arcserve®

Rev:1.5

# Arcserve UDP & Arcserve OneXafe 連携ガイド（プライベート OneSystem 編）

**改定履歴**

2022 年 11 月　Rev 1.0 リリース

・前提ソフトウェア：Arcserve UDP 8.1 & OneXafe 4.0.0 & OneSystem 4.8

2023 年 3 月　Rev 1.1 リリース

・前提ソフトウェア：同上

・変更点：6 章 4 節および 7 章の追加

2023 年 5 月　Rev 1.2 リリース

・変更点：5 章 1 節の記述変更

2024 年 1 月　Rev 1.3 リリース

・変更点：複数ノードクラスタに関する記述の修正

2024 年 4 月　Rev 1.4 リリース

・変更点：P.16 画面ショットの誤表記の修正

2024 年 7 月　Rev 1.5 リリース

・変更点：8 章 シャットダウン方法の追加

# 1. はじめに

**ランサムウェア対策に、オンプレミスで使える不変ストレージ Arcserve OneXafe！！**

2022 年現在、データを暗号化して身代金を要求するランサムウェアが国内外で猛威を振るっています。特に被害が目立つのが、本番データのみならずバックアップデータも暗号化される事例です。犯罪者集団はバックアップがランサムウェア対策の要であることに気付き始めており、バックアップデータへの攻撃を強めています。

サイバー攻撃からバックアップデータを守る定番の方法はテープなどのメディアのオフライン保管です。しかし、この方法は定期的なメディアの交換が必要です。また、一定期間データの変更が不可能な、不変（Immutable）ストレージを提供するクラウド サービスもありますが、インターネット経由での接続になるので大容量のデータを預けにくいという課題があります。

Arcserve OneXafe（以下、本ガイド中では 「OneXafe」と呼称） はこのような課題を解決する第 3 の選択肢です。一見普通の NAS に見えながら、内部にスナップショットを保持するという構造を取るため、メディア交換の手間なくバックアップデータを保護できます。さらに実効容量 32 TB 以上のストレージで、バックアップ先としては十分なデータをオンプレミス環境に保持できます。

本ガイドでは、イメージバックアップ ソフト Arcserve UDP の二次バックアップ先として OneXafe を利用するための設定手順を解説します。Arcserve UDP は継続的な増分バックアップと独自の重複排除機能で、ランサムウェア対策に求められる複数世代のバックアップ データを少ないストレージ使用量で保持できます。また、本ガイドでは、Arcserve UDP のバックアップ データがサイバー攻撃で破壊された場面を想定し、OneXafe からのバックアップデータの復旧方法も紹介します。

このソリューションがランサムウェアの被害を防ぐ一助となれば幸いです。

# 2. OneXafe の用語と構成要素

## 2.1. 用語

以下、OneXafe を利用する上で使用するコンポーネント名を説明します。

### OneSystem

複数の OneXafe を統合管理する管理コンポーネントです。アカウントの登録や、共有フォルダの設定、スナップショットの保存期間の設定などを行えます。クラウドに構築された パブリック OneSystem と、オンプレミス環境に構築できる プライベート OneSystem の二種類があり、OneXafe を利用する上でいずれかの OneSystem を使用する必要があります。

本ガイドでは プライベート OneSystem を使用する方法を解説します。

### OneXafe Web コンソール（GUI）

OneXafe への IP アドレスの割り当てや、OneSystem への登録など、基本的な設定を行うための Web コンソールです。

### OneXafe ローカル コンソール（CLI）

OneXafe に直接接続したキーボードとモニタで操作できるコマンド ライン インターフェースです。スナップショットの操作や OneXafe に割り当てられている IP アドレスなどの確認を行えます。exconsole と呼ぶこともあります。

### iDRAC（integrated Dell Remote Access Controller）

ハードウェアの管理ツールです。OneXafe 4500 シリーズでは DELL 社のサーバを使用しており、ハードウェアの管理・設定に iDRAC を使用します。また、iDRAC の仮想コンソール機能を使用して、ネットワーク経由で OneXafe ローカル コンソールを操作する事も出来ます。

### Oneblox

OneXafe の旧称です。本ガイドでは製品画面上で指定されているものを除き、原則「OneXafe」と呼称します。

**StorageCraft**

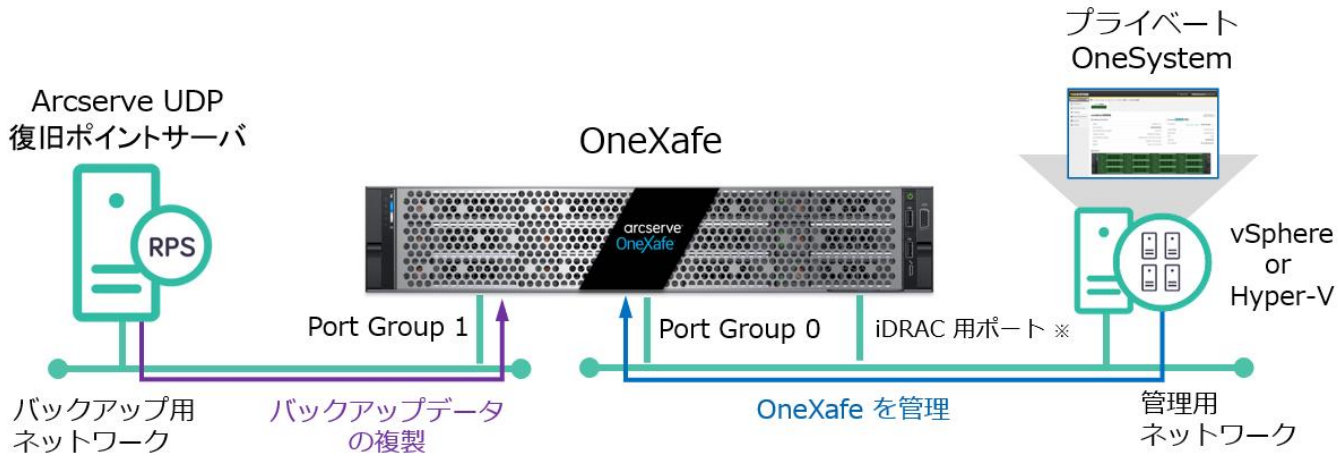
OneXafe の旧開発元/販売元です。2021 年に Arcserve と合併しました。

## 2.2. 構成

本ガイドでは以下の構成を想定し、主に OneXafe の設定方法/使用方法を解説します。

・バックアップ ソフトとして Arcserve UDP を使用します。
※ 本ガイドでは Arcserve UDP 8.1 での操作方法を紹介していますが、2023 年 3 月時点で最新の Arcserve UDP 9.0 でも操作感に違いはございません。
・Arcserve UDP 復旧ポイントサーバに保存されたバックアップ データを OneXafe 上に作成したデータストアに複製（レプリケート）します。
・OneXafe を管理するために プライベート OneSystem を利用します。
・プライベート OneSystem は仮想アプライアンスで、vSphere または Hyper-V 環境で動作します。

本ガイドで想定する構成




※ iDRAC 用ポートは Port Group 0 のネットワークと分けることも可能

# 3. OneXafe とプライベート OneSystem の初期設定

本章では OneXafe とプライベート OneSystem の初期設定方法を解説します。

## 3.1. プライベート OneSystem の要件

プライベート OneSystem の仮想アプライアンスの構築に必要な要件は以下となります。

a. 仮想ホスト（ Microsoft Hyper-V もしくは VMware ESXi )
b. インターネット接続　　注 1.
c. Arcserve サポート ポータルのアカウント
d. 電子メールアドレス　　注 2
e. ドメインネームサーバ（DNS） 注 2

注 1. インターネット接続はプライベート OneSystem の構築時のみの利用も可能です。
注 2 . 社内クローズドネットワーク上の SMTP サーバおよび DNS サーバをご利用出来ます。

a. プライベート OneSystem 4.8 の仮想アプライアンスは以下の仮想ホスト上で動作します。
vSphere 環境: VMware ESXi 6.5、6.7、7.0 （各 Update 含む）
Hyper-V 環境: Windows Server 2012 R2、2016、2019、2022

※ 仮想アプライアンスで必要なリソースや稼働する仮想ホストなどの詳細な動作要件については以下を参照ください。
https://support.arcserve.com/s/article/OneSystem-Compatibility-Matrix?language=ja

b. プライベート OneSystem はアカウント登録の際に TCP/443（Outbound） ポートを使い、外部 (Arcserve ライセンス サーバ) に接続します。
接続するホストの情報は以下のページを確認してください。

**Arcserve OneXafe プライベート OneSystem 展開ガイド**
**- プライベート OneSystem とライセンス サーバー間の通信**
http://documentation.arcserve.com/Arcserve-OneXafe/Available/JPN/OX_POS/default.htm#comm_between_pvtos_lic_server.htm

c. プライベート OneSystem のアクティベーション(有効化)の際に Arcserve サポート ポータルのアカウントを利用いたします。
Arcserve サポート ポータルのアカウントをお持ちでない場合は、以下を参照してあらかじめアカウントの作成を行ってください。

**Arcserve サポート ポータル マニュアル**
https://support.arcserve.com/s/article/202937699?language=ja

d. プライベート OneSystem の管理コンソールを操作する管理者アカウント用に電子メール アドレスを用意します。

e. プライベート OneSystem の仮想アプライアンスを DNS に登録し、d. の管理者アカウント用電子メールと SMTP サーバが利用出来るようにします。

### 3.2. 適用手順の概要

以下、プライベート OneSystem を使用して OneXafe を導入するための大まかな手順を記載します。
次節以降でこの手順の詳細を説明します。

**【 OneXafe 】**

1. OneXafe を設置し、ケーブル等を接続します。
2. （iDRAC を使用する場合）iDRAC の管理者アカウントのパスワードを変更します。
3. OneXafe Web コンソールにアクセスし、クラスタを設定します。
4. OneXafe Web コンソールで IP アドレスを設定します。

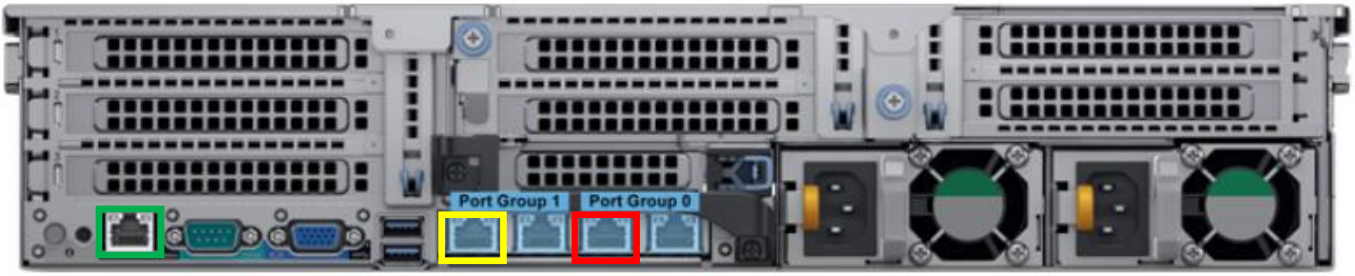
**【 プライベート OneSystem 】**

1. プライベート OneSystem のインストール モジュールをダウンロードします。
2. プライベート OneSystem の仮想アプライアンスを VMware ESXi ホストもしくは Hyper-V ホストに登録します。
3. プライベート OneSystem にアクセスし、メール アドレスを使用してユーザ アカウントを登録します。
4. OneXafe Web コンソール にアクセスし、プライベート OneSystem を登録します。
5. プライベート OneSystem コンソールで OneXafe を リング（クラスタ）に登録し、設定を行います。

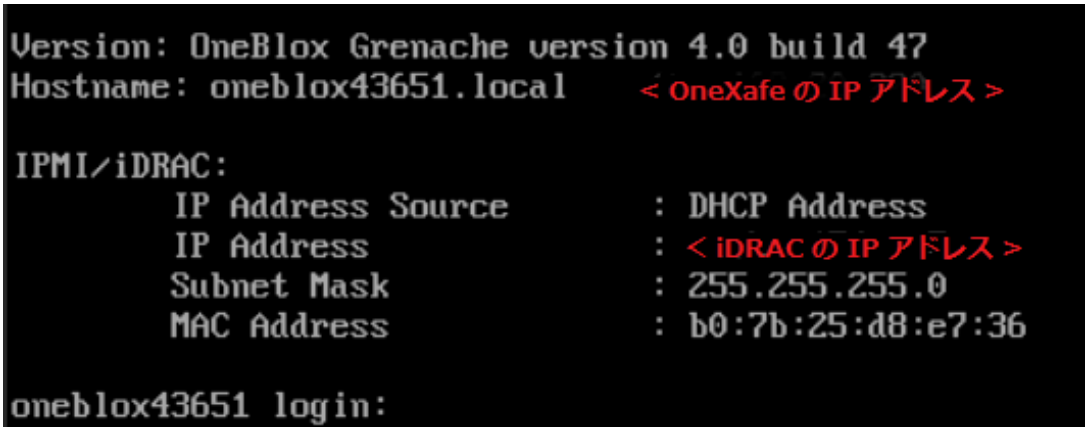
### 3.3. OneXafe の設置と iDRAC のパスワード設定

本節では OneXafe を設置し、iDRAC 管理者アカウントのパスワードを変更します。iDRAC は強力な管理機能で、OneXafe 上のデータを破壊することも出来てしまいます。そのため、**iDRAC を使用する場合は、必ず iDRAC の管理者パスワードを変更してください。**逆に iDRAC を使用しない場合は、本節の Step 3. ~6. の手順を省略できます。

**Step 1.** OneXafe を水平で安定した場所に設置し、背面にモニタとキーボード、電源ケーブル、LAN ケーブルを接続します。LAN ケーブルは管理用の “Port Group 0” のポート （赤枠） とデータ転送用の “Port Group 1” のポート （黄枠）に接続してください。また、必要に応じ iDRAC 用ポート （以下の画像左下、COM ポートの左隣にある LAN ポート （緑枠）） にも LAN ケーブルを接続します。




**Step 2.** OneXafe の背面にモニタや USB キーボードを接続し、OneXafe ローカル コンソールを開きます。OneXafe の IP アドレスや IPMI（iDRAC） の IP アドレス、その他の情報がモニタに表示されます。この情報を見るのにユーザ名やパスワードは不要です。



もし iDRAC ポートに IP アドレスが割り当てられていない（「0.0.0.0」と表示される）場合は、以下の手順で静的 IP アドレスを割り当てます。

**2-a.** OneXafe ローカル コンソールに “admin” でログインします。パスワードは OneXafe Web コンソールと同じです。デフォルトの パスワードは “config” です。ログインしたら、以下のコマンドを順に実行します。（左肩の数字は入力しません。）

1. ipmi
2. lan static <<iDRAC ポートの静的 IP アドレス>> <<サブネット マスク>>
3. apply

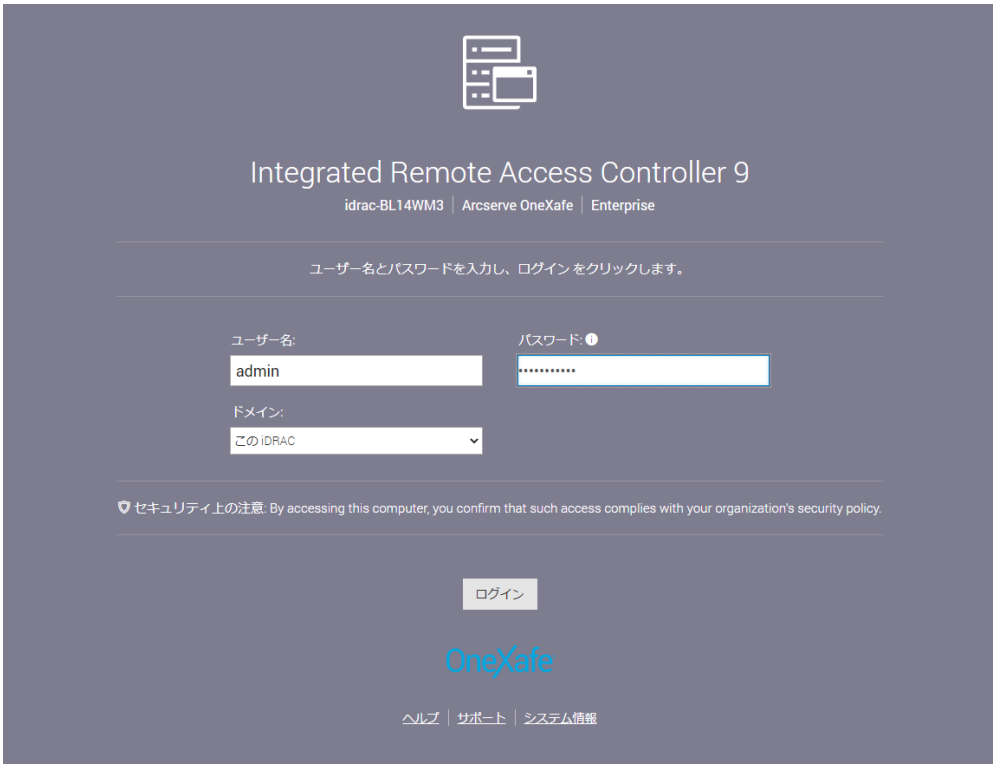
**2-b.** 以下のコマンドを入力し、iDRAC ポートに静的 IP アドレスが割り当てられている事を確認します。

1. show lan

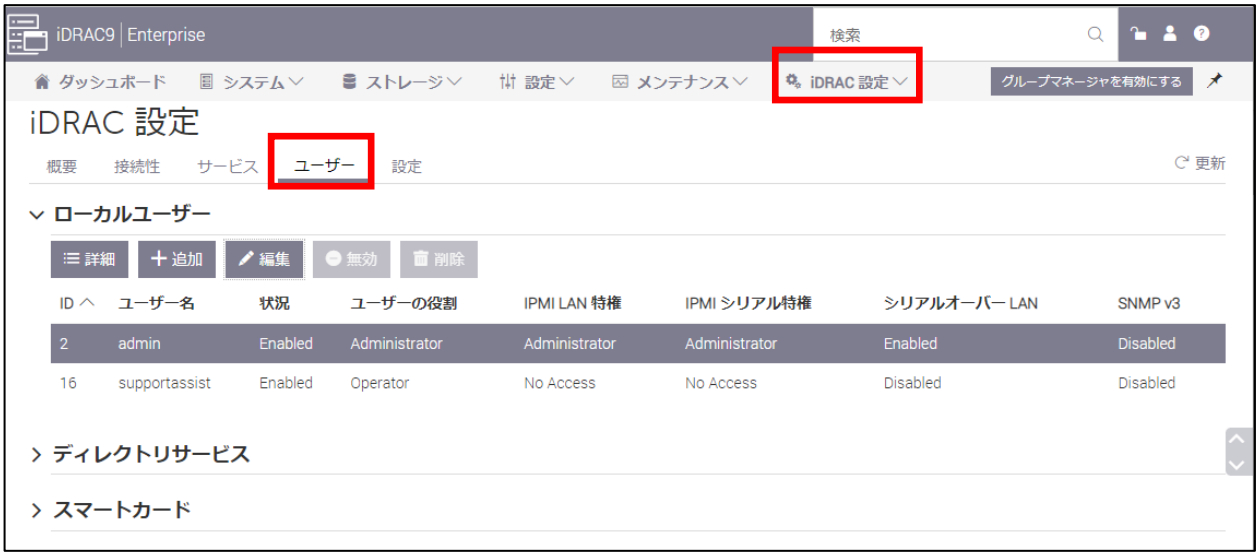
**Step 3.** パスワードを変更するには、まず iDRAC と同じネットワークに接続した Windows PC の Web ブラウザに Step 2. で取得した iDRAC の IP アドレスを入力します。

例：http://192.168.x.x

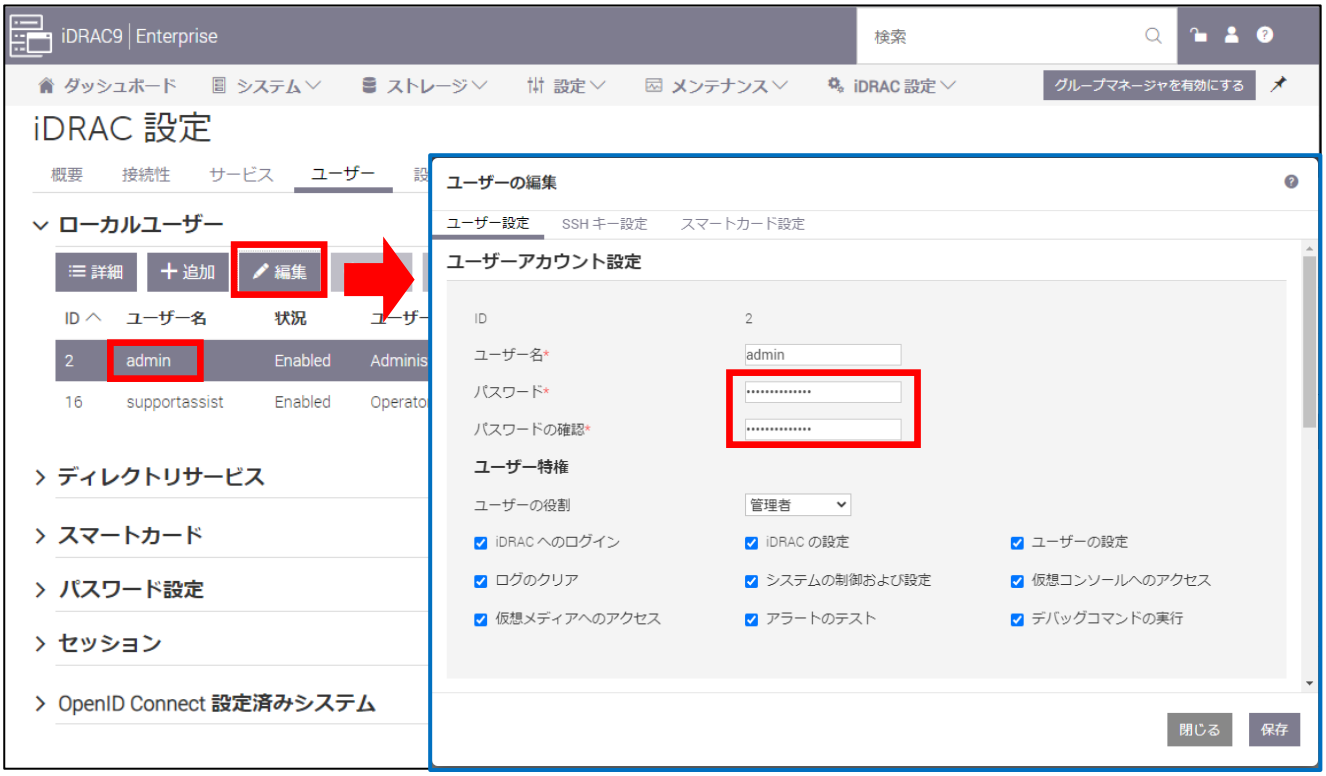
**Step 4.** iDRAC の管理画面が開かれます。デフォルトの[ユーザー名]/[パスワード]（admin/config）を入力し、[ログイン] ボタンをクリックします。



**Step 5.** iDRAC のメニューから [iDRAC 設定] を開き、[ユーザー] を選択して [ローカルユーザー] を表示します。




**Step 6.** [ユーザー名] から “admin“ を選択した上で、 [編集] をクリックして [ユーザーの編集] 画面を開きます。[パスワード] と [パスワードの確認] に新しいパスワードを入力して [閉じる] をクリックして iDRAC のパスワードを変更します。



## 3.4. OneXafe 単一ノードクラスタの設定

本節では OneXafe クラスタを設定します。クラスタは OneXafe の管理単位で、OneXafe を使用するにはクラスタの作成が必要です。本手順書の操作は OneXafe の筐体数が 1 台の構成で行います。
なお、複数筐体でのクラスタ構成については、本手順書に合わせて以下の構成ガイドを参照ください。

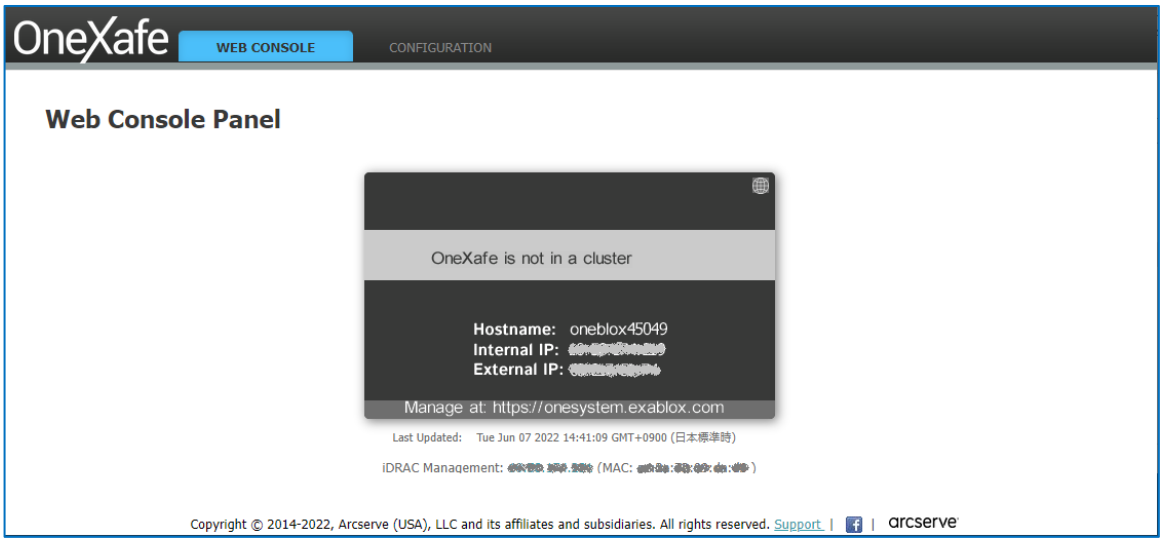
**Arcserve OneXafe 複数ノード クラスタ構成ガイド**
https://www.arcserve.com/sites/default/files/2023-10/OneXafe-Multi-Node-Cluster-Guide.pdf

**Step 1.** OneXafe Web コンソールにアクセスするため、OneXafe と同じネットワークに接続した Windows PC の Web ブラウザ に前節で取得した OneXafe の IP アドレスを入力します。

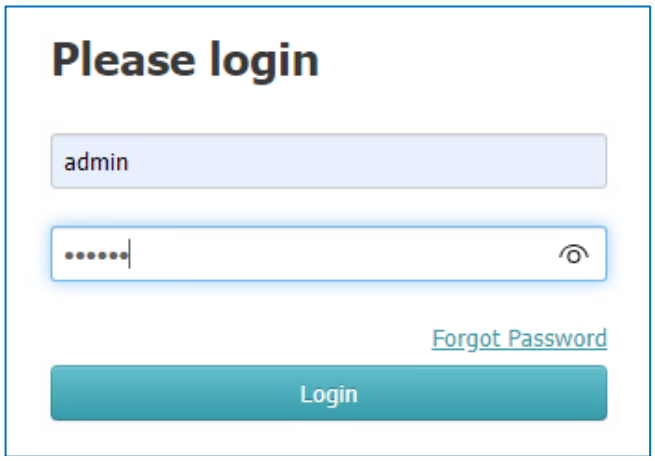
例：http://192.168.x.x

もし OneXafe が接続しているネットワークに DHCP サーバが存在しない場合、”169.x.x.x” という IP アドレスが割り当てられ表示されるはずです。この IP アドレスをブラウザに入力し、OneXafe Web コンソールに接続してください。

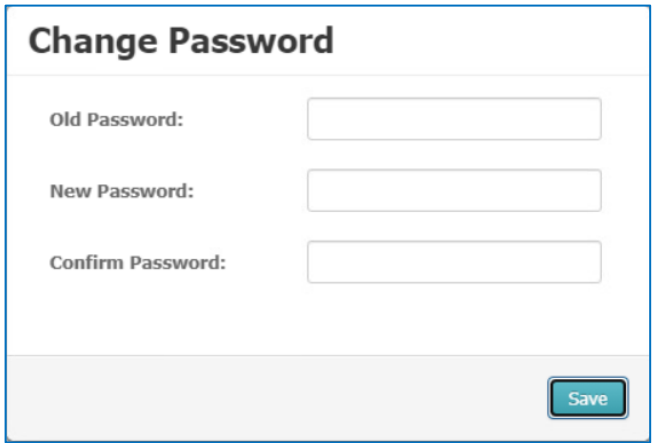
**Step 2.** OneXafe Web コンソールの画面上部に表示される [CONFIGURATION] をクリックします。



**Step 3.** デフォルト ユーザ名 “admin” とデフォルト パスワード ”config” を入力します。




**Step 4.** パスワードの変更を求められるので、安全なパスワードを入力します。



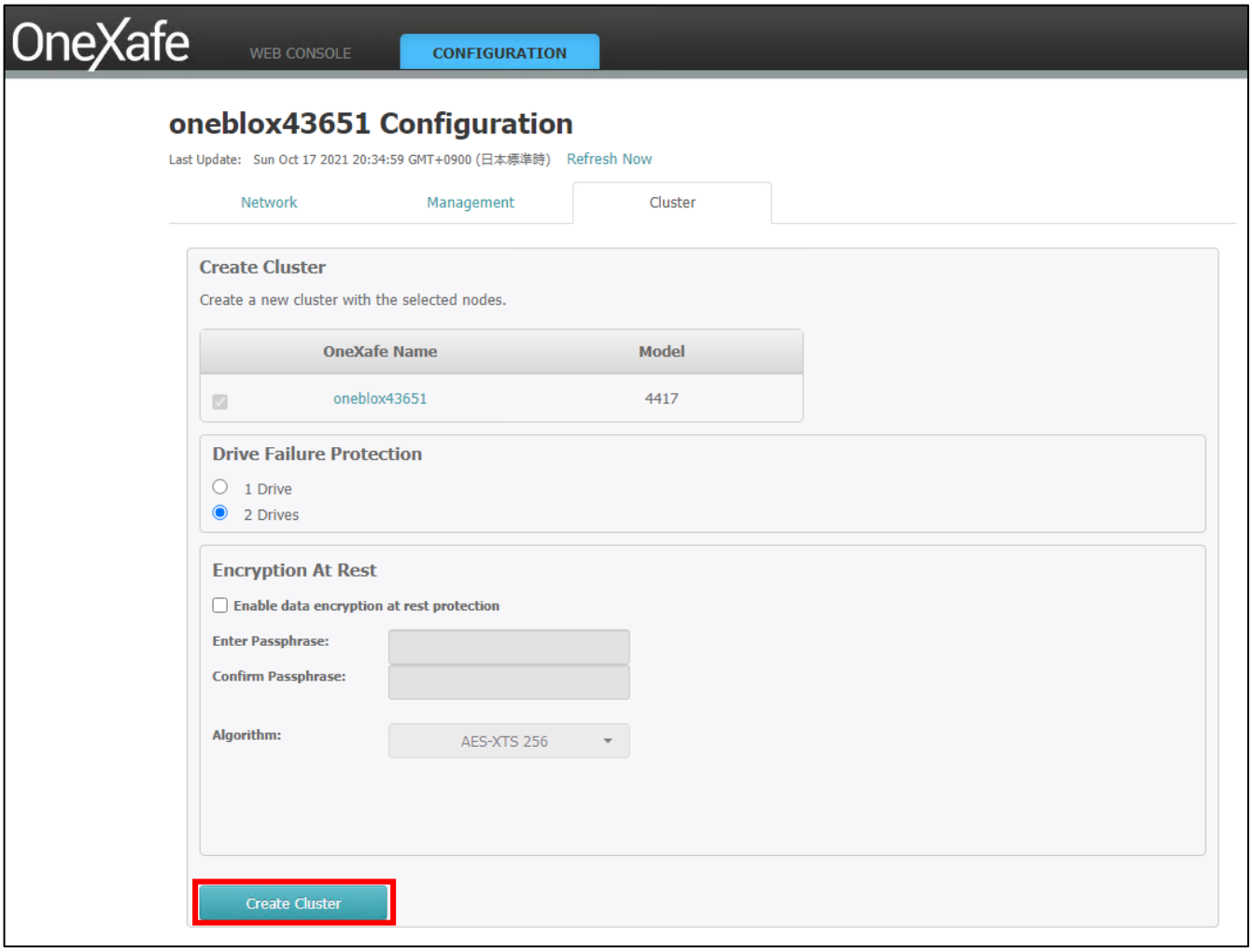
**Step 5.** 新しいクラスタを作るには、[Cluster] タブを開き、以下の操作を行います。

a. OneXafe ノードを選択します。

b. [Drive Failure Protection] ではデフォルトの “2 Drives” を選択します。

c. [Enable data encryption at rest protection] チェック ボックスは無効のままにします。

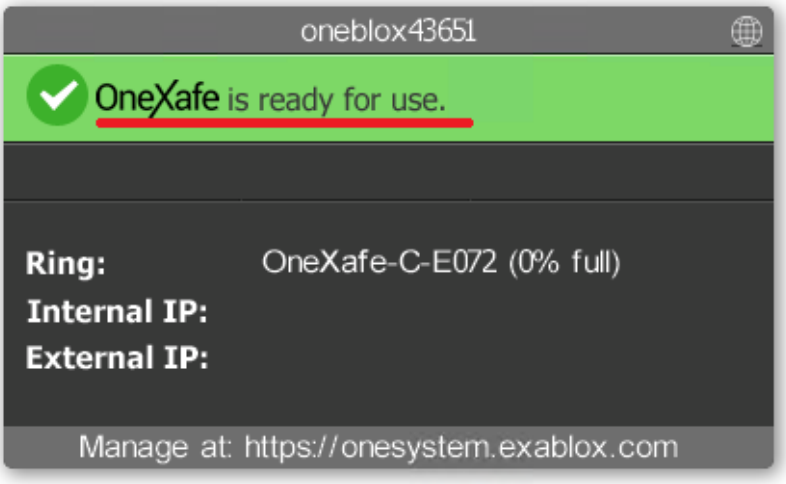
d. [Create Cluster] ボタンをクリックします。




**Step 6.** [Yes, Create Cluster] をクリックすると、以下のメッセージが表示され、クラスタの作成が始まります。


Note：クラスタが作成されるまで、ページにとどまることをお勧めします。 画面から移動したり、追加の変更を加えたりしようとすると、警告メッセージが表示されます。

**Step 7.** クラスタが作成され、使用できる状態になると、[WEB CONSOLE] タブのステータスが更新されます。




### 3.5. OneXafe の IP アドレスを設定

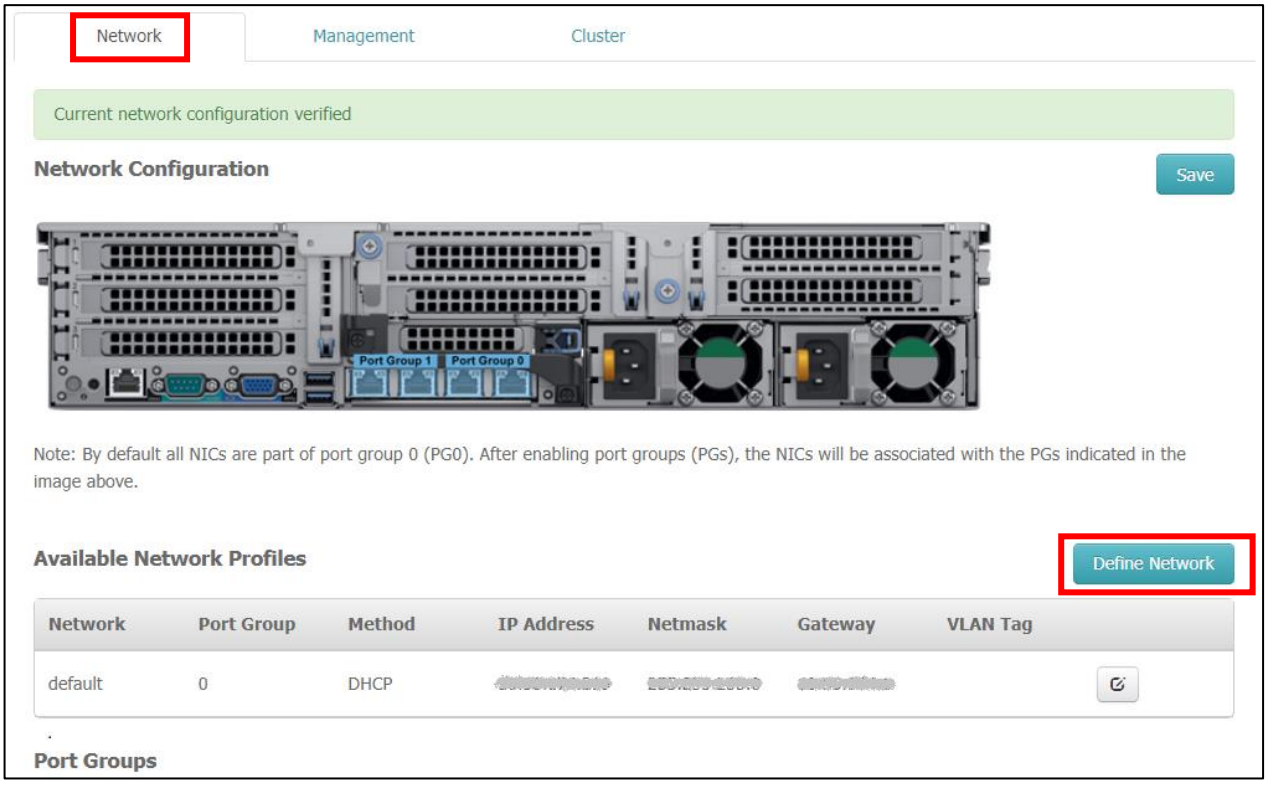
OneXafe の 各 Port Group に IP アドレスを設定します。

本ガイドの設定では、プライベート OneSystem と OneXafe を接続する管理用ネットワークは ”Port Group 0“ を、Arcserve UDP 復旧ポイントサーバ （RPS） と OneXafe を接続するバックアップ用ネットワークは “Port Group 1“ を使用します。

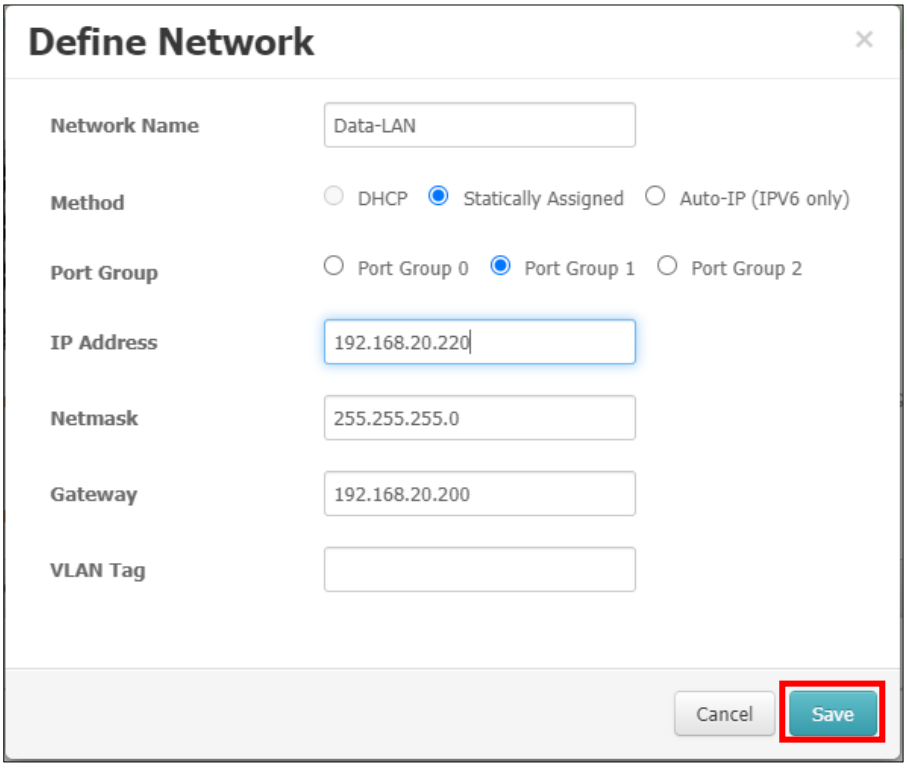
本ガイドではプライベート OneSystem に OneXafe を登録する管理用 IP 設定を簡略化するため ”Port Group 0“ は DHCP サーバの利用を設定していますが、静的（Static） IP アドレスを設定することも可能です。一方、“Port Group 1“ については静的（Static） IP アドレスを設定する必要があります。

なお、本ガイドの構成とは異なり、”Port Group 0“ を管理用ネットワーク兼バックアップ用ネットワークとして利用することも出来ます。

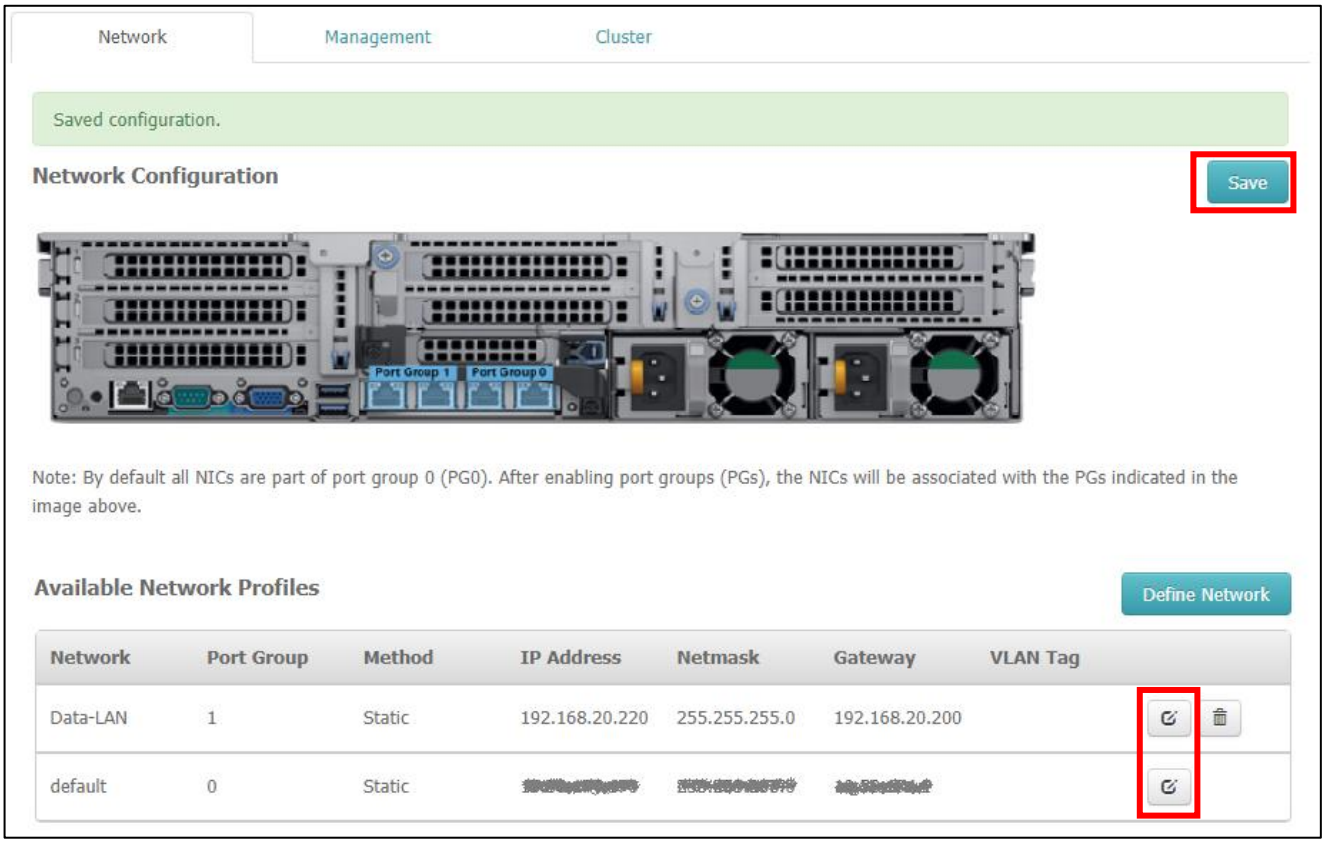
**Step 1.** “Port Group 1“ を定義するためには [CONFIGURATION] から [Network] タブを開き [Define Network] をクリックします。




**Step 2.** [Network Name] に何か名称を入力後、“Statically Assigned”、 “Port Group 1” を選択し、IP アドレスやその他、必要なネットワーク設定を入力して、[Save] をクリックします。



**Step 3.** “Port Group 1” の設定を確認し、[Save] をクリックします。なお、“Port Group 0” や “Port Group 1” の設定を変更する場合は、各ネットワーク プロファイルの右横にある [編集] アイコンをクリックします。




NOTE:
DHCP で割り当てられた IP アドレスを使って OneXafe Web コンソールにログインしており、その IP アドレスを静的 IP アドレスに変更した場合、OneXafe Web コンソールに再度アクセスするために新しい静的 IP アドレスを入力する必要があります。

以下、管理用ネットワーク（Port Group 0）と、データパス用ネットワーク（Port Group 1）の 2 つを設定する場合のベスト プラクティスです。

**管理ネットワーク（デフォルト） - Port Group 0**

・高速な接続は求められません。10GbE もしくは 1 GbE でも十分です。
・DHCP もしくは、静的 IP アドレスを設定します。
・OneSystem との接続のため、Path MTU discovery が使用されます。

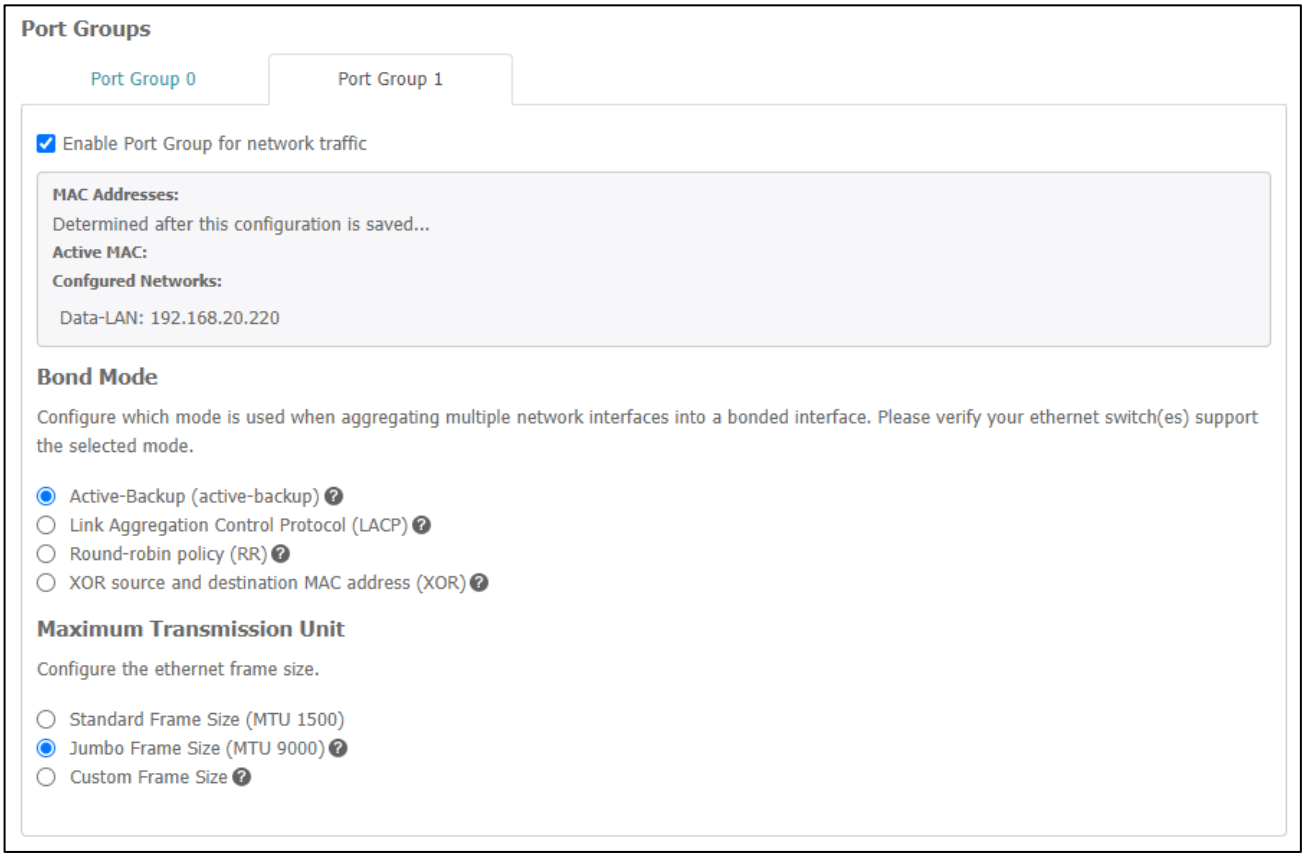
### データ パス – Port Group 1

SMB 共有などデータの転送に使われます。

・ネットワーク機器が対応している場合は、高速な通信のために LACP を選択いただけます。

・静的 IP アドレスを設定してください。

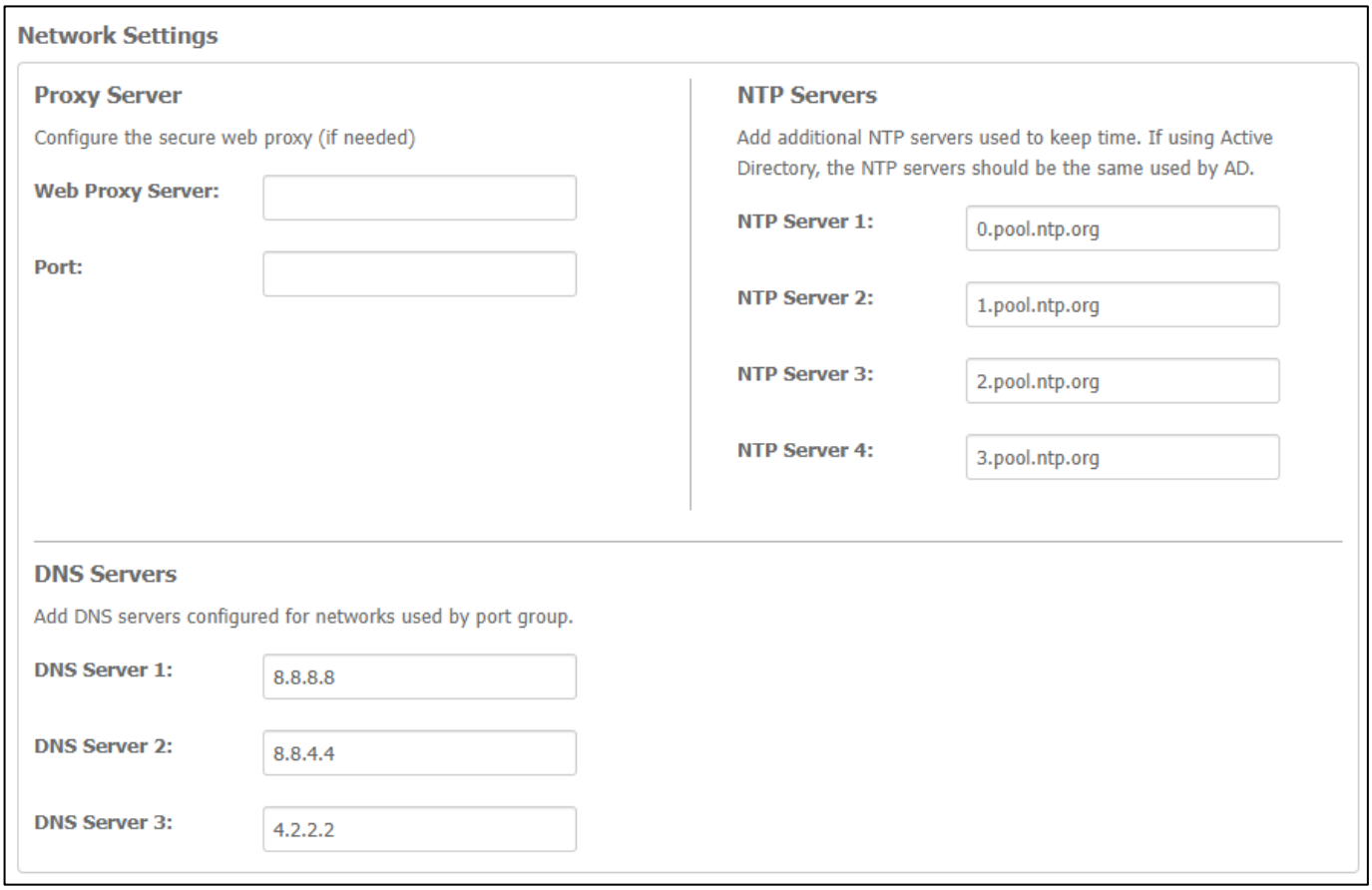
・MTU はご利用のスイッチに合わせてください。



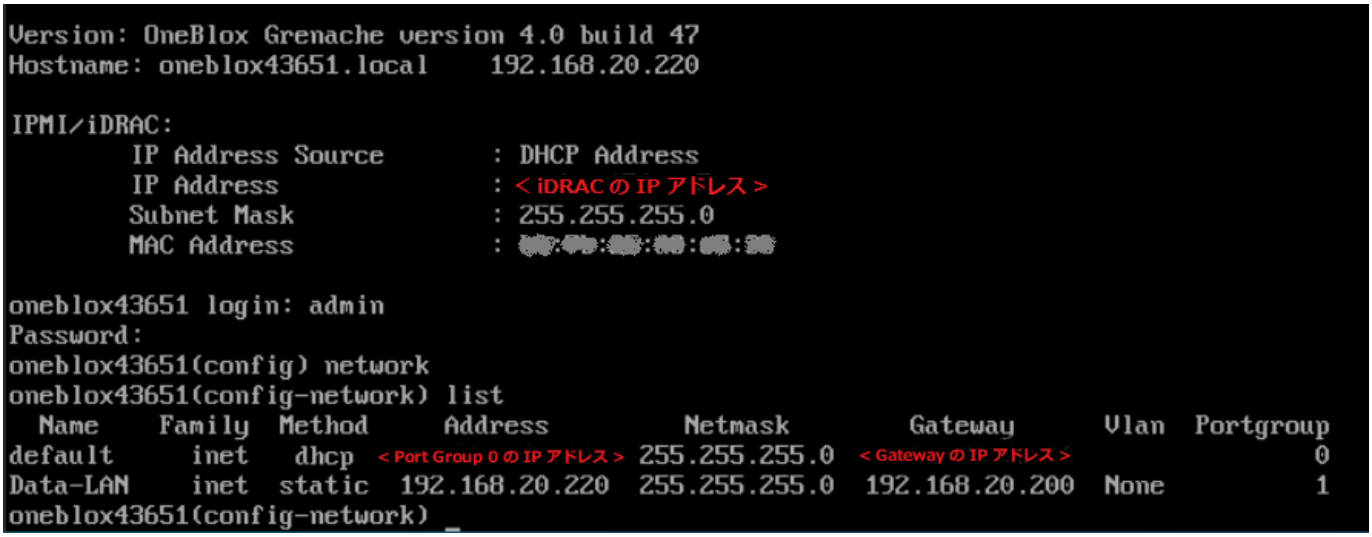

また、[Network] タブでは、Web Proxy サーバ、NTP サーバ、DNS サーバの指定ができます。必要に応じて指定してください。設定変更後は、**Step 3.** と同じ [Save] をクリックします。

※　Web Proxy サーバおよび、NTP サーバを指定しない場合でも特に問題ございません。

”Port Group 1” で設定した IP アドレスは、必要に応じて DNS に登録します。この際、”Port Group 0” の IP アドレスとは別のホスト名で登録してください。DNS が利用出来ないネットワークの場合は、IP アドレスを使用して OneXafe に接続してください。




NOTE:　OneXafe ローカルコンソールの画面で、IP アドレスなどが更新されていないようであれば、OneXafe の再起動を行ってください。



## 3.6. VMware 環境へのプライベート OneSystem 仮想アプライアンスの展開

プライベート OneSystem の仮想アプライアンスを VMware 環境で実行する場合は、
以下の手順に従ってプライベート OneSytem の仮想アプライアンスを展開します。

**注：**プライベート OneSystem の仮想アプライアンスを Hyper-V 環境で展開する場合は、
P.25 からの「**3.7. Hyper-V 環境へのプライベート OneSystem 仮想アプライアンスの展開**」
を参照ください。

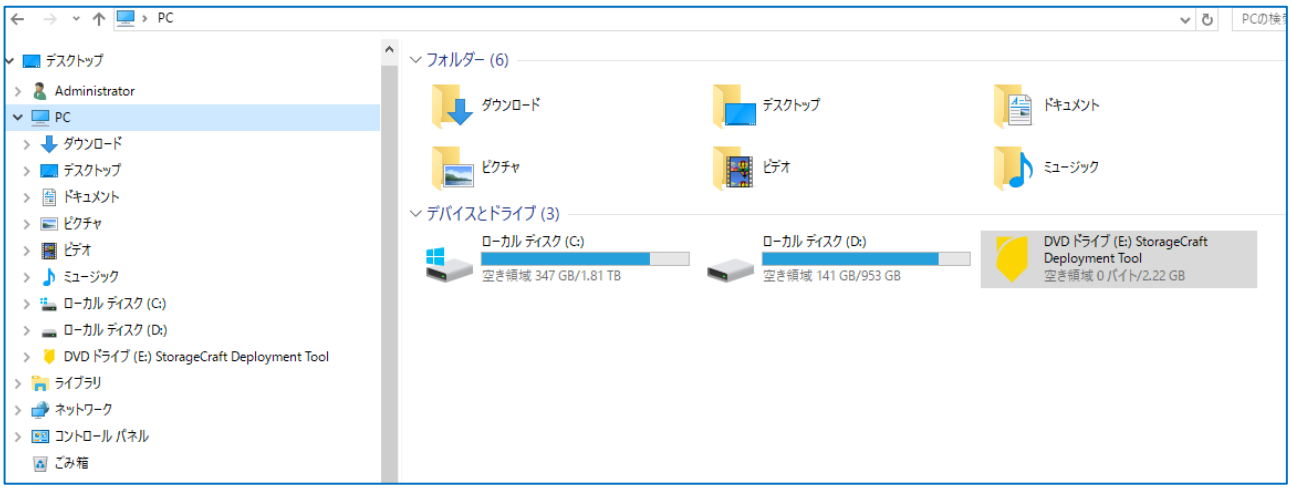
**Step 1.** Arcserve サポート ポータル内の以下のページから プライベート OneSystem 仮想アプライアンスの展開用ファイルをダウンロードします。ファイルは ISO 形式で、サイズは約 2.3 GB です。

**Arcserve OneSystem 4.8 ダウンロード リンク**

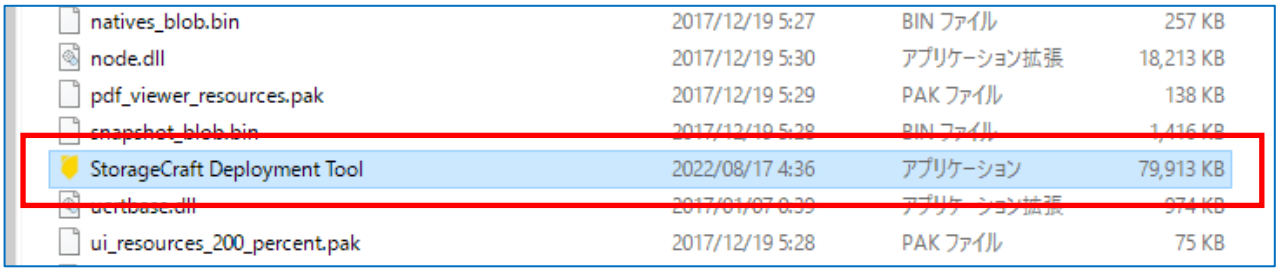
https://support.arcserve.com/s/article/OneSystem-Download-Link?language=ja

・展開ツール ISO： “StorageCraftDeploymentTool-4.8.XXX.iso”　* “XXX”は数字

**Step 2.** ダウンロードした ISO を Windows 上のドライブとしてマウントします。

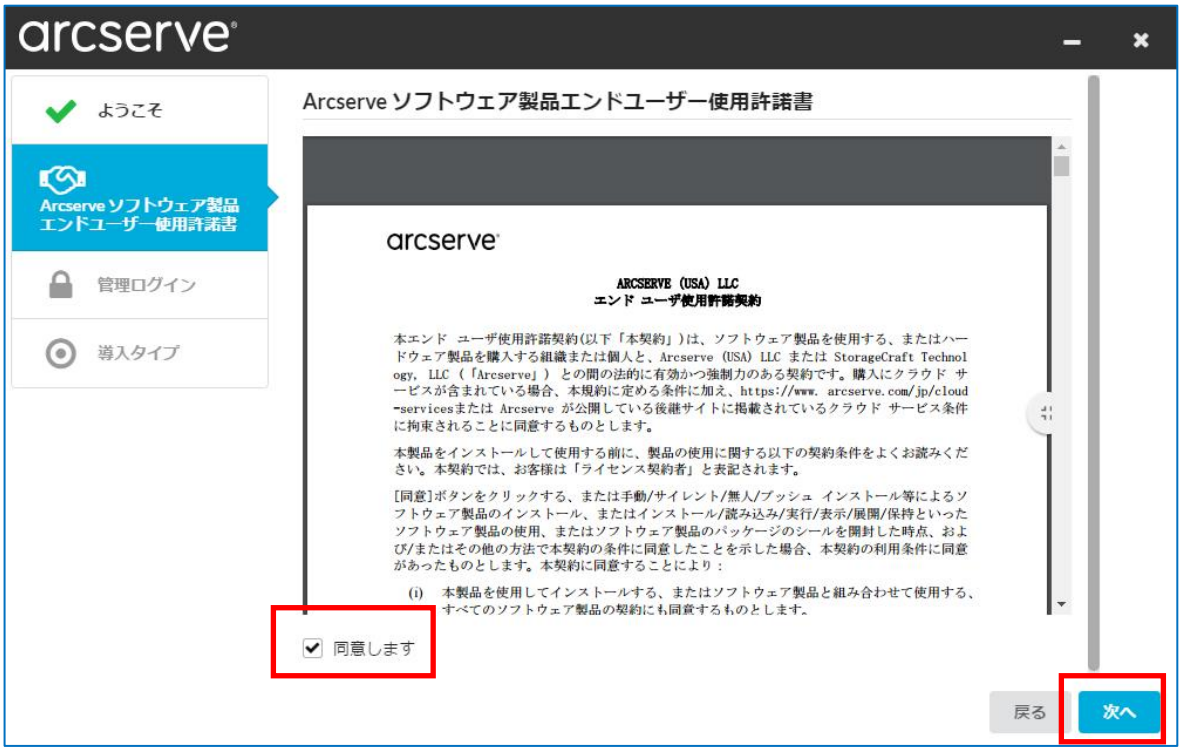



**Step 3.** マウントしたドライブを展開して直下にある“StorageCraft Deployment Tools .exe “をクリックして実行します。



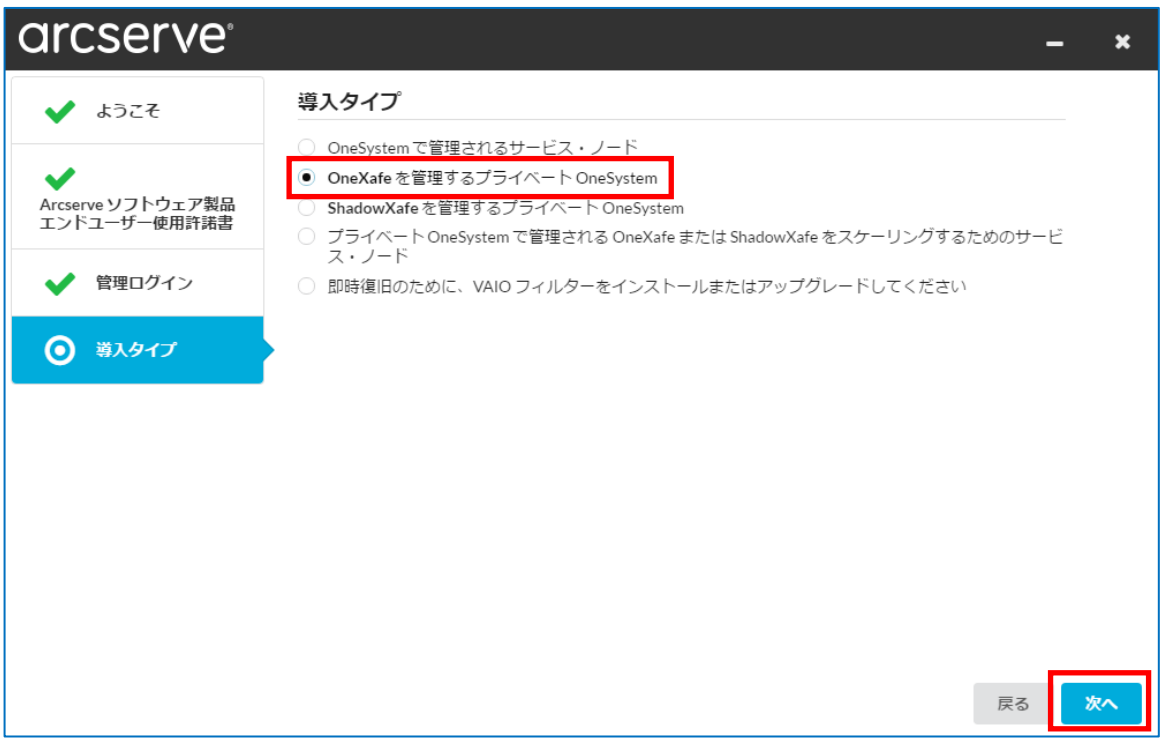
**Step 4.** Arcserve 導入ツール の [ようこそ] 画面で [次へ] をクリックします。


**Step 5.** [Arcserve ソフトウェア製品エンドユーザー使用許諾書]で使用許諾契約に同意いただけましたら、[同意します] にチェックを入れて [次へ] をクリックします。

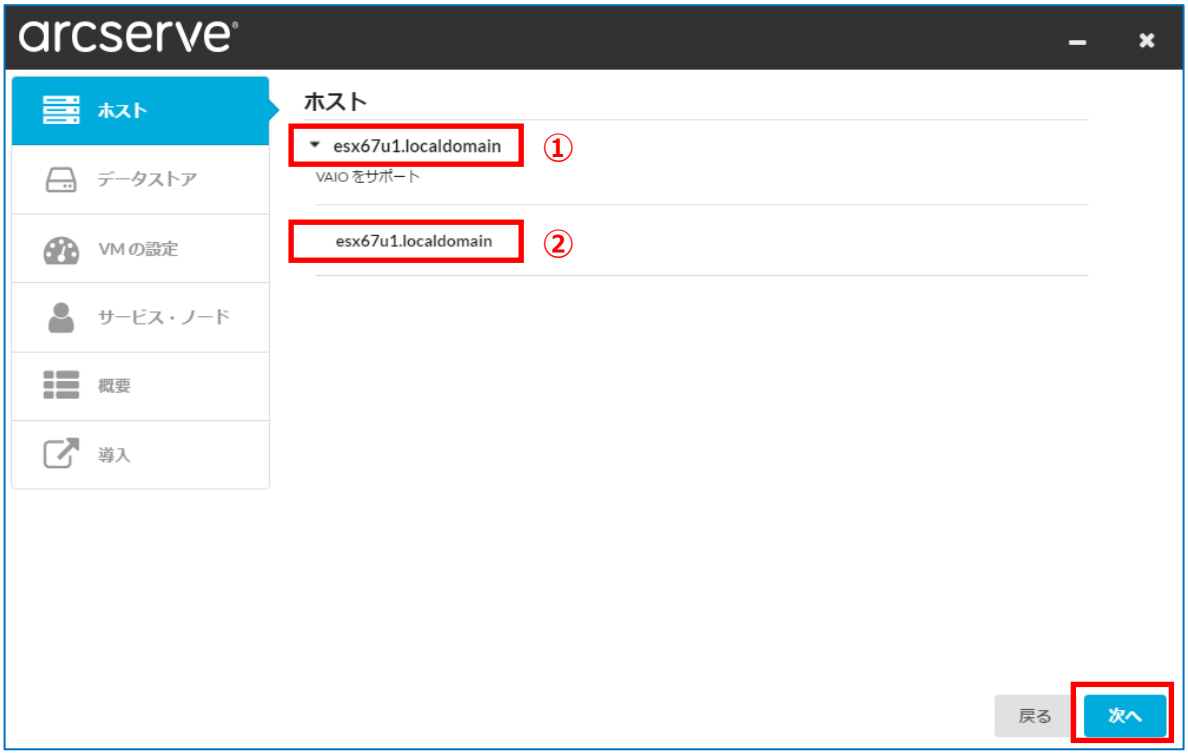


**Step 6.** [管理ログイン] の [管理ソリューション] には ”vCenter または ESXi ホストのアドレス” を選択し、[接続情報] に仮想アプライアンスを実行させる ”ESX ホスト名” か ”IP アドレス” と ”ポート番号”（デフォルトは “443”）を入力します。[ログイン資格情報] をそれぞれ入力後、[次へ] をクリックします。


**Step 7.** [導入タイプ] では、“**OneXafe** を管理するプライベート OneSystem” を選択し、[次へ] をクリックします。

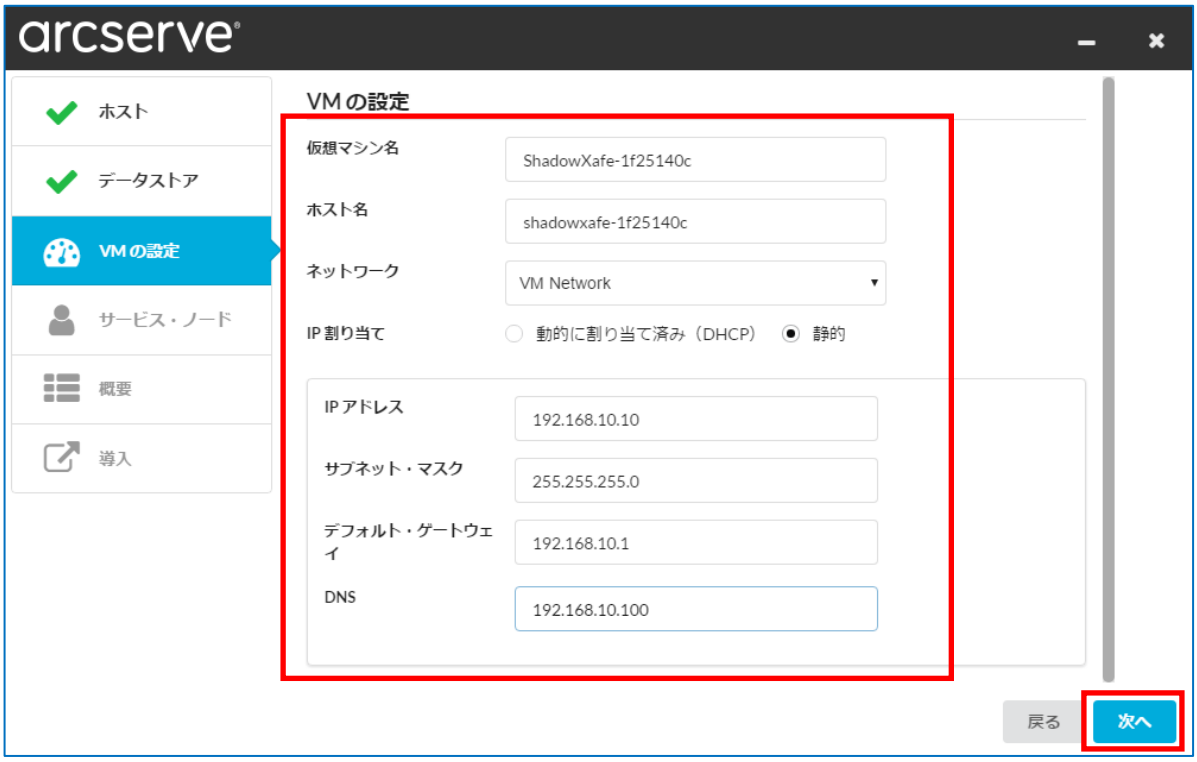


**Step 8.** [ホスト] で表示された ESXi ホスト名をクリック“①”し、下側に表示された ESXi ホストを選択”②”して、[次へ]をクリックします。




**Step 9.** [データストア] で [データストア・プロビジョニング] を指定し、表示されているデータストア名をクリックして [次へ] をクリックします。

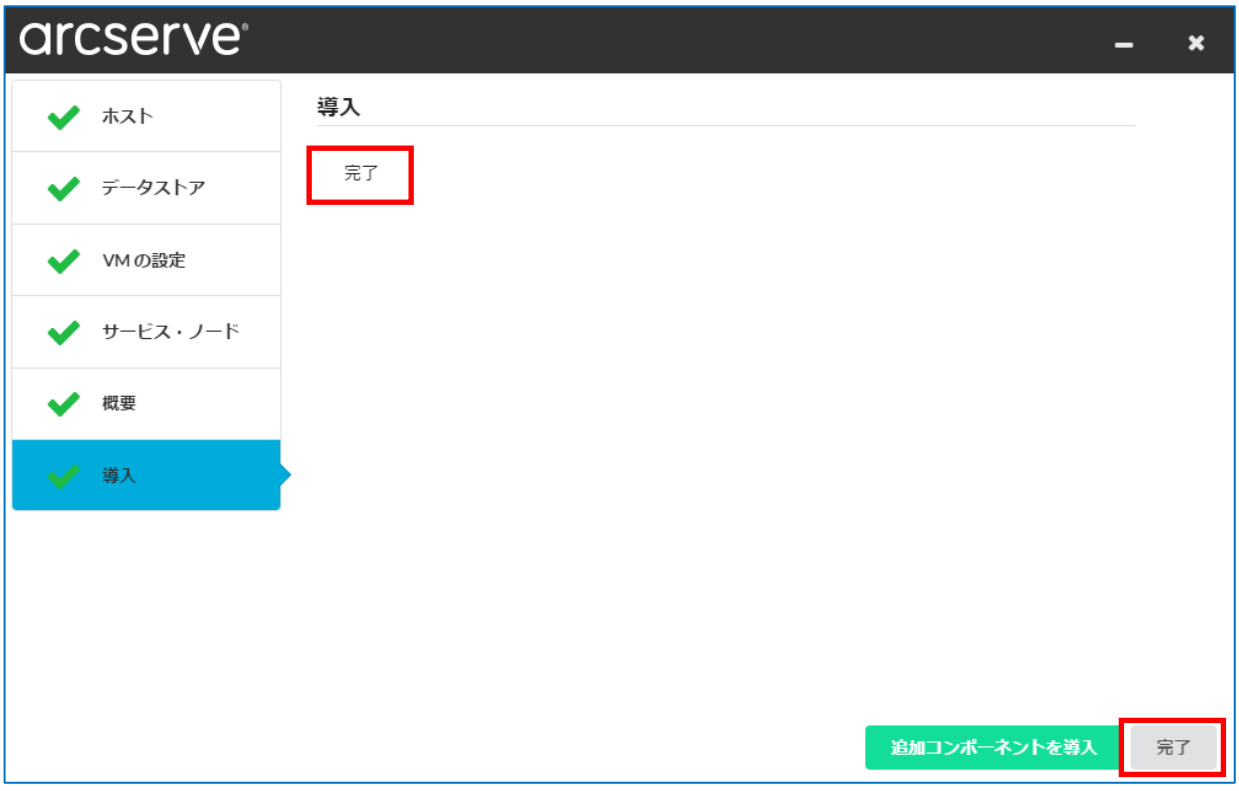
**Step 10.** [VM の設定] で [仮想マシン名] と [ホスト名]を任意の名前に変更し、[ネットワーク] で仮想マシンが使用する VMware ネットワークを選択します。[IP 割り当て] は “動的に割り当て済み (DHCP)”（デフォルト）か、“静的” を選択して [IP アドレス] などを指定します。[次へ] をクリックします。




**Step 11.** [サービス・ノード] で管理者の [ユーザー名] と [パスワード] を入力し、[次へ] をクリックします。

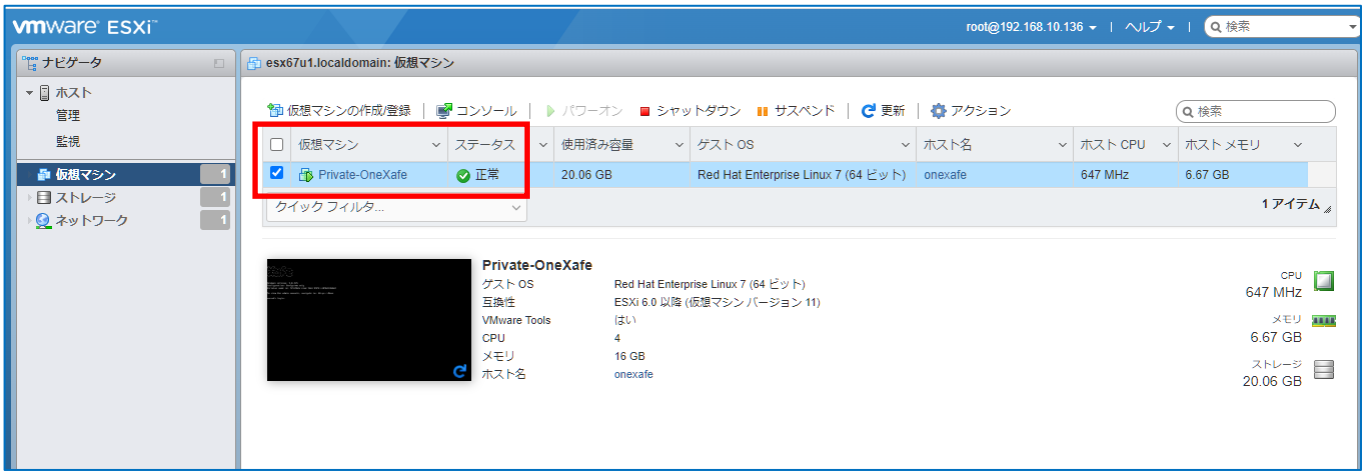
**Step 12.** [概要] で設定した内容を確認し、問題無ければ [導入] をクリックします。
設定した内容に間違いがあれば、[戻る] をクリックして各設定画面から修正を行ってください。


**Step 13.** [導入] で ”完了” の表示を確認したら、画面右下の [完了] をクリックし、仮想アプライアンスの展開を終了します。



仮想アプライアンスの展開後、VMware の管理コンソールにプライベート OneSystem の仮想マシンが登録されて、自動的に起動していることを確認してください。

もし、仮想マシンが起動していない場合は [パワーオン] を実行します。



### 3.7. Hyper-V 環境へのプライベート OneSystem 仮想アプライアンスの展開

プライベート OneSystem の仮想アプライアンスを Hyper-V 環境で実行する場合は、
以下の手順に従ってプライベート OneSystem の仮想アプライアンスを展開します。

**Step 1.** Arcserve サポート ポータル内の以下のページからプライベート OneSystem 仮想アプライアンスの展開用ファイルをダウンロードします。ファイルは MSI 形式で、サイズは約 19 MB です。

**Arcserve OneSystem 4.8 ダウンロード リンク**

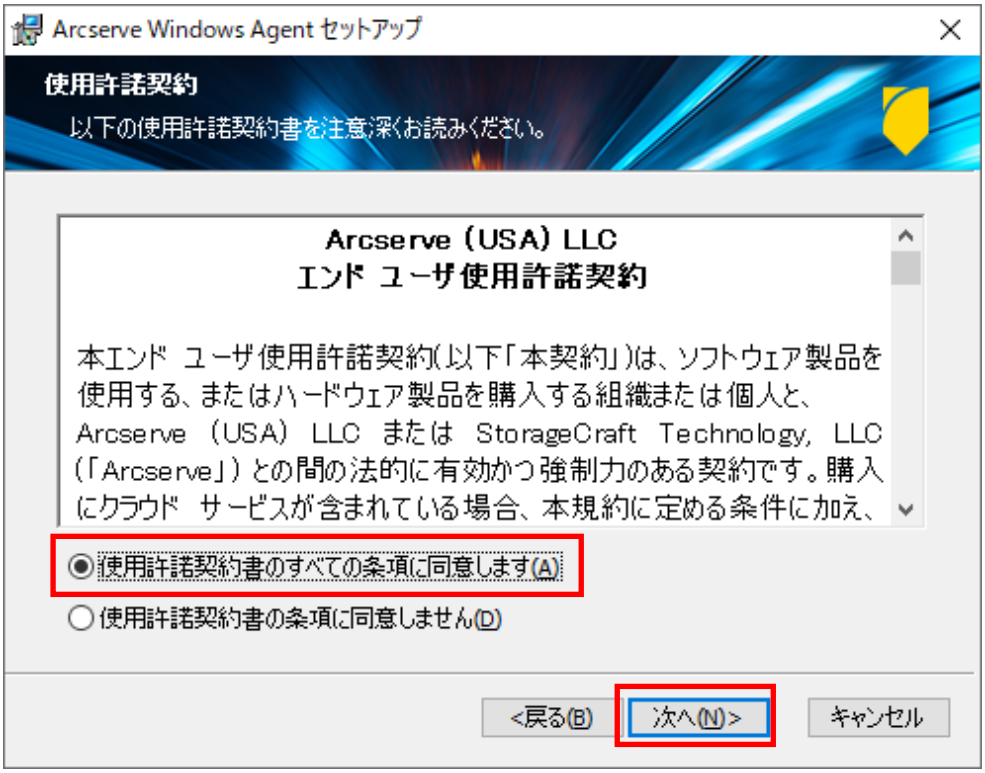
https://support.arcserve.com/s/article/OneSystem-Download-Link?language=ja

・エージェント MSI ： “StorageCraftAgent-4.8.XXX.win64.msi　* “XXX”は数字

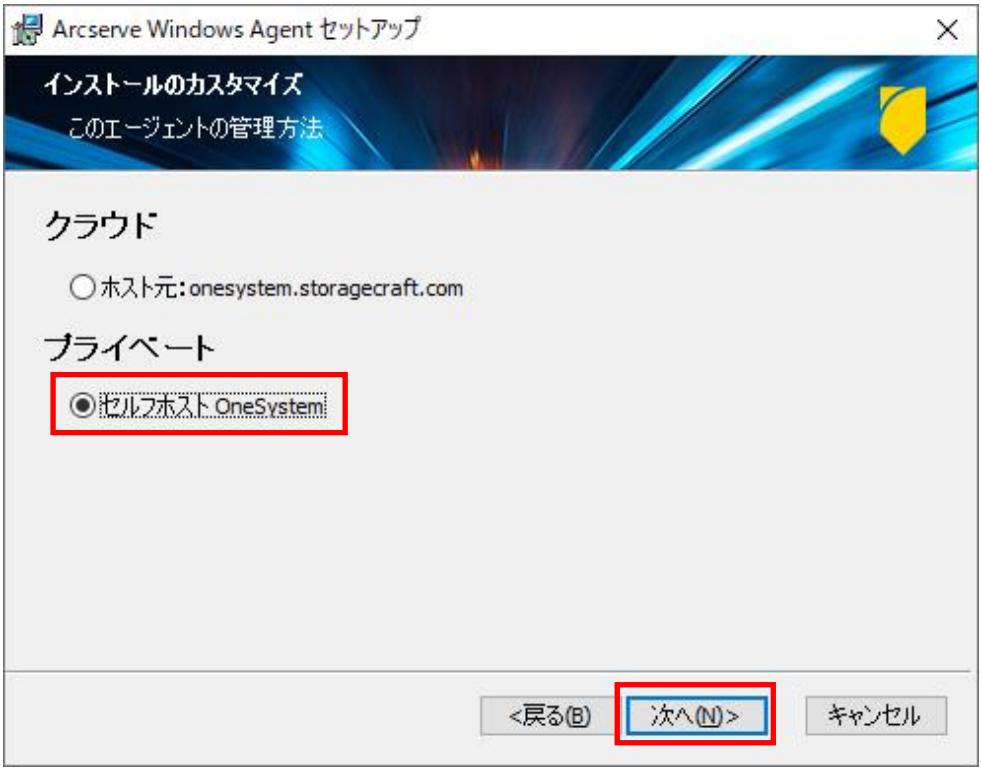
**注意!!：** Hyper-V 用プライベート仮想アプライアンスのデータは、インターネット経由でダウンロードいたします。このため、仮想アプライアンスの展開時は Hyper-V ホストが直接インターネットに接続できる構成が必要です。

**Step 2.** ダウンロードした MSI ファイルを実行すると、[Arcserve Windows Agent セットアップ] のウィザード画面が表示されるので、[次へ] をクリックします。

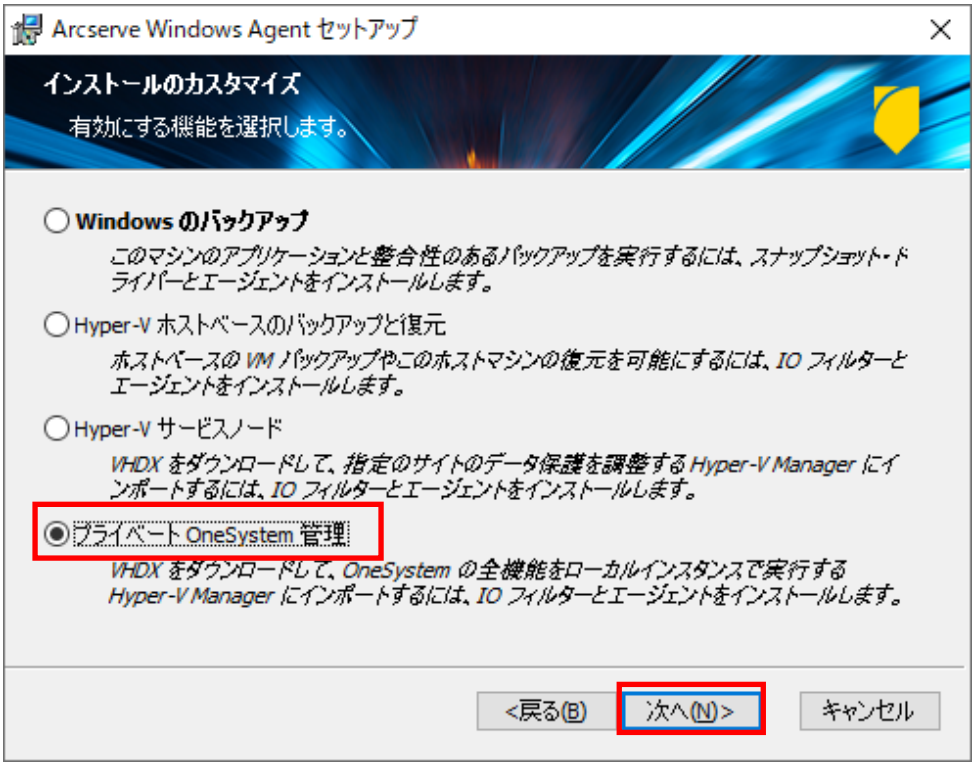
**Step 3**. [使用許諾契約] で使用許諾契約に同意いただけましたら、“使用許諾契約書のすべての条項に同意します” にチェックを入れて [次へ] をクリックします。



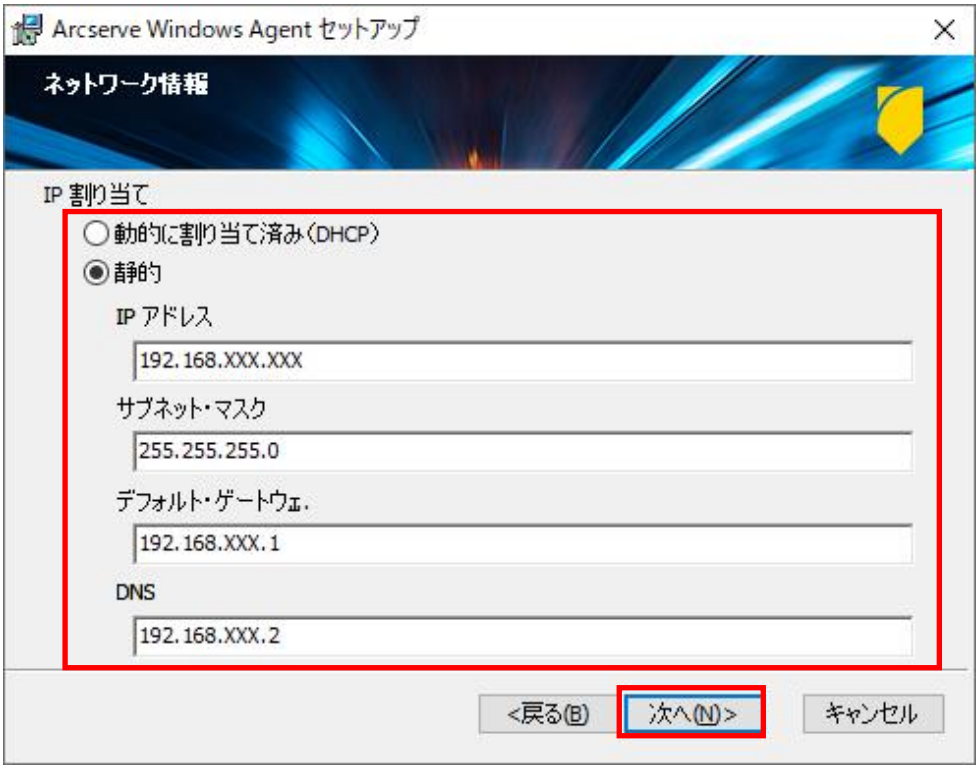

**Step 4.** [インストールのカスタマイズ] で [プライベート] の “セルフホスト OneSystem” を選択し、[次へ] をクリックします。



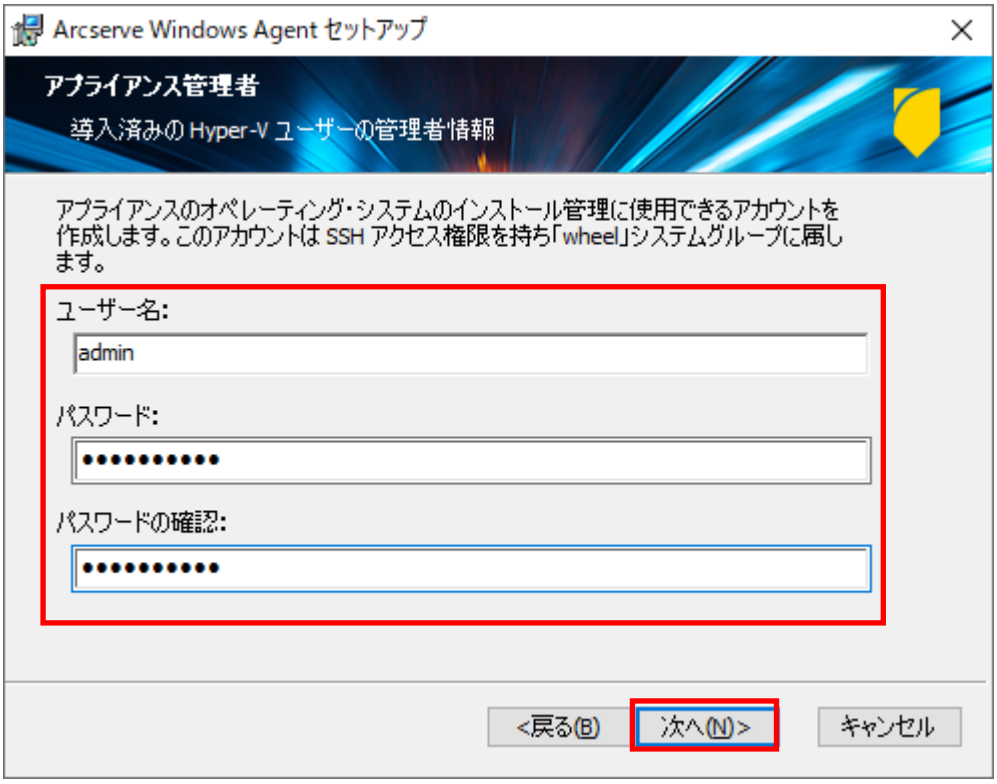
**Step 5.** 次の [インストールのカスタマイズ] では “プライベート OneSystem 管理” を選択し、[次へ] をクリックします。



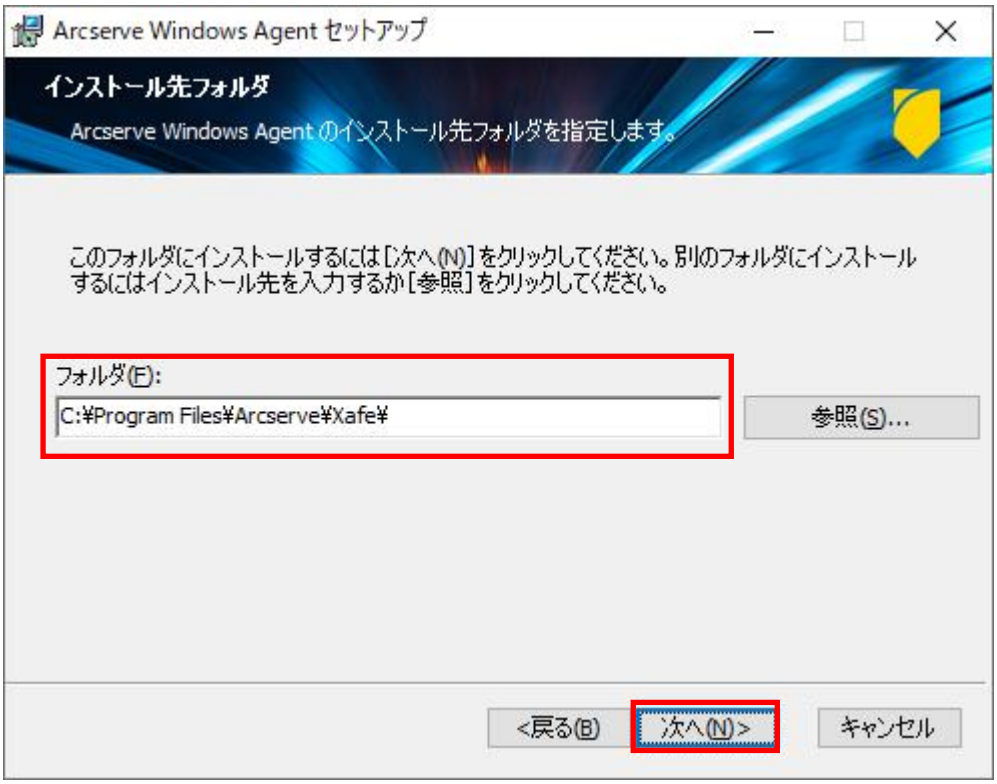

**Step 6.** [ネットワーク情報] の [IP 割り当て] で、“動的に割り当て済み(DHCP)”（デフォルト）か、“静的” を選択して [IP アドレス] などを指定して [次へ] をクリックします。



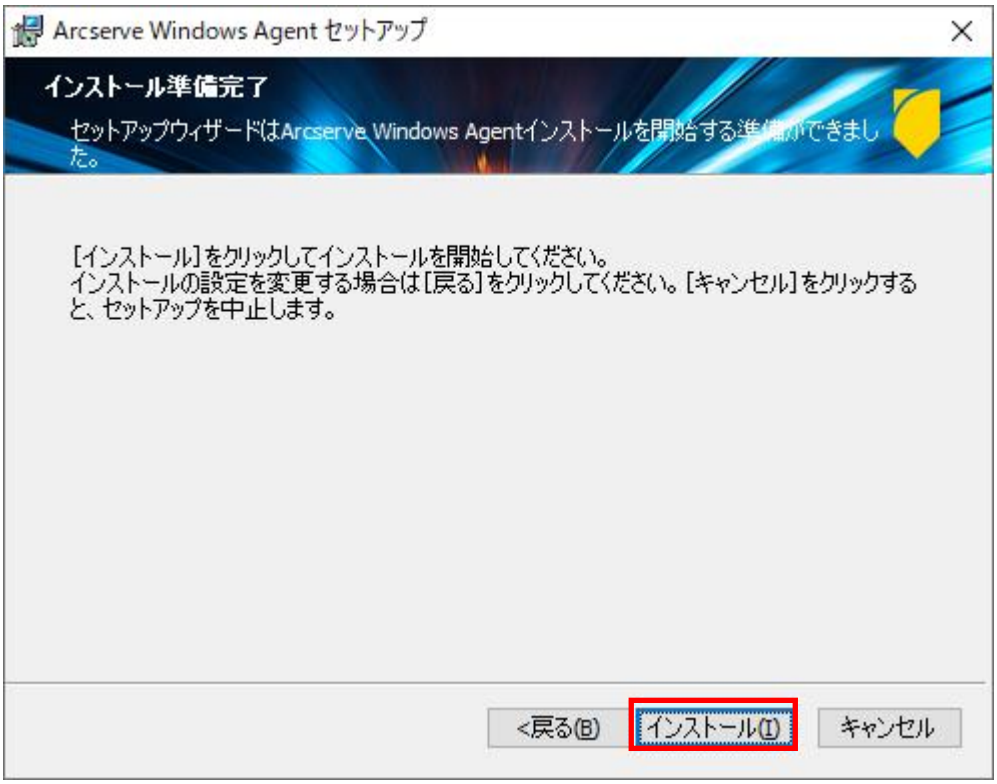
**Step 7.** [アプライアンス管理者] で管理者の [ユーザー名] と [パスワード] を入力し [次へ] をクリックします。



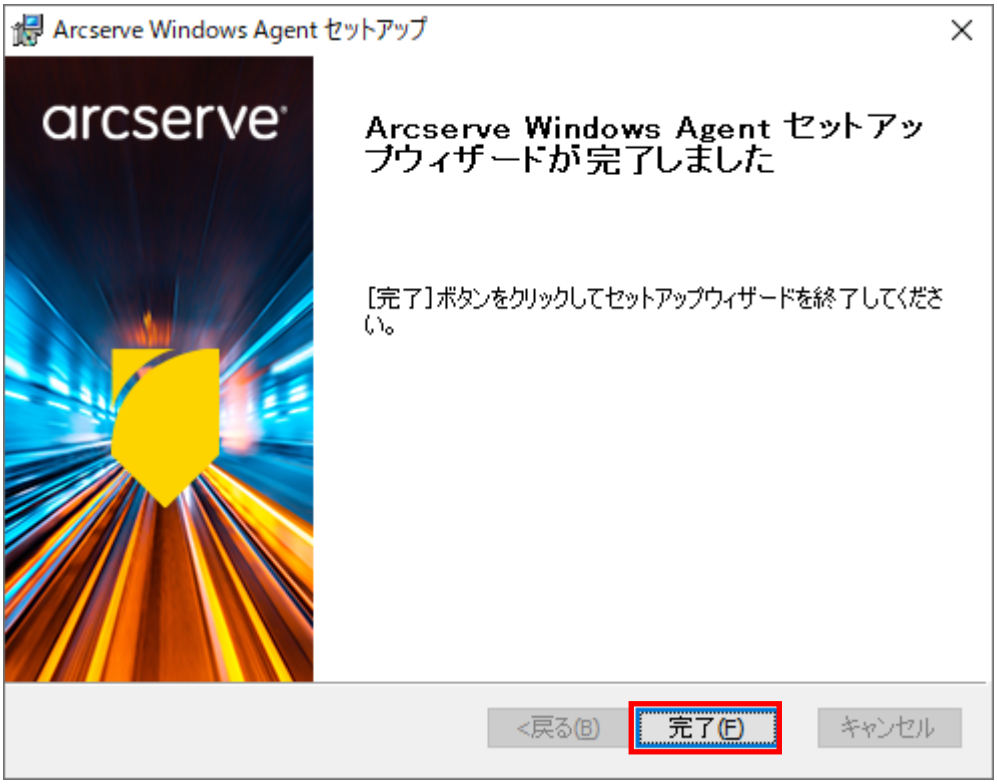

**Step 8.** [インストール先フォルダ] で、プライベート OneSystem で使用する Arcserve Windows Agent のインストール先を指定し、[次へ] をクリックします。



**Step 9.** [インストール準備完了] で、[インストール] をクリックします。



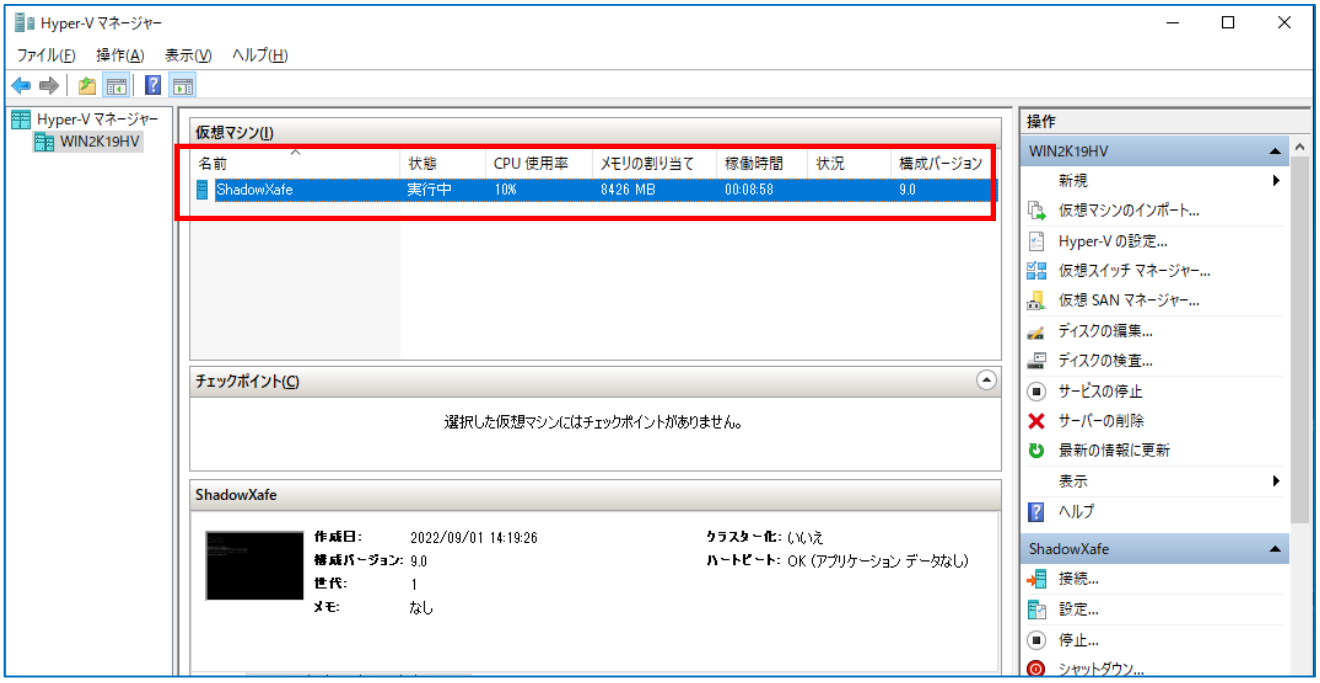

**Step 10.** Arcserve Windows Agent のインストールが終了すると ”セットアップが完了しました” のメッセージが表示されるので、[完了] をクリックします。



Arcserve Windows Agent のインストール終了後、しばらくするとインターネット経由で仮想アプライアンスが Hyper-V ホストに展開されます。

※ インターネット経由でダウンロードされる仮想アプライアンスのデータ量は約 4.5GB です。
仮想アプライアンスの展開にかかる時間はお客様の環境に依存いたします。

Hyper―V マネージャーにプライベート OneSystem の仮想マシンが登録されて、自動的に起動していることを確認してください。
登録後、しばらくしても仮想マシンが起動しない場合は[起動]を実行します。

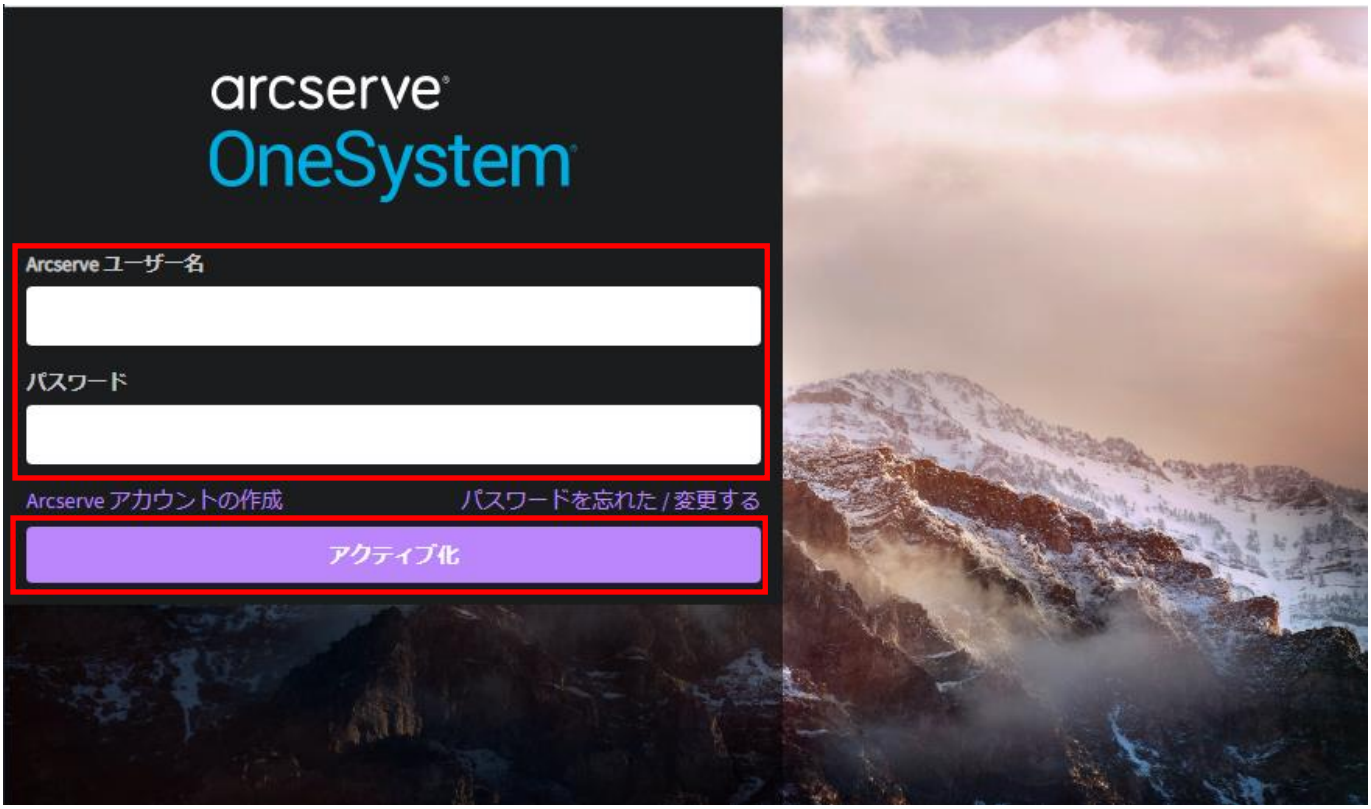


### 3.8. プライベート OneSystem の管理者アカウントの登録

**Step 1.** Web ブラウザにプライベート OneSystem 仮想アプライアンスのホスト名か IP アドレスの URL を入力し、プライベート OneSystem にアクセスします。

https://<プライベート OneSystem ホスト名> or <IP アドレス>

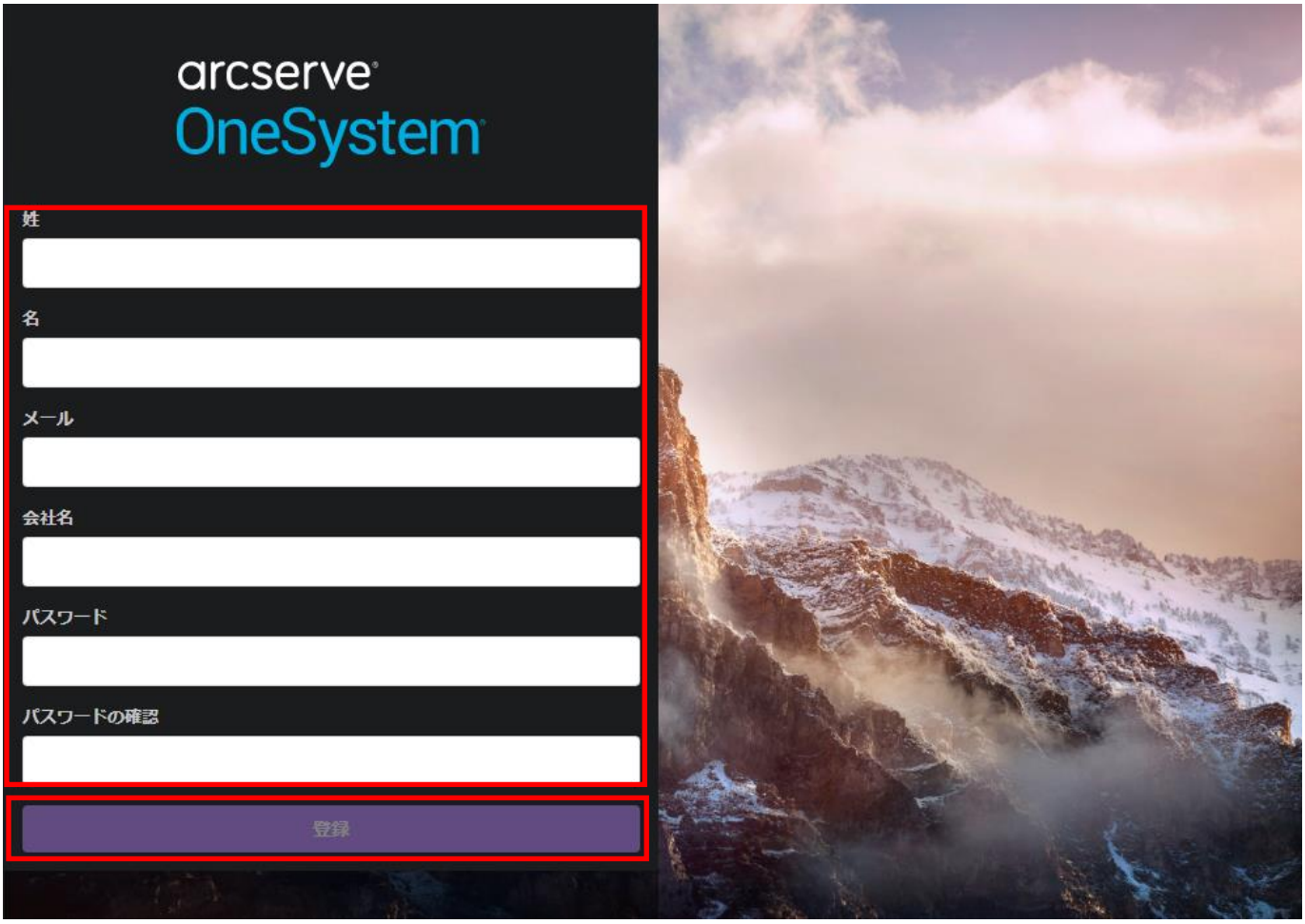
**Step 2.** [Arcserve ユーザー名] と [パスワード] に ”Arcserve サポート ポータルのアカウント” とパスワードをそれぞれ入力し、[アクティブ化] をクリックします。



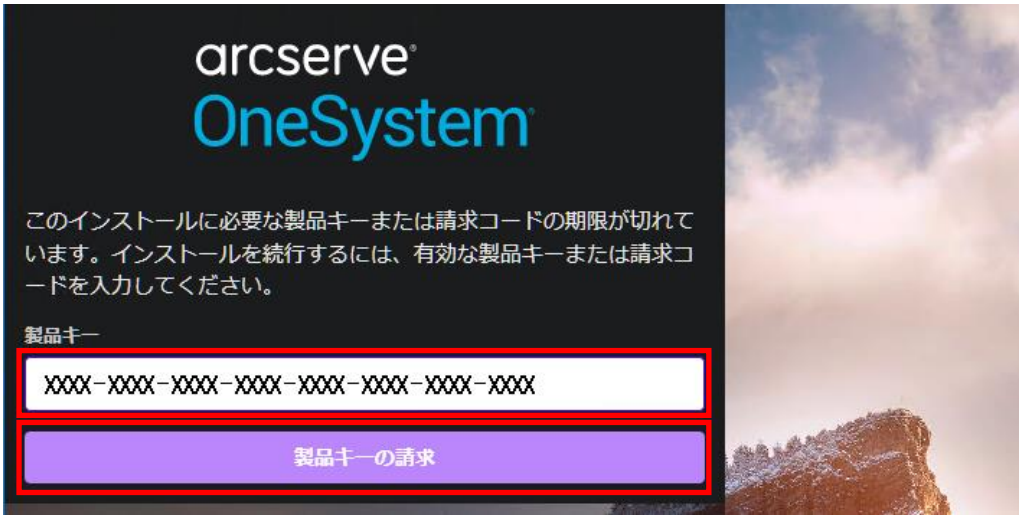

※ ”Arcserve サポート ポータルのアカウント”をお持ちでない場合は、[Arcserve アカウントの作成] をクリックして、アカウントを新規に作成してください。
アカウントの作成手順は以下を参照ください。

**Arcserve サポート ポータル マニュアル**
https://support.arcserve.com/s/article/202937699?language=ja

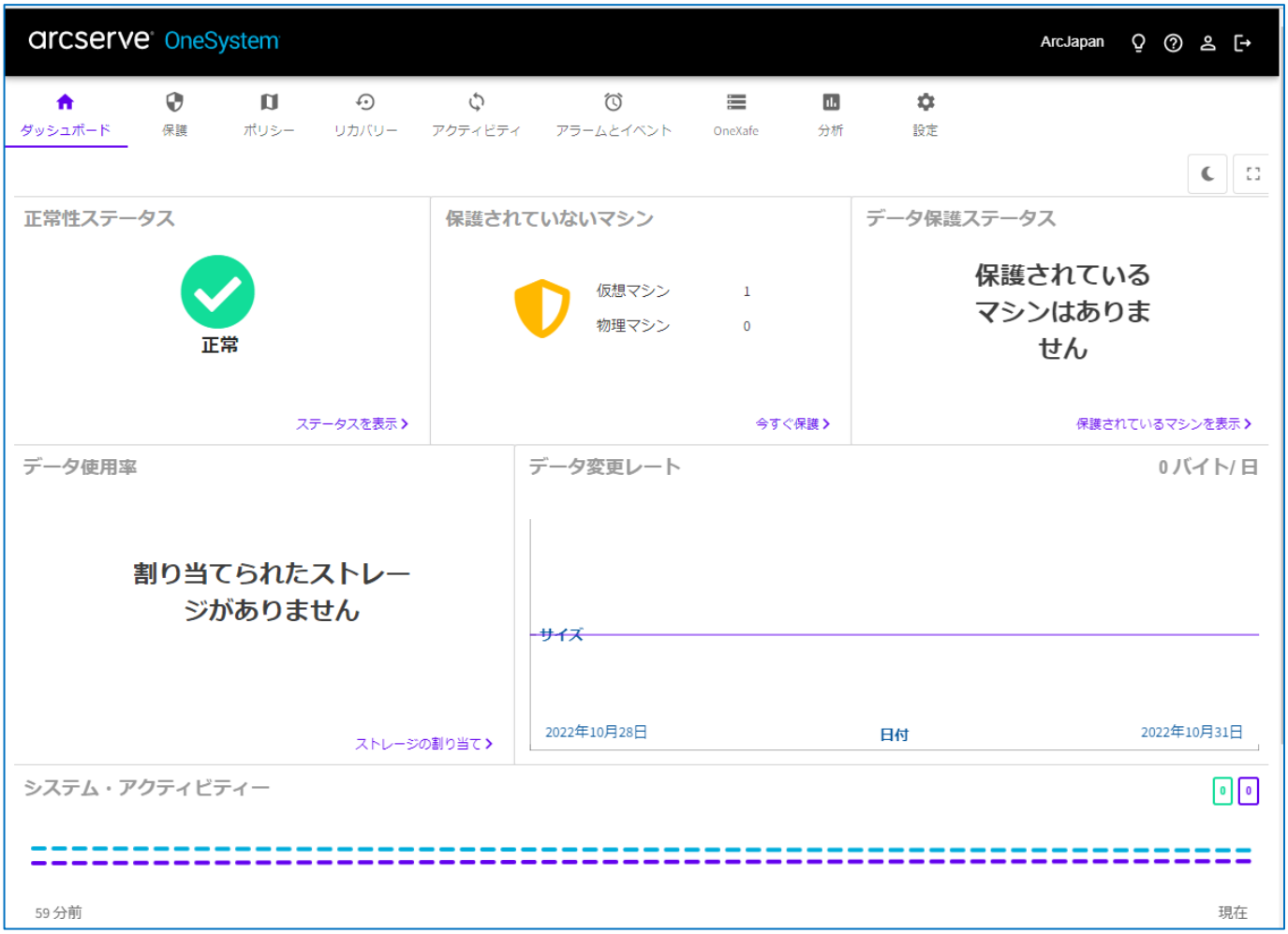
**Step 3.** [姓]、「名」、[会社名] をそれぞれ入力します。
[メール] と [パスワード] は、プライベート OneSystem 用管理者アカウントのメールアドレスと任意のパスワードを入力します。すべての項目を入力後、[登録] をクリックします。




**Step 4.** 製品キー（OneXafe 購入時に Arcserve が発行するライセンス プログラム証書に記載されています。）を入力し、[製品キーの請求] をクリックします。



プライベート OneSystem のコンソール画面が表示されると管理者アカウントの登録は終了です。

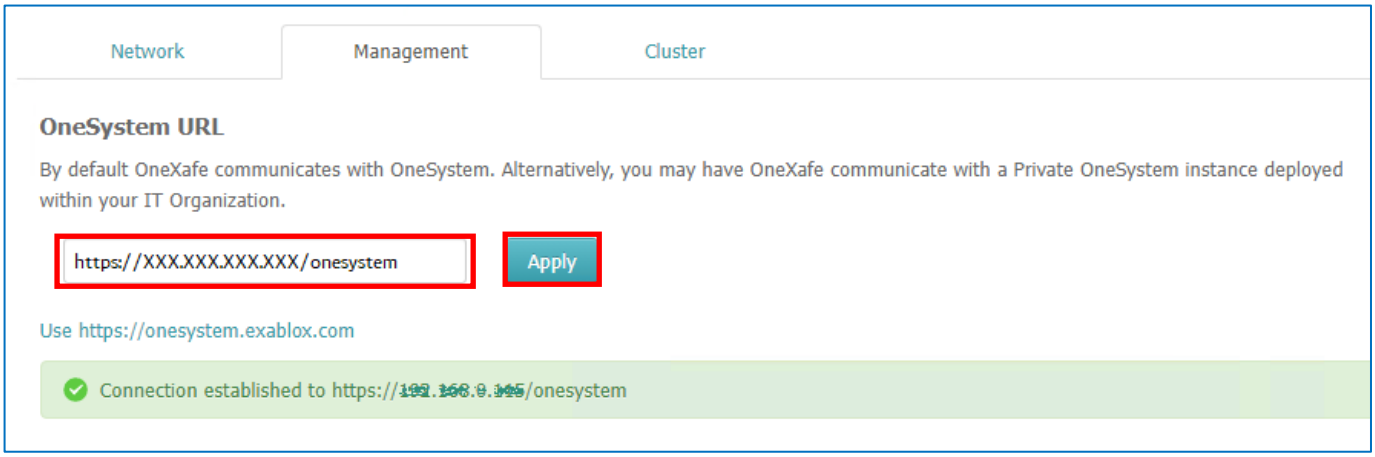


## 3.9. プライベート OneSystem への OneXafe の登録

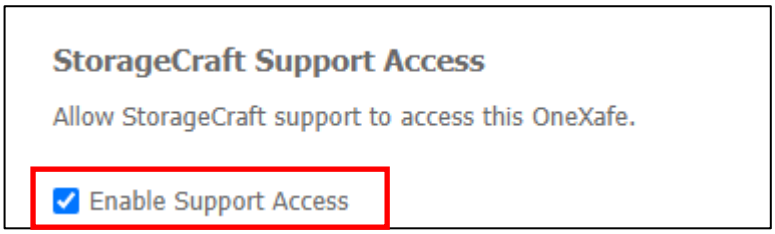
本節では、OneXafe を プライベート OneSystem から管理できるように登録します。

**Step 1.** OneXafe Web コンソールにて、[CONFIGURATION] をクリックして設定ページに移動します。[Management] タブを選択します。[OneSystem URL] 以下にプライベート OneSystem の URL を入力したら、[Apply] ボタンをクリックします。（デフォルトではパブリック OneSystem の URL が設定済）

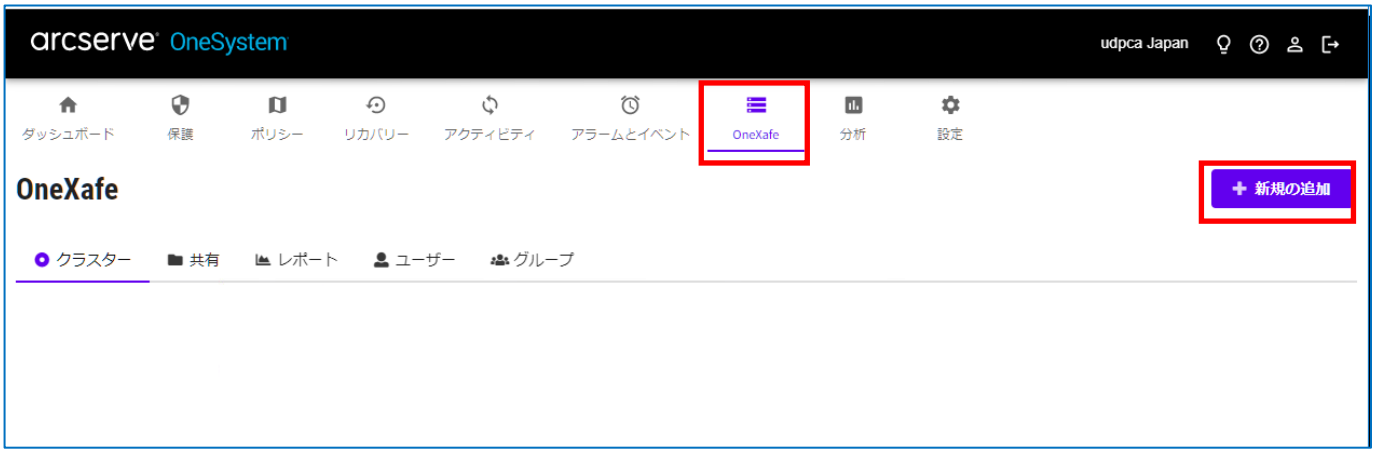
プライベート OneSystem の URL:
**https://<仮想アプライアンスのホスト名>もしくは<IP アドレス>/onesystem**




**Step 2.** OneXafe からインターネットに接続可能な環境の場合、[StorageCraft Support Access]（Arcserve によるリモートアクセス） を利用可能にするチェックボックスを有効にすることを強くお勧めしています。

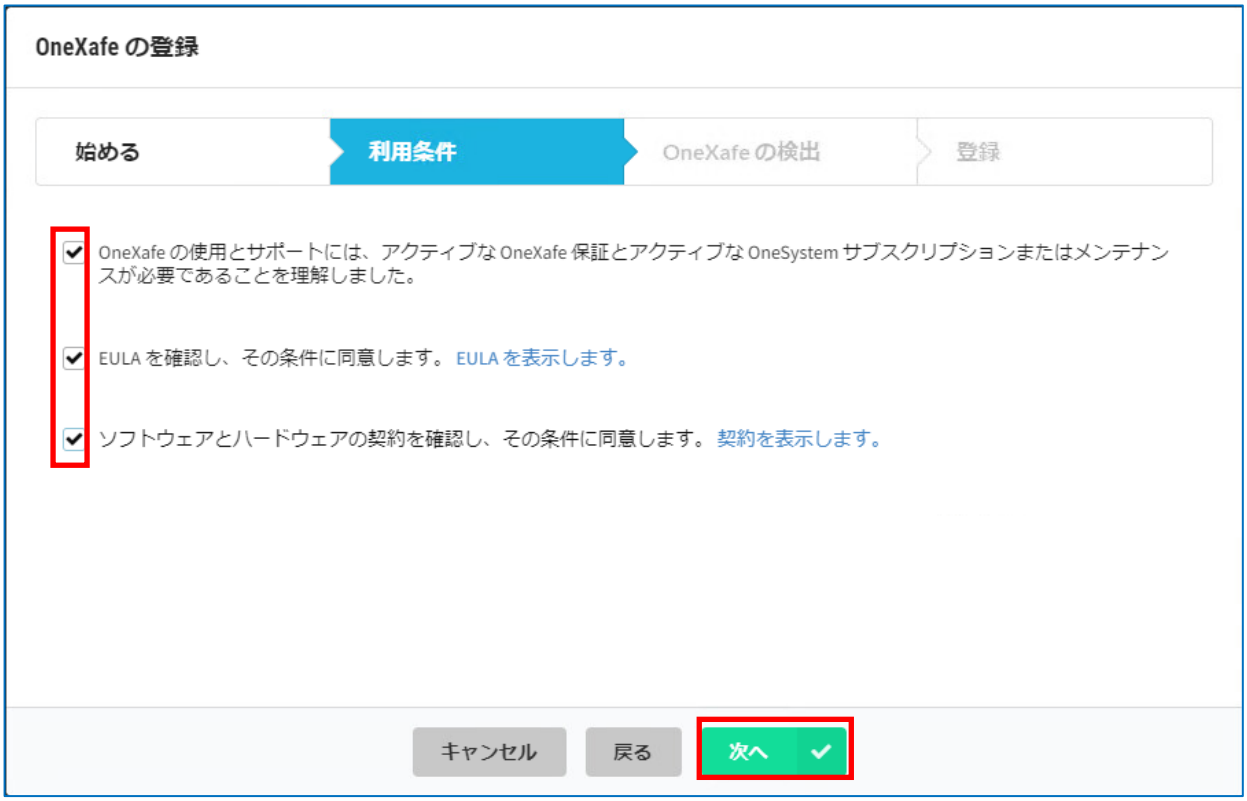


**Step 3.** プライベート OneSystem の画面に戻り、[OneXafe] を選択し、[新規の追加] をクリックします。




**Step 4.** OneXafe の登録ウィザードが始まります。[次へ] をクリックします。

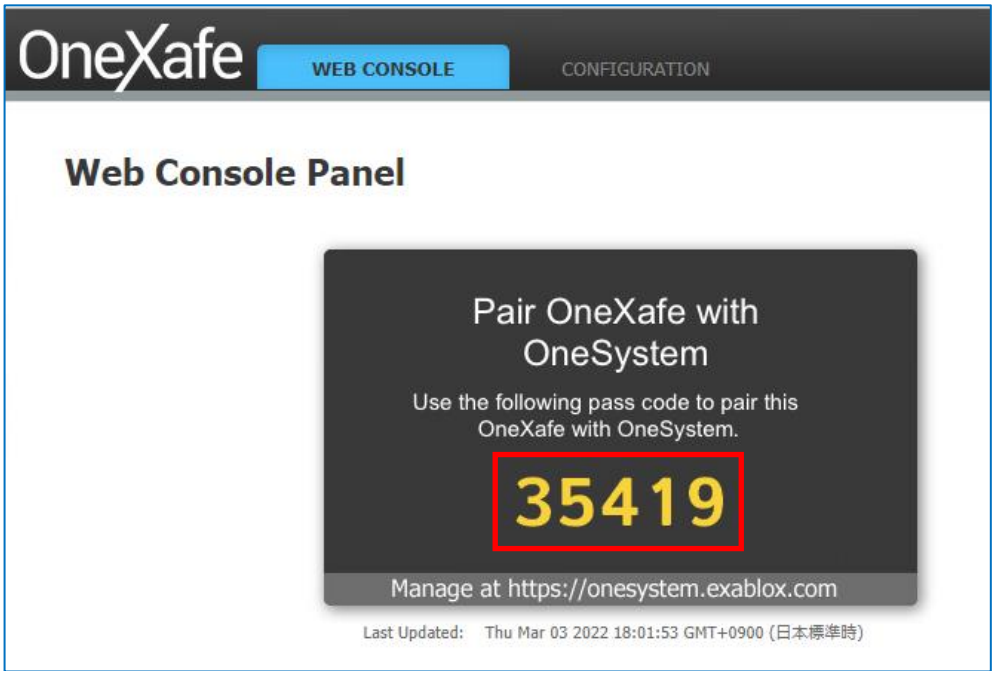
**Step 5.** 約款等を確認し、チェック ボックスにすべてチェックを入れて [次へ] をクリックします。




**Step 6.** [次へ] をクリックし、OneXafe を検出します。

**Step 7.** OneXafe が検出されると自動でクラスターに配置されますので、[選択] をクリックします。

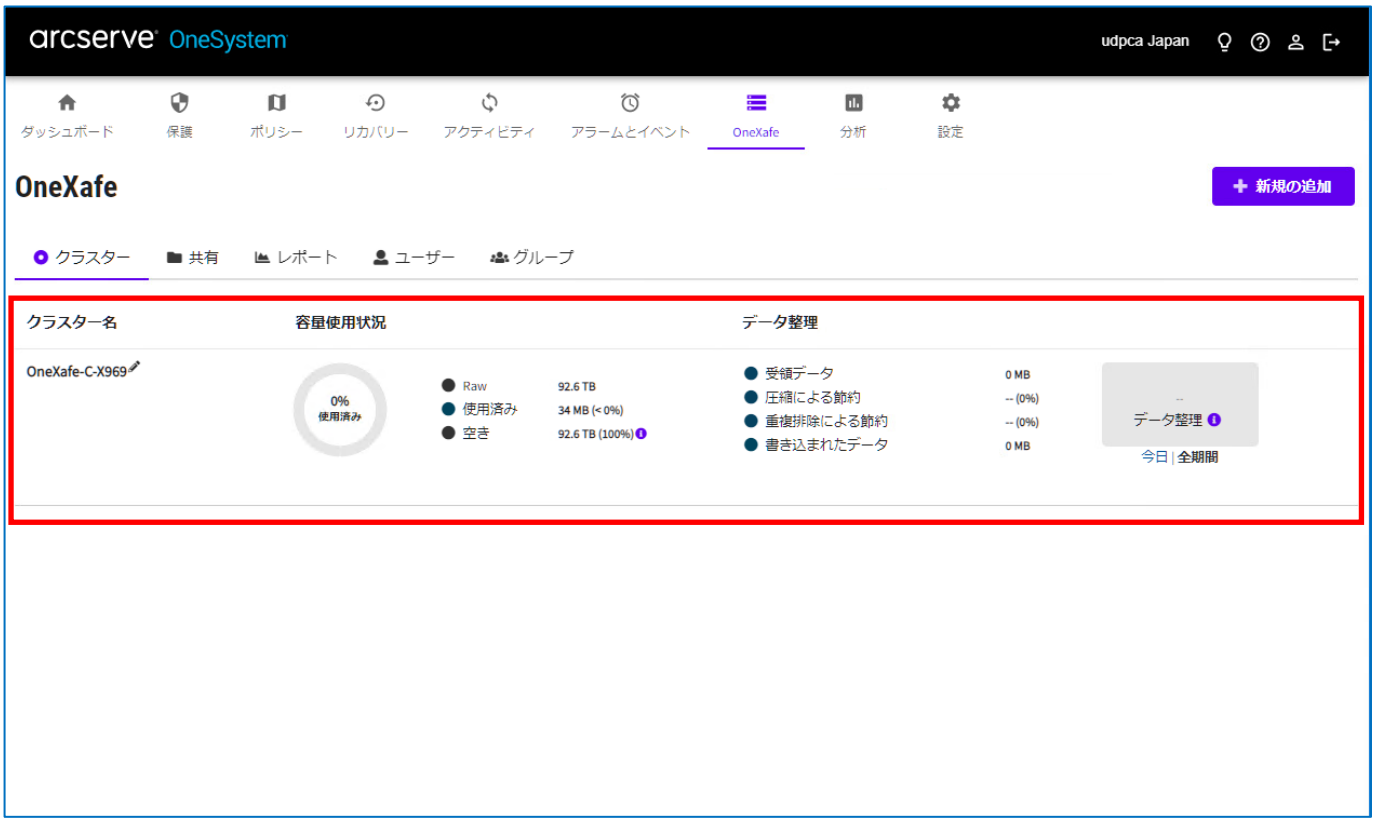

**Step 8.** [選択] をクリックするとパスコードの入力を求められます。ここで画面を OneXafe Web コンソールに切り替えると、以下の画面のように、数字 5 桁のパスコードが表示されています。
（画面のパスコードはサンプルです。実際のパスコードは設定ごとに異なります）



**Step 9.** プライベート OneSystem の画面でパスコードを入力し、[登録] をクリックします。


**Step 10.** 登録が完了すると、以下の画面が表示されますので、[閉じる] をクリックします。

OneXafe の登録ウィザードの画面を閉じると、登録された OneXafe の情報が表示されます。




## 3.10. プライベート OneSystem 管理者アカウントに対する 2 要素認証の有効化

OneSystem の管理者アカウントは共有設定やスナップショット保存期間などを変更できる強力なアカウントです。サイバー攻撃によりデータを破壊されるリスクを減らすため、2 要素認証を有効にすることをお勧めします。設定方法は以下のガイドをご覧ください。

**Arcserve OneXafe Private OneSystem 展開 ガイド - 2 要素認証**

http://documentation.arcserve.com/Arcserve-OneXafe/Available/JPN/OX_POS/default.htm#two_factor_authentication.htm

なお、2 要素認証に Google Authenticator を使う場合は、設定後に必ず Google Authenticator のバックアップを取ってください。アカウントを設定したモバイル端末 の故障/紛失、機種変更、アカウントの誤消去などにより、認証コードの確認ができなくなる場合があります。

# 4. OneXafe での SMB 共有の設定

本章では、OneXafe に SMB 共有を作成する方法を説明します。ここで作成した共有フォルダを、次章で Arcserve UDP のデータストア デスティネーション（バックアップ データの複製先）として利用します。

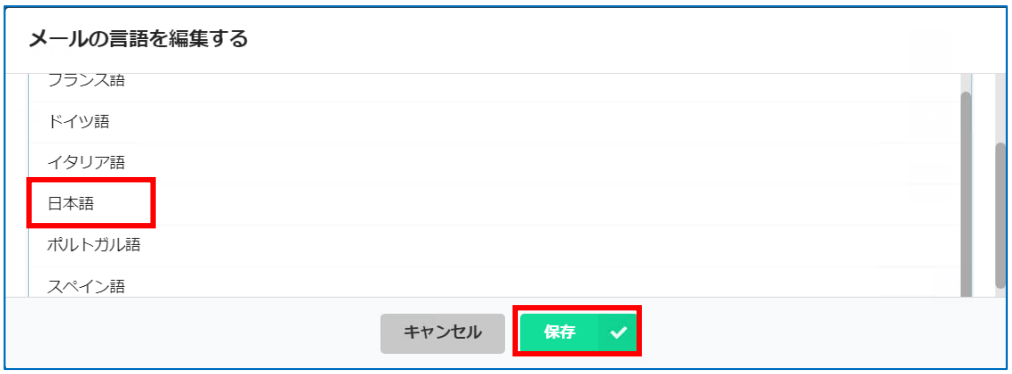
## 4.1. SMTP サーバの設定

次節の OneSystem ユーザ アカウントの登録を行うために、本節で SMTP サーバの設定を行います。

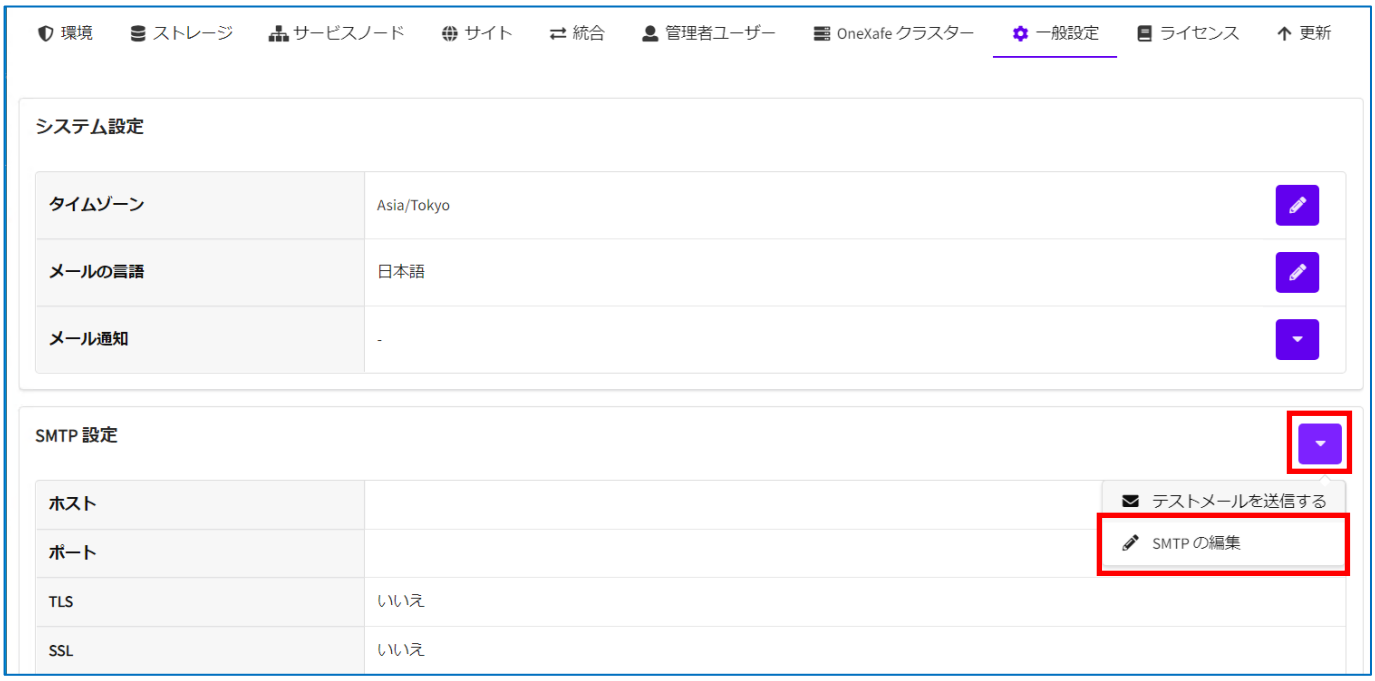
**Step 1.** OneXafe を管理する プライベート OneSystem にログインして [設定] を選択し、[一般設定] を開きます。


**Step 2.** [システム設定] の [メールの言語] の右側にあるボタンをクリックします。

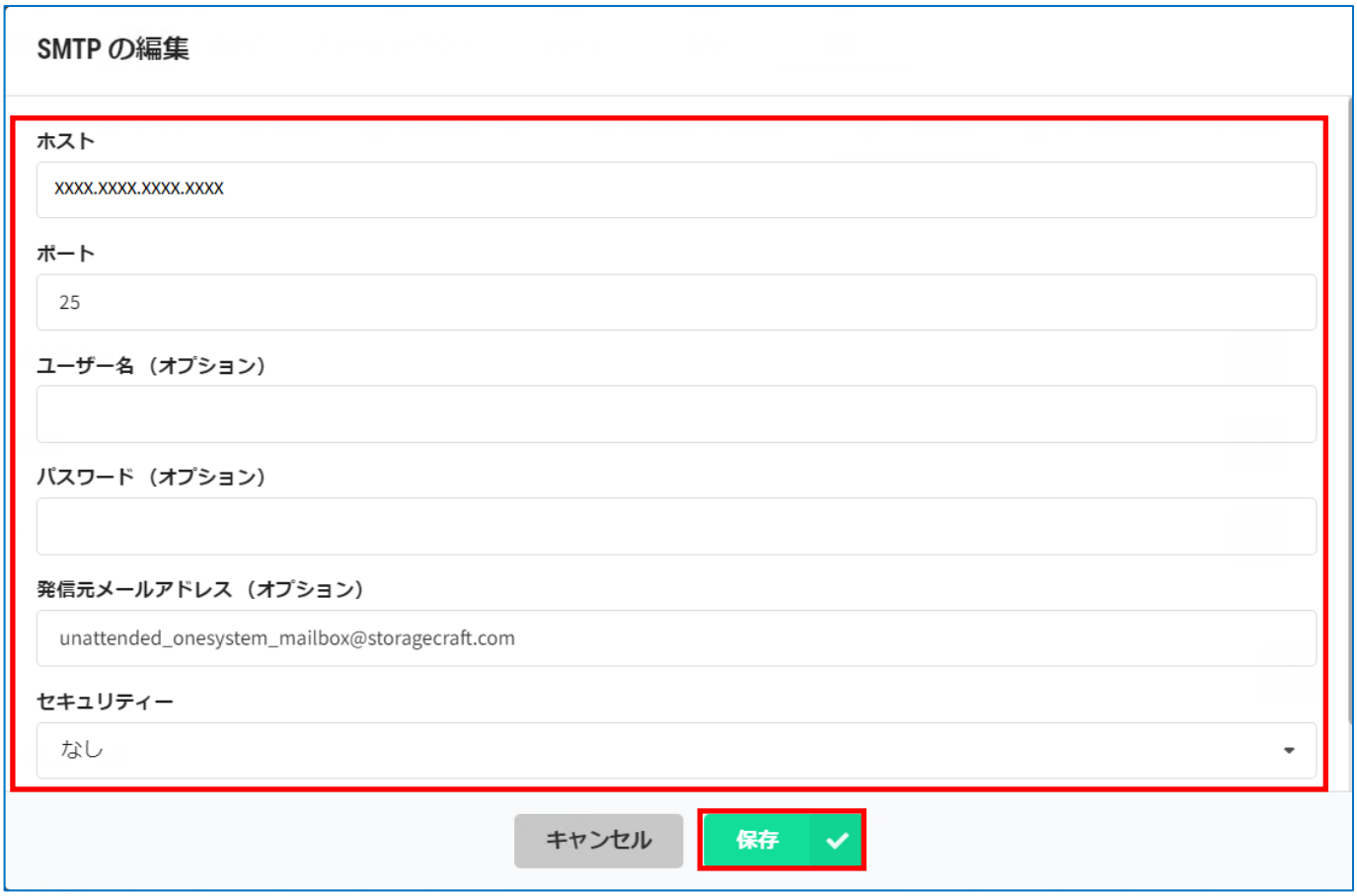

**Step 3.** [メールの言語を編集する] から“日本語”を選択し、[保存] をクリックします。



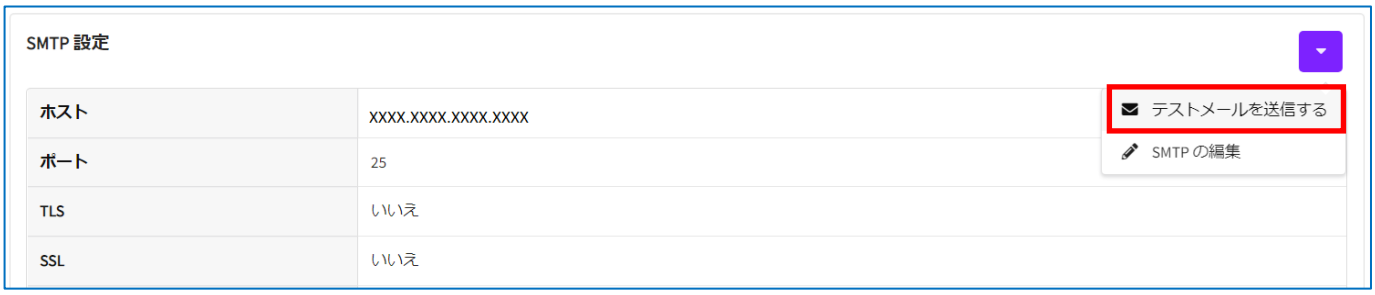
**Step 4.** [SMTP 設定] の右側にあるプルダウンメニューを開き、[SMTP の編集] をクリックします。



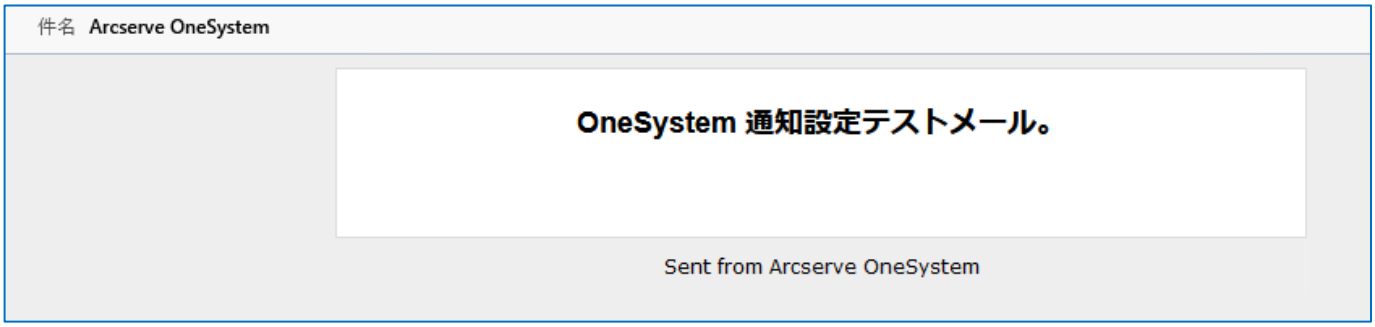

**Step 5.** SMTP サーバの情報を入力し、 [保存] をクリックします。



**Step 6.** [SMTP 設定]のプルダウンメニューから、[テストメールを送信する]をクリックします。




**Step 7.** プライベート OneSystem 用管理者アカウントのメールアドレスに “Arcserve OneSystem” という件名の通知設定テストメールが届くことを確認します。



### 4.2. OneSystem ユーザ アカウントの作成

本節では OneXafe の SMB 共有にアクセスするためのユーザを作成します。

Note: OneSystem を Active Directory（AD） と連携させると、組織内のすべての AD ユーザに共有フォルダへの読み取り/書き込みアクセス権が付与されます。

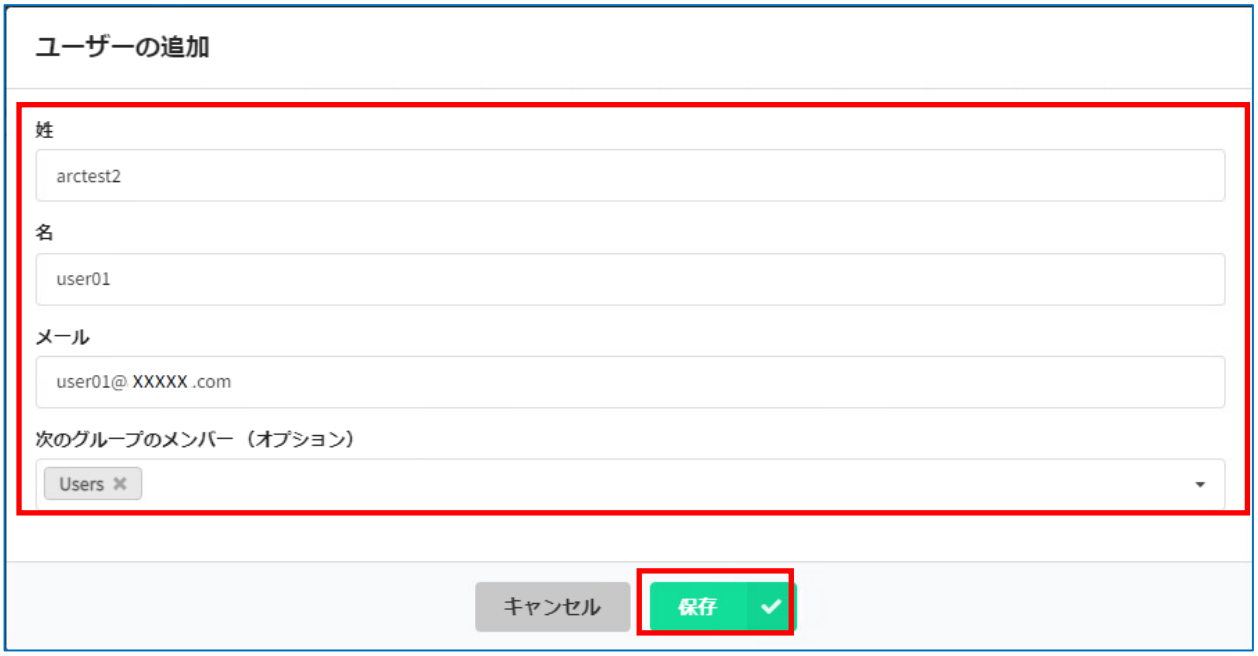
OneXafe を一般のファイルサーバではなくバックアップ データの保存先として利用する場合、OneXafe を Active Directory ドメインに**参加させない**事をお勧めします。これは、Active Directory が危険にさらされた場合に備え、バックアップデータを分離しておくためです。

必要に応じて、管理者、ユーザ、グループを共有に追加する事ができます。これによりリストされたメンバーに明示的なアクセス権が付与されます。

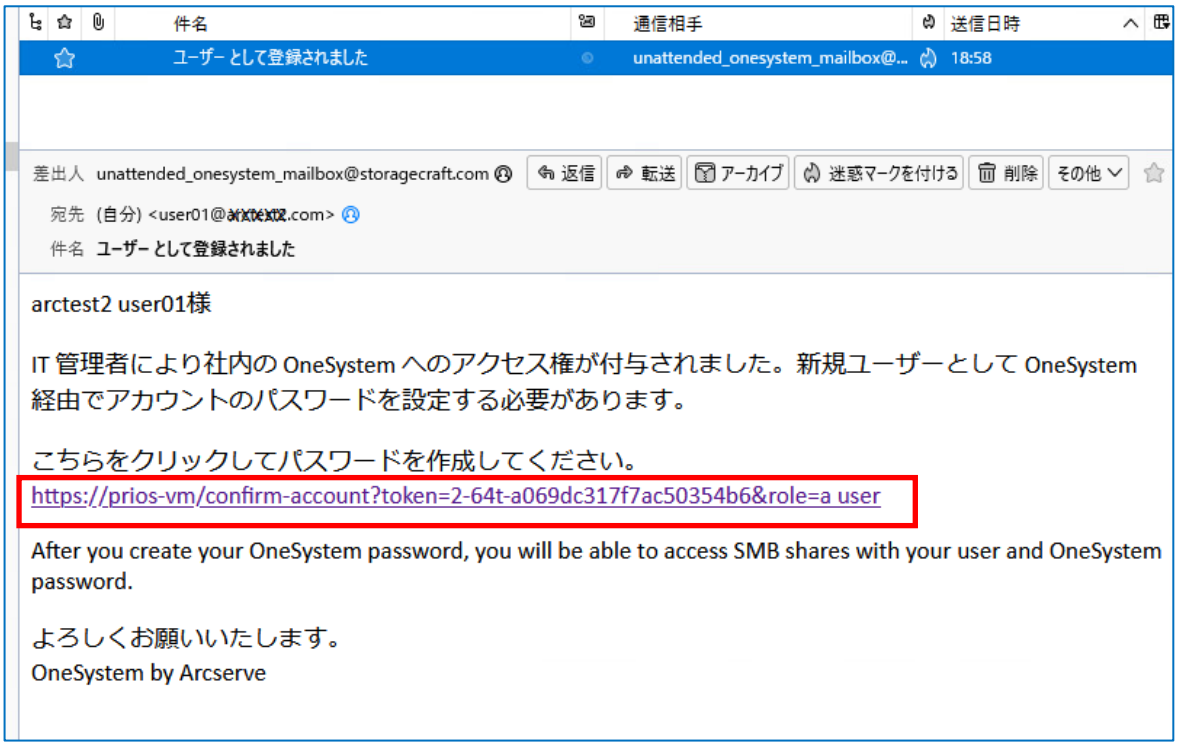
AD ユーザ以外で、新規ユーザを作成する場合は、AD ユーザ以外のメール アカウントを利用してください。

**Step 1.** プライベート OneSystem の [OneXafe] から [ユーザー] を開き、[ユーザーの追加] をクリックします。

**Step 2.** [姓]、[名]、[メール] をそれぞれ入力し、必要に応じてグループメンバーを指定して、[保存] をクリックします。




**Step 3.** Step2 で登録したメールアドレスに “ユーザーとして登録されました” という件名のアクティベーション メールが届きます。メール中のリンクをクリックしてプライベート OneSystem にアクセスします。



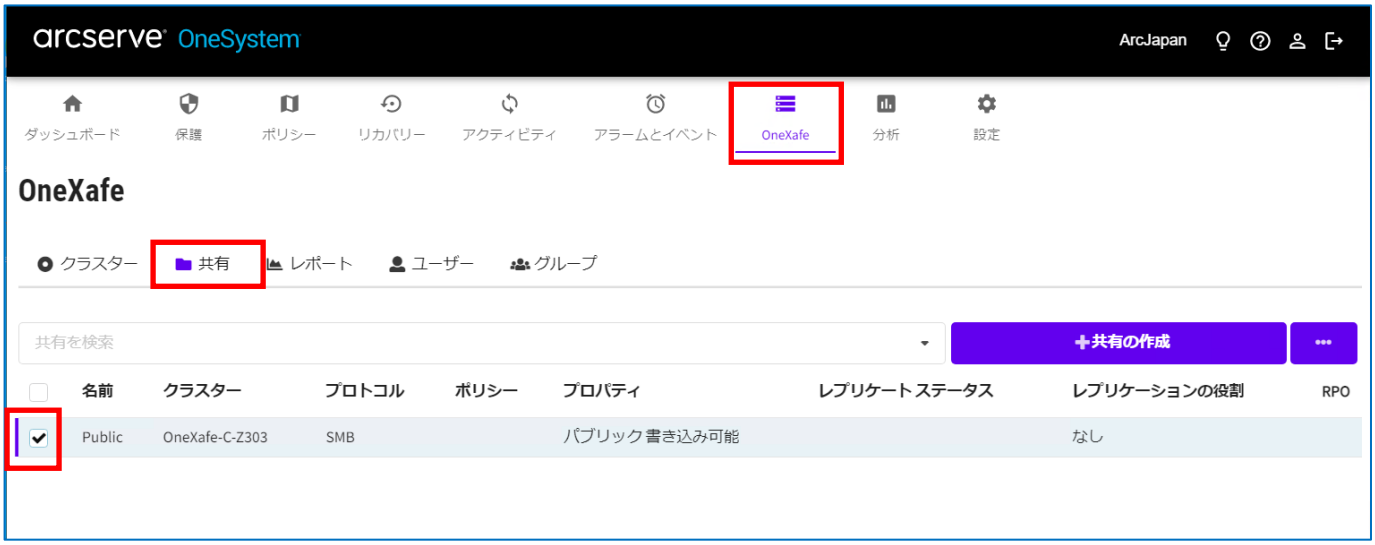
**Step 4.** 画面に表示される条件に従って新しいパスワードを入力し、[パスワードのリセット] をクリックします。


**Step 5.** [パスワードは正常にリセットされました] と表示されましたらブラウザを閉じて作業は終了です。

### 4.3. SMB 共有の作成

次に Arcserve UDP のデータストア デスティネーションとなる SMB 共有を作成します。

**Step 1.** デフォルトで作成されている SMB 共有の ”Public“ は、誰でもアクセス出来る権限で設定されているため、削除しておきます。プライベート OneSystem の [OneXafe] から [共有] を選択し、デフォルトで作成されている SMB 共有の ”Public“ をチェックします。

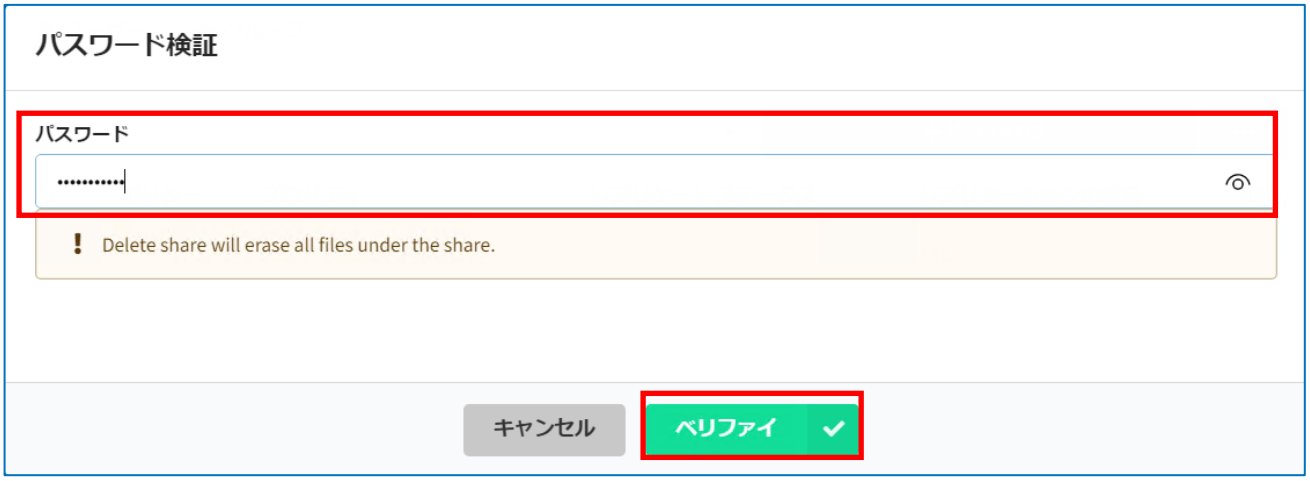



**Step 2.** 右上のボタン メニューから [削除] をクリックします。

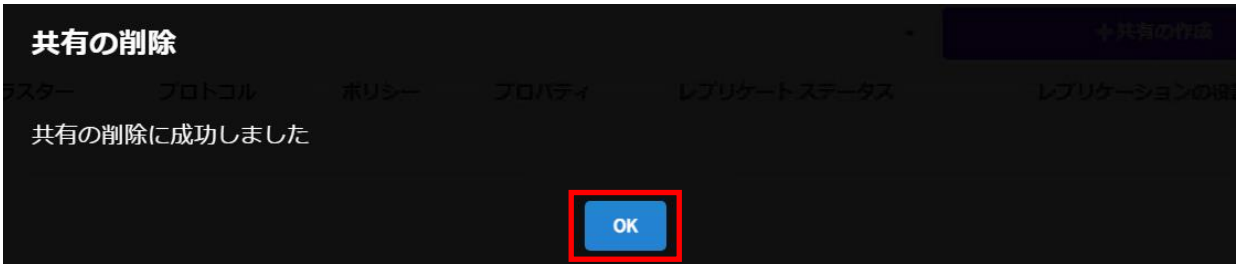

**Step 3.** 削除の確認メッセージで [はい] をクリックし、OneSystem の管理者パスワードを入力して [ベリファイ] をクリックし、“Public“ を削除します。

<削除の確認画面>

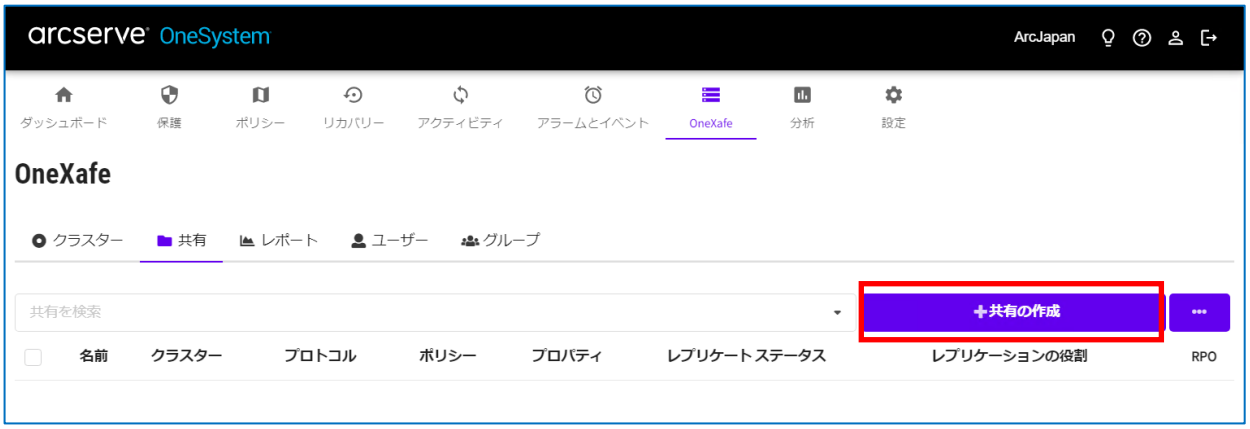

<パスワード入力画面>



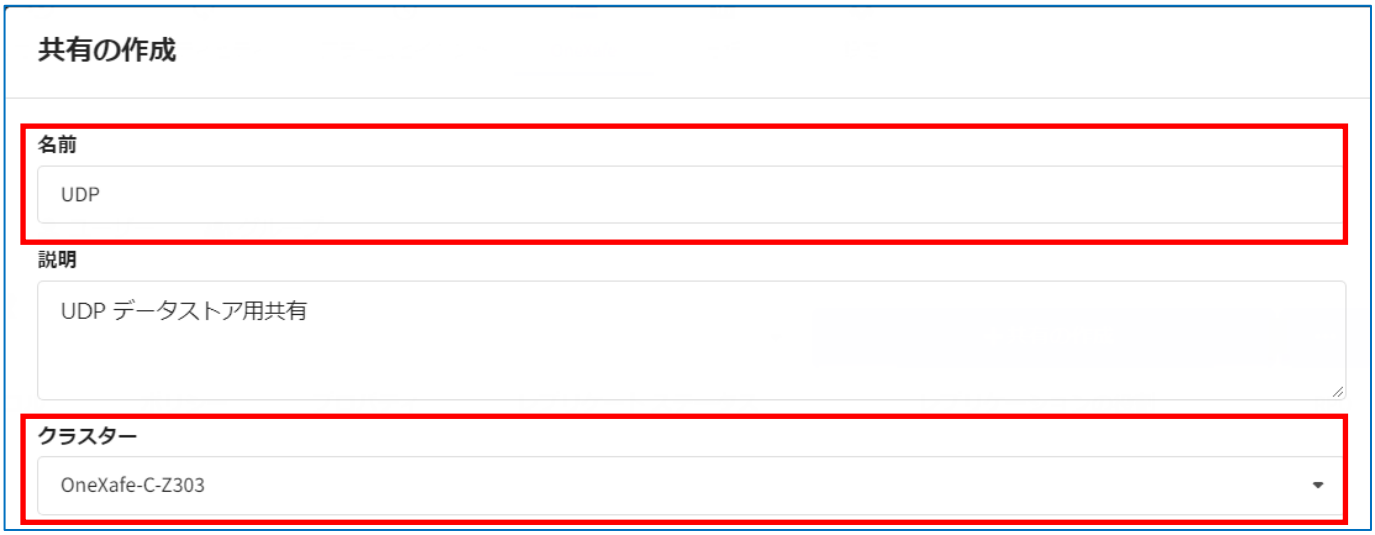

**Step 4.** 削除の成功メッセージで [OK] をクリックします。



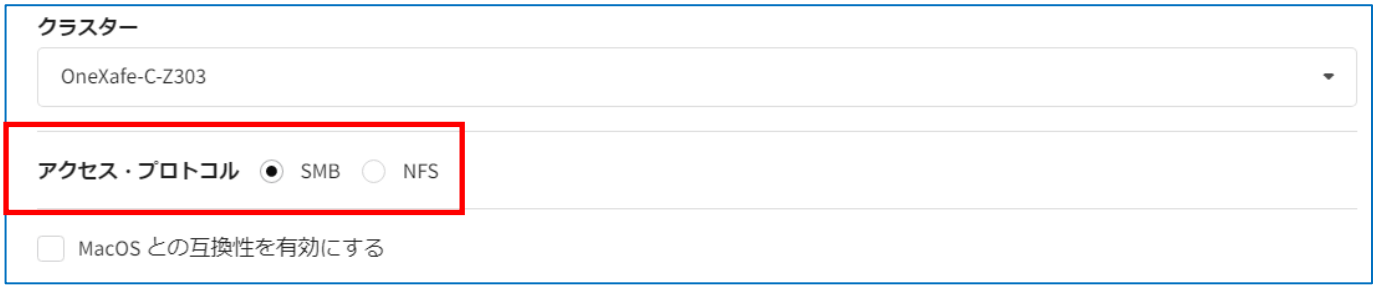

**Step 5.** 続いて新規に SMB 共有を作成するため、[+共有の作成] をクリックします。



**Step 6.** [共有の作成] 画面で [名前] に共有名を入力します（ここで登録した共有名は、共有フォルダにアクセスする際の UNC パス内で使用します）。また [クラスター] のドロップダウン リストから、前章で登録したクラスタを選択します。




**Step 7.** [アクセス・プロトコル] として “SMB” を選択します。



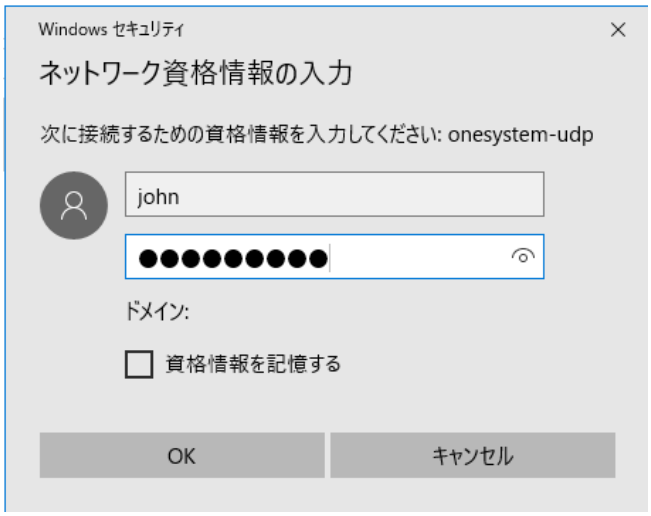

**Step 8.** 特定のユーザに読み取り/書き込み権限を付与するため、[共有アクセス] で “制限されたユーザーとグループ” を選択します。ドロップダウン リストからバックアップに使用するアカウントのみを選択して追加します。 そのアカウントの [アクセス権] 列で、”読み取り/書き込み” 権限を指定します。

**Step 9.** [ストレージ ポリシー] では “バックアップ / リカバリー” ポリシーを選択します。スナップショットの保存期間はデフォルトで 1 週間です。
ここまでの設定を確認したら画面下の [作成] ボタンをクリックして共有を作成します。


**Step 10.** 共有が作成され読み取り/書き込み権限が付与されたら、共有へのアクセスを確認します。バックアップ用ネットワークに接続している Windows マシン（Arcserve UDP がインストールされたサーバ）にログインし、エクスプローラで以下の形式でパスを指定します。

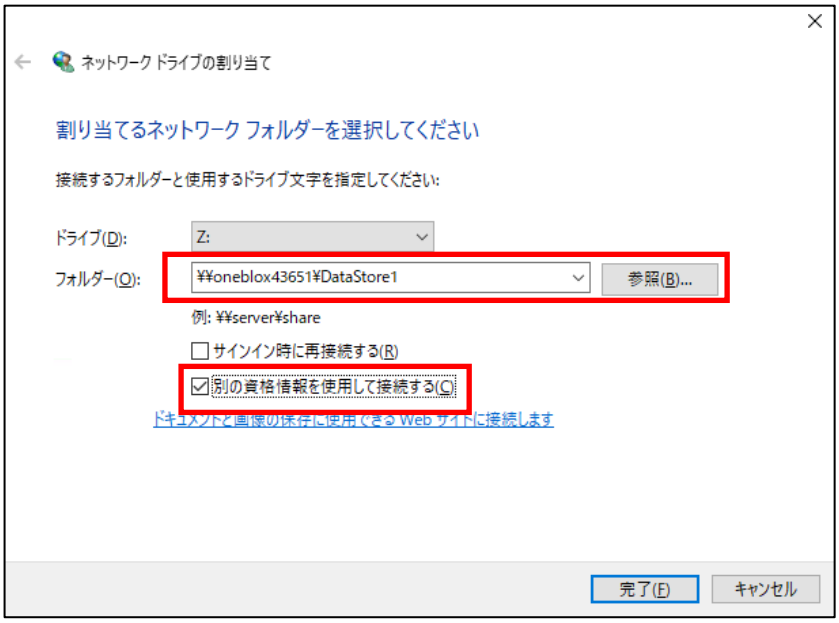
**¥¥<バックアップ用ネットワークの ホスト名もしくは IP アドレス>¥<本節で設定した共有名>**

この時、本節で権限を与えたユーザがログインして共有にアクセスできます。そのためには、OneSystem ユーザ アカウントの前半部分とパスワードを入力します。例えば、”john@mycompany.com” というメールアドレスの場合、 “john” をユーザ名として使用し、これに相当する OneSystem パスワードを入力します。

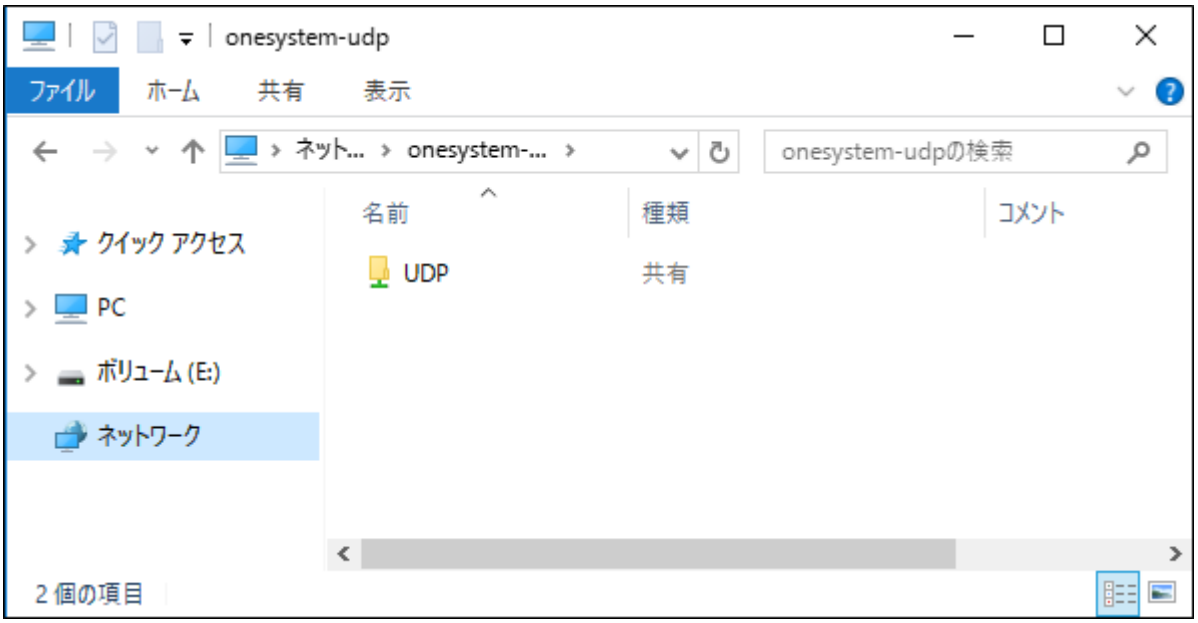


<参考>

エクスプローラなどから UNC パスを指定しても OneXafe の共有フォルダにアクセス出来ない場合や OneXafe の共有フォルダが表示されない場合はネットワーク ドライブとして割り当ててください。Windows の [ネットワーク ドライブの割り当て] のメニューの [フォルダー] で、OneXafe の共有フォルダの UNC パスを入力し、[参照] をクリックすると OneXafe の共有フォルダにアクセス出来るようになります。（必要に応じて [ネットワーク資格情報] を入力してください）




**Step 11.** OneXafe の共有フォルダがエクスプローラから表示されることを確認します。

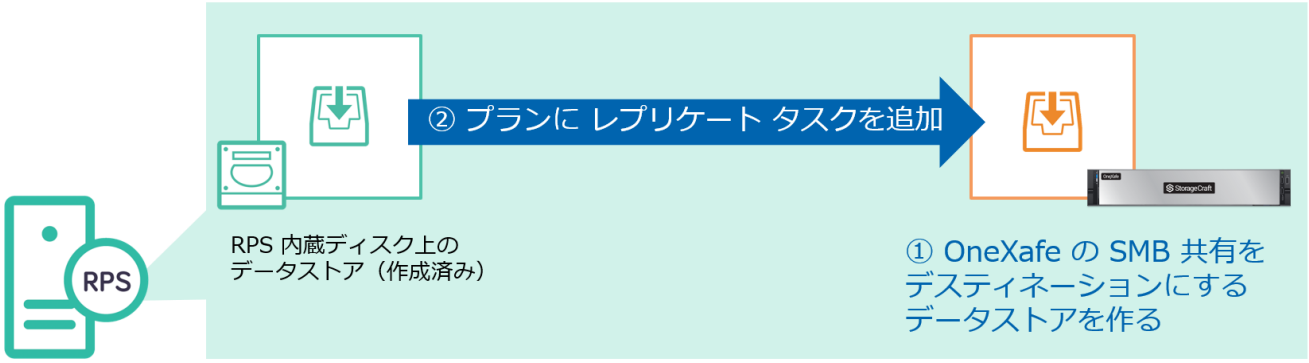


## 5. Arcserve UDP によるバックアップデータの二次複製

本章では、以下の手順を解説します。

① Arcserve UDP 復旧ポイント サーバ（以下、RPS）のデータストアを作成し、前章で作成した OneXafe 共有フォルダをデスティネーションとする。

② Arcserve UDP のプランにローカル レプリケート タスクを追加し、RPS に保存されたバックアップ データを OneXafe へ複製する。




なお、Arcserve UDP コンソールや RPS のインストール、RPS へデータをバックアップするプランの作成については、解説を割愛します。これらの設定方法については以下の資料を参考にしてください。

**Arcserve UDP 8.x 環境構築ガイド - コンソール + 復旧ポイント サーバ インストール編**

https://www.arcserve.com/sites/default/files/wp-doc/udp-80-console-install-guide.pdf

### 5.1. OneXafe を使った RPS データストアの作成

バックアップ データの複製先となるデータストアを新しく作成します。

**Step 1.** Arcserve UDP コンソールにログインし、[リソース] タブで [復旧ポイント サーバ] を開きます。対象の RPS を右クリックし [データストアの追加] をクリックします。

**Step 2.** 新しいデータストアの設定を入力します。以下の設定を行ってください。

・デデュプリケーションを有効にします。

・デデュプリケーション ブロック サイズは 64 KB にします。

・データ ストア フォルダ、データ デスティネーション、インデックス デスティネーションはすべて OneXafe の SMB 共有フォルダ内に作成された個々のフォルダのパス (例：¥¥共有フォルダ名¥フォルダ名)をそれぞれ指定します。

・ハッシュ デスティネーションは RPS のローカル パスに指定します。

・レプリケート元のデータストアで暗号化が有効な場合、今回追加するデータストアも暗号化を有効にする必要があります。

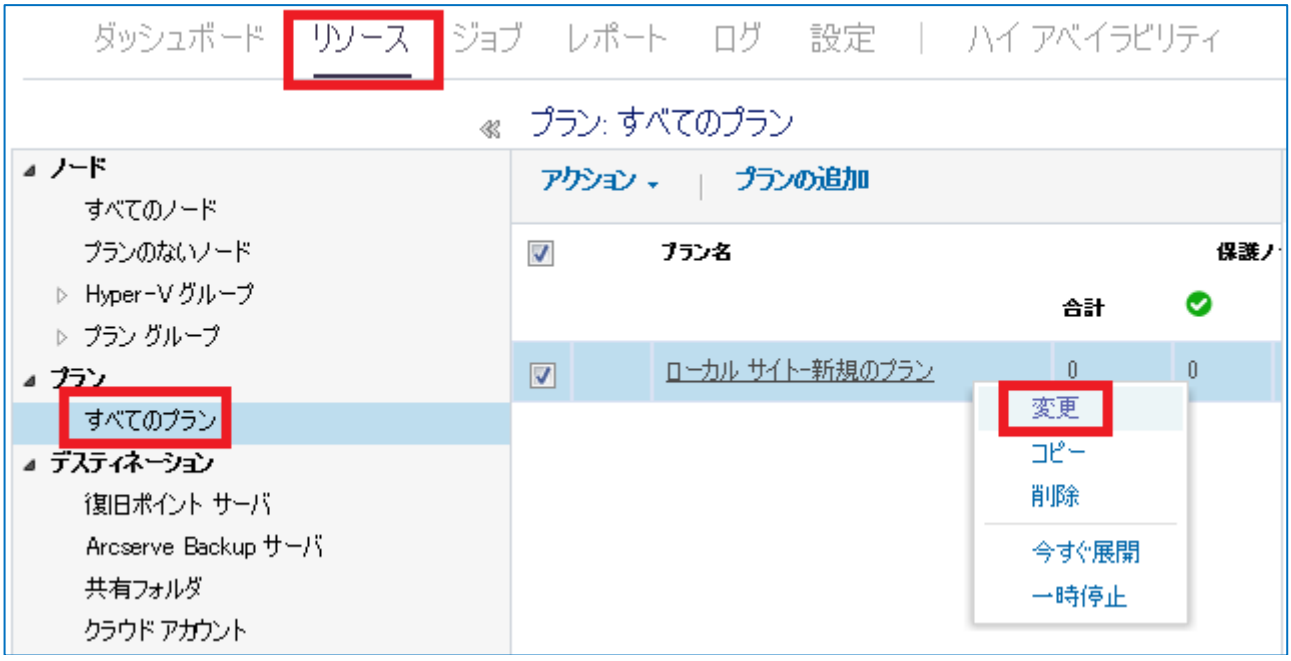

Note：ハッシュは RPS のローカル ディスクに保存されます。また、SSD を使用しない場合、全量が RPS のメモリに展開されます。RPS には十分なリソースを確保してください。

**Step 3.** 設定を保存すると、データストアが実行中の状態になります。

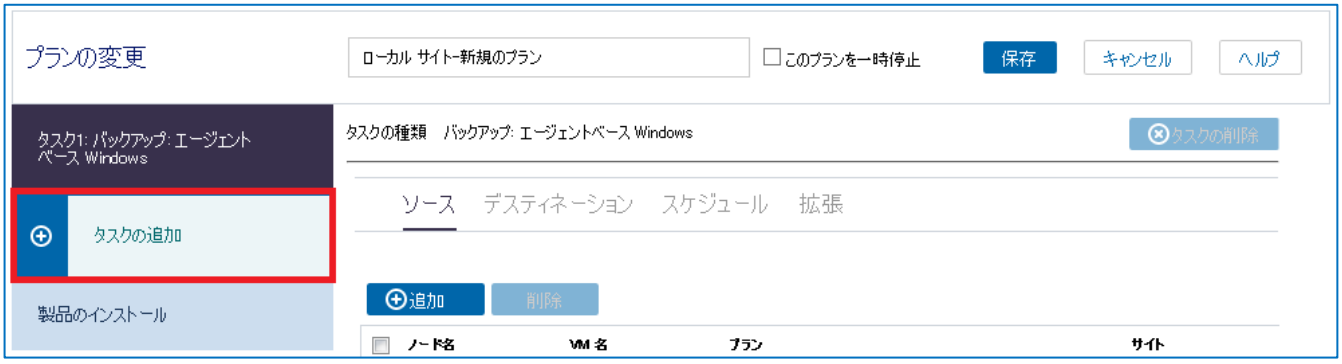

## 5.2. OneXafe への復旧ポイントのレプリケート

前項で作成したデータストアにバックアップデータをレプリケートするプランを作成します。

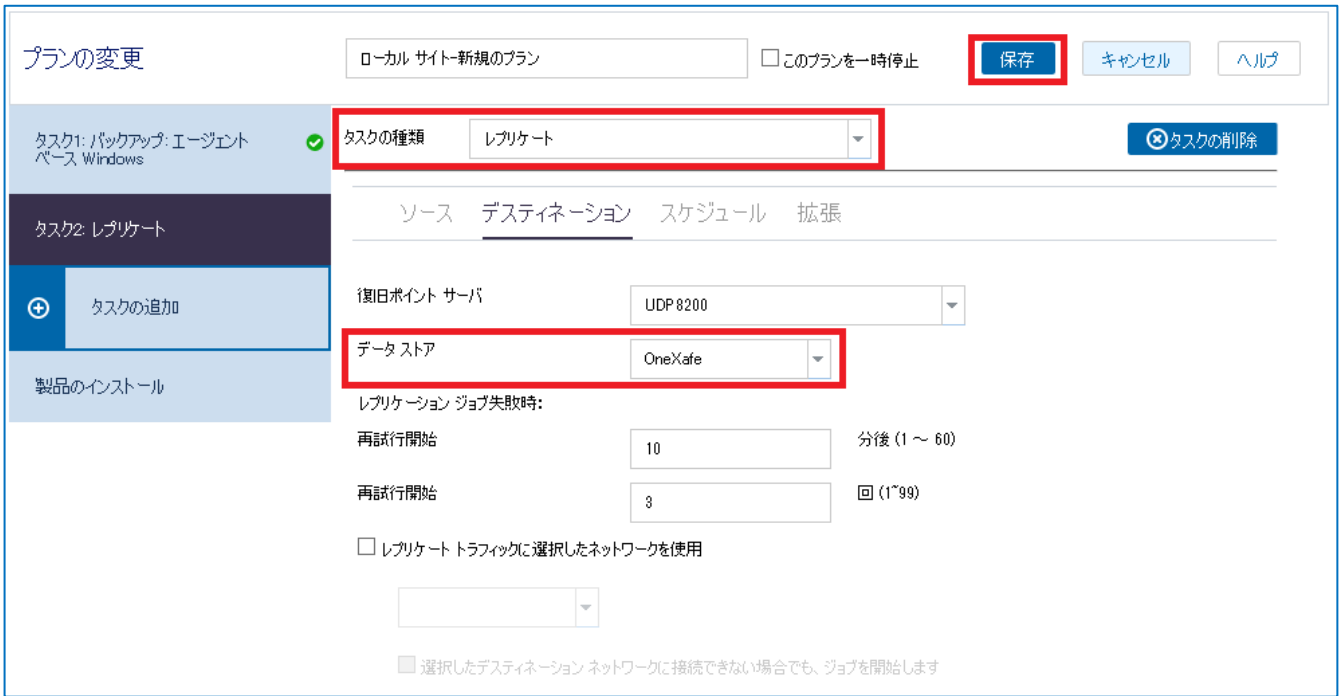
**Step 1.** Arcserve UDP コンソールを開き、[リソース] – [すべてのプラン] を開きます。RPS に元々存在していたデータストアにバックアップするプランを右クリックし [変更] を開きます。




**Step 2.** [タスクの追加] をクリックし [レプリケート] タスクを追加します。



**Step 3.** [デスティネーション] タブで、前項で作成したデータストアを指定します。プランの変更を保存します。以後、プランに従ってバックアップが実行されると、OneXafe をデスティネーション パスとするデータストアにバックアップデータがレプリケートされます。



# 6. ランサムウェア攻撃からの復旧

ランサムウェアや標的型攻撃などで Arcserve UDP の RPS が攻撃され、バックアップ データが破壊されたと想定します。この場合、以下の手順で復旧します。

① Windows Server のフレッシュ インストール
② 新しいパスワードの作成
③ Arcserve UDP のフレッシュ インストール
④ 適切な OneXafe スナップショットを特定し、新しい共有に反映
⑤ RPS のデータストアをインポートして再設定

本章では、このうち、④ と ⑤ の手順を解説します。

## 6.1. 適切なスナップショットの特定

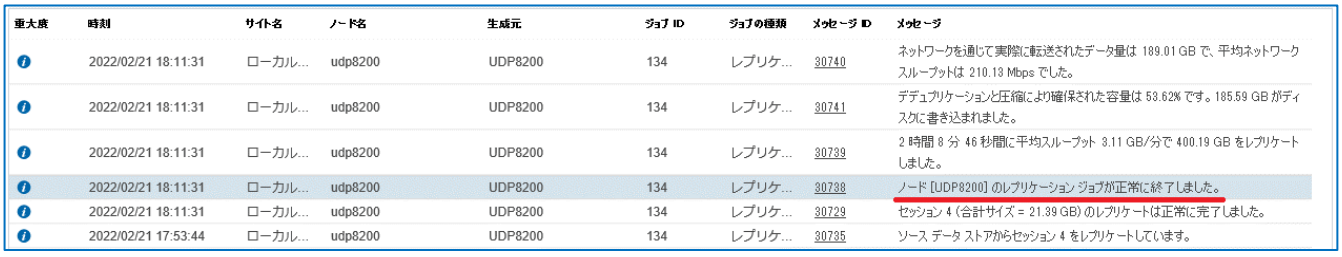
**Step 1.** Arcserve UDP のアクティビティ ログからバックアップが実行された正確な日時を特定します。

1-a. Arcserve UDP コンソールにログインし、すべてのノードをクリックします。

1-b. OneXafe SMB 共有上のデータストアにバックアップデータがレプリケートされているノードを選択します。

1-c. 右側のパネルで、特定のレプリケート ジョブをクリックします。


1-d アクティビティ ログが表示されるので、レプリケート ジョブが完了した正確な時刻を記録します。



| 重大度 | 時刻 | サイト名 | ノード名 | 生成元 | ジョブ ID | ジョブの種類 | メッセージ ID | メッセージ |
|---|---|---|---|---|---|---|---|---|
| i | 2022/02/21 18:11:31 | ローカル... | udp8200 | UDP8200 | 134 | レプリケ... | 30740 | ネットワークを通じて実際に転送されたデータ量は 189.01 GB で、平均ネットワーク スループットは 210.13 Mbps でした。 |
| i | 2022/02/21 18:11:31 | ローカル... | udp8200 | UDP8200 | 134 | レプリケ... | 30741 | デデュプリケーションと圧縮により確保された容量は 53.62% です。185.59 GB がディスクに書き込まれました。 |
| i | 2022/02/21 18:11:31 | ローカル... | udp8200 | UDP8200 | 134 | レプリケ... | 30739 | 2 時間 8 分 46 秒間に平均スループット 3.11 GB/分で 400.19 GB をレプリケートしました。 |
| i | 2022/02/21 18:11:31 | ローカル... | udp8200 | UDP8200 | 134 | レプリケ... | 30738 | ノード [UDP8200] のレプリケーション ジョブが正常に終了しました。 |
| i | 2022/02/21 18:11:31 | ローカル... | udp8200 | UDP8200 | 134 | レプリケ... | 30729 | セッション 4 (合計サイズ = 21.39 GB) のレプリケートは正常に完了しました。 |
| i | 2022/02/21 17:53:44 | ローカル... | udp8200 | UDP8200 | 134 | レプリケ... | 30735 | ソース データ ストアからセッション 4 をレプリケートしています。 |

Note：Arcserve UDP コンソールがサイバー攻撃で破壊された場合、本 Step は実行できません。レポート通知機能などを活用し、日常的にジョブの成否を確認する事をお勧めします。レポート通知機能については以下の記事を参考にしてください。

**Arcserve UDP：一通のメールで全台のバックアップ状況をチェックできる ～ レポートのメール送信**
https://arcserve.txt-nifty.com/blog/2016/04/arcserve-udp-28.html

**Step 2.** Arcserve UDP のジョブ実行時間を基に、OneXafe の UI から適切なスナップショットを特定します。以下の方法でスナップショット一覧を表示できます。

**2-a.** OneXafe ローカル コンソールに “admin” でログインします。
（パスワードは OneXafe Web コンソールと同じです）
ログインしたら、以下のコマンドを順に実行します。（左肩の数字は入力しません。）

1. Share
2. Snapshot list <<共有フォルダ名>> Japan

**2-b.** Arcserve UDP でバックアップジョブが成功した直後に作成されたスナップショットを確認します。
[Converted(Japan)] が日本時間（JST）で表示されたスナップショットの取得時刻です。

```
oneblox43651 login: admin
Password:
oneblox43651(config) share
oneblox43651(config-share) list
   Name     Protocol  Writeable  Retention  Compression   Dedupe   FullAudit
UDP             SMB       True      1week          lz4  variable       False
oneblox43651(config-share) snapshot list UDP Japan
Snapid       Timestamp          Converted(Japan)
2875    2022-05-27-00.15.48  2022-05-27-16.15.48+0900
2923    2022-05-28-00.10.49  2022-05-28-16.10.49+0900
2971    2022-05-29-00.14.36  2022-05-29-16.14.36+0900
3024    2022-05-30-00.25.19  2022-05-30-16.25.19+0900
```

## 6.2. 復旧に必要な認証情報

復旧に当たっては以下の認証情報が必要になります。

・OneXafe iDRAC
・OneXafe Local admin アカウント （コマンドライン）
・OneSystem admin アカウント （管理用）
・OneSystem user アカウント （RPS のデータストアへアクセスする用途）

・Arcserve UDP システム：Windows Server の Administrator と IPMI

・Arcserve UDP RPS データストアの暗号化パスワード（暗号化が有効な場合に限る）

・Arcserve UDP プランのパスワード（設定している場合）

## 6.3. OneXafe スナップショットを新しい共有に反映する

OneXafe スナップショットを新しい共有に反映するには、OneXafe ローカル コンソールで以下のコマンドを順に実行します。

**1.** enable

**2.** snapshot list <<共有フォルダ名>> Japan

```
oneblox43651(config) share
oneblox43651(config-share) enable
oneblox43651(config-share) snapshot list UDP Japan
Snapid       Timestamp           Converted(Japan)
2875    2022-05-27-00.15.48  2022-05-27-16.15.48+0900
2923    2022-05-28-00.10.49  2022-05-28-16.10.49+0900
2971    2022-05-29-00.14.36  2022-05-29-16.14.36+0900
3024    2022-05-30-00.25.19  2022-05-30-16.25.19+0900
3074    2022-05-31-00.06.41  2022-05-31-16.06.41+0900
3121    2022-06-01-00.09.31  2022-06-01-16.09.31+0900
3130    2022-06-01-04.17.07  2022-06-01-20.17.07+0900
3132    2022-06-01-05.18.38  2022-06-01-21.18.38+0900
3134    2022-06-01-06.19.43  2022-06-01-22.19.43+0900
3136    2022-06-01-07.21.14  2022-06-01-23.21.14+0900
3138    2022-06-01-08.22.40  2022-06-02-00.22.40+0900
3140    2022-06-01-09.24.20  2022-06-02-01.24.20+0900
3142    2022-06-01-10.26.38  2022-06-02-02.26.38+0900
3144    2022-06-01-11.29.37  2022-06-02-03.29.37+0900
3145    2022-06-01-12.00.07  2022-06-02-04.00.07+0900
3147    2022-06-01-13.01.46  2022-06-02-05.01.46+0900
3149    2022-06-01-14.04.53  2022-06-02-06.04.53+0900
3151    2022-06-01-15.08.23  2022-06-02-07.08.23+0900
3153    2022-06-01-16.09.05  2022-06-02-08.09.05+0900
3155    2022-06-01-17.09.33  2022-06-02-09.09.33+0900
3157    2022-06-01-18.11.58  2022-06-02-10.11.58+0900
3159    2022-06-01-19.13.29  2022-06-02-11.13.29+0900
3161    2022-06-01-20.15.01  2022-06-02-12.15.01+0900
3163    2022-06-01-21.15.04  2022-06-02-13.15.04+0900
3165    2022-06-01-22.15.07  2022-06-02-14.15.07+0900
3167    2022-06-01-23.18.07  2022-06-02-15.18.07+0900
3169    2022-06-02-00.18.19  2022-06-02-16.18.19+0900
3171    2022-06-02-01.18.22  2022-06-02-17.18.22+0900
3173    2022-06-02-02.12.27  2022-06-02-18.12.27+0900
3174    2022-06-02-02.42.29  2022-06-02-18.42.29+0900
3175    2022-06-02-03.12.31  2022-06-02-19.12.31+0900
oneblox43651(config-share)
```

**3.** snapshot promote <<古い共有フォルダ名>> <<スナップショット ID（Snapid）>> <<新しい共有フォルダ名 >>

※ スナップショット ID（Snapid）は下図の赤枠箇所です。復旧したい時点のスナップショットを指定してください。

```
3169    2022-06-02-00.18.19  2022-06-02-16.18.19+0900
3171    2022-06-02-01.18.22  2022-06-02-17.18.22+0900
3173    2022-06-02-02.12.27  2022-06-02-18.12.27+0900
3175    2022-06-02-03.12.31  2022-06-02-19.12.31+0900
3176    2022-06-02-03.42.33  2022-06-02-19.42.33+0900
oneblox43651(config-share) snapshot promote UDP 3171 UDP-recovery
UDP successfully cloned to UDP-recovery. Waiting for share to be available ...
Destination share UDP-recovery available. Promoting snapshot id 3171
Snapshot promotion complete.
oneblox43883(config-share)
```

**4.** update <<新しい共有フォルダ名>> --writeable

**5.** disable

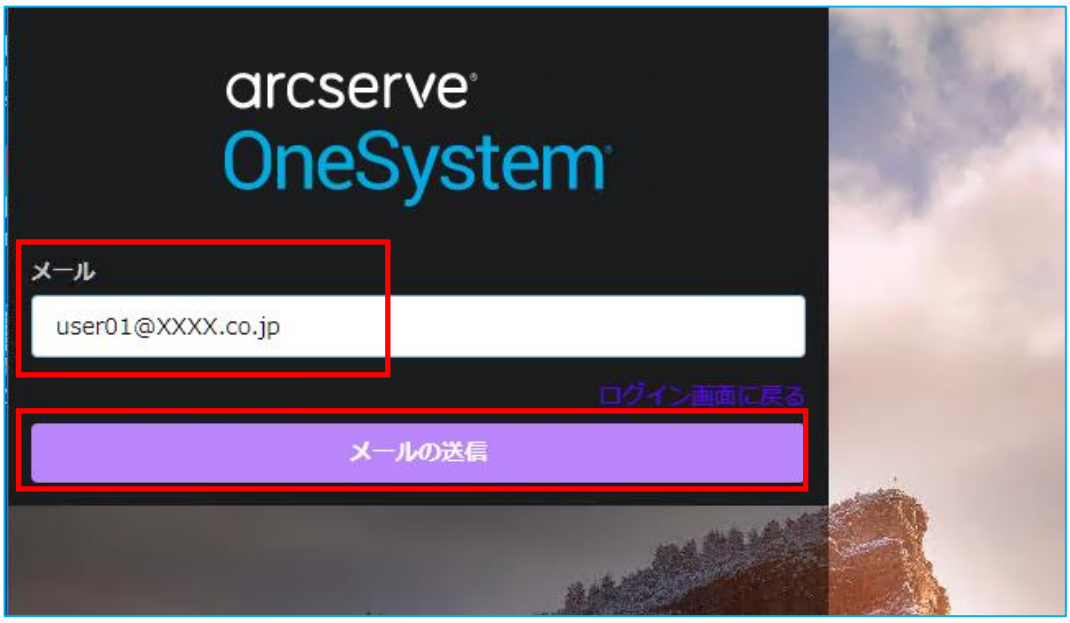
```
oneblox43883(config-share) update UDP-recovery --writeable
oneblox43883(config-share) disable
oneblox43883(config-share) list
    Name      Protocol  Writeable  Retention  Compression   Dedupe   FullAudit
UDP               SMB       True      1week          lz4  variable      False
UDP-recovery      SMB       True      1week          lz4  variable      False
oneblox43883(config-share)
```

### 6.4. OneXafe の共有フォルダにアクセス権限を持つユーザアカウントのパスワード変更方法

前節で新規に作成された共有フォルダに不正にアクセス出来ないようにプライベート OneSystem に登録されたユーザアカウントのパスワードを以下の手順で変更します。

**Step 1.** プライベート OneSystem のログイン画面を表示して、[パスワードを忘れた / 変更する] をクリックします。


**Step 2.** パスワードを変更したいユーザ アカウントのメールアドレスを入力し、[メールの送信] をクリックします。



**Step 3.** 以下のような [成功しました!] の画面が表示されましたら、パスワードを変更したいユーザ アカウントのメールボックスを確認します。


**Step 4.** プライベート OneSystem から以下のようなメールがユーザアカウントに届きますので、メール中にある URL をクリックして表示されたパスワード指定画面で新しいパスワードを入力し、変更作業を完了させます。

Thank you for contacting Arcserve,

パスワード変更のリクエストを受信しました。

このリクエストを行った場合は、下記のリンクをクリックしてパスワードを変更してください。

https://prios48/reset-password?token=4-66q-09f1a74fc8eea21d2138

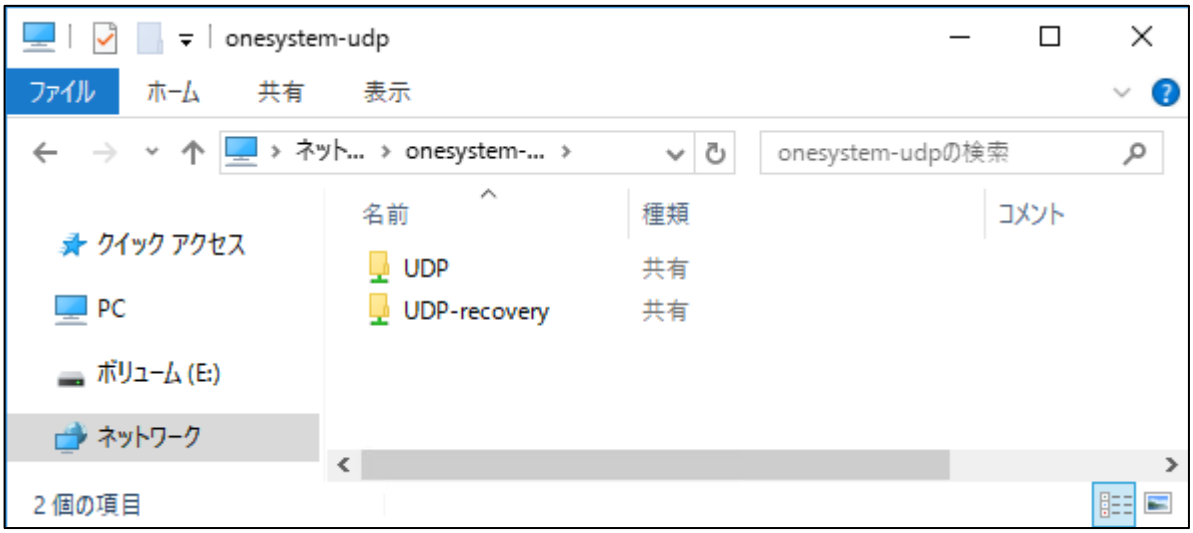
パスワードを変更したくない場合には、このメッセージを無視してください。

よろしくお願いいたします。
OneSystem by Arcserve

## 6.5. Arcserve UDP デデュプリケーション データストアのインポート

この節では、新しくインストールされた Arcserve UDP 復旧ポイントサーバにデデュプリケーション データストアをインポートします。

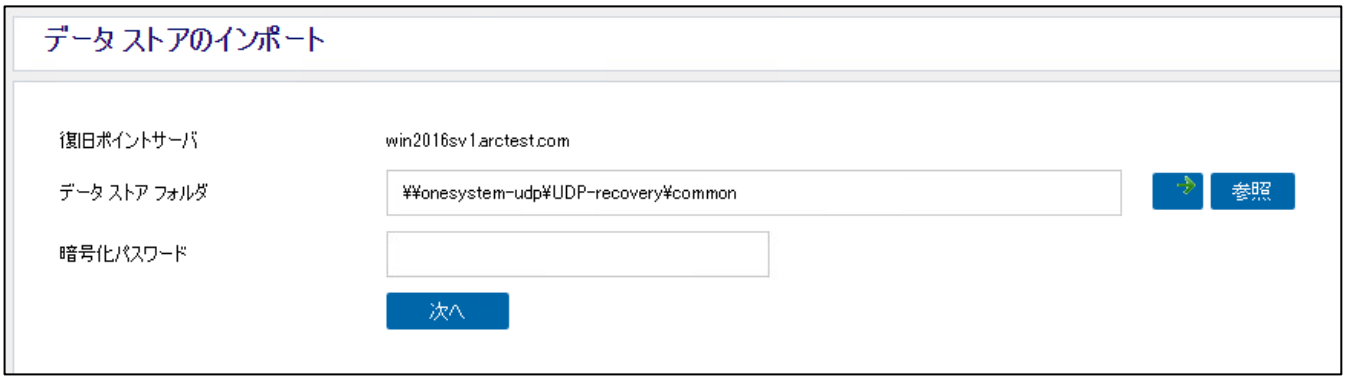
**Step 1.** 復旧ポイントサーバのエクスプローラで、新しい共有フォルダが参照出来るかを確認します。

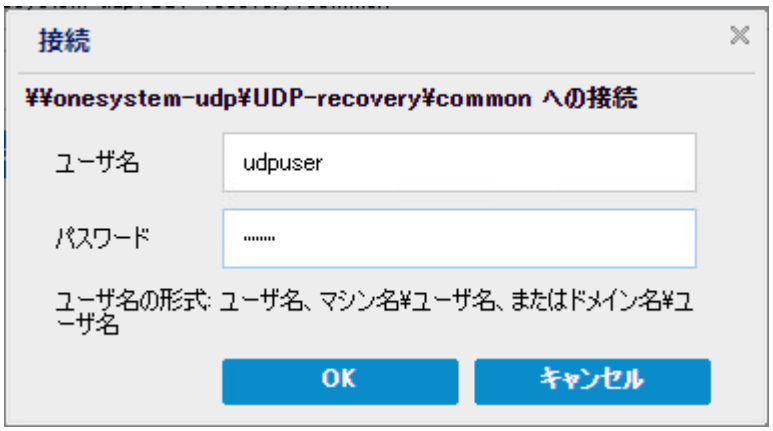



**Step 2.** Arcserve UDP コンソールにログインします。 [リソース] タブを開き、左ペインの [復旧ポイントサーバ] を開きます。

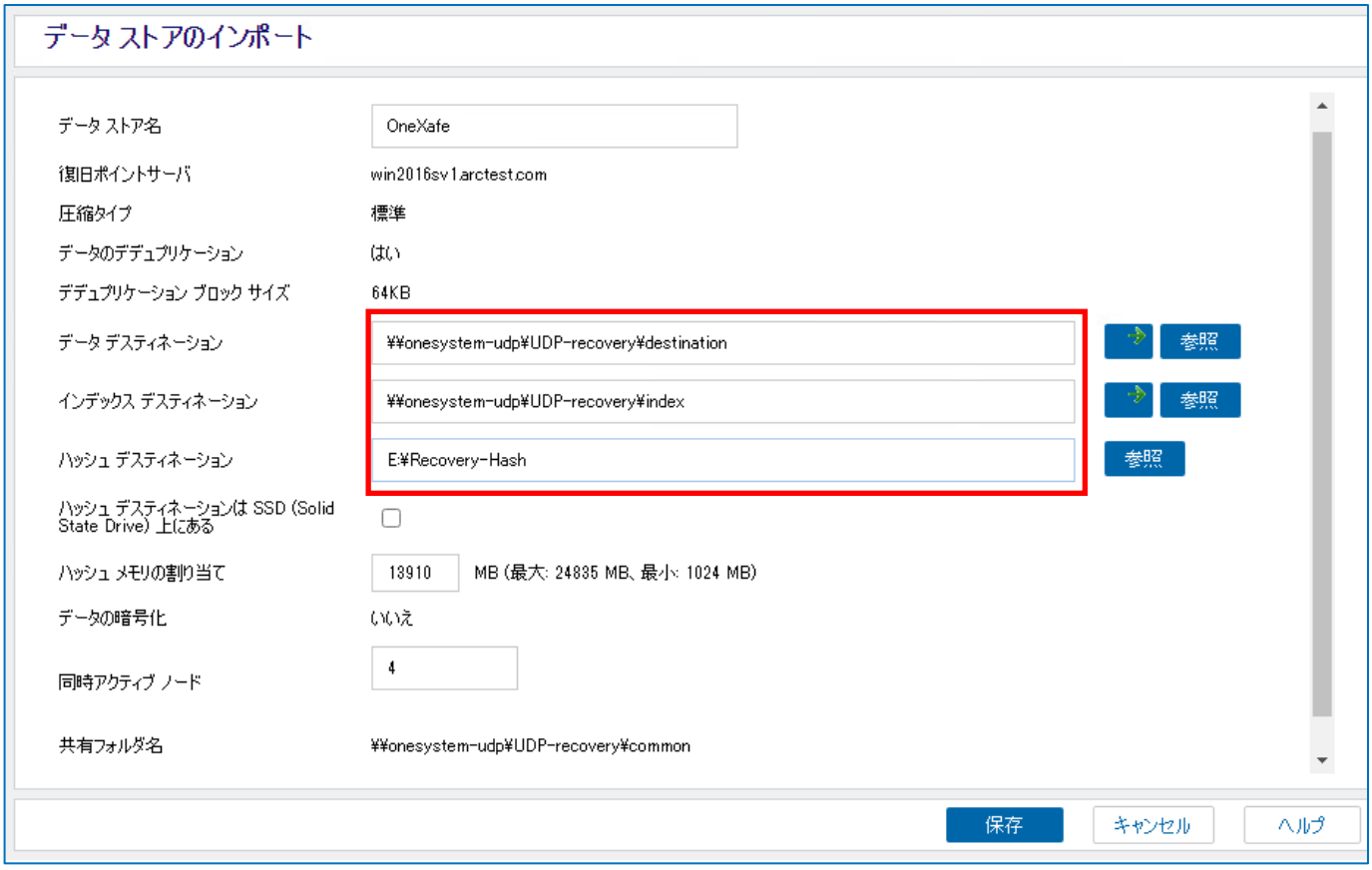
**Step 3.** 復旧ポイントサーバを右クリックし、メニューから [データストアのインポート] を選択します。

**Step 4.** [データストアのインポート] 画面が開きます。[データストア フォルダ] パスを入力し、右矢印ボタンをクリックして OneXafe の共有フォルダへの接続情報を入力して[OK]ボタンをクリック後、[次へ] をクリックします。



**Step 5.** [データストアのインポート] 画面にて、共有フォルダ名を参考に、適切な データ デスティネーションとインデックス デスティネーションのパスを指定します。
ハッシュ デスティネーションには RPS の空のフォルダのパスを指定します。[保存] をクリックすると、データストアがリストア限定モードもしくはエラーでインポートされます。
Note：リストア限定モードの場合は必要なファイル/フォルダのリストアができます。




**Step 6.** ハッシュ データを再作成するため、RPS のコマンド プロンプトを開き、以下のパスに移動します。
C:¥Program Files¥Arcserve¥Unified Data Protection¥Engine¥BIN

最初に as_dsmgr.exe を以下のように実行してインポートしたデータストアを停止させます。

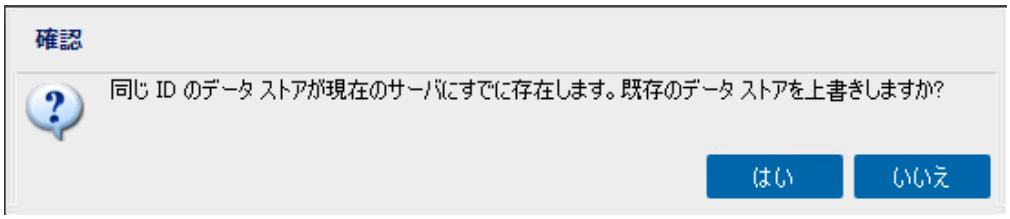
as_dsmgr /StopDS <<データストア名>>

次に as_gddmgr.exe を以下のように実行します。

as_gddmgr -Scan RebuildHashWithIndexPath <<インデックス デスティネーション パス>>
-NewHashPath <<新しいハッシュ デスティネーション パス>>

```
C:¥Program Files¥Arcserve¥Unified Data Protection¥Engine¥BIN>as_dsmgr.exe /StopDS OneXafe

************************************************************

Stop data store "OneXafe" successfully.

************************************************************

C:¥Program Files¥Arcserve¥Unified Data Protection¥Engine¥BIN>as_gddmgr -Scan RebuildHashWithIndexPath
 ¥¥onesystem-udp¥UDP-recovery¥index -NewHashPath E:¥Recovery-Hash

Start to calculate ref count...
-Processing index file [2/2]...Succeeded.
-Writing refcount file [2/2]...Succeeded.
Finished calculating ref count.

Start to rebuild hash database...
-Processing refcount file [2/2]...Succeeded.
-Flushing hash database...Succeeded.
-Processing redundant data...Succeeded.
Succeeded to rebuild hash database.

Please import the data store to link the new hash path as its hash destination.

C:¥Program Files¥Arcserve¥Unified Data Protection¥Engine¥BIN>_
```

**Step 7.** ハッシュ再作成の完了後、as_dsmgr.exe などでデータストアを手動で開始すると、既存のプランのデスティネーションとしてこの新しいデータストアを指定できるようになります。こうする事で、この新しいデータストアでバックアップを行えます。新しい共有を古いデータストアが存在する RPS にインポートした場合、以下のメッセージが表示されますが、[はい] をクリックして上書きします。




古いデータが完全に削除され、認証情報が新しく作り直された Arcserve UDP サーバにデータストアをインポートする事をお勧めします。

### 6.6. 既知の制限事項

・OneXafe では新しい共有に反映されたスナップショットは元々の共有と同じユーザ アクセス権が割り当てられています。スナップショットを共有に反映する間、元と異なるアクセス権限を設定する事はできません。OneSystem ログインで共有が作成された後は、新しい共有のアクセス権を変更する事ができます。

・OneXafe 共有上の復旧ポイントは、Windows エクスプローラで復旧ポイント ビューに変更する事はできません。

# 7. プライベート OneSystem 仮想アプライアンスのバックアップ方法

**注意!!**：本章に記載されているプライベート OneSystem のバックアップは必ずお客様自身で行ってください。プライベート OneSystem が破損した場合、設定情報は失われ OneXafe 上の共有フォルダやアカウントの管理が行えなくなります。また、プライベート OneSystem のバックアップを Arcserve が行う事はありません。

プライベート OneSystem 仮想アプライアンス（以下、本章では“仮想アプライアンス“と省略）は、整合性の取れたバックアップを取得するために、サービスが停止した状態でバックアップを行う必要があります。
本章では Arcserve UDP による仮想マシンのエージェントレス バックアップ機能を利用し、仮想アプライアンスを停止した状態で丸ごとバックアップ/リストアする方法を紹介します。


仮想アプライアンスを停止状態でバックアップするため、以下のようにバックアップ実行の前後に仮想アプライアンスの停止と再起動を実行します。

1．仮想アプライアンスの停止
2．エージェントレスバックアップ
3．仮想アプライアンスの再起動

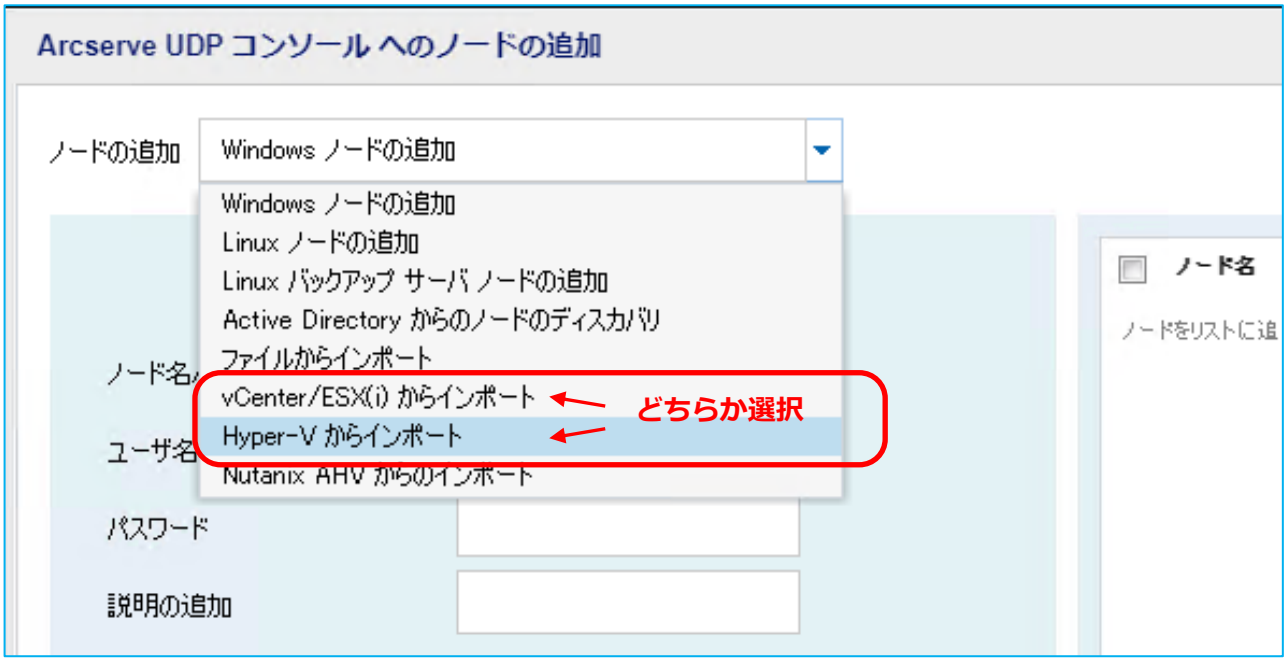
仮想アプライアンスの内部にはリモートからファイルを配置することがセキリティ上出来ないため、Arcserve UDP のエージェントレスバックアップのプランに、仮想アプライアンスを停止/起動させるスクリプトを組み込んで実行させる事が出来ません。
このため、Arcserve UDP の PowerShell インターフェース (PowerCLI)を利用してバックアップを実行します。

本章では Arcserve UDP の PowerCLI を利用した仮想アプライアンスのバックアップ方法を解説し、Hyper-V 環境および VMware 環境での仮想アプライアンスの停止と起動方法のサンプルを掲載します。

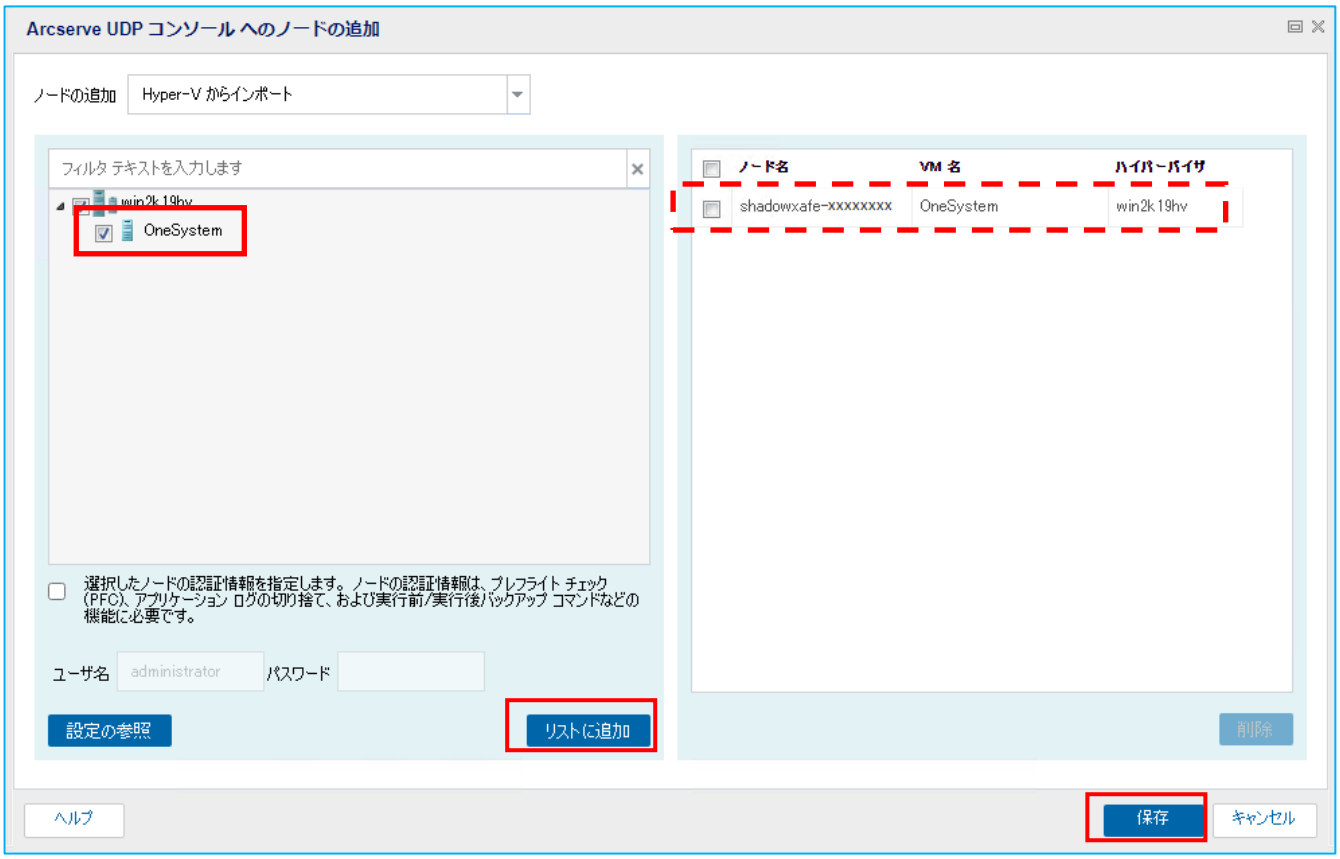
## 7.1. 仮想アプライアンスのエージェントレス バックアップのプラン作成

仮想アプライアンスをバックアップするスクリプトを作成する前に、Arcserve UDP コンソールで仮想アプライアンスをエージェントレス バックアップするプランを作成いたします。

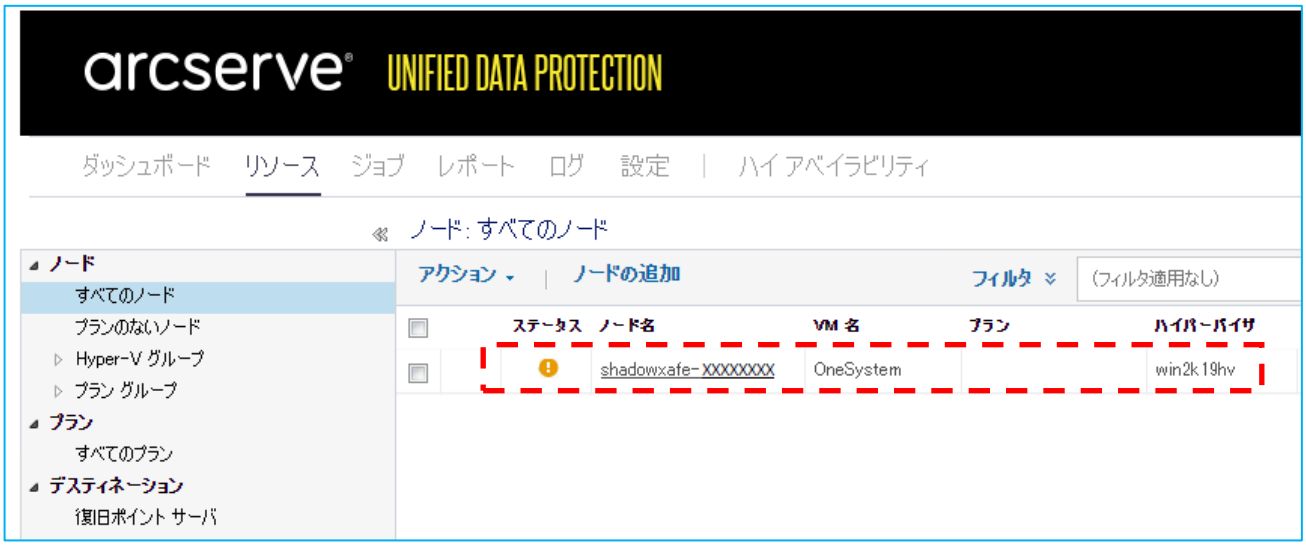
**Step 1.** Arcserve UDP コンソールから [リソース] を開いて [ノード] から [ノードの追加] をクリックします。[Arcserve UDP コンソール へのノードの追加] の画面で [ノードの追加] の選択画面から仮想アプライアンスを実行する仮想環環境に合わせ Hyper-V であれば “Hyper-V からインポート”、VMware であれば “vCenter/ESX(i) からインポート“ のどちらかを選択します。



**Step 2.** 仮想環境の情報を入力する画面で、Hyper-V ホストもしくは vCenter(ESX ホスト)の情報および、管理者のユーザ名、パスワードなどの情報を入力して [接続] をクリックします。
以下画面の左側に表示される仮想アプライアンスにチェックをして [リストに追加] をクリックすると右側に仮想アプライアンスの情報が表示されることを確認して [保存] をクリックして画面を閉じます。

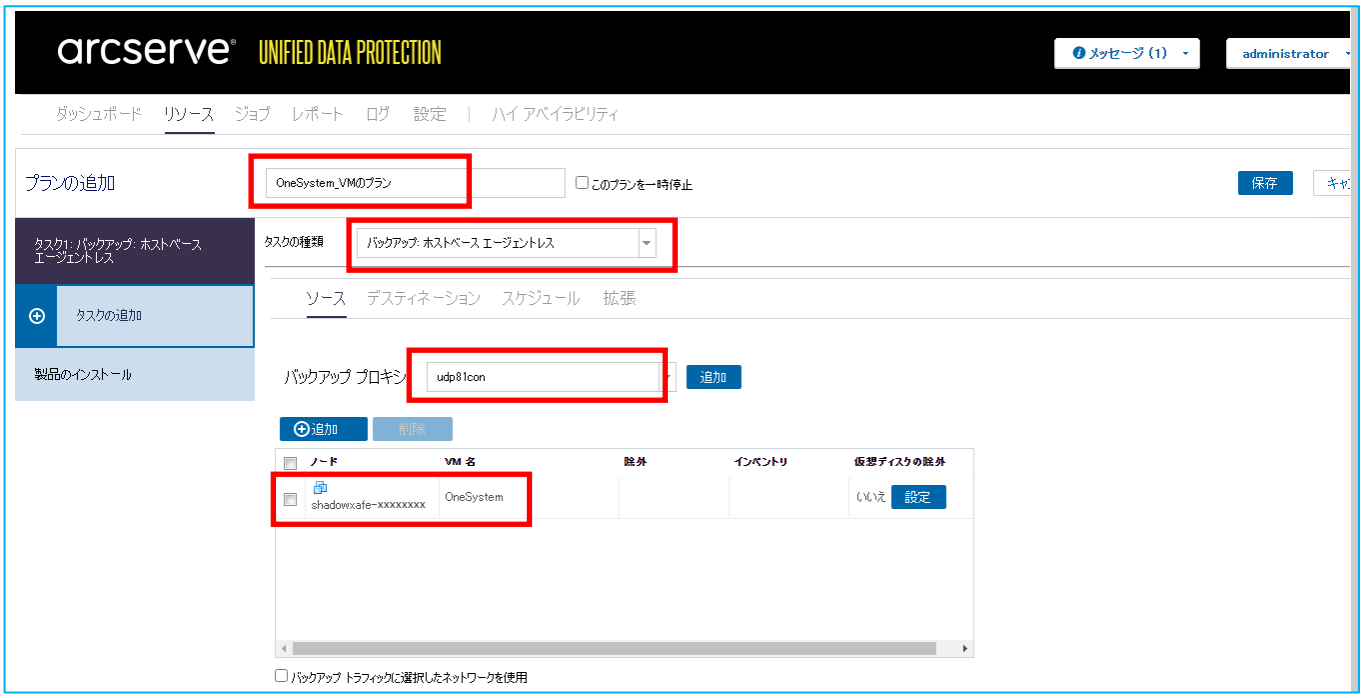



**Step 3.** Arcserve UDP コンソールの [リソース] - [ノード] に仮想アプライアンスが登録されたことを確認します。



**Step 4.** [リソース] - [プラン] から [プランの追加] をクリックします。任意のプラン名を入力後、[タスクの種類] で [バックアップ: ホストベース エージェントレス] を選択します。[ソース] タブで [バックアップ プロキシ] に Arcserve UDP Windows Agent が導入されたサーバを指定し、 [ノード] の [追加] をクリックして仮想アプライアンスを追加します。

※　Hyper-V 環境の場合は Hyper-V ホストに Arcserve UDP Windows Agent をインストールして [バックアップ プロキシ] として指定してください。




**Step 5.** [デスティネーション] を設定後、 [スケジュール] で [日次増分バックアップ] を選択して [削除] ボタンをクリックします。バックアップ スケジュールがすべて削除されたことを確認し、[保存] をクリックします。

※ バックアップは Arcserve UDP の PowerCLI を利用するため、プランでは無くタスク スケジューラなどでスケジュールを設定して実行します。

**Step 6.** [リソース] で作成したプランが表示されていればプラン作成作業は終了です。

## 7.2. バックアップ プランを実行する Arcserve UDP の PowerCLI スクリプトの作成

**Step 1.** 仮想アプライアンスをバックアップするバックアップ プロキシサーバにログインします。

**Step 2.** Arcserve UDP Windows Agent のインストール先フォルダ配下 “¥Engine” に ¥PowerCLI フォルダがあることを確認します。

<参考> Arcserve UDP Windows Agent のデフォルトのインストール先の場合：
C:¥Program Files¥Arcserve¥Unified Data Protection¥Engine¥PowerCLI

※ Windows PowerShell を管理者モードで画面を開き、¥PowerCLI フォルダに移動して以下のコマンドを実行すると、UDPPowerCLI.ps1 のコマンドオプションやサンプルなどの情報が確認出来ます。

```
PS C:¥Program Files¥Arcserve¥Unified Data Protection¥Engine¥PowerCLI>
    get-help .¥UDPPowerCLI.ps1
```

Arcserve UDP の PowerCLI の使用方法や Windows PowerShell のスクリプト実行ポリシーの設定変更、”-UDPConsolePasswordFile” オプションで指定する暗号化されたパスワードファイルの作成方法については以下を参照ください。

[Arcserve 製品ブログ] Arcserve UDP：Windows のバックアップを PowerShell から実行する方法
https://arcserve.txt-nifty.com/blog/2020/04/post-c96781.html

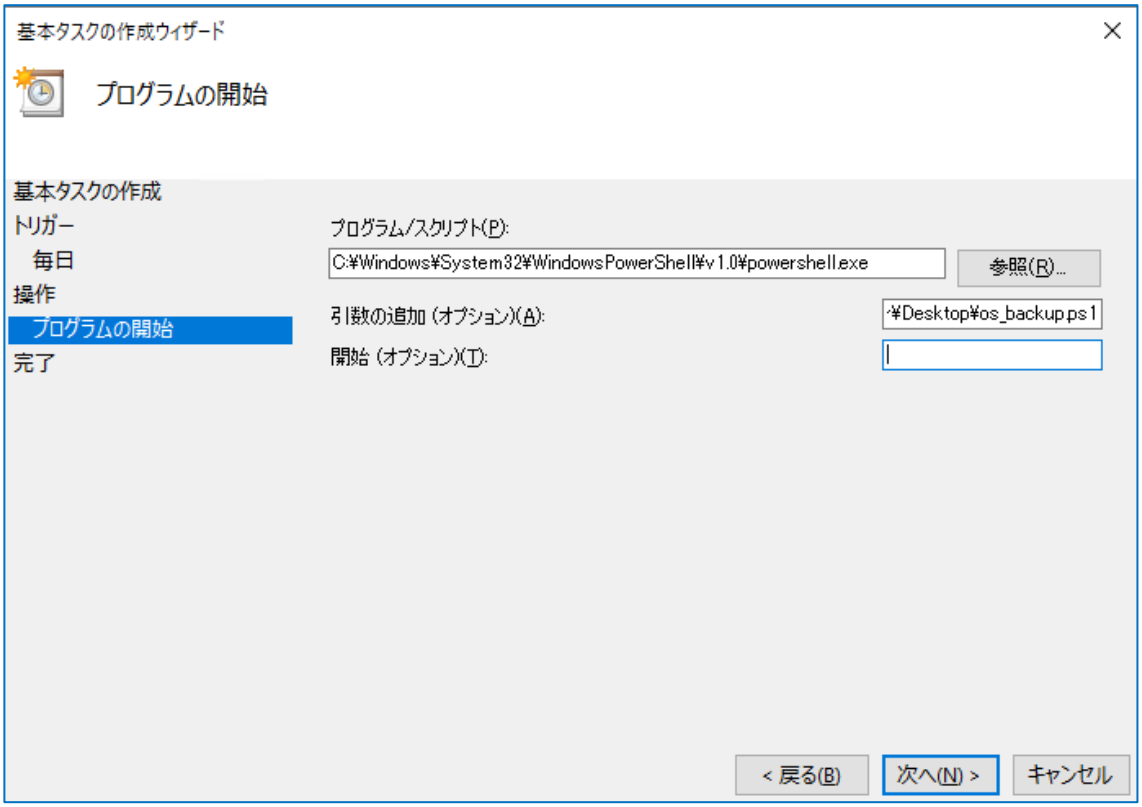
**Step 3.** メモ帳などテキストエディタを開き、Arcserve UDP の PowerCLI でバックアップを行う PowerShell スクリプトファイル (*.ps1)を作成します。スクリプト中では、バックアップ実行の前後に仮想アプライアンスの停止と再起動処理を追加してください。Hyper-V 環境および VMware 環境で仮想マシンの停止と再起動を行う PowerShell コマンドを含んだスクリプトの例をそれぞれ次節以降で紹介いたします。

**Step 4.** Windows の [管理ツール] からタスク スケジューラを起動します。[基本タスクの作成] メニューから作成ウィザードの画面を開き、タスクの [名前] を入力します。[トリガー] の実行時間と間隔についてはご利用環境の運用要件に合わせて設定を行います。なお、本資料では Windows タスク スケジューラを使った方法を紹介しますが、それ以外のジョブ管理ツールを利用しても問題ございません。

※ バックアップ中にプライベート OneSystem の仮想アプライアンスが停止していても、OneXafe の共有フォルダへのアクセスは可能です。
このため、Arcserve UDP による通常の業務サーバのバックアップに関係無く、任意のタイミングで仮想アプライアンスのバックアップを実行できます。

**Step 5.** タスクの [操作] については [プログラムの開始] を選択し、以下をそれぞれ設定します。

[プログラム/スクリプト]
"C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe"
[引数]
"-executionpolicy remotesigned C:¥<"スクリプトファイルのフォルダ名">¥<"ps1 ファイル名">




**Step 6.** 作成ウィザードの最後に [完了] をクリックして、タスクの作成を終了します。

タスク スケジューラの [操作] の [引数] で指定した"ps1 ファイル" について、Hyper-V 環境または VMware 環境で仮想アプライアンスをバックアップ前後で停止、再起動させるコマンドを含めたスクリプトのサンプルを次節以降で掲載します。
なお、**Hyper-V 環境または VMware 環境で仮想アプライアンスを停止、再起動させるコマンドは各仮想化ベンダー**

**が提供しておりますので、不具合等のサポートは仮想化ベンダーにお問い合わせください。**
**サンプルのスクリプトをご利用の際には仮想アプライアンスの実環境でのバックアップ検証を充分に行っていただくことをお勧めいたします。**

### 7.3. Hyper-V 環境での仮想アプライアンスの停止と起動スクリプトのサンプル

以下では、Hyper-V 環境に展開された仮想アプライアンスを Arcserve UDP でエージェントレスバックアップするスクリプトのサンプルを記載します。
ご使用の環境に応じ、変更してご利用ください。

```
# 以下 2 行目から 5 行目の変数（' '内）をご利用環境に応じて指定してください。
$PrivateOneSystem = '仮想アプライアンス名'
$UDPConsole ='UDP コンソールのホスト名'
$PasswordFilePath ='管理者パスワードが記載されたファイル'
$PlanName ='プラン名'

# バックアップ開始前に仮想アプライアンスをシャットダウンする。
Stop-VM -Name $PrivateOneSystem

# Arcserve UDP のエージェントレス バックアップを開始
cd 'C:¥Program Files¥arcserve¥Unified Data Protection¥Engine¥PowerCLI'
.¥UDPPowerCLI.ps1 -Command Backup -UDPConsoleServerName $UDPConsole -
UDPConsoleProtocol https -UDPConsolePort 8015 -UDPConsoleUserName administrator
-UDPConsolePasswordFile $PasswordFilePath -planName $PlanName -BackupJobType
Incr

# Arcserve UDP がスナップショットを取得するまで 300 秒待機。
Start-Sleep -Seconds 300

# 仮想アプライアンスを起動。
Start-VM -Name $PrivateOneSystem
```

## 7.4. VMware 環境での仮想アプライアンスの停止と起動スクリプトのサンプル

以下では、VMware 環境に展開された仮想アプライアンスを Arcserve UDP でエージェントレス バックアップするスクリプトのサンプルを記載します。ご使用の環境に応じ、変更してご利用ください。また、VMware PowerCLI はあらかじめスクリプトの実行環境にインストールしてください。

```
# 以下 2 行目から 6 行目の変数（' '内）をご利用環境に応じて指定してください。
$VMwareHost = 'ESXi ホスト名もしくは vCenter Server ホスト名'
$PrivateOneSystem = '仮想アプライアンス名'
$UDPConsole ='UDP コンソールのホスト名'
$PasswordFilePath ='管理者パスワードが記載されたファイル'
$PlanName ='プラン名'

# 仮想アプライアンスが実行する仮想ホストまたは vCenter サーバに接続
Connect-VIServer -Server $VMwareHost -force

# バックアップ開始前に仮想アプライアンスをシャットダウンする。
Shutdown-VMguest -VM $PrivateOneSystem -Confirm:$False

# Arcserve UDP のエージェントレス バックアップを開始
cd ‘C:¥Program Files¥arcserve¥Unified Data Protection¥Engine¥PowerCLI’
.¥UDPPowerCLI.ps1 -Command Backup -UDPConsoleServerName $UDPConsole -
UDPConsoleProtocol https -UDPConsolePort 8015 -UDPConsoleUserName administrator -
UDPConsolePasswordFile $PasswordFilePath -planName $PlanName -BackupJobType
Incr

# Arcserve UDP がスナップショットを取得するまで 300 秒待機。
Start-Sleep -Seconds 300

# 仮想アプライアンスを起動。
Start-VM -VM $PrivateOneSystem -Confirm:$False

# 仮想ホストまたは vCenter サーバへのアクセスを切断
Disconnect-VIServer -Server $VMwareHost  -Confirm:$False
```

仮想アプライアンスを実行する仮想ホストまたは vCenter サーバに接続する場合にユーザ名とパスワードが要求される場合は、以下のコマンドを最初に実行してログイン情報をあらかじめ設定しておきます。

New-VICredentialStoreItem -Host <ESXi ホスト or vCenter Server 名> -User <管理者アカウント> -Password <パスワード>

※ それぞれ“<>” 内を環境に合わせて入力します。

<参考>
上記 VMware PowerCLI 以外にスクリプトを使って VMware 仮想マシンを停止や起動させる手段として、vSphere の REST API を利用する方法もございます。
REST API の利用方法について VMware 社のドキュメント等を参照ください。

## 7.5. 仮想アプライアンスのリストア方法

**Step 1.** Arcserve UDP コンソールから[VM のリストア]をクリックします。

**Step 2.** リストア方式で [VM の復旧] を選択します。


**Step 3.** リストアのウィザードを進め、リストア対象の復旧ポイントの指定や各オプションを必要に応じて指定し、最後に [完了] をクリックしてリストアを実行します。

**Step 4.** リストア(VM の復旧)のジョブが正常終了したことを確認しましたら、仮想アプライアンスを起動(もしくはリストアのオプションで自動起動)し、プライベート OneSystem にログインして復旧を確認します。

“VM の復旧“ の正常終了イベント


# 8. OneXafe のシャットダウン

計画停電などで OneXafe のシャットダウンが必要となった場合、以下のいずれかの方法でシャットダウンが行えます。

## 8.1. OneXafe を直接操作する場合

OneXafe 筐体のフロント右上にある電源ボタン  を押下してシャットダウンを実行します。
Arcserve OneXafe は HDD に書き込む前のデータブロックはすべて不揮発性メモリに記録しているため、電源断でダーティ シャットダウンしたとしてもデータが失われることはありません。

## 8.2. iDRAC からシャットダウンする場合

iDRAC のダッシュボードページより、[正常なシャットダウン] を展開し、[システムの電源を切る] を選択します。

### 8.3. プライベート OneSystem からシャットダウンする場合

プライベート OneSystem の [OneXafe] の画面から [クラスター] を選択し、[クラスター名]から対象の OneXafe の ring を選択します。


[アクション] をクリックして[OneXafe のシャットダウン]を選択します。

## 9. 製品情報および FAQ はこちら

Arcserve シリーズ ポータルサイト
https://www.arcserve.com/jp/

Arcserve OneXafe 製品ドキュメント
https://support.arcserve.com/s/article/storagecraft-onexafe-user-guide?language=ja

Arcserve OneXafe 注意/制限事項
https://support.arcserve.com/s/article/OneXafe-Notice?language=ja

Arcserve OneXafe よくある質問と回答
https://support.arcserve.com/s/article/OneXafe-FAQ?language=ja

Arcserve UDP 動作要件、注意/制限事項
https://support.arcserve.com/s/topic/0TO1R000001MGBkWAO/arcserve-udp-compatibility-matrix?language=ja

Arcserve UDP 製品ドキュメント（マニュアル）
https://support.arcserve.com/s/topic/0TO1R000001MGBiWAO/arcserve-udp-documentation?language=ja

Arcserve UDP サポート / FAQ
https://support.arcserve.com/s/article/205002865?language=ja

以上