Dell Data Guardian

Windows、Mac、モバイル、およびウェブ管理者ガイド v2.0

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

Windows、Mac、モバイル、およびウェブ管理者ガイド

2018 - 08

Rev. A01

目次

1

はじめに

すべてのポリシー情報とその説明は AdminHelp で参照できます。

作業を開始する前に

1 クライアントを導入する前に、Dell Server をインストールしてください。次に示すように、正しいガイドを探し、記載されている手順に従った後、このガイドに戻ります。

- *Security Management Server Installation and Migration Guide*（Security Management Server インストールおよびマイグレーションガイド）
- *Security Management Server Virtual Quick Start Guide and Installation Guide*（Security Management Server Virtual クイックスタートガイド / インストールガイド）
- 希望のポリシーを設定しているかを確認します。**?** のマークから AdminHelp を参照します。画面の右上にあります。AdminHelp はポリシーの設定および変更、Dell Server でのオプションを理解するのに役立つよう設計されたページヘルプです。

2 本書の「要件」の章をすべて読んでください。

3 ユーザーにクライアントを導入します。

Dell ProSupport へのお問い合わせ

デル製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 4310039）にご連絡ください。

さらに、デル製品のオンラインサポートも dell.com/support からご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスタグまたはエクスプレスサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の各国の電話番号を記載したページを参照してください。

2

要件

Dell Server

Windows、Mac、モバイル用の Data Guardian には Security Management Server または Security Management Server Virtual の v9.6 以上が必要です。Data Guardian ウェブクライアントには Security Management Server または Security Management Server Virtual の v9.8 以上が必要です。ここでは、特定のバージョンに言及する必要（Security Management Server Virtual を使用する場合は手順が異なる場合など）がない限り、両方のサーバとも Dell Server と呼びます。

Data Guardian for Windows

- 導入中は、IT ベストプラクティスに従う必要があります。これには、初期テスト向けの管理されたテスト環境や、ユーザーへの時間差導入が含まれますが、それらに限定されるものではありません。
- インストール、アップグレード、アンインストールを実行するユーザーアカウントは、ローカルまたはドメイン管理者ユーザーである必要があります。これは、Microsoft SMS または Dell KACE などの導入ツールによって一時的に割り当てることができます。昇格された権限を持つ非管理者ユーザーはサポートされません。
- インストールまたはアンインストールを開始する前に、重要なデータをすべてバックアップします。
- インストール中は、外付け（USB）ドライブの挿入や取り外しを含め、コンピュータに変更を加えないでください。
- Data Guardian は、Microsoft Office 2016 の特定のバージョンならびに Microsoft Office 365 Business および Business Premium でサポートされます。Office 365 Business Essentials ではサポートされていません。
- クラウドの暗号化の場合、コンピュータでは、1 つ（文字値）の割り当て可能なディスクドライブを利用できる必要があります。
- ターゲットデバイスが https://yoursecurityservername.domain.com:8443/cloudweb/register および https://yoursecurityservername.domain.com:8443/cloudweb にアクセスできることを確認します。
- Data Guardian の導入前は、ターゲットデバイスでクラウドストレージのアカウントセットアップが行われていない状態にしておくことが最善です。

  ユーザーが既存のアカウントを引き続き使用する場合は、Data Guardian をインストールする前に、暗号化しないままにするファイルが同期クライアントから移動されていることを確認する必要があります。
- ユーザーは、クライアントをインストールした後に、コンピュータを再起動する必要があります。
- Data Guardian は、同期クライアントの動作と競合しません。したがって、管理者とユーザーは、Data Guardian を導入する前に、これらのアプリケーションの動作を理解しておく必要があります。詳細については、Box のサポート（https://support.box.com/home）、Dropbox のサポート（https://www.dropbox.com/help）、または OneDrive のサポート（http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other）を参照してください。
- 保護された Office ドキュメントは、Data Guardian のコンパニオンソリューションである Mozy、ならびに他のクラウド製品、電子メール製品、および NFS ストレージ製品でサポートされます。
- Office 2010 を実行している場合：ポリシーが Office ドキュメントおよびマクロ有効ドキュメントを保護するよう設定されている場合、Office 2010 Service Pack 1 以上（v14.0.6029 以上）が必要です。Microsoft Office 2010 スイートにサービスパックが適用されているかどうかを確認するには、https://support.microsoft.com/en-us/kb/2121559 を参照してください。このアップデートを適用しないと、保護されたドキュメントにアクセスすることはできません。新しい Office ドキュメントは、スイープ機能が有効ではない限り、ポリシーにかかわらず保護されません。次のスイープが、Office ドキュメントを保護されたファイルに変換しますが、ユーザーは、Office のサポートされるバージョンがないとそれらのファイルにアクセスできません。
- Dell Encryption は必須ではありませんが、使用する場合は、Encryption クライアントを v8.12 以降にする必要があります。
- Data Guardian は、Windows システムの復元ツールまたは Windows インサイダープレビューをサポートしていません。
- Microsoft のフォルダリダイレクトは、Data Guardian ではサポートされません。
- IPv6 はクラウド暗号化ではサポートされません。
- 最新のマニュアルや技術アドバイザリーについて、dell.com/support を定期的に確認してください。

前提条件

まだインストールされていない場合、インストーラは Microsoft Visual C++ 2015 再頒布可能パッケージ（x86 および x64）をインストールします。

メモ:
Windows 7 および Windows 8.1 の場合、Windows Update でコンピュータが最新の状態になっている必要があります。詳細については、https://support.microsoft.com/ja-jp/help/2919355 および https://support.microsoft.com/ja-jp/help/2999226 を参照してください。

Data Guardian には、Microsoft .Net 4.5.2 以降が必要です。デルの工場から出荷されるすべてのコンピュータには、.Net 4.5.2 が事前インストールされています。ただし、Dell ハードウェア上にインストールしていない、または旧型の Dell ハードウェア上で Data Guardian をアップグレードしている場合は、インストール / アップグレード失敗を防ぐため、Data Guardian をインストールする前に、インストールされている .Net のバージョンを検証し、必要に応じてバージョンをアップデートするようにしてください。インストールされている .NET のバージョンを検証するには、インストール対象のコンピュータで http://msdn.microsoft.com/ja-jp/library/hh925568(v=vs.110).aspx に記載されている手順を実行します。Microsoft .Net Framework 4.5.2 をインストールするには、https://www.microsoft.com/en-us/download/details.aspx?id=42643 に移動してください。

ハードウェア

最小限のハードウェア要件は、オペレーティングシステムの最小要件を満たしている必要があります。次の表では、Windows クライアント向けの対応ハードウェアが詳しく説明されています。

Windows ハードウェア

- 200 MB の空きディスク容量（オペレーティングシステムに応じて異なります）
- 10/100/1000 または Wi-Fi ネットワークインタフェースカード
- TCP/IP がインストールされアクティブ化されている

クラウド内のストレージを対象にデータを暗号化する場合、ディスクドライブに割り当てるアルファベット文字がコンピュータで 1 つ空いている必要があります。

オペレーティングシステム

次の表では、対応オペレーティングシステムが詳しく説明されています。

Windows オペレーティングシステム（32 ビットと 64 ビット）

- Windows 7 SP1：Enterprise、Professional、Ultimate
- Windows 8.1 Update 0 ~ 1：Enterprise Edition、Pro Edition
- Windows 10：Education、Enterprise、Pro バージョン 1607（Anniversary Update/Redstone 1）からバージョン 1803（Spring Creators Update/Redstone 4）

メモ:
クライアントは、これらのオペレーティングシステムのいずれかを実行している必要があります。それ以外の場合はブロックされます。必要に応じて、レジストリキーを設定し、管理者がブロックを上書きできるようにします。

Redstone 4 サポートでは、オペレーティングシステムをアップグレードする前に、エージェントをアップグレードする必要があります。

メモ:
Data Guardian は、Microsoft の Windows Defender Exploit Guard (WDEG) (Redstone 3 以降の場合) または Enhanced Mitigation Experience Toolkit (EMET) (Redstone 2 以前の場合) に対応していません。

Windows 7 では、Data Guardian 監査イベントの位置情報ポリシーはサポートされません。

Data Guardian では、1 台のコンピュータに複数バージョンの Office がインストールされている場合はサポートされません。

クラウドストレージプロバイダ

次の表は、Data Guardian for Windows と連携するクラウドストレージプロバイダの詳細を示しています。最新のクラウドストレージプロバイダ情報は頻繁にリリースされます。新しいバージョンは、実稼動環境に導入する前に、Data Guardian でテストすることをお勧めします。

クラウドストレージプロバイダ

- Dropbox
- ビジネス向け Dropbox (Windows のみ)

  メモ:
  お客様の会社でお使いの Dell Server のバージョンによっては、ビジネス用アカウントにリンクされている個人用 Dropbox アカウントのすべてのファイルとフォルダが暗号化される場合があります。
- Box

  メモ:
  Box Tools および Box Edit は Data Guardian でサポートされていません。Box Tools を使用するとブルースクリーンが表示される場合があります。
- Google Drive

  メモ:
  Google のバックアップおよび同期はサポートされません。
- OneDrive
- OneDrive for Business
- Unified OneDrive

  メモ:
  Unified OneDrive は、OneDrive と OneDrive for Business の統合同期クライアントです。

Microsoft Office

Data Guardian は、次のバージョンの Office をサポートしています。ただし、インストールされている Office のバージョンは 1 つだけである必要があります。

Microsoft Office

- Office 2010 SP2
- Office 2013 SP1

Microsoft Office

- Office 2016
- Office 365 ProPlus：Deferred 1705、Semi-Annual 1708、および Monthly 1803

Data Guardian for Mac

以下に Mac クライアント向けの対応ハードウェアを示します。

Mac ハードウェア

- Intel Core 2 Duo、Core i3、Core i5、Core i7、または Xeon プロセッサ
- 2 GB RAM
- 10 GB の空きディスク容量

オペレーティングシステム

以下に、対応オペレーティングシステムを示します。

Mac オペレーティングシステム

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

クラウドストレージプロバイダ

Data Guardian for Mac のインタフェースでは、ポリシー設定に基づいて以下が表示されます。ユーザーは、クラウド同期クライアントをダウンロード、またはインストールする必要はありません。

クラウドストレージプロバイダ

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Data Guardian for Mobile アプリケーション

以下に Data Guardian for Mobile アプリケーションをサポートするオペレーティングシステムを一覧します。

Android オペレーティングシステム

- 4.4 ~ 4.4.4 KitKat
- 5.0 ~ 5.1.1 Lollipop
- 6.0 ~ 6.0.1 Marshmallow
- 7.0 ~ 7.1.2 Nougat
- 8.0 ~ 8.1 Oreo

iOS オペレーティングシステム

- iOS 9.x
- iOS 10.x ~ 10.3
- iOS 11 ~ 11.3

Data Guardian for Web

Data Guardian ウェブクライアントを有効にするには、管理者がウェブクライアントをホストする仮想マシンをセットアップして、Dell Server の v9.8 以降と通信します。

次の仮想環境は、Data Guardian ウェブクライアントの展開に使用できます。

仮想環境

- VMware ESXi 6.0
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-60/index.jsp を参照してください。

- VMware ESXi 5.5
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）

仮想環境

- オペレーティングシステムは必要ありません
- 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
- ハードウェアは VMware 最小要件を満たしている必要があります
- イメージ専用リソース用に最小 4 GB の RAM
- 詳細については、http://pubs.vmware.com/vsphere-55/index.jsp を参照してください。

ウェブブラウザ

Data Guardian は、Internet Explorer、Mozilla Firefox、Google Chrome、および Microsoft Edge で使用できます。

Mac では、Safari もサポートされます。

言語サポート

これらのクライアントは複数言語ユーザーインターフェイス（MUI）対応で、次の言語をサポートしています。

言語サポート

- EN - 英語
- ES - スペイン語
- FR - フランス語
- IT - イタリア語
- DE - ドイツ語
- JA - 日本語
- KO - 韓国語
- PT-BR - ポルトガル語（ブラジル）
- PT-PT - ポルトガル語（ポルトガル（イベリア））

3

Windows での Data Guardian の設定とインストール

Data Guardian クライアントのレジストリ設定

この項では、レジストリ設定の理由に関係なく、ローカル クライアント コンピュータでの Dell ProSupport 承認レジストリ設定すべてについて詳しく説明します。レジストリ設定が 2 つの製品で重複している場合は、それぞれのカテゴリでリストされます。

これらのレジストリ変更は管理者のみが行うべきであり、すべての状況に適しているわけではなく、機能しない場合もあります。

- トラブルシューティングに役立つようにログレベルを引き上げることができます。次のレジストリ設定を作成または変更します。

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

  ログレベルはデフォルトで 0xf (15) に設定されます。

  使用可能な値：

  Off=0x0 (0)

  Critical=0x1 (1)

  Error=0x3 (3)

  Warning=0x7 (7)

  Information=0xf (15)

  Debug=0x1f (31)

- Data Guardian のインストール後、内部ユーザーは自動的にアクティブ化されます。必要に応じてレジストリ設定を変更し、自動的なアクティブ化をオーバーライドできます。
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  DWORD 値: DisableAutomaticActivation=1

  メモ:
  また、Dell Server でドメインのエイリアスを確認することもできます。「自動アクティブ化の問題のトラブルシューティング」を参照してください。

Data Guardian 用のサーバの設定

管理者が設定したポリシーに基づき、Data Guardian は次のようなデータを保護します。

- ローカルに保存された Office 文書。さまざまな方法で他のユーザーと共有したり、リムーバブルメディアに保存したりできます。これらの Office ドキュメント（.docx、.pptx、.xlsx、.docm、.pptm、.xlsm、.pdf）は保護されます。
- クラウドベースのファイル共有システム - Windows コンピュータまたはモバイルデバイスは、クラウドストレージ用のデータを取得し、そのデータを暗号化し、暗号化されたデータをクラウドにアップロードします。

自社が Data Guardian を Office ドキュメントまたはクラウドストレージのみに使用しているのか、あるいはその両方に使用しているのかを、ユーザーに通知します。

Dell Security Management Server Virtual for Data Guardian の設定

Data Guardian をサポートするように Dell Security Management Server Virtual を設定するには、管理コンソールで Data Guardian ポリシーの 1 つまたは両方を **オン** にします。

- 保護対象 *Office* 文書 - エンタープライズレベルのみ
- *Cloud Encryption* - エンタープライズ、エンドポイントグループ、またはエンドポイントレベル

Dell Security Management Server for Data Guardian の設定

Data Guardian をサポートするように Dell Security Management Server を設定するには、管理コンソールで Data Guardian ポリシーの 1 つまたは両方を **オン** にします。

- 保護対象 *Office* 文書 - エンタープライズレベルのみ
- *Cloud Encryption* - エンタープライズ、エンドポイントグループ、またはエンドポイントレベル

次に、クラウドクライアントのダウンロードを許可するための Security Server の設定を行います。

Data Guardian のダウンロードを許可するための Security Management Server の設定

本項では、ユーザーが Windows Data Guardian クライアントを Security Management Server からダウンロードする場合に必要な手順について詳しく説明します。

1 Security Management Server で *<Security Server install dir>\webapps\root\cloudweb\brand\dell\resources* に移動し、テキストエディタで *messages.properties* を開きます。

2 エントリが次のようになっていることを確認します。

```
download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe
```

3 エントリを次のように編集します。

```
download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe
```

4 ファイルを保存して閉じます。

5 <Security Server install dir> に移動し、その下に Download という名前の新しいフォルダを作成します（ Security Server\Download ）。

6 Download フォルダ内で、別の新しいフォルダを作成して、cloudweb（ Security Server\Download\cloudweb ）という名前を付けます。

7 Data Guardian の 64 ビットと 32 ビットのセットアップファイルを cloudweb フォルダに追加して、DataGuardian64.exe、DataGuardian32.exe など、必要に応じてそれぞれの名前を変更します。
これらはユーザー定義ですが、versions.xml ファイル内のファイル名と一致する必要があります。

8 Security Server を再スタートして、変更を有効にします。

Windows Data Guardian クライアントの自動ダウンロードに向けた Security Management Server の設定（ オプション ）

自動ダウンロードの場合、versions.xml ファイルとバイナリは同じ場所に存在している必要があります。クライアントはこの場所にアクセスできる必要があります。したがって、IIS を使用できます。また、作成した **Security Server\Download\cloudweb** フォルダを使用できます。cloudweb フォルダを使用している場合は、このサンプル設定に従います。

1 **Security Server\Download\cloudweb** フォルダに移動します(「Data Guardian クライアントのダウンロードを許可するための Security Server の設定」の手順 6 を参照)。

2 このフォルダ内に DataGuardianUpdate という名前でフォルダを作成します。

> **メモ:**
> この例では DataGuardianUpdate ですが、任意の名前を選択できます。

3 アップデートした実行ファイルを DataGuardianUpdate フォルダに入れます。

4 DataGuardianUpdate フォルダに *versions.xml* ファイルを作成します。

5 テキストエディタで *versions.xml* を開き、ファイル名のパスが実際の環境と一致していることを確認します。

例：

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version：更新された実行ファイルのファイルバージョンです。

setup.exe ファイル名：実行可能ファイルのセットアップ名はユーザーが定義します。ただし、この名前は、messages.properties ファイル内のセットアップ名と一致する必要があります（「Data Guardian クライアントのダウンロードを許可するための Security Server の設定」の手順 3 を参照)。

6 ファイルを保存して閉じます。

7 バイナリをこのフォルダに追加します。

8 IIS を使用している場合は、IIS を再起動します。

9 管理コンソールに Dell 管理者としてログインします。

10 左ペインで **ポピュレーション** > **エンタープライズ**をクリックすると、セキュリティポリシー タブが表示されます。

11 Data Guardian テクノロジグループで、**クラウドの暗号化** > **詳細設定を表示する** をクリックします。

12 ソフトウェアアップデートサーバの *URL* ポリシーまでスクロールして、**https://<お使いのホスト URL>** > **/DataGuardianUpdate** と入力します。

> **メモ:**
> DataGuardianUpdate は、上記の例と一致させるための例です。

13 **保存** をクリックして、コミットキューにポリシーの変更を保存します。

14 **管理** > **コミット**の順にクリックします。

15 コメントを入力して、**ポリシーのコミット** をクリックします。

Data Guardian を使用しているコンピュータの再イメージ化

コンピュータを再イメージ化する必要があり、Data Guardian がインストールされている場合は、オフラインで作業したことがあり、保護対象の Office 文書をオフライン時に作成したかどうかをユーザーに確認してください。オフラインで文書を作成していた場合、それらの文書に対してオフラインキーが生成され、それらのキーは Dell Server にエスクロー（ 委託 ）されていません。

1 Dell Server にエスクローされなかった Data Guardian のオフライン生成キーをリカバリする方法については、リカバリガイド)を参照してください。

2 コンピュータを再イメージする前に、オフラインキーフォルダを確認します。

最初のエスクローキーが作成されると、Data Guardian フォルダが C:\Program Files\Dell に追加されます。Data Guardian > オフラインキーフォルダに移動します。OfflineKeys フォルダが存在しない場合、ユーザーの マイドキュメント フォルダを確認します。

管理対象アプリケーションで Microsoft の Exploit Guard または EMET を無効にする

Windows 10 では、次のアプリケーションが有効化されているか、OS に組み込まれている場合があります。

- Redstone 3 以降 - Windows Defender Exploit Guard (WDEG)
- Redstone 2 以前 - Enhanced Mitigation Experience Toolkit (EMET)

これらの機能が有効化されているか組み込まれている場合、設定を変更して Data Guardian の以下の管理対象アプリケーションを無効にする必要があります。

- winword.exe
- powerpnt.exe
- excel.exe
- acrord32.exe

Windows Defender Exploit Guard (WDEG)

管理対象アプリケーションを無効にするには、次の手順に従います。

1 **Windows Defender セキュリティセンター** を開きます。
2 **アプリとブラウザコントロール** をクリックします。
3 画面の下までスクロールして、**Exploit protection の設定** をクリックします。
4 **プログラム設定** を選択します。
5 **+** をクリックして、上記の管理対象アプリケーションをそれぞれ追加します。
6 各管理対象アプリケーションの プロパティ で、オン に設定されているオプションの 上書き チェックボックスを選択して、オプションを **オフ** に切り替えます。

> **メモ:**
> 管理対象アプリケーションが開いていて、.exe の再起動を指示するダイアログが表示された場合、上記の手順を完了してから再起動します。

7 **適用** をクリックします。
8 **はい** をクリックします。
プログラム設定 で、変更したオプションに基づいて上書きされた内容が、その管理対象アプリケーションの画面に表示されます。

Enhanced Mitigation Experience Toolkit (EMET)

管理対象アプリケーションを無効にするには、次の手順に従います。

1 **アプリケーションの構成**画面を開きます。
2 **ROP Caller Check** および **Export Address Table Address Filter (EAF)** オプションで、上記の管理対象アプリケーションのチェックボックスをオフにします。

クラウドストレージ保護プロバイダプロファイルの管理

Data Guardian はユーザーのファイルを暗号化して、Dell Server に監査イベントを送信します。サポートされている各クラウドストレージプロバイダの動作を変更するには、各プロバイダを次の値のいずれかに設定します。

値	説明
保護	プロバイダ / 接続を許可し、ファイルを暗号化し、ファイル / フォルダのアクティビティに関する監査イベントを送信します。
ブロック	プロバイダ / 接続へのアクセスをすべてブロックします。
許可	監査ファイル / フォルダのアクティビティを除き、暗号化なしで、プロバイダ / 接続のパススルーを許可します。
バイパス	暗号化または監査なしで、プロバイダ / 接続の保護をバイパスします。この値を設定すると、クラウドストレージプロバイダフォルダはクライアントコンピュータの Data Guardian 仮想ドライブには表示されません。

詳細については、Dell Server のリモート管理コンソールからアクセスできる *AdminHelp* を参照してください。

フルアクセスリストのユーザーの許可 / ブラックリストのユーザーの拒否

Data Guardian を使用するように Dell Server への登録を許可する外部ユーザーを判別できます。セキュリティ確保のため、リストを慎重に設定、管理します。

- 内部ユーザーはドメイン内のユーザーです。
- 外部ユーザーとは、ドメインが異なるユーザーのことであり、内部ユーザーが業務上の機密文書を共有する別組織のユーザーか、ドメイン外のデバイスからコンピュータにアクセスする内部ユーザーのどちらかです。

組織のドメインに属していないユーザーが Data Guardian を使用できるよう登録を許可するには：

1 リモート管理コンソールの左ペインで、**管理 > 外部ユーザー管理** とクリックします。

2 **追加** をクリックします。

3 登録アクセスタイプを選択します：

ブラックリスト - ユーザーまたはドメインの登録をブロックします。ユーザーは保護対象の Office 文書または .xen ファイルを開くことができません。

フルアクセスリスト - ユーザーまたはドメインの登録および全ファイルアクセスを許可します。ユーザーまたはドメインがブラックリストにも含まれている場合は、アクセスは許可されません。

4 ドメイン / 電子メールの入力 フィールドに、ドメイン全体のアクセスを設定するためにユーザーのドメインを入力するか、そのユーザーに対するアクセスのみを設定するために電子メールアドレスを入力します。

メモ: ホスト環境の外部モバイルユーザーについては、電子メールは小文字で入力する必要があります。

5 **追加** をクリックします。

フルアクセスリスト / ブラックリストの使い方の詳細については、管理コンソールからアクセスできる *AdminHelp* を参照してください。

Data Guardian のインストール

Data Guardian のインストールには、次の 2 つの方法があります。

- Data Guardian のインタラクティブなインストール
- コマンドラインによる Data Guardian のインストール

クラウド同期クライアント内のファイルおよびフォルダを保護するには、Data Guardian ユーザーが次のタスクを実行する必要があります。Data Guardian クライアントをインストールしたら、クラウドストレージプロバイダをダウンロードする必要があります。

- 管理者は、使用するクラウド同期プロバイダを指定する必要があります。

または

- 会社でこれらのプロバイダのいずれかを使用する場合は、Dropbox Business または OneDrive for Business / Unified OneDrive をダウンロードおよびインストールするためのリンクをユーザーに提供します。Dropbox Business ユーザーは、Data Guardian 経由で Dropbox Business に接続する必要があることに注意してください。

非暗号化ファイルがある既存フォルダ

Data Guardian の導入時には、ターゲットデバイスで、クラウドストレージプロバイダのアカウントセットアップが行われていない状態にしておくことが最善です。

Data Guardian をインストールする前に、ローカルコンピュータと同期されているフォルダで、クラウドストレージプロバイダのアカウントが設定されている場合：

- クラウドと同期している既存のファイルとフォルダは、平文のままになります。
- それらの既存のフォルダにファイルを追加すると、それらのファイルも平文のままになります。
- クラウドから同期したファイルは、暗号化されます。

  既存のファイルを暗号化する場合は、DDG VDisk virtual drive (Data Guardian のインストール時に作成) に移動し、クラウド同期クライアント内に新しいサブフォルダを作成し、既存のファイルをそのフォルダに移動します。

  または

  コンテンツが大量の場合、マネージャまたは管理者は一時的にフォルダの管理メニューを要求できます。

フォルダの管理メニュー

一部のマネージャまたは管理者は複数のユーザーによって共有されているフォルダのトラブルシューティングを一時的に実行する必要があります。管理者に、フォルダの管理 オプションの権限を要求することができます。通常、これは一時的なオプションです。

Windows への Data Guardian の対話形式によるインストール

Data Guardian をインストールするには、ローカル管理者である必要があります。ユーザーが製品をインストールする場合は、インストールメディアの場所を通知します。

作業を開始する前に

状況に応じて、サーバと Data Guardian 製品は、次の操作を行います。

ホスティング Dell セキュリティセンター	オンプレミス (Dell 管理サーバ用)	クラウド暗号化
将来のリリース用。	デルのセキュリティ管理サーバの名前がわかっていることを確認します。	コンピュータには、ディスクドライブへの割り当て用に英字が 1 つ空いている必要があります。

Data Guardian のインストール

Data Guardian をインストールした後に、コンピュータを再起動する準備をしておきます。

1 Data Guardian のインストーラをダウンロードするには、管理者に指定された場所に移動します。

2 オペレーティングシステムに基づいて、32 ビットまたは 64 ビットのいずれかを選択して (通常、**setup32.exe** または **setup64.exe** です) ローカルコンピュータにコピーします。

3 ファイルをダブルクリックしてインストーラを起動します。

4 セキュリティ警告が表示された場合は、**実行** をクリックします。

5 言語を選択し、**OK** をクリックします。

6 Microsoft Visual C++ 2015 再頒布可能パッケージ、または Microsoft .NET Framework 4.5.2 Client Profile をインストールするプロンプトが表示された場合は、**OK** をクリックします。

7 ようこそ 画面で **次へ** をクリックします。

8 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

9 宛先フォルダ 画面で、**次へ** をクリックして、**C:\Program Files\Dell\Data Guardian** のデフォルトの場所にインストールします。

C: では、ユーザー フォルダ、Windows フォルダまたはドライブのルートに Data Guardian をインストールしないでください。エラーが発生します。

10 **オンプレミス Dell 管理サーバ** を選択します。

ホスティング Dell セキュリティセンター	オンプレミス Dell 管理サーバ
将来のリリース用。	*デル管理サーバ名：* フィールドには、このコンピュータが通信するサーバ名 (server.domain.com など) を入力します。www または http (https) を含める必要はありません。この情報は管理者によって提供されます。 管理者に指示されない限り、*SSL Trust* 検証の有効化 チェックボックスをクリアしないでください。

11 **次へ** をクリックします。

12 デル管理サーバ情報の確認 画面で、サーバの URL アドレスが正しいことを確認します。インストーラが www または http (https)、およびポートを追加します。**次へ** をクリックします。

13 管理タイプ ウィンドウでは、次のオプションを選択します。

- 内部使用：会社のドメイン内の電子メールアドレスを持つユーザー。

14 **インストール** をクリックしてインストールを開始します。

ステータスウィンドウにインストールの進捗状況が表示されます。

15 インストール完了 画面が表示されたら、**終了** をクリックします。

16 **はい** をクリックして再起動します。

Data Guardian のインストールが完了します。

17 エンドユーザーにアクティブ化の確認を指示します。アクティブ化すると、Data Guardian のシステムトレイアイコンに緑色のチェックマーク  が表示されます。企業内で Data Guardian を導入した方法によっては、すぐにアクティブにならないことがあります。アクティブ化されない場合は、エンドユーザーが手動でアクティブ化を行う必要があります。ホスト環境で、手動でアクティブにしたユーザーは、コンピュータまたは Data Guardian サービスを再起動するたびに再アクティブ化を再開する必要があります。『*Data Guardian User Guide*』(Data Guardian ユーザーガイド) を参照してください。

コマンドラインによる Data Guardian のインストール

- コマンドラインのスイッチおよびパラメータは大文字と小文字を区別します。
- コマンドラインで空白などの特殊文字を 1 つ、または複数含む値は、エスケープされた引用符で囲むようにしてください。
- 次の表に、インストールで使用できるスイッチの詳細を示します。

スイッチ	意味
/V	setup.exe 内の .msi に変数を渡します。入力内容は、常にプレーンテキストの引用符で囲む必要があります。
/S	サイレントモード

オプション	意味
/QB	**キャンセル** ボタン付きの進捗状況ダイアログ、再起動のプロンプト表示
/QB!	**キャンセル** ボタンなしの進捗状況ダイアログ、再起動のプロンプト表示
/QN	ユーザーインタフェースなし

- 次の表は、インストールで使用できるパラメータの詳細です。

パラメータ
SERVER=<ServerName>（アクティブ化のための Dell サーバの FQDN）
ENTERPRISE=1（内部ユーザー）
ENABLESSLTRUST=0（SSL トラスト検証を無効にします）
REBOOT=SUPPRESS（Null 値は自動再起動を許可し、SUPPRESS は再起動を無効にします）

コマンドラインの例

- 次の例では、SSL トラスト検証なしで、内部ユーザー用に Data Guardian をサイレントインストールします。ログは C:\Library\Logs\Install.log に保存されます。

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library
\Logs\install.log" ENABLESSLTRUST=0"
```

ドメインコントローラでの GPO の設定による資格の有効化

- お使いのクライアントが Dell Digital Delivery から資格を得る場合は、これらの手順に従ってドメインコントローラに GPO を設定し、資格を有効にします（このサーバは、Dell Server を実行しているサーバとは異なる場合があります）。
- ワークステーションは、GPO が適用されている OU のメンバーである必要があります。
- Dell Server との通信に送信ポート 443 が使用可能であることを確認します。ポート 443 が何らかの理由でブロックされている場合、資格機能は機能しません。

1 クライアントを管理するドメインコントローラで、**スタート** > **管理ツール** > **グループポリシーの管理** の順にクリックします。
2 ポリシーが適用される OU を右クリックし、**このドメインでの GPO の作成** と **このコンテナにリンクする** を選択します。
3 新しい GPO の名前を入力し、ソーススターター GPO には（なし）を選択して、**OK** をクリックします。
4 作成された GPO を右クリックして **編集** を選択します。
5 グループポリシー管理エディタがロードされます。**コンピュータ設定** > **プリファレンス** > **Windows 設定** > **レジストリ** の順にアクセスします。
6 レジストリを右クリックし、**新規** > **レジストリ項目** の順に選択します。次のように設定します。

アクション：作成

ハイブ：HKEY_LOCAL_MACHINE

キーパス：SOFTWARE\Dell\Dell Data Protection

値の名前：Server

値の種類：REG_SZ

値のデータ：<Dell Server の IP アドレス>

7 **OK** をクリックします。

8 ログアウトしてもう一度ワークステーションにログイン、または **gpupdate /force** を実行してグループポリシーを適用します。

Data Guardian のアンインストール

- **エンドユーザー** がローカル管理者アカウントを持っている場合、Data Guardian をアンインストールできます。詳細については、*Data Guardian* ユーザーガイドを参照してください。本項では、Data Guardian をアンインストールする管理者の手順について説明します。

> **重要: DDG VDisk virtual drive 上の Office 以外のファイル**
> Data Guardian をアンインストールする前に、DDG VDisk virtual drive 以外の場所に重要なファイルをすべて移動します。エンドユーザーのコンピュータから Data Guardian がアンインストールされると、クラウド内のフォルダとファイルは暗号化されて読み取れなくなります。このエンドユーザーが会社を退職し、他のユーザーの誰ともそのフォルダまたはファイルを共有していない場合、データは読み取ることはできませんが、セキュリティ保護されます（ファイルを表示するには、Data Guardian を再インストールします）。
>
> Data Guardian をアンインストールしても、保護された Office ドキュメントは暗号化されたままです。復号化する方法ついては、リカバリガイド > *Data Guardian* のリカバリ を参照してください。

コマンドラインでのアンインストール

- Data Guardian クライアントインストーラは、マスターインストーラから抽出された後、**C:\Dell\DataGuardian_XXbit_setup.exe** に置かれます。
- 次の例は、Data Guardian クライアントをサイレントアンインストールします。

```
setup.exe /x /s /v" /qn"
```

指示に従ってコンピュータを再起動します。

Dropbox Business での Data Guardian の使用

Data Guardian と連携している Dropbox Business は、基本的な Dropbox のほかに追加機能を提供します。

ビジネスおよび個人用 Dropbox フォルダの保護方法に関するポリシーを設定することができます。会社でビジネスおよび個人用のアカウントを使用している場合、エンドユーザーは各アカウントタイプの暗号化について理解する必要があります。「ビジネスおよび個人用アカウントのポリシー」を参照してください。

ビジネスおよび個人用アカウントのポリシー

会社には、チームのメンバーがビジネスおよび個人用のアカウントの使用に関するガイドラインが設けられている場合があります。また、会社によってはビジネスおよび個人用のアカウントの両方の使用は、特定のユーザーにのみ許可する場合があります。

> **メモ:**
> 会社でビジネスおよび個人用のアカウントの両方を許可し、エンドユーザーが両方の使用を選択できる場合は、そのユーザーは両方のアカウントタイプのフォルダ管理について理解しておく必要があります。

次の表では、*Dropbox* 暗号化個人用フォルダポリシーの設定に基づいて暗号化を説明します。

暗号化	ポリシーの設定	導入時の考慮事項
すべてのビジネスおよび個人用のファイルおよびフォルダを暗号化する。	ポリシー > Dropbox 暗号化個人用フォルダ > **選択済み** に設定（デフォルト）	Data Guardian を展開する前に、ユーザーはクラウドストレージ同期フォルダ内の既存のビジネス用ファイルを、同期用フォルダの外にバックアップしてください。 非暗号化しておく必要のある個人用ファイルを持っているユーザーは、ファイルをビジネス同期用

暗号化	ポリシーの設定	導入時の考慮事項
		フォルダの外に移動させるか、個人用アカウントからビジネス用の同期クライアントのリンクを外します。 Data Guardian の導入後、クラウドファイルおよびフォルダは Data Guardian を実行しているコンピュータまたはデバイスでのみ表示できるようになります。個人用フォルダを誤って暗号化した場合は、Dell Data Guardian ユーザーガイドの「個人用アカウントのフォルダの復号化」を参照してください。
すべてのビジネス用アカウントファイルおよびフォルダを暗号化する。 個人用アカウントのファイルおよびフォルダを非暗号化したままにする。	ポリシー > Dropbox 暗号化個人用フォルダ > **未選択** に設定	オプションの Dropbox 暗号化個人用フォルダのメッセージ ポリシーを使用して、ビジネス用ファイルを個人用アカウント (保護されない) に **保存しない** ようユーザーに通知するカスタム化メッセージを表示できます。このメッセージは、次の場合に表示されます。 • ユーザーがログインする度に表示 • ユーザーが個人用 Dropbox アカウントに新規ファイルまたはフォルダを作成または追加した時に表示 Dropbox 暗号化個人用フォルダポリシーをエンドポイントまたはエンドポイントグループで **False** に設定した場合、これらのエンドポイントのすべてのユーザーの個人用アカウントは、暗号化されないままになります。

ビジネスおよび個人用フォルダ

会社にビジネス向け Dropbox があり、エンドユーザーにビジネスおよび個人用フォルダの両方を持つことを許可する場合に、エンドユーザーが保護されていない秘密ファイルをビジネス用フォルダにコピーする場合に備えて、すべてのビジネス用ファイルに拡張子「.xen」が使用されていることを確認するためにレポートを実行することが推奨されます。「Data Guardian のトラブルシューティング」を参照してください。

レポートの表示

Data Guardian 環境の情報は、管理コンソールに表示されます。クラウド同期クライアントフォルダおよび保護対象 Office 文書の監査イベントについては、**レポート >** 監査イベント を選択します。

デバイスの詳細、Shield の詳細、または監査イベントのコンプライアンスと監視が目的の場合、**レポート > レポートの管理** を参照してください。

詳細については、管理コンソールからアクセスできる *AdminHelp* を参照してください。

Data Guardian のトラブルシューティング

詳細画面の使用

トラブルシューティングやサポートの問題については、詳細 画面を使用します。例 :

- フォルダを作成しても暗号化しない場合は、**詳細** > **ファイル** > **フォルダ状態** の順に選択して、状態を確認します。

- エンドユーザーがサポートを要求した場合は、拡張詳細画面を設定し、**詳細** > **ポリシー** タブを選択するよう指示できます。このタブには、適用されるポリシーがリストされます。
- トラブルシューティングのログを表示します。

拡張症再画面の使用

- **<Ctrl><Shift>** を押した状態で、Data Guardian システムトレイアイコンをクリックし、**詳細** を選択します。
- ファイルおよびフォルダに加えて、次の情報が表示されます。

  セキュリティ：キー、キータイプ、状態が表示されます。このペインには、保護対象の Office ファイルが Dell Server に送信されるまで一時的に表示されます。時間はポーリング間隔によって異なります。

  監査：モジュール、ユーザー ID、イベントタイプがリストされます。この監査ログでは情報はキューに入っており、指定した間隔で Dell Server に送信されます。管理者は、監査のために管理コンソールの左ペインから **監査イベント** を表示できます。

  ポリシー：ポリシー名と値がリストされます。

ログファイルの表示

- 詳細画面の左下角から **ログの表示** をクリックします。

  ログファイルは、**C:\ProgramData\Dell\Data Guardian** でも確認できます。

  保護対象 Office 文書のログファイルは、Custom.xml フォルダにあります。

自動アクティブ化の問題のトラブルシューティング

複数のユーザーに対して Data Guardian が自動的にアクティブ化されない場合は、Data Guardian クライアントのレジストリ設定を変更できます。Dell Server のエイリアスも確認する必要があります。

1 管理コンソールで、**ポピュレーション > ドメイン** に移動して、ドメインとすべてのサブドメインを選択します。
2 ドメイン詳細 ページで、**設定** タブを選択します。
3 エイリアス フィールドで、すべてのエイリアスが正しいことを確認します。

一時的なフォルダ管理権限の提供

管理者またはユーザーにフォルダの一時的な管理権限を与えることができます。たとえば、Data Guardian をインストールする前から、ユーザーがクラウドにファイルをアップロードしていた場合、同期クライアントフォルダ内でフォルダごとに暗号化を管理させるために、一部のユーザーに一時的なフォルダ管理権限を与えることができます。

フォルダ管理権限を与えるには：

1 管理コンソールで、**ポピュレーション** > **エンドポイント** をクリックします。
2 エンドポイントを検索またはクリックし、**セキュリティポリシー** タブをクリックします。
3 **クラウドの暗号化** を選択し、**詳細設定の表示** をクリックします。
4 フォルダ管理を有効にする の横にあるチェックボックスをクリックして、ポリシーを選択します。
5 **保存** をクリックします。
6 左ペインで、**管理** > **コミット** をクリックします。

7 コメントを入力して、**ポリシーのコミット** をクリックします。

メモ:
フォルダが暗号化されたら、またはトラブルシューティングが完了したら、フォルダ管理を有効にする ポリシーチェックボックスをオフにして、そのエンドポイントのポリシーを無効にすることをお勧めします。

エンドポイント上のフォルダを管理するには：

1 同期クライアントフォルダ内にフォルダを作成してファイルを追加すると、ファイルがクラウドで暗号化されます。

2 Data Guardian システムトレイアイコンをクリックし、**フォルダの管理** を選択します。

クラウド同期フォルダの階層ビューが同期クライアントごとに表示されます。すべてのフォルダがデフォルトで選択されています。暗号化しないフォルダは、選択を解除します。フォルダの管理 でフォルダの選択を解除すると、そのフォルダ内の既存ファイルは復号化スイープによって復号化されます。そのフォルダ内の新規ファイルは、ローカルドライブ上またはクラウド内で暗号化されません。

メモ:
クラウドまたは Data Guardian 仮想ドライブ内にあるフォルダで、なおかつ、フォルダの管理 で選択解除したフォルダに、暗号化されたファイルをドラッグすると、そのファイルは暗号化されたままになり、ファイルの内容を表示できなくなります。また、フォルダを別の Data Guardian ユーザーと共有する場合、このユーザーが フォルダの管理 ポリシーを有効にしていなければ、このユーザーに対してそれらのファイルは暗号化されたままであり、このユーザーはその内容を表示することができません。

3 既存のフォルダを暗号化するには、そのフォルダの暗号化を手動でオンにします。ファイルは、そのファイルがクラウドに同期されるときに暗号化されます。

よくあるご質問（FAQ）

フォルダ管理についてのよくあるご質問（FAQ）

質問

別のユーザーと共有したファイルがあるフォルダを持っています。そのフォルダの内容を復号化するために、システムトレイで **Data Guardian > フォルダの管理** ユーティリティを使用したのですが、最近になってファイルがクラウドで再度暗号化されました。そのフォルダはフォルダの管理ユーティリティで表示されなくなっており、クラウドでこれらのファイルを復号化できなくなりました。

回答

暗号化キー ID のフォルダとの関連付けは、そのフォルダにファイルを追加した最初のユーザーに基づいて行われます。ユーザーがフォルダを作成しても、それにファイルを追加しなければ、キーはそのフォルダに関連付けられません。フォルダの管理ユーティリティでフォルダを表示できるのは、暗号化キー ID がそのフォルダに設定されたユーザーのみです。フォルダで暗号化キー ID を設定されているユーザーがフォルダの管理ユーティリティでそのフォルダの選択を解除し、別の Data Guardian ユーザーとそのフォルダを共有すると、2 番目のユーザーの Data Guardian がフォルダの内容を再暗号化します。

解決策

1 新規フォルダを作成します。

2 暗号化すべきすべてのファイルを新規フォルダに移動します。

3 システムトレイで **Dell Data Guardian** > **フォルダの管理** ユーティリティを再度使用して、これらのファイルを復号化します。

メモ:
別の Data Guardian ユーザーと共有しているフォルダの内容を復号化する場合、その他のユーザーの Data Guardian クライアントによってそれらを暗号化するポリシーが実施されます。最も一般的な方法としては、フォルダの管理ユーティリティを使用して、他の Data Guardian ユーザーと共有されていないファイルのみを復号化します。

質問

フォルダの管理ユーティリティを使用して選択解除した復号化フォルダに同期していますが、ウェブブラウザ経由でフォルダをアップロードしようとすると、暗号化されたファイルしかアップロードできません。

回答

Data Guardian は、クラウド内のフォルダをアクティブに検索するようには設計されていませんが、暗号化されていないフォルダでは、Data Guardian は同期クライアント経由で同期することができます。これは、同期クライアントがこの環境を制御しているからです。ウェブブラウザ経由で処理されるファイルは、暗号化される必要があります。

解決策

同期フォルダにファイルを追加してください。

質問

コンピュータからクラウドベースのファイル共有システムを最近アンインストールしたのですが、フォルダの管理ユーティリティを開くと、いまだにいずれかの同期クライアントがオプションとしてリストされています。

回答

Data Guardian は、サードパーティーソフトウェアのインストールまたはアンインストールを監視しません。オプションが引き続きリストされているのは、これらのクライアントがアンインストール時に既存のファイルを削除するようには設計されていないためです。同期クライアントがインストールされていない状態でも、これらのファイルは Data Guardian によって保護されたままとなります。

解決策

アンインストールした同期クライアントオプションを フォルダの管理 ユーティリティから削除するには、残しておきたいすべてのフォルダ / ファイルを同期フォルダから出してから、同期フォルダを削除します。フォルダを削除した後、それはフォルダの管理ユーティリティにリストされなくなります。

その他のよくあるご質問（ FAQ ）

質問

ユーザーは Data Guardian を使用しており、保護対象の Office 文書がありますが、コピーまたは貼り付けを実行できません。

回答

Data Guardian の場合、一部の機能はシステムトレイから実行します。ユーザーがシステムトレイを変更したかどうかを確認します。

解決策

デフォルトのシステムトレイ設定を使用する必要があります。ユーザーはデフォルトのシステムトレイ設定を維持する必要があります。

質問

混乱を招くファイル名 ポリシーを GUID から拡張子のみに変更しました。以前に同期していたフォルダでは、ファイルが依然として GUID ファイル名の形式に暗号化されます。なぜですか。

回答

Security Management Server/Security Management Server Virtual でポリシーを変更しても、Data Guardian はそのフォルダの以前のポリシーを維持します。新たに作成したフォルダには、新しいポリシーが適用され、**拡張子のみ** 形式に暗号化されます。

解決策

古いファイルに **拡張子のみ** 形式を再適用するには、その形式を切り取って、新しいポリシーを適用する新規フォルダに貼り付けてください。

4

Mac での Data Guardian の設定とインストール

Data Guardian for Mac は、クラウド暗号化プロバイダ内でのファイル共有用に設計されています。ただし、Mac に対して保護されている Office 文書 ポリシーが有効になっている場合、ファイルがユーザーによってローカル Mac に保存されると、すべてのファイル監査およびトレーサビリティは失われます。厳密なファイル監査およびトレーサビリティが組織で必要な場合は、*Mac Data Guardian* アクティベーションの許可 ポリシーを **未選択** に設定し、Data Guardian が Mac 上でアクティブ化されないようにします。

サーバタスク

前提条件

これらのタスクを実行する前に、次の事柄を確認してください。

- Dell Server およびそのコンポーネントをインストールします。次のいずれかを参照してください。
  - *Security Management Server* のインストールおよびマイグレーションガイド
  - *Security Management Server Virtual* クイックスタートガイドおよびインストールガイド
- 管理コンソールで、適切な Dell 管理者役割を割り当てます。

ポリシー

Data Guardian はデフォルトでユーザーのファイルを暗号化して、Security Management Server Virtual に監査イベントを送信します。ここでは、特定のバージョンに言及する必要（ Dell Security Management Server Virtual を使用する場合は手順が異なる場合など ）がない限り、両方のサーバともデルサーバと呼びます。

監査イベントに地理位置情報データを含める場合は、Wifi を有効にする必要があります。地理位置情報と監査イベントの詳細については、*AdminHelp* を参照してください。

サポートされている各クラウドストレージプロバイダのデフォルト動作を変更するには、クラウドストレージプロテクションプロバイダポリシーを設定してください。企業が特定のクラウドストレージプロバイダを希望する場合は、他のプロバイダに対するこのポリシーを **ブロック** に設定してください。ポリシーについては、管理コンソールからアクセスできる *AdminHelp* を参照してください。

メモ:
このポリシーのバイパスオプションは Windows 向けです。Mac に対して バイパス を選択すると、エンドユーザに 許可 と表示されます。

クラウドクライアントのダウンロードを許可する Security Server の設定

これらのタスクを実行する前に、次の事柄を確認してください。

- Dell Server およびそのコンポーネントをインストールします。次のいずれかを参照してください。
  - *Security Management Server* のインストールおよびマイグレーションガイド
  - *Security Management Server Virtual* クイックスタートガイドおよびインストールガイド
- 管理コンソールで、適切な Dell 管理者役割を割り当てます。

Security Management Server

1 Security Management Server で <Security Server install dir>\webapps\cloudweb\brand\dell\resources\ に移動します。
2 テキストエディタで **messages.properties** ファイルを開きます。
3 エントリが次のようになっていることを確認します。
ローカル インストールの場合：

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

リモート インストールの場合：

```
download.deviceWin.mode=remote

download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

4 ファイルを保存して閉じます。
5 <Security Server install dir> に移動し、Download という名前のフォルダを作成します（Security Server\Download）。
6 ダウンロードフォルダ内に、CloudWeb フォルダ（Security Server\Download\CloudWeb）を作成します。
7 Dell Data Guardian インストーラを作成したフォルダに追加します。

Virtual Edition：異なるクラウドクライアントバージョンの手動インストール

ユーザーによる最新 Dell Data Guardian インストーラのダウンロードを許可するためのアクションは不要です。最新のインストーラが Security Management Server Virtual セキュリティサーバにプリインストールされています。

Security Management Server Virtual セキュリティサーバに異なる Data Guardian インストーラのバージョンを手動でインストールするには、message.properties ファイルをアップデートします。

1 次の場所に移動します。
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 テキストエディタで **messages.properties** ファイルを開きます。
ローカル インストールの場合：

```
download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

リモート インストールの場合：

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

3 ファイルを保存して閉じます。

4 そのファイルを /opt/dell/server/security-server/download/cloudweb にコピーします。

5 このフォルダに Data Guardian インストーラを追加します。

フルアクセスリストのユーザーの許可 / ブラックリストのユーザーの拒否

フルアクセスリストとブラックリストのエントリは、Data Guardian の使用のために Dell Server に登録できるユーザーを決定します。

フルアクセスリスト

フルアクセスリストは、特定のユーザーまたはユーザーグループによる Dell Server への登録と Data Guardian の利用を許可します。

外部ユーザーは、登録を許可するためにフルアクセスリストに配置する必要があります。次の例を参照して、ユーザーの登録を許可します。

ユーザータイプ	入力内容
すべての organization.com 電子メールアドレス	`organization.com`
特定のユーザー	`jdoe@organization.com`
すべての Gmail ユーザー	`gmail.com`

ブラックリスト

ブラックリストでは、特定のユーザーまたはユーザーグループの Dell Server への登録と Data Guardian の利用を禁止します。ブラックリストに電子メールアドレスを入力されたユーザーは、Data Guardian に登録できないと通知するメッセージを受信します。

メモ:
ユーザーがすでに登録されている場合、このリストはこれらのユーザーの Data Guardian の利用を禁止**しません**。

フルアクセスリストで承認グループのメンバーになっている特定のユーザーを除外する場合は、このブラックリストを使用することができます。さらに、ドメイン全体をブラックリストに指定できます。この指定では、そのドメインの電子メールアドレスを持つすべてのユーザーが登録できなくなります。次の例を参照して、ユーザーまたはグループによる Dell Server への登録を禁止します。

ユーザータイプ	入力内容
すべての organization.com 電子メールアドレス	`organization.com`
特定のユーザーおよびその電子メールアドレス	`jdoe@organization.com`
すべての Gmail ユーザー	`gmail.com`

フルアクセスリスト / ブラックリストを変更するには、次の手順に従ってください。

1 リモート管理コンソールの左ペインで、**管理 > 外部ユーザー管理** とクリックします。

2 **追加** をクリックします。

3 登録アクセスタイプを選択します：

ブラックリスト - ユーザーまたはドメインの登録をブロックします。ユーザーは、保護されている Office 文書または .xen ファイルを開けません。

フルアクセスリスト - ユーザーまたはドメインの登録およびすべてのファイルアクセスを許可します。ユーザーまたはドメインがブラックリストにも含まれている場合は、アクセスは許可されません。

4 ドメイン / 電子メールの入力 フィールドで、ドメイン全体のアクセスを設定するためにユーザーのドメインを入力するか、そのユーザーに対するアクセスのみを設定するために電子メールアドレスを入力します。

5 **追加** をクリックします。

フルアクセスリスト / ブラックリストの使い方の詳細については、Dell Server のリモート管理コンソールからアクセスできる *AdminHelp* を参照してください。

外部ユーザーは、保護されているファイルへのキーのため、内部ユーザーからのアクセスを要求することができます。内部ユーザーが利用できない場合は、リモート管理コンソールを使用してアクセスをへのアクセスを許可または拒否することができます。

1 **管理 > キー要求管理** の順に選択します。

2 詳細については、**?**（ヘルプ）を選択してください。

クライアント関連の作業

前提条件

- ターゲットデバイスが次にアクセスできることを確認します。
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- インストールを実行しているユーザーが、インストールのためのローカル管理者アカウントを持っていることを確認します。
- コマンドラインを使用してインストールしている場合、ユーザーがアクティブ化を行うセキュリティサーバの完全修飾ドメイン名を把握しておくようにしてください。

ベストプラクティス

導入中は、IT のベストプラクティスに従ってください。ベストプラクティスには以下が挙げられますが、これらに限定されません。

- 初期テストのために制御されたテスト環境
- ユーザーへのスタッガ化された導入

クライアントのインストール

ホワイトリストに追加済みのユーザーは、この時点で https://yoursecurityservername.domain.com:8443/cloudweb/register で登録することができます。

ユーザーは登録後に、ログインして適切なクライアントをダウンロードするために https://yoursecurityservername.domain.com:8443/cloudweb に誘導する電子メールを受信します。

エンドユーザーは通常、https://yoursecurityservername.domain.com:8443/cloudweb で登録後、ユーザー自身で Mac クライアントをインストールするため、管理者の Mac クライアントのインストールはオプションです。

ただし、組織から Mac クライアントのインストールを求められる場合にはインストールすることもできます。ユーザーインタフェースを使用して、または組織で利用可能なプッシュテクノロジーを使用するコマンドラインによって Data Guardian クライアントをインストールします。エンドユーザーによる登録およびアクティブ化は、どちらも引き続き必須です。

旧バージョンの Cloud Edition からのアップグレード

企業に旧バージョンの Cloud Edition があり、Data Guardian にアップグレードする場合、旧バージョンの Cloud Edition は削除されます。

メモ:
企業が Cloud Edition から Data Guardian にアップグレードする場合、ユーザーは Data Guardian をクラウドストレージプロバイダと再リンクする必要があります。認証の詳細については、オンラインの Dell Data Guardian ヘルプを参照してください。

インストールオプション

クライアントのインストール / アップグレードを行うには、次のいずれかを選択します。

- インタラクティブなインストール - これは Data Guardian for Mac をインストールする最も簡単な方法です。ただし、この方法は、1 台のコンピュータごとにクライアントをインストールする計画の場合にのみ使用してください。

  または

- コマンドラインでのインストール - この高度なインストール方法については、管理者がコマンドラインの構文を使用して実行する必要があります。この方法は、スクリプト形式のインストール、バッチファイルの使用、または組織で利用できる任意のプッシュテクノロジーに活用できます。

インタラクティブなインストール

1 Data Guardian クライアントの場合、**Dell-Data-Guardian--0.x.x.xxxx.dmg** にインストーラがあります。
2 インストールまたはアップグレードするには、DDPSL-Explorer-0.x.x.xxxx.dmg 内の**.pkg** ファイルを使用します。これには、スクリプト形式のインストール、バッチファイル、または組織で利用できる任意のプッシュテクノロジーを使用できます。
3 **Dell-Data-Guardian-x.x.x** パッケージをダブルクリックします。
4 **続行** をクリックします。
5 はじめに ウィンドウで、**続行** をクリックします。
6 ソフトウェアライセンス契約 ウィンドウで、**続行** をクリックします。
7 **同意する** をクリックして続行します。
8 構成タイプ ウィンドウで、**オンプレミス Dell 管理サーバ**を選択します。

メモ:
ホストされた *Dell* セキュリティセンター は、将来のリリース用です。

9 インストールの種類 ウィンドウで、次のいずれかを実行します。
- **インストール** をクリックして、手順 9 に進みます。
- **インストール場所を変更** をクリックします。
  1 宛先の選択ウィンドウで、すべてのユーザーまたは単一のユーザーを選択します。
  2 **続行** をクリックします。
  3 **インストール** をクリックして、手順 9 に進みます。

10 ダイアログにユーザーの名前とパスワードを入力し、**ソフトウェアのインストール** をクリックします。
11 サマリ ウィンドウで、**閉じる** をクリックします。
12 「エンドユーザーのアクティブ化」を参照してください。

メモ:
企業が Cloud Edition から Data Guardian にアップグレードする場合、ユーザーは Data Guardian をクラウドストレージプロバイダと再リンクする必要があります。認証の詳細については、オンラインの Dell Data Guardian ヘルプを参照してください。

13 .dmg ウィンドウを閉じ、Finder を開きます。

コマンドラインでのインストール

1 .dmg をマウントします。
2 次の installer コマンドを使用して、パッケージのコマンドラインでのインストールを実行します。

```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```

3 ユーザーに Data Guardian をアクティブ化するよう指示します。「エンドユーザーのアクティブ化」を参照してください。

エンドユーザーのアクティブ化

初めて Mac 上で Dell Data Guardian を開いた後で、次の手順に従います。

1 Finder で、**アプリケーション** を選択し、**Dell Data Guardian** をダブルクリックします。
2 Dell Server ウィンドウが開いたら、Dell Server のアドレスを入力して **保存** をクリックします。

資格情報 ウィンドウが開きます。

3 ドメイン電子メールアドレスとドメインパスワードを入力します。
4 **ログイン** をクリックして、Dell Data Guardian をアクティブ化します。

Dell Data Guardian アプリケーションが開き、アクティブ化が成功すると、クラウドストレージプロバイダの名前が薄い色で左側のペインに表示されます。

すべてのユーザーが同じクラウドプロバイダを使用して共同作業することを企業が希望している場合、管理者は、そのプロバイダのみを有効にして、他のプロバイダが表示されないようにするポリシーを設定できます。

Dell Data Guardian アプリケーションの認証が取り消されたか期限切れになった場合も、クラウドストレージプロバイダの名前がグレー表示されます。

5 左ペインでクラウドストレージプロバイダを選択します。
ウィンドウが開き、資格情報のためのプロンプトが表示されます。認証されると、クラウドストレージプロバイダの名前がアクティブ化されます。

6 認証の詳細については、オンラインの Dell Data Guardian ヘルプを参照してください。

Data Guardian のアンインストール

本項では、Data Guardian をアンインストールする管理者の手順について説明します。アンインストールを実行するには、ローカル管理者アカウントが必要です。エンドユーザーがローカル管理者アカウントを持っている場合、そのユーザーは自分で Data Guardian for Mac をアンインストールできます。

Data Guardian を削除するには、次のいずれかを実行します。

Finder

1 <オプション> キーを押しながら、メニューバーから、**進む** を選択します。
2 **~/Library/Application Support/Dell** フォルダを開きます。
3 **DellDataGuardian** フォルダを右クリックして、**ゴミ箱に移動** を選択します。
4 メニューバーの **進む** から、アプリケーションフォルダを開き、**Dell Data Guardian** アプリケーションをごみ箱に移動します。
5 **OK** をクリックします。
6 プロンプトが表示されたら、Administrator パスワードを入力します。

ターミナル

次のいずれか、または両方の場所に Data Guardian が存在する可能性があります。

1 以下のコマンドを使用します。
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 **DellDataGuardian** フォルダを削除します。

5

ウェブクライアント用 Data Guardian の設定とインストール

このウェブクライアントは、ユーザーが Data Guardian クライアントをインストールしなくても保護されている Office ドキュメントまたは .xen ファイルを表示できるようにします。一般的なルールとして、デルでは、最初に Security Management Server または Security Management Server Virtual をインストールすることを推奨しています。

OVA ファイルのダウンロード

Data-Guardian-Web は初期インストール時に OVA ファイルとして配信されます。Open Virtual Application (オープン仮想アプリケーション) は仮想マシンで実行されるソフトウェアを配信するために使用されます。

OVA ファイルのダウンロード手順

1 Data Guardian 製品サポート ページに移動します。
2 **ドライバおよびダウンロード** をクリックします。
3 <OS バージョン> のすべての利用可能なアップデートを表示 の隣にある **OS の変更** をクリックし、**VMware ESXi 6.0** または **VMware ESXi 5.5** のいずれかを選択します。
4 「表示基準 : 」で **すべて表示** を選択します。
5 Dell Data Security で **ダウンロード** を選択します。

Data Guardian for Web のインストール

Data-Guardian-Web のインストールおよび設定

作業を開始する前に、すべてのシステムと仮想環境の要件が満たされていることを確認してください。

1 インストールしたメディアで Data Guardian ファイルを探し、**Data-Guardian-Web-1.x.x.ova** をダブルクリックして VMware にインポートします。
2 Data-Guardian-Web の電源を入れます。
3 ライセンス契約の言語を選択し、**EULA を表示する** を選択します。
4 ライセンス契約を読み、**EULA に同意する** を選択します。
5 アップデートが利用可能な場合、**同意する** を選択します。
6 デフォルトパスワードの変更プロンプトが表示されたら、**はい** を選択します。
7 *ddguser* パスワードの設定 画面で、現在 (デフォルト) のパスワードである **ddguser** を入力し、次に固有のパスワードを入力して、同じ固有のパスワードを再入力してから **OK** を選択します。

   パスワードには次の文字が含まれている必要があります。

   - 少なくとも 8 文字
   - 少なくとも 1 つの大文字
   - 少なくとも 1 つの数字
   - 少なくとも 1 つの特殊文字

8 *ddgconsole* および *ddgsupport* アカウントでも、上の手順を繰り返します。

メモ:
名前と同じデフォルトパスワードを保持するには、**キャンセル** をクリックします。パスワードを変更するには、現在のパスワード フィールドに **ddgconsole** または **ddgsupport** と入力します。

9 ホスト名の設定 ダイアログで、Backspace キーを使用してデフォルトホスト名を削除します。FQDN ホスト名を入力して、**OK** を選択します。

10 複数のノードとロードバランサがある場合は、ロードバランサのホスト名を入力します。

11 ネットワークの設定 ダイアログで、以下のいずれかのオプションを選択し、**OK** を選択します。

- （デフォルト）DHCP を使用
- （推奨）DHCP の使用 フィールドで、スペースバーを押して X を削除し、該当する場合は、静的 IP、ネットワークマスク、デフォルトゲートウェイ、DNS サーバー 1、DNS サーバー 2、DNS サーバー 3 の各アドレスを手動で入力します。

メモ:
静的 IP を使用する場合は、DNS サーバーにもホストエントリを作成する必要があります。

12 scp 画面が表示された場合、OK をクリックしないでください。最初に .cer ファイルと .key ファイルをアプリケーションに追加するか、CA の .pfx または .p7b ファイルから抽出する必要があります。「WinSCP ツールの使用」を参照してください。

メモ:
これらのファイルを解凍する前に scp 画面で OK をクリックした場合、Data-Guardian-Web を再スタートして、ネットワークの設定構成 ダイアログで操作を行う必要があります。

WinSCP ツールの使用

Windows で、ddgconsole アカウントを使用して、SSL 証明書ファイルおよび SSL キーファイルに対して scp を実行します。

1 Windows で、WinSCP ツールを開きます。

2 WinSCP ページで、ホスト名を入力します。

3 デフォルトの ddgconsole ユーザー名とデフォルトのパスワード（または変更したユーザー名とパスワード）を入力します。

4 **ログイン** をクリックします。

5 証明書とキー、.pfx ファイル、または .p7b ファイルを、ローカルドライブから **opt/dell/files** ディレクトリにドラッグします。

6 .pfx ファイルまたは .p7b ファイルを追加した場合、プロンプトが表示されたらパスワードを入力します。証明書とキーが CA から抽出され、**apache2/ssl/folder** に追加されます。

.pfx または .p7b ファイルをドラッグする代わりに、証明書を手動で抽出することもできます。サンプルコードは次のとおりです。

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

.pfx ファイルからプライベートキーを解凍するサンプルコードは次のとおりです。

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

7 管理コンソールの scp 画面に戻ります。

管理コンソール

管理コンソールの scp 画面で、次の手順を実行します。

1 **OK** をクリックします。*Apache2* リバースプロキシ証明書のインストール 画面が開き、証明書がリスト表示されます。

2 証明書を選択して **Enter** を押します。

3 以下のいずれかを行います。

- WinSCP ツールでキーを追加した場合は、次の画面でそのキーを選択して **Enter** を押します。
- WinSCP ツールで .pfx ファイルまたは .p7b ファイルのパスワードを入力した場合は、プロンプトが表示されたらそのパスワードを入力して、**OK** をクリックします。

4 デルサーバ設定画面で、サーバホスト名を入力し、**OK** をクリックします。ダイアログにプロビジョニングに使用する URL が一覧表示されます。URL は次の形式で表示されます: **https://node.domain.com/edap-admin-ui/provision_node**

メモ:
node.domain.com は、ホスト名の設定 で入力した名前です。URL はそのノードを指します。

5 ブラウザを開き、URL を入力します。

6 Dell Data Guardian のノードプロビジョニングページが開いたら、**ノードプロビジョニングの開始** をクリックします。

7 ログインページで、ドメインの電子メールとパスワードを入力して **ログイン** をクリックします。Dell Data Guardian はプロビジョニングの成功を知らせるダイアログを表示しします。

8 URL が表示された管理コンソール画面に戻り、**OK** をクリックします。アプリケーションサーバが再起動し、管理コンソールのメインメニューが開きます。

追加タスク：

- URL を内部ユーザーに提供して、Data Guardian のウェブクライアントにアクセスできるようにします。
  - 単一ノードの場合、URL は **https://nodename/** の形式で表示されます。nodename は ホスト名の設定 画面で入力したホスト名が反映されます。
  - 複数ノードの場合、URL は **https://loadBalancerName/** の形式で表示されます。nodename は ホスト名の設定 画面で入力したロードバランサのホスト名が反映されます。
- 今後、この VM をアップデートする、またはログを確認するためにサーバにアクセスする場合は、この VM の SSH を有効にする必要があります。**基本設定 > SSH の設定** の順に選択して ddgsupport ユーザーの SSH を有効にします。
- 管理コンソールで、ノードベースのウェブポータルのポリシーを変更する場合は、アプライアンスを再起動する必要があります。「アプライアンスの再起動」を参照してください。再起動後は、ddguser 資格情報でログインする必要があります。

管理コンソールを開く

https://server.domain.com:8443/webui/ で管理コンソールを開きます。

デフォルトの資格情報は **superadmin/changeit** です。

管理コンソールにアクセスするには、次のウェブブラウザがサポートされています。

- Internet Explorer 11.x 以降
- Mozilla Firefox 41.x 以降
- Google Chrome 46.x 以降
- Safari

Data Guardian の基本端末設定タスク

基本設定タスクは、メインメニューからアクセスできます。

ホスト名の変更

このタスクはいつでも完了できます。を使用して開始することは必須ではありません。

1 基本設定 メニューから、**ホスト名** を選択します。

2 Backspace キーを使用して、既存の Data-Guardian-Web ホスト名を削除し、新しいホスト名に置き換えて **OK** を選択します。

ネットワーク設定の変更

このタスクはいつでも完了できます。を使用して開始することは必須ではありません。

1 基本設定メニューから、**ネットワーク** を選択します。
2 ネットワークの設定 画面で以下のいずれかのオプションを選択し、**OK** を選択します。
   - （デフォルト）DHCP を使用する（IPv4）。
   - （推奨）DHCP を使用する でスペースバーを押して X を削除し、手動で次の該当するアドレスを入力します。

     静的 IP

     ネットワークマスク

     デフォルトゲートウェイ

     DNS サーバー 1

     DNS サーバー 2

     DNS サーバー 3

     静的な設定では、IPv6 または IPv4 のいずれかを選択します。

   メモ:
   静的 IP を使用する場合は、DNS サーバーにホストエントリを作成する必要があります。

ユーザーパスワードの変更

このタスクはいつでも完了できます。を使用して開始することは必須ではありません。

次のユーザーのパスワードを変更できます。

- ddguser（端末管理者） - このユーザーは、Data Guardian 端末とそのメニューにアクセスできます。
- ddgconsole（シェルアクセス） - このユーザーは、Data Guardian シェルにアクセスできます。シェルアクセスは、ネットワーク管理者がネットワーク接続をチェックしてトラブルシューティングを行うために使用できます。
- ddgsupport（Dell ProSupport 管理者） - このユーザーは Dell ProSupport 専用です。セキュリティ上の理由により、このアカウントのパスワードは管理者自身でコントロールします。

1 基本設定 メニューから、**ユーザーパスワードの変更** を選択します。
2 ユーザーパスワードの変更 画面で変更するユーザーパスワードを選択し、**Enter** を選択します。
3 パスワードの設定 画面で現在のパスワードを入力し、新規パスワードを入力して同じ新規パスワードを再入力してから **OK** を選択します。
   パスワードには次の文字が含まれている必要があります。

   - 少なくとも 8 文字
   - 少なくとも 1 つの大文字
   - 少なくとも 1 つの数字
   - 少なくとも 1 つの特殊文字

   メモ: 別のユーザーアカウントを選択するには、キーボードの "スペースバー" キーを押して、選択リストを表示します。

SSH の有効化

このタスクはいつでも完了できます。を使用して開始することは必須ではありません。

SSH は、サポート管理者のログイン、シェルアクセス、端末のコマンドラインインタフェース用に有効化します。

1 基本設定 メニューから、**SSH** を選択します。
2 SSH を有効にするユーザーをハイライトし、スペースバーを押して **X** を入力し、**OK** を選択します。

サービスの開始または停止

この作業は、必要な場合にのみ実行するようにしてください。

1 すべてのサービスを同時に開始または停止するには、基本設定 メニューから **アプリケーションの起動** または **アプリケーションの停止** のいずれかを選択します。
2 確認プロンプトで **はい** を選択します。

メモ: サーバー状態の変更には、最大 2 分かかる場合があります。

アプライアンスの再起動

この作業は、必要な場合にのみ実行するようにしてください。

1 基本設定 メニューから、**アプライアンスの再起動** を選択します。
2 確認プロンプトで **はい** を選択します。
3 再起動後、Data Guardian にログインします。

アプライアンスのシャットダウン

この作業は、必要な場合にのみ実行するようにしてください。

1 基本設定 メニューから、下にスクロールして **アプライアンスのシャットダウン** を選択します。
2 確認プロンプトで **はい** を選択します。
3 再起動後、Data Guardian にログインします。

管理者のタスク

端末言語の設定または変更

設定変更を行ったときは、常にサービスを再起動することがベストプラクティスです。

1 メインメニューで、**言語の設定** を選択します。
2 矢印キーを使用して使用する言語を選択します。

システムスナップショットログの生成

Dell ProSupport のシステムスナップショットログを生成するには、メインメニューで **サポートツール** を選択します。

1 サポートツール メニューから、**システムスナップショットログの生成** を選択します。
2 ファイルが作成されたことを示すメッセージが表示されたら、**OK** を選択します。