

ホワイトペーパーシリーズ：

Windows Storage Server 2012/2012 R2

サポート終了（EoS）への緊急対応

ストレージ移行サービスによる

最新 LAN DISK Z への移行ガイド

2023年9月1日

内容

1 概要	2
1.1 このホワイトペーパーについて	2
1.2 NAS の OS サポート終了、すぐに移行が必要な理由	2
1.3 Windows Server IoT ベースの後継製品に移行するメリット	3
2 ストレージ移行サービスを使用したドメイン環境の移行	6
2.1 ストレージ移行サービスとは	6
2.2 システム要件	7
2.3 実施環境	8
2.4 Windows Admin Center を準備する	8
2.5 オークストレーターサーバーを準備する	11
2.6 移行元と移行先の準備	14
2.7 移行ジョブを作成して実行する	15
2.8 カットオーバーして移行先サーバーへの移行を完了する	26

本文書は、株式会社アイ・オー・データ機器（以下、「アイ・オー・データ」とします）が、アイ・オー・データの特定の商品に関する機能・性能や技術についての説明を記述した参考資料となります。当該商品の利用という目的の範囲内で自由に使用、複製をしていただけますが、アイ・オー・データの事前の書面による承諾なしに、改変、掲示、転載等の行為は禁止されます。また、あくまで参考資料として提供いたしますので、内容については一切保証を致しかねます。アイ・オー・データサポートセンターでは内容に関するお問い合わせは承っておりません。以下の内容をご了承いただいた場合のみご利用ください。(1)アイ・オー・データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるものではありません。(2)アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のいかなる保証をするものではありません。(3)アイ・オー・データは、本文書を利用したこと、または利用しなかったことにより生じるいかなる損害についても責任を負うものではありません。(4)アイ・オー・データは、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報については、<https://www.iodata.jp/>をご覧ください。

1 概要

1.1 このホワイトペーパーについて

このホワイトペーパーに示すガイドは、Windows Storage Server 2012 または 2012 R2 を搭載する LAN DISK Z シリーズの利用者向けに、後継 OS である Windows Server IoT 2019 for Storage または Windows Server IoT 2022 for Storage を搭載する LAN DISK Z シリーズの NAS デバイスに移行する手順を説明します。

この移行ガイドでは、Windows Server 2019 以降が標準で備える「ストレージ移行サービス（記憶域の移行サービス、Storage Migration Service）」を使用して NAS デバイス間のデータおよび設定を移行します。

ストレージ移行サービス、ワークグループ環境と Active Directory ドメイン環境での移行をサポートしていますが、中・大規模な Active Directory ドメイン環境における移行を想定しています。

ストレージ移行サービスを使用した移行では、データだけでなく、コンピューター名、IP アドレス、ローカルユーザーやグループ、共有設定、アクセス制御リスト (ACL) を含むセキュリティ記述子やその他のファイル属性も移行できるため、新しい NAS デバイスに切り替え後も、切り替え前と同じ UNC 名やネットワークドライブマッピングを使用した、ユーザーやアプリケーションによるファイルアクセスを継続することができます。切り替え後も移行元の NAS デバイスからデータが削除されることはないため、データを失う心配もありません。

1.2 NAS の OS サポート終了、すぐに移行が必要な理由

Windows Storage Server 2012/2012 R2 を搭載した LAN DISK Z シリーズには、10 年（メインストリーム 5 年 + 延長サポート 5 年）のマイクロソフトによる OS の製品サポートが提供されてきましたが、そのサポートは Windows Server 2012/2012 R2 と同じく 2023 年 10 月 10 日に終了します。

OS の製品サポートが終了した後も NAS デバイスとして使い続けることはできますが、サポートが終了すると OS のセキュリティ更新プログラムが提供されなくなり、マルウェアへの感染によるデータ損失（データ破壊やランサムウェアによる暗号化と復号化のための身代金の要求など）や情報漏えい、マルウェアの感染拡大（NAS デバイスの共有を介して）といったセキュリティリスクが増大します。

ドライバーやアプリケーションなどの周辺ソフトウェアのサポートも、OS のサポート終了とともに停止へと向かうこととなります。また、ハードウェアの保証切れによりハードウェア障害への対応が困難になります（LAN DISK Z シリーズは標準 5 年保証）。これらの問題に対応できなくなると、ビジネスの継続に著しい影響を与える可能性があります。



Windows Storage Server 2012/2012 R2 向けに ESU の提供なし

マイクロソフトは Windows Server 2012/2012 R2、および SQL Server 2012 に対して、製品サポート終了後も最大 3 年間、セキュリティ更新プログラムを受け取ることができる「拡張セキュリティ更新プログラム（Extended Security Update、ESU）」を有料（オンプレミスや Azure 以外のホスディ

ング環境上のインスタンス) または無料 (Azure 上のインスタンス) で提供します。

ESU を利用すると、すぐに後継バージョンや代替ソリューション (クラウドベースのサービスなど) に移行することができない場合に、セキュリティを確保しながら、移行のための時間的な猶予を得ることができます。ただし、有料 (オンプレミスや Azure 以外のホスティング環境上のインスタンス) の ESU は、エンタープライズ契約 (EA) の下でソフトウェアアシュアランス (SA) を契約している顧客に対して販売されます。OEM ライセンスである Windows Storage Server に対して ESU の提供はありません。そのため、サポート終了まで、あるいはサポート終了後、速やかに後継製品や代替ソリューションに移行する必要があります。

SQL Server および Windows Server の拡張セキュリティ更新プログラム

 <https://www.microsoft.com/ja-jp/windows-server/extended-security-updates>

1.3 Windows Server IoT ベースの後継製品に移行するメリット

Windows Server 2012/2012 R2 ベースのアプリケーションサーバーやデータベース、その他のさまざまな役割サービスを実行するサーバーは、オンプレミスやクラウド (PaaS/SaaS)、ハイブリッド環境など、移行先の選択肢がさまざまであり、移行方法も選択した移行先に応じてさまざまです。これに対して、Windows Storage Server 2012/2012 R2 搭載の LAN DISK Z シリーズの NAS デバイスはファイルサーバーという単機能サーバーであり、後継 OS である Windows Server IoT 2019 または 2022 for Storage 搭載の同シリーズの後継製品に比較的簡単に、データだけでなくその設定を含めて、安全かつ確実に移行することができます。

適切な移行ツールを使用することで、UNC パスやアクセス制御リスト (ACL) を維持したまま移行できるだけでなく、OS が後継バージョンになることでパフォーマンス向上やセキュリティの強化など、さまざまなメリットを得られます。

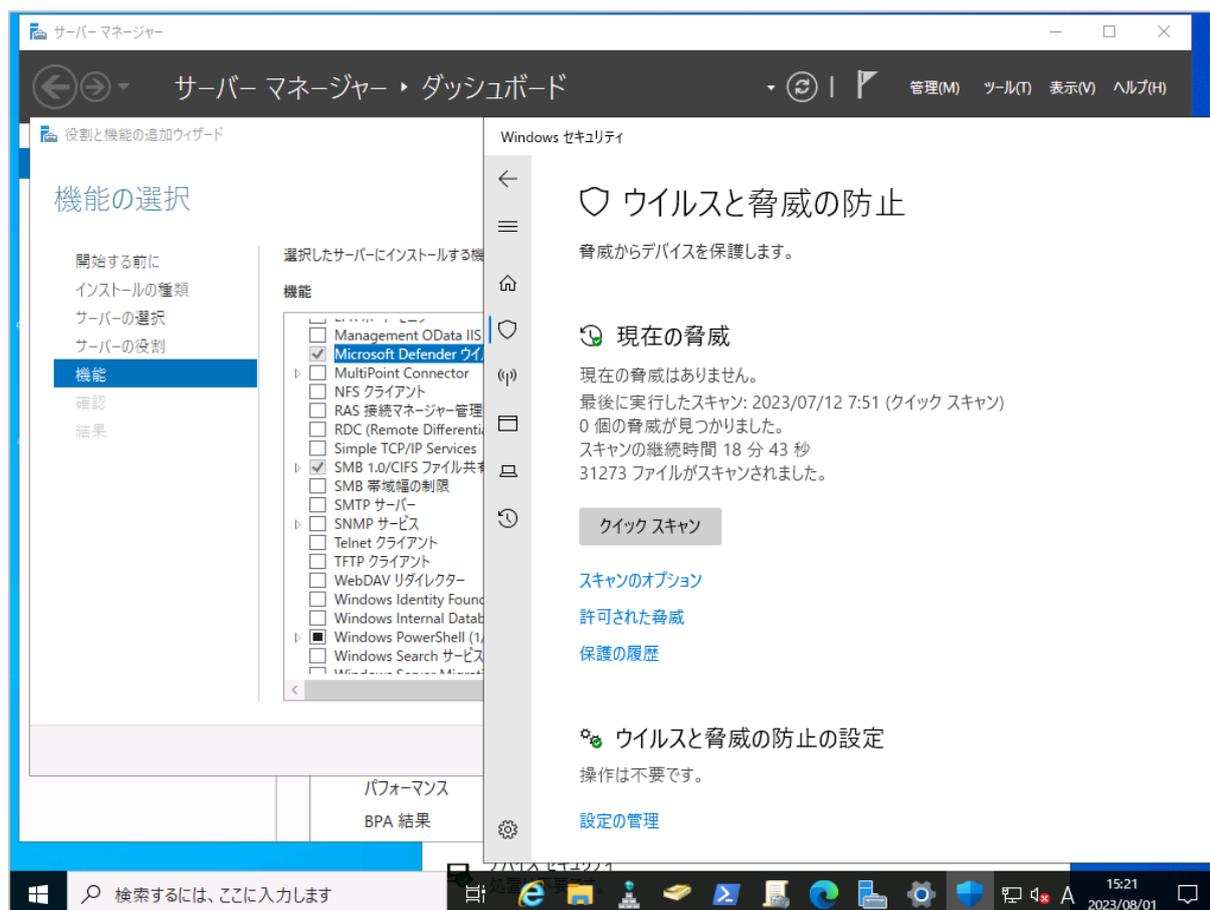
例えば、Windows Server IoT 2019/2022 for Storage は、最新の「SMB (サーバーメッセージブロック) 3.1.1」をサポートしており^{*1}、Windows 10/11 クライアントデバイスと高い親和性があります。SMB 3.1.1 では、SMB 暗号化の高速化や機能強化 (暗号化アルゴリズムの追加) が行われている他、Windows 10 および Windows Server 2016 以降のバージョンでもいくつかの新機能が追加されています。

Windows Server の SMB 3 プロトコルを使用したファイル共有の概要

 <https://learn.microsoft.com/ja-jp/windows-server/storage/file-server/file-server-smb-overview>

^{*1} Windows Storage Server 2012 は SMB 3.0、Windows Storage Server 2012 R2 は SMB 3.0.2 が最上位の SMB バージョンです。

また、ウイルス対策およびネットワーク検査サービスとして Microsoft Defender ウィルス対策 (Microsoft Defender Antivirus) を OS に標準搭載しており、サードパーティのウイルス対策製品を導入しなくても、マルウェアから保護されます (画面 1-1)。有料の Microsoft Defender for Cloud (Microsoft Defender for Servers) を導入すると、クラウド (Azure) ベースの統合管理でセキュリティ体制をさらに強化できます。Microsoft Defender for Cloud は、Windows Admin Center に統合された Azure ハイブリッドサービスの 1 つでもあります。



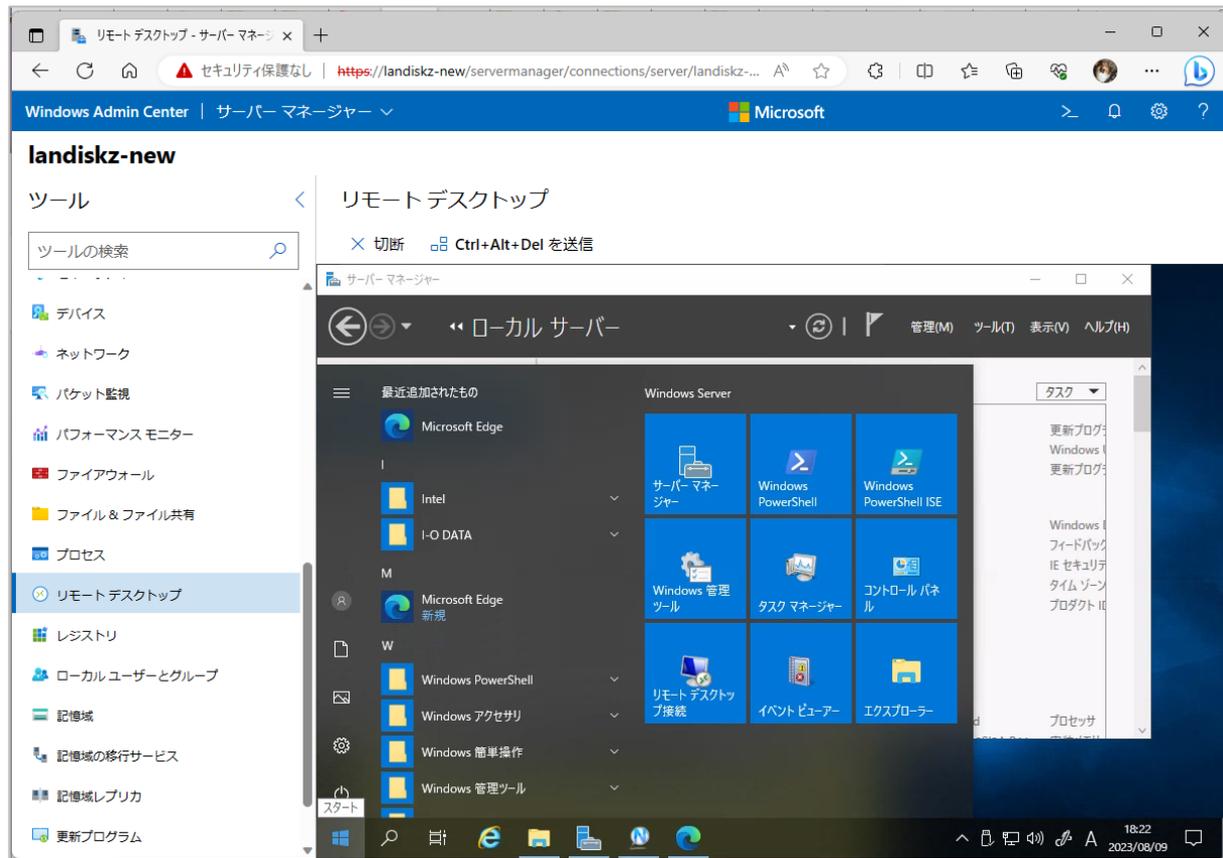
画面 1-1 サードパーティのウイルス対策製品が導入されていない場合、Microsoft Defender ウイルス対策が既定で有効になる

さらに、Windows Server およびクラスターの管理アプリである「Windows Admin Center (WAC)」(無料)を導入することで、モダンブラウザ (Microsoft Edge や Google Chrome) を使用して、NAS デバイスをリモート管理することができます。Windows Storage Server や Windows Server IoT for Storage は NAS 専用の管理ツールを提供せず、サーバーマネージャーや Microsoft 管理コンソール (MMC) スナップインなど Windows Server 標準の GUI 管理ツールを使用して管理しますが、Windows Admin Center を使用すると、GUI 管理ツールを使い分ける必要がなく、リモートデスクトップ接続や PowerShell リモートコマンドを含む、さまざまな管理操作をモダンブラウザだけで実行することができます (画面 1-2)。

なお、Windows Admin Center は Windows Server 2012/2012 R2 (Windows Storage Server を含む) の管理もサポートしていますが (インストールは非サポート)、WMF 5.1 の追加インストールが必要な上に、管理機能の一部が制限されます。Windows Server IoT for Storage は Windows Admin Center による管理のために追加のコンポーネントを必要としません。Windows Admin Center による LAN DISK Z シリーズの管理については、以下のホワイトペーパーでも説明しています。

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 (全 4 編) / 3.集中管理編

<https://www.iodata.jp/biz/whitepaper/index.htm#IoT2019-04>



画面 1-2 Windows Admin Center によるリモート管理に標準対応

2 ストレージ移行サービスを使用したドメイン環境の移行

中・大規模なドメイン環境において、Windows Server 2019 以降のストレージ移行サービスを使用した NAS デバイスの移行手順について説明します。

2.1 ストレージ移行サービスとは

ストレージ移行サービス（記憶域の移行サービス、Storage Migration Service）は、Windows Server 2019 以降の Windows Server でサポートされる新しいサーバーの機能です。このサービスを使用すると、ネットワーク上の SMB/CIFS 共有にあるデータを、オンプレミスの Windows Server ベースのファイルサーバー（物理サーバーまたは仮想マシン）または Azure 仮想マシン（Azure VM）に、SMB プロトコルを使用してデータ転送することができ、ファイルサーバーの移行やクラウドへの移行を実現します。

ストレージ移行サービスは、コンピューター名、ドメイン参加設定、IP アドレス、共有設定（SMB 共有のすべてのフラグと設定）、ローカルユーザーとグループ、SMB 共有および NTFS ファイルシステムのアクセス制御リスト（ACL）を移行先サーバーに転送するオプションも用意されています。これにより、ユーザーやアプリケーションは UNC パスやネットワークドライブマッピングを変更することなく、移行先サーバーにアクセスできるようになります。

ストレージ移行サービスは PowerShell のモジュール（StorageMigrationService モジュール）として実装されていますが、Windows Admin Center の「記憶域の移行サービス」拡張機能（既定でインストールされます）を使用すると、ウィザードベースの GUI を使用してジョブを作成し、実行状態を確認することができます。また、複数の移行元と移行先のマッピングを追加して、一括実行することもできます。



ストレージ移行サービスの制限

ストレージ移行サービスを使用したファイルサーバーの移行では、以下の制限があります。

- ローカルユーザーとグループの移行はサポートされますが、移行されたローカルユーザーのアカウントは移行先で無効にされ、複雑でランダムな 127 文字のパスワードが割り当てられます。これは、移行元で旧アカウントのパスワードを忘れてしまっていた場合や、旧アカウントに簡単な（脆弱な）パスワードを使用していた場合、移行先でセキュリティ関連の問題が引き継がれる事態を回避するのに役立つ仕様です。ローカルユーザーのアカウントを引き続き使用するには、移行後にアカウントを有効にして新しいパスワードを割り当てる必要があります。なお、組み込みのユーザーおよびグループは、ソースと宛先で同じ名前が使用され、再利用されます（ランダムなパスワードの設定やアカウントの無効化は行われません）。
- 複数のサーバーを 1 つのサーバーに統合することはできません。ただし、スタントアロンサーバーを、1 つのクラスター上の複数のファイルサーバーリソースに移行することは可能です。
- ボリュームシャドウコピーサービス（VSS）によって作成されたファイルの以前のバージョンを移行することはできません。そのファイルの最新バージョンのみが移行されます。

- ストレージ移行サービスは、移行元デバイスの NTFS ボリュームから移行先デバイスの NTFS ボリュームへの移行を、暗号化ファイルシステム (EFS、ただしドメインアカウントによる暗号化のみ) や NTFS 圧縮の状態を含めてサポートしますが、NTFS から ReFS への異なるファイルシステム間の移行はできません。

2.2 システム要件

Active Directory ドメイン環境でストレージ移行サービスを利用する場合のシステム要件を以下に示します。ワークグループ環境の場合は、Active Directory ドメイン要件は不要です。

- **Active Directory ドメイン** … Active Directory ドメイン環境でストレージ移行サービスを利用する場合、オーケストレーターサーバー、移行元サーバー、移行先サーバー、Windows Admin Center の動作する Windows 10/11 デバイスまたは Windows Server は、すべて同じドメインに参加している必要があります。ストレージ移行サービスでは、異なるドメイン間の移行はサポートされません。
- **オーケストレーターサーバー** … Windows Server 2019 または Windows Server 2022 (Server Core またはデスクトップエクスペリエンス) の物理サーバーまたは仮想マシンが 1 台必要です。オーケストレーターサーバーにはストレージ移行サービスがインストールされ、移行ジョブを制御します。これには、少なくとも 2 コアの CPU と 2GB のメモリを搭載していることが推奨されます。Windows Server 2019 を使用する場合、累積的な更新プログラムによってストレージ移行サービスに変更や機能強化が行われているため、最新の累積更新プログラムをインストールしてください (少なくとも 2021 年 4 月リリースの OS ビルド 17763.1911 以降を実行している必要があります)。
- **移行元サーバー** … Windows Server 2003 以降の Windows Server のサーバーとクラスター、Samba 3.6/4.2/4.3/4.7/4.8 を実行する Linux サーバー、NetApp ONTAP 9 を実行する NetApp CIFS サーバーがサポートされます。Windows Storage Server 2012/2012 R2 は Windows Server 2012/2012 R2 と同等であり、移行元サーバーとしてサポートされます。
- **移行先サーバー** … Windows Server 2012 R2 以降の Windows Server (移行先側のストレージ移行サービスプロキシによる高速転送を利用できる Windows Server 2019 以降を推奨) のサーバーとクラスターがサポートされます。Windows Server IoT 2019/2022 for Storage は Windows Server 2019/2022 と同等であり、移行先サーバーとしてサポートされます。移行先サーバーは、少なくとも 2 コアの CPU と 2GB のメモリを搭載していることが推奨されます。
- **最新の Windows Admin Center** … Windows 10 または Windows 11 デバイスまたは Windows Server 2016 (デスクトップエクスペリエンスまたは Server Core インストール) 以降にインストールされた Windows Admin Center が必要です。ストレージ移行サービスは、Windows Admin Center バージョン 2103 以降でサポートされます。このガイド制作時点の最新バージョンは Windows Admin Center バージョン 2306 です (Windows Admin Center の新バージョンがリリースされると、その日から 30 日後に旧バージョンはサポートされなくなることに注意してください)。Windows Admin Center のドメインコントローラーへのインストールはサポートされませんが、オーケストレーターサーバーへのインストールは可能です。

2.3 実施環境

ストレージ移行サービスを利用した NAS デバイス間のデータと設定の移行は、すべてオーケストレーターサーバーに接続した Windows Admin Center から実行します。移行ジョブを作成して、移行元サーバーからインベントリを収集し、移行先サーバーにデータを転送して、最後に移行先サーバーにカットオーバー（一括移行）して新旧 NAS デバイスを切り替えます（図 2-1）。

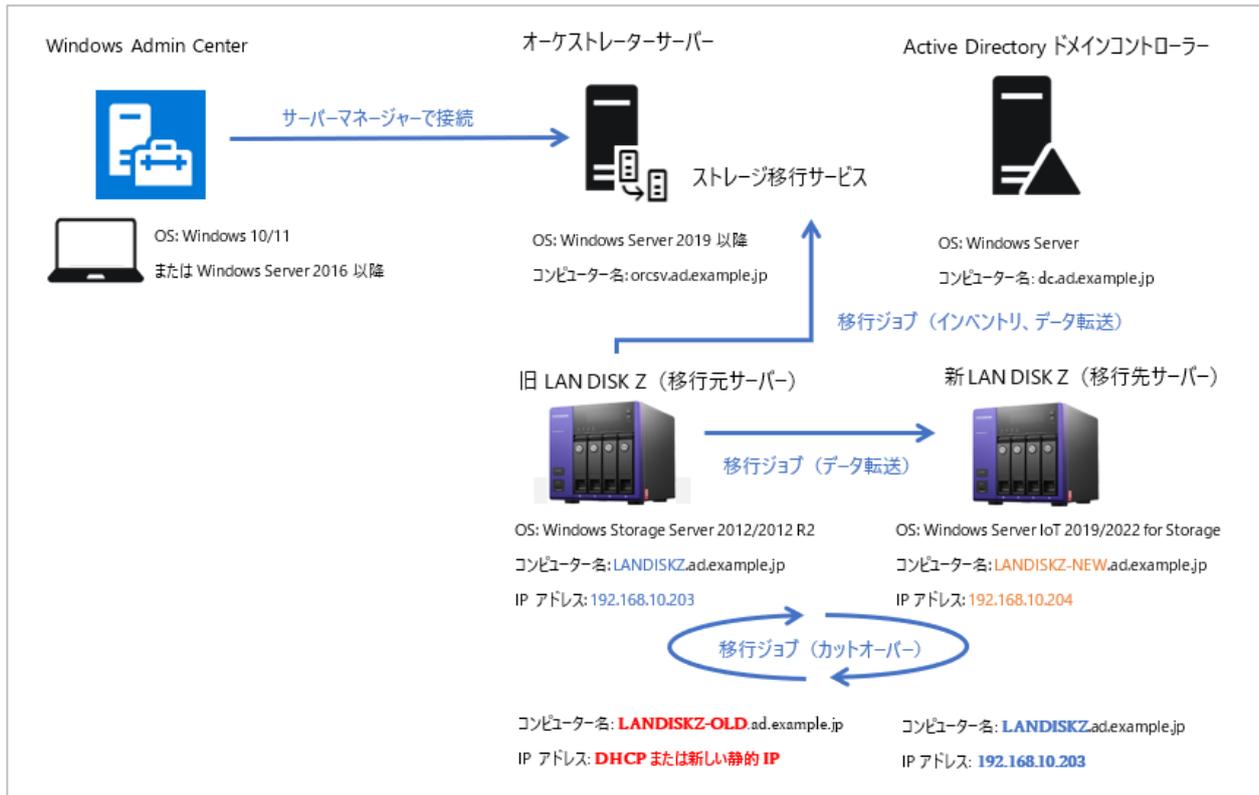


図 2-1 ストレージ移行サービスによる NAS デバイス間のデータと設定の移行手順のイメージ

2.4 Windows Admin Center を準備する

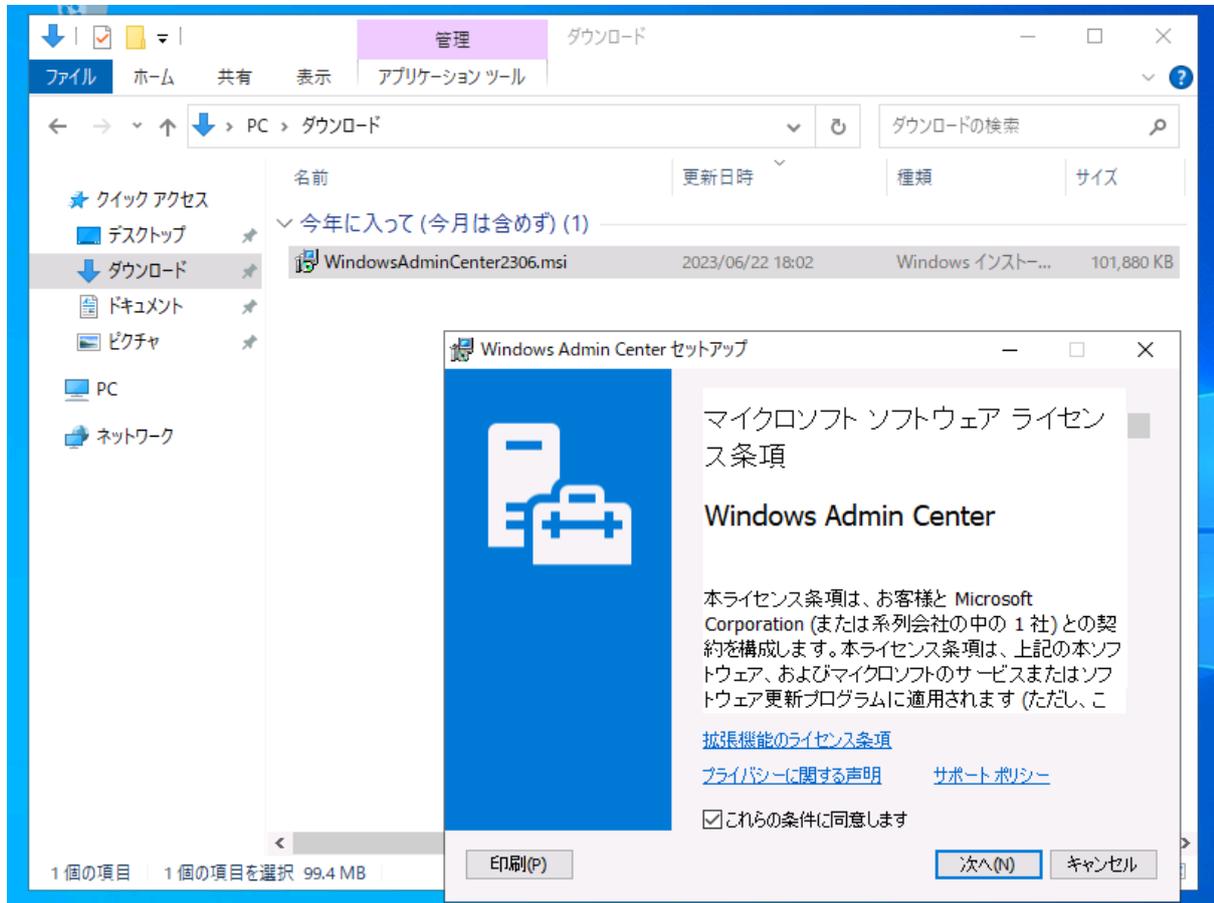
Active Directory ドメインのメンバーとなっている Windows 10/11 デバイスまたは Windows Server 2016 (デスクトップエクスペリエンスまたは Server Core インストール) 以降に Windows Admin Center をインストールします。ストレージ移行サービスのためには、移行元および移行先の NAS デバイスとは別のシステムに Windows Admin Center の管理環境を用意する必要があります。

Windows Admin Center | Microsoft Evaluation Center

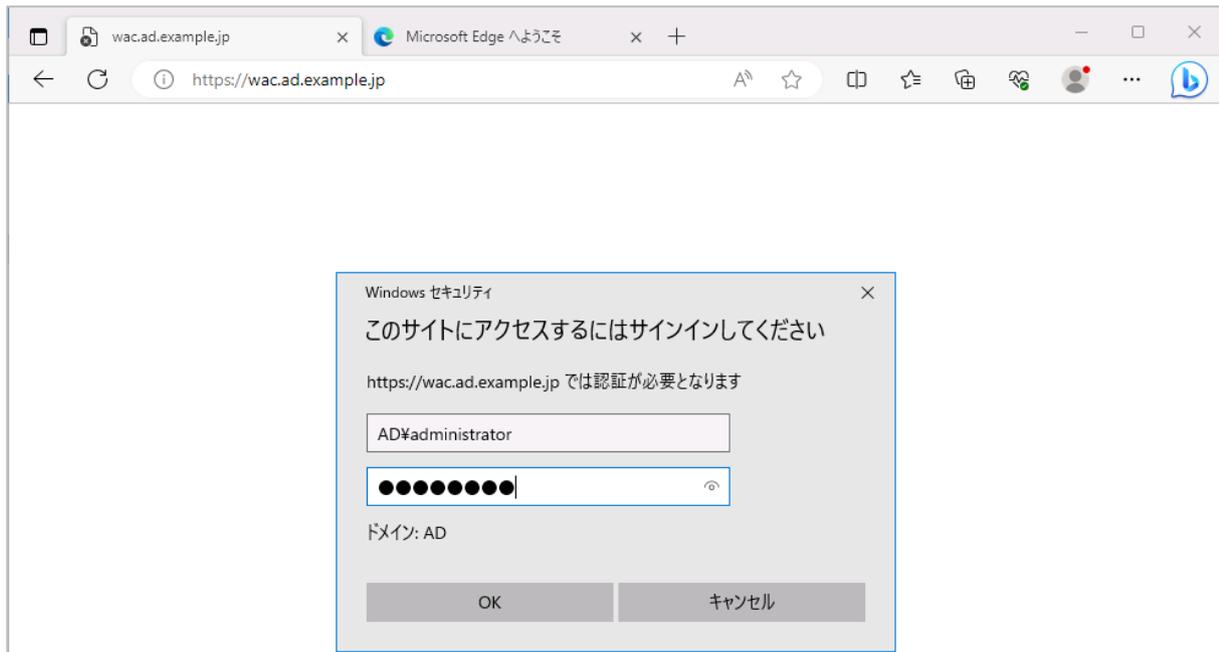
🌐 <https://www.microsoft.com/ja-jp/evalcenter/evaluate-windows-admin-center>

Windows Admin Center の管理環境がまだない場合は、以下の URL から Windows Admin Center の最新バージョンの MSI (Windows インストーラーパッケージ) 形式のインストーラーをダウンロードして実行し、ローカルクライアントモード (Windows 10/11 の場合) またはゲートウェイサーバーモード (Windows Server の場合) でインストールしてください (画面 2-1)。インストールの際には、すべて既定の設定を受け入れ、自己署名証明書 (または Active Directory 証明書サービスなどの証明機関で発行された有効な TLS 証明書) を使用してセットアップします。

ローカルクライアントモードの場合、Windows 10/11 のスタートメニューから「Windows Admin Center」を起動し、Microsoft Edge で **https://localhost:6516** を開きます。ゲートウェイサーバーモードの場合は、ローカルまたはリモートの Microsoft Edge から **https://<ゲートウェイサーバーの FQDN> (:443)** にアクセスします。ゲートウェイサーバーに接続する際には、ドメイン管理者の資格情報を入力してください（画面 2-2）。ローカルクライアントモードの場合、接続時に資格情報の入力は要求されません。

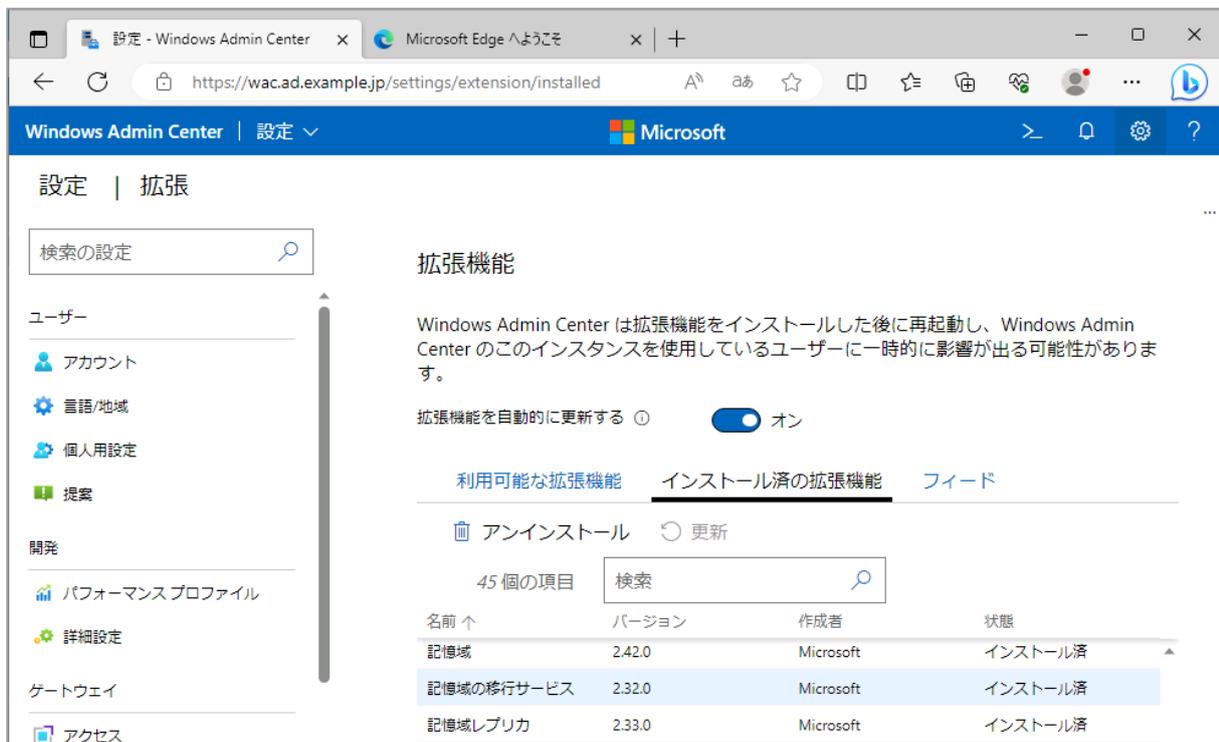


画面 2-1 NAS デバイスやドメインコントローラーとは別の Windows 10/11 デバイスまたは Windows Server 2016 以降に Windows Admin Center の最新バージョンをインストールする



画面 2-2 ドメイン管理者の資格情報（ドメイン名¥Administrator など）を入力してゲートウェイサーバーに接続する

Windows Admin Center の管理環境を用意したら、「設定（） | 拡張」を開き、拡張機能の更新が利用可能であればすべてインストールしてください（画面 2-3）。特に、ストレージ移行サービスのためには、「記憶域の移行サービス」拡張機能が必要です。この拡張機能は Windows Admin Center に既定でインストールされますが、最新バージョンがインストールされていること（利用可能な更新がない状態）を確認してください。



画面 2-3 利用可能な拡張機能の更新があれば、すべてインストールしておく

2.5 オークストレーターサーバーを準備する

ドメインメンバーとして、オークストレーターサーバーのシステム要件を満たすサーバーが存在する場合は、そのサーバーをオークストレーターサーバーとして利用できます。利用可能なサーバーがない場合は、物理サーバーまたは仮想マシンとして新規に導入する必要があります。利用可能な Windows Server のライセンスがない場合は、ストレージ移行サービスを利用して移行が完了するまで、Windows Server 2022 Evaluation（180 日評価版）を一時的に利用することもできます。

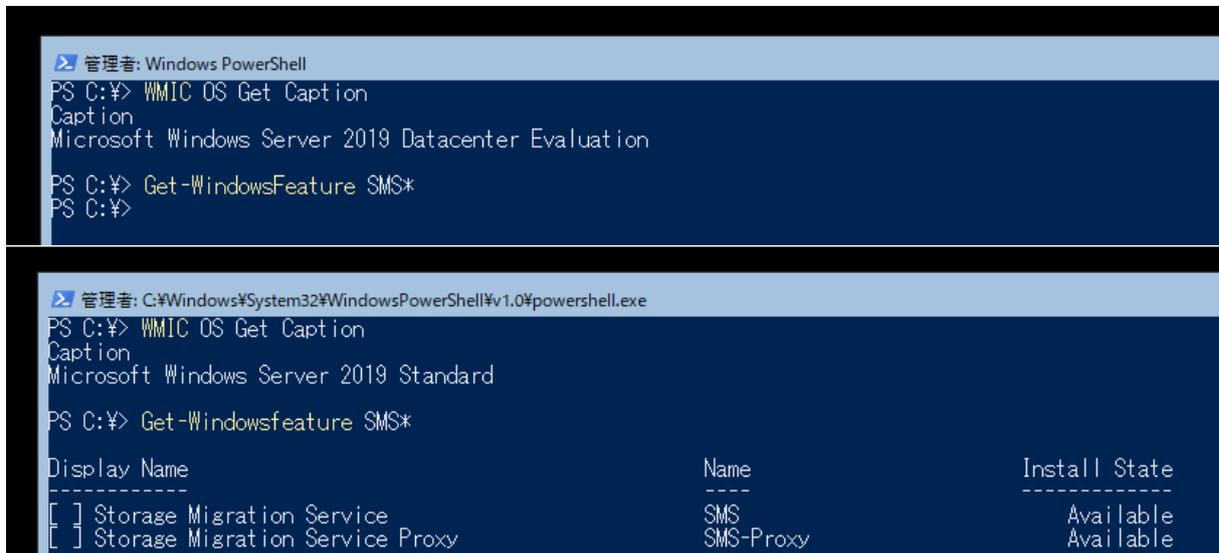
Windows Server 2022 | Microsoft Evaluation Center

 <https://www.microsoft.com/ja-jp/evalcenter/evaluate-windows-server-2022>



Windows Server 2019 評価版と Essentials の既知の問題

オークストレーターサーバーとして、Windows Server 2019 評価版および Essentials エディションは使用できません。Windows Server 2019 評価版および Essentials エディションにはストレージ移行サービスおよびストレージ移行サービスプロキシのサーバーの機能が含まれていないため、Windows Admin Center で管理される Windows Server 2019 評価版の「サーバermaneージャー」に「記憶域の移行サービス」ツールは表示されず、オークストレーターサーバーとして機能させることができません。これは Windows Server 2019 評価版および Essentials エディションのメディアの既知の問題であり、Windows Server 2019 製品版の他のエディションおよび Windows Server 2022 評価版/製品版には影響しません。

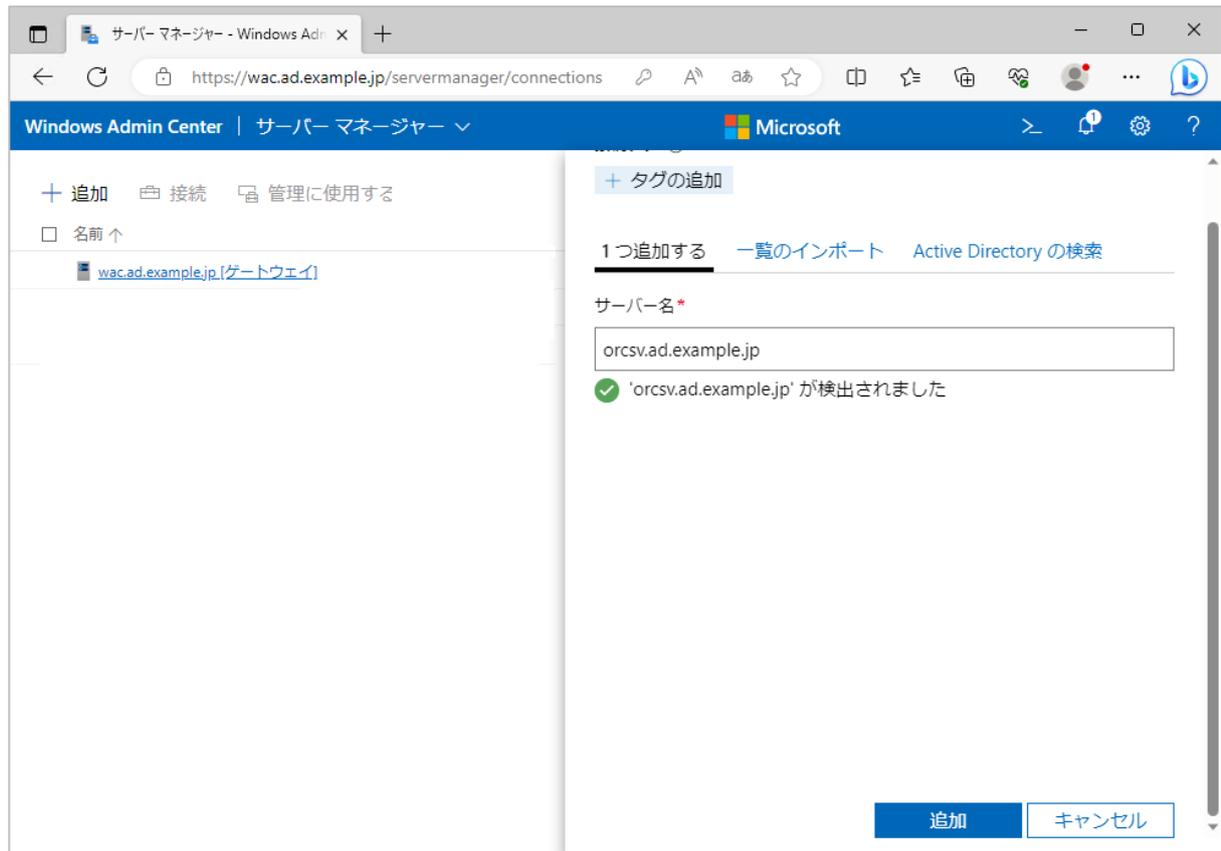


```
管理: Windows PowerShell
PS C:\> WMIC OS Get Caption
Caption
Microsoft Windows Server 2019 Datacenter Evaluation
PS C:\> Get-WindowsFeature SMS*
PS C:\>
```

```
管理: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\> WMIC OS Get Caption
Caption
Microsoft Windows Server 2019 Standard
PS C:\> Get-Windowsfeature SMS*
Display Name                                     Name                                     Install State
-----
[ ] Storage Migration Service                    SMS                                     Available
[ ] Storage Migration Service Proxy              SMS-Proxy                             Available
```

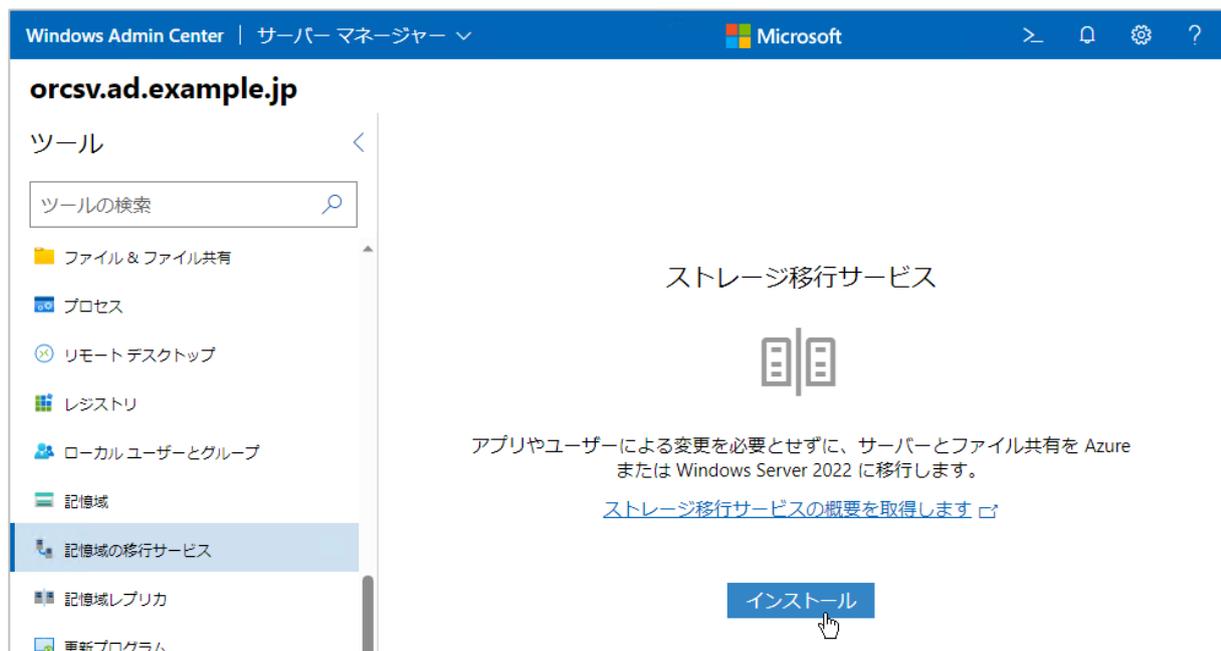
画面 2-4 Windows Server 2019 評価版および Essentials エディションにはストレージ移行サービスの機能が含まれないという既知の問題がある

オークストレーターサーバー用のサーバーの準備ができれば、Windows Admin Center に管理対象のサーバーとして追加します（画面 2-5）。サーバーを追加する際に資格情報の入力が必要された場合は、ドメイン管理者の資格情報を入力してください。



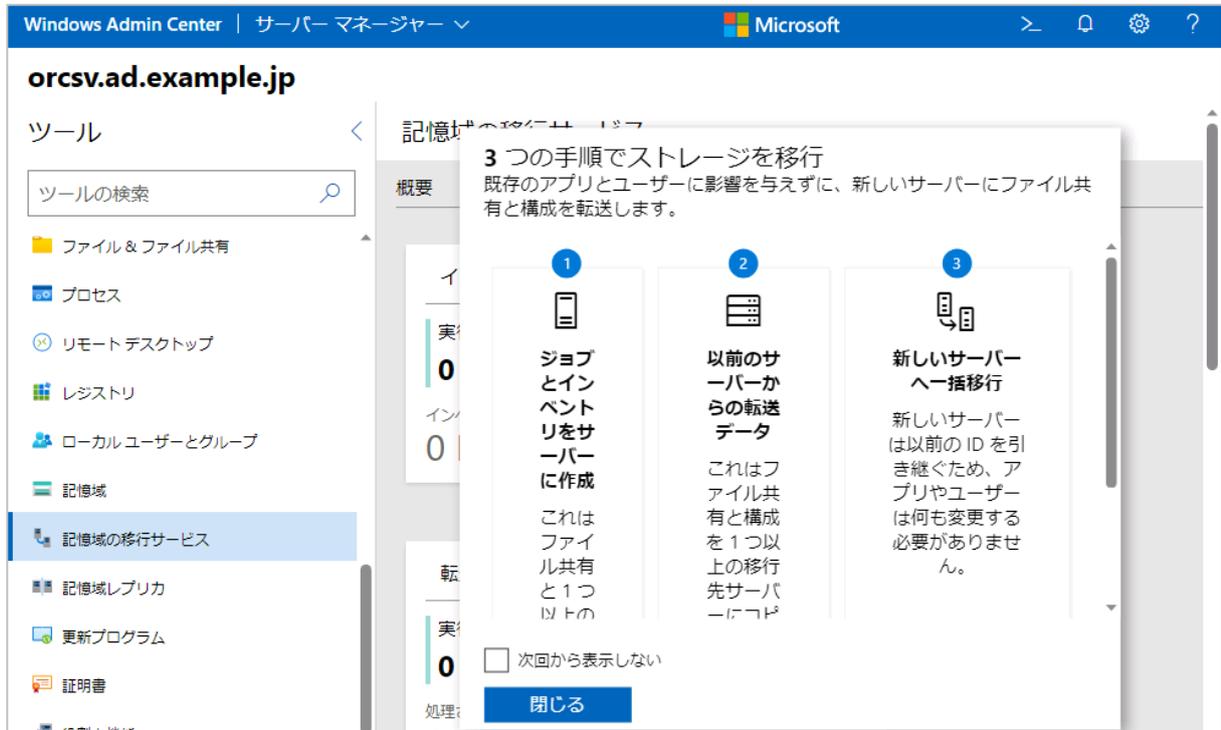
画面 2-5 「+ 追加」をクリックして、オーケストレーターサーバーにする Windows Server 2019 または Windows Server 2022 のサーバーを管理対象として追加する

オーケストレーターサーバー用のサーバーを追加したら、そのサーバーに接続し、「ツール | 記憶域の移行サービス」を開きます。ここで「インストール」をクリックして、オーケストレーターサーバーにストレージ移行サービスのサーバーの機能をインストールします（画面 2-6）。



画面 2-6 「ツール | 記憶域の移行サービス」の「インストール」をクリックする

ストレージ移行サービスの機能のインストールが完了すると、ストレージ移行サービスを使用した移行手順の概要が表示されるので、確認して「閉じる」をクリックします（画面 2-7）。



画面 2-7 ストレージ移行サービスの機能のインストールが完了すると、ストレージ移行サービスの手順の概要が表示される

最後に、Windows Admin Center の「ファイアウォール」ツールを開き、「着信規則」で以下のファイアウォール規則がすべて（またはドメイン）プロファイルで有効になっていることを確認します。上の 2 つストレージ移行サービスのインストールによって既定で有効化されます（画面 2-8）。最後の規則は、通常、手動で有効化する必要があります（画面 2-9）。

- SMS（任意-受信）
- SMSプロキシ（任意-受信）
- ファイルとプリンターの共有（SMB 受信）



画面 2-8 ストレージ移行サービスのファイアウォール規則が有効になっていることを確認する



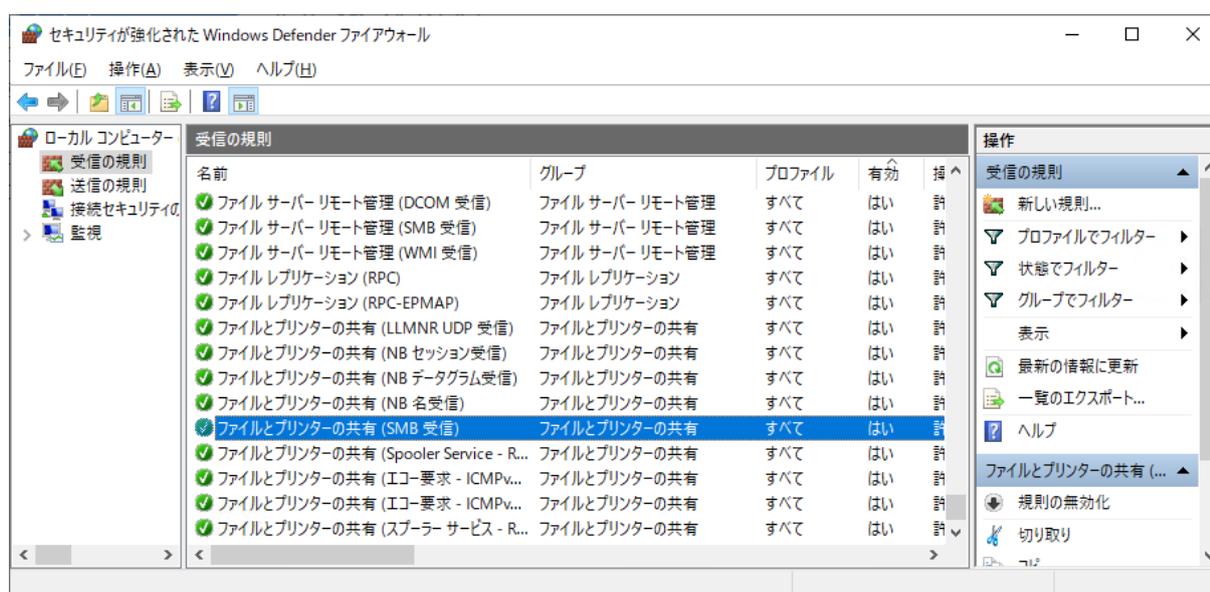
画面 2-9 「ファイルとプリンターの共有 (SMB 受信)」を有効にする

以上で、オーケストレーターサーバーの準備ができました。

2.6 移行元と移行先の準備

移行元と移行先の NAS デバイスでは、「受信の規則」で以下のファイアウォール規則がすべて（またはドメイン）プロファイルで有効になっている必要があります。各 NAS デバイスにリモートデスクトップ接続して、「セキュリティが強化された Windows Defender ファイアウォール」(wf.msc) を開き、確認して、無効になっている場合は有効にしてください（画面 2-10）。Windows Admin Center に NAS デバイスを管理対象として登録済みであれば、Windows Admin Center の「ファイアウォール」ツールを使用することもできます。

- ファイルとプリンターの共有 (SMB 受信)
- Netlogon サービス (NP 受信)
- Windows Management Instrumentation (DCOM 受信)
- Windows Management Instrumentation (WMI 受信)



画面 2-10 移行元と移行先の両方で、必要なファイアウォールの例外が有効になっていることを確認する

2.7 移行ジョブを作成して実行する

「記憶域移行サービス」ツールが示す移行手順の概要（前出の画面 2-7）が示すように、ストレージ移行サービスは、次の 3 つのステップでデータと設定を移行元から移行先に転送します。

ステップ 1 ジョブの作成と移行元からのインベントリ収集（フェーズ：インベントリ） … 移行ジョブを作成し、移行元デバイスのデータと構成の情報を収集します。

ステップ 2 移行元から移行先へのデータ転送（フェーズ：転送） … 移行元デバイスのボリュームと移行先デバイスのボリュームをマップし、データ転送を開始します。

ステップ 3 新しいデバイスへのカットオーバー（フェーズ：一括移行） … 移行元から移行先のデバイスへのカットオーバーを実施し、IP アドレスとコンピューター名を新しいデバイスに移行します。

移行の手順で示す移行元および移行先デバイスの設定は、以下の表のとおりです。

項目	移行元デバイス	移行先デバイス
OS	Windows Storage Server 2012 R2	Windows Server 2019 IoT for Storage
コンピューター名→ カットオーバー後	LANDISKZ → LANDISKZ-OLD	LANDISK-NEW → LANDISKZ
ドメイン	ad.example.jp	ad.example.jp
IP アドレス→カット オーバー後	192.168.10.203 → DHCP	192.168.10.204 → 192.168.10.203
共有	SMBShare	
パス	D:¥Share¥SMBShare	

表 3-1 移行元と移行先の環境および設定

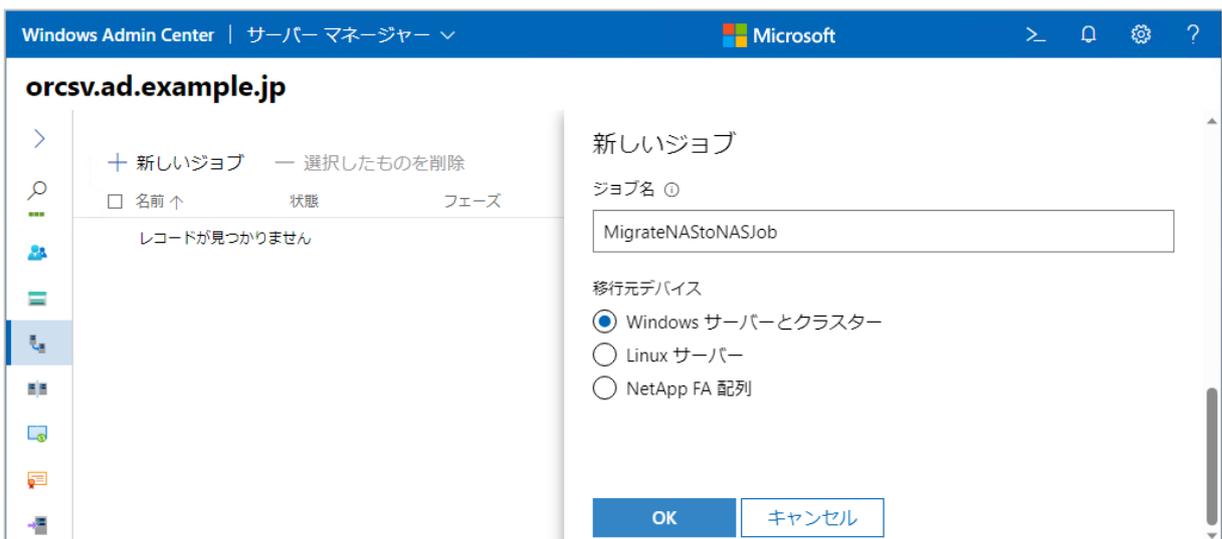
以下の手順に従って、ステップ 1 を実施します。

1. Windows Admin Center の「サーバーマネージャー」でオーケストレーターサーバーにドメイン管理者の資格情報で接続します。
2. 「記憶域の移行サービス」ツールを開き、「+新しいジョブ」をクリックします（画面 2-11）。



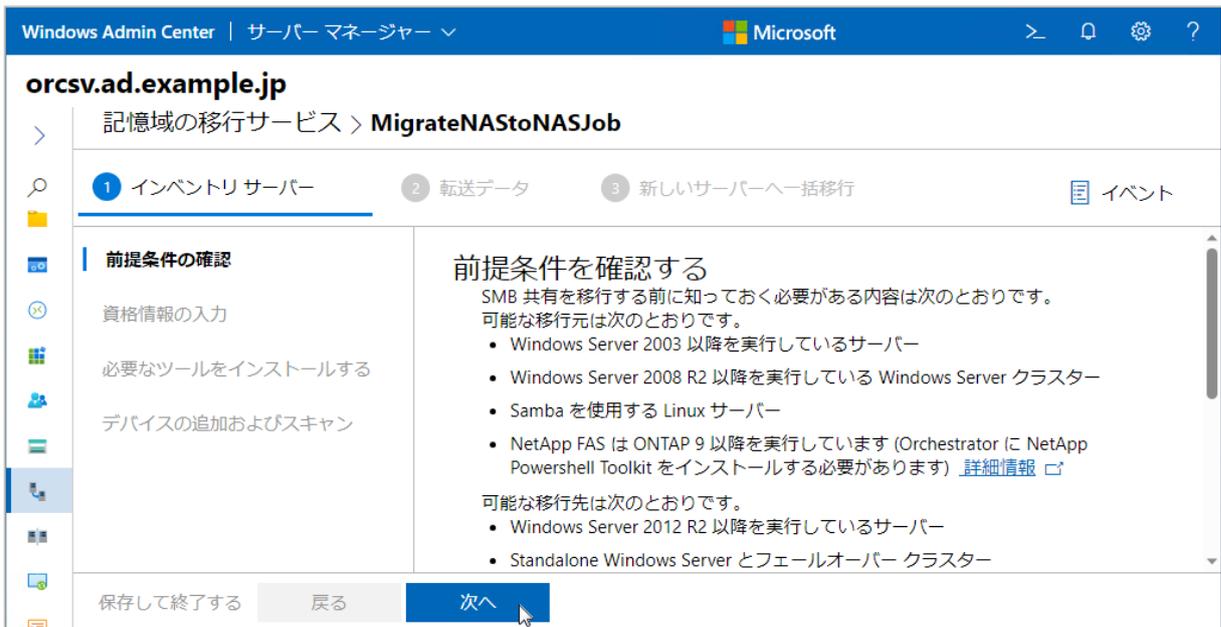
画面 2-11 Windows Admin Center でオーケストレーターサーバーに接続し、「記憶域の移行サービス」ツールを開き、「+新しいジョブ」をクリックする

- 「新しいジョブ」パネルが開くので、「ジョブ名」に半角英数字のみを使用して分かりやすいジョブ名を入力し、「移行元デバイス」として「Windows サーバーとクラスター」を選択します。Windows Server ベースの NAS デバイスは、ストレージ移行サービスでは「Windows サーバー」と同じように扱うことができます（画面 2-12）。



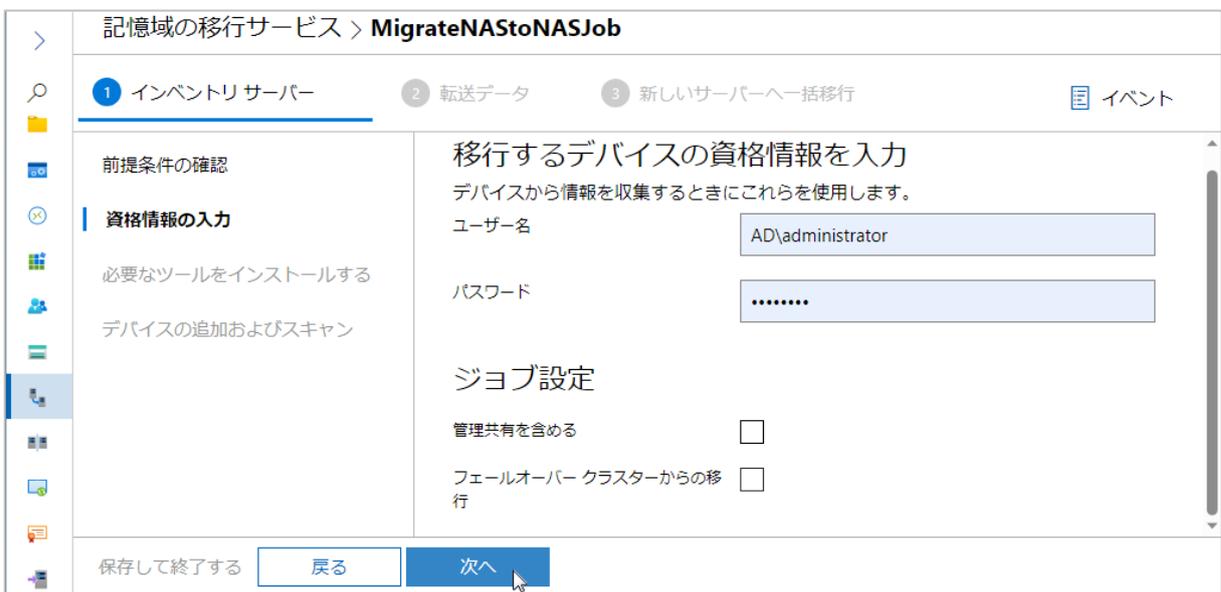
画面 2-12 新しいジョブに分かりやすい名前（英数字のみ使用可）を付けて「Windows サーバーとクラスター」を選択する

- 移行ジョブのウィザードが開始します。「① インベントリサーバー（Inventory server、より適切な訳は“サーバーのインベントリ”）」の「前提条件の確認」ページで前提条件の内容を確認し、「次へ」をクリックします。なお、移行ジョブはウィザードの左下にある「保存して終了する」をクリックことで、途中までの状態を保存し、後で再開することができます（画面 2-13）。移行ジョブの再開時には、完了済みフェーズ（インベントリ、転送、一括移行）をスキップして次のフェーズに進む、または前回のフェーズを再実行できます。



画面 2-13 「前提条件の確認」ページで「次へ」をクリックする

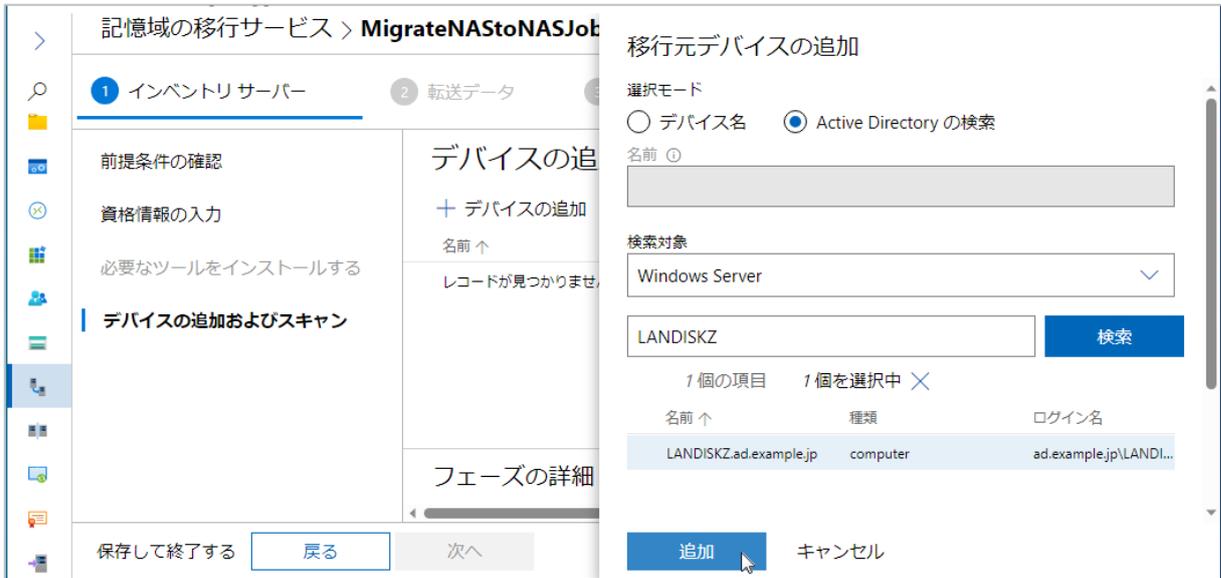
- 「資格情報の入力」ページで、移行元のデバイスの資格情報としてドメイン管理者の資格情報（ドメイン名¥Administrator など）を入力し、「ジョブ設定」の「管理共有を含める」と「フェールオーバークラスターからの移行」の2つのチェックボックスをオフにした状態で「次へ」をクリックします（画面 2-14）。



画面 2-14 ドメイン管理者の資格情報を入力する

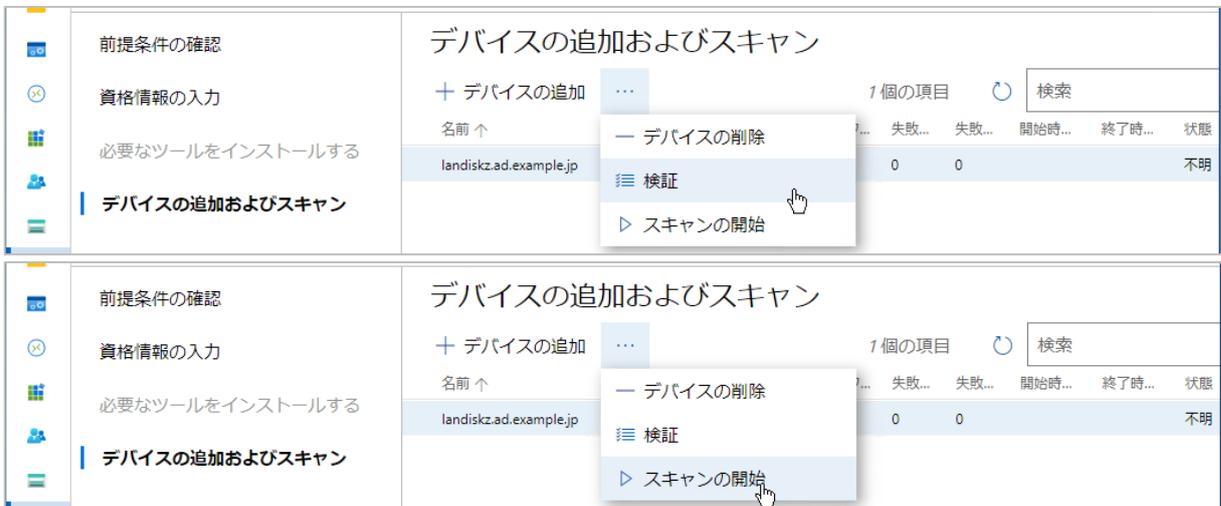
- 「必要なツールをインストールする」ページで「次へ」をクリックします。移行元が Windows Server を実行するデバイスで非クラスター構成の場合、オーケストレーターサーバーに追加のツールがインストールされることはありません。クラスターからの移行の場合、ここで「フェールオーバークラスター管理ツール (RSAT-Clustering-Mgmt)」の機能がインストールされます。
- 「デバイスの追加およびスキャン」ページで「+デバイスの追加」をクリックし、「移行元デバイスの追

加」パネルでデバイスのコンピューター名を直接入力するか、Active Directory から検索して移行元デバイスを追加します（画面 2-15）。



画面 2-15 移行元デバイスを追加する

- 追加したデバイスを選択し、「☰ 検証」をクリックします。検証結果が「合格」となったら、「▷ スキャンの監視」をクリックします（画面 2-16）。検証結果が「合格」以外を報告した場合は、検証結果のリンクをクリックして問題を確認し、問題を取り除いてから再検証してください。

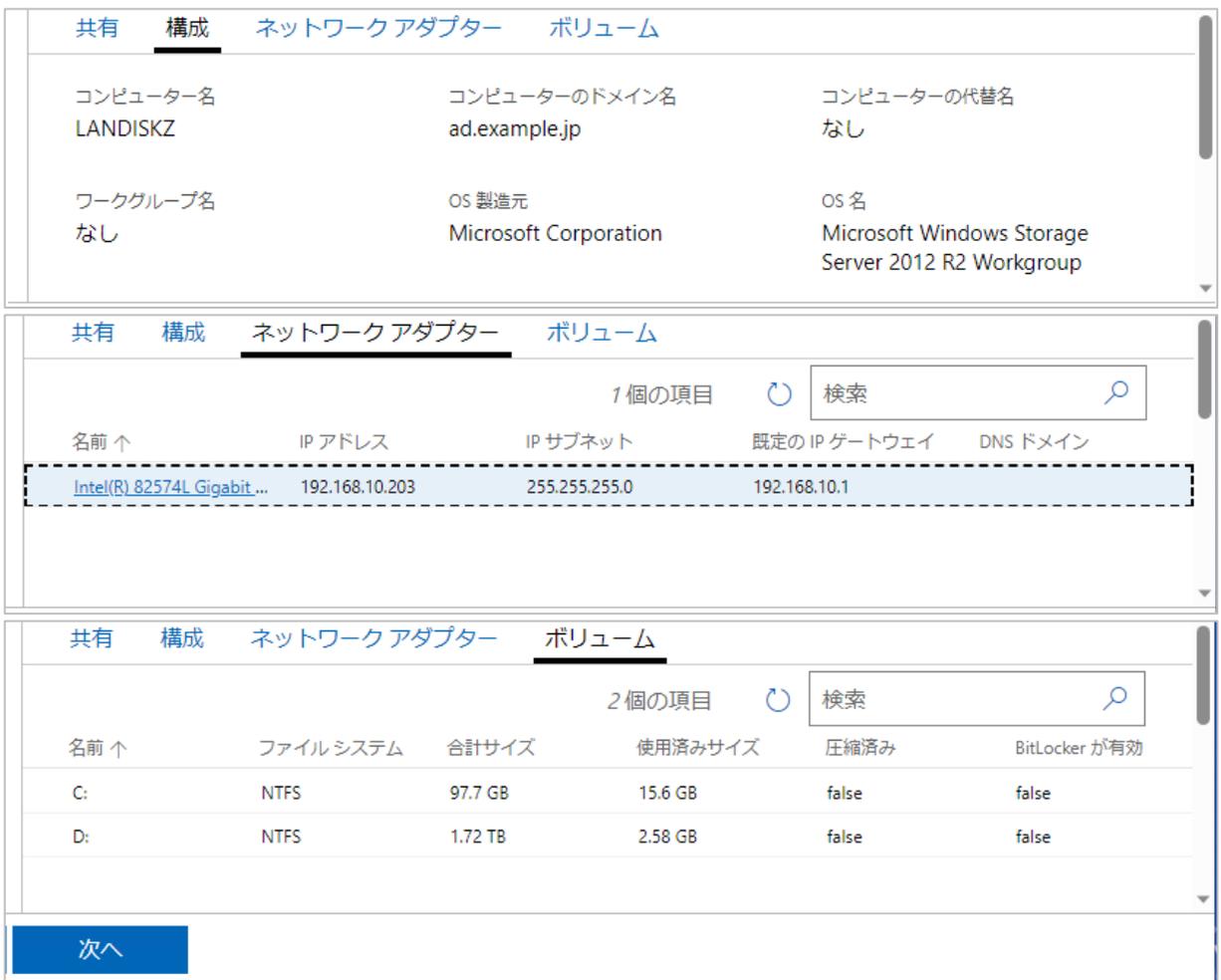


画面 2-16 追加したデバイスを「☰ 検証」し、「▷ スキャンの開始」を実行する

- スキャンが完了するとページが更新されます。移行元デバイスの「状態」が「成功」となったことを確認します（画面 2-17）。また、移行元デバイスを選択して、インベントリされた共有、構成、ネットワークアダプター、ボリュームを確認します。最後に「次へ」をクリックして、次のステップ（転送フェーズ）へと進みます（画面 2-18）。



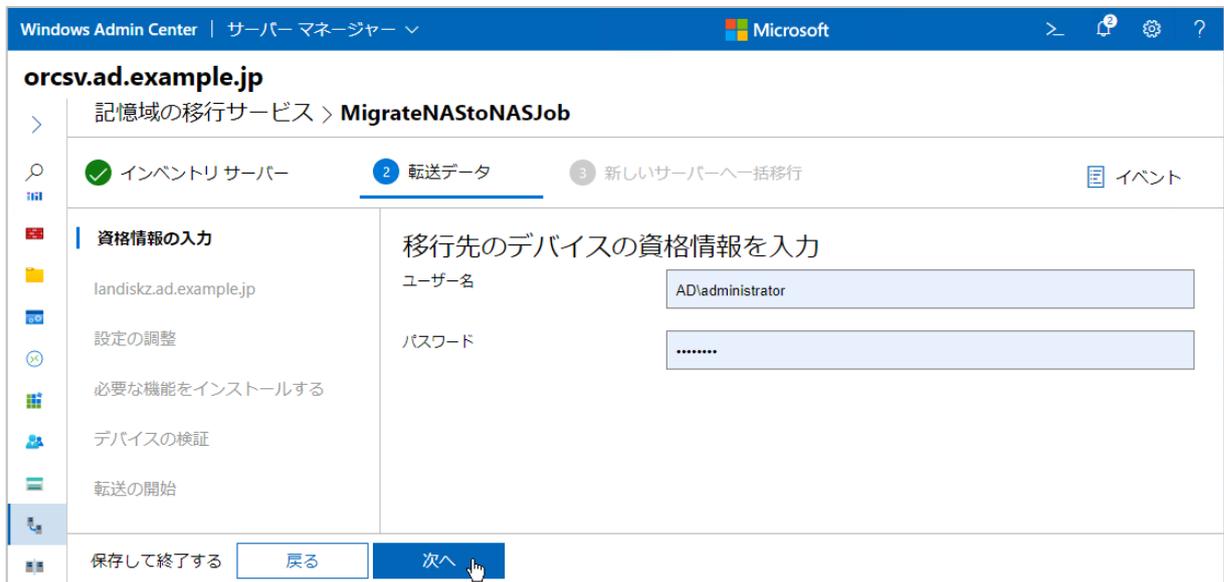
画面 2-17 スキャン結果を確認する



画面 2-18 移行元デバイスのインベントリを確認し、「次へ」をクリックする

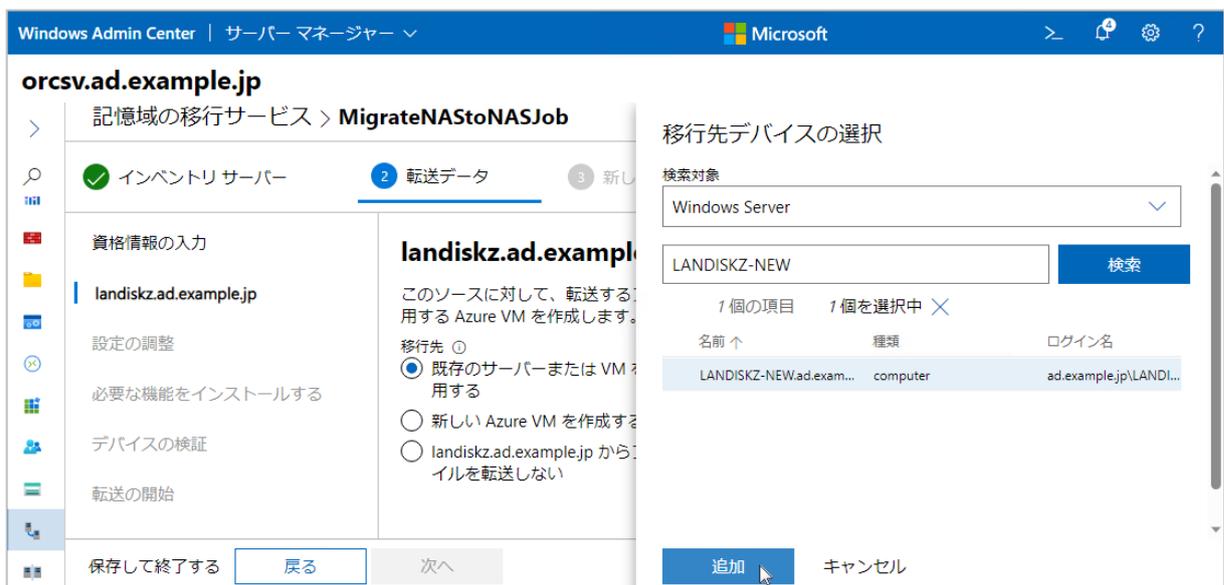
続いて、ウィザードは移行手順のステップ 2（転送フェーズ）に進みます。

1. 移行ジョブのウィザードは「② 転送データ (Transfer data、より適切な訳は“データ転送”)」に進みます。最初の「資格情報の入力」ページで移行先デバイスの資格情報としてドメイン管理者の資格情報 (ドメイン名¥Administrator など) を入力し、「次へ」をクリックします (画面 2-19)。



画面 2-19 ドメイン管理者の資格情報を入力する

2. 「<移行元のデバイス名>の移行先を指定してください」のページで、「移行先」として「既存のサーバーまたは VM を使用する」を選択し、「参照」をクリックして Active Directory から移行先デバイスを検索し、「追加」をクリックします (画面 2-20)。なお、移行先デバイスがワークグループ環境の場合は、テキストボックスにコンピューター名を直接入力してください。



画面 2-20 移行先のデバイスを指定する

3. 移行先デバイスを指定したら「スキャン」をクリックします (画面 2-21)。「スキャン」ボタンは「参照」ボタンのすぐ横にありますが、解像度が低いと見えないかもしれません。その場合は Tab キーを使用して「スキャン」ボタンまで移動してください。



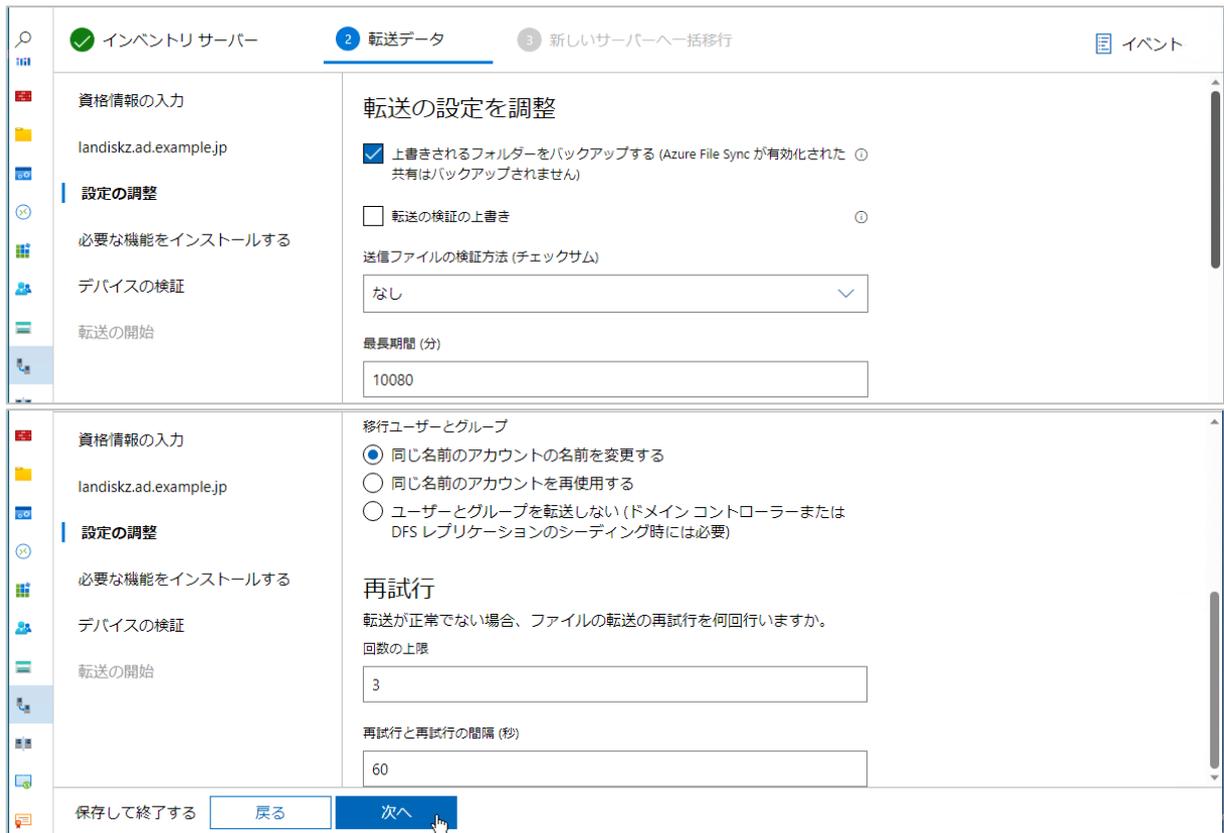
画面 2-21 「スキャン」をクリックしてスキャンの完了を待つ

4. スキャンが完了するとページが更新されるので、移行元デバイスのボリューム（ソースボリューム）と移行先ボリュームのマップを確認し、移行する共有フォルダーが選択されていることを確認して、「次へ」をクリックします（画面 2-22）。



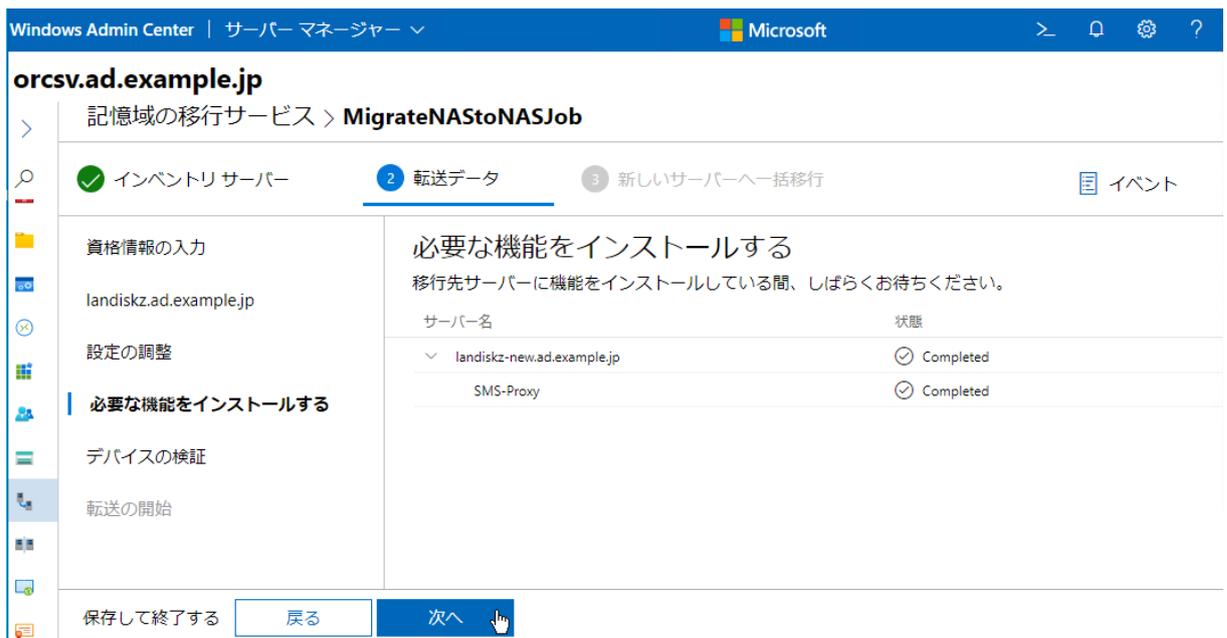
画面 2-22 ボリュームのマップと移行する共有を選択する

5. 「設定の調整」ページでローカルユーザーとグループの転送方法や、再試行回数などを必要に応じて調整し、「次へ」をクリックします（画面 2-23）。通常は、既定のまま進みます。既定では、「同じ名前のアカウントの名前を変更する」が選択されます。この設定では、移行元デバイスのすべてのローカルユーザーとグループが移行され、移行先に同じ名前のアカウントが見つかった場合、移行先デバイスの既存のユーザーまたはグループは新しい名前に変更されます。ただし、組み込みのユーザーおよびグループ（Administrator や Administrators）は、移行元と移行先デバイスで同じ名前を使用します。



画面 2-23 「設定の調整」ページでは、通常、既定値を受け入れ「次へ」をクリックする

- 「必要な機能をインストールする」ページで、移行先デバイスに必要な機能がインストールされるまでしばらく待ち、ストレージ移行サービスプロキシ (SMS-Proxy) のインストールが完了したことを確認したら、「次へ」をクリックします (画面 2-24)。インストールを開始するために資格情報の入力が必要だった場合は、ドメイン管理者 (ドメイン名¥Administrator など) の資格情報を入力してください。



画面 2-24 移行先デバイスにストレージ移行サービスプロキシ (SMS-Proxy) がインストールされる



資格情報の暗号化エラー

移行先デバイスへの必要な機能のインストール時に資格情報の入力が必要とされたとき、正しい資格情報を入力しているのにも関わらず、以下の画面 2-25 のようなエラーが表示される場合は、「キャンセル」をクリックして資格情報の入力パネルを閉じ、ウィザードの左下にある「保存して終了する」をクリックしてウィザードを終了します。その後、ブラウザを再起動して、「サーバーマネージャー」に移行先デバイスを登録し、ドメイン管理者の資格情報を使用してエラーなしで接続できることを確認してください。接続できることを確認したら、オーケストレーターサーバーの「記憶域の移行サービス」ツールから移行ジョブを再開します。



画面 2-25 このようなエラーが表示された場合は、「保存して終了する」をクリックしてウィザードの現在までの状態を保存して、問題に対処する

- 「デバイスの検証」ページで「☰ 検証」をクリックします。検証結果が「合格」となれば問題ありません。合格以外の結果（警告）が報告された場合は、その内容を確認して、問題を取り除きます（画面 2-26）。



画面 2-26 「☰ 検証」をクリックしてその結果を確認する

前の手順 6 で転送先デバイスにストレージ移行サービスプロキシ (SMS-Proxy) がインストールされますが、特定の状況下では登録に失敗し、「警告：移行先プロキシが見つかりませんでした」という検証エラーが報告されます。この問題を解決するには、オーケストレーターサーバーの PowerShell で以下のコマンドラインを実行し（画面 2-27）、もう一度「☰ 検証」をクリックします。ワークグループ構成の場合はこの検証エラーを解消する方法がないため、無視して「転送の開始」へと進んでください（ただし、オーケストレーターサーバーの SMS-Proxy が代わりに使用されるため、転送は低速になります）。

PS C:¥> Register-SMSProxy -ComputerName <移行先デバイスの FQDN> -Force

画面 2-27 「警告：移行先プロキシが見つかりませんでした」検証エラーを回避する

8. デバイスの検証が合格したら「次へ」をクリックし、「転送の開始」ページで「▶ 転送の開始」をクリックします（画面 2-28）。

画面 2-28 「▶ 転送の開始」をクリックしてデータ転送を開始する

9. データ転送が開始され、「フェーズの詳細」ペインにデータ転送の進行状況が表示されます（画面 2-29）。



画面 2-29 データ転送の進行状況

10. データ転送が完了したら、状態が「成功」したことを確認します（画面 2-30）。他の状態が報告された場合は、「フェーズの詳細」の「転送の詳細」タブを表示し、「↓ 転送ログ」や「↓ エラーログのみ」をクリックして、ログファイル（CSV 形式）をダウンロードし、エラーの内容を確認します。ファイルのロックなどでスキップされたファイルがある場合は、ウィザードを再開して「▷ 転送の差異」を実行して、差分を転送します。ストレージ移行サービスは転送済みデータとフォルダーを認識するため、同じ移行ジョブで同じフォルダーが複数回コピーされることはありません。なお、スキップされたファイルが少数の場合は、カットオーバー後にデバイス間で手動でコピーすることもできます。



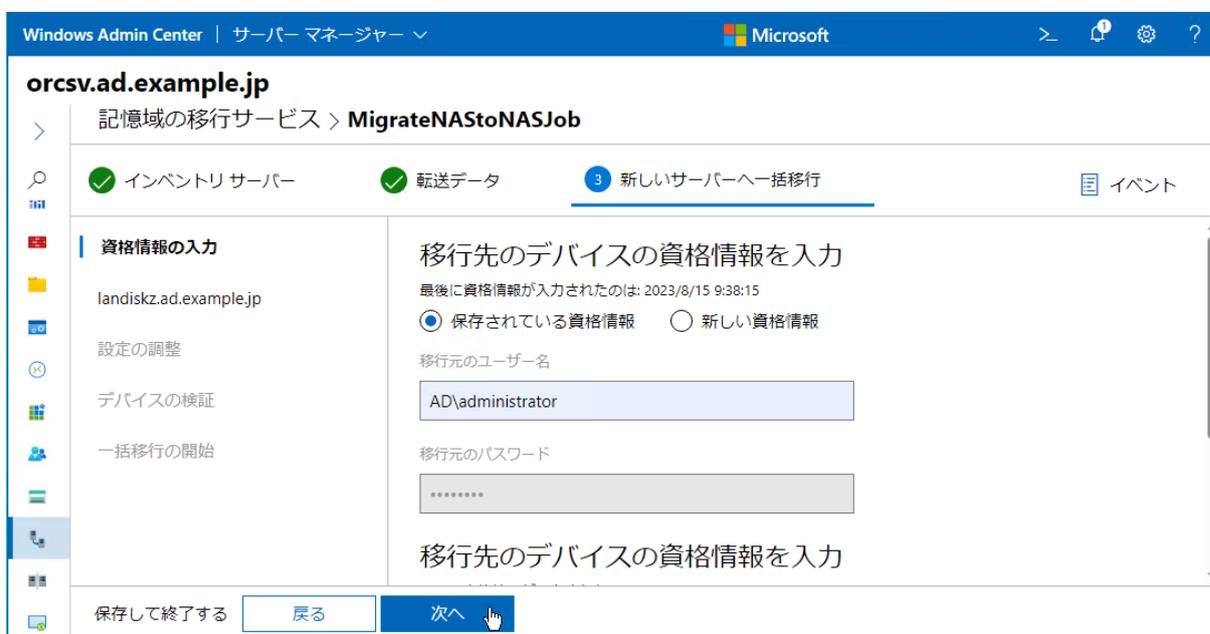
画面 2-30 転送結果とログを確認する（この例ではエラーログが 0KB であるため、エラーなし）

11. ステップ 2 のデータ転送が完了したら、「次へ」をクリックして次のステップ（一括移行フェーズ）へと進みます。

2.8 カットオーバーして移行先サーバーへの移行を完了する

データ転送が完了したら、新しいデバイスにカットオーバー（一括移行）して、IP アドレスとコンピューター名を切り替えます。

1. 移行ジョブのウィザードの「③ 新しいサーバーへ一括移行（Cut over to the new servers）」に進みます。ウィザードを中断した場合は、Windows Admin Center の「サーバーマネージャー」でオーケストレーターサーバーに接続し、「記憶域の移行サービス」ツールを開き、移行ジョブを再開して「③ 新しいサーバーへ一括移行」まで進みます。
2. 「資格情報の入力」ページでは「次へ」をクリックし、前回使用された保存されている資格情報（ドメイン管理者の資格情報）を再利用します（画面 2-31）。保存されている資格情報が利用できない場合は（ウィザードを中断後に再開した場合など）、「新しい資格情報」を選択して、ドメイン管理者（ドメイン名¥Administrator など）の資格情報を入力してください。



画面 2-31 移行ジョブの「③ 新しいサーバーへ一括移行」を開始する

3. 「<移行元デバイス>から<移行先デバイス>への一括移行を構成」ページで、「このデバイスを含める」、「ネットワーク設定を移行する」、「すべてのネットワークアダプターが移行されました」の 3 つのチェックボックスが選択されていることを確認し、移行元デバイスのネットワークアダプターの現在の設定を、移行先デバイスのどのネットワークアダプターに移行するか選択します（画面 2-32）。

また、移行元デバイスのネットワークアダプターにカットオーバー後に割り当てる IP アドレスを DHCP（推奨）または静的に設定します。静的な IP アドレスを設定する場合は、未使用の IP アドレスを指定してください。DHCP と静的 IP アドレスのいずれの場合でも、自動または固定割り当てされた DNS サーバーの設定は変更されません。さらに、「一括移行後に、移行元デバイスの名前を変更」で「ランダムに生成された名前を使用」または「新しい名前の選択」を選択し、「新しい名前の選択」を選択した場合は、カットオーバー後に移行元デバイスに設定するコンピューター名を入力し、「次へ」をクリックします。

インベントリサーバー 転送データ 3 新しいサーバーへ一括移行 イベント

資格情報の入力
landiskz.ad.example.jp
設定の調整
デバイスの検証
一括移行の開始

landiskz.ad.example.jp から landiskz-new.ad.example.jp への一括移行を構成

このデバイスを含める ネットワーク設定を移行する すべてのネットワークアダプターが移行されました

移行元のネットワークアダプター	移行先のネットワークアダプター
イーサネット Intel(R) 82574L Gigabit Network Connection IP 情報: 192.168.10.203/255.255.255.0 静的に割り当てられた IP アドレス DHCP の使用 <input checked="" type="checkbox"/>	イーサネット Intel(R) I210 Gigabit Network Connection #2 IP 情報: 192.168.10.204/255.255.255.0

一括移行後に、移行元のデバイスの名前を変更

ランダムに生成された名前を使用
 新しい名前の選択

新しい移行元コンピューターの名前: LANDISKZ-OLD

保存して終了する 戻る 次へ

画面 2-32 移行元デバイスと移行先デバイスのネットワークとコンピューター名を確認、設定する

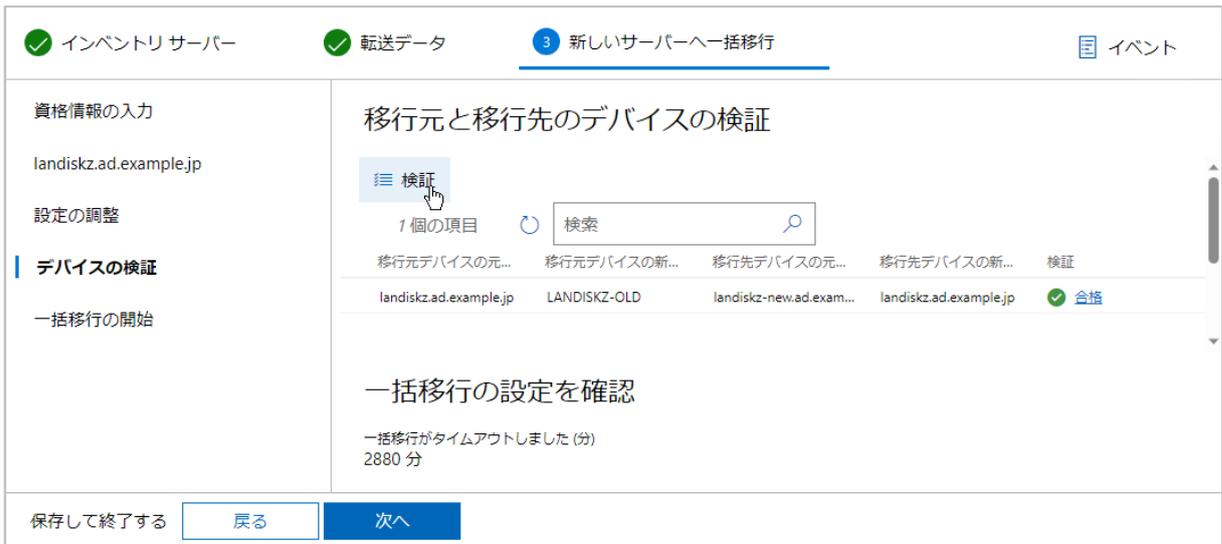


移行元デバイスと移行先デバイスの IP アドレスの入れ替えは不可

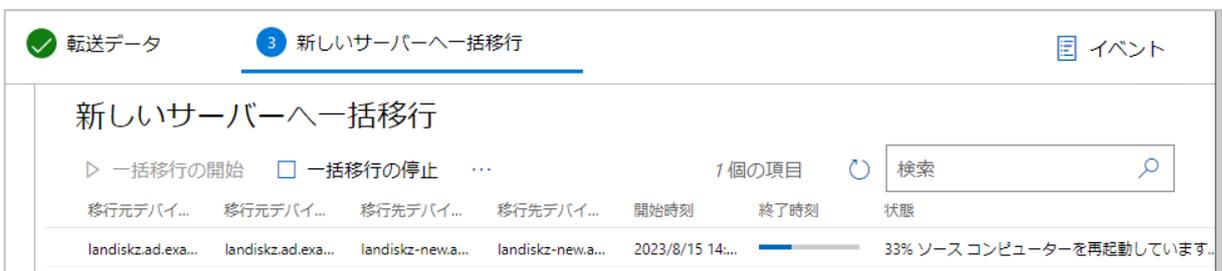
カットオーバー時に移行元デバイスのネットワークに静的 IP アドレスを設定する場合、移行先デバイスで使用していた IP アドレスを指定すると、一括移行の開始後に「38% ソースコンピューターのネットワークインターフェイスのマップ」でハングします（IP アドレスが 2 つのデバイスで重複した状態になります）。この状態でハングしてしまった場合は、オーケストレーターサーバーの PowerShell で以下のコマンドラインを実行し、移行ジョブのフェーズを「一括移行」から「転送」に戻します。その後、移行元デバイスのネットワーク設定やドメイン参加設定を元の状態に戻し、一括移行を再試行します。

```
PS C:\> Remove-SMSCutover -Name <移行ジョブの名前>
```

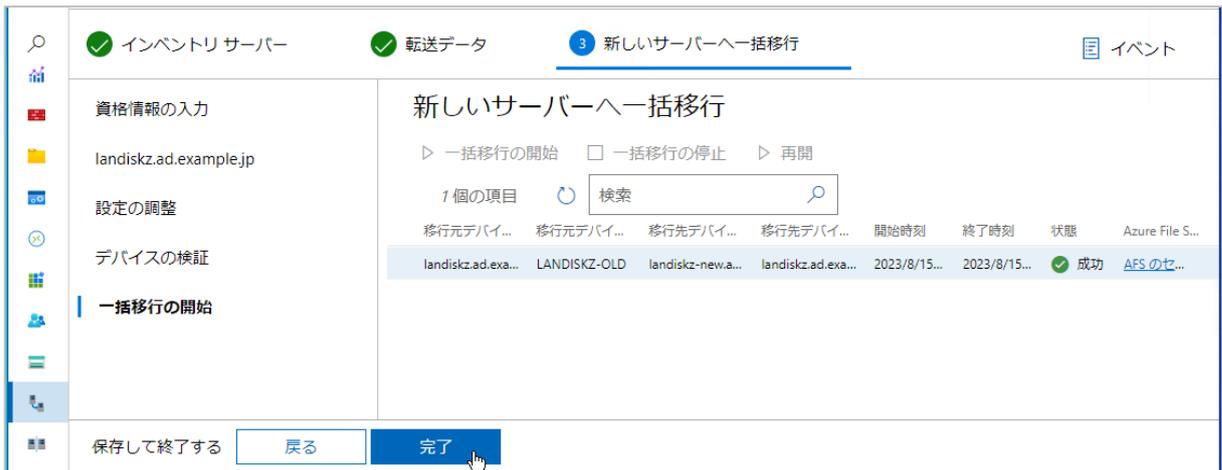
- 「設定の調整」ページでは、「AD 認証情報を入力する」で「保存されている資格情報」を選択し、「次へ」をクリックします。
- 「デバイスの検証」ページで「☰ 検証」をクリックし、検証結果が「合格」と表示されることを確認したら、「次へ」をクリックします（画面 2-33）。それ以外の検証結果が報告された場合は、検証結果のリンクをクリックして、問題を確認し、取り除いてから再度、「☰ 検証」を実行してください。



6. 「一括移行の開始」ページで「▷ 一括移行の開始」をクリックします（画面 2-34）。一括移行を開始すると、移行元デバイス（ソースコンピューター）と移行先デバイスが何度か再起動されます（画面 2-35）。開始する前に、移行元および移行先デバイスにローカルまたはリモートデスクトップ接続経由でログオン中のユーザーがある場合はログオフさせてください。移行中、デバイスの再起動や Active Directory および DNS の情報更新とレプリケーションの影響で、クライアントアクセスは一時的に利用できなくなります。

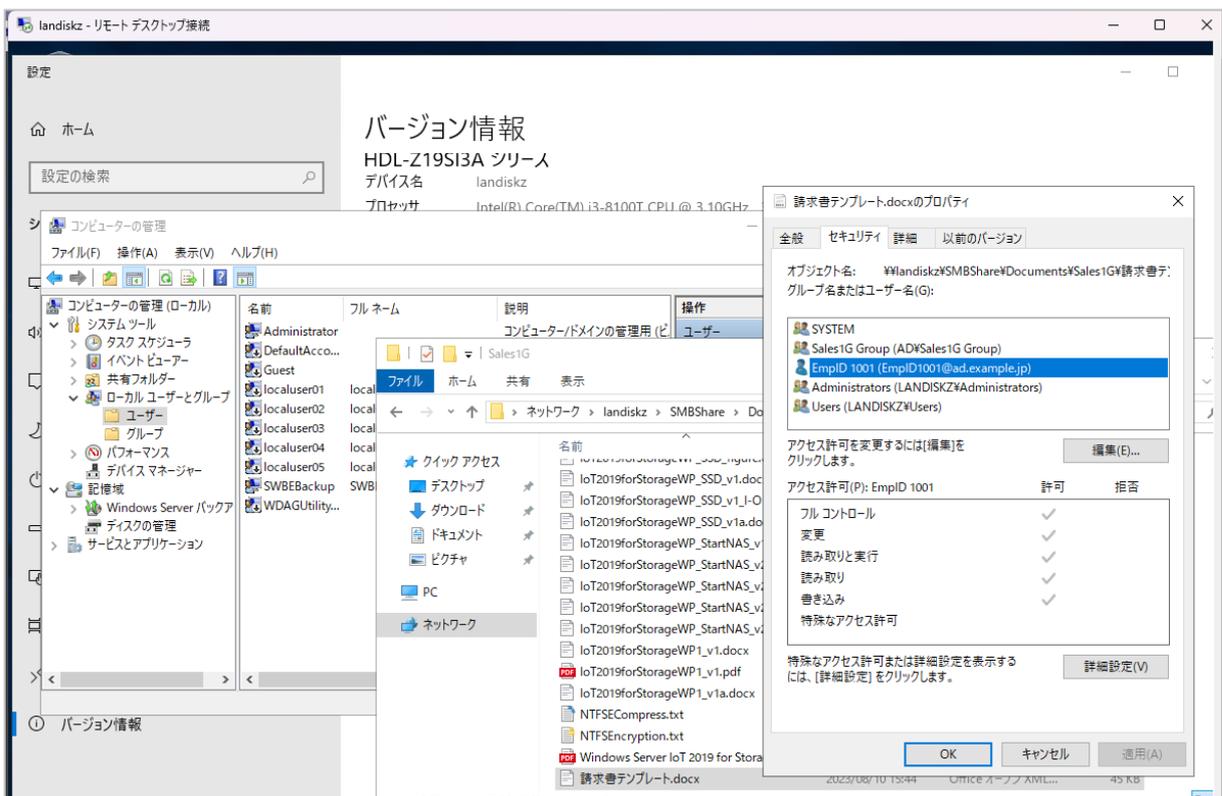


7. 一括移行フェーズの状態が「成功」したことを確認し、「完了」をクリックします（画面 2-36）。



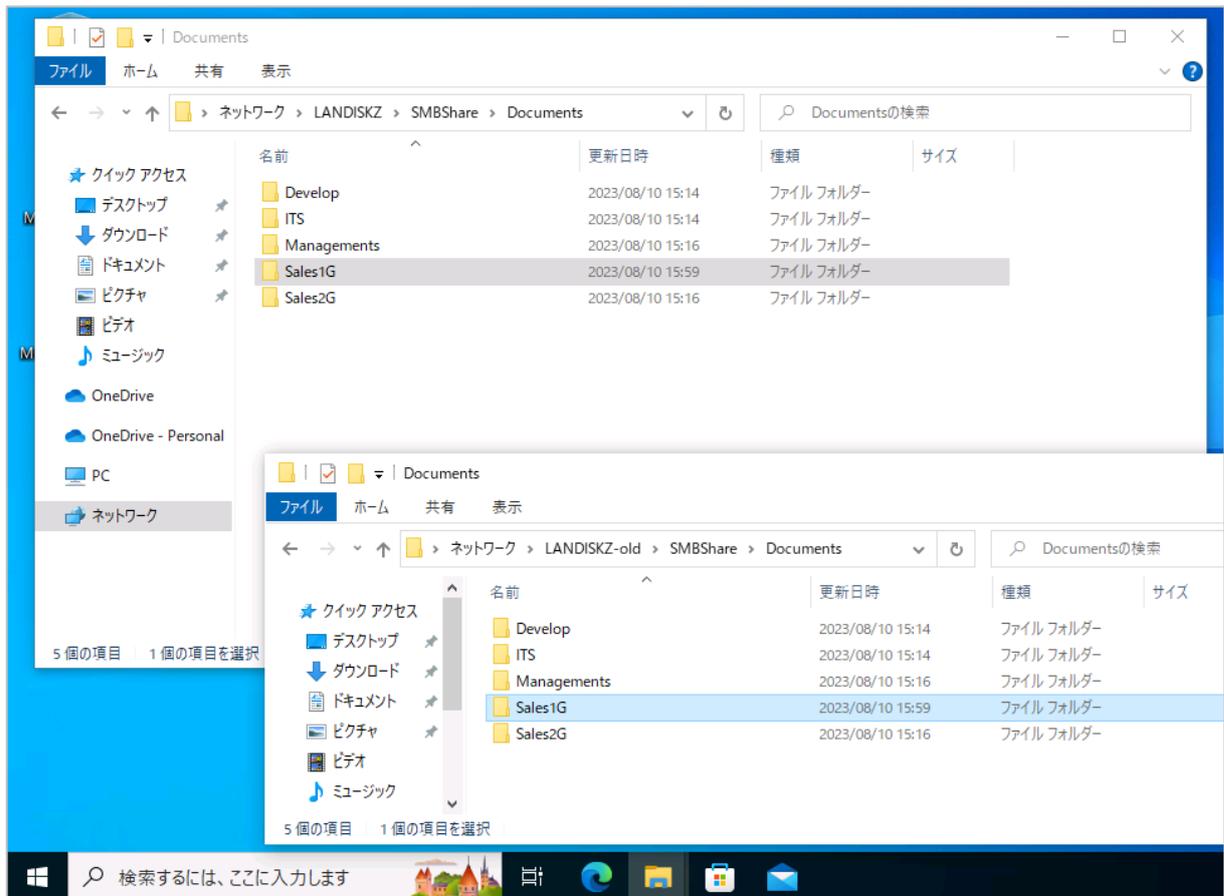
画面 2-36 一括移行フェーズの完了

- これで移行元デバイスのコンピューター名と IP アドレスは、移行先デバイスに切り替わりました。移行先デバイスにリモートデスクトップ接続して、コンピューター名やネットワークの設定、共有、データ、およびアクセス制御リスト (ACL) やその他の属性 (NTFS 圧縮や暗号化)、ローカルユーザーとグループが移行されていることを確認します (画面 2-37)。



画面 2-37 移行先デバイスに設定とデータが移行されたことを確認する

クライアントからアクセスする際のネットワークパス (UNC 名やネットワークドライブの割り当て) は、何も設定を変更しなくても、新しい移行先デバイスに対して有効になります。また、移行元デバイスは、カットオーバー後の名前 (ランダムな名前または指定した名前) で引き続きアクセスすることができます。(画面 2-38)。



画面 2-38 新しいデバイスの共有へのクライアントからのアクセスは、古いデバイスで使用していたパスをそのまま使用できる。古いデバイスが撤去されるまでは、古いデバイスの共有へのアクセスも可能

i 手でカットオーバーする

移行ジョブの新しいデバイスへのカットオーバー（一括移行）が何らかのエラーで成功しない場合でも、移行ジョブのデータ転送まで進んでいる場合は、移行ジョブを削除して、以下の手順を手動で行うことで、新しいデバイスに切り替えることができます。ただし、この場合、移行元デバイスのコンピュータアカウントのセキュリティ設定の一部や、ローカルユーザーとグループの設定は移行されません。

- 移行元デバイスをワークグループ構成にして、ドメインから切り離す（要再起動）。
- 移行元デバイスのコンピューター名と IP アドレスをカットオーバー後の値に変更する（要再起動）。
- 移行元デバイスをドメインに参加させる（要再起動）。
- 移行先デバイスのコンピューター名と IP アドレスを移行元デバイスの元の値に変更する（要再起動）。

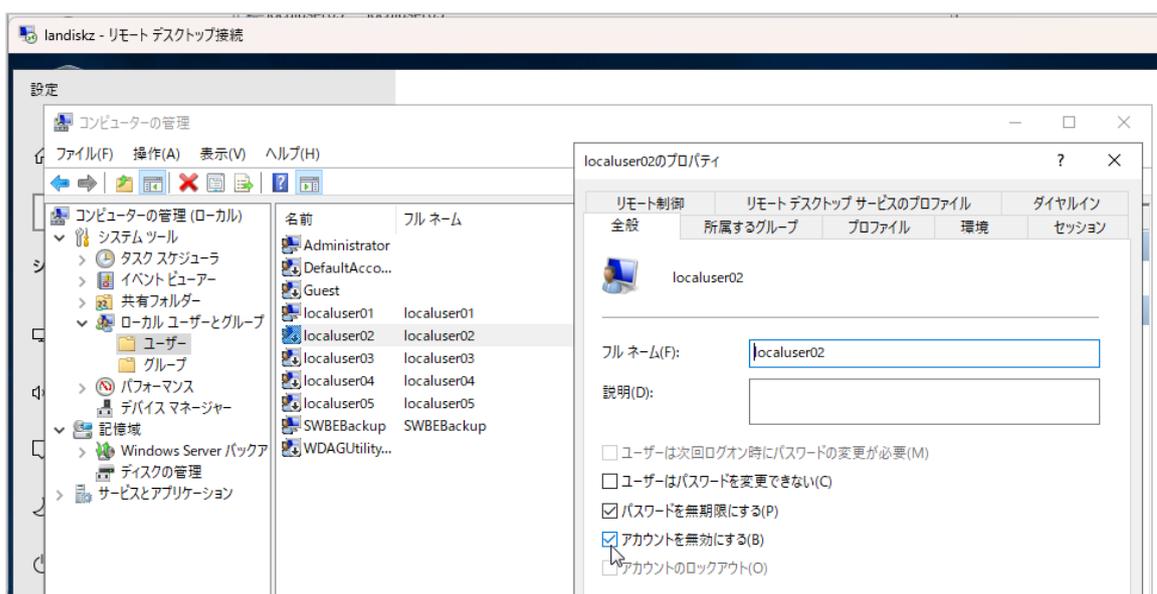


移行後に必要な作業

NAS デバイスを移行した後、次の作業を行う必要があります。

- 移行されたローカルユーザーの有効化とパスワードの再設定

ローカルユーザーとグループを新しいデバイスに移行した場合、移行されたローカルユーザーのアカウント（Administrator など組み込みのアカウントは除く）は移行先で無効にされ、複雑でランダムな 127 文字のパスワードが割り当てられます。ローカルユーザーのアカウントを引き続き使用するには、移行後にアカウントを有効にして新しいパスワードを割り当てる必要があります（画面 2-39）。Active Directory ドメインのアカウントとグループには影響しません。



画面 2-39 移行されたローカルユーザーにはランダムなパスワードが設定され、無効化される

- 移行元 NAS デバイスの撤去

移行元の NAS デバイスは、別のコンピューター名と別の IP アドレスで引き続き稼働し、データを保持しています。ファイルのロックなどで移行に失敗したファイルがある場合は、移行元の NAS デバイスから個別に移行先の NAS デバイスにメディアまたはネットワーク経由で手動でコピーできます。

すべての移行が完了したことを確認できた場合は、NAS デバイスをシャットダウンして電源をオフにし、ネットワークから切断して、その後、撤去します。なお、万が一、移行元のデータが必要になった場合に備えて、完全な撤去までにはある程度の期間を考慮することをお勧めします。

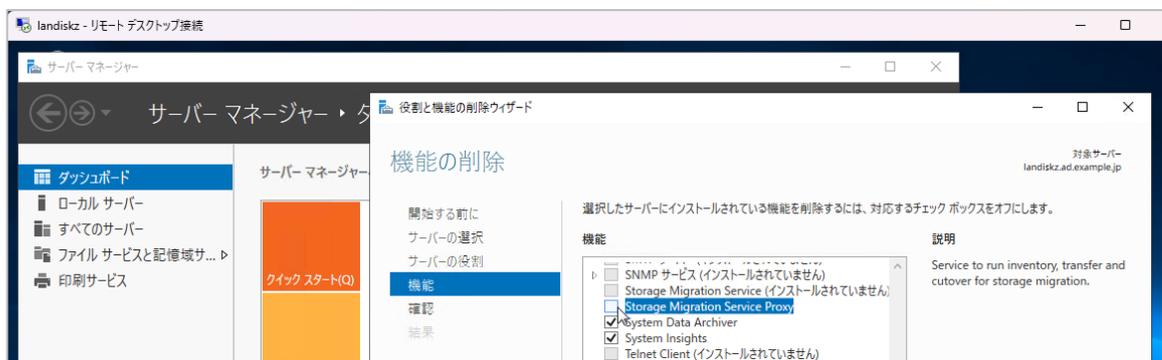
移行完了後は、Windows Admin Center のオーケストレーターサーバーから移行ジョブを削除することができます（画面 2-40）。



画面 2-40 移行ジョブの削除

- 移行先の NAS デバイスからの機能の削除

移行先の NAS デバイスには、オーケストレーターサーバーによりストレージ移行サービスプロキシ (Storage Migration Service Proxy、SMS-Proxy) のサーバーの機能がインストールされます。移行完了後は、Windows Admin Center の「サーバーマネージャー」の「役割と機能」ツールを使用して、またはリモートデスクトップ接続して「サーバーマネージャー」から開始する「役割と機能の削除」ウィザードを使用して、この機能を削除することができます (画面 2-41)。このサーバーの機能の削除には、OS の再起動が必要です。



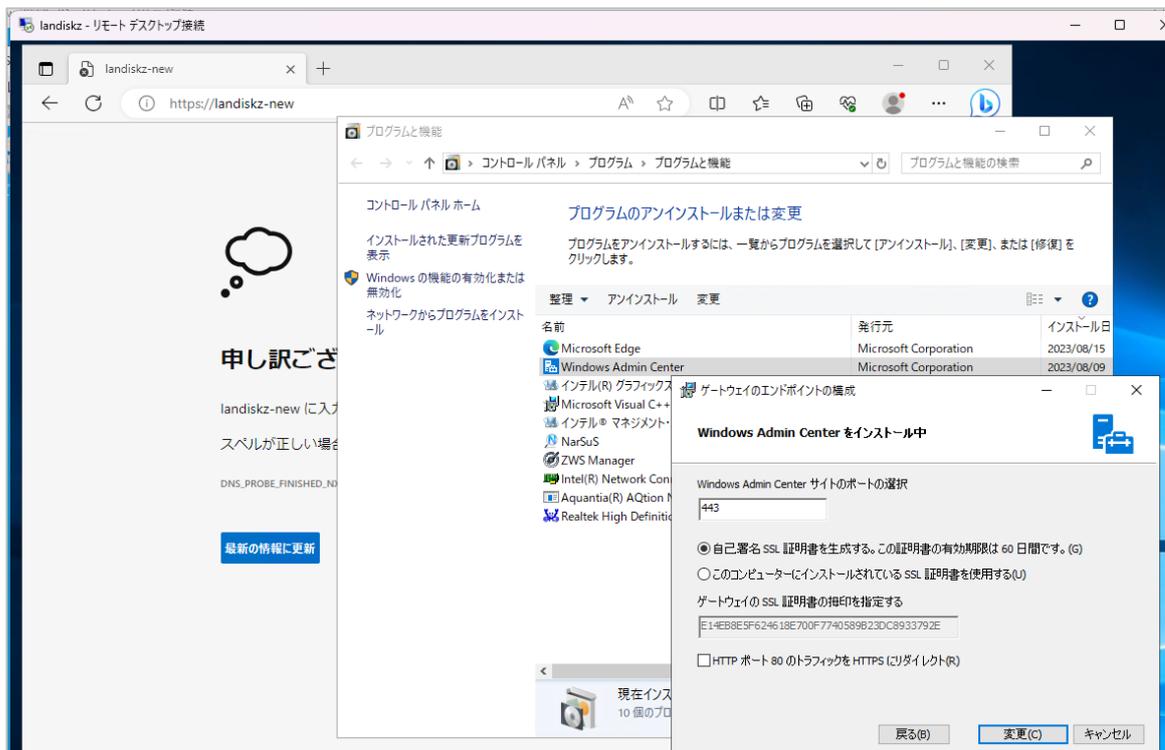
画面 2-41 移行先デバイスからのストレージ移行サービスプロキシの削除

- 移行先の NAS デバイスの証明書の確認

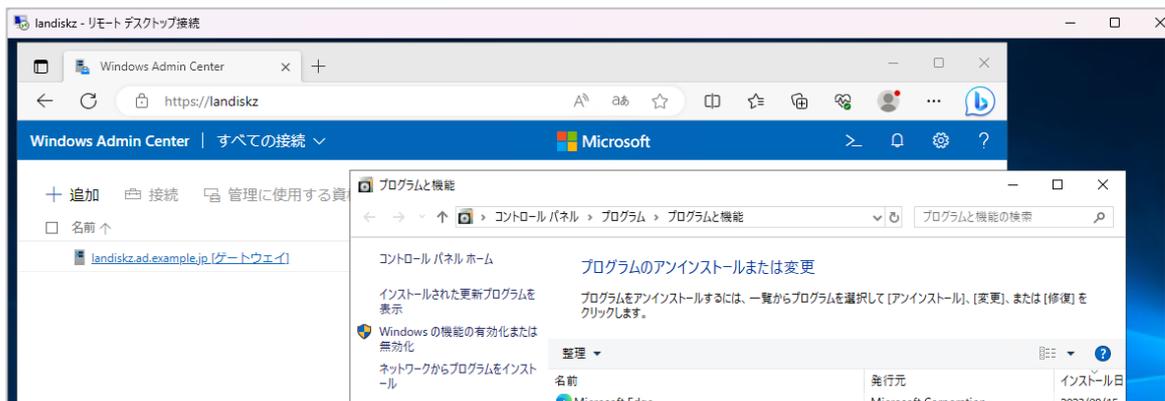
Active Directory 証明書サービスなどで発行された証明書や自己署名証明書を使用している場合 (IIS の Web サイトやゲートウェイモードの Windows Admin Center の TLS 証明書、リモートデスクトップ接続認証用のサーバー証明書など)、移行先のコンピューター名の変更されても、既存の証明書が自動的に変更されたり、再発行されることはありません。そのため、既存の証明書には、カットオーバー前のコンピューター名が含まれている場合があります。「証明書」スナップイン (Certlm.msc) やアプリケーションの管理ツールを使用して、使用されている既存の証明書を調べ、必要に応じて新しい証明書を発行して再設定してください。

例えば、NAS デバイスでゲートウェイサーバーモードの Windows Admin Center を自己署名証明書を使用してインストールしていた場合は、「プログラムのアンインストールまたは変更」

(appwiz.cpl) から「変更」を実行し、自己署名証明書を再生成する必要があります (画面 2-41、画面 2-42)。Active Directory 証明書サービスの証明書を使用していた場合は、新しい FQDN に対して証明書を再発行し、証明書を入れ替えます。



画面 2-41 コンピューター名が変更されたため、Windows Admin Center の証明書の変更が必要になる



画面 2-42 証明書の入れ替えにより、証明書エラーが解消される

著者紹介

山内 和朗 (やまうち かずお)

2023-2024 Microsoft MVP - Cloud and Datacenter Management

🌐 <https://mvp.microsoft.com/ja-JP/mvp/profile/655880b4-3c9a-e411-93f2-9cb65495d3c4>

略歴

フリーランスのテクニカルライター。大手 Sier のシステムエンジニア、IT 専門誌の編集者、地方の中堅企業のシステム管理者を経て、2008 年にフリーランスに。「山市良」の筆名で IT 専門誌や IT 系 Web メディアへの寄稿、IT ベンダーの Web コンテンツの制作、技術文書（ホワイトペーパー）の執筆、Windows 系技術書の執筆や翻訳を行う。2008 から現在まで Microsoft MVP Award を毎年受賞。岩手県花巻市在住。

近著

『[インサイド Windows 第7版 下](#)』（訳書、日経 BP 社、2022 年）

『[Windows 版 Docker&Windows コンテナー テクノロジ入門](#)』（日経 BP 社、2020 年）

『[Windows Server 2016 テクノロジ入門 改訂新版](#)』（日経 BP 社、2019 年）

『[Windows トラブル解決コマンド&テクニック集](#)』（日経 BP 社、2018 年）

『[インサイド Windows 第7版 上](#)』（訳書、日経 BP 社、2018 年）

『[Windows Sysinternals 徹底解説 改訂新版](#)』（訳書、日経 BP 社、2017 年）

ブログ

山市良のえめなんとかわーるど

🌐 <https://yamanxworld.blogspot.com/>