進化する明日へ Continue thinking

I-O DATA

ホワイトペーパーシリーズ：

Windows Server IoT 2019 for Storage で構築する企業向け最新ファイルサーバー

1. インフラ編
2. 運用管理編
3. 集中管理編
4. **ハイブリッドクラウド編**

2019 年 6 月 30 日

内容

このガイドを利用する上での注意点

このガイドで説明する Windows Admin Center、Azure サービス、その他のクラウドサービスは、2019 年 6 月時点の情報に基づいています。UI や機能は、ツールやサービスのバージョンアップや機能拡張により、変更される可能性があることをご了承ください。

1　概要

1.1　このガイドについて

このガイドは、Windows Server IoT 2019 for Storage Standard または Workgroup を搭載する LAN DISK Z シリーズの NAS デバイスを導入するにあたり、パブリッククラウドとのハイブリッド利用シナリオについて説明します。オンプレミスの Windows Server ベースのファイルサーバーとして利用できる LAN DISK Z の NAS デバイスが、パブリッククラウドとどのような関係があるのか、どのように連携、統合することができ、どのような利点があるのかを説明します。

1.2　ハイブリッドクラウドの利用シナリオ

オンプレミス（社内設置）のファイルサーバーとして利用できる LAN DISK Z は、インターネット上で提供されるパブリッククラウドとはまったく関係性が無いように思えるかもしれません。しかしながら、Windows Server ベースの NAS デバイスは、パブリッククラウドが提供する各種サービスとさまざまな方法で連携することが容易です。オンプレミスのサーバーやプライベートクラウドとパブリッククラウドの両方を適切に組み合わせて利用することを、一般的にハイブリッドクラウドと呼びます。

パブリッククラウドとハイブリッドクラウド

「パブリッククラウド」とは、クラウド事業者の世界規模のインフラストラクチャとネットワーク網上に構築され、コンピューティング環境をマルチテナント（共有）、オンデマンド、かつセルフサービスで利用者に提供する各種サービスです。代表的なものに、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）などがあります。これに対して、クラウドの技術をオンプレミスのデータセンターに応用したものを「プライベートクラウド」と呼びます。

クラウドのサービスには、その提供形態によって SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）の大きく 3 つのタイプに分けることができます。SaaS はすぐに利用を開始できるソフトウェア（例：Office 365）、PaaS は利用者が開発した Web アプリを展開して実行できるアプリケーションプラットフォーム、IaaS は仮想マシンの展開および実行環境です。

クラウドのサービスは多様化しており、中には従来の 3 つのタイプに明確に区分できないものもあります。また、パブリッククラウドだけで完結しない利用シナリオも増えてきました。オンプレミスのサーバーやプライベートクラウドとパブリッククラウドのサービスを連携、統合したハイブリッドクラウドの利用シナリオです。ハイブリッドクラウドの利用シナリオとしては、バックアップ、障害・災害対策（事業継続性計画）、ID 管理の統合、セキュリティ、システム運用管理・監視、自動化などがあります。

Azure のハイブリッドサービス

Windows Server IoT 2019 for Storage を搭載する LAN DISK Z は、Windows Server ベースのファイルサーバーそのものであり、Azure のサービスとの親和性が非常に高いという利点があります。このガイドでは、以下の 3 つのサービスとのハイブリッド利用について説明します。

- **Azure Update Management（更新の管理）** —— オンプレミスおよび Azure 上の Windows およ

び Linux の更新に対応したクラウドベースの更新管理サービスです。オンプレミスの複数のサーバーおよび Azure 上の複数の仮想マシンの更新プログラムの検出とインストールの開始スケジュール、および再起動を一元的に制御できます。Azure Update Management は更新プログラムそのものを提供するものではなく、オンプレミスの Windows Server の場合は、Windows Update または社内に展開済みの Windows Server Update Services（WSUS）を更新プログラムの提供元として使用します。LAN DISK Z は、Azure Update Management を使用して更新を管理することができます。

- **Azure Backup** —— オンプレミスの Windows Server のデータと Azure 上のリソース（Azure 仮想マシンや Azure ファイル共有など）のバックアップと回復に対応したクラウドベースのバックアップサービスです。バックアップデータはクラウドのストレージに格納されます。LAN DISK Z に保存されるデータは、Azure Backup を利用して Azure のクラウドストレージにスケジュールバックアップすることができ、NAS デバイスに突然に襲い掛かる障害や災害に対してもクラウドという遠隔地（国内または海外のデータセンター）でデータを保護することができます。

- **Azure File Sync（ファイル同期）** —— オンプレミスの Windows Server のディレクトリと Azure ストレージアカウントの Azure ファイル共有（File サービス）を双方向に同期するファイル同期サービスです。このサービスもまた、LAN DISK Z と連携できます。Azure ファイル共有はインターネット経由でセキュアにアクセス可能な SMB 共有を提供するもので、オンプレミス側の障害時に、ユーザーに対してファイルへのアクセスを継続提供することができます。Azure ファイル共有は、SMB v3 クライアントからアクセスすることができ、ネットワークトラフィックは SMB 暗号化でエンドツーエンドで保護されます。SMB 暗号化については、このガイドのシリーズの『1. インフラ編』で説明しました。また、Azure File Sync のクラウドの階層化を利用すると、アクセス頻度の少ないファイルをクラウド側にのみ保存して、オンプレミス側のディスク使用を節約することができます。

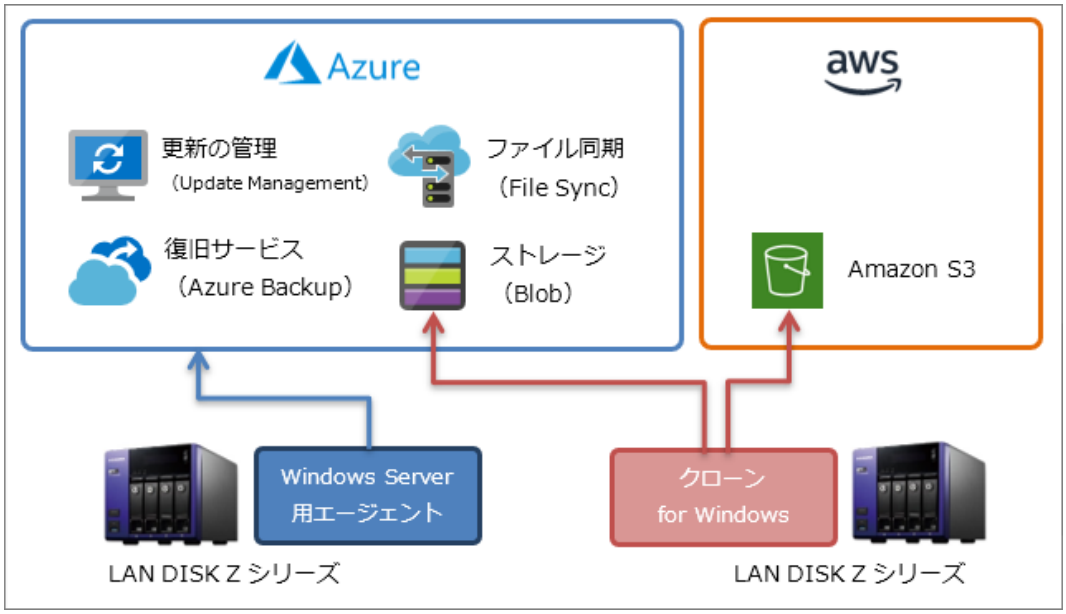
同期先としてのクラウドストレージ（クローン for Windows）

アイ・オー・データの「クローン for Windows」は、LAN DISK Z の NAS デバイス間で共有フォルダーや設定情報を同期するツールです。NAS デバイス間の同期は、スケジュール設定に基づいてマスターからスレーブに対して一方向で行われます。NAS デバイス間の同期の他、マスターまたはスレーブから外付けハードディスクへのデータの同期、マスターまたはスレーブから Microsoft Azure の BLOB ストレージや AWS の Amazon S3（Simple Storage Service）へデータを同期するクラウドストレージ同期にも対応しています。

Azure Backup と同様に、クローン for Windows のクラウドストレージ同期を利用すると、NAS デバイスに突如襲い掛かる障害や災害から遠隔地でデータを保護できます。同期先のクラウドの選択肢があること、そして代替の NAS デバイスに対するデータ復旧のシンプルさが、クローン for Windows の特徴と言えるでしょう。

1.3 実施環境について

このガイドでは、Microsoft Azure のサービスとの連携を中心に説明します。クローン for Windows のクラウドストレージ同期については、Microsoft Azure または Amazon S3 のいずれかを利用できます。Microsoft Azure のサービスを利用するには Azure アカウント（30 日の無料アカウントを含む）が、Amazon S3 を利用するには AWS アカウント（12 か月の無料アカウントを含む）が必要になります。



クラウドサービスの利用コストについて

Microsoft Azure の各サービスおよび Amazon S3 のサービスの利用コストについては、各サービスの料金表で確認してください。

Automation の価格（Azure Update Management）
https://azure.microsoft.com/ja-jp/pricing/

Azure Backup の価格
https://azure.microsoft.com/ja-jp/pricing/details/backup/

Azure Files の料金（Azure FileSync）
https://azure.microsoft.com/ja-jp/pricing/details/storage/files/

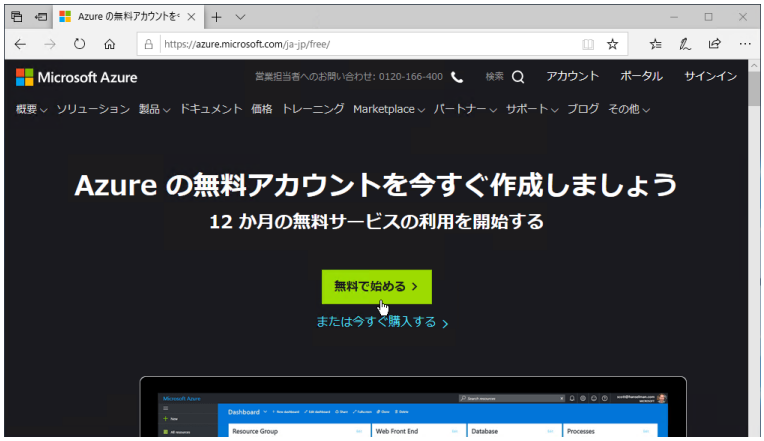
ブロック BLOB の料金
https://azure.microsoft.com/ja-jp/pricing/details/storage/blobs/

Amazon S3 の料金
https://aws.amazon.com/jp/s3/pricing/

Azure 無料アカウントについて

Microsoft Azure のアカウントをお持ちでない場合は、30 日間の無料アカウントにサインアップすることで試用することができます。無料アカウントにサインアップすると、30 日間、Azure クレジット枠 22,500 円（$200 相当、日本円の利用枠は為替の変動によって変更される場合があります）の範囲内でほとんどのサービスを制限なく利用できるほか、サインアップ後 12 か月間、一部の有料サービスを無料で利用できる特典が提供されます。

Azure 無料アカウントのサインアップは、以下のサイトの［無料で始める >］をクリックして開始できます。サインアップのためには、Microsoft アカウント、Office 365 の組織アカウント、または GitHub アカウントが必要です。また、有効なクレジットカード情報の登録が必要です（無料期間中の請求は発生しません）。30 日の無料期間が過ぎると、デプロイ済みのリソースを維持したまま従量課金制に移行することができます。



Azure 無料アカウント
https://azure.microsoft.com/ja-jp/free/

AWS 無料アカウントについて

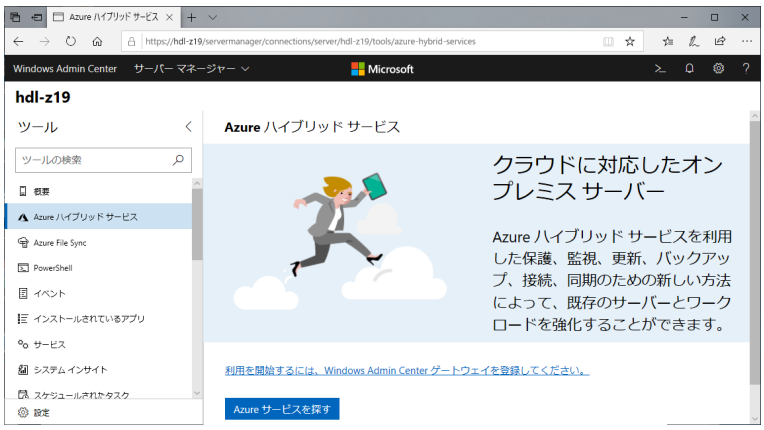
AWS アカウントをお持ちでない場合は、12 か月の AWS 無料アカウントにサインアップすることで試用することができます。AWS 無料アカウントには、Amazon EC2、Amazon S3、Amazon DynamoDB を含む 12 か月の無料利用枠が提供されます。

AWS 無料アカウントへのサインアップは、以下のサイトの［AWS アカウントを今すぐ無料で作成 »］をクリックして開始できます。サインアップのためには、有効なメールアドレスおよびクレジットカード情報の登録が必要です（無料期間中の請求は発生しません）。

Amazon S3｜無料
https://aws.amazon.com/jp/s3/

Windows Admin Center の管理環境の準備

Microsoft Azure のハイブリッドサービスは、標準的なセットアップ方法でオンプレミスの Windows Server や、Windows Server IoT 2019 for Storage を搭載する LAN DISK Z と連携することができます。HTML5 ベースの管理ツールである Windows Admin Center の管理環境があると、Azure ハイブリッドサービスとの連携、統合機能を提供しているため、セット



アップの複雑な部分のほとんどを Windows Admin Center の中で簡単な操作で完了することができ、すぐに利用を開始することができます。

このガイドのシリーズの『3. 集中管理編』では、Windows 10（バージョン 1709 以降）に導入するデスクトップモードの Windows Admin Center、または LAN DISK Z（または Windows Server 2016 以降を実行する他のサーバー）に導入するゲートウェイモードの Windows Admin Center について説明しました。このガイドでは、いずれかの管理環境が導入済みであることを想定し、Windows Admin Center を利用した簡単なセットアップ方法を説明します。

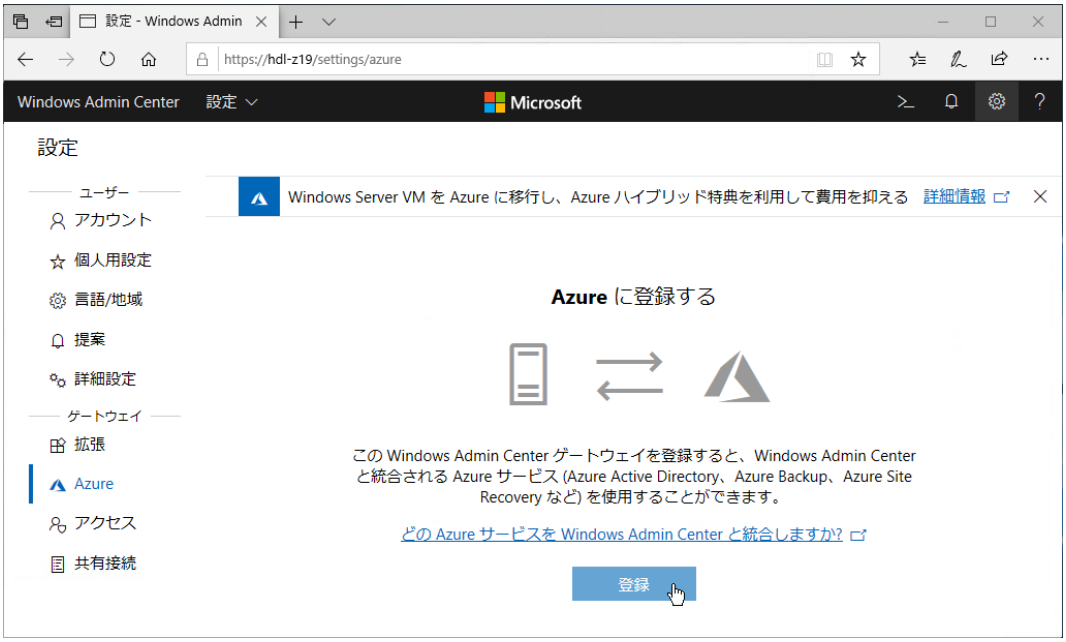
2. LAN DISK Z での Azure サービスのハイブリッド利用

Windows Admin Center を使用して、LAN DISK Z と Azure ハブリッドサービスを連携させる手順について説明します。デスクトップモードまたはゲートウェイモードの Windows Admin Center が既に導入済みであることを前提とします。

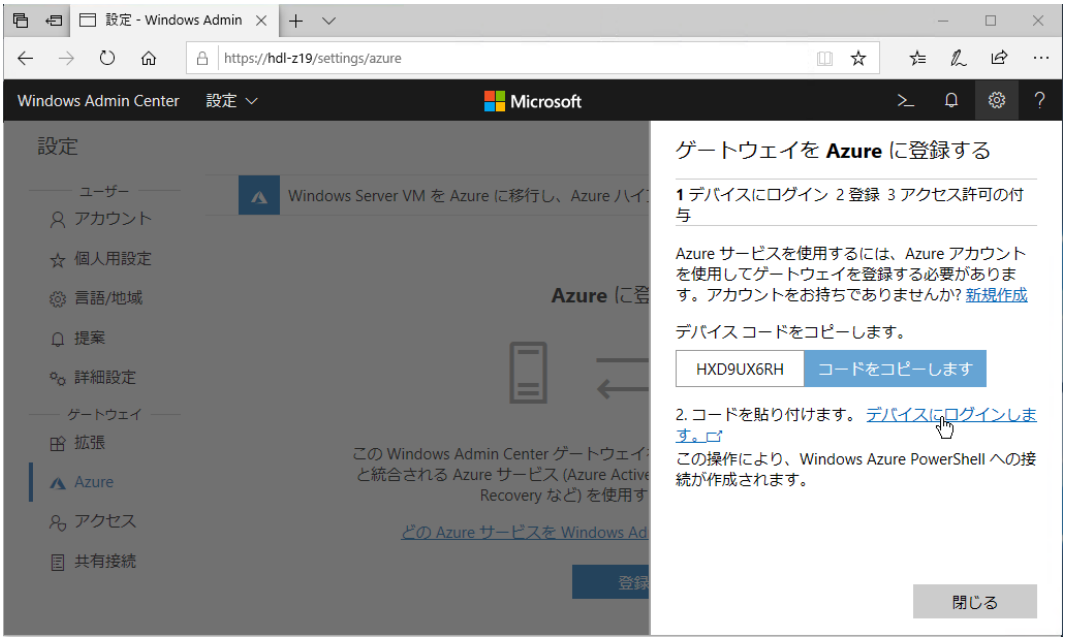
2.1 Windows Admin Center と Azure の統合

Windows Admin Center で Azure ハイブリッドサービスの各種サービスをセットアップして利用するためには、事前に Azure に Windows Admin Center のゲートウェイ（この場合、デスクトップモードの Windows Admin Center もゲートウェイとして機能します）を登録します。

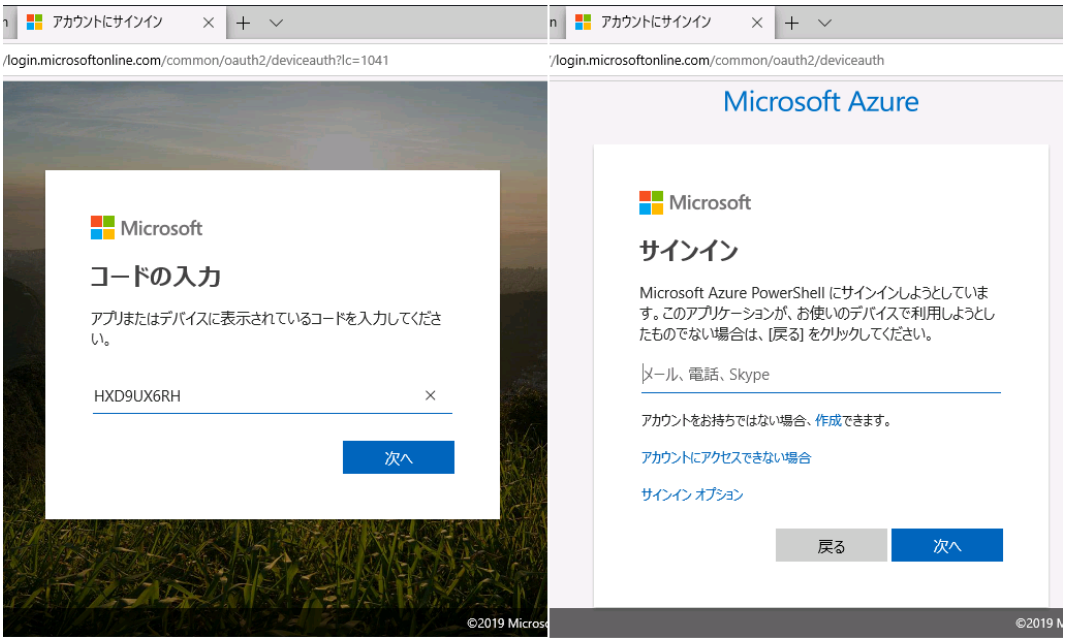
1. デスクトップモードまたはゲートウェイモードの Windows Admin Center サイトのトップページを開き、[設定]（⚙アイコン）をクリックして、[— ゲートウェイ —] の [Azure] ページを開きます。このページにある［登録］をクリックして、ゲートウェイの登録を開始します。



2. ［ゲートウェイを Azure に登録する 1. デバイスにログイン］のページが表示されるので、[コードをコピーします] をクリックし、表示されているデバイスコードをクリップボードにコピーします。次に、［デバイスにログインします。］のリンクをクリックします。

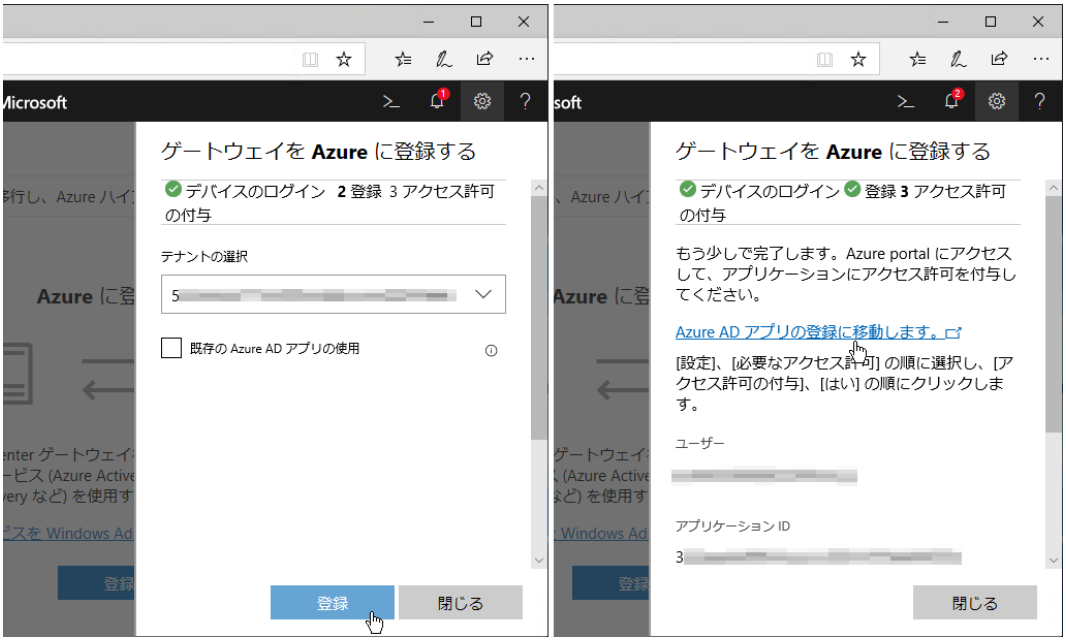


3. 別のウィンドウ（またはタブ）に［コードの入力］ページが表示されるので、先ほどクリップボードにコピーしたコードを貼り付けます。続いて、Microsoft Azure の「アカウントにサインイン」ページが表示されるので、Azure アカウントの資格情報を入力してサインインを完了します。

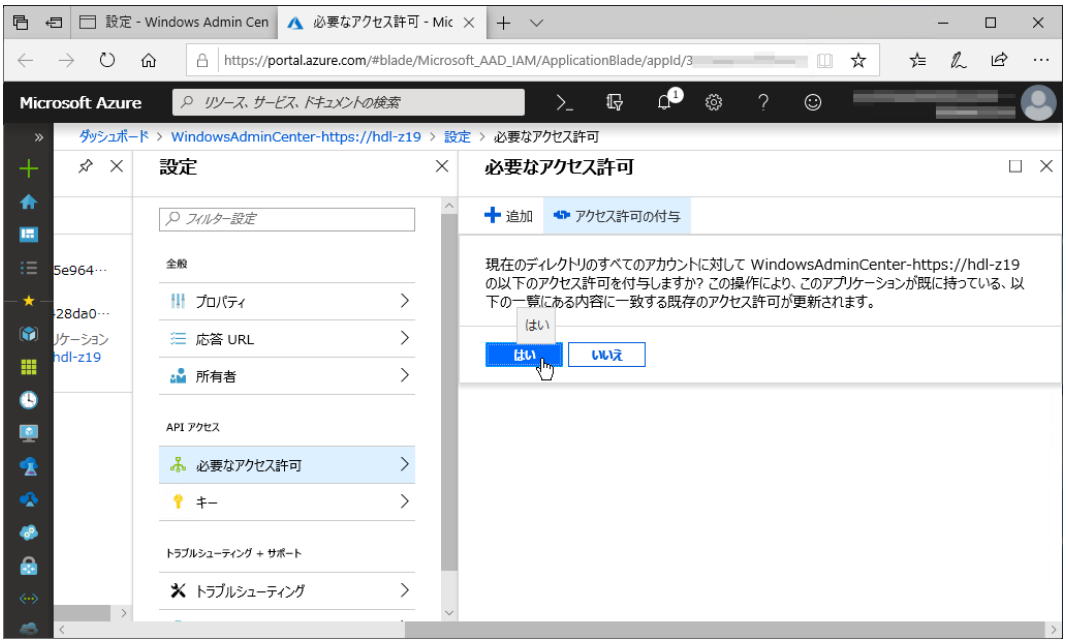


4. 「デバイスの Microsoft Azure PowerShell アプリケーションにサインインしました。このウィンドウは閉じて構いません」と表示されたら、「アカウントにサインイン」ページのウィンドウ（またはタブ）を閉じ、Windows Admin Center の先ほどのページに戻ります。

5. ［ゲートウェイを Azure に登録する 2. 登録］に切り替わるので、テナントの選択を確認し（Azure Active Directory のディレクトリが複数ある場合は適切なテナント ID を選択してください）、［登録］をクリックします。［ゲートウェイを Azure に登録する 3. アクセス許可の付与］に切り替わるので、［Azure AD アプリの登録に移動します。］リンクをクリックします。



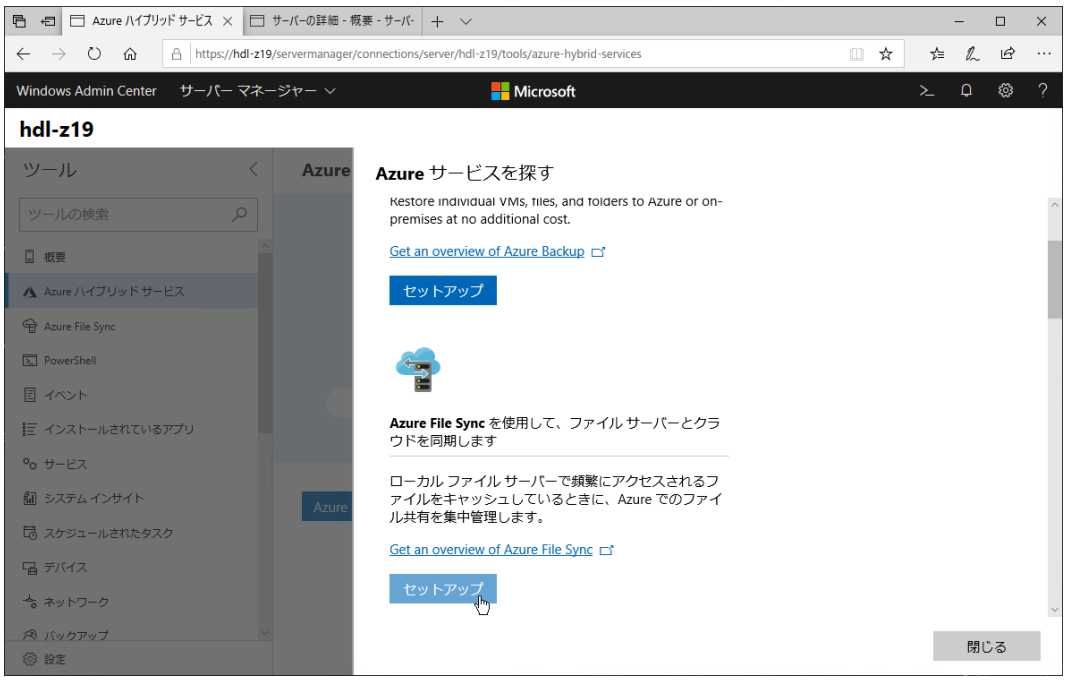
6. ［Azure AD アプリの登録に移動します。］リンクをクリックすると、別のウィンドウ（またはタブ）に Azure ポータルの該当ページが開くので、［設定］―［必要なアクセス許可］の順番にクリックし、［アクセス許可の付与］をクリックして、最後に［はい］をクリックします。完了したら、Azure ポータルのウィンドウ（タブ）はここで閉じて構いません。



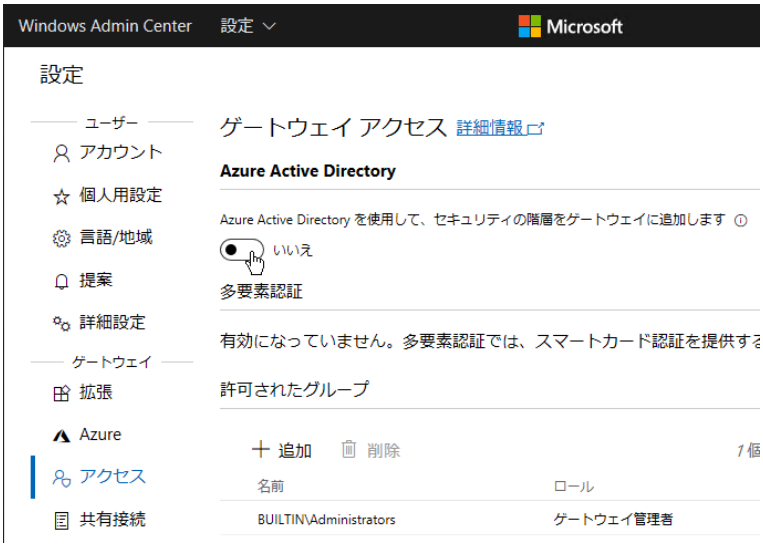
7. Windows Admin Center の［設定］の［Azure］ページに戻り、ゲートウェイの登録情報が表示されることを確認します。Azure のサービスの利用を停止して登録を解除するには、このページの［登録解除］をクリックします（登録を解除する前に利用中の各サービスでの利用の停止作業や、Azure ポータルでのリソースの削除などが必要です）。

以上で Azure へのゲートウェイの登録が完了しました。Windows Admin Center のサーバー管理ページの［Azure ハイブリッドサービス］を開くと、［Azure サービスを探す］をクリックして、Windows Admin Center でサポートされる Azure サービスのセットアップを開始することができます。Azure サービスのセ

ットアップは、関連する個別の管理ページ（[更新プログラム]、[バックアップ]、[Azure File Sync] など）から開始することもできます。



Azure Active Directory の認証によるゲートウェイ接続のセキュリティ強化について



ゲートウェイモードの Windows Admin Center を Microsoft Azure と統合すると、ゲートウェイの Windows Admin Center サイトへの接続時の認証に加え、Azure Active Directory の ID 認証（多様初認証やスマートカード認証にも対応）を要求できるようになります。ゲートウェイへのアクセスに Azure Active Directory の ID 認証を追加するには、[設定]（⚙アイコン）の [― ゲートウェイ ―] の下にある［アクセス］ページを開き、［Azure Active Directory を使用して、セキュリティの階層をゲートウェイに追加します］を［はい］に切り替え、指示された設定を Azure Active Directory 側で行います。

2.2 Azure Update Management による更新管理の一元化

Windows Admin Center の［更新プログラム］ページでは、管理対象のサーバーの更新プログラムのチェックを手動で開始し、不足している更新プログラムを評価した上で、更新プログラムのインストールを手動

で開始することができます。更新プログラムのインストールを完了するために再起動が必要になる場合は、再起動の開始時刻をスケジュールすることが可能です。

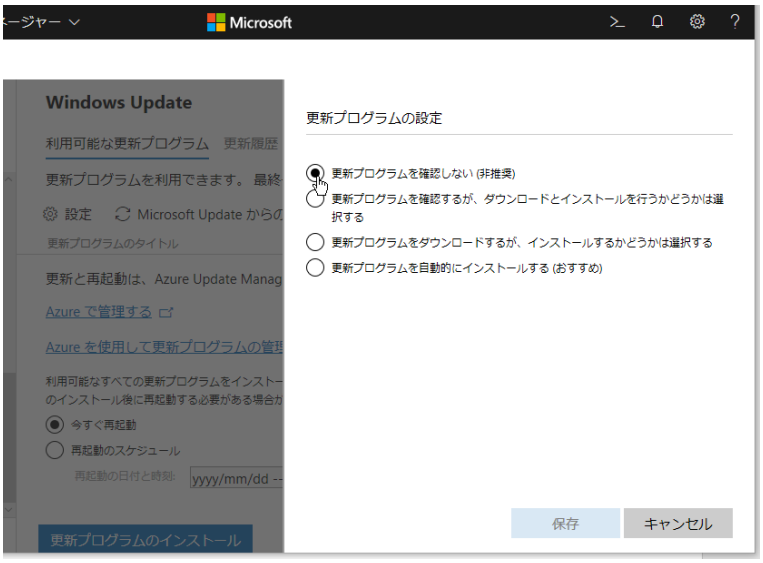
Windows Admin Center の［更新プログラム］ページの更新管理機能は、Azure Update Management に切り替えることが可能です。Azure Update Management に切り替えることで、1 台以上の管理対象に対する更新プログラムのインストールの開始をスケジュールすることができるため、業務時間外に更新プログラムのインストールと再起動までを自動化することが可能です。Azure Update Management は、Azure ポータル（https://portal.azure.com/）の［Automation アカウント］ブレードにある［更新プログラムの管理］ページで更新ステータスの評価やスケジュールを管理することができる他、最大 500 台（このガイド制作時点）までのオンプレミスおよび Azure 上の複数のサーバーを一元的に管理することができます。

LAN DISK Z は、Windows Admin Center の［更新プログラム］ページと、Azure Update Management のどちらで管理することもできます。

Windows Update の自動更新の無効化

更新プログラムの管理を Windows Admin Center や Azure Update Management で行う場合は、サーバー側の Windows Update で自動更新をオフ（手動更新）にしてください。自動更新が有効になっていると、意図しないタイミングでインストールが開始されたり、再起動が行われたりする場合があります。

Windows Admin Center の［更新プログラム］ページの［設定］をクリックすると、サーバー側の Windows Update の現在の設定の確認と変更が可能です。Windows Admin Center で管理するためには、［更新プログラムを確認しない（非推奨）］（Windows Server の既定）を選択します。

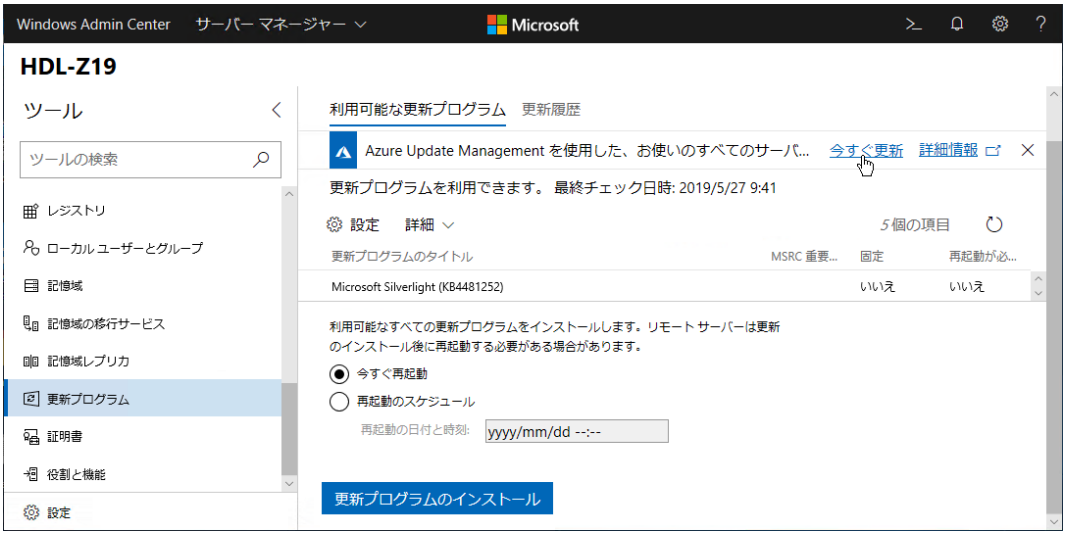


更新管理を Azure Update Management に切り替える

Azure Update Management は、通常、Azure ポータルを使用してオンプレミスのサーバーのエージェントや Azure 仮想マシンの更新をセットアップします。Windows Admin Center を利用すると、ここで示すようにオンプレミスの更新管理環境を簡単に Windows Admin Center だけでセットアップを完了できます。

1. Windows Admin Center で管理対象の LAN DISK Z に接続し、［Azure ハイブリッドサービス］ページの［Azure サービスを探す］をクリックして［Azure Update Management を使用すると、すべてのサーバー上の更新プログラムを一元管理できます］を探し、［セットアップ］をクリックします。または、

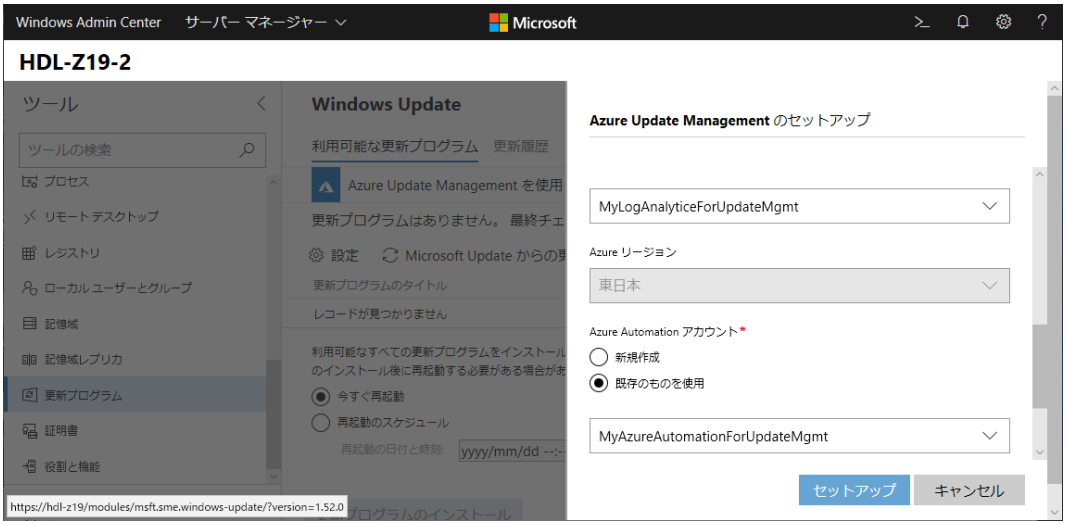
Windows Admin Center の［更新プログラム］ページを開き、［Azure Update Management を使用した、お使いのすべてのサーバーにおける一元管理の更新プログラム］のメッセージの横にある［いますぐ更新］リンクをクリックします。



2. ［アカウントにサインイン］ページがポップアップウィンドウで開かれた場合は（サインインされた状態でない場合）、Azure アカウントの資格情報を入力してサインインします。

3. ［Azure Update Management のセットアップ］が開くので、以下の情報を入力または選択して［セットアップ］をクリックします。はじめての利用（1 台目のセットアップ）の場合は［新規作成］、2 台目以降は［既存のものを使用］を選択してセットアップすることで、Azure ポータルの同じ［更新プログラムの管理］ページで複数のサーバーを一元管理できるようになります。Azure リージョンはすべて同じ場所にしてください。

Azure サブスクリプション	Azure アカウントのサブスクリプションを選択
リソースグループ（新規作成または既存のものを使用）	リソースグループ名
	Azure リージョン（例：東日本）
Log Analytics ワークスペース（新規作成または既存のものを使用）	一意のワークスペース名
	Azure リージョン（例：東日本）
Azure Automation アカウント（新規作成または既存のものを使用）	アカウント名
	Azure リージョン（例：東日本）

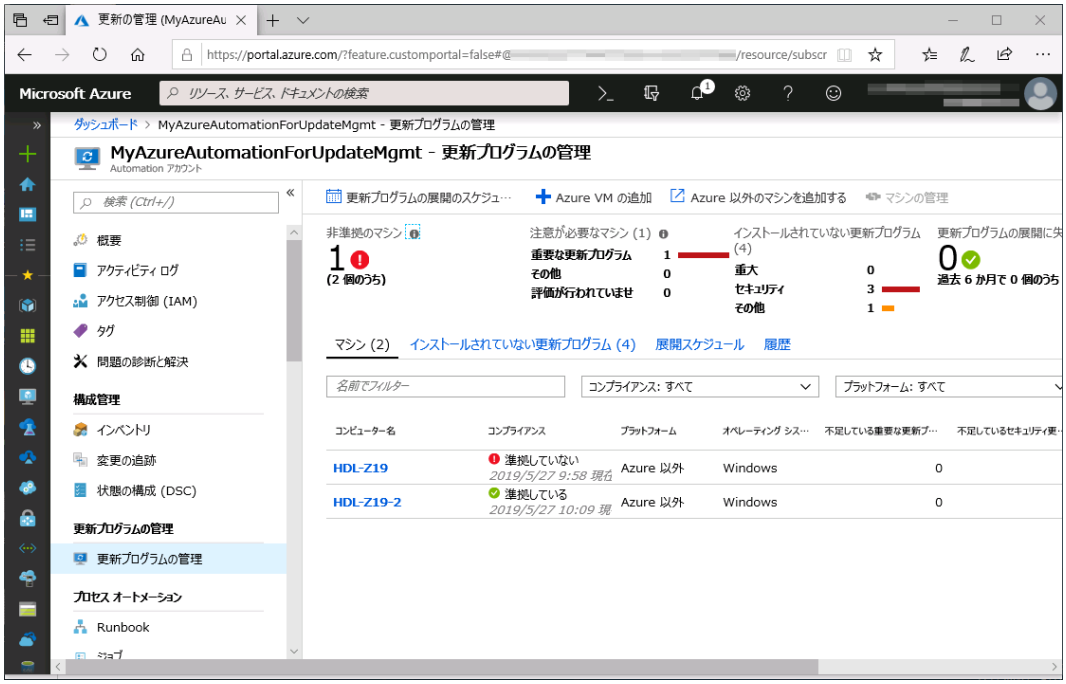


4. セットアップは数分で完了します。セットアップが完了すると［Update Management のセットアップ Update Management が正常にセットアップされました］という通知メッセージが表示され、［更新プログラム］ページは［更新と再起動は、Azure Update Management によって管理されています］に変化します。また、Azure ポータルの［更新プログラムの管理］ブレードにアクセスするための［Azure で管理する］リンクが提供されます。セットアップが失敗した場合は、エラー情報を確認して、エラーの原因（一意でない名前の使用など）を取り除いてから再セットアップしてください。

5. 更新を一元管理したい LAN DISK Z の NAS デバイスやサーバーが他にある場合は、同じリソースグループ、同じ Log Analytics ワークスペース、同じ Azure Automation アカウントを指定して Azure Update Management をセットアップします。

サーバーの更新ステータスを評価する

Windows Admin Center の［更新プログラム］ページにある［Azure で管理する］リンクをクリックすると、Azure ポータルのセットアップ先の［Automation アカウント］ブレード内の［更新プログラムの管理］ページが開きます。管理者はこのページで 1 台以上のサーバーの更新を一元管理することができ、不足している更新プログラムの数やその詳細情報の確認や、更新プログラムの展開スケジュールの作成、展開スケジュールの実行履歴の確認などを行います。



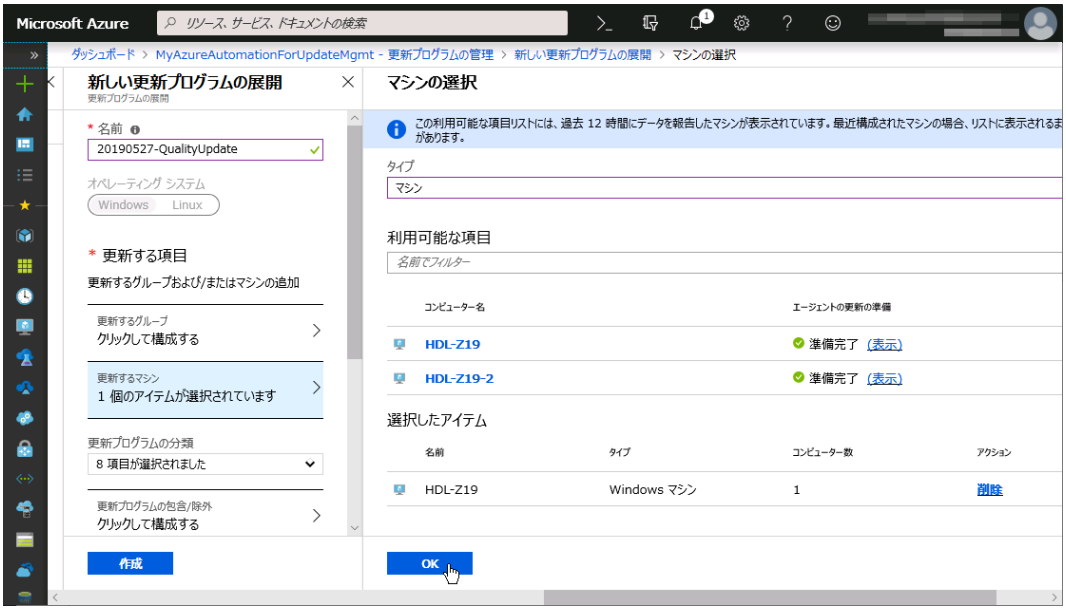
更新プログラムの展開スケジュールを作成する

1 台以上の管理対象に不足している更新プログラムがある場合は、一度だけの更新プログラムの展開スケジュールを作成して、更新プログラムのインストールの開始時刻を指定し、自動実行させることができます。毎月の更新を自動実行するように、実行スケジュールを日単位の間隔指定、週単位の間隔指定（週と曜日の指定）、または月単位の日付または曜日指定（特定の日付、月の最終日、または第 1～4／最終の曜日指定）の展開スケジュールを作成し、繰り返し実行させることもできます。

例えば、一度だけの更新プログラムの展開スケジュールを作成するには、次の手順で操作します。

1. ［更新プログラムの展開スケジュール］をクリックし、［新しい更新プログラムの展開］ページを開きます。展開スケジュールに分かりやすい名前を付け、［オペレーティングシステム］として［Windows］を選択します。

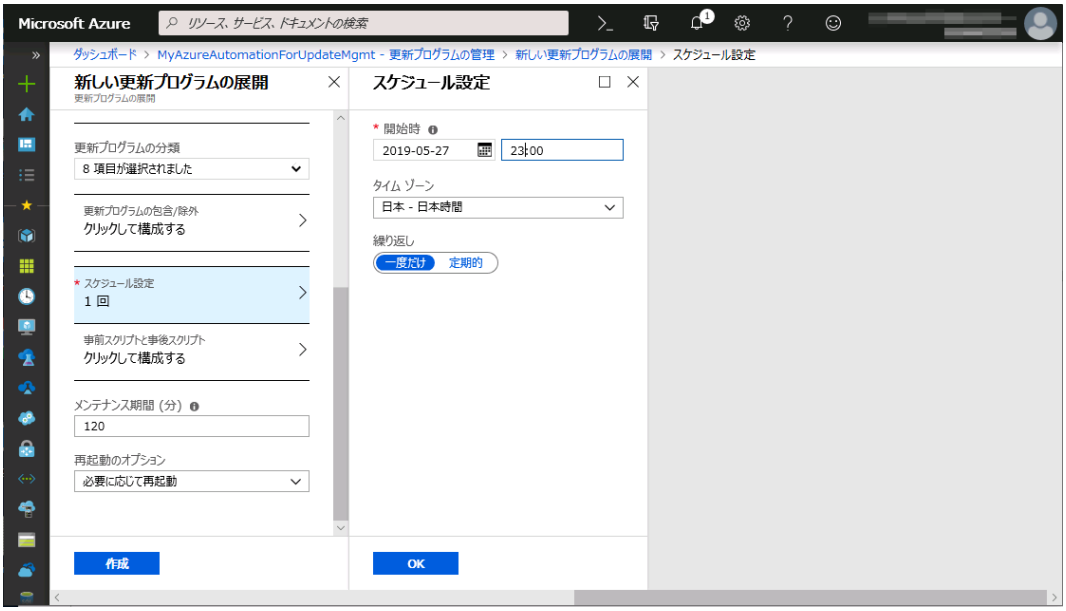
2. ［更新する項目］の下にある［更新するマシン（クリックして構成する）>］をクリックして開き、［タイプ］のドロップダウンリストから［マシン］を選択します。登録済みの管理対象のサーバーが一覧表示されるので、1 台以上の更新対象を選択し、［OK］をクリックします。なお、［更新するグループ（クリックして構成する）>］はクエリに基づいて動的に対象を指定することもできますが、オンプレミスのサーバーについてはこのガイドの制作時点でプレビュー機能であるため、このガイドでは説明しません。



［エージェントの更新の準備］列の確認

更新プログラムの展開スケジュールを作成する際には、［エージェントの更新の準備］列に［準備完了］と表示されていることを確認してください。長時間、Azure Update Management サービスに接続していないサーバーでは、エージェントが古くなっており、更新プログラムを受け取るためにはエージェントの状態の修正が必要になる場合があります。

3. ［スケジュール設定（クリックして構成する）>］をクリックし、［スケジュール設定］を開いて更新プログラムのインストールを開始する時刻を選択します。一度だけのスケジュールを作成する場合、［開始時］で日付と時刻を指定し、［タイムゾーン］を選択して、［繰り返し］の［一度だけ］を選択し、［OK］をクリックします。



6. 最後に、[メンテナンス期間（分）] と [再起動のオプション] を指定し、[作成] をクリックします。[メンテナンス期間（分）] は再起動を開始してから、更新プログラムのインストールを開始してから再起動が完了するまで Azure Update Management のサービスが待機する期間です。既定は 120 分ですが、30 分～180 分（6 時間）の範囲で指定します。メンテナンス期間の最後の 20 分は再起動のために確保されているため、メンテナンス期間が短いと一部の更新プログラムがインストールされない可能性があることに注意してください。[再起動のオプション] としては、[必要に応じて再起動]（既定）、[再起動しない]、[常に再起動]、[再起動のみ－更新プログラムのインストールは行われません] の 4 つから選択できます。

以上で一度だけの展開スケジュールの作成が完了しました。スケジュール済みの展開スケジュールは、[更新プログラムの管理] ページの [展開スケジュール] タブで、展開スケジュールの実行状況や実行結果は [履歴] タブで確認することができます。

更新ステータスの評価が反映されるまでの時間について

[更新プログラムの管理] ページの [マシン] タブの [コンプライアンス] 列に表示される情報は、Windows の場合は最後の 12 時間に受信した更新プログラムの評価データに基づいています（Linux の場合は最後の 3 時間）。更新プログラムの展開スケジュールによって更新プログラムがインストールされると新しい評価データが Azure Update Management サービスに報告されますが、[コンプライアンス] 列に反映されるまではメンテナンス期間（30 分～6 時間）が終了するまでかかる場合があります。

2.3 Azure Backup によるクラウドバックアップ

Windows Admin Center の [バックアップ] ページは、Azure Backup と統合されたクラウドベースのバックアップの管理専用のものです。一度、Azure Backup をセットアップし、バックアップスケジュールの設定を行うと、スケジュールに従って自動的にバックアップが行われるようになります。

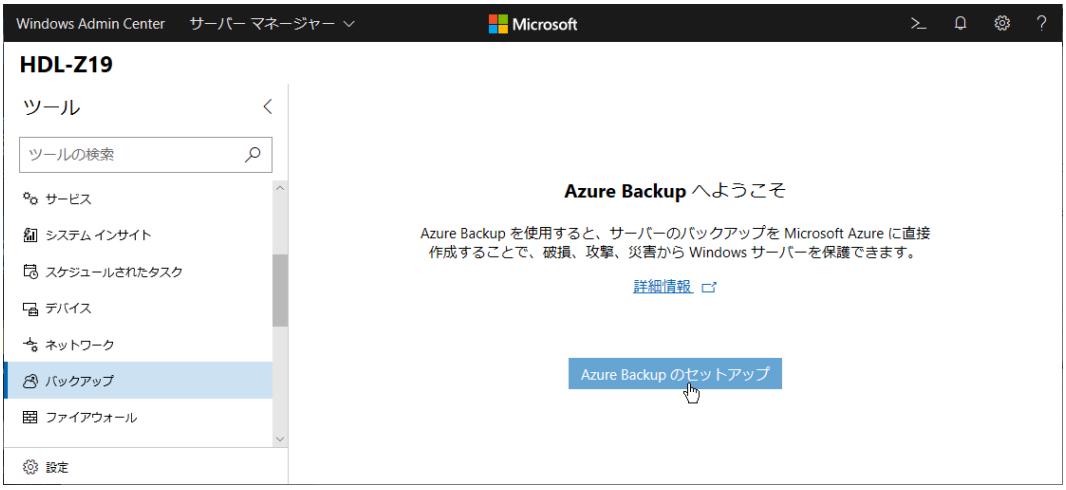
Azure Backup を利用すると、1 台以上のオンプレミスの Windows Server のデータ、Azure 上の Windows および Linux 仮想マシン、および Azure ストレージのデータを一元的に保護できます。Windows Server IoT 2019 for Storage を搭載する LAN DISK Z 上のデータは、Azure Backup で保護することができます。

Azure Backup のセットアップ

通常の方法でオンプレミスのサーバーを Azure Backup で保護するように Azure Backup をセットアップするには、Azure ポータルで Recovery Services コンテナーを作成し、Azure ポータルからエージェントをダウンロードしてオンプレミスのサーバーにインストールした上で、エージェントとともにインストールされる [Microsoft Azure Backup] スナップインを使用してサーバーの登録やバックアップスケジュールの作成を行います。Windows Admin Center を利用すると、ここで示すようにオンプレミスのサーバーのクラウドバックアップを Windows Admin Center だけで簡単にセットアップできます。

1. Windows Admin Center で管理対象の LAN DISK Z の NAS デバイスに接続し、[Azure ハイブリッド

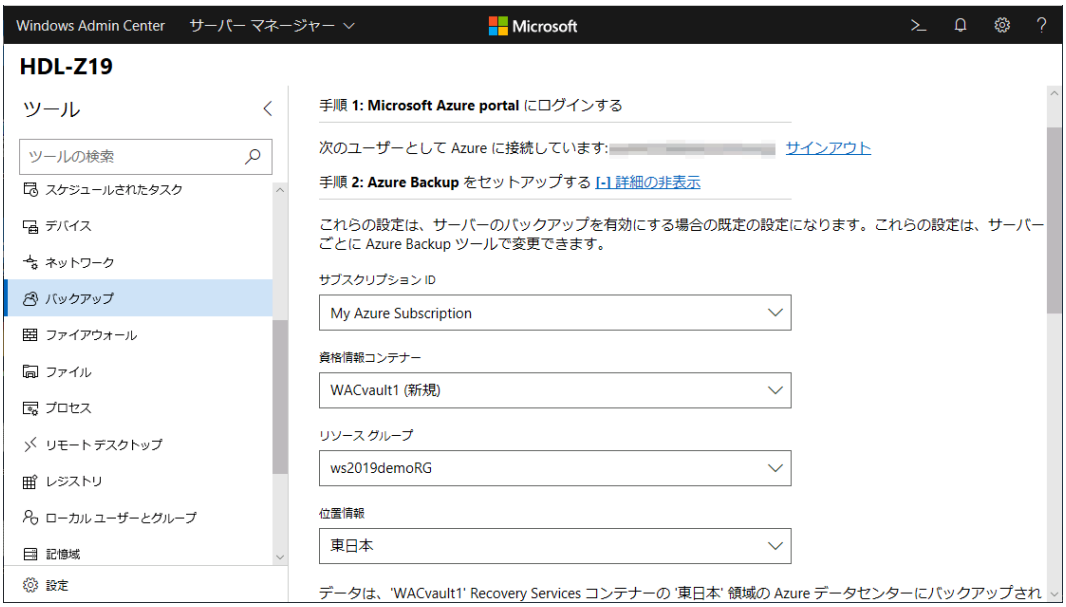
サービス］ページの［Azure サービスを探す］またはをクリックして［Simplify data protection and protect against ransomware with Azure Backup（Azure Backup を使用して、データ保護を簡素化し、ランサムウェアから保護します）］を探し、［セットアップ］をクリックします。または、Windows Admin Center の［バックアップ］ページを開き、［Azure Backup のセットアップ］をクリックします。



2. ［アカウントにサインイン］ページがポップアップウィンドウで開かれた場合は（サインインされた状態でない場合）、Azure アカウントの資格情報を入力してサインインします。

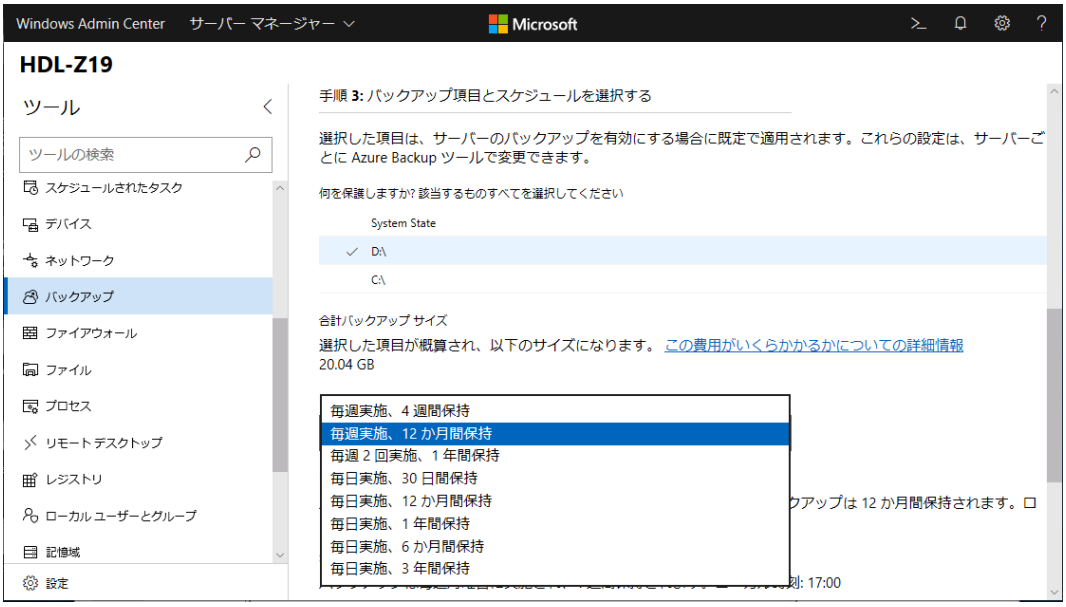
3. ［Azure Backup］ページが開くので、［手順 1: Microsoft Azure portal にログインする］で Azure アカウントのサインイン状態を確認します。

4. ［手順 2: Azure Backup をセットアップする］で［サブスクリプション ID］を確認し、［資格情報コンテナー］、［リソースグループ］、［位置情報］を選択します。Azure Backup をはじめて利用する場合（1 台目の保護設定の場合）、［資格情報コンテナー］は［名前（新規）］を選択してください。［リソースグループ］は［名前（新規）］または既存のリソースグループのいずれかを選択します。［位置情報］では Azure リージョンを選択します。バックアップデータを国内データセンターに保持したい場合は、［西日本］または［東日本］リージョンを選択してください。



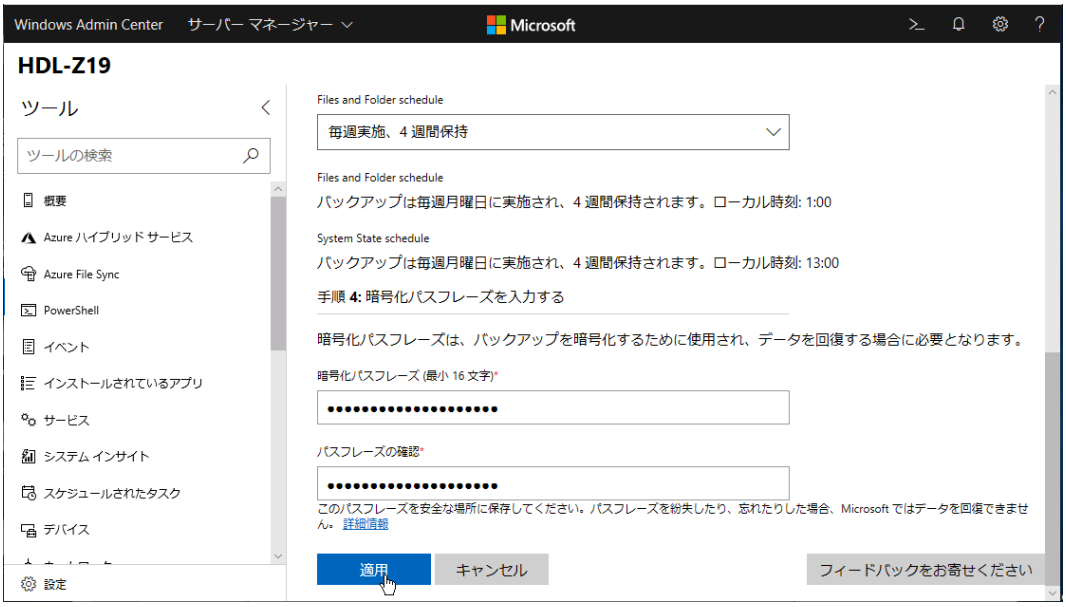
2 台目以降の保護を行う場合は、既存の［資格情報コンテナー］と［リソースグループ］から選択することで、複数サーバーのバックアップのコスト管理（料金計算）を一本化できます。

5. ［手順 3: バックアップ項目とスケジュールを選択する］の［何を保護しますか？該当するものすべてを選択してください]の一覧から保護対象のボリュームやシステム状態(System State)を選択します。保護対象を選択すると、[合計バックアップサイズ] にバックアップ対象の容量が示され、コストの見積もりに利用できます。

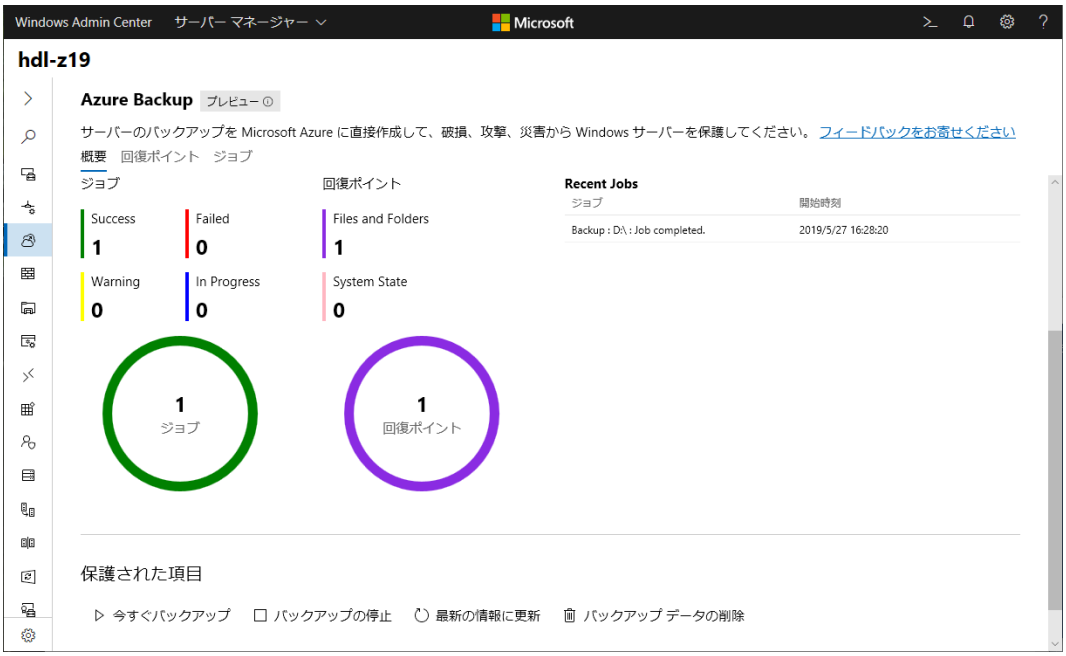


> システム状態のバックアップについて
>
> システム状態（System State）のバックアップは、サーバーのフルバックアップを目的としたものではなく、ベアメタル回復（まっさらなディスクへのシステムの回復）には使用できません。システム状態のバックアップは、Active Directory のディレクトリ、証明書サービス、ファイルサーバーのフェールオーバークラスターの重要な設定設定やファイルアクセスを保護するポリシー設定、IIS Web サーバーのメタベースの保護を目的としたものです。

6. バックアップデータは暗号化された上でクラウドに送信され、暗号化された状態のままクラウドストレージに保存されます。最後に［手順 4: 暗号化パスフレーズを入力する］で暗号化に使用される 16 文字以上のパスフレーズを 2 回入力します。このパスフレーズはバックアップ元とは別のサーバーにデータを回復する際に必要となるため、電子的または紙の控えを残す際には、安全な場所に保管するようにしてください。クラウド側にはパスフレーズは保存されないため、パスフレーズを紛失すると、データを回復する最後の手段を失うことになります。



7. Windows Admin Center が Azure 側の Recovery Services コンテナーの作成や、保護対象のサーバーへの Azure Backup エージェントのインストール、サービスへのサーバーの登録、バックアップのスケジュールおよびポリシー設定などを行います。セットアップが完了すると、Windows Admin Center の［バックアップ］ページに Azure Backup の登録情報やバックアップジョブの実行ステータス、回復ポイントの数などが表示されるようになります。また、[保護された項目] にある [▷今すぐバックアップ] をクリックすると、スケジュールされた日時を待たずにバックアップを開始することができます。なお、初回のバックアップは全データを転送する必要があるため、通常よりも時間がかかります。2 回目以降のバックアップは、増分バックアップとなるため、比較的短時間で終了します。

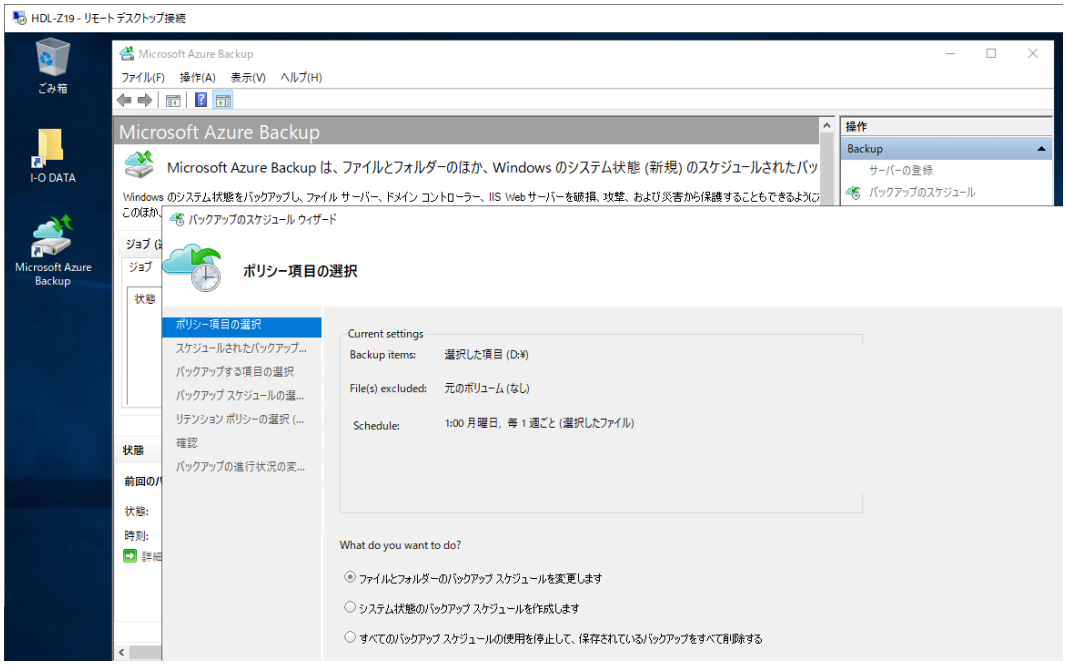


バックアップ項目の詳細なカスタマイズ

Windows Admin Center の［バックアップ］ページでは、バックアップ項目やスケジュール設定が簡素化されており、詳細な設定を行えません。ファイルやフォルダー単位のバックアップ、バックアップからの除

外、詳細なスケジュールの調整を行いたい場合は、Azure Backup の標準の管理ツールである［Microsoft Azure Backup］スナップインを使用します。

管理対象のサーバーにリモートデスクトップ接続し、デスクトップにある［Microsoft Azure Backup］スナップインをクリックして、[操作] ペインの [バックアップのスケジュール] をクリックします。Windows Admin Center の［バックアップ］ページでセットアップしたバックアップ設定は、ここから詳細に編集することができます。

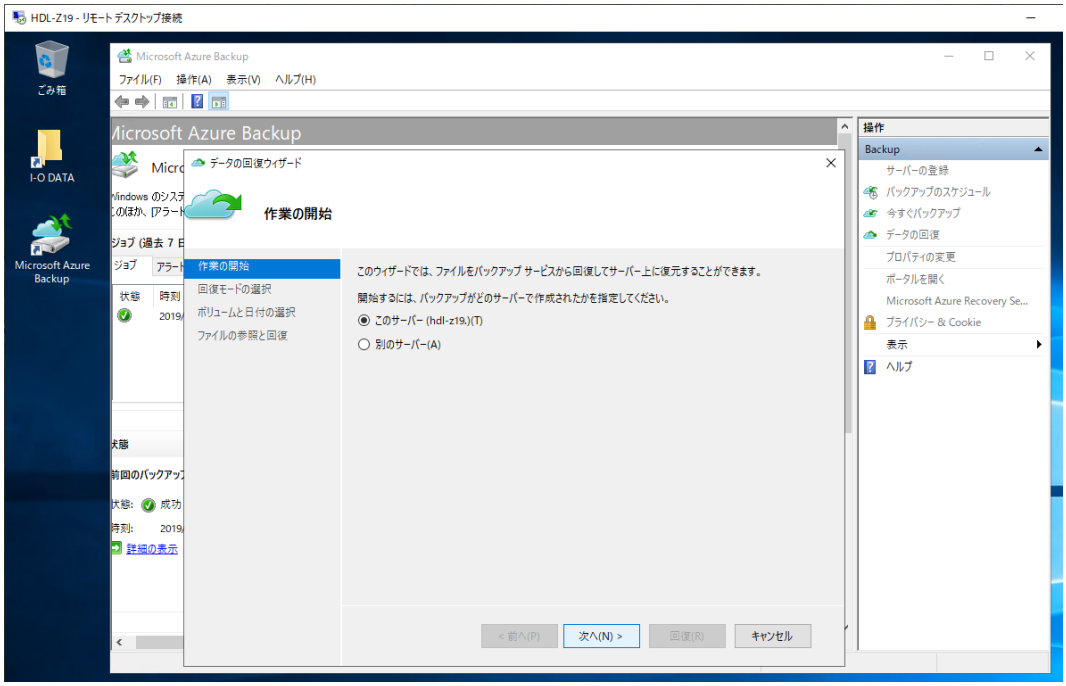


データ重複除去で最適化されたデータのバックアップについて

データ重複除去が有効化されたボリュームまたはボリューム上のフォルダーを Azure Backup でバックアップする場合、最適化されたデータをそのままバックアップすることはできません。Azure Backup エージェントはデータ重複除去で最適化されたデータを通常のデータに変換し、そのデータをバックアップ用に最適化（圧縮）および暗号化した上で、Recovery Services コンテナーに転送します。そのため、バックアップデータのサイズがディスクの使用サイズよりも大きくなる可能性があります。

バックアップからの回復

Azure Backup でクラウドにバックアップされたデータは、元の場所または別の場所に回復（復元）することができます。ただし、Windows Admin Center の［バックアップ］ページは、バックアップからの回復操作のための機能を提供しません（2019 年 6 月時点のバージョンの拡張機能の場合）。回復操作は、管理対象のサーバーに Azure Backup エージェントとともにインストールされた［Microsoft Azure Backup］スナップインを使用して行います。［Microsoft Azure Backup］スナップインの［操作］ペインにある［データの回復］をクリックすると、［データの回復ウィザード］が開始するので、このウィザードを使用してバックアップからボリューム（またはシステム状態）を回復します。



同じサーバーにデータを回復する場合、ボリューム単位で同じ場所または別の場所に回復することができます。バックアップに含まれるボリュームをローカルドライブにマウントして、コピー操作でファイルやフォルダーを個別に回復することもできます。

別のサーバーにデータを回復する場合は、Azure ポータルの［Recovery Services コンテナー］ブレードの［はじめに］からダウンロードできる資格情報コンテナーの資格情報ファイル（拡張子.VaultCredentials、有効期限 2 日間）と、サーバーの登録時に設定した暗号化パスフレーズの入力が必要になります。

2.4　Azure File Sync によるクラウドストレージとの同期

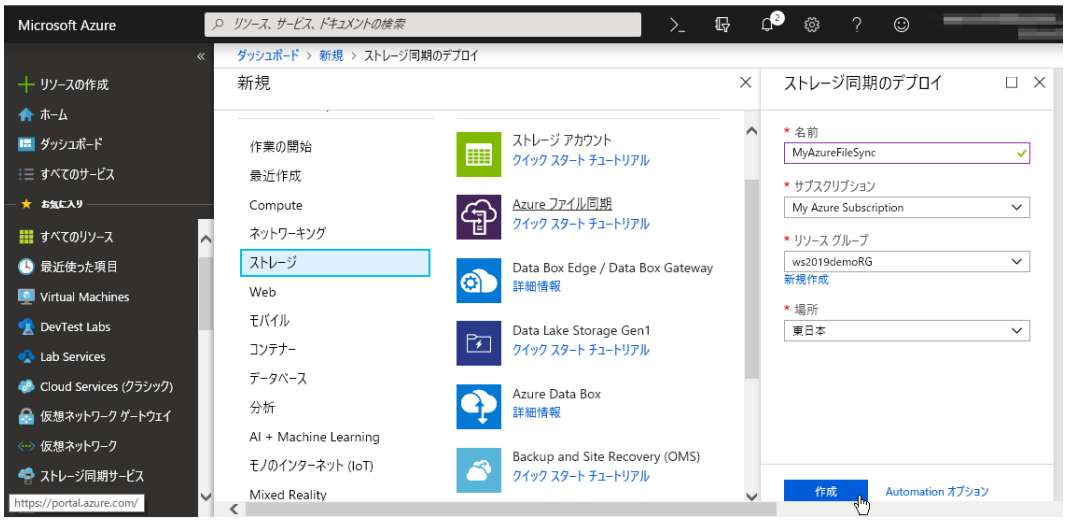
Azure File Sync は、オンプレミスの Windows Server と Microsoft Azure のクラウドストレージである Azure ファイル共有（File サービス）を双方向に同期する、ストレージ同期サービスです。Azure File Sync を利用するには、クラウド側のエンドポイントとオンプレミス側のエンドポイントをそれぞれセットアップする必要があります。Windows Admin Center の［Azure File Sync］ページは、Azure File Sync のオンプレミス側のエージェントの展開とセットアップを簡素化します。

Windows Server IoT 2019 for Storage を搭載する LAN DISK Z は、Azure File Sync と連携することができます。LAN DISK Z と Azure File Sync を連携することにより、オンプレミスとクラウドの両方でデータを多重化できます。また、オンプレミスの NAS デバイスが障害や災害の影響で利用できない場合でも、Azure ファイル共有という代替手段を使用したファイルアクセスをエンドユーザーに提供することができ、業務への影響を最小限にできます。SMB v3 でのみアクセス可能な Azure ファイル共有のマルチプトコル対応（SMB v1/v2/v3、NFS、FTP など）とネットワーク遅延の改善のために、NAS デバイスをキャッシュサーバーとして利用するというシナリオもあります。、

Azure File Sync サービスの事前準備（Azure ポータル）

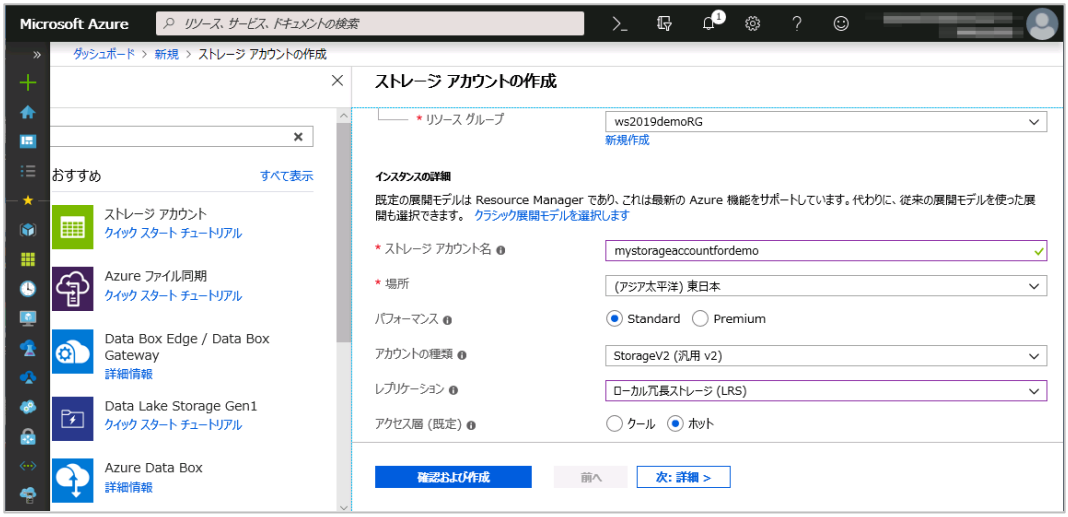
Azure File Sync を利用するには、事前に Azure File Sync のクラウド側のサービスを準備しておく必要が

あります。それには、Azure ポータル（https://portal.azure.com/）に Azure アカウントの資格情報でサインインし、[＋リソースの作成] をクリックして、[ストレージ] – [ファイル Azure ファイル同期] をクリックします。[ストレージ同期のデプロイ] でサービスの名前とリソースグループ（新規または既存）、場所（Azure リージョン）を選択し、[作成] をクリックします。Azure リージョンは、次に準備する Azure ストレージアカウントと一致させる必要があります。データを国内データセンターに保持したい場合は、[西日本] または [東日本] リージョンを選択してください。

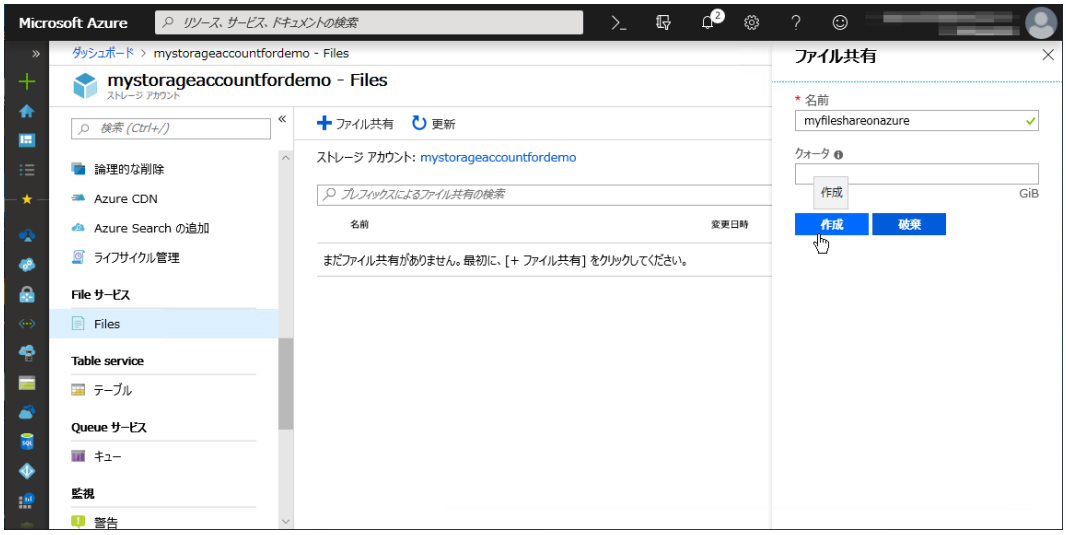


Azure ストレージアカウントの事前準備（Azure ポータル）

Azure File Sync は、オンプレミスのファイルやフォルダーを、Azure ファイル共有（Files サービス、汎用 v2 または汎用 v1 の Azure ストレージアカウントでサポート）との間で同期します。同期先となる Azure ファイル共有がまだない場合は、事前に準備しておきます。それには、Azure ポータル（https://portal.azure.com/）に Azure アカウントの資格情報でサインインし、[＋リソースの作成] をクリックして、[ストレージ] – [ストレージアカウント] をクリックします。[ストレージアカウントの作成] でリソースグループ（新規または既存）を選択し、[ストレージアカウント名] に一意の名前（小文字と数字のみ）を入力して、[場所]（Azure リージョン）と [アカウントの種類]（汎用 V2 または汎用 v1）を選択して作成します。データを国内データセンターに保持したい場合は、[西日本] または [東日本] リージョンを選択してください。冗長化オプションなどその他の項目については、適宜構成してください。



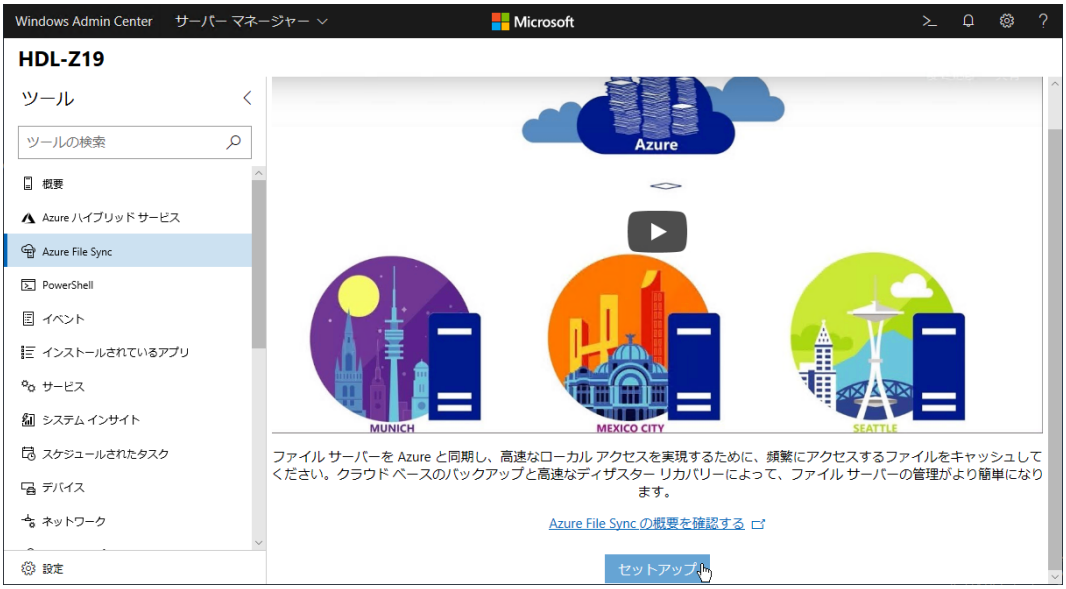
ストレージアカウントの展開が完了したら、そのリソースに移動し、[File サービス – Files] ページを開きます。[＋ファイル共有] をクリックして [名前] を入力し（小文字、数字、ハイフンのみ）、ファイル共有を作成します。



Azure File Sync のセットアップ（Windows Admin Center）

続いて、Windows Admin Center の [Azure File Sync] ページを使用してオンプレミス側のサーバーを準備します。オンプレミス側では、サーバーへの Azure File Sync エージェントのインストール、Azure File Sync サービスへのサーバーの登録などの作業が必要ですが、Windows Admin Center がこれらの作業を簡素化してくれます。

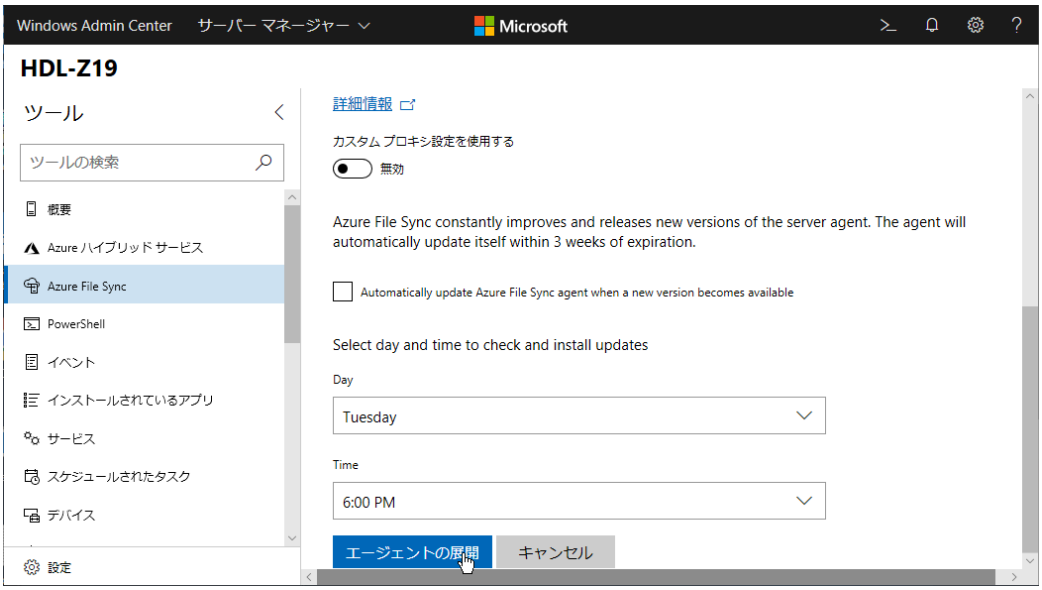
1. Windows Admin Center で管理対象の LAN DISK Z に接続し、[Azure ハイブリッドサービス] ページの [Azure サービスを探す] またはをクリックして [Azure File Sync を使用して、ファイルサーバーとクラウドを同期します] を探し、[セットアップ] をクリックします。または、Windows Admin Center の [Azure File Sync] ページを開き、[セットアップ] をクリックします。



2. [1. 同期エージェントの展開] ページに [このサーバーには、Azure File Sync エージェントがインス

トールされていません］と表示されるので、［次へ］をクリックします。

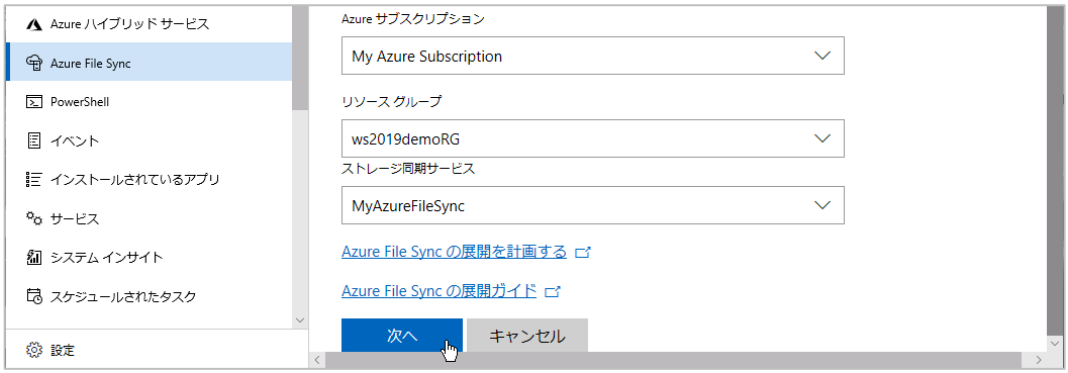
3. ［更新 – このサーバーで Microsoft Update をオプトインする］を選択します。［カスタムプロキシを設定する］は、サーバーのインターネットアクセス環境に合わせて構成してください。［Automatically update Azure File Sync agent when a new version becomes available（新しいバージョンが利用可能になったときに Azure File Sync エージェントを自動的に更新する）］をチェックし、新しいバージョンの確認とインストールを行う曜日と時刻を指定して（後で構成するバックアップスケジュールと重ならないように）、［エージェントの展開］をクリックします。



4. Azure File Sync エージェントが管理対象のサーバーにダウンロードおよびインストールされます。エージェントの展開が完了すると、［Azure File Sync エージェントが正常にダウンロードされ、インストールされました］という通知があり、［1. 同期エージェントの展開］ページの［エージェントの展開］が［次へ］に切り替わるので、［次へ］をクリックします。

5. ［アカウントにサインイン］ページがポップアップウィンドウで開かれた場合は（サインインされた状態でない場合）、Azure アカウントの資格情報を入力してサインインします。Azure アカウントのサインインが完了すると、［2. ストレージ同期サービス］に移動します。

6. ［2. ストレージ同期サービス］では、リソースグループを選択し、そのリソースグループに事前に準備しておいた Azure File Sync サービスを選択して、［次へ］をクリックします。

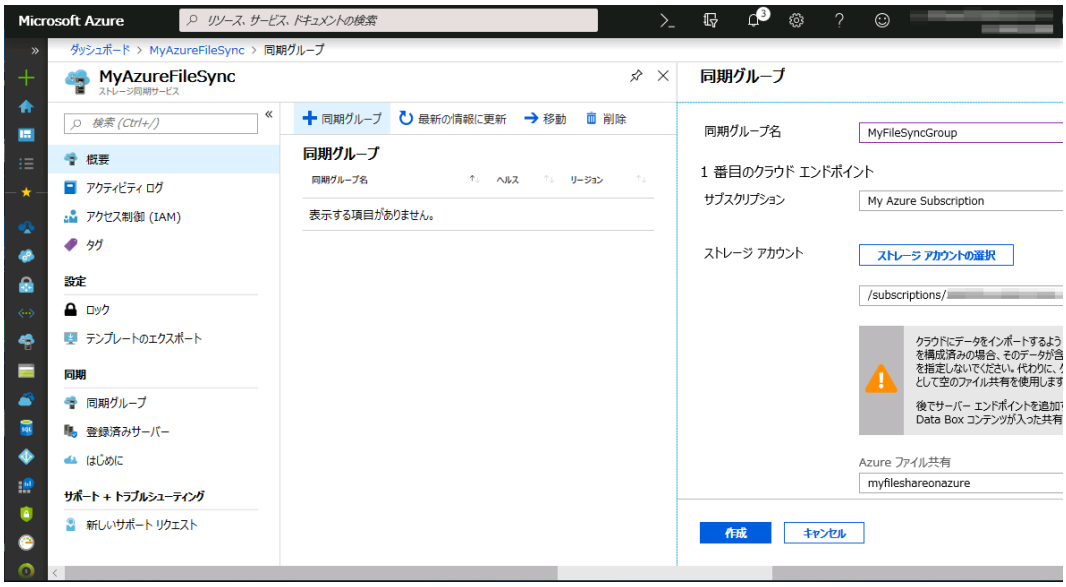


7. ［3. サーバーの登録］に移動するので、［サーバーの登録］をクリックして Azure File Sync サービスにこのサーバーを登録します。［サーバーがストレージ同期サービスに正常に登録されました］という通知が表示され、［3. サーバーの登録］の［サーバーの登録］が［完了］に切り替わるので、［完了］をクリックします。

同期グループの作成（Azure ポータル）

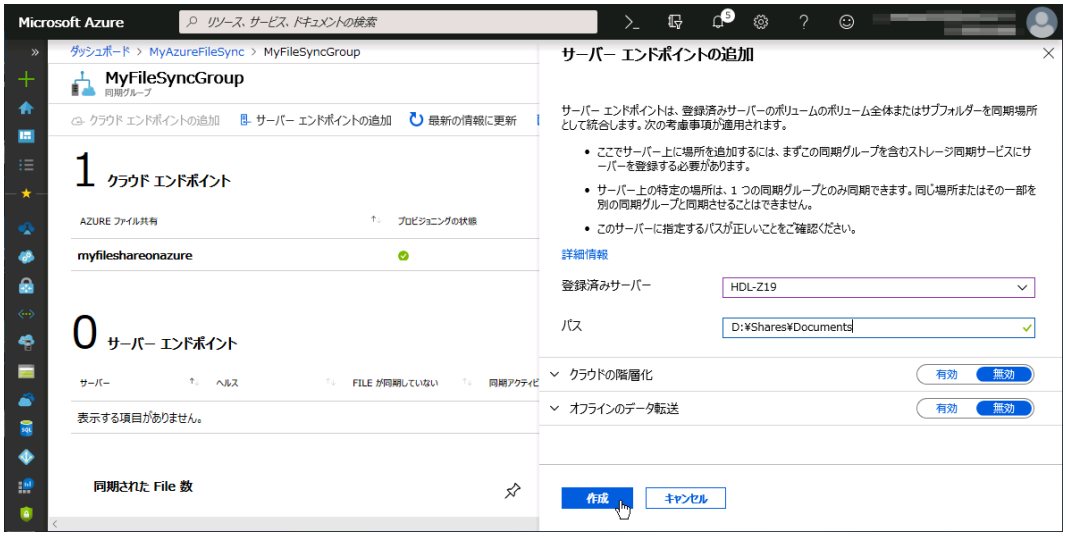
最後に、オンプレミスのエンドポイント（サーバー）とクラウドのエンドポイント（Azure ファイル共有）の同期ペアを定義する同期グループを作成します。

再び Azure ポータル（https://portal.azure.com/）に戻り、［ストレージ同期サービス］ブレードで Azure File Sync のサービスを開いたら、［＋同期グループ］をクリックします。［同期グループ名］に分かりやすい名前を入力し、［ストレージアカウントの選択］をクリックして、事前に準備しておいたストレージアカウントを選択し、Azure ファイル共有を選択します。［作成］をクリックすると、クラウドエンドポイントだけを含む同期グループが作成されます。

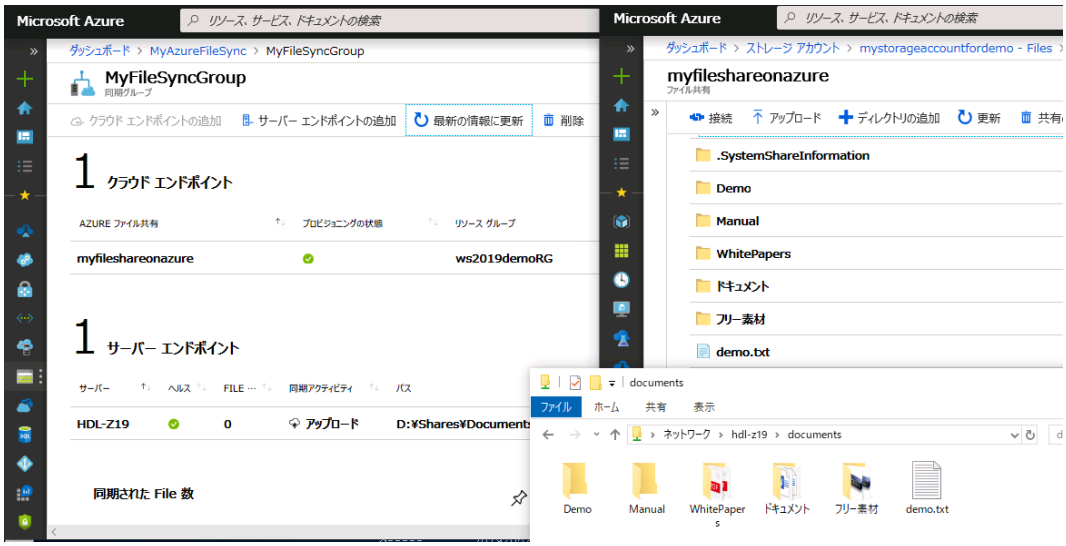


サーバーエンドポイントを追加するために、作成した同期グループを開いて［サーバーエンドポイントの追加］をクリックし、［登録済みサーバー］のドロップダウンリストからサーバー（Windows Admin Center から登録したサーバー）を選択して、同期するサーバーのローカルのディレクトリパス（ドライブ名:¥から）を入力し、［作成］をクリックします。

> クラウドの階層化について
>
> Azure File Sync の同期グループでは「クラウドの階層化」がサポートされます。クラウドの階層化とは、クラウドエンドポイント（Azure ファイル共有）に全データを保存し、サーバーエンドポイントにはアクセス頻度の高いファイルのみをキャッシュすることで、パフォーマンスへの影響を抑制しながら、オンプレミス側のストレージ使用を節約する機能です。



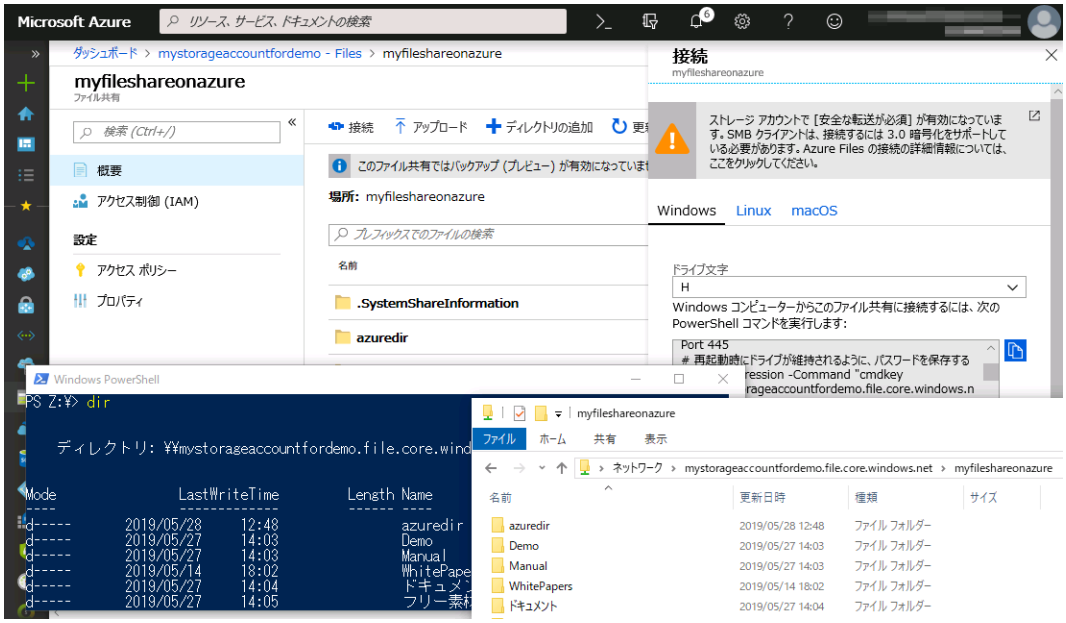
同期グループにサーバーエンドポイントが追加されると、クラウドエンドポイントに対する同期（アップロード）がスタートします。



> Azure ファイル共有に加えられた変更のオンプレミスへの同期について
>
> サーバーエンドポイントに対する変更は、即座に検出され、クラウドエンドポイントに対して同期（アップロード）されます。これに対して、Azure ポータルまたは SMB アクセスを使用してクラウドエンドポイントの Azure ファイル共有に加えられた変更は即座に行われることはありません。Azure ファイル共有に加えられた変更は、24 時間に 1 回実行されるクラウドエンドポイントに対する変更検出ジョブによって検出され、その後、サーバーエンドポイントに同期（ダウンロード）されます。

Azure ファイル共有へのアクセス

Azure ファイル共有には、SMB v3 クライアントのコマンドプロンプト、Windows PowerShell、エクスプローラーなどからインターネット経由でアクセスすることができます。その方法は、Azure ポータルで Azure ファイル共有の［接続］で確認することができます。



Azure ファイル共有にアクセスするためのファイアウォール設定について

Azure ファイル共有に SMB クライアントからアクセスするためには、経由するネットワークデバイスで出力方向の TCP ポート 445（Direct Hosting of SMB）の通信が許可されている必要があります。利用中のネットワークデバイスによっては（特に、一般家庭でも利用されるブロードバンドルーター）、TCP ポート 445 を含むインターネットへの SMB トラフィック（TCP ポート 139 や 445）を拒否する設定がされていることがあるので留意してください。

Azure ファイル共有をクラウド側でバックアップする（プレビュー）

Azure Backup は、Azure ファイル共有のスケジュールバックアップと回復をプレビュー機能としてサポートしています。Azure File Sync を使用してオンプレミスのサーバーを Azure ファイル共有に同期し、Azure ファイル共有上のデータを Azure Backup を使用してクラウド側でバックアップすることで、データの保存とアクセスの多重化とバックアップ保護を両立できます。この利用シナリオでは、オンプレミスのサーバーを Azure Backup で直接クラウドにバックアップするのとは異なり、オンプレミス側でバックアップのための負荷が発生しません。

Azure ファイル共有の Azure Backup によるバックアップについて詳しくは、以下の公式ドキュメントで確認してください。

Azure ファイル共有のバックアップ
https://docs.microsoft.com/ja-jp/azure/backup/backup-azure-files

3. クローン for Windows によるクラウドストレージとの同期

LAN DISK Z に付属するソフトウェア「クローン for Windows」を使用すると、NAS デバイスのディレクトリを Microsoft Azure の BLOB ストレージ（ブロック BLOB）または Amazon S3 のクラウドストレージに同期することができます。Azure Backup や Azure File Sync と同様にパブリッククラウドという遠隔地にデータを退避できるため、NAS デバイスに直接降りかかる障害が災害から企業のデータを確実に保護することができます。Azure Backup や Azure File Sync との違いは、アイ・オー・データ純正の専用ツールであり、簡単に導入できること、そしてクラウドプロバイダーの選択肢があることです。

クラウドストレージの事前準備（Azure または AWS）

クローン for Windows のクラウドストレージ同期を利用するために、Microsoft Azure または Amazon Web Services（AWS）に同期先となるクラウドストレージを事前に準備しておきます。

Microsoft Azure を利用する場合は、ブロック BLOB をサポートする Azure ストレージアカウント（汎用 v2、汎用 v1、ブロック BLOB、または BLOB）を作成し、ストレージアカウントの［Blob service］にコンテナーを作成します。データを国内データセンターに保持したい場合は、［西日本］または［東日本］リージョンにストレージアカウントを準備してください。クローン for Windows のクラウドストレージ同期のためには、BLOB ストレージの以下の情報が必要になります。プライマリアクセスキーは、Azure ポータル（https://portal.azure.com/）でストレージアカウントの［設定－アクセスキー］ページを開くと確認できます。

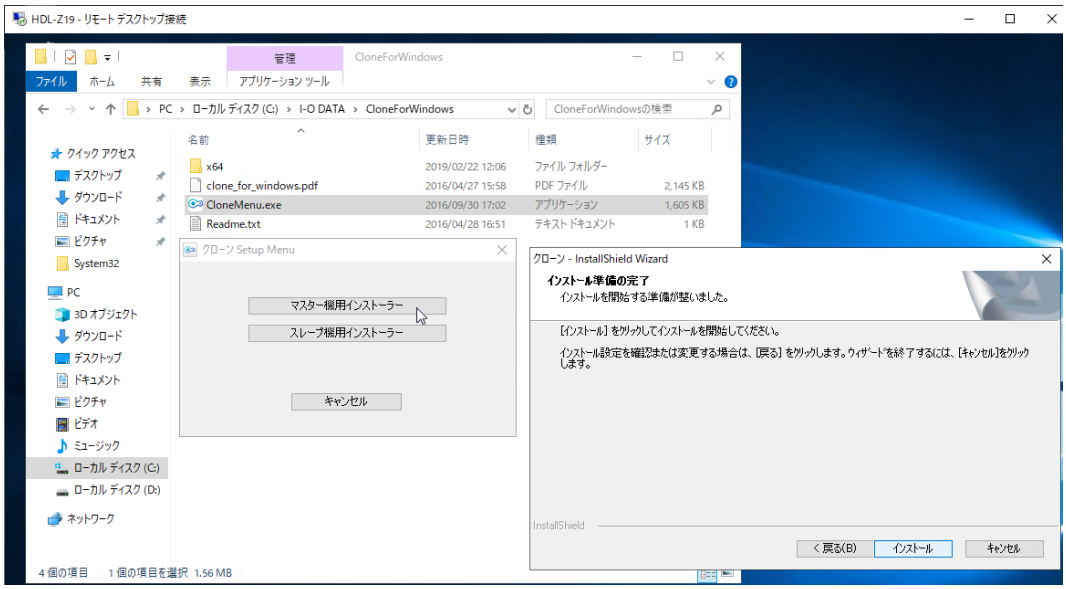
- ストレージアカウント名
- プライマリアクセスキー
- コンテナー名

AWS を利用する場合は、Amazon S3 にバケットを作成します。データを国内データセンターに保持したい場合は、[アジアパシフィック(東京)]リージョンにバケットを準備してください。クローン for Windows のクラウドストレージ同期のためには、Amazon S3 のバケットの以下の情報が必要になります。Amazon S3 のコンソール（https://s3.console.aws.amazon.com/s3/home）にサインインし、[セキュリティ認証情報]ページから確認できます。

- バケット名
- アクセスキーID
- シークレットキー

クローン for Windows のインストール

LAN DISK Z に付属するクローン for Windows を、同期元になる LAN DISK Z の Windows Server にインストールします。それには、リモートデスクトップ接続を使用して LAN DISK Z のコンソールに接続し、クローン for Windows のセットアップメニュー［CloneMenu.exe］を実行して、［マスター機用インストーラー］をクリックします。インストール時に特別な設定は必要ありません。また、インストール後にサーバーの再起動も必要ありません。

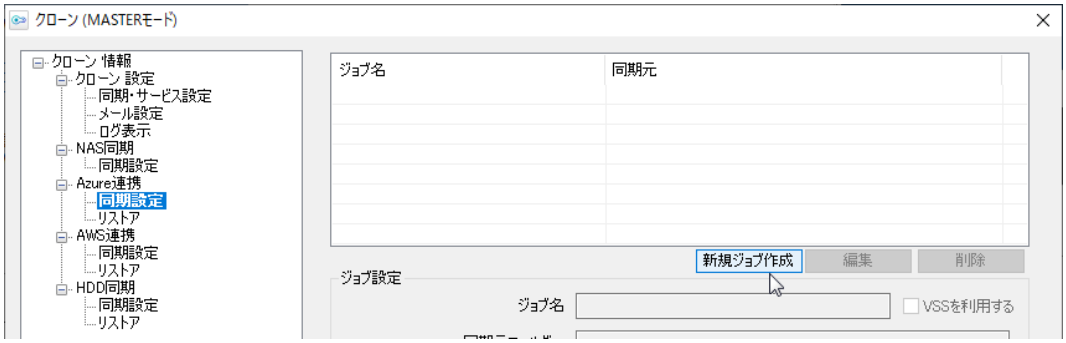


利用シナリオによっては（後述します）、［マスター機用インストーラー］ではなく、［スレーブ機用インストーラー］の方をクリックしてスレーブモードとしてインストールします。

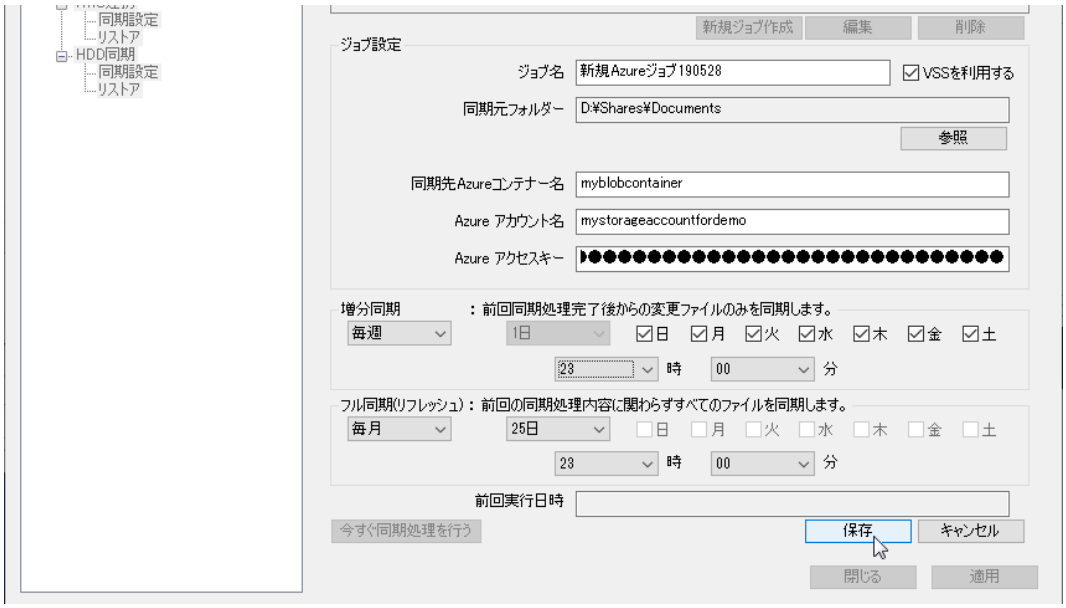
クラウドストレージ同期のセットアップ

クローン for Windows のインストールが完了したら、［スタート］メニューを開き、［I-O DATA］－［クローン］をクリックして［クローン（MASTER モード）］ウィンドウを開きます。スレーブモードとしてインストールした場合は、代わりに［クローン（SLAVE モード）］ウィンドウが開きます。

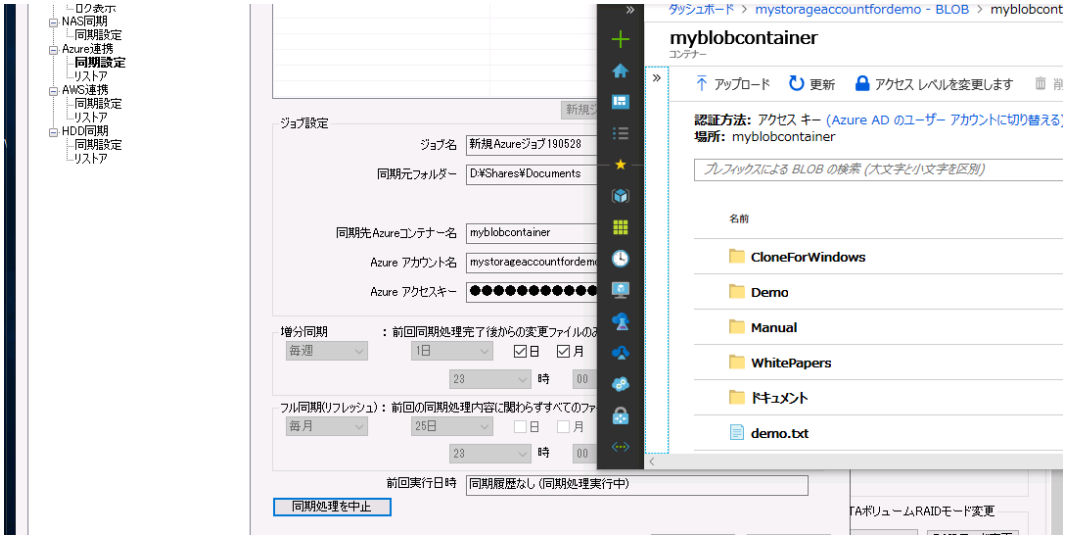
Azure ストレージアカウントの BLOB コンテナーに同期する場合は、［Azure 連携－同期設定］をクリックし、［新規ジョブ作成］をクリックします。Amazon S3 バケットに同期する場合は、［AWS 連携－同期設定］をクリックし、［新規ジョブ作成］をクリックします。



［ジョブ名］に自動生成されたジョブ名をそのまま受け入れるか、分かりやすい名前に変更したら、［参照］をクリックして同期元のサーバーのディレクトリパスを指定します。Azure ストレージアカウントの BLOB コンテナーの情報または Amazon S3 バケットの情報を入力し、［増分同期］と［フル同期（リフレッシュ）］の 2 つの同期スケジュールを調整し、［保存］をクリックします。



以上でクローン for Windows のクラウドストレージ同期のセットアップは完了です。［Azure 連携－同期設定］または［AWS 連携－同期設定］で作成したジョブを選択し、［今すぐ同期処理を行う］、［はい］の順番にクリックすると、指定したクラウドストレージに対して初回のフル同期を開始することができます。



データ重複除去で最適化されたファイルの同期について

クローン for Windows は、ファイル単位で同期を行います。データ重複除去が有効化されたボリューム上のファイルを対象とした場合、最適化されたデータは通常のデータに変換された上で同期先に転送されます。そのため、バックアップデータのサイズがディスクの使用サイズよりも大きくなる可能性があります。

クラウドストレージからの復旧について

このガイドでは、クローン for Windows のクラウドストレージ同期のセットアップ手順についてのみ説明しています。LAN DISK Z の NAS デバイスが利用できなくなった場合のクラウドストレージからの復旧手順については、以下のマニュアルの『お使いの LAN DISK がダウンしたら』－クラウドストレージからの復旧』を参照してください。

画面で見るマニュアル／ファイル同期ツール クローン for Windows
https://www.iodata.jp/lib/manual/pdf2/clone_for_windows.pdf

LAN DISK Z 間のリレー同期の延長

クローン for Windows の本来の機能は、LAN DISK Z の 2 台の NAS デバイス間で、マスター機からスレーブ機へデータとシステム設定を一方向に同期（リレー同期）するものです。データとともに設定の同期も行われるため、万が一マスター機が利用できなくなった場合でも自動または手動でスレーブ機をマスターに昇格し、短時間でクライアントからのファイルアクセスが可能な状態に復旧させることができます。

クローン for Windows のクラウドストレージ同期の設定は、マスター機とスレーブ機のどちらで構成することもできます。2 台の NAS デバイス間のリレー同期をさらに延長するものとして、スレーブ機からクラウドストレージへの同期をセットアップすることで、同期対象が大容量になる場合でも、クラウドストレー

ジ同期のジョブの負荷がクライアントからのファイルアクセスに影響するのを回避することができます。