\Orchestrating a brighter world NEC

mdxII User’s Manual

Ver. 1

NEC Corporation

Education and Science Division

Revision History

Ver.	Date	Subject	Description
1	Mar. 28, 2024	All	New edition

目次

1. Introduction

This document is a user manual (for project managers) of Osaka University mdxII.
It provides information necessary to use the system, including creating and operating virtual machines in mdxII.

In this document, commands are expressed as follows. The shaded part is the command. Also, a prompt with "#" indicates execution as a root user, and a prompt with "$" indicates execution as a user other than root. Some command execution results start with #. Please note that the command part is shaded.
The "[XXX]" in front of the prompt represents the host name. This is written when executing a command on a specific host.
The notation "<XXX>" before the prompt represents a specific username. This is written when the command is executed as a specific user.

```
Example 1：
$ Command execution as a user other than root (LDAP account or local account)

Example 2：
# Execute command as root user

Example 3：
[host]# Command to be executed as root user on host

Example 4：
<user>$ user Command executed as user
```

1.1. Terminology

- Project manager
  A user who applies for a project, creates a virtual infrastructure environment from the user portal, applies for data aggregation object storage, and uses the data transfer portal.

- Project user
  A user who uses the virtual infrastructure environment created by the project administrator.

- System administrator
  This is the administrator of this system who receives project applications and registers projects in the system.

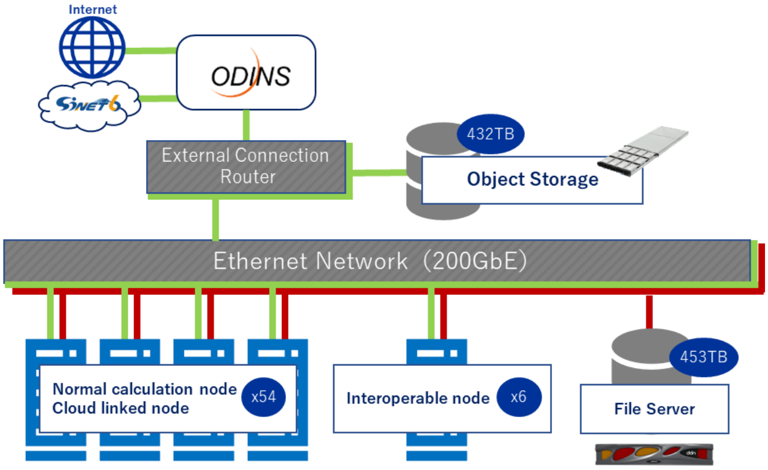
1.2. Service List

The following services are provided.

Service	How to apply	Reference
Normal calculation node/Cloud linked node (OpenStack)	Apply from the project application website	
Interoperable node (VMware)	Email request to system administrator	
File Server	● Volume usage from instance No application required as it can be used from the user portal	
	● Luster mount from instance After creating an OpenStack (or VMware) instance and assigning a public IP address Email request to system administrator	
Object Storage	Apply from user portal	
Project Data Portal	Apply from user portal *Applications can only be made when the application for object storage is completed.	
User Data Portal	Request by email to system administrator	

1.3. System Overview

mdxII is a system consisting of normal computing nodes, cloud-linked nodes, interoperable nodes, file servers, and object storage for data aggregation. Each resource is provided by a virtual machine.



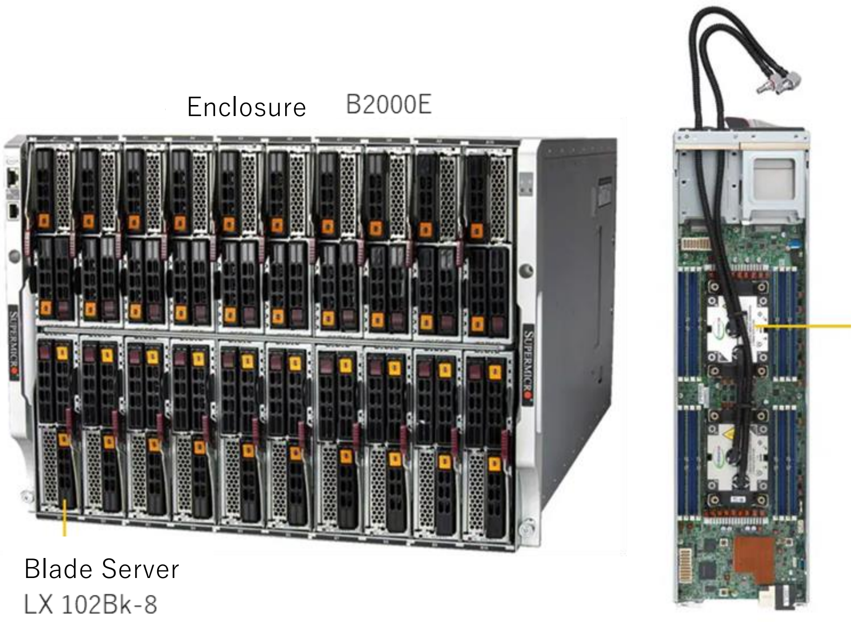
1.3.1. Normal calculation node/Cloud linked node

It consists of a total of 60 general-purpose computing nodes that serve as normal computing nodes, cloud-linked nodes, and interoperability nodes. The number of nodes and the role of each node are shown in the table below.

Role	Number of nodes	Description
Normal calculation node・ Cloud linked node	54	Configured as a Red Hat OpenStack Compute node
Interoperable Node	6	configured as VMware ESXi

The hardware configuration per node is as follows.

Item	Configuration details
Server device name	NEC LX 102Bk-8
CPU	Intel® Xeon® Platinum 8480+ Processor ・Number of cores: 56 ・Base operating frequency: 2.0GHz ・Hyper-threading enabled
Number of CPUs	2
Memory	512GiB (32GiB DDR5-4800 ECC RDIMM x16)
Drive	960GB SATA SSD x1
Network I/F	Servie：200GbE x2 Management：25GbE x1 * Limited to 200GbE for 20 nodes.



1.3.2. File Server

A Luster appliance, DDN EXAScaler, is configured using DDN ES400NVX2.

There are two data storage areas: the "data area" that stores data for each project, and the "virtual disk area" that stores virtual machine data. The total available capacity is 453.24TB for data area and 100TB for virtual disk area.

DDN ES400NVX2

1.3.3. Object storage

It consists of Cloudian HyperStore HAS-1610 and provides mdx II object storage services.

Total available capacity is 432TB.

Cloudian HyperStore HAS-1610

1.4. Project application and user portal

1.4.1. Project application web

You can access the project application website from the URL below. Access requires authentication by GakuNin. You can apply for a new project on the project application web.

https://project-register.osaka.mdx.jp

If you do not have a GakuNin account, please email the system administrator with the following information. If you wish to change the submitted project information, please contact the system administrator by email.

For the procedure for project application, please refer to "3. Project application ".

1.4.2. User Portal

After completing the project application, you can access the user portal from the URL below. Two-step authentication using One-Time Password authentication and GakuNin authentication (or local authentication) is required to access the user portal.

*One-Time Password information will be contacted by the system administrator after project registration is completed.

https://portal.osaka.mdx.jp

There are two types of accounts available on the portal:

- GakuNin account
  - An academic certification federation built by NII in collaboration with universities across the country.
    https://www.gakunin.jp

- Local account
  - mdxII dedicated account

1.5. Resource Unit

1.5.1. Data unit

Memory, virtual disk, and storage capacity are displayed as numbers calculated using powers of 2.
Units using a binary prefix (KiB/MiB/GiB, etc.) are standard for expressing numerical values calculated as powers of 2.
Although it is semi-used, mdxII displays it using commonly seen units using the SI prefix (KB/MB/GB,etc.).

example)
1[MiB] = 1024[KiB] → 1[MiB] is displayed as 1[MB] in mdxII
1[GiB] = 1024[MiB] → 1[GiB] is displayed as 1[GB] in mdxII

1.5.2. CPU Pack

mdx uses a unit called CPU pack as the unit of usage of CPU resources.
A CPU pack is a set that includes the number of virtual CPUs and virtual memory. The amount of resources that can be used with 1 CPU pack is as follows.

Name	Number of vitual CPUs	Amount of virtual memory
CPU Pack	1	2048MB(2GB)

1.6. Contact information

For inquiries regarding projects or service applications, please contact us using the contact information below.

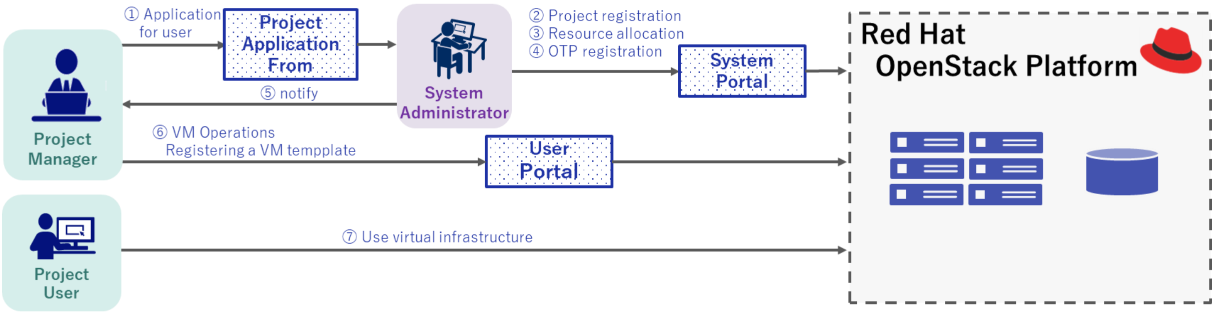
- System administrator
  - Email address ：mdx2-system@cmc.osaka-u.ac.jp
  - Phone number ：06-6879-8813

2. Usage flow

It describes the flow of using each service.

2.1. Normal calculation node/Cloud linked node (RHOSP)

The flow of using the Red Hat OpenStack Platform environment for normal calculation nodes and cloud-linked nodes is shown in the diagram below.



2.2. File Server

File server services can be used in the following ways.

- Attach to the instance as an OpenStack volume (Cinder)
  - Available from the user portal. For usage instructions, please refer to "4.1.10.1. Using Cinder volumes ".
- Luster mount from OpenStack virtual machine
  - Can be used from OpenStack virtual machines. To use it, you will need to request an application by email to the system administrator. For usage instructions, please refer to "4.1.10.2. Lustre Mount".
- Luster mount from VMware virtual machine
  - Can be used from VMware virtual machines. To use it, you will need to request an application by email to the system administrator. Please refer to "4.6.3. Lustre Mount" for usage instructions.
- sftp access from ProjectDataPortal (Nextcloud) via instance
  - It can be used from Nextcloud, which is available on a project-by-project basis. Please refer to "4.4. Project Data Portal" for usage instructions.
- S3 access from myDataPortal (Nextcloud)
  - Available from Nextcloud, which is available on a per-user basis. Please refer to "4.5. myDataPortal" for usage instructions.
- S3 access via internet
  - Please refer to "4.2.1. S3 Access Method" for usage instructions.

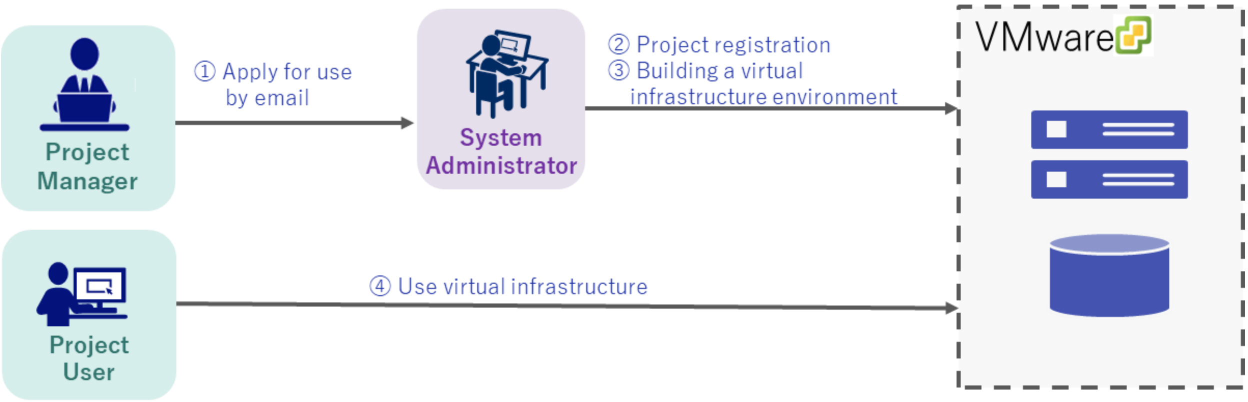
2.3. mdx II object storage

File server services can be used in the following ways.

- S3 access from ProjectDataPortal (Nextcloud)
  - Please refer to "4.4. Project Data Portal" for usage instructions.
- S3 access from myDataPortal (Nextcloud)
  - Please refer to "4.5. myDataPortal" for usage instructions.
- Usage via the Internet: S3 access
  - Please refer to "4.3. Object Storage" for usage instructions.

2.4. Interoperable Node (VMware)

The flow of using the VMware environment for interoperable nodes is shown in the diagram below. Interoperable nodes do not provide a user portal. Apply for use by emailing the system administrator. After applying, a system administrator will create and provide a virtual machine. Please refer to "4.6. Interoperable Node（VMware）" for details on how to apply.



3. Project application

Apply for a project by following the steps in "3.1. New Application." The items required to be entered in the project application are shown in the table below.

Item name	Contents
Project Name	Project name
User Name	Username (*Not required for GakuNin account)
Full Name	Applicant's full name
Institiution	Name of applicant's institution
Mail Address	Applicant's email address
CPU Pack	Total number of CPU packs used in the project *1 CPU pack = CPU 1 core, memory 2 GiB
Available Volume(GB)	Total storage capacity used by the project *Does not include capacity used for Luster mount.
Max number of Floating IP	Maximum number of floating IP addresses used in the project *Floating IP address is an address required to enable the virtual machine to communicate with the external network.
Billing Name	Name of billing contact person
Billing Mail Address	Address Billing contact email address
Billing Phone Number	Billing contact phone number
Billing Affiliation	Affiliation name of the billing contact person

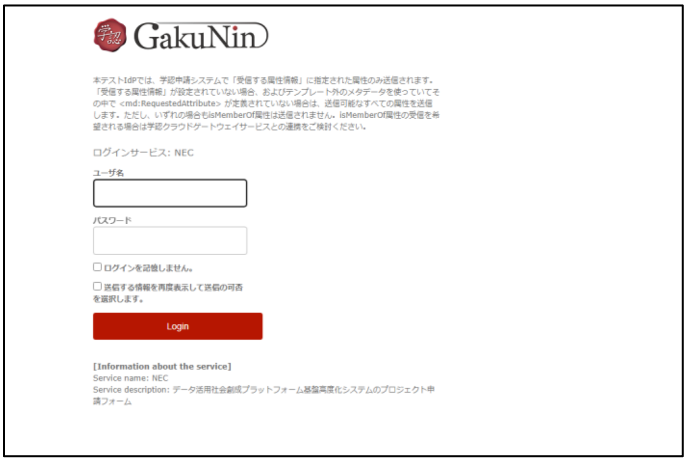
3.1. New application

3.1.1. GakuNin account

Apply for a project from the project application website using the following steps.

(1) Access the following URL from your web browser
https://project.osaka.mdx.jp/mdx_project

(2) Enter your GakuNin account username and password.



本テストIdPでは、学認申請システムで「受信する属性情報」に指定された属性のみ送信されます。「受信する属性情報」が設定されていない場合、およびテンプレート外のメタデータを使っていてその中で <md:RequestedAttribute> が定義されていない場合は、送信可能なすべての属性を送信します。ただし、いずれの場合もisMemberOf属性は送信されません。isMemberOf属性の受信を希望される場合は学認クラウドゲートウェイサービスとの連携をご検討ください。

ログインサービス: NEC

ユーザ名

パスワード

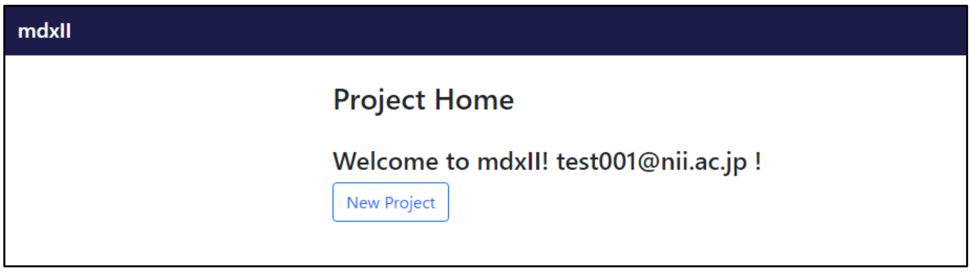
□ ログインを記憶しません。

□ 送信する情報を再度表示して送信の可否を選択します。

Login

[Information about the service]
Service name: NEC
Service description: データ活用社会創成プラットフォーム基盤高度化システムのプロジェクト申請フォーム

(3) Press the "New Project" button on the Project Home page.



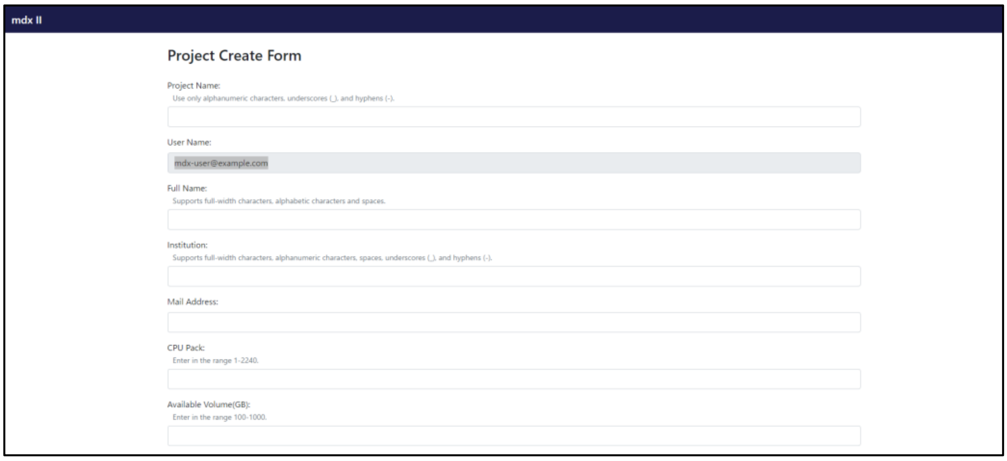
Project Home

Welcome to mdxII! test001@nii.ac.jp !

New Project

(4) Enter the items in the table below on the Project Create Form page.

項目	設定例	備考
Project Name	mdxII-project	Only alphabetic characters (large and small), numbers, _ (underbar), - (hyphen) are allowed.
User Name	test001@nii.ac.jp	User name. GakuNin ePPN is entered.
Full Name	mdxII 太郎	Applicant's full name
Institution	mdxII 大学	Applicant's Institution
Mail Address	mdxII@example.com	Applicant's mail address
CPU Pack	320	Total number of CPU packs used in the project (1~2240)
Available Volume(GB)	500	Total storage capacity used by the project.
Max number of Floating IP	4	Maximum number of floating IP (1~16)
Billing Name	mdxII 次郎	Name of billing contact person
Billing Mail Address	mdxII-admin@example.com	Address billing contact email address
Billing Phone Number	01234587890	Billing contact phone number
Billing Affiliation	mdxII 大学	Affiliation name of the billing contact person



mdx II

Project Create Form

Project Name:
Use only alphanumeric characters, underscores (_), and hyphens (-).

User Name:
mdx-user@example.com

Full Name:
Supports full-width characters, alphabetic characters and spaces.

Institution:
Supports full-width characters, alphanumeric characters, spaces, underscores (_), and hyphens (-).

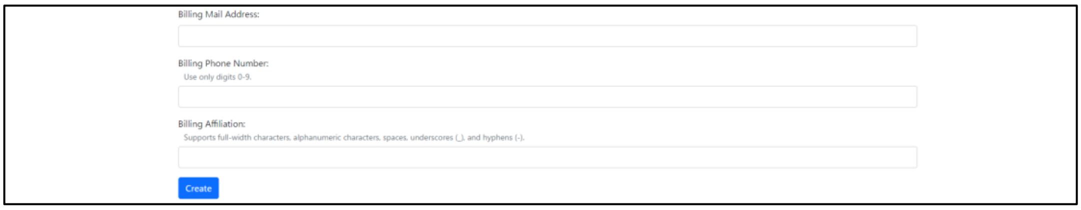
Mail Address:

CPU Pack:
Enter in the range 1-2240.

Available Volume(GB):
Enter in the range 100-1000.

(5) (5) Check the entered values.

(6) Click the "Create" button at the bottom of the Project Create Form page to complete the application. *Please note that there is no confirmation page.

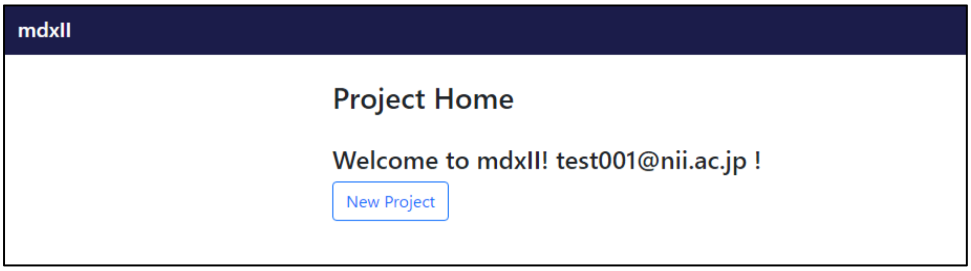


Billing Mail Address:

Billing Phone Number:
Use only digits 0-9.

Billing Affiliation:
Supports full-width characters, alphanumeric characters, spaces, underscores (_), and hyphens (-).

(7) Once the application is completed, you will be redirected to the Project Home page.



mdxII

Project Home

Welcome to mdxII! test001@nii.ac.jp !

3.1.2. Other than GakuNin account

Fill out the application format below and send the application via email to the system administrator.

----- Project application format -----

Project Name : *Project name Only alphabetical characters (large and small), numbers, _ (underbar), - (hyphen) are possible

User Name : *User name Only alphabetic characters (large and small), numbers, _ (underbar), - (hyphen) are possible

Full Name : *Applicant name

Institution : *Applicant's affiliated institution name

Mail Address : *Applicant email address

CPU Pack : *Number of CPU packs (1~2240)

Available Volume(GB) : *Storage capacity (100~1000)

Max number of Floating IP : *Maximum number of floating IP addresses (1~16))

```
Billing Name                  : *Name of billing person
Billing Mail Address          : *Billing person's email address
Billing Phone Number          : *Billing person phone number
Billing Affiliation           : *Billing person affiliation name
-------------------------------------------
```

Below is an example.

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

3.2. Change request

The project application website only accepts new applications. If you would like to change your project information, please contact your system administrator via email.

4. How to user

4.1. Normal calculation node/Cloud linked node (OpenStack)

4.1.1. Information when registering a project

When registration is completed after applying for a project, the system administrator will notify you of the following information.

- Account name
- URL of the QR code required for One-Time Password registration

*If you applied using a local account instead of a GakuNin account, please enter the local password. You will also receive an initial password.

4.1.2. Installing the two-step authentication app

To log in to the user portal via SSH, you need to pass two-step authentication using One-Time Password. there is. Please prepare the application required for two-step verification and install it on your own device.

The following applications can be used as two-step authentication applications:

OS	application	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	Added as an extension to Google Chrome and Microsoft Edge
macOS	Step Two	Apple App Store
	Google Authenticator	Added as a Google Chrome extension

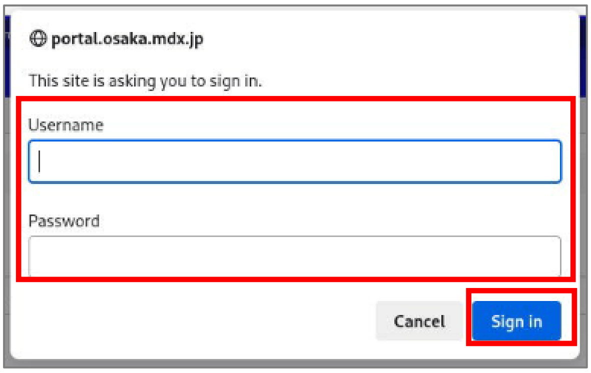
4.1.3. Login to the user portal

There are two steps to log in to the user portal: One-Time Password authentication and GakuNin (or local authentication). If you want to log in with your GakuNin account, please log in according to the steps in "4.1.3.1. GakuNin account login". If you want to log in with a local account, follow the steps in "4.1.3.2. Local Account" to log in.

4.1.3.1. GakuNin account login

(1) Access the following URL from a web browser.
https://portal.osaka.mdx.jp

(2) A pop-up will appear asking you to enter your username and password. Enter your username and One-Time Password confirmed using the two-step authentication application and click the [Sign in] button.



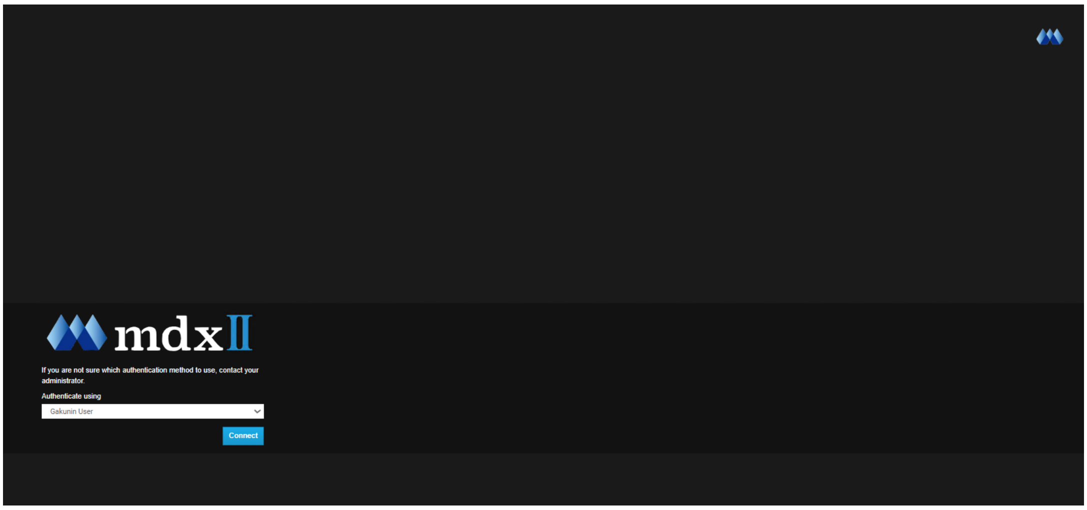
portal.osaka.mdx.jp

This site is asking you to sign in.

Username

Password

(3) If One-Time Password authentication is successful, the user portal login screen will be displayed.

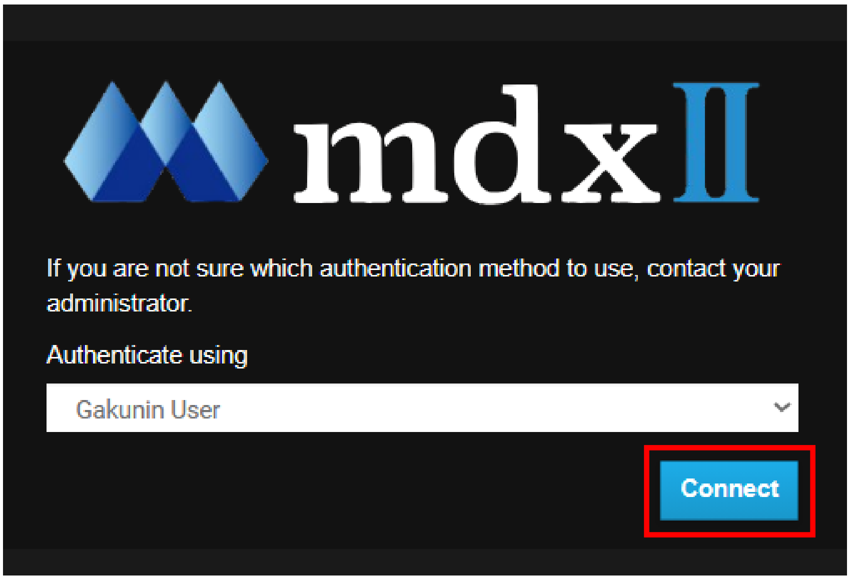


If you are not sure which authentication method to use, contact your administrator.

Authenticate using

Gakunin User

(4) Click the [Connect] button.



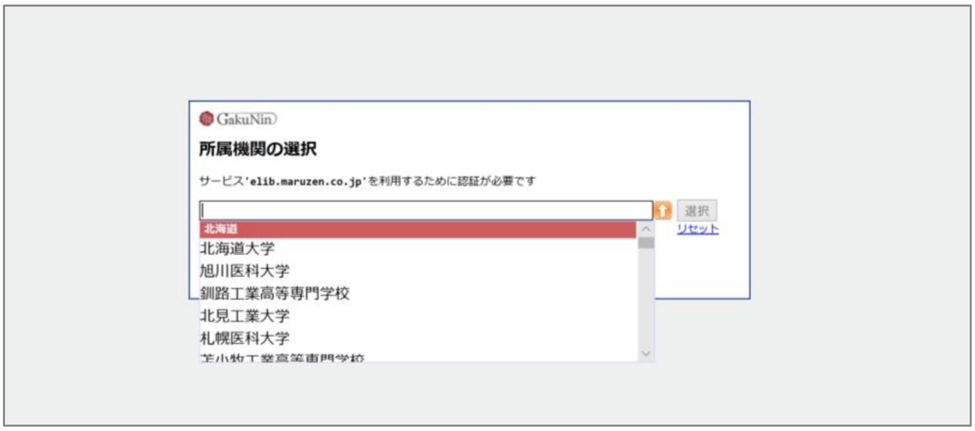
If you are not sure which authentication method to use, contact your administrator.

Authenticate using

Gakunin User

(5) The GakuNin login screen will be displayed. Select your institution from [Affiliated institution]

and click the "Select" button.



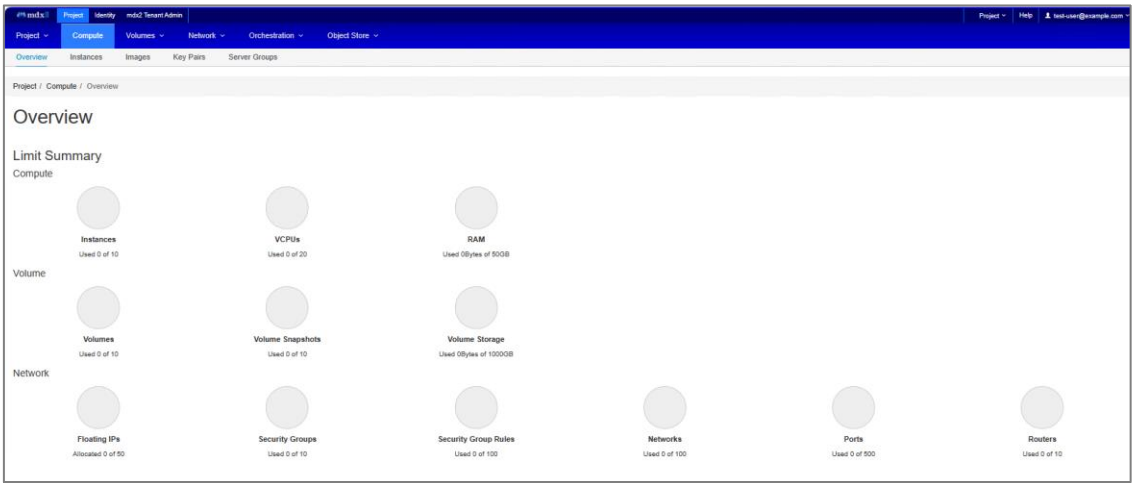
所属機関の選択

サービス'elib.maruzen.co.jp'を利用するために認証が必要です

北海道
北海道大学
旭川医科大学
釧路工業高等専門学校
北見工業大学
札幌医科大学
苫小牧工業高等専門学校

(6) The login screen for your institution's IdP will be displayed, so enter your GakuNin account username and password.

(7) If GakuNin authentication is successful, the user portal dashboard will be displayed.



Overview

Limit Summary

Compute

Instances Used 0 of 10
VCPUs Used 0 of 20
RAM Used 0Bytes of 50GB

Volume

Volumes Used 0 of 10
Volume Snapshots Used 0 of 10
Volume Storage Used 0Bytes of 1000GB

Network

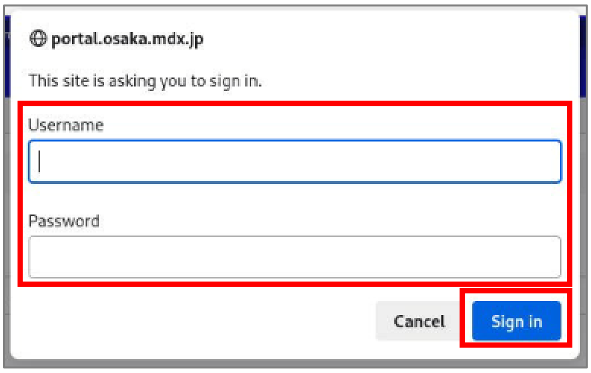
Floating IPs Allocated 0 of 50
Security Groups Used 0 of 10
Security Group Rules Used 0 of 100
Networks Used 0 of 100
Ports Used 0 of 500
Routers Used 0 of 10

4.1.3.2. Local account

(1) Access the following URL from your web browser.

https://portal.osaka.mdx.jp

(2) A pop-up will appear asking you to enter your username and password. Enter your username and One-Time Password confirmed using the two-step authentication application and click the [Sign in] button.



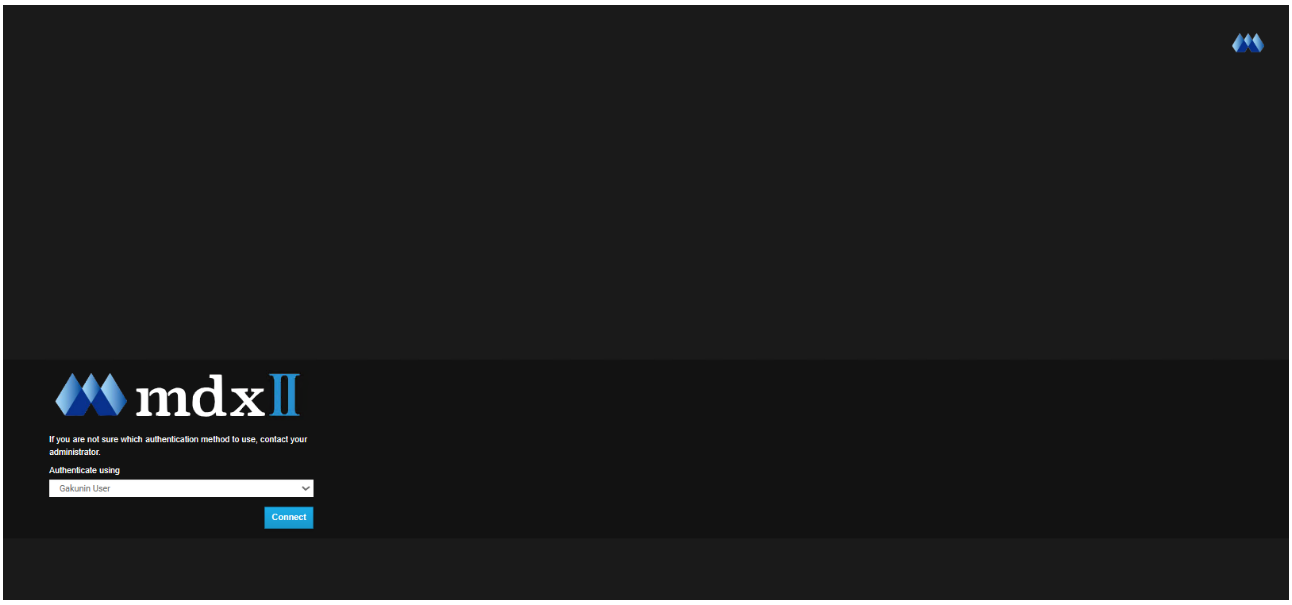
portal.osaka.mdx.jp

This site is asking you to sign in.

Username

Password

(3) If One-Time Password authentication is successful, the user portal login screen will be displayed.

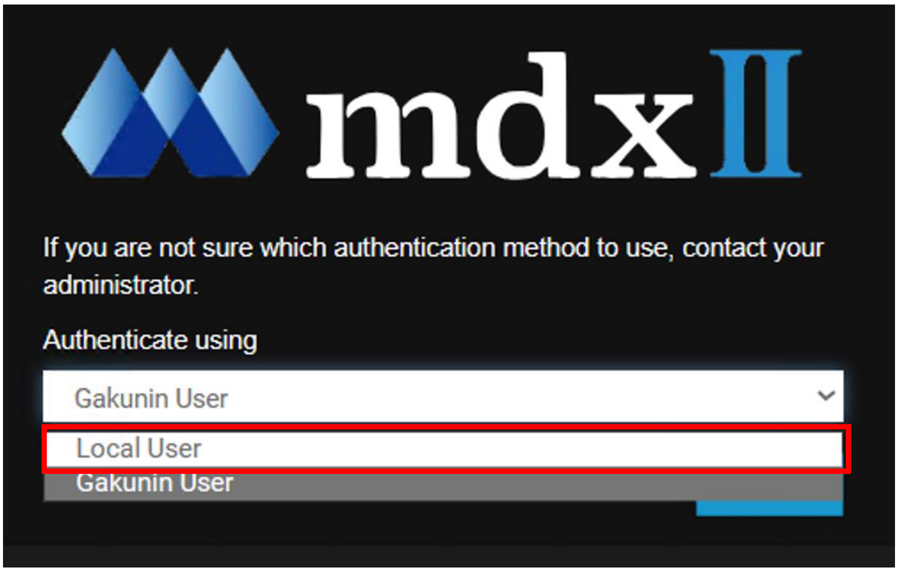


If you are not sure which authentication method to use, contact your administrator.

Authenticate using

Gakunin User

(4) Select [Local User] from the pull-down menu and click the [Connect] button.

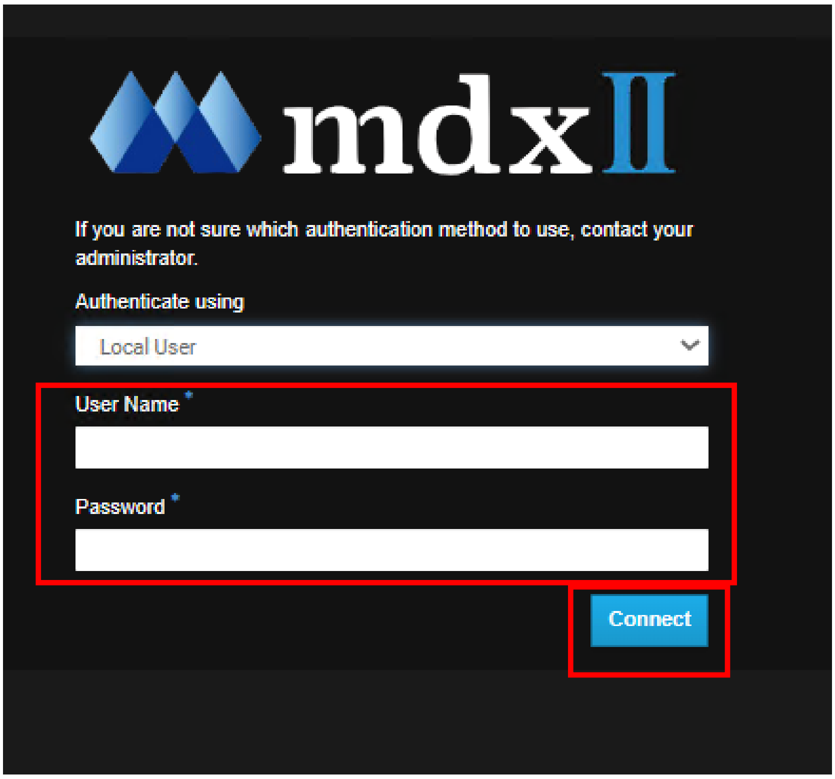


If you are not sure which authentication method to use, contact your administrator.

Authenticate using

Gakunin User

(5) Enter the local user's username and password in [User Name] and [Password] and click the [Connect] button.



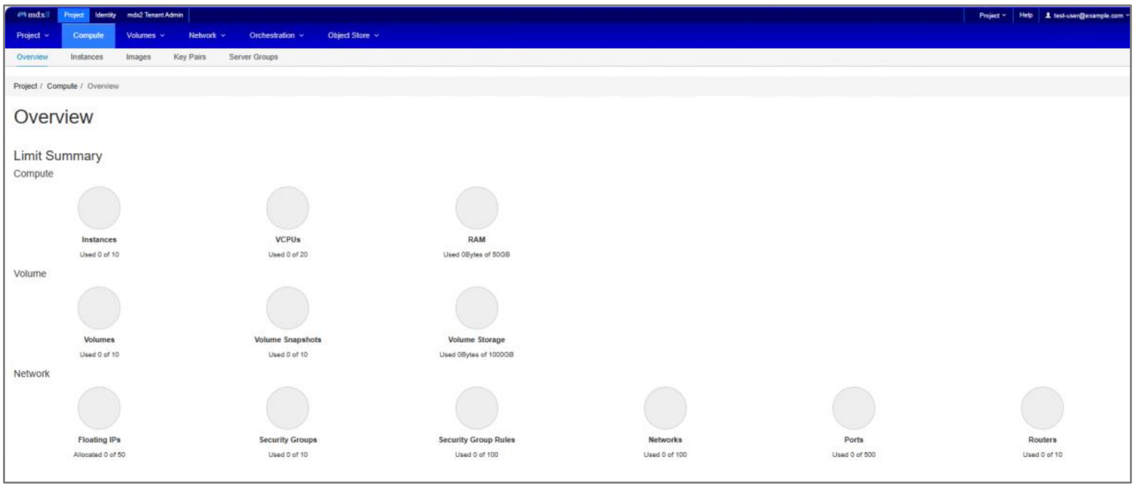
If you are not sure which authentication method to use, contact your administrator.

Authenticate using: Local User

User Name *

Password *

(6) If authentication is successful, the user portal dashboard will be displayed.



Overview

Limit Summary

Compute

Instances: Used 0 of 10

VCPUs: Used 0 of 20

RAM: Used 0Bytes of 50GB

Volume

Volumes: Used 0 of 10

Volume Snapshots: Used 0 of 10

Volume Storage: Used 0Bytes of 1000GB

Network

Floating IPs: Allocated 0 of 50

Security Groups: Used 0 of 10

Security Group Rules: Used 0 of 100

Networks: Used 0 of 100

Ports: Used 0 of 500

Routers: Used 0 of 10

4.1.4. Creating a network

There are two types of networks that connect virtual machines. If you want to Luster mount the file server area on a virtual machine, use the "Network for Luster", and if you do not want to use Luster mount, use the "Private network". The features of each network are as follows.

- Network for Luster
  - Shared network between projects

- The network address is 192.168.100.0/23, and an IP address is automatically assigned by DHCP when creating a virtual machine.
- Connection to the Internet is possible by assigning a floating IP to the virtual machine.
- Used for Luster mount of file server area
  *Since the network is shared with other projects, please set appropriate access restrictions using security groups (ACL). For details on how to set up a security group, please refer to "4.1.6. Creating a security group".

- Private network
  - Closed network within the project
  - Network address can be freely set by the user.
  - Connection to the Internet is possible by assigning a floating IP to the virtual machine.

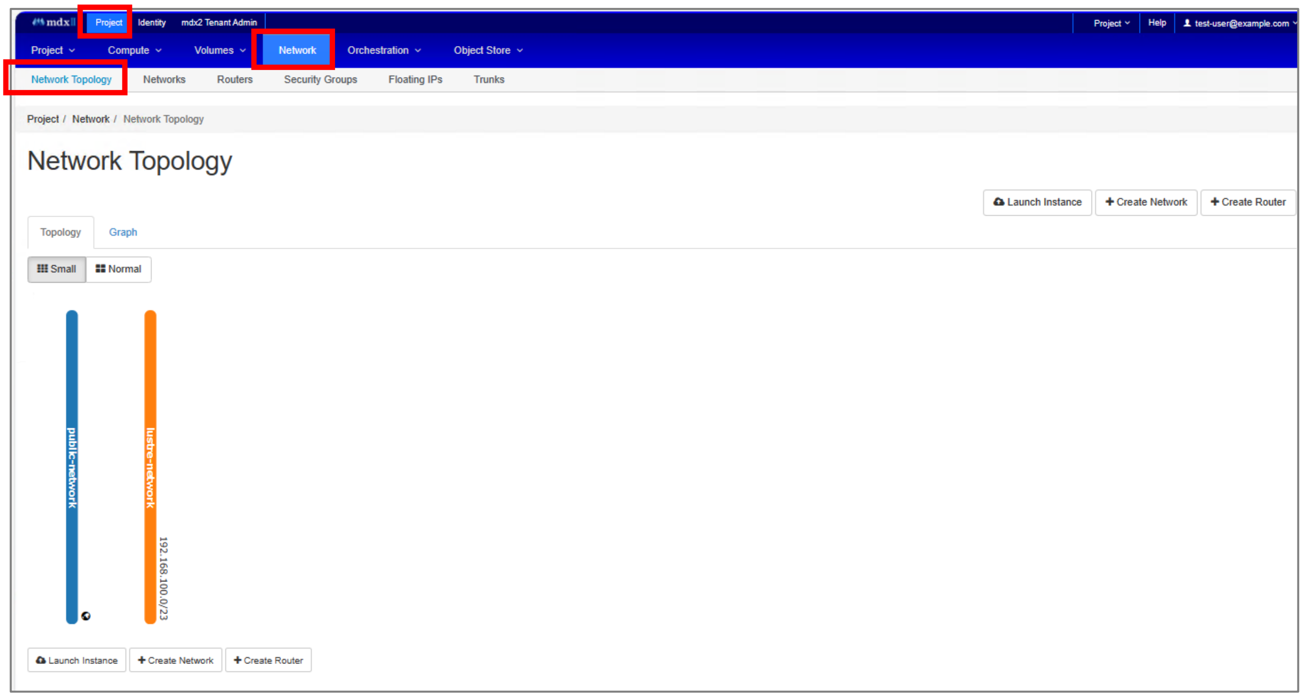
Follow the steps below according to the network you are using.

4.1.4.1. Network for Luster

The network for Luster is already created on the system side, so no operations are required. Proceed to step「4.1.5. Create a key pair」.

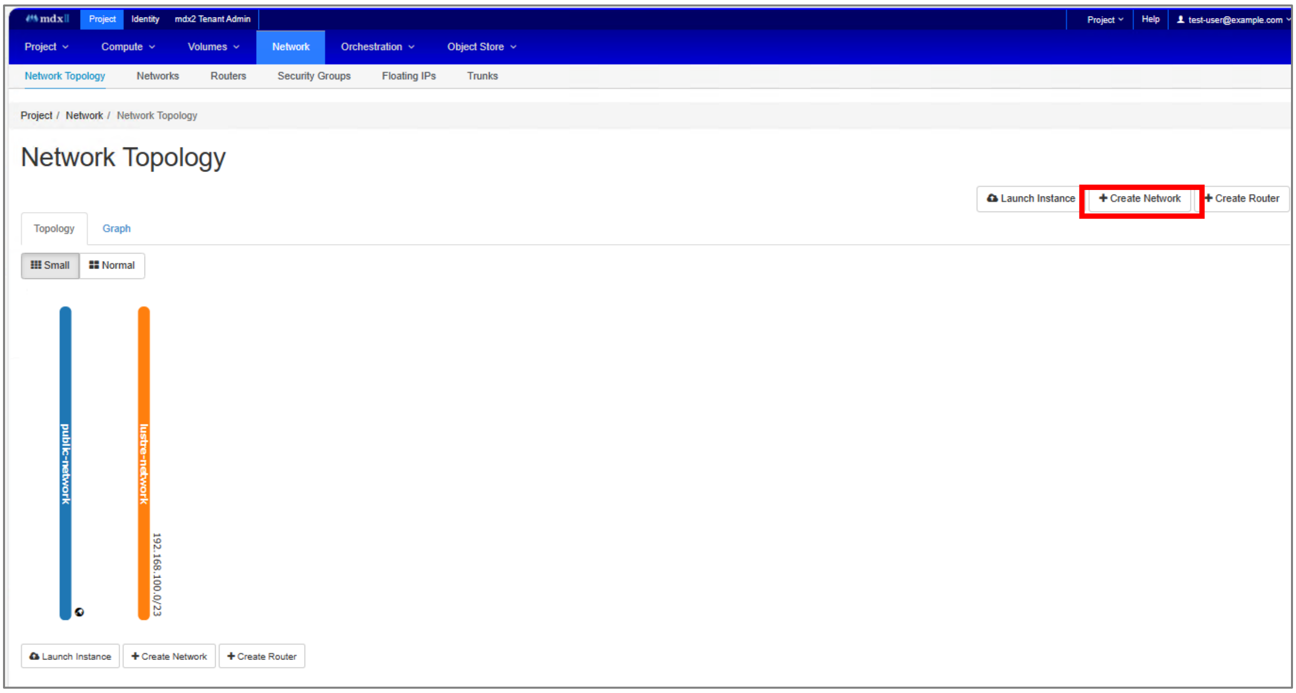
4.1.4.2. Private network

(1) Click the [Project] menu > [Network] panel > [Network Topology] tab.



*In the initial state, the external access network "public-network" and the Luster network "lustre-network" are displayed.

(2) Click the [Create Network] button.



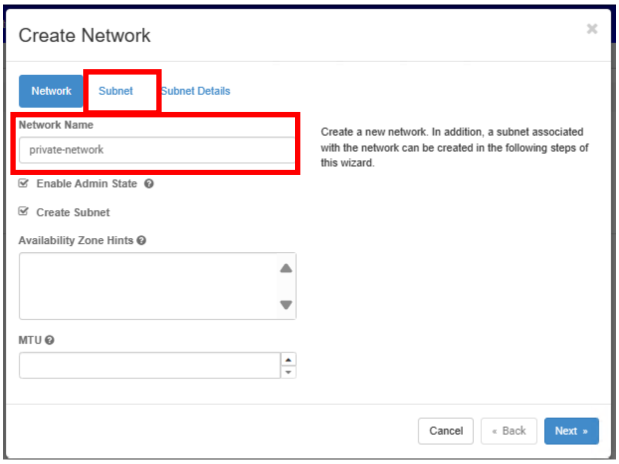
public-network

lustre-network

192.168.100.0/23

(3) Enter the following on the network creation screen and click the [Subnet] tab.

・Network Name: *Optional



Network Name: private-network

☑ Enable Admin State

☑ Create Subnet

Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.

(4) Enter the following items and click the [Subnet Details] tab.

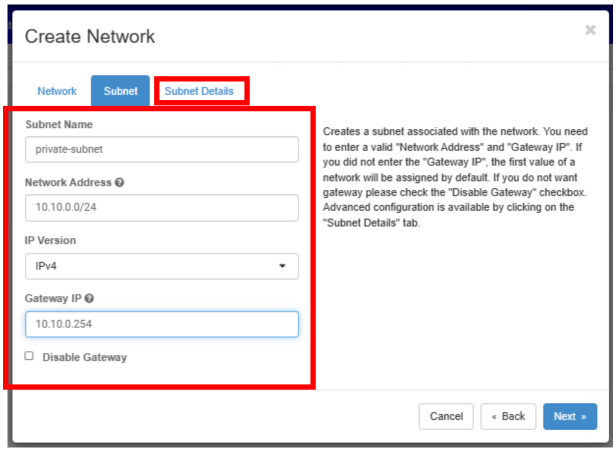
・Subnet Name: *Optional

・Network Address: *Optional

・IP Version: IPv4

・Gateway IP: *Enter one IP address from among the network addresses

・Disable Gateway: Not checked


Create Network

Subnet Name: private-subnet

Network Address: 10.10.0.0/24

IP Version: IPv4

Gateway IP: 10.10.0.254

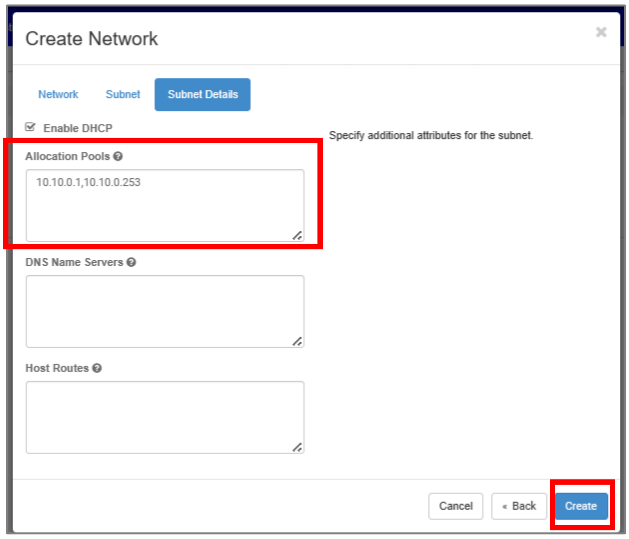
□ Disable Gateway

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

(5) Enter the following items and click the [Create] button.

・Enable DHCP: *Check this if you want to automatically assign an IP address to the virtual machine put in.

・Allocation Pools: *Assigns to the virtual machine from among the specified network addresses Specify IP address range


Create Network

☑ Enable DHCP

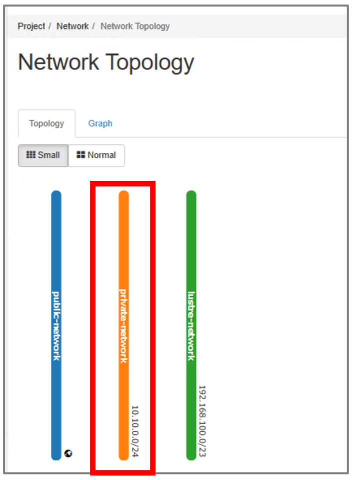
Allocation Pools: 10.10.0.1,10.10.0.253

DNS Name Servers:

Host Routes:

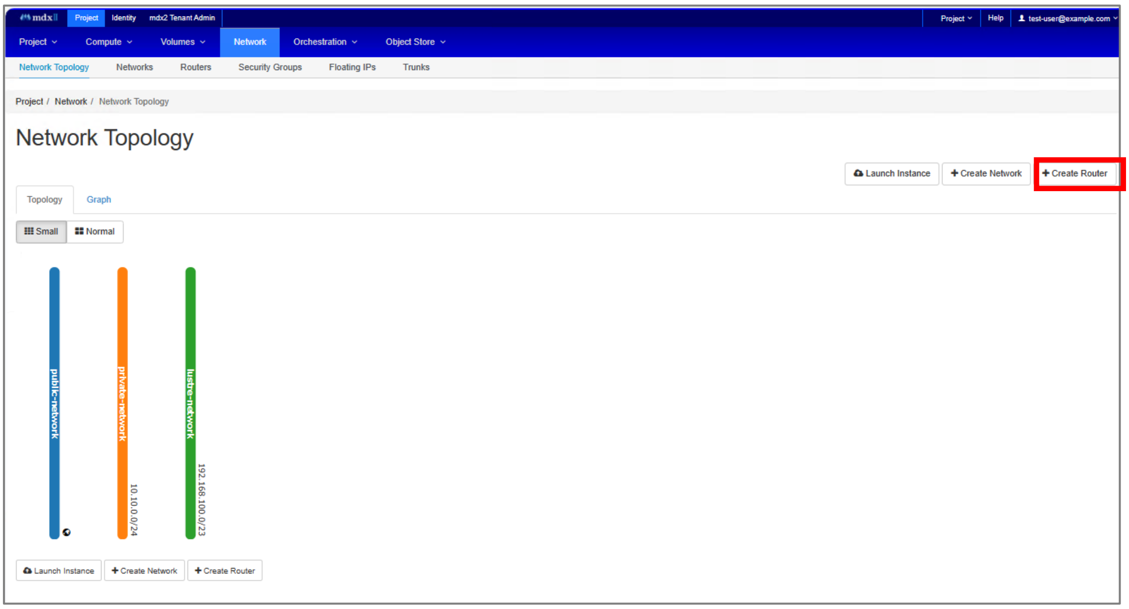
Specify additional attributes for the subnet.

(6) The created private network will be displayed on the network topology screen.


Project / Network / Network Topology

Network Topology

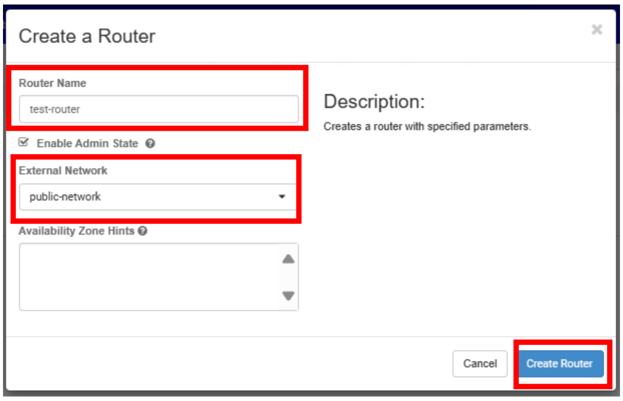
(7) Next, click the [+Create Router] button.



(8) Enter the following items and click the [Create Router] button.

・Router Name: *Optional

・External Network: public-network



Create a Router

Router Name: test-router

☑ Enable Admin State

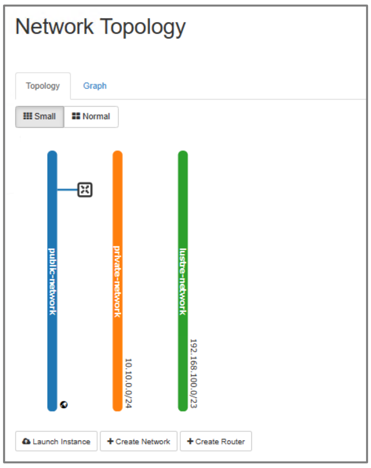
External Network: public-network

Availability Zone Hints

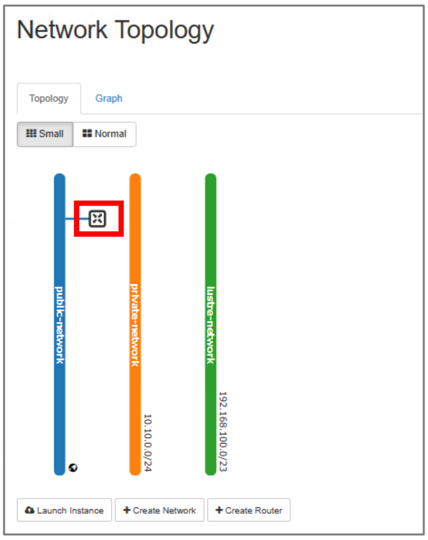
Description:

Creates a router with specified parameters.

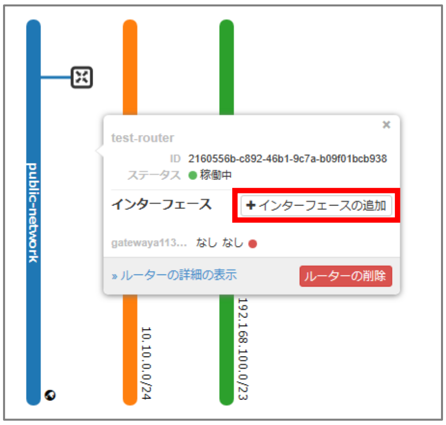
(9) The created virtual router will be displayed on the network topology screen with it connected to public-netwrok.



(10) Next, click the virtual router icon.



(11) Click the [+Add Interface] button.


test-router

ID 2160556b-c892-46b1-9c7a-b09f01bcb938

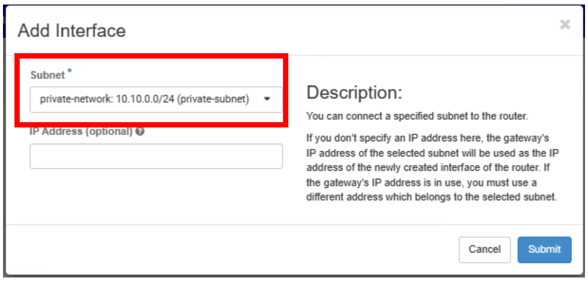
ステータス ● 稼働中

インターフェース

gatewaya113... なし なし ●

(12) Select the following and click the [Submit] button.

・Subnet:private-network


Add Interface

Subnet *: private-network: 10.10.0.0/24 (private-subnet)

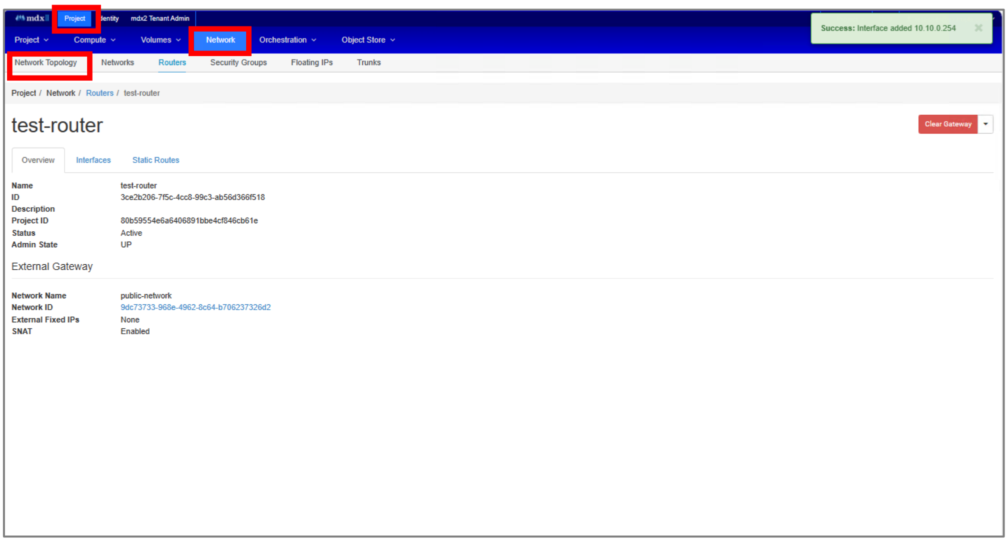
IP Address (optional)

Description:

You can connect a specified subnet to the router.

If you don't specify an IP address here, the gateway's IP address of the selected subnet will be used as the IP address of the newly created interface of the router. If the gateway's IP address is in use, you must use a different address which belongs to the selected subnet.

(13) To go to the created virtual router screen, click the [Project] menu > [Network] panel > [Network Topology] tab again.



Success: Interface added 10.10.0.254

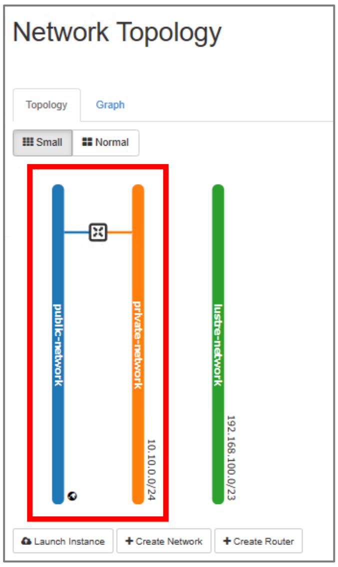
test-router

Name test-router
ID 3ce2b206-7f5c-4cc8-99c3-ab56d366f518
Description
Project ID 80b59554e6a6406891bbe4cf846cb61e
Status Active
Admin State UP

External Gateway

Network Name public-network
Network ID 9dc73733-968e-4962-8c64-b706237326d2
External Fixed IPs None
SNAT Enabled

(14) Confirm that the created virtual router and the created private network are connected.



4.1.5. Create a key paire

Register the SSH key pair for SSH access to the virtual machine. There are two ways to register a key pair:

- Import and register the public key of the SSH key created in advance (recommended)
- Create and register a new key pair
  - You cannot set a key passphrase when creating a new key pair. Please use this only when using the virtual machine to check its operation.

Please follow the steps below according to each registration method.

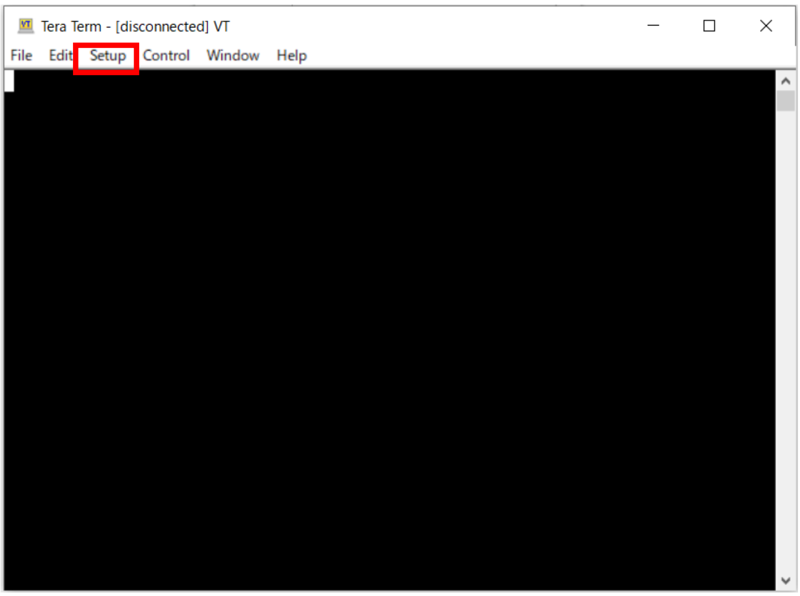
4.1.5.1. Registration by importing SSH keys

(1) Create an SSH key in advance on your work terminal. The following is an example created using TeraTerm terminal software.

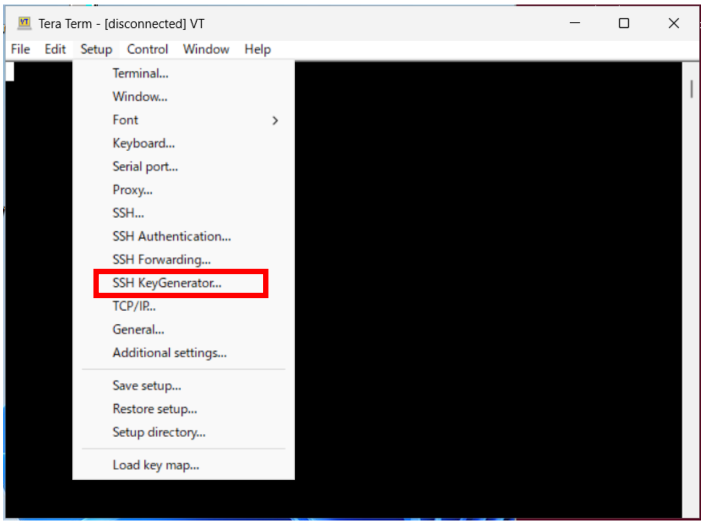
① Download and install TeraTerm from the URL below on your work terminal.
https://github.com/TeraTermProject/teraterm/releases

② Start TeraTerm.

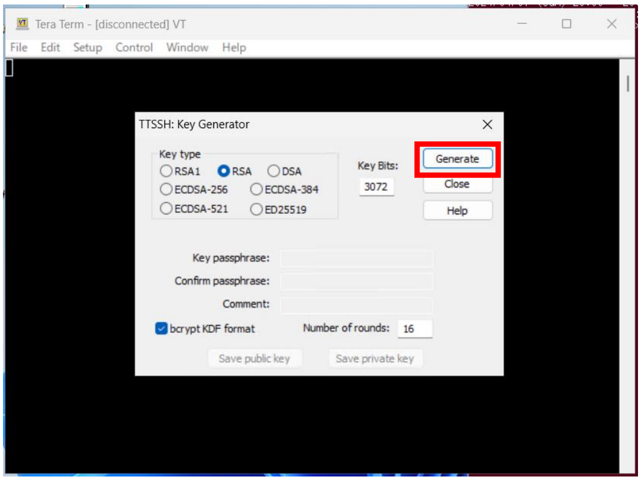
③ Click the [SetUp] tab.



④ Click [SSH KeyGenerator..].



⑤ Click the [Generate] button.



Key type
○ RSA1 ● RSA ○ DSA
○ ECDSA-256 ○ ECDSA-384
○ ECDSA-521 ○ ED25519

Key Bits: 3072

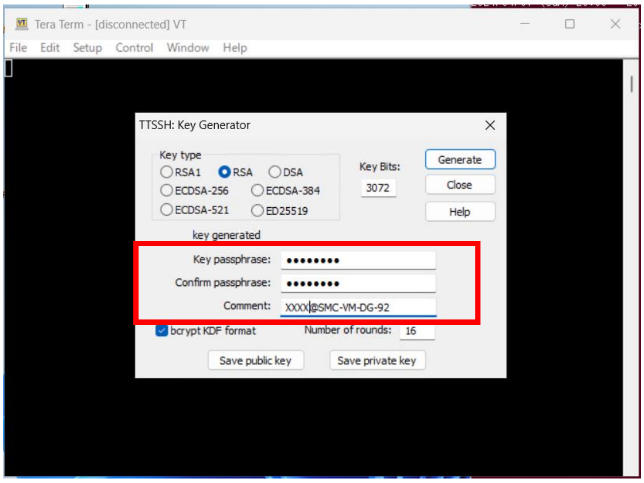
Key passphrase:

Confirm passphrase:

Comment:

☑ bcrypt KDF format Number of rounds: 16

⑥ Enter the passphrase to be set for the SSH key in [Key Passphrase] and [Confirm Passphrase].



Key type
○ RSA1 ● RSA ○ DSA
○ ECDSA-256 ○ ECDSA-384
○ ECDSA-521 ○ ED25519

Key Bits: 3072

key generated

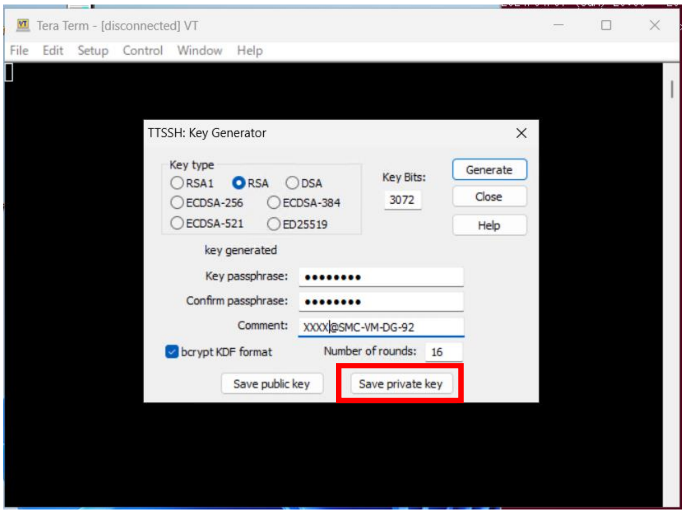
Key passphrase: ••••••••

Confirm passphrase: ••••••••

Comment: XXXX@SMC-VM-DG-92

☑ bcrypt KDF format Number of rounds: 16

⑦ Press the [Save private key] button to save the private key. The private key is required for SSH access to the virtual machine, so please store it securely so that it is not leaked or lost.



Key type
○ RSA1 ● RSA ○ DSA
○ ECDSA-256 ○ ECDSA-384
○ ECDSA-521 ○ ED25519

Key Bits: 3072

key generated

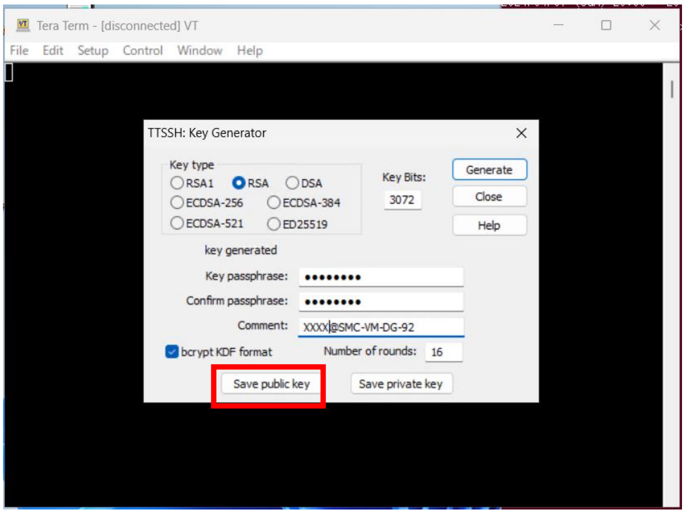
Key passphrase: ••••••••

Confirm passphrase: ••••••••

Comment: XXXX@SMC-VM-DG-92

☑ bcrypt KDF format Number of rounds: 16

⑧ Click the [Save public key] button to save the public key. The public key is used to register a key pair.



Key type
○ RSA1 ● RSA ○ DSA
○ ECDSA-256 ○ ECDSA-384
○ ECDSA-521 ○ ED25519

Key Bits: 3072

key generated

Key passphrase: ••••••••

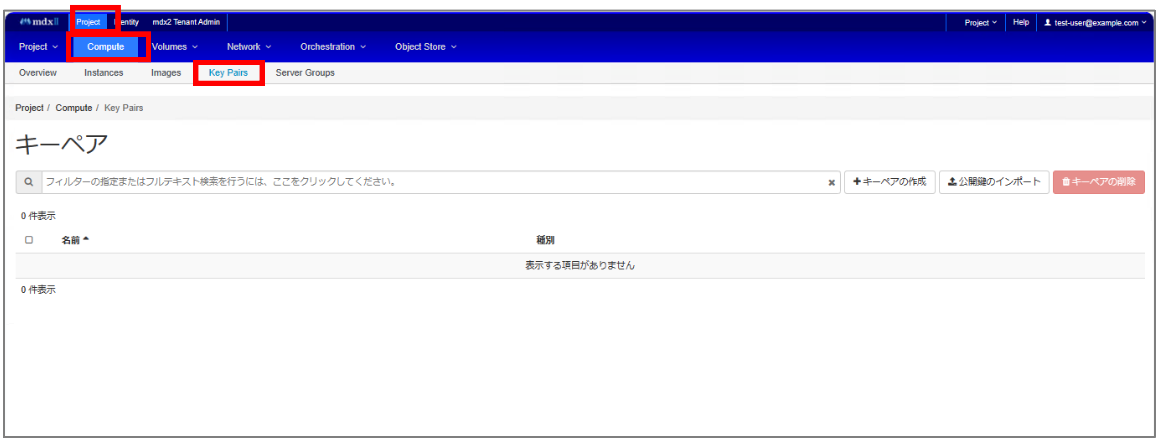
Confirm passphrase: ••••••••

Comment: XXXX@SMC-VM-DG-92

☑ bcrypt KDF format Number of rounds: 16

(2) Log in to the user portal. Please refer to "4.1.3. Login method" for the login method.

(3) Click the [Project] menu > [Compute] panel > [Key Pairs] tab.



Project / Compute / Key Pairs

キーペア

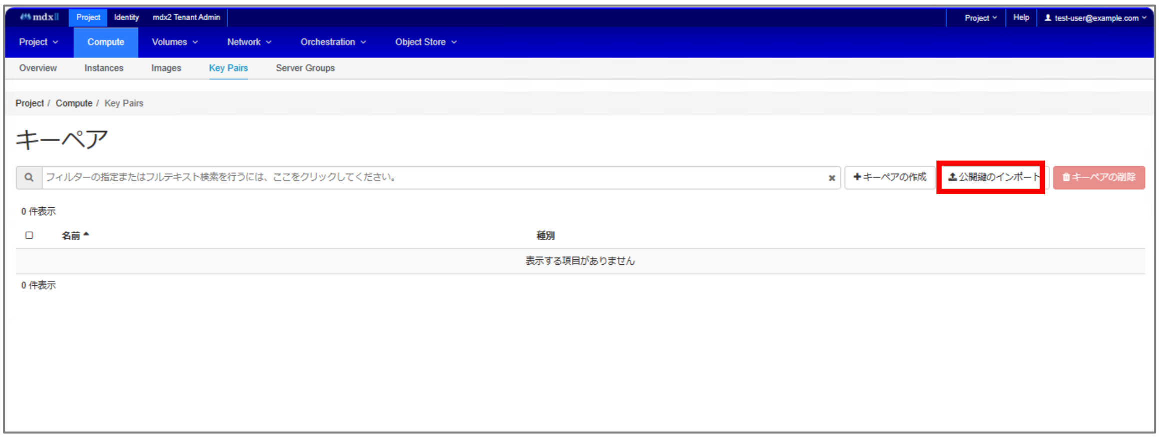
フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

0 件表示

□	名前 ▲	種別
表示する項目がありません		

0 件表示

(4) Click the [Import public key] button.



Project / Compute / Key Pairs

キーペア

フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

0 件表示

□	名前 ▲	種別
表示する項目がありません		

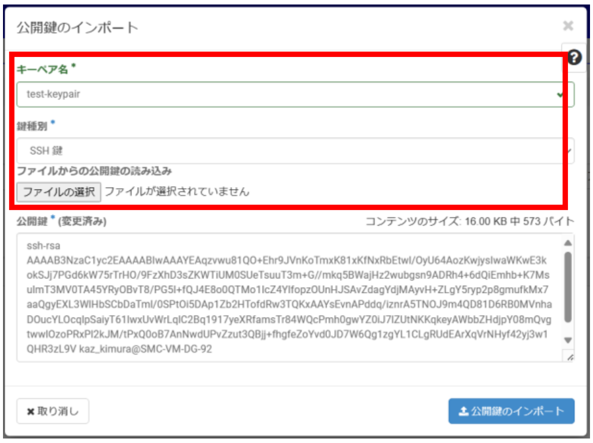
0 件表示

(5) Enter and select the following on the public key import screen, and click the [Import public key] button.

・Key pair name: *Optional

・Key type: SSH key

・Select file: *Select the public key you created.



公開鍵のインポート

キーペア名 *

test-keypair

鍵種別 *

SSH 鍵

ファイルからの公開鍵の読み込み

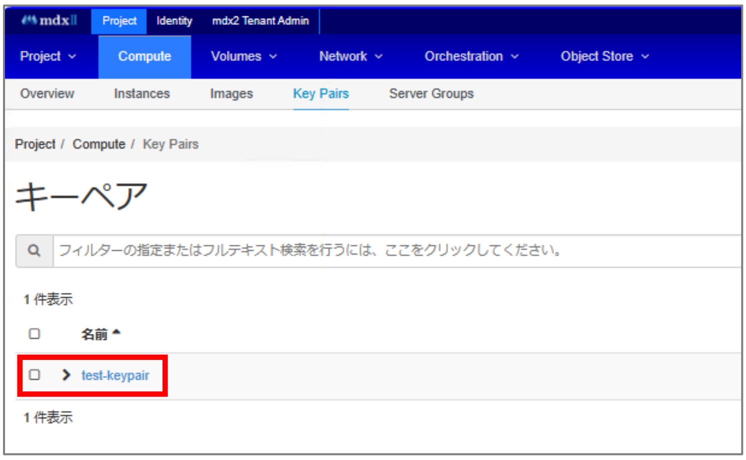
ファイルの選択 ファイルが選択されていません

公開鍵 * (変更済み) コンテンツのサイズ: 16.00 KB 中 573 バイト

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAYEAqzvwu81QO+Ehr9JVnKoTmxK81xKfNxRbEtwl/OyU64AozKwjyslwaWKwE3k
okSJj7PGd6kW75rTrHO/9FzXhD3sZKWTiUM0SUeTsuuT3m+G//mkq5BWajHz2wubgsn9ADRh4+6dQiEmhb+K7Ms
ulmT3MV0TA45YRyOBvT8/PG5I+fQJ4E8o0QTMo1IcZ4YIfopzOUnHJSAvZdagYdjMAyvH+ZLgY5ryp2p8gmufkMx7
aaQgyEXL3WIHbSCbDaTml/0SPtOi5DAp1Zb2HTofdRw3TQKxAAYsEvnAPddq/iznrA5TNOJ9m4QD81D6RB0MVnha
DOucYLOcqlpSaiyT61lwxUvWrLqlC2Bq1917yeXRfamsTr84WQcPmh0gwYZ0iJ7lZUtNKKqkeyAWbbZHdjpY08mQvg
twwlOzoPRxPl2kJM/tPxQ0oB7AnNwdUPvZzut3QBjj+fhgfeZoYvd0JD7W6Qg1zgYL1CLgRUdEArXqVrNHyf42yj3w1
QHR3zL9V kaz_kimura@SMC-VM-DG-92
```

(6) Once the key pair registration is complete, the registered key pair will be displayed in the list. Your web browser will start downloading the private key, so download it.*This key will be used to access the virtual machine, so please keep it carefully in case it gets lost or leaked.

(7) Once the key pair registration is complete, the registered key pair will be displayed in the list.



キーペア

フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

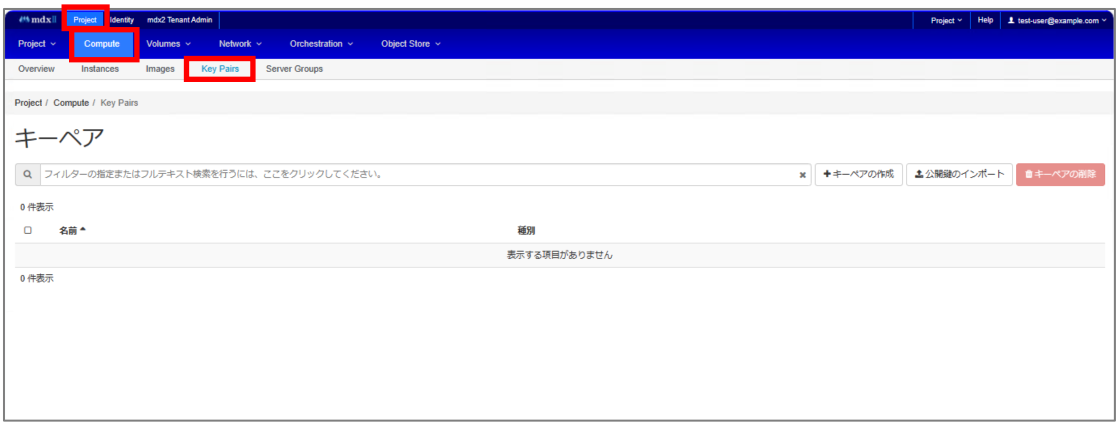
1 件表示

□	名前
□	test-keypair

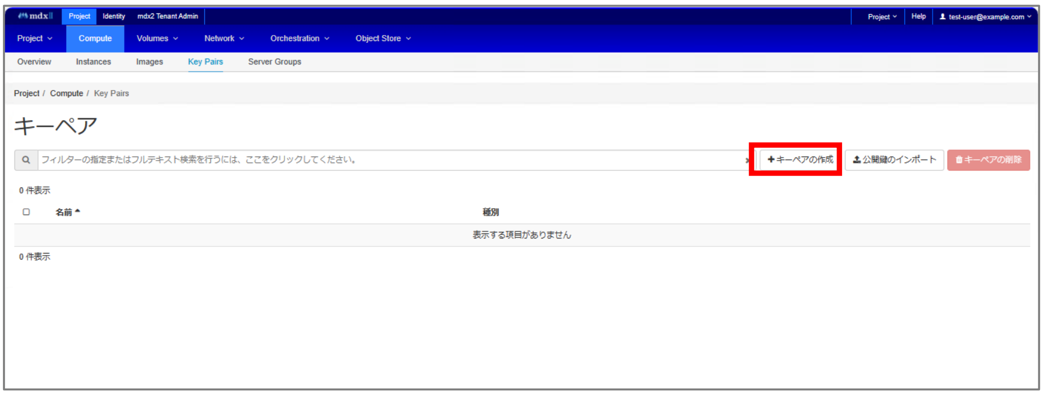
1 件表示

4.1.5.2. Registration by new creation

(1) Click the [Project] menu > [Compute] panel > [Key Pair] tab.



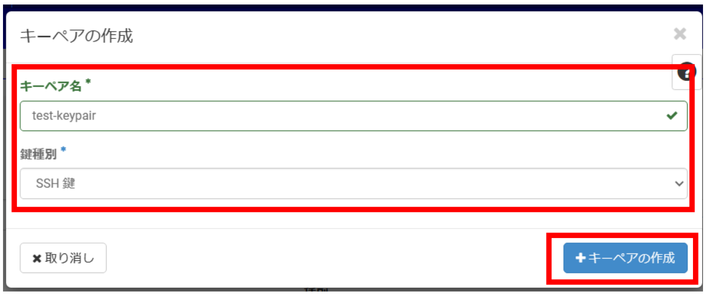
(2) Click the [Create Key Pair] button.



(3) Enter the following items and click the [Create Key Pair] button.

・Key pair name: *Optional

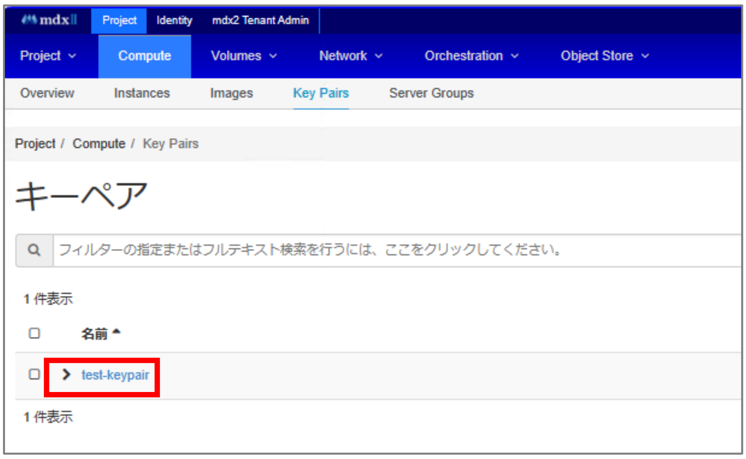
・Key type: SSH key


キーペアの作成

キーペア名 *: test-keypair

鍵種別 *: SSH 鍵

(4) Once the key pair registration is complete, the registered key pair will be displayed in the list.



1 件表示

□	名前 ▲
□	> test-keypair

1 件表示

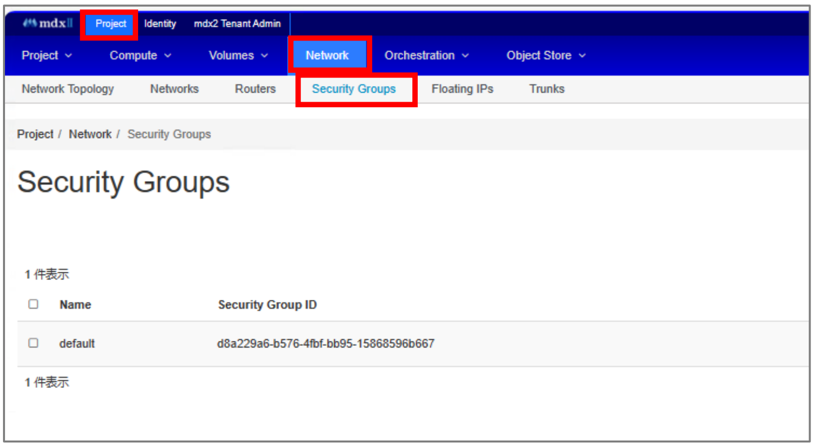
4.1.6. Creating a security group

A security group is a set of IP filter rules that control the sending and receiving of communications on virtual machines.

By default, a security group called "default" is provided. "default" allows all outgoing traffic and denies all incoming traffic from sources other than virtual machines in the same security group.

You can also create a new security group for your project. Below are the steps to create a new rule and apply a rule that allows ICMP and SSH.

(1) Click the [Project] menu > [Network] panel > [Security Groups] tab.

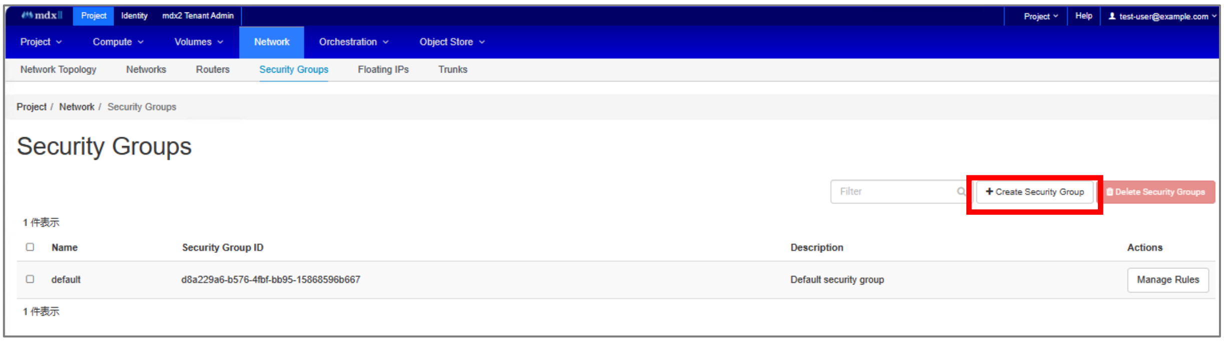


1 件表示

□	Name	Security Group ID
□	default	d8a229a6-b576-4fbf-bb95-15868596b667

1 件表示

(2) Click the [+Create Security Group] button.

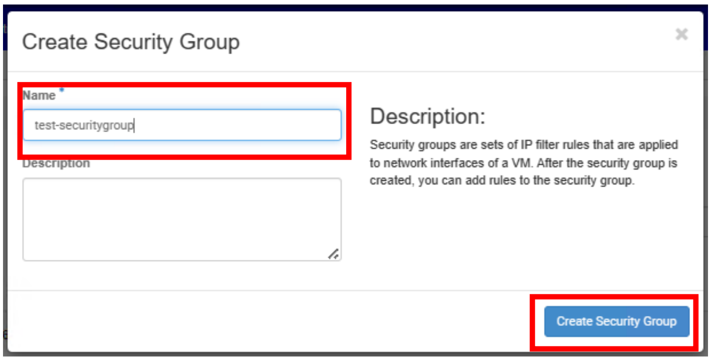


1 件表示

□	Name	Security Group ID	Description	Actions
□	default	d8a229a6-b576-4fbf-bb95-15868596b667	Default security group	Manage Rules

1 件表示

(3) Click the [Create Security Group] button.



Create Security Group

Name *

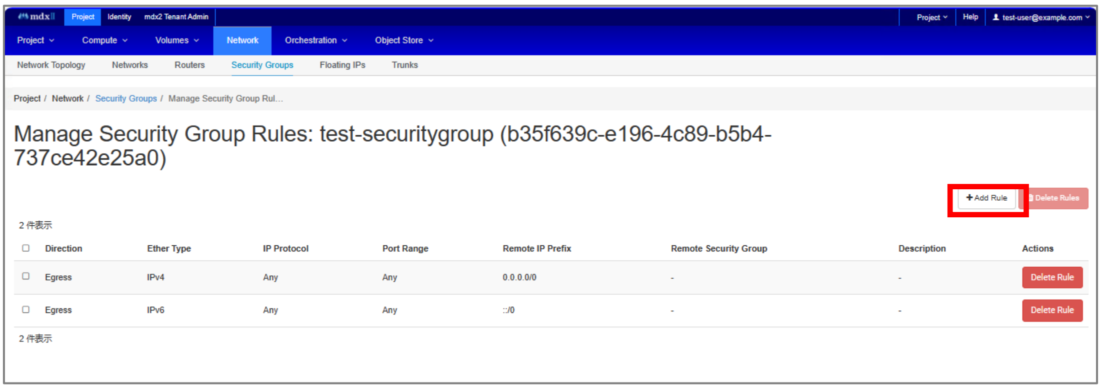
test-securitygroup

Description

Description:

Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

(4) Click the [+Add Rule] button.



Project / Network / Security Groups / Manage Security Group Rul...

Manage Security Group Rules: test-securitygroup (b35f639c-e196-4c89-b5b4-737ce42e25a0)

2 件表示

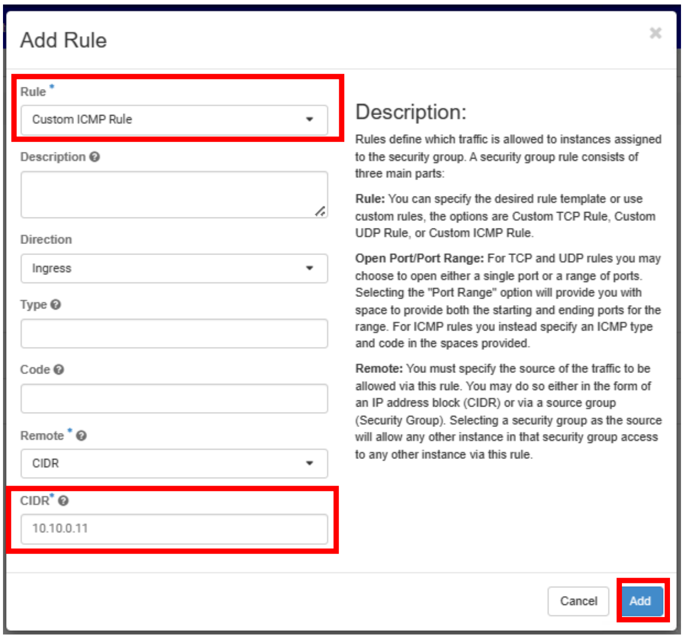
□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
□	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule

2 件表示

(5) Enter the following items and click the [Add] button.

・Rules: Custom ICMP Rule

・CIDR: *Enter the IP address of the access source to be allowed.



Add Rule

Rule *: Custom ICMP Rule

Description

Direction: Ingress

Type

Code

Remote *: CIDR

CIDR *: 10.10.0.11

Description:

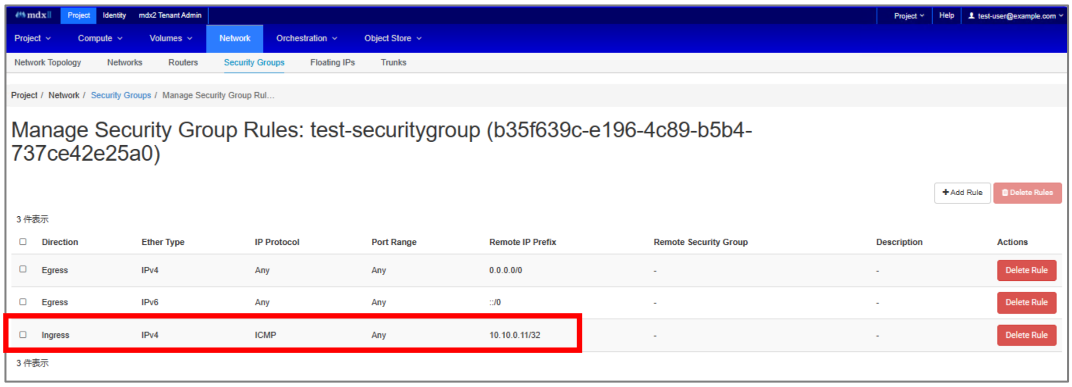
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

(6) The created ICMP rules will be displayed in a list.



Project / Network / Security Groups / Manage Security Group Rul...

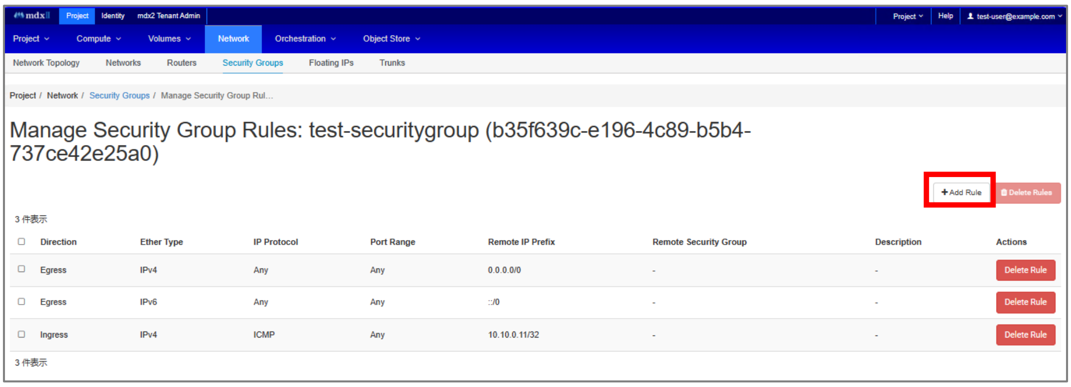
Manage Security Group Rules: test-securitygroup (b35f639c-e196-4c89-b5b4-737ce42e25a0)

3 件表示

☐	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	10.10.0.11/32	-	-	Delete Rule

3 件表示

(7) Click the [+Add Rule] button.



Project / Network / Security Groups / Manage Security Group Rul...

Manage Security Group Rules: test-securitygroup (b35f639c-e196-4c89-b5b4-737ce42e25a0)

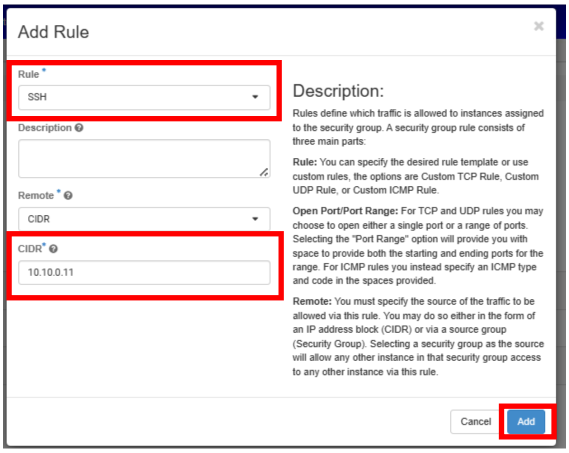
3 件表示

☐	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	10.10.0.11/32	-	-	Delete Rule

3 件表示

(8) Enter the following items and click the [Add] button.

- Rule: SSH
- CIDR: *Enter the IP address of the access source to be allowed.



Add Rule

Rule * SSH

Description

Remote * CIDR

CIDR* 10.10.0.11

Description:

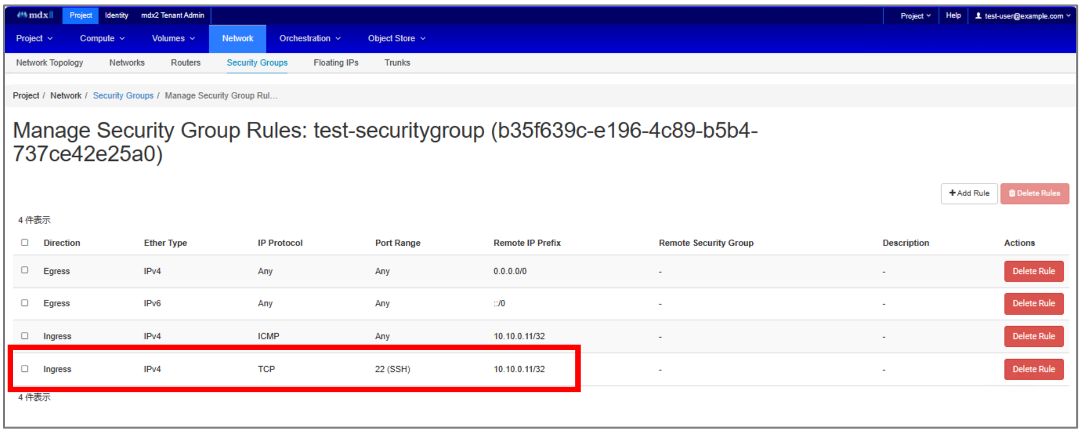
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

(9) The SSH rules you created will be displayed in a list.



Manage Security Group Rules: test-securitygroup (b35f639c-e196-4c89-b5b4-737ce42e25a0)

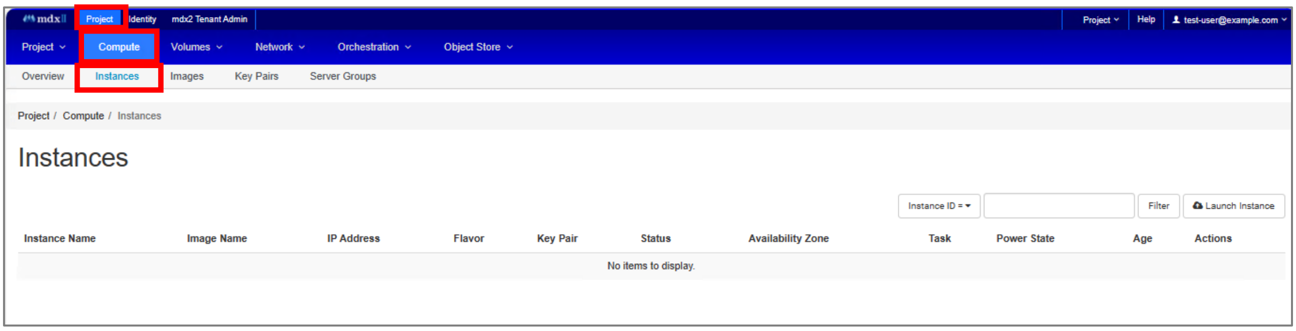
4 件表示

□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
□	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
□	Ingress	IPv4	ICMP	Any	10.10.0.11/32	-	-	Delete Rule
□	Ingress	IPv4	TCP	22 (SSH)	10.10.0.11/32	-	-	Delete Rule

4 件表示

4.1.7. Creating a virtual machine

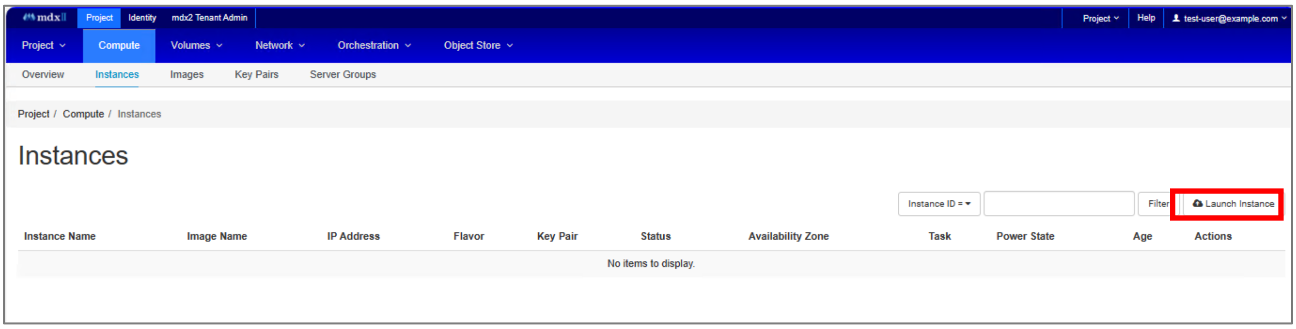
(1) Click the [Project] menu > [Compute] panel > [Instances] tab.



Instances

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
No items to display.										

(2) Click the [Launch Instance] button.

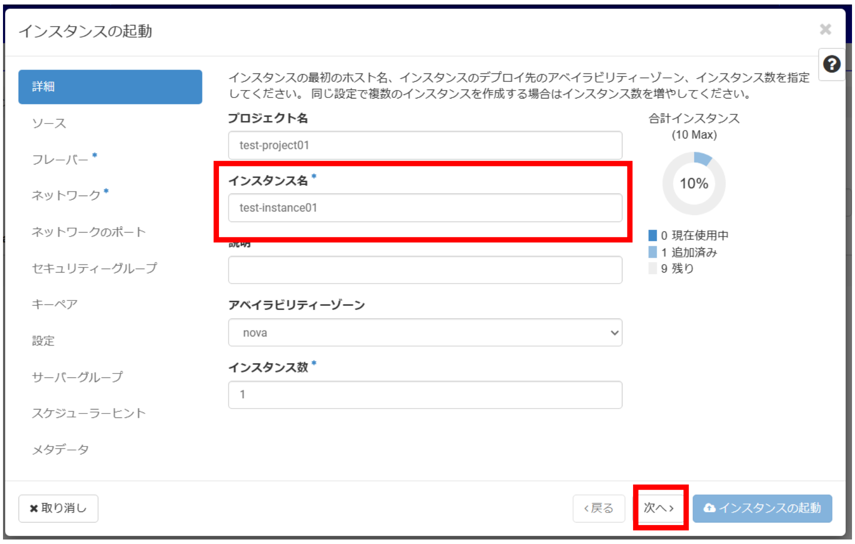


Instances

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
No items to display.										

(3) Enter the following items and click the [Next] button.

・Instance name: *Optional



インスタンスの最初のホスト名、インスタンスのデプロイ先のアベイラビリティーゾーン、インスタンス数を指定してください。 同じ設定で複数のインスタンスを作成する場合はインスタンス数を増やしてください。

プロジェクト名: test-project01

インスタンス名 *: test-instance01

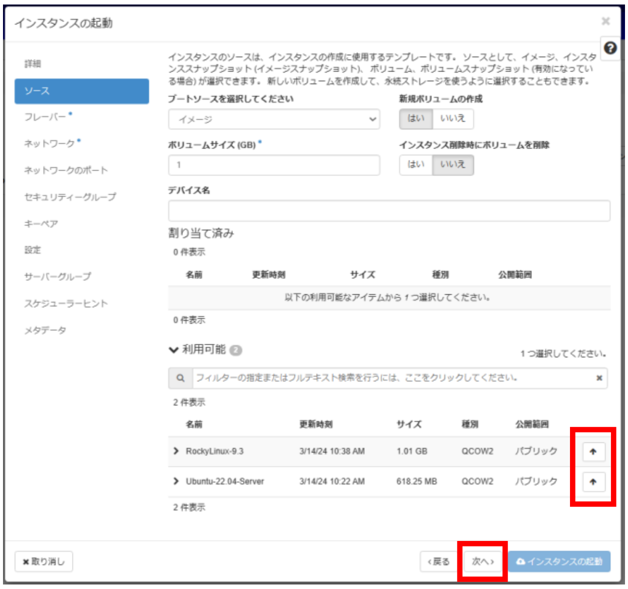
説明:

アベイラビリティーゾーン: nova

インスタンス数 *: 1

合計インスタンス
(10 Max)
10%
0 現在使用中
1 追加済み
9 残り

(4) Click the [↑] button of the image you want to use as the virtual machine's OS image from the available column. Click the Next button. The OS images prepared on the system side are RockyLinux 9.3 and Ubuntu 22.04 Server.



インスタンスのソースは、インスタンスの作成に使用するテンプレートです。ソースとして、イメージ、インスタンススナップショット (イメージスナップショット)、ボリューム、ボリュームスナップショット (有効になっている場合) が選択できます。新しいボリュームを作成して、永続ストレージを使うように選択することもできます。

ブートソースを選択してください: イメージ

新規ボリュームの作成: [✓ はい] いいえ

ボリュームサイズ (GB) *: 1

インスタンス削除時にボリュームを削除: はい [✓ いいえ]

デバイス名:

割り当て済み

0 件表示

名前	更新時刻	サイズ	種別	公開範囲
以下の利用可能なアイテムから 1 つ選択してください。				

0 件表示

利用可能 2　　1 つ選択してください。

フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

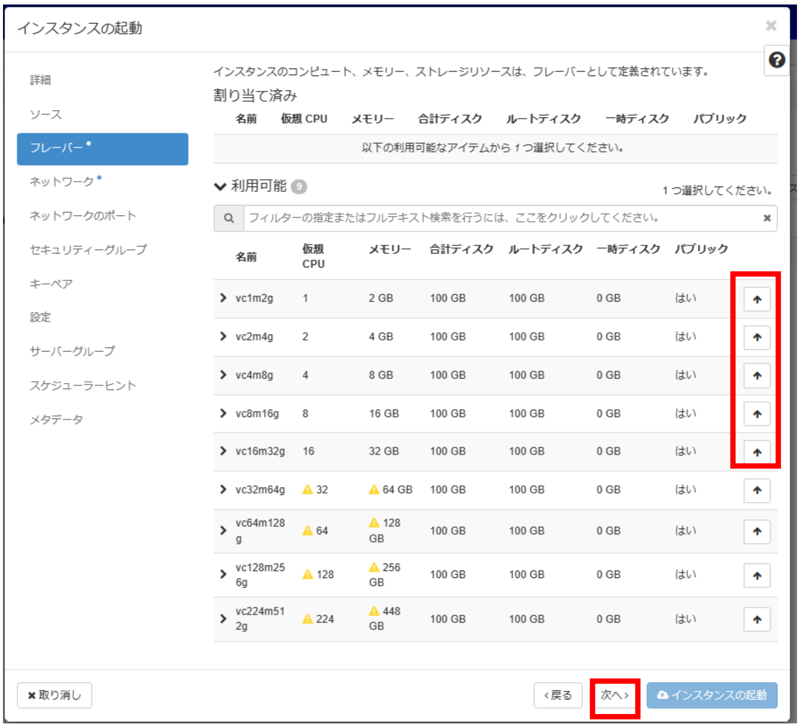
2 件表示

名前	更新時刻	サイズ	種別	公開範囲	
RockyLinux-9.3	3/14/24 10:38 AM	1.01 GB	QCOW2	パブリック	↑
Ubuntu-22.04-Server	3/14/24 10:22 AM	618.25 MB	QCOW2	パブリック	↑

2 件表示

(5) Click the [↑] button of the flavor that you want to select as the amount of resources to allocate to the virtual machine, and then click the [Next] button. If you use Luster mount, please select vc8m16g or higher flavor.

*Flavors with a yellow triangle mark cannot be used because they have exceeded the project quota.



インスタンスのコンピュート、メモリー、ストレージリソースは、フレーバーとして定義されています。

割り当て済み

名前	仮想 CPU	メモリー	合計ディスク	ルートディスク	一時ディスク	パブリック
以下の利用可能なアイテムから 1 つ選択してください。						

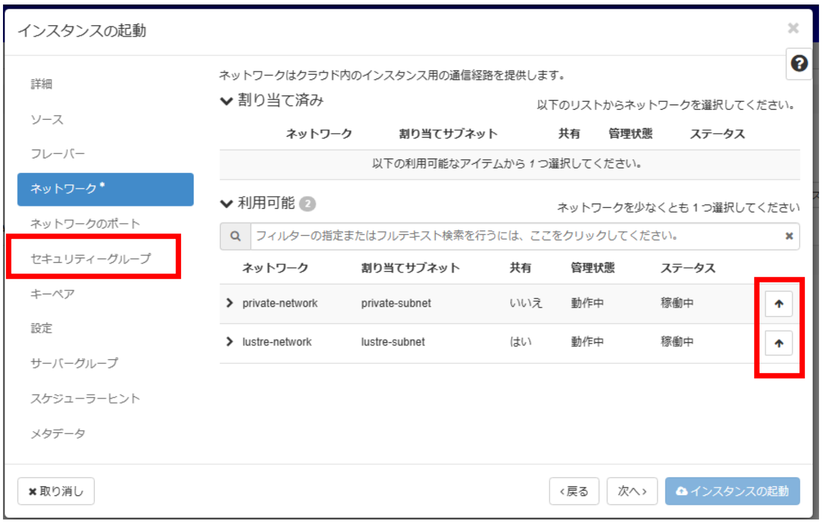
利用可能 9

1 つ選択してください。

フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

名前	仮想 CPU	メモリー	合計ディスク	ルートディスク	一時ディスク	パブリック
vc1m2g	1	2 GB	100 GB	100 GB	0 GB	はい
vc2m4g	2	4 GB	100 GB	100 GB	0 GB	はい
vc4m8g	4	8 GB	100 GB	100 GB	0 GB	はい
vc8m16g	8	16 GB	100 GB	100 GB	0 GB	はい
vc16m32g	16	32 GB	100 GB	100 GB	0 GB	はい
vc32m64g	⚠ 32	⚠ 64 GB	100 GB	100 GB	0 GB	はい
vc64m128g	⚠ 64	⚠ 128 GB	100 GB	100 GB	0 GB	はい
vc128m256g	⚠ 128	⚠ 256 GB	100 GB	100 GB	0 GB	はい
vc224m512g	⚠ 224	⚠ 448 GB	100 GB	100 GB	0 GB	はい

(6) Click the [↑] button for the network that connects to the virtual machine and click the [Security Group] tab.



ネットワークはクラウド内のインスタンス用の通信経路を提供します。

割り当て済み

以下のリストからネットワークを選択してください。

ネットワーク	割り当てサブネット	共有	管理状態	ステータス
以下の利用可能なアイテムから 1 つ選択してください。				

利用可能 2

ネットワークを少なくとも 1 つ選択してください

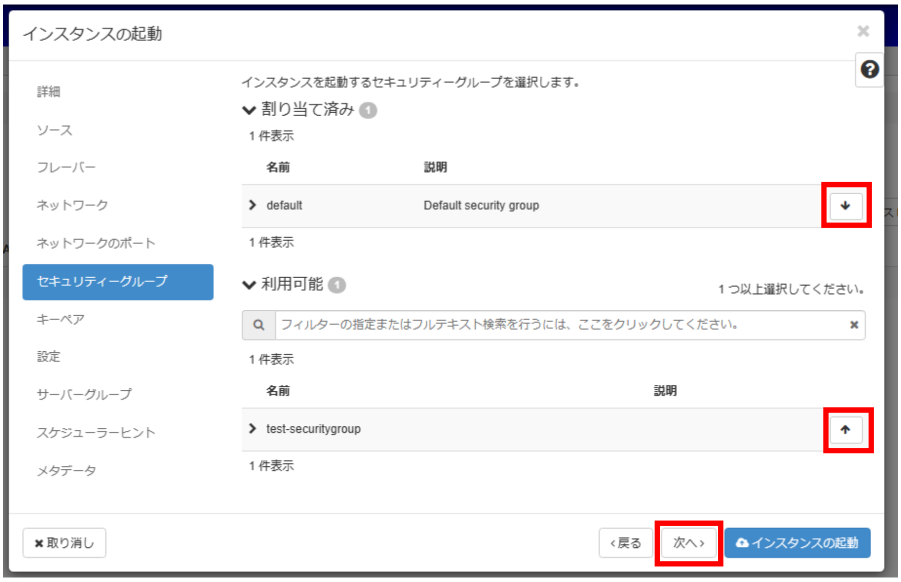
フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

ネットワーク	割り当てサブネット	共有	管理状態	ステータス
private-network	private-subnet	いいえ	動作中	稼働中
lustre-network	lustre-subnet	はい	動作中	稼働中

(7) Select the security group to apply to the virtual machine. [default] is applied by default. To change to the security group you created, click the [↑] button for the security group you want to select, and then click the [↓] button for [default].

After selecting the security group, click the [Next] button.

*Multiple selections are possible.



インスタンスを起動するセキュリティーグループを選択します。

割り当て済み 1

1 件表示

名前	説明
default	Default security group

1 件表示

利用可能 1　　1 つ以上選択してください。

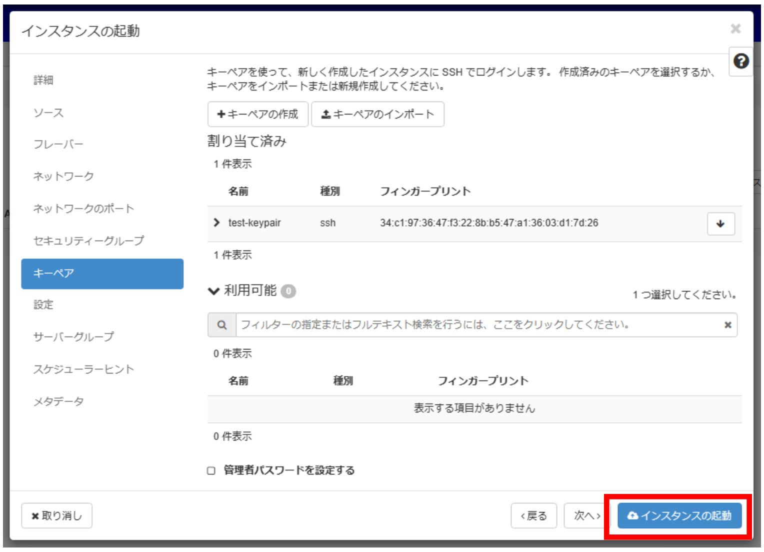
フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

1 件表示

名前	説明
test-securitygroup	

1 件表示

(8) Select the key pair (SSH public key) to be registered in the virtual machine. If there is only one registered key pair, it will be selected by default. If there are multiple key pairs, select the key pair to register using the [↑][↓] buttons. After selecting, click the [Create Instance] button.



キーペアを使って、新しく作成したインスタンスに SSH でログインします。 作成済みのキーペアを選択するか、キーペアをインポートまたは新規作成してください。

割り当て済み

1 件表示

名前	種別	フィンガープリント
test-keypair	ssh	34:c1:97:36:47:f3:22:8b:b5:47:a1:36:03:d1:7d:26

1 件表示

利用可能 0　　1 つ選択してください。

フィルターの指定またはフルテキスト検索を行うには、ここをクリックしてください。

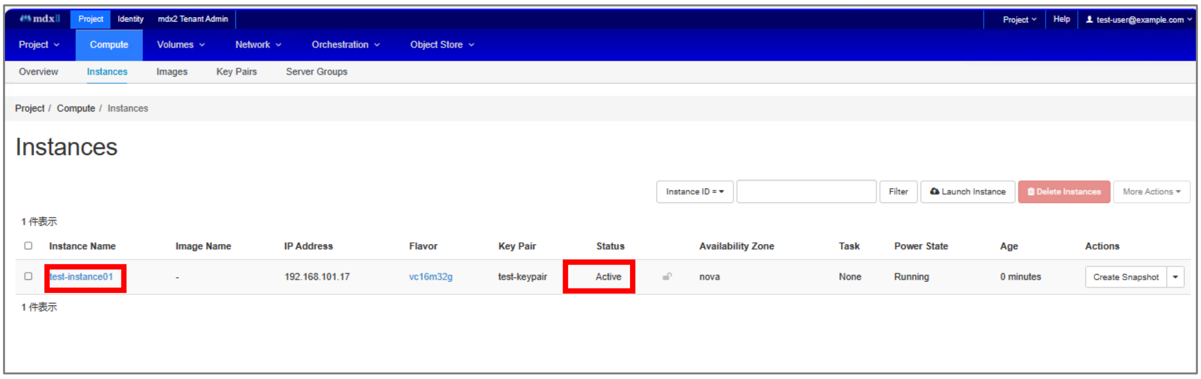
0 件表示

名前	種別	フィンガープリント
表示する項目がありません		

0 件表示

□ 管理者パスワードを設定する

(9) Confirm that the created virtual machine is displayed in the instance list and its Status is "Active".



Instances

1 件表示

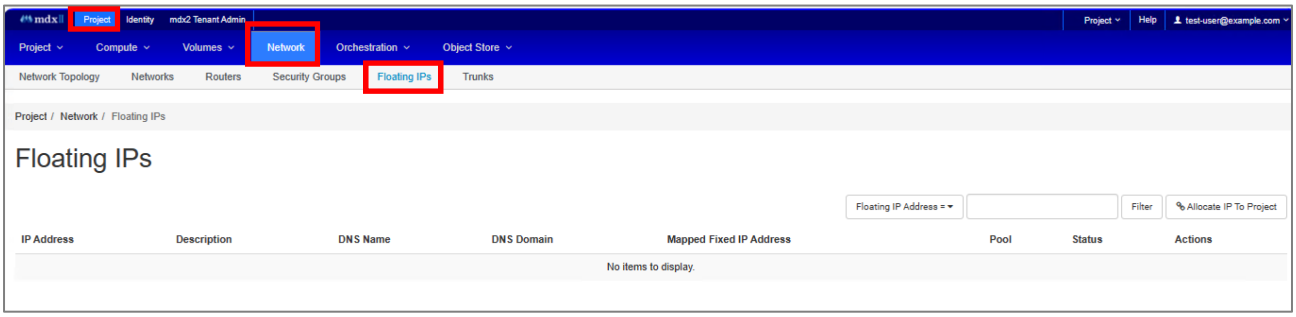
□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status		Availability Zone	Task	Power State	Age	Actions
□	test-instance01	-	192.168.101.17	vc16m32g	test-keypair	Active		nova	None	Running	0 minutes	Create Snapshot

1 件表示

4.1.8. Granting Floating IP

By assigning a floating IP to a virtual machine, you can enable communication with external networks such as the Internet.

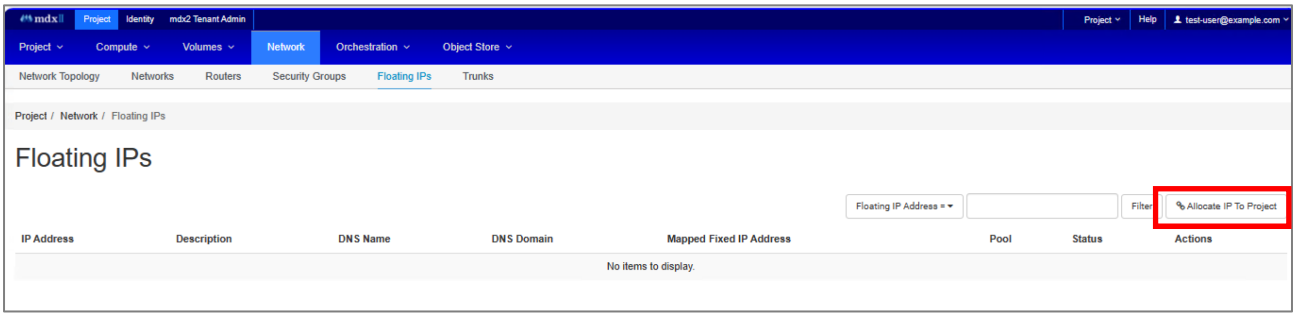
(1) Click the [Project] menu > [Network] panel > [Floating IPs] tab.



IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions

No items to display.

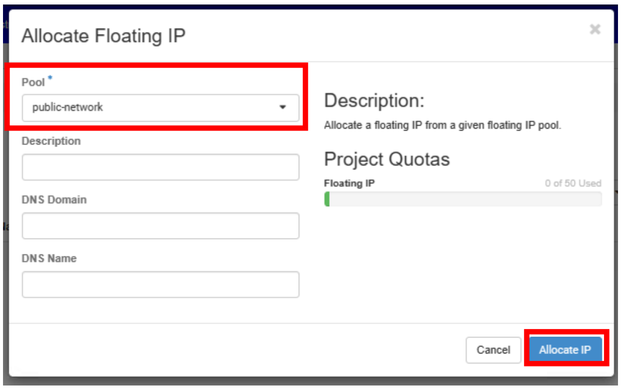
(2) Click the [Allocate IP To Project] button.



IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions

No items to display.

(3) Select "public-network" from the [Pool] pull-down menu and click the [Allocate IP] button.



Pool *: public-network

Description:

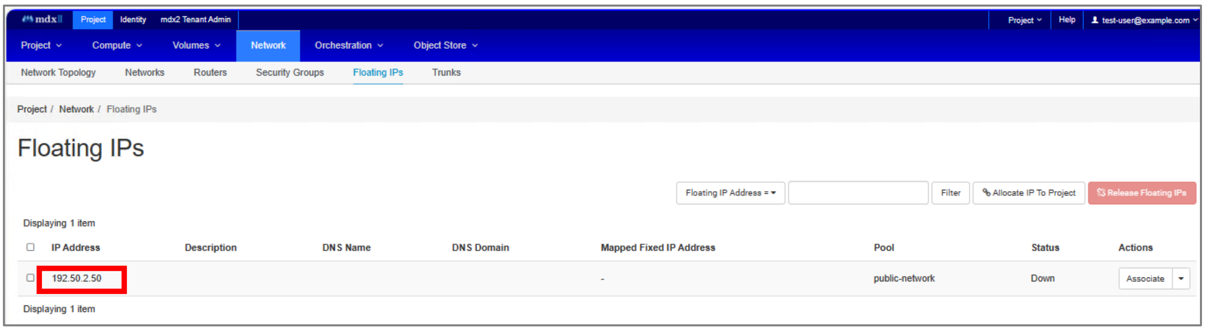
DNS Domain:

DNS Name:

Description:
Allocate a floating IP from a given floating IP pool.

Project Quotas
Floating IP 0 of 50 Used

(4) The IP address secured in the Floating IP list will be displayed.

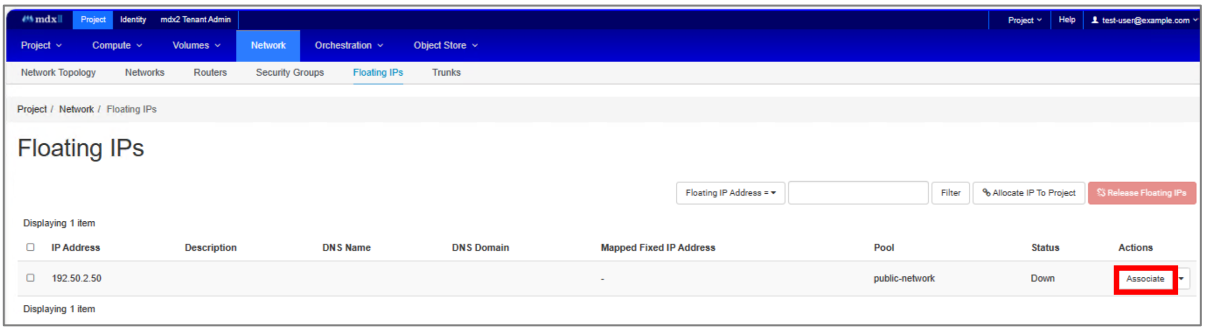


Displaying 1 item

□	IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions
□	192.50.2.50				-	public-network	Down	Associate

Displaying 1 item

(5) Click the [Associate] button.

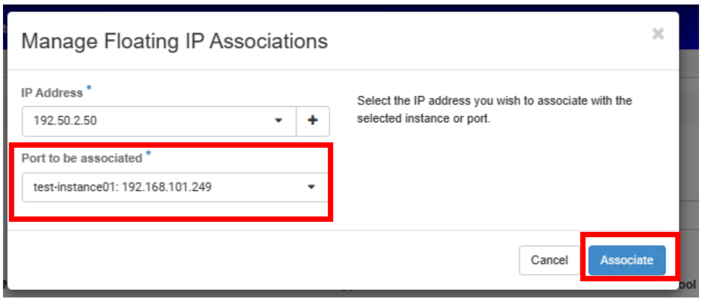


Displaying 1 item

	IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions
□	192.50.2.50				-	public-network	Down	Associate

Displaying 1 item

(6) Select the virtual machine to which you want to allocate a floating IP from the pull-down menu of [Port to be associated], and click the [Associate] button.

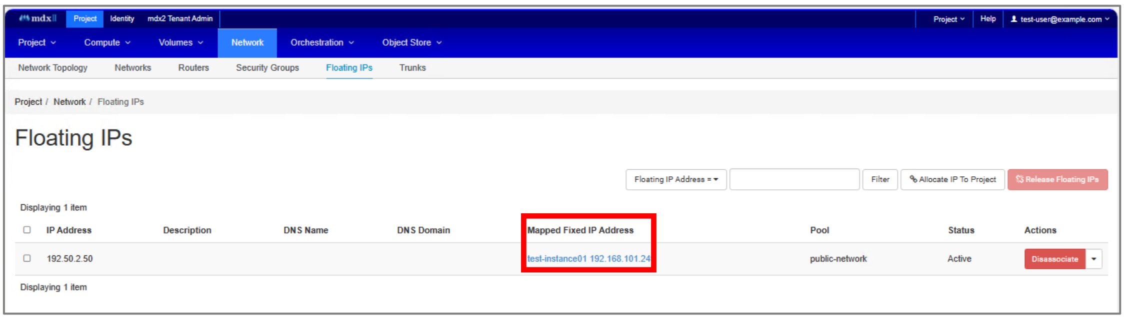


IP Address *
192.50.2.50

Port to be associated *
test-instance01: 192.168.101.249

Select the IP address you wish to associate with the selected instance or port.

(7) Confirm that the virtual machine name and Floating IP assigned to Mapped Fixed IP Address in the list are displayed.



Displaying 1 item

	IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions
□	192.50.2.50				test-instance01 192.168.101.24	public-network	Active	Disassociate

Displaying 1 item

4.1.9. Accessing virtual machines

Access the floating IP assigned to the virtual machine using SSH. For SSH access, specify the private key of the key pair specified when creating the virtual machine. The command to access via SSH is as follows.

```
$ ssh -i <SSH private key> -l <initial username> <Floating IP of virtual machine>

Example)
$ ssh -i ~/.ssh/id_rsa_mdx -l mdxuser   192.50.2.50
```

*Create a virtual machine from the RockyLinux 9.3 and Ubuntu 22.04 LTS OS images prepared on the system side. If created, the initial user name will be "mdxuser".
*If SSH access to the virtual machine is not possible, make sure the necessary communication is allowed in the security group. Please confirm that.

4.1.10. Use of file server

It is possible to use the file server area from a virtual machine. There are two ways to use it:

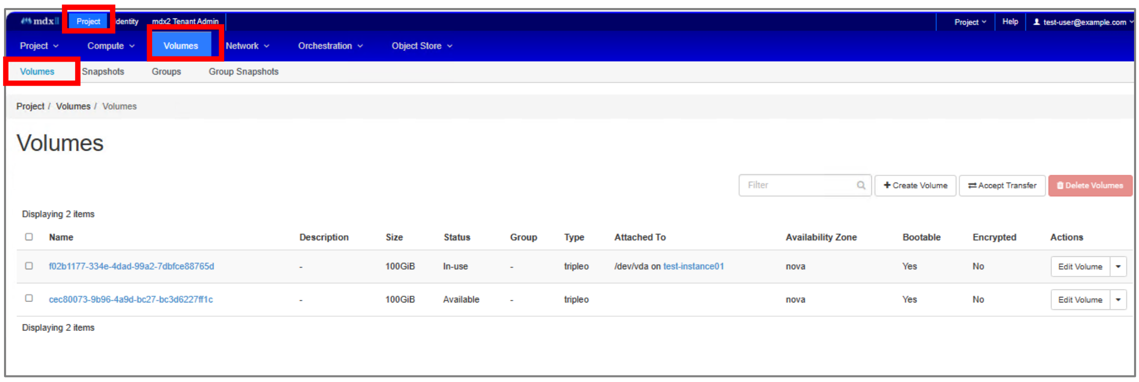
- Use Cinder volume
  - File server area can be used more easily than Luster mount.
  - Only one virtual machine can be connected to one Cinder volume.
  - Available capacity is within the project quota (resource amount limit)

- Use with Luster mount from virtual machine
  - Access performance is higher than using Cinder volume.
  - To use it, you need to apply to the system administrator and set up the Luster client.
  - Available capacity is specified at the time of application separately from the project quota.

Please follow the steps below according to your usage.

4.1.10.1. Using Cinder volumes

(1) Click the [Project] menu > [Volume] panel > [Volumes] tab.



Project / Volumes / Volumes

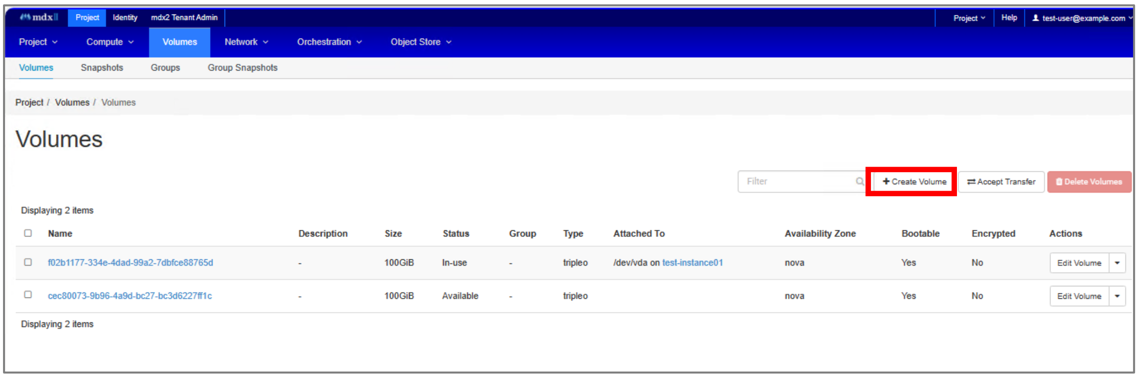
Volumes

Displaying 2 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume

Displaying 2 items

(2) Click the [+Create Volume] botton.



Project / Volumes / Volumes

Volumes

Displaying 2 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume

Displaying 2 items

(3) Enter the following items and click the [Create Volume] button.

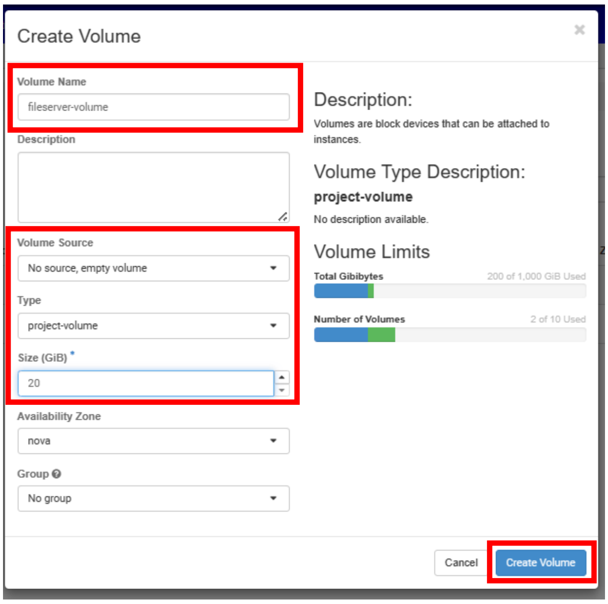
*The default for [Type] is "tripleo", but be sure to select "project-volume".

・Volume Name: *Optional

・Volume Source: No source specified (empty volume)

・Type: project-volume

・Size(GiB): *Specify the capacity you want to use within the quota



Create Volume ×

Volume Name: fileserver-volume

Description:

Volume Source: No source, empty volume

Type: project-volume

Size (GiB) *: 20

Availability Zone: nova

Group: No group

Description:

Volumes are block devices that can be attached to instances.

Volume Type Description:

project-volume

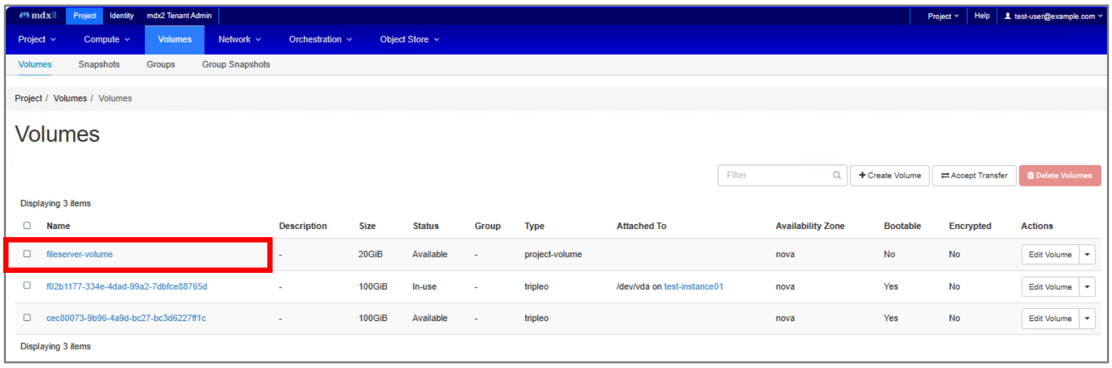
No description available.

Volume Limits

Total Gibibytes: 200 of 1,000 GiB Used

Number of Volumes: 2 of 10 Used

(4) The created volume will be displayed in the volume list.



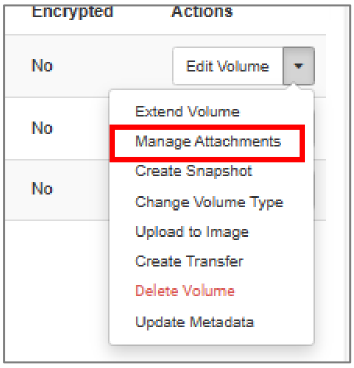
Volumes

Displaying 3 items

☐	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
☐	fileserver-volume	-	20GiB	Available	-	project-volume		nova	No	No	Edit Volume ▾
☐	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume ▾
☐	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume ▾

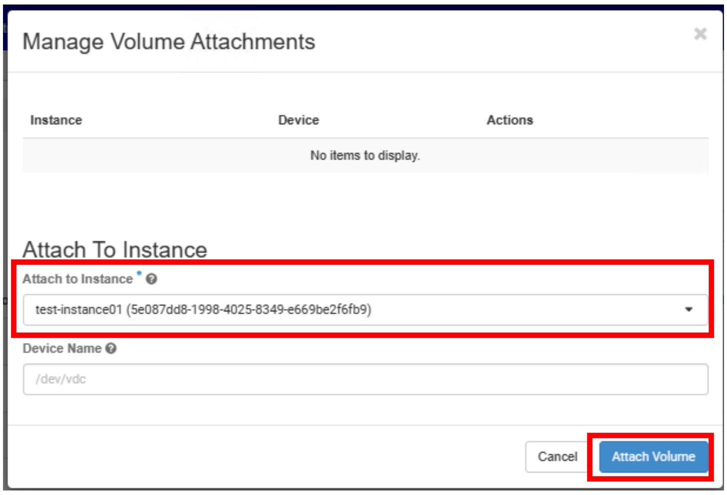
Displaying 3 items

(5) Click [Manage Attachments] from the pull-down menu on the right side of the volume you created.



(6) Enter the following items and click the [Attach Volume] button.

・Attach to Instance: *Specify the instance to which the volume will be connected



Manage Volume Attachments

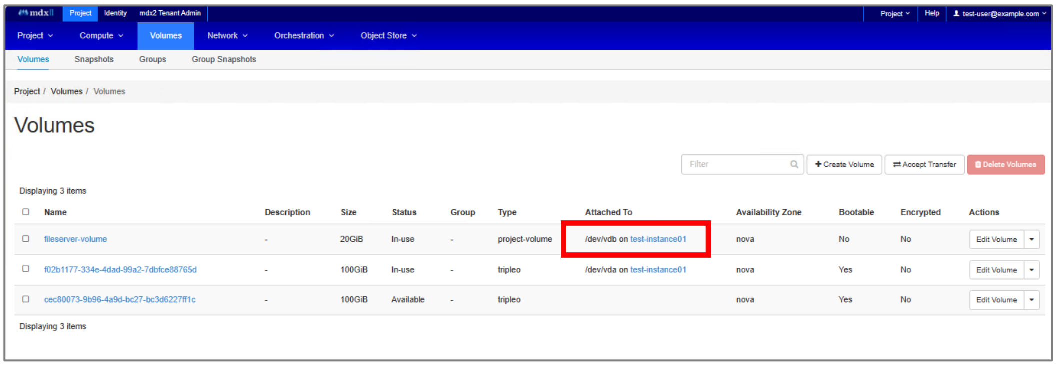
Instance	Device	Actions
No items to display.		

Attach To Instance

Attach to Instance *: test-instance01 (5e087dd8-1998-4025-8349-e669be2f6fb9)

Device Name: /dev/vdc

(7) Confirm that the virtual machine name and device name to which the volume is attached are displayed in Attached To in the volume list.



Project / Volumes / Volumes

Volumes

Displaying 3 items

	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	fileserver-volume	-	20GiB	In-use	-	project-volume	/dev/vdb on test-instance01	nova	No	No	Edit Volume
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume

Displaying 3 items

These are the steps to connect a volume to a virtual machine.

The connected volume can be seen from the virtual machine using the device name confirmed above (e.g. /dev/vdb). Since the contents of the volume are empty, you will need to create a file system depending on your usage.

The following procedure describes an example of using a connected volume as an XFS file system.

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

4.1.10.2. Lustre Mount

Please send an email to your system administrator with the following information and request to use Luster mount.

```
----- Luster mount usage application format -----
Project name: *Enter the project name
Virtual machine IP address: *IP address assigned to the virtual machine (192.168.[100,10
1].X)
   Usage capacity: *Listed in GB
   -----------------------------------------------------------
```

*Based on the above information, the system administrator will set the necessary information on the file server.

After your system administrator notifies you that Luster mounts are available, you will need to configure the Luster client on your virtual machine. The RokcyLinux 9.3 and Ubuntu 22.04 LTS OS images prepared on the system side include Luster client packages and configuration files.
The following describes how to mount Luster on a virtual machine created with an OS image prepared by the system.

(1) Log in to the virtual machine and switch to the root account using sudo su, etc.

(2) Check the interface name where the Luster network IP address (192.168.[100,101].X) is set on the virtual machine.

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

(3) Correct the interface name specified in /etc/modprobe.d/lustre.conf to the confirmed interface name. *Bold parts will be corrected.

```
   # 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) Correct the interface name specified in /etc/sysconfig/lustre_client to the confirmed interface name.
* The file path is different between Rocky Linux (RHEL series) and Ubuntu Server.
*Bold parts will be corrected.

- Rocky Linux

```
   # vi /etc/sysconfig/lustre_client
   …omission…
```

```
#+++++++++++++++++++++++++++++++++++++++
# LNET Interface
#
IF1=eth0
…omission…
```

- Ubuntu Server

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

(5) Start lustre_client.service.

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

(6) Confirm that Luster mount is possible.

```
# 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) Enable automatic startup of lustre_client.service so that Lustre mounts automatically when the virtual machine OS starts. (Any)

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

These are the steps to configure the Luster client.
When handling data in the file server area, please use the "/lustre" directory mounted by Lustre.

4.2. File Server

4.2.1. S3 Access Method

The file-server system includes a server for S3 access. The S3 endpoint of the file server is below.
S3 endpoint: s3gwlustre.osaka.mdx.jp

In order to synchronize your local data on the file server and access it from the rclone command (described later) or online storage service, you need to create an access key/secret key and an S3 bucket to which the user will connect.

Since work is required on the S3 access server of the file server, ask your system administrator for the settings. If you wish to use S3, please send a request email using the format below.

E-mail：mdx2-system@cmc.osaka-u.ac.jp
Subject： Configuration request for file server S3 access

```
Dear System Administrators

I would like to configure S3 access to the file server.

full name:
 Project name:
 User name:
 UID:
 GID:
 Bucket name:
```

- Bucket name: Set arbitrarily using half-width alphanumeric characters

rclone is one way to access S3 using CLI. Install the following packages to remotely connect to a bucket on a file server with rclone. (For Rocky)

```
$ sudo dnf install rclone
```

In order to access S3 with the rclone command, you need to set remote connection config. You can add, edit, and delete settings interactively using the following commands.

```
$ rclone config
```

Below, select the numbered option to set new connection config. To complete the setup, you have to get the access key and secret key of the connected S3.

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

```
    ¥ "s3"
(omitted)
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.
(omitted)
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.
(omitted)
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
--------------------
```

Verify that you can access S3 with the connection settings created above. The following command can output a list of files existing in the bucket.

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

For example, use the following command to transfer data.

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

4.3. Object Storage

4.3.1. Application for use

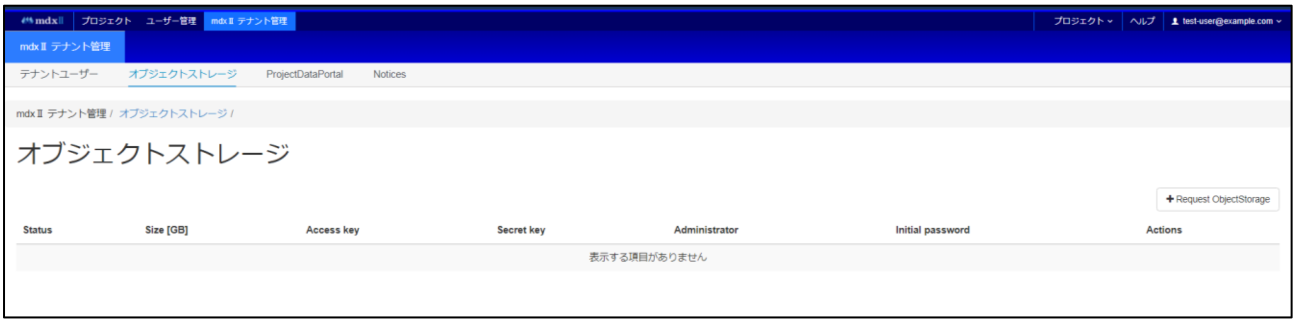
This section describes how to apply for object storage usage on the object storage application management screen. And, how to change the size after completing the object storage application.

4.3.1.1. New application for object storage

After logging in to OpenStaack, please proceed as follows from the tabs at the top of the page.

mdx II tenant management > Object Storage

You can apply for new object storage on the object storage application management page. The number of object storages that can be requested per project is 1. Click the "Request ObjectStorage" button on the right side of the page.

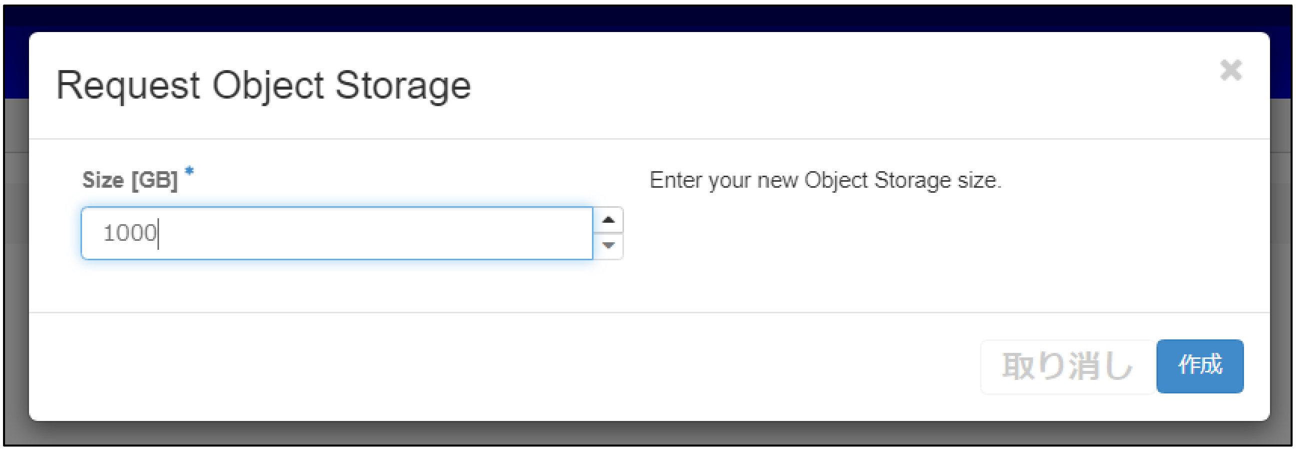


オブジェクトストレージ

Status	Size [GB]	Access key	Secret key	Administrator	Initial password	Actions
表示する項目がありません						

When you press the "Request ObjectStorage" button, a form to enter the size will be displayed as shown below. Please enter the size (GB) of object storage you are requesting.

The size that can be requested is 1,000 GB to 100,000 GB. To apply with the size you entered, press the "Create" button.



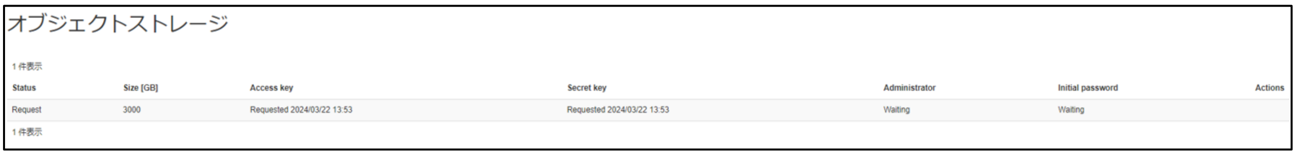
Request Object Storage

Size [GB] *

1000

Enter your new Object Storage size.

Once the application is completed, the application information will be displayed in the table. After applying, "Request" will be displayed in the Status column. Please wait for the object storage configuration to complete. You may have to wait up to 10 minutes. Please try refreshing the page/re-logging after 10 minutes.



オブジェクトストレージ

1 件表示

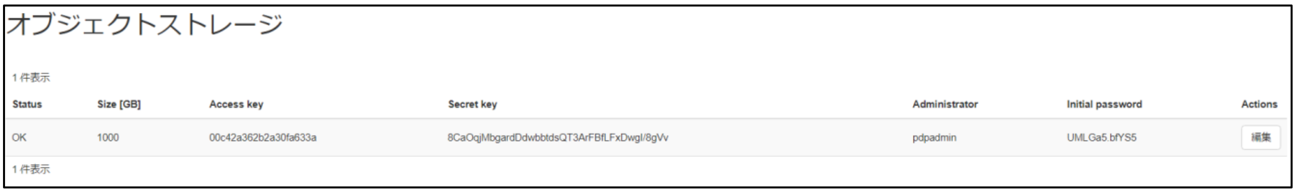
Status	Size [GB]	Access key	Secret key	Administrator	Initial password	Actions
Request	3000	Requested 2024/03/22 13:53	Requested 2024/03/22 13:53	Waiting	Waiting	

1 件表示

When the object storage settings are completed, the Status column will become "OK" and connection information will be shown in the image below. Please confirm that the credential information is displayed in the Access key column and Secret key column.

In addition, object storage management user information is displayed in the Administrator column and Initial password column. This is required to log in to Nextcloud and LDAP Account Manager, which are applied from the ProjectDataPortal application management page.

*The Initial password value is fixed and continues to be displayed. Please change your password after logging in for the first time.



オブジェクトストレージ

1 件表示

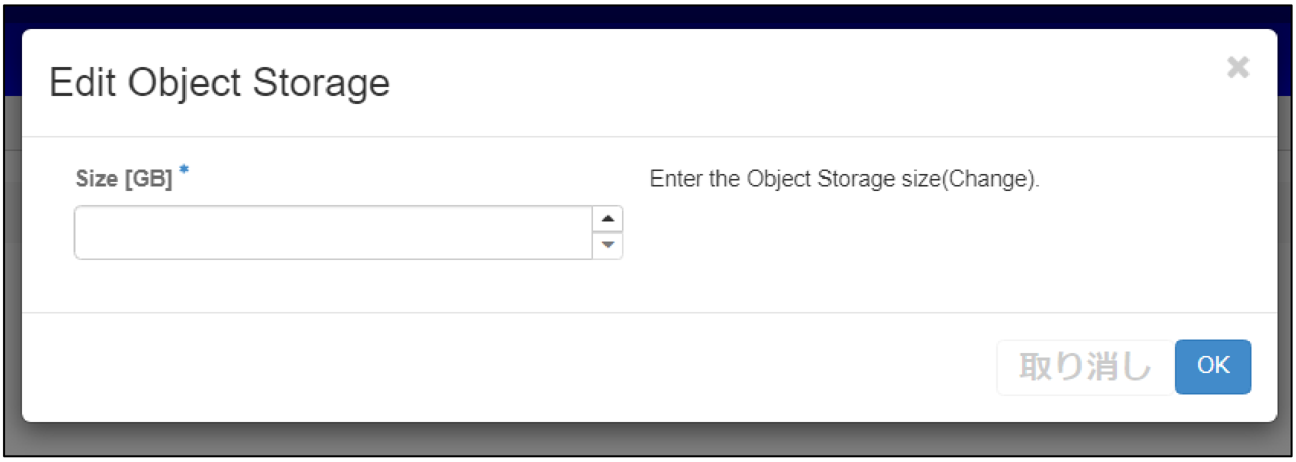
Status	Size [GB]	Access key	Secret key	Administrator	Initial password	Actions
OK	1000	00c42a362b2a30fa633a	8CaOqjMbgardDdwbbtdsQT3ArFBfLFxDwgl/8gVv	pdpadmin	UMLGa5.bfYS5	編集

1 件表示

4.3.1.2. Resizing object storage

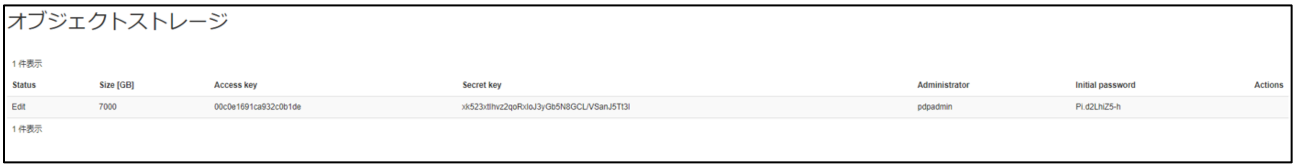
After completing the object storage settings, the "Edit" button will be available from the Actions column. By pressing the edit button, you can apply to change the size of the configured object storage. After pressing the edit button, the following size change request form will be displayed.

You cannot reduce the size from the already set size, you can only request an expansion. The maximum size that can be requested is 100,000 GB. If you wish to change the size you have entered, please press the "OK" button.



Once the change request is complete, the changed size will be displayed in the Size [GB] column of the table. After applying, "OK" will still be displayed in the Status column, but please refrain from pressing the "Edit" button again. If you wait for about 2 minutes and refresh the page/log in again, the Status column will be updated to "Edit".

Please wait for the object storage configuration to complete. You may have to wait up to 10 minutes. Please try refreshing the page/re-logging in every 10 minutes.


オブジェクトストレージ

1 件表示

Status	Size [GB]	Access key	Secret key	Administrator	Initial password	Actions
Edit	7000	00c0e1691ca932c0b1de	xk523xtlhvz2qoRxloJ3yGb5N8GCL/VSanJ5Tt3l	pdpadmin	Pi.d2LhiZ5-h	

1 件表示

Once the object storage configuration is complete, the Status column will be "OK". There is no change in the connection information from before the resize.

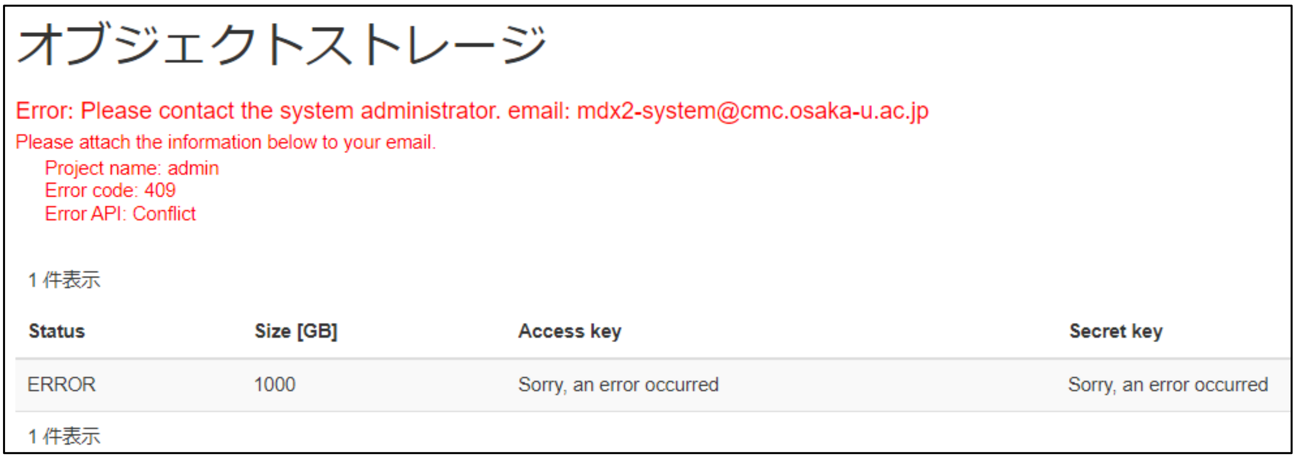
4.3.1.3. Object storage configuration error

After applying for object storage, object storage may return an API error during configuration. Even if an error occurs, the reconfiguration process will be performed and the configuration may be completed.

If the situation does not improve even after waiting 30 minutes from the time the error occurred, please send an email to the address below.

E-mail：mdx2-system@cmc.osaka-u.ac.jp

If you can attach the error information displayed in the email, it may help us resolve the issue more smoothly.



オブジェクトストレージ

Error: Please contact the system administrator. email: mdx2-system@cmc.osaka-u.ac.jp

Please attach the information below to your email.

Project name: admin
Error code: 409
Error API: Conflict

1 件表示

Status	Size [GB]	Access key	Secret key
ERROR	1000	Sorry, an error occurred	Sorry, an error occurred

1 件表示

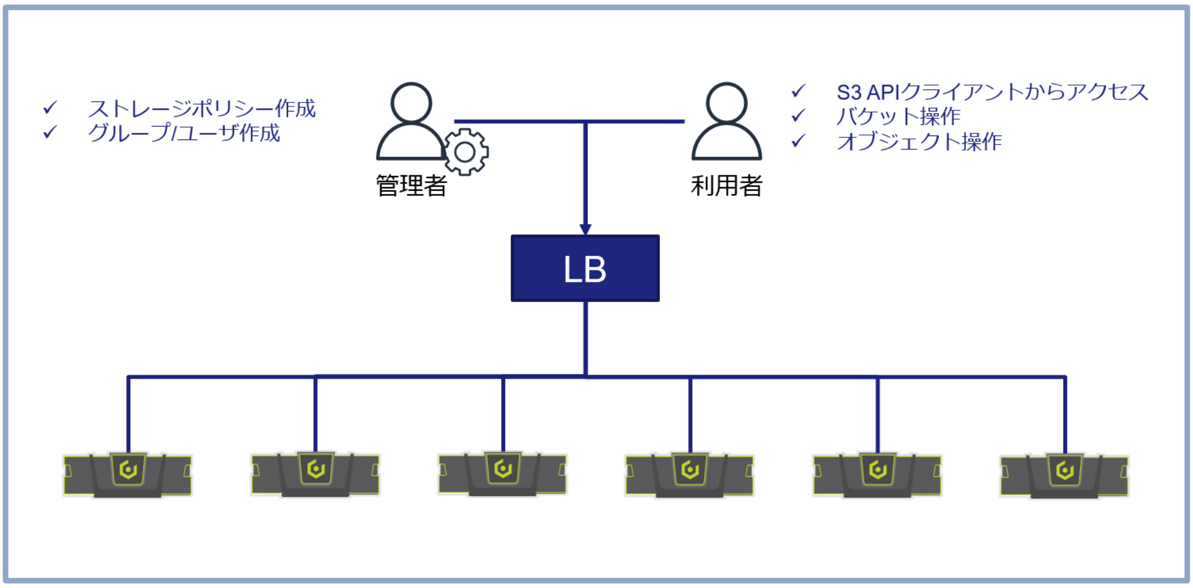
4.3.2. How to use

Unlike conventional storage (such as NAS), object storage not only has high scalability but also implements many mechanisms to safely protect and fold files (hereinafter referred to as objects). We use HyperStore (revised, HyperStore).

HyperStore can be said to be the standard for cloud storage, and is highly compatible with the Amazon S3 API, allowing objects to be manipulated through various client applications that support the Amazon S3 API.

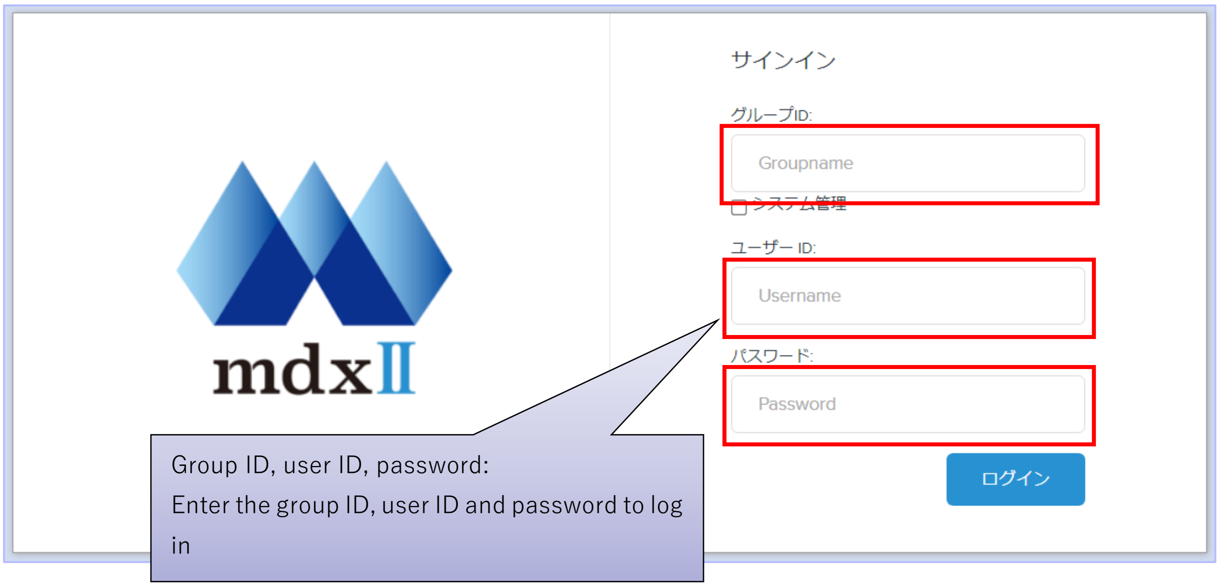
You can use the Cloudian Management Console (hereinafter referred to as CMC), which is a web GUI, to operate HyperStore.

- HyperStore access image
  HyperStore is accessed via IP network (HTTP/HTTPS).
  Users create a storage destination called a "bucket" in HyperStore and perform object operations.



4.3.2.1. CMC Operation：Login

Access CMC "https://s3object-portal.osaka.mdx.jp:443" from your browser（Chrome, FireFox recommended).

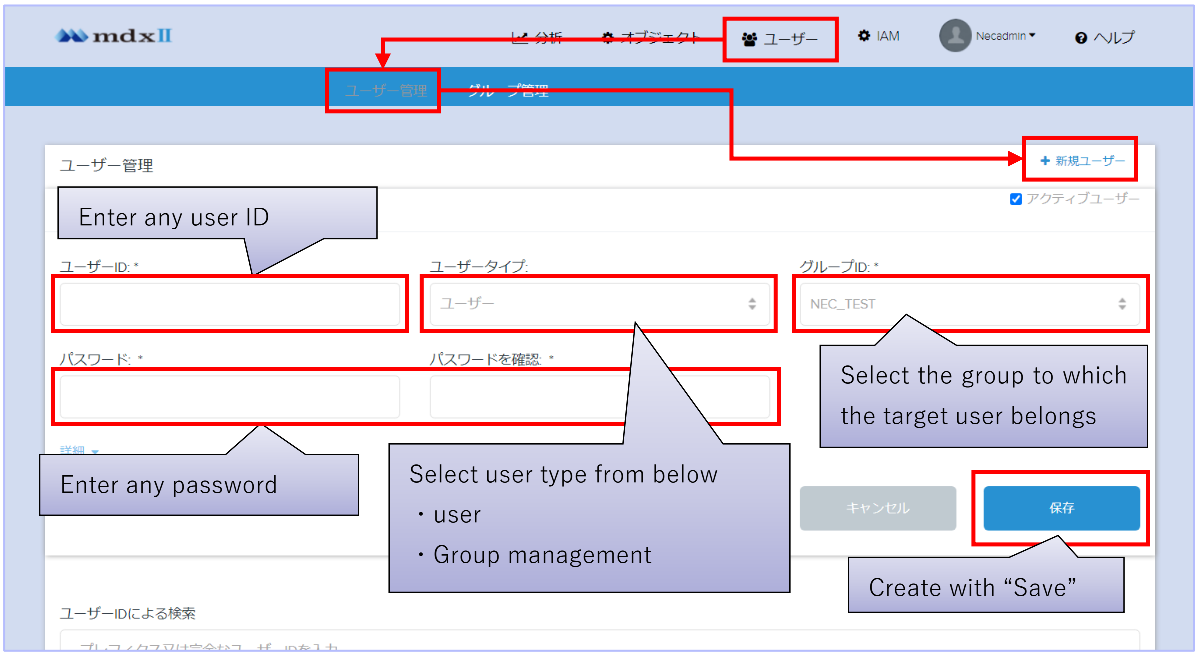


Group ID, user ID, password:
Enter the group ID, user ID and password to log in

4.3.2.2. CMC Operation：User creation

Go to the user management screen by selecting the "User" menu > "User management" tab.
Create a user to use HyperStore from "+New User".

※ User creation will be performed by the group administrator.



Enter any user ID

Select the group to which the target user belongs

Enter any password

Select user type from below
・user
・Group management

Create with “Save”

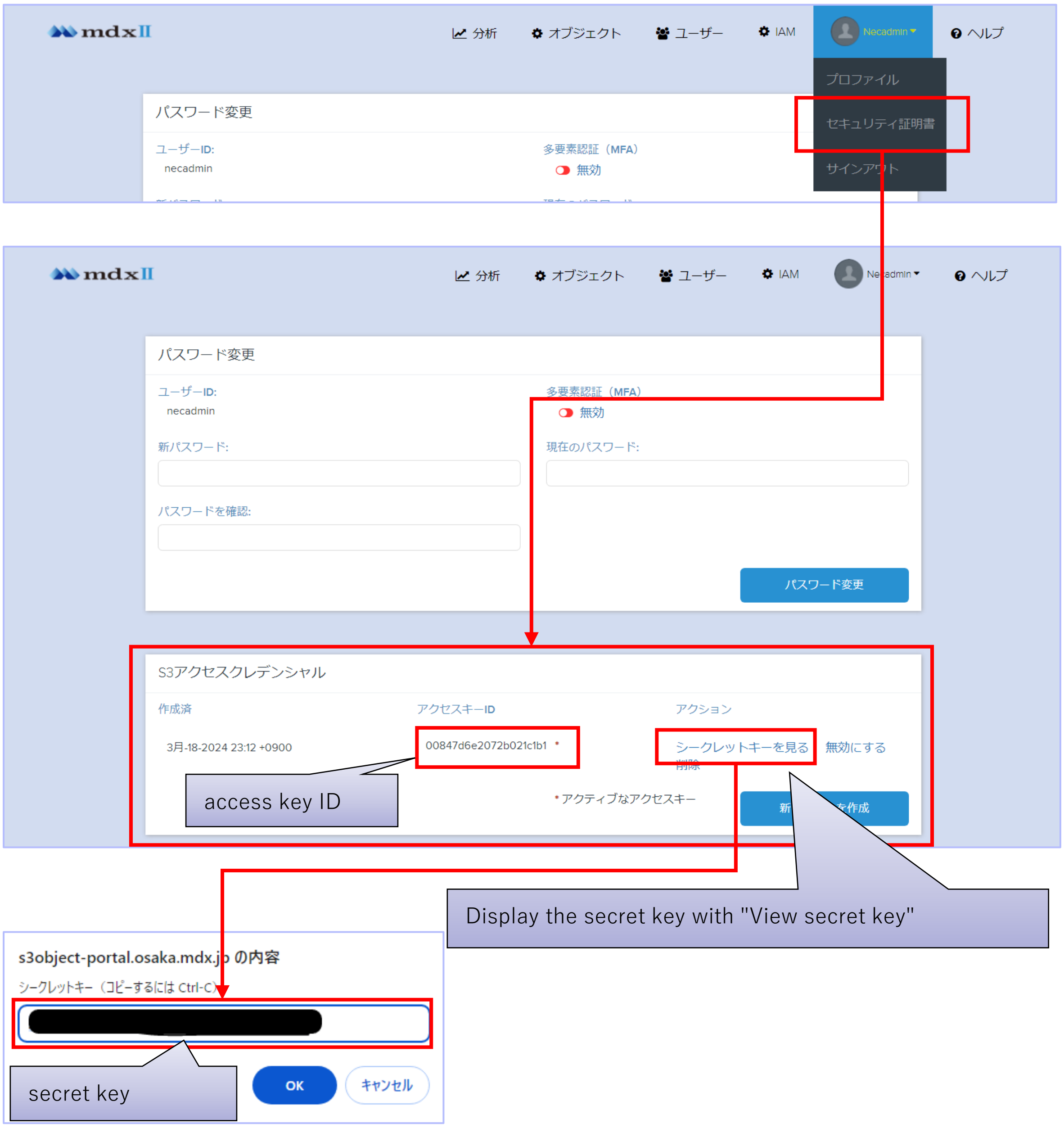
4.3.2.3. CMC Operation：Obtaining user credentials

User credentials are visible to each user.

Go to the user credentials screen by selecting "Username" > "Security Certificate" at the top right of the screen.

User credentials (access key ID, secret key) are required when accessing S3 from the client system.

※ Up to 5 user credentials can be acquired per user. (Default value)



パスワード変更

ユーザーID: necadmin

多要素認証（MFA） 無効

新パスワード:

現在のパスワード:

パスワードを確認:

S3アクセスクレデンシャル

作成済	アクセスキーID	アクション
3月-18-2024 23:12 +0900	00847d6e2072b021c1b1 *	シークレットキーを見る 無効にする 削除

* アクティブなアクセスキー

access key ID

Display the secret key with "View secret key"

s3object-portal.osaka.mdx.jp の内容

シークレットキー（コピーするには Ctrl-C）

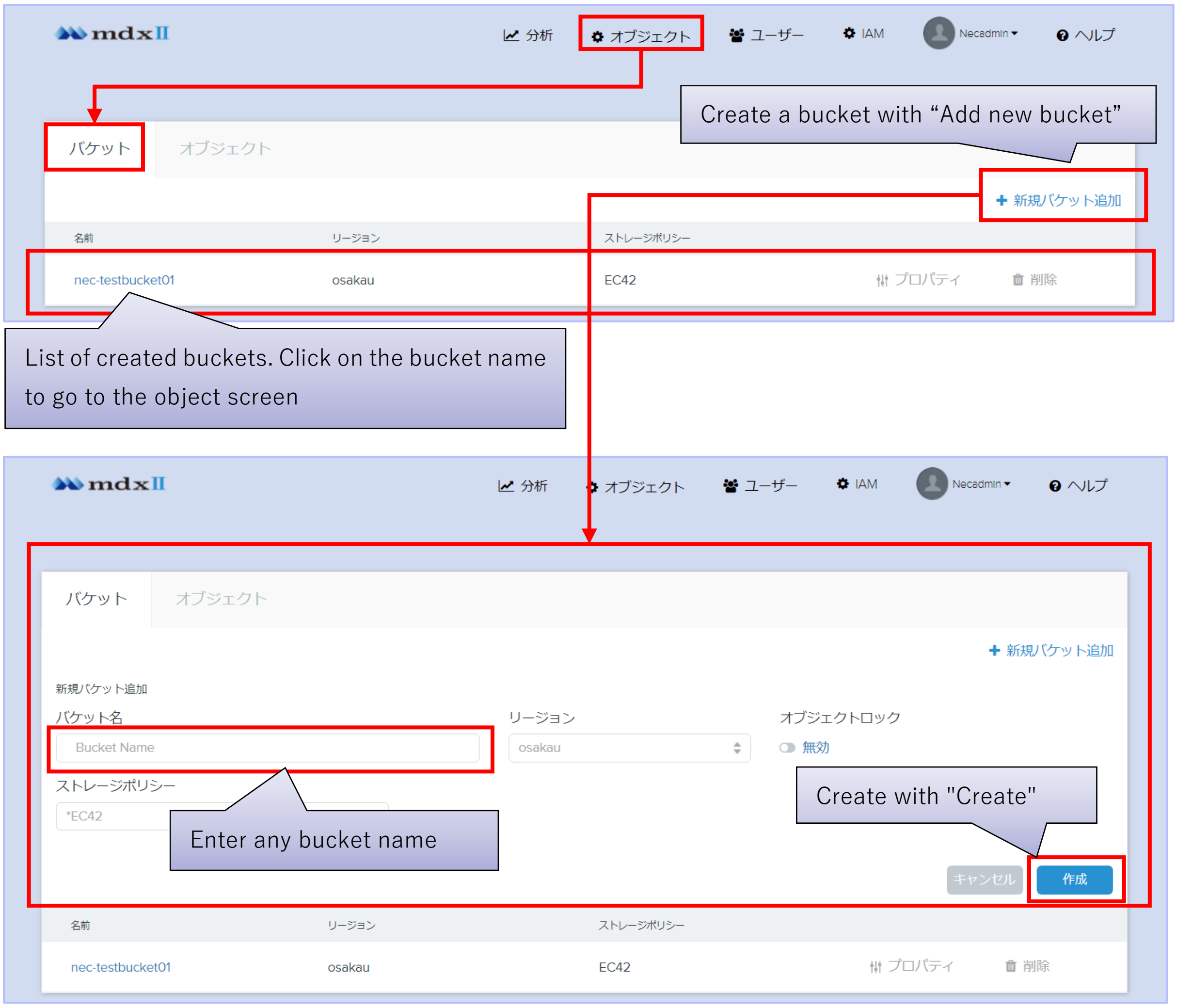
[redacted]

secret key

4.3.2.4. CMC Operation：Bucket creation

Create an area called a "bucket" to store objects.

Go to the bucket list screen from the "Object" menu > "Bucket" and press "+Add new bucket" to display the new bucket addition screen.



Create a bucket with “Add new bucket”

List of created buckets. Click on the bucket name to go to the object screen

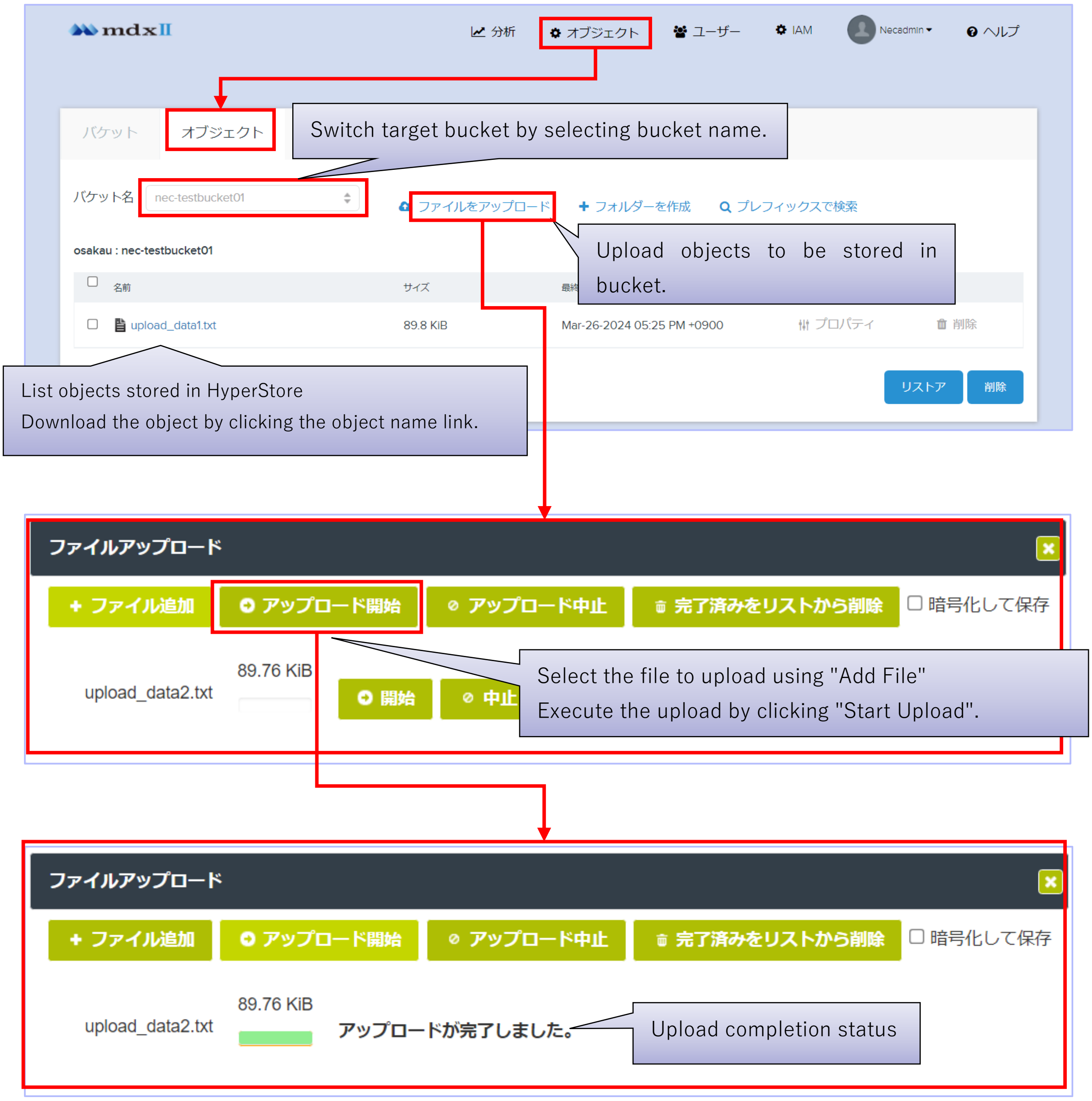
Enter any bucket name

Create with "Create"

4.3.2.5. CMC Operation：Listing/uploading objects

Displays a list of objects, uploads them to a bucket, etc.

Go to the object list screen by selecting the "Object" menu > "Object" tab.



Switch target bucket by selecting bucket name.

Upload objects to be stored in bucket.

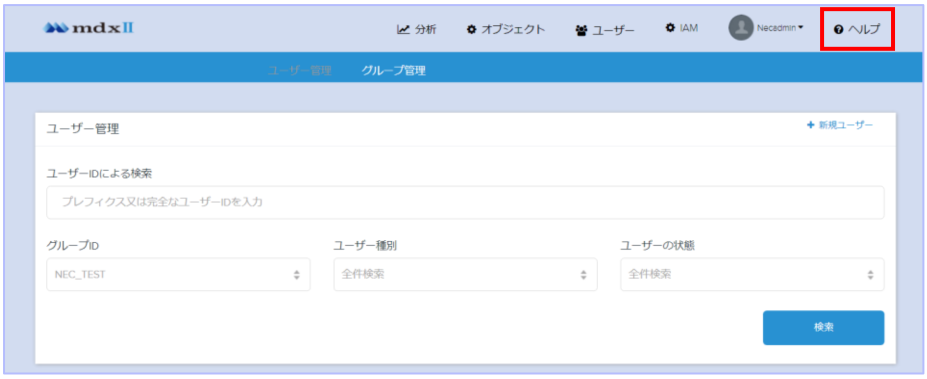
List objects stored in HyperStore
Download the object by clicking the object name link.

Select the file to upload using "Add File"
Execute the upload by clicking "Start Upload".

Upload completion status

4.3.2.6. CMC Operation：help

You can check how to operate each menu from the "Help" menu at the top right of the screen.



4.4. Project Data Portal

4.4.1. Application for use

This section describes how to apply for use of Nextcloud on the ProjectDataPortal application management screen.

You can apply for Project Data Portal only after completing the object storage settings. For details on how to apply for object storage use, please refer to chapter 4.3 mdx II Object Storage.

After logging in to OpenStaack, please proceed as follows from the tabs at the top of the page.

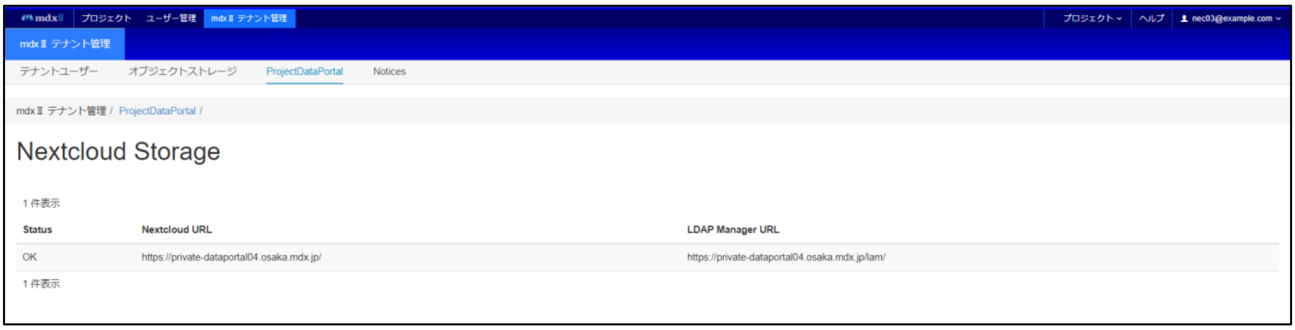
mdx II tenant management > ProjectDataPortal

You can apply to use Nextcloud on the ProjectDataPortal application management page. The number of applications that can be submitted per project is 1. Click the "Request Nextcloud Storage" button on the right side of the page. A confirmation modal will then ask, "Do you submit an application for Nextcloud storage?" If you agree, please press the "Submit" button.

Once the application is completed, the application information will be displayed in the table. After applying, "Request" will be displayed in the Status column. Please wait for Nextcloud configuration to complete. You may have to wait up to 10 minutes. Please try refreshing the page/re-logging in after 10 minutes.

When Nextcloud settings are completed, the Status column will show "OK" and connection information will be shown in the image below. Please confirm that URL information is displayed in the Nextcloud URL column and LDAP Manager URL column.

These are the URLs to Nextcloud and LDAP Account Manager respectively. To log in, please enter the values in the Administrator column and Initial password column on the object storage application management page.



Nextcloud Storage

1 件表示

Status	Nextcloud URL	LDAP Manager URL
OK	https://private-dataportal04.osaka.mdx.jp/	https://private-dataportal04.osaka.mdx.jp/lam/

1 件表示

It may take some time to complete the Nextcloud settings. If the information is not updated even after waiting 30 minutes, please send an email to the address below.

E-mail：mdx2-system@cmc.osaka-u.ac.jp

4.4.2. How to use

4.4.2.1. pre-study

To log in to the project data transfer portal, two-factor authentication using Google Authenticator etc. is required. Please prepare and install the application necessary for two-factor authentication on your own device (smartphone etc.).

The following two-factor authentication applications have been confirmed as usable:

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
macOS	Step Two	Apple App Store

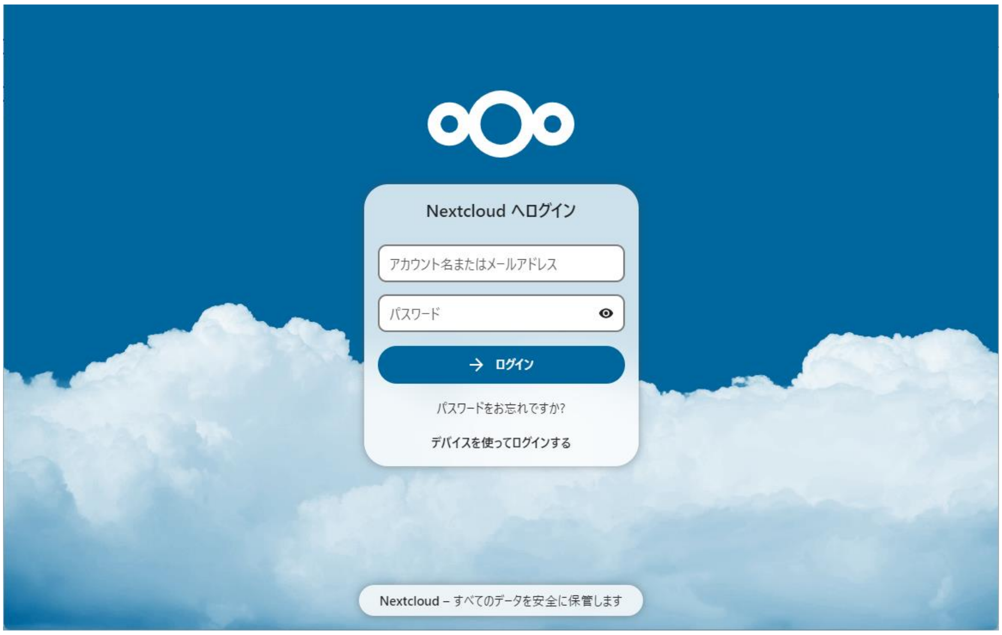
4.4.2.2. Tasks for Group Administrators

4.4.2.2.1. Setting Up Two-Factor Authentication (Nextcloud)

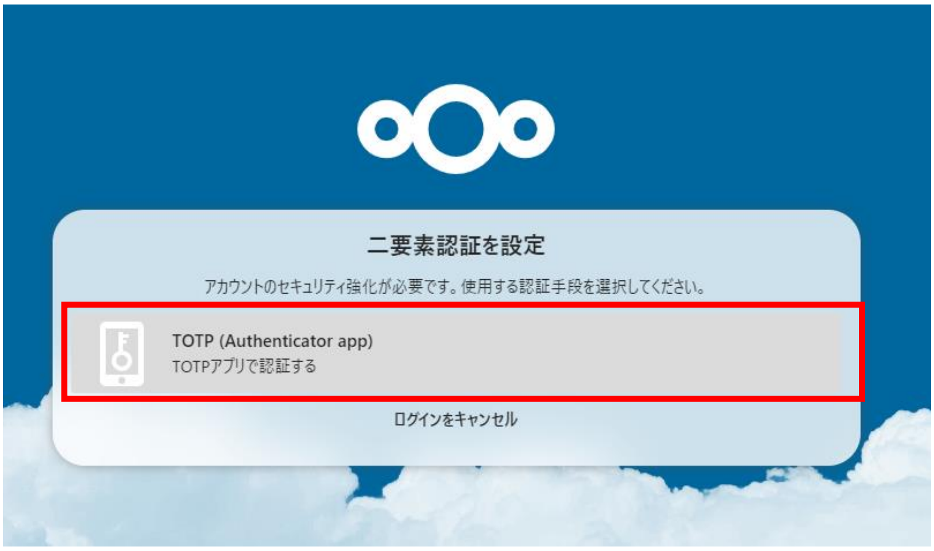
(1) Open a web browser and connect to the "Nextcloud URL" displayed on the project data transfer portal application screen.

https://[string set for each tenant].osaka.mdx.jp/

Enter the "Account Name or Email Address" and "Password" displayed under "Administrator Account" and "Initial Password" on the data aggregation object storage application screen.


Nextcloud へログイン
アカウント名またはメールアドレス
パスワード
ログイン
パスワードをお忘れですか?
デバイスを使ってログインする
Nextcloud – すべてのデータを安全に保管します

(2) Click on「TOTP (Authenticator app) TOTP アプリで認証する」.



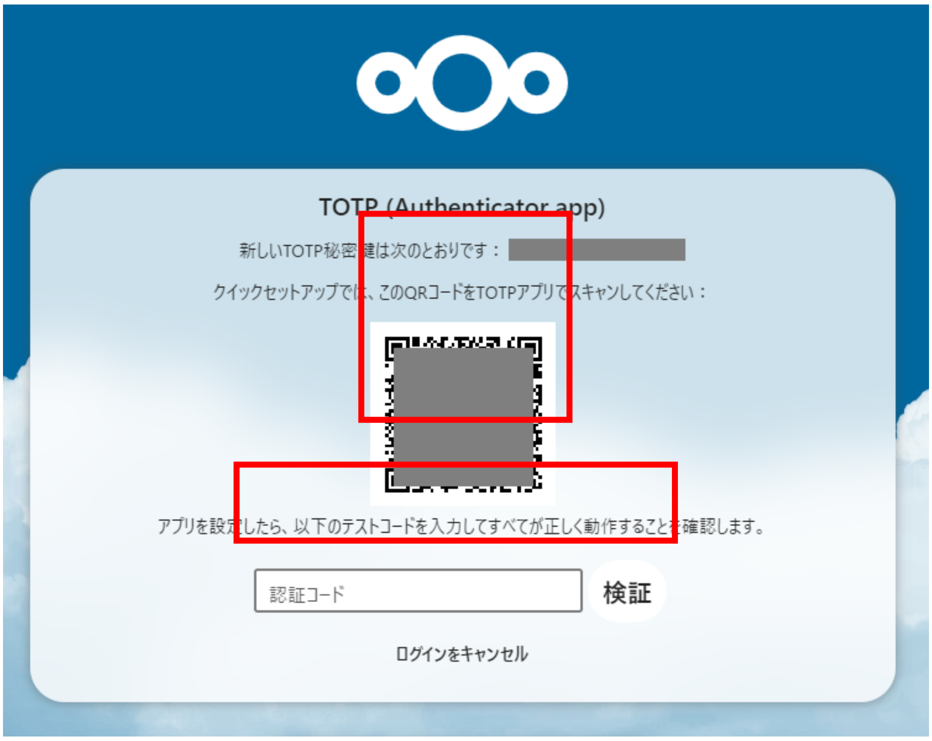
二要素認証を設定

アカウントのセキュリティ強化が必要です。使用する認証手段を選択してください。

TOTP (Authenticator app)
TOTPアプリで認証する

ログインをキャンセル

(3) A QR code will be displayed, so use the two-factor authentication app prepared in the preparations to scan it. Then enter the authentication code displayed in the app and click "Verify".



TOTP (Authenticator app)

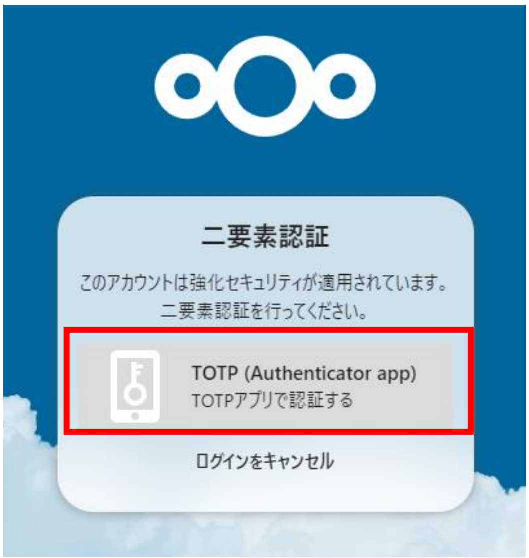
新しいTOTP秘密鍵は次のとおりです：[redacted]

クイックセットアップでは、このQRコードをTOTPアプリでスキャンしてください：

[redacted]

アプリを設定したら、以下のテストコードを入力してすべてが正しく動作することを確認します。

(4) Click 「TOTP (Authenticator app) TOTP アプリで認証する」again.



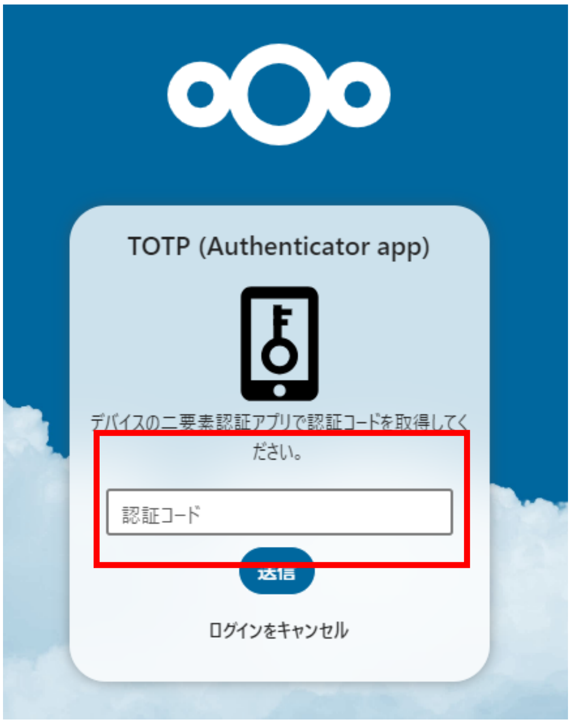
二要素認証

このアカウントは強化セキュリティが適用されています。
二要素認証を行ってください。

TOTP (Authenticator app)
TOTPアプリで認証する

ログインをキャンセル

(5) Enter the authentication code corresponding to the QR code scanned earlier and click "Submit".



TOTP (Authenticator app)

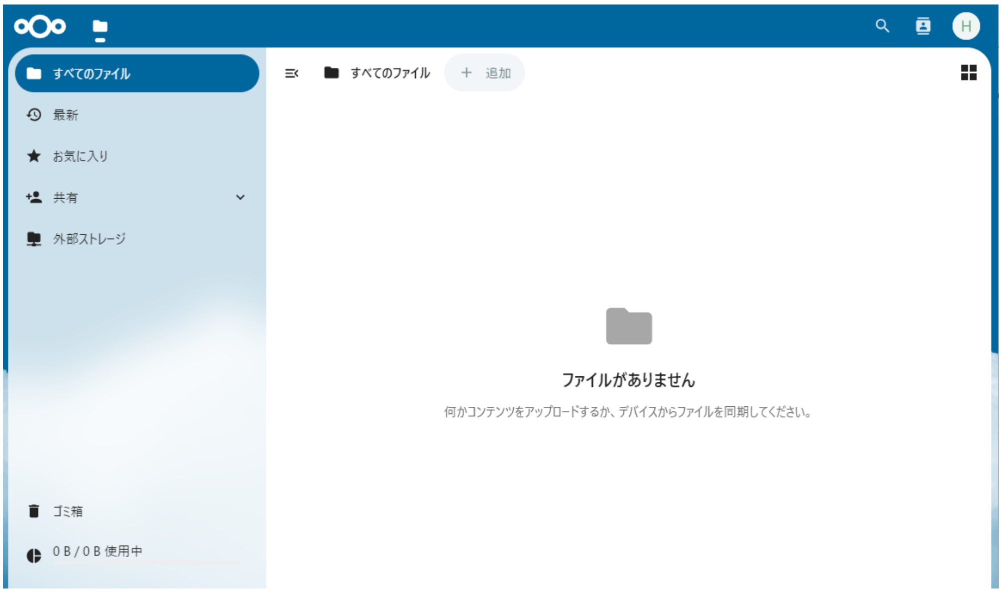
デバイスの二要素認証アプリで認証コードを取得してください。

認証コード

送信

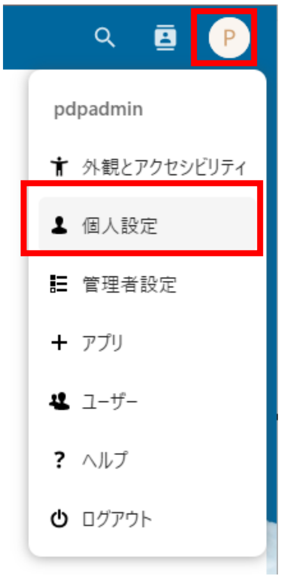
ログインをキャンセル

(6) If login is successful, the home screen will be displayed.

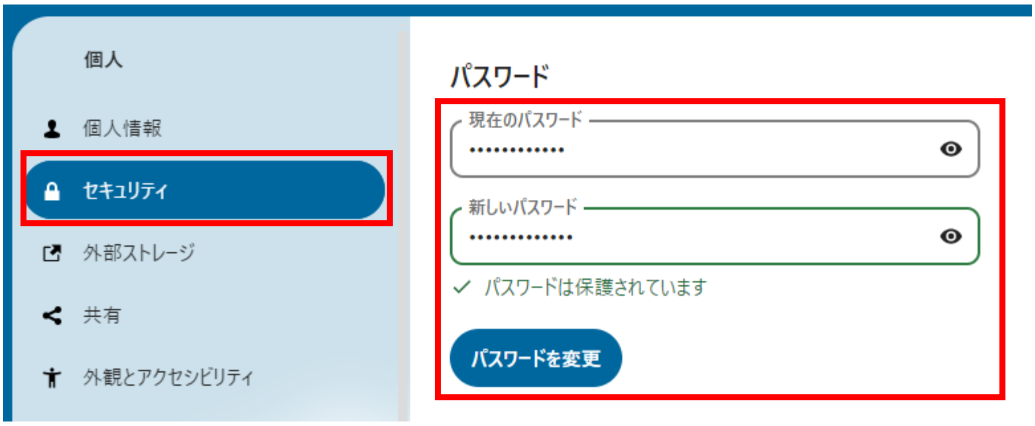


4.4.2.2.2. Change password (Nextcloud)

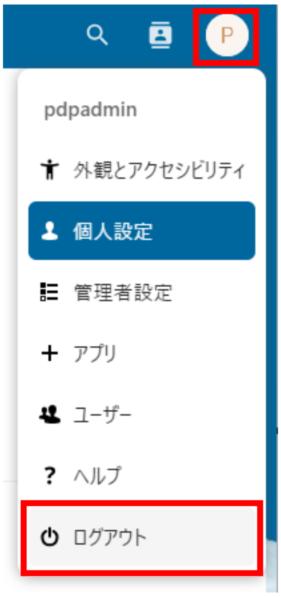
1. Log in to Nextcloud.
2. Click "Personal Settings" from the icon in the upper right corner.



3. Click "Security" from the left menu to display the password entry screen. Enter "Current Password" and "New Password" and click "Change Password".



4. After changing your password, log out. Click "Logout" from the icon in the upper right corner.

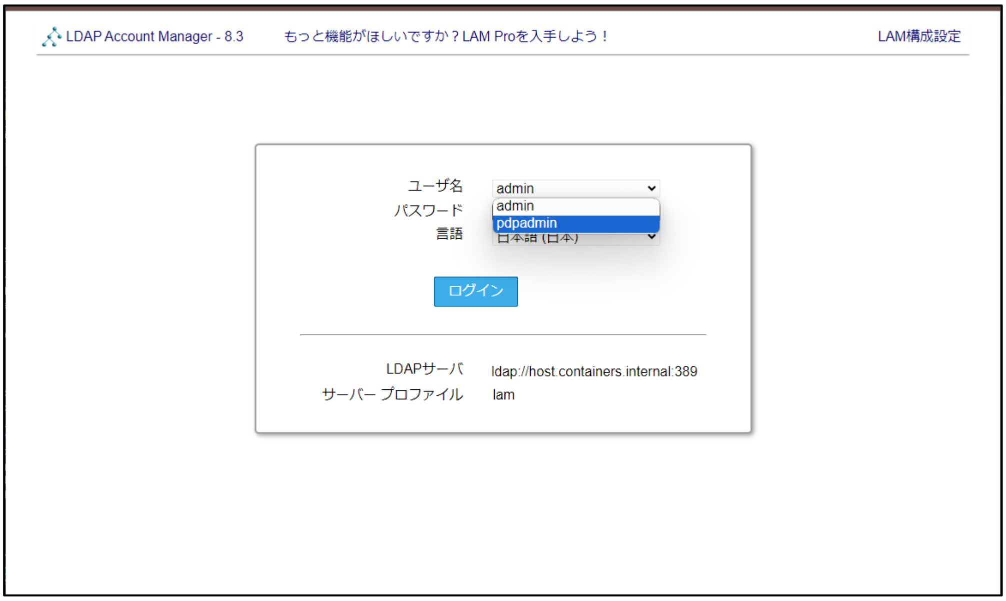


4.4.2.2.3. LDAP group administrator password change (LDAP Account Manager)

1. Open a web browser and connect to the [Admin URL" displayed on the application screen for using the project data transfer portal.

https://[Character string set for each tenant.].osaka.mdx.jp/lam/

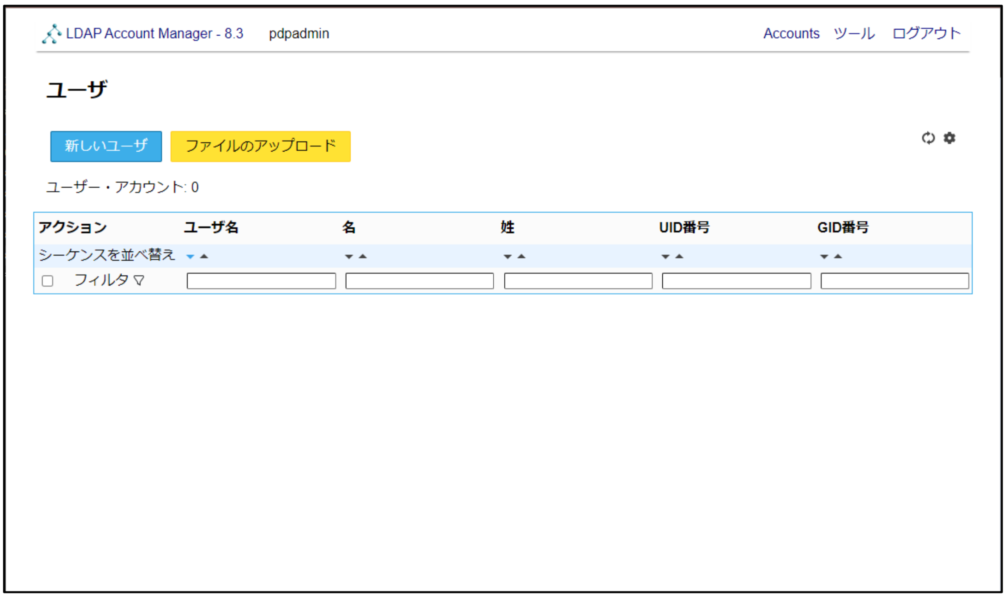
Please enter the "Username" and "Password" by referring to the "Administrator Account" and "Initial Password" displayed on the application screen for using object storage for data aggregation.


LDAP Account Manager - 8.3
もっと機能がほしいですか？LAM Proを入手しよう！
LAM構成設定
ログイン

ユーザ名 admin
admin
pdpadmin
パスワード
言語 日本語 (日本)

LDAPサーバ ldap://host.containers.internal:389
サーバー プロファイル lam

2. If the login is successful, the user addition screen will be displayed.

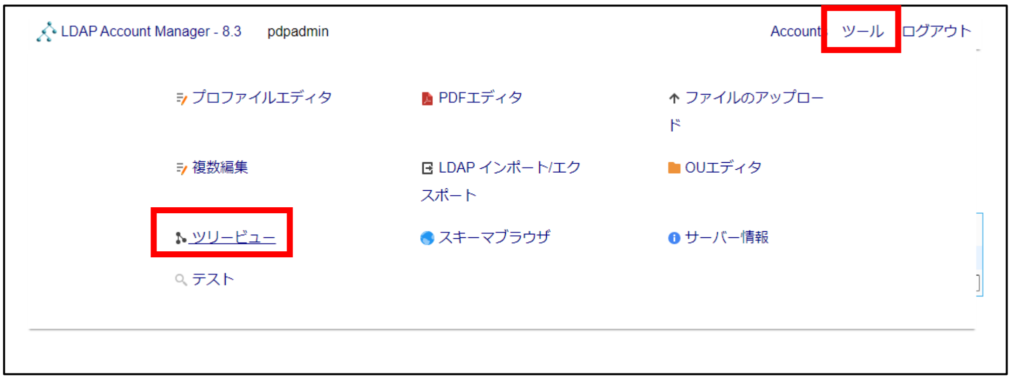


ユーザ

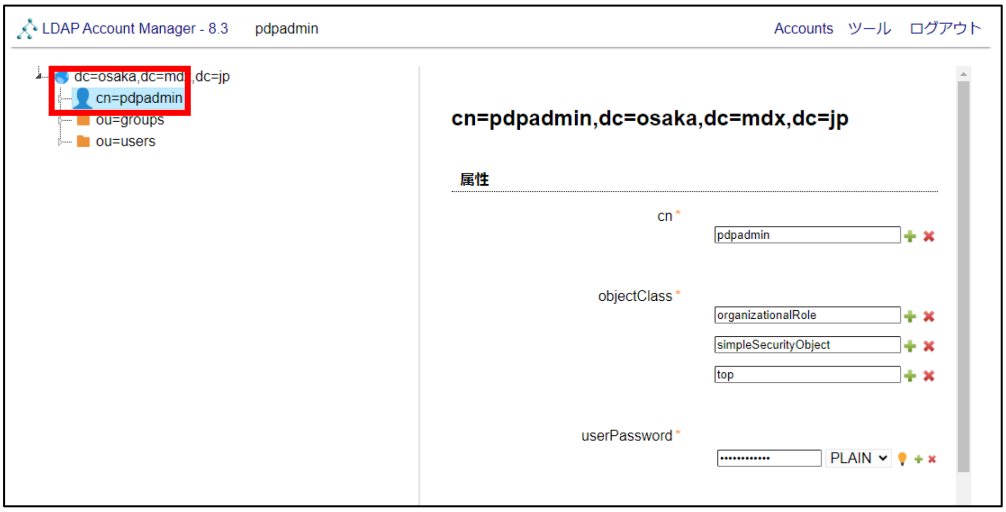
ユーザー・アカウント: 0

アクション	ユーザ名	名	姓	UID番号	GID番号
シーケンスを並べ替え	▾▴	▾▴	▾▴	▾▴	▾▴
□ フィルタ ▽					

3. From the tools in the top right, click Tree View.



4. Click「cn=[username」from the displayed tree view.



LDAP Account Manager - 8.3 pdpadmin

Accounts ツール ログアウト

dc=osaka,dc=mdx,dc=jp
cn=pdpadmin
ou=groups
ou=users

cn=pdpadmin,dc=osaka,dc=mdx,dc=jp

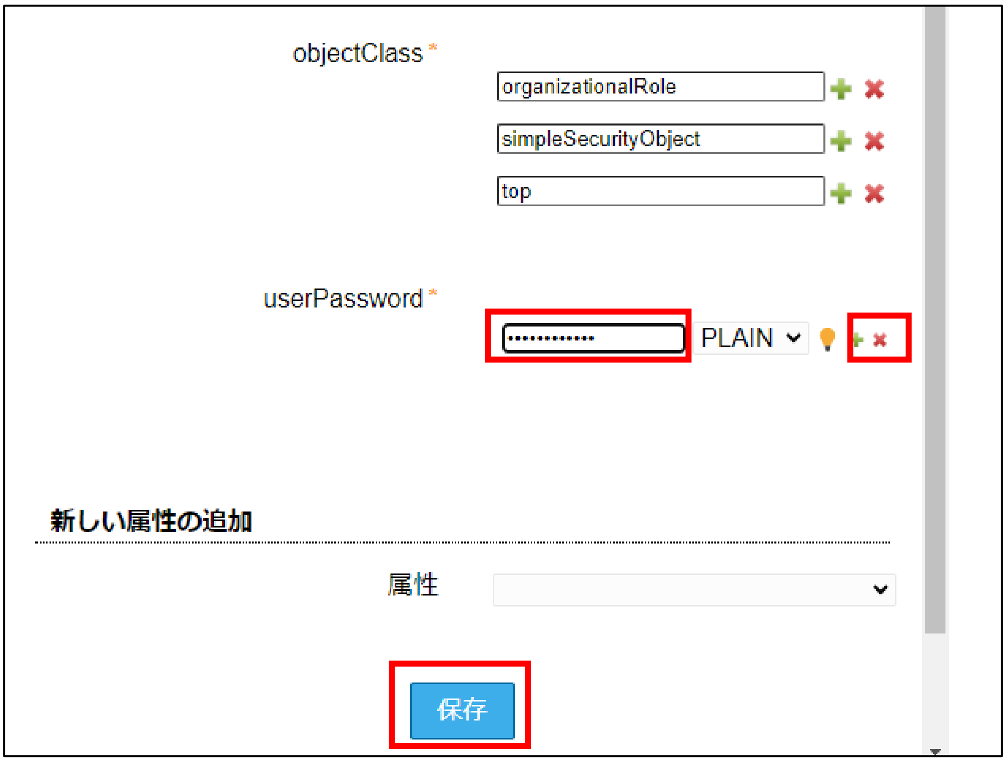
属性

cn * pdpadmin

objectClass * organizationalRole
simpleSecurityObject
top

userPassword * •••••••••••• PLAIN

5. Enter "userPassword" at the bottom on the right side.
Clear your input with the × button and set a new password.
When you have finished entering your information, click Save. (You cannot set the same password)



objectClass * organizationalRole
simpleSecurityObject
top

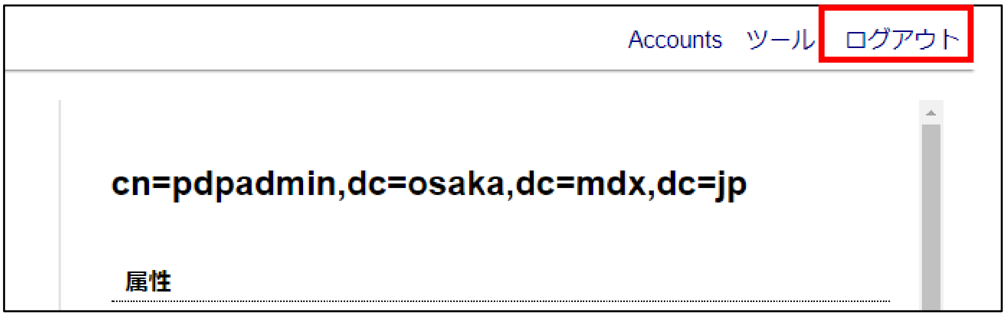
userPassword * •••••••••••• PLAIN

新しい属性の追加

属性

保存

6. No particular message will be displayed, so click "Logout" in the upper right to log out.



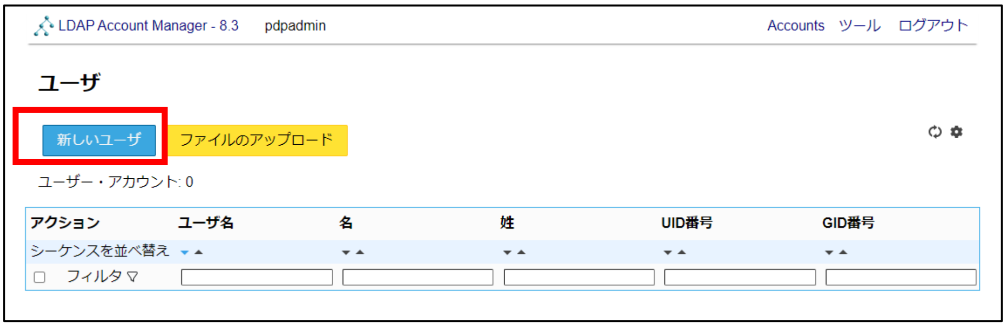
cn=pdpadmin,dc=osaka,dc=mdx,dc=jp

4.4.2.2.4. User registration (LDAP Account Manager)

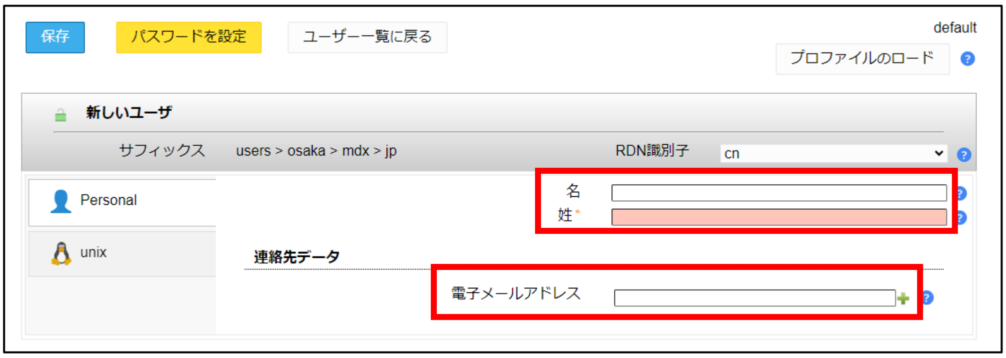
The required input items are as follows.

tab	Input items	remarks
Personal	Last name	
	First name	
	email address	
Unix	ユーザ名	This will be your Nextcloud login ID. Enter alphanumeric characters (starting with a letter).
Set password	password	Be sure to click the [OK] button.

1. Log in to LDAP Account Manager and click New User.



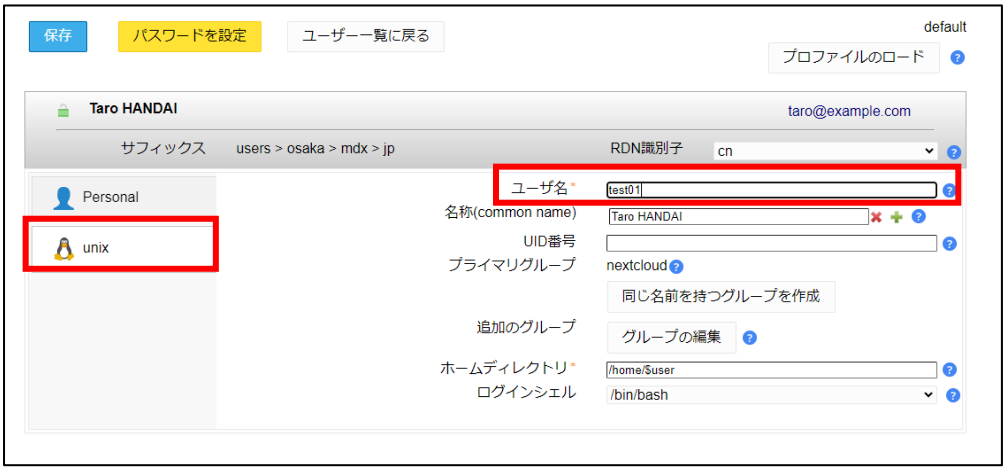
2. Enter your Personal information.



サフィックス users > osaka > mdx > jp

RDN識別子 cn

3. Click unix and enter the information.



Taro HANDAI taro@example.com

サフィックス users > osaka > mdx > jp RDN識別子 cn

ユーザ名* test01

名称(common name) Taro HANDAI

UID番号

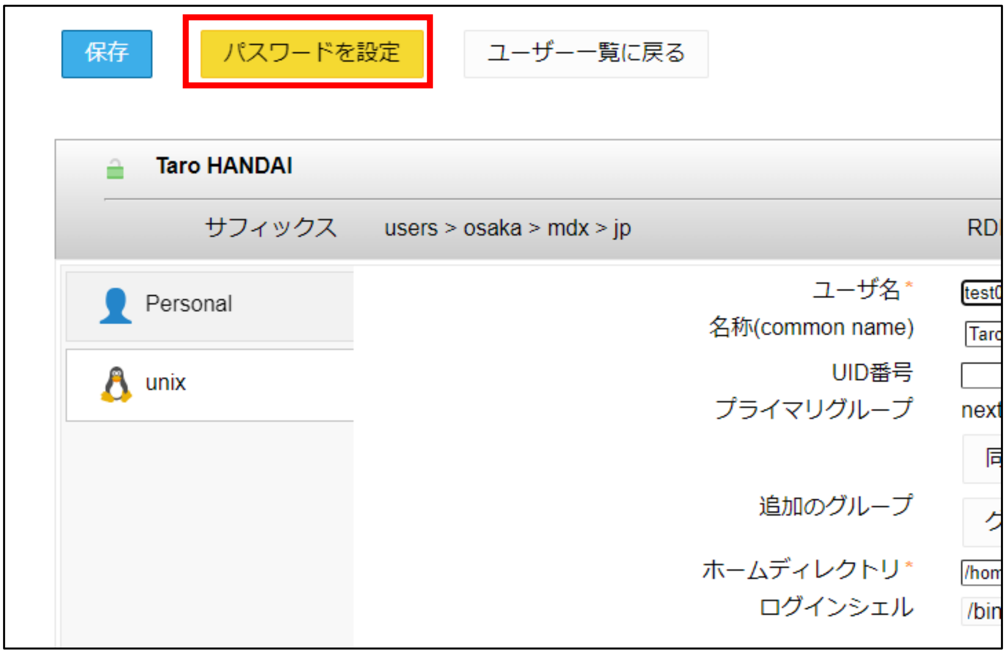
プライマリグループ nextcloud

追加のグループ

ホームディレクトリ* /home/$user

ログインシェル /bin/bash

4. Click Set Password, enter your password, and click OK.



Taro HANDAI

サフィックス users > osaka > mdx > jp RD

ユーザ名* test0

名称(common name) Tarc

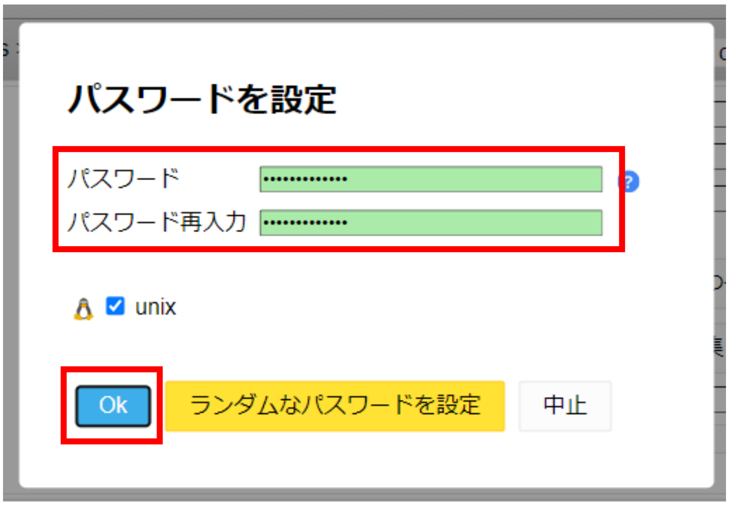
UID番号

プライマリグループ next

追加のグループ

ホームディレクトリ* /hom

ログインシェル /bin



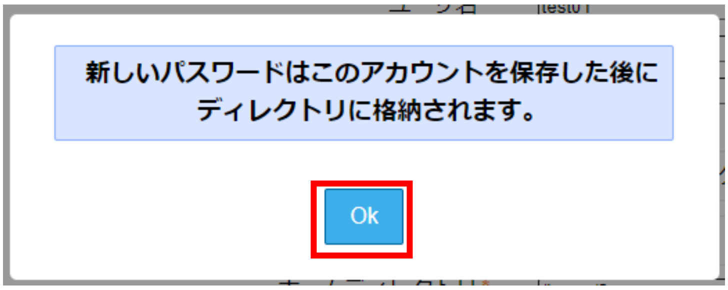
パスワードを設定

パスワード ••••••••••••

パスワード再入力 ••••••••••••

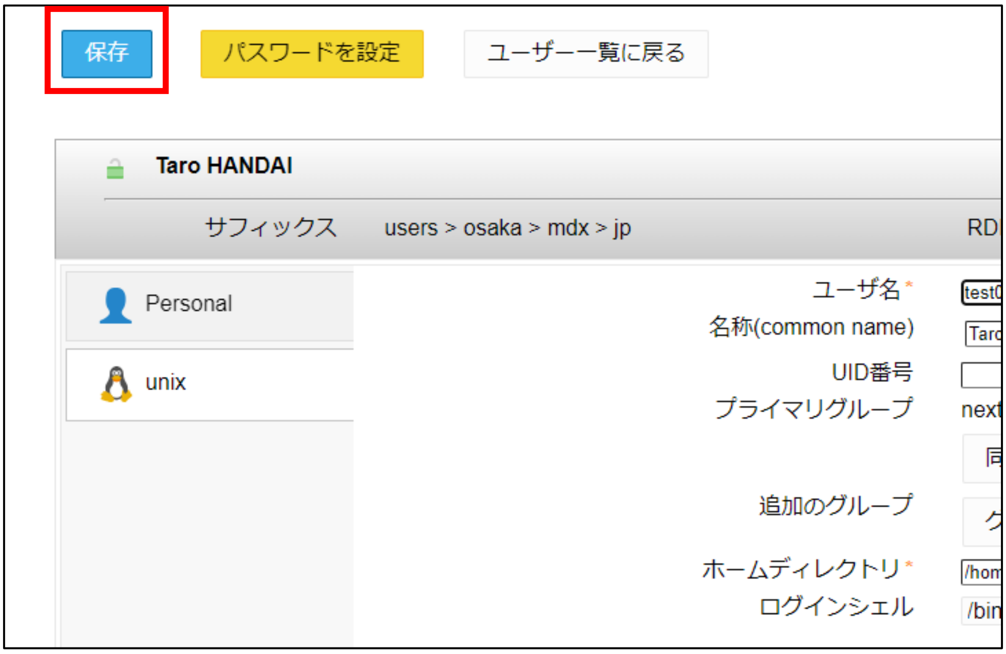
☑ unix

5. In the confirmation dialog, click the OK button.



新しいパスワードはこのアカウントを保存した後に
ディレクトリに格納されます。

6. Click Save.



Taro HANDAI

サフィックス users > osaka > mdx > jp

RD

ユーザ名* test0

名称(common name) Taro

UID番号

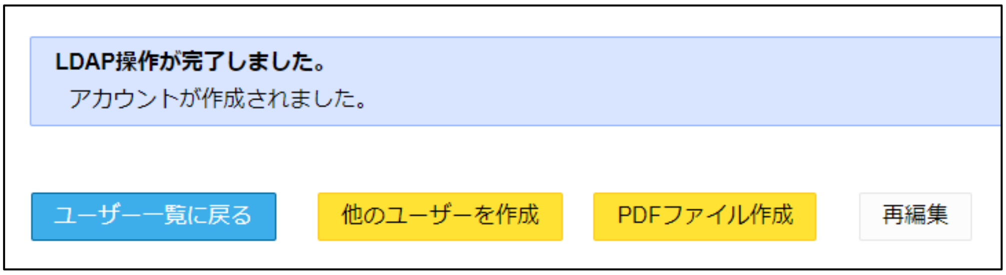
プライマリグループ next

追加のグループ

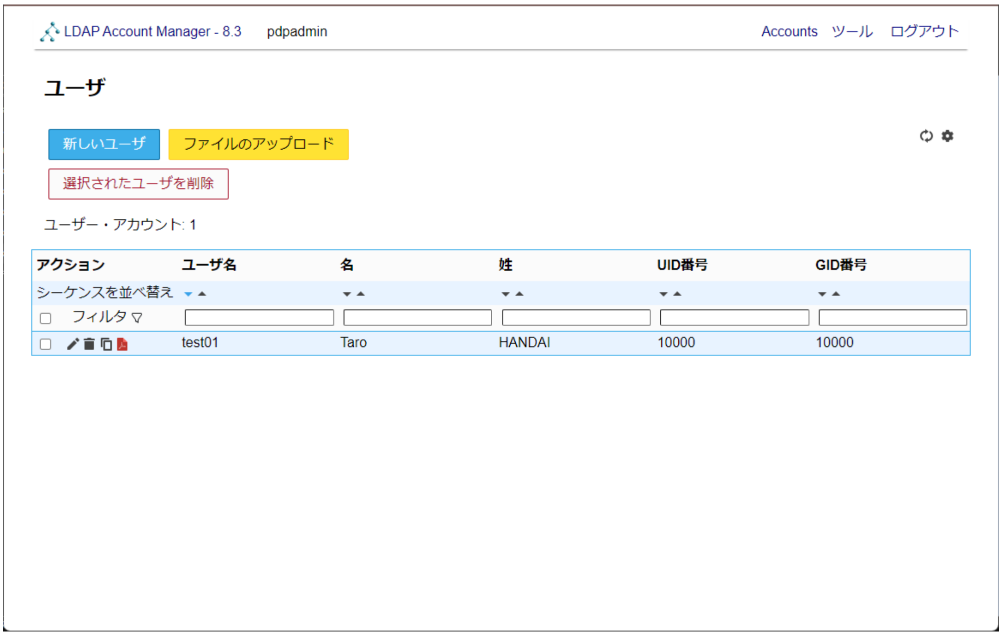
ホームディレクトリ* /hom

ログインシェル /bin

7. Confirm that "Account has been created." is displayed and the created user is displayed in the user list.



LDAP操作が完了しました。
アカウントが作成されました。



ユーザー・アカウント: 1

アクション	ユーザ名	名	姓	UID番号	GID番号
シーケンスを並べ替え	▼▲	▼▲	▼▲	▼▲	▼▲
□ フィルタ ▽					
□	test01	Taro	HANDAI	10000	10000

This completes user registration. Please notify the user of the Nextcloud URL and registered username and password.

That's all for group administrators.

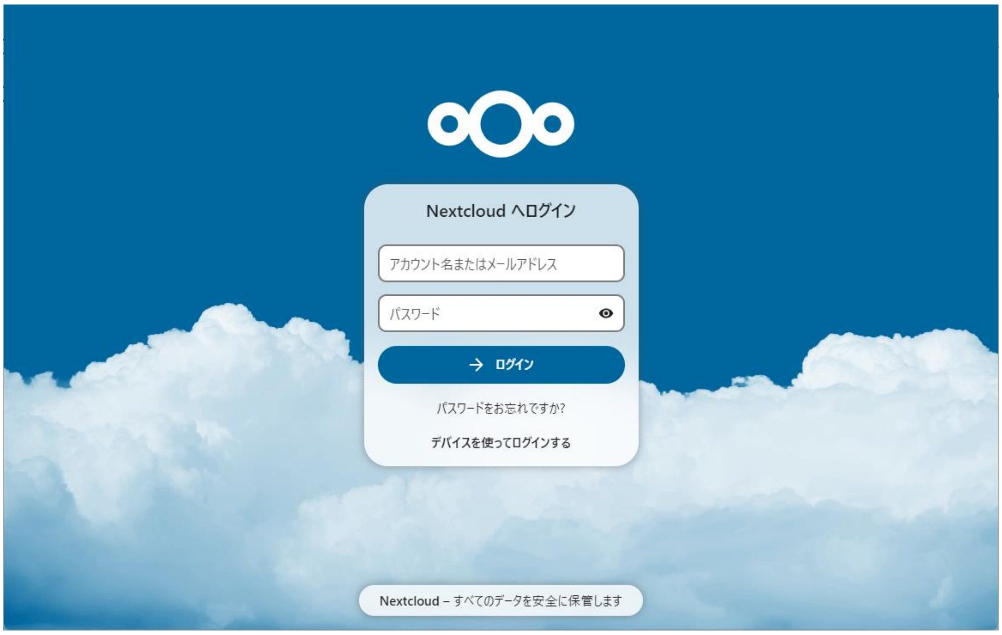
4.4.2.3. User work

4.4.2.3.1. Setting up two-step authentication (Nextcloud)

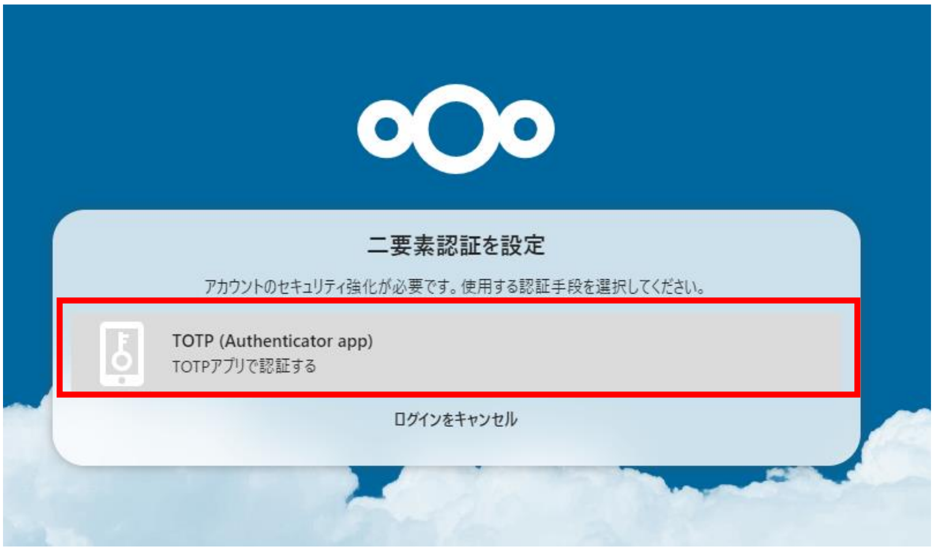
1. Open a web browser and connect to the Nextcloud URL notified by the group administrator.

https://[Character string set for each tenant.].osaka.mdx.jp/

For "Account Name or Email Address" and "Password", please enter the "Username" and "Password" notified by the group administrator.

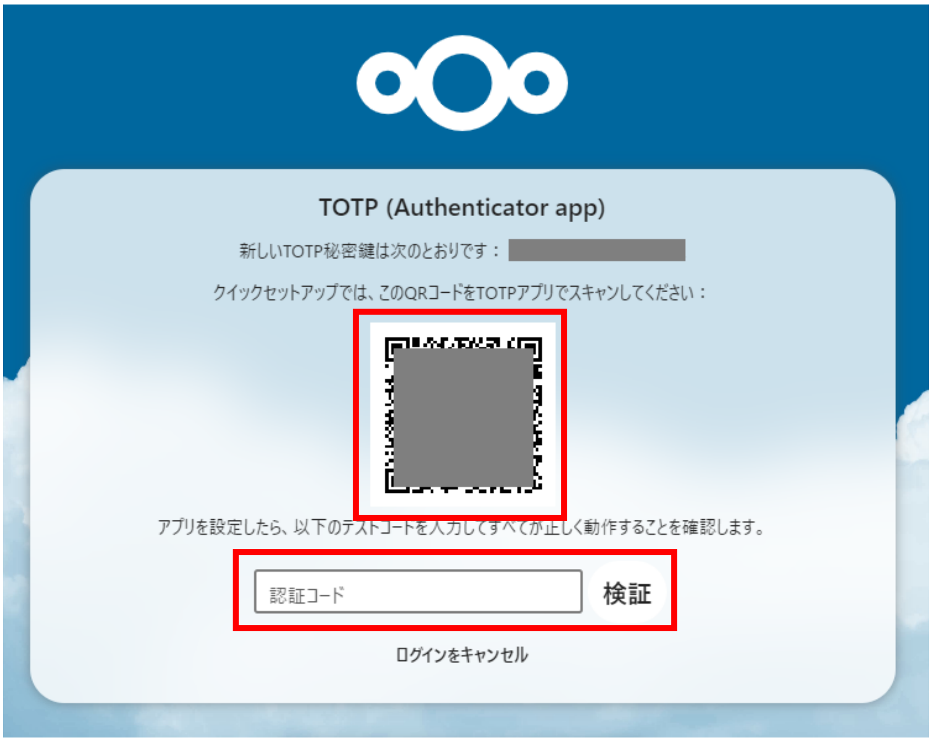

Nextcloud へログイン
アカウント名またはメールアドレス
パスワード
→ ログイン
パスワードをお忘れですか?
デバイスを使ってログインする
Nextcloud – すべてのデータを安全に保管します

2. Click "TOTP (Authenticator app)".


二要素認証を設定

アカウントのセキュリティ強化が必要です。使用する認証手段を選択してください。

3. A QR code will be displayed, so scan it using the two-factor authentication app you prepared in advance. Then enter the verification code displayed in the app and click "Verify".



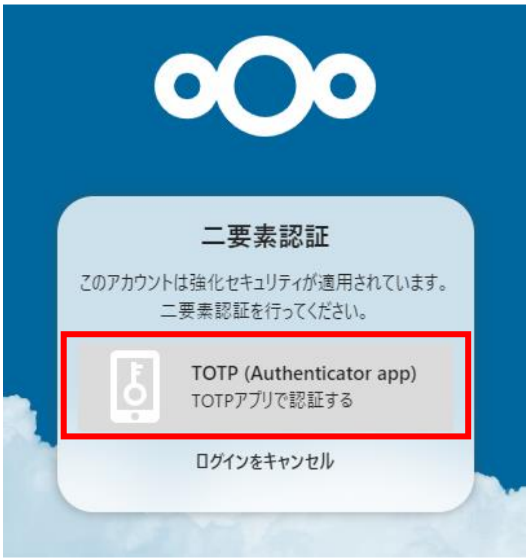
TOTP (Authenticator app)

新しいTOTP秘密鍵は次のとおりです： [redacted]

クイックセットアップでは、このQRコードをTOTPアプリでスキャンしてください：

アプリを設定したら、以下のテストコードを入力してすべてが正しく動作することを確認します。

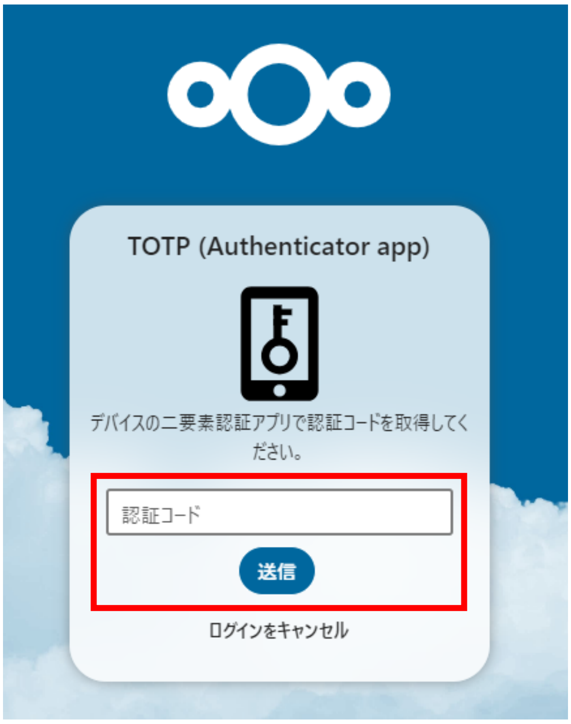
4. Click "TOTP (Authenticator app)" again.



二要素認証

このアカウントは強化セキュリティが適用されています。
二要素認証を行ってください。

5. Enter the authentication code that corresponds to the QR code you scanned earlier and click "Send".



TOTP (Authenticator app)

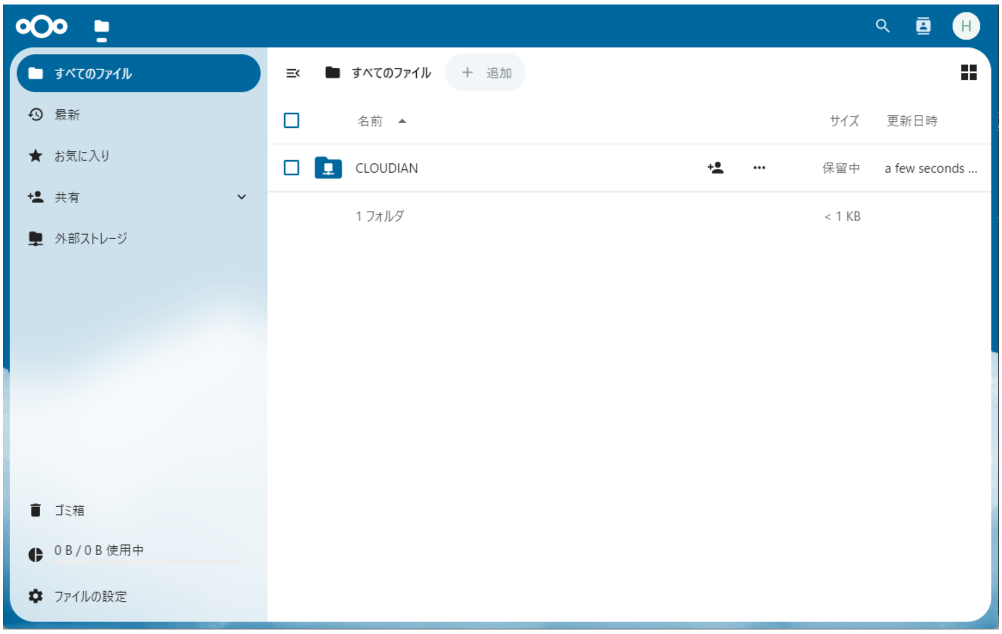
デバイスの二要素認証アプリで認証コードを取得してください。

認証コード

送信

ログインをキャンセル

6. After successful login, the home screen will be displayed. If a user area has already been created in the object storage area, it will be mounted and displayed in the "CLOUDIAN" directory as shown below.



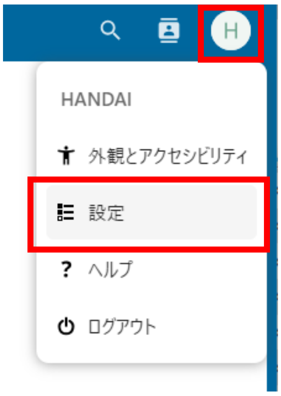
すべてのファイル
最新
お気に入り
共有
外部ストレージ
ゴミ箱
0 B / 0 B 使用中
ファイルの設定

すべてのファイル ＋ 追加

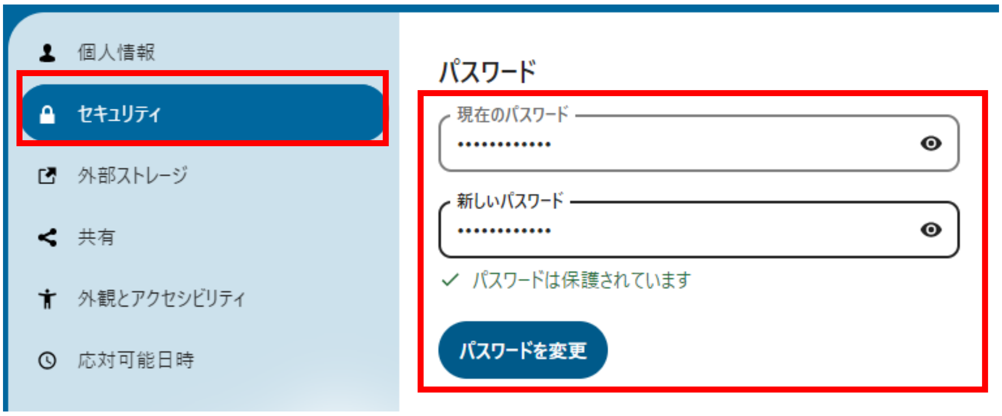
名前	サイズ	更新日時
CLOUDIAN	保留中	a few seconds ...
1 フォルダ	< 1 KB	

4.4.2.3.2. Change password (Nextcloud)

1. Log in to Nextcloud.
2. Click "Settings" from the icon in the upper right corner.



3. Click "Security" from the left menu to display the password entry screen. Enter "Current Password" and "New Password" and click "Change Password".



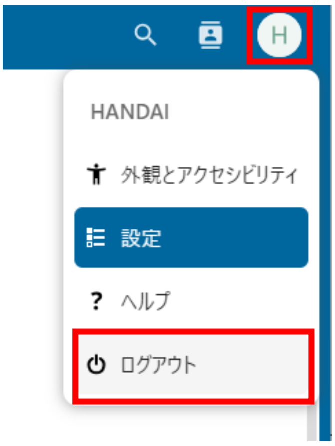
パスワード

現在のパスワード: ••••••••••••

新しいパスワード: ••••••••••••

✓ パスワードは保護されています

4. After changing your password, log out. Click "Logout" from the icon in the upper right corner.



4.4.2.3.3. Troubleshooting method

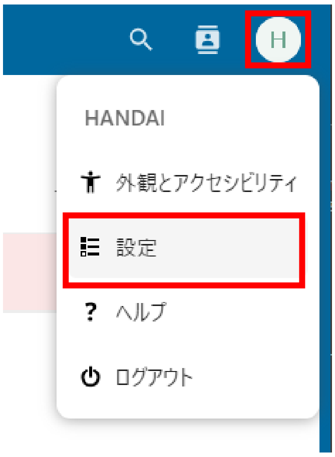
The user-only area of the object storage area turns red and cannot be used.

If the CLOUDIAN folder is displayed in red as shown below, the object storage area cannot be used.

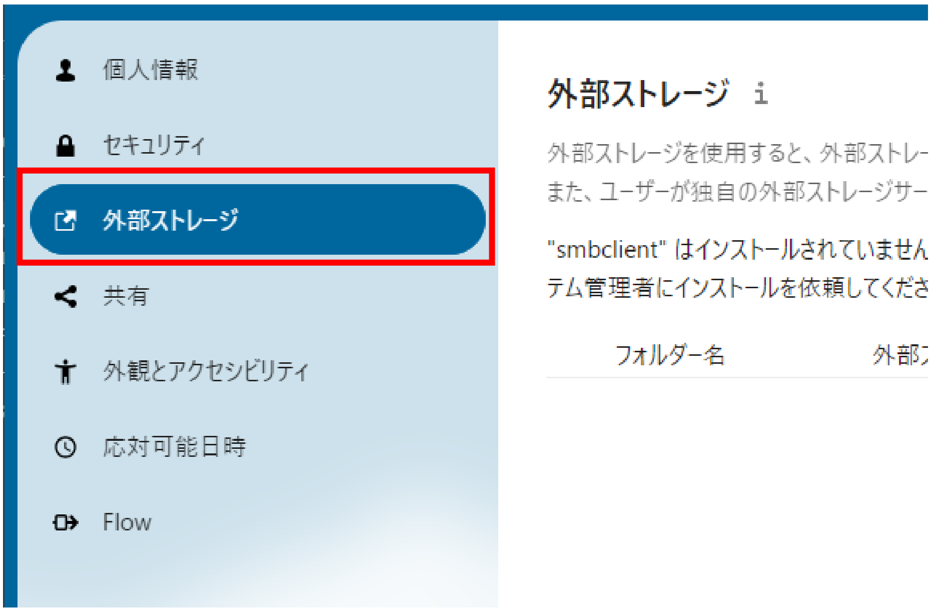
In this case, please perform the remount procedure once.

Remount procedure

1. Click "Settings" from the icon in the upper right corner.



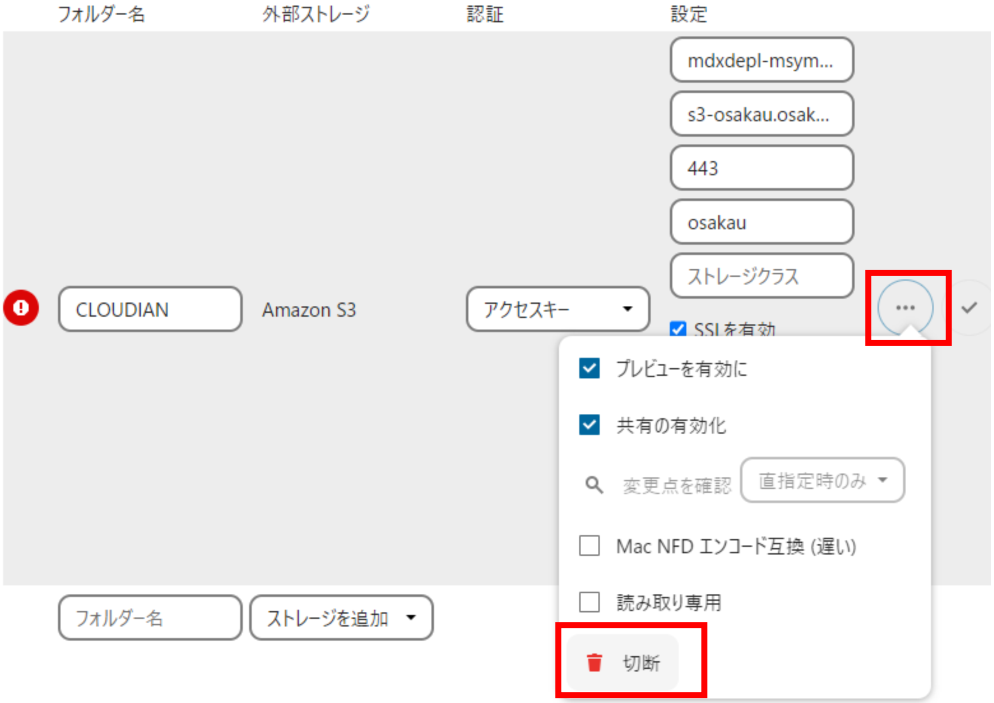
2. Click "External Storage" from the left menu.



外部ストレージを使用すると、外部ストレー
また、ユーザーが独自の外部ストレージサー

"smbclient" はインストールされていません
テム管理者にインストールを依頼してくださ

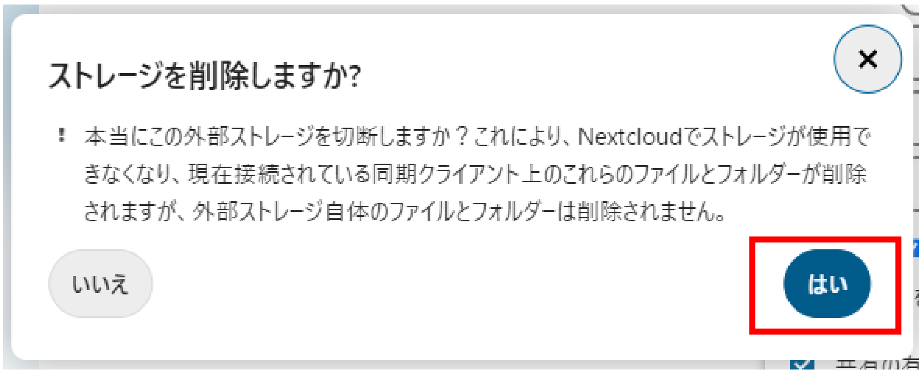
3. Click the “…” icon and click “Disconnect” from the menu that appears.



フォルダー名	外部ストレージ	認証	設定
CLOUDIAN	Amazon S3	アクセスキー	mdxdepl-msym... s3-osakau.osak... 443 osakau ストレージクラス ☑ SSLを有効

☑ プレビューを有効に
☑ 共有の有効化
変更点を確認 直指定時のみ
☐ Mac NFD エンコード互換 (遅い)
☐ 読み取り専用
切断

4. A confirmation message will appear, click Yes.

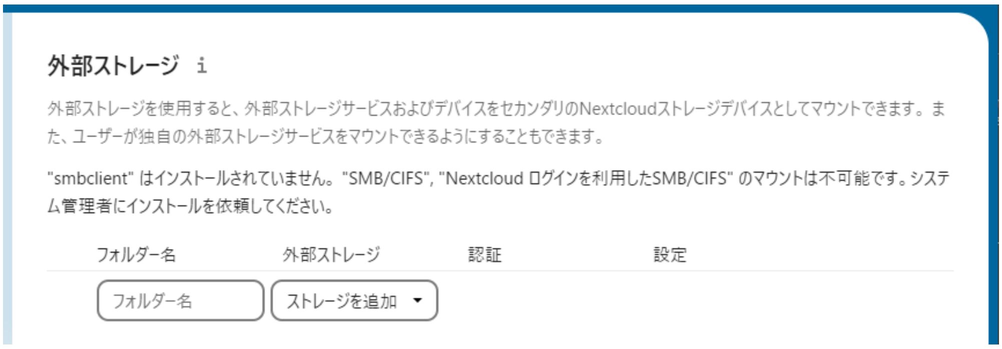


ストレージを削除しますか?

! 本当にこの外部ストレージを切断しますか？これにより、Nextcloudでストレージが使用できなくなり、現在接続されている同期クライアント上のこれらのファイルとフォルダーが削除されますが、外部ストレージ自体のファイルとフォルダーは削除されません。

5. External storage information will be cleared.

After performing this procedure, wait up to 10 minutes for the object storage area to be mounted again.



外部ストレージ i

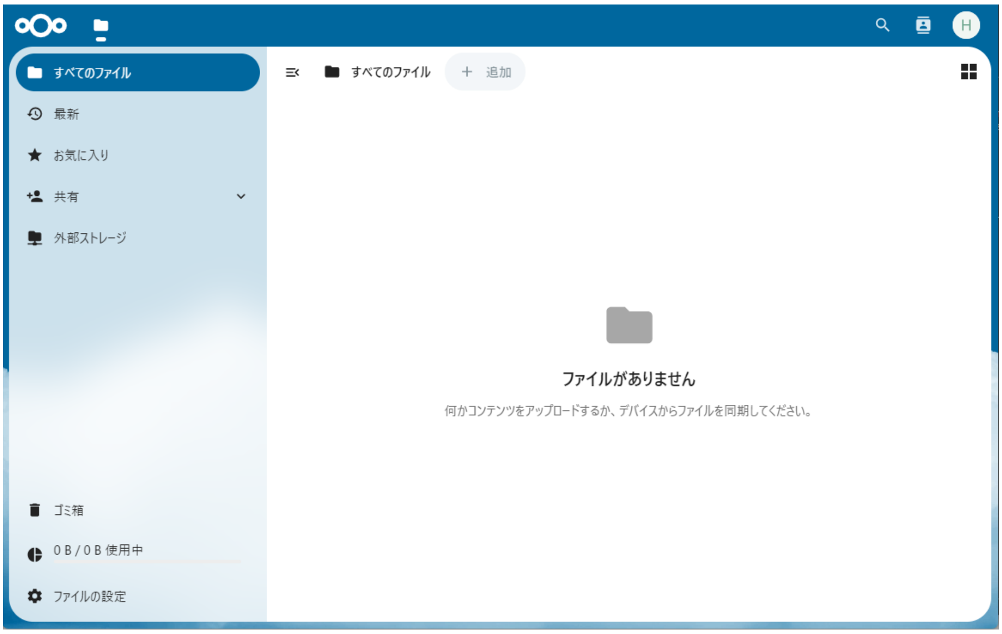
外部ストレージを使用すると、外部ストレージサービスおよびデバイスをセカンダリのNextcloudストレージデバイスとしてマウントできます。また、ユーザーが独自の外部ストレージサービスをマウントできるようにすることもできます。

"smbclient" はインストールされていません。"SMB/CIFS", "Nextcloud ログインを利用したSMB/CIFS" のマウントは不可能です。システム管理者にインストールを依頼してください。

フォルダー名	外部ストレージ	認証	設定
フォルダー名	ストレージを追加		

User-only area folder not created

After the group administrator registers the user (4.4.2.2.4), it will take up to 20 minutes to create the user-only area of the object storage area.



ファイルがありません

何かコンテンツをアップロードするか、デバイスからファイルを同期してください。

4.5. myDataPortal

4.5.1. Application for use

Using Nextcloud's external storage connection plugin, you can connect to Luster file systems and object storage that support S3 connectivity. Please use it to transfer data between external storages. myDataPortal is not intended to store large amounts of data. Please use it only for data transfer purposes.

If you wish to use this service, please send an email to the system administrator with the following information.

E-mail ：mdx2-system@cmc.osaka-u.ac.jp
Subject ：myDataPortal new application

```
Dear System Administrators

I'll apply to use myDataPortal.

full name:
Project name:
User name:
E-mai:
```

Project name: Please enter the project name applied on the project application form.
Username: Username registered on Nextcloud. Please write in half-width alphanumeric characters.
E-mail: Email address registered on Nextcloud.

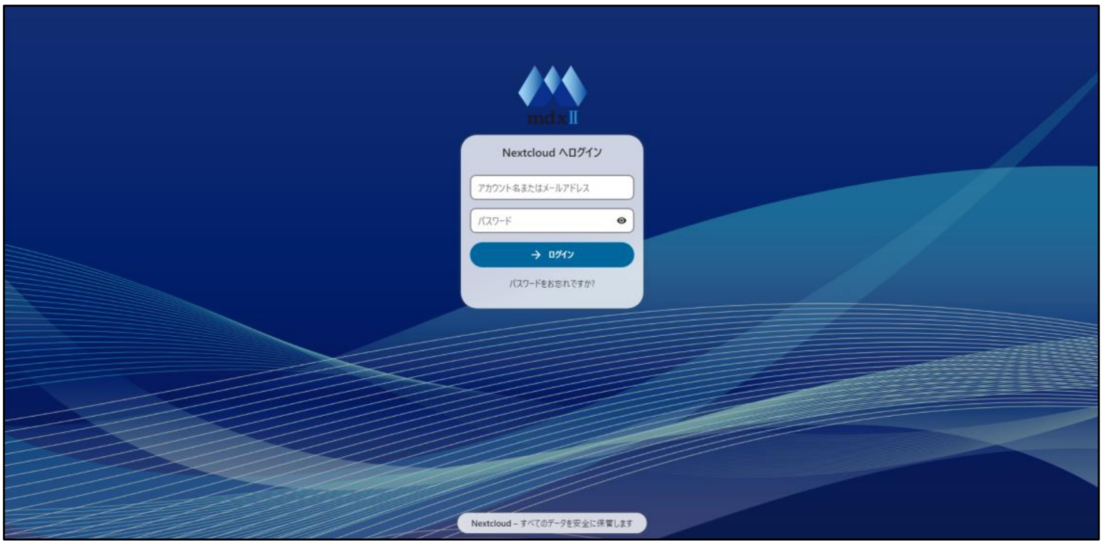
4.5.2. Login

Two-factor authentication is required to log in to Nextcloud: password authentication and OTP (one-time password) authentication. To enable OTP registration, please prepare a mobile app such as Google Authenticator or a browser OTP extension in advance.

After receiving the user registration completion notification email from the system administrator, you will be able to log in to Nextcloud. The email contains the following information:

User name
Initial password
E-mail
Group name

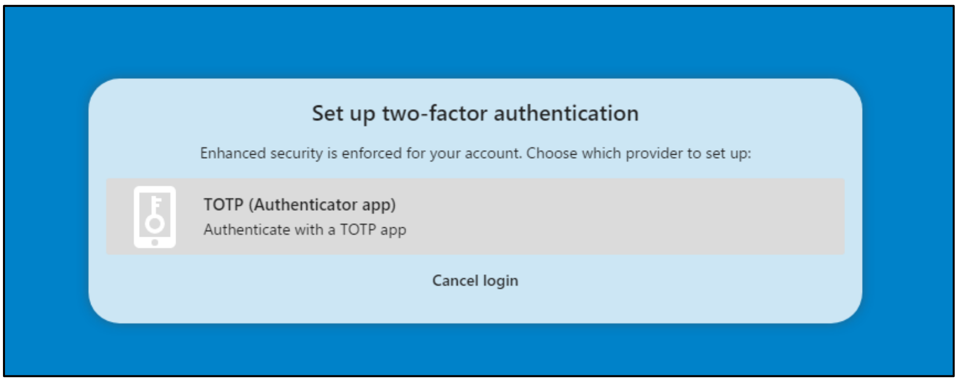
Access the URL below.
URL：https://dataportal.osaka.mdx.jp/



mdxII
Nextcloud へログイン
アカウント名またはメールアドレス
パスワード
ログイン
パスワードをお忘れですか?
Nextcloud – すべてのデータを安全に保管します

In the input field on the login page, enter the user name and initial password written in the user registration completion notification email.

After authentication is complete, you will see a message saying "Set up two-factor authentication". Prepare the app for OTP registration and select "TOTP".

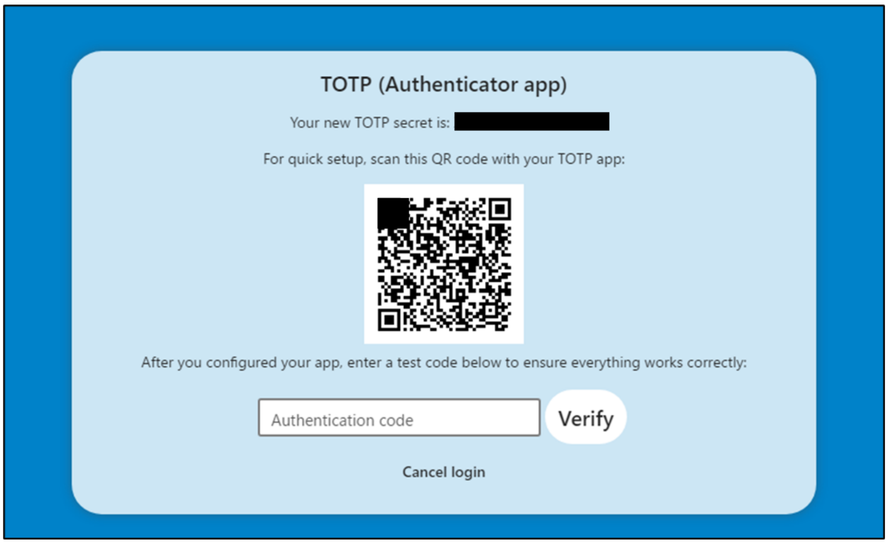


Set up two-factor authentication

Enhanced security is enforced for your account. Choose which provider to set up:

Get the URL displayed in the OTP registration app, or register the OTP using the "TOTP secret" value. Enter the 6-digit number displayed on the OTP registration app into the "Authentication code" field and press the "Verify" button.

***The QR code and secret key will be displayed only when you log in for the first time. Please don't forget to register your OTP.**



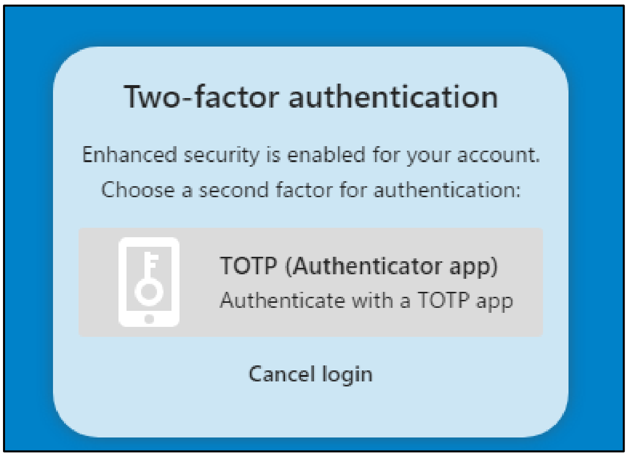
TOTP (Authenticator app)

Your new TOTP secret is: [redacted]

For quick setup, scan this QR code with your TOTP app:

After you configured your app, enter a test code below to ensure everything works correctly:

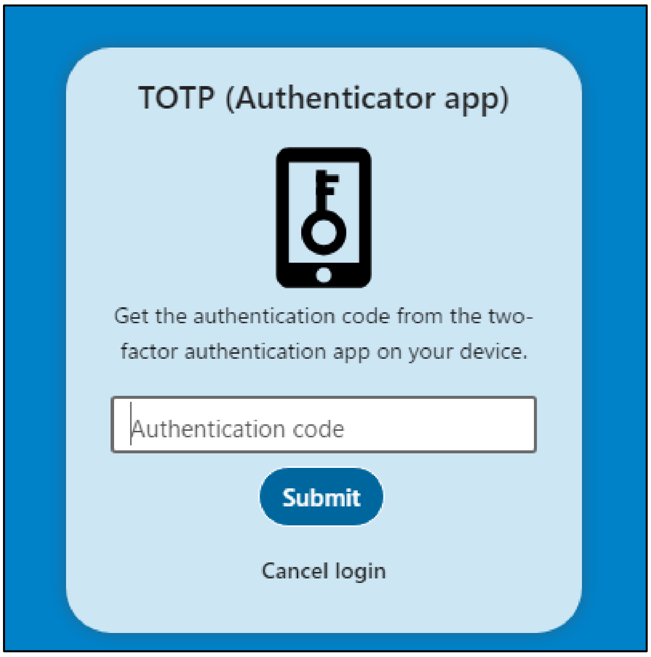
You will be asked to select an authentication method again, so select "TOTP".



Two-factor authentication

Enhanced security is enabled for your account. Choose a second factor for authentication:

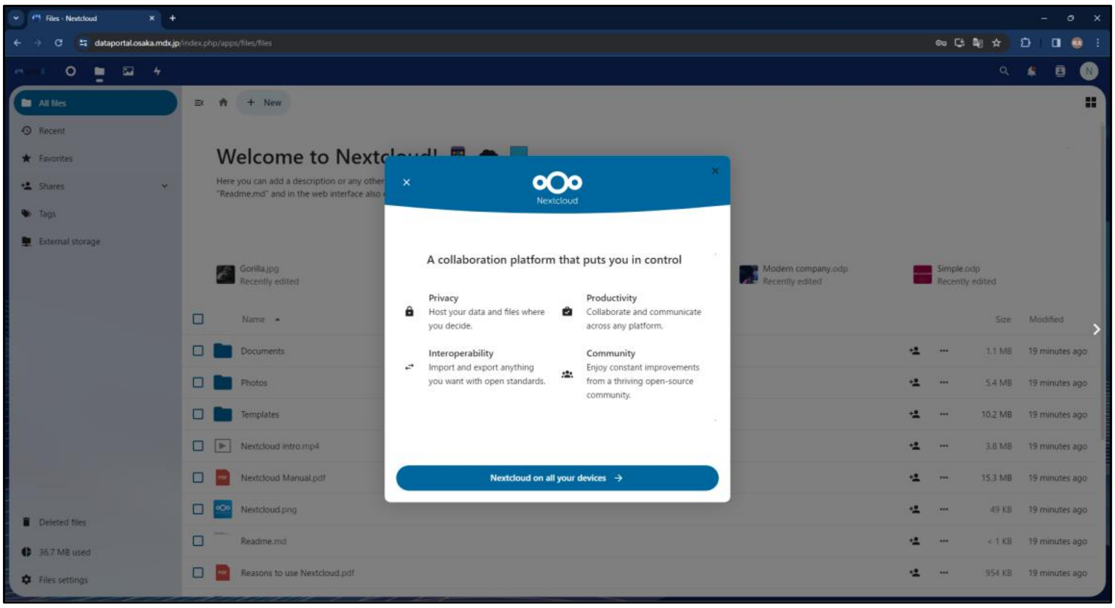
Finally, an OTP input field for authentication will be displayed. Enter the 6-digit number displayed on the OTP registration app into the "Authentication code" field and press the "Submit" button.



TOTP (Authenticator app)

Get the authentication code from the two-factor authentication app on your device.

After successful login, the dashboard will be displayed.



Welcome to Nextcloud!

Here you can add a description or any other ... "Readme.md" and in the web interface also ...

A collaboration platform that puts you in control

Privacy
Host your data and files where you decide.

Productivity
Collaborate and communicate across any platform.

Interoperability
Import and export anything you want with open standards.

Community
Enjoy constant improvements from a thriving open-source community.

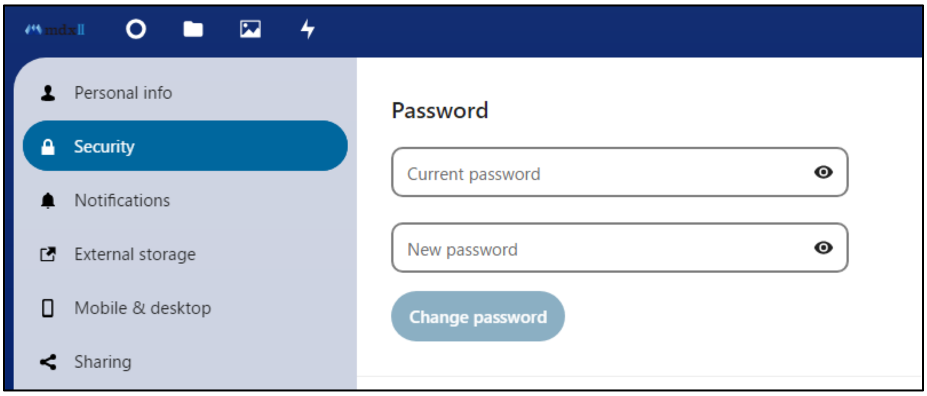
Gorilla.jpg
Recently edited

Modern company.odp
Recently edited

Simple.odp
Recently edited

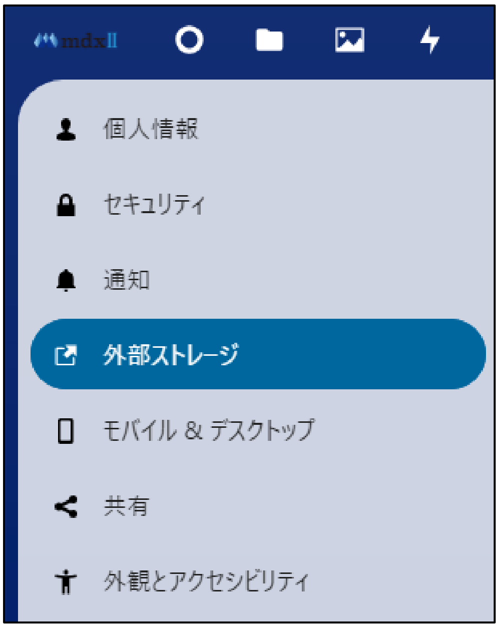
Name	Size	Modified
Documents	1.1 MB	19 minutes ago
Photos	5.4 MB	19 minutes ago
Templates	10.2 MB	19 minutes ago
Nextcloud intro.mp4	3.8 MB	19 minutes ago
Nextcloud Manual.pdf	15.3 MB	19 minutes ago
Nextcloud.png	49 KB	19 minutes ago
Readme.md	< 1 KB	19 minutes ago
Reasons to use Nextcloud.pdf	954 KB	19 minutes ago

Change the initial password. Click "Settings" on the user icon to move to the personal settings screen. Please change it from "Security" on the left vane and "Password" at the top.

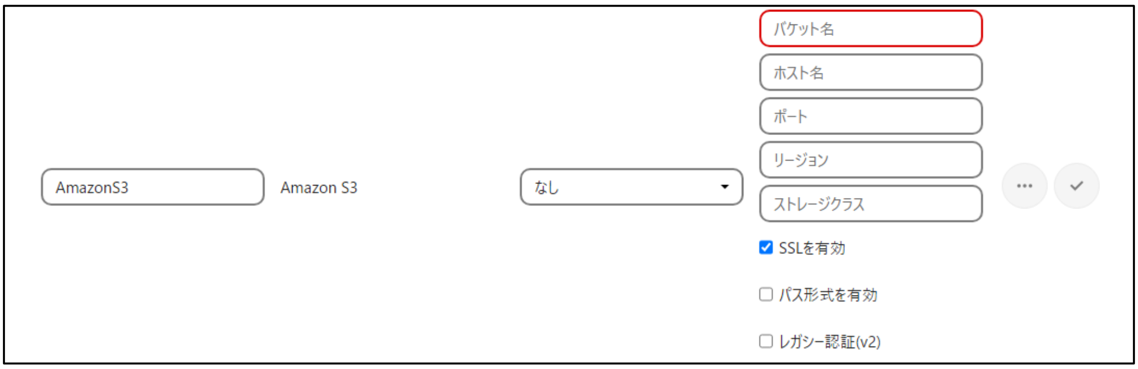


4.5.3. How to use

Nextcloud allows you to connect to online storage that supports S3 by using the external storage plugin. Click "Settings" on the user icon and select "External Storage" on the left pane.



Select Amazon S3 from the Add Storage dropdown in the External Storage column.



AmazonS3 | Amazon S3 | なし

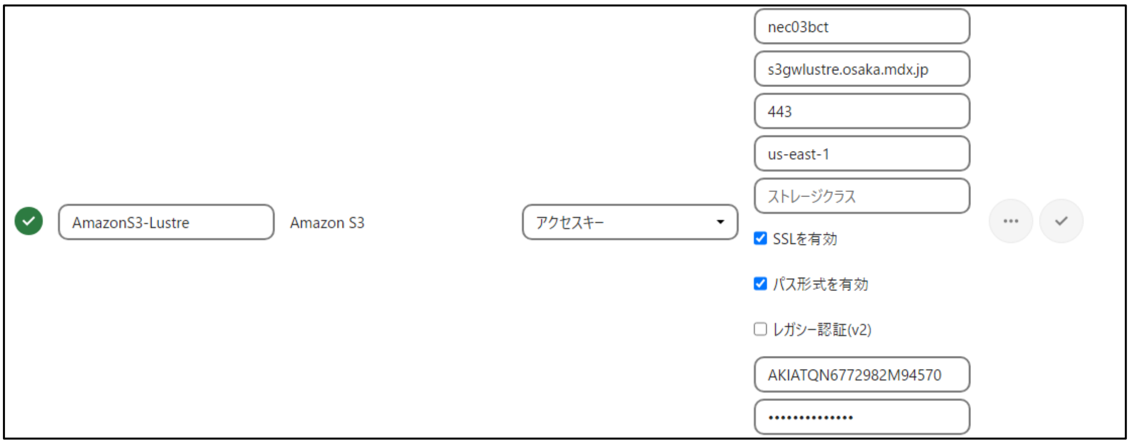
☑ SSLを有効

□ パス形式を有効

□ レガシー認証(v2)

4.5.3.1. Luster file system connection settings

The figure and table below are examples of connection information settings.



AmazonS3-Lustre

Amazon S3

アクセスキー

nec03bct

s3gwlustre.osaka.mdx.jp

443

us-east-1

ストレージクラス

☑ SSLを有効

☑ パス形式を有効

☐ レガシー認証(v2)

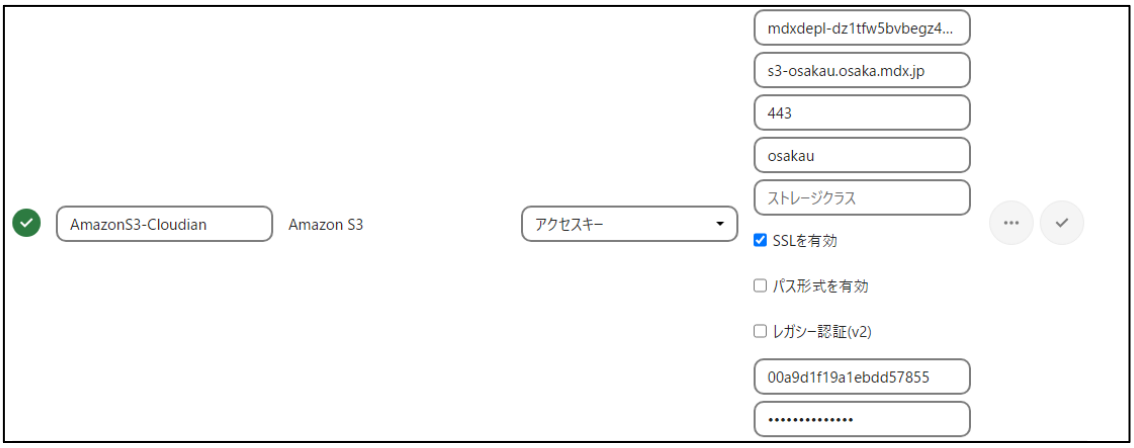
AKIATQN6772982M94570

••••••••••••••

Setting	Example	Explanation
Folder name	AmazonS3-Lustre	Any
external storage	Amazon S3	Only Amazon S3 can be selected.
certification	Access key	Select access key.
bucket name	nec03bct	Bucket name to connect to.
hostname	s3gwlustre.osaka.mdx.jp	Enter the S3 endpoint. An example is the S3 server endpoint of this system file server.
port	443	Enter if specified.
region	us-east-1	Enter if specified.
storage class	-	S3 storage class. If not entered, the default "STANDARD" class will be set.
Enable SSL	Check	Check to enable SSL.
Enable path format	Check	Check this if you want to access in path format.
Legacy authentication	-	Check if you want to perform legacy authentication.
access key	****************	Access key for the connection destination.
secret key	****************	Connection festival secret key.

4.5.3.2. Object storage connection settings

The figure and table below are examples of connection information settings.



AmazonS3-Cloudian

Amazon S3

アクセスキー

mdxdepl-dz1tfw5bvbegz4...

s3-osakau.osaka.mdx.jp

443

osakau

ストレージクラス

☑ SSLを有効

□ パス形式を有効

□ レガシー認証(v2)

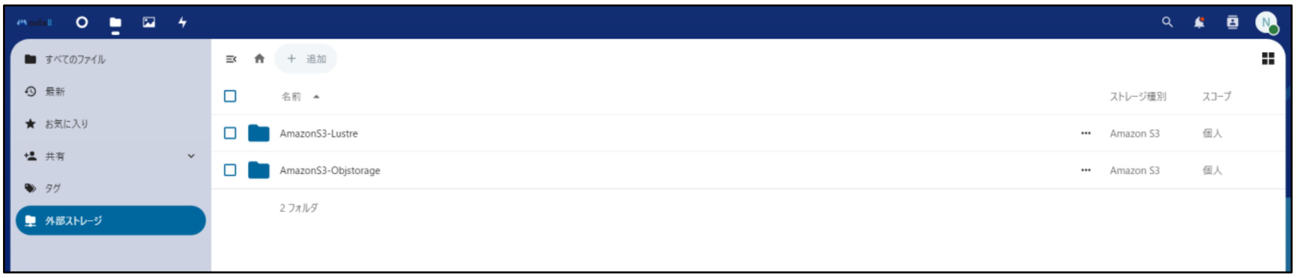
00a9d1f19a1ebdd57855

•••••••••••••••

Setting	Example	Explanation
Folder name	AmazonS3-Objstorage	Any
external storage	Amazon S3	Only Amazon S3 can be selected.
certification	Access key	Select access key.
bucket name	mdxdepl-dz1tfw5bvbegz4kpl2vn	Bucket name to connect to.
hostname	s3-osakau.osaka.mdx.jp	Enter the S3 endpoint. An example is the S3 server endpoint for this system object storage.
port	443	Enter if specified.
region	osakau	Enter if specified.
storage class	-	S3 storage class. If not entered, the default "STANDARD" class will be set.
Enable SSL	Check	Check to enable SSL.
Enable path format	-	Check this if you want to access in path format.
Legacy authentication	-	Check if you want to perform legacy authentication.
access key	***************	Access key for the connection destination.
secret key	***************	Connection festival secret key.

4.5.3.3. Using external storage

You can access your storage from the Files tab at the top of the page. You can operate the configured storage from "External Storage" on the left vane. Continuing to keep large amounts of data in the local area may cause capacity strain.



	名前		ストレージ種別	スコープ
□	AmazonS3-Lustre	•••	Amazon S3	個人
□	AmazonS3-Objstorage	•••	Amazon S3	個人
	2 フォルダ			

4.6. Interoperable Node（VMware）

4.6.1. Application for use

Please provide the following information to the system administrator via email when requesting a virtual machine.Also, attach the public key to use for public key authentication to connect to the virtual machine.

Blue text is comments.

----- 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　※Fill out the following items for each virtual machine requested, with N as the machine number from 1
　　利用 OS　　　　　：※Select from RockyLinux/Ubuntu Server/User's own template
　　CPU パック数　　：※1 CPU pack = 1 CPU core + 2GiB memory
　　ボリューム容量　　：※Describe in GB
　　グローバル IP 数　：※At least 1 is required for SSH access

The following is an example for filling out the form.

----- 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　　　　　　　　　　　：**Test Taro**
所属機関名　　　　　　　　：**Test University1**
連絡先メールアドレス　　　：**xxxx@xxx.com**

```
請求先担当者氏名　　　　　：Test Jiro
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　　：Test University2
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　　　　　　　　：User's own template
    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. How to use

Connect to the virtual machine using SSH command or terminal software with public key authentication. The public key used for SSH connection needs to be submitted to the system administrator in advance.

※Do not change the IP address set for the virtual machine, as you will lose

(1) First SSH aaccess

<Login from UNIX-based OS (Linux, MacOS)>

Example) Login to to the virtual machine.

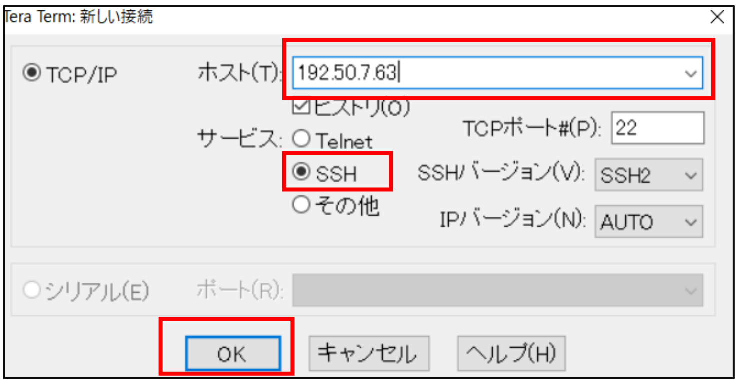
```
$ ssh mdxuser@< virtual machine’s IP address>
The authenticity of host ‘< virtual machine’s Info>’ can’t be established.
RSA key fingerprint is 32:fd:73:4e:7f:aa:5d:3c:2e:ab:37:83:d6:55:98:e2.
Are you sure you want to continue connecting (yes/no)? yes
Warning Permanently added ‘< virtual machine’s Info >’ to the list of known hosts.
Enter passphrase for key ‘<>’:
```

<Login from Microsoft® Windows®>

Access with SSH from a terminal software.

Example) Instructions for SSH access using “Tera Term Pro” free software.

- Start Tera Term Pro and open “Tera Term: New connection” dialog
- Select TCP / IP.
- Enter the Virtual Machine’s IP addresse in the host field.
- Select SSH as the service.
- Click OK



Tera Term: 新しい接続

● TCP/IP　ホスト(T): 192.50.7.63

☑ヒストリ(O)

サービス: ○Telnet　●SSH　○その他

TCPポート#(P): 22

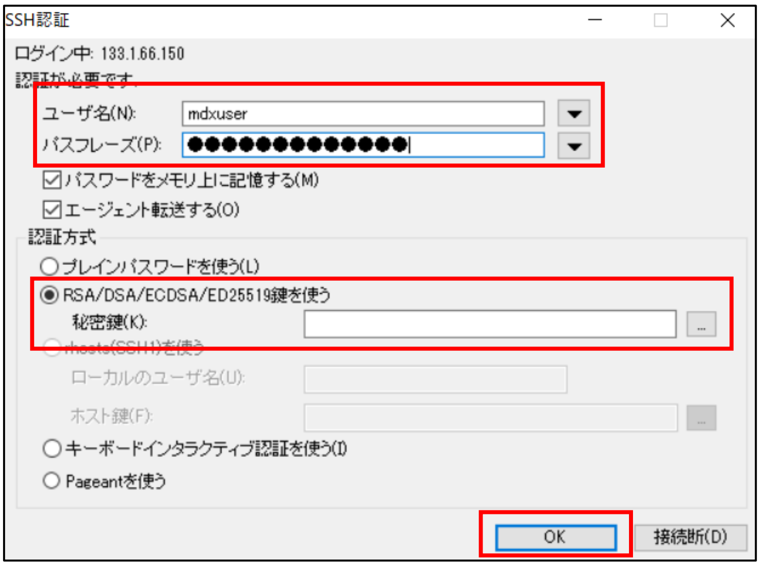
SSHバージョン(V): SSH2

IPバージョン(N): AUTO

○シリアル(E)　ポート(R):

OK　キャンセル　ヘルプ(H)

- In SSH authentication screen, select " RSA/DSA/ECDSA/ED25519 key を使う" for authentication method, and select the created private key.
- Enter username and passphrase for the private key, and click OK.



SSH認証

ログイン中: 133.1.66.150

認証が必要です.

ユーザ名(N): mdxuser

パスフレーズ(P): ●●●●●●●●●●●●●●

☑パスワードをメモリ上に記憶する(M)

☑エージェント転送する(O)

認証方式

○プレインパスワードを使う(L)

●RSA/DSA/ECDSA/ED25519鍵を使う

秘密鍵(K):

○rhosts(SSH1)を使う

ローカルのユーザ名(U):

ホスト鍵(F):

○キーボードインタラクティブ認証を使う(I)

○Pageantを使う

OK　接続断(D)

4.6.3. Lustre Mount

Please send an email to your system administrator with the following information and request to use Luster mount.

```
----- Luster mount usage application format   -----
Project name: *Enter the project name
Virtual machine IP address: *IP address assigned to the virtual machine (172.16.10.X)
Usage capacity: *Listed in GB
-----------------------------------------------------------
```

*Based on the above information, the system administrator will set the necessary information on the file server.

After your system administrator notifies you that Luster mounts are available, you will need to configure the Luster client on your virtual machine. The RokcyLinux 9.3 and Ubuntu 22.04 LTS OS images prepared on the system side include Luster client packages and configuration files.
The following describes how to mount Luster on a virtual machine created with an OS image prepared by the system.

(1) Log in to the virtual machine and switch to the root account using sudo su, etc.

(2) Check the interface name where the Luster network IP address (192.168.[100,101].X) is set on the virtual machine.

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

(3) Correct the interface name specified in /etc/modprobe.d/lustre.conf to the confirmed interface name. *Bold parts will be corrected.

```
# 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) Correct the interface name specified in /etc/sysconfig/lustre_client to the confirmed interface name.
* The file path is different between Rocky Linux (RHEL series) and Ubuntu Server.
*Bold parts will be corrected.

- Rocky Linux

```
# vi /etc/sysconfig/lustre_client
…omission…
#++++++++++++++++++++++++++++++++++++++
# LNET Interface
#
```

```
IF1=eth0
…omission…
```

- Ubuntu Server

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

(5) Start lustre_client.service.

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

(6) Confirm that Luster mount is possible.

```
# 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) Enable automatic startup of lustre_client.service so that Lustre mounts automatically when the virtual machine OS starts. (Any)

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

These are the steps to configure the Luster client.
When handling data in the file server area, please use the "/lustre" directory mounted by Lustre.

5. Feature Description

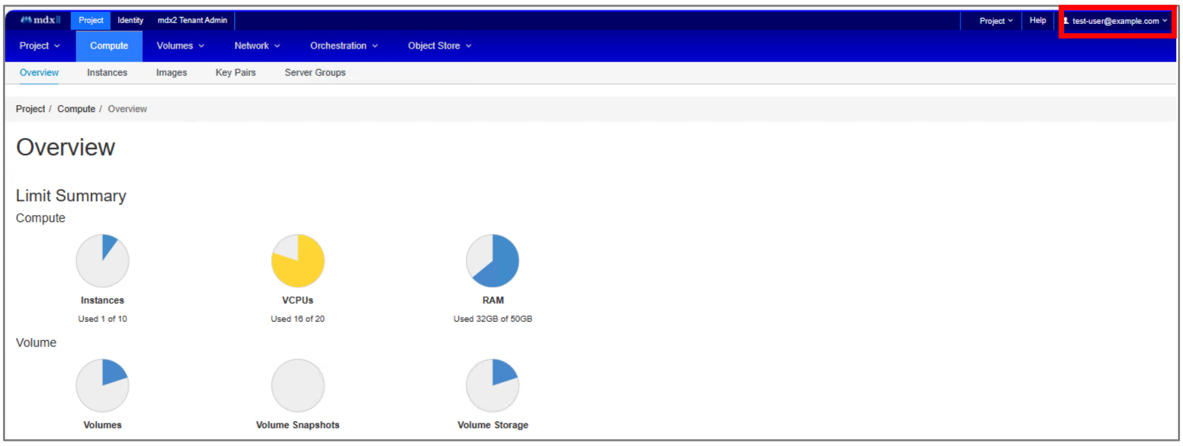
5.1. User Portal

The user portal consists of the OpenStack Dashboard. This section describes the various functions available on the user portal.

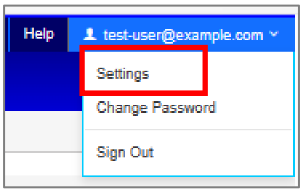
5.1.1. Change language

You can change language settings on the user portal.

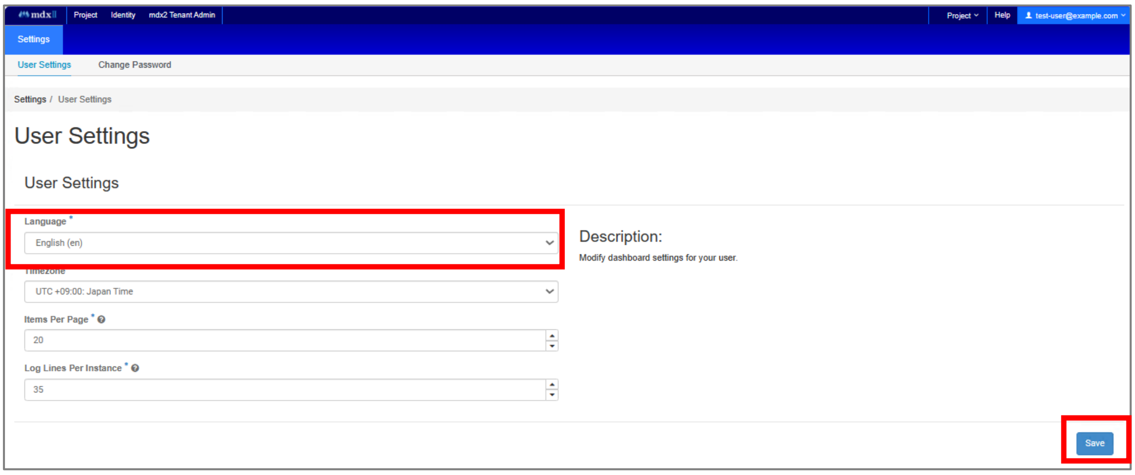
(1) Click on the user name at the top right of the Dashboard.



(2) Click [Settings].



(3) Select the language you want to use from the [Language] pull-down menu and click the [Save] button.



User Settings

User Settings

Language * English (en)

Timezone UTC +09:00: Japan Time

Items Per Page * 20

Log Lines Per Instance * 35

Description:

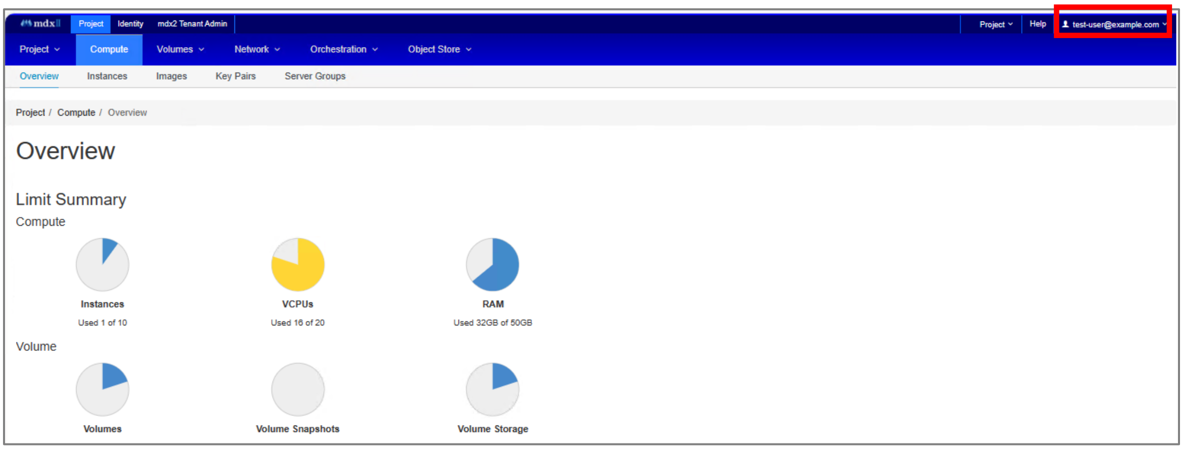
Modify dashboard settings for your user.

5.1.2. Changing the local password

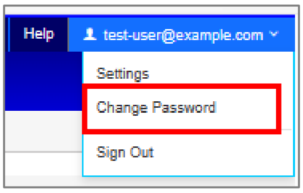
If you use a local account, you can change your local password.

*If you are using a GakuNin account, a local password will not be issued when applying for a project. If you have applied for an additional local password and have a password, you can change your password by following the steps described in this section.

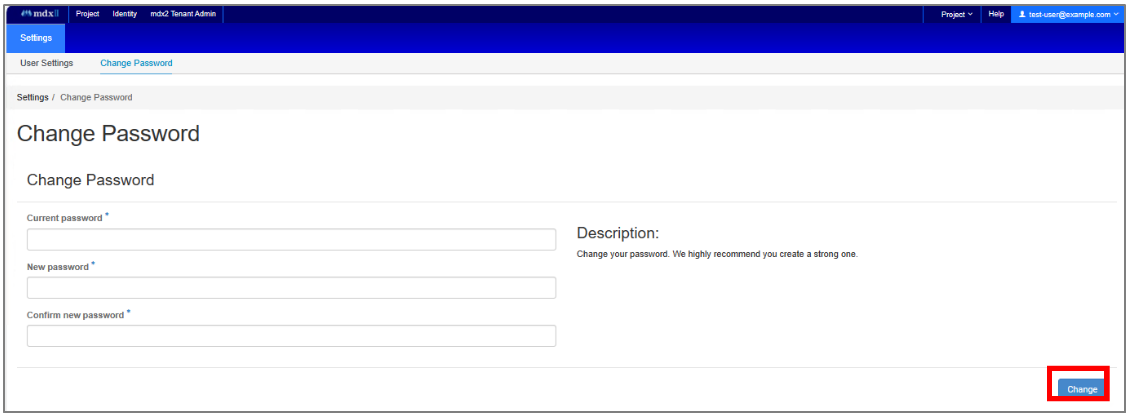
(1) Click on the user name at the top right of the Dashboard.



(2) Click [Change Password].



(3) Enter the following items and click the [Change] button.

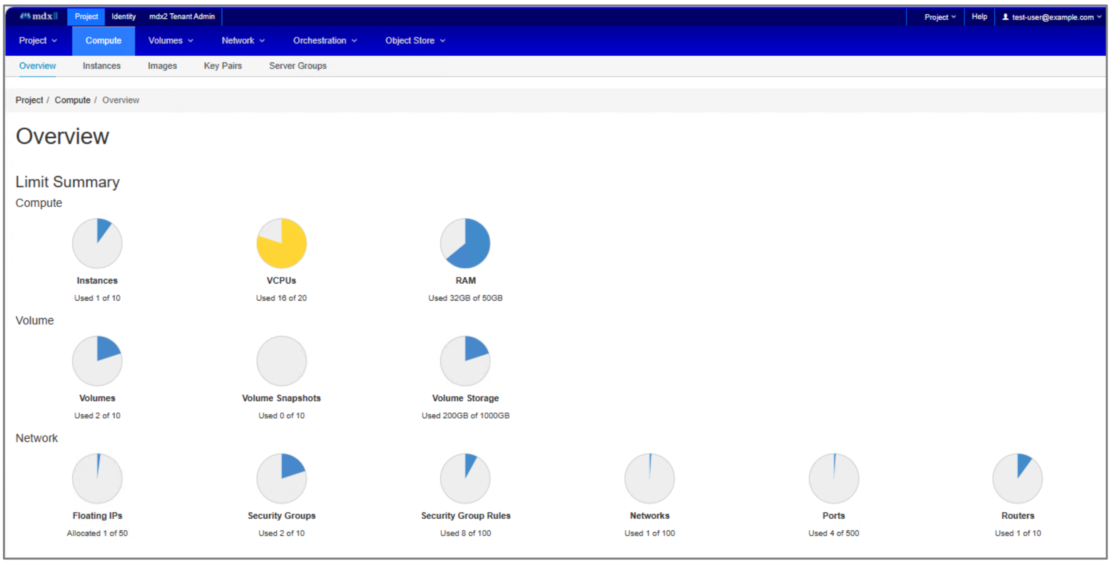


Description:

Change your password. We highly recommend you create a strong one.

5.1.3. Confirmation of resource amount

You can understand the status of the amount of resources in your project using the pie chart that is displayed when you log in to the user portal. The amount of resources being used against the project quota (limit value) is displayed in blue.



Overview

Limit Summary

Compute

Instances	VCPUs	RAM
Used 1 of 10	Used 16 of 20	Used 32GB of 50GB

Volume

Volumes	Volume Snapshots	Volume Storage
Used 2 of 10	Used 0 of 10	Used 200GB of 1000GB

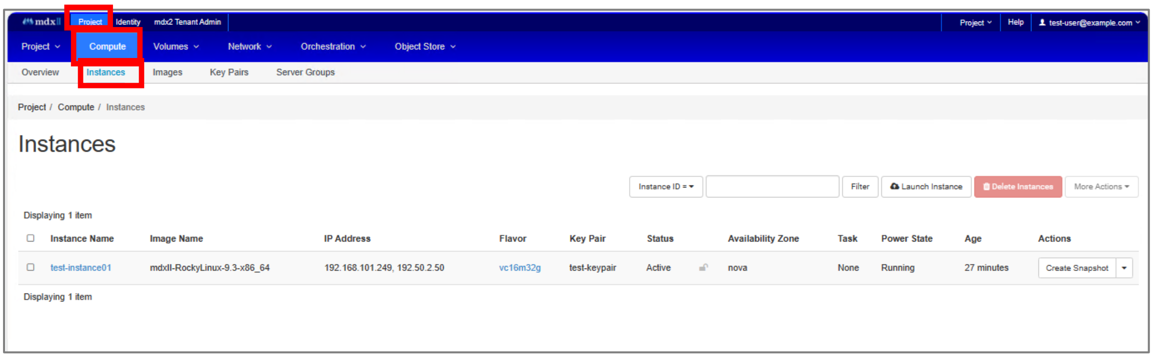
Network

Floating IPs	Security Groups	Security Group Rules	Networks	Ports	Routers
Allocated 1 of 50	Used 2 of 10	Used 8 of 100	Used 1 of 100	Used 4 of 500	Used 1 of 10

5.1.4. Virtual Machine Console

Virtual machines can be accessed from the console. When accessing from the console, a password must be set for the user in the virtual machine.

(1) Click the [Project] menu > [Compute] panel > [Instances] tab.



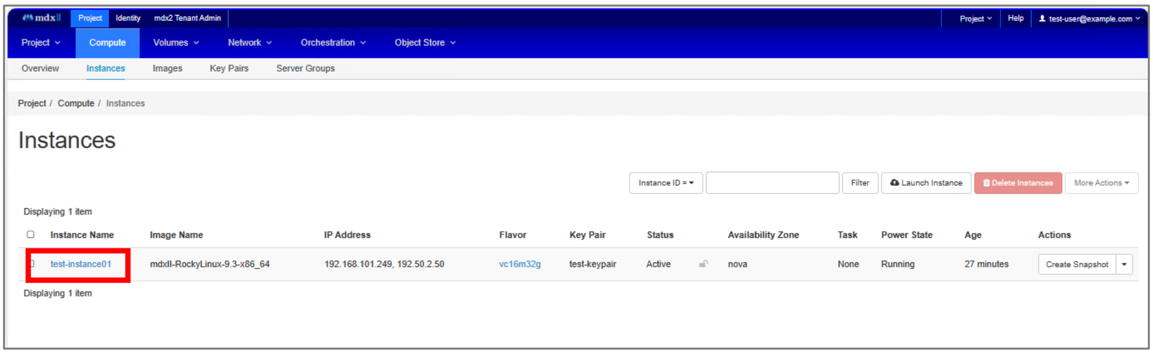
Instances

Displaying 1 item

□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	test-instance01	mdxII-RockyLinux-9.3-x86_64	192.168.101.249, 192.50.2.50	vc16m32g	test-keypair	Active	nova	None	Running	27 minutes	Create Snapshot

Displaying 1 item

(2) Click the instance name on the virtual machine where you want to open the console.



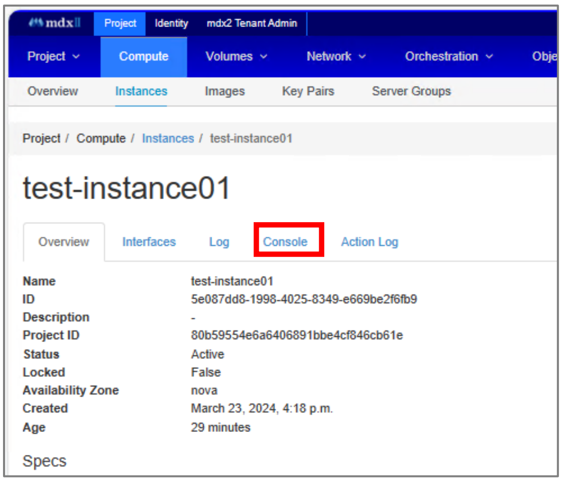
Instances

Displaying 1 item

□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	test-instance01	mdxII-RockyLinux-9.3-x86_64	192.168.101.249, 192.50.2.50	vc16m32g	test-keypair	Active	nova	None	Running	27 minutes	Create Snapshot

Displaying 1 item

(3) Click the [Console] tab.

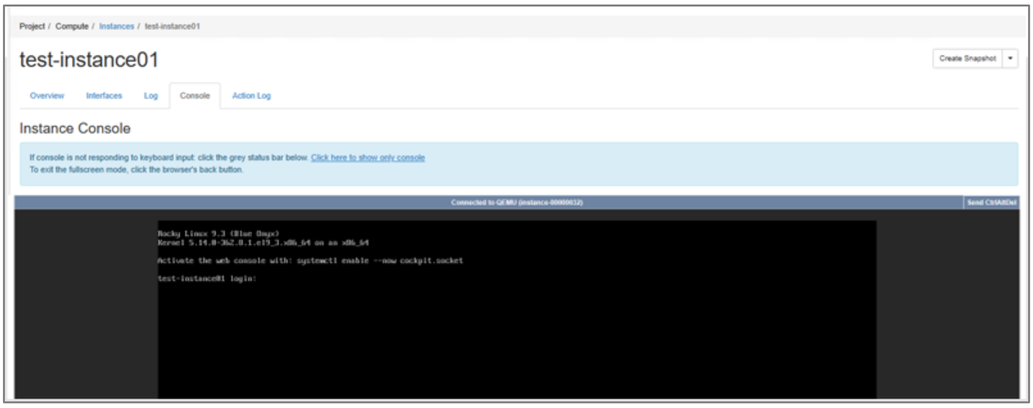


test-instance01

Name	test-instance01
ID	5e087dd8-1998-4025-8349-e669be2f6fb9
Description	-
Project ID	80b59554e6a6406891bbe4cf846cb61e
Status	Active
Locked	False
Availability Zone	nova
Created	March 23, 2024, 4:18 p.m.
Age	29 minutes

Specs

(4) The console screen will open and you can access the virtual machine using password authentication.


Project / Compute / Instances / test-instance01
Create Snapshot
Overview
Interfaces
Log
Console
Action Log
Connected to QEMU (instance-00000032)
Send CtrlAltDel

test-instance01

Instance Console

If console is not responding to keyboard input: click the grey status bar below. Click here to show only console
To exit the fullscreen mode, click the browser's back button.

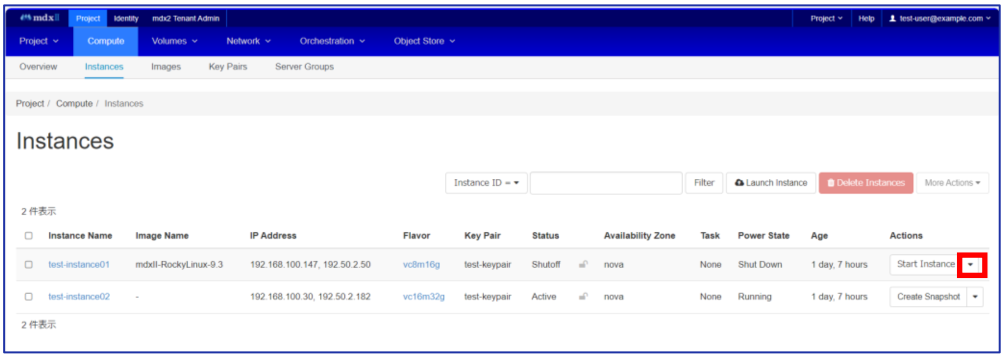
```
Rocky Linux 9.3 (Blue Onyx)
Kernel 5.14.0-362.8.1.el9_3.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

test-instance01 login:
```

5.1.5. Changing the flavor of a virtual machine

It is possible to change the flavor of the virtual machine and resize the amount of resources.

(1) Shut down the target virtual machine.

(2) Click the pull-down menu on the right side of the target virtual machine on the instance screen.



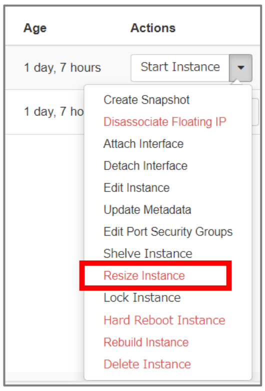
Instances

2 件表示

□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	test-instance01	mdxII-RockyLinux-9.3	192.168.100.147, 192.50.2.50	vc8m16g	test-keypair	Shutoff	nova	None	Shut Down	1 day, 7 hours	Start Instance ▾
□	test-instance02	-	192.168.100.30, 192.50.2.182	vc16m32g	test-keypair	Active	nova	None	Running	1 day, 7 hours	Create Snapshot ▾

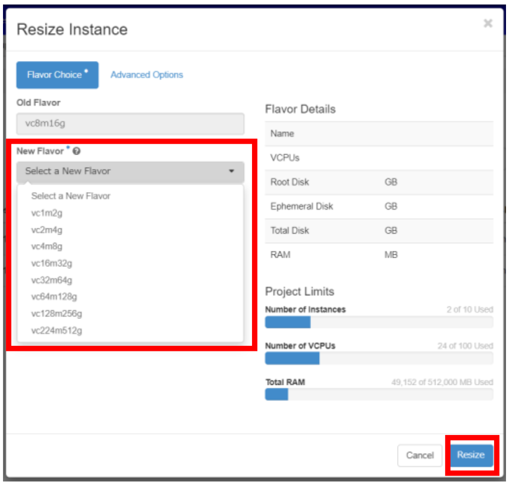
2 件表示

(3) Click [Resize Instance].

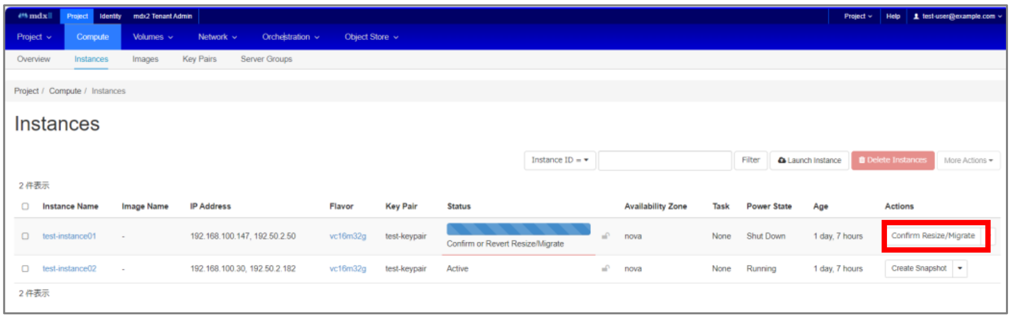


(4) Enter the following items and click [Resize].

・New flavor: *Select the flavor to resize



(5) Click the [Confirm Resize/Migration] button.



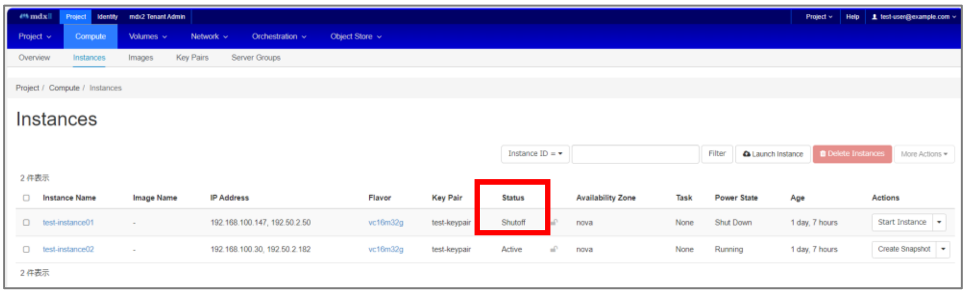
Instances

2 件表示

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
test-instance01	-	192.168.100.147, 192.50.2.50	vc16m32g	test-keypair	Confirm or Revert Resize/Migrate	nova	None	Shut Down	1 day, 7 hours	Confirm Resize/Migrate
test-instance02	-	192.168.100.30, 192.50.2.182	vc16m32g	test-keypair	Active	nova	None	Running	1 day, 7 hours	Create Snapshot

2 件表示

(6) When the resizing process is completed, the Status will change to "Shut off".



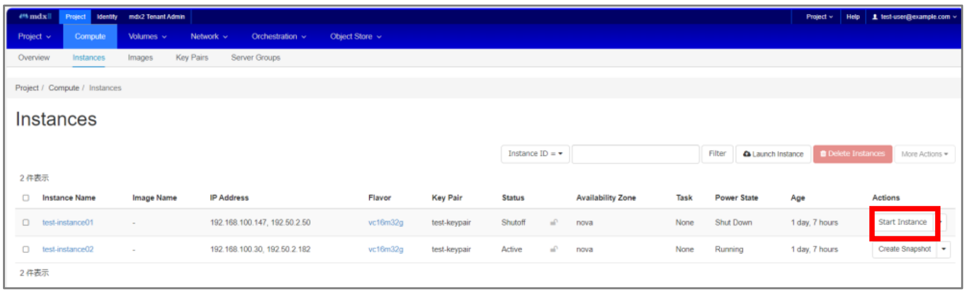
Instances

2 件表示

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
test-instance01	-	192.168.100.147, 192.50.2.50	vc16m32g	test-keypair	Shutoff	nova	None	Shut Down	1 day, 7 hours	Start Instance
test-instance02	-	192.168.100.30, 192.50.2.182	vc16m32g	test-keypair	Active	nova	None	Running	1 day, 7 hours	Create Snapshot

2 件表示

(7) Click the [Start Instance] button to start the instance.



Instances

2 件表示

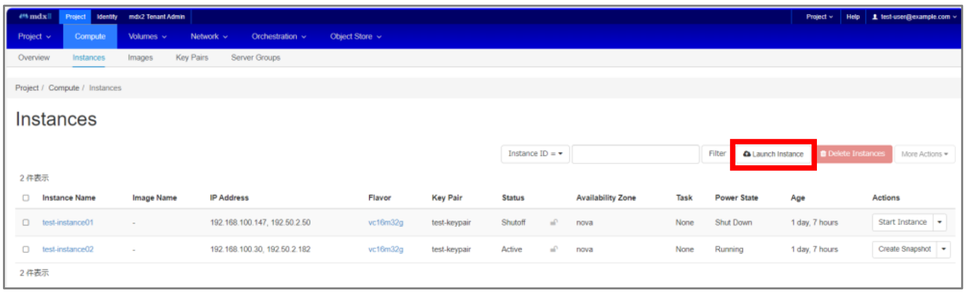
□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	test-instance01	-	192.168.100.147, 192.50.2.50	vc16m32g	test-keypair	Shutoff	nova	None	Shut Down	1 day, 7 hours	Start Instance
□	test-instance02	-	192.168.100.30, 192.50.2.182	vc16m32g	test-keypair	Active	nova	None	Running	1 day, 7 hours	Create Snapshot

2 件表示

5.1.6. Multi-deployment of virtual machines

It is possible to create multiple virtual machines with the same configuration at the same time.

(1) Click the [Launch Instance] button on the instance screen.



Instances

2 件表示

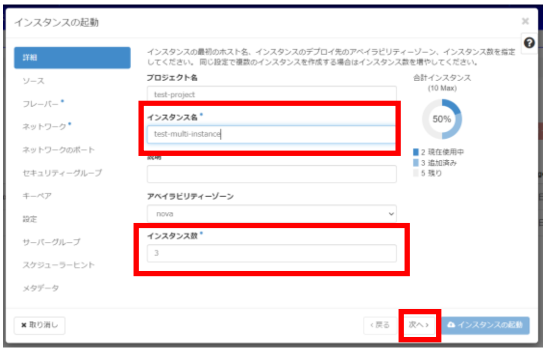
□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	test-instance01	-	192.168.100.147, 192.50.2.50	vc16m32g	test-keypair	Shutoff	nova	None	Shut Down	1 day, 7 hours	Start Instance
□	test-instance02	-	192.168.100.30, 192.50.2.182	vc16m32g	test-keypair	Active	nova	None	Running	1 day, 7 hours	Create Snapshot

2 件表示

(2) Enter the following items and click the [Next] button.

・Instance name: *Optional ("-<serial number>" will be automatically added to the end of the value entered here)

・Number of instances: *Number of virtual machines you want to create at the same time



インスタンスの起動

インスタンスの最初のホスト名、インスタンスのデプロイ先のアベイラビリティーゾーン、インスタンス数を指定してください。 同じ設定で複数のインスタンスを作成する場合はインスタンス数を増やしてください。

プロジェクト名: test-project

インスタンス名 *: test-multi-instance

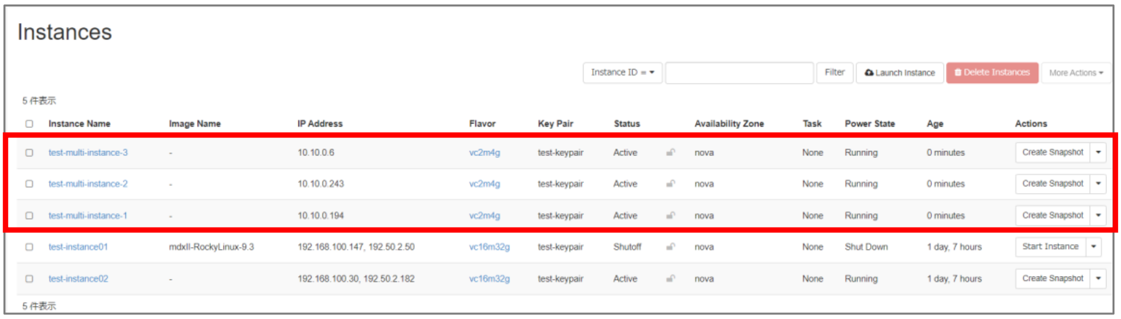
説明:

アベイラビリティーゾーン: nova

インスタンス数 *: 3

(3) Perform the remaining instance creation operations according to (4) to (8) in "4.1.7. Creating a virtual machine" to create an instance.

(4) Virtual machines for the specified number of instances are created at the same time and added to the list.



5 件表示

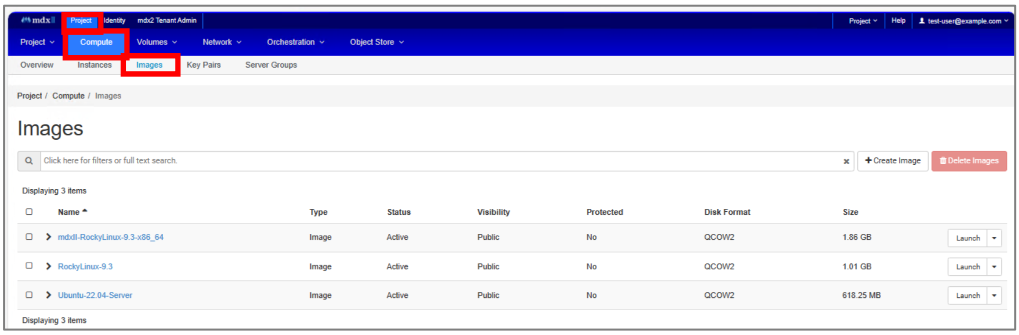
□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	test-multi-instance-3	-	10.10.0.6	vc2m4g	test-keypair	Active	nova	None	Running	0 minutes	Create Snapshot ▾
□	test-multi-instance-2	-	10.10.0.243	vc2m4g	test-keypair	Active	nova	None	Running	0 minutes	Create Snapshot ▾
□	test-multi-instance-1	-	10.10.0.194	vc2m4g	test-keypair	Active	nova	None	Running	0 minutes	Create Snapshot ▾
□	test-instance01	mdxII-RockyLinux-9.3	192.168.100.147, 192.50.2.50	vc16m32g	test-keypair	Shutoff	nova	None	Shut Down	1 day, 7 hours	Start Instance ▾
□	test-instance02	-	192.168.100.30, 192.50.2.182	vc16m32g	test-keypair	Active	nova	None	Running	1 day, 7 hours	Create Snapshot ▾

5 件表示

5.1.7. Upload ISO file/Virtual Machine Image

By uploading an ISO file such as an OS installer or a virtual machine image (QCOW2, etc.) and creating an image, you can create a virtual machine from the image.

(1) Click the [Project] menu > [Compute] panel > [Images] tab.

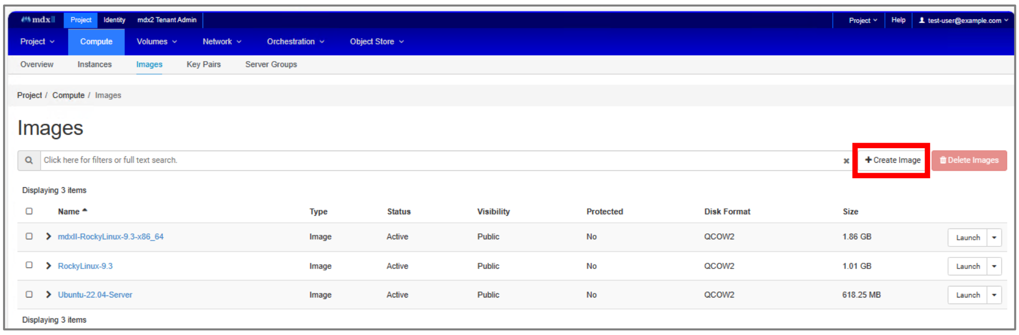


Displaying 3 items

□	Name ▴	Type	Status	Visibility	Protected	Disk Format	Size	
□	mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch ▾
□	RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch ▾
□	Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch ▾

Displaying 3 items

(2) Click the [Create Image] button.



Displaying 3 items

□	Name ▴	Type	Status	Visibility	Protected	Disk Format	Size	
□	mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch ▾
□	RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch ▾
□	Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch ▾

Displaying 3 items

(3) Enter the following items and click the [Create Image] button.

・Image Name: Any

・Image Source: *Select the file to upload

・Format: *Select according to the format of the uploaded file

・Images Sharing: Private

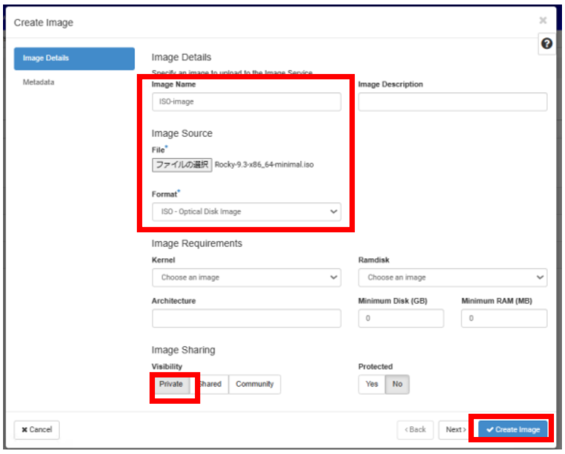
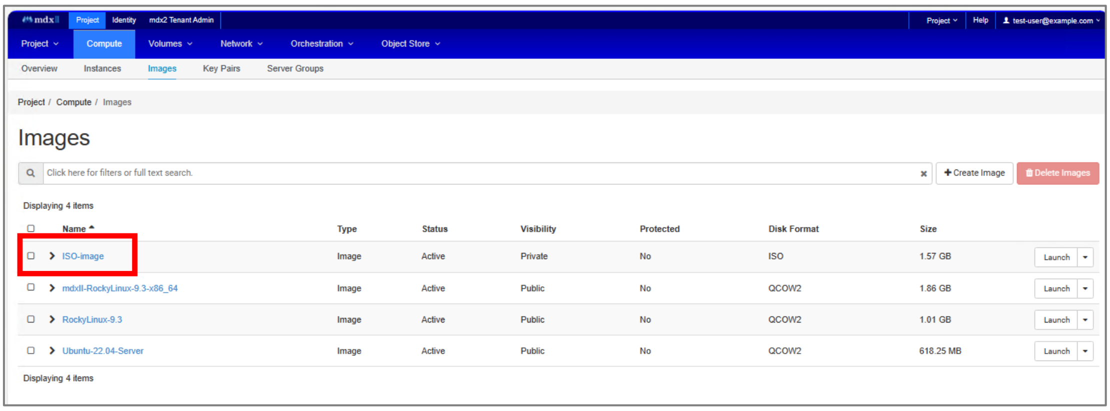


Image Name: ISO-image
Image Description:
Image Source
File*: ファイルの選択 Rocky-9.3-x86_64-minimal.iso
Format*: ISO - Optical Disk Image
Kernel: Choose an image
Ramdisk: Choose an image
Architecture:
Minimum Disk (GB): 0
Minimum RAM (MB): 0
Visibility: [✓ Private] Shared Community
Protected: Yes [✓ No]

(4) The created image will be displayed.



Displaying 4 items

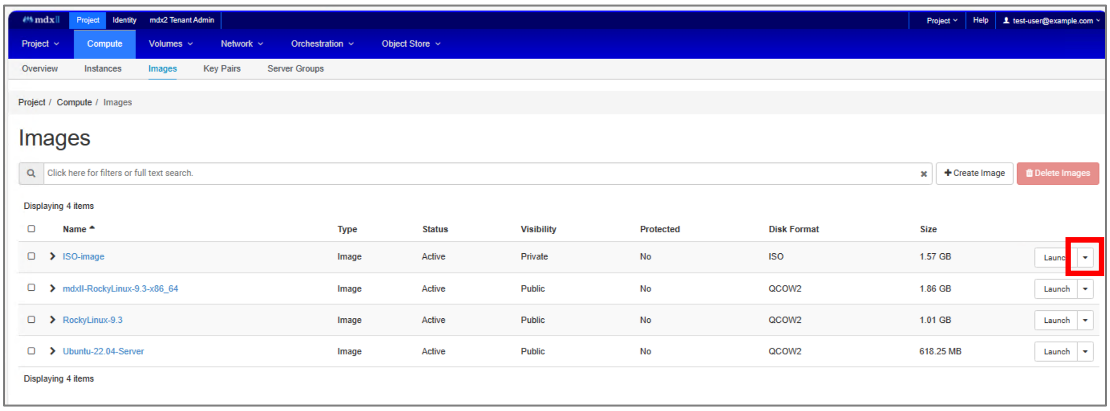
☐	Name ▲	Type	Status	Visibility	Protected	Disk Format	Size	
☐	› ISO-image	Image	Active	Private	No	ISO	1.57 GB	Launch ▾
☐	› mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch ▾
☐	› RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch ▾
☐	› Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch ▾

Displaying 4 items

5.1.8. Mount ISO file

If you want to mount an ISO file on a virtual machine, create the ISO file as a volume and attach it to the virtual machine.

(1) Click the pull-down menu to the right of the image you created.

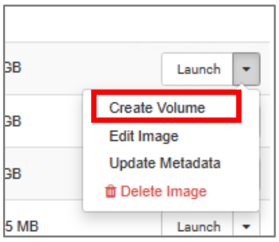


Displaying 4 items

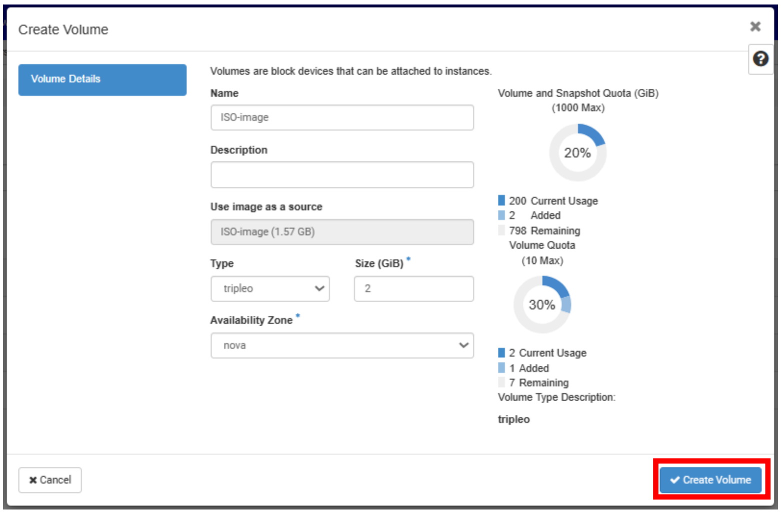
☐	Name ▲	Type	Status	Visibility	Protected	Disk Format	Size	
☐	› ISO-image	Image	Active	Private	No	ISO	1.57 GB	Launch ▾
☐	› mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch ▾
☐	› RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch ▾
☐	› Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch ▾

Displaying 4 items

(2) Click [Create Volume].



(3) Click the [Create Volume] button.



Create Volume

Volume Details

Volumes are block devices that can be attached to instances.

Name: ISO-image

Description:

Use image as a source: ISO-image (1.57 GB)

Type: tripleo

Size (GiB) *: 2

Availability Zone *: nova

Volume and Snapshot Quota (GiB)
(1000 Max)
20%
200 Current Usage
2 Added
798 Remaining

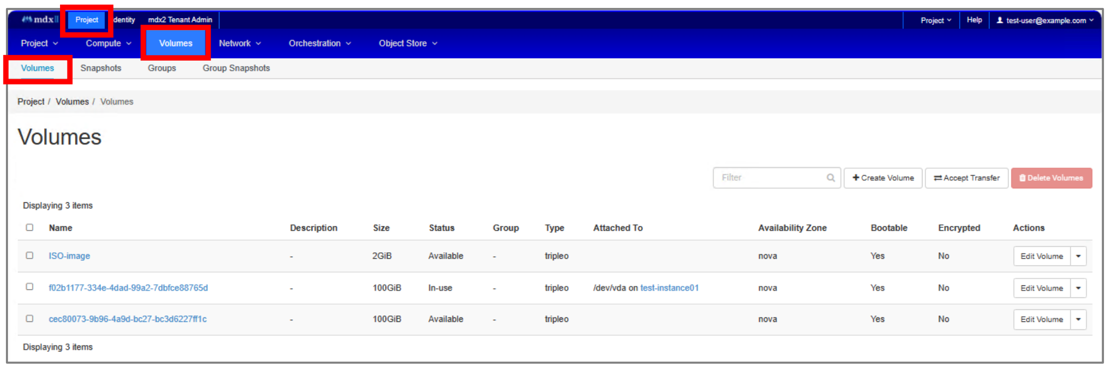
Volume Quota
(10 Max)
30%
2 Current Usage
1 Added
7 Remaining

Volume Type Description:
tripleo

✖ Cancel

✔ Create Volume

(4) Click the [Project] menu > [Volumes] panel > [Volumes] tab.



Project / Volumes / Volumes

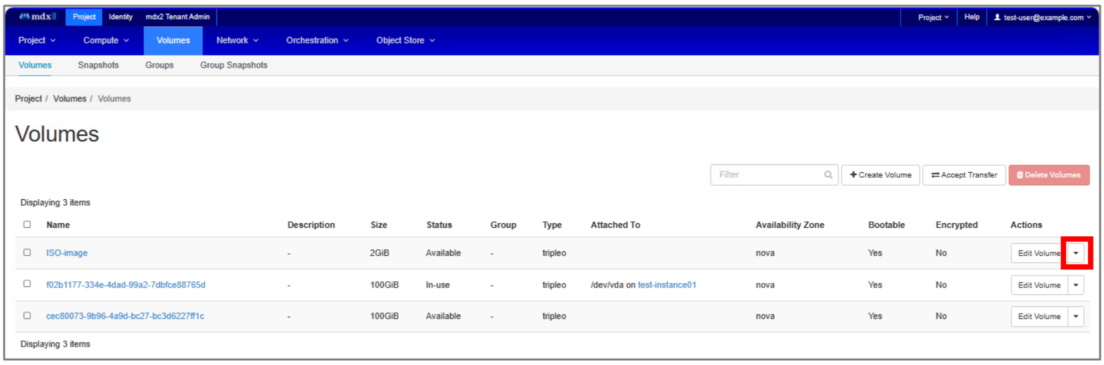
Volumes

Displaying 3 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	ISO-image	-	2GiB	Available	-	tripleo		nova	Yes	No	Edit Volume ▾
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume ▾
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume ▾

Displaying 3 items

(5) Click the drop-down menu to the right of the volume you created.



Project / Volumes / Volumes

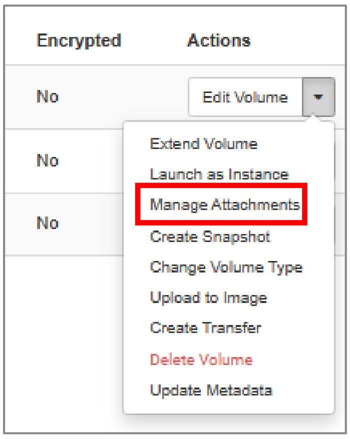
Volumes

Displaying 3 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	ISO-image	-	2GiB	Available	-	tripleo		nova	Yes	No	Edit Volume ▾
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume ▾
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume ▾

Displaying 3 items

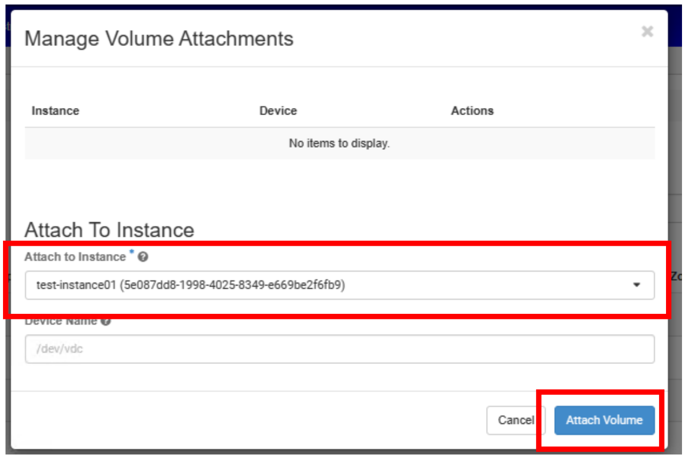
(6) Click [Manage Attachements].



Encrypted	Actions
No	Edit Volume ▾
No	
No	

(7) Enter the following items and click the [Attach Volume] button.

・Attach to Instance: *Specify the instance where you want to use the ISO file



Manage Volume Attachments

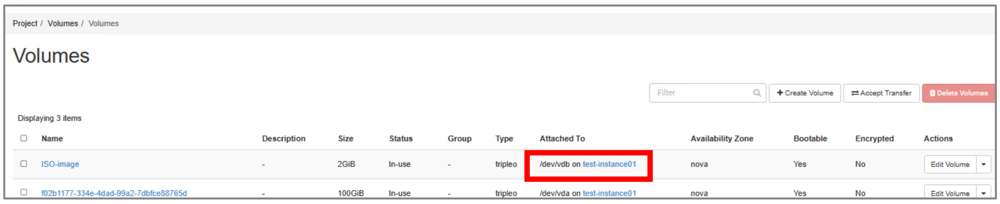
Instance	Device	Actions
No items to display.		

Attach To Instance

Attach to Instance *: test-instance01 (5e087dd8-1998-4025-8349-e669be2f6fb9)

Device Name: /dev/vdc

(8) Confirm that the virtual machine name and device name to which the volume is attached are displayed in Attached To in the volume list.



Project / Volumes / Volumes

Volumes

Displaying 3 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	ISO-image	-	2GiB	In-use	-	tripleo	/dev/vdb on test-instance01	nova	Yes	No	Edit Volume ▾
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume ▾

(9) Mount the volume of the ISO file connected to the virtual machine to a directory. Below is an example.

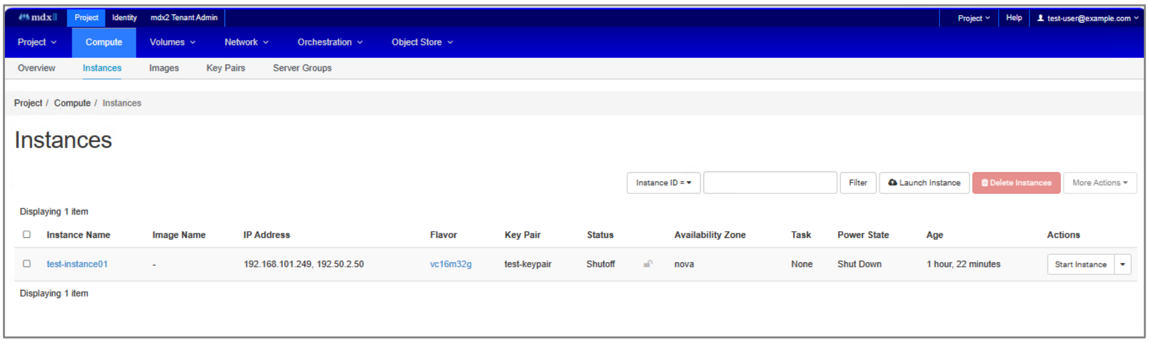
```
# mkdir /mnt/iso
# mount -o loop /dev/vdb /mnt/iso
```

5.1.9. Creating an image file from a virtual machine

You can back up a virtual machine by creating an image from it. You can also download the created image.

(1) Shut down the target virtual machine.

(2) Click the [Project] menu > [Compute] panel > [Instances] tab.

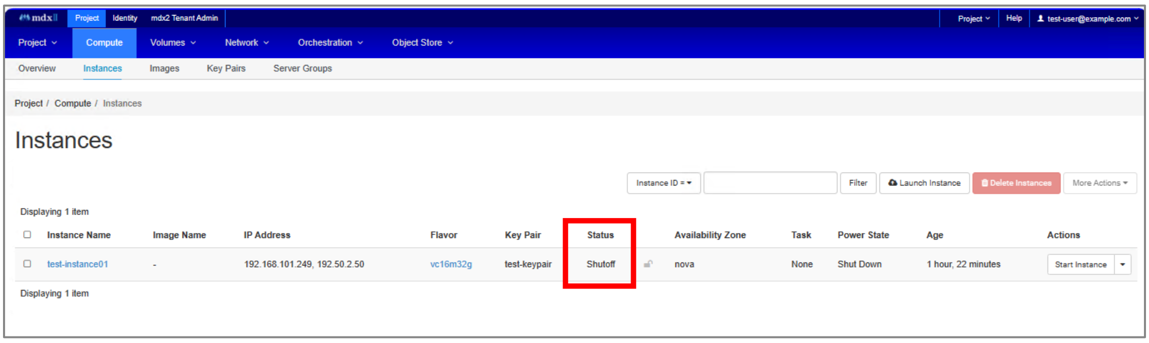


Displaying 1 item

□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status		Availability Zone	Task	Power State	Age	Actions
□	test-instance01	-	192.168.101.249, 192.50.2.50	vc16m32g	test-keypair	Shutoff		nova	None	Shut Down	1 hour, 22 minutes	Start Instance

Displaying 1 item

(3) Confirm that the Status of the target virtual machine is "Powered Off".

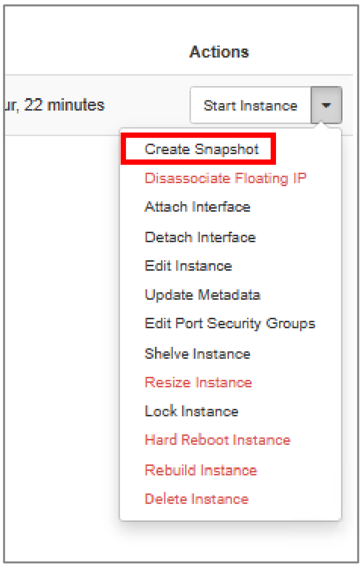


Displaying 1 item

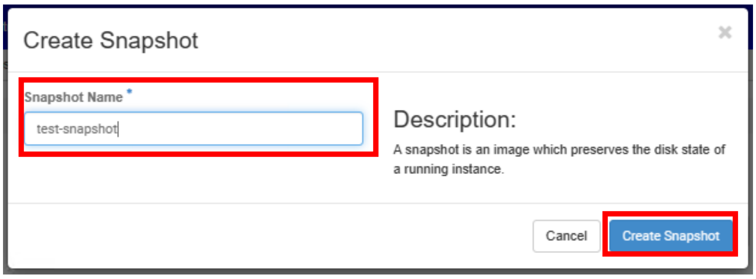
□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status		Availability Zone	Task	Power State	Age	Actions
□	test-instance01	-	192.168.101.249, 192.50.2.50	vc16m32g	test-keypair	Shutoff		nova	None	Shut Down	1 hour, 22 minutes	Start Instance

Displaying 1 item

(4) Click [Create Snapshot] from the pull-down menu on the right side of the target virtual machine.



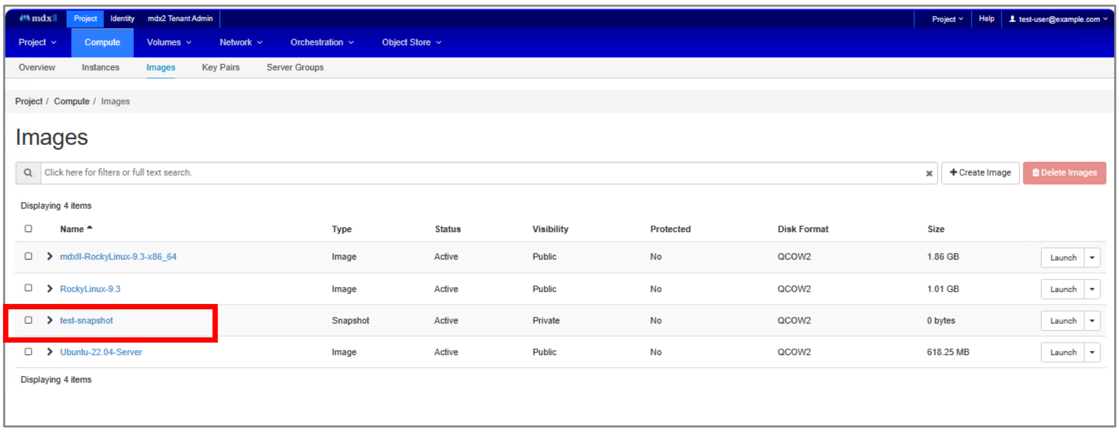
(5) Enter any snapshot name in [Snapshot Name] and click the [Create Snapshot] button.



Snapshot Name *: test-snapshot

Description:
A snapshot is an image which preserves the disk state of a running instance.

(6) The created snapshot will be displayed in the image list. Snapshots save the difference from when they were taken, so the size is displayed here as "0 bytes".



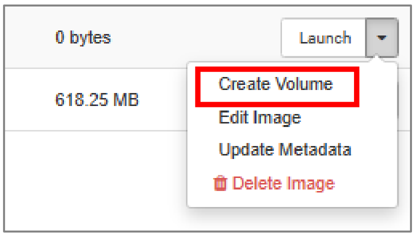
Images

Displaying 4 items

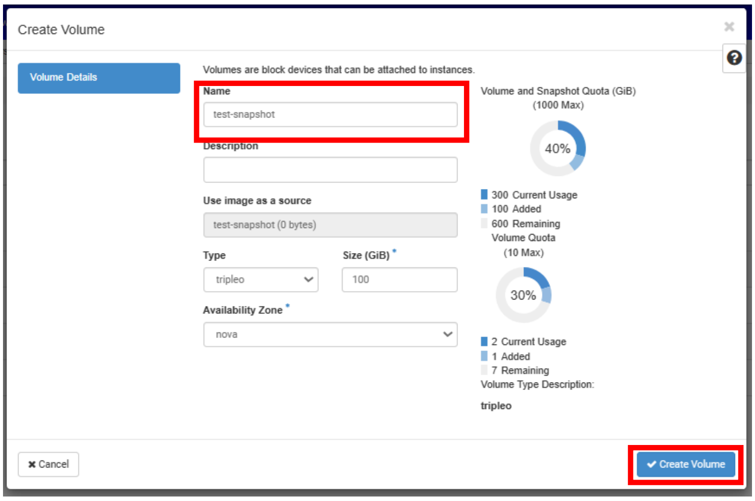
	Name	Type	Status	Visibility	Protected	Disk Format	Size	
□	mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch
□	RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch
□	test-snapshot	Snapshot	Active	Private	No	QCOW2	0 bytes	Launch
□	Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch

Displaying 4 items

(7) Click [Create Volume] from the pull-down menu to the right of the created snapshot.



(8) Enter any volume name in [Name] and click the [Create Volume] button.



Volumes are block devices that can be attached to instances.

Name: test-snapshot

Description:

Use image as a source: test-snapshot (0 bytes)

Type: tripleo

Size (GiB) *: 100

Availability Zone *: nova

Volume and Snapshot Quota (GiB) (1000 Max)

300 Current Usage
100 Added
600 Remaining

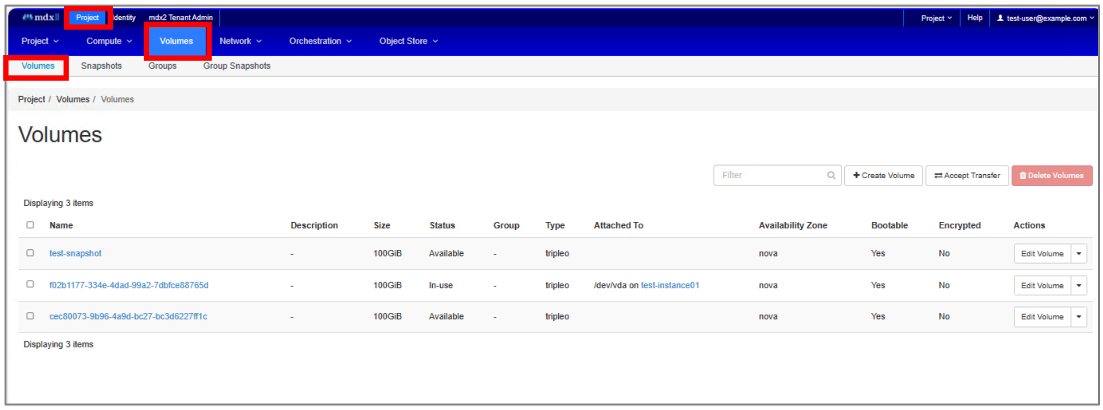
Volume Quota (10 Max)

2 Current Usage
1 Added
7 Remaining

Volume Type Description:

tripleo

(9) Click the [Project] menu > [Volumes] panel > [Volumes] tab.



Project / Volumes / Volumes

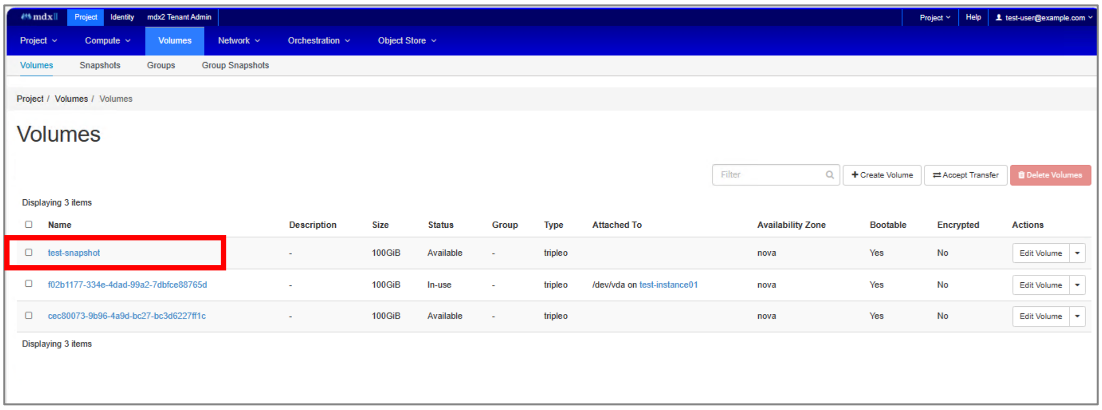
Volumes

Displaying 3 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	test-snapshot	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume

Displaying 3 items

(10) The created volume will be displayed.



Project / Volumes / Volumes

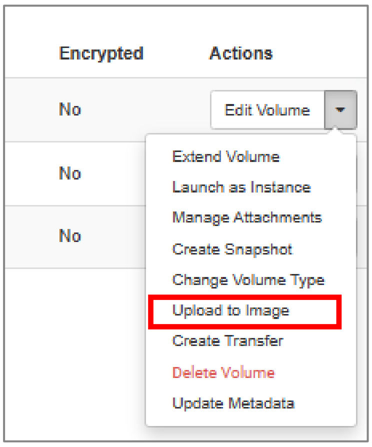
Volumes

Displaying 3 items

□	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
□	test-snapshot	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume
□	f02b1177-334e-4dad-99a2-7dbfce88765d	-	100GiB	In-use	-	tripleo	/dev/vda on test-instance01	nova	Yes	No	Edit Volume
□	cec80073-9b96-4a9d-bc27-bc3d6227ff1c	-	100GiB	Available	-	tripleo		nova	Yes	No	Edit Volume

Displaying 3 items

(11) Click [Upload to Image] in the pull-down menu to the right of the volume you created.

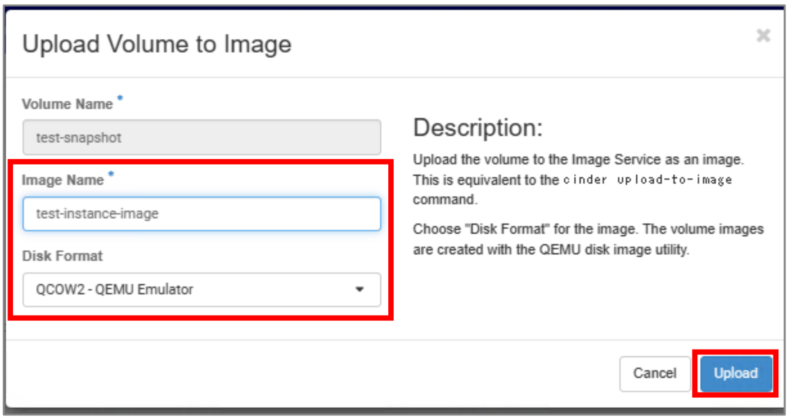


Encrypted	Actions
No	Edit Volume
No	
No	

(12) Enter the following items and click the [Upload] button.

・Image Name: *Optional

・Disc Format: *Change according to the file format you want to use



Upload Volume to Image

Volume Name *: test-snapshot

Image Name *: test-instance-image

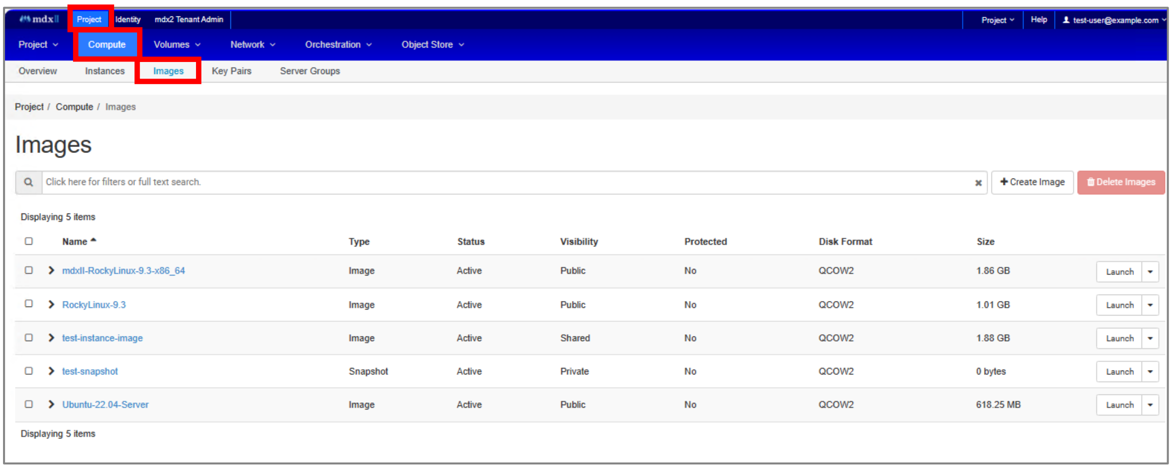
Disk Format: QCOW2 - QEMU Emulator

Description:

Upload the volume to the Image Service as an image. This is equivalent to the `cinder upload-to-image` command.

Choose "Disk Format" for the image. The volume images are created with the QEMU disk image utility.

(13) Click the [Project] menu > [Compute] panel > [Images] tab.



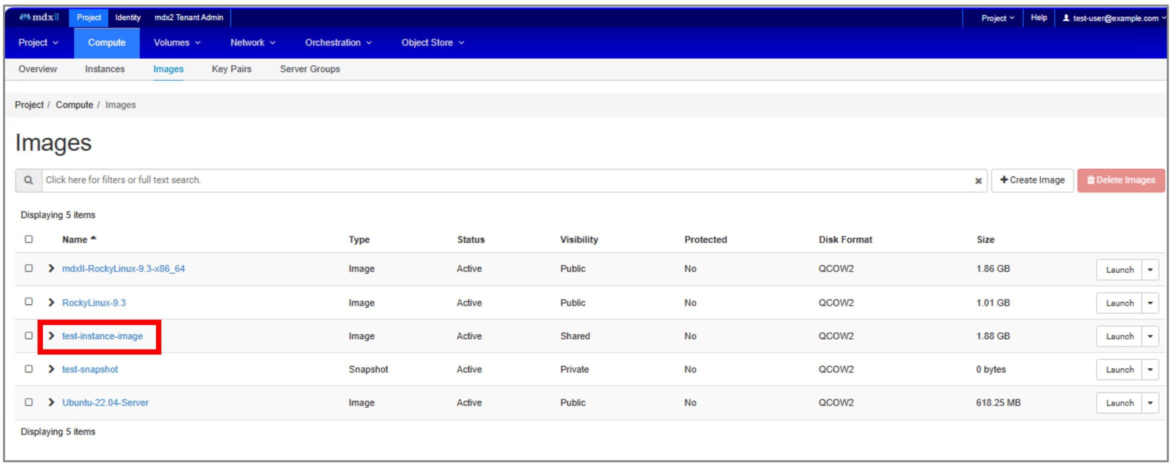
Images

Displaying 5 items

	Name	Type	Status	Visibility	Protected	Disk Format	Size	
□	mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch
□	RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch
□	test-instance-image	Image	Active	Shared	No	QCOW2	1.88 GB	Launch
□	test-snapshot	Snapshot	Active	Private	No	QCOW2	0 bytes	Launch
□	Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch

Displaying 5 items

(14) Confirm that the uploaded image has been created.



Images

Displaying 5 items

	Name	Type	Status	Visibility	Protected	Disk Format	Size	
□	mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch
□	RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch
□	test-instance-image	Image	Active	Shared	No	QCOW2	1.88 GB	Launch
□	test-snapshot	Snapshot	Active	Private	No	QCOW2	0 bytes	Launch
□	Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch

Displaying 5 items

This completes the steps to create an image from a virtual machine.

Also, there is no problem in deleting the snapshots and volumes used in the image file creation process if they are no longer needed.

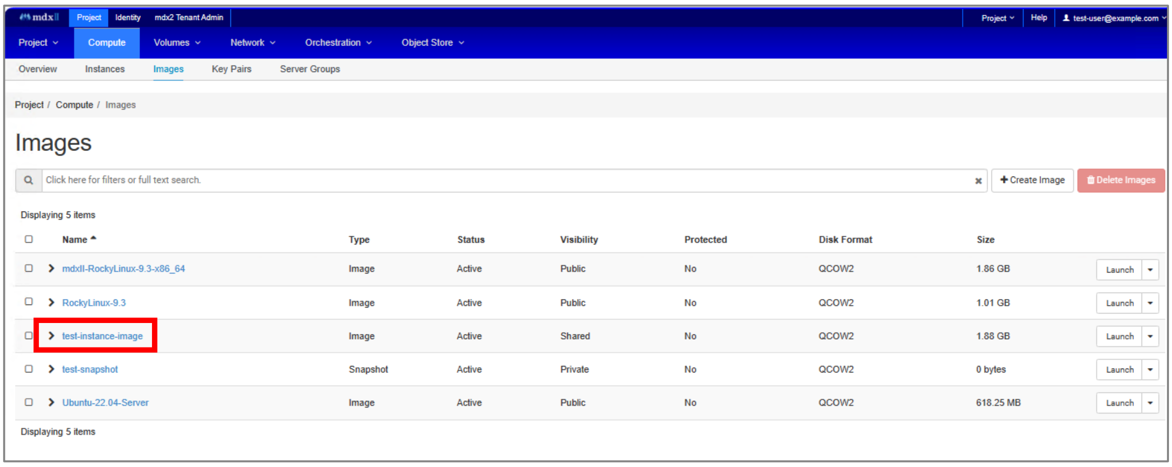
5.1.10. Downloading image files

Image files cannot be downloaded from the user portal GUI screen. To download an image file, use OpenStack API access.

A local password is required to access the OpenStack API. If you are using a GakuNin account, a local password will not be set when applying for a project. If you wish to download the image file, please email the system administrator to request a local password.

Please download the image file using OpenStack API access from your own device. Below are the steps to download from a Linux environment.

(1) Click the image name of the image you want to download on the image screen of the user portal.



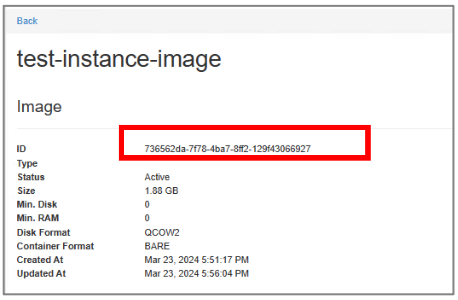
Images

Displaying 5 items

	Name	Type	Status	Visibility	Protected	Disk Format	Size	
□	mdxII-RockyLinux-9.3-x86_64	Image	Active	Public	No	QCOW2	1.86 GB	Launch
□	RockyLinux-9.3	Image	Active	Public	No	QCOW2	1.01 GB	Launch
□	test-instance-image	Image	Active	Shared	No	QCOW2	1.88 GB	Launch
□	test-snapshot	Snapshot	Active	Private	No	QCOW2	0 bytes	Launch
□	Ubuntu-22.04-Server	Image	Active	Public	No	QCOW2	618.25 MB	Launch

Displaying 5 items

(2) Make a note of the image ID displayed on the displayed image screen.



test-instance-image

Image

ID	736562da-7f78-4ba7-8ff2-129f43066927
Type	
Status	Active
Size	1.88 GB
Min. Disk	0
Min. RAM	0
Disk Format	QCOW2
Container Format	BARE
Created At	Mar 23, 2024 5:51:17 PM
Updated At	Mar 23, 2024 5:56:04 PM

(3) Use curl command to access OpenStack API. If the curl package is not installed on your device, install it.

(4) Create the authentication file required for OpenStack API access.

*<Username> is displayed at the top right of the user portal screen, not the GakuNin account username.

This will be your username.

*<Local password> is not the password of your GakuNin account, but the password provided by the system administrator at the time of application The password will be issued by.

```
  $ 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) Access the OpenStack API using the curl command and save the output results.

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

(6) Check and copy the authentication token information (bold) from the saved output result.

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

(7) Check and copy the authentication token information (bold) from the saved output result.

```
  $ token="XXXXXXXXXXXXX”
```

(8) Access the API using the curl command and download the image file.
*For <Image ID>, enter the ID of the image file you wrote down.
*<Download file name> specifies any image file name (test.qcow2, etc.).

```
  $ curl -i -X GET -H "X-Auth-Token: $token" https://portal.osaka.mdx.jp:13292/v2/images/
<Image ID>/file --output <Download File Name>
```