのユーザーガイドを参照してください。
12. (オプション) [Show Advanced Options] スイッチをオンにして、詳細な構成オプションを表示します。

各オプションの詳細については、各プラグ インのユーザー ガイドを参照してください。
13. [FINISH] をクリックします。

[Policy] ウィザードを使用したバックアップのスケジュール設定

スケジュール設定されたバックアップは自動的に実行され、バックアップが継続的に実行されるようにします。バックアップを毎日、毎週、毎月実行するようにスケジュール設定できます。

[Policy] ウィザードを使用して、バックアップのポリシーを作成することで、バックアップをスケジュール設定できます。

[Policy] ウィザードで、次の手順を実行します。

手順

1. 新しいバックアップ ポリシーにメンバーを割り当てます。
2. 新しいバックアップ ポリシーにデータセットを割り当てます。

データセットを作成するには、[Policy] ウィザードを使用するか、[Settings] > [Dataset] > [Add] を選択します。
3. 新しいバックアップ ポリシーをスケジュールに割り当てます。

スケジュールを作成するには、[Policy] ウィザードを使用するか、[Settings] > [Schedule] > [Add] を選択します。
4. 新しいバックアップ ポリシーに保存ポリシーを割り当てます。

保存ポリシーを作成するには、[Policy] ウィザードを使用するか、
[Settings] > [Retention] > [Add] を選択します。

5. バックアップ ポリシーのスケジュール設定を有効にします。

データセット カタログ

Avamar システムには、事前構成された一連のデータセットがデフォルトで含まれています。これらのデータセットをクライアントのスケジュール設定されたバックアップで使用できます。または、カスタムデータセットを作成することができます。

注

Avamar サーバーで事前構成されているインストール済みのデータセットの設定を編集したり、削除したりすることはできません。ユーザー定義のデータセットの変更は、選択したデータセットを使用する既存のバックアップ ポリシーに影響します。ユーザー定義のデータセットの設定を編集する場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

Base Dataset

Base Dataset では、一連の最小、つまりベースラインのバックアップ要件が定義されます。Base Dataset の初期設定は次のとおりです。

- ソース データ プラグ インを使用しない
- 除外または包含リストの明示的なエントリーはない

このデータセットは基本的に空です。

Default Dataset

Default Dataset では、デフォルト グループの永続的なバックアップ選択を定義します。Default Dataset の初期設定は次のとおりです。

- 利用可能なすべてのソース データ プラグ イン
- 除外または包含リストの明示的なエントリーはない

これにより、デフォルト グループのすべてのメンバーは、プラットフォームのタイプにかかわらず、クライアント コンピューターをバックアップできます。

次の表にリストされたディレクトリは、除外リストに明示的に指定されていない場合でも、その性質上、すべてのバックアップから除外されます。

表 32 Default Dataset バックアップから除外されるディレクトリ

除外されるディレクトリとファイル	説明
.snapshot/	NetApp のマウント
VARDIR/f_cache.dat	ローカル avtar ファイル キャッシュ
VARDIR/p_cache.dat	ローカル avtar は「is present」キャッシュ

UNIX Dataset

UNIX Dataset は、AIX、FreeBSD、HP-UX、Linux、Solaris の各クライアント用に最適化されています。UNIX Dataset の初期設定は次のとおりです。

- AIX、FreeBSD、HP-UX、Linux、Macintosh OS X、Solaris のファイル システム ソース データ プラグ インのみ

- さまざまな temp ディレクトリ (/tmp、/var/tmp、/usr/tmp)、コア ダンプ ファイル (core)、ローカル キャッシュ ファイル (*cache.dat、*scan.dat) の明示的な除外
- 包含リストの明示的なエントリーはない

次の表にリストされたディレクトリは、除外リストに明示的に指定されていない場合でも、その性質上、すべての UNIX Dataset バックアップから除外されます。

表 33 UNIX Dataset バックアップから除外されるディレクトリ

除外されるディレクトリとファイル	説明
.snapshot/	NetApp のマウント
VARDIR/f_cache.dat	ローカル avtar キャッシュ ファイル
VARDIR/p_cache.dat	ローカル avtar キャッシュ ファイル
/proc	リストアできない疑似ファイル システム
/dev	root として実行中でない場合のみ除外
/devices	Solaris の場合のみ除外

Windows Dataset

Windows Dataset は、Microsoft Windows クライアント用に最適化されています。Windows Dataset の初期設定は次のとおりです。

- Windows ファイル システム ソース データ プラグ インのみ
- 除外または包含リストの明示的なエントリーはない

次の表にリストされたディレクトリは、除外リストに明示的に指定されていない場合でも、その性質上、すべての Windows Dataset バックアップから除外されます。

表 34 Windows Dataset バックアップから除外されるディレクトリ

除外されるディレクトリとファイル	説明
.snapshot/	NetApp のマウント
VARDIR/f_cache.dat	ローカル avtar キャッシュ ファイル
VARDIR/p_cache.dat	ローカル avtar キャッシュ ファイル
以下のレジストリ キーによって参照されるすべてのファイル。 <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control \BackupRestore \FilesNotToBackup • HKEY_CURRENT_USER\SYSTEM \CurrentControlSet\Control \BackupRestore \FilesNotToBackup 	Microsoft によりバックアップ対象からはずすよう明示的に指定されたファイル
インターネット一時ファイル	Internet Explorer 一時ファイル
outlook.ost	Outlook ローカル キャッシュ ファイル

表 34 Windows Dataset バックアップから除外されるディレクトリ (続き)

除外されるディレクトリとファイル	説明
outlook*.ost	Outlook ローカル キャッシュ ファイル

VMware Image Dataset

VMware Image Dataset は、イメージ バックアップで VMware エンティティを保護するためのデフォルトのデータセットです。さまざまな点において、VMware Image Dataset は他のデータセットより簡素化されています。

- 使用可能なソース データ プラグ インは、Linux と Windows 仮想ディスクのみです。いずれもデフォルトで選択されています。
- **[Select Files and/or Folders]** オプションのほか、**[Exclusions]** タブ、**[Inclusions]** タブは無効になっています。
- 更新ブロック追跡は、組み込みの `utilize_changed_block_list=true` プラグ イン オプションのステートメントを使用して、デフォルトで有効化されています。

VMware Image Dataset を使用して、VMware エンティティをバックアップする際の詳細については、「Avamar for VMware ユーザー ガイド」を参照してください。

データセットの追加

データセットでは、スケジュール設定されたバックアップに含まれるデータと、バックアップに使用するオプションを指定します。1 個のクライアントまたはクライアントのグループで実行するスケジュール設定されたバックアップ用に、少なくとも 1 個のデータセットを作成してください。クライアント データを分離するには、複数のデータセットを作成します。

注

Avamar サーバで、バックエンド ストレージに Data Domain を使用している場合、Data Domain システムがデフォルトのバックアップ ストレージ場所になります。**[Options]** タブでシステムを変更することができます。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Settings]** をクリックします。
[Setting] パネルが表示されます。
2. **[Dataset]** タブをクリックします。
3. **[ADD]** をクリックします。
[Create Dataset] ウィンドウが表示されます。
4. **[Dataset Name]** フィールドに、データセットの名前を入力します。
名前には、英数字 (A-Z、a-z、0-9) および次の特殊文字を含めることができます。ピリオド (.)、ハイフン (-)、下線 (_)。Unicode 文字または次に示す特殊文字は使用しないでください。` ~ ! @ # \$ % ^ & * () = + [] { } | \ / ; : ' " < > , ?
5. **[Plugins]** リストから、バックアップに使用するプラグ インを選択します。
6. **[Options]** タブをクリックして、グラフィカル コントロールを使用するか、オプション名と値をテキスト エントリーとして入力することにより、プラグ イン オプションを設定します。
(オプション) **[Show Advanced Options]** スイッチをオンにして、詳細な構成オプションを表示します。

プラグ イン オプションを使用すると、データセットの動作をさらに細かくカスタマイズできます。各プラグ インのユーザー ガイドには、プラグ インで使用できるオプションが詳しく説明されています。

7. **[Source Data]** タブをクリックして、このデータセットにデータを提供するソース データ プラグ インを定義します。
 - クライアントにインストールされているすべてのプラグ インのデータを含める場合は、**[Select All Data for All Local File Systems]** を選択します。
 - 特定のプラグ インからのデータのみを含め、データセットを特定のデータだけに制限するには、次の手順を実行します。
 - a. **[Plugins]** リストから、バックアップに使用するプラグ インを選択します。追加のオプションが **[Select Plug-In Type]** リストの下に表示されます。
 - b. プラグ インで利用可能なすべてのデータをバックアップするには、次の手順を実行します。
 - オプションを選択します。
 - **[Select Files and/or Folders]** を選択して、データへのパスを入力します。
 - c. バックアップするデータへのパスを入力するには、**[File/Folder Path]** フィールドにパスを入力し、**[Add]** をクリックします。
データセットのデータへのパスを指定することで、スケジュール設定されたバックアップをデータのセットに制限します。パスを入力するときは、次のルールが適用されます。
 - ファイル システム プラグ インを使用している場合、パス内で最初に表示されるアスタリスク(*)はフォルダーのワイルドカードとしてみなされます。例えば、Windows コンピューター上のすべてのユーザーで My Documents フォルダーを指定するには、**C:\Documents and Settings*\My Documents** と入力します。
 - Macintosh 上のすべてのユーザーで Documents フォルダーを指定するには、**/Users/*/Documents** と入力します。
 - データパスを指定する場合、最初のアスタリスク(*)のみがフォルダーのワイルドカードとみなされます。2つ目以降のアスタリスクは文字どおり解釈されます。
 - パスには、英数字(A-Z、a-z、0-9)と、ワイルドカードとしてアスタリスク(*)を含めることができます。データパスには、次に示す文字を使用しないでください。
~!@#\$%^&(){}[]|,`';#: *?<>'"&.

8. **[Submit]** をクリックします。

データセットの変更は、次のスケジュール設定されたバックアップから有効になります。すでに開始されたバックアップまたは完了したバックアップには影響はありません。

データセットの編集

データセットを編集するには、次の手順を実行します。

注

Avamar サーバーで事前構成されているインストール済みのデータセットの設定を編集したり、削除したりすることはできません。ユーザー定義のデータセットの変更は、選択したデータセットを使用する既存のバックアップ ポリシーに影響します。ユーザー定義のデータセットの設定を編集する場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Dataset] タブをクリックします。
構成済みのデータセットのリストが表示されます。
3. リストから、編集するデータセットを選択して [EDIT] をクリックします。
[Edit DataSet] ウィンドウが表示されます。
4. [Edit DataSet] ウィンドウで、次のタスクを完了します。
 - a. [Plugins] リストから、バックアップに使用するプラグ インを選択します。
 - b. [Option] タブで、グラフィカル コントロールを使用するか、オプション名と値をテキスト エントリーとして入力することにより、プラグ イン オプションを編集します。
(オプション) [Show Advanced Options] スイッチをオンにして、詳細な構成オプションを表示します。

プラグ イン オプションを使用すると、データセットの動作をさらに細かくカスタマイズできます。各プラグ インのユーザー ガイドには、プラグ インで使用できるオプションが詳しく説明されています。
 - c. [Source Data] タブをクリックして、このデータセットにデータを提供するソース データ プラグ インを定義します。
 - クライアントにインストールされているすべてのプラグ インのデータを含める場合は、[Select All Data for All Local File Systems] を選択します。
 - 特定のプラグ インからのデータのみを含め、データセットを特定のデータだけに制限するには、次の手順を実行します。
 - a. [Plugins] リストから、バックアップに使用するプラグ インを選択します。
追加のオプションが [Select Plug-In Type] リストの下に表示されます。
 - b. プラグ インで利用可能なすべてのデータをバックアップするには、次の手順を実行します。
 - オプションを選択します。
 - [Select Files and/or Folders] を選択して、データへのパスを入力します。
 - c. バックアップするデータへのパスを入力するには、[File/Folder Path] フィールドにパスを入力し、[Add] をクリックします。
データセットのデータへのパスを指定することで、スケジュール設定されたバックアップをデータのセットに制限します。パスを入力するときは、次のルールが適用されます。
 - ファイル システム プラグ インを使用している場合、パス内で最初に表示されるアスタリスク (*) はフォルダーのワイルドカードとみなされます。例えば、Windows コンピューター上のすべてのユーザーで My Documents フォルダーを指定するには、C:\Documents and Settings*\My Documents と入力します。
 - Macintosh 上のすべてのユーザーで Documents フォルダーを指定するには、/Users/*/Documents と入力します。
 - データパスを指定する場合、最初のアスタリスク (*) のみがフォルダーのワイルドカードとみなされます。2 つ目以降のアスタリスクは文字どおり解釈されません。

- パスには、英数字 (A-Z, a-z, 0-9) と、ワイルドカードとしてアスタリスク (*) を含めることができます。データパスには、次に示す文字を使用しないでください。~!@#\$%^&(){}[]|,` ;#: *?<>' "&。
- クライアントにインストールされているすべてのプラグインのデータを含める場合は、**[Select All Data for All Local File Systems]** を選択します。
- 特定のプラグインからのみのデータを含め、データセットを特定のデータだけに制限するには、次の手順を実行します。
 - a. **[Plugins]** リストから、バックアップに使用するプラグインを選択します。追加のオプションが **[Select Plug-In Type]** リストの下に表示される場合があります。
 - b. プラグインで利用可能なすべてのデータをバックアップするには、次の手順を実行します。
 - オプションを選択します。
 - **[Select Files and/or Folders]** を選択し、バックアップに含めるデータを参照します。
 - c. バックアップするデータへのパスを入力するには、**[File/Folder Path]** フィールドにパスを入力し、**[Add]** をクリックします。データセットのデータへのパスを指定することで、スケジュール設定されたバックアップをデータのセットに制限します。データへのパスは、参照または入力することができます。パスを入力する際にはいくつかのルールが適用されます。

ファイルシステムプラグインを使用している場合は、パス内で最初に表示されるアスタリスク (*) はフォルダーのワイルドカードとみなされます。例えば、Windows コンピューター上のすべてのユーザーで My Documents フォルダを指定するには、`c:\Documents and Settings*\My Documents` と入力します。Macintosh 上のすべてのユーザーで Documents フォルダを指定するには、`/Users/*/Documents` と入力します。

通知

データパスを指定する場合、最初のアスタリスク (*) のみがフォルダーのワイルドカードとみなされます。2 つ目以降のアスタリスクは文字どおり解釈されます。

パスには、英数字 (A-Z, a-z, 0-9) と、ワイルドカードとしてアスタリスク (*) を含めることができます。データパスには、次に示す文字を使用しないでください。~!@#\$%^&(){}[]|,` ;#: *?<>' "&。

5. **[Submit]** をクリックします。

データセットの変更は、次のスケジュール設定されたバックアップから有効になります。すでに開始されたバックアップまたは完了したバックアップには影響はありません。

データセットの削除

データセットを削除するには、次の手順を実行します。

はじめに

データセットがクライアントまたはグループに現在割り当てられていないことを確認します。クライアントまたはグループに割り当てられているデータセットは削除できません。

注

Avamar サーバーで事前構成されているインストール済みのデータセットの設定を編集したり、削除したりすることはできません。ユーザー定義のデータセットの変更は、選択したデータセットを使用する既存のバックアップ ポリシーに影響します。ユーザー定義のデータセットの設定を編集する場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Settings**] をクリックします。
2. [**Dataset**] タブをクリックします。
構成済みのデータセットのリストが表示されます。
3. リストから、削除するデータセットを選択して [**DELETE**] をクリックします。
確認のメッセージが表示されます。
4. [**YES**] をクリックします。

スケジュールの管理

このセクションでは、スケジュールを管理する方法について説明します。

AUI Policy ウィザードを使用したバックアップのスケジュール設定

スケジュール設定されたバックアップは自動的に実行され、バックアップが継続的に実行されるようにします。バックアップを毎日、毎週、毎月実行するようにスケジュール設定できます。

Policy ウィザードを使用してバックアップ ポリシーを作成することにより、バックアップのスケジュールを設定できます。

[**Policy**] ウィザードで次の手順を実行します。ポリシー、データセット、スケジュール、および保存設定の詳細については、「Avamar Administration Guide」を参照してください。

手順

1. 新しいバックアップ ポリシーにメンバーを割り当てます。
2. 新しいバックアップ ポリシーにデータセットを割り当てます。
データセットを作成するには、[**Policy**] ウィザードを使用するか、**[Settings] > [Dataset] > [Add]** を選択します。
3. 新しいバックアップ ポリシーをスケジュールに割り当てます。
スケジュールを作成するには、[**Policy**] ウィザードを使用するか、**[Settings] > [Schedule] > [Add]** を選択します。
4. 新しいバックアップ ポリシーに保存ポリシーを割り当てます。
保存ポリシーを作成するには、[**Policy**] ウィザードを使用するか、**[Settings] > [Retention] > [Add]** を選択します。
5. バックアップ ポリシーのスケジュール設定を有効にします。

スケジュール

スケジュールは再使用可能なオブジェクトであり、バックアップ、カスタム イベント プロファイルのメール通知、ポリシー ベースのレプリケーションが実行される時間を制御します。

スケジュール タイプ

Avamar スケジュールを設定すれば、次の表に示すいずれかのインターバルでシステム アクティビティを繰り返して実行することができます。

表 35 スケジュール タイプ

スケジュールタイプ	説明
Daily	システム アクティビティを日に 1 回以上、毎日繰り返します。Daily スケジュールでは、ジョブの重複を防ぐため、アクティビティの期間を制限する必要があります。
Weekly	システム アクティビティを週に 1 日以上、毎週繰り返します。Weekly スケジュールでは、最も早いアクティビティの開始時刻、およびアクティビティの停止時刻（実行中でも）を定義する必要があります。
Monthly	システム アクティビティを特定のカレンダー日付または毎月の指定曜日（毎月の第 1 日曜日など）に繰り返します。Monthly スケジュールでは、最も早いアクティビティの開始時刻、およびアクティビティの停止時刻（実行中でも）を定義する必要があります。

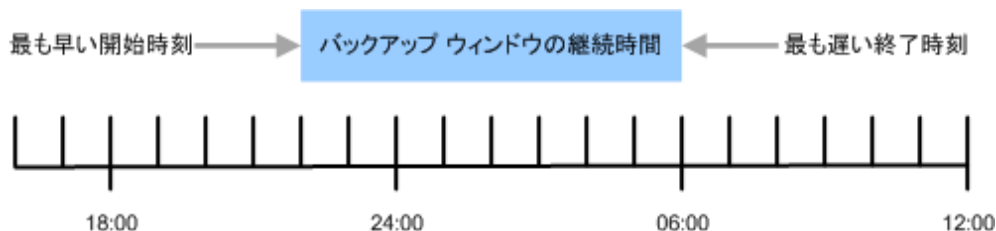
開始時間、終了時間、継続期間のスケジュール設定

スケジュールを作成する際には、スケジュールを有効にする時期、および中止する時期も定義します。例えば、特定の開発プロジェクトに使用するクライアント コンピューターが将来の特定の日付で使用停止になるとわかっていると仮定します。バックアップに対しては、特定の日付に自動的にバックアップを停止するスケジュールを作成できます。同様に、大規模なサイトを管理している場合、事前にスケジュールを作成してバックアップ ポリシーに割り当てることで、指定した期日にスケジュールを有効にすることができます。このようなバックアップ ポリシー バックアップは、スケジュールが有効になるまで実行されません。

スケジュール設定されたアクティビティが 2 日間に及ぶことも多いので、Avamar はスケジュールにより開始されるどのアクティビティにも、十分なバックアップ ウィンドウの時間を割り当てます。これは重要なことですので理解しておいてください。例えば、最も早い開始時刻が午後 10 時、終了時刻が翌朝の午前 6 時、有効期日が今年の 12 月 31 日のスケジュールがあるとします。12 月 31 日の夜にアクティビティは予定どおりに開始され、完了するまで実行されます。通常は翌年の 1 月 1 日の朝までかかります。ただし、このスケジュールでは、1 月 1 日以降、スケジュール設定された新しいアクティビティは開始されません。

次の図では、デフォルトのスケジュールの初期設定を使用して、スケジュールの開始時刻、終了時刻、継続時間がどのように相互に関係するかを示します。

図 12 開始時間、終了時間、継続期間のスケジュール設定



このシステム アクティビティは午後 10 時（22:00）に開始され、翌日午前 6 時（06:00）まで実行できます。有効な時間は 8 時間です。

実際には、スケジュール済みアクティビティが定刻に開始または終了することはほとんどありません。サーバー ロードが実際の開始時刻に影響し、アクティビティの複雑さが実際の終了時刻に影響しま

す。アクティビティの複雑さには、バックアップ対象の新しいクライアント データの量、開始するバックアップ ポリシー バックアップの数、送信する必要のあるメールの数などが含まれます。

スケジュールの開始時間を指定すると、システム アクティビティを開始できる最も早い時点としてその時刻が設定されます。また、終了時間とはシステム アクティビティが終了する、可能な範囲で最も遅い時間になります。

スケジュール タイムゾーン

スケジュールの作成または編集を行う際、すべての時間は **Avamar Administrator** クライアントのローカル タイムゾーンに対応して表示されます。例えば、太平洋標準時で午後 10 時に次のランタイムのスケジュールを作成すると仮定すると、東部標準時に存在する管理ユーザーには、次の日の午前 1 時（3 時間後）に次のランタイムのスケジュールが表示されます。

スケジュール カタログ

Avamar システムには、事前設定されたスケジュールのセットがデフォルトで含まれています。これらのスケジュールを使用することも、カスタム スケジュールを作成することも可能です。

注

Avamar サーバーで事前構成されているインストール済みのスケジュールの設定を編集したり、削除したりすることはできません。ユーザー定義のスケジュールの変更は、選択したスケジュールを使用する既存のバックアップ ポリシーに影響します。ユーザー定義のスケジュールの設定を編集する場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

デフォルトでは、次のスケジュールが使用できます。

表 36 スケジュール カタログ

スケジュール名	説明
Default Schedule	デフォルト グループのバックアップ スケジュールを制御します。初期設定では、1 日 1 回午後 10 時に実行するように設定されています。これらの設定を編集する場合は、デフォルト グループのすべてのメンバーに変更が適用されます。
Default Replication Schedule	レプリケーション グループのレプリケーションを制御します。
Default Tiering Schedule	クラウド階層化で Avamar バックアップを Data Domain からクラウドに移動し、これらのバックアップのシームレスなリカバリーを実行するためのバックアップ スケジュールを制御します。
Daily Schedule	Avamar には、あらかじめ定義された Daily Schedule が用意されています。
Evaluation Schedule	評価プロファイルのメール通知が送信される時期を制御します。初期設定では、毎週月曜日の午前 6 時に実行するように設定されています。
Notification Schedule	カスタム イベント プロファイルのメール通知メッセージが送信される時期を制御します。
Override Daily Schedule	[Override group schedules] が有効化されているクライアントが選択可能な開始時刻を定義します。このスケジュールは編集可能です。[Override group schedules] 設定には、このスケジュールのコピーは使用されません。
Statistics Schedule	Avamar サーバの各種統計（例えば、Avamar サーバの [Bytes protected] の詳細値）を取得または算出する頻度を制御します。このスケジュールのデフォルト設定は 1 時間ごとです。

表 36 スケジュール カタログ (続き)

スケジュール名	説明
Usage Intelligence Schedule	Avamar サーバでレポート作成情報を収集し、ESRS Gateway 経由で Avamar サポートに転送する頻度を制御します。

スケジュールの追加

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Settings**] をクリックします。
2. [**Schedule**] タブをクリックします。
3. [**Add**] をクリックします。
[**Create Schedule**] ダイアログ ボックスが表示されます。
4. [**Schedule Name**] フィールドに、スケジュールの名前を入力します。
名前には、次の文字を使用しないでください。~!@#\$%^&(){}[]|,` ;#\/*?<>' "&。
5. [**Backup Window**] フィールドに、時間数を入力します。
6. [**Recurrence Type**] セクションで、次のようにスケジュール タイプを選択します。

表 37 スケジュールの各タイプの設定

スケジュールタイプ	設定
Daily	<p>繰り返しパターンをインターバルで選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> a. [By interval] を選択します。 b. [From] フィールドで、スケジュールを有効にする時刻を選択します。スケジュールを直ちに有効にするには、現在の時刻を選択します。 c. [To] フィールドで、スケジュールを終了する時刻を選択します。 d. インターバルを選択します。 e. [Add] をクリックします。 選択した時刻がリストに表示されます。 f. [NEXT] をクリックします。 <p>繰り返しパターンをポイント イン タイムで選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> a. [By time point] を選択します。 b. 時刻を指定します。スケジュールを直ちに有効にするには、現在の時刻を選択します。 c. [Add] をクリックします。 選択した時刻がリストに表示されます。 d. [NEXT] をクリックします。 <p>注</p> <p>ジョブの重複を防ぐため、スケジュール設定されたシステム アクティビティの期間を制限します。</p>

表 37 スケジュールの各タイプの設定（続き）

スケジュールタイプ	設定
Weekly	スケジュールを実行する曜日の横のチェックボックスを選択します。
Monthly	<p>アクティビティを特定のカレンダー日付または毎月の指定した週の曜日のどちらで繰り返すかを選択します。</p> <ul style="list-style-type: none"> アクティビティを特定のカレンダー日付で繰り返すには、[Day of every month] を選択し、リストから日付を選択します。 アクティビティを毎月の指定曜日で繰り返すには、[The ... of every month] を選択し、リストから日付を選択します。

7. [NEXT] をクリックします。

[Recurrence Pattern] パネルが表示されます。

8. スケジュールの実行頻度を選択します。

a. 繰り返しパターンを選択します。インターバルまたは時点で選択することができます。

b. インターバル実行の長さを選択し、[ADD] をクリックします。

選択した時刻がリストに表示されます。

c. [NEXT] をクリックします。

[Activities Constraint] ページが表示されます。

9. [Activities Constraint] ページで、次のタスクを実行します。

a. [Select schedule start time] フィールドで、[At] フィールドと [From] フィールドを使用して、アクティビティの動作時間を定義します。日付を変更することができます。

時刻を入力すること、または時刻を選択して矢印ボタンで時刻を変更することができます。

サーバーの作業負荷により、アクティビティの開始時刻は影響を受けます。また、クライアントに対してバックアップを初めて行う場合、指定された終了時刻を過ぎてもバックアップは継続できます。同じクライアントでも初回のバックアップは、次回以降のバックアップに比べて長い時間がかかるため、この動作が許可されています。

b. [Select schedule stop time] フィールドで、スケジュールの終了日オプションを選択します。

スケジュールを中止する時期を選択します。

- スケジュールを無期限に実行できるようにするには、[No End Date] を選択します。

- ある特定の日付でスケジュールを中止するには、[End after] を選択し、リストから日付を選択します。

10. [FINISH] をクリックします。

スケジュールの編集

注

Avamar サーバーで事前構成されているインストール済みのスケジュールの設定を編集したり、削除したりすることはできません。ユーザー定義のスケジュールの変更は、選択したスケジュールを使用する既存のバックアップポリシーに影響します。ユーザー定義のスケジュールの設定を編集する場合、クライアントレベルでバックアップポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップポリシーの全メンバーに変更が適用されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Schedule] タブをクリックします。
3. スケジュールを選択して、[EDIT] をクリックします。
[Edit Schedule] ダイアログ ボックスが表示されます。
4. スケジュール設定を編集します。
5. [OK] をクリックします。

スケジュールの削除

スケジュールがグループに現在割り当てられていないことを確認します。スケジュールがグループに割り当てられている場合、そのスケジュールを削除することはできません。

注

Avamar サーバーで事前構成されているインストール済みのスケジュールの設定を編集したり、削除したりすることはできません。ユーザー定義のスケジュールの変更は、選択したスケジュールを使用する既存のバックアップポリシーに影響します。ユーザー定義のスケジュールの設定を編集する場合、クライアントレベルでバックアップポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップポリシーの全メンバーに変更が適用されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Schedule] タブをクリックします。
3. スケジュールを選択して、[DELETE] をクリックします。
4. 確認メッセージ ダイアログ ボックスで、[YES] をクリックします。

ルールの管理

Avamar サーバーはルールを使用して、自動検出された仮想マシンへのドメインのマッピングおよびバックアップポリシーの自動割り当てを行います。

新しいルールを作成したり、既存のルールを編集したり、ルールを削除したりすることができます。

ルールの作成

Avamar サーバーはルールを使用して、自動検出された仮想マシンへのドメインのマッピングおよびバックアップポリシーの自動割り当てを行います。

ルールを作成する際には、ルールが相互に排他的であることを確認し、1 台の仮想マシンが複数のルール下で認定される状況が起こらないようにします。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Rule] タブをクリックします。
3. ドメイン ツリーで、クライアントの vCenter ドメインまたはサブドメインを選択します。
4. [Setting] ページで、次のタスクを完了します。
 - a. [Add] をクリックします。

[New Rule] ウィンドウが表示されます。

5. [Rule Name] フィールドに、ルールの名前を入力します。
6. [Match Type] フィールドで、ルールがリストにあるフィルター メカニズムの一部に一致する必要があるのか ([Any])、またはすべてに一致する必要があるのか ([All]) を選択します。

この選択によって、仮想マシンを選択する複数の異なるフィルターを設定でき、設定したフィルターが相互に作用して正しい仮想マシンを選択する方法を決定できます。たとえば、仮想マシンを選択するために仮想マシンのフォルダーのパスを使用するフィルターと、仮想マシンの命名規則を使用する別のフィルターを作成することができます。

このルール下に含める仮想マシンを決定するには、このオプションを使用します。

- 定義済みのフォルダー パスにあり、命名規則にも従っている仮想マシンのみを含めるには [All] を選択します。
このステップでは、フォルダー パスにあるが命名規則に従っていない仮想マシンを除外します。また、命名規則に従っているがフォルダー パスにない仮想マシンも除外します。
- 仮想マシンのフォルダー パスにある仮想マシンまたは命名規則に従っている仮想マシンのいずれかを含めるには、[Any] を選択します。

7. フィルターを追加するには、次の手順を実行します。
 - a. + をクリックします。
このステップによって、フィルターのリストに行が追加されます。
 - b. [Filter] 列で、フィルター タイプを選択します。
たとえば、仮想マシンの命名規則を使用するフィルターを作成するには、[VM Name] を選択し、vCenter 仮想マシンのタグを使用するフィルターを作成するには、[VM Tag] を選択します。
 - c. [Operator] 列で、オペランドを選択します。
たとえば、フィルター タイプに [VM Name] を選択し、オペランドに [begins with] を選択した場合は、フィルター テキストで始まるすべての仮想マシンが選択されます。
 - d. [Value] 列に、フィルター テキストを入力します。
たとえば、名前がテキスト文字列 [HR_] で始まるすべての仮想マシンを選択するフィルターを作成するには、フィルター タイプに [VM Name]、オペランドに [begins with] を選択し、フィルター テキストに [HR_] と入力します。
8. 追加のフィルターを作成するには、+ をクリックします。
このステップによって、フィルターのリストに行が追加されます。
9. 既存のフィルターを削除するには、[Delete] をクリックします。
10. [Submit] をクリックします。

タグに変更を加えると、変更が有効になるまで最大で 12 時間かかる可能性があります。このため、タグの編集は慎重に行うか、vCenter が Avamar サーバと自動同期する、同期化された vCenter の操作を実行します。

ルールの編集

ルールを編集する際には、ルールが相互に排他的であることを確認し、1 台の仮想マシンが複数のルール下で認定される状況が起こらないようにします。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Rule] タブをクリックします。
3. ドメイン ツリーで、クライアントの vCenter ドメインまたはサブドメインを選択します。
4. [Setting] ページで、次のタスクを完了します。
 - a. VMware エンティティを含むフォルダーを選択します。
 - b. リストから、編集するルールを選択して [EDIT] をクリックします。

[Edit Rule] ウィンドウが表示されます。

5. [Rule Name] フィールドに、ルールの名前を入力します。
6. [Match Type] フィールドで、ルールがリストにあるフィルター メカニズムの一部に一致する必要があるのか ([Any])、またはすべてに一致する必要があるのか ([All]) を選択します。

この選択によって、仮想マシンを選択する複数の異なるフィルターを設定でき、設定したフィルターが相互に作用して正しい仮想マシンを選択する方法を決定できます。たとえば、仮想マシンを選択するために仮想マシンのフォルダーのパスを使用するフィルターと、仮想マシンの命名規則を使用する別のフィルターを作成することができます。

このルール下に含める仮想マシンを決定するには、このオプションを使用します。

- 定義済みのフォルダー パスにあり、命名規則にも従っている仮想マシンのみを含めるには [All] を選択します。
このステップでは、フォルダー パスにあるが命名規則に従っていない仮想マシンを除外します。また、命名規則に従っているがフォルダー パスにない仮想マシンも除外します。
- 仮想マシンのフォルダー パスにある仮想マシンまたは命名規則に従っている仮想マシンのいずれかを含めるには、[Any] を選択します。

7. フィルターを追加するには、次の手順を実行します。
 - a. + をクリックします。
このステップによって、フィルターのリストに行が追加されます。
 - b. [Filter] 列で、フィルター タイプを選択します。
たとえば、仮想マシンの命名規則を使用するフィルターを作成するには、[VM Name] を選択し、vCenter 仮想マシンのタグを使用するフィルターを作成するには、[VM Tag] を選択します。
 - c. [Operator] 列で、オペランドを選択します。
たとえば、フィルター タイプに [VM Name] を選択し、オペランドに [begins with] を選択した場合は、フィルター テキストで始まるすべての仮想マシンが選択されます。
 - d. [Value] 列に、フィルター テキストを入力します。

たとえば、名前がテキスト文字列 [HR_] で始まるすべての仮想マシンを選択するフィルターを作成するには、フィルター タイプに [VM Name]、オペランドに [begins with] を選択し、フィルター テキストに [HR_] と入力します。

8. 追加のフィルターを作成するには、+ をクリックします。

このステップによって、フィルターのリストに行が追加されます。

9. 既存のフィルターを削除するには、次の手順に従います。

- a. ファイルを選択します。
- b. [Actions] 列で、[Delete] をクリックします。

10. [Submit] をクリックします。

タグに変更を加えると、変更が有効になるまで最大で 12 時間かかる可能性があります。このため、タグの編集は慎重に行うか、vCenter が Avamar サーバと自動同期する、同期化された vCenter の操作を実行します。

ルールの削除

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Rule] タブをクリックします。
3. ドメイン ツリーで、クライアントの vCenter ドメインまたはサブドメインを選択します。
4. [Setting] ページで、次のタスクを完了します。
 - a. リストからルールを選択します。
 - b. [DELETE] をクリックします。

保存ポリシー

バックアップの保存ポリシーにより、システムにバックアップを保存する期間を指定できます。

保存ポリシーは、バックアップが行われるとき、各バックアップに割り当てられます。オン デマンド バックアップを実行する場合、カスタム保存ポリシーを指定するか、スケジュール設定されたバックアップの際にクライアント グループに自動的に割り当てられる保存ポリシーを作成します。

保存期限が切れたバックアップには、自動的に削除のマークが付けられます。削除は、システム アクティビティが低い時間帯にバッチ処理で行われます。

これまでに行われた個別のバックアップに対しては、必要に応じて保存期間の設定を手動で変更することができます。ただし、保存ポリシーの設定を変更しても、変更が適用されるのは変更後に行われるバックアップのみです。これまで行われたバックアップに対しては、保存期間の設定は同じ状態のまま変わりません。したがって、バックアップが増えすぎる前に、サイトにとっての最良の保存ポリシーを検討し、導入しておくことが重要です。

保存期間の設定には、次の 2 つのタイプがあります。

- 基本的な保存期間の設定では、確定有効期限日を指定します。
- 高度な保存期間の設定では、保存する日単位、週単位、月単位、年単位のバックアップの数を指定します。

基本的な保存期間の設定

基本的な保存期間の設定では、次の表のいずれかの設定を使用して、確定有効期限日をバックアップに割り当てます。

表 38 基本的な保存期間の設定

保存期間の設定	説明
Retention Period	確定保存期間を、バックアップが行われてからの日数、週数、月数、年数で定義することができます。例えば、バックアップの有効期限を 6 か月後に指定できます。
End date	有効期限日としてカレンダー日付を割り当てることができます。例えば、2013 年 12 月 31 日にバックアップの有効期限が切れるように指定できます。
No end date	バックアップを無期限に保存することができます。システムが存続する限り、この保存ポリシーを割り当てたすべてのバックアップを保持する場合には、この設定が便利です。

通知

32 ビットの Windows または 32 ビットの Linux クライアント コンピューターのバックアップの場合、2106 年 2 月 7 日より後の日付に保存期間を割り当てないでください。32 ビットの Windows クライアントに長期の保存期間を割り当てると、バックアップが例外付きで完了します。32 ビット Linux クライアントでは、バックアップは完了しますが、Avamar Administrator に表示されません。

高度な保存期間の設定

高度な保存期間の設定を使用している場合、日次、週次、月次、年次でシステム内で保持するバックアップの数を指定して、バックアップの有効期限を動的に割り当てることができます。

スケジュール設定された日次バックアップの場合、一部のバックアップには次のような高度な保存期間のタイプが自動的に割り当てられます。

- 毎日最初に正常終了したスケジュール設定されたバックアップが、日次バックアップに認定されます。
- 毎週最初に正常終了したスケジュール設定されたバックアップが、週次バックアップに認定されます。
- 毎月最初に正常終了したスケジュール設定されたバックアップが、月次バックアップに認定されます。
- 毎年最初に正常終了したスケジュール設定されたバックアップが、年次バックアップに認定されます。

高度な保存期間のタイプを割り当てるために、日は 00:00:01 GMT から始まり、週は日曜日から始まり、月はその月の最初のカレンダー日から始まり、年は 1 月 1 日から始まるとします。

通知

オン デマンド バックアップには高度な保存期間の設定は適用できません。オン デマンド バックアップはいつでも実行することができるため、本質的に非同期的な処理です。システムは日次、週次、月次、年次のいずれかとしてオン デマンド バックアップをタグ付けできません。

スケジュール設定された日次バックアップと高度な保存期間の設定が指定された保存ポリシーを常に使用するようにはしてください。システムに日次バックアップがないと、**[Always keep: n weeks of daily backups]** の設定は効果がなくなるためです。使用するスケジュールによっては、日次のバックアップがシステムに存在しないこともあります。例えば、週単位のバックアップのみを実行するグループにスケジュールを割り当てる場合、システムには日単位のバックアップが存在しないことになります。

保存ポリシー カタログ

Avamar システムには、事前構成された保存ポリシーのセットがデフォルトで含まれています。これらの保存ポリシーをクライアントのスケジュール設定されたバックアップで使用できます。または、カスタム保存ポリシーを作成することができます。

注

Avamar サーバーで事前構成されているインストール済みの保存ポリシーの設定を編集したり、削除したりすることはできません。ユーザー定義の保存ポリシーの変更は、選択した保存ポリシーを使用する既存のバックアップ ポリシーに影響します。ユーザー定義の保存ポリシーの設定を編集した場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

デフォルトで次の表に示す保存ポリシーを利用可能です。

表 39 保存ポリシー カタログ

保存ポリシー名	説明
Minimal Retention	サイト全体で最小限の基本的な保存設定を徹底させることができます。例えば、他の保存ポリシーの設定に関係なく、すべてのバックアップを最低 90 日間保存することができます。この機能は、個々の組織が実装している他の保存ポリシーに関係なく、サイト全体に標準の最小保存期間を適用する必要がある企業に適しています。Minimal Retention ポリシーは、最小保存期間の設定のみを制御するグローバルなシステム オブジェクトです。したがって、Minimal Retention ポリシーをバックアップ ポリシーに割り当てることはできません。
Default Retention	デフォルト グループのバックアップ保存設定を定義します。デフォルトでは、Default Retention ポリシーは 60 日間の保存期間を割り当て、日々のバックアップを 60 日間保持します。
End User On Demand Retention	Avamar Windows クライアントで [Back Up Now] コマンドを使用する場合など、クライアントが開始するオン デマンド バックアップの保存設定を制御します。オン デマンド バックアップには高度な保存期間の設定は適用されないため、この保存ポリシーでは高度な保存期間の設定は無効になります。End User On Demand Retention ポリシーは、クライアントが開始するオン デマンド バックアップの保存期間のみを制御する、グローバルなシステム オブジェクトです。したがって、End User On Demand Retention ポリシーをバックアップ ポリシーに割り当てることはできません。
Monthly Retention	バックアップ後の有効期限を 1 か月に設定します。
Weekly Retention	バックアップ後の有効期限を 1 週間に設定します。

保存ポリシーの追加

[Administration] ウィンドウでは、保存ポリシーを追加または削除することができます。

注

保存ポリシーを 14 日以上に指定することがベスト プラクティスです。保存ポリシーを 14 日未満で作成すると、アラートが表示されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Retention] タブをクリックします。
3. [Add] をクリックします。
[Add Retention Policy] ダイアログ ボックスが表示されます。
4. [Retention Name] フィールドに、この保存ポリシーの名前を入力します。
保存ポリシー名には、次に示す文字を使用しないでください。~!@%^%(){}[]|,`#
\/:*?<>'"&。
5. 特定の日数、週数、月数、または年数の経過後に自動的にバックアップを削除するには、次のようにします。
 - a. [Retention period] を選択します。
 - b. 日数、週数、月数、または年数を指定します。
6. 特定のカレンダー日付に自動的にバックアップを削除するには、次のようにします。
 - a. [End date period] を選択します。
 - b. カレンダーでその日付に移動します。
7. クライアントがアクティブである期間バックアップを保存しておく場合は、[No end date] を選択します。
8. スケジュール設定されたバックアップの保存ポリシーをオーバーライドするには、次のようにします。
 - a. [Override basic retention policy for scheduled backups] を選択します。
 - b. 保持する日次、週次、月次、年次のバックアップの最大数を指定します。
9. [保存] をクリックします。

保存ポリシーの編集**注**

Avamar サーバーで事前構成されているインストール済みの保存ポリシーの設定を編集したり、削除したりすることはできません。ユーザー定義の保存ポリシーの変更は、選択した保存ポリシーを使用する既存のバックアップ ポリシーに影響します。ユーザー定義の保存ポリシーの設定を編集した場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Retention] タブをクリックします。
3. 保存ポリシーを選択して、[EDIT] をクリックします。
[Edit Retention Policy] ダイアログ ボックスが表示されます。
4. 保存ポリシー設定を編集します。
5. [保存] をクリックします。

保存ポリシーの削除

保存ポリシーがクライアントまたはバックアップ ポリシーに現在割り当てられていないことを確認します。クライアントまたはバックアップ ポリシーに割り当てられている保存ポリシーは削除できません。

注

Avamar サーバーで事前構成されているインストール済みの保存ポリシーの設定を編集したり、削除したりすることはできません。ユーザー定義の保存ポリシーの変更は、選択した保存ポリシーを使用する既存のバックアップ ポリシーに影響します。ユーザー定義の保存ポリシーの設定を編集した場合、クライアントレベルでバックアップ ポリシー設定をオーバーライドし、別のデータセットを割り当てない限り、バックアップ ポリシーの全メンバーに変更が適用されます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Settings] をクリックします。
2. [Retention] タブをクリックします。
3. 保存ポリシーを選択して、[DELETE] をクリックします。
4. 確認メッセージ ダイアログ ボックスで [YES] をクリックします。

バックアップ ポリシーについて

Avamar では、バックアップの自動化と、ユーザー コミュニティのセグメント（グループ）全体で一貫したルールとシステム動作のために、バックアップ ポリシーを使用します。

Members

メンバーは、スケジュール設定されたバックアップを実行するために特定のバックアップ ポリシーに追加されたクライアント マシンです。ドメイン管理者の標準ルールが適用されるため、クライアントはバックアップ ポリシーが存在するドメイン、またはサブドメイン内に配置する必要があります。

Backup Policy

バックアップ ポリシーを作成する際に、グループのデータセット、スケジュール、保存ポリシーを指定します。これら 3 つのオブジェクトで、[バックアップ ポリシー] が構成されます。バックアップ ポリシーは、そのバックアップ ポリシーのすべてのメンバーのバックアップ動作を制御します。

クライアントに明示的なデータセットまたは保存ポリシーの割り当てを作成して、クライアントのバックアップ ポリシー データセットと保存ポリシー設定をオーバーライドすることができます。ただし、スケジュールはバックアップ ポリシーだけに適用されます。個別のクライアントには適用されません。

Default Group

Avamar システムには、デフォルト グループが含まれています。デフォルトの Avamar サーバ構成では、デフォルト グループは常にシステムのデフォルト データセット、スケジュール、保存ポリシーを使用します。これらシステムのデフォルトの割り当ては変更できません。ただし、システムのデフォルト データセット、スケジュール、保存ポリシーの設定を編集することは可能です。

他のバックアップ ポリシーが作成されていない場合、新しいクライアントは自動的にデフォルト グループに追加されます。

VMware groups

次の表では、VMware 環境に適用される特別なグループについて説明しています。

表 40 VMware groups

グループ	説明
Default Group	Avamar システムには、デフォルト グループが含まれています。デフォルトの Avamar サーバ構成では、デフォルト グループは常にシステムのデフォルト データセット、スケジュール、保存ポリシーを使用します。これらシステムのデフォルトの割り当ては変更できません。ただし、システムのデフォルト データセット、スケジュール、保存ポリシーの設定を編集することは可能です。 他にグループが作成されていない場合、新しいクライアントは自動的にデフォルト グループに追加されます。
Default Proxy Group	デフォルト プロキシ グループは、VMware Image Proxy クライアントのデフォルト グループです。デフォルト プロキシ グループは削除できません。デフォルト プロキシ グループを有効にしても、プロキシ クライアントで設定した、他のプラグインが実行するスケジュール設定されたバックアップと競合することはありません。
Default Virtual Machine Group	新規仮想マシン クライアントは、登録されると、自動的にデフォルト仮想マシン グループに追加されます。デフォルト仮想マシン グループを手動で削除することはできませんが、vCenter ドメインを削除すると、自動的に削除されます。

バックアップ ポリシーの管理

[Policies] ページでは、バックアップ ポリシー タスクと情報にアクセスできます。

[Policies] ページには、選択した Avamar サーバー上の各バックアップ ポリシーのサマリーが表示されます。

バックアップ ポリシー オブジェクトには、次の子オブジェクトが含まれます。

- スケジュール：スケジュール バックアップが実行された場合
- 保存ポリシー：バックアップ アプライアンスにバックアップを保存する期間
- データセット：オプションのバックアップ パラメーター
- メンバー：バックアップ ポリシーからクライアントを追加および削除する

バックアップ ポリシーの作成

バックアップ ポリシーを作成する際に、クライアントまたはクライアントのグループに適用されるデータセット、スケジュール、保存設定を定義します。バックアップ ポリシーには、少なくとも 1 個の Avamar クライアントを含める必要があります。バックアップ ポリシーに 2 個以上のクライアントが含まれる場合は、これらのクライアントは同一の Avamar ドメインに属している必要があります。クライアントレベルでバックアップ ポリシーの設定をオーバーライドできます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[Backup Policy] をクリックします。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。
バックアップ ポリシーのサブドメインを選択するには、[Include Sub-domain] スイッチをオンに切り替えます。
3. バックアップ ポリシーを追加するには、[ADD] をクリックします。

[Policy] ウィザードが表示され、[Properties] ページが表示されます。

バックアップ ポリシーのプロパティの構成

バックアップ ポリシーの名前の作成、バックアップ ポリシーの有効化、オーバーライド スケジュールの設定、自動プロキシ マッピングの有効化など、バックアップ ポリシーのプロパティを構成することができます。

[Policy] ウィザードの [Properties] ページから次のタスクを実行します。

[Policy] ウィザードの [Properties] ページにアクセスするには、左側の AUI ナビゲーション ペインで、>>をクリックし、[Backup Policy] > [ADD] をクリックします。

手順

1. [Name] フィールドに、バックアップ ポリシーの名前を入力します。
2. スケジュール設定されたクライアント バックアップにこのバックアップ ポリシーを使用するには、[Enabled] チェックボックスをオンにします。
チェックボックスをオフにすると、バックアップ ポリシーのバックアップが無効になります。
3. このバックアップ ポリシーに割り当てられているスケジュールをオーバーライドするには、[Override Schedule] を選択します。
 - 次回のスケジュール設定したバックアップをスキップするには、[Skip Next Backup] を選択します。
 - 次回のスケジュール設定したバックアップを1回のみ実行するには、[Run Next Backup Once] を選択します。
4. [Auto proxy mapping] を有効にするには、チェックボックスをオンにします。
5. リストからプロキシを選択します。
6. 選択したクライアントにバックアップ ポリシーを適用するか、選択したクライアントからバックアップ ポリシーを削除してウィザードを完了するには、[NEXT] をクリックします。
[Members] ページが表示されます。

バックアップ ポリシーへのメンバーの追加または削除

選択したクライアントにバックアップ ポリシーを適用したり、選択したクライアントからバックアップ ポリシーを削除したりするなど、バックアップ ポリシーの属性を構成することができます。バック ポリシーを編集するときに、クライアントを作成、追加、削除する時点でクライアントを追加することができます。

[Policy] ウィザードの [Members] ページにアクセスするには、左側の AUI ナビゲーション ペインで、>>をクリックし、[Backup Policy] をクリックします。

[Policy] ウィザードの [Members] パネルで、次の手順を実行します。

手順

1. ドメイン ツリーで、バックアップ ポリシーのドメインを選択します。
ログイン アカウントでは、ドメインのクライアントのみを表示できます。すべてのクライアントを表示するには、root ドメインにログインします。
2. クライアントをバックアップ ポリシーに追加するには、次のようにします。
 - a. クライアントのリストで、追加するクライアントを選択します。
 - b. [NEXT] をクリックします。

このタスクが完了すると、Avamar サーバーは選択したクライアントにバックアップ ポリシーを適用します。

3. バックアップ ポリシーからクライアントを削除するには、次のようにします。

- a. クライアントのリストで、削除するクライアントを選択します。
- b. **[NEXT]** をクリックします。

この手順により、選択したクライアントとバックアップ ポリシー間の関連が削除されます。このタスクが完了すると、バックアップ ポリシーが選択したクライアントに適用されることはありません。

4. データセットをバックアップ ポリシーに追加してウィザードを完了するには、**[NEXT]** をクリックします。

[Dataset] パネルが表示されます。

バックアップ ポリシーへのデータセットの追加

データセットの追加を含め、バックアップ ポリシーの属性を構成することができます。

[Policy] ウィザードの **[Dataset]** ページから次のタスクを実行します。

[Policy] ウィザードの **[Properties]** ページにアクセスするには、左側の AUI ナビゲーション ペインで、**>>** をクリックし、**[Backup Policy]** > **[ADD]** をクリックします。

注

Avamar サーバで、バックエンド ストレージに Data Domain を使用している場合、Data Domain システムがデフォルトのバックアップ ストレージ場所になります。**[Options]** タブでシステムを変更することができます。

手順

1. **[Dataset]** フィールドで、ドロップダウン リストからデータセットを選択します。
2. **[Dataset Name]** フィールドに、データセットの名前を入力します。

名前には、英数字 (A-Z、a-z、0-9) および次の特殊文字を含めることができます。ピリオド (.)、ハイフン (-)、下線 (_)。Unicode 文字または次に示す特殊文字は使用しないでください。` ~ ! @ # \$ % ^ & * () = + [] { } | \ / ; : ' " < > , ?

3. クライアントにインストールされているすべてのプラグ インのデータを含める場合は、**[Select All Data for All Local File Systems]** を選択します。
4. **[Plugins]** リストから、バックアップに使用するプラグ インを選択します。
5. **[Option]** タブをクリックして、グラフィカル コントロールを使用するか、オプション名と値をテキスト エントリーとして入力することにより、プラグ イン オプションを設定します。

(オプション) **[Show Advanced Options]** スイッチをオンにして、詳細な構成オプションを表示します。

プラグ イン オプションを使用すると、データセットの動作をさらに細かくカスタマイズできます。各プラグ インのユーザー ガイドには、プラグ インで使用できるオプションが詳しく説明されています。

6. **[Source Data]** タブをクリックして、このデータセットにデータを提供するソース データ プラグ インを定義します。
 - クライアントにインストールされているすべてのプラグ インのデータを含める場合は、**[Select All Data for All Local File Systems]** を選択します。
 - 特定のプラグ インからのデータのみを含め、データセットを特定のデータのみ制限するには、次の手順を実行します。

- a. **[Plugins]** リストから、バックアップに使用するプラグインを選択します。
追加のオプションが **[Select Plug-In Type]** リストの下に表示されます。
 - b. プラグインで利用可能なすべてのデータをバックアップするには、次の手順を実行します。
 - オプションを選択します。
 - **[Select Files and/or Folders]** を選択して、データへのパスを入力します。
 - c. バックアップするデータへのパスを入力するには、**[File/Folder Path]** フィールドにパスを入力し、**[Add]** をクリックします。
データセットのデータへのパスを指定することで、スケジュール設定されたバックアップをデータのセットに制限します。パスを入力するときは、次のルールが適用されます。
 - ファイルシステムプラグインを使用している場合、パス内で最初に表示されるアスタリスク(*)はフォルダーのワイルドカードとしてみなされます。例えば、Windows コンピューター上のすべてのユーザーで My Documents フォルダーを指定するには、`C:\Documents and Settings*\My Documents` と入力します。
 - Macintosh 上のすべてのユーザーで Documents フォルダーを指定するには、`/Users/*/Documents` と入力します。
 - データパスを指定する場合、最初のアスタリスク(*)のみがフォルダーのワイルドカードとみなされます。2つ目以降のアスタリスクは文字どおり解釈されます。
 - パスには、英数字 (A-Z, a-z, 0-9) と、ワイルドカードとしてアスタリスク(*)を含めることができます。データパスには、次に示す文字を使用しないでください。
~!@#\$%^&(){}[]|,`';#:?*<>'"&.
7. スケジュールをバックアップポリシーに追加してウィザードを完了するには、**[NEXT]** をクリックします。

[Schedule] ページが表示されます。

バックアップポリシーへのスケジュールの追加

スケジュールの追加を含め、バックアップポリシーの属性を構成することができます。

[Policy] ウィザードの **[Schedule]** ページから次のタスクを実行します。

[Policy] ウィザードの **[Schedule]** ページにアクセスするには、左側の AUI ナビゲーションペインで、>>をクリックし、**[Backup Policy]** > **[ADD]** をクリックします。

手順

1. 既存のスケジュールを選択するには、**[Schedule]** ドロップダウンリストからスケジュールタイプを選択し、**[NEXT]** をクリックします。
[Retention] ウィンドウが表示されます。
2. スケジュールを編集するには、次のようにします。
 - a. **[Schedule]** フィールドで、編集するスケジュールをドロップダウンリストから選択します。
 - b. **[Edit Schedule]** スイッチを **[ON]** に切り替えます。
 - c. スケジュールの設定を編集し、**[NEXT]** をクリックします。
[Retention] ウィンドウが表示されます。
3. スケジュールを追加するには、次の手順に従います。
 - a. **[Schedule]** フィールドで、ドロップダウンリストから **[New]** を選択します。

b. **[Schedule Name]** フィールドに、スケジュールの名前を入力します。

名前には、次の文字を使用しないでください。~!@#\$%^&(){}[]|,`;\:/:*?<>'\"&。

c. **[Backup Window]** フィールドに、時間数を入力します。

d. **[Recurrence Type]** セクションで、次のようにスケジュール タイプを選択します。

表 41 スケジュールの各タイプの設定

スケジュールタイプ	設定
Daily	<p>繰り返しパターンをインターバルで選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [By interval] を選択します。 [From] フィールドで、スケジュールを有効にする時刻を選択します。スケジュールを直ちに有効にするには、現在の時刻を選択します。 [To] フィールドで、スケジュールを終了する時刻を選択します。 インターバルを選択します。 [Add] をクリックします。 選択した時刻がリストに表示されます。 [NEXT] をクリックします。 <p>繰り返しパターンをポイント イン タイムで選択するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [By time point] を選択します。 時刻を指定します。スケジュールを直ちに有効にするには、現在の時刻を選択します。 [ADD] をクリックします。 選択した時刻がリストに表示されます。 [NEXT] をクリックします。[Retention] ウィンドウが表示されます。 <p>注</p> <p>ジョブの重複を防ぐため、スケジュール設定されたシステム アクティビティの期間を制限します。</p>
Weekly	<ol style="list-style-type: none"> スケジュールを実行する曜日の横のチェックボックスを選択します。 [Select schedule start time] フィールドで、[At] フィールドと [From] フィールドを使用して、アクティビティの動作時間を定義します。日付を変更することができます。 時刻を入力すること、または時刻を選択して矢印ボタンで時刻を変更することができます。 <p>サーバーの作業負荷により、アクティビティの開始時刻は影響を受けます。また、クライアントに対してバックアップを初めて行う場合、指定された終了時刻を過ぎてもバックアップは継続できます。同じクライアントでも初回のバックアップは、次回以降のバックアップに比べて長い時間がかかるため、この動作が許可されています。</p>

表 41 スケジュールの各タイプの設定 (続き)

スケジュールタイプ	設定
	<p>c. [Select schedule stop time] フィールドで、スケジュールの終了日オプションを選択します。 スケジュールを中止する時期を選択します。</p> <ul style="list-style-type: none"> スケジュールを無期限に実行できるようにするには、[No End Date] を選択します。 ある特定の日付でスケジュールを中止するには、[End after] を選択し、リストから日付を選択します。 <p>d. [NEXT] をクリックします。[Retention] ウィンドウが表示されます。</p>
Monthly	<p>a. アクティビティを特定のカレンダー日付または毎月の指定した週の曜日のどちらかで繰り返すかを選択します。</p> <ul style="list-style-type: none"> アクティビティを特定のカレンダー日付で繰り返すには、[Day of every month] を選択し、リストから日付を選択します。 アクティビティを毎月の指定曜日で繰り返すには、[The ... of every month] を選択し、リストから日付を選択します。 <p>b. [Select schedule start time] フィールドで、[At] フィールドと [From] フィールドを使用して、アクティビティの動作時間を定義します。日付を変更することができます。 時刻を入力すること、または時刻を選択して矢印ボタンで時刻を変更することができます。</p> <p>サーバーの作業負荷により、アクティビティの開始時刻は影響を受けます。また、クライアントに対してバックアップを初めて行う場合、指定された終了時刻を過ぎてもバックアップは継続できます。同じクライアントでも初回のバックアップは、次回以降のバックアップに比べて長い時間がかかるため、この動作が許可されています。</p> <p>c. [Select schedule stop time] フィールドで、スケジュールの終了日オプションを選択します。 スケジュールを中止する時期を選択します。</p> <ul style="list-style-type: none"> スケジュールを無期限に実行できるようにするには、[No End Date] を選択します。 ある特定の日付でスケジュールを中止するには、[End after] を選択し、リストから日付を選択します。 <p>d. [NEXT] をクリックします。[Retention] ウィンドウが表示されます。</p>

バックアップポリシーへの保存ポリシーの適用

保存ポリシーの追加を含め、バックアップポリシーの属性を構成することができます。

[Policy] ウィザードの **[Retention]** ページから次のタスクを実行します。

[Policy] ウィザードの **[Schedule]** ページにアクセスするには、左側の AUI ナビゲーション ペインで、>>をクリックし、**[Backup Policy]** > **[ADD]** をクリックします。

注

保存ポリシーを 14 日以上に指定することがベストプラクティスです。保存ポリシーを 14 日未満で作成すると、アラートが表示されます。

手順

1. 既存のスケジュールを選択するには、[**Retention**] ドロップダウン リストからスケジュール タイプを選択し、[**NEXT**] をクリックします。
[**Summary**] ウィンドウが表示されます。
2. 保存ポリシーを編集するには、次のようにします。
 - a. [**Retention**] フィールドで、編集する保存ポリシーをドロップダウン リストから選択します。
 - b. [**Edit Retention**] スイッチを [**ON**] に切り替えます。
 - c. 保存設定を編集し、[**NEXT**] をクリックします。
[**Retention**] ウィンドウが表示されます。
3. 保存ポリシーを追加するには、次のようにします。
 - a. [**Retention**] フィールドで、ドロップダウン リストから [**New**] を選択します。
 - b. [**Retention Name**] フィールドに、スケジュールの名前を入力します。
名前には、次の文字を使用しないでください。~!@#\$%^&(){}[]|,`~;#\/:*? <>' " &。
 - c. [**Backup Window**] フィールドに、時間数を入力します。
 - d. [**Recurrence Type**] セクションで、次のようにスケジュール タイプを選択します。
4. 特定の日数、週数、月数、または年数の経過後に自動的にバックアップを削除するには、次のようにします。
 - a. [**Retention period**] を選択します。
 - b. 日数、週数、月数、または年数を指定します。
5. 特定のカレンダー日付に自動的にバックアップを削除するには、次のようにします。
 - a. [**End date period**] を選択します。
 - b. カレンダーでその日付に移動します。
6. クライアントがアクティブである期間バックアップを保存しておく場合は、[**No end date**] を選択します。
7. スケジュール設定されたバックアップの保存ポリシーをオーバーライドするには、次のようにします。
 - a. [**Override basic retention policy for scheduled backups**] を選択します。
 - b. 保持する日次、週次、月次、年次のバックアップの最大数を指定します。
8. バックアップ ポリシーのサマリーを確認してウィザードを完了するには、[**NEXT**] をクリックします。
[**Summary**] ページが表示されます。

バックアップ ポリシーの編集

プロパティの設定、メンバー、データセット、スケジュール、保存ポリシーの追加や変更を含め、バックアップ ポリシーを編集できます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[**Backup Policy**] をクリックします。
[**Policy**] ページが表示されます。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。
バックアップ ポリシーのサブドメインを選択するには、[**Include Sub-domain**] スイッチをオンに切り替えます。
3. リストからバックアップ ポリシーを選択して、[**Edit**] をクリックします。
[**Policy**] ウィザードが表示され、必要なバックアップ ポリシーの設定を変更できます。

バックアップ ポリシーのコピー

同じドメイン内でバックアップ ポリシーをコピーすることができます。バックアップ ポリシーを別のドメインにコピーすることはできません。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[**Backup Policy**] をクリックします。
[**Policy**] ページが表示されます。
2. コピーするバックアップ ポリシーを選択します。
3. [**MORE ACTIONS**] > [**Copy Policy**] を選択します。
[**Copy Policy**] ダイアログ ボックスが表示されます。
4. 新しいバックアップ ポリシーの名前を入力します。
5. クライアント リスト全体をこの新しいバックアップ ポリシーにコピーする場合は、[**Include Client Members**] チェックボックスをオンにします。
6. [**OK**] をクリックします。

バックアップ ポリシーの有効化と無効化

スケジュール設定されたバックアップがクライアントのグループに対して実行されないように、バックアップ ポリシーを無効化できます。通常、このステップは、システムがさまざまなメンテナンス アクティビティを行える状態にしておくために実行します。

バックアップ ポリシーを無効化する場合、スケジュール設定されたバックアップを再開するには、バックアップ ポリシーを再度有効化する必要があります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[**Backup Policy**] をクリックします。
[**Policy**] ページが表示されます。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。
バックアップ ポリシーのサブドメインを選択するには、[**Include Sub-domain**] スイッチをオンに切り替えます。

3. リストからバックアップ ポリシーを選択します。
4. バックアップ ポリシーを有効化するには、[**MORE ACTIONS**] > [**Enable Policy**] をクリックします。
5. バックアップ ポリシーを無効化するには、[**MORE ACTIONS**] > [**Disable Policy**] をクリックします。

バックアップ ポリシーの削除

はじめに

バックアップ ポリシーを削除する場合は、その削除するバックアップ ポリシー内のすべてのクライアントを別のバックアップ ポリシーに割り当てます。そうすることで、それらのクライアントのスケジュール設定されたバックアップを中断なく続行できます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[**Backup Policy**] をクリックします。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。
バックアップ ポリシーのサブドメインを選択するには、[**Include Sub-domain**] スイッチをオンに切り替えます。
3. 削除するバックアップ ポリシーを選択して、[**DELETE**] をクリックします。
確認のメッセージが表示されます。
4. [**YES**] をクリックします。

バックアップ ポリシーのオン デマンド バックアップの開始

インスタンスを保護すると、そのインスタンスが特定のバックアップ ポリシーに割り当てられます。1つのインスタンスに複数のバックアップ ポリシーを割り当てることができます。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[**Backup Policy**] をクリックします。
[**Policy**] ページが表示されます。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。
バックアップ ポリシーのサブドメインを選択するには、[**Include Sub-domain**] スイッチをオンに切り替えます。
3. リストからバックアップ ポリシーを選択し、[**START BACKUP**] をクリックします。
インスタンスは、バックアップ ポリシーで指定されたスケジュールと保存ポリシーに基づいて保護を受けます。

バックアップ ポリシーのスケジュール バックアップを有効にする

スケジュール バックアップは、有効化されたバックアップ ポリシーでのみ実行されます。[**New Group**] ウィザードの最初のページで [**Enabled**] チェックボックスを選択しない限り、バックアップ ポリシーはデフォルトで無効化されています。バックアップ ポリシーを作成したときに有効化しなかった場合は、[**Policy**] ウィンドウのメニュー オプションを使用して、バックアップを有効化します。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから、[**Backup Policy**] をクリックします。
[**Policy**] ページが表示されます。
2. ドメイン ツリーで、バックアップ ポリシーのドメインまたはサブドメインを選択します。
バックアップ ポリシーのサブドメインを選択するには、[**Include Sub-domain**] スイッチをオンに切り替えます。
3. リストからバックアップ ポリシーを選択します。
4. バックアップ ポリシーを有効化するには、[**MORE ACTIONS**] > [**Enable Policy**] をクリックします。
5. バックアップ ポリシーを無効化するには、[**MORE ACTIONS**] > [**Disable Policy**] をクリックします。

バックアップのモニタリング

[**Activity Monitor**] を使用して、バックアップ/リストア処理のステータス情報を監視および表示することができます。

[**Activity Monitor**] にアクセスするには、ナビゲーション ペインを開き、[**Activity**] をクリックします。[**Activity Monitor**] に、すべてのアクティビティのリストが表示されます。

注

AUI [**Activity Monitor**] ウィンドウは、1366 ピクセル以上の画面に合わせて最適化されています。小さな画面では、表示の問題が発生する可能性があります。AUI を正しく表示するには、ディスプレイの幅が 1366 ピクセル以上であることを確認します。

[**Activity Monitor**] には、表示される情報をフィルターするためのオプションが用意されています。

- アクティビティを期間別にフィルター：デフォルトでは、[**Activity Monitor**] には最新の 5000 クライアント アクティビティが表示されます。別の期間を選択するには、[**Filter activities by duration**] ドロップダウン リストで、[**Last 24 hours**] または [**Last 72 hours**] を選択します。
- ドメイン別にアクティビティをフィルター：デフォルトでは、[**Activity Monitor**] にはドメインに関係なくすべてのアクティビティが表示されます。特定のドメインのアクティビティのみを表示するには、[**Filter activities by domain**] ドロップダウン リストで、ドメインまたはサブドメインを選択します。
- ステータス別にアクティビティをフィルター：デフォルトでは、[**Activity Monitor**] にはステータスに関係なくすべてのアクティビティが表示されます。特定のステータスのアクティビティのみを表示するには、[**Activity Monitor**] の上部で、次のいずれかのオプションを選択します。
 - キャンセル済み
 - Completed
 - Completed with Exceptions (完了したが例外発生)
 - Failed
 - Running
 - Waiting

アクティビティをクライアント、開始時刻、プラグイン、またはタイプ別にフィルターするには、それぞれの列で [▼] をクリックします。

[**Activity Monitor**] には、アクティビティの開始日時と、アクティビティ中に検証された合計バイト数が表示されます。

アクティビティの詳細を表示するには、[◀◀] をクリックして、[**Details**] パネルを展開します。

バックアップのキャンセル

バックアップは完了前であればいつでもキャンセルできます。キャンセルには、5分以上かかる場合があります。バックアップがキャンセルよりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Activity**] をクリックします。
[**Activity Monitor**] にアクティビティのリストが表示されます。
2. リストからバックアップを選択します。
3. [**CANCEL**] をクリックします。
確認ダイアログ ボックスが表示されます。
4. [**YES**] をクリックします。

完了したバックアップの管理

オンデマンドバックアップまたはスケジュール設定されたバックアップを実行した後に、バックアップの検証、バックアップの設定の変更、バックアップの削除を実行できます。

完了した管理対象のバックアップの検索

完了したバックアップを見つけるには、特定のカレンダー日または特定の日付範囲に実行されたバックアップを検索するか、特定の保存タイプが指定されたバックアップを検索します。

通知


Avamar では、通常、ディレクトリ、フォルダー、ファイル名で特定の多言語文字の使用をサポートしています。ただし、多言語文字が正しく表示されるかどうかは、クライアント コンピューターの Java のロケール、および、クライアント コンピューターにインストールされているシステム フォントがその言語と互換性があるかどうか、によって決まります。多国語文字で作成されたバックアップを参照する際に、適切なフォントがインストールされていない場合、システムが判定できない文字は四角形で表示されます。この処理はあくまで表示時における制限事項であり、そのディレクトリ、フォルダー、ファイルをリストアできなくなるわけではありません。多言語文字のサポート情報については、「Avamar リリースノート」を参照してください。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。
[**Asset Management**] ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストから、管理対象のバックアップを持つクライアントを選択します。

4. 右側の **[Client Summary]** パネルで、**[VIEW MORE]** をクリックします。
5. **[Backups]** タブをクリックします。

このクライアントの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、クライアントのリストアに使用できます。

6. 日付別にバックアップを検索するには、次のようにします。
 - a.  をクリックします。
 - b. **[From]** フィールドおよび **[To]** フィールドで、日付範囲を指定します。
 - c. **[RETRIEVE]** をクリックします。

その日付範囲のバックアップのリストが表示されます。

バックアップの有効期限日の変更

バックアップの有効期限日を変更できます。バックアップの有効期限が切れると、Avamar ユーザーは有効期限切れのバックアップからデータをリカバリすることができなくなります。ガベージコレクションのプロセスが夜間に実行され、クリーンアップによって、孤立データ（有効期限が切れたバックアップ固有のデータ）からのスペースが再利用されます。

有効期限日は、選択した特定の日付か、特定の日数、週数、月数、年数の保存期間として指定できます。クライアントが Avamar サーバーでアクティブである限り、バックアップをバックアップストレージに維持するように構成することもできます。

手順

1. 左側の AUI ナビゲーション ペインで、**[>>]** をクリックしてから **[Asset Management]** をクリックします。
[Asset Management] ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストから、管理対象のバックアップを持つクライアントを選択します。
4. 右側の **[Client Summary]** パネルで、**[VIEW MORE]** をクリックします。
5. **[Backup]** タブをクリックします。
このクライアントの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、クライアントのリストアに使用できます。
6. 有効期限を変更するバックアップを選択します。
7. **[MORE ACTIONS]** > **[Change expiration date]** を選択します。
[Change expiration date] ダイアログ ボックスが表示されます。
8. 新しい有効期限の日付を選択します。
 - ある特定の時間が経過した後に、Avamar サーバからこのバックアップを自動的に削除する場合は、**[Retention period]** を選択し、保存期間の日数、週数、月数、年数を指定します。
 - ある特定のカレンダー日付に、Avamar サーバからこのバックアップを自動的に削除する場合は、**[End date]** を選択し、カレンダーでその日付を参照します。
 - このクライアントが Avamar サーバでアクティブである限り、このバックアップを保持する場合は、**[No end date]** を選択します。
9. **[OK]** をクリックします。
確認のメッセージが表示されます。

バックアップの保存タイプの変更

特定の詳細機能をサポートするため、Avamar Administrator では 1 つ以上の保存タイプをすべてのバックアップに自動的に割り当てます。例えば、Avamar システムで最初に作成されたバックアップは、日次、週次、月次、年次のいずれかでタグ付けされます。バックアップに割り当てられた保存タイプは、手動で変更することができます。

バックアップに割り当てられた保存タイプを手動で変更する場合、特に複数の保存タイプが割り当てられている場合は、保持する必要がある日次、週次、月次、年次のバックアップを誤って削除しないように注意してください。例えば、日次、週次、月次、または年次で割り当てている保存タイプのバックアップを考えてみましょう。年次の保存タイプの保存先を削除すると、年次のバックアップが長期間に渡り、システムに存在しなくなります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから **[Asset Management]** をクリックします。

[Asset Management] ウィンドウが表示されます。

2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストから、管理対象のバックアップを持つクライアントを選択します。
4. 右側の **[Client Summary]** パネルで、**[VIEW MORE]** をクリックします。
5. **[Backup]** タブをクリックします。

このクライアントの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、クライアントのリストアに使用できます。

6. 有効期限を変更するバックアップを選択します。
7. **[MORE ACTIONS]** > **[Change retention type]** を選択します。

[Change retention type] ダイアログ ボックスが表示されます。

8. バックアップの次のいずれかの保存タイプを選択します。
 - このバックアップに日単位、週単位、月単位、年単位の保存タイプを明示的に割り当てた場合は、**[Tags]** を選択し、保存タイプの横のチェックボックスを選択します。
 - バックアップに日単位、週単位、月単位、年単位の保存タイプを明示的に割り当てない場合は、**[Not tagged]** を選択します。このバックアップはタグ付けなしに認定されます。
9. **[OK]** をクリックします。

確認のメッセージが表示されます。

Avamar Administrator を使用したバックアップの検証

バックアップからファイルをリストアできるかどうかを検証することができます。この検証では、バックアップ内のすべてのファイルの「バーチャル」リストアが開始されますが、ファイルが実際にクライアントのファイル システムにリストアされるわけではありません。

手順

1. Avamar Administrator で、**[Backup & Restore]** 起動リンクをクリックします。
[Backup, Restore and Manage] ウィンドウが表示されます。
2. バックアップを見つけます。手順については、[完了した管理対象のバックアップの検索](#) (147 ページ) を参照してください。
3. **[Backup History]** リストで、検証するバックアップを選択します。

4. **[Actions]** > **[Validate Backup]** を選択します。
[Select Client to Perform Validation] ダイアログ ボックスが表示されます。
5. バックアップを検証するクライアントを選択します。
 - バックアップが本来実行されたクライアントと同じクライアントでバックアップを検証するには、**[Validate using the backup client]** を選択します。
 - 別のクライアントでバックアップを検証するには、**[Validate using a different client]** を選択し、**[Browse]** をクリックしてクライアントを参照します。
6. **[Validation Plug-in Type]** リストで、バックアップを検証するプラグインを選択します。選択したクライアントにインストール済みのプラグインだけがリストに表示されます。
7. **[Avamar encryption method]** リストから、検証中のクライアント/サーバ間のデータ転送に使用する暗号化方式を選択します。

注

バックアップ検証での暗号化は、元のバックアップで使用された暗号化設定にかかわらず、デフォルトで **[high]** に設定されています。

8. **[OK]** をクリックします。
確認メッセージが表示されます。
9. **[OK]** をクリックします。

必要条件

バックアップ検証が、**[Activity]** ウィンドウにアクティビティとして表示されます。バックアップの監視またはキャンセルを行う場合と同じ方法で、バックアップ検証アクティビティを監視およびキャンセルすることができます。手順については、[バックアップのモニタリング](#) (146 ページ) および [バックアップのキャンセル](#) (65 ページ) を参照してください。

バックアップ統計情報を表示

完了したバックアップの詳細な統計情報をダッシュボードで表示できます。

ダッシュボードにアクセスするには、左側の AUI ナビゲーション ペインで、**>>** をクリックし、**[Dashboard]** をクリックします。

[Dashboard] ウィンドウの **[Jobs | Backups]** パネルには、保存されているバックアップの統計情報が表示されます。

表 42 **[Jobs | Backups]** パネル

ステータス	説明
Running	実行中のバックアップ アクティビティを示します。
Scheduled	開始するようにキューに登録されているスケジュール バックアップ アクティビティを示します。
Complete	最後のジョブの実行中に正常にバックアップされたホストの数を示します。これは、各バックアップジョブの後に更新されます。バックアップ間のジョブの変更を反映するために、ジョブを再度実行する必要があります。たとえば、10 個のホストが正常にバックアップされたことをジョブが報告した場合、システムは 1 つのホストのみが保持されるようにジョブを編集します。ジョブが再度実行されるまで、この数字は 10 となります。成功した場合、数値は 1 に変更されます。

表 42 [Jobs | Backups] パネル (続き)

ステータス	説明
Failed	最後のジョブが実行されたときに正常にバックアップされなかったホストの数を示します。これは、各バックアップジョブの後に更新されます。バックアップ間のジョブの変更を反映するために、ジョブを再度実行する必要があります。たとえば、10 個のホストのバックアップに失敗したことをジョブが報告した場合、システムは 1 つのホストのみが保持されるようにジョブを編集します。ジョブが再度実行されるまで、この数字は 10 となります。ジョブが失敗した場合、数値は 1 に変更されます。

[Backup Statistics] ダイアログ ボックスの情報

次の情報が、[Backup Statistics] ダイアログ ボックスのタブに表示されます。

表 43 [Backup Statistics] ダイアログ ボックスの情報

タブ	情報
Details	v_activities_2 データベースビューからの詳細情報。v_activities_2 database ビューの詳細については、「Avamar レポート ガイド」を参照してください。
ファイル	バックアップ内のファイルのリストです。
File Aggregation	バックアップ内のリソースを大量に消費するファイルタイプの代表的なサンプルであり、ファイルタイプごとに重複排除の統計情報を集計します。
Options	バックアップの特殊オプションです。
Errors	バックアップ中に発生したエラーです。

バックアップの削除

バックアップを削除する場合、Avamar はそのバックアップ内のすべてのデータを、直ちにかつ完全にサーバから削除します。

手順

- 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Asset Management] をクリックします。
[Asset Management] ウィンドウが表示されます。
- ドメイン ツリーで、クライアントのドメインを選択します。
- クライアントのリストから、管理対象のバックアップを持つクライアントを選択します。
- 右側の [Client Summary] パネルで、[VIEW MORE] をクリックします。
- [Backup] タブをクリックします。

このクライアントの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、クライアントのリストアに使用できます。

- 削除するバックアップを選択し、[DELETE] をクリックします。

確認のメッセージが表示されます。

7. **[YES]** をクリックします。

第 7 章

リストアとリカバリ

本章は、次のトピックで構成されています。

- [バックアップからのデータのリストア](#) 154
- [リストアの監視](#) 157
- [リストアのキャンセル](#) 158
- [Windows クライアント システムのリカバリ](#) 159
- [Red Hat および CentOS Linux システムのリカバリ](#) 159
- [SUSE Linux システムのリカバリ](#) 166
- [Oracle Solaris システム リカバリ](#) 173

バックアップからのデータのリストア

リストア対象のバックアップは、日付またはバックアップのコンテンツで検索できます。リストアを実行する際は、元の場所、異なる場所、複数の場所のいずれかにリストアできます。

通知

リストア先のオプションはプラグインのタイプにより異なります。例えば、SQL Server プラグインでは SQL Server の代わりにファイルにリストアすることができ、Oracle プラグインでは複数の場所にリストアすることはできません。各プラグインのユーザーガイドには、使用可能なオプションや使用可能なリストアの各タイプの実行方法が詳しく説明されています。

バックアップの検索

データをリストアする際の最初のステップは、リストア対象のデータを含むバックアップを見つけることです。Avamar クライアントのバックアップを見つけるには、特定の日付またはコンテンツで検索できます。

次の状況のいずれか、または複数に当てはまる場合は、日付でバックアップを検索します。

- 単一のバックアップセットにクライアントのすべてのデータを保存している場合。
- リストア対象のデータの正確なパス名または名前が不明である場合。
- リストア対象のバックアップが、特定の日付やイベント以前のものである場合。例えば、データが消失あるいは破損したおおよその時期が分かっており、その日付よりも前のバックアップを検索できる場合が該当します。
- 具体的なバックアップのタイプがわかっている場合。例えば、毎週水曜日の夜と土曜日の夜にディザスタリカバリバックアップを実行していて、ボリューム全体のバックアップを毎日実行している場合です。サーバをビルドし直す必要がある場合、データ消失の原因となったイベントに直近の日付で、ディザスタリカバリバックアップを選択します。

次の状況のいずれか、または複数に当てはまる場合は、コンテンツでバックアップを検索します。

- 個別のバックアップセットにクライアントのデータをバックアップした場合。
- 同一のファイルの複数のバージョンを表示して、リストア対象のバージョンを決定することを希望する場合。
- バックアップの日付またはバックアップのコンテンツは不明だが、リストア対象のデータ名が分かっている場合。

通知

Avamar では、通常、ディレクトリ、フォルダー、ファイル名で特定の多言語文字の使用をサポートしています。ただし、多言語文字が正しく表示されるかどうかは、クライアントコンピューターの Java のロケール、および、クライアントコンピューターにインストールされているシステムフォントがその言語と互換性があるかどうか、によって決まります。多国語文字で作成されたバックアップを参照する際に、適切なフォントがインストールされていない場合、システムが判定できない文字は四角形で表示されます。この処理はあくまで表示時における制限事項であり、そのディレクトリ、フォルダー、ファイルをリストアできなくなるわけではありません。多言語文字のサポート情報については、「Avamar リリースノート」を参照してください。

日付によるバックアップの検索

手順

1. 左側の AUI ナビゲーション ペインで [>>] をクリックしてから、[**Asset Management**] をクリックします。
[**Asset Management**] ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
3. クライアントのリストから、管理対象のバックアップを持つクライアントを選択します。
4. 右側の [**Client Summary**] パネルで、[**VIEW MORE**] をクリックします。
5. [**Backup**] タブをクリックします。

このクライアントの完了したバックアップのリストが表示されます。このリストのすべてのバックアップを、クライアントのリストアに使用できます。

6. 日付別にバックアップを検索するには、次のようにします。
 - a. [**SEARCH**] をクリックします。
 - b. [**From**] フィールドおよび [**To**] フィールドで、日付範囲を指定します。
 - c. [**RETRIEVE**] をクリックします。

その日付範囲のバックアップのリストが表示されます。

元のクライアントへのリストア

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。
[**Asset Management**] ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。

ログイン アカountの対象となるドメイン外のクライアントは表示することはできません。すべてのクライアントを表示するには、root ドメインにログインします。

Avamar クライアントのリストが、ドメイン リストの下のパネルに表示されます。

3. クライアントのリストから、リカバリするクライアント コンピューターを選択します。
4. (オプション) 日付別にバックアップを検索するには、次のようにします。
 - a. 右側のパネルで、[**VIEW MORE**] をクリックします。
 - b. [**SEARCH**] をクリックします。
 - c. [**From**] フィールドおよび [**To**] フィールドで、日付範囲を指定します。
 - d. [**RETRIEVE**] をクリックします。
 - e. バックアップの一覧から、バックアップを選択します。

その日付範囲のバックアップのリストが表示されます。

5. [**Restore**] タブをクリックします。
[**Restore**] ウィザードが表示され、[**Destination Client**] パネルが右側に表示されま

6. [**Destination Client**] パネルで、次の手順を実行します。
 - a. [**Restore to original client**] を選択します。
 - b. [**NEXT**] をクリックします。[**Backup Content**] パネルが表示されます。
7. [**Backup Content**] パネルで、次の手順を実行します。
 - a. 左のパネルで、ツリーからフォルダーを選択します。
[**Backup Content**] パネルには、バックアップ内のデータベースのリストが表示されます。
 - b. 右のパネルで、リストアするデータベースを選択します。
 - c. [**NEXT**] をクリックします。[**Destination Location**] パネルが表示されます。
8. [**Destination Location**] パネルで、次の手順を実行します。
 - a. [**Restore everything to its original location**] を選択します。
 - b. [**Next**] をクリックします。[**More Options**] パネルが表示されます。
9. (オプション) [**More Option**] パネルで、[**Show Advanced Options**] スイッチをオンにして、詳細な構成オプションを表示します。
各オプションの詳細については、各プラグインのユーザーガイドを参照してください。
10. [**NEXT**] をクリックします。
[**Summary**] ページが表示されます。
11. 表示された情報を確認し、[**FINISH**] をクリックします。

異なるクライアントへのリストア

手順

1. 左側の AUI ナビゲーション ペインで、[>>>] をクリックしてから [**Asset Management**] をクリックします。
[**Asset Management**] ウィンドウが表示されます。
2. ドメイン ツリーで、クライアントのドメインを選択します。
ログイン アカウントの対象となるドメイン外のクライアントは表示することはできません。すべてのクライアントを表示するには、root ドメインにログインします。
Avamar クライアントのリストが、ドメイン リストの下のパネルに表示されます。
3. クライアントのリストから、リカバリするクライアント コンピューターを選択します。
4. (オプション) 日付別にバックアップを検索するには、次のようにします。
 - a. 右側のパネルで、[**VIEW MORE**] をクリックします。
 - b. [**SEARCH**] をクリックします。
 - c. [**From**] フィールドおよび [**To**] フィールドで、日付範囲を指定します。
 - d. [**RETRIEVE**] をクリックします。

- e. バックアップの一覧から、バックアップを選択します。
その日付範囲のバックアップのリストが表示されます。
5. **[Restore]** タブをクリックします。
[Restore] ウィザードが表示され、**[Destination Client]** パネルが右側に表示されま
す。
6. **[Destination Client]** パネルで、次の手順を実行します。
 - a. **[Restore everything to a different client]** を選択します。
 - b. ドメイン ツリーで、クライアントのドメインを選択します。
 - c. クライアントのリストから、宛先クライアントを選択します。
クライアントが **[Destination Client]** フィールドに表示されます。
 - d. **[NEXT]** をクリックします。
[Backup Content] パネルが表示されます。
7. **[Backup Content]** パネルで、次の手順を実行します。
 - a. 左のパネルで、ツリーからフォルダーを選択します。
[Backup Content] パネルには、バックアップ内のデータベースのリストが表示されます。
 - b. 右のパネルで、リストアするデータベースを選択します。
 - c. **[NEXT]** をクリックします。
[Destination Location] パネルが表示されます。
8. **[Destination Location]** パネルで、次の手順を実行します。
 - a. **[Restore everything to a different location]** を選択します。
 - b. **[Restore Location]** フィールドに、データをリストアするターゲットの場所へのファイル パ
スを入力します。
例 : E:/dbrestore_dir/
 - c. **[NEXT]** をクリックします。
[More Options] パネルが表示されます。
9. (オプション) **[More Option]** パネルで、**[Show Advanced Options]** スイッチをオンに
して、詳細な構成オプションを表示します。
各オプションの詳細については、各プラグインのユーザー ガイドを参照してください。
10. **[NEXT]** をクリックします。
[Summary] ページが表示されます。
11. 表示された情報を確認し、**[FINISH]** をクリックします。

リストアの監視

[Activity Monitor] では、バックアップおよびリストア処理のステータス情報を監視および表示することができま

す。**[Activity Monitor]** にアクセスするには、ナビゲーション ペインを開き、**[Activity]** をクリックしま
す。**[Activity Monitor]** に、すべてのアクティビティのリストが表示されます。

注

AUI [Activity Monitor] ウィンドウは、1366 ピクセル以上の画面に合わせて最適化されています。小さな画面では、表示の問題が発生する可能性があります。AUI を正しく表示するには、ディスプレイの幅が 1366 ピクセル以上であることを確認します。

[Activity Monitor] には、表示される情報をフィルターするためのオプションが用意されています。

- アクティビティを期間別にフィルター：デフォルトでは、[Activity Monitor] には最新の 5000 クライアント アクティビティが表示されます。別の期間を選択するには、[Filter activities by duration] ドロップダウン リストで、[Last 24 hours] または [Last 72 hours] を選択します。
- ドメイン別にアクティビティをフィルター：デフォルトでは、[Activity Monitor] にはドメインに関係なくすべてのアクティビティが表示されます。特定のドメインのアクティビティのみを表示するには、[Filter activities by domain] ドロップダウン リストで、ドメインまたはサブドメインを選択します。
- ステータス別にアクティビティをフィルター：デフォルトでは、[Activity Monitor] にはステータスに関係なくすべてのアクティビティが表示されます。特定のステータスのアクティビティのみを表示するには、[Activity Monitor] の上部で、次のいずれかのオプションを選択します。
 - キャンセル済み
 - Completed
 - Completed with Exceptions (完了したが例外発生)
 - Failed
 - Running
 - Waiting

アクティビティをクライアント、開始時刻、プラグ イン、またはタイプ別にフィルターするには、それぞれの列で [▼] をクリックします。

[Activity Monitor] には、アクティビティの開始日時と、アクティビティ中に検証された合計バイト数が表示されます。

アクティビティの詳細を表示するには、[◀◀] をクリックして、[Details] パネルを展開します。

リストアのキャンセル

リストアは完了前であればいつでもキャンセルできます。キャンセルには、5 分以上かかる場合があります。リストアがキャンセルの終了よりも前に完了することがあります。

手順

1. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [Activity] をクリックします。
[Activity Monitor] にアクティビティのリストが表示されます。
2. リストからリストアを選択します。
3. [CANCEL] をクリックします。
確認ダイアログ ボックスが表示されます。
4. [YES] をクリックします。

Windows クライアント システムのリカバリ

Windows クライアント システムのリカバリに必要なバックアップに関する包括的な詳細情報や、リカバリを実行する処理手順については、「Avamar for Windows Server ユーザー ガイド」を参照してください。

Red Hat および CentOS Linux システムのリカバリ

次のトピックでは、Red Hat または CentOS Linux クライアント システムを元のシステム状態にリストアする方法について詳しく説明します。

パーティション テーブルの再構築

Linux クライアントのシステム リカバリを実行する前に、リカバリ元の Avamar バックアップで使用されているパーティション テーブルを再構築する必要があります。このアクションは、一時クライアント コンピューターで `avtar --showlog mounts` コマンドを実行して実施します。このアクションで、出力を調べて、ターゲット リカバリ クライアントにオペレーティング システムをインストールするときに作成するパーティションの数とサイズを判断します。

手順

1. 次の手順でバックアップを見つけます。

このステップで取得した情報を使用して、システム状態のリカバリーを実行します。

- a. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。

[**Asset Management**] ウィンドウが表示されます。

- b. ドメイン ツリーで、クライアントのドメインを選択します。
- c. クライアントのリストから、リカバリーする元の Linux クライアントを選択します。
- d. 左側の [**Client Summary**] パネルで、[**VIEW MORE**] をクリックします。
- e. [**Backups**] タブをクリックします。
- f. システム状態のリカバリに使用するフル システム バックアップを見つけます。
- g. バックアップ ラベル番号をメモします。
- h. システム状態リカバリ手順の情報のために AUI は開いたままの状態にします。

2. Avamar サーバとネットワーク接続している一時クライアント コンピューター上で、コマンド シェルを開き、root としてログインします。

3. 以下のコマンドを入力します。

```
/usr/local/avamar/bin/avtar --avamaronly --showlog mounts --
server=Avamar_server --id=username --ap=password --path=/domain/
client --labelnumber=n
```

各項目の意味は次のとおりです。

- Avamar_server は、Avamar サーバの IP アドレスまたは DNS で定義された完全修飾ホスト名です。
- username および password は、リストアを実行するために十分なロールと権限を持つユーザー アカウントのログイン認証情報です。

- `/domain/client` は、Avamar サーバの元の Linux クライアントの完全な場所です。
 - `n` は、システム状態のリカバリに使用するバックアップのラベル番号です。
4. コマンド出力をチェックし、`mount_decision` で開始するエントリーを見つけます。

例：

```
mount_decision: reason="starting_point" fstype="ext3"
path="/"
mount_decision: reason="default_backup" fstype="ext3"
path="/boot"
mount_decision: reason="default_backup" fstype="ext3"
path="/home"
```

これらは元のシステムのマウント ポイントのエントリーです。出力の前半に、これらのマウント ポイントのそれぞれに対するエントリーがあります。例：

```
mount: status="user_directed_backup" path="/" hdev="/dev/
root" kind="ext3" blksize=4096 freeblks=1189334
maxblks=2405872 freefiles=2259654 maxfiles=2432000
dev=2050

mount: status="default_backup" path="/boot" hdev="/dev/
sda1" kind="ext3" blksize=1024 freeblks=183371
maxblks=194442 freefiles=50167 maxfiles=50200 dev=2049

mount: status="default_backup" path="/home" hdev="/dev/
sdb1" kind="ext3" blksize=4096 freeblks=1027161
maxblks=5158925 freefiles=2530548 maxfiles=2621440
dev=2065
```

これらのエントリーには、マウント ポイントのサイズおよびパス情報が含まれています。

5. `blksize` 値と `maxblks` 値を乗算して、元のファイル システムのサイズまたは各マウント ポイントを計算します (単位：バイト)。

通知

`blksize` 値と `maxblks` 値の乗算により、元のデバイスで使用される空き領域が計算されます。ただし、リストア処理で使用する最小インストールで十分な領域を確保できるように、2 GB～3 GB の空き領域を追加して `root` パーティションを作成する必要があります。

6. 個別のファイル システムからマウントされるパスをメモします。この情報は後でリストア処理で必要になります。

ターゲット リカバリ クライアントの準備

手順

1. リカバリ先ディスクが、ターゲット リカバリ クライアントに接続されていることを確認します。
2. 互換 OS の最小インストールを実行します。この処理手順を実行する前に、次の内容について理解しておく必要があります。
 - 最小インストールとは、[Desktop - Gnome] などのデスクトップ環境のエントリーをインストールで選択してはならないことを意味しています。
 - [Customize Now] ダイアログ ボックスの [Base System] カテゴリで、[Base] オプションを選択します。すべての他のオプションは無効のままにします。

- 互換 OS とは、同じバージョンを意味しています。たとえば、Avamar サーバー上の元のクライアントバックアップが RHEL3 クライアントで実行された場合、ターゲットリカバリクライアントに RHEL3 をインストールします。
 - [パーティションテーブルの再構築](#) (159 ページ) で収集された情報を使用して、元の構成のレプリケートに必要な数だけパーティションを作成します。
3. (オプション) `/etc/fstab` ファイルのコピーを保存して、リストアされた `/etc/fstab` ファイルと比較できるようにします。
 4. Linux 用 Avamar クライアントをインストールします。Data Domain システムへのバックアップに関する指示については、「Avamar バックアップ クライアント ユーザー ガイド」を参照してください。

Red Hat または CentOS Linux クライアントのシステム リカバリを実行する

はじめに

[パーティションテーブルの再構築](#) (159 ページ) と [ターゲットリカバリクライアントの準備](#) (160 ページ) で説明されているステップを実行します。

手順

1. リカバリターゲットクライアントを、インストールメディア (CD/DVD1) から起動します。
 - Red Hat または CentOS 4、5 のいずれかでは、コマンドプロンプトに `linux rescue` を入力します。
 - Red Hat または CentOS 6.0 では、**[Rescue installed system]** を選択します。
 - Red Hat または CentOS 7.0 以降の場合：
 - a. **[Troubleshooting]** を選択します。
 - a. **[Rescue a Red Hat Enterprise Linux system]** を選択します。
2. 画面上に表示される指示に従います。

IP アドレス、ネットワークマスク、デフォルトゲートウェイおよび DNS サーバーの値を指定してネットワークを必ず有効にしてください。一時的なホスト名および IP、またはリストアするコンピューターの元の情報を使用できます。
3. Red Hat または CentOS 7.0 以降では、次の手順を実行してネットワークを設定します。
 - a. `root` としてログインします。
 - b. `chroot /mnt/sysimage`
 - c. `/etc/hosts`、`/etc/resolv.conf`、`/etc/sysconfig/network` をネットワークの構成に応じて変更します。
 - d. 変更を反映するために、ネットワークサービスを再起動します。


```
service network restart
```
 - e. `exit` と入力してシングルユーザーモードに戻ります。
4. インストーラーでインストールを検索し、読み取り/書き込みとして `/mnt/sysimage` ファイルシステムがマウントできるようにします。

`/mnt/sysimage` ファイルシステムは、リストアのターゲットであり、**[リカバリ先ディスク]** とも呼ばれます。

注

root ファイル システムを直接 `/mnt/sysimage` にリストアすることはできません。これは、ネットワーク マウント ポイントを経由せずにリストア処理をローカル パーティションのみに限定する方法がないためです。したがって、直接 `/mnt/sysimage` にリストアを行うと、ファイルがすべてのパーティションからコピーされるので、必要なファイルがすべてリストアされる前に、`/mnt/sysimage` がいっぱいになる可能性があります。

5. 次のディレクトリがすべて `LD_LIBRARY_PATH` システム変数に存在することを確認します。

- `/lib`
- `/lib64`
- `/usr/lib`
- `/usr/lib64`
- `/mnt/sysimage/lib`
- `/mnt/sysimage/lib64`
- `/mnt/sysimage/usr/local/avamar/lib`

`LD_LIBRARY_PATH` に存在しないディレクトリがあれば、追加します。

6. UNIX テキスト エディターで `/tmp/avtar.cmd` 一時フラグ ファイルを作成します。例：

```
cd /tmp; vi avtar.cmd --bindir=/mnt/sysimage/usr/local/avamar/bin --
vardir=/mnt/sysimage/usr/local/avamar/var --sysdir=/mnt/
sysimage/usr/local/avamar/etc --server=Avamar_server --account=
domain/client --id=username --ap=password --target=.
```

ここで、

- `Avamar_server` は、Avamar サーバーの IP アドレス、または DNS で定義されている完全修飾ホスト名です。
- `/domain/client` は、Avamar サーバーの元の Linux クライアントの完全な場所です。
- `username` および `password` はリストアを実行するために十分なロールと権限を持つユーザー アカウントのログイン認証情報です。

7. 元ルート(/)の下に存在していたほとんどのディレクトリは、次の手順でリストアします。

通知

この時点では root ファイル システム以外のファイル システムに存在するファイルのリストアは行わないでください。これらのディレクトリとファイルは後でこの手順でリストアされます。

- a. クライアントの `/mnt/sysimage` ディレクトリで一時リストア ディレクトリを作成し、次の例に似たコマンドを入力して、ディレクトリを変更します。

```
mkdir /mnt/sysimage/restorecd /mnt/sysimage/restore
```

- b. root ファイル システムの内容を、次のとおりに 1 行のコマンドラインで入力して、バックアップからリストアします。

```
/mnt/sysimage/usr/local/avamar/bin/avtar.bin -x --
flagfile=/tmp/avtar.cmd --labelnumber=n [--exclude=./boot --
exclude=./home] /
```

ここで、n はシステム状態のリカバリに使用するバックアップのラベル番号です。

--exclude=path オプションを使用して、個別のマウントポイントとして特定されたパスを除外します。これらのディレクトリとファイルは後でこの手順で個別にリストアされます。前述のコマンドで使用した最初の2つの--exclude オプションは、例として含まれています。これらの値は、リストアしているシステムに適したオプションで置き換えます。exclude オプションは、元のバックアップのrootとの相対関係で指定します。例えば、--exclude=/boot ではなく、--exclude=./boot と指定します。

- c. リストアされた各ディレクトリで次の例に似たコマンドを入力して、元のディレクトリを/mnt/sysimage から削除し、リストアされたディレクトリを/mnt/sysimage/restore ディレクトリから/mnt/sysimage に移動します。

```
rm -rf /mnt/sysimage/etcmv /mnt/sysimage/restore/etc /mnt/
sysimage/etc
```

- d. /mnt/sysimage/restore に正常にリストアされた各ディレクトリで、これまでのステップを繰り返します。

8. ルート(/)ディレクトリ内の個々のファイルのリストア。

- a. 次のコマンドを入力して、ディレクトリを/mnt/sysimage/restore に変更します。

```
cd /mnt/sysimage/restore
```

- b. 次のコマンドを入力して、root (/) ディレクトリ内の個々のファイルをリストアします。

```
mv /* /mnt/sysimage mv /* /mnt/sysimage
```

9. 他のマウントポイントをリストアします。

- a. コマンドプロンプトで df -h と入力して、ファイルシステムが期待どおりにマウントされているかを確認します。

- b. マウントされたファイルシステムの予想されるセットと出力を比較します。不一致があれば、デバイスを正しいマウントポイントにマウントします。

- c. 次の例に似たコマンドを入力して、ディレクトリを各マウントポイントに変更します。

```
cd /mnt/sysimage/home
```

- d. 一時リストアディレクトリを作成して、次の例に似たコマンドを入力し、ディレクトリを変更します。

```
mkdir ./restored ./restore
```

- e. 次のコマンドを入力して、マウントポイントのコンテンツをリストアします。

```
/mnt/sysimage/usr/local/avamar/bin/avtar.bin -x --
flagfile=/tmp/avtar.cmd --labelnumber=n /home
```

ここで、n はリストアに使用するバックアップのラベル番号であり、/home はマウントポイントの例です。

- f. マウントポイントのディレクトリに戻り、次の例に似たコマンドを入力して、リストアディレクトリ以外のすべてのファイルを削除します。

```
alias ls=/usr/bin/lscd /mnt/sysimage/home; rm -rf `ls --hide
restore`rm -rf ./.*
```

- g. ディレクトリを `restore` ディレクトリに変更し、次のコマンドを入力して、コンテンツをマウントポイントの正しい場所に移動します。

```
cd ./restore;mv `ls -A ./` ..
```

- h. 次のコマンドを入力して、`restore` ディレクトリを削除します。

```
cd ../rmdir restore
```

- i. 残りの各マウントポイントで、ステップ d~i を繰り返します。

10. 次の手順で、最終的なシステムチェックを実行します。

- a. `/mnt/sysimage/etc/fstab` を検査し、新しいシステムにマウントする必要がある各ファイルシステムについて、有効なステートメントがあることを確認します。

デバイスを `fstab` ファイルに表示するには、デバイスのパス、ボリュームラベル、UUID (Universally Unique Identifier) の 3 種類の方法があります。

ファイルシステムのこの情報は、`/mnt/sysimage/lib/udev/vol_id` `device_path` を入力して確認できます。ここで `device_path` はデバイスへの `/dev` パスです。

このプログラムがシステムに存在しない場合は、`/mnt/sysimage/sbin/blkid` `device_path` と入力します。

最小システムインストール時にパーティションを手動で作成した場合、デバイス UUID が変更された可能性があります。`/mnt/sysimage/etc/fstab` でデバイス UUID を更新します。一部のボリュームでラベルが見つからない場合、`/mnt/sysimage/sbin/e2label device_path label` を入力してラベルを設定します。

- b. `fstab` を慎重に再確認します。

リストアされたシステムは、`fstab` エントリーがストレージデバイスの構成と完全に一致しない場合は正常に起動できません。そのため、インストールメディアのレスキューシステムは、`/mnt/sysimage` にマウントするファイルシステムの検出が困難になります。

注

リカバリ用にターゲットクライアントを準備した際に、`fstab` ファイルの参照コピーを保存した場合は、そのファイルでディスク情報を確認できます。リストアされた `fstab` ファイルに手動による変更がほとんど加えられていないシステムの場合、リストアされたファイルのコピーの代わりに参照 `fstab` ファイルを使用することが可能な場合もあります。

- c. 次のコマンドを入力して、`/mnt/sysimage/restore` に他のファイルが存在しないことを確認します。

```
ls -al /mnt/sysimage/restore
```

- d. ディレクトリが空の場合は、次のコマンドを入力して、このディレクトリを削除します。

```
rmdir /mnt/sysimage/restore
```

- e. ディレクトリが空でないためにこのコマンドが失敗する場合は、`root (/)` にあるほとんどのディレクトリをリストアした際に、移動できなかったディレクトリが存在する可能性があります。ディレクトリをリストアの正しい場所に移動します。

11. `exit` と入力してコマンド シェルを終了し、システムを再起動します。
Red Hat または CentOS 6 システムを再起動する場合は、メニューが表示されます。
12. [`reboot`]、[`OK`] を選択し、[`Enter`] キーを押します。
システムが再起動します。
13. インストール メディアを取り出し、通常どおりに起動します。
14. クライアントが正しく動作することを確認します。

Red Hat または CentOS Linux クライアントのシステム リカバリに関するトラブルシューティング

次のトピックでは、Red Hat または CentOS Linux クライアントのシステム リカバリを実行した後で発生する可能性のある問題のトラブルシューティングについて、詳しく説明します。

システム リカバリ後の起動障害のトラブルシューティング

リストアされたシステムがリストア処理手順の終わりに起動しない場合、最小 OS によってインストールされた GRUB のバージョンが、サーバでの以前のバージョンと異なる可能性があります。リストア環境で起動し、GRUB を再インストールします。

手順

1. クライアントをインストール メディアからレスキュー オプションを使用して開始し、リストア環境で起動します。
2. 起動プロセスでリストアされたオペレーティング システムが見つからない場合は、このオペレーティング システムの `fstab` が適切に構成されていない可能性があります。パーティションを手動でマウントし、このファイルのコンテンツを修正します。
3. 次のコマンドを入力して、GRUB を再インストールします。

```
chroot /mnt/sysimagegrub-install device
```

ここで、`device` は起動デバイス（例：`/dev/sda`）です。

4. `exit` と入力して、`chroot` 環境を終了します。
5. `exit` と入力してコマンド シェルを終了し、システムを再起動します。
Red Hat または CentOS 6 システムを再起動する場合は、メニューが表示されます。
6. [`reboot`]、[`OK`] を選択し、[`Enter`] キーを押します。
システムが再起動します。
7. インストール メディアを取り出し、通常どおりに起動します。

Linux クライアントのシステム リカバリ後にネットワーク設定をリストアする

システムが新しいハードウェアにリストアされたことが OS によって検出された場合、ネットワーク設定がデフォルトに戻される可能性があります（例えば、固定 IP ではなく、DHCP 名前解決）。設定を手動で再構成することにより、以前のネットワーク設定をリカバリできます。

以前の設定を確認するには、`/etc/sysconfig/network-scripts` にある `.bak` ファイルをテキスト エディターで開きます。これらのファイルには有益な情報が含まれていますが、それらには以前のハードウェアの MAC アドレス情報が含まれているため、未修正の形で現在の構成で使用してはいけません。

SUSE Linux システムのリカバリ

次のトピックでは、SUSE Linux クライアント システムを元のシステム状態にリストアする方法について説明します。

パーティション テーブルの再構築

Linux クライアントのシステム リカバリを実行する前に、リカバリ元の Avamar バックアップで使用されているパーティション テーブルを再構築する必要があります。このアクションは、一時クライアント コンピューターで `avtar --showlog mounts` コマンドを実行して実施します。このアクションで、出力を調べて、ターゲット リカバリ クライアントにオペレーティング システムをインストールするときに作成するパーティションの数とサイズを判断します。

手順

1. 次の手順でバックアップを見つけます。
このステップで取得した情報を使用して、システム状態のリカバリーを実行します。
 - a. 左側の AUI ナビゲーション ペインで、[>>] をクリックしてから [**Asset Management**] をクリックします。
[Asset Management] ウィンドウが表示されます。
 - b. ドメイン ツリーで、クライアントのドメインを選択します。
 - c. クライアントのリストから、リカバリーする元の Linux クライアントを選択します。
 - d. 左側の [**Client Summary**] パネルで、[**VIEW MORE**] をクリックします。
 - e. [**Backups**] タブをクリックします。
 - f. システム状態のリカバリに使用するフル システム バックアップを見つけます。
 - g. バックアップ ラベル番号をメモします。
 - h. システム状態リカバリ手順の情報のために AUI は開いたままの状態にします。
2. Avamar サーバとネットワーク接続している一時クライアント コンピューター上で、コマンド シェルを開き、`root` としてログインします。
3. 以下のコマンドを入力します。

```
/usr/local/avamar/bin/avtar --avamaronly --showlog mounts --
server=Avamar_server --id=username --ap=password --path=/domain/
client --labelnumber=n
```

各項目の意味は次のとおりです。

- `Avamar_server` は、Avamar サーバの IP アドレスまたは DNS で定義された完全修飾ホスト名です。
- `username` および `password` は、リストアを実行するために十分なロールと権限を持つユーザー アカウントのログイン認証情報です。
- `/domain/client` は、Avamar サーバの元の Linux クライアントの完全な場所です。
- `n` は、システム状態のリカバリに使用するバックアップのラベル番号です。

4. コマンド出力をチェックし、`mount_decision` で開始するエントリーを見つけます。

例：

```
mount_decision: reason="starting_point" fstype="ext3"
path="/"
mount_decision: reason="default_backup" fstype="ext3"
path="/boot"
mount_decision: reason="default_backup" fstype="ext3"
path="/home"
```

これらは元のシステムのマウント ポイントのエントリーです。出力の前半に、これらのマウント ポイントのそれぞれに対するエントリーがあります。例：

```
mount: status="user_directed_backup" path="/" hdev="/dev/
root" kind="ext3" blksize=4096 freeblks=1189334
maxblks=2405872 freefiles=2259654 maxfiles=2432000
dev=2050

mount: status="default_backup" path="/boot" hdev="/dev/
sda1" kind="ext3" blksize=1024 freeblks=183371
maxblks=194442 freefiles=50167 maxfiles=50200 dev=2049

mount: status="default_backup" path="/home" hdev="/dev/
sdb1" kind="ext3" blksize=4096 freeblks=1027161
maxblks=5158925 freefiles=2530548 maxfiles=2621440
dev=2065
```

これらのエントリーには、マウント ポイントのサイズおよびパス情報が含まれています。

5. `blksize` 値と `maxblks` 値を乗算して、元のファイル システムのサイズまたは各マウント ポイントを計算します (単位：バイト)。

通知

`blksize` 値と `maxblks` 値の乗算により、元のデバイスで使用される空き領域が計算されます。ただし、リストア処理で使用する最小インストールで十分な領域を確保できるように、2 GB～3 GB の空き領域を追加して `root` パーティションを作成する必要があります。

6. 個別のファイル システムからマウントされるパスをメモします。この情報は後でリストア処理で必要になります。

ターゲット リカバリ クライアントの準備

手順

1. リカバリ先ディスクが、ターゲット リカバリ クライアントに接続されていることを確認します。
2. 互換 OS の最小インストールを実行します。この処理手順を実行する前に、次の内容について理解しておく必要があります。
 - 最小インストールとは、[**Base System**] および [**Minimal System (Appliances)**] パッケージのみが [**Software selection**] ページからインストールされることを意味します。その他のパッケージはインストールされないように、すべて選択を解除するようにしてください。
 - 互換 OS とは、同じバージョンを意味しています。例えば、Avamar サーバ上の元のクライアントバックアップが SLES10 クライアントで実行された場合、ターゲット リカバリ クライアントに SLES10 をインストールします。
 - [パーティション テーブルの再構築](#) (159 ページ) で収集された情報を使用して、元の構成のレプリケートに必要な数だけパーティションを作成します。

3. (オプション) `/etc/fstab` ファイルのコピーを保存して、リストアされた `/etc/fstab` ファイルと比較できるようにします。
4. Linux 用 Avamar クライアントをインストールします。Data Domain システムへのバックアップに関する指示については、「Avamar バックアップ クライアント ユーザー ガイド」を参照してください。

SUSE Linux クライアントのシステム リカバリを実行する

はじめに

[パーティションテーブルの再構築](#) (159 ページ) と [ターゲット リカバリ クライアントの準備](#) (167 ページ) で説明されているステップを実行します。

手順

1. リカバリ ターゲット クライアントを、インストール メディア (CD-ROM/DVD1) から起動し、**[Rescue System]** を選択します。
2. リカバリ ターゲット クライアントでコマンド シェルを開き、`root` としてログインします。
3. 次のコマンドを入力して、最小インストールで作成された `root` パーティションを `/mnt` にマウントします。

```
mount /dev/sda# /mnt
```

ここで、`/dev/sda#` は `root` ファイル システムを含むデバイスです。Linux 論理ボリューム マネージャーを使用するようにドライブが構成されている場合、`root` デバイスは `/dev/VolGroup##/LogVol##` の形式になっていることがあります。

4. 次のコマンドを入力して仮想ファイル システムを `/mnt` ツリーに再バインドします

```
mount --rbind /proc /mnt/procmount --rbind /sys /mnt/sysmount --rbind /dev /mnt/dev
```

5. 次のコマンドを入力して、現在のファイル システムの `root` を変更します。

```
chroot /mnt
```

6. 次のコマンドを入力して、前提条件で構成されたように、ネットワークを開始します。

```
rcnetwork start
```

7. 次のコマンドを入力して、自動マウント ファイル システムをマウントし、適切なファイル システムがマウントされたことを確認します。

```
mount -a;df -h
```

8. ファイル システムが存在しない場合 (例えば、`/boot` が自動マウントに設定されていない場合)、追加の `mount` コマンドを使用して、それらを正しい場所に手動でマウントします。

9. `exit` と入力して、`chroot` 環境を終了します。

10. 次のコマンドを入力して、`chroot` 環境から作業中のリストア環境にネットワーク名前解決ファイルをコピーします。

```
cp /mnt/etc/resolv.conf /etc/resolv.conf
```

11. 次のディレクトリがすべて `LD_LIBRARY_PATH` システム変数に存在することを確認します。

- `/lib`
- `/lib64`

- /usr/lib
- /usr/lib64
- /mnt/lib
- /mnt/lib64
- /mnt/usr/local/avamar/lib

LD_LIBRARY_PATH に存在しないディレクトリがあれば、追加します。

12. UNIX テキスト エディターで/tmp/avtar.cmd 一時フラグ ファイルを作成します。例：

```
cd /tmpvi avtar.cmd--bindir=/mnt/usr/local/avamar/bin--
vardir=/mnt/usr/local/avamar/var--sysdir=/mnt/usr/local/avamar/
etc--server=Avamar_server--account=/domain/client--id=username--
ap=password--target=.
```

ここで、

- Avamar_server は、Avamar サーバの IP アドレスまたは DNS で定義された完全修飾ホスト名です。
- /domain/client は、Avamar サーバの元の Linux クライアントの完全な場所です。
- username および password はリストアを実行するために十分なロールと権限を持つユーザーアカウントのログイン認証情報です。

13. 元ルート(/)の下に存在していたほとんどのディレクトリは、次の手順でリストアします。

通知

この時点では root ファイル システム以外のファイル システムに存在するファイルのリストアは行わないでください。これらのディレクトリとファイルは後でこの手順でリストアされます。

- a. クライアントの/mnt ディレクトリで一時リストア ディレクトリを作成し、次の例に似たコマンドを入力して、ディレクトリを変更します。

```
mkdir /mnt/restorecd /mnt/restore
```

- b. root ファイル システムの内容を、次のとおりに入力して、バックアップからリストアします。

```
/mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/
avtar.cmd --labelnumber=n [--exclude=./boot --exclude=./
home] /
```

ここで、n はシステム状態のリカバリに使用するバックアップのラベル番号です。

--exclude=path オプションを使用して、個別のマウント ポイントとして特定されたパスを除外します。これらのディレクトリとファイルは後でこの手順で個別にリストアされます。

前述のコマンドで使用した最初の 2 つの--exclude オプションは、例として含まれています。これらの値は、リストアしているシステムに適したオプションで置き換えます。

exclude オプションは、元のバックアップの root との相対関係で指定します。例えば、--exclude=/boot ではなく、--exclude=./boot と指定します。

- c. リストアされた各ディレクトリで次の例に似たコマンドを入力して、元のディレクトリを/mnt から削除し、リストアされたディレクトリを/mnt/restore ディレクトリから/mnt に移動します。

```
rm -rf /mnt/etcmv /mnt/restore/etc /mnt/etc
```

d. /mnt/restore に正常にリストアされた各ディレクトリで、これまでのステップを繰り返します。

14. ルート(/)ディレクトリ内の個々のファイルのリストア。

a. `cd /mnt/restore` と入力して、ディレクトリ/mnt/restore をに変更します。

b. 次のコマンドを入力して、root (/) ディレクトリ内の個々のファイルをリストアします。

```
mv /* /mntmv /*.* /mnt
```

15. 他のマウント ポイントをリストアします。

a. コマンド プロンプトで `df -h` と入力して、ファイル システムが期待どおりにマウントされているかを確認します。

b. マウントされたファイル システムの予想されるセットと出力を比較します。不一致があれば、デバイスを正しいマウント ポイントにマウントします。

c. 次の例に似たコマンドを入力して、ディレクトリを各マウント ポイントに変更します。

```
cd /mnt/home
```

d. 一時リストア ディレクトリを作成して、次の例に似たコマンドを入力し、ディレクトリを変更します。

```
mkdir ./restorecd ./restore
```

e. 次のコマンドを入力して、マウント ポイントのコンテンツをリストアします。

```
/mnt/usr/local/avamar/bin/avtar.bin -x --flagfile=/tmp/  
avtar.cmd --labelnumber=n /home
```

ここで、n はリストアに使用するバックアップのラベル番号であり、/home はマウント ポイントの例です。

f. マウント ポイントのディレクトリに戻り、次の例に似たコマンドを入力して、リストア ディレクトリ以外のすべてのファイルを削除します。

```
alias ls=/usr/bin/lscd /mnt/home; rm -rf `ls --hide restore`rm  
-rf /*.*
```

g. ディレクトリを restore ディレクトリに変更し、次のコマンドを入力して、コンテンツをマウント ポイントの正しい場所に移動します。

```
cd ./restore;mv `ls -A ./` ..
```

h. 次のコマンドを入力して、restore ディレクトリを削除します。

```
cd ../rmdir restore
```

i. 残りの各マウント ポイントで、ステップ d~i を繰り返します。

16. 次の手順で、最終的なシステム チェックを実行します。

a. /mnt/etc/fstab を検査し、新しいシステムにマウントする必要がある各ファイル システムについて、有効なステートメントがあることを確認します。

デバイスを `fstab` ファイルに表示するには、デバイスのパス、ボリューム ラベル、UUID (Universally Unique Identifier) の 3 種類の方法があります。

ファイル システムのこの情報は、`/mnt/lib/udev/vol_id device_path` を入力して確認できます。ここで `device_path` はデバイスへの `/dev` パスです。

最小システム インストール時にパーティションを手動で作成した場合、デバイス UUID が変更された可能性があります。`/mnt/etc/fstab` でデバイス UUID を更新します。一部のボリュームでラベルが見つからない場合、`/mnt/sbin/e2label device_path label` を入力してラベルを設定します。

- b. `fstab` を慎重に再確認します。

リストアされたシステムは、`fstab` エントリーがストレージ デバイスの構成と完全に一致しない場合は正常に起動できません。そのため、インストール メディアのレスキュー システムは、`/mnt` にマウントするファイル システムの検出が困難になります。

注

リカバリ用にターゲット クライアントを準備した際に、`fstab` ファイルの参照コピーを保存した場合は、そのファイルでディスク情報を確認できます。リストアされた `fstab` ファイルに手動による変更がほとんど加えられていないシステムの場合、リストアされたファイルのコピーの代わりに参照 `fstab` ファイルを使用することが可能な場合もあります。

- c. 次のコマンドを入力して、`/mnt/sysimage/restore` に他のファイルが存在しないことを確認します。

```
ls -al /mnt/restore
```

- d. ディレクトリが空の場合は、次のコマンドを入力して、このディレクトリを削除します。

```
rmdir /mnt/restore
```

- e. ディレクトリが空でないためにこのコマンドが失敗する場合は、`root (/)` にあるほとんどのディレクトリをリストアした際に、移動できなかったディレクトリが存在する可能性があります。ディレクトリをリストアの正しい場所に移動します。

17. `reboot` と入力して、システムを再起動します。
18. インストール メディアを取り出し、通常どおりに起動します。
19. クライアントが正しく動作することを確認します。

SUSE Linux クライアントのシステム リカバリをトラブルシューティングする

次のトピックでは、SUSE Linux クライアントのシステム リカバリを実行した後で発生する可能性のある問題のトラブルシューティングについて、詳しく説明します。

システム リカバリ後の起動障害のトラブルシューティング

リストアされたシステムがリストア処理手順の終わりに起動しない場合、最小 OS によってインストールされた GRUB のバージョンが、サーバでの以前のバージョンと異なる可能性があります。リストア環境で起動し、GRUB を再インストールします。

手順

1. 次の手順で、リストア環境で起動します。
 - a. リカバリ ターゲット クライアントを、インストール メディア (CD/DVD1) から起動し、**[Rescue System]** を選択します。

- b. リカバリ ターゲット クライアントでコマンド シェルを開き、**root** としてログインします。
 - c. 次のコマンドを入力して、最小インストールで作成された **root** パーティションを **/mnt** にマウントします。


```
mount /dev/sda# /mnt
```

ここで、**/dev/sda#**は **root** ファイル システムを含むデバイスです。Linux 論理ボリューム マネージャーを使用するようにドライブが構成されている場合、**root** デバイスは **/dev/VolGroup##/LogVol##** の形式になっていることがあります。
 - d. 次のコマンドを入力して仮想ファイル システムを **/mnt** ツリーに再バインドします


```
mount --rbind /proc /mnt/procmount --rbind /sys /mnt/sysmount
--rbind /dev /mnt/dev
```
 - e. 次のコマンドを入力して、現在のファイル システムの **root** を変更します。


```
chroot /mnt
```
 - f. 次のコマンドを入力して、前提条件で構成されたように、ネットワークを開始します。


```
rcnetwork start
```
 - g. 次のコマンドを入力して、自動マウント ファイル システムをマウントし、適切なファイル システムがマウントされたことを確認します。


```
mount -a;df -h
```
 - h. ファイル システムが存在しない場合（例えば、**/boot** が自動マウントに設定されていない場合）、追加の **mount** コマンドを使用して、それらを正しい場所に手動でマウントします。
2. 次のコマンドを入力して、**GRUB** を再インストールします。


```
chroot /mntgrub-install device
```

ここで、**device** は起動デバイス（例：**/dev/sda**）です。
 3. **exit** と入力して、**chroot** 環境を終了します。
 4. **reboot** と入力して、システムを再起動します。
 5. インストール メディアを取り出し、通常どおりに起動します。

Linux クライアントのシステム リカバリ後にネットワーク設定をリストアする

システムが新しいハードウェアにリストアされたことが OS によって検出された場合、ネットワーク設定がデフォルトに戻される可能性があります（例えば、固定 IP ではなく、DHCP 名前解決）。設定を手動で再構成することにより、以前のネットワーク設定をリカバリできます。

以前の設定を確認するには、**/etc/sysconfig/network-scripts** にある **.bak** ファイルをテキスト エディターで開きます。これらのファイルには有益な情報が含まれていますが、それらには以前のハードウェアの **MAC** アドレス情報が含まれているため、未修正の形で現在の構成で使用してはいけません。

Oracle Solaris システム リカバリ

次のトピックでは、Oracle Solaris クライアント システムを元のシステム状態にリストアする方法について説明します。

Oracle Solaris システム リカバリのための準備

Oracle Solaris システムのシステム リカバリを実行する前に、環境が次の前提条件を満たしていることを確認してください。

重要なシステム ファイルを使用した利用可能なバックアップ

Oracle Solaris クライアント システムを元のシステム状態に正常にリストアするには、ローカル ファイル システム全体の Avamar バックアップと、次の重要なシステム ファイルおよび仮想ファイル システムが存在する必要があります。バックアップ中に以下の表に示されるターゲットのトラバースを強制実行することにより、この処理が可能になります。

表 44 Oracle Solaris クライアントのシステム リカバリ バックアップのターゲット場所

ターゲット	説明
mntfs	/etc/svc/volatile
tmpfs	/etc/mnttab
cacheufs	Solaris Cache File System
fdfs	Solaris File Descriptor File System
fifofs	Solaris FIFO File System
nameufs	Solaris Name File System
specufs	Solaris Device Special File System
swapufs	Solaris Swap File System
tufs	Solaris Translucent File System

これらのターゲットが確実にバックアップに含まれるようにするには、次のバックアップ方法のいずれかを使用します。

- Avamar Administrator で、プラグ イン オプションの **[Force traversal of the specified file system type(s)]** ボックスで、
`mntfs, tmpfs, cacheufs, fdfs, fifofs, nameufs, specufs, swapufs, tufs` を指定して、オンデマンド バックアップまたはデータセットにこれらのターゲットを明示的に追加します。
- `avtar` コマンドラインで、`--forceufs="mntfs, tmpfs, cacheufs, fdfs, fifofs, nameufs, specufs, swapufs, tufs"` を指定します。

利用可能な/var および/opt ファイル システム

元のファイル システム テーブルには、`/opt` および `/var` 用のパーティションが存在する必要があります。`/opt` および `/var` 用のパーティションは、Solaris を読み取り専用モードで開始するとマウントされます。

これらのパーティションがマウントされない場合は、クライアントに最小バージョンの Solaris をインストールする際に、`/opt` および `/var` 用に新たに一時ファイル システムを作成する必要があります。

その他のファイル システム

`zfs` またはその他のアドオン ファイル システムを使用している場合、システム リカバリを開始する前に、これらのファイル システムが適切に再作成され、マウントされていることを確認します。

Solaris の最小バージョンのインストール

元のシステムと可能な限り一致するファイル システムのレイアウトを作成します。`/opt` および `/var` に個別のファイル システムが存在するようにします。

Oracle Solaris クライアントのシステム リカバリの実行

はじめに

[Oracle Solaris システム リカバリのための準備](#) (173 ページ) のステップを実行します。

手順

1. プラットフォームに応じて、`reboot -- cdrom` と入力するか、BIOS メニューで起動順序を変更して、CD から起動します。
2. (Solaris 11 および 10 のみ) 起動オプション メニューで次のいずれかのオプションを選択します。
 - [3. Solaris Interactive Text (Desktop session)]
 - [4. Solaris Interactive Text (Console session)]
3. クライアントホスト名、IP アドレス、デフォルト ゲートウェイ、企業 DNS サーバーを入力するダイアログが表示されたら、各項目を入力します。
4. 次のようにコマンド プロンプトを終了して、シェル プロンプトに戻ります。
 - Solaris 8 では、Solaris Web Start を備えた Solaris にソフトウェアをインストールするようにプロンプトで指示されたら、[!] キーを押します。
 - Solaris 10 または 11 では、インストール タイプを選択するようにプロンプトで指示されたら、[F5] キーを押して終了し、次に [F2] キーを押して終了を確認します。
5. 次のコマンドを入力して、`/a` の下にある `/` パーティションをリストアのターゲットとしてマウントします。


```
mount /dev/dsk/c1t0d0s0 /a
```

`root` ボリュームに対して、サイト固有のディスク パーティション パラメーターとマウント パラメーターを指定します。
6. 次のコマンドを入力して、`/opt` の下にある `/opt` パーティションをマウントします。


```
mount /dev/dsk/c1t0d0s5 /opt
```

`/opt` ボリュームに対して、適切なサイト固有のディスク パーティション パラメーターとマウント パラメーターを使用します。
7. 次のコマンドを入力して、`/var` の下にある `/var` パーティションをマウントします。


```
mount /dev/dsk/c1t0d0s4 /var
```

`/var` ボリュームに対して、適切なサイト固有のディスク パーティション パラメーターとマウント パラメーターを使用します。
8. `/a` の下にある各マウント ポイントに、追加のファイル システムをすべてマウントします。マウント ポイントが存在しない場合は、作成します。例えば、次のコマンドを入力して、ファイル システム `/data01` を `c1t0d0s7` にマウントします。

```
mount /dev/dsk/c1t0d0s7 on /a/data01
```

9. 「Avamar バックアップ クライアント ユーザー ガイド」で説明されている手順に従って、Solaris 用 Avamar クライアントソフトウェアの適切なバージョンをインストールします。

通知

/etc/init.d/avagent および/usr/bin に/etc/rc.d/rcX.d および各種リンクを作成しようとする、「ルート (/) の空き領域が 0 バイトである」という内容の警告、および、読み取り専用ファイル システムに関するエラーが表示されます。ただし、この警告にかかわらず、すべてのバイナリは正しく/opt/AVMRclnt/bin にインストールされます。

10. 次のコマンドを入力して、/etc を/a/etc にリストアします。

```
cd /a/etc/opt/AVMRclnt/bin/avtar -x --server=Avamar_server --id=username --password=password --account=/domain/client --target=. /etc --labelnumber=n --overwrite=always
```

ここで、

- Avamar_server は、Avamar サーバーのホスト名または IP アドレスです。
- username および password は、このクライアントのバックアップにアクセス可能なロールを持つユーザーの Avamar ログイン認証情報です。
- /domain/client は、リストアする対象の Avamar ドメインと Solaris クライアントです。
- n は、リストアするバックアップのラベル番号です。ラベル番号を指定しない場合は、最新のバックアップがリストアに使用されます。

通知

root ファイル システムを直接/a にリストアすることはできません。これは、ネットワーク マウントポイントを経由せずにリストア処理をローカル パーティションのみに限定する方法がないためです。直接/a にリストアすると、ファイルがすべてのパーティションからコピーされるので、必要なファイルがすべてリストアされる前に、/a がいっぱいになる可能性があります。

11. /a/etc/vfstab を確認して、ローカル ファイル システムの元のマウントポイントを検証します。
12. Avamar Administrator で、[**Backup & Restore**] 起動リンクをクリックします。
[**Backup, Restore and Manage**] ウィンドウが表示されます。
13. [**Restore**] タブをクリックします。
14. [Clients] のツリーから元の Solaris クライアントを選択します。
15. リストアに使用するバックアップを検索し、選択します。
16. 元は「root (/)」の下に存在したディレクトリとファイルを検査します。
17. 元は「root (/)」の下に存在したディレクトリごとに次のステップを実行します。
- a. このディレクトリが存在しない場合は、同じ名前でも/aの下に空のディレクトリを手動で作成します。
 - b. ディレクトリをそのディレクトリに変更します。
 - c. コマンドラインから、バックアップのディレクトリの内容をリストアします。

例えば、/usr をリストアする際に使用する次のコマンドについて考えてみましょう。

```
mkdir /a/usr; cd /a/usr/opt/AVMRclnt/bin/avtar -x --
server=Avamar_server --id=username --password=password --
account=/domain/client --labelnumber=n --overwrite=always --
target=. /usr
```

元々、root パーティションに/opt と/var があつた場合、/a/opt と/a/var にリストアすることができます。/opt と/var が分離されたファイル システムであつた場合、/a/newopt や/a/newvar など、新しい一時的な場所にリストアします。すべてのリストアが完了したら、/a/newopt の内容を/opt に、/a/newvar の内容を/var に移動します。

18. 当初 root の下に存在した個々のファイルをリストアするには、次のように--norecursion オプションとともにリストア コマンドを実行して、ファイルをサブディレクトリに下げることなく、リストアします。

```
/opt/AVMRclnt/bin/avtar -x --server=Avamar_server --id=username
--password=password --account=/domain/client --labelnumber=n --
norecursion --overwrite=always --target=. /
```

19. 通常の方法でクライアントを再起動し、正常に動作することを確認します。

第 8 章

サーバー管理

本章は、次のトピックで構成されています。

• サーバーのシャットダウンと再起動.....	178
• サーバー アクティビティの一時停止と再開.....	182
• クライアント セッションの管理.....	183
• クライアント エージェントとプラグ インの管理.....	186
• バックアップ ウィンドウとメンテナンス ウィンドウ.....	188
• チェックポイント.....	190
• Avamar ソフトウェアのアクティブ化とサーバ ライセンスのインストール.....	193
• サービスの管理.....	195
• サーバー パスワードと OpenSSH キーを変更する.....	196
• MCS 構成設定.....	198
• NAT (ネットワーク アドレス変換) の使用.....	201
• シングル ノード サーバーでネットワーク設定を編集する.....	203
• Web ブラウザからのログインにカスタムのセキュリティ通知を追加する.....	203
• サーバー担当者情報の表示と編集.....	203
• バックアップの移行.....	204

サーバーのシャットダウンと再起動

Avamar サーバを構成するコンポーネントは、次のように段階的にシャットダウンされます。

- メンテナンスおよび他の指定されたアクティビティの一環としての、Avamar ソフトウェアまたは個別のサブシステムのシャットダウン。
- 完全に電源をオフにする一環としての、Avamar ソフトウェア、オペレーティング システム、ハードウェアのシャットダウン。

次のトピックでは、両方のプロセスについて詳細に説明します。

Avamar サブシステムの管理

`dpnctl` プログラムを使用すると、Avamar ソフトウェアまたは選択したサブシステムをコマンドライン インターフェイスを使用して安全にシャットダウンおよび再起動できます。このプロセスは、オペレーティング システムの再起動から独立しています。

Avamar ソフトウェアをシャットダウンまたは再起動すると、すべての Avamar サブシステムが 1 つのグループとして停止または再起動します。

Avamar ソフトウェアをシャットダウン

はじめに

完全にシャットダウンする前に、最新かつ検証済みのチェックポイントが存在することを確認します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin OpenSSH` キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl stop` と入力します。

確認メッセージのプロンプトで、EM Tomcat のローカル インスタンスをシャットダウンするかどうか尋ねられます。

3. ローカルの EM Tomcat インスタンスをシャットダウンするには、`y` と入力して、**[Enter]** キーを押します。

シャットダウンが完了するまで、出力でシャットダウン プロセスのステータスが表示されます。

Avamar ソフトウェアの再開

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin OpenSSH` キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl start`と入力します。
出力に確認メッセージが表示されます。
3. `y`を入力してソフトウェアの再開を開始し、次に **[Enter]** を押します。
再起動が完了するまで、出力で再起動プロセスのステータスが表示されます。

MCS の停止

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin`としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin`としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin` OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl stop mcs`と入力します。

MCS の起動

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin`としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin`としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin` OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl start mcs`と入力します。
3. `dpnctl start sched`と入力して、スケジュール設定された処理を再開します。

MCS ステータスの取得

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin`としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin`としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin` OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl status mcs`と入力します。

EM Tomcat サーバーの停止

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin`としてサーバーにログインします。
 - マルチ ノード サーバーの場合、`admin`としてユーティリティ ノードにログインします。
2. `dpnctl stop emt`と入力します。

EM Tomcat サーバーの起動

はじめに

EM Tomcat サーバーが正しくシャットダウンされたことを確認します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin`としてサーバーにログインします。
 - マルチ ノード サーバーの場合、`admin`としてユーティリティ ノードにログインします。
2. `dpnctl start emt`と入力します。

EM Tomcat サーバー ステータスの取得

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin`としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin`としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin OpenSSH` キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl status emt`と入力します。

サーバの電源オフまたは再起動

Avamar Administrator を使用して、Avamar ソフトウェア、オペレーティング システム、ハードウェア (該当する場合) を含めた Avamar サーバの電源を安全にオフにしたり再起動したりすることができます。

注

Avamar Data Store では、このプロセスによってすべてのノードの電源がオフになったり再起動したりします。

動作条件

Avamar サーバの電源をオフまたは再起動する前に、次の動作条件を完了します。

- すべてのバックアップ、リストア、データ移動操作を停止します。
シャットダウン プロセスは、すべてのアクティブな操作を終了してから処理を続行します。
- すべてのアクティブな Avamar インストール マネージャーパッケージの操作を完了します。

- 過去 36 時間以内に、チェックポイントの妥当性検査を行っていることを確認します。
- 過去 12 時間以内に MCS がフラッシュされたことを確認します。
- すべてのガベージ コレクションおよび HFS チェック操作を完了または停止します。
シャットダウン プロセスは、すべてのアクティブな操作を終了してから処理を続行します。
- 十分な空き領域が存在することを確認します。
サーバ使用率を、総容量の 85%未満、および Avamar サブシステムの使用可能ストレージ容量の 62%未満にする必要があります。

サーバの電源オフ

サーバの電源をオフにして、サイトの電源停止や物理的な機器の移動などのメンテナンスをできるようにします。

手順

1. Avamar Administrator で、[**Server**] 起動リンクをクリックします。
[**Server**] ウィンドウが表示されます。
2. [**Server Management**] タブをクリックします。
3. 電源をオフにするサーバを選択します。
4. [**Actions**] > [**Shut Down Avamar System**] を選択します。
確認ダイアログ ボックスが表示されます。
5. [**Yes**] をクリックします。
サーバは、差し迫ったシャットダウンに関する通知を発行します。
6. [**OK**] をクリックします。
サーバで、電源オフ処理が開始されます。

結果

以下のログに、詳細情報および進捗の最新情報が表示されます。

- /usr/local/avamar/var/log/avosshutdown.log
- /usr/local/avamar/var/log/dpnctl.log

必要条件

メンテナンスの完了後、次の方法のいずれかでサーバの電源をオンにします。

- フロント コントロール パネルにある電源ボタン (Gen4S)
- 背面 I/O パネルにある電源/リセット ボタン (Gen4T)
- RMM4 または RMC の電源コントロール ウィンドウ
- 仮想環境制御コンソールまたはコントロール インターフェイス

マルチ ノード サーバの場合は、各ストレージ ノードの電源を順にオンにしてから、ユーティリティ ノードの電源をオンにします。

注

ストレージ ノードより前にユーティリティ ノードの電源をオンすると、起動プロセスに遅延をきたす可能性があります。

サーバーの再起動

手順

1. Avamar Administrator で、**[Server]** 起動リンクをクリックします。
[Server] ウィンドウが表示されます。
2. **[Server Management]** タブをクリックします。
3. 再起動するサーバを選択します。
4. **[Actions]** > **[Reboot Avamar System]** を選択します。
確認ダイアログ ボックスが表示されます。
5. **[Yes]** をクリックします。
サーバは、差し迫った再起動に関する通知を発行します。
6. **[OK]** をクリックします。
サーバで、再起動プロセスが開始されます。

結果

以下のログに、詳細情報および進捗の最新情報が表示されます。

- /usr/local/avamar/var/log/avosshutdown.log
- /usr/local/avamar/var/log/dpnctl.log

サーバー アクティビティの一時停止と再開

バックアップおよびリストア、スケジュール設定された処理、メンテナンス アクティビティは、一時停止および再開することができます。

バックアップとリストアの一時停止と再開

手順

1. Avamar Administrator で、**[Server]** 起動リンクをクリックします。
[Server] ウィンドウが表示されます。
2. **[Server Management]** タブをクリックします。
3. 左のパネルで、Avamar サーバ ノードを選択します。
4. **[Actions]** メニューを開き、**[Suspend Backups/Restores]** または **[Resume Backups/Restores]** を選択します。
確認メッセージが表示されます。
5. **[はい]** をクリックします。

スケジュールされた操作の一時停止と再開

手順

1. Avamar Administrator で、**[Tools]** > **[Manage Schedules]** を選択します。
[Manage All Schedules] ウィンドウが表示されます。
2. **[Suspend All]** または **[Resume All]** をクリックします。

メンテナンス アクティビティの一時停止と再開

手順

1. Avamar Administrator で、[**Server**] 起動リンクをクリックします。
[**Server**] ウィンドウが表示されます。
2. [**Actions**] メニューを開き、[**Suspend Maintenance Activities**] または [**Resume Maintenance Activities**] を選択します。
確認メッセージが表示されます。
3. [**OK**] をクリックします。

クライアント セッションの管理

クライアント セッションの詳細ログを表示して、バックアップまたはリストアのトラブルシューティングまたは解析を実行できます。必要であれば、予期しないシステム動作が発生した場合に、クライアント セッションをキャンセルしたり、クライアントをリセットしたりすることが可能です。

クライアント セッションのモニタリング

[**Session Monitor**] では、アクティブなクライアント バックアップとリストア セッションのリストが表示されます。

手順

1. Avamar Administrator で、[**Server**] 起動リンクをクリックします。
[**Server**] ウィンドウが表示されます。
2. [**Session Monitor**] タブをクリックします。
次の表では、[**Session Monitor**] の各セッションごとに情報を記載しています。

表 45 [Session Monitor] タブのプロパティ

プロパティ	説明
[User]	
User	Avamar ユーザー ID (アカウント名)。
Path	Avamar サーバにおける階層場所を指定します。このオプションは、パスの宛先の先頭にスラッシュ (/) が付いている場合を除き、ユーザーのホームの場所に相対で、先頭がスラッシュの場合は絶対パスになります。
Domain	このユーザーが存在する Avamar ドメイン。
Client ID	この Avamar クライアントにユニークな識別子。
[Session]	
Type	このアクティビティは、avtarbackup または avtarrestore のいずれかです。

表 45 [Session Monitor] タブのプロパティ (続き)

プロパティ	説明
Root	バックアップの作成、リストア、検証のいずれかが行われるファイル システムの最上位。
Start time	このクライアント セッションが開始された日付と時刻。
Plug-in	このアクティビティに使用するプラグ イン。
Session ID	このクライアント セッションのユニークな識別子。
Work order ID	このアクティビティのユニークな識別子。
Elapsed	このクライアント セッションが実行されている時間。
Progress bytes	このアクティビティ中に検証したバイト数の合計。
New bytes	Avamar サーバまたは Data Domain システムにバックアップされた新しいバイト数のパーセンテージ。この値が低い場合は、重複排除のレベルが高いことを示します。
[System]	
Name	クライアントのホスト名。
OS name	このクライアントで使用されているオペレーティング システム。
App version	Avamar クライアント ソフトウェア バージョン。

クライアント セッションの詳細ログの表示

クライアント セッションの詳細ログを表示して、解析またはトラブルシューティングを実行することができます。

手順

1. Avamar Administrator で **[Activity]** 起動リンクをクリックします。

[Activity] ウィンドウが表示されます。

2. **[Activity Monitor]** タブをクリックします。

デフォルトでは、Activity Monitor に 72 時間以内のすべてのクライアント バックアップ アクティビティの詳細ログが表示されます。

3. 次の手順で、セッション ログのオプションを指定します。

- a. **[Action]** > **[Session Log Options]** を選択します。

[Session Log Options] ダイアログ ボックスが表示されます。

- b. **[Show HTML logs]** を選択すると、セッション ログ サマリーが HTML 形式で表示され、**[Show raw logs]** を選択すると、セッション ログ サマリーが未フォーマットのテキストとして表示されます。

- c. (オプション) HTML ログ形式を選択する場合は、**[Show debug information]** チェックボックスを選択すると、セッション ログ サマリーにトラブルシューティング情報が含まれます。

- d. **[OK]** をクリックします。
4. リストからアクティビティを1つ選択します。
5. **[Actions]** > **[View Session Log]** を選択します。
[Activity Session Drill-down] ダイアログ ボックスが表示されます。
6. セッション ログ サマリーでは次のタスクのすべてを実行できます。
 - (HTML フォーマットのみ) **[Log Files]** セクションで、ハイパーリンクをクリックして、ログ ファイルに移動します。
 - セッション ログ サマリーで特定のテキスト文字列を検索するには、**[Find]** フィールドでテキスト文字列を入力し、**[Next]** または **[Previous]** をクリックします。
 - セッション ログ サマリーのトップに戻るには、**[Back to Top]** をクリックします。
 - セッション ログ サマリーをファイルにエクスポートするには、**[Export]** をクリックして、ファイルの場所を指定し、**[Save]** をクリックします。
 - セッション ログ サマリーのコンテンツを更新するには、**[Refresh]** をクリックします。
7. **[Close]** をクリックします。

Avamar サポート用の Zip ファイルの作成

[Activity] ウィンドウでは、Avamar サポート用にセッション ログ情報の Zip ファイルを作成し、その Zip ファイルを Avamar サーバにアップロードすることができます。

手順

1. Avamar Administrator で **[Activity]** 起動リンクをクリックします。
[Activity] ウィンドウが表示されます。
2. リストからアクティビティを1つ選択します。
3. **[Actions]** > **[Download Support Bundle]** を選択します。
[Download Support Bundle] ダイアログ ボックスが表示されます。
4. Zip ファイルのあるディレクトリを参照します。
5. **[Save]** をクリックします。
進行状況ダイアログ ボックスに、処理のステータスが表示されます。
6. 処理が完了したら、進行状況ダイアログ ボックスで **[Close]** をクリックします。
7. Zip ファイルを作成し、Avamar サーバにコピーするには、**[Actions]** > **[Upload Support Bundle to Server]** の順に選択します。
アップロードプロセスでは、セッション ログ サマリー情報の Zip ファイルが作成され、この Zip ファイルが Avamar サーバの /tmp フォルダにコピーされます。進行状況ダイアログ ボックスに、処理のステータスが表示されます。

クライアント セッションのキャンセル

クライアントがバックアップまたはリストアを実行している間に、まれに予想外のシステム動作が発生する場合があります。このような場合は、Avamar Administrator からクライアント セッションを強制的に終了させる必要がある場合があります。

手順

1. Avamar Administrator で、**[Server]** 起動リンクをクリックします。
[Server] ウィンドウが表示されます。

2. **[Session Monitor]** タブをクリックします。
アクティブなクライアント セッションのリストが表示されます。
3. キャンセルするクライアント セッションを選択します。
4. **[Actions]** > **[Cancel Session]** を選択します。
ダイアログ ボックスでキャンセルの進行状況が表示されます。
5. キャンセルが完了したら、**[Close]** をクリックします。

必要条件

クライアント セッションをキャンセルできない場合は、クライアントをリセットします。このステップにより、クライアント上のアクティブな avtar セッションが、直ちに強制終了されます。

クライアントのリセット

クライアントをリセットすると、そのクライアントのアクティブなクライアント avtar セッションが直ちに強制終了されます。ほとんどの場合、クライアントをリセットする前に、クライアント セッションをキャンセルします。

手順

1. Avamar Administrator で、**[Policy]** 起動リンクをクリックします。
[Policy] ウィンドウが表示されます。
2. **[Policy Management]** タブをクリックします。
3. **[Clients]** タブをクリックします。
4. リセットするクライアントを選択します。
5. **[Actions]** メニューから、**[Client]** > **[Reset Client]** を選択します。

クライアント エージェントとプラグ インの管理

クライアントが Avamar サーバと通信するときは必ず、そのクライアントが識別されるために以下の情報を送信します。

- クライアント ID
- 特定のエージェントのバージョン
- クライアントで実行されているビルド
- クライアントに現在インストールされているプラグ インのリスト (バージョンとビルド)

既知の非互換性の問題で、場合によっては、クライアント エージェントまたはプラグ インの特定のバージョン (すべてのビルド) または特定のビルドが実行されているすべてのクライアントへの Avamar サーバのアクセスを拒否する必要があります。

プラグ インの特定のバージョン (すべてのビルド) またはビルドが実行されているすべてのクライアントのプラグ インの以下の動作を個別に許可または禁止することもできます。

- クライアントから開始されるクライアント アクティブーション
- クライアントから開始されるオン デマンド バックアップ
- スケジュール設定バックアップ
- リストア
- バックアップ検証

- サーバーに格納されているバックアップを参照する機能

「廃止」と指定された特定バージョン（すべてのビルド）または特定ビルドの Avamar サーバへのアクセスは拒否されます。クライアント エージェントまたはプラグインとインストールされたサーバー ソフトウェアの特定のバージョンの間に互換性がないことが判明した場合のみ、ビルドが「廃止」と指定されず、潜在的な問題を回避するには、該当のバージョンまたはビルドのプロパティを編集する機能を使用してこの「廃止」の指定をオーバーライドすることはできません。

ビルドレコードの追加

特定のクライアントエージェントまたはプラグインビルドに MCS のデータベースレコードを追加できます。ビルドレベルのみでレコードを追加できます。新しいバージョンレコードは、Avamar サーバソフトウェア アップグレードの後、自動的に追加されます。

手順

1. Avamar Administrator で、[Tools] > [Manage Agents & Plug-ins] を選択します。
[Manage All Agents & Plug-ins] ウィンドウが表示されます。
2. 左のパネルで、ビルドのエージェントまたはプラグインのバージョンを選択します。
3. [New] をクリックします。
[New Build] ダイアログ ボックスが表示されます。
4. [Build] ボックスで、有効なエージェントまたはプラグインのビルド番号を入力します。
5. このエージェントまたはプラグインビルドを持つクライアントへの Avamar サーバ アクセスを拒否する場合は、[Disable] チェックボックスを選択します。
6. (オプション) [Comment] ボックスにわかりやすいコメントを入力します。
7. [OK] をクリックします。

バージョンまたはビルドレコードの編集

手順

1. Avamar Administrator で、[Tools] > [Manage Agents & Plug-ins] を選択します。
[Manage All Agents & Plug-ins] ウィンドウが表示されます。
2. 左のパネルで、エージェントまたはプラグインを選択します。
3. 右のパネルで、編集するバージョンまたはビルドを選択します。
4. [Edit] をクリックします。
[Edit Build] ダイアログ ボックスが表示されます。
5. このエージェントまたはプラグインビルドを持つクライアントへの Avamar サーバ アクセスを拒否する場合は、[Disable] チェックボックスを選択します。
6. (オプション) [Comment] ボックスにわかりやすいコメントを入力します。
7. [OK] をクリックします。

ビルドレコードの削除

特定のクライアントエージェントまたはプラグインビルドに MCS のデータベースレコードを削除できます。バージョン全体のレコードを削除することはできません。

手順

1. Avamar Administrator で、[Tools] > [Manage Agents & Plug-ins] を選択します。
[Manage All Agents & Plug-ins] ウィンドウが表示されます。
2. 左のパネルで、エージェントまたはプラグインを選択します。
3. 右のパネルで、削除するビルドを選択します。
[Delete] をクリックします。

クライアントが開始するすべてのアクティベーションを無効化する

クライアントによる Avamar サーバとのアクティブ化を一時的に回避して、システムがメンテナンス アクティビティをサポートできる状態にすることができます。クライアントによるアクティブ化が回避されている場合、クライアントの招待は機能しません。

手順

1. Avamar Administrator で、[Tools] > [Manage Agents & Plug-ins] を選択します。
[Manage All Agents & Plug-ins] ウィンドウが表示されます。
2. [Disable All Client Initiated Activations] をクリックします。
3. クライアントが開始するアクティベーションを再度有効化するには、[Enable All Client Initiated Activations] をクリックします。

クライアントが開始するすべてのバックアップを無効化する

Avamar クライアントによるオン デマンド バックアップの開始を一時的に回避して、システムがさまざまなメンテナンス アクティビティをサポートできる状態にすることができます。

手順

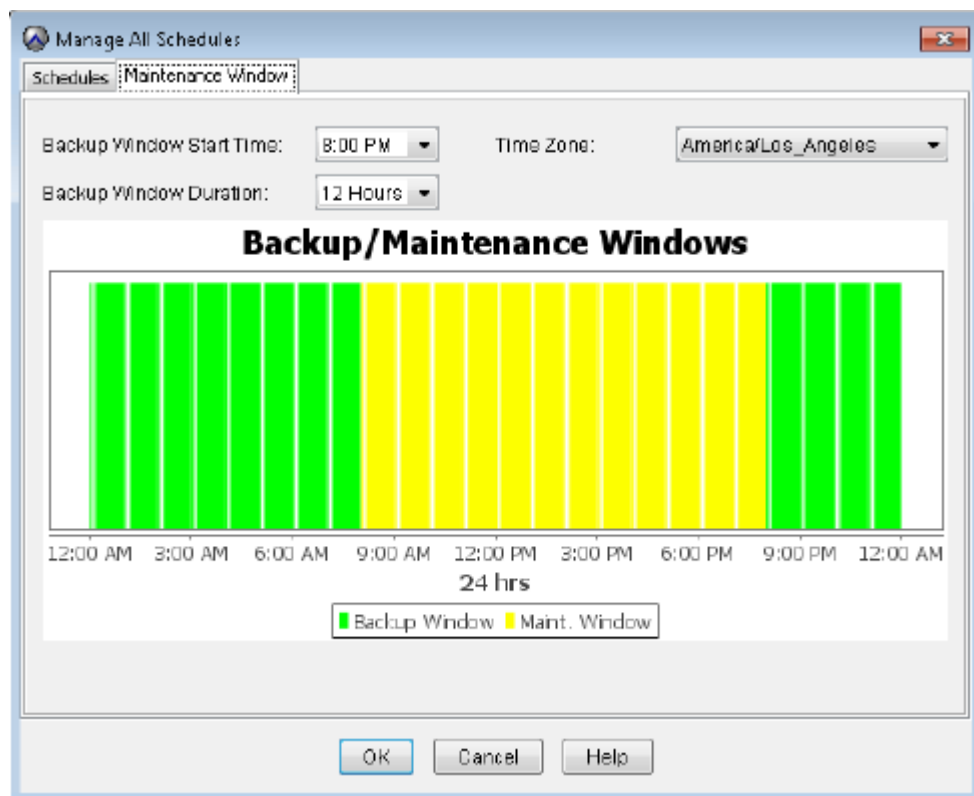
1. Avamar Administrator で、[Tools] > [Manage Agents & Plug-ins] を選択します。
[Manage All Agents & Plug-ins] ウィンドウが表示されます。
2. [Disable All Client Initiated Backups] をクリックします。
3. クライアントが開始するオン デマンド バックアップを再度有効化するには、[Enable All Client Initiated Backups] をクリックします。

バックアップ ウィンドウとメンテナンス ウィンドウ

1 日の 24 時間が、バックアップ ウィンドウとメンテナンス ウィンドウの 2 つのオペレーション ウィンドウに分割されます。

以下の図にデフォルトのバックアップ ウィンドウとメンテナンス ウィンドウを示します。

図 13 デフォルトのバックアップ ウィンドウとメンテナンス ウィンドウ



バックアップ ウィンドウ

バックアップ ウィンドウは、それぞれの日のうち、スケジュール設定された通常のバックアップを実行するために予約されている部分です。バックアップ ウィンドウの間に実行されるメンテナンス アクティビティはありません。

デフォルトのバックアップ ウィンドウはローカル サーバー時間の午後 8 時に開始し、翌朝の午前 8 時まで 12 時間にわたり、無停止で続行されます。バックアップ ウィンドウの開始時刻と継続時間はカスタマイズできます。

メンテナンス ウィンドウ

メンテナンス ウィンドウは、次の表に挙げる所定のサーバー メンテナンス アクティビティを実行するために予約された 1 日の時間帯です。

表 46 Avamar サーバのメンテナンス アクティビティ

アクティビティ	説明
チェックポイント	サーバ ロール バックのために取得された Avamar サーバのスナップショット。
チェックポイントの検証	特定のチェックポイントの整合性を検証する内部操作。チェックポイントの検証は、HFS (ハッシュ ファイル システム) チェックとも呼ばれます。HFS チェックに合格したチェックポイントは、サーバ ロール バックに使用するために十分な信頼性を備えていると見なすことができます。

表 46 Avamar サーバのメンテナンス アクティビティ (続き)

アクティビティ	説明
ガベージ コレクション	削除済みまたは期限切れのバックアップからストレージ領域をリカバリする内部操作。

メンテナンス ウィンドウの間もバックアップとリストアの実行は可能ですが、これを行うとバックアップ、リストア、メンテナンスの各アクティビティのパフォーマンスが落ちます。このため、メンテナンス ウィンドウの間はバックアップ、リストア、管理アクティビティを最小限に抑えてください。短時間の間、バックアップまたは管理アクティビティを実行できない場合があります。

デフォルトのメンテナンス ウィンドウはローカル サーバ時間の午前 8 時に開始し、午後 8 時まで 12 時間にわたり、無停止で続行されます。メンテナンス ウィンドウを直接カスタマイズすることはできませんが、メンテナンス ウィンドウの開始時刻と所要時間はバックアップ ウィンドウの設定から生成されます。

バックアップ ウィンドウとメンテナンス ウィンドウの編集

バックアップ ウィンドウとメンテナンス ウィンドウを編集するには、バックアップ ウィンドウの開始時間と継続時間に加えて、バックアップ ウィンドウとメンテナンス ウィンドウのタイムゾーンを設定します。

バックアップ ウィンドウの継続時間を変更すると、メンテナンス ウィンドウの継続時間にも影響します。例えば、バックアップ ウィンドウの継続時間を 12 時間から 14 時間に変更すると、メンテナンス ウィンドウの継続時間が 2 時間減ります。

次に挙げるベスト プラクティスは、システム アクティビティのスケジュール設定を行う場合に適用されます。

- **メンテナンス ウィンドウ中のオン デマンド バックアップを控える**
 メンテナンス ウィンドウの最初の 1 時間半の間に (ほとんどのシステムでは、ローカル時間の午前 8 時から午後 8 時まで)、クライアント コンピューターからオン デマンド バックアップを開始しないようユーザーにアドバイスすることをお勧めします。
- **オン デマンド メンテナンス アクティビティの開始を避ける**
 チェックポイント、チェックポイントの検証、またはガベージ コレクションなどのメンテナンス アクティビティを手動で開始すると、その手動で開始された操作が完了するまで、スケジュール設定されたすべてのメンテナンス アクティビティが一時的に無効になります。オン デマンド メンテナンス アクティビティを開始する必要がない限り、スケジュール設定されたメンテナンス アクティビティを信頼して、毎日の各アクティビティに十分時間が割り当てられるようにすることをお勧めします。

手順

1. Avamar Administrator で、[Tools] > [Manage Schedules] を選択します。
 [Manage All Schedules] ウィンドウが表示されます。
2. [Maintenance Window] タブをクリックします。
3. 対応するリストから新しい値を選択し、バックアップ ウィンドウの開始時間、期間、タイムゾーンを変更します。
4. [OK] をクリックします。

チェックポイント



チェックポイントとは、ディザスタリカバリを目的として取られるシステム全体のバックアップのことです。

チェックポイントは、メンテナンス ウィンドウ中に自動的に実行されます。また、チェックポイントはいつでも手動で開始することが可能です。

サーバー ストレージ容量を再利用するために、チェックポイントを削除することができます。

Avamar Administrator の [Server] ウィンドウにある [Checkpoint Management] タブでは、個々のチェックポイントのステータスが表示されます。次の表では、チェックポイントの状態として可能性のあるものを挙げています。

表 47 チェックポイントの状態

状態	説明
	チェックポイントは検証に失敗したか、完了する前にキャンセルされました。
	チェックポイントの検証が実施されていません。
	このチェックポイントに対する妥当性検査は実行中です。
	チェックポイントの検証にパスしました。

チェックポイントの作成

チェックポイントは、メンテナンス ウィンドウ中に自動的に実行されます。また、チェックポイントはいつでも手動で開始することが可能です。

手順

1. Avamar Administrator で、[Server] 起動リンクをクリックします。
[Server] ウィンドウが表示されます。
2. [Checkpoint Management] タブをクリックします。
3. [Actions] > [Create Checkpoint] を選択します。
進行状況ダイアログ ボックスに、処理のステータスが表示されます。
4. チェックポイントが完了したら、[Close] をクリックします。

チェックポイントの削除

また、サーバーのストレージ容量を増やすために、チェックポイントを削除することもできます。一般的には、検証済みのチェックポイントを削除する前に、検証されていないチェックポイントを削除するようにしてください。

手順

1. Avamar Administrator で、[Server] 起動リンクをクリックします。
[Server] ウィンドウが表示されます。
2. [Checkpoint Management] タブをクリックします。
3. チェックポイントを選択して、[Actions] > [Delete Checkpoint] 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。

チェックポイントのロールバック

ロールバックとは、検証済みチェックポイントに格納されているデータを使用して、既知の正常な状態にまで Avamar サーバを戻すプロセスのことです。Avamar リリース 7.x サーバをバージョン 4.x 以前のチェックポイントにロールバックすることはできません。

はじめに

チェックポイントが実行された後に Avamar サーバにノードを追加した場合は、そのノードのエントリーを `probe.out` ファイルから削除します。

ロールバックには、検証済みのチェックポイントを使用します。チェックポイントの検証は、各メンテナンスウィンドウ中に実行されます。

注

次のメンテナンスウィンドウが完了する前に検証が完了したチェックポイントが必要な場合は、Avamar サポートに問い合わせ、支援を受けてください。

手順

1. コマンドシェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバには、`admin` としてサーバにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin OpenSSH` キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl stop` と入力して、サーバをシャットダウンします。
3. `cp1ist` と入力してチェックポイントのリストを表示します。

次の例のように、チェックポイントのリストが表示されます。

```
cp.20140106170113 Fri Jan 6 17:01:13 2014 valid hfs del
nodes 4 stripes 396
cp.20140107170042 Sat Jan 7 17:00:42 2014 valid hfs del
nodes 4 stripes 396
cp.20140108170040 Sun Jan 8 17:00:40 2014 valid hfs ...
nodes 4 stripes 396
cp.20140109170043 Mon Jan 9 17:00:43 2014 valid hfs ...
nodes 4 stripes 396
```

ここで、

- `cp.yyyymmddhhmmss` はチェックポイント ID です。
 - `valid hfs` は、検証済みのチェックポイントを示します。
 - `valid par` は、部分的に検証済みのチェックポイントを示します。
4. ロールバックに使用するチェックポイントのチェックポイント ID を記録します。

特定の古いチェックポイントにロールバックする必要があるに限り、通常は完全に検証済みの最新のチェックポイントにロールバックします。

5. 次のコマンドを入力して、ロールバックを開始します。

```
rollback.dpn --cptag=checkpoint_id >& file
```


ここで、`checkpoint_id` はチェックポイント ID であり、`file` は一時ファイルです。

6. ロールバックが完了するまで待ちます。Avamar サーバのデータ量によっては、ロールバックに 1 時間かかる場合があります。

ロールバックが完了したら、コマンドプロンプトに制御が戻ります。

7. ロールバック時に作成されたユーザー定義の一時ファイルを開いて、ロールバックが正常に完了し、エラーが発生していないことを確認します。

ロールバックが正常に完了したら、サーバーは自動的に再起動します。

データの整合性アラートの消去

データの整合性を維持するために、Avamar サーバはチェックポイント検証に失敗するたびにアラートを発行します。このアラートを消去する唯一の方法は、Avamar サポートに問い合わせ、リセットコードを入手し、そのコードを **[Clear Data Integrity Alert]** ダイアログボックスに入力することです。

はじめに

リセットコードを Avamar サポートから入手します。

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[Event Management]** タブをクリックします。
3. ウィンドウ下部近くにある **[Unacknowledged Events]** タブをクリックします。
4. **[Actions]** > **[Event Management]** > **[Clear Data Integrity Alert]** を選択します。
[Clear Data Integrity Alert] ダイアログボックスが表示されます。
5. **[Enter reset code]** フィールドにリセットコードを入力して、**[OK]** をクリックします。

Avamar ソフトウェアのアクティブ化とサーバライセンスのインストール

Avamar サーバには永続的な操作を行うためのライセンスキーが必要です。Avamar ソフトウェアは、Dell EMC 共通ライセンスプラットフォームを使用してライセンス供与されます。

インストール後、Avamar ソフトウェアは、フル機能を使用できる 90 日間の評価期間を開始します。評価期間が終了すると、Avamar サーバはライセンスなしの状態になります。有効なライセンスキーがない状態では、Avamar サーバは複数の機能の実行を停止するか制限します。

Avamar ソフトウェアのアクティブ化

共通ライセンスプラットフォームを使用して Avamar ソフトウェアをアクティブ化するには、この手順を使用します。

はじめに

この手順では、送信されてきた LAC (ライセンス認証) メールに記載されている LAC (ライセンス認証コード) が必要です。このメールが見つからない場合は、メールを licensing@emc.com に送信して、ライセンス認証に関するメールを再送するようにリクエストしてください。メールには Avamar 製品 SO 番号を記してください。Avamar 製品 SO 番号は必須です。

手順

1. LAC（ライセンス認証）メールに記載されているログイン認証情報を使用して、Support Zone (<https://support.emc.com>) にログインします。
2. [Service Center] ドロップダウンリストで、[Manage Licenses] をクリックします。
3. 製品のリストから [Avamar] を選択します。
4. [Activate my software] をクリックします。
[Activation wizard] が表示されます。
5. LAC（ライセンス認証コード）を入力して [Search] をクリックし、ライセンス取得可能な製品を検索します。
6. ウィザードのプロンプトに従い、ライセンス情報をすべて入力します。
7. ライセンス キーが生成された後、ソフトウェアのライセンスに使用されるキーをダウンロードします。

ライセンスのインストールとアクティブ化

Avamar からライセンス キー ファイルを受け取ったら、Avamar サーバーにライセンスをインストールして、アクティブ化します。

はじめに

[Avamar ソフトウェアのアクティブ化](#)（193 ページ）の処理手順に従って、Avamar ライセンス キーを取得します。

手順

1. WinSCP または同等のプログラムを使用して、ライセンス キー ファイルをシングル ノード サーバーの /tmp ディレクトリ、またはマルチ ノード サーバーのユーティリティ ノード上の /tmp ディレクトリにコピーします。
2. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、admin としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. admin としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

3. `dpnctl status gsan` と入力して、Avamar サーバ サブシステム（別名 GSAN）が実行されていることを確認します。

GSAN が実行されている場合は、出力に `up` のステータスが表示されます。

4. 正しいコマンド シーケンスを使用して、Avamar ライセンス キー ファイルでファイルの権限を変更し、ライセンスをアクティブ化します。

サーバーのステータス	コマンド シーケンス
Running	a. <code>chmod 644 /tmp/license_key_file</code> b. <code>avmaint license /tmp/license_key_file -- avamaronly</code> ここで、 <code>license_key_file</code> はライセンス キー ファイルです。

サーバーのステータス	コマンド シーケンス
Not running	<pre>a. cd /usr/local/avamar/etc b. mv license.lic license.lic.old c. cp /tmp/license_key_file license.lic d. chmod 644 license.lic</pre> <p>ここで、license_key_file はライセンス キー ファイルです。</p>

- Avamar サーバが実行されていない場合は、`dpnctl start` と入力して起動します。
- Avamar サーバを再起動した後で、次のコマンドを入力して、サーバライセンスが適切にインストールされていることを確認します。

```
avmaint license --avamaronly
```

コマンド シェルにライセンス情報が表示されます。

サービスの管理

Avamar Administrator の **[Administration]** ウィンドウにある **[Services Administration]** タブで、Avamar サーバの個々のサービスについて開始、停止、一時停止、再開を実行できます。

手順

- Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
- [Services Administration]** タブをクリックします。
- 次のように、サービスを管理します。
 - サービスを開始するには、サービスを右クリックして、**[Start]** を選択します。
 - サービスを停止するには、サービスを右クリックして、**[Stop]** を選択します。
 - 明示的に再開させるまでサービスを一時停止するには、サービスを右クリックして、**[Suspend]** を選択します。
 - 一時停止させたサービスを再開するには、サービスを右クリックして、**[Resume]** を選択します。

[Services Administration] タブの情報

次の情報が **[Services Administration]** タブに表示されます。

表 48 **[Services Administration]** タブの情報

Name	説明
Hostname	Avamar サーバの DNS 名。
IP Address	Avamar サーバの IP アドレス。
Load Average	過去 1 分間の CPU スレッド数の平均値。
Last Administrator Datastore Flush	前回の MCS フラッシュの日付と時刻。

表 48 [Services Administration] タブの情報 (続き)

Name	説明
PostgreSQL database	MCS データベースのステータス。
Web Services	MCS Web サービスのステータス。
Web Restore Disk Space Available	MCS Web サービスで restore Zip ファイルの作成に使用できるハード ディスクドライブのバイト数。
Login Manager	Avamar Login Manager サービスのステータス。
snmp sub-agent	Avamar SNMP サブエージェント サービスのステータス。
ConnectEMC	ConnectEMC サービスのステータス。
VMware vCenter Connection Monitor	VMware vCenter 接続のステータス。このサービスは、少なくとも 1 個の vCenter クライアントがシステムに追加された場合にのみ表示されます。
snmp daemon	Avamar SNMP マスター エージェント サービスのステータス
ssh daemon	Avamar SSH (Secure Shell) サービスのステータス。
syslog daemon	Avamar syslog サービスのステータス。
Data Domain SNMP Manager	構成済み Data Domain システムを監視するための SNMP サービスのステータス。
Remote Backup Manager Service	Replicas at Source 機能で使用する外部バックアップ マネージャー サービスのステータス。
RabbitMQ	RabbitMQ メッセージ ブロカー サービスのステータス。
Replication job	Avamar サーバーでのレプリケーション ジョブのステータス。

注

[**Services Administration**] タブのサービス リストは、Avamar システムの構成に応じて異なります。

サーバー パスワードと OpenSSH キーを変更する

change-passwords ユーティリティを使用して、オペレーティング システム ユーザー アカウントおよび Avamar サーバー ユーザー アカウントのパスワードを変更します。また change-passwords を使用して、これらのアカウントの SSH キーを作成、変更します。

change-passwords ユーティリティに従って、次の操作を実行します。

- admin および root の各オペレーティング システム アカウントのパスワードを変更する
- root、MCUser、repluser、viewuser の各内部 Avamar サーバー アカウントのパスワードを変更する

- SSH キーの作成と変更

手順

- スケジュール設定された全操作の一時停止 :
 - Avamar Administrator で、[Tools] > [Manage Schedules] を選択します。
 - [Manage All Schedules] ウィンドウで [Suspend All] をクリックします。
- コマンド シェルを開きます。
 - サーバーに admin としてログインします。
 - 次のコマンドを入力して、ユーザーを root に切り替えます。


```
su -
```
 - グリッドの場合、次のコマンドを入力して、rootid OpenSSH キーをロードします。


```
ssh-agent bashssh-add /root/.ssh/rootid
```
- change-passwords を入力して、ユーティリティを開始します。
マルチ ノード サーバーでは、すべてのノードでパスワードを変更するか、選択したノードでパスワードを変更するかを指定するように、出力のプロンプトで要求されます。
- y と入力すると、すべてのノードでパスワードを変更し、n と入力すると、選択したノードでパスワードを変更します。その後、[Enter] キーを押します。
出力により、root 操作で許可される SSH プライベート キーを指定するかどうかを示すようにプロンプトで要求されます。
- [n] と入力し、[Enter] キーを押します。
出力により、admin または root のいずれかのオペレーティング システム ユーザー アカウントのパスワードを変更するかどうかを指定するようにプロンプトで要求されます。
- y と入力すると、パスワードを変更し、n と入力すると、パスワードの変更プロセスがスキップされます。その後、[Enter] キーを押します。
- 1 つ前のステップで y と入力した場合は、システム プロンプトに従って、1 個または複数の admin または root のいずれかのオペレーティング システム ユーザー アカウントのパスワードを変更します。
出力により、SSH キーを変更するかどうかを指定するようにプロンプトで要求されます。
- y を入力して SSH キーの変更または作成を行います。または n を入力して [Enter] キーを押します。
- 1 つ前のステップで y と入力した場合は、システム プロンプトに従って、キーの変更または作成を行います。
出力により、Avamar サーバー パスワードを変更するかどうかを指定するようにプロンプトで要求されます。
- プロンプトが表示されて y と入力すると、MCUser、Avamar root、repluser、viewuser のパスワードが変更され、パスワードの変更を希望しない場合は、n と入力します。その後、[Enter] キーを押します。
- 1 つ前のステップで y と入力した場合は、システム プロンプトに従って、パスワードの変更を行います。
出力により、このユーティリティ セッション中に行われたパスワードまたは SSH キーへの変更を受け入れるか拒否するかをプロンプトで要求されます。

12. 変更を受け入れるには **y** と入力し、変更を行うことなくユーティリティ セッションを終了するには、**n** と入力します。その後、**[Enter]** キーを押します。

出力で、操作のステータスが表示されます。

13. 操作が完了したら、次の手順でスケジュール設定された処理を再開します。
 - a. Avamar Administrator で、**[Tools]** > **[Manage Schedules]** を選択します。
 - b. **[Manage All Schedules]** ウィンドウで **[Resume All]** をクリックします。

MCS 構成設定

Avamar Administrator は、クライアントとサーバ両方のソフトウェア アプリケーションで構成されます。サーバまたはクライアントのいずれかのプリファレンス ファイルを編集して、各アプリケーションを個別に構成することができます。

サーバ プリファレンス ファイル `mcserver.xml` への変更は、すべての Avamar Administrator セッションに影響します。クライアント プリファレンス ファイル `mcclient.xml` への変更は、そのクライアント上の Avamar Administrator セッションのみに影響します。いずれのファイルも、JSDK 1.4 API によって参照される `preferences.dtd` XML DTD (Document Type Definition) に準拠します。

デフォルトとライブ コピー

システム上には、これらのファイルについてそれぞれ 2 個のコピーがあります。

- 初期のデフォルト コピーは、インストール後に各アプリケーションを初期化する際に使用されません。
- ライブ コピーは、アプリケーションによって使用される現在の設定を含んでいます。

デフォルト コピーは、各アプリケーションの `/lib` ディレクトリに存在します。ライブ コピーは、「ライブ ファイル」ディレクトリに置かれます。次の表では、各アプリケーションのデフォルトのライブ ファイル ディレクトリを挙げています。

表 49 MCS 構成ファイルのデフォルトのライブ ファイル ディレクトリ

アプリケーション	デフォルトのライブ ファイル ディレクトリ
サーバ	<code>/usr/local/avamar/var/mc/server_data/prefs</code>
クライアント	<code>install_directory/var/mc/gui_data/prefs</code> 。ここで、 <code>install_directory</code> は通常、Microsoft Windows コンピューターでは <code>C:\Program Files\avs\administrator</code> 、Linux コンピューターでは <code>/usr/local/avamar</code> です。

初期化の動作

サーバ アプリケーションまたはクライアント アプリケーションが初期化されると、`\lib` ディレクトリ内のデフォルトの各プリファレンス ファイルがメモリにロードされ、ライブ ファイル ディレクトリにレプリケートされます。

注

実行中の MCS の再初期化は非常に危険です。これを行うと、ライブ ファイルに格納されているカスタムのプリファレンス設定が完全に上書きされ、システム構成がデフォルト設定に戻ります。このステップが行われると、以前のフラッシュ（バックアップ）から、上書きされたカスタム プリファレンス設定を回復する必要があります。

アップグレードの動作

サーバーのアップグレード時、新しいデフォルトの `mcserver.xml` ファイル内で `merge="delete"` 属性でマークされている `mcserver.xml` エントリーはすべて、新しいライブ コピーにマージされません。これらのエントリーは削除されます。これらのエントリーはデフォルトの `mcserver.xml` ファイルに保持され、アップグレードされたお客様のシステムで、これらのプリファレンス設定が削除されたことが MCS で認識されます。

ライブ `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` ファイルのすべてのエントリーに `merge="keep"` 属性を手動で追加できます。 `merge="keep"` 属性の付いた設定は、アップグレード後に新しいライブ コピーで保持されます。

MCS データのバックアップ

ハードウェア障害から保護するために、MCS は毎時間、システム チェックポイントの一部として、自動的に固有データを Avamar サーバにバックアップ、つまり [フラッシュ] します。フラッシュは、avtar クライアント セッションによって実行されます。また、オン デマンド フラッシュを強制実行することもできます。

フラッシュ プロセスでは、次の表に示すタイム スタンプ ファイルを生成します。

表 50 MCS バックアップのタイム スタンプ ファイル

ファイル	説明
<code>flush.timestamp</code>	各フラッシュの実行前に、 <code>flush.timestamp</code> が <code>server_data</code> ディレクトリに作成されます。このファイルには、フラッシュの日時が記録されます。サーバのロールバック時には、このファイルがリストアされ、選択された日時へのロールバックが行われていることを確認するために使用されます。 <code>flush.timestamp</code> のコンテンツにも、 <code>mcserver.sh --status</code> コマンドを使用してアクセスできます。
<code>init.timestamp</code>	システム初期化中、 <code>init.timestamp</code> ファイルが <code>server_data</code> ディレクトリに作成または上書きされます。このファイルには、システム初期化の日時が記録され、選択された日時に初期化が成功していることを検証するために使用されます。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバには、`admin` としてサーバにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。

b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. オン デマンドの MCS フラッシュを開始するには、次のコマンドを入力します。

```
mcservers.sh --flush
```

MCS データのリストア

はじめに

特定のバックアップに MCS データをリストアする場合は、Avamar Administrator でバックアップを参照するか、avtar コマンドを使用して、バックアップのラベル番号を見つけます。

- Avamar Administrator で、[**Backup, Restore and Manage**] ウィンドウを開き、/MC_BACKUPS アカウントにあるバックアップを参照します。
- 1 行のコマンド ラインで、次のコマンドを入力します。

```
avtar --backups --id=root --ap=password --path=/MC_BACKUPS --hfsaddr=Avamar_server --count=n
```

ここで、password は（オペレーティング システムの root パスワードではなく）Avamar の root ユーザー アカウントのパスワードです。また、Avamar_server は Avamar サーバの IP アドレスまたは DNS 名であり、n は表示するバックアップ数です。通常、1 台の Avamar サーバにつき、合計 26 回の MCS フラッシュが毎日実行されます。フラッシュは、1 時間あたり 1 回に加えて、午前中と午後のシステム チェックポイント中にそれぞれ 1 回ずつ実行されます。そのため、過去の特定の日数におけるすべての MCS バックアップを表示するには、--count=n を 26 の倍数として指定します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバには、admin としてサーバにログインします。
 - マルチ ノード サーバには、
 - a. admin としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. dpnctl stop mcs と入力して、MCS を停止します。
3. 次のコマンドのうちいずれかを入力して、MCS をリストアします。
 - 最新のバックアップにリストアするには、mcservers.sh --restore と入力します。
 - 特定のバックアップにリストアするには、mcservers.sh --restore --labelnum=n と入力します。ここで、n はバックアップのラベル番号です。
4. /usr/local/avamar/var/mc/server_log/restore.log を開いて、リストアが成功したことを確認します。
5. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```


デフォルトの MCS 構成設定に戻す

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバには、`admin` としてサーバにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin OpenSSH` キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. `dpnctl stop mcs` と入力して、MCS を停止します。
3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```

4. 次のコマンドを入力して、`mcserver.xml` の名称を `old.mcserver.xml` に変更します。

```
mv mcserver.xml old.mcserver.xml
```

5. 次のコマンドを 1 行のコマンドラインに入力して、デフォルトのサーバ プリファレンス ファイルをカレント ディレクトリにコピーします。

```
cp /usr/local/avamar/lib/mcserver.xml /usr/local/avamar/var/mc/server_data/prefs/mcserver.xml
```

6. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```

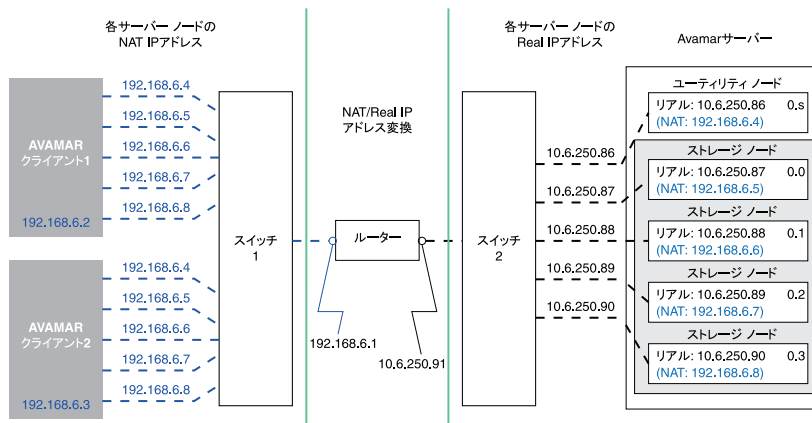
NAT（ネットワーク アドレス変換）の使用

Avamar クライアントは、NAT を経由した一連のアドレスを使用して Avamar ストレージ ノードにアクセスできます。

NAT 情報を Avamar サーバで使用できるようにするには、`probe.xml` ファイルにストレージ ノードの `nat-address` エlementを含める必要があります。クライアントが Avamar サーバ上のユーティリティ ノードに初めて接続した後、Avamar サーバによって、各クライアントのストレージ ノードにルーティング可能なアドレスのセットが提供されます。`nat-address` Elementが存在しない場合、クライアントは事前構成済みの「実際の」（未変換の）ネットワーク インターフェイス アドレスを使用します。

次の図では、Avamar で NAT を使用する 1x4 マルチ ノード サーバ構成の例を示します。

図 14 NAT を使用したマルチ ノード サーバー構成



次の手順では、各 Avamar ノードに（Avamar クライアントから見て）一意のアドレスがあること、またネットワークでルータを構成して、透過的な 1 対 1 のネットワーク アドレス変換が適用されていることを仮定しています。また、これらの手順を使用して、シングル ノード サーバー設定で NAT を使用可能にすることもできます。

手順

1. dpnnetutil または nodedb のいずれかのプログラムを使用して、NAT アドレスを probe.xml に追加します。

コマンド	コマンド プロンプトの例
dpnnetutil	<pre>su - rootdpnnetutil</pre> <p>dpnnetutil によって表示される対話型のプロンプトに対応します。</p>
nodedb	<pre>nodedb update if --addr=10.6.250.87 --new-nat=192.168.6.4=192.168.6.5</pre>

2. Avamar ストレージ サブシステムが停止中の場合、`dpnctl start gsan` と入力して再起動します。
3. Avamar ストレージ サブシステムが実行中の場合、次のコマンドを入力して、probe.xml ファイルを再度読み取ります。


```
avmaint networkconfig /usr/local/avamar/var/probe.xml --avamaronly
```
4. avregister (UNIX) または avregister.bat (Windows) コマンド、または Avamar Administrator を使用して、クライアントを登録します。

NAT に関する一般的な問題のソリューション

NAT が使用されているかどうかを判断するために、クライアントと Avamar サーバはネットワーク接続している必要があります。次の表に、一般的な NAT 接続と構成の問題のソリューションを示します。

表 51 NAT に関する一般的な問題のソリューション

問題	ソリューション
Avamar サーバが FATAL ERROR メッセージで終了する。	<p>probe.xml ファイルについて次の点を確認してください。</p> <ul style="list-style-type: none"> • /usr/local/avamar/var/ディレクトリに存在する。 • 有効な XML ファイルであり、ノードリソースデータベース形式に準拠している。 • NAT IP アドレスを正しく示している。 <p>nodedb print --say コマンドを使用して probe.xml の内容を表示します。--say オプションは、現在のノードリソースデータベースのパスと名前を示します。</p>
サーバー/クライアント接続が失敗する。	<p>ping、tracert、tracert、iperf などのネットワーク診断ツールを使用して、ネットワーク接続を確認します。</p>

シングル ノード サーバーでネットワーク設定を編集する

シングル ノード サーバでネットワーク設定を編集する方法の手順については、Avamar サポート (<https://support.EMC.com>) から入手可能な「Changing the Name and IP Addressing of Avamar Systems Technical Note」を参照してください。

Web ブラウザからのログインにカスタムのセキュリティ通知を追加する

Avamar Web Restore のログイン ページにカスタムのセキュリティ通知を含めることができます。この通知は通常、許可されたユーザーのみにアクセスが許可されるという内容を示します。また、この通知には不正アクセスに対するペナルティも示されます。

手順

1. テキスト エディターで disclaimer_Web_Restore.txt という名前のファイルを作成します。
2. 通知コンテンツをファイルに追加します。
通知コンテンツには、基本的な HTML タグや CSS インライン スタイルが使用できます。
3. シングル ノード サーバーの次の場所、またはグリッドのユーティリティ ノードにファイルをコピーします。

```
/usr/local/avamar/var/em/server_data/
```

サーバー担当者情報の表示と編集

Avamar サーバでは、Avamar に報告するすべてのイベントで、Avamar サーバの担当者情報のほか、システムが重大な閾値を超えることを回避するために役立つ容量レポートも送信します。この情報を最新に保ちます。

サーバーのロールバックは、チェックポイントの時点で存在している担当者情報を適用します。ロールバックが完了したら、担当者情報を表示または編集して、この情報を最新の状態に維持します。

手順

1. Avamar Administrator で [Help] > [View/Edit Contact Information] を選択します。

[View/Edit Contact Information] ダイアログボックスが表示されます。次の表には、このダイアログボックスの読み取り専用フィールドが挙げられています。

表 52 [View/Edit Contact Information] ダイアログボックスの読み取り専用フィールド

フィールド	説明
[System ID]	サーバの初期導入時に作成した一意の Avamar サーバ識別子。このフィールドは、読み取り専用です。
[AVE]	このサーバが AVE (Avamar Virtual Edition) サーバの場合は [Y] (Yes)、そうでない場合は [N] (No)。このフィールドは、読み取り専用です。

2. 担当者情報を編集します。

表 53 [View/Edit Contact Information] ダイアログボックスの編集可能フィールド

フィールド	説明
[Avamar site ID]	サーバーの初期導入時に指定した一意のお客様のサイト識別子。
[Data Domain S/N]	このサーバーに追加された Data Domain システムのシリアル番号。Data Domain システムが追加されていない場合は、タイプ ([N/A])。
[Server location]	お客様のサイトにある Avamar サーバの物理的な場所。
[Company Information]	この Avamar サーバを所有する企業の名前と住所。
[Contact Information]	この Avamar サーバの主要担当者の氏名、電話番号、メールアドレス。

3. [OK] をクリックします。

バックアップの移行

Avamar で、GSAN、Data Domain、ハイブリッドバックアップデータのソースサーバーから宛先サーバーへの自動移行を実行できるようになりました。

Avamar サーバーは、次のバックアップタイプの自動移行のみをサポートします。

- Linux ファイル システム
- Windows ファイル システム
- NDMP

バックアップデータを自動的に移動するには、宛先サーバーから移行ジョブをトリガーします。移行ジョブが開始されると、移行ツールによって、バックアップデータがソースサーバーから宛先サーバーに移動されます。

注

多数の小容量ファイルがあるバックアップでは、移行のパフォーマンスが低下する可能性があります。

混在する既存の Avamar および Data Domain システムを Avamar および Data Domain システムに移行する方法の手動ステップについては、「Avamar Mixed-source (GSAN and Data Domain) Backups Migration Technical Note」を参照してください。

第 9 章

サーバーの監視

本章は、次のトピックで構成されています。

• 毎日のサーバー監視の推奨	208
• アクティビティのモニタリング	208
• サーバーのステータスと統計のモニタリング	211
• イベントの監視	226
• syslog を使用したサーバのモニタリング	237
• SNMP を使用したサーバーのモニタリング	243
• Avamar サーバ ログ ファイルの表示	246
• 監査ログ	247
• Avamar サポートへの自動通知	248
• システムの整合性の検証	256

毎日のサーバー監視の推奨

Avamar サーバを適切に動作させるために、次の表に示されるシステム監視タスクを毎日実行することを推奨しています。

表 54 システム監視ツールおよびタスク

監視ツール	監視タスク
Activity Monitor	完了時に例外が確認されるバックアップなど、正常ではないクライアント アクティビティを調査します。
Server Monitor	最後のチェックポイントおよび検証済みチェックポイントが最近のものか確認します。それらが過去 24 時間以内に実行されていることが理想です。
Event Monitor	システム エラーまたは警告があれば、それについて調査します。
[Unacknowledged Events] リスト	未確認のイベントを調査、特定（確認）します。

通知

Email Home 機能と ConnectEMC 機能を有効にします。これらの機能は、日次データの整合性チェックのステータスや他の重要なサーバ メッセージを Avamar サポートに自動的にメール送信します。

アクティビティのモニタリング

手順

1. Avamar Administrator で **[Activity]** 起動リンクをクリックします。

[Activity] ウィンドウが表示されます。

2. **[Activity Monitor]** タブをクリックします。

Activity Monitor で利用可能な情報の詳細については、[Activity Monitor の詳細](#) (208 ページ) を参照してください。

3. (オプション) Activity Monitor で表示される情報をフィルターして、特定の状態、タイプ、グループ、クライアント、プラグ インに関連するアクティビティのみを表示します。

- a. **[Actions]** > **[Filter]** を選択します。

[Filter Activity] ダイアログ ボックスが表示されます。

- b. フィルター条件を定義して、**[OK]** をクリックします。

Activity Monitor の詳細

デフォルトで、Activity Monitor タブには、過去 72 時間に発生した最近の 5,000 件のクライアント アクティビティが表示されます。Activity Monitor に表示される情報の量を増やしたり、減らしたりするには、`/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` ファイルで `com.avamar.mc.wo_completed_job_retention_hours` 設定を編集して、MCS を再起動します。

次の表では、Activity Monitor で利用可能な情報を詳しく説明しています。

表 55 Activity Monitor で利用可能なセッションの詳細

列	説明
ステータス	バックアップ、リストア、検証アクティビティのステータス。各ステータスの詳細については、Avamar Administrator のオンライン ヘルプを参照してください。
Error Code	アクティビティが正常に完了しなかった場合、数値のエラー コードが表示されます。エラー コードをダブルクリックすると、詳細な説明が表示されます。
Start Time	このアクティビティが開始した実際の日付と時刻。括弧で括られたローカル タイムゾーンで表示します。DST（夏時間）の移行補正は自動的に行われます。
Elapsed Time	このアクティビティの経過時間。
End Time	このアクティビティが終了する日時。有効なタイムゾーン（かっこ内に表示）に調整されます。DST（夏時間）の移行補正は自動的に行われます。
Type	アクティビティのタイプ。各タイプの詳細については、Avamar Administrator のオンライン ヘルプを参照してください。
Server	アクティビティが発生した時点のサーバ。Avamar サーバまたは Data Domain システム。
Progress Bytes	このアクティビティ中に検証したバイト数の合計。
New Bytes	Avamar サーバまたは Data Domain システムにバックアップされた新しいバイト数のパーセンテージ。この値が低い場合は、重複排除のレベルが高いことを示します。

表 56 Activity Monitor で利用可能なクライアントの詳細

列	説明
client	Avamar クライアント名。
Domain	Avamar サーバ内のクライアントのフルの場所。
OS	クライアントのオペレーティング システム。
Client Release	Avamar クライアント ソフトウェア バージョン。このアクティビティが VMware イメージ バックアップまたはリストアの場合、この値はイメージ プロキシ クライアントで実行中の Avamar クライアント ソフトウェアのバージョンになります。
Proxy	このアクティビティが VMware イメージ バックアップまたはリストアの場合、この値は仮想マシンの代わりにバックアップまたはリストアを実行するプロキシ クライ

表 56 Activity Monitor で利用可能なクライアントの詳細 (続き)

列	説明
	ントの名前になります。その他すべてのアクティビティに対しては空白です。

表 57 Activity Monitor で利用可能なポリシーの詳細

列	説明
Sched. Start Time	このアクティビティの開始をスケジュール設定した日付と時刻です。
Sched. End Time	このアクティビティの終了をスケジュール設定した日付と時刻です。
Elapsed Wait	このアクティビティがアクティビティ キューに存在した合計時間です。つまり、スケジュール設定した開始時間から実際の開始時間を差し引いた時間です。
Group	このアクティビティを開始するグループ。以下のいずれかの値を指定します。 <ul style="list-style-type: none"> アクティビティがスケジュール設定バックアップの場合は、このスケジュール設定アクティビティが開始されたときにクライアントがメンバーだったグループです。 その他のバックアップ、リストア、および確認アクティビティに対して、[On-demand] が表示されます。 このアクティビティがスケジュール設定されたレプリケーションの場合、この値はレプリケーション グループになります。 オン デマンドレプリケーション アクティビティには [Admin On-Demand Group] と表示されます。
Plug-in	このアクティビティに使用するプラグ イン。
Retention	このバックアップに割り当てられている保存タイプ。次の値のうちの1つ、または複数になります。 <ul style="list-style-type: none"> [D] : 日単位 [W] : 週単位 [M] : 月単位 [Y] : 年単位 [N] : 特定の保存タイプはなし
Schedule	アクティビティがスケジュール設定されたバックアップの場合、このアクティビティを開始したスケジュールが表示されます。Avamar Administrator またはクライアントで開始された他のすべてのアクティビティについて

表 57 Activity Monitor で利用可能なポリシーの詳細（続き）

列	説明
	て、[On-Demand] または [End User Request] がそれぞれ表示されます。
Dataset	バックアップ作成に使用されるデータセットの名前。アクティビティのタイプがレプリケーション ジョブである場合、この列には、レプリケーション先システム上でのレプリケーション元システム名、およびレプリケーション元システム上でのレプリケーション先名が表示されます。
WID	作業オーダー ID。このアクティビティのユニークな識別子。

サーバーのステータスと統計のモニタリング

Avamar Administrator の [Server] ウィンドウでは、Avamar サーバ全体、Avamar サーバの個々のノード、構成済みのすべての Data Domain システムについて、ステータスと統計を監視できます。

[Server] ウィンドウには、次のタブが表示されます。

- [Server Monitor] タブでは、Avamar サーバの CPU、ネットワーク、ハードドライブに関するパフォーマンス統計をまとめたビューを表示します。個別のサブタブにより、構成済みのすべての Data Domain システムについて、同様の情報が提供されます。
- [Server Management] タブには、Avamar サーバおよび構成済みのすべての Data Domain システムを含む、サーバ ハードウェア リソースの詳細ビューが表示されます。
- [Session Monitor] タブには、アクティブなクライアント バックアップとリストア セッションのリストが表示されます。
- [Checkpoint Management] タブには、この Avamar サーバで実行されたすべてのシステム チェックポイントに関する詳細情報が表示されます。
- [Data Domain NFS Datastores] タブには、構成済みのすべての Data Domain システムで実行される VMware Instant Access 用の一時 NFS 共有が表示されます。Instant Access の詳細については、「Avamar for VMware ユーザー ガイド」を参照してください。

[Server Monitor] タブ

Avamar Administrator の [Server] ウィンドウにある [Server Monitor] タブには、Avamar サーバおよび構成済みのすべての Data Domain システム用に個別のタブが表示されます。

[Avamar] タブ

[Server Monitor] の [Avamar] タブでは、Avamar サーバの CPU、ネットワーク、ハードドライブに関するパフォーマンス統計をまとめたビューが表示されます。

次の表では、[Avamar] タブで表示される情報について説明します。

表 58 [Server Monitor] の [Avamar] タブに表示されるノードの詳細

プロパティ	説明
Status indicators	<p>ノードのステータス。以下のいずれかの値を指定します。</p> <ul style="list-style-type: none"> オンライン (グリーン) : ノードは正常に機能しています。 読み取り専用 (ブルー) : このステータスは通常、バックグラウンド処理が実行され、バックアップが一時停止になると発生します。 タイムアウト (グレー) : MCS はこのノードと通信できませんでした。 不明 (イエロー) : ノードのステータスを判断できません。 オフライン (レッド) : ノードに問題が発生しています。ConnectEMC が有効になっている場合、SR (サービスリクエスト) がログに記録されます。既存のサービスリクエストを表示するには、Avamar サポートに移動します。ナレッジベースで KB000457963「Troubleshooting Node Offline\GSAN Degraded Issues on an Avamar System」を検索してください。
ID	<p>Avamar サーバの各ノードには、ユニークな論理識別子がつけられています。このノード ID は、<code>module.node</code> の形式で表示されます。</p> <hr/> <p>注</p> <p>モジュールとノード番号はゼロから始まります。つまり、1 番目のモジュールの 3 番目のノードを表す ID は 0.2 となります。</p>

表 59 [Server Monitor] の [Avamar] タブに表示される CPU の詳細

プロパティ	説明
Load	過去 1 分間の CPU スレッド数の平均値。
User	実際のサーバーからの命令を実行するために消費した CPU 容量の割合 (オペレーティングシステムのオーバーヘッド以外のすべて)。
Sys	オペレーティングシステムのオーバーヘッドで消費された CPU 容量の割合。

表 60 [Server Monitor] の [Avamar] タブに表示されるネットワークの詳細

プロパティ	説明
ping	このノードが、Ping 要求に応答するまでに費やした秒数。

表 60 [Server Monitor] の [Avamar] タブに表示されるネットワークの詳細 (続き)

プロパティ	説明
In	KB/秒でレポートされている受信したパケット スループット。
Out	KB/秒でレポートされている送信したパケット スループット。

表 61 [Server Monitor] の [Avamar] タブに表示されるディスクの詳細

プロパティ	説明
Reads	オペレーティング システムから報告された、1 秒あたりのハードドライブの平均読み取り回数。
Writes	オペレーティング システムから報告された、1 秒あたりのハードドライブの平均書き込み回数。
Utilization	サーバーで利用可能なストレージ容量の合計に対する現在使用中の容量の割合。

[Data Domain] タブ

[Server Monitor] の [Data Domain] タブでは、Data Domain システムの各ノードに関する CPU、ディスク アクティビティ、ネットワーク アクティビティの情報を表示します。

次の表では、[Data Domain] タブで利用可能な情報を説明しています。

表 62 [Server Monitor] の [Data Domain] タブに表示されるノードの詳細

プロパティ	説明
Status indicators	<p>ノードのステータス。以下のいずれかの値を指定します。</p> <ul style="list-style-type: none"> OK (グリーン) : Data Domain システムは正常に機能しています。 警告 (イエロー) : Data Domain システムに問題がありますが、バックアップとリストアは継続可能です。 エラー (レッド) : Data Domain システムに問題があり、バックアップおよびリストアは問題が解決するまで停止されます。 <p>ステータスがイエローまたはレッドの場合、追加のステータス情報を表示し、問題を特定して解決することができます。詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。</p>
Name	社内 DNS で定義される Data Domain システムのホスト名。

表 63 [Server Monitor] の [Data Domain] タブに表示される CPU の詳細

プロパティ	説明
Busy Avg.	平均の CPU 使用率。
Max	最大の CPU 使用率。

表 64 [Server Monitor] の [Data Domain] タブに表示されるディスク (KB/S) の詳細

プロパティ	説明
Read	ディスク読み取りのスループット (KiB/S)。
Write	ディスク書き込みのスループット (KiB/S)。
Busy	ディスク I/O 使用率。

表 65 [Server Monitor] の [Data Domain] タブに表示されるネットワーク (KB/S) の詳細

プロパティ ^a	説明
Eth#1	Desc : ネットワーク インターフェイスの説明。 In/Out : ネットワーク インターフェイス 1 のネットワーク帯域幅使用率 (KB/秒)。
Eth#2	Desc : ネットワーク インターフェイスの説明。 In/Out : ネットワーク インターフェイス 2 のネットワーク帯域幅使用率 (KB/秒)。
Eth#3	Desc : ネットワーク インターフェイスの説明。 In/Out : ネットワーク インターフェイス 3 のネットワーク帯域幅使用率 (KB/秒)。
Eth#4	Desc : ネットワーク インターフェイスの説明。 In/Out : ネットワーク インターフェイス 4 のネットワーク帯域幅使用率 (KB/秒)。

a. Eth#列の数字は、構成済み Data Domain システムがサポートするネットワーク インターフェイスの最大数に依存します。

[Server Management] タブ

Avamar Administrator の [Server] ウィンドウにある [Server Management] タブには、Avamar サーバおよび構成済みのすべての Data Domain システムの両方を含む、サーバのハードウェアリソースの詳細ビューが表示されます。

Avamar サーバ情報はツリーの [Avamar] フォルダーの下に表示され、構成済みの Data Domain システムはツリーの [Data Domain] フォルダーの下に表示されます。

ツリー内で選択されるアイテムにより、ウィンドウの右側のパネルの情報が変更されます。

表 66 [Server Management] タブでの選択項目に基づいたデータの表示

選択したアイテム	[Server Management] タブの右側のパネルに表示される情報
サーバー ノード	保護対象のバイト数のサマリー
Avamar または Data Domain ノード	<空欄>
Avamar サーバ名	Avamar サーバの詳細情報
モジュール	選択したモジュールの詳細情報
ノード	選択したノードの詳細情報
パーティション	選択した論理ハード ディスク ドライブ パーティションの詳細情報
Data Domain システム	選択した Data Domain システムの詳細情報

通知

Avamar のライセンスはデシマル単位で提供されます。そのため、[Total capacity] と [Capacity used] はデシマル単位で [Server Management] タブに表示されます。容量を出力する、その他の製品のすべての部分はバイナリ単位で表示されます。

バイト保護サマリー

次の表では、[Server Management] タブの [Bytes Protected Summary] プロパティに関する詳細が示されています。

この量は、クライアント側での圧縮前のサイズです。

表 67 [Server Management] タブの [Bytes Protected Summary] プロパティ

プロパティ	説明
Properties	Avamar サーバおよび構成済み Data Domain システムの名前。
Values	サーバーまたは Data Domain システムの保護されているデータのバイト数。この量は、クライアント側での圧縮前のサイズです。

サーバー情報

次の表では、[Server Management] タブで Avamar サーバを選択したときに表示される [Server Information] について説明しています。

表 68 [Server Management] タブに表示されるサーバーの詳細

プロパティ	説明
Active sessions	現在アクティブなクライアント セッションの数。詳細情報については、[Session Monitor] タブをクリックします。
Total bytes free in partitions	OS レベルの空きディスク サイズ。

表 68 [Server Management] タブに表示されるサーバーの詳細 (続き)

プロパティ	説明
Server bytes reserved	現在のストライプ ファイルが占有する最大サイズ。
Total capacity	サーバーの合計ストレージ容量。
Server Utilization	サーバーで利用可能なストレージ容量の合計に対する現在使用中の容量の割合。この値は、[Server Monitor] の [Avamar] タブに表示される [Disk Utilization] の最大値から得られるため、Avamar サーバ ストレージ使用率の絶対最大値を示します。すべてのモジュール、ノード、ドライブにまたがった実際の使用率はそれよりも若干低い可能性があります。
Bytes protected (client pre-comp size)	このサーバー上にバックアップされている (保護されている) クライアント データの合計 (バイト)。この量は、クライアント側での圧縮前のサイズです。
Bytes protected quota (client pre-comp size)	このサーバー上に保護目的で許可されているクライアント データの最大容量 (バイト)。この量は、クライアント側での圧縮前のサイズです。
License expiration	このサーバーのライセンスの使用期間が終了するカレンダー日付。恒久ライセンスの場合、値は never になります。
Time since Server initialization	この Avamar サーバが初期化されてから経過した時間数、日数、分数。
Last checkpoint	最後にサーバー チェックポイントが実施された日付と時刻。チェックポイントは通常、1日に2回実施されます。
Last validated checkpoint	最後にサーバー チェックポイントが検証された日付と時刻。チェックポイントの検証は通常、1日に1回実施されます。そのため、[Last validated checkpoint] の時刻と [Last checkpoint] の時刻は、この情報を表示する時間によって異なる場合があります。 注 [Last validated checkpoint] と [Last checkpoint times] の時刻に 36 時間以上の差がある場合は、チェックポイントの検証が実施されておらず、問題が発生しています。
System Name	ユーザーが割り当てた Avamar サーバの名前。
System ID	この Avamar サーバのユニークな識別子。
HFSAddr	HFS (Hash File System) Addr (address)。バックアップクライアントがこの Avamar サーバに接続するのに使用するホスト名、または IP アドレス。

表 68 [Server Management] タブに表示されるサーバーの詳細 (続き)

プロパティ	説明
HFSPort	HFS データ用ポート。バックアップ クライアントがこの Avamar サーバに接続するのに使用するデータ用ポート。デフォルトのポートは 27000 です。
IP Address	この Avamar サーバの IP アドレス。HFSAddr が IP アドレスの場合、この値は HFSAddr と同じになります。

表 69 [Server Management] タブに表示されるメンテナンス アクティビティの詳細

プロパティ	説明
Suspended	以下のいずれかの値を指定します。 <ul style="list-style-type: none"> No: サーバ メンテナンス アクティビティは、現在一時停止中ではありません (つまり、サーバ メンテナンス アクティビティは次のメンテナンス ウィンドウで通常どおり実行されます)。 Yes: サーバ メンテナンス アクティビティは現在一時停止中です。

表 70 [Server Management] タブに表示されるガベージ コレクションの詳細

プロパティ	説明
Status	以下のいずれかの値を指定します。 <ul style="list-style-type: none"> Idle: ガベージ コレクションは現在実行されていない。 Processing: ガベージ コレクションは実行中である。
Result	以下のいずれかの値を指定します。 <ul style="list-style-type: none"> OK: 前回のガベージ コレクション アクティビティは正常に完了した。 Error code: 前回のガベージ コレクション アクティビティは正常に完了していない。
Start time	前回のガベージ コレクション アクティビティが開始された日付と時刻。
End time	前回のガベージ コレクション アクティビティが終了した日付と時刻。
Passes	前回のガベージ コレクション アクティビティ中の合計パス数。
Bytes recovered	前回のガベージ コレクション アクティビティ中にリカバリされたストレージ領域 (バイト数) の合計量。
Chunks deleted	前回のガベージ コレクション アクティビティ中に削除されたデータ チャンクの合計数。

表 70 [Server Management] タブに表示されるガベージコレクションの詳細 (続き)

プロパティ	説明
Index stripes	インデックス ストライプの合計数。
Index stripes processed	前回のガベージ コレクション アクティビティ中に処理されたインデックス ストライプの合計数。

モジュール情報

次の表では、[Server Management] タブの [Module] プロパティに関する詳細が示されません。

表 71 [Server Management] タブのモジュールのプロパティ

プロパティ	説明
Total bytes free in partitions	OS レベルの空きディスク サイズ。
Server bytes reserved	現在のストライプ ファイルが占有する最大サイズ。
Total capacity	サーバーの合計ストレージ容量。
Server Utilization	サーバーで利用可能なストレージ容量の合計に対する現在使用中の容量の割合。この値は、[Server Monitor] の Avamar タブに表示される [Disk Utilization] の最大値から得られるため、Avamar サーバ ストレージ使用率の絶対最大値を示します。すべてのモジュール、ノード、ドライブにまたがった実際の使用率はそれよりも若干低い可能性があります。
Number of nodes	このモジュールにあるノード数の合計。
IP address	このモジュールの基本 IP アドレス。

ノード情報

次の表では、[Server Management] タブの [Node] プロパティに関する詳細を示します。

表 72 [Server Management] の [Node Information] 領域の [Status indicators]

プロパティ	説明
Status indicators	以下のいずれかの値を指定します。 <ul style="list-style-type: none"> オンライン (グリーン) : ノードは正常に機能している。 読み取り専用 (ブルー) : このオプションは通常、バックグラウンド操作として、バックアップが一時停止されると発生します。 タイムアウト (グレー) : MCS はこのノードと通信できなかった。 不明 (イエロー) : ノードのステータスを判断できない。

表 72 [Server Management] の [Node Information] 領域の [Status indicators]

プロパティ	説明
	<ul style="list-style-type: none"> オフライン (レッド) : ノードに問題が発生している。ConnectEMC が有効になっている場合は、SR (サービス リクエスト) が記録されているはずでず。既存のサービス リクエストを表示するには、Avamar サポートに移動します。ナレッジベースで KB000457963「Troubleshooting Node Offline\GSAN Degraded Issues on an Avamar System」を検索してください。

表 73 [Server Management] の [Node Information] 領域に表示されるサーバーの詳細

プロパティ	説明
State	<p>サーバーの現在の稼働状態。以下のいずれかの値を指定します。</p> <ul style="list-style-type: none"> ONLINE : ノードは正常に機能している。 DEGRADED : 1つ、または複数のディスク エラーが検出された。 OFFLINE : ノードに問題が発生している。ConnectEMC が有効になっている場合は、SR (サービス リクエスト) が記録されているはずでず。既存のサービス リクエストを表示するには、Avamar サポートに移動します。ナレッジベースで KB000457963「Troubleshooting Node Offline\GSAN Degraded Issues on an Avamar System」を検索してください。 READONLY : 通常、バックグラウンド処理が実行され、バックアップが一時停止されると、発生する。
Runlevel	<p>サーバーの現在の稼働状態。以下のいずれかの値を指定します。</p> <ul style="list-style-type: none"> fullaccess : この Avamar サーバは、フル稼働している。 admin : Avamar サーバではすべての機能が利用できるが、管理者の root アカウントを持つユーザーだけがサーバへのアクセスを許可されている。 adminonly : Avamar サーバではすべての機能が利用できるが、管理者の root アカウントを持つユーザーだけがサーバへのアクセスを許可されている。 adminreadonly : Avamar サーバは読み取り専用状態になっており、管理者の root アカウントを持つユーザーだけがサーバへのアクセスを許可されている。

表 73 [Server Management] の [Node Information] 領域に表示されるサーバーの詳細 (続き)

プロパティ	説明
	<ul style="list-style-type: none"> • readonly : Avamar サーバは読み取り専用状態。リストアは実行できるが、新しいバックアップは作成されない。 • suspended : スケジューラを再度有効化するまで、スケジュール設定バックアップが無効になる。 • synchronizing : Avamar サーバがストライプの準備または同期化を行っている。一時的な条件。一部の機能の実行が遅延されることがあります。
Accessmode	<p>サーバーの現在のアクセスレベル。フル サーバ アクセスモードは通常、3 つの 4 ビット フィールドで表されます。例: mhpu+mhpu+0000 最上位の 4 ビットはサーバ権限を示し、中間の 4 ビットは root ユーザー権限を示します。最下位の 4 ビットは、他の全ユーザーの権限を示します。これらのフィールドの各ビットは、以下の情報を示します。</p> <ul style="list-style-type: none"> • m : 移行が許可されている。 • h : HFS (ハッシュ ファイル システム) が書き込み可能。 • p : 固定ストアは書き込み可能。 • u : ユーザー アカウンティングは書き込み可能。
Port	イントラ ノードの通信に使用されるデータ用ポート。
Dispatcher	このノードと通信するために各種ユーティリティが使用するデータ用ポート。
Server uptime	この Avamar サーバが初期化されてから、経過した時間数、日数、および分数。
Server bytes reserved	現在のストライプ ファイルが占有する最大サイズ。
Amount of reserved used	ストライプ ファイルおよびキャッシュ内のバックアップデータのサイズ。
Total capacity	サーバーの合計ストレージ容量。
Capacity used	特定の用途に使用されたサーバーの合計ストレージ容量。
Server Utilization	ノードで利用可能なストレージ容量の合計に対する現在使用中の容量の割合。
Number of stripes	このノードのストライプの合計数。
サーバーのバージョン	このノードで実行する Avamar ソフトウェアのバージョン。

表 74 [Server Management] の [Node Information] 領域に表示される OS の詳細

プロパティ	説明
Version	このノードで実行されている現在のオペレーティングシステムのバージョン。
Node uptime	このノードが最後に起動されてから経過した時間数、日数、および分数。
Total bytes free in partitions	OS レベルの空きディスク サイズ。
Total bytes used in partitions	OS レベルの使用済みディスク サイズ。
Load average	過去 1 分間の CPU スレッド数の平均値。
CPU %	このノードで現在使用中の CPU の割合。
Ping time (sec)	このノードが、ping 要求に応答するまでに費やした秒数。
Disk reads	1 秒あたりのハードドライブの読み取り処理回数。
Disk writes	ハードドライブの 1 秒あたりの書き込み処理回数。
Network reads	このノードのネットワーク接続で 1 秒に読み取るキロバイト数。
Network writes	このノードのネットワーク接続で 1 秒に書き込むキロバイト数。

表 75 [Server Management] の [Node Information] 領域に表示されるハードウェアの詳細

プロパティ	説明
IP address	このノードの IP アドレス。
MAC address	MAC (Media Access Control) アドレス。Avamar サーバでこのノードをユニークに識別する低レベルのハードウェア アドレス。
Number of partitions	このノードの論理ハードドライブパーティションの合計数。
Generation	ハードウェア プラットフォームのタイプ。
一般的な説明	ハードウェア プラットフォームのタイプの説明。

パーティション情報

次の表では、[Server Management] タブでパーティションを選択したときに表示される [Partition Information] に関する詳細を示します。

表 76 [Server Management] の [Partition Information] 領域の [Status indicators]

プロパティ	説明
Status indicators	以下のいずれかの値を指定します。

表 76 [Server Management] の [Partition Information] 領域の [Status indicators] (続き)

プロパティ	説明
	<ul style="list-style-type: none"> オンライン (グリーン) : パーティションは正常に機能している。 オフライン (イエロー) : パーティションに1つ以上のオフライン ストライプがある。ConnectEMC が有効になっている場合は、SR (サービス リクエスト) が記録されているはず。既存のサービス リクエストを表示するには、Avamar サポート用 Web サイトに移動します。 読み取り専用 (青) : パーティションが読み取り専用になっている。 非機能 (赤) : パーティションが機能していない。Avamar サポート Web サイトで、ナレッジベース KB000465715「Suspended Partitions \Stripes and Hfscheck Failures on Avamar (Symptom Code 22632)」を検索してください。
Server bytes reserved	現在のストライプ ファイルが占有する最大サイズ。
Amount of reserved used	ストライプ ファイルおよびキャッシュ内のバックアップ データのサイズ。

表 77 [Server Management] の [Node Information] 領域に表示されるサーバーの詳細

プロパティ	説明
Total capacity	サーバーの合計ストレージ容量。
Capacity used	サーバーの使用済み合計ストレージ容量。
Server Utilization	使用中のパーティションで使用可能なストレージ容量の合計の割合。
State	<p>このパーティションにおける現在の稼働状態を示します。以下のいずれかの値を指定します。</p> <ul style="list-style-type: none"> ONLINE : パーティションは正常に機能している。 MIGRATING : 通常の操作に起因するかどうかに関係なく発生する移行の状態。 OFFLINE : 通常の操作に起因するかどうかに関係なく発生する移行の状態。 READY : 通常の操作に起因するかどうかに関係なく発生する移行の状態。 RESTARTING : 通常の操作に起因するかどうかに関係なく発生する移行の状態。
Number of offline stripes	メディア エラーが原因でオフラインとなっている、このパーティション上のストライプの合計数。

表 77 [Server Management] の [Node Information] 領域に表示されるサーバーの詳細 (続き)

プロパティ	説明
Number of transitioning stripes	通常の操作に起因するかどうかに関係なく発生する移行の状態にある、このパーティション上のストライプの合計数。
Properties	各種オペレーティング システムのプロパティ (既知の場合)。
Values	オペレーティング システムのプロパティの設定 (既知の場合)。
Total bytes free in partitions	OS レベルの空きディスク サイズ。
Total bytes used in partitions	OS レベルの使用済みディスク サイズ。

Data Domain システム情報

次の表は、[Server Management] タブの Data Domain システムのプロパティに関する詳細を示します。

表 78 [Server Management] タブの Data Domain システムのプロパティ

プロパティ	説明
Status indicators	以下のいずれかの値を指定します。 <ul style="list-style-type: none"> オンライン (グリーン) : Data Domain システムは正常に機能しています。 オフライン (イエロー) : Data Domain システムはオフラインです。詳細については、Avamar サポートから入手可能な「Data Domain Offline Diagnostics Suite User Guide」を参照してください。 読み取り専用 (ブルー) : Data Domain システムが読み取り専用になっています。 非機能 (レッド) : Data Domain システムは機能していません。詳細については、「Data Domain Offline Diagnostics Suite User Guide」を参照してください。
IPv4 Hostname	社内 DNS で定義される Data Domain システムの IPv4 ホスト名。
IPv6 Hostname	社内 DNS で定義される Data Domain システムの IPv6 ホスト名。
Total Capacity (post-comp size)	Data Domain システムの圧縮データの合計容量。
Server Utilization (post-comp use%)	データ圧縮後に何らかの理由のために Data Domain システムで使用される容量の割合。

表 78 [Server Management] タブの Data Domain システムのプロパティ (続き)

プロパティ	説明
Bytes Protected (client pre-comp size)	Data Domain システムで保護されている (バックアップされている) データの合計バイト数。この値はデータが圧縮される前のバイト数です。
File System Available (post-comp avail)	DDFS で圧縮データで使用可能なディスク領域の合計容量。
File System Used (post-comp used)	DDFS で圧縮データで使用されるディスク領域の合計容量。
Username	該当する場合、バックアップ、リストア、レプリケーションのために Avamar が Data Domain システムへのアクセスに使用する Data Domain OST (OpenStorage) アカウントのユーザー名。このユーザー名は、Data Domain システムが Avamar 構成に追加される際に指定されます。
Default Replication Storage System	Data Domain システムがデフォルトのレプリケーションストレージとして構成されているかどうかを示します。Data Domain システムを Avamar 構成に追加する際に、このオプションを選択またはクリアします。
Target For Avamar Checkpoint Backups	Data Domain システムに Avamar チェックポイントバックアップを保存するかどうかを指定します。
Maximum Streams For Avamar Checkpoint Backups	Data Domain システムの Avamar チェックポイントバックアップ用の予約済みストリームの最大数。
Maximum Streams	バックアップとリストアの実行時に Avamar が一度に使用できる Data Domain システムのストリームの最大数。システムを Avamar 構成に追加する際に、Data Domain システム用にこの数字が構成されます。
Maximum Streams Limit	Data Domain システムのバックアップ書き込みストリームの最大数。
Instant Access Limit	インスタント アクセス リストアから生成された仮想マシンの台数の制限。
DDOS Version	Data Domain システムの DD OS (Data Domain オペレーティング システム) バージョン番号。
Serial Number	Data Domain システムのディスクのメーカーのシリアル番号。
Model number	Data Domain システムのモデル番号。
Encryption Strength	Data Domain システム上の DDboost クライアントのデフォルトのグローバル暗号化強度。値は none、medium、high です。
Authentication Mode	Data Domain システム上の DDboost クライアントのデフォルトのグローバル認証モード。値は none、one-way、two-way、anonymous です。

表 78 [Server Management] タブの Data Domain システムのプロパティ (続き)

プロパティ	説明
Monitoring Status	Data Domain システムの監視ステータス。使用可能な値の詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。
Monitoring status details	<p>モニタリング ステータスが [OK] 以外の値である場合、補足情報が [Monitoring Status] 行の下にあるリストに示されます。以下のエントリーは、使用可能な値を示します。</p> <hr/> <p>注</p> <p>これらの各値に起因しているエラー状態をトラブルシューティングする方法の詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。</p> <hr/> <p>DD Boost ライセンス ステータス (以下のいずれか)。</p> <ul style="list-style-type: none"> • DDBoost Licensed • DDBoost not Licensed <p>DD Boost ステータス (以下のいずれか)。</p> <ul style="list-style-type: none"> • DDBoost Enabled • DDBoost Disabled <p>DD Boost ユーザーが有効か無効か (以下のいずれか)。</p> <ul style="list-style-type: none"> • DDBoost User Enabled • DDBoost User Disabled <p>DD Boost ユーザー ステータス (以下のいずれか)。</p> <ul style="list-style-type: none"> • DDBoost User Valid • DDBoost User Changed <p>DD Boost オプション ステータス (以下のいずれか)。</p> <ul style="list-style-type: none"> • DDBoost Option Enabled • DDBoost Option Disabled • DDBoost Option not Available <p>非 OST ユーザーのステータス (構成済みの場合) (以下のいずれか)。</p> <ul style="list-style-type: none"> • Non-ost user state is Unknown • Non-ost user Invalid • Non-ost user disabled • Non-ost user is not an admin user

表 78 [Server Management] タブの Data Domain システムのプロパティ (続き)

プロパティ	説明
	<p>注</p> <p>非 OST ユーザーが構成されていない場合、非 OST ユーザーの行は表示されません。</p> <hr/> <p>SNMP ステータス (以下のいずれか)。</p> <ul style="list-style-type: none"> • SNMP Enabled • SNMP Disabled <p>Data Domain ファイル システムのステータス (以下のいずれか)。</p> <ul style="list-style-type: none"> • File System Running • File System Enabled • File System Disabled • File System Unknown • File system status unknown since SNMP is disabled <p>Avamar サーバと Data Domain システム間でメンテナンス操作 (チェックポイント、HFS チェック、ガベージコレクションなど) の同期化が発生するかどうか (以下のいずれか)。</p> <ul style="list-style-type: none"> • Synchronization of maintenance operations is off. • Synchronization of maintenance operations is on.
Cloud Tier	クラウド階層のステータス。有効化されている場合は、クラウド ユニット名を表示するか、disabled として表示します。

イベントの監視

すべての Avamar システム アクティビティと動作ステータスは、イベントとして MCS にレポートされます。Avamar イベントの例としては、クライアントの登録や起動、バックアップの成功と失敗、ハードディスクのステータスがあります。

各イベントには、以下の表の情報が含まれます。

表 79 イベント情報

情報	説明
Event code	一意識別子
Date and time	イベントが報告された日時
Category	イベントのカテゴリ :

表 79 イベント情報 (続き)

情報	説明
	<ul style="list-style-type: none"> • SYSTEM • APPLICATION • USER • セキュリティ
タイプ	イベントのタイプ : <ul style="list-style-type: none"> • INTERNAL • ERROR • WARNING • INFORMATION • DEBUG
Summary	イベントの内容を 1 行でまとめたもの
発生元のハードウェア	イベントを報告したシステム ノード
発生元のソフトウェア	イベントを報告したシステムまたはアプリケーション モジュール

イベント通知

次の機能は、特定のイベント発生時に通知を生成します。

ポップアップ アラート

個々のイベントを構成して、イベントが発生するたびにグラフィカルなポップアップ アラートを生成することができます。ポップアップ アラートを表示するには、Avamar Administrator を実行している必要があります。

ACK が必要なリスト

特定のタイプのイベントが発生した場合に、Avamar システム管理者の確認が必要となるように指定できます。

メール メッセージ

特定のタイプのイベントが発生した場合に、指定された受信者のリストにメール メッセージを送信するように指定できます。メール通知はすぐに送信することも、スケジュール設定された時刻に一括送信することもできます。

一般的なバッチ送信メールによる通知メッセージ内容は、次の例のようになります。

表 80 バッチ送信メールによる通知メッセージの例

```
MCS: avamar-1.example.com

MCS Version: 7.1.0-nnn
Avamar Server: avamar-1.example.com
Avamar Server Version: 7.1.0-nnn

Event profile: My Custom Profile
```

表 80 バッチ送信メールによる通知メッセージの例 (続き)

Count of events: 3

Summary of events:

Type

```

-----
INFORMATION
INFORMATION
INFORMATION
    
```

Type	Code	Count	Summary
-----	-----	-----	-----
INFORMATION	22207	1	New group
INFORMATION	22208	1	created
INFORMATION	22209	1	Group modified
			Group deleted

```

Event Code = 22207
Event Date/Time = 5/10/14 09:58:20 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = New group created
Software Source = MCS:CR
    
```

```

Event Code = 22209
Event Date/Time = 5/10/14 09:58:25 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group deleted
Software Source = MCS:CR
    
```

```

Event Code = 22208
Event Date/Time = 5/10/14 10:55:28 PDT
Event Type = INFORMATION
Event Severity = OK
Event Summary = Group modified
Software Source = MCS:CR
    
```

Syslog のサポート

特定のタイプのイベントが発生した場合に、イベントを受信する **syslog** デーモン用に構成されたフィルタリングルールに基づいて、**Avamar** がローカルまたはリモートの **syslog** ファイルにログを記録するように指定できます。ログ エントリーの調査機能を持つサードパーティ製のモニタリングツールおよびユーティリティは、**syslog** ファイルにアクセスして処理し、**Avamar** のイベント情報をより大規模なサイトアクティビティおよびステータスレポートに統合できます。

SNMP のサポート

Avamar SNMP 実装では、**Avamar** サーバ イベントとアクティビティ完了ステータスにアクセスする方法を 2 つ用意しています。

- SNMP 要求には、SNMP 管理アプリケーションがリモートの SNMP 対応クライアント（この場合は Avamar サーバ）から情報を「プル」するためのメカニズムが備わっています。
- SNMP トラップには、指定された Avamar イベントが発生すると必ず、Avamar サーバが SNMP 管理アプリケーションに情報を「プッシュ」するメカニズムが備わっています。SNMP トラップを出力するようにイベントタイプを構成できます。

使用状況インテリジェンス

Avamar サーバでレポート作成情報を自動的に収集し、ESRS Gateway 経由で Avamar サポートに転送できます。

イベント プロファイル

プロフィールとは、特定のイベントコードを論理的にグループ化するために使用される通知管理機能で、これらのイベントが発生した場合にどの通知を送信するべきかを指定します。

イベントプロフィールには、2 種類の基本タイプがあります。

- **[System profile]** : システム イベント プロファイルは 1 つだけ存在します。このプロフィールには、実行可能なすべてのシステム イベントコードが含まれています。
- **[Custom profiles]** : カスタム プロファイルは、特定のシステム イベントが発生した際に各種通知を送信するために使用します。カスタム プロファイルは必要な数だけ作成できます。このステップで、システム イベントを構成し、それらのイベントが発生したときに通知を生成します。

プロフィール カタログ

Avamar システムには、事前構成されたイベントプロフィールのセットがデフォルトで含まれています。

システム プロファイル

システム イベント プロファイルは 1 つだけ存在します。このプロフィールには、実行可能なすべてのシステム イベントコードが含まれています。

Evaluation profile

評価プロフィールは、システムの評価をサポートするために主に使用します。このプロフィールが有効な場合、このプロフィールによってメール通知が生成され、2 週間分の [Activities - DPN Summary] レポートの情報がメールに添付されます。[Activities - DPN Summary] レポートの詳細については、「Avamar レポートガイド」を参照してください。

High Priority Events profile

優先度の高いイベントプロフィールはデフォルトで有効になっています。この特別なイベントプロフィールは、次の情報を Avamar サポート (emailhome@avamar.com) に 1 日 2 回自動的にメール メッセージで送信します。

- 日々のデータ整合性チェック処理のステータス
- 特定の Avamar サーバ警告と情報メッセージ
- Avamar サーバ エラー

優先度の高いイベントプロフィールに対して変更できるのは、[Recipient Email List] へのメールアドレスの追加のみです。優先度の高いイベントプロフィールのカスタム設定が必要な場合は、プロフィールをコピーして、そのコピーを編集します。

ローカル SNMP トラップ プロファイル

ローカル SNMP トラップ プロファイルは読み取り専用で、テスト目的でのみ使用することを想定しています。このプロフィールにより、トラップが正常に生成されて、ローカル snmptrapd プロセスで受信され、このプロセスによって、トラップ情報が syslog ファイルに書き込まれたことを確認できます。

ローカル syslog プロファイル

これが有効の場合、Avamar サーバのローカル `syslogd` プロセスを使用して、ローカル `syslog` プロファイルがステータスをレポートします。

使用状況インテリジェンス プロファイル

Avamar サーバでレポート作成情報を自動的に収集し、ESRS Gateway 経由で Avamar サポートに転送できます。

システム イベント プロファイルの編集

システム イベント プロファイルには、発生する可能性のあるすべてのシステム イベント コードが含まれています。システム イベント プロファイルを編集して、イベントによって Avamar Administrator でポップアップ アラートを生成するか、共通の未確認イベント リストにエントリーを生成するか、そのいずれも実行しないかを制御できます。

手順

1. Avamar Administrator で、**[Tools]** > **[Manage Profiles]** を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルで **[System Profile]** を選択して、**[Edit]** をクリックします。
[Edit Profile] ダイアログ ボックスがイベント コードのリストとともに表示されます。
3. イベントが発生するたびに Avamar Administrator でグラフィカルなポップアップ アラートを表示するには、イベントの横にある **[GUI Alert]** チェックボックスを選択します。
4. イベントが発生するたびに共通の未確認イベント リストにエントリーを追加するには、**[Acknowledgement Required]** チェックボックスを選択します。
5. **[OK]** をクリックします。

カスタム イベント プロファイルの作成

カスタム イベント プロファイルによって、特定のシステム イベントが発生した際に通知を送信できます。

自分がログインするドメイン以外のシステム イベントとプロファイルを表示することはできません。このステップはユーザーが編集できるプロファイルおよびプロファイルに追加できる特定のイベントに影響しません。

手順

1. Avamar Administrator で、**[Tools]** > **[Manage Profiles]** を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルで、カスタム イベント プロファイルのドメインを選択し、**[New]** をクリックします。
[New Profile] ウィザードが表示されます。
3. **[Profile Name]** ボックスに、このイベント プロファイルの名前を入力します。
4. **[Profile Type]** は **[Email, Syslog, and SNMP Trap Notification]** のデフォルト設定のままにします。

注

使用状況インテリジェンス機能は、事前構成済みの使用状況インテリジェンスのプロファイルを使用するため、使用状況インテリジェンス プロファイル タイプに基づくプロファイルを作成しません。このステップにより冗長データが Avamar サポートに送信されます。

5. このプロファイルを有効化または無効化するかを選択するには、[**Profile Enabled**] チェックボックスを選択または選択解除します。
6. このプロファイルでメール通知を有効化するかどうかを選択するには、[**Email Enabled**] チェックボックスを選択または選択解除します。
7. メール通知を有効化した場合は、メール通知をイベントが発生した直後に送信するか、スケジュール設定に基づいて送信するかを指定します。
 - メール通知をイベントが発生した直後に送信するには、[**Send data as events occur**] を選択します。
 - メール通知をスケジュール設定に基づいて送信するには、[**Send data on a schedule**] を選択した後、リストからスケジュールを選択します。
8. このプロファイルでシステムログ通知を有効化または無効化するかを選択するには、[**Syslog Notification – Enabled**] チェックボックスを選択または選択解除します。
9. このプロファイルで SNMP 通知を有効化または無効化するかを選択するには、[**SNMP Trap Notification – Enabled**] チェックボックスを選択または選択解除します。
10. [**Next**] をクリックします。
[**Event Codes**] ページが表示されます。
11. [**All Codes**] タブをクリックして、通知をトリガーするエラーの横にある [**Notify**] チェックボックスを選択します。

通知

イベントの横に表示されているアスタリスク (*) は、他のイベント通知がスケジュール設定に基づいて送信されている場合でも、イベントが発生したときに通知が送信される重大度のイベントであることを示します。

12. [**All Codes**] タブをクリックして、通知をトリガーする監査イベントの横にある [**Notify**] チェックボックスを選択します。

通知

イベントコードの横に表示されているアスタリスク (*) は、アスタリスクが付いていないイベント通知がスケジュールに従って送信されている場合でも、アスタリスクが付いているイベントは、イベントが発生するたびに通知が送信される重要度のイベントであることを示します。

13. このカスタム イベント プロファイルを最上位レベル（ドメインやサブドメインではない）で追加する場合、容量フォーキャスト アラートのコントロールに使用するパラメーターを指定します。
 - a. [**Parameters**] タブをクリックします。
 - b. パラメーターの横のチェックボックスを選択し、新しいパラメーター値を入力します。
 - c. 必要に応じて、各パラメーターについて前のステップを繰り返します。
14. [**Next**] をクリックします。
[**Attachments**] ページが表示されます。
15. (オプション) プロファイルにメール通知メッセージが含まれている場合は、[**Attach Server status in email (XML)**] チェックボックスを選択すると、Avamar サーバの全体的なステータスに関するレポートが XML 形式でメッセージに含まれます。
16. (オプション) メール通知メッセージに Avamar サーバ ログを含めるには、[**Attach Server logs in email**] チェックボックスを選択して、[**Directory**] ボックスに Avamar サーバ ログ

の場所のフルパスを入力します。デフォルトの場所は `/usr/local/avamar/var/cron/` です。

17. メール通知メッセージに含めるレポートを指定します。
 - a. メッセージに含めるレポートの横の **[Attach]** チェックボックスを選択します。
 - b. レポートの横のチェックボックスで、レポートを送信するファイル形式を選択します。**[XML]**、**[CSV]**、**[TXT]** のいずれかを選択できます。
 - c. **[Since Count]** および **[Since Unit]** フィールドを使用して、各通知メッセージとともに送信するこのタイプの履歴レポートの数を指定します。例えば、過去 2 か月のレポートを送信します。

次の値が **[Since Count]** リストで選択できます。

- **[day(s) ago]**
- **[week(s) ago]**
- **[month(s) ago]**
- **[since last modified]**

18. **[Next]** をクリックします。
[Email Notification] ページが表示されます。

19. プロファイルにメール通知メッセージが含まれている場合は、次の手順でメール通知メッセージの受信者とオプションを指定します。
 - a. **[Email Subject Header]** ボックスに、通知メッセージ用のメールの件名を入力します。
 - b. メールを受信者をリストに追加するには、**[Enter Recipient]** ボックスに有効なメールアドレスを入力して、**[+]** をクリックします。
 - c. (オプション) **[Recipient Email List]** から受信者を削除するには、受信者を選択して、**[-]** をクリックします。
 - d. メール通知メッセージの本文にすべての添付ファイルを挿入する場合は、**[Inline attachment]** チェックボックスを選択します。

通知

添付ファイルを挿入すると、メールメッセージが非常に長くなる場合があります。

- e. テスト用メールメッセージをすぐに送信する場合、**[Send Email]** をクリックします。
テスト用メールメッセージが正常に送信された場合は、`Email accepted by transport layer` 確認メッセージが表示されます。
20. **[Next]** をクリックします。
[Syslog Notification] ページが表示されます。
21. プロファイルにシステムログ通知メッセージが含まれている場合は、次の手順でシステムログ通知パラメーターを指定します。
 - a. **[Address (IP or hostname)]** ボックスに、`syslogd` プロセスを実行している Avamar サーバノードの IP アドレスまたはホスト名を入力します。
 - b. **[Port Number]** ボックスに、`syslog` 通信用に使用されるポート番号を入力します。

- c. 拡張イベント コード情報をシステムログ メッセージに含めるかどうかを選択するには、**[Include extended event data]** チェックボックスを選択または選択解除します。

この拡張された情報は次のタグを使用して区切られます。

```
<Code>
<Type>
<Severity>
<Category>
<HwSource>
<Summary>
<active>
<lastEmailSendDate>
<domain>
<scheduleID>
<num_prefs>
<name>
<isSystem>
```

- d. **[Facility]** リストで、次のいずれかを選択します：**[user]**、**[local0]**、**[local1]**、**[local2]**、**[local3]**、**[local4]**、**[local5]**、**[local6]**、**[local7]**

- e. システムログ通知パラメーターをテストするには、**[Send Test Syslog Entry]** をクリックします。

22. **[Next]** をクリックします。

[SNMP Trap Notification] ページが表示されます。

23. プロファイルに SNMP 通知メッセージが含まれる場合は、次の手順で SNMP 通知パラメーターを指定します。

- a. **[SNMP Trap address (IP or hostname)]** ボックスに、SNMP トラップの受信および処理が可能なアプリケーションを実行しているコンピューターの IP アドレスまたはホスト名を入力します。

- b. **[Port Number]** ボックスに、SNMP トラップをリスンするホスト サーバのポート番号を入力します。デフォルトのデータ用ポートは 162 です。

- c. **[SNMP Community]** ボックスに、SNMP トラップ リスナーが使用するよう構成されている、SNMP コミュニティの名前を入力します。

SNMP コミュニティとは、ローカルの Net-SNMP エージェントが SNMP 管理アプリケーションでエージェント自体を認証するために使用するテキスト文字列です。

- d. SNMP 通知パラメーターをテストするには、**[Send Test SNMP Trap]** をクリックします。

24. **[Finish]** をクリックします。

カスタム イベント プロファイルの編集

特定のシステム イベントの通知用にカスタム イベント プロファイルを作成した後で、プロファイルにあるすべてのプロパティを編集できます。

自分がログインするドメイン以外のシステム イベントとプロファイルを表示することはできません。このステップはユーザーが編集できるプロファイルおよびプロファイルに追加できる特定のイベントに影響します。

手順

1. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルで、カスタム イベント プロファイルを選択して、[Edit] をクリックします。
[Edit Profile] ダイアログ ボックスが表示されます。
3. カスタム イベント プロファイルを編集します。各プロパティは、プロファイルを作成する場合と同じです。
4. [OK] をクリックします。

カスタム イベント プロファイルのコピー

プロファイルをコピーすると、すでに作成したプロファイルと同じプロパティを使用したカスタム イベント プロファイルを作成できます。プロファイルは同じドメインまたは別のドメインにコピーできます。

手順

1. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルでプロファイルを選択して、[Copy] をクリックします。
[Save As] ダイアログ ボックスが表示されます。
3. [Save As] ボックスに新しいカスタム イベント プロファイルの名前を入力します。
4. (オプション) 新しいカスタム イベント プロファイルを異なるドメインにコピーするには、[...] ボタンをクリックして新しいドメインを参照し、[OK] をクリックします。
5. [OK] をクリックします。

カスタム イベント プロファイル通知のテスト

短いメール メッセージを送信するか、syslog ファイルに短いメッセージを書き込むことで、カスタム イベント プロファイルの通知メカニズムをテストできます。

手順

1. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルで、カスタム イベント プロファイルを選択して、[Edit] をクリックします。
[Edit Profile] ダイアログ ボックスが表示されます。
3. カスタム イベント プロファイルを次のようにテストします。
 - テスト用メール メッセージを送信するには、[Email Notification] タブを選択して、[Send Email] をクリックします。
 - テスト用メッセージをシステムログ ファイルに書き込むには、[Syslog Notification] タブを選択して、[Send Test Syslog Entry] をクリックします。
 - テスト用 SNMP トラップ メッセージを送信するには、[SNMP Trap Notification] タブを選択して、[Send Test SNMP Trap] をクリックします。

テスト用メッセージが正常に送信された場合は、確認メッセージが表示されます。
4. [OK] をクリックします。
5. [Edit Profile] ダイアログ ボックスを閉じるには、[OK] をクリックします。

カスタム イベント プロファイルの有効化と無効化

イベント プロファイルを無効化すると、プロフィールを再度有効にするまで、メール通知は送信されません。システム イベント プロファイルを除き、任意のプロファイルを無効化することができます。

手順

1. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルで、イベント プロファイルを選択します。
3. イベント プロファイルを無効化するために [Disable] をクリックするか、イベント プロファイルを有効化するために [Enable] をクリックします。

カスタム イベント プロファイルの削除

システム イベント ログを除き、任意のカスタム イベント プロファイルを完全に削除することができます。

手順

1. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. イベント プロファイルを選択し、[Delete] をクリックします。
確認メッセージが表示されます。
3. [はい] をクリックします。

[Event Monitor] でイベントを表示する

手順

1. Avamar Administrator で、[Administration] 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. [Event Management] タブをクリックします。
3. [Event Monitor] タブをクリックします (ウィンドウの下部に位置)。
[Event Monitor] の各列の詳細については、Avamar Administrator のオンライン ヘルプを参照してください。
4. [Event Monitor] の表示モードを次のように選択します。
 - 定義した日付範囲の最新の 5,000 件のシステム イベントを表示するには、[Query] を選択します。
 - 過去 24 時間の最新の 5,000 件のシステム イベントを表示するには、[Monitor] を選択します。
5. (オプション) [Event Monitor] に表示されるイベントをフィルターします。
 - a. [Actions] メニューを開いて、[Event Management] > [Filter] を選択します。
[Filter] ダイアログ ボックスが表示されます。
 - b. [Event Monitor] で [Query] 表示モードを選択した場合は、[From Date] および [To Date] フィールドを使用して、表示するイベントの日付範囲を選択します。
 - c. [Category] リストから、表示するイベントのカテゴリを選択します。

- d. **[Type]** リストから、表示するイベントのタイプを選択します。
- e. **[Severity]** リストから、表示するイベントの重大度を選択します。
- f. すべてのドメインのイベントを表示するには、**[All Domains]** を選択します。または、特定のドメインのイベントを表示するには、**[Domain]** を選択して、ドメイン名を参照または入力します。
- g. イベントコードデータの XML 要素で特定のキーワード（大文字と小文字を区別）を含むイベントのみを表示するには、**[Data]** ボックスにキーワードを入力します。
この基準により、イベント属性全体を重要なキーワードで容易にフィルター処理できるようになります。例えば、**[Event Monitor]** の表示を **error** でフィルターすると、任意の XML 属性（例えば、カテゴリ、タイプ、重大度）に **error** という文字を含むすべてのイベントが返されます。
- h. すべてのソース、Avamar サーバのみ、すべての Data Domain システム、単一の Data Domain システムのいずれからのイベントを表示するかを選択します。
 - すべてのソースからのイベントを表示するには、**[Source]** リストの **[All Sources]** のデフォルト選択を維持します。
 - Avamar サーバからのみのイベントを表示するには、**[Source]** リストから **[Avamar]** を選択します。
 - すべての Data Domain システムからのイベントを表示するには、**[Source]** リストから **[Data Domain Systems]** を選択し、**[All Systems]** のデフォルト選択を維持します。
 - 単一の Data Domain システムからのイベントを表示するには、**[Source]** リストから **[Data Domain Systems]** を選択し、**[System]** オプションを選択した後、Data Domain システムを入力するか、参照します。
- i. **[More]** をクリックすると、追加のフィルター基準が表示されます。
- j. 特定のイベントコードを持つイベントのみを **[Event Monitor]** で表示するには、**[Only include codes]** を選択して、リストでコードの追加および削除を実行します。または、特定のイベントコードを持つイベントを **[Event Monitor]** から除外するには、**[Exclude codes]** を選択して、リストでコードの追加および削除を実行します。
- k. **[OK]** をクリックします。

イベントカタログの表示

すべてのイベントコードおよびサマリー情報のシーケンシャルリストが、Avamar サーバの `/usr/local/avamar/doc/event_catalog.txt` で参照できます。Web ブラウザーを使用して、`event_catalog.txt` を参照することも可能です。

手順

1. Web ブラウザを開き、次の URL を入力します。

```
https://Avamar_server
```

ここで、`Avamar_server` は Avamar サーバの DNS 名または IP アドレスです。

[Avamar Web Restore] ページが表示されます。

2. **[Documentation]** をクリックします。

[Avamar Documentation] ページが表示されます。

3. **[Avamar Event Codes]** の横にあるプラス アイコンをクリックします。
4. **[event_catalog.txt]** をクリックします。
このファイルが Web ブラウザーで開きます。

システム イベントの確認

システム イベントが発生するたびに確認を要求するように構成されている場合は、Avamar サーバ管理者によって明示的にクリアまたは確認されるまで、イベントは未確認のイベントリストに残ります。

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[Event Management]** タブをクリックします。
3. ウィンドウ下部近くにある **[Unacknowledged Events]** タブをクリックします。
4. 次のようにイベントを確認します。
 - 1 件以上のイベントを確認するには、イベント エントリーを選択して、**[Actions]** > **[Event Management]** > **[Acknowledge Unacknowledged Events]** を選択します。
 - リストにあるすべてのイベントを確認するには、**[Actions]** > **[Event Management]** > **[Clear All Alerts]** を選択します。

エラー イベントのカスタマイズ

デフォルトでは、Avamar ソフトウェアは `/var/log/messages` を継続的に監視し、大文字と小文字の区別なく、検索文字列 `error` が発生しているかどうかを検索します。`error` が発生した場合は、**ERROR** タイプのイベント コードを作成します。このデフォルトの動作はカスタマイズ可能です。

手順

1. 追加の検索文字列（大文字と小文字の区別なし）を定義して、これらによっても Avamar **ERROR** イベントが作成されるようにします。
2. `/usr/local/avamar/var/mc/server_data/adminlogpattern.xml` に検索文字列を追加します。

syslog を使用したサーバのモニタリング

システムログを使用する UNIX および Linux システム上のシステム ログ機能では、システム ログのメッセージを収集して、指定したログ ファイルに書き込みます。**syslog** 形式でイベント情報を送信するように、Avamar サーバを構成することができます。

Avamar サーバは、**syslog** と **syslog-ng** の両方の実装をサポートします。

注

Avamar サーバの **syslog** のモニタリングを構成する担当者は、基本的な **syslog** の概念に精通した人物が望ましいです。基本的な **syslog** の概念と実装方法の詳細は、このガイドの範囲外になります。関連情報については、www.syslog.org を参照してください。

オペレーティング システム レベルでは、システムのモニタリングおよびログは `syslogd` プロセスを使用して、システム ログのメッセージを収集し、指定されたログ ファイルにそれらを書き込みます。`syslogd` プロセスはすべての Avamar サーバ ノードでローカルに実行されます。

ただし、追加の構成を行わない場合、各ノードの `syslogd` はそのノードのシステム情報のみを収集し、そのノードのローカル ログ ファイルに書き込みます。`syslog` の観点から見た場合、各 Avamar サーバ ノードは、他のサーバ ノードの存在について認識しません。また、ユーティリティ ノードの `syslog` プロセスでは、Avamar MCS (Management Console Server) が Avamar イベント情報を収集し、ログを行うことを認識しません。

Avamar イベントプロファイルを構成して、Avamar サーバ イベントのメッセージを `syslog` 形式で作成し、このデータを Avamar サーバ ユティリティ ノードで実行されている `syslogd` プロセスに送信するようにできます。

次の表では、イベントプロファイルによる Avamar サーバ イベント データと各種 `syslog` フィールドとのマッピング方法を示します。

表 81 `syslog` フィールドの Avamar イベント データへのマッピング

システムログのフィールド	Avamar イベント データ
Facility	User または Local#。ここで、#は 0~7 の数字です。
Priority	次の値のいずれか (Avamar イベントタイプによる) : <ul style="list-style-type: none"> • <code>debug</code> : Avamar イベントタイプが <code>DEBUG</code> の場合 • <code>err</code> : Avamar イベントタイプが <code>ERROR</code> の場合 • <code>info</code> : Avamar イベントタイプが <code>INFO</code> の場合 • <code>none</code> : Avamar イベントタイプが <code>INTERNAL</code> の場合 • <code>warning</code> : Avamar イベントタイプが <code>WARNING</code> の場合
Date	Avamar イベントの日付
Time	Avamar イベントの時間
Hardware source	Avamar イベントのハードウェア ソース
Software source	Avamar イベントのソフトウェア ソース
Message	Avamar イベント コードの次の各フィールド。 <ul style="list-style-type: none"> • <code>event code</code> • <code>category</code> • <code>summary</code> • <code>event data</code>

ローカル `syslog` の構成

Avamar サーバ `syslog` モニタリングを実装するための最も基本的な方法は、ユーティリティ ノードで実行されるローカル `syslogd` プロセスに Avamar イベント情報を出力するように MCS を構成す

ることです。ローカル `syslogd` サービスによって、単一のローカル ログ ファイルに Avamar イベント情報とオペレーティング システムのメッセージがマージされます。

手順

1. 次の手順で、Avamar サーバ上でローカル `syslog` のイベント プロファイルを有効化します。
 - a. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
 - b. 左のパネルで [Local Syslog] イベント プロファイルを選択し、[Enable] をクリックします。
2. SLES 11 以降を使用するシングル ノード サーバーおよびユーティリティ ノードでは、次の手順でローカル ユーティリティ ノードの `syslogd` プロセスを構成して、UDP データ用ポート 514 で MCS のイベント メッセージをリスンするようにします。

- a. コマンド シェルを開き、シングル ノード サーバーまたはマルチ ノード サーバーのユーティリティ ノードに `admin` としてログインします。
- b. `su -` と入力して、ユーザーを `root` に切り換えます。
- c. テキスト エディターで `/etc/syslog-ng/syslog-ng.conf` を開きます。
- d. 次のエントリーを検索します。

```
#
# uncomment to process log messages from network:
#
# udp(ip("0.0.0.0") port(514));
```

- e. 次のエントリー (コメントを含む) を追加します。

```
#
# uncomment to process log messages from MCS:
#
udp(ip("0.0.0.0") port(514));
```

- f. ファイルを保存して閉じます。
- g. 次のコマンドを入力して、システムログ プロセスを再開します。

```
service syslog restart
```

- h. 次のコマンドを入力して、システムログがポート 514 でリスンしていることを確認します。

```
netstat -nap | grep 514
```

以下の出力が、コマンド シェルに表示されます。

```
udp 0 0 127.0.0.1:514 127.0.0.1:* 8043/syslog-ng
```

リモート syslog の構成

リモート `syslog` モニタリングには、次の機能があります。

- リモート ログ ホストに `syslog` データを送信するように各サーバ ノードを構成する。
- Avamar サーバ イベント メッセージを `syslog` 形式でリモート ログ ホストに送信するカスタム `syslog` イベント プロファイルを作成する。

Avamar サーバのリモート `syslog` モニタリングを実装するサイトではほとんどのケースですでにリモート ログ ホストが構成され、導入されています。

多くの各種 **syslog** モニタリング ツールが利用可能です。UDP データ用ポート 514 で LAN 接続を介してリモート **syslog** メッセージをリスンするように構成されている限り、どのような **syslog** モニタリング ツールも通常、Avamar と連携できます。

通知

セキュリティを最大限向上させるために、リモート **syslog** モニタリングを実装してください。

手順

1. Avamar サーバ イベント メッセージを **syslog** 形式でリモート ログ ホストに送信するカスタム **syslog** イベント プロファイルを作成します。
2. システムログ メッセージをリモート ログ ホストに送信するように、すべてのサーバー ノードを構成します。
3. UDP データ用ポート 514 で LAN 接続を介してシステムログ メッセージをリスンするように、リモート ログ ホストを構成します。
4. リモート ログ ホストでファイアウォールが有効になっている場合、定義済み IP 範囲でポート 514 の UDP トラフィックを許可するようにファイアウォールを構成します。

カスタム システムログ イベント プロファイルの作成

手順

1. Avamar Administrator で、[Tools] > [Manage Profiles] を選択します。
[Manage All Profiles] ウィンドウが表示されます。
2. 左のパネルで [Local Syslog] イベント プロファイルを選択し、[Copy] をクリックします。
[Save As] ダイアログ ボックスが表示されます。
3. [Save As] フィールドに新しいカスタム イベント プロファイルの名前を入力します。
4. ドメインを root (/) のままにします。カスタム **syslog** プロファイルは root ドメイン内に存在している必要があります。
5. [OK] をクリックします。
6. [Manage All Profiles] ダイアログ ボックスで、作成したカスタム システムログ イベント プロファイルを選択して、[Edit] をクリックします。
[Edit Profile] ダイアログ ボックスが表示されます。
7. [Syslog Notification] タブを選択し、次の手順でシステムログ通知パラメーターを指定します。
 - a. [Address (IP or hostname)] フィールドで、リモート ログ ホストの IP アドレスまたはホスト名を入力します。
 - b. [Port Number] フィールドで、ポート番号を [514] のままにします。
 - c. 拡張イベント コード情報をシステムログ メッセージに含めるには、[Include extended event data] オプションを選択します。

この拡張された情報は次のタグを使用して区切られます。

```
<Code>
<Type>
<Severity>
<Category>
<HwSource>
<Summary>
```



```

<active>
<lastEmailSendDate>
<domain>
<scheduleID>
<num_prefs>
<name>
<isSystem>

```

- d. **[Facility]** リストで、次の値のいずれかを選択します：**[user]**、**[local0]**、**[local1]**、**[local2]**、**[local3]**、**[local4]**、**[local5]**、**[local6]**、**[local7]**
8. (オプション) システムログ通知パラメーターをテストするには、**[Send Test Syslog Entry]** をクリックします。
9. **[OK]** をクリックします。

システムログ メッセージをリモート ログ サーバーに送信するサーバー ノードの構成

リモートの **syslog** を構成するプロセスの一環として、すべての Avamar サーバ ノードを構成して、UDP データ用ポート 514 上の LAN 接続を介し、**syslog** メッセージをリモート ログ サーバに送信する必要があります。

手順

1. コマンド シェルを開きます。
 - a. サーバーに **admin** としてログインします。
 - b. 次のコマンドを入力して、ユーザーを **root** に切り替えます。

```
su -
```
 - c. グリッドの場合、次のコマンドを入力して、**rootid** OpenSSH キーをロードします。

```
ssh-agent bashssh-add /root/.ssh/rootid
```
2. テキスト エディターで **/etc/syslog-ng/syslog-ng.conf** を開きます。
3. 次のエントリーを追加します。

```
destination logserver {udp("ip_address" port(514)); };
log { source(src); destination(logserver); };
```

ここで、**ip_address** はリモート ログ ホストの IP アドレスです。
4. ファイルを保存して閉じます。
5. 次のコマンドを入力して、システムログ プロセスを再開します。

```
service syslog restart
```
6. マルチ ノード サーバーでは、各ノードでここまでのステップを繰り返します。

システムログを実行する RHEL リモート ログ ホストの構成

手順

1. コマンド シェルを開き、**root** としてリモート ログ ホストにログインします。
2. テキスト エディターで **/etc/sysconfig/syslog** を開きます。
3. 次のエントリーを検索します。

```
SYSLOGD_OPTIONS="-m 0"
```

4. エントリーに `-r` パラメーターを追加します。

```
SYSLOGD_OPTIONS="-r -m 0"
```

5. ファイルを保存して閉じます。
6. 次のコマンドを入力して、`syslogd` プロセスを再開します。

```
service syslog restart
```

syslog-ng を実行する SLES リモート ログ ホストの構成

手順

1. コマンド シェルを開き、`root` としてリモート ログ ホストにログインします。
2. テキスト エディターで `/etc/syslog-ng/syslog-ng.conf` を開きます。
3. 次のエントリーを検索します。

```
#
# uncomment to process log messages from network:
#
# udp(ip("0.0.0.0") port(514));
```

4. 次のようにエントリーのコメントを解除します。

```
#
# uncomment to process log messages from network:
#
udp(ip("0.0.0.0") port(514));
```

5. ファイルを保存して閉じます。
6. 次のコマンドを入力して、システムログ プロセスを再開します。
7. 次のコマンドを入力して、システムログがポート 514 でリスンしていることを確認します。

```
service syslog restart
```

```
netstat -nap | grep 514
```

以下の出力が、コマンド シェルに表示されます。

```
udp 0 0 0.0.0.0:514 0.0.0.0:* 8043/syslog-ng
```

リモート ログ ホストでのファイアウォールの構成

リモート ログ ホストでファイアウォールが有効になっている場合、定義済み IP 範囲でポート 514 の UDP トラフィックを許可するようにファイアウォールを構成します。

手順

1. リモート ログ メッセージのソース IP アドレスを `iptables` または別のファイアウォールで制約し、リモート ログ ホスト上の DoS（サービス拒否）攻撃を回避します。

次の `iptables` のルールの例では、Avamar サーバ ノードの IP アドレス範囲でクライアント システム ログを許可します。

```
# Rules to allow remote logging for syslog(-ng) on the log
HOST system
iptables -A INPUT -p udp -s 192.168.1.0/24 --dport 514 -j
ACCEPT
```

ここで、`192.168.1.0/24` は、Avamar サーバ ノードの IP アドレス範囲内にあります。

次の `iptables` のルールの例では、1 行で各 Avamar サーバ ノードの IP アドレスを指定し、そのノードの NIC（ネットワーク インターフェイス カード）の Mac アドレスを含めます。

```
iptables -A INPUT -p udp -s 192.168.1.12 -m mac --mac-source 00:50:8D:FD:E6:32 --dport 514 -j ACCEPT
```

```
iptables -A INPUT -p udp -s 192.168.1.13 -m mac --mac-source 00:50:8D:FD:E6:33 --dport 514 -j ACCEPT
```

```
iptables -A INPUT -p udp -s 192.168.1.14 -m mac --mac-source 00:50:8D:FD:E6:34 --dport 514 -j ACCEPT
```

```
iptables -A INPUT -p udp -s 192.168.1.15 -m mac --mac-source 00:50:8D:FD:E6:35 --dport 514 -j ACCEPT
```

...

クライアント側の送信システムログ トラフィックに対するルールは必要ありません。

2. 変更が有効になるように、リモート ログ ホストのファイアウォール サービスをリスタートします。
3. 変更を有効にするには、次のように、すべてのサーバ ノードおよびリモート ログ ホストで `syslog-ng` サービスをリスタートします。
`service syslog restart`

SNMP を使用したサーバーのモニタリング

SNMP（Simple Network Management Protocol）は、アプリケーション、ハードウェア デバイスまたはソフトウェア アプリケーションおよび任意の数のモニタリング アプリケーションまたはデバイス間のイベント通知情報の通信とモニタリングに使用されるプロトコルです。

注

SNMP 経由でイベント情報を送信できるよう、Avamar サーバを設定する担当者は、基本的な SNMP の概念に精通した人物が望ましいです。基本的な SNMP の概念と実装方法の詳細は、このガイドの範囲外になります。関連情報については、Web サイト www.net-snmp.org を参照してください。

Avamar SNMP 実装では、SNMP リクエストと SNMP トラップを使用して、Avamar サーバ イベントおよびアクティビティ ステータスにアクセスします。Avamar サーバは、SNMP バージョン v1、v2c をサポートします。

SNMP 要求

SNMP 要求には、SNMP 管理アプリケーションがリモートの SNMP 対応アプリケーションまたはデバイス（この場合は Avamar サーバ）から情報を「プル」するためのメカニズムが備わっています。SNMP 管理アプリケーションは、Avamar サーバで実行する SNMP マスター エージェントに要求を送信します。SNMP マスター エージェントは次に、Avamar SNMP サブエージェントと通信します。SNMP サブエージェントは MCS に要求を送信します。MCS はデータを取得し、Avamar SNMP サブエージェントに送信します。SNMP サブエージェントは、SNMP マスター エージェント経由で管理アプリケーションにこれを送信します。データ用ポート 161 は、SNMP 要求のデフォルトのデータ用ポートです。

Avamar から直接購入した Avamar サーバは、Net-SNMP マスター エージェントを使用します。他の業界標準ハードウェアで構築された Avamar サーバの場合は、ハードウェア メーカーが提供する SNMP マスター エージェントを使用します。

SNMP トラップ

SNMP トラップによって、指定された Avamar イベントが発生すると、Avamar サーバが SNMP 管理アプリケーションに情報を「プッシュ」するメカニズムが提供されます。データ用ポート 162 は、

SNMPトラップのデフォルトのデータ用ポートです。通常、SNMP 管理アプリケーションは、指定したリモートホストによって生成された任意のSNMPトラップをリスンしています。

SNMP を使用したサーバーのモニタリングの構成

手順

1. SNMP 管理アプリケーションで Avamar サーバを監視できるようにするには、Avamar MIB (管理情報ベース) 定義ファイル (AVAMAR-MCS-MIB.txt) を、SNMP 管理アプリケーションで使用するマスター MIB にロードします。

MIB には、監視可能な情報や、各 SNMP アプリケーションまたはデバイスに送信されるトラップの定義が含まれます。

次の表では、Avamar MIB 定義ファイルの場所を示しています。

表 82 Avamar MIB 定義ファイルの場所

コンピューターのタイプ	MIB の場所
シングル ノード サーバー	/usr/local/avamar/doc
マルチノード サーバー	/usr/local/avamar/doc on the utility node
Avamar Administrator を備えたコンピューター	install_dir/doc、ここで install_dir は通常、次のとおりです。 <ul style="list-style-type: none"> • Microsoft Windows コンピューターでは C:\Program Files\avs\administrator • Linux コンピューターでは /usr/local/avamar • Solaris コンピューターでは /opt/AVMRcons1

Avamar MIB 定義ファイルのコピーは、シングル ノード サーバとユーティリティ ノードの /usr/share/snmp/mibs ディレクトリにも存在します。このコピーは、Avamar SNMP サブエージェントで使用され、移動や分散されない必要があります。

2. Net-SNMP エージェントを構成します。手順については、[Net-SNMP エージェントの構成 \(244 ページ\)](#) を参照してください。
3. 指定した Avamar サーバ イベントを SNMP トラップに出力するカスタム イベント プロファイルを構成します。手順については、[SNMP トラップ用にカスタム イベント プロファイルを作成する \(246 ページ\)](#) を参照してください。

Net-SNMP エージェントの構成

avsetup_snmp コマンドライン ユーティリティによって、Net-SNMP エージェントを構成し、Avamar SNMP サブ エージェントを使用して、Avamar サーバと通信します。

手順

1. コマンド シェルを開きます。
 - a. サーバーに admin としてログインします。
 - b. 次のコマンドを入力して、ユーザーを root に切り替えます。

```
su -
```

c. グリッドの場合、次のコマンドを入力して、rootid OpenSSH キーをロードします。

```
ssh-agent bashssh-add /root/.ssh/rootid
```

2. 次のコマンドを入力して、このユーティリティを起動します。

```
cd /root/avsetup_snmp
```

出力により、SNMP リクエストをリスンするポートを指定するようにプロンプトで要求されます。

3. 次のように SNMP リクエストのデータ用ポートを選択します。

- デフォルトの SNMP 要求データ用ポート 161 を使用する場合は、[Enter] キーを押します。
- 別の SNMP 要求データ用ポートを使用する場合は、データ用ポート番号を入力し、[Enter] キーを押します。

avsetup_snmp によって SNMP コミュニティを検出できなかった場合は、出力により、SNMPv3 読み取り/書き込みユーザー ベースのアクセスを可能にするかどうかを指定するようにプロンプトで要求されます。

4. 「[n]」と入力し、[Enter] キーを押します。

出力により、SNMPv3 読み取り専用ユーザー ベースのアクセスを可能にするかどうかを指定するようにプロンプトで要求されます。

5. 「[n]」と入力し、[Enter] キーを押します。

出力により、SNMPv1/v2c 読み取り/書き込みのコミュニティ アクセスを可能にするかどうかを指定するようにプロンプトで要求されます。

6. 「[n]」と入力し、[Enter] キーを押します。

出力により、SNMPv1/v2c 読み取り専用のコミュニティ アクセスを可能にするかどうかを指定するようにプロンプトで要求されます。

7. [y] のデフォルト値を受け入れるには、[Enter] キーを押します。

出力により、read-only アクセスを追加するコミュニティの名前を指定するようにプロンプトで要求されます。SNMP コミュニティとは、ローカルの Net-SNMP エージェントが SNMP 管理アプリケーションでエージェント自体を認証するために使用するテキスト文字列です。

8. SNMP コミュニティ名を入力して、[Enter] キーを押します。

出力により、このコミュニティ名を受け入れる元のホスト名またはネットワーク アドレスを指定するようにプロンプトで要求されます。

9. すべてのホスト名またはネットワーク アドレスからコミュニティ名を受け入れるには、[Enter] キーを押します。

出力により、このコミュニティを制限する OID を指定するようにプロンプトで要求されます。

10. 制限は指定しない場合は、[Enter] キーを押します。

出力により、別のコミュニティを構成するかどうかを指定するようにプロンプトで要求されます。

11. 「[n]」と入力し、[Enter] キーを押します。

出力で、/etc/snmp/snmpd.conf が作成および実行され、system_setup グループが構成されたことが通知されます。その後、出力により、システムの場所を指定するようにプロンプトで要求されます。

12. Avamar サーバの物理的な場所を入力し、[Enter] キーを押します。

出力により、担当者情報を指定するようにプロンプトで要求されます。

13. 担当者情報を入力し（例えば、メール アドレス、内線番号など）、**[Enter]** キーを押します。
出力により、`sysServices.0` OID の値を正しく設定するかどうかを指定するようにプロンプトで要求されます。
14. **[[n]]** と入力し、**[Enter]** キーを押します。
出力で、`/etc/snmp/snmpd.conf` がインストールされ、`snmpd` が有効化されたことが通知されます。

SNMP トラップ用にカスタム イベント プロファイルを作成する

SNMP を使用したサーバのモニタリングを構成するプロセスの一環として、カスタム イベント プロファイルを作成し、指定した Avamar サーバ イベントを SNMP トラップに出力します。

デフォルトの Avamar の構成には、**[Local SNMP Trap]** プロファイルが含まれており、これにより Avamar サーバ イベント メッセージがローカルの Net-SNMP トラップ リスナー (`snmptrapd` プロセス) に出力されます。ただし、**Local SNMP Trap** プロファイルを編集できません。このプロファイルはテストの目的に限定して使用され、ローカル `snmptrapd` プロセスがトラップの生成と受信を正常に実行できることを確認します。次にこのプロセスは、トラップ情報をシステムログ ファイルに書き込みます。通常、次のステップは、別のカスタム プロファイルを構成して Avamar SNMP トラップをリモート Net-SNMP トラップ リスナーに送信する操作になります。

手順

1. [カスタム イベント プロファイルの作成](#) (230 ページ) で説明されているステップを使用して、カスタム イベント プロファイルを作成します。
[New Profile] ウィザードの最初のページで、SNMP トラップ通知を有効化するオプションを選択します。
2. **[SNMP Trap Notification]** ページが表示されるまで、ウィザードを続行します。
3. **[SNMP Trap address (IP or hostname)]** ボックスに、SNMP トラップの受信および処理が可能なアプリケーションを備えたコンピューターの IP アドレスまたはホスト名を入力します。
4. **[Port Number]** ボックスに、SNMP トラップをリスンするホストコンピューターのポート番号を入力します。
5. **[SNMP Community]** ボックスに、SNMP トラップ リスナーが使用するように構成されている、SNMP コミュニティの名前を入力します。
6. (オプション) SNMP 通知パラメーターをテストするには、**[Send Test SNMP Trap]** をクリックします。
7. **[Finish]** をクリックします。

Avamar サーバ ログ ファイルの表示

デフォルトでは、Avamar ストレージ プロセスのログ ファイル (`gsan.log`) はサイズが 25 MB に制限され、常に最新の情報を記載しています。追加の履歴ログ ファイル (例: `gsan.log.1`、`gsan.log.2` など) が存在する場合もあります。コマンドライン操作を使用して、これらのログ ファイルを収集および表示することができます。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。

- マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin OpenSSH` キーをロードします。


```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```
- 2. 新しいユーザー定義の一時ディレクトリを作成し、次のコマンドを入力して、ディレクトリをこれに変更します。


```
mkdir directorycd directory
```

 ここで、`directory` はディレクトリ名です。
- 3. 次のコマンドを入力して、ストレージ ノードのログ ファイルのコピーを取得します。


```
getlogs
```

`getlogs` コマンドでは、特定のノードから重要なログ ファイルを収集して、単一の `tar` ファイル (`nodelogs.tgz`) に圧縮します。その後、これらのファイルを現在の作業ディレクトリにある番号付きのサブディレクトリにコピーします。
- 4. `nodelogs.tgz` ファイルを調べ、文字列 `ERROR` を含むすべてのエントリーを探します。これを実施するために、次に示すシェル コマンドを実行し、文字列 `ERROR` を含むすべての `nodelogs.tgz` エントリーをユーザー定義の一時ファイルに書き出します。


```
for p in [01].[!sm]*/nodelogs.tgz; do tar xzf $p | grep ERROR; cur/gsan.log*rm -rf cur/*done
```
- 5. 次のコマンドを入力して、ユーザー定義の一時ディレクトリを削除します。


```
cd ../rm -rf directory
```

監査ログ

監査ログには、ユーザーによって開始されたシステム アクションのログが永続的に保管されます。このログのデータがあれば、`Avamar` を展開して、セキュリティ ポリシーの実行、セキュリティ違反やポリシーからの逸脱の検出を行い、適切なユーザーにこれらのアクションの責任を課することができます。

ユーザーが開始したアクションのみがログに記録されます。スケジュール設定されたバックアップ、メンテナンス アクティビティなどのユーザー アカウントなしでシステムが開始したアクションはログに記録されません。

カテゴリーが `SECURITY`、タイプが `AUDIT` のシステム イベントは、`Avamar` 監査ログ機能を実装するために使用されます。監査ログ エントリーの基本データはシステム イベントなので、この情報は次の 2 か所で取得できます。

- Event Monitor (他のすべてのシステム イベントも含む)
- Audit Log (監査ログ エントリーでもあるイベントのみ含む)

デフォルトでは、監査ログ情報は 1 年間保持されます。

監査ログの保存期間を延長または短縮するには、`/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml` で `clean_db_audits_days` の値を編集して、`MCS` を再起動します。

監査ログの表示

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[Event Management]** タブをクリックします。
3. ウィンドウの下部にある **[Audit Log]** タブをクリックします。
[Audit Log] の各列の詳細については、Avamar Administrator のオンライン ヘルプを参照してください。
4. **[Audit Log]** の表示モードを次のように選択します。
 - 定義した日付範囲の最新の 5,000 件の監査ログ エントリーを表示するには、**[Query]** を選択します。
 - 過去 24 時間の最新の 5,000 件の監査ログ エントリーを表示するには、**[Monitor]** を選択します。
5. (オプション) 次の手順に従って、**[Audit Log]** で表示されるエントリーをフィルターします。
 - a. **[Actions]** メニューを開いて、**[Event Management]** > **[Filter]** を選択します。
[Filter] ダイアログ ボックスが表示されます。
 - b. **[Audit Log]** で **[Query]** 表示モードを選択した場合は、**[From Date]** および **[To Date]** フィールドを使用して、表示するエントリーの日付範囲を選択します。
 - c. **[Severity]** リストから、表示するログ エントリーの重大度を選択します。
 - d. すべてのドメインのログ エントリーを表示するには、**[All Domains]** を選択します。または、特定のドメインのエントリーを表示するには、**[Domain]** を選択して、ドメイン名を参照または入力します。
 - e. 監査ログ エントリー データの XML 要素で特定のキーワード（大文字と小文字を区別）を含むログ エントリーのみを表示するには、**[Data]** ボックスにキーワードを入力します。
 この基準により、ログ エントリー属性全体を重要なキーワードで容易にフィルター処理できるようになります。例えば、ログを `error` でフィルターすると、任意の XML 属性（例えば、カテゴリ、タイプ、重大度）に `error` という文字を含むすべてのログ エントリーが返されます。
 - f. 詳細なフィルター基準を表示するには、**[More]** をクリックします。
 - g. 特定のイベントコードを持つイベントのみに **[Audit Log]** を制限するには、**[Only include codes]** を選択して、リストでコードの追加および削除を行います。または、特定のイベントコードを持つイベントを監査ログから除外するには、**[Exclude codes]** を選択して、リストからコードの追加および削除を行います。
 - h. **[OK]** をクリックします。

Avamar サポートへの自動通知

Email Home と ConnectEMC の機能により、Avamar カスタマー サポートに通知が自動的に送信されます。これらの通知には、高い優先度のイベントのアラートや、日次レポートなどが含まれ、Avamar サーバの監視を容易にします。

Integrated Data Protection Appliance など、ソリューションの一部に Avamar サーバが含まれている環境では、自動通知にはそのソリューションのタイプやその他の関連する詳細情報が含まれま

す。この情報により、アラートのための適切なルーティングが確保され、保守性が向上するとともに、お客様のアクションが不要になります。

使用状況インテリジェンス

使用状況インテリジェンスは、Avamar サーバで自動的にレポート作成情報を収集し、Avamar サポートに転送できるようにする機能です。Avamar サポートに送信されるレポートのタイプは、Avamar サーバのライセンス取得方法によって異なります。

この機能を使用する要件は、次のとおりです。

- ESRS Gateway がローカル環境にインストールされ導入されている。
- ESRS で登録を許可するための認証情報がある。

ESRS ライセンスのインストールとアクティブ化

ESRS で Avamar を使用するには、ESRS ライセンスが含まれる Avamar ライセンス キー ファイルが必要です。

Avamar ライセンス キー ファイルをインストールしアクティブ化する方法の詳細については、[ライセンスのインストールとアクティブ化](#) (194 ページ) を参照してください。

ESRS Gateway 証明書の Avamar サーバのキーストアへのインポート

Avamar サーバを ESRS Gateway に登録する前に、ESRS Gateway の証明書を Avamar サーバのキーストアにインポートする必要があります。

手順

1. ESRS Gateway の証明書を、次のようにエクスポートします。
 - a. ブラウザで `https://esrs_gateway:9443` を参照します。

ここで、`esrs_gateway` はローカルの ESRS Gateway のホスト名または IP アドレスです。
 - b. ブラウザの機能を使用して、証明書をエクスポートします。

例えば、Internet Explorer 11 の場合は以下のように実行します。

 - a. [URL] フィールドでロック アイコンをクリックし、[View Certificates] を選択します。
 - b. [詳細] タブをクリックしてください。
 - c. [Copy to File] をクリックし、[Certificate Export Wizard] の手順を実行します。
2. エクスポートされた証明書を、Avamar サーバの一時的な場所にコピーします。
3. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバには、`admin` としてサーバにログインします。
 - マルチ ノード サーバの場合、`admin` としてユーティリティ ノードにログインします。
4. 次のコマンドを入力して、ユーザーを `root` に切り替えます。

```
su -
```

5. 1 行に次のコマンドを入力して、キーストアをバックアップします。

```
cp -p /usr/local/avamar/lib/rmi_ssl_keystore /usr/local/avamar/lib/rmi_ssl_keystore.bak
```

- 1 行に次のコマンドを入力して、キーストアに ESRS サーバ証明書をインポートします。

```
keytool -importcert -keystore /usr/local/avamar/lib/  
rmi_ssl_keystore -storepass changeme -file <certfile>.crt
```

ここで<certfile>は、パスを含む ESRS サーバ証明書の名前です。

- 次のコマンドを入力して、MCS を再開します。

```
mcsserver.sh --restart
```

ESRS への Avamar の登録

使用状況インテリジェンス機能を有効にするには、ESRS（EMC Secure Remote Support）に Avamar サーバを登録する必要があります。

手順

- Avamar Administrator で、[Tools] > [Manage ESRS] を選択します。
[Edit ESRS Gateway Information] ウィンドウが表示されます。
- [ESRS Gateway] フィールドに ESRS Gateway の IP アドレスを入力します。
- [Port] フィールドに、ESRS Gateway のポート番号を入力します。
- Dell EMC サポートの認証情報のユーザー名とパスワードを入力します。
- [Register] をクリックします。
- メッセージ ウィンドウに登録が成功したことが示されます。[OK] をクリックしてこのウィンドウを閉じます

結果

ESRS Gateway に Avamar サーバが登録されると、使用状況インテリジェンス機能の詳細な構成は必要ありません。

E メール ホーム

Avamar Email Home 機能では、構成、容量、全般的なシステムに関する情報を 1 日 1 回 Avamar サポートに自動的に送信し、必要に応じて、ほぼリアルタイムに重要なアラートを提供します。

デフォルトでは、通知スケジュールのメール メッセージは毎日午前 6 時と午後 3 時に送信されません。通知スケジュールでは、これらのメッセージが送信されるタイミングを制御します。

Email Home メール設定の編集

Email Home の構成および有効化は、Avamar サーバのインストール時に行います。インストール後に Email Home のメール設定を編集することが可能です。

手順

- コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバには、admin としてサーバにログインします。
 - マルチ ノード サーバには、
 - admin としてユーティリティ ノードにログインします。
 - 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. 次のコマンドを入力して、ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```

3. UNIX テキスト エディターで `mcserver.xml` を開きます。

4. `com.avamar.asn.module.mail` ノードを見つけます。

`com.avamar.asn.module.mail` ノードには、`smtpHost` および `admin_mail_sender_address` のエントリーが含まれます。

5. `smtpHost` エントリーの値が、`smtp.example.com` などの、**Email Home** メッセージを送信するために使用される送信 SMTP メール サーバーの DNS 名であることを確認します。

このエントリーの値が不正確な場合は、この値を編集します。

通知

Avamar サーバー インストールまたはアップグレードでは、`smtpHost` エントリーの値が自動的に入力されます。ほとんどの場合、Avamar サーバから発信されるメール メッセージをインターネットを介して、送信 SMTP メール サーバから Avamar サポートに送信するには、準備が必要です。

6. `admin_mail_sender_address` エントリーの値として、企業の送信 SMTP メール サーバーにアクセスできる有効なメール アドレスを指定します。

通知

有効なメール アドレスからメッセージを送信できるように [Email Home] 機能を構成していない場合、[Email Home] 機能で生成されたメッセージは受信メール サーバで拒否されます。Avamar サポートは、プログラムで生成されたこれらのメッセージが拒否されたことをまったく認識できません。さらに、有効な送信メール アカウントが不明なため、これらのメッセージが送信されなかったことを示す送信者への警告は、問題を修正できる人には表示されません。

7. 変更を保存して、ファイルを閉じます。
8. 次のコマンドを入力して、MCS を再開します。

```
dpnctl stop mcspdncctl start
```

9. コマンド シェルを閉じます。

ConnectEMC

ConnectEMC は、Avamar サーバ上で実行され、情報を Avamar サポートに送信するプログラムです。ConnectEMC は、通常、優先度の高いイベントが発生したときにアラートを送信し、また、1 日 1 回レポートを送信するように構成されています。

ConnectEMC は、ESRS (EMC Secure Remote Support) と統合されています。ただし、ESRS がインストールされ、動作可能で、Avamar サーバがネットワークを通じてアクセス可能であることが条件です。ESRS の導入の詳細については、Avamar 担当営業にお問い合わせください。

ConnectEMC は、Avamar サーバ ソフトウェアのインストール時に初期構成されますが、Avamar Administrator を使用すると、ユーザーが構成可能な次の 3 種類の転送形式で、サーバの動作後も ConnectEMC 設定を管理できます。

- プライマリ転送
- フェイルオーバー転送
- 通知転送

プライマリ転送とフェイルオーバー転送では、高い優先度のイベントが発生すると、アラートを送信します。プライマリ転送が使用され、これに失敗した場合はフェイルオーバー転送が使用されます。

通知転送は、一定の条件の下で、メール通知メッセージを1つまたは複数のお客様のメールアドレスに送信します。

また、MCS によって ConnectEMC メッセージを生成および送信するかを制御するには、ConnectEMC の有効化、無効化、停止、開始を実行します。

ConnectEMC の有効化/無効化

ConnectEMC を無効化すると、ConnectEMC が再度有効化されるまで、MCS は ConnectEMC メッセージの生成を停止します。MCS によって、ConnectEMC メッセージの生成を継続しながらも、メッセージをキューイングすることを可能にするには、ConnectEMC を停止します。

手順

1. Avamar Administrator で、[Tools] > [Manage ConnectEMC] を選択します。
[Manage ConnectEMC] ウィンドウが表示されます。
2. MCS によって ConnectEMC メッセージを生成および送信するかどうかを、次のように指定します。
 - MCS によるメッセージの生成を停止するには、[Disable] をクリックします。
 - メッセージの生成を再開するには、[Enable] をクリックします。
 - メッセージの生成を継続しながらも、メッセージをキューイングするには、[Stop] をクリックします。
 - メッセージの送信を開始するには、[Start] をクリックします。

ConnectEMC を無効化する場合は、プロンプトでパスワードを入力するように指示されます。

3. 有効なパスワードを入力し、[OK] をクリックします。

プライマリ転送およびフェイルオーバー転送の編集

手順

1. Avamar Administrator で、[Tools] > [Manage ConnectEMC] を選択します。
[Manage ConnectEMC] ウィンドウが表示されます。
2. 左のパネルで [Primary Transport] または [Failover Transport] を選択して、[Edit] をクリックします。
[Edit Primary/Secondary Transport] ダイアログ ボックスが表示されます。
3. [Transport Type] リストから転送タイプを選択します。
 - [Email]
 - [FTP]
 - [HTTPS]

注

FTP または HTTPS 転送タイプを使用するには、動作可能なセキュア リモート サポート ゲートウェイが必要です。

4. (メール専用) **[Email]** を選択した後で、次のステップを完了します。
 - a. **[SMTP Host (Email Server)]** フィールドに、メール サーバーのホスト名または IPv4 アドレスを入力します。
 - b. **[Email Address]** フィールドに、これらのメール メッセージの受信者を 1 人以上入力します。E メール アドレスが複数ある場合はコンマで区切って列挙します。
 - c. **[Email Sender Address]** フィールドで、メッセージの送信元のメール アドレスを指定します。
 - d. (オプション) 詳細設定を構成するには、**[Advanced]** をクリックして、**[Edit Advanced Email Settings]** ダイアログ ボックスで次の設定を指定します。
 - **[Retries]** : 失敗をレポートする前に再試行する回数。デフォルト設定は 5 回です。
 - **[Timeout]** : 操作タイムアウトをレポートする前に待機する秒数。デフォルト設定は 5 分 (300 秒) です。
 - **[Description]** : **[Manage ConnectEMC]** ウィンドウに表示されるこの転送の説明。デフォルトの説明は Email Transport です。
 - **[Email Subject]** : メール の 件 名。デフォルトの件名は Avamar ConnectEMC Notification Email です。

Avamar サポートの指示がない限り、メールの件名を変更しないでください。Avamar スпам フィルターでは、他の件名になっているメール メッセージを拒否できます。
 - e. **[OK]** をクリックします。
5. (FTP 専用) **[FTP]** を選択した後で、次のステップを完了します。
 - a. **[IP Address]** フィールドに、IPv4 アドレスを入力します。
 - b. **[Username]** フィールドに、FTP ユーザ名を入力します。設定は、FTP サーバー ソフトウェアによって異なります。
 - c. **[Password]** フィールドにユーザ名のパスワードを入力します。
 - d. (オプション) 詳細設定を構成するには、**[Advanced]** をクリックして、**[Edit Advanced FTP Settings]** ダイアログ ボックスで次の設定を指定します。
 - **[Retries]** : 失敗をレポートする前に再試行する回数。デフォルト設定は 5 回です。
 - **[Timeout]** : 操作タイムアウトをレポートする前に待機する秒数。デフォルト設定は 5 分 (300 秒) です。
 - **[Description]** : **[Manage ConnectEMC]** ウィンドウに表示されるこの転送の説明。デフォルトの説明は FTP Transport です。
 - **[FEP Folder]** : 「ConnectEMC FEP (Front End Processor)」の一意的のカスタマー UNIX パス。Avamar サポートによって提供されるフォルダーの場所を使用します。
 - **[FTP Port]** : IP ポート。デフォルト設定はポート 21 です。

- **[Mode]** : **[Active]**、**[Passive]** のいずれか。デフォルト設定は **[Active]** です。
Avamar サポートの指示がない限り、メールの件名を変更しないでください。Avamar スпам フィルターでは、他の件名になっているメール メッセージを拒否できます。
- e. **[OK]** をクリックします。
6. (HTTPS 専用) **[HTTPS]** を選択した後で、次のステップを完了します。
- a. **[URL]** フィールドに、Secure Remote Support ホーム ページの有効な URL を入力します。
有効な URL では次の形式を使用します。
`https://home_name[:port]/target_directory`
ここで、**home_name**、**port**、**target_directory** はそれぞれホーム名、データ用ポート、ターゲット ディレクトリです。
Avamar サポートによって提供された URL を使用します。
- b. (オプション) 詳細設定を構成するには、**[Advanced]** をクリックして、**[Edit Advanced HTTPS Settings]** ダイアログ ボックスで次の設定を指定します。
- **[Retries]** : 失敗をレポートする前に再試行する回数。デフォルト設定は 5 回です。
 - **[Timeout]** : 操作タイムアウトをレポートする前に待機する秒数。デフォルト設定は 5 分 (300 秒) です。
 - **[Private Key Pass Phrase]** : プライベート キー ファイルに関連づけられたパスワード。
 - **[Private Key File]** : プライベート キー ファイルのファイル名。
 - **[Client Certificate]** : 使用するクライアント証明書。デフォルト設定は、「Default」で、これは MCS が使用する証明書を使用します。それ以外は、クライアント証明書のファイル名を入力してください。
 - **[Server CA Bundle]** : root 証明書のリストを含むファイル。
 - **[Verify Server Name]** : サーバー名を確認するかどうか。[Yes] または [No] のいずれかです。デフォルトの設定は [No] です。
- c. **[OK]** をクリックします。
- サンプル キー ファイルは、`/opt/connectemc/certs/および https-privatekey.pem` で提供されています。サンプル クライアント証明書は、`/opt/connectemc/certs/および https-cert.pem` で提供されています。サンプル root 証明書バンドルは、`/opt/connectemc/certs/および https-ca-cert.pem` で提供されています。
7. **[Edit Primary/Secondary Transport]** ダイアログ ボックスで **[OK]** をクリックします。

通知転送の編集

手順

1. Avamar Administrator で、**[Tools]** > **[Manage ConnectEMC]** を選択します。
[Manage ConnectEMC] ウィンドウが表示されます。
2. **[Notification Transport]** を選択し、**[Edit]** をクリックします。
[Edit Notification Transport] ダイアログ ボックスが表示されます。

3. **[Notification Type]** リストから、次のいずれかのタイプを選択します。
 - **[On Success]** : イベント ファイルが EMC に正常に転送されたときに受信者に通知します。
 - **[On Failure]** : イベント ファイルが EMC に正常に転送されなかったときに受信者に通知します。
 - **[On Success or Failure]** : 結果にかかわらず、イベント ファイルを EMC に転送しようと試行したときに受信者に通知します。
 - **[On All Failure]** : イベント ファイルを EMC に転送しようとした試行がすべて失敗したときに受信者に通知します。
4. **[SMTP Host (Email Server)]** ボックスに、メール サーバーのホスト名または IPv4 アドレスを入力します。
5. **[Email Address]** ボックスに、これらのメール メッセージの受信者を 1 人以上入力します。E メール アドレスが複数ある場合はコンマで区切って列挙します。
6. **[Email Sender Address]** ボックスに、通知の送信元のメール アドレスを入力します。
7. (オプション) 詳細設定を指定するには、**[Advanced]** をクリックして、**[Edit Advanced Email Settings]** ダイアログ ボックスで次の設定を指定します。
 - a. **[Retries]** ボックスで、失敗をレポートする前に再試行を行う回数を指定します。デフォルト設定は 5 回です。
 - b. **[Timeout]** ボックスで、操作タイムアウトをレポートする前に待機する秒数を指定します。デフォルト設定は 300 秒 (5 分) です。
 - c. **[Description]** ボックスで、**[Manage ConnectEMC]** ウィンドウに表示されるこの転送の説明を指定します。デフォルトの説明は Email Transport です。
 - d. **[Email Subject]** ボックスで、メールの件名を指定します。デフォルトの件名は Avamar ConnectEMC Notification Email です。

通知

Avamar サポートの指示がない限り、メールの件名を変更しないでください。EMC スパムフィルターでは、他の件名になっているメール メッセージを拒否できます。

- e. **[Email Format]** リストで、メールの形式を ASCII または HTML のいずれかから選択します。デフォルト設定は [ASCII] です。
 - f. 通知メール メッセージに添付ファイルを使用して ConnectEMC に送信するかどうかを選択するには、**[Include CallHome Data]** チェックボックスを選択または選択解除します。
 - g. **[OK]** をクリックします。
8. **[Edit Notification Transport]** ダイアログ ボックスで、**[OK]** をクリックします。

サイト名の編集

手順

1. コマンド シェルを開きます。
 - a. サーバーに admin としてログインします。
 - b. 次のように入力して、ユーザーを root に切り換えます。

```
su -
```

2. 次のコマンドを入力して、ユーティリティを起動し、サイト名を切り替えます。

```
cd /root
```

```
avsetup_connectemc.pl --site_name=site_name
```

site_name はお客様のサイトの名前です。

3. ConnectEMC を無効化してから有効化します。
詳細については、[ConnectEMC の有効化/無効化](#)を参照してください。
4. MCS を再起動します。
詳細については、[MCS の起動](#)を参照してください。

トランスポートのテスト

手順

1. Avamar Administrator で、[Tools] > [Manage ConnectEMC] を選択します。
[Manage ConnectEMC] ウィンドウが表示されます。
2. [テスト] をクリックします。

サイト名の編集

手順

1. コマンド シェルを開きます。
 - a. サーバーに admin としてログインします。
 - b. 次のように入力して、ユーザーを root に切り換えます。

```
su -
```
2. 次のコマンドを入力して、ユーティリティを起動し、サイト名を切り替えます。

```
cd /root
```

```
avsetup_connectemc.pl --site_name=site_name
```

site_name はお客様のサイトの名前です。
3. ConnectEMC を無効化してから有効化します。
詳細については、[ConnectEMC の有効化/無効化](#)を参照してください。
4. MCS を再起動します。
詳細については、[MCS の起動](#)を参照してください。

システムの整合性の検証

Avamar サーバの整合性を検証するには、まず、検証されたチェックポイントが存在することを確認する必要があります。

また、チェックポイントが実行されてから、エラーが発生していないことを確認するため、サーバー ログ ファイルを収集し、確認することもできます。手順については、[Avamar サーバ ログ ファイルの表示](#) (246 ページ) を参照してください。

手順

1. Avamar Administrator で、**[Server]** 起動リンクをクリックします。
[Server] ウィンドウが表示されます。
2. **[Server Management]** タブをクリックします。
3. 左のパネルで Avamar サーバ名を選択します。
4. **[Last validated checkpoint]** フィールドに、最新の日付が表示されていることを確認します。

第 10 章

容量管理

本章は、次のトピックで構成されています。

- [容量使用率の情報](#).....260
- [容量の制限と閾値](#).....260
- [容量フォーキャスト](#).....261
- [容量制限と動作のカスタマイズ](#).....261

容量使用率の情報

リアルタイムの容量使用率情報を表示するには、単一のサーバーの場合は Avamar Administrator、複数のサーバーの場合は Backup & Recovery Manager を使用します。

Avamar Administrator では、Avamar Administrator ダッシュボードの [Capacity] パネルと、[Server] ウィンドウの [Server Management] タブで、単一の Avamar サーバの容量使用率情報を表示します。

複数のサーバの容量使用率情報は Backup & Recovery Manager で入手します。この機能の詳細については、Backup & Recovery Manager 製品ドキュメントを参照してください。

容量の制限と閾値

次の表では、Avamar サーバがさまざまな消費ストレージ閾値を超えた場合の動作について説明します。

表 83 容量の制限と閾値







ストレージ使用率	ステータス	説明
75%未満		システムには、今後実行するバックアップを保存するために適切な容量があります。
75%		サーバー ストレージ使用率を調査して、今後実行するバックアップを格納するために適切な容量がサーバーにあるかどうかを確認してください。
80%		ポップアップ通知によって、利用可能なストレージ容量の 80%がサーバーによって消費されたことが警告されます。サーバー ストレージ使用率を調査して、今後実行するバックアップを格納するために適切な容量がサーバーにあるかどうかを確認してください。
90%		サーバー ストレージ使用率を調査して、今後実行するバックアップを格納するために適切な容量がサーバーにあるかどうかを確認してください。
95%		サーバーがデフォルトのヘルス チェック制限に達しています。これは、サーバーが依然として「正常稼働」できる利用可能なストレージ容量です。Avamar は進行中のバックアップをすべて完了しますが、ディスパッチャーは新しいバックアップ アクティビティを停止します。Avamar

表 83 容量の制限と閾値 (続き)

ストレージ使用率	ステータス	説明
		Administrator にログインすると、通知が表示されます。あとでバックアップ アクティビティを再開するには、システム イベントを確認します。ヘルス チェック制限はカスタマイズできますが、95%よりも高い上限は推奨されません。手順については、 容量制限と動作のカスタマイズ (261 ページ) を参照してください。
100%		サーバーは読み取り専用制限に達しており、サーバーにすでに格納されたデータの整合性を確保するために、自動的に読み取り専用に変更されました。ConnectEMC が有効になっている場合、SR (サービス リクエスト) がログに記録されます。システムの既存の SR を表示するには、Avamar サポート Web サイトにアクセスして、ナレッジベース KB000472030 「Avamar Capacity Troubleshooting, Issues and Questions - All Capacity (Resolution Path)」を検索します。

容量フォーキャスト

すべての Avamar サーバはストレージ容量の消費レートを継続的に追跡、分析し、そのレートでストレージ容量を継続して消費できる期間を予測します。この予測処理はバックグラウンドで実行されます。

Avamar サーバと構成済みの Data Domain システムの容量予測の結果は、Avamar Administrator の [Capacity] パネルで確認できます。詳細については、[\[Capacity\] パネル](#) (47 ページ) を参照してください。

容量制限と動作のカスタマイズ

容量制限とシステムの動作を制御する設定をカスタマイズするには、Avamar Administrator の選択ファイルを編集します。

Avamar Administrator の容量設定の編集

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。

- シングル ノード サーバーには、**admin** としてサーバーにログインします。
- マルチ ノード サーバには、
 - a. **admin** としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、**admin OpenSSH** キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. 次のコマンドを入力して、MCS (Management Console Server) をシャットダウンします。

```
dpnctl stop mcs
```

3. 次のコマンドを入力して、ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```

4. テキスト エディターで `mcservers.xml` を開きます。
5. プリファレンス ファイルの `com.avamar.mc.mcs` セクションを見つけます。
6. 次の設定を編集します。

表 84 mcservers.xml での容量設定

設定	説明	デフォルト値
capErrPercent	容量使用率がこのパーセンテージに達すると、容量状態アイコンが赤色になります。	95%
capForecastDataDays	予測に使用する容量使用率データ履歴の量。	30 日
capForecastDataMinDays	予測に必要な容量使用率データ履歴の最小量。	14 日
capForecastReachedDays	予測容量がここで指定した日数を下回った場合、Avamar Administrator によって、確認を要求するイベントの生成と、ログイン時のポップアップ アラートの表示が開始されます。	30 日
capMonitorIntervalMin	この設定では、Avamar Administrator によって予測容量が確認される頻度を制御します。	1 日 (毎日)
capReachedPercentage	合計の容量使用率がこのパーセンテージ閾値に達すると、Avamar Administrator プロセスはシステムが一杯であることを通知するイベント通知を生成します。	95%
capWarnPercent	容量使用率がこのパーセンテージに達すると、容量状態アイコンが黄色になります。	80%
hcMonitorIntervalMin	この設定では、Avamar Administrator によってヘルス チェック (消費された容量がヘルス チェ	1 日 (毎日)

表 84 mcserver.xml での容量設定 (続き)

設定	説明	デフォルト値
	ック制限に達したかどうかを確認すること) が実行される頻度を制御します。	
hcOffsetROPercentage	サーバー読み取り専用制限 (100%) からこのパーセンテージを引くと、ヘルス チェック制限の値になります。	5%
hcReminderIntervalMin	この設定では、ヘルス チェック制限に達した後、Avamar Administrator によってイベントとポップアップ アラートが発行される頻度を制御します。	60 分 (毎時)

7. 変更を保存して、ファイルを閉じます。
8. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```


第 11 章

レプリケーション

本章は、次のトピックで構成されています。

- [Avamar レプリケーションの概要](#)..... 266
- [Replicas at Source の有効化](#)..... 272
- [ポリシー ベースのレプリケーションの構成](#)..... 273
- [AUI でのオン デマンドレプリケーションの実行](#)..... 282
- [コマンド ラインレプリケーションの実行](#)..... 283
- [レプリケーションのモニタリング](#)..... 295
- [AUI でのレプリケーション タスクのキャンセル](#)..... 295
- [ターゲット システム上のレプリカからバックアップをリストアする](#)..... 296
- [Replicas at Source をサポートする MCS 構成パラメーター](#)..... 297

Avamar レプリケーションの概要

Avamar レプリケーション ジョブでは、ソース Avamar システムから代替ターゲットにクライアント バックアップをコピーします。

バックアップを代替ターゲットにレプリケーションすることにより、ソース Avamar システムに障害が発生した場合にデータロスから保護します。

レプリケーションのタイプ

Avamar では、ポリシー ベースのレプリケーションとコマンドライン レプリケーションを実行するオプションを提供しています。

AUI でのポリシー ベースのレプリケーション

ポリシー ベースのレプリケーションでは、レプリケーション プロセスの優れた制御が可能です。ポリシー ベースのレプリケーションでは、AUI で次に挙げるレプリケーション設定を定義する [レプリケーション グループ] を作成できます。

- レプリケーション グループ メンバー、ドメインまたはクライアント
- レプリケーション タスクの優先度の順位
- レプリケートするバックアップ（保存設定またはバックアップ日に基づく）
- 各クライアントでレプリケートできるバックアップの最大数
- レプリカのターゲット システム
- レプリケーション スケジュール
- レプリカの保存

CLI でのコマンドライン レプリケーション

コマンドラインでオン デマンドのレプリケーションを実行するには、ユーティリティ ノードにログインして、`avrepl` CLI（コマンドライン インターフェイス）を使用します。コマンドライン レプリケーションでは、レプリケーション プロセスの優れた制御が可能です。`avrepl` コマンドのオプションでは、次のレプリケーション設定を定義します。

- レプリケートする対象のドメインまたはクライアント
- レプリケートするバックアップ。次の設定に基づきます。
 - バックアップに使用されるプラグ イン
 - バックアップの保存設定
 - バックアップ日
- 各クライアントでレプリケートできるバックアップの最大数
- レプリカのターゲット システム
- レプリカの保存

レプリケーションのスケジュール設定

レプリケーション タスクのスケジュール方法は、使用するレプリケーションのタイプによって異なります。ポリシー ベースのレプリケーションでは、バックアップ スケジュールの定義方法と同じようにスケジュールを定義します。ユーティリティ ノードで `avrepl` コマンドを実行して手動でレプリケーション タスクを開始するため、コマンドライン レプリケーションでは、スケジュールを定義しません。

AUI でポリシー ベースのレプリケーションのスケジュールを定義する

AUI でポリシー ベースのレプリケーションのスケジュールを設定するには、次のようにします。

1. 左側のナビゲーション ペインで、[>>] をクリックします。
2. [Administration] > [Settings] をクリックし、ドメインを選択します。
3. [Schedules] タブをクリックしてから [+ ADD] をクリックします。

日次、週次、月次のインターバルでレプリケーション タスクを自動的に開始するために、このウィンドウからスケジュールを定義します。また、自動的に実行されないアドホック（オン デマンド）のスケジュールも使用できます。

このスケジュールでは、レプリケーション ウィンドウを設定するために、開始時刻と終了時刻を指定します。

タイムゾーンに関する考慮事項

AUI を使用してレプリケーション タスクをスケジュール設定する場合、AUI Web ブラウザーを実行しているシステムのタイムゾーンでの開始時刻が表示されることに注意してください。開始時刻は、ソースシステムのタイムゾーンおよびターゲットシステムのタイムゾーンでは表示されません。

例えば、太平洋標準時のタイムゾーンにある AUI Web ブラウザーを、東部標準時のタイムゾーンにあるソースシステムとともに使用する場合を考えます。ソースシステムは、2つのタイムゾーン間の3時間の時差を補正します。午後8時と太平洋標準時での開始時刻が AUI で指定されている場合、ソースシステムでは東部標準時の午後11時にレプリケーション タスクが開始されることとなります。

レプリケーションのスケジュール設定のベストプラクティス

各レプリケーション セッションで、より多くのクライアント バックアップが正常にレプリケートされるように、バックアップ アクティビティが少ない時間帯に、レプリケーション タスクをスケジュール設定するようにしてください。スケジュールを設定するときは、完了したクライアント バックアップのみがレプリケートされるという事実も考慮してください。

ポリシー ベースのレプリケーションでは、スケジュール設定された各レプリケーション タスクの実行中にすべてのバックアップが正常にレプリケートされるように、各レプリケーション グループのサイズを考慮してください。グループが非常に大きくなって、一部のバックアップのレプリケーションが正常に完了しなくなったら、スケジュールを編集して時間を長くしたり、別々に実行される小さなグループに分割したりします。

レプリケーション認証

ポリシー ベースのレプリケーションを構成する場合、レプリケーション ポリシーを構成するときに、ターゲットシステムのみアカウントの有効な認証情報を指定します。一方、CLI ベースのレプリケーションでは、ソース Avamar システムとターゲットシステムの有効な認証情報をコマンド プロンプトで指定する必要があります。

AUI でのポリシー ベースのレプリケーションでは、[Add New Replication Destination] ウィザードを使用してターゲットシステムを追加する際に認証情報を指定します。

1. 左側のナビゲーション ペインで、[>>] をクリックします。
2. [Administration] > [System] に移動します。
3. [Replication Destination] タブをクリックして、[+ Add] をクリックします。

CLI レプリケーションでは、コマンド プロンプトで `--[replscript]dstid` および `--dstpassword` オプションを使用して、ターゲットシステムのユーザー アカウントとパスワードを指定します。ソースシステムのユーザー アカウントとパスワードを指定するには、`--[avatar]id` および `--password` オプションを使用します。

ソース Avamar システムでは、`repluser` アカウントがレプリケーションのデフォルトのアカウントです。コマンドライン レプリケーションで `repluser` アカウントを使用する際は、コマンドから `--[avatar]id` オプションを省略して、`--password` オプションで `repluser` アカウントのパスワード

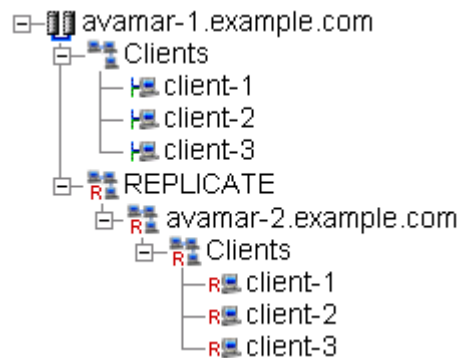
ドを指定します。Avamar システムのデフォルトのアカウントとパスワードの完全なリストについては、「Avamar 製品セキュリティ ガイド」を参照してください。

ターゲット Avamar システムのレプリカの場合

ターゲット Avamar システムでは、レプリカは REPLICATE ドメインにあります。このドメインには、ソース Avamar システムのクライアント階層を複製したツリーが含まれています。

次の図では、avamar-1.example.com ターゲット Avamar システムに、ローカル クライアントと、avamar-2.example.com ソース サーバからのレプリカが両方とも含まれています。

図 15 レプリケーションドメイン構造の例



REPLICATE ドメイン内のデータはすべて読み取り専用です。REPLICATE ドメインのレプリカでは、次の操作のみを実行できます。

- レプリカの有効期限の変更
- バックアップ統計の表示
- レプリカの削除

[Replicas at Source \(268 ページ\)](#) では、Replicas at Source 機能について説明します。この機能は、ターゲットシステムの REPLICATE ドメインではなく、レプリケーション ソース Avamar サーバでレプリカを管理できます。

Replicas at Source

Replicas at Source を使用している場合、レプリケーション ソースになる Avamar サーバで Avamar Administrator セッションを使用して、レプリカの表示と管理を行います。

機能

Replicas at Source 機能は、Avamar サーババージョン 7.2 以降に備わっています。[Replicas at Source の有効化 \(272 ページ\)](#) では、この機能を有効化する方法について説明します。

次の表では、ソース Avamar サーバで Replicas at Source が提供する機能について説明します。

表 85 ソース Avamar サーバで使用できる Replicas at Source 機能

機能	説明
Restore タブでのレプリカの表示	レプリカは、Avamar Administrator にある [Backup, Restore and Manage] ウィンドウの [Restore] タブにバックアップとともに表示されます。

表 85 ソース Avamar サーバで使用できる Replicas at Source 機能（続き）

機能	説明
レプリカ設定の管理	Avamar Administrator または CLI を使用して、レプリカで次のアクションを実行します。 <ul style="list-style-type: none"> 有効期限の変更 保存期間の変更 Delete 確認 統計の表示
レプリカからのリストア	バックアップに適用できる同じ方法で、レプリカを選択してリストアします。
定期的な同期化	ソース Avamar システムは、アクティブな各ターゲットシステムと定期的に同期化します。デフォルトの同期間隔は 12 時間です。しばらくの間、最新の変更が反映されない可能性があります。この同期化には、次のアクションがあります。 <ul style="list-style-type: none"> 有効期限設定の変更の適用 保存設定の変更の適用 ローカル リストの削除（レプリカがリモートターゲットに存在しない場合） ローカル リストの追加（リストにないレプリカがリモートターゲットで見つかった場合）

注

Replicas at Source は、仮想マシン バックアップのレプリカをサポートしません。

統合

一部の Avamar タスクは Replicas at Source を統合します。これらのタスクについて説明するセクションには、Replicas at Source 機能の統合に関する情報があります。次の表に、Replicas at Source の統合について概要を示します。

表 86 Replicas at Source と Avamar タスクの統合に関する説明

タスク	説明
リモート ターゲット管理	ソース Avamar サーバからのレプリカがターゲットシステムに存在している場合、ソース Avamar サーバからのリモート ターゲット リストの削除を防止します。ターゲットシステムからのリモート ターゲット リストの削除とソース サーバの全レプリカの削除を強制するオーバーライド オプションを含めます。
リストア	レプリカは、Avamar Administrator にある [Backup, Restore and Manage] ウィンドウの [Restore] タブにバックアップとともに一覧表示されます。バックアップがソース Avamar システムに存

表 86 Replicas at Source と Avamar タスクの統合に関する説明（続き）

タスク	説明
	在しており、レプリカがリモートターゲットシステムに存在している場合、Avamar システムはリストアにバックアップを使用します。
クライアントの破棄	クライアントを廃棄する場合、Replicas at Source はレプリカの保存と有効期限に関する追加の選択肢を表示します。
クライアントの削除	クライアントを削除する場合、Replicas at Source は、クライアントのレプリカを削除するオプションも表示します。
サービス管理	Avamar Administrator で [Administration] ウィンドウの [Services Administration] タブに、外部バックアップ マネージャー サービスを追加します。このサービスには、標準的なサービス アクションが含まれています。Start、Stop、Restart、View Properties を使用できます。外部バックアップ マネージャー サービスを停止すると、Avamar Administrator は Replicas at Source によるレプリカの管理を停止します。
MCS	Replicas at Source は、カスタマイズ可能な設定を mcserver.xml に追加します。
MCCLI	Replicas at Source は、mccli backup show の出力にホスト名と位置情報を追加します。また Replicas at Source には、次のコマンドの実行時にレプリカを識別するための --location オプションがあります。 <ul style="list-style-type: none"> • mccli backup validate • mccli backup delete • mccli backup edit • mccli backup restore

レプリカの保存

バックアップをレプリケートすると、ソース Avamar システム上のバックアップの保存設定が、ターゲットシステム上のレプリカに自動的に適用されます。ただし、レプリカの保存設定は変更可能です。

レプリケーションの実行前の保存設定

AUI のポリシー ベースのレプリケーションでは、レプリケーション グループを構成する際に、**[Replication Policy]** ウィザードの **[Retention]** ページで、レプリカに異なる保存設定を指定します。

コマンド ライン レプリケーションでは、--[avtar]expires オプションを使用して、レプリカに異なる保存設定を指定します。

レプリケーションの実行後の保存設定

[Replicas at Source] を有効にし、ソース Avamar サーバーでの Avamar Administrator セッションを使用してターゲット システム上のレプリカの保存期間を設定するか、AUI を使用してターゲット Avamar システムにログインし、レプリケーションの実行後にレプリカの有効期限を手動で変更します。[バックアップの有効期限日の変更](#) (148 ページ) では、バックアップの保存設定を変更する手順を説明します。これらの手順は、Avamar システム上のレプリカにも適用されます。

Data Domain システムを使用したレプリケーション

Avamar システムが Data Domain システムにバックアップを格納する場合、Avamar レプリケーションは DD Boost を使用して元の Data Domain システムからバックアップをコピーして、別の Data Domain システムにレプリカを作成します。

サポートされるレプリケーション構成

次の表では、DD Boost を使用した Avamar レプリケーションのためにサポートされるレプリケーション構成を示します。

表 87 DD Boost を使用した Avamar レプリケーションのためのレプリケーション構成

バックアップ ストレージ	レプリケーション ストレージ
シングル Data Domain システム	シングル Data Domain システム
シングル Data Domain システム	複数の Data Domain システム
複数の Data Domain システム	シングル Data Domain システム
複数の Data Domain システム	複数の Data Domain システム

レプリケーション ストレージに複数の Data Domain システムが存在している構成では、ソース Avamar サーバのドメインをターゲット Data Domain システムにマッピングすることで、レプリカを受信するシステムを制御します。デフォルトのターゲットを使用して Data Domain システムを指定します。ターゲット Data Domain システムが特定されていない場合、Avamar はデフォルトのターゲットにレプリケートします。

「Avamar および Data Domain システム統合ガイド」では、ストレージ マッピングのステップや、デフォルトのターゲット Data Domain システムの指定について説明します。

レプリケーションの詳細

次の詳細が、Data Domain システムを使用する Avamar レプリケーションに適用されます。

- レプリケーション時のデータ転送は、中継的なステー징なしで Data Domain システム間で実行されます
- レプリケーションは DD Boost を使用してバックアップをコピーし、レプリカを書き込みます
- Data Domain レプリケーション ライセンスが必要です
- Data Domain レプリケーションを使用しません
- レプリケーションは Avamar サーバで構成され、監視されます
- レプリケーション タスクのスケジュール設定では、Avamar レプリケーション スケジュールのみを使用します
- Data Domain 管理ツールは使用されません

Replicas at Source の有効化

Replicas at Source 機能は、Avamar サーバー バージョン 7.2 以降に備わっています。この機能を有効化するには、`mcserver.xml` を変更して、[Remote Backup Manager] Service を開始します。

はじめに

バージョン 7.2 以降の Avamar サーバー ソフトウェアをインストールするか、このバージョンにアップグレードします。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、`admin` OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```
2. 次のコマンドを入力して、MCS を停止します。

```
dpnctl stop mcs
```
3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```
4. テキスト エディターで `mcserver.xml` を開きます。
5. `repl` コンテナ エlement で、`allow_dest_replica_management` パラメーターの値を `true` に設定します。

デフォルト値は `false` です。
6. `repl` コンテナ エlement で、`show_external_backups` パラメーターの値を `true` に設定します。

デフォルト値は `true` です。
7. `repl` コンテナ エlement で、`allow_manage_remote_backups_at_source` パラメーターの値を `true` に設定します。

デフォルト値は `true` です。
8. 変更を保存して、ファイルを閉じます。
9. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```
10. クライアント バックアップと関連づけられた Avamar サーバ (ソース サーバ) で Avamar Administrator にログインします。
11. Avamar Administrator で、[Administration] 起動リンクをクリックします。

[Administration] ウィンドウが表示されます。

12. **[Services Administration]** タブをクリックします。
13. **[Remote Backup Manager Service]** を右クリックして、**[Start]** を選択します。

結果

Avamar サーバで Replicas at Source 機能が有効化されます。

ポリシー ベースのレプリケーションの構成

AUI でポリシー ベースのレプリケーションを使用するための準備を行うには、次のタスクを完了する必要があります。

はじめに

クライアント バックアップと関連づけられた Avamar サーバ (ソース サーバ) で AUI にログインします。

次のいくつかのステップでは、AUI でポリシー ベースのレプリケーションを構成するためのタスクを順を追って簡単に説明します。各ステップについては、それぞれのタスク セクションで詳細に説明します。

手順

1. レプリカを格納する各システムのレプリケーション ターゲットを、ソース サーバ (ターゲット システム) から追加します。
レプリケーション ターゲット システムを追加する方法については、[レプリケーション ターゲットとしての Avamar システムの追加](#) セクションを参照してください。
2. 日次、週次、月次のスケジュールを作成し、レプリケーションのスケジュール設定に使用します。
3. 1 個以上のレプリケーション グループを作成して、ポリシー ベースのレプリケーションの設定を定義します。

レプリケーション ターゲット

Avamar サーバでのポリシー ベースのレプリケーションの構成を開始するには、レプリケーション ターゲットを追加します。

レプリケーション ターゲットとして追加するために、サポートされるデータ ストレージ システムの接続情報を入力します。

Avamar は、他の Avamar システムへのレプリケーションや、DD Boost を使用した Data Domain システムへのレプリケーションをサポートします。Avamar システムは、異なるバージョンの Avamar サーバ ソフトウェアを実行している別の Avamar システムにレプリケートできますが、同じサーバ ソフトウェア バージョンの場合に最善の結果が得られます。

レプリケーション ターゲットとしての Avamar システムの追加

レプリケーション ターゲットとして追加するために、Avamar システムの接続情報を入力します。

手順

1. AUI で、**[Administration]** > **[System]** に移動します。
2. **[Replication Destination]** タブをクリックして、**[+ Add]** をクリックします。
[Add New Replication Destination] ウィザードが表示されます。
3. **[Name]** フィールドにターゲット Avamar システムの参照名を入力します。
4. **[Encryption]** ドロップダウンから、暗号化レベルを選択します。

選択した暗号化レベルは、ターゲット Avamar システムへのレプリケーション データ転送に適用されます。デフォルトの設定は **[High]** であり、変更しないでください。ただし、ソースが認

証を使用し、ターゲットが認証を使用しないように構成されている場合は例外として [none] に設定する必要があります。

5. **[Target Server Address]** フィールドに、ターゲット Avamar システムの DNS 名または IP アドレスを入力します。
6. ターゲット Avamar システムとの通信で使用するために、**[Target server connection port]** には、ソース Avamar システムのアウトバウンド ポートの番号を入力します。
デフォルト ポート値は 27000 です。
[High] レベルの **[Encryption]** を選択すると、ファイアウォール経由で接続できるようにポートにオフセットが適用されます。デフォルトのオフセットは+2000 です。このオフセットを編集するには、mcserver.xml での secured_port_offset の選択を手動で編集してから、MCS を再開します。
7. ターゲットシステム上の MCS とのデータ接続に使用するために、**[Target MCS connection port]** フィールドには、ターゲット Avamar サーバーのインバウンド ポートの番号を入力します。
デフォルト ポート値は 28001 です。
8. **[User ID on target server]** には、ターゲット Avamar システムで backup 権限と admin 権限を持つアカウントのユーザー名を入力します。
通常、repluser または root を入力します。

注

アクセスを root ドメインの下位ドメインに制限されているユーザーの場合（テナント アクセス）、ソース Avamar サーバーとターゲットシステムの両方で Avamar サーバー バージョン 7.2 以降を実行する必要があります。

9. **[Password on target server]** フィールドに、ユーザー名と関連づけられたパスワードを入力します。
10. **[VALIDATE]** をクリックします。
ソース Avamar システムは、指定された設定を使用して、ターゲット Avamar システムで認証されます。
検証が正常に完了すると、**[OK]** ボタンが有効になります。
11. **[OK]** をクリックして、レプリケーションのターゲットを追加し、ウィザードを終了します。

結果

AUI は、レプリケーション ターゲットを **[Replication Destinations]** タブのリストに追加します。

レプリケーション ターゲットの編集

レプリケーション ターゲットの接続情報を変更します。

手順

1. AUI で、**[Administration]** > **[System]** に移動します。
2. **[Replication Destination]** タブをクリックして、編集するレプリケーション ターゲットをハイライト表示します。
3. **[Edit]** をクリックします。
[Edit replication destination] ウィザードが表示されます。

4. レプリケーション ターゲットの設定を編集し、[VALIDATE] をクリックします。
5. 検証が正常に完了したら、[OK] をクリックします。

結果

選択したレプリケーション ターゲットの設定を AUI が変更します。

デフォルトの Data Domain ターゲットの設定

ターゲット Data Domain システムが複数存在するレプリケーションの環境では、どちらの Data Domain システムがデフォルトのターゲットであるかを指定できます。AUI の [Storage Mapping] タブで、ターゲット Data Domain システムが特定されていない場合、Avamar がデータをレプリケートする先の Data Domain システムがデフォルトのターゲットになります。

手順

1. AUI で、[Administration] > [System] に移動します。
[System] ウィンドウが表示されます。
2. [Data Domain] タブをクリックすると、構成済みの Data Domain システムのリストが表示されます。
3. デフォルトの Data Domain ターゲットを追加する必要がある場合は、[+ ADD] をクリックします。Data Domain システムがすでに表示されている場合は、システムを選択し、[Edit] をクリックします。
[Add Data Domain] または [Edit Data Domain] ウィザードが表示されます。
4. ウィザードのページを下にスクロールして [Misc] セクションに移動し、[Use system as default replication storage] チェックボックスをオンにします。
5. [VALIDATE] をクリックします。

結果

選択したレプリケーション ターゲットの設定を AUI が変更します。

Data Domain システムへのドメインのマッピング

ターゲット Data Domain システムが複数存在する場合、ソース Data Domain システムからレプリケートするデータを、どのシステムが受信するかを制御することができます。ターゲット Data Domain システムを指定するには、ソース Avamar サーバのドメインをターゲット Data Domain システムにマップします。マッピングを行わない場合は、Avamar はデータをソース Data Domain システムからデフォルトのターゲットにレプリケートします。

注

最初のレプリケーションが行われるまで、ソース Avamar サーバのドメインはターゲット Data Domain システムにマッピングできません。最初のレプリケーション時に、データはデフォルトのターゲットにレプリケートされます。

手順

1. AUI で、[Administration] > [System] に移動します。
[System] ウィンドウが表示されます。
2. [Storage Mapping] タブをクリックし、[+ ADD] をクリックします。
[Add Storage Mapping] ダイアログが表示されます。
3. リストから、レプリケーション ターゲットとして使用する Data Domain システムを選択します。

4. **[Submit]** をクリックします。

レプリケーション ターゲットレコードの削除

レプリケーション ターゲットのレコードをソース Avamar システムから削除します。

Avamar Administrator の **[Replicas at Source]** を使用してレプリケーション ターゲットレコードを削除する場合、**[Replicas at Source]** が有効になっていると、Avamar システムはレプリケーション ターゲット システム上のレプリカをチェックします。ソース Avamar システムと関連づけられたレプリカが存在する場合、Avamar Administrator ではレプリケーション ターゲットレコードが削除されないようになっています。レプリカが存在しているときでも、レプリケーション ターゲットレコードを削除する場合は、この設定をオーバーライドしてください。

[Replicas at Source] 機能が無効になっていると、Avamar システムはレプリケーション ターゲットレコードを削除する前にレプリケーション ターゲット システム上のレプリカを確認しません。既存のレプリカは、使用期間が終了するまで、またはターゲット システム インターフェイスを使用して削除するまで、レプリケーション ターゲット システムに残されます。

表 88 Replicas at Source

Replicas at Source	結果
Enabled	Avamar システムは、レプリケーション ターゲット システムでレプリカを確認し、レプリカが存在しない場合は、レプリケーション ターゲットレコードを削除します。Avamar システムがレプリカを確認しないようにし、また、レプリカがレプリケーション ターゲット システムに存在する場合でも、レプリケーション ターゲットレコードを削除するように設定するには、 [Check for remote backups before deletion] をオフにして [Yes] をクリックします。
Disabled	Avamar システムは、レプリケーション ターゲットレコードを削除します。

手順

1. AUI で、**[Administration]** > **[System]** に移動します。
2. **[Replication Destination]** タブをクリックして、削除するレプリケーション ターゲットレコードを選択します。
3. **[削除]** アイコンをクリックします。
確認ダイアログが表示されます。
4. 削除を確定するには、**[YES]** をクリックします。

レプリケーション グループ

レプリケーション グループを使用すると、ポリシー ベースのレプリケーションの設定を定義できます。

レプリケーション グループのオプションには以下が含まれます。

- レプリケーション グループのドメイン メンバーとクライアント メンバー
- レプリケーションのバックアップ タイプ
- レプリケートするバックアップの数
- ターゲットのサーバ
- レプリケーションのスケジュール
- レプリケートされたバックアップがターゲット サーバーに保持される期間

先にレプリケートされるバックアップ データを決める優先度を指定できます。レプリケーション グループのメンバーを定義する際は、[Member(s)] リストでメンバーが表示されている順序によって、レプリケートされるバックアップ データの順序が決まります。

[Member(s)] リストで単独で表示されているクライアントが、ドメインのメンバーでもある場合でも、クライアントのバックアップ データは一度のみレプリケートされます。

[Member(s)] リストで単独のクライアントがドメインよりも高い優先度で表示されている場合は、単独のクライアントのバックアップ データは、ドメイン内の他のクライアントのバックアップ データよりも先にレプリケートされます。

AUI でのレプリケーション ポリシー/グループの作成

はじめに

- ターゲット Avamar サーバをソース Avamar サーバの構成に追加します。
- (オプション) グループのレプリケーションを実行するタイミングを指定するスケジュールを作成します。

手順

1. AUI の左側のナビゲーション ペインで [>>] をクリックします。
2. [Policy] > [Replication Policy] に移動します。
[Replication Policy] ウィンドウが表示されます。
3. [Replication Policy] ウィンドウで [+ ADD] をクリックします。
[Policy] ウィザードが表示されます。
4. [Properties] ページで、レプリケーション グループの名前を入力し、[Enabled] を選択してレプリケーション グループのレプリケーションを有効にします。
5. プール ベースのレプリケーションを使用して Data Domain のソースから Data Domain のターゲットへの複数の並列レプリケーション バックアップを有効にする場合は、[Replicate client backups in parallel] を選択します。それ以外の場合は、[Default Mode] を選択します。
 - a. 最適化をサポートするプラグ インに対して VSR 最適化を使用するようにレプリケーション プラグ インに指示するには、[Optimize Virtual Synthetic Replication (VSR)] を選択します。

注

VSR 最適化には、[Replication order of client backups] を [Oldest to Newest] にする必要があります。このオプションはデフォルトでオンになっています。プールベースのレプリケーションのすべての順序オプションに従うことを要求するには、プラグ インに関係なく、このオプションを選択解除します。

- b. [Replication order of client backups] に、次のいずれかを選択します。
 - [Oldest to Newest] では、最も古いバックアップから順にレプリケーションを開始します。
 - [Newest to Oldest] では、最も新しいバックアップから順にレプリケーションを開始します。
6. [NEXT] をクリックします。
[Members] ページが表示されます。

7. **[Members]** ページで、レプリケーション グループのメンバーに必要とされるステップを完了します。

レプリケーション グループのメンバ ー	ステップ
すべてのクライ アント	[Replicate all clients] を選択して [NEXT] をクリックします。
特定のドメインま たはクライアント	<p>a. [Choose Membership] を選択します。</p> <p>b. レプリケーション グループに追加するには、[>] をクリックしてドメイン/クライアントのリストを展開し、ドメイン/クライアントの横にあるチェックボックスを選択または選択解除します。</p> <p>選択したメンバーがテーブルに追加されます。</p> <p>c. レプリケーション グループからメンバーを削除するには、テーブルのエントリーの横にある [-] をクリックします。</p> <p>d. [NEXT] をクリックします。</p>

8. **[Backup Filters]** ページで、レプリケートするバックアップのタイプに対して必要なステップを完了します。

レプリケートするバック アップのタイプ	ステップ
レプリケーション グル ープのすべてのメンバ ーからのすべてのバックア ップ	[Replicate all backups] を選択します。
特定のバックアップ	<p>a. [Include/Exclude backups by date, type, and more] を選択します。</p> <p>b. [Select Backup Filter] をクリックします。</p> <p>[Backup Filter] ダイアログ ボックスが表示されます。</p> <p>c. レプリケートするバックアップのタイプを [Daily]、[Weekly]、[Monthly]、[Yearly]、[No tag] から選択します。少なくとも1つのバックアップ タイプを選択する必要があります。</p> <p>d. レプリケーション グループのメンバーである各クライアントをレプリケートするには、バックアップの最大数を指定します。</p> <p>すべてのバックアップをレプリケートするには(上限なし)、[No limit for number of backups per client] を選択します。</p> <p>各メンバー クライアントで、特定の数の最新バックアップをレプリケートするには、[Limit to] を選択して、バックアップの上限となる最大数を指定します。</p> <p>e. レプリケーション グループのメンバーである各クライアントで、レプリケートするバックアップの日付制限を指定します。</p>

レプリケートするバックアップのタイプ	ステップ
	<p>バックアップが実行された日付に関係なく、すべてのバックアップをレプリケートするには、[No Date Restrictions] を選択します。</p> <p>最近の任意の期間に実行されたバックアップのみをレプリケートするには、[Last] を選択して、レプリケーションに含める過去の [Day(s)]、[Weeks(s)]、[Month(s)]、[Year(s)] のいずれかの数値を指定します。</p> <p>任意の日付範囲の間に実行されたバックアップのみをレプリケートするには、[Range] を選択して、開始日時を [From] フィールドに指定するか、終了日時を [To] フィールドに指定します。または、これらの両方のフィールドを指定します。</p> <p>f. [OK] をクリックします。</p>

9. [**NEXT**] をクリックします。
[**Schedule**] ページが表示されます。
10. [**Schedule**] ページで、[**Select Existing Schedule**] ドロップダウンを使用して、デフォルトのレプリケーション スケジュールを選択するか、作成した別のスケジュールを選択します。
11. [**NEXT**] をクリックします。
[**Retention**] ページが表示されます。
12. [**Retention**] ページで、レプリケートされたバックアップの有効期限が宛先サーバーで切れる時期を指定します。
 - 現在の有効期限設定に基づいて、レプリケートされたバックアップの有効期限を終了するには、[**Keep current backup expiration**] を選択します。
 - 現在の使用期間の終了設定とは異なる時期に、レプリケートされたバックアップの有効期限を終了するには、[**Set expiration by backup type**] を選択して、各バックアップタイプを保持する日数、週数、月数、年数のいずれかを指定します。

バックアップが複数のタイプで構成される場合、レプリケートされたバックアップの有効期限は、最も有効期限の長いバックアップタイプで指定した値に設定されます。例えば、日次バックアップと月次バックアップの両方が実行されたバックアップの場合、レプリケートされたバックアップの有効期限は月次バックアップで指定した値に設定されます。
13. [**NEXT**] をクリックします。
[**Destination**] ページが表示されます。
14. [**Destination**] ページで、バックアップのレプリケート先とする既存の宛先サーバーをテーブルから選択するか、[**+ ADD DESTINATION**] をクリックすると表示される [**Add replication destination**] ダイアログで宛先サーバーを選択します。
15. [**NEXT**] をクリックします。
[**Summary**] ページが表示されます。
16. [**Summary**] ページで、レプリケーション ポリシーの構成の詳細を確認します。このページには、高度な構成の詳細を指定するオプションも用意されています。
 - 高度な構成を実行しない場合は、[**FINISH**] をクリックします。

- 構成の詳細をより細かく指定する場合は、ページの下部までスクロールし、**[Advanced Parameters]** をクリックします。

[Advanced Parameters] をクリックすると、ダイアログが表示されます。

17. (オプション) レプリケーション グループには、次の詳細パラメーターを指定します。また、**[Show Advanced Options]** スライダーを右に移動して、追加のフィールドを表示することもできます。詳細オプションが **[太字]** で表示されます。
 - a. 特定のプラグ インからのバックアップのみをレプリケートするには、**[Include plug-in specific backups]** フィールドで数値のプラグ イン ディスクリプタを指定します。
 複数のエントリーはコンマで区切り、すべてのバックアップをレプリケートするには、このボックスを空白のままにします。数値のプラグ イン ディスクリプタのリストについては、[数値のプラグ イン ディスクリプター](#) (291 ページ) を参照してください。
 - b. 特定のプラグ インからのバックアップをレプリケーションから除外するには、**[Exclude plug-in specific backups]** フィールドで数値のプラグ イン ディスクリプタを指定します。
 複数のエントリーはコンマで区切り、すべてのバックアップをレプリケートするには、このボックスを空白のままにします。
 - c. **[Excludes clients containing PATTERN from replication]** では、複数のエントリーはコンマで区切り、すべてのバックアップをレプリケートするにはこのボックスを空白のままにします。
 - d. 特定のバックアップのみをレプリケートするには、**[Backup sequence number]** フィールドでバックアップ シーケンス番号を指定するか、**[Backup label]** フィールドでバックアップ ラベルを指定します。フル バックアップ シーケンス番号またはラベルを指定します。
 - e. 特定のパターンに一致するラベルを持つバックアップをレプリケートするには、**[Backup label pattern]** フィールドでパターンを指定します。
 - f. **[Informational message level]** ドロップダウンから、レプリケーション ログ ファイル内の参考メッセージに対して詳細度を選択します。
 - すべての参考メッセージを抑制するが、エラーおよび警告はログ ファイルに記録するには、**[No informationals]** を選択します。
 - エラーおよび警告とともに、参考メッセージの一部をログ ファイルに記録するには、**[Some informationals]** を選択します。
 - エラーおよび警告とともに、追加のステータス情報をログ ファイルに記録するには、**[Many informationals]** を選択します。
 - すべての参考メッセージ、エラー、警告など最大限の情報をログ ファイルに記録するには、**[All informationals]** を選択します。
 - g. より詳細な時系列情報と重複除外の統計情報をレプリケーション ログ ファイルに含めるかどうかを指定するには、**[Report advanced statistics]** チェックボックスを選択または選択解除します。
 - h. **[List contents being replicated]** ドロップダウンで、レプリケーション ログ ファイルに含めるレプリケートされたバックアップに関する情報量を次から指定します。
 - **[No file listing]**
 - **[List file names]**
 - **[List files and dates]**

レプリケーション ログ ファイルにファイル情報を含める場合は、慎重に行ってください。レプリケーションのパフォーマンスが低下し、ログ ファイルのサイズが非常に大きくなります。

- i. トラブルシューティングのためにログ ファイルに最大量の情報を書き込むには、[**Enable debugging messages**] チェックボックスを選択します。

レプリケーション プロセスでは、非常に大きなログ ファイルが生成されます。

- j. [**Maximum concurrent processes**] ドロップダウンから、同時にレプリケートするクライアントの最大数を選択します。

- k. ネットワーク使用率を特定のレート (Mbps 単位) に低下させるには、[**Network usage throttle**] フィールドでメガビット数を指定します。

ネットワーク使用率に制限を設けない場合は、0 (ゼロ) を指定します。T1 回線帯域の 50%相当を使用するには、0.772 と指定します。

- l. Data Domain システムにプール ベースのレプリケーションが構成されている場合は、クライアントレプリケーションの順序を [**Client list ordering**] ドロップダウンで選択します。

- m. プール ベースのレプリケーションが Data Domain システムに構成されている場合、[**Maximum number of Data Domain Replication Streams**] フィールドに、並列で起動できる avtar プロセスの最大数を入力するか、矢印を使用します。

- n. 詳細パラメーターを入力したら、[**OK**] をクリックして構成の詳細を保存し、ダイアログを終了してから、[**FINISH**] をクリックします。

レプリケーション ポリシー/グループの有効化または無効化

レプリケーション ポリシー/グループを無効化し、スケジュール設定されたレプリケーションがそのグループに対して実行されないようにすることができます。通常、このステップは、システムがメンテナンス アクティビティを行える状態にしておくために実行します。レプリケーション グループを無効化した場合、スケジュール設定されたレプリケーションを再開するには、グループを再度有効化する必要があります。

手順

1. AUI の左側のナビゲーション ペインで [>>>] をクリックします。
2. [**Policy**] > [**Replication Policy**] に移動します。
[**Replication Policy**] ウィンドウが表示されます。
3. 目的のレプリケーション ポリシーを選択し、[**Edit**] アイコンをクリックします。
Policy ウィザードが表示されます。
4. [**Enabled**] チェックボックスをオンにしてグループを有効化するか、チェックボックスをオフにしてグループを無効化します。
5. [**NEXT**] をクリックしてウィザードの残りのステップを順に移動し、[**FINISH**] をクリックして変更を保存します。

グループが有効化されている場合、[**Replication Policy**] ウィンドウの [**Enabled**] 列に [**True**] と表示されます。グループが無効化されている場合、[**Replication Policy**] ウィンドウの [**Enabled**] 列に [**False**] と表示されます。

レプリケーション ポリシー/グループの編集

手順

1. 左側の AUI ナビゲーション ペインで [>>>] をクリックします。
2. [**Policy**] > [**Replication Policy**] に移動します。

- [**Replication Policy**] ウィンドウが表示されます。
3. 目的のレプリケーション グループを選択し、[**Edit**] アイコンをクリックします。
[**Replication Policy**] ウィザードが表示されます。
 4. レプリケーション グループの設定を編集します。
グループの作成時に指定したものと同一設定を使用します。
 5. [**Finish**] をクリックします。

レプリケーション ポリシー/グループの削除

ソース Avamar サーバーの構成からレプリケーション グループを削除すると、宛先サーバーにすでにレプリケートされているグループのデータはすべて、レプリケートされたバックアップの有効期限が切れるか、バックアップが削除されるまで、宛先サーバーに残ります。

手順

1. AUI の左側のナビゲーション ペインで [>>>] をクリックします。
2. [**Policy**] > [**Replication Policy**] に移動します。
[**Replication Policy**] ウィンドウが表示されます。
3. 削除するレプリケーション グループを選択し、[**Delete**] アイコンをクリックします。
確認メッセージが表示されます。
4. [**YES**] をクリックします。

AUI でのオン デマンド レプリケーションの実行

AUI でのポリシー ベースのレプリケーションを使用すると、レプリケーション グループのオン デマンド レプリケーションを実行できます。オン デマンド レプリケーションとは、1 回限りのデータのレプリケーションをレプリケーション グループで行うものです。ポリシー ベースのレプリケーションを構成した後、レプリケーション グループの最初のレプリケーションを作成するために、オン デマンド レプリケーションの実行が必要になることがあります。システム メンテナンス、ソフトウェアのインストール、ソフトウェア アップグレードを行う前にも、オン デマンド レプリケーションを実行します。

[**Policy**] > [**Replication Policy**] に移動して、[**Replication Policy**] ウィンドウからポリシーを選択することにより、AUI でオン デマンド レプリケーションを実行できます。

[**Policy**] ウィンドウからオン デマンド レプリケーションを実行する

手順

1. 左側の AUI ナビゲーション ペインで [>>>] をクリックします。
2. [**Policy**] > [**Replication Policy**] に移動します。
[**Replication Policy**] ウィンドウが表示されます。
3. テーブルから目的のレプリケーション グループのポリシーを選択します。
4. [**実行**] をクリックします。

レプリケーション アクティビティが開始されたことを示す確認メッセージが表示されます。メッセージ内の [**Activity**] リンクをクリックするか [**Activity**] ウィンドウに移動して、進行状況を確認することができます。

結果

レプリケーション アクティビティが完了すると、レプリケートされたバックアップが **[Asset Management]** ウィンドウに表示されます。

1. **[Asset Management]** ウィンドウに移動して、**[Domain]** パネルからドメインを選択します。
2. **[Asset Management]** パネルからクライアントを選択し、**[Client Summary]** パネルで **[VIEW MORE]** をクリックします。

注

ソース Avamar システムでは、現在、ローカル バックアップのみが一覧表示されます。リモート バックアップの場合は、ターゲット システムにログインします。

コマンドラインレプリケーションの実行

avreplCLI (コマンドライン インターフェイス) を使用して、ソース Avamar サーバからターゲット Avamar サーバにデータをレプリケートすることができます。

avrepl バイナリはサーバー ユーティリティ ノードの `\usr\local\avamar\bin` ディレクトリにあります。admin または root としてログインし、その場所からコマンドを実行します。

コマンド リファレンス

次のトピックでは、avrepl コマンドによってサポートされるオペレーションおよびオプションに関する参照情報を提供します。

構文

```
avrepl --operation=replicate [options] [target]
```

操作

avrepl でサポートされている唯一の操作は--operation=replicate であり、これによりソース Avamar サーバからターゲット Avamar サーバにデータがレプリケートされます。

オプション

レプリケーションの動作を制御するには、avrepl コマンド オプションを使用します。

アカウント オプション

avrepl コマンドのアカウント オプションにより、レプリケーション用にターゲット Avamar サーバに接続するための認証情報を指定できます。

avrepl コマンドでは、次のアカウント オプションを利用できます。

表 89 avrepl コマンドのアカウント オプション

オプション	説明
--account=location --acnt=location --path=location	ターゲット Avamar サーバの階層的な場所を指定します。このオプションは現在のホームの場所に相対的になります。ただし、パス指定でプレフィックスとしてスラッシュ (/) を使用している場合は、絶対パスとして扱われます。デフォルトのアカウントは REPLICATE です。

表 89 avrepl コマンドのアカウント オプション (続き)

オプション	説明
<code>--[replscript]dstaddr=destination_server</code>	ターゲット Avamar サーバの DNS 名または IP アドレスを指定します。異なるバージョンのサーバー間のレプリケーションがサポートされます。ただし、最適な結果を得るためには、ターゲットサーバの Avamar サーバソフトウェアが、ソース Avamar サーバと同一のバージョンか、より新しいバージョンであるようにします。
<code>--[replscript]dstid=repluser</code>	ターゲット Avamar サーバの認証に使用する Avamar ユーザー ID とドメインを指定します。 注 repluser アカウントは、すべてのターゲットサーバーでの信頼性の高い動作が認められている唯一のユーザーアカウントです。
<code>--dstpassword=password</code> <code>--dstap=password</code> <code>--dstpswd=password</code>	ターゲット Avamar サーバでの repluser アカウントのパスワードを指定します。
<code>--[replscript]dstpath=domain</code>	レプリケートされたソースデータを保存するターゲット Avamar サーバ上の場所 (domain) を指定します。デフォルト値は最上位ディレクトリ (/) であり、これにより、ソース Avamar サーバに対応して名づけられた新しいドメインに、レプリケートされたデータが格納されます。このオプションを <code>--[replscript]srcpath</code> オプションとともに使用します。このオプションを <code>--[replscript]dppname</code> オプションと併せて使用することはできません。
<code>--[replscript]dstport=port</code>	ターゲット Avamar サーバへの接続時に使用されるデータ用ポートを指定します。デフォルト値は 27000 です。
<code>--hfsaddr=Avamar_server</code> <code>--server=Avamar_server</code>	ソース Avamar サーバの DNS 名または IP アドレスを指定します。
<code>--[avtar]id=user@auth</code>	ソース Avamar サーバでの認証に使用する Avamar ユーザー ID と認証システムを指定します。デフォルト値は repluser であり、これは Avamar サーバ上のデフォルトのレプリケーションユーザーアカウントです。Avamar 認証システムで認証するには、auth に avamar を指定します。例: <code>--[avtar]id=jdoe@avamar</code> 。
<code>--password=password</code> <code>--ap=password</code> <code>--pswd=password</code>	ソース Avamar サーバでの認証に使用する Avamar ユーザー ID のパスワードを指定します。

ログ オプション

avrepl コマンドのログ オプションにより、avrepl ログ ファイルのパスとファイル名を指定して、プラグインによってログファイルに書き込まれる情報量を制御することができます。

avrepl コマンドでは、次のログ オプションを利用できます。

表 90 avrepl コマンドのログ オプション

オプション	説明
--[avtar]informationals=n	ステータス メッセージの情報レベルを設定します。ここで n は 1 桁の整数値です。
--[avtar]noinformationals={true false}	すべてのステータス メッセージを無効化するには true を指定します。
--[avtar]statistics={true false}	true を指定すると、より詳細な時系列情報と重複排除の統計情報がレプリケーション ログ ファイルに含まれます。
--log=file --logfile=file	avrepl プラグ イン ログ ファイルのフル パスとファイル名を指定します。
--nostdout={true false}	STDOUT への出力を無効化するには true を指定します。ただし、--log または --logfile オプションを使用すると、出力は継続してログ ファイルに記録されます。
--nowarnings={true false}	警告メッセージを無効化するには true を指定します。
--quiet={true false}	すべてのメッセージを抑制するには true を指定します。このオプションは、--[avtar]noinformationals=true と --nowarnings=true の両方を使用する場合と同等です。
--verbose --v	ステータス メッセージおよび警告メッセージを含む、すべてのメッセージを有効化するには、--verbose または --v のいずれかを指定します。冗長性のレベルを制御するには、--verbose=n を指定します。デフォルト値は--verbose=6 です。

レプリケーション オプション

avrepl コマンドのレプリケーション オプションを使用すると、レプリケート対象のバックアップの選択や、レプリケートされたバックアップをターゲット サーバーに保持する期間などのレプリケーション機能の制御が可能です。

avrepl コマンドでは、次のレプリケーション オプションを利用できます。

表 91 avrepl コマンドのレプリケーション オプション

オプション	説明
--[avtar]after=timestamp	timestamp またはそれ以降に一致するバックアップのみをレプリケートするように指定します。timestamp には、ローカル タイム ゾーンの 24 時間表記の値を使用し、yyyy-mm-dd hh:mm:ss の構文に準拠します。部分的な timestamp 値が使用可能です。値は、最後に指定された値で解決されます。たとえば、2014-02 と 2014-02-01 00:00:00 は等しくなります。また、このオプションを--[avtar]before=timestamp とともに使用して、有効な日付範囲を定義することも可能です。この日付範囲内に実行されたバックアップのみがレプリケートされます。
--[avtar]allsnapups={true false}	デフォルト値は true であり、これによりすべてのバックアップがレプリケートされます。false に指定すると、各クライアントの最近のバックアップのみがレプリケートされます。--[avtar]count オプションを指定す

表 91 avrep1 コマンドのレプリケーション オプション (続き)

オプション	説明
	ると、--[avtar]count オプションによって-- [avtar]allsnapups オプションがオーバーライドされます。指定した数の最新のバックアップのみが各クライアントでレプリケートされます。
--[avtar]before=timestamp	timestamp より前に実行されたバックアップのみをレプリケートするように指定します。timestamp には、ローカル タイム ゾーンの 24 時間表記の値を使用し、yyyy-mm-dd hh:mm:ss の構文に準拠します。部分的な timestamp 値が使用可能です。値は、最後に指定された値で解決されます。たとえば、2014-02 と 2012-02-01 00:00:00 は等しくなります。また、このオプションを-- [avtar]after=timestamp とともに使用して、有効な日付範囲を定義することも可能です。この日付範囲内に実行されたバックアップのみがレプリケートされます。
--[avtar]count=n	レプリケートされたバックアップが、各クライアントの最近のバックアップのこの最大数 (n) に制限されます。
--[avtar]exclude-pluginid-list=list	指定されたプラグ インで実行されたバックアップを除外します。ここで、list はプラグ イン ID のコマ区切りリストです。
--[avtar]expires={n period timestamp}	次のように、レプリケートされたバックアップをターゲット サーバーに保持する期間を指定します。 <ul style="list-style-type: none"> • 日数 (n)。 • 特定の日数、週数、月数、年数のいずれかで指定する有効期限 (period)。期間を指定するには、次の値の 1 つを使用します。 <pre>days=n weeks=n months=n years=n</pre> ここで、n は正の整数です。例えば、-- [avtar]expires=years=2 と指定すると、レプリケートされたバックアップが 2 年間ターゲット サーバーに保持されます。また、--[avtar]expires=30 と-- [avtar]expires=days=30 は同等です。 • レプリケートされたバックアップの有効期限が切れる日時を timestamp で指定します。ローカル タイム ゾーンの 24 時間表記の値を使用し、yyyy-mm-dd hh:mm:ss の構文に準拠します。部分的な timestamp 値が使用可能です。値は、最後に指定された値で解決されます。例えば、2014-02 は 2014-02-01 00:00:00 に相当します。
--[avtar]pluginid-list=list	指定されたプラグ インで実行されたバックアップのみをレプリケートします。ここで、list はプラグ イン ID のコマ区切りリストです。
--[avtar]retention-type={daily weekly monthly yearly none}	次のいずれかの保存タイプのバックアップのみをレプリケートします。 <ul style="list-style-type: none"> • daily • weekly

表 91 avrepl コマンドのレプリケーション オプション (続き)

オプション	説明
	<ul style="list-style-type: none"> monthly yearly none <p>none と指定すると、特定の保存タイプが設定されていないバックアップのみがレプリケートされます。</p>
--[replscript]dpnname=source_server --dpn=source_server	ターゲット サーバの REPLICATE ドメインにあるレプリケートされたファイルで、パスの一部としてソース Avamar サーバ (source_server) を示すために使用する名前を指定します。ソース サーバの完全修飾ドメイン名を入力してください。このオプションは-- [replscript]dstpath または-- [replscript]srcpath オプションとともに指定することはできません。
--[replscript]dstencrypt={ssl tls}	ターゲット サーバの avtar、avmaint、avmgr で指定した暗号化方式を有効化します。有効な暗号化方式は ssl と tls です。
--[replscript]srcpath=domain	レプリケーションを開始するソース Avamar サーバの場所 (domain) を指定します。この場所に含まれるデータのみがレプリケートされます。デフォルト設定は最上位ドメイン (/) であり、これによりサーバ全体がレプリケートされます。このオプションを-- [replscript]dstpath オプションとともに使用します。このオプションを-- [replscript]dpnname オプションと併せて使用することはできません。
--backup-type=type	指定されたタイプのバックアップのみがレプリケートされます。ここで、type は次のいずれかの値を指定します。 <ul style="list-style-type: none"> differential differential_full incremental incremental_full level0_full synthetic_full
-- max-ddr-streams=n	バックエンドの Data Domain システムを対象とする、並列に開始できる avtar プロセスの最大数を設定します。
--optimize-vsr={true false}	--use-pool-based が true に設定されている場合、--vsr-plugin-ids と組み合わせて使用し、このオプションは最適化をサポートするプラグインとともに VSR (仮想シンセティックレプリケーション) の最適化を使用する必要があるかどうかを識別します。VSR 最適化では、その他の設定に関係なく、レプリケーションを最古から最新への順序で行う必要があります。このオプションのデフォルト設定は true です。プールベースのレプリケーションのすべての順序オプションに従うことを要求するには、プラグインに関係なく、このオプションを false に設定します。

表 91 avrepl コマンドのレプリケーション オプション (続き)

オプション	説明
<code>--ordering-criterion=order</code>	<p><code>--use-pool-based</code> が <code>true</code> に設定されている場合、このオプションによりバックアップがレプリケートされる順番が指定されます。使用可能な値は、次のとおりです。</p> <ul style="list-style-type: none"> • <code>oldest-to-newest</code> 最も古いバックアップから順にレプリケーションを開始します。このオプションが指定されていない場合は、これがデフォルト設定です。 • <code>newest-to-oldest</code> 最新のバックアップから順にレプリケーションを開始します。 • <code>largest-to-smallest</code> 最大のバックアップから順にレプリケーションを開始します。 • <code>smallest-to-largest</code> 最小のバックアップから順にレプリケーションを開始します。
<code>--use-pool-based={true false}</code>	<p><code>true</code> の場合、プールベースのレプリケーション モードを有効にします。このモードでは、1 つの <code>Data Domain</code> ストレージ システムから別の <code>Data Domain</code> ストレージ システムにレプリケートするときに並列ですべてのクライアント バックアップをレプリケートします。</p>
<code>--vsr-plug-in-ids=plug-in-ids</code>	<p><code>--optimize-vsr</code> が <code>true</code> に設定されている場合は、VSR (仮想シンセティック レプリケーション) の最適化を使用する必要があるプラグインのプラグイン ID がこのオプションにより一覧表示されます。デフォルトでは、NDMP と VMware のプラグインが VSR 最適化を使用します。その他のプラグインはサポートされていません。</p>
<code>--within={days weeks months years}=n</code>	<p>最近の <code>days</code>、<code>weeks</code>、<code>months</code>、<code>years</code> のいずれかの間に実行されたバックアップをレプリケートします。ここで、<code>n</code> は正の整数です。例えば、<code>--within=months=3</code> と指定すると、各クライアントの 3 か月分のバックアップがレプリケートされます。</p>

Avamar 専用オプション

Avamar 専用オプションを利用すると、通常は Avamar 担当者のみが使用するために予約されている高度な機能にアクセスできます。これらの高度な機能を誤用するとデータを失う場合があります。これらのオプションについて不明な点がある場合、Avamar サポートに問い合わせ、使用前に詳細情報を確認してください。

avrepl コマンドでは、次の Avamar 専用オプションを利用できます。

表 92 avrepl コマンドの Avamar 専用の高度なオプション

オプション	説明
<code>--bindir=path</code>	<p>Avamar バイナリ ファイルを含むディレクトリを指定します。デフォルト値は <code>/usr/local/avamar/bin</code> です。</p>
<code>--[avtar]exp-delta={days weeks months years}=n</code>	<p>ターゲット サーバー上のレプリケートされたバックアップの有効期限日を、指定した日数、週数、月数、年数 (<code>n</code>) で変更します。値には、正または負の整数を指定できます。例えば、<code>--[avtar]exp-delta=days=-2</code> と指定すると、ターゲット サーバー上のバックアップ</p>

表 92 avrepl コマンドの Avamar 専用の高度なオプション (続き)

オプション	説明
	の有効期限日が 2 日減少します。-- [avtar] exp-delta を -- [avtar] expires とともに使用しないでください。
-- [avtar] expiration-policy= type = period	<p>指定した期間 (period) 内で特定の保存タイプ (type) のバックアップをレプリケートします。ここで、type は次のいずれかの値になります。</p> <ul style="list-style-type: none"> • dailies • weeklies • monthlies • yearlies <p>period は次のいずれかの値になります。</p> <ul style="list-style-type: none"> • days=n • weeks=n • months=n • years=n <p>ここで、n は正の整数です。例えば、-- [avtar] expiration-policy=dailies=years=2 と指定すると、各クライアントの 2 年分の日次バックアップがレプリケートされます。-- [avtar] expiration-policy オプションが -- [avtar] expires よりも優先されます。</p>
-- [avtar] label= name -- f= name	レプリケートするバックアップのラベルを指定します。複数の値をコンマで区切ります。
-- [avtar] label-pattern= pattern	指定したパターン (pattern) に一致するラベルを持つバックアップをレプリケートします。アスタリスク (*) や疑問符 (?) など、一般的なグロブ演算子 (ワイルドカード) が許可されます。複数のパターンはコンマで区切ります (例: ---- [avtar] label-pattern=temp, tmp)。また、単一のコマンドで ---- [avtar] label-pattern オプションを複数回指定することも可能です。
-- [avtar] sequencenumber= n -- [avtar] labelnumber= n	レプリケートするバックアップのシーケンス番号を指定します。複数のエントリはコンマで区切ります。
-- [avtar] throttle= n	基盤となる avtar プロセスがデータをサーバーに送信するレートを制御します。このオプションを指定する場合、avtar は各パケットを送信した後、Mbps (1 秒あたりのメガビット) 単位で指定した最大帯域幅をネットワーク使用率が超えないようにするために一時停止します。例えば、-- [avtar] throttle=5 では 10 Mbps 接続の半分を使用し、-- [avtar] throttle=0.772 では T1 リンクの半分に使用率が制限されます。
-- [replscript] exclude= pattern	pattern を含むドメインまたはクライアントをレプリケーションから除外します。ここで、 pattern はドメイン名またはクライアント名で一致するパターンです。アスタリスク (*) や疑問符 (?) など、一般的なグロブ演算子 (ワイルドカード) が許可されます。例えば、--

表 92 avrepl コマンドの Avamar 専用の高度なオプション (続き)

オプション	説明
	[replscript]exclude=spot と指定すると、パターン spot を含む名前のドメインまたはクライアントがすべて除外されます。-- [replscript]exclude=/clients/ と指定すると、/clients ドメインのすべてのクライアントが除外されます。複数のパターンはコンマで区切ります (例: -- [replscript]exclude=spot, /clients/)。また、単一のコマンドで-- [replscript]exclude オプションを複数回指定して、複数のパターンを指定することも可能です。
--[replscript]forcecreate={true false}	true と指定すると、すべてのソース サーバー アカウントをターゲット サーバーで作成するように強制します。これは、レプリケーション内にアカウントのデータがない場合でも強制されます。デフォルト値は false であり、これにより、データをレプリケートするクライアントのみで、アカウントがターゲット サーバーに作成されます。
--[replscript]force-move={1 0}	1 (true) と指定すると、ターゲット サーバーのバックアップ アカウントへの移動が強制されます。移動を強制しない場合は 0 (false) と指定します。
--[replscript]fullcopy={true false}	true と指定すると、完全な [root-to-root] レプリケーション モードをアサートし、これによってソース サーバー全体の完全な論理コピーがターゲット サーバーに作成されます。レプリケートされたデータは REPLICATE ドメインにコピーされませんが、ソース クライアントがターゲット サーバーに登録されたかのように、root ドメインに直接追加されます。この方法でレプリケートされたソース サーバー データは、ターゲット サーバーで完全に変更可能です。
--[replscript]globalcid={true false}	true と指定すると、レプリケーション中にグローバル CID (クライアント ID) が使用されます。グローバル CID は主に、root-to-root レプリケーションの後で、サーバー間の迅速なフェイルオーバーを可能にするために使用されます。true はデフォルトの設定です。
--[replscript]reportonly={true false}	true と指定すると、レポートのみの動作モードをアサートします。レポートのみの動作モードは、実際にはデータをターゲット サーバーに保存することなく、レプリケーション ジョブを実行し、アクティビティによりターゲット サーバーで消費される可能性があるストレージの量を事前に決定するために使用されます。
--[replscript]restore={true false}	true と指定すると、リストア動作モードをアサートします。すでにソース Avamar サーバをターゲット Avamar サーバにレプリケーションしている場合は、ターゲット サーバから avrepl を実行して、このコマンドを-- [replscript]dpnname=original_source_server オプションとともに指定し、Avamar サーバにデータをリストアすることが可能です。
--[replscript]small-client-mb=n	クライアントの新しいデータが「小さい」と判断される閾値 (単位: MB) デフォルト設定は 128 MB の新しいデータです。0 と指定すると、この最適化が無効化されます。
--rechunk={disable enable default}	レプリケートされたデータを再チャンクし、ターゲット サーバーのデータ重複排除を最大化するかどうかを制御します。次の値のいずれかを使用します。

表 92 avrepl コマンドの Avamar 専用の高度なオプション (続き)

オプション	説明
	<ul style="list-style-type: none"> • <code>disable</code> : ターゲット サーバーに保存する前にデータを再チャンクしません。 • <code>enable</code> : ターゲット サーバーに保存する前にデータを再チャンクし、データ重複排除を最大化します。 • <code>default</code> : ソース サーバーとターゲット サーバーのチャンク パラメーターが異なる場合、自動的にデータを再チャンクします。

ヘルプ オプション

`--help` オプションにより、`avrepl` コマンドで利用可能なオプションのリストが表示されます。

```
avrepl --help
```

バージョン オプション

`--version` オプションにより、`avrepl` コマンドのソフトウェア バージョンが表示されます。

```
avrepl --version
```

ターゲット一覧

特定のクライアントまたは Avamar ドメインをレプリケートするには、`avrepl` コマンドの末尾にクライアントおよびドメインのリストを含めます。複数のエントリーはスペースで区切ります。

リストを指定しない場合は、ソース Avamar サーバにあるすべてのクライアント バックアップがレプリケーションに含まれます。

数値のプラグ イン ディスクリプター

一部のコマンド オプションでは、1 個以上の数値のプラグ イン ディスクリプターを値に使用する必要があります。次の表では、有効な数値のプラグ イン ディスクリプターを挙げています。

表 93 数値のプラグ イン ディスクリプター

ディスクリプター	プラグ イン名
1,000	Linux avagent
1001	Linux avtar
1002	Linux Oracle RMAN
1003	Linux NDMP
1009	Linux DB2
1014	Linux Lotus
1016	Linux VMware image
1019	Linux VMware File Level Restore (FLR)
1024	Linux extended retention
1025	Linux extended retention restore

表 93 数値のプラグ イン ディスクリプター (続き)

ディスクリプター	プラグ イン名
1029	Linux Sybase
1030	Linux SAP
1034	Linux extended retention import
1035	Linux VDR Migration
1038	Linux VMware image restore
1039	Linux vApp image
2000	Oracle Solaris avagent
2001	Oracle Solaris avtar
2002	Oracle Solaris RMAN
2009	Oracle Solaris DB2
2014	Oracle Solaris Lotus
2029	Oracle Solaris Sybase
2030	Oracle Solaris SAP
3,000	Windows avagent
3001	Windows avtar
3002	Windows Oracle RMAN
3004	Windows Exchange message
3005	Windows Exchange database
3006	Windows SQL
3009	Windows DB2
3011	Windows Exchange 2007 database
3012	Windows Exchange 2007 web
3014	Windows Lotus
3015	Windows VSS
3016	Windows VMware image
3017	Windows MOSS
3018	Windows Exchange VSS
3019	Windows VMware File Level Restore (FLR)
3026	Windows MOSS VSS
3027	Windows Exchange Granular Level Restore (GLR)
3028	Windows MOSS Granular Level Restore (GLR)
3029	Windows Sybase
3030	Windows SAP

表 93 数値のプラグ イン ディスクリプター (続き)

ディスクリプター	プラグ イン名
3032	Windows Hyper-V VSS
3033	Windows Hyper-V Granular Level Restore (GLR)
3036	Windows cluster file system
3041	Windows VMware Granular Level Restore (GLR)
4,000	HP-UX avagent
4001	HP-UX avtar
4002	HP-UX Oracle RMAN
4009	HP-UX DB2
4029	HP-UX Sybase
4030	HP-UX SAP
5,000	IBM AIX avagent
5001	IBM AIX avtar
5002	IBM AIX Oracle RMAN
5009	IBM AIX DB2
5014	IBM AIX Lotus
5029	IBM AIX Sybase
5030	IBM AIX SAP
6000	Mac OSX avagent
6001	Mac OSX avtar
7003	NetApp NDMP
8003	EMC Celerra NDMP
10000	Novell NetWare avagent
10001	Novell NetWare avtar
10003	Novell NetWare NDMP
11000	FreeBSD avagent
11001	FreeBSD avtar
12000	SCO OpenServer avagent
12001	SCO OpenServer avtar
13000	SCO:UnixWare avagent
13001	SCO:UnixWare avtar
14003	EMC Isilon NDMP

CLI の使用例

avrepl コマンドの使用例を参照し、オプションを使用してレプリケーションの動作を制御する方法の詳細を確認してください。

avrepl コマンドでは次のオプションを指定します。

表 94 avrepl コマンドに必要なオプション

オプション	説明
<code>--operation=replicate</code>	avrepl のコマンド オペレーション。
<code>--[replscript]dpnname=source_server</code>	ソース Avamar サーバの完全修飾ドメイン名。
<code>--[avtar]id=user@auth</code>	ソース Avamar サーバのユーザー アカウント。デフォルト値は repluser です。repluser アカウントを使用するには、 <code>--[avtar]id</code> を省略して、 <code>repluser</code> オプションで <code>--password</code> アカウントのパスワードのみを指定します。
<code>--password=password</code>	ソース Avamar サーバ上のユーザー アカウントのパスワード。
<code>--[replscript]dstaddr=destination_server</code>	ターゲット Avamar サーバ。
<code>--[replscript]dstid=repluser</code>	ターゲット Avamar サーバの認証に使用する Avamar ユーザー ID とドメインを指定します。 注 repluser アカウントは、すべてのターゲット サーバでの信頼性の高い動作が認められている唯一のユーザー アカウントです。
<code>--dstpassword=password</code> <code>--dstap=password</code> <code>--dstpswd=password</code>	ターゲット Avamar サーバでの repluser アカウントのパスワードを指定します。

ターゲット サーバでファイアウォールがインストールおよび有効化されている場合は、`--[replscript]dstencrypt` または `ssl` のうち、適切な暗号化方式で `tls` オプションを指定します。

すべてのクライアント バックアップをレプリケートする

次のコマンドでは、すべてのクライアント バックアップが `avamar-1.example.com` ソース サーバから `replication-server-1.example.com` ターゲット サーバにレプリケートされます。ソース サーバのユーザー アカウントは `jdoue@avamar` (Avamar 内部認証システムによる `jdoue` ユーザー アカウント) であり、パスワードは `password` です。ターゲット サーバのユーザー アカウントは `repluser` であり、パスワードは `password` です。

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoue@avamar --
password=password --[replscript]dstaddr=replication-
server-1.example.com --[replscript]dstid=repluser --
dstpassword=password --[replscript]dstencrypt=ssl
```

特定のクライアントまたはドメインのバックアップをレプリケートする

次のコマンドでは、client1 と client2 のクライアントに加えて、domain3 ドメインのすべてのクライアントのすべてのバックアップがレプリケートされます。

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
password=password --[replscript]dstaddr=replication-
server-1.example.com --[replscript]dstid=repluser --
dstpassword=password --[replscript]dstencrypt=ssl client1 client2
domain3
```

特定のタイプのバックアップをレプリケートする

次のコマンドでは、client1 と client2 のクライアントで 2014 年 2 月 1 日より後に実行された、すべてのフル（レベル 0）バックアップがレプリケートされます。

```
avrepl --operation=replicate --
[replscript]dpnname=avamar-1.example.com --[avtar]id=jdoe@avamar --
ap=password --[replscript]dstaddr=replication-server-1.example.com --
[replscript]dstid=repluser --dstpassword=password --
[replscript]dstencrypt=ssl --[avtar]after=2014-02-01 --backup-
type=level0_full client1 client2
```

レプリケーションのモニタリング


レプリケーションが正常に実行されていることを確認したり、問題のトラブルシューティングを行ったりするには、レプリケーションを監視します。

AUI の **[Monitor]** > **[Activity]** ウィンドウにより、オン デマンドおよびスケジュール設定された両方のレプリケーション アクティビティに関するステータス情報を表示することができます。

AUI でのレプリケーションの監視

AUI の **[Activity]** ウィンドウにより、オン デマンドレプリケーション アクティビティとスケジュール設定されたレプリケーション アクティビティに関するステータス情報を表示することができます。

手順

1. 左側の AUI ナビゲーション ペインで、>> をクリックし、**[Monitor]** > **[Activity]** に移動します。
[Activity Monitor] が開き、すべてのアクティビティのリストが表示されます。レプリケーション ジョブは、**[Type]** 列の **[Replication Source]** を示します。さらに、ビューをフィルタリングして、レプリケーション ジョブのみを表示することもできます。
2. 結果をフィルタリングしてレプリケーション アクティビティのみを表示するには、次のようにします。
 - a. **[Type]** 列の横にある  をクリックします。
 - b. **Replication Source** と入力します。

AUI でのレプリケーション タスクのキャンセル

ポリシー ベースのレプリケーション タスクは、タスクの完了前であればいつでも、AUI の **[Activity]** ウィンドウでキャンセルできます。キャンセルは 5 分以上かかる場合があることに注意してください。ま

た、キャンセルが行われる前にレプリケーション タスクが完了した場合、タスクはキャンセルされません。

手順

1. AUI で、[**Monitor**] > [**Activity**] に移動します。
すべてのアクティビティのリストが表示されます。
2. [**Activity**] ウィンドウで、キャンセルするレプリケーション タスクを選択し、[**CANCEL**] をクリックします。
確認メッセージが表示されます。
3. [**YES**] をクリックします。

ターゲット システム上のレプリカからバックアップをリストアする

ターゲット サーバーの REPLICATE ドメインにあるクライアントから、レプリケートしたデータをリストアします。オリジナルのバックアップのソースであるクライアントを含めて、ターゲット サーバーでドメインのメンバーになっているクライアントはすべてリストア ターゲットにできます。

この方法を使用してレプリカからデータをリストアするのは、ソース Avamar サーバが使用不可になっているときと、Replicas at Source 機能がソース Avamar システムで有効になっていないときです。

注

リストアは、[**Avamar Administrator**] のみでサポートされます。

手順

1. リストア ターゲットになるクライアントを、レプリケートされたデータを管理するターゲット Avamar サーバに登録してアクティブ化します。
 - a. Windows クライアントで Avamar システム トレイ アイコンを右クリックして、[**Manage**] > [**Activate Client**] を選択します。
[**Activate Client Setup**] ダイアログ ボックスが表示されます。
 - b. ターゲット Avamar サーバのホスト名を [**Administrator Server Address**] ボックスに入力します。
 - c. **Administrator Server Port** ボックスに [**28001**] と入力します。
 - d. [**Client Domain**] ボックスに、クライアントの Avamar ドメインを入力します。
 - e. [**Activate**] をクリックします。
2. Avamar Administrator で、[**Backup & Restore**] 起動リンクをクリックします。
[**Backup, Restore and Manage**] ウィンドウが表示されます。
3. [**Restore**] タブをクリックします。
左上のパネルにドメインのリストが表示されます。
4. REPLICATE ドメインを選択して、ソース Avamar サーバのホスト名を選択します。
5. オリジナルのバックアップのソースになるクライアントが含まれているドメインを選択します。
6. リストからクライアントを選択します。
7. [**By Date**] タブまたは [**By File/Folder**] タブをクリックして、リストアするデータを選択します。

注

[バックアップからのデータのリストア \(154 ページ\)](#) では、バックアップを見つけてリストアを実行する別の方法について説明します。

8. **[Actions]** > **[Restore Now]** を選択します。
[Restore Options] ダイアログ ボックスが表示されます。
9. **[Restore Destination Client]** ボックスの横にある **[Browse]** をクリックして、リストアターゲットにするクライアントを見つけて選択します。
リストアターゲットとして REPLICATE ドメインにあるクライアントを選択しないでください。clients ドメインまたは Avamar サーバ上の別のドメインに表示されたクライアントを選択します。
10. **[Restore Plug-in]** リストからのリストアを使用するには、プラグ インを選択します。
11. **[Avamar encryption method]** リストから、リストア中のクライアント/サーバー間のデータ転送に使用する暗号化方式を選択します。

注

クライアント/サーバ接続に使用する暗号化テクノロジーとビット強度は、クライアント オペレーティング システムや Avamar サーバのバージョンなど、いくつかの要因によって変化します。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。

12. **[Restore everything to a different location]** または **[Restore everything to multiple locations]** を選択します。
13. **[Items Marked for Restore]** リストの下にある **[Set Destination]** をクリックして、データをリストアするターゲットパスを選択します。
14. このリストアにプラグ イン オプションを含めるには、**[More Options]** をクリックし、その設定を行います。
15. **[Restore Options]** ダイアログ ボックスで、**[OK]** をクリックします。
[Restore Request] ダイアログ ボックスに、リストアが開始されたことが表示されます。
16. **[Close]** をクリックします。
17. (オプション) リストアターゲット クライアントの登録をソース Avamar サーバに戻します。
ソース Avamar サーバを使用できる場合にこのステップを実行します。

Replicas at Source をサポートする MCS 構成パラメーター

mcserver.xml の構成パラメーターで Replicas at Source の MCS 管理を構成します。

[Replicas at Source の構成の変更 \(299 ページ\)](#) では、mcserver.xml の変更方法について説明します。次の表では、mcserver.xml の Replicas at Source パラメーターについて説明します。

表 95 Replicas at Source をサポートする MCS 構成パラメーター

コンテナ	パラメーター	デフォルト値	説明
repl	external_sync_interval_minute	120	ターゲットシステムからソース Avamar システム上の MCS データベースにレプリカ メタデータを同期化するインターバルを分数で設定します。 get_backups_from_external_server を true に設定すると、このパラメーターがオーバーライドされます。
repl	allow_dest_replica_management	false	リモートターゲットシステムとソース Avamar サーバの間でレプリカ メタデータの同期化を許可するには、true に設定します。同期化を無効化して結果的に Replicas at Source 機能を無効化するには、false に設定します。
repl	get_backups_from_external_server	false	デフォルトの動作をオーバーライドして、ターゲットシステムからレプリカ メタデータを直接取得するように MCS に強制するには、この値を true に設定します。デフォルトでは、MCS は定期的な同期化でレプリカ メタデータをターゲットシステムから取得します。この同期化で、メタデータはソース Avamar システム上のローカル MCS データベースに書き込まれます。Avamar Administrator はローカル データベースにアクセスしてレプリカ情報を表示します。
repl	show_external_backups	true	Restore タブのレプリカリストを有効化するには true に設定します。Restore タブのレプリカリストを無効化するには false に設定します。
ebms	ebms_home	lib/mcebms.war	外部バックアップ マネージャー サービスのために Web アーカイブ ファイルの場所を設定します。
ebms	ebms_descriptor	/WEB-INF/web.xml	外部バックアップ マネージャー サービスのために XML 記述子ファイルの場所を設定します。
ebms	ebms_port	9090	外部バックアップ マネージャー サービスのためにインバウンド (リスン) ポートを設定します。

表 95 Replicas at Source をサポートする MCS 構成パラメーター (続き)

コンテナ	パラメーター	デフォルト値	説明
ebms	ebms_use_https	true	外部バックアップ マネージャー サービスに、ターゲット システムとの通信に SSL/TLS 暗号化を使用することを強制するには、 true に設定します。
mon	ebmsIntervalMinutes	720	Remote Backup Manager Service の状態を確認するインターバルを分数で設定します。
mon	ebmsFailEventIntervalMinutes	120	Remote Backup Manager Service の stop イベントと fail イベントに関して更新情報を発行するインターバルを分数で設定します。
mon	ebmsMonitorTimeout	300	Remote Backup Manager Service の状態を確認しようとする時間を分数で設定します。
repl	allow_manage_remote_backups_at_source	true	ソース Avamar サーバでレプリカの管理を許可するには、 true に設定します。管理には、次のような作業があります。有効期限の削除、変更、保存の変更。ソース Avamar サーバでレプリカの管理を無効化するには、 false に設定します。

Replicas at Source の構成の変更

Replicas at Source 機能の構成を変更するには、`mcserver.xml` でパラメーター値を変更します。

このトピックでは、`mcserver.xml` で Replicas at Source 構成パラメーターを変更する方法について説明します。構成パラメーターの詳細については、[Replicas at Source をサポートする MCS 構成パラメーター \(297 ページ\)](#) を参照してください。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、**admin** としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. **admin** としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、**admin OpenSSH** キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. 次のコマンドを入力して、MCS を停止します。

```
dpnctl stop mcs
```

3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```

4. テキストエディターで `mcserver.xml` を開きます。
5. パラメーターのコンテナー エレメントを見つけて、そのエレメント内でパラメーターを見つけます。
6. パラメーターの値を変更します。
7. 変更を保存して、ファイルを閉じます。
8. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```

Replicas at Source のリストア

Avamar サーバーで **Replicas at Source** 機能を有効化している場合、Avamar Administrator では、バックアップがリストされている同じテーブルで、レプリカが **[Restore]** タブにリストされます。

Avamar Administrator の **[Restore]** タブを使用して、レプリカからデータを表示してリストアします。レプリカには次の情報が表示されます。

- **[Type]** 列に `Remote`
- **[Server]** 列ではリモートターゲットシステムの名前/IP アドレスとシステムタイプ

注

Avamar Administrator で `Local` と `Remote` の両方のバックアップデータがリストされた場合、Avamar システムは、データのリストアに常にローカル バックアップを使用します。ただし、`Remote` としてリストされたバックアップデータが検証のために選択された場合、Avamar システムは参照されるレプリカのステージングと検証を行います。

[Replicas at Source](#) (268 ページ) では、**Replicas at Source** 機能の詳細について説明します。

第 12 章

サーバー更新とホットフィックス

本章は、次のトピックで構成されています。

- [Avamar サーバ ソフトウェア アップデート プロセスの概要](#) 302
- [Avamar Downloader Service のインストールと構成](#) 305
- [EMC リポジトリから新しいパッケージをダウンロードする](#) 306
- [Avamar サーバでのパッケージのダウンロードおよびインストール](#) 306
- [Avamar サーバ上のインストール パッケージのリストの表示](#) 307
- [Avamar サーバからのパッケージの削除](#) 309
- [インストール履歴の表示](#) 310
- [レガシー Avamar Downloader Service の使用](#) 311
- [Avamar Downloader Service に関する問題のトラブルシューティング](#) 319

Avamar サーバ ソフトウェア アップデート プロセスの概要

Avamar では、Avamar サーバ ソフトウェアのアップデートおよびホットフィックスを定期的に提供しています。Avamar は、アップデート パッケージおよびホットフィックス パッケージを EMC リポジトリに格納します。Avamar Downloader Service を使用すると、インストール パッケージを Avamar サーバにダウンロードするか、またはローカルの Windows サーバにダウンロードして Avamar サーバにパッケージをプッシュすることが可能です。次に Avamar インストール マネージャーを使用して、Avamar サーバにパッケージをインストールします。

必要な場合、古いインストール パッケージを Avamar サーバのローカル リポジトリから削除した後で Avamar Downloader Service から再度ダウンロードすることも可能です。

インターネット アクセスが使用不可である場合、Avamar Downloader Service を使用する代わりに、ユーティリティ ノードまたはシングル ノード サーバの `/data01/avamar/repo/packages` ディレクトリに手動でパッケージをコピーします。次に Avamar インストール マネージャーを使用して、Avamar サーバにパッケージをインストールします。

Avamar Downloader Service

Avamar リリース 7.3 より前は、Avamar Downloader Service は個別のスタンドアロン Microsoft Windows コンピューターにインストールされました。Avamar リリース 7.3 以降、ダウンロード サービスも Avamar インストール マネージャーと統合され、Avamar サーバで利用可能です。レガシーのダウンロード サービスをスタンドアロン Microsoft Windows コンピューター上で使用するか、または Avamar インストール マネージャーと統合された新しいダウンロード サービスを使用することができます。

カスタマー サポートでは通常、Avamar サーバのインストールまたはアップグレード中に Avamar Downloader Service ソフトウェアをインストールします。また、Avamar Downloader Service を Avamar サーバから各自でダウンロードして、このソフトウェアをインストールすることも可能です。

EMC リポジトリ サーバへのアクセスに制限があるプライベート ネットワークに Avamar Downloader Service コンピューターが存在する場合は、Avamar Downloader Service コンピューターと EMC リポジトリ サーバ間の通信のためにプロキシ サーバをセットアップできます。

セキュリティ

Avamar Downloader Service は、HTTP 接続を介した SSL (Secure Socket Layers) を使用し、EMC リポジトリへの送信を暗号化します。Avamar Downloader Service は、ダウンロードした各パッケージを検証し、パッケージが正しく署名され、送信されたことを確認します。

レガシー Avamar Downloader Service

レガシーの Avamar Downloader Service コンピューターは、インターネット上の Avamar サイトおよびすべての内部 Avamar サーバへのネットワーク アクセスを可能にするスタンドアロン Microsoft Windows コンピューターです。

レガシー Avamar Downloader Service は Windows サービスとして実行され、EMC リポジトリを監視します。デスクトップ ショートカット、タスク トレイ アイコン、Windows のスタートメニュー アイテムから、レガシー Avamar Downloader Service ユーザー インターフェイスにアクセスし、これを使用してダウンロード サービスを構成し、EMC リポジトリでインストール パッケージを確認できます。Avamar Downloader Service モニタでは、サービスのステータス メッセージが表示されます。

レガシーの Avamar Downloader Service では、確認済みのシステム リストにある Avamar システムから受信する、インストール パッケージのリクエストのみを受け入れます。

ローカル リポジトリ

Avamar Downloader Service コンピューター上の `C:\Program Files\EMC\Avamar Downloader Service\repository` ディレクトリは、ダウンロードされたインストール パッケージのローカル リポジトリとして機能します。

注

クライアント インストール パッケージの名称を変更しないでください。Avamar プッシュ アップグレード メカニズムは、名称変更されたパッケージと互換性はありません。

ローカル リポジトリにある `manifest.xml` ファイルには、現在 EMC リポジトリからダウンロード可能なすべてのサーバー、クライアント、ワークフローのパッケージのリストが記載されています。

AvInstaller および Avamar インストール マネージャー

AvInstaller プロセスでは、Avamar サーバへのインストール パッケージのダウンロードおよびインストール処理を制御します。Avamar インストール マネージャープロセスを管理するには、AvInstaller を使用します。

インストール

カスタマー サポートでは、Avamar サーバのインストールまたはアップグレード中に AvInstaller をインストールします。AvInstaller は、マルチ ノード環境のユーティリティ ノード、またはシングル ノード環境のサーバ上にインストールします。

ローカル リポジトリ

AvInstaller は、Avamar ユーティリティ ノードまたはシングル ノード サーバ上の `/data01/avamar/repo/packages` ディレクトリを、ダウンロードされたインストール パッケージのローカル リポジトリとして使用します。AvInstaller はまた、インストール中にパッケージの展開に使用する一時ディレクトリも管理します。

新しいパッケージを使用できるかどうかを判断するために、Avamar Downloader Service は 1 日 1 回自動的にマニフェスト ファイルを EMC リポジトリからダウンロードします。レガシー Avamar Downloader Service が使用されている場合は、既知の Avamar システムごとに更新されたマニフェスト ファイルがローカル リポジトリに送信されます。AvInstaller はマニフェスト ファイルを使用して、EMC リポジトリからダウンロード可能なすべてのソフトウェア パッケージに関する現在の情報を取得します。

ユーザー インターフェイス

Avamar インストール マネージャーユーザー インターフェイスを使用して AvInstaller を管理します。Avamar インストール マネージャーは AvInstaller とともに自動的にインストールされます。Avamar インストール マネージャーは次の機能を提供します。

- Avamar Downloader Service 経由でソフトウェア パッケージをダウンロードします。
- Avamar サーバにパッケージをインストールします。
- Avamar サーバのリポジトリにあるソフトウェア パッケージのリストを表示します。
- ストレージの容量を確保するには、以前のインストール パッケージを Avamar サーバから削除します。
- Avamar サーバのソフトウェア インストール ヒストリを表示します。

AvInstaller プロセスのステータスの確認

AvInstaller プロセスのステータスを確認するには、

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、**admin** としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. **admin** としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、**admin OpenSSH** キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. **dpnctl status avi** と入力します。

`dpnctl status avi` コマンドからの出力は、次のようになります。

```
dpnctl: INFO: avinstaller status: up.
```

AvInstaller プロセスの停止

AvInstaller プロセスを停止するには、以下の手順を実行します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバの場合は、**admin** としてサーバにログインし、**su -** と入力してユーザーを **root** に切り替えます。
 - マルチ ノード サーバの場合は、**admin** としてユーティリティ ノードにログインし、**su -** と入力してユーザーを **root** に切り替えます。
2. **avinstaller.pl --stop** と入力します。
3. **avinstaller.pl --test** と入力して、AvInstaller プロセスが停止したかどうかを確認します。

`avinstaller.pl --test` コマンドからの出力は、次のようになります。

```
Avistart process:
INFO: AVI is not running.
```

AvInstaller プロセスの再起動

AvInstaller プロセスを再起動するには、次の手順を実行します。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバの場合は、**admin** としてサーバにログインし、**su -** と入力してユーザーを **root** に切り替えます。
 - マルチ ノード サーバの場合は、**admin** としてユーティリティ ノードにログインし、**su -** と入力してユーザーを **root** に切り替えます。
2. **avinstaller.pl --start** と入力します。
3. **avinstaller.pl --test** と入力して、AvInstaller プロセスが実行中かどうかを確認します。

avinstaller.pl --test コマンドからの出力は、次のようになります。

```
Avistart process pid:
INFO: AVI is running.
```

Avamar Downloader Service のインストールと構成

Avamar Downloader Service は Avamar ソフトウェア インストール処理の一環としてインストールされます。

[レガシー Avamar Downloader Service の使用](#) (311 ページ) には、スタンドアロンの Microsoft Windows マシン上にレガシーの Avamar Downloader Service ソフトウェアをインストールし構成する方法に関する情報が含まれています。

Avamar Downloader Service の構成

EMC リポジトリ サーバーからパッケージをダウンロードするには、使用する前に Avamar Downloader Service を構成します。構成タスクの一部で、プロキシ サーバ設定を指定して、Avamar サポートのログイン情報を提供します。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。
 - a. 次のように URL を入力します。


```
https://Avamar-server/avi
```

 ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能なホスト名です。

Avamar インストール マネージャーのログイン ページが表示されます。
 - b. **[User Name]** フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、**[Password]** フィールドにパスワードを入力します。
 - c. **[Login]** をクリックします。
2. **[Configuration]** をクリックします。

[Configuration] ウィンドウが開きます。
3. 製品の購入時に Avamar ライセンスとともに受け取った Avamar サポートの **[Username]** と **[Password]** を指定します。
4. (オプション) ダウンローダー サービスで、Avamar サポートと通信するときにプロキシ サーバがファイアウォールを通過する必要がある場合は、**[Enable Proxy]** を選択してプロキシ サーバを有効にします。プロキシ サーバのホスト名または IP アドレス、ポート番号を指定します。
 - a. プロキシ サーバのホスト名または IP アドレス、ポート番号を指定します。
 - b. プロキシ サーバに認証が必要な場合、プロキシ サーバの **[Username]** と **[Password]** を入力します。
5. **[Save]** をクリックします。

EMC リポジトリから新しいパッケージをダウンロードする

EMC リポジトリで新しいサーバー、クライアント、ワークフローの各パッケージを確認して、そのパッケージをインストールするためにダウンロードすることができます。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。

- a. 次のように URL を入力します。

```
https://Avamar-server/avi
```

ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能なホスト名です。

Avamar インストール マネージャーのログイン ページが表示されます。

- b. [User Name] フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、[Password] フィールドにパスワードを入力します。

- c. [Login] をクリックします。

2. [Configuration] をクリックします。

[Configuration] ウィンドウが開きます。

3. [Check for New Packages] をクリックします。

[Check for New Packages] ダイアログ ボックスが表示され、ステータス メッセージが表示されます。Avamar サーバーによって、EMC リポジトリ サーバーからローカル リポジトリにマニフェスト ファイルがダウンロードされます。次に、Avamar サーバーはマニフェスト ファイルを処理して、現在のサーバー構成に適用されるパッケージを判別します。

パッケージがダウンロード可能になると、各パッケージの定義に従って、[SW Releases]、[SW Upgrades]、[SW Updates]、[Maintenance] タブに表示されます。

4. [Check for New Packages] ダイアログ ボックスで [Close] をクリックします。

5. [SW Releases]、[SW Upgrades]、[SW Updates]、[Maintenance] タブのパッケージで、[Download] をクリックして、EMC リポジトリからパッケージを取得します。

Avamar サーバでのパッケージのダウンロードおよびインストール

Avamar インストール マネージャーを使用して、ソフトウェア パッケージ、パッチ、ホットフィックスをダウンロードしてインストールします。

はじめに

最低 2 GB の RAM を備えたコンピューターを使用してください。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。

- a. 次のように URL を入力します。

```
https://Avamar-server/avi
```

ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能なホスト名です。

Avamar インストール マネージャーのログイン ページが表示されます。

- b. **[User Name]** フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、**[Password]** フィールドにパスワードを入力します。
- c. **[Login]** をクリックします。
2. パッケージに **[Download]** ボタンが表示されている場合は、このボタンをクリックして、パッケージをローカルリポジトリにダウンロードします。
ダウンロードが完了すると、**[Download]** ボタンが **[Install]** ボタンと **[Delete]** ボタンに置き換わります。
3. インストールを開始するには、**[Install]** をクリックします。
パッケージの背景色が黄色に変わり、初期化が開始されます。初期化プロセスが完了すると、**[Installation Setup]** ページが表示されます。
4. インストール設定情報を入力します。
一部のパッケージでは設定情報が必要ありません。
5. 高度な設定を実行するには、**[Show advanced settings]** を選択します。
6. **[Continue]** をクリックします。

[Installation Progress] ページで、インストールのステータスが表示されます。

通知

パッケージのインストール中にブラウザを閉じた場合、インストールは停止しません。インストールのモニタリングを再開するには、ブラウザ ウィンドウを開き、Avamar インストール マネージャーにログインしてください。

7. すべてのインストールの指示に対応します。
インストールが完了すると、ワークフロー パッケージの **[Install]** ボタンが **[Run]** ボタンになります。**[Run]** ボタンにより、再度ワークフロー パッケージを実行することができます。

Avamar サーバ上のインストール パッケージのリストの表示

Avamar インストール マネージャーの **[Repository]** タブで、Avamar サーバのリポジトリにあるインストール パッケージのリストを表示します。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。
 - a. 次のように URL を入力します。
`https://Avamar-server/avi`
ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能なホスト名です。

Avamar インストール マネージャーのログイン ページが表示されます。
 - b. **[User Name]** フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、**[Password]** フィールドにパスワードを入力します。
 - c. **[Login]** をクリックします。
2. **[Repository]** をクリックします。
[Repository] タブが表示されます。

3. (オプション) 列の見出しをクリックして、リストに表示されているパッケージのソート順序をトグルすることができます。

Avamar サーバへのインストール パッケージのアップロード

[Repository] タブの [Package Upload] 機能を使用して、ローカル ハード ドライブ、またはフラッシュ ドライブなど接続されているその他のメディアから、Avamar サーバにパッケージをアップロードします。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。
 - a. 次のように URL を入力します。
`https://Avamar-server/avi`
 ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能なホスト名です。

 Avamar インストール マネージャーのログイン ページが表示されます。
 - b. [User Name] フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、[Password] フィールドにパスワードを入力します。
 - c. [Login] をクリックします。
2. [Repository] をクリックします。
 [Repository] タブが表示されます。
3. [Browse] をクリックし、アップロードするパッケージを選択します。

注

Internet Explorer ブラウザのバージョン 9~11 は、4 GB の最大アップロード サイズをサポートします。バージョン 6~8 では、2 GB の最大アップロード サイズをサポートします。

パッケージのアップロードが完了すると、自動的に [Repository] テーブルに表示されます。

Repository タブの見出し

Avamar サーバのリポジトリにあるパッケージが Avamar インストール マネージャーの [Repository] タブに表示されます。最近インストールされたパッケージはリストの最下部に表示されます。

次の表では、各パッケージで表示される情報について説明します。

表 96 Repository タブの情報

見出し	説明
FileName	パッケージの名前。
Status	パッケージのステータス : <ul style="list-style-type: none"> • [Waiting] : AvInstaller サービスがパッケージを EMC リポジトリにコピーしています。 • [Checksum] : AvInstaller サービスがパッケージのチェックサムを算出しています。

表 96 Repository タブの情報 (続き)

見出し	説明
	<ul style="list-style-type: none"> • [Unsigned] : AvInstaller サービスがパッケージのシグネチャを検証しています。 • [Extracting] : AvInstaller サービスがターボールからパッケージを展開しています。 • [Accepted] : パッケージが完全に EMC リポジトリにダウンロードされ、インストールの準備ができました。 • [Rejected] : 転送中に問題が発生したため、あるいは、ダウンロードは正常に完了したが、現在の状態のシステムには適用できなかったため、パッケージが拒否されました。
注	ステータスの簡単な説明。
Last Updated	最後にステータスが更新された日付と時刻。

Avamar サーバからのパッケージの削除

ソフトウェア パッケージのインストールが正常に完了した後、AvInstaller サービスによって、このパッケージが自動的に Avamar システムのリポジトリから削除されます。インストールされないパッケージを手動で削除します。

制限つきのパッケージを削除できるのは、カスタマー サポートのみです。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。
 - a. 次のように URL を入力します。

```
https://Avamar-server/avi
```

ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能な hostname です。

Avamar インストール マネージャーのログイン ページが表示されます。
 - b. **[User Name]** フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、**[Password]** フィールドにパスワードを入力します。
 - c. **[Login]** をクリックします。
2. **[Package List]** でパッケージを選択します。
3. パッケージの隣にある **[Delete]** ボタンをクリックします。

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。

インストール履歴の表示

Avamar サーバのソフトウェアのインストール、アップデート、ホットフィックスの歴史は、Avamar インストール マネージャーの **[History]** タブで確認できます。

手順

1. Web ブラウザを開いて、Avamar インストール マネージャーにログインします。
 - a. 次のように URL を入力します。
`https://Avamar-server/avi`
 ここで、Avamar-server は IP アドレス、または Avamar サーバの解決可能なホスト名です。

 Avamar インストール マネージャーのログイン ページが表示されます。
 - b. **[User Name]** フィールドに Avamar 管理者ユーザー アカウントのユーザー名を入力し、**[Password]** フィールドにパスワードを入力します。
 - c. **[Login]** をクリックします。
2. **[History]** をクリックします。
[History] タブが表示されます。
3. (オプション) リストに表示されているパッケージのソート順序をトグルするには、いずれかの列の見出しをクリックします。
4. (オプション) **[Show]** リストからフィルター値を選択し、パッケージのリストをフィルタリングします。
5. (オプション) リストにあるパッケージの詳細を表示するには、パッケージの行を選択します。
6. (オプション) 進行中のステータスにあるパッケージでログ ファイルを表示するには、**[Details]** テーブルで **[Logs]** をクリックします。
7. (オプション) **[Export]** をクリックして、ログ情報を Microsoft Excel または PDF ファイルにエクスポートします。

インストール履歴情報

[History] 列

次の表では、各パッケージの Avamar インストール マネージャー **[History]** タブで表示される情報について説明します。

表 97 **[History]** タブにある情報

見出し	説明
Title	パッケージの名前。
Version	Avamar サーバ ソフトウェアのバージョン。
Description	パッケージの簡単な説明。
Status	パッケージのステータス： <ul style="list-style-type: none"> • Available : パッケージはマニフェストにあり、ダウンロード可能です。

表 97 [History] タブにある情報 (続き)

見出し	説明
	<ul style="list-style-type: none"> • Completed : パッケージのインストールは完了しています。 • Processing : パッケージのインストールが進行中です。 • Ready : パッケージをインストールする準備ができています。 • Removed : パッケージは、Avamar グリッドから削除されています。
Last Updated	パッケージの最後のステータス更新が行われた日時。

[Details] 列

次の表では、[Details] テーブル ([History] タブの右下のパネルにある) の表示情報について説明します。

表 98 [History] タブの [Details]

[Details] テーブルの列見出し	説明
Status	パッケージのステータス詳細。 <ul style="list-style-type: none"> • Available : パッケージはマニフェストにあり、ダウンロード可能です。 • Ready : パッケージをインストールする準備ができています。 • Deployed : インストール初期化の開始。 • Deploying : パッケージ展開の開始。 • Processing : パッケージ インストールの開始。 • Completed : パッケージ インストールの完了。 • Removed : パッケージの削除。
Last Updated	パッケージ ステータス メッセージに対応する日付と時間。
Logs	進行中のステータスにあるパッケージで [Logs] ボタンが表示されます。 [Logs] をクリックすると、ウィンドウが開き、パッケージのインストールのために実行されたタスクの詳細が確認できます。

レガシー Avamar Downloader Service の使用

次のトピックでは、Microsoft Windows システムでレガシー Avamar Downloader Service ソフトウェアの準備、インストール、構成、使用を行う方法のほか、ソフトウェアのアップデートおよびアンインストールの方法について説明します。

レガシー Avamar Downloader Service のインストール要件

レガシー Avamar Downloader Service は 32 ビットまたは 64 ビットいずれかのアプリケーションで利用できます。Avamar サーバへのネットワーク アクセスを備えた Microsoft Windows サーバにレガシー Avamar Downloader Service をインストールします。このシステムはデスクトップまたはラップトップシステムのいずれかです。

次の表には、レガシー Avamar Downloader Service をインストールするコンピューターのインストール要件が挙げられています。

表 99 レガシー Avamar Downloader Service のインストール要件

ハードウェア/ソフトウェア	要件
オペレーティング システム	<ul style="list-style-type: none"> • Microsoft Windows Server 2016 • Microsoft Windows 10 • Microsoft Windows Server 2012 (64 ビットのみ) • Microsoft Windows Server 2008 R2 • Microsoft Windows 8 • Microsoft Windows 7 SP1
ファイル システム	任意のファイル システム
ハード ディスク ドライブの空き領域	12 MB (最小)
RAM	20 MB (最小)

Avamar の最新のリリースでは、TLS 1.2 のみをサポートしています。旧バージョンのオペレーティング システムでは、TLS 1.2 を有効化するための手順や更新が必要になる場合があります。詳細については、「Avamar 製品セキュリティ ガイド」を参照してください。

Windows 7、Windows 2008、Windows 2012 に対して TLS 1.2 を有効化するには、Microsoft サポート サイトのドキュメントを参照してください。

レガシー Avamar Downloader Service ソフトウェアのダウンロード

Avamar サーバの [**Avamar Web Restore**] ページからレガシー Avamar Downloader Service ソフトウェアをダウンロードします。

手順

1. Windows ホスト システムに管理者としてログインします。
2. Web ブラウザに次の Avamar サーバの URL を入力します。

`https://Avamar_server`

Avamar_server は Avamar システム ネットワークのホスト名 (DNS で定義されたもの) または IP アドレスです。

[**Avamar Web Restore**] ページが表示されます。

3. [**Downloads**] をクリックします。

[**Downloads**] リストが表示されます。

4. Windows コンピューターのプラットフォーム見出しの横にある **[+]** をクリックします。
5. Windows コンピューターのオペレーティング システム見出しの横にある **[+]** をクリックします。
6. **[AvamarDownloaderService-windows-platform-version.exe]** のリンクをクリックします。

各項目の意味は次のとおりです。

- **platform** は Windows プラットフォームのタイプ（32 ビットまたは 64 ビット）です。
- **version** は、Avamar サーバー ソフトウェアのバージョンです。

ファイルを実行するか、ファイルを保存するかを求めるダイアログ ボックスが表示されます。

7. インストール ファイルを一時ディレクトリに保存します。

レガシー Avamar Downloader Service ソフトウェアのインストール

手順

1. Windows ホスト コンピューターに管理者としてログインします。
2. **AvamarDownloaderService-windows-platform-version.exe** を含むディレクトリを参照し、このファイルをダブル クリックして、インストールを開始します。
[Microsoft Visual C++ 2010 Redistributable Maintenance] セットアップ アプリケーションが開きます。
3. 使用許諾契約書に同意してから、**[Install]** をクリックします。
Visual C++ランタイムがインストールされるまで待ちます。
4. **[Finish]** をクリックします。
セットアップ ウィザードが開き、最初に **[Welcome]** ページが表示されます。
5. **[Next]** をクリックします。
[Destination Folder] ページが表示されます。
6. Avamar Downloader Service インストール用にフォルダーを指定します。
 - デフォルトのフォルダーである `C:\Program Files\EMC\Avamar Downloader Service` を受け入れるには、**[Next]** をクリックします。
 - 別のフォルダーを指定するには、**[Change]** をクリックして、フォルダーを参照します。その後、**[Next]** をクリックします。**[Ready to install Avamar Downloader Service]** ページが表示されます。
7. **[Install]** をクリックします。
[Installing Avamar Downloader Service] ページが表示され、インストールの進行状況が表示されます。インストールが完了すると、**[Completed the Avamar Downloader Service Setup Wizard]** ページが表示されます。
8. **[Finish]** をクリックします。
インストールによって、コントロール パネルとシステム トレイに Avamar Downloader Service アイコンが追加されます。また、インストールによって、Windows サービスに AvamarDownloaderService も追加されます。

HTTPS の有効化

レガシーの Avamar Downloader Service をホスティングしている Microsoft Windows コンピューターで、HTTPS 機能を有効にする必要があります。状況によっては、コンピューターですでに

HTTPS が有効である可能性があります。有効になっていない場合は、コンピューターで次のステップを実行します。

手順

1. [コントロール パネル] > [Windows ファイアウォール] > [詳細設定] を選択します。
[セキュリティが強化された Windows ファイアウォール] コンソールが表示されます。
2. ナビゲーション ペインで、[送信の規則] をクリックします。
3. [操作] パネルで、[保存] をクリックします。
[新規の送信の規則ウィザード] が表示されます。
4. [ポート] を選択して [次へ] をクリックします。
5. [Specific remote ports] を選択して、テキスト ボックスに「443」と入力し、[Next] をクリックします。
6. [接続を許可する] をクリックし、[次へ] をクリックします。
7. デフォルトの設定を受け入れて、[次へ] をクリックします。
8. アウトバウンドの規則に名前（例えば、「Avamar Downloader Service」）を指定して、[Finish] をクリックします。
[New Outbound Rule Wizard] が表示されます。
9. [Outbound Rules] ペインで、前述で作成したアウトバウンドの規則（リストの一番上にあります）を右クリックして、[Properties] を選択します。
[Properties] ウィンドウが表示されます。
10. [プログラムおよびサービス] タブを選択します。
11. [設定] をクリックします。
12. [このサービスに適用する] を選択します。
13. サービスのリストから Avamar Downloader Service を選択し、[OK] をクリックします。
14. [適用] をクリックし、[OK] をクリックします。
15. [セキュリティが強化された Windows ファイアウォール] コンソールを閉じます。

レガシー Avamar Downloader Service の構成

EMC リポジトリ サーバーからパッケージをダウンロードするには、使用する前に Avamar Downloader Service を構成します。構成タスクには、接続の確認、既知のシステム リストの作成、プロキシ サーバー設定の指定などがあります。

はじめに

Avamar Downloader Service ソフトウェアをインストールします。

手順

1. Avamar Downloader Service コンピューターで、Avamar Downloader Service タスクトレイ アイコンを右クリックし、[Configure Service] を選択します。
Avamar Downloader Service 構成ウィザードが開き、最初に [Welcome] ページが表示されます。
2. (オプション) manifest.xml ファイルのローカル バージョンを使用するには、[Disable Internet access Use only local files] を選択します。
Avamar Downloader Service コンピューターがインターネット経由で EMC リポジトリに接続できない場合、このオプションを使用します。

3. 構成ウィザードの [Welcome] ページで [Next] をクリックします。
[Avamar Credentials] ページが表示されます。
4. このページでは、製品の購入時に Avamar ライセンスで受け取った Avamar サポートの [Username] と [Password] を指定（および確認）して、[Next] をクリックします。
[Proxy Configuration] ページが表示されます。

注

後で Avamar 認証情報を編集するには、タスクトレイアイコンを右クリックし、[Show Advanced Settings] を選択して、[Show Advanced Settings] ウィンドウを開きます。

5. (オプション) 次の Avamar 認証情報を指定して、さらにプロキシ サーバのホスト名または IP アドレス、およびポート番号を指定します：[Username]、[Password]、[Confirm Password]。

Avamar Downloader Service コンピューターから EMC リポジトリ サーバーへのリクエストのために、中継機能としてプロキシ サーバーを使用するには、プロキシ サーバー情報を指定します。またこのページでは、[Use Authentication] を選択できます。

たとえば、Avamar Downloader Service コンピューターがプライベート ネットワークにあり、EMC リポジトリ サーバーへのアクセスが制限されている場合に、プロキシ サーバーを使用します。

6. [Next] をクリックします。
[Avamar Systems] ページが表示されます。
7. [Add] をクリックします。
[Avamar Downloader Service - Add Known System] ダイアログ ボックスが表示されます。
8. 次のように、Avamar サーバのホスト名、ユーザー名、パスワードを指定します。
 - a. [Hostname] ボックスに Avamar サーバの IP アドレスまたはホスト名を入力します。
 - b. [Username] ボックスに root と入力して、Linux オペレーティング システムの root ユーザーを指定します。
 - c. [Password] および [Confirm password] ボックスに、root ユーザーのパスワードを入力します。
9. [OK] をクリックします。
構成プロセスでホスト名を解決できない場合は、参考メッセージが表示されます。[Yes] をクリックしてシステムを追加するか、[No] をクリックして追加操作をキャンセルします。オフラインのシステムなど、ホスト名が解決されていない場合も、システムを確認済みのシステムリストに追加できます。
10. 他の Avamar サーバを追加します。
11. すべての Avamar サーバを追加したら、[Next] をクリックします。
[Review Configuration] ページが表示されます。
12. 構成の詳細を確認し、[Finish] をクリックします。

必要条件

必要に応じて構成ウィザードを再度実行して、プロキシ サーバのホスト名、IP アドレス、ポート番号のいずれかを編集したり、確認済みのシステム リストを編集して、Avamar サーバの追加および削除を行ったりすることが可能です。

レガシー Avamar Downloader Service ソフトウェアのアップデート

Avamar Downloader Service を使用して、Avamar Downloader Service ソフトウェアのアップデートを確認し、アップデートをダウンロードおよびインストールします。

手順

1. Avamar Downloader Service のタスクトレイ アイコンを右クリックし、[**Check for Updates**] を選択します。

アップデートが利用可能な場合、メッセージ Update is ready to install が表示されます。

利用可能なアップデートがない場合は、Your software is up to date のメッセージが表示されます。

[**Avamar Downloader Service Updater**] ダイアログ ボックスが表示されます。

2. アップデートが利用可能な場合は、[**Install**] をクリックします。

Avamar Downloader Service のセットアップウィザードが表示されます。

3. プロンプトに従って、ウィザードを実行し、新しいソフトウェアビルドをインストールします。

レガシー Avamar Downloader Service のアンインストール

Windows の Avamar Downloader Service プログラムと機能コンソールで [] をアンインストールします。

手順

1. Avamar Downloader Service コンピューターで、実行中の全アプリケーションを閉じます。
2. Windows の [コントロール パネル] から [プログラムと機能] を開きます。
3. [名前] 列で Avamar Downloader Service を選択します。
4. [**Uninstall**] をクリックします。

結果

アンインストール プロセスにより、ファイル キャッシュ コンテンツや構成アイテムを含むすべてのファイルに加えて、Windows レジストリ エントリーが削除されます。Avamar Downloader Service

EMC リポジトリから新しいパッケージをダウンロードする

EMC リポジトリで新しいサーバー、クライアント、ワークフローの各パッケージを確認して、そのパッケージをインストールするためにダウンロードすることができます。

はじめに

Avamar Downloader Service のステータスが OK または Waiting for configuration であることを確認します。これ以外の場合、新しいパッケージをチェックすることはできません。

手順

1. Avamar Downloader Service のタスクトレイ アイコンを右クリックして、[**Check for New Packages**] を選択します。

[**Check for New Packages**] ダイアログ ボックスが表示され、ステータス メッセージが表示されます。Avamar Downloader Service によって、EMC リポジトリから Windows サーバのローカル リポジトリと、確認済みのシステム リストにある Avamar サーバにマニフェスト ファイルがダウンロードされます。

ステータス メッセージの横のチェックマークはプロセスが成功したことを示します。ステータス メッセージの横の X は処理が失敗したことを示します。

2. 失敗したプロセスの詳細を表示するには、ステータス メッセージの横にある X をダブル クリックします。
3. [**Check for New Packages**] ダイアログ ボックスで [**Close**] をクリックします。

ダウンロード可能なパッケージのリストを表示する

Avamar Downloader Service コンピューター上のリポジトリ フォルダーにある manifest.xml ファイルには、EMC リポジトリから現在ダウンロード可能なソフトウェア パッケージのリストが記載されています。

手順

1. Avamar Downloader Service のタスク トレイ アイコンを右クリックして、[**Open Repository**] を選択します。

Windows Explorer が開き、C:\Program Files\EMC\Avamar Downloader Service\Repository フォルダーが表示されます。そこに manifest.xml ファイルが含まれます。

2. manifest.xml を開いて、パッケージ情報を確認します。

パッケージ名には .avp のファイル名拡張子が使用されており、<filename>のタグ内に表示されます。

EMC リポジトリの接続性の表示

リポジトリ接続設定を編集した後、またはパッケージのダウンロードが失敗した後で、Avamar Downloader Service コンピューターが EMC リポジトリ サーバに接続できることを確認します。

手順

1. Avamar Downloader Service のタスク トレイ アイコンを右クリックして、[**Run Diagnosis**] を選択します。

プロセスのステータスは、[**Run Diagnosis**] ダイアログ ボックスに表示されます。ステータス メッセージの横にある [X] は、ネットワーク接続に問題があることを示します。障害の横に表示される [X] をクリックすると、[**Error Information**] ダイアログ ボックスでエラーの詳細が表示されます。

[**Run Diagnosis**] ダイアログ ボックスが表示され、ネットワーク接続を確認するプロセスが自動的に開始されます。

2. (オプション) この検証プロセスを完了前に停止するには、[**Stop System Check**] をクリックします。
3. 検証が完了したら、[**Close**] をクリックします。

Avamar Downloader Service ステータスのモニタリング

Avamar Downloader Service コンピューターにログインすると、自動的に Avamar Downloader Service モニターが起動します。このモニターを使用して、Avamar Downloader Service のステータスを表示します。

手順

- モニターのステータスを表示するには、Avamar Downloader Service タスクトレイアイコンにマウスを重ねます。

ポップアップ ウィンドウが開き、ステータス メッセージが表示されます。

次の表で、Avamar Downloader Service モニターのステータス メッセージについて説明します。

表 100 Avamar Downloader Service モニターのステータス メッセージ

ステータス メッセージ	説明
Avamar Downloader Service	デフォルト ステータス メッセージです。
Authentication Failure with the EMC Repository.	HTTP 基本認証に失敗しました。
Authentication Failure with one or more "Known Systems."	以下を含む HTTP 基本認証に失敗しました。 <ul style="list-style-type: none"> ▪ EMC リポジトリとの通信エラー。 ▪ SSL (Secure Socket Layers) ハンドシェイクエラー。 ▪ HTTP 接続の切断。 ▪ HTTP NAK (negatively acknowledged message)。
Failed communication with one or more "Known Systems."	考えられる原因 : <ul style="list-style-type: none"> ▪ SSL ハンドシェイク エラー。 ▪ HTTP 接続の切断。 ▪ HTTP NAK。
Failed file download from the EMC repository.	ファイル転送が中断された。
Failed file transfer to one or more known systems.	ファイル転送が中断された。
Network Error	HTTPS ブラウザ設定では、Avamar Downloader Service が Avamar オンライン サポート サイトからファイルをリクエストしないようになっています。
Out of space.	Avamar Downloader Service ファイル キャッシュがいっぱいです。ディスク領域を解放するため、ローカル リポジトリからファイルを削除してください。
Running.	サービスが実行中であり、すべての確認済みシステムおよび EMC リポジトリと通信中です。
Socket failure on host computer.	考えられる原因 :

表 100 Avamar Downloader Service モニターのステータス メッセージ (続き)

ステータス メッセージ	説明
	<ul style="list-style-type: none"> ■ ホスト コンピューターでソケット リソースが不足している。 ■ NIC のバインディングの問題。 ■ Winsock 内でデッドロックが発生している。
Waiting for configuration.	Avamar Downloader Service はインストール済みですが、構成されていません。

Avamar Downloader Service モニターの停止と起動

Avamar Downloader Service コンピューターにログインすると、自動的に Avamar Downloader Service モニターが起動します。

手順

- モニタを停止するには、Avamar Downloader Service タスクトレイ アイコンを右クリックし、[Exit] を選択します。
- モニタを起動するには、Windows の [Start] メニューを開き、[All Programs] > [Avamar Downloader Service version] > [Avamar Downloader Service Monitor] の順に選択します。

Avamar Downloader Service に関する問題のトラブルシューティング

Avamar Downloader Service に関する一般的な問題を解決します。

パッケージのダウンロードが失敗する

現象：ユーティリティ ノードまたはシングル ノード サーバーが Windows ホスト コンピューターにアクセスできません。またパッケージをダウンロードすると、以下のようなメッセージが表示されます。

The selected package cannot be downloaded.

解決策：ユーティリティ ノードで、IP アドレス、完全修飾ドメイン名、/etc/hosts コンピューターの短い名前を指定した行を Avamar Downloader Service ファイルに追加します。

基本的な入力：10.6.172.50 avamar-1.example.com avamar-1

一時的な IPv6 アドレスによるパッケージ ダウンロードの失敗

現象：Avamar Downloader Service がパッケージのダウンロードに失敗して、connection refused エラーが表示されました。

考えられる原因：一時的な IPv6 アドレスがすべてのオペレーティング システムで使用されています。connection refused エラーは一時的な IPv6 アドレスの使用により発生します。Windows Vista、Windows 2008 Server、最新版の Windows では一時的な IPv6 アドレスがデフォルトで使用されます。

解決策：この問題を回避するには、Avamar Downloader Service コンピューターで一時的な IPv6 アドレスをブロックします。netsh コンピューターのコマンド プロンプトで、次の各 Avamar Downloader Service コマンドを入力します。各 netsh コマンドを個別の行に入力します。

```
netsh interface ipv6 set privacy state=disabled store=activenetsh
interface ipv6 set privacy state=disabled store=persistentnetsh
interface ipv6 set global randomizeidentifiers=disabled
```

```
store=activenetsh interface ipv6 set global  
randomizeidentifiers=disabled store=persistent
```


第 13 章

Avamar Client Manager

本章は、次のトピックで構成されています。

- [Avamar Client Manager の概要](#) 322
- [Avamar Client Manager の起動](#) 325
- [グローバル ツール](#) 326
- [概要](#) 336
- [クライアント](#) 340
- [ポリシー](#) 358
- [キュー](#) 360
- [ログ](#) 361

Avamar Client Manager の概要

Avamar Client Manager は Web ベースの管理アプリケーションであり、大規模な事業や企業向けに Avamar クライアントの一元管理機能を提供します。Avamar Client Manager により、多数の Avamar クライアントを容易に管理できます。

Avamar Client Manager は、サポートされているネイティブ オペレーティング システム上の Avamar クライアントおよび VMware 仮想マシンで実行されているサポート対象のオペレーティング システム上の Avamar クライアントと連携して機能します。Avamar Client Manager は、仮想センター、仮想マシン、仮想プロキシ構成を介して Avamar クライアントと連携できません。Avamar Client Manager ユーザー インターフェイスでは、サポートされている Avamar クライアントが表示され、サポートされていないクライアントはすべて表示されません。

接続セキュリティ

コンピューターと Avamar サーバ間のデータ転送の安全を確保するために、HTTPS を使用して安全な接続を確立します。

この形式の HTTP プロトコルでは、送信前にメッセージが暗号化され、受信時に復号化されます。HTTPS は、すべてのログイン情報の転送、およびレジストレーションとアクティベーション操作時のすべてのデータ転送に使用されます。

標準の HTTP プロトコルを介したユーザー インターフェイスからの Avamar サーバへのアクセス試行は、平文の転送を防ぐために、すべて HTTPS にリダイレクトされます。

Apache Web サーバー認証

Avamar Client Manager ユーザー インターフェイスでは、セキュアな Web ページのみを使用しており、これらのページにアクセスする Web ブラウザでは認証に関する警告が表示されます。この警告は、Apache Web サーバにトラステッド公開鍵の証明書を実インストールすれば表示されません。このオプションは Avamar で提供されます。

「Avamar 製品セキュリティ ガイド」では、Apache Web サーバーのトラステッド公開鍵の証明書を取得し、インストールする方法について説明します。

session time-out 時間の編集

Web ブラウザと Avamar Client Manager サーバとの間で 72 時間以上インタラクションがない状態でセッションが実行されていると、Avamar Client Manager によってセッションが終了されます。セッションの自動タイムアウトによって、Avamar Client Manager からアクセス可能な資産のセキュリティが確保されます。タイムアウト時間は長くすることも短くすることもできます。

Avamar Client Manager がセッションを終了したら、セッションを実行していた Web ブラウザーのウィンドウまたはタブを閉じて Avamar Client Manager をリスタートします。コミット タスクが進行中の間、Avamar Client Manager はセッションを終了しません。

手順

1. コマンド シェルを開きます。
 - a. サーバーに admin としてログインします。
 - b. 次のコマンドを入力して、ユーザーを root に切り替えます。

```
su -
```

- c. グリッドの場合、次のコマンドを入力して、rootid OpenSSH キーをロードします。

```
ssh-agent bashssh-add /root/.ssh/rootid
```

2. 次のコマンドを入力して、EM Tomcat サーバーを停止します。

```
dpnctl stop emt
```

3. テキスト エディターで次のファイルを開きます。

```
/usr/local/avamar-tomcat/webapps/aam/WEB-INF/web.xml
```

4. `session-timeout` タグの値を新しい値（単位：分）に変更します。

次の例では、`session-timeout` タグがデフォルト値である 4320 分（72 時間）に設定されます。

```
<session-config>
  <session-timeout>4320</session-timeout>
</session-config>
```

5. ファイルを保存して閉じます。
6. 次のコマンドを入力して、EM Tomcat サーバーを開始します。

```
dpnctl start emt
```

JavaScript time-out 時間の増加

Avamar Client Manager ユーザー インターフェイスでは、JavaScript を使用して、多くのタスクを実行します。場合によっては、Avamar Client Manager ユーザー インターフェイスのスクリプトが完了するには、Web ブラウザのデフォルトのスクリプトの `time-out` 値で許可されている時間よりも長くかかることがあります。

このような場合、メッセージが表示され、スクリプトが停止します。[Continue] をクリックすると、スクリプトの実行を完了できます。

このメッセージが表示されないようにするには、スクリプトの `time-out` 時間を増やします。ステップは Web ブラウザーによって異なります。

Windows の Internet Explorer で JavaScript の time-out 時間を増やす

手順

1. `Regedt32.exe` などのレジストリ エディターを開きます。
2. 次のレジストリ キーを開きます。

```
HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer
\Styles
```

キーが存在しない場合、作成します。

3. このキーに `MaxScriptStatements` という DWORD 値を作成します。
4. DWORD の値を 20,000,000 に設定します。
この数字は、スクリプトのステートメントを表します。
5. Web ブラウザーを再起動します。

Firefox での JavaScript の time-out 時間の増加

手順

1. ブラウザーのアドレスバーに `about:config` と入力します。
警告メッセージが表示されます。
2. **[I'll be careful, I promise!]** をクリックします。
[Preferences] ウィンドウが表示されます。
3. **[Filter]** で `dom.max_script_run_time` と入力します。
スクリプトの実行時間設定が表示されます。
4. 設定をダブルクリックします。
[Enter integer value] ダイアログ ボックスが表示されます。
5. 30 と入力して **[OK]** をクリックします。
6. ブラウザーを再起動します。

Avamar Client Manager の構成プロパティ

Avamar Client Manager では通常、デフォルトの構成に変更を加える必要はありません。ただし、特定の展開の要件に適合するように一部のプロパティを調整できます。

Avamar Client Manager のプロパティは `/usr/local/avamar/etc/acm.properties` ファイルにあります。

次の表は、プロパティに関する詳細を示します。

表 101 Avamar Client Manager の構成プロパティ

プロパティ	説明	デフォルト値
<code>activation.retry.attempts</code>	アクティベーションを失敗と見なすまでクライアント アクティベーションのアクティブ化を試行する回数。	24
<code>activation.retry.frequency.minutes</code>	クライアント アクティベーションの試行間の分数。	120
<code>move.getactivities.retry.attempts</code>	クライアントが非アクティブであるかどうかを決定するチェックの回数 (この結果、移動が可能)。	7
<code>move.getactivities.frequency.seconds</code>	クライアントが非アクティブであるかどうかを決定する各チェック間の秒数 (この結果、移動が可能)。	5
<code>move.queue.error.codes</code>	移動タスクの失敗をキューに追加するかどうかを決定する、エラー コードのコンマ区切りリストを設定します。移動の失敗によりこれらのエラー コードのいずれか 1 つが生成される場合、その移動はキューに追加されます。none の値を使用すると、失敗したすべての移動タスクがキューに追加されなくなります。empty の値を使用すると、失敗したすべての移動タスクがキューに追加されます。	22271、22280、22282、22295、30006、30012、30016、30017、30019
<code>move.retry.attempts</code>	失敗した移動タスクの再試行の回数を設定します。	24
<code>move.retry.frequency.minutes</code>	再試行の間の時間のスパンを設定します (単位: 分)。	120
<code>orgu.name.append.domain</code>	ユーザー インターフェイスの [Client Information] 領域に表示されるクライアントが、クライアント ホスト名ま	true

表 101 Avamar Client Manager の構成プロパティ (続き)

プロパティ	説明	デフォルト値
	たは完全修飾ドメイン名のいずれを使用して表示されるかを決定します。デフォルト値は各クライアントの完全修飾ドメイン名を表示します。	
toolbar.displaytime.client	Avamar Client Manager 内に表示される時間を、Web ブラウザのホスト コンピューターのタイムゾーンにするか、Avamar サーバのタイムゾーンにするかを決定します。デフォルト値は Web ブラウザのホスト コンピューターのタイムゾーンを使用します。	true
upgrade.freeform.flags	作業オーダーのアップグレードのためにキー/値フラグを渡すことができます。値は、KV ペアのコンマ区切りリストです。例： upgrade.freeform.flags=key1=val1, key2=val2, key3=val3	デフォルト値なし

Avamar Client Manager の構成プロパティの変更

手順

1. コマンド シェルを開きます。
 - a. サーバーに admin としてログインします。
 - b. 次のコマンドを入力して、ユーザーを root に切り替えます。

```
su -
```
 - c. グリッドの場合、次のコマンドを入力して、rootid OpenSSH キーをロードします。

```
ssh-agent bashssh-add /root/.ssh/rootid
```
2. 次のコマンドを入力して、現在の作業ディレクトリを変更します。

```
cd /usr/local/avamar/etc
```
3. Avamar Client Manager のプロパティ ファイルである acm.properties をテキスト エディタで開きます。
4. プロパティの値を編集します。
5. ファイルを保存して閉じます。
6. 次のコマンドを入力して、EM Tomcat サーバーを再開します。

```
dpnctl stop emt
dpnctl start emt
```

Avamar Client Manager の起動

Web ブラウザに Avamar Client Manager URL を入力して Avamar Client Manager を起動します。Avamar Client Manager は Backup & Recovery Manager で起動することもできます。

手順

1. Web ブラウザを開き、次の URL を入力します。

`https://Avamar_server/aam`

ここで、Avamar_server は、Avamar Client Manager プロセスを実行している Avamar サーバの解決可能なホスト名または IP アドレスです。

2. [User Name] に、Avamar サーバの管理者アカウントのユーザー名を入力します。
3. [Password] に、アカウントのパスワードを入力します。

結果

Avamar Client Manager は、[Overview] ページの [Server Summary] セクションを開きます。

ログイン ページ

ログイン ページは、ユーザー名とパスワードを要求することで Avamar Client Manager UI へのアクセスを制限します。

[ログイン] ページでは、Avamar サーバに登録されている管理者アカウントと比較してユーザー名とパスワードを認証します。Avamar Client Manager にアクセスできるのは、Avamar Client Manager プロセスを実行している Avamar サーバで管理者権限を持つアカウントのみです。

正常にログインすると、Avamar Client Manager UI が開かれて [Overview] ページの [Server Summary] セクションが表示されます。

グローバル ツール

Avamar Client Manager には、複数のページで使用できるツールがいくつかあります。

これらのツールは、以下のタスクに便利です。

- Avamar サーバの追加
- Avamar サーバの削除
- Avamar サーバの設定の変更
- 作業する Avamar サーバの選択
- ページのサマリー表示のフィルター
- 詳細に関連したコンテキストの表示
- ページからの情報のエクスポート
- ツール チップの有効化

Avamar サーバの追加

Avamar サーバの Avamar クライアントを管理できるようにするには、Avamar サーバを Avamar Client Manager に追加します。

はじめに

次の情報を確認します。

- 名前解決できる Avamar サーバのホスト名または IP アドレス。
- Avamar サーバのインバウンド RMI ポート。

- Avamar サーバの MCUser アカウントのパスワード。

手順

1. [Overview] ページの [Server Summary] セクションを参照します。
2. [Add Server] をクリックします。
[Add Server] ウィンドウが表示されます。
3. [System name (or) IP] に、名前解決できる Avamar サーバのホスト名または IP アドレスを入力します。
4. [Port] に Avamar サーバのインバウンド RMI ポートを入力します。
このフィールドには、デフォルト値の 9443 が表示されます。デフォルト以外のポートが Avamar サーバで使用されている場合を除いて、デフォルト値は変更しないでそのままにしてください。
5. [MCUser Password] に、Avamar サーバの MCUser アカウントのパスワードを入力します。
6. [Save] をクリックします。

結果

Avamar Client Manager が値を確認して Avamar サーバを追加します。

Avamar サーバの削除

Avamar サーバの Avamar クライアントを管理できないようにするには、Avamar サーバを Avamar Client Manager から削除します。

手順

1. [Overview] ページの [Server Summary] セクションを参照します。
2. 削除する Avamar サーバを選択します。
Avamar Client Manager プロセスをホストしている Avamar サーバは削除できません。
3. [Remove Server] をクリックします。
警告ダイアログ ボックスが表示されます。
4. [Yes] をクリックします。

結果

Avamar Client Manager は、選択された Avamar サーバを管理サーバのグループから削除します。

Avamar サーバの設定の変更

Avamar サーバでインバウンド RMI ポートまたは MCUser アカウントのパスワードを変更すると、Avamar Client Manager で Avamar サーバを管理できなくなります。Avamar Client Manager による管理を再び有効化するには、Avamar サーバの格納された設定を編集します。

はじめに

次の情報を確認します。

- Avamar サーバの新しいインバウンド RMI ポート。
- Avamar サーバの MCUser アカウントの新しいパスワード。

手順

1. Avamar サーバのすべてのアクティビティを一時停止します。
サーバー アクティビティの一時停止と再開 (182 ページ) では、Avamar サーバのアクティビティを一時停止する方法を説明しています。
2. [Overview] ページの [**Server Summary**] セクションを参照します。
3. Avamar サーバーを選択します。
4. [**Edit Server**] をクリックします。
[Edit Server] ウィンドウが表示されます。
5. [**Port**] に、選択した Avamar サーバのインバウンド RMI ポートを入力します。
6. [**MCUser Password**] に、選択した Avamar サーバの MCUser アカウントのパスワードを入力します。
7. [**Save**] をクリックします。

結果

Avamar Client Manager が値を確認して、Avamar サーバの管理を再び有効化します。

サーバーの選択

特定サーバーの情報を表示して作業を行うには、[**Server Selection**] フィールドを使用します。

はじめに

ユーザー インターフェイスの左側の [**Navigation**] パネルを拡張すると、パネルの上部にサーバ選択フィールドが表示されます。サーバー選択フィールドが選択可能なアクティブ状態で表示されているページを参照します。

手順

1. サーバー選択フィールドの矢印のアイコンをクリックします。
 サーバ選択フィールドが表示されない場合は、ユーザー インターフェイスの左側の [**Navigation**] パネルを拡張します。サーバー選択フィールドが現在のページの表示に関連していない場合は、グレー表示の状態が表示されます。この場合、アクティブ状態ではないため、選択はできません。
2. サーバーのリストから、サーバーを選択します。
 ページの表示が更新されます。サーバーとそのタスクに関する情報が表示されます。

フィルター

Avamar Client Manager には、広範囲にわたるフィルターがあります。

現在のページにリストするオブジェクトの決定にフィルターを使用します。フィルターは多くのオブジェクトと組み合わせることができます。オブジェクトのタイプと使用できるフィルターは、そのページのコンテキストによって異なります。Avamar Client Manager でフィルターできるオブジェクトのタイプは、以下のとおりです。

- サーバ
- クライアント
- ポリシー
- グループ
- タスク

- ログ エントリー

現在のコンテキストに適用されているフィルターは、ページ上部の [Filters] バーに表示されます。

名前による検索

検索文字列をオブジェクト名と比較してオブジェクトを検索するには、[Search] フィールドを使用します。

はじめに

[Filters] バーに次の検索可能フィールドの 1 個が表示されているビューを参照します。

- User name
- クライアント名
- [Group name]
- Domain name

リストを同一または類似した名前のオブジェクトに限定するには、検索を使用します。

手順

1. 検索可能フィールドの横にある矢印をクリックします。

テキスト入力ボックスが表示されます。

2. テキスト入力ボックスに検索する文字列を入力します。

Avamar Client Manager は、入力された検索文字列をオブジェクトの名前と比較して、一致したオブジェクトをリストに含めます。一致したオブジェクトとは、名前の一部に検索文字列が含まれているオブジェクトです。

3. 拡大鏡アイコンをクリックします。

結果

Avamar Client Manager がリストを更新して、検索文字列に一致する名前が付いたオブジェクトのみが表示されます。

例 1 ユーザー名での検索

ユーザー名に「eng」という文字を含むユーザーを持つすべてのクライアントを含めるには、テキスト入力フィールドに*eng*と入力します。

必要条件

(オプション) 検索文字列を削除してすべてのオブジェクトを表示するには、テキスト エントリー フィールドの横の [X] をクリックします。

検索文字列のルール

検索文字列とは、名前検索フィールドに入力する 1 つ以上の文字です。Avamar Client Manager は、検索文字列をすべてのオブジェクト名と比較します。検索文字列がオブジェクト名の全体または一部と一致すると、Avamar Client Manager はそのオブジェクト名を結果に追加します。

検索文字列のルールは以下のとおりです。

- 最大 24 文字
- アスタリスク (*) 文字は、0 文字または 1 文字以上の文字列を表すために使用できます。
- ピリオド文字で始めることはできません。

- 次の表の「文字」列に挙げられた文字はすべて含めることはできません。

表 102 検索文字列に使用できない文字

文字	名称	Unicode
/ ^a	斜線	002F
:	コロン	003A
;	セミコロン	003B
?	疑問符	003F
"	引用符	0022
<	小なり記号	003C
>	大なり記号	003E
\	逆の斜線	005C
,	コンマ	002c
~	チルダ	007E
!	感嘆符	0021
@	単価記号	0040
#	番号記号	0023
\$	ドル記号	0024
%	パーセント記号	0025
^	サーカムフレックス アクセント	005E
	縦線	007C
&	アンパサンド	0026
'	アポストロフィ	0027
`	グレーブ アクセント	0060
(左括弧	0028
)	右括弧	0029
{	左波括弧	007B
}	右波括弧	007D
[左角括弧	005B
]	右角括弧	005D

- a. この除外ルールの例外として、[Policies] ページの [Domain Name] フィルターで斜線を使用できません。

アクティビティ タイプ フィルターの使用

リストのオブジェクトをあるタイプのアクティビティに限定するには、アクティビティ タイプ フィルターを使用します。

はじめに

[Filters] バーに [Activity Type] が含まれるビューを参照します。

手順

1. **[Filters]** バーで、**[Activity Type]** の横の矢印をクリックします。
次の値を含む選択リストが表示されます。**[Backup]** および **[Restore]**。
2. 値を選択します。
バックアップ タスクのみをリストする場合は、**[Backup]** を選択します。リストア タスクのみをリストする場合は、**[Restore]** を選択します。

例えば、**[Clients]** ページの **[Idle Clients]** セクションで、**[Activity Type]** フィルターから **[Backup]** を選択します。Avamar Client Manager が、定義された期間中にバックアップ アクティビティが一切ないクライアントだけにリストを限定します。

結果

Avamar Client Manager は、選択したアクティビティタイプを使用して結果をフィルターします。

クライアント ステータス フィルターの使用

指定されたクライアント ステータスのクライアントをリストに追加するには、クライアント ステータス フィルターを使用します。

はじめに

[Filters] バーに **[Client Status]** が含まれるビューを参照します。

手順

1. **[Filters]** バーで、**[Client Status]** の横の矢印をクリックします。
そのコンテキストのすべてのクライアントに対するクライアント ステータスの選択リストが表示されます。
2. ステータスを選択します。
例えば、**[Clients]** ページの **[Add Clients]** セクションで、**[Client Status]** フィルターから **[Activation Failure]** を選択します。Avamar Client Manager が、最低 1 回はアクティベーションの試みに失敗したことのある登録済みコンピューターにリストを限定します。Avamar Client Manager がリストを更新します。選択したクライアント ステータスのエントリーのみがリストに表示されます。
3. (オプション) これらのステップを繰り返して、追加のステータスを選択します。

結果

Avamar Client Manager がリストを更新します。選択したクライアント ステータスのエントリーのみがリストに表示されます。

故障基準フィルターの使用

Avamar Client Manager が失敗クライアントのリストに含めるクライアントを定義するには、故障基準フィルターを使用します。

はじめに

[Filters] バーに **[Failure Criteria]** が含まれるビューを参照します。

手順

1. **[Filters]** バーで、**[Failure Criteria]** の横の矢印をクリックします。
次の値を含む選択リストが表示されます。**[At least one activity failed]**、**[All activities failed]**、**[Last activity failed]**。
2. 値を選択します。

選択した値によって、Avamar Client Manager が失敗クライアントのリストに含まれるクライアントが判断されます。Avamar Client Manager は、選択したアクティビティ ステータスに一致したクライアントのみを含めます。

例えば、[**Last activity failed**] を選択します。Avamar Client Manager がリストを更新し、最も直近のアクティビティが失敗したクライアントのみを含めます。失敗アクティビティはバックアップでもリストアでもかまいません。

結果

Avamar Client Manager がリストを更新します。アクティビティ ステータスが選択した値と一致するクライアントのみが、リストに表示されます。

OS フィルターの使用

リストを特定オペレーティング システムのクライアントに限定するには、OS フィルターを使用します。

はじめに

[**Filters**] バーに [**OS**] が含まれるビューを参照します。

手順

1. [**Filters**] バーで、[**OS**] の横の矢印をクリックします。
そのコンテキストのすべてのクライアントの OS バージョンのリストが表示されます。
2. OS のバージョンを選択します。
Avamar Client Manager がリストを更新します。選択した OS バージョンのクライアントのみがリストに表示されます。
3. (オプション) 追加の OS バージョンを選択するには、これらのステップを繰り返します。

結果

Avamar Client Manager がリストを更新します。選択した OS バージョンのクライアントのみがリストに表示されます。

期間フィルターの使用

表示結果をカレンダーの日付で区切るには、期間フィルターを使用します。

はじめに

[**Filters**] バーに [**Period**] が含まれるビューを参照します。

手順

1. [**Filters**] バーで、[**Period**] の横の矢印をクリックします。
次の値を含む選択リストが表示されます。[**Before**]、[**After**]、[**On**]。
2. 値を選択します。
3. 選択した値の横の矢印をクリックします。
日付エントリー フィールドと小さなカレンダー アイコンが表示されます。
4. カレンダー アイコンをクリックして特定の日付を参照し、日付をクリックします。
または、日付エントリー フィールドに m/d/yy というフォーマットで日付を入力して拡大鏡のアイコンをクリックします。
Avamar Client Manager がリストを更新します。指定した期間のエントリーのみがリストに表示されます。
5. (オプション) 他の値を使用してこれらのステップを繰り返し、さらに結果を絞り込みます。

結果

Avamar Client Manager がリストを更新します。指定した期間のエントリーのみがリストに表示されます。

ステータス フィルターの使用

リストを特定ステータスのエントリーに限定するには、ステータス フィルターを使用します。

はじめに

[Filters] バーに [Status] が含まれるビューを参照します。

手順

1. [Filters] バーで、[Status] の横の矢印をクリックします。
そのコンテキストのすべてのエントリーに対する全ステータスの選択リストが表示されます。
2. ステータスを選択します。
Avamar Client Manager がリストを更新します。選択したステータスのエントリーのみがリストに表示されます。
3. (オプション) 追加のステータスを選択するには、これらのステップを繰り返します。

結果

Avamar Client Manager がリストを更新します。選択したステータスのエントリーのみがリストに表示されます。

ステータス コード フィルターの使用

リストを特定ステータス コードのエントリーに限定するには、ステータス コード フィルターを使用します。

はじめに

[Filters] バーに [Status Code] が含まれるビューを参照します。

手順

1. [Filters] バーで、[Status Code] の横の矢印をクリックします。
そのコンテキストのすべてのエントリーに対するステータス コードの選択リストが表示されます。
2. ステータス コードを選択します。
Avamar Client Manager がリストを更新します。選択したステータス コードを持つエントリーのみがリストに表示されます。
3. (オプション) 追加のステータス コードを選択するには、これらのステップを繰り返します。

結果

Avamar Client Manager がリストを更新します。選択したステータス コードのエントリーのみがリストに表示されます。

成功基準フィルターの使用

Avamar Client Manager が成功クライアントのリストに含めるクライアントを定義するには、成功基準フィルターを使用します。

はじめに

[Filters] バーに [Success Criteria] が含まれるビューを参照します。

手順

1. **[Filters]** バーで、**[Success Criteria]** の横の矢印をクリックします。
次の値を含む選択リストが表示されます。**[At least one activity successful]**、**[All activities successful]**、**[Last activity successful]**。
2. 値を選択します。
選択した値によって、Avamar Client Manager が成功したクライアントのリストに含むクライアントが判断されます。Avamar Client Manager は、選択したアクティビティ ステータスに一致したクライアントのみを含めます。
例えば、**[Last activity successful]** を選択します。Avamar Client Manager によって、リストが更新され、バックアップまたはリストアが成功したクライアントのみが表示されます。

結果

Avamar Client Manager がリストを更新します。アクティビティ ステータスが選択した値と一致するクライアントのみが、リストに表示されます。

バージョン フィルターの使用

リストを、Avamar クライアント ソフトウェアの特定バージョンのクライアントに限定するには、バージョン フィルターを使用します。

はじめに

[Filters] バーに **[Version]** が含まれるビューを参照します。

手順

1. **[Filters]** バーで、**[Version]** の横の矢印をクリックします。
そのコンテキストのすべてのクライアントに対する Avamar クライアント ソフトウェア バージョンの選択リストが表示されます。
2. バージョンを選択します。
Avamar Client Manager がリストを更新します。選択したソフトウェア バージョンのクライアントのみがリストに表示されます。
3. (オプション) 追加のソフトウェア バージョンを選択するには、これらのステップを繰り返します。

結果

Avamar Client Manager がリストを更新します。選択したソフトウェア バージョンのクライアントのみがリストに表示されます。

詳細の表示

コンテキスト関連の詳細を表示するには、**[Details]** パネルを使用します。

はじめに

[Details] パネル、または右側に **[Details]** バーが含まれるビューを参照します。

手順

1. ページの右側で、**[Details]** バーをクリックします。
[Details] パネルが拡張します。
2. **[Summary]** からオブジェクトを選択します。
ページのコンテキストにより、オブジェクト タイプが決まります。オブジェクトは、クライアントでもグループでもかまいません。複数のオブジェクトを選択できます。

選択したオブジェクトの詳細情報が [Details] パネルに表示されます。

3. (オプション) 複数のオブジェクトを選択する場合、[Details] パネル下部のページングコントロールを使用して各選択オブジェクトの情報を表示します。

データのエクスポート

選択したサマリーを Excel スプレッドシートにダウンロードするには、エクスポートを使用します。

はじめに

ページ バーに [Export] が含まれるページビューを参照します。

手順

1. ページ バーで、[Export] をクリックします。
Avamar Client Manager が、サマリーのすべての情報をエクスポートデータに含めます。
Web サーバーが、サマリー情報の入った Excel ファイルをブラウザにプッシュします。
2. ファイルをローカルに保存します。
3. ファイルを開くには、Excel フォーマットのスプレッドシートを読み取ることができるアプリケーションを使用します。

1 ページのエントリー数の制限の設定

サマリー リストに表示されるエントリー数の制限値を増やします。

デフォルトでは、Avamar Client Manager はサマリー リストを 1 ページ 25 エントリーに制限しています。エントリー数が現在の 1 ページの制限を超える場合は、複数ページにわたってエントリーが表示されます。多くのエントリーを見やすくするために、1 ページのエントリー数の制限を増やすことができます。

手順

1. Avamar Client Manager 下部のステータス バーで、[Entries Per Page] をクリックします。
選択したリストが表示されます。
2. リスト上の番号をクリックします。

結果

Avamar Client Manager は、選択した数を新しい制限値として設定し、ページを更新します。

ツールチップの表示

ユーザー インターフェイスのさまざまなエレメントに対する簡潔なヘルプ メッセージを表示するには、ツールチップを有効化して表示します。

手順

1. Avamar Client Manager 下部のステータス バーから、[Show Tooltips] を選択します。
2. ツールチップがあるユーザー インターフェイス エレメント上にポインターを移動します。
ツールチップがあるエレメントは次のとおりです。

- Dashboard chart sections
- Controls

- Column headings

概要

[Overview] ページでは、Avamar クライアントの管理に関する高度な情報へのアクセスを提供します。また Avamar サーバの管理者向けにツールを提供します。

[Overview] ページの左側のメニューから、

- **[Server Summary]**
選択した Avamar サーバの情報表示、Avamar サーバの追加、Avamar サーバの削除、Avamar サーバの設定の編集を行う場合は、**[Server Summary]** を選択します。
- [ダッシュボード]
選択した Avamar サーバのクライアント バックアップの情報を表示するには、**[Dashboard]** を選択します。

サーバ サマリー

[Overview] ページの **[Server Summary]** セクションには、Avamar Client Manager で管理する Avamar サーバに関する情報の列が表示されます。

[Filters] バーから使用可能なフィルターを使用すれば、この情報をフィルタリングできます。列見出しをクリックすれば、リストのソート方法を変更できます。

次の各列で、非ゼロ値をクリックすると、その列の情報に関するより詳細なレポートが表示されます。

- Active Clients
- アイドル状態のクライアント
- Successful Clients
- Failed Clients

[Server Summary] 列

次の表では、[Overview] ページの **[Server Summary]** セクションで使用される列について説明します。

表 103 [Server Summary] セクションで使用される列

列	説明
Server	Avamar サーバのホスト名または IP アドレス。
Version	Avamar サーバにインストールされる Avamar サーバ ソフトウェアのバージョン。
Total Clients	Avamar サーバに登録されている合計クライアント数。廃棄されたクライアントを含まない。
Active Clients	指定期間中にアクティビティ（バックアップまたはリストア）を行った合計クライアント数。
Idle Clients	指定期間中にバックアップ アクティビティを行っていない合計クライアント数。

表 103 [Server Summary] セクションで使用される列 (続き)

列	説明
Successful Clients	バックアップ ステータスが [Successful Backups] フィルターの値セットと一致する合計クライアント数。バックアップの平均時間もあります。
Failed Clients	指定期間中にバックアップが失敗した合計クライアント数。
Clients with Restore	指定期間中にリストア アクティビティ (成功または失敗) を行った合計クライアント数。

ダッシュボード

[Overview] ページの [Dashboard] セクションは、指定したサーバーのグラフィカルなスナップショットビューを提供します。

ダッシュボードではパネルに情報が表示されます。パネルを拡張したり、折りたたんだり、削除したりして、必要なビューを作成します。

使用のためのヒント：

- パネルを折りたたんだり拡張したりするには、パネルのタイトル バーの矢印アイコンをクリックします。
- ダッシュボードのデフォルトビューに戻るには、Web ブラウザのページを再ロードします。

パネルの期間の設定

表示されるデータの日数を定義するには、パネルの期間を設定します。

はじめに

[Overview] ページの [Dashboard] セクションを参照します。次のパネルのいずれかが表示されます。[Analyze]、[Backup Report]、[Backup Trend]。

手順

1. パネル上で、期間フィールドの矢印アイコンをクリックします。

期間フィールドが使用できるのは次のパネルです。

- Analyze
- Backup Report
- Backup Trend

期間リストが表示されます。

2. 期間を選択します。

次の中から選択します。

- Last 24 hours
- Last 7 days
- Last 30 days

選択した期間データに基づいて、Avamar Client Manager がパネルを更新します。

[Client] パネル

[Client] パネルは、選択したサーバの合計潜在クライアント数を円グラフで表示します。次の合計クライアント数が色分けされます。

- **Activated**
緑色は、選択したサーバがアクティブ化されているクライアントの割合を示します。
- **Not activated**
赤色は、選択したサーバが登録されているがアクティブ化はされていないクライアントの割合を示します。
- **Free**
灰色は、選択したサーバで使用可能な未使用クライアント接続の割合を示します。

[Server] パネル

[Server] パネルは、選択したサーバに関する情報をグリッド表示します。

表 104 [Server] パネルのサーバ情報

列	説明
Node Type	サーバのノードタイプ : Single または Multi を指定。
Active Backup	実行中のバックアップの数。
Backup in Queue	サーバのキューで実行を待っているバックアップの数。
Replication	レプリケーション ジョブの現在の状態。 <ul style="list-style-type: none"> • Running • Not running
Status	サーバの Management Console Server (MCS) システムの現在の状態。 <ul style="list-style-type: none"> • Active • Down

[Backup Trend] パネル

[Backup Trend] パネルは、定義された期間中の特定の時点でバックアップされたデータのサイズを示す折れ線グラフです。X 軸は選択した期間中のポイント イン タイムを表します。Y 軸は各ポイント イン タイムでバックアップされたデータのサイズを表します。

点と点の間の線は、時間の経過に伴うバックアップ データの変化のトレンドを表します。

[Client Type] パネル

[Client Type] パネルは、選択されたサーバを対象として、次のカテゴリーごとに、アクティブ化されたクライアントの数を棒グラフで表示します。

- 標準
他の 3 つのどのカテゴリーにも属さないすべてのアクティブ化されたクライアント。
- vMachine

ゲスト クライアント。ホスト コンピューター上で実行されている Avamar クライアント ソフトウェアを通じてバックアップされる仮想コンピューター。

- プロキシ
プロキシ仮想マシン クライアント。VMware イメージのバックアップとリストアに Avamar を使用するクライアント。
- vCenter
vCenter ホストのバックアップにより vCenter 管理インフラストラクチャを保護する Avamar クライアント。

[Analyze] パネル

[**Analyze**] パネルは、選択期間中の次の各状態にあるクライアントの数を棒グラフで表示します。

- **Successful**
成功したバックアップが最低 1 つあるクライアント。
- **Failed**
バックアップ アクティビティはあるが、成功したバックアップのないクライアント。
- **Idle**
バックアップ アクティビティのないクライアント。

[Backup Report] パネル

指定期間中に開始されたバックアップについては、[**Backup Report**] パネルに次の各結果の数が棒グラフで表示されます。

- **成功**
バックアップに成功し完了（エラーのある場合とない場合を含む）。
- **失敗**
バックアップが異常終了。
- **キャンセル済み**
バックアップの完了前にキャンセル。

[Client Queues] パネル

[**Client Queues**] パネルは、次の各キューにあるクライアントの数を棒グラフで表示します。

- **Upgrade**
- **Move to server**
- **Activation**

[Storage Capacity] パネル

[**Storage Capacity**] パネルは、選択したサーバーの総ストレージ容量を円グラフで表示します。それぞれ次のように色分けされています。

- **Used**
赤色は、データが保存されている使用中のストレージの割合を示します。
- **Free Capacity**
緑色は、使用可能な未使用中のストレージの割合を示します。

[Backup Health] パネル

[**Backup Health**] パネルは、特定期間にわたりバックアップ データが保持されているクライアントの数を棒グラフで表示します。このパネルで使用する期間は、1 日、30 日間、60 日間、90 日間です。

棒グラフで、X 軸は Avamar がデータを保持する期間を示しており、Y 軸はクライアント数を示しています。

クライアント

[Clients] ページでは、Avamar クライアントと連携する情報およびツールを提供します。

このページでは、次の操作を行うことができます。

- エンタープライズ ドメインのコンピューターを選択し、Avamar クライアントとして追加する
- 各クライアントに関する詳細情報の表示
- クライアントの移動、破棄、削除
- クライアントのグループ関係の変更
- クライアントの Avamar ソフトウェアのアップグレード

[Clients] ページの各セクションを参照するには、左側のメニューから選択を行います。

クライアントおよびサーバー ツール

Avamar Client Manager には、Avamar クライアントと Avamar サーバの管理に役立つツールがいくつかあります。

各コンテキストに関係のあるツールだけが表示されます。ツールによる変更は、選択したクライアントおよび選択したサーバに対して適用されます。ツールを起動するには、ツールのコマンド ボタンをクリックします。

Avamar ドメインの作成

Avamar サーバの管理階層に分岐を追加するには、Avamar ドメインを作成します。

はじめに

[Create Domain] に含まれる、[Add New Clients] ダイアログ ボックスまたは [Client Move] ダイアログ ボックスのいずれかのビューを参照します。

手順

1. [Domain Selection] ペインで、新しいドメインのロケーションを選択します。
新しいドメインを root ドメインの直下に置く場合は、サーバー アイコンを選択します。新しいドメインを別のドメインの下に置く場合は、そのドメインを選択します。
2. [Create Domain] をクリックします。
[New Domain] ダイアログ ボックスが表示されます。
3. [New Domain Name] にドメインの名前を入力します。
Avamar では次の文字をドメイン名に使用することはできません (=`~!@#$%^&(){}[]|,`:#\/:*?<>'\"&+)`。
4. (オプション) [Contact]、[Phone]、[Email]、[Location] フィールドに情報を入力します。
5. [OK] をクリックします。

結果

Avamar Client Manager が選択したサーバに新しいドメインを追加し、新しいドメインが [Domain Selection] ペインに表示されます。

クライアントのグループ関係の表示

クライアントに適用するポリシーの判断には、クライアントを含むグループを表示します。

はじめに

[Actions] バーに **[Group Associations]** が含まれるビューを参照します。

クライアントのグループ関係は、クライアントのバックアップ データセット、クライアントのバックアップ スケジュール、クライアントのバックアップ保存期間を決定します。

手順

1. クライアントを選択します。
2. **[Group Associations]** をクリックします。

結果

[Groups for Client] ダイアログ ボックスが表示され、クライアントのグループがリストされます。

クライアントへのグループ関係の追加

グループのポリシーをクライアントに適用するには、グループ関係をクライアントに追加します。

はじめに

[Actions] バーに **[Group Associations]** が含まれるビューを参照します。

このタスクにより、クライアントとグループ間に関係ができます。Avamar サーバがグループのポリシーをクライアントに適用します。

手順

1. クライアントを選択します。
2. **[Group Associations]** をクリックします。
3. **[Groups for Client]** ダイアログ ボックスで、**[Add Groups]** をクリックします。
[Add Groups for Client] ダイアログ ボックスが表示されます。
4. グループを選択します。
複数のグループを選択できます。
5. **[Add]** をクリックします。

結果

Avamar Client Manager が、グループ関係をクライアントに追加します。

グループの作成

クライアントへの割り当てに使用可能な新しいポリシーのセットを作成するには、ポリシーを伴ったグループを作成します。クライアントをグループに追加する場合や、クライアントを新しいドメインやサーバーに移動する場合には、**[Create Group]** コマンドが使用できます。

はじめに

[Create Group] に含まれる、**[Add Groups]** ダイアログ ボックスまたは **[Client Move]** ダイアログ ボックスのいずれかのビューを参照します。

手順

1. **[Create Group]** をクリックします。
[Client Move] ダイアログ ボックスでドメインを選択して、ボタンを有効化します。

[**Create Group in Domain**] ダイアログ ボックスが表示されます。

2. [**Group Name**] で、新しいグループの名前を入力します。

Avamar では次の文字をグループ名に使用することはできません (=~!@#\$%^&()*{}[]|,` ;# \/:*?<>' "&+)

3. (オプション) グループに割り当てたクライアントのスケジュール設定バックアップを有効化するには、[**Enable**] を選択します。

グループに割り当てるクライアントのスケジュール設定バックアップを無効化するには、このチェックボックスをクリアします。

4. [**Dataset**] で、グループのデータセットを選択します。
5. [**Schedule**] で、グループのスケジュールを選択します。
6. [**Retention Policy**] で、グループの保存ポリシーを選択します。
7. [**OK**] をクリックします。

結果

Avamar Client Manager が、選択したドメインにグループを作成します。

クライアントからのグループ関係の削除

クライアントへのグループ ポリシーの適用を止めるには、クライアントからグループ関係を削除します。

はじめに

[**Actions**] バーに [**Group Associations**] が含まれるビューを参照します。

このタスクにより、クライアントとグループ間の関係が削除されます。このタスクが完了すると、グループのポリシーがクライアントに適用されることはありません。

手順

1. クライアントを選択します。
2. [**Group Associations**] をクリックします。
3. [**Groups for Client**] ダイアログ ボックスで、グループを選択します。
複数のグループを選択できます。
4. [**Remove**] をクリックします。

結果

Avamar Client Manager が、クライアントと選択したグループとの間の関係を削除します。

クライアントに対するグループ ポリシー設定のオーバーライド

クライアントに適用されたポリシーを変更するには、そのグループのポリシーをオーバーライドします。

はじめに

[**Actions**] バーに [**View/Edit Details**] が表示されているビューを参照すると、クライアントリストにクライアントが表示されます。

手順

1. クライアントを選択します。
2. [**Actions**] バーで、[**View/Edit Details**] をクリックします。
[**Client Details**] ダイアログボックスが表示されます。

3. **[Advanced]** タブを選択します。

ポリシーのオーバーライド設定は、表示されているクライアントの現在の状態とともに表示されます。

4. 設定を選択またはクリアして、クライアントの現在の状態に変更を加えます。

5. **[OK]** をクリックします。**結果**

Avamar Client Manager が、クライアントのグループ ポリシー設定を変更します。

グループ ポリシーのオーバーライド設定

クライアントに適用されたポリシーを変更するには、ポリシー 上書き設定のどれかを使用します。

次の表は、**[Client Details]** ダイアログ ボックスの **[Advanced]** タブのポリシー オーバーライド設定を説明したものです。

表 105 **[Client Details]** の **[Advanced]** タブの設定

設定	説明
Override group retention	グループ設定と異なるクライアント保存設定に割り当てることが可能です。このオプションの選択後、 [Select an existing retention policy] リストから選択することにより保存設定を割り当てます。
Select an existing retention policy	クライアントに割り当てることができる使用可能な保存設定のリストです。このリストを使用するには、まず [Override group retention] を選択します。
Disable all backups	クライアントのすべてのバックアップを無効化します。データのリストアは可能です。
Activated	登録されたクライアントをアクティブ化された状態に置きます。この設定をクリアすると、バックアップまたはリストアを実行することができなくなります。
Allow client-initiated backups	クライアントからのバックアップ開始が可能です。
Allow file selection for client-initiated backups	クライアントが開始したバックアップに含めるファイルが選択可能です。グループのデータセットに対する [Exclude] リストは適用されません。
Allow client to add to dataset	クライアントのグループにフォルダーが追加可能です。この設定には、次のルールが適用されます。 <ul style="list-style-type: none"> Avamar サーバは、グループの [Exclude] リストおよび [Include] リストによって、追加データをフィルターします。 追加データは、クライアントに割り当てられた各グループのスケジュール設定およびオン デマンドバックアップにあります。 フォルダーを追加または削除するには、Avamar クライアント Web ユーザー インターフェイスにアクセスしている必要があります。
Allow client to override daily group schedules	グループの開始時間と異なるスケジュール設定バックアップの開始時間の選択が可能です。前提条件：

表 105 [Client Details] の [Advanced] タブの設定 (続き)

設定	説明
	<ul style="list-style-type: none"> Avamar サーバの [Override] スケジュールに時間エントリーを追加します。 クライアントのグループに日単位のスケジュールを割り当てます。 ユーザーが新しいスケジュールを選択できるようにするには、Avamar クライアント Web ユーザーインターフェイスにアクセス可能にします。
Allow client to override retention policy on client-initiated backups	<p>[Select an existing retention policy] で指定した保存ポリシーを、クライアントが開始したバックアップに割り当てます。前提条件：</p> <ul style="list-style-type: none"> [Override group retention] を有効化します。 [Allow client initiated backups] を有効化します。

クライアントに関するサマリー情報の表示

クライアントとそのユーザーに関する情報を参照するには、Client Details を使用します。

はじめに

[Actions] バーに [View/Edit Details] が表示されているビューを参照すると、クライアントリストにクライアントが表示されます。

手順

1. クライアントを選択します。
2. [Actions] バーで、[View/Edit Details] をクリックします。
[Client Details] ダイアログボックスが表示されます。
3. [Summary] タブを選択します。

結果

クライアントに関する情報が表示されます。クライアントに関連したユーザーのリストも表示されます。

サーバー上のクライアント名の変更

コンピューターのホスト名を変更する場合、このコンピューターを Avamar クライアントとして識別するために、Avamar サーバで使用される名前も変更します。

はじめに

このタスクを実行する前に、コンピューターと DNS でホスト名を変更してください。[Actions] バーに [View/Edit Details] が表示されているビューを参照すると、クライアントリストにコンピューターが表示されます。

手順

1. クライアントを選択します。
2. [Actions] バーで、[View/Edit Details] をクリックします。

[**Client Details**] ダイアログボックスが表示されます。

3. [**Summary**] タブを選択します。
4. [**Client name**] にコンピューターの新しいホスト名を入力します。
5. [**OK**] をクリックします。

結果

Avamar Client Manager は、以前のホスト名を、Avamar サーバ上の Avamar クライアントの新しいホスト名に置き換えます。

クライアントのバックアップ履歴の表示

Avamar サーバが予定されたバックアップを完了したかどうかを判断するには、クライアントのバックアップ履歴を表示します。

はじめに

[**Actions**] バーに [**View/Edit Details**] が表示されているビューを参照すると、クライアントリストにクライアントが表示されます。

手順

1. クライアントを選択します。
2. [**Actions**] バーで、[**View/Edit Details**] をクリックします。

[**Client Details**] ダイアログボックスが表示されます。

3. [**Backups**] タブを選択します。
4. [**From**] で、表示する最も古い日付を選択します。
5. [**To**] で、表示する最も新しい日付を選択します。
6. (オプション) [**On-demand backups**] を選択します。

この選択を行うと、ユーザーが起動したバックアップが結果に含まれます。この選択をクリアすると、それらのバックアップは除外されます。

7. (オプション) [**Scheduled backups**] を選択します。

この選択を行うと、グループスケジュールによって起動されたバックアップが結果に含まれます。この選択をクリアすると、それらのバックアップは除外されます。

結果

フィルターの設定と一致したクライアントのバックアップのリストが表示されます。

クライアントのインストールされたプラグインの表示

Avamar クライアントにインストールされた Avamar プラグインを表示すると、バックアップのデータタイプの判断が容易になります。

はじめに

[**Actions**] バーに [**View/Edit Details**] が表示されているビューを参照すると、クライアントリストにクライアントが表示されます。

手順

1. クライアントを選択します。
2. [**Actions**] バーで、[**View/Edit Details**] をクリックします。

[**Client Details**] ダイアログボックスが表示されます。

3. **[Plug-ins]** タブを選択します。

結果

クライアントにインストールされたプラグインが表示されます。

サーバーからのクライアントの削除

Avamar サーバからクライアントのレコードとバックアップを削除するには、サーバからクライアントを削除します。

はじめに

クライアントリストにクライアントが表示されるビューを参照すると、**[Action]** バーに **[Delete]** が表示されます。

Avamar Client Manager が Avamar サーバからクライアントを削除すると、Avamar サーバによりそのクライアントのすべてのアクティビティが停止し、クライアントのバックアップが削除され、クライアントのすべてのレコードがサーバのデータベースから削除されます。

手順

1. クライアントを選択します。
2. **[Actions]** バーで、**[Delete]** をクリックします。
3. **[Confirm]** ダイアログ ボックスに自分のパスワードを入力します。
Avamar Client Manager にログインするときのアカウントのパスワードを使用します。
4. **[OK]** をクリックします。
[Alert] ダイアログ ボックスが表示されます。
5. **[OK]** をクリックします。

結果

Avamar Client Manager がバックグラウンド処理を実行し、クライアントの情報およびデータをすべてをサーバから削除します。

[Add Clients]

[Add Clients] セクションは、エンタープライズ コンピューターを Avamar クライアントとして登録してアクティブ化するための情報とツールを提供します。

[Add Clients] セクションを使用して、エンタープライズのコンピューターに関する情報をインポートします。サポートされる LDAP の命名規則または CSV ファイルから情報をインポートします。

インポートした後、クライアントのステータスおよびクライアント名によって情報をフィルターして、Avamar クライアント候補の選択に役立てます。

Avamar Client Manager を使用して、選択したコンピューターの Avamar サーバへの登録およびアクティブ化を行います。アクティベーション処理を完了するには、Avamar クライアント ソフトウェアをコンピューター上にインストールし、サーバから Avamar クライアント プロセスにアクセスする必要があります。通常のワークフローでは、コンピューターのアクティベーションを選択する前に、クライアント ソフトウェアをコンピューターにインストールします。

ディレクトリ サービス情報

エンタープライズのディレクトリ サービスを使用して、Avamar Client Manager に対して潜在的 Avamar クライアント コンピューターの情報を提供できます。

潜在的 Avamar クライアント コンピューターに関する情報を持つ、サポートされるディレクトリ サービスを使用します。Avamar Client Manager はディレクトリ サービスをクエリーして、クライアントに関

する情報を入手します。さらに可能であれば、ディレクトリドメインなどのディレクトリ保守サービス体制ユニットやディレクトリグループの情報も入手します。

ディレクトリサービスの方法を使用してドメインでコンピューターの情報を取得するには、ディレクトリサービスを使用するように事前に Avamar Client Manager を構成してください。

ディレクトリサービスの方法では、次のような要件があります。

- Avamar Client Manager を実行しているサーバーからディレクトリサービスへの TCP/IP アクセス。
- ディレクトリサービスに対する読み取りアクセスのためのユーザー アカウントのアカウント情報。
- インポートしたいコンピューターのディレクトリサービスドメインの名前。

ディレクトリ サービスからの情報のインポート

コンピューターを Avamar クライアントとして追加する準備として、コンピューターに関する情報をディレクトリサービスからインポートします。

はじめに

次の操作を実行します。

- ディレクトリサービスを使用するように、Avamar Client Manager を構成します。
- ユーザー名に加えて、ディレクトリサービスへの読み取りアクセスのためのアカウントの関連ドメインおよびパスワードを入手します。
- インポートしているコンピューターのディレクトリサービスドメインの名前を使用可能にします。

手順

1. 左側のメニューから、[Clients] > [Add Clients] をクリックします。
2. [Actions] バーの [New Clients] をクリックします。
[Client Information Source] ダイアログ ボックスが表示されます。
3. [Active Directory] を選択します。
4. [User Domain] で、ディレクトリサービスへのアクセスに使用しているアカウントのドメインを選択します。
ディレクトリサービスドメインをこのリストに加えるには、管理ガイドを参照します。
5. [User Name] に、アカウントの名前を入力します。
6. [Password] に、アカウントのパスワードを入力します。
7. [Directory Domain] で、インポートするコンピューター情報のディレクトリサービスドメインの名前を選択します。
8. [OK] をクリックします。

結果

Avamar Client Manager が、ディレクトリサービスから情報をインポートします。

必要条件

インポートされたコンピューター情報を使用して、Avamar サーバのクライアントとしてコンピューターを選択およびアクティブ化します。

CSV ファイル情報

CSV (Comma-Separated Values) ファイルを使用して、潜在的 Avamar クライアントのコンピューター情報を Avamar Client Manager に提供することができます。

CSV ファイルは、手動で作成するか、Microsoft System Center Configuration Manager または Microsoft Systems Management Server などのシステム管理ツールの出力を使用して作成します。

Avamar クライアント ソフトウェアをコンピューターのグループにインストールしたときにシステム管理ツールが生成した出力を使用して、CSV ファイルを作成することができます。ただし、Avamar Client Manager には、Avamar クライアント ソフトウェアが正常にインストールされたクライアントのみが表示されます。

CSV ファイルのアップロード中、Avamar Client Manager はファイルのフォーマットが正しいことをチェックし、問題があった場合はアップロードをキャンセルします。

CSV ファイル形式

正しいフォーマットの CSV ファイルは以下のルールに準拠しています。

- 最低 2 行ある。
- 値はコンマのみで区切られます。
- ファイルの最初の行は、値の各タイプのリテラル名で構成されていなければならない。最初の値の名前は **Hostname**。2 番目の値の名前は **Group**。
- 2 番目の行およびそれに続くすべての行には、値が最低 1 つなくてはならないが、3 つ以上あってはならない。
- 最初の値はコンピューターの有効なホスト名であり、続いてコンマがある必要があります。
- 2 番目の値はオプションですが、存在する場合は、コンピューターのディレクトリ サービスの論理グループ名である必要があります。該当するコンピューターに対して 2 番目の値が存在しない場合、Avamar Client Manager はそのコンピューターを階層表示の root レベルに表示します。
- 2 番目の値では、ディレクトリ サービスの論理グループ名の階層レベルを分離するために、フォワードスラッシュ (/) を使用します。

クライアントリストの作成または編集にスプレッドシート ソフトウェアを使用する場合は、コンマ区切り値を作成しようとして値にコンマを付けないでください。スプレッドシート ソフトウェア内で値にコンマを追加すると、不適切な形式のファイルになる可能性があります。エディターでクライアントリストを CSV ファイル タイプで保存する際に、ファイル変換プロセスの一環としてエディターがコンマの区切り文字を追加するためです。フォーマットをチェックするためには、クライアントリストを平文のエディターで開きます。

正しくフォーマットされたクライアントリスト ファイルの例

正しくフォーマットされたクライアントリスト ファイルは、平文のエディターでは次のように見えます。

```
Hostname, Group
User1-desktop.Acme.corp.com, acme.corp/USA/MA
User1-laptop.Acme.corp.com, acme.corp/USA/CA/SFO
User2-desktop.Acme.corp.com, acme.corp/Engineering
User3-desktop.Acme.corp.com,
User4-desktop.Acme.corp.com,
```

ファイルの最初の行は、値の各タイプのリテラル名のリストです。

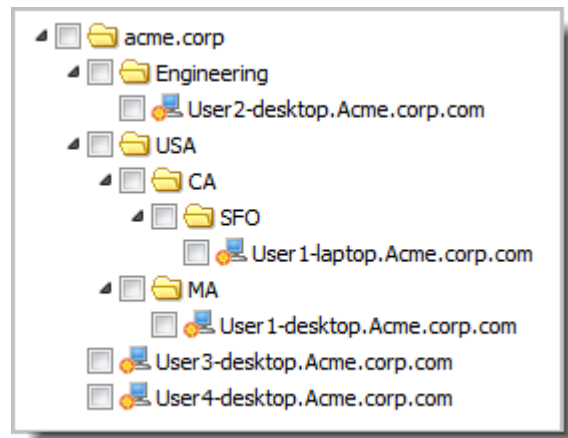
2 行目には、ホスト名 `User1-desktop.Acme.corp.com`、区切り文字のコンマ、グループ `acme.corp/USA/MA` が含まれます。

3 行目には、ホスト名 `User1-laptop.Acme.corp.com`、区切り文字のコンマ、グループ `acme.corp/USA/CA/SFO` が含まれます。

4 行目には、ホスト名 `User2-desktop.Acme.corp.com`、区切り文字のコンマ、グループ `acme.corp/Engineering` が含まれます。

5 行目と 6 行目には、ホスト名 `User3-desktop.Acme.corp.com` と `User4-desktop.Acme.corp.com` のみが表示され、その後それぞれコンマが付きます。フォーマットルールでは、グループがない時にもコンマが必要です。この 2 行にはグループがリストされていないため、どちらのホスト名も階層表示の root レベルに表示されます。

図 16 CSV ファイルの例をアップロードした後のビュー



CSV ファイルでの情報のアップロード

コンピューターを Avamar クライアントとして追加する準備をするために、コンピューターに関する情報を CSV (Comma-Separated Values) ファイルにアップロードします。

はじめに

正しくフォーマットされた CSV ファイルを生成または作成し、Web ブラウジングの可能なコンピューターにコピーを作成します。

手順

1. 左側のメニューから、[Clients] > [Add Clients] をクリックします。
2. [Actions] バーの [New Clients] をクリックします。
[Client Information Source] ダイアログ ボックスが表示されます。
3. [CSV File] ファイルを選択します。
4. [Browse] をクリックします。
[Choose File to Upload] ダイアログ ボックスが表示されます。
5. CSV ファイルの場所を参照して選択し、[Open] をクリックします。
6. [Client Information Source] ダイアログ ボックスで [OK] をクリックします。

結果

Avamar Client Manager が CSV ファイルの情報をアップロードします。

必要条件

アップロードされたコンピューター情報を使用して、Avamar サーバのクライアントとしてコンピューターを選択およびアクティブ化します。

アクティベーション

アクティベーションによりコンピューターと Avamar サーバの関係が変化し、Avamar サーバからコンピューターのバックアップの管理ができるようになります。

関係は、次の表に示す 3 種類の状態で切り替わっていきます。

表 106 クライアント アクティベーション時の関係の状態

状態	説明
No relationship	コンピューターはサーバーからは不明です。この状態にあるコンピューターは、最初にコンピューター情報を Avamar Client Manager に追加した時点で、 [Add Clients] に表示されます。
Registered	Avamar Client Manager が、このコンピューターに関する情報を Avamar サーバのデータベースに追加済みです。この状態にあるコンピューターは、Avamar Client Manager によってアクティベーション処理が開始され、Avamar サーバへの登録が完了した後で、 [Registered Clients] に表示されます。これらのコンピューターの変更された状態も [Add Clients] に表示されます。
Activated	このコンピューターには、Avamar クライアントソフトウェアがインストールされ、実行中です。クライアント ソフトウェアとサーバーは、お互いを確認するために暗号化されたキーを交換し、通信中です。この状態にあるコンピューターは、アクティベーションが完了すると [Activated Clients] に表示されます。これらのコンピューターの変更された状態も [Add Clients] と [Registered Clients] に表示されます。

アクティベーション処理中のコンピューターは、**[Activation]** の **[Queues]** ページに表示されません。Avamar Client Manager は、試行に成功するか 24 回の試行限度に達するまで 2 時間おきにコンピューターのアクティブ化を試みます。処理が完了すると、Avamar Client Manager はこのビューからコンピューターを削除し、**[Activation]** の **[Logs]** ページにエントリーを追加します。

バックアップ管理を有効化するコンピューターのアクティブ化

クライアントのバックアップ管理を有効化するためには、Avamar サーバでクライアントをアクティブ化します。

はじめに

アクティブ化するコンピューターに Avamar クライアント ソフトウェアをインストールし、ディレクトリ サービスまたは CSV ファイルのどちらかからコンピューターに関する情報をインポートします。

手順

1. 左側のメニューで、**[Clients]** > **[Add Clients]** をクリックします。

エンタープライズのコンピューターが階層化されて表示されます。Avamar Client Manager は、インポートされた情報からこの表示を生成します。

2. アクティブ化するコンピューターを検索するには、階層を参照または検索します。
3. アクティブ化する各コンピューターを選択します。

フォルダーのすべてのコンピューターを選択するには、フォルダーを拡張してコンピューターを表示して、そのフォルダーを選択します。

4. **[Activate]** をクリックします。

[Server - Domain Selection] ダイアログ ボックスが表示されます。

5. サーバのリストを拡張して、Avamar ドメインを選択します。

Avamar Client Manager が、選択したサーバおよびドメインに対して、アクティベーションの間にコンピューターを割り当てます。

6. **[Next]** をクリックします。

[Server - Group Selection] ダイアログ ボックスが表示されます。

7. 1つまたは複数のグループを選択します。

Avamar Client Manager が、選択した1つ以上のグループに対して、アクティベーションの間にコンピューターを割り当てます。

8. **[Finish]** をクリックします。

結果

Avamar Client Manager が、アクティベーション タスクをキューに送ります。

必要条件

アクティベーション処理のステータスを判断するには、**[Queues]** ページの **[Activation]** セクションを確認します。処理の完了後、**[Logs]** ページの **[Activation]** セクションを確認して、最終的なステータスを判断します。

[Registered Clients]

Avamar サーバによって登録されていながらも、アクティブ化されていないクライアントは、**[Registered Clients]** セクションに表示されます。

[Registered Clients] セクションは、クライアントを選択して、以下のクライアント関連タスクを実行するのに使用します。

- アクティブ化
- 削除
- グループとの関連付け
- 詳細の表示と編集
- グループ オーバーライド設定の追加と削除

登録したクライアントのアクティブ化

登録時にアクティブ化に失敗した登録済みのクライアントのバックアップ管理を有効化するには、**[Registered Clients]** セクションからアクティブ化を行います。

はじめに

アクティブ化する対象のコンピューターに Avamar クライアント ソフトウェアをインストールします。

Avamar サーバのクライアントとしてのコンピューターのアクティベーションに失敗しても、Avamar Client Manager はこのコンピューターをサーバに登録します。アクティベーションを妨げている問題を解決します。次に登録済みクライアントのアクティベーションを再試行します。

手順

1. 左側のメニューで、**[Clients]** > **[Registered Clients]** をクリックします。
2. アクティブ化する各クライアントを選択します。
3. **[Activate]** をクリックします。

結果

Avamar Client Manager が、アクティベーション タスクをキューに送ります。

必要条件

アクティベーション処理のステータスを判断するには、**[Queues]** ページの **[Activation]** セクションを確認します。処理の完了後、**[Logs]** ページの **[Activation]** セクションを確認して、最終的なステータスを判断します。

アクティブ化されたクライアント

選択した Avamar サーバのアクティブ化されたクライアントは、[**Activated Clients**] セクションに表示されます。

[**Activated Clients**] セクションを使用して、以下のタスクを実行できます。

- クライアントの別サーバーへの移動
- クライアントの別 Avamar ドメインへの移動
- クライアントの破棄
- クライアントの削除
- クライアントのグループ関係の管理
- クライアントの詳細の表示と編集
- グループ オーバーライド設定の追加と削除

クライアントの新サーバーへの移動

新しい Avamar サーバを使用して Avamar クライアントを管理するには、Avamar クライアントの登録、アクティベーション、バックアップを新しいサーバに移動します。

はじめに

次の操作を実行します。

- [Avamar サーバの追加](#) (326 ページ) に記載されているように、Avamar Client Manager にターゲットサーバを追加します。
- Avamar サーバ ソフトウェア バージョン 5.0.1.31 以降のサーバにアクティブ化されているクライアントを選択します。
- バージョン 6.x より前の Avamar サーバでアクティブ化されたクライアントは、そのサーバの MCS プロセスを完全に初期化します。

手順

1. 左側のメニューで、[**Clients**] > [**Activated Clients**] をクリックします。
2. クライアントを選択します。
NDMP クライアントは選択しないでください。Data Domain サーバにバックアップがあるクライアントは選択しないでください。
3. [**Actions**] バーで [**Move**] をクリックします。
[**Client Move**] ダイアログ ボックスの [**Domain Selection**] ペインが表示されます。
4. [**Domain Selection**] ペインの上部のサーバ選択リストから、移動ターゲットの Avamar サーバを選択します。
ターゲットサーバのドメインが [**Domain Selection**] ペインに表示されます。
5. [**Domain Selection**] ペインでターゲットドメインを選択します。
6. [**Next**] をクリックします。
[**Client Move**] ダイアログ ボックスの [**Group Selection**] ペインが表示されます。
7. ターゲットグループを選択します。
オプションで、複数のターゲットグループを選択することができます。Avamar Client Manager が、選択したすべてのグループにクライアントを追加します。

8. **[Group Selection]** ペイン下部の **[Replicate Existing Backups]** で、値を選択します。

オプション	説明
All	すべてのクライアントのバックアップをターゲット サーバにレプリケートします。
Last	最新のバックアップのみレプリケートします。
None	バックアップをレプリケートしません。

レプリケーションにより、ターゲット サーバからバックアップが使用可能になります。

9. (オプション) **[Delete From Source]** で次の操作を実行します。
- このオプションを選択して、ソース サーバからすべてのクライアントのバックアップを削除します。
 - ソース サーバのクライアントの登録をソース サーバの **MC_RETIRE**D ドメインに確実に移動して、ソース サーバにはクライアントのバックアップのコピーを保存します。
10. **[Finish]** をクリックします。
- [Confirm Replication Authentication]** ダイアログ ボックスが表示されます。
11. **[Source Server]** にソース サーバの **repluser** アカウントのパスワードを入力します。
12. **[Target Server]** にターゲット サーバの **repluser** アカウントのパスワードを入力します。
13. **[OK]** をクリックします。

結果

Avamar Client Manager が、バックグラウンド処理で選択したターゲットにクライアントを移動します。

クライアントの別 Avamar ドメインへの移動

Avamar クライアントと Avamar サーバの管理関係を変更するために、クライアントを別の Avamar ドメインに移動することができます。

はじめに

Avamar サーバ ソフトウェア バージョン 6.x 以降のサーバにアクティブ化されているクライアントを選択します。

手順

- 左側のメニューで、**[Clients]** > **[Activated Clients]** をクリックします。
- クライアントを選択します。
- [Actions]** バーで **[Move]** をクリックします。
[Client Move] ダイアログボックスが表示されます。
- [Client Move]** ダイアログ ボックスの **[Domain Selection]** ペインで、ターゲット ドメインを選択します。
- [Next]** をクリックします。
[Group Selection] ペインが **[Client Move]** ダイアログ ボックスに表示されます。
- ターゲット グループを選択します。

オプションで、複数のターゲット グループを選択することができます。Avamar Client Manager が、選択したすべてのグループにクライアントを追加します。

7. **[Finish]** をクリックします。
アラート ボックスが表示されます。
8. **[OK]** をクリックします。

結果

Avamar Client Manager が、バックグラウンド処理で選択したターゲットにクライアントを移動します。

クライアントの廃棄

Avamar クライアントのバックアップを停止するには、Avamar クライアントを廃棄します。Avamar Client Manager は破棄した時点のバックアップを保存するため、必要に応じてデータをリストアすることができます。

手順

1. 左側のメニューで、**[Clients]** > **[Activated Clients]** をクリックします。
2. クライアントを選択します。
複数のクライアントを選択できます。選択した保存ポリシー設定が選択したすべてのクライアントに適用されます。
3. **[Actions]** バーで **[Retire]** をクリックします。
[Retire Client] ダイアログ ボックスが表示されます。
4. **[Select Retention Policy]** でオプションを 1 つ選択します。

オプション	説明
[Retire client and retain backups with existing expiration date]	既存の保存期間の間、Avamar サーバがバックアップを保持します。
[Retire client and retain all backups indefinitely]	手動でバックアップを削除するまで、Avamar サーバがバックアップを保持します。
[Retire client and reset backup expiration date]	[New Expiration Date] に設定した日付まで、Avamar サーバがバックアップを保持します。

5. 前のステップで **[Retire client and reset backup expiration date]** を選択した場合は、**[New Expiration Date]** で日付を選択します。
[Confirm] ダイアログ ボックスが表示されます。
6. **[Yes]** をクリックします。
[Alert] ダイアログ ボックスが表示されます。
7. **[OK]** をクリックします。

結果

バックグラウンド処理で、Avamar Client Manager が選択したクライアントを破棄します。

失敗したクライアント

バックアップまたはリストア アクティビティに成功しなかったクライアントが、**[Failed Clients]** セクションに表示されます。

[Failed Clients] セクションを使用して、以下のタスクを実行できます。

- クライアントの削除
- クライアントのグループ関係の管理
- クライアントの詳細の表示と編集
- グループ オーバーライド設定の追加と削除

失敗したクライアントで作業する場合は、次の表の説明にあるフィルターを使用します。

表 107 失敗したクライアントのフィルター

フィルター	説明
Period	Avamar Client Manager で詳しく調べる期間を指定します。
Activity Type	Avamar Client Manager で詳しく調べるアクティビティのタイプを指定します。
Failure Criteria	Avamar Client Manager で使用される故障閾値を定義します。

アイドル状態のクライアント

アクティブ化されているが、指定された期間中にアクティビティがなかった Avamar クライアントです。
[Idle Clients] セクションに表示されます。

アイドル状態のクライアントで作業する場合は、[Period] フィルターを使用して Avamar Client Manager でアクティビティを詳しく調べる期間を指定し、[Activity Type] フィルターを使用してアクティビティのタイプを指定します。

[Idle Clients] セクションを使用して、以下のタスクを実行できます。

- クライアントの削除
- クライアントのグループ関係の管理
- クライアントの詳細の表示と編集
- グループ オーバーライド設定の追加と削除

クライアントのアップグレード

[Upgrade Clients] セクションでは、Avamar クライアントにアップグレードおよびホットフィックスを適用するために使用できる情報とツールが提供されます。

[Upgrade Clients] セクションを使用して、以下のタスクを実行できます。

- サーバーへの更新パッケージのダウンロード
- アップグレード パッケージの選択
- 選択したクライアントに対するアップグレード パッケージの適用
- 更新パッケージのサーバーからの削除

[Upgrade Clients] セクションの要件

Avamar Client Manager の [Upgrade Clients] セクションを使用する前に、次を実行してください。

- 各クライアントまたはプラグ インに、「E-Lab Navigator」の「Avamar Push Client upgrade compatibility」の表に記載されている最低限のクライアント バージョンをインストールします。

注

Windows クラスタ ノード上の Avamar クライアント ソフトウェアをアップグレードするための [Upgrade Clients] 機能の使用は、サポートされていません。「Avamar for Windows Server ユーザー ガイド」では、Windows クラスタ ノードで Avamar クライアント ソフトウェアをアップグレードする方法が説明されています。

- Avamar Downloader Service をインストール、構成、実行します。Avamar Downloader Service で、アップグレード機能に必要なクライアント パッケージとプラグ イン パッケージを取得します。このサービスは、パッケージをプルし、それらを Avamar データ サーバ サブシステム (GSAN) 上にプッシュします。GSAN でパッケージが更新されると、パッケージが Avamar Client Manager の [Select Package] ウィンドウに表示され、アップグレードが実行可能になります。

複数システム的环境

複数の Avamar システムを含む Avamar の環境では、いずれか 1 つの Avamar システム (Managing システム) で実行している Avamar Client Manager を使用して、他の Avamar システム (Managed システム) と関連づけられたクライアントを管理することができます。

Managed システムは、次の要件を満たしている必要があります。

- Managed システムは、Managing システム上の Avamar Client Manager に追加されます。Managing システムの Avamar Client Manager に Managed システムを追加することにより、Managed システムでのクライアント アップグレードのサポートに必要な情報が Managing システムに提供されます。
- Managed システムは、Managing システムに「近いバージョン」(2 バージョン以上前でないバージョン) の Avamar ソフトウェアを実行しています。

近いバージョンの要件により、Managed システムのクライアントで必要になるすべてのパッケージが Managing システムを通じて環境で利用できるようになります。

近いバージョンの要件を満たさない Avamar システムと関連づけられたクライアントにクライアント アップグレードの完全サポートを提供するには、それらのシステムで Avamar Client Manager を実行します。

アップグレードおよびホットフィックス パッケージのダウンロード

Avamar Client Manager を使用して、アップグレードおよびホットフィックス パッケージを Avamar サーバにダウンロードします。

はじめに

次の操作を実行します。

- Avamar Downloader Service と AvInstaller サービスをインストールして設定します。以下のタスクの情報については、管理ガイドを参照してください。
- Avamar サーバを選択します。

Avamar クライアントにアップグレードまたはホットフィックス パッケージを適用する前に、Avamar クライアントに関係づけられた Avamar サーバにパッケージをダウンロードします。

手順

1. 左側のメニューで、[Clients] > [Upgrade Clients] をクリックします。
2. [Actions] バーで [Select Package] をクリックします。
[Upgrade Client] ダイアログ ボックスが表示されます。

3. パッケージの **[Status]** 列で **[Download]** をクリックします。

パッケージのステータスは、Available である必要があります。

結果

Avamar Client Manager がダウンロードを開始します。進捗バーが表示されます。ダウンロードが終了すると、Avamar Client Manager が次の順にパッケージ ステータスを更新します：

Waiting、Processing、Ready。

アップグレード パッケージの選択

Avamar クライアントに適用するアップグレード パッケージまたはホットフィックス パッケージを選択します。

はじめに

次の操作を実行します。

- Avamar Downloader Service と AvInstaller サービスをインストールして設定します。以下のタスクの情報については、管理ガイドを参照してください。
- Avamar サーバを選択します。
- 選択した Avamar サーバにアップグレードまたはホットフィックス パッケージをダウンロードします。

手順

1. 左側のメニューで、**[Clients]** > **[Upgrade Clients]** をクリックします。
2. **[Actions]** バーで **[Select Package]** をクリックします。

[Upgrade Client] ダイアログ ボックスが表示されます。

3. パッケージを選択します。

パッケージを選択するには、パッケージのステータスが **[Ready]** になっている必要があります。

4. **[Select]** をクリックします。

[Upgrade Client] ダイアログ ボックスが閉じます。

結果

アップグレードまたはホットフィックスが適用可能な Avamar クライアントが表示されます。

必要条件

クライアントを選択して、アップグレードまたはホットフィックス パッケージを適用します。

アップグレード パッケージの適用

Avamar クライアントを選択して、アップグレード パッケージまたはホットフィックス パッケージを適用します。

はじめに

アップグレード パッケージまたはホットフィックス パッケージを選択します。選択したパッケージが適用可能な Avamar クライアントのリストが表示されます。

通知

Avamar NDMP アクセラレーター ノード (アクセラレーター ノード) にアップグレードを適用すると、アクセラレーター ノードは実行中のバックアップをドロップすることになります。アップグレードの後、アクセラレーター ノードは NDMP バックアップを正常に開始して完了します。

手順

1. アップグレードまたはホットフィックスが適用可能な Avamar クライアントのリストから、クライアントを選択します。
複数のクライアントを選択できます。
2. [Actions] バーで [Upgrade] をクリックします。

結果

Avamar Client Manager が選択したクライアントのアップグレードを開始します。アップグレードはバックグラウンドで実行されます。

必要条件

[Queues] ページの [Upgrade] セクションで、アップグレードの進行状況をトラッキングします。
[Logs] ページの [Upgrade] セクションに、アップグレードの最終的なステータスが表示されます。

アップグレードおよびホットフィックス パッケージの削除

Avamar Client Manager を使用して、アップグレードとホットフィックス パッケージを Avamar サーバから削除します。

はじめに

不必要なアップグレードまたはホットフィックス パッケージがある Avamar サーバを選択します。

手順

1. 左側のメニューで、[Clients] > [Upgrade Clients] をクリックします。
2. [Actions] バーで [Select Package] をクリックします。
[Upgrade Client] ダイアログ ボックスが表示されます。
3. パッケージを選択します。
削除できるパッケージは、ステータスが [Ready] のパッケージのみです。
4. [Delete] をクリックします。

結果

Avamar Client Manager が、選択したパッケージを Avamar サーバから削除します。

ポリシー

[Policies] ページから、グループ ポリシー タスクと情報にアクセスします。

[Policies] ページには、選択した Avamar サーバ上の各グループ ポリシーのサマリーが表示されます。

[Policies] ページを使用して、次のタスクが行えます。

- グループへのクライアントの追加
- グループからのクライアントの削除
- グループのデータセット ポリシー、保存ポリシー、スケジュール ポリシーの詳細の表示

グループへのクライアントの追加

選択したクライアントにグループのポリシーを適用するには、クライアントをグループに追加します。

このタスクを完了すると、選択したクライアントとグループが関連づけられます。次に Avamar サーバがグループのポリシーを選択したクライアントに適用します。

手順

1. **[Policies]** > **[Groups]** をクリックします。
2. グループを選択します。
3. **[Edit Group Members]** をクリックします。
[Edit Group Members] ダイアログ ボックスが表示されます。
4. **[Add]** をクリックします。
[Add Clients to Group] ダイアログ ボックスが表示されます。
5. クライアントを選択します。
複数のクライアントを選択できます。
6. **[Add]** をクリックします。

結果

Avamar Client Manager がグループにクライアントを追加します。

グループからのクライアントの削除

グループのポリシーを選択したクライアントから削除するには、クライアントをグループから削除します。このタスクにより、選択したクライアントとグループ間の関連が削除されます。このタスクが完了すると、グループのポリシーが選択したクライアントに適用されることはありません。

手順

1. **[Policies]** > **[Groups]** をクリックします。
2. グループを選択します。
3. **[Edit Group Members]** をクリックします。
[Edit Group Members] ダイアログ ボックスが表示されます。
4. クライアントを選択します。
複数のクライアントを選択できます。
5. **[Remove]** をクリックします。

結果

Avamar Client Manager がグループからクライアントを削除します。

グループのデータセット ポリシーの表示

グループのデータセット ポリシーの詳細を表示するには、**[Policies]** ページでグループのエントリーを使用します。

手順

1. Avamar サーバを選択します。
2. **[Policies]** > **[Groups]** をクリックします。
選択したサーバーのグループのサマリー表示が表示されます。
3. グループのエントリーでは、**[Dataset]** 列で、データセット ポリシーの名前をクリックします。

結果

選択したグループのデータセット ポリシーの詳細が、ダイアログ ボックスに表示されます。

グループの保存ポリシーの表示

グループの保存ポリシーの詳細を表示するには、[Policies] ページでグループのエントリーを使用します。

手順

1. Avamar サーバを選択します。
2. [Policies] > [Groups] をクリックします。
選択したサーバーのグループのサマリー表示が表示されます。
3. グループのエントリーでは、[Retention] 列で、保存ポリシーの名前をクリックします。

結果

選択したグループの保存ポリシーの詳細が、ダイアログ ボックスに表示されます。

グループのスケジュール ポリシーの表示

グループのスケジュール ポリシーの詳細を表示するには、[Policies] ページでグループのエントリーを使用します。

手順

1. Avamar サーバを選択します。
2. [Policies] > [Groups] をクリックします。
選択したサーバーのグループのサマリー表示が表示されます。
3. グループのエントリーでは、[Schedule] 列で、スケジュール ポリシーの名前をクリックします。

結果

選択したグループのスケジュール ポリシーの詳細が、ダイアログ ボックスに表示されます。

キュー

[Queues] ページから、Avamar Client Manager のアクティビティ キューにアクセスします。

[Queues] ページは、選択した Avamar サーバーのアクティブおよびペンディング Avamar Client Manager タスクのサマリーを表示します。タスクは、タスクのタイプによって別々のセクションに表示されます。

表 108 [Queues] ページでのタスクタイプ

タスクのタイプ	参照パス	説明
Activation	[Queues] > [Activation]	アクティブなタスクと保留中のタスクの中で、クライアントのアクティベーションに関連したタスクを表示します。
Delete	[Queues] > [Delete]	アクティブなタスクと保留中のタスクの中で、Avamar サーバーからのクライアントの削除に関連したタスクを表示します。
Move	[Queues] > [Move]	アクティブなタスクと保留中のタスクの中で、任意の Avamar サーバーから別のサーバーへのクライアントの移動に関連したタスクを表示します。

表 108 [Queues] ページでのタスクタイプ (続き)

タスクのタイプ	参照パス	説明
Retire	[Queues] > [Retire]	アクティブなタスクと保留中のタスクの中で、Avamar クライアントの廃棄に関連したタスクを表示します。
Upgrade	[Queues] > [Upgrade]	アクティブなタスクと保留中のタスクの中で、Avamar クライアントのソフトウェアのアップグレードに関連したタスクを表示します。

[Queues] ページを使用して、次のタスクが行えます。

- アクティブおよびペンディング タスクの詳細の表示
- タスクのキャンセル

タスクのキャンセル

ペンディングされているタスクが実行されないようにするには、そのタスクをキャンセルします。

タスクがペンディング状態の場合は、キャンセルによりタスクの実行を取りやめることができます。

手順

1. 左側のメニューで [Queues] > [task_queue] をクリックします。ここで、task_queue はキャンセルしているタスクのタイプに対応した [Queues] ページのセクションです。

例えば、クライアント アクティベーションをキャンセルするには、[Queues] > [Activation] をクリックします。

2. タスクを選択します。
3. [Cancel] をクリックします。
Confirmation ダイアログ ボックスが表示されます。
4. [OK] をクリックします。

結果

Avamar Client Manager が、キューからタスクを削除し、タスクをキャンセルし、ログにエントリーを追加します。

ログ

[Logs] ページから、Avamar Client Manager ログにアクセスします。

[Logs] ページは、Avamar Client Manager ログのサマリーを表示します。生成されるエントリーのタスクのタイプによって、ログ エントリーは別々のセクションに表示されます。

表 109 [Logs] ページでのタスクタイプ

タスクタイプ	参照パス	説明
Activation	[Logs] > [Activation]	クライアント アクティベーションに関連するログ エントリーを表示します。
Delete	[Logs] > [Delete]	Avamar サーバからのクライアントの削除に関連したログ エントリーを表示します。

表 109 [Logs] ページでのタスクタイプ (続き)

タスクタイプ	参照パス	説明
Move	[Logs] > [Move]	任意の Avamar サーバから別のサーバへのクライアントの移動に関連したログ エントリーを表示します。
Retire	[Logs] > [Retire]	Avamar クライアントの廃棄に関連するログ エントリーを表示します。
Upgrade	[Logs] > [Upgrade]	Avamar クライアントのソフトウェアのアップグレードに関連したログ エントリーを表示します。

- **Activation**
[Logs] > [Activation] をクリックすると、クライアント アクティベーションに関連するログ エントリーが表示されます。
- **Delete**
[Logs] > [Delete] をクリックすると、Avamar サーバからのクライアントの削除に関連したログ エントリーが表示されます。
- **Move**
[Logs] > [Move] をクリックすると、任意の Avamar サーバから別のサーバへのクライアントの移動に関連したログ エントリーが表示されます。
- **Retire**
[Logs] > [Retire] をクリックすると、Avamar クライアントの廃棄に関連したログ エントリーが表示されます。
- **Upgrade**
[Logs] > [Upgrade] をクリックすると、Avamar クライアントのソフトウェアのアップグレードに関連したログ エントリーが表示されます。

[Logs] ページを使用して、次のタスクが行えます。

- ログ エントリーの表示
- アップグレードのクライアント ログの表示
- セクションのすべてのログ エントリーの消去

Avamar クライアントのアップグレード後のクライアント ログの表示

アップグレードの試行完了後に、Avamar クライアントのローカル ログを表示します。

はじめに

Avamar Client Manager を使用して、アップグレード パッケージまたはホットフィックスを Avamar クライアントに適用します。

Avamar クライアントのローカル ログに、クライアントのアップグレード失敗の理由に関する詳細が表示されます。

手順

1. 左側のメニューで、[Logs] > [Upgrade] をクリックします。
2. ページの右側で、[Details] バーをクリックします。
[Details] パネルが拡張します。
3. [Summary] でクライアントの更新ログエントリーを選択します。
選択したログ エントリーの詳細情報が [Details] パネルに表示されます。

4. **[Details]** パネルの **[Log]** で **[View Log]** をクリックします。

結果

[Upgrade Log] ウィンドウが開き、そのクライアントのローカル ログがウィンドウに表示されます。

必要条件

(オプション) クライアントのローカル ログから情報を選択してコピーします。コピーした情報を、テキストエディターにペーストします。

セクションのすべてのログ エントリーの消去

Avamar Client Manager では、**[Logs]** ページのタスク セクションからすべてのログ エントリーを削除する方法が提供されます。

はじめに

タスクを少なくとも 1 つ完了し、**[Logs]** ページのタスク セクションの 1 つにログ エントリーを生成します。

手順

1. 左側のメニューで、**[Logs]** > **[task_log]** をクリックします。ここで、task_log は **[Logs]** ページのセクションです。
例えば、アップグレードのすべてのエントリーをクリアするには、**[Logs]** > **[Upgrade]** をクリックします。
2. **[Clear All]** をクリックします。
[Alert] ダイアログ ボックスが表示されます。
3. **[Yes]** をクリックします。

結果

Avamar Client Manager が、選択したセクションのログ エントリーをすべて削除します。

第 14 章

Avamar デスクトップ/ラップトップ

本章は、次のトピックで構成されています。

• Avamar デスクトップ/ラップトップの概要	366
• Avamar デスクトップ/ラップトップの要件	367
• Avamar クライアント ソフトウェアのインストール	370
• Avamar デスクトップ/ラップトップのユーザー 認証	373
• Avamar デスクトップ/ラップトップ ユーザー インターフェイス	378
• Avamar デスクトップ/ラップトップを使用したバックアップ	384
• Avamar デスクトップ/ラップトップを使用したリストア	390
• クライアントのバックアップおよびリストア アクティビティの履歴	395
• Avamar デスクトップ/ラップトップ パラメーターの編集	395
• クライアント ログの場所	397

Avamar デスクトップ/ラップトップの概要

Avamar デスクトップ/ラップトップは、Windows および Macintosh 用の Avamar クライアントソフトウェアであり、企業のデスクトップおよびラップトップ コンピューターに拡張機能を追加します。Avamar デスクトップ/ラップトップの多くの機能は、サポートされる Linux コンピューターでも利用可能です。

クライアントのインストールと管理

企業環境では、Microsoft SMS (Systems Management Server) 2003 などのシステム管理ツールを使って、Windows および Macintosh のデスクトップおよびラップトップ コンピューターに、Avamar デスクトップ/ラップトップのインストールを実行することができます。

また、インストール ウィザードを起動して、Avamar デスクトップ/ラップトップ ソフトウェアをローカルにインストールすることも可能です。

クライアント インストール後に、Avamar Client Manager Web ブラウザー ユーザー インターフェイスを使用して、クライアントのアクティブ化、アップグレード、分析、管理を実行できます。

ユーザー認証

Avamar Client Manager のユーザーは、社内の Active Directory または OpenLDAP 対応ディレクトリ サービスを通して認証され、この際に Kerberos 暗号化を使用する場合も、使用しない場合もあります。また、組み込み型の Avamar 認証や、Avamar 認証と LDAP 認証の組み合わせを使用してユーザーを認証することも可能です。

パススルー認証により、ユーザーはログイン スクリーンを使用せずに Web ユーザー インターフェイスにアクセスすることができます。セキュアなメッセージ メカニズムによって、クライアント コンピューターからの情報に基づき、ユーザーが認証されます。また、パススルー認証によって、管理者は非ドメイン ユーザーがコンピューターの各自のローカル アカウントにファイルをリストアできるように設定できます。

ユーザー インターフェイス

Avamar デスクトップ/ラップトップの機能は、次の 2 種類のユーザー インターフェイスから利用可能です。

- クライアントユーザー インターフェイス (クライアントのローカルユーザー インターフェイス) は、Windows 用 Avamar クライアントまたは Mac OS X 用 Avamar クライアントのいずれかをインストールすると、クライアント コンピューターにインストールされます。クライアントユーザー インターフェイスを使用すると、Windows コンピューターでは通知領域 (「システムトレイ」) に、Mac コンピューターではメニュー バーに Avamar アイコンが表示されます。Windows でこのアイコンを右クリックするか、Mac でこのアイコンをクリックすると、クライアントメニューが開き、ここからバックアップ、リストア、プログラム設定、ログにアクセスできます。
- Web ユーザー インターフェイス (Web ブラウザー ユーザー インターフェイス) を使用すると、オンデマンド バックアップまたはリストアの開始や、クライアント コンピューターのバックアップおよびリストア アクティビティの表示、クライアント コンピューターの他のバックアップ設定の構成を実行できます。

バックアップ

ユーザーは、クライアントメニューのシングル クリックを使用するか、Web ユーザー インターフェイスを開いて、インタラクティブなオン デマンド バックアップを実行することで、オン デマンド バックアップを開始できます。オン デマンド バックアップの動作をカスタマイズするオプションには、次のものがあります。

- ユーザーによるオン デマンド バックアップ セットの作成を可能にする。
- 各クライアント コンピューターで 1 日に実行できるバックアップの総数を制限する。
- オン デマンド バックアップの保存ポリシーを変更する。
- オン デマンド バックアップを無効化する。

すべての Avamar デスクトップ/ラップトップクライアントで、スケジュール設定されたバックアップを実行してください。スケジュール設定された日次バックアップでは、利用可能な時間のリストを作成して、バックアップの異なる開始時間をユーザーが選択できるようにすることが可能です。システムは、選択した時間以降できるだけ早く、バックアップを実行します。

また、クライアントが所属するグループで定義されたソース データに、ユーザーがフォルダーを追加できるようにすることも可能です。このフォルダーは、クライアントのオン デマンド バックアップとスケジュール設定されたバックアップの両方に含まれます。

リストア

ユーザーはフォルダー、ファイル、ファイル バージョンを検索または参照して、元の場所または同じコンピューターの新しい場所にリストアできます。データは同じ名前または新しい名前でもリストアできます。

データを同じ名前で元の場所にリストアする場合は、リストア プロセスによって、既存のローカル ファイル バージョンが、リストアされたファイルで上書きされます。このタイプのリストアは、既存のローカル バージョンにエラーやデータ破損の問題がある場合に便利です。

既存のローカル ファイル バージョンが上書きされることを回避するには、新しい場所にリストアするか、新しい名前を付けてリストアします（あるいはその両方を実行します）。

ドメイン ユーザーは、ユーザー プロファイルを所有するすべての Windows または Mac コンピューターから、ログインしている Windows または Mac コンピューターにファイルをリストアできます。

大規模のリストア タスクによってネットワーク パフォーマンスが影響を受けている場合は、ユーザーがリストア可能なデータ量に制限を設けることができます。

ユーザーは、一度に 1 個のリストア タスクのみを開始できます。追加のリクエストはブロックされ、メッセージがユーザーに表示されます。この動作を変更して、ユーザーが複数のリストア タスクを開始できるようにすることが可能です。

アクティビティ ヒストリ

Web ユーザー インターフェイスの [History] ページでは、クライアント コンピューターのリストアおよびバックアップ タスクのステータスについて、14 日分の履歴が表示されます。さらにその期間にバックアップされたフォルダーとファイルの一覧も確認できます。ソース コンピューターにユーザー プロファイルを所有しているドメイン ユーザーの場合は、異なるコンピューターからソース コンピューターのアクティビティ履歴を表示できます。

Avamar デスクトップ/ラップトップの要件

企業のデスクトップおよびラップトップ クライアントに対応する最適な Avamar システムの導入特性を判断する際には、Avamar フィールド セールズ担当者とは協力してください。環境が以降のトピックに記載する要件を満たしている必要があります。

任意の企業におけるデスクトップおよびラップトップに対応した Avamar システムの要件の説明については、このガイドでは扱いません。各企業のデスクトップおよびラップトップ トポロジーでは多くの違いがあるために、このガイドが用意されています。

クライアント コンピューターの要件

Avamar デスクトップ/ラップトップを使用する Avamar クライアント コンピューターは、次のセクションに記載される最小要件を満たす必要があります。

オペレーティング システム要件

Avamar デスクトップ/ラップトップクライアント コンピューターには、Avamar クライアントとともに使用することがサポートされている Windows、Mac、Linux のいずれかのオペレーティング システムが必要です。完全な最新のリストについては、「E-Lab Navigator」を参照してください。

「Avamar バックアップ クライアント ユーザー ガイド」で指定された要件を満たす Windows Server、Mac OS X Server、Linux コンピューターが、サーバー クラスのクライアントとしてサポートされます。一般的に、Avamar Desktop/Laptop の機能拡張は、サーバー クラスのコンピューターでもデスクトップやノートパソコンと同様に動作します。相違点は次のとおりです。

- サーバークラスのコンピューターでは、[Client] メニューまたは [Backup] 通知で [Back Up Now] をクリックすると、コンピューターに個別に割り当てられたデータセットのバックアップが起動されます。

コンピューターに割り当てられたデータセットを表示または編集するには、AUI を使用してクライアントのポリシー設定を編集します。[データセットの編集](#)に手順が記載されています。

- バッテリー電源で動作しているコンピューターでのバックアップを無効化する Avamar デスクトップ/ラップトップの機能は、サーバー クラスのコンピューターでは利用できません。

サーバー クラスのコンピューターでは、バックアップが常に有効化されています。

- Windows サーバークラスコンピューターや Macintosh サーバークラスコンピューターでローカル始動のリストアを無効化すると、それ以降、AUI を使用した場合にのみリストアを実行できるようになります。

ただし、サーバー クラスのコンピューターでローカルの管理権限を持つユーザーは、別のコンピューターにバックアップをリストアできます。

ハードウェア要件

次の表では、Avamar デスクトップ/ラップトップ クライアント コンピューターのハードウェア要件を挙げています。

表 110 Avamar デスクトップ/ラップトップのハードウェア要件

カテゴリ	要件
CPU	1 GHz
RAM	1 GB
ハード ディスクドライブの空き領域	ソフトウェアのインストール用に最小 250 MB のハードディスク空き領域。スナップショットテクノロジーとシステム状態のバックアップでは、領域の追加が必要になることがあります。
ネットワーク インターフェイス	次のいずれか。 <ul style="list-style-type: none"> • 10BaseT 以上で、使用しているプラットフォーム用の最新ドライバーを使って構成される • IEEE 802.11a/b/g で、使用しているプラットフォーム用の最新ドライバーを使って構成される

サポートされる Avamar プラグイン

Avamar デスクトップ/ラップトップでは、次の Avamar ファイル システム プラグインを使用したバックアップおよびリストアをサポートします。

- Windows
- Mac
- Linux

Avamar デスクトップ/ラップトップは、他のオペレーティング システムのアプリケーション プラグインまたはファイル システム プラグインをサポートしません。

ポート要件

TCP データ用ポートは、Avamar サーバーとの双方向通信が可能であることが必要です。

Web ブラウザの要件

Avamar デスクトップ/ラップトップ ユーザー インターフェイスで使用する Web ブラウザは、JavaScript 対応であることに加えて、他の要件も満たしている必要があります。

次の表では、サポートされる Web ブラウザを挙げています。

表 111 Avamar デスクトップ/ラップトップでサポートされる Web ブラウザ

オペレーティング システム	サポート対象の Web ブラウザ
Windows	<ul style="list-style-type: none"> Windows Internet Explorer Mozilla Firefox
Macintosh	Apple Safari
Linux	Mozilla Firefox

注

Avamar ソフトウェアで使用するブラウザは、TLS 1.2 暗号化をサポートする必要があります。

次の表に示した環境変数のいずれかを使用して Web ブラウザーを起動します。

表 112 Avamar デスクトップ/ラップトップで Web ブラウザを起動するための環境変数

ブラウザ	環境変数
KDE	kfmclient
GNOME	gnome-open
その他	BROWSER

ネットワークの条件

Avamar デスクトップ/ラップトップ環境のネットワークは、次の表に示す要件を満たしている必要があります。

表 113 Avamar デスクトップ/ラップトップのネットワーク要件

カテゴリ	要件
プロトコル	TCP/IP
ルーター	Avamar サーバと各クライアント コンピューター間の TCP パケット ルーティングを許可すること。
ファイアウォール (FireWall)	Avamar サーバと各クライアント コンピューター間で、TCP データ用ポート 28002 を使用した双方向通信が可能であること。

表 113 Avamar デスクトップ/ラップトップのネットワーク要件 (続き)

カテゴリ	要件
ネーム システム	各クライアントと Avamar サーバ間の接続が、DHCP や VPN アクセスによって IP アドレスが変更された場合でも、確立されていること。

Avamar クライアント ソフトウェアのインストール

多数の Windows または Mac コンピューターに Avamar クライアント ソフトウェアをインストールする場合には、システム管理ツールを使用する方法が推奨されます。システム管理ツールを使用すると、多くのコンピューターへのソフトウェアのプッシュ インストールをリモートで短時間に実行できます。

多くの場合、ソフトウェアが正常にインストールされたコンピューターのリストをシステム管理ツールで生成することも可能です。このリストを Avamar Client Manager で使用して、コンピューターを登録およびアクティブ化することができます。

Windows 用 Avamar クライアントをインストールする際は、複数のサイレント インストール オプションを使用できます。

通知

クライアント インストール パッケージの名称を変更しないでください。Avamar プッシュ アップグレード メカニズムは、名称変更されたパッケージと互換性はありません。

サポートされているシステム管理ツール

リモート インストールは次のシステム管理ツールでテストおよび承認されています。

- Windows コンピューター上の Microsoft SMS (Systems Management Server) 2003
- Mac コンピューターでの SMS with Quest Software's Quest Management Xtensions for SMS

次のリストにあるツールをはじめとする他のシステム管理ツールを使用して、Avamar クライアント ソフトウェアのプッシュ インストールをリモートで実行することもあります。

- Microsoft System Center Configuration Manager 2007
- IBM Tivoli Management Framework
- HP OpenView ServiceCenter
- Symantec Altiris
- Apple Remote Desktop

システム管理ツールはそれぞれ異なります。ソフトウェアを一連のコンピューターにプッシュするために必要なステップは、ツールによって異なります。ツールの説明書を参照して、これらのタスクを実行するために必要なステップを確認します。

Windows コンピューターへのプッシュ インストール

手順

1. Windows 用 Avamar クライアント用インストーラー パッケージを、システム管理ツールがアクセスできる場所にコピーします。
2. 正しいインストーラー パッケージを各コンピューターにコピーするように、システム管理ツールを設定します。

3. ソフトウェアをインストールするコンピューターを指定します。
4. 次の形式を使用して、インストール起動コマンドを提供します。

```
msiexec /qn /I "path_to_MSI_pkg" SERVER=server DOMAIN=domain
GROUP="groups" UICOMPONENT={0|1} PROGRESSBAR={true|false}
BALLOONMESSAGE={true|false} BACKUPREMINDER=days
```

次の表では、インストール起動コマンドの引数について詳細を説明しています。

表 114 プッシュ インストールの起動コマンドの引数

パラメーター	説明
"path_to_MSI_pkg"	インストーラー パッケージの場所へのフル パスをコンピューターのファイル システムの root に対する相対パスで指定します。
SERVER=server	クライアントに割り当てられた Avamar サーバの IP アドレスまたは完全修飾ドメイン名を指定します。この引数が指定されない場合、または正しくない場合は、クライアントは正常にインストールされますが、アクティブ化されません。
DOMAIN=domain	クライアントの Avamar ドメインを指定します。パスは、パスを示すスラッシュ文字 (Unicode 002F: /) で始まる必要があります。デフォルト値は /clients です。
GROUP=groups	クライアントの Avamar バックアップ グループのコンマ区切りリストを指定します。各グループへのパスは、パスを示すスラッシュ文字 (Unicode 002F: /) で始め、グループパスを引用符で囲む必要があります。例: GROUP="/clients/text,/clients/admin"。デフォルト値は "/Default Group" です。
UICOMPONENT={0 1}	Avamar クライアントを標準 GUI で有効化するか (1)、ユーザー インターフェイスを使用しないエージェント プロセスとして有効化するか (0) を指定します。0 を指定すると、残りのオプションはすべて無視されます。
PROGRESSBAR={true false}	タスクの実行中にクライアントに進行状況ウィンドウを表示するか (true)、非表示にするか (false) を指定します。
BALLOONMESSAGE={true false}	タスクの実行中にクライアントにバルーン メッセージを表示するか (true)、非表示にするか (false) を指定します。
BACKUPREMINDER=days	最後のバックアップからバックアップ通知が表示されるまでの日数を指定します。日数に使用可能な値は 1~7 と、Never です。デフォルト値は 3 です。

UICOMPONENT、PROGRESSBAR、BALLOONMESSAGE、BACKUPREMINDER で設定された値は、クライアント ユーザー インターフェイスのクライアント メニューにあるオプションを使用してユーザーが変更できます。また、アップグレード中にこれらの値を変更することも可能です。

5. システム管理ツールのインストール処理を開始します。

Macintosh コンピューターでのプッシュ インストール

手順

1. Mac OS X 用 Avamar クライアント用インストーラー パッケージを、システム管理ツールがアクセスできる場所にコピーします。
2. 正しいインストーラー パッケージを各コンピューターにコピーするように、システム管理ツールを設定します。
3. ソフトウェアをインストールするコンピューターを指定します。
4. 以下のようにインストール開始コマンドを指定します。

```
/usr/sbin/installer -pkg "path_to_install_pkg" -target
install_location
```

ここで、`path_to_install_pkg` は、コンピューターのファイル システムの `root` に対する相対パスで指定した、インストーラー パッケージの場所へのフル パスです。また、`install_location` はソフトウェアをインストールする場所です。通常、`install_location` は `root (/)` を指定しますが、任意のローカル ボリュームを指定できます。

5. システム管理ツールのインストール処理を開始します。

必要条件

Mac OS X 用 Avamar クライアントをインストールした後、一部のクライアントの再起動が必要になる場合があります。この再起動の原因は、これらのコンピューターで設定されたプロセス データ サイズに変更があったことです。インストーラーは、処理中にプロセス データ サイズが 96 MB 未満であるかどうかを確認しています。Mac OS X 用 Avamar クライアントの最適なパフォーマンスを実現するには、最低 96 MB のプロセス データ サイズが必要です。

プロセス データ サイズが 96 MB 未満の場合、インストーラーはこのサイズを 96 MB に拡張し、再起動を促す通知を表示します。直ちに再起動するか、後で再起動するようにボタンをクリックせずにメッセージを 30 秒より長く放置しておく、通知が非表示にされ、2 時間後に再度表示されます。

コンピューターの再起動を選択しながらも、再起動処理が中断された場合は、通知が再度表示されることはありません。プロセス データ サイズの変更を完了するには、必ずコンピューターを再起動してください。

ローカル クライアントのインストール

ローカルに Avamar デスクトップ/ラップトップ ソフトウェアをインストールするには、グラフィックのインストール インターフェイスを起動します。インストールが終了すると、コンピューターを Avamar サーバに登録し、アクティブ化する準備ができます。

ローカル インストールを実行する場合、ダウンロードリンクからクライアント インストーラーをダウンロードできます。ダウンロードリンクが無効の場合、他のファイル転送方法を使用して、クライアント インストーラーをコンピューターに転送する必要があります。

ローカル インストールを使用する場合、以下のようなデメリットがあります。

- 数千台単位のコンピューターを 1 台 1 台実行する場合、時間がかかる。
- Avamar Client Manager でコンピューター グループの登録、またはアクティブートに使用できるリストが提供されない。

「Avamar バックアップ クライアント ユーザー ガイド」には、Avamar デスクトップ/ラップトップのローカルインストール、アップグレード、アンインストールについての詳細情報が記載されています。

Avamar クライアント ソフトウェアのアンインストール

Avamar クライアント ソフトウェアをクライアント コンピューターからアンインストールすると、それ以降、そのクライアントにスケジュール設定されたバックアップは実行されなくなります。ソフトウェアをアンインストールした後は、バックアップをクライアントにリストアできなくなります。

Avamar クライアント ソフトウェアをアンインストールする際は、クライアントのバックアップを維持することも、削除することも可能です。

- クライアントのバックアップを維持し、これらのバックアップを別のクライアントにリストアするには、Avamar Administrator を使用して、クライアントを破棄します。
- クライアントのバックアップを削除するには、Avamar Administrator を使用してクライアントを削除します。

クライアントの破棄または削除は、Avamar クライアント ソフトウェアのアンインストール前後のいずれかに行います。

Windows でのアンインストール

手順

1. Windows の [プログラムの追加と削除] または [プログラムと機能] アプレットを開きます。
2. 現在インストールされているプログラムのリストで、[Avamar for Windows] を選択します。
3. [Remove] をクリックします。
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。

Mac でのアンインストール

手順

1. ターミナル (シェル) セッションを開きます。
2. 管理者としてログインします。

アンインストール コマンドを実行するには、root (スーパーユーザー) 権限が必要です。root 権限でこのコマンドを実行するには、sudo コマンドを使用します。管理者アカウントまたは sudoers にリストされた別のアカウントが sudo には必要です。

3. 次のコマンドを入力して、uninstall スクリプトを実行します。

```
sudo /usr/local/avamar/bin/avuninstall.sh
```

Avamar デスクトップ/ラップトップのユーザー認証

Avamar デスクトップ/ラップトップでは、ユーザーを認証し、アクセス権限を強制することによってバックアップ データを保護します。Avamar デスクトップ/ラップトップは Avamar システムで実行される別のサーバ プロセスを使用して、内部および外部の方法を通じて認証を容易に行います。すべての Avamar システム インストールには Avamar デスクトップ/ラップトップサーバ プロセスが含まれていません。

パススルー認証

パススルー認証は、暗号化されたチャネルを使用して、クライアント コンピューターからユーザー資格情報にアクセスし、その認証情報をファイル オーナーシップ プロパティと関連付けます。クライアントコ

コンピューターのオペレーティング システムは、コンピューターへのログイン時、または CAC (Common Access Card) テクノロジーを通じてユーザー資格情報を取得します。

Avamar デスクトップ/ラップトップは、パススルー認証を透過的に実行します。ユーザーは、Avamar デスクトップ/ラップトップ ログイン スクリーンを表示することなく、ファイルのバックアップおよびリストアを実行できます。

Avamar デスクトップ/ラップトップは、デフォルトではパススルー認証を有効化します。これは Windows コンピューターおよび Mac コンピューターのユーザーに制限されます。Windows では、ローカル管理者権限のあるユーザーは、新たにログインせずに、コンピューター上のどのユーザーが所有するファイルもリストアすることができます。

パススルー認証は、LDAP 認証でサポートされています。

パススルー認証のためのローカル ユーザー アクセスの有効化

Avamar デスクトップ/ラップトップを構成して、パススルー認証を通じたローカル ユーザー アクセスを行うことができます。ローカル ユーザーとは、ドメイン アカウントの代わりにローカル コンピューターのアカウントを通じて認証されたユーザーを指します。

ローカル ユーザー アクセスを有効化すると、ローカル ユーザーは Avamar クライアントの Web ユーザー インターフェイスにアクセスして、自分が所有するデータを認証されたコンピューターにリストアすることができます。

ローカル ユーザー アクセスでは、Windows コンピューターまたは Mac コンピューターでのパススルー認証が必要です。デフォルトでは、ローカル ユーザー アクセスは無効になっています。

注

ローカル ユーザー アクセスを有効化すると、このサーバに関連づけられたすべてのクライアントおよびバックアップに適用されます。ローカル ユーザー アクセスを有効化する前に、組織内のセキュリティ上の影響を慎重に検討してください。ローカル ユーザー認証は、一般的にドメイン認証よりセキュリティは低下します。

パススルー認証のためにローカル ユーザー アクセスを有効化するには、Avamar サーバ上の `dtlt.properties` ファイルで `allowLocalUsers` プロパティのコメント解除を行い、`#allowLocalUsers=false` を `allowLocalUsers=true` に変更して、値を `true` に設定します。

パススルー認証の無効化

パススルー認証を無効にすることで、すべてのユーザーに Avamar デスクトップ/ラップトップのログイン画面からログインすることを徹底させることができます。パススルー認証を無効化する場合、Windows ユーザーと Mac ユーザーに対して他の認証方法を設定します。

パススルー認証を無効化するには、Avamar サーバ上の `dtlt.properties` ファイルで `userLoginRequired` プロパティの値を `true` に設定します。

LDAP 認証

Avamar デスクトップ/ラップトップを構成してディレクトリ サービスのユーザー名およびパスワードでユーザー認証し、サポートされる LDAP ディレクトリ サービスを使用します。

認証プロセスでは、デフォルトでは SASL (Simple Authentication and Security Layer) バインドで Kerberos を使用します。または、認証プロセスを構成して Simple バインドで平文を使用する認証プロセスを使用します。パススルー認証では SASL バインドのみがサポートされています。平文の Simple バインドはパススルー認証と互換性がありません。

LDAP 認証を使用すると、ユーザーはドメイン ディレクトリ サービスを通じて認証されたドメイン アカウントによって、クライアント コンピューターにログインします。ローカル アカウントを使用するには、ローカル ユーザー アクセスを有効化します。

ユーザー データのセキュリティの向上を図るために、Avamar デスクトップ/ラップトップでは、Windows ユーザーまたは Mac ユーザーのドメイン ユーザー名をクライアント コンピューターから取得し、Avamar デスクトップ/ラップトップログイン スクリーンの読み取り専用フィールドに表示します。

注

バックアップからファイルをリストアするために、Mac の root アカウントを使用することはできません。

Avamar デスクトップ/ラップトップの LDAP 認証の構成

SASL バインドで Kerberos を使用するか、Simple バインドで平文を使用して、サポートされる LDAP ディレクトリ サービスを通じてユーザーを認証するために Avamar デスクトップ/ラップトップを構成するには、LDAP 構成ファイルを編集します。

はじめに

- ディレクトリ サービスに関する情報を使用して、Avamar を構成します。手順については、[サポートされる LDAP ディレクトリ サービスの情報を追加する](#) (91 ページ) を参照してください。
- Avamar デスクトップ/ラップトップ サーバの構成で、認証を分離するために使用するドメイン コンポーネントが正しく設定されていることを確認します。
- SASL バインドで Kerberos を使用するには、Macintosh コンピューターからの LDAP ユーザー認証に使用する Kerberos 領域がデフォルトの Kerberos 領域であることを確認します。

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[LDAP Management]** タブをクリックします。
3. **[Edit LDAP file]** をクリックします。
4. テキスト領域で、次のように user-login-module キーを編集または作成します。
 - SASL バインドで Kerberos を指定するには、user-login-module=kerberos と設定します。
 - Simple バインドで平文を指定するには、user-login-module=ldap と設定します。

Kerberos はデフォルト値です。Avamar デスクトップ/ラップトップは、キーが指定されていない場合にこの値とみなします。
5. **[Save]** をクリックします。
6. **[Close]** をクリックします。

Kerberos 暗号化タイプの変更

Kerberos による LDAP 認証を使用する場合、Kerberos 暗号化タイプの変更が必要になることがあります。

Avamar デスクトップ/ラップトップでは、LDAP サーバーとの通信に、デフォルトで MIT Kerberos 暗号化タイプ「DES cbc mode with CRC-32」を使用します。この暗号化の種類は、Active Directory 環境で KDC (キー配布センター) と競合する可能性があります。競合が発生すると、KDC has no support for encryption type というメッセージが表示されます。この

問題を解決するには、指定した暗号化タイプを `krb5.conf` 構成ファイルから削除し、KDC によって暗号化タイプを選択できるようにします。

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[LDAP Management]** タブをクリックします。
3. **[Edit KRB5 file]** をクリックします。
4. テキスト領域で、次のエントリーを検索します。

```
[libdefaults]
default_tgs_etypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
default_tkt_etypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
```

5. これらのエントリーを次のようにコメントアウトします。

```
[libdefaults]
#default_tgs_etypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
#default_tkt_etypes = des3-cbc-sha1-kd des-cbc-crc des-cbc-md5
```

6. **[Save]** をクリックします。
7. **[Close]** をクリックします。

Avamar 認証

Avamar 認証を使用し、内部の Avamar ドメイン情報に基づいて、ユーザーを認証するように Avamar デスクトップ/ラップトップを構成できます。

Avamar 認証は、Avamar root レベル、Avamar ドメイン レベル、Avamar サブドメイン レベルで認証されるユーザーに対して機能します。このメカニズムでは、まずサブドメイン レベルでチェックを実行します。そのレベルでユーザー名が見つかった場合は、認証を継続します。ユーザー名が見つからなかった場合は、次の上のレベルがチェックされます。このステップは、ユーザー名が見つかるまで、またはユーザー名が見つからずに Avamar の root に達するまで続行します。

例えば、ログイン コンピューター `123abc.example.com` が `/clients/mountain` Avamar サブドメインでアクティブ化されている場合は、ユーザー名が見つかるまで、このメカニズムによって次の順番で Avamar システムがチェックされます。

1. `/clients/mountain` (アクティブ化したサブドメイン)
2. `/clients` (次の上のレベル)
3. `/` (root)

Avamar 認証を使用する場合は、クライアント コンピューターに静的かつ解決可能な完全修飾ドメイン名が必要です。さらに、ユーザーはクライアント コンピューターにローカル ログイン アカウントまたはドメイン ログイン アカウントを所有し、クライアント コンピューターに関連づけられた Avamar ドメインにアカウントを所有していることが必要です。

Avamar デスクトップ/ラップトップでは、Avamar 認証でアカウントにアクセスを付与する際に、Avamar ユーザー アカウントに割り当てられた役割を適用します。ユーザーは、その役割で許可され

ている操作のみを実行できます。唯一の例外があります。それは **[Restore only operator]** 役割を持つユーザーは、Avamar デスクトップ/ラップトップからバックアップを起動できることです。

Avamar 認証の設定

Avamar Administrator の LDAP Management タブで Avamar 認証を使用するように Avamar システムを構成します。

はじめに

Avamar ユーザー レコードをドメイン レベルのリストに追加します。手順については、[ドメインへのユーザーの追加](#) (112 ページ) を参照してください。

手順

1. Avamar Administrator で、**[Administration]** 起動リンクをクリックします。
[Administration] ウィンドウが表示されます。
2. **[LDAP Management]** タブをクリックします。
3. **[Edit LDAP file]** をクリックします。
4. 次のように `user-login-module` キーを編集または作成します。
 - Avamar 認証に加えて、構成および有効化された他のすべての認証方式を使用するには、`user-login-module=mix` を設定します。
 - Avamar 認証に加えて、LDAP を除く構成および有効化された他のすべての認証方式を使用するには、`user-login-module=avamar` を設定します。
5. テキスト領域で、次のキー/値ペアを入力します。

```
avamar-authentication-domains=/domain1,/domain2,/domain3,/. . .
```

ここで `domain1`、`domain2`、`domain3` は、コンマ区切りリストに指定された Avamar ドメイン名です。各ドメイン名では、`root` パス識別子を先頭に指定する必要があります。/。

例えば、Avamar 認証を次のドメインのために使用する場合：

```
/
/clients/accounting
/clients/shipping
```

キー/値のペアを次のように入力します。

```
avamar-authentication-domains=//clients/accounting,/clients/
shipping
```

6. **[Save]** をクリックします。
7. **[Close]** をクリックします。

混合認証

同一の環境で複数の認証方式を使用できます。

複数の認証方式を有効にすると、認証プロセスは次の順序で実行されます。

1. Avamar ドメインにあるクライアントのユーザーが、Avamar 認証を使用して認証されます。
2. Avamar ドメインにあるクライアントにログインしていないユーザーが、パススルー認証を使用して認証されます。

3. 混合認証が有効化されており、LDAP が構成されている場合、LDAP を使用して、指定された Avamar ドメインに割り当てられたクライアントにログインしていない、ユーザーを認証します。

Avamar デスクトップ/ラップトップ ユーザー インターフェイス

Avamar デスクトップ/ラップトップ機能は、クライアント ユーザー インターフェイスおよび Web ユーザー インターフェイスを通して利用できます。

クライアント ユーザー インターフェイス

クライアント ユーザー インターフェイス（クライアントのローカル ユーザー インターフェイス）は、Windows 用 Avamar クライアントまたは Mac OS X 用 Avamar クライアントのいずれかをインストールすると、クライアント コンピューターにインストールされます。クライアント ユーザー インターフェイスを使用すると、Windows コンピューターでは通知領域（「システムトレイ」）に、Mac コンピューターではメニュー バーに Avamar アイコンが表示されます。Windows でこのアイコンを右クリックするか、Mac でこのアイコンをクリックすると、クライアント メニューが開き、ここからバックアップ、リストア、プログラム設定、ログにアクセスできます。

次の表では、クライアント ユーザー インターフェイスで利用可能な機能を挙げています。

表 115 Avamar デスクトップ/ラップトップ クライアント ユーザー インターフェイスの機能

クライアント メニュー アイテム	説明
Back Up Now	シングル クリックによるオン デマンド バックアップを起動します。
Back Up...	インタラクティブなオン デマンド バックアップを起動します。
Restore...	インタラクティブなリストアを起動します。
[Settings] > [Show Backup Reminder (days)]	コンピューターが 1~7 日間バックアップされていないことを知らせるために、バックアップ通知を表示するタイミングを制御します。[Never] を選択して、この通知を無効化することもできます。
[Settings] > [Show Progress Bar]	バックアップ中に [Progress] ウィンドウを表示するかどうかを制御します。[Progress] ウィンドウからバックアップのキャンセル、一時停止、ログの表示を実行できます。
[Settings] > [Show Balloon Messages]	サポートされる Windows コンピューターで、Avamar アイコンの横にシステム ステータスのバルーン メッセージを表示するかどうかを制御します。
[Settings] > [Back Up On Battery Power]	コンピューターがバッテリー電源で動作している場合に、スケジュール設定されたバックアップまたはオン デマンド バックアップをこのコンピューターに実行できるかどうかを制御します。
[Settings] > [Back Up On Wireless]	コンピューターがワイヤレス接続のみでネットワークに接続されている場合に、スケジュール設定されたバックアップまたはオン デマンド バックアップをこのコンピューターに実行できるかどうかを制御します。

表 115 Avamar デスクトップ/ラップトップ クライアント ユーザー インターフェイスの機能 (続き)

クライアント メニュー アイテム	説明
Languages	クライアント ユーザー インターフェイスの言語を選択できます。
[Manage] > [Activate Client]	クライアントをアクティブ化して、クライアントに固有の ID を提供し、クライアントを特定の Avamar サーバにリンクさせます。
[Manage] > [View Console]	クライアント コンソールを開き、ここからタスクのローカル ステータス レコード、エージェント ログ、コンソール ログ、およびワークオーダー ログにアクセスします。
[Manage] > [Create ZIP File of Logs]	管理者がバックアップおよびリストアの問題を診断するために必要なログの ZIP ファイルを作成します。
(Mac のみ) Client Agent Tasks	バックアップ エージェントのプロセスを停止または再開します。
(Mac のみ) Logs	エージェント ログ、コンソール ログのほか、管理者がバックアップおよびリストアの問題を診断するために必要なログの ZIP ファイルを作成するための機能へのアクセスを提供します。
About	Avamar デスクトップ/ラップトップのバージョン、サーバー、著作権の情報を提供します。
Help	クライアントが Avamar サーバでアクティブ化されている場合に、Avamar デスクトップ/ラップトップのオンライン ヘルプを起動します。
Exit	Avamar クライアントをシャットダウンします。

Web ユーザー インターフェイス

Web ユーザー インターフェイス (Web ブラウザー ユーザー インターフェイス) を使用すると、オンデマンド バックアップまたはリストアの開始や、クライアント コンピューターのバックアップおよびリストア アクティビティの表示、クライアント コンピューターの他のバックアップ設定の構成を実行できます。

次の表では、Web ユーザー インターフェイスの主な構成要素について説明します。

表 116 Avamar デスクトップ/ラップトップ Web ユーザー インターフェイスの機能

構成要素	説明
Avamar デスクトップ/ラップトップ ロゴ	Web ユーザー インターフェイスの左上隅にある Avamar ロゴおよびデスクトップ/ラップトップ ロゴを置き換えて、Web ユーザー インターフェイスのブランドを変更できます。
設定メニュー	Web ユーザー インターフェイスの右上隅にある設定メニューによって、次のような Web ユーザー インターフェイス構成の設定を制御できます。 <ul style="list-style-type: none"> ツールチップを表示するかどうか

表 116 Avamar デスクトップ/ラップトップ Web ユーザー インターフェイスの機能 (続き)

構成要素	説明
	<ul style="list-style-type: none"> Web ユーザー インターフェイスの言語 [Search]、[Browse]、[History] の各ページで表示されるエントリーの数 リストアを実行する際に表示されるデフォルトのページ 完全な Web ユーザー インターフェイスを使用するか、参照のみモードを使用して、[Search] と [History] のページのみを表示するか
更新アイコン	Web ユーザー インターフェイス ページを更新します。
ヘルプ メニュー	Avamar デスクトップ/ラップトップのオンライン ヘルプ と、ソフトウェアのバージョン情報へのアクセスを提供します。
[Search] ページ	クライアント コンピューターにあるリストア対象のファイルおよびフォルダーを検索できます。
[Browse] ページ	クライアント コンピューターにあるリストア対象のファイルおよびフォルダーを参照できます。
[Backup] ページ	クライアントが割り当てられたバックアップ グループや、スケジュール設定された次のバックアップに関する情報を提供します。また、クライアントが割り当てられたグループのグループ ポリシーを使用して、クライアントのオン デマンド バックアップを実行することも可能です。[Backup] ページで [Add Data] ボタンが有効化されていると、ユーザーはスケジュール設定されたバックアップおよびオン デマンド バックアップのグループ データセットにフォルダーを追加できます。
[History] ページ	<p>このコンピューターで実行されたバックアップおよびリストア アクティビティについて、14 日分の次のような記録を提供します。</p> <ul style="list-style-type: none"> バックアップ アクティビティのステータスと、各バックアップで転送されたファイル データの一覧表示 リストア アクティビティのステータス
ステータス バー	スケジュール設定された前回のバックアップと次のバックアップの実行日時のほか、前回のバックアップの結果を表示します。ステータス バーには、過去 14 日間の情報が表示されます。前回のバックアップが過去 14 日間より前に行われたものである場合、ステータス バーには No backups found というメッセージが表示されます。ただし、クライアントのグループに割り当てられている保存ポリシーが 14 日間よりも長ければ、[Browse] ページや [Search] ページで依然としてファイルを表示できます。

制限付きのユーザー インターフェイス

Avamar サーバでは、クライアント バックアップ内のファイルおよびディレクトリの数が約 400 万個を超える場合、または Avamar デスクトップ/ラップトップに割り当てられたメモリが不足している場合は、制限付きの Web ユーザー インターフェイスのバージョンをクライアントに表示します。

クライアント バックアップに多数のファイルおよびディレクトリが含まれる場合

このような変更を引き起こす正確なファイルとディレクトリの数は、Avamar サーバで利用可能なメモリに基づいて決まります。

バックアップ内に保存可能なファイルとディレクトリの数には上限はありません。

割り当てられたメモリが不足している場合

制限付きの Web ユーザー インターフェイスのバージョンは、現在の Avamar デスクトップ/ラップトップのリクエストに対処するために Avamar サーバが必要とするメモリが、Avamar デスクトップ/ラップトップに割り当てられているメモリを上回る場合にも、この Avamar サーバにアクセスするすべてのクライアントで表示されます。

この問題を回避するには、各ユーザーがセッション終了時に Web ユーザー インターフェイスからログアウトするように促すことが有効です。

制限付きの Web ユーザー インターフェイスの説明

制限付きの Web ユーザー インターフェイスのバージョンには、次の変更が加えられています。

- Web ユーザー インターフェイスには [Search] および [History] の各ページが表示されません。
- [Browse] ページでファイル バージョンが参照できません。
- [Restore] は、コンピューター上のローカル管理者権限を持ったユーザーのみに許可されるようになります。非管理者ユーザーは、サーバー クラスのコンピューターでローカルで所有するファイルを含む、すべてのファイルをリストアできません。
- リストア データ サイズの制限は強制されません。

Apache Web サーバー認証

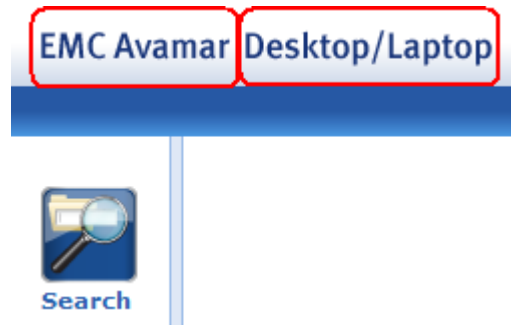
ユーザー セキュリティを保護するために、Web サーバーが信頼済み公開鍵の証明書にページを提供しない場合、セキュア Web ページにアクセスすると、Web ブラウザが認証の警告を表示します。Avamar デスクトップ/ラップトップの Web ユーザー インターフェイスはセキュアな Web ページのみを使用しており、この警告はそのページにアクセスするブラウザで表示されます。警告を回避するには、Avamar 付属の Apache Web サーバにトラステッド公開鍵の証明書をインストールします。

「Avamar 製品セキュリティ ガイド」では、Apache Web サーバーのトラステッド公開鍵の証明書を取得し、インストールする方法について説明します。

Web ユーザー インターフェイスのブランド変更

Avamar クライアントの Web ユーザー インターフェイスのブランドを変更するには、ユーザー インターフェイスの左上隅にある 2 個のロゴ グラフィックを置き換えます。

図 17 Avamar クライアント Web ユーザー インターフェイスの置き換え可能なグラフィック



手順

1. 代わりに使用する 2 つのグラフィックを作成し、`ProductNameAvamar.png` および `ProductNameDTLT.png` と名前をつけます。
 代わりに使用するグラフィックは、次の要件を満たしている必要があります。
 - ファイル形式が `.png` (Portable Network Graphic) であること。
 - 背景が透明であり、グラフィックのテキストと画像の背景のグラデーションが見えること。
 - `ProductNameAvamar.png` は幅が 97 ピクセルで、高さが 18 ピクセルであること。
 - `ProductNameDTLT.png` は幅が 128 ピクセルで、高さが 18 ピクセルであること。
2. コマンド シェルを開きます。
 - a. サーバーに `admin` としてログインします。
 - b. 次のコマンドを入力して、ユーザーを `root` に切り替えます。

```
su -
```
 - c. グリッドの場合、次のコマンドを入力して、`rootid` OpenSSH キーをロードします。

```
ssh-agent bashssh-add /root/.ssh/rootid
```
3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar-tomcat-7.0.59/webapps/dtlt/images/banner
```
4. 次のコマンドを入力して、元のグラフィックのバックアップ コピーを作成します。

```
cp ProductNameAvamar.png ProductNameAvamar.png_origcp
  ProductNameDTLT.png ProductNameDTLT.png_orig
```
5. 新しいロゴを、`ProductNameAvamar.png` および `ProductNameDTLT.png` として現在の作業ディレクトリに移動します。
6. 新しいグラフィックが表示されない場合は、Web ブラウザーで以前表示したファイルのキャッシュ コピーを削除して、ページの更新を行います。

Web ユーザー インターフェイス ポートの変更

Web ユーザー インターフェイスへのアクセスには、Avamar サーバとクライアントの Web ブラウザとの間で HTTPS 通信が必要です。Avamar クライアントのメニューを使用してユーザーがバックアップまたはリストアのリクエストを行うと、クライアント上のデフォルトの Web ブラウザは、標準の HTTPS ポートであるポート 443 で Avamar サーバにコンタクトするように指示されます。Avamar サーバでは、

このポート 443 への初期リクエストは、Web ユーザー インターフェイスの HTTPS ポートであるポート 8443 に切り換えられます。初期コンタクト ポートを変更するには、クライアントの `avsccl.cfg` 構成ファイルとサーバーの Apache SSL 構成ファイルを編集します。

手順

1. 次の手順で、クライアント コンピューターの `avsccl.cfg` ファイルを編集し、新しいポート番号を使用するように設定します。
 - a. テキスト エディターで `avsccl.cfg` を開きます。

Windows クライアントでは、このファイルは `%SystemDrive%\Program Files\avs\var` ディレクトリにあります。他のすべてのクライアントでは、このファイルは `/usr/local/avamar/var` ディレクトリにあります。

この場所に `avsccl.cfg` が存在しない場合は、このファイルを作成してください。
 - b. ファイルに次の行を追加します。


```
--dtltp-port=n
```

ここで、`n` は初期コンタクト ポート番号です。
 - c. `avsccl.cfg` を保存して、閉じます。
 - d. クライアントを再起動します。
2. 次の手順で、Avamar サーバの Apache SSL 構成ファイルを編集します。
 - a. コマンド シェルを開き、シングル ノード サーバー、またはマルチ ノード サーバーのユーティリティ ノードで `admin` としてログインします。
 - b. Apache SSL 構成ファイルをテキスト エディターで開きます。

Red Hat Enterprise Linux では、ファイルは `/etc/httpd/conf.d/ssl.conf` です。SuSE Linux Enterprise Server では、ファイルは `/etc/apache2/vhosts.d/vhost-ssl.conf` です。
 - c. HTTPS ポートリスニング ディレクティブを見つけて、`Listen 443` を `Listen n` に変更します。ここで、`n` は初期コンタクト ポート番号です。
 - d. ファイルを保存して閉じます。
 - e. `apachectl restart` と入力して、Apache サーバー プロセスを再開します。

安全なトークン time-out 値の変更

Avamar デスクトップ/ラップトップには、クライアントの Web ブラウザー内でバックアップまたはリストアセッションを開始するために使用する URL の一部として、安全な一時トークンが含まれています。トークンの有効期限が切れる前、またはセッションが拒否される前に、クライアントの Web ブラウザで Avamar サーバとの HTTPS 接続を確立する必要があり、確立できない場合はバックアップまたはリストアを実行できません。デフォルトの time-out 値である 20 秒は編集可能です。

手順

1. コマンド シェルを開き、次のいずれかの方法を使用してログインします。
 - シングル ノード サーバーには、`admin` としてサーバーにログインします。
 - マルチ ノード サーバには、
 - a. `admin` としてユーティリティ ノードにログインします。

b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

2. 次のコマンドを入力して、MCS を停止します。

```
dpnctl stop mcs
```

3. 次のコマンドを入力して、作業ディレクトリを変更します。

```
cd /usr/local/avamar/var/mc/server_data/prefs
```

4. テキスト エディターで mcserver.xml を開きます。

5. <node name="dtlt">セクションで、<entry key="expire_data_after_secs" value="20" /> from 20 の値を編集して、新しい time-out 値を秒単位で設定します。

6. 変更を保存して、ファイルを閉じます。

7. 次のコマンドを入力して、MCS およびスケジューラを開始します。

```
dpnctl start mcs
dpnctl start sched
```

クライアントが代替のファイル参照方式を使用するように強制する

Avamar クライアントの Web ユーザー インターフェイスでは、クライアント コンピューターで OS 固有のファイル参照サービスを使用して、ファイル マネージャ インターフェイスを提供しており、ユーザーはこれによってバックアップまたはリストア対象のローカル ファイルおよびフォルダーを選択します。ただし、クライアントが NAT を使用していたり、クライアントのポート 28002 がファイアウォール ルールによってブロックされていたりして、これらのサービスが利用できない場合は、代替のファイル参照方式が提供されます。クライアントが代替のファイル参照方式を使用するように要求できます。

この変更を行う理由の 1 つとして、リムーバブル メディアのサポートが挙げられます。デフォルトのファイル参照方式では、リムーバブル メディアがサポートされませんが、代替のファイル参照方式ではサポートされます。

代替となる方式では、Java アプレットを使用してファイル参照サービスを実現します。デフォルトのサービスが使用できない場合、ユーザーが代替方式を選択して許可すると、Java アプレットがロードされます。アプレットのロード中には、Avamar サーバの Web サイト認定書に関する認証警告、および Java アプレットのデジタル署名がユーザーに表示される場合があります。これらの警告を確認しなければ、アプレットがロードされません。

アプレットのロードが完了すると、Web ページは最新の情報に自動的に更新され、Avamar クライアントの Web ユーザー インターフェイスでアプレットを使用できるようになります。ユーザーがタスクを再開できるのは、ページが最新の情報に更新された後になります。

クライアントが代替のファイル参照方式を使用するように強制するには、Avamar サーバ上の dtlt.properties ファイルで useAppletToBrowseLocalFile プロパティを追加し、値を true に設定します。

Avamar デスクトップ/ラップトップを使用したバックアップ

Avamar デスクトップ/ラップトップでは、クライアント バックアップを開始する方法がいくつかあります。

次の表では、クライアント バックアップを開始する方法、その方法で使用できるオプションについて説明します。

表 117 Avamar デスクトップ/ラップトップ クライアント バックアップを開始する方法の説明

方法	説明	オプション	Dataset
Scheduled	Avamar サーバは、クライアントのグループに指定されたスケジュールに従って、クライアントを自動的にバックアップします。	<ul style="list-style-type: none"> User selected backup time Add data 	スケジュール設定グループに対して指定されたデータセット、またはコンピューターに割り当てられたデータセット。[Add Data] を有効化した場合、データセットにはユーザーが追加したフォルダーも含まれます。
Single-click	ユーザーがクライアントで [Back Up Now] をクリックすると、Avamar サーバはクライアントのバックアップをキューイングします。	<ul style="list-style-type: none"> Add data 	コンピューターに関連づけられた各グループのデータセット、またはコンピューターに割り当てられたデータセット。[Add Data] を有効化した場合、データセットにはユーザーが追加したフォルダーも含まれます。
対話的	ユーザーが [Back Up] をクリックすると、Web ユーザー インターフェイスが表示されます。ユーザーは使用可能な開始オプションとデータ オプションから選択して、[Backup] ページで [Back Up Now] をクリックします。Avamar サーバは、Avamar サーバのバックアップ キューにバックアップを追加します。	<ul style="list-style-type: none"> Add data On-demand backup set 	クライアントに割り当てられたグループの中からユーザーが選択したグループのデータセット。[Add Data] を有効化した場合、データセットにはユーザーが追加したフォルダーも含まれます。[Select Now] (オン デマンド バックアップ セット オプション) が有効化されており、クリックされた場合、データセットにはユーザーが選択したファイルとフォルダーのみが含まれます。

スケジュール設定されたバックアップ

Avamar デスクトップ/ラップトップクライアント コンピューターのスケジュール設定されたバックアップは、環境にある他の Avamar クライアント コンピューターをバックアップするのと同じ方法で行います。Avamar Administrator を使用してバックアップのデータセット、スケジュール、保存ポリシー、グループを作成します。

Web ユーザー インターフェイスの Avamar デスクトップ/ラップトップ Backup ページには [] クライアントと関連づけられたグループが表示されます。

また [Backup] ページには、Avamar デスクトップ/ラップトップクライアントと関連づけられたグループごとに、スケジュール設定された次のバックアップ時間も表示されます。グループのポリシーは、通常、そのグループのバックアップのスケジュール開始時間を決定します。個々の Avamar デスクトップ/ラップトップ クライアントで、ユーザーがクライアントのスケジュール設定されたバックアップに異なる開始時間を選択できるようにすることができます。

スケジュール設定されたバックアップの開始時間をユーザーが選択可能にする

グループ ポリシーで割り当てられたスケジュール設定バックアップの開始時間と異なる開始時間を、Avamar デスクトップ/ラップトップ クライアントのユーザーが選択できるように設定します。

Avamar デスクトップ/ラップトップ クライアントのこの機能を有効化すると、ユーザーは Web ユーザー インターフェイスの [Backup] ページに表示される管理者定義時間のリストから時間を選択できるようになります。ここで選択した開始時間は、クライアントでスケジュール設定された後続のバックアップすべてを実行する際に適用されます。

保護機能に脆弱性が生じないように、管理者が Avamar デスクトップ/ラップトップ Override Daily Schedule からその時間を削除した場合でも、[] クライアントではユーザーが選択したバックアップ開始時間が引き続き使用されます。次回ユーザーが Web ユーザー インターフェイスにログインする

と、Avamar デスクトップ/ラップトップ Backup ページから新しい開始時間を選択するように [] にプロンプトが表示されます。

Avamar サーバーは、ユーザーが選択した開始時間とクライアントのグループを関連づけます。グループからクライアントを削除すると、そのクライアントに対してユーザーが選択した開始時間も削除されます。

手順

1. 日次スケジュールを使用するグループにクライアントが所属していることを確認します。
2. AUI を使用して、[**Override Daily Schedule**] に時間エントリを追加します。

注

[**Override Daily Schedule**] に、Avamar サーバのタイムゾーンを使用する時刻の値が表示されます。Avamar デスクトップ/ラップトップは、[**Backup**] ページに時間を表示するときに、クライアントのタイムゾーンを使用します。

3. Avamar Administrator を使用して、クライアントに対して [**Allow override of group's daily schedule**] を有効化します。

[Add data] オプション

スケジュール設定されたバックアップとオン デマンド バックアップでは、Avamar デスクトップ/ラップトップクライアント コンピューターのグループ ポリシー ベースのバックアップに含めるフォルダーをユーザーが指定できます。

[Add data] オプションが有効化されている場合、Avamar デスクトップ/ラップトップクライアント コンピューターが属している各グループのデータセットに、ユーザー選択のフォルダーを追加することで、Avamar デスクトップ/ラップトップはクライアント コンピューターのバックアップ データセットを作成します。Avamar デスクトップ/ラップトップは、各グループのデータセット ポリシーでの除外と包含をユーザーが指定したフォルダーに適用します。

Avamar Administrator を使用してこのオプションを有効化します。

[Add data] オプションを有効化した後、ユーザーは Web ユーザー インターフェイスの [**Backup**] ページで [**Add Data**] をクリックして、フォルダーを選択し、それらのフォルダーを追加できます。

シングル クリック バックアップ

ユーザーは、クライアント メニューまたはバックアップ通知ダイアログ ボックスで Avamar デスクトップ/ラップトップ Back Up Now ボタンを 1 回クリックすることで、[] クライアント コンピューターでオン デマンド バックアップを開始できます。

シングル クリック バックアップに含まれるデータは、クライアント コンピューターのオペレーティング システムによって異なります。次の表では、特定のオペレーティング システムのために含まれているデータについて説明します。[Add data] オプションを有効化した場合、Avamar デスクトップ/ラップトップはユーザーが選択したフォルダーもバックアップ データに追加します。

表 118 シングル クリックによるオン デマンド バックアップのデータセット

オペレーティング システム	バックアップに含まれるデータ
<ul style="list-style-type: none"> • Windows • Mac 	クライアントが所属する各グループのデータセット

表 118 シングル クリックによるオン デマンド バックアップのデータセット (続き)

オペレーティング システム	バックアップに含まれるデータ
<ul style="list-style-type: none"> • Linux • Windows サーバ • Mac OS X サーバ 	コンピュータに割り当てられたデータセット

インタラクティブなバックアップ

対話形式のバックアップでは、ユーザーはクライアントと関連づけられたバックアップ グループを選択して、そのグループの設定を使用してクライアントをバックアップできます。オン デマンド バックアップ セットを有効化した場合、対話形式のバックアップでは、ユーザーはむしろ選択したファイルとフォルダーのみのバックアップを選択することもできます。

グループの選択

1つのグループのインタラクティブなバックアップを実行するには、次の手順を実行します。

1. クライアントメニューで **[Backup]** を選択します。
2. Web ユーザー インターフェイスの **[Backup]** ページでバックアップ グループを選択します。
3. **[Back Up Now]** をクリックします。

ユーザーがグループの対話形式のバックアップを実行する場合、選択したグループと関連づけられたすべてのポリシーがバックアップに適用されます。

グループの対話形式のバックアップでは、選択したグループのみがバックアップされるため、グループの対話形式のバックアップはシングル クリック バックアップとは異なります。

ファイルとフォルダーの選択

クライアントに割り当てられたグループ ポリシーにかかわらず、ユーザーが Avamar デスクトップ/ラップトップ クライアントで選択したファイルをバックアップできるようにするには、オン デマンド バックアップ セットを有効化します。オン デマンド バックアップ セットを有効化すると、Avamar デスクトップ/ラップトップ クライアントになっている Windows、Mac、Linux コンピューターのユーザーは、オン デマンド バックアップでバックアップするためにフォルダーとファイルのセットを作成できます。ユーザーは複数のセットを作成して、再使用のために保存することができます。また、セットに基づくバックアップを Avamar サーバのバックアップ キューに送信できます。

オン デマンド バックアップ セットは、Avamar デスクトップ/ラップトップ クライアントに割り当てられたグループ ポリシーに基づいてバックアップされたデータを変更することはありません。

Avamar デスクトップ/ラップトップ クライアントから開始できるオン デマンド バックアップ セット バックアップの数は、Avamar サーバを構成して制限することができます。

Data Domain にバックアップ データを保存するには、次の情報を考慮します。

- Avamar サーバ用に Data Domain システムが構成される場合、オン デマンド バックアップは GSAN に保存されます。
- Avamar サーバ用に 1つの Data Domain システムが構成されている場合、オン デマンド バックアップは Data Domain に保存されます。
- Avamar サーバ用に複数の Data Domain システムが構成されている場合、オン デマンド バックアップは、使用可能なスペースの多い Data Domain に送信されます。

ユーザーによるオン デマンド バックアップ セットの作成を可能にする

Avamar デスクトップ/ラップトップを使用する Windows、Mac、Linux クライアントのユーザーに、オン デマンド バックアップ セットの作成を許可します。

手順

1. クライアントのグループ ポリシー設定を上書きすることにより、Avamar Administrator の **[Allow file selection on client initiated backups]** 設定を有効にします。
2. Avamar サーバ上の `dtlt.properties` ファイルで `allowUserInitiatedBackupsFileSelection` キーの値を `true` に変更します。
3. ユーザーは次の手順でオン デマンド バックアップ セットを作成します。
 - a. Avamar デスクトップ/ラップトップ クライアント コンピューターで、Avamar アイコンを右クリックして、**[Back Up...]** を選択します。
Web ユーザー インターフェイスの **[Backup]** ページが開きます。
 - b. **[Select folders and files to backup]** で、**[Select Now]** をクリックします。
[On-Demand Backup Sets] ダイアログ ボックスが表示されます。
 - c. バックアップするには、**[OK]** をクリックし、フォルダーおよびファイルを選択します。
 - d. バックアップ セットを再使用するために保存するには、**[Save backup set as]** でバックアップ セットの名前を入力して、**[Save]** をクリックします。
 - e. (オプション) オン デマンド バックアップ セットのバックアップをバックアップ キューに追加するように Avamar サーバに指示するには、**[Start Backup]** をクリックして **[OK]** をクリックします。
4. ユーザーは、保存済みのオン デマンド バックアップ セットのバックアップをバックアップ キューに追加するように Avamar サーバに指示します。
 - a. Avamar デスクトップ/ラップトップ クライアント コンピューターで、Avamar アイコンを右クリックして、**[Back Up...]** を選択します。
Web ユーザー インターフェイスの **[Backup]** ページが開きます。
 - b. **[Select folders and files to backup]** で、**[Select Now]** をクリックします。
[On-Demand Backup Sets] ダイアログ ボックスが表示されます。
 - c. **[Load Backup Set]** で、バックアップ セットを選択します。
 - d. **[Start Backup]** をクリックして **[OK]** をクリックします。

オン デマンド バックアップの制限の設定

Avamar サーバのタスク キューにユーザーが追加できるオン デマンド バックアップ セット バックアップの数に制限を設定します。

デフォルトでは、Avamar サーバはオン デマンド バックアップ セット バックアップに次のルールを使用します。

- タスク キューでは、クライアントからのオン デマンド バックアップ セット バックアップを、一度に1つだけ実行することができます。
- クライアントのバックアップを実行している場合、オン デマンド バックアップ セット バックアップを開始することはできません。

- ユーザーがタスク キューに追加できるクライアントのオン デマンド バックアップ セット バックアップの数には制限がありません。

Avamar デスクトップ/ラップトップクライアント コンピューターに対して 1 日に実行できるオン デマンド バックアップ セット バックアップの数に制限を設定するには、Avamar サーバの `dtlt.properties` ファイルで `restrictBackupsPerDay` プロパティを設定します。

次の表に、使用可能な値を示します。

表 119 `restrictBackupsPerDay` プロパティでサポートされる値

値	説明
false	1 日に正常に実行できるオン デマンド バックアップ セット バックアップの数に制限はありません。[No limit] がデフォルト設定です。
0	ユーザーは、オン デマンド バックアップ セット バックアップを実行できません。
n	各クライアントに対して、オン デマンド バックアップ セット バックアップを、1 日に n 回よりも多く実行することはできません。ここで n は 100 以下の正の整数です。day は Avamar サーバのタイムゾーンで午前 0 時から午前 0 時までと定義されます。

指定値は、Avamar サーバでアクティブ化されたすべてのクライアントに適用されます。Avamar デスクトップ/ラップトップ クライアント コンピューターのすべてのユーザーによる、正常に完了したバックアップのすべてが、1 日に許可されるバックアップの総数に加算されます。

注

この制限は、ユーザーが作成したオン デマンド バックアップ セットに基づくバックアップのみに適用されます。

オン デマンド バックアップの無効化

ユーザーは Avamar デスクトップ/ラップトップ クライアント コンピューターからオン デマンド バックアップを実行できなくなります。この設定は、シングル クリックのオン デマンド バックアップと対話形式のオン デマンド バックアップの両方に適用されます。

手順

1. Avamar Administrator で、[Policy] 起動リンクをクリックします。
[Policy] ウィンドウが表示されます。
2. [Clients] タブをクリックします。
3. 単一のクライアントまたは複数のクライアントでオン デマンド バックアップを無効化します。

クライアントの数	オン デマンド バックアップを無効化するステップ
1	<ol style="list-style-type: none"> a. クライアントを選択し、[Edit] をクリックします。 b. [Edit Client] ダイアログ ボックスで、[Allow client initiated backups] を選択解除します。

クライアントの 数	オン デマンド バックアップを無効化するステップ
	c. [OK] をクリックします。
2 個以 上	<p>a. クライアントを選択し、[Edit] をクリックします。</p> <p>b. [Edit Multiple Clients] ダイアログ ボックスで [Allow client initiated backups] を [No] に変更します。</p> <p>c. [Apply Change] をクリックします。</p> <p>d. [OK] をクリックします。</p>

オン デマンド バックアップの保存ポリシーを変更する

[End User On Demand Retention] ポリシーでは、オン デマンド バックアップのデータ保存を制御します。Avamar サーバの [End User On Demand Retention] ポリシーは、Avamar Administrator を使用して変更することができます。変更は、該当するサーバとともにアクティベートされたクライアントから開始したすべてのオン デマンド バックアップに適用されます。変更が適用されるのは、変更後に実行されたオン デマンド バックアップのみです。

手順

1. Avamar Administrator で、[Tools] > [Manage Retention Policies] を選択します。
[Manage All Retention Policies] ウィンドウが表示されます。
2. リストから [End User On Demand Retention] を選択し、[Edit] をクリックします。
[Edit Retention] ダイアログ ボックスが表示されます。
3. [Retention period] に数字を入力し、時間の単位 ([days]、[weeks]、[months] または [years]) を選択します。
4. [OK] をクリックします。

Avamar デスクトップ/ラップトップを使用したリストア

次のトピックでは、Avamar デスクトップ/ラップトップでリストアを実行し、リストアに関連する設定を制御する際の情報について説明します。

リストア対象のデータを見つける

Avamar デスクトップ/ラップトップ ユーザーは、Web ユーザー インターフェイスを使用して、リストア対象のフォルダー、ファイル、ファイル バージョンを参照または検索することができます。

リストア対象のデータを参照する

左側のメニューから [Browse] を選択して、ツリー ビューでクライアント コンピューターのバックアップを表示し、リストア対象のフォルダーおよびファイルを参照して見つけます。

クライアントのすべてのバックアップではなく、特定のバックアップを参照するには、[Backup Date] と [Time] を使用して、バックアップの日付と時間を選択します。

リストア対象のデータを検索する

Web ユーザー インターフェイスの左側のメニューから [Search] を選択して、リストアする特定のフォルダーまたはファイルを検索します。検索を開始するには、検索文字列を検索フィールドに入力し

て、[**Search**] をクリックします。検索結果は収集されるとすぐに表示され、進行状況インジケータによって、検索時間に関する情報が提供されます。

検索フィールドに指定する検索文字列は、255 文字以内である必要があり、大文字と小文字は区別されません。検索文字列でサポートされるワイルドカードには、0 文字以上を示すアスタリスク (*) や 1 文字を示す疑問符 (?) があります。

文字列は、クライアント コンピューターのバックアップにあるすべてのフォルダーとファイルの名前と照合されます。フォルダーまたはファイル名のすべてまたは一部がこの文字列に一致すると、そのフォルダーまたはファイル名が検索結果に表示されます。

ファイル バージョンを選択する

クライアント コンピューターのバックアップには、バックアップされているファイルの多くについて、複数のバージョンが含まれます。ファイルをバックアップした後に変更した場合、次のバックアップに新しいバージョンのファイルが含まれます。各バージョンは、Avamar 管理者が設定した保存期間に達するまで保持されます。

クライアント バックアップに含まれるファイルのバージョン数は、次のような多くの要因によって異なります。

- バックアップされたデータを保持する期間
- バックアップの頻度
- ファイルが編集される頻度

クライアントのバックアップに複数のバージョンのファイルが含まれている場合は、リストア対象のデータを参照または検索する際に、バージョン アイコンがファイル名の横に表示されます。最新のバージョンではないファイルのバージョンを選択するには、バージョン アイコンをクリックして、希望するバージョンを選択します。その後、クライアント コンピューターにある既存ファイルを上書きするか、新しい名前でのファイル バージョンをリストアするかを選択します。

リストアのタイプ

Avamar デスクトップ/ラップトップ ユーザーは、元の場所、または同じコンピューター上の新しい場所にデータをリストアできます。データは同じ名前または新しい名前でもリストアできます。

データを同じ名前で元の場所にリストアする場合は、リストア プロセスによって、既存のローカル ファイル バージョンが、リストアされたファイルで上書きされます。このタイプのリストアは、既存のローカル バージョンにエラーやデータ破損の問題がある場合に便利です。

既存のローカル ファイル バージョンが上書きされることを回避するには、新しい場所にリストアするか、新しい名前を付けてリストアします（あるいはその両方を実行します）。

ドメイン ユーザーは、ユーザー プロファイルを所有するすべての Windows または Mac コンピューターから、ログインしている Windows または Mac コンピューターにファイルをリストアできます。Avamar サーバにある `dtlt.properties` ファイルの

`disableRestoreFromAlternateComputer` プロパティの値を `true` に設定して、別のコンピューターからのリストアを無効にすることができます。これは、すべてのクライアントに影響するグローバルなプロパティです。

リストアでの Linux および Mac の制限事項

ルートフォルダーへの書き込みアクセス権がない Linux および Mac のユーザーは、Avamar デスクトップ/ラップトップを使用して完全なディレクトリ構造を元の場所にリストアすることはできません。オペレーティング システムではこのタイプのリストアを、ルートフォルダーへの許可されていない書き込みが試みられたものとみなし、これを防止します。

次のすべての条件に当てはまる場合、完全なディレクトリ構造のリストアを試みると失敗します。

- ルートフォルダーへの書き込みアクセス権を持たないユーザー アカウントでユーザーが Mac または Linux のコンピューターにログインしている。

- ユーザーが Avamar 認証方式を使用して Avamar デスクトップ/ラップトップ Web ユーザー インターフェイスにログインしている。
- Avamar デスクトップ/ラップトップ Browse ページで、ユーザーが完全なディレクトリ構造を選択している。
- ユーザーがリストア用に新しい場所を選択していない。

解決策

この制限を回避するには、次のリストア方法のいずれかを使用します。

- 完全なディレクトリ構造を新しい場所にリストアする。
- ディレクトリ構造内のすべてのファイルより少ない量をリストアする。
たとえば、リストア セットの最も深い階層のフォルダーから 1 つのファイルをクリアします。オペレーティング システムでは、後続のリストアをルート フォルダーの下のフォルダーへの一連の書き込み処理として認識するため、すべてのファイルよりも少ない量のリストアがうまく機能します。

リストア要件

別のコンピューターからリストアするには、リストアを実行する前に、権限に関する要件やその他の要件について確認してください。

リストアの権限

ユーザーが参照、検索、リストアできるデータは、ユーザー ログイン アカウントの権限によって異なります。

ユーザーがリストア対象のデータを検索または参照する際は、現在のログイン認証情報と、クライアント コンピューターからバックアップされているデータに基づいて、表示される結果がフィルターされます。次の表ではフィルター機能に関する詳細が説明されています。

表 120 Avamar デスクトップ/ラップトップ データリストアのフィルター機能

データタイプ	Windows 上のフィルター機能	Mac 上のフィルター機能
フォルダ	ログイン ユーザーが所有者であるすべてのフォルダー、またはログイン ユーザーの属するグループが所有権を持つすべてのフォルダー、およびログイン ユーザーに権限が与えられているフォルダーまたはファイルを含むすべてのフォルダーが表示される。	ログイン ユーザーが所有者として読み取り権限を持つすべてのフォルダー、またはフォルダーのグループ権限やその他の権限に基づいてログイン ユーザーが読み取り権限を持つすべてのフォルダーが表示される。
ファイル	ログイン ユーザーが所有するすべてのファイルが表示される。	ログイン ユーザーが所有するすべてのファイルが表示される。

ユーザーがリストア対象のデータを参照する際、次のアクションが発生します。

- ユーザーが所有権を持たないフォルダーは、ユーザーが所有権を持つフォルダーまたはファイルへのファイル システム パスに表示されます。このオプションは、コンピューター上のファイル システムをより正確に表示するために役立ちます。
- フォルダーの横にグレーのチェックボックスが表示されます。このフォルダーをパスに含むフォルダーまたはファイルをリストアする際に、このフォルダーはリストアされません。

ユーザーは、各自のログイン認証情報によってオペレーティング システムの書き込み権限がリストア場所に与えられている場合のみ、データをリストアできます。クライアント コンピューター上のデータと同じパスと名前を持つデータをリストアするには、まずログイン認証情報によってユーザーが既存データの所有者として認証されてから、リストアが実行される必要があります。

Windows でファイルをリストアするには、ローカル セキュリティでログイン アカウントに Restore files and directories ユーザー権限が設定されている必要があります。このユーザー権限は、Administrators グループまたは Backup Operators グループに属しているアカウントにデフォルトで割り当てられます。これらのいずれのグループにも属さないアカウントや、このユーザー権限を含む他のグループにも属さないアカウントには、このアカウントを使用してデータをリストアする前に、この権限を割り当てます。

別のコンピューターからリストアを行う場合の要件

別のコンピューターからリストアを行うには、次の表にある要件を満たしてください。

表 121 Avamar デスクトップ/ラップトップで別のコンピューターからリストアを行う場合の要件

カテゴリ	要件
オペレーティング システム	<ul style="list-style-type: none"> Windows オペレーティング システム Mac オペレーティング システム <p>注</p> <p>Windows コンピューターと Mac コンピューター間のリストアはサポートされています。</p>
アカウント タイプ	ドメイン
プロファイル	<p>ソース コンピューターとターゲット コンピューターが、ユーザーのドメイン アカウントのローカル プロファイルを備えていること。</p> <p>注</p> <p>ドメイン アカウントのローカル プロファイルは、ユーザーが初めてコンピューターにログインすると、自動的に作成されます。</p>
Avamar クライアント	バージョン 7.0 以降がソースとターゲットの両方にインストールされていること。
Avamar サーバ	ソースとターゲットのいずれも、同じ Avamar サーバでアクティブ化されており、このサーバが Avamar 7.0 以降を実行していること。
バックアップ	<p>少なくとも 1 つは認定されたバックアップがあること。認定されたバックアップは、以下の操作の後、完了したバックアップを指します。</p> <ul style="list-style-type: none"> Avamar デスクトップ/ラップトップ 7.0 以降がソース コンピューターにインストールされていること。 ユーザーのドメイン アカウントのローカル プロファイルが、ソース コンピューターで作成されていること。

デフォルトでは、バックアップ時に Windows ソース コンピューターのローカル管理者権限を持つユーザーは、所有権にかかわらず、ソース コンピューターからのファイルをターゲット コンピューターにリストアすることができます。この動作を変更し、そのアクセスを彼らが所有しているファイルに制限することができます。Windows 管理者のファイル アクセスを制限するには、Avamar サーバ上の

`dtlt.properties` ファイルで `checkAlternateComputerOwnership` プロパティの値を `true` に変更します。

リストアの制限

単一のリストア タスクで処理するデータ量や、クライアント コンピューターで実行するコンカレント リストア タスクの数を制限することができます。

リストア データ サイズ制限

Avamar クライアント ユーザーには、通常、単一のタスクでリストアされるデータ量に制限はありません。このデフォルト設定によって、ユーザーは単一のタスクでバックアップ全体をリストアすることができます。大量のリストア タスクによって、ネットワークに望ましくない負荷がかかる可能性があります。大量のリストア タスクにより発生するネットワーク負荷をコントロールするためには、リストア データ サイズ制限を設定します。

制限を設定すると、個々のユーザーはその制限を超えたデータを 1 回のリストア タスクで実行できなくなります。ユーザーが制限を超えたファイルをリストアするには、制限を越えない範囲でタスクを複数回実行するか、管理者がリストアを実行する必要があります。

通知

リストア データ サイズ制限は、サーバー クラスのクライアント（大量のバックアップ データセットを持つクライアント）には適用されないように設計されています。

リストア データ サイズ制限を指定するには、Avamar サーバ上の `dtlt.properties` ファイルで `limitRestoreSize` キーのコメント解除を行い、データ サイズ制限の値を MB 単位で設定します。

リストア キュー制限

Avamar クライアントの Web ユーザー インターフェイスでは、リストア タスクがすでにキューに存在しているクライアントのリストア リクエストをブロックすることで、ネットワークとサーバの負荷を最小限に抑えます。1 つのリストア タスクがペンディング中に、新しいリストアを開始するユーザーには、リクエストはブロックされるというメッセージが送られます。ペンディング中のタスクが完了した後で、ユーザーは新しいリストア タスクを開始できます。この動作を変更して、ユーザーが複数のリストア タスクを開始できるようにすることが可能です。その変更は、Avamar サーバのすべてのクライアントが対象になります。

リストア キュー制限を削除するには、Avamar サーバ上の `dtlt.properties` ファイルで `disallowMultipleRestores` プロパティの値を `false` に変更します。

レプリケートされたバックアップのリストア

Avamar Client Manager のレプリケーション コマンドを使用して、Avamar クライアントを新しい Avamar サーバに移動することが可能です。クライアントを移動すると、新しいサーバにクライアントのバックアップがレプリケートされます。Avamar デスクトップ/ラップトップは、Web ユーザー インターフェイスで参照や検索に使用可能になるまで、レプリケートされたバックアップにインデックスを作成する必要があります。

クライアントが移動された後で、ユーザーがクライアントの Web ユーザー インターフェイスからログインすると、**[Replicated Backups Available]** ダイアログ ボックスが表示されます。ユーザーは、レプリケートされたバックアップのインデックス作成を開始するか、インデックス作成を開始せずにダイアログ ボックスを閉じることができます。ユーザーがインデックス作成を開始せずにダイアログ ボックスを閉じると、アラート アイコンが Web ユーザー インターフェイスのバナー バーに表示されます。このアラート アイコンからインデックス作成を開始することも可能です。

新しいサーバに移動されたコンピューターに対しては、インデックス作成は一度限りのタスクです。このタスクは、開始された同じセッション内で実行されます。これが完了すると、Avamar デスクトップ/

ラップトップは更新コマンドを Web ブラウザに送信します。レプリケートされたバックアップからのデータは、Web ユーザー インターフェイスに表示されます。

クライアントのバックアップおよびリストア アクティビティの履歴

Avamar デスクトップ/ラップトップ Web ユーザー インターフェイスの **[History]** ページでは、クライアント コンピューターで実行されたバックアップおよびリストア アクティビティの 14 日間分の記録が表示されます。

[History] ページの **[Activity History]** セクションには、過去 14 日間に開始された各バックアップおよびリストアに関する情報が表示されます。また、このセクションにはバックアップに関するより詳細な情報へのリンクも提供されます。この情報には、アクティビティの結果、開始日時、アクティビティの所要時間、データ量、ワークオーダー ID が含まれます。バックアップのアクティビティ ラベルをクリックすると、バックアップのデータセットに含まれるファイルのリストが表示されます。

異なるコンピューターのバックアップ履歴を表示するには、このリストから希望するコンピューターを選択します。異なるコンピューターのバックアップ履歴を表示する前に、[別のコンピューターからリストアを行う場合の要件](#) (393 ページ) で説明されている要件を満たしてください。

Avamar デスクトップ/ラップトップ パラメーターの編集

Avamar デスクトップ/ラップトップのプロパティ ファイルである `dtlt.properties` を使用すると、Avamar サーバーに接続しているすべての Avamar デスクトップ/ラップトップ クライアントの機能に影響を及ぼすパラメーターを変更できます。ファイルは Avamar サーバーの次の場所にありません。`/usr/local/avamar/etc/dtlt.properties`。

手順

1. コマンド シェルを開きます。
 - a. サーバーに `admin` としてログインします。
 - b. 次のコマンドを入力して、ユーザーを `root` に切り替えます。


```
su -
```
 - c. グリッドの場合、次のコマンドを入力して、`rootid` OpenSSH キーをロードします。


```
ssh-agent bashssh-add /root/.ssh/rootid
```
2. 次のコマンドを入力して、ディレクトリを `/usr/local/avamar/etc` に変更します。


```
cd /usr/local/avamar/etc
```
3. テキスト エディターで `dtlt.properties` を開きます。
4. パラメーターを作成または編集します。
5. ファイルを保存して閉じます。

Avamar デスクトップ/ラップトップパラメーター

次の表では、`dtlt.properties` ファイルで利用可能なパラメーターを挙げています。

表 122 Avamar デスクトップ/ラップトップパラメーター

パラメーター	説明
allowLocalUsers	パススルー認証のためのローカル ユーザー アクセスを有効化および無効化します。パラメーターの前につけられた#を削除して、このパラメーターのコメント解除を行い、値を true に設定して、パススルー認証のためのローカル ユーザー アクセスを有効化します。デフォルト値である false を使用すると、パススルー認証のためのローカル ユーザー アクセスが無効化されます。
allowServerRestores	サーバー クラスのコンピューターに対するローカル始動のリストアを有効化または無効化します。デフォルト値である true を使用すると、サーバー クラスのコンピューターに対するリストアが有効化され、false と指定すると、サーバー クラスのコンピューターに対するリストアが無効化されます。
allowUserInitiatedBackupsFileSelection	オン デマンド バックアップでバックアップの対象となるフォルダーおよびファイルのセットをユーザーが作成する機能を有効化または無効化します。選択可能なバックアップ セットを有効化するには、Avamar Administrator でクライアントの [Allow file selection on client initiated backups] 設定を有効化した後、allowUserInitiatedBackupsFileSelection パラメーターの値を true に設定します。選択可能なバックアップ セットを無効化するには、デフォルト値の false を使用します。
checkAlternateComputerOwnership	ローカル管理者権限を持つユーザーが、ソース コンピューターからあらゆるファイルをリストアできるか、所有するファイルのみをリストアできるかを制御します。true と指定すると、ローカル管理者がリストアできるのは所有するファイルのみに限られ、デフォルト値である false を使用すると、ローカル管理者はソース コンピューターからあらゆるファイルをリストアできます。
disableRestoreFromAlternateComputer	別のコンピューターからのリストアを有効化または無効化します。true と指定すると、別のコンピューターからのリストアが無効化され、デフォルト値の false を使用すると、別のコンピューターからのリストアが有効化されます。
disallowMultipleRestores	ユーザーがクライアント コンピューターで同時に複数のリストア タスクを開始できるかどうかを制御します。false と指定すると、同時に複数のリストアを実行でき、デフォルト値である true を使用すると、同時に複数のリストアを実行することはできません。
limitRestoreSize	単一のタスクでリストアされるデータ量を制限するかどうかを制御します。上限を指定するには、limitRestoreSize パラメーターのコメント解除を行って、MB 単位でデータ サイズの上限を指定します。デフォルトの上限は 500 MB です。
maxDirectoryDepth	バックアップの各階層分岐で、Avamar デスクトップ/ラップトップサーバーがインデックス作成時にスキャンするネストされるサブフォルダーの数を指定します。デフォルト値は 3000 です。
restrictBackupsPerDay	1日にクライアント コンピューターで実行できるオン デマンド バックアップの数に制限を設けるかどうかを制御し、制限を設ける場合は、バックアップの最大数を指定します。1日に正常に実行できるオン デマンド バック

表 122 Avamar デスクトップ/ラップトップパラメーター (続き)

パラメーター	説明
	アップの数を制限しない場合は、デフォルト値である <code>false</code> を使用します。0 と指定すると、クライアント コンピューターでのオン デマンド バックアップが無効化されます。1 日に正常に実行できるオン デマンド バックアップの数を制限するには、100 以下の正の整数で上限を指定します。
<code>useAppletToBrowseLocalFile</code>	ユーザーがクライアント コンピューターの OS 固有のファイル参照サービスを使用するか、代替のファイル参照方式を使用するかを制御します。 <code>true</code> と指定すると、ユーザーが OS 固有のファイル参照サービスを使用できるようになり、 <code>false</code> と指定すると、ユーザーが代替のファイル参照方式を使用するように強制されます。デフォルト値は <code>false</code> です。
<code>userLoginRequired</code>	パススルー認証を有効化および無効化します。デフォルト値である <code>false</code> を使用すると、パススルー認証が有効化され、 <code>true</code> を使用すると、パススルー認証が無効化されます。

クライアント ログの場所

クライアント コンピューターのローカル ログは、バックアップ/リストア処理、および UI 機能に関する情報を提供します。

使用可能なログ

次の表にクライアント コンピューターで使用可能なログがリストされています。

表 123 クライアントで使用可能なログ

ログ タイプ	ログ ファイル名	説明
Workorder	<code>workorder_name.log</code> 。この <code>workorder_name</code> は、タスクの完全名です。	特定のタスクに関する詳細な情報が表示されます。
Agent	<code>avagent.log</code>	コンピューター上のすべてのバックアップとリストアのアクティビティのステータスに関する情報を提供します。
Console	<code>avsccl.log</code>	ユーザー インターフェイスのパフォーマンスに関する情報を提供します。コンソール ログは、コンピューター上のユーザーごとに作成されます。

これらのログはクライアント ユーザー インターフェイスからアクセスできますが、直接アクセスすることもできます。

Windows コンピューターのログへのパス

Windows コンピューターの場合、ログは次の表のパスから入手できます。

表 124 Windows コンピューターでのログへのパス

ログ	パス
Workorder	%SystemDrive%\Program Files\avs \var\clientlogs\
Agent	%SystemDrive%\Program Files\avs \var\
Console	%APPDATA%\Avamar\

Linux および Mac コンピューターでのログへのパス

Linux および Mac コンピューターの場合、ログは次の表のパスから入手できます。

表 125 Linux および Mac コンピューターでのログへのパス

ログ	パス
Workorder	/usr/local/avamar/clientlogs
Agent	/var/avamar/
Console	Linux の場合 : \$HOME/ Mac の場合 : \$HOME/.avamardata/

第 15 章

Data Domain システムの統合

本章は、次のトピックで構成されています。

- [Data Domain システム統合の概要](#)..... 400
- [Data Domain システムの追加の準備](#)..... 405
- [Data Domain システムの追加](#)..... 409

Data Domain システム統合の概要

Avamar バックアップを 1 つまたは複数の Data Domain システムで保存することができ、データをそのバックアップからシームレスにリストアすることができます。

ファイル システムとアプリケーション データの両方を Data Domain システムにバックアップできます。Data Domain システムの Avamar バックアップ用ストレージは、変更率の高い大容量データベースのある環境にお勧めです。一方、Avamar サーバには、次のようなバックアップを保存します。

- ファイル システムのバックアップ
- 仮想マシンのバックアップ
- リモート オフィスのバックアップ
- 変更率の低いデータベースのバックアップ

Data Domain システムに VMware イメージ バックアップを保存した場合、インスタント アクセス機能を使用すれば、失われた仮想マシンまたは破損した仮想マシンをそのバックアップから起動できます。

Data Domain システムには、単一ノード サーバまたは AVE (Avamar Virtual Edition) の Avamar チェックポイントを保存することもできます。

Avamar と Data Domain の統合

DD OS ソフトウェアは、Data Domain システムでデータの重複排除を制御します。DD Boost (Data Domain Boost) ライブラリは、ソースで重複排除されたデータを Data Domain システムに送信するために、Avamar システム向けのインターフェイスを提供しています。

Avamar は API ベースの統合により DD Boost ライブラリを使用し、Data Domain ファイル システムのディレクトリ、ファイル、その他の項目にアクセスし、操作します。DD Boost API を通じて、Data Domain システムのプロパティや機能の一部に対するインターフェイスを、Avamar システムに提供します。このインターフェイスにより、Avamar システムは、Data Domain システムに格納されたバックアップ イメージを制御できます。またこれにより Avamar は、メンテナンス アクティビティを管理し、リモートの Data Domain システムへのレプリケーションを制御できます。

DD Boost は、バックアップ クライアントと、Avamar ユーティリティ ノードまたは Avamar シングル ノード システムにインストールします。DD Boost は、Avamar クライアントまたはサーバのソフトウェアをインストールすると自動的にインストールされます。

特定のバックアップ データセットを、Avamar サーバまたは Data Domain システムに保存するかどうかを指定できます。

バックアップ ターゲットに Avamar サーバを選択した場合、各ホスト上の Avamar クライアントが重複排除セグメント処理を実行します。Avamar クライアントは、バックアップ データとその関連するメタデータを Avamar サーバに送信します。

バックアップ ターゲットに Data Domain システムを選択した場合、バックアップ データは Data Domain システムに転送されます。同時に Avamar クライアントは、関連するメタデータを格納のために Avamar サーバに送信します。Avamar 管理システムは、このメタデータにより、Avamar システムにリストアされたデータを最初にステージングしなくても、Data Domain システムからリストア処理を直接実行できます。

データリカバリの処理は、バックアップ管理者に対して透過的です。バックアップ管理者は、同じ Avamar リカバリ プロセスを現在の Avamar システムに対してもネイティブに使用します。

Data Domain でのファイル システムのバックアップ

次のオペレーティング システムの場合に、Avamar は、ファイル システム バックアップの Data Domain システム ストレージをサポートします。

- Windows および Windows Server
- IBM AIX
- HP-UX (IA-64 のみ、ONCPlus Library リビジョン 11.31.06 以上が必要です)
- Solaris (Solaris 10 の SPARC では、クライアント側での重複排除は無効であり、Data Domain システムで重複排除を実行します)
- RHEL (Red Hat Enterprise Linux)
- SLES (SUSE Linux Enterprise Server)
- Mac 10.8、10.9、10.10

注

サポートされるのは 64 ビット オペレーティング システムのみです。

「E-Lab Navigator」で互換性に関する詳細情報を提供します。

Data Domain システムでのアプリケーションのバックアップ

Data Domain システムでは、次の Avamar プラグ インからのアプリケーション データのバックアップを保存できます。

- DB2 用 Avamar プラグ イン
- Exchange VSS 用 Avamar プラグ イン
- Hyper-V VSS 用 Avamar プラグ イン
- Lotus Domino 用 Avamar プラグ イン
- Oracle 用 Avamar プラグ イン
- SAP with Oracle 用 Avamar プラグ イン
- SharePoint VSS 用 Avamar プラグ イン
- Sybase ASE 用 Avamar プラグ イン
- SQL Server 向け Avamar プラグ イン

Data Domain システムには、VMware イメージ バックアップと Avamar NDMP アクセラレーターによるバックアップも保存できます。

Data Domain Cloud Disaster Recovery

Data Domain クラウド DR (クラウド ディザスタリカバリ) ソリューションは、クラウド内の仮想マシンをリカバリする機能を提供することで、オンプレミスの仮想マシンのディザスタリカバリを容易にします。

クラウド DR をオンプレミスの Avamar ソフトウェアとオンプレミスの Data Domain ストレージと共に使用して、仮想マシン データのバックアップをパブリック クラウドにレプリケーションし、Amazon Web Services EC2 (Elastic Compute Cloud) インスタンスとして完全な仮想マシンをリカバリして本番環境のディザスタリカバリを実行できます。

Data Domain クラウドのディザスタリカバリでの Avamar の使用方法の詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。

VMware インスタント アクセス

Data Domain システムに VMware イメージ バックアップを保存した場合、インスタント アクセス機能を使用すれば、失われた仮想マシンまたは破損した仮想マシンをそのバックアップから起動できます。

インスタント アクセス機能を使用すると、仮想マシンのイメージ バックアップは、Data Domain システムへの一時 NFS 共有に対して行われます。その後、vSphere Client を使用して仮想マシンの電源がオンにし、vCenter 内のデータストアへの仮想マシンの vMotion を開始できます。vMotion が完了すると、リストアされた仮想マシン ファイルは Data Domain システムに存在しなくなります。そのときに、Avamar Administrator を使用して Data Domain システムにある NFS 共有を削除します。

注

インスタント アクセス機能を使用するときは、長時間、Data Domain システムで仮想マシンを実行状態にしておかないでください。Data Domain システム上で仮想マシンを実行する場合、ワークフローのためにパフォーマンスが落ちます。

インスタント アクセス機能を使用せずに、本番環境で仮想マシンをリストアすることもできます。Avamar ソフトウェアで CBT (Changed Block Tracking) を活用すると、リカバリプロセスの速度が劇的に向上します。

インスタント アクセス、およびイメージ バックアップのリストアの詳細については、「Avamar for VMware ユーザー ガイド」を参照してください。

クラウド階層

Data Domain システムに Avamar バックアップ データを保存するときに、クラウドにバックアップを階層化するように構成することもできます。

Data Domain Cloud Tier のサポートは Avamar 7.4 から開始されました。DD Cloud Tier は、データを Data Domain からクラウドに移動します。Avamar Administrator から、クラウド階層を構成して Avamar のバックアップを Data Domain からクラウドに移動でき、これらのバックアップのシームレスなリカバリを実行できます。

Data Domain Cloud Tier のディザスタリカバリのサポートは Avamar 7.5 から開始されました。Data Domain が消失した場合はクラウドからバックアップをリカバリできます。また、クラウドから Avamar サーバをリカバリすることもできます。

Data Domain のクラウド階層の詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。

Data Domain システムでのチェックポイント

DD OS 5.3 以上を使用する Data Domain システムには、単一ノード サーバまたは AVE (Avamar Virtual Edition) の Avamar チェックポイントを保存できます。チェックポイントとは、ディザスタリカバリを目的とした Avamar サーバのシステム全体のバックアップです。

Data Domain システム上のチェックポイントのストレージは、次のオプションを含まない環境でお勧めします。

- セカンダリの Avamar サーバへのレプリケーション
- クライアント バックアップの大半を Data Domain システムに保存する環境

Data Domain システムにチェックポイントのストレージを構成するには、Avamar Administrator の Data Domain システムを追加または編集するときに [Use as target for Avamar Checkpoint Backups] チェックボックスを選択します。

Avamar サーバを Data Domain システムのチェックポイントにロールバックする際にサポートが必要な場合は、Avamar プロフェッショナル サービスの担当者にお問い合わせください。

Data Domain システム ストリーム

各 Data Domain システムには、パフォーマンスを維持しながら同時に持続できる接続およびデータ ストリームの数にソフト制限があります。ストリームの数は、Data Domain システムのモデルにより異なります。

Data Domain システムを Avamar サーバに追加するときに、Avamar が使用できるストリームの最大数を設定します。Avamar サーバはバックアップ ストリーム値を使用して、コンカレントなバックアップまたはリストア ジョブの数を制限します。

Data Domain システムが完全に Avamar サーバ専用の場合は、Avamar Administrator に入力されるストリーム値は該当する Data Domain システムのモデルがサポートする最大ストリーム数に一致する可能性があります。その他のサードパーティ アプリケーションまたは Avamar サーバと Data Domain システムを共有する場合は、ストリーム数のサブセットを割り当てる必要があります。

マルチストリーム バックアップをサポートする各 Avamar バックアップ クライアントで、適切な数のストリームを使用するように（通常はデータベース数に基づいて）構成することができます。このステップは、Avamar バックアップ ジョブの構成時にマルチ ストリーミング構成を使用して行います。バックアップまたはリストア処理が完了すると、ストリームはリリースされます。割り当てられるストリームの数は、同時にデータをバックアップする Avamar クライアントの数とタイプに依存します。

Data Domain システムを使用したレプリケーション

Avamar システムが Data Domain システムにバックアップを格納する場合、Avamar レプリケーションは DD Boost を使用して元の Data Domain システムからバックアップをコピーして、別の Data Domain システムにレプリカを作成します。

サポートされるレプリケーション構成

次の表では、DD Boost を使用した Avamar レプリケーションのためにサポートされるレプリケーション構成を示します。

表 126 DD Boost を使用した Avamar レプリケーションのためのレプリケーション構成

バックアップ ストレージ	レプリケーション ストレージ
シングル Data Domain システム	シングル Data Domain システム
シングル Data Domain システム	複数の Data Domain システム
複数の Data Domain システム	シングル Data Domain システム
複数の Data Domain システム	複数の Data Domain システム

レプリケーション ストレージに複数の Data Domain システムが存在している構成では、ソース Avamar サーバのドメインをターゲット Data Domain システムにマッピングすることで、レプリカを受信するシステムを制御します。デフォルトのターゲットを使用して Data Domain システムを指定します。ターゲット Data Domain システムが特定されていない場合、Avamar はデフォルトのターゲットにレプリケートします。

「Avamar および Data Domain システム統合ガイド」では、ストレージ マッピングのステップや、デフォルトのターゲット Data Domain システムの指定について説明します。

レプリケーションの詳細

次の詳細が、Data Domain システムを使用する Avamar レプリケーションに適用されます。

- レプリケーション時のデータ転送は、中継的なステージングなしで Data Domain システム間で実行されます
- レプリケーションは DD Boost を使用してバックアップをコピーし、レプリカを書き込みます
- Data Domain レプリケーション ライセンスが必要です
- Data Domain レプリケーションを使用しません
- レプリケーションは Avamar サーバで構成され、監視されます
- レプリケーション タスクのスケジュール設定では、Avamar レプリケーション スケジュールのみを使用します
- Data Domain 管理ツールは使用されません

Data Domain システムのステータスの監視とレポート

Avamar は、稼働状態の監視、システム アラート、容量レポートのためのデータを、SNMP (Simple Network Management Protocol) を使用して Data Domain システムで収集および表示できます。

SNMP により、Avamar サーバのアクティビティ、イベント、容量、システム ステータスを監視すると同じ方法で、Data Domain のアクティビティ、イベント、容量、システム ステータスを監視することができます。SNMP の各設定は、Data Domain システムが Avamar 構成に追加される際に構成します。

レポート作成の詳細については、「Avamar レポート ガイド」を参照してください。システムを分析するには、レポートを実行します。

Data Domain システムのシステム ステータスの監視について詳しくは、「Avamar および Data Domain システム統合ガイド」を参照してください。

Data Domain システム統合のセキュリティ

ここでは、Avamar および Data Domain 統合環境の暗号化およびユーザー アクセスに対するセキュリティの詳細を説明します。

暗号化

DD Boost ライブラリは Avamar クライアントと DDOS 5.5 以降の Data Domain システム間のデータの暗号化をサポートします。DD Boost ライブラリは Avamar クライアントと DDOS 5.4 の Data Domain システム間のデータの暗号化をサポートしません。

Avamar クライアントから Avamar サーバへのバックアップは常に圧縮され暗号化されています。

ユーザー アクセス

Data Domain システムへのユーザー アクセスの許可には注意が必要です。ユーザーには Data Domain システムへのアクセス許可を与えないでください。またデータは手動で削除してください。

接続された Data Domain システムへのデータの移行

バックアップ データを Avamar サーバから接続された Data Domain システムに直接移行することはできません。

Avamar クライアントのバックアップ ターゲットとして Avamar サーバではなく Data Domain システムを使用し始めるためには、Data Domain システムを使用するようにデータセットを編集します。Data Domain システムへのバックアップの実行を開始します。バックアップ ターゲットを Data Domain システムに変更する場合は、フル バックアップを行います。

Data Domain システムへのバックアップの実行が成功したら、それまでのバックアップを Avamar サーバから削除できます。

Data Domain へのバックアップ適用

管理者は、Data Domain をバックアップのストレージ ターゲットとして選択することに加えて、構成済みの Data Domain をターゲットとしていないバックアップを拒否するように Avamar サーバを構成することができます。この適用では、Avamar Administrator と AUI を使用して構成したバックアップと、コマンドライン インターフェイスやその他のツールから構成したバックアップを対象としています。

バックアップ適用が無効な状態で、Data Domain をストレージ ターゲットとして指定せずにバックアップが実行された場合、Avamar サーバはバックアップ データとメタデータの両方を保存します。このシナリオでは、容量使用率に関して予期しない問題につながる可能性があります。バックアップ適用が有効な状態では、Data Domain をストレージ ターゲットとして指定していないバックアップは、警告を出して失敗します。Data Domain ストレージ ターゲットを指定するバックアップは、通常どおり継続します。

バックアップ適用は、デフォルトでは無効になっています。この状態では、サーバの動作は以前の Avamar リリースと変更はありません。

注

バックアップ適用は、MCS からのデータなど、Avamar サーバのメンテナンス バックアップを保存およびレプリケートするための通常の方法には影響しません。

バックアップの適用を構成すると、ソース Avamar サーバにバックアップが保存されている環境でのレプリケーションの動作に影響します。適用モードを選択すると、ソース Avamar サーバのソフトウェア要件が課される場合もあります。

詳細については、「Avamar および Data Domain システム統合ガイド」を参照してください。

Data Domain システムの追加の準備

Data Domain システムを Avamar 構成に追加する前に Avamar サーバと Data Domain システムの両方をインストールして構成します。追加する環境がシステム要件を満たしていることを確認し、Data Domain システム上に DD Boost のユーザー アカウントを作成しておいてください。

Data Domain システム統合のシステム要件

Data Domain システムを Avamar の構成に追加する前に、環境が必要なシステム要件を満たしていることを確認してください。

次の表では Data Domain システム要件が挙げられています。

表 127 Data Domain システム要件

機能または仕様	Avamar と組み合わせて使用する場合の要件
DD OS (Data Domain Operating System)	DD OS 5.3 以降
DD Boost	DD Boost 2.6 以降

表 127 Data Domain システム要件 (続き)

機能または仕様	Avamar と組み合わせて使用する場合の要件
	<p>注</p> <p>DD Boost ソフトウェアは、Data Domain システムがテープをエミュレートすることなく、バックアップ サーバとストレージ システムとの通信を可能にします。DD Boost には、バックアップ サーバ上で動作するコンポーネントと Data Domain システム上で動作するコンポーネントの 2 つのコンポーネントが存在します。Avamar のコンテキストでは、バックアップ サーバ上で実行されるコンポーネント (DD Boost ライブラリ) は Avamar クライアントに統合されています。DD Boost ソフトウェアはオプション製品であり、Data Domain システムで動作するにはライセンスが必要です。</p>
Data Domain デバイス タイプ	Avamar は、必要な DD OS バージョンの実行をサポートするあらゆる Data Domain システムをサポートします。
Data Domain ファイル システム	Data Domain File System の有効化は、Data Domain System Manager または CLI を使用して行います。ファイル システムの操作を有効化してから、Avamar Administrator で Data Domain システムのステータスが正しく反映されるまでに、最大 10 分かかることがあります。Data Domain システムで DD Extended Retention オプションを使用している場合は、さらに多少の遅れが発生します。Avamar Administrator にステータスが正確に表示されるまでは、バックアップ、リストア、システム メンテナンスの操作は行わないでください。これらの操作を行った場合、バックアップ、リストア、システム メンテナンスの操作は失敗する可能性があります。
DD Boost	Data Domain システムで DD Boost を有効化します。DD Boost を有効にすると、DD Boost で有効化されたクライアントでは、DD Boost が優先接続方式になります。この方式は DD Boost 機能の利点を活用できるクライアントには好ましいことですが、そうではないその他のクライアントにはパフォーマンスの低下をもたらす可能性があります。このような相互作用を回避するには、アップグレードを行う段階では特に、適正評価と効果的なデータ収集が重要です。
DD Boost ユーザー アカウント	DD Boost ライブラリは、Data Domain システムで作成される一意のログイン アカウント名を使用します。このアカウント名は、DD Boost アカウントと呼ばれます。Data Domain システム 1 つにつき、1 つの DD Boost アカウントのみ有効です。アカウント名および/またはパスワードが変更された場合は、Data Domain 構成オプションを編集して、直ちに Avamar システムを更新する必要があります。DD Boost アカ

表 127 Data Domain システム要件（続き）

機能または仕様	Avamar と組み合わせて使用する場合の要件
	ラック情報の更新に失敗すると、整合性チェックのエラーまたはバックアップ/リストアの問題が発生する可能性があります。DD Boost アカウントには、管理者権限が必要です。

容量要件

Data Domain システムと Avamar サーバに格納するデータ量を評価する際は、バックアップストレージのニーズを慎重に評価します。Data Domain システムに対してその他のサーバから送られるデータの予測を追加します。

Data Domain システムのストレージ容量が最大容量に達すると、容量が追加されるか古いバックアップが削除されるまで、Data Domain システムへの次のバックアップは行われません。

他のバックアップ製品を使用する場合の要件

Data Domain システムは、その他のサードパーティ製バックアップおよびアーカイブソフトウェアを使用できます。Avamar サーバは、Data Domain システムの独占的な所有権を前提にしていません。システムをその他のソフトウェア製品と共有する場合は、サイジングの評価が適切であることを確認してください。

Avamar サーバは、ネイティブの Data Domain システムのスナップショット機能とレプリケーション機能を使用しません。レプリケーションは、DD Boost SDK ライブラリを通じたコピーおよびクローン作成によって実行されます。ただし、その他のサードパーティ製品がネイティブの Data Domain システムスナップショット機能とレプリケーション機能を使用する可能性があります。この場合、Data Domain システム全体のスナップショットまたは Data Domain システム全体のレプリケーションには、Avamar のデータも含まれます。

ネットワークの条件

Avamar サーバとすべての Data Domain システムが、同一のローカルネットワーク上に存在する必要があります。Avamar サーバと Data Domain システムを WAN（Wide Area Network）経由で接続しないでください。WAN を使用する構成はサポートされていません。

ソース Avamar サーバおよび Data Domain システムから、ターゲット Avamar サーバおよび Data Domain システムへの WAN を経由したデータのレプリケーションは、Avamar レプリケーションで行うことができます。

Data Domain システムを Avamar サーバに統合する前に、十分なネットワーク帯域幅が使用可能であることを確認してください。ネットワークインフラストラクチャが Data Domain システムの最大のスループットが必要とする以上の帯域幅を提供していることを確認してください。このステップにより、リストア、レベルゼロバックアップ、レベルゼロバックアップに続く差分バックアップにおいて、Data Domain システムで可能な最大のスループットを実現します。

ネットワーク構成は次の要件も満たしている必要があります。

- FQDN（完全修飾ドメイン名）を各 Data Domain システムに割り当てます。
- Data Domain システムを登録する際には、ホスト名の代わりに IP アドレスを使用しないでください。IP アドレスを使用すると、登録されたインターフェイスだけを経由する最適化された二重トラフィックを経路指定する機能が制限される可能性があります。
- Data Domain システムの DNS が正しく構成されていることを確認します。

- 正引き/逆引き DNS 参照が Avamar サーバ、Data Domain システム、すべてのバックアップ/リストア クライアントの間で機能することを確認してください。
- ホスト名のルーティング不可能な IP アドレスへの変換には、Host ファイルを使用します。
- 代替またはローカル IP インターフェイスに関連付けるために、セカンダリ ホスト名を作成しないでください。

NTP の要件

Avamar サーバ、Data Domain システム、すべての Avamar クライアントが同一の NTP (Network Time Protocol) サーバを使用している必要があります。

ポート使用とファイアウォールの要件

Avamar と Data Domain システム間の通信を有効化するためには、次のドキュメントのポート使用とファイアウォールの要件をレビューして導入します。このドキュメントは、Avamar サポートから入手できます。

- 「Avamar 製品セキュリティ ガイド」
- 「Port Requirements for Allowing Access to Data Domain System Through a Firewall Technical Note」

Data Domain を 8 TB または 16 TB AVE に追加するときの追加の構成設定

Data Domain システムを 8 TB または 16 TB の AVE (Avamar Virtual Edition) に追加する前に、Dell EMC では、次の Avamar GSAN 設定を変更して、システム パフォーマンスを向上させることを推奨しています。

- `avmaint config maxcompdatastripe=20971520 --avamaronly`
- `avmaint config checkdiratomicrefs=true --avamaronly`

DD Boost ユーザー アカウントの作成

Avamar の構成に Data Domain システムを追加する前に、DD Boost を有効化し、Avamar サーバの DD Boost ユーザー アカウントを作成して、Data Domain システムを準備します。このアクションを実行して、バックアップおよびリストア (該当する場合は、さらにレプリケーション) 用の Data Domain システムへアクセスします。

アカウントの作成後に DD Boost アカウント名またはパスワードを変更する場合は、必ず Avamar Administrator で Data Domainsh システム構成を編集してください。編集しなければ、すべてのバックアップ、リストア、メンテナンス アクティビティが失敗します。

手順

1. Data Domain CLI に管理者ユーザーとしてログインし、次のコマンドを入力することで、Data Domain システム上で DD Boost を無効にします。

```
ddbboost disable
```

2. 以下のコマンドを入力して、管理者の権限で DD Boost ユーザー アカウントを作成します。

```
user add username role admin
```

この username は新しいアカウントのユーザー名です。

3. 次のコマンドを入力して、この新しいアカウントを DD Boost ユーザーとして設定します。

```
ddbboost set user-name username
```

この username はアカウントのユーザー名です。

4. 次のコマンドを入力して、DD Boost を有効化し、変更を反映させます。

```
ddbboost enable
```

Data Domain システムの追加

Data Domain システムを Avamar に追加するには、認証情報を使用して Data Domain システムを認証するか、キーベースの SSH を使用します。Data Domain システムの認証情報（ユーザー名/パスワード）を指定してログインする方法が無効になっている場合は、Avamar サーバーから SSH 公開キー（/usr/local/avamar/lib/ddr_key.pub）をインポートし、Data Domain システムに手動でキーを追加してから接続する必要があります。Data Domain システムの認証情報を指定してログインする方法が無効になっている場合、Data Domain システムにログインするための追加のアクセス権を持っていることを確認してください。

はじめに

キーベースの SSH で Data Domain システムを認証する場合は、次の手順を実行します。

1. Data Domain システムに sysadmin として、あるいは avamar_ostuser 権限を使用してログインします。avamar_ostuser は Data Domain システム上の Avamar の DD Boost ユーザーの名前です。
2. 次のコマンドを入力して、Avamar サーバーから Data Domain システム上の SSH で許可されたキーファイルに SSH 公開キー（/usr/local/avamar/lib/ddr_key.pub）を追加します。
`adminaccess add ssh-key user Avamar_ostuser`
3. 次のコマンドを入力して、公開キーが Data Domain システムに正常に追加されたことを確認します。
`adminaccess show ssh-key user Avamar_ostuser`

手順

1. Avamar Administrator で、[Server] 起動リンクをクリックします。
[Server] ウィンドウが表示されます。
2. [Server Management] タブをクリックします。
3. [Actions] > [Add Data Domain System] を選択します。
[Add Data Domain System] ダイアログ ボックスが表示されます。
4. [System] タブで、次の Data Domain システム情報を指定します。
 - a. [Data Domain System Name] ボックスに、Data Domain システムの完全修飾ドメイン名を入力します。

注

代替またはローカルの IP インターフェイスに関連する IP アドレス、またはセカンダリホスト名を使用しないでください。最適化された重複排除トラフィックを経路指定することにより、Avamar の機能を制限する可能性があります。

- b. [DDBoost User Name] ボックスに、バックアップ、リストア、レプリケーションのために Avamar が Data Domain システムにアクセスする際に使用する、DD Boost アカウントのユーザー名を入力します。
- c. [Password] ボックスに、バックアップ、リストア、レプリケーションのために Avamar が Data Domain システムにアクセスする際に使用する、アカウントのパスワードを入力します。

- d. **[Verify Password]** ボックスに、確認のためにパスワードを再入力します。
- e. Avamar に複数台の Data Domain システムを関連づけている場合は、そのうちの 1 台をデフォルトのレプリケーション ストレージに指定できます。このシステムがデフォルトのレプリケーション ストレージの場合は、**[Use system as default replication storage]** を選択します。
- f. シングル ノードの Avamar サーバまたは AVE (Avamar Virtual Edition) サーバのチェックポイントを、Avamar サーバではなく Data Domain システム上に保存するには、**[Use as target for Avamar Checkpoint Backups]** チェックボックスを選択します。
- g. **[Use certificate authentication for REST communication]** チェックボックスをオンにし、REST ベースの通信を使用して Data Domain システムで操作を実行する際に、証明書ベースの認証を使用できるようにします。

注

[Use certificate authentication for REST communication] チェックボックスは Avamar AUI にのみ表示されます。

- h. Data Domain システムがサポートするストリームの最大数を表示するには、**[Verify]** をクリックします。
- i. バックアップとリストアを実行するために、Avamar が一度に使用できるストリームの最大数を指定します。
 - 定義されたストリーム数を指定するには、**[Max used by Avamar]** ボックスに数字を入力します。
 - サポートされるストリームの総数に対する割合 (%) に基づいて、次のようにストリームの最大数を指定します。
 - a. **[Max used by Avamar]** ボックスに割合 (%) を入力します。
 - b. **[As percentage of the max limit]** チェックボックスを選択します。

Data Domain システムがサポートするストリームの最大数と、その他のアプリケーションがストリームを使用して Data Domain システムとの間でデータの送受信を行っているかどうかという両方の点を考慮します。

Data Domain システムとの間の書き込みと読み取りで使用可能なすべてのストリームを使用する場合、1 つまたは複数のストリームが使用できるようになるまで、Avamar はバックアップまたはリストアのリクエストをキューに入れます。

- 5. SNMP を構成するには、**[SNMP]** タブをクリックします。
SNMP 構成により、Avamar はシステムの稼働状態のモニタリング、システム アラート、容量レポートのためにデータを収集して表示することができます。
- 6. 次のように SNMP 構成を確認します。
 - **[Getter/Setter Port Number]** ボックスには、SNMP オブジェクトを受信し設定する Data Domain システムのポートのリストが表示されます。デフォルト値は 161 です。
 - **[SNMP Community String]** ボックスには、Avamar が Data Domain システムへの read-only アクセスに使用するコミュニティ文字列が表示されます。
 - **[Trap Port Number]** ボックスには、Avamar サーバのトラップ ポートのリストが表示されます。デフォルト値は 163 です。
- 7. クラウド階層機能を構成するには、**[Tiering]** タブをクリックします。

Avamar ソフトウェアは、クラウド階層を使用して Avamar のバックアップ データを Data Domain システムからクラウドに移動します。

8. **[OK]** をクリックします。
進行状況を示すメッセージが表示されます。
9. 操作が完了したら、**[Close]** をクリックします。

結果

Data Domain システムを Avamar 構成に追加すると、Avamar は Data Domain システムに Avamar サーバ用の MTree を作成します。MTree は DD Boost パス内に作成されたディレクトリを示します。Data Domain システムは最大で 100 個の MTree をサポートします。その制限値に達すると、Data Domain システムを Avamar 構成に追加できなくなります。

付録 A

コマンド シェル サーバー ログイン

本付録は、次のトピックで構成されます。

- [ユーザー アカウント](#)..... 414
- [コマンド シェル セッションの開始](#)..... 414
- [ユーザー ID の切り替え](#)..... 414
- [sudo の使用](#)..... 415

ユーザー アカウント

以下のユーザー アカウントは、通常、システムの管理およびメンテナンス タスクに使用されます。

- root
- admin

admin アカウントでは、SSH (Secure Shell) による認証が必要です。

コマンド シェル セッションの開始

admin ユーザーとして、SSH を介して Avamar サーバまたはユーティリティ ノードにログインします。このアクションは、Avamar システムのメンテナンス タスクや構成のために実行します。

はじめに

注

Avamar 7.5.1 での暗号形式の変更により、PuTTY 0.7 以降、WinSCP 5.11.1 (ビルド 7725) 以降が必要になりました。

手順

- シングル ノード サーバーでコマンド シェル セッションを開始するには、コマンド シェルを開いて、サーバーに admin としてログインします。
- マルチ ノード サーバーでコマンド シェル セッションを開始するには、次の手順を実行します。
 - a. コマンド シェルを開き、admin としてユーティリティ ノードにログインします。
 - b. 次のコマンドを入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

- c. プロンプトが表示されたら、admin_key パスフレーズを入力し、[Enter] キーを押します。

ユーザー ID の切り替え

コマンド シェル セッションのユーザーを root に切り換えるには su と入力し、以前のログイン ID に戻すには exit と入力します。コマンド シェル セッションのユーザーを admin に切り換えるには、admin OpenSSH キーをロードすることも必要です。

手順

1. su - admin と入力して、ユーザーを admin のユーザー アカウントとログイン シェルに切り換えます。
2. パスワードを要求するプロンプトが表示されたら、admin のパスワードを入力して、[Enter] キーを押します。
3. 次のように入力して、admin OpenSSH キーをロードします。

```
ssh-agent bashssh-add ~admin/.ssh/admin_key
```

注

シェル セッションのアクティブなユーザー アカウント (ログイン ID) を判別するには、`whoami` と入力します。

sudo の使用

Gen4 以降の Avamar Data Store では、`admin` ユーザー アカウントは自動的に `sudoers` ファイルに追加されます。このオプションにより、`admin` ユーザーは実行できるコマンドが制限されます。コマンドを制限しないためには、オペレーティング システムの `root` 権限が必要になります。

sudo によるコマンドのプレフィックス

`su` コマンドでユーザーを `root` に切り換えなくても、各コマンドのプレフィックスとして `sudo` を使用すると、`root` 権限の必要なコマンドを、`admin` ユーザーが直接発行できるようになります。

例えば、次のコマンドによって `MyPackage.rpm` がインストールされます。

```
sudo rpm -ivh MyPackage.rpm
```

パスワードを入力するダイアログが表示されたら、パスワードを入力して、**[Enter]** キーを押します。

他のコマンドのプレフィックスとして `sudo` を使用すると、定期的に `admin` パスワードを再入力するようにプロンプトで要求されることがあります。

付録 B

プラグ イン オプション

本付録は、次のトピックで構成されます。

- [プラグ イン オプションの設定方法](#)..... 418
- [バックアップ オプション](#)..... 418
- [リストア オプション](#)..... 421

プラグ イン オプションの設定方法

プラグ イン オプションにより、オン デマンド バックアップ、リストア、スケジュール設定されたバックアップの特定のアクションを制御することができます。操作とプラグ インのタイプによって、利用可能なプラグ イン オプションが異なります。

AUI のプラグ イン オプションは、オン デマンド バックアップまたはリストア ウィザードに対して、またはスケジュール設定されたバックアップのデータセットを作成するときに、指定することができます。プラグ イン オプションは、GUI（グラフィカル ユーザー インターフェイス）コントロール（テキスト ボックス、チェックボックス、ラジオ ボタンなど）で設定します。[Key] フィールドと [Value] フィールドにオプションと値を入力します。

通知

Avamar ソフトウェアは、[More Options] パネルの [Show Free Form] セクションに入力された情報のチェックまたは妥当性検査を行いません。[Key] および [Value] フィールドの値によって、オプションの GUI コントロールで指定された設定はオーバーライドされます。

バックアップ オプション

表示されるバックアップ オプションは、プラグ インのタイプによって異なります。

このセクションは、以下のプラグ インのバックアップ オプションを示します。

- AIX ファイル システム
- FreeBSD ファイル システム
- HP-UX ファイル システム
- Linux ファイル システム
- Macintosh ファイル システム
- NetWare ファイル システム
- SCO OpenServer ファイル システム

Microsoft Windows 向けの Avamar プラグ インのバックアップ オプションについては、「Avamar for Windows Server ユーザー ガイド」を参照してください。SQL Server、SharePoint VSS などアプリケーション プラグ インのバックアップ オプションについては、プラグ インのユーザー ガイドを参照してください。

次の表に、オン デマンド バックアップの実行時に使用できるオプション、またはリストされるファイル システム プラグ インのスケジュール設定バックアップのデータセットを構成するときに使用できるオプションを示します。

表 128 バックアップ プラグ イン オプション

オプション	説明
Store backup on Data Domain system	バックアップを、Avamar サーバーではなく、構成済みの Data Domain システムに保存します。バックアップを Data Domain システムに保存するには、チェックボックスを選択し、リストから Data Domain システムを選択します。

表 128 バックアッププラグインオプション（続き）

オプション	説明
Encryption method to Data Domain system	クライアントと Data Domain システム間のデータ転送に使用される暗号化方式を指定します。
Backup label	この説明的なラベルをバックアップに割り当てます。

表 129 SMS 認証（NetWare のみ）用のバックアッププラグインオプション

オプション	説明
Server login ID	SMS ログイン ユーザー名を指定します。例えば、CN=admin.O=HOSTNAME_CTX。
Server password	SMS ログイン ユーザー名のパスワードを指定します。
Snapshot stored-on pool	snapshot stored-on pool の名前を指定します。

表 130 ログ用のバックアッププラグインオプション

オプション	説明
List backup contents	ログ ファイルに含まれるバックアップ対象の情報量を指定します。この情報の内容は次のとおりです。 <ul style="list-style-type: none"> • No file listing • List file names • List files and dates
Informational message level	ログ ファイルに含まれる参考メッセージの数を指定します。次のオプションがあります。 <ul style="list-style-type: none"> • [No informationals] : すべての「informational」メッセージが表示されません。ただし、「errors」および「warnings」のメッセージはログ ファイルに記録されます。 • [Some informationals] : ログ ファイルに一部の参考メッセージが記録されます。 • [Many informationals] : ログ ファイルに追加のステータス情報が記録されます。 • [All informationals] : 最大限の情報が表示されます。すべての参考メッセージ、エラー、警告がログ ファイルに含まれます。
Report advanced statistics	指定した場合、より詳細な時系列情報と重複排除の統計情報がログ ファイルに書き込まれます。
Enable debugging messages	指定した場合、最大の情報がログ ファイルに書き込まれます。このため、ログ ファイルが非常に大きくなります。

表 131 ファイル システム スキャン用のバックアップ プラグ イン オプション

オプション	説明
Do not traverse any mounts	指定した場合、このバックアップ中にマウント ポイントはスキャンされません。
Traverse fixed-disk mounts	指定した場合、このバックアップ中に、ハード ディスク ファイル システム マウント ポイントのみがスキャンされます。
Traverse fixed-disk and remote network mounts	指定した場合、このバックアップ中に、ハード ディスクと NFS ネットワーク マウント ポイントの両方がスキャンされます。
Force traversal of specified file system type(s)	このバックアップ中にスキャン対象としない1つ以上のファイル システムのタイプ (nfs、ext2、jfs、xfs など) のコンマ区切りのリストを受け入れます。

表 132 前処理スクリプト用のバックアップ プラグ イン オプション

オプション	説明
Run user-defined script at beginning of backup	バックアップ セッションの最初にユーザー定義スクリプトを実行します。スクリプトは /usr/local/avamar/etc/scripts に存在する必要があります。
Abort backup if script fails	指定した場合、スクリプトが「0 (ゼロ)」以外のステータス コードを返すと、バックアップの実行を停止します。

表 133 後処理スクリプト用のバックアップ プラグ イン オプション

オプション	説明
Run user-defined script at end of backup	バックアップ セッションの最後にユーザー定義スクリプトを実行します。スクリプトは /usr/local/avamar/etc/scripts に存在する必要があります。
Exit process with script failure exitcode	avtar が、標準の avtar 終了コードではなく、スクリプトの終了コードで終了するかどうかを指定します。

表 134 バックアップ プラグ イン クライアント キャッシュ オプション

オプション	説明
Check client-side caches and report inconsistencies	選択した場合、バックアップは実行されません。代わりに、Avamar で Avamar サーバでのクライアント キャッシュ ファイルの妥当性検査チェックを行います。
Check and repair client-side caches	選択した場合、バックアップは実行されません。代わりに、Avamar で Avamar サーバでのクライアント キャッシュファイルの妥当性検査チェックを行い、不整合を修復します。
Maximum client file cache size (MBs)	最大クライアント ファイル キャッシュ サイズを MB 単位で指定します。負の値は RAM の分数を示します。例えば、-8 は、物理 RAM の 1/8 がクライアント ファイル キャッシュに割り当てられることを意味します。

表 134 バックアップ プラグ イン クライアント キャッシュ オプション (続き)

オプション	説明
Maximum client hash cache size (MBs)	最大クライアントハッシュ キャッシュ サイズを MB 単位で指定します。負の値は RAM の分数を示します。例えば、-8 は、物理 RAM の 1/8 がクライアントハッシュ キャッシュに割り当てられることを意味します。

表 135 バックアップ プラグ インの高度なオプション

オプション	説明
Client-side flag file	追加オプション設定を含むクライアントのフラグ ファイルへのパスを指定します。
Network usage throttle (Mbps)	ネットワーク利用帯域の制限を Mbit/秒で指定します。例えば、0 = 無制限、T1 回線帯域の 50%相当 = 0.72。
Directly connect to all server nodes	指定した場合、サーバーへの複数の接続を確立します。複数の接続により、バックアップのパフォーマンスを改善できます。

表 136 バックアップあたりのクォータ制限

オプション	説明
Soft limit size (MBs)	バックアップのソフトリミット サイズを指定します。バックアップソースのサイズがソフトリミットを超えた場合、バックアップは警告ありで成功します。ソフトリミットとハードリミットの両方のサイズを指定する場合は、ソフトリミットサイズがハードリミットサイズよりも小さいことを確認します。
Hard limit size (MBs)	バックアップのハードリミット サイズを指定します。バックアップソースのサイズがハードリミットを超えた場合、バックアップは失敗します。

リストア オプション

利用できるリストア オプションは、プラグ インのタイプによって異なります。

このセクションは、以下のプラグ インのバックアップ オプションを示します。

- AIX ファイル システム
- FreeBSD ファイル システム
- HP-UX ファイル システム
- Linux ファイル システム
- Macintosh ファイル システム
- NetWare ファイル システム
- SCO OpenServer ファイル システム

Microsoft Windows 向けの Avamar プラグ インのリストア オプションについては、「Avamar for Windows Server ユーザー ガイド」を参照してください。SQL Server、SharePoint VSS などアプリケーション プラグ インのリストア オプションについては、プラグ インのユーザー ガイドを参照してください。

ファイル システム プラグ インのリストア オプション

次の表に、リストに記載されているファイル システム プラグ インを使用してリストアを実行するとき
使用できるオプションを示します。

表 137 ファイル システム プラグ インのリストア オプション

オプション	説明
Overwrite existing files	リストア対象のファイルが存在する場合の動作を制御します。次のいずれかを選択します。 <ul style="list-style-type: none"> • Never • Always • Generate New Name • If Modified • If Newer
Encryption method from Data Domain system	バックアップが Data Domain システムに保存される場合、Data Domain システムからクライアントへのデータ転送に使用する暗号化方式を選択します。

(NetWare のみ) SMS 認証リストア オプション

次の表では、SMS 認証 (NetWare のみ) を使用してリストアを実行する際に使用できるオプション
について説明します。

表 138 (NetWare のみ) SMS 認証リストア プラグ イン オプション

オプション	説明
Server login ID	(NetWare のみ) SMS ログイン ユーザー名を指定します。例えば、 CN=admin.O=HOSTNAME_CTX。
Server password	(NetWare のみ) SMS ログイン ユーザー名のパスワードを指定します。

リストア プラグ イン オプションのログ

次の表に、リストアを実行するとき使用できるログ オプションを示します。

表 139 リストア プラグ イン オプションのログ

オプション	説明
List backup contents	ログ ファイルに含まれるバックアップ対象の情報量を指定します。この情報の内容は次のとおりです。 <ul style="list-style-type: none"> • No file listing • List file names • List files and dates
Informational message level	ログ ファイルに含まれる参考メッセージの数を指定します。次のオプションがあります。

表 139 リストア プラグ イン オプションのログ (続き)

オプション	説明
	<ul style="list-style-type: none"> • [No informationals] : すべての「informational」メッセージが表示されません。ただし、「errors」および「warnings」のメッセージはログ ファイルに記録されます。 • [Some informationals] : ログ ファイルに一部の参考メッセージが記録されます。 • [Many informationals] : ログ ファイルに追加のステータス情報が記録されます。 • [All informationals] : 最大限の情報が表示されます。すべての参考メッセージ、エラー、警告がログ ファイルに含まれます。
Report advanced statistics	指定した場合、より詳細な時系列情報と重複排除の統計情報がログ ファイルに書き込まれます。
Enable debugging messages	指定した場合、最大の情報がログ ファイルに書き込まれます。このため、ログ ファイルが非常に大きくなります。

前処理スクリプト リストア プラグ イン オプション

次の表に、リストアを実行するときに使用できる前処理スクリプト オプションを示します。

表 140 前処理スクリプト リストア プラグ イン オプション

オプション	説明
Run user-defined script at beginning of restore	リストア セッションの最初にユーザー定義スクリプトを実行します。スクリプトは <code>/usr/local/avamar/etc/scripts</code> に存在する必要があります。
Abort restore when script fails	スクリプトがゼロ以外のステータス コードを返す場合、リストアを停止するかどうかを指定します。

後処理スクリプト リストア プラグ イン オプション

次の表に、リストアを実行するときに使用できる後処理スクリプト オプションを示します。

表 141 後処理スクリプト リストア プラグ イン オプション

オプション	説明
Run user-defined script at end of restore	リストア セッションの最後にユーザー定義スクリプトを実行します。スクリプトは <code>/usr/local/avamar/etc/scripts</code> に存在する必要があります。
Exit process with script failure exitcode	<code>avtar</code> が、標準の <code>avtar</code> 終了コードではなく、スクリプトの終了コードで終了するかどうかを指定します。

クライアント キャッシュ リストア プラグイン オプション

次の表に、リストアを実行するときに表示できるクライアント キャッシュ オプションを示します。

表 142 クライアント キャッシュ リストア プラグイン オプション

オプション	説明
Check client-side caches and report inconsistencies	選択した場合、リストアは実行されません。代わりに、Avamar で Avamar サーバでのクライアント キャッシュ ファイルの妥当性検査チェックを行います。
Check and repair client-side caches	選択した場合、リストアは実行されません。代わりに、Avamar で Avamar サーバでのクライアント キャッシュファイルの妥当性検査チェックを行い、不整合を修復します。
Rebuild client-side caches from most recent backup	データはリストアされません。選択した場合、Avamar は、前回のバックアップのコンテンツを使ってクライアント側のファイルのキャッシュ ファイルを再作成します。

高度なリストア プラグイン オプション

次の表に、リストアを実行するときに表示できる高度なプラグイン オプションを示します。

表 143 高度なリストア プラグイン オプション

オプション	説明
Do not descend into subdirectories	指定した場合、指定したトップレベルのディレクトリのみリストアを行い、サブディレクトリはリストアしません。
Recreate original path beneath target directory	指定した場合、指定したターゲット ディレクトリの下にファイルとディレクトリへの元のパスを再作成します。例えば、 <code>/usr/MyDir/MyFile</code> を <code>/tmp</code> にリストアし、このオプションを選択した場合は、リストアされたファイルへのフルパスは <code>/tmp/usr/MyDir/MyFile</code> になります。
Directly connect to all server nodes	指定した場合、サーバーへの複数の接続を確立します。複数の接続により、特定の環境でのリストア パフォーマンスが向上します。

付録 C

Avamar Web Restore ページへのファイルの追加

本付録は、次のトピックで構成されます。

- [Avamar Web Restore の \[Downloads\] ページへのファイルの追加](#).....426
- [Avamar Web Restore の \[Documentation\] ページへのファイルの追加](#).....427

Avamar Web Restore の [Downloads] ページへのファイルの追加

ご使用の環境に固有のソフトウェア ファイルを [Downloads] ページに追加できます。このページは、Avamar デスクトップ/ラップトップの [Avamar Web Restore] ページからアクセスできます。

インストール時に、[Downloads] ページにデフォルトのソフトウェア ファイルが追加されます。必要な場合は、[Downloads] ページに追加のソフトウェアを含めます。

手順

1. シェル コマンドを開き、管理者としてサーバーにログインします。
2. 次のコマンドを入力して、ディレクトリを /data01/avamar/src/downloads/ に変更します。

```
cd /data01/avamar/src/downloads/
```

3. 次のコマンドを入力してフォルダーを作成します。

```
mkdir folder_name
```

ここで、`folder_name` はファイルを配置する場所です。たとえば `Golden_Tenant` フォルダーを指定します。

4. ディレクトリを /data01/avamar/src/downloads/folder_name に変更します。

例：

```
cd /data01/avamar/src/downloads/Golden_Tenant
```

5. ユーザーがダウンロードできるようにするファイルを、フォルダーにコピーします。
6. 次のコマンドを入力して、ディレクトリを /usr/local/avamar/httpds/downloads/ に変更します。

```
cd /usr/local/avamar/httpds/downloads/
```

7. XML ファイルを作成して、フォルダーを定義します。

たとえば、`Golden Tenant` フォルダーでは、XML ファイルは次の例のようになります。

```
<?xml version="1.0" encoding="UTF-8"?>
<download
  heading="Golden Tenant"
  displayName="Plug-Ins"
  path="/DPNInstalls/downloads/Golden_Tenant/" />
```

各項目の意味は次のとおりです。

- `heading` : ルート フォルダー名を定義します。
 - `displayName` : サブフォルダー名を定義します。
 - `path` : ディスク上のソフトウェア ファイルの場所を定義します。/DPNInstalls/downloads は Avamar サーバー上の /data01/avamar/src/downloads を指します。
8. [Downloads] ページを更新して、新しくアップロードされたファイルが表示されることを確認します。

Avamar Web Restore の [Documentation] ページへのファイルの追加

ご使用の環境に固有のドキュメントを [Documentation] ページに追加できます。このページは、Avamar デスクトップ/ラップトップの [Avamar Web Restore] ページからアクセスできます。

インストール時に、[Documentation] ページのオンライン サポートリンクをクリックすると、最新の Avamar ドキュメントにアクセスできます。必要な場合は、[Documentation] ページに追加のガイドやマニュアルを含めてください。

手順

1. シェル コマンドを開き、管理者としてサーバーにログインします。
2. 次のコマンドを入力して、ディレクトリを `/space/avamar/doc/downloads/` に変更します。

```
cd /space/avamar/doc/downloads/
```

3. ユーザーがダウンロードできるようにするファイルを、フォルダーにコピーします。
4. 次のコマンドを入力して、ディレクトリを `/usr/local/avamar/httpds/docs/` に変更します。

```
cd /usr/local/avamar/httpds/docs/
```

5. XML ファイルを作成して、ドキュメントを定義します。

たとえば、『Golden Tenant User Guide』では、XML ファイルは次の例のようになります。

```
<?xml version="1.0" encoding="UTF-8"?>
<download
  heading="40"
  displayName="Golden Tenant User Guide"
  path="/axiondocs/cur/GoldTenantUG.pdf/" />
```

各項目の意味は次のとおりです。

- **heading** : デフォルト値を 40 に設定します。
 - **displayName** : [Documentation] ページに表示されるドキュメントの名前を定義します。
 - **path** : ディスク上のドキュメント ファイルの場所を定義します。/axiondocs/cur は Avamar サーバー上の `/space/avamar/doc/downloads` を指します。
6. 新しくアップロードされたファイルが表示されることを確認するには、[Documentation] ページを更新します。

用語集

記号

バックアップ ポリシー AUI では、バックアップ ポリシーはクライアントまたはクライアントのグループに適用されるデータセット、スケジュール、保存期間の設定を指定します。バックアップ ポリシーには、少なくとも 1 個の Avamar クライアントを含める必要があります。バックアップ ポリシーに 2 個以上のクライアントが含まれる場合は、これらのクライアントは同一の Avamar ドメインに属している必要があります。クライアントレベルでバックアップ ポリシーの設定をオーバーライドできます。

A

Avamar Administrator サポートされている Windows または Linux クライアント コンピューターからリモートで Avamar システムを管理するために使用するグラフィカル管理コンソール ソフトウェア アプリケーション。

Avamar Downloader サービス ターゲットの Avamar システムにソフトウェア インストール パッケージを配信する Windows ベースのファイル配信システムです。

Avamar Web Access ファイルをクライアントに素早くリストアするために、Avamar サーバーへのアクセスを提供するブラウザベースのユーザー インターフェイス。

Avamar インストール マネージャー インストール パッケージを管理する Web インターフェイスです。

Avamar クライアント Avamar ソフトウェアを実行し、ネットワーク接続を介して Avamar サーバーにアクセスするコンピューターまたはワークステーション。Avamar クライアント ソフトウェアは、[クライアント エージェント] と 1 個以上の [プラグ イン] で構成されます。

Avamar サーバー Avamar クライアント/サーバー システムのサーバー コンポーネント。Avamar サーバーは、すべての保護対象のクライアントから効率的にバックアップを保存する、高可用性を備えたフォールトトレラントシステムです。このサーバーには、データのリストア、クライアント アクセス、リモートシステム管理に不可欠なプロセスとサービスも備えられています。Avamar サーバーは、複数のネットワークストレージノードに対する分散アプリケーションとして実行されます。

AvFS (Avamar File System) 通常はアクセスできない Avamar HFS のブラウズ可能な仮想ファイル システムのビュー。Avamar File System では、Avamar サーバー上に保存されているすべてのバックアップに対し、個々のファイルのレベルまでの読み取り専用アクセスを提供します。これによって、Avamar サーバーはバックアップとリストア用のリポジトリとしてばかりでなく、オンラインで長期的な履歴を保持する戦略的な企業の情報ストアとして使用できます。

AvInstaller パッケージのインストールを実行し、レポートするバックエンド サービスです。

C

ConnectEMC Avamar サーバ上で実行され、情報を Avamar サポートに送信するプログラム。ConnectEMC は、通常、優先度の高いイベントが発生したときにアラートを送信し、また、1 日 1 回レポートを送信するように構成されています。

D

DNS ドメイン ネーム サーバー。ドメイン名を特定の IP アドレスに割り当てるための分散された動的ディレクトリ サービス。

E

E メール ホーム High Priority Events プロファイルと Notification スケジュールを使用して、サーバ エラーとステータス メッセージを定期的に Avamar サポートに送信するオプション機能。

EMC リポジトリ サーバー インストール パッケージ、クライアント インストール パッケージ、マニフェスト ファイルを含むリポジトリです。リポジトリは、EMC ネットワーク上にあります。EMC のそれぞれのお客様は、自らが利用可能なファイルを含むダウンロード センターを備えています。Avamar Downloader Service から EMC リポジトリへの送信は、HTTP 接続を介して SSL で暗号化されます。

EMT (EM Tomcat サーバー) Avamar EMT (EM Tomcat サーバー) により、Avamar システム情報の表示に不可欠なサービスと、標準 Web ブラウザーを使用して Avamar システムを管理するメカニズムが提供されます。EMT は MCS と直接通信します。

ESRS EMC セキュア リモート サポート。

H

HFS ハッシュ ファイル システム。クライアント バックアップの保存に使用される Avamar サーバー内のコンテンツ アドレス ストレージ エリア。

HFS チェック Avamar HFS (ハッシュ ファイル システム) チェックは、特定のチェックポイントの整合性を検証する内部処理です。チェックポイントが HFS チェックに合格すると、サーバーのロール バックで使用できる信頼性があると考えられます。

J

JRE Java Runtime Environment。

L

LAN Local Area Network。

LOFS Loopback File System。

M

MAC アドレス Media Access Control アドレス。一般にハードウェア機器の最低レベルに埋め込まれているハードウェア アドレスで、ネットワーク上の各デバイスを一意に識別するために使用します。

MCS 管理コンソール サーバー。Avamar サーバーの一元管理（スケジュール設定、モニタリング、管理）を提供するサーバー サブシステム。MCS は、[Avamar Administrator] で使用されるサーバー側のプロセスも実行します。

N

NAT Network Address Translation。

NDMP Network Data Management Protocol。データを NAS システムからバックアップ サーバーに移動するために使用するオープン プロトコルです。

NFS ネットワーク ファイル システム。

NIS Network Information Service。Avamar サーバーにログインするために使用できる外部認証システム。

NTP Network Time Protocol。クライアント コンピューターまたはサーバー コンピューターの時刻の同期を制御します。

O

ODBC Open DataBase Connectivity。データを処理している DBMS（データベース管理システム）に関係なく、任意のアプリケーションから任意のデータにアクセスできるようにするための標準のデータベース アクセス メソッド。

OpenLDAP Open Lightweight Directory Access Protocol。Avamar サーバーにログインするために使用できる外部認証システム。

P

PAM Pluggable Authentication Module。個々のアプリケーションがユーザーを認証する方法をローカルシステムの管理者が定義できるようにするための Linux ライブラリ。

R

RAIN Redundant Array of Independent Nodes。Avamar モジュールでシングル ノードに障害が発生した場合に、Avamar サーバーが可用性を維持し、データ ストレージを維持できるようにする、柔軟なフォールトトレラント アーキテクチャ。

RDMS リレーショナル データベース管理システム。

S

SSH セキュア シェル。パスワード入力を求める代わりに暗号化されたセキュリティ キーを使用して認証するリモート ログイン ユーティリティです。これによって、保護されていないパスワードがネットワークを介して転送されることを防止できます。

T

TFTP Trivial File Transfer Protocol。ディレクトリまたはパスワード機能を持たない TCP/IP FTP プロトコルのバージョン。

V

VLAN Virtual Local Area Network。

あ

アクセラレータ Avamar NDMP Accelerator (アクセラレータ) は専用の Avamar サーバー ノードであり、Avamar システムの一部として使用されると、NDMP (Network Data Management Protocol) を使用した NAS (ネットワーク接続型ストレージ) システムのバックアップおよびリストアが可能になります。

アクティベーション CID (クライアント ID) をクライアントに送信するプロセス。クライアントは受け取った CID を、クライアント ファイル システム上の暗号化ファイルに保存します。

以下も参照してください。 クライアントのアクティベーション

<

クライアント エージェント MCS (管理コンソール サーバー) およびそのクライアントにインストールされているプラグ インと通信するクライアント上で実行される、プラットフォーム固有のソフトウェア プロセス。

クライアント登録 Avamar サーバーでの同一性を確立するプロセス。Avamar は、クライアントを認識すると、一意の CID (クライアント ID) をクライアントに割り当てます。クライアント ID は [クライアントのアクティベーション] の際にクライアントに送信されます。

以下も参照してください。 登録

クライアントのアクティベーション クライアント ID (CID) をクライアントに送信するプロセス。クライアントは受け取った CID を、クライアント ファイル システム上の暗号化ファイルに保存します。

以下も参照してください。 アクティベーション

グループ 1つ以上の Avamar クライアントで構成される Avamar Administrator 内の組織のレベル。Avamar グループのすべてのクライアントでは、同一のグループ ポリシーを使用し、これには [データセット]、[スケジュール]、[保存ポリシー] が含まれます。

グループ ポリシー Avamar Administration では、グループ ポリシーは、Avamar グループのすべてのクライアントの [Dataset]、[Schedule]、および [Retention Policy] として定義されます。

し

システムの移行 「root-to-root」レプリケーションを使用して、ソース Avamar サーバー上のすべてのデータを新しいターゲットサーバーにコピーする計画的操作。グローバル クライアント ID（グローバル CID）を使用する場合、これまでソースサーバーにバックアップされていたクライアントは、新しいターゲットサーバーに再登録せずに透過的に処理を継続できます。

す

スケジュール グループ内のクライアントのバックアップの実行頻度と、実行日の開始時刻および終了時刻を制御する機能。スケジュールは、名前を付けて複数のグループに関連付けることができる永続的で再利用可能な Avamar ポリシーです。

ストレージ ノード データの保管機能を提供する Avamar サーバー内のノード。

て

データセット クライアント グループ全体のバックアップに含まれる、または排除される、サポートされた各プラットフォームの一連のファイル、ディレクトリ、およびファイル システムを定義するポリシー。データセットは、名前をつけて複数のグループに関連づけることができる固定の再利用可能な Avamar ポリシー。

と

登録 Avamar サーバーでの同一性を確立するプロセス。Avamar は、クライアントを認識すると、一意の CID（クライアント ID）をクライアントに割り当てます。クライアント ID は [クライアントのアクティベーション] の際にクライアントに送信されます。

以下も参照してください。 クライアント登録

ドメイン 名前が付けられた制御管理領域に多数のクライアントを編成するために使用する Avamar Administrator の機能。

に

認証システム Avamar サーバーへのユーザー アクセスを許可するために使用する、ユーザー名とパスワードのシステム。Avamar では、独自の avs（内部認証システム）に加えて、複数の外部認証システム（OpenLDAP、Windows Active Directory、NIS、SMB）がサポートされます。

の

ノード 処理能力とハード ディスク ドライブ ストレージからなるネットワーク ストレージ サブシステムであり、Avamar ソフトウェアを実行します。

は

バックアップ 個々のファイル、選択されたデータ、またはバックアップ全体としてリストアできるクライアントデータのポイントインタイムコピー。

パッケージ EMC リポジトリから利用可能な Avamar ソフトウェア インストール ファイル、ホットフィックス パッチ、OS パッチ。パッケージには、次の 3 種類があります。

- **Client** : Avamar ファイル システムまたはアプリケーション バックアップ ソフトウェアのリリース。
- **Server** : 新しいリリースの Avamar サーバー ソフトウェア、サービス パック、またはオペレーティング システム、MC、GSAN のパッチ。
- **Workflow** : ノードの追加やノードの交換などのオペレーションを実行するパッケージ。

パッケージ ファイルでは、.avp のファイル拡張子を使用します。

ふ

プラグ イン クライアント上に常駐する特定の種類のデータを認識する Avamar クライアント ソフトウェア。

プラグ イン オプション バックアップまたはリストア機能を制御するためにバックアップ時やリストア時に指定するオプション。

フルレプリケーション root-to-root レプリケーションでは、ソース システム全体の完全な論理コピーをターゲット システムに作成します。レプリケーションされたデータは REPLICATE ドメインにコピーされません。その代わりに、ソース クライアントがターゲット システムに登録したように、root ドメインに追加されます。この方法でレプリケートされたソース サーバー データは、ターゲット システムで自由に変更することもできます。このレプリケーション方法は、通常、システムの移行（小規模の Avamar の構成から、より大規模な、場合によってはマルチ ノード構成への移行）、またはシステムの交換（災害復旧などの場合）のために使用します。

ほ

保存設定 Avamar サーバー上のバックアップを自動的に削除する時間設定。Avamar サーバーから削除しないバックアップには、永続的な保存設定を指定できます。保存設定は、名前を付けて複数のグループに関連付けることができる永続的かつ再利用可能な Avamar ポリシーです。

ポリシー 名前を付けて複数のグループに適用できる、クライアント バックアップのためのルールのセット。グループにはデータセット、スケジュール、保存ポリシーがあります。

ま

マニフェスト ファイル 現在、EMC リポジトリからダウンロード可能なサーバー、クライアント、ワークフロー パッケージをすべて一覧表示した XML ファイル。

も

モジュール Avamar 1.2.0 以前のマルチ ノード Avamar サーバーではデュアル モジュール同期 RAIN アーキテクチャを使用していました。このアーキテクチャでは、ノードは個別の VLAN 上の 2 つの個別の機器キャビネットに均等に分散されていました。「モジュール」という用語は、このアーキテクチャを記述してサポートするために使用する論理構造です（以前のマルチ ノード Avamar サーバーは、プライマリ モジュールとセカンダリ モジュールで構成されていました）。このレガシー システムも引き続きサポートされます。ただし、新しいマルチ ノード Avamar サーバーではシングル モジュール アーキテクチャを利用しているため、Avamar Administrator によって「モジュール詳細」情報が提供されるものの、モジュールはサーバー全体と論理的に同等です。

ゆ

ユーティリティ ノード 拡張性に優れたマルチ ノード Avamar サーバーでは、単一のユーティリティ ノードによって基本内部サービスがサーバーに提供されます。このサービスには、MCS、DNS（Domain Name System）、外部認証、NTP（Network Time Protocol）、Web アクセスが含まれます。ユーティリティ ノードはこれらの基本サービスの実行専用であるため、バックアップの保存には使用できません。

り

リストア 1 つ以上のファイル システム、ディレクトリ、ファイル、データ オブジェクトをバックアップから取得し、そのデータを指定された場所へ書き込む処理。

れ

レプリカ バックアップのレプリケートされたコピー。

レプリケーション レプリケーションは、Avamar システムがデータの読み取り専用コピーをリモート システムに格納できるようにするオプション機能です。レプリケートしたデータは、クライアント バックアップのレプリカおよび Avamar システム データのコピーとして使用できます。レプリケーションは、Avamar システムの災害復旧をサポートします。

ろ

ローカル リポジトリ ユーティリティ ノードまたはシングル ノード サーバー上の `/data01/avamar/repo/packages` ディレクトリ。このディレクトリには、EMC リポジトリからの最新のマニフェスト ファイルがあります。Avamar Downloader Service は、EMC リポジトリからのパッケージをローカル リポジトリにプッシュします。お客様のサイトでインターネットへのアクセスが許可されていない場合は、ローカル リポジトリにパッケージを手動でコピーできます。

ロール 各ユーザーが Avamar サーバーで実行できる操作を制御する Avamar Administrator の設定。ロールは、ユーザーごとに割り当てられます。

