Orchestrating a brighter world NEC

mdxII 利用マニュアル

第 2 版

日本電気株式会社
文教・科学ソリューション統括部

改版履歴

版数	年月日	該当項目	概要説明
1	2024/03/26	全項目	新規作成
2	2024/04/26	4.3.1.1 4.3.2	オブジェクトストレージ接続情報表示のタイムラグについて追記 CMC の略称を削除

目次

1. はじめに

本ドキュメントは、大阪大学 mdx II の利用者（プロジェクト管理者）向けの手順書です。mdx II における仮想マシンの作成や操作など、システムを利用するのに必要な情報を提供します。

本ドキュメントではコマンドを以下のように表記しています。網掛け部分がコマンドとなります。また、プロンプト部分を「#」としたものは root ユーザ、「$」としたものは root 以外のユーザの実行を表します。いくつかのコマンド実行結果において、#から始まるものがあります。コマンド部分は網掛けの場所となりますので、ご注意ください。

プロンプトの前に「[XXX]」で表記したものはホスト名を表します。特定のホストでコマンドを実行する場合に記載しております。

プロンプトの前に「<XXX>」で表記したものは特定のユーザ名を表します。特定のユーザでコマンドを実行する場合に記載しております。

例 1：
$ root 以外のユーザ（LDAP アカウントやローカルアカウント）でのコマンド実行

例 2：
root ユーザでのコマンド実行

例 3：
[host]# host で、root ユーザで実行するコマンド

例 4：
<user>$ user ユーザで実行するコマンド

1.1. 用語説明

- プロジェクト管理者
  プロジェクトの申請を行い、ユーザポータルから仮想インフラ環境の作成やデータ集約用オブジェクトストレージ、データ転送用ポータルの利用申請を行うユーザです。

- プロジェクトユーザ
  プロジェクト管理者にて作成した仮想インフラ環境を利用するユーザです。

- システム管理者
  プロジェクト申請をうけてシステムにプロジェクトを登録する本システムの管理者です。

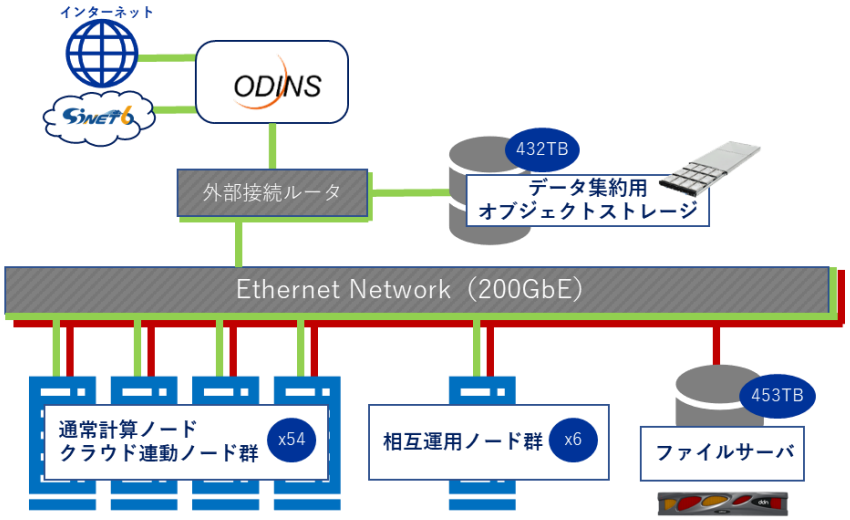
1.2. 提供サービス

提供するサービスは以下の通りです

サービス	申請方法	参照先
通常計算ノード・クラウド連動ノード (OpenStack)	プロジェクト申請 Web から申請	「3. プロジェクト申請」
相互運用ノード (VMware)	システム管理者宛にメール申請	「4.6.相互運用ノード (VMware)」
ファイルサーバ	● インスタンスからのボリューム利用 ユーザポータルから利用可能なため申請は不要	「4.1.10.1. Cinder ボリュームの利用」
	● インスタンスからの Lustre マウント OpenStack(または VMware)のインスタンスの作成およびパブリック IP アドレスの付与後にシステム管理者宛にメール申請	「4.1.10.2. Lustre マウント」
オブジェクトストレージ	ユーザポータルから申請	「4.3. mdx II オブジェクトストレージ」
プロジェクト用データ転送用ポータル	ユーザポータルから申請 ※オブジェクトストレージの申請が完了した場合のみ申請が可能です。	「4.4. ProjectDataPortal」
ユーザ用データ転送用ポータル	システム管理者宛にメール形式で申請	「4.5. myDataPortal」

1.3. システム概要

mdx II は、通常計算ノード・クラウド連動ノード、相互運用ノード、ファイルサーバ、データ集約用オブジェクトストレージで構成されるシステムです。



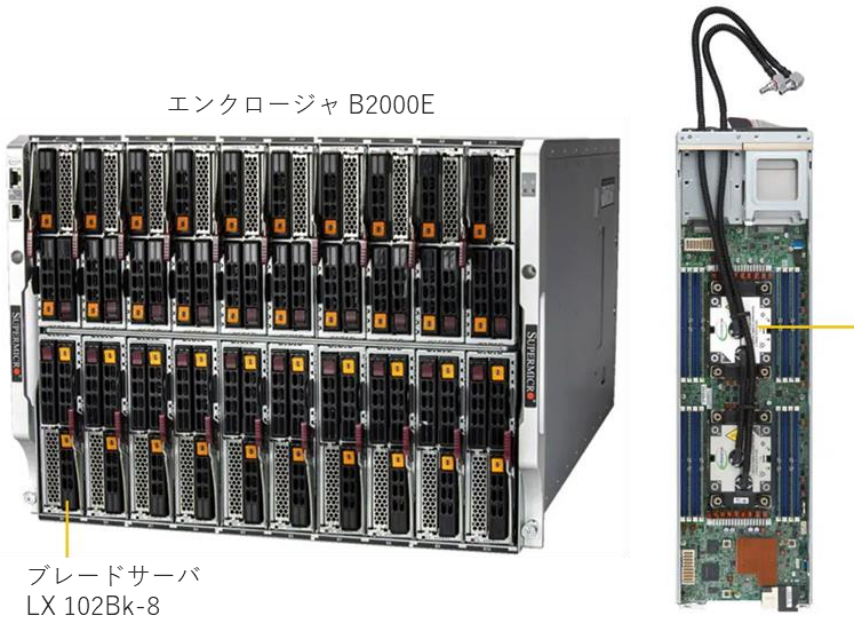
1.3.1. 汎用計算ノード

通常計算ノード・クラウド連動ノード、および相互運用ノードの役割を担う汎用計算ノードは計 60 ノードで構成されます。各ノード数と役割の内容については下表の通りです。

役割	ノード数	説明
通常計算ノード・ クラウド連動ノード	54	Red Hat OpenStack の Compute ノードとして構成
相互運用ノード	6	VMware ESXi として構成

1 ノード当たりのハードウェア構成は以下になります。

項目	構成内容
サーバ機器名	NEC LX 102Bk-8
CPU	インテル® Xeon® Platinum 8480+ プロセッサー ・コア数：56 ・ベース動作周波数：2.0GHz ・ハイパースレッディング有効
CPU 数	2
メモリ	512GiB (32GiB DDR5-4800 ECC RDIMM x16)
ドライブ	960GB SATA SSD x1
ネットワーク I/F	サービス用：200GbE x2 管理用：25GbE x1 ※20 ノードで 200GbE の制限あり。



1.3.2. ファイルサーバ

DDN ES400NVX2 を用いて、Lustre アプライアンスである DDN EXAScaler を構成しています。

データの格納領域には、プロジェクト毎のデータを格納する「データ領域」と仮想マシンのデータを格納する「仮想ディスク領域」の 2 つがあります。利用可能な総容量はデータ領域が 453.24TB、仮想ディスク領域が 100TB になります。

DDN ES400NVX2

1.3.3. データ集約用オブジェクトストレージ

Cloudian HyperStore HAS-1610 で構成され、mdx II オブジェクトストレージのサービスを提供します。利用可能な総容量は 432TB です。

Cloudian HyperStore HAS-1610

1.4. プロジェクト申請とユーザポータル

1.4.1. プロジェクト申請フォーム

プロジェクト登録を申請するために、下記の URL からプロジェクト申請フォームへのアクセスが可能です。アクセスには学認による認証が必要です。プロジェクト申請 Web では、プロジェクトの新規申請が可能です。

https://project.osaka.mdx.jp/mdx_project

学認アカウントをお持ちでない場合は、システム管理者宛にメールにてご申請ください。申請済みのプロジェクト情報の変更をご希望される場合もシステム管理者宛にメールでご連絡ください。

プロジェクト申請の手順については、「3. プロジェクト申請」をご参照ください。

1.4.2. ユーザポータル

プロジェクト申請の完了後に、ユーザポータルへのアクセスが可能です。ユーザポータルへのアクセスには、One-Time Password 認証と学認認証（またはローカル認証）による 2 段階認証が必要になります。One-Time Password の登録に必要な QR コード情報はプロジェクト登録の完了後にシステム管理者からご連絡します。ユーザポータルへは下記 URL からアクセスが可能です。

https://portal.osaka.mdx.jp

ユーザポータルで利用可能なアカウントは以下の 2 種類あります。

- 学認アカウント
  - 全国の大学等と NII が連携して構築する学術認証フェデレーション
    https://www.gakunin.jp
- ローカルアカウント
  - mdxII 専用のアカウント

1.5. 資源単位

1.5.1. データ単位

メモリや仮想ディスク、ストレージの容量を 2 のべき乗で計算した数値で表示しています。

2 のべき乗で計算した数値を表すには 2 進接頭辞を用いた単位(KiB/MiB/GiB など)が標準利用されますが、mdxII では一般的によく見られる SI 接頭辞を用いた単位(KB/MB/GB など)を利用して表示しています。

例)

1[MiB] = 1024[KiB] → mdxII では 1[MiB] を 1[MB] と表示
1[GiB] = 1024[MiB] → mdxII では 1[GiB] を 1[GB] と表示

1.5.2. CPU パック

mdxII では CPU 資源の利用単位として CPU パックという単位を使用します。

CPU パックは仮想 CPU 数と仮想メモリがセットになったものです。1CPU パックで利用できる資源量は以下の通りです。

名称	仮想 CPU 数	仮想メモリ量
CPU パック	1	2048MB(2GB)

1.6. お問い合わせ先

プロジェクトやサービスの申請などのお問い合わせについては、下記の連絡先へお問い合わせください。

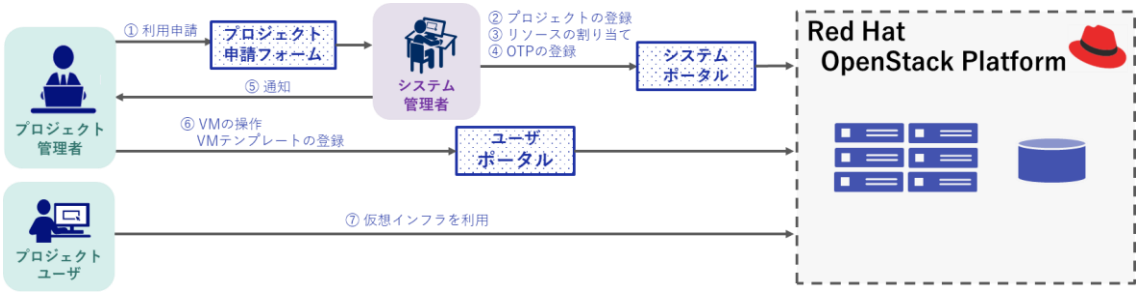
- システム管理者
  - メールアドレス：mdx2-system@cmc.osaka-u.ac.jp
  - 電話番号 ：06-6879-8813

2. 利用の流れ

各サービスの利用の流れについて記載しています。

2.1. 通常計算ノード・クラウド連動ノード(RHOSP)

通常計算ノード・クラウド連動ノードの Red Hat OpenStack Platform 環境の利用の流れは下図の通りです。



2.2. ファイルサーバ

ファイルサーバのサービスは、以下の方法で利用が可能です。

- OpenStack ボリューム(Cinder)としてインスタンスにアタッチ
  - ユーザポータルから利用が可能です。利用手順は「4.1.10.1. Cinder ボリュームの利用」をご参照ください。
- OpenStack 仮想マシンから Lustre マウント
  - OpenStack の仮想マシンから利用が可能です。利用の際はシステム管理者にメールで申請依頼が必要になります。利用手順は「4.1.10.2. Lustre マウント」をご参照ください。
- VMware 仮想マシンから Lustre マウント
  - VMware の仮想マシンから利用が可能です。利用の際はシステム管理者にメールで申請依頼が必要になります。利用手順は「4.6.3. Lustre マウント」をご参照ください。
- ProjectDataPortal（Nextcloud）からインスタンス経由で sftp アクセス
  - プロジェクト単位で利用可能な Nextcloud から利用が可能です。利用手順は「4.4. ProjectDataPortal」をご参照ください。
- myDataPortal（Nextcloud）から S3 アクセス
  - ユーザ単位で利用可能な Nextcloud から利用可能です。利用手順は「4.5. myDataPortal」をご参照ください。
- インターネット経由の S3 アクセス
  - 利用手順は「4.2.1. S3 アクセス方法」をご参照ください。

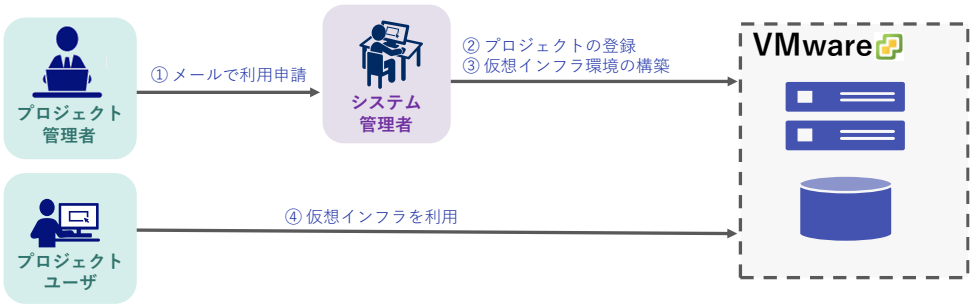
2.3. mdx II オブジェクトストレージ

mdxII オブジェクトストレージのサービスは、以下の方法で利用が可能です。

- プロジェクト用データ転送用ポータル(Nextcloud)から S3 アクセス
  - 利用手順は「4.4. ProjectDataPortal」をご参照ください。
- ユーザ用データ転送用ポータル(Nextcloud)から S3 アクセス
  - 利用手順は「4.5. myDataPortal」をご参照ください。
- インターネット経由の利用：S3 アクセス
  - 利用手順は「4.3. mdx II オブジェクトストレージ」をご参照ください。

2.4. 相互運用ノード(VMware)

相互運用ノードの VMware 環境の利用の流れは下図の通りです。相互運用ノードではユーザポータルの提供はありません。システム管理者宛にメールにて利用を申請します。申請後にシステム管理者にて仮想マシンを作成して提供します。申請方法については「4.6. 相互運用ノード (VMware)」をご参照ください。



3. プロジェクト申請

「3.1. 新規申請」の手順に従い、プロジェクトの申請を行います。プロジェクト申請で入力が必要な項目は下表の通りです。

項目名	内容
Project Name	プロジェクト名
User Name	ユーザ名（※学認アカウントの場合は不要）
Full Name	申請者の氏名
Instituition	申請者の所属機関名
Mail Address	申請者のメールアドレス
CPU Pack	プロジェクトで利用する総 CPU パック数 ※1CPU パック＝CPU 1 コア、メモリ 2 GiB
Available Volume(GB)	プロジェクトで利用する総ストレージ容量 ※Lustre マウントで利用する容量は含まれません。
Max number of Floating IP	プロジェクトで利用するフローティング IP アドレスの最大数 ※フローティング IP アドレスは仮想マシンを外部ネットワークと通信可能にするために必要なアドレスです。
Billing Name	請求先担当者の氏名
Billing Mail Address	請求先担当者のメールアドレス
Billing Phone Number	請求先担当者の電話番号
Billing Affiliation	請求先担当者の所属名

3.1. 新規申請

3.1.1. 学認アカウントをお持ちの場合

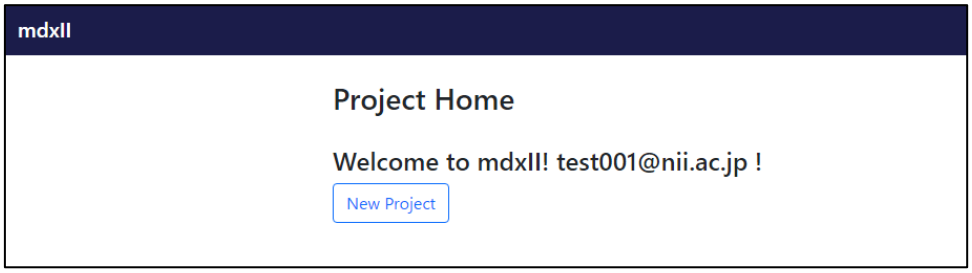
プロジェクト申請フォームの Web から以下の手順でプロジェクトの申請を行います。

(1) Web ブラウザから下記 URL にアクセスします。
https://project.osaka.mdx.jp/mdx_project

(2) 「所属している機関を選択」のプルダウンメニューから所属の機関を選択し、「選択」ボタンをクリックします。

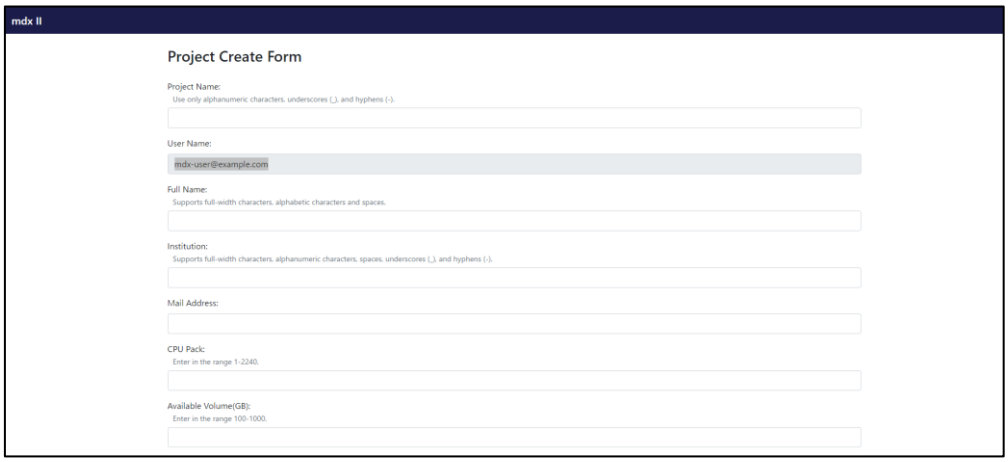
(3) 学認アカウントのユーザ名とパスワードを入力します。

(4) Project Home 画面で「New Project」ボタンを押下します。



(5) Project Create Form 画面で下表の項目を入力します。

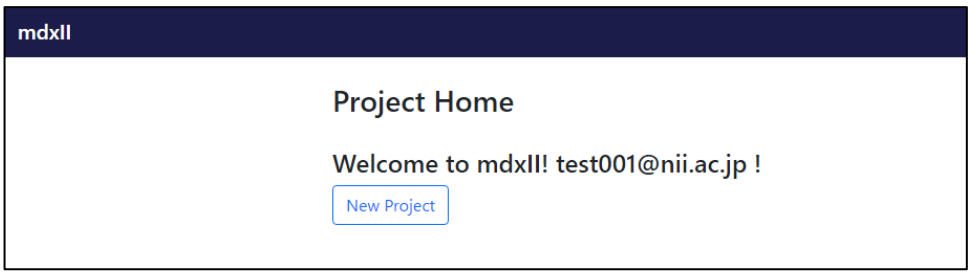
項目	設定例	備考
Project Name	mdxII-project	プロジェクト名。英字(大小),数字,_(アンダーバー), -(ハイフン)のみ可能
User Name	test001@nii.ac.jp	ユーザ名。学認 ePPN を代入
Full Name	mdxII 太郎	申請者氏名
Institution	mdxII 大学	申請者所属機関名
Mail Address	mdxII@example.com	申請者メールアドレス
CPU Pack	320	CPU パック数（1~2240）
Available Volume(GB)	500	ストレージ容量（100~1000）
Max number of Floating IP	4	フローティング IP アドレスの最大数(1~16)
Billing Name	mdxII 次郎	請求先担当者氏名
Billing Mail Address	mdxII-admin@example.com	請求先担当者メールアドレス
Billing Phone Number	01234587890	請求先担当者電話番号
Billing Affiliation	mdxII 大学	請求先担当者所属名



(6) 申請内容を確認します。

(7) Project Create Form 画面最下部の「Create」ボタンを押下し、申請を完了します。※ 確認画面はございません。

(8) 成功すると Project Home 画面に遷移します。



3.1.2. 学認アカウントをお持ちでない場合

以下の申請フォーマットを記入の上、システム管理者宛にメールで申請を行います。

```
----- プロジェクト申請フォーマット -----
Project Name                 ：※プロジェクト名　英字(大小),数字, _(アンダーバー), -(ハイフン)のみ可能
User Name                    ：※ユーザ名　　英字(大小),数字, _(アンダーバー), -(ハイフン)のみ可能
Full Name                    ：※申請者氏名
Institution                  ：※申請者所属機関名
Mail Address                 ：※申請者メールアドレス
CPU Pack                     ：※CPU パック数（1~2240）
Available Volume(GB)         ：※ストレージ容量（100~1000）
Max number of Floating IP    ：※フローティング IP アドレスの最大数（1~16）
Billing Name                 ：※請求先担当者氏名
Billing Mail Address         ：※請求先担当者メールアドレス
```

```
Billing Phone Number          : ※請求先担当者電話番号
Billing Affiliation           : ※請求先担当者所属名
-----------------------------------------------------
```

以下は記載例になります。

```
Project Name                  : mdxII-project
User Name                     : mdxII-user
Full Name                     : mdxII 太郎
Institution                   : mdxII 大学
Mail Address                  : mdxII@example.com
CPU Pack                      : 320
Available Volume(GB)          : 500
Max number of Floating IP     : 4
Billing Name                  : mdxII 次郎
Billing Mail Address          : mdxII-admin@example.com
Billing Phone Number          : XX-XXXX-XXXX
Billing Affiliation           : mdxII 大学
```

3.2. 変更申請

プロジェクト申請 Web では、新規の申請のみ受け付けています。プロジェクト情報の変更をご希望の場合は、システム管理者にメールにてご連絡ください。

4. 利用方法

4.1. 通常計算ノード・クラウド連動ノード（OpenStack）

4.1.1. プロジェクト登録時の情報

プロジェクト申請後に登録が完了するとシステム管理者より以下の情報が通知されます。

- アカウント名
- One-Time Password 登録に必要な QR コードの URL

※学認アカウントではなく、ローカルアカウントで申請した場合は、ローカルパスワードの初期パスワードも通知されます。

4.1.2. 2 段階認証用アプリのインストール

ユーザポータルに SSH ログインするためには、 One-Time Password による 2 段階認証を通る必要があります。 2 段階認証に必要となるアプリケーションを用意し、ご自身の端末にインストールしてください。

2 段階認証アプリケーションとしては以下のようなアプリケーションが使用できます。

OS	アプリケーション	備考
Android	Google Authenticator	Google Play Store
iOS	Google Authenticator	Apple App Store
Windows	WinAuth	https://winauth.github.io/winauth/download.html
	Google Authenticator	Google Chrome、Microsoft Edge の拡張機能として追加
macOS	Step Two	Apple App Store
	Google Authenticator	Google Chrome の拡張機能として追加

4.1.3. ユーザポータルへのログイン

ユーザポータルへのログインは One-Time Password 認証と学認（またはローカル認証）の 2 段階があります。学認アカウントでログインする場合は、「4.1.3.1. 学認アカウントのログイン」の手順に従ってログインしてください。ローカルアカウントでログインする場合は、「4.1.3.2 . ローカルアカウント」の手順に従ってログインしてください。

4.1.3.1. 学認アカウントのログイン

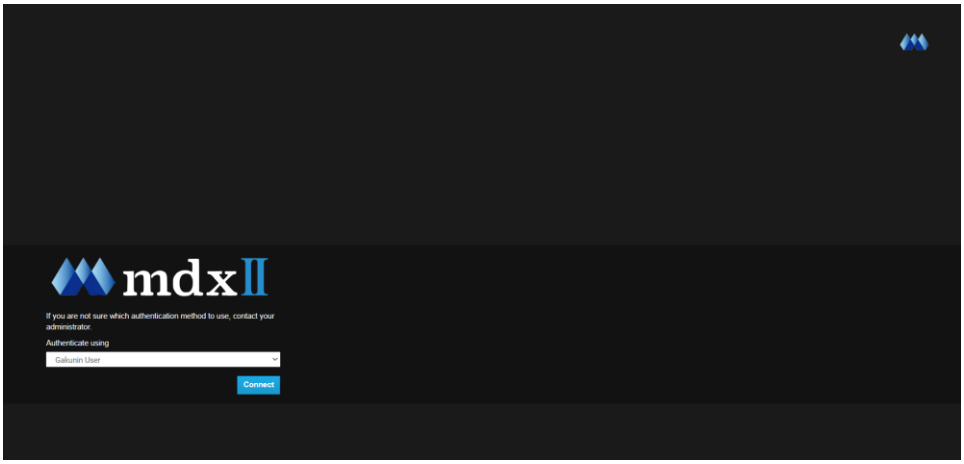
(1) Web ブラウザから下記 URL にアクセスします。

https://portal.osaka.mdx.jp

(2) ポップアップが表示され、ユーザ名とパスワードの入力が要求されます。ユーザ名と 2 段階認証アプリケーションで確認した One-Time Password のパスワードを入力して[サインイン]ボタンをク

リックします。

(3) One-Time Password の認証に成功するとユーザポータルのログイン画面が表示されます。

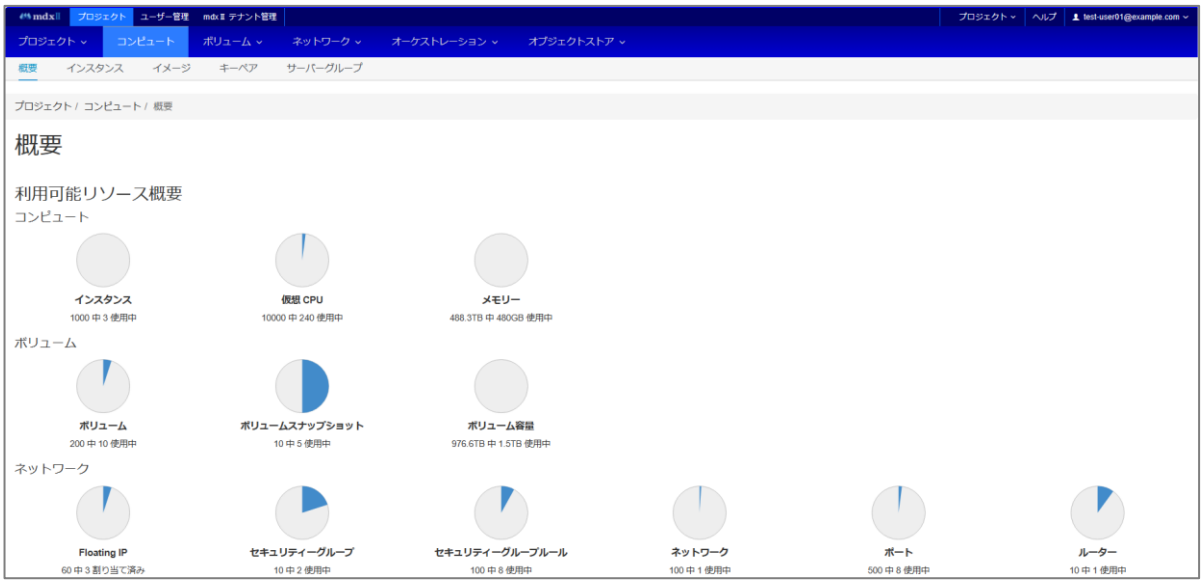


(4) [Connect]ボタンをクリックします。

(5) 学認のログイン画面が表示されるため、[所属機関]から所属の機関を選択して「選択」ボタンをクリックします。

(6) 所属機関の IdP のログイン画面が表示されるため、学認アカウントのユーザ名とパスワードを入力します。

(7) 学認の認証に成功するとユーザポータルのダッシュボードが表示されます。

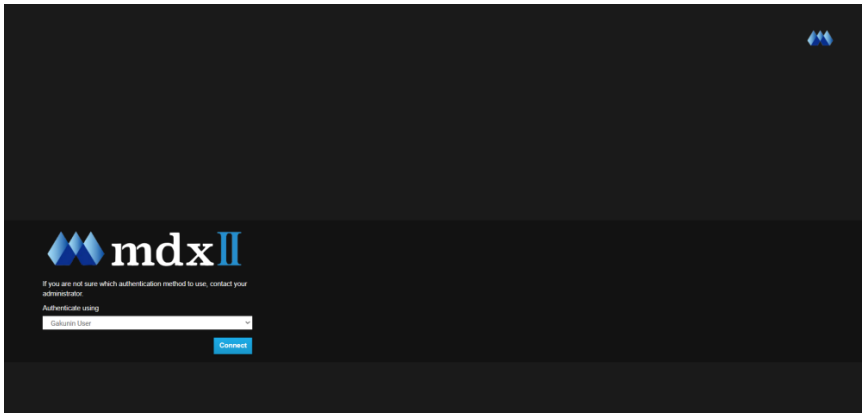


4.1.3.2. ローカルアカウント

(1) Web ブラウザから下記 URL にアクセスします。
https://portal.osaka.mdx.jp

(2) ポップアップが表示され、ユーザ名とパスワードの入力が要求されます。ユーザ名と 2 段階認証アプリケーションで確認した One-Time Password のパスワードを入力して[サインイン]ボタンをクリックします。

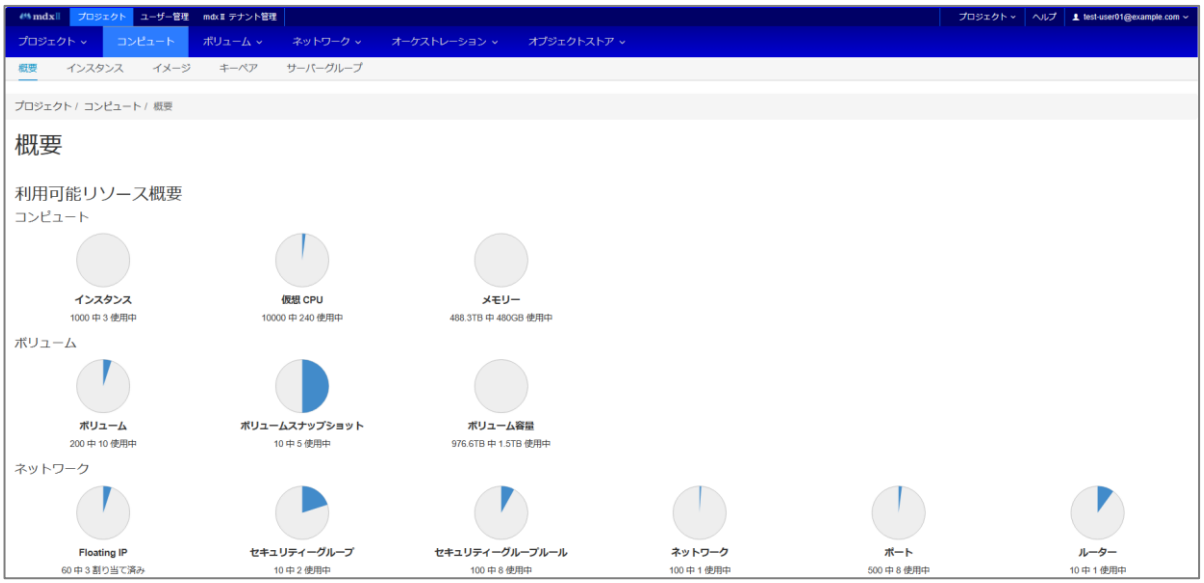
(3) One-Time Password の認証に成功するとユーザポータルのログイン画面が表示されます。



(4) プルダウンメニューで[Local User]を選択して[Connect]ボタンをクリックします。

(5) [ユーザー名]と[パスワード]にローカルユーザのユーザ名とパスワードを入力して[Connect」ボタンをクリックします。

(6) 認証に成功するとユーザポータルのダッシュボードが表示されます。



4.1.4. ネットワークの作成

仮想マシンを接続するネットワークは 2 種類あります。仮想マシンでファイルサーバの領域を Lustre マウントする場合は「Lustre 用ネットワーク」を利用し、Lustre マウントを利用しない場合は「プライベートネットワーク」を利用します。それぞれのネットワークの特長は以下の通りです。

- Lustre 用ネットワーク
  - プロジェクト間で共有のネットワーク
  - ネットワークアドレスは 192.168.100.0/23 であり、仮想マシン作成時に DHCP により自動で IP アドレスを付与
  - 仮想マシンに Floating IP を付与することでインターネットへの接続が可能
  - ファイルサーバ領域の Lustre マウントで利用
    ※他のプロジェクトと共有するネットワークのため、セキュリティグループ（ACL）により適切にアクセス制限を設定してください。セキュリティグループの設定方法は「4.1.6. セキュリティグループの作成」をご参照ください。

- プライベートネットワーク
  - プロジェクト内に閉じたネットワーク
  - ネットワークアドレスはユーザにて自由に設定が可能
  - 仮想マシンに Floating IP を付与することでインターネットへの接続が可能

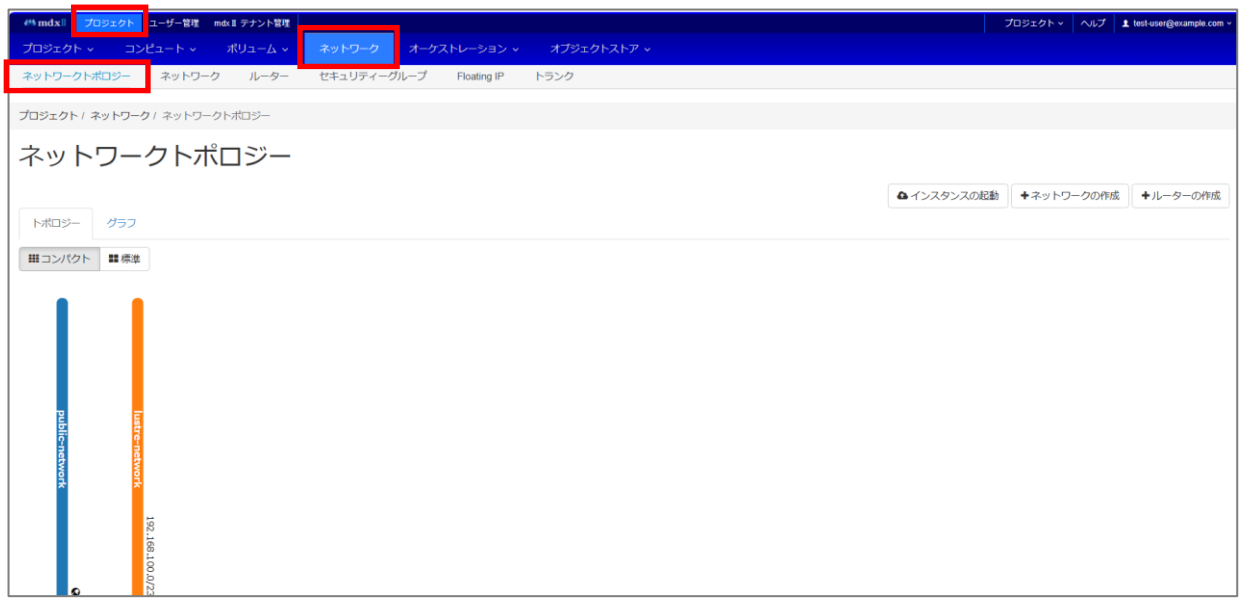
それぞれ利用するネットワークに合わせて以下の手順に従ってください。

4.1.4.1. Lustre 用ネットワーク

Lustre 用ネットワークはシステム側で事前に作成されているため、必要な操作はありません。
「4.1.5. キーペアの登録」の手順に進んでください。

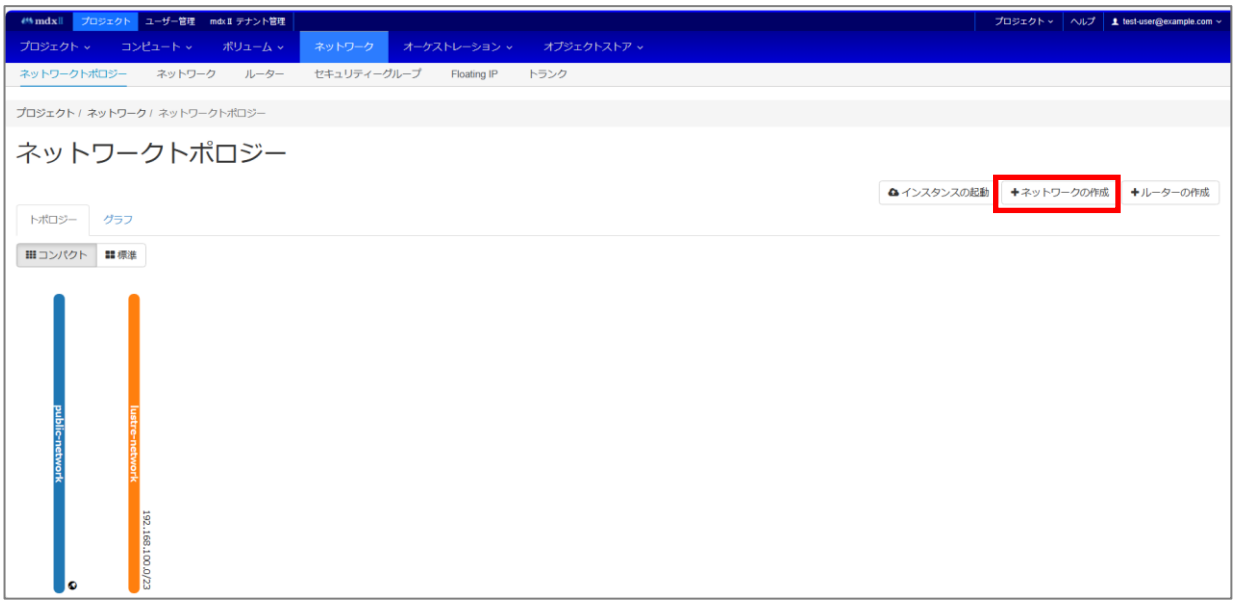
4.1.4.1. プライベートネットワーク

(1) [プロジェクト]メニュー ＞ [ネットワーク]パネル ＞ [ネットワークトポロジー]タブをクリックします。



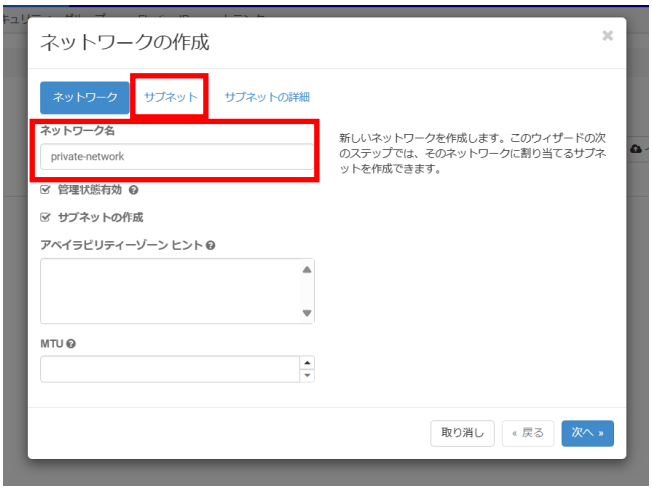
※初期状態では外部アクセス用ネットワーク「public-network」と Lustre 用ネットワーク「lustre-network」が表示されます。

(2) [ネットワークの作成]ボタンをクリックします。



(3) ネットワークの作成画面で以下を入力して [サブネット]タブをクリックします。

・ネットワーク名：※任意



(4) 以下の項目を入力して[サブネットの詳細]タブをクリックします。

・サブネット名　　：※任意
・ネットワークアドレス　：※任意
・IP バージョン　　：IPv4
・ゲートウェイ IP　　：※ネットワークアドレスの中から 1 つの IP アドレスを記載
・ゲートウェイなし　　：チェックなし

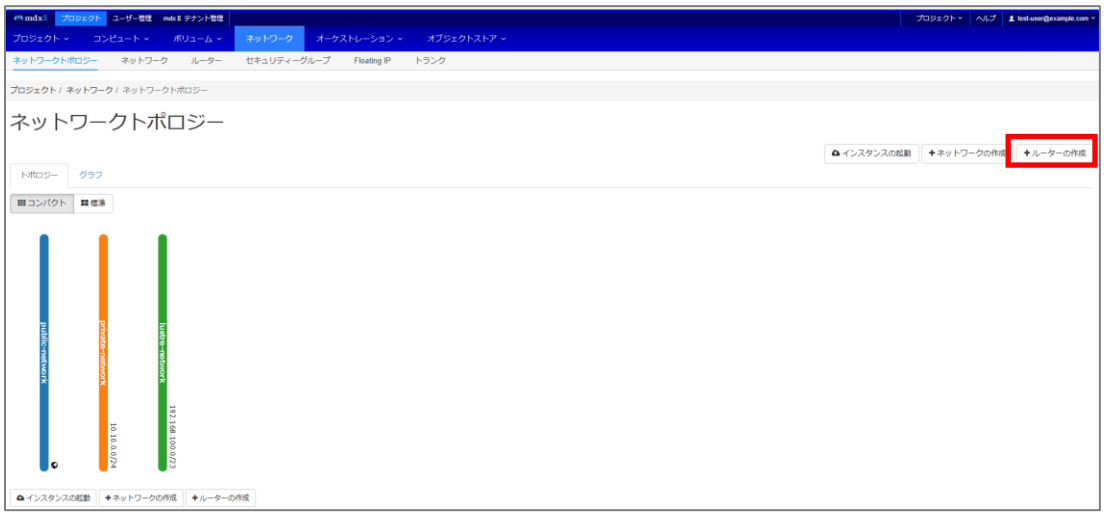
(5) 以下の項目を入力して[作成]ボタンをクリックします。

・DHCP 有効　　：※仮想マシンに自動で IP アドレスを付与したい場合はチェックを入れる

・IP アドレス割り当てプール：※指定したネットワークアドレスの中から仮想マシンに割り当てる IP アドレスレンジを指定

(6) 作成したプライベートネットワークがネットワークトポロジー画面に表示されます。

(7) 次に[+ルーターの作成]ボタンをクリックします。



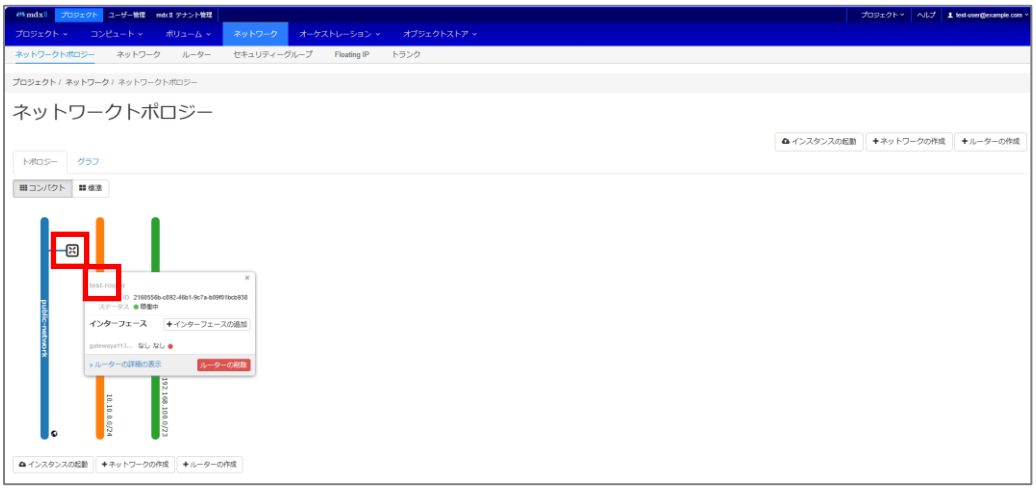
(8) 以下の項目を入力して[ルーターの作成]ボタンをクリックします。

・ルーター名：※任意

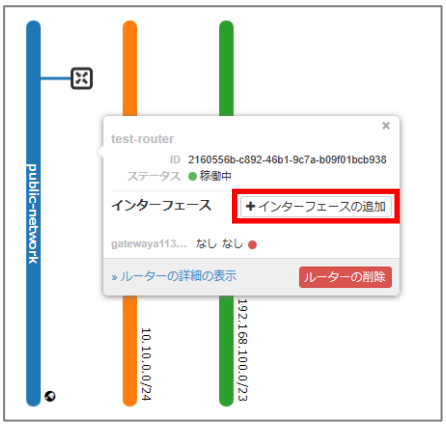
・外部ネットワーク：public-network

(9) 作成した仮想ルーターが public-netwrok に接続された状態でネットワークトポロジー画面に表示されます。

(10) 次に仮想ルーターのアイコンをクリックします。

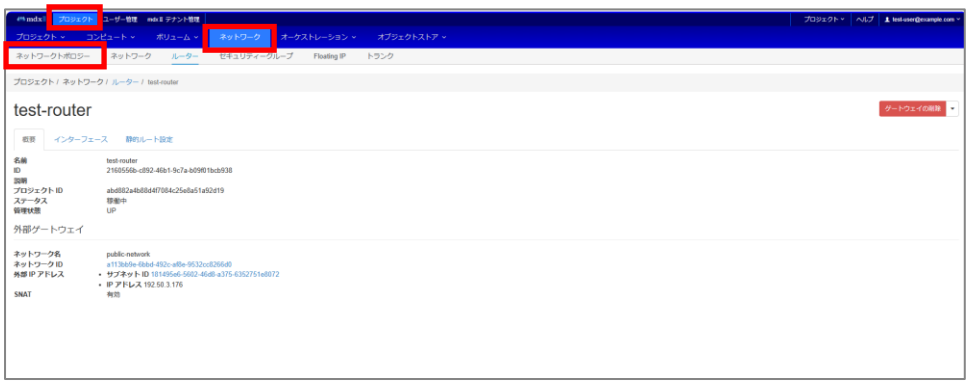


(11) [+インターフェースの追加]ボタンをクリックします。

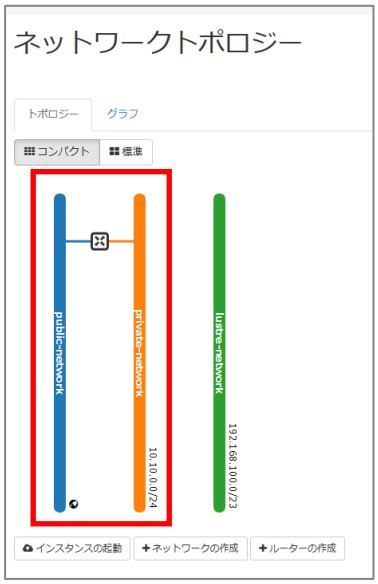


(12) 以下を選択して[送信]ボタンをクリックします。

(13) 作成した仮想ルーターの画面に遷移するため、再度、[プロジェクト]メニュー ＞[ネットワーク]パネル ＞[ネットワークトポロジー]タブをクリックします。



(14) 作成した仮想ルーターと作成したプライベートネットワークが接続されていることを確認します。



4.1.5. キーペアの登録

仮想マシンに SSH アクセスするための SSH 鍵のキーペアを登録します。キーペアの登録には以下の 2 つの方法があります。

- 事前に作成した SSH 鍵の公開鍵をインポートして登録（推奨）
- 新規にキーペアを作成して登録
  - ➢ 新規のキーペアの作成では鍵のパスフレーズが設定できません。仮想マシンを動作確認などで利用する場合のみご利用ください。

それぞれの登録方法に合わせて、以下の手順を実施してください。

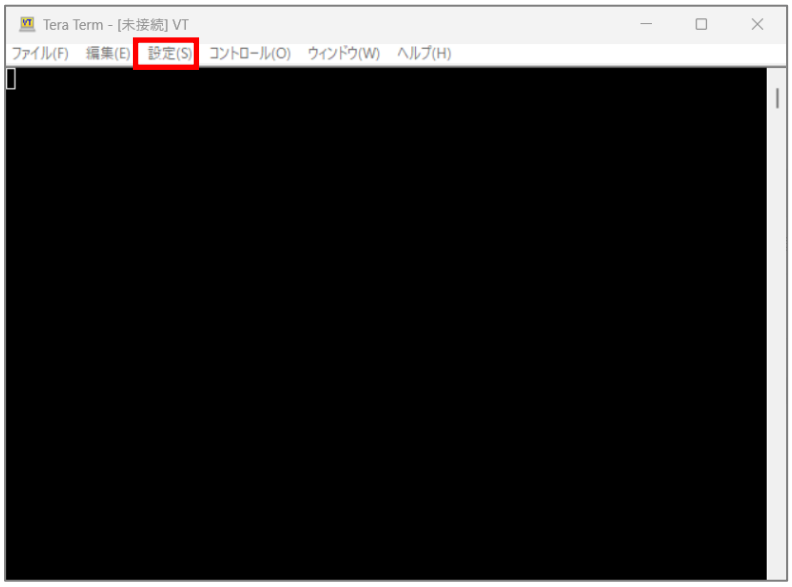
4.1.5.1. SSH 鍵のインポートによる登録

(1) 作業端末で事前に SSH 鍵を作成します。以下は TeraTerm のターミナルソフトで作成する例になります。

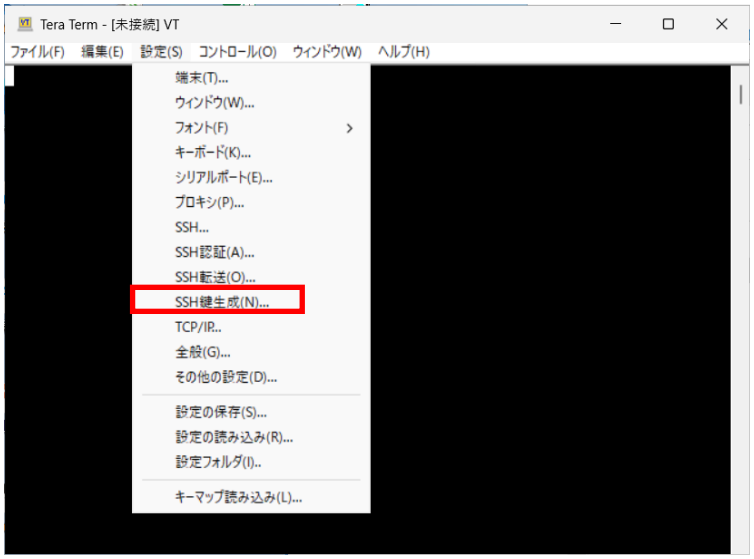
① 作業端末で下記 URL から TeraTerm をダウンロードしてインストールします。
https://github.com/TeraTermProject/teraterm/releases

② TeraTerm を起動します。

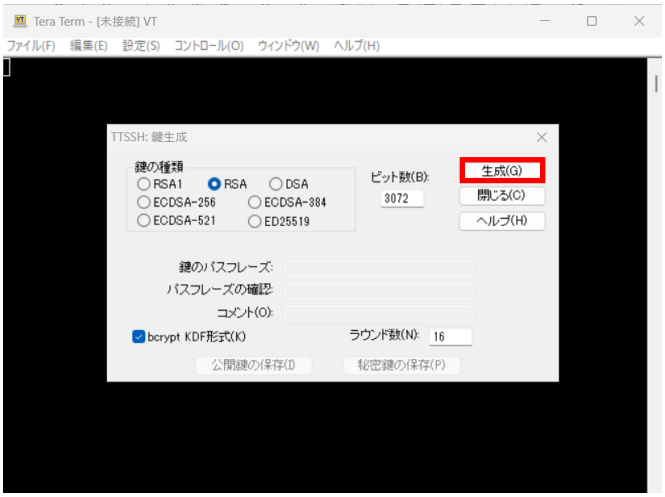
③ [設定]タブをクリックします。



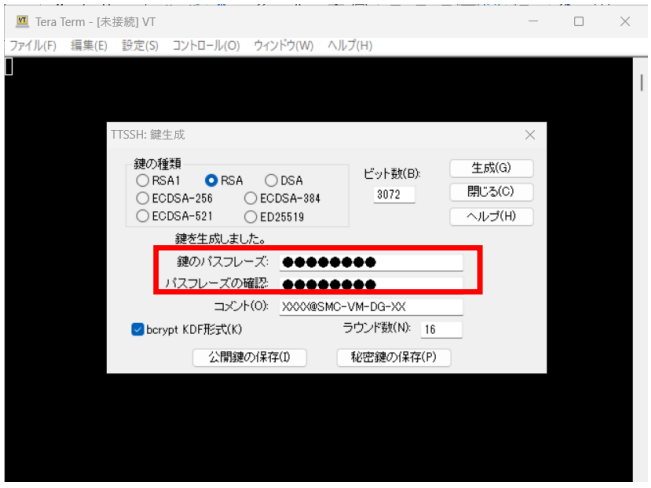
④ [SSH 鍵生成(N)]をクリックします。



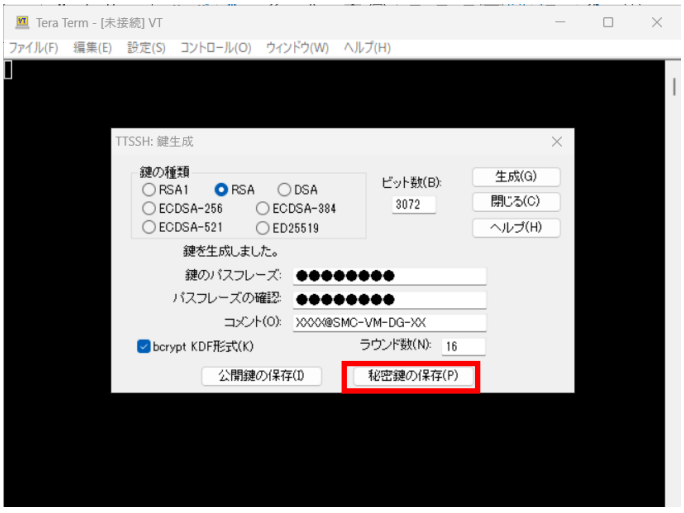
⑤ [生成(G)]ボタンをクリックします。



⑥ [鍵のパスフレーズ]と[パスフレーズの確認]でSSH鍵に設定するパスフレーズを入力します。



⑦ [秘密鍵の保存]ボタンを押して秘密鍵を保存します。秘密鍵は仮想マシンへのSSHアクセスで必要になりますので、漏洩、紛失しないように厳密に保管してください。



⑧ [公開鍵の保存]ボタンをクリックして公開鍵を保存します。公開鍵はキーペアの登録で利用します。

(2) ユーザポータルにログインします。ログイン方法は「4.1.3. ユーザポータルへのログイン」をご参照ください。

(3) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[キーペア]タブをクリックします。

(4) [公開鍵のインポート]ボタンをクリックします。

(5) 公開鍵のインポート画面で以下を入力、選択して[公開鍵のインポート]ボタンをクリックします。

・キーペア名　　：※任意
・鍵種別　　：SSH 鍵
・ファイルの選択：※作成した公開鍵を選択します。

(6) Web ブラウザで秘密鍵のダウンロードが開始されるため、ダウンロードします。
※この鍵を利用して仮想マシンにアクセスするため、紛失、漏洩品用に注意して保管してください。

(7) キーペアの登録が完了すると一覧に登録したキーペアが表示されます。

4.1.5.2. 新規作成による登録

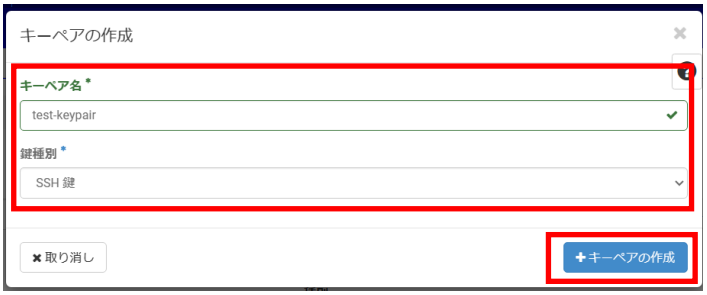
(1) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[キーペア]タブをクリックします。

(2) [キーペアの作成]ボタンをクリックします。

(3) 以下の項目を入力して[キーペアの作成]ボタンをクリックします。

・キーペア名：※任意

・鍵種別　　：SSH 鍵



(4) キーペアの登録が完了すると一覧に登録したキーペアが表示されます。

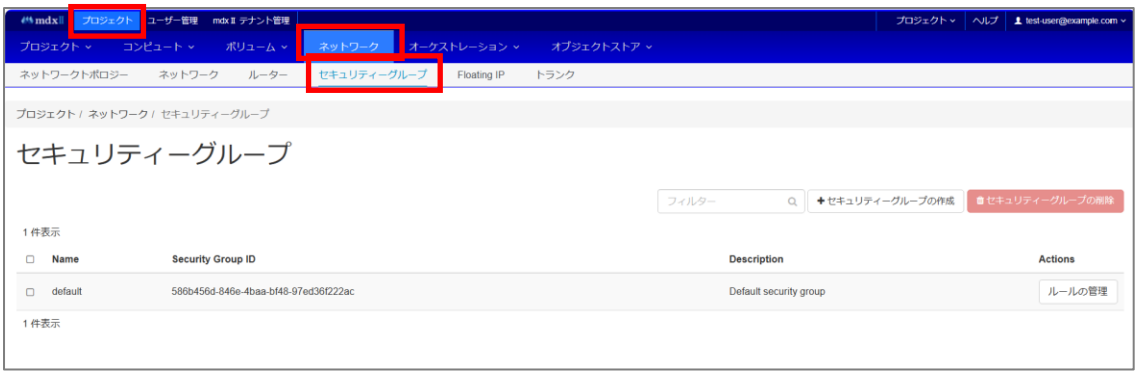
4.1.6. セキュリティグループの作成

セキュリティグループは、仮想マシンにおいて通信の送信/受信を制御する IP フィルタールールのセットです。

デフォルトでは「default」というセキュリティグループが用意されています。「default」はすべての送信トラフィックを許可し、同じセキュリティーグループの仮想マシン以外の送信元からの着信トラフィックをすべて拒否します。

セキュリティグループはプロジェクト用に新規に作成することも可能です。以下は新規に作成して ICMP と SSH を許可するルールを適用する手順を記載しています。

(1) [プロジェクト]メニュー ＞ [ネットワーク]パネル ＞ [セキュリティグループ]タブをクリックします。



(2) [+セキュリティグループの作成]ボタンをクリックします。

(3) [+セキュリティグループの作成]ボタンをクリックします。

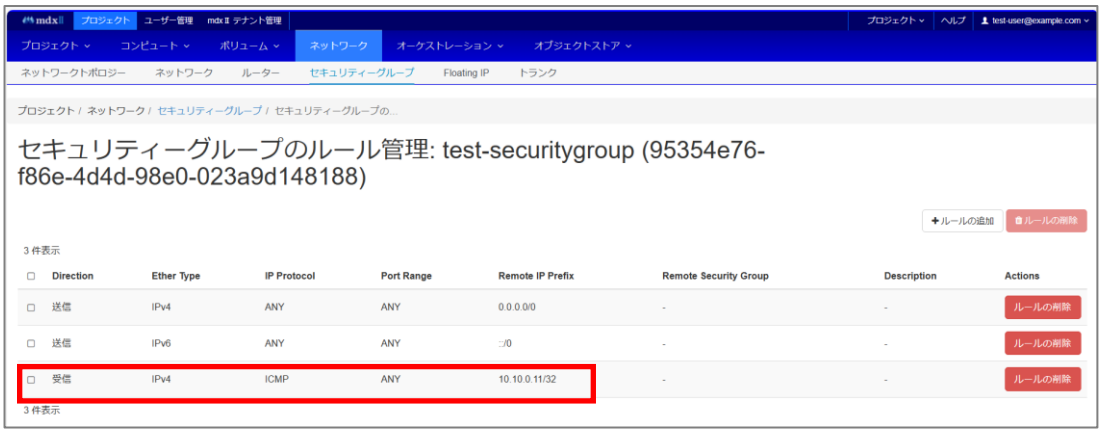
(4) [+ルールの追加]ボタンをクリックします。

(5) 以下の項目を入力して[追加]ボタンをクリックします。

・ルール：カスタム ICMP ルール

・CIDR ：※許可するアクセス元の IP アドレスを記載します。

(6) 作成した ICMP のルールが一覧に表示されます。



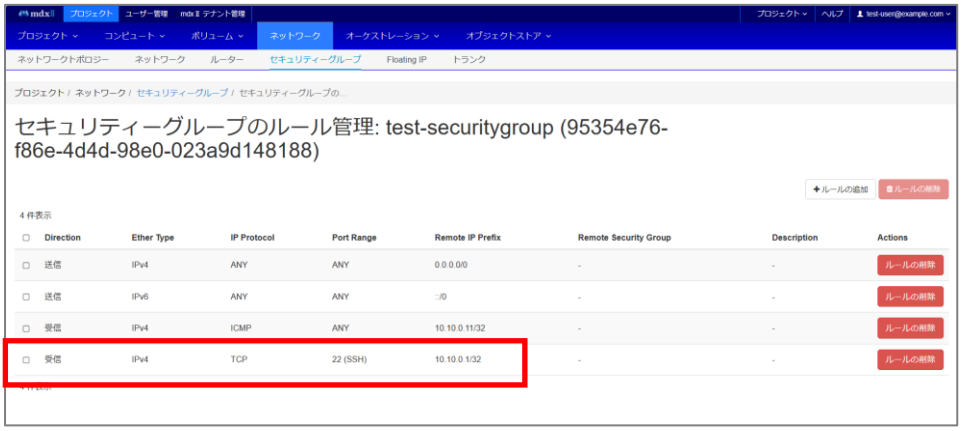
(7) [+ルールの追加]ボタンをクリックします。

(8) 以下の項目を入力して[追加]ボタンをクリックします。

・ルール：SSH

・CIDR ：※許可するアクセス元の IP アドレスを記載します。

(9) 作成した SSH のルールが一覧に表示されます。



4.1.7. 仮想マシンの作成

(1) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[インスタンス]タブをクリックします。

(2) [インスタンスの起動]ボタンをクリックします。

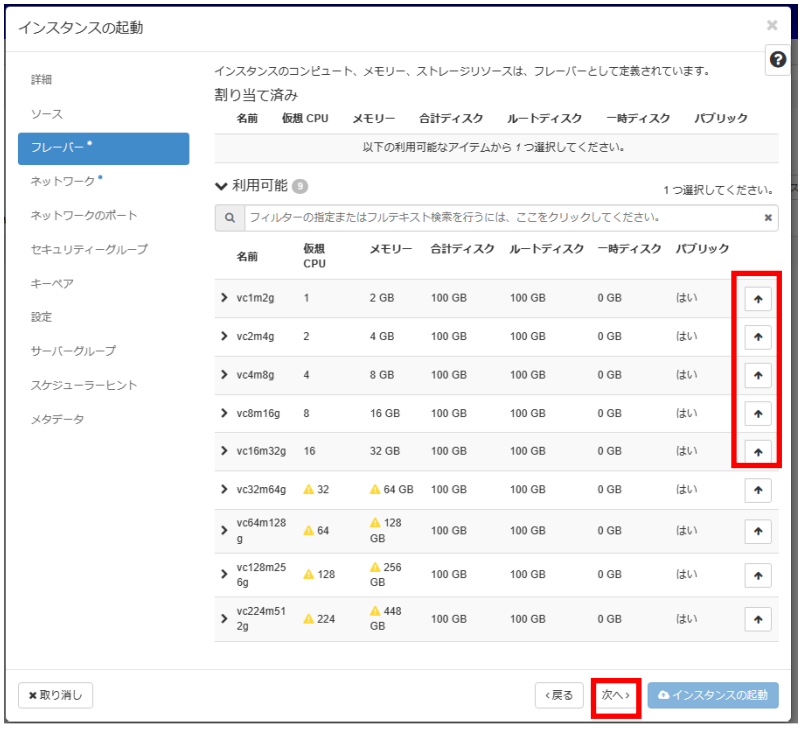
(3) 以下の項目を入力して[次へ]ボタンをクリックします。

・インスタンス名：※任意

(4) 利用可能欄から仮想マシンの OS イメージとするイメージの[↑]ボタンをクリックします。 [次へ]ボタンをクリックします。システム側で用意している OS イメージは RockyLinux 9.3 と Ubuntu 22.04 Server になります。

(5) 仮想マシンに割り当てる資源量として選択するフレーバーの[↑]ボタンをクリックして[次へ]ボタンをクリックします。**Lustre マウントを利用する場合は vc8m16g 以上のフレーバーを選択してください。**

※黄色の三角マークが表示されているフレーバーは、プロジェクトのクォータを超過しているため利用できません。



(6) 仮想マシンに接続するネットワークの[↑]ボタンをクリックして[セキュリティーグループ]タブをクリックします。

(7) 仮想マシンに適用するセキュリティーグループを選択します。デフォルトでは[default]が適用されています。作成したセキュリティーグループに変更する場合は選択するセキュリティーグループの[↑]ボタンをクリックし、[default]の[↓]ボタンをクリックします。
セキュリティーグループの選択後に[次へ]ボタンをクリックします。
※複数選択が可能です。

(8) 仮想マシンに登録するキーペア(SSH 公開鍵)を選択します。登録済みのキーペアが 1 つの場合は、デフォルトで選択されます。複数のキーペアがある場合は[↑][↓]ボタンで登録するキーペアを選択してください。選択後、[インスタンスの作成]ボタンをクリックします。

(9) インスタンスの一覧で作成した仮想マシンが表示され、Status が「稼働中」であることを確認します。

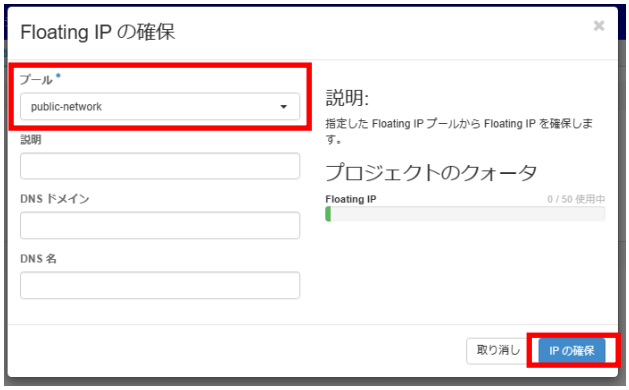
4.1.8. Floating IP の付与

Floating IP を仮想マシンに割り当てることで、インターネット等の外部ネットワークとの通信を有効にすることができます。

(1) [プロジェクト]メニュー ＞[ネットワーク]パネル ＞[Floating IP]タブをクリックします。

(2) [Floating IP の確保]ボタンをクリックします。

(3) [プール]のプルダウンメニューから「public-network」を選択して[IP の確保]ボタンをクリックします。

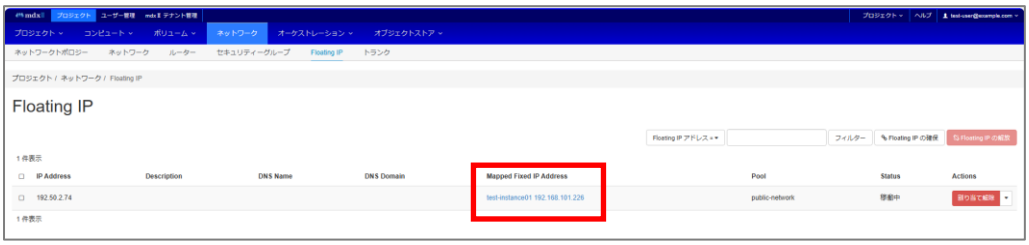


(4) Floating IP の一覧で確保した IP アドレスが表示されます。

(5) [割り当て]ボタンをクリックします。

(6) IP を割り当てるポートのプルダウンメニューで Floating IP を割り当てる仮想マシンを選択して、[割り当て]ボタンをクリックします。

(7) 一覧の Mapped Fixed IP Address に割り当てた仮想マシン名と Floating IP が表示されていることを確認します。



4.1.9. 仮想マシンへのアクセス

仮想マシンに割り当てた Floating IP あてに SSH でアクセスします。SSH アクセスには仮想マシン作成時に指定したキーペアの秘密鍵を指定します。SSH でアクセスするコマンドは以下になります。

```
$ ssh -i <SSH 秘密鍵> -l <初期ユーザ名> <仮想マシンの Floating IP>

例)
$ ssh -i ~/.ssh/id_rsa_mdx -l mdxuser   192.50.3.74
```

※システム側で用意している RockyLinux9.3 と Ubuntu 22.04 LTS の OS イメージから仮想マシンを作成した場合、初期ユーザ名は「mdxuser」になります。

※仮想マシンに SSH アクセスできない場合、セキュリティグループで必要な通信が許可されていることを確認してください。

4.1.10. ファイルサーバ領域の利用

仮想マシンからファイルサーバの領域を利用することが可能です。利用方法として以下の 2 つがあります。

- Cinder ボリュームを利用
  - Lustre マウントより容易にファイルサーバ領域を利用可能
  - 1 つの Cinder ボリュームは 1 つの仮想マシンのみ接続可能
  - 利用可能な容量はプロジェクトのクォータ（資源量の制限値）の範囲内

- 仮想マシンから Lustre マウントで利用
  - Cinder ボリュームの利用よりアクセス性能が高い
  - 利用にはシステム管理者への申請と Lustre クライアントの設定が必要
  - 利用可能な容量はプロジェクトのクォータとは別に申請時に指定

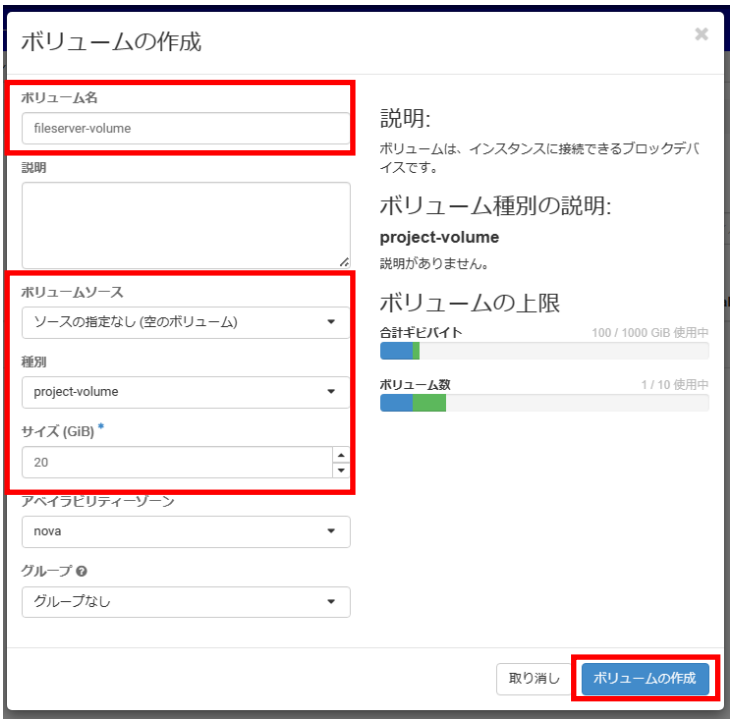
それぞれの利用に合わせて、以下の手順を実施してください。

4.1.10.1. Cinder ボリュームの利用

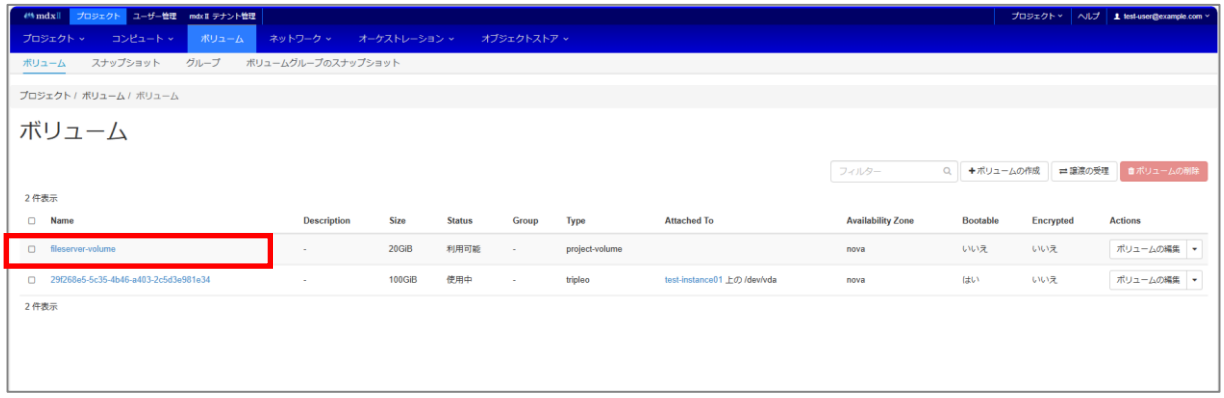
(1) [プロジェクト]メニュー ＞[ボリューム]パネル ＞[ボリューム]タブをクリックします。

(2) 以下の項目を入力して[ボリュームの作成]ボタンをクリックします。
※[種別]ではデフォルトが「tripleo」になっていますが、必ず「project-volume」を選択してください。

・ボリューム名：※任意
・ボリュームソース：ソースの指定なし（空のボリューム）
・種別：project-volume
・サイズ：※利用したい容量をクォータの範囲内で指定　・



(3) ボリュームの一覧に作成したボリュームが表示されます。

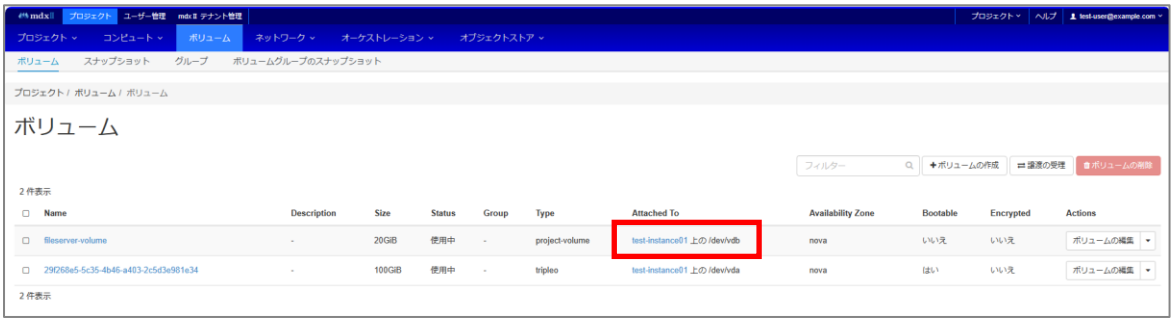


(4) 作成したボリュームの右側にあるプルダウンメニューから[接続の管理]をクリックします。

(5) 以下の項目を入力して[ボリュームの接続]ボタンをクリックします。

・インスタンスへの接続：※ボリュームを接続するインスタンスを指定

(6) ボリューム一覧の Attached To でボリュームを接続した仮想マシン名とデバイス名が表示されることを確認します。



仮想マシンへのボリュームの接続手順は以上になります。

接続したボリュームは仮想マシンから上記で確認したデバイス名(例:/dev/vdb)で見えます。ボリュームの中身は空の状態のため、用途に応じてファイルシステムの作成が必要になります。

以下の手順は接続したボリュームを XFS のファイルシステムとして利用する例を記載しています。

```
# mkfs -t xfs /dev/vdb
# mkdir /data
# mount -t xfs /dev/vdb /data
```

4.1.10.2. Lustre マウント

システム管理者あてに以下の情報を記載の上、メールにて Lustre マウントの利用を申請してください。

```
----- Lustre マウント利用申請フォーマット -----
プロジェクト名              ：※プロジェクト名を記載
仮想マシンの IP アドレス  ：※仮想マシンに割り当てられた IP アドレス(192.168.[100,101].X)
利用容量                    ：※GB 単位で記載
-------------------------------------------------
```

※上記の情報をもとにシステム管理者にてファイルサーバに必要な情報を設定します。

システム管理者から Lustre マウントの利用可能の通知がきた後、仮想マシンで Lustre クライアントの設定が必要になります。システム側で用意している RokcyLinux 9.3 と Ubuntu 22.04 LTS の OS イメージでは Lustre クライアントのパッケージと設定ファイルが組み込まれています。

以下はシステム側が用意した OS イメージで作成した仮想マシンで Lustre マウントする方法を記載しています。

(1) 仮想マシンにログインして sudo su などで root アカウントに切り替えます。

(2) 仮想マシンで Lustre 用ネットワークの IP アドレス(192.168.[100,101].X)が設定されているインターフェース名を確認します。

```
# ip address show
…省略…
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc fq_codel state UP gro
up default qlen 1000
…省略…
```

(3) /etc/modprobe.d/lustre.conf でインターフェース名の指定を確認したインターフェース名に修正します。※太字箇所を修正します。

```
# vi /etc/modprobe.d/lustre.conf
options lnet networks=tcp(eth0)
options lnet lnet_transaction_timeout=100
options ksocklnd rx_buffer_size=16777216
options ksocklnd tx_buffer_size=16777216
options ksocklnd conns_per_peer=8
options ksocklnd nscheds=8
```

(4) lustre_client ファイルでインターフェース名の指定を確認したインターフェース名に修正します。
Rocky Linux（RHEL 系）と Ubuntu Server ではファイルパスが異なります。
※太字箇所を修正します。

- Rocky Linux の場合

```
# vi /etc/sysconfig/lustre_client
…省略…
#++++++++++++++++++++++++++++++++++++++
# LNET Interface
#
IF1=eth0
…省略…
```

- Ubuntu Server の場合

```
# vi /etc/lustre_client
…省略…
#++++++++++++++++++++++++++++++++++++++
# LNET Interface
#
IF1=eth0
…省略…
```

(5) lustre_client.service を起動します。

```
# systemctl start lustre_client.service
```

(6) Lustre マウントができていることを確認します。

```
# df -h -t lustre
Filesystem                                                  Size  Used Avail Use% Mounted on
10.10.0.16@tcp:10.10.0.18@tcp:10.10.0.17@tcp:10.10.0.19@tcp:/lustre  503T  520G  497T   1% /lustre
```

(7) 仮想マシンの OS 起動時に自動で Lustre マウントするように lustre_client.service の自動起動を有効にします。(任意)

```
# systemctl enable lustre_client.service
```

Lustre クライアントの設定手順は以上になります。
ファイルサーバ領域でデータを扱う場合は Lustre マウントした「/lustre」のディレクトリをご利用ください。

4.2. ファイルサーバ

4.2.1. S3 アクセス方法

ファイルサーバは S3 アクセス用サーバ備えます。ファイルサーバの S3 エンドポイントは下記です。

S3 エンドポイント： s3gwlustre.osaka.mdx.jp

自身のローカルデータをファイルサーバ上に同期し、rclone コマンド（後述）やオンラインストレージサービスからアクセスするためには、アクセスキー・シークレットキーの作成およびユーザが接続する S3 バケットの作成が必要です。

これらの設定には、ファイルサーバの S3 アクセス用サーバでの作業が含まれるため、システム管理者に設定を依頼します。S3 利用を希望される場合は下記のフォーマットで依頼メールをお送りください。

宛先メールアドレス　：mdx2-system@cmc.osaka-u.ac.jp
件名　　：ファイルサーバ S3 アクセスのための接続情報構成依頼

```
システム管理者各位

ファイルサーバへの S3 アクセス設定を依頼します。

氏名：
プロジェクト名：
ユーザ名：
UID：
GID：
バケット名：
```

・バケット名：半角英数で任意に設定

CLI で S3 にアクセスする方法として rclone があります。rclone でリモートからファイルサーバ上のバケットに接続するために次のパッケージをインストールします。（Rocky の場合）

```
$ sudo dnf install rclone
```

rclone コマンドで S3 アクセスするためには、接続情報を設定する必要があります。次のコマンドで対話的に設定の追加・編集・削除の操作を行うことができます。

```
$ rclone config
```

下記では数字選択式に接続情報を新たに設定しています。設定を完了するには接続先 S3 のアクセスキーとシークレットキーが必要です。

```
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
```

n/s/q> **n**

name> **nec03-lustre**

Option Storage.

Type of storage to configure.

Enter a string value. Press Enter for the default ("").

Choose a number from below, or type in your own value.

（略）

4 / Amazon S3 Compliant Storage Providers including AWS, Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio, SeaweedFS, and Tencent COS

　￥"s3"

（略）

Storage> **4**

Option provider.

Choose your S3 provider.

Enter a string value. Press Enter for the default ("").

Choose a number from below, or type in your own value.

（略）

14 / Any other S3 compatible provider

　￥"Other"

provider> **14**

Option env_auth.

Get AWS credentials from runtime (environment variables or EC2/ECS meta data if no env vars).

Only applies if access_key_id and secret_access_key is blank.

Enter a boolean value (true or false). Press Enter for the default ("false").

Choose a number from below, or type in your own value.

1 / Enter AWS credentials in the next step.

　￥"false"

2 / Get AWS credentials from the environment (env vars or IAM).

　￥"true"

env_auth> **1**

Option access_key_id.

AWS Access Key ID.

Leave blank for anonymous access or runtime credentials.

Enter a string value. Press Enter for the default ("").

access_key_id> ******************

Option secret_access_key.

AWS Secret Access Key (password).

Leave blank for anonymous access or runtime credentials.

Enter a string value. Press Enter for the default ("").

secret_access_key> ******************

Option region.
Region to connect to.
Leave blank if you are using an S3 clone and you don't have a region.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 / Use this if unsure.
1 | Will use v4 signatures and an empty region.
 ¥ ""
 / Use this only if v4 signatures don't work.
2 | E.g. pre Jewel/v10 CEPH.
 ¥ "other-v2-signature"
region> us-east-1
Option endpoint.
Endpoint for S3 API.
Required when using an S3 clone.
Enter a string value. Press Enter for the default ("").
endpoint> s3gwlustre.osaka.mdx.jp
Option location_constraint.
Location constraint - must be set to match the Region.
Leave blank if not sure. Used when creating buckets only.
Enter a string value. Press Enter for the default ("").
location_constraint>
Option acl.
Canned ACL used when creating buckets and storing or copying objects.
This ACL is used for creating objects and if bucket_acl isn't set, for creating buckets too.
For more info visit https://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html#canned-acl
Note that this ACL is applied when server-side copying objects as S3
doesn't copy the ACL from the source but rather writes a fresh one.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value.
 / Owner gets FULL_CONTROL.
1 | No one else has access rights (default).
 ¥ "private"
 / Owner gets FULL_CONTROL.
 (略)
acl> 1
Edit advanced config?
y) Yes
n) No (default)

```
y/n> n
--------------------
[nec03-lustre]
type = s3
provider = Other
access_key_id = ***************
secret_access_key = ***************
region = us-east-1
endpoint = s3gwlustre.osaka.mdx.jp
acl = private
--------------------
```

上記で作成した接続設定で S3 にアクセスできることを確認します。次のコマンドではバケットに存在するファイル一覧を出力できます。

```
$ rclone ls nec03-lustre:
        40 nec03bct/hello.txt
104857600 nec03bct/testfile01
```

データを転送するためには例えば次のコマンドを用います。

```
$ rclone copy hello.txt nec03-lustre:nec03bct
```

4.3. mdx II オブジェクトストレージ

4.3.1. 利用申請

オブジェクトストレージ申請管理画面でのオブジェクトストレージの利用申請、オブジェクトストレージ申請完了後のサイズの変更方法について記載します。

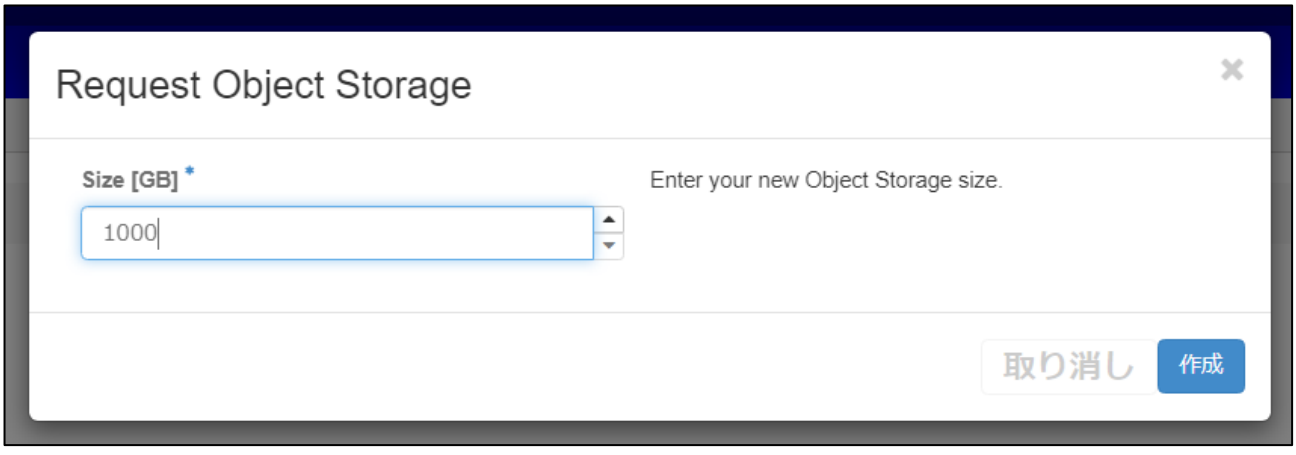
4.3.1.1. オブジェクトストレージ新規申請

OpenStaack にログイン後、画面上部のタブから下記のようにお進みください。
mdx II テナント管理 ＞ オブジェクトストレージ

オブジェクトストレージ申請管理画面では、新規オブジェクトストレージの申請が可能です。プロジェクトごとに申請できるオブジェクトストレージ数は 1 です。画面右側の「Request ObjectStorage」ボタンを押下してください。

「Request ObjectStorage」ボタンを押下すると、下図のようにサイズを入力するフォームが表示されます。申請するオブジェクトストレージのサイズ（GB）をご入力ください。

申請可能なサイズは、1,000 GB ~ 100,000 GB です。入力したサイズで申請する際は、「作成」ボタンを押下してください。



申請が完了すると申請情報がテーブルに表示されます。申請後 Status 列には「Request」が表示されます。オブジェクトストレージ設定の完了をお待ち下さい。最長で 10 分お待ちいただく可能性がございます。10 分を目安にページの更新/再ログインをお試しください。

オブジェクトストレージ設定が完了すると、Status 列は「OK」となり下図のように接続情報が払い出されます。Access key 列、Secret key 列にクレデンシャル情報が表示されていることをご確認ください。

また、Administrator 列、Initial password 列にはオブジェクトストレージ管理ユーザ情報が表示されます。こちらは、ProjectDataPortal 申請管理画面から申請する Nextcloud および LDAP Account Manager へのログインに必要となります。

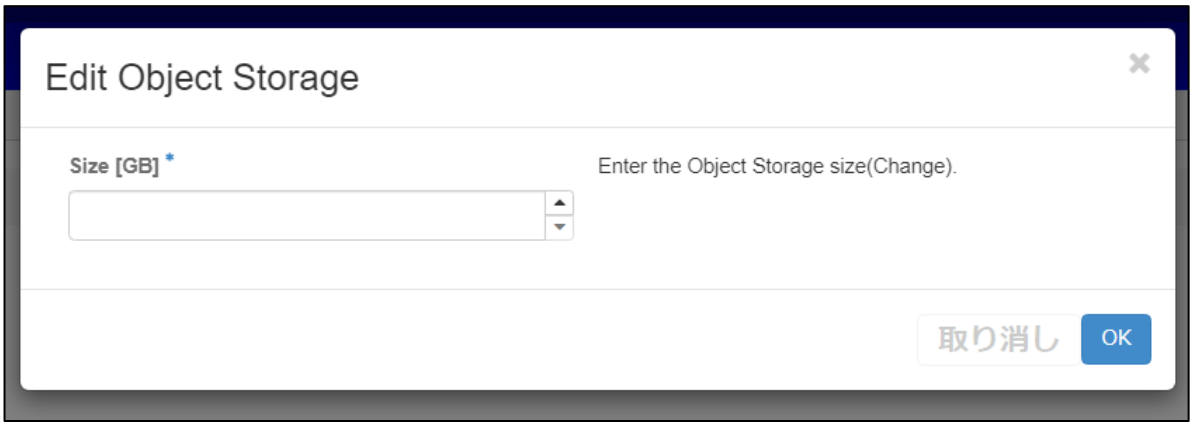
※ Initial password の値は固定で表示され続けます。初回ログイン後のパスワードご変更をお願いします。

※ 再ログインした際に、一時的に、ステータスが「Request」となり接続情報が表示されないことがあります。内部的にデータの更新を行っておりますので、2,3 分ほどお待ちいただき、タブを更新していただくと接続情報が表示されるようになります。

4.3.1.2. オブジェクトストレージのサイズ変更

オブジェクトストレージの設定完了後は、Actions 列から「編集」ボタンが利用可能となります。編集ボタンを押下すると、設定済みのオブジェクトストレージのサイズ変更申請を行うことができます。編集ボタンを押下後、下記のサイズ変更申請用のフォームが表示されます。

すでに設定されているサイズから引き下げることはできず、拡張申請のみ可能です。申請可能なサイズ上限は 100,000 GB です。入力したサイズで変更申請する際は、「OK」ボタンを押下してください。



変更申請が完了すると変更されたサイズがテーブルの Size [GB]列に表示されます。申請後 Status 列には「OK」が表示されたままですが、**再度「編集」ボタンを押下することはお控えください。**2 分ほど待機

しページの更新/再ログインを行うと Status 列が「Edit」に更新されます。

オブジェクトストレージ設定の完了をお待ち下さい。最長で 10 分お待ちいただく可能性がございます。10 分を目安にページの更新/再ログインをお試しください。

オブジェクトストレージ設定が完了すると、Status 列は「OK」となります。変更申請前と接続情報の変化はございません。

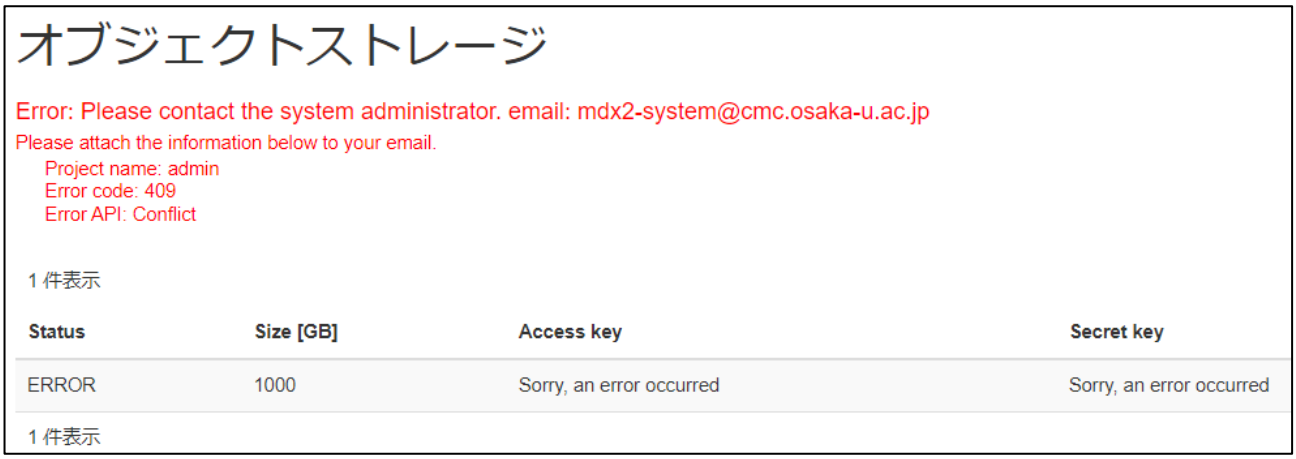
4.3.1.3. オブジェクトストレージの設定エラー

オブジェクトストレージの申請後、設定が完了するまでにオブジェクトストレージが API エラーを返すことがあります。エラーが発生した場合も再設定処理が行われ、設定が完了する場合もあります。

エラー発生時から 30 分お待ちいただいても状況が改善しない場合、恐れ入りますが下記アドレスにメールをいただけますようお願いいたします。

メールアドレス：mdx2-system@cmc.osaka-u.ac.jp

メール文面には表示されるエラー情報の添付をいただけますと、対処がスムーズに進む場合がございます。



4.3.2. 利用方法

オブジェクトストレージは従来型ストレージ（NAS など）にはない、高い拡張性を有するだけではなくファイル（以降、オブジェクト）を安全に保護・格納する多くの仕組みが実装されています。mdxII ではオブジェクトストレージとして Cloudian HyperStore（以降、HyperStore）を採用しています。

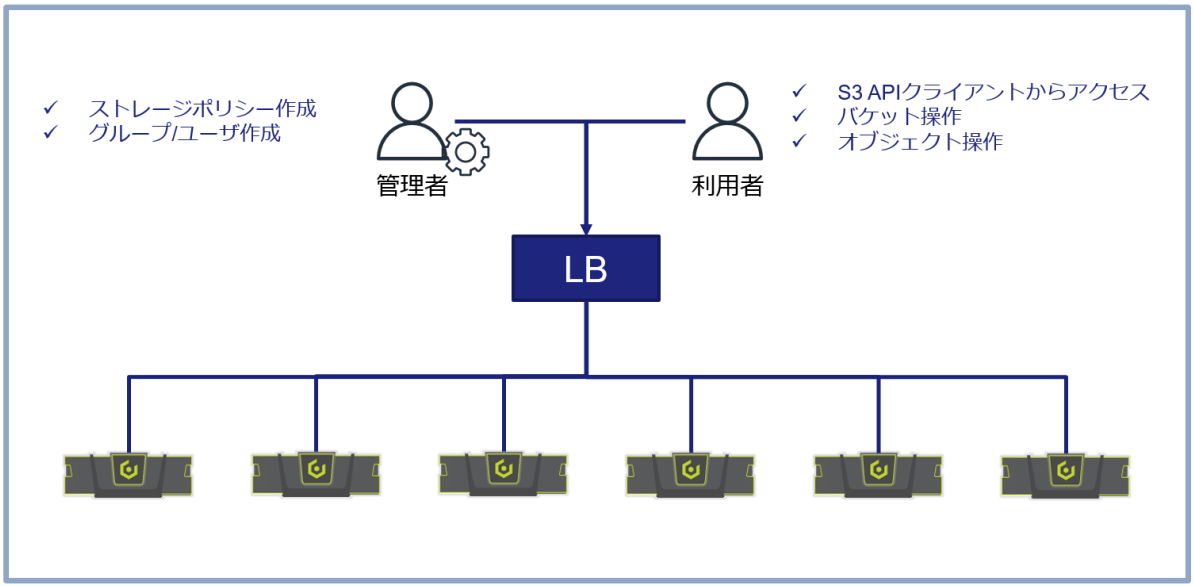
HyperStore はクラウドストレージの標準とも言える、Amazon S3 の API と高い互換性を有しており、Amazon S3 API に対応した様々なクライアントアプリケーションを介して、オブジェクトの操作を行うことができます。

HyperStore を操作するため Web GUI である Cloudian Management Console を利用することができます。

- HyperStore アクセスイメージ

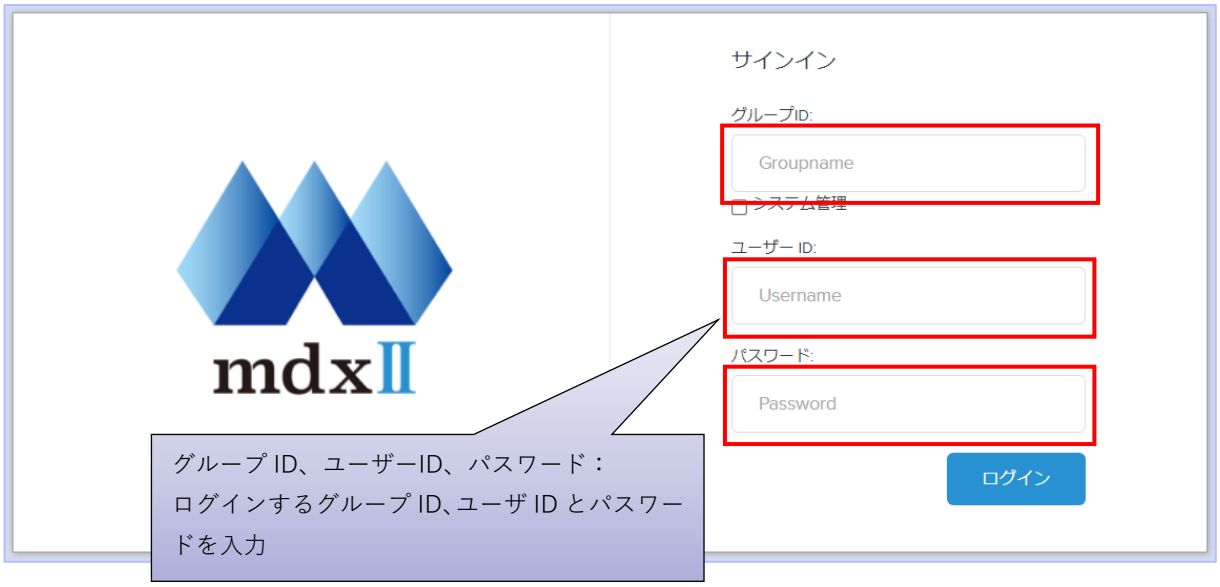
  HyperStore は IP ネットワーク（HTTP/HTTPS）経由でアクセスします。

  利用者は HyperStore に「バケット」と呼ばれる格納先を作成し、オブジェクト操作を実施します。



4.3.2.1. ログイン

ブラウザ（Chrome, FireFox 推奨）より、Cloudian Management Console「https://s3object-portal.osaka.mdx.jp:443」にアクセスします。

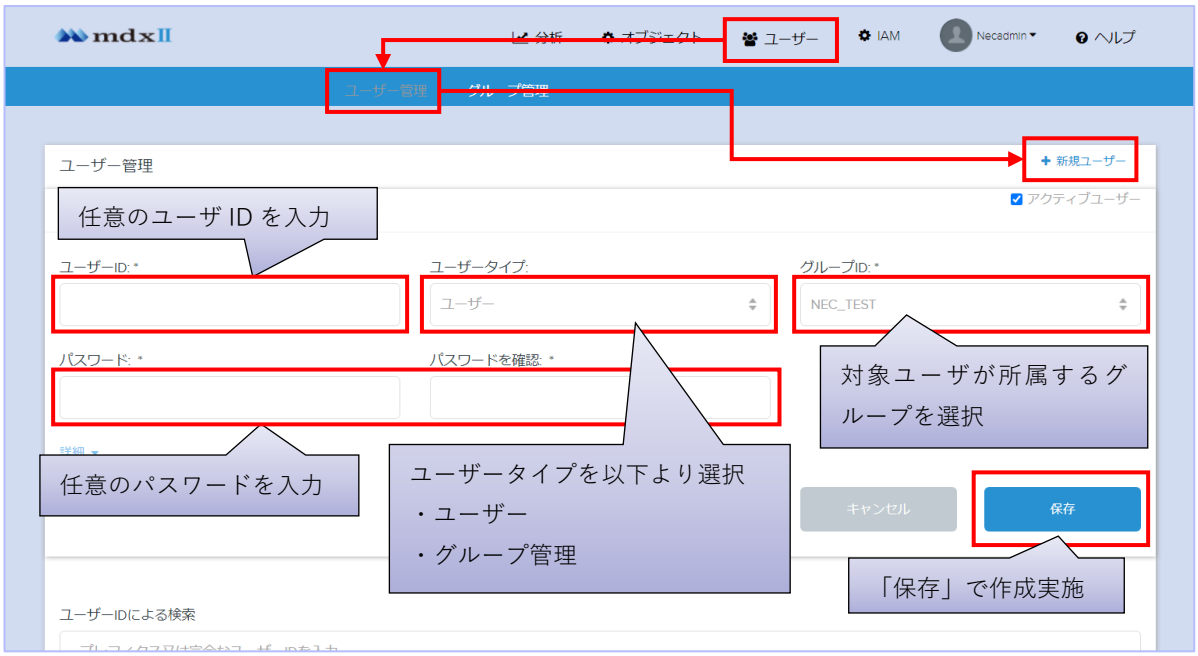


4.3.2.2. ユーザー作成

「ユーザー」メニュー ＞「ユーザー管理」タブ よりユーザー管理画面に遷移します。

「＋新規ユーザー」より、HyperStore を使用する為のユーザを作成します。

※　ユーザ作成はグループ管理者にて実施します。



4.3.2.3. ユーザクレデンシャルの取得

ユーザクレデンシャルは、各ユーザから確認できます。

画面右上の「ユーザ名」＞「セキュリティ証明書」 よりユーザクレデンシャル画面に遷移します。

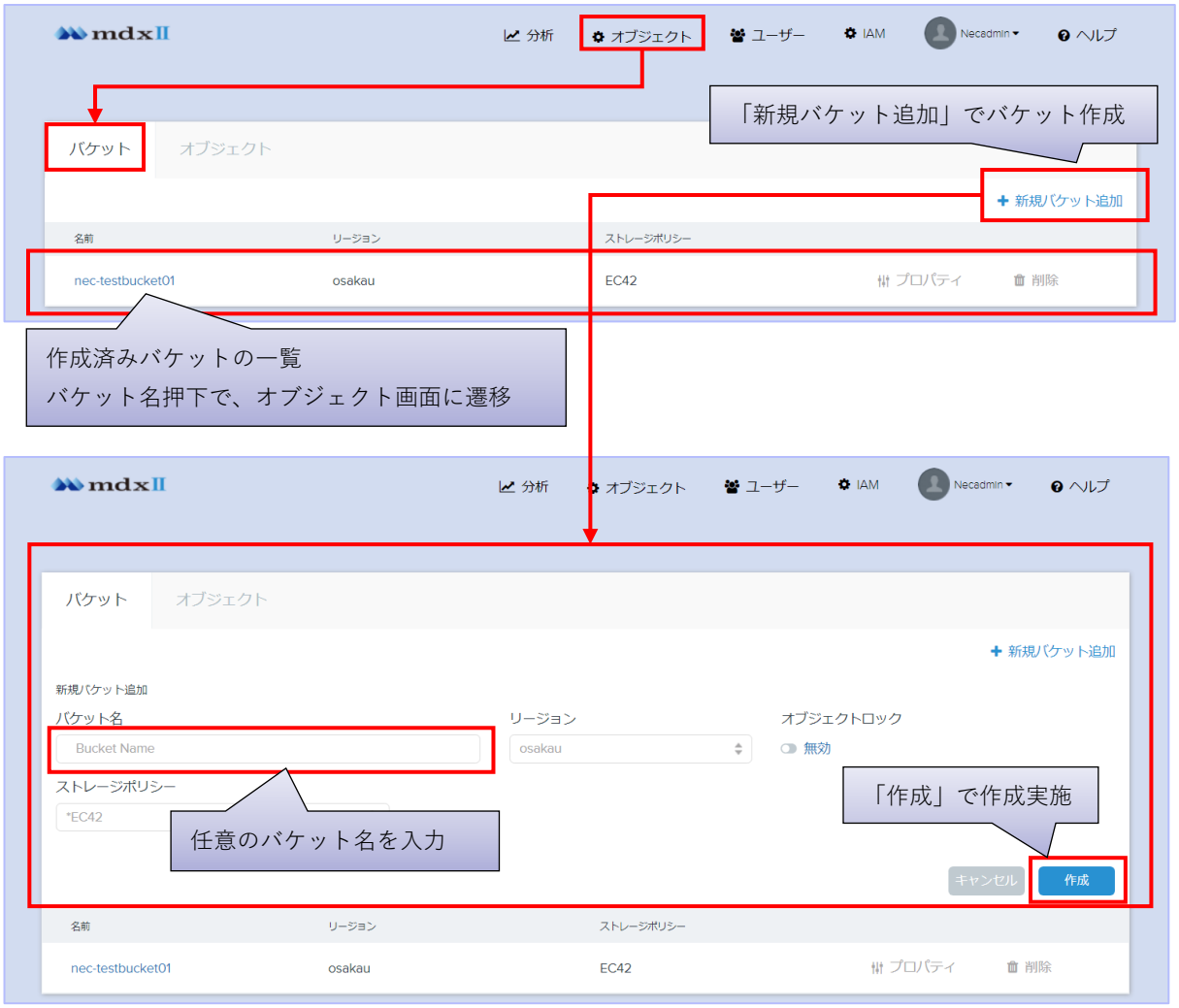
ユーザクレデンシャル（アクセスキーID、シークレットキー）は、クライアントシステムから S3 アクセスする場合に必要となります。

※　ユーザクレデンシャルは 1 ユーザあたり 5 つまで取得できます。（デフォルト値）

4.3.2.4. バケット作成

「バケット」と呼ばれるオブジェクトを格納する領域を作成します。

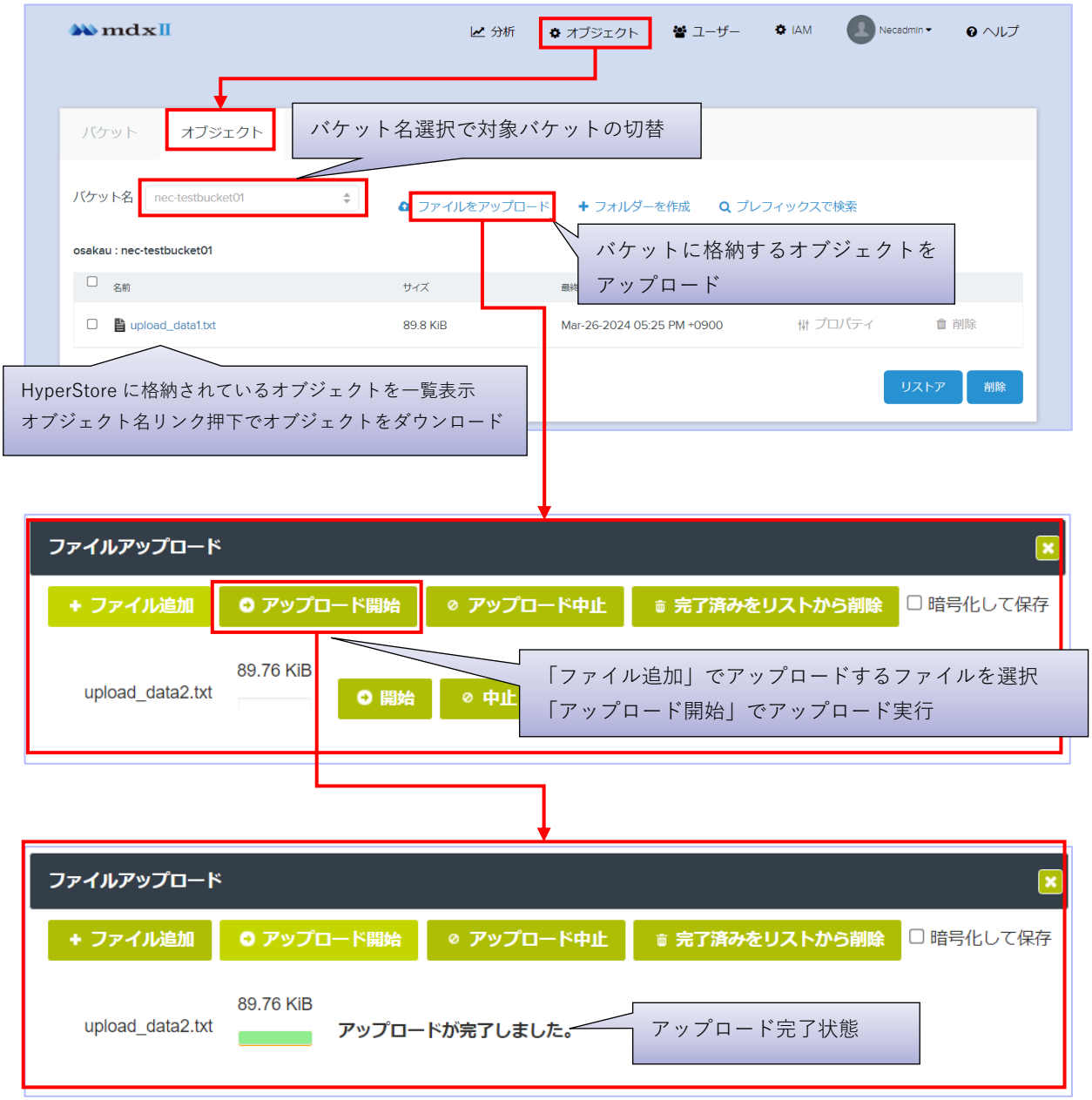
「オブジェクト」メニュー ＞「バケット」 よりバケット一覧画面に遷移し「＋新規バケット追加」押下で新規バケット追加画面を表示します。



4.3.2.5. オブジェクトの一覧表示・アップロード

オブジェクトの一覧表示やバケットへのアップロード等を行います。

「オブジェクト」メニュー ＞「オブジェクト」タブ よりオブジェクト一覧画面に遷移します。



4.3.2.6. ヘルプ

各メニューの操作方法については画面右上の「ヘルプ」メニューから確認することができます。

4.4. ProjectDataPortal

4.4.1. 利用申請

ProjectDataPortal 申請管理画面での、Nextcloud の利用申請方法について記載します。

オブジェクトストレージの設定完了後にはじめて ProjectDataPortal 申請が可能となります。オブジェクトストレージ利用申請方法は、4.3 mdx II オブジェクトストレージ の章をご参照ください。

OpenStaack にログイン後、画面上部のタブから下記のようにお進みください。

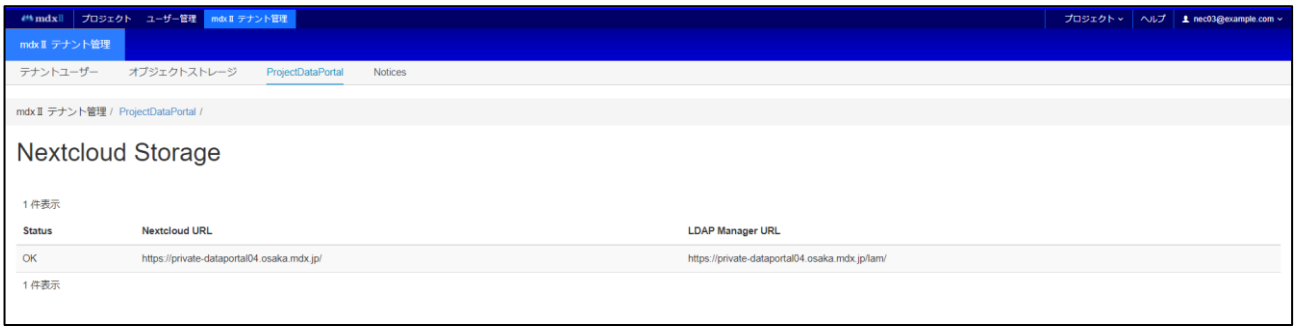
mdx II テナント管理 ＞ ProjectDataPortal

ProjectDataPortal 申請管理画面では、Nextcloud の利用申請が可能です。プロジェクトごとに申請できる数は 1 です。画面右側の「Request Nextcloud Storage」ボタンを押下してください。すると、確認用のモーダルで「Do you submit an application for Nextcloud storage?」のように問われます。よろしければ、「Submit」ボタンを押下してください。

申請が完了すると申請情報がテーブルに表示されます。申請後 Status 列には「Request」が表示されます。Nextcloud 設定の完了をお待ち下さい。最長で 10 分お待ちいただく可能性がございます。10 分を目安にページの更新/再ログインをお試しください。

Nextcloud の設定が完了すると、Status 列は「OK」となり下図のように接続情報が払い出されます。Nextcloud URL 列、LDAP Manager URL 列にそれぞれ URL 情報が表示されていることをご確認ください。

それぞれ Nextcloud および LDAP Account Manager への URL です。ログインにはオブジェクトストレージ申請管理画面の Administrator 列、Initial password 列の値をご入力ください。



Nextcloud の設定完了まで時間を要する可能性がございます。30 分お待ちいただいても情報が更新されない場合、恐れ入りますが下記アドレスにメールをいただけますようお願いいたします。

メールアドレス：mdx2-system@cmc.osaka-u.ac.jp

4.4.2. 利用方法

4.4.2.1. 事前準備

プロジェクト用データ転送用ポータルにログインするためには、Google Authenticator 等を利用した 2 段階認証を実施する必要があります。2 段階認証に必要となるアプリケーションを用意し、**ご自身の端末(スマートフォン等)にインストール**してください。

以下の 2 段階認証アプリケーションが使用できることを確認済みです。

OS	アプリケーション	備考
Android	Google Authenticator	Google Play ストア
iOS	Google Authenticator	Apple App Store
Windows	WinAuth	https://winauth.github.io/winauth/download.html
macOS	Step Two	Apple App Store

4.4.2.2. グループ管理者様作業

4.4.2.2.1. 2 段階認証の設定(Nextcloud)

(1) Web ブラウザを開き、プロジェクト用データ転送用ポータルの利用申請画面に表示された「Nextcloud URL」に接続します。

https://[テナント毎に設定される文字列].osaka.mdx.jp/

「アカウント名またはメールアドレス」および「パスワード」は、データ集約用オブジェクトストレージの利用申請画面に表示される「管理者アカウント」および「初期パスワード」を参照して入力してください。

(2) 「TOTP (Authenticator app) TOTP アプリで認証する」をクリックします。

(3) QR コードが表示されるので、事前準備で用意した 2 要素認証アプリを使用し、スキャンを行います。その後、アプリに表示された認証コードを入力し、「検証」をクリックします。

(4) 再度、「TOTP (Authenticator app) TOTP アプリで認証する」をクリックします。

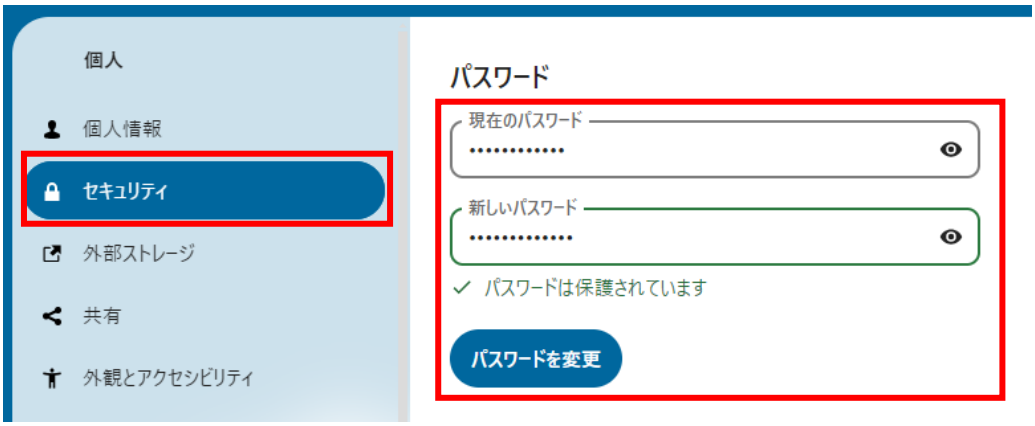
(5) 先ほどスキャンした QR コードに対応する認証コードを入力し、「送信」をクリックします。

(6) ログインに成功すると、ホーム画面が表示されます。

4.4.2.2.2. パスワードの変更(Nextcloud)

1. Nextcloud にログインします。
2. 右上のアイコンから、「個人設定」をクリックします。

3. 左側のメニューから「セキュリティ」をクリックし、パスワード入力画面を表示します。「現在のパスワード」「新しいパスワード」をそれぞれ入力し、「パスワードを変更」をクリックします。



4. パスワードを変更後、ログアウトします。右上のアイコンから「ログアウト」をクリックします。

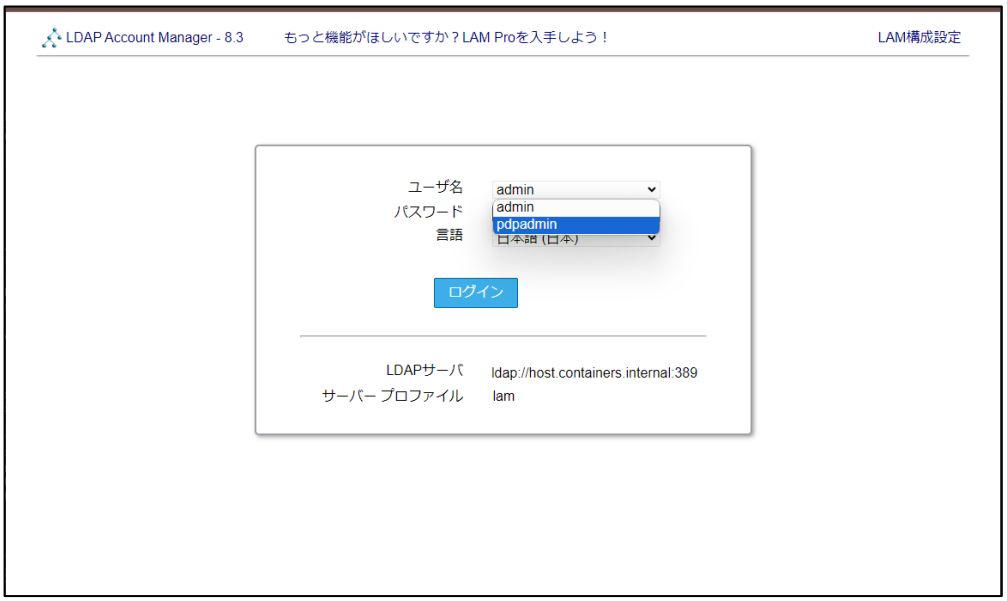
4.4.2.2.3. LDAP グループ管理者パスワード変更(LDAP Account Manager)

1. Web ブラウザを開き、プロジェクト用データ転送用ポータルの利用申請画面に表示された「Admin URL」に接続します。

   https://[テナント毎に設定される文字列].osaka.mdx.jp/lam/

   ※「lam」(エルエーエム)

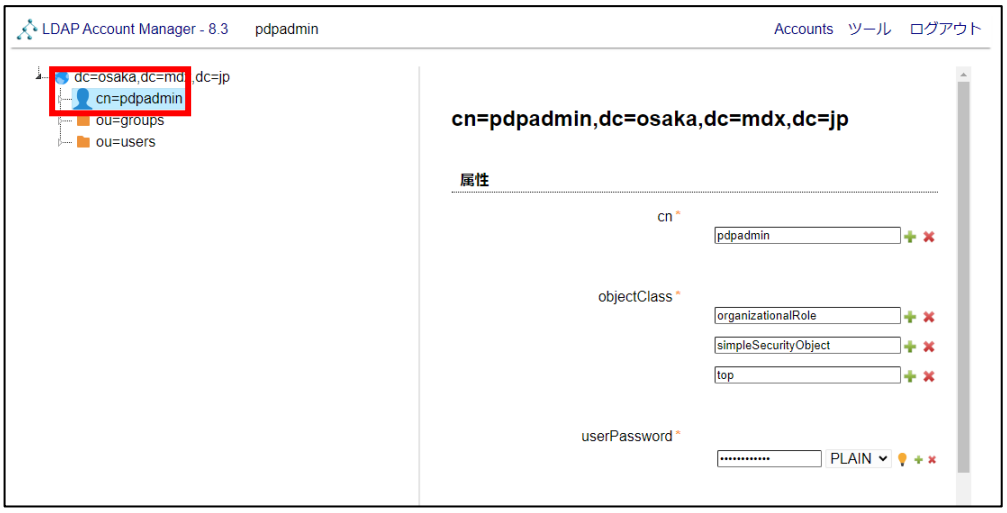
「ユーザ名」および「パスワード」は、データ集約用オブジェクトストレージの利用申請画面に表示される「管理者アカウント」および「初期パスワード」を参照して入力してください。



2. ログインに成功すると、ユーザ追加画面が表示されます。

3. 右上のツールから、ツリービューをクリックします。

4. 表示されたツリービューから、「cn=[ユーザ名]」をクリックします。



5. 右側の下方にある「userPassword」を入力します。
   ×ボタンで入力をクリアし、新しいパスワードを設定してください。
   入力が終わったら、「保存」をクリックします。(同じパスワードは設定できません)

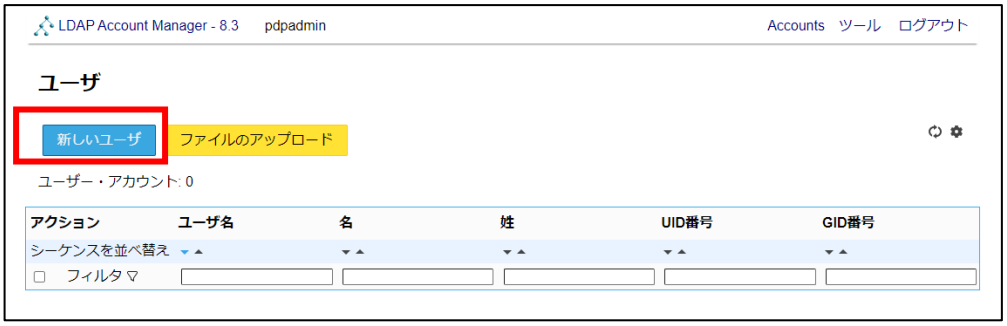
6. 特にメッセージは表示されませんので、右上の「ログアウト」をクリックしてこのままログアウトします。

4.4.2.2.4. 利用者の登録(LDAP Account Manager)

必要な入力項目は、以下の通りとなります。

タブ	入力項目	備考
Personal	姓	
	名	
	電子メールアドレス	
Unix	ユーザ名	Nextcloud のログイン ID になります。英数字(英字から始まる)で入力します。
パスワードを設定	パスワード	[OK]ボタンを必ずクリックしてください。

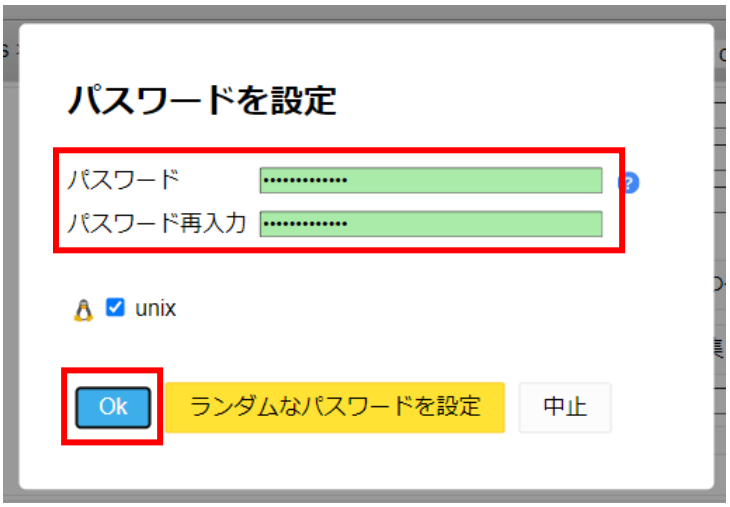
1. LDAP Account Manager にログインし、「新しいユーザ」をクリックします。



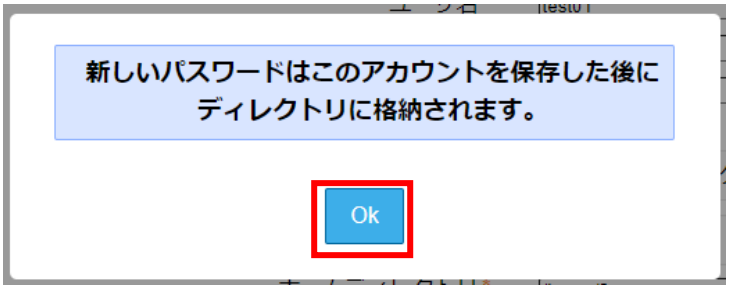
2. 「Personal」の情報を入力します。

3. 「unix」をクリックし、情報を入力します。

4. 「パスワードを設定」をクリックし、パスワードを入力して「OK」をクリックします。

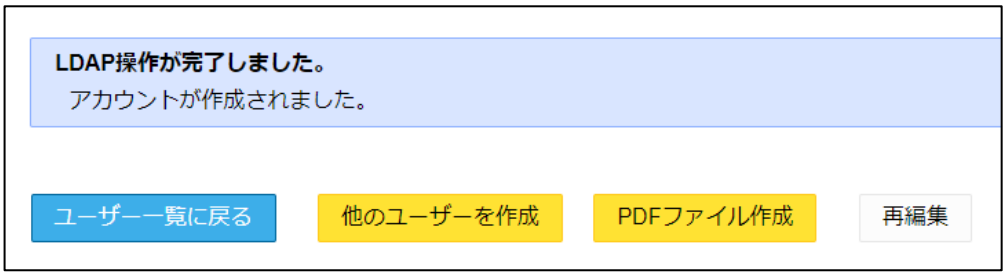


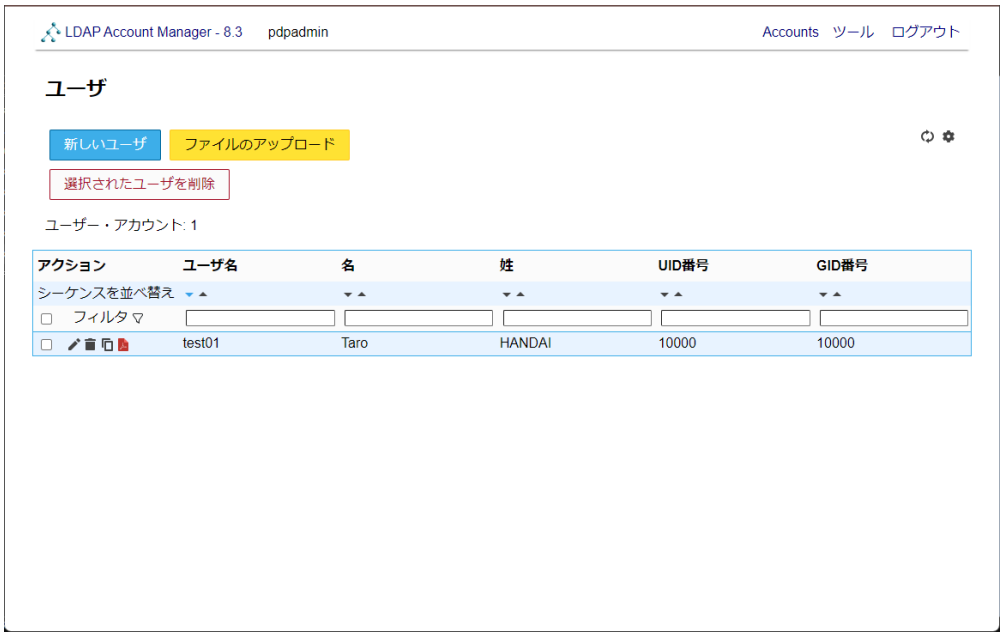
5. 確認ダイアログで、「OK」ボタンをクリックします。



6. 「保存」をクリックします。

7. 「アカウントが作成されました。」と表示され、ユーザー一覧に作成したユーザが表示されることを確認します。





以上で、利用者の登録は完了です。利用者に、Nextcloud の URL と登録したユーザ名およびパスワードを通知してください。

グループ管理者様の作業は以上です。

4.4.2.3. 利用者様作業

4.4.2.3.1. 2 段階認証の設定(Nextcloud)

1. Web ブラウザを開き、グループ管理者様から通知のあった Nextcloud URL に接続します。

https://[テナント毎に設定される文字列].osaka.mdx.jp/

「アカウント名またはメールアドレス」および「パスワード」は、グループ管理者様から通知された「ユーザ名」および「パスワード」を入力してください。

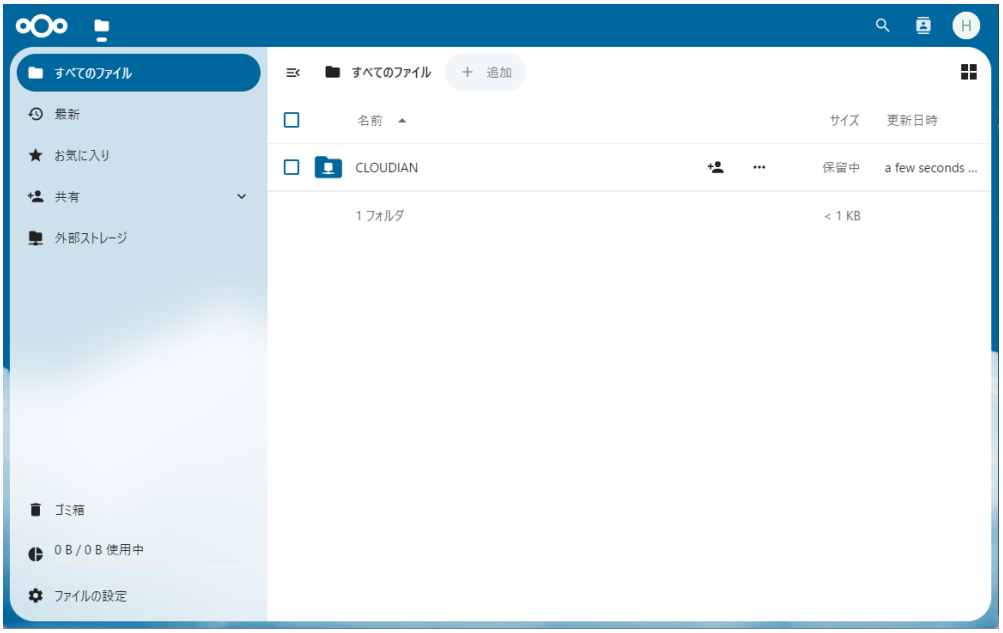
2. 「TOTP (Authenticator app) TOTP アプリで認証する」をクリックします。

3. QR コードが表示されるので、事前準備で用意した 2 要素認証アプリを使用し、スキャンを行います。その後、アプリに表示された認証コードを入力し、「検証」をクリックします。

4. 再度、「TOTP (Authenticator app) TOTP アプリで認証する」をクリックします。

5. 先ほどスキャンした QR コードに対応する認証コードを入力し、「送信」をクリックします。

6. ログインに成功すると、ホーム画面が表示されます。既にオブジェクトストレージ領域にユーザ領域が作成されている場合は、以下の様に「CLOUDIAN」ディレクトリにマウントして表示されます。



4.4.2.3.2. パスワードの変更(Nextcloud)

1. Nextcloud にログインします。
2. 右上のアイコンから、「設定」をクリックします。

3. 左側のメニューから「セキュリティ」をクリックし、パスワード入力画面を表示します。「現在のパスワード」「新しいパスワード」をそれぞれ入力し、「パスワードを変更」をクリックします。

4. パスワードを変更後、ログアウトします。右上のアイコンから「ログアウト」をクリックします。

4.4.2.3.3. トラブル対処方法

オブジェクトストレージ領域のユーザ専用領域が赤くなって使用できない

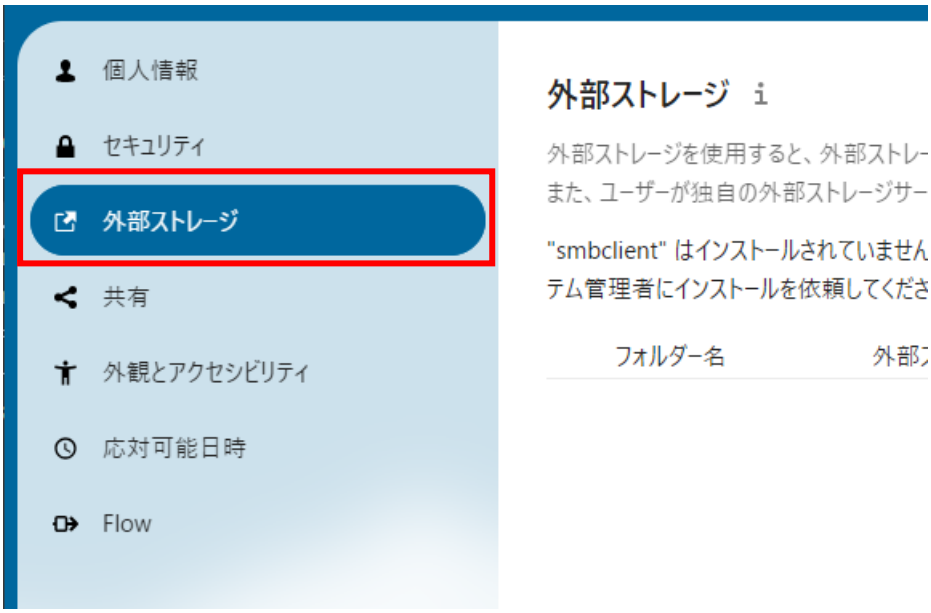
以下の様に CLOUDIAN フォルダが赤く表示されている場合、オブジェクトストレージ領域が使用できません。

この場合、一旦再マウント手順を実施してください。

再マウント手順

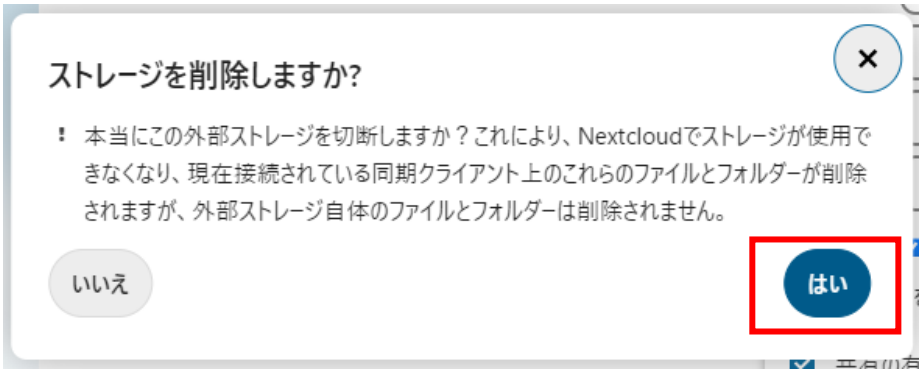
1. 右上のアイコンから「設定」をクリックします。

2. 左側メニューより「外部ストレージ」をクリックします。



3. 「…」アイコンをクリックし、表示されたメニューから「切断」をクリックします。

4. 確認メッセージが表示されるので、「はい」をクリックします。



5. 外部ストレージ情報がクリアされます。
   この手順を実施後、最大 10 分程度待つことにより、再度オブジェクトストレージ領域がマウントされます。

ユーザー専用領域フォルダが未作成

グループ管理者様が利用者の登録(4.4.2.2.4)を実施した後、オブジェクトストレージ領域のユーザ専用領域作成までに最大で 20 分程度掛かります。

4.5. myDataPortal

4.5.1. 利用申請

Nextcloud の外部ストレージ接続機能を用いて、S3 接続をサポートする Lustre ファイルシステムやオブジェクトストレージと接続できます。外部ストレージ間でのデータ転送にご利用ください。myDataPortal は大量のデータ格納を意図しておりません。容量の逼迫の原因となるため、データ転送の目的でのご使用をお願いします。

ご利用を希望の場合は、システム管理者宛に以下の情報をご記載の上、メールにてご申請ください。

宛先メールアドレス　：mdx2-system@cmc.osaka-u.ac.jp
件名　　：myDataPortal 新規利用申請

システム管理者各位

myDataPortal の利用を申請します。

氏名：
プロジェクト名：
ユーザ名：
メールアドレス：

- 「プロジェクト名」はプロジェクト申請フォームで申請したプロジェクト名をご記載ください。
- 「ユーザ名」は Nextcloud 上に登録されるユーザ名です。半角英数でご記載ください。
- 「メールアドレス」は Nextcloud 上に登録されるメールアドレスです。

4.5.2. ログイン

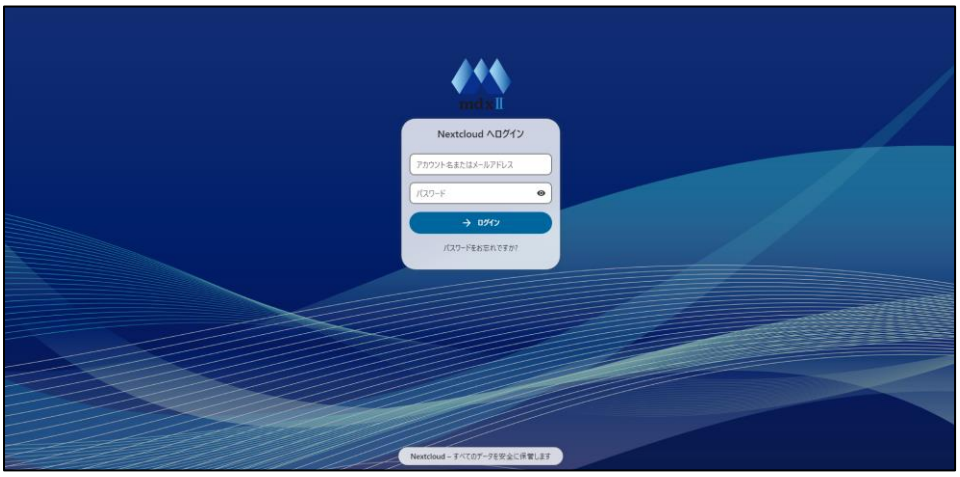
Nextcloud へのログインには、パスワード認証と OTP（ワンタイムパスワード）認証の 2 要素認証が求められます。OTP の登録ができるよう、**あらかじめ Google Authenticator などのモバイルアプリやブラウザの OTP 拡張機能をご用意いただくようお願いいたします。**

システム管理者からユーザ登録完了通知メールを受信した後、Nextcloud へのログインが可能になります。メールには下記の情報が含まれます。

- ユーザ名
- 初期パスワード
- メールアドレス
- グループ名

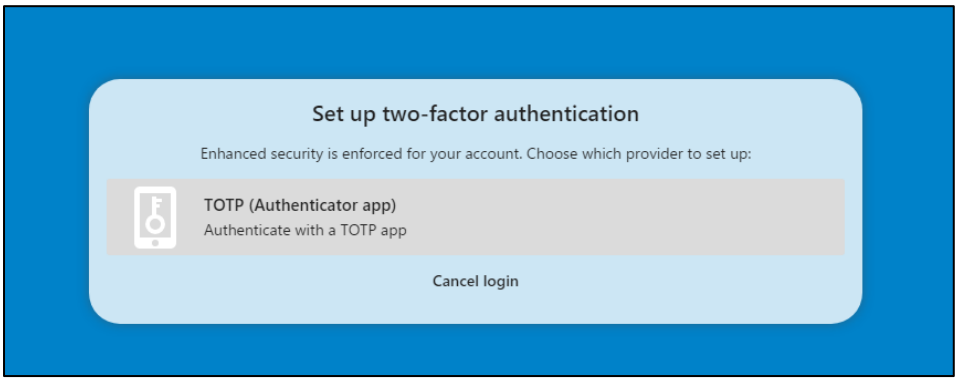
下記の URL にアクセスします。

URL：https://dataportal.osaka.mdx.jp/



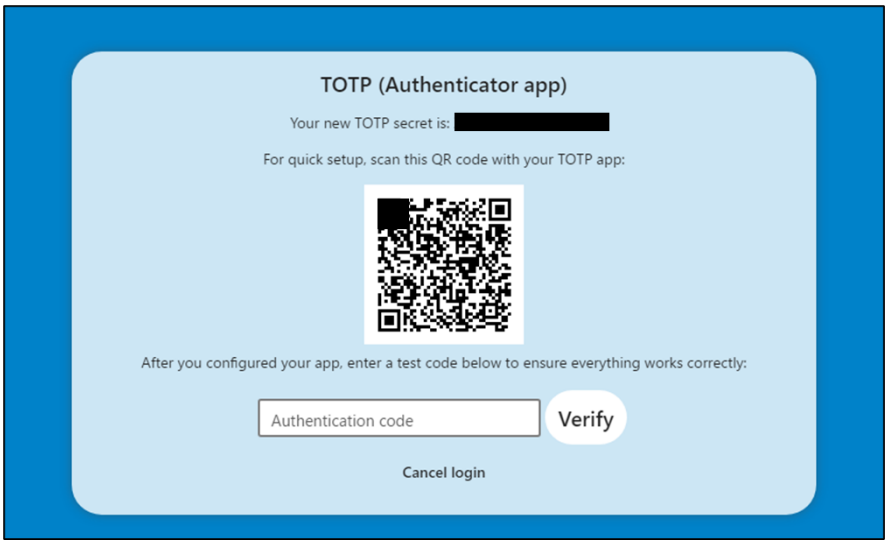
ログイン画面の入力欄に、ユーザ登録完了通知メールに記載のユーザ名と初期パスワードを入力します。

認証完了後、「Set up two-factor authentication」との表示があります。OTP 登録用のアプリをご準備のうえ、「TOTP」を選択します。

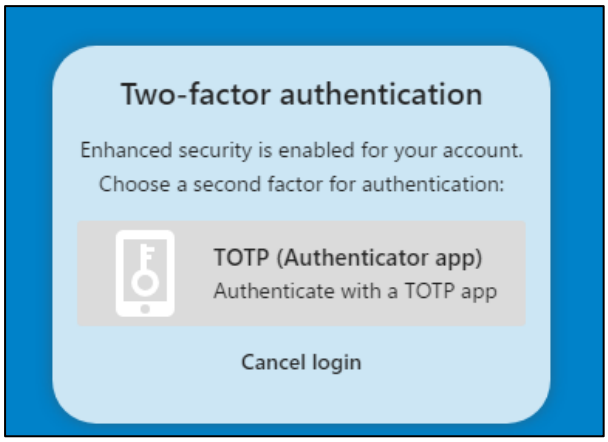


OTP 登録用のアプリで表示される URL を読み込む、または「TOTP secret」の値を用いて OTP を登録します。OTP 登録用アプリに表示される 6 桁の数字を「Authentication code」欄に入力し、「Verify」ボタンを押下します。

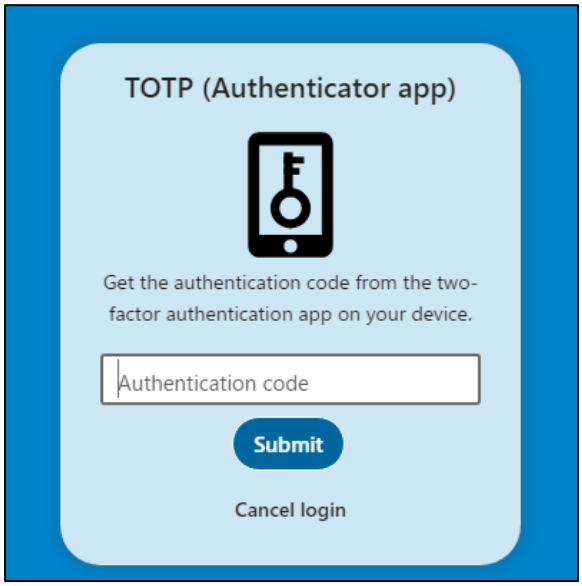
※　**QR コードおよびシークレットキーは初回ログイン時にのみ表示されます。**OTP の登録を忘れずに行ってください。



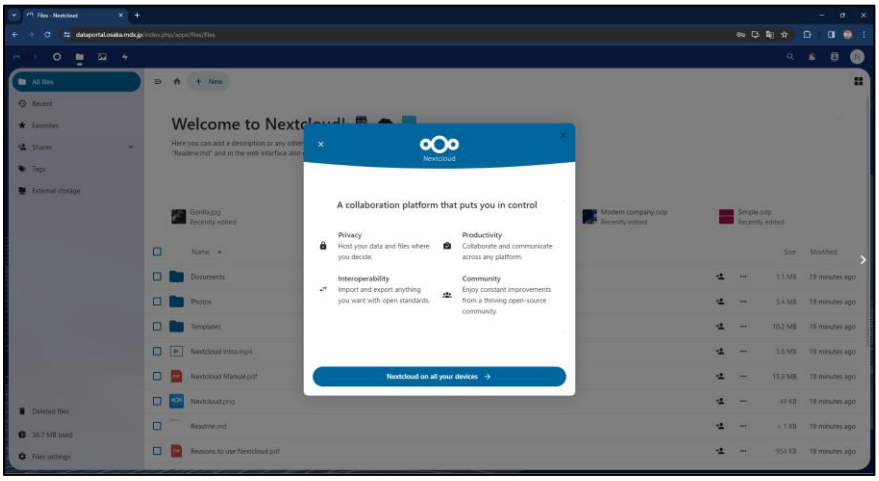
再度、認証方法の選択を要求されますので、「TOTP」を選択します。



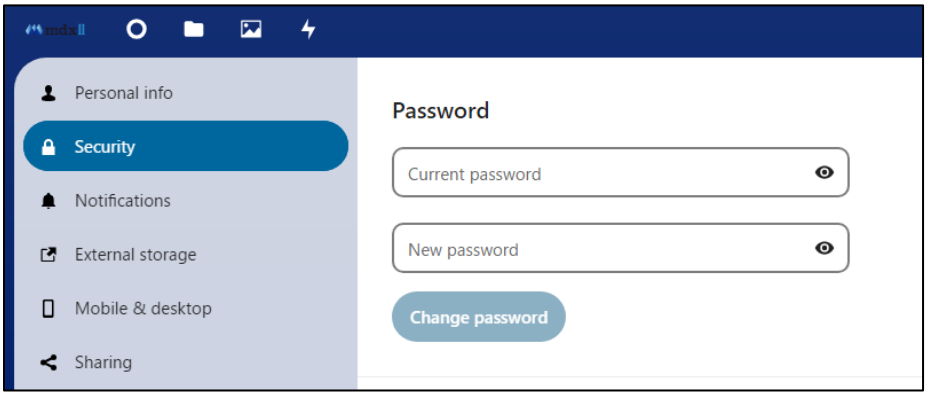
最後に、認証のための OTP 入力欄が表示されます。OTP 登録用アプリに表示される 6 桁の数字を「Authentication code」欄に入力し、「Submit」ボタンを押下します。



ログイン成功後、ダッシュボードが表示されます。



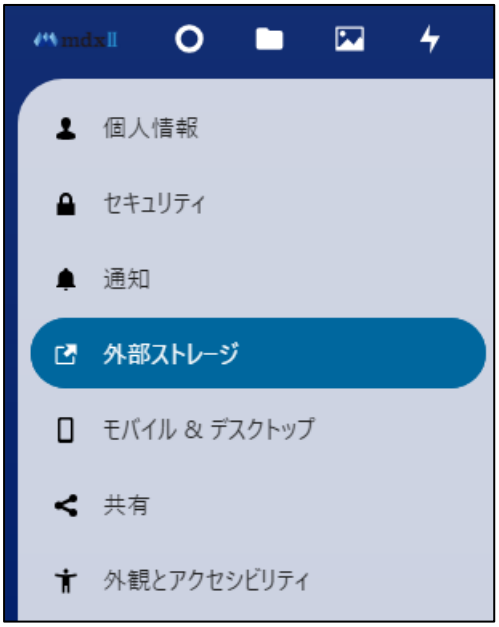
初期パスワードの変更を行います。ユーザアイコンの「Settings」を押下し、個人設定画面に移動します。左ペインの「Security」から上部の「Password」より変更をお願いします。



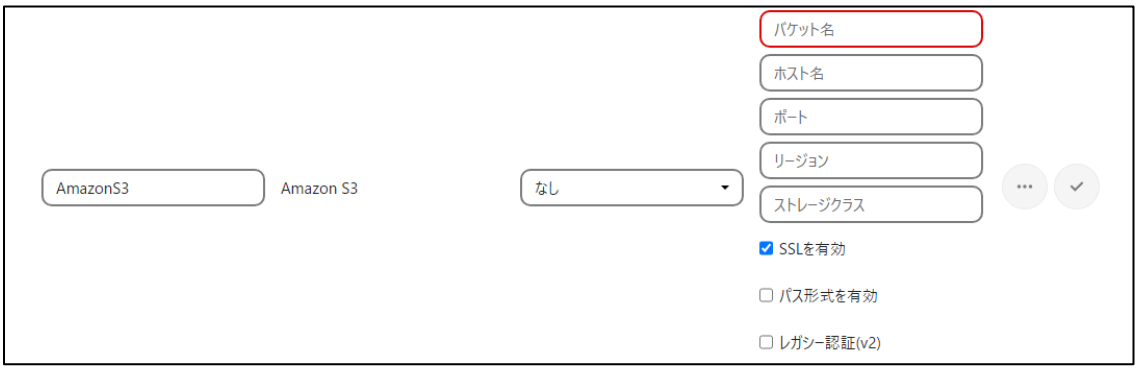
左ペインの「Personal Info」からは、言語等の設定を行うことができます。

4.5.3. 利用方法

Nextcloud では、外部ストレージ接続機能（外部ストレージプラグイン）を利用することで、S3 をサポートするオンラインストレージと接続することができます。ユーザアイコンの「設定」を押下し、左ペインの「外部ストレージ」を選択します。



外部ストレージ列の「ストレージを追加」プルダウンから「Amazon S3」を選択します。



4.5.3.1. Lustre ファイルシステム接続設定

下図および下表は接続情報の設定例です。

項目	設定例	説明
フォルダ名	AmazonS3-Lustre	任意
外部ストレージ	Amazon S3	Amazon S3 のみ選択可。
認証	アクセスキー	アクセスキーを選択。
バケット名	nec03bct	接続するバケット名。
ホスト名	s3gwlustre.osaka.mdx.jp	S3 エンドポイントを入力。例は本システムファイルサーバの S3 サーバエンドポイント。
ポート	443	指定がある場合は入力。
リージョン	us-east-1	指定がある場合は入力。
ストレージクラス	-	S3 ストレージクラス。未入力の場合はデフォルトの「STANDARD」クラスが設定。
SSL を有効	チェック	SSL を有効にする場合はチェック。
パス形式を有効	チェック	パス形式でアクセスする場合はチェック。
レガシー認証	-	レガシー認証を行う場合はチェック。
アクセスキー	**********	接続先のアクセスキー。
シークレットキー	**********	接続祭のシークレットキー。

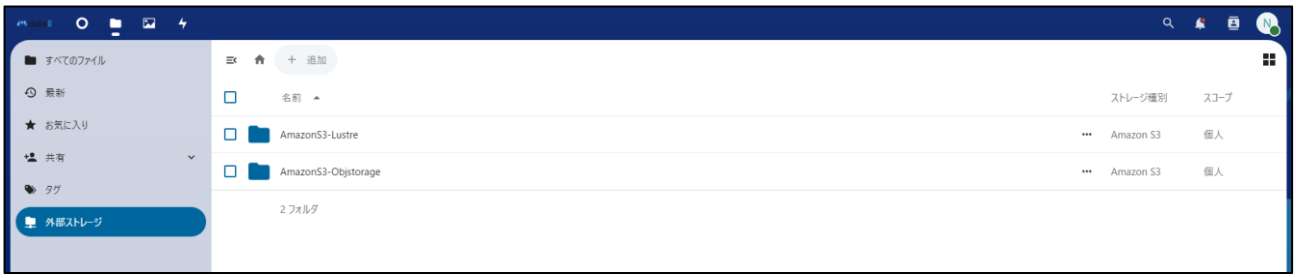
4.5.3.2. オブジェクトストレージ接続設定

下図および下表は接続情報の設定例です。

項目	設定例	説明
フォルダ名	AmazonS3-Objstorage	任意
外部ストレージ	Amazon S3	Amazon S3 のみ選択可。
認証	アクセスキー	アクセスキーを選択。
バケット名	mdxdepl-dz1tfw5bvbegz4kpl2vn	接続するバケット名。
ホスト名	s3-osakau.osaka.mdx.jp	S3 エンドポイントを入力。例は本システムオブジェクトストレージの S3 サーバエンドポイント。
ポート	443	指定がある場合は入力。
リージョン	osakau	指定がある場合は入力。
ストレージクラス	-	S3 ストレージクラス。未入力の場合はデフォルトの「STANDARD」クラスが設定。
SSL を有効	チェック	SSL を有効にする場合はチェック。
パス形式を有効	-	パス形式でアクセスする場合はチェック。
レガシー認証	-	レガシー認証を行う場合はチェック。
アクセスキー	**********	接続先のアクセスキー。
シークレットキー	**********	接続祭のシークレットキー。

4.5.3.3. 外部ストレージの利用

画面上部のファイルタブからご自身のストレージにアクセス可能です。左ベインの「外部ストレージ」より、設定したストレージを操作することができます。大容量のデータをローカル領域に保持し続けると容量逼迫の原因になる可能性がございます。



4.6. 相互運用ノード（VMware）

4.6.1. 利用申請

システム管理者宛に以下の情報を記載の上、メールにてご申請ください。
また、仮想マシンには公開鍵認証で接続するため、使用する公開鍵をメールに添付してください。

青文字部分はコメント

```
----- 相互運用ノード利用申請フォーマット -----
プロジェクト名                  :
氏名                            :
所属機関名                      :
連絡先メールアドレス            :
請求先担当者氏名                :
請求先担当者メールアドレス      :
請求先担当者電話番号            :
請求先担当者所属機関名          :
利用仮想マシン数                :
  仮想マシン N   ※N は数字で 1 から記載。利用仮想マシン数分、以下の項目を記載。
    利用 OS                     :※RockyLinux/Ubuntu Server/ユーザ持参のテンプレートから選択
    CPU パック数                :  ※1CPU パックあたり「1CPU コア+メモリ 2GiB」
    ボリューム容量              :  ※GB 単位で記載
    グローバル IP 数            :  ※SSH アクセス用に 1 つは必須。
-------------------------------------------------
```

以下は記載例

```
----- 相互運用ノード利用申請フォーマット -----
プロジェクト名                  :test-project
氏名                            :テスト太郎
所属機関名                      :テスト大学 1
連絡先メールアドレス            :xxxx@xxx.com
請求先担当者氏名                :テスト次郎
請求先担当者メールアドレス      :xxxx@xxx.com
請求先担当者電話番号            :xx-xxxx-xxxx
請求先担当者所属機関名          :テスト大学 2
利用仮想マシン数                :3
  仮想マシン 1
    利用 OS                     :Rocky Linux
    CPU パック数                :2
    ボリューム容量              :100GB
    グローバル IP 数            :1
  仮想マシン 2
```

利用 OS　　：**Ubuntu Server**
CPU パック数　　：**2**
ボリューム容量　　：**100GB**
グローバル IP 数　　：**1**
仮想マシン 3
利用 OS　　：**ユーザ持参のテンプレート**
CPU パック数　　：**10**
ボリューム容量　　：**2000GB**
グローバル IP 数　　：**1**

4.6.2. 利用方法

SSH コマンドまたはターミナルソフトウェアを用いて、公開鍵認証方式で仮想マシンに SSH 接続します。SSH 接続する際に使用する公開鍵は、事前にシステム管理者に送付しておく必要があります。
※仮想マシンに設定されている IP アドレスを変更すると仮想マシンに接続できなくなるため変更しないでください。

(1) 初回 SSH アクセス

UNIX 系 OS(Linux、macOS)からのログイン

ssh コマンドを使います。仮想マシンに ログインする例は以下の通りです。

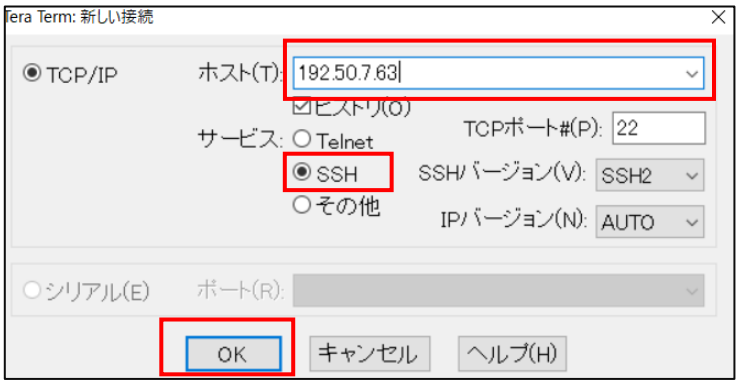
```
$ ssh mdxuser@<仮想マシンの IP アドレス>
The authenticity of host '<仮想マシンの情報>' can't be established.
RSA key fingerprint is 32:fd:73:4e:7f:aa:5d:3c:2e:ab:37:83:d6:55:98:e2.
Are you sure you want to continue connecting (yes/no)? yes
Warning Permanently added '<仮想マシンの情報>' to the list of known hosts.
Enter passphrase for key '<秘密鍵のパスフレーズ>':
```

Windows マシンからのログイン

フリーソフトウェア 「Tera Term Pro」 を用いた例を説明します。

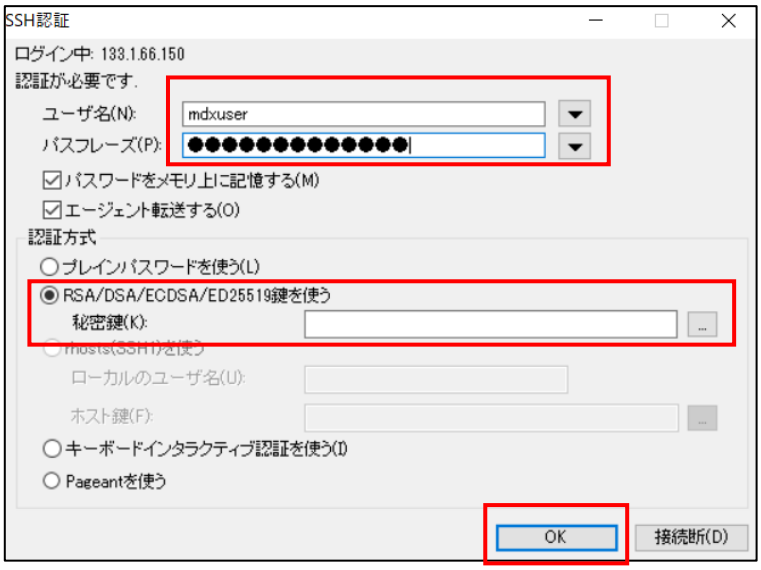
「Tera Term Pro」 を起動し、「Tera Term: New connection ダイアログ」において

・ TCP/IP を選択します。
・ホスト欄に仮想マシンの IP アドレスを入力 します。
・サービスは SSH を選択します。
・ OK をクリックします。



・SSH 認証画面で認証方式として「RSA/DSA/ECDSA/ED25519 鍵を使う」を選択し、作成した秘密鍵を選択します。

・ユーザ名と作成した鍵のパスフレーズを入力し、OK をクリックします



4.6.3. Lustre マウント

システム管理者あてに以下の情報を記載の上、メールにて Lustre マウントの利用を申請してください。

```
----- Lustre マウント利用申請フォーマット -----
プロジェクト名          ：※プロジェクト名を記載
仮想マシンの IP アドレス ：※仮想マシンに割り当てられた IP アドレス(172.16.10.X)
利用容量                ：※GB 単位で記載
-------------------------------------------------
```

※上記の情報をもとにシステム管理者にてファイルサーバに必要な情報を設定します。

システム管理者から Lustre マウントの利用可能の通知がきた後、仮想マシンで Lustre クライアントの設定が必要になります。システム側で用意している RokcyLinux 9.3 と Ubuntu 22.04 LTS の OS イメージでは Lustre クライアントのパッケージと設定ファイルが組み込まれています。

以下はシステム側が用意した OS イメージで作成した仮想マシンで Lustre マウントする方法を記載しています。

(7) 仮想マシンにログインして sudo su などで root アカウントに切り替えます。

(8) 仮想マシンで Lustre 用ネットワークの IP アドレス(172.16.10.X)が設定されているインターフェース名を確認します。

```
# ip address show
…省略…
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc fq_codel state UP gro
up default qlen 1000
…省略…
```

(9) /etc/modprobe.d/lustre.conf でインターフェース名の指定を確認したインターフェース名に修正します。※太字箇所を修正します。

```
# vi /etc/modprobe.d/lustre.conf
options lnet networks=tcp(eth0)
options lnet lnet_transaction_timeout=100
options ksocklnd rx_buffer_size=16777216
options ksocklnd tx_buffer_size=16777216
options ksocklnd conns_per_peer=8
options ksocklnd nscheds=8
```

(10) /etc/sysconfig/lustre_client でインターフェース名の指定を確認したインターフェース名に修正します。Rocky Linux（RHEL 系）と Ubuntu Server ではファイルパスが異なります。
※太字箇所を修正します。

- Rocky Linux の場合

```
# vi /etc/sysconfig/lustre_client
…省略…
#++++++++++++++++++++++++++++++++++++++
# LNET Interface
#
IF1=eth0
…省略…
```

- Ubuntu Server の場合

```
# vi /etc/lustre_client
…省略…
#++++++++++++++++++++++++++++++++++++++
```

```
# LNET Interface
#
IF1=eth0
…省略…
```

(11) lustre_client.service を起動します。

```
# systemctl start lustre_client.service
```

(12) Lustre マウントができていることを確認します。

```
# df -h -t lustre
Filesystem                                                  Size  Used Avail Use% Mounted on
10.10.0.16@tcp:10.10.0.18@tcp:10.10.0.17@tcp:10.10.0.19@tcp:/lustre  503T  520G  497T   1% /lustre
```

(13) 仮想マシンの OS 起動時に自動で Lustre マウントするように lustre_client.service の自動起動を有効にします。(任意)

```
# systemctl enable lustre_client.service
```

Lustre クライアントの設定手順は以上になります。

ファイルサーバ領域でデータを扱う場合は Lustre マウントした「/lustre」のディレクトリをご利用ください。

5. 機能説明

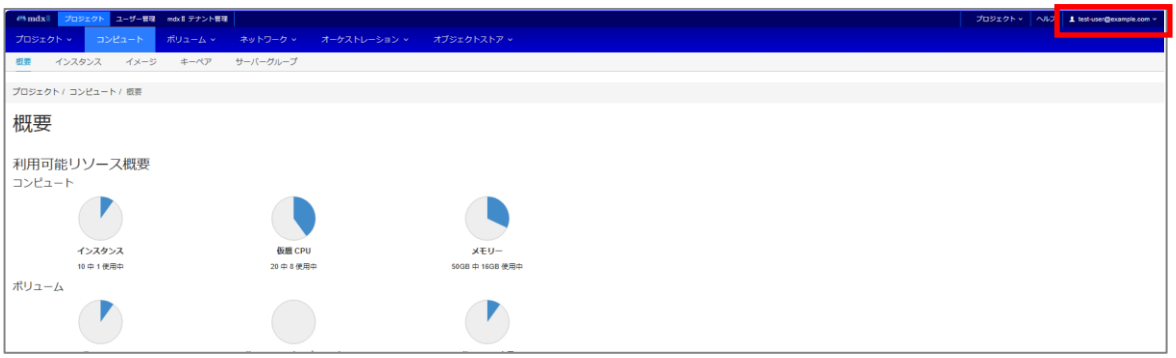
5.1. ユーザポータル

ユーザポータルは OpenStack の Dashboard で構成されます。ユーザポータルで利用可能な各種機能について本節で記載しています。

5.1.1. 言語変更

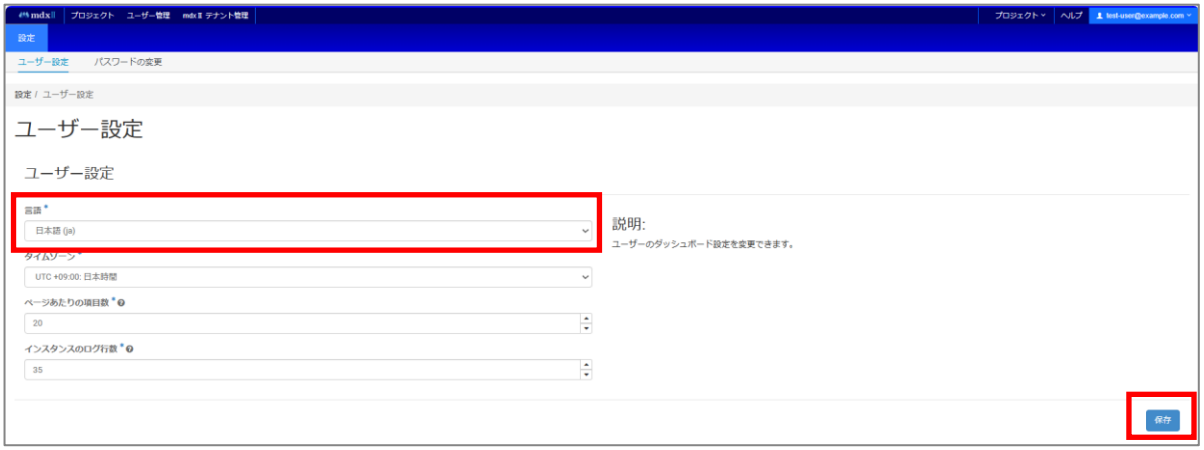
ユーザポータルでは言語設定の変更が可能です。

(1) Dashboard の右上にあるユーザ名箇所をクリックします。



(2) [設定]をクリックします。

(3) [言語]のプルダウンメニューで利用したい言語を選択して[保存]ボタンをクリックします。

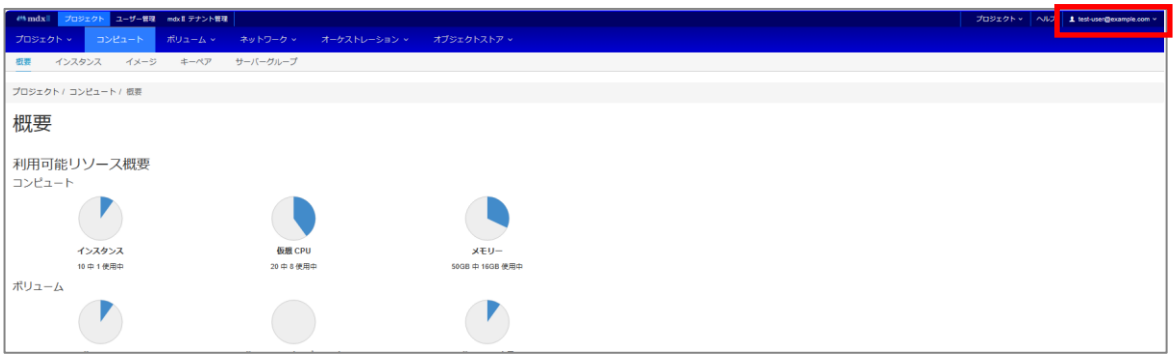


5.1.2. ローカルパスワードの変更

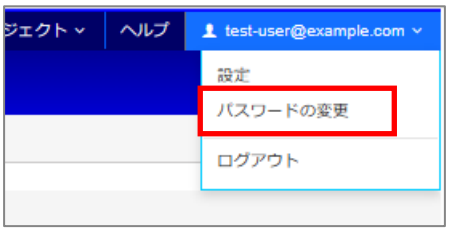
ローカルカウントをご利用の場合、ローカルパスワードの変更が可能です。

※学認アカウントをご利用の場合、プロジェクト申請時はローカルパスワードは発行されません。追加でローカルパスワードの発行を申請してパスワードをお持ちの場合は、本項に記載の手順でパスワードの変更が可能です。

(1) Dashboard の右上にあるユーザ名箇所をクリックします。



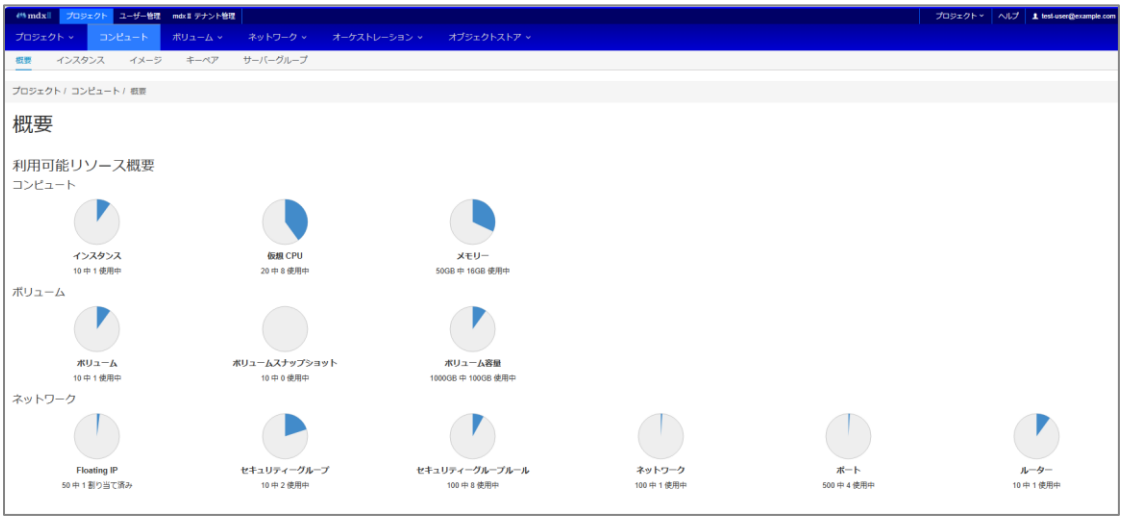
(2) [パスワードの変更]をクリックします。



(3) 以下の項目を入力して[変更]ボタンをクリックします。

5.1.3. 資源量の確認

ユーザポータルにログインした際に表示される円グラフによりプロジェクト内の資源量の状況を把握できます。プロジェクトのクォータ（制限値）に対して利用中の資源量が青色で表示されます。



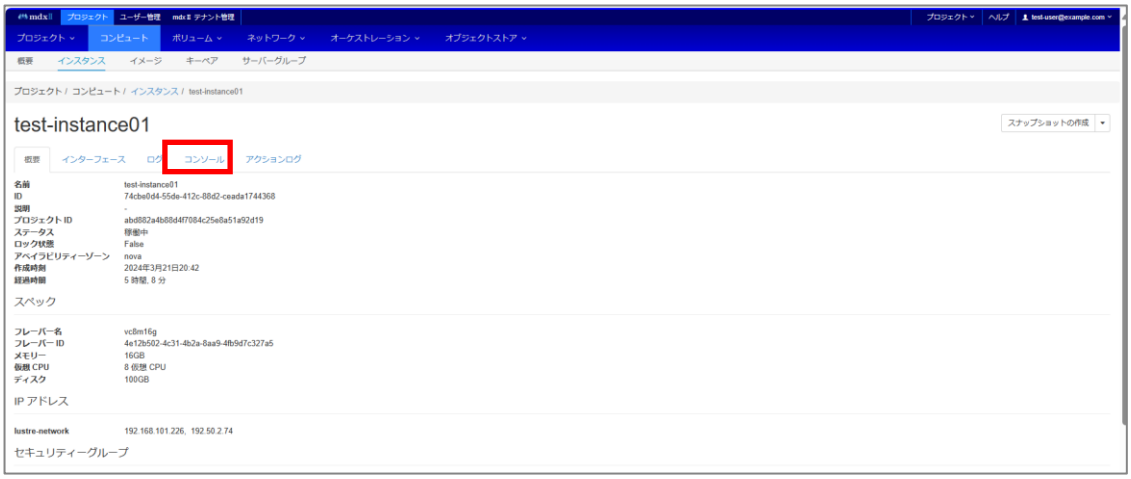
5.1.4. 仮想マシンのコンソール

仮想マシンにコンソールからアクセスが可能です。コンソールからアクセスする場合は仮想マシン内のユーザにパスワードを設定しておく必要があります。

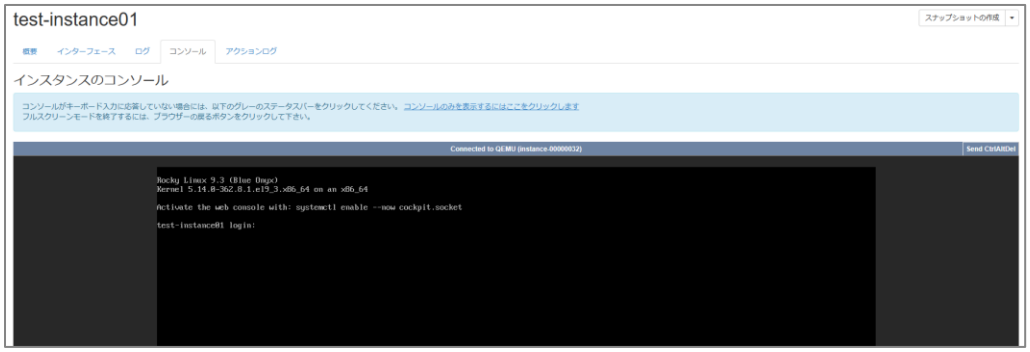
(1) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[インスタンス]タブをクリックします。

(2) コンソールを開く仮想マシンでインスタンス名をクリックします。

(3) [コンソール]タブをクリックします。



(4) コンソール画面が開き、仮想マシンにパスワード認証でアクセスが可能です。



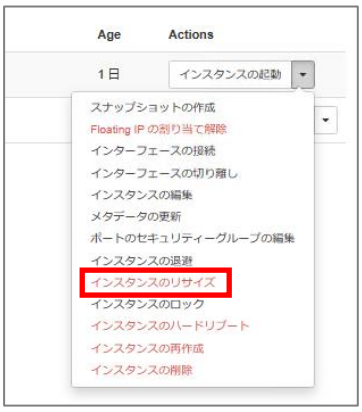
5.1.5. 仮想マシンのフレーバー変更

仮想マシンのフレーバーを変更してリソース量をリサイズすることが可能です。

(1) 対象の仮想マシンをシャットダウンします。

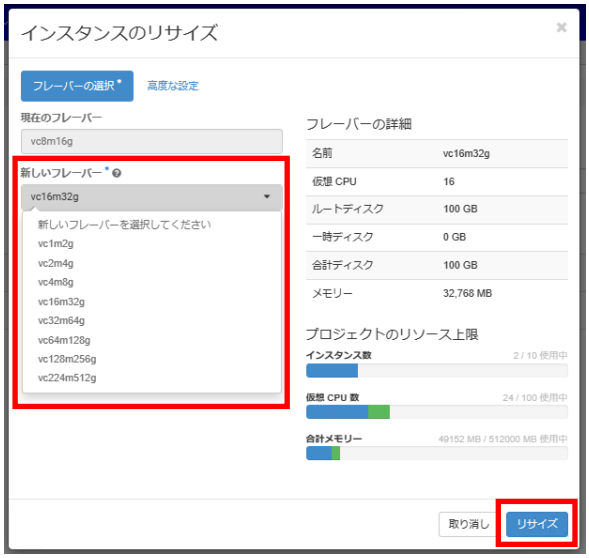
(2) インスタンス画面で対象の仮想マシンの右側にあるプルダウンメニューをクリックします。

(3) [インスタンスのリサイズ]をクリックします。

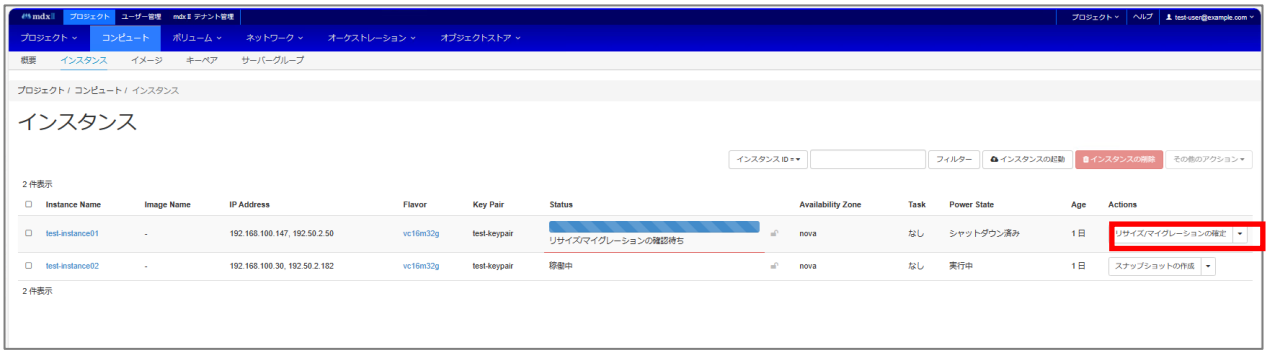


(4) 以下の項目を入力して[リサイズ]をクリックします。

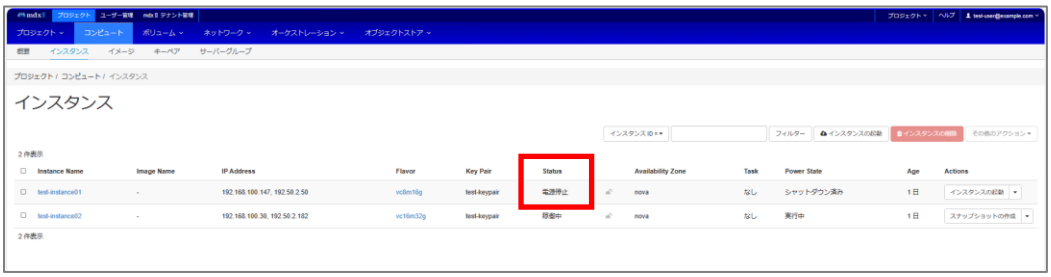
・新しいフレーバー：※リサイズするフレーバーを選択



(5) 「リサイズ/マイグレーションの確定」ボタンをクリックします。



(6) リサイズ処理が完了すると Status が「電源停止」になります。



(7) [インスタンスの起動]ボタンをクリックしてインスタンスを起動します。

5.1.6. 仮想マシンのマルチデプロイ

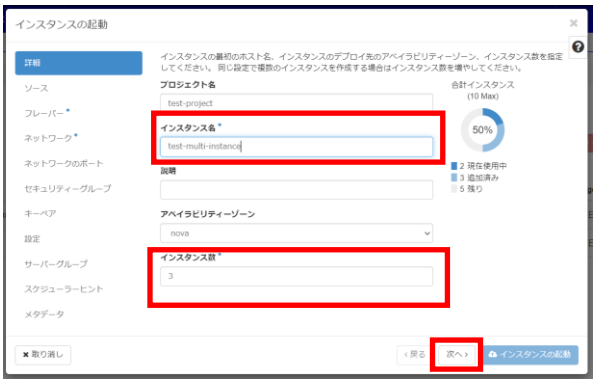
同じ構成の仮想マシンを複数同時に作成することが可能です。

(1) インスタンス画面で[インスタンスの起動]ボタンをクリックします。

(2) 以下の項目を入力して[次へ]ボタンをクリックします。

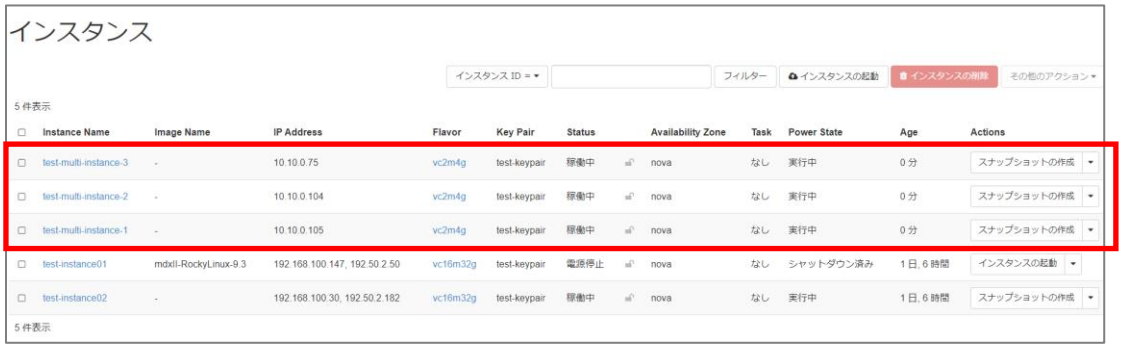
・インスタンス名：※任意　（ここで入力した値の末尾に「-<連番>」が自動で付与されます）

・インスタンス数：※同時に作成したい仮想マシン数



(3) 残りのインスタンス作成の操作は「4.1.7. 仮想マシンの作成」の(4)～(8)に従い実施し、インスタンスを作成します。

(4) 指定したインスタンス数分の仮想マシンが同時に作成され、一覧に追加されます。



5.1.7. ISO ファイル・仮想マシンイメージのアップロード

OS インストーラなどの ISO ファイルや仮想マシンイメージ(QCOW2 など)をアップロードしてイメージを作成することで、イメージから仮想マシンの作成が可能です。

(1) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[イメージ]タブをクリックします。

(2) [イメージの作成]ボタンをクリックします。

(3) 以下の項目を入力して[イメージの作成]ボタンをクリックします。

・イメージ名：任意

・イメージソース：※アップロードするファイルを選択

・形式：※アップロードしたファイルの形式に合わせて選択

・イメージの共有 公開範囲：プライベート

(4) 作成したイメージが表示されます。

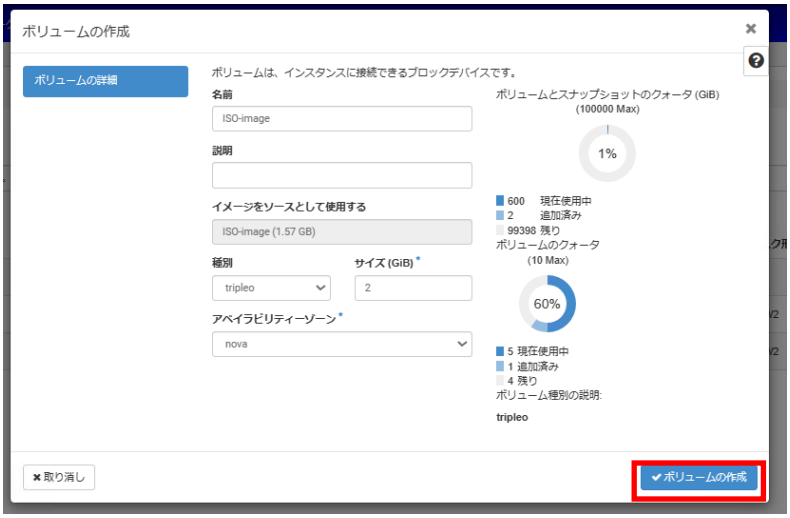
5.1.8. ISO ファイルのマウント

「5.1.8. ISO ファイルのマウント」でアップロードした ISO イメージを仮想マシンにマウントすることが可能です。ISO ファイルを仮想マシンにマウントする場合、ISO ファイルをボリュームとして作成し、仮想マシンにアタッチします。

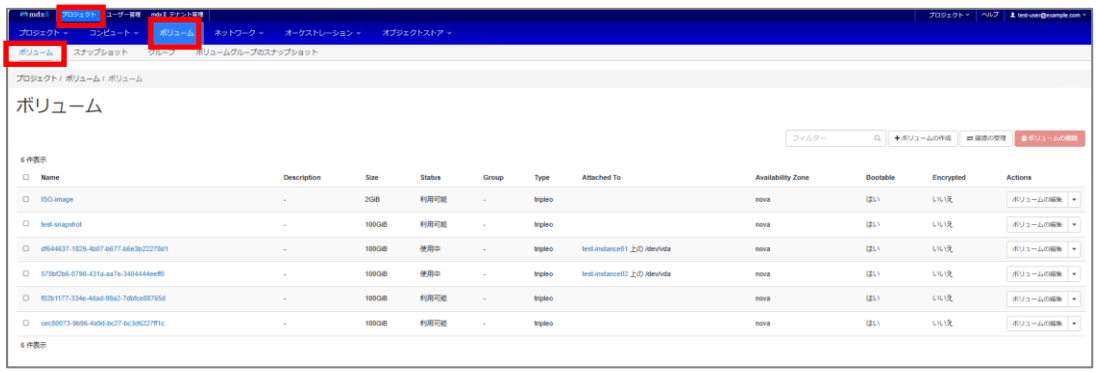
(1) ISO ファイルのイメージの右側にあるプルダウンメニューをクリックします。

(2) [ボリュームの作成]をクリックします。

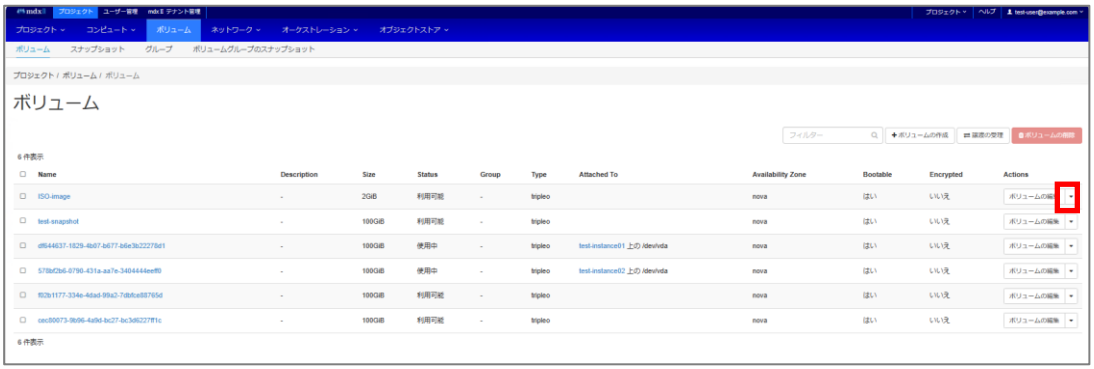
(3) [ボリュームの作成]ボタンをクリックします。



(4) [プロジェクト]メニュー> [ボリューム]パネル> [ボリューム]タブをクリックします。



(5) 作成したボリュームの右側にあるプルダウンメニューをクリックします。

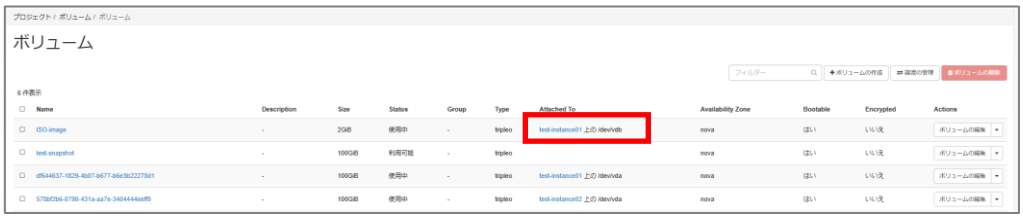


(6) [接続の管理]ボタンをクリックします。

(7) 以下の項目を入力して[ボリュームの接続]ボタンをクリックします。

・インスタンスへの接続: ※ISO ファイルをマウントするインスタンスを指定

(8) Attached To に仮想マシン名とデバイス名が表示されることを確認します。



(9) 仮想マシンで接続した ISO ファイルのボリュームを任意のディレクトリにマウントして利用します。以下は例になります。

```
# mkdir /mnt/iso
# mount -o loop /dev/vdb /mnt/iso
```

5.1.9. 仮想マシンからイメージの作成

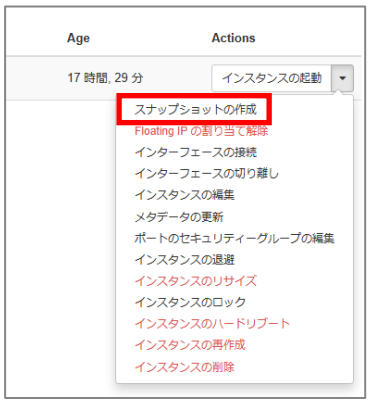
仮想マシンからイメージを作成することで、仮想マシンをバックアップすることができます。また作成したイメージをダウンロードすることも可能です。

(1) 対象の仮想マシンをシャットダウンします。

(2) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[インスタンス]タブをクリックします。

(3) 対象の仮想マシンの Status が「電源停止」になっていることを確認します。

(4) 対象の仮想マシンの右側のプルダウンメニューから「スナップショットの作成」をクリックします。

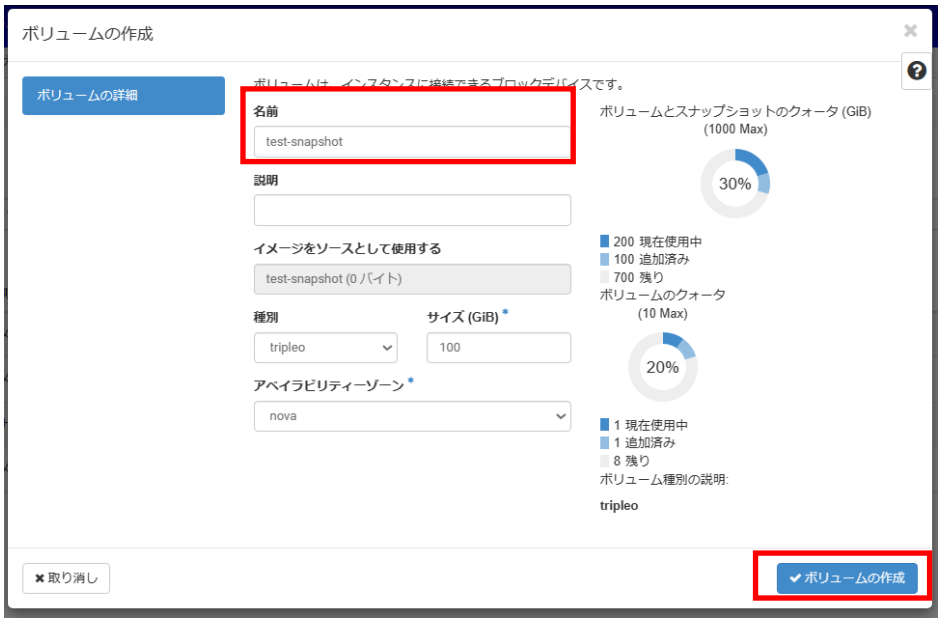


(5) [スナップショット名]に任意のスナップショット名を入力して[スナップショットの作成]ボタンをクリックします。

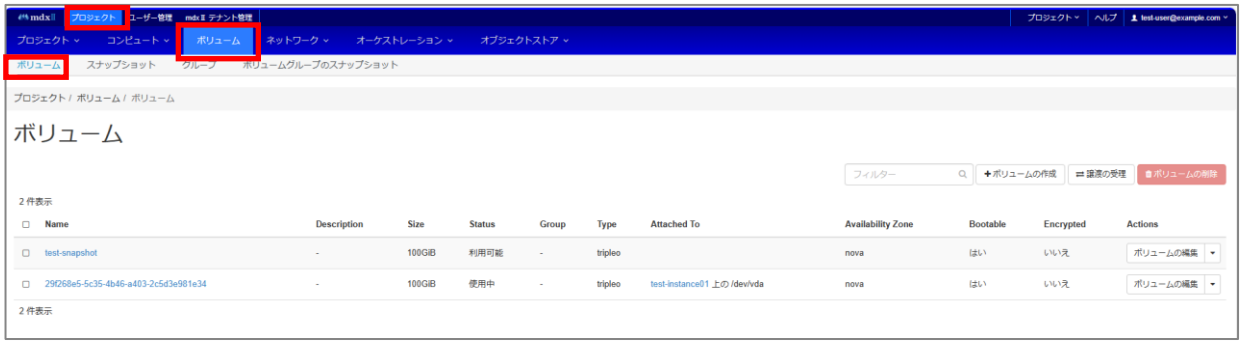
(6) イメージの一覧に作成したスナップショットが表示されます。スナップショットは取得時からの差分を保存しますので、ここではサイズが「0 バイト」で表示されます。

(7) 作成したスナップショットの右側にあるプルダウンメニューから[ボリュームの作成]をクリックします。

(8) [名前]で任意のボリューム名を入力して[ボリュームの作成]ボタンをクリックします。



(9) [プロジェクト]メニュー ＞[ボリューム]パネル ＞[ボリューム]タブをクリックします。



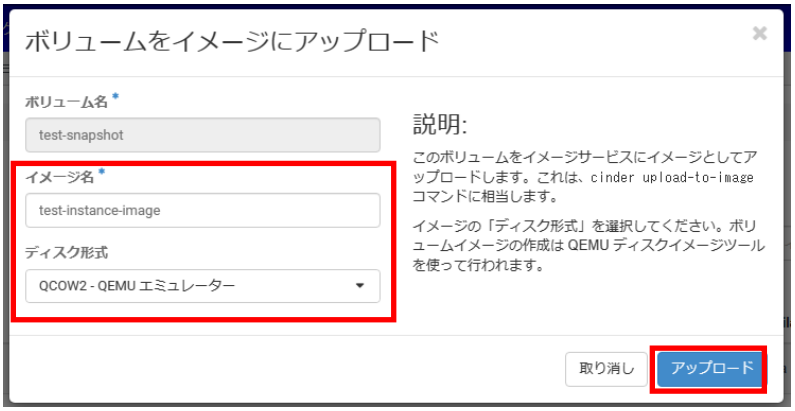
(10) 作成したボリュームが表示されます。

(11) 作成したボリュームの右側にあるプルダウンメニューで[イメージにアップロード]をクリックします。

(12) 以下の項目を入力して [アップロード]ボタンをクリックします。

・イメージ名：※任意

・ディスク形式：※利用したいファイル形式に合わせて変更



(13) [プロジェクト]メニュー ＞[コンピュート]パネル ＞[イメージ]タブをクリックします。

(14) アップロードしたイメージが作成されていることを確認します。

仮想マシンからのイメージの作成手順は以上です。

またイメージファイルの作成過程で利用したスナップショットとボリュームについて、不要な場合は削除して問題ありません。

5.1.10. イメージファイルのダウンロード

ユーザポータルの GUI 画面からはイメージファイルのダウンロードはできません。イメージファイルをダウンロードする場合は、OpenStack の API アクセスによりダウンロードします。

OpenStack の API にアクセスするには、ローカルパスワードが必要になります。学認アカウントをご利用の場合、プロジェクト申請時にローカルパスワードは設定されません。イメージファイルのダウンロードをご希望の場合は、システム管理者宛にメールにてローカルパスワードの発行を申請してください。

OpenStack の API アクセスによるイメージファイルのダウンロードは、ご自身の端末より実施をお願いいしします。以下は Linux 環境からダウンロードを実施する手順になります。

(1) ユーザポータルのイメージ画面でダウンロードしたいイメージのイメージ名をクリックします。

(2) 表示されたイメージの画面で表示されるイメージの ID をメモします。

(3) OpenStack の API アクセスのために curl コマンドを利用します。ご自身の端末で curl パッケージが未インストールの場合はパッケージをインストールします。

(4) OpenStack の API アクセスに必要な認証ファイルを作成します。
※<ユーザ名>は学認アカウントのユーザ名ではなくユーザポータル画面の右上に表示されるユーザ名になります。
※<ローカルパスワード>は学認アカウントのパスワードではなく、申請時にシステム管理者より発行されたパスワードになります。

```
$ vi auth.json
{
    "auth": {
        "identity": {
            "methods": ["password"],
            "password": {
                "user": {
                    "name": "<ユーザ名> ",
                    "password": "<ローカルパスワード>",
                    "domain": { "name": "Default" }
                }
            }
        },
        "scope": {
            "project": {
                "name": "test-project",
                "domain": { "name": "Default" }
            }
        }
    }
}
```

(5) curl コマンドで OpenStack の API にアクセスし出力結果を保存します。

```
$ curl -v -sS -X POST -H "Content-Type: application/json"  -d @auth.json https://portal.osaka.mdx.jp:13000/v3/auth/tokens > curl.out
```

(6) 保存した出力結果から認証トークンの情報(太字箇所)を確認してコピーします。

```
$ view curl.out
...省略...
< x-subject-token: XXXXXXXXXXXXX
...省略...
```

(7) コピーしたトークン情報を環境変数に格納します。

```
$ token="XXXXXXXXXXXXX"
```

(8) curl コマンドで API アクセスしてイメージファイルをダウンロードします。

※<イメージの ID>はメモしたイメージファイルの ID を入力します。

※<ダウンロードファイル名>は任意のイメージファイル名(test.qcow2 など)を指定します。

```
$ curl -i -X GET -H "X-Auth-Token: $token" https://portal.osaka.mdx.jp:13292/v2/images/<イメージの ID>/file --output <ダウンロードファイル名>
```