Dell EMC Data Protection Advisor

バージョン 18.1

インストールおよび管理ガイド

302-004-935
REV 02

DELL EMC

2018 年年 7 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。

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

目次

図 7

表 9

序文 11

第 1 章 DPA のインストールの準備 15

概要 16
システム要件 16
DPA サーバー プラットフォーム 16
データストア ストレージ 17
権限 17
NTP 時間の同期化 17
インストールに関する考慮事項 18
仮想インフラストラクチャのメモリーおよび CPU の構成 18
OS リソースの最適化 18
DPA での通信設定 19
DPA ポートの設定 20
インストールと構成の概要 22

第 2 章 DPA のインストール 29

DPA サーバーのインストール 30
Datastore Service のインストール 30
Application Service のインストール 32
アプリケーションのクラスタリング 34
データストア レプリケーション 45
DPA エージェントのインストール 53
DPA エージェントのインストール 53
DPA Agent 登録パスワードの設定 55
バックアップ アプリケーション データをさかのぼって収集するように DPA バージョン 18.1 エージェントを構成する 55
コマンド ラインを使用したインストール 56
DPA インストール後の作業 61
DPA アプリケーション サーバーの暗号化 64
アプリケーション サーバー クラスタの暗号化 65
DPA でのアンチウイルス ソフトウェアの構成 65
アップグレード 66
アップグレードの前提条件 66
DPA のアップグレード 67
DPA エージェントのアップグレード 68
DPA バージョン 6.5 エージェントおよびバージョン 6.5 サーバーとあわせた、バージョン 6.5 以前の DPA エージェントのアップグレード 68

2.12 より前の glibc を実行している Linux バージョンにおける DPA のアップグレード 69
既存のクラスタのアップグレード..... 69
DPA 6.3 以降によるデータストア レプリケーションを使用したアップグレード..... 70
DPA バージョン 6.3 以前によるデータストア レプリケーションを使用したアップグレード..... 71
データストア レプリケーションと既存のクラスタがある場合のアップグレード..... 71

第 3 章 DPA の管理 73

ライセンス管理..... 74
DPA にバンドルされた評価版ライセンス..... 74
DPA のライセンス タイプ..... 74
DPA での CLP ライセンスと WLS ライセンスの共存..... 74
期限切れのライセンス..... 74
ライセンスの削除..... 74
新規ライセンスの追加..... 75
一時ライセンスの有効期限を示す自動ポップアップの無効化..... 75
ユーザーとセキュリティ..... 75
ユーザー アカウント..... 75
ユーザーの役割と権限..... 78
外部認証、LDAP 統合、バインディング..... 81
ユーザー プロビジョニングの自動化..... 83
システム設定..... 87
バックアップ フィールドとリストア解決フィールドの構成..... 87
設定の表示と編集..... 88
システム設定..... 88
エージェントレスでの検出機能..... 91
サーバー データの削除..... 92
データ削除スケジュールの構成..... 92
Root Cause Analysis Settings..... 93
DPA Web コンソールを使用した履歴のバックアップ データの収集..... 94
サポート バンドルの生成..... 94
デジタル証明書..... 95
期間..... 95
DPA のタイム ゾーン..... 95
レポートの自動的な優先順位づけ..... 96
スケジュール..... 97
Manage Data Collection Defaults..... 97
サイトの管理..... 116
アプリケーション サービスの管理..... 117
Linux で DPA アプリケーションを非 root ユーザーとして実行する..... 117
インストールまたはアップグレードをしてから TLS プロトコル バージョン 1.2 を設定する..... 117
サービス情報のカスタマイズ..... 118
クラスタリング管理..... 121
データストア サービス管理..... 123
データストアのバックアップ..... 123
データストア レプリケーション管理..... 125
DPA データベース スーパーユーザーのパスワード..... 129
DPA コマンド ライン操作..... 130

UNIX ユーザーへの DPA config ファイルのソーシング.....130
dpa CLI コマンド..... 130
dpa agent コマンド.....132
dpa application コマンド.....134
dpa datastore コマンド.....142
dpa サービス コマンド.....150
履歴バックアップ ジョブ データのロード.....151

第 4 章 DPA での環境の検出 155
検出用の環境の構成.....156
検出の概要..... 156
監視対象のオブジェクトの定義.....156
［Discovery Wizard］を実行する前に.....158
バックアップ アプリケーションの監視.....160
データベースの監視.....174
クラウド ベースのソリューションを使用したアプリケーションの監視.....185
ホスト監視..... 186
プライマリ ストレージの監視.....191
保護ストレージの監視.....194
スイッチおよび I/O デバイスの監視..... 198
仮想化管理.....199
クラスタの監視.....200
ホストまたはオブジェクトの手動による検出.....201
検出後のジョブ データ収集について..... 203
監視対象オブジェクトおよびグループ..... 203
オブジェクトの概要..... 203
グループ.....205
オブジェクト属性..... 206
Smart Group.....206
DPA Web コンソールを使用した履歴のバックアップ データの収集.....209
ポリシー、ルール、アラートの構成.....209
ポリシーとアラートの概要..... 209
ポリシー.....210
ポリシーとイベント生成..... 236
スクリプトからアラートを生成するパラメータ.....237
ルール テンプレート..... 239
ポリシーの適用..... 239

第 5 章 DPA のアンインストール 241
ソフトウェアのアンインストール..... 242
サイレント コマンド ラインを使用したアンインストール.....242
Windows のユーザー インタフェースでのアンインストール.....242
エージェントのみのアンインストール..... 242

第 6 章 トラブルシューティング 243
インストールのトラブルシューティング.....244
DPA サーバーのパスワードを変更した後、DPA エージェントが再起動または登録されない..... 244
インストール後に Linux で発生する DPA データストアの起動の障害..... 244
Windows Server 2012 での DPA Web コンソールの起動の失敗.....244

インストール後のメモリーの調整 244
アップグレード中のエラー メッセージ 245
ログ ファイル 245
デフォルト ログの詳細レベルの変更 245
インストール ログ ファイルの表示 245
サーバー ログ ファイルの表示 246
サーバー ログ ファイル 246
エージェント ログ ファイルの表示 246
ログ ファイルの管理 246
Windows を実行する仮想マシンにおける代替のログ ローテーションの有効化 246
インストーラー ログ ファイルの誤りがあるメモリー データ 247
DPA Web コンソールを使用した、デバッグ モードでの DPA エージェント リクエストの実行 247
modtest のデフォルトの削除スケジュール 248
Generate Support Bundle 248
データ コレクションのトラブルシューティング 248
データ コレクションのトラブルシューティング： 最初のアクション 248
データ コレクションのトラブルシューティング： 2 番目のアクション 248
EMC サポートへの送信用ログ ファイルの準備 249
レプリケーション解析用クライアント/ストレージ検出に関するトラブルシューティング 249
リモート実行を使用したクライアント/ストレージ検出 249
エージェントを使用したクライアント/ストレージの検出 251
一般的なクライアント/ストレージの検出 251
間違ったリカバリ ポイント時間の同期 254
レポートの出力失敗に関するトラブルシューティング 255
レポートの生成と発行に関する問題のトラブルシューティング 255
システム クロックの同期 255

図

1 DPA ポートとプロトコル.....19
2 DPA のインストール ワークフロー.....23
3 DPA アプリケーション ノードとアプリケーションを監視している DPA エージェント間の関係..... 156
4 マルチレベル Smart Group のオブジェクト ライブラリの構成例.....208

図

表

1 改訂履歴....11
2 表記規則....13
3 DPA アプリケーション ポートの設定....20
4 DPA データストアのポート設定....21
5 DPA エージェントのポート設定....21
6 DPA クラスタのポート設定....21
7 インストールと構成の概要 23
8 インストーラー コマンド ライン オプション....57
9 データストア インストーラーの変数....58
10 データストア詳細オプションのレプリケーション変数....58
11 データストア エージェントの変数....59
12 アプリケーション インストーラーの変数....59
13 アプリケーション サーバー エージェントの変数....60
14 アプリケーション サーバー クラスタの詳細オプションの変数....60
15 スタンドアロン エージェント インストーラーの変数....61
16 パスワード ポリシー....76
17 パスワード履歴のポリシー....77
18 ログイン制限....77
19 Password Expiration....78
20 ユーザーの役割....78
21 DPA での LDAP 認証の構成....81
22 オープン LDAP サーバー設定....84
23 データ コレクション エージェント設定 88
24 サーバー設定....89
25 SharePoint 設定....90
26 レプリケーション解析設定....91
27 エージェントレス検出の設定....91
28 収集データのデフォルトの保存期間....93
29 システム生成データのデフォルトの保存期間....93
30 モジュール別データ コレクション リクエスト オプション....98
31 VTL テンプレート....118
32 コマンドとオプションの略語 131
33 データ監視のセットアップの概要 157
34 [Discovery Wizard] によるデータ コレクション構成用の、接続性の詳細 158
35 HP Data Protector 6.1 パッチ ID....165
36 システム監視モジュール....186
37 マルチレベル Smart Group の例....207
38 キャパシティ プランニング....221
39 変更管理....222
40 構成....222
41 データ保護....223
42 ライセンス....225
43 パフォーマンス....225
44 プロビジョニング....225
45 復旧可能性....226
46 リソース使用率....229
47 Service Level Agreement....231
48 状態....231
49 トラブルシューティング....233

50 復旧可能性チェック 235
51 スクリプト フィールド パラメータ 237
52 スクリプト アラート引数 238
53 クライアント/ストレージ検出の問題とソリューション 250
54 エージェントを使用したクライアント/ストレージの検出に関する問題とソリューション 251
55 一般的なクライアント/ストレージの検出に関する問題とソリューション 252

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、EMC では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、このドキュメント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、またはこのマニュアルの説明どおりに動作しない場合には、EMC のテクニカル 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。EMC オンライン サポート（https://support.emc.com）にアクセスして、このマニュアルの最新バージョンを使用していることを確認してください。

目的

このドキュメントでは、DPA をインストールし、データ保護環境を監視する目的で DPA を設定する方法を説明します。このドキュメントでは、ユーザーとロールの作成、システム設定の更新、ポリシーの作成、データ収集のトラブルシューティングなどの管理機能についても説明します。

ISO 9001 認証

この製品の設計、開発を管理する管理システムは、ISO 9001:2015 認定を受けています。

対象読者

このドキュメントは、システム管理者を対象としています。このマニュアルの読者は、次のタスクに精通している必要があります。

- バックアップおよびレプリケーション環境を構成するさまざまなハードウェアおよびソフトウェアのコンポーネントを識別する。
- バックアップおよびレプリケーション オペレーションを構成するための手順に従う。
- 問題を特定してソリューションを実装するためのガイドラインに従う。

改訂履歴

次の表に、このドキュメントの改訂履歴を示します。

表 1 改訂履歴

リビジョン	日付	説明
01	2018 年 7 月 6 日	DPA18.1 のこのドキュメントの最初のリリース
02	2018 年 7 月 13 日	更新されたセクション：DPA エージェントのアップグレード （68 ページ）

関連ドキュメント

DPA マニュアル セットには、次のマニュアルが含まれます。

- 「Data Protection Advisor Custom Reporting Guide」
- 「Data Protection Advisor Data Collection Reference Guide」
- 「Data Protection Advisor インストールおよび管理ガイド」
- 「Data Protection Advisor Migrator Technical Notes」

- 「Data Protection Advisor online help system」
- 「Data Protection Advisor 製品ガイド」
- 「Data Protection Advisor Release Notes」
- 「Data Protection Advisor レポート リファレンス ガイド」
- 「Programmers' Guide to Using Data Protection Advisor REST API」
- 「Data Protection Advisor Security Configuration Guide」
- 「Data Protection Advisor Software Compatibility Guide」
- 「その他のテクニカル ノートおよびホワイト ペーパー」

このマニュアルで使用される特記事項の表記規則
EMC では、特別な注意を要する事項に次の表記法を使用します。

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 2 表記規則

[太字]	ボタン、フィールド、タブ名、メニュー パスなど（ユーザーが選択またはクリックする）インターフェイス要素の名前を示す
「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： • 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 • パス名、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のある内容を示す（例：x、y、z）
...	省略記号は、例の中で省略した必須ではない情報を示す

問い合わせ先
EMC のサポート情報、製品情報、ライセンス情報は、次の場所で入手できます。

製品情報
ドキュメント、リリース ノート、ソフトウェア アップデートや、EMC 製品の詳細については、EMC オンライン サポート（https://support.emc.com）を参照してください。

テクニカル サポート
EMC オンライン サポート（https://support.emc.com）にアクセスして、［サービス センター］をクリックします。サイト内に EMC テクニカル サポートへの問い合わせ方法がいくつか表示されます。サービス リクエストを開始するには、有効なサポート契約が必要です。有効なサポート契約を結ぶ方法の詳細や、アカウントに関する質問については、EMC 担当営業にお問い合わせください。

オンライン コミュニティ
共通の関心を持つユーザーとの連絡、会話、製品サポート、ソリューションの内容については、EMC 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 EMC 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。

ご意見
マニュアルの精度、構成および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は、DPAD.Doc.Feedback@emc.com までお送りください。

第 1 章

DPA のインストールの準備

この章は、次のセクションで構成されています。

- 概要 16
- システム要件 16
- インストールに関する考慮事項 18
- DPA での通信設定 19
- DPA ポートの設定 20
- インストールと構成の概要 22

概要

DPA のすべての導入には、以下のインストールが含まれます。

- 1 台のホストへの DPA データストア サーバーと DPA エージェント
- 別のホストへの DPA アプリケーション サーバーと DPA エージェント

DPA をインストールするときは、インストール ウィザードの手順に従ってこれらのコンポーネントを配置します。

同じホストへのアプリケーション サーバーとデータストア サーバーのインストールはサポートされていません。複数のアプリケーション サーバーを同じデータストア サーバーに接続できます。その場合、各追加アプリケーション サーバーは専用のホストを使用し、DPA クラスタとしてインストールされます。システム監視およびリモート データ コレクションのために、追加の DPA エージェントをインストールできます。DPA はデータストア レプリケーションをサポートし、継続性があり、安全で信頼性の高いレプリケーションを可能にします。これにより、DPA は、プライマリ データストア（マスター）のレプリカ コピー（スレーブ）を維持できるようになり、単一障害点の障害に対する復元性を実現します。

システム要件

DPA での基本的な最小システム要件は次のとおりです。「Data Protection Advisor Software Compatibility Guide」では、システム要件の総合リストが提供されています。

DPA サーバー プラットフォーム

DPA サーバーは、64 ビット版のオペレーティング システムのみをサポートしています。お客様のアカウント担当者と協力して、ご使用の環境に最適なサイズ設定を確認します。

メモリー要件

- 16 GB RAM/4 コア（DPA データストア サーバー用）
- 16 GB RAM/4 コア（DPA アプリケーション サーバー用）

ハード ディスク ドライブ要件：

- 18GB のローカル接続ディスク ストレージ、アプリケーション サーバー用
- 20GB のローカル接続ディスク ストレージ、データストア サーバー用
- 3 GB の空き領域（データベースのアップグレード用）

注

アプリケーション システムとデータストア システムの同じ場所への配置は、本番システムではサポートされません。同じ場所にシステムを配置するオプションがインストーラーで提供されていても、選択すると、サポートされていないとのダイアログが本番システムのディスプレイに表示されます。

- DPA アプリケーション サーバーと DPA データストア サーバーを使用して、他のアプリケーションを実行しないでください。DPA アプリケーション サーバー ホストと DPA データストア サーバー ホストのリソースは、DPA 専用にする必要があります。
- 仮想環境で DPA を実行する場合、割り当てられる CPU およびメモリーは DPA サーバー用に予約する必要があります

- DPA インストーラーのソフト閾値は 7892 MB、ハード閾値は 5844 MB です。ソフト閾値がインストールの続行を許可しても、ハード閾値が許可しません。
- 内部 DPA リソース使用のサイズ設定とチューニングがインストール時に自動で行われます。インストール時にリソース（CPU、メモリー）が他のアプリケーションで使用されていると、DPA のパフォーマンスが低下する場合があります。
- オペレーティング システム：
  - 64 ビット オペレーティング システムのみをサポートします
  - Microsoft Windows Server 2008 R2、2012、2012 R2（x64 のみ）、2016
  - Red Hat Linux ES/AS 6.0、6.2、6.4（64 ビット）、6.5、6.8、7、7.1、7.2、7.3、7.4（64 ビット）
    Update Agent（up2date）を実行して、オペレーティング システムの最新のパッチがインストールされていることを確認します
  - SUSE Linux 12 x86（64 ビット）

  Update Agent（up2date）を実行して、オペレーティング システムの最新のパッチがインストールされていることを確認します

  パフォーマンスの向上のため、libaio をシステムにインストールしてシステムの `LD_LIBRARY_PATH` で使用できるようにすることをお勧めします

データストア ストレージ

パフォーマンス上の理由により、NAS ベースのファイル システム（CIFS または NFS 共有）に DPA データストア サーバーをインストールすることは推奨しません。ファイル システムに必要な I/O を管理する帯域幅がない可能性があるためです。

ほとんどの導入で、標準のデータストア ファイル システム レイアウトを使用できますが、高度なインストール オプションを使用し、多様なファイル システムを多様なファイル システムに分散させると、インストール中のパフォーマンスを最適化できます。

権限

インストールが失敗しないように、ソフトウェアをインストールする前に以下の権限があることを確認してください。

- Windows：
  - 管理者権限（フルアクセスのあるドメインまたはローカル）
  - UAC（ユーザー アカウント制御）が有効になっている場合は、［管理者として実行］を使用します
- UNIX/Linux：
  - root ユーザー
  - セキュリティ ソフトウェアを使用して、root アカウントへのアクセスを管理する場合、root になった後で権限が新しいユーザーの作成を許可することを確認します。これには、作成するアカウントのデフォルト ホーム ディレクトリを作成する機能が含まれます。

NTP 時間の同期化

DPA サーバーと DPA エージェント ホストを同期するには、Network Time Protocol（NTP）を使用可能にしておくことをお勧めします。これにより、正確で整合性のとれたデータ コレクションとなります。

DPA のユーザー認証プロセスでは、クライアント マシンのシステム クロック時間とサーバーのシステム クロック時間が誤差 1 分以内で同期する必要があります。

インストールに関する考慮事項

DPA インストール ウィザードには、マスター データストアとスレーブ データストアによるデータストア レプリケーションの構成、およびクラスタ化されたアプリケーション オブジェクトの構成のための、高度なオプションがあります。これらのオプションの一方または両方を使用する場合は、以下に従ってください。

- インストールの開始前に、最終導入トポロジーを計画します。
- すべてのホストおよび IP アドレスを決定し、使用できるようにしておきます。

高度なインストールを計画している場合は、担当営業に高度なアーキテクチャ ソリューション設計の支援を依頼してください。

仮想インフラストラクチャのメモリーおよび CPU の構成

仮想化されたインフラストラクチャに DPA を導入する場合は、次の手順を実行します。

手順

- 割り当てるメモリーは、各 VM 専用に予約してください。
- DPA のアプリケーション VM およびデータストア VM を、リソース割り当て共有が高に設定されたリソース プールに配置します。または、各個別 VM に対して高共有割り当てを選択します。
- データストア ディスクに対しては Thick Provision Eager Zeroed を選択します。ディスク割り当てを Thick Provision Eager Zeroed にするとすべての領域は事前に割り当てられ、システムが利用可能になる前に、フル ディスク ファイルはゼロになります。

OS リソースの最適化

一般的なチューニング

インストール中、インストーラーは導入中のホスト環境に対して、DPA Datastore Service をチューニングします。このチューニングは、ホストが DPA 専用であることを前提としており、ディスク領域、合計メモリー、CPU コアなどのリソースが考慮されます。DPA Datastore Service の存続期間中、これらの物理リソースのいずれかが増減した場合、データストア ホストで dpa datastore tune コマンドを実行します。詳細については、dpa datastore tune（149 ページ）を参照してください。

チューニングに関するハードウェアの問題

最適なパフォーマンスが問題となる導入では、Datastore ホスト サーバーに使用するハードウェアのタイプと質が Datastore Service の性能に著しく影響を与えます。

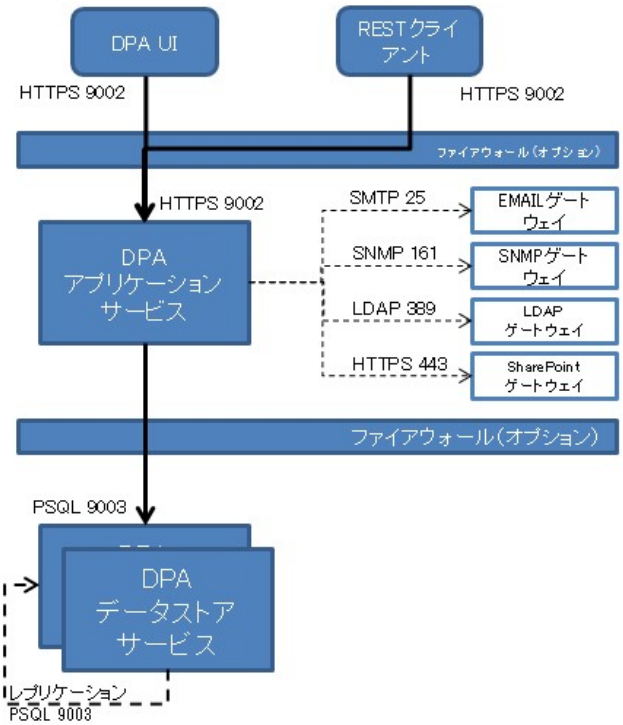
通常、システムの RAM およびディスク スピンドルが多いほど性能が向上します。これは、RAM が余っていれば、ディスクへのアクセスが少なくなるためです。また、スピンドルが余っていれば、読み書きが複数のディスクに分散され、スループットが向上し、ドライブ ヘッドの輻輳が減少します。

本番に備えて、DPA Application Service と DPA Datastore Service は異なるハードウェアに配置する必要があります。これにより Datastore Service 専用により多くのハードウェアが割り当てられるだけでなく、アプリケーション データやシステム データではなく、オペレーティング システムのディスク キャッシュに入る Datastore データの量が増えます。

DPA での通信設定

DPA サーバーと DPA エージェントの間の通信を確保するには、次の図に示すように、ネットワークにファイアウォールを構成して、これらのポートでの通信を許可します。監視するものによっては、ファイアウォールで他のポートの追加構成が必要になる場合があります。たとえば、Avamar を監視する場合、Avamar サーバーと DPA エージェントの間にポート 5555 を開きます。詳細については「DPA での環境の検出」を参照してください。

図 1 DPA ポートとプロトコル



注

*アプリケーション サーバーとコレクターは 1 台の場合も複数台の場合もあります。

上の図の矢印は、開始の向きを示しています。DPA エージェントは、9002 で DPA アプリケーション サーバーへの接続を開始します。ファイアウォールの場合、これは何がどのポートで接続を開始し、他の側で何がリスンしているかに基づきます。DPA エージェントから DPA アプリケーション サーバーへの通信は、9002 および 3741 TCP で行われます。エージェントと DPA サーバーの間の通信は、安全であり、暗号化され、圧縮されています。

図 1 DPA ポートとプロトコル （続き）

次の表では、DPA が正常に機能するために導入ホストで必要となる追加ポートについて詳細が示されています。示されているポートは、接続を受け付け、確立された接続で応答を返すことができる必要があります。一部のネットワーク ベンダーは、このようなハンドシェーク通信を双方向と説明しており、そのようなネットワーク セキュリティ デバイスはこれに対応しているはずです。

DPA ポートの設定

次の表に DPA が正常に機能するために必要なポートを列挙します。監視対象システムによっては、DPA エージェントに追加ポートが必要になる場合もあります。インストール要件の詳細については、「Data Protection Advisor インストールおよび管理ガイド」を参照してください。

表 3 DPA アプリケーション ポートの設定

ポート	説明	トラフィックの方向
25	SMTP サービスに使用する TCP ポート	SMTP サーバーに送信するアウトバウンド接続。
80	SharePoint サービスに使用する TCP ポート	SharePoint サーバーに送信するアウトバウンド接続。
161	SNMP サービスに使用する UDP ポート	SNMP デバイスに送信するアウトバウンド接続。
389 と 636（SSL 経由）	LDAP 統合に使用する TCP ポート	LDAP サーバーに送信するアウトバウンド接続。
3741	DPA エージェントの通信に使用する TCP ポート。	DPA エージェントに送信するアウトバウンド接続。
4447	サービス内通信に使用する TCP ポート	インバウンド接続
4712	サービス内通信に使用する TCP ポート	ローカルホスト接続
4713	サービス内通信に使用する TCP ポート	ローカルホスト接続
5445	サービス内通信に使用する TCP ポート	ローカルホスト接続
5455	サービス内通信に使用する TCP ポート	ローカルホスト接続
8090	サービス内通信に使用する TCP ポート	ローカルホスト接続
9002	HTTPS サービスに使用する TCP ポート。	UI、CLI、REST API のクライアントから SSL 経由で受信するインバウンド接続。
9003	DPA データストアの通信に使用する TCP ポート。	DPA データストアに送信するアウトバウンド接続。

表 3 DPA アプリケーション ポートの設定 （続き）

ポート	説明	トラフィックの方向
9005	Jboss 管理に使用する TCP ポート	ローカルホスト接続
9999	Jboss 管理に使用する TCP ポート	ローカルホスト接続

表 4 DPA データストアのポート設定

ポート	説明	トラフィックの方向
3741	DPA エージェントの通信に使用する TCP ポート。	DPA アプリケーション サーバーから受信するインバウンド接続。
9002	HTTPS サービスに使用する TCP ポート。	SSL 経由で DPA アプリケーション サーバーに送信するアウトバウンド接続。
9003	DPA データストアの通信に使用する TCP ポート。	DPA アプリケーション サーバーから受信するインバウンド接続。

表 5 DPA エージェントのポート設定

ポート	説明	トラフィックの方向
3741	DPA エージェントの通信に使用する TCP ポート。	DPA アプリケーション サーバーから受信するインバウンド接続。
9002	HTTPS サービスに使用する TCP ポート。	SSL 経由で DPA アプリケーション サーバーに送信するアウトバウンド接続。

表 6 DPA クラスタのポート設定

ポート	説明	トラフィックの方向
25	SMTP サービスに使用する TCP ポート	SMTP サーバーに送信するアウトバウンド接続。
80	SharePoint サービスに使用する TCP ポート	SharePoint サーバーに送信するアウトバウンド接続。
161	SNMP サービスに使用する UDP ポート	SNMP デバイスに送信するアウトバウンド接続。
389 と 636（SSL 経由）	LDAP 統合に使用する TCP ポート	LDAP サーバーに送信するアウトバウンド接続。
3741	DPA エージェントの通信に使用する TCP ポート。	DPA エージェントに送信するアウトバウンド接続。
4447	サービス内通信に使用する TCP ポート	インバウンド接続

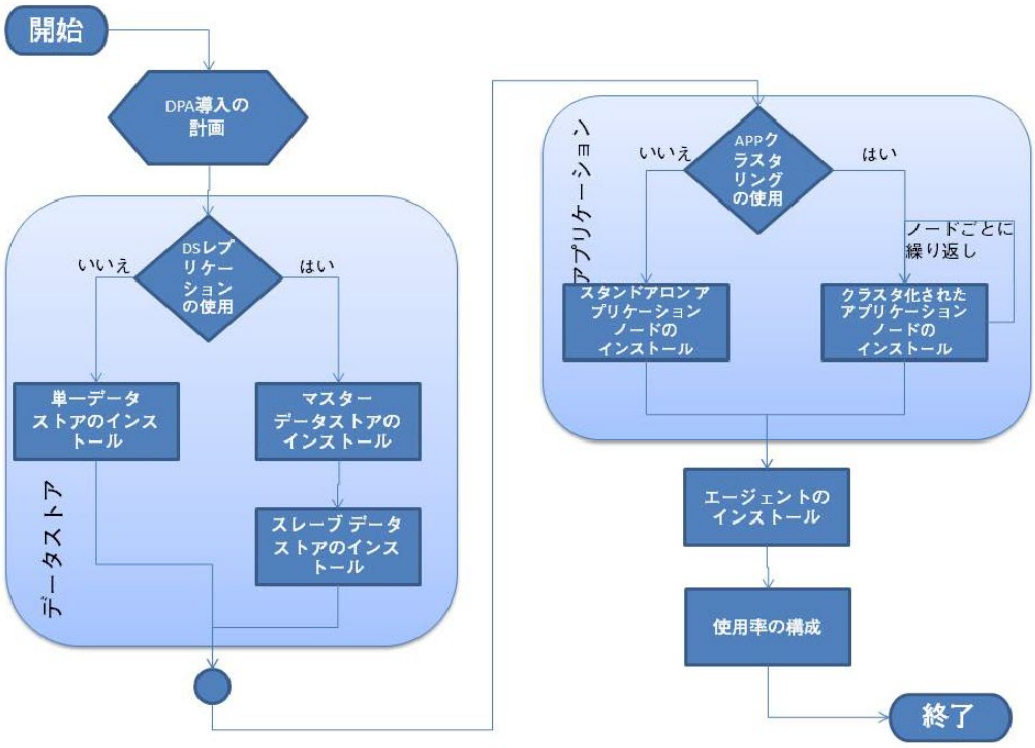
表 6 DPA クラスタのポート設定 （続き）

ポート	説明	トラフィックの方向
4712	サービス内通信に使用する TCP ポート	ローカルホスト接続
4713	サービス内通信に使用する TCP ポート	ローカルホスト接続
5445	サービス内通信に使用する TCP ポート	クラスタの双方向接続
5455	サービス内通信に使用する TCP ポート	クラスタの双方向接続
7500	UDP 経由のマルチキャスト	クラスタの双方向接続
7600	TCP 経由のマルチキャスト	クラスタのインバウンド接続
8090	サービス内通信に使用する TCP ポート	ローカルホスト接続
9002	HTTPS サービスに使用する TCP ポート。	UI、CLI、REST API のクライアントから SSL 経由で受信するインバウンド接続。
9003	DPA データストアの通信に使用する TCP ポート。	DPA データストアに送信するアウトバウンド接続。
9005	Jboss 管理に使用する TCP ポート	ローカルホスト接続
9876	TCP 経由のマルチキャスト	クラスタの双方向接続
9999	Jboss 管理に使用する TCP ポート	ローカルホスト接続
23364	TCP 経由のマルチキャスト	クラスタの双方向接続
45688	TCP 経由のマルチキャスト	クラスタの双方向接続
45689	TCP 経由のマルチキャスト	クラスタの双方向接続
45700	UDP 経由のマルチキャスト	クラスタの双方向接続
54200	UDP 経由のマルチキャスト	クラスタの双方向接続
54201	UDP 経由のマルチキャスト	クラスタの双方向接続
55200	UDP 経由のマルチキャスト	クラスタの双方向接続
55201	UDP 経由のマルチキャスト	クラスタの双方向接続
57600	TCP 経由のマルチキャスト	クラスタの双方向接続

インストールと構成の概要

DPA のインストール ワークフローでは、さまざまな構成で DPA をインストールするためのタスクのおおまかなワークフローが提供されます。

図 2 DPA のインストール ワークフロー



インストールと構成の概要には、DPA のインストールとデータ監視の構成のために実行が必要なタスクのリストが示されています。

表 7 インストールと構成の概要

アクション	コメント
ホスト コンピューターのセットアップ	
DPA サーバーのインストールに使用するホストを 2 つ以上用意します。 1 つは最初の DPA アプリケーション サーバー用、もう 1 つはデータストア用です。 各サーバーのオペレーティング システムが、一方のサービスの IO パフォーマンス ニーズと、他のサービスの RAM およびキャッシュ要件を正しく適切に管理でき、2 つのサービスがリソースで相互に競合しないように、データストアとアプリケーション サーバーには異なるホストが必要です。	DPA を、すでに他のアプリケーションを実行しているサーバーにインストールしないでください。本番環境でのインストールでは、アプリケーション サービスおよびデータストア サービスに使用するホストが 1 つずつ必要です。少なくとも 2 GB の一時領域がある専用サーバーを使用することを推奨します。詳細については、「互換性ガイド」を参照してください。
DPA エージェントのインストールに使用するホストを用意します（オプション）。	DPA サーバーが Windows 上で実行されていて、検出されたホストも Windows である場合、検出されたホストにエージェントをインストールする必要はありません。ただし、DPA サーバー ホストにインストールしたエージェントは、DPA サーバーの監視用にのみ使用することをお勧めします。

表 7 インストールと構成の概要 （続き）

アクション	コメント
	DPA サーバーが Linux ホスト上に存在していて、Windows ホストのクライアント検出を実行している場合は、Windows エージェントに DPA エージェントを少なくとも 1 個インストールする必要があります。
DPA およびそのすべてのコンポーネントが、ウイルス対策ソフトウェアで例外として構成されていることを確認します。	例外として定義されていない場合、ウイルス対策ソフトウェアによって DPA コンポーネントがシャットダウンされたり、関連づけられているファイルが隔離されたりすることがあります。
複数のアプリケーション サーバーをインストールする場合は（DPA クラスタリング）、ネットワーク インフラストラクチャおよび共有ディレクトリをプロビジョニングします。	• DPA アプリケーション サーバー専用の VLAN を割り当てます。専用の VLAN を手配できない場合は、DPA クラスタに使用できる UDP マルチキャスト グループ アドレスをネットワーク管理者に要求します。 • サービスの復元性と品質を高めるには、DPA アプリケーション サーバーへのゲートウェイとしてハードウェア ロード バランシング スイッチをプロビジョニングします。 • すべてのアプリケーション サーバーがアクセスできる共有ディレクトリを設定します。DPA は、この共有ディレクトリを、スケジュール設定されたレポートおよびすべてのアプリケーション サーバーがアクセスする必要のある他の一時ファイルの書き込みに使用します。
VMware または Hyper-V の要件を確認します。	DPA は、VMware または Hyper-V 環境内の Linux または Windows の仮想マシン上で動作することが認定されています。詳細については、『ソフトウェア互換性ガイド』を参照してください。
仮想インフラストラクチャのメモリーおよび CPU を構成します。	仮想インフラストラクチャのメモリーおよび CPU の構成（18 ページ）で詳細を参照してください。
DPA サーバー間の通信用のファイアウォールを、開くか無効にします。	安全な通信を使用してポート 9002 でアプリケーション サーバーに接続する場合は、ブラウザーの設定で安全な通信に対して TLS（Transport Layer Security）の設定が有効になっていることを確認します。 DPA サーバーへのインストールでは、オペレーティング システム/ソフトウェア ベースのファイアウォールを、無効にすることも、DPA コンポーネントをインストールする前に DPA アプリケーション サーバー、DPA データストア サーバー、DPA エージェント間の通信用にポートを開くこともできます。 通常、DPA サーバーおよび DPA エージェントが存在するネットワークは安全であり、ネットワーク ファイアウォールの内側にあります。つまり、オペレーティング シス

表 7 インストールと構成の概要 （続き）

アクション	コメント
	テム/ソフトウェア ベースのファイアウォールを無効にしてもかまいません。オペレーティング システム/ソフトウェア ベースのファイアウォールを有効なままにする場合は、必要なポートを開く/ブロック解除する必要があります。詳細については、DPA での通信設定 (19 ページ) を参照してください。 Linux を使用していて、ファイアウォールを無効にする場合は、次のコマンドを実行して無効にし、起動後または再起動後にファイアウォールが無効のままであることを確認します。 • **iptables stop** を実行します。 • chkconfig ユーティリティを **iptables off** に設定します。
DPA サーバーおよびエージェント ホストにホスト オペレーティング システムをインストールし、必要なすべてのパッチをインストールします。	『ソフトウェア互換性ガイド』に必要なアーキテクチャとパッチをリストしています。
最新リリースの DPA アプリケーション サーバーの準備が完了した後、必要なすべてのソフトウェアをエージェント ホストにインストールします。	アプリケーションまたはデバイスをリモートでモニタリングしているときは、エージェント ホストに追加ソフトウェアをインストールする必要がある場合があります。たとえば、NetWorker をリモートで監視するためにエージェントを使用する場合、エージェント ホストに NetWorker クライアントをインストールする必要があります。詳細については、DPA での環境の検出 (155 ページ) を参照してください。
DNS が環境で有効にされていない場合、SharePoint サーバーの IP アドレスと FQDN を DPA アプリケーション サーバーのホスト ファイルに追加します。	DPA と SharePoint を統合するには、SharePoint にレポートを発行し、SharePoint ポートを構成できるように、IP アドレスと FQDN が必要です。SharePoint ポートは構成可能です。ポートが指定されていない場合、デフォルトのポートは 80 です。SharePoint の［設定］ダイアログ ボックスの［既存の URL］フィールドに入った標準的な URL を使用してポートを設定できます。詳細については、システム設定 (88 ページ) の SharePoint 設定テーブルを参照してください。
DPA サーバーで LDAP ユーザー認証を使用する場合は、構成に必要な情報を収集します。	LDAP ユーザー認証を構成するには次の情報が必要です。 • LDAP サーバー名/IP • SSL の使用有無 • LDAP サーバー ポート • LDAP のバージョン • ベース ディレクトリの識別名 • 識別属性

表 7 インストールと構成の概要 （続き）

アクション	コメント
DPA のバイナリをダウンロードして保存します。	DPA サーバーとエージェントのバイナリは、http://support.emc.com.の DPA ダウンロード セクションからダウンロードできます。 DPA サーバーおよびエージェントのバイナリをローカルに保存します。
DPA ライセンスの入手と保存	
インストールの間に簡単にアクセスできるように、必要なライセンス ファイルをローカル マシンに保存します。DPA のインストール ウィザードでは、ライセンスのインストール時にライセンス ファイルの参照を求められます。	プライマリ データストア サーバーの IP アドレスを知っている必要があります。 DPA ライセンスの取得、または使用可能で必要な DPA ライセンスの種類の詳細については、担当営業までお問い合わせください。
• 移行されていない新規インストールの場合：監視対象のすべてのコンポーネントの DPA ライセンスを取得します。 • 移行した 5.x インストールの場合：既存のライセンスが移行されます。 • DPA インスタンスで DPA の新機能と拡張された容量を利用するには、CLP ライセンスが必要です。容量の拡張が不要で、最新リリースの DPA の新しい機能に移行しない場合は、CLP ライセンスのインポートは不要です。DPA バージョン 5.x からバージョン DPA に移行する場合、既存ライセンスはご使用の構成およびデータとともに移行されます。容量の追加または既存の WLS ライセンスでの機能を変更しない場合、WLS ライセンスは、CLP ライセンスより前にインポートされた場合にのみ CLP ライセンスとの同時保有が可能になります。DPA での CLP ライセンスと WLS ライセンスの共存（74 ページ）で詳細を参照してください。	インストール後、DPA を管理するには DPA ライセンスが必要です。 DPA には 90 日間の評価版ライセンスがバンドルされています。この評価版ライセンスは DPA がインストールされた時点で作成され、最大で 90 日間使用可能で、すべての機能にアクセスできます。90 日間の評価期間中にライセンスをインポートすると、評価版ライセンスは削除され、インポートしたライセンスに基づいて DPA の機能にアクセスできます。 必要な DPA ライセンスや、DPA をインストールするためのライセンス購入については、担当営業までお問い合わせください。
Solutions Enabler（SE）ライセンスを用意します。	• Symmetrix ごとの HBA 単位に最小でもゲートキーパーが 1 個必要です。 • 1 個の Solutions Enabler ホストで、すべての VNX/CLARiX アレイの IP アドレスによる検出が可能です。VNX/CLARiX の検出の場合、DPA サーバー上に Solutions Enabler をインストールすることを推奨します。 • ストレージ アレイの検出に必要な Solutions Enabler のバージョンについては、『「ソフトウェア互換性ガイド」』を参照してください。
DPA のインストール	

表 7 インストールと構成の概要 （続き）

アクション	コメント
DPA ソフトウェアをインストールします。	インストール指示に従って、DPA サーバーとエージェントをインストールします。Datastore Service のインストール（30 ページ）、Application Service のインストール（32 ページ）および DPA エージェントのインストール（53 ページ）を参考にしてください。
ホスト アレイの検出および Solutions Enabler ホストの構成	
Symmetrix および VNX/CLARiX のアレイ検出の構成	レプリケーション解析用のストレージ アレイの構成（191 ページ）で詳細を参照してください。このセクションのステップは、レプリケーション分析のためにストレージ アレイ、データベース、または Microsoft Exchange Server を監視している場合にのみ適用されます。
Symmetrix または VNX/CLARiX のストレージ アレイを検出するために使用する Solutions Enabler ホストを用意します。	ストレージ アレイの検出に必要な Solutions Enabler のバージョン、および Solutions Enabler ホストにインストールする必要のあるソフトウェアについては、『「ソフトウェア互換性ガイド」』を参照してください。このホストは、SAN 接続による Symmetrix アレイへの接続が可能である必要があります。このホストは、VNX/CLARiX 接続用に TCP ポート 443 または 2163 が有効に設定されている必要があります。
データ保護モニタリングの環境の構成	
DPA エージェント ホストと監視対象のサーバーまたはデバイスとの間の必要なポートが開いていて、プロトコルを介した通信が可能であることを確認します。	DPA での通信設定（19 ページ）に、エージェントと監視対象のデバイスまたはサーバーとの間の通信に必要なプロトコルおよびデフォルトの DPA ポートを示します。
監視対象のデバイスまたはサーバーへの接続に使用する DPA 認証情報に不足がないことを確認するか、新しい認証情報の詳細を用意しておきます。	権限（17 ページ）に、DPA とともにインストールされる DPA 認証情報のデフォルト設定を示します。
RecoverPoint の監視をセットアップします（該当する場合）。	RecoverPoint のエージェント ホストおよびアプリケーション ホストの要件は、RecoverPoint の監視（191 ページ）に示されています。
アプリケーション ホストのインポートを検出および構成します（Microsoft Exchange またはデータベースを監視する場合）。	• リモート エージェントを使用してホストをインポートしている場合は、DPA サーバーがエージェント ホストを解決できる必要があります。 • エージェントなしでアプリケーション検出が実行中の場合は、レプリケーション解析の構成（189 ページ）を参考にしてください。
データ保護ポリシーの定義	
準拠していることを DPA が監視するポリシーの詳細を決めます。	レプリケーション分析の場合、データ保護ポリシーの詳細は次の内容で構成されます。 • レプリケーションのタイプ（SRDF/S、SRDF/A、MirrorView、RecoverPoint など）。

表 7 インストールと構成の概要　（続き）

アクション	コメント
	• レプリケーションをポイント イン タイムとするか、継続的とするか。 • レプリケーション ターゲットの宛先。 データ保護レポートに使用するポリシーは次のとおりです。 • チャージバック ポリシー：データ保護操作の財務コスト分析用。 • 保護ポリシー：RTO（Recovery Time Objective：目標復旧時間）および RPO（Recovery Point Objective：目標復旧時点）のデータ保護目標へのコンプライアンスを解析するため。 ポリシー（210 ページ）で詳細を参照してください。

第 2 章

DPA のインストール

この章は、次のセクションで構成されています。

- DPA サーバーのインストール 30
- DPA エージェントのインストール 53
- コマンド ラインを使用したインストール 56
- DPA インストール後の作業 61
- アップグレード 66

DPA サーバーのインストール

DPA サーバーのインストールには 2 つの段階があります。

1. Datastore Service のインストール
2. Application Service のインストール

クラスタリングを伴うインストールの詳細については、アプリケーションのクラスタリング（34 ページ）を参照してください。データストア レプリケーションを使用したインストールの詳細については、データストア レプリケーション（45 ページ）を参照してください。

データストア サービスの前にアプリケーション サービスをインストールすると、アプリケーション サービスのインストールが失敗します。インストール中に問題が発生した場合は、トラブルシューティング（243 ページ）を参照してください。

このセクションの処理手順は、新規インストールに適用できます。以前サポートされていた DPA から DPA18.1 にアップグレードし、バージョン 18.1 をインストールするには、「アップグレード」を参照してください。DPA のリリース ノートに、サポートされているアップグレードに関する情報が記載されています。

Linux インストール環境で UI の実行がサポートされている場合、DPA インストーラーは Windows と Linux で実行されます。次の手順で、Windows 64 ビット環境でのインストールについて説明します。

Datastore Service のインストール

この手順では、クラスタリングやデータストア レプリケーションを伴わない、通常のデータストア インストールを実装します。

はじめに

- 完全ローカル アクセスが可能なローカル管理者またはドメイン管理者としてログインします。
- UAC が Windows ホスト上で有効な場合、［管理者として実行］でインストーラーを起動します。
- インストール バイナリをサーバーまたはローカル マシンにコピーします。
- UNIX/Linux にインストールする場合は、root としてログインしていることを確認してください。特定の SU タイプのセキュリティ ソフトウェアを通じて root になった後にインストールすると、データストア サーバーに関する問題が発生する可能性があります。たとえば、`sesu` コマンドを使用した後などです。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- エージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。Linux IPv6 でインストールする場合、データストア サーバーの IPv6 インターフェイス ID も必要です。データストアのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、Linux エージェント マシンで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

```
fe80::9c9b:36f:2ab:d7a2%2
```

ここで%の前の値はアプリケーション サーバーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値はインターフェイス ID（この例では `2`）を示します。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションをアクティブ化します。［**Next**］をクリックします。
4. ［Installation Options］スクリーンで、データストア サービスのインストールを選択し、［**Next**］をクリックします。
5. 高度なインストールを実行しない場合、［**Next**］をクリックして、インストール ウィザードに従います。

   高度なインストールを実行する場合は、［Advanced Installation］スクリーンの［Show Advanced Installation Options］チェックボックスを選択し、［Next］をクリックして、インストール ウィザードに従います。

   ［Advanced Options］は次のとおりです。

   - ［**Do not register DPA services**］：オペレーティング システム マネージャーによってデータストア サービスが登録されないようにします。これにより、ホストの再起動後に、データストア サービスが開始されなくなります。サービスをオペレーティング システムにインストールするには、DPA コマンド ライン インターフェイスを使用する必要があります。
   - ［**Do not start DPA services**］：インストール後にデータストア サービスが開始されないようにします。サービスを開始するには、DPA コマンド ライン インタフェースを使用する必要があります。
   - ［**Install with advanced datastore layout**］：さまざまなディスクに分散された必須ファイル システムでデータストア サービスを構成し、パフォーマンスを最適化します。
6. 選択を求められたら、インストール フォルダーを選択します。

   デフォルトの場所を選択するか、別のフォルダーの場所を参照します。
7. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。

   インストールが実行されます。

   十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。
8. プロンプトが表示されたら、DPA アプリケーション サーバーからの接続をデータストアがリスンする IP アドレスを選択します。
9. プロンプトが表示されたら、ステップ 8 のデータストアを使用する DPA アプリケーション サーバーの IP アドレスを入力し、［**Add**］、［**Next**］の順にクリックします。
10. プロンプトが表示されたら、データストアのパスワードを指定します。

    データストアのパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
      - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
      - 1 つ以上の数字を含んでいること
      - 1 つ以上の特殊文字を含んでいること

- dpa datastore dspassword コマンドは、DPA データストアのパスワードをリセットするために使用できます。dpa datastore dspassword（144 ページ）で詳細を参照してください。

11. プロンプトが表示されたら、DPA エージェントのパスワードを指定します。

    エージェントのパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
        - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
        - 1 つ以上の数字を含んでいること
        - 1 つ以上の特殊文字を含んでいること
    - dpa agent --set-credentials コマンドは、DPA エージェントのパスワードをリセットするために使用できます。詳細は、dpa agent --set-credentials を参照してください。

12. DPA データストア サーバーのインストールが完了したら、［**Done**］をクリックします。

Application Service のインストール

この手順では、クラスタリングやデータストア レプリケーションを伴わない通常のインストール方法で、アプリケーション サービスを導入します。

はじめに

- DPA サーバーとエージェントとの間で安全に通信するには、`dpa app agentpwd` アプリケーション サーバー ホストで DPA CLI コマンドを使用し、エージェント登録パスワードを設定します。また、すべての DPA エージェント ホストで、このパスワードを設定する必要があります。詳細については、dpa application agentpwd を参照してください。次に、アプリケーション サービスを再起動します。このパスワードが、各エージェントに設定されていることを確認します。
- エージェント インストール バイナリを、サーバーまたはローカル マシンにコピーします。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- データストア サービス オプションがオンになっていること、およびデータストア サービスが稼働していることを確認します。
- Linux IPv6 で［Advanced Options］を指定してインストールする際、エージェントが別のアプリケーション サーバーまたはロードバランサーと通信する必要がある場合は、たとえばクラスタではエージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。アプリケーション サーバーのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、アプリケーション サーバーで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

```
fe80::9c9b:36f:2ab:d7a2%2
```

ここで、%の前の値は、エージェントが接続しようとしているアプリケーション サーバーまたはロードバランサーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値は、現在のアプリケーション サーバーのインターフェイス ID（この例では `2`）を示します。

- ESRS-VE をリモート トラブルシューティング（推奨）に使用する予定がある場合は、DPA をインストールする前に、ESRS-VE 環境をインストールし、構成しておく必要があります。ESRS-VE のインストールについての詳細は、EMC オンライン サポートの EMC セキュア リモート サービス ランディング ページ（https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition）を参照してください。

アプリケーション サービスのインストール処理は、データストア サービスのインストールと似ています。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションを有効化します。［**Next**］をクリックします。
4. ［Installation Options］画面で、アプリケーション サービスのインストールを選択し、［**Next**］をクリックします。
5. 高度なインストールを実行しない場合、［**Next**］をクリックして、インストール ウィザードに従います。

   ［Advanced Options］は次のとおりです。

   - ［**Do not register DPA services**］：オペレーティング システムのサービス マネージャーにサービスが登録されないようにします。このオプションを使用すると、ホストの再起動後に DPA サービスが開始されなくなります。
   - ［**Do not start DPA services**］：インストール後に DPA サービスが開始されないようにします。サービスを開始するには、DPA コマンド ライン インターフェイスを使用する必要があります。
   - ［**Install the DPA services as clusterable**］：存在する DPA クラスタを検出して参加するように DPA サービスを構成します。

     残りのインストールは、データストアのインストールと似ています。
6. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。インストールが実行されます。

   十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。

   注

   アプリケーション サーバーとデータストアの通信に必要なファイアウォールやデータストアが開いていない場合、データストア接続障害エラーが発生する可能性があります。詳細については、DPA での通信設定（19 ページ）を参照してください。

   ---

7. ［**Connect to Remote DPA Datastore**］のステップで、以前にインストールした DPA データストア サーバーの IP アドレスを入力します。

   インストールが再開されます。

8. プロンプトが表示されたら、DPA エージェントが通信する DPA アプリケーション サーバー ホストの名前または IP アドレスを指定します。デフォルトでは、エージェントは IP アドレス 127.0.0.1 のローカル アプリケーション サーバーと通信します。クラスタ構成の場合は、アプリケーション サーバーの前に配置されたロード バランシング スイッチの IP アドレスを指定します。［**Next**］をクリックします。

DPA アプリケーション サービスのインストールが完了しました。

9. プロンプトが表示されたら、データストアのパスワードを指定します。

   データストアのパスワードに関して次の点に注意してください。

   - 空白のパスワードはサポートされていません。
   - 最小文字数は、9 文字です。
   - 必須条件は次のとおりです。
     - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
     - 1 つ以上の数字を含んでいること
     - 1 つ以上の特殊文字を含んでいること
   - dpa application dspassword は、DPA データストアのパスワードを設定します。dpa application dspassword（137 ページ）で詳細を参照してください。

10. プロンプトが表示されたら、管理者のパスワードを指定します。

    管理者のパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
      - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
      - 1 つ以上の数字を含んでいること
      - 1 つ以上の特殊文字を含んでいること
    - dpa app adminpassword コマンドを使用すると、DPA データストア サービスの稼働中に DPA 管理者のパスワードをリセットし、DPA 管理者アカウントを有効にすることができます。詳細については、dpa application adminpassword（134 ページ）を参照してください。

11. ［**Done**］をクリックします。

    インストールが完了したら、DPA サーバーを起動し、サーバーのライセンスを取得します。DPA インストール後の作業（61 ページ）で詳細を参照してください。

アプリケーションのクラスタリング

DPA は、1 台の DPA データストア サーバーで稼働する複数の DPA アプリケーション サーバーにより、クラスタ化された構成で設定できます。クラスタリングにより、アプリケーション サーバーを動的に開始し、他のアプリケーション サーバーと作業負荷をシェアして、需要が減少したときに停止する機能が得られます。

クラスタ化されたアプリケーション サーバーには、次のような多数のメリットがあります。

- 復元性の向上
- ユーザーが提供するロード バランシング スイッチの背後に配置されたとき、作業負荷のロード バランシング
- DPA の導入を迅速に拡張する機能
- 柔軟な、環境に配慮したリソース管理
- 単一障害点の削減

複数のアプリケーション サーバーがクラスタとして構成されたら、月末のレポート作成やその他の使用量の多い期間に対応して追加のサーバーの電源をオンにするなど、負荷に基づいて、個々のアプリケーション サーバーを開始および終了できます。稼働中のクラスタに新しいサーバーを追加して、負荷の影響を受けたパフォーマンスを改善できます。

すべてのクラスタ ノードが同じ IP タイプの IP アドレス指定（IPv4 アドレスまたは IPv6 アドレス）を使用していることを確認します。

以下のようにアプリケーション クラスタリングを構成できます。

- 新規インストールでは、クラスタリングを伴うマスター アプリケーション サービスのインストール（38 ページ）とクラスタリングを伴うスレーブ アプリケーション サービスのインストール（42 ページ）が情報を提供します。
- アップグレード中は、既存のクラスタのアップグレード（69 ページ）とデータストア レプリケーションと既存のクラスタがある場合のアップグレード（71 ページ）が詳細情報を提供します。
- インストールや構成の後は、DPA 導入後にアプリケーション サーバーをクラスタに追加（121 ページ）が詳細情報を提供します。

クラスタリングの制限事項と推奨事項

クラスタを構成するときは、以下の制限事項と推奨事項に従います。

- DPA は 1 つのクラスタに最大で次の 4 つのノードをサポートします。
  - 1 つのマスター
  - 3 つのスレーブ
- アプリケーション サーバーの個々のクラスタは、固有の LAN/VLAN 上にある必要があります。
  - LAN のスパニングはできません。
  - クラスタリングは UDP ブロードキャスト ベースです。
- クラスタは LAN 経由でデータストアと通信できます。
- DPA アプリケーション サーバーのオブジェクト間のロードを管理するには、アプリケーション サーバー クラスタの前に物理ロード バランシング スイッチを配置する必要があります。ソフトウェア ロード バランシング スイッチの使用は推奨されません。
- DPA Web コンソールからアクセスできる構成は、データストアに保存され、クラスタ全体でアクセスできます。「dpa application プロモート」など dpa エグゼクティブ ユーティリティの使用が必要になる構成操作は、実行されるオブジェクトに対してローカルです。DPA 導入後にアプリケーション サーバーをクラスタに追加（121 ページ）および dpa application コマンド（134 ページ）には、dpa application promote コマンドに関する詳細情報が記載されています。
- アプリケーション サーバー クラスタリングを導入する場合は、すべてのクラスタ構成を完了してからアプリケーション サーバーで暗号化を有効にします。

データストア サービスのインストール

この手順には、ロード バランサー、データストア、マスター アプリケーション サーバーと 1 つ以上のスレーブ アプリケーション サーバーを使用したクラスタの導入が含まれています。

はじめに

- 完全ローカル アクセスが可能なローカル管理者またはドメイン管理者としてログインします。
- UAC が Windows ホスト上で有効な場合、［管理者として実行］でインストーラーを起動します。
- インストール バイナリをサーバーまたはローカル マシンにコピーします。

- UNIX/Linux にインストールする場合は、root としてログインしていることを確認してください。特定の SU タイプのセキュリティ ソフトウェアを通じて root になった後にインストールすると、データストア サーバーに関する問題が発生する可能性があります。たとえば、`sesu` コマンドを使用した後などです。
- UNIX/Linux にインストールする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- 必ずアプリケーション ノードの両方からアクセスできるように一般的なレポート用共有ディレクトリを作成します。たとえば、Windows クラスタの Datastore1 `\\WinClusterDS1\cluster_share` に作成します。共有ディレクトリは、DPA サービスを所有している ClusterApp1 と CulsterApp2 内のユーザーの読み取り/書き込み権限である必要があります。
- エージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。Linux IPv6 でインストールする場合、データストア サーバーの IPv6 インターフェイス ID も必要です。データストアのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、Linux エージェント マシンで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  ここで%の前の値はアプリケーション サーバーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値はインターフェイス ID（この例では `2`）を示します。
- すべてのマシンが vCenter 内の同一のネットワーク アダプタ上にあることを確認します。
- データストア レプリケーションをインストールする場合：
  - インストールの開始前に、最終導入トポロジーを計画します。ECN（EMC コミュニティ ネットワーク）に、導入の計画に関するガイダンスとベスト プラクティスが記載されている関連資料があります。
  - すべてのホストおよび IP アドレスを決定し、使用できるようにしておきます。
  - クラスタ化されたノードを含めて、すべてのデータストア サーバーまたはアプリケーション サーバーが同じ IP タイプの IP アドレス指定（IPv4 アドレスまたは IPv6 アドレス）を使用していることを確認します。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションをアクティブ化します。［**Next**］をクリックします。
4. ［Installation Options］スクリーンで、データストア サービスのインストールを選択し、［**Next**］をクリックします。
5. 高度なインストールを実行しない場合、［**Next**］をクリックして、インストール ウィザードに従います。

   高度なインストールを実行する場合は、［Advanced Installation］スクリーンの［Show Advanced Installation Options］チェックボックスを選択し、［Next］をクリックして、インストール ウィザードに従います。

［Advanced Options］は次のとおりです。

- ［**Do not register DPA services**］：オペレーティング システム マネージャーによってデータストア サービスが登録されないようにします。これにより、ホストの再起動後に、データストア サービスが開始されなくなります。サービスをオペレーティング システムにインストールするには、DPA コマンド ライン インターフェイスを使用する必要があります。
- ［**Do not start DPA services**］：インストール後にデータストア サービスが開始されないようにします。サービスを開始するには、DPA コマンド ライン インタフェースを使用する必要があります。
- ［**Install with advanced datastore layout**］：さまざまなディスクに分散された必須ファイル システムでデータストア サービスを構成し、パフォーマンスを最適化します。

  ［Advanced Installation Options］を選択すると、インストーラで後から、このサーバーのデータストア レプリケーションの構成やレプリケーションの役割の選択も行うことができます。

6. 選択を求められたら、インストール フォルダーを選択します。

   デフォルトの場所を選択するか、別のフォルダーの場所を参照します。

7. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。

   インストールが実行されます。

   十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。

8. ［**Datastore Listening Addresses**］ウィンドウで、DPA アプリケーション サービスからの接続をデータストア サービスがリスンする IP アドレスを指定します。
9. ［**Configure Datastore Access**］ウィンドウで、データストアを使用する DPA アプリケーション サーバーの IP アドレスを入力し、［**Add**］、［**Next**］の順にクリックします。

   クラスタ構成では各 DPA アプリケーション サーバーの IP アドレスを入力します。

10. ［**Datastore Agent Address**］ウィンドウで、ロード バランサー IP アドレスとなる、データストア エージェントの代替アドレスを入力します。
11. データストア レプリケーションを構成する場合は、［**Enable datastore replication**］>［を選択し、このサーバーのレプリケーションの役割］ > ［**SLAVE**］を選択します。［次へ］をクリックします。

    a. マスター データストア サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。

    b. ［**Configure Agent**］ウィンドウで入力を求められたら、インストールした DPA エージェントが通信する必要がある DPA アプリケーション サービスの完全修飾ドメイン名または IP アドレスを入力します。

       デフォルトでは、エージェントはウィザードで前に指定したアプリケーション サーバーと通信します。

    c. Linux IPv6 環境で使用している場合は、次の形式でのロードバランサーの完全修飾ドメイン名または IP アドレスを入力します。`IPV6Address%Interface_Id`

       ［**Next**］をクリックします。

12. プロンプトが表示されたら、データストアのパスワードを指定します。

    データストアのパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。

- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること
- dpa datastore dspassword コマンドは、DPA データストアのパスワードをリセットするために使用できます。dpa datastore dspassword（144 ページ）で詳細を参照してください。

13. DPA データストア サーバーのインストールが完了したら、［**Done**］をクリックします。
14. コマンド プロンプトで `dpa svc status` コマンドを実行し、データストア サービスが実行中であることを確認します。
15. すべてのデータストア ノードにデータベース接続プールのサイズを設定します。コマンド：

    `# dpa ds tune --connections xxx <RAM>GB`（ここで **xxx** はアプリケーション サーバーあたり約 250 となり、RAM は RAM の容量を示します。たとえば、2 ノード クラスタでは、**xxx** に 500 という数字を設定します）。

    クラスタでデータストア レプリケーションが有効化されている場合は、すべてのデータストア スレーブに対してこのコマンドを実行します。

クラスタリングを伴うマスター アプリケーション サービスのインストール

はじめに

- インストール バイナリをサーバーまたはローカル マシンにコピーします。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- データストア サービスが稼働中であることを確認します。
- UNIX/Linux にインストールする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- Linux IPv6 で［Advanced Options］を指定してインストールする際、エージェントが別のアプリケーション サーバーまたはロードバランサーと通信する必要がある場合は、たとえばクラスタではエージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。アプリケーション サーバーのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、アプリケーション サーバーで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  ここで、%の前の値は、エージェントが接続しようとしているアプリケーション サーバーまたはロードバランサーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値は、現在のアプリケーション サーバーのインターフェイス ID（この例では `2`）を示します。
- インストールの開始前に、最終導入トポロジーを計画します。ECN（EMC コミュニティ ネットワーク）に、導入の計画に関するガイダンスとベスト プラクティスが記載されている関連資料があります。

- すべてのホストおよび IP アドレスを決定し、使用できるようにしておきます。これには、アプリケーション サーバーの前に配置するロード バランシング スイッチに構成されている IP アドレスを含みます。
- すべてのクラスタ ノードが同じ IP タイプの IP アドレス指定（IPv4 アドレスまたは IPv6 アドレス）を使用していることを確認します。
- すべてのノードで共有される共通のディレクトリを指定します。これは、DPA アプリケーション ノードで生成されたレポートが格納される場所です。
- アプリケーション サーバー クラスタリングを UNIX にインストールする場合は、UNIX の NFS または CIFS ネットワーク共有に割り当てられたローカル ディレクトリに対する共通の共有ディレクトリを指定してください。
  - クラスタ内のすべてのアプリケーション ノードに、同じ UID および GID を持つユーザー名を作成してください。インストール時には、有効な UNIX ユーザー名とパスワードでログオンするように求められます。ftpuser や bin などのシステム ユーザー名は使用できません。
  - 指定した共有ディレクトリに対する読み取りおよび書き込みアクセス権を持っていることを確認してください。
  - パスがネットワーク共有に関連づけられているかどうかを確認してください。
- アプリケーション サーバー クラスタリングを Windows にインストールする場合は、共通の共有ディレクトリを UNC（Windows の汎用命名規則）パスとして指定してください。
  - 指定したパスを必ず確認します。
  - ユーザー アカウント（ユーザー名とパスワード）に対して、前のステップで指定した共有の読み取りおよび書き込みアクセス権を構成および付与します。このユーザー アカウントに対して、Windows の［サービスとしてログオン］のアクセス権限が有効化されている必要があります。
- ESRS-VE をリモート トラブルシューティング（推奨）に使用する予定がある場合は、DPA をインストールする前に、ESRS-VE 環境をインストールし、構成しておく必要があります。ESRS-VE のインストールについての詳細は、EMC オンライン サポートの EMC セキュア リモート サービス ランディング ページ（https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition）を参照してください。

アプリケーション サービスのインストール処理は、データストア サービスのインストールと似ています。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションを有効化します。［**Next**］をクリックします。
4. ［Installation Options］画面で、アプリケーション サービスのインストールを選択し、［**Next**］をクリックします。
5. ［**Show Advanced Installation Options**］が有効であることを確認し、［**Next**］をクリックします。

   ［Advanced Options］は次のとおりです。

   - ［**Do not register DPA services**］：オペレーティング システムのサービス マネージャーにサービスが登録されないようにします。このオプションを使用すると、ホストの再起動後に DPA サービスが開始されなくなります。

- ［**Do not start DPA services**］：インストール後に DPA サービスが開始されないようにします。サービスを開始するには、DPA コマンド ライン インターフェイスを使用する必要があります。
- ［**Install the DPA services as clusterable**］：存在する DPA クラスタを検出して参加するように DPA サービスを構成します。

  クラスタにアプリケーション オブジェクトを追加する場合、［Install the DPA services as clusterable］を選択し、ウィザードの手順に従います。

  アプリケーション サーバーのレポートに使用する共通の場所を入力するように求められたら、すべてのノードで共有されている共通のディレクトリを指定します。複数のアプリケーション ノードを実行している場合、レポートの共有ディレクトリは必ず指定する必要があります。

  UNIX にインストールする場合、「はじめに」で指定した共有に対する読み取りおよび書き込みアクセス権を持った、有効なユーザーを表すユーザー アカウントのユーザー名を指定するようインストーラーで求められます。

  Windows にインストールする場合、必要な共通および共有の UNC フォルダーを構成し、指定したそのディレクトリへのアクセス権を持ったドメインのユーザー名とパスワードを入力します。詳細については、「はじめに」を参照してください。

  残りのインストールは、データストアのインストールと似ています。

6. ［**Application Advanced Options**］ウィンドウで［**Install the DPA services as clusterable**］が有効であることを確認し、［**Next**］をクリックします。
7. ［Identify the DPA Datastore to connect to］ウィンドウでデータストアの IP アドレスを指定し、［**Next**］をクリックします。
8. ［**Application Cluster Address**］ウィンドウで、アプリケーション サーバーがリスンする IP アドレスを選択し、［**Next**］をクリックします。
9. ［**Application Cluster Options**］ウィンドウで、アプリケーションの役割としてドロップダウンメニューから［**Master**］を選択し、［**Next**］をクリックします。
10. ［**Choose a Folder**］ウィンドウで、レポートに使用する共有フォルダーを指定し、［**Next**］をクリックします。
11. ［**Usernamer**］ウィンドウで、DPA サービスの所有者となったユーザーのユーザー名とパスワードを指定します。［**Next**］をクリックします

    ステップ 11 で指定した共有フォルダーの読み取り権限と書き込み権限がこのユーザーに付与されていることを確認します。

    ドメインの場合、ユーザー名は必ず<Domain\User>の形式にします。ドメイン以外の場合、ユーザー名は<HOSTNAME\User>の形式にします。
12. ［**Enter Alternative Agent Address**］ウィンドウで、ロード バランサーの IP アドレスとして別のエージェントのアドレスを指定し、［**Next**］をクリックします。
13. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。インストールが実行されます。

    十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。

注

アプリケーション サーバーとデータストアの通信に必要なファイアウォールやデータストアが開いていない場合、データストア接続障害エラーが発生する可能性があります。詳細については、DPA での通信設定（19 ページ）を参照してください。

---

14. ［**Connect to Remote DPA Datastore**］のステップで、以前にインストールした DPA データストア サーバーの IP アドレスを入力します。

    インストールが再開されます。

15. プロンプトが表示されたら、データストアのパスワードを指定します。

    データストアのパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
        - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
        - 1 つ以上の数字を含んでいること
        - 1 つ以上の特殊文字を含んでいること
    - dpa datastore dspassword コマンドは、DPA データストアのパスワードをリセットするために使用できます。dpa datastore dspassword（144 ページ）で詳細を参照してください。

16. プロンプトが表示されたら、管理者のパスワードを指定します。

    管理者のパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
        - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
        - 1 つ以上の数字を含んでいること
        - 1 つ以上の特殊文字を含んでいること
    - dpa app adminpassword コマンドを使用すると、DPA データストア サービスの稼働中に DPA 管理者のパスワードをリセットし、DPA 管理者アカウントを有効にすることができます。詳細については、dpa application adminpassword（134 ページ）を参照してください。

17. ［**Done**］をクリックします。

    インストールが完了したら、DPA サーバーを起動し、サーバーのライセンスを取得します。詳細については、DPA インストール後の作業（61 ページ）を参照してください。

18. コマンド プロンプトで `dpa app con` コマンドを実行し、アプリケーション サーバーの構成を確認します。

    `dpa app con` コマンドの実行後はバインド アドレスが 0.0.0.0 に設定されています。DPA はあらゆる接続アドレスに対し、これを行います。

    この出力で、オペレーション モードがクラスタであり、クラスタの役割がマスターであることが示されます。

19. マルチキャスト アドレスをクラスタに追加する場合は、次の要領でクラスタをスタンドアロンにデモートしてからクラスタ ノードにプロモートします。

    クラスタにマルチキャスト アドレスを追加しない場合は、ステップ 19 に進みます。

    a. コマンド プロンプトで、`dpa app stop` コマンドを実行し、アプリケーション サーバーを停止させます。

b. `dpa app demote` コマンドを実行し、ノードをスタンドアロン ノードにデモートします。

c. `dpa app promote` コマンドを実行し、アプリケーションのノードをクラスタにプロモートします。バインド アドレス、マルチキャスト アドレス、共有フォルダーのパスを必ず組み込みます。役割も必ず指定します。

20. コマンド プロンプトで、`dpa app start` コマンドを実行し、アプリケーション サービスを開始します。

21. `server.log` ファイルの「`DPA master started successfully`」というメッセージでインストールと構成が正常に行われていることを確認します。

クラスタリングを伴うスレーブ アプリケーション サービスのインストール

はじめに

- インストール バイナリをサーバーまたはローカル マシンにコピーします。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- データストア サービスが稼働中であることを確認します。
- UNIX/Linux にインストールする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- Linux IPv6 で［Advanced Options］を指定してインストールする際、エージェントが別のアプリケーション サーバーまたはロードバランサーと通信する必要がある場合は、たとえばクラスタではエージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。アプリケーション サーバーのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、アプリケーション サーバーで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

```
fe80::9c9b:36f:2ab:d7a2%2
```

ここで、%の前の値は、エージェントが接続しようとしているアプリケーション サーバーまたはロードバランサーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値は、現在のアプリケーション サーバーのインターフェイス ID（この例では `2`）を示します。

- インストールの開始前に、最終導入トポロジーを計画します。ECN（EMC コミュニティ ネットワーク）に、導入の計画に関するガイダンスとベスト プラクティスが記載されている関連資料があります。
- すべてのホストおよび IP アドレスを決定し、使用できるようにしておきます。これには、アプリケーション サーバーの前に配置するロード バランシング スイッチに構成されている IP アドレスを含みます。
- すべてのクラスタ ノードが同じ IP タイプの IP アドレス指定（IPv4 アドレスまたは IPv6 アドレス）を使用していることを確認します。
- すべてのノードで共有される共通のディレクトリを指定します。これは、DPA アプリケーション ノードで生成されたレポートが格納される場所です。
- アプリケーション サーバー クラスタリングを UNIX にインストールする場合は、UNIX の NFS または CIFS ネットワーク共有に割り当てられたローカル ディレクトリに対する共通の共有ディレクトリを指定してください。
  - クラスタ内のすべてのアプリケーション ノードに、同じ UID および GID を持つユーザー名を作成してください。インストール時には、有効な UNIX ユーザー名とパスワードでログオンするように求められます。**ftpuser** や **bin** などのシステム ユーザー名は使用できません。

- 指定した共有ディレクトリに対する読み取りおよび書き込みアクセス権を持っていることを確認してください。
- パスがネットワーク共有に関連づけられているかどうかを確認してください。

- アプリケーション サーバー クラスタリングを Windows にインストールする場合は、共通の共有ディレクトリを UNC（Windows の汎用命名規則）パスとして指定してください。
  - 指定したパスを必ず確認します。
  - ユーザー アカウント（ユーザー名とパスワード）に対して、前のステップで指定した共有の読み取りおよび書き込みアクセス権を構成および付与します。このユーザー アカウントに対して、Windows の［サービスとしてログオン］のアクセス権限が有効化されている必要があります。
- ESRS-VE をリモート トラブルシューティング（推奨）に使用する予定がある場合は、DPA をインストールする前に、ESRS-VE 環境をインストールし、構成しておく必要があります。ESRS-VE のインストールについての詳細は、EMC オンライン サポートの EMC セキュア リモート サービス ランディング ページ（https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition）を参照してください。

アプリケーション サービスのインストール処理は、データストア サービスのインストールと似ています。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションを有効化します。［**Next**］をクリックします。
4. ［Installation Options］画面で、アプリケーション サービスのインストールを選択し、［**Next**］をクリックします。
5. ［**Show Advanced Installation Options**］が有効であることを確認し、［**Next**］をクリックします。

   ［Advanced Options］は次のとおりです。

   - ［**Do not register DPA services**］：オペレーティング システムのサービス マネージャーにサービスが登録されないようにします。このオプションを使用すると、ホストの再起動後に DPA サービスが開始されなくなります。
   - ［**Do not start DPA services**］：インストール後に DPA サービスが開始されないようにします。サービスを開始するには、DPA コマンド ライン インターフェイスを使用する必要があります。
   - ［**Install the DPA services as clusterable**］：存在する DPA クラスタを検出して参加するように DPA サービスを構成します。

     クラスタにアプリケーション オブジェクトを追加する場合、［Install the DPA services as clusterable］を選択し、ウィザードの手順に従います。

     アプリケーション サーバーのレポートに使用する共通の場所を入力するように求められたら、すべてのノードで共有されている共通のディレクトリを指定します。複数のアプリケーション ノードを実行している場合、レポートの共有ディレクトリは必ず指定する必要があります。

     UNIX にインストールする場合、「はじめに」で指定した共有に対する読み取りおよび書き込みアクセス権を持った、有効なユーザーを表すユーザー アカウントのユーザー名を指定するようインストーラーで求められます。

Windows にインストールする場合、必要な共通および共有の UNC フォルダーを構成し、指定したそのディレクトリへのアクセス権を持ったドメインのユーザー名とパスワードを入力します。詳細については、「はじめに」を参照してください。

残りのインストールは、データストアのインストールと似ています。

6. [**Application Advanced Options**] ウィンドウで [**Install the DPA services as clusterable**] が有効であることを確認し、[**Next**] をクリックします。
7. [Identify the DPA Datastore to connect to] ウィンドウでデータストアの IP アドレスを指定し、[**Next**] をクリックします。
8. [**Application Cluster Address**] ウィンドウで、アプリケーション サーバーがリスンする IP アドレスを選択し、[**Next**] をクリックします。
9. [**Application Cluster Options**] ウィンドウで、アプリケーションの役割としてドロップダウンメニューから [**Slave**] を選択し、[**Next**] をクリックします。
10. [**Application Cluster Option**] ウィンドウで、スレーブの通信相手となるマスター ノードの IP アドレスか FQDN を指定し、[**Next**] をクリックします。
11. [**Usernamer**] ウィンドウで、DPA サービスの所有者となったユーザーのユーザー名とパスワードを指定します。[**Next**] をクリックします

    ステップ 10 で指定した共有フォルダーの読み取り権限と書き込み権限がこのユーザーに付与されていることを確認します。

    ドメインの場合、ユーザー名は必ず<Domain\User>の形式にします。ドメイン以外の場合、ユーザー名は<HOSTNAME\User>の形式にします。
12. [**Enter Alternative Agent Address**] ウィンドウで、ロード バランサーの IP アドレスとなる別のエージェント アドレスを指定し、[**Next**] をクリックします。
13. プリインストール サマリーの、特にディスク領域情報を確認し、[**Install**] をクリックします。インストールが実行されます。

    十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。

    注

    アプリケーション サーバーとデータストアの通信に必要なファイアウォールやデータストアが開いていない場合、データストア接続障害エラーが発生する可能性があります。詳細については、DPA での通信設定（19 ページ）を参照してください。

    ---

14. [**Connect to Remote DPA Datastore**] のステップで、以前にインストールした DPA データストア サーバーの IP アドレスを入力します。

    インストールが再開されます。

15. プロンプトが表示されたら、データストアのパスワードを指定します。

    データストアのパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
      - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
      - 1 つ以上の数字を含んでいること

- 1 つ以上の特殊文字を含んでいること

- dpa datastore dspassword コマンドは、DPA データストアのパスワードをリセットするために使用できます。dpa datastore dspassword（144 ページ）で詳細を参照してください。

16. プロンプトが表示されたら、管理者のパスワードを指定します。

    管理者のパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
        - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
        - 1 つ以上の数字を含んでいること
        - 1 つ以上の特殊文字を含んでいること
    - dpa app adminpassword コマンドを使用すると、DPA データストア サービスの稼働中に DPA 管理者のパスワードをリセットし、DPA 管理者アカウントを有効にすることができます。詳細については、dpa application adminpassword（134 ページ）を参照してください。

17. ［**Done**］をクリックします。

    インストールが完了したら、DPA サーバーを起動し、サーバーのライセンスを取得します。詳細については、DPA インストール後の作業（61 ページ）を参照してください。

18. コマンド プロンプトで `dpa app con` コマンドを実行し、アプリケーション サーバーの構成を確認します。

    この出力で、オペレーション モードがクラスタであり、クラスタの役割がスレーブであることが示されます。

19. マルチキャスト アドレスをクラスタに追加する場合は、次の要領でクラスタをスタンドアロンにデモートしてからクラスタ ノードにプロモートします。

    クラスタにマルチキャスト アドレスを追加しない場合は、ステップ 19 に進みます。

    a. コマンド プロンプトで、`dpa app stop` コマンドを実行し、アプリケーション サーバーを停止させます。

    b. `dpa app demote` コマンドを実行し、ノードをスタンドアロン ノードにデモートします。

    c. `dpa app promote` コマンドを実行し、アプリケーションのノードをクラスタにプロモートします。バインド アドレス、マルチキャスト アドレス、共有フォルダーのパスを必ず組み込みます。必ず役割をスレーブに指定し、マスター ノードの IP アドレスも指定します。次に例を挙げます。

    `dpa app promote --bind 10.10.211.212 --multicast 210.1.2.33 --role SLAVE 10.10.211.213 --path \\WinClusterDS1\cluster_share`

20. コマンド プロンプトで、`dpa app start` コマンドを実行し、アプリケーション サービスを開始します。

21. `server.log` ファイルの「`DPA slave started successfully`」というメッセージでインストールと構成が正常に行われていることを確認します。

データストア レプリケーション

DPA データストア レプリケーションは、DPA でプライマリ データストア（Master）のレプリカ コピー（Slave）を維持して単一障害点に対する復旧性を実現することで、継続的、安全、信頼できるレ

プリケーションを有効化します。スレーブはカスケード方式で、必要に応じて標準のマスター スレーブ構成に追加できます。

マスター データストアに障害が発生すると、手動フェイルオーバー コマンドを使用してスレーブをマスターの役割に更新し、その後アプリケーション オブジェクトがこの新しいマスターを使用するように構成できます。再構成が有効になるまでには通常、DPA アプリケーションやデータストア サービスを起動する場合と同じくらいの時間がかかります。詳細はデータストア サーバーのフェイルオーバーの実行（127 ページ）で参照してください。

導入あたりのマスター データストア数は 1 個です。インストール時はすべてのデータストアがマスターです。スレーブ データストアとマスター データストアが通信できると、レプリケーションが有効になります。アプリケーション サーバーが起動されると、データのレプリケーションが開始されます。

データストア レプリケーションは、以下の要領で構成できます。

- 新規インストールでは、データストア レプリケーションを伴うマスター データストア サービスのインストールおよびデータストア レプリケーションを伴うスレーブ データストア サービスのインストールが情報を提供します。
- アップグレード中は、DPA 6.3 以降によるデータストア レプリケーションを使用したアップグレード（70 ページ）とデータストア レプリケーションと既存のクラスタがある場合のアップグレード（71 ページ）が情報を提供します。
- インストールや導入の後は、導入後のデータストア レプリケーションの構成（125 ページ）が詳細情報を提供します。

すべてのデータストア ノードで、同じ IP タイプの IP アドレス（IPv4 アドレスまたは IPv6 アドレス）が使用されるようにします。

データストア レプリケーションの構成

手順

1. インストール中またはインストール後に、スレーブ データストアを構成します。
2. インストール中またはインストール後に、マスター データストアを構成します。
3. アプリケーション サーバーをインストールします。すでにインストールされている場合は起動します。

データストア レプリケーションを伴うマスター データストア サービスのインストール

この手順では、データストア レプリケーションを実装しながらマスター データストア インストールを実装します。

はじめに

- 完全ローカル アクセスが可能なローカル管理者またはドメイン管理者としてログインします。
- UAC が Windows ホスト上で有効な場合、［管理者として実行］でインストーラーを起動します。
- インストール バイナリをサーバーまたはローカル マシンにコピーします。
- UNIX/Linux にインストールする場合は、root としてログインしていることを確認してください。特定の SU タイプのセキュリティ ソフトウェアを通じて root になった後にインストールすると、データストア サーバーに関する問題が発生する可能性があります。たとえば、`sesu` コマンドを使用した後などです。
- UNIX/Linux にインストールする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。

- エージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。Linux IPv6 でインストールする場合、データストア サーバーの IPv6 インターフェイス ID も必要です。データストアのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、Linux エージェント マシンで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  ここで%の前の値はアプリケーション サーバーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値はインターフェイス ID（この例では `2`）を示します。
- インストールの開始前に、データストア レプリケーションの最終導入トポロジーを計画します。ECN（EMC コミュニティ ネットワーク）に、導入の計画に関するガイダンスとベスト プラクティスが記載されている関連資料があります。
- すべてのホストおよび IP アドレスを決定し、使用できるようにしておきます。
- クラスタ化されたノードを含めて、すべてのデータストア サーバーまたはアプリケーション サーバーが同じ IP タイプの IP アドレス指定（IPv4 アドレスまたは IPv6 アドレス）を使用していることを確認します。
- 選択したアプリケーション サーバーが、マスター データストアが使用しているものと同一であることを確認します。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションをアクティブ化します。［**Next**］をクリックします。
4. ［Installation Options］スクリーンで、データストア サービスのインストールを選択し、［**Next**］をクリックします。
5. ［**Show Advanced Installation Options**］チェックボックスを［**Advanced Installation**］画面で選択し、［**Next**］をクリックします。
6. ［**Install with advanced datastore layout**］を選択し、［**Next**］をクリックします。
7. 選択を求められたら、インストール フォルダーを選択します。

   デフォルトの場所を選択するか、別のフォルダーの場所を参照します。
8. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。

   インストールが実行されます。

   十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。
9. ［**Datastore Listening Addresses**］ウィンドウで、DPA アプリケーション サービスからの接続をデータストア サービスがリスンする IP アドレスを指定します。
10. ［**Configure Datastore Access**］ウィンドウで、データストアを使用する DPA アプリケーション サーバーの IP アドレスを入力し、［**Add**］、［**Next**］の順にクリックします。

    クラスタ構成では各 DPA アプリケーション サーバーの IP アドレスを入力します。

11. ［**Datastore Agent Address**］ウィンドウで、ロード バランサー IP アドレスとなる、データストア エージェントの代替アドレスを入力します。
12. ［**Enable datastore replication**］ > ［を選択し、このサーバーのレプリケーションの役割として］ > ［**SLAVE**］を選択します。［**Next**］をクリックします。
    a. マスター データストア サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。
    b. ［**Configure Agent**］ウィンドウで入力を求められたら、インストールした DPA エージェントが通信する必要がある DPA アプリケーション サービスの完全修飾ドメイン名または IP アドレスを入力します。

       デフォルトでは、エージェントはウィザードで前に指定したアプリケーション サーバーと通信します。
    c. クラスタ化された DPA アプリケーション サーバーを使用する場合は、ロードバランサーの完全修飾ドメイン名/IP アドレスを入力します。アプリケーション サーバー/ロードバランサーの IPV6 アドレスを次の形式で入力します。**`IPV6Address%Interface_Id`**

       クラスタの場合およびクラスタ化された DPA アプリケーション サーバーまたは Linux IPv6 アプリケーション サーバーを使用する場合、IPV6%Interface_Id を手動で入力する必要があるため、完全修飾ドメイン名/IP アドレスのデフォルト値は空白です。その他すべての場合、完全修飾ドメイン名/IP アドレスとして、アプリケーション サーバーの IP アドレスのデフォルト値が自動的に入力されます。

       ［**Next**］をクリックします。
13. プロンプトが表示されたら、データストアのパスワードを指定します。

    データストアのパスワードに関して次の点に注意してください。
    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
      - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
      - 1 つ以上の数字を含んでいること
      - 1 つ以上の特殊文字を含んでいること
    - dpa datastore dspassword コマンドは、DPA データストアのパスワードをリセットするために使用できます。dpa datastore dspassword（144 ページ）で詳細を参照してください。
14. DPA データストア サーバーのインストールが完了したら、［**Done**］をクリックします。
15. コマンド プロンプトで `dpa svc status` コマンドを実行し、データストア サービスが実行中であることを確認します。
16. すべてのデータストア ノードにデータベース接続プールのサイズを設定します。コマンド：

    `# dpa ds tune --connections xxx <RAM>GB`（ここで xxx はアプリケーション サーバーあたり約 250 となり、RAM は RAM の容量を示します。たとえば、2 ノード クラスタでは、xxx に 500 という数字を設定します）。

    クラスタでデータストア レプリケーションが有効化されている場合は、すべてのデータストア スレーブに対してこのコマンドを実行します。

データストア レプリケーションを伴うスレーブ データストア サービスのインストール

この手順では、データストア レプリケーションを実装しながらスレーブ データストア インストールを実装します。

はじめに

- 完全ローカル アクセスが可能なローカル管理者またはドメイン管理者としてログインします。
- UAC が Windows ホスト上で有効な場合、［管理者として実行］でインストーラーを起動します。
- インストール バイナリをサーバーまたはローカル マシンにコピーします。
- UNIX/Linux にインストールする場合は、root としてログインしていることを確認してください。特定の SU タイプのセキュリティ ソフトウェアを通じて root になった後にインストールすると、データストア サーバーに関する問題が発生する可能性があります。たとえば、`sesu` コマンドを使用した後などです。
- UNIX/Linux にインストールする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- エージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。Linux IPv6 でインストールする場合、データストア サーバーの IPv6 インターフェイス ID も必要です。データストアのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、Linux エージェント マシンで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  ここで%の前の値はアプリケーション サーバーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値はインターフェイス ID（この例では `2`）を示します。
- インストールの開始前に、データストア レプリケーションの最終導入トポロジーを計画します。ECN（EMC コミュニティ ネットワーク）に、導入の計画に関するガイダンスとベスト プラクティスが記載されている関連資料があります。
- すべてのホストおよび IP アドレスを決定し、使用できるようにしておきます。
- クラスタ化されたノードを含めて、すべてのデータストア サーバーまたはアプリケーション サーバーが同じ IP タイプの IP アドレス指定（IPv4 アドレスまたは IPv6 アドレス）を使用していることを確認します。
- 選択したアプリケーション サーバーが、マスター データストアが使用しているものと同一であることを確認します。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションをアクティブ化します。［**Next**］をクリックします。
4. ［Installation Options］スクリーンで、データストア サービスのインストールを選択し、［**Next**］をクリックします。

5. ［**Show Advanced Installation Options**］チェックボックスを［**Advanced Installation**］画面で選択し、［**Next**］をクリックします。
6. ［**Install with advanced datastore layout**］を選択し、［**Next**］をクリックします。
7. 選択を求められたら、インストール フォルダーを選択します。

   デフォルトの場所を選択するか、別のフォルダーの場所を参照します。
8. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。

   インストールが実行されます。

   十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。
9. ［**Datastore Listening Addresses**］ウィンドウで、DPA アプリケーション サービスからの接続をデータストア サービスがリスンする IP アドレスを指定します。
10. ［**Configure Datastore Access**］ウィンドウで、データストアを使用する DPA アプリケーション サーバーの IP アドレスを入力し、［**Add**］、［**Next**］の順にクリックします。

    クラスタ構成では各 DPA アプリケーション サーバーの IP アドレスを入力します。
11. ［**Datastore Agent Address**］ウィンドウで、ロード バランサー IP アドレスとなる、データストア エージェントの代替アドレスを入力します。
12. ［**Enable datastore replication**］ > ［を選択し、このサーバーのレプリケーションの役割として］ > ［**SLAVE**］を選択します。［**Next**］をクリックします。
    a. マスター データストア サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。
    b. ［**Configure Agent**］ウィンドウで入力を求められたら、インストールした DPA エージェントが通信する必要がある DPA アプリケーション サービスの完全修飾ドメイン名または IP アドレスを入力します。

       デフォルトでは、エージェントはウィザードで前に指定したアプリケーション サーバーと通信します。
    c. クラスタ化された DPA アプリケーション サーバーを使用する場合は、ロードバランサーの完全修飾ドメイン名/IP アドレスを入力します。アプリケーション サーバー/ロードバランサーの IPV6 アドレスを次の形式で入力します。**`IPV6Address%Interface_Id`**

       クラスタの場合およびクラスタ化された DPA アプリケーション サーバーまたは Linux IPv6 アプリケーション サーバーを使用する場合、IPV6%Interface_Id を手動で入力する必要があるため、完全修飾ドメイン名/IP アドレスのデフォルト値は空白です。その他すべての場合、完全修飾ドメイン名/IP アドレスとして、アプリケーション サーバーの IP アドレスのデフォルト値が自動的に入力されます。

       ［**Next**］をクリックします。
13. DPA データストア サーバーのインストールが完了したら、［**Done**］をクリックします。
14. コマンド プロンプトで `dpa svc status` コマンドを実行し、データストア サービスが実行中であることを確認します。
15. すべてのデータストア ノードにデータベース接続プールのサイズを設定します。コマンド：

    `# dpa ds tune --connections xxx <RAM>GB`（ここで **xxx** はアプリケーション サーバーあたり約 250 となり、RAM は RAM の容量を示します。たとえば、2 ノード クラスタでは、**xxx** に 500 という数字を設定します）。

クラスタでデータストア レプリケーションが有効化されている場合は、すべてのデータストア スレーブに対してこのコマンドを実行します。

データストア レプリケーションを伴うアプリケーション サービスのインストール

アプリケーション サービスのインストールには、完全性を維持するためにこのインストール手順が含まれています。データストア レプリケーションには、アプリケーション サービスを実装する特別な方法はありません。

はじめに

- インストール バイナリをサーバーまたはローカル マシンにコピーします。
- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- データストア サービス オプションがオンになっていること、およびデータストア サービスが稼働していることを確認します。
- UNIX/Linux にインストールする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- Linux IPv6 で［Advanced Options］を指定してインストールする際、エージェントが別のアプリケーション サーバーまたはロードバランサーと通信する必要がある場合は、たとえばクラスタではエージェントが通信するアプリケーション サーバーの IP アドレスが分かっていることを確認してください。アプリケーション サーバーのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、アプリケーション サーバーで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  ここで、%の前の値は、エージェントが接続しようとしているアプリケーション サーバーまたはロードバランサーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値は、現在のアプリケーション サーバーのインターフェイス ID（この例では `2`）を示します。
- ESRS-VE をリモート トラブルシューティング（推奨）に使用する予定がある場合は、DPA をインストールする前に、ESRS-VE 環境をインストールし、構成しておく必要があります。ESRS-VE のインストールについての詳細は、EMC オンライン サポートの EMC セキュア リモート サービス ランディング ページ（https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition）を参照してください。

アプリケーション サービスのインストール処理は、データストア サービスのインストールと似ています。

手順

1. DPA サーバーのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。契約書の末尾までスクロールし、使用許諾契約書の条項に同意するオプションを有効化します。［**Next**］をクリックします。
4. ［**Installation Options**］画面で、アプリケーション サービスのインストールを選択し、［**Next**］をクリックします。
5. 高度なインストールを実行しない場合、［**Next**］をクリックして、インストール ウィザードに従います。

6. プリインストール サマリーの、特にディスク領域情報を確認し、［**Install**］をクリックします。インストールが実行されます。

   十分なディスク領域がない場合は、インストールをキャンセルするか、DPA のインストール先として別のドライブを選択します。

   注

   アプリケーション サーバーとデータストアの通信に必要なファイアウォールやデータストアが開いていない場合、データストア接続障害エラーが発生する可能性があります。詳細については、DPA での通信設定（19 ページ）を参照してください。

7. ［**Connect to Remote DPA Datastore**］のステップで、以前にインストールした DPA マスター データストア サーバーの IP アドレスを入力します。

   インストールが再開されます。

8. プロンプトが表示されたら、DPA エージェントが通信する DPA アプリケーション サーバー ホストの名前または IP アドレスを指定します。デフォルトでは、エージェントは IP アドレス 127.0.0.1 のローカル アプリケーション サーバーと通信します。クラスタ構成の場合は、アプリケーション サーバーの前に配置されたロード バランシング スイッチの IP アドレスを指定します。［**Next**］をクリックします。

   DPA アプリケーション サービスのインストールが完了しました。

9. プロンプトが表示されたら、データストアのパスワードを指定します。

   データストアのパスワードに関して次の点に注意してください。

   - 空白のパスワードはサポートされていません。
   - 最小文字数は、9 文字です。
   - 必須条件は次のとおりです。
     - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
     - 1 つ以上の数字を含んでいること
     - 1 つ以上の特殊文字を含んでいること
   - dpa datastore dspassword コマンドは、DPA データストアのパスワードをリセットするために使用できます。dpa datastore dspassword（144 ページ）で詳細を参照してください。

10. 管理者のパスワードを設定します。

    管理者のパスワードに関して次の点に注意してください。

    - 空白のパスワードはサポートされていません。
    - 最小文字数は、9 文字です。
    - 必須条件は次のとおりです。
      - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
      - 1 つ以上の数字を含んでいること
      - 1 つ以上の特殊文字を含んでいること
    - dpa app adminpassword コマンドを使用すると、DPA データストア サービスの稼働中に DPA 管理者のパスワードをリセットし、DPA 管理者アカウントを有効にすることができます。詳細については、dpa application adminpassword（134 ページ）を参照してください。

11. ［**Done**］をクリックします。

    インストールが完了したら、DPA サーバーを起動し、サーバーのライセンスを取得します。詳細については、DPA インストール後の作業（61 ページ）を参照してください。

データストア レプリケーションのベスト プラクティス

データストア レプリケーションでは、次のベスト プラクティスに従います。

- マスター データストアとスレーブ データストア間の役割が変更された場合は、必ずデータストア サービスを再開する必要があります。
- レプリケーション構成コマンド **dpa ds rep** を使用して、レプリケーションのステータスを確認します。マスター データストアで **dpa ds rep** コマンドを実行すると、レプリケーションがストリーミングされているか、何がスレーブ データストアであるかが表示されます。スレーブ データストアでこのコマンドを実行すると、何がマスター データストアであるかが表示されます。
- データストアをエクスポートする前に、データストア ファイル セットのエクスポート先となる空のディレクトリを必ずデータストアに作成します。たとえば、**/tmp/export** などです。
- マスター データストアとスレーブ データストアのパフォーマンス仕様は同じであり、同じバージョンの DPA にインストールする必要があります。

DPA エージェントのインストール

このセクションでは、エージェント専用インストール パッケージを使用して DPA エージェントをインストールする方法について説明します。これは、新規インストールに適用できます。

エージェントは DPA アプリケーション サーバーとデータストア サーバーに自動的にインストールされます。したがって、DPA サーバーではこの手続きを実行しないでください。以前の DPA サービス パックから DPA18.1 にアップグレードし、最新バージョンの DPA18.1 をインストールするには、「アップグレード」を参照してください。

DPA エージェントのインストール

次の手順では、Windows 環境での DPA エージェントのインストールについて説明します。

はじめに

- ポートが DPA サーバー間の通信用に開かれているか無効化されているかを確認します。詳細については、インストールと構成の概要（22 ページ）を参照してください。
- エージェントが通信する DPA アプリケーション サーバーの IP アドレスが分かっていることを確認してください。Linux IPv6 でインストールする場合、エージェントの IPv6 インターフェイス ID も必要です。エージェントのインストールの［**Configure Agent**］ウィンドウで、この情報の入力を求められます。IPv6 インターフェイス ID を取得するには、Linux エージェント マシンで `ip addr show` コマンドを実行し、出力結果を使用して IPv6 インターフェイス ID を見つけます。次に例を挙げます。

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  ここで**%**の前の値は DPA アプリケーション サーバーの IPv6（この例では `fe80::9c9b:36f:2ab:d7a2`）を示し、後ろの値はエージェントのインターフェイス ID（この例では `2`）を示します。

手順

1. DPA エージェントのバイナリをダブル クリックしてインストールを開始します。
2. ［**Next**］をクリックします。
3. ［End User License Agreement］を読んで、同意します。［**Next**］をクリックします。
4. インストール フォルダーを選択して［**Next**］をクリックします。
5. プリインストール サマリーを確認して［**Install**］をクリックします。
6. エージェント インストール オプションを選択します。
   - ［**Do not start DPA Agent service**］: このオプションにより、インストール後に DPA エージェント サービスが開始されません。

     このオプションを選択する場合、コマンド ラインから DPA エージェントを手動で開始する必要があります。

     ［Do not start DPA Agent service］を選択した場合は［**Next**］をクリックします。

     DPA エージェントと通信する DPA サーバーの完全修飾ドメイン名または IP アドレスを入力します。
   - ［エージェントは **Oracle Database** の監視に使用されます。］DPA エージェントを使用して Oracle Database を監視するには、このオプションを選択します。

     このオプションを選択した場合は、DPA エージェントが Oracle Database のデバイス ドライバ ファイルを見つけることができるディレクトリを参照します。
7. ［**Next**］をクリックします。
8. ［**Configure Agent**］ウィンドウで、DPA エージェントと通信する DPA アプリケーション サーバーの完全修飾ドメイン名または IP アドレスを入力します。

   Linux IPv6 でインストールし、Linux エージェントをインストールする場合、Linux エージェントの IPv6 インターフェイス ID を入力します。

   ［**Next**］をクリックします。
9. DPA データストアのインストール時に設定したものと同じエージェント パスワードを設定します。

   エージェントのパスワードに関して次の点に注意してください。
   - 空白のパスワードはサポートされていません。
   - 最小文字数は、9 文字です。
   - 必須条件は次のとおりです。
     - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
     - 1 つ以上の数字を含んでいること
     - 1 つ以上の特殊文字を含んでいること
10. ［**Done**］をクリックしてインストールを完了します。
11. エージェント サービスを再起動します。

必要条件

DPA Agent 登録パスワードの設定（55 ページ）の手順に従って操作します。

DPA Agent 登録パスワードの設定

DPA Agent をインストールしたら、パスワードを設定します。

手順

1. **`dpaagent --set-credentials`** を実行し、DPA Agent パスワードを設定します。

   コマンドの詳細については、「dpaagent --set-credentials」を参照してください。

バックアップ アプリケーション データをさかのぼって収集するように DPA バージョン 18.1 エージェントを構成する

デフォルトでは、新しくインストールされた DPA エージェントは、現在の日付と時刻からバックアップ アプリケーション データの収集を開始します。監査またはその他の理由により、過去数日内の失敗したバックアップのアラートを確認する場合、または何らかの理由により数日分のバックアップ アプリケーション データを収集する場合、ユーザーが定義した時間数に従ってデータを収集するように、新しくインストールした DPA エージェントを構成できます。

はじめに

この手順では、DPA18.1 以降がインストールされている必要があります。

Linux の場合

手順

1. DPA エージェントのインストール ただし、DPA エージェントは起動しないでください。
2. 次の 2 行を `dpa.config` ファイルに追加します。

   `VARIABLE_NAME=NUMBER_OF_BACKUP_HOURS`

   `export VARIABLE_NAME`

   ここで、VARIABLE_NAME は、各バックアップ アプリケーションで次のようになります。

   NetWorker：AGENT_NSR_JOB_STARTTIME

   Avamar：AGENT_AXION_JOB_STARTTIME

   TSM：AGENT_TSM_JOB_STARTTIME

   HPDP：AGENT_DP_JOB_STARTTIME

   CommVault：AGENT_CV_JOB_STARTTIME

   NetBackup：AGENT_NB_JOB_STARTTIME

   ArcServe：AGENT_AS_JOB_STARTTIME

   DB2：AGENT_DB2_JOB_STARTTIME

   SAP HANA：AGENT_SAP_HANA_JOB_STARTTIME

   RMAN：AGENT_RMAN_JOB_STARTTIME

   MSSQL：AGENT_MSSQLDB_JOB_STARTTIME

   NUMBER_OF_BACKUP_HOURS は、現在の時間からさかのぼるバックアップ時間数です。

たとえば、dpa.config の次の 2 行により、DPA エージェントは 14 日前のデータから収集を開始するようになります。

```
AGENT_AXION_JOB_STARTTIME=336
export AGENT_AXION_JOB_STARTTIME
```

3. DPA エージェントを起動します。

Windows の場合

手順

1. 次の情報を使用して、システム レジストリ キーをレジストリ パス HKEY_LOCAL_MACHINE\SOFTWARE\emc\DPA\AGENT にエクスポートします。

   VARIABLE_NAME=NUMBER_OF_BACKUP_HOURS

   ここで、VARIABLE_NAME は、各バックアップ アプリケーションで次のようになります。

   NetWorker：NSR_JOB_STARTTIME

   Avamar：AXION_JOB_STARTTIME

   TSM：TSM_JOB_STARTTIME

   HPDP：DP_JOB_STARTTIME

   CommVault：CV_JOB_STARTTIME

   NetBackup：NB_JOB_STARTTIME

   ArcServe：AS_JOB_STARTTIME

   DB2：DB2_JOB_STARTTIME

   SAP HANA：SAP_HANA_JOB_STARTTIME

   RMAN：RMAN_JOB_STARTTIME

   MSSQL：MSSQLDB_JOB_STARTTIME

   NUMBER_OF_BACKUP_HOURS は、現在の時間からさかのぼるバックアップ時間数です。

   たとえば、 avamar.reg ファイルの内容として次の 3 行を追加し、それを cmd から起動してレジストリにエクスポートすると、DPA エージェントは 14 日前の NetWorker のデータから収集を開始するようになります。

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\emc\DPA\AGENT]

   NSR_JOB_STARTTIME="336"
   ```

2. DPA エージェントをインストールして起動します。

コマンド ラインを使用したインストール

適切なコマンド ラインを使用します。

はじめに

DPA をいずれかの UNIX OS にインストールする場合は、`chmod 755` コマンドを実行して、バイナリ実行権限を変更してください。

- Linux

```
DPA-<component>-Linux-<architecture>-<version>.xxx.install.bin
[option]
```

ここで、option は、表 7 でサイレントまたは対話型インストールに表示されているオプションのいずれかです。

次に例を挙げます。**DPA-Agent-Linux-x86_64-6.5.0.1.bin -i silent -DUSER_INSTALL_DIR="/opt/custom/emc/dpa"**

- AIX

```
./DPA-<component>-AIX-<architecture>-<version>.bin
```

次に例を挙げます。**./DPA-Agent-AIX-PPC64-6.5.0.1.bin**

- Windows

```
DPA-<component>-Windows-<architecture>-
<version>.xxx.install.exe [option]
```

ここで、option は、表 7 でサイレントまたは対話型インストールに表示されているオプションのいずれかです。

次に例を挙げます。**DPA-Agent-Windows-x86_64-6.5.0.1.exe -i silent -DUSER_INSTALL_DIR="C:\custom\emc\dpa"**

DPA インストール後の作業（61 ページ）にあるステップを必ず実行します。

表 8 インストーラー コマンド ライン オプション

オプション	説明
-?	オンライン ヘルプを表示します
-i [swing | console | silent]	インストーラのユーザー インタフェース モードを指定します。 swing：グラフィカル インターフェイス console：コンソールのみ silent：ユーザーとの対話操作なし
-D <name>="<value>"	コマンド ラインに設定して（-D オプションを使用）デフォルトのインストーラーの値を上書きするか、またはレスポンス ファイルに記載して-f オプションとともに使用できるインストーラーの名前と値のペアを示します。 値の前後に引用符を使用する必要があります。 例： -D<variable name>="<value>" ここで、

表 8 インストーラー コマンド ライン オプション （続き）

オプション	説明
	次に例を挙げます。**DPA-Agent-Linux-x86_64-6.5.0.1.bin -i silent -DPort="3740"** <variable name>と<value>の説明が以下の表に記載されています。

表 9 データストア インストーラーの変数

変数名	説明	指定可能な値	デフォルト値
USER_INSTALL_DIR	インストール先	有効なパス	Windows: C:\Program Files\EMC\DPA Linux: /opt/emc/dpa
CHOSEN_INSTALL_SET	インストール セット	DS	N/A
VAR_INSTALL_SERVICE	データストア サービスをインストールする詳細オプション	TRUE/FALSE	TRUE
VAR_START_SERVICE	データストア サービスを開始/停止する詳細オプション	TRUE/FALSE	TRUE
VAR_DATASTORE_DATA_LOCATION	パフォーマンス最適化のためにデータストア サーバーのデータ ディレクトリを指定する、データストア レイアウトの詳細オプション	有効なパス	$USER_INSTALL_DIR$\services\datastore\
VAR_DATASTORE_XLOG_LOCATION	パフォーマンス最適化のためにデータストア サーバーの Xlog ディレクトリを指定する、データストア レイアウトの詳細オプション	有効なパス	$USER_INSTALL_DIR$\services\datastore\data\
VAR_USERNAME（Linux のみ）	データストア サービスをインストールするための既存の UNIX ユーザー アカウントを指定する詳細オプション	既存のユーザー名	N/A
VAR_DATASTORE_BIND_ADDRESSES	Postgres がリスンする IP アドレス	有効な IP アドレス	N/A
VAR_DATASTORE_CLIENTS_ADDRESSES IPAddress of	データストア サービスに接続するアプリケーション サーバーの IP アドレス	「,」で区切った有効な IP アドレス	N/A
VAR_APOLLO_USER_PASSWORD	DPA データストアのパスワード	（インストール時に設定または DPA CLI を使用してリセット）	N/A

表 10 データストア詳細オプションのレプリケーション変数

変数名	説明	指定可能な値	デフォルト値
VAR_DATASTORE_REPLICATION	データストア レプリケーションのための役割	MASTER/SLAVE	N/A
VAR_DATASTORE_REPLICATION_	マスターまたはスレーブの IP アドレス。	マスターまたはスレーブの有効な IP アドレス	N/A

表 10 データストア詳細オプションのレプリケーション変数 （続き）

変数名	説明	指定可能な値	デフォルト値
	VAR_DATASTORE_REPLICATION_ROLE を「MASTER」と設定した場合、スレーブの IP アドレスを入力する必要があり、VAR_DATASTORE_REPLICATION_ROLE を「SLAVE」と設定した場合はマスターの IP アドレスを入力する必要があります。		

表 11 データストア エージェントの変数

変数名	説明	指定可能な値	デフォルト値
VAR_AGENT_APPLICATION_ADDRESS データストア エージェントを管理するための DPA サーバーの完全修飾ドメイン名または IP アドレス	データストア エージェントを管理するための DPA サーバーの完全修飾ドメイン名または IP アドレス Linux IPv6 の場合、<IPv6Address>%<Interface_Id_Of_Datastore_Agent>	有効な IP アドレスまたはホスト名	複数のアプリケーション サーバーがある場合およびデータストア サービスが Linux IPv6 アプリケーション サーバーと通信する場合、この値は空です。それ以外の場合、デフォルト値は VAR_DATASTORE_CLIENTS_ADDRESSES と同じになります。
VAR_AGENT_START_SERVICE	データストア エージェントをインストール後に開始/停止する詳細オプション	TRUE/FALSE	TRUE
VAR_AGENT_ORACLE_DIRECTORY	データストア エージェントによる Oracle の監視に使用される詳細オプション。Oracle Database のデバイス ドライバー ファイルがあるパス	有効なパス	N/A

表 12 アプリケーション インストーラーの変数

変数名	説明	指定可能な値	デフォルト値
USER_INSTALL_DIR	インストール先	有効なパス	Windows：C:\Program Files\EMC\DPA Linux：/opt/emc/dpa
CHOSEN_INSTALL_SET	インストール セット	アプリケーション	N/A
VAR_INSTALL_SERVICE	アプリケーション サービスをインストールする詳細オプション	TRUE/FALSE	TRUE
VAR_START_SERVICE	アプリケーション サービスをインストール後に開始/停止する詳細オプション	TRUE/FALSE	TRUE

表 12 アプリケーション インストーラーの変数 （続き）

変数名	説明	指定可能な値	デフォルト値
VAR_APPLICATION_DATASTORE_ADDRESS	データストア サーバーの IP アドレス	データストア サービスがインストールおよび実行されている有効な IP アドレス	N/A
VAR_ADMIN_PASSWORD	DPA アプリケーションの管理者パスワード	（インストール時に設定または DPA CLI を使用してリセット）	N/A
VAR_APOLLO_USER_PASSWORD	DPA データストアのパスワード	（インストール時に設定または DPA CLI を使用してリセット）	N/A

表 13 アプリケーション サーバー エージェントの変数

変数名	説明	指定可能な値	デフォルト値
VAR_AGENT_APPLICATION_ADDRESS	アプリケーション サーバーのエージェントを管理するための DPA サーバーの完全修飾ドメイン名または IP アドレス	有効な IP アドレスまたはホスト名	127.0.0.1
VAR_AGENT_START_SERVICE	アプリケーション サーバーのエージェントをインストール後に開始/停止する詳細オプション	TRUE/FALSE	TRUE
AVAR_AGENT_ORACLE_DIRECTORY	アプリケーション サーバーのエージェントによる Oracle の監視に使用される詳細オプション。 Oracle Database のデバイス ドライバー ファイルがあるパス	有効なパス	N/A

表 14 アプリケーション サーバー クラスタの詳細オプションの変数

変数名	説明	指定可能な値	デフォルト値
VAR_APPLICATION_ADDRESS	アプリケーション サーバーを他の DPA アプリケーション ノードに通知するためにアプリケーション サーバーによって使用される IP アドレス。	有効な IP アドレス	N/A
VAR_APPLICATION_CLUSTER_ROLE	クラスタ内のアプリケーション ノードの役割	MASTER/SLAVE	N/A
VAR_APPLICATION_MASTER_ADDRESS	VAR_APPLICATION_CLUSTER_ROLE="SLAVE"の場合は、この値を入力する必要があります。	有効な IP アドレス	N/A
VAR_APPLICATION_REPORT_DIRECTORY	ネットワーク共有レポート フォルダーのパス	有効なパス	N/A
VAR_APPLICATION_REPORT_USERNAME	共有レポート フォルダーに対するアクセス権限があり、アプリケーション サービスの所有者になるユーザー	Windows の場合、既存の DOMAIN\\Username UNIX の場合、既存のユーザー名	N/A

表 14 アプリケーション サーバー クラスタの詳細オプションの変数 （続き）

変数名	説明	指定可能な値	デフォルト値
VAR_APPLICATION_REPORT_PASSWORD（Windows のみ）	前述のユーザーのパスワード		N/A

表 15 スタンドアロン エージェント インストーラーの変数

変数名	説明	指定可能な値	デフォルト値
USER_INSTALL_DIR	インストール先	有効なパス	Windows：`C:\Program Files\EMC\DPA` Linux： `/opt/emc/dpa`
VAR_AGENT_APPLICATION_ADDRESS	このエージェントの有効な IP アドレスまたはホスト名を管理するための DPA サーバーの完全修飾ドメイン名または IP アドレス。	Linux IPv6 の場合、<IPv6Address>%<Interface_Id_Of_Agent>	N/A
VAR_AGENT_START_SERVICE	エージェントをインストール後に開始/停止する詳細オプション	TRUE/FALSE	TRUE
VAR_AGENT_ORACLE_DIRECTORY	Oracle の監視に使用される詳細オプション。Oracle Database のデバイス ドライバー ファイルがあるパス	有効なパス	N/A

DPA インストール後の作業

DPA をインストールまたはアップグレードして DPA Web コンソールにアクセスすると、DPA サーバーの初期化プロセスの状態を示すメッセージが表示されます。この初期化プロセスが完了するまでに 10 分ほどかかります。

初期化中、DPA によってデータベース スキーマ、テーブル、ビュー、DPA データストアが作成されます。また、さまざまなシステム レポートとダッシュボード テンプレート、デフォルトのシステム ユーザー、解析エンジン ルールセットや、その他さまざまなデフォルトおよび初期オブジェクトが作成されます。ネットワーク接続時間はこれらすべてのアクションが完了する速度に影響します。DPA のインストール後に、必ず次のステップを実行してください。

手順

1. DPA18.1 にアップグレードまたは移行した場合、DPA18.1 を使用する前に、ブラウザの参照履歴/キャッシュを削除します。
2. （オプション） 次のステップを実行して、初期化が進行中であるか完了しているかを確認します。
   a. Linux へのインストールで、デフォルト以外の場所にインストールした場合は、ログアウトしてセッションに戻ります。または、新しいログイン ウィンドウから実行してください。

      dpa.sh svc status を実行する前に実行コマンド パスを見つけるため、新しいシェルが必要です。

   b. DPA アプリケーション サーバーで、<install_dir>\services\applications に移動します。

c. *.rar、*.ear、*.war の各ファイルについて、*.deployed、*.isdeploying、.failed 拡張子を確認します。

- ファイルの拡張子が*.isdeploying である場合、サーバーの初期化が進行中です。
- ファイルの拡張子が*.deployed の場合はサーバーの初期化が完了しており、DPA Web コンソールにログインできます。
- ファイルの拡張子が*.failed である場合、サーバーの初期化が失敗しています。テクニカル サポートに問い合わせください。

3. Web コンソールを起動して DPA インストールの成功を確認します。

Web コンソールを起動するときは、すべての DPA サービスが実行されている必要があります。Web コンソールを起動するには、Web ブラウザーに Adobe Flash のプラグインが必要です。

a. ブラウザーを起動し、ポート 9002 で https を経由して DPA サーバーに接続します。必ずポップアップ ブロッカーをすべて無効にしてください。次に例を挙げます。

```
https://<server_name>:9002
```

ここで、server_name はサーバーまたは localhost の名前または IP アドレスです。

または、

```
https://<server_name>:9002/flexui url
```

を使用します（引き続き Flex ベースの DPA18.1 Web コンソールを使用する場合）。

b. ユーザー名とパスワードを入力します。ユーザー名とパスワード フィールドでは、大文字と小文字が区別されます。

c. [**Login**] をクリックします

4. DPA サーバーにライセンスを追加します。

DPA サーバーは、90 日間の一時ライセンスでインストールされます。

アップグレードしていても、容量を追加しない場合や、DPA18.1 の新機能に変更しない場合は、ライセンスの変更は必要ありません。

DPA インスタンスで DPA18.1 の新機能と拡張された容量を利用するには、CLP ライセンスが必要です。DPA のバージョン 5.x からバージョン DPA18.1 に移行する場合は、ご使用の構成やデータと一緒に既存ライセンスも移行されます。詳細については DPA での CLP ライセンスと WLS ライセンスの共存（74 ページ）を参照してください。

CLP ライセンスを追加する場合は、ファイル拡張子.lic のライセンス ファイルを選択してください。

WLS ライセンスを追加する場合は、ファイル拡張子.wls のライセンス ファイルを選択してください。

ライセンス ファイルをインストールした後、ライセンス ファイルを登録するために DPA Web コンソールを終了するように求められます。

5. DPA Web コンソールに再度ログインします。

6. （推奨）手順 4 で CLP ライセンスを追加した場合は、DPA アプリケーション サーバーを ESRS-VE に登録してください。登録することで、カスタマー サポートによる DPA インスタンスのサポートが有効になります。

   次の点に注意してください。

   - 以前に登録された ESRS をアップグレードする場合、その ESRS がすでに登録されていることを知らせる次のエラーが表示される可能性があります。
     ```
     [ERROR] This node is already registered with an EMC
     Secure Remote Support Service.
     ```
     その後、ESRS に、ホスト IP が使用できなくなっていることを知らせる以下のエラーが表示されます。
     ```
     [ERROR] This node failed to delete with EMC Secure
     Remote Support Service.
     ```
     ```
     Offline: Validation error
     ```
     詳細については、EMC ナレッジ ベース記事「xxxxxx」（http://www.support.emc.com で入手可能）を参照してください。これは環境の問題で、DPA とは無関係です。
   - 新規インストール後に ESRS を登録するには、ESRS-VE がインストール済みで、DPA アプリケーション サーバーからアクセスできる必要があります。ESRS-VE をリモート トラブルシューティング（推奨）に使用する予定がある場合は、DPA をインストールする前に、ESRS-VE 環境をインストールし、構成しておく必要があります。ESRS-VE のインストールについての詳細は、EMC オンライン サポートの EMC セキュア リモート サービス ランディング ページ（https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition）を参照してください。「Data Protection Advisor Software Compatibility Guide」に、サポートされている ESRS-VE モジュールとバージョン情報が記載されています。
   - 1 つのアプリケーション サービスを登録してください。登録には、DPA データストアとアプリケーション サーバーがともに含まれます。
   - クラスタ環境を使用している場合は、マスター アプリケーション サーバーを ESRS に登録してください。アプリケーション サーバーがマスターとスレーブのどちらのサーバーかを確認するには、`dpa app con` コマンドを使用します。詳細については、CLI のセクションを参照してください。
   - EMC Secure Remote Support のユーザー名とパスワードの入力を促されたら、EMC オンライン サポートの登録用認証情報を入力します。次に例を挙げます。

     ```
     dpa app support --register 10.11.110.111
     Dell EMC Data Protection Advisor
     Enter Data Protection Advisor Administrator username :
     Enter Data Protection Advisor Administrator password :
     Enter EMC Secure Remote Support username :
     Enter EMC Secure Remote Support password :
     ```
   - 次の点に注意してください。クラスタ環境では、ESRS に登録したアプリケーション サーバーを使用してスケジュール レポートを作成しないでください。リスナーのスケジュール レポートまたはデータ コレクションに関連した問題はすべて、クラスタ内のアプリケーション サーバーに伝播します。

   a. アプリケーション サーバーへのログインは、Windows または PuTTY for Linux のリモート デスクトップ接続を使用して行ってください。

   b. DPA サーバーを登録するには、`dpa app support --register ESRS_IP` コマンドを入力してください。

ESRS_IP は、ESRS ゲートウェイの IP アドレスです。次に例を挙げます。

```
C:\Program Files\EMC\DPA\services\bin>dpa app support --
register 10.11.110.111
```

c. 指示が出たら、EMC セキュア リモート サポートのユーザー名とパスワードを入力します。

入力した IP アドレスによる DPA サーバーの登録リクエストが承認され、コマンドが正しく実行されたことが出力に示されます。

7. （推奨）手順 6 で、DPA アプリケーション サーバーを ESRS-VE に登録した場合は、DPA アプリケーション サーバーで正常稼働サービスを有効にします。DPA アプリケーション サーバーで、次のように入力します。

   a. **$ dpa health install**

   b. **$ dpa health start**

8. （オプション）レプリケーションの監視に関するアラートを構成する場合は、必ず解析ポリシーに対応する復旧可能性ルールを作成し、ルールを目的のオブジェクトに割り当てます。［**Policies**］ > ［**Analysis Policies**］の順に移動します。

9. （オプション）以前の 6.x バージョンからアップグレードした場合に、［Data Domain Overview］ダッシュボードと［Data Domain Details］ダッシュボードを表示するには、次の手順を実行します。

   a. ［**Dashboard**］ > ［**+**アイコン］ > ［**Open Existing Dashboard**］の順に移動します。

   ［**Open Existing Dashboard**］ウィンドウが表示されます。

   b. ［**Data Domain**］を選択し、［OK］をクリックします。

10. （オプション）Data Domain OS 5.7 以降を監視する場合、以下の手順で物理容量レポートのデータ収集の構成を確認できます。

    a. Data Domain OS 5.7 のボックスに、リクエストを手動で割り当てます。

    b. Data Domain の統計情報が収集され、スケジュールが作成されるようにリクエストを実行します。その後、最初のレポートを実行する準備が整うと、データが返されます。

DPA アプリケーション サーバーの暗号化

アプリケーション サーバーと DPA Web コンソール間で送受される情報を暗号化するには、アプリケーション サーバーに証明書をインストールする必要があります。

DPA アプリケーション サーバーの暗号化

初期設定では、DPA アプリケーション サーバーと DPA Web コンソール間をフローする情報は、DPA アプリケーション サーバーに組み込まれた自己署名証明書を使用して暗号化されます。この証明書は、キー ストア パスワードとともにインストール時に生成されます。

開始する前に

- アプリケーション サーバー用の信頼できる証明書とプライベート キーを CA にリクエストして取得します。
- 信頼できる証明書とキーストア ファイル内部のプライベート キーをマージします。詳細については、CA ベンダーのドキュメントを参考にしてください。
- アプリケーション サーバー クラスタリングを導入する場合は、すべてのクラスタ構成を完了してからデータストアとアプリケーション サーバーで暗号化を有効にします。

手順

1. `dpa app impcert -kf` コマンドを使用して自己署名証明書をインポートします。

   `dpa app impcert -kf "C:\work\new.keystore" -al newkey -pw password`

   これは、新しく生成されたキーストア ファイルのパスワードです。このパスワードは、`C:\work\new.keystore` にあります。

2. DPA アプリケーション サービスをリスタートします。`dpa app --help` コマンドを実行すると追加情報を確認できます。
3. （オプション） DPA のアクセスに使用するブラウザに証明書をインストールします。選択したブラウザーの手順に従います。

   安全な接続を使用すると、初期接続を確立して DPA を開くのに数分かかる場合があります。

アプリケーション サーバー クラスタの暗号化

アプリケーション サーバー クラスタの暗号化には、CA の 1 つのドメイン（ワイルドカード）の証明書が必要です。DPA アプリケーションのすべてのクラスタ ノードにこの証明書をインストールします。

クラスタ内アプリケーションのノードごとに個別の証明書をインストールする必要があります。

DPA でのアンチウイルス ソフトウェアの構成

次のアンチウイルス設定を構成します。特定のアンチウイルス ソフトウェアのマニュアルを参照し、これらのプロセスのリアルタイム監視や読み取りファイルの監視が発生しないようにソフトウェアを構成する方法を確認します。

すべての DPA ファイル システムをアンチウイルス ソフトウェアの監視対象とする必要はなく、特定のファイル システムやプロセスのスキャンでディスク IO アクティビティが増加した結果、全体のパフォーマンスが引き下げられる可能性もあります。

手順

1. 次のファイルとプロセスはアンチウイルスの監視から除外します。

   Linux でアンチウイルス ソフトウェアを構成している場合、次のファイル名には `.exe` 拡張子が付いていません。

   - DPA アプリケーション サーバー：
     - `<install_dir>services\executive\wrapper.exe`
     - `<install_dir>\agent\bin\dpaagent.exe`
     - `<install_dir>\services\_jre\bin\java.exe`
   - DPA データストア サーバー：
     - `<install_dir>\services\datastore\engine\bin\postgres.exe`
     - `<install_dir>\agent\bin\dpaagent.exe`

2. 以下の特定のディレクトリは、アンチウイルス ソフトウェアの監視対象から除外します。

   - DPA アプリケーション サーバー：
     - `<install_dir>\services\standalone\**`

- <install_dir>\services\tmp**
- <install_dir>\services\shared**

- DPA データストア サーバーのファイル スペース：

注

データストアのインストールで高度なファイル システム レイアウトを選択した場合は、次のデフォルト値とは異なる代替ディレクトリが使用される可能性があります。

- <install_dir>\services\datastore\data**
- <install_dir>\services\datastore\data\pg_log**

アップグレード

以前の DPA リリースから、DPA DPA18.1 およびマイナー リリースにアップグレードが可能です。「Data Protection Advisor Release Notes」に、サポートされているアップグレードの情報が記載されています。

DPA18.1 アップグレード インストーラには、TLS プロトコル バージョン 1.2 のみを使用するオプションを提供していない点に注意してください。また DPA は、アップグレード後も既存の TLS プロトコル バージョン設定を保持します。アップグレード後のみ、TLS プロトコル バージョンを 1.2 に変更できます。詳しくは、インストールまたはアップグレードをしてから TLS プロトコル バージョン 1.2 を設定するを参照してください。

アップグレードの前提条件

DPA サーバーのアップグレードを実行するための、一連の推奨されるベスト プラクティスが用意されています。

- dpa ds export コマンドで DPA データストアをバックアップします。詳細については、データストアのバックアップ（123 ページ）を参照してください。DPA インストーラーにより操作が指示されます。
- データストアやアプリケーション サーバーのアップグレードでは、サーバー アップグレードの一環で、対象サーバーの DPA エージェントもアップグレードされます。スタンドアロンの DPA エージェントのみの場合は、DPA エージェント単体に対し、個別にアップグレードを実行する必要があります。
- DPA サーバーとエージェントとの間で安全に通信するには、dpa app agentpwd アプリケーション サーバー ホストで DPA CLI コマンドを使用し、エージェント登録パスワードを設定します。また、すべての DPA エージェント ホストで、このパスワードを設定する必要があります。詳細については、dpa application agentpwd を参照してください。次に、アプリケーション サービスを再起動します。このパスワードが、各エージェントに設定されていることを確認します。バージョン 6.5 より前の DPA エージェントを実行しながら、バージョン 18.1 のエージェントにアップグレードする場合を除きます。詳細については、DPA バージョン 6.5 エージェントおよびバージョン 6.5 サーバーとあわせた、バージョン 6.5 以前の DPA エージェントのアップグレード（68 ページ）を参照してください。
- [dpa app ver]を実行し、出力を記録して、システムにインストールされている以前の DPA 6.x のビルドをメモします。この出力は、パッケージのインストールを確認するときに重要です。
- DPA アプリケーション サーバーを停止します。DPA アプリケーション サーバーを実行しているホストのフル バックアップを実行することをお勧めします。

- DPA データストアを停止します。DPA データストア サーバーを実行しているホストのフル バックアップを実行することをお勧めします。
- インフラストラクチャが VM で実行されている場合、DPA のアプリケーション サーバーとデータストア サーバーを停止し、アップグレードの問題が発生した際に簡単にリストアできるように、DPA のアプリケーション サーバーとデータストア サーバーのスナップショットを作成します。
- ブラウザ キャッシュをクリアします。
- 管理者/root 権限があることを確認します。
- UNIX/Linux でアップグレードする場合は、システムに InstallAnywhere 用の `unzip` コマンドがインストールされていることを確認してください。
- クラスタ環境でパッチをアップグレードまたはインストールする場合は、すべてのサーバーで DPA アプリケーション サービスを停止します。まずデータストアをアップグレードし、次にアプリケーション サーバーをアップグレードします。アプリケーション サービスを停止する必要があります。サービスが別々のマシン上にある場合にインストーラがサービスを停止できないためです。
  アップグレードした DPA アプリケーションを起動します。残りのクラスタ アプリケーション サーバーをアップグレードする前に、初期化が完了し、DPA Web コンソールにログインできることを確認します。
- データベースのアップグレードに関連して、次の点に留意してください。
  - データベースのアップグレード用に、3 GB の空き領域があることを確認します。
  - glibc のバージョンが 2.12 以上の Linux バージョンを実行していることを確認します。glibc のバージョンが 2.12 未満の Linux バージョンを実行している場合は、2.12 より前の glibc を実行している Linux バージョンにおける DPA のアップグレード （69 ページ）に記載されている手順を使用してください。
- 現在、既存の DPA バックアップ ライセンスで RMAN レポート用の DPA を使用している場合は、エンタープライズ アプリケーション ライセンス用の DPA についてアカウント担当者にお問い合わせください。エンタープライズ アプリケーションの DPA ライセンスでは、DPA 6.3 およびマイナー リリースへのアップグレード時に、DPA に報告される RMAN サーバーの数を増やすことができます。インストール後に、DPA 6.3 およびマイナー リリースに DDBEA ライセンスを入力します。DPA 6.2 Release Notes に DDBEA のライセンスに関する詳細情報が記載されています。
- DPA 6.1 からアップグレードする場合は、アップグレードする前に、必ず収集リクエストの保存期間を確認し、組織のポリシーに合わせて編集します。データ コレクション リクエストには、DPA 6.1 の異なるデフォルトの保存期間が含まれています。

DPA のアップグレード

この DPA アップグレード手順は、クラスタまたはデータストア レプリケーションが構成されておらず、実行している Linux バージョンの glibc バージョンが 2.12 以上の場合に使用します。

はじめに

データベースのテーブルスペースが異なるファイル システムに存在するように構成されている場合の、アップグレード インストールのサポートを追加します。

- アップグレードの前提条件（66 ページ）で指定された前提条件を必ず実行します。
- インストーラーは、admin/root ユーザーとして実行します。

glibc のバージョンが 2.12 未満の Linux バージョンを実行している場合は、2.12 より前の glibc を実行している Linux バージョンにおける DPA のアップグレード （69 ページ）に記載されている手順に従ってください。

手順

1. まだ行っていない場合は、アプリケーション サービスをシャットダウンします。
2. データストアをアップグレードします。インストーラーで指示されているインストールのステップに従います。既存の DPA インストール ディレクトリが正しく指定されていることを確認します。

   DPA 更新パッケージは、既存の DPA パッケージと同じインストール ディレクトリにインストールする必要があります。
3. アプリケーション サーバーをアップグレードします。インストーラーで指示されているインストールのステップに従います。インストーラーで既存の DPA インストール ディレクトリが正しく指定されていることを確認します。

   DPA 更新パッケージは、既存の DPA パッケージと同じインストール ディレクトリにインストールする必要があります。
4. DPA Web コンソールをリスタートします。
5. ファイルがインストール フォルダーに配置されるまで待ちます。

   Windows の場合：`C:\Program Files\EMC\DPA\<install_dirservices\applications`

   Linux の場合： `/opt/emc/dpa/services/applications`

   ［DPA web console UI spash］ページにアップグレードのステータスが表示されます。
6. DPA インストール後の作業（61 ページ）に記載されているステップを実行します。

DPA エージェントのアップグレード

手順

1. DPA エージェント サービスをシャットダウンします。
2. 使用している OS 用のエージェント インストーラーを使用して、エージェントをアップグレードします。インストーラーで指示されているインストールのステップに従います。

   DPA 更新パッケージは、既存の DPA パッケージと同じインストール ディレクトリにインストールする必要があります。

   アップグレード中は、エージェントを停止することを検討してください。保持しているリクエストがアップグレード中に失敗する場合があります。アップグレードが完了すると、DPA エージェントは正常に動作を続けます。

DPA バージョン 6.5 エージェントおよびバージョン 6.5 サーバーとあわせた、バージョン 6.5 以前の DPA エージェントのアップグレード

エージェント パスワードをサポートしていない、DPA エージェントを 6.5 より前のバージョンの実行が必要になる場合があります。このような状況では、DPA サーバーにエージェント登録パスワードを設定すると、エージェント パスワードをサポートしない、旧バージョンの DPA エージェントがすべて接続に失敗します。このような状況を回避するには、以下の手順に従ってください。

サポートされなくなったシステムでバージョン 6.5 より前の DPA エージェントを実行し、収集する必要があります。また、エージェントの数が多すぎると一度にアップグレードすることができない場合があります。

手順

1. DPA サーバーをバージョン 6.5 にアップグレードします。

エージェントの登録パスワードは設定しないでください。3. 旧バージョンのエージェントをアンインストールしてから 6.5 をインストールしないでください。

2. 通常のアップグレード プロセスに従って、バージョン 6.5 にアップグレードする必要がある DPA エージェントをアップグレードします。

   DPA エージェントをアップグレードするプロセスでは、エージェント パスワードを設定する必要はありません。これは、エージェント パスワードを設定するように要求する、新規インストールとは異なります。

2.12 より前の glibc を実行している Linux バージョンにおける DPA のアップグレード

はじめに

- アップグレードの前提条件（66 ページ）で指定された前提条件を必ず実行します。
- インストーラーは、admin/root ユーザーとして実行します。

手順

1. アプリケーション サービスを停止します。
2. データストアをエクスポートします。詳細については、データストアのバックアップ（123 ページ）を参照してください。
3. DPA の最新バージョン、および glibc バージョン 2.12 を実行している Linux バージョンを使用して、新しいデータストアをインストールします。
4. 新しくインストールされたデータストア（DPA の最新バージョン、および glibc バージョンが 2.12 であるサポート対象の Linux バージョンを使用）に、既存のデータストアをインポートします。
5. 新たにインストールされ、インポートされたデータストアに、DPA アプリケーション サーバーをポイントします。`dpa app configure --master <datastore_ip>`を実行します。
6. データストアをアップグレードします。DPA のアップグレード（67 ページ）の処理手順に従います。

既存のクラスタのアップグレード

この手順により、既存のクラスタをアップグレードします。

はじめに

- アップグレードの前提条件（66 ページ）で指定されたすべての手順を必ず実行します。
- UNIX マシンを実行している場合は、root ユーザーであることを確認してください。
- DPA アプリケーションとデータストア サーバーのロードバランサーを停止します。ロードバランサーを停止するコマンドは OS によって異なります。各 OS のマニュアルを参考にしてください。

手順

1. 次のクラスタ アプリケーション ノードのアプリケーション サービスを停止します。

   a. スレーブ アプリケーション サーバーを停止します。

   b. マスター アプリケーション サーバーを停止します。

   コマンド：

   ```
   # dpa app stop
   ```

2. DPA データストア サーバーをアップグレードします。

a. DPA インストーラーを起動して、指示に従います。

b. データストアがインストールされ、正しく開始されたことを確認してください。

詳細については、DPA インストール後の作業（61 ページ）を参照してください。

3. マスター アプリケーション ノードをアップグレードします。

a. DPA インストーラーを起動して、指示に従います。

b. アプリケーション サービスが開始するまで待ちます。`server.log` ファイルに `DPA master started successfully` のような出力が含まれることを確認します。

4. スレーブ アプリケーション ノードをアップグレードします。

a. DPA インストーラーを起動して、指示に従います。

b. アプリケーション サービスが開始するまで待ちます。`server.log` ファイルに `DPA slave started successfully` のような出力が含まれることを確認します。

5. DPA アプリケーション サーバーとデータストア サーバーのロードバランサー アプリケーションを再起動します。ロードバランサーを起動するコマンドは OS によって異なります。各 OS のマニュアルを参考にしてください。

DPA 6.3 以降によるデータストア レプリケーションを使用したアップグレード

データストア レプリケーションを有効にしてアップグレードするには、次の処理手順に従います。

はじめに

- アップグレードの前提条件（66 ページ）で指定されたすべての手順を必ず実行します。
- UNIX マシンを実行している場合は、root ユーザーであることを確認してください。
- 次のステップに進む前に、各ステップのすべてのプロセスを確実に完了してください。

手順

1. まだ行っていない場合は、アプリケーション サーバーでアプリケーション サービスを停止します。コマンド：

```
# dpa app stop
```

2. スレーブ データストアをアップグレードします。

DPA インストーラーを起動して、指示に従います。

カスケード レプリケーションを実装する場合は、まずチェーンの終端に位置するデータストアをアップグレードします。

3. マスター データストアをアップグレードします。

DPA インストーラーを起動して、指示に従います。

4. アプリケーション サーバーをアップグレードします。

DPA インストーラーを起動して、指示に従います。

5. データストア レプリケーションが実行されていることを確認します。コマンド：

```
# dpa ds rep
```

出力には STREAMING と表示されます。

DPA バージョン 6.3 以前によるデータストア レプリケーションを使用したアップグレード

レプリケーション スレーブ データストアをアップグレードする場合を除き、データストア レプリケーションのアップグレードは自動化され、ユーザーの操作は必要ありません。

はじめに

- アップグレードの前提条件（66 ページ）で指定されたすべての手順を必ず実行します。
- UNIX マシンを実行している場合は、root ユーザーであることを確認してください。
- 次のステップに進む前に、各ステップのすべてのプロセスを確実に完了してください。

手順

1. すべてのサービスを終了します。
   a. アプリケーション サーバで# dpa app stop を実行します。
   b. マスター データストアで# dpa ds stop を実行します。
   c. スレーブ データストアで、# dpa ds stop を実行します。
2. マスター データストアをアップグレードします。
   a. DPA インストーラーを起動して、指示に従います。
   b. データストア レプリケーションが実行されていることを確認します。**`# dpa ds rep`** を実行します。
3. マスター データストアのコピーを作成します。「**`dpa ds rep -e <empty_dir>`**」と入力します。
4. 既存のスレーブ データストアをアンインストールします。
5. マスター データストアと同じインストール場所に、データストア サーバを新規インストールし、新しくインストールしたデータストア サーバをスレーブ データストアとして構成します。「**`dpa.sh ds rep --role SLAVE <IP of master>`**」と入力します。

   サービスを開始または停止しないでください。
6. マスター コピーを使用して、スレーブ データストアを初期化します。「**`dpa ds rep -i <master_copy>`**」と入力します。
7. スレーブ データストアを起動します。
8. アプリケーション サーバをアップグレードします。

データストア レプリケーションと既存のクラスタがある場合のアップグレード

データストア レプリケーションと既存のクラスタを使用しているシステムのアップグレードは、この手順に従って行います。

はじめに

- アップグレードの前提条件（66 ページ）で指定されたすべての手順を必ず実行します。
- UNIX マシンを実行している場合は、root ユーザーであることを確認してください。
- DPA アプリケーションとデータストア サーバーのロードバランサーを停止します。ロードバランサーを停止するコマンドは OS によって異なります。各 OS のマニュアルを参考にしてください。

手順

1. まだ行っていない場合は、クラスタ アプリケーション ノード上のアプリケーション サービスを停止します。

a. スレーブ アプリケーション サーバーを停止します。

b. マスター アプリケーション サーバーを停止します。

コマンド：

```
# dpa app stop
```

2. DPA 6.3 以降によるデータストア レプリケーションを使用したアップグレード（70 ページ）に記載されているステップを実行します。

   DPA バージョン 6.3 以前を使用してアップグレードする場合、「DPA バージョン 6.3 以前によるデータストア レプリケーションを使用したアップグレード」に記載されている手順で実行してください。

3. スレーブ アプリケーション ノードをアップグレードします。

   a. DPA インストーラーを起動して、指示に従います。

   b. アプリケーション サービスが開始するまで待ちます。`server.log` ファイルに `DPA slave started successfully` のような出力が含まれることを確認します。

4. DPA アプリケーション サーバーとデータストア サーバーのロードバランサー アプリケーションを再起動します。ロードバランサーを起動するコマンドは OS によって異なります。各 OS のマニュアルを参考にしてください。

第 3 章

DPA の管理

この章は、次のセクションで構成されています。

- ライセンス管理 74
- ユーザーとセキュリティ 75
- システム設定 87
- アプリケーション サービスの管理 117
- データストア サービス管理 123
- DPA コマンド ライン操作 130

ライセンス管理

このセクションでは、DPA でのライセンス管理方法について説明します。

DPA にバンドルされた評価版ライセンス

DPA には 90 日間の評価版ライセンスがバンドルされています。

この評価版ライセンスは DPA がインストールされた時点で作成され、最大で 90 日間使用可能で、すべての機能にアクセスできます。90 日間の評価期間中にライセンスをインポートすると、評価版ライセンスは削除され、インポートしたライセンスに基づいて DPA の機能にアクセスできます。

DPA のライセンス タイプ

DPA は、［CLP］（［Common Licensing Platform］）ライセンス タイプを使用します。

CLP ライセンスは、製品名が DPA に変更されるまで DPA で使用されていた［WLS］（［Wysdm Licensing System］）ライセンス タイプと共存し、特定の状況においてはリプレースされます。

DPA での CLP ライセンスと WLS ライセンスの共存

DPA 機能を利用するには、CLP ライセンスが必要です。

容量の拡張が不要であるか、DPA 6.2 より後の DPA バージョンの DPA 機能に変更しない場合は、CLP ライセンスのインポートは不要です。ただし、DPA 6.2 より前の DPA バージョンから DPA の最新バージョンにアップグレードする場合は、アップグレードまたは移行後に licensing@emc.com に問い合わせて、すべての WLS ライセンスについてレガシー ライセンスから CLP ライセンスへの移行のサポートを受けてください。DPA バージョン 5.x から DPA の最新バージョンに移行する場合、既存ライセンスはご使用の構成およびデータとともに移行されます。CLP ライセンスの追加は、DPA の最新バージョンの機能を使用する場合と現在のライセンスの容量を拡張する場合にのみ必要です。

CLP ライセンスはリプレース モデルで機能します。CLP ライセンスをインポートすると、同じタイプの既存のライセンスがすべてリプレースされます。さらに、ベースとエンタープライズ ライセンスの機能は、各 CLP ライセンスに移動されます。同じタイプの CLP ライセンスを注文する際には既存のライセンス数を把握している必要があり、その後新しく必要な容量を追加して注文の合計を出します。DPA インストールのライセンスを購入する方法については、担当営業までお問い合わせください。

以前の旧 DPA のバージョンから移行またはアップグレードされたシステムには、WLS ライセンスが含まれます。WLS と CLP は、同じ機能用でない場合に限り、共存が可能です。

期限切れのライセンス

ライセンスの期限が切れた場合、期限切れのライセンスで有効化されているすべてのオブジェクトで実行されたレポートのレポート タイトルにライセンス違反の警告が表示されます。また、期限切れのライセンスで有効化されているモジュール コンポーネントについては、新しいオブジェクトを Web コンソールに追加することができません。

ライセンスの削除

ライセンスを削除すると、そのライセンスの対象オブジェクトに対してレポートを実行したときにライセンス違反の警告が表示されます。そのタイプの新しいオブジェクトは、交換用ライセンスが提供されるまで Web コンソールに追加できません。

有効期限がある一時ライセンスを使用する場合、［License Expiration］ダイアログが表示され、一時ライセンスの有効期限を通知します。パーマネント ライセンスは表示されません。

新規ライセンスの追加

［**Admin**］ > ［**System**］の順にクリックし、［**Manage Licenses**］をクリックします。

一時ライセンスの有効期限を示す自動ポップアップの無効化

［**User Properties**］ > ［**Show License Expiration**］の順にクリックしてチェックボックスをオフにします。

ユーザーとセキュリティ

ユーザー アカウント

DPA にはデフォルトで 4 つのデフォルト ユーザーがあります。それは、アドミニストレーター、アプリケーション所有者、エンジニア、そしてユーザーです。

管理者アカウントは、DPA インストール後に有効となっている唯一のアカウントです。ユーザーは、DPA のインストール処理中に管理者アカウントのパスワードを設定します。

DPA にアクセスするには、事前に管理者が他のデフォルト ユーザー アカウント用にパスワードを設定する必要があります。管理者が他のユーザー アカウントのパスワードを設定しない場合、アカウントは無効な状態のままになります。

ユーザーの管理

DPA 管理者は、［**Manage Users**］セクションでユーザー アカウントを管理できます。［**Admin**］ > ［**Users & Security**］ > ［**Manage Users**］の順にクリックします。このセクションで、管理者はユーザー アカウントの作成、編集、表示、削除を実行できます。

新規ユーザー アカウントの作成

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Users**］の順にクリックします。
2. ［**Create User**］をクリックします。

   または、既存のユーザーを選択し、［**Save As**］をクリックして既存ユーザーのコピーを作成します。

3. ［**Create User Properties**］タブで、それぞれのタブの情報を更新します。
   a. ［**User Properties**］タブで、名前、ログオン名、役割、認証タイプ、パスワードを指定します。
   b. LDAP を使用してユーザーを認証する場合は、LDAP 認証タイプを選択します。
   c. ［**Report Preferences**］、［**Preferences and Appearance**］タブで、環境設定や表示設定を割り当てます。ユーザーに割り当てる役割によって、アクセスできる DPA の領域が決まります。
   d. ［**OK**］をクリックして、設定を確認します。
4. ［**Close**］をクリックします。

ユーザー アカウントの編集と削除

DPA 管理者は、デフォルトの管理者アカウントを除き、任意の DPA ユーザー アカウントを編集、削除できます。

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Users**］の順にクリックします。
2. 編集または削除するユーザーを選択します。
   - ［**Edit**］をクリックし、ユーザーの名前、役割、パスワード、レポートや表示の設定など、目的の項目をカスタマイズします。
   - 削除するには［**Delete**］、［**Yes**］の順にクリックします。
3. ［**Close**］をクリックします。

ユーザー アカウントのパスワードの変更

DPA 管理者は［**Manage Users**］でユーザー アカウントのパスワードを変更できます。非管理者ユーザーは、DPA Web コンソールの右上にあるギア アイコンをクリックし、［**View User Properties**］で自分のパスワードを変更できます。

手順

1. ［**Admin**］ > ［**Users and Security**］ > ［**Manage Users**］の順にクリックします。
2. パスワードを変更するユーザー アカウントを選択し、［**Edit**］をクリックします。
3. ［**Edit User Properties**］に移動し、［**Authentication Type**］として［**Password**］に設定します。
4. ［**Password**］フィールドに新しいパスワードを入力し、同じパスワードを［**Confirm Password**］フィールドに再度入力します。

   DPA のパスワードに関して、次の点に注意してください。

   - 空白のパスワードはサポートされていません。
   - 最小文字数は、9 文字です。
   - 必須条件は次のとおりです。
     - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
     - 1 つ以上の数字を含んでいること
     - 1 つ以上の特殊文字を含んでいること
5. ［**OK**］をクリックします。

セキュリティの設定

ユーザー セキュリティ設定を構成できます。［**Admin**］ > ［**Users & Security**］の順に移動します。

表 16 パスワード ポリシー

設定	説明
Minimum number of characters	DPAWeb コンソールのパスワードに必要な最小文字数。最小値は 9 です。文字数の上限はありません。DPA は Latin 文字のみをサポートしています。

表 16 パスワード ポリシー （続き）

設定	説明
Must use uppercase characters	DPAWeb コンソールのパスワードに大文字が必要となります。デフォルトで有効化されます。
Must use lowercase characters	DPAWeb コンソールのパスワードに小文字が必要となります。デフォルトで有効化されます。
Must use special characters	DPAWeb コンソールのパスワードに特殊文字が必要となります。デフォルトで有効化されます。
Must use numeric characters	DPAWeb コンソールのパスワードに数字が必要となります。デフォルトで有効化されます。

表 17 パスワード履歴のポリシー

設定	説明
Password History	パスワード履歴の制限を有効化します。
Limit of password history	DPA において、同じユーザーに対して以前のパスワードと同じパスワードを指定できる回数。デフォルト値は 1 です。最大値は 10 です。デフォルトで有効化されます。 ［**Limit of password history**］を［**1**］のままにすると、ユーザーはパスワードを現在のパスワードに変更できません。 ［**Limit of password history**］の値を 1 より大きい値に設定すると、ユーザーはパスワードを現在のパスワードに変更することも前のパスワードに変更することもできません。DPA には、前のパスワードがすでに設定済みであること、ユーザーは新しいパスワードを指定する必要があることを示すメッセージが表示されます。

表 18 ログイン制限

設定	説明
Login limit	DPAWeb コンソールへのログイン試行数に対する制限を有効化します。
Limit of login attempts	DPA がユーザーに DPAWeb コンソールへのログイン試行を許可する回数。デフォルト値は 5 です。範囲は 1～10 です。
Lockout timeout	指定されたログイン制限を超えた後、DPA が一時的にユーザーを DPAWeb コンソールからロックアウトする時間の長さ。デフォルト値は 3 分です。範囲は 1～60 分です。

表 19 Password Expiration

設定	説明
Password Expiration	パスワードの有効期限を有効にします。デフォルト値は off です。
Password expiration period (days)	DPA パスワードが有効である日数。デフォルト値は 90 です。最大値は 180 です。

ユーザーの役割と権限

役割は、ユーザーに許可される権限を処理するために使用します。ユーザーは、適切な役割に割り当てられることで、自身の権限を取得します。

DPA ではデフォルトで次の 4 つの役割が提供されます。それは、アドミニストレーター、アプリケーション所有者、エンジニア、そしてユーザーです。デフォルトのユーザーの役割が設定されており、変更できません。

次の表でデフォルトの役割の権限について説明します。

表 20 ユーザーの役割

ユーザーの役割	権限
管理者	すべての構成とレポート機能を実行できます。
アプリケーション所有者	すべてのレポート機能を実行し、認証情報の設定を変更できます。
エンジニア	すべてのレポート機能とほとんどの構成機能を実行できます。 エンジニアは、ユーザーやユーザーの役割を作成または変更したり、システム設定を変更したりすることはできません。
ユーザー	レポート機能だけを実行できます。

新しいユーザーの役割の作成

DPA 管理者は、許可や設定をカスタマイズしたカスタム ユーザーの役割を新規作成できます。

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Roles**］の順にクリックします。
2. ［**Create Role**］をクリックするか、既存の役割をクリックして［**Save As**］をクリックします。

   ［**Save As**］を選択し、コピーを作成します。
3. ［**User Role Properties**］ウィンドウで、
   a. ［**Name**］フィールド、［**Description**］フィールドに新しい役割の名前と説明を入力します。
   b. 権限、アクセス可能なグループ、ダッシュボード、メニューを設定します。
   c. ［**OK**］をクリックして、設定を確認します。
4. ［**Close**］をクリックします。

ユーザーの役割の編集と削除

DPA 管理者は、カスタム ユーザーの役割のみを編集、削除できます。デフォルトのユーザーの役割の編集、削除はできません。削除対象の役割を割り当て済みのユーザーに別の役割を割り当てるまでは、役割は削除できません。

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Roles**］の順にクリックします。
2. 編集または削除するカスタム ユーザーの役割を選択します。
   - ［**Edit**］をクリックして、権限、アクセス可能なグループ、ダッシュボード、メニューをカスタマイズします。
   - ユーザーの役割を削除するには、［**Delete**］、［**Yes**］の順にクリックします。

ユーザーの役割でのユーザーの表示

［**Admin**］ > ［**Users & Security**］ > ［**Manage Roles**］の順にクリックします。DPA 管理者は、［**Manage Roles**］タブで、特定のユーザー役割名を選択すると、ユーザーの役割と関連づけられたユーザーを表示できます。デフォルトの役割のリスト（管理者、アプリケーション所有者、エンジニア、ユーザー）が、インストール以降に追加された新規の役割とともに表示されます。

特定のグループのみを表示するユーザー制限

レポートの実行中に特定のグループまたはバックアップの構成アイテムを表示できる DPA ユーザーを設定できます。

はじめに

対象は既存のグループに限定されます。

ユーザーは、デフォルトでは DPA オブジェクト インベントリの全体を表示できます。その一方で、特定のユーザーが表示できる DPA オブジェクト インベントリを制限することもできます。たとえば、サービス プロバイダーは DPA オブジェクト インベントリに個々の顧客に応じたグループを構成することがあります。サービス プロバイダーは、個々の顧客が DPA にログインしたとき、自分が所属する顧客グループ内で構成された特定のオブジェクト インベントリのみを対象とするレポートを表示、実行するように構成することができます。

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Roles**］の順にクリックします。
2. 必要なカスタム役割を作成するか、編集するカスタム ユーザーの役割を選択し、［**Edit**］をクリックします。
3. ［**Accessible Groups**］タブを選択します。

   用意されたすべてのグループの一覧が表示されます。
4. 役割ごとにアクセス可能なグループを選択し、［**>**］または［**>>**］をクリックして、すべてのグループを移動します。
5. ［**OK**］をクリックして、設定を確認します。
6. ［**Close**］をクリックします。

ユーザー グループの制限

特定のユーザー グループまたはロールが、システム属性を更新したりグループを作成または変更したりする権限なしに、カスタム属性の値を設定できるようにするよう、ユーザー グループを制限できます。

はじめに

- 管理者として DPA サーバーにログインします。

手順

1. Read Inventory ロールを作成します。
   a. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Roles**］の順に選択し、［**Create Role**］をクリックします。

      ［**User Role Properties**］ダイアログ ボックスが表示されます。

   b. 次のように各フィールドに入力します。

      ［**Name**］フィールドで、ロールに付与する名前を入力します。たとえば、［**Read Inventory**］などです。

      必要に応じて、［**Description**］フィールドに説明を入力します。

   c. ［**Inventory**］以下の［**Privilges**］タブで、［**View existing objects and group management**］を選択します。

   d. ［**Accessible Groups**］で、表示させたいグループを選択し、［**Move selected groups**］をクリックして、［**Close**］をクリックします。
2. Read Inventory ユーザーを作成します。
   a. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Users**］の順に選択し、［**Create Role**］をクリックします。

      ［**Create User Properties**］ダイアログ ボックスが表示されます。

   b. 次のように各フィールドに入力します。

      ［**Name**］フィールドで、ユーザーに付与する名前を入力します。たとえば、［**Read**］と入力します。

      ［**Logon**］フィールドで、ユーザーが入力すべきログオンを指定します。たとえば、**Read** と入力します。

      ［**Role**］フィールドで、ステップ 1 の［Read Inventory］ロールに対して作成したものを選択します。

      ［**Authentication**］フィールドで、ドロップダウンから希望の認証タイプを選択します。［Password］を選択した場合、パスワードを指定し、確定します。

   c. ［**OK**］をクリックします。
3. Assign Attribute and Read Inventory ロールを作成します。
   a. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Roles**］の順に選択し、［**Create Role**］をクリックします。

      ［**User Role Properties**］ダイアログ ボックスが表示されます。

   b. 次のように各フィールドに入力します。

      ［**Name**］フィールドで、ロールに付与する名前を入力します。たとえば、［**Assign Attribute and Read Inventory Role**］などです。

      必要に応じて、［**Description**］フィールドに説明を入力します。

   c. ［**Privileges**］タブの［**Inventory**］で、［**Assign/unassign attributes**］を選択します。

［**View existing objects and group management**］権限が自動的に選択されます。

d. ［**Accessible Groups**］タブで、表示させたいグループを選択し、［**Move selected groups**］をクリックして、［**Close**］をクリックします。

4. Assign Attribute and Read Inventory ユーザーを作成します。

a. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Users**］の順に選択し、［**Create Role**］をクリックします。

［**Create User Properties**］ダイアログ ボックスが表示されます。

b. 次のように各フィールドに入力します。

［**Name**］フィールドで、ユーザーに付与する名前を入力します。たとえば、［**Assign**］などです。

［**Logon**］フィールドで、ユーザーが入力すべきログオンを指定します。たとえば、**`Assign`** などです。

［**Role**］フィールドで、Assign Attribute and Read Inventory ロールに対してステップ 3 で作成したものを選択します。

［**Authentication**］フィールドで、ドロップダウンから希望の認証タイプを選択します。［Password］を選択した場合、パスワードを指定し、確定します。

c. ［**OK**］をクリックします。

必要条件

外部認証、LDAP 統合、バインディング

DPA は、LDAP（Lightweight Directory Access Protocol）を介して外部認証方式の構成をサポートします。DPA は、LDAP サーバーとして Microsoft Active Directory と OpenLDAP をサポートします。

内部認証方法が構成されている場合にのみ、ユーザー アカウントのパスワードが、DPA データストアに保存されます。外部認証の方法では、パスワードは LDAP サーバーに保存されます。LDAP 認証を有効化するには、［**Admin**］ > ［**Users & Security**］ > ［**Manage External Authentication**］の順に選択します。

DPA は 2 種類の LDAP バインド方法（匿名バインドと簡易バインド）をサポートしています。匿名バインドを構成するには、［外部認証の管理］タブで［匿名バインド］チェックボックスをオンにします。簡易バインドでは、必ず［匿名のバインド］チェックボックスをオフにします。また、読み取りアクセスを持つユーザーの名前とパスワードが設定されていることを確認します。

LDAP 認証の構成

次のフィールドは、DPA の LDAP 認証の構成で使用します。

表 21 DPA での LDAP 認証の構成

フィールド	説明
サーバー	LDAP サーバーのホスト名。必ず DPA サーバーから解決できるホスト名にします。

表 21 DPA での LDAP 認証の構成 （続き）

フィールド	説明
Use SSL	このオプションを選択すると、SSL 接続で LDAP サーバーに接続できます。
ポート	次のとおり、LDAP サーバーがリクエストをリスンするポート。 • 非 SSL 接続の場合はポート 389 • SSL 接続の場合はポート 636 グローバル カタログ サーバーとして構成されている Microsoft Active Directory を使用する場合は、次の要領に従い［Manage External Authentication］ダイアログ ボックスで指定します。 • 非 SSL 接続の場合はポート 3268 • SSL 接続の場合はポート 3269
LDAP のバージョン	サーバーで使用されている LDAP のバージョン。DPA は、バージョン 2 および 3 をサポートしています。
Base Name	可能なすべてのユーザーの場所。この場所はディレクトリに対するすべてのクエリーの起点として使用されます。 入力値には、ディレクトリ ベースの識別名（DC=eng、DC=company、DC=com など）を使用します。
識別属性	ユーザー アカウントの検索に使用する LDAP または Active Directory の属性（Active Directory の sAMAccountName、OpenLDAP の uid など）
Anonymous Bind	DPA では、2 種類の LDAP バインディングをサポートしています。 • Anonymous Bind - 匿名バインドで LDAP サーバーに接続する場合は、チェックボックスをオンにする • Simple Bind：簡易バインドを使用するチェックボックスをオフにしておきます。これで［Username］フィールドと［Password］フィールドが有効になります。
ユーザー名	定義された検索ベースで LDAP ディレクトリの検索を許可された LDAP サーバー上のユーザーのバインド DN。
パスワード	ユーザーのパスワード。
確認	クリックすると、LDAP サーバーでユーザー認証をテストできます。LDAP サーバーに正常に接続できたかどうかを伝えるメッセージが表示されます。

LDAP 認証を使用した新規ユーザー アカウント作成

DPA 管理者は、LDAP バインドを構成しテストすると、LDAP サーバーの認証を必要とするユーザー アカウントを作成、編集できるようになります。

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage External Authentication**］の順に移動します。
2. ［**Authentication type**］フィールドで、［**LDAP**］値を設定します。
3. ユーザーの識別名（DN）または識別属性の値を［**External Name**］フィールドに入力します。

   Active Directory が統合されている場合は、識別属性の値は sAMAccountName となるのが一般的です。OpenLDAP の場合は UID が一般的です。

ユーザー プロビジョニングの自動化

ユーザー プロビジョニングの自動化が LDAP サーバーに組み込まれている場合、DPA で使用できます。自動ログイン機能を有効にしておくと、新しいユーザーが DPA へのログインに成功したとき、DPA がユーザー アカウントを自動的に新規作成できるようになります。

新しいユーザーに割り当てられたユーザーの役割は、［自動ログイン］タブで構成できます。管理者は、デフォルトのユーザーの役割か LDAP グループ マッピングに基づく役割を構成できます。

自動ログイン：デフォルトのユーザーの役割

［Auto login］タブにデフォルトのユーザーの役割が設定されている場合は、DPA が自動作成したすべての新規ユーザーにこの役割が割り当てられます。自動ログイン機能で作成されたユーザーの完全なリストは［**Manage Users**］タブで表示できます。［Authentification type］フィールドには値 LDAPAUTO が入力されます。

手順

1. DPA で LDAP 統合を構成、テストします。
2. ［**Admin** ］ > ［**Users & Security**］ > ［**Manage External Authentication**］ > ［ **Auto-login Properties** ］ > ［**Edit**］の順に開き、［**Enable Auto-login**］にフラグを立てます。
3. ［Default User Role］ドロップダウン リストで役割を選択します。
4. ［**OK**］をクリックして、設定を確認します。
5. ［**Manage External Authentication**］タブで ［**OK**］をクリックして閉じます。

   自動ログインによる認証に成功すると、DPA により、DPA 内にユーザー アカウントが自動作成されます。

自動ログイン：LDAP グループのマッピング

DPA 管理者は、自動ログイン設定で特定の LDAP グループに DPA ユーザーの役割を割り当てることができます。

手順

1. 自動ログインをデフォルトのユーザーの役割で構成します。

2. 以下の要領で［**Enable Group Mapping**］チェックボックスをオンにし、グループ マッピングを有効にします。
   - ［**Group Base**］フィールドで、対象グループの識別名を指定します。例：**cn=users,dc=eng,dc=company,dc=com**
   - ［**Group Attribute**］フィールドで、グループ検索に使用する LDAP 属性を指定します。通常、Active Directory なら CN か sAMAccountName、OpenLDAP なら uid がこれに相当します。
   - ［**Group Member Attribute**］フィールドで、グループ内のメンバーを特定する属性を指定します。通常、Active Directory なら member、OpenLDAP なら memberUid がこれに相当します。
3. ［**Add**］をクリックし、［**Group Mapping**］セクションに新しく 1 行を追加します。
4. ［**LDAP Group Name**］で、このユーザー役割を割り当てるグループの名前を設定します。
5. ［**User Role**］のドロップダウン リストに用意された役割の 1 つを選択します。
6. ［**Add**］、［**Remove**］、［**Up**］、［**Down**］でグループ マッピングを整理します。
7. ［**OK**］をクリックし、設定を確認します。
8. ［**Manage External Authentication**］タブで［**OK**］をクリックして閉じます。

グループ マッピング

DPA は、グループ マッピング機能を使用して、指定された LDAP グループを DPA の役割に割り当てることで、ユーザーが所属する LDAP グループに応じた DPA の役割をユーザーに割り当てることができます。

複数の LDAP グループに所属するメンバーには、マッピング テーブルで最初のグループに割り当てられた DPA の役割が付与されます。より多くの権限を持つ DPA の役割に割り当てられる LDAP グループを必ずリストの一番上に配置します。グループ マッピング リストに含まれるグループのメンバーではないユーザーには、デフォルトのユーザーの役割が割り当てられます。［上へ］ボタンと［下へ］ボタンがあり、表内で目的とする場所に表のエントリーを移動させることができます。

LDAP 統合の構成：シナリオの設定

次の LDAP 統合シナリオには、次の設定が使用されています。これらの設定値はただのサンプルです。

表 22 オープン LDAP サーバー設定

設定の説明	設定
サーバー名	lab.emc.com
LDAP 管理者	cn=admin dc=lab,dc=emc dc=com
グループ	Administrators: cn=administrators,ou=groups,dc=lab,dc=emc,dc=com
	Users: cn=users,ou=groups,dc=lab,dc=emc,dc=com
	Support: cn=support,ou=groups,dc=lab,dc=emc,dc=com

表 22 オープン LDAP サーバー設定 （続き）

設定の説明	設定
ユーザー	Paul Abbey: uid=PAbbey,ou=people,dc=lab,dc=emc,dc=com（ユーザー メンバー）
	John Smith: uid=JSmith,ou=people,dc=lab,dc=emc,dc=com（サポート メンバー）
	Tom Baley: uid=TBaley,ou=people,dc=lab,dc=emc,dc=com（マーケティング メンバー）

シナリオ：簡易バインドと LDAP の統合の構成

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage External Authentication**］の順に選択します。
2. ［User］フィールドで次の値を確認または入力します。
   - ［**Use LDAP Authentication**］：選択
   - ［**Server**］：`lab.emc.com`
   - ［**Use SSL**］：選択（オプション）
   - ［**Port**］：`686`
   - ［**LDAP Version**］：`3`
   - ［**Base Name**］：`dc=lab,dc=emc,dc=com`
   - ［**Identification Attribute**］：`uid`（`Active Directory` を統合する場合は `sAMAccountName`）
   - ［**Anonymous Bind**］：選択解除
   - ［**Username**］：`cn=admin,dc=lab,dc=emc,dc=com`
   - ［パスワード］：`<admin_password>`
3. ［**Validate**］をクリックし、LDAP バインドの妥当性を確認します。

   妥当性検査に失敗した場合は、DPA アプリケーション サーバーからの LDAP 接続性と LDAP サーバーのパラメーターを確認します。
4. ［**Test user**］をクリックし、LDAP バインドの妥当性を確認します。

   次のユーザー名とパスワードを使用します。

   ユーザー名：`PAbbey`

   パスワード：`<PAbbey_password>`
5. ［**OK**］をクリックし、LDAP ユーザー認証を確認します。

   認証に失敗した場合は、LDAP サーバーのユーザー名とパスワードが正しいかどうかを確認します。
6. ［**Manage External Authentication**］で：［**OK**］をクリックし、設定を確認して閉じます。

7. ［**Admin**］ > ［**Users & Security**］ > ［**Manage Users**］の順に選択し、［**Create User**］をクリックします。
8. ［**User Properties**］タブに次の値を入力します。
   - ［**Name**］：`Paul Abbey`
   - ［**Logon**］：`Pabbey`
   - ［**External Name**］：`PAbbey`
   - Role：［ユーザー］
   - Authentication Type：［**LDAP**］
9. ［**OK**］をクリックし、このアカウントがユーザー アカウント リストに含まれていることを確認します。
10. ［**Close**］をクリックします。

シナリオ：グループ マッピングを伴う自動ユーザー プロビジョニングの構成

手順

1. ［**Admin**］ > ［**Users & Security**］ > ［**Manage External Authentication**］の順に選択します。
2. ［User］フィールドで次の値を確認または入力します。
   - ［**Use LDAP Authentication**］：選択
   - ［**Server**］：`lab.emc.com`
   - ［**Use SSL**］：選択（オプション）
   - ［**Port**］：`686`
   - ［**LDAP Version**］：`3`
   - ［**Base Name**］：`dc=lab,dc=emc,dc=com`
   - ［**Identification Attribute**］：`uid（Active Directory を統合する場合は sAMAccountName）`
   - ［**Anonymous Bind**］：選択解除
   - ［**Username**］：`cn=admin,dc=lab,dc=emc,dc=com`
   - ［パスワード］：`<admin_password>`
3. ［**Validate**］をクリックし、LDAP バインドの妥当性を確認します。

   妥当性検査に失敗した場合は、DPA アプリケーション サーバーからの LDAP 接続性と LDAP サーバーのパラメーターを確認します。
4. ［**Test user**］をクリックし、LDAP バインディングを確認します。

   次のユーザー名とパスワードを使用します。

   ユーザー名：`PAbbey`

   パスワード：`<PAbbey_password>`
5. ［**Edit**］をクリックします。
6. ［**Enable Auto Login**］チェックボックスをオンにし、デフォルトのユーザーの役割として［**User**］が選択されていることを確認します。
7. ［**Enable Group Mapping**］チェックボックスをオンにし、次の値を確認または入力します。

- ［**Group Base**］：`ou=groups,dc=lab,dc=emc,dc=com`
- ［**Group Attribute**］：`cn`
- ［**Group Member Attribute**］：［**memberUid**（**Active Directory** 統合対象のメンバー）］

8. ［**Add**］をクリックします。

   ［**LDAP Group Name**：］［**Support**］

   ［**Role**：］［**Engineer**］

9. ［**Close**］をクリックします。
10. John Smith としてログインします。

    エンジニアの役割を持つ新規ユーザー アカウント「JSmith」を作成する必要があります。

11. ログアウトします。
12. Tom Baley としてログインします。

    ユーザーの役割を持つ新規ユーザー アカウント「TBaley」を作成する必要があります。

システム設定

DPA エージェント、サーバー、データストアに関するデフォルトのシステム設定を変更できます。

バックアップ フィールドとリストア解決フィールドの構成

DPA では、失敗ジョブに解決策を追加できるように、最大 5 つまでカスタム バックアップとリストアによる解決のフィールドを作成しておき、後日、解決策を表示して障害の原因を確認できます。

たとえば、失敗したバックアップの詳細な解決情報を含む外部チケット システムを参照するフィールドを作成できます。管理者は、カスタム フィールドの形式を制御し、フィールドを必須フィールドまたはオプション フィールドに設定できます。

手順

1. ［**Admin**］ > ［**System**］ > ［**Manage Custom Resolutions**］の順に選択します。

   ［Manage Custom Solutions］ダイアログ ボックスが表示されます。

2. リスト内の適切な行を選択し、［**Edit**］をクリックします。

   ［**Resolution Custom Field**］ダイアログ ボックスが表示されます。

3. カスタム フィールドを有効にする場合は、［**Active**］を選択します。
4. フィールドのラベルを入力します。

   このフィールド ラベルは［**Backup Resolution**］および［**Add Resolution**］ダイアログ ボックスで使用されます。

5. ［**Input Cast**］フィールドで、カスタム フィールドに保存されるデータのタイプを選択します。

   データ タイプ例：

   - フラグ（True または False）
   - 整数値
   - 10 進値
   - テキスト

6. （オプション）［**Mandatory**］を選択すると、解決策の作成または追加時にテキスト タイプ フィールドへの入力を管理者に義務付けることができます。他のフィールド タイプでは、ユーザーが値を指定しない場合は、解決にデフォルト値が使用されます。
7. ［**OK**］をクリックします。

必要条件

適宜、バックアップやリストアによる解決をドリルダウン レポートに組み込みます。

［Job Details Popup］ドリルダウン メニューを使用する、すべてのシステム レポートに Add/View Backup Resolution アクションを組み込むこともできます。

1. ［**Reports**］、［**Report Templates**］、［**Custom Report Templates**］の順に移動し、バックアップによる解決策を追加するレポートを選択して、［**Edit**］をクリックします。
2. ［**Preview**］タブを選択します。
3. ［**Drilldowns**］をクリックしてドリルダウン レポート メニューを表示し、［**Same drilldown menu for all Columns**］を選択します。
4. 次のとおり、解決オプションを使用してポップアップ メニューを編集、または作成します。
   a. ［**Action**］を選択し、次のバックアップ、リストアによる解決オプションの 1 つを選択します。
      - バックアップによる解決の追加
      - リストアによる解決の追加
      - バックアップによる解決の表示
      - リストアによる解決の表示

      以上のほかに、選択済みアラートの表示、除外編集、ギャップの詳細、関連アラートの表示、履歴のリクエストなどのオプションもあります。
   b. ［**Automatic**］を選択します。
   c. ［**OK**］をクリックします。

設定の表示と編集

システム設定を表示または編集するには、［**Admin**］＞［**System**］＞［**Configure System Settings**］の順に選択します。

システム設定

DPA システムには、データ コレクション エージェント、サーバー、SharePoint、レプリケーション解析、エージェントレス検出についての設定があります。次の表は、各エージェント設定を示しています。

表 23 データ コレクション エージェント設定

設定	説明
［Data Collection Agent Status］	ログ ファイルの収集を有効にします。デフォルトで有効化されます。
［Data Collection Agent Version］	現在ホストにインストールされている DPA データ コレクション エージェントのバージョン。
［Data Collection Agent Port］	データ コレクション エージェントがリクエストをリスンする際に使用するポートです。

表 23 データ コレクション エージェント設定 （続き）

設定	説明
Concurrency	データ コレクション エージェントがデータを収集するために使用するスレッドの最大数。デフォルト スレッド数は 5 です。
Log Level	データ コレクション エージェントがログ ファイルに書き込むときの詳細レベル。たとえば［Fatal］を選択すると、重大なエラーのみがログ ファイルに書き込まれます。
［Log File］	ホスト上のログ ファイルの場所。
［Max Log File Size (MB)］	ログ ファイルの最大サイズ。このサイズに達すると、新しいログ ファイルが作成されます（MB 単位）。ログ ファイルのサイズを無制限にするには、この値を 0 に設定します。
［Max Number of Log Files］	システムに保持するログ ファイルの最大数。現在のログ ファイルのサイズが最大値を超過した結果、新しいファイルが作成されると、最も古いログ ファイルが削除される。
［Max Forward Queue Length］	サーバーがオフラインの場合に、エージェントによりローカルに格納される最大リクエスト数。
［Max Forward Queue Size (MB)］	サーバーがオフラインの場合に、DPA データ コレクション エージェントによりローカルに格納される全リクエストの最大合計サイズ（MB 単位）。無制限を指定するか、選択したサイズを指定できます。
［Reload Data Collection Agent］	データ コレクション エージェントを手動で再ロードできる。この操作は、データ コレクション エージェントに影響する構成の変更が、DPA Web コンソールで行われた場合に自動的に実行されます。
［Remove Data Collection Agent］	選択したデータ コレクション エージェントを削除します。
［Make Agent Default］	選択したデータ コレクション エージェントをデフォルト ホストにします。

表 24 サーバー設定

設定		説明
グローバル データ コレクション エージェント設定	［Binary Multiplier］	このグローバル設定をオンに切り替えると、デフォルトによりすべてのエージェントでバイナリ乗数が使用されるようになります。バイナリ マルチプライアは、すべての入力データを 1024 KB = 1 MB として変換します。バックアップ サーバーからの入力データが 1000 KB = 1 MB として変換される場合のみ NetWorker エージェントに適用されます。他のアプリケーションを監視する場合、バイナリ マルチプライアは無視されます。
	［Timeout(s)］	エージェントと対話するときにサーバーが使用するタイムアウト設定。デフォルトは 120 秒です。
グローバル メール設定	メール サーバーのホスト名	DPA から送信する際の、メール メッセージの転送先メール サーバー。
	［Mail From Address］	DPA から送信されたメール メッセージに割り当てられたメール アドレス。

表 24 サーバー設定 （続き）

設定		説明
	［Mail Server Port］	メール サーバーのポート番号。
［Global Logging Settings］	［Global Logging Settings］	解析エンジン、構成、リスナー、パブリッシャ、復旧可能性解析、レポーター、および REST API のグローバル ログ設定。設定は、INFO、DEBUG、DEBUG LOW、WARN、ERROR、FATAL です。
［Data Deletion］	［Data Deletion］	環境から収集したデータを削除するスケジュール。デフォルトは、毎日午前 9 時～午後 5 時です。
根本原因分析	［Root Cause Analysis Settings］	［Root Cause Analysis Summary］を有効化するオプション。
		［Root Cause Analysis Deletion］を有効化するオプション。デフォルトの削除設定では、200 日より前のデータが削除されます。期間はユーザーが構成できます。
サポート バンドルの生成	サポート バンドルの生成	サポート zip ファイルを生成するオプション。
	［Include all logs］	すべてのログを含めるオプションです。選択されていない場合、DPA は最新のログ ファイルのみを収集します。選択した場合、DPA はすべての履歴ログ ファイルを収集します。デフォルトでは、選択されません。
DB エクスポート	データベース エクスポート経過通知	DPA データベース エクスポートが最新と見なされる期間を設定するオプションです。 デフォルト値は 1 週間です。最小値は 1 日です。 この期間が経過して、期間中に新しい DPA データストアのエクスポートがなければ、アラートが発行されます。

表 25 SharePoint 設定

設定		説明
［Name］	［Name］	DPA SharePoint Server 設定で作成した SharePoint サイトのユーザー定義名。
サイト	［Site URL］	公開用の SharePoint の宛先 URL HTTP プロトコルのデフォルト ポートは 80、HTTPS のデフォルトは 443 です。 明示的にポートを指定することもできます。たとえば、http ポート 24438 をサイト URL に設定するには、次のように入力します。 **`http://sharepoint-2013:24438/sites/demo2/`**

表 25 SharePoint 設定 （続き）

設定		説明
ユーザー	［Username］	SharePoint のアカウントに関連づけられたユーザー名

表 26 レプリケーション解析設定

設定		説明
レプリケーション解析	［Client-Server Time Difference］	デフォルトは 10 分です。
	［Symmetrix and CLARiiON Log Level］	Symmetrix および CLARiX のログ設定 INFO と DEBUG を設定できます。
	［Support Symmetrix Masking Reports］	Symmetrix マスキング レポートのサポートを有効にします。デフォルトで有効化されます。
	［Support Application Discovery Impersonation］	アプリケーション検出偽装のサポートを有効にします。デフォルトで有効化されます。
表示設定	［Display dirty Recovery Points］	ダーティ リカバリ ポイントの表示を有効にします。デフォルトで有効化されます。
	［Aggregate Recovery Points］	リカバリ ポイントの統合を有効にします。デフォルトで有効化されます。
	［Minimum number of recovery points to aggregate］	デフォルトは 3 です。最小値は 1 です。最大値はありません。

エージェントレスでの検出機能

エージェントレスでの検出設定を次の表で説明します。

表 27 エージェントレス検出の設定

設定	説明
［Sudo Program Path］	エージェントを使用しない検出設定の sudo プログラム パス。デフォルト パスは`/usr/local/bin/sudo` です。sudo コマンドは `/sbin` または `/usr/sbin` にある場合もあります。

表 27 エージェントレス検出の設定 （続き）

設定	説明
［Agent Response Timeout］	タイムアウトまでに、エージェントからのレスポンスを DPA が待機する時間。
［Telnet/SSH Login Prompt Timeout］	タイムアウトまでに、Telnet/SSH セッションが計算されるのを DPA が待機する時間。
［Telnet/SSH Handshake Timeout］	タイムアウトまでに、Telnet/SSH のハンドシェイクを DPA が待機する時間。
［Delete files created on the client during agentless discovery］	検出の終了時に、分析されたオブジェクトから一時ファイルを削除するかどうかが定義されます。 デフォルトでは、ファイルは削除されます。

サーバー データの削除

DPA には、収集データおよびシステム生成データの、デフォルトのデータ削除スケジュールが実装されています。収集データとは、［Manage Data Collection Defaults］ 内で構成されるリクエストによって収集されるデータです。システム生成データとは、ログ メッセージ、レポート履歴、アラートなどのシステム プロセスによって生成されるデータです。

データが保存期間を過ぎると、削除の対象となります。このデータは、データ削除スケジュールに基づいて消去されます。未処理項目は次のスケジュール設定された開始時刻までキューに残り、この時点でデータの削除が続行されます。

収集データの削除ジョブのスケジュール設定に現在使用されているスケジュールは削除できません。削除しようとすると、エラー メッセージが表示されます。

削除される収集データやシステム生成データは、たとえば次のように `server.log` でトラッキングされます。

```
Deleted 10 rows from table host_config
Deleted 10 rows from Request History
Deleted 10 rows from reportlogentry
Deleted 10 rows from dpa_request_statistics
Deleted 10 rows from reporterjob
```

デフォルトのデータ削除スケジュールは、毎日午前 9 時～午後 5 時です。

データ削除スケジュールの構成

［Schedule Properties］ で、使用する新しいスケジュールを構成および指定できます。

データ削除を構成するには、［**Admin**］ > ［**System**］ > ［**Configure System Settings**］ > ［**Server**］ > ［**Data Deletion**］ の順に選択します。詳細については、DPA オンライン ヘルプを参照してください。

デフォルトの保存期間

次の表に、収集データのデフォルトの保存期間に関する情報を示します。

表 28 収集データのデフォルトの保存期間

システム情報	デフォルトの保存期間
構成データ	365 日間
ステータス データ	90 日間
パフォーマンス・データ	30 日
ジョブ データ	無期限
占有率データ	365 日間

収集データのデフォルトの保存期間は、［**Admin**］>［**System**］>［**Manage Data Collection Defaults**］でユーザーが構成できます。

次の表に、システム生成データのデフォルトの保存期間に関する情報を示します。システム生成データのデフォルトの保存期間を、ユーザーが構成することはできません。

表 29 システム生成データのデフォルトの保存期間

ポリシー	デフォルトの保存期間
アラート（analysisalert 表）	365 日間
レポート履歴（reporterjob 表）	365 日間
エージェント エラー ログ エントリ（reportlogentry 表）	14 日
リクエスト統計情報（dpa_request_statistics 表）	28 日

Root Cause Analysis Settings

［Root Cause Analysis Summary］を設定して、［Systems Settings］から定期的なスケジュールで可能性のある根本原因を判断できます。根本原因解析の結果データを削除するようにシステムをスケジュールすることもできます。［Root Cause Analysis Deletion］設定では、200 日より前のデータが削除されます。期間はユーザーが構成できます。［Root Cause Analysis Summary］および［Root Cause Analysis Deletion］はデフォルトで有効化されます。

［Root Cause Analysis Summary］の無効化

［**Admin**］>［**System**］>［**Configure System Settings**］>［**Server**］>［**Root Cause Analysis Settings**］>［**Disable Root Cause Analysis**］の順に選択し、［**OK**］をクリックします。

［Root Cause Analysis Deletion］の無効化

［**Admin**］>［ **System**］>［**Configure System Settings**］>［**Server**］>［**Root Cause Analysis Settings**］>［**Disable Root Cause Analysis Deletion**］の順に選択し、［**OK**］をクリックします。

DPA Web コンソールを使用した履歴のバックアップ データの収集

Avamar、BackupExec、DB2、HP DataProtector、NetWorker、NetBackup、Oracle RMAN、SAP HANA、TSM では、履歴のバックアップ データを収集できます。

DPA Web コンソールを使用して履歴のバックアップ データを収集するときは、次の点を考慮します。

- ホスト単位では履歴のバックアップ データを収集できません。構成ツリーで 1 段階下に相当するアプリケーション オブジェクトのレベルで対応する必要があります。たとえば、NetWorker から履歴のデータを収集するには、ホスト レベル オブジェクトの下に相当する Networker のアプリケーション オブジェクトを選択します。
- 履歴のバックアップは、JobMonitor リクエストからのみ収集できます。

手順

1. Web コンソールで、［**Inventory** ］ > ［**Group Management**］の順に選択します。
2. 構成ツリーで、履歴のバックアップ データを収集するアプリケーション オブジェクトを選択します。

   アプリケーション オブジェクトの［**Details**］ウィンドウが開きます。
3. ホスト詳細ウィンドウで、［**Data Collection**］タブを選択します。
4. ［**Data Collection**］で、JobMonitor リクエストを選択します。
5. ［**Run**］を右クリックし、［**Gather historical data**］を選択します。
6. ［ **Gather historical data** ］ウィンドウで ［**OK**］をクリックします。

   同じ認証情報とデータ オプションはリクエスト自体で使用できます。
7. ［**Close**］をクリックすると、DPA が履歴のバックアップ データを収集していることを確認するダイアログ ボックスが表示されます。
8. ［**History**］をクリックして収集されたテストを表示します。オレンジ色でハイライト表示されている行に、履歴のバックアップの収集結果が示されています。

サポート バンドルの生成

［Generate Support Bundle］オプションはサポート ツールです。［Generate Support Bundle］では、ファイル システムに提供されているリソースの zip アーカイブを DPA Web コンソールから直接生成および保存します。

分析のために、EMC テクニカル サポート エンジニアから、サポート バンドルの生成とその送信を求められることがあります。zip ファイルは、`support.zip` フォルダに次のローカル エージェント ログとして保存されています。

- dpaagent.log
- dpaagent.log.0
- dpaagent.log.1

デフォルトの場所はユーザーが構成できます。

サポート バンドルの生成

手順

1. ［**Admin**］>［**System**］>［**Configure System Settings**］>［**Server**］>［**Generate Support Bundle**］の順に選択し、［**OK**］をクリックします。

2. プロンプトが表示されたら、DPA 管理者資格情報を入力します。

デジタル証明書

DPA では、識別および暗号化のために自己署名デジタル証明書が使用されます。DPA アプリケーション サーバーの暗号化（64 ページ）に情報が提供されています。

期間

レポートを実行するか、スケジュール設定されたレポートを作成する場合は、どの期間についてレポートを実行するのか、たとえば直ちに、または先週、を決定する必要があります。デフォルトでは定義済みの期間がいくつか提供されおり、カスタム期間を作成することができます。

レポートのカスタム期間の作成

カスタム期間を作成するには、［**Admin**］ > ［**System**］ > ［**Manage Time Periods**］の順に選択します。

DPA のタイム ゾーン

DPA は環境のデータを収集し、収集したデータを UTC 形式で DPA データベースに格納します。

DPA データベースがバックアップ サーバー、アプリケーション、ホスト、またはスイッチから受信するタイムスタンプが東部標準時など、ローカル タイム ゾーンで付与される場合、DPA エージェントはそのタイム スタンプを UTC に変換してから DPA サーバーに送信します。そのデータに関するレポートの作成については、設定可能な設定がいくつかあります。レポートのタイム ゾーンの設定（95 ページ）で詳細を参照してください。

レポートのタイム ゾーンの設定

次のタイム ゾーン設定により、DPA レポートに確実に目的のタイム ゾーンを表示できます。

検出されたオブジェクトの詳細
［Discovery Wizard］を使用してオブジェクトを検出した後は、プロパティを選択し、そのオブジェクトの配置場所のタイム ゾーンを指定できます。検出されたオブジェクトの［**Details**］ウィンドウで、ドロップダウン リストから［**Time zone**］を選択します。

ユーザー環境設定
［**User Preferences**］ > ［**View User Properties**］ > ［**Preferences**］の順に移動して、データを表示するタイム ゾーンを選択できます。［Global Settings］セクションの［**Time zone**］ドロップダウン リストで、タイム ゾーンを選択します。

Windows のプロパティ
タイム ゾーンに対応した期間を作成できます。［**Window Properties**］ウィンドウで、新しい期間を作成し、［**Adjust for time zone**］オプションが選択されていることを確認します。［**Adjust for time zone**］が選択され、オブジェクトがバックアップ クライアントの場合、そのバックアップ クライアント自体にまだタイム ゾーンが明示的に設定されていなければ、DPA は親バックアップ サーバーをチェックして、タイム ゾーンに対応したレポートを作成します。

表形式のレポート
表形式のレポートを構成することを選択し、バックアップ サーバーの名前を検索するために参照するフィールドを指定することにより、タイムスタンプ付きで実行された Time Zone オブジェクトを表示できます。レポート エディターで、［**Report Format**］ > ［**Table Format**］ > ［**Table Styles**］の順に移動します。［Data Fields］セクションの下で［**Time Zone from Report Field**］オプションが選択されていることを確認します。

例：All Jobs レポートのタイム ゾーンの設定

この例では、All Jobs レポートのタイム ゾーンを、米国/ニューヨークのタイム ゾーンに配置された NetWorker サーバー向け、および欧州/ロンドンのタイム ゾーンに配置されたデータベース管理者向けに設定する方法を示しています。

何も設定を変更しないうちは、すべてのレポートと表示出力は UTC で表示されます。

手順

1. ［**User Preferences** ］ > ［**View User Properties**］ > ［ **Preferences**］の順に移動し、［Global Settings］セクションの［**Time zone**］ドロップダウン リストから［**Europe/London**］を選択します。［**OK**］をクリックします。

   NetWorker サーバーで All Jobs レポートを実行すると、DPA が結果レポートを UTC で表示します。

2. New York にある NetWorker サーバーのタイム ゾーンを以下の手順で更新します。

   a. ［**Inventory**］ > ［**Object Library**］の順に選択して、NetWorker ホストまで移動します。

   b. 目的の NetWorker ホストを選択し、［**Details**］ウィンドウで［**Time zone**］ドロップダウン リストから［**America/New York**］を選択します。

   c. ［**OK**］をクリックします。

   ユーザーのタイム ゾーン設定やレポートの設定がまだ変更されていないため、この時点での出力は UTC のままです。米国/ニューヨークのタイム ゾーンには変更されません。

3. タイム ゾーンに対応したカスタム期間を作成します。［**Window Properties**］に移動して、カスタム タイム ゾーンを作成します。`Adjust for time zone` オプションを選択していることを確認します。

   この結果、オブジェクトのタイム ゾーンを基準とした時刻のレポート クエリーが作成されます。したがって、NetWorker サーバーがニューヨークにあるため、DPA はニュー ヨークのタイム ゾーンで、カスタム期間のクエリーを実行します。

4. 各日付フィールドが、［Server］フィールドのタイム ゾーンで目的の日付形式で表示されるように、レポートの表形式を編集します。

   a. レポート エディターで［**Report Format**］ > ［**Table Format**］ > ［**Table Styles**］の順に移動します。

   b. ［Date Fields］セクションの下で［**Date Format**］ドロップダウンから目的の日付形式を選択し、`Time Zone from Report Field` オプションが選択されていることを確認します。

   c. ［**OK**］をクリックします。

   DPA が、NetWorker サーバーのタイム ゾーン（この例では米国/ニューヨーク）のタイム スタンプで、レポートを更新します。

レポートの自動的な優先順位づけ

DPA アプリケーション サーバーあたりの同時実行できるレポートのデフォルト数は 10 です。このデフォルト設定は構成できます。DPA アプリケーション サーバーあたりの同時実行できるレポートの最大数は 50、最小数は 2 です。

DPA では、同時実行がスケジュール設定されているレポートや同時実行されているレポートが自動的にキューに入れられ、前にスケジュール設定されているレポートの実行後に、自動的にレポートが再試行されます。また、Web コンソールから開始するレポートは、サーバーから実行される自動的な

スケジュール設定されたレポート（スケジュール設定されたアラートのテストを含む）より優先されます。

Web コンソールから実行されるレポートが優先されるほか、これらのレポート用に、最低 30%の固定の同時スペースがサーバー上に予約されます。たとえば、同時セットが 10 個の場合、サーバー上では 3 個の同時実行スペースが Web コンソール レポート用に予約されます。このため、最大 10 個の Web コンソール レポートのうち、3 個以上を特定の時点で同時に実行できます。同時に実行できるスケジュール設定されたレポートは、7 個しかありません。

コンカレント レポートの設定

手順

1. コンカレント レポートの設定を構成するには、［**Admin**］ > ［**System**］ > ［**Configure Report Settings**］ > ［**Concurrency**］の順に選択します。

必要条件

DPA Web コンソールで同時使用率の設定を変更した後は、必ず DPA アプリケーション サービスをリスタートします。クラスタ環境では、すべての DPA アプリケーション サーバーをリスタートします。これで、レポート エンジン サービスに同時使用率の新しい値を反映させることができます。

スケジュール

スケジュールは、スケジュール設定されたレポートをいつ実行するのか、またはダッシュボード ビュー ブロックをいつ生成するのかを定義したり、［Protection Policy］で指定されたバックアップ ウィンドウを定義したりするために使用されます。デフォルトでは定義済みのスケジュールがいくつか提供されており、カスタム スケジュールを作成することもできます。

スケジュールは、各スケジュールが特定の結果を生成したり、特定のレポートを実行する時刻を定義するコンポーネントで構成されています。スケジュール エディタを使用すると、2 種類の方法でスケジュールを作成できます。

- 基本エディタ：週単位でのみスケジュールを作成し、スケジュールの日時を編集できます。
- 拡張エディタ：スケジュール パラメータを手作業で編集することにより、さらに複雑なスケジュールを作成できます。

基本エディタで作成したスケジュールは、拡張エディタを使用して編集できます。ただし、拡張エディタで作成し保存したスケジュールを基本エディタで編集できません。

スケジュールの作成

スケジュールを作成するには、［**Admin**］ > ［**System**］ > ［**Manage Schedules**］の順に選択します。

Manage Data Collection Defaults

DPA リクエストには、いつ、どのようにデータをオブジェクトから収集するかについてのデータが入っています。データ コレクションのデフォルトは、［Discovery Wizard］がオブジェクトへのリクエストの割り当てに使用するテンプレートです。［**Admin**］ > ［**System**］ > ［**Manage Data Collection Defaults**］でグローバル デフォルト設定を設定できます。

すべてのリクエストには、データ収集頻度とリクエストに関連する一連のオプションがデフォルトとして設定されています。特定のオブジェクトについて、［Discovery Wizard］で取得するグローバル データ コレクションのデフォルト値を編集できます。DPA オンライン ヘルプでは、リクエストの編集に関する情報が提供されています。

監視対象デバイスにエージェントを配置せずに、DPA を使用して特定のタイプのデータを収集できます。これを行うには、別のコンピューター（DPA サーバーなど）にあるエージェントで、データをリモー

トで収集します。リモートでデータを収集する場合は、エージェントのホストはプロキシ サーバーと見なされます。エージェントはプロトコルを使用してリモート コンピューターからデータを収集し、そのデータを DPA サーバーに転送して戻します。使用されるプロトコルは、収集するデータのタイプに応じて異なります。

IP スイッチやファイバー チャネル スイッチなどの特定のデバイス タイプでは、スイッチにエージェントを直接インストールすることができないため、常にリモートでデータを収集する必要があります。

DPA 内でリモート データ収集を構成するには、リクエストの割り当て時に詳細を構成します。［Discovery Wizard］でオブジェクトを作成した場合は、この構成はすでに作成されています。ただし、プロキシまたは認証情報の詳細を変更した場合は、必要に応じてその詳細を変更します。［Retention Periods on Requests］が、［Edit Request］ダイアログ ボックスを使用して個々のリクエストに設定されています。データ コレクション ポリシーのデフォルトの保存期間については、表 15 を参照してください。

モジュール別データ コレクション リクエスト オプション

以下の表では、モジュール別データ コレクション リクエスト オプションについて説明します。

表 30 モジュール別データ コレクション リクエスト オプション

モジュール	オプション名	値	説明
ARCserve	dateformat	%d/%m/%Y %T（日、月、年、時刻）。	使用する日付形式。 `dateformat` オプションは、次のリクエストのオプションの中に存在する。 • ジョブ監視 • ボリュームの状態 注意 1 に、時刻の形式に関する追加情報を記載しています。
Avamar	capacityfactor	1.075	Avamar の小数の容量係数。 `capacityfactor` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	dbname	mcdb	データベース名 `dbname` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ジョブ監視 • ステータス リクエスト
	dbport	5555	データベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ジョブ監視 • ステータス リクエスト

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
	ジョブ コレクション内の秒数	86400	Jobmonitor を 1 回実行するごとにリクエストがジョブ データを収集する最大時間を変更します。デフォルトは 1 日の秒数である 86400 です。値は変更可能です。
Backup Exec	dbserver	デフォルト値なし	データベース サーバー インスタンス。`dbserver` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ジョブ監視 • ステータス • ボリュームの状態
CLARiX VNX	コネクタ	デフォルト値なし	CLARiX 情報インポート リクエストのコネクタを示す
	EventLog History Polling	21	それを過ぎると CLARiX 情報インポート リクエストのポーリングに含まれなくなる、データの経過時間（日数）
Celerra	port	デフォルト値なし	整数の HTTPS/HTTP ポート番号。`port` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
	secure	True	HTTP ではなく HTTPS を使用してリクエストを送信することを示す。`secure` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	timeout	1800	HTTP リクエストのタイムアウト（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
CommVault Simpana	appversion	0	使用する CommVault Simpana のバージョン。`appversion` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • Client Occupancy

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• ジョブ監視 • ステータス • ボリュームの状態
	dbserver	デフォルト値なし	DB サーバー名。`dbserver` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • Client Occupancy • ジョブ監視 • ステータス • ボリュームの状態
	setBackupJobsWithErrsToSuccess	False	True に設定すると、Completed w/one or more errors ステータスで完了した CommVault バックアップ ジョブが成功ジョブとして DPA により報告されます。`setBackupJobsWithErrsToSuccess` オプションはジョブ監視リクエスト内にあります。
Data Domain	timeout	10	SSH タイムアウト値（秒）。SSH の `timeout` オプションは、次のリクエストのオプションの中に存在する。 • 分析 • 構成 SSH • パフォーマンス SSH • ステータス SSH • SSH PCR
	timeout	10	SNMP タイムアウト値（秒）。SNMP の `timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
DataProtector	timeout	900	構成リクエストのコマンドを実行するためのタイムアウト値（秒）
	timeout	300	コマンドを実行するためのタイムアウト値（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 内部データベース

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• ジョブ監視 • Service Status • ステータス • ボリュームの状態
	ignorefailedclones	False	ジョブ監視リクエストの失敗したクローン ジョブでソース オブジェクトについての情報を収集しないことを示す
	nojobmedia	False	ジョブ監視リクエストで各ジョブに関連づけられたメディア情報を収集しないことを示す
	occupancy	False	ジョブ監視リクエストで占有統計情報の収集を有効化することを示す
	timeformat	デフォルト値なし	ジョブ監視リクエストでの omnidb の時刻の形式。 注意 2 に、時刻の形式に関する追加情報を記載しています。
DB2	ジョブ コレクション内の秒数	86400	Jobmonitor を 1 回実行するごとにリクエストがジョブ データを収集する最大時間を変更します。デフォルトは 1 日の秒数である 86400 です。値は変更可能です。
	データベース ポート	50000	データベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • ジョブ監視
EDL	timeout	10	SNMP タイムアウト値（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
ファイバ チャネル スイッチ	timeout	10	SNMP タイムアウト値（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
Host System Monitoring	ディスク	True	構成およびレプリケーション リクエストでホスト ディスク情報を含めることを示す

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
	ESXRequestParameters.ESX_CREDENTIALS	デフォルト値なし	構成およびレプリケーション リクエストの VMware ESX サーバー認証情報
	ESXRequestParameters.ESX_SERVER	デフォルト値なし	構成およびレプリケーション リクエストで使用される ESXServer サーバーの名前
	fchba	True	ホスト FC HBA 情報を含める。`fchba` オプションは、次のリクエストのオプションの中に存在する。 • 構成およびレプリケーション • パフォーマンス • ステータス
	fs	True	ホスト ファイル システム情報を含める。`fs` オプションは、次のリクエストのオプションの中に存在する。 • 構成およびレプリケーション • パフォーマンス • ステータス
	host	True	基本ホスト情報を含める。`host` オプションは、次のリクエストのオプションの中に存在する。 • 構成およびレプリケーション • ステータス
	logical	False	論理ネットワーク インターフェイスを含める。`logical` オプションは、次のリクエストのオプションの中に存在する。 • 構成およびレプリケーション • パフォーマンス • ステータス
	メモリー	True	ホスト メモリー情報を含める。`memory` オプションは、次のリクエストのオプションの中に存在する。 • 構成およびレプリケーション • パフォーマンス • ステータス
	netint	True	ホスト ネットワーク インターフェイス情報を含める。`netint` オプションは、次のリクエストのオプションの中に存在する。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• 構成およびレプリケーション • パフォーマンス • ステータス
	remote	False	リモートにマウントされたファイル システムを含める。`remote` オプションは、次のリクエストのオプションの中に存在する。 • 構成およびレプリケーション • パフォーマンス • ステータス
	REPLICATION_MONITORING_OPTION	False	構成およびレプリケーション リクエストのレプリケーション監視の有効化
	srm	True	構成およびレプリケーション リクエストで disk/fs 情報のために srm ライブラリを利用する
	Time Offset(seconds)	0	構成およびレプリケーション リクエストの時間オフセット（秒）
	ディスク	True	ホスト ディスク情報を含める。`disk` オプションは、次のリクエストのオプションの中に存在する。 • パフォーマンス • ステータス
	fullpath	False	ステータス リクエストのプロセス名のフル パスを含める
	process	True	ステータス リクエストでプロセス実行ホストの情報を含める
	specific	デフォルト値なし	ステータス リクエストのみで指定のプロセスを監視する（Windows のみ）。
illuminator clarapi エンジン検出	TIME_OFFSET_OPTION	0	illuminator clarapi エンジン検出リクエストの時間オフセット（秒）
HP ディスク アレイ	port	5989	HP EVA ディスク アレイの CIM プロバイダー ポート。`port` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
HP 仮想ライブラリ システム	port	5989	HP VLS ディスク アレイへのポート。`port` オプションは、次のリクエストのオプションの中に存在する。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• 構成 • ステータス
	SSLflag	True	HP VLS ディスク アレイに対する SSL フラグの有効化。`SSLflag` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	timeout	600	HP VLS ディスク アレイのタイムアウト（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
illuminator symapi エンジン検出	Symapi Version	デフォルト値なし	illuminator symapi エンジン検出リクエストの SYMAPI バージョンを示す
	TIME_OFFSET_OPTION	0	時間オフセット（秒）。`TIME_OFFSET_OPTION` オプションは、次のリクエストのオプションの中に存在する。 • illuminator symapi エンジン検出 • symmetrix 情報インポート
	Allow Management over SRDF	False	illuminator symapi エンジン検出リクエストで SRDF の管理を許可する。
	SYMAPI DB Path	デフォルト値なし	illuminator symapi エンジン検出リクエストの SYMAPI データベース パスを示す
IP スイッチ	timeout	10	ステータス、パフォーマンス、構成リクエストのタイムアウト値（秒）
SQL Server データベース	dbparams	デフォルト値なし	データベースごとのパラメーター/認証情報を指定する XML。`dbparams` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ジョブ監視 • ステータス
	dbport	1433	データベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• 構成 • ジョブ監視 • ステータス
	HomeDir	デフォルト値なし	mssql アプリケーション検出リクエストのアプリケーション ホーム ディレクトリ情報
	Tools Director	デフォルト値なし	mssql アプリケーション検出リクエストのツール ディレクトリ プロパティ情報
	Virtual Computer Name	デフォルト値なし	mssql アプリケーション検出リクエストの仮想コンピューター名プロパティ情報
NearStore	timeout	10	SNMP タイムアウト値（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
NetBackup	timeout	3600	コマンド タイムアウト（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • Client Occupancy • 構成 • ジョブ監視 • メディア サーバーのステータス • ステータス • ボリュームの状態
	timeout	30	コマンド タイムアウト（分単位）。`timeout` オプションは、SLP ジョブ ステータス リクエストのオプションの中にあります。
	EMMserver	デフォルト値なし	EMM（Enterprise Media Manager）のホスト名。マスター サーバー ホストでない場合にのみ必要。`EMMserver` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	timeformat	デフォルト値なし	構成リクエストのライセンス有効期限の日付と時刻の形式

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
	timeformat	デフォルト値なし	ジョブ監視リクエストの bpdbjobs の時刻形式 注意 1 と 2 に、時刻の形式に関する追加情報を記載しています。
	partialasfailed	False	ジョブ監視リクエストで部分的に成功したジョブを失敗とマークする
	Whether to include container jobs	False	`True` に設定すると、DPA は子ジョブのほかに、親/コンテナ ジョブの行も収集します。デフォルト リクエストまたは個々のオブジェクトで設定が可能です。
	command timeout	300	データ収集のための外部コマンドの実行に使用されるタイムアウト（秒）。 `command timeout` オプションは、SLP ジョブ ステータス リクエストの中にあります。
	Max data time range each request will gather	86400	SLP ジョブ ステータスを 1 回実行するごとにリクエストがジョブ データを収集する最大時間を変更します。デフォルトは 1 日の秒数である 86400 です。値は変更可能です。
NetWorker	command timeout	3600	データ収集のための外部コマンドの実行に使用されるタイムアウト（秒）。 `command timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス • ClientStatus • JobMonitor • 占有 • ボリュームの状態
	mminfo timeformat	デフォルト値なし	メディア データベースのタイム スタンプを bpdbjobs 時刻形式で返す形式。ジョブの開始時刻と終了時刻のデコードに使用されます。デフォルトでは、このオプションは無効で、モジュールは値の自動計算を行います。 `mminfo timeformat` オプションはジョブ監視リクエスト内にあります。
	include jobs from media DB	True	NetWorker メディア データベースからの成功ジョブの検索をオフにできます。DPA

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			は、NetWorker ジョブ データベースのほかに、メディア データベースから完了したジョブを検索します。バックアップの開始に外部スケジューラを使用しない場合は、これを `False` に設定することで、ジョブ監視リクエストの実行を高速化します。 `include jobs from media DB` オプションはジョブ監視リクエスト内にあります。
	各リクエスト データ ポーリングの最大バッチ期間	86400	Jobmonitor を 1 回実行するごとにリクエストがジョブ データを収集する最大時間を変更します。デフォルトは 1 日の秒数である 86400 です。値は変更可能です。
NetWorker	individual ping timeout	10	バックアップ クライアントからの ping 応答のタイムアウトに使用されるタイムアウト（秒）。 `individual ping timeout` オプションは、クライアント ステータス リクエスト内にあります。
	nsrexecd port	7937	NetWorker クライアント プロセスのリスン ポート。 `nsrexecd port` オプションは、クライアント ステータス リクエスト内にあります。
	Number of concurrent pings	20	一度に ping を実行するクライアントの数。 `Number of concurrent pings` オプションは、クライアント ステータス リクエスト内にあります。
	List of critical clients to ping	デフォルト値なし	コンマで区切った、ping 対象の重要なクライアントのリストを保持しているファイルの名前。 `List of critical clients to ping` オプションは、クライアント ステータス リクエスト内にあります。
	Path and name of file used to store temporary occupancy data before processing	デフォルト値なし	処理の前に一時占有データを格納するためのファイルのパスと名前。値は、エージェント ホストの有効なパスである必要があります。Windows の `C:\temp` や UNIX/Linux の `/tmp` など。場合によっては、オプションを有効にするために、設定後にエージェントを再起動する必要があります。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			`Path and name of file used to store temporary occupancy data before processing` オプションは、占有リクエスト内にあります。
	Forces short client names	true/false	短いバージョンのクライアント名を返すかどうか。 `Forces short client names` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス • ClientStatus • JobMonitor • ClientOccupancy
	time format used to determine bootstrap time	False	NetWorker から結果で返されるタイム スタンプをデコードするための時刻形式を指定します。デフォルトでは、このオプションは無効で、モジュールは最適と推測される方法で時刻形式をデコードします。 `time format used to determine bootstrap time` オプションは、ステータス リクエスト内にあります。
	time format used to determine volume access time	False	ボリュームに最後にアクセスされた時刻のタイム スタンプをデコードするときに使用する時刻形式。デフォルトでは、このオプションは設定されず、モジュールは時刻形式を自動で計算します。 `time format used to determine volume access time` オプションはボリューム リクエスト内にあります。
	time format used to determine volume retention period	False	ボリュームの保存時刻のタイム スタンプをデコードするときに使用する時刻形式。デフォルトでは、このオプションは設定されず、モジュールは時刻形式を自動で計算します。 `time format used to determine volume retention period` オプションはボリューム リクエスト内にあります。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
	Whether to include failed jobs which are retried	False	DPA エージェントは、バックアップ ジョブの最終ステータスのみを収集します。 このジョブ オプションを `False` に設定して、ジョブ実行の前に長い遅延があると、再試行が失敗して、ジョブ失敗の報告が遅れます。再試行が成功すると、DPA データベースにはジョブのエントリーが 1 つ記録され、ジョブが成功として示されます。 このジョブ オプションを `True` に設定すると、DPA エージェントはすべての失敗した試行とジョブの最終ステータスを収集して、DPA データベースに送ります。たとえば、ジョブが 1 回再試行して成功すると、DPA データベースにはジョブの 2 つのエントリーが記録されます (1 つは失敗、1 つは成功)。試行がともに失敗すると、DPA データベースは 2 つのジョブ エントリーがともに失敗であると DPA データベースに記録します。 All Jobs - No Restarts レポートを使用すると、失敗した試行がフィルターされ、ジョブの最終ステータスのみを表示できます。
Oracle	dbparams	デフォルト値なし	スキーマごとのパラメーター/認証情報を指定する XML。`dbparams` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	dbport	1521	整数のデータベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	HomeDir	デフォルト値なし	Oracle アプリケーション検出リクエストのアプリケーション ホーム ディレクトリ情報
	ArchivesPattern	デフォルト値なし	Oracle アプリケーション検出リクエストのアプリケーション アーカイブ パターン情報
	LogPattern	デフォルト値なし	Oracle アプリケーション検出リクエストのアプリケーション ログ パターン情報
	LogsDir	デフォルト値なし	Oracle アプリケーション検出リクエストのアプリケーション ログ ディレクトリ情報

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
PostgresSQL データベース	dbparams	デフォルト値なし	スキーマごとのパラメーター/認証情報を指定する XML。`dbparams` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	dbport	5432	データベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	initialdb	postgres	このポートに接続する初期データベース。`initialdb` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
PureDisk	dbport	10085	データベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • Client Occupancy • 構成 • ジョブ監視
	dbserver	デフォルト値なし	データベース サーバー ホスト。`dbserver` オプションは、次のリクエストのオプションの中に存在する。 • Client Occupancy • 構成 • ジョブ監視
RecoverPoint	scanforrecover	False	構成リクエストの復旧可能性のスキャン
	Time Offset (in seconds)	0	構成リクエストのタイム オフセット（秒）
	timeout	300	SSH タイムアウト値（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス cs • パフォーマンス

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
	filename	long_term_stats.tar.gz	パフォーマンス cs リクエストの統計ファイル名
	workdir	../tmp	パフォーマンス cs リクエストの作業ディレクトリ
RecoverPoint for VMs	Time Offset (in seconds)	0	構成リクエストのタイム オフセット（秒）
	timeout	300	REST API のタイムアウト値（秒単位）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス CS • パフォーマンス • ステータス
RMAN	dbport	1521	Oracle TNS リスナー ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • ジョブ監視制御ファイル • ジョブ監視リカバリ カタログ
	ジョブ コレクション内の秒数	86400	Jobmonitor を 1 回実行するごとにリクエストがジョブ データを収集する最大時間を変更します。デフォルトは 1 日の秒数である 86400 です。値は変更可能です。
	RMAN スキーマ	デフォルト値なし	
SAP HANA	データベース ポート	30115	ジョブ監視リクエストのデータベース ポート
	ジョブ コレクション内の秒数	86400	Jobmonitor を 1 回実行するごとにリクエストがジョブ データを収集する最大時間を変更します。デフォルトは 1 日の秒数である 86400 です。値は変更可能です。
Symmetrix	コネクタ	デフォルト値なし	Symmetrix 情報インポート リクエストのコネクタを示す
	Gather HBA Information	True	Symmetrix 情報インポート リクエストの HBA 情報を収集する
	Time Offset (in seconds)	0	構成リクエストのタイム オフセット（秒）
	Symaudit History Polling	21	この期間を過ぎると Symaudit リクエストのポーリングに含まれなくなる、データの経過時間（日数）

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
テープ ライブラリ	timeout	10	SNMP タイムアウト（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
TSM	timeout	デフォルト値なし	TSM サーバーに送信されたコマンドの内部タイムアウト（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • Client Occupancy • ジョブ監視 • プロセス監視 • ボリュームの状態
	timeout	3600	構成リクエストで TSM サーバーに送信されたコマンドの内部タイムアウト（秒）
	timeout	900	ステータス リクエストで TSM サーバーに送信されたコマンドの内部タイムアウト（秒）
	tsmhost	デフォルト値なし	TSM サーバーのホスト名。`tsmhost` オプションは、次のリクエストのオプションの中に存在する。 • Client Occupancy • 構成 • ジョブ監視 • プロセス監視 • ステータス • ボリュームの状態
	tsmport	1500	TSM サーバーのポート。`tsmhost` オプションは、次のリクエストのオプションの中に存在する。 • Client Occupancy • 構成 • ジョブ監視 • プロセス監視 • ステータス • ボリュームの状態
	disableprivatevolumes	False	プライベート ボリュームのレポート作成を無効化する。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			`disableprivatevolumes` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ボリュームの状態
	backupsets	True	ジョブ監視リクエストのバックアップ セットを収集するかどうか
	filterbynoderegtime	True	ノード登録の前にジョブ監視リクエストに失敗したジョブをフィルター処理する
	Whether to gather failed jbos from the activity log	False	有効にして `True` に設定した場合、失敗したバックアップの発生を示す TSM アクティビティ ログのメッセージも、DPA で失敗ジョブとして報告されます。 `Whether to gather failed jbos from the activity log` オプションはジョブ監視リクエスト内にあります。
	processingtype	デフォルト値なし	ジョブ監視リクエストで処理するジョブのソース。SUMMARY または ACTLOG になります。
	OPTION_LIB_MANAGER_CRED	OptionDefinition.Type.Credential	ボリュームの状態リクエストのライブラリ マネージャー認証情報
	ignorewarnings	デフォルト値なし	成功として扱う警告コード（コンマ区切りの文字列）。
VMware	port	443	VMware サーバーのポート。`port` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
	timeout	3600	VMware ホストに送信されたコマンドの内部タイムアウト（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
	usessl	True	SSL over HTTP を使用する。`usessl` オプションは、次のリクエストのオプションの中に存在する。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• 構成 • パフォーマンス • ステータス
	vmwarehost	デフォルト値なし	VMware サーバーのホスト名。`vmwarehost` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • パフォーマンス • ステータス
VMware VDP（vSphere Data Protection）	capacityfactor	1.075	小数を含む容量係数。`capacityfactor` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ステータス
	dbname	mcdb	データベース名 `dbname` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ジョブ監視 • ステータス リクエスト
	dbport	5555	データベース ポート。`dbport` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • ジョブ監視 • ステータス リクエスト
VPLEX	port	443	構成リクエスト用の HTTPS/HTTP ポート
Webserver	ページ	デフォルト値なし	応答リクエストに対して取得する Web ページ
	port	80	Web サーバー ポート。`port` オプションは、次のリクエストのオプションの中に存在する。 • 構成 • レスポンス
Xsigo	timeout	10	SNMP タイムアウト値（秒）。`timeout` オプションは、次のリクエストのオプションの中に存在する。

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
			• 構成 • パフォーマンス • ステータス
注 サポートされている時刻形式：	1.	• %c - ロケール固有 • %x %X - ロケール固有（代替形式） • %m/%d/%y %I:%M:%S %p - ハードコード化された 12 時間制の米国の日付形式 • %m/%d/%Y %I:%M:%S %p • %d/%m/%y %I:%M:%S %p - ハードコード化された 12 時間制のヨーロッパの日付形式 • %d/%m/%Y %I:%M:%S %p • %m/%d/%y %r • %m/%d/%Y %r - ロケール固有 • %d/%m/%y %r • %d/%m/%Y %r • %d/%m/%y %T • %d/%m/%Y %T • %m/%d/%y %T	日付と時刻の形式に含まれる要素の意味： • %c：現在のロケールの形式を使用した日付と時刻 • %x：現在のロケールの形式を使用した日付 • %X：現在のロケールの形式を使用した時刻 • %m：整数の月（1～12） • %d：整数の日付（00～31） • %y,%Y：整数の世紀なしの年（0～99） • %I：12 時間形式の時刻（1～12） • %M：整数の分（0～59） • %S：整数の秒（0～59） • %p：AM/PM と等価なロケールの要素 • %r：12 時間の am/pm 形式 • %T：時刻（時間:分:秒のエイリアス）

表 30 モジュール別データ コレクション リクエスト オプション （続き）

モジュール	オプション名	値	説明
		• %m/%d/%Y %T • %x - ロケール固有 • %m/%d/%Y • %m/%d/%y • %d/%m/%y • %d/%m/%Y • %d.%m.%Y %T	
	2.	• %c • %x %X • %x, %X	

サイトの管理

`Site` 属性は、`Credentials` や `Schedule` といった他の属性と同様、オブジェクト プロパティ ダイアログ内で設定できます。`Site` 属性は、すべての上位オブジェクトやコンポーネント オブジェクトに割り当てることができます。DPA では、`Site` 属性をグループ オブジェクトに割り当てることはできません。オブジェクトは `Site` 属性によって検索できます。

［**Admin**］ > ［**System**］ > ［**Manage Sites**］の順に選択して、サイトの追加、編集、削除を行います。

サイトの作成、編集、削除

手順

1. ［**Admin**］ > ［**System**］ > ［**Manage Sites**］の順に選択します。

   ［**Manage Sites**］ウィンドウが表示されます。
2. 以下のとおり、目的に合わせて各手順を実行します。
   - サイトの作成：
     a. ［**Create Site**］をクリックします。
     ［**Create Site**］ダイアログが表示されます。
     b. ［**Site Name**］フィールドで、サイトの名前を入力します。
     c. ［**Location**］フィールドで、ご自分のサイトに一番近い地理的場所の名前を 3 文字以上入力し、表示されるリストから適切な場所を選択します。
     d. ［**Select Location**］をクリックして、［**OK**］を選択します。
   - サイトの編集：
     a. サイトのリストから、編集するサイトを選択します。［**Edit Site**］ダイアログが表示されます。

b. 目的のフィールドを編集して、［**OK**］をクリックします。

- サイトの削除：
  a. サイトのリストから、削除するサイトを選択します。［**Delete Site**］ダイアログが表示されます。
  b. 適宜、サイトの削除を確定またはキャンセルします。

アプリケーション サービスの管理

Linux で DPA アプリケーションを非 root ユーザーとして実行する

Linux ではデフォルトで、DPA アプリケーションは root ユーザーの下で実行されます。非 root ユーザーとして実行されるように DPA アプリケーションを構成するには、DPA アプリケーション サーバーで次の手順を実行します。

手順

1. DPA アプリケーション サービスを停止します。**dpa app stop** と入力します。
2. DPA アプリケーションを実行するために使用する OS ユーザーを作成します。

   または、apollosuperuser アプリケーションを実行するために使用される OS ユーザー名 dpaservices を DPA グループから選択します。

   apollosuperuser ユーザーは、DPA のインストール時に作成されます。
3. DPA サービスのインストール ディレクトリの所有権を、DPA アプリケーションを実行する OS ユーザーに移転します。**chown --dereference -LR <user_to_run_dpa>:<group_of_user> <dpa_install_dir>/services** と入力します。
4. <dpa_install_dir>/services/executive/applnsvc.sh ファイルを変更します。**RUN_AS_USER=**の行を **RUN_AS_USER=<user_to_run_dpa>**に変更します。
5. DPA アプリケーション サービスを起動します。**dpa app start** と入力します。
6. (オプション) サードパーティのスクリプト（スケジュールされたレポート用の前処理スクリプト、発行設定の後処理スクリプト、分析ポリシー用のスクリプトなど）を構成した場合は、ステップ 4 で示すように、スクリプトの OS ユーザーを<user_to_run_dpa>に変更します。

   以前は root ユーザーの下で実行していたスクリプトを新しい OS ユーザーの下で実行すると、DPA アプリケーションが権限拒否エラーになる場合があります。

インストールまたはアップグレードをしてから TLS プロトコル バージョン 1.2 を設定する

DPA のインストールまたはアップ グレードを行った後でのみ、dpa application tlslevel コマンドを使用して TLS プロトコル バージョンを 1.2 に設定できます。

手順

1. DPA アプリケーション サーバーを停止します。タイプ：

   dpa app stop
2. dpa application tlslevel コマンドを実行し、TLS プロトコル バージョンをバージョン 1.2 のみに設定します。「**dpa app tls 1.2**」と入力します。
3. DPA アプリケーション サーバーを起動します。タイプ：

dpa app start

サービス情報のカスタマイズ

このセクションでは、管理者のみが実行できるタイプの DPA サービスのカスタマイズについて説明します。DPA を実行しているホストに物理的にアクセスできる必要があります。

「Data Protection Advisor 製品ガイド」で、ビューレット、ダッシュボード、レポートのカスタマイズに関する詳細を参照してください。ユーザーはこれらのカスタマイズを実行できます。

VTL テンプレート

HTML に公開する際にパブリッシャー プロセスがレポートを作成する場合、レポートのデフォルト レイアウトおよびスタイルを特定するために DPA サーバー上の `vtltemplates` ディレクトリにある VTL テンプレートが使用されます。デフォルトでは、DPA サーバーのプロセスは次のテンプレート ファイルを使用します。`reportcard.vtl`, `chart.vtl`、および `table.vtl` ですが、別のテンプレート ファイルも使用できます。DPA サーバー プロセスによって公開されたレポートの外観を変更するテンプレート ファイルを作成することができます。

テンプレートのタイプは次のとおりです。

- Default は、Renderer にデフォルトの VTL を使用します。
- pivot は、ピボット テーブルを生成するためのものです。
- pivot.css は、CSS を使用してピボット テーブルを生成するためのものです。
- pivot.controlpanel.css は、CSS を使用してコントロール パネル内にピボット テーブルを生成するためのものです。

次の表に、VTL テンプレートを示します。

表 31 VTL テンプレート

VTL テンプレート	説明	テンプレート タイプ
chart.vtl	HTML 出力用に、面、コラム、線、円、およびトポロジーを生成する Chart レンダラーによって使用されます。	デフォルト
chart.controlpanel.css.vtl	これが CSS を使用するという点を除いては、chart.vtl と同じです。	N/A
chart.css.vtl	これが CSS を使用するという点を除いては、chart.vtl と同じです。	css
email.attach.vtl	電子メールへの添付ファイルとしてレポートを送信する際に使用されます。	N/A
email.image.embed.vtl	電子メール内にレポートを埋め込むために使用されます。	N/A
email.notification.vtl	レポートが公開された後に送信できる通知を作成するのに使用されます。	N/A
healthstatus.vtl	稼働状態に使用されます。	デフォルト

表 31 VTL テンプレート （続き）

VTL テンプレート	説明	テンプレート タイプ
healthstatus.controlpanel.css.vtl	これが CSS を使用するという点を除いては、healthstatus.vtl と同じです。また、最下位に日付およびバージョンは含まれません。	N/A
healthstatus.css.vtl	これが CSS を使用するという点を除いては、healthstatus.vtl と同じです。	css
reportcard.vtl	ReportCard に使用されます。	デフォルト
reportcard.controlpanel.css.vtl	これが CSS を使用するという点を除いては、reportcard.vtl と同じです。また、最下位に日付およびバージョンは含まれません。	N/A
reportcard.css.vtl	これが CSS を使用するという点を除いては、reportcard.vtl と同じです。	css
table.controlpanel.css.vtl	これが CSS を使用するという点を除いては、table.vtl と同じです。また、最下位に日付およびバージョンは含まれません。	N/A
table.vtl	テーブルに使用されます。	デフォルト
table.css.vtl	これが CSS を使用するという点を除いては、table.vtl と同じです。	css
table.pivot.controlpanel.css.vtl	これが CSS を使用するという点を除いては、table.pivot.vtl と同じです。また、最下位に日付およびバージョンは含まれません。	pivot.controlpanel.css
table.pivot.css.vtl	これが CSS を使用するという点を除いては、table.pivot.vtl と同じです。	pivot.css
table.pivot.vtl	ピボット テーブルに使用されます。	pivot
timeline.vtl	タイムライン グラフに使用されます。HTML が VTL に埋め込まれます。	デフォルト
timeline.controlpanel.css.vtl	これが CSS を使用するという点を除いては、timeline.vtl と同じです。また、最下位に日付およびバージョンは含まれません。	N/A
timeline.css.vtl	これが CSS を使用するという点を除いては、timeline.vtl と同じです。	css

例：パート 1：テーブル VTL テンプレートにメッセージと会社の詳細を追加する

日次または週次レポートを顧客に HTML 形式で送信する必要がある場合は、スケジュールされたレポートでこれを行います。その後、カスタム VTL テンプレートを作成することにより、スケジュールされたレポートにカスタム テキスト（メッセージや会社の連絡先情報など）を追加できます。カスタム テキストは、このテンプレートを使用するすべての HTML レポートで表示されます。

手順

1. DPA サーバー上の `styles` または `vtltemplates` ディレクトリの中にテーブル テンプレート、`table.vtl` をコピーし、名前を変更します。たとえば、会社の EMC に関するテーブル レポート用の VTL テンプレートを作成している場合、`table.<companyName.vtl` という命名標準を使用し、その後、テーブル テンプレートを次の名前に変更します：`table.emc.vtl`
2. テキスト エディターで VTL を開きます。
3. HTML タグを使用して、本文に次のようなテキストを追加します。

```
<body bgcolor="$background"><font face="Arial, Verdana,
                Helvetica, Sans-serif" color="$foreground">

<body>
Dear customer,
<p>
Your daily system status report is below.
<p>
Thank you,<br>
EMC Corporation
<p>
US Phone:1-800-555-5555<br>
Email:support@EMC.com<br>
Website: www.EMC.com
<p>
<table>
...
</table>
</body>
```

4. Save the VTL.

例：パート 2：スケジュール レポートでカスタム VTL テンプレートを使用する

カスタム VTL テンプレートが存在するので、スケジュール レポート ウィザードでこの VTL を選択します。

手順

1. DPA Web コンソールで、スケジュール レポートを新規に作成するか、既存のスケジュール レポートを更新します。
2. ［**Publish Settings**］で、Web ページ（.html）レポート形式を選択し、残りのフィールドを完成させます。
3. ［**Advanced**］で、EMC テンプレートを選択し、［**OK**］をクリックします。Default という名前のテンプレートは、未編集の **table.vtl** です。
4. テスト アイコンをクリックし、パブリッシャーにスケジュール レポートを送信します。ファイルに公開する場合は、デフォルトのディレクトリに進んでレポートを表示してから、VTL テンプレートに必要な更新を行います。レポートのデフォルト ディレクトリは、`<install-dir \services\shared\report-results\scheduled` です。

5. これ以上 VTL テンプレートに更新が必要でない場合は、保存し、スケジュール レポート エディタを終了します。

カスタム テンプレートのインポートとエクスポート

[Custom Templates]セクションでは、カスタム レポート テンプレートおよびカスタム ダッシュボードを DPA 5.5.1 以降からインポートし、WDS ファイルからの DPA にエクスポートすることができます。XML に対するインポートとエクスポートはサポートされていません。システム テンプレートをインポートまたはエクスポートすることはできません。インポートされるレポートは DPA でサポートされている必要があります。

次のニーズを満たすために、カスタム レポート テンプレートおよびカスタム ダッシュボードをインポートおよびエクスポートできます。

- DPA5.x からのカスタム レポートのインポート
- EMC プロフェッショナル サービスによって作成されたカスタム レポートのインポート
- カスタム レポートをバックアップするためのエクスポート
- 動作していないカスタム レポートを EMC カスタマー サポートに送信し、トラブルシューティングしてもらうためのエクスポート

カスタム レポート テンプレートをインポートおよびエクスポートする方法の詳細については、「Data Protection Advisor online help system」システムを参照してください。

クラスタリング管理

DPA 導入後にアプリケーション サーバーをクラスタに追加

DPA CLI を使用して DPA を導入し、DPA が動作可能になった後で、デフォルトのインストール状態であるスタンドアロン サーバーとしてインストール済みである DPA アプリケーション サーバーをクラスタの一部になるように変更する場合、この処理手順を使用します。

はじめに

- DPA エージェントを停止します。
- UNIX マシンを実行している場合は、root ユーザーであることを確認してください。

この処理手順のコマンドは、UNIX 用の形式になっています。

手順

1. スレーブになるノードを構成しない場合は、ステップ 2 に進みます。スタンドアロンのアプリケーション サーバーがクラスタ内のスレーブ ノードとなる場合は、メッセージ キューを空にします。
   a. データ コレクション エージェントを停止します。
   b. フォルダ`/opt/emc/dpa/services/standalone/data/messaginglargemessages` にメッセージがないことを確認します。メッセージがない場合は、ステップ d に進みます。
   c. `/opt/emc/dpa/services/standalone/data/messaginglargemessages` フォルダが空でない場合は、アプリケーションのマスター ノードとスレーブ ノードの両方で、次の REST コールを実行します。

      HTTPS 操作：`GET`

      REST URL：https://<hostname>:9002/dpa-api/support/queues?name=DLQ

      出力には次のような 1 行が含まれることになります。
      `<currentTotalMessageCount>21</currentTotalMessageCount>`

たとえば、この例では「>21<」が messaginglargemessages folder /opt/emc/dpa/services/standalone/data/messaginglargemessages フォルダーのファイル数と一致する必要があります。ファイル数が一致しない場合は、メッセージング キューが空になるまで待機します。

2. すべてのデータストア ノードにデータベース接続プールのサイズを設定します。コマンド：

   # dpa ds tune --connections xxx <RAM>GB ここで **xxx** はアプリケーション サーバーあたり約 **250** となります。たとえば、**2** ノード クラスタでは **500** となります。

   クラスタでデータストア レプリケーションが有効化されている場合は、すべてのデータストア スレーブに対してこのコマンドを実行します。

3. UNIX を実行していない場合は、ステップ 4 に進みます。UNIX マシンの稼働中は、次の要領で UNIX アプリケーション サーバーのファイル記述子の数を増やします。

   a. edit /etc/sysctl.conf ファイルを編集して **fs.file-max = 512000** という行を追加します。

   b. プロンプトで、**# sysctl -p** を実行します。

   c. /etc/security/limits.conf ファイルを編集して*** - nofile 65535** という行を追加します。

   d. プロンプトで、**# ulimit -n 65535** を実行します。

4. 最初のノードでアプリケーション サーバーを停止します。コマンド：

   # dpa app stop

5. アプリケーション サーバーをクラスタ化が可能な状態にプロモートします。コマンド：

   dpa app promote --role MASTER --bind <MASTER_IP> --path <Path to network share>

   dpa app promote コマンドは、デフォルトのマルチキャスト ポート 239.1.2.10 を使用します。このコマンドに、オプション パラメーターとして別のマルチキャスト ポートを指定することもできます。すべてのクラスタ ノードで同じマルチキャスト アドレスを使用していることを確認してください。

6. アプリケーション サーバーを起動します。コマンド：

   # dpa app start

7. ノードがマスターとして開始していることを server.log で確認します。

   1 つのクラスタに設定できるマスター ノードは 1 つだけです。

8. 追加のスレーブ ノードをインストールします。

必要条件

アップグレード後に次の構成を適用します。

- レポート構成の設定
  1. DPA Web コンソールにログインします。
  2. ［**Admin**］ > ［**System**］に移動し、［**Configure Report Settings**］ > ［**Concurrency**］に移動します。
  3. クラスタの［**Maximum Concurrent Reports per Application server**］を［**6**］に設定します。

クラスタからのアプリケーション サーバーの削除

DPA CLI を使用してアプリケーション サーバーをクラスタから削除し、変換してスタンドアロンに戻します。

手順

1. アプリケーション サーバーで、「**dpa application stop**」と入力して、アプリケーション サービスを停止します。アプリケーション サービスはクラスタから削除する前に停止する必要があります。
2. アプリケーション サーバーで、「**dpa application demote**」と入力し、アプリケーションを稼働中のクラスタからデモートします。
3. アプリケーション サーバーで、「**dpa application configure**」と入力して、アプリケーションがクラスタから削除されていることを確認します。

   タイプ `STANDALONE` として表示されます。
4. アプリケーション サーバーで、「**dpa application start**」と入力してアプリケーション サービスを開始し、アプリケーション サーバー機能をリストアします。

   dpa CLI コマンド（130 ページ）で、DPA クラスタリングの CLI コマンドに関する詳細を参照してください。

パスワードの変更に関するクラスタの考慮事項

ドメイン ユーザーのパスワードが変更された場合は、DPA アプリケーション ノードをアンインストールおよび再インストールする必要がある。

- 次のコマンドを実行します。

```
dpa app uninstall
dpa app install  --user (DOMAIN\username) --password (password)
```

  ここで、

  - （DOMAIN\username）は、アプリケーション サービスの実行に使用するユーザー アカウント。［サービスとしてログオン］Windows 権限も有効化する必要があります。
  - <password>は、ユーザーが指定したパスワード。

データストア サービス管理

レプリケーションには次の制限があります。

- ビジー環境でのベスト プラクティスは、エクスポートが完了し、スレーブ データストアにインポートされたら、マスター データストアと再同期できるように、データストア レプリケーションのエクスポートに合わせてアプリケーション サーバーを停止する方法です。
- DPA は、マスター データストアからのデータストア レプリケーション エクスポートのみをサポートしています。DPA は、スレーブ データストアから実行されるデータストア レプリケーション エクスポートをサポートしていません。

データストアのバックアップ

ベスト プラクティスとして、DPA データストアを定期的にバックアップすることをお勧めします。特に、新しいバージョンへのアップグレードや新しいハードウェアへの移行などの大規模な変更を DPA に加え

る前に、バックアップするようにしてください。データストアの内容のエクスポートは、DPA インスタンス全体のバックアップの一部分です。

エクスポートした DPA データストアのインポートは、同じバージョンの DPA データストアでのみサポートされます。

DPA データストアのエクスポート

このエクスポート コマンドを使用すると、完全で一貫したデータストアのコピーが、ローカル ファイル システムの、オプションとして指定できる場所にエクスポートされます。

エクスポートのデフォルトのフォルダー/サブディレクトリは、datastore-<バージョン> <日付と時刻>です。

例：`datastore-6_3_0_90597-2017-10-01-1135`

コマンド ライン プロンプトから次のコマンドを入力します。**dpa datastore export [options]**

デフォルトでは、エクスポートされるデータストア フォルダーは、エクスポート コマンドを実行したときと同じディレクトリに保存されます。

エクスポートされたデータストア ディレクトリを特定のディレクトリに保存するには、コマンド ラインの末尾で場所を指定します。たとえば、次のコマンド ラインでは、指定された場所である `C:\`にフォルダーをエクスポートします。**C:\Program Files\EMC\DPA\services\bin>dpa datastore export C:**

DPA データストアのパイプへのエクスポート

このエクスポート形式を使用すると、Avamar が内容を読み取ることができる場所から、完全で一貫したデータストアのコピーが名前付きパイプにストリーミングされます。

コマンド ライン プロンプトから次のコマンドを入力します。**dpa datastore export --pipeline**

例：**dpa datastore export --pipeline /mydir/mypipe**

DPA では、`ds export` コマンドを使用した Avamar へのバックアップと、Avamar に対するバックアップの直接パイプ処理がサポートされます。詳細については、「名前付きパイプ」を使用した Avamar へのバックアップのパイプ処理方法に関する Avamar のドキュメントを参照してください。

データストアのエクスポート後

`dpa ds export` コマンドは、DPA データストアのすべてのエクスポート ファイルを含むフォルダーを作成します。このフォルダーに対して推奨されるアクションは次のとおりです。

DPA データストアのすべてのエクスポート ファイルを含むフォルダーは、Avamar、NetWorker、または他のバックアップ アプリケーションを使用してバックアップする必要があります。

Avamar を使用している場合、まずコンテンツを復元してから、DPA へのインポートを実行する必要があります。

NetWorker を使用している場合は、これらのデータストアのエクスポート フォルダーを別個のファイル システムに配置し、NetWorker ブロック ベースのバックアップ方法を使用して、このフォルダーを効率的にバックアップすることを検討してください。

DPA データストアのインポート

`dpa datastore import` コマンド ライン オプションは、データストア ファイルの内容を DPA データストアにインポートするために使用されます。

手順

1. DPA アプリケーション サービスを停止します。

2. データストアをインポートします。
3. DPA アプリケーション サーバーを起動します。
4. コマンド ライン プロンプトから次を入力します。

   dpa app stop dpa datastore import [options] <filename> dpa app start この場合、［<filename>］は事前にエクスポートされたデータストア ファイルです。`import` コマンドにより、既存のデータストアの内容が、データストア エクスポート ファイルに含まれる内容でリプレースされます。

必要条件

DPA CLI コマンドの完全なリストを表示するには、コマンド ライン プロンプトで **dpa --help** と入力します。詳細については、DPA コマンド ライン操作（130 ページ）を参照してください。

データストア レプリケーション管理

導入後のデータストア レプリケーションの構成

すでにインストール済みで動作可能なシステムにデータストア レプリケーションを構成する場合は、この処理手順を使用します。このセクションの CLI コマンドは、Linux RHEL 用にフォーマットされています。

手順

1. データストア サーバーがスレーブとしてインストールされていることを確認します。そうでない場合は、データストア サーバーをスレーブ データストアとして構成します。**dpa.sh ds rep --role SLAVE <IP of master>**を実行してデータストア サーバーをスレーブにします。
2. スレーブ データストアがオフラインになった後の統合（128 ページ）にある処理手順に従ってください。

カスケード データストア レプリケーションの構成

カスケード データストア レプリケーションは、DPA CLI を使用してインストールした後でのみ、構成することができます。カスケード データストア レプリケーションを使用すると、マスター データストアからスレーブ データスト チェーン（いずれか 1 つはリモートにすることができます）へのレプリケーションが実行されます。このセクションの CLI コマンドは、Linux RHEL 用にフォーマットされています。

はじめに

- すべてのアプリケーション サーバーを停止します。**dpa.sh app stop** と入力します。
- すべてのデータストア サーバーを停止します。**dpa.sh ds stop** と入力します。
- インポート/エクスポート機能が動作するためには、データストアのインストール ディレクトリが各データストア マシンで同じである必要があります。

手順

1. マスター データストアで、次のコマンドを実行します。

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role master
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --addSlave <ip_of_replicating_slave> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

2. レプリケーション元のスレーブ データストアで、次のコマンドを実行します。

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role replicating_slave <ip_of_master> <DPA_HOME>/emc/dpa/

services/bin/dpa.sh ds rep --addSlave <ip_of_slave>
<DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

3. スレーブ データストアで、次のコマンドを実行します。

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role slave <ip_of_replicating_slave> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

4. スレーブ データストアをマスター データストアの最新データストア コピーと同期します。

   a. 各データストアについて、マスター データストアに、マスター データストアのファイル セットのエクスポート先となる空のディレクトリを作成します。

      例： `/tmp/export`

   b. マスター データストアで次のコマンドを実行し、次のコマンド実行時にマスター データストアの動作が止まらないようにします。

      dpa.sh ds rep --export /tmp/export

   c. 適切なプラットフォームを使用して、スレーブ データストア上の空のディレクトリへのファイルのコピーを指示します。

   d. レプリケーション元のスレーブ データストアで、次のコマンドを実行します。

      <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/export <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

   e. スレーブ データストアで、次のコマンドを実行します。

      <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/export <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

5. データストアでレプリケーションが実行されていることを確認します。次のコマンドを実行します。

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep

   レプリケーション元のスレーブ データストアの出力結果は、次のようになります。

```
<DPA_HOME>/emc/dpa/services/logs # /binary/emc/dpa/
services/bin/dpa.sh ds rep

Data Protection Advisor

[INFO] Replication State : REPLICATING_SLAVE (for
10.11.111.110)
[INFO] Defined Slaves
                          : 10.11.111.111/12

[INFO]                                        SLAVE       BYTES
LAG      STATUS
[INFO]                              10.11.111.111
0      streaming

[INFO] SLAVE is behind the MASTER by 0 [HH:MM:SS]

Command completed successfully.
```

6. アプリケーション サーバーを起動します。タイプ：**dpa.sh app start**

必要条件

マスター データストアが失敗した場合は、DPA が引き続き機能するように、レプリケーション元のスレーブ データストアまたはスレーブ データストアを新しいマスターに設定することができます。詳細についてはデータストア サーバーのフェイルオーバーの実行（127 ページ）を参照してください。

データストア サーバーのフェイルオーバーの実行

マスター データストアに障害が発生した場合は、スレーブ データストアへのフェイルオーバーを実行します。

はじめに

スレーブ データストアが稼働していることを確認します。

手順

1. スレーブ データストアで次のように入力します。

   dpa.sh ds rep --failover

2. アプリケーション サーバを停止します。次のように入力します。

   dpa.sh app stop

3. アプリケーション サーバが新しいマスター データストアをポイントするように再構成します。次のように入力します。

   dpa.sh app con -m <hostname/IP of new MASTER>

4. データストアが実行されていることを確認します。次のように入力します。

   dpa.sh ds status
   出力は INSTALLED、STOPPED、または RUNNING です。

5. 稼働していない場合は、起動してください。次のように入力します。

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

6. アプリケーション サーバを起動します。次のように入力します。

   dpa.sh app start

データストアの再構成

スレーブ データストアにフェイルオーバーし、前のマスター データストアをスレーブ データストアとして再構成する場合は、この手順を使用します。

手順

1. 新しいマスター データストアで、新しいマスター データストアの IP で［**addSlave**］コマンドを使用します。次のように入力します。

   dpa.sh ds rep --addSlave <ip_of_master>

2. 新しいマスター データストアを再開します。次のように入力します。

   dpa.sh ds restart

3. 新しいマスター データストアをエクスポートします。次のように入力します。

   dpa.sh ds rep --export /export

4. 新しいスレーブ データストアを SLAVE として構成します。次のように入力します。

   dpa.sh ds rep --role SLAVE <ip of MASTER>

5. スレーブ データストアを停止します。次のように入力します。

   dpa.sh ds stop

6. マスター データストアをスレーブ データストアにインポートします。次のように入力します。

   dpa.sh ds rep --import c:\import

7. スレーブ データストア サーバを起動します。次のように入力します。

   dpa.sh ds start

スレーブ データストアがオフラインになった後の統合

この手順は、データストア レプリケーションが構成済みであり、スレーブ データストアが停止している場合に適用できます。この処理手順は、すでに動作可能になっている導入環境にデータストア レプリケーションを導入する場合にも適用できます。次に、スレーブ データストアを再統合します。

データストア レプリケーションは、短時間オフラインになった後（たとえば、アプリケーション サーバーの再起動後）、自動的に再開されます。データストアは、再インストールが必要になる前に約 6 時間のダウンタイムが許可されるように構成されています。ただし、これはおよその値であり、負荷の高いサーバーは、ダウンした時間がこれより短くても再インストールが必要になる場合があります。ご使用の導入環境の閾値を決定するためにテストを実行することをお勧めします。

この手順は、スタンドアロンのスレーブ データストアを分離後に再同期する場合にも適用できます。分離の例としては、ネットワークの停止や、マスター データストアとスレーブ データストア間の通信の切断などがあります。

手順

1. マスター データストアに、マスター データストアのファイル セットのエクスポート先となる空のディレクトリを作成します。例： `/tmp/export`
2. 実行中のマスター データストアから、マスター データストアのファイル セットをエクスポートします。タイプ：

   dpa.sh ds rep --export /tmp/export

3. スレーブ データストアに、マスター データストアのファイル セットのコピー先となる空のディレクトリを作成します
4. 適切なプラットフォームを使用して、スレーブ データストア上の空のディレクトリへのファイルのコピーを指示します。
5. スレーブ データストアをインポートします。タイプ：

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/import
   ここで、 `<DPA_Home>`は DPA のインストール場所です。

6. スレーブ データストア サーバーを起動します。タイプ：

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds が起動します。この <DPA_Home>は、DPA のインストール場所になります。この時点で、スレーブ データストアのステータスは STARTED です。

7. レプリケーションが正常に機能していることを確認します。マスター データストアで次のように入力します。

   bin/dpa.sh ds rep
   スレーブ データストアに関する次のような出力が表示されます。`EMC Data Protection Advisor [INFO] Replication State : SLAVE (for 10.11.111.112) Command completed successfully.`

スレーブがダウン後に再起動された場合、マスター データストアでの **catchup** の遅延バイト数とステータスを示す次のような出力が表示されます。

```
EMC Data Protection Advisor

[INFO] Replication State : MASTER
[INFO] Defined Slaves
                          : 10.11.111.111/12

[INFO]                                        SLAVE
BYTES LAG      STATUS
[INFO]                              10.11.111.111
11245376      catchup

Command completed successfully.
```

遅延が解消されると、**streaming** というステータスを示す次のような出力が表示されます。

```
EMC Data Protection Advisor

[INFO] Replication State : MASTER
[INFO] Defined Slaves
                          : 10.11.111.111/12

[INFO]                                        SLAVE
BYTES LAG      STATUS
[INFO]
10.11.111.111               0      streaming

Command completed successfully.
```

データストア レプリケーションの停止

データストア レプリケーションを停止するには、スレーブ データストアを停止します。スレーブ データストアで、「**dpa.sh ds stop**」と入力します。

DPA データベース スーパーユーザーのパスワード

DPA データストアでは、1 つの DPA データベース スーパーユーザー アカウント **apollosuperuser** が提供されます。**apollosuperuser** は、実際に DPA データベースを所有するユーザーであり、DPA データベース内のすべてのアクセス制限をオーバーライドできます。

デフォルトでは、DPA データベースにはローカル マシンからのみ、そのアカウントを使用してアクセスできます。`dpa datastore superpassword` CLI コマンドにより、**apollosuperuser** のパスワードを変更できます。詳細については、「**Data Protection Advisor** インストールおよび管理ガイド」の **dpa datastore** コマンドのセクションを参照してください。

DPA コマンド ライン操作

UNIX ユーザーへの DPA config ファイルのソーシング

テクニカル サポート エンジニアは、エージェント バイナリ（デバッグ モードと bkupjob での DPA エージェント リクエストを含む）を実行する前の DPA config ファイルと UNIX でのコマンド ライン操作のソーシングを要求することがあります。

手順

1. DPA インストール ディレクトリの `/etc` フォルダーに移動します。
2. 次のコマンドを実行します。

結果

```
cd <DPA install dir>/agent/etc
. ./dpa.config
```

DPA config ファイルは、DPA エージェントで使用されるさまざまな環境変数とパスを設定します。指示されたときに実行すると、ユーザーが作業しているシェルが正しく設定されることが保証されます。テクニカル サポート エンジニアによって指示されたときにこの処理手順を実行しないと、CLI コマンドの障害が発生することがあります。

dpa CLI コマンド

デフォルトの DPA インストールでは、dpa CLI コマンドは、UNIX および Linux の場合は `<install_dir>/services/bin` に、Windows の場合は`<install_dir>\services\bin` にあります。

次のシンタクスを使用します。
Windows の場合：

```
dpa <service_part> <command> [options]
```

Linux/UNIX の場合：

```
 dpa.sh <service_part> <command> [options]
```

<service_part>は、アプリケーション、データストア、エージェント、サービスのいずれかです。サービスコンポーネントには、アプリケーション サービス、データストア サービス、エージェント サービスがすべて含まれます。

```
dpa application <command> [options]
```

```
dpa datastore <command> [options]
```

```
dpa agent <command>
```

```
dpa service <command> [options]
```

DPA server `start/stop/restart` コマンドは、現在のホストにインストールされているサービスにのみ適用されます。たとえば、DPA データストアで **`dpa server stop`** を実行した場合、DPA アプリケーション サーバーで実行されているサービスは停止しません。

コマンドとオプションの略語の例

dpa コマンドでは、コマンドの略語がサポートされます。 次の表は、いくつかの略語を示しています。コマンドで利用できるオプションについては、各 dpa コマンドを参照してください。

表 32 コマンドとオプションの略語

コマンドとオプション	略語
--add	-a
--bind	-b
--cluster	-c
--delete	-d
--help	-h
--master	-m
--pipeline	-p
--platform	-p
tune	tun
dpa application	dpa app
dpa datastore	dpa ds
dpa service	dpa svc

dpa agent コマンド

dpa agent コマンドを使用して、DPA エージェント サービスを管理します。dpa agent コマンドは、ローカル エージェントにのみ適用できます。

```
dpa agent start
dpa agent stop
dpa agent status
dpa agent restart
dpa agent install
dpa agent uninstall

dpaagent --set-credentials
```

サービスを開始、停止、または再開した後、完了に数分間かかり、直ちに状態が変化しない場合があります。

dpa agent start

DPA エージェントを起動します。このコマンドが動作するには、エージェント サービスがインストールされ、停止している必要があります。

```
dpa agent start
```

dpa agent stop

DPA エージェントを停止します。このコマンドが動作するには、エージェント サービスがインストールされ、動作している必要があります。

```
dpa agent stop
```

dpa agent status

エージェント サービスのステータスを表示します。例：RUNNING、STOPPED

```
dpa agent status
```

dpa agent restart

エージェント サービスを再起動します。このコマンドは最初にエージェント サービスを停止してからサービスを開始します。このコマンドが動作するには、エージェント サービスが動作している必要があります。

```
dpa agent restart
```

dpa agent install

エージェント サービスをインストールします。このエージェント サービスは、通常のオペレーティング システム サービス コマンドにより管理できる、システム管理サービスとして動作します。サービスのライフサイクルの管理も、このコマンドライン ツールにより管理できます。このコマンドによりサービスがインストー

ルされますが、サービスは自動的に起動されません。エージェント サービスがすでにインストールされている場合、このコマンドは失敗します。

```
dpa agent install
```

dpa agent uninstall

エージェント サービスをアンインストールします。

```
dpa agent uninstall
```

dpaagent --set-credentials

DPA エージェントの登録パスワードを設定します。このコマンドは、次のファイルの場所にあります。

- UNIX および Linux の場合：<agent_install_dir>/agent/bin
- Windows の場合：<agent_install_dir>\agent\bin

```
dpaagent --set-credentials
```

エージェントのパスワードに関して、次の点に注意してください。

- 空白のパスワードはサポートされていません。
- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること

例

C:\Program Files\EMC\DPA\agent\bin>dpaagent --set-credentials

```
DPA
Enter new password for the agent connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the agent connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all
agents use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application コマンド

dpa application コマンドを使用して、DPA アプリケーション サービスを管理します。

```
dpa application  [options]
dpa application agentpwd [options]
dpa application adminpassword [options]
dpa application configure [options]

dpa application dspassword [options]
dpa application demote [options]

dpa application install [options]
dpa application importcertificate [options]
dpa application ping [options]
dpa application promote [options] [<Application Server_IP_Address>]
dpa application restart [options]
dpa application start [options]
dpa application status [options]
dpa application stop [options]
dpa application support [options] <ESRS_IP address>
dpa application tls [options]
dpa application tune <value>MB|GB [options]
dpa application uninstall [options]
dpa application version [options]
```

サービスを開始、停止、または再開した後、完了に数分間かかり、直ちに状態が変化しない場合があります。

dpa application adminpassword

DPA 管理者パスワードをリセットします。データストア サービスの稼働中にコマンドを実行する必要があります。

```
dpa application adminpassword [options]
dpa app pwd [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--version：ツールのバージョン情報を表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

管理者のパスワードに関して次の点に注意してください。

- 空白のパスワードはサポートされていません。
- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること

例

C:\Program Files\EMC\DPA\services\bin>dpa app adminpassword

```
DPA
Enter new administrator password.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new admin password :
[INFO] Your new password has been set.
[INFO] You must restart all DPA application nodes for this new
password to be used.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application agentpwd

アプリケーション側で DPA エージェント登録パスワードを設定します。

```
dpa application agentpassword [options]
dpa app agentpwd [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--version：ツールのバージョン情報を表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

エージェントのパスワードに関して、次の点に注意してください。

- 空白のパスワードはサポートされていません。
- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること

例

C:\Program Files\EMC\DPA\services\bin>dpa app agentpwd

```
DPA
Enter new password for the agent connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the agent connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all
agents use the same new password value.
```

```
Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application configure

通信相手のデータストアおよびクラスタの指定を含め、アプリケーション サービスを構成します。このコマンドが動作するには、アプリケーション サービスが停止している必要があります。

```
dpa application configure [options]
dpa app con [options]
```

コマンド オプション

--master (-m) <IP_address>：通信相手のデータストアを特定します。

--bind (-b) <IP_address>：アプリケーション サービスにバインド アドレスを設定します。

--httprotocol (-hp) <http status>：HTTP プロトコルをオンまたはオフにします。使用できる値は、**TRUE**（HTTP プロトコルをオンにする）と **FALSE**（HTTP プロトコルをオフにする）です。

オプションを指定しないでコマンドを実行した場合、出力にはアプリケーション サーバーが現在どのように構成されているかに関する情報が表示されます。出力のオペレーション モードは、アプリケーションがクラスタ内にあるか、スタンドアロンかを特定します。

例

スタンドアロン クラスタ サーバーの出力：

```
C:\Program Files\EMC\DPA\services\bin>dpa app con
DPA
[INFO] Bind Address      : 0.0.0.0
[INFO] Datastore Service : 127.0.0.1
[INFO] Operation Mode    : STANDALONE
```

マスターの出力：

```
DPA
[INFO] Bind Address      : 0.0.0.0
[INFO] Datastore Service : 127.0.0.1
[INFO] Operation Mode    : CLUSTER
[INFO] Cluster Role      : MASTER
[INFO] Cluster Address   : 10.64.213.61
[INFO] Multicast Address : 239.1.2.61
```

dpa application demote

クラスタ環境からアプリケーション サービスをデモートします。アプリケーション サービスはスタンドアロン オブジェクト インスタンスとして動作します。このコマンドが動作するには、アプリケーション サービスがインストールされ、停止している必要があります。

```
dpa application demote [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--version：ツール バージョン情報を表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
dpa application demote
dpa app demote
```

dpa application dspassword

DPA データストアのパスワードを構成します。

```
dpa application dspassword [options]
dpa app dspwd [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--version：ツールのバージョン情報を表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

データストアのパスワードに関して次の点に注意してください。

- 空白のパスワードはサポートされていません。
- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること

例

C:\Program Files\EMC\DPA\services\bin>dpa app dspassword

```
DPA
Enter new password for the datastore connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the datastore connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all
datastore nodes use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application install

アプリケーション サービスをインストールします。アプリケーション サービスは、通常のオペレーティング システム サービス コマンドにより管理できる、システム管理サービスとして動作します。サービスのライフサイクルの管理も、このコマンドライン ツールにより管理できます。このコマンドによりサービスがインス

トールされますが、自動的に開始されません。アプリケーション サービスがすでにインストールされている場合、このコマンドは失敗します。

```
dpa application install [options]
```

コマンド オプション

--user (-U) (DOMAIN\username)：指定された共有パスへの読み取りおよび書き込みアクセス権を持つユーザー アカウント。指定されたユーザーは、サービスとしてログオン Windows 権限が有効化されている必要があります。

--password (-pass) <password>：指定されたユーザーのパスワード（Windows のみ）。ユーザーは、パスワードを変更した場合、アプリケーション サービスをアンインストールし、再びインストールする必要があります。

--help (-h)：ヘルプ スクリーンを表示します

--version：ツール バージョン情報を表示します

--quiet：警告および警告とエラーのみを表示します

dpa application importcertificate

DPA で提供された証明書を使用せずに、独自の証明書を DPA アプリケーションにインポートしてデータを暗号化できます。

```
dpa application importcertificate [options]
dpa app impcert [options]
```

コマンド オプション

--certificatefile (-cf) <certificatefile>：インポートする証明書（X.509 形式）のパスを設定します。

--keystorefile (-kf) <keystorefile>：インポートする証明書を含むキーストアのパスを設定します。

--alias (-al) <alias>：特定のキーストアにアクセスする際に使用する証明書のエイリアスを設定します。

--password (-pw) <password>：特定のキーストアにアクセスする際に使用するパスワードを設定します。

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
dpa app impcert -kf "C:\work\new.keystore" -al newkey -pw password
```

dpa application ping

送信元のアプリケーション オブジェクトと定義されたマスター データストア サービスの間の接続をテストします。

```
dpa application ping [options]
dpa app pin [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラーのみを表示します

dpa application promote

クラスタ環境にアプリケーション サービスをプロモートします。アプリケーション サービスは、オブジェクトのクラスタ内のオブジェクトとして動作します。サービスのライフサイクルの管理も、このコマンドラインツールにより管理できます。このコマンドが動作するには、アプリケーション サービスがインストールされ、停止している必要があります。

```
dpa application promote [options]
```

コマンド オプション

--bind (-b) <IP_address>：アプリケーション サービスにバインド アドレスを設定します。

--user (-u) <username>：UNIX の場合： （username）は、共有フォルダーの読み取りおよび書き込みアクセス権を持つユーザー アカウントです。省略されている場合は、ルート ユーザーが使用されます。Windows の場合： （DOMAIN\Username）は、共有フォルダーの読み取り/書き込みアクセス権を持つユーザー アカウントです。省略されている場合は、ローカル システム ユーザーが使用されます。このユーザー アカウントは、［サービスとしてログオン］ Windows 権限が有効化されている必要があります。

--path (-p) <path>：クラスター間で共有されているパス

--multicast (-m) <multicast address>：相互に通信するクラスター アプリケーション ノードによって使用されるマルチキャスト アドレスを設定します。クラスター内のすべてのアプリケーション ノードは同じマルチキャスト アドレスを使用する必要があります。

--help (-h)：ヘルプ スクリーンを表示します

--role (-r) <role>：クラスター内のアプリケーションの役割を定義します。可能な値は MASTER と SLAVE <MASTER_IP>です。

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
dpa app promote --bind 192.168.1.0 --role MASTER --user user1 --
path \\shared
```

dpa application restart

アプリケーション サービスを再開します。このコマンドは最初にアプリケーション サービスを停止してからサービスを開始します。このコマンドが動作するには、アプリケーション サービスが動作している必要があります。

```
dpa application restart [options]
```

コマンド オプション

-platform (-p)：プラットフォームのバージョン情報を含みます

--help (-h)：ヘルプ スクリーンを表示します

quiet：警告とエラー メッセージ以外の出力を表示しません

dpa application start

アプリケーション サービスを起動します。このコマンドが動作するには、アプリケーション サービスがインストールされ、停止している必要があります。

```
dpa application start [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

DPA サービスを開始および停止するときの遅延

DPA サービスを開始するときに、Web コンソールの起動が遅く感じる場合があります。DPA サービスをインストールしたばかりの場合、Web コンソールの起動の際に最長 10 分間の遅延が発生します。同様に、DPA サービスを再起動する場合、Web コンソールの起動の際に約 3 分間の遅延が発生する場合があります。

注

DPA Web コンソールを起動する場合は、DPA サービスを実行している必要があります。

dpa application status

アプリケーション サービスのステータスを表示します。例：RUNNING (STARTING...)、RUNNING、STOPPED

```
dpa application status [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
# dpa application status
DPA
The status of the Application Service is RUNNING
```

dpa application stop

アプリケーション サービスを停止します。このコマンドが動作するには、アプリケーション サービスがインストールされ、動作している必要があります。

```
dpa application stop [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa application support

DPA アプリケーション サーバーに ESRS（EMC セキュア リモート サポート）ゲートウェイを構成します。

ESRS-VE をリモート トラブルシューティング（推奨）に使用する予定がある場合は、DPA をインストールする前に、ESRS-VE 環境をインストールし、構成しておく必要があります。ESRS-VE のインストールについての詳細は、EMC オンライン サポートの EMC セキュア リモート サービス ランディング ページ（https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition）を参照してください。.

```
dpa application support [options]
```

```
dpa app support [options]
```

コマンド オプション

--register (-r) <ESRS_IP address>：DPA アプリケーションを ESRS ゲートウェイに登録します

--update (-u) <DPA_new_IP address>：新しい DPA サーバー IP アドレスで ESRS ゲートウェイを更新します

--deregister (-d)：DPA アプリケーション サーバーを ESRS ゲートウェイから登録解除します

--ping (-p) <ESRS_IP address>：ping を実行して DPA アプリケーション サーバー/ノード情報を取得します

--help (-h)：ヘルプ スクリーンを表示します

例

```
C:\Program Files\EMC\DPA\services\bin>dpa app support --register
10.11.110.111
```

dpa application tlslevel

DPA アプリケーション サービスの TLS プロトコル バージョンを設定します。このコマンドによりサービスがインストールされますが、サービスは自動的に開始されません。アプリケーション サービスがすでにインストールされている場合、このコマンドは失敗します。

```
dpa application tlslevel [options]
dpa app tls [options]
```

コマンド オプション

1.2 — DPA アプリケーション サービスの TLS プロトコル バージョンを、TLS バージョン プロトコル 1.2 のみに設定します。

1.0 — DPA アプリケーション サービスの TLS プロトコル バージョンを、TLS バージョン プロトコル 1.0、1.1、1.2 に設定します。

--help (-h)：ヘルプ スクリーンを表示します

--version：ツール バージョン情報を表示します

--quiet：警告および警告とエラーのみを表示します

例

```
dpa app tls 1.2
```

dpa application tune

使用可能なホスト メモリ リソースのアプリケーション サービスの調整可能パラメーターを構成します。

```
dpa application --tune <size> MB|GB
dpa app tune <size> MB|GB
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa application uninstall

アプリケーション サービスをアンインストールします。

```
dpa application uninstall [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa application version

アプリケーション サービスを構成するさまざまな機能ライブラリのバージョン情報を表示します。機能ライブラリには、Apollo、Controller、DPA（DPA）、RemoteX、UI などがあります。

```
dpa application version [options]
```

コマンド オプション

-platform (-p)：プラットフォームのバージョン情報を含みます

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
# dpa application version
[INFO] Version for     Apollo EAR is 1.0.0.3304
[INFO] Version for Controller RAR is 18.1.xxx
[INFO] Version for DPA EAR is 18.1.xxx
[INFO] Version for    Remotex EAR is 1.0.0.3304
[INFO] Version for         UI WAR is 18.1.x.local
```

dpa datastore コマンド

dpa datastore コマンドを使用して、DPA データストア サービスを管理します。

```
dpa datastore [options]
dpa datastore configure [options]
dpa datastore dspassword [options]
dpa datastore export [options]
```

```
dpa datastore import [options] <import_filename>
dpa datastore install [options]

dpa datastore logtz <time zone>
dpa datastore recreate [options]
dpa datastore replicate [options]
dpa datastore restart [options]
dpa datastore start [options]
dpa datastore status [options]
dpa datastore stop [options]
dpa datastore superpassword [options]
dpa datastore support [options] <ESRS_IP address>
dpa datastore tune <size>MB|GB [options]
dpa datastore uninstall [options]

dpa datastore supportbundle [options] <directory of output file>
dpa datastore version
```

サービスを開始、停止、または再開した後、完了に数分間かかり、直ちに状態が変化しない場合があります。

dpa datastore configure

データストア サービスに対して許可されている接続のリストへのアプリケーション サービスの追加または削除を含め、データストア サービスを構成します。

```
dpa datastore configure [options]
dpa ds configure [options]
```

コマンド オプション

--bind <IP_address>：データストア サービスにバインド アドレスを設定します。デフォルトは 127.0.0.1 です

通知

--bind は、--add または--delete で指定できません。

-add <IP_address>：有効なデータストア クライアントとしてアプリケーション サービス ノードを追加します

--delete <IP_address>：有効なデータストア クライアントとしてアプリケーション サービス ノードを削除します

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
dpa datastore con --add 111.111.1.1
```

dpa datastore dspassword

DPA データストアのパスワードをリセットします。データストア サービスの稼働中にコマンドを実行する必要があります。

```
dpa datastore dspassword [options]
dpa ds pwd [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--version：ツールのバージョン情報を表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

データストアのパスワードに関して次の点に注意してください。

- 空白のパスワードはサポートされていません。
- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること

例

C:\Program Files\EMC\DPA\services\bin>dpa ds dspassword

```
DPA
Enter new password for the datastore connection from the
application node.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the datastore connection from the
application node:
[INFO] Your new password has been applied to the datastore.
[INFO] For this new password to be used you must ensure that all
DPA application nodes use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa datastore export

データストアの内容を指定したファイル名またはパイプラインにエクスポートします。このコマンドが動作するには、データストア サービスがインストールされ、動作している必要があります。存在する既存のファイル名は上書きされます。

```
dpa datastore export [options]
```

```
dpa datastore export [options] <directory>
```

コマンド オプション

--pipeline：パイプにエクスポートします

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
C:\Program Files\EMC\DPA\services\bin>dpa datastore export C:\
```

エクスポートのデフォルト ファイル名を次に示します。datastore-<version> <date and time>

例：datastore-6_2_0_90597-2014-10-01-1135

dpa datastore import

データストア エクスポート ファイルの内容をデータストアにインポートします。インポート ファイルはローカル ファイル システムで使用できることが必要です。コマンドを実行する前にこのデータストアと通信するすべてのアプリケーション サーバーの停止を求めるプロンプトが表示されます。import コマンドを実行するには、データストア サービスが動作している必要があります。

```
dpa datastore import [options] <filename>
```

ここで、<filename>はすでにエクスポートしてあるデータストア ファイルです。import コマンドにより、既存のデータストアの内容が、データストア エクスポート ファイルに含まれる内容でリプレースされます。

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

<import_filename>：インポートするエクスポートされたファイルのファイル名

例

```
# dpa datastore import datastore-2013-02-20-1205
DPA
Datatstore imported from file : datastore-2013-02-20-1205
Imported to the datastore successfully
```

dpa datastore install

データストア サービスをインストールします。データストア サービスは、通常のオペレーティング システム サービス コマンドにより管理できる、システム管理サービスとして動作します。サービスのライフサイクルの管理も、このコマンドライン ツールにより管理できます。このコマンドによりサービスがインストールされますが、自動的に開始されません。データストア サービスがすでにインストールされている場合、このコマンドは失敗します。

```
dpa datastore install [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します。--version：ツール バージョン情報を表示します。--quiet：警告とエラー メッセージ以外の出力を表示しません。

dpa datastore logtz

DPA データベース ログ タイム ゾーンの設定

```
dpa datstore logtz <time zone>
```

```
dpa ds logstz <time zone>
```

例

dpa datstore logtz 'Europe/Moscow' DPA データストア ログのタイム ゾーンを「Europe/Moscow」に設定

dpa datstore logtz DPA データストア ログのタイム ゾーンを GMT に設定

dpa datastore recreate

データストアを再作成し、内容を出荷時設定に戻します。

説明

dpa datastore recreate [options]

```
dpa ds rec [options]
```

コマンド オプション

--force (-f)：現在のデータストア データを上書きする優先プロンプト

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

構文

dpa データストアのレプリケーション

データストア サービスを構成して、他のインスタンスにレプリケートします。

説明

```
dpa ds rep [options]
```

コマンド オプション

--addSlave (-a) <hostname/IP of SLAVE> : スレーブ データストアをマスター データストアに追加します

-deleteSlave (-d) <hostname/IP of SLAVE> : スレーブ データストアをマスター データストアから削除します

--role (-r) MASTER：スレーブ データストアの役割をマスター データストアに再定義します

--role (-r) SLAVE <IP of MASTER>：マスター データストアの役割をスレーブ データストアに再定義します

--failover：スレーブ データストアとマスター データストア間で、フェイルオーバーを開始します

--import (-i) <import>：指定したディレクトリにあるレプリカを使用して、SLAVE データストアを初期化します

--export (-e) <export>：MASTER データストアのクローンを指定したディレクトリに作成します

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

構文

dpa datastore restart

データストア サービスを再開します。このコマンドは最初にデータストア サービスを停止してからサービスを開始します。このコマンドが動作するには、データストア サービスが動作している必要があります。

```
dpa datastore restart [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa datastore start

データストア サービスを開始します。このコマンドが動作するには、データストア サービスがインストールされ、停止している必要があります。

```
dpa datastore start [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa datastore status

データストア サービスのステータスを表示します。例：RUNNING (STARTING...)、RUNNING、STOPPED

```
dpa datastore status [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
# dpa datastore status
DPA
```

```
The status of the Datastore Service is RUNNING
```

dpa datastore stop

データストア サービスを停止します。このコマンドが動作するには、データストア サービスがインストールされ、動作している必要があります。

```
dpa datastore stop [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa datastore superpassword

DPA データストア スーパーユーザーのパスワードをリセットします。スーパーユーザーは、DPA データベースを所有しているユーザーです。データストア サービスの稼働中にコマンドを実行する必要があります。

データストア レプリケーションを使用する場合は、すべてのデータストア ノードでこのコマンドを実行する必要があります。最初にマスター ノードでコマンドを実行し、その後で他のすべてのレプリケーション スレーブ ノードでコマンドを実行します。

```
dpa datastore superpassword [options]
dpa ds superpwd  [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--version：ツールのバージョン情報を表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

データストアのパスワードに関して次の点に注意してください。

- 空白のパスワードはサポートされていません。
- 最小文字数は、9 文字です。
- 必須条件は次のとおりです。
  - 1 つ以上の英大文字と 1 つ以上の英小文字を含んでいること
  - 1 つ以上の数字を含んでいること
  - 1 つ以上の特殊文字を含んでいること

例

C:\Program Files\EMC\DPA\services\bin>dpa ds superpassword

```
DPA
Enter new password for the superuser owning the database.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the superuser owning the database:
[INFO] Your new password has been applied to the superuser owning
```

```
the database.

Command completed succcessfully.
```

dpa datastore supportbundle

サポート情報を収集し、DPADPA Datastore サポート バンドルの zip ファイルを、指定したディレクトリに格納します。

```
dpa datastore supportbundle [options] <directory of output file>
dpa ds supbd [options] <directory of output file>
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa datastore tune

使用可能なホスト メモリ リソースとデータベース接続のデータストア サービスの調整可能パラメーターを構成します。

```
dpa datastore tune <size>MB|GB [options]
dpa ds tune <size>MB|GB [options]
```

コマンド オプション

--connections (-c) <connections>：許可されるコンカレント データストア接続の最大数

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa datastore uninstall

データストア サービスをアンインストールします。

```
dpa datastore uninstall [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa datastore version

データストアのバージョンおよびパッチ番号をクエリーします。

```
dpa datstore version [options]
```

```
dpa ds version [options]
```

コマンド オプション

--help (-h)：ヘルプ スクリーンを表示します

dpa サービス コマンド

dpa サービス コマンドを使用して、DPA アプリケーション、DPA データストア、DPA エージェントのサービスを管理します。

```
dpa service install [options]
dpa service restart [options]
dpa service start [options]
dpa service status [options]
dpa service stop [options]
dpa service uninstall [options]
```

dpa service install

データストア サービスをインストールし、次にアプリケーション サービスをインストールします。このサービスは、通常のオペレーティング システム サービス コマンドにより管理できる、システム管理サービスとして動作します。サービスのライフサイクルの管理も、このコマンドライン ツールにより管理できます。このコマンドによりサービスがインストールされますが、自動的に起動されません。サービスがすでにインストールされている場合、このコマンドは失敗します。

```
dpa service install [options]
dpa svc install [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa service restart

アプリケーションおよびデータストア サービスを再開します。このコマンドは、アプリケーション サービスを停止し、データストア サービスを停止してから、データストア サービスおよびアプリケーション サービスを起動します。このコマンドが動作するには、サービスが動作している必要があります。

```
dpa service restart [options]
dpa svc restart [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa service start

データストア サービスを起動し、次にアプリケーション サービスを起動します。このコマンドが動作するには、サービスがインストールされ、停止している必要があります。

```
dpa service start [options]
dpa svc start [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa service status

アプリケーションおよびデータストア サービスのステータスを表示します。例：RUNNING (STARTING...)、RUNNING、STOPPED

```
dpa service status [options]
dpa svc status [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

例

```
# dpa service status
DPA
The status of the Datastore Service is RUNNING
The status of the Application Service is RUNNING (STARTING ...)
```

dpa service stop

アプリケーション サービスを停止し、次にデータストア サービスを停止します。このコマンドが動作するには、サービスがインストールされ、動作している必要があります。

```
dpa service stop [options]
dpa svc sop [options]
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

dpa service uninstall

アプリケーション サービスをアンインストールし、次にデータストア サービスをアンインストールします。

```
dpa service uninstall [options] <certificate> <key>
dpa svc uninstall [options] <certificate> <key>
```

コマンド オプション

--help：ヘルプ スクリーンを表示します

--quiet：警告とエラー メッセージ以外の出力を表示しません

履歴バックアップ ジョブ データのロード

履歴バックアップ データの収集には、DPA Web コンソールを使用する方法が推奨されています。

はじめに

DPA Web コンソールを使用した履歴のバックアップ データの収集（94 ページ）で詳細を参照してください。

バックアップ アプリケーション オブジェクトが作成されリクエストが割り当てられると、エージェントはバックアップ ジョブに関するデータの収集をすぐに開始してデータベースに格納します。ただし、エージェントは、DPA でオブジェクトを作成する前に実行されたバックアップ ジョブに関するデータも収集できます。

注

DPA サーバーにデータをコミットするには、インストール済みのエージェントがあらかじめ起動され、正常に DPA サーバーに登録されている必要があります。ただし、履歴データをロードするためには、現時点で実行されている必要はありません。

各バックアップ モジュールには、インストールしたエージェントの bin ディレクトリ（`<DPA_HOME>/emc/dpa/agent/bin` ディレクトリ）に、同等の実行可能プログラムがあります。
<DPA_Home>は、DPA のインストール場所です。

説明

次の例では、NetWorker サーバーで実行されたバックアップ ジョブ データを収集します。

構文

例

```
<install_dir>/agent/bin/dpaagent_modnetworker -c -f jobmonitor -t
NetWorkerServer_IP -B "01/01/2012 00:00:00" -E "01/01/2012 00:00:00"
```

パラメーター-?を指定して実行可能プログラムを実行すると、有効なコマンド ライン オプションが表示されます。「通常の」データ収集と動作の整合性を保つには、リクエスト（timeformat など）に適用可能なモジュール オプションの明示的な指定が必要な場合があります。特に DataProtector の jobmonitor リクエストの場合、占有の計算に履歴データを含めたい場合は、占有オプションの明示的な指定が必要です。オプションの詳細については、「Data Protection Advisor Data Collection Reference Guide」を参照してください。占有オプションの詳細については、「Job Monitor」セクションを参照してください。

履歴バックアップ データをロードするには、次のパラメーターを指定してコマンド ラインからエージェントのバイナリを実行します。特に次を使用する必要があります。

- -f <function name>：実行するデータ コレクション機能の名前。常に jobmonitor になります。必須。
- -t <target host>：バックアップ アプリケーション サーバーのホスト アドレス。デフォルトは localhost です。
- -B <start time>：バックアップ ジョブを収集する開始時刻。形式は、dd/mm/yyyy hh:mm:dd です。
- -E <end time>：バックアップ ジョブを収集する終了時刻。形式は、dd/mm/yyyy hh:mm:dd です。
  開始時刻と終了時刻は、UNIX のエポック時刻形式でもかまいません。

  <start time>を指定して<end time>を指定しない場合、<end time>には現在の時刻が設定されます。この場合、<start time>以降に終了したバックアップ ジョブがすべて含められます。

  <end time>を指定して<start time>を指定しない場合、<start time>には 0 が設定されます。この場合、<end time>より前に終了したバックアップ ジョブがすべて含められます。
- -i：TSM インスタンス名（TSM のみ）。

- -l <log file name>：履歴データをロードするコマンドの実行時に生成するログ ファイルの名前およびパス。
  デフォルトのログ ファイルの場所は、コマンドが実行される場所です。
- -U：バックアップ アプリケーションと接続するためのユーザー名（TSM および Avamar のみ）。
- -P：バックアップ アプリケーションと接続するためのパスワード（TSM および Avamar のみ）。
- -c- Commit：モジュールに、データを DPA サーバーに送信するように指示します。必須。必須。

次の例では、Avamar サーバーで実行されたバックアップ ジョブ データを収集します。

例

```
dpaagent_modavamar.exe -f jobmonitor -t De-dup-muc.corp.emc.com -U
viewuser -P viewuser1 -c -B "01/01/2012 00:00:00" -l /tmp/
mod_avamar.log
```

ジョブの要約レポート

ジョブの要約レポートは、バックアップ サーバで実行された、バックアップおよび保守ジョブ全体の概要を提供します（すべてのジョブ、成功したジョブ、失敗したジョブなど）。要約レポートは、データストア中の最新のデータを使用して、正確な要約結果を生成します。

説明

エージェントのコマンド ライン オプションを使用して履歴バックアップ ジョブ データがロードされている間、要約レポートに表示される合計が不正確になる可能性があります。すべての履歴ジョブ データがロードされてから、ロードされた履歴期間の要約レポートを実行することをお勧めします。

構文

第 4 章

DPA での環境の検出

この章は、次のセクションで構成されています。

- 検出用の環境の構成 156
- ホストまたはオブジェクトの手動による検出 201
- 検出後のジョブ データ収集について 203
- 監視対象オブジェクトおよびグループ 203
- ポリシー、ルール、アラートの構成 209

検出用の環境の構成

検出の概要

次の図は、データ保護インフラストラクチャの監視用に導入された DPA アプリケーション オブジェクトと DPA エージェント間の関係を示しています。

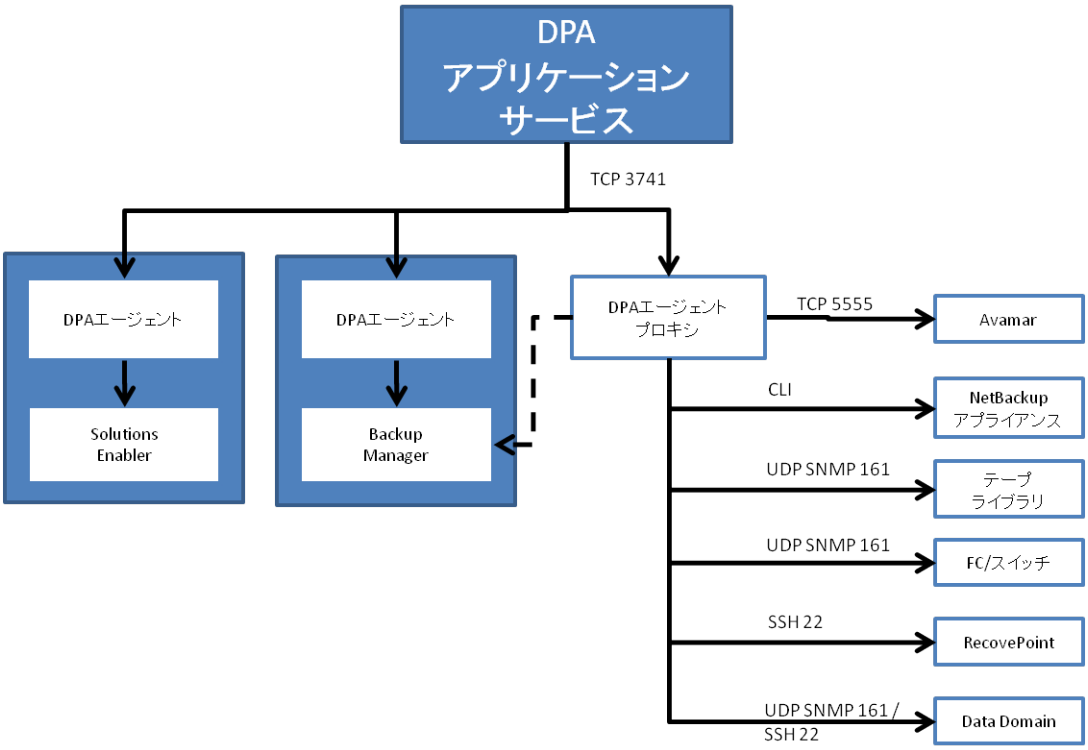
一部のタイプのデバイスは、プロキシとして導入された DPA エージェントを使用して監視する必要があります。通常、プロキシは、監視されるオブジェクトがハードウェアで、エージェント インストールへのアクセスが不可能な場合に使用されます。ほとんどのタイプのバックアップ マネージャーは、バックアップ マネージャーと同じホストに直接インストールされているエージェントによって監視するか、バックアップ マネージャーのリソースが制約されている場合はプロキシ エージェントを使用してリモートで監視できます。

DPA は、バックアップ プール名に関して、大文字と小文字を区別しません。たとえば、次のようにプールを定義するとします。

- test_name
- Test_name
- Test_Name

この場合、DPA は構成ツリーに 1 つのオブジェクトを作成します。範囲に関するレポートを実行してこのオブジェクトを選択すると、1 セットの数字しか表示されません。

図 3 DPA アプリケーション ノードとアプリケーションを監視している DPA エージェント間の関係



監視対象のオブジェクトの定義

DPA で監視対象のオブジェクトを定義するには、次の表の手順に従います。

表 33 データ監視のセットアップの概要

ステップ	説明
ライセンスの確認	デバイス、ホストまたは環境を監視するためのライセンスが購入済みおよびインストール済みであるかどうかをチェックします。
エージェントのインストール	DPA サーバー ホスト以外のホストからオブジェクトを監視している場合は、DPA エージェントをインストールする必要があります。DPA エージェントのインストール（53 ページ）を参照してください。
サード パーティ製バイナリのインストールまたは監視用オブジェクトの定義	このステップは、リモートまたはエージェントレス（プロキシ）のデータ コレクションに必要です。 監視対象オブジェクトと接続するために、DPA ホストまたはリモート エージェント ホストにバイナリをインストールする必要が生じることがあります。監視対象オブジェクトに関するアカウントまたは接続を定義する必要が生じる場合もあります。 次のセクションでは、すべてのオブジェクトの前提条件となる構成について説明します。 • レプリケーション解析の構成（189 ページ） • レプリケーション解析用のストレージ アレイの構成（191 ページ） • バックアップ アプリケーションの監視（160 ページ） • データベースの監視（174 ページ） • RecoverPoint の監視（191 ページ） • オペレーティング システムの監視（186 ページ） • テープ ライブラリの監視（196 ページ） • スイッチおよび I/O デバイスの監視（198 ページ） • ファイル サーバーの監視（191 ページ） • 保護ストレージの監視（194 ページ） • StorageTek ACSLS Manager の監視（196 ページ） • ディスク マネージメント サーバーの監視（193 ページ） • VMware 環境の監視（199 ページ）
DPA 認証情報の作成または変更	認証情報には、監視対象オブジェクトと接続するために使用される情報が保存されます。デフォルトの認証情報を変更するか、直前のステップからアカウント詳細を使用して新しい認証情報を作成する必要が生じる場合があります。
［Discovery Wizard］を実行します。	［Discovery Wizard］を使用して、監視対象オブジェクトを定義します。

表 33 データ監視のセットアップの概要 （続き）

ステップ	説明
	［**Inventory**］ > ［**System**］ > ［**Run Discovery Wizard**］の順に選択します。
データ コレクションのデフォルト設定の変更	すべてのリクエストについてデフォルトの保存期間を確認し、必要であれば変更します。 データ コレクション リクエストは、［Discovery Wizard］によって作成されたオブジェクトに割り当てられます。デフォルトのデータ コレクションを変更する場合は、［**Admin**］ > ［**Systems**］ > ［**Manage Data Collection Defaults**］の順に選択します。
データ コレクションのテスト	少なくとも 10 分間リクエストを実行した後で、データを含むオブジェクトからレポートを実行します（たとえば、Backup Job Summary または、構成レポート）。

［Discovery Wizard］を実行する前に

手順

1. インストールされているライセンスを確認します。DPA Web コンソールで、［**Admin**］ > ［**System**］ > ［**Manage Licenses**］の順に選択します。

   ［Discovery Wizard］での構成に使用できるオプションは、DPA を使用してインストールしているライセンスのタイプにより異なります。正しいライセンスがインストールされていない場合、そのデバイスまたはホストを作成するオプションはウィザードでは無効にされます。

2. Linux ホストで検出を実行している場合は、ホストに libstdc++.so.6 ライブラリがインストールされていることを確認します。
3. 次の表で示す接続の詳細を記録しておきます。

表 34 ［Discovery Wizard］によるデータ コレクション構成用の、接続性の詳細

項目	［Discovery Wizard］で入力に注意すべき値
DPA サーバーまたはエージェント（エージェントが DPA サーバーのリモートにある場合）のネットワーク構成情報	
Hostname	Value：
IP アドレス	Value：
ネットワーク マスク	Value：
プライマリ DNS サーバー アドレス	Value：
セカンダリ DNS サーバー アドレス	Value：
ゲートウェイ アドレス	Value：

表 34 ［Discovery Wizard］によるデータ コレクション構成用の、接続性の詳細 （続き）

項目	［Discovery Wizard］で入力に注意すべき値
タイム ゾーン	Value：
SSH を介する仮想ディスクの検出に必要な認証情報	
ESX Server の IP アドレス	Value：
ESX Server の root 認証情報	Value：
サーバーおよびアレイの検出に必要な認証情報	
サーバー名/IP	
SSH の認証情報	Value：
RPC の認証情報	Value：
WMI の認証情報	Value：
Solutions Enabler ホストの認証情報 root/管理者認証情報が必要です	Value：
RPA の認証情報	Value：
Oracle Database の監視に必要な認証情報	
必要な Oracle ユーザー名およびパスワード	Value：
Oracle サービス名およびポート（特に Oracle SID および TNS ポート）	Value：
Oracle RMAN 監視 RMAN スキーマにカタログ アクセスする Oracle ユーザーで、ユーザー名とパスワードが必要です	Value：
Oracle ホスト名	Value：
Oracle スキーマ監視 1 つの Oracle SID に複数の RMAN スキーマが存在する場合、RMAN スキーマ所有者およびユーザー名とパスワードが必要です。	Value：
SQL Server データベースに必要な認証情報	
SQL データベースのユーザー アカウント	Value：
SQL Server インスタンス	Value：
SQL データベース名	Value：
PostgreSQL の認証情報	
PostgreSQL のユーザー アカウント（スーパーユーザーでなければなりません）	Value：
バックアップ サーバー、テープ ライブラリ、I/O デバイスの認証情報	
CommVault のユーザー アカウント	Value：
Avamar のユーザー アカウント	Value：

表 34 ［Discovery Wizard］によるデータ コレクション構成用の、接続性の詳細 （続き）

項目	［Discovery Wizard］で入力に注意すべき値
Avamar 7.1 以降、Avamar には viewuser アカウントのデフォルト パスワードは付属していません。viewuser アカウントのパスワードは、Avamar のインストール時に設定します。Avamar 7.1 以降を検出する場合に、以前のバージョンからアップグレードされていなければ、DPA で新しい認証情報を作成する必要があります。 ［**Admin**］ > ［**User**］ > ［**Set Credentials**］の順に選択します。	
HP Data Protector のユーザー アカウント	
TSM インスタンスごとに IBM TSM ホスト、TSM インスタンス名、TSM ポートおよび TSM のユーザー名とパスワードが必要です	Value：
Symantec Backup Exec のユーザー アカウント	Value：
Symantec PureDisk のユーザー アカウント	Value：
Data Domain の SNMP コミュニティ文字列 Data Domain の SSH ユーザー名およびパスワードで、Data Domain のシステム管理者のデフォルト認証情報と異なるユーザー名およびパスワードが好ましいです。 両方のメカニズムでデータ コレクションをするため両方必要です。	Value：
EDL の SNMP コミュニティ文字列	Value：
ファイバ チャネル スイッチ用の SNMP 文字列	Value：
テープ ライブラリ用の SNMP コミュニティ文字列	Value：
IP スイッチ用の SNMP コミュニティ文字列	Value：

バックアップ アプリケーションの監視

このセクションでは、バックアップ アプリケーションを監視する方法について説明します。

CA BrightStor ARCserve の監視

CA BrightStor ARCserve サーバは、CA BrightStor ARCserve サーバで実行されているエージェントから、または環境内のその他の Windows コンピュータで実行されているエージェントから監視されます。

CA BrightStor ARCserve の監視用に［Discovery Wizard］を開始する前に

はじめに

- ARCserve サーバーの名前解決できるホスト名または IP アドレスを知っておく必要があります。
- ARCserve 11.x が実行されている場合、ホスト名は短縮形である必要があります。エイリアスは使用できません。

手順

1. ARCserve Manager を、エージェントが実行されているコンピューターにインストールします。

   エージェントの認証情報は、既存の ARCserve のアカウントと一致する必要があります。

2. DPA が 14 日前からのジョブ データを収集するようにする場合、ARCserve のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。

CommVault Simpana の監視

CommVault Simpana サーバは、CommVault Simpana データベースで実行されているエージェントから、または環境内の他の Windows コンピュータで実行されているエージェントから監視します。

CommVault Simpana の監視用に［Discovery Wizard］を開始する前に

CommVault SQL Server で Windows 認証を使用している場合は、DPA エージェント サービスを指定されたアカウントで実行する必要があります。DPA エージェント サービス用に選択する指定アカウントには、CommVault SQLServer データベースの読み取りアクセスの権限が必要です。

または、SQL 認証が使用される場合は、CommVault リクエスト用の DPA 認証情報を定義する必要があります（例：ユーザー名は cvadmin、パスワードは cvadmin ユーザーのパスワード）。

次の情報が必要です。

- CommVault サーバーの名前解決できるホスト名または IP アドレス。
- CommVault データベースがサーバーに対してリモートである場合は、データベースのホスト名およびインスタンス名。

DPA が 14 日前からのジョブ データを収集するようにする場合、CommVault Simpana のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］> ［**Object Library**］> ［**[**オブジェクトの選択**]**］> ［**Data Collection**］の順に選択します。

Avamar の監視

Avamar サーバーは、環境内の任意のリモート コンピューターにインストールされている DPA エージェントを使用して監視します。これには DPA サーバーが含まれます。Avamar サーバーまたはストレージ オブジェクトには DPA エージェントをインストールしません。

バージョン 7.2 以降で基本的な Avamar グリッドの監視を有効にするには、サポート対象の DPA 展開で、［**Remote Data Collection Unit**］が選択されていることを確認します。

ソース グリッドがレポートの範囲として選択されている場合に［Clone Operations］レポートがデータを表示できるようにするには、Avamar レプリケーション設定の Job Monitor リクエストを使用して、ソース Avamar グリッドを監視する必要があります。

Avamar の監視用に［Discovery Wizard］を起動する前に、

Avamar サーバーをリモートから監視するために追加のソフトウェアは必要ありません。

はじめに

［Discovery Wizard］を起動する前に、Avamar サーバーの名前解決できるホスト名または IP アドレスを知っておく必要があります。

手順

1. Avamar からデータを収集するために、DPA を Avamar データベースに直接接続します。Avamar のデフォルト ポート 5555 で mcdb データベースに接続します。これらのパラメーターが変更されている場合は、Avamar Configuration、Avamar Job Monitor、Avamar Status のリクエストのオプションを編集し、使用中のデータベース名とポートを指定します。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。
2. DPA が 14 日前からのジョブ データを収集するようにする場合、Avamar のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。
3. Avamar 7.1 以降を検出する場合に、以前のバージョンからアップグレードされていなければ、DPA で新しい認証情報を作成する必要があります。［**Admin**］ > ［**User**］ > ［**Set Credentials**］の順に選択します。

   Avamar 7.1 以降、Avamar には viewuser アカウントのデフォルト パスワードは付属していません。viewuser アカウントのパスワードは、Avamar のインストール時に設定します。
4. ［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択して、DPA Web コンソールの［Default Avamar Credentials］で新しい認証情報を作成します（ユーザー名/パスワードはアップグレード時にリセットされます）。

   DPA をデータベースに接続する場合は、viewuser アカウントを使用してデータベースにログインします。

Avamar 検出後のジョブ データ収集について

DPA 内に Avamar を検出した後の Avamar ジョブ データ収集について説明します。

- 新しい Avamar サーバーが検出されると、DPA は 14 日前からのジョブ データを収集します。
- Jobmonitor リクエストが実行されるたびに、DPA は最大で「バッチ期間」に相当する量のデータを収集します。この値は設定可能で、デフォルトは 1 日分のデータです。
- Jobmonitor リクエストがいくつか実行されると、収集されたジョブの期間が現時点に追いつき、新しいバックアップが収集されます。
- 最後の Jobmonitor が終了してから新しい Jobmonitor リクエストが実行されるまでのデフォルトの時間は 5 分です。これはすべてのリクエストと同様に設定可能です。

詳細については、モジュール別データ コレクション リクエスト オプションを参照してください。

NetWorker の監視

バックアップ サーバーで実行されているエージェントから、または環境内の任意のリモート コンピュータにインストールされている DPA サーバーで実行されているエージェントをリモートで使用して、NetWorker を監視します。

NetWorker の監視用に［Discovery Wizard］を開始する前に

NetWorker をリモート監視している場合は、NetWorker クライアント パッケージをエージェントのホストにインストールする必要があります。NetWorker モジュールはコマンド（`jobquery` や `nsradmin` など）を使用して NetWorker サーバーと通信し、NetWorker クライアント パッケージ内のバイナリへのアクセスを必要とします。

はじめに

- ［Discovery Wizard］を起動する前に、NetWorker サーバーの名前解決できるホスト名または IP アドレスを知っておく必要があります。
- NetWorker 9.0.0.4 以降を監視する場合は、NetWorker サーバーの認証情報があることを確認してください。DPA エージェントが `nsrauth` を発行して nsradmin を実行できるように、NetWorker サーバーの認証情報を入力するよう求められます。

手順

1. NetWorker 9.0.0.4 以降をリモート監視する場合、NetWorker クライアントと NetWorker 拡張クライアントをインストールします。NetWorker 9 のクライアントと拡張クライアントは、DPA エージェント ホストにインストールされる必要があります。以前のバージョンの NetWorker クライアントがある場合は、アップグレードする必要があります。古いバージョンの NetWorker を監視しているが、DPA エージェントを使用して NetWorker9 サーバーも監視している場合は、NetWorker 9 のクライアントと拡張クライアントを使用して他のバージョンを監視する必要があります。
2. NetWorker 7.6 以降をリモート監視する場合、DPA ユーザーおよびプロキシ ホストを、NetWorker Administrators User Group の［Users］リストに追加する必要があります。たとえば、NetWorker をホスト DPA エージェント ホストからリモート監視しており、エージェントが Windows ユーザーの DPA エージェントとして実行されている場合、管理者のプロパティの［Users］リストに次の行を追加する必要があります。

   ```
   user=DPAAgent,host=DPAAgentHost
   ```

3. DPA が 14 日前からのジョブ データを収集するようにする場合、NetWorker のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。

NetWorker 検出後のジョブ データ収集について

DPA 内に NetWorker を検出した後の NetWorker ジョブ データ収集について説明します。

- 新しい NetWorker サーバーが検出されると、DPA は 14 日前からのジョブ データを収集します。
- Jobmonitor リクエストがいくつか実行されると、収集されたジョブの期間が現時点に追いつき、新しいバックアップが収集されます。

この操作の結果として、jobmonitor リクエストが現在のジョブ データを収集し始めるには 7 時間かかります。その理由は、各リクエストはデフォルトで 30 分間隔で実行されるようスケジュール設定されており、リクエストごとに 1 日分のデータが収集されるためです。詳細については、モジュール別データ コレクション リクエスト オプションを参照してください。

HP Data Protector の監視

HP Data Protector サーバは、HP Data Protector Cell Manager 上で実行されているエージェントから監視することも、別のコンピュータ上のエージェントからリモート監視することもできます。

HP Data Protector の監視用に［Discovery Wizard］を開始する前に

Cell Manager をリモートで監視する場合は、HP Data Protector のリモート監視（166 ページ）で説明したのと同じ手順に従ってください。

注

ステータス リクエストは `omnisv` コマンドに依存するため、HP Data Protector サーバーをリモートで監視する際は、このリクエストを割り当てることはできません。このコマンドは、Data Protector サーバーでのみ使用できます。

［Manager of Managers］オプションを使用する Data Protector 環境を監視する場合、リモート Data Protection サーバーを監視しているかのように DPA を構成する必要があります。

HP Data Protector をリモート監視する場合は、HP Data Protector クライアント ソフトウェアをエージェントのホストにインストールし、Data Protector Cell Manager で、レポートの実行権限を持つようにクライアントを構成する必要があります。エージェント ホストからの接続性のテストについては、HP Data Protector のリモート監視（166 ページ）を参照してください。

DPA が 14 日前からのジョブ データを収集するようにする場合、HP Data Protector のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。

占有データ収集

デフォルトでは、占有データ収集は HP Data Protector で有効になっていません。占有データ収集を有効化するには、DataProtector Jobmonitor リクエストの占有オプションを有効化し、［**Edit Request**］ダイアログで DataProtector Client Occupancy リクエストを Data Protector クライアントに割り当てる必要があります。

DP_OCCUPANCY_DB_PATH 環境変数を使用して、jobmonitor リクエストの実行時に占有データが格納される場所を DPA エージェントで制御できます。DP_OCCUPANCY_DB_PATH 環境変数を使用しない場合、占有データは一時ディレクトリに格納されます。

注

HP DataProtector の占有情報を収集すると、Data Protector サーバーのパフォーマンスに重大な影響を与えます。

Linux での占有データベースの場所の変更

手順

1. DPA エージェントを停止します。
2. `cd` コマンドを使用して、`/opt/emc/dpa/agent/etc` ディレクトリにアクセスします。
3. `dpa.custom` ファイルを編集します。ファイルの最後に次のエントリーを追加します。

   ```
   COLLECTOR_DP_OCCUPANCY_DB_PATH=/your/absolute/path/
   export COLLECTOR_DP_OCCUPANCY_DB_PATH
   ```

   パスの末尾にバック スラッシュ（/）文字を含めてください。

4. DPA エージェントをリスタートします。

Windows での占有データベースの場所の変更

手順

1. DPA エージェントを停止します。
2. 管理者ユーザーとして regedit.exe を実行します。
3. HKEY_LOCAL_MACHINE レジストリ キーを拡張します。

4. SOFTWARE レジストリ キーを拡張します。
5. EMC レジストリ キーがまだ存在しない場合は作成します。
6. DPA レジストリ キーがまだ存在しない場合は作成します。
7. Agent レジストリ キーがまだ存在しない場合は作成します。
8. DP_OCCUPANCY_DB_PATH という名前の新しい文字列レジストリ値を作成し、値を目的のディレクトリ パスに設定します。

   次に例を挙げます。`C:\DPA\OccupancyData\`パスにバック スラッシュ（\）文字を含めてください。
9. DPA エージェントをリスタートします。

omnirpt パッチ

HP は、Data Protector 6.1 用のパッチをリリースしました。DPA で Data Protector 6.1 をサポートするには、このパッチを Data Protector 6.1 にインストールする必要があります。

次の表に、必要なパッチ ID をプラットフォーム別にリストします。

表 35 HP Data Protector 6.1 パッチ ID

プラットフォーム	パッチ ID
Windows	DPWIN_00417
HPUX PA-Risc	PHSS_39512
HPUX IA64	PHSS_39513
Linux	DPLNX_00077
Solaris	DPSOL_00371

パッチは HP（www.hp.com）から、ステータスが General Release のものを入手できます。HP ホーム ページの［Search］フィールドにパッチ ID を入力します。パッチのダウンロード ページにリダイレクトされます。

リストア ジョブ データと更新済み占有保存時間の構成

次の手順を行って、jobmonitor 機能のリストア ジョブ データと更新済み占有保存時間を取得します。

手順

1. HP Data Protector Manager UI で、［**Internal Database**］ > ［**Global Options**］の順に選択します。
2. 次のオプションを追加します。

オプション	**説明**
EnableRestoreReportStats	拡張リストア セッション データを有効にします
LogChangedProtection	占有の変更された保存期間をログに記録します

   両オプションの値を［**1**］に設定し、ともに［**In Use**］を選択します。
3. `omnisv` コマンドで HP Data Protector サービスを再起動して変更内容を反映します。

HP Data Protector のリモート監視

Cell Manager を監視するコンピューターにクライアント ソフトウェアをインストールする必要があります。

手順

1. Data Protector Manager の管理 GUI を起動し、クライアントを追加します。
2. クライアントにインストールするソフトウェア コンポーネントを選択する場合は、［**User Interface**］オプションが選択されていることを確認します。

   Cell Manager からデータを収集するには、DPA Data Protector モジュールが、`omnirpt` や `omnicellinfo` などのコマンドにアクセスする必要があります。これらのコンポーネントは、ユーザー インターフェイス コンポーネントをインストールした場合にのみインストールされるため、このオプションを選択することが重要です。

3. Cell Manager でのレポートの実行権限を持つようにクライアントを構成します。エージェント プロセスを実行するユーザーを最初に決定します。
   - UNIX システムでは、エージェントは常に root ユーザーとして実行されます。
   - Windows システムでは、エージェントは DPA エージェント サービス ユーザーとして実行されます。Windows システムのサービスのユーザーを確認するには、Windows サービス コントロール マネージャーを起動し、DPA エージェント サービスの詳細を表示します。
4. エージェントのユーザー名に一致するユーザーを Cell Manager で作成します。ホストの名前を［**user definition**］フィールドに入力します。
5. ［レポート作成および通知］権限と［個人用オブジェクトの参照］権限を持つ Data Protector ユーザー グループにユーザーを追加します。

   通常、ユーザーを admin グループに追加することになります。ただし、ユーザーがその他の管理者権限を継承できないようにするには、レポート作成および通知権限と個人用オブジェクトの参照権限を持つ新しいグループを作成して、そのグループにユーザーを追加します。

6. エージェントのホストから次のコマンドを実行し、リモート認証権限が正しく設定されていることを確認します。

   ```
   omnirpt -tab -report list_sessions -timeframe 06/01/01 12:00
   06/01/30 12:00
   ```

   正しく実行されると、このコマンドは、指定した期間内に Data Protector サーバーで実行されたすべてのセッションのリストを返します。レポートを実行するには権限が不十分であることを示すエラーが表示された場合は、Data Protector サーバーで構成の設定を確認します。

IBM TSM（Tivoli Storage Manager）の監視

TSM サーバーを、TSM サーバー上で実行されているエージェントから監視するか、または別のホスト（DPA サーバーなど）で実行されているエージェントからリモート監視します。TSM をリモート監視する場合は、TSM のリモート監視（168 ページ）でサーバーを構成する前に DPA の説明に従ってください。

TSM の監視用に［Discovery Wizard］を開始する前に

TSM の認証情報では、TSM Administrator の名前とパスワードを使用する必要があります。Administrative ユーザーは、システムに関するすべての権限を持っている必要はありません。Analyst または Operator 権限で十分です。

手順

1. 監視対象のサーバーが共有ライブラリ クライアントの場合、特定のデータを収集するために、サーバーのライブラリ マネージャーへのクエリーを実行するには、次の DPA 環境変数（UNIX）またはレジストリ設定（Windows）を使用して、エージェントを設定します。
   - AGENT_TSM_LIBMGRUSERNAME
   - AGENT_TSM_LIBMGRPASSWORD

   デフォルトでは、エージェントは、ライブラリ クライアントのクエリーとライブラリ マネージャのクエリーに同じ認証情報を使用します。
2. DPA が 14 日前からのジョブ データを収集するようにする場合、TSM のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。
3. ［Discovery Wizard］を使用して TSM オブジェクトを作成した後で作成される TSM 認証情報を変更するには、［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択します。

Gresham Clareti EDTGresham Clareti EDT

デバイスの制御に Gresham Clareti EDT を使用している Tivoli Storage Manager 環境では、DPA は EDT を使用して通信を行い、

- `elm.conf`
- `rc.edt`

DPA は、次の場所にある `elm.conf` を読み取ります。

- Windows では、EDT によって EDT_DIR という環境変数が設定されます。DPA は EDT_DIR に指定された場所を検索します。
- UNIX では、DPA は最初に `/opt/GESedt-acsls/bin` で `elm.conf` を探します。見つからない場合、AIX では DPA は`/usr/lpp/dtelm/bin` で探します。その他の UNIX/Linux では、DPA は`/opt/OMIdtelm/bin` で探します。

これらのディレクトリに `elm.conf` ファイルが存在しない場合、必要に応じて、`AGENT_TSM_ELMCONF_FILENAME` という名前のレジストリ変数（Windows）または環境変数（UNIX）に `elm.conf` の場所を設定できます。

DPA は次の場所にある `rc.edt` ファイルを読み取ります。

- Windows では、DPA は環境変数 EDT_DIR に指定された場所を検索します。
- UNIX では、DPA は最初に `/opt/GESedt-acsls/SSI` で `rc.edt` を探します。見つからない場合、AIX では DPA は `/usr/lpp/dtelm/bin` で探します。その他の UNIX/Linux では、DPA は`/opt/OMIdtelm/bin` で探します。

これらのディレクトリに `rc.edt` ファイルが存在しない場合、必要に応じて、`AGENT_TSM_RCEDT_FILENAME` という名前のレジストリ変数（Windows）または環境変数（UNIX）に `rc.edt` の場所を設定できます。

注

EDT を使用している TSM 環境ではエージェントがこれらのファイルから読み取りを行って構成データを収集する必要があるため、エージェントは TSM サーバーと同じサーバーに存在する必要があります。

TSM のリモート監視

TSM インスタンスをリモートで監視する場合は、TSM インスタンスを監視するホストに TSM クライアント ソフトウェアをインストールする必要があります。TSM モジュールは、TSM クライアント ソフトウェアに含まれる `dsmadmc` コマンドを使用して TSM インスタンスに接続し、そのデータを収集します。

Windows コンピューターに対する TSM クライアントのデフォルトのインストールでは、DPA が必要とする管理コンポーネントはインストールされません。管理コンポーネントをインストールするには：

手順

1. TSM クライアントのインストール時に、プロンプトが表示されたら［**Custom**］をクリックします。
2. ［**Administrative Client Command Line Files**］を選択し、［**Next**］をクリックします。

   TSM クライアントのインストールが続行されます。
3. TSM クライアントのインストールが完了したら、［スタート］メニューから TSM バックアップ アーカイブ GUI を起動して、クライアントを初めて初期化します。ウィザードを使用してクライアントを構成します。
4. クライアントを構成するには、デフォルト値［**Help me configure the TSM Backup Archive Client**］を使用し、［**Next**］をクリックします。プロンプトが表示されたら、既存のオプション ファイルをインポートするか、新しいファイルを作成します。
5. デフォルト値［**Create a new options file**］をそのまま使用します。`dsm.opt` というブランクのオプション ファイルを TSM のインストール ディレクトリ（デフォルトは `baclient`）下の `C:\Program Files\Tivoli\TSM` ディレクトリに作成する必要があります。
6. ウィザードを使用して操作を続けます。新しいオプション ファイルが作成されるまで、ウィザードのすべてのウィンドウに入力します。

TSM 検出後のジョブ データ収集について

DPA 内に TSM を検出した後の TSM ジョブ データ収集について説明します。

- 新しい TSM サーバーが検出されると、DPA は 14 日前のジョブ データから収集を開始します。
- 次回ジョブ監視リクエストを実行すると、現在のポーリング間隔が次の日に設定され、次の日のデータが収集されます。
- 現在のポーリング間隔は、ジョブ監視リクエストが実行されるごとに、14 日前から 1 日ずつ進み、2 週間分のデータが収集されるまで各日のデータが収集されます。そこから、通常どおりデータ コレクションが再開されます。
- ポーリング間隔のデフォルト値は 1 日です。この値は、TSM の［Job Monitor］リクエスト オプション セクション下でユーザー設定できます。

詳細については、モジュール別データ コレクション リクエスト オプションを参照してください。

Symantec Backup Exec の監視

Symantec Backup Exec サーバーは、Backup Exec データベースで実行されているエージェントから、または環境内の他の Windows コンピューターで実行されているエージェントから監視します。

DPA エージェント サービスは、BackupExec サーバーを使用して認証できる指定アカウントで実行する必要があります。

Symantec Cluster Server および Microsoft Cluster Server 環境でのバックアップ サーバーの監視

このセクションでは、Symantec Cluster Server および MSCS（Microsoft Cluster Server）環境でバックアップ サーバーを監視するための構成情報を示します。

サポートするプラットフォーム

- Symantec Cluster Server は Linux および Solaris でサポートされています。
- MSCS は、Windows 上でサポートされています。

サポートされているプラットフォームのバージョンについては、「Data Protection Advisor Software Compatibility Guide」を参照してください。

クラスタの一部として構成されたバックアップ アプリケーションの監視

いくつかの方法で、クラスタの一部として構成されたバックアップ アプリケーションを監視できます。

クラスタ環境でバックアップ アプリケーションを監視するには：

手順

1. クラスタの外部のシステムにリモート エージェントをインストールします。次の事項を確認：
   - エージェントは、必要なポートを使用してクラスタの仮想サーバーにアクセスできる。
   - エージェントには、必要なバックアップ アプリケーション バイナリがインストールされている。
2. DPA の［Discovery Wizard］を使用して、クラスタの仮想サーバーを検出します。
3. リモート エージェントを使用してデータを収集します。

結果

この構成では、サーバーがフェイルオーバーした場合、クラスタ名は常に解決され、バックアップ データを提供します。

クラスタの一部として構成されたバックアップ アプリケーションを監視する代替処理手順
クラスタ環境でバックアップ アプリケーションを監視し、ローカル ホスト リソースを監視するには

手順

1. ホストの監視専用のローカル エージェントをクラスタの各ホストにインストールします。
2. 物理サーバーのエージェントの 1 つを選択して、仮想サーバーを監視します。

Symantec Backup Exec の監視用に［Discovery Wizard］を開始する前に

Symantec Backup Exec バックアップ サーバをリモート監視するには、エージェントを、ローカル システム アカウントではなく、指定ユーザーとして実行する必要があります。エージェントをインストールする場合は、ローカル システム アカウントを使用してエージェントを実行するのか、または指定ユーザーとして実行するのかを尋ねるプロンプトが表示されます。

Backup Exec の認証情報では、Backup Exec サーバ上の Windows 管理者アカウントのユーザー名とパスワードを使用しなければなりません。

［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択して、［Discovery Wizard］を使用して Backup Exec オブジェクトを作成した後に作成される Backup Exec Credentials を変更します。

Backup Exec のリモート監視

エージェントが実行されていることを確認するには、Windows Service Control Manager を起動します（[スタート] > [設定] > [コントロール パネル] > [管理ツール] > [サービス]）。DPA エージェント サービスを右クリックして、[Properties] を選択します。

手順

1. サービスの [Properties] パネルで [**Log On**] タブを選択します。
2. [**This Account**] を選択します。
3. ローカル管理者アカウントのユーザー名およびパスワードを入力してサービスを実行します。
4. サービス アカウントの詳細を変更し、[**OK**] をクリックします。
5. サービスを再起動して、変更を有効にします。

Symantec NetBackup の監視

Symantec NetBackup サーバーを、NetBackup Master Server 上で実行されているエージェントから監視するように、または、DPA サーバーなどの別のホストで実行されているエージェントから監視するように構成します。

Symantec NetBackup をプロキシ エージェントから監視する場合、プロキシ エージェントは同じ EMM（NetBackup Media Manager）ドメイン内にある NetBackup マスター サーバーを監視できます。これは、EMM ドメインごとにエージェントが必要であることを意味します。

Symantec NetBackup の監視用に［Discovery Wizard］を開始する前に

メディア サーバー ステータス データを収集できるのは、エージェントがメディア サーバー自体にインストールされている場合だけです。プロキシを介して収集することはできません。

openfiles、エラー、およびマウント情報を収集するには、jobmonitor リクエストで `timeformat` オプションを指定する必要があります。例：%m/%d/%Y %T
DPA が 14 日前からのジョブ データを収集するようにする場合、NetBackup のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、[**Inventory**] > [**Object Library**] > [**[**オブジェクトの選択**]**] > [**Data Collection**] の順に選択します。

リモート データ収集用の NetBackup 認証の構成

データをリモートで収集するには、次のように構成する必要があります。

- NetBackup サーバ ソフトウェアのコンポーネントである NetBackup リモート管理コンソールは、エージェントのホストにインストールする必要があります。
- エージェントのホストが、NetBackup Master Server を正常に解決できる。
- NetBackup Master Server がエージェントのホストを正常に解決できる。

次のセクションでは、UNIX および Windows で NetBackup Master Server からエージェント ホストを解決する方法について説明します。

UNIX でのリモート データ コレクション用の NetBackup 認証の構成
NetBackup Master Server が UNIX コンピューター上で稼働している場合、エージェントが実行されているホストの名前を、NetBackup Master Server の `bp.conf` ファイルに追加する必要があります。

ホストを追加するには、次の手順で行います。

手順

1. `/usr/openv/netbackup/bp.conf` を編集用に開き、次の行を追加します。

   `SERVER =Agenthost`
   ここで、Agenthost はエージェントのホスト名です。エージェントのホスト名は Master Server によって名前解決できなければなりません。

2. Master Server で NetBackup を再起動して、変更を有効にします。

Windows でのリモート データ コレクション用の NetBackup 認証の構成
NetBackup Master Server が Windows コンピュータ上で稼働している場合、エージェント ホストの名前を NetBackup の管理コンソールを介して追加します。

手順

1. NetBackup Server で［**NetBackup Administration Console**］を起動し、［**Master Server Properties**］ダイアログ ボックスを開きます。
   - ［**Netbackup Management**］ > ［**Host Properties**］ > ［**Master Servers**］の順に選択する。
2. 右側のパネルで［**Host**］をダブル クリックします。
3. ［**Master Servers Properties, Servers**］フィールドで、Master Server にアクセスできる追加サーバーのリストに、エージェント ホストの名前を入力します。
4. ［**OK**］をクリックします。
5. NetBackup サービスをリスタートします。または、マシンを再起動して変更をアクティブ化します。

Symantec PureDisk の監視

Symantec PureDisk サーバを、PureDisk Server 上で実行されているエージェントから監視するように、または、別のホストで実行されているエージェントから監視するように構成します。
Symantec PureDisk は、SUSE Linux 10 上でのみ監視できます。root ユーザーを使用して PureDisk からデータを収集することはできません。

Symantec PureDisk の監視用に［Discovery Wizard］を開始する前に

PureDisk サーバーは、ファイアウォールを実装します。ファイアウォールによって、DPA が PureDisk からデータ コレクションをできないようになるか、PureDisk サーバーにインストールしたエージェントと通信できないようになることがあります。データ コレクションと通信を正常に行うために、次のセクションでは、DPA でサーバーを構成する前に、PureDisk サーバーを構成する方法を説明します。

構成プロセスは、監視対象の PureDisk のバージョンに応じて異なります。

ファイアウォールの手動構成（PureDisk バージョン 6.5 よりも前）

手順

1. root ユーザーとして PureDisk サーバにログインします。
2. 次のコマンドを実行して PureDisk ファイアウォールを停止します。

   `/etc/init.d/pdiptables stop`

3. `/etc/puredisk/iptables-rules` ファイル内でこの行の直後に次の行のいずれかを挿入して、ファイルを編集します。

```
-A INPUT -p icmp -j ACCEPT
```

注

行をファイル内の正しい場所に挿入することが重要です。正しい場所に挿入されていないと、コマンドが機能しません。

- PureDisk サーバにインストールしたエージェントを使用して PureDisk を監視している場合は、次の行を追加します。

  -A INPUT -p tcp -m tcp --dport 3741 -j ACCEPT

- 別のホストで実行されているエージェントから PureDisk を監視している場合は、次の行を追加します。

  -A INPUT -p tcp -m tcp --dport 10085 -j ACCEPT

4. 次のコマンドを実行して PureDisk ファイアウォールを再起動します。

   /etc/init.d/pdiptables start

IP テーブル ルールの更新（PureDisk バージョン 6.5）

PureDisk バージョン 6.5 では、ファイアウォールは手動構成できません。PureDisk IP テーブルを更新するには、次の手順を実行します。

手順

1. テキスト エディターで次のファイルを開きます。

   ```
   /etc/puredisk/custom_iptables_rules
   ```

2. PureDisk サーバーに DPA エージェントがインストールされている場合は、ルール ファイルに次の行（タブで区切られた 3 個の列）を追加します。

   ```
   tcp     {controller_host_ip}     3741
   ```

   これにより、コントローラ ホストから PureDisk サーバー上のポート 3741 の DPA エージェントに接続できるようになります。

3. リモート ホストに DPA エージェントがインストールされている場合は、ルール ファイルに次の行（タブで区切られた 3 個の列）を追加します。

結果

```
tcp     {agent_host_ip}     10085
```

これにより、エージェント ホストから PureDisk サーバー上のポート 10085 の Postgres データベースに接続できるようになります。

シングル ホストまたは次の例のように（スラッシュ マスクを含めることで）サブネット全体のいずれかを指定できます。

```
tcp    10.64.205.0/24                  10085
```

/etc/puredisk/custom_iptables_rules ファイルにより、このファイル自体の構成に関する追加情報が提供されます。

VMware vSphere Data Protection の監視

VMware VDP/A（vSphere Data Protection）サーバーの監視は、環境内の任意のリモート コンピューターにインストールされている DPA エージェント（DPA サーバーなど）を使用して行います。

DPA エージェントは、VMware vSphere Data Protection サーバーにインストールしないでください。

VDP/A の監視用に［Discovery Wizard］を開始する前に

VMware vSphere Data Protection サーバーをリモートから監視するために追加のソフトウェアは必要ありません。

はじめに

VMware vSphere Data Protection サーバーの解決可能なホスト名または IP アドレスが必要です。

VMware vSphere Data Protection サーバーからデータを収集するため、DPA は直接、VDP/A データベースに接続します。デフォルト ポート 5555 でデータベースに接続します。ポートは構成できません。

VDP 5.5、5.8、6.0 の監視用

手順

1. `postgressql.conf` ファイルを編集します。次の行のコメント処理を解除し、`localhost` を `localhost, Agent_IP_Address` に変更します。

```
vi /data01/avamar/var/mc/server_data/postgres/data/
postgresql.conf
listen_addresses='localhost,Agent_IP_Address'
```

2. `pg_hba.conf` ファイルを編集します。2 番目の行として次を追加します。

```
vi /data01/avamar/var/mc/server_data/postgres/data/pg_hba.conf
host all all Agent_IP_Address/0 trust
```

3. firewall.base`vi /etc/firewall.base` を編集します。
   a. Postgres db サービスへのリモート アクセスを有効にします。
   b. `firewall.base` ファイルの末尾に次の数行を追加します。

```
iptables -I INPUT 1 -p tcp --dport 5555 -j ACCEPT
iptables -I INPUT 1 -p tcp --dport 5558 -j ACCEPT
```

4. VDP アプライアンスを再起動します。

Data Domain Backup Enterprise Applications の監視

DPA では、NetWorker を使用しない Oracle RMAN のバックアップなど、別のバックアップ アプリケーションを使用せずにデータベースをバックアップするために、DDBEA（Data Domain Backup Enterprise Applications）がサポートされます。サポートされているデータベースについては、「EMC Data Protection Advisor Software Compatibility Guide」を参照してください。

Enterprise App で Oracle RMAN のバックアップを監視する場合は、Oracle および Oracle RMAN の監視（177 ページ）に記載されている処理手順に従います。

エンタープライズ アプリケーションによる Microsoft SQL サーバーのバックアップを監視する場合は、Microsoft SQL Server の監視（176 ページ）の手順に従います。

エンタープライズ アプリケーションによる PostgreSQL のバックアップを監視する場合は、PostgreSQL の監視（183 ページ）の手順に従います。

エンタープライズ アプリケーションによる SAP HANA のバックアップを監視する場合は、SAP HANA の監視（184 ページ）の手順に従います。

データベースの監視

このセクションでは、データベースを監視する方法について説明します。

DB2 の監視

DB2 データベースは、DB2 サーバーと同じホストで実行されているエージェントから監視することも、DPA サーバーなどの別のホストで実行されているエージェントから監視することもできます。DPA エージェントは、Windows または Linux 上で実行する必要があります。

DB2 の監視用に［Discovery Wizard］を開始する前に

DPA エージェントが DB2 データベースからデータを収集するには、DB2 クライアントの.jar ファイルを DPA プラグインのディレクトリにコピーする必要があります。

手順

1. 「の下に<DPA_install_dir>\agent\plugins」という名前のディレクトリを作成します。
2. DB2 クライアントの jar ファイル「db2jcc4.jar」を、..\EMC\dpa\agent\の下の「plugins」フォルダーにコピーします。

   カスタムの場所やパスを使用する場合は、タグ <PLUGINSDIR>path </PLUGINSDIR> in dpaagent_config.xml を追加します。これは、<DPA_install_dir>\agent\etc の下にあります。

   ここで、path はステップ 1 で作成したディレクトリのパスです。

   例：<PLUGINSDIR>c:\program files\emc\dpa\agent\plugins</PLUGINSDIR>
3. DPA が 14 日前からのジョブ データを収集するようにする場合、TSM のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［ オブジェクトの選択］ > ［**Data Collection**］の順に選択します。

権限

DB2 でデータを収集するための適切な権限があることを確認します。

以下に対して、選択操作の権限があることを確認します。

- sysibmadm.db_history ビュー。
- <user_name>.UTILSTOP_DPABACKUP と sysibm.syscolumns テーブル。これは、DB2 バージョン 11.1.1.1 以降の場合に必要です。

Backup All Jobs レポートにサイズ フィールドを表示するよう DB2 を設定する

DPA Agent が DB2 バックアップ サイズ値とともに DPA サーバーにデータを送信させるには、DB2 データベース自体に DB2 EVENT MONITOR DPABACKUP を作成する必要があります。

はじめに

- DPA では、DB2 バージョン 11.1.1 以降に対してのみ、バックアップ サイズの計算をサポートしています。
- イベント モニターは、DB2 Jobmonitor リクエストに認証情報が割り当てられている同一ユーザーが作成する必要があります。

この手順は、DB2 データベース上で実行してください。DB2 上でこれらのステップを実行する方法の詳細については、ベンダーのドキュメントを参照してください。

手順

1. イベントの作成：**`CREATE EVENT MONITOR DPABACKUP FOR CHANGE HISTORY WHERE EVENT IN (BACKUP) WRITE TO TABLE autostart`**
2. イベント モニタを有効にします。
3. イベント モニタを `DPABACKUP state 1` に設定します。
4. イベントが正しく作成されていることを確認します。オンラインでデータベースのバックアップを実行します。「**`backup database sample online`**」と入力します。

   新しいレコードが、テーブル内に存在します。
5. ［*__from UTILSTOP_DPABACKUP__］を選択します。

検出後のジョブ データ収集について

DPA でアプリケーションを検出した後のジョブ データ収集について説明します。

このセクションの情報は、次のアプリケーションに適用されます。

- NetWorker
- Avamar
- TSM
- HP DataProtector
- Commvault Simpana
- NetBackup
- ArcServ
- DB2
- SAP HANA
- RMAN
- MSSQL

上記のアプリケーションに関して、次のことに注意してください。

- この機能を有効にした場合、新しいサーバーが検出されると、DPA は 14 日前のジョブ データから収集を開始します。
- 次回ジョブ監視リクエストを実行すると、現在のポーリング間隔が次の日に設定され、次の日のデータが収集されます。

- 現在のポーリング間隔は、ジョブ監視リクエストが実行されるごとに、14 日前から 1 日ずつ進み、2 週間分のデータが収集されるまで各日のデータが収集されます。そこから、通常どおりデータ コレクションが再開されます。
- ポーリング間隔のデフォルト値は 1 日です。この値は、[Job Monitor] リクエスト オプション セクションでユーザー設定できます。
- データ コレクションを設定する際、[**Frequency**] は、必ず [各リクエストがデータを収集する最大時間範囲] よりも小さい値にする必要があります。そうしないと、リクエストが現在の時刻およびリクエストが実行される各時刻に間に合わずに遅れてしまい、残りのデータを収集できなくなります。

詳細については、モジュール別データ コレクション リクエスト オプションを参照してください。

Microsoft SQL Server の監視

Microsoft SQL Server の監視は、SQL Server データベースで実行中のエージェントから、または環境内の他の Windows コンピューターで実行中のエージェントから行う必要があります。DPA エージェント サービスは、Microsoft SQL Server で認証可能な指定アカウントで実行する必要があります。

必ず SQL Server ブラウザー サービスの SQLBrowser.exe への受信接続を許可するようにファイアウォールの受信規則を指定します。UDP ポート 1434 を使用します。

Microsoft SQL Server の監視用に［Discovery Wizard］を開始する前に

Windows 認証を使用して SQL Server に接続するには、DPA エージェントは、ローカル システム アカウントではなく、MS-SQL アクセス権を持つ指定ユーザーとして実行される必要があります。データベースの構成を続行する前に、サービスが正しいユーザーとして実行されていることを確認します。

クラスタ化された SQL Server のインストールを監視するには、DPA エージェントがクラスタの物理ノードにローカルでインストールされている場合でも、リモートのターゲットとして監視するように DPA を設定します。ターゲット名は、クラスタのエイリアス名に設定する必要があります。
データベースの監視を選択しない場合でも、DPA 検出のテスト中に、DPA エージェントが DPA マスターと MSDB データベースの両方に読み取りアクセスができることを確認します。

Microsoft SQL Server を監視するためのエージェント要件

必要なデータを収集するには、エージェントは SQL Server のマスター データベースに接続できる必要があります。エージェントでは、次のいずれかを実行できます。

- リクエストの認証情報を使用して SQL Server 認証を使用する（設定されている場合）。
- 監視対象のデータベース リスト内の明示的なマスター データベースに対する認証情報を使用して SQL Server 認証を使用する（設定されている場合）
- これらが設定されていない場合は、エージェントはエージェント プロセスのログイン ID を使用して Windows 認証を使用します。

これらのいずれもマスター データベースへの接続に十分でない場合は、リクエストではデータは収集できません。

Microsoft SQL Server を監視するためのユーザー アカウント要件

データを正常に収集するには、SQL Server データベースへの接続に使用されるユーザー アカウントに、特定の権限が付与されている必要があります。dbo アクセス権を持つ SQL Server ユーザーには、デフォルトで適切な権限が付与されます。

dbo アクセス権を持つユーザーで接続しない場合、次のようにユーザーを構成します。

- ユーザーをパブリック役割でデータベースにマップします。
- VIEW SERVER STATE および VIEW DEFINITION 権限を明示的に付与します（SQL Server 2005 限定）。
  VIEW SERVER STATE 権限はサーバ レベルで付与されます。VIEW DEFINITION 権限は、サーバ レベル（名前 VIEW ANY DEFINITION）、またはデータベース、スキーマ、個々のオブジェクト レベルで付与できます。
- システムの実行権限を明示的に許可します `stored procedure xp_readerrorlog`。

SQL Server 2005 および 2008

すべてのデータベース テーブルの VIEW DEFINITION 権限といったサーバ規模の権限を、エージェントで使用される SQL Server ログインに付与するには、SQL Server に管理者として接続し、次のコマンドを実行します。

```
GRANT VIEW SERVER STATE TO <login\domain> GRANT VIEW ANY DEFINITION TO <login\domain>
```

ただし、監視する特定のデータベースだけに VIEW DEFINITION 権限を付与するには、SQL Server に管理者として接続して、次のコマンドを実行します。

```
GRANT VIEW SERVER STATE TO [login\domain] GRANT VIEW DEFINITION ON DATABASE :: <dbname> TO <username>
```

システム ストアド プロシージャ xp_readerrorlog の実行許可を付与するには、次を実行します。

```
USE Master GO GRANT EXECUTE ON OBJECT::sys.xp_readerrorlog TO ddDBO GO
```

レプリケーション解析用の Microsoft SQL Server の監視

DPA サーバーは、すべてのデータベースの接続権限および TEMPDB データベースの書き込み権限を持つデータベース ユーザーとして接続する必要があります。Windows 認証の場合、ユーザーは、すべての SQL Server データベースに接続でき、TEMPDB データベースの書き込み権限がなければなりません。

Oracle および Oracle RMAN の監視

DPA は、Oracle の 2 つの部分からデータを収集できます。その 1 つは Oracle データベース自体で、データベース インスタンスに関するメトリックを収集します。もう 1 つは Oracle RMAN です。いずれの場合も、Oracle クライアント ソフトウェアをインストールする必要があります。

DPA には、DPA エージェントを伴う OCI（Oracle クライアント）ライブラリは付属していません。インストール先となるプラットフォームや OS に適した Oracle インスタント クライアント ソフトウェアを、oracle.com からダウンロードできます。アーキテクチャのバージョンを、OS や Oracle のバージョンと一致させるようにしてください。たとえば、Oracle の 12c データベースからデータを収集するには、Oracle 12c インスタント クライアント バージョンを使用します。バージョンが混在する Oracle からデータを収集する場合、環境内で最新のインスタント クライアント バージョンを使用します。DPA エージェントが Oracle データベースまたは Oracle RMAN からデータを収集するには、DPA は Oracle の次のライブラリを必要とします。

- `libociei.so`
- `libocci.so`
- `libclntsh.so`
  `libclntsh.so` ライブラリに対して現在の Oracle ビルド ディレクトリへのシンボリック リンクを作成する必要があります。詳細については、UNIX で現在の Oracle ビルド ディレクトリへのシンボリック リンクを作成する（178 ページ）を参照してください。

DPA エージェントで動作させるには、AGENT_ORACLE_CLIENT_PATH に手動でコピーする必要があります。

これは、Windows では OCI.DLL で、UNIX では libclntsh.so です。

注

ライブラリは DPA エージェントと同じプラットフォーム用である必要があります。たとえば、64 ビットの Windows DPA エージェントがインストールされている場合は、64 ビットの Windows Oracle ライブラリを使用する必要があります。

Oracle Database Instant Client は http://www.oracle.com/technetwork/database/features/instant-client/index.html からダウンロードできます。

DPA エージェントのインストール中に、エージェントを利用して Oracle を監視するかどうかを指定するように求められます。利用する場合は Oracle クライアント ライブラリの場所を指定します。Windows では、このアクションによってレジストリが設定され、UNIX では dpa.config ファイル内の環境変数を変更します。インストール プロセスが完了した後でライブラリの場所を変更する場合は、このステップを手作業で実行する必要があります。

UNIX で現在の Oracle ビルド ディレクトリへのシンボリック リンクを作成する

libclntsh.so ライブラリに対して現在の Oracle ビルド ディレクトリへのシンボリック リンクを作成する必要があります。DPA エージェントで動作させるには、AGENT_ORACLE_CLIENT_PATH に手動でコピーする必要があります。

手順

1. rpm コマンドを使用してインストールします。**rpm -i oracle.instantclient<version.build.architecture>.rpm** を実行します。

   例：**rpm -i oracle.instantclient12.1-basic-12.1.0.2.0-1.x86.rpm**
   出力 /usr/lib/oracle/12.1/client64/lib には、最新の Oracle クライアントが示されています。例： libclntsh.so.12.1

2. libclntsh.so に対するシンボリック リンクを作成し、ファイルの実行権限を追加します。**ln-s libclntsh.so < version.build.architecture > libclntsh.so chmod 755 *** を実行します。

   例：**ln -s libclntsh.so.21.1 libclntsh.so chmod 755 ***

3. /usr/lib/oracle に現在の Oracle ビルドが作成されていることを確認します（http://docs.oracle.com/cd/B19306_01/server.102/b14357/ape.htm）。

Windows

手順

1. Oracle インスタント クライアント ソフトウェアの場所でレジストリ エントリーを更新します。
   a. Oracle クライアント ソフトウェアがあるフォルダに移動します。
   b. regedit を使用して、Oracle インスタント クライアント ソフトウェアの場所を手動で編集します。

Oracle データベースおよび Oracle RMAN を監視するための手作業での DPA Agent の構成

- 手作業で DPA Agent を構成して Oracle RMAN を監視するには次の手順を実行します。Windows で、次のように値のタイプが REG_SZ である「HKLM/Software/EMC/DPA/Agent」レジストリを設定します。

値の名前：ORACLE_CLIENT_PATH

値のデータ：<directory containing the Oracle client libraries - oci.dll>

注

レジストリ キーは、DPA Agent のインストール中に［Oracle database to be monitored］オプションを選択した場合に作成されます。レジストリ キーが作成されない場合は、手作業で作成する必要があります。

- UNIX では、dpa.config ファイルを変更します。

dpa.config ファイルは<installdir>/agent/etc/dpa.config にあります。AGENT_ORACLE_CLIENT_PATH=という行を検索し、変数を Oracle クライアント ライブラリ（libclntsh.so）が含まれるディレクトリに設定します。

dpa.config ファイルを変更して Oracle クライアントのパスを含めた場合は、Agent サービスを再開します。

注

RMAN ライセンス要件について、EMC 担当営業にお問い合わせください。

Oracle の監視用に［Discovery Wizard］を開始する前に

データ保護データの Oracle データベースを監視するには、エージェントが Oracle ユーザーとしてデータベースに接続している必要があります。

はじめに

DPA では、Oracle サーバーのオペレーティング システム パスワードは要求されません。DPA で要求される Oracle ユーザー名とパスワードは、RMAN カタログまたはシステム カタログのクエリーにのみ使用されます。

Oracle データベースのデータを正常に収集するには、このユーザーが次のテーブルとビューで選択を実行する権限を持っている必要があります。

- V_$INSTANCE
- V_$PROCESS
- V_$DATABASE
- V_$PARAMETER
- DBA_DATA_FILES
- V_$SYSTEM_PARAMETER
- V_$DATAFILE
- V_$SESS_IO
- V_$SESSION
- DBA_FREE_SPACE
- V_$SESSMETRIC（Oracle 10 のみ）
- DBA_TABLESPACES
- DBA_TEMP_FILES
- DBA_EXTENTS

- USER_EXTENTS
- V$LOGFILE
- V$LOG
- AUDIT_ACTIONS
- V$CONTROLFILE

デフォルトでは、SYSDBA の役割を持つユーザーはこれらの権限を持っているため、監視用にデータベースを構成する場合、SYSDBA の役割を持つユーザーを指定することをお勧めします。
SYSDBA の役割を持つユーザーを接続に使用しない場合は、別のユーザーを作成し、次の例のように、これらのテーブルに権限を明示的に付与するか、「create session」権限を付与してから SELECT_CATALOG_ROLE 権限を付与します。

注

クラスタ セットアップから Oracle データを取得するには、次の情報が必要になります。

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT ON V_$INSTANCE TO limited_user;
GRANT SELECT ON V_$PROCESS TO limited_user;
GRANT SELECT ON V_$DATABASE TO limited_user;
GRANT SELECT ON V_$PARAMETER TO limited_user;
GRANT SELECT ON DBA_DATA_FILES TO limited_user;
GRANT SELECT ON V_$SYSTEM_PARAMETER TO limited_user;
GRANT SELECT ON V_$DATAFILE TO limited_user;
GRANT SELECT ON V_$SESS_IO TO limited_user;
GRANT SELECT ON V_$SESSION TO limited_user;
GRANT SELECT ON DBA_FREE_SPACE TO limited_user;
GRANT SELECT ON DBA_TABLESPACES TO limited_user;
GRANT SELECT ON DBA_EXTENTS TO limited_user;
GRANT SELECT ON USER_EXTENTS TO limited_user;
GRANT SELECT ON DBA_TEMP_FILES TO limited_user;
GRANT SELECT ON V_$LOGFILE TO limited_user;
GRANT SELECT ON V_$LOG TO limited_user;
GRANT SELECT ON  AUDIT_ACTIONS TO limited_user;
GRANT SELECT ON V_$CONTROLFILE TO limited_user;
exit;
```

または

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
exit
```

Oracle データベース 12c RAC インストールで CDB（コンテナ データベース）に接続する場合、監視用にデータベースを構成する際に、SYSDBA の役割を持つ一般的なユーザーを使用できます。接続に SYSDBA の役割を持つユーザーを使用したくない場合は、別のユーザーを作成することができます。この場合、「c##」または「C##」のプレフィックスを付加し、上記の例のように、これらのテーブルに権限を付与するか、「create session」権限を付与してから SELECT_CATALOG_ROLE 権限を付与します。

PDB（プラガブル データベース）に接続する場合、監視用にデータベースを構成する際に、SYSDBA の役割を持つ一般的なユーザーを使用できます。SYSDBA の役割を持つ一般的なユーザーを接続に使用しない場合は、別の PDB 専用のローカル ユーザーを作成し、これらの PDB テーブルに権限を明示的に付与するか、PDB に「create session」権限を付与してから SELECT_CATALOG_ROLE 権限を付与します。

RMAN の監視用に［Discovery Wizard］を開始する前に

データ保護データの RMAN データベースを監視するには、エージェントが Oracle ユーザーとしてデータベースに接続している必要があります。

はじめに

Oracle DBA、RMAN カタログ、またはシステム カタログ クエリーから次の接続パラメーターの情報を入手してください。

- RMAN カタログの Oracle SID
- RMAN カタログに使用する Oracle TNS ポート
- 必要な特権を持つ Oracle RMAN ユーザー名/パスワード。これは、SELECT のみの特権または SELECT_CATALOG_ROLE 特権です。1 台の Oracle サーバーに複数の RMAN カタログがある場合は、それぞれのスキーマにユーザー名とパスワードが必要です。すべての RMAN カタログ/スキーマで同じユーザー名/パスワードを使用することをお勧めします。
- RMAN スキーマの所有者名と、1 台の Oracle サーバーに複数の RMAN カタログがある場合は、すべての RMAN スキーマ所有者名

Oracle RMAN ジョブ監視リカバリ カタログのデータを正常に収集するには、このユーザーが次のテーブルとビューで選択を実行する権限を持っている必要があります。

- V_$RMAN_CONFIGURATION
- RC_BACKUP_SET
- V$PROXY_DATAFILE
- RC_RMAN_BACKUP_JOB_DETAILS
- RC_BACKUP_DATAFILE
- RC_BACKUP_PIECE
- RC_DATAFILE
- RC_DATABASE
- RC_BACKUP_CONTROLFILE
- RC_BACKUP_CONTROLFILE_DETAILS
- RC_BACKUP_DATAFILE_DETAILS
- RC_RMAN_STATUS
- RC_BACKUP_ARCHIVELOG_DETAILS
- RC_BACKUP_REDOLOG
- RCVER
- PRODUCT_COMPONENT_VERSION

Oracle ジョブ監視制御ファイルのデータを正常に収集するには、このユーザーが次のテーブルとビューで選択を実行する権限を持っている必要があります。

- V_$RMAN_CONFIGURATION
- V_$RMAN_STATUS
- V_$BACKUP_DATAFILE
- V_$BACKUP_PIECE
- V$BACKUP_SET
- V$PROXY_DATAFILE

- V$RMAN_BACKUP_JOB_DETAILS
- V$DATABASE
- V$DATAFILE
- V$BACKUP_DATAFILE_DETAILS
- V$BACKUP_ARCHIVELOG_DETAILS
- V$BACKUP_REDOLOG
- RCVER
- PRODUCT_COMPONENT_VERSION

デフォルトでは、SYSDBA の役割を持つユーザーはこれらの権限を持っているため、監視用にデータベースを構成する場合、SYSDBA の役割を持つユーザーを指定することをお勧めします。
SYSDBA の役割を持つユーザーを接続に使用しない場合は、別のユーザーを作成し、次の例のように、これらのテーブルに権限を明示的に付与するか、「create session」権限を付与してから SELECT_CATALOG_ROLE 権限を付与します。

注

クラスタ セットアップから Oracle データを取得するには、次の情報が必要になります。

Oracle RMAN ジョブ監視リカバリ カタログの場合：

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT ON V_$RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON RC_BACKUP_SET TO limited_user;
GRANT SELECT ON V$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON RC_RMAN_BACKUP_JOB_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_DATAFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_PIECE TO limited_user;
GRANT SELECT ON RC_DATAFILE TO limited_user;
GRANT SELECT ON RC_DATABASE TO limited_user;
GRANT SELECT ON RC_BACKUP_CONTROLFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_CONTROLFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_DATAFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_RMAN_STATUS TO limited_user;
GRANT SELECT ON RC_BACKUP_ARCHIVELOG_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_REDOLOG TO limited_user;
exit;
```

または

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
exit
```

デフォルトでは、仮想カタログ ユーザーは基本リカバリ カタログにアクセスできません。メタデータにアクセスするには、以下の権限を付与する必要があります。

```
GRANT RECOVERY_CATALOG_OWNER to limited_user;
 GRANT CATALOG for DATABASE db to limited_user;
```

Oracle ジョブ監視制御ファイルの場合：

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT ON V_$RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON V_$BACKUP_DATAFILE TO limited_user;
GRANT SELECT ON V_$BACKUP_PIECE TO limited_user;
GRANT SELECT ON V_$RMAN_STATUS TO limited_user;
GRANT SELECT ON V_$BACKUP_SET TO limited_user;
GRANT SELECT ON V_$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON V_$RMAN_BACKUP_JOB_DETAILS TO limited_user;
GRANT SELECT ON V_$DATABASE TO limited_user;
GRANT SELECT ON V_$BACKUP_DATAFILE_DETAILS TO limited_user;
GRANT SELECT ON V_$DATAFILE TO limited_user;
GRANT SELECT ON V_$BACKUP_ARCHIVELOG_DETAILS TO limited_user;
GRANT SELECT ON V_$BACKUP_REDOLOG TO limited_user;
GRANT SELECT ON V_$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON V_$RMAN_BACKUP_JOB_DETAILS TO limited_user;
exit;
```

または

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
exit
```

Oracle データベース 12c RAC インストールで CDB（コンテナ データベース）に接続する場合、監視用にデータベースを構成する際に、SYSDBA の役割を持つ一般的なユーザーを使用できます。接続に SYSDBA の役割を持つユーザーを使用したくない場合は、別のユーザーを作成することができます。この場合、「c##」または「C##」のプレフィックスを付加し、上記の例のように、これらのテーブルに権限を付与するか、「create session」権限を付与してから SELECT_CATALOG_ROLE 権限を付与します。

PDB（プラガブル データベース）に接続する場合、監視用にデータベースを構成する際に、SYSDBA の役割を持つ一般的なユーザーを使用できます。SYSDBA の役割を持つ一般的なユーザーを接続に使用しない場合は、別の PDB 専用のローカル ユーザーを作成し、これらの PDB テーブルに権限を明示的に付与するか、PDB に「create session」権限を付与してから SELECT_CATALOG_ROLE 権限を付与します。

DPA が 14 日前からのジョブ データを収集するようにする場合、Oracle RMAN のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［**[**オブジェクトの選択**]**］ > ［**Data Collection**］の順に選択します。

PostgreSQL の監視

PostgreSQL データベースは、PostgreSQL データベースと同じホストで実行されているエージェントから監視することも、DPA サーバーなど、別のホストで実行されているエージェントから監視することもできます。

PostgreSQL の監視用に［Discovery Wizard］を開始する前に

PostgreSQL データベースを監視するには、エージェントが PostgreSQL スーパー ユーザーとしてデータベースに接続する必要があります。スーパーユーザーは、デフォルトで正しい権限を持っています。監視用データベースを構成する際には、スーパー ユーザーを指定することが推奨されます。

スーパー ユーザーを作成するには、PostgreSQL 管理者がスーパーユーザーであり、次の例のようにアカウントを作成する必要があります。

CREATE ROLE xxxxx WITH login superuser password yyyyyy ;

ここで、xxxxx は新しいユーザー名、yyyyyy は新しいユーザーのパスワードです。

データベースにスーパー ユーザーとして接続しない限り、次のパラメーターはデータベース サーバ パラメーター テーブルに入力されません。

- config_file
- DATA_DIRECTORY
- dynamic_library_path
- external_pid_file
- hba_file
- ident_file
- krb_server_keyfile
- log_directory
- log_filename
- preload_libraries
- unix_socket_directory

スーパー ユーザーとして接続しない限り、次のアイテムも使用できません。

- データファイル構成テーブル内で、データファイルへのフル パスを data_directory パラメーターで検出できるファイルのパスとして表示できない。代わりに(postgres data directory)という文字列が表示される。
- 接続ステータス テーブル内で、f_command フィールドと f_status フィールドに正しい情報が入力されない。これらのフィールドは<insufficient privileges>に設定される。

スーパーユーザーとしてデータベースに接続すると、すべてのフィールドに値が入力されます。

SAP HANA の監視

SAP HANA データベースは、SAP HANA データベースと同じホストで実行されているエージェントから監視することも、別のホストで実行されている DPA サーバーなどのエージェントから監視することもできます。DPA エージェントは、Windows または Linux 上で実行する必要があります。

SAP HANA の監視用に［Discovery Wizard］を開始する前に

DPA エージェントが SAP HANA データベースからデータを収集するには、SAP HANA のクライアント.jar ファイルを DPA プラグインのディレクトリにコピーする必要があります。

手順

1. 「の下に<DPA_install_dir>\agent\plugins」という名前のディレクトリを作成します。
2. SAP HANA のクライアント jar ファイル「ngdbc.jar」を「の下の..\EMC\dpa\agent\plugins」フォルダーにコピーします。

   カスタムの場所やパスを使用する場合は、タグ <PLUGINSDIR>path </PLUGINSDIR> in dpaagent_config.xml を追加します。これは、<DPA_install_dir>\agent\etc の下にあります。

   ここで、path はステップ 1 で作成したディレクトリのパスです。

例：<PLUGINSDIR>c:\program files\emc\dpa\agent\plugins</PLUGINSDIR>

3. DPA が 14 日前からのジョブ データを収集するようにする場合、TSM のデータをただちにレポートに表示するには、ジョブ監視リクエストのデフォルトの履歴データを有効にします。DPA Web コンソールで、［**Inventory**］ > ［**Object Library**］ > ［ オブジェクトの選択］> ［**Data Collection**］の順に選択します。

SAP HANA のデータ検出のための権限

SAP HANA でデータを収集するには、データベース ユーザーは SELECT クエリーを実行するための権限を有する必要があります。

DPA エージェントは資格情報を使用して以下のテーブルにアクセスします。

- M_BACKUP_CATALOG ビュー
- M_BACKUP_CATALOG_FILES ビュー

通常、データを読み取るには、PUBLIC ロールに付与された権限で十分です。詳細については、SELECT クエリーを実行するために必要な権限について記載されたベンダー情報を参照してください。

クラウド ベースのソリューションを使用したアプリケーションの監視

このセクションでは、クラウド ベースのソリューションに展開されている DPA を使用してアプリケーションを監視する方法について説明します。

Amazon Web Services 上でのアプリケーションの監視

DPA は、オンプレミスや Amazon Web Services 内でサポートされるバックアップ アプリケーションや監視アプリケーションの検出と監視のため、Amazon Web Services やオンプレミスへの DPA の導入をサポートします。サポートされるバックアップ アプリケーションや監視アプリケーションの詳細については、「Data Protection Advisor Software Compatibility Guide」を参照してください。

はじめに

- Amazon Web Services を使用することで、監視を計画しているオブジェクトと同じ Amazon Web Services スペース内に、DPA データ コレクション エージェントを設定するようにします。
- VPN を使用してクラウド ベースのソリューション上に展開されたアプリケーションを監視するために DPA を設定する場合、VPN 全体でポートとプロトコルが提供されるようにしてください。非標準のポートを使用する場合、クラウド サービス プロバイダーまたは Amazon Web Services と連携しながら、非標準ポートをオープンします。DPA ポート設定は、標準 DPA ポートに関する情報を提供します。

手順

1. Amazon Web Services 環境に DPA を展開します。
   DPA のインストールについては、DPA のインストール（29 ページ）を参照してください。具体的な製品要件については、Amazon Web Services ドキュメントを参照してください。
2. Amazon Web Services 内の DPA インスタンスでサポートされているアプリケーションを検出します。
   情報については、この章の各セクションを参照してください。たとえば、NetWorker の検出と監視については、NetWorker の監視（162 ページ）を参照してください。

Microsoft Azure 上のアプリケーションの監視

DPA は、サポートされるバックアップ アプリケーションやモニタリング アプリケーションの検出と監視のため、Azure 内での DPA の導入をサポートします。サポートされるバックアップ アプリケーションや監視

アプリケーションの詳細については、「Data Protection Advisor Software Compatibility Guide」を参照してください。

手順

1. Azure 環境に DPA を展開します。

   DPA のインストールについては、DPA のインストール（29 ページ）を参照してください。具体的な製品要件については、Azure ドキュメントを参照してください。

2. Azure 内の DPA インスタンスでサポートされているアプリケーションを検出します。

   情報については、この章の各セクションを参照してください。たとえば、NetWorker の検出と監視については、NetWorker の監視（162 ページ）を参照してください。

ホスト監視

このセクションでは、ホスト監視について説明します。

DPA は、ホストの検出時に次の 2 つのオプションを提供します。

- ホスト システムの監視、オペレーティング システムの構成、パフォーマンス、ステータスの監視。
- レプリケーションの監視、ストレージのレプリケーション分析の実行。

オペレーティング システムの監視

オペレーティング システムの構成、パフォーマンス、ステータスを監視するには、Discovery Wizard Host System を使用します。次の表で説明されているように、さまざまなタイプの情報を収集する複数の DPA モジュールがあります。

表 36 システム監視モジュール

Module	説明
ホスト	オペレーティング システムのタイプに関する基本的な情報を収集します。
Disk	ホストに接続されたディスクの構成、状態、パフォーマンスに関する情報を収集します。
ファイバ・チャネル HBA	コンピュータ上で構成されているファイバ チャネル HBA の構成、状態、パフォーマンスに関する情報を収集します。
File system	ホストにマウントされたファイル システムの構成、状態、パフォーマンスに関する情報を収集します。
メモリー	ホストのメモリーの構成、状態、パフォーマンスに関する情報を収集します。
NetIntNetInt	ホストのネットワーク インタフェース カードの構成、状態、パフォーマンスに関する情報を収集します。
プロセス	ホストで実行されているすべてのプロセスに関する情報を収集します。
プロセッサ	ホスト上のすべての CPU の構成、状態、パフォーマンスに関する情報を収集します。

UNIX オペレーティング システムからのデータ収集

UNIX コンピュータでシステム監視を行う場合、監視対象のホスト上にエージェントをインストールします。ただし UNIX コンピュータからリモートでシステム情報を集めることはできません。

データ収集のための UNIX 用エージェント ホストの検出

UNIX ホストは、root アクセス権を持つ SSH または telnet/ftp を使用して検出されます。

セキュリティの要件により、root 認証情報を DPA に提供することが許可されていない場合、sudo は、sudoers ファイルに構成されている特定のコマンドを使用できるよう、一時的にユーザーの認証情報を root に昇格させることができる回避方法になります。

DPA ストレージ検出のための sudoers ファイルの変更
UNIX ホストに root 以外のユーザーとしてログインし、sudo を使用して SCSI コマンドを正常に実行できるため、ホストのストレージ関連情報を検出できます。次の例は、sudoers ファイルに追加する必要のある内容です

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a
sudoers file.
#
# Host alias specification
# User alias specification
# Cmnd alias specification
# Defaults specification
# User privilege specification
root    ALL=(ALL) ALL
# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL
# Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
user_alias ALL = (ALL) PASSWD: /var/tmp/IllumAgent/apolloreagent
# Defaults specification
# User privilege specification
root ALL=(ALL) ALL
CMGU ALL=NOPASSWD:CMGEMC
# Uncomment to allow people in group wheel to run all commands
# %wheel ALL=(ALL) ALL
# Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
# Samples
# %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users localhost=/sbin/shutdown -h now
```

#cmguser ALL=(ALL) NOPASSWD: ALL

Windows オペレーティング システムからのデータ収集

Windows ホストからパフォーマンス データを収集するには、監視している Windows ホスト上に WMI（Windows Management Infrastructure）をインストールする必要があります。

ファイバ チャネル HBA 情報を除き、すべてのシステム監視情報を Windows コンピュータからリモート収集できます。ファイバ チャネル HBA 情報を収集するには、コンピュータにエージェントがインストールされている必要があります。Windows ホストのリモート監視（188 ページ） に、リモートで Windows ホストを監視するために必要なステップの詳細が記載されています。

エージェントがインストールされているシステム用にシステム監視を設定するには、システム監視リクエストを監視対象のホストまたはグループに割り当てます。

データ収集のための Windows 用エージェント ホストの検出

エージェントを使用せずにアプリケーション検出が行われている場合、Windows ホスト検出では、Replication Analysis and WMI for System Information の RPC（リモート プロシージャ コール）を使用します。

RPC 通信の確認

手順

1. Windows の［スタート］メニュー から［ファイル名を指定して実行］ダイアログ ボックスを開きます。
2. 次のように入力します。

   ```
   net use \\<servername>\admin$ /user:<username>
   ```

3. ［**Enter**］をクリックします。パスワードを入力します。
4. 接続に成功すると、次のメッセージが返されます。`The command completed successfully`。
5. ネットワーク マップを削除します。次のように入力します。

   ```
   net use \\servername\admin$ /delete
   ```

WMI 通信の確認

手順

1. Windows の［スタート］メニュー から［ファイル名を指定して実行］ダイアログ ボックスを開きます。
2. 「WBEMtest」と入力し、［Windows Management Instrumentation テスト］ダイアログ ボックスの［接続］をクリックします。
3. ［接続］フィールドに**\\<servername\root\cimv2** と入力します。
4. ［資格証明］フィールドに、監視しているアプリケーション ホストへの接続に使用するユーザー名とパスワードを入力します。
5. ［接続］をクリックして、［Windows Management Instrumentation テスト］ダイアログ ボックスに戻ります。［**Query**］をクリックします。
6. ［**Enter Query**］フィールドに、次のように入力します。

   ```
   select * from win32_processor
   ```

7. ［**Apply**］をクリックします。

   WMI が接続されると、アプリケーション ホストからのデータが表示されます。

Windows ホストのリモート監視

ファイバ チャネル HBA 情報を除き、すべてのシステム情報を Windows コンピューターからリモート収集できます。Windows コンピューターをリモート監視するには、エージェントを別の Windows コンピューターにインストールする必要があります。UNIX コンピューター上で実行されているエージェントから Windows コンピューターをリモート監視することはできません。

別の Windows コンピューターから Windows ホストを監視するには、監視を行うコンピューター上で、DPA エージェント サービスを管理者として実行する必要があります。エージェント サービスのログイン パラメーターの変更（188 ページ）に詳細が記載されています。

エージェント サービスのログイン パラメーターの変更

これが必要かどうかを確認します。エージェント サービスのログイン パラメーターを変更するには：

手順

1. Windows サービス コントロール マネージャーを起動します （[スタート] > [設定] > [コントロール パネル] > [管理ツール] > [サービス]）。
2. DPA［Agent service］を選択します。
3. 右クリックし、メニューから［ **Properties**］を選択します。
4. ［プロパティ］ダイアログ ボックスの［ログオン］タブを選択します。
5. ［**This Account**］を選択します。
6. サービスを実行する際の管理者のユーザー名とパスワードを入力します。
7. ［**OK**］をクリックし、サービスを再起動します。

リモート コンピュータでのアクティビティの監視

手順

1. 監視するコンピュータのホスト オブジェクトを Web コンソールで作成します。オブジェクトの名前はリモート ホストのホスト名です。ホスト名は、オブジェクトを監視するエージェントが実行されているコンピュータから名前解決できなければなりません。
2. そのオブジェクトにリクエストを割り当てて、収集するデータを指定します。
3. 各リクエストをプロキシ リクエストとしてマークし、詳細を入力します。
4. プロキシの詳細を入力するには、［**Proxy Host**］フィールドにエージェントのホストの名前を入力します。
5. 監視するコンピュータで管理者アカウントの Windows 認証情報を作成します。このアカウントは、ローカル管理者の名前か、ドメイン管理者の名前にできます。
6. エージェントを再ロードすることにより、サーバを監視するエージェントに、変更を通知します。

ホストのシステム データの監視

ホスト、または環境の別のホストで実行されているエージェントからアプリケーション ホストのシステム データを監視します。

システム データのホストの監視用に［Discovery Wizard］を開始する前に
システム データは、UNIX ホストにローカルなエージェントにより UNIX システムからだけ収集できます。

レプリケーション解析の構成
ストレージ レプリケーション解析の実行には、［Discovery Wizard］を使用します。

はじめに

- ProtectPoint のバックアップやリカバリを構成するため、アプリケーション検出が可能なこと、または Replication Monitoring フラグが設定済みであることを確認します。
- ProtectPoint のバックアップと構成のため、ProtectPoint で保護するホストの時間と、アプリケーションがマップされたストレージ アレイを管理する Solutions Enabler ホストの時間が同期している（差は 1 分以内）ことを確認します。
- 監視対象ホストと復旧可能性プロセスの間の通信が有効になっていることを確認します。
  - Windows サーバーをリモートで監視するには、RPC サービスが有効であり、復旧可能性エージェントにアクセスできる必要があります。
  - UNIX や Linux のアプリケーションをリモートで監視するには、SSHD を有効にし、復旧可能性エージェントに確実にアクセスできるようにする必要があります。
  - UNIX や Linux のアプリケーションをリモートで監視するには、FTP/Telnet サービスを有効にし、復旧可能性エージェントに確実にアクセスできるようにする必要があります。

Microsoft Exchange Server の監視

Microsoft Exchange Server を検出するには、Microsoft Exchange Server が稼働しているホストを検出する必要があります。Exchange Server は、Exchange Server と同じホストにインストールされているエージェントから、またはリモートでインストールされているエージェントから復旧可能性を監視できます。

注

Microsoft Exchange では、レプリケーション分析、および Exchange サーバ ホストからのシステム情報のみの監視が可能です。

Microsoft Exchange Server の監視用に［Discovery Wizard］を開始する前に

DPA を Exchange Server に接続するときに使用されるアカウントは、Exchange の読み取り専用管理者権限およびローカル管理者権限を持つドメイン ユーザーでなければなりません。DPA は、1 個のクラスタでの 2 個の Exchange 情報ストアのレプリケーション分析をサポートしていません。を Exchange アプリケーションに接続するには、Exchange 読み取り専用管理者権限が必要です。Windows からディスク情報を取得するには、ローカル管理者権限を保有するオペレーティング システム ユーザーである必要があります。

レプリケーション解析用の Oracle の監視

Oracle データベースでレプリケーション分析を監視するには、エージェントは、次のテーブルおよびビューで選択を実行できる Oracle ユーザーとしてデータベースに接続する必要があります。

- DBA_DATA_FILES
- DBA_TEMP_FILES
- DBA_TABLESPACES
- V_$DATAFILE
- V_$LOGFILE
- V_$CONTROLFILE
- V_$LOG_HISTORY
- V_$ARCHIVED_LOG
- V_$INSTANCE
- V_$DATABASE
- V_$PARAMETER
- DICT
- DBA_TAB_COLUMNS

Windows プラットフォーム上の Oracle を監視する場合は、認証情報で指定されたオペレーティング システム ユーザーは ORA_DBA グループに属している必要があります。UNIX では、UNIX 認証を使用する場合に、データベースで認証情報を指定する必要はありません。

Oracle 統計の更新

行数およびテーブルとインデックスのサイズに関する正確な数値を収集するには、定期的に Oracle 統計を更新することが重要です。Oracle マニュアルでは、Oracle 統計を更新するようにジョブを設定する方法の詳細が説明されています。

スキーマに関する Oracle 統計を更新する方法の 1 つとして、次のコマンドを実行することがあります。

```
exec dbms_stats.gather_schema_stats(ownname => '***SCHEMANAME***',
estimate_percent => 5, cascade => true, options => 'GATHER');
```

RecoverPoint の監視

RecoverPoint は、リモートでインストールされた DPA サーバーなどのエージェントから監視する必要があります。

RecoverPoint を検出する場合、DPA は 1 つの管理 IP の検出のみをサポートします。さらに、DPA は管理 IP の監視のみをサポートしており、RPA IP の監視はサポートしていません。RPA IP を監視せず、必ず管理 IP を監視してください。

プライマリ ストレージの監視

このセクションでは、プライマリ ストレージを監視する方法について説明します。

DPA ではプライマリ ストレージを次のカテゴリーに分類します。

- ファイル サーバー
- レプリケーション解析用のストレージ アレイ
- ディスク管理サーバー

ファイル サーバーの監視

このセクションでは、ファイル サーバーを監視する方法について説明します。

EMC File Storage の監視

EMC File Storage は、たとえば、DPA サーバーなど、リモート コンピューターで実行されているエージェントから監視する必要があります。

注

EMC File Storage は、Celerra File Storage とも呼ばれます。

レプリケーション解析用のストレージ アレイの構成

DPA は、VNX Block、CLARiX、Symmetrix、および VPLEX の各ストレージ アレイを監視します。これらのストレージ アレイが EMC RecoverPoint によってレプリケートされている場合は、完全なレプリケーション分析を有効にするために追加の構成が必要です。

EMC VPLEX アレイのポート

DPA は、TCP ポート 443 で VPLEX と接続します。

VPLEX アレイの検出

VPLEX ストレージ アレイを DPA サーバーから監視するか、DPA エージェントがインストールされている任意のホストからリモートで監視することができます。

DPA は、管理されているすべてのストレージ アレイを検出し、オブジェクト ライブラリ インベントリでオブジェクトを作成します。

VNX Block/CLARiX アレイのポート

DPA は、TCP ポート 443 で VNX Block/CLARiX に接続します。ただし、VNX Block/CLARiX がポート 2163 を使用するように設定されている場合は、ポート 2163 を使用します。

VNXBlock/CLARiX アレイの検出

EMC VNXBlock/CLARiX ストレージ アレイは、プロキシ サーバーからリモートで、または最後の手段としては DPA サーバーなどの異なるホスト上で実行するエージェントから、監視する必要があります。これは SE ホストまたはコネクタとも呼ばれます。

SE ホストは、SE ホストにインストールされた DPA エージェントによる検出や、特権ユーザーの資格情報が必要なエージェントなしのメカニズムによる検出に使用できます。

DPA は、管理されているすべてのストレージ アレイを検出し、オブジェクト ライブラリ インベントリでオブジェクトを作成します。

EMC Solutions Enabler がインストールされているホストの名前を指定する必要があります。

Symmetrix アレイの検出

Symmetrix ストレージ アレイは、別のホスト（DPA サーバーなど）で実行されているエージェントからリモート監視する必要があります。

複数のホストと複数のストレージ アレイを構成するには、[Discovery Wizard]を使用します。DPA は、管理されているすべてのストレージ アレイを検出し、オブジェクト ライブラリ インベントリにオブジェクトを作成します。

Solutions Enabler がインストールされているホストの名前を指定する必要があります。

Solutions Enabler がデフォルトで Solutions Enabler のローカルに保存されるデバイス グループを表示するには、次の要領で、Solutions Enabler のオプション ファイルの `Global Name Services` を開く必要があります。

1. `/./emc/API/symapi/config/`でオプション ファイルを開きます。
2. 該当する行を見つけます。

   ```
   #SYMAPI_USE_GNS = ENABLE
   ```

   ここでコメント処理を外すと、次のようになります。**`SYMAPI_USE_GNS = ENABLE`**
3. ファイルを保存します。
4. `stordaemon list` コマンドを実行し、GNS サービスが実行中であることを確認します。
5. `symcfg disco` コマンドを実行します。

Symmetrix および VNX/CLARiX でのホストを介さない検出の実行

レプリケーション監視でホスト検出を行うには、ホストにローカル エージェントをインストールするか、ホスト アクセス用の認証情報を含むリモート エージェントを導入する必要があります。いずれの方法もお客様のセキュリティ ポリシーによって妨げられることがあります。

エージェントレス オプションを使用するには、Solutions Enabler ホストの認証情報を提供する必要があります。ホストを介さない検出の前提条件は、Symmetrix アレイの検出（192 ページ）で説明した条件と同じです。

レプリケーション データを収集するための、RecoverPoint を使用するストレージ アレイの構成

ご使用の VNX/CLARiX または Symmetrix ストレージ アレイが EMC RecoverPoint でレプリケートされている場合は、DPA により RecoverPoint レプリケーション処理のレプリケーション分析が提供されます。

RecoverPoint のレプリケーション分析を実行するには、VNX/CLARiX または Symmetrix ストレージ アレイのいずれかと、RecoverPoint ホストを正しい順序で DPA に構成する必要があります。

手順

1. ［Discovery Wizard］を使用して、RecoverPoint でレプリケートしたストレージ アレイに接続している Solutions Enabler ホスト用のホスト オブジェクトを作成します。
2. ホストと接続しているアレイを検出します。
3. ［Discovery Wizard］を使用して Symmetrix または VNX/CLARiX アレイを構成します。
4. ストレージ アレイからレプリケーション ポリシー データをインポートします。
5. RecoverPoint の監視（191 ページ）の説明に従って、EMC RecoverPoint アプライアンスのデータ監視を構成します。

6. RecoverPoint Configuration リクエストが、ストレージ アレイのレプリケーションを処理する RecoverPoint アプライアンス オブジェクトに割り当てられていることを確認します。このリクエストを実行します。
7. RecoverPoint Configuration リクエストが実行され、十分な時間が経過すると、DPA は RecoverPoint のレプリケーション分析データを収集し始めます。レポートはストレージ アレイ オブジェクトから実行できます。［**Replication Analysis**］領域には、ストレージおよびリカバリ ポイントのマッピングが表示されます。

EMC File Storage の監視用に［Discovery Wizard］を開始する前に

EMC File Storage モジュールは、XML API を介して EMC File Storage から情報を収集し、EMC File Storage Control Station から直接に情報を収集します。EMC File Storage に対する特定の権限を持つ管理者を作成する必要があります。

手順

1. EMC File Storage Manager Web ブラウザー インターフェイスに管理者としてログインします。

   コマンド ライン インターフェイスを使用して DPA 管理者を作成することもできます。
2. ［**Security**］ > ［**Administrators**］に移動します。
3. ユーザー名を DPA などにして、新しい管理者を作成します。
4. ［**Local Only Account**］を選択して、管理者のパスワードを入力し確認します。
5. 少なくとも opadmin レベルの権限を持つ［**Primary Group**］を選択します。DPA では、opadmin で割り当てられる以上の権限は必要ではありません。
6. 次のクライアント アクセス オプションを有効にします。
   - ［XML API v2 allowed］
   - ［Control Station shell allowed］
7. ［**OK**］をクリックします。

結果

EMC File Storage との接続に使用する DPA 認証情報には、作成した EMC File Storage 管理者のユーザー名およびパスワードが含まれている必要があります。

ディスク マネージメント サーバーの監視

このセクションでは、ディスク マネージメント サーバーを監視する方法について説明します。

HP Command View の監視

HP EVA ディスク アレイを、Command View ホストで実行されているエージェントから HP Command View を介して、または別のホスト（DPA サーバーなど）で実行されているエージェントからリモート監視します。

データ収集に使用するユーザー名とパスワードは、CommandView CIM サーバーで定義されている有効なユーザー名とパスワードに一致していなければなりません。これは CommandView 管理インターフェイスから構成できます。

DPA は、デフォルトのセキュア ポートである 5989 で SMI-S を使用して、HP Command View からデータを収集します。

保護ストレージの監視

このセクションでは、データ保護ストレージの監視方法について説明します。

Data Domain の監視

DPA は、Data Domain バックアップ アプライアンスを監視します。DDOS 4.8 では、テープ ドライブとテープ ライブラリのステータスおよび構成情報のみが返されます。データを収集する Data Domain システムで、Data Domain 分析リクエストを有効にする必要があります。

Data Domain の監視用に［Discovery Wizard］を開始する前に

Data Domain バックアップ アプライアンスでは、ポート 161 上の SNMP およびポート 22 上の SSH を有効化する必要があります。また、SNMP コミュニティ文字列も設定する必要があります。これは、コマンド ラインから実行できます。

はじめに

- Data Domain システムで SSH リクエストを実行するためのユーザー役割権限があることを確認します。
- Data Domain OS 5.7 以降を監視するには、ユーザーに PCR（物理容量レポート作成）を実行する管理者権限があることを確認します。

手順

1. sysadmin アカウントを使用して、Data Domain アプライアンス コンソールにログインします。
2. 次のコマンドを入力して、既存の構成を確認します。

   snmp show ro-communities

   snmp add ro-community <string> hosts <host IP address>
   <string>は選択されているコミュニティ文字列（public など）、<host IP address>は Data Domain の監視に使用している DPA エージェントの IP アドレスです。SNMP をいったん無効にし、再度有効にして新しい文字列が有効になるようにします。

   ```
   snmp disable
   snmp enable
   ```

   public というコミュニティ文字列を使用していない場合は、Data Domain 認証情報で使用されているコミュニティ文字列を変更する必要があります。

   SNMP 設定は、Data Domain Enterprise Manager インターフェイスの［**System Settings**］タブでも設定できます。

3. DPA Data Domain の SSH 認証情報を編集して、Data Domain デバイス上で構成される SSH のユーザー名とパスワードを指定します。DPA Web コンソールで、［**Admin** ］ > ［ **System** ］ > ［ **Manage Credentials**］の順に選択します。

   この情報は必須で、

   - Data Domain OS 5.7 以降の監視にあたり、SSH PCR データ コレクションの構成の確認に使用します。
     - リクエストが実行されると、コマンドのポーリング期間に統計情報を収集し、Data Domain の物理容量の測定スケジュールを作成します。それから Data Domain が統計情報を収集します。収集された統計情報は、以後のリクエストを実行する際に DPA サーバーに送信されます。このため、初めてリクエストが実行されるときは、レポ

ートに収集されるデータはありません。データが収集され、レポートに取り込まれるのは 2 度目の実行時からとなります。DPA インストール後の作業（61 ページ）で詳細を参照してください。

- コマンドのポーリング期間は丸 1 日単位に切り上げられます。コマンドのポーリング期間の値は、コマンドのポーリング期間が 2 日間以上となるように、プロビジョニングでポーリング期間の 2 倍に設定されます。たとえば、ポーリング期間が 24 時間以内に設定されている場合、DPA は 2 日間の統計情報を収集します。ポーリング期間が 3 日間に設定されている場合、DPA は、6 日間の統計情報を収集します。

- これにより、Data Domain からデバイス、デバイス グループ、プール、静的イメージ、ProtectPoint SnapVX Backup and Recovery のアクセス グループの LUN 情報を取得します。ProtectPoint SnapVX のバックアップ/リカバリを実行する DPA の構成（195 ページ）で情報を確認します。

以上は他の情報より優先して確認します。

ProtectPoint SnapVX のバックアップ/リカバリを実行する DPA の構成

DPA 環境のホストに収集された情報を DPA 環境の VMAX3 に収集された情報を関連づけるには、DPA を構成して、代わりにその情報を DPA 環境の Data Domain に収集された情報に関連づける必要があります。

はじめに

- ProtectPoint で保護するホストの時間と、アプリケーションがマップされたストレージ アレイを管理する Solutions Enabler ホストの時間が同期している（差は 1 分以内）ことを確認します。
- サポートされるバージョンと OS の要件については、「Data Protection Advisor Software Compatibility Guide」を参照してください。
  - ProtectPoint
  - Solutions Enabler
  - VMAX3
  - Data Domain

手順

1. レプリケーション解析用のホストを構成します。

   詳細については、を参照してください。アプリケーションを検出できること、または Replication Monitoring フラグが設定されていることを確認します。これは、ProtectPoint のバックアップ/リカバリの構成に必要です。

2. VMAX3 と SE ホストを検出します。

   詳細については、Symmetrix アレイの検出（192 ページ）を参照してください。

3. Data Domain ホストを検出します。

   詳細については、Data Domain の監視（194 ページ）を参照してください。Data Domain の検出ウィザードで SSH 認証情報が指定されていることを確認します。これは、Data Domain からデバイス、デバイス グループ、プール、静的イメージ、アクセス グループなどの LUN の情報を取得するために必要です。

必要条件

必要な場合は、保護ポリシーに新しい保護ルールを追加して、Linked、StaticImage、SnapVX Missing Recovery Point のアラートが生成されるようにします。

StorageTek ACSLS Manager の監視

StorageTek ACSLS Manager はリモート監視できません。ACSLS AIX または ACSLS Solaris ホストに DPA エージェントをインストールする必要があります。

StorageTek ACSLS Manager の監視用に［Discovery Wizard］を開始する前に

エージェントが監視対象の StorageTek ACSLS Manager サーバーにインストールされ、実行中になっている必要があります。

エージェントをインストールしたら、DPA.config ファイルの ACS_HOME の値が、ACSLS のインストール場所に一致することを確認します。DPA.config ファイル内の ACSDBDIR の値が、ACSLS DB フォルダへのパスと一致することを確認します（デフォルトは export/home/ACSDB 1.0）。

テープ ライブラリの監視

DPA はテープ ライブラリに関する情報、およびそのテーブル ライブラリ内のドライブに関する情報を収集できます。ホスト名を指定する際には、テープ ライブラリを監視しているホストで解決できるテープ ライブラリ名を指定します。

テープ ライブラリの監視用に［Discovery Wizard］を開始する前に

テープ ライブラリの認証情報には、［**Credential Properties**］ダイアログ ボックスの［**Password**］フィールドに含まれるテープ ライブラリの読み取り専用コミュニティ文字列が含まれていなければなりません。テープ ライブラリでコミュニティ文字列を変更していない場合は、コミュニティ文字列を［**public**］に設定します。

［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択して、［Discovery Wizard］を使用してテープ ライブラリ オブジェクトを作成した後に作成されるテープ ライブラリの認証情報を変更します。

IBM System Storage TS 3500 テープ ライブラリの監視

Tape Library Specialist Web インタフェースを使用して、IBM System Storage TS 3500 テープ ライブラリの SNMP（Simple Network Management Protocol）を有効にします。SNMP リクエストを有効にするには：

手順

1. ブラウザの URL 行に Ethernet IP アドレスを入力します。
2. ［**Manage Access**］ > ［**SNMP Settings**］の順に選択します。［**SNMP Trap Setting**］フィールドで現在の設定を表示し、クリックして SNMP リクエストを有効にします。
3. ［**SNMP Requests Setting**］フィールドが［**Enabled**］に設定されていることを確認します。

IBM TotalStorage 3583 テープ ライブラリの監視

IBM TotalStorage 3583 テープ ライブラリの SNMP を有効にするように URM（Remote Management Unit）を構成します。SNMP を有効にするには：

手順

1. RMU で［**Configuration**］をクリックします。
2. ［SNMP Configuration］領域で次の手順を実行します。
   - この機能を有効にするには、［**SNMP Enabled**］フィールドで［**ON**］を選択します。

- SNMP アラートを有効または無効にするには、［**Alerts Enabled**］フィールドで［**ON**］または［**OFF**］を選択します。
- ［**Manager**］フィールドに SNMP サーバー アドレスを入力します。
- ［**Public Name**］フィールドに読み取り専用 SNMP コミュニティの名前を入力します。
- ［**Private Name**］フィールドに読み取り/書き込み SNMP コミュニティの名前を入力します。

3. ［**Submit**］をクリックし、変更を確認します。
4. パスワードを入力し、［**Confirm**］をクリックします。必要な場合、ブラウザをリダイレクトします。
5. ［**Done**］をクリックし、再起動します。

IBM TotalStorage 3584 テープ ライブラリの監視

IBM TotalStorage 3584 テープ ライブラリの Web インタフェースから SNMP を有効にするには、次の手順を実行します。

手順

1. Tape Library Specialist Web インターフェイスの［Welcome］スクリーンで、［**Manage Access**］ > ［**SMNP Settings**］の順に選択します。
2. ［**SNMP Trap Setting**］フィールドで、現在の設定を確認し、SNMP リクエストを有効または無効にするボタンを選択します。
1. 別な方法を使用してオペレータ パネルから SNMP リクエストを有効にするには：
3. テープ ライブラリ オペレーター パネルの［Activity］スクリーンで、［**MENU**］>［**Settings**］>［**Network**］>［**SNMP**］>［**Enable/Disable SNMP Requests**］ > ［**ENTER**］の順に選択します。

   SNMP リクエストの現在のステータスが画面に表示されます。
4. ［**UP**］または［**DOWN**］を押して SNMP メッセージングを［ENABLED］または［DISABLED］に指定し、［**ENTER**］を押します。

   新しい設定を受け入れて前の画面に戻るには、［**BACK**］を押します。

   再度表示された［Enable/Disable SNMP Requests］画面に新しい設定が表示されます。

Oracle SL24 Tape Autoloader および SL48 テープ ライブラリの監視

RMI（Remote Management Interface）を構成し、Oracle StorageTek SL24 Tape Autoloader または SL48 テープ ライブラリの SNMP を有効にします。SNMP を有効にするには：

手順

1. RMI で、［**Configuration**］ > ［**Network**］に移動します。
2. ［**SNMP Enabled**］チェックボックスが有効になっていることを確認します。
3. ［**Community Name**］文字列は、DPA のこのテープ ライブラリの接続に使用される認証情報に含まれている必要があります。
4. ［**Submit**］をクリックし、変更を確認します。

HP StorageWorks テープ ライブラリの監視

NeoCenter ユーティリティを構成して、テープ ライブラリの SNMP を有効にします。SNMP を有効にするには：

手順

1. NeoCenter ユーティリティをホストから起動します。
2. ［Main］スクリーン メニューから［**Configure**］を選択します。［**Configure**］ダイアログ ボックスが表示されます。
3. ［**SNMP Traps**］タブを選択します。
4. 使用できるいずれかの［**Trap Address**］フィールドで、DPA サーバーの IP アドレスを入力します。

スイッチおよび I/O デバイスの監視

このセクションでは、スイッチおよび I/O デバイスの監視方法を説明します。

ファイバー チャネル スイッチの監視

DPA は、ファイバ チャネル スイッチ上のポートの構成、接続性ステータス、スループットなどに関する情報を収集します。

ホスト名を指定する際には、エージェントのホストで解決できるスイッチ名を指定します。

ファイバー チャネル スイッチの監視用に［Discovery Wizard］を開始する前に

Brocade スイッチが確実にすべてのデータを返すようにするには、Fibre Channel Alliance MIB がロードされ、スイッチで有効になっていることを確認します。この MIB は、デフォルトではスイッチにインストールされません。FA-MIB サポートを Brocade スイッチで有効にするには、管理者としてログインして、snmpmibcapset コマンドを実行します。FA-MIB パラメータを［Yes］に変更します。［Enter］をクリックしてその他の設定のデフォルト値を受け入れます。

次に例を挙げます。

```
telnet <switch>
> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
 FE-MIB SW-MIB FA-MIB SW-TRAP FA-TRAP
 FA-MIB (yes, y, no, n): [yes]
 SW-TRAP (yes, y, no, n): [enter]
 FA-TRAP (yes, y, no, n): [enter]
 SW-EXTTRAP (yes, y, no, n): [enter]
>
```

IP スイッチの監視

ホスト名を指定する場合は、エージェントのホストで解決できるスイッチ名を指定します。

IP スイッチの監視用に［Discovery Wizard］を開始する前に

IP スイッチの認証情報には、［**Credential Properties**］ダイアログ ボックスの［**Password**］フィールドに含まれる IP スイッチの SNMP コミュニティ文字列が含まれていなければなりません。IP スイッチでコミュニティ文字列を変更していない場合は、コミュニティ文字列を public に設定します。

［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択して、［Discovery Wizard］を使用して IP スイッチ オブジェクトを作成した後に作成される IP Switch Credentials を変更します。

Xsigo I/O Director の監視

Xsigo I/O Director のホスト名を指定する場合は、エージェントのホストで解決できる Director のホスト名または IP アドレスを指定します。

Xsigo I/O Director の監視用に［Discovery Wizard］を開始する前に

Xsigo Director SNMP の認証情報では、認証情報の［**Password**］フィールドに Director の SNMP コミュニティ文字列が含まれていなければなりません。Director でコミュニティ文字列を変更していない場合は、コミュニティ文字列を public に設定します。

［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択し、必要に応じてデフォルトの Xsigo Director SNMP 認証情報を変更するか、新しい認証情報を作成します。

仮想化管理

このセクションでは、仮想化環境を監視する方法について説明します。

VMware 環境の監視

VMware 環境を、VirtualCenter Server で実行されているエージェントから監視するか、DPA サーバーなどの別のホストで実行されているエージェントからリモート監視します。

- ［Discovery Wizard］を使用して、vCenter Server を DPA に追加できます。［**Admin**］ > ［**System**］ > ［**Discovery Wizard**］ > ［**Virtualization Management**］の順に選択します。
- vCenter Server を追加するには、vCenter ホスト名および vCenter ユーザーの認証情報を入力する必要があります。
- vCenter ホストのみを監視するか、vCenter ホストに接続されている仮想マシンも監視するかを選択できます。
  - 仮想マシンの監視を選択すると、DPA から vCenter Server に対してクエリーが実行され、仮想マシンのリストが表示されます。vCenter Server に多数の仮想マシンが構成されている場合は、検出処理に時間がかかる場合があります。
  - 仮想マシンごとに、DPA でホストを検出するかどうかを選択できます。ホストを検出すると、DPA インベントリにホストが追加されます。
  - 検出で選択される仮想マシンごとに、構成、パフォーマンス、および解析データを収集する Host System Monitoring と、レプリケーション解析を有効にする Replication Monitoring を有効にするかどうかを選択できます。
  - Host System Monitoring で選択される仮想マシンごとに、仮想マシンの監視に使用する DPA エージェントを指定できます。Ctrl キーまたは Shift キーを押しながらクリックして複数のシステムを選択することで、複数台のマシンの DPA エージェントを同時に変更できます。
    - Windows 仮想マシンでは、リモート DPA エージェント（DPA サーバーにインストールされている DPA エージェントなど）、またはローカル エージェント（各 Windows 仮想マシンにインストールされている DPA エージェントなど）を使用して、Host System Monitoring を実行させることができます。
    - UNIX/Linux 仮想マシンでは、ローカル エージェント上の Host System Monitoring 用の仮想マシンに DPA エージェントがインストールされている必要があります。
  - 仮想マシンごとのホスト監視を選択する場合は、リモート エージェントで監視中の Windows 仮想マシンごとに、Windows 認証情報を入力する必要があります。認証情報

は、ローカル管理者またはドメイン管理者です。Ctrl キーまたは Shift キーを押しながらクリックして複数のシステムを選択することで、複数台のマシンの認証情報を同時に変更できます。vCenter を監視中の場合は、こうした認証情報の入力は不要です。

- 検出された仮想マシンは、DPA の vCenter オブジェクトの下に表示され、デフォルトで［Configuration］/［Servers］/［Application Servers］グループにも追加されます。表示される仮想マシンのグループは変更、追加できます。
  ［**Admin** ］ > ［ **System** ］ > ［ **Discovery Wizard** ］ > ［ **Destination Group.**］の順に選択します。

- vCenter の［Discovery Wizard］の最後のスクリーンに、選択したオプションのサマリーが表示されます。［**Finish**］をクリックすると、DPA にオブジェクトが追加され、選択されている監視オプションが有効になります。

RecoverPoint for VMs の監視

RecoverPoint for VMs の監視は、リモート インストールされたエージェント（DPA サーバーなど）から行う必要があります。DPA エージェントは、Windows または Linux 上で実行する必要があります。

仮想マシンの RecoverPoint を検出する場合、DPA は 1 つの管理 IP の検出のみをサポートします。さらに、DPA は管理 IP の監視のみをサポートしており、RPA IP の監視はサポートしていません。RPA IP を監視せず、必ず管理 IP を監視してください。

RecoverPoint の監視用に［Discovery Wizard］を開始する前に

DPA は、ポート 22 の安全な SSH 接続を介して RecoverPoint 環境 CLI（コマンド ライン インターフェイス）に接続できる必要があります。DPA は、デフォルトの CLI ユーザー admin を使用して RecoverPoint アプライアンスに接続しますが、SSH を使用して CLI コマンドをリモートで実行する十分な権限を持つ定義された任意のユーザーでも可能です。監視アカウントで十分です。

ただし、ユーザー boxmgmt は RecoverPoint インストール マネージャーを自動的に起動するために予約されているため、DPA は RecoverPoint ユーザー boxmgmt で接続してはいけません。

デフォルト ユーザーが「monitor」となる RecoverPoint 4.1 を実行している場合は、DPA で指定されたデフォルト ユーザーが存在しなくなっているため、新しいユーザーを作成する必要があります。RecoverPoint 4.1 をインストールした後で新しいユーザーを作成しない場合、DPA からの EMC RecoverPoint 認証情報でのリクエストは失敗します。

クラスタの監視

このセクションでは、クラスタを監視する方法について説明します。

Microsoft Server フェールオーバー クラスタの監視

Microsoft Server フェールオーバー クラスタを検出するには、クラスタ内の各マシンにエージェントをインストールする必要があります。サポートされているバージョンについては、「Data Protection Advisor Software Compatibility Guide」を参照してください。

Microsoft Server フェールオーバー クラスタは、DPA Discovery Wizard のリモート エージェントで検出する必要があります。このエージェントは、クラスタのいずれかのマシンにインストールされている必要があります。DPA には、次の 2 つの検出オプションがあります。

- ［**Monitor Cluster and hosts which are included in cluster**］: このオプションを選択すると、DPA はクラスタ構成リクエストとクラスタ ステータス リクエストに関連するクラスタを自動的に選択します。
  DPA は、ホスト監視リクエスト、ホスト構成リクエスト、ホスト ステータス リクエストを、クラスタに属するすべてのホストに割り当てます。

- ［**Monitor only Cluster**］: このオプションを選択すると、DPA はクラスタ構成リクエストとクラスタ ステータス リクエストに関連するクラスタを自動的に選択します。

注

クラスタに属するホストには、リクエストは割り当てられません。

Veritas Cluster Server と Veritas Infoscale Availability の監視

Veritas Cluster Server と Veritas Infoscale Availability を検出するには、クラスタ内の各マシンにエージェントをインストールする必要があります。サポートされているバージョンについては、「Data Protection Advisor Software Compatibility Guide」を参照してください。

Veritas Cluster Server と Veritas Infoscale Availability は、DPA Discovery Wizard のリモート エージェントで検出する必要があります。このエージェントは、クラスタのいずれかのマシンにインストールされている必要があります。DPA には、次の 2 つの検出オプションがあります。

- ［**Monitor Cluster and hosts which are included in cluster**］: このオプションを選択すると、DPA はクラスタ構成リクエストとクラスタ ステータス リクエストに関連するクラスタを自動的に選択します。
  DPA は、ホスト監視リクエスト、ホスト構成リクエスト、ホスト ステータス リクエストを、クラスタに属するすべてのホストに割り当てます。
- ［**Monitor only Cluster**］: このオプションを選択すると、DPA はクラスタ構成リクエストとクラスタ ステータス リクエストに関連するクラスタを自動的に選択します。

注

クラスタに属するホストには、リクエストは割り当てられません。

ホストまたはオブジェクトの手動による検出

この処理手順は、CLARiX、Symmetrix、VNX、VPLEX アレイの検出には適用されません。

注

表示されるステップは、検出するオブジェクトによって異なります。

手順

1. 次のいずれかを実行します。
   - ［**Inventory**］ > ［**Object Search**］に移動します。
   - ［**Admin**］ > ［**Run Discovery Wizard**］に移動します。
2. ［**Objects to Discover**］で、次のいずれかを選択します。
   - ［**Host**］を選択してから［Host］を選択します。
   - ［**Primary Storage**］を選択してから［File Storage］または［VPLEX］を選択します。
   - ［**Protection Storage**］を選択してから、［Data Domain］、［Disk Library］、［NetApp NearStore］、［Tape Library］のいずれかを選択します。
   - ［**Switch**］を選択してから、Fibre Channel スイッチ、IP スイッチ、Xsigo スイッチのいずれかを選択します。
3. ホストまたはオブジェクトを手動で検出するオプションを選択します。

4. ホスト名または IP アドレス、エイリアス、オペレーティング システム、認証情報、リモート データ コレクション エージェント、またはポートで、アプリケーション ホストを識別します。プライマリ ストレージ、保護ストレージ、またはスイッチを検出する場合は、ステップ 8 に進みます。
5. 検出する各ホストに［**Host System Monitoring**］または［**Replication Monitoring**］を選択します。［Replication Monitoring］オプションは、ストレージ容量ライセンスがある場合にのみ使用できます。検出時のオプションを選択しない場合、後で［Add Requests］とそのオプションを実行できます。
6. このアプリケーションのデータを、ローカル データ コレクション エージェントまたはリモート データ コレクション エージェントのどちらが収集するかを選択します。［**Host System Monitoring**］を選択し、ホストで Linux、UNIX、または Windows 以外のプラットフォームを実行している場合は、ローカル データ コレクション エージェントを選択します。リモート データ コレクション エージェントの場合は、エージェントがインストールされているホストを選択します。

   注

   ［**Viewing and editing Data Collection defaults**］領域で RecoverPoint、RecoverPoint for VM、または VPLEX のデータ コレクション エージェントを指定した場合、デフォルトでここにエージェントが表示されます。

   エージェントを追加または編集するには、次の表で説明するフィールドを指定します。

フィールド	説明
Hostname	データ コレクション エージェントがインストールされるホストの名前。
Display Name	データ コレクション エージェントがインストールされるホストの表示名。
Operating System	データ コレクション エージェントがインストールされるホストのオペレーティング システム。
Host System Monitoring	このホストの構成、パフォーマンス、ステータスを監視する場合に選択します。
Replication Monitoring	このホストのレプリケーション解析を実行する場合に選択します。

7. ホスト システム監視とリモートのデータ コレクション エージェントまたはエージェントレスを選択した場合は、アプリケーション ホストの認証情報を選択または設定します。

   注

   ［**Viewing and editing Data Collection defaults**］領域で RecoverPoint、RecoverPoint for VM、または VPLEX の認証情報を指定した場合、デフォルトでここに認証情報が表示されます。

8. （オプション）オブジェクトへの接続をテストします。テストが失敗して、ホストや認証情報のエラーが表示されたら、［**Back**］をクリックし、問題を解決して再テストします。
9. （オプション）オブジェクトを 1 つまたは複数のグループに追加します。複数のオブジェクトを選択するには、［**Ctrl**］または［**Shift**］を押してクリックします。
10. （オプション）カスタム属性が定義されている場合は、検出したオブジェクトに適用する属性を選択します。属性は［**Admin**］ > ［**Manage Custom Attributes**］で作成します。
11. ［**Finish**］をクリックして検出ジョブを開始します。オブジェクトは、オブジェクト ライブラリと選択した宛先グループに追加されます。

検出後のジョブ データ収集について

DPA でアプリケーションを検出した後のジョブ データ収集について説明します。

このセクションの情報は、次のアプリケーションに適用されます。

- NetWorker
- Avamar
- TSM
- HP DataProtector
- Commvault Simpana
- NetBackup
- ArcServ
- DB2
- SAP HANA
- RMAN
- MSSQL

上記のアプリケーションに関して、次のことに注意してください。

- この機能を有効にした場合、新しいサーバーが検出されると、DPA は 14 日前のジョブ データから収集を開始します。
- 次回ジョブ監視リクエストを実行すると、現在のポーリング間隔が次の日に設定され、次の日のデータが収集されます。
- 現在のポーリング間隔は、ジョブ監視リクエストが実行されるごとに、14 日前から 1 日ずつ進み、2 週間分のデータが収集されるまで各日のデータが収集されます。そこから、通常どおりデータ コレクションが再開されます。
- ポーリング間隔のデフォルト値は 1 日です。この値は、［Job Monitor］リクエスト オプション セクションでユーザー設定できます。
- データ コレクションを設定する際、［**Frequency**］は、必ず［各リクエストがデータを収集する最大時間範囲］よりも小さい値にする必要があります。そうしないと、リクエストが現在の時刻およびリクエストが実行される各時刻に間に合わずに遅れてしまい、残りのデータを収集できなくなります。

詳細については、モジュール別データ コレクション リクエスト オプションを参照してください。

監視対象オブジェクトおよびグループ

オブジェクトの概要

DPA は、データ保護環境のアプリケーションおよびデバイスを検出し、これらの論理エンティティおよび物理エンティティをオブジェクトとしてオブジェクト ライブラリに保存します。検出されたオブジェクトは、オブジェクト ライブラリの次のカテゴリーにグループ分けされます。

- アプリケーション
- ホスト
- ストレージ

- スイッチ

オブジェクトには次のルールが適用されます。

- 複数のオブジェクトが同じ名前を共有することはできない
- オブジェクトは、別のオブジェクトと同じエイリアスを持つことはできない

オブジェクト ライブラリにより、オブジェクトとその属性を確認できます。

オブジェクトの検索

オブジェクトを検索して、複数のオブジェクトのデータ コレクション リクエストを一度に変更できます。

手順

1. ［**Select Inventory**］ > ［**Object search**］の順にクリックします。
2. 検索条件を入力します。
   - ［**Name**］フィールドに、ホスト名、アプリケーション名、スイッチ名などのオブジェクト名を入力します。
   - ［**Types**］フィールドで、オブジェクト タイプを選択します。最上位のオブジェクト タイプ（ホスト、スイッチなど）、バックアップ アプリケーション以下のバックアップ サーバー/バックアップ クライアント/バックアップ プール、すべてのアプリケーション オブジェクト タイプを選択できます。
   - ［**Groups**］フィールドで、オブジェクト グループまたは Smart Group を選択します。
   - Smart Groups などのグループに含まれないオブジェクトを検索する場合は、［**Groups**］フィールドで［**Not In**］を選択します。デフォルトでは、［**In**］が選択されています。
   - ［**Requests**］フィールドで、リクエストでフィルターします。割り当てられていないリクエストで検索するには、［**Not Assigned**］を選択します。デフォルトでは、［**Assigned**］が選択されています。
   - ［**Agent**］フィールドで、データ コレクション エージェントからエージェントを選択します。
   - ［**Attributes**］フィールドで、属性を選択します。割り当てられていない属性で検索する場合、［**Select Attributes**］ダイアログで［**Not Assigned**］を選択します。デフォルトでは、［**Assigned**］が選択されています。［Not Assigned］を選択しないと、［Value］と［Clear］列が無効になります。

   バックアップ アプリケーション以下のバックアップ クライアント/バックアップ プールの検索では、次の点に注意してください。

   - バックアップ クライアントとプールの検索では、［**Requests**］および［**Agent**］検索オプションは使用できません。
   - バックアップ クライアントとプールの検索結果には、データ コレクションのリクエストと割り当ては行えません。

   ［**Types**］フィールドと［**Groups**］フィールドが、レポート範囲構成ツリー内と同じように整理されます。複数の検索条件を入力すると、それらは AND 条件で結合されます。
3. ［**Search**］をクリックします。

   検索結果は 500 項目まで表示されます。項目が 500 個以下になるように、検索条件で制限してください。

オブジェクトの表示

［**Inventory**］ > ［**Object Library**］の順に選択します。

複数オブジェクトの属性の表示および編集

この手順により、オブジェクト検索から返された複数のオブジェクトを選択し、複数のオブジェクトに割り当てられた属性を一度に表示して編集できます。

手順

1. 属性を表示または編集するオブジェクトを検索します。

   オブジェクトの検索（204 ページ） を参照してください。

2. 検索で返されたオブジェクトを選択し、右クリックして［**Set Attributes**］を選択します。

   ［**Attributes – Multiple Objects**］ウィンドウが表示されます。

3. 選択したオブジェクトの属性を編集するには、［**Name**］列の横のチェック ボックスをオンにして［**OK**］をクリックします。

オブジェクトに対するデータ コレクションの編集

検出プロセスの一環として、DPA の［Discovery Wizard］はデータ コレクションのリクエストをオブジェクト作成中にオブジェクトに直接割り当てます。特定のオブジェクトに対するデフォルトのデータ コレクション リクエストを編集するには、次のようにします。

オブジェクトの検索（204 ページ）にデータ コレクション リクエストの編集に関する追加情報が記載されています。

手順

1. ［**Inventory**］ > ［**Object Library**］の順に選択します。
2. ［ホストを選択して］ > ［**Data collection**］ > ［タブをクリックします。］
3. ［**Properties**］をクリックします。
4. リクエストを選択して［**Edit**］をクリックします。

結果

Manage Data Collection Defaults（97 ページ）にデフォルトのデータ コレクション リクエストに関する情報が記載されています。「Data Protection Advisor online help system」セットには、データ コレクション リクエストを追加、編集、表示する処理手順が記載されています。

グループ

グループはオブジェクトの集まりです。たとえば、アプリケーションで使用するオブジェクトのグループを作成できます。こうすると、グループにポリシーを適用する場合、ポリシーはグループ内のすべてのオブジェクトに適用されます。

注

オブジェクトは複数のグループに存在することができます。

構成グループ

構成グループはデフォルトで作成されます。構成グループは、データ保護環境をサーバ、スイッチ、およびストレージにグループ分けする初期構造を備えて作成されます。［Discovery Wizard］で検出されたすべてのデータ保護ホスト、デバイス、およびアプリケーションはまず、構成グループに追加されます。構成グループから削除されているオブジェクトは削除されません。構成グループから削除されたオブジェクトは［Groups］ではなく［Objects］の下に表示されます。

グループの作成

手順

1. ［**Inventory**］ > ［**Group Management**］の順に移動します。
2. オブジェクト インベントリで［**Groups**］を選択し、［**Create Group**］をクリックします。
3. 新しいグループの名前を入力します。
4. オブジェクト インベントリで、グループに追加するホストまたはホスト グループを選択します。
5. 新しく作成したグループにホストをコピー&ペーストします。

   元のオブジェクト インベントリからホストをカットまたは削除しないようにします。

オブジェクト属性

オブジェクト属性は、オブジェクトに関して DPA が保持する情報を拡張します。カスタム属性を作成した後、カスタム属性設定に従って有効なオブジェクトでその属性を有効化し、値を割り当てることができます。

オブジェクトを作成または編集するとき、属性は 1 個以上の特定のオブジェクト タイプに関連づけるようフィルターされ、特定の値に一致する既存の属性を持つオブジェクトにのみフィルターされます。

たとえば、オペレーティング環境の物理的コンポーネント（ホスト、ストレージ アレイ、スイッチなど）用の資産の識別子を表す Asset Tag 属性を作成します。Asset Tag 属性は、データベース、インスタンス、プロセスなどの論理コンポーネントに割り当てできる必要はありません。

属性定義の中で、Asset Tag は、物理オブジェクト タイプのサブセットに関連づけるように構成されます。たとえば、「Business Unit」の属性を持つ物理オブジェクト タイプにだけ関連づけるように、この属性をさらに構成することもできます。

Smart Group

Smart Group を使用すると、管理者権限を持つユーザーは、DPA レポートの結果から得た情報で動的に取得されるグループを作成できます。Smart Group は、カスタム レポートを実行し、その後レポートの結果に基づいてオブジェクトを作成します。

Smart Group の主なメリットは、高度な柔軟性を提供することです。管理者は、Smart Group を設定して、特定のビジネスおよび技術的な条件に一致するオブジェクトの一覧を動的に作成できます。

Smart Group の作成

Smart Group の作成については、「Data Protection Advisor online help system」を参照してください。付帯オプションの詳細については、マルチレベル Smart Group（207 ページ）とシングルレベル Smart Group（208 ページ）を参照してください。

手順

1. ［**Inventory**］ > ［**Group Management**］の順に選択します。
2. ［**Create Group**］、次に［**Create Smart Group**］をクリックします。
3. Smart Group の名前を［**Smart Group Name**］フィールドに指定します。
4. Smart Group のタイム ゾーンを指定します。
5. Select an option: ［**Single-level Smart Group**］または［**Multilevel Smart Group**］を選択して、［**Configure Smart Group Level**］をクリックします。
6. ［**Generation Frequency**］を指定します。

- DPA で、スケジュールした時刻に Smart Group を作成する場合は、頻度として［**Once a day at**］か、［**Schedule**］を選択します。
- 作成または編集時に Smart Group を作成する場合は、回数に［**On demand**］を選択します。

7. 選択した各レポート オブジェクトのフィールドを指定し、［**OK**］をクリックします。
8. コンテンツ ノードで履歴を保存してレポートを作成するように Smart Group を構成する場合は、［**Enable History**］を［**On**］に設定します。

   デフォルトでは、［**Enable History**］は［**Off**］に構成されています。
9. 以下のいずれかをクリックします。
   - ［**Save and Run**］：［Generation Frequency］のタイプを［**Once a day at**］または［**Schedule**］に設定した場合。
   - ［**OK**］：［Generation Frequency］のタイプを［**On demand**］に設定した場合。

マルチレベル Smart Group

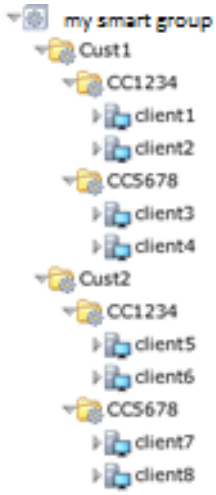
Smart Group に基づく 1 レベルの子オブジェクトのみを返すシングルレベル Smart Group とは異なり、マルチレベル Smart Group は単一の Smart Group から複数レベルの子オブジェクトを作成できます。また、各レベルで使用するフィールドを構成できるほか、作成するオブジェクトのタイプも指定できます。構成できるレベルの数に制限はありません。必要であれば、マルチレベル Smart Group を使用してご使用の DPA 環境の完全なマッピングを作成することもできます。

たとえば、次の表に示すデータを返す Smart Group で使用されるレポートを、実行したときに以下の図に示すオブジェクト構成を返すように構成できます。

表 37 マルチレベル Smart Group の例

お客様	コスト センター	クライアント
Cust1	CC1234	Client1
Cust1	CC1234	Client2
Cust1	CC5678	Client3
Cust1	CC5678	Client4
Cust2	CC1234	Client5
Cust2	CC1234	Client6
Cust2	CC5678	Client7
Cust2	CC5678	Client8

図 4 マルチレベル Smart Group のオブジェクト ライブラリの構成例



チャージ バックやデータ保護のポリシーを Smart Group または返される子オブジェクトのいずれかに割り当て、構造が最後に更新されたまたは生成されたタイミングを把握できます。デフォルトでは、Smart Group は毎日生成されます。また、階層グループを外部データ ソースと統合することができるため、単一階層の Smart Group を作成してすでに外部システムやデータベースに存在する可能性があるオブジェクト構造を作成できます。

これを表示、拡張してレポートを作成できるのは、その Smart Group を閲覧する権限があるユーザーのみです。

シングルレベル Smart Group

シングルレベル Smart Group は、1 つの階層レベルに含まれるレポートからの単一のオブジェクト セットです。解析やスケジュール設定レポートなど、通常のオブジェクトと同じアイテムを割り当てることができます。それにより DPA は、オブジェクトを出力する Smart Group のアラートおよびレポートを生成できます。

たとえば、ある金融会社では、各バックアップ クライアントの最初の 2 文字が、クライアントが割り当てられている事業単位を示すという決まりがあるとします。最初の 2 文字が am ならば、バックアップ クライアントは、アセット アセスメント（asset management）グループに属します。ビジネスの性質上、毎日多数のクライアントが作成、名前変更、あるいは削除されます。DPA 管理者は、毎日のグループ構成の更新に長い時間をかける代わりに、既存の Backup Client Configuration レポートを使用して各バックアップ クライアントを一覧表示する Smart Group を作成できます。Smart Group では、管理者は a と m で始まるクライアントだけを含むように結果をフィルターできます。

DPA は、バックアップ サーバーからデータを取得するたびにクライアント構成リストを自動的に更新するため、このリストは常にバックアップ環境で行われる変更が反映され、最新の状態に保たれます。

その他の例としては、次のようなものがあります。

- exch を含むすべてのバックアップ クライアント
- E:ドライブを持つすべてのホスト。
- 最終日に重大度 1 のアラートを生成したすべてのオブジェクト。

Smart Group ヒストリ

Smart Group ヒストリを使用すると、履歴に基づいてコンテンツ ノードを格納してレポートを作成できます。

［Smart Group History］設定を使用すると、Smart Group 内の変更についてレポートを作成できるため、サービス プロバイダーは正確な履歴に基づいて課金できます。

［Enable History］設定をオンにすると、Smart Group が生成されるごとに順番に、履歴が格納されます。設定をオフにすると、すべての履歴が削除され、Smart Group が再生成された時点の状態のみが格納されます。デフォルトでは、［Enable History］は［**Off**］に設定されています。

DPA Web コンソールを使用した履歴のバックアップ データの収集

Avamar、BackupExec、DB2、HP DataProtector、NetWorker、NetBackup、Oracle RMAN、SAP HANA、TSM では、履歴のバックアップ データを収集できます。

DPA Web コンソールを使用して履歴のバックアップ データを収集するときは、次の点を考慮します。

- ホスト単位では履歴のバックアップ データを収集できません。構成ツリーで 1 段階下に相当するアプリケーション オブジェクトのレベルで対応する必要があります。たとえば、NetWorker から履歴のデータを収集するには、ホスト レベル オブジェクトの下に相当する Networker のアプリケーション オブジェクトを選択します。
- 履歴のバックアップは、JobMonitor リクエストからのみ収集できます。

手順

1. Web コンソールで、［**Inventory** ］ > ［**Group Management**］の順に選択します。
2. 構成ツリーで、履歴のバックアップ データを収集するアプリケーション オブジェクトを選択します。

   アプリケーション オブジェクトの［**Details**］ウィンドウが開きます。
3. ホスト詳細ウィンドウで、［**Data Collection**］タブを選択します。
4. ［**Data Collection**］で、JobMonitor リクエストを選択します。
5. ［**Run**］を右クリックし、［**Gather historical data**］を選択します。
6. ［ **Gather historical data** ］ウィンドウで［**OK**］をクリックします。

   同じ認証情報とデータ オプションはリクエスト自体で使用できます。
7. ［**Close**］をクリックすると、DPA が履歴のバックアップ データを収集していることを確認するダイアログ ボックスが表示されます。
8. ［**History**］をクリックして収集されたテストを表示します。オレンジ色でハイライト表示されている行に、履歴のバックアップの収集結果が示されています。

ポリシー、ルール、アラートの構成

ポリシーとアラートの概要

DPA には、DPA によるアラートの生成方法、バックアップとレプリケーションのパフォーマンス測定方法、チャージ バック レポート値の決定方法を制御するカスタマイズ可能なポリシーとルールが含まれます。

ポリシー

DPA ポリシーは、環境内でバックアップおよびレプリケーションがどのように動作する必要があるかについてのユーザー データ（復旧可能性ポリシーおよびデータ保護ポリシー）、またはストレージおよびデータ保護動作のコストについてのユーザー データ（チャージバック ポリシー）のコレクションです。

復旧可能性レポート、バックアップ レポート、サービス レベルの管理レポートで、環境内の動作がポリシー設定と比較してどうか（たとえば、復旧可能性チェーンのストレージ アレイにおけるギャップ）またはバックアップ サーバーが目標復旧時点を満たしていないかが表示されます。

DPA には、次のポリシー タイプがあります。

- 解析ポリシー：1 つ以上のルールのコレクションで、主にアラート生成に使用します。アラートがデフォルトで［**Alerts**］セクションに表示されます。ポリシーを編集して、イベントをメール、スクリプト、SNMP トラップ、または Windows イベント ログに送信できます。ポリシーとイベント生成（236 ページ）で詳細を参照してください。
- 保護ポリシー：環境内でバックアップおよびレプリケーションがどのように動作すべきかについてのユーザー データのコレクションです。これらのポリシーは復旧可能性と保護ルールから構成されます。これらは主に、アラートの生成に使用されます。アラートがデフォルトで［**Alerts**］セクションに表示されます。
- チャージバック ポリシー：チャージバック レポートの、ストレージおよびデータ保護動作のコストを判断する場合に使用します。

デフォルトでは、解析、保護、およびチャージバックのポリシーは、すべてのオブジェクトおよびグループについてオフです。

解析ポリシー

分析ポリシーは、1 つのオブジェクトまたはグループに割り当てられた 1 つ以上のルールのコレクションです。ルールにはアラートを発行するタイミングのロジックが含まれています。解析エンジンは、監視したデータとルールの条件と比較して、ルールと一致したとき、アラートをトリガーします。イベント ベースのルールでは、DPA サーバーに流れ込むデータに応答してアラートをトリガーします。スケジュール ベースのルールは定期的に DPA データストアのデータをルールと比較して一致を検出します。アラートにはダイナミック テキスト情報を含むことができ、レポートへの使用中のリンクを含むことも可能です。アラートを生成できるのは解析ポリシーだけです。

解析ルール テンプレート

解析ルール テンプレートは、ルールのロジックを定義する一連の指示です。ルール テンプレートが解析ポリシーに追加されると、Analysis Engine が特定の動作を行い、結果生じたイベントを Web コンソールの［**Advisor**］セクションに表示します。

ルール テンプレートは、ルール名とそのルールの実行方法を指定する詳細で構成されます。

たとえば、ファイル システムの使用率が 1 時間以内に 90%を超える可能性があるかどうかを監視するルール テンプレートを作成できます。

解析ポリシーには、異なるオブジェクト タイプに適用される複数のルールが入っています。Analysis Engine は、ある指定のオブジェクトに該当するルールのみ実行します。たとえば、オブジェクトがスイッチの場合、Analysis Engine は、スイッチに適用されるポリシー中のルールのみ実行します。

イベント ベースのルールとスケジュール ベースのルール

イベント ベースのルールは、DPA サーバーにストリーミングしているデータにリアルタイムに対応して、アラートをトリガーします。イベント ベースのルールには次の 5 タイプの条件があります。

- 条件フィルター：バックアップの失敗など、設定された条件でアラートがトリガーされます。条件フィルターは、イベント ベース ルールの最も一般的な条件です。

- イベントの欠如：エージェントの停止などのイベントが、定義された期間内に発生しない場合にアラートがトリガーされます。
- 予測：ファイルシステムがいっぱいになるなど、イベントが定義された期間中に発生した場合にアラートがトリガーされます。
- 構成の変更：アクティブまたは非アクティブ、バージョン、OS タイプ、特定のフィールド、特定のパーセンテージの増減など、構成内に何らかの変更があった場合にアラートがトリガーされます。
- インベントリの変更：新しい RMAN インスタンスなど、新しいタイプのノードが自動作成された場合にアラートがトリガーされます。

スケジュール ベース ルールは定期的に実行され、アラートを発行するかどうかを確認します。データを収集するために設定したスケジュールのタイプによっては、DPA サーバーで問題が検出されてから数時間後にアラートが送信されることがあります。

スケジュール ベース ルールとイベント ベース ルールの両方で、ルールを含むポリシーを作成し、該当するノードのグループにポリシーを適用して、ポリシーが適用されたノードで受信された新しいデータが、ルールの条件を満たすエンティティを含んでいることを確認する必要があります。DPA Web コンソールは機能豊富なルール エディタです。使用すると、必要に応じてイベント ベース ルールとスケジュール ベース ルールを両方とも作成、編集、カスタマイズできます。解析ルールの作成（211 ページ）で詳細を参照してください。

解析ルール コンポーネントに関するガイドライン

解析ルールを作成するときは、アラートを設定するルールのカテゴリー、アラートの監視および作成の対象となるオブジェクト タイプ、アラートの対象となるオブジェクトの属性といった主要コンポーネントを検討してください。

DPA には、解析ルールのシステム ルール テンプレートの堅牢なリポジトリが含まれています。カスタム解析ルールを作成する前に、ニーズを満たす解析ルールが存在しないことを確認します。［**Policies**］ > ［**Analysis Policies**］ > ［**System Rule Templates**］の順に移動します。［System Rule Template］を選択して編集すると、DPA はこのポリシーの構築に使用されたカスタマイズを消去します。つまり、DPA がどのようにポリシーを構築したかは確認できません。

解析ルールのカテゴリー

カテゴリーは、DPA で解析ルールを保存するために使用されます。作成した解析ルールのフィルタリングや検索にも使用されます。作成する解析ルールのカテゴリー選択に厳格な基準はありません。カスタム解析ルールを作成する場合は、設定するルールの記憶や検索に最適なカテゴリーをドロップダウンから選択します。「Data Protection Advisor online help system」は解析ポリシーのカテゴリーに関する情報を提供します。

オブジェクト タイプと属性

選択するオブジェクト タイプと属性は、監視対象のオブジェクトやそのオブジェクトに関して収集されるデータなど、アラートをトリガーする状況に依存します。DPA が監視するオブジェクトで収集されるデータについてサポートが必要な場合は、「Data Protection Advisor Data Collection Reference Guide」でオブジェクトと属性の情報を確認できます。このとき、各モジュール機能内のテーブル名がオブジェクトにマッピングされ、各テーブルのフィールド名が属性にマッピングされています。オブジェクト タイプとアラートのトリガーで、このルールの情報を構成してから、フィルターを適用できます。

解析ルールの作成

DPA ルール エディタを使用して、解析ルール テンプレートを作成します。次にプロセスの概要を詳しく説明します。「Data Protection Advisor online help system」には、解析ルール テンプレートの作成、編集、コピーの方法に関する詳細が記載されています。

これは、解析ルールを作成する一般的な手順です。この手順の後にイベント ベースおよびスケジュール ベースの解析ルールの具体例を記載します。

手順

1. DPA Web コンソールで、［**Policies**］ > ［**Analysis Policies**］ > ［**Rules Templates**］に移動します。
2. ［**Create Rule Template**］をクリックします。

   これにより、ルール エディタが開きます。
3. このルールでトリガーされるアラートの名前と説明を入力します。
4. ルールに関連したカテゴリーを選択します。

   ルール カテゴリーおよびその説明については、「Data Protection Advisor online help system」を参照してください。
5. ルールがイベント ベースかスケジュール設定ルールかを指定します。

   イベント ベースのルールは、DPA サーバーにストリーミングしているデータに応えてアラートをトリガーします。スケジュール ベースのルールは、アラートを発行するか定期的に確認するために実行します。

   ルールがスケジュール ベースのルールである場合は、［**Report Parameters Default Values**］を設定します。
6. 適切なオブジェクト タイプを選択します。
   - 階層別
   - 機能別
7. いつ、どのようにアラートをトリガーするか定義します。

   DPA は `Lack of event` トリガーの `Number of samples` をテストするオプションをサポートしていませんが、DPA Web コンソールではこのオプションがまだ有効と表示されるので注意してください。DPA では、`Number of samples` オプションが `Time window` に対してまだサポートされています。

条件フィルターのイベント ベース ルールの作成

イベント ベースのルールは、DPA サーバーにストリーミングしているデータにリアルタイムに対応して、バックアップの失敗など、設定された条件でアラートをトリガーします。条件フィルターは、イベント ベースのルールの最も一般的な条件です。

次の手順は、バックアップが失敗したときに、アラートをトリガーするルールを作成するためのものです。

手順

1. ［**Policies**］ > ［**Analysis Policies**］ > ［**Custom Rule Templates**］の順に移動し、［**Create Custom Rule Template**］をクリックします。
2. そのルールに設定する条件に合ったルール名を［**Name/Alert Message**］フィールドに入力します。

   例：**`Backup Failed`**

   必要に応じて条件の説明も入力できます。これはオプションです。

   「Backup Failed」というシステム テンプレート ルールはすでにあり、適宜編集できます。この例では、このルールを最初から作成する方法を示します。
3. ［**Category**］フィールドで、設定するルールに最適のカテゴリーをドロップダウン リストから選択します。

   例：［**Data Protection**］

この例では、保護されていないデータに対してアラートをトリガーするため、［Data Protection］が最適のカテゴリーです。

4. オブジェクト タイプを構成します。この例では、各バックアップ クライアントでのバックアップの失敗に対してアラートをトリガーするので、［Backupjob］オブジェクトを選択します。

   a. ［**Object Type**］で［**Select**］をクリックします。

      ［**Select Object Types**］ウィンドウが開きます。

   b. ［Backup Applications］、［BackupClient］オブジェクトの順に展開し、［**Backupjob**］を［**Select Object Type**］リストから選択して［**Select Object Type**］をクリックします。

      フィルター機能を使用すると、監視対象のオブジェクトを簡単に検索できます。

      選択するオブジェクト タイプは、アラートをトリガーするシナリオによって異なります。

5. アラートのトリガーを構成します。この例では、失敗したジョブのみを確認するので、失敗したジョブのみを検出するように、トリガーを選択して条件フィルターを設定します。

   a. ［**Alert Trigger**］で［**Select**］を選択します。

      ［**Select Alert Trigger**］ウィンドウが開きます。

   b. ［**Conditions Filter**］ラジオ ボタンを選択し、［**Select and Edit Filter**］をクリックします。

      ［**Edit Filter**］ウィンドウが開きます。

   c. ［**Select Attribute**］をクリックします。

      ［**Select Attribute** ］ウィンドウが開きます。

   d. ［**Attribute**］ラジオ ボタンが選択されていることを確認し、［**Browse**］をクリックします。

      ［**Browse Attributes**］ウィンドウが開きます。

   e. ［Backupjob Category］で AttributeName ［**Status**］の行を選択し、［**Select Attribute**］、［**OK**］の順にクリックします。

      フィルター機能を使用すると、目的のカテゴリーと Attributename を簡単に検索できます。

   f. ［**Select Operator**］をクリックし、［**Is**］の値を設定して［**OK**］をクリックします。

   g. ［**Select Value**］をクリックし、［**Static Value**］ラジオ ボタンを選択して、ドロップダウンから［**failed**］の値を選択し、［ **OK**］をクリックします。

   h. ［**Select Attribute**］ウィンドウで［**OK**］をクリックし、［**Edit Filter**］ウィンドウで［**OK**］をクリックします。

   アラートを構成するシナリオは、アラートのトリガー ルールの構成方法、およびさらなるフィルタリング方法（該当する場合）に影響を与えます。

6. 次の要領でアラートを構成します。

   a. ［**Alert**］で［**Select**］をクリックします。

      ［**Edit Alert**］ウィンドウが開きます。

   b. ［**Alert Fields**］タブで、ドロップダウン リストから重大度を選択します。

   c. ［**Description & Resolution**］タブで、アラートと一緒に送信する説明と解決策の情報を構成します。

d. ［Associated Reports］タブでシステム テンプレート レポートを選択するか、アラート時に生成するカスタム レポートを作成します。

7. 保存オプションのいずれかをクリックします。

構成の変更に対するイベント ベース ルールの作成

イベント ベース ルールは、DPA サーバーにストリーミングしているデータにリアルタイムに対応して、あらゆるタイプの構成変更に対しアラートをトリガーします。たとえば、アクティブまたは非アクティブ、バージョン、OS タイプ、特定のフィールド、DPA が監視する任意のメトリックにおける特定の比率の増減などの変更に対応します。

次の手順は、クライアントをアクティブから非アクティブに変更するためのものです。

手順

1. ［**Policies**］ > ［**Analysis Policies**］ > ［**Custom Rule Templates**］の順に移動し、［**Create Custom Rule Template**］をクリックします。
2. アラートをトリガーする構成変更に適したルール名を、［**Name/Alert Message**］フィールドに入力します。

   例：`client active status changed`

   必要に応じて条件の説明も入力できます。これはオプションです。
3. ［**Category**］フィールドでドロップダウンから［**Change Management**］を選択します。
4. 以下の手順でオブジェクト タイプを構成します。
   a. ［**Object Type**］で［**Select**］をクリックします。

      ［**Select Object Types**］ウィンドウが開きます。

   b. ［Backup Applications］を展開し、［**Select Object Type**］リストから［**Backup Client**］を選択して［**Select Object Type**］をクリックします。
5. アラートのトリガーを構成します。この例では、アクティブから非アクティブに変わったクライアントを確認するために、適切なトリガーを選択します。
   a. ［**Alert Trigger**］で［**Select**］を選択します。

      ［**Select Alert Trigger**］ウィンドウが開きます。

   b. ［**Change Control**］ラジオ ボタンを選択し、［**Select and Edit Filter**］をクリックします。

      ［**Edit Alert Trigger - Change Control**］ウィンドウが開きます。

   c. ドロップダウン リストから［**ClientConfig**］を選択します。
   d. ［**Active**］の横にあるチェックボックスをオンにし、［**OK**］をクリックします。

      このルール構成では、アクティブ、非アクティブの変更に限らず、このフィールドのあらゆる変更でアラートがトリガーされます。

   すべてのクライアント上の構成変更を確認するため、条件のフィルターは不要です。
6. 次の要領でアラートを構成します。
   a. ［**Alert**］で［**Select**］をクリックします。

      ［**Edit Alert**］ウィンドウが開きます。

   b. ［**Alert Fields**］タブで、ドロップダウン リストから重大度を選択します。
   c. ［**Description & Resolution**］タブで、アラートと一緒に送信する説明と解決策の情報を構成します。

d. ［Associated Reports］タブでシステム テンプレート レポートを選択するか、アラート時に生成するカスタム レポートを作成します。

7. 保存オプションのいずれかをクリックします。

イベントの欠落に対するイベント ベース ルールの作成

イベント ベース ルールは、DPA サーバーにストリーミングしているデータにリアルタイムに対応して、エージェント停止などで、定義された期間にイベントが発生しなかった場合にアラートをトリガーします。

次の手順は、本番エージェントの停止に対してアラートをトリガーし、本番エージェントが停止しているあいだ、1 時間ごとにアラートを生成し続けるルールを作成するためのものです。

手順

1. ［**Policies**］ > ［**Analysis Policies**］ > ［**Custom Rule Templates**］の順に移動し、［**Create Custom Rule Template**］をクリックします。
2. そのルールに設定するイベントの欠落に合ったルール名を［**Name/Alert Message**］フィールドに入力します。

   例：`DPA Agent down`

   必要に応じて条件の説明も入力できます。これはオプションです。
3. ［**Category**］フィールドで、設定するルールに最適のカテゴリーをドロップダウン リストから選択します。

   例：［**Administrative**］
4. オブジェクト タイプを構成します。この例では、停止したエージェントを確認するため、AgentStatus を選択します。

   a. ［**Object Type**］で［**Select**］をクリックします。

   ［**Select Object Types**］ウィンドウが開きます。

   b. ［Host］オブジェクトを展開し、［**Select Object Type**］リストから［**AgentStatus**］を選択して［**Select Object Type**］をクリックします。

   フィルター機能を使用すると、監視対象のオブジェクトを簡単に検索できます。

   選択するオブジェクト タイプは、アラートをトリガーするシナリオによって異なります。
5. アラートのトリガーを構成します。この例では、停止した本番エージェントのみを確認するため、停止したエージェントのみを検索するように、トリガーを選択して条件フィルターを設定します。

   a. ［**Alert Trigger**］で［**Select**］を選択します。

   ［**Select Alert Trigger**］ウィンドウが開きます。

   b. ［**Event/Data Collection Did Not Occur**］ラジオ ボタンを選択し、［**Select and Edit Alert Trigger**］をクリックします。

   ［**Edit Alert Trigger**］ウィンドウが開きます。

   c. オプション 1 では、監視対象を選択し、［**Event did not occur**］と［**AgentStatus**］のラジオ ボタンを選択します。

   d. オプション 2 では、［**Keep Generating**］の隣のラジオ ボタンを選択します。

   e. オプション 3 では、本番を「prod」で表すなど、命名規則を使用してホスト名のタイプを指定する場合、［**Edit Conditions Filter**］ラジオ ボタンを選択して［**Select Attribute**］をクリックします。

f. [**Value Type**] フィールドの [**Attribute**] ラジオ ボタンが選択されていることを確認し、[**Attribute**] フィールドの [**Browse**] をクリックします。

g. [**Browse Attributes**] で [**name**] 属性を選択し、[**OK**] をクリックします。

h. [**Select Operator**] をクリックし、[**Contains**] の値を設定して [**OK**] をクリックします。

i. [**Select Value**] をクリックし、[**Static Value**] ラジオ ボタンを選択します。[**Value**] フィールドに「`prod`」と入力し、[**OK**] をクリックします。

j. [**Edit Filter**] ウィンドウで [**OK**] をクリックします。

k. オプション 4 では、[**Time Period**] の隣のラジオ ボタンを選択し、ドロップダウンから [**Static Value**]、数字のドロップダウンから [**1**]、期間のドロップダウンから [**hours**] を選択し、[**OK**] をクリックします。

アラートを構成するシナリオは、アラートのトリガー ルールの構成方法、およびさらなるフィルタリング方法（該当する場合）に影響を与えます。

6. 次の要領でアラートを構成します。

a. [**Alert**] で [**Select**] をクリックします。

[**Edit Alert**] ウィンドウが開きます。

b. [**Alert Fields**] タブで、ドロップダウン リストから重大度を選択します。

c. [**Description & Resolution**] タブで、アラートと一緒に送信する説明と解決策の情報を構成します。

d. [Associated Reports] タブでシステム テンプレート レポートを選択するか、アラート時に生成するカスタム レポートを作成します。

7. 保存オプションのいずれかをクリックします。

インベントリの変更に対するイベント ベース ルールの作成

イベント ベース ルールは、DPA サーバーにストリーミングしているデータにリアルタイムに対応して、新しいタイプのノードが自動作成された場合にアラートをトリガーします。

次の手順は、RMAN バックアップ クライアント インスタンスが自動作成されたときにアラートをトリガーするルールを作成するためのものです。

手順

1. [**Policies**] > [**Analysis Policies**] > [**Custom Rule Templates**] の順に移動し、[**Create Custom Rule Template**] をクリックします。
2. そのルールに設定する条件に合ったルール名を [**Name/Alert Message**] フィールドに入力します。

   例：`new RMAN database backed up to central recovery catalog`

   必要に応じて条件の説明も入力できます。これはオプションです。
3. [**Category**] フィールドで、設定するルールに最適のカテゴリーをドロップダウン リストから選択します。

   例：[**Configuration**]
4. オブジェクト タイプを構成します。この例では、新規の RMAN バックアップ クライアント インスタンスに対しアラートをトリガーするため、OracleRMANBackupclient オブジェクトを選択します。

a. [**Object Type**] で [**Select**] をクリックします。

[**Select Object Types**] ウィンドウが開きます。

b. [Host]、[Applications and Databases]、[Oracle Application] の順に展開し、[**Select Object Type**] リストから [**OracleRMANBackupclient**] を選択して [**Select Object Type**] をクリックします。

フィルター機能を使用すると、監視対象のオブジェクトを簡単に検索できます。

選択するオブジェクト タイプは、アラートをトリガーするシナリオによって異なります。

5. アラートのトリガーを構成します。この例では、新規作成されたオブジェクトのみを確認するので、インベントリ変更のみを検出するように、トリガーを選択して条件フィルターを設定します。

a. [**Alert Trigger**] で [**Select**] を選択します。

[**Select Alert Trigger**] ウィンドウが開きます。

b. [**Inventory changes**] ラジオ ボタンを選択し、[**Select and Edit Filter**] をクリックします。

[**Edit Alert Trigger - inventory Change**] ウィンドウが開きます。

c. オプション 1 では、[**Select operations to monitor**]、[**Created**] が選択されていることを確認して [**OK**] をクリックします。

アラートを構成するシナリオは、アラートのトリガー ルールの構成方法、およびさらなるフィルタリング方法（該当する場合）に影響を与えます。

6. 次の要領でアラートを構成します。

a. [**Alert**] で [**Select**] をクリックします。

[**Edit Alert**] ウィンドウが開きます。

b. [**Alert Fields**] タブで、ドロップダウン リストから重大度を選択します。

c. [**Description & Resolution**] タブで、アラートと一緒に送信する説明と解決策の情報を構成します。

d. [Associated Reports] タブで、システム テンプレート レポートを選択するか、アラート時に生成するカスタム レポートを作成します。

7. 保存オプションのいずれかをクリックします。

予測のイベント ベース ルールの作成

イベント ベース ルールは、DPA サーバーにストリーミングしているデータにリアルタイムに対応して、定義されたイベントが定義された期間に発生した場合にアラートをトリガーします。

次の手順は、Avamar サーバーの使用率がその時点から 24 時間以内に 90%に達すると予測されたときにアラートを発動させるルールを作成するためのものです。

手順

1. [**Policies**] > [**Analysis Policies**] > [**Custom Rule Templates**] の順に移動し、[**Create Custom Rule Template**] をクリックします。
2. そのルールに設定する条件に合ったルール名を [**Name/Alert Message**] フィールドに入力します。

例：`Avamar server predicted to reach 90% in next 24 hours`

必要に応じて条件の説明も入力できます。これはオプションです。

「Backup Failed」というシステム テンプレート ルールはすでにあり、適宜編集できます。この例では、このルールを最初から作成する方法を示します。

3. ［**Category**］フィールドで、設定するルールに最適のカテゴリーをドロップダウン リストから選択します。

   例：［**Resource Utilization**］

4. オブジェクト タイプを構成します。この例では、Avamar バックアップ サーバーにアラートを送信するため、［Backup Application］オブジェクトを選択します。

   a. ［**Object Type**］で［**Select**］をクリックします。

      ［**Select Object Types**］ウィンドウが開きます。

   b. ［Backup Applications］、［Backup Server］の順に展開し、［**Select Object Type**］リストの［**Backup Application**］を選択して［**Select Object Type**］をクリックします。

      フィルター機能を使用すると、監視対象のオブジェクトを簡単に検索できます。

      選択するオブジェクト タイプは、アラートをトリガーするシナリオによって異なります。

5. アラートのトリガーを構成します。この例では、特定期間に特定のバックアップ サーバーの使用率がターゲットに達する場合のみを確認するため、予測に基づく動向のみを検索するように、トリガーを選択して条件フィルターを設定します。

   a. ［**Alert Trigger**］で［**Select**］を選択します。

      ［**Select Alert Trigger**］ウィンドウが開きます。

   b. ［**Predictive Time**］ラジオ ボタンを選択し、［**Select and Edit Filter**］をクリックします。

      ［**Edit Filter**］ウィンドウが開きます。

   c. オプション 1 では、予測する属性を選択し、［**Browse**］を選択します。

      ［**Select Attribute** ］ウィンドウが開きます。

   d. ［BackupApplication Object Type］で AttributeName ［**Utilization**］の行を選択し、［**Select Attribute**］、［**OK**］の順にクリックします。

      フィルター機能を使用すると、目的のカテゴリーと Attributename を簡単に検索できます。

   e. オプション 2 では、しきい値を設定し、［**Static Value**］を選択して「90」と入力するか、この値までスクロールします。

   f. オプション 3 では、アラートを送信するタイミングを指定し、［**Static Value**］を選択して、用意されたドロップダウンでそれぞれ［**1**］と［**Days**］を選択します。

   g. この例に該当する条件フィルターがないため、オプション 4 は省きます。

   h. オプション 5 では、予測の方法を選択し、デフォルトの選択内容をそのまま維持します。

   i. ［**OK**］をクリックします。

   アラートを構成するシナリオは、アラートのトリガー ルールの構成方法、およびさらなるフィルタリング方法（該当する場合）に影響を与えます。

6. 次の要領でアラートを構成します。

   a. ［**Alert**］で［**Select**］をクリックします。

      ［**Edit Alert**］ウィンドウが開きます。

b. ［**Alert Fields**］タブで、ドロップダウン リストから重大度を選択します。

c. ［**Description & Resolution**］タブで、アラートと一緒に送信する説明と解決策の情報を構成します。

d. ［Associated Reports］タブでシステム テンプレート レポートを選択するか、アラート時に生成するカスタム レポートを作成します。

7. 保存オプションのいずれかをクリックします。

スケジュール ベース ルールの作成

スケジュール ベースのルールは定期的に DPA データストアのデータをルールと比較し、トラッキングする特定の問題との一致を検出します。この処理にはレポートが使用されます。システム テンプレート レポートまたはカスタム レポートを使用できます。

次の手順は、バックアップ クライアントが 3 回失敗した場合にアラートをトリガーするルールを作成するためのものです。

手順

1. ［**Policies**］ > ［**Analysis Policies**］ > ［**Custom Rule Templates**］の順に移動し、［**Create Custom Rule Template**］をクリックします。
2. そのルールに設定する条件に合ったルール名を［**Name/Alert Message**］フィールドに入力します。

   例：`schedule based three strikes failed backup`

   必要に応じて条件の説明も入力できます。これはオプションです。

   「Backup Failed」というシステム テンプレート ルールはすでにあり、適宜編集できます。この例では、このルールを最初から作成する方法を示します。
3. ［**Type**］フィールドで、ドロップダウンから［**Scheduled**］を選択します。
4. ［**Category**］フィールドで、設定するルールに最適のカテゴリーをドロップダウン リストから選択します。

   例：［**Data Protection**］
5. レポートを選択します。この例では、バックアップ クライアントが 3 回失敗した場合にアラートをトリガーするため、［Three Strike Failed Client］レポートを選択します。

   a. ［**Select Report Template**］で［**System Report Templates**］をクリックします。

   b. ［**System Template Name**］リストから［**Three Strike Failed Client**］を選択し、［**Select Template and Edit Options**］をクリックします。

   フィルター機能を使用すると、監視対象のオブジェクトを簡単に検索できます。

   選択するオブジェクト タイプは、アラートをトリガーするシナリオによって異なります。
6. オプションを構成します。

   a. ［Number of Alerts］で、ニーズに最適なオプションを選択します。

   ［**Generate a separate alert for each row**］を選択すると、DPA から各クライアントに対して別々にアラートが送信されます。この情報は、細分性が高く便利です。ただし、多数のクライアントでアラートを発動させる場合は、大量のアラートが表示されます。

   ［**Generate one alert for all rows**］を選択すると、DPA からトップ レベルのノードに対してアラートが送信されます。これは、多数のクライアントを保有しているためにアラート数を減らしたい場合に役立ちますが、情報の細分性が低くなってしまいます。

b. [Default] の設定で、[**Select Schedule**] をクリックし、[Manage Schedule] オプションのいずれかを選択するか、[**Create Schedule**] をクリックして、ルールを実行するタイミングを定めた独自のスケジュールを作成します。

[Manage Schedule] オプションのうち、[**Always**] の選択は推奨されません。このオプションではサーバーにかかる負荷が大きいためです。

c. 必ず期間の選択内容を確認し、デフォルト値をそのまま採用するか、選択内容を変更します。

d. [**OK**] をクリックします。

7. 次の要領でアラートを構成します。

a. [**Alert**] で [**Select**] をクリックします。

[**Edit Alert**] ウィンドウが開きます。

b. [**Alert Fields**] タブで、ドロップダウン リストから重大度を選択します。

c. [**Description & Resolution**] タブで、アラートと一緒に送信する説明と解決策の情報を構成します。

d. [**Associated Reports**] タブで、システム テンプレート レポートを選択するか、アラート時に生成するカスタム レポートを作成します。

e. [**Rule Objects**] タブでは、[**Object Type**] を選択し、ドロップダウンから [**Name Field**] と [**Sub Name Field**] を選択する必要があります。

8. 保存オプションのいずれかをクリックします。

解析ルールの解析ポリシーへの追加

ルール テンプレートが解析ポリシーに追加されると、Analysis Engine が特定の動作を行い、結果生じたイベントを Web コンソールの [**Alerts**] セクションに表示します。

解析ポリシーには、さまざまな種類のオブジェクトに適用する複数の解析ルールが入っています。DPA は、適用された解析ポリシーから適切なツールをオブジェクトに自動的に適用します。たとえば、DPA ではスイッチのルールはバックアップ サーバーではなく、スイッチのみに適用されます。

Analysis Engine のアクションのログ ファイル

`actions.log` には、成功した Analysis Engine のアクションの通知 1 つにつき 1 個のレコードが作成されます。

Analysis Engine のアクションは次のいずれかです。

- メール
- SNMP
- scrpt
- Windows イベント ログ

`actions.log` には、成功したアクションに関する情報のみ含まれます。失敗したアクションの情報や警告などは含まれません。 `actions.log` のデフォルトの場所は、`$instalationDir\services\logs` です。この場所はユーザーが変更することはできません。

分析ポリシー ルール カテゴリー

キャパシティ プランニング

キャパシティ プランニング分析ポリシーでは、リソースが間もなく不足する可能性があることを示すイベントに関するアラートを作成します。以下の表では、これらのジョブについて説明します。

プールとストレージ アレイの分析ポリシーに関するアラートの割り当て
オブジェクトに次の分析ポリシーを割り当てる場合に推奨される重大度レベル。

- ストレージ プールの限界：重大度 3
- ストレージ プールの限界：重大度 2
- ストレージ アレイの限界：重大度 1

表 38 キャパシティ プランニング

ルール	説明	パラメーター
ファイル システムの限界	今後 2 週間以内にファイル システムの使用率が 90%を超えると予想される場合にアラートを生成します。	予想される最大使用率：100% 予測する時間数：336
バックアップ クライアント ライセンスの不足	ライセンスにより監視が許可される追加のコンピュータの台数が 25 台未満の場合にアラートを生成します。	クライアント ライセンスの最大数：25
ストレージ プールの限界	増加傾向に従うと、選択した期間でプールにスペースがなくなる場合にアラートを生成します。	許可される最小空き領域：0 予測する日数：90
ストレージ プールの限界	新しい LUN を物理的に割り当てるためのスペースがプールになくなった場合にアラートを生成します。	初期使用済み容量：3
ストレージ アレイの限界	新しい LUN を割り当てるためのスペースがプールになく、ストレージ アレイに使用可能な空きディスクがない場合にアラートを生成します。	初期使用済み容量：2
空テープの残量が少ない	6 週間以内にテープ プールの空テープがなくなると予想される場合にアラートを生成します。	予想される最大数：0 予測する時間数：1,008
TSM データベースの限界	TSM データベースの使用率が 2 週間以内に 100 %に達すると予想される場合にアラートを生成します。	予測する時間数：336 予想される最大使用率：100
TSM データベースの使用率が高い	TSM リカバリ ログの使用率が 2 週間以内に 100 %に達すると予想される場合にアラートを生成します。	予測する時間数：336 予想される最大使用率：100

変更管理
変更管理分析ポリシーは、環境内の変更に関するアラートを生成します。以下の表では、これらのジョブについて説明します。

表 39 変更管理

ルール	説明	パラメーター
バックアップ クライアント構成の変更	バックアップ クライアント構成が変更された場合にアラートを生成します。	N/A
バックアップ デバイス構成の変更	バックアップ デバイス構成が変更された場合にアラートを生成します。	N/A
バックアップ グループ構成の変更	バックアップ グループ構成が変更された場合にアラートを生成します。	N/A
ディスクのファームウェア レベルの変更	ディスクのファームウェア レベルが変更された場合にアラートを生成します。	N/A
ディスクのシリアル番号の変更	ディスクのシリアル番号が変更された場合にアラートを生成します。	N/A
オブジェクトのオペレーティング システムの変更	オブジェクトのオペレーティング システムが変更された場合にアラートを生成します。	N/A
RecoverPoint アクティブ RPA の変更	最後に分析を実行してからアクティブな RPA が変更された場合にアラートを生成します。	N/A
仮想マシンのコンシステンシー グループ コピーに対応する RecoverPoint が無効	仮想マシンのコンシステンシー グループ コピーに対応する RecoverPoint が無効の場合にアラートを生成します。	N/A
RecoverPoint RPA リンク ステータスの変更	最後に分析を実行してから RPA リンクのステータスが変更された場合にアラートを生成します。	N/A
テープ ドライブのファームウェア レベルの変更	テープ ドライブのファームウェア レベルが変更された場合にアラートを生成します。	N/A
テープ ドライブのシリアル番号の変更	テープ ドライブのシリアル番号が変更された場合にアラートを生成します。	N/A

構成

構成分析ポリシーは、デバイスまたはアプリケーションの構成に関する問題について環境を監視します。以下の表では、これらのジョブについて説明します。

表 40 構成

ルール	説明	パラメーター
バックアップ クライアントが非アクティブ	バックアップ クライアントが実行するようにスケジュール設定されていない場合にアラートを生成します。	該当なし

表 40 構成 （続き）

ルール	説明	パラメーター
ファイル サーバのエクスポートが LUN と同じボリュームで実行された	ファイル サーバのエクスポートが LUN と同じボリュームで実行された場合にアラートを生成します。	該当なし
特定のボリューム上の LUN	LUN が vol0 で構成された場合にアラートを生成します。	ボリューム：vol0
IP オート ネゴシエーションの不一致	ホストとそのスイッチ ポートとの間でオート ネゴシエーションの不一致が発生した場合にアラートを生成します。	該当なし
IP 二重化の不一致	オブジェクトとスイッチの間で二重化の不一致が発生した場合にアラートを生成します。	該当なし
不十分な仮想メモリ	コンピュータ上の仮想メモリの量が物理メモリの 1.5 倍未満のときにアラートを生成します。	該当なし
ボリュームの優先順位が異常	ボリュームの優先順位が正常な値以外に設定されている場合にアラートを生成します。	該当なし

データ保護

データ保護分析ポリシーは、環境のバックアップやリカバリの問題に関連する例外を監視します。次の表で、監視対象のジョブについて説明します。

表 41 データ保護

ルール	説明	パラメーター
アプリケーションのリストア時間の見積りが長すぎる	アプリケーションのリストア時間の見積りが 12 時間を超える場合にアラートを生成します。	目標復旧時間：12 時間
アプリケーションの RPO（Recovery Point Objective：目標復旧時点）を満たせなかった	アプリケーションに正しいバックアップがない状態が 72 時間を超えた場合にアラートを生成します。	目標復旧時点：72 時間
バックアップの失敗	バックアップに失敗した場合にアラートを生成します。	該当なし
1 分以内に成功したバックアップがない	2 回以上連続してバックアップに失敗した場合にアラートを生成します。	失敗の最大数：2
バックアップが平均よりも大きい	過去 14 日間にわたり、バックアップ ジョブが平均サイズの 2 倍になった場合にアラートを生成します。	履歴日数：14 日間 偏差：100%
バックアップが何日も実行されていない	過去 3 日間にわたりホストにバックアップがない場合にアラートを生成します。	バックアップのない最大日数：3

表 41 データ保護 （続き）

ルール	説明	パラメーター
サーバ操作と同時にバックアップが実行された	バックアップ サーバ上の次のいずれかの操作と重なる期間に完了したバックアップがあった場合にアラートを生成します。 • ボリュームの削除 • 有効期限切れ • ストレージ プールのコピー • ムーブ • データベース バックアップ • まったく不要 • 再生	なし。
バックアップ スパンが複数にわたっている	バックアップ スパンがテープ 3 本を超えた場合にアラートを生成します。	テープの最大数：3
フル バックアップが平均よりも小さい	フル バックアップが通常のサイズの 50%未満になった場合にアラートを生成します。	履歴日数：14 日間 偏差：50%
フル バックアップが何日も実行されていない	過去 14 日間にわたりホストでフル バックアップに成功しなかった場合にアラートを生成します。	バックアップのない最大日数：14
ミラーが数時間更新されなかった	リモート ディスク ミラーが 2 日以上更新されなかった場合にアラートを生成します。	最大消失時間：48 時間
フル バックアップでないバックアップが多すぎる	最後のフル バックアップの後に 7 回連続してバックアップ ジョブが生成された場合にアラートを生成します。	フル バックアップでないバックアップの最大数：7
NetWorker ブートストラップが生成されない	過去 48 時間に NetWorker ブートストラップが実行されなかった場合にアラートを生成します。	ブートストラップのない最大時間：デフォルトは 48 時間
サーバ操作と同時に TSM データベースのバックアップが実行された	他のバックアップを含め、バックアップ サーバ上で他の処理を実行している最中にデータベース バックアップ処理が完了した場合に、アラートを生成します。	なし。
TSM データベース バックアップが発生	過去 24 時間以内に TSM データベースのバックアップが行われた場合にアラートを生成します。バックアップが行われなかった場合は、最後の TSM バックアップ時刻を返します。	時間：24 時間

ライセンス

ライセンス分析ポリシーは環境を監視し、ライセンスの問題に関するアラートを生成します。次の表で、これらのポリシーについて詳細に説明します。

表 42 ライセンス

ルール	説明	パラメーター
License expired	DPA のライセンスの期限が切れた場合にアラートを生成します。	N/A
ライセンスの期限切れが近い	次の週にライセンスの期限が切れる場合にアラートを生成します。	期限切れまでの最小日数：デフォルトでは 7 日間

パフォーマンス

パフォーマンス分析ポリシーは環境を監視し、パフォーマンスの問題に関するアラートを生成します。以下の表では、これらのジョブについて詳しく説明します。

表 43 パフォーマンス

ルール	説明	パラメーター
バックアップが平均よりも遅い	過去 2 週間にわたり、バックアップ ジョブのパフォーマンスが平均の 50%未満になった場合にアラートを生成します。	履歴日数：14 偏差：50%
バックアップ ジョブの実行時間が長すぎる	バックアップの実行時間が 18 時間を超えた場合にアラートを生成します。	最大実行時間：18 時間
ファイル サーバのキャッシュ ヒット率が低い	ファイル サーバのキャッシュ ヒット率が 80%未満になった場合にアラートを生成します。	最小キャッシュ ヒット率：80%
フル バックアップに成功したが遅い	フル バックアップの実行速度が 300 KB/秒未満になった場合にアラートを生成します。	最小予測速度：300 KB/秒

プロビジョニング

プロビジョニング分析ポリシーは、プロビジョニング オペレーションを必要とする可能性があるイベントに関するアラートを生成します。以下の表でジョブについて説明します。

表 44 プロビジョニング

ルール	説明	パラメーター
ファイル システムのスナップショット領域の使用率が低い	過去 14 日間にわたり、スナップショットのピーク使用率が 80%未満になった場合にアラートを生成します。	使用率の調査日数：14 スナップショットの最小ピーク使用率：80%

復旧可能性

復旧可能性に関する復旧可能性解析ポリシー アラート。以下の表では、これらのジョブについて説明します。

表 45 復旧可能性

ルール	説明	パラメーター
TF/Snap に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
MirrorView/A に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
MirrorView/S に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
RecoverPoint/A に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
RecoverPoint/S に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
SanCopy に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
継続的な SRDF/S に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
ポイント イン タイムの SRDF/S に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
復旧可能性のデータ消失リスク	復旧可能性のデータ消失リスク	N/A
継続的な SRDF/A に関するコンシステンシー グループのチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
ポイント イン タイムの SRDF/A に関するコンシステンシー グループのチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
継続的な SRDF-S/EDP に関するコンシステンシー グループのチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
ポイント イン タイムの SRDF-S/EDP に関するコンシステンシー グループのチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A

表 45 復旧可能性 （続き）

ルール	説明	パラメーター
SRDF/A に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
SRDF/S に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
SV/クローンに関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
SV/Snap に関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
TF/ミラーに関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
TF/クローンに関する災害復旧ホストの可視性のチェック	リカバリ ポイントのデバイスのマッピング、マスキング、可視化は災害復旧ホストが実行	N/A
継続的な SRDF-A/EDP に関するコンシステンシー グループのチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
ポイント イン タイムの SRDF-A/EDP に関するコンシステンシー グループのチェック	リカバリ ポイントのデバイスが同一のコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効であることのチェック	N/A
ポイント イン タイムの SV/クローンに関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの SV/Snap に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの TF/ミラーに関する コンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの TF/クローンに関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A

表 45 復旧可能性 （続き）

ルール	説明	パラメーター
ポイント イン タイムの TF/Snap に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの MirrorView/A に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの MirrorView/S に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの RecoverPoint/A に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの RecoverPoint/S に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの SanCopy に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
ポイント イン タイムの SNAPVX に関するコンシステント デバイス レプリケーションのチェック	ベスト プラクティス チェック。コンシステンシーの操作が発行されなかった場合はアラートが生成されますが、ベンダーは推奨しています。	N/A
アプリケーションの整合性違反	整合性のとれていないレプリケーション：レプリケーション プロセス中にアプリケーションがバックアップ モードに入っていなかった	N/A
バックアップ モードに入っていないアプリケーション	レプリケーション作成中にアプリケーションがバックアップ モードに入っていなかった	N/A
コンシステンシー グループが無効	コンシステンシー グループが無効になっています。	N/A
無効なレプリケーション	オブジェクト用のイメージが失敗したか、スケジュールどおりに実行されなかった	N/A
Logs not on Disk	アプリケーション ログ ファイルがディスク上にない	N/A

表 45 復旧可能性 （続き）

ルール	説明	パラメーター
デバイスのすべてがレプリケーション グループに属してはいない	このデバイスはレプリケーション グループに属していない	N/A
Not Protected Logs	整合性のとれていないレプリケーション：ファイルはリカバリに必要だが保護されていない	N/A
Partially Replicated	オブジェクトの一部がレプリケート済み	N/A
継続的なレプリケーションが停止済み	継続的なレプリケーションが停止済み	N/A
ストレージ オブジェクトが保護されていない	アプリケーション ストレージ オブジェクトが保護されていない	N/A
連続的レプリケーションのリンク ステータスが停止中	連続的アプリケーションのリンク ステータスが停止中	N/A

リソース使用率

リソース使用率分析ポリシーは、環境内のリソースの使用率に関する問題が原因で発生したイベントに関するアラートを生成します。以下の表では、これらのジョブについて詳しく説明します。

表 46 リソース使用率

ルール	説明	パラメーター
スナップショットの総使用率が高い	スナップショットの総使用率が指定された閾値を超えた場合にアラートを生成します。	スナップショットの最大総使用率：デフォルトで 90%
CPU 過負荷	過去 30 分間にわたり、ホストの CPU 使用率が 90%を超えた場合にアラートを生成します。	CPU の最大利用率 : デフォルトで 90% 時間（分）: 30 分間
ディスク過負荷	30 分間にわたり、ホスト上のディスクが 90%以上ビジーになった場合にアラートを生成します。	最大ディスク ビジー率：90% 時間（分）: デフォルトで 30 分間
ファイバ チャネル ポートの使用率が高い	ファイバ チャネル ポートがその最大スループットの 70%を超えた場合にアラートを生成します。	最大使用率：70%
ファイバ チャネル ポートに BB クレジットがない	ファイバ チャネル ポートのバッファ間クレジットがなくなった場合にアラートを生成します。	該当なし
ファイル システムのファイル使用率が高い	ファイル システム上のファイルの数が許容最大数の 90%を超えた場合にアラートを生成します。	ファイル システムの最大ファイル使用率：90%
ファイル システムのスナップショット使用率が高い	ファイル システムのスナップショット使用率が 90%を超えた場合にアラートを生成します。	ファイル システムの最大スナップショット使用率：デフォルトで 90%

表 46 リソース使用率 （続き）

ルール	説明	パラメーター
ファイル システムの使用率が高く、増加中	ファイル システムの使用率が 90% を超え、増加中の場合にアラートを生成します。	ファイル システムの最大使用率：デフォルトで 90%
メモリ使用率が高い	ホスト上のメモリ使用率が 90%を超えた場合にアラートを生成します。	メモリの最大使用率：デフォルトで 90%
ネットワーク使用率が高い	ネットワーク インタフェースがその定格スループットの 70%を超えた場合にアラートを生成します。	最大使用率：デフォルトで 70%
RecoverPoint ジャーナルの使用率が高い	RPA のジャーナルの使用率が指定した警告または重大閾値を超えた場合にアラートを生成します。	警告閾値 重大閾値
RecoverPoint ジャーナルの使用率が高い	RPA の SAN の使用率が指定した警告または重大閾値を超えた場合にアラートを生成します。	警告閾値 重大閾値
RecoverPoint RPA WAN の使用率が高い	RPA の WAN の使用率が指定した警告または重大閾値を超えた場合にアラートを生成します。	警告閾値 重大閾値
RecoverPoint のレプリケーション遅延が大きい	レプリケーション時間またはデータ遅延が指定した警告または重大閾値を超えた場合にアラートを生成します。	時間遅延警告閾値 時間遅延重大閾値 データ遅延警告閾値 データ遅延重大閾値
TSM データベースの使用率が高い	TSM データベースの使用率が 90%を超えた場合にアラートを生成します。	最大データベース使用率：90%
期限切れプロセスの期間が予想を超えた	TSM 期限切れプロセスに 1 時間以上かかっているか、過去 7 日間の平均期限切れプロセス時間よりも 25%長くかかっている場合にアラートを生成します。	増加率：25% 期間：7 最大期間：1
TSM リカバリ ログの使用率が高い	TSM データベースの使用率が 90%を超えた場合にアラートを生成します。	最大リカバリ ログ使用率：90%

SLA（Service Level Agreement）

SLA（Service Level Agreement）分析ポリシーは、SLA 違反に関するアラートを生成します。以下の表では、SLA ジョブについて説明します。

表 47 Service Level Agreement

ルール	説明	パラメーター
バックアップに成功したが SLA 要件を満たさなかった	バックアップに成功したにもかかわらず、バックアップ ウィンドウを外れた場合にアラートを生成します。	該当なし

状態

状態カテゴリー分析ポリシーは、監視されているデバイスまたはアプリケーションの現在の状態が一致しないという問題が発生した場合にアラートを生成します。以下の表では、ステータス ジョブについて説明します。

表 48 状態

名	説明	ルール	パラメーター
バックアップ サーバのエラー	バックアップ サーバのエラーが記録された場合にアラートを生成します（TSM のみ）。	バックアップ サーバのエラー	N/A
仮想マシンのコンシステンシー グループのコピーのリンク停止	仮想マシンに対応する RecoverPoint のコンシステンシー グループのコピーは有効ですが、リンクが停止しています。	仮想マシンのコンシステンシー グループのコピーのリンク停止	エンティティ。CgCopyStatus 条件「有効が False（または 0。要チェック）」 フィールド：データ転送「有効」以外
CPU がオフライン	CPU がオフラインの場合にアラートを生成します。	CPU がオフライン	N/A
エージェントのハートビート失敗	エージェントがハートビートの送信に失敗した場合にアラートを生成します。	エージェントのハートビート失敗	N/A
エージェントのログ ファイルのメッセージ	エージェントのログ ファイルに表示されるメッセージに関するアラートです。	エージェントのログ メッセージ	N/A
ディスクの障害	ディスクに障害が発生した場合にアラートを生成します。	ディスクの障害	N/A
EDL フェイルオーバーの発生	EDL アプライアンスが他のアプライアンスにフェイルオーバーした場合にアラートを生成します。	EDL フェイルオーバーの発生	N/A
ファンが非アクティブ	デバイス上のファンが非アクティブな場合にアラートを生成します。	ファンが非アクティブ	N/A
ファイバ チャネル ポートの状態が変化した	ファイバ チャネル ポートの状態が変化した場合にアラートを生成します。	ファイバ チャネル ポートの状態が変化した	N/A

表 48 状態 （続き）

名	説明	ルール	パラメーター
使用可能なバックアップ デバイスが 75%未満	バックアップ サーバ上のバックアップ デバイスが 75%未満になった場合にアラートを生成します。	使用可能なバックアップ デバイスが x%未満	バックアップ デバイスの最小の可用性：デフォルトで 75%
使用できないバックアップ デバイスが 3 台を超えた	バックアップ サーバ上で 4 台以上のバックアップ デバイスが停止した場合にアラートを生成します。	使用できないバックアップ デバイスが多い	停止したデバイスの最大数：3
ネットワーク インタフェースの状態が変化	ネットワーク インタフェースでリンク アップまたはリンクダウン イベントが発生した場合にアラートを生成します。	ネットワーク インタフェースの状態が変化	N/A
オブジェクト再起動	ホストが再起動された場合にアラートを生成します。	オブジェクト再起動	N/A
オブジェクトのステータスが非アクティブ	オブジェクトのステータスがアクティブ以外に変わった場合にアラートを生成します。	オブジェクトのステータスが非アクティブ	N/A
PSU が非アクティブ	電源装置がアクティブでない場合にアラートを生成します。	PSU が非アクティブ	N/A
パブリッシャがハング	前回のポーリング以後パブリッシャのキューが変更されていない場合にアラートを生成します。	パブリッシャのキューがハング	N/A
サーバのログ ファイルのメッセージ	サーバのログ ファイルに表示されるメッセージに関するアラートです。	サーバのログ メッセージ	N/A
テープ ドライブにクリーニングが必要	テープ ドライブをクリーニングしなければならない場合にアラートを生成します。	テープ ドライブにクリーニングが必要	N/A
テープ ドライブが OK でない	テープ ドライブが OK 以外の状態を報告している場合にアラートを生成します。	テープ ドライブが OK でない	N/A
テープ ライブラリが OK でない	テープ ライブラリが OK 以外の状態を報告している場合にアラートを生成します。	テープ ライブラリが OK でない	N/A

表 48 状態 （続き）

名	説明	ルール	パラメーター
温度計が非アクティブ	温度計が非アクティブになった場合にアラートを生成します。	温度計が非アクティブ	N/A
温度計の過熱	デバイス上の温度計が過熱状態を示している場合にアラートを生成します。	温度計の過熱	N/A
書き込み可能なテープの待機時間が 30 分を超えた	バックアップ サーバによる書き込み可能なテープの待機時間が 30 分を超えた場合にアラートを生成します。	書き込み可能なデバイスを待機	最大未処理デバイス数：デフォルトで 0 アラート発生までの時間（分）：デフォルトで 30 分間
Xsigo ファンが公称速度の 90 %未満	Xsigo Director のファンの速度が公称速度の 90 %未満に下がった場合にアラートを生成します。	Xsigo ファン速度が予想未満	チェック比率：デフォルトは 90%。

トラブルシューティング

トラブルシューティング分析ポリシーは、環境内の問題のトラブルシューティングに役立ちます。以下の表では、これらのジョブについて説明します。

表 49 トラブルシューティング

ルール	説明	パラメーター
クライアントのネットワーク エラーによるバックアップの失敗	ネットワーク エラーが増えたときに、バックアップに失敗した場合にアラートを生成します。	該当なし
クライアント上の高い CPU 利用率によるバックアップ ジョブの失敗	コンピュータ上の CPU 使用率が 90%を超えているときに、クライアントでバックアップが失敗した場合にアラートを生成します。	プロセッサの最大使用率：デフォルトで 90%
クライアント上の高いメモリ使用率によるバックアップ ジョブの失敗	クライアント上のメモリ使用率が 90%を超えているときに、クライアントでバックアップが失敗した場合にアラートを生成します。	メモリの最大使用率：デフォルトで 90
クライアント上の高いサーバ使用率によるバックアップの失敗	バックアップ サーバ上の CPU 使用率が 90%を超えているときに、クライアントでバックアップが失敗した場合にアラートを生成します。	プロセッサの最大使用率：デフォルトで 90%
サーバ上の高いメモリ使用率によるバックアップの失敗	バックアップ サーバ上のメモリ使用率が 90%を超えているときに、バックアップに失敗した場合にアラートを生成します。	メモリの最大使用率：デフォルトで 90%

表 49 トラブルシューティング （続き）

ルール	説明	パラメーター
サーバのネットワーク エラーによるバックアップの失敗	バックアップ サーバ上のネットワーク エラーが増えたときに、バックアップに失敗した場合にアラートを生成します。	該当なし
数時間のディスク障害	ディスクの障害が 48 時間を超えて継続している場合にアラートを生成します。 Linux および Solaris に適用されます。	最大障害時間：デフォルトで 48 時間
ファイバ チャネル ポートがエラーを報告	ファイバ チャネル ポートがエラーを報告している場合にアラートを生成します。	該当なし
ファイバ チャネル ポートが x%を超えるエラーを報告	ファイバ チャネル ポートを通るすべてのフレームのうち、1%を超えるフレームでエラーが発生した場合にアラートを生成します。	最大エラー率：デフォルトで 1%
ネットワーク インタフェースがエラーを報告	ネットワーク インタフェースでエラーが発生している場合にアラートを生成します。	該当なし
ネットワーク インタフェースが x%を超えるエラーを報告	ネットワーク インタフェースを通るパケットのうち、1%を超えるパケットでエラーが発生した場合にアラートを生成します。	最大エラー率：デフォルトで 1%
テープ ドライブがエラーを報告	テープ ドライブでエラーの数が増えたときにアラートを生成します。	リカバリ可能なエラーを含む：デフォルトで False

保護ポリシー

保護ポリシーは、SLA およびデータ消失リスク レポートを定義して、バックアップ ウィンドウでバックアップを実行したかどうかを計算し、アプリケーションまたはホストがその RTO（目標復旧時間）と RPO（目標復旧時点）を満たしているかどうかを計算するために使用されます。また、保護ポリシーはアプリケーション、ホスト、デバイスのレプリケーションまたはバックアップ方法を決定します。ポリシーは、次を決定づけるルール セットで構成され、オブジェクトに割り当てられます。

- レプリケーション：コピーのタイプ、レプリケーション レベルおよびスケジュール。
- バックアップ：バックアップ レベルおよびスケジュール。

DPA レポートは、オブジェクトのデータ保護ポリシーと、実際に行われているレプリケーションまたはバックアップを比較し、ポリシーの準拠レベルを表示します。

復旧可能性チェック

復旧可能性チェックは、復旧可能性解析を構成した場合に、DPA が環境に対して実行する追加の整合性チェックです。復旧可能性チェックでは、あるユーザーの特定の要件（災害復旧など）に対してストレージおよび復旧可能性環境が構成されていることを確認します。

復旧可能性チェックが有効化されていて、DPA が不整合を検出した場合、保護ポリシー違反または復旧可能性リクエストにより作成されるエクスポージャと同様に、復旧可能性チェックはエクスポージャを作成します。復旧可能性チェックのエクスポージャは、エクスポージャ レポートに表示されます。

次の表で説明するとおり、ギャップを識別するシステム復旧可能性チェックには 3 種類あります。

表 50 復旧可能性チェック

復旧可能性チェック	説明
コンシステンシー グループ チェック	リカバリ ポイントの複数のデバイスが同じコンシステンシー グループ内に構成され、そのコンシステンシー グループが有効化されていることをチェックします。コンシステンシー グループが存在しない場合、このリカバリ ポイントに、整合性違反ギャップが生成されます。
コンシステント デバイス レプリケーション チェック	イメージを作成したときに、整合性オプションが使用されたかどうかをチェックします（該当する場合）。これはベスト プラクティス チェックです。整合性オプションが使用されていなかった場合、このリカバリ ポイントに整合性違反ギャップが生成されます。
DR ホスト可視性チェック	リカバリ ポイントのデバイスが、ディザスタリカバリ ホストにマップされ、マスクされ、このホストに認識されていることを確認します。そうではない場合、整合性違反ギャップが生成されます。

チャージバック ポリシー

チャージバック レポートでは、お客様の環境におけるバックアップ、リストアおよびデータ保護レプリケーション操作の財務的コスト分析を実行できます。DPA では、コストをバックアップ クライアントごとに計算し、そのクライアントの責任を持つビジネス ユニットにチャージ バックできます。

DPA は、データ バックアップおよびリストア用のモデルと、RecoverPoint によるストレージ データの保護とレプリケーション用の 2 つのモデルを使用して、チャージバックを計算します。DPA では、各タイプの入力に基づいてクライアントのチャージ バックが計算されます。

バックアップのチャージ バック

DPA では、バック アップされた GB あたりのコストとその他のバックアップ コストに基づいて、バックアップのチャージ バックが発生します。

［Cost Per GB Backed Up］では、次の入力情報を使用します。

- Base Size：コスト設定のベースになるベースライン バックアップのサイズ（GB）。
- Base Cost：指定したベース サイズを最大とするバックアップの総所有コスト。
- Cost of Each Additional GB：ベース サイズを超えるバックアップの 1GB あたりの追加コスト。

DPA ではチャージ バック ポリシーからの他のバックアップ コストを取得し、次の入力情報を使用します。

- Cost Per Backup：バックアップ 1 回あたりのコスト（チャージ バック ポリシーから取得）。
- Cost per GB Retained：保存されたギガバイトあたりのコスト（チャージ バック ポリシーから取得）。
- Cost Per Restores：リストア 1 回あたりのコスト（チャージ バック ポリシーから取得）。
- Cost per GB Restored：リストアされたギガバイトあたりのコスト（チャージ バック ポリシーから取得）。

- Cost Per Tape：バックアップに使用されたテープあたりのコスト（チャージ バック ポリシーから取得）。

ストレージのチャージ バック

DPA では、保存された GB あたりのコスト、レプリケートされた GB あたりのコスト、スナップ数に基づいて、ストレージのチャージ バックが発生します。

［Cost Per GB Stored］では、次の入力情報を使用します。

- Cost Based On：使用済みまたは割り当て済みのストレージのいずれかに基づいてチャージ バックを計算。
- Base Size：割り当て済みのベース ストレージ領域（GB）。
- Base Cost：ベース サイズの 1 回分の料金。
- Cost of Each Additional GB：ベース サイズ超過分の 1GB あたりの料金。

［Cost Per GB Replicated］では、次の入力情報を使用します。

- Base Size：割り当て済みのベース ストレージ領域（GB）。
- Base Cost：ベース サイズの 1 回分の料金。
- Cost of Each Additional GB：ベース サイズ超過分の 1GB あたりの料金。

［Snaps］では、次の入力情報を使用します。

- Cost Per GB：1GB あたりの料金。

チャージバック ポリシーを使用してこれらの各パラメーターの値を指定できます。DPA では、さまざまなコスト構成要素を各々加算することにより、クライアントの総所有コストを計算します。たとえば、チャージバック モデルとしてバックアップごとに 5 ドル、バックアップした 1 GB ごとに 0.20 ドル課金するなら、チャージバック ポリシーにこれらのフィールドを指定し、他のパラメータの値は指定しなくてすみます。

コスト センターにバックアップ クライアントのオブジェクトを割り当てると、DPA はチャージ バック コストをコスト センターごとに計算します。コスト センターが未割り当てのオブジェクト用にデフォルトのコスト センターがあります。

複数のチャージ バック ポリシーを作成して、クライアントまたはクライアント グループ別に異なるポリシーを割り当てることも可能です。たとえば、あるバックアップ クライアント グループにはバックアップの実行回数でチャージ バック コストを計算し、他のグループにはバックアップ プロセスで使用したテープ本数で計算する場合、チャージ バック ポリシーを 2 個作成して各クライアント グループに関連づけることができます。

ポリシーとイベント生成

解析ポリシーによって一致する条件が検出されると、DPA によりイベントが生成されます。すべてのイベントは自動的に DPA データストアのログに記録されます。Web コンソールの［**Alerts**］セクションですべてのイベントを表示できます。

ポリシーを編集して、以下を実行できます。

- メールを生成する
- スクリプトを実行する
- SNMP トラップを送信する
- Windows イベント ログにイベントを書き込む

ポリシーのルールの編集

ポリシーのすべてのルールを編集するには、［**Policies**］ > ［**Analysis Policies**］ > ［**Edit**］ > ［**Edit Policy-based actions**］に移動します。

または、アクションをルールごとに編集します。アクションをルールごとに編集するには、次のようにします。

手順

1. ［**Policies** ］ > ［ **Analysis Policies**］ > ［（ポリシーを選択して） **Edit**］の順にクリックします。
2. ［Analysis Rules］で、編集するルールの名前をハイライト表示し、［**Edit Actions**］をクリックします。
3. ［**Edit Actions**］ウィンドウで、［Rule-based actions］ラジオ ボタンが選択されていることを確認します。
1. または［Inventory］領域から、ポリシーのすべてのルールまたはルールごとに、編集または上書きします。これは、ポリシーの編集権限を持つ役割にのみ適用されます。
4. ［**Inventory**］でオブジェクトを選択します。
5. ［**Properties**］を選択します。
6. オブジェクトの［**Details**］ウィンドウ内で、［ **Policies**］タブをクリックします。
7. ［**Edit Override Settings**］をクリックします。

   ［**Edit Override Settings**］は、役割にこの操作の実行権限がある場合にのみ使用可能です。そうでない場合、オプションは［**View Settings**］です。
8. オブジェクトの［ **Override Policy Settings**］ウィンドウ内で、ルール単位レベルまたはポリシー レベルで該当する変更を行い、変更が終了したら［**OK**］をクリックします。

結果

「Data Protection Advisor online help system」には、Analysis Rule テンプレートの作成、編集、コピーに関する追加情報が記載されています。

スクリプトからアラートを生成するパラメータ

スクリプトを任意のディレクトリに置くことができます。ただし、クラスタ環境ではスクリプトを一度だけ入力する必要があるので、`<install-dir>/services/shared/ directory` を使用することをお勧めします。別の場所を選択した場合、クラスタ環境では、すべての DPA アプリケーション サーバーにスクリプトを手動でコピーする必要があります。

以下の表では、アクションを実行するために使用するスクリプトのパラメーターについて説明しています。

表 51 スクリプト フィールド パラメータ

パラメーター	説明
ノード	アラートが適用されるノードの名前。
テキスト	ルールセットの定義に基づいたテキストのエラー メッセージ。
重大度	アラートの重大度（Critical、Error、Warning、Informational）。

表 51 スクリプト フィールド パラメータ （続き）

パラメーター	説明
［Name］	このアラートをトリガーした分析の名前。
アラート ID/イベント ID	このアラートを一意的に識別する ID。
最初の発生	このアラートが最初に発生した時刻を示すタイムスタンプ。
最後の発生	このアラートが最後に発生した時刻を示すタイムスタンプ。
数	このアラートが発行された回数。
ビュー	分析が割り当てられているビューの名前。
ノード	分析が割り当てられているノードの名前。
カテゴリー	ルールのカテゴリー（可能な値：Administrative、AssetManagement、CapacityPlanning、ChangeManagement、Compliance、Configuration、DataProtection、Execution、Performance、Provisioning、Recoverability、ResourceUtilization、SLA、Status、System、Troubleshooting）。

以下の表に、アラート アクションでスクリプトに渡される引数を示します。

表 52 スクリプト アラート引数

パラメーター	説明
$1	イベント ノード
$2	イベント メッセージ
$3	イベント重要度（分析プロパティで設定）
$4	イベントを発生させた分析の名前
$5	アラート ID（このスクリプト実行で一意）
$6	イベント ID（このアラートで一意）
$7	最初の発生（タイムスタンプ）
$8	最後の発生。
$9	数。
$10	カテゴリー。
$11	アラートの説明。

注

UNIX 環境でスクリプトを実行している場合、2 桁のパラメーターを中括弧で囲む {xx} 必要があります たとえば、`$ {11}`。

ルール テンプレート

ルールとは、条件が満たされたかどうか、アラートを生成するかどうかを判定するために DPA Analysis Engine が使用する一連の指示のことです。たとえば、ファイル システムの限界ルールには、将来のある時点でファイル システムが特定の閾値を超えるかどうかを判断するための一連のルールが含まれています。

解析ジョブは、ルールを使用することで、DPA データベース内の情報に基づいて解析やアラートの生成を実行します。DPA をインストールすると、多数の定義済みルールがインストールされます。これらを使用して、環境で発生する可能性のある主な問題を監視できます。これらのルールは、解析ポリシーを実装するベースとして使用できます。DPA には、まったく新規のルールを作成するのに使用できるルール エディタが用意されています。

［ルール テンプレート］という用語は、ルールの定義とルール インスタンスを区別する場合に使用します。ルール テンプレートはルールのロジックを定義します。ルール テンプレートが解析ポリシーに追加されると、Analysis Engine が実行するルール インスタンス（つまり、ルール）になります。また、ルール テンプレートがポリシーに追加されると、ユーザーは任意のパラメーターの値を指定できます。これにより、ルールを異なるポリシーで再利用できます。

たとえば以下のようなものです。

Tier 1 のポリシーでは、使用ディスク領域が 80%に達するとアラートが生成される可能性があります。Tier 2 のポリシーでは、使用ディスク領域が 90%に達するとアラートが生成される可能性があります。これは、使用率に関するパラメーターを使用する同じルール テンプレートで処理できます。

ポリシーの適用

ポリシーは、グループまたはオブジェクトに直接適用できます。オブジェクトに直接適用されたポリシーが常に優先されます。ポリシーをグループ レベルで設定した場合、自分のポリシーを持たないグループ内のオブジェクトはグループのポリシーを継承します。最上位のグループ レベルにあるポリシーを適用するのが良いでしょう。ポリシーは Smart Group には適用できません。

オブジェクトがあるグループから別のグループへ移動する場合、最近適用されたポリシーが実装されます。たとえば、オブジェクトをグループ A からグループ B に移動する場合、オブジェクトはグループ B のポリシーを継承します。

管理者または［Edit Node］権限のある任意のユーザーは、ポリシーをグループまたはオブジェクトに適用できます。

第 5 章

DPA のアンインストール

この章は、次のセクションで構成されています。

- ソフトウェアのアンインストール 242
- エージェントのみのアンインストール 242

ソフトウェアのアンインストール

このセクションでは、UNIX/Linux 環境および Windows 環境で DPA をアンインストールする方法について説明します。

手順

1. 次のコマンドを実行します。

   <DPA_install_directory>/_uninstall/Uninstall_Data_Protection_Advisor

   サイレント アンインストールを実行する場合は、コマンドに`-i silent` を追加します。アンインストーラーから入力は要求されません。

結果

DPA データストアをアンインストールするとき、アンインストーラーにより製品インストール時にインストールされた機能が削除され、データベースも削除されるという警告が表示されます。

サイレント コマンド ラインを使用したアンインストール

- UNIX/Linux マシンでは、コマンド シェルを起動し、_uninstall ディレクトリに移動して、次のコマンドを入力します。**./Uninstall_Data_Protection_Advisor -i silent**
- Windows マシンでは、コマンド ラインから次のコマンドを入力します。
  Uninstall_Data_Protection_Advisor.exe -i silent

Windows のユーザー インタフェースでのアンインストール

手順

1. ［スタート］ > ［コントロール パネル］ > ［プログラムと機能］の順に選択します。
2. インストールされているアプリケーションのリストから、［**Data Protection Advisor**］をアンインストールします。

エージェントのみのアンインストール

DPA アプリケーション サーバーまたはデータストア サーバーからエージェントのみをアンインストールすることはできません。

DPA エージェントをアップグレードする場合は、既存の DPA アプリケーション サーバーまたはデータストア サーバーでエージェントのみをアップグレードします。アップグレード（66 ページ）に、アップグレードの実行に関する情報を示します。

第 6 章

トラブルシューティング

この章は、次のセクションで構成されています。

- インストールのトラブルシューティング 244
- ログ ファイル 245
- データ コレクションのトラブルシューティング 248
- レプリケーション解析用クライアント/ストレージ検出に関するトラブルシューティング 249
- レポートの出力失敗に関するトラブルシューティング 255
- レポートの生成と発行に関する問題のトラブルシューティング 255
- システム クロックの同期 255

インストールのトラブルシューティング

DPA サーバーのパスワードを変更した後、DPA エージェントが再起動または登録されない

インストール時に DPA サーバーのパスワードを変更した後、DPA エージェントが再起動または登録されない場合は、DPA サーバーでエージェントのパスワードが変更されたが、DPA エージェントのパスワードがそれと一致するように変更されていないことが原因である可能性があります。

DPA エージェントが再起動または登録されるようにするには、エージェントのパスワードを、DPA サーバーで設定されたものと同じ値に設定します。詳細については、DPA エージェントのインストール（53 ページ）を参照してください。

インストール後に Linux で発生する DPA データストアの起動の障害

特定の状況では、DPA データストアを実行するシステムのカーネル設定をデータストア用に調整して、正しく起動されるようにする必要があります。

データストアの起動が失敗し、DPA ログ ファイル中のエラーが共有メモリー セグメントを示している場合、システム仕様に従って、次のファイルで指定される値の調整が必要な場合があります。

- Linux：**/etc/sysctl.conf** の SHMMAX と SHMMIN のチューニング値を調べます。

Windows Server 2012 での DPA Web コンソールの起動の失敗

Windows Server 2012 で DPA Web コンソールの起動が失敗した場合、次の項目を確認します。

- IE ESC（Internet Explorer Enhanced Security Configuration）によって、DPA Web コンソールが起動されなくなっている。［Continue to prompt when website content is blocked］オプションをオフにしてブロックの通知を停止しないでください。DPA が［Starting services. Please wait］の状態から動かなくなるためです。
  この回避策は、IE ESC を無効化することです。
- Windows Server 2012 の Internet Explorer が Flash をサポートしていない。この回避策は、Windows Server 2012 のデスクトップ操作性を有効化することです。

インストール後のメモリーの調整

DPA アプリケーションとデータストア サービスが最初からインストールされている場合、システム RAM に基づいて自動的にメモリー パラメーターがチューニングされます。ホストにインストールされた RAM の量を後で増減する場合、DPA メモリー パラメーターが正しく調整されるように `tune` コマンドを実行する必要があります。

`tune` コマンドを実行するときは、ホストにインストールされている RAM の容量を指定する必要があります。たとえば、アプリケーション サーバーのメモリーが 64 GB に変更され、データストアのメモリーは 32 GB に変更された場合は、それぞれ以下のコマンドを実行します。

- アプリケーション サーバー上：**`dpa app tune 64 GB`**
- データストア サーバー上：**`dpa ds 32 GB`**

DPA は、コマンドで指定された分のメモリー容量を使用するよう自動的に構成されます。

アップグレード中のエラー メッセージ

アップグレード プロセス中にエラーが発生した場合、DPA サーバーが停止します。これは以下の条件下で発生する可能性があります。

- SQL アップグレード スクリプトのエラー
  - 結果：サーバーが停止し、続行できません。
  - 推奨される対処：EMC テクニカル サポートに連絡してください。
- システム メタデータ アップグレードのエラー（例：システム レポート、ルール テンプレート）
  - 結果：サーバーは停止しますが、アップグレードの続行を選択できます。
  - 推奨される対処：このメッセージを無視して DPA サーバーのアップグレードを続行できます。ただし、DPA システムが不安定になる可能性があります。サーバーのアップグレードを中止した場合は、EMC テクニカル サポートに連絡してください。
- カスタム データ アップグレードのエラー（例：カスタム解析ルール）
  - 結果：問題を示すエラー メッセージが表示されます。

```
Suggested action: You can disregard this message and continue
with the DPA server upgrade. However, you should expect the
custom rule that failed to upgrade not to work. An error is
recorded in the log file.
```

ログ ファイル

ログ ファイルにより、問題をトラブルシューティングする際の重要な情報が提供されます。

注

次のセクションでは、標準的な DPA インストールでのログ ファイルの場所について説明します。デフォルトのインストール ディレクトリを変更した場合は、ログ ディレクトリの場所は異なります。

デフォルトでは、警告メッセージ、エラー メッセージ、参考メッセージがログに含まれます。これらの情報では、複雑な問題をトラブルシューティングするときに十分な情報が提供されません。

デフォルト ログの詳細レベルの変更

［**Admin**］ > ［**System**］ > ［**Configure System Settings**］の順にクリックします。

インストール ログ ファイルの表示

インストール中に、ファイル `Data_Protection_Advisor_Install_[two-digit date]_[two-digit month]__[year]_[two-digit hour]_[two-digit minute]_[two-digit seconds].log` が生成され、ここにすべてのログ メッセージが含まれます。インストール成功の場合、このファイルはインストール ディレクトリ（ `/opt/emc/dpa/_install` など）にあります。UNIX プラットフォームへのインストールが失敗した場合、ファイルはシステム ドライブのルートにあります。Windows プラットフォームでは、ファイルはデスクトップにあります。

サーバー ログ ファイルの表示

DPA はサーバー ログ ファイルを次の場所に生成します。

- UNIX： `/opt/emc/dpa/services/logs`
- Windows：`C:\Program Files\EMC\Data Protection Advisor \services\logs`

サーバー ログ ファイル

次のログ ファイルのデフォルトの場所は、`<install_dir>\services\logs\` です。

- `Server.log`：DPA アプリケーション サーバーから生成されたすべてのログ コメントが含まれる
- `actions.log`：Analysis Engine の成功したアクションのみが含まれる
- `reportengine.log`：DPA レポート エンジンから生成されたすべてのログ コメントが含まれる
- `listener.log`：エージェント データを受け取って処理するサーバーに関連する、DPA リスナーから生成されたすべてのログ コメントが含まれる

エージェント ログ ファイルの表示

エージェント ログ ファイルは、次の場所に生成されます。

- UNIX： `/opt/emc/dpa/agent/logs`
- Windows： `C:\Program Files\EMC\Data Protection Advisor\agent \log\agent.log`

ログ ファイルの管理

ログ ファイルがその最大サイズに達し、ログ ファイルの最大数がログ ファイル ディレクトリに設定されている場合、DPA ではそのプロセスの最も古いログ ファイルが削除され、新しいログ ファイルが作成されます。ログ ファイルの最大ログ ファイル サイズと最大数を変更できます。また、必要に応じて、ログ ファイルの場所を変更することもできます。

Windows を実行する仮想マシンにおける代替のログ ローテーションの有効化

Windows を実行する仮想マシンにおいて、ファイルのロックが原因でログがローテーションされない既知の問題があります。これを修正するには、代替のログ ローテーション手法を有効化します。これによりログの使用方法が変わり、 `agent.log` ファイルの代わりに最も数が大きいログが最新になります。これは、DPA-24288 に関連します。

手順

1. 次のストリング レジストリを作成します。

   `HKLM\SOFTWARE\EMC\DPA\Agent\ALTLOGROTATE`

2. 値を **true** に設定します。

インストーラー ログ ファイルの誤りがあるメモリー データ

インストール ログ ファイルの一番上に示されている［Free Memory］と［Total Memory］のデータには誤りがあります。正しい［Free Memory］と［Total Memory］のデータはログ ファイルの下の方、STDERR ENTRIES の下にあります。

Executing IAUpdatePostgesconfFile: [INFO] の下に表示される［Corrected Total Memory］データは、DPA データストア サービスで使用されるデータを表します。

DPA Web コンソールを使用した、デバッグ モードでの DPA エージェント リクエストの実行

デバッグ モードでの DPA エージェント リクエスト（別名［modtest］）はサポート ツールです。データ コレクションのデフォルト値で問題が発生する場合は、EMC テクニカル サポートのエンジニアにより、DPA Web コンソールからエージェント リクエストのデバッグ モードを実行するよう指示される場合があります。DPA エージェント リクエストをデバッグ モードで実行し、DPA Web コンソールから直接 zip ファイルをダウンロードできます。この際、DPA サーバーで zip ファイルを取得し、解析用に送信する必要はありません。エージェント リクエストのデバッグ モードで選択したリクエストが実行され、デバッグ ログ レベルで出力とログ メッセージが取得され、デフォルトでそのレポート xml が zip ファイルとして <DPA_HOME>\services\shared\modtests に格納されます。ここで、<DPA_HOME>は DPA のインストール場所です。

DPA Web コンソールを使用して、DPA エージェント リクエストをデバッグ モードで実行する場合は、次の点を考慮します。

- コレクション リクエストが無効な場合は、テストを実行できません。
- オブジェクトでコレクション リクエストを適用できない場合は、テストを実行できません。
- Google Chrome を実行している場合：URL のデフォルトのセキュリティ設定を低に変更する必要があります。
  ［**Trusted Sites**］に移動し、URL を［Trusted Sites］リストに追加して、セキュリティを［**low**］に設定します。

手順

1. Web コンソールで、［**Inventory** ］ > ［ **Object Library**］を選択します。
2. ［Object Library］で、［**All hosts**］の下の DPA サーバーを選択します。
3. ホスト詳細ウィンドウで、［**Data Collection**］ > ［タブ］を選択します。
4. ［**Data Collection**］で、［Request］を選択します。
5. ［ **Run**］を右クリックし、［ **Run in Debug**］を選択します。
6. ［**Run in Debug - host/status**］ウィンドウで、認証情報とデータ オプションを選択します。
7. テストが実行されていることを確認して、表示されるダイアログ ボックスで［**Close**］をクリックします。
8. ［**History**］をクリックして収集されたテストを表示します。オレンジ色で強調表示される行は、デバッグ モードでの DPA エージェント リクエストからの結果を示します。
9. テスト結果をクリックします。［Windows Security Login］が表示されたら、DPA サーバーの認証情報を入力して［**OK**］をクリックします。
10. 正常に収集されたテストにアクセスするには、<DPA_HOME>\services\shared\modtests に移動します。

リモート Web ブラウザーを表示している場合は、リクエストの履歴を表示してオレンジ色の modtest 行をクリックして、ご使用のマシン（ブラウザーがインストールされているマシン）に zip を転送するためのリンクをダウンロードできます。

modtest のデフォルトの削除スケジュール

DPA は、毎週日曜日午前 4 時に DPA サーバーから modtest ファイルを削除します。DPA は、7 日前より古いすべてのテスト結果ファイルを削除します。このスケジュールは構成できません。

Generate Support Bundle

［Generate Support Bundle］オプションはサポート ツールです。サポート バンドルの生成（94 ページ） に詳細が記載されています。

データ コレクションのトラブルシューティング

このセクションでは、データ収集の際に発生した問題を診断するためのステップについて説明します。次のシナリオについて考えてみましょう。

- DPA が正常にインストールされました。
- ［Discovery Wizard］が正常に実行され、監視するオブジェクトが作成されました。
- リクエストがオブジェクトに割り当てられ、エージェントが再ロードされました。
- エージェントがデータを収集するために十分な時間（15 分間）がすでに経過しています。
- 適切なレポートが実行されました。このオブジェクトに対するデータは存在するはずですが、データは返されていません。

データ コレクションのトラブルシューティング： 最初のアクション

Agent Errors レポートにより返されたエラーを確認し、可能であれば、エラーを修正します（たとえば、認証の問題を解決します）。

手順

1. レポートに対して選択されている期間が正しことを確認します。
2. オブジェクトに正しいリクエストが割り当てられていることを確認します。

   ［**Inventory**］ > ［**Object Library**］ > ［(ノードを選択)］ > ［**Data Collection**］の順に選択します。リクエストが正しく構成されていることを確認します。
3. リクエストを再実行します。

データ コレクションのトラブルシューティング： 2 番目のアクション

手順

1. 解決できるエージェント エラーが報告されない場合は、［**Admin**］ > ［**System**］の順に選択し、［**Configure System Settings**］をクリックして、データ コレクション エージェントの設定を確認します。
2. エージェントがアクティブであることをステータスが示している場合は、エージェントがインストールされているオペレーティング システムで、このプロセスがアクティブであることを確認します。
3. Web コンソールで Agent ログ レポート、Agent Status レポート、Data Collection History レポートの順に実行します。

4. レポートを再実行します。引き続きレポートでデータが表示されない場合は、エージェント ログを開いて問題を探します。たとえば、エージェントのインストール中に不正な値が入力されていないかどうかを確認します。ログ ファイル（245 ページ） でログ ファイルの表示方法について説明しています。

EMC サポートへの送信用ログ ファイルの準備

手順

1. ログ ファイル（245 ページ）の説明に従って、［System Settings］で、プロセスのログ レベルを［**Debug**］に設定します。
2. エージェント プロセスを停止します。
3. ログ ファイルが保存されているディレクトリに移動します。そのプロセスに対する既存のログ ファイルをすべて名前変更するか、または削除します。
4. プロセスを再起動します。

   エージェントを再起動すると、このエージェントに割り当てられたリクエストがすべて再ロードされ、データ コレクション ルーチンが開始されます。これにより、すべてのリクエストが確実に試行されます。新しいログ ファイルを開始すると、不必要に長いログ ファイルから問題を検索する必要がなくなります。

5. ［**Inventory**］ > ［**Object Library**］ > ［(ノードを選択)］ > ［**Data Collection**］の順に選択し、［**History**］を選択します。

   または、Agent History レポートを生成します。

6. リクエストを再実行し、データが収集されないことを確認します。
7. ［ **System Settings**］ > ［**Log Level**］の順に選択し、［**Info**］に設定します。
8. EMC サポートに送信するために、ログのコピーを作成します。

レプリケーション解析用クライアント/ストレージ検出に関するトラブルシューティング

このセクションでは、レプリケーション解析用に VNX Block/CLARiX または Symmetrix ストレージ アレイを構成しようとしたときに発生した問題を診断するためのステップについて説明します。次のシナリオを前提にしています。

- DPA が正常にインストールされました。
- DPA サーバーおよびストレージ アレイ ホストは、「「Data Protection Advisor Software Compatibility Guide」」で指定されている要件を満たしています。
- Solutions Enabler は正常にインストールされています。

リモート実行を使用したクライアント/ストレージ検出

以下の表では、クライアントまたはストレージをリモートで （つまり DPA エージェントを使用せずに）検出しようとしたときに発生する可能性のある問題とそのソリューションについて説明します。

表 53 クライアント/ストレージ検出の問題とソリューション

問題	解決策
クライアント検出の失敗。認証が定義されていないか、ログインできない。	• DPA で認証情報を作成（[Admin] > [System] > [Manage Credentials]）し、クライアントに割り当てます。 • 認証情報で指定されたユーザー名およびパスワードでクライアントに接続できることをチェックします。 • 接続に su または sudo が不要であることを確認します。必要な場合は、認証情報で正しいパラメーターが指定されていることを確認します。
クライアント検出の失敗。RPC を使用してクライアントに接続できなかった、または指定されたログイン セッションが存在しない。	• 認証情報で指定されたユーザー名およびパスワードでクライアントに接続できることをチェックします。 • ドメイン名とあわせてユーザー名も指定したことを確認します。リモート コンピューターの場合は `<domain>\<username >`、ローカル コンピューターの場合は<computer name>\<username>です。ほとんどの場合、`localhost\<username>`を使用できます。 • admin 共有（\\hostname\Admin$）を使用して、DPA サーバーからホストにアクセスできるかどうかをチェックします。 • 前記のアクションをすべて試した後でエラーが存在する場合は、DPA サーバー サービスの［Log on as］の値を、ローカル システムから、管理者権限を持つ他のユーザーに変更します。ローカル管理者も設定できます。
クライアント検出の失敗。RPC を使用してクライアントに接続できなかった。ネットワーク パスが見つからなかった。	• クライアントの名前、IP、エイリアスが正しく定義されているか、DPA サーバーからアクセス可能かをチェックします。 • admin 共有（ `\\hostname\Admin$` ）を使用して DPA サーバーからホストにアクセスできるかどうかチェックします。 共有にアクセスできない場合は、ファイアウォールによりブロックされていないかチェックします。
クライアント検出の失敗。ユーザーがデバイスのマッピング情報を取得できる十分な権限を持っていない。	• リモートの実行権限に関して、システム要件に従います。 • ユーザーの認証情報に管理者権限を割り当てます。 • クライアントに接続しているユーザーが、パス/var/tmp に対して書き込みおよび実行権限を持っていることをチェックします。（UNIX）

表 53 クライアント/ストレージ検出の問題とソリューション （続き）

問題	解決策
クライアント検出の失敗。SCP を使用してクライアントに検出用ファイルを送信できなかった。 または FTP を使用してクライアントに検出用ファイルを送信できなかった。	`/var/tmp` の空きディスク領域をチェックします。
クライアント検出の失敗。エラー（977）。重複した IO 操作が進行中。	ホストにアンチウイルス ソフトウェアがインストールされていないことを確認します。アンチウイルス ソフトウェアによって **irxsvs.exe** の操作がブロックされる場合があります。アンチウイルス ソフトウェアで **irxsvs.exe** ファイルを許可してアンチウイルスによるブロックを無効化します。
次のエラーのためクライアント検出が失敗する。<client_name> irx errMsg: Unable to connect host:<client_name> with user:<domain> \<username> using RPC irx output: Error (1203): No network provider accepted the given network path.	次のサービスが実行中であることを確認します：サーバー、コンピューター ブラウザ、ワークステーション。
sudo の使用時に、Host Config リクエストから AIX ホストに関するボリューム グループ情報が返されず、次のメッセージが表示されることがある。SymMapVgShow exited with code 161 (SYMAPI_C_VG_NOT_AVAILABLE) SessionId: 0 - for VG:<vg_name> with type: 2(AIX LVM) VolumeGroup information will not be parsed.	これは、sudo を使用するように認証情報が構成されている場合にのみ発生します。sudoers ファイルに次の行を追加します。Defaults env_keep += "ODMDIR"

エージェントを使用したクライアント/ストレージの検出

次の表に、DPA エージェントを使用してクライアントやストレージを検出する際に発生する可能性のある問題とソリューションを示します。

表 54 エージェントを使用したクライアント/ストレージの検出に関する問題とソリューション

問題	解決策
Client Discovery リクエストで、インストール済みのエージェントを使用する代わりにリモート実行が使用されている。	ホストにエージェントがインストールされていることを確認します。 DPA サーバーが、エージェント用のコントローラとして定義されていることを確認します。 エージェント サービスを再起動します。

一般的なクライアント/ストレージの検出

次の表に、DPA からクライアントやストレージを検出する際に発生する可能性のある一般的な問題とソリューションを示します。

表 55 一般的なクライアント/ストレージの検出に関する問題とソリューション

問題	解決策
クライアント検出が終了し、次の警告が表示された。 Failed to discover application storage objects for application <application_name> on client <client_name>.	• アプリケーションが実行されており、接続可能かどうかチェックします。 • DPA 認証情報で構成されているユーザーに、アプリケーションのシステム データをクエリーできる十分な権限があるかどうかチェックします。
クライアント検出の失敗。どの IP にも接続できない。	• Windows Proxy Collector からのポート 25011 とポート 135 がファイアウォールによってブロックされていないかを確認します。
クライアント検出が終了し、次の警告が表示された。 Home directory was not found for application.	［**Admin**］ > ［**System**］ > ［**Manage Credentials**］の順に選択します。 ［**Edit**］をクリックして認証情報を編集します。
サポートされていないタイプのファイル システム <filesystem_name>が検出された。	DPA はこのタイプのファイル システムをサポートしません。 次回のクライアント検出でこの警告を回避するために、このファイル システムに関する検出を無視できます。 DPA では、このファイル システムのリカバリ データは表示されません。
クライアント検出が失敗し、次のエラーが表示された。 Please verify that you have enough disk space and write permission. または Failed to unpack file on client <client_name>.	システム要件に従う十分なディスク領域が、ホストのルート ファイルシステムにあることを確認します。
クライアント検出が終了し、次の警告が表示された。 Can't find or no permission to execute file <home_dir>.	• 検出された<home_dir>がクライアントに存在するかどうかを確認します。 • 検出されたホーム ディレクトリ内のファイル sqlplus に、DPA で実行できる十分な権限があるかどうか確認します。
クライアント検出が終了し、次のエラーが表示された。 Timeout waiting for agent response on client <client_name>.	1. DPA で、［**Admin** ］ > ［**System**］ > ［**Configure System Settings**］の順に選択して［**Select Server**］をクリックします。 2. パラメータ Timeout(s)をデフォルトの 120 からより大きな値に変更します。 または、 DPA サーバーで 2 個のネットワーク カードが有効になっているかどうか、クライアントからこの両方にアクセスできるかどうかをチェックします。クライアントからこれ

表 55 一般的なクライアント/ストレージの検出に関する問題とソリューション （続き）

問題	解決策
	らのカードのいずれかにアクセスできない場合は、クライアントがアクセスできないネットワーク カードを無効化します。
ECC 6.1 への接続中に、クライアント検出が終了し次のエラーが表示された。 Error Import Clients for w2k3-96-52.dm1nprlab.com finished with errors. Check previous error messages for further information. Unable to logon (Connection refused).	次のコマンドを含むバッチ ファイルを実行します。 `%ECC_INSTALL_ROOT%\tools\JRE\Nt\latest\bin\java -cp %ECC_INSTALL_ROOT%\ECCAPIServer\class;%ECC_INSTALL_ROOT%\ECCAPIServer\ecc_inf\exec\eccapiclient.jar; com.emc.ecc.eccapi.client.util.EccApiPopulateRandomPassword ApiClient` 追加の `classpath` パラメーターは、ECC classes ディレクトリ内からこのコマンドを使用しなかった場合に限り、必要となります。
クライアント検出により、ESX 4.1 上の VFMS で LUN が解決されない。 仮想デバイスを、それらが常駐するリモート ストレージと関連づけようとしたときに、仮想マシンのホスト ESX が VM（DNS 構成）の名前を解決できない場合、関連づけは失敗して仮想デバイスはローカル デバイスとして表示される。	ESX 上で適切に DNS を構成するか、ESX ホスト ファイルに VM 名と IP を追加します。
CLARiX 情報リクエストのインポートが失敗して次のエラー メッセージが表示される。 "An error occurred while data was being loaded from a Clariion ClarEventGet exited with code 3593 (SYMAPI_C_CLARIION_LOAD_ERROR) "	この CLARiX の SE ホストで次の `SYMCLI` コマンドを実行します。 symcfg sync -clar

Host configuration request exceeds 60 minutes	`services/remotex/deploy/<platform>/apolloreagent.ini` ファイルで、`TIMEOUT` の値を 3600 以上（7200 など）に設定します。ここで、<platform>はリクエストが超過したホストを示します（DPA サーバーではありません）。
	`<REARGS>`
	`<LOGFILE>apolloreagent.log</LOGFILE>`
	`<LOGLEVEL>Info</LOGLEVEL>`
	`<WORKINGDIR>.</WORKINGDIR>`
	`<TIMEOUT>7200</TIMEOUT>`
	`</REARGS>`

間違ったリカバリ ポイント時間の同期

DPA サーバーと監視対象のストレージ アレイ間に時差がある場合は、予定された時間と一致しない時間とあわせて、リカバリ ポイントが表示される場合があります。たとえば、システム管理者が 2:00 でリカバリ ポイントを開始したにもかかわらず、DPA ではリカバリ ポイントは 4:00 と表示されます。

検出リクエストには、時差を補正する Time Offset オプションがあり、リカバリ ポイントが同じ時間で表示されるようにできます。ユーザーは、DPA サーバーとストレージ アレイ ホストとの正確なオフセット値を計算する必要があります。

次の手順では、Solutions Enabler ホストは、SYMAPI/CLARAPI Engine Discovery リクエストが割り当てられた DPA ホストを参照します。

タイム オフセットは秒単位で計算されます。

VNX/CLARiX での間違ったリカバリ ポイント時間の同期

VNX/CLARiX と DPA サーバー間のタイム オフセットを計算するには、次の手順を実行します。

手順

1. navicli コマンド `getsptime` を使用して、VNX/CLARiX の時間をクエリーします。
2. 同時に Solutions Enabler ホストの時間もクエリーします。
3. Solutions Enabler ホストの時間と DPA サーバーの時間が同じ（タイム ゾーンの違いがない）場合は、次のように計算します。

   タイム オフセット = Solutions Enabler ホストの時間 - VNX/CLARiX の時間。

4. それ以外の場合で、Solutions Enabler ホストの時間と DPA サーバーの時間にも時差がある場合は、次のように計算します。

   タイム オフセット = （DPA サーバーの時間 - Solutions Enabler ホストの時間） - VNX/CLARiX の時間。

5. リクエストのタイム オフセットを設定します。詳細については、タイム オフセットの構成（255 ページ）を参照してください。

Symmetrix での間違ったリカバリ ポイント時間の同期

Symmetrix と DPA サーバー間のタイム オフセットを計算するには、次の手順を実行します。

手順

1. DPA サーバーの時間をクエリーします。
2. 同時に Solutions Enabler ホストの時間もクエリーします。
3. Solutions Enabler ホストの時間と DPA サーバーの時間が異なる場合は、次のように計算します。

   タイム オフセット = DPA サーバーの時間 - Solutions Enabler ホストの時間。

4. それ以外の場合は、Symmetrix にタイム オフセットを設定する必要はありません。
5. リクエストのタイム オフセットを設定します。詳細については、タイム オフセットの構成（255 ページ）を参照してください。

タイム オフセットの構成

タイム オフセットを計算したら、リクエストに値を設定します。タイム オフセット値を設定するには、次の手順を実行します。

手順

1. ［**Inventory**］>［**Object Library**］>［(**Solutions Enabler** ホストを選択)］>［**Data Collection**］の順に選択します。
2. 関連するリクエストを選択し、［**Edit**］をクリックします。
3. 計算したタイム オフセットの［**Client-server Time Difference**］(秒単位または分単位）を設定します。
4. ［適用］をクリックします。

レポートの出力失敗に関するトラブルシューティング

レポートを保存した後にメッセージ `Please wait while generating report` により異常停止し、かつ Internet Explorer を使用している場合、XMLHTTP オプションを有効化していないことが原因である可能性があります。XMLHTTP オプションを有効化するには、次のようにします。

これは、DCE-1546 が関連します。

手順

1. ［**Internet Options**］ > ［**Advanced**］の順にクリックします。
2. ［**Security**］にスクロールして［**Enable Native XMLHTTP Support**］を選択し、［**OK**］をクリックします。

レポートの生成と発行に関する問題のトラブルシューティング

スケジュール設定されたレポートの生成に失敗した、または正しく生成されたが発行に失敗した場合は、次のアクションを実行します。

- カスタム レポートの場合は、［**Run Reports**］領域でレポート テンプレートが正しく設計されていることを確認します。
- レポート テンプレートが［**Run Reports**］領域で正しく実行されることを確認します。
- レポート テンプレートが適切な形式で正しく保存（エクスポート）されていることを確認します。
- スケジュール設定されたレポートについて、`server.log` にあるエラー/警告を確認します。

これらのアクションで問題が解決しない場合は、EMC テクニカル サポートに問い合わせます。

システム クロックの同期

ユーザー認証プロセスの一環として、DPA は、クライアント マシンとサーバーのシステム クロック時間の差が 1 分未満であることを前提にしています。クロック時間が同期されていない場合、次のエラーメッセージが表示されます。

```
User Authentication failed due to the times on the client and
server not matching. Ensure that the times are synchronized.
```

この問題を解決するには、クライアントとサーバーのシステム クロック時間が同期されていることを確認します。

NTP を使用して、DPA サーバーとすべての DPA エージェント ホストを同期することも推奨します。このことは正確なデータ コレクションのためには不可欠です。