

# 統合開発クラウド スタートアップ

2021 年 12 月

株式会社 NTT データ

システム技術本部

生産技術部

---

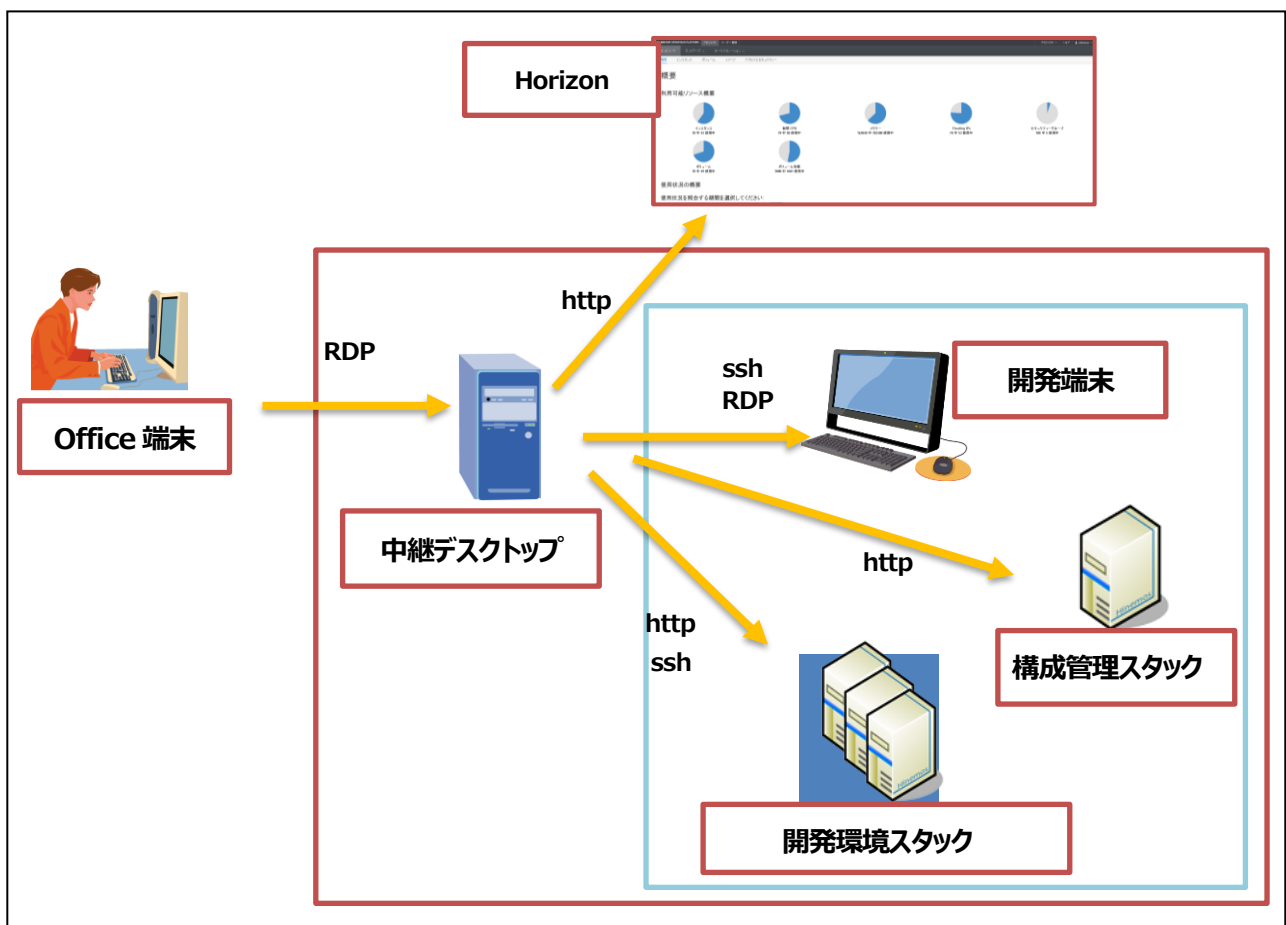
# 目次

1. はじめに.....	2
1-1. 目的 .....	2
1-2. 全体フロー .....	3
1-3. 用語集.....	4
2. 事前確認 .....	6
2-1. ダッシュボードにログイン .....	6
2-2. 中継デスクトップの IP アドレス確認 .....	9
3. 環境にアクセス .....	11
3-1. 中継デスクトップにログイン .....	12
3-2. OpenStack の Horizon にアクセス .....	17
3-3. セキュリティーグループの作成 .....	19
3-4. 端末(Windows10)の作成 - ①ボリューム作成 .....	26
3-5. 端末(Windows10)の作成 - ②インスタンスの作成 .....	28
3-6. OpenStack 上の端末にアクセス.....	34
4. 開発環境構築例.....	37
4-1. キーペアを作成する.....	37
4-2. 開発端末 (RHEL61_64bit) の作成 - ①ボリューム作成.....	40
4-3. 開発端末 (RHEL61_64bit) の作成 - ②インスタンス作成.....	43
4-4. 構成管理スタック(Puppet)の作成.....	48
4-5. 開発環境スタック(WEB、DB、AP サーバ)の作成 .....	53
4-6. 開発環境へのアクセス - ①スタックの IP アドレス確認.....	57
4-7. 開発環境へのアクセス - ②Puppet 管理画面アクセス .....	59
4-8. 開発環境へのアクセス - ③AP サーバアクセス.....	61
5. その他.....	65
5-1. アクセスユーザの追加について .....	65
5-2. 外部インターネット接続について .....	65
5-3. Office 端末とのデータのやりとりについて .....	66
5-4. OpenStack の容量追加について.....	66
5-5. その他のスタック紹介 .....	67
5-6. 統合開発クラウドよろず相談窓口.....	67

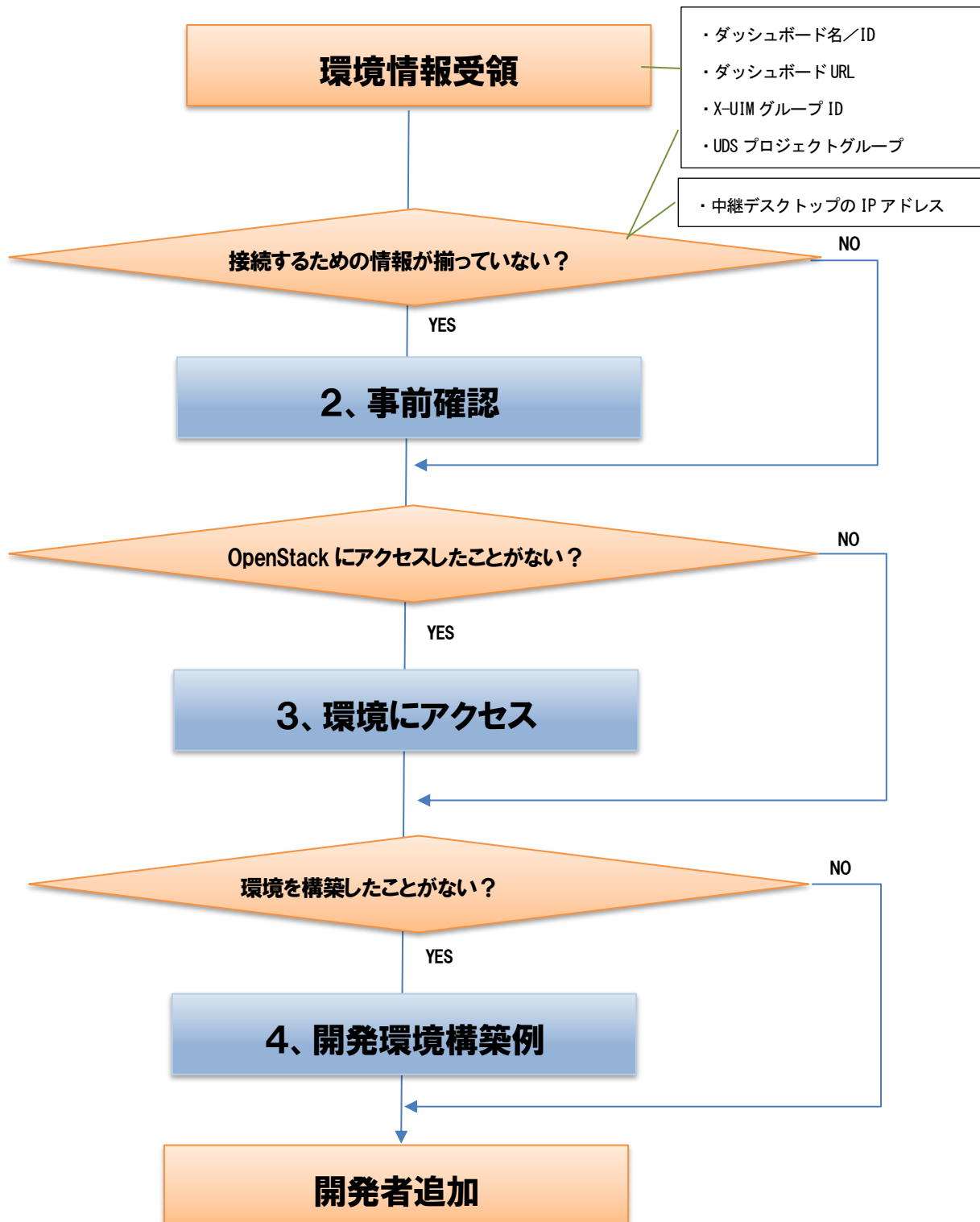
# 1. はじめに

## 1-1. 目的

本資料は、案件の担当者が自社の Office 端末から「統合開発クラウド」上の OpenStack テナントで、通常の端末作成と、デリバリ機能を用いて開発環境を構築し、アクセスするまでの手順を記載する。



## 1-2. 全体フロー



## 1-3. 用語集

統合開発クラウドの基本用語を以下に示す。

表 1-3-1. 基本用語

項目	説明
案件	統合開発クラウドの基本的な提供単位。案件ごとに独立したダッシュボードが利用できる。
開発ダッシュボード (ダッシュボード)	案件ごとに作成する、統合開発クラウドのサービス利用時の入り口。
ダッシュボード管理者	開発ダッシュボードを管理者権限で利用できる管理者。開発ダッシュボードから各サービスの利用を申請できる。通常のプロジェクトにおけるインフラチームのリーダやそれに準ずる役割が相当する。
ダッシュボード利用者	開発ダッシュボードを利用者権限で利用できる利用者。開発ダッシュボード経由で各案件のダッシュボード情報を参照できる。構築済みのサーバ環境に直接 SSH や RDP 等でログインする作業、すなわち通常のプロジェクトの開発や試験の作業担当者が相当する。
テナント管理者	プロジェクト環境の統合開発クラウドリソースの管理者。OpenStack 管理画面を利用可能。
テナント利用者	本サービス上のプロジェクト環境の利用者。
スタック構成	本サービス上でシステムが動作する環境の単位。各プロジェクトにおいては試験環境の 1 面に相当。
テナント	プロジェクトが任意の設定で利用可能な専用の空間。テナント間のネットワークはセグメント分割されている。
社内ネットワーク	各社が保有し運用管理する各社の業務の遂行を目的としたネットワークをいう。 社内ネットワークには、以下が含まれる。 <ul style="list-style-type: none"><li>・ 役員、社員、協働者が社内システムやインターネットのサービスを利用するためのネットワーク</li><li>・ 社員、協働者がシステム開発を行うためのネットワーク（開発ネットワーク）</li><li>・ 社外ネットワークとのすべての接続点 等</li></ul>
開発ネットワーク	社内ネットワークのうち、社員、協働者がシステム開発を行うためのネットワークをいう。
社外ネットワーク	社内ネットワークに含まれないネットワークをいう。 社外ネットワークには、以下が含まれる。 <ul style="list-style-type: none"><li>・ 社内ネットワークへのリモートアクセスするための電話、ISDN 網</li><li>・ インターネット</li><li>・ 他社ネットワーク</li></ul>
ETRANPOT (エトランポット)	株式会社 NTT データが運用する、NTT データ・NTT データグループ会社及びインターネット上で利用するユーザ間における、セキュアなファイル転送システム。



## 2. 事前確認

ここでは、受領した情報からダッシュボードにログインおよび中継デスクトップサーバの IP アドレスを確認する手順を説明いたします。

### 2-1. ダッシュボードにログイン

- 1、社内ネットワークの PC (Office 用端末) のブラウザ(Internet Explorer)で「開発ダッシュボードログイン」画面を開く。

#### 注釈

開発ダッシュボードログイン画面の URL：  
【[https://udc-dashboard.x-network.jp/dsbd/user\\_login](https://udc-dashboard.x-network.jp/dsbd/user_login)】

#### 注意

「利用可能なダッシュボードが存在しません」が表示された場合は、別のアカウントでログインしている可能性があります。  
1 度すべてのブラウザを閉じていただき、再度ログイン画面から該当のアカウントを入力してください。

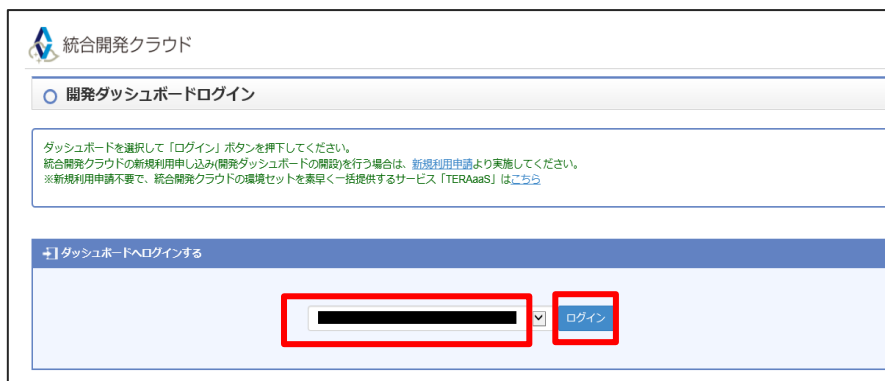
※ログイン画面が表示された場合は、表 2-1-1 の内容を入力して「Login」ボタンをクリックする。

表 2-1-1. ログイン画面入力項目

項番	名称	X-UIM プロジェクトグループ(G-UIM)	X-UIM プロジェクトグループ(X-UIM)
1	ログイン ID (利用者 ID)	・G-UIM アカウント	・X-UIM アカウント CURE 申請で入手した ID (U から始まる 7 桁) を入力してください。
2	会社識別子	個社の会社識別子	nttdata
3	パスワード	G-UIM アカウントのパスワード	X-UIM アカウントのパスワード



## 2、「開発ダッシュボードへログインする」内の「ダッシュボードのプルダウンリスト」から該当のダッシュボードを選択し、「ログイン」ボタンを押下する。



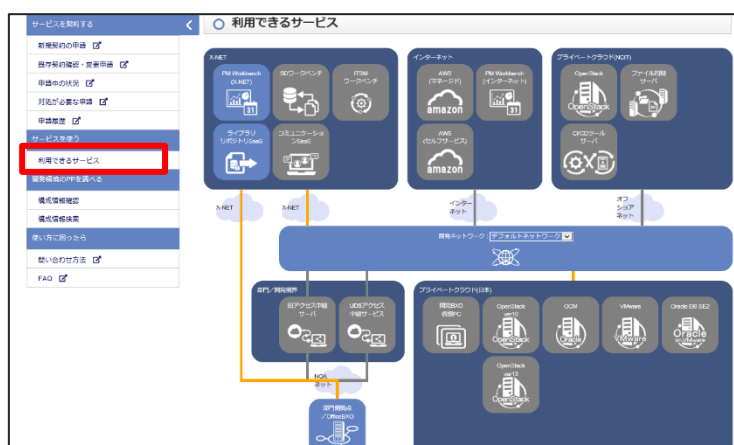
## 3、「ダッシュボード」が表示されることを確認する。



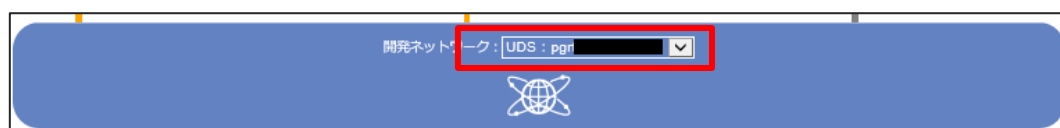
請求年月	利用期間	請求額	ステータス
2021年1月	1/1~1/31		金額未確定

## 2-2. 中継デスクトップの IP アドレス確認

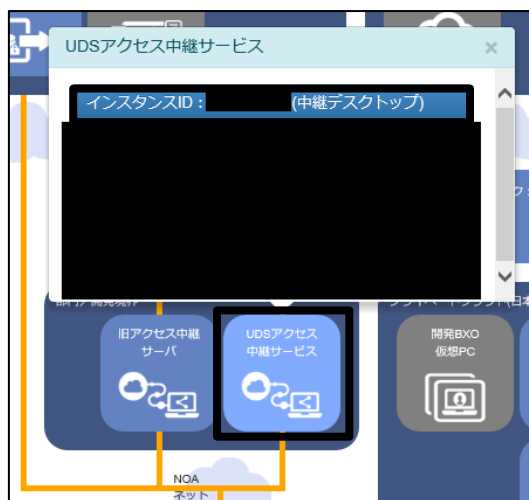
1、「ダッシュボード」内の「サービスを使う」にある「利用できるサービス」を押下する。



2、「開発ネットワーク」のプルダウンを「デフォルトネットワーク」から「UDS:pgrgrp 会社識別子 0000」に変更する。



3、「部門／開発境界」の「UDS アクセス中継サービス」を押下し、「インスタンス ID (中継デスクトップ)」を押下する。



4、アクセス情報(NOA ネット側)の IP アドレス(中継デスクトップのアドレス)を確認し、「×」で閉じる。

インスタンスID: (中継デスクトップ)

認証・認可情報

RDPログイン可能グループ

監査ログ参照可能グループ

※ご自身が当該グループに所属しているかは、WorkflowSystem(グループ管理者検索)から確認してください。  
※グループメンバーの追加は、グループの管理者または副管理者にて、WorkflowSystem(申請管理)より「新規申請」プロジェクトグループメンバー(追加申請)を選択して申請してください。

利用区分	ログインID	パスワード
NTTデータ社員	JAPAN氏名コード	X-UIMで設定
NTTデータ協働者	JAPANU*****	X-UIMで設定
社外ユーザ	GUESTlg*****	WorkflowSystemで設定

アクセス情報(NOAネット側)

RDPアドレス 10.201.0.18

### 3. 環境にアクセス

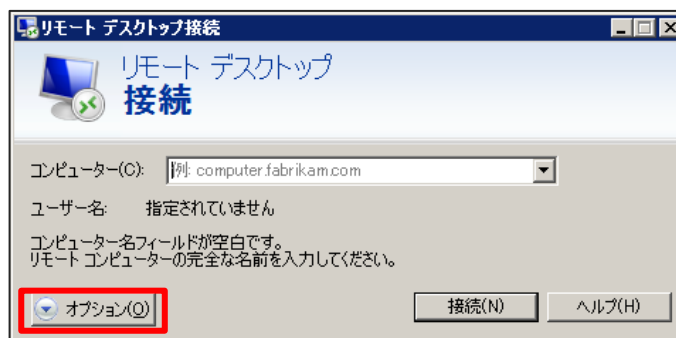
---

ここでは中継デスクトップの IP アドレスが必要となります。必ず「2-2. 中継デスクトップの IP アドレス確認」の手順でご確認をお願いいたします。

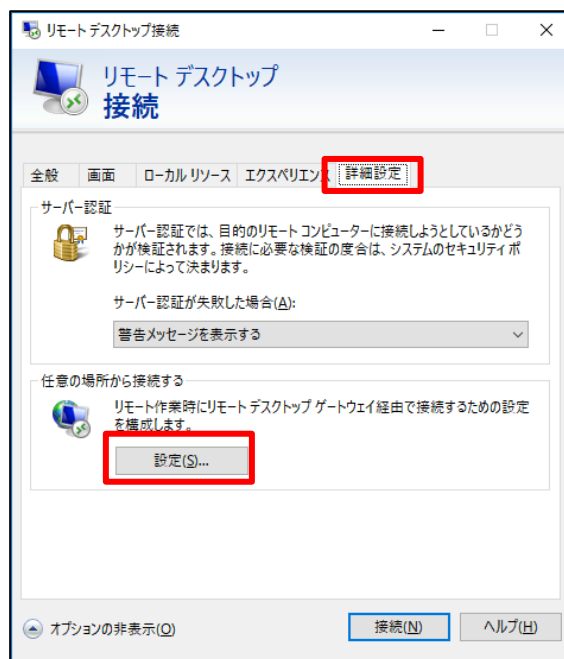
## 3-1. 中継デスクトップにログイン

---

- 1、社内ネットワークの PC (Office 用端末) で「リモートデスクトップ接続」をダブルクリックし、「オプション」を押下する。



- 2、詳細設定タブをクリックし、「設定」を押下する。



### 3、接続設定で表 3-1-2 の内容を設定し、「OK」を押下する。

RD ゲートウェイ サーバー設定

リモート デスクトップ  
接続

接続設定

☐ 自動的に RD ゲートウェイ サーバーの設定を検出する(A)

☒ 次の RD ゲートウェイ サーバー設定を使用する(U):

サーバー名(S): harsgg0001.x-network.jp

ログオン方法(L): 後で選択できるようにする

☒ ローカルアドレスには RD ゲートウェイ サーバーを使用しない(B)

☐ RD ゲートウェイ サーバーを使用しない(D)

ログオン設定

ユーザー名: 指定されていません

この RD ゲートウェイ サーバーに接続するときは資格情報が要求されます。

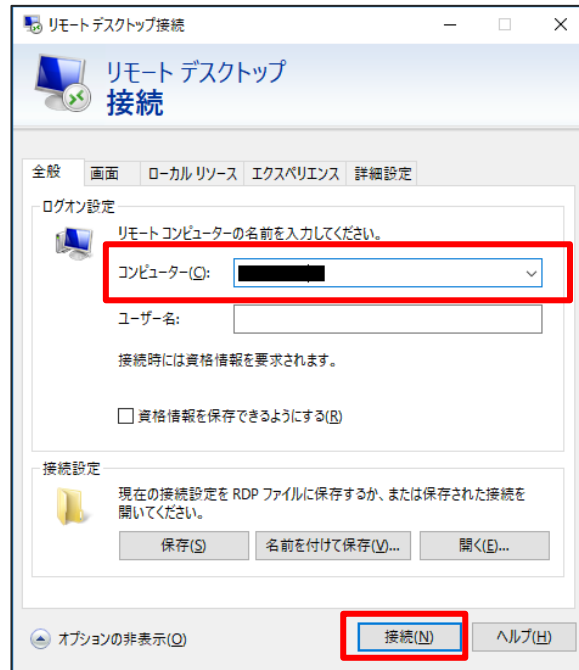
☐ リモート コンピューターに RD ゲートウェイ の資格情報を使用する(E)

OK キャンセル

表 3-1-2 設定内容

項番	名称	選択／入力項目の説明
1	次の RD ゲートウェイサーバー設定を使用する	チェックをつける
2	サーバ名	以下のいずれかを入力する harsgg0001.x-network.jp harsgg0002.x-network.jp harsgg0003.x-network.jp harsgg0004.x-network.jp harsgg0005.x-network.jp
3	ローカルアドレスには RD ゲートウェイサーバーを使用しない	チェックをはずす

4、全般タブから、対象の中継デスクトップ(RDP) アドレスを入力し、「接続」を押下する。



5、RD ゲートウェイ サーバーの資格情報の入力画面が表示されるので、表 3-1-3、または表 3-1-4 の情報を入力し、「OK」を押下する。

表 3-1-3 入力内容(UDS プロジェクトグループを X-UIM で作成していた場合)

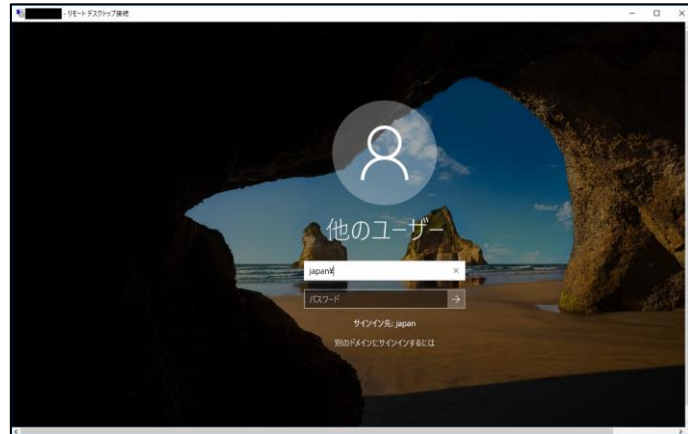
項番	名称	入力項目の説明
1	ユーザー名	japan¥ <X-UIM ログイン ID> 入力例： japan¥U123456
2	パスワード	X-UIM アカウントのパスワード

表 3-1-4 入力内容(UDS プロジェクトグループを G-UIM で作成していた場合)

項番	名称	入力項目の説明
1	ユーザー名	japan¥ <G-UIM ログイン ID> _ <会社識別子> 入力例： japan¥G123456_nttdxxxx
2	パスワード	G-UIM アカウントのパスワード



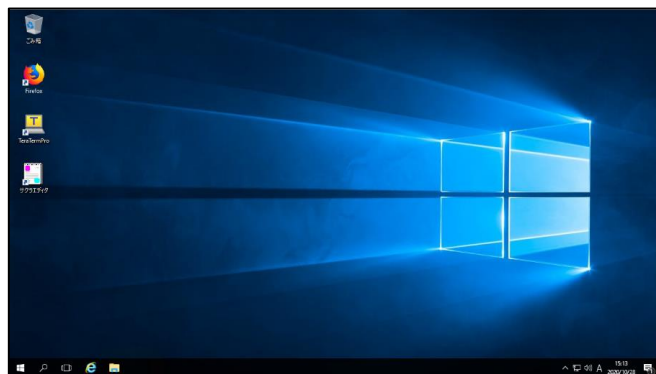
6、中継デスクトップの「ログイン画面」で、表 3-1-3、または表 3-1-4 の情報を入力する。



#### 注釈

UDS グループで作成したユーザ (gt\*\*) でログインする場合は、「guest¥gt\*\*」を入力してください。

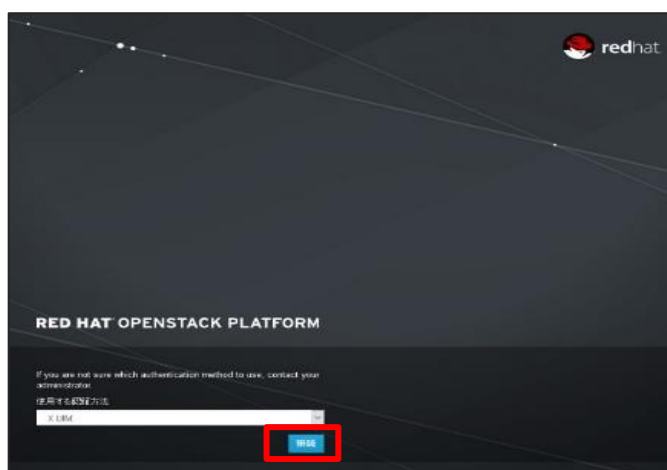
7、「Windows のデスクトップ」画面が表示され、中継デスクトップにログインしたことを確認する。



## 3-2. OpenStack の Horizon にアクセス

---

1、Firefox を起動し、受領した「ダッシュボード URL」を記述し、「OpenStack 管理ダッシュボードのログイン画面」を開き、「接続」ボタンを押下する。



### 注釈

OpenStack 管理ダッシュボードがセッションタイムアウトした際にも上記画面に切り替わるため、再接続する場合は「接続」ボタンを押下してください。

### 注意

下記は、表示が消えるまで「キャンセル」ボタンを押下してください。

ユーザー名とパスワードを入力してください

?

プロキシ moz-proxy://xproxy.nttdata.co.jp:8080 がユーザー名とパスワードを要求しています。サイトからのメッセージ: "McAfee Web Gateway"

ユーザー名:

パスワード:

☐ パスワードマネージャーにこのパスワードを保存する。

OK

キャンセル

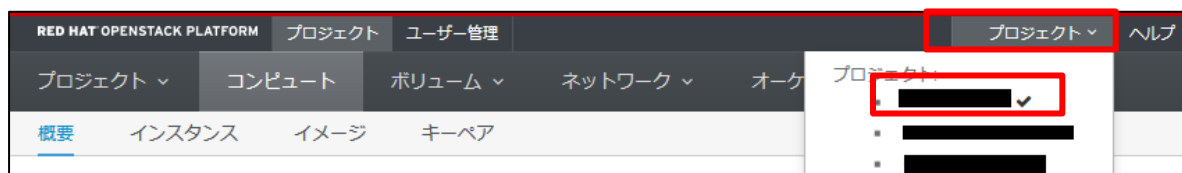
## 2、表 3-2-1 の内容を記述して「Login」ボタンをクリックする。

表 3-2-1 ログイン時の入力内容

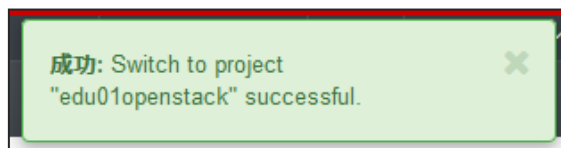
項番	名称	X-UIM プロジェクトグループ(G-UIM)	X-UIM プロジェクトグループ(X-UIM)
1	ログイン ID (利用者 ID)	・G-UIM アカウント	・X-UIM アカウント CURE 申請で入手した ID (U から始まる 7 桁) を入力してください。
2	会社識別子	個社の会社識別子	nttdata
3	パスワード	G-UIM アカウントのパスワード	X-UIM アカウントのパスワード

## 3、画面右上の「プロジェクト」を押下し、「該当の OpenStack テナント識別子」に「✓」が付いていることを確認する。

「該当の OpenStack テナント識別子」に「✓」がついていない場合には、  
「該当の OpenStack テナント識別子」を押下し、プロジェクト(テナント)を移動する。



下記の画面がサイト右上に表示されるのを確認する。



### 注釈

失敗と表示された場合はもう一度「該当の OpenStack テナント識別子」を押下してください。

### 3-3. セキュリティグループの作成

1、ダッシュボード上部タブより、「ネットワーク」→「セキュリティグループ」を押下する。



2、「セキュリティグループの作成」ボタンを押下する。



3、「セキュリティグループの作成」画面で「名前」に表 3-3-1 の内容を入力し、「セキュリティグループの作成」ボタンを押下する。

RED HAT OPENSTACK PLATFORM プロジェクト ユーザー管理 プロジェクト ヘルプ

### セキュリティグループの作成

名前 \*

tenant-security-group-all\_open

説明:

セキュリティグループは、VM のネットワークインターフェースに適用される IP フィルタリングルールの集合です。セキュリティグループ作成後に、作成したセキュリティグループにルールを追加することができます。

説明

取り消し セキュリティグループの作成

group	name	id	rules
default	default	41302000-0504-4243-8411-0c1b6277300a	
tenant-security-group-all_open	tenant-security-group-all_open	59b131fb-d5ce-4197-ad88-160ad8df06ec	

表 3-3-1 入力内容

項番	名称	値
1	名前	tenant-security-group-all_open

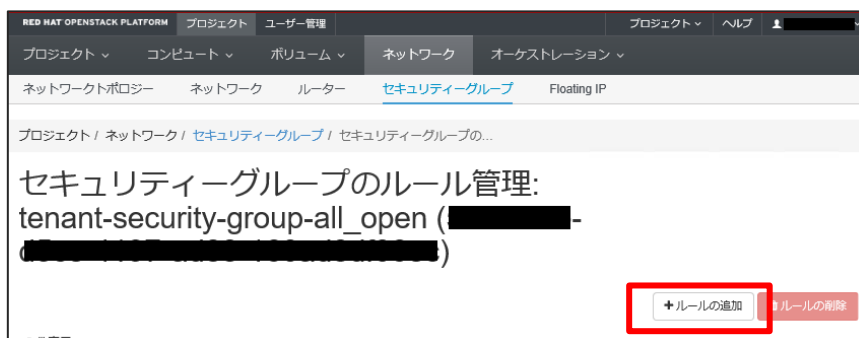
#### 注釈

ここではすべてのアクセスを許可する設定でセキュリティグループを作成いたします。  
作成しない場合、デフォルトがインスタンスに適用されますが、デフォルトでは中継デスクトップからのアクセスも不可となるため、必ずセキュリティグループの作成とインスタンスへの設定をお願いいたします。

4、「アクセスとセキュリティ」画面で「tenant-security-group-all\_open」が追加されたことを確認し、「ルールの管理」を押下する。



5、「セキュリティーグループのルール管理」画面で「+ルール追加」ボタンを押下する。



6、「ルールを追加」画面で表 3-3-2 のとおりに選択し、「追加」ボタンを押下する。

**ルール**

ALL TCP

方向

受信

接続相手

CIDR

0.0.0.0/0

説明:

ルールは、セキュリティグループに割り当てられたインスタンスに対して許可する通信を定義します。セキュリティグループルールは3つの部分から構成されます。

ルール: 希望のルールテンプレートを指定するか、カスタムルールを設定することができます。カスタムルールにはTCP、UDP、ICMPルールがあります。

開放するポート/ポート範囲: TCP および UDP の場合、ポート番号またはポート範囲を選択できます。「ポート範囲」オプションを選択すると、範囲の開始ポートおよび終了ポートを空白区切りで指定できます。ICMP の場合、ICMP タイプおよびコードを空白区切りで指定します。

接続相手: このルールにより許可される通信のソースを指定する必要があります。IP アドレスブロック (CIDR) またはソースグループ (セキュリティグループ) で指定します。接続元としてセキュリティグループを選択すると、そのセキュリティグループに所属するすべてのインスタンスが、このルールが適用されるすべてのインスタンスにアクセスできるようになります。

取り消し 追加

表 3-3-2 選択内容

項番	項目名	選択値
1	ルール	ALL TCP
2	方向	受信
3	接続相手	CIDR
4	CIDR	0.0.0.0/0

7、「セキュリティグループのルール管理」画面で、ルールが追加されたことを確認する。



8、「セキュリティグループのルール管理」画面で、「ルールの追加」ボタンを押下する。





9、「ルールの追加」画面で表 3-3-3 のとおりに選択し、「追加」ボタンを押下する

ルール \*

ALL ICMP

方向

受信

接続相手 \* ⓘ

CIDR

CIDR ⓘ

0.0.0.0/0

説明:

ルールは、セキュリティグループに割り当てられたインスタンスに対して許可する通信を定義します。セキュリティグループルールは 3 つの部分から構成されます:  
  
ルール: 希望のルールテンプレートを指定するか、カスタムルールを設定することができます。カスタムルールには TCP、UDP、ICMP ルールがあります。  
  
開放するポート/ポート範囲: TCP および UDP の場合、ポート番号またはポート範囲を選択できます。「ポート範囲」オプションを選択すると、範囲の開始ポートおよび終了ポートを空白区切りで指定できます。ICMP の場合、ICMP タイプおよびコードを空白区切りで指定します。  
  
接続相手: このルールにより許可される通信のソースを指定する必要があります。IP アドレスブロック (CIDR) またはソースグループ (セキュリティグループ) で指定します。接続元としてセキュリティグループを選択すると、そのセキュリティグループに所属するすべてのインスタンスが、このルールが適用されるすべてのインスタンスにアクセスできるようになります。

取り消し

追加

表 3-3-3 選択内容

項番	項目名	選択値
1	ルール	ALL ICMP
2	方向	受信
3	接続相手	CIDR
4	CIDR	0.0.0.0/0

注釈

ルールは、デフォルトが拒否のため、許可するものを作成します。

## 10、「セキュリティグループのルール管理」画面で、ルールが追加されたことを確認する。



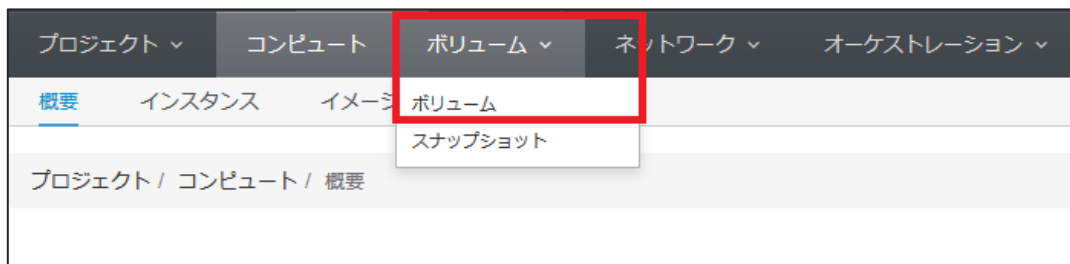
### 注釈

誤って作成したルールは「ルールの削除」ボタンで削除することが可能です。

### 3-4. 端末(Windows10)の作成 - ①ボリューム作成

---

1、「ボリューム」→「ボリューム」を選択する。



2、「+ボリュームの作成」ボタンを押下する。



3、「ボリュームの作成」画面で、表 3-4-1 のとおりに入力し、「ボリュームの作成」ボタンを押下する。

ボリュームの作成

ボリューム名  
vol-win10

説明  
説明

ボリュームソース  
イメージ

イメージをソースとして使用する  
Win10ProVer1909\_64bit\_20191118 (4.8 GB)

種類  
AZ01-STG01

サイズ (GiB)  
32

アベイラビリティゾーン  
AZ01

説明:  
ボリュームは、インスタンスに接続できるブロックデバイスです。

ボリューム種別の説明:  
AZ01-STG01  
説明がありません。

ボリュームの上限  
合計ギガバイト 0 / 1000 GB 使用中  
ボリューム数 0 / 10 使用中

取り消し ボリュームの作成

表 3-4-1 入力内容

項番	項目名	値
1	ボリューム名	vol-win10
2	ボリュームソース	イメージ
3	イメージをソースとして使用する	Win10ProVer1909_64Bit_20191118 (4.8GB)
4	種類	AZ01-STG01
5	容量 (GB)	5→32
6	アベイラビリティゾーン	AZ01

4、「ステータス」が「利用可能」と表示されることを確認する。

RED HAT OPENSTACK PLATFORMプロジェクトユーザー管理プロジェクトヘルプ

プロジェクトコンピュートボリュームネットワークオークストレーション

ボリュームスナップショット

プロジェクト / ボリューム / ボリューム

ボリューム

フィルター

+

ボリュームの作成

≡

設定の受理

🗑

ボリュームの削除

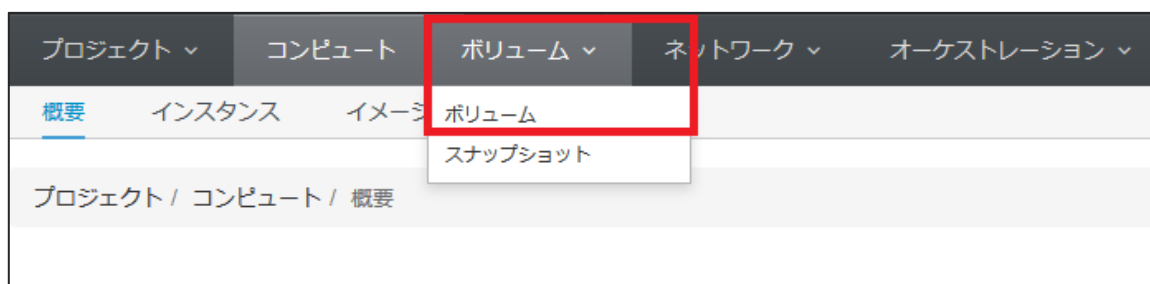
1 件表示

<input type="checkbox"/>	名前	説明	サイズ	ステータス	種類	接続先	アベイラビリティゾーン	起動可能	暗号化	アクション
<input type="checkbox"/>	vol-win10	-	32GiB	利用可能	AZ01-STG01	AZ01	はい	いいえ	ボリュームの編集	

1 件表示

## 3-5. 端末(Windows10)の作成 - ②インスタンスの作成

1、「ボリューム」→「ボリューム」を押下する。



2、「アクション」項目の「 ▼ 」を押下し、「 インスタンスとして起動 」を選択する。



### 注釈

「ステータス」が「利用可能」と表示されていることを確認してから、インスタンスを起動してください。

3、「インスタンスの起動」画面で、表 3-5-1 のとおりに「インスタンス名」を入力する。

表 3-5-1 入力内容

項番	項目名	値
1	インスタンス名	Win10

4、「フレーバー」を押下して切り替え、「2cpu4gb」の「↑」を押下し「割り当て済み」に追加する。

## 5、「ネットワーク」タブを選択し、「利用可能ネットワーク」にあるネットワーク「provider」が「割り当て済み」にあることを確認する。

インスタンスの起動

詳細

ソース

フレイバー

**ネットワーク**

ネットワークのポート

セキュリティグループ

キーペア

設定

サーバーグループ

スケジューラーヒント

メタデータ

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 ① 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	共有	管理状態	ステータス
1 > provider	いいえ	動作中	稼働中

▼ 利用可能 ① ネットワークを少なくとも1つ選択してください。

以下の利用可能なアイテムから1つ選択してください。

ネットワーク	共有	管理状態	ステータス
利用できるアイテムがありません。			

✕ 取り消し

< 戻る 次へ >

インスタンスの起動

※割り当てられていない場合は、「利用可能ネットワーク」にあるネットワーク「provider」を追加する。

インスタンスの起動

詳細

ソース

フレイバー

**ネットワーク\***

ネットワークのポート

セキュリティグループ

キーペア

設定

サーバーグループ

スケジューラーヒント

メタデータ

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	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 ① ネットワークを少なくとも1つ選択してください。

以下の利用可能なアイテムから1つ選択してください。

ネットワーク	共有	管理状態	ステータス
> provider	いいえ	動作中	稼働中

✕ 取り消し

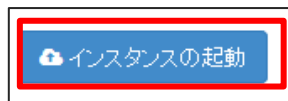
< 戻る 次へ >

インスタンスの起動

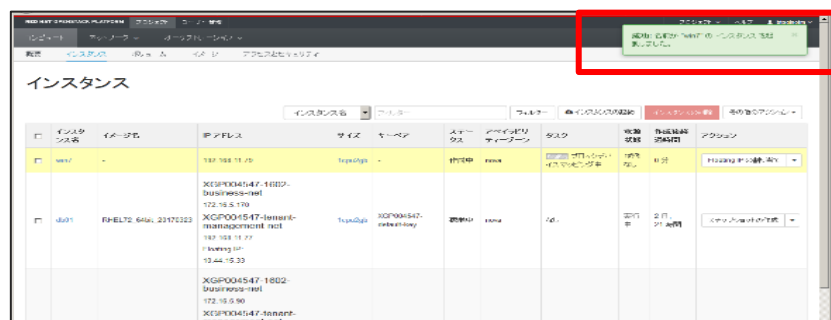
6、「セキュリティグループ」タブを押下し、「tenant-security-group-all\_open」の「↑」を押下する。



7、画面右下の「インスタンスの起動」を押下する。



8、ウェブブラウザの右上部に、下図のようなポップアップ画面が表示されることを確認する。※すぐに表示は消えます。

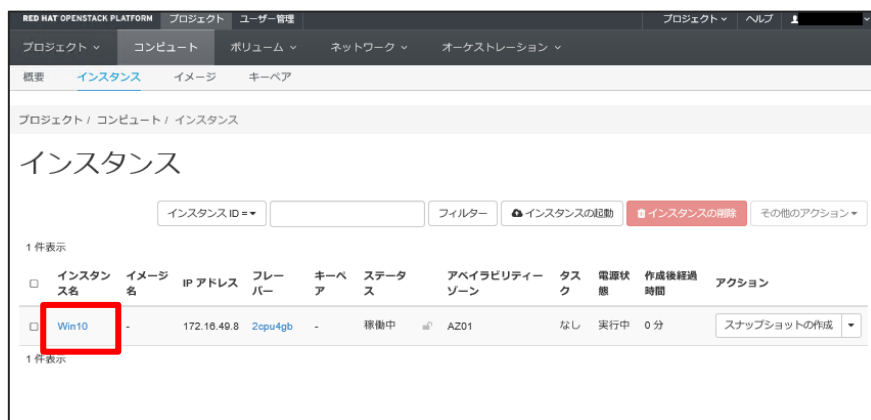




9、「コンピュート」→「インスタンス」を選択し、作成したインスタンスのステータスが「稼働中」であることを確認する。



10、インスタンス名「Win10」を押下する。



11、「ログ」タブを押下する。



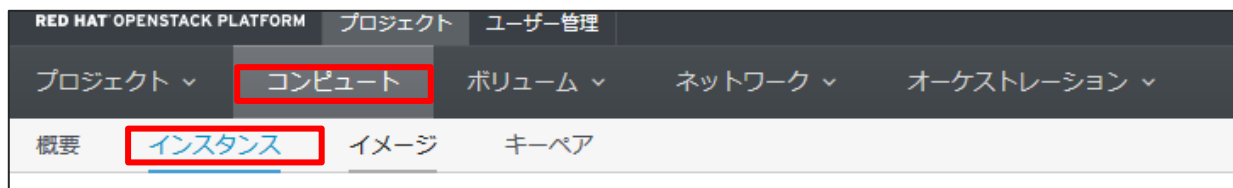
## 12、ログの最下部に「Stopping service cloudbase-init stop\_service」のメッセージが出力されていることを確認する。

```
2016-10-24 15:26:58.629 1784 INFO cloudbaseinit.plugins.windows.winmcertificateauth [-] WinRM certificate authentication cannot be config
2016-10-24 15:26:58.629 1784 INFO cloudbaseinit.init [-] Executing plugin 'LocalScriptsPlugin'
2016-10-24 15:26:58.629 1784 INFO cloudbaseinit.init [-] Plugins execution done
2016-10-24 15:26:58.629 1784 INFO cloudbaseinit.init [-] Stopping Cloudbase-Init service
2016-10-24 15:27:01.645 1784 DEBUG cloudbaseinit.osutils.windows [-] Stopping service cloudbase-init stop_service c:\program files\cloudba
¥cloudbaseinit¥osutils¥windows.py:715
```

### 注釈

Windows10 インスタンスの完成は、3分程度時間が必要なため、構築直後に下記のログは表示されません。

## 13、「コンピュート」→「インスタンス」を押下する。

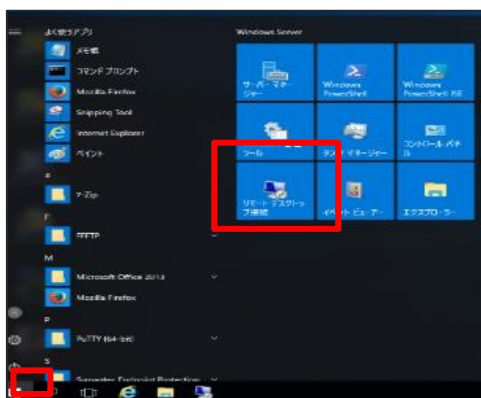


## 14、「インスタンス名」が「win10」の「IP アドレス」を確認する。



## 3-6. OpenStack 上の端末にアクセス

1、「中継デスクトップ」上の「デスクトップ」画面で「Windows キー」を押下し、「リモートデスクトップ接続」を押下する。



2、「オプションの表示」を押下し、表 3-6-1 のとおりに入力後「接続」ボタンを押下する。

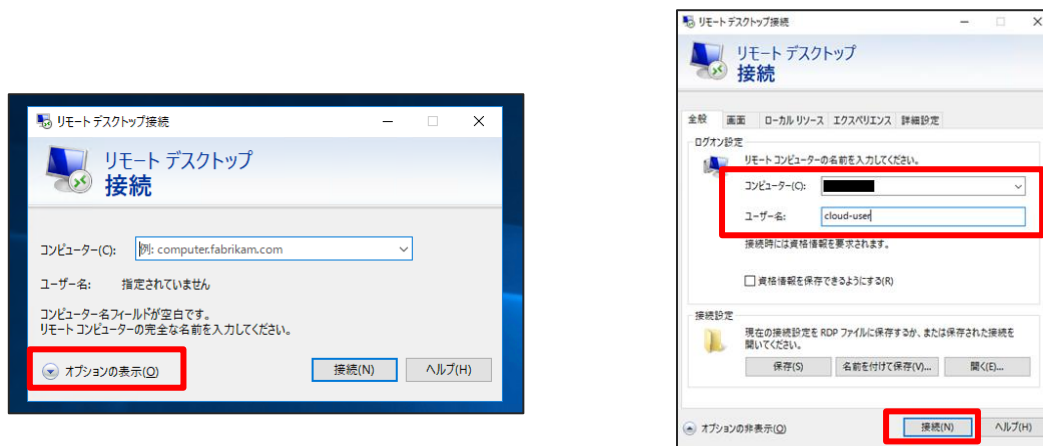


表 3-6-1 入力内容

項番	名称	値
1	コンピューター	Win10 の IP アドレス
2	ユーザー名	cloud-user

### 3、表 3-6-2 のとおりにパスワードを入力し、「OK」ボタンを押下する。

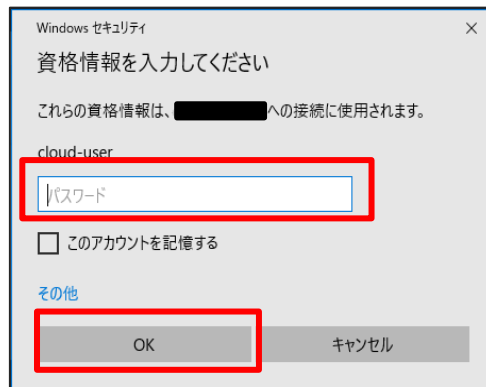
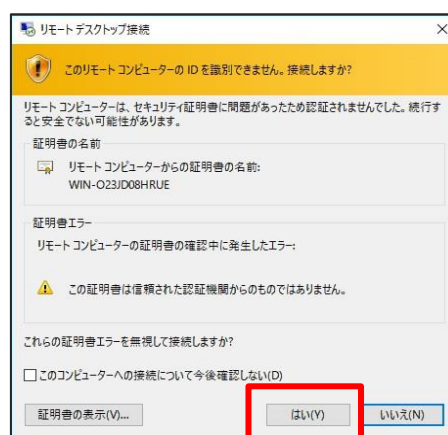


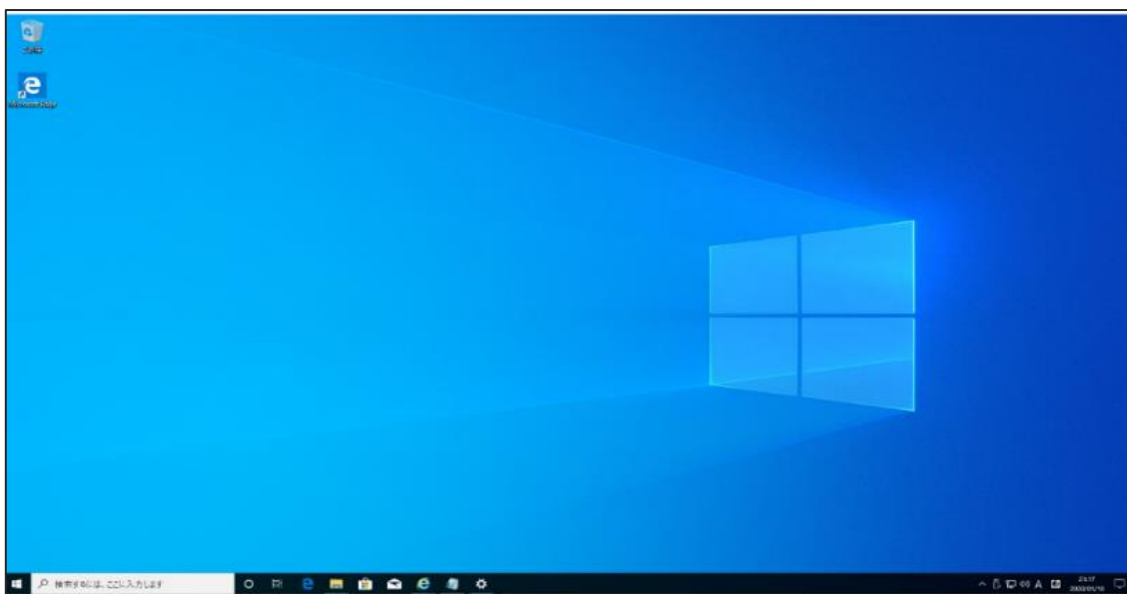
表 3-6-2 入力内容

項番	名称	値
1	パスワード	Nttdata0

### 4、「リモートデスクトップ接続」画面で、「はい」を押下する。



5、「Windows10 のデスクトップ」画面が表示され、開発端末にログインしたことを確認する。



# 4. 開発環境構築例

ここでは、RHEL の開発端末およびデリバリ機能を利用して構成管理と開発環境スタックによる構築、アクセスする手順を説明いたします。

## 4-1. キーペアを作成する

1、「コンピュート」→「キーペア」→「+キーペアの作成」を押下する。



2、「キーペア名」に以下の値を入力し「キーペアの作成」ボタンを押下する。

キーペアの作成

キーペア名\*

opst-self-key

× 取り消し

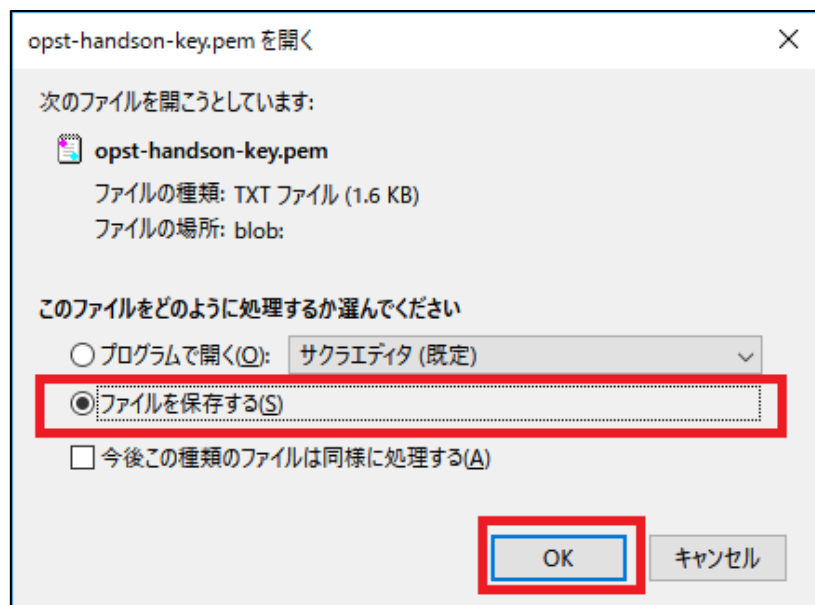
+ キーペアの作成

キーペアは、インスタンスの起動後にそのインスタンスにログインするために使用します。自分で認識できるキーペア名を付けてください。名前に使用できるのは、英数字、空白文字、ダッシュのみです。

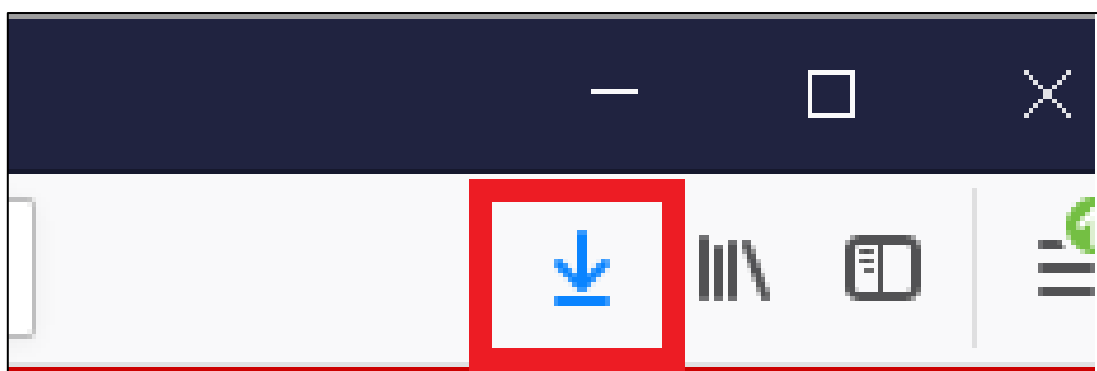
表 4-1-1 入力内容

項目	値
キーペア名	opst-self-key

3、「ファイルを保存する」を選択し、「OK」ボタンを押下する。



4、ウェブブラウザ右上ダウンロードボタンより、キーペアの格納先を確認する。



5、「コンピュート」→「キーペア」と押下し、「キーペア名」に「opst-self-key」が追加されたことを確認する。

The screenshot shows the AWS Management Console interface. At the top, there are tabs for 'プロジェクト' (Project), 'コンピュート' (Compute), 'ボリューム' (Volumes), 'ネットワーク' (Network), and 'オーケストレーション' (Orchestration). The 'コンピュート' tab is selected. Below the tabs, there are sub-tabs: '概要' (Overview), 'インスタンス' (Instances), 'イメージ' (Images), and 'キーペア' (Keys). The 'キーペア' sub-tab is selected and underlined. The breadcrumb path 'プロジェクト / コンピュート / キーペア' is displayed. The main heading is 'キーペア'. Below the heading is a search bar with the placeholder text 'フィルターを指定するにはここをクリックしてください。' and a '+ キーペアの作成' button. Below the search bar, it says '4 件表示'. There is a list of key pairs, each with a checkbox and a name. The third item in the list, 'opst-self-key', is highlighted with a red rectangular box. Below the list, it says '4 件表示' again.

名前 ^
>
>
> opst-self-key
>



## 4-2. 開発端末 (RHEL61\_64bit) の作成 - ①ボリューム作成

1、「ボリューム」→「ボリューム」を押下する。

詳細

ソース

プレースター

ネットワーク

ネットワークのポート

仮想マシンのディレクトリ

キーペア

設定

サーバーグループ

スケジューラーヒント

メタデータ

インストールのコンピュート、メモリー、ストレージリソースは、プレーヤーとして割り当て済み

名前

仮想 CPU

メモリー

合計ディスク

パブリック

利用可能

フィルターを指定するにはここをクリックしてください。

1 つ選択してください。

名前	仮想 CPU	メモリー	合計ディスク	パブリック
> 2cpu4gb	2	4 GB	0 GB	はい
> 8cpu16gb	8	16 GB	0 GB	はい
> 16cpu16gb	16	16 GB	0 GB	はい
> 4cpu4gb	4	4 GB	0 GB	はい
> 16cpu32gb	16	32 GB	0 GB	はい
> 4cpu16gb	4	16 GB	0 GB	はい
> 8cpu32gb	8	32 GB	0 GB	はい
> 8cpu8gb	8	8 GB	0 GB	はい
> 2cpu2gb	2	2 GB	0 GB	はい
> 1cpu1gb	1	1 GB	0 GB	はい
> 1cpu2gb	1	2 GB	0 GB	はい
> 2cpu8gb	2	8 GB	0 GB	はい

2、「+ボリュームの作成」ボタンを押下する。

プロジェクト ▾ コンピュート ▾ ボリューム ネットワーク ▾ オークストレーション ▾

ボリューム スナップショット

プロジェクト / ボリューム / ボリューム

# ボリューム

フィルター

+ボリュームの作成

### 3、「ボリュームの作成」画面で、下記の値を入力し、「ボリュームの作成」ボタンを押下する。

ボリューム名

vol-rhel61-X-UIIM

説明

ボリュームソース

イメージ

イメージをソースとして使用する

RHEL61\_64bit\_20170831 (340.0 MB)

種別

AZ01-STG01

サイズ (GiB)

20

アベイラビリティゾーン

AZ01

説明:

ボリュームは、インスタンスに接続できるブロックデバイスです。

ボリューム種別の説明:

AZ01-STG01

説明がありません。

ボリュームの上限

合計ギバイト 220 / 2048 GiB 使用中

ボリューム数 5 / 10 使用中

取り消し

ボリュームの作成

表 4-2-1 入力内容

項目	値
ボリューム名	vol-rhel61-X-UIIM
説明	なし
ボリュームソース	イメージ
イメージをソースとして使用する	RHEL61_64bit_20170831(340.0MB)
種別	AZ01-STG01
サイズ (GB)	20
アベイラビリティゾーン	AZ01

#### 注釈

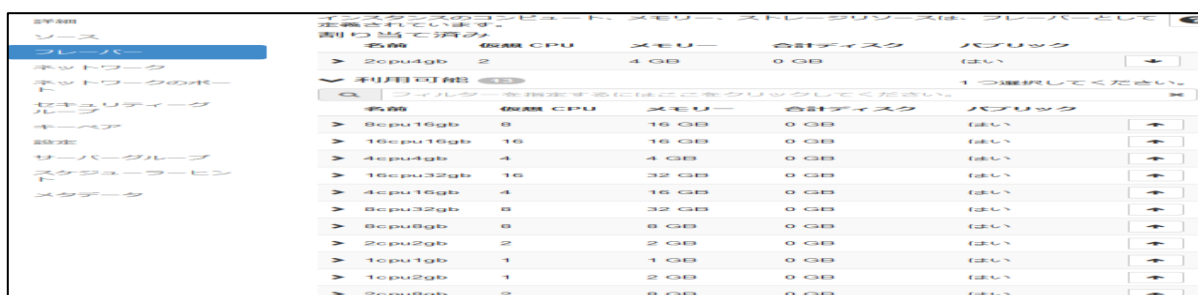
統合開発クラウドでは様々なイメージを用意しております。詳細はポータルサイトでご確認ください。

#### 4、ステータスが「利用可能」と表示されることを確認する。

プロジェクト ▾    コンピュート ▾ <b>ボリューム</b> ネットワーク ▾    オークストレーション ▾						
ボリューム    スナップショット						
プロジェクト / ボリューム / ボリューム						
ボリューム						
6 件表示						
<input type="checkbox"/>	名前	説明	サイズ	ステータス	種別	接続先
<input type="checkbox"/>	vol-rhel61-X-UIM	-	20GiB	利用可能	AZ01-STG01	

## 4-3. 開発端末 (RHEL61\_64bit) の作成 - ②インスタンス作成

1、「ボリューム」→「ボリューム」を押下する。



2、「ボリューム」タブで、「vol-rhel61-X-UIIM」のステータスが、「利用可能」と表示されていることを確認し、アクション項目の「▼」を押下し、「インスタンスとして起動」を押下する。



### 3、「インスタンス名」を入力し、「フレーバー」を押下する。

インスタンスの起動

詳細

ソース

フレーバー\*

ネットワーク\*

ネットワークのポート

セキュリティグループ

キーペア

設定

サーバーグループ

スケジューラーヒント

メタデータ

インスタンス名\*

rhel61-X-UIIM

説明

アベイラビリティゾーン

AZ01

インスタンス数\*

1

合計インスタンス (10 Max)

60%

5 現在使用中  
1 追加済み  
4 残り

✕ 取り消し

< 戻る

次へ >

インスタンスの起動

表 4-3-1 入力内容

項目	値
インスタンス名	rhel61-X-UIIM

### 4、「フレーバー」タブ内「1cpu2gb」の「↑」を押下し、「次へ」を押下する。

インスタンスの起動

詳細

ソース

フレーバー\*

ネットワーク\*

ネットワークのポート

セキュリティグループ

キーペア

設定

サーバーグループ

スケジューラーヒント

メタデータ

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

以下の利用可能なアイデムから1つ選択してください。

利用可能 11

1つ選択してください。

フィルタを指定するにはここをクリックしてください。

名前	数値 CPU	メモリー	合計ディスク	パブリック
8cpu16gb	8	16 GB	0 GB	はい
16cpu16gb	16	16 GB	0 GB	はい
4cpu4gb	4	4 GB	0 GB	はい
16cpu32gb	16	32 GB	0 GB	はい
4cpu16gb	4	16 GB	0 GB	はい
1cpu2gb	1	2 GB	0 GB	はい
2cpu8gb	2	8 GB	0 GB	はい

ソース

フレーバー

ネットワーク\*

ネットワークのポート

セキュリティグループ

キーペア

設定

サーバーグループ

スケジューラーヒント

メタデータ

利用可能 11

フィルタを指定するにはここをクリックしてください。

名前	数値 CPU	メモリー	合計ディスク	パブリック
1cpu2gb	1	2 GB	0 GB	はい
8cpu16gb	8	16 GB	0 GB	はい
16cpu16gb	16	16 GB	0 GB	はい
4cpu4gb	4	4 GB	0 GB	はい
16cpu32gb	16	32 GB	0 GB	はい
4cpu16gb	4	16 GB	0 GB	はい

✕ 取り消し

< 戻る

次へ >

インスタンスの起動

## 5、「ネットワーク」タブで、「利用可能ネットワーク」にあるネットワーク「provider」の「↑」を押下し、「割り当て済みネットワーク」に追加する。



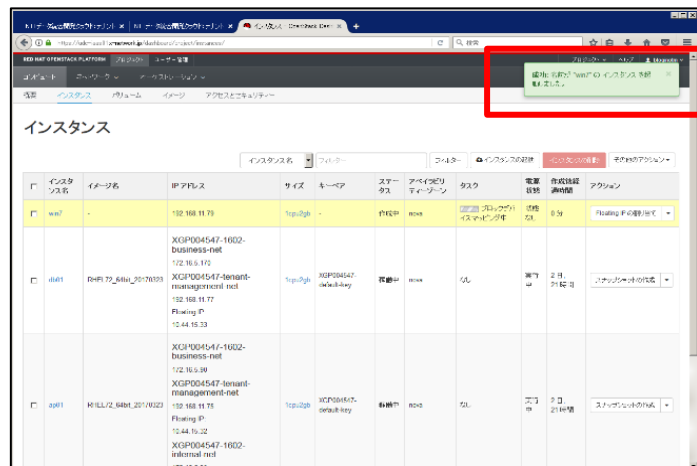
## 6、「セキュリティグループ」タブを選択し、「tenant-security-group-all\_open」の「↑」を押下し、「割り当て済み」に追加する。



## 7、「キーペア」タブを選択し、「opst-self-key」の「↑」を押下し、「インスタンスの起動」を押下する。



## 8、ウェブブラウザ右上部に下図のようなポップアップ画面が表示されることを確認する。



9、「コンピュート」→「インスタンス」と押下し、作成したインスタンスの「ステータス」が「稼働中」であることを確認する。

プロジェクト

コンピュート

ボリューム

ネットワーク

オーケストレーション

概要

インスタンス

イメージ

キーペア

プロジェクト / コンピュート / インスタンス

インスタンス

インスタンス ID

フィルター

インスタンスの起動

6 件表示

<input type="checkbox"/>	インスタンス名	イメージ名	IP アドレス	フレーバー	キーペア	ステータス	アベイラビリティゾーン	タスク	電源状態
<input type="checkbox"/>	rhel61-X-UIIM	-	172.17.1.15	1cpu2gb	OPSThandson-key	稼働中	 AZ01	なし	実行中

### 注釈

開発端末 (RHEL61\_64bit) のアクセスは、「4-8. 開発環境へのアクセス - ③AP サーバアクセス」を参照し、ホストの入力時に「開発端末 (RHEL61\_64bit) の IP アドレス」を入力してください。



## 4-4. 構成管理スタック(Puppet)の作成

開発環境スタック作成に必須となりますので必ず作成してください。

1、「オーケストレーション」→「スタック」を押下する。



2、「スタック」画面で「+スタックの起動」ボタンを押下する。



3、「テンプレートの指定方法」で「URL」を選択する。



#### 4、「テンプレート URL」に以下の URL を入力し、「次へ」ボタンを押下する。

テンプレートの選択

テンプレートの指定方法 \*

URL

テンプレート URL ⓘ  
ain/HEAD:/PuppetEnterprise\_2017\_2\_20170707.yaml

環境設定の指定方法

ファイル

環境設定ファイル ⓘ  
参照... ファイルが選択されていません。

説明:

テンプレートは、インフラストラクチャー、サービス、およびアプリケーションのデプロイメントの自動化に使用されます。

利用可能なテンプレートの指定方法のオプションから、このスタックの作成に使用するテンプレートの指定方法を選択してください。

取り消し

次へ

#### テンプレート URL

http://hudcmm21.x-network.jp/public/git/heat\_templates/blob\_plain/HEAD:/PuppetEnterprise\_2017\_2\_20170707.yaml

5、「スタックの起動」画面で以下を入力、選択し「起動」ボタンを押下する。

スタックの起動

スタック名

cm01-X-UIIM

作成タイムアウト時間 (分単位)

60

☐ 失敗時のロールバック

ユーザー " " のパスワード

\*\*\*\*\*

CM Server Flavor

2cpu8gb

CM Server Name

cm01-X-UIIM

CM Server Size (GB)

40

Tenant Default Key

Tenant ID

edu01openstack

Tenant Security Group

tenant-security-group-all\_open

説明:

指定された値を用いて新しいスタックを作成します。

取り消し

起動

表 4-4-1 入力内容

項目	値
スタック名	cm01-X-UIIM
作成タイムアウト時間（分単位）	60
失敗時のロールバック	チェックを入れる
ユーザー"*****"のパスワード	ログインユーザの X-UIIM パスワード
CM Server Flavor	2cpu8gb
CM Server Name	cm01-X-UIIM
CM Server Size (GB)	40
Tenant Default Key	opst-self-key
Tenant ID	<テナント名 : >
Tenant Security Group	tenant-security-group-all_open

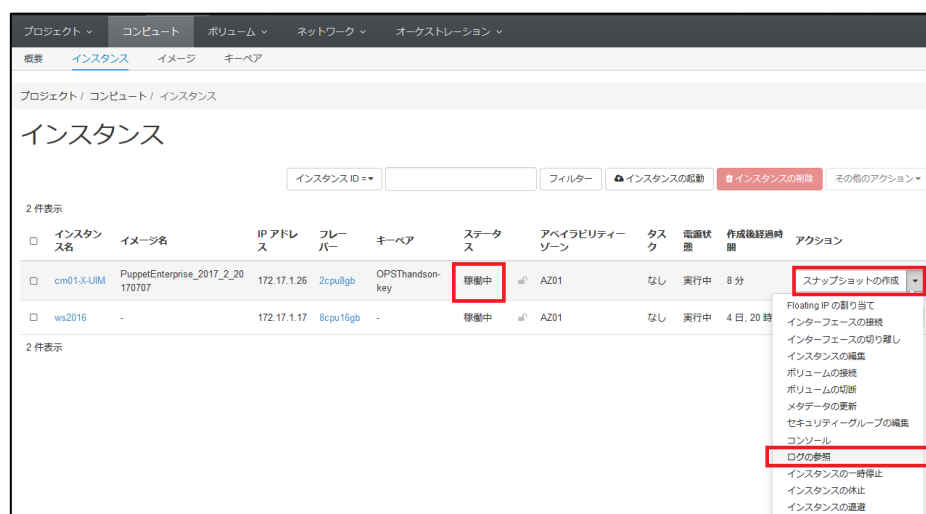
## 6、作成対象スタックの「ステータス」が「作成中」であることを確認する。




### 注釈

※ステータスは数分で「作成完了」と表示されますが、スタック内で初期化スクリプトを実行するため、5-20 分程度待つ必要があります。

## 7、「コンピュート」→「インスタンス」を押下し、作成対象スタックのステータスが「稼働中」であることを確認し、スナップショットの作成の▼」→「ログの参照」を押下する。



## 9、ログの最終行に「Cloud-init v. X.X.X finished ~」が出力されていることを確認する。



```
[ 312.534557] cloud-init[10004]: /var/cache/yum/x86_64/7Server/devcloud-rhel-base/packages/libnss-keyring-3.8.0-3.el7.x86_64.rpm: V3 RSA/SHA256 Signature, key ID 3d564689: OK
[ 312.538971] cloud-init[10004]: Importing GPG key 0xF431D051:
[ 312.540907] cloud-init[10004]: Userid : "Red Hat, Inc. (release key 2)"<security@redhat.com>"ci-info: +++++Authorized keys from /home/cloud-user/.ssh/authorized_keys f
ci-info: -----
ci-info: | Keytype | Fingerprint (md5) | Options | Comment |
ci-info: |-----|-----|-----|-----|
ci-info: | ssh-rsa | 9b:be:6b:6b:fe:fd:31:af:67:58:58:53:00:1f:33:82 | - | Generated-by-Nova |
ci-info: |-----|-----|-----|-----|
[ 312.557252] cloud-init[10004]: Fingerprint: 567e 347a d004 4ade 55ba 8a5f 199e 2f91 fd43 1d51
[ 312.559914] cloud-init[10004]: Package : redhat-release-server-7.2-9.el7.x86_64 (@anaconda/7.2)
[ 312.562634] cloud-init[10004]: From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
[ 312.564753] cloud-init[10004]: Importing GPG key 0x2FA658E0:
[ 312.566339] cloud-init[10004]: Userid : "Red Hat, Inc. (auxiliary key)"<security@redhat.com>"
[ 312.568189] cloud-init[10004]: Fingerprint: 43a6 e49c 4a38 f4be 9abf 2a53 4568 9c88 2fa6 58e0
[ 312.569970] cloud-init[10004]: Package : redhat-release-server-7.2-9.el7.x86_64 (@anaconda/7.2)
[ 312.572051] cloud-init[10004]: From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
[ 312.574516] cloud-init[10004]: RPMDB yum
[ 312.578172] cloud-init[10004]: Provision done: 2019-09-04 16:34:43.165847
ec2:
ec2: #####
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 b4:02:81:62:ea:7c:79:a0:93:76:45:26:60:87:3a:23 (ECDSA)
ec2: 256 6c:04:82:e2:ac:c8:24:b8:39:76:dc:f5:ec:c5:4a:20 (ED25519)
ec2: 2048 b0:9c:5e:6a:a9:62:65:5a:12:32:40:b5:4d:76:76:7f (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #####
ec2: -----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbGlzdHkiNTYAAAAIbmlkdHh0bm50cDQ1b2V0eS42VWVjC/23jCcNncuQ7g+GzG6+Mwup58kGxhHjeSchFZEKSBxSRk/OPxXBAJ7Y=
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINjnduZNU2XLK8+ZsII1TYXIM5kPFU9jy8o8vukHwOK
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQC9qXeyLwDzIuKY1IoEdpa1W5p4ckqC90kZBoYsX+n4UuUk+9u8iHtmkzK1YsiTo6vb0SiBHDp6EVosHPS3vkPF4ZcQzLxYhMhUjKtfoK7rIYLw9Ku4KG8gtPoP678rV3P0nN6W
-----END SSH HOST KEY KEYS-----
[ 312.603666] cloud-init[10004]: Cloud-init v. 0.7.6 finished at 2019-09-04 16:34:43.165847 UTC. Distro: rhel7.2
```

### 注釈

上記ログが出力されていない場合、初期構築が完了していないため、時間をおいて再度ログを確認してください。

## 4-5. 開発環境スタック(WEB、DB、AP サーバ)の作成

1、「オーケストレーション」→「スタック」を押下する。



2、「スタックの起動」ボタンを押下する。



3、「テンプレートの選択」画面で、テンプレートの指定方法のプルダウンから「URL」を選択する。



4、「テンプレート URL」に以下の値を入力し「次へ」ボタンを押下する。

テンプレートの選択

テンプレートの指定方法

URL

テンプレート URL

templates/blob\_plain/HEAD:/OSS\_SINGLE\_V2\_0.yaml

環境設定の指定方法

ファイル

環境設定ファイル

参照... ファイルが選択されていません。

説明:

テンプレートは、インフラストラクチャー、サービス、およびアプリケーションのデプロイメントの自動化に使用されます。

利用可能なテンプレートの指定方法のオプションから、このスタックの作成に使用するテンプレートの指定方法を選択してください。

取り消し

次へ

表 4-4-1 入力内容

項目	入力内容
テンプレート URL	http://hudcmm21.x-network.jp/public/git/heat_templates/blob_plain/HEAD:/OSS_SINGLE_V2_0.yaml

注釈

スタックの詳細については、ポータルサイトの「マニュアル」内の「デリバリーサービス」をご参照ください。

5、「スタックの起動」画面で以下を入力、選択し「起動」ボタンを押下する。

スタックの起動

スタック名 \* ⓘ  
oss-X-UIIM

説明:  
指定された値を用いて新しいスタックを作成します。

作成タイムアウト時間 (分単位) ⓘ  
60

☐ 失敗時のロールバック ⓘ

ユーザー "\*\*\*\*\*" のパスワード ⓘ  
\*\*\*\*\*

CM Server IP Address ⓘ  
172.17.1.26

CM Server Name ⓘ  
cm01-X-UIIM

Manifest Update (public manifest only) ⓘ  
-

CM Server PuppetSV Type ⓘ  
PE

Tenant Default Key ⓘ  
.

Tenant Security Group ⓘ  
tenant-security-group-all\_open

取り消し 起動

表 4-4-2 入力内容

項目	値
スタック名	oss-X-UIIM
作成タイムアウト時間 (分単位)	60
失敗時のロールバック	チェックを入れる
ユーザー“*****”のパスワード	ログインユーザの X-UIIM パスワード
CM Server IP Address	<cm01-provider-ip>
CM Server Name	cm01-X-UIIM
Manifest Update (public manifest only)	-
CM Server PuppetSV Type	PE
Tenant Default key	opst-self-key
Tenant Security Group	tenant-security-group-all_open

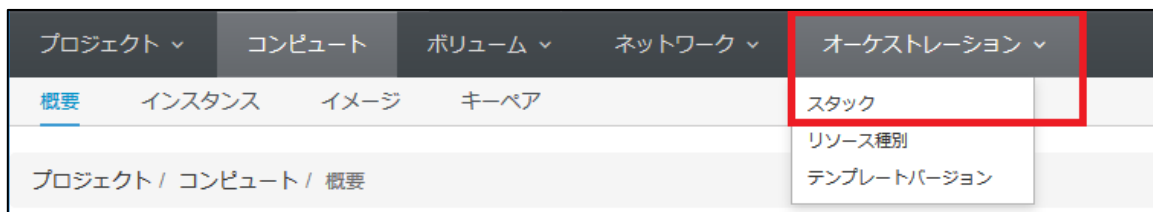


6、「スタック」画面で、作成対象スタックの「ステータス」が「作成中」であることを確認する。

プロジェクト ▾    コンピュート ▾    ボリューム ▾    ネットワーク ▾    オークストレーション			
スタック    リソース種別    テンプレートバージョン			
プロジェクト / オークストレーション / スタック			
スタック			
スタック名 = ▾    フィルター    +スタックの起動    ●スタックのプレビュー			
2 件表示			
<input type="checkbox"/>	スタック名	作成時刻	ステータス
<input type="checkbox"/>	oss-X-UIIM	0 分	作成中
<input type="checkbox"/>	cm01-X-UIIM	42 分	作成完了
2 件表示			

## 4-6. 開発環境へのアクセス - ①スタックの IP アドレス確認

1、「オーケストレーション」→「スタック」タブを選択する。



2、「スタック名」一覧から「oss-X-UIIM」を選択する。



### 3、「概要」タブを押下し「出力」に表示されている IP アドレスを確認する。

プロジェクト

コンピュート

ボリューム

ネットワーク

スタック

リソース種別

テンプレートバージョン

プロジェクト / オークストレーション / スタック / oss-X-UIIM

oss-X-UIIM

トポロジー

概要

リソース

イベント

テンプレート

名前

oss-X-UIIM

ID

1fb7aec3-1b01-43d5-8221-26d310ae0df1

説明

OSS\_SINGLE\_V2\_0\_20180122-1

ステータス

作成時刻

25 分

最終更新

なし

ステータス

Create\_Complete: Stack CREATE completed successfully

出力

ap01-provider-ip

Provider-NW IP Address

172.17.1.5

db01-provider-ip

Provider-NW IP Address

172.17.1.19

web01-provider-ip

Provider-NW IP Address

172.17.1.33

#### 注釈

IP アドレスが表示されない場合、5分ほど時間をおいてから F5 キーを押下すると表示されます。

### 4、同様に「cm01-X-UIIM」の「cm01-provider-ip」の IP アドレス(構成管理スタックの IP アドレス)を確認する。

プロジェクト

コンピュート

ボリューム

ネットワーク

オーケストレーション

スタック

リソース種別

テンプレートバージョン

プロジェクト / オーケストレーション / スタック / cm01-X-UIIM

cm01-X-UIM

トポロジー

概要

リソース

イベント

テンプレート

名前

ID

説明

cm01-X-UIIM

f0ba8307-94b9-480e-a235-893c625b8fe8

PuppetEnterprise\_2017\_2\_20170707-2

ステータス

作成時刻

最終更新

ステータス

18 分

なし

Create\_Complete: Stack CREATE completed successfully

出力

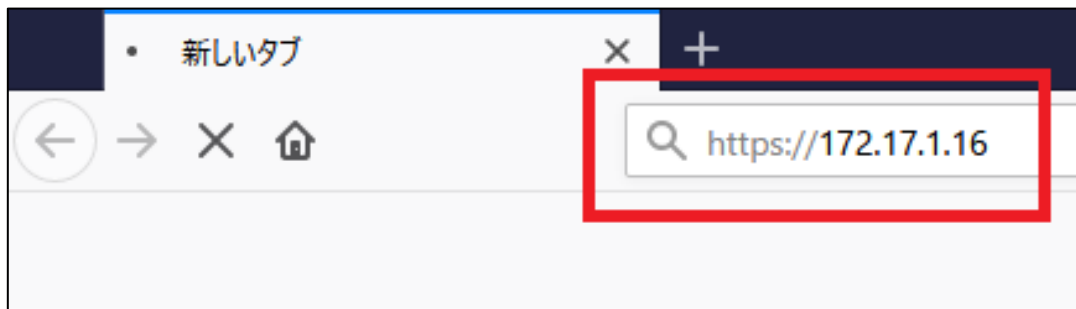
cm01-provider-ip

Provider-NW IP Address.

172.17.1.26

## 4-7. 開発環境へのアクセス - ②Puppet 管理画面アクセス

1、Firefox を起動し、アドレスバーに以下の URL を入力する。



URL
https://<cm01-provider-ip>

2、「詳細」ボタンを押下し、表示されたエラー内容の「危険性を承知続行」ボタンを押下する。



3、Puppet Enterprise のログイン画面が表示されることを確認し、下記を入力し「ログイン」ボタンを押下する。

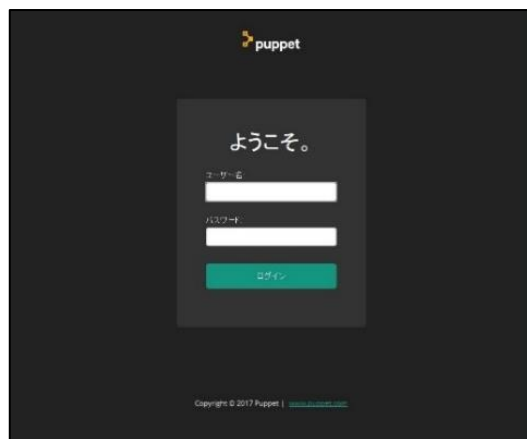
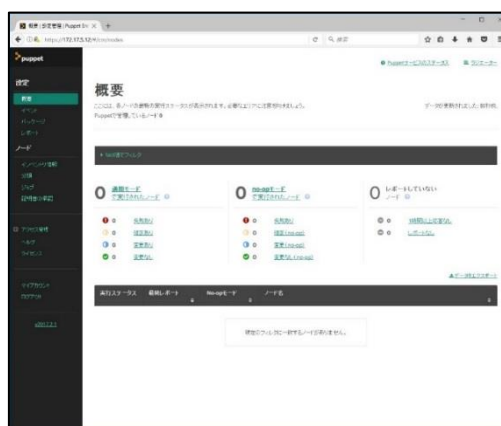


表 4-7-1 入力内容

項目	値
ユーザー名	admin
パスワード	admin

4、「Puppet 管理ダッシュボード」画面が表示されることを確認する。



## 4-8. 開発環境へのアクセス - ③AP サーバアクセス

1、「Tera Term」を起動し、ホスト名に以下の値を入力し「OK」ボタンを押下する。

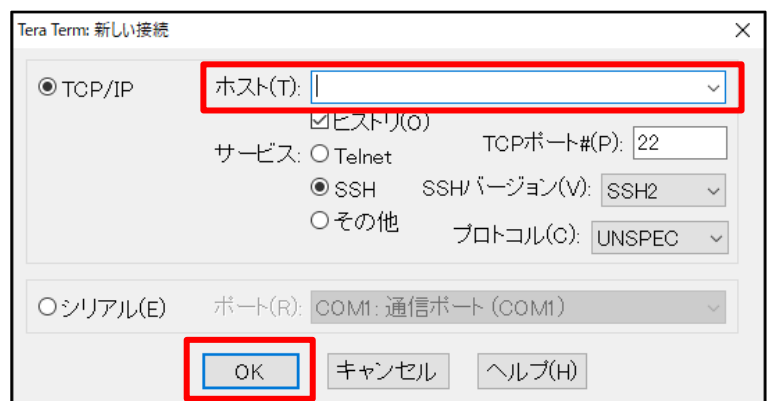
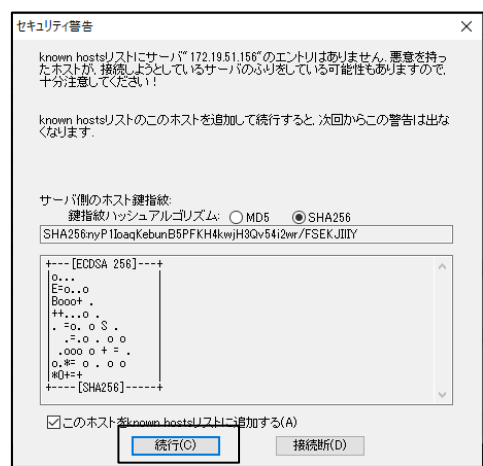


表 4-8-1 入力内容

項目	値
ホスト	<ap01-provider-ip>

2、「続行」を押下する。



3、「ユーザ名」を入力し、「RSA/DSA/ECDSA/ED25519 鍵を使う」を選択、「秘密鍵」ボタンを押下する。

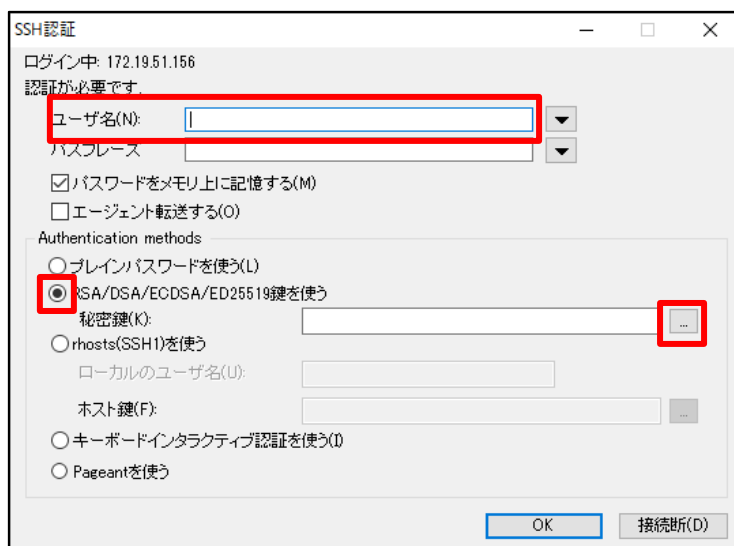
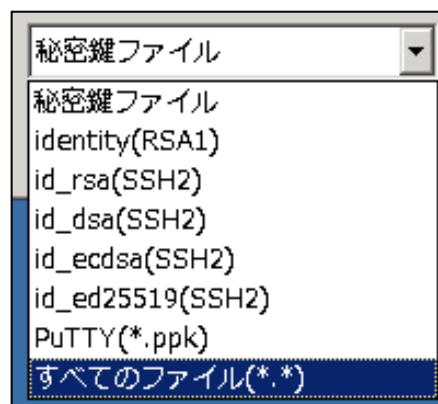
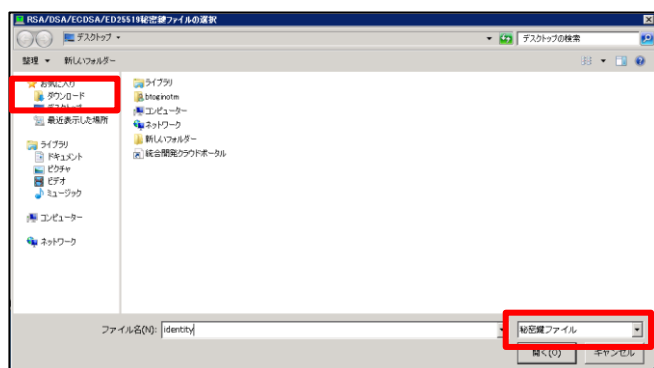


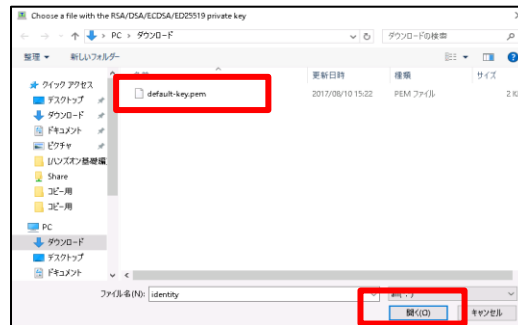
表 4-8-2 入力内容

項目	値
ユーザ名	cloud-user

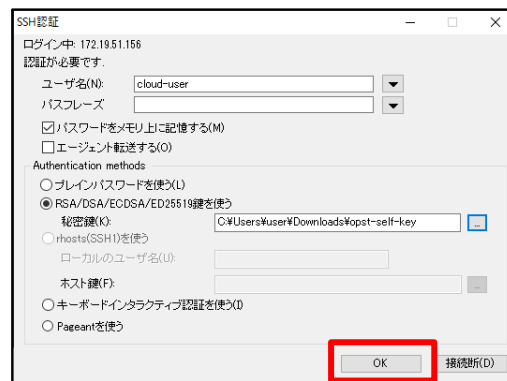
4、ダウンロードフォルダを選択し、「秘密鍵ファイル」から「すべてのファイル」を選択する。



5、一覧から「opst-self-key」を選択し「開く」ボタンを押下する。



6、「OK」ボタンを押下する。



7、コマンドを実行し、Tomcat の配置とプロセスの存在を確認する。

```
172.17.11.32 - root@ap01 ~ - VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
Last login: Tue Jan 28 19:02:47 2020 from 172.17.1.11
[cloud-user@ap01 ~]$ sudo su -
最終ログイン: 2020/01/28 (火) 19:03:45 JST日時 pts/0
[root@ap01 ~]# ls /opt/tomcat/
LICENSE  RELEASE-NOTES  bin  lib  temp  work
NOTICE  RUNNING.txt    conf  logs  webapps
[root@ap01 ~]# ps -ef | grep tomcat
root      10801    1  0 19:07 ?        00:00:00 cat /opt/tomcat/logs/catalina.fo
tomcat    10807    1  2 19:07 ?        00:00:01 /usr/lib/jvm/java-1.8.0-openjdk/
bin/java -Djava.util.logging.config.file=/opt/tomcat/conf/logging.properties -Dj
ava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Dtomcat.process=
agentlib:heartstats -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pk
s=org.apache.catalina.webresources -classpath /opt/tomcat/bin/bootstrap.jar:/opt
/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/opt/tomcat -Dcatalina.home=/opt/tom
cat -Djava.io.tmpdir=/opt/tomcat/temp org.apache.catalina.startup.Bootstrap star
t
root      10938 10916  0 19:08 pts/0    00:00:00 grep --color=auto tomcat
[root@ap01 ~]#
```



項番	コマンド
1	sudo su -
結果	最終ログイン: yyyy/mm/dd (曜日) hh:mm:ss JST 日時 pts/0
2	ls /opt/tomcat/
結果	LICENSE RELEASE-NOTES bin lib temp work NOTICE RUNNING.txt conf logs webapps
3	ps -ef   grep tomcat
結果	root 10801 1 0 19:07 ? 00:00:00 cat /opt/tomcat/logs/catalina.fifo tomcat 10807 1 2 19:07 ? 00:00:01 /usr/lib/jvm/java-1.8.0-openjdk/bin/java -Djava.util.logging.config.file=/opt/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Dtomcatprocess -agentlib:heapstats -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -classpath /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/opt/tomcat -Dcatalina.home=/opt/tomcat -Djava.io.tmpdir=/opt/tomcat/temp org.apache.catalina.startup.Bootstrap start root 10936 10916 0 19:08 pts/0 00:00:00 grep --color=auto tomcat

## 8、以下のコマンドを実行し、ログアウトする。

項番	コマンド
1	exit
2	exit

### 注釈

WEB サーバ、DB サーバも同様にログイン可能です。ホストの入力時にそれぞれの「IP アドレス」を入力してください。

## 5. その他

---

統合開発クラウドについて補足いたします。

### 5-1. アクセスユーザの追加について

---

OpenStack 環境を利用するユーザは、UDS プロジェクトグループが **G-UIM** で登録されている場合は G-UIM で中継デスクトップにログインでき、OpenStack 上の各インスタンスにアクセス可能となります。

UDS プロジェクトグループが **X-UIM** で登録されている場合は、**UDS プロジェクトグループで社外ユーザを作成**することで、X-UIM を所持していなくても上記同様の操作が可能です。詳細はポータルサイトの「追加申請用ユーザ登録手順書」をご参照ください。

### 5-2. 外部インターネット接続について

---

ダッシュボードにて、ホワイトリスト申請を行うことで、指定された URL への OpenStack 上のインスタンスからアクセスが可能となります。

### 5-3. Office 端末とのデータのやりとりについて

ETRAPOT を用いたデータ転送を推奨しております。詳細はポータルサイトの「ETRAPOT 接続手順書」をご参照ください。

### 5-4. OpenStack の容量追加について

OpenStack を払い出した直後では vcpu:20 コア、メモリ:50GB、ストレージ:1TB となっております。

	メモリ(MB)	CPU(コア数)	ストレージ (GB)
テナント用クォータ	51,200	20	1,000
全テナント用クォータ	51,200	20	1,000
標準提供枠	102,400	40	2,048
超過クォータ	0	0	0
利用料金		¥0	¥0
利用料金総額			¥0

追加する場合はダッシュボード内の「既存契約確認・変更申請」内の「OpenStack テナント申請」を変更し、申請してください。

変更申請	カテゴリ	識別子	最終更新日	申請者	詳細
	UDSアクセス申請サービス申請		2021/01/27		
	OpenStackテナント申請		2020/07/13		
	統合開発セキュリティ基盤(UDS)申請		2020/03/13		

## 5-5. その他のスタック紹介

---

本資料では、開発環境スタックを用いましたが、ほかにも Docker によるコンテナ実行基盤スタック、開発端末管理スタックによる各種サーバの自動基盤構築、CI/CD ツールスタック等、各種スタックをポータルサイトにて紹介しております。

## 5-6. 統合開発クラウドよろず相談窓口

---

よろず相談窓口では、統合開発クラウドに関する各種ご相談を対面にて承っております。既に統合開発クラウドをご利用頂いている方、これからご利用を検討されている方問いませんので、ぜひご相談ください。

### 注釈

よろず相談窓口の URL:

【 [https://nttdataudc.service-now.com/udc?id=kb\\_article&sys\\_id=ab0445451bf2c4d029d433b5cc4bcb52](https://nttdataudc.service-now.com/udc?id=kb_article&sys_id=ab0445451bf2c4d029d433b5cc4bcb52) 】