

Arcserve UDP & Arcserve OneXafe 連携ガイド

(パブリック OneSystem 編)

1. はじめに	1
2. OneXafe の用語と構成要素	2
2.1. 用語	2
2.2. 構成	3
3. OneXafe とパブリック OneSystem の初期設定	4
3.1. パブリック OneSystem の要件.....	4
3.2. 適用手順の概要	4
3.3. OneXafe の設置と iDRAC のパスワード設定.....	5
3.4. OneXafe 単一ノードクラスタの設定	8
3.5. OneXafe の IP アドレスを設定	11
3.6. パブリック OneSystem の初期設定	16
3.7. パブリック OneSystem への OneXafe の登録	18
3.8. OneSystem 管理者アカウントに対する 2 要素認証の有効化	22
4. OneXafe での SMB 共有の設定	23
4.1. OneSystem アカウントの作成.....	23
4.2. SMB 共有の作成	27
5. Arcserve UDP によるバックアップデータの二次複製	32
5.1. OneXafe を使った RPS データストアの作成	33
5.2. OneXafe への復旧ポイントのレプリケート	35
6. ランサムウェア攻撃からの復旧	37
6.1. 適切なスナップショットの特定	37
6.2. 復旧に必要な認証情報	38
6.3. OneXafe スナップショットを新しい共有に反映する	39



6.4.	Arcserve UDP デデュープリケーション データストアのインポート	41
6.5.	既知の制限事項	45
7.	製品情報および FAQ はこちら	46

改定履歴

2022 年 6 月	Rev 1.0 リリース (前提ソフトウェア : Arcserve UDP 8.1 & OneXafe 4.0.0)
2022 年 6 月	Rev 1.1 リリース OneSystem 2 要素認証の有効化手順追加および画面ショット変更
2022 年 9 月	Rev 1.2 リリース OneXafe のネットワーク設定に関する追記など
2022 年 9 月	Rev 1.3 リリース iDRAC ポートの IP アドレス設定手順などを追記
2023 年 5 月	Rev 1.4 リリース 5 章 1 節の記述変更
2024 年 1 月	Rev 1.5 リリース 複数ノードクラスタに関する記述の修正
2024 年 4 月	Rev 1.6 リリース P.15 画面ショットの誤表記の修正



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。

本ガイドではパブリック 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

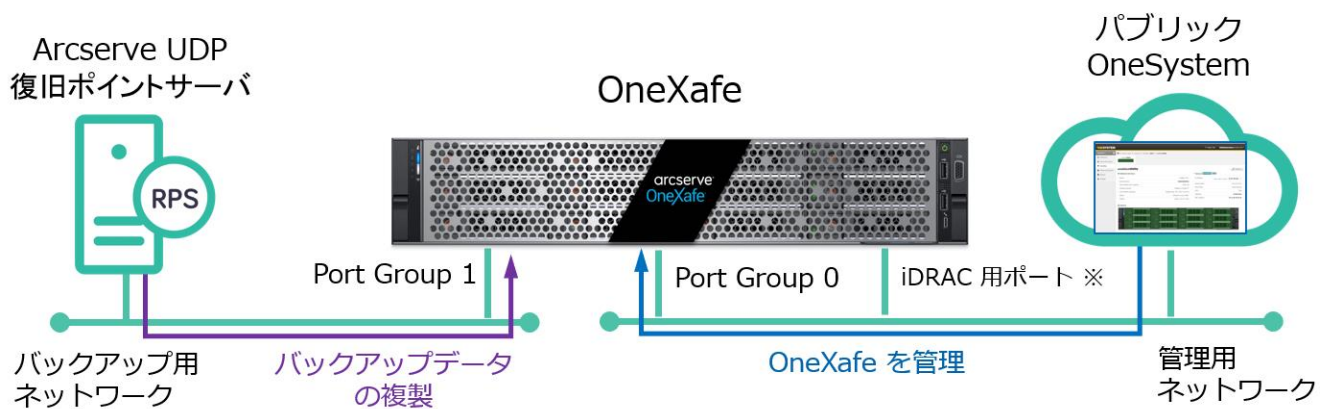
OneXafe の旧開発元/販売元です。2021 年に Arcserve と合併しました。

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。
- ・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 を管理するためのパブリック OneSystem を利用します。

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 とパブリック OneSystem の初期設定

本章では OneXafe とパブリック OneSystem の初期設定方法を解説します。

3.1. パブリック OneSystem の要件

- ・パブリック OneSystem はクラウド上の無償のサービスで、導入や構築などの作業は不要です。
- ・パブリック OneSystem に登録するアカウントとして、インターネット上で利用できる電子メール アドレスが必要です。
- ・OneXafe をパブリック OneSystem が管理できるようにするため、OneXafe の “Port Group 0” のネットワークがインターネットにアクセス出来ることが必要です。
“Port Group 1” のネットワークと iDRAC 用ポートは、インターネットへの接続は特に必要ありません。
- ・OneXafe は TCP/443 (Outbound) ポートを使い、パブリック OneSystem 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 ユーザ ガイド - OneSystem と OneXafe の通信で有効にする必要がある特定のファイアウォール設定

https://documentation.arcserve.com/Arcserve-OneXafe/Available/JPN/OX_UG/Default.htm#Firewall_Settings_OneSystem_OneXafe_communication.htm

3.2. 適用手順の概要

以下、パブリック OneSystem を使用して OneXafe を導入いただく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。

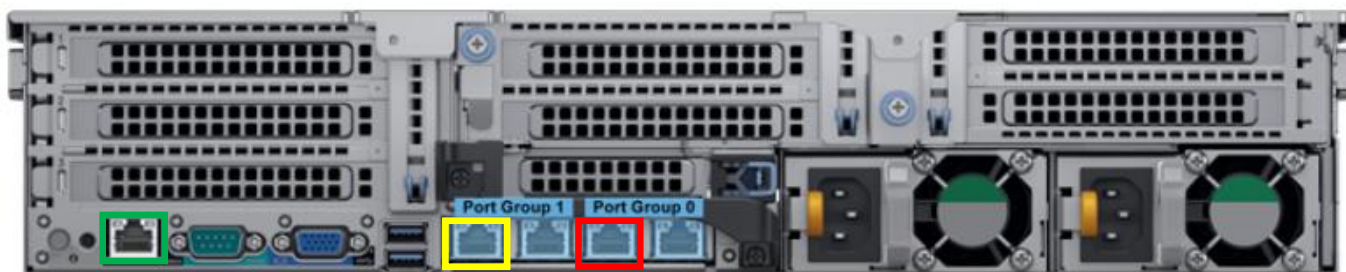
1. OneXafe を設置し、ケーブル等を接続します。
2. (iDRAC を使用する場合) iDRAC の管理者アカウントのパスワードを変更します。
3. OneXafe Web コンソールにアクセスし、クラスタを設定します。
4. OneXafe Web コンソールで IP アドレスを設定します。
5. パブリック OneSystem にアクセスし、メール アドレスを使用してユーザ アカウントを登録します。
6. OneXafe Web コンソール にアクセスし、パブリック OneSystem に登録します。
7. パブリック OneSystem コンソールで OneXafe を ring に登録し、使い始めるための設定を行います。



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。

```
Version: OneBlox Grenache version 4.0 build 47
Hostname: oneblox43651.local < OneXafe の IP アドレス >

IPMI/iDRAC:
  IP Address Source      : DHCP Address
  IP Address             : < iDRAC の IP アドレス >
  Subnet Mask            : 255.255.255.0
  MAC Address            : b0:7b:25:d8:e7:36

oneblox43651 login:
```

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. iDRAC の管理者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。

Integrated Remote Access Controller 9
idrac-BL14WM3 | Arcserve OneXafe | Enterprise

ユーザー名とパスワードを入力し、ログインをクリックします。

ユーザー名: admin

パスワード: [masked]

ドメイン: このiDRAC

🔒 セキュリティ上の注意: By accessing this computer, you confirm that such access complies with your organization's security policy.

ログイン

OneXafe

[ヘルプ](#) | [サポート](#) | [システム情報](#)

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

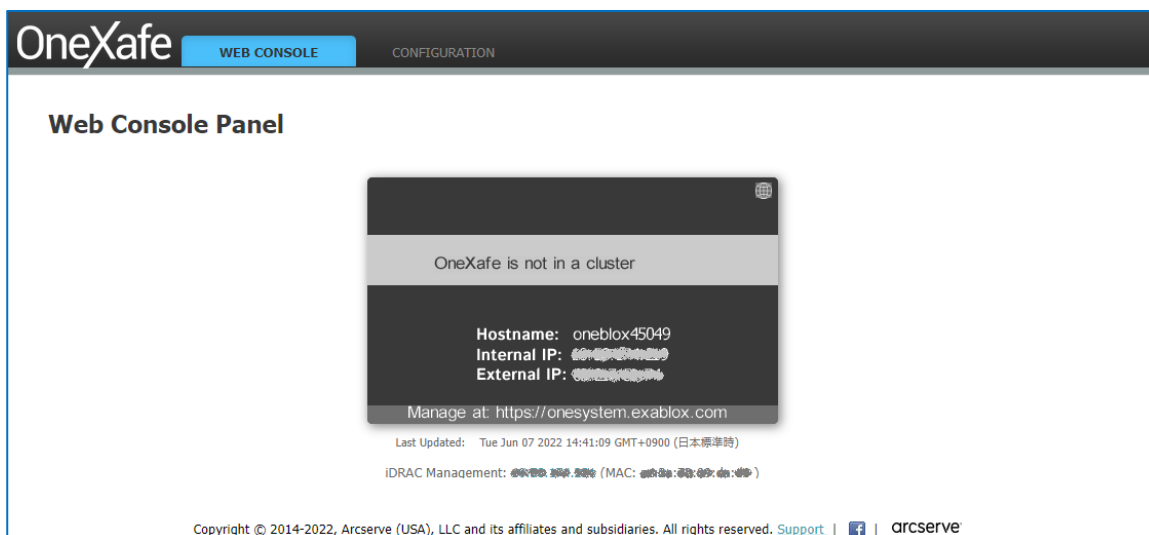
<https://www.arcserve.com/sites/default/files/2023-10/OneXafe-Multi-Node-Cluster-Guide.pdf>

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。

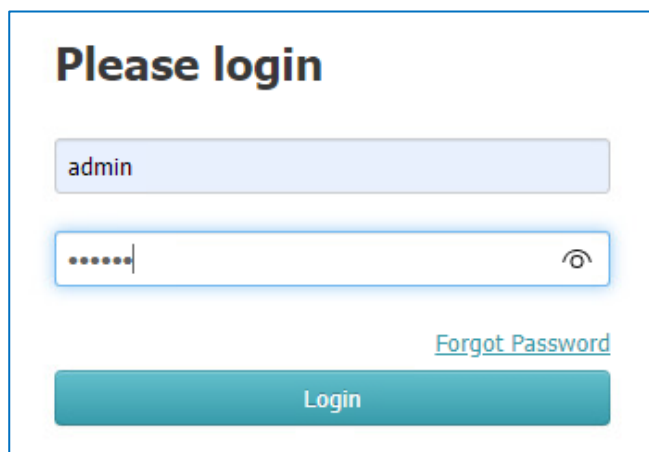
例 : <http://192.168.x.x>

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が、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。

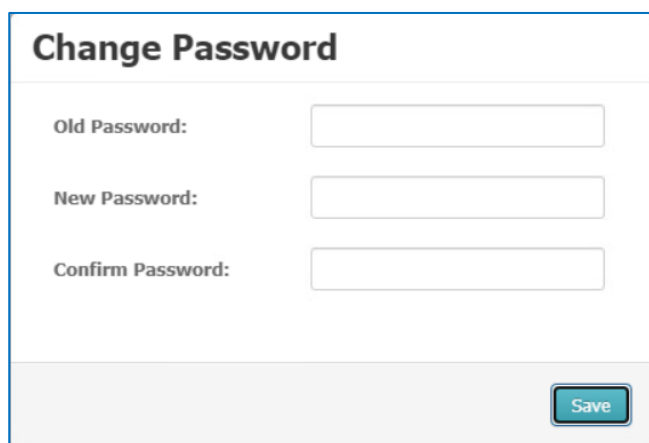


Step 3. デフォルト ユーザ名 "admin" とデフォルト パスワード "config" を入力します。



The screenshot shows a login interface with the heading "Please login". It contains a text input field with "admin" entered, a password input field with masked characters and a visibility icon, a "Forgot Password" link, and a teal "Login" button.

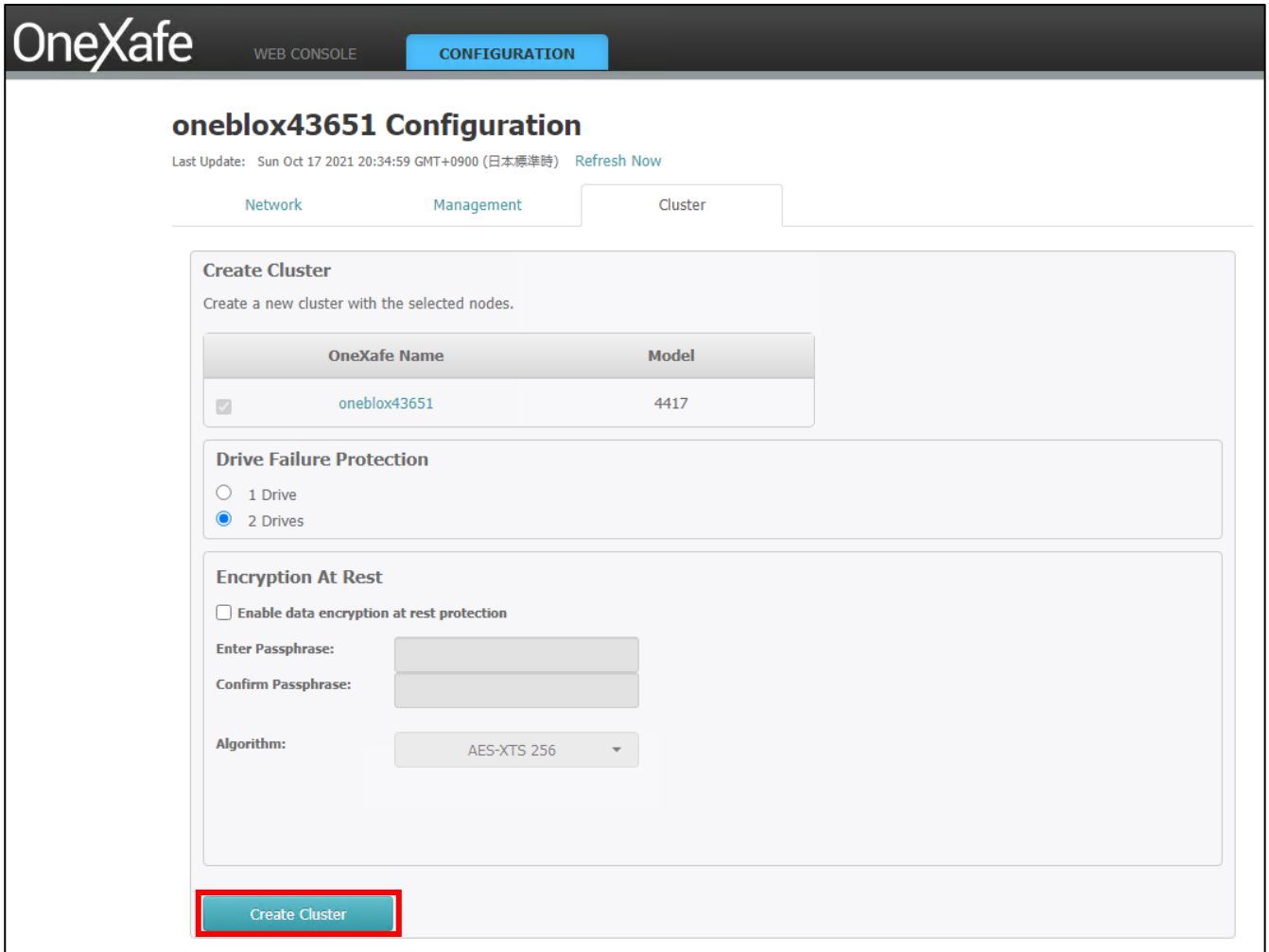
Step 4. パスワードの変更を求められるので、安全なパスワードを入力します。



The screenshot shows a "Change Password" form. It has three input fields labeled "Old Password:", "New Password:", and "Confirm Password:". A teal "Save" button is located at the bottom right of the form.

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。

- OneXafe ノードを選択します。
- [Drive Failure Protection] ではデフォルトの“2 Drives”を選択します。
- [Enable data encryption at rest protection] チェックボックスは無効のままにします。
- [Create Cluster] ボタンをクリックします。



The screenshot shows the OneXafe WEB CONSOLE CONFIGURATION page for 'oneblox43651'. The 'Cluster' tab is active. The 'Create Cluster' section is highlighted with a red box. It contains a table with the following data:

OneXafe Name	Model
<input checked="" type="checkbox"/> oneblox43651	4417

Below the table, the 'Drive Failure Protection' section has '2 Drives' selected. The 'Encryption At Rest' section has 'Enable data encryption at rest protection' unchecked, and the 'Algorithm' dropdown is set to 'AES-XTS 256'. The 'Create Cluster' button is highlighted with a red box.

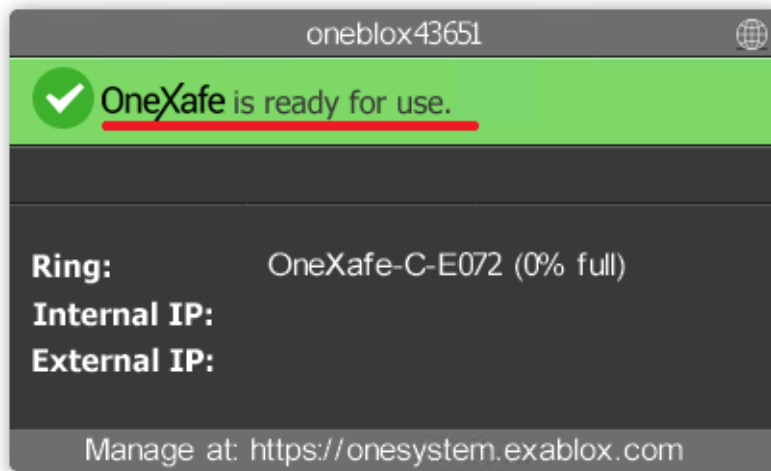
Step 6. [Yes, Create Cluster] をクリックすると、以下のメッセージが表示され、クラスタの作成が始まります。

⚙️ Waiting for drives to come online ...

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、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、[WEB CONSOLE] タブのステータスが更新されて緑色の画面が表示されると、OneXafe が使用できる状態となります。



3.5. OneXafe の IP アドレスを設定

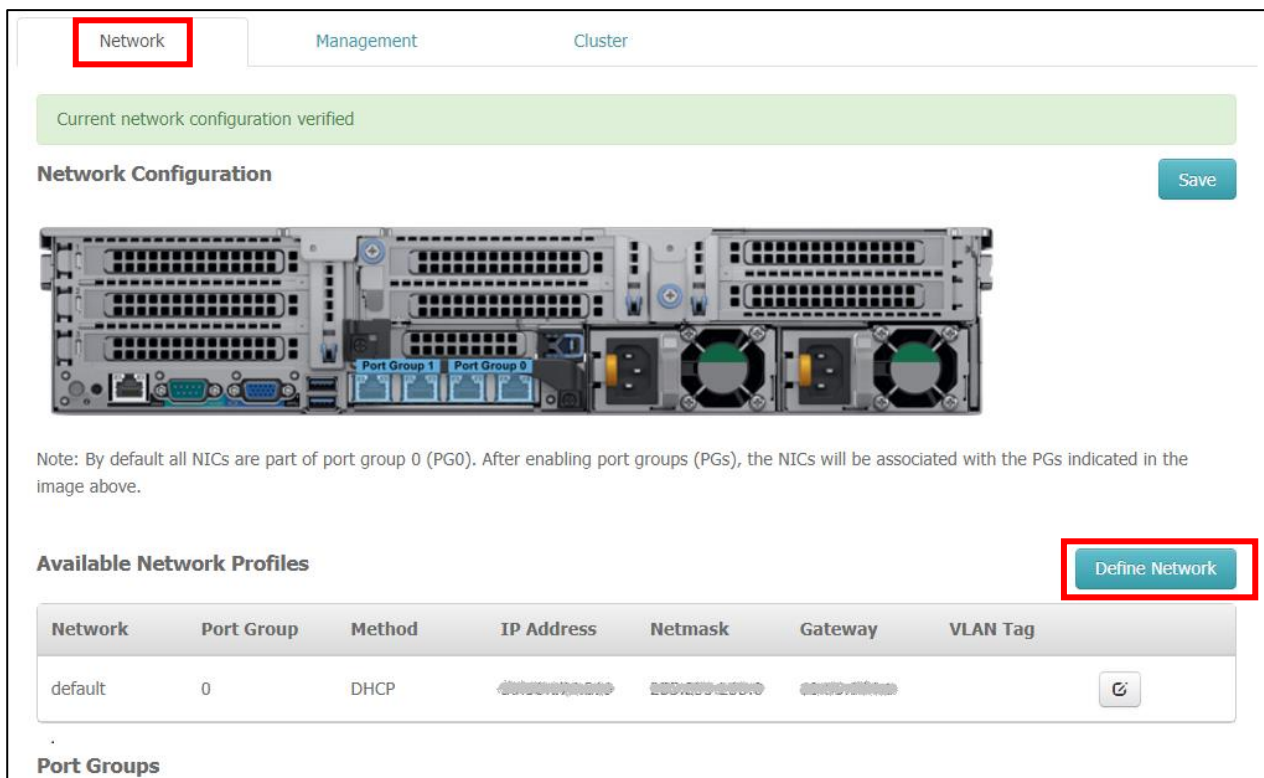
OneXafe の 各 Port Group に IP アドレスを設定します。

本ガイドの設定では、パブリック 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。

本ガイドではパブリック 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. まず、“Port Group 1” を定義します。[CONFIGURATION] から [Network] タブを開き [Define Network] をクリックします。



Current network configuration verified

Network Configuration Save

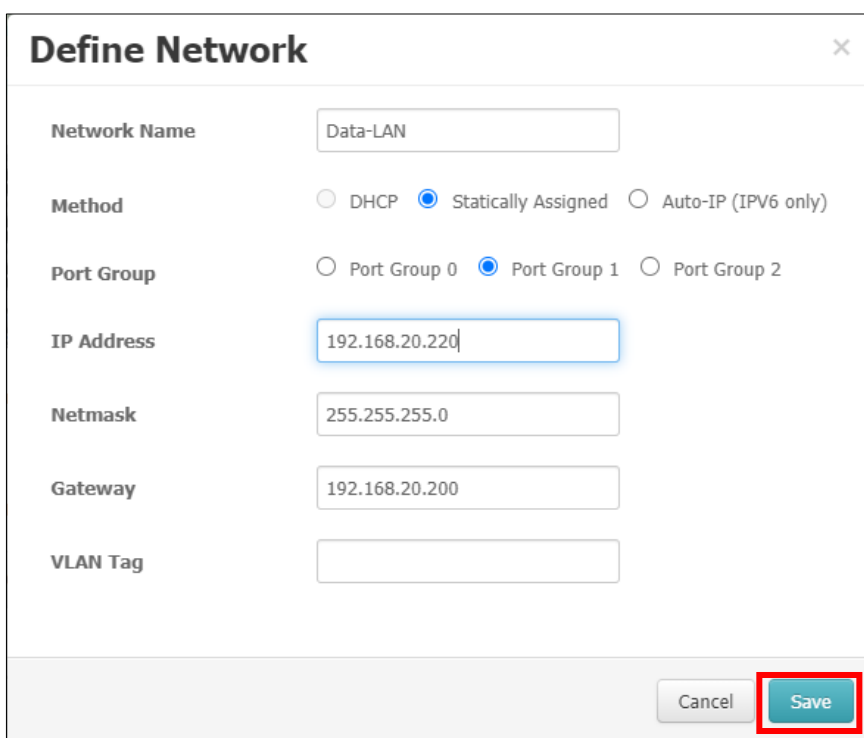
Note: By default all NICs are part of port group 0 (PG0). After enabling port groups (PGs), the NICs will be associated with the PGs indicated in the image above.

Available Network Profiles Define Network

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
default	0	DHCP	192.168.20.220	255.255.255.0	192.168.20.200	

Port Groups

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。



Define Network ×

Network Name

Method DHCP Statically Assigned Auto-IP (IPV6 only)

Port Group Port Group 0 Port Group 1 Port Group 2

IP Address

Netmask

Gateway

VLAN Tag

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。

Network Configuration

Save

Note: By default all NICs are part of port group 0 (PG0). After enabling port groups (PGs), the NICs will be associated with the PGs indicated in the image above.

Available Network Profiles

Network	Port Group	Method	IP Address	Netmask	Gateway	VLAN Tag
Data-LAN	1	Static	192.168.20.220	255.255.255.0	192.168.20.200	[Edit] [Delete]
default	0	Static	[Redacted]	[Redacted]	[Redacted]	[Edit]

Define Network

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。1 GbE で十分です。
- ・DHCP もしくは、静的 IP アドレスを設定します。
- ・Maximum Transmission Unit(MTU) の値は変更する必要はありません。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 を選択頂けます。
- ・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。

Port Groups

Port Group 0 Port Group 1

Enable Port Group for network traffic

MAC Addresses:
Determined after this configuration is saved...

Active MAC:

Configured Networks:
Data-LAN: 192.168.20.220

Bond Mode

Configure which mode is used when aggregating multiple network interfaces into a bonded interface. Please verify your ethernet switch(es) support the selected mode.

Active-Backup (active-backup) ?

Link Aggregation Control Protocol (LACP) ?

Round-robin policy (RR) ?

XOR source and destination MAC address (XOR) ?

Maximum Transmission Unit

Configure the ethernet frame size.

Standard Frame Size (MTU 1500)

Jumbo Frame Size (MTU 9000) ?

Custom Frame Size ?

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。

重要：パブリック OneSystem と通信するため、必ず外部の DNS サーバ（例：“8.8.8.8” など）を指定してください。

“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。



Network Settings	
<p>Proxy Server Configure the secure web proxy (if needed)</p> <p>Web Proxy Server: <input type="text"/></p> <p>Port: <input type="text"/></p>	
<p>NTP Servers Add additional NTP servers used to keep time. If using Active Directory, the NTP servers should be the same used by AD.</p> <p>NTP Server 1: <input type="text" value="0.pool.ntp.org"/></p> <p>NTP Server 2: <input type="text" value="1.pool.ntp.org"/></p> <p>NTP Server 3: <input type="text" value="2.pool.ntp.org"/></p> <p>NTP Server 4: <input type="text" value="3.pool.ntp.org"/></p>	
<p>DNS Servers Add DNS servers configured for networks used by port group.</p> <p>DNS Server 1: <input type="text" value="8.8.8.8"/></p> <p>DNS Server 2: <input type="text" value="8.8.4.4"/></p> <p>DNS Server 3: <input type="text" value="4.2.2.2"/></p>	

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。

```
Version: OneBlox Grenache version 4.0 build 47
Hostname: oneblox43651.local 192.168.20.220

IPMI/iDRAC:
  IP Address Source      : DHCP Address
  IP Address             : < iDRAC の IP アドレス >
  Subnet Mask            : 255.255.255.0
  MAC Address            : 00:00:00:00:00:00

oneblox43651 login: admin
Password:
oneblox43651(config) network
oneblox43651(config-network) list
  Name      Family  Method  Address          Netmask          Gateway          Vlan  Portgroup
default    inet    dhcp    < Port Group 0 の IP アドレス > 255.255.255.0    < Gateway の IP アドレス > 0
Data-LAN   inet    static  192.168.20.220  255.255.255.0    192.168.20.200  None  1
oneblox43651(config-network) _
```

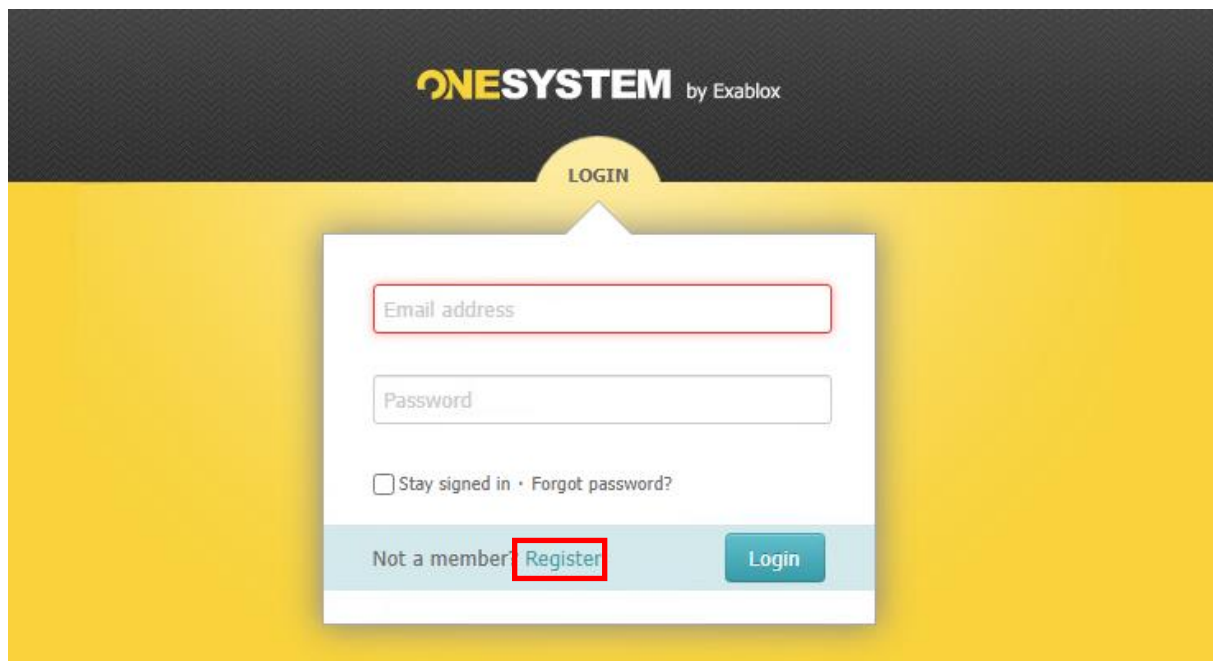


3.6. パブリック OneSystem の初期設定

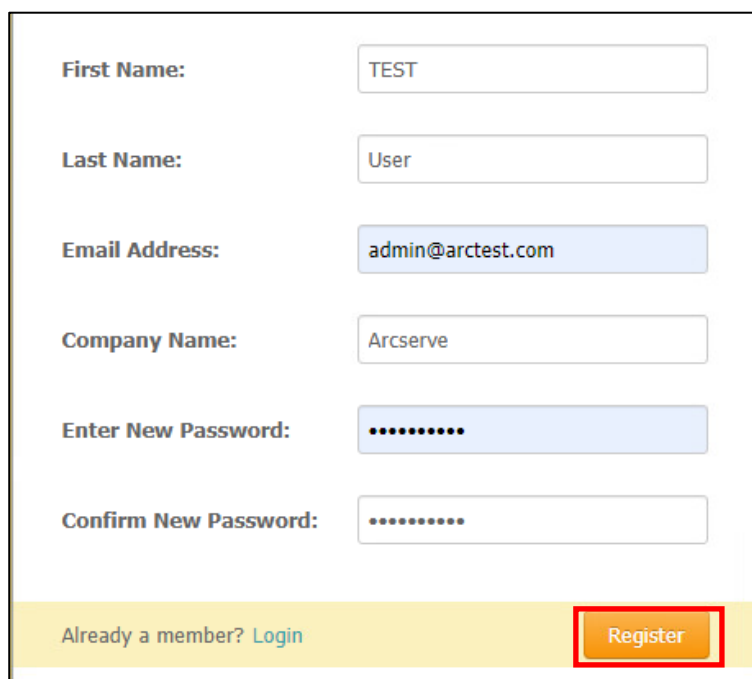
以下の手順に従い、パブリック OneSystem を設定します。

Step 1. Web ブラウザに以下の URL を入力し、パブリック OneSystem にアクセスします。

<https://onesystem.exablox.com>



Step 2. パブリック OneSystem の LOGIN 画面で [register] をクリックし、新しい OneSystem サービスとユーザを作成します。



Step 3. “Welcome to OneSystem by StorageCraft!” という件名のメールが登録したメール アカウントに届きます。メールが届いたら本文中にある URL をクリックします。もし 10 分経過しても届かない場合はスパム フォルダを確認してください。

Hello TEST User,

Thank you for registering an account with OneSystem. To activate your account, please click here:

<http://onesystem1032.arctest.com/account/activate/611515bd540783b9c5e1796f61a89d1cd7de17b8>

Thanks,

OneSystem by StorageCraft

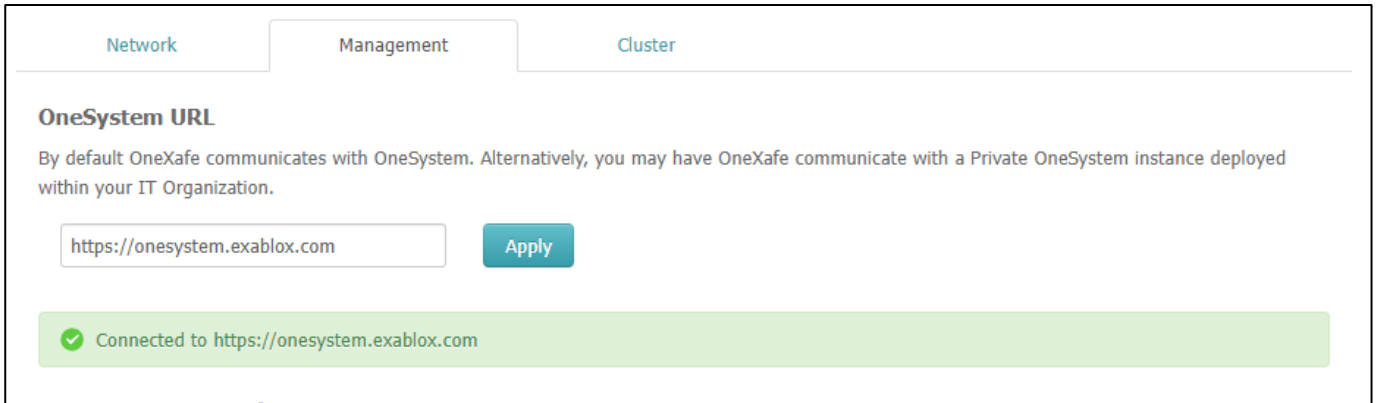
URL をクリックすると、OneSystem の画面が表示されてユーザ アカウントの登録は終了です。



3.7. パブリック OneSystem への OneXafe の登録

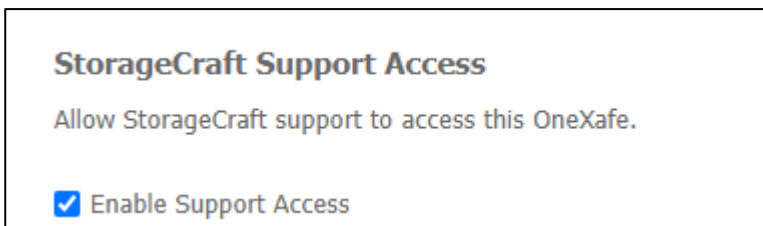
本節では、OneXafe をパブリック OneSystem から管理できるように登録します。

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] 以下にパブリック 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）



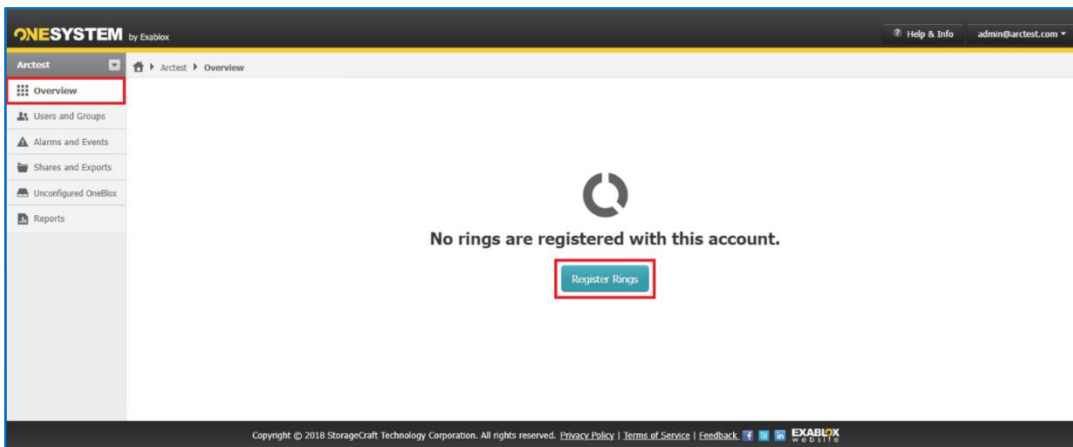
The screenshot shows the 'Management' tab selected in the OneXafe Web console. Under the heading 'OneSystem URL', there is a text input field containing 'https://onesystem.exablox.com' and an 'Apply' button. Below the input field, a green confirmation message reads: 'Connected to https://onesystem.exablox.com'.

Step 2. StorageCraft Support access (Arcserve によるリモートアクセス) を有効にするチェックボックスは、本番環境ではこの機能を有効にすることを強くお勧めしています。

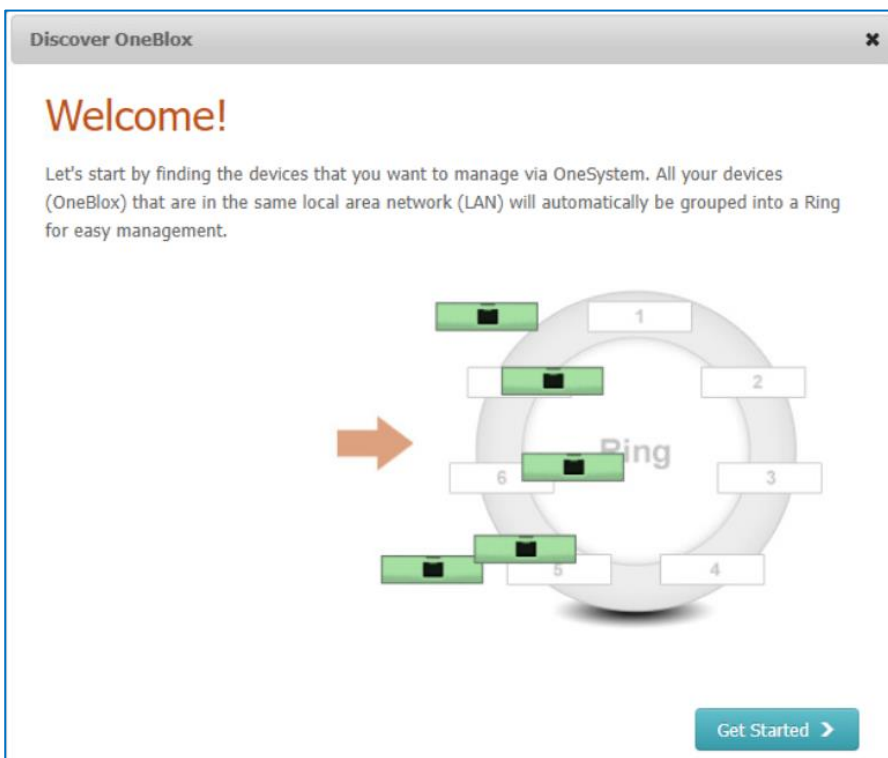


The screenshot shows the 'StorageCraft Support Access' section. It includes the text 'Allow StorageCraft support to access this OneXafe.' and a checked checkbox labeled 'Enable Support Access'.

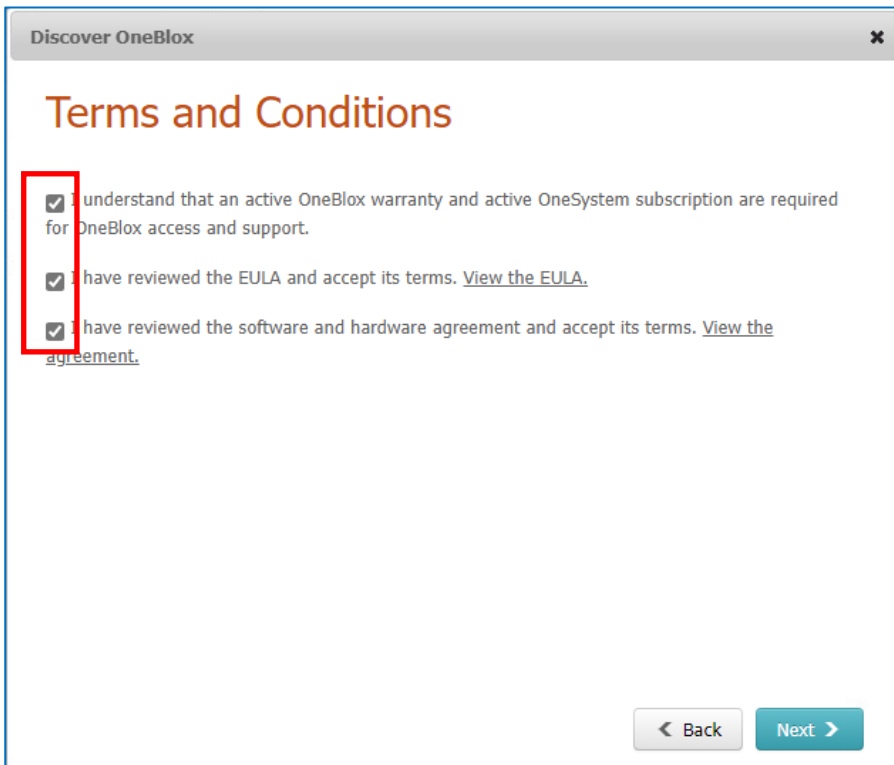
Step 3. 再度パブリック OneSystem にログインし、Ring を登録します。[Overview] – [Register Rings] をクリックします。



Step 4. ウィザードが始まります。[Get Started] をクリックします。



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



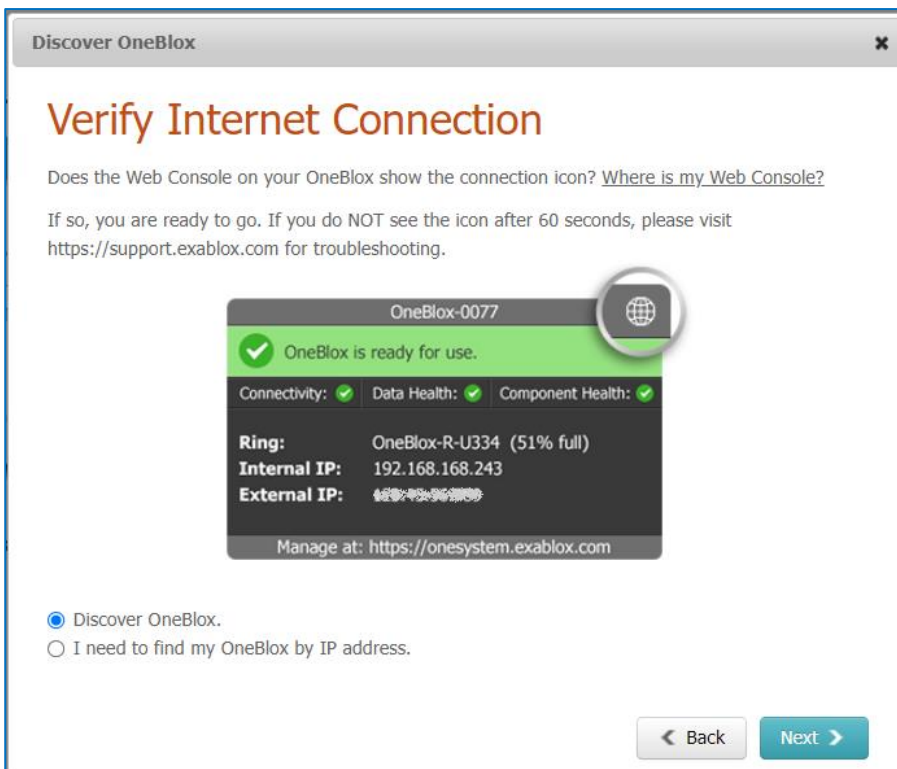
Discover OneBlox

Terms and Conditions

- I understand that an active OneBlox warranty and active OneSystem subscription are required for OneBlox access and support.
- I have reviewed the EULA and accept its terms. [View the EULA.](#)
- I have reviewed the software and hardware agreement and accept its terms. [View the agreement.](#)

< Back Next >

Step 6. [Next] をクリックし、OneXafe を検出します。



Discover OneBlox

Verify Internet Connection

Does the Web Console on your OneBlox show the connection icon? [Where is my Web Console?](#)

If so, you are ready to go. If you do NOT see the icon after 60 seconds, please visit <https://support.exablox.com> for troubleshooting.

OneBlox-0077

OneBlox is ready for use.

Connectivity: Data Health: Component Health:

Ring: OneBlox-R-U334 (51% full)

Internal IP: 192.168.168.243

External IP: 192.168.168.243

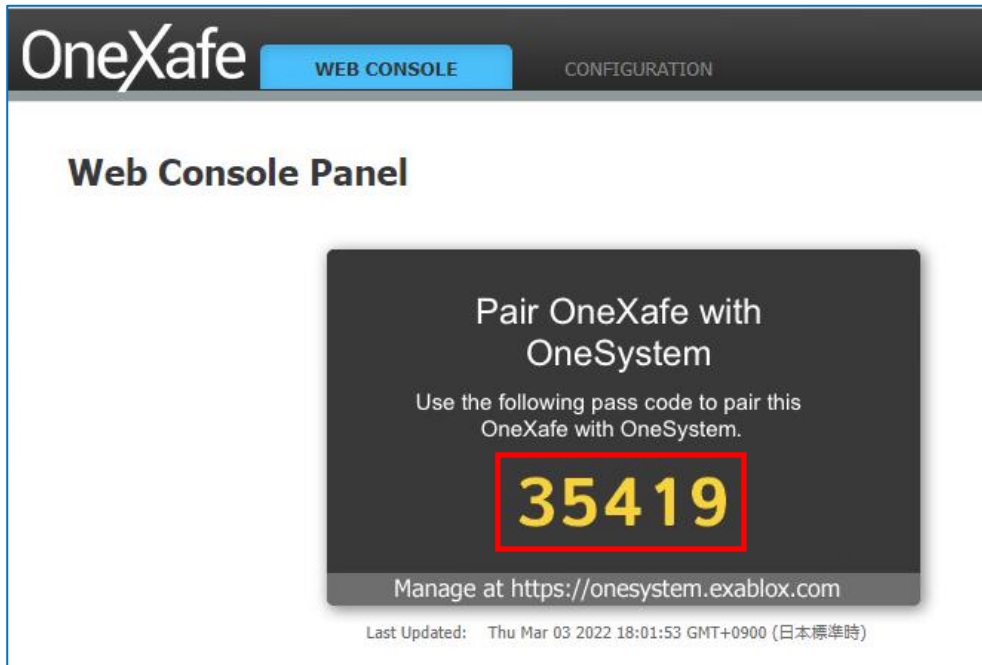
Manage at: <https://onesystem.exablox.com>

Discover OneBlox.
 I need to find my OneBlox by IP address.

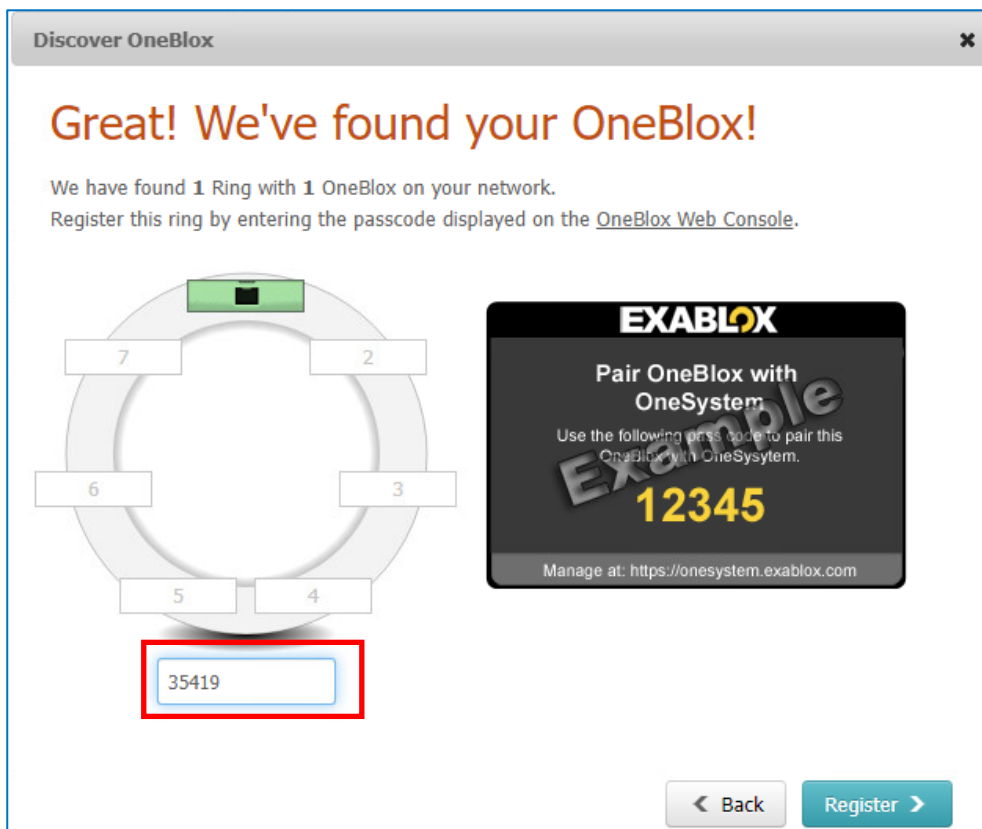
< Back Next >

Step 7. OneXafe が検出でき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 1 つ目の画面のように、数字 5 桁のパスコードが表示されています。

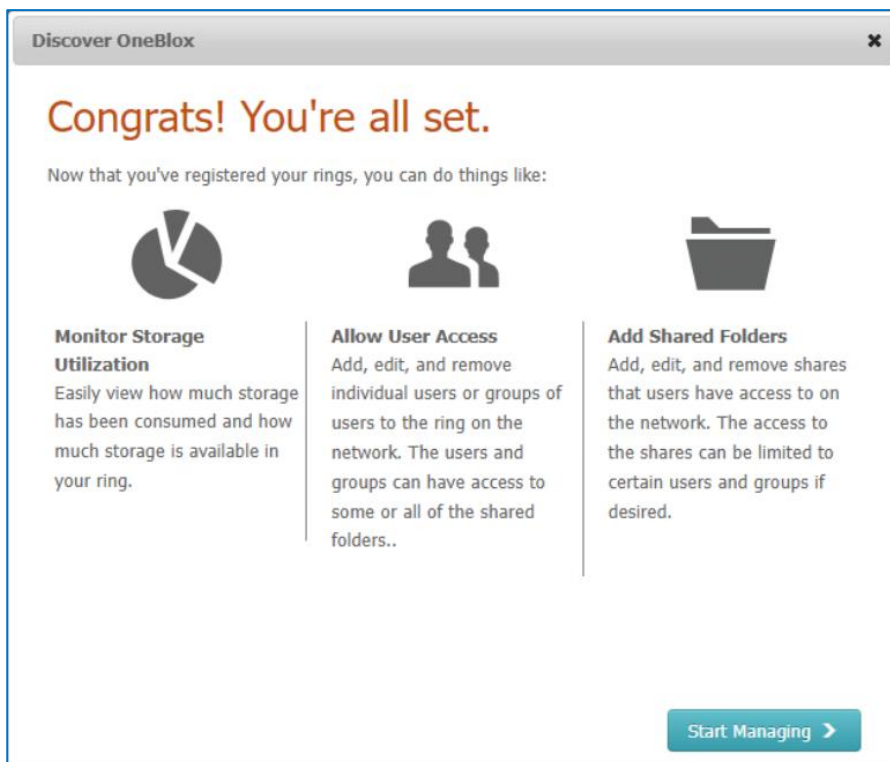
(画面のパスコードはサンプルです。実際のパスコードは設定ごとに異なります)



パスコードを入力し、[Register] をクリックします。



Step 8. 登録できると、以下の画面が表示されます。[Start Managing] をクリックするとパブリック OneSystem 上で、登録した OneXafe を管理できるようになります。



3.8. 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 ユーザ ガイド - 2 要素検証を有効にしてセキュリティを強化する方法

https://documentation.arcserve.com/Arcserve-OneXafe/Available/JPN/OX_UG/Default.htm#How%20do%20I%20enable%20two-factor%20Verification%20for%20additional%20security.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. OneSystem 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。

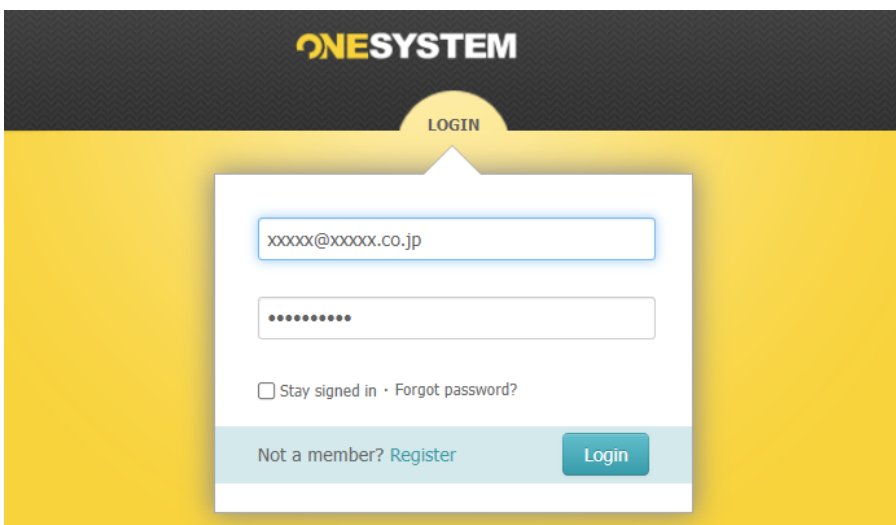
Note: OneSystem を Active Directory (AD) と連携させると、組織内のすべての AD ユーザに共有フォルダへの読み取り/書き込みアクセス権が付与されます。

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. OneXafe を管理するパブリック OneSystem にログインします。入力するアカウント名/パスワードは、前章 [3.6. パブリック OneSystem の初期設定] で登録したパブリック OneSystem の管理者アカウントのものを 사용합니다。



Step 2. Overview page で対象の OneXafe に該当する ring をクリックします。選択された ring の Dashboard page が表示されます。

ONESYSTEM by Exablos

OneXafe-C-N516

Dashboard

Users and Groups

OneBlox

Shares and Exports

Reports

Settings

OneXafe-C-N516

CAPACITY UTILIZATION

Used Capacity:	268.4 MB (<0.1%)
Available Capacity:	190.7 TB (97.0%)
Free Capacity:	196.6 TB (100.0%)
Raw Capacity:	196.6 TB
Cluster State:	Healthy
Encryption Status:	Disabled

DATA REDUCTION

Data Received:	0.0 MB
Compression Savings:	0.0 MB
Deduplication Savings:	0.0 MB
Data Written:	0.0 MB
Total Reduction Ratio:	--

Today | Lifetime

LATEST ACTIVE ALARMS & EVENTS
- No active alarms. -

Step 3. [User and Groups] をクリックし、[Add User] をクリックします。

Dashboard

Users and Groups

OneBlox

Shares and Exports

Reports

Settings

Users and Groups

Users	Groups
Add User	New User

Search Users

First name:

Step 4. [First name]、[Last name]、[Email address] を入力します。[Role] が “User” になっていることを確認し、[Save] ボタンをクリックします。

New User ✕ Cancel Save

First name:

Last name:

Email address:

Role:

User

Admin

Delegated Admin
Use this role for an admin that is not in your organization but will manage your rings. ?

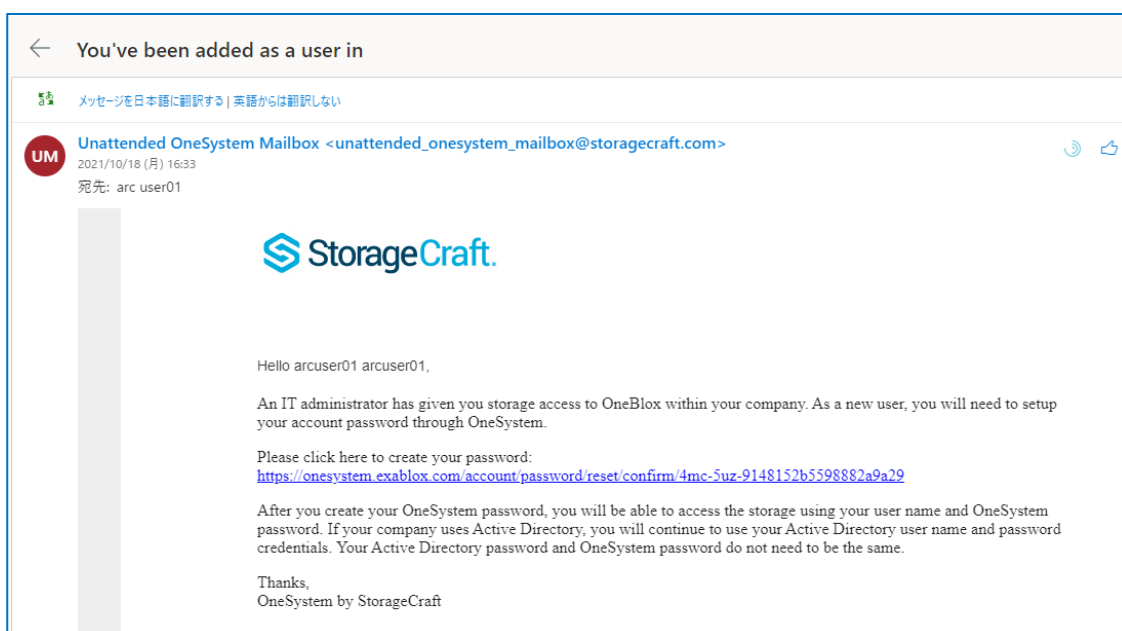
Group Member of: Add new Group

Users

Share Access: Select or type a share...

Share Name ^	Ring	Access By	Permission	
Public	OneXafe-C-E072	Anyone	Read/Write	🔒 ...

Step 5. Step4 で登録したメールアドレスに “You’ve been added as a user …” という題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、パブリック OneSystem にアクセスします。



Step 6. 新しいパスワードを入力して、この章で作成した新しいユーザ アカウントで OneSystem にログインします。

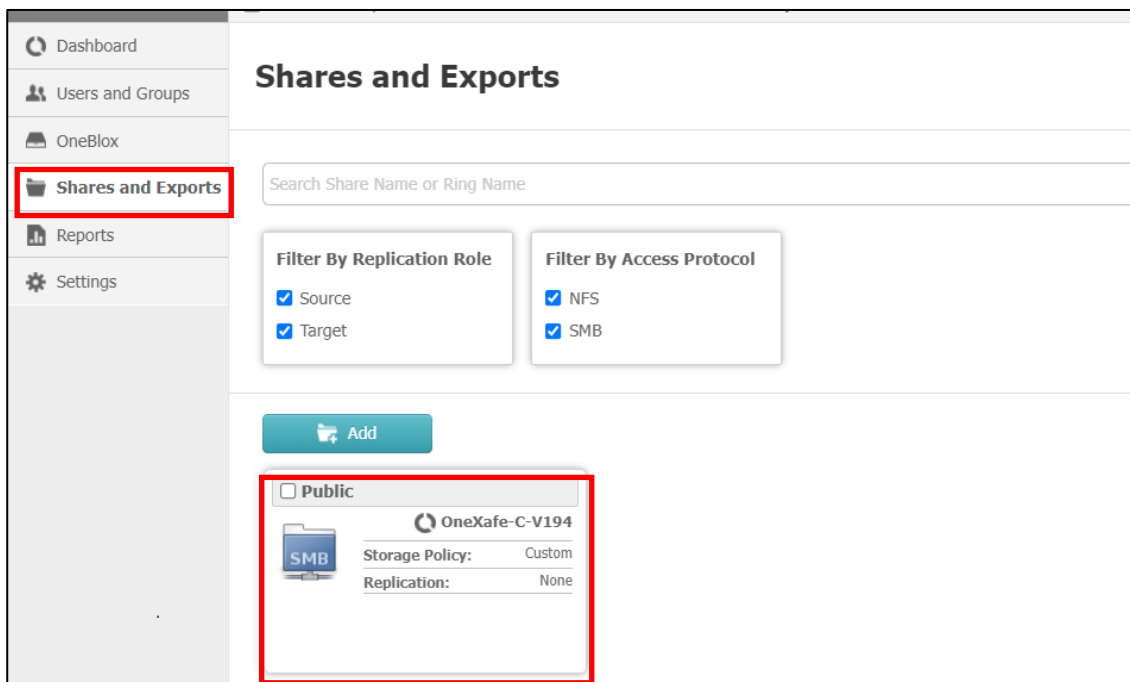
The image shows a screenshot of the OneSystem web interface. At the top, the 'ONESYSTEM' logo is displayed in white on a dark background. Below the logo, the word 'PASSWORD' is written in a yellow semi-circle. The main content area is a white box with a yellow border, titled 'Create New Password'. It contains two input fields for passwords, both filled with dots. The second field has a blue border and a cursor. At the bottom of the white box is a teal button labeled 'Create New Password'.

作成した OneSystem アカウントの [Role] が “User” の場合、OneSystem コンソールではパスワード変更しか出来ません。OneXafe の管理やユーザ登録、SMB 共有の作成は、管理者アカウント ([Role] が “admin”) をご利用ください。

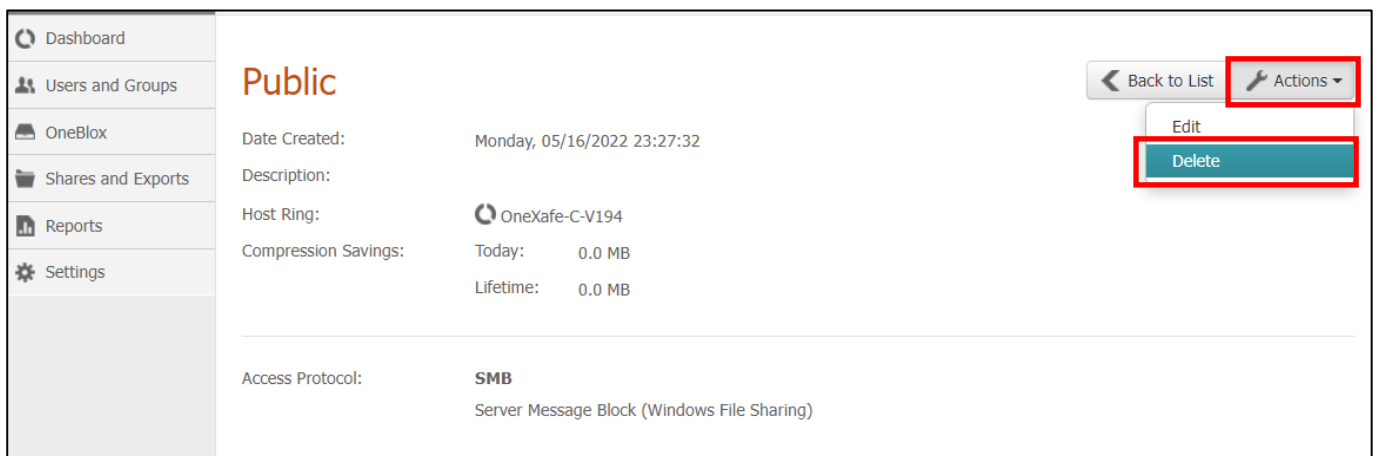
4.2. SMB 共有の作成

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。改めて、管理者アカウントで OneSystem にログインします。

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 (Anyone) で設定されているため、削除しておきます。OneSystem コンソールの [Shares and Exports] をクリックし、デフォルトで作成されている SMB 共有の "Public" をクリックします。

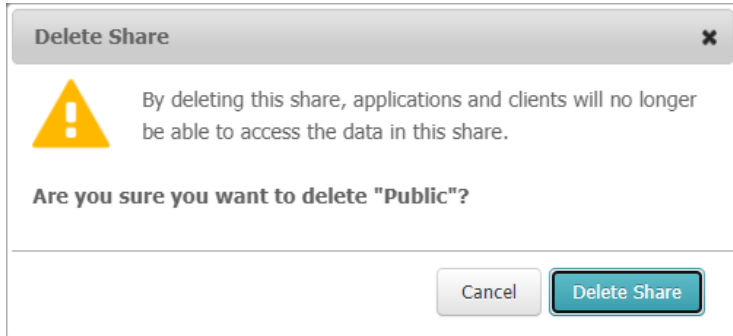


Step 2. 右上の [Action] メニューから [Delete] をクリックします。



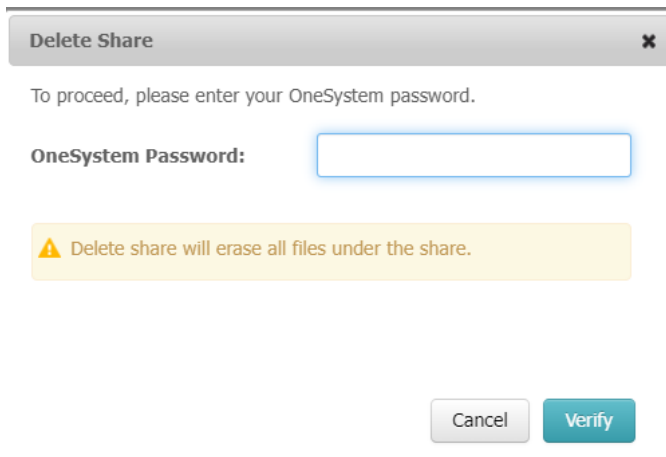
Step 3. 削除の確認メッセージで [Delete Share] をクリックし、OneSystem の管理者パスワードを入力して “Public” を削除します。

<削除の確認画面>



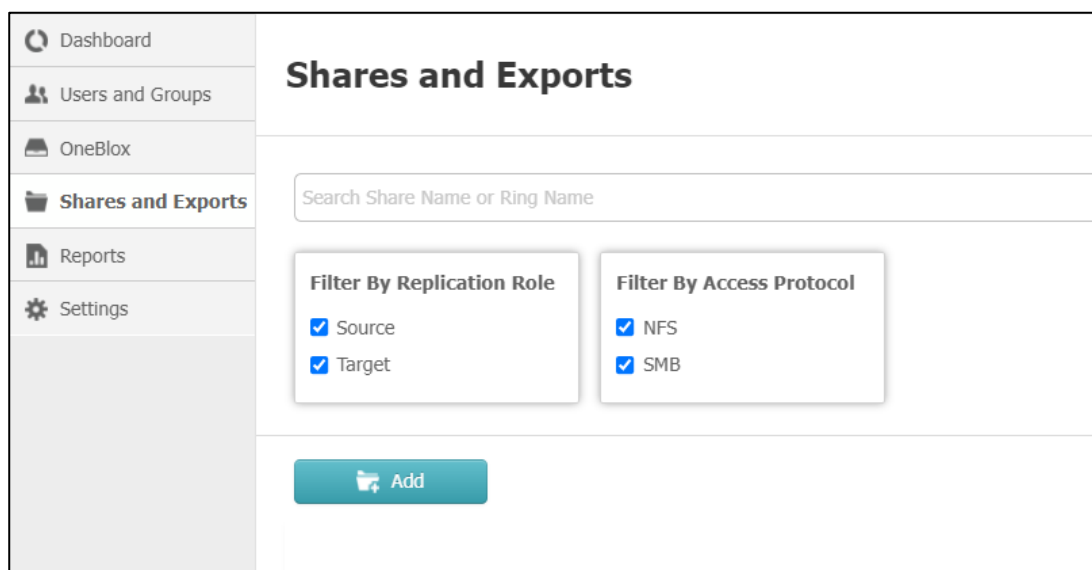
The dialog box titled "Delete Share" contains a yellow warning triangle icon. The text reads: "By deleting this share, applications and clients will no longer be able to access the data in this share." Below this, it asks "Are you sure you want to delete 'Public'?" At the bottom right, there are two buttons: "Cancel" and "Delete Share".

<パスワード入力画面>



The dialog box titled "Delete Share" contains the text: "To proceed, please enter your OneSystem password." Below this is a text input field labeled "OneSystem Password:". A yellow warning banner below the input field states: "Delete share will erase all files under the share." At the bottom right, there are two buttons: "Cancel" and "Verify".

Step 4. 続いて新規に SMB 共有を作成するため、[Shares and Exports] の [Add] ボタンをクリックします。



The interface shows a sidebar with navigation options: Dashboard, Users and Groups, OneBlox, Shares and Exports (selected), Reports, and Settings. The main content area is titled "Shares and Exports" and includes a search bar for "Share Name or Ring Name". There are two filter boxes: "Filter By Replication Role" with checkboxes for "Source" and "Target" (both checked), and "Filter By Access Protocol" with checkboxes for "NFS" and "SMB" (both checked). At the bottom, there is a blue "Add" button with a folder icon.

Step 5. [New Share/Export] 画面で [Name] 欄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 [Host Ring] 欄のドロップダウン リストから、前章で登録した Ring を選択します。



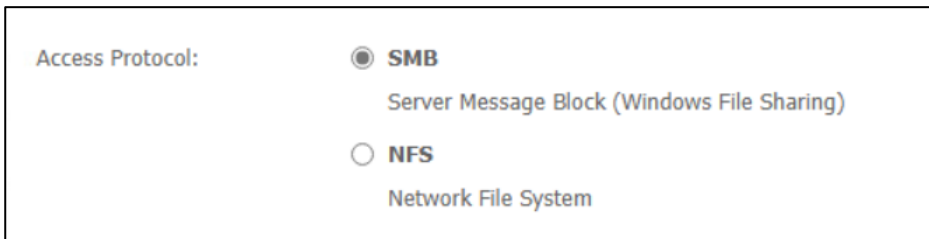
New Share/Export Cancel Save

Name:

Description:

Host Ring:

Step 6. [Access Protocol] として “SMB” を選択します。

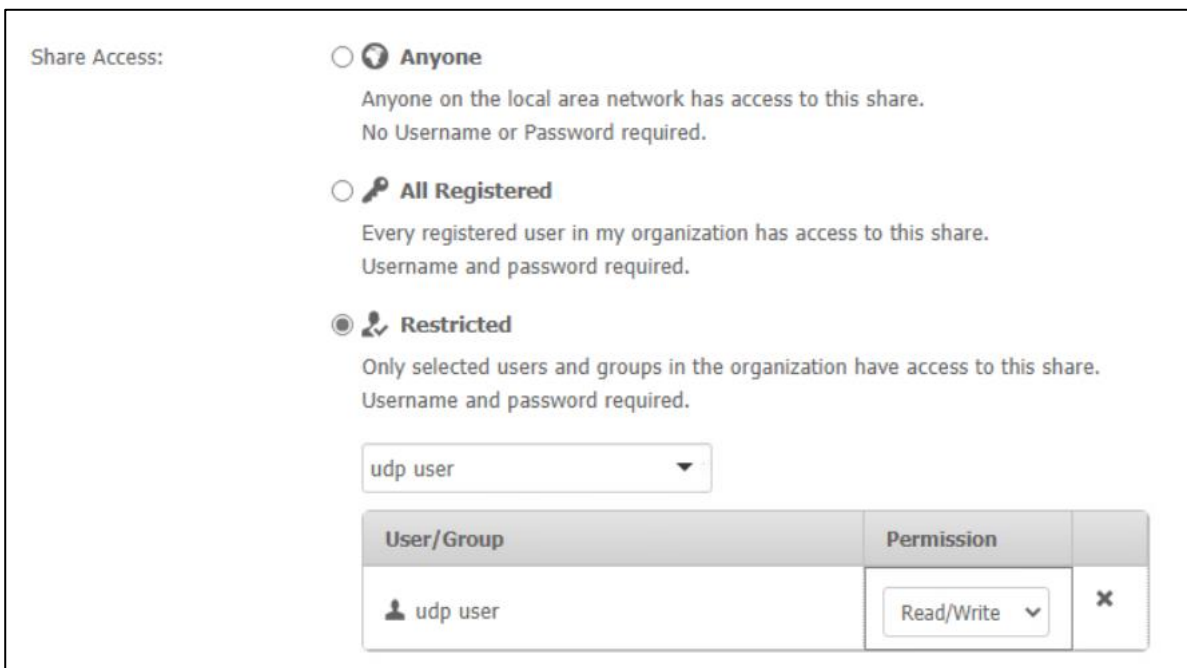


Access Protocol:

SMB
Server Message Block (Windows File Sharing)

NFS
Network File System

Step 7. 特定のユーザに読み取り/書き込み権限を付与するため、[Share Access] で “Restricted” 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 [Permission] 列で、“Read/Write（読み取り/書き込み）” 権限を指定します。



Share Access:

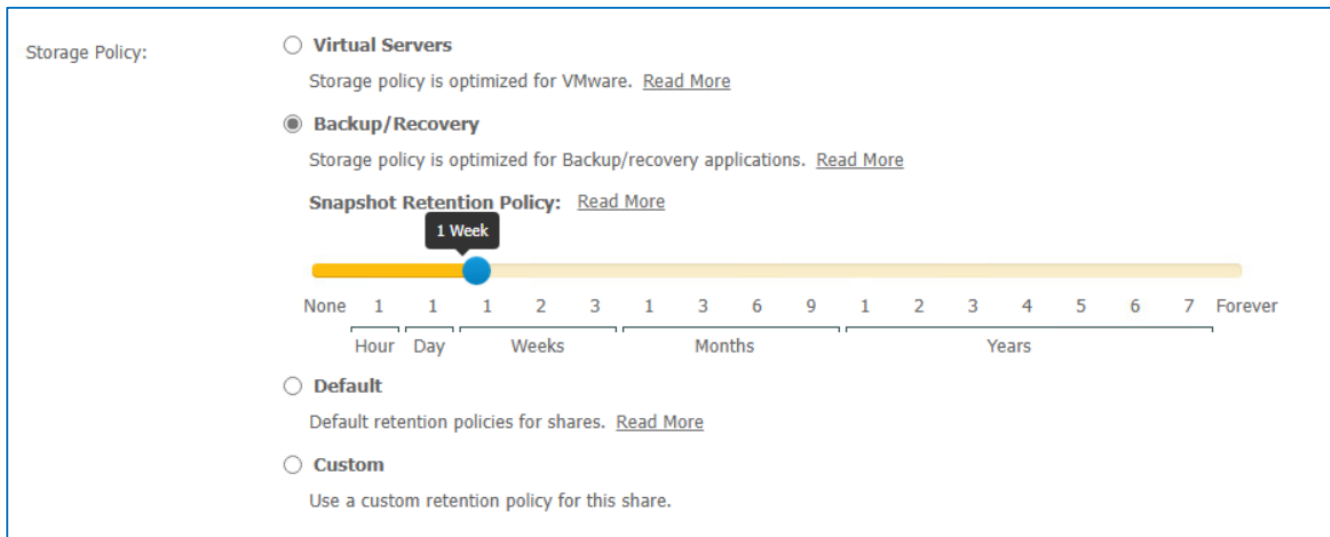
Anyone
Anyone on the local area network has access to this share.
No Username or Password required.

All Registered
Every registered user in my organization has access to this share.
Username and password required.

Restricted
Only selected users and groups in the organization have access to this share.
Username and password required.

User/Group	Permission	
udp user	Read/Write	×

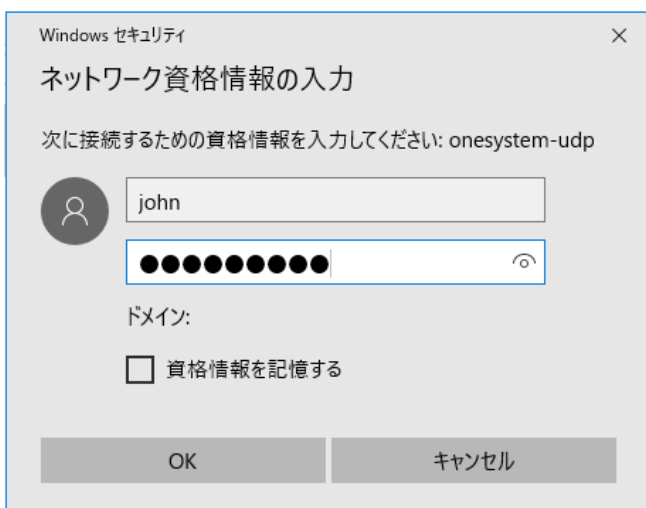
Step 8. [Storage Policy] では“Backup/Recovery”ポリシーを選択します。スナップショットの保持ポリシー（Snapshot Retention Policy）はデフォルトで 1 Week ですが、要件に応じて変更頂けます。ここまでの設定を確認したら画面右上に戻り、[Save] ボタンをクリックして共有を作成します。



Step 9. 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。

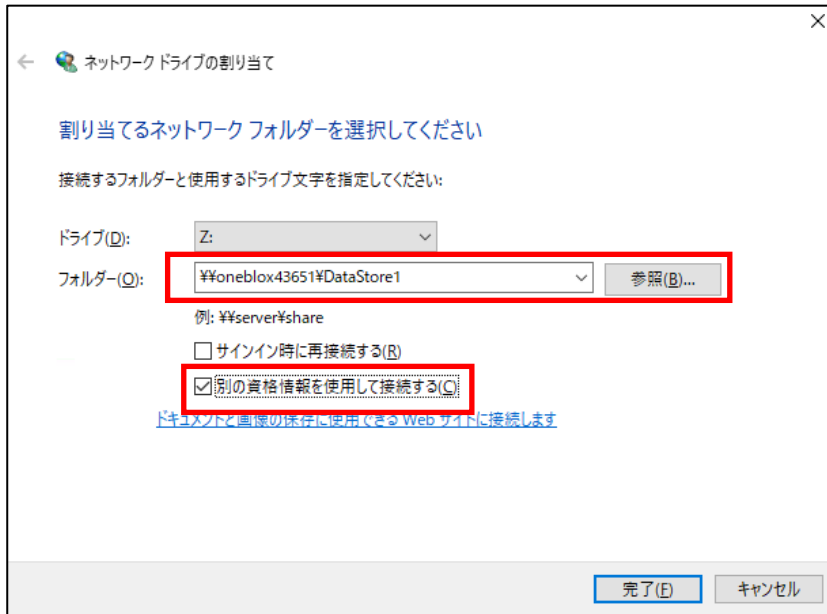
¥¥<バックアップ用ネットワークの ホスト名もしくは IP アドレス>¥¥<本節で設定した共有名>

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。

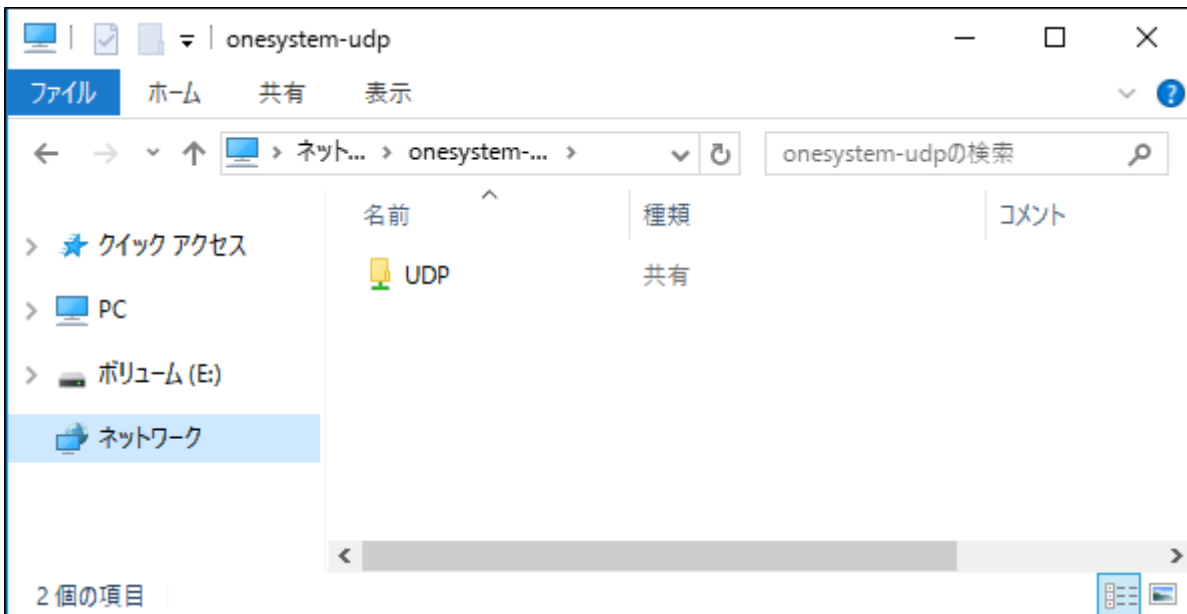


<参考>

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）



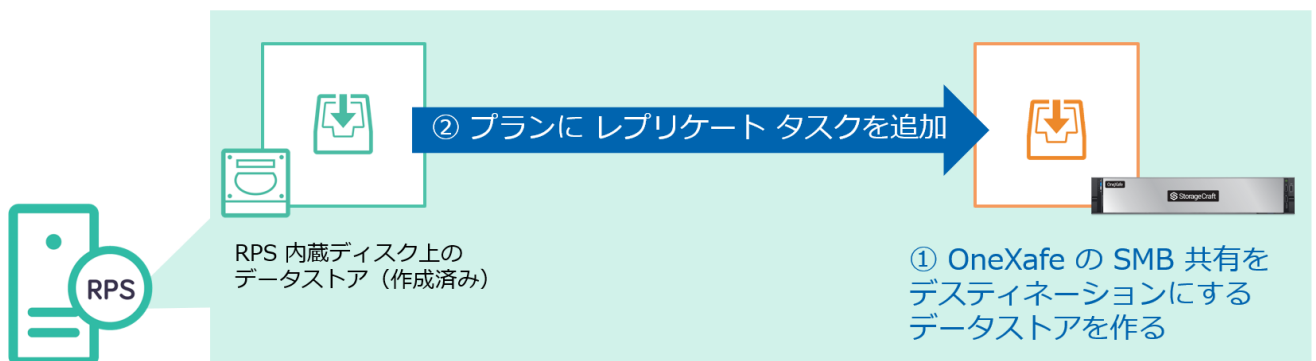
Step 10. OneXafe の共有フォルダがエクスプローラから表示されることを確認します。



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。



The screenshot shows the Arcserve UDP console interface. The top navigation bar includes 'ダッシュボード', 'リソース', 'ジョブ', 'レポート', 'ログ', '設定', and 'ハイ アベイラビリティ'. The 'リソース' tab is selected. Below the navigation bar, the breadcrumb path is 'デスティネーション: 復旧ポイントサーバ'. The main content area is divided into a left sidebar and a main table. The sidebar has sections for 'ノード', 'プラン', and 'デスティネーション'. Under 'デスティネーション', '復旧ポイント サーバ' is selected. The main table has columns for '名前', 'ステータス', and 'プラン数'. A context menu is open over the 'UDP 8200' entry, with options: '更新...', '削除', 'データストアの追加', 'データストアのインポート', 'RPS ジャンプスタート', '復旧ポイントサーバのインストール/アップグレード', and 'アドホック レプリケーション'. The 'データストアの追加' option is highlighted.

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。

データストアの作成

一般ルールを参照するか、デデュプリケーションのストレージ容量要件を次で推定できます: [要件プランニングのクイックリファレンス。](#)

🔔 デデュプリケーション、圧縮、暗号化を有効化または無効化する設定は、データストアの作成後は変更できません。

復旧ポイントサーバ	UDP8200		
データストア名	<input type="text"/>		
データストアフォルダ	(OneXafe SMB 共有フォルダ内のフォルダを指定します。)		<input type="button" value="参照"/>
同時アクティブ ノードの制限	<input type="text" value="4"/>		
<input checked="" type="checkbox"/> デデュプリケーションの有効化 (← チェックが入っていることを確認します。)			
デデュプリケーション ブロック サイズ	<input type="text" value="64 KB"/>	 デデュプリケーション テープ バックアップ リストア (←64 KB に変更します。)	
ハッシュ メモリの割り当て	<input type="text" value="12628"/>	MB (最大: 32658 MB、最小: 1024 MB)	
<input type="checkbox"/> ハッシュ デスティネーションは SSD (Solid State Drive) 上にある			
データ デスティネーション	(OneXafe SMB 共有フォルダ内のフォルダを指定します。)		<input type="button" value="参照"/>
インデックス デスティネーション	(OneXafe SMB 共有フォルダ内のフォルダを指定します。)		<input type="button" value="参照"/>
ハッシュ デスティネーション	(RPS のローカル ストレージ内のフォルダを指定します。)		<input type="button" value="参照"/>
<input checked="" type="checkbox"/> 圧縮を有効にする			
圧縮タイプ	<input checked="" type="radio"/> 標準 <input type="radio"/> 最大		
<input type="checkbox"/> 暗号化の有効化			
<input type="checkbox"/> デスティネーションの容量が上限に近づく、電子メール アラートを送信する			

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。

名前	ステータス	プラン数	保存されたデータ	デデュリケーション	圧縮
UDP 8200					
OneXafe	✓	0	0 バイト	0%	0%
UDP 8200_data_store	✓	1	1.00 TB	0%	9%

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。

ダッシュボード **リソース** ジョブ レポート ログ 設定 | ハイ アベイラビリティ

プラン: すべてのプラン

プラン名	合計	保護ノ
ローカル サイト-新規のプラン	0	0

変更
コピー
削除
今すぐ展開
一時停止

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。

プランの変更

ローカル サイト-新規のプラン このプランを一時停止

タスクの種類: バックアップ: エージェントベース Windows

タスクの追加

追加 削除

ノード名	VM 名	プラン	サイト
------	------	-----	-----



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。

プランの変更

ローカル サイト新規のプラン このプランを一時停止 **保存** キャンセル ヘルプ

タスク1: バックアップ: エージェントベース Windows タスクの種類 レプリケート **タスクの削除**

タスク2: レプリケート

ソース デスティネーション スケジュール 拡張

復旧ポイント サーバ UDP 8200

データストア OneXafe

レプリケーション ジョブ失敗時:

再試行開始 10 分後 (1 ~ 60)

再試行開始 3 回 (1~99)

レプリケートトラフィックに選択したネットワークを使用

選択したデスティネーション ネットワークに接続できない場合でも、ジョブを開始します

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。

The screenshot shows the Arcserve UDP console interface. The top navigation bar includes 'ダッシュボード', 'リソース', 'ジョブ', 'レポート', 'ログ', '設定', and 'ハイ アベイラビリティ'. The main content area is titled 'ノード: すべてのノード' and shows a list of nodes. The 'udp8200' node is selected. On the right side, the '最新のジョブ (仮スナップ)' section is expanded to show '最近のイベント'. A red box highlights the 'レプリケーション (イン)' event, which occurred on 2022/02/21 at 16:02:45.

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
🔴	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 210.18 Mbps でした。
🔴	2022/02/21 18:11:31	ローカル...	udp8200	UDP8200	134	レプリケ...	30741	デデュPLICATION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。
🔴	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。
🔴	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。
🔴	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。
🔴	2022/02/21 17:53:44	ローカル...	udp8200	UDP8200	134	レプリケ...	30725	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. share
2. enable
3. snapshot list <<共有フォルダ名>>

```
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)
```



4. 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)

```

5. update <<新しい共有フォルダ名>> --writeable

6. 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)

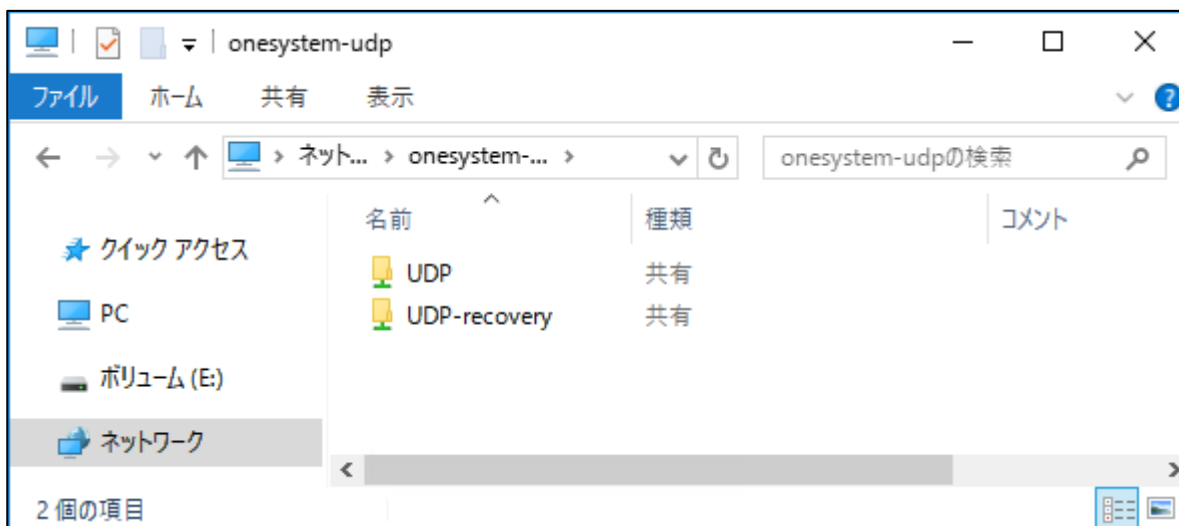
```



6.4. 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。

The screenshot shows a dialog box titled "データストアのインポート" (Data Store Import). It contains the following fields and buttons:

- 復旧ポイントサーバ (Recovery Point Server): win2016sv1.arctest.com
- データストアフォルダ (Data Store Folder): ¥¥onesystem-udp¥UDP-recovery¥common
- 暗号化パスワード (Encryption Password): [Empty field]
- Buttons: 次へ (Next), 参照 (Reference)

The screenshot shows a dialog box titled "接続" (Connection) with a close button (X). The title bar also contains the text "¥¥onesystem-udp¥UDP-recovery¥common への接続". It contains the following fields and buttons:

- ユーザ名 (Username): udpuser
- パスワード (Password): [Masked with dots]
- ユーザ名の形式 (Username format): ユーザ名、マシン名¥ユーザ名、またはドメイン名¥ユーザ名
- Buttons: OK, キャンセル (Cancel)

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。

データストアのインポート

データストア名	<input type="text" value="OneXafe"/>	
復旧ポイントサーバ	win2016sv1.arctest.com	
圧縮タイプ	標準	
データのデデュPLICATION	(はい)	
デデュPLICATION ブロック サイズ	64KB	
データ デスティネーション	%%onesystem-udp%UDP-recovery%destination	参照
インデックス デスティネーション	%%onesystem-udp%UDP-recovery%index	参照
ハッシュ デスティネーション	E:%Recovery-Hash	参照
ハッシュ デスティネーションは SSD (Solid State Drive) 上にある	<input type="checkbox"/>	
ハッシュ メモリの割り当て	<input type="text" value="13910"/> MB (最大: 24835 MB、最小: 1024 MB)	
データの暗号化	(いいえ)	
同時アクティブ ノード	<input type="text" value="4"/>	
共有フォルダ名	%%onesystem-udp%UDP-recovery%common	

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>>
```

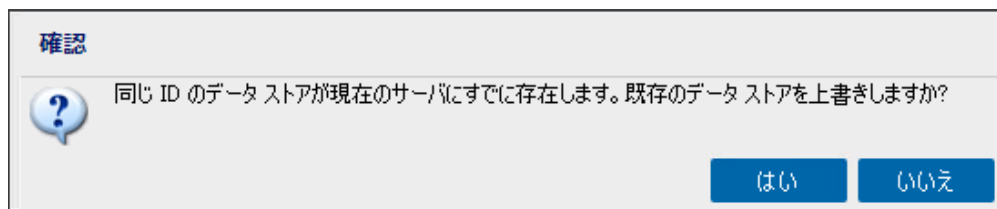
次に as_gddmgr.exe を以下のように実行します。

```
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。こうすることで、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。

6.5. 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. 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 UDP 8.x 動作要件

<https://support.arcserve.com/s/article/Arcserve-UDP-8-0-Software-Compatibility-Matrix?language=ja>

Arcserve UDP 8.x 注意 / 制限事項

<https://support.arcserve.com/s/article/2021032301?language=ja>

Arcserve UDP 8.x 製品ドキュメント

<https://support.arcserve.com/s/article/Arcserve-UDP-8-0-Documentation?language=ja>

Arcserve UDP サポート / FAQ

<https://support.arcserve.com/s/article/205002865?language=ja>

Arcserve OneXafe 注意 / 制限事項

<https://support.arcserve.com/s/article/OneXafe-Notice?language=ja>

以上

