システム管理
Virtual Desktop Service

NetApp
May 03, 2022

目次

システム管理

ドメイン管理者（「レベル **3** 」）アカウントを作成します

概要

場合によっては 'VDS 管理者は環境を管理するためにドメインレベルの資格情報を必要としますVDS では、「レベル 3 」または「 .tech 」アカウントと呼ばれます。

ここでは、適切な権限を使用してこれらのアカウントを作成する方法について説明します。

Windows Server ドメインコントローラ

内部でホストされているドメインコントローラ（または VPN/Express ルート経由で Azure にリンクされているローカル DC ）を実行している場合、 .tech アカウントは Active Directory Manager で直接実行できます。

1. ドメイン管理（ .tech ）アカウントを使用して、ドメインコントローラ（ CWMGR1 、 DC01 、または既存の VM ）に接続します。
2. 必要に応じて、新しいユーザを作成します。
3. 「 Level3 Technician 」セキュリティグループにユーザを追加します

   [management.System Administre.create domain admin アカウント 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

a. 「 Level3 Technician 」セキュリティグループが見つからない場合は、グループを作成して「 CW インフラストラクチャ」セキュリティグループのメンバーにしてください。

[management.System Administration.create domain admin アカウント 0fc27] |

Management.System_Administration.create_domain_admin_account-0fc27.png

管理者アカウントとエンドユーザアカウントを区別するためには、ユーザ名の最後に「 .tech 」を追加することをお勧めします。

Azure AD ドメインサービス

Azure AD ドメインサービスで実行されている場合、または Azure AD のユーザを管理している場合は、通常の Azure AD ユーザとして Azure Management Portal でこれらのアカウントを管理（パスワードの変更など）できます。

新しいアカウントを作成し、次のロールに追加することで、必要な権限が付与されます。

1. AAD DC 管理者
2. ClientDHPAccess
3. ディレクトリ内のグローバル管理者。

管理者アカウントとエンドユーザアカウントを区別するためには、ユーザ名の最後に「 .tech 」を追加することをお勧めします。

[]

第三者への一時的なアクセスの提供

概要

クラウド解決策に移行する際には、サードパーティへのアクセスを提供することが一般的です。

VDS 管理者は、多くの場合、これらのサードパーティに、「最低限必要」のセキュリティアクセスポリシーに従うための同レベルのアクセス権を付与しないことを選択します。

サードパーティの管理者アクセス権を設定するには 'VDS にログインして組織モジュールに移動し ' 組織内をクリックしてユーザーとグループをクリックします

次に、サードパーティ用の新しいユーザアカウントを作成し、 Admin Access セクションが表示されるまで下にスクロールして、管理者権限を有効にするチェックボックスをオンにします。

[]

次に 'VDS 管理者に管理者アクセスのセットアップ画面が表示されますユーザーの名前、ログイン、パスワードを変更する必要はありません。多要素認証を適用してアクセス権のレベルを選択する場合は、電話番号や電子メールを追加してください。

VAR や ISV などのデータベース管理者にとって、必要なアクセスモジュールは一般的に *Servers* のみです。

[]

保存すると、エンドユーザーは標準の仮想デスクトップユーザー資格情報を使用して VDS にログインすることで、自己管理機能にアクセスできます。

新しく作成されたユーザーがログインすると、割り当てたモジュールのみが表示されます。組織を選択し、 [サーバー] セクションまでスクロールダウンして、指定したサーバー名に接続できます（たとえば、 XYZ > D1 、 XYZ は会社コード、 D1 はサーバーがデータサーバーであることを示します）。以下の例では、割り当てを実行するために TSD1 サーバーに接続するように指示します。

[]

バックアップスケジュールを設定します

概要

VDS では、 Azure を含む一部のインフラプロバイダでネイティブバックアップサービスを設定および管理できます。

Azure

Azure では、 VDS でネイティブを使用してバックアップを自動的に設定できます "Azure クラウドバックアップ" ローカル冗長ストレージ（ LRS ）を使用。必要に応じて、地理的冗長ストレージ（ GRS ）を Azure Management Portal で設定できます。

- バックアップポリシーは、サーバタイプごとに個別に定義できます（デフォルトで推奨されます）。また 'VDS UI から個別のマシンにスケジュールを割り当てることができますこの設定は ' ワークスペースページでサーバ名をクリックすることで ' サーバの詳細ビューに移動して適用できます (以下のビデオ : 個別のバックアップポリシーの設定を参照)
  - データ
    - 毎日 7 回、毎週 5 回、毎月 2 回のバックアップを作成します。ビジネス要件に基づいて保持期間を延長
    - これは、専用のデータサーバと、アプリケーションおよびデータベース用のアドオン VPS VM の両方に当てはまります。
  - インフラ
    - CWMGR1 –毎日バックアップし、毎日 7 、毎週 5 、毎月 2 回保持します。
    - RDS ゲートウェイ - 毎週バックアップし、週 4 回保持します。
    - HTML5 ゲートウェイ–毎週バックアップし、週 4 回保持します。
  - パワーユーザ（別名 VDI ユーザ）
    - データは D1 サーバまたは TSD1 サーバに格納する必要があるため、 VM をバックアップしないでください。
    - 一部のアプリケーションではデータがローカルに格納されるため、特別な考慮事項があることに注意してください。
    - VM に障害が発生した場合、別の VM のクローニングを使用して新しい VM を作成できます。VDI VM が 1 つだけ（または一意の VM のビルドが 1 つ）しかない場合は、その VM を完全に再構築する必要がないように VM をバックアップすることを推奨します。
    - すべての VDI サーバをバックアップするのではなく、必要に応じて、 1 つの VM を手動で構成して Azure Management Portal で直接バックアップすることで、コストを最小限に抑えることができます。
  - TS

        - データは D1 サーバまたは TSD1 サーバに格納する必要があるため、 VM をバックアップしないでください。
        - 一部のアプリケーションではデータがローカルに格納されるため、特別な考慮事項があることに注意してください。
        - VM に障害が発生した場合、別の VM のクローニングを使用して新しい VM を作成できます。TS VM が 1 台しかない場合は、その VM を完全に再構築する必要がないようにバックアップすることを推奨します。
        - すべての TS サーバをバックアップするのではなく、必要に応じて、 1 台の VM を手動で構成して Azure Management Portal に直接バックアップすることで、コストを最小限に抑えることができます。
    - TSData を参照してください
        - 毎日 7 回、毎週 5 回、毎月 2 回のバックアップを作成します。ビジネス要件に基づいて保持期間を延長

- ポリシーは、バックアップを毎日または毎週実行するように設定できますが、 Azure ではそれ以上の頻度のスケジュールがサポートされません。
- 日次スケジュールの場合は、バックアップの優先実行時間を入力します。週次スケジュールの場合は、バックアップを実行する曜日と時刻を入力します。注：時間を午前 12 時に設定すると、 Azure バックアップで原因の問題が発生する可能性があるため、午前 12 時 1 分を推奨します。
- 日単位、週単位、月単位、年単位のバックアップを保持する数を定義します。

導入時のデフォルトを設定

[]

環境全体に対して **Azure** バックアップを設定するには、次の手順を実行します。

1. ［ Deployments Detail ］ ページに移動し、 ［ Backup Defaults ］ を選択します
2. ドロップダウンメニューからサーバタイプを選択します。サーバタイプは次のとおりです。

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to
them
TS: these are terminal servers that Users launch sessions on
TSData: these are servers doubling as terminal and data servers.
```

    - これにより、導入全体の包括的なバックアップ設定が定義されます。これらは、必要に応じて後でサーバー固有のレベルでオーバーライドおよび設定できます。
3. 設定ホイールをクリックし、表示される編集ポップアップをクリックします。
4. 次のバックアップ設定を選択します。

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. 最後に、 [スケジュールの作成（または編集）] をクリックして、これらの設定を配置します。

個々のバックアップポリシーを設定する

サーバー固有の統合バックアップ設定を適用するには、 **Workspace** 詳細ページに移動します。

1. [Servers] セクションまでスクロールダウンし、サーバの名前をクリックします
2. [スケジュールの追加] をクリックします
3. 必要に応じてバックアップ設定を適用し、 [スケジュールの作成] をクリックします

バックアップからリストアしています

特定の **VM** のバックアップをリストアするには、まずその **Workspace** 詳細ページに移動します。

1. [Servers] セクションまでスクロールダウンし、サーバの名前をクリックします
2. [Backups] セクションまで下にスクロールし、ホイールをクリックしてオプションを展開し、いずれかを選択します
3. サーバへのリストアまたはディスクへのリストア（バックアップからドライブを接続して、バックアップから VM の既存のバージョンにデータをコピーできるようにする）
4. 他のリストアの場合と同様に、この時点からリストアを続行します。

コストは、維持するスケジュールによって異なり、 Azure のバックアップコストが全体的に発生します。VM のバックアップ価格については、 Azure Cost Calculator で確認できます。 https://azure.microsoft.com/en-us/pricing/calculator/

仮想マシンのクローニング

概要

Virtual Desktop Service （ VDS ；仮想デスクトップサービス）では、既存の仮想マシン（ VM ）をクローニングできます。この機能は、定義されたユーザー数の増加に応じてサーバーユニット数の可用性を自動的に向上させるように設計されています。また、使用可能なリソースプールに追加のサーバーを追加

管理者は次の 2 つの方法で VDS のクローニングを使用します。

1. 必要に応じて、既存のクライアントサーバから新しいサーバを自動的に作成します
2. パートナーが定義および管理するルールに基づいてリソースを自動拡張するための新しいクライアントサーバの事前自動作成

クローニングして共有サーバを追加する

クローンは、既存の仮想マシンのコピーです。クローニング機能は、ゲストオペレーティングシステムとアプリケーションのインストールに時間がかかるため、時間を節約し、管理者の規模を拡大するのに役立ちます。クローンを使用すると、仮想マシンのコピーを 1 つのインストールおよび設定プロセスから作成できます。通常は次のようになります。

1. 必要なすべてのアプリケーションと設定を TS または TSD サーバにインストールする
2. [ワークスペース]>[サーバー] セクション >[ソースサーバーの歯車アイコン]>[クローン] の順に選択します
3. クローンプロセスの実行を許可する（通常は 45 ~ 90 分）
4. 最後の手順では、クローンサーバをアクティブにして、 RDS プールに配置し、新しい接続を受け入れます。クローン作成されたサーバでは ' クローン作成後に個別の設定が必要になる場合があるため 'VDS は管理者が手動でサーバをローテーションするのを待機します

必要な回数だけ繰り返します。[]

共有セッションホスト環境でユーザの容量を増やすには、セッションホストのクローニングは簡単なプロセスであり、いくつかの手順を踏むだけで済みます。

1. クローニングするセッションホストを選択し、マシンに現在ログインしているユーザがないことを確認します。
2. VDS で、ターゲットクライアントのワークスペースに移動します。[Servers] セクションまでスクロールし、歯車アイコンをクリックして [Clone] を選択します。この処理にはかなりの時間がかかり、ソースマシンがオフラインになります。完了までに 30 分以上かかります。

   [] []

3. このプロセスでは、サーバをシャットダウンし、サーバを別のイメージに複製し、お客様の次の TS# にイメージを Sysprep します。サーバーのリストに、「 *Type=Staged _ and _Status=Activation Required* 」と表示されます。

   []

4. サーバにログオンし、サーバが本番稼働可能な状態になっていることを確認します。

   []

5. 準備ができたら、 [Activate] をクリックしてサーバをセッションホストプールに追加し、ユーザ接続の受け入れを開始します。

   []

VDS クローニングプロセスの定義

ステップバイステップのプロセスの詳細については ' クローンサーバの操作の VDS>Deployment>Task History を参照してくださいこのプロセスには 20 以上の手順があります。最初にハイパーバイザーにアクセスしてクローンプロセスを開始し、最後にクローンサーバをアクティブ化します。クローニングプロセスは、次のような重要な手順で構成されます。

- DNS を設定し、サーバ名を設定します

- StaticIP を割り当てます
- ドメインに追加します
- Active Directory を更新します
- VDS DB の更新（ CWMGR1 上の SQL インスタンス）
- クローン用のファイアウォールルールを作成します

タスク履歴だけでなく、すべてのクローニングプロセスの詳細な手順は、各パートナーの Virtual Desktop Deployment の CWMGR1 の CwVmAutomationService ログに表示できます。これらのログファイルの確認については、文書化しています "こちらをご覧ください"。

新しいサーバの自動作成

この VDS 機能は、定義されたユーザー数の増加に応じてサーバーユニット数の可用性を自動的に向上させるように設計されています。

パートナーは VDS （""） > Client > Overview – VM Resources > Auto-Scalingパートナーが自動スケーリングを有効 / 無効にしたり、クライアントごとにカスタムルールを作成したりできるように、いくつかのコントロールが公開されています。たとえば、ユーザー数 / サーバー数、ユーザーあたりの RAM 容量、 CPU あたりのユーザー数などです。

> 上記では、仮想デスクトップ環境全体で自動クローン作成が有効になっていることを前提としています。たとえば、すべての自動クローン作成を停止するには、 Advanced （詳細）ウィンドウで、 Server Creation （サーバーの作成） → Automated Cloning Enabled （自動クローン作成有効）のチェックを外します。

自動クローンプロセスはいつ実行されますか。

自動クローンプロセスは、毎日のメンテナンスの実行が設定されているときに実行されます。デフォルトは午前 0 時ですが、編集可能です。日々のメンテナンスの一環として、各リソースプールに対してリソースの変更スレッドを実行します。Change Resources スレッドは、プールの構成を使用するユーザーの数に基づいて、必要な共有サーバーの数を決定します（カスタマイズ可能。サーバごとに 10 、 21 、 30 などのユーザーを指定できます）。

新しいサーバの「オンデマンド」自動作成

この VDS 機能を使用すると、使用可能なリソースプールに追加サーバを自動的に「オンデマンド」でクローニングできます。

VDS 管理者が VDS にログインし、組織またはワークスペースモジュールの下で特定のクライアントを検索し、概要タブを開きます。Servers Tile には、すべてのサーバ（ TSD1 、 TS1 、 D1 など）が一覧表示されます。個々のサーバのクローンを作成するには、サーバ名の右端にある歯車をクリックし、 [クローン] オプションを選択します。

通常、このプロセスには約 1 時間かかります。ただし、期間は VM のサイズと、基盤となるハイパーバイザーで使用可能なリソースによって異なります。複製されるサーバは再起動が必要になるため、通常は営業時間外またはスケジュールされた保守期間中に実行します。

TSData サーバーのクローンを作成する場合、重複するファイルがないように、 c:\Home 、 c:\Data 、 c:\Pro の各フォルダを削除します。この場合、クローニングプロセスは失敗します。これらのファイルの削除に問題がありました。このエラーはあいまいです。通常は、ファイルまたはプロセスが開いているためにクローニン

グイベントが失敗したことを意味します。次に、すべての AV を無効にしてください（このエラーを説明する可能性があるため）。

ディスク容量の自動拡張機能

概要

ネットアップでは、管理者がドキュメントにアクセスして保存するためのスペースを常に確保しておく必要があることを認めています。これにより、 VM にバックアップを正常に完了するための十分な空き領域が確保され、管理者とそのディザスタリカバリおよびビジネス継続性計画を有効にして活用できるようになります。この点を考慮して、ドライブがスペース不足になると、使用中の管理対象ディスクを自動的に次の階層に拡張する機能を構築しました。

これは、 Azure のすべての新しい VDS 環境にデフォルトで適用される設定です。これにより、すべての環境でユーザーとテナントのバックアップがデフォルトで保護されます。

管理者は、 [配置（ Deployments ）] タブに移動し、展開を選択して、そこから CWMGR1 サーバに接続することで、この状態を確認できます。次に、デスクトップの DCConfig ショートカットを開き、 Advanced をクリックして下にスクロールします。

[]

管理者は、 DCConfig の同じ詳細セクションで、管理対象ディスクの次の階層に移動する前に、空き容量（ GB ）または空き容量（ % ）をドライブの空き容量に変更できます。

[]

いくつかの実用的なアプリケーション例：

- ドライブに 50 GB 以上の空き容量があることを確認するには、 MinFreeSpaceGB を 50 に設定します
- ドライブの 15% 以上が空いていることを確認するには、 MinFreeSpacePercent を 10 から 15 に設定します。

このアクションは、サーバのタイムゾーンの午前 0 時に実行されます。

Azure Key Vault で VDS クレデンシャルにアクセスする

概要

CWASetup 5.4 は、以前の Azure 導入方法からの出発点です。構成と検証のプロセスが合理化され、導入を開始するために必要な情報量が削減されます。削除されたプロンプトの多くは、ローカル VM 管理者、 SMTP アカウント、テクニカルアカウント、 SQL SA などのアカウントのクレデンシャルまたはアカウントです。これらのアカウントは、自動的に生成されて Azure Key Vault に格納されるようになりました。デフォルトでは、これらの自動生成されたアカウントにアクセスするには、次の手順を実行する必要があります。

- 「キーボールト」リソースを検索し、そのリソースをクリックします。

  [幅 = 75%]

- [設定] で、 [タレット] をクリックします。次の項目を表示する権限がないことを示すメッセージが表示されます。

[幅 = 75%]

- 「アクセスポリシー」を追加して、 Azure AD アカウント（グローバル管理者やシステム管理者など）にこれらの重要なキーへのアクセスを許可します。

  [幅 = 75%]

- この例では、グローバル管理者が使用されています。プリンシパルを選択したら、 [選択] 、 [追加] の順にクリックします。

  [幅 = 75%]

- [Save （保存）] をクリックします。

  [幅 = 75%]

- アクセスポリシーが追加されました：

  [幅 = 75%]

- 「小塔」を再訪問して、アカウントが導入アカウントにアクセスできることを確認します。

  [幅 = 75%]

- たとえば、 CWMGR1 にログインしてグループポリシーを更新するためにドメイン管理者の資格情報が必要な場合は、各エントリをクリックして、 cjDomainAdministratorName および cjDomainAdministratorPassword の文字列を確認します。

  [幅 = 75%]

  [幅 = 75%]

- 値の表示またはコピー：

  [幅 = 75%]

監視とアンチウイルスを適用します

概要

Virtual Desktop Service （ VDS ）の管理者は、プラットフォームインフラストラクチャ（ CWMGR1 以上で構成）とその他のすべてのインフラストラクチャおよび仮想マシン（ VM ）の両方を監視する責任があります。ほとんどの場合、管理者はインフラ（ハイパーバイザーや SAN ）の監視をデータセンターや IaaS プロバイダと直接調整します。管理者は、ターミナルサーバとデータサーバの監視を担当します。通常は、 Remote Management and Monitoring （ RMM ）解決策を適切に導入します。

ウイルス対策は、管理者の責任です（プラットフォームインフラストラクチャおよびターミナル / データサーバ VM の両方）。このプロセスを合理化するため、 Azure サーバ用の VDS では、デフォルトで Windows Defender が適用されています。

サードパーティ製ソリューションをインストールする場合は、ファイアウォールや VDS の自動化を妨げる可能性のあるその他のコンポーネントを含めないようにしてください。

特に、非常に特定のアンチウイルスポリシーがデフォルトで設定されている場合、これらのアンチウイルスエージェントが仮想デスクトップサービスによって管理されるサーバーにインストールされていると、悪影響を及ぼす可能性があります。

全般的なガイダンスとしては、 VDS プラットフォームの自動化は一般にアンチウイルス製品やアンチマルウェア製品の影響を受けませんが、すべてのプラットフォームサーバ（ CWMGR1 、 RDGateways 、 HTML5Gateway 、 FTP など）で次のプロセスの例外 / 除外を追加することをお勧めします。

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

さらに、クライアントサーバ上の次のプロセスを安全にリストすることをお勧めします。

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

マッピングされたドライブの追加と移動

概要

デフォルトでは、エンドユーザーセッションに公開される 3 つの共有フォルダがあります。これらのフォルダは定義済みのストレージレイヤにあります。これは、ファイルサーバ（ TSD1 または D1 ）または Azure Files 、 Azure NetApp Files 、 NetApp CVO 、ネットアップ CVS などのストレージサービスに該当します。

明確にするため、この記事では、会社コード「 NECA 」の顧客例を使用します。 この例では、単一の TDS1 サーバが NECATSD1 という名前で配置されていることを前提としています。フォルダを別の VM （「 NECAD1 」という名前）に移動するプロセスを進めます。この方法は、次の例に示すように、同じマシン上のパーティション間または別のマシン間で移動する場合に使用できます。

フォルダの開始場所：

- データ : NECATSD1\C:\data\NECA\ (TSD1 は、最初のターミナルサーバであり、データサーバとしても機

能することを意味します)

- FTP ： NECATSD1\C ： \ftp\NECA\
- ホーム： NECATSD1\C ： \home\NECA/

フォルダの終了場所：

- データ： NECAD1\G ： \data\NECA/ （ D1 は最初のデータサーバであることを意味します）
- FTP ：同じプロセスが適用されます。 3 倍に記述する必要はありません
- 自宅：同じプロセスが適用され、 3 倍に説明する必要はありません

NECAD1 で G ：のディスクを追加します

1. 共有フォルダを E ：ドライブに配置するには、ハイパーバイザーを介して追加する必要があります（例 Azure Management Portal ）にアクセスし、初期化してフォーマットします

   []

2. 既存のフォルダ（ NECATSD1 、 C:\ 上）を新しい場所（ NECAD1 、 G:\ 上）にコピーします。
3. 元の場所から新しい場所にフォルダをコピーします。

   []

元のフォルダ共有からの情報の収集（ NECATSD1 、 C ： \data\NECA/ ）

1. 元の場所にあるフォルダとまったく同じパスを使用して、新しいフォルダを共有します。
2. 新しい NECAD1 、 G:\data\ フォルダを開きます。この例では、会社コード「 NECA 」という名前のフォルダが表示されます。

   []

3. 元のフォルダ共有のセキュリティ権限をメモします。

   []

4. ここでは一般的な設定を示しますが、保持する必要がある既存のカスタマイズがある場合には、元の設定をコピーすることが重要です。他のすべてのユーザ / グループの権限は、新しいフォルダ共有から削除する必要があります
   - System ：許可されているすべての権限
   - LocalClientDHPAccess （ローカルマシン上）：許可されているすべての権限
   - ClientDHPAccess （ドメイン上）：許可されているすべての権限
   - NECA - （ドメイン上の）すべてのユーザ：「フルコントロール」を除くすべての権限

共有パスとセキュリティ権限を新しい共有フォルダに複製します

1. 新しい場所（ NECAD1 、 G ： \data\NECA/ ）に戻り、同じネットワークパス（マシンを除く）で NECA フォルダを共有します。この例では、「 NECA-DATA$ 」と入力します。

[]

2. ユーザセキュリティの場合は、すべてのユーザを追加し、ユーザの権限を照合するように設定します。

   []

3. すでに存在する可能性のある他のユーザ / グループの権限を削除します。

   []

グループポリシーの編集 (フォルダが新しいマシンに移動された場合のみ)

1. 次に、グループポリシー管理エディタでドライブマップを編集します。Azure AD ドメインサービスの場合、マッピングは次の場所にあります。

   ```
   “Cloud Workspace Users > User Configuration > Preferences > Windows
   Settings> Drive Maps”
   ```

   []

2. グループポリシーが更新されると、次回各ユーザーが接続すると、マップされたドライブが新しい場所を参照して表示されます。
3. この時点で、 NECATSD1 、 C:\ にある元のフォルダを削除できます。

トラブルシューティング

エンドユーザーが赤い X 印の付いたドライブを見たら、ドライブを右クリックして [切断] を選択します。ログアウトしてから再度ドライブに戻ってください。[]