



Zscaler Private Access(ZPA) 基本操作ガイド

Rev.1.1

2024年 4月

ノックス株式会社



- ※ 本出版物の著作権はノックス株式会社が権利を保有しています。本出版物の配布は、Zscaler サービスのサブスクリプション購入者による使用のみを目的としています。
- ※ 本出版物中に用いられている商標については、全て該当する会社が権利を保有しています。
- ※ 当社の許可なく、本出版物の複製・転載・配布を禁じます。
- ※ 本出版物は無保証で提供されるものであり、当社は本製品についてその商品性、特定の目的に対する適合性、使用による権利侵害の不発生を保証するものではなく、かつこれに限定されずいかなる事項についても明示的または暗示的に保証しません。
- ※ 本出版物には技術的内容に関して不適切な部分および誤植部分が含まれている恐れがあります。当社は事前の通知なく本出版物の内容を改訂する場合があります。
- ※ クラウド側のバージョンアップにより設定項目が追加、変更される可能性があります。

Copyright(C)2024ノックス株式会社

目次

1. ZPA 設定の流れ	6
2. ZPA 管理ポータルへのログイン	7
2-1. 概要	7
2-2. ZPA 管理ポータルへのログイン方法	7
2-3. ZPA 管理ポータルの管理者設定方法	7
2-3-1. 管理者ロールの設定方法	7
2-3-2. 管理者の追加方法	8
3. IDP CONFIGURATION	10
3-1. 概要	10
3-2. IDP の設定方法	10
4. APP CONNECTOR	13
4-1. 概要	13
4-2. PROVISIONING KEY の作成	13
4-3. APP CONNECTOR の作成	15
4-3-1. App Connector のデプロイ	16
4-3-2. App Connector コンソールへのログイン	17
4-3-3. ネットワークアドレスの設定	17
4-3-4. DNS サーバーの設定	18
4-3-5. Provisioning Key の適用	18
5. APPLICATION SEGMENT	20
5-1. 概要	20
5-2. APPLICATION SEGMENT の作成	20
5-3. 【補足】SERVER GROUP/SERVERS の推奨設定	22
5-3-1. 推奨設定	22
5-3-2. 例外設定	23
6. ACCESS POLICY	25
6-1. 概要	25
6-2. ACCESS POLICY の作成	25
6-3. 【補足】ポリシーの RULE ORDER について	26

7. TIMEOUT POLICY	27
7-1. 概要	27
7-2. DEFAULT TIMEOUT POLICY	27
7-3. TIMEOUT POLICY の作成	27
8. CLIENT FORWARDING POLICY	29
8-1. 概要	29
8-2. CLIENT FORWARDING POLICY の作成	29



本書について

本書は Zscaler の導入時にスムーズに設定が行えることを目指した導入マニュアルです。

本書は基本的な設定・流れの把握を目的としています。また、難解さを極力避けるようにしていますので、一部内容に関して不足や補足が必要な個所がある場合がありますが、本書の趣旨をご理解の上、ご利用いただきますようお願い申し上げます。

なお、詳細な内容解説については、恐れ入りますが英語版の各種ドキュメントおよびヘルプをご参照くださいますようお願い申し上げます。

ヘルプページ：<https://help.zscaler.com/>

通信要件:

<https://config.zscaler.com/zscaler.net/zscaler-app>

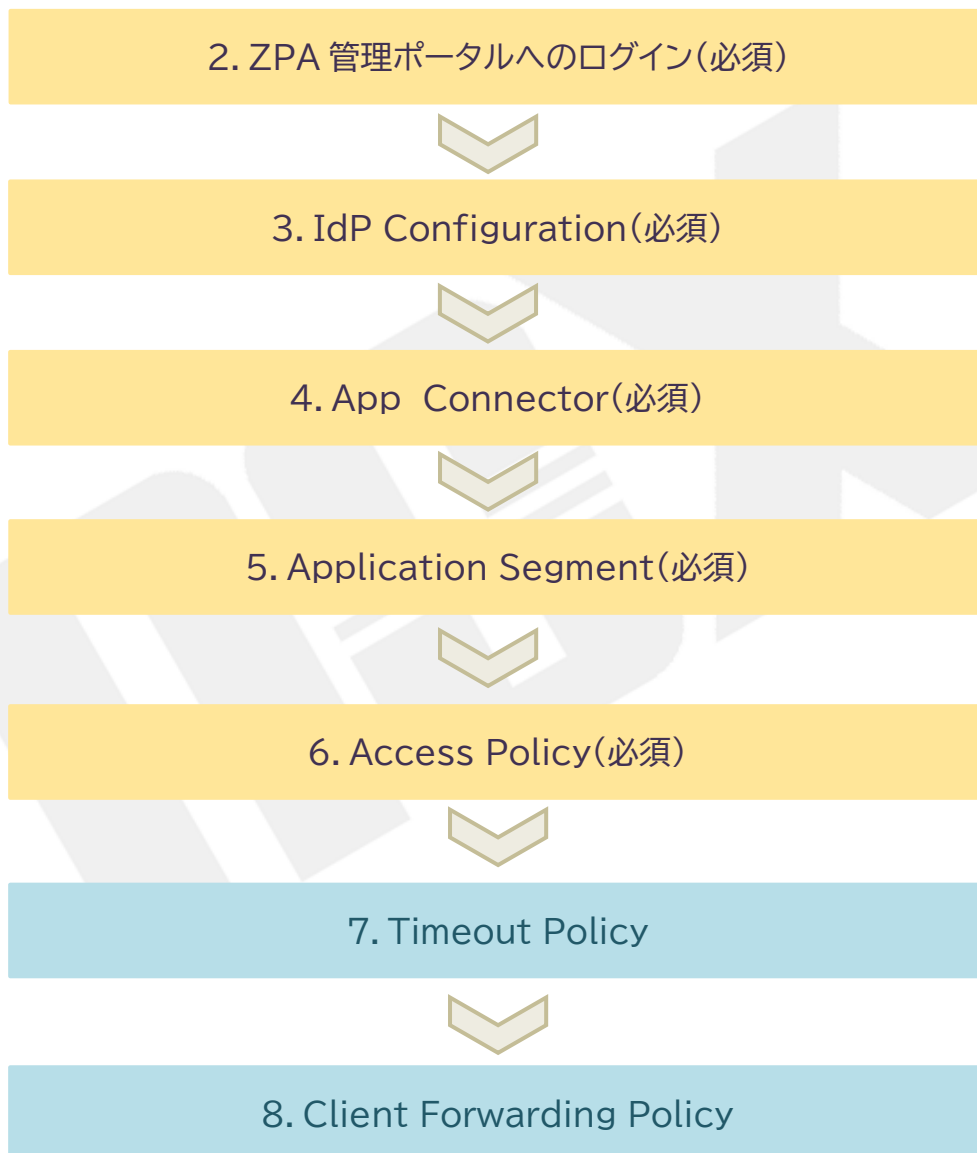
<https://config.zscaler.com/private.zscaler.com/zpa>

1. ZPA 設定の流れ

1-1. 概要

Zscaler Private Access(ZPA)の基本的な設定手順について説明します。

1-2. ZPA サービス設定フロー



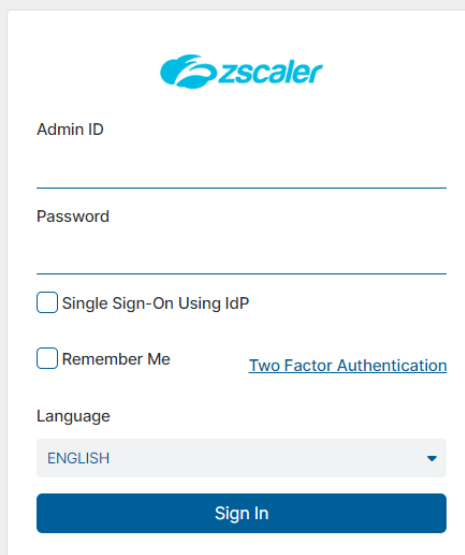
2. ZPA 管理ポータルへのログイン

2-1. 概要

ZPA 管理ポータルへのログイン方法について説明します。

2-2. ZPA 管理ポータルへのログイン方法

- (1) 弊社からご連絡したログイン ID、パスワードを使用して、ZPA 管理ポータルへログインをします。
ポータルサイトの URL は「admin.private.zscaler.com」です。



The screenshot shows the login interface for the ZPA Admin Portal. It includes the Zscaler logo, an 'Admin ID' input field, a 'Password' input field, and two checkboxes: 'Single Sign-On Using IdP' and 'Remember Me'. A link for 'Two Factor Authentication' is located next to the 'Remember Me' checkbox. Below these is a 'Language' dropdown menu currently set to 'ENGLISH'. At the bottom of the form is a blue 'Sign In' button.

2-3. ZPA 管理ポータルの管理者設定方法

本項では ZPA 管理ポータルにログインをすることができる管理者の設定方法について説明します。

2-3-1. 管理者ロールの設定方法

管理者ロールでは、それぞれの管理者に対してどのような権限を与えるかをロールとして設定します。

- (1) ZPA 管理ポータルを開きます。
- (2) 左側メニューより、「Configuration Control」>「Administration Control」>「Roles」より管理者に与えられる権限を設定します。
- (3) 右上の「Add Role」をクリックします。
- (4) それぞれのメニューに対しての権限を設定し、「Save」をクリックします。

Add Role

Name

Description

ACCESS CONTROL [Expand All](#)

> Administration Control Enable Disable

> Authentication Enable Disable

> Branch Connector Management Enable Disable

> Browser Isolation Enable Disable

> Certificate Management Enable Disable

> API Key Management Enable Disable

Save Cancel

Administration Control Enable Disable

The following settings are recommended for Administration Control

Administrators Full Read Only

Client Connector IP Assignment Full Read Only

Roles Read Only

Zscaler Cloud Sandbox Full Read Only

Audit Logs Full Read Only

Disaster Recovery Full Read Only

User Portal AUP Full Read Only

Fullに権限を与えるか、
Read Only(閲覧のみ)の指定が
可能です。

2-3-2. 管理者の追加方法

- (1) ZPA ポータルを開き、左側メニュー「Configuration Control」>「Administration Control」>「Administrators」をクリックします。
- (2) 「Add Administrator」をクリックします。
- (3) 設定内容を入力し、「Save」をクリックします。

Add Administrator ✕

Admin ID
demo@hogehoge.co.jp

Email
demo@hogehoge.co.jp

Phone
+8100000000000

Role
ZPA Administrator ⊕ ▾

Status
 Enabled Disabled

Two Factor Authentication
 On Off

Force Password Reset
 Yes No

Pin Session
 Yes No

Password

Roll を指定します。

3. IdP Configuration

3-1. 概要

ZPA を利用するためには、SAML 認証が必要となります。

ZPA で SAML 認証を行うにあたり、ご利用の IdP との連携のための設定が必要です。

本項では IdP の設定方法について説明します。

3-2. IdP の設定方法

(1) ZPA ポータルを開き、左側メニュー「Authentication」>「User Authentication」>「IdP Configuration」をクリックします。

(2) 「Add IdP Configuration」をクリックします。

(3) 必要事項を入力し、「Next」をクリックします。

Add IdP Configuration

1 IdP Information 2 SP Metadata 3 Create IdP

Name

Single Sign-On

Admin User

User SP Certificate Rotation

ZPA User SSO Service Provider Certificate - Jan 18 03:14:07 2038 GMT

Domains

Select

Use with Arbitrary Domains

Enabled Disabled

Next Cancel

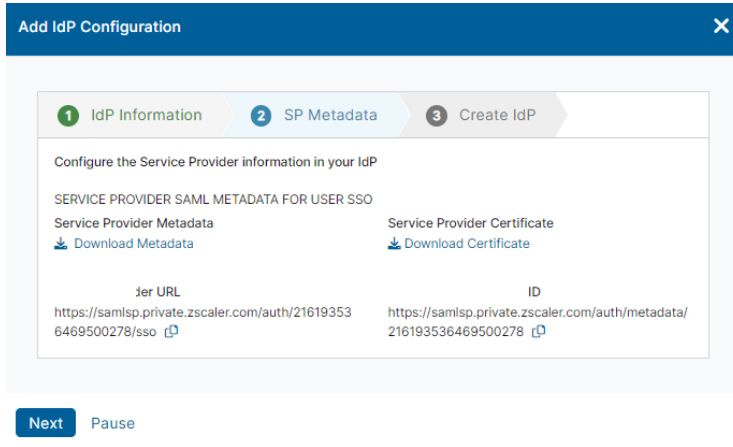
Domains
ZPA ポータルに登録されているドメインが表示されます。
ドメインを追加したい場合は弊社サポート窓口までご連絡ください。

Name: 半角英数で入力します。

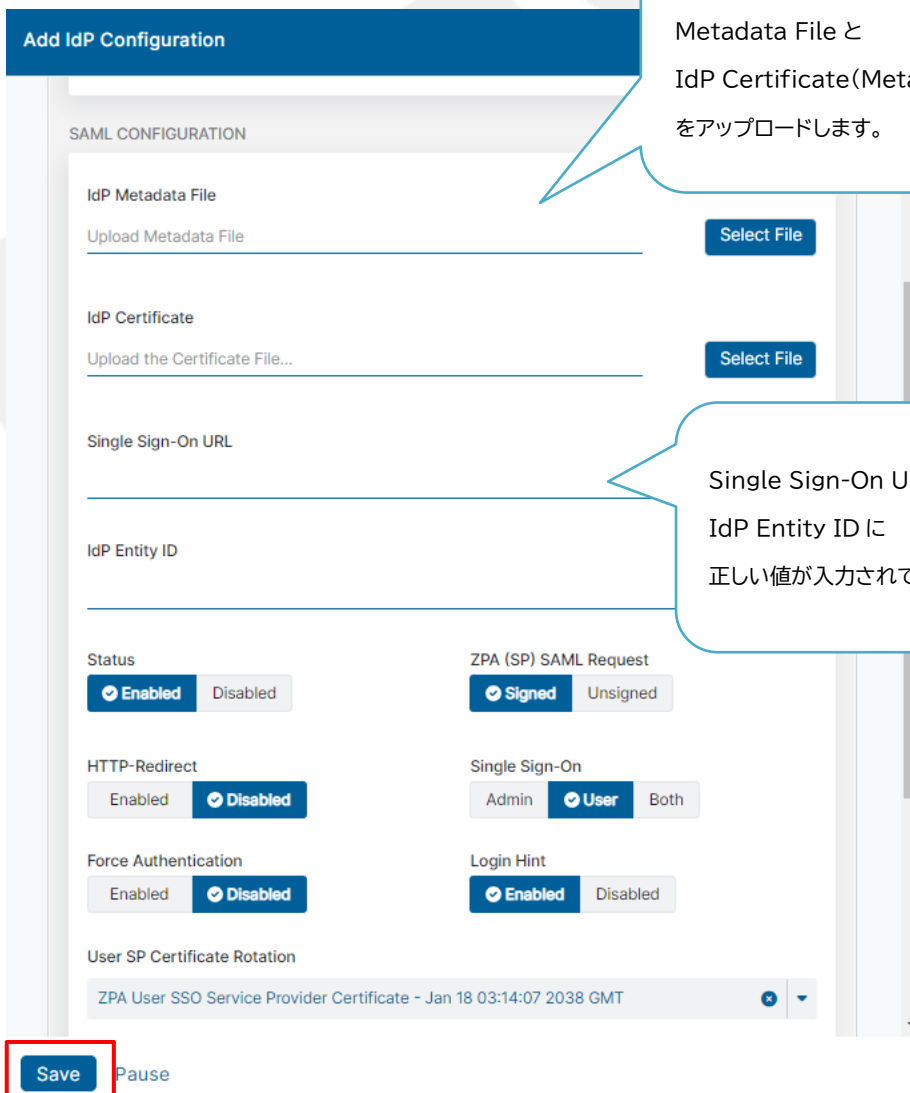
Single Sign-On: ユーザー認証用か、管理ポータルにログインをする管理者の認証用かを選択します。

Domains: 認証に利用をするドメインを選択します。

- (4) IdP 側での設定が必要な、Metadata や Service Provider URL 等が表示されるので、情報を控えて、「Pause」をクリックします。
 ご利用の IdP 側で控えた情報の設定が必要です。



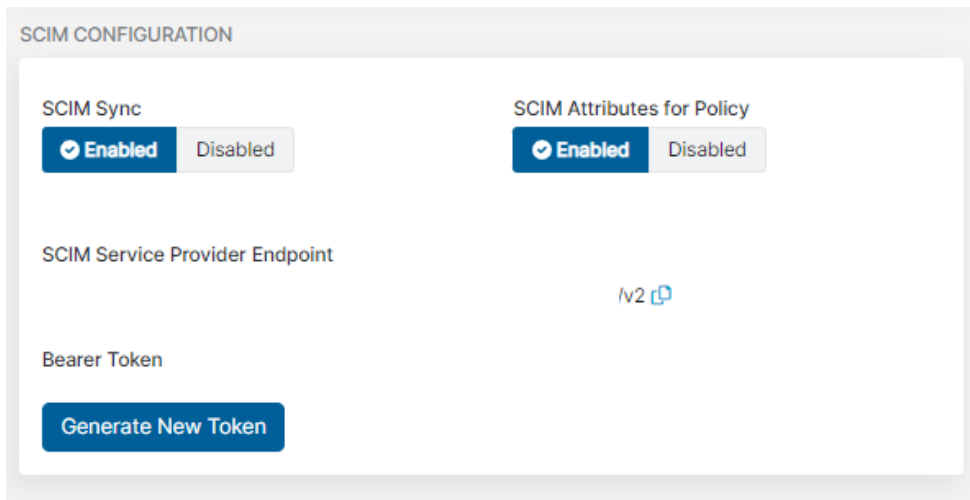
- (5) 各設定項目を入力し、「Save」をクリックします。



IdP 側からダウンロードした Metadata File と IdP Certificate (Metadata に含まれない場合) をアップロードします。

Single Sign-On URL と IdP Entity ID に正しい値が入力されているかご確認ください。

ご利用の IdP 側が SCIM に対応している場合は、SCIM の利用が可能です。
SCIM を利用する場合は下記設定を有効にご設定ください。



SCIM CONFIGURATION

SCIM Sync Enabled Disabled

SCIM Attributes for Policy Enabled Disabled

SCIM Service Provider Endpoint v2

Bearer Token

[Generate New Token](#)

「SCIM Service Provider Endpoint」の情報を控えます。

「Generate New Token」をクリックし、トークンを発行後 IdP 側での設定が必要となります。

4. App Connector

4-1. 概要

本項では App Connector の設定方法について説明します。

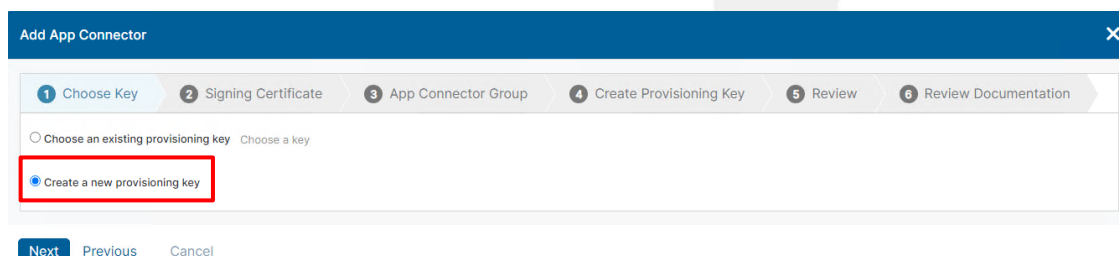
4-2. Provisioning Key の作成

(1) ZPA ポータルを開き、左側メニュー「Configuration&Control」>

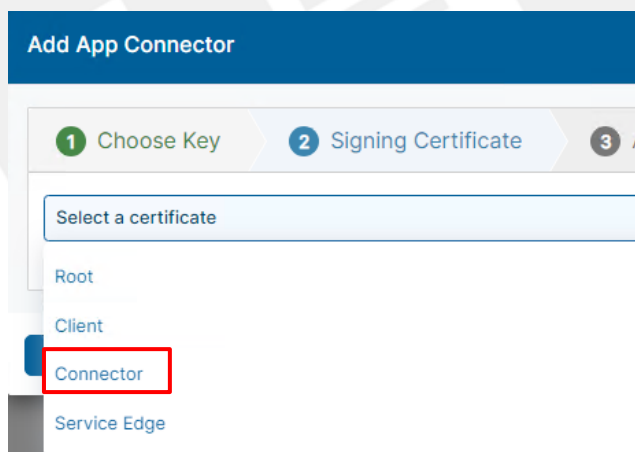
「Private Infrastructure」>「App Connectors」をクリックします。

(2)「Add App Connector」をクリックします。

(3)「Create a new provisioning key」を選択し、「Next」をクリックします。



(4)「Select a certificate」のプルダウンを開き「Connector」を選択し、「Next」をクリックします。



(5)「Add Connector Group」のタブを選択し、各設定項目を入力し「Next」をクリックします。

Add App Connector
✕

1 Choose Key 2 Signing Certificate 3 App Connector Group 4 Create Provisioning Key 5 Review 6 Review Documentation

Select App Connector Group Add App Connector Group

Name Status

Demo
 Enabled
 Disabled

Description

IPv4 DNS Resolution Only TCP Quick Acknowledgement

Enabled Disabled Enabled Disabled

Disaster Recovery Disable AppProtection

Enabled Disabled Yes No

VERSION PROFILE CONFIGURATION

Persist Local Version Profile Version Profile

Enabled Disabled Default (Inherited from customer level mapping)

半角英数で名称を指定します。

App Connector Software Update Schedule

Monday + - at 00:00

Next Periodic Software Update is on

📍 App Connector Location

Tokyo, 日本

App Connector を設置するロケーションを入力します。
ここで設定されたロケーションの情報に従い ZPA クラウドと通信を行う形となるため、正しい情報を入力してください。

日本、東京都

Latitude	Longitude	Country Code
35.6764225	139.650027	JP

Location Details

日本、東京都

Next
Previous
Cancel

App Connector のソフトウェアアップデートを実施する時間を指定します。

※1つの Connector Group 配下で、複数の App Connector を設定している場合、順次1つずつアップデートを実施します。

(6) Provisioning Key の名称を定義します。

Add App Connector

1 Choose Key 2 Signing Certificate

Name
Demo

Maximum Reuse of Provisioning Key
10

該当の Provisioning Key を利用して
デプロイできる App Connector の数
を指定します。

Next Previous Cancel

(7) 内容を確認の上、「Save」をクリックします。

Add App Connector

1 Choose Key 2 Signing Certificate 3 App Connector Group

Certificate Name
Connector
App Connector Group
Demo
Provisioning Key
Demo

Review all of the information before clicking Save

Save Previous Cancel

(8) Provisioning Key が表示されるので、メモ帳などに控えておきます。

4-3. App Connector の作成

本項ではApp Connectorの作成方法について説明します。

本書では例として Vmware プラットフォームに App Connector の作成を実施しています。
サポートプラットフォームは下記の通りです。

サポートプラットフォーム

- Amazon Web Service(AWS)
- CentOS

- Oracle
- Redhat
- Microsoft Azure
- Microsoft Hyper-V
- Vmware アプライアンス(Vmware vCenter)
- Vmware アプライアンス (vSphere Hypervisor (ESXi))
- Nutanix
- Docker
- Openshift

4-3-1. App Connector のデプロイ

App Connector を各プラットフォームの手順に従ってデプロイします。

各プラットフォームのデプロイの手順に関しましては下記URLをご確認ください。

AmazonWeb Services(AWS)

<https://help.zscaler.com/zpa/connector-deployment-guide-amazon-web-services>

CentOS, Oracle, Red Hat

<https://help.zscaler.com/zpa/connector-deployment-guide-centos-oracle-and-redhat>

Microsoft Azure

<https://help.zscaler.com/zpa/connector-deployment-guide-microsoft-azure>

Microsoft Hyper-V

<https://help.zscaler.com/zpa/connector-deployment-guide-microsoft-hyper-v>

VMware

<https://help.zscaler.com/zpa/connector-deployment-guide-vmware-platforms>

Nutanix

<https://help.zscaler.com/zpa/app-connector-deployment-guide-nutanix-ahv>

Docker

<https://help.zscaler.com/zpa/app-connector-deployment-guide-docker>

OpenShift

<https://help.zscaler.com/zpa/app-connector-deployment-guide-openshift>

4-3-2. App Connector コンソールへのログイン

App Connector コンソールへログインをします。

デフォルトのユーザー名とパスワードは以下の通りです。

```
UM Default Username: admin
UM Default Password: zscaler

Zscaler Private Access Connector (CentOS Linux 7 (Core))
Kernel 3.10.0-1160.105.1.el7.x86_64 on an x86_64

zpa-connector login: admin
Password: _
```

Username:admin
Password:zscaler

4-3-3. ネットワークアドレスの設定

ネットワークアドレスの設定を行います。

(1) スタティック IP の場合、「sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0」を実行し、ネットワークの設定を下記のように書き換えます。

BOOTPROTO="none"

IPADDR="xxx.xxx.xxx.100"(App Connector の IP)

NETMASK="255.255.255.0"

GATEWAY="xxx.xxx.xxx.254"(デフォルトゲートウェイの IP)

```
BOOTPROTO="none"
IPADDR="172.17.
NETMASK="255.255.255.0"
GATEWAY="172.17.
~
~
~
```

(2)「sudo systemctl restart network」を実行し、ネットワーク設定を再起動します。

4-3-4. DNS サーバーの設定

DNS サーバーの設定を行います。

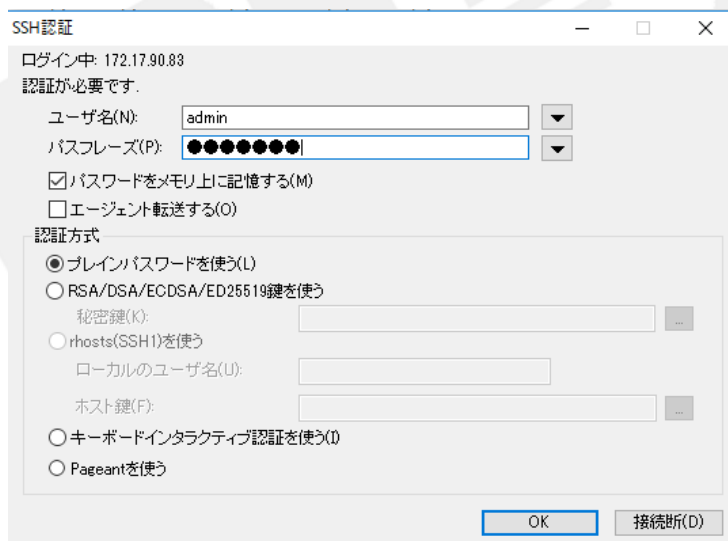
(1)「sudo vi /etc/resolv.conf」を実行し、参照先の DNS サーバーを下記のように指定します。
nameserver xxx.xxx.xxx.xxx(任意のアドレス)

```
nameserver 10.  
~  
~
```

4-3-5. Provisioning Key の適用

ZPA ポータル側で作成をした Provisioning Key を App Connector に適用します。

(1)「sudo systemctl start sshd」を実行し、SSH を起動させ、SSH にて管理アクセスを実施します。



(2)「sudo systemctl stop zpa-connector」を実行し、App Connector を一時停止します。

(3) 下記2つのコマンドを実行します。

```
「sudo touch /opt/zscaler/var/provision_key」
```

```
「sudo chmod 644 /opt/zscaler/var/provision_key」
```

- (4) 「sudo vi /opt/zscaler/var/provision_key」を実行し、発行された Provisioning Key をコピー&ペーストします。
- (5) 「sudo cat /opt/zscaler/var/provision_key」を実行し、Provisioning Key の内容が正しいかを確認します。
- (6) 「sudo systemctl start zpa-connector」を実行し、App Connector を起動します。
- (7) 「sudo systemctl status zpa-connector」を実行し、ステータスが「Active」になっていることを確認します。

```
● zpa-connector.service - Zscaler Private Access Connector
   Loaded: loaded (/usr/lib/systemd/system/zpa-connector.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-02-14 05:16:22 UTC; 6 days ago
     Main PID: 20828 (zpa-connector)
    CGroup: /system.slice/zpa-connector.service
            └─20828 /opt/zscaler/bin/zpa-connector
            └─24403 zpa-connector-child
            └─24440 guacd -l 4822 -b 127.0.0.1 -p /opt/zscaler/var/guacd/var/run/guacd.pid -L debug -f
```

- (8) ZPA 管理ポータル内、「Configuration&Control」>「Private Infrastructure」>「App Connectors」にて作成した App Connector が追加されていることを確認します。

5. Application Segment

5-1. 概要

ZPA の対象としたいアプリケーションを登録したものを「Application Segment」と呼んでいます。

本項では「Application Segment」の設定方法について説明します。

5-2. Application Segment の作成

Application Segment の作成方法について説明します。

- (1) ZPA 管理ポータルを開き、「Resource Management」>「Application Management」>「Application Segments」をクリックします。
- (2) 「Add Application Segment」をクリックします。
- (3) 各種設定を入力し、「Next」をクリックします。

Add Application Segment

1 Define Applications 2 Segment Group 3 Server Groups 4 Servers 5 Review 6 Policies

GENERAL INFORMATION

Name

Status Enabled Disabled

Disaster Recovery Enabled Disabled

Source IP Anchor Enabled Disabled

Description

半角英数で指定します。

APPLICATIONS

search by name, certificate, port, protocol

Applications

Enter a domain or IP address

Access Type Browser Access AppProtection

アクセス先となる宛先を IP アドレスまたは、FQDN で指定をします。
ワイルドカードでの指定や、IP アドレスレンジでの指定も可能です。
※ワイルドカードは先頭のみ利用可能です。

CLIENT CONNECTOR ACCESS

Default Port Ranges: Select

TCP Keepalive: Enabled Disabled

TCP Port Ranges: From... To... アプリケーションの受信ポートを指定します。

UDP Port Ranges: From... To...

ADDITIONAL CONFIGURATION

Double Encryption: Enabled Disabled

ICMP Access: Enabled Disabled

Bypass during Reauthentication: Enabled Disabled

Bypass: Use Client Forwarding Policy, Use Client Forwarding Policy, Always, On Corporate Network

COMMON CONFIGURATION

Health Reporting: Continuous On Access None

App Connector Selection Method: Closer to Application Closer to User

ユーザーが ZPA をバイパスしてアプリケーションにアクセスできるタイミングを指定します。デフォルトでは「Client Forwarding Policy」が指定されています。

Bypass

- Use Client Forwarding Policy
- Use Client Forwarding Policy
- Always
- On Corporate Network

Use Client Forwarding Policy
⇒ Client Forwarding Policy の設定内容に従う

Always
⇒ 常にバイパスする

On Corporate Network
⇒ 社内ネットワーク接続時にバイパスする

(4)「Add Segment Group」のタブを選択し、各種設定を入力し、「Next」をクリックします。ここでは Application Segments に紐づける「Segment Group」を定義します。Segment Group を指定したポリシーの作成が可能です。

Select Segment Group | **Add Segment Group**

Name

Description

Status: Enabled Disabled

Next Previous Skip Cancel

- (5) 「Add Server Group」のタブを選択し、各種設定を入力し、「Next」をクリックします。
 ここでは、「Server Group」を定義します。

- (6) 設定内容を確認し、「Save」をクリックします。

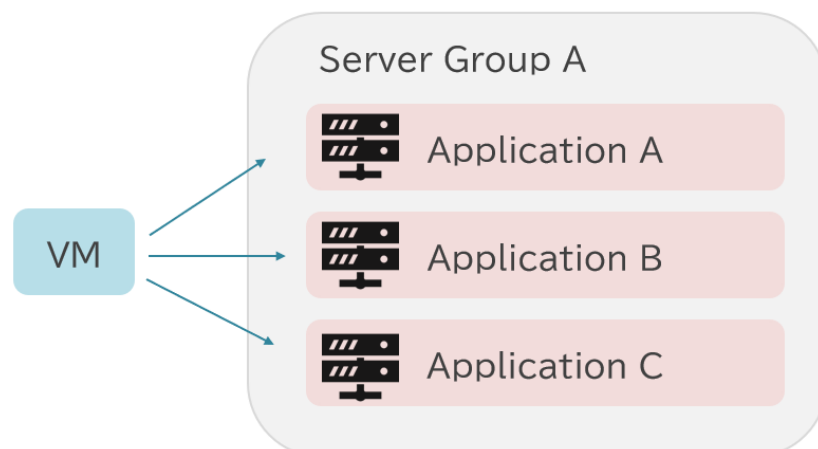
5-3. 【補足】Server Group/Servers の推奨設定

5-3-1. 推奨設定

複数のサーバーやアプリケーションに接続をする場合、「Server」単体を設定せず、「Dynamic Server Discovery」を有効化した Server Groups を設定します。基本的に「Servers」の設定は使用しません。

Dynamic Server Discovery を有効にすることで IP アドレスでの指定や FQDN に加えてワイルドカードを使用することが可能となります。

(例) 複数のサーバーやアプリケーションにアクセスする構成



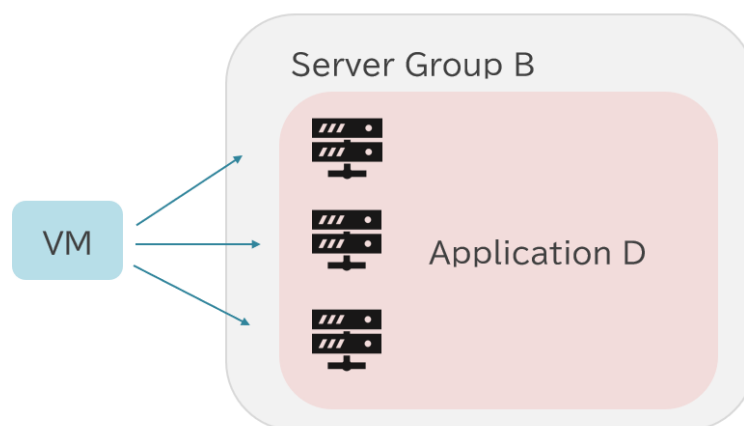
- (1) ZPA ポータルを開き、左側メニュー「Configuration & Control」をクリックし、「Server Groups」をクリックします。
- (2) 「Add Server Groups」をクリックします。
- (3) 設定内容を入力し、「Save」をクリックします」

※「Server Groups」の追加は、「Application Segment」作成時でも可能です。

5-3-2. 例外設定

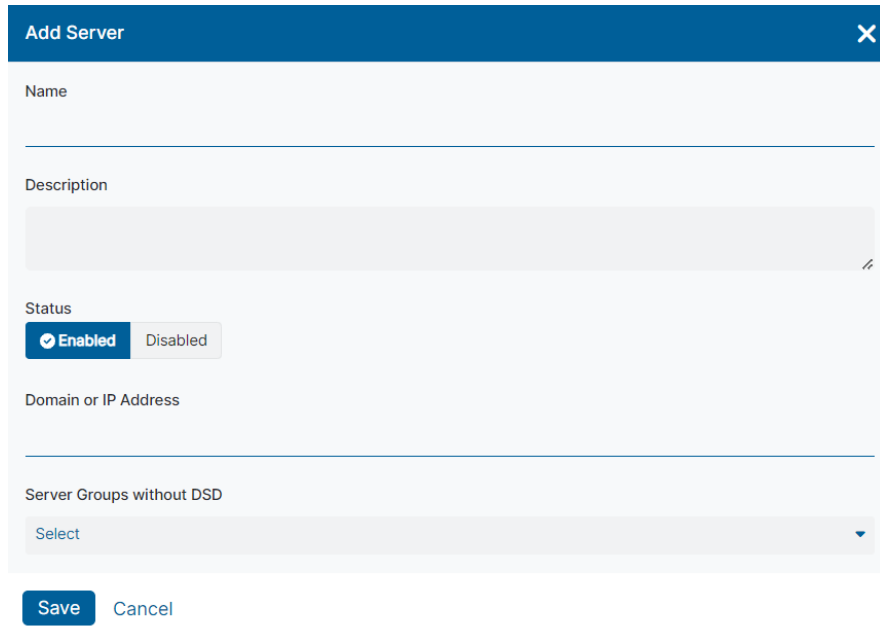
基本的に「Servers」の設定は利用しませんが、下記のような構成の場合は「Servers」に各サーバーのアドレスを登録します。

(例)単一のアプリケーションを複数のサーバーで構成している場合



「Servers」に各サーバーのアドレスを登録し、「Server Group」にて登録済みの各サーバーを指定することで、App Connector 側でロードバランシングを行うことが可能です。

- (1) ZPA ポータルを開き、左側メニュー「Configuration & Control」をクリックし、「Servers」をクリックします。
- (2) 「Add Server」をクリックします。
- (3) 設定内容を入力し、「Save」をクリックします



- (4) ZPA ポータルを開き、左側メニュー「Configuration & Control」をクリックし、「Server Groups」をクリックします。
- (5) 「Add Server Groups」をクリックします。
- (6) 「Dynamic Server Discovery」を Disable に変更の上、設定内容を入力し、「Save」をクリックします



6. Access Policy

6-1. 概要

ZPA 経由でのアクセスを実現するために、作成した Application Segment に対してのアクセス制御用のポリシーの作成が必要です。

本項では Access Policy の設定方法について説明します。

6-2. Access Policy の作成

Access Policy の作成方法について説明します。

(1) ZPA 管理ポータルを開き、左側メニュー「Policy」>「Access Policy」をクリックします。

(2) 「Add Rule」をクリックします。

(3) 設定内容を入力し「Save」をクリックします。

Add Access Policy

Name

Description

ACTION

Rule Action: Allow Access Block Access Require Approval

App Connector Selection Method: All App Connector groups

Message to User

CRITERIA

Applications
Branch Connector Groups
Client Connector Posture Profiles
Client Connector Trusted Networks
Client Types
Cloud Connector Groups
Country Codes
Locations
Machine Groups
Platforms
SAML and SCIM Attributes

+ Add Criteria

Save Cancel

CRITERIA

- Application Segments
 - Select one or more application segments
- OR
- Segment Groups
 - Select one or more segment groups
- AND
- SAML and SCIM Attributes
 - Select one or more SAML and SCIM attributes

対象の宛先を「Application Segments」または「Segment Groups」で指定します。

対象のユーザー等を指定したい場合は、SAML and SCIM Attributes で指定をします。

6-3. 【補足】ポリシーの Rule Order について

ポリシーは「Rule Order」が若い順に評価されます。

Rule Order	Name	Rule Action
> 1	Allow Internal Application Group	✔ Allow Access
> 2	AP-1	✔ Allow Access
> 3	Ebihara Test	✔ Allow Access

左側の数字をクリックし、任意の数字を入力することで Rule Order の順番を変更することが可能です。

Rule Order

- > 1
- >
- > 3

7. Timeout Policy

7-1. 概要

ZPA はリモートアクセスを実現するための製品なので、機密性の高い情報にアクセスをする場合があります。そのため、一定の期間ごとに再認証を求めめるためのポリシーを Timeout Policy を作成することで定義することが可能です。

本項では Timeout Policy の設定方法について説明します。

7-2. Default Timeout Policy

ZPA 側で用意されているデフォルトのタイムアウトポリシーは 7 日間で設定されています。

最後に ZPA で認証を行ってから 7 日経過後に ZPA の対象の宛先にアクセスをした際に再認証が求められる動作となります。

Default Rule

Name	Timeouts
Default_Rule	AUTHENTICATION TIMEOUT 7 Day(s)
	IDLE CONNECTION TIMEOUT Default
Description	CRITERIA
This is the default Timeout Policy rule	<ul style="list-style-type: none"> Application Segments Any Application Segment OR Segment Groups Any Segment Group AND SAML and SCIM Attributes Any SAML and SCIM Attributes from any IdP AND Client Types Any Client Type AND Client Connector Posture Profiles Any Posture Profile AND Platforms Any Platform

7-3. Timeout Policy の作成

Timeout Policy の作成方法について説明します。

- (1) ZPA ポータルを開き、左側メニュー「Policy」>「Timeout Policy」をクリックします。
- (2) 「Add Rule」をクリックします。

(3) 設定内容を入力し「Save」をクリックします。

Add Timeout Policy [X]

Name

Description

認証タイムアウトの期間を指定します。
最小値は「10分」となります。

TIMEOUTS

Authentication Timeout

Never Specific Interval 2 Day(s)

Day(s)
Hour(s)
Minute(s)

Message to User

一定以上セッションがアイドル状態になった場合に、セッションをタイムアウト(切断)させることができます。

Idle Connection Timeout

Default Specific Interval 10 Minute(s)

CRITERIA

Applications
Client Connector Posture Profiles
Client Types
Platforms
SAML and SCIM Attributes
+ Add Criteria

「Add Criteria」をクリックし、対象の Application Segment やユーザー等を指定します。

Save Cancel

8. Client Forwarding Policy

8-1. 概要

Client Forwarding Policy は ZPA から除外したい宛先がある場合に利用するためのポリシーとなります。ZPA から除外をしたい宛先がある場合は、下記の手順で設定を行います。

- (1) 除外をしたい対象の宛先を登録した Application Segments を作成する
- (2) 上記(1)で作成をした Application Segments を指定した Client Forwarding Policy を作成する

本項では、Client Forwarding Policy の設定方法について説明します。

8-2. Client Forwarding Policy の作成

Client Forwarding Policy の作成方法について説明します。

- (1) ZPA ポータルを開き、左側メニュー「Policy」>「Client Forwarding Policy」をクリックします。
- (2) 「Add Rule」をクリックします。
- (3) 設定内容を入力し「Save」をクリックします

Add Client Forwarding Policy

Name

Description

ACTION

Rule Action

Forward to ZPA Only Forward Allowed Applications Bypass ZPA

アクションを指定します。

Forward to ZPA
⇒ZPA にトラフィックを転送します。

Only Forward Allowed Applications
⇒Access Policy にて許可されたアプリケーションのみ ZPA に転送します。

Bypass ZPA
⇒ZPA から除外されます。

ACTION

Rule Action

Forward to ZPA
 Only Forward Allowed Applications
 Bypass ZPA

CRITERIA

「Add Criteria」をクリックし、対象の Application Segment 等の条件を指定します。

- Applications
- Branch Connector Groups
- Client Connector Posture Profiles
- Client Connector Trusted Networks
- Client Types
- Cloud Connector Groups
- Machine Groups
- Platforms
- SAML and SCIM Attributes

