FUJITSU Hybrid IT Service FJcloud-O
IaaS 次世代仮想ファイアーウォール
powered by Palo Alto Networks

VM-series

スタートガイド

Version 1.10

FUJITSU LIMITED

まえがき

本書の目的

本書は、FUJITSU Hybrid IT Service FJcloud-O IaaS（以降、IaaS）- 次世代仮想ファイアーウォール powered by Palo Alto Networks VM-series（以下、Palo Alto Networks と言います）のインストール手順および、IaaS 上での設定手順例について記載しております。本書の記載内容に沿って Palo Alto Networks をご利用ください。

本書は、西日本第 3 リージョン、東日本第 3 リージョンを対象としています。

本書の読者

本書は、Palo Alto Networks をご利用になる方を対象としています。本書のご利用にあたり、基本的な IaaS の操作方法、ネットワークの知識を有していることを前提としております。あらかじめご了承ください。

本書の適用製品

本書の内容は以下の製品に適用されます。

- PAN VM50 Basic
- PAN VM50 Bundle1
- PAN VM50 Bundle2
- PAN VM100 Basic
- PAN VM100 Bundle1
- PAN VM100 Bundle2
- PAN VM300 Basic
- PAN VM300 Bundle1
- PAN VM300 Bundle2
- PAN VM500 Basic
- PAN VM500 Bundle1
- PAN VM500 Bundle2

本書における語句の定義

本書で使用される語句の定義を下表に示します。

語句	定義の説明
Palo Alto Networks（パロアルトネットワークス）	FUJITSU Hybrid IT Service FJcloud-O IaaS 次世代仮想ファイアーウォール powered by Palo Alto Networks VM-series の略称です。
IaaS	FUJITSU Hybrid IT Service FJcloud-O IaaS の略称です。
Active	Palo Alto Networks の装置二重化機能を有効にした場合の現用装置(アクティブ)です。
Passive	Palo Alto Networks の装置二重化機能を有効にした場合の待機装置(パッシブ)です。

語句	定義の説明
仮想 IP アドレス	2 台の Palo Alto Networks で共有するため、割り当てる IP アドレスです。冗長切り替え後に片方の Palo Alto Networks に引き継がれます。
SSL-VPN	インターネットから SSL-VPN の接続です。
FW	ファイアーウォール(FireWall)の略称です。
interface	Palo Alto Networks のネットワークインターフェースの名称です。

マニュアル

本書は設定に関する初期段階の説明を記載しております。 Palo Alto Networks の機能詳細は、本書と同 Web ページに掲載の機能説明書をご覧ください。下表に製品マニュアルの種類と目的・用途を示します。

マニュアル名称	目的・用途
FUJITSU Hybrid IT Service FJcloud-O IaaS / FJcloud-ベアメタル 機能説明書 /Palo Alto Networks 提供サービス	FUJITSU Hybrid IT Service FJcloud-O で提供する Palo Alto Networks VM-Series の機能を記載しています。
FUJITSU Hybrid IT Service FJcloud-O IaaS / FJcloud-ベアメタル API リファレンス(東日本リージョン３／西日本リージョン３)	Palo Alto Networks VM-Series のライセンス管理を行うための API について、リファレンス情報を記載しています。

本書の利用範囲について

本書は国内提供のみといたします。

Palo Alto Networks の使用条件について

Palo Alto Networks をご使用いただくにあたり、ライセンス条項に同意いただく必要がございます。Palo Alto Networks をご使用の前に、以下の Web ページに掲載のライセンス条項をお読みいただき、同意のうえ Palo Alto Networks をご使用ください。

Palo Alto Networks の使用に関するライセンス条項
https://jp.fujitsu.com/solutions/cloud/fjcloud/-o/document/pdf/paloaltonetworks-covenant.pdf

お願い

- 本資料の無断複製、転載を禁じます。
- 本資料は仕様変更等により予告なく内容を変更する場合がございます。あらかじめご注意願います。
- 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。

変更履歴

版数	更新日	変更箇所	概要
1.0	2021 年 4 月 19 日	初版作成	
1.1	2021 年 6 月 1 日	本書の適用製品に VM500 を追加 2.3 留意事項の項番 1 を追記 5.2 keyField 改行コードに関する追記 5.7 Palo Alto Networks バージョンアップを追加	記載追記
1.2	2021 年 7 月 16 日	2.3 留意事項の項番 11 を追記	記載追記
1.3	2021 年 9 月 15 日	2.3 留意事項の項番 12 を追記 2.4 本書で作成するシステム構成へ記載追記	記載追記
1.4	2021 年 10 月 18 日	2.4 本書で作成するシステム構成の記載変更 3.1 仮想ネットワーク作成の記載変更 3.2 仮想ルータ作成の記載変更 3.4 セキュリティグループ作成の記載変更 3.5 アンチアフィニティ設定の記載変更 3.6 Management-net 用 FW 作成の記載変更 3.7 VPN 接続作成の記載変更 4　仮想サーバ作成の記載変更 5.8 Palo Alto Networks 参照 URL を追記	記載変更 記載追記
1.5	2022 年 4 月 20 日	3.4 セキュリティグループルールにプロトコル 99 番の許可設定を追加	記載追記
1.6	2022 年 5 月 19 日	2.3 留意事項の項番 13 を追記	記載追記
1.7	2022 年 10 月 17 日	5.2 本章の見出し名とライセンスファイルの作成手順の記載変更 5.3 ライセンスファイル登録手順の記載変更 5.7 バージョンアップ参照 URL の記載変更	記載変更
1.8	2023 年 2 月 16 日	5.4 Palo Alto Networks のライセンス無効化(トークンファイルの入手)の記載追記	記載追記
1.9	2023 年 4 月 20 日	3.4 セキュリティグループ作成の記載変更(ステートレスで作成するように変更)	記載変更
1.10	2024 年 6 月 17 日	2.3 留意事項の項番 14 を追記	記載追記

目次

第 1 章　Palo Alto Networks の概要、機能一覧

FUJITSU Hybrid IT Service FJcloud-O IaaS 次世代仮想ファイアーウォール powered by Palo Alto Networks VM-seriesは、IaaS上で動作する仮想アプライアンスソフトウェアであり、アプリケーション、ユーザー、およびコンテンツの情報を元にトラフィックを分類し、アクセス制御を行う機能を持っています。

1.1　Palo Alto Networks が提供する機能について

IaaS 上の Palo Alto Networks は、以下の製品マニュアルのうち機能説明書に記載されている機能を提供します。

・Palo Alto Networks シリーズ

プロダクト一覧

https://www.paloaltonetworks.jp/prisma/vm-series

第 2 章　Palo Alto Networks ご利用の流れ

本章では、Palo Alto Networks をご利用いただくための作業の流れや留意点について説明します。

2.1　Palo Alto Networks の使用手順について

Palo Alto Networks を使用するためには VM 配備後、ライセンスのアクティベーションを実行する必要があります。

ライセンスのアクティベーション方法は 5 章を参照してください。

2.2　Palo Alto Networks 設定の流れ

本書では、Palo Alto Networks を含むシステムの作成を事例として、Palo Alto Networks の設定方法を説明します。図 2-2-1 に設定の流れの全体を示します。

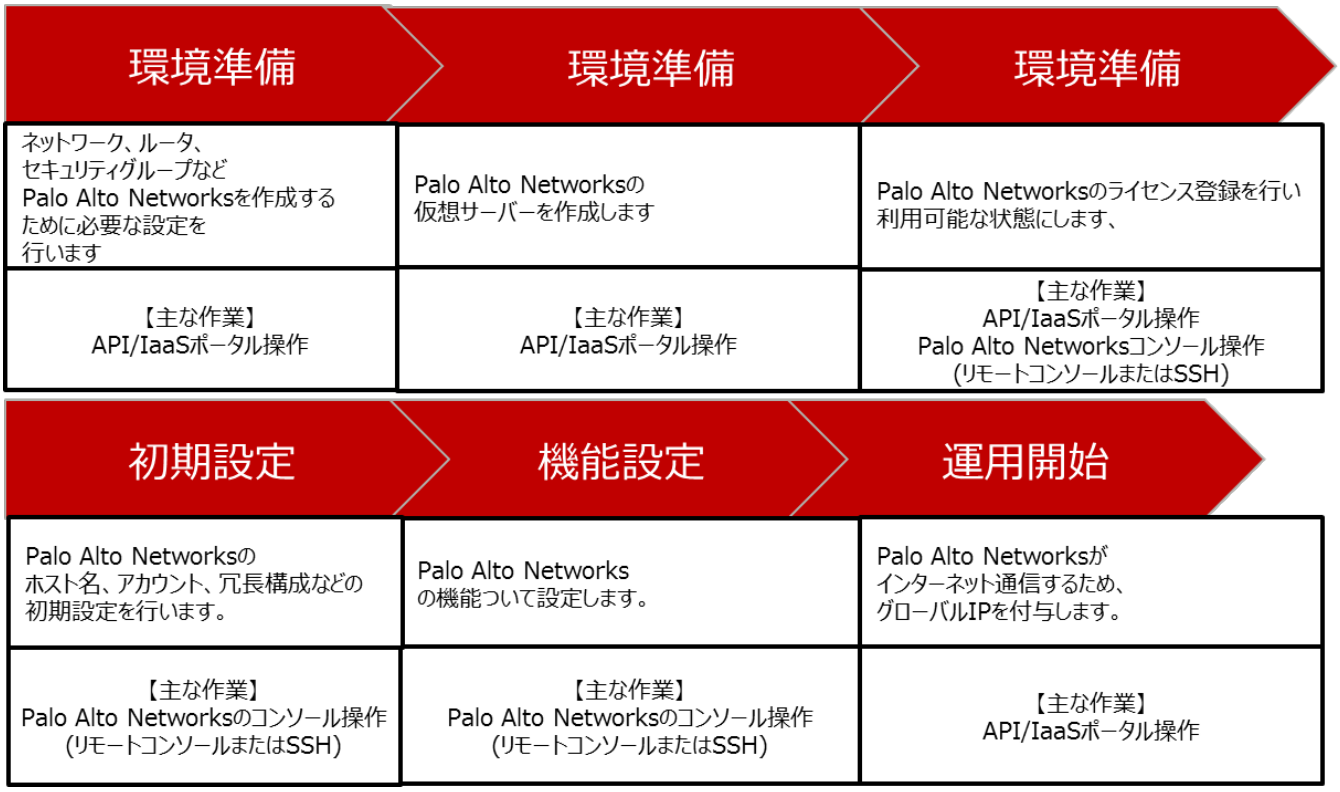


図 2-2-1：Palo Alto Networks 設定の流れ

2.3　留意事項

作業を始める前に表 2-1 の留意事項をよくお読みください。

表 2-3-1：留意事項

項番	留意事項	該当する章番号
1	仮想サーバタイプは Palo Alto Networks VM50,VM100；S3-2 ， VM300；S3-4 ，VM500;C3-8 固定のため、S3-2/S3-4/C3-8 以外は指定しないでください。S3-2/S3-4/C3-8 以外を指定した場合、Palo Alto Networks の動作は保証しておりません。 また、オートスケールには対応しておりません。	4 章
2	Palo Alto Networks に割り当てるディスクボリュームは boot 時に/dev/vda に 60GB 必要です。60GB 未満または 60GB を超えたサイズを指定した場合、Palo Alto Networks の動作は保証しておりません。 また、ボリュームのリサイズや追加アタッチには対応しておりません。 ログ保存が必要な場合、別途 Syslog サーバ等環境をご用意ください。	5 章
3	冗長化構成の Palo Alto Networks 仮想サーバを作成する際、異なるホスト上で動作するよう、アンチアフィニティ機能を設定してください。また、Palo Alto Networks に繋がっているサブネット上の仮想サーバは、アンチアフィニティ機能の設定を推奨します。	4 章
4	セキュリティレベル向上のため、VM 配備後は必ず admin ユーザーのパスワード変更を実施してください。	5 章
5	Palo Alto Networks はキーペアには対応しておりません。そのため、キーペアを割り当ててもキーを用いてログインすることはできません。	3 章
6	Palo Alto Networks の性能について、お客様にて環境構築後に性能測定を実施してから使用することを推奨いたします。	-
7	Palo Alto Networks の冗長構成における HA2 ポートのキープアライブタイムアウト値については、30 秒以上を推奨いたします。デフォルト値は 10 秒になります。 タイムアウト値「HA2 keep-alive」の変更方法は以下 URL をご参照ください。 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-high-availability/configure-ha-settings	-
8	Palo Alto Networks は CLI での API 実行に対応しておりません。Curl が実行できる環境にて Palo Alto Networks のライセンスファイル取得をお願いいたします。	
9	Palo Alto Networks の仮想インターフェース最大数は 25 ですが、IaaS 仕様上、仮想ルータのインターフェース最大数は 10 となります。	
10	Palo Alto Networks の冗長構成切り替え方式は、仮想 MAC を指定する方式を利用しないでください。	
11	Palo Alto Networks のシグネチャ更新はインターネット接続環境(Outbound通	

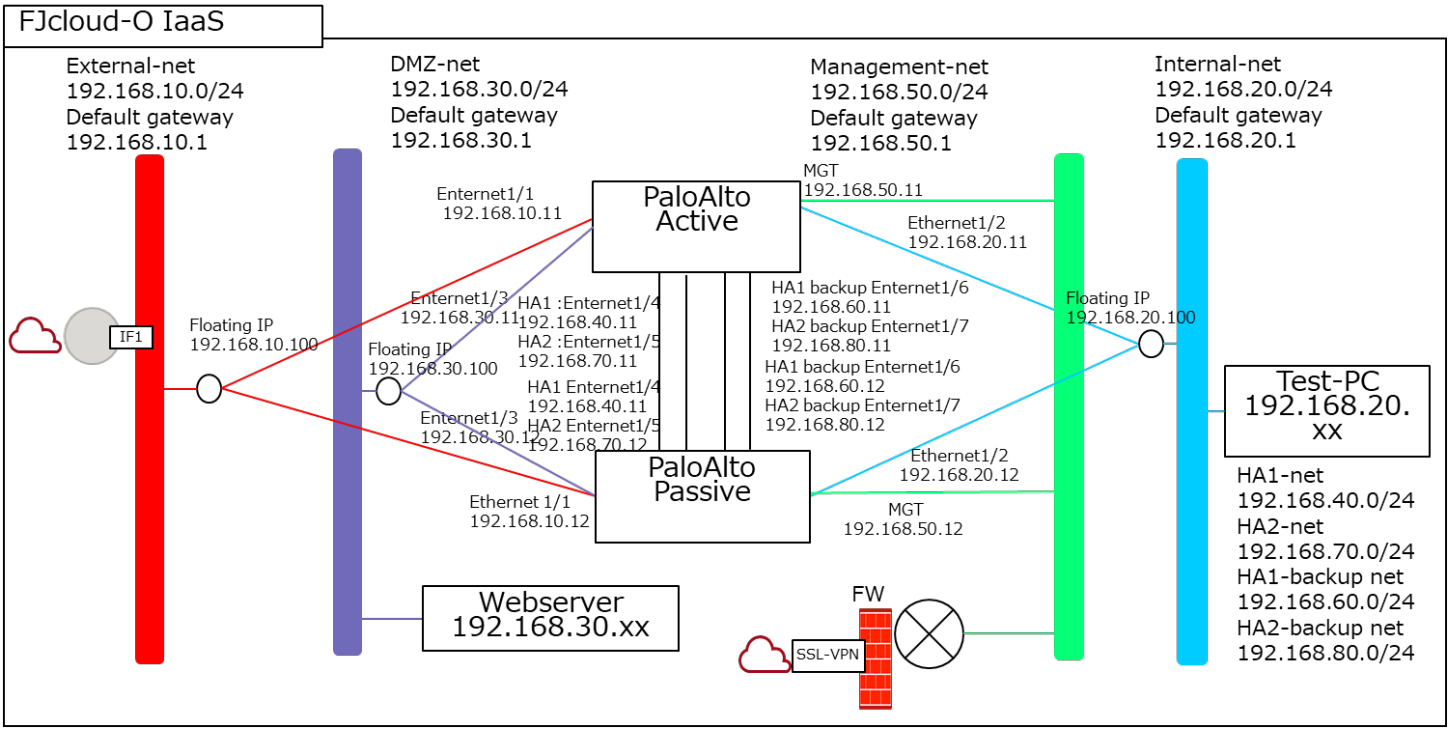
項番	留意事項	該当する章番号
	信のみを許可）を準備して、お客様で更新してください。	
12	Palo Alto Networks のポートデタッチはインスタンスをシャットダウンした状態で実施してください。	
13	Palo Alto Networks の ZoneProtection 機能を使用する場合、ゾーンプロテクションプロファイルの SYN フラッド防御は利用しないでください。 SYN フラッド防御の設定箇所： Palo Alto Networks仮想マシンのGUI画面で、Networkタブ→左ペインのネットワークプロファイル→ゾーンプロテクションをクリック ・フラッド制御でSYNの左側のチェックがついていないこと  	
14	PaloAlto ではセキュリティを強化するために、製品とサービス間の暗号化された通信パスごとに個別の証明書を使用しています。 WildFire、URL フィルタリング、DNS セキュリティの接続に影響があるため、これらの機能を利用する場合は以下を追加で対応してください。 ■ ヘルプデスク窓口へ対象の PAN-OS のシリアル No と作業予定日時(開始・終了)の候補を 3 つほどご連絡ください。 ※メールの件名は、「PaloAlto 内蔵証明書の追加作業に関する依頼」としてください ※作業予定日時の 5 営業日以上前にご連絡ください ■ 作業開始時にヘルプデスク窓口にてシリアル No を元に PaloAlto 社ポータルサイトで OTP(One-time Password)を発行します。10 分以内を目途に以下のフォーマットでお客様にメールで通知しますので、メールをご確認ください。 フォーマット： PAN-OS: <シリアル No> Password: <OTP>	

項番	留意事項	該当する章番号
	Expires On: 6/17/2024 7:00:00 PM (PT) ※Expires On(有効期限)は発行から 1 時間後です。PT 表記のため JST に読み替えるには+17 時間してください。 ■ 以下の手順で PAN-OS GUI で OTP を入力し、デバイス証明書を取得してください。 (1) Device タブ > Setup > Management タブ > Device Certificate > Get certificate (リンク)をクリック (2) One-time Password のテキストボックスに、メール通知された OTP を入力し、OK をクリック (3) Device Certificate 内の Current Device Certificate Status が Valid であることを確認 補足： ・デバイス証明書の取得には、下記に掲載の FQDN とポートへのアクセスを許可している必要があります。 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/certificate-management/obtain-certificates/device-certificate ・作業時に正常にデバイス証明書が取得できない場合、以下の手順で Tech-Support ファイルとパケットキャプチャを取得してください。 (1) Tech-Support ファイルの取得 (2) パケットキャプチャの取得	

2.4　本書で作成するシステム構成

以降の章では、IaaS 上で Palo Alto Networks を含んだシステムの設定方法を事例として紹介しております。本事例を参考にして構築してください。図 2-4-1 に、本書で作成するシステム構成を示します。

本マニュアルに記載した事例以外の構成に関しては、Palo Alto Networks 社のマニュアル、および IaaS マニュアルを参照してください。



※Test-PC はアクセステストの用途を想定しております。

※External-net、DMZ-net、Internal-net において、PaloAlto に設定する IP は、Floating IP アドレスになります。

参照 URL

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability /set-up-activepassive-ha/prerequisites-for-activepassive-ha.html

図 2-4-1：Palo Alto Networks を含むシステム構成

第 3 章　【共通設定】環境準備

本章では、Palo Alto Networks 作成前に必要となる環境準備作業について説明します。

■本章に記載のコマンドは、jq コマンドが使用できる環境で実行してください。

■API で使用するエンドポイントや変数について、以降の説明では下記の表記をしております。エンドポイントについては IaaS マニュアルを参照してください。

- $COMPUTE：compute サービスのエンドポイント
- $NETWORK：ネットワークサービスのエンドポイント
- $OS_AUTH_TOKEN：取得した API のトークン
- $PROJECT_ID ：設定するプロジェクトの ID

3.1　仮想ネットワークの作成

システムで利用するプライベートネットワークを作成します。

後述①②の手順で、システム構成に従い 6 つプライベートネットワークを作成します。

［ネットワーク例］

- External-net
  - NetworkAddress　:192.168.10.0
  - GatewayIP　:192.168.10.1
- Internal-net
  - NetworkAddress　:192.168.20.0
  - GatewayIP　:192.168.20.1
- DMZ-net
  - NetworkAddress　:192.168.30.0
  - GatewayIP　:192.168.30.1
- HA1-net
  - NetworkAddress　:192.168.40.0
  - GatewayIP　:192.168.40.1
- Management-net
  - NetworkAddress　:192.168.50.0
  - GatewayIP　:192.168.50.1
- HA1-backupnet
  - NetworkAddress　:192.168.60.0
  - GatewayIP　:192.168.60.1

- HA2-net
  - NetworkAddress　:192.168.70.0
  - GatewayIP　:192.168.70.1

- HA2-backupnet
  - NetworkAddress　:192.168.80.0
  - GatewayIP　:192.168.80.1

① 仮想ネットワークを作成します。操作は API を使用してください。(図 3-1-1～3-1-5)

＜External-net(192.168.10.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=External-net ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※1　名前は任意で指定してください。
※2　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:38:53Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:38:53Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
    "name": "External-net"
  }
}
```


図 3-1-1：External-net 作成

＜Internal-net(192.168.20.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=Internal-net ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※1　名前は任意で指定してください。
※2　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:39:18Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:39:18Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "139edbe8-bf0e-46dc-8281-ab319d2b6291",
    "name": "Internal-net"
  }
}
```


図 3-1-2：Internal-net 作成

＜DMZ-net (192.168.30.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=DMZ-net ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※1　名前は任意で指定してください。
※2　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:39:39Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:39:39Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "4cbb2b5a-9db6-4ccc-9f7c-375c544d6d4f",
    "name": "DMZ-net"
  }
}
```


図 3-1-3：DMZ-net 作成

＜HA1-net(192.168.40.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=HA1-net ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※1　名前は任意で指定してください。
※2　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:40:19Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:40:19Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "2a3d8643-5fd5-43cc-9849-2b8aa85d0a90",
    "name": "HA1-net"
  }
}
```


図 3-1-4：HA1-net 作成

＜Management-net(192.168.50.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=Management-net ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※1　名前は任意で指定してください。
※2　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:40:36Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:40:36Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "bed53dcc-986b-43b9-91b1-374bc1adf2c8",
    "name": "Management-net"
  }
}
```


図 3-1-5：Management-net 作成

＜HA1-backupnet (192.168.60.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=HA1-backupnet ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※3　名前は任意で指定してください。
※4　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:40:55Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:40:55Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "57a50333-2587-467d-9a33-8d4e4649e864",
    "name": "HA1-backupnet"
  }
}
```


図 3-1-6：HA1-backupnet 作成

＜HA2-net(192.168.70.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=HA2-net ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※5　名前は任意で指定してください。
※6　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:41:13Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:41:13Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "bbc94352-e63c-4401-a31e-e039543e57fd",
    "name": "HA2-net"
  }
}
```


図 3-1-7：HA2-net 作成

＜HA2-backupnet (192.168.80.0/24)＞

コマンド例

```
[root@K5-Host ]# NETWORK_NAME=HA2-backupnet ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/networks -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"network":  {"name":  "'$NETWORK_NAME'","admin_state_up":  true,"project_id": "'$PROJECT_ID'","shared": false}}' | jq .
```

※7　名前は任意で指定してください。
※8　Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "network": {
    "status": "ACTIVE",
    "router:external": false,
    "availability_zone_hints": [],
    "availability_zones": [],
    "description": "",
    "subnets": [],
    "shared": false,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:41:33Z",
    "tags": [],
    "ipv6_address_scope": null,
    "mtu": 8950,
    "updated_at": "2021-09-24T06:41:33Z",
    "admin_state_up": true,
    "revision_number": 2,
    "ipv4_address_scope": null,
    "is_default": false,
    "port_security_enabled": true,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "f84de3bb-28c7-44c6-ad3b-9a64dc90b6ac",
    "name": "HA2-backupnet"
  }
}
```


図 3-1-8：HA2-backupnet 作成

② Subnet、Gateway を設定します。(図 3-1-7～図 3-1-12)

＜External-subnet (192.168.10.0/24)＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.10.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=External-subnet ※2
[root@K5-Host ]# NETWORK_ID=作成した External-net の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'"}}' | jq .
```

※1 サブネットアドレスで指定してください。
※2 名前は任意で指定してください。
※3 作成した External-net の ID で指定してください。
※4 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:42:23Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.10.2",
        "end": "192.168.10.254"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "076ce999-9383-425a-bb89-6ddd908376e2",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.10.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.10.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "External-subnet",
    "enable_dhcp": true,
    "network_id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:42:23Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-7：External subnet、ゲートウェイの設定例

＜Internal-subnet（192.168.20.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.20.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=Internal-subnet ※2
[root@K5-Host ]# NETWORK_ID=作成した Internal-net の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'", "allocation_pools":[{"start":"192.168.20.101", "end":"192.168.20.200"}]}}' | jq .
```

※1 サブネットアドレスで指定してください。
※2 名前は任意で指定してください。
※3 作成した Internal-net の ID で指定してください。
※4 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:43:09Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.20.101",
        "end": "192.168.20.200"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "fb20278c-9ffb-49e1-88c8-4fe7bd24ce1f",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.20.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.20.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "Internal-subnet",
    "enable_dhcp": true,
    "network_id": "139edbe8-bf0e-46dc-8281-ab319d2b6291",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:43:09Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-8：Internal-subnet、ゲートウェイの設定例

＜DMZ-subnet（192.168.30.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.30.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=DMZ-subnet ※2
[root@K5-Host ]# NETWORK_ID=作成した DMZ-net の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'"}}' | jq .
```

※1 サブネットアドレスで指定してください。
※2 名前は任意で指定してください。
※3 作成した application ネットワークの ID で指定してください。
※4 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:43:57Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.30.2",
        "end": "192.168.30.254"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "281f3ee3-fbfe-4eba-8a7e-65ff045eb0e4",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.30.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.30.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "DMZ-subnet",
    "enable_dhcp": true,
    "network_id": "4cbb2b5a-9db6-4ccc-9f7c-375c544d6d4f",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:43:57Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-9：DMZ-subnet、ゲートウェイの設定例

＜HA1-subnet（192.168.40.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.40.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=HA1-subnet ※2
[root@K5-Host ]# NETWORK_ID=作成した HA1-net の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'", "allocation_pools":[{"start":"192.168.40.100", "end":"192.168.40.200"}]}}' | jq .
```

※1 サブネットアドレスで指定してください。
※2 名前は任意で指定してください。
※3 作成した HA1-net の ID で指定してください。
※4 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:44:44Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.40.100",
        "end": "192.168.40.200"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "643a5d9e-afb6-42f2-8079-c4a8942cd59c",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.40.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.40.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "HA1-subnet",
    "enable_dhcp": true,
    "network_id": "2a3d8643-5fd5-43cc-9849-2b8aa85d0a90",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:44:44Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-10：HA1 subnet、ゲートウェイの設定例

＜Management-subnet（192.168.50.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.50.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=Management-Subnet ※2
[root@K5-Host ]# NETWORK_ID=作成した Management-net の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'"}}' | jq .
```

※1 サブネットアドレスで指定してください。
※2 名前は任意で指定してください。
※3 作成した Management-net の ID で指定してください。
※4 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:45:27Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.50.2",
        "end": "192.168.50.254"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.50.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.50.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "Management-Subnet",
    "enable_dhcp": true,
    "network_id": "bed53dcc-986b-43b9-91b1-374bc1adf2c8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:45:27Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-11：Management subnet、ゲートウェイの設定例

＜HA1-backupsubnet（192.168.60.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.60.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=HA1-backupsubnet ※2
[root@K5-Host ]# NETWORK_ID=作成した HA1-backupnet の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'", "allocation_pools":[{"start":"192.168.60.100", "end":"192.168.60.200"}]}}' | jq .
```

※5 サブネットアドレスで指定してください。
※6 名前は任意で指定してください。
※7 作成した HA1-backup ネットワークの ID で指定してください。
※8 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:46:19Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.60.100",
        "end": "192.168.60.200"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "2166cb55-2725-4d75-81e4-02390da14a74",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.60.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.60.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "HA1-backupsubnet",
    "enable_dhcp": true,
    "network_id": "57a50333-2587-467d-9a33-8d4e4649e864",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:46:19Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-12：HA1-backupsubnet、ゲートウェイの設定例

＜HA2-subnet（192.168.70.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.70.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=HA2-subnet ※2
[root@K5-Host ]# NETWORK_ID=作成した HA2-net の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'", "allocation_pools":[{"start":"192.168.70.100", "end":"192.168.70.200"}]}}' | jq .
```

※9 サブネットアドレスで指定してください。
※10 名前は任意で指定してください。
※11 作成した HA2-net の ID で指定してください。
※12 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:47:12Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.70.100",
        "end": "192.168.70.200"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "eeebfce9-590b-42cf-9995-95ddb193ef4d",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.70.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.70.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "HA2-subnet",
    "enable_dhcp": true,
    "network_id": "bbc94352-e63c-4401-a31e-e039543e57fd",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:47:12Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```

図 3-1-13：HA2 subnet、ゲートウェイの設定例

＜HA2-backupsubnet（192.168.80.0/24）＞

コマンド例

```
[root@K5-Host ]# CIDR=192.168.80.0/24 ※1
[root@K5-Host ]# SUBNET_NAME=HA2-backupsubnet ※2
[root@K5-Host ]# NETWORK_ID=作成した HA2-backupnet の ID ※3
[root@K5-Host ]# PROJECT_ID=テナントの ID ※4

[root@K5-Host ]# curl -s $NETWORK/v2.0/subnets -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"subnet": {"ip_version": 4,"cidr": "'$CIDR'","name": "'$SUBNET_NAME'","network_id": "'$NETWORK_ID'","project_id": "'$PROJECT_ID'", "allocation_pools":[{"start":"192.168.80.100", "end":"192.168.80.200"}]}}' | jq .
```

※13 サブネットアドレスで指定してください。
※14 名前は任意で指定してください。
※15 作成した HA2-backup ネットワークの ID で指定してください。
※16 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "subnet": {
    "updated_at": "2021-09-24T06:48:00Z",
    "ipv6_ra_mode": null,
    "allocation_pools": [
      {
        "start": "192.168.80.100",
        "end": "192.168.80.200"
      }
    ],
    "host_routes": [],
    "revision_number": 0,
    "ipv6_address_mode": null,
    "underlay": null,
    "id": "f89db32a-19bd-4d8f-b83b-5f317d833afa",
    "dns_nameservers": [],
    "nuage_uplink": null,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "gateway_ip": "192.168.80.1",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_l2bridge": null,
    "description": "",
    "tags": [],
    "service_types": [],
    "cidr": "192.168.80.0/24",
    "subnetpool_id": null,
    "vsd_managed": false,
    "name": "HA2-backupsubnet",
    "enable_dhcp": true,
    "network_id": "f84de3bb-28c7-44c6-ad3b-9a64dc90b6ac",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:48:00Z",
    "ip_version": 4,
    "nuagenet": null
  }
}
```


図 3-1-14：HA2-backupsubnet、ゲートウェイの設定例

3.2　仮想ルータの作成

外部接続用の仮想ルータを作成します。

① External-net 用ルータを作成します。操作は API を使用してください。(図 3-2-1 ～ 図 3-2-3)

＜ルータ作成＞

コマンド例

```
[root@K5-Host ]# ROUTER_NAME=External-router ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID  ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/routers -X POST -H "X-Auth-Token:$OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"router": {"name": "'$ROUTER_NAME'", "tenant_id": "'$PROJECT_ID'"}}' | jq .
```

※1 名前は任意で指定してください。
※2 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "router": {
    "status": "ACTIVE",
    "rt": "65534:65174",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_vnid": 7440560,
    "description": "",
    "tags": [],
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_rd": "65534:1164",
    "admin_state_up": true,
    "updated_at": "2021-09-24T06:48:28Z",
    "name": "External-router",
    "nuage_backhaul_rt": "65534:62916",
    "ecmp_count": 1,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "revision_number": 0,
    "routes": [],
    "external_gateway_info": null,
    "created_at": "2021-09-24T06:48:28Z",
    "rd": "65534:35522",
    "id": "ca944316-0d9d-4a0a-96eb-42cbf18d2607",
    "nuage_underlay": "off"
  }
}
```


図 3-2-1：Extarnal router の作成例

＜External-net 接続用インターフェースの作成＞

- サブネット：External-net に所属するサブネット
- IP アドレス：任意(ゲートウェイ IP を推奨します)

コマンド例

```
[root@K5-Host ]# PORT_NAME=External-subnetRouterPort ※1
[root@K5-Host ]# NETWORK_ID="External-net の ID"
[root@K5-Host ]# SUBNET_ID="External-subnet の ID"
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.10.1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port":{"network_id": "'$NETWORK_ID'", "name": "'$PORT_NAME'", "fixed_ips":
[{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}]}}' | jq .
```

※1 【任意】名前は任意で指定してください。

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T06:49:37Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 6,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "076ce999-9383-425a-bb89-6ddd908376e2",
        "ip_address": "192.168.10.1"
      }
    ],
    "id": "349bfba3-06f9-42e6-a250-470b0ff42ce8",
    "security_groups": [
      "e5f83e3d-c866-4a09-82c8-471515e1e118"
    ],
    "mac_address": "fa:16:3e:5d:b4:64",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "External-subnetRouterPort",
    "admin_state_up": true,
    "network_id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:49:36Z",
    "binding:vnic_type": "normal"
  }
}
```


図 3-2-2：External-net 用のインターフェースの作成例

＜インターフェースを External router にアタッチ＞

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="作成した External-router の ID"
[root@K5-Host ~]# PORT_ID="作成した External-subnetRouterPort の ID"
[root@K5-Host ~]# curl -s $NETWORK/v2.0/routers/$ROUTER_ID/add_router_interface -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port_id": "'$PORT_ID'" }' | jq .
```

実行結果例

```
{
  "network_id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
  "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
  "subnet_id": "076ce999-9383-425a-bb89-6ddd908376e2",
  "subnet_ids": [
    "076ce999-9383-425a-bb89-6ddd908376e2"
  ],
  "port_id": "349bfba3-06f9-42e6-a250-470b0ff42ce8",
  "id": "ca944316-0d9d-4a0a-96eb-42cbf18d2607"
}
```

図 3-2-3：External-net 用のインターフェースを仮想ルータにアタッチ

② VPN 接続を行うための Management ルータを作成します。操作は API を使用してください。(図 3-2-4～図 3-2-6)

＜ルータ作成＞

コマンド例

```
[root@K5-Host ]# ROUTER_NAME=Management-router ※1
[root@K5-Host ]# PROJECT_ID=テナントの ID  ※2

[root@K5-Host ]# curl -s $NETWORK/v2.0/routers -X POST -H "X-Auth-Token:$OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"router": {"name": "'$ROUTER_NAME'", "tenant_id": "'$PROJECT_ID'"}}' | jq .
```

※1 名前は任意で指定してください。
※2 Palo Alto Networks のテナント ID を指定してください。

実行結果例


```
{
  "router": {
    "status": "ACTIVE",
    "rt": "65534:7406",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_vnid": 967362,
    "description": "",
    "tags": [],
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_rd": "65534:56148",
    "admin_state_up": true,
    "updated_at": "2021-09-24T06:51:03Z",
    "name": "Management-router",
    "nuage_backhaul_rt": "65534:42056",
    "ecmp_count": 1,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "revision_number": 0,
    "routes": [],
    "external_gateway_info": null,
    "created_at": "2021-09-24T06:51:03Z",
    "rd": "65534:51726",
    "id": "3092eb35-8193-4ee9-957c-db5d9a64c9f1",
    "nuage_underlay": "off"
  }
}
```


図 3-2-4：Management router の作成例

＜Management-net 接続用インターフェースの作成（図 3-2-5)＞

- サブネット：Management-net に所属するサブネット
- IP アドレス：任意(ゲートウェイ IP を推奨します)

コマンド例

```
[root@K5-Host ]# PORT_NAME=Management-SubnetRouterPort ※1
[root@K5-Host ]# NETWORK_ID="Management-net の ID"
[root@K5-Host ]# SUBNET_ID="Management-subnet の ID"
[root@K5-Host ]# FIXED_IP_ADDRESS=192.168.50.1
[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port":{"network_id": "'$NETWORK_ID'", "name": "'$PORT_NAME'", "fixed_ips":
[{"subnet_id": "'$SUBNET_ID'", "ip_address": "'$FIXED_IP_ADDRESS'"}]}}' | jq .
```

※1 【任意】名前は任意で指定してください。

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T06:52:03Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 6,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b",
        "ip_address": "192.168.50.1"
      }
    ],
    "id": "2aca575a-88f5-4cd2-b036-0ad592bcc2c0",
    "security_groups": [
      "e5f83e3d-c866-4a09-82c8-471515e1e118"
    ],
    "mac_address": "fa:16:3e:38:10:f0",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "Management-SubnetRouterPort",
    "admin_state_up": true,
    "network_id": "bed53dcc-986b-43b9-91b1-374bc1adf2c8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:52:03Z",
    "binding:vnic_type": "normal"
  }
}
```


図 3-2-5： Management-router 用のインターフェースの作成例

＜インターフェースを仮想ルータにアタッチ＞

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="Management-router の ID"
[root@K5-Host ~]# PORT_ID=" Management-SubnetRouterPort の ID"
[root@K5-Host ~]# curl -s $NETWORK/v2.0/routers/$ROUTER_ID/add_router_interface -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port_id": "'$PORT_ID'" }' | jq .
```

実行結果例

```
{
  "network_id": "bed53dcc-986b-43b9-91b1-374bc1adf2c8",
  "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
  "subnet_id": "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b",
  "subnet_ids": [
    "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b"
  ],
  "port_id": "2aca575a-88f5-4cd2-b036-0ad592bcc2c0",
  "id": "3092eb35-8193-4ee9-957c-db5d9a64c9f1"
}
```

図 3-2-6：Management-router 用のインターフェースをアタッチ

③　仮想ルータ経由でインターネットにアクセスするため、External-router のゲートウェイ設定で外部仮想ネットワークを設定します。(図 3-2-7)

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="作成した External-router の ID"
[root@K5-Host ~]# EXT_NET_ID="グローバル IP ネットワークの ID" ※1
[root@K5-Host ~]# curl -s  $NETWORK/v2.0/routers/$ROUTER_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:  application/json"  -d  '{"router":  {"external_gateway_info":  {  "network_id": "'$EXT_NET_ID'"}}}' | jq .
```

※1　本例では fip-net を指定します。

実行結果例


```
{
  "router": {
    "status": "ACTIVE",
    "rt": "65534:65174",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_vnid": 7440560,
    "description": "",
    "tags": [],
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_rd": "65534:1164",
    "admin_state_up": true,
    "updated_at": "2021-09-24T06:53:48Z",
    "name": "External-router",
    "nuage_backhaul_rt": "65534:62916",
    "ecmp_count": 1,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "revision_number": 3,
    "routes": [],
    "external_gateway_info": {
      "network_id": "5234aa88-9cd8-49bd-b613-d0006eacb87b",
      "enable_snat": true,
      "external_fixed_ips": [
        {
          "subnet_id": "f345719a-0127-4410-a5ab-af5f795e9ac3",
          "ip_address": "133.162.84.120"
        }
      ]
    },
    "created_at": "2021-09-24T06:48:28Z",
    "rd": "65534:35522",
    "id": "ca944316-0d9d-4a0a-96eb-42cbf18d2607",
    "nuage_underlay": "snat"
  }
}
```


図 3-2-7：仮想ルータのゲートウェイ設定で外部仮想ネットワークを設定

④ VPN 接続で使用するため、Management-router のゲートウェイ設定で外部仮想ネットワークを設定します。(図 3-2-8)

コマンド例

```
[root@K5-Host ~]# ROUTER_ID="作成した Management-router の ID"
[root@K5-Host ~]# EXT_NET_ID="グローバル IP ネットワークの ID" ※1
[root@K5-Host ~]# curl -s  $NETWORK/v2.0/routers/$ROUTER_ID -X PUT -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"router": {"external_gateway_info": {  "network_id": "'$EXT_NET_ID'"}}}' | jq .
```

※1 本例では fip-net を指定します。

実行結果例


```
{
  "router": {
    "status": "ACTIVE",
    "rt": "65534:7406",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_vnid": 967362,
    "description": "",
    "tags": [],
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "nuage_backhaul_rd": "65534:56148",
    "admin_state_up": true,
    "updated_at": "2021-09-24T06:55:18Z",
    "name": "Management-router",
    "nuage_backhaul_rt": "65534:42056",
    "ecmp_count": 1,
    "net_partition": "bede9aa2-f720-4671-90fd-6b342f9564ac",
    "revision_number": 3,
    "routes": [],
    "external_gateway_info": {
      "network_id": "5234aa88-9cd8-49bd-b613-d0006eacb87b",
      "enable_snat": true,
      "external_fixed_ips": [
        {
          "subnet_id": "f345719a-0127-4410-a5ab-af5f795e9ac3",
          "ip_address": "133.162.84.21"
        }
      ]
    },
    "created_at": "2021-09-24T06:51:03Z",
    "rd": "65534:51726",
    "id": "3092eb35-8193-4ee9-957c-db5d9a64c9f1",
    "nuage_underlay": "snat"
  }
}
```


図 3-2-8：仮想ルータのゲートウェイ設定で外部仮想ネットワークを設定

3.3　キーペアについて

Palo Alto Networks はキーペアに対応していないため、作成したキーペアを利用して、ログインはできません。

そのため、キーペアは割り当てをしなくて構いません。

3.4 セキュリティグループの作成

Palo Alto Networks 用のセキュリティグループを作成します。API で以下を実施してください。

① Palo Alto Networks 用のセキュリティグループを作成します。(図 3-4-1)

コマンド例

```
[root@K5-Host ~]# SG_NAME=Paloalto-SG ※1
[root@K5-Host ~]# SG_STATEFUL=false
[root@K5-Host ~]# curl -s $NETWORK/v2.0/security-groups -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"security_group": {"name": "'$SG_NAME'", "stateful":
"'${SG_STATEFUL}'"}}' | jq .
```

※1 【任意】名前は任意で指定してください。

実行結果例


```
{
  "security_group": {
    "description": "",
    "tags": [],
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:56:05Z",
    "updated_at": "2021-09-24T06:56:05Z",
    "security_group_rules": [
      {
        "direction": "egress",
        "protocol": null,
        "description": null,
        "tags": [],
        "port_range_max": null,
        "updated_at": "2021-09-24T06:56:05Z",
        "revision_number": 0,
        "id": "9b6de908-cf37-45aa-8cef-71729bdd911e",
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "created_at": "2021-09-24T06:56:05Z",
        "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
        "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
        "port_range_min": null,
        "ethertype": "IPv4",
        "project_id": "df5b1a54f3994aac9ecf0553bd65bbee"
      },
      {
        "direction": "egress",
        "protocol": null,
        "description": null,
        "tags": [],
        "port_range_max": null,
        "updated_at": "2021-09-24T06:56:05Z",
        "revision_number": 0,
        "id": "ce710c82-cd31-444a-8cb1-ea3aec51717b",
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "created_at": "2021-09-24T06:56:05Z",
        "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
        "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
        "port_range_min": null,
```

```
        "ethertype": "IPv6",
        "project_id": "df5b1a54f3994aac9ecf0553bd65bbee"
      }
    ],
    "stateful": false,
    "revision_number": 2,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
    "name": "Paloalto-SG"
  }
}
```


図 3-4-1: Palo Alto Networks 用のセキュリティグループを作成

② 作成したセキュリティグループのルールを定義します。API で以下を実施してください。Palo Alto Networks は内部で FW の設定を行うため、本例では以下の推奨ルールを設定しております。

【推奨ルール】

egress IPv6 - (全許可)

egress IPv4 - (全許可)

ingress IPv4 icmp 0.0.0.0/0 (全許可)

ingress IPv4 tcp 1-65535 0.0.0.0/0(全許可)

ingress IPv4 udp 1-65535 0.0.0.0/0(全許可)

egress プロトコル 99 - (全許可)

ingress プロトコル 99 - (全許可)

※Palo Alto Networks 内部で FW 機能を有しているため、セキュリティグループはすべて許可します。

■ tcp をすべて許可するルールを作成し、適用します。(図 3-4-2)

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=tcp
[root@K5-HOST ]# MIN_PORT_NUM=1
[root@K5-HOST ]# MAX_PORT_NUM=65535
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","port_range_min": '$MIN_PORT_NUM',"port_range_max": '$MAX_PORT_NUM',"protocol": "'$PROTCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例

```
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": "tcp",
    "description": "",
    "ethertype": "IPv4",
    "remote_ip_prefix": "0.0.0.0/0",
    "port_range_max": 65535,
    "updated_at": "2021-09-24T06:56:59Z",
    "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
    "port_range_min": 1,
    "revision_number": 0,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:56:59Z",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "124ce0a7-d84a-485a-b521-1323fb0c877e"
  }
}
```

図 3-4-2:tcp 許可ルールを作成

■ udp をすべて許可するルールを作成し、適用します。(図 3-4-3)

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=udp
[root@K5-HOST ]# MIN_PORT_NUM=1
[root@K5-HOST ]# MAX_PORT_NUM=65535
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","port_range_min":
'$MIN_PORT_NUM',"port_range_max": '$MAX_PORT_NUM',"protocol": "'$PROTCOL'","remote_ip_prefix":
"'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例

```
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": "udp",
    "description": "",
    "ethertype": "IPv4",
    "remote_ip_prefix": "0.0.0.0/0",
    "port_range_max": 65535,
    "updated_at": "2021-09-24T06:57:41Z",
    "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
    "port_range_min": 1,
    "revision_number": 0,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:57:41Z",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "a68a1050-2dfe-4eb8-a051-ef3976a63e14"
  }
}
```

図 3-4-3:udp 許可ルールを作成

■ icmp をすべて許可するルールを作成し、適用します。(図 3-4-4)

コマンド例

```
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=icmp
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'","protocol":
"'$PROTCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例

```
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": "icmp",
    "description": "",
    "ethertype": "IPv4",
    "remote_ip_prefix": "0.0.0.0/0",
```

```
    "port_range_max": null,
    "updated_at": "2021-09-24T06:58:19Z",
    "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
    "port_range_min": null,
    "revision_number": 0,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T06:58:19Z",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "83f914a1-3669-4db3-9c2d-d20113b3e523"
  }
}
```

図 3-4-4：icmp 許可ルールを作成

■ プロトコル 99 番の通信をすべて許可するルールを作成し、適用します。(図 3-4-5)

コマンド例

```
# ingress ルールの作成
[root@K5-HOST ]# DIRECTION=ingress
[root@K5-HOST ]# PROTCOL=99
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'" ,"protocol": "'$PROTCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .

# egress ルールの作成
[root@K5-HOST ]# DIRECTION=egress
[root@K5-HOST ]# PROTCOL=99
[root@K5-HOST ]# REMOTE_IP=0.0.0.0/0
[root@K5-HOST ]# SG_ID="作成したセキュリティグループの ID"
[root@K5-HOST ]# curl -s $NETWORK/v2.0/security-group-rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"security_group_rule":{"direction": "'$DIRECTION'" ,"protocol": "'$PROTCOL'","remote_ip_prefix": "'$REMOTE_IP'", "security_group_id": "'$SG_ID'"}}' | jq .
```

実行結果例

```
# ingress ルール作成結果
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "ingress",
    "protocol": "99",
    "description": "",
    "ethertype": "IPv4",
    "remote_ip_prefix": "0.0.0.0/0",
    "port_range_max": null,
    "updated_at": "2022-03-28T05:13:08Z",
    "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
    "port_range_min": null,
    "revision_number": 0,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2022-03-28T05:13:08Z",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "4382c569-d994-4e2b-a0f9-d390dfd5422c"
  }
}
```

```
# egress ルール作成結果
{
  "security_group_rule": {
    "remote_group_id": null,
    "direction": "egress",
    "protocol": "99",
    "description": "",
    "ethertype": "IPv4",
    "remote_ip_prefix": "0.0.0.0/0",
    "port_range_max": null,
    "updated_at": "2022-03-28T05:14:16Z",
    "security_group_id": "c6433ceb-d167-4d78-9500-653ae240b4cf",
    "port_range_min": null,
    "revision_number": 0,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2022-03-28T05:14:16Z",
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "id": "e8485b78-872a-4db9-b8fa-1ef48dc7c0dc"
  }
}
```

図 3-4-5:プロトコル 99 番許可ルールを作成

3.5　アンチアフィニティの設定

Palo Alto Networks で冗長構成を組む場合は、異なるホスト上で動作するよう配置するために、アンチアフィニティを設定します。

(図 3-5-1)

コマンド例

```
[root@K5-Host ]# NAME=Paloalto_ServerGr
[root@K5-Host ]# POLICY="anti-affinity"
[root@K5-Host ]# curl -k $COMPUTE/v2.1/$PROJECT_ID/os-server-groups -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:application/json" -d '{"server_group":{ "name": "'$NAME'", "policies": [ "'$POLICY'" ]}}' | jq .
```

実行結果例

```
{
  "server_group": {
    "members": [],
    "metadata": {},
    "id": "70673576-57ef-4133-9df3-3c02ea6b5396",
    "policies": [
      "anti-affinity"
    ],
    "name": "Paloalto_ServerGr"
  }
}
```

図 3-5-1：アンチアフィニティの設定

3.6　Management-net 用 FW の作成

①　Firewall ルールの作成

本手順では、以下のポリシーと設定します。(図 3-6-1～3-6-4)

その他のルールについては要件に合わせ設定をしてください。

1. VPN クライアントアドレスから Management-net への通信許可
2. 0.0.0.0/0 から VPN エンドポイントへの接続許可
3. Management-netから0.0.0.0/0への通信許可
4. その他の拒否設定

＜VPN クライアントアドレスから Management-net への通信許可＞

コマンド例

```
[root@K5-Host ]# RULE_NAME=ALLOW_VPNCIDER
[root@K5-Host ]# ACTION=allow
[root@K5-Host ]# SOURCE_IP=192.168.246.0/24
[root@K5-Host ]# DEST_IP=192.168.50.0/24

[root@K5-Host ]# curl -s $NETWORK/v2.0/fw/firewall_rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"firewall_rule": {"name": "'$RULE_NAME'","action": "'$ACTION'","source_ip_address": "'$SOURCE_IP'", "destination_ip_address": "'$DEST_IP'", "enabled": true}}' | jq .
```

実行結果例

```
{
  "firewall_rule": {
    "protocol": null,
    "description": "",
    "source_port": null,
    "source_ip_address": "192.168.246.0/24",
    "destination_ip_address": "192.168.50.0/24",
    "firewall_policy_id": null,
    "position": null,
    "destination_port": null,
    "id": "981d1b0a-4918-4066-9599-6cda21870848",
    "name": "ALLOW_VPNCIDER",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "enabled": true,
    "action": "allow",
    "ip_version": 4,
    "shared": false
  }
}
```

図 3-6-1：Firewall ルール作成①

＜Management-net から 0.0.0.0/0 への通信許可＞

コマンド例

```
[root@K5-Host ]# RULE_NAME=ALLOW_EGRESS
[root@K5-Host ]# ACTION=allow
[root@K5-Host ]# SOURCE_IP=192.168.50.0/24
[root@K5-Host ]# DEST_IP=0.0.0.0/0

[root@K5-Host ]# curl -s $NETWORK/v2.0/fw/firewall_rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"firewall_rule": {"name": "'$RULE_NAME'","action": "'$ACTION'","source_ip_address": "'$SOURCE_IP'", "destination_ip_address": "'$DEST_IP'", "enabled": true}}' | jq .
```

実行結果例

```
{
  "firewall_rule": {
    "protocol": null,
    "description": "",
    "source_port": null,
    "source_ip_address": "192.168.50.0/24",
    "destination_ip_address": "0.0.0.0/0",
    "firewall_policy_id": null,
    "position": null,
    "destination_port": null,
    "id": "d6b525f5-8112-4350-9100-b0399ed2b356",
    "name": "ALLOW_EGRESS",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "enabled": true,
    "action": "allow",
    "ip_version": 4,
    "shared": false
  }
}
```

図 3-6-2：Firewall ルール作成②

＜0.0.0.0/0 から VPN エンドポイントへの接続許可＞

コマンド例

```
[root@K5-Host ]# RULE_NAME=ALLOW_VPNACCESS
[root@K5-Host ]# ACTION=allow
[root@K5-Host ]# SOURCE_IP=0.0.0.0/0
[root@K5-Host ]# DEST_IP=192.168.90.5

[root@K5-Host ]# curl -s $NETWORK/v2.0/fw/firewall_rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"firewall_rule": {"name": "'$RULE_NAME'","action": "'$ACTION'","source_ip_address": "'$SOURCE_IP'", "destination_ip_address": "'$DEST_IP'", "enabled": true}}' | jq .
```

実行結果例

```
{
  "firewall_rule": {
    "protocol": null,
    "description": "",
    "source_port": null,
    "source_ip_address": "0.0.0.0/0",
    "destination_ip_address": "192.168.90.5",
    "firewall_policy_id": null,
    "position": null,
    "destination_port": null,
    "id": "140ecd9b-de48-4bec-9b82-ef72402d97cb",
    "name": "ALLOW_VPNACCESS",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "enabled": true,
    "action": "allow",
    "ip_version": 4,
    "shared": false
  }
}
```

図 3-6-3：Firewall ルール作成③

＜その他拒否設定＞

※以下は設定例です。拒否設定内容は要件により変更してください。

コマンド例

```
[root@K5-Host ]# RULE_NAME=ALL_DENY
[root@K5-Host ]# ACTION=deny

[root@K5-Host ]# curl -s $NETWORK/v2.0/fw/firewall_rules -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"firewall_rule": {"name": "'$RULE_NAME'", "action": "'$ACTION'", "enabled": true}}' | jq .
```

実行結果例

```
{
  "firewall_rule": {
    "protocol": null,
    "description": "",
    "source_port": null,
    "source_ip_address": null,
    "destination_ip_address": null,
    "firewall_policy_id": null,
    "position": null,
    "destination_port": null,
    "id": "91e16a07-5b1c-4d8b-9388-2c649c83a012",
    "name": "ALL_DENY",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "enabled": true,
    "action": "deny",
    "ip_version": 4,
    "shared": false
  }
}
```

図 3-6-4：Firewall ルール作成④

② Firewall ポリシーの作成

以下の API で Firewall ポリシーを作成します。(図 3-6-5)

コマンド例

```
[root@K5-Host ]# ALLOW_VPNCIDER_ID="ALLOW_VPNCIDER ルールの ID"
[root@K5-Host ]# ALLOW_VPNACCESS_ID="ALLOW_VPNACCESS ルールの ID"
[root@K5-Host ]# ALLOW_EGRESS_ID="ALLOW_EGRESS ルールの ID"
[root@K5-Host ]# ALL_DENY_ID="ALL_DENY ルールの ID"
[root@K5-Host ]# POLICY_NAME=Management_FW_POLICY

[root@K5-Host ]# curl -s $NETWORK/v2.0/fw/firewall_policies -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"firewall_policy": {"firewall_rules": ["'$ALLOW_VPNCIDER_ID'","'$ALLOW_VPNACCESS_ID'","'$ALLOW_EGRESS_ID'","'$ALL_DENY_ID'"],"name": "'$POLICY_NAME'"}}' | jq .
```

実行結果例

```
{
  "firewall_policy": {
    "name": "Management_FW_POLICY",
    "firewall_rules": [
      "981d1b0a-4918-4066-9599-6cda21870848",
      "140ecd9b-de48-4bec-9b82-ef72402d97cb",
      "d6b525f5-8112-4350-9100-b0399ed2b356",
      "91e16a07-5b1c-4d8b-9388-2c649c83a012"
    ],
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "audited": false,
    "shared": false,
    "id": "8e4312f0-3d79-442a-adc6-cc4e35572006",
    "description": ""
  }
}
```

図 3-6-5：Firewall ポリシー作成

③ Firewall の作成

以下の API で Firewall を作成し、Management-router を紐づけします。(図 3-6-6)

コマンド例

```
[root@K5-Host ]# FIREWALL_POLICY_ID="Management_FIREWALL_POLICY の ID"
[root@K5-Host ]# ROUTER_ID="Management-router の ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/fw/firewalls -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"firewall": {"admin_state_up": true,"firewall_policy_id": "'$FIREWALL_POLICY_ID'","router_ids": ["'$ROUTER_ID'"]}}' | jq .
```

実行結果例

```
{
  "firewall": {
    "status": "ACTIVE",
    "router_ids": [
      "3092eb35-8193-4ee9-957c-db5d9a64c9f1"
    ],
    "name": "",
    "admin_state_up": true,
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "firewall_policy_id": "8e4312f0-3d79-442a-adc6-cc4e35572006",
    "id": "ce486ab7-06a5-4ebf-98a2-889e82f3d191",
    "description": ""
  }
}
```

図 3-6-6：Firewall 作成

3.7　VPN 接続の作成

①　VPN サービスの作成

Palo Alto Networks に SSH アクセスするための VPN サービスを作成します。

下記の通り、API で作成してください。(図 3-7-1)

コマンド例

```
[root@K5-Host ~]# NFV="API リファレンスに記載の VPN 作成 API のエンドポイント" ※1
[root@K5-Host ~]# SUBNET_ID="Management-subnet の ID" ※2
[root@K5-Host ~]# ROUTER_ID="Management-router の ID" ※3
[root@K5-Host ~]# VPN_NAME="VPN 接続名" ※4
[root@K5-Host ~]# curl -k $NFV/vpn/nfv/vpnservices -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"vpnservice": {"subnet_id": "'$SUBNET_ID'","router_id": "'$ROUTER_ID'","name": "'$VPN_NAME'","admin_state_up": true}}' | jq .
```

※1　$NFV は API リファレンスに記載のエンドポイントを指定してください。
https://doc.cloud.global.fujitsu.com/lib/iaas/jp/api-reference/v3/web/k5-iaas-api-reference/reference/nfv_vs_create_vpn_service.html
※2　前手順で作成した Management-Subnet を指定してください
※3　前手順で作成した Management-router を指定してください。
※4　任意のサービス名を指定してください

実行結果例

```
{
  "vpnservice": {
    "id": "708694",
    "subnet_id": "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b",
    "router_id": "3092eb35-8193-4ee9-957c-db5d9a64c9f1",
    "name": "Paloalto-VPN",
    "admin_state_up": true
  }
}
```

図 3-7-1：VPN サービスの設定

② SSL-VPN 接続の作成

作成した VPN サービスに新たに SSL-VPN 接続を作成します。

下記の通り、API で作成してください。(図 3-7-2)

※SSL-VPN 接続の作成には数分かかります。

コマンド例

```
[root@K5-Host ~]# NFV="API リファレンスに記載の VPN 作成 API のエンドポイント" ※1
[root@K5-Host ~]# SSL_NAME="SSL-VPN 接続名" ※2
[root@K5-Host ~]# CIDR="192.168.246.0/24" ※3
[root@K5-Host ~]# VPN_SERVICE="VPN サービスの ID" ※4
[root@K5-Host ~]# curl -k $NFV/vpn/nfv/ssl-vpn-v2-connections -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type:  application/json" -d '{"ssl_vpn_v2_connection": {"name": "'$SSL_NAME'","admin_state_up":
true,"client_address_pool_cidr": "'$CIDR'","vpnservice_id": "'$VPN_SERVICE'"}}' | jq .
```

※1 $NFV は API リファレンスに記載のエンドポイントを指定してください。
https://doc.cloud.global.fujitsu.com/lib/iaas/jp/api-reference/v3/web/k5-iaas-api-reference/reference/nfv_vs_create_vpn_service.html
※2 任意の接続名を指定してください。
※3 任意のアドレス範囲をサブネット形式で指定してください。
※4 前手順で作成した VPN サービスの ID を指定してください。

実行結果例

```
{
  "ssl_vpn_v2_connection": {
    "id": "708696",
    "name": "Paloalto_SSL_VPN",
    "admin_state_up": true,
    "client_address_pool_cidr": "192.168.246.0/24",
    "vpnservice_id": "708694"
  }
}
```

図 3-7-2：VPN 接続の設定

③ SSL-VPN 接続の状態確認

作成した VPN 接続の情報を取得します。

下記のとおり、API で作成してください。(図 3-7-3)

コマンド例

```
[root@K5-Host ~]# NFV="API リファレンスに記載の VPN 作成 API のエンドポイント" ※1
[root@K5-Host ~]# SSL_VPN_ID="作成した SSL-VPN 接続の ID"

[root@K5-Host ~]# curl -k $NFV/vpn/nfv/ssl-vpn-v2-connections/${SSL_VPN_ID} -X GET -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" | jq .
```

※1 $NFV は API リファレンスに記載のエンドポイントを指定してください。
https://doc.cloud.global.fujitsu.com/lib/iaas/jp/api-reference/v3/web/k5-iaas-api-reference/reference/nfv_vs_create_vpn_service.html

実行結果例


```
{
  "ssl_vpn_v2_connection": {
    "status": "ACTIVE",
    "tenant_id": "afec1e70779e4467bd2e6a56972c6dc8",
    "name": "Paloalto_SSL_VPN",
    "admin_state_up": true,
    "client_address_pool_cidr": "192.168.246.0/24",
    "credential_id": "",
    "vpnservice_id": "749414",
    "id": "749476",
    "extension": false,
    "availability_zone": null,
    "protocol": "tcp",
    "security_groups": null,
    "access_points": [
      {
        "External_address": "133.162.74.173",
        "Internal_gateway": null,
        "client_address_pool_cidr": "192.168.246.0/24",
        "floatingips": null
      }
    ],
    "detail": ""
  }
}
```


図 3-7-3：VPN 接続の状態確認

本章では、 Palo Alto Networks および関連する仮想サーバの作成手順について説明します。

■本章に記載のコマンドは、jq コマンドが使用できる環境で実行してください。

■本章および次章の Palo Alto Networks 仮想サーバの構築は、必ず記載されている手順どおりに実施してください。

トラブルや手順ミスなどで継続できない場合、構築中の仮想サーバを破棄したうえで本章からやり直してください。

4.1　Palo Alto Networks 用共有ポートの作成

Palo Alto Networks の active と passive で共有するポートを作成します。

＜External-net 用共有ポート(192.168.10.100)＞

External-net で使用する共有ポートを作成します。

コマンド例

```
[root@K5-Host ]# PORT_NAME=External-virtual-port
[root@K5-Host ]# IP_ADDRESS=192.168.10.100
[root@K5-Host ]# NETWORK_ID="External-net ネットワークの ID"
[root@K5-Host ]# SG_ID=" Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true, "name": "'$PORT_NAME'", "network_id": "'$NETWORK_ID'", "fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}], "security_groups": ["'$SG_ID'"], "device_owner": "nuage:vip"}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:14:07Z",
    "device_owner": "nuage:vip",
    "revision_number": 6,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "076ce999-9383-425a-bb89-6ddd908376e2",
        "ip_address": "192.168.10.100"
      }
    ],
    "id": "a9eab7c2-344b-4432-87ff-71a7cccb47e6",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:7f:de:f2",
    "nuage_floatingip": null,
```

```
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "name": "External-virtual-port",
    "admin_state_up": true,
    "network_id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:14:07Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-1-1：共有ポートの作成①

＜Internal-net 用共有ポート(192.168.20.100)＞

Internal-net で使用する共有ポートを作成します。

コマンド例

```
[root@K5-Host ]# PORT_NAME=Internal-virtual-port
[root@K5-Host ]# IP_ADDRESS=192.168.20.100
[root@K5-Host ]# NETWORK_ID="Internal-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port": {"admin_state_up": true, "name": "'$PORT_NAME'", "network_id":
"'$NETWORK_ID'", "fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}], "security_groups": ["'$SG_ID'"],
"device_owner": "nuage:vip"}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:15:00Z",
    "device_owner": "nuage:vip",
    "revision_number": 6,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "fb20278c-9ffb-49e1-88c8-4fe7bd24ce1f",
        "ip_address": "192.168.20.100"
      }
    ],
    "id": "c1edc41f-5c26-4b03-a33e-5b7db6b39dcb",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:ba:9f:49",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "name": "Internal-virtual-port",
    "admin_state_up": true,
    "network_id": "139edbe8-bf0e-46dc-8281-ab319d2b6291",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:15:00Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-1-2：共有ポートの作成②

＜DMZ-net 用共有ポート(192.168.30.100)＞

DMZ-Net で使用する共有ポートを作成します。

コマンド例

```
[root@K5-Host ]# PORT_NAME=DMZ-virtual-port
[root@K5-Host ]# IP_ADDRESS=192.168.30.100
[root@K5-Host ]# NETWORK_ID="DMZ-Net ネットワークの ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true, "name": "'$PORT_NAME'", "network_id": "'$NETWORK_ID'", "fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}], "security_groups": ["'$SG_ID'"], "device_owner": "nuage:vip"}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:15:48Z",
    "device_owner": "nuage:vip",
    "revision_number": 6,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "281f3ee3-fbfe-4eba-8a7e-65ff045eb0e4",
        "ip_address": "192.168.30.100"
      }
    ],
    "id": "bdfd4553-8d13-4226-a28b-ad5c360ed922",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:24:65:ff",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "name": "DMZ-virtual-port",
    "admin_state_up": true,
    "network_id": "4cbb2b5a-9db6-4ccc-9f7c-375c544d6d4f",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:15:47Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-1-3：共有ポートの作成③

4.2 Palo Alto Networks の作成(active)

＜ポートの作成＞

Palo Alto Networks にアタッチするポートを作成します。

■External-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=External-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.10.11
[root@K5-Host ]# NETWORK_ID="External-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"
[root@K5-Host ]# VIP=192.168.10.100

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true,"name": "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled": true,"allowed_address_pairs": [{"ip_address": "'$VIP'"}],"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [
      {
        "ip_address": "192.168.10.100",
        "mac_address": "fa:16:3e:16:72:19"
      }
    ],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:17:11Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "076ce999-9383-425a-bb89-6ddd908376e2",
        "ip_address": "192.168.10.11"
      }
    ],
    "id": "ccf071d8-8597-460a-97a2-78ab971b55ee",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:16:72:19",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "External-port-active",
    "admin_state_up": true,
    "network_id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
```

```
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:17:11Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-2-1：External-net 用ポートの作成

■Internal-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=Internal-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.20.11
[root@K5-Host ]# NETWORK_ID="Internal-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"
[root@K5-Host ]# VIP=192.168.20.100

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true,"name": "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled": true,"allowed_address_pairs": [{"ip_address": "'$VIP'"}],"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [
      {
        "ip_address": "192.168.20.100",
        "mac_address": "fa:16:3e:63:da:a7"
      }
    ],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:18:13Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "fb20278c-9ffb-49e1-88c8-4fe7bd24ce1f",
        "ip_address": "192.168.20.11"
      }
    ],
    "id": "ef2326fb-8f85-4585-9fea-89f985ff03ae",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:63:da:a7",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "Internal-port-active",
    "admin_state_up": true,
    "network_id": "139edbe8-bf0e-46dc-8281-ab319d2b6291",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:18:12Z",
    "binding:vnic_type": "normal"
  }
}
```

図 4-2-2：Internal-net 用ポートの作成

■DMZ-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=DMZ-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.30.11
[root@K5-Host ]# NETWORK_ID="DMZ-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"
[root@K5-Host ]# VIP=192.168.30.100

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"allowed_address_pairs":  [{"ip_address": "'$VIP'"}],"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [
      {
        "ip_address": "192.168.30.100",
        "mac_address": "fa:16:3e:f7:51:12"
      }
    ],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:19:08Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "281f3ee3-fbfe-4eba-8a7e-65ff045eb0e4",
        "ip_address": "192.168.30.11"
      }
    ],
    "id": "8513915b-1d11-4405-a796-d5c668b11233",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:f7:51:12",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "DMZ-port-active",
    "admin_state_up": true,
    "network_id": "4cbb2b5a-9db6-4ccc-9f7c-375c544d6d4f",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:19:08Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-2-3：Internal-net 用ポートの作成

■HA1-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA1-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.40.11
[root@K5-Host ]# NETWORK_ID="HA1-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:21:28Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "643a5d9e-afb6-42f2-8079-c4a8942cd59c",
        "ip_address": "192.168.40.11"
      }
    ],
    "id": "f7f1be79-7db8-4a76-8858-d1e319ab99a5",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:03:0a:98",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA1-port-active",
    "admin_state_up": true,
    "network_id": "2a3d8643-5fd5-43cc-9849-2b8aa85d0a90",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:21:27Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-2-4：HA1-network 用ポートの作成

■HA2-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA2-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.70.21
[root@K5-Host ]# NETWORK_ID="HA2-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:22:19Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "eeebfce9-590b-42cf-9995-95ddb193ef4d",
        "ip_address": "192.168.70.21"
      }
    ],
    "id": "346c62dd-c732-4f3d-9570-74c2bb7d7f1b",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:f2:f0:95",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA2-port-active",
    "admin_state_up": true,
    "network_id": "bbc94352-e63c-4401-a31e-e039543e57fd",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:22:19Z",
    "binding:vnic_type": "normal"
  }
}
```

図 4-2-5：HA1-network 用ポートの作成

■Management-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=Management-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.50.11
[root@K5-Host ]# NETWORK_ID="Management-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:23:08Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b",
        "ip_address": "192.168.50.11"
      }
    ],
    "id": "a4a8cfd9-bc5a-4135-9e1a-3cbc59aa9ca2",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:23:9e:17",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "Management-port-active",
    "admin_state_up": true,
    "network_id": "bed53dcc-986b-43b9-91b1-374bc1adf2c8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:23:08Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-2-6：Management-net 用ポートの作成

■HA1-backupnet 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA1backup-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.60.11
[root@K5-Host ]# NETWORK_ID="HA1-backupnet の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:24:09Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "2166cb55-2725-4d75-81e4-02390da14a74",
        "ip_address": "192.168.60.11"
      }
    ],
    "id": "ff8d86e8-152b-4866-bafe-cb954fb7d29d",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:a0:50:a3",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA1backup-port-active",
    "admin_state_up": true,
    "network_id": "57a50333-2587-467d-9a33-8d4e4649e864",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:24:09Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-2-7：HA1-backupnet 用ポートの作成①

■HA2-backupnet 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA2backup-port-active
[root@K5-Host ]# IP_ADDRESS=192.168.80.21
[root@K5-Host ]# NETWORK_ID="HA1-backupnet の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id":"'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address":"'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:25:23Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "f89db32a-19bd-4d8f-b83b-5f317d833afa",
        "ip_address": "192.168.80.21"
      }
    ],
    "id": "333c043c-ef94-41f7-87a0-bfefe1a5ca1f",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:92:a8:b1",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA2backup-port-active",
    "admin_state_up": true,
    "network_id": "f84de3bb-28c7-44c6-ad3b-9a64dc90b6ac",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:25:23Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-2-8：HA1-backupnet 用ポートの作成②

＜Palo Alto Networks の作成＞

Palo Alto Networks の active を作成します。アンチアフィニティで作成するので、API で実行してください。

コマンド例

```
[root@K5-Host ~]# VM_NAME=Paloalto_active ※1
[root@K5-Host ~]# IMAGE_REF_ID=“Palo Alto Networks の ImageID”
[root@K5-Host ~]# FLAVOR_ID=“Palo Alto Networks の FlavorID” ※2
[root@K5-Host ~]# VOL_SIZE=60 ※3
[root@K5-Host ~]# DEVICE_NAME=/dev/vda ※4
[root@K5-Host ~]# SOURCE=image ※5
[root@K5-Host ~]# DESTINATION=volume ※6
[root@K5-Host ~]# ISDELETE=true ※7
[root@K5-Host ~]# EXTERNAL_PORT=“External-port-active の ID”
[root@K5-Host ~]# INTERNAL_PORT=“Internal-port-active の ID”
[root@K5-Host ~]# DMZ_PORT=“DMZ-port-active の ID”
[root@K5-Host ~]# HA1_PORT=“HA1-port-active の ID”
[root@K5-Host ~]# HA2_PORT=“HA2-port-active の ID”
[root@K5-Host ~]# MANAGEMENT_PORT=“Management-port-active の ID”
[root@K5-Host ~]# HA1backup_PORT=“HA1backup-port-active の ID”
[root@K5-Host ~]# HA2backup_PORT=“HA2backup-port-active の ID”
[root@K5-Host ~]# SG_NAME=“「SecurityGroup の作成で作成した」グループ名”
[root@K5-Host ~]# GROUP_ID=“アンチアフィニティの設定で作成したグループ ID” ※8

[root@K5-Host ~]# curl -k $COMPUTE/v2.1/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '
{"server":{"name":"'$VM_NAME'","imageRef":"","flavorRef":"'$FLAVOR_ID'","block_device_mapping_v2":[{"boot_i
ndex":"0","uuid":"'$IMAGE_REF_ID'","volume_size":"'$VOL_SIZE'","device_name":"'$DEVICE_NAME'","source_type"
:"'$SOURCE'","destination_type":"'$DESTINATION'","delete_on_termination":"'$ISDELETE'"}],"networks":[{"port
":"'$MANAGEMENT_PORT'"},{"port":"'$EXTERNAL_PORT'"},{"port":"'$INTERNAL_PORT'"},{"port":"'$DMZ_PORT'"},{"po
rt":"'$HA1_PORT'"},{"port":"'$HA2_PORT'"},{"port":"'$HA1backup_PORT'"},{"port":"'$HA2backup_PORT'"}],"secur
ity_groups":[{"name":"'$SG_NAME'"}]},"os:scheduler_hints":{"group":"'$GROUP_ID'"}}' | jq .
```

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 【任意】名前は任意で指定してください。
※2 【固定】仮想サーバタイプ ID は、2.3 留意事項の項番 1 を参照の上、指定してください。
※3 【固定】60GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】Palo Alto Networks の削除時にボリュームも削除する場合は指定してください。
※8 【固定】

図 4-2-9: Palo Alto Networks の作成(active)

4.3 Palo Alto Networks の作成(standby)

＜ポートの作成＞

Palo Alto Networks にアタッチするポートを作成します。

■External-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=External-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.10.12
[root@K5-Host ]# NETWORK_ID="External-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"
[root@K5-Host ]# VIP=192.168.10.100

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type:
application/json" -d '{"port": {"admin_state_up": true,"name": "'$PORT_NAME'","network_id":
"'$NETWORK_ID'","port_security_enabled": true,"allowed_address_pairs": [{"ip_address":
"'$VIP'"}],"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [
      {
        "ip_address": "192.168.10.100",
        "mac_address": "fa:16:3e:05:cc:05"
      }
    ],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:47:26Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "076ce999-9383-425a-bb89-6ddd908376e2",
        "ip_address": "192.168.10.12"
      }
    ],
    "id": "fcfe2b3e-9faf-4b34-a0db-d023445ea0f2",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:05:cc:05",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "External-port-standby",
    "admin_state_up": true,
    "network_id": "ed2cf8e7-0283-4eb8-897c-d583eec3aed8",
```

```
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:47:26Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-3-1：External-net 用ポートの作成

■Internal-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=Internal-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.20.12
[root@K5-Host ]# NETWORK_ID="Internal-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"
[root@K5-Host ]# VIP=192.168.20.100

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true,"name": "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled": true,"allowed_address_pairs": [{"ip_address": "'$VIP'"}],"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [
      {
        "ip_address": "192.168.20.100",
        "mac_address": "fa:16:3e:8c:96:5e"
      }
    ],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:48:01Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "fb20278c-9ffb-49e1-88c8-4fe7bd24ce1f",
        "ip_address": "192.168.20.12"
      }
    ],
    "id": "db50d3f9-d829-46eb-90e6-4486dd354581",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:8c:96:5e",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "Internal-port-standby",
    "admin_state_up": true,
    "network_id": "139edbe8-bf0e-46dc-8281-ab319d2b6291",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:48:00Z",
    "binding:vnic_type": "normal"
  }
}
```

図 4-3-2：Internal-net 用ポートの作成

■DMZ-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=DMZ-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.30.12
[root@K5-Host ]# NETWORK_ID="DMZ-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"
[root@K5-Host ]# VIP=192.168.30.100

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true,"name": "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled": true,"allowed_address_pairs": [{"ip_address": "'$VIP'"}],"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [
      {
        "ip_address": "192.168.30.100",
        "mac_address": "fa:16:3e:b0:0b:52"
      }
    ],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:48:39Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "281f3ee3-fbfe-4eba-8a7e-65ff045eb0e4",
        "ip_address": "192.168.30.12"
      }
    ],
    "id": "dfbd2cd4-4cbf-4cb1-ab76-c577489948ce",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:b0:0b:52",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "DMZ-port-standby",
    "admin_state_up": true,
    "network_id": "4cbb2b5a-9db6-4ccc-9f7c-375c544d6d4f",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:48:39Z",
    "binding:vnic_type": "normal"
  }
}
```

図 4-3-3：Internal-net 用ポートの作成

■HA1-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA1-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.40.12
[root@K5-Host ]# NETWORK_ID="HA1-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"port": {"admin_state_up": true,"name": "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled": true,"fixed_ips": [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例

```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:49:10Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "643a5d9e-afb6-42f2-8079-c4a8942cd59c",
        "ip_address": "192.168.40.12"
      }
    ],
    "id": "89931a9f-0365-4b7c-a641-3bb378618726",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:e4:64:5f",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA1-port-standby",
    "admin_state_up": true,
    "network_id": "2a3d8643-5fd5-43cc-9849-2b8aa85d0a90",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:49:10Z",
    "binding:vnic_type": "normal"
  }
}
```

図 4-3-4：HA1-network 用ポートの作成

■HA2-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA2-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.70.22
[root@K5-Host ]# NETWORK_ID="HA2-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:49:40Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "eeebfce9-590b-42cf-9995-95ddb193ef4d",
        "ip_address": "192.168.70.22"
      }
    ],
    "id": "15730faa-1482-4eff-baad-8d1567ee6b52",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:5a:ad:40",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA2-port-standby",
    "admin_state_up": true,
    "network_id": "bbc94352-e63c-4401-a31e-e039543e57fd",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:49:40Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-3-5：HA1-network 用ポートの作成

■Management-net 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=Management-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.50.12
[root@K5-Host ]# NETWORK_ID="Management-net の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:50:12Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "fdea2ff3-ff48-4b66-b28a-c1e56f87ab4b",
        "ip_address": "192.168.50.12"
      }
    ],
    "id": "fe22c3c4-a75d-495e-9438-93bfd14c608a",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:a8:71:ce",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "Management-port-standby",
    "admin_state_up": true,
    "network_id": "bed53dcc-986b-43b9-91b1-374bc1adf2c8",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:50:11Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-3-6：Management-net 用ポートの作成

■HA1-backupnet 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA1backup-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.60.12
[root@K5-Host ]# NETWORK_ID="HA1-bachupnet の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id": "'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address": "'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:50:55Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "2166cb55-2725-4d75-81e4-02390da14a74",
        "ip_address": "192.168.60.12"
      }
    ],
    "id": "57c6a802-858e-45f6-b66d-9ed68698a3c1",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:3b:e3:53",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA1backup-port-standby",
    "admin_state_up": true,
    "network_id": "57a50333-2587-467d-9a33-8d4e4649e864",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:50:55Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-3-7：HA1-backupnet 用ポートの作成①

■HA2-backupnet 用ポート

コマンド例

```
[root@K5-Host ]# PORT_NAME=HA2backup-port-standby
[root@K5-Host ]# IP_ADDRESS=192.168.80.22
[root@K5-Host ]# NETWORK_ID=" HA2-backupsubnet の ID"
[root@K5-Host ]# SG_ID="Paloalto-SG セキュリティグループの ID"

[root@K5-Host ]# curl -s $NETWORK/v2.0/ports -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json"  -d  '{"port":  {"admin_state_up":  true,"name":  "'$PORT_NAME'","network_id":"'$NETWORK_ID'","port_security_enabled":  true,"fixed_ips":  [{"ip_address":"'$IP_ADDRESS'"}],"security_groups": ["'$SG_ID'"]}}' | jq .
```

実行結果例


```
{
  "port": {
    "allowed_address_pairs": [],
    "extra_dhcp_opts": [],
    "updated_at": "2021-09-24T07:51:17Z",
    "nuage_policy_groups": null,
    "device_owner": "",
    "revision_number": 5,
    "port_security_enabled": true,
    "fixed_ips": [
      {
        "subnet_id": "f89db32a-19bd-4d8f-b83b-5f317d833afa",
        "ip_address": "192.168.80.22"
      }
    ],
    "id": "e16ca8bf-96a3-4913-9d1c-ce6f552b1523",
    "security_groups": [
      "c6433ceb-d167-4d78-9500-653ae240b4cf"
    ],
    "mac_address": "fa:16:3e:6d:09:b7",
    "nuage_floatingip": null,
    "project_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "status": "DOWN",
    "description": "",
    "tags": [],
    "device_id": "",
    "nuage_redirect_targets": [],
    "name": "HA2backup-port-standby",
    "admin_state_up": true,
    "network_id": "f84de3bb-28c7-44c6-ad3b-9a64dc90b6ac",
    "tenant_id": "df5b1a54f3994aac9ecf0553bd65bbee",
    "created_at": "2021-09-24T07:51:17Z",
    "binding:vnic_type": "normal"
  }
}
```


図 4-3-8：HA1-backupnet 用ポートの作成②

＜Palo Alto Networks の作成＞

Palo Alto Networks の standby を作成します。アンチアフィニティで作成するので、API で実行してください。

コマンド例

```
[root@K5-Host ~]# VM_NAME=Paloalto_standby ※1
[root@K5-Host ~]# IMAGE_REF_ID=“Palo Alto Networks の ImageID”
[root@K5-Host ~]# FLAVOR_ID=“Palo Alto Networks の FlavorID” ※2
[root@K5-Host ~]# VOL_SIZE=60 ※3
[root@K5-Host ~]# DEVICE_NAME=/dev/vda ※4
[root@K5-Host ~]# SOURCE=image ※5
[root@K5-Host ~]# DESTINATION=volume ※6
[root@K5-Host ~]# ISDELETE=true ※7
[root@K5-Host ~]# EXTERNAL_PORT=“External-port-standby の ID”
[root@K5-Host ~]# INTERNAL_PORT=“Internal-port-standby の ID”
[root@K5-Host ~]# DMZ_PORT=“DMZ-port-standby の ID”
[root@K5-Host ~]# HA1_PORT=“HA1-port-standby の ID”
[root@K5-Host ~]# HA2_PORT=“HA2-port-standby の ID”
[root@K5-Host ~]# MANAGEMENT_PORT=“Management-port-standby の ID”
[root@K5-Host ~]# HA1backup_PORT=“HA1backup-port-standby の ID”
[root@K5-Host ~]# HA2backup_PORT=“HA2backup-port-standby の ID”
[root@K5-Host ~]# SG_NAME=“「SecurityGroup の作成で作成した」グループ名”
[root@K5-Host ~]# GROUP_ID=“アンチアフィニティの設定で作成したグループ ID” ※8

[root@K5-Host ~]# curl -k $COMPUTE/v2.1/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H
"Content-Type: application/json" -d '
{"server":{"name":"'$VM_NAME'","imageRef":"","flavorRef":"'$FLAVOR_ID'","block_device_mapping_v2":[{"boot_i
ndex":"0","uuid":"'$IMAGE_REF_ID'","volume_size":"'$VOL_SIZE'","device_name":"'$DEVICE_NAME'","source_type"
:"'$SOURCE'","destination_type":"'$DESTINATION'","delete_on_termination":"'$ISDELETE'"}],"networks":[{"port
":"'$MANAGEMENT_PORT'"},{"port":"'$EXTERNAL_PORT'"},{"port":"'$INTERNAL_PORT'"},{"port":"'$DMZ_PORT'"},{"po
rt":"'$HA1_PORT'"},{"port":"'$HA2_PORT'"},{"port":"'$HA1backup_PORT'"},{"port":"'$HA2backup_PORT'"}],"secur
ity_groups":[{"name":"'$SG_NAME'"}]},"os:scheduler_hints":{"group":"'$GROUP_ID'"}}' | jq .
```

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 【任意】名前は任意で指定してください。
※2 【固定】仮想サーバタイプ ID は、2.3 留意事項の項番 1 を参照の上、指定してください。
※3 【固定】60GB 固定です。
※4 【固定】
※5 【固定】
※6 【固定】
※7 【任意】Palo Alto Networks の削除時にボリュームも削除する場合は指定してください。
※8 【固定】

図 4-3-9: Palo Alto Networks の作成(standby)

4.4　仮想サーバの作成

仮想サーバ(WebServer、test-pc)を作成します。(図 4-4-1)

以下は WebServer の作成例です。同様に test-pc も作成してください。※の部分以外はお客様の任意の値となります。

コマンド例

```
[root@K5-Host ~]# VM_NAME=WebServer
[root@K5-Host ~]# IMAGE_REF_ID=“WebServer として利用したい任意の Image の ID”
[root@K5-Host ~]# FLAVOR_ID=“仮想サーバスペック ID 例 C3-2: 88445c68-4f27-4220-9414-ceb5f1931bda”
[root@K5-Host ~]# VOL_SIZE=“ボリュームサイズ(GB)”
[root@K5-Host ~]# DEVICE_NAME=/dev/vda
[root@K5-Host ~]# SOURCE=image
[root@K5-Host ~]# DESTINATION=volume
[root@K5-Host ~]# ISDELETE=true
[root@K5-Host ~]# KEYNAME=“キー名”
[root@K5-Host ~]# INSTANCE_MAX=1
[root@K5-Host ~]# INSTANCE_MIN=1
[root@K5-Host ~]# NETWORK_ID1=“DMZ-Net の ID” ※1
[root@K5-Host ~]# SG_NAME=“セキュリティグループ名”
[root@K5-Host ~]# GROUP_ID=“「アンチアフィニティの設定で」作成したグループ ID” ※2
[root@K5-Host ~]# curl -k $COMPUTE/v2.1/$PROJECT_ID/servers -X POST -H "X-Auth-Token: $OS_AUTH_TOKEN" -H "Content-Type: application/json" -d '{"server": {"name": "'$VM_NAME'", "imageRef": "", "flavorRef": "'$FLAVOR_ID'","block_device_mapping_v2":[ {"boot_index": "0", "uuid":"'$IMAGE_REF_ID'", "volume_size": "'$VOL_SIZE'", "device_name": "'$DEVICE_NAME'", "source_type": "'$SOURCE'", "destination_type": "'$DESTINATION'", "delete_on_termination": "'$ISDELETE'"} ], "key_name": "'$KEYNAME'", "max_count": '$INSTANCE_MAX', "min_count": '$INSTANCE_MIN', "networks": [{"uuid": "'$NETWORK_ID1'"}], "security_groups": [{"name": "'$SG_NAME'"}]},"os:scheduler_hints": {"group": "'$GROUP_ID'"}}'

※$COMPUTE は compute サービスの API エンドポイントを指定してください。
※$PROJECT_ID はご利用の Project の ID を指定してください。

※1 前手順で作成した DMZ-Net を指定してください。
※2 前手順で作成したサーバグループを指定してください。
```

図 4-4-1:仮想サーバの作成

第 5 章　Palo Alto Networks ライセンス登録

本章では、Palo Alto Networks に対してライセンスを登録する手順を説明します。

5.1　Palo Alto Networks の Web アクセスログイン

Palo Alto Networks に Web アクセスし、以降の作業を実施します。
本書の Palo Alto Networks (active)では、https://192.168.50.11 へアクセスします。

初期アカウント、パスワードは以下になります。
アカウント admin
パスワード admin

図 5-1-1：Palo Alto Networks に Web アクセス

初回ログイン時、パスワード変更を求められます。適切なパスワードを設定してください。
Palo Alto Networks の Web アクセスについては、以下「Launch the Web Interface」を参照してください。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/use-the-web-interface/launch-the-web-interface.html

パスワード変更後、ログインし、commit(コミット)を実施し、設定を保存してください。
Commit を実施せず、5.3 でライセンス適用すると再起動が発生し、パスワードが初期値に戻ります。

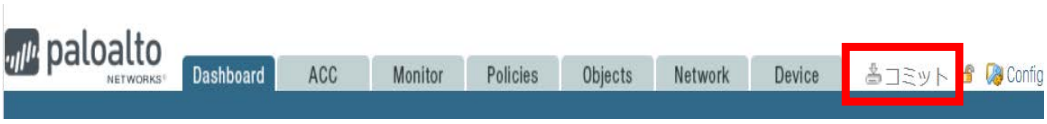


図 5-1-2：commit(コミット)

参考

■Limitations

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-release-notes/pan-os-9-1-release-information/limitations.html

---

PAN-128908

If an admin user password is changed but no commit is performed afterward, the new password does not persistent after a reboot. Instead, the admin user can still use the old password to log in, and the calculation of expiry days is incorrect based on the password change timestamp in the database.

表示されたダッシュボード画面の「一般的な情報」より

CPUID、UUID の情報をメモしてください。

Palo Alto Networks (passive)でも同様の操作で CPUID、UUID の情報を取得してください。

図 5-1-3：Palo Alto Networks CPU ID, UUID 確認

5.2　ライセンスファイルの作成（ライセンスアクティベート API の実行）

Palo Alto Networks の機能を使用するには、ライセンスキーを Palo Alto Networks GUI 画面から登録する必要があります。

ライセンスアクティベート API(※)を実行して、Palo Alto Networks インスタンスとライセンスを紐づけして、各サブスクリプションのライセンスキーを入手します。(図 5-2-1 ライセンスアクティベート API の実行)

※ ライセンスアクティベート API の詳細については、以下 API リファレンスページを参照してください。
https://doc.cloud.global.fujitsu.com/lib/iaas/jp/api-reference/v3/web/k5-iaas-api-reference/reference/vas_lm_license_activation/

利用するサブスクリプションごとに API レスポンス内の”keyField”の値をテキストファイル(本章では「ライセンスファイル」と呼称します)として保存します。

「図 5-2-1 ライセンスアクティベート API の実行」で、ライセンスファイルを bash コマンドラインで自動作成する手順を記載します。

手動でライセンスファイルを作成する場合は、以下の点(※)に留意してください。

※　keyField には改行コード(¥n)が含まれます。
　　改行コードに以下の対処を行い、テキストファイルとして保存します。
　　- 文中の改行コード（¥n）は実際の改行に修正
　　- 末尾の改行コード（¥n）を削除
　例）keyField が“abcde¥nfghij¥n”の場合、テキストファイルを以下とおり保存します。
　　abcde
　　fghij

■API 実行を実施した際にエラーが発生した場合、お手数ですが以下の情報を採取して、ヘルプデスクにお問い合わせください。
・コマンドを実行した際の作業ログ

コマンド例
事前に取得する認証トークン（OS_AUTH_TOKEN）は、Palo Alto Networks のインスタンスが所属するテナント情報を元に取得してください。 [root@K5-Host]# CPUID=ダッシュボードより確認した CPUID の値　※1 [root@K5-Host]# UUID=ダッシュボードより確認した UUID の値 [root@K5-Host]# PROJECT_ID=テナントの ID ※2 [root@K5-Host]# PAN_EP=https://app2-image.<region>.cloud.global.fujitsu.com ※3 [root@K5-Host]# curl -s -H "X-Auth-Token: $OS_AUTH_TOKEN" ¥ --data-urlencode cpuid=$CPUID ¥ --data-urlencode uuid=$UUID ¥ --data-urlencode projectid=$PROJECT_ID ¥ $PAN_EP/api/license/activate　¥ -o activate.json

※1 Palo Alto Networks の GUI で表示されている CPUID を正しく入力してください。誤るとサポートを受けられない可能性があります。
※2 Palo Alto Networks インスタンスのテナント ID を入力してください。
※3 利用リージョンによって<region>の値を修正してください。
　東日本リージョン 3 の場合：https://app2-image.jp-east-3.cloud.global.fujitsu.com
　西日本リージョン 3 の場合：https://app2-image.jp-west-3.cloud.global.fujitsu.com

上記ファイルの keyField 個数より、作成するライセンスファイル数を確認します。
```
[root@K5-Host ]# COUNT=`cat activate.json | jq .[].keyField | wc -l`
[root@K5-Host ]# COUNT=`expr $COUNT - 1`
```

上記で確認した数値を元に改行処理を行い、ライセンスファイルを作成します。
```
[root@K5-Host ]# for i in $(seq 0 $COUNT); do cat activate.json | jq .[${i}].keyField | sed -e 's/¥¥n/¥n/g' | sed -e 's/¥"//g' > license-key${i}.txt; done
```

実行結果例

PAN VM50 Bundle2 の場合、以下のとおりライセンスファイルが作成されます。

```
license-key0.txt
license-key1.txt
license-key2.txt
license-key3.txt
license-key4.txt
license-key5.txt
license-key6.txt
```

ライセンスアクティベート API レスポンス例

-o オプションを付与せずにライセンスアクティベート API を実行すると、以下のとおり出力されます。
(表示上、改行して見やすくしています。)


```
[
    {
        "PropertyChanged": null,
        "cpuidField": null,
        "drrField": null,
        "errmsgField": null,
        "expirationField": "3/18/2021 12:00:00 AM",
        "featureField": "Threat Prevention",
        "feature_descField": "Threat Prevention",
        "keyField": "XXXXXXXXXXXXXXXXXX",
        "lfidField": "1281787626",
        "mac_baseField": null,
        "mac_countField": null,
        "partidField": "PAN-VM-50-TP",
        "regDateField": "2021-01-17T21:32:49",
        "serialnumField": "015354000058687",
        "startDateField": "1/17/2021",
        "typeField": "SUB",
        "uuidField": null,
        "vm_capacityField": null
    },
    {
        "PropertyChanged": null,
        "cpuidField": null,
        "drrField": null,
        "errmsgField": null,
        "expirationField": "3/18/2021 12:00:00 AM",
```

```
        "featureField": "PAN-DB URL Filtering",
        "feature_descField": "Palo Alto Networks URL Filtering License",
        "keyField": "YYYYYYYYYYYYYYYYYYYY",
        "lfidField": "1281787629",
        "mac_baseField": null,
        "mac_countField": null,
        "partidField": "PAN-VM-50-URL4",
        "regDateField": "2021-01-17T21:32:49",
        "serialnumField": "015354000058687",
        "startDateField": "1/17/2021",
        "typeField": "SUB",
        "uuidField": null,
        "vm_capacityField": null
    },
  {
    :
  },
    : 省略
  {
    :
  }
]
```


図 5-2-1：ライセンスアクティベート API の実行

ご参考） ライセンス情報再取得 API の実行

インスタンスに一度紐づけしたライセンスの情報は、以下の再取得 API を実行して参照できます。

コマンド例

```
[root@K5-Host ]# CPUID=ダッシュボードより確認した CPUID の値
[root@K5-Host ]# UUID=ダッシュボードより確認した UUID の値
[root@K5-Host ]# PROJECT_ID=テナントの ID ※1
[root@K5-Host ]# PAN_EP=https://app2-image.<region>.cloud.global.fujitsu.com ※2
[root@K5-Host ]# curl -s -H "X-Auth-Token: $OS_AUTH_TOKEN" ¥
 --data-urlencode cpuid=$CPUID ¥
 --data-urlencode uuid=$UUID ¥
 --data-urlencode projectid=$PROJECT_ID ¥
 $PAN_EP/api/license/reacquire | jq .
```

※1 Palo Alto Networks インスタンスのテナント ID を入力してください。
※2 利用リージョンによって<region>の値を修正してください。
　　東日本リージョン 3 の場合：https://app2-image.jp-east-3.cloud.global.fujitsu.com
　　西日本リージョン 3 の場合：https://app2-image.jp-west-3.cloud.global.fujitsu.com

実行結果例


```
[
    {
        "PropertyChanged": null,
        "cpuidField": null,
        "drrField": null,
        "errmsgField": null,
        "expirationField": "3/18/2021 12:00:00 AM",
        "featureField": "Threat Prevention",
        "feature_descField": "Threat Prevention",
        "keyField": "XXXXXXXXXXXXXXXXXX",
```

```
        "lfidField": "1281787626",
        "mac_baseField": null,
        "mac_countField": null,
        "partidField": "PAN-VM-50-TP",
        "regDateField": "2021-01-17T21:32:49",
        "serialnumField": "015354000058687",
        "startDateField": "1/17/2021",
        "typeField": "SUB",
        "uuidField": null,
        "vm_capacityField": null
    },
    {
        "PropertyChanged": null,
        "cpuidField": null,
        "drrField": null,
        "errmsgField": null,
        "expirationField": "3/18/2021 12:00:00 AM",
        "featureField": "PAN-DB URL Filtering",
        "feature_descField": "Palo Alto Networks URL Filtering License",
        "keyField": "YYYYYYYYYYYYYYYYYYYY",
        "lfidField": "1281787629",
        "mac_baseField": null,
        "mac_countField": null,
        "partidField": "PAN-VM-50-URL4",
        "regDateField": "2021-01-17T21:32:49",
        "serialnumField": "015354000058687",
        "startDateField": "1/17/2021",
        "typeField": "SUB",
        "uuidField": null,
        "vm_capacityField": null
    },
  {
    :
  },
    : 省略
  {
    :
  }
]
```


図 5-2-2：ライセンス情報再取得 API の実行

5.3 Palo Alto Networks のライセンスファイル登録

Palo Alto Networks 2 台にそれぞれ Web アクセスでログイン後、ライセンスファイルを登録します。(図 5-3-1～図 5-3-3)

1. Web アクセスでログイン後、上段タブ「デバイス」をクリック
2. 左側のライセンスをクリック
3. ライセンス管理で「ライセンスキーの手動アップロード」をクリック

図 5-3-1：Palo Alto Networks のライセンス登録①

4. ライセンスのインストールで、「ファイルを選択」をクリック
5. 5.2 で取得したライセンスファイルを選択
6. Web アクセスでログイン後、上段タブ「デバイス」をクリック
7. OK をクリック

図 5-3-2：Palo Alto Networks のライセンス登録②

8. 警告画面で OK をクリック

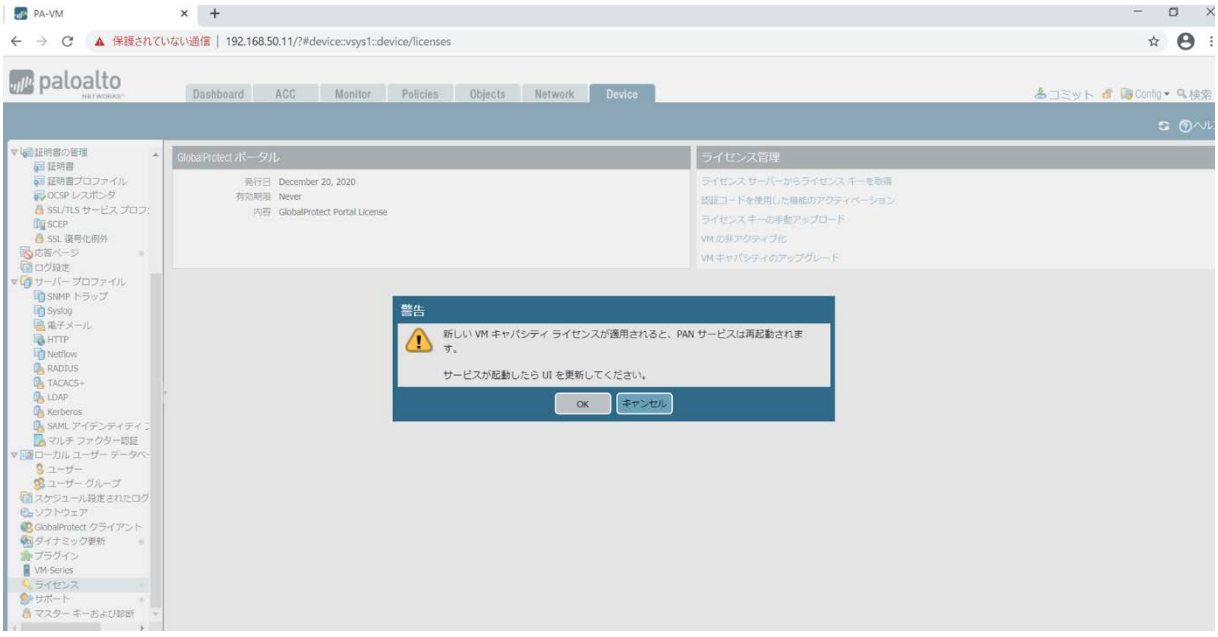


図 5-3-3：Palo Alto Networks のライセンス登録③

ライセンスが登録されると、ライセンスが表示されます。
全てのライセンスファイルを上記手順で登録してください。

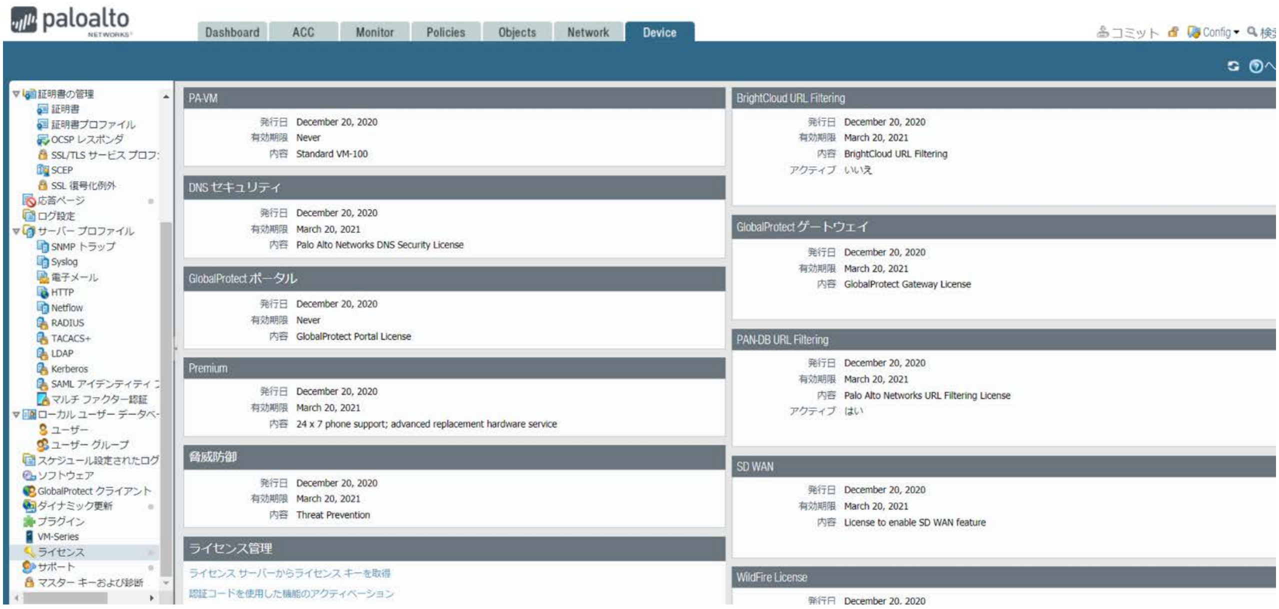


図 5-3-4：Palo Alto Networks のライセンス登録④

■Palo Alto Networks VM を削除する際は､削除前に以下の手順でライセンス無効化の処理を実施してください｡(図 5-3-2)

■Palo Alto Networks VM を作成してから削除するまでが課金の対象になります。

5.4 Palo Alto Networks のライセンス無効化(トークンファイルの入手)

Palo Alto Networks に Web アクセスし、「Device」タブの「ライセンス」画面内の「ライセンス管理」より「VM の非アクティブ化」をクリックします。

その後表示されるポップアップ（下記図 5-4-1：VM の非アクティブ化参照）にて「手動で実行」を押下します。

※「続行」ボタンは押下しないでください。

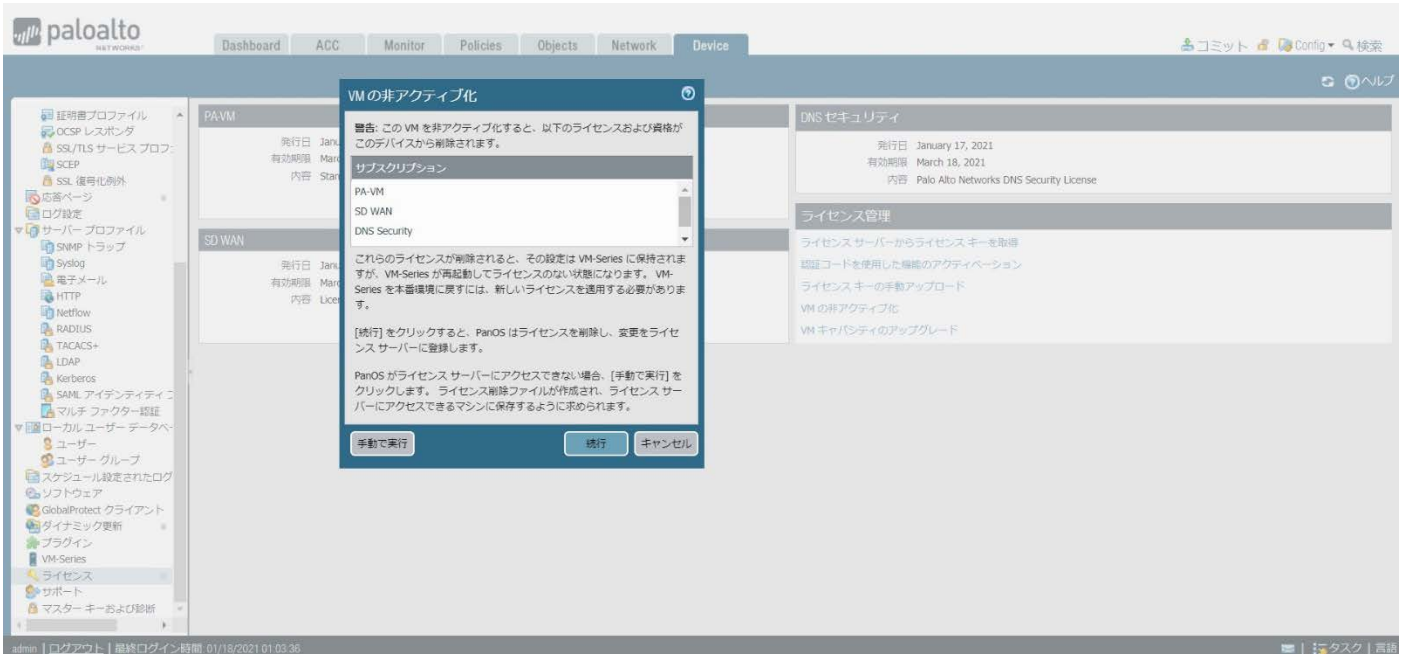


図 5-4-1：VM の非アクティブ化

その後のポップアップ画面（図 5-4-2：手動による VM の非アクティブ化）にて「ライセンストークンのエクスポート」リンクよりトークンファイルをダウンロードしてください。
トークンファイルのダウンロード完了後、「今すぐ再起動」を押下し、その後のポップアップで「はい」を押下してください。
※リンクが表示されない、またはダウンロードしないで画面を閉じた場合は、CLI による以下の手順でトークンファイルの値を取得することが可能です。

1. トークンファイル名を出力 ： show license-token-files
2. トークンファイルの値を出力 ： show license-token-files name ＜トークンファイル名＞

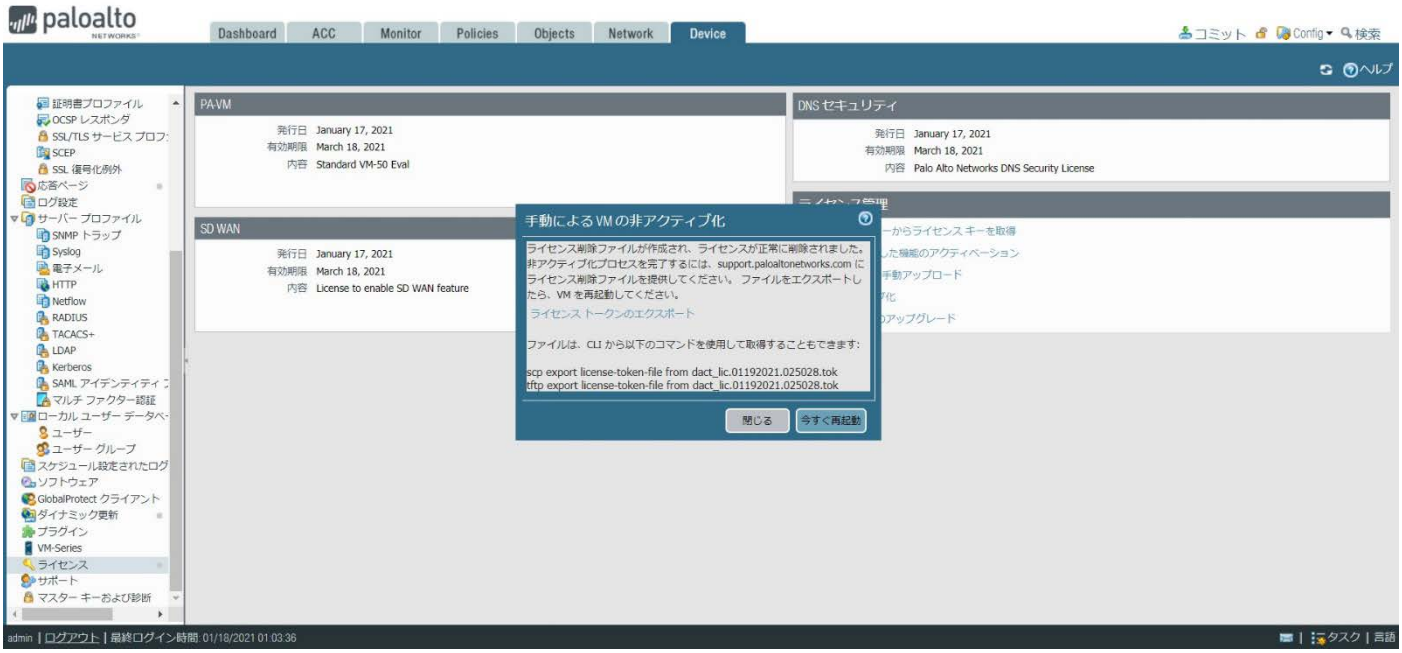


図 5-4-2：手動による VM の非アクティブ化

■ライセンスの登録処理、無効化処理を実施した際にエラーが発生した場合、お手数ですが以下の情報を採取して、ヘルプデスクにお問い合わせください。

・実行した際の作業ログまたは画面コピー

5.5　ライセンスディアクティベート API の実行

5.4 で入手したトークンファイルを用いて下記の API 実行によりインスタンスに紐づいたライセンスを無効化します。実行後はレスポンスボディに含まれる successField の値が Y となっていることを確認してください。

コマンド例

事前に取得する認証トークン（OS_AUTH_TOKEN）は、Palo Alto Networks のインスタンスが所属するテナント情報を元に取得してください。

```
[root@K5-Host ]# PROJECT_ID=テナントの ID ※1
[root@K5-Host ]# PAN_EP=https://app2-image.<region>.cloud.global.fujitsu.com ※2
[root@K5-Host ]# curl -s -H "X-Auth-Token: $OS_AUTH_TOKEN" ¥
--data-urlencode projectid=$PROJECT_ID ¥
--data-urlencode encryptedtoken@dact_lic.tok ¥
$PAN_EP/api/license/deactivate | jq .
```

※1 Palo Alto Networks インスタンスのテナント ID を入力してください
※2 利用リージョンによって<region>の値を修正してください。
　　東日本リージョン 3 の場合：https://app2-image.jp-east-3.cloud.global.fujitsu.com
　　西日本リージョン 3 の場合：https://app2-image.jp-west-3.cloud.global.fujitsu.com

実行結果例


```
[
    {
        "PropertyChanged": null,
        "errorField": null,
        "featureNameField": "",
        "isBundleField": null,
        "issueDateField": "",
        "serialNumField": "007054000128706",
        "successField": "Y"
    },
    {
        "PropertyChanged": null,
        "errorField": null,
        "featureNameField": "",
        "isBundleField": null,
        "issueDateField": "",
        "serialNumField": "007054000128706",
        "successField": "Y"
    },
:    (省略)
    }
]
```


図 5-5-1：ライセンスディアクティベート API の実行

5.6 Palo Alto Networks 初期設定

Palo Alto Networks の初期設定については、以下の Palo Alto Networks 社マニュアルを参照してください。

初期設定
■Perform Initial Configuration
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/integrate-the-firewall-into-your-management-network/perform-initial-configuration.html

設定ガイド
■PAN-OS® Administrator’s Guide
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin.html

5.7 Palo Alto Networks バージョンアップ

バージョンアップの手順は以下の Palo Alto Networks 社マニュアルを参照してください。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/upgrade-to-pan-os-91/upgrade-the-firewall-to-pan-os-91

単体構成の場合は、Upgrade a Standalone Firewall to PAN-OS 9.1 を選択し参照してください。
冗長構成の場合は、Upgrade an HA Firewall Pair to PAN-OS 9.1 を選択し参照してください。

5.8 Palo Alto Networks 参照 URL

既知の問題などにつきましては、PAN-OS のリリースノートを参照してください。
ページ右上の CURRENT VERSION:から対象バージョンを切替えてご確認いただけます。
[PAN-OS Release Notes]
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-release-notes.html

PAN-OS の重大な問題などについては以下のサイトを参照してください。
[CRITICAL ISSUES ADDRESSED IN PAN-OS RELEASES]
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm68CAC

PAN-OS の脆弱性などは以下のサイトを参照してください。
https://security.paloaltonetworks.com/

6.1　仮想ルータの FW ルールの設定

仮想ルータの FW ルールを適切に設定してください

FW の設定方法は「IaaS 機能説明書」および「IaaS API リファレンス」を参照してください。

6.2　Palo Alto Networks の仮想 IP アドレスにグローバル IP アドレスを割当

Palo Alto Networks の仮想 IP アドレスにグローバル IP アドレスを割り当て、Palo Alto Networks の運用を開始します。(図 6-2-1)

詳細は、以下の　図 6-2-1：Palo Alto Networks の IP アドレスにグローバル IP アドレス割当を参照してください。

コマンド例
作成したポート(External-virtual-port のポートのアドレス)にグローバル IP アドレスを割当 [root@K5-Host]# NETWORK_ID=“グローバル IP ネットワークの ID” [root@K5-Host]# PORT_ID=“共有ポートの ID”(※1) curl -s $NETWORK/v2.0/floatingips -X POST -H "X-Auth-Token:$OS_AUTH_TOKEN" -H "Content-Type:application/json" -d '{"floatingip":{"floating_network_id":"'$NETWORK_ID'", "port_id":"'$PORT_ID'"}}' | jq . 上記設定を完了後、WebServer の参照先 DNS サーバやデフォルトゲートウェイの設定(※2)を確認し、インターネットからグローバル IP アドレスにアクセスし、疎通を確認し設定は完了です。 ※1　4-1 共有ポートで作成した External-virtual-port の PORT_ID を指定してください ※2　WebServer のデフォルトゲートウェイは Palo Alto Networks DMZ-Network 側の dmz-floating-ip を指定してください

図 6-2-1：Palo Alto Networks の仮想 IP アドレスにグローバル IP アドレスを割当

以上で本書における導入事例の説明は終了です。

FUJITSU Hybrid IT Service FJcloud-O IaaS

次世代仮想ファイアーウォール

powered by Palo Alto Networks

VM-series スタートガイド 1.10 版

発行日 2024 年 6 月