



はじめての ZPA (Zscaler Private Access)

ゼットスケラー 株式会社

ZSCALER CONFIDENTIAL INFORMATION

コンテンツ一覧

コンテンツ一覧	2
1. 本ドキュメントについて	3
2. 環境について	4
2-1. SAML認証基板について	4
2-2. トポロジー図について	5
3. 基本設定	7
3-1. SP (ZPA) とIdP (okta) のSAML認証連携設定	7
3-2. Connector, Zscaler App Enroll用の証明書作成	29
3-3. Connectorのインストール.....	34
3-4. Application Segmentation / Access Policyの設定	50
3-5. Zscaler Appのインストール	70
4. 動作確認	75
4-1. 社内リソースへのアクセス	76
4-2. ログの確認	81
5. Dynamic Server Discovery について	83
6. その他の設定	95
5-1. Forwarding Profile, App Profileの設定	95
5-2. Device Postureの設定	100

1. 本ドキュメントについて

本ドキュメントは Zscaler Private Access（以降 ZPA）を初めて触る方を主な対象として、基本的な設定から動作確認までの流れの手順を纏めたドキュメントとなります。本ドキュメントを通して、ZPA の基本的な設定や動作イメージを理解することが可能です。

本ドキュメントは、詳細な内容を避け可能な限りシンプルかつポイントを絞るよう心掛けています。より詳細な情報については、オンラインドキュメント「<https://help.zscaler.com/zpa>」も合わせてご確認ください。

本ドキュメントに記載の内容は、技術的な内容を含めお客様実環境での動作を保証するものではありません。

ZPA の導入をご検討の場合には、弊社担当や販売パートナー様にご連絡の上、お客様実環境での動作確認、検証を実施いただくことを強く推奨いたします。

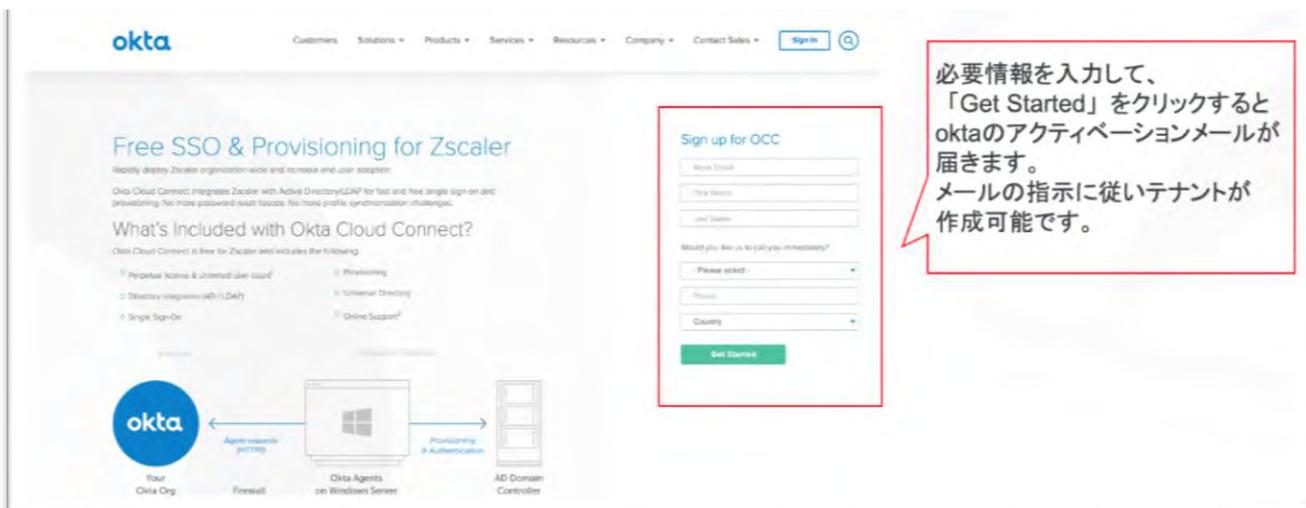
2. 環境について

2-1. SAML 認証基板について

ZPA を使用するためには SAML 認証基板（okta や Azure AD など）と連携させる必要があります。「<https://www.okta.com/zscaler/>」 より ZPA のみ SAML 連携可能な Okta のテナントを無料で作成が可能です。

本ドキュメントでは、SAML 認証基板として okta を使用します。

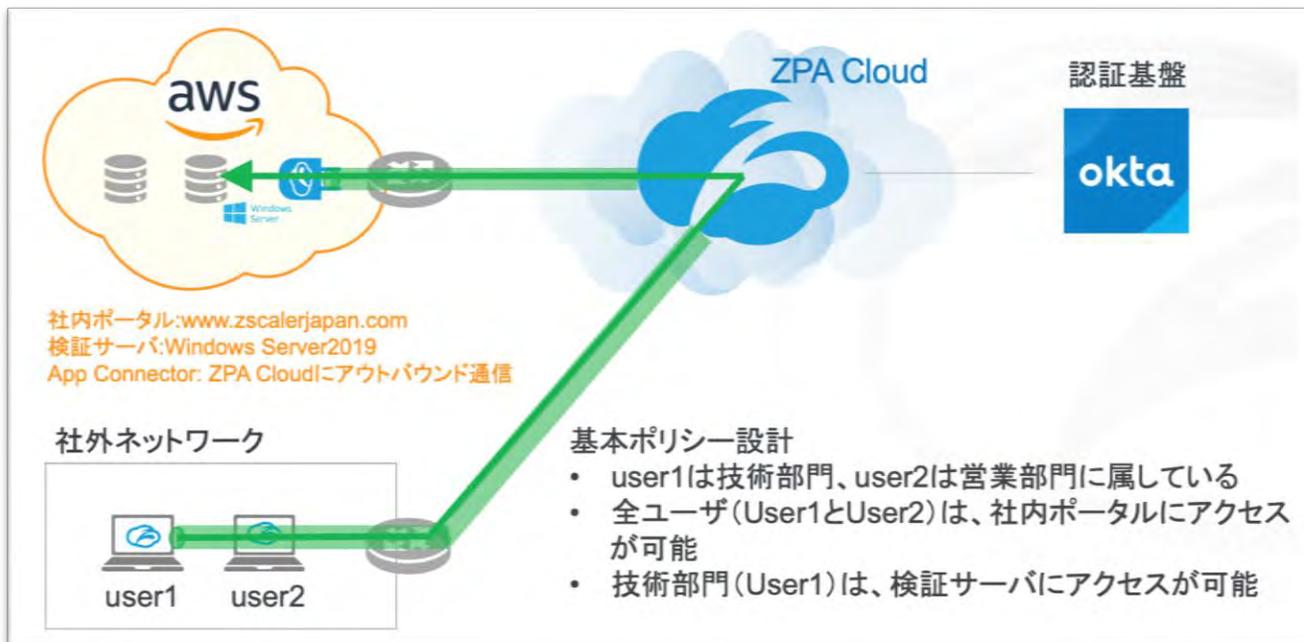
SAML 認証基板を持ってないけれど ZPA を触ってみたいという方は、テナントのリクエストをして下さい。



The screenshot shows the Okta website's landing page for Zscaler integration. The main heading is "Free SSO & Provisioning for Zscaler". Below this, there is a "Sign up for OCC" form with fields for Work Email, First Name, Last Name, Phone, and Country. A green "Get Started" button is at the bottom of the form. A red box highlights the form area. A callout bubble with a red border and a pointer to the "Get Started" button contains the following Japanese text:

必要情報を入力して、「Get Started」をクリックすると okta のアクティベーションメールが届きます。メールの指示に従いテナントが作成可能です。

2-2. トポロジー図について



Note

- ✓ ZPA では、Zscaler App – ZPA Cloud 間の TLS トンネルと Connector - ZPA Cloud 間の TLS トンネルを紐付けすることにより、社外端末から社内アプリのアクセスを実現
- ✓ Connector は常にアウトバウンド方向 (Connector -> ZPA Cloud) にトンネルを構築するため、Connector 自身に Public IP を付与する必要がない

本ドキュメントの「3. 基本設定」章では、シンプルかつ短時間で ZPA 環境を構築するために上記トポロジー図中の主に以下 4 つの手順が含まれます。

※AWS 内の VPC やサーバのデプロイは含まれていません

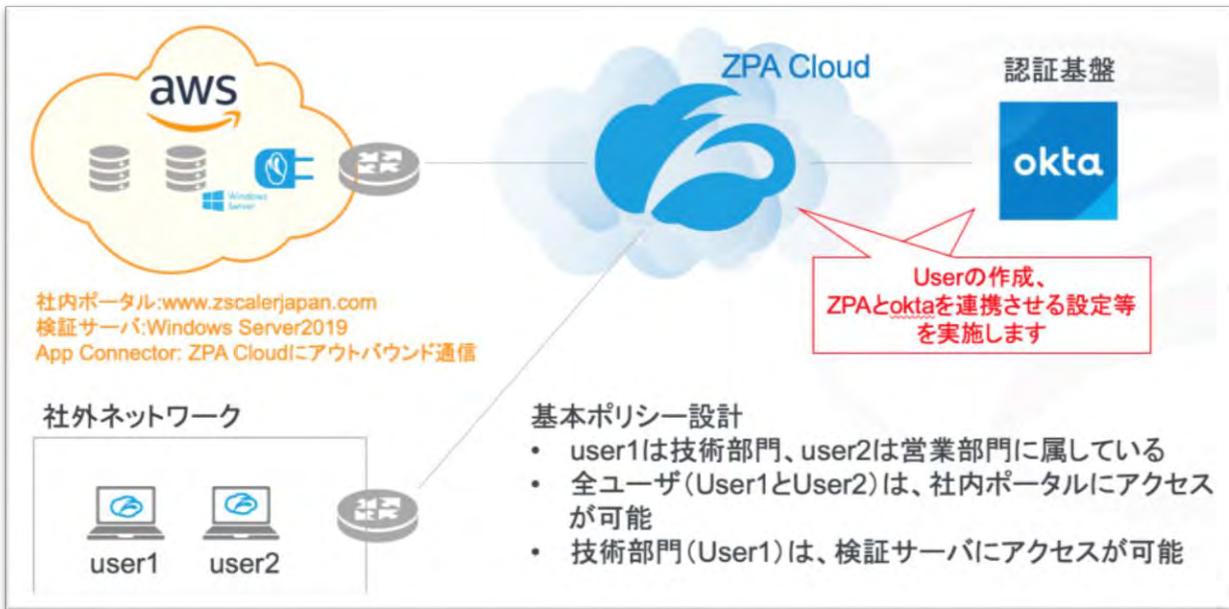
- SP (ZPA) と IdP (okta) の連携
- Zscaler App (user1 のみ) 、Connector のインストール

- Application Segmentation、Access Policy の設定（社内アプリの定義、どのユーザがどのアプリにアクセス可能かの定義）
- 動作確認

「5. その他の設定」章では、より柔軟な設計をするための情報を記載しておりますので、こちらもご確認ください。

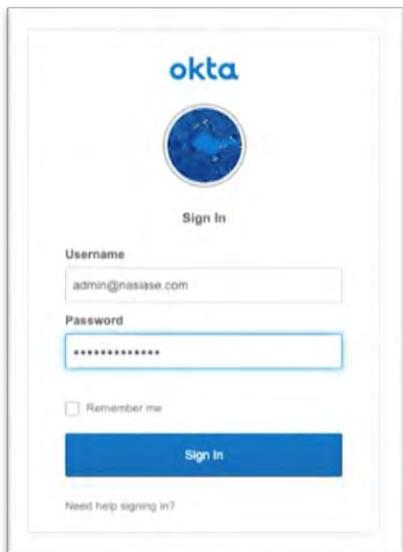
3. 基本設定

3-1. SP (ZPA) と IdP (okta) の SAML 認証連携設定



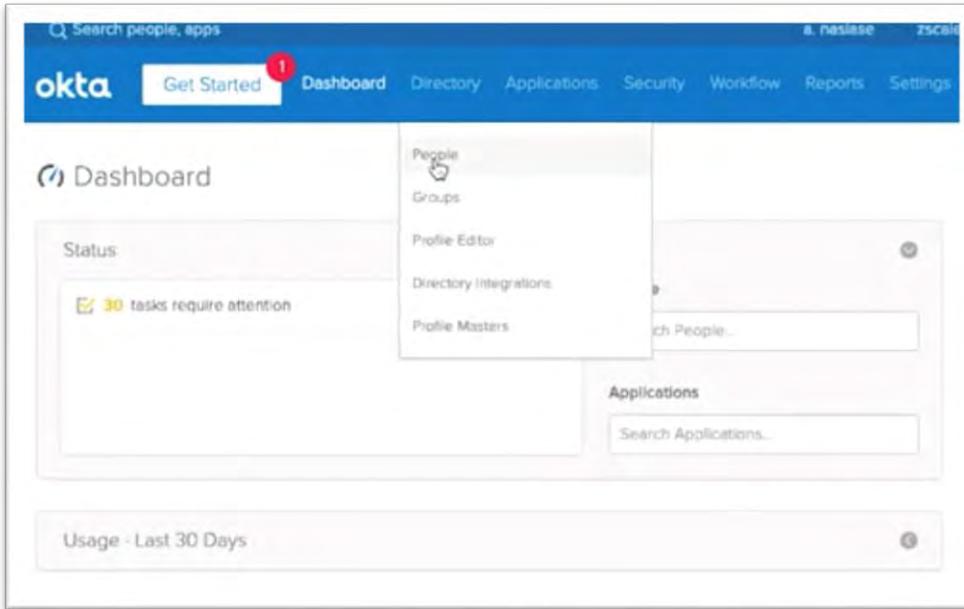
Step1. ユーザ (user1、user2) の作成

okta に admin アカウントでログインします。

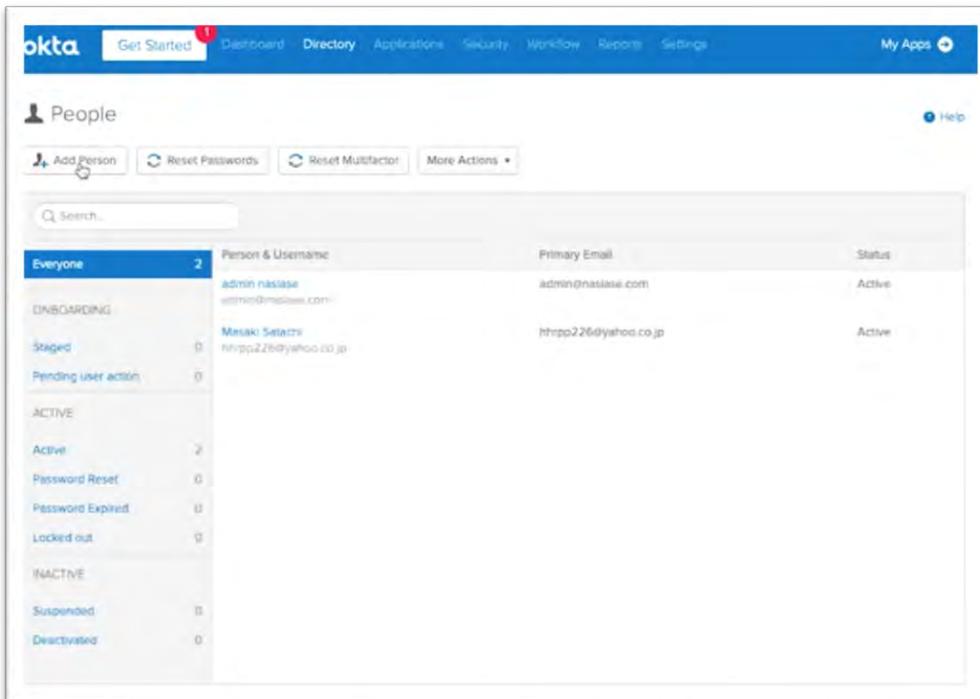


はじめての ZPA

Directoryより、[People] をクリックします。



[Add Person]をクリックします。



はじめての ZPA

下図を参考に必要事項を記入して、user1、user2 を作成します。

The 'Add Person' form for user1 contains the following information:

- First name: user1
- Last name: nashiase
- Username: user1@nashiase.com
- Primary email: user1@nashiase.com
- Secondary email (optional):
- Groups (optional): You haven't added any groups
- Password: Set by admin
- User must change password on first login

Buttons at the bottom: Save, Save and Add Another, Cancel.

The 'Add Person' form for user2 contains the following information:

- First name: user2
- Last name: nashiase
- Username: user2@nashiase.com
- Primary email: user2@nashiase.com
- Secondary email (optional):
- Groups (optional): You haven't added any groups
- Password: Set by admin
- User must change password on first login

Buttons at the bottom: Save, Save and Add Another, Cancel.

Step2. Tech_Div (技術部門) と Sales_Div (営業部門) のグループの作成

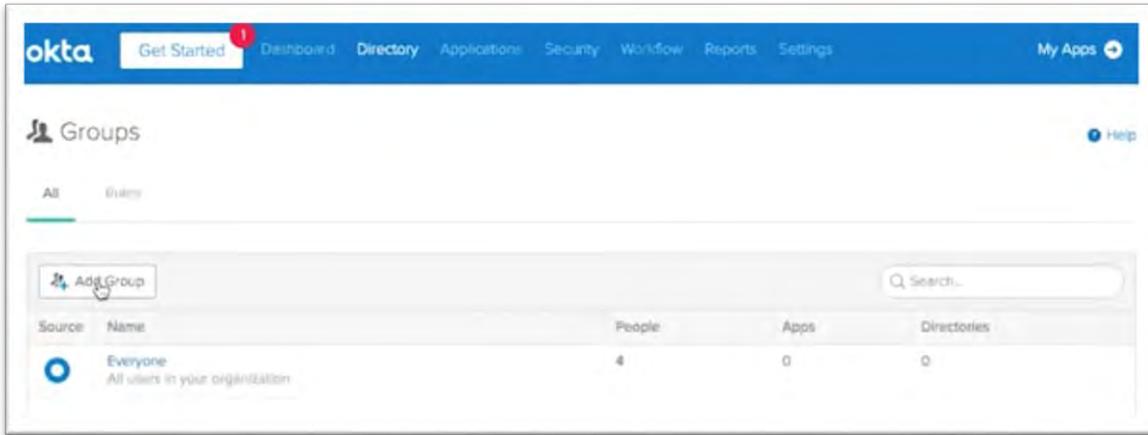
Directory より、[Groups]をクリックします。

The screenshot shows the Okta Directory page. The 'Groups' menu item is highlighted in the navigation pane on the left. The main content area shows a table of users:

Person & Username	Primary Email	Status
admin nashiase admin@nashiase.com	admin@nashiase.com	Active
user1 nashiase user1@nashiase.com	user1@nashiase.com	Active
user2 nashiase user2@nashiase.com	user2@nashiase.com	Active
Mesaki Satachi hhpp226@yahoo.co.jp	hhpp226@yahoo.co.jp	Active

はじめての ZPA

[Add Group]をクリックします。



Add Group

Add groups so you can quickly perform actions across large sets of people.

Name:

Group Description:

Add Group

Add groups so you can quickly perform actions across large sets of people.

Name:

Group Description:

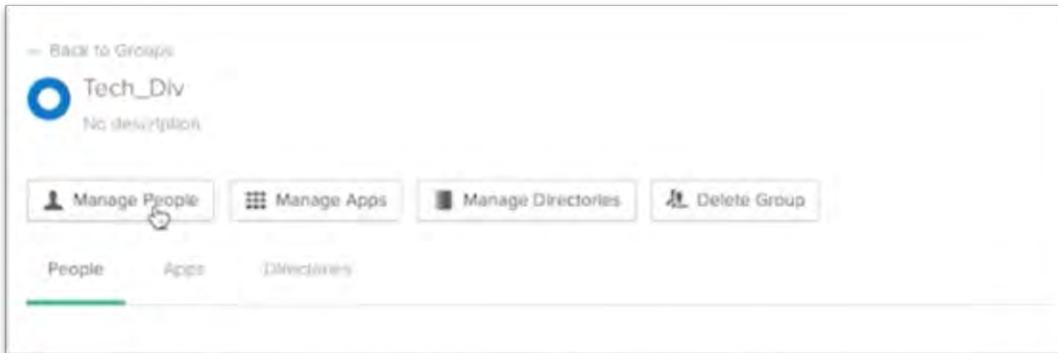
Step4. User のグループ紐付け (user1 に Tech_Div を Sales_Div に user2)

[Tech_Div]をクリックします。

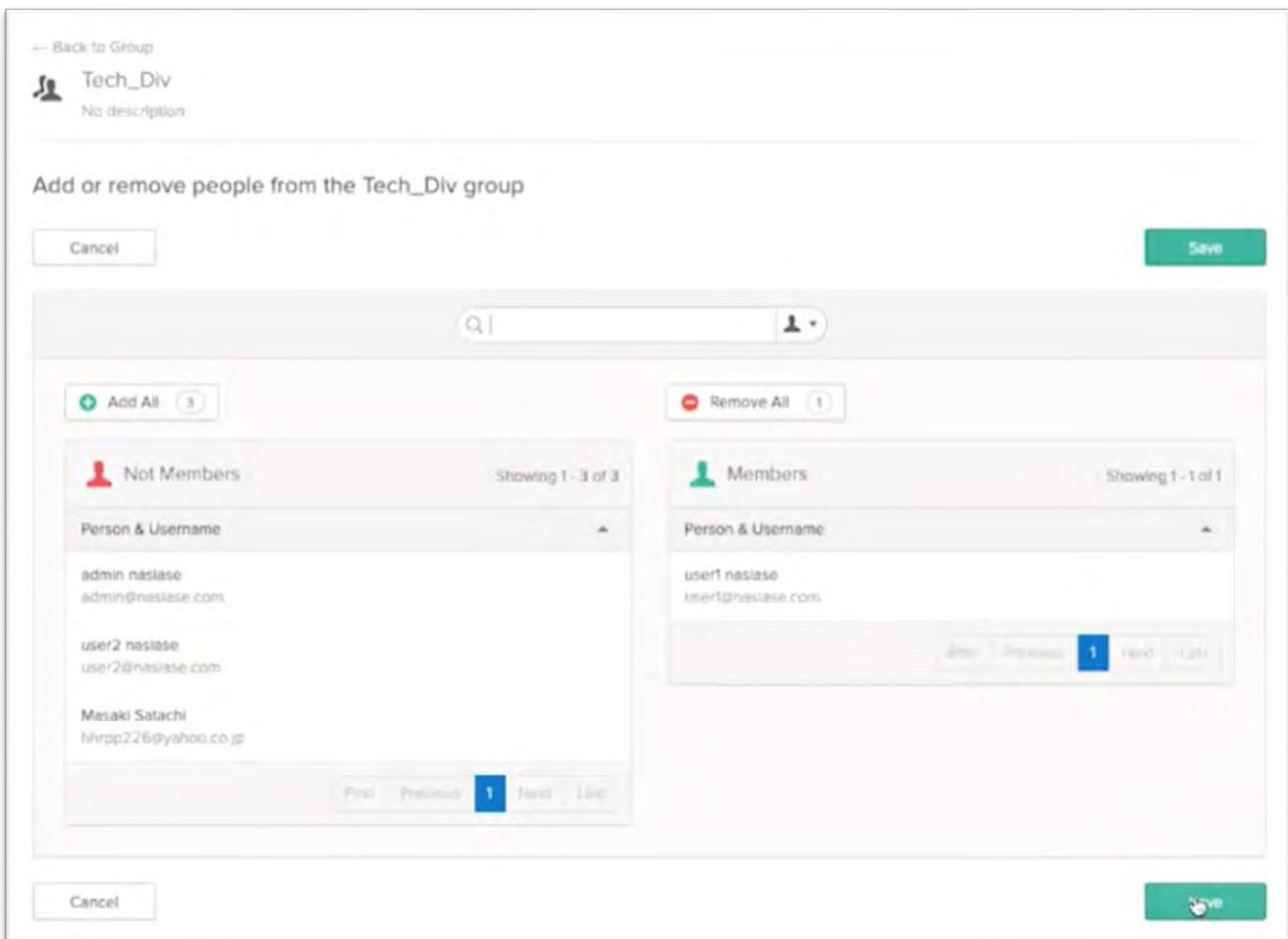


はじめての ZPA

[Manage People]をクリックします。

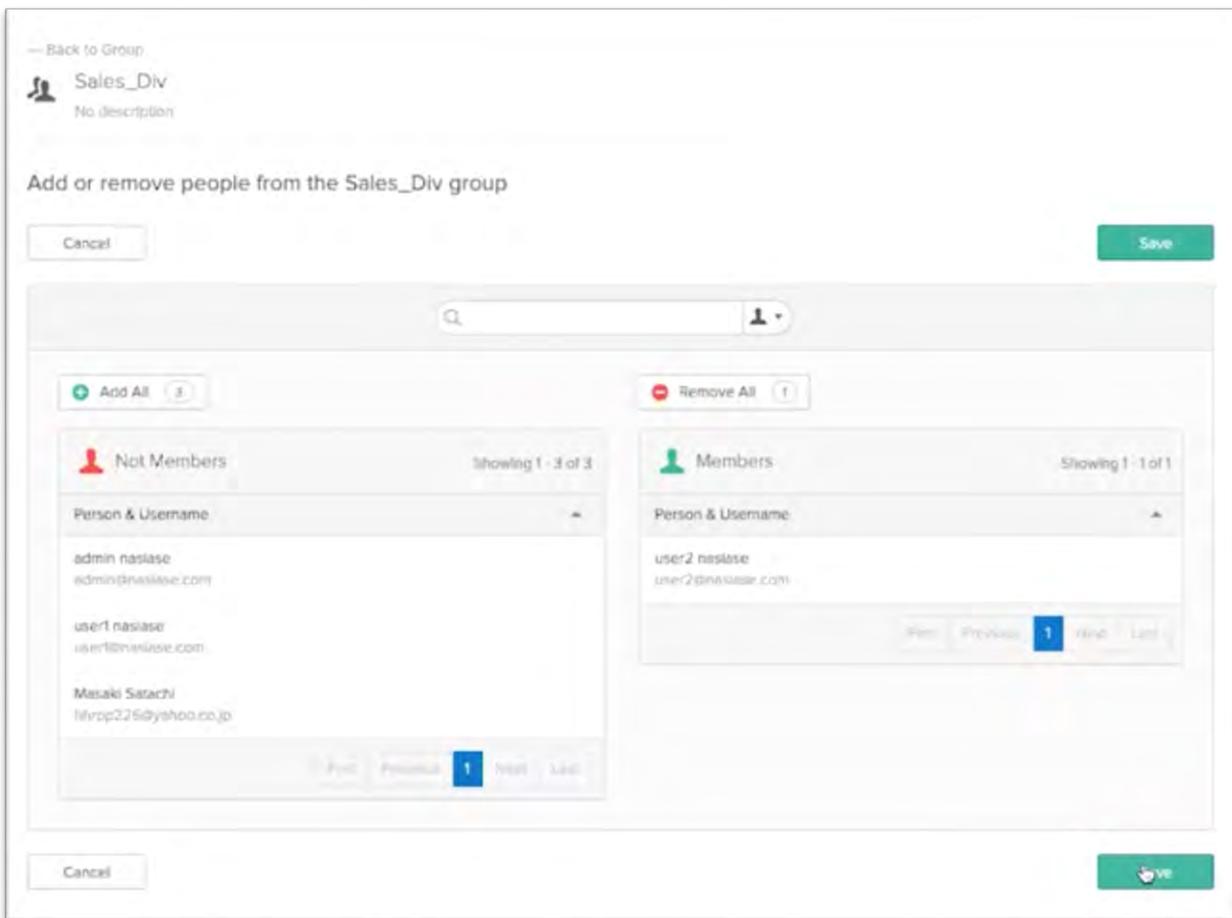
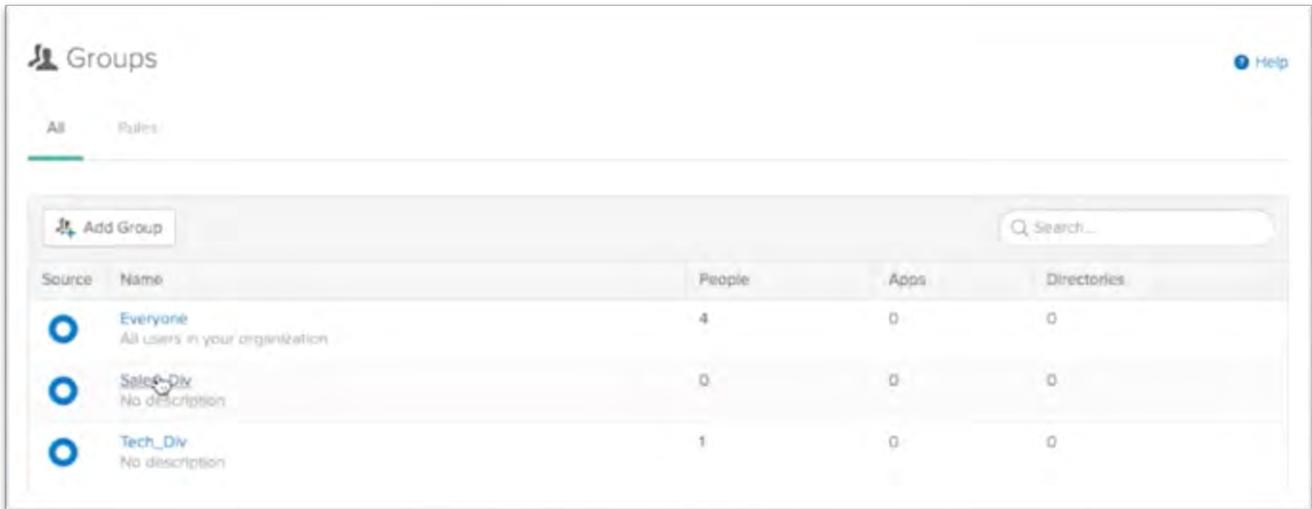


user1 を選択して[save]をクリックします。



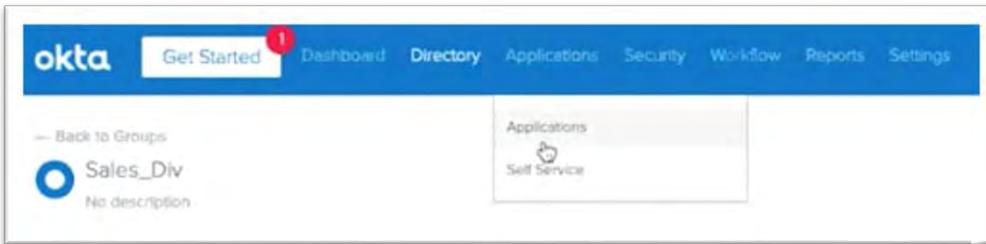
はじめての ZPA

同様の手順で、user2 を Sales_Div に紐付けます。

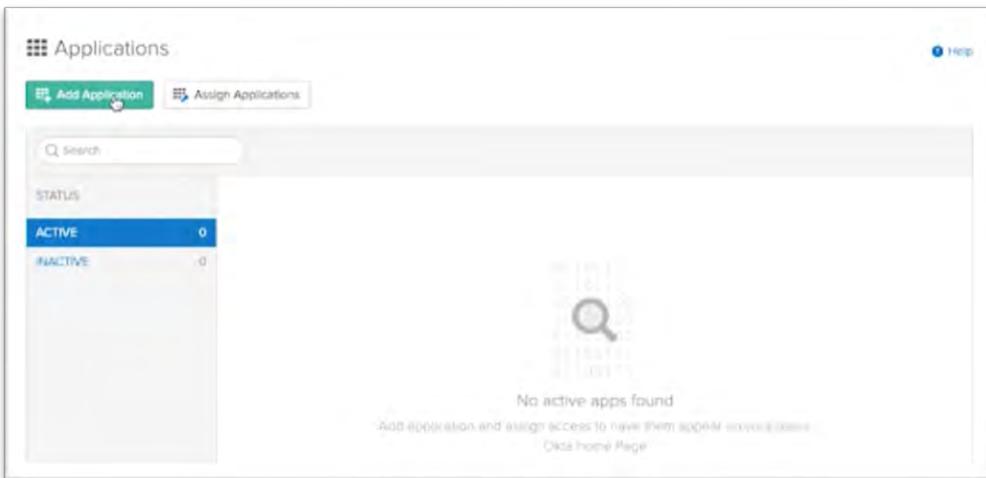


Step5. oktaにアプリケーション (ZPA) の登録

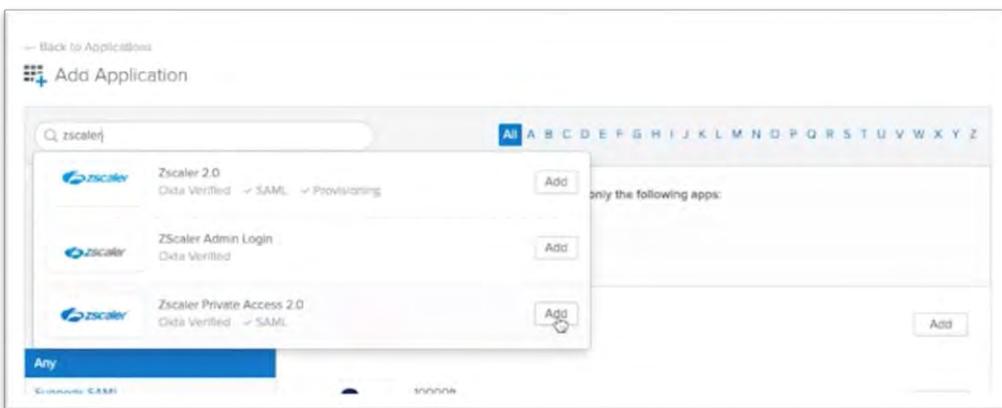
Applications より、[Applications]をクリックします。



[Add Application]をクリックします。



Zscaler Private Access を登録します。



はじめての ZPA

The screenshot shows the 'Add Zscaler Private Access 2.0' configuration page. The 'General Settings' tab is active, showing a 'Required' section. The 'Application label' is set to 'Zscaler Private Access 2.0'. Under 'Application Visibility', there are two unchecked checkboxes: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile App'. A 'General settings' note states: 'All fields are required to add this application unless marked optional.' Buttons for 'Cancel' and 'Done' are at the bottom.

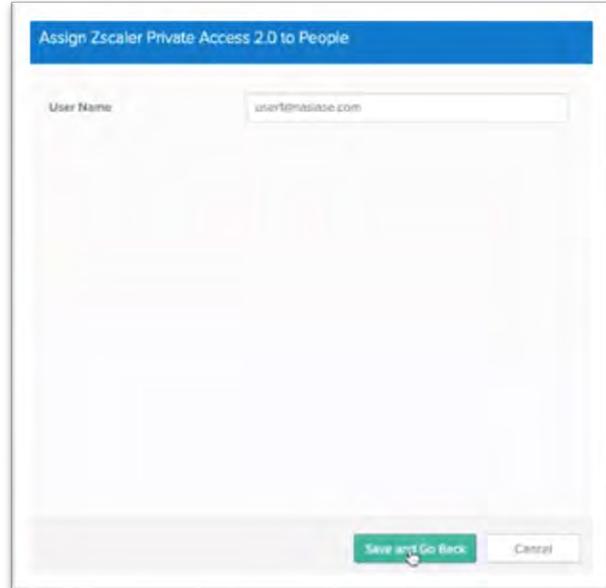
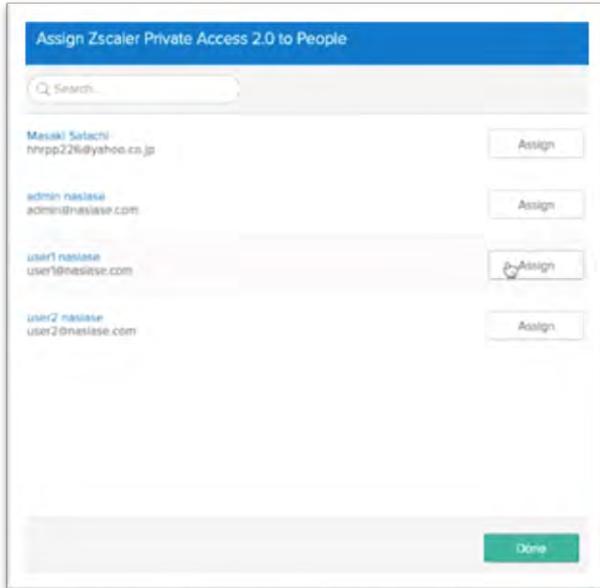
Step6. ZPAへのuserアサイン

Assign より、[Assign to People]をクリックします。

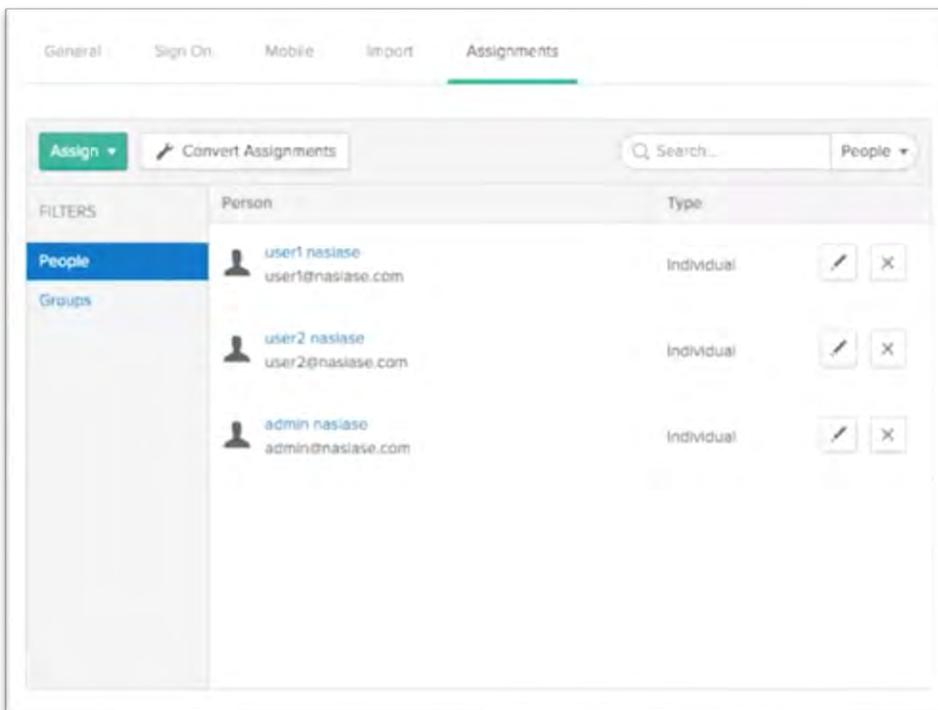
The screenshot shows the 'Zscaler Private Access 2.0' configuration page, 'Assignments' tab. The 'Assign' dropdown menu is open, showing 'Assign to People' and 'Assign to Groups'. The 'Assign to People' option is highlighted. The main area shows a search bar and a 'People' dropdown. Below, a search icon and the text 'No users found' are visible.

はじめての ZPA

[Assign]をクリックして、user1 をアサインします。

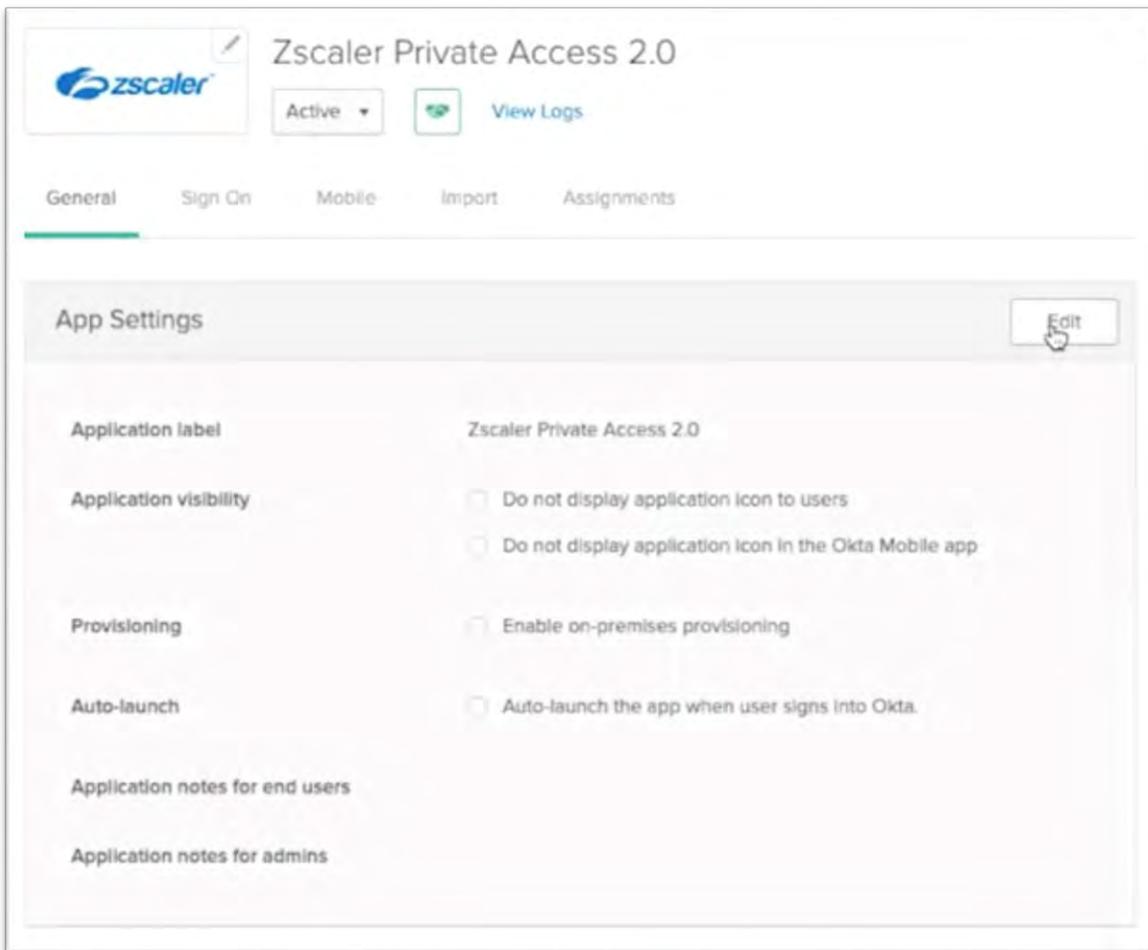
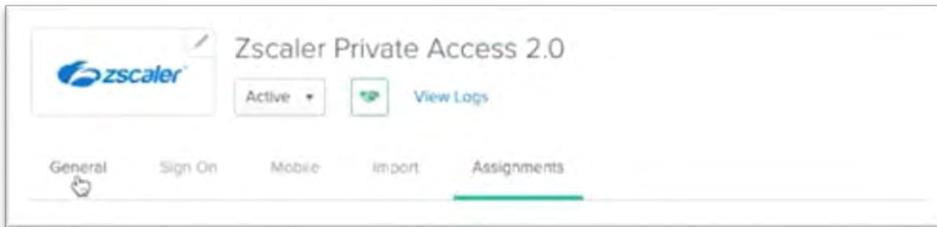


同様の手順で必要な user をアサインします。



Step7. Applicationラベルの変更

Generalより、[Edit]をクリックします。



はじめての ZPA

Application label 欄を任意に変更し、[Save]をクリックします。

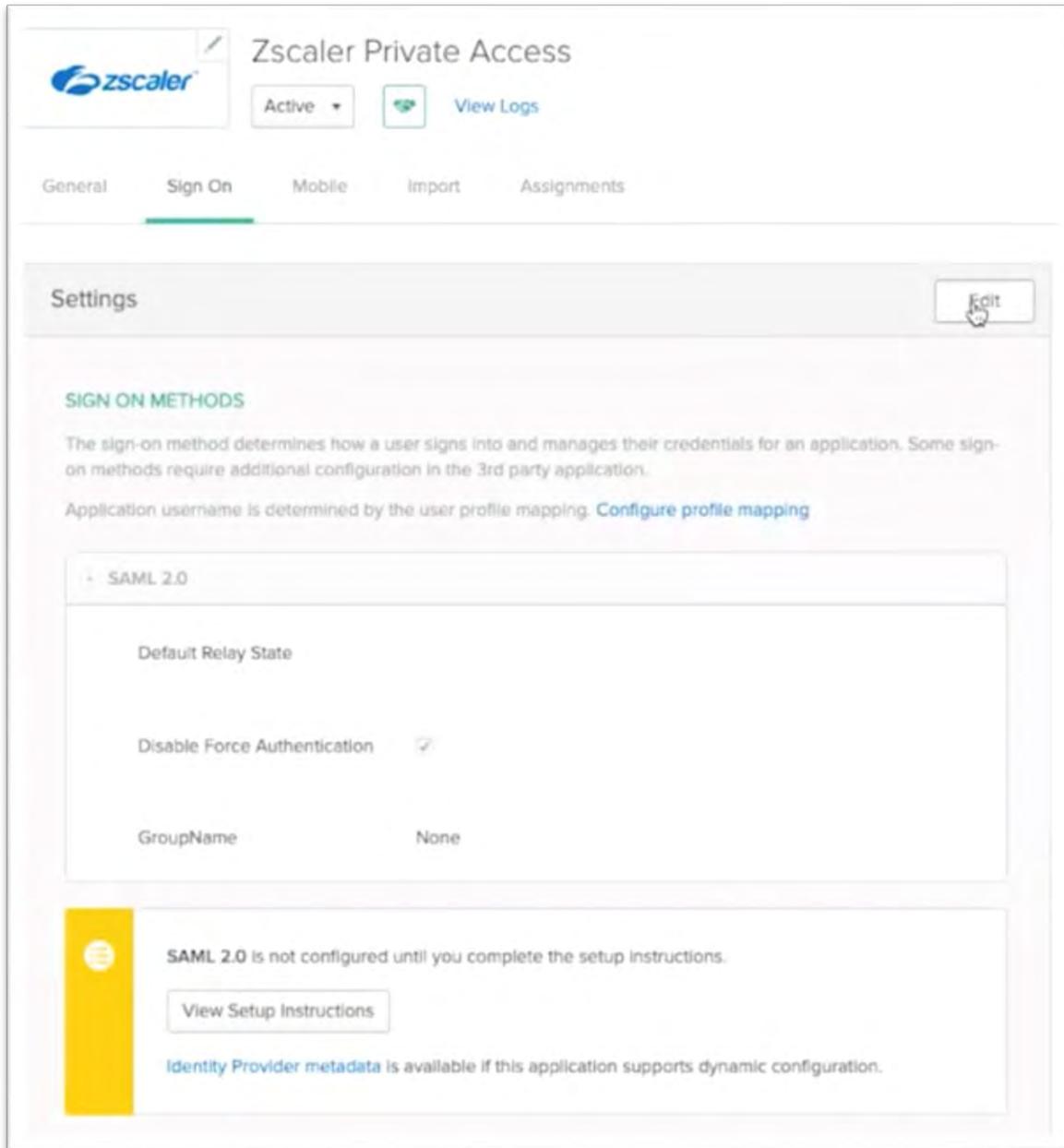
The screenshot displays the Zscaler Private Access 2.0 configuration page. At the top, the Zscaler logo is on the left, and the title 'Zscaler Private Access 2.0' is on the right. Below the title, there is a status indicator 'Active' with a dropdown arrow and a 'View Logs' button. A navigation bar contains tabs for 'General', 'Sign On', 'Mobile', 'Import', and 'Assignments', with 'General' being the active tab. The main content area is titled 'App Settings' and includes a 'Cancel' button in the top right corner. The settings are organized into several sections:

- Application label:** A text input field containing 'Zscaler Private Access'. Below it, a note states: 'This label displays under the app on your home page'.
- Application visibility:** Two checkboxes: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile App', both of which are currently unchecked.
- Provisioning:** A checkbox 'Enable on-premises provisioning', which is unchecked.
- Auto-launch:** A checkbox 'Auto-launch the app when user signs into Okta', which is unchecked.
- Application notes for end users:** A text area for notes, with a note below it stating: 'This note will be accessible to all end users via their dashboard'.
- Application notes for admins:** A text area for notes, with a note below it stating: 'This note will only be accessible to admin on this page'.

At the bottom right of the 'App Settings' dialog, there is a green 'Save' button with a mouse cursor hovering over it.

Step8. ZPAとokta間のSAML認証連携設定

Sign On -> Settingsより、[Edit]をクリックします。



はじめての ZPA

「Disable Force Authentication」にチェックが入っていることを確認し、Group Name を「Matches regex」に変更し「.*」を入力します。

Identity Provider metadata のリンク先のファイル（メタデータ）を PC 保存します。

The screenshot shows the 'Sign On' configuration page in the Zscaler ZPA console. The 'Sign On' tab is selected, and the 'Settings' section is expanded. Under 'SIGN ON METHODS', the 'SAML 2.0' method is selected. The 'Disable Force Authentication' checkbox is checked. The 'GroupName' is set to 'Matches regex' with the value '.*' entered in the adjacent text box. A yellow warning banner at the bottom indicates that SAML 2.0 is not fully configured until setup instructions are followed.

General Sign On Mobile Import Assignments

Settings Cancel

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State
All IDP-initiated requests will include this RelayState.

Disable Force Authentication
Never prompt user to re-authenticate.

GroupName Matches ...

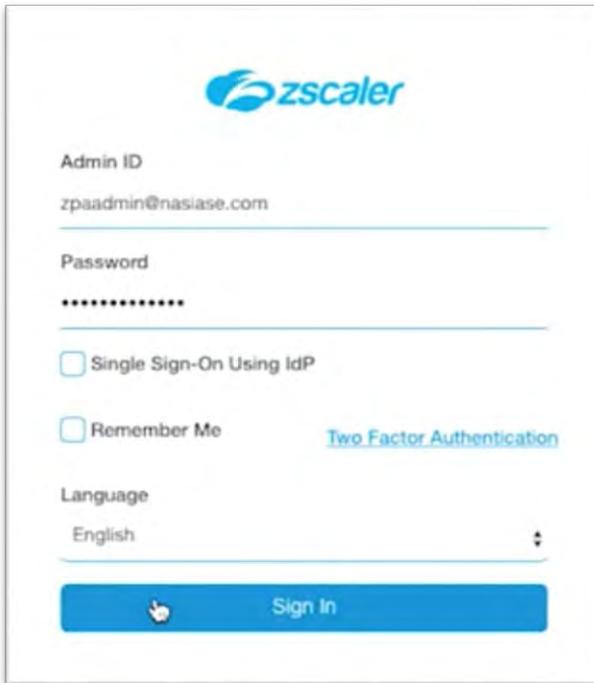
SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

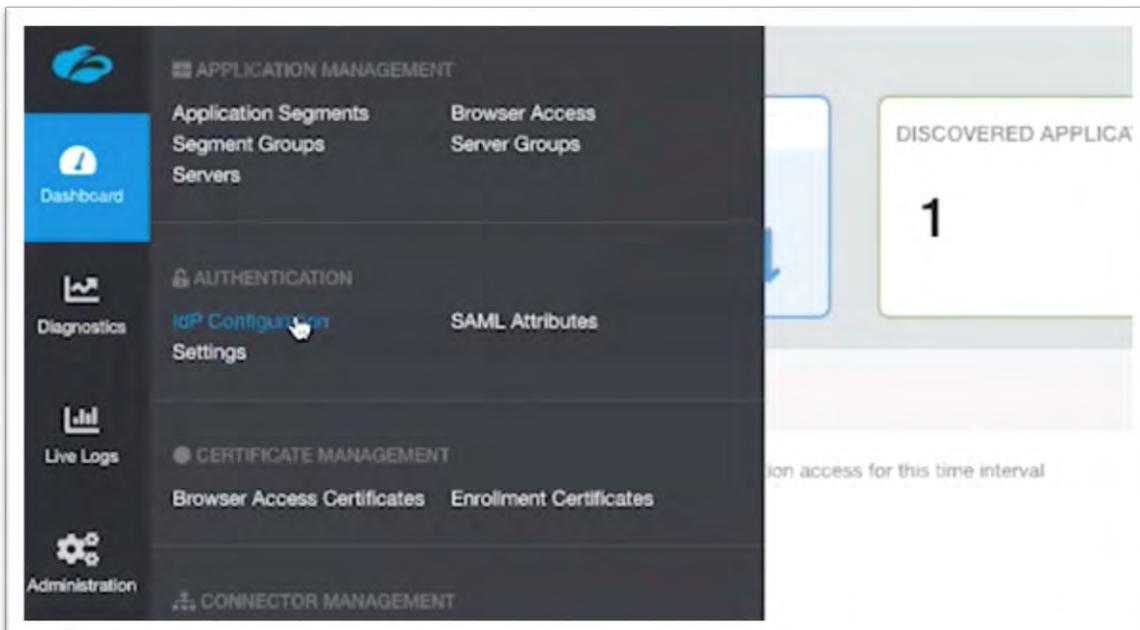
はじめての ZPA

ZPA ポータルにログインします。



The screenshot shows the Zscaler login page. At the top is the Zscaler logo. Below it, there are input fields for 'Admin ID' (containing 'zpaadmin@nasiase.com') and 'Password' (masked with dots). There are two checkboxes: 'Single Sign-On Using IdP' and 'Remember Me'. A link for 'Two Factor Authentication' is visible. A 'Language' dropdown menu is set to 'English'. At the bottom is a blue 'Sign In' button with a mouse cursor hovering over it.

Administration -> AUTHENTICATION -> IdP Configuration より、IdP のプロフィールを作成します。



はじめての ZPA

[Add IdP Configuration]をクリックします。



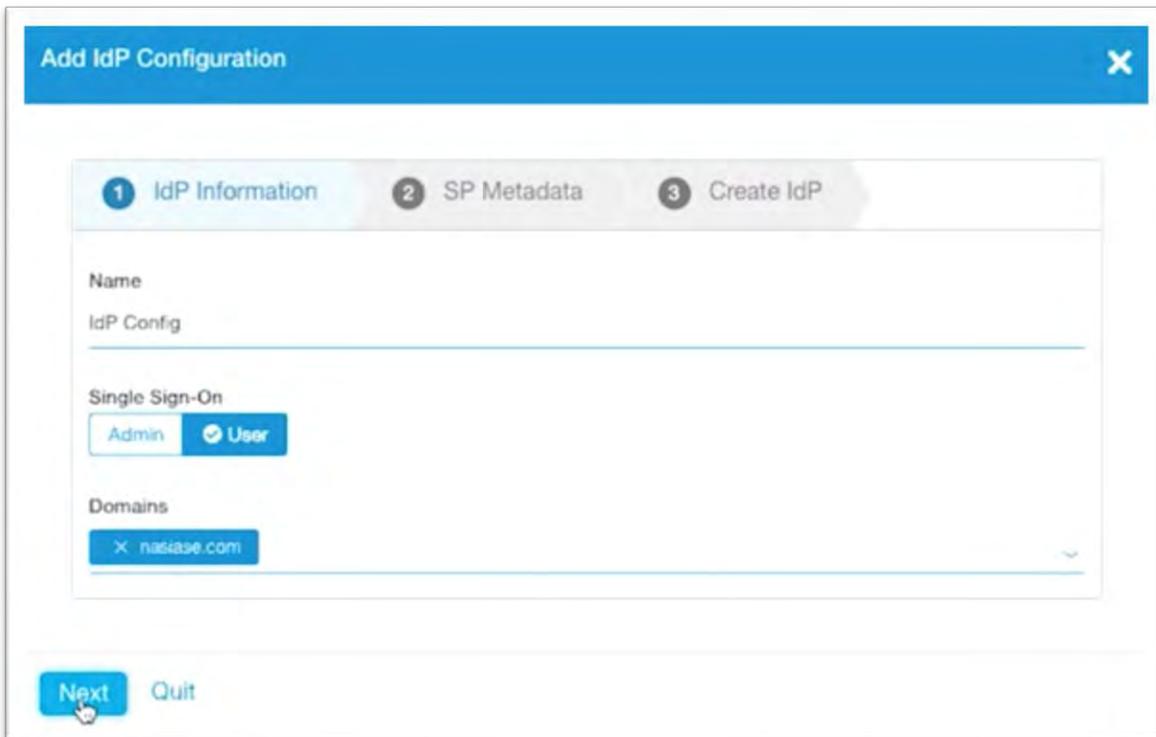
必要事項を記入、設定し [Next] をクリックします。

+++++

Name: 任意の名前

Domains: 申請いただいたドメイン名

+++++



はじめての ZPA

「Service Provider URL」、「Service Provider Entity ID」を okta のポータルにコピーペーストします。

Add IdP Configuration [X]

1 IdP Information 2 SP Metadata 3 Create IdP

Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata
[Download Metadata](#)

Service Provider Certificate
[Download Certificate](#)

Service Provider URL
https://samisp.private.zscaler.com/auth/72076300767985753/sso

Service Provider Entity ID
https://samisp.private.zscaler.com/auth/metadata/72076300767985753

Copied!

Next Pause

[Save]をクリックします。

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL
https://samisp.private.zscaler.com/auth/72076300767985753/sso
Please enter your Service Provider URL. Refer to the Setup Instructions above to obtain this value.

Service Provider Entity ID
s://samisp.private.zscaler.com/auth/metadata/72076300767985753
Please enter your Service Provider Entity ID. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

Application username format
Okta username

Update application username on
Create and update

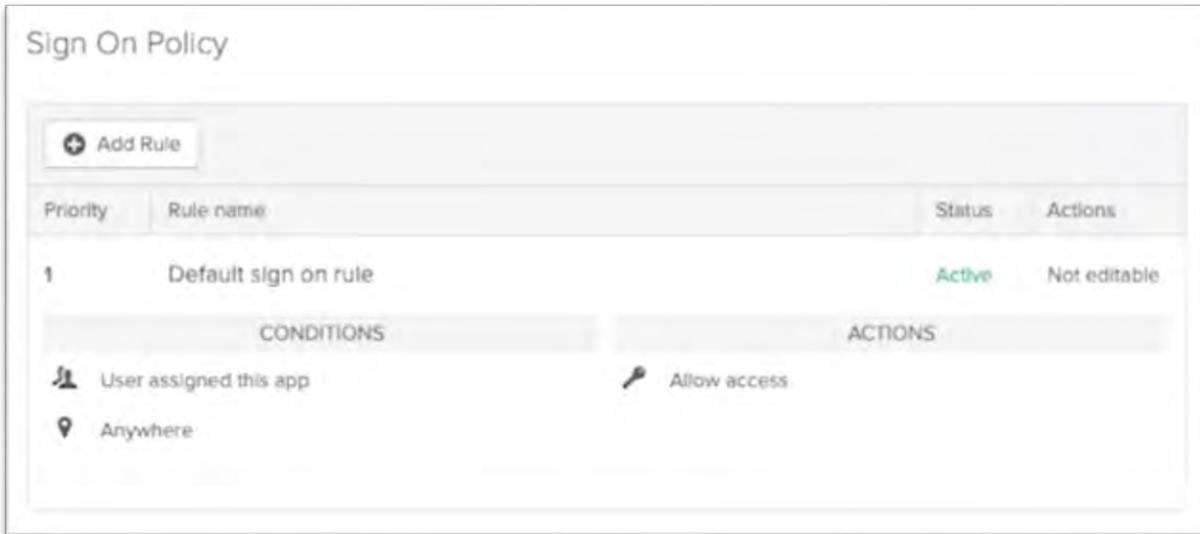
Password reveal
 Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

Save

はじめての ZPA

Sign On Policy の内容を確認します、こちらで okta 側の設定は完了です。



Sign On Policy

+ Add Rule

Priority	Rule name	Status	Actions
1	Default sign on rule	Active	Not editable

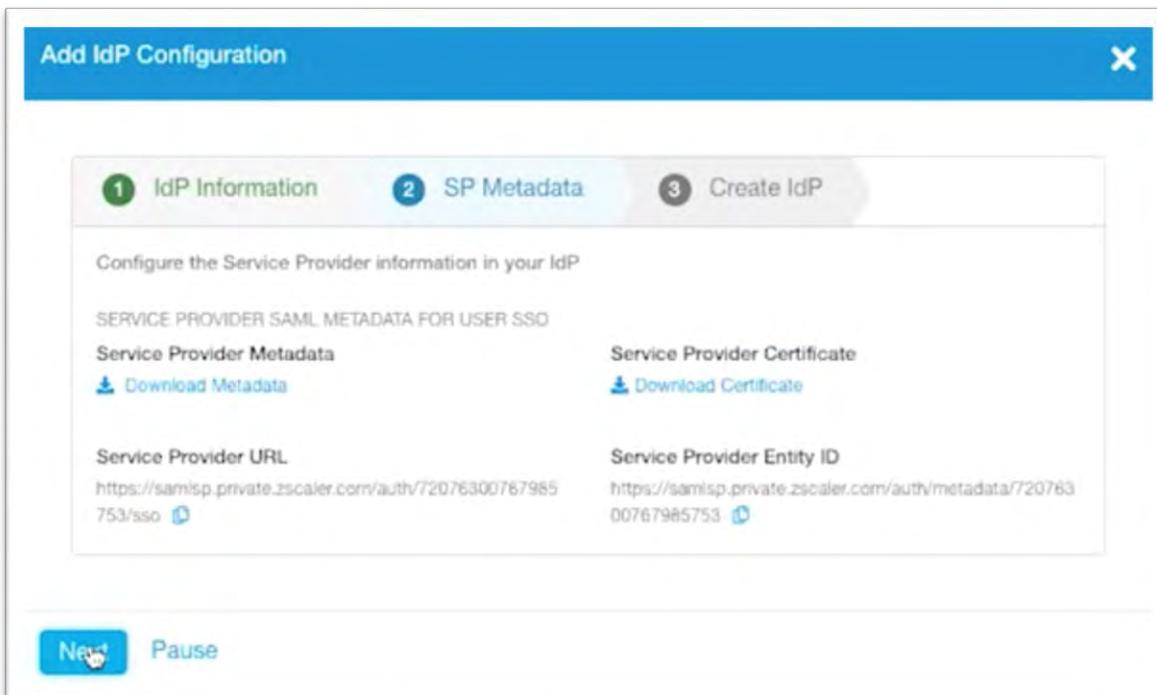
CONDITIONS

- User assigned this app
- Anywhere

ACTIONS

- Allow access

[Next]をクリックし、ZPA 側の設定を続けます。



Add IdP Configuration

1 IdP Information 2 SP Metadata 3 Create IdP

Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata [Download Metadata](#)

Service Provider Certificate [Download Certificate](#)

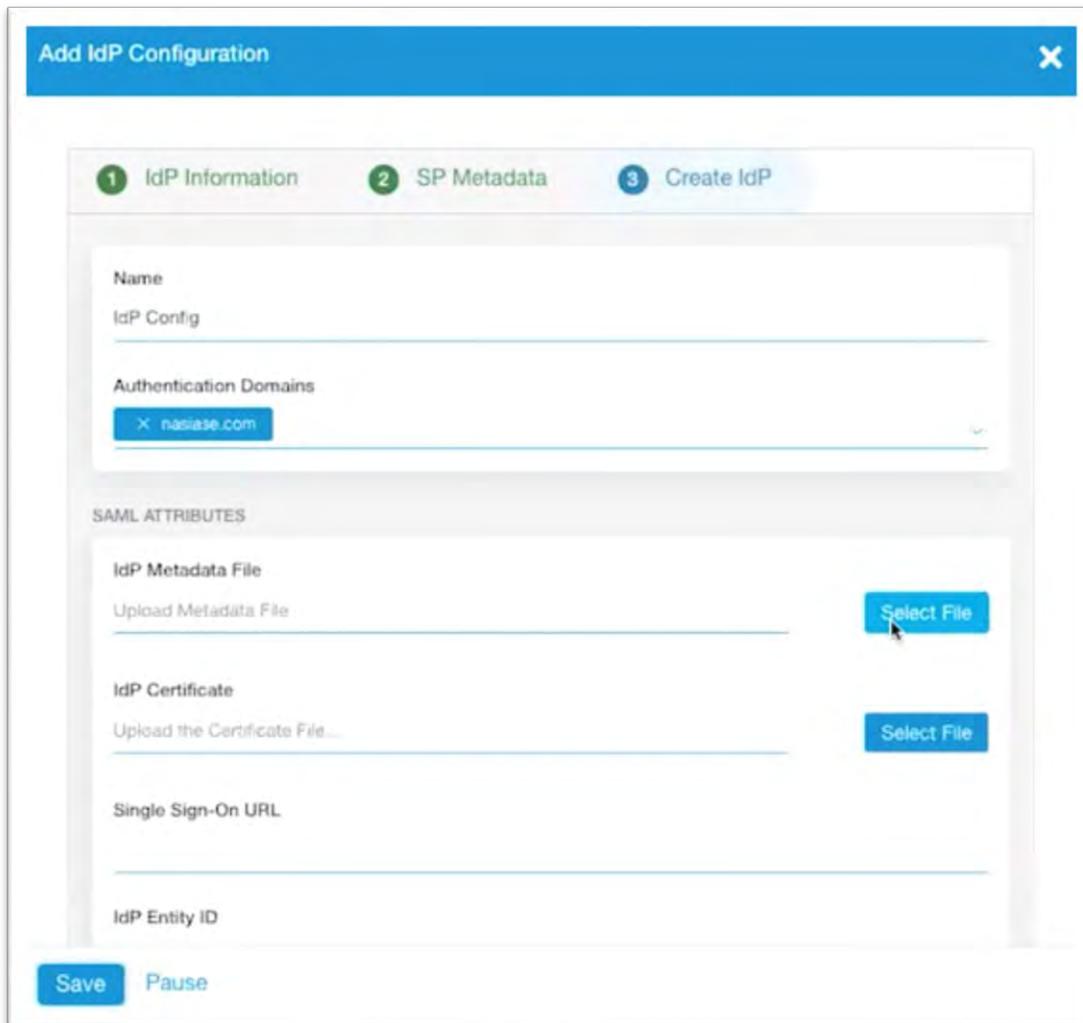
Service Provider URL <https://samisp.private.zscaler.com/auth/72076300767985753/sso>

Service Provider Entity ID <https://samisp.private.zscaler.com/auth/metadata/72076300767985753>

Next Pause

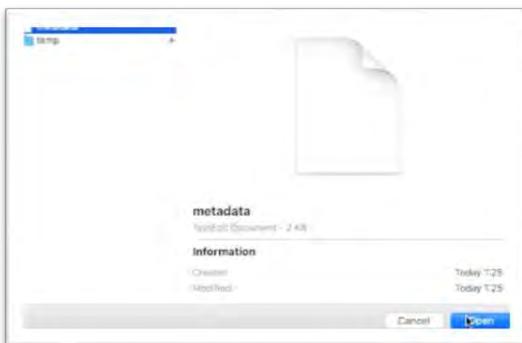
はじめての ZPA

IdP Metadata File より、[Select File]をクリックします。



The screenshot shows a web-based configuration window titled "Add IdP Configuration". It features a progress indicator with three steps: "1 IdP Information", "2 SP Metadata", and "3 Create IdP". The "IdP Information" section includes a "Name" field containing "IdP Config" and an "Authentication Domains" list with "nasiae.com". Under the "SAML ATTRIBUTES" section, there are two "Select File" buttons: one for "IdP Metadata File" and one for "IdP Certificate". Other fields include "Single Sign-On URL" and "IdP Entity ID". At the bottom, there are "Save" and "Pause" buttons.

ダウンロードした Metadata File を選択すると、情報が自動でインポートされます。



はじめての ZPA

[Save]をクリックします。

Add IdP Configuration

SAML ATTRIBUTES

IdP Metadata File
metadata Change Remove

IdP Certificate
Upload the Certificate File... Select File

-----BEGIN CERTIFICATE-----
MIIDsDCCApigAwIBAgJGAXCcEL52MA0GCsqGSib3DQEBECwUAMIgYMQswCQYDVQQGEwJVUzETMB
EG
A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuiEZYyYW5jaXNjbzENMAAsGA1UECgwET2t0YTE
U

Single Sign-On URL
https://yahoo-co-zscaler.okta.com/app/zscaler_private_access/exk41hoy4JmgOZjGM4x6/sso/saml

IdP Entity ID No file chosen
http://www.okta.com/exk41hoy4JmgOZjGM4x6

Status Enabled Disabled

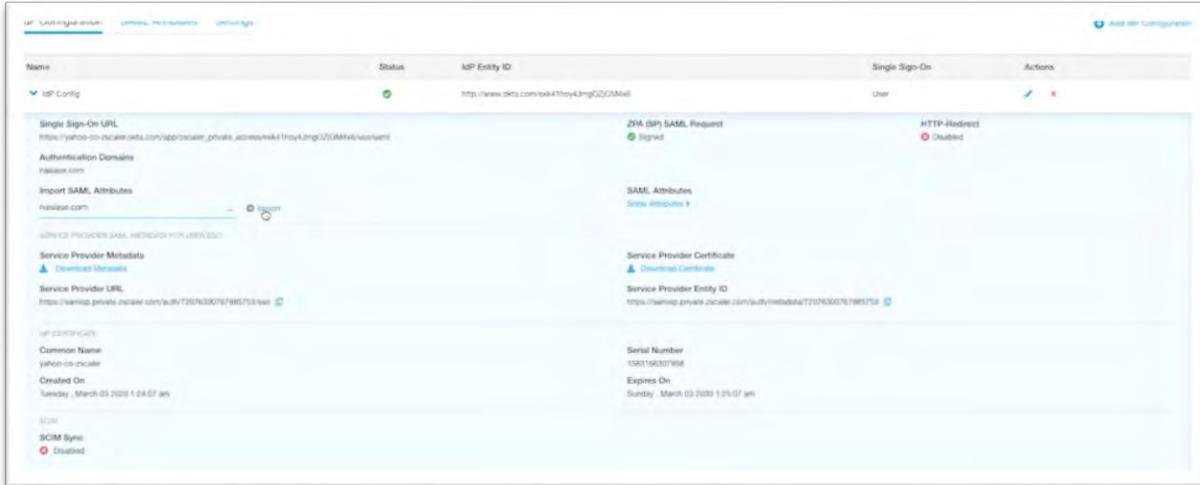
ZPA (SP) SAML Request Signed Unsigned

HTTP-Redirect Enabled Disabled

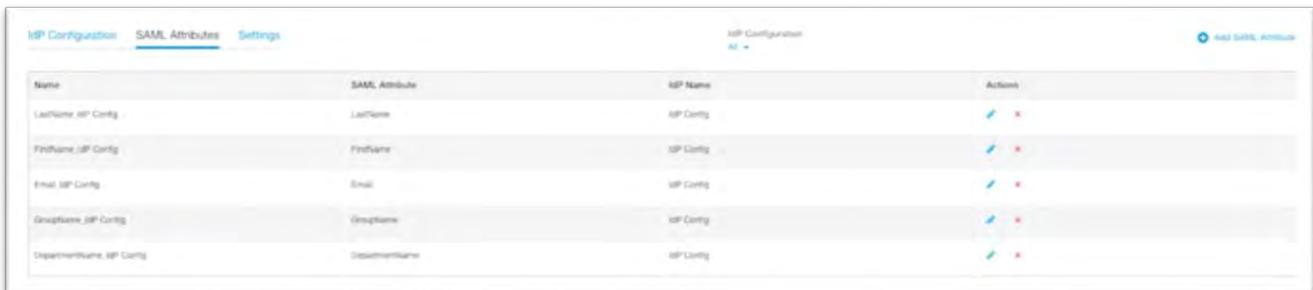
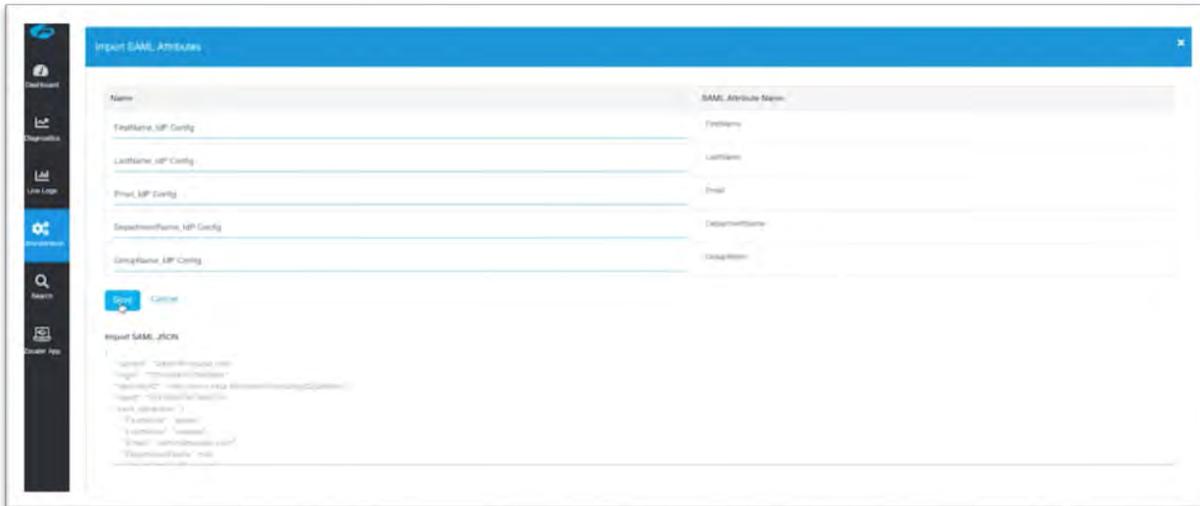
Save Pause

はじめての ZPA

Import SAML Attributes より、[import]をクリックします。

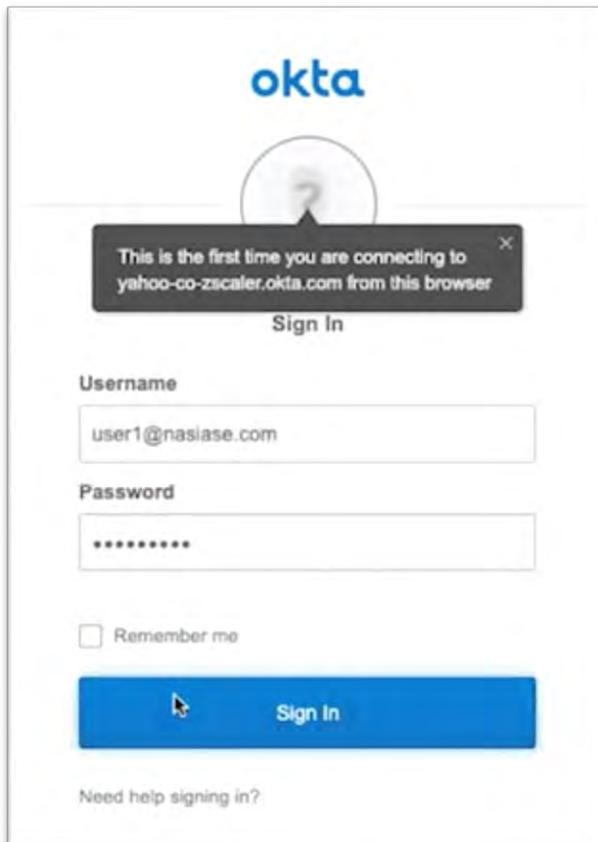


[Save]をクリックします。

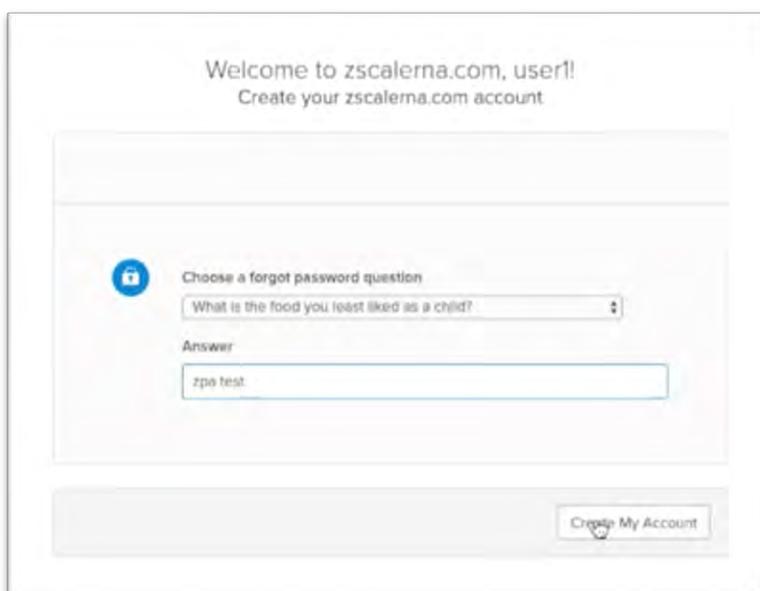


はじめての ZPA

作成した user は、ログインすることでアクティベーションされるので、user1 と user2 でログインします。

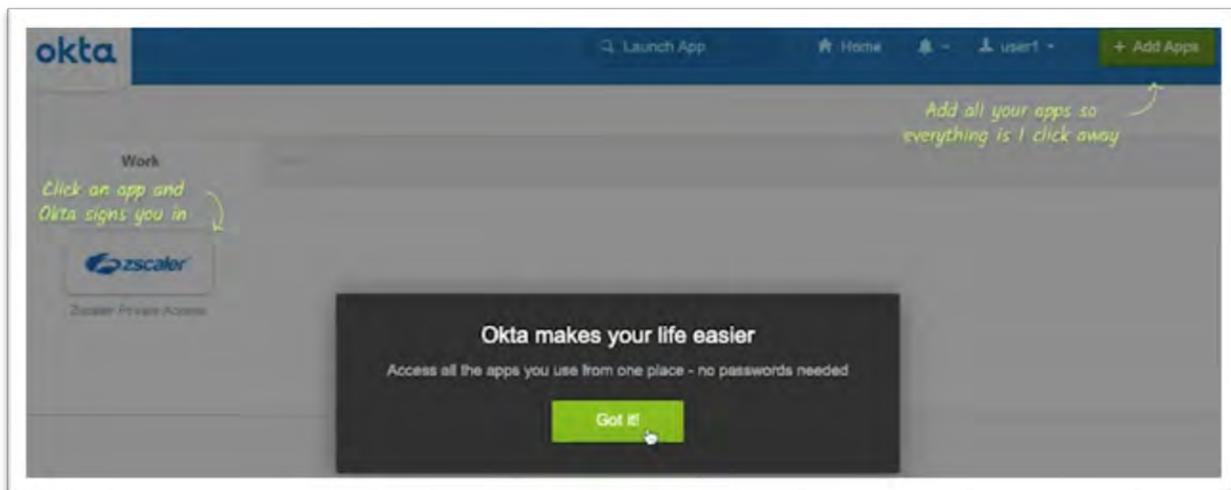


The image shows the Okta Sign In interface. At the top is the Okta logo. Below it is a placeholder for a user profile picture. A dark notification box with a close button (X) contains the text: "This is the first time you are connecting to yahoo-co-zscaler.okta.com from this browser". Below the notification is a "Sign In" button. The form includes a "Username" field with the text "user1@nasiase.com", a "Password" field with masked characters "*****", and a "Remember me" checkbox which is unchecked. A large blue "Sign In" button is at the bottom of the form. Below the button is the text "Need help signing in?".

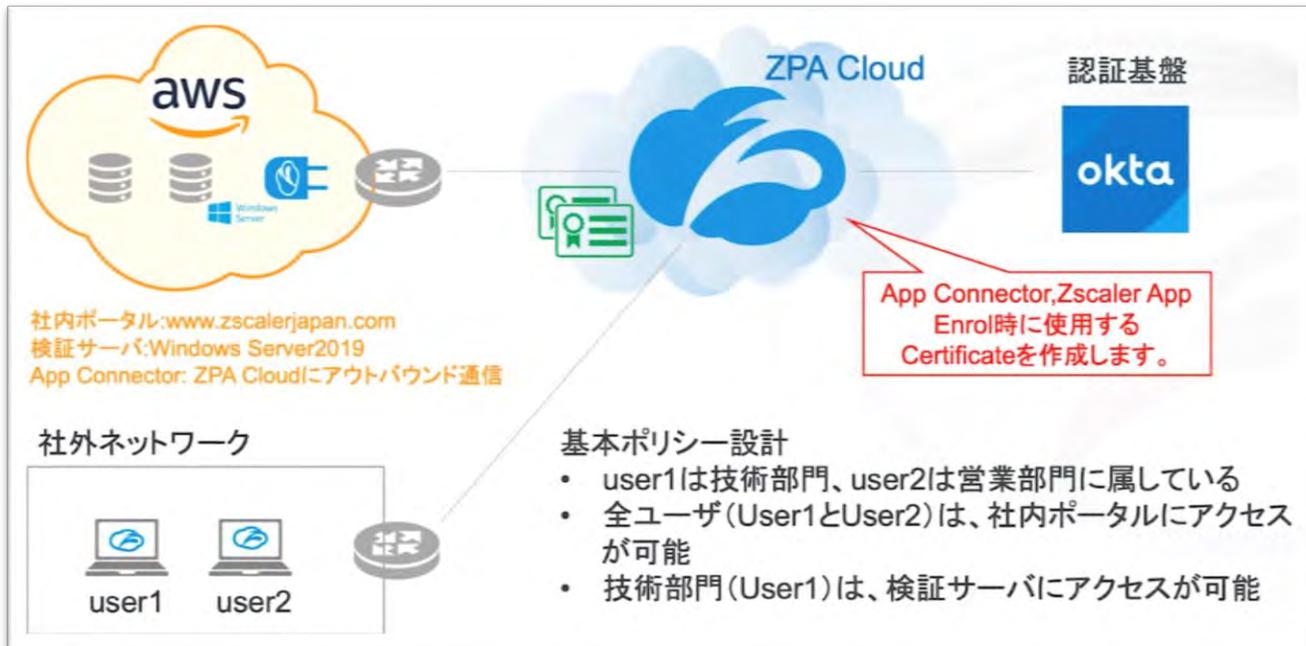


The image shows the Zscaler account creation screen. At the top, it says "Welcome to zscalerna.com, user!" and "Create your zscalerna.com account". Below this is a form with a lock icon and the text "Choose a forgot password question". The question field contains "What is the food you least liked as a child?". Below the question is an "Answer" field containing "zpa test". At the bottom right of the form is a "Create My Account" button.

はじめての ZPA



3-2. Connector, Zscaler App Enroll 用の証明書作成

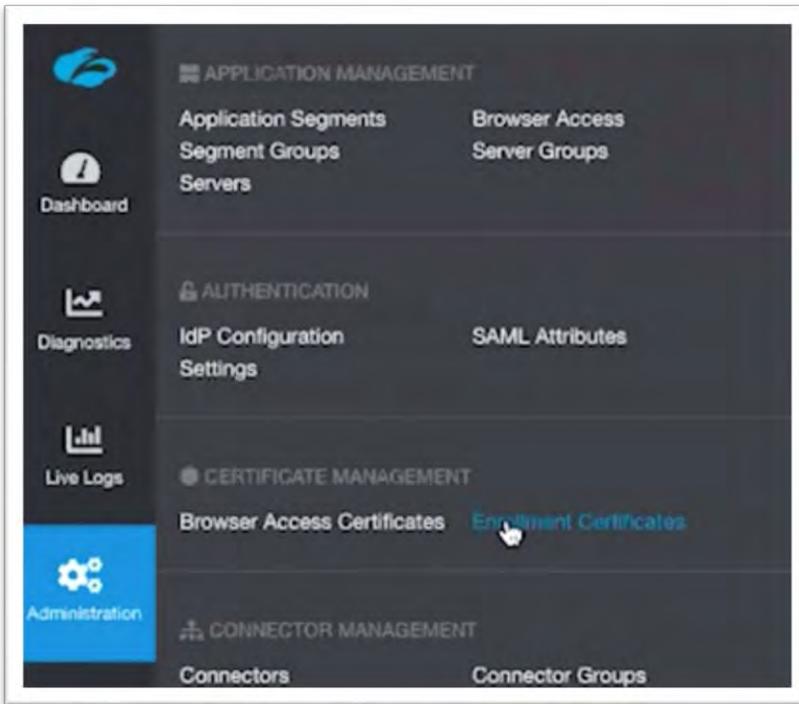


Notes

- ✓ Connector、Zscaler App (PC) は、それぞれ ZPA が持つ中間 CA 証明書でサインされたクライアント証明書を使ってクライアント認証を実施
- ✓ クライアント認証により、Zscaler App – ZPA Cloud 間、Zscaler App – ZPA Cloud 間で TLS トンネルを構築

Step1. Root CA 証明書の作成

Administration -> CERTIFICATE MANAGEMENT -> Enrollment Certificates より、Root CA 証明書を作成します。



[Generate Certificate] をクリックします。



はじめての ZPA

必要事項を記入、設定し [Generate] をクリックします。

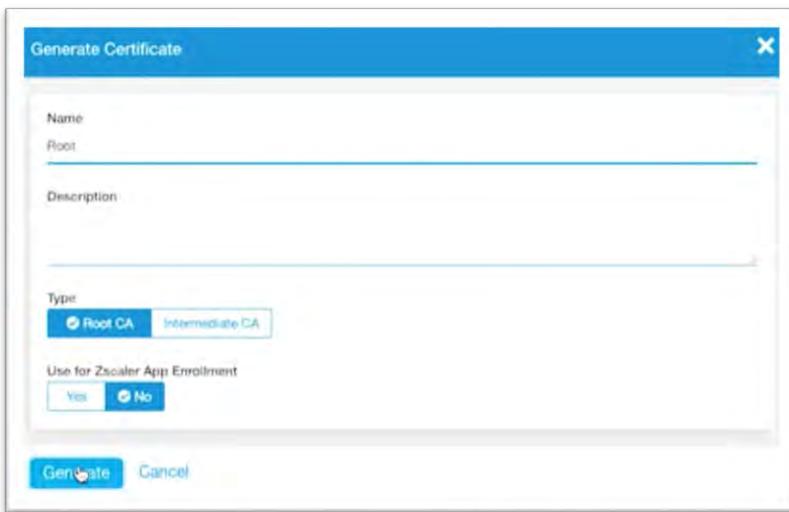
+++++

Name: 任意の名前

Type: Root CA

Use for Zscaler App Enrollment: No

+++++



Step2. Connector Enrollment 用の中間 CA 証明書の作成

[Generate Certificate] をクリックします。



Name	Creation Date	Expiry Date	Common Name	Actions
root	Tuesday, March 17, 2020 1:37:18 am	Thursday, March 10, 2026 1:37:18 am	pawasa.com/Root	

はじめての ZPA

必要事項を記入、設定し [Generate] をクリックします。

+++++

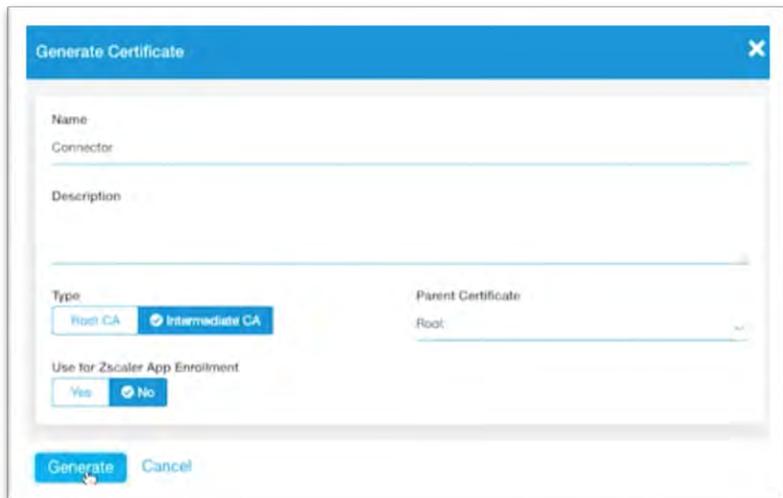
Name: 任意の名前

Type: Intermediate CA

Parent Certificate: Step1 で作成した Root CA 証明書

Use for Zscaler App Enrollment: No

+++++



Step3. Zscaler App Enrollment 用の中間 CA 証明書の作成

[Generate Certificate] をクリックします。



はじめての ZPA

必要事項を記入、設定し [Generate] をクリックします。

+++++

Name: 任意の名前

Type: Intermediate CA

Parent Certificate: Step1 で作成した Root CA 証明書

Use for Zscaler App Enrollment: Yes

+++++

Generate Certificate

Name

Client

Description

Type

Root CA Intermediate CA

Parent Certificate

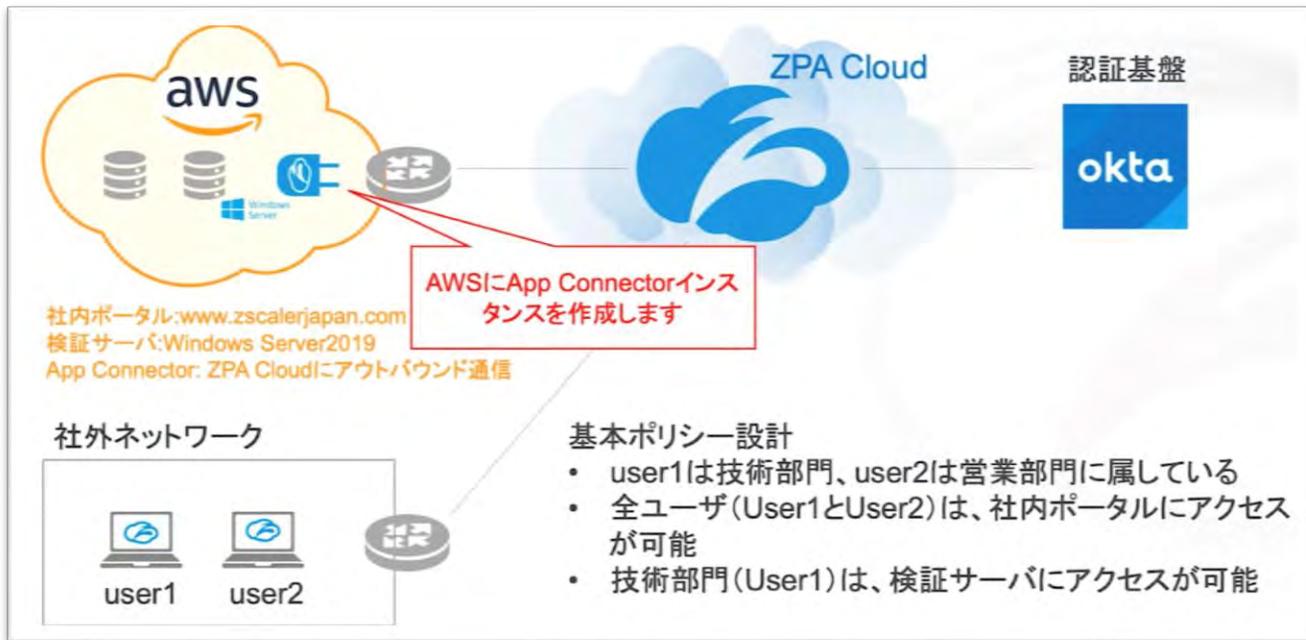
Root

Use for Zscaler App Enrollment

Yes No

Generate Cancel

3-3. Connector のインストール

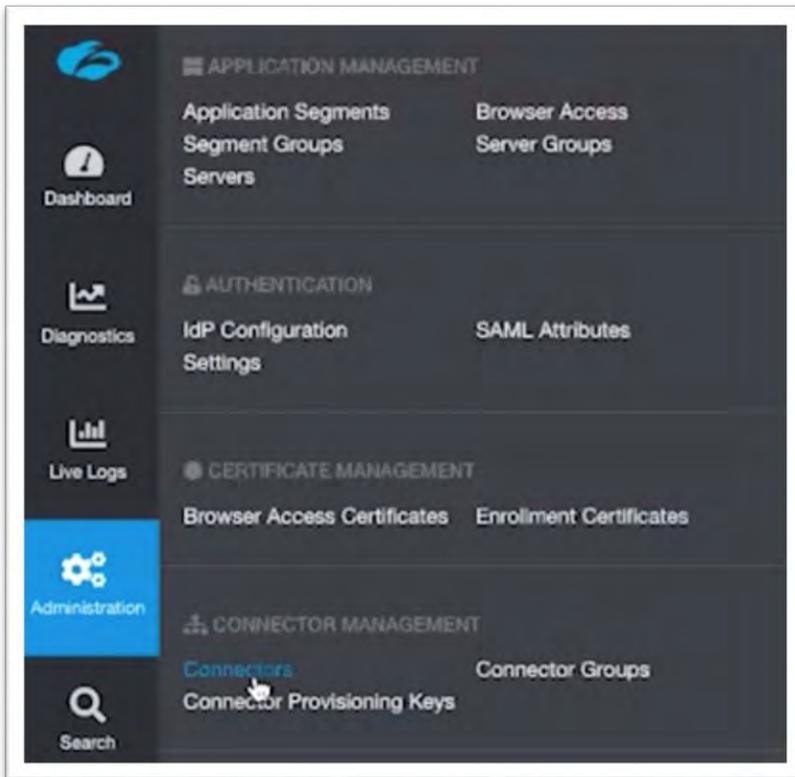


Note

- ✓ 本ドキュメントでは、AWS でのインストール方法を紹介
- ✓ その他の supported platform やインストール方法などの詳細については、
「<https://help.zscaler.com/zpa/about-connectors>」を参照
- ✓ 基本的に 1 つの DC には 1 つの Connector Group の設定

Step1. Connector のプロフィール作成

Administration -> CERTIFICATE MANAGEMENT -> Connectors より、プロフィールを作成します。

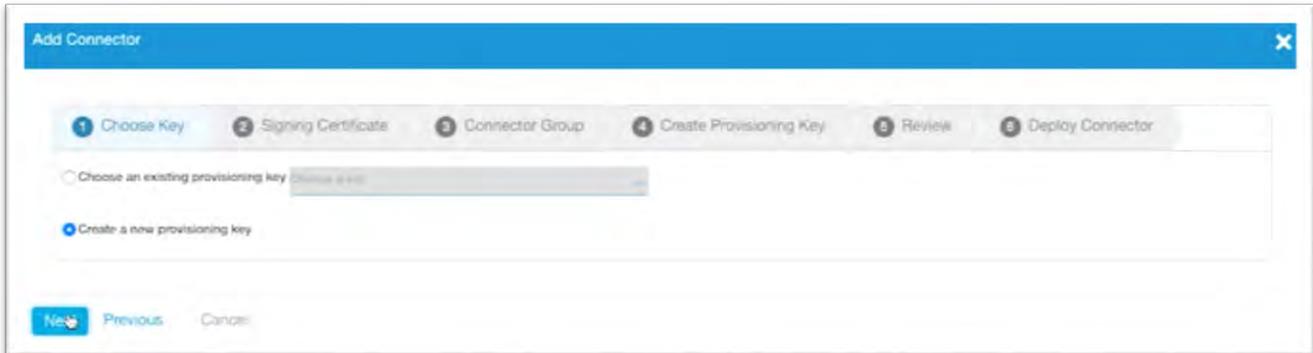


[Add Connector]をクリックします。

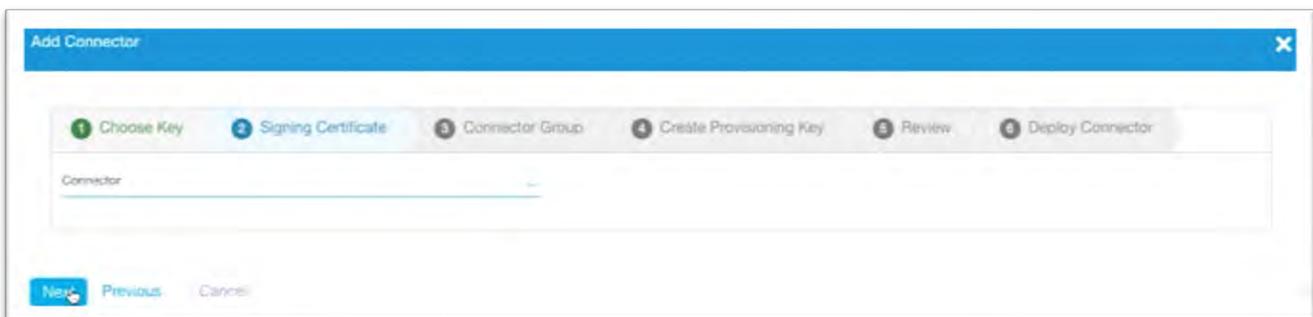
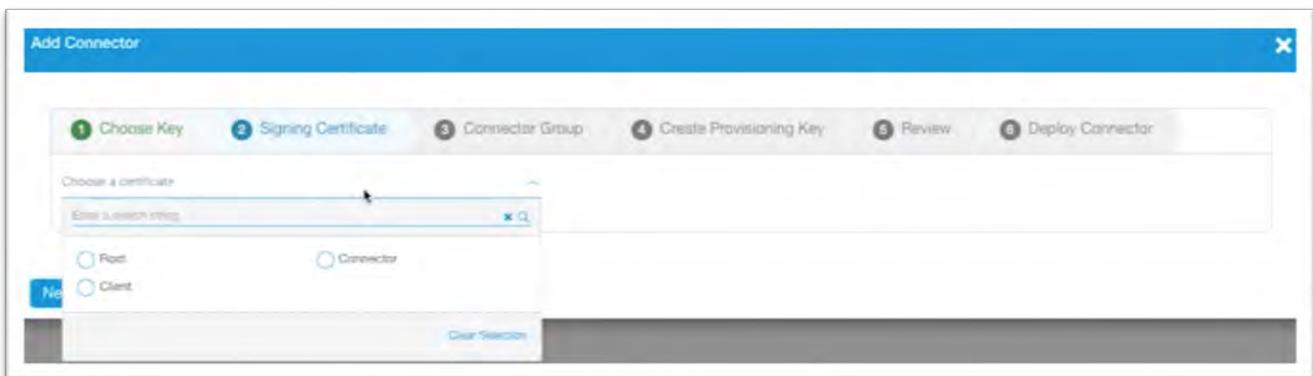


はじめての ZPA

Create a new provisioning key にチェックをつけ、[Next] をクリックします。



Choose a certificate を「3-2. Connector,Zscaler App Enroll用の証明書作成」の Step2 で作成した証明書を選択し、[Next] をクリックします。



はじめての ZPA

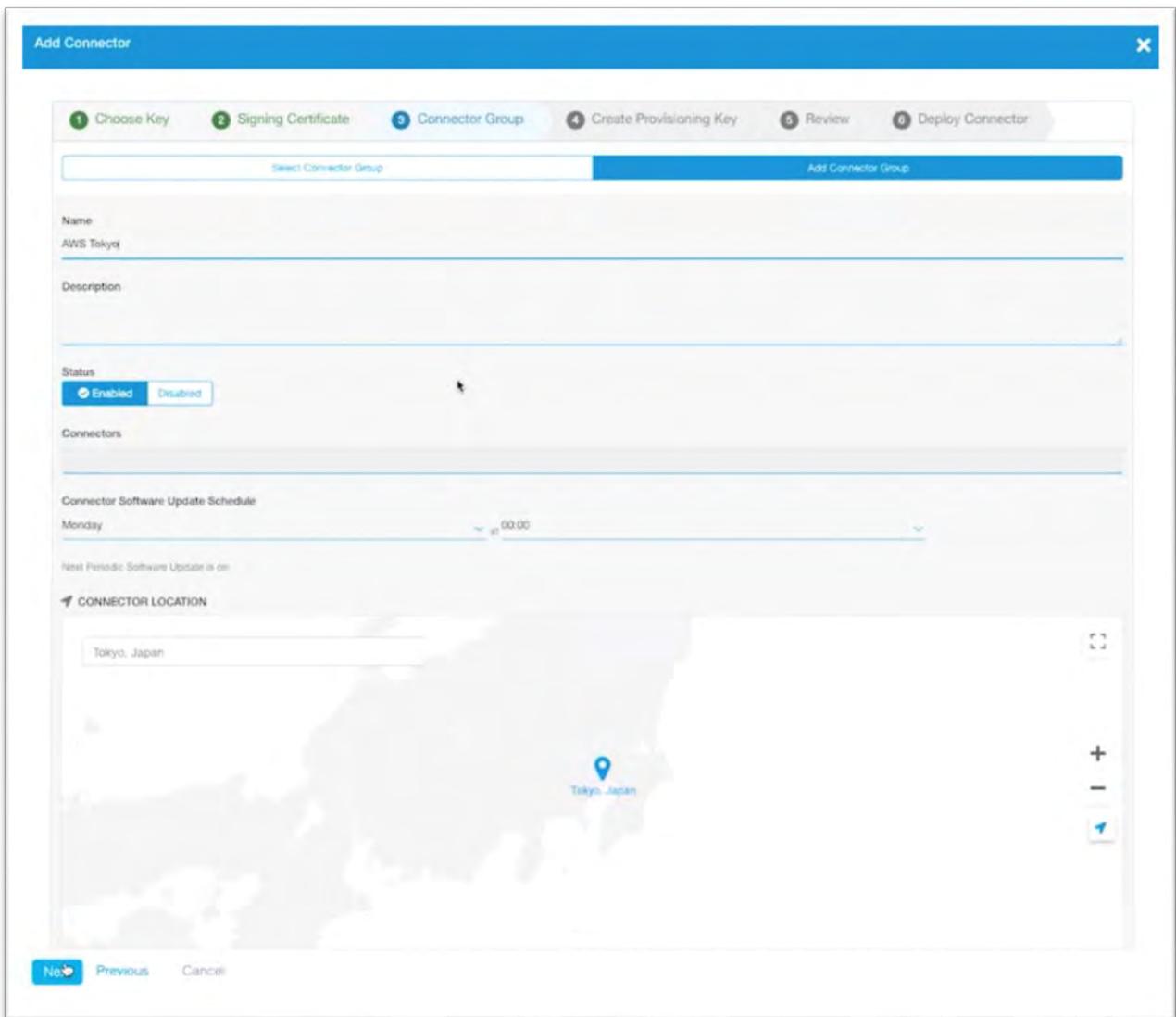
必要事項を記入し [Next] をクリックします。

+++++

Name: 任意の名前

CONNECTOR LOCATION: Connector の設置場所

+++++



はじめての ZPA

必要事項を記入し [Next] をクリックします。

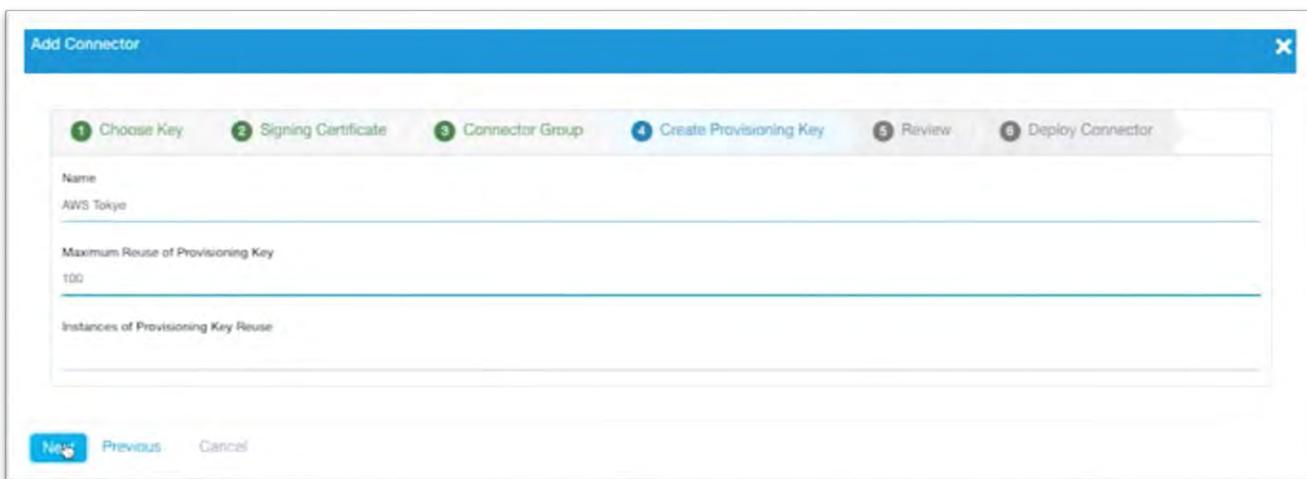
+++++

Name: 任意の名前

Maximum Reuse of Provisioning Key: 任意の値

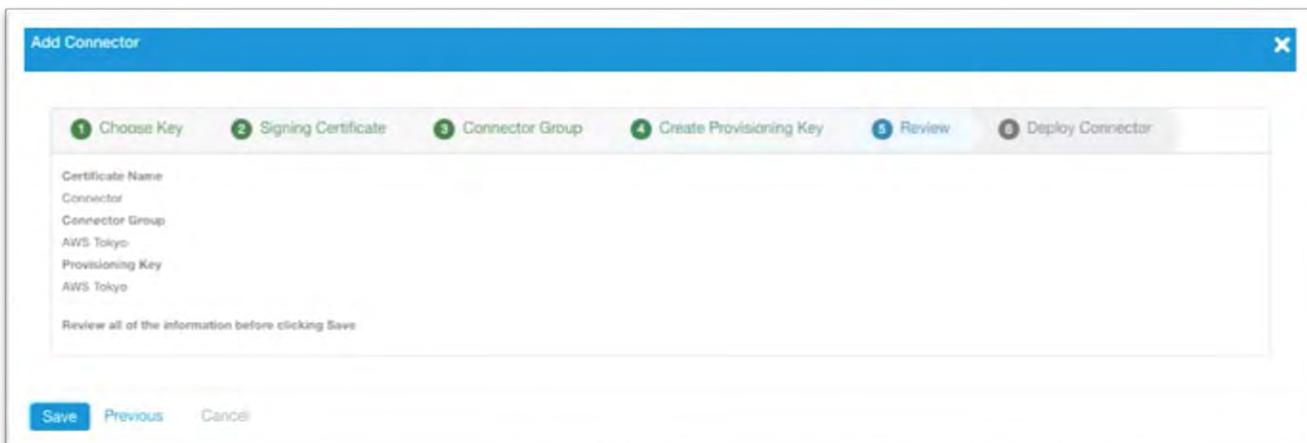
Instances of Provisioning Key Reuse: 任意の値

+++++



The screenshot shows the 'Add Connector' dialog box with a progress bar at the top indicating six steps: 1. Choose Key, 2. Signing Certificate, 3. Connector Group, 4. Create Provisioning Key (highlighted), 5. Review, and 6. Deploy Connector. The main content area contains three input fields: 'Name' with the value 'AWS Tokyo', 'Maximum Reuse of Provisioning Key' with the value '100', and 'Instances of Provisioning Key Reuse' which is empty. At the bottom, there are three buttons: 'Next' (highlighted in blue), 'Previous', and 'Cancel'.

内容を確認して、[Save]をクリックします。

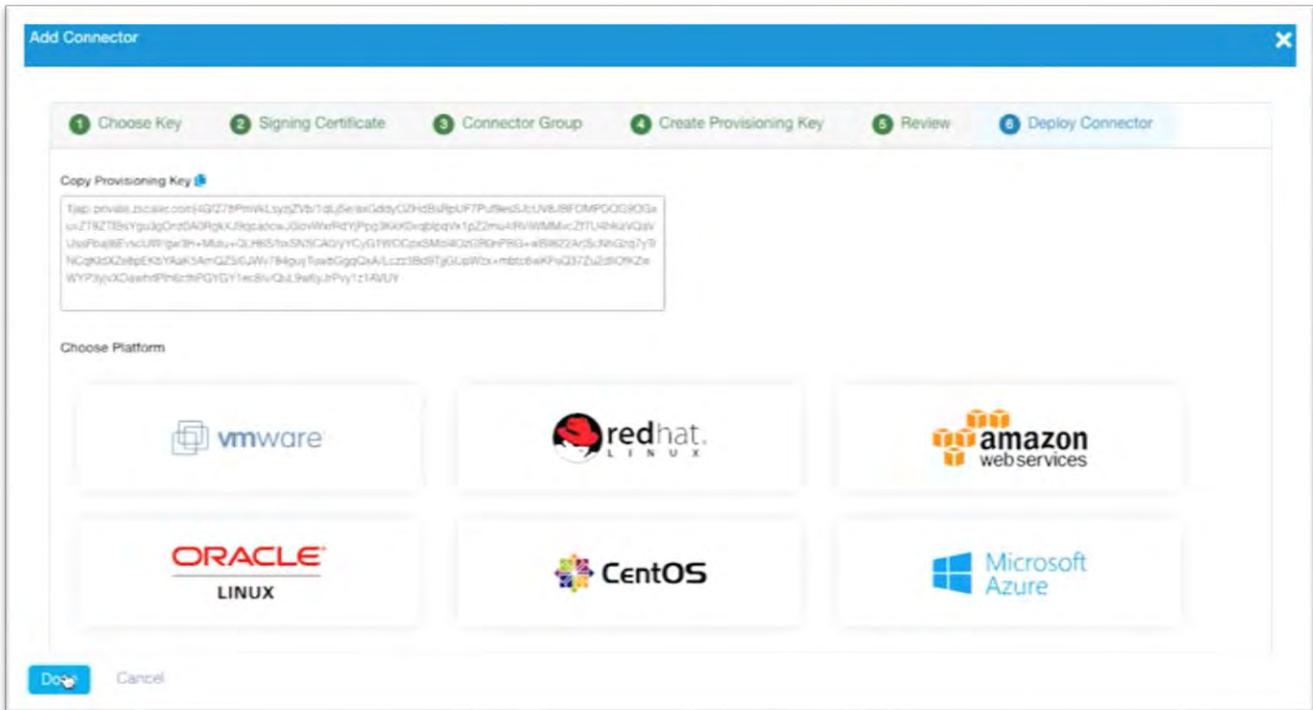


The screenshot shows the 'Add Connector' dialog box with the progress bar updated to Step 5: Review (highlighted). The main content area now displays a summary of the configuration: 'Certificate Name' (empty), 'Connector' (empty), 'Connector Group' (empty), 'AWS Tokyo' (empty), 'Provisioning Key' (empty), and 'AWS Tokyo' (empty). Below the summary, there is a text prompt: 'Review all of the information before clicking Save'. At the bottom, there are three buttons: 'Save' (highlighted in blue), 'Previous', and 'Cancel'.

はじめての ZPA

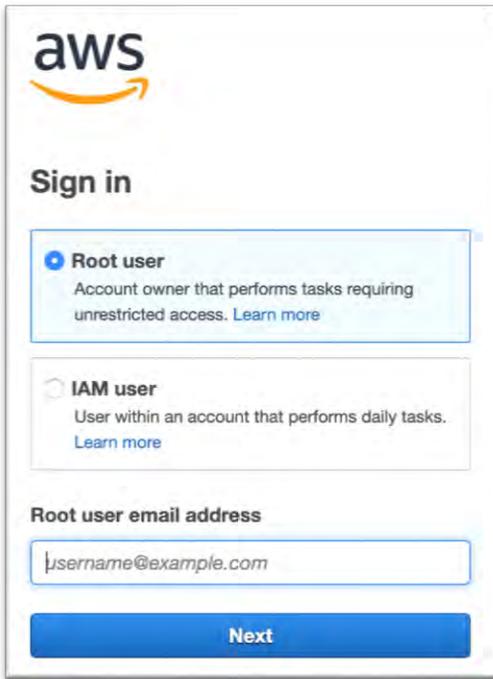
[Done]をクリックします。

なお、Choose Platform より各 Platform をクリックすると、より詳細な情報（インスタンスの必要スペックなど）が確認可能です。

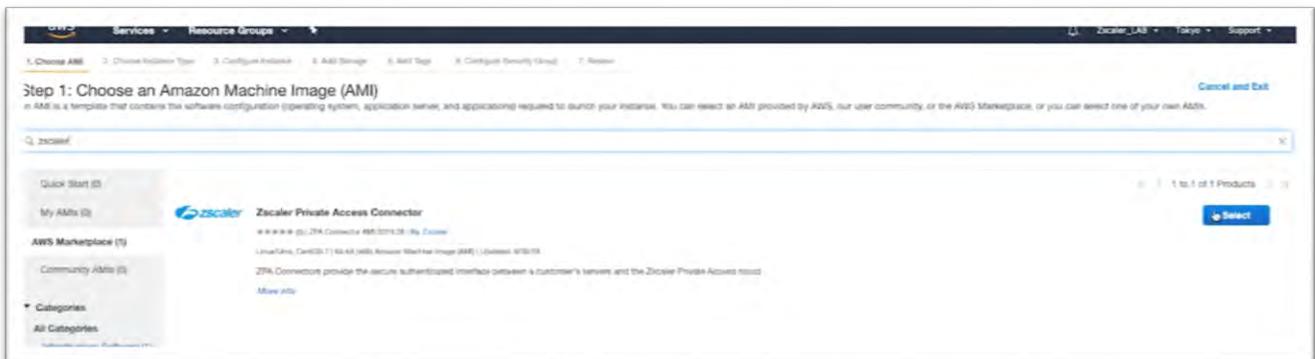


Step2. Connector のインストール

AWS にログインします。



AWS Marketplace より、「Zscaler Private Access Connector」を選択します。



はじめての ZPA

内容を確認して、[Continue] をクリックします。

Zscaler Private Access Connector



Zscaler Private Access Connector
Connectors can be co-located with your enterprise applications, or they can be deployed in any location that has connectivity to the applications. Typically, they are deployed on network segments that can access secured applications and the ZPA cloud simultaneously, such as in a DMZ. Connectors only connect outbound; they do not need any inbound ...

[More info](#)
[View Additional Details in AWS Marketplace](#)

Product Details

By	Zscaler
Customer Rating	***** (0)
Latest Version	ZPA Connector AMI 2019.08
Base Operating System	Linux/Unix, CentOS 7
Delivery Method	64-bit (x86) Amazon Machine Image (AMI)
License Agreement	End User License Agreement
On Marketplace Since	8/30/19
AWS Services Required	Amazon EC2, Amazon EBS, Amazon VPC

Highlights

- Provides the secure authenticated interface between a customers servers and

Pricing Details
Bring Your Own License (BYOL)

Hourly Fees

Instance Type	Software	EC2	Total
t3a.medium	\$0.00	\$0.049	\$0.049/hr
t3a.large	\$0.00	\$0.099	\$0.099/hr
t3a.xlarge	\$0.00	\$0.198	\$0.198/hr
t3a.2xlarge	\$0.00	\$0.392	\$0.392/hr
t3.medium	\$0.00	\$0.054	\$0.054/hr
t3.large	\$0.00	\$0.109	\$0.109/hr
t3.xlarge	\$0.00	\$0.218	\$0.218/hr
t3.2xlarge	\$0.00	\$0.435	\$0.435/hr
m5a.large	\$0.00	\$0.112	\$0.112/hr
m5a.xlarge	\$0.00	\$0.224	\$0.224/hr
m5a.2xlarge	\$0.00	\$0.448	\$0.448/hr
m5a.4xlarge	\$0.00	\$0.896	\$0.896/hr
m5.large	\$0.00	\$0.124	\$0.124/hr
m5.xlarge	\$0.00	\$0.248	\$0.248/hr
m5.2xlarge	\$0.00	\$0.496	\$0.496/hr
m5.4xlarge	\$0.00	\$0.992	\$0.992/hr

[Cancel](#) [Continue](#)

Instance Type は t3.xlarge を選択し、[Next: Configure Instance Details]をクリックします。

Services - Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

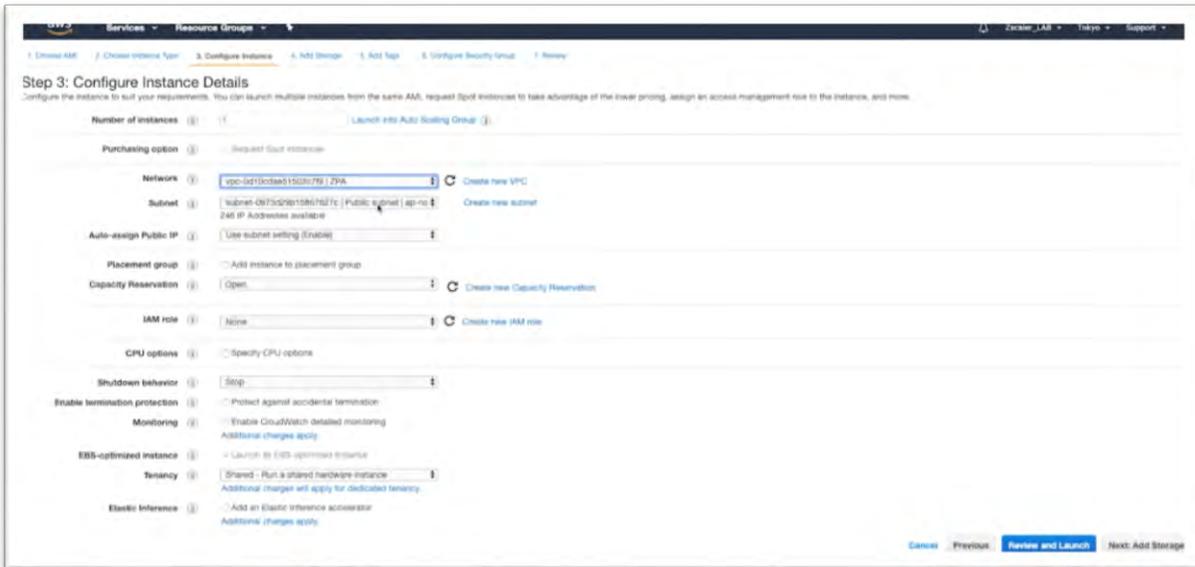
Step 2: Choose an Instance Type

Instance Type	General purpose	RAM (GB)	Storage	OS	Price	Free tier	Network	Accelerated Provisioning
t3.xlarge	General purpose	8	30	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.nano	General purpose	2	0.5	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.micro	General purpose	2	1	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.small	General purpose	2	2	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.medium	General purpose	2	4	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.large	General purpose	2	8	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.xlarge	General purpose	4	16	EBS only	---	Yes	Up to 5 Gbps	Yes
t3a.2xlarge	General purpose	8	32	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.nano	General purpose	2	0.5	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.micro	General purpose	2	1	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.small	General purpose	2	2	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.medium	General purpose	2	4	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.large	General purpose	2	8	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.xlarge	General purpose	4	16	EBS only	---	Yes	Up to 5 Gbps	Yes
t3.2xlarge	General purpose	8	32	EBS only	---	Yes	Up to 5 Gbps	Yes
m5a.xlarge	General purpose	2	8	1 x 75 (SSD)	---	Yes	Up to 10 Gbps	Yes
m5a.2xlarge	General purpose	4	16	1 x 150 (SSD)	---	Yes	Up to 10 Gbps	Yes

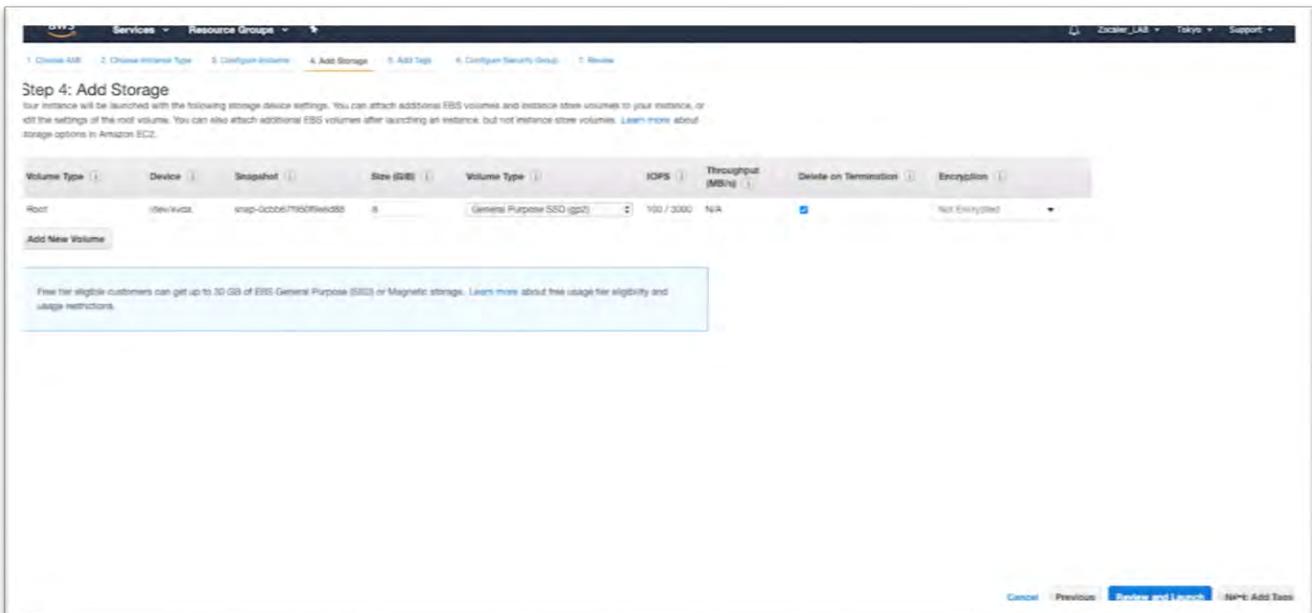
[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

はじめての ZPA

Network を社内リソースがある VPC に変更し、[Next: Add Storage]をクリックします。

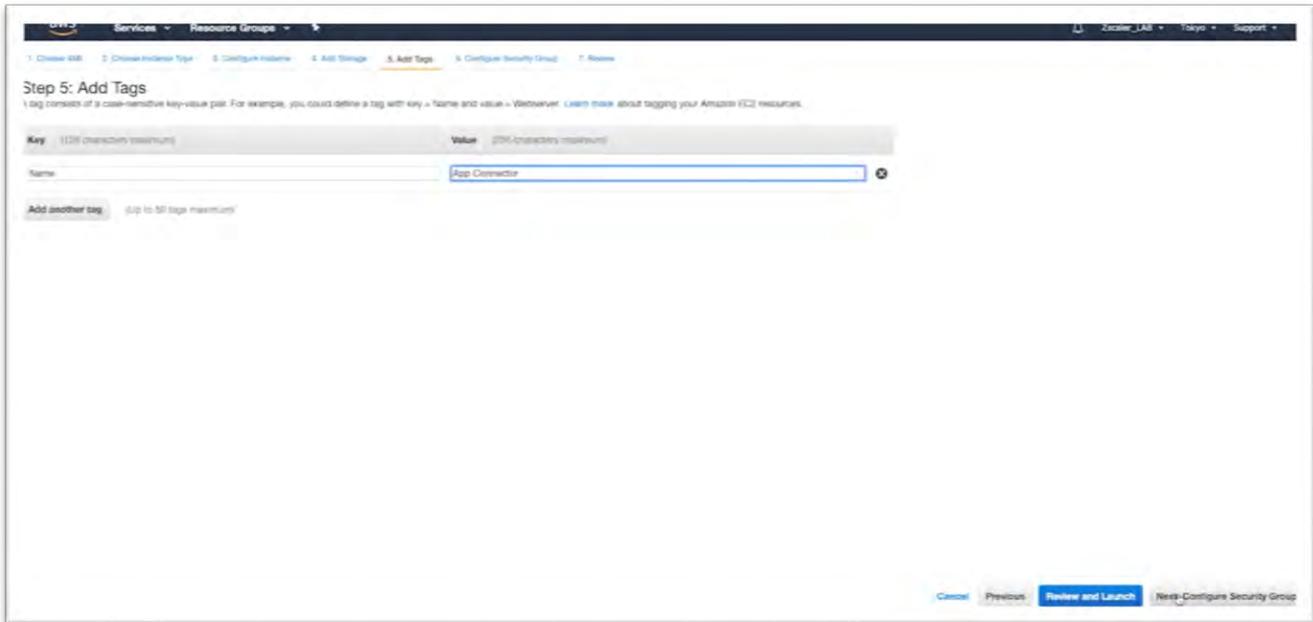


Storage は変更せずに、[Next: Add tags]をクリックします。

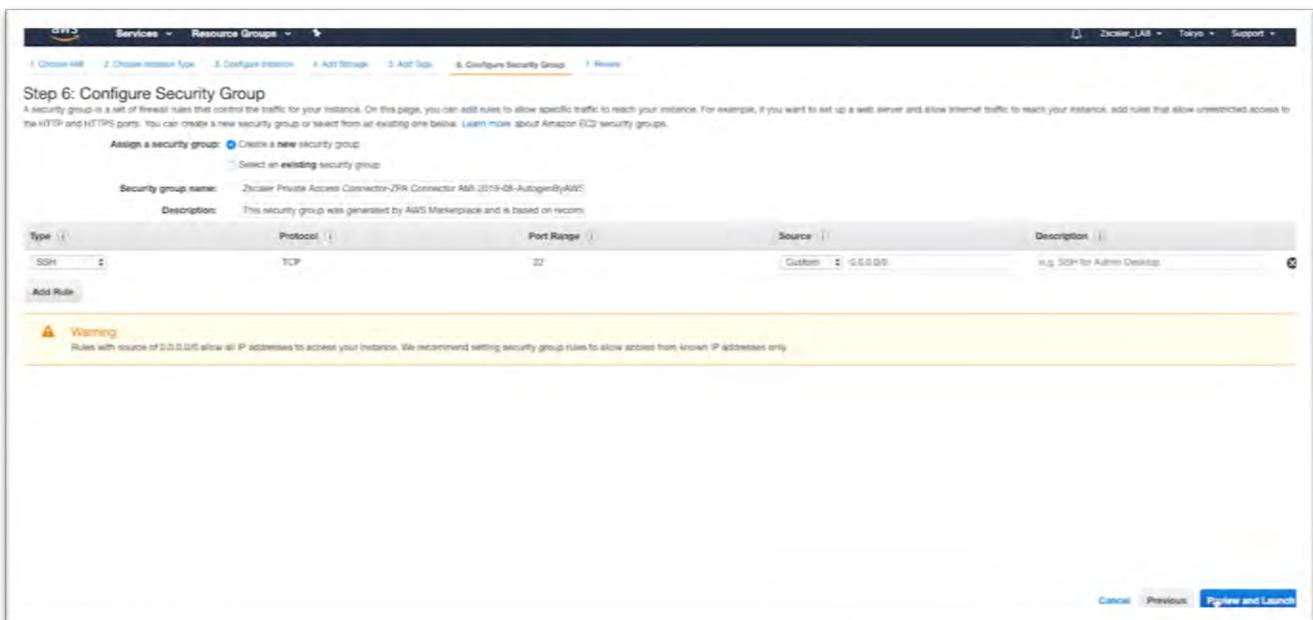


はじめての ZPA

必要に応じてわかりやすいように Tags を作成して、[Next: Configure Security Group] をクリックします。

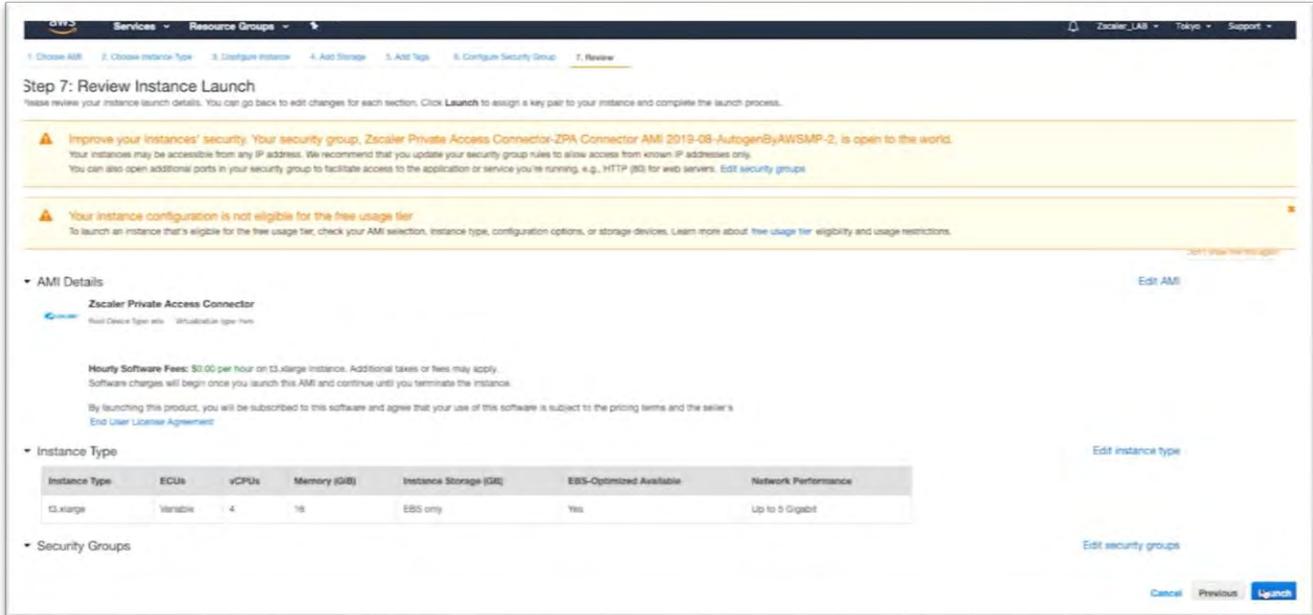


何も変更せずに[Review and Launch]をクリックします。

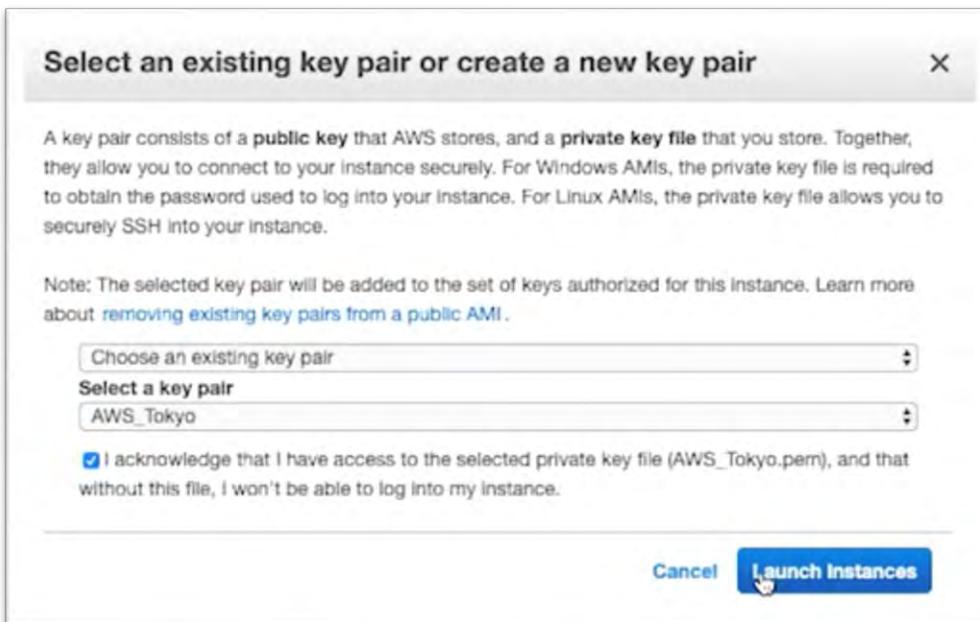


はじめての ZPA

内容を確認して、[Launch]をクリックします。

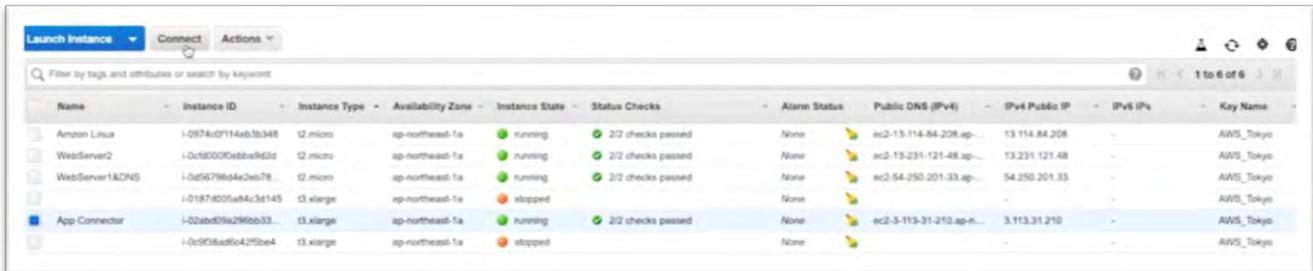


SSH でログインする際に使用する Key Pair を選択し、[launch Instances]をクリックします。



はじめての ZPA

Instance のデプロイが完了（AWS ですと約 4 分）したら、[Connect]をクリックし、SSH のコマンドを確認します（user は root ではなく admin に変更）。



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name
Amazon Linux	i-0974d0114eb3b348	t2.micro	ap-northeast-1a	running	2/2 checks passed	None	ec2-13-114-84-208.ap-...	13.114.84.208	-	AWS_Tokyo
WebServer2	i-0d40003e8ba9d2c	t2.micro	ap-northeast-1a	running	2/2 checks passed	None	ec2-13-231-121-48.ap-...	13.231.121.48	-	AWS_Tokyo
WebServer1&DNS	i-0d5679e4a2e678	t2.micro	ap-northeast-1a	running	2/2 checks passed	None	ec2-54-250-201-33.ap-...	54.250.201.33	-	AWS_Tokyo
App Connector	i-02ab405a4c3e145	t3.xlarge	ap-northeast-1a	stopped	-	None	-	-	-	AWS_Tokyo
	i-02ab405a4c3e145	t3.xlarge	ap-northeast-1a	running	2/2 checks passed	None	ec2-3-113-31-210.ap-n...	3.113.31.210	-	AWS_Tokyo
	i-0c93a46c42f5e4	t3.xlarge	ap-northeast-1a	stopped	-	None	-	-	-	AWS_Tokyo

Connect to your instance

Connection method

- A standalone SSH client
- Session Manager
- EC2 Instance Connect (browser-based SSH connection)

To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (AWS_Tokyo.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 AWS_Tokyo.pem
```
4. Connect to your instance using its Public DNS:

```
ec2-3-113-31-210.ap-northeast-1.compute.amazonaws.com
```

Example:

```
ssh -i "AWS_Tokyo.pem" root@ec2-3-113-31-210.ap-northeast-1.compute.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

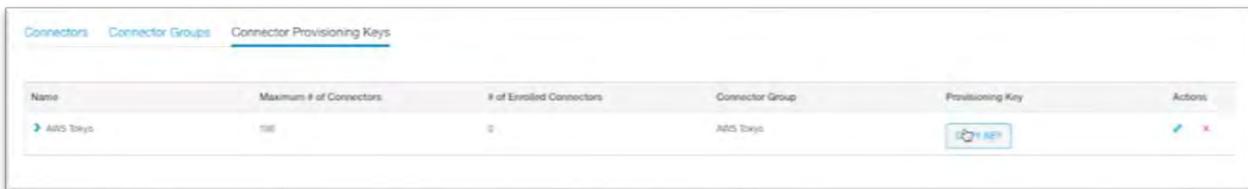
はじめての ZPA

ログインが成功したら、以下のコマンドを実行します。

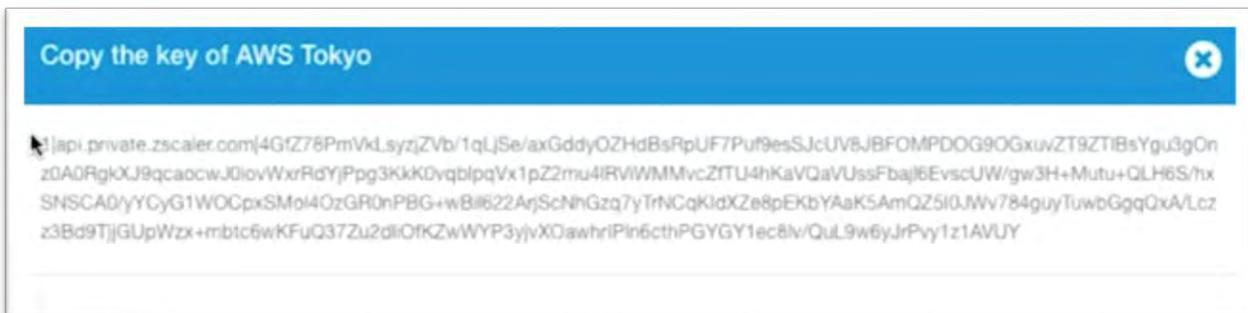
1. `sudo systemctl stop zpa-connector`
2. `sudo touch /opt/zscaler/var/provision_key`
3. `sudo chmod 644 /opt/zscaler/var/provision_key`
4. `sudo vi /opt/zscaler/var/provision_key`

作成したファイルにプロビジョニングキーをペーストして保存します。

プロビジョニングキーは、Connector Provisioning Keysより[COPY KEY]をクリックして確認可能です。



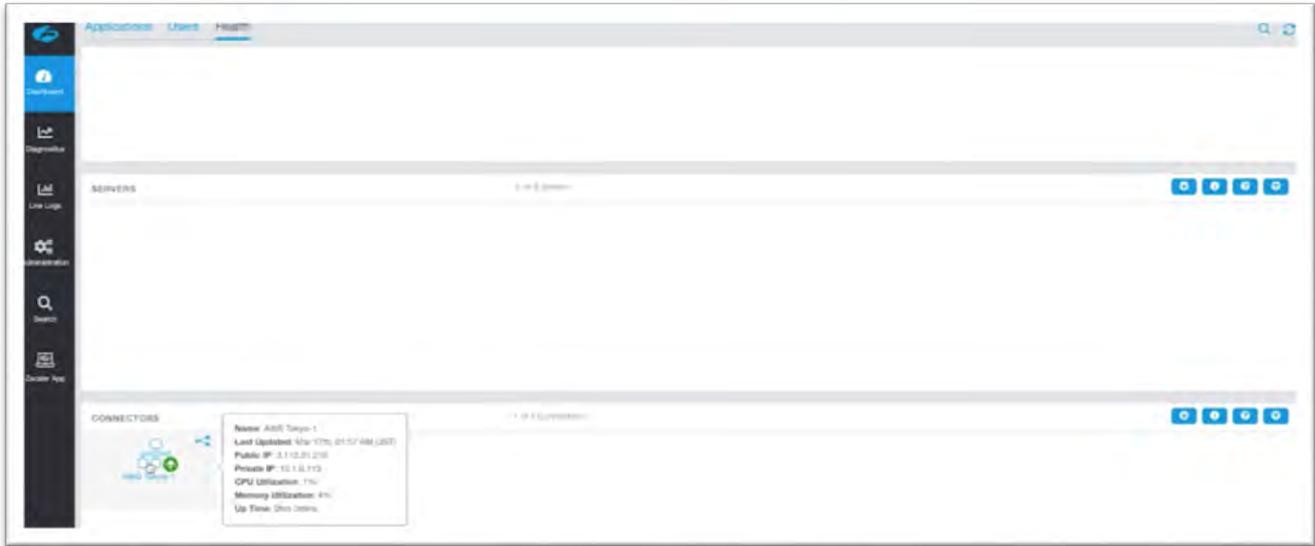
Name	Maximum # of Connectors	# of Enrolled Connectors	Connector Group	Provisioning Key	Actions
AWS Tokyo	100	0	AWS Tokyo		 



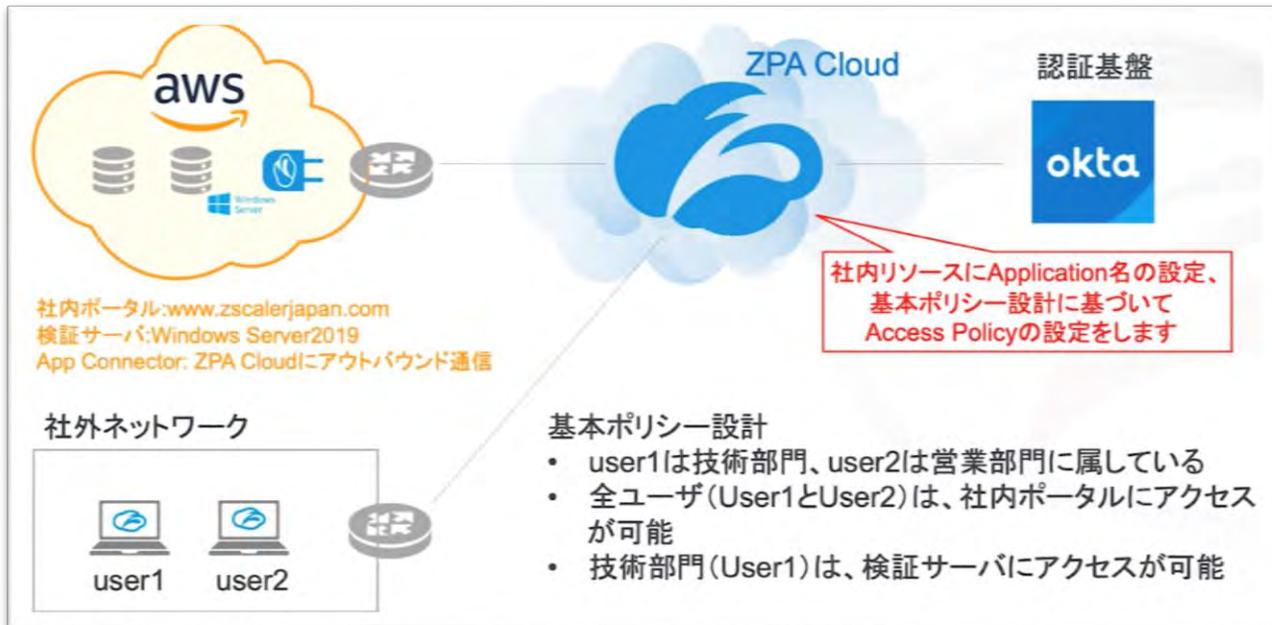
Copy the key of AWS Tokyo

```
!|api.private.zscaler.com|4GfZ78PmVklSyzjZVb/1qLjSe/axGddyOZHdBsRpUF7Puf9esSjCuvBjBFOMPDOG9OGxuvZT9ZTIBsYgu3gOn  
z0A0RgkXJ9qcaocwJ0lovWxrRdYjPpg3Kkk0vqblpqVx1pZ2mu4IRVWMMvcZFTU4hKaVQaVUssFbajl6EvscUW/gw3H+Mutu+QLH6S/hx  
SNSCA0/yYCyG1WOCpxSMoI4OzGR0nPBG+wBll622ArjScNhGzq7yTrNCqKidXZe8pEKbYAaK5AmQZ5i0JWv784guyTuwbGgqQxAVLcz  
z3Bd9TjJGUpWzx+mbtc6wKFuQ37Zu2dliOfKZwWYP3yJvXDawhriPin6cthPGYGY1ec8lv/QuL9w6yJrPvy1z1AVUJ
```


はじめての ZPA

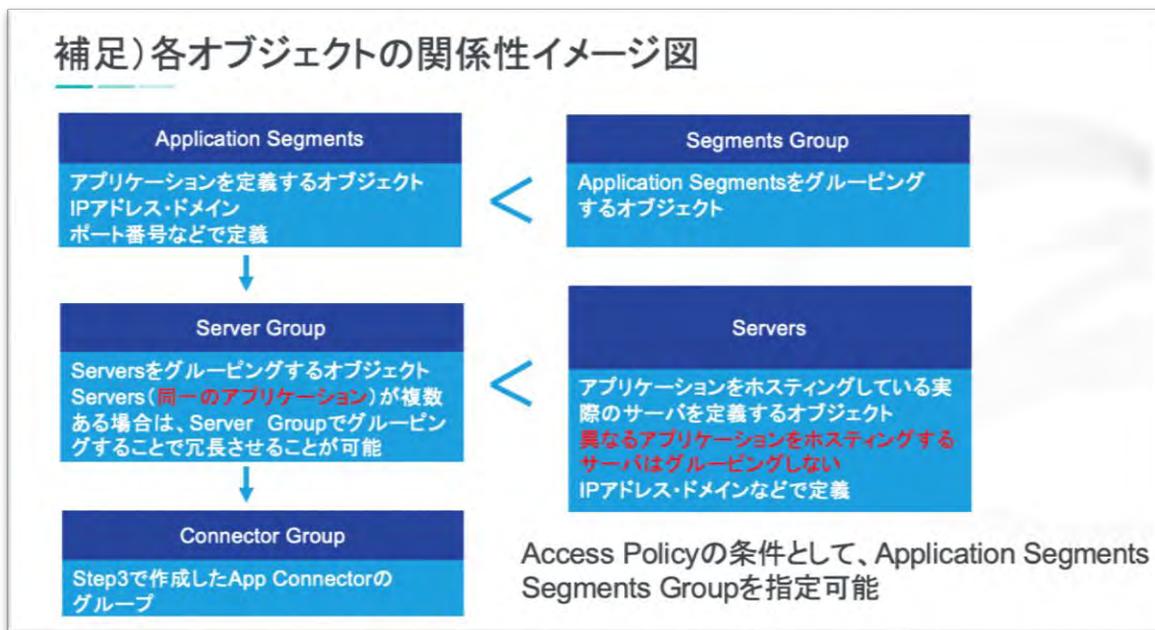


3-4. Application Segmentation / Access Policy の設定



Notes

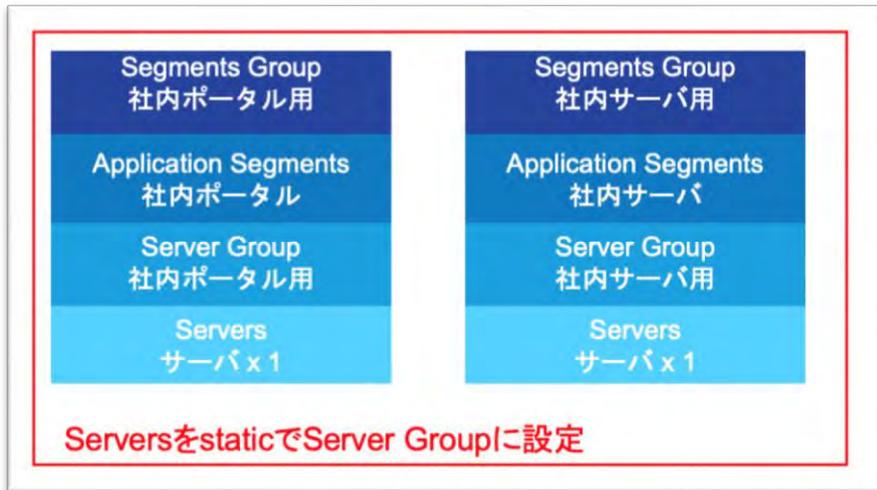
✓ 本手順で作成するオブジェクトの関係性イメージ図



はじめての ZPA

- ✓ 本章では、Servers を static に設定

実際の環境では、Server Group の設定に Dynamic Server Discovery を使用
設定方法については [\(5. Dynamic Server Discovery について\)](#) を参照

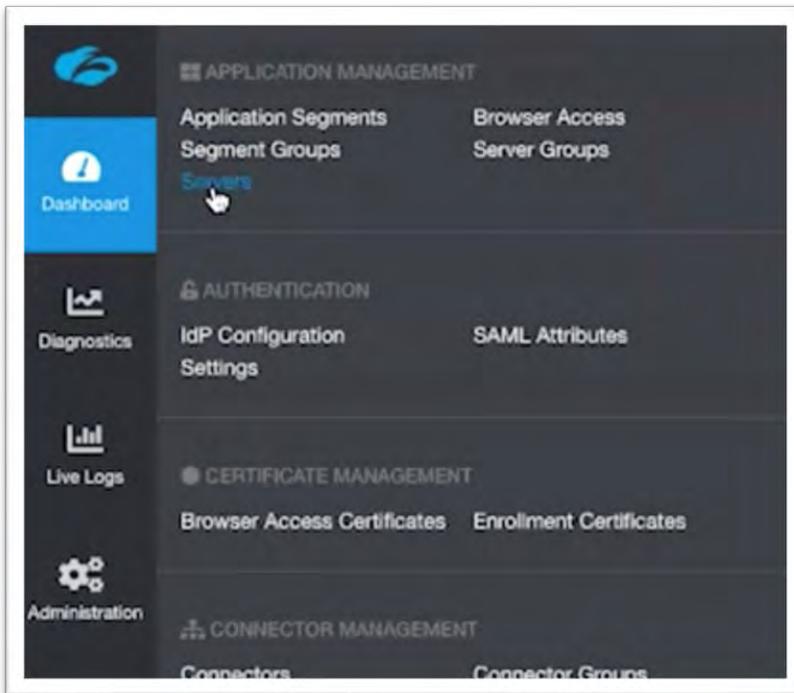


- ✓ 社内アプリへアクセスが発生した際の内部処理イメージ

Access Policyに設定しているApplication SegmentsまたはSegments Groupにヒット
-> 紐づいている Server Groupの処理 -> Server Groupが紐づいているApp
Connectorの処理 -> 社内アプリ

Step 1 . Servers / Server Groups の作成の作成

Administration -> APPLICATION MANAGEMENT より、Servers のオブジェクトを作成します。



[Add Server]をクリックします。



はじめての ZPA

必要事項を記入、設定し [Save] をクリックします。

+++++

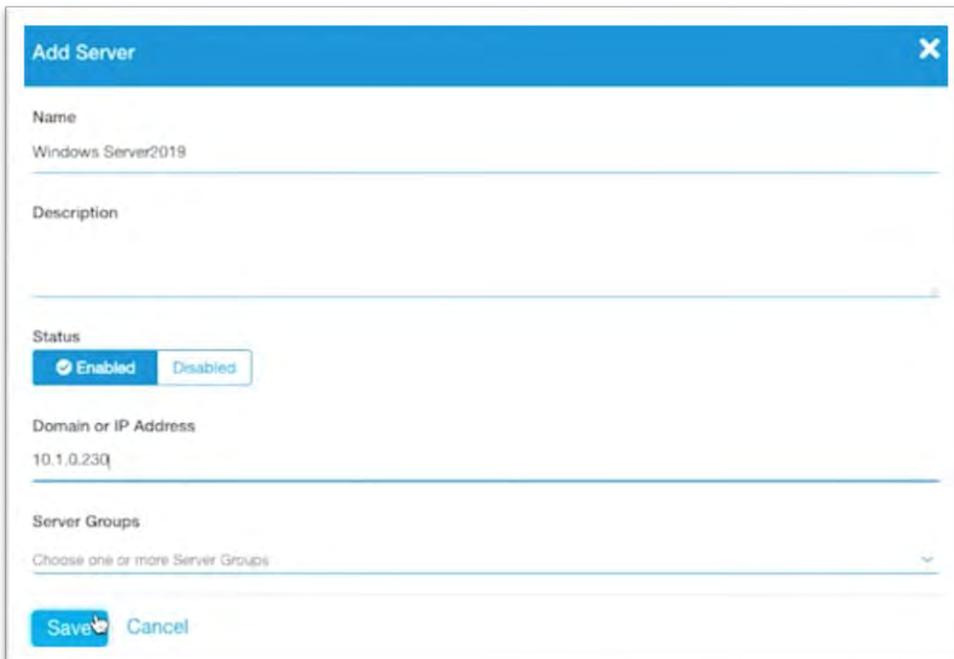
Name: 任意の名前

Status: Enabled

Domain or IP Address: ドメイン名 or IP アドレス

+++++

社内サーバの設定例



The screenshot shows a dialog box titled "Add Server". The fields are filled with the following information:

- Name: Windows Server2019
- Description: (empty)
- Status: Enabled (selected)
- Domain or IP Address: 10.1.0.230
- Server Groups: Choose one or more Server Groups

Buttons at the bottom: Save, Cancel

社内ポータルの設定例

Add Server [X]

Name
Web Server1

Description

Status
 Enabled Disabled

Domain or IP Address
www.zscalerjapan.com

Server Groups
Choose one or more Server Groups

Save Cancel

Server Groups より、[Add Server Group]をクリックします。

Name	Status	Domain or IP Address	Actions
Web Server1		www.zscalerjapan.com	

Name	Status	Dynamic Server Discovery	Connector Groups	Actions
Server Group				

はじめての ZPA

必要事項を記入、設定し [Save] をクリックします。

+++++

Name: 任意の名前

Status: Enabled

Dynamic Server Discovery: Off (※)

Servers: グルーピングする Servers を選択

Connector Groups: Step3-3 で作成した Connector Group

+++++

※Dynamic Server Discovery を使用することで、社内アプリケーションの定義をサブネットや* (ワイルドカード) を使用することが可能です。設定方法については、「5-2. Dynamic Server Discoveryの設定」を参照してください

社内サーバの設定例

The screenshot shows a dialog box titled "Add Server Group". It contains the following fields and controls:

- Name:** Tech Windows Server
- Description:** (Empty text area)
- Status:** Radio buttons for "Enabled" (selected) and "Disabled".
- Dynamic Server Discovery:** Radio buttons for "On" and "Off" (selected).
- Servers:** A list containing "Windows Server2019".
- Connector Groups:** A list containing "AWS Tokyo".
- Buttons:** "Save" and "Cancel" at the bottom left.

社内ポータルの設定例

Add Server Group [X]

Name
intra web site

Description

Status: Enabled Disabled

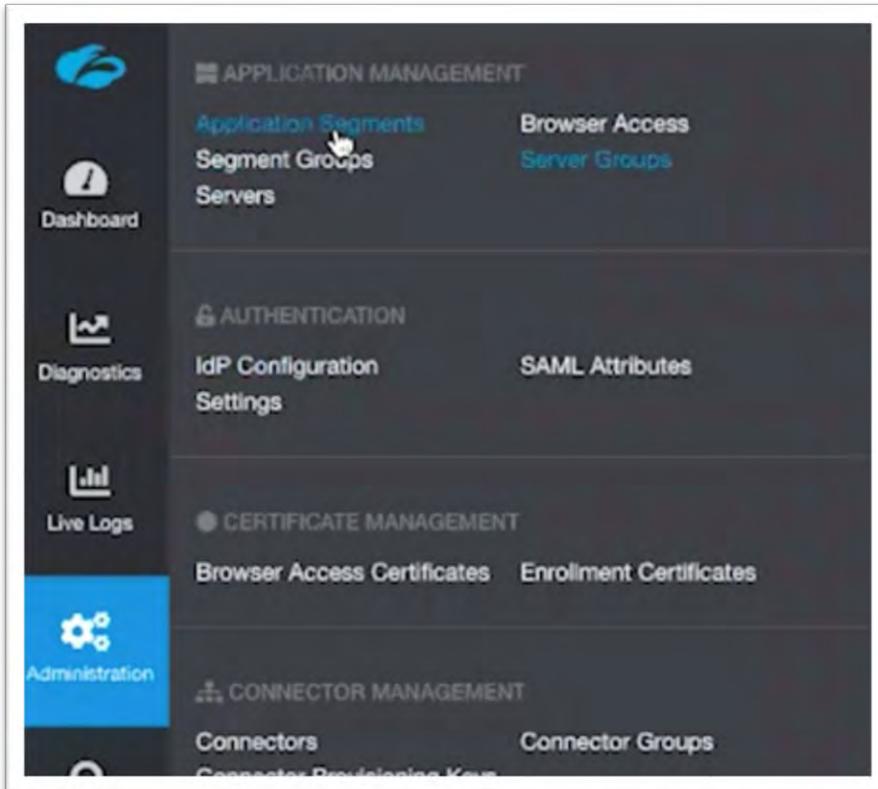
Dynamic Server Discovery: On Off

Servers:

Connector Groups:

Step2. Application Segments / Segment Groups の作成

Administration -> APPLICATION MANAGEMENT -> Application Segments より、Application Segments を作成します。



[Add Application Segment]をクリックします



必要事項を記入し [Next] をクリックします。

はじめての ZPA

+++++

Name: 任意の名前

Status: Enabled

APPLICATIONS: ドメイン名 or IP アドレス

TCP Port Ranges: アプリケーションのポート番号

Connector Groups: Step3-3 で作成した Connector Group

+++++

社内サーバの設定例

Add Segment Group を選択し、必要事項を記入、設定し [Next] をクリックします。

はじめての ZPA

+++++

Name: 任意の名前

Status: Enabled

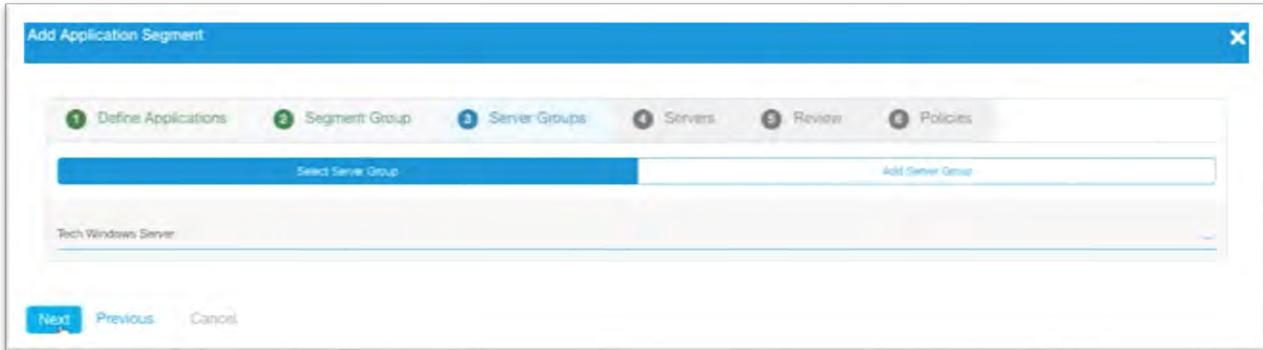
+++++

The screenshot shows the 'Add Application Segment' dialog box with the 'Segment Group' step selected. The progress bar at the top indicates the current step. Below the progress bar, there are two buttons: 'Select Segment Group' and 'Add Segment Group'. The 'Name' field contains 'Tech Windows Server'. The 'Description' field is empty. The 'Status' is set to 'Enabled' with a radio button. At the bottom, there are 'Next', 'Previous', and 'Cancel' buttons.

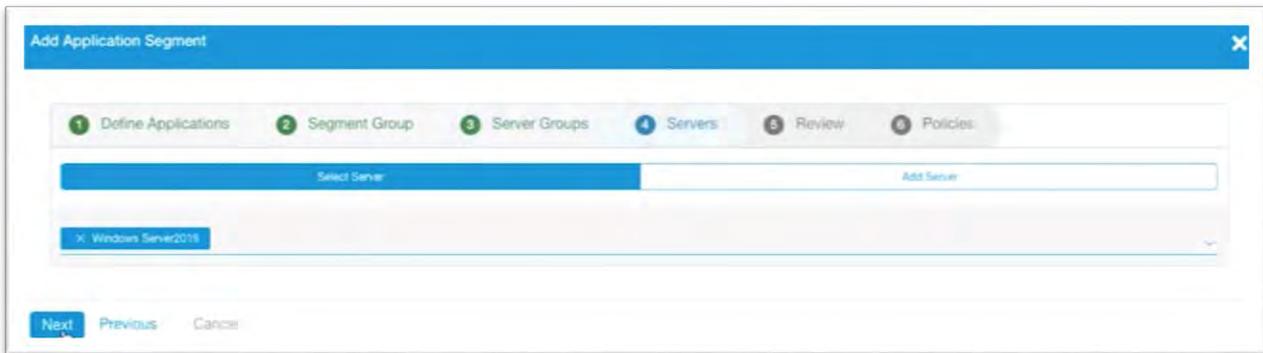
Step1 で作成した Application Segments に対応する Server Group を選択し、[Next]をクリックします。

The screenshot shows the 'Add Application Segment' dialog box with the 'Server Groups' step selected. The progress bar at the top indicates the current step. Below the progress bar, there are two buttons: 'Select Server Group' and 'Add Server Group'. The 'Select a Server Group' dropdown menu is open, showing a search bar and two options: 'Intra web site' and 'Tech Windows Server'. The 'Intra web site' option is selected. At the bottom, there are 'Next', 'Previous', and 'Cancel' buttons.

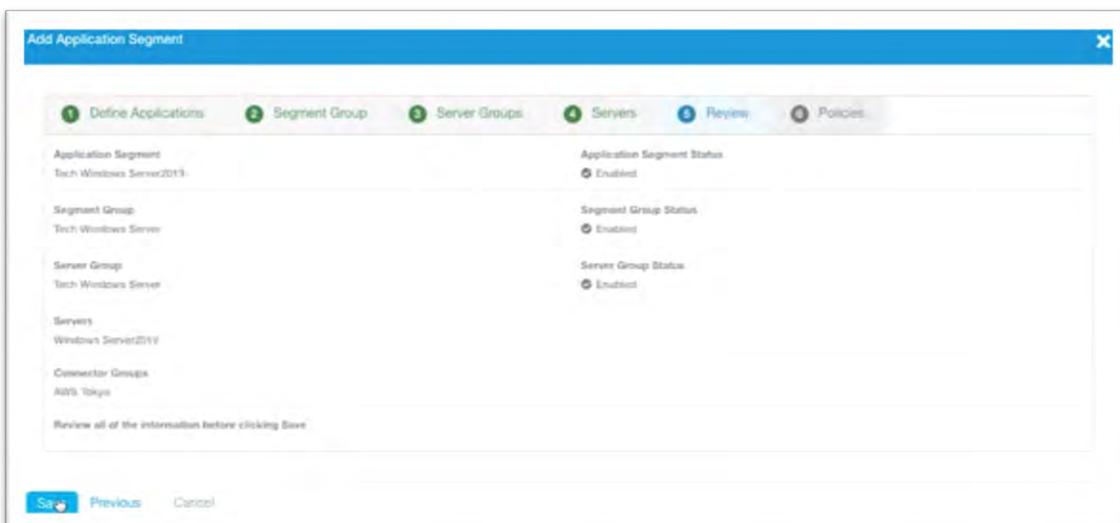
はじめての ZPA



Server Groups に紐づいている Servers を確認して、[Next]をクリックします。

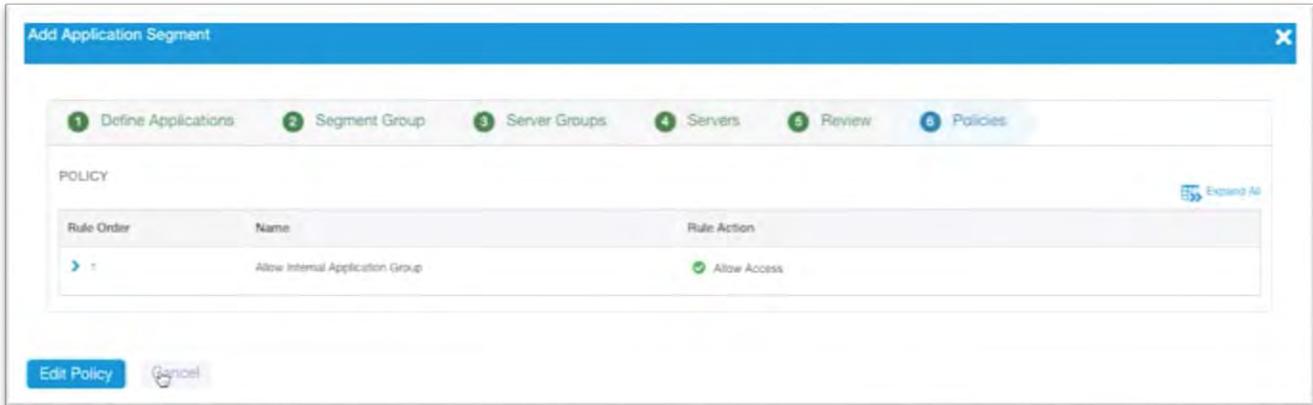


内容を確認して[Save]をクリックします。

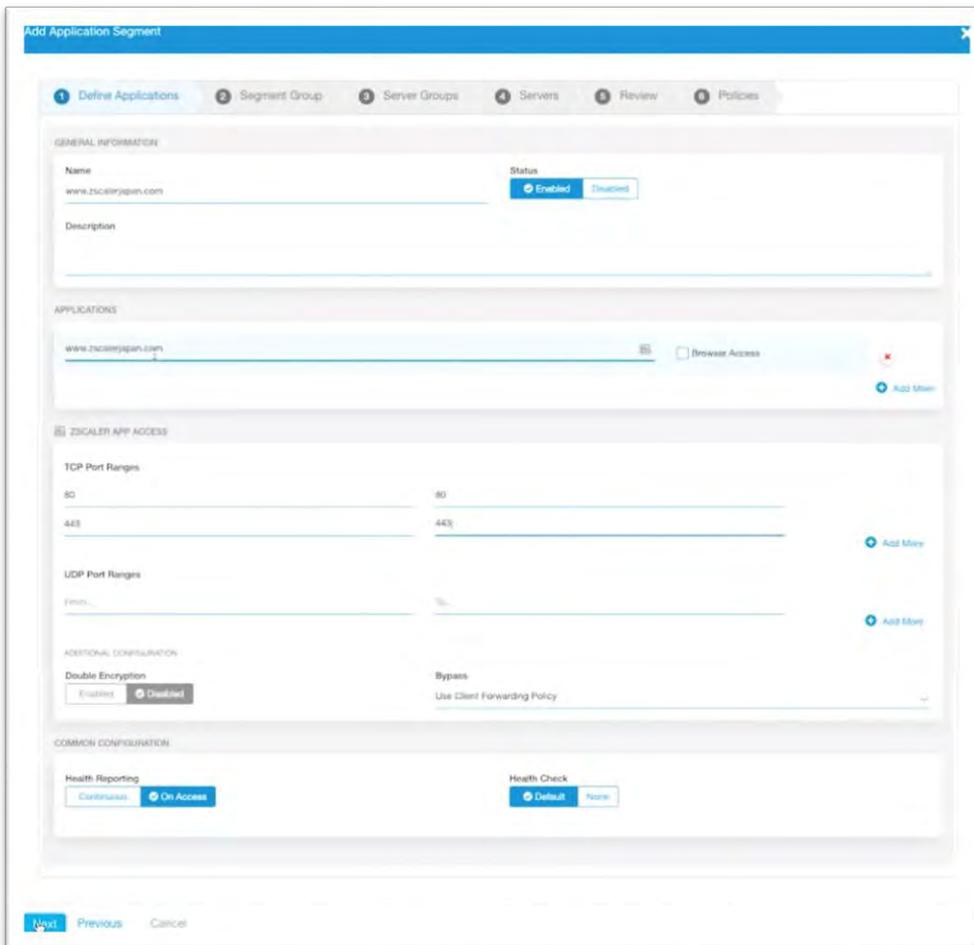


はじめての ZPA

Access Policy は後で設定するので、[Cancel]をクリックします。



社内サーバの設定例



はじめての ZPA

Add Application Segment [Close]

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

Select Segment Group Add Segment Group

Name
Intra web site

Description

Status
 Enabled Disabled

Next Previous Cancel

Add Application Segment [Close]

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

Select Server Group Add Server Group

Select a Server Group

Enter a search string [Clear] [Search]

Intra web site Server Group

Tech Windows Server

Clear Selection

Add Application Segment [Close]

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

Select Server Add Server

Web Server1

Next Previous Cancel

はじめての ZPA

Add Application Segment ✕

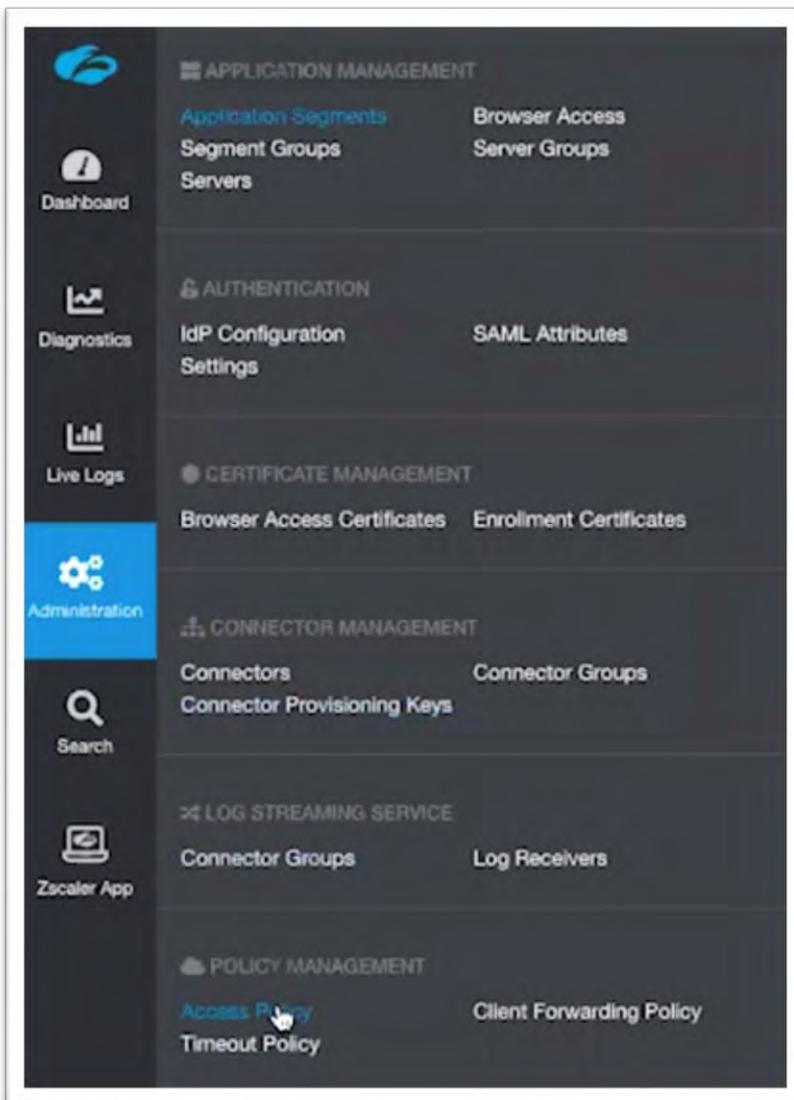
1 Define Applications 2 Segment Group 3 Server Groups 4 Servers 5 Review 6 Policies

Application Segment www.zscalerjapan.com	Application Segment Status <input checked="" type="radio"/> Enabled
Segment Group Intra web site	Segment Group Status <input checked="" type="radio"/> Enabled
Server Group Intra web site	Server Group Status <input checked="" type="radio"/> Enabled
Servers Web Server1	
Connector Groups AWS Tokyo	

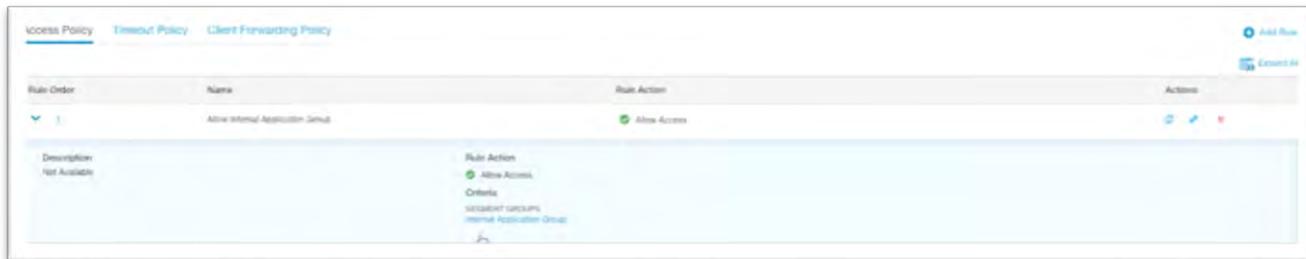
Review all of the information before clicking Save

Step3. Access Policy の作成

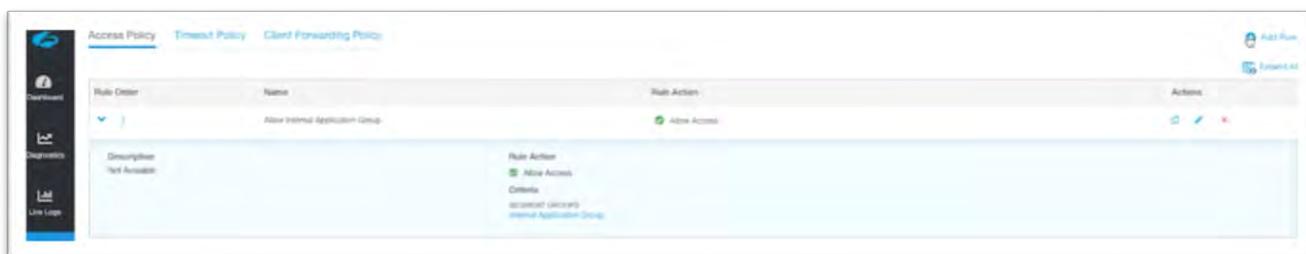
Administration -> POLICY MANAGEMNET -> Access Policy より、Access Policy を作成します。



はじめての ZPA



[Add rule]をクリックします。



まずは、営業部門が社内サーバにアクセス禁止という Policy を作成します。

必要事項を記入、設定し [Save] をクリックします。

+++++

Name: 任意の名前

Rule Action: Block Access

Message to User: 任意のメッセージ

Application Segments: Tech Windows Server2019 (※1)

SAML Attributes: GroupName_IdP Config = Sales_Div (※2)

+++++

※1 社内サーバの Application Segments

※2 「3-1. SP (ZPA) と IdP (okta) の SAML 認証連携設定」の Step3 で作成した
営業部門の Attribute

はじめての ZPA

Add Access Policy ✕

Name
Deny Tech Server for Sales_Div

Description

ACTION

Rule Action:

Message to User: You don't have a permission to access this site.

CRITERIA

Application Segments
 Tech Windows Server2019

or

Segment Groups
Select one or more segment groups

AND

SAML Attributes ⊕ Select IdP

↳ IdP Config

GroupName_IdP Config = Sales_Div ⊕ Add More

AND

Client Types
Any client type

AND

Zscaler App Posture Profiles
Select a posture profile ⊕ Add More

AND

Zscaler App Trusted Networks
Select one or more trusted networks

はじめての ZPA

次に、全員（技術部門、営業部門）が社内サーバにアクセス可能という Policy を作成します。

必要事項を記入、設定し [Save] をクリックします。

+++++

Name: 任意の名前

Rule Action: Allow Access

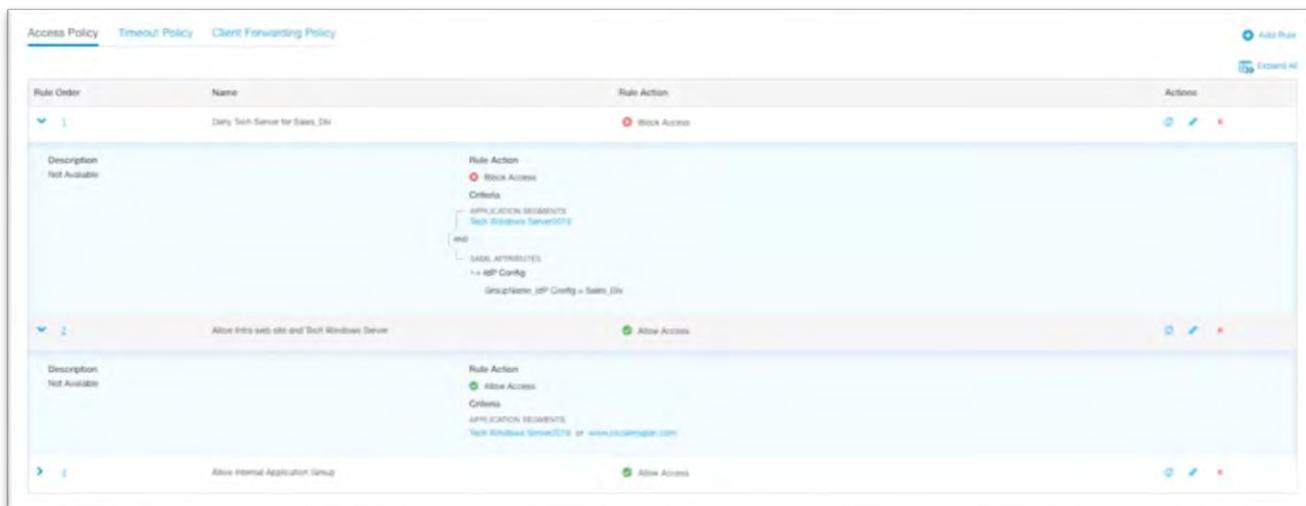
Application Segments: Tech Windows Server2019、www.zscalerjapan.com（※1）

SAML Attributes: なし（※2）

+++++

※1 社内サーバと社内ポータルサーバの Application Segments

※2 全員（技術部門、営業部門）という条件なので、SAML Attributes は設定しません



はじめての ZPA

Add Access Policy ✕

Name
Allow Intra web site and Tech Windows Server

Description

ACTION

Rule Action **Message to User**

Allow Access Block Access _____

CRITERIA

Application Segments
 Tech Windows Server2019 www.zscalerjapan.com

OR

Segment Groups
Select one or more segment groups

AND

SAML Attributes [+ Select IdP](#)
Any SAML attribute from any IdP

AND

Client Types
Any client type

AND

Zscaler App Posture Profiles
Select a posture profile [+ Add More](#)

AND

Zscaler App Trusted Networks
Select one or more trusted networks

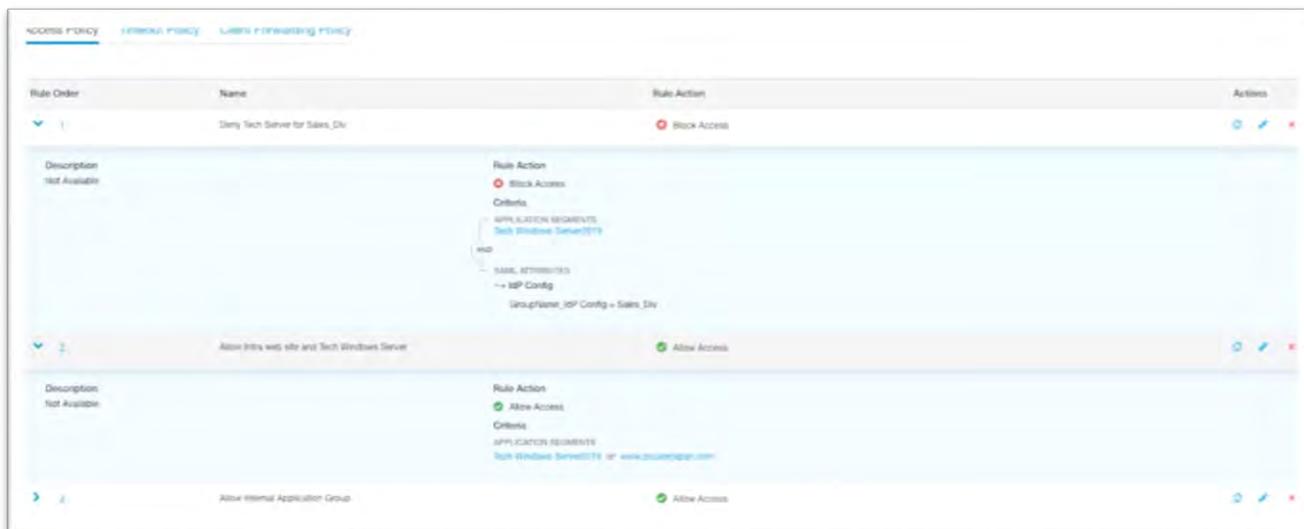
はじめての ZPA

Access Policyの精査は上から順に評価され、マッチしたポリシーが適応されます。
その後のポリシーの評価はされません。

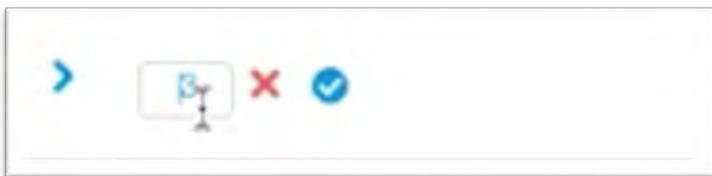
このため、想定した動作のためにはポリシーの順番を考慮する必要があります。

例)

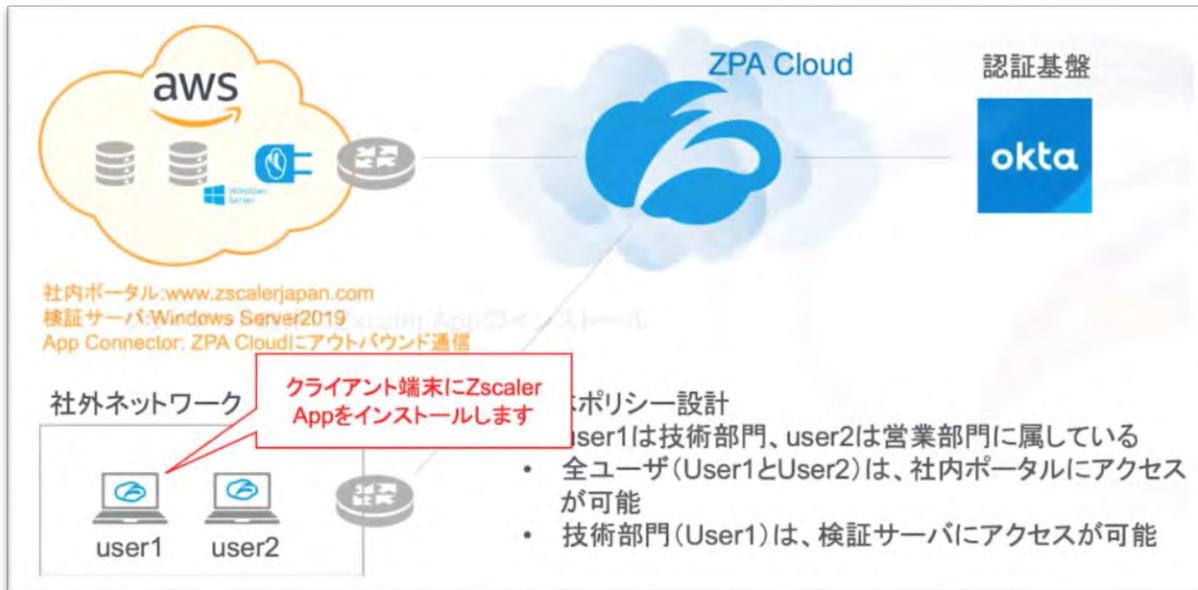
User	アクセス先	適応ポリシー	アクション
営業部門	社内ポータル	No2	Allow
営業部門	社内サーバ	No1	Deny
技術部門	社内ポータル	No2	Allow
技術部門	社内サーバ	No2	Allow



ポリシーの順番は番号をクリックすることで変更することが可能です。

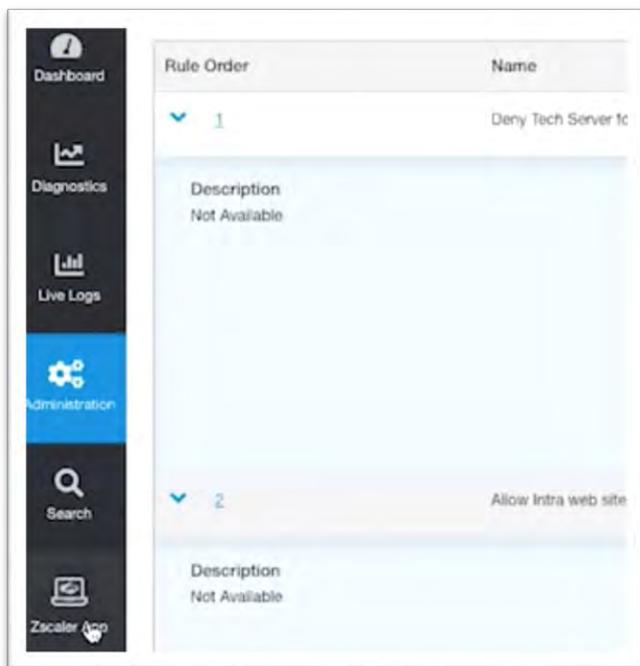


3-5. Zscaler App のインストール

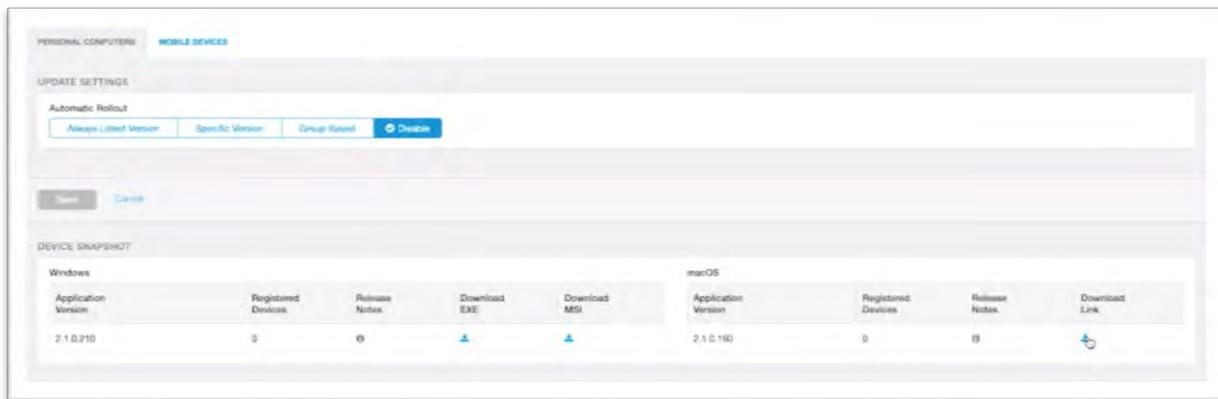
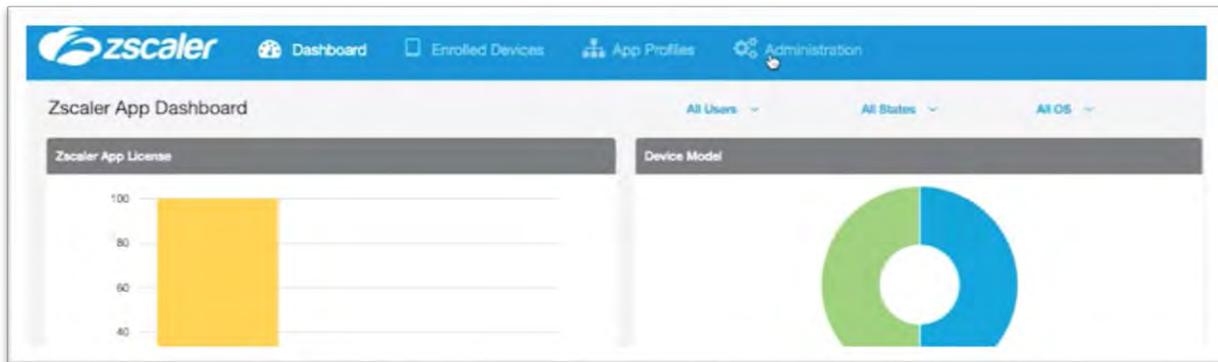


Step1. ZscalerApp のインストーラーダウンロード

Zscaler App -> Administration より、インストーラーをダウンロードします。



はじめての ZPA

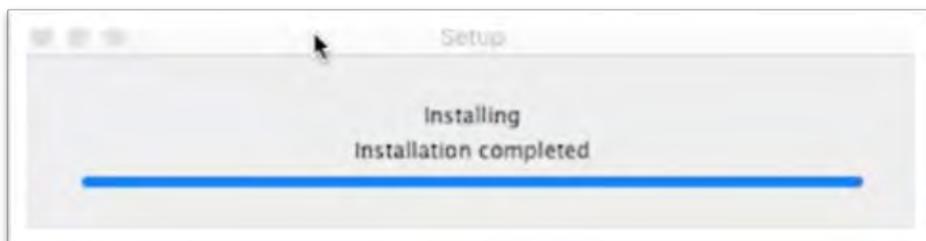
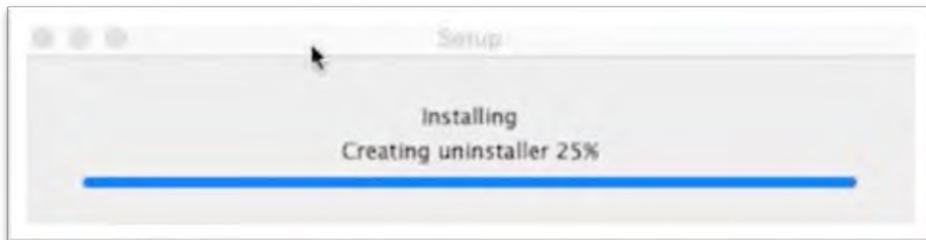


Step2. ZscalerApp のインストール

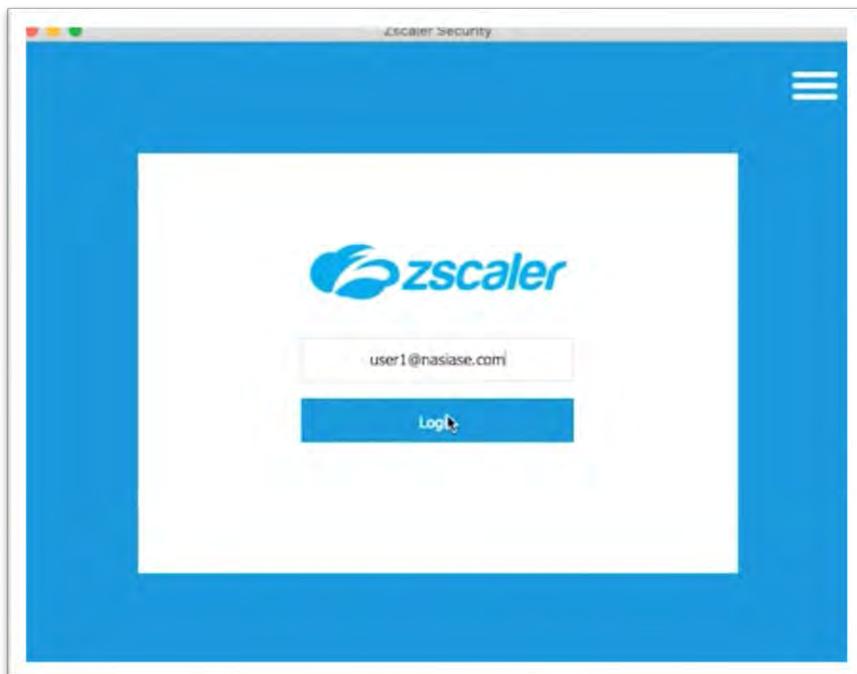
ダウンロードしたインストーラーを PC で実行します。

Name	Size	Kind	Date Added
Zscaler-osx-2.1.0.190-installer	25.9 MB	Application	Today 2:24
Zscaler-osx-2.1...-installer.app.zip	24.9 MB	ZIP archive	Today 2:24
AWS_Tokyo.pem	2 KB	printabl...archive	Today 1:40
metadata	2 KB	TextEdit	Today 1:25

はじめての ZPA

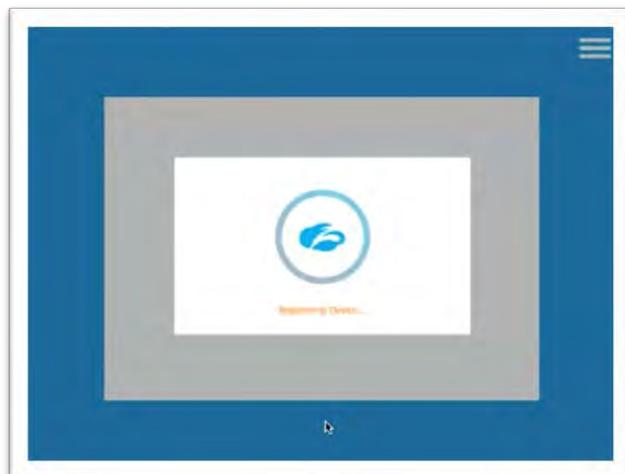
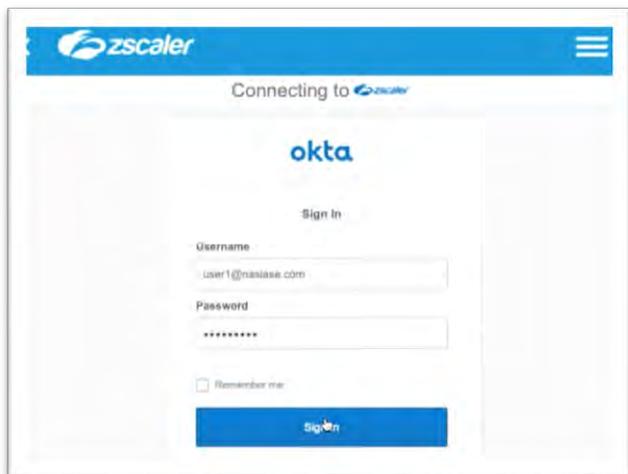


ユーザ名を入力して、[Login]をクリックします。

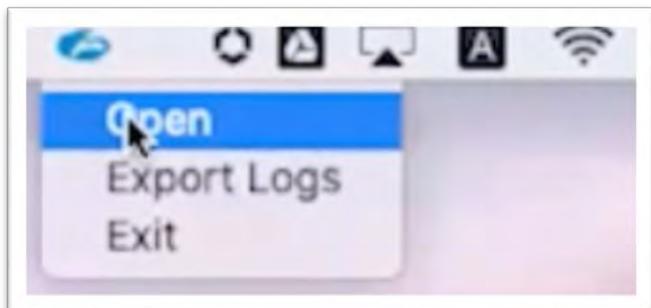


はじめての ZPA

Username、Password を入力して、[Signin]をクリックします。

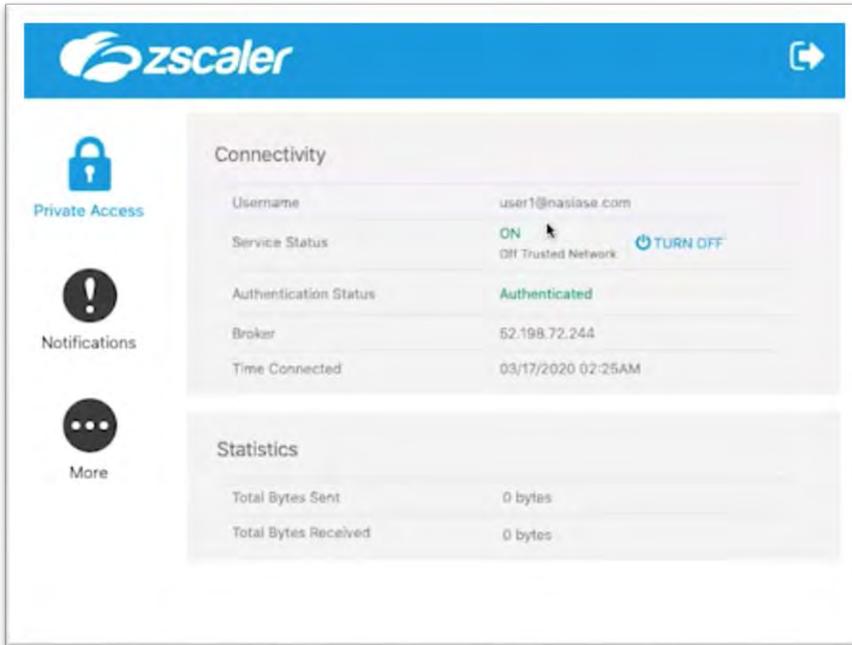


インストールされた、Zscaler App の[Open]をクリックします。

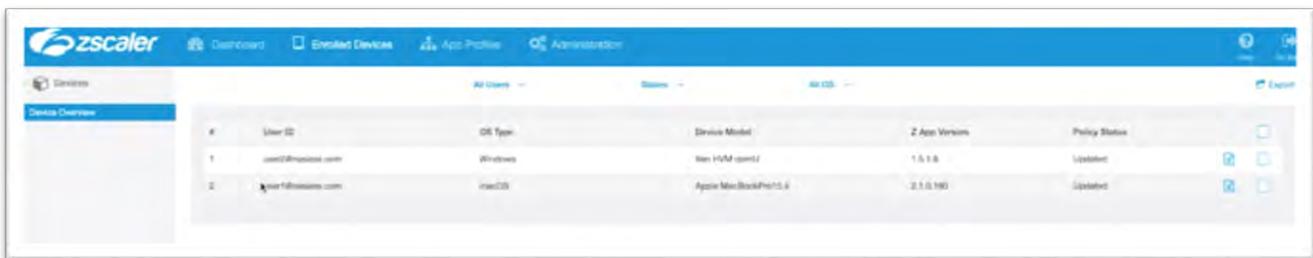


はじめての ZPA

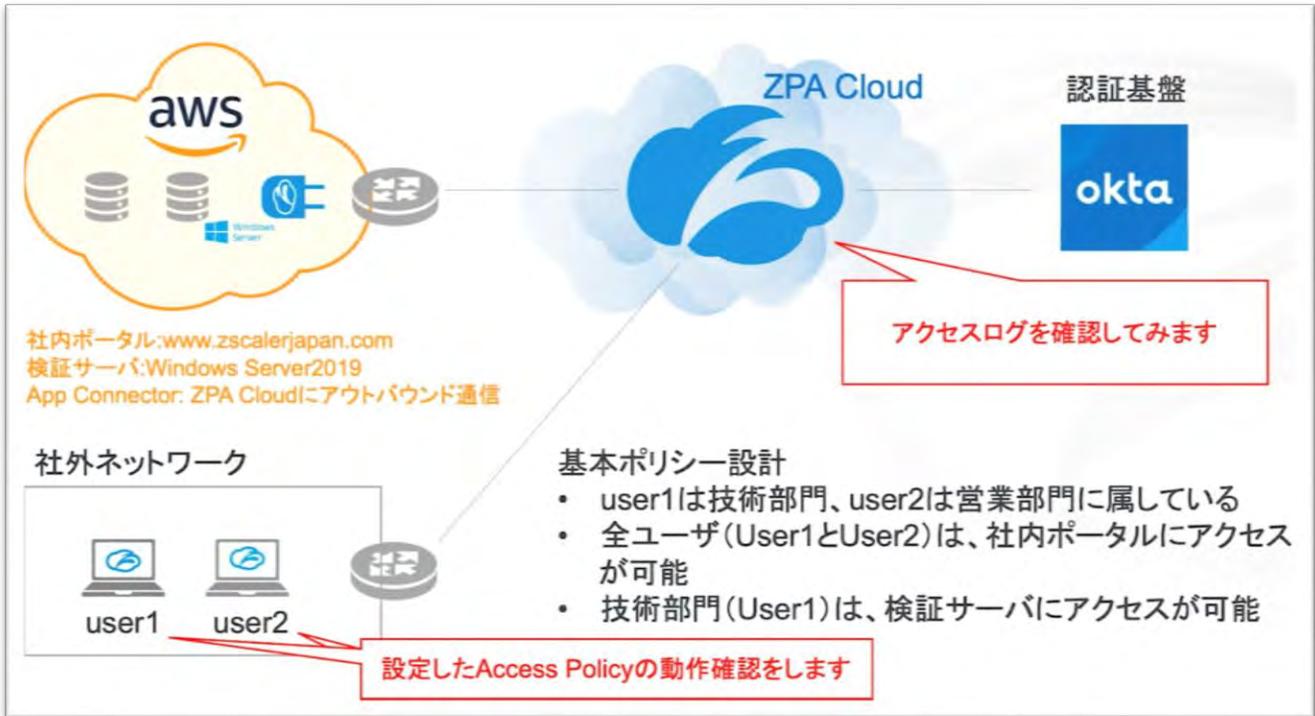
Authenticated Status が Authenticated となっていることを確認します。



Enrolled Devices から、user1 が Enroll されていることが確認できます。



4. 動作確認



4-1.社内リソースへのアクセス

Step1. user1 でのアクセス

社内ポータルサイトに http と https でアクセスすると、定義した社内 Application のページが表示されます。

http の場合

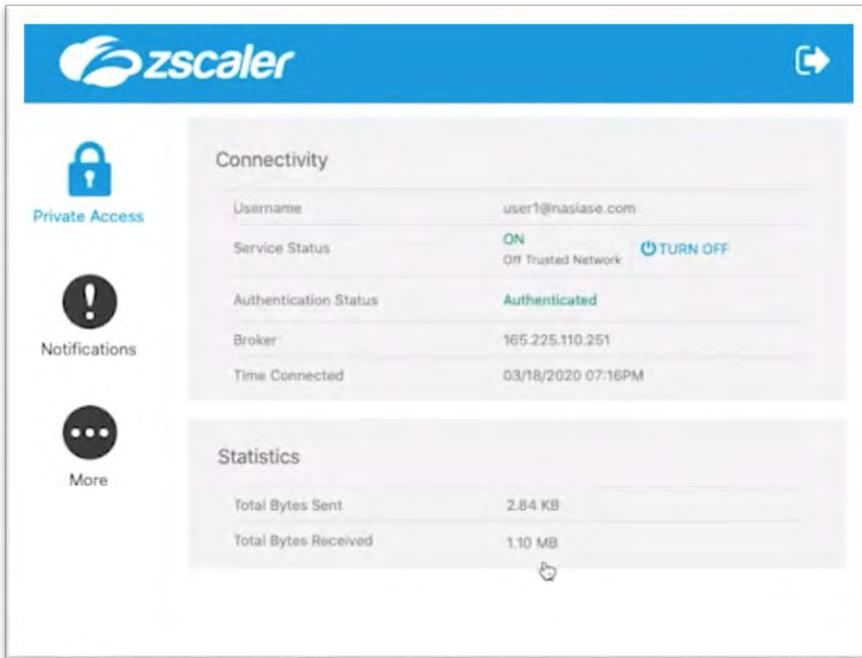


https の場合

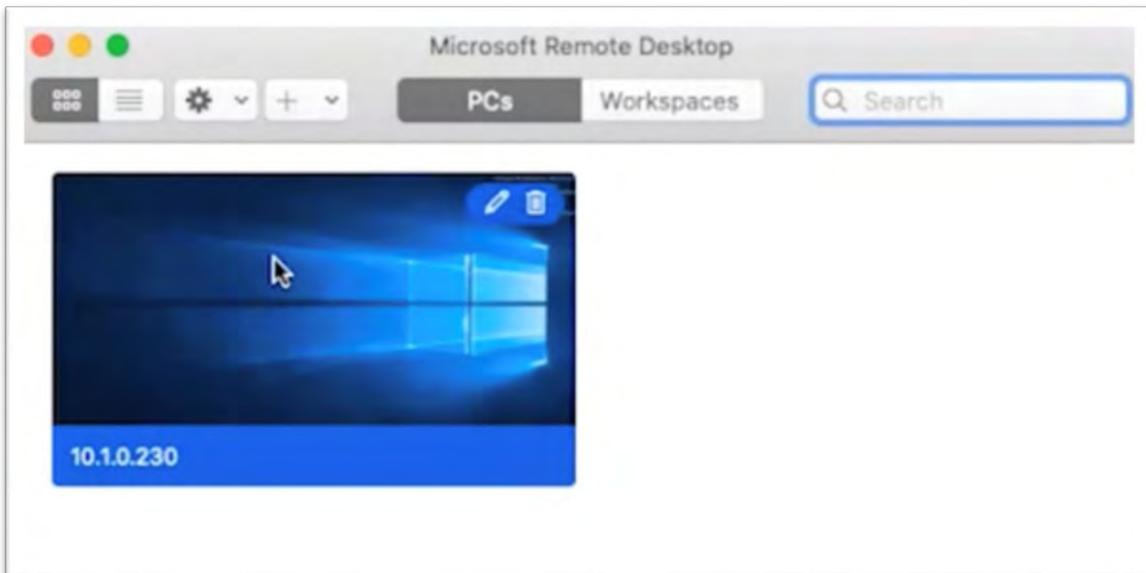


はじめての ZPA

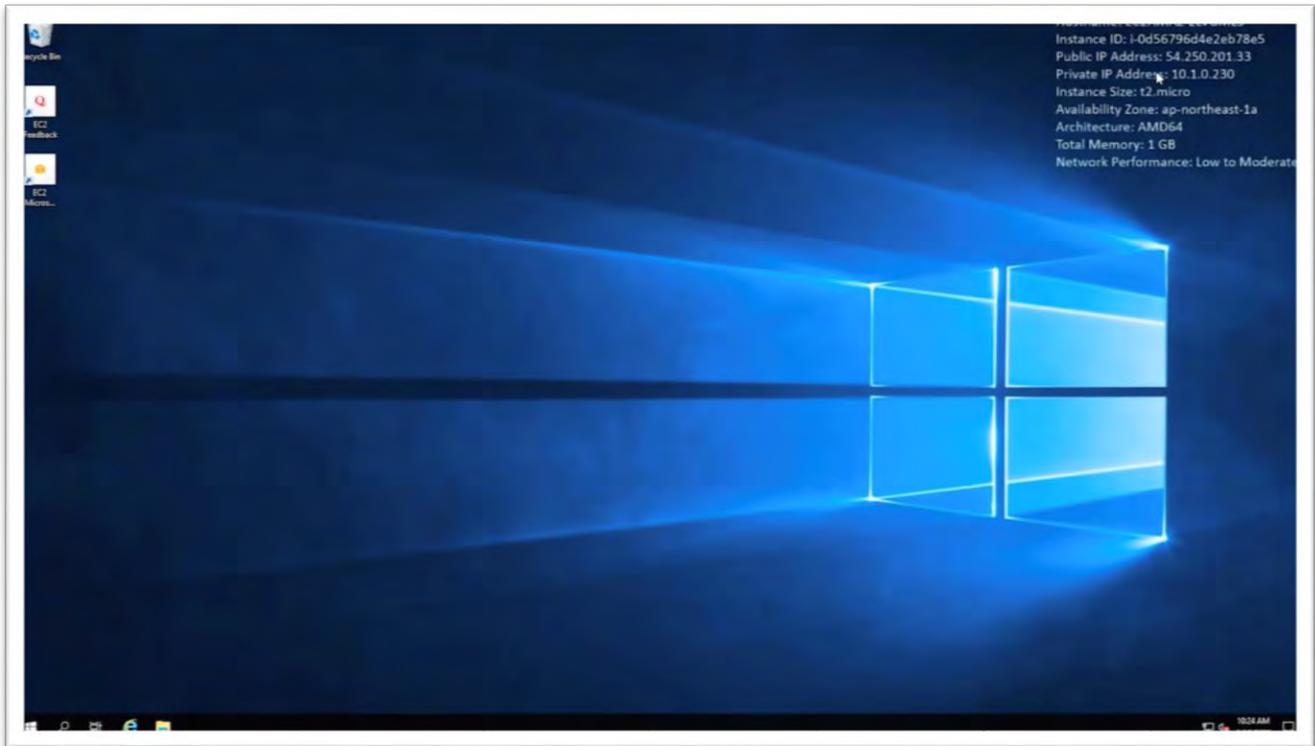
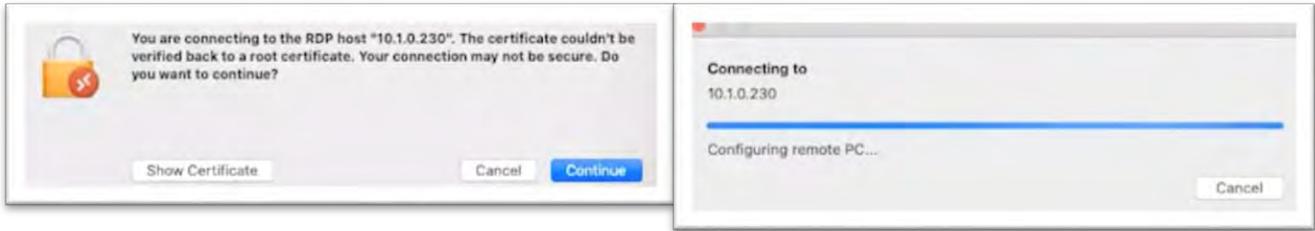
Zscaler App からバイトの送受信数がカウントアップしていることも確認できます。



社内サーバへの RDP アクセスも成功します。

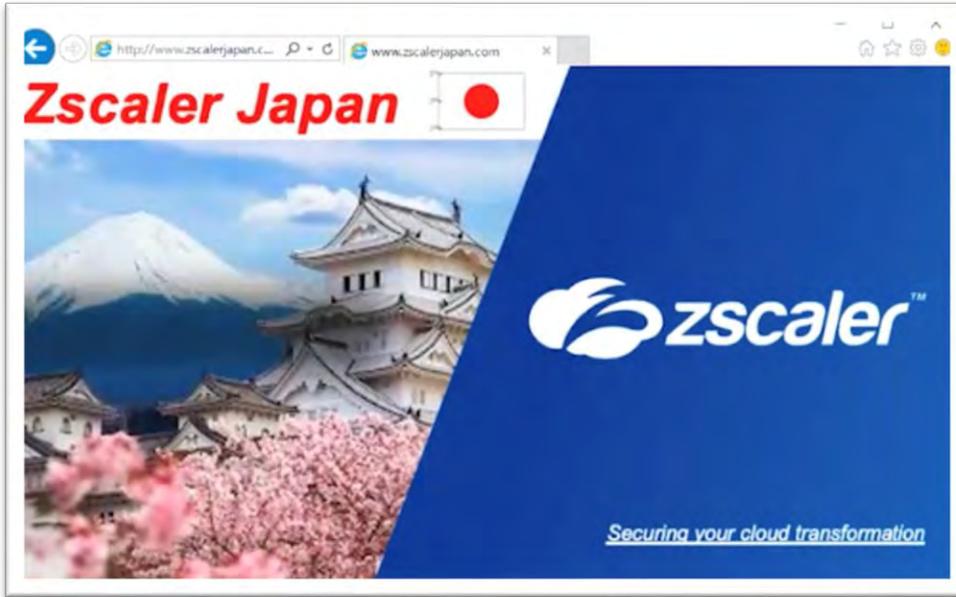


はじめての ZPA

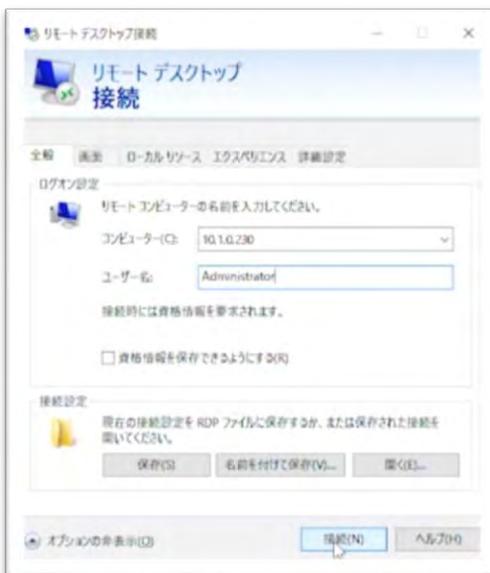


Step2. user2 でのアクセス

user1 と同様に user2 でも社内ポータルサイトにアクセスをしてみます。
問題なくページが表示されます。

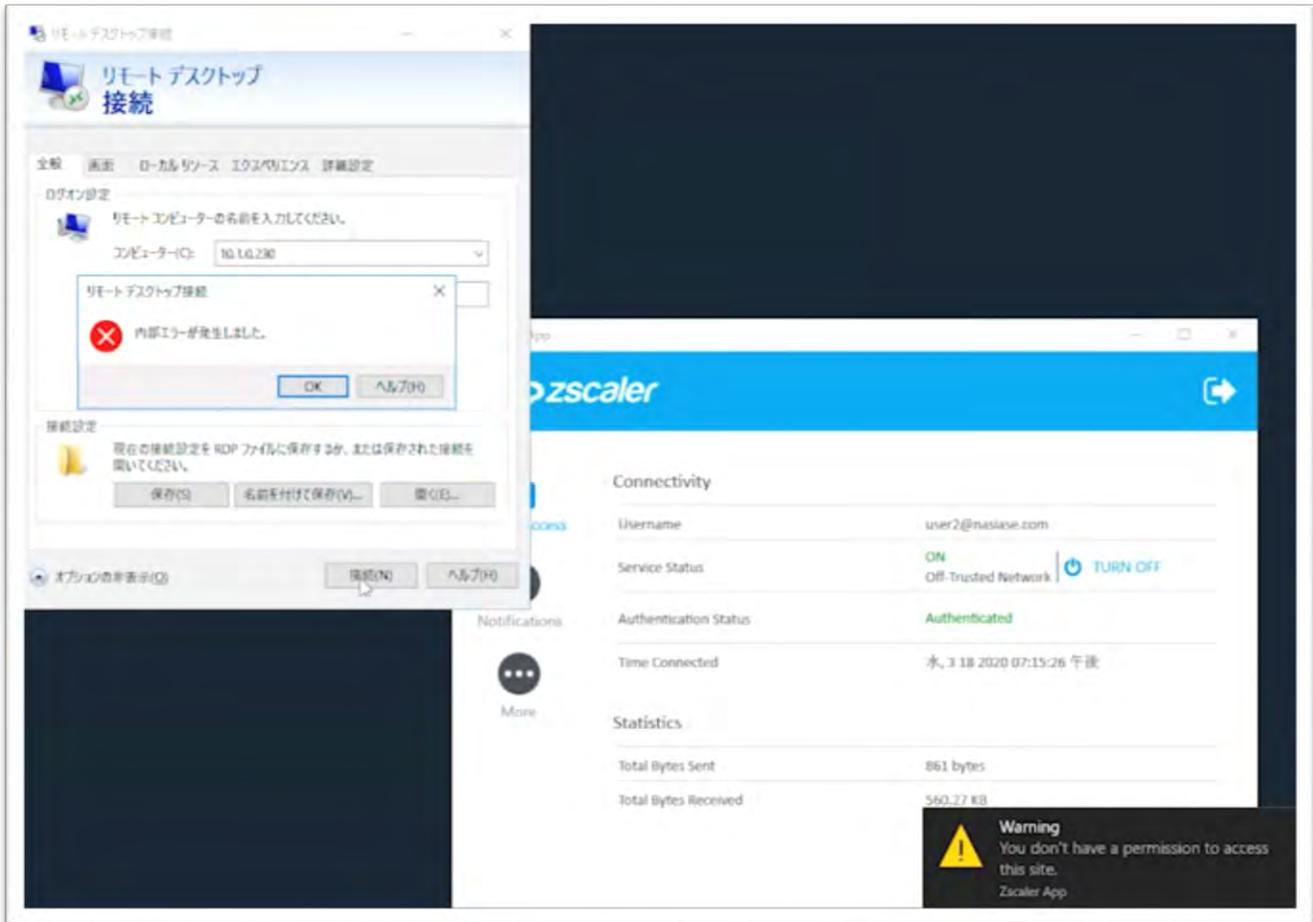


しかし、社内サーバへの RDP アクセスはポリシーに基づき失敗します。



はじめての ZPA

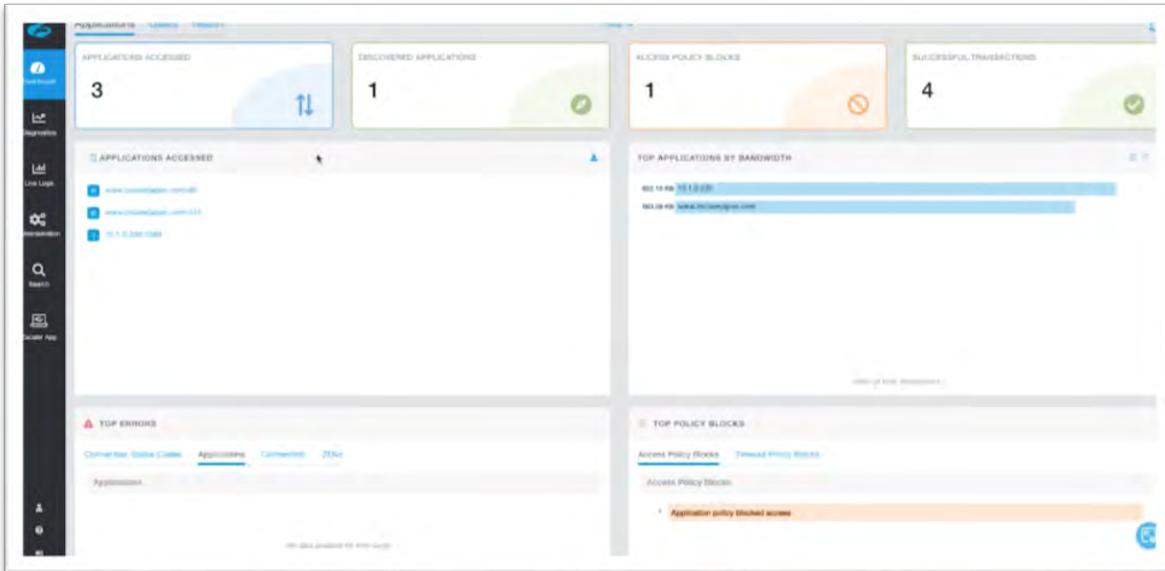
設定した警告メッセージも表示されます。



4-2. ログの確認

Step1. 統計情報の確認

Dashboard -> Application より、アプリケーションの統計情報が確認できます。



Step 2. ログの詳細確認

Dashboard -> Diagnostics より、各アクセス毎のログが確認できます。

The screenshot shows the ZPA Diagnostics log view. It includes a summary of log statistics and a detailed table of log entries.

Log Summary:

- TOTAL: 17
- ERRORS: 0
- ACCESS POLICY BLOCKS: 3
- TIMEDOUT POLICY BLOCKS: 0
- SUCCESSFUL: 12
- INFO: 2

Log Table:

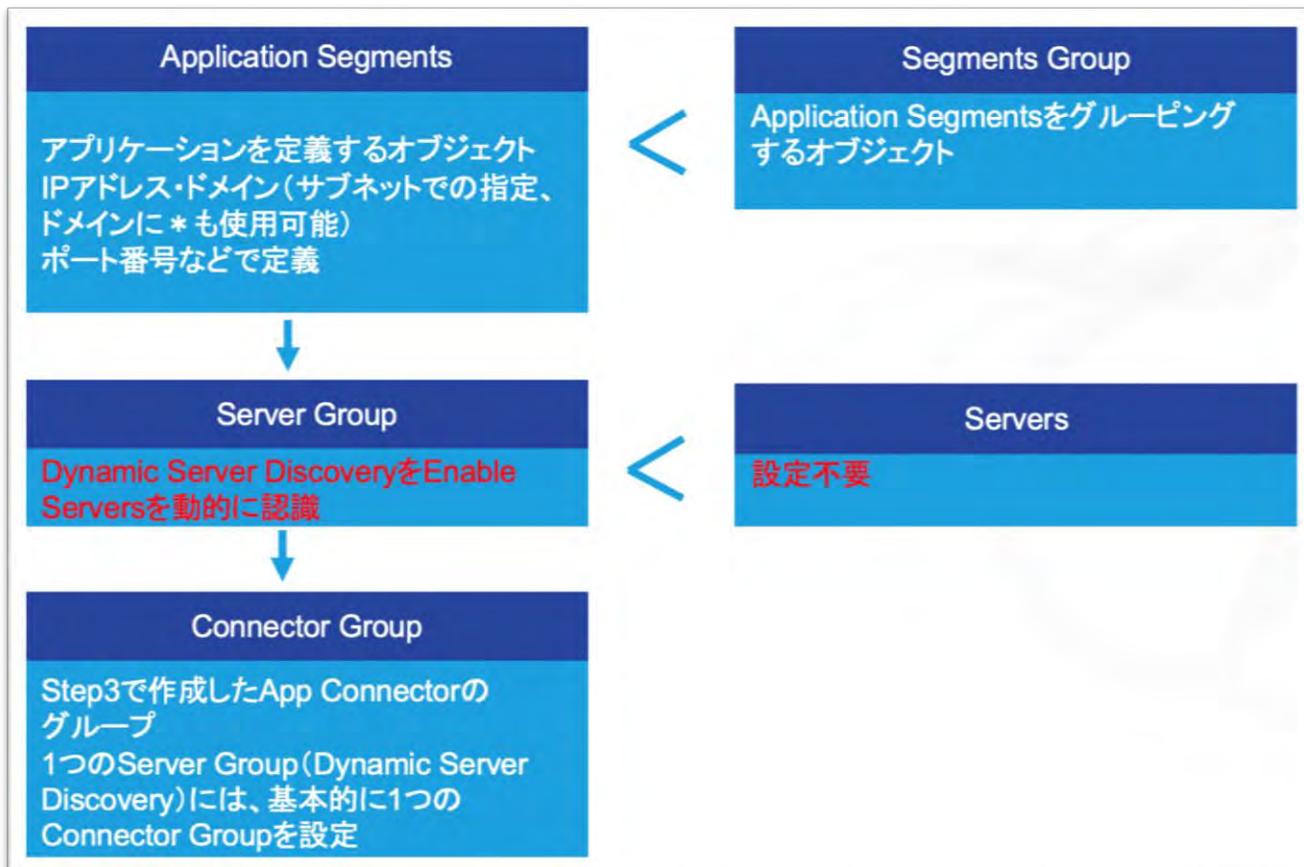
Connection	UTC	Policy	User	ZEN	Connector	Application
Mar 18, 19:28:57.279 JST	...	Allow from server for sales (in)	user1@zscaler.com	AP-JP-4455	No connector can reach this application.	15.1.5.230.1088 TCP
Mar 18, 19:28:57.407 JST	...	Allow from web site and Tech (in)	user1@zscaler.com	AP-JP-4455	AW5 Stage 1	www.zscaler.com: 80 TCP
Mar 18, 19:28:57.438 JST	...	Allow from web site and Tech (in)	user2@zscaler.com	AP-JP-4455	AW5 Stage 1	www.zscaler.com: 80 TCP
Mar 18, 19:28:57.469 JST	...	Allow from web site and Tech (in)	user1@zscaler.com	AP-JP-4454	AW5 Stage 1	15.1.5.230.1088 TCP
Mar 18, 19:28:57.498 JST	...	Allow from web site and Tech (in)	user1@zscaler.com	AP-JP-4454	AW5 Stage 1	www.zscaler.com: 443 TCP
Mar 18, 19:28:57.528 JST	...	Allow from web site and Tech (in)	user1@zscaler.com	AP-JP-4454	AW5 Stage 1	www.zscaler.com: 443 TCP
Mar 18, 19:28:57.557 JST	...	Allow from web site and Tech (in)	user1@zscaler.com	AP-JP-4454	AW5 Stage 1	www.zscaler.com: 80 TCP
Mar 18, 19:28:57.587 JST	...	Allow from web site and Tech (in)	user1@zscaler.com	AP-JP-4454	AW5 Stage 1	www.zscaler.com: 80 TCP

はじめての ZPA

ドリルダウンをすることで、より詳細な情報が確認できます。

Connection	UTM Policy	User	ZEN	Connector	Application
START TIME Mar 18, 19:26:07.275 JST	ADDRESS POLICY NAME Deep Tech Server for Sales, Jst	USER/EMAIL user@thelocal.com	ZONE AP-JP-4402	NAME No connector can match this application	APPLICATIONS & PROTOCOLS 15.1.2.20:3389 TCP
END TIME Mar 18, 19:26:07.276 JST	ACTION Deny	IP 15.112.81.175	LOCATION Shinjuku City, JP	PORT & PROTOCOL Unavailable TCP	APPLICATION GROUP Tech Windows Service2019
STATUS CODE Application policy blocked access	POLICY ID Z0N9A82R7M5274	LOCATION Tokyo, JP	POLICY PROTECTION 0 ms	LOCATION Unavailable	SUBKEY IP/PORT & PROTOCOLS Unavailable:3389 TCP
INTERNAL SOURCE CODE SWK_MF_SETUP_FAIL_REJECT...		CLIENT TYPE Zscaler App	IP/PORT/CLIENT 0/0/0	CONNECTOR ID Unavailable	APPLICATION ID Z0N9A82R7M5274
STATUS Closed Connection		USER AGENT Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0	75 TO CONNECTION 0/0	CONNECTOR APP ACT 0 ms	CONNECTOR ID Unavailable
DURATION 0ms			90 FROM CONNECTION 0/0	CONNECTOR GROUP NAME Unavailable	CONNECTOR ID Unavailable
TOTAL BYTES 0 B			75 TO CLIENT 0/0	CONNECTOR GROUP ID Unavailable	GROUP DESCRIPTION Default
CONNECTION ID D0y1fM6u0aKX7Lp-M9uJal...					
CONNECTION STATUS LINK [Refresh] [Close]					
▶ Mar 18, 19:26:53.807 JST	Allow intra web site and Tech S...	user@thelocal.com	AP-JP-4402	4402 Tokyo-1	www.zscaler.com:443 TCP
▶ Mar 18, 19:26:53.808 JST	Allow intra web site and Tech S...	user@thelocal.com	AP-JP-4402	4402 Tokyo-1	www.zscaler.com:443 TCP
▶ Mar 18, 19:27:10.624 JST	Allow intra web site and Tech S...	user@thelocal.com	AP-JP-4402	4402 Tokyo-1	15.1.2.20:3389 TCP
▶ Mar 18, 19:27:51.498 JST	Allow intra web site and Tech S...	user@thelocal.com	AP-JP-4402	4402 Tokyo-1	www.zscaler.com:443 TCP
▶ Mar 18, 19:27:51.498 JST	Allow intra web site and Tech S...	user@thelocal.com	AP-JP-4402	4402 Tokyo-1	www.zscaler.com:443 TCP

5. Dynamic Server Discovery について



「3-4. Application Segmentation / Access Policyの設定」の

「Step 1 . Servers / Server Groupsの作成」では、社内アプリケーションの定義にServersをstaticに設定しました。Dynamic Server Discoveryを使うことで、IPアドレスでの指定やFQDNに加え、IPアドレスをサブネットやドメインに*（ワイルドカード）も使用可能です。使用可能な場合、アプリケーションの定義にDynamic Server Discoveryを使用してください。

Notes

- ✓ 使用可能な場合、アプリケーションの定義には Dynamic Server Discovery を使用
- ✓ 基本的には 1 つの Server Group (Dynamic Server Discovery) には 1 つの Connector Group を設定
- ✓ 基本的には 1 つの DC (社内 DC、AWS Tokyo、AWS Korea など) に対しては、1 つの Server Group を設定

Step1. Dynamic Server Discovery の設定

Server Group のオブジェクトを作成する際、Dynamic Server Discovery を On に設定し、[Save]をクリックします。

The screenshot shows the 'Edit Server Group' dialog box with the following details:

- Title:** Edit Server Group
- Name:** All Application in AWS Tokyo
- Description:** (Empty text area)
- Status:** Enabled (checked)
- Dynamic Server Discovery:** On (checked)
- Connector Groups:** AWS Tokyo
- Buttons:** Save, Cancel

はじめての ZPA

必要に応じて、他 DC 用の Connector group を追加します。

The screenshot shows a dialog box titled "Add Server Group". It contains the following fields and controls:

- Name:** All Application in AWS Korea
- Description:** (Empty text area)
- Status:** Enabled (selected), Disabled
- Dynamic Server Discovery:** On (selected), Off
- Connector Groups:** AWS Korea (selected)
- Buttons:** Save, Cancel

Application Segment を作成する際に、APPLICATIONS を*（ワイルドカード）を使って「*.zscalerjapan.com」、サブネットを使用して「10.1.0.0/24」と設定します。

これにより社内アプリケーションを1つずつ定義せずに、「*.zscalerjapan.com」にマッチする「www.zscalerjapan.com」や「drive.zscalerjapan.com」などの80番/443番ポート、10.1.0.0/24セグメントの3389番ポートに対する社内アプリケーションの定義が完了します。

はじめての ZPA

Edit Application Segment ✕

GENERAL INFORMATION

Name
zscalerjapan

Status
 Enabled Disabled

Description

APPLICATIONS

*.zscalerjapan.com Browser Access

[+ Add More](#)

ZSCALER APP ACCESS

TCP Port Ranges

<input type="text" value="80"/>	<input type="text" value="80"/>
<input type="text" value="443"/>	<input type="text" value="443"/>

[+ Add More](#)

UDP Port Ranges

<input type="text" value="From..."/>	<input type="text" value="To..."/>
--------------------------------------	------------------------------------

[+ Add More](#)

ADDITIONAL CONFIGURATION

Double Encryption
 Enabled Disabled

Bypass
Use Client Forwarding Policy

COMMON CONFIGURATION

Health Reporting
 Continuous On Access

Health Check
 Default None

Server Groups
 All Intra Web Site

Segment Group
Zscaler

[Save](#) [Cancel](#)

はじめての ZPA

Edit Application Segment ✕

Name
Tech Windows Server2019

Status
 Enabled Disabled

Description

APPLICATIONS

10.1.0.0/24 Browser Access

[+ Add More](#)

ZSCALER APP ACCESS

TCP Port Ranges

3389 3389 [+ Add More](#)

UDP Port Ranges

From... To... [+ Add More](#)

ADDITIONAL CONFIGURATION

Double Encryption
 Enabled Disabled

Bypass
Use Client Forwarding Policy

COMMON CONFIGURATION

Health Reporting
 Continuous On Access

Health Check
 Default None

Server Groups
 All Application in AWS Tokyo

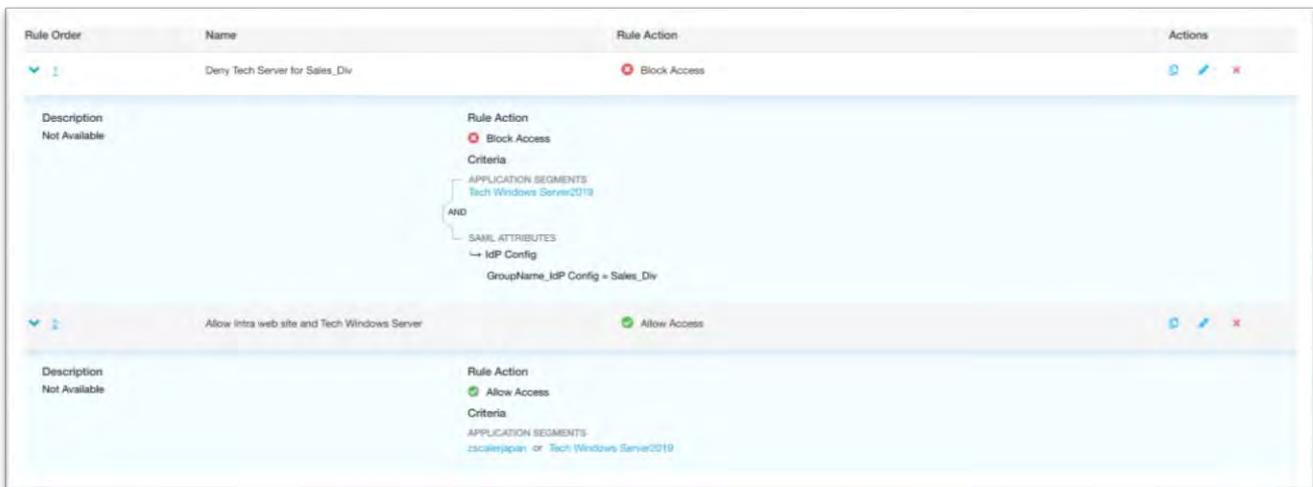
Segment Group
Tech Windows Server

[Save](#) [Cancel](#)

Step2. Access Policy の設定

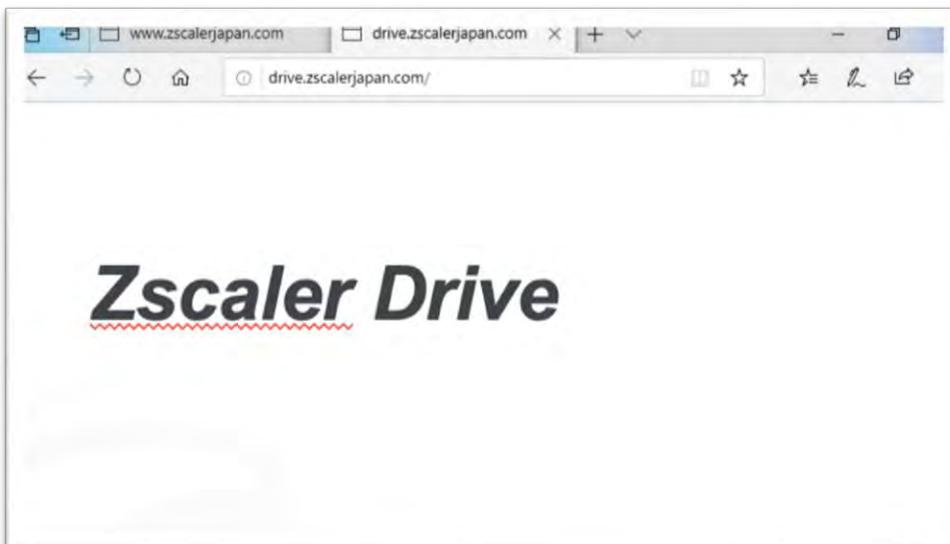
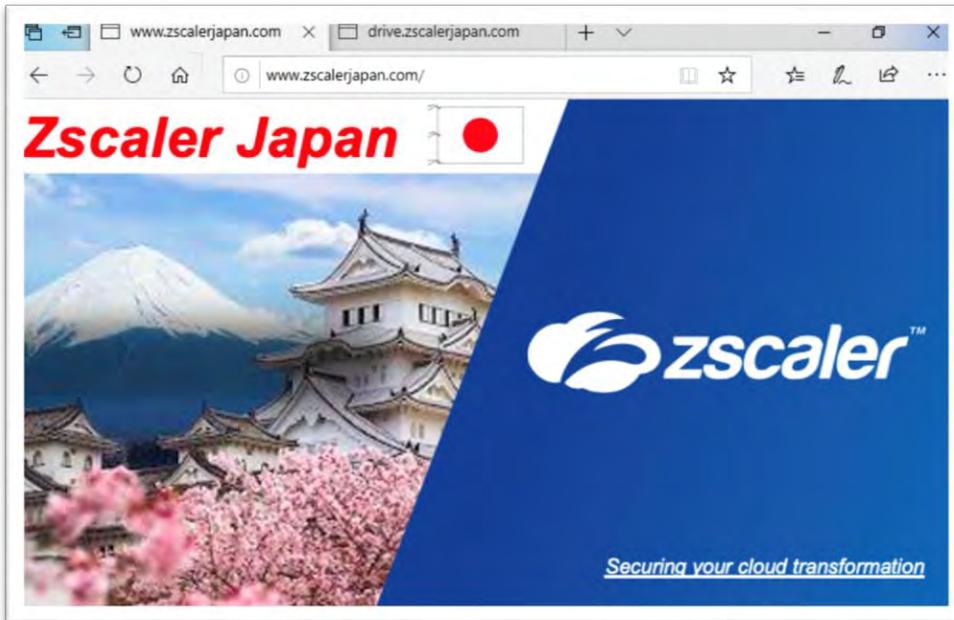
Application Segments に Step1 で作成したオブジェクトを設定します。

※営業部門は、社内サーバにアクセス禁止



Step3. 動作確認

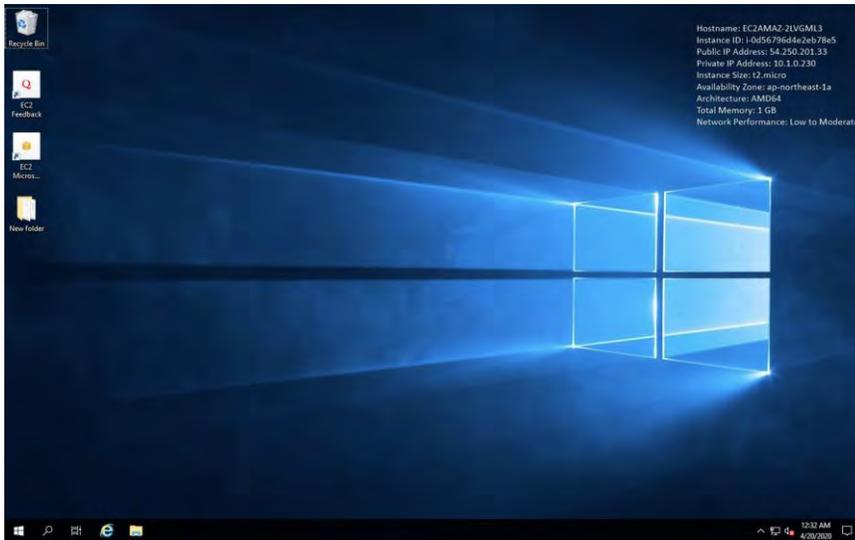
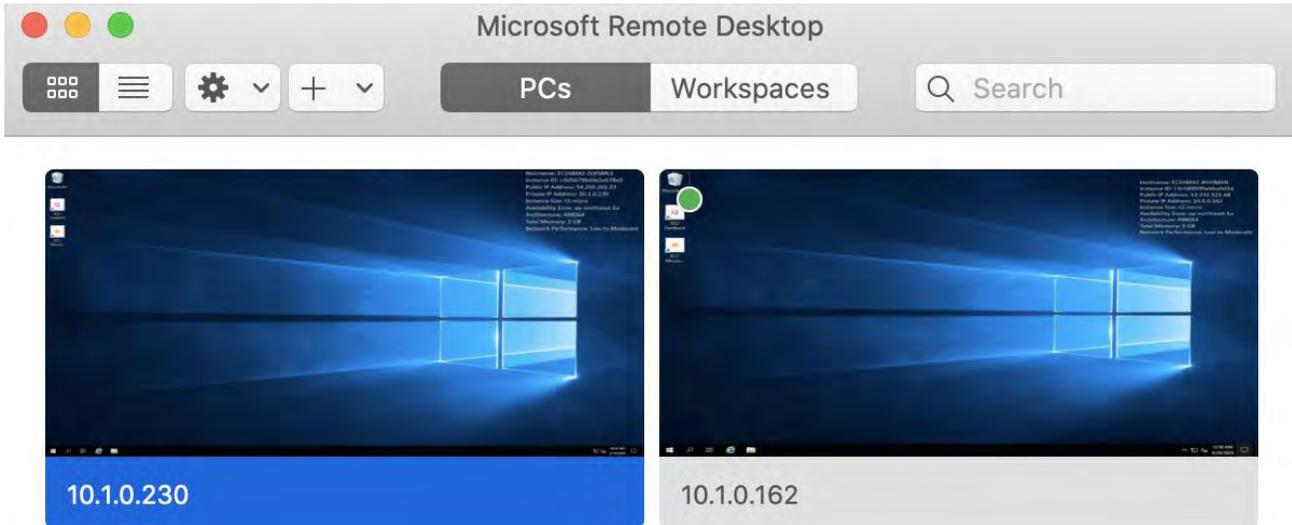
「www.zscalerjapan.com」と「drive.zscalerjapan.com」へアクセスを実施します。
「*.zscalerjapan.com」にマッチするため、ページが表示されます。



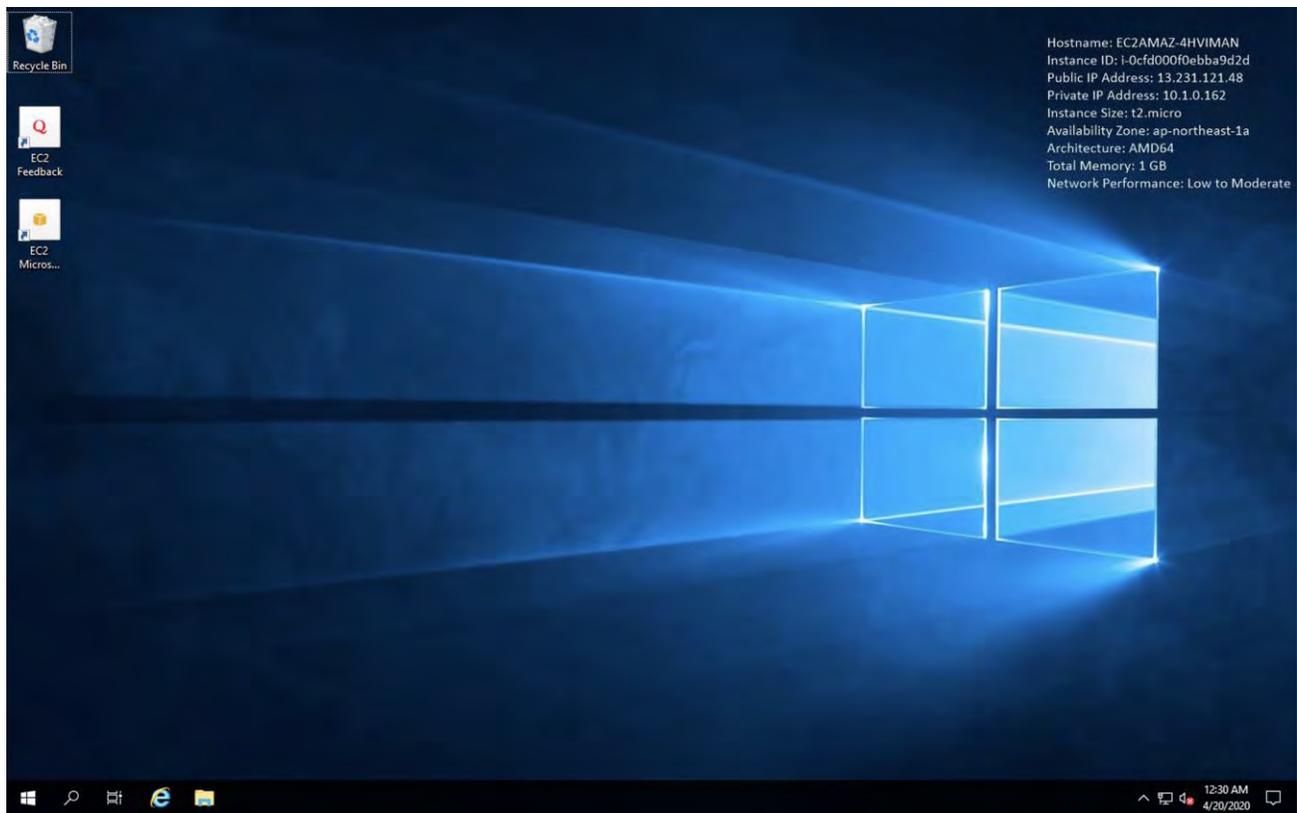
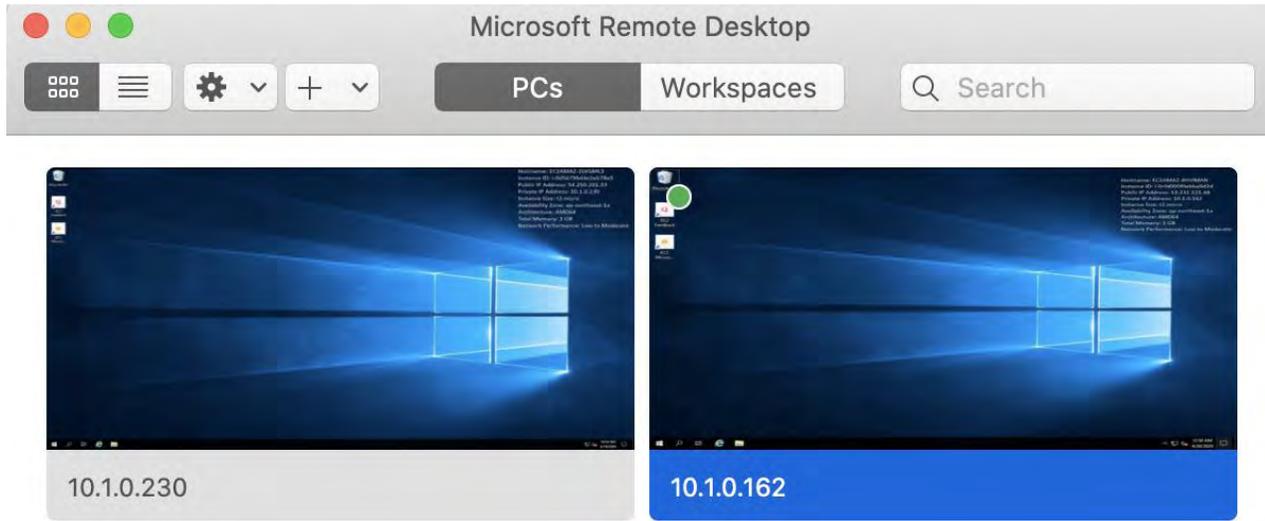
はじめての ZPA

「10.1.0.230」と「10.1.0.162」に RDP でアクセスを実施します。

「10.1.0.0/24」のサブネットにマッチするため、RDP が成功されます。

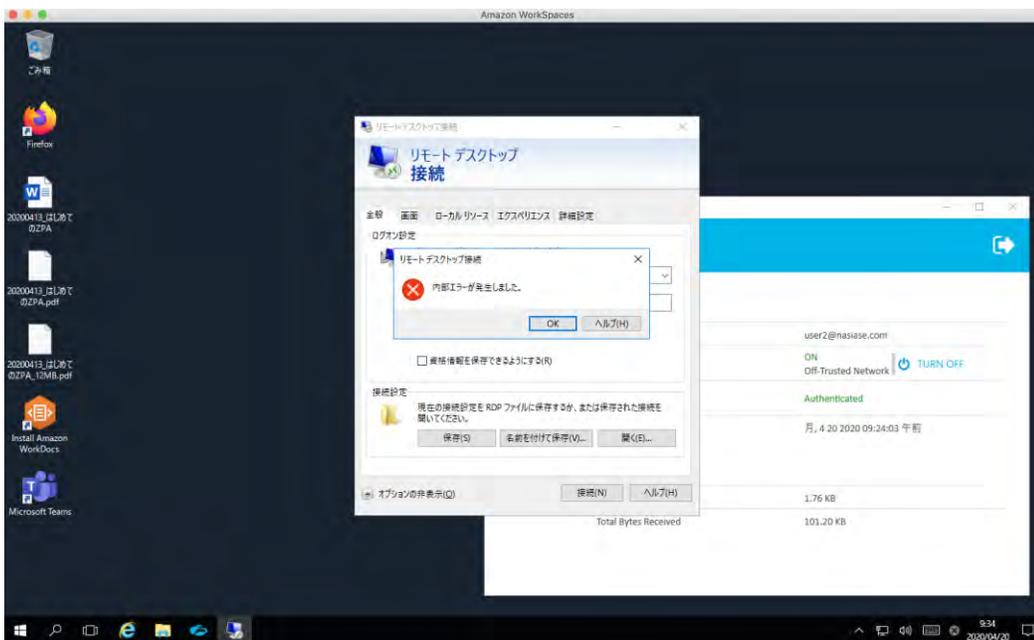
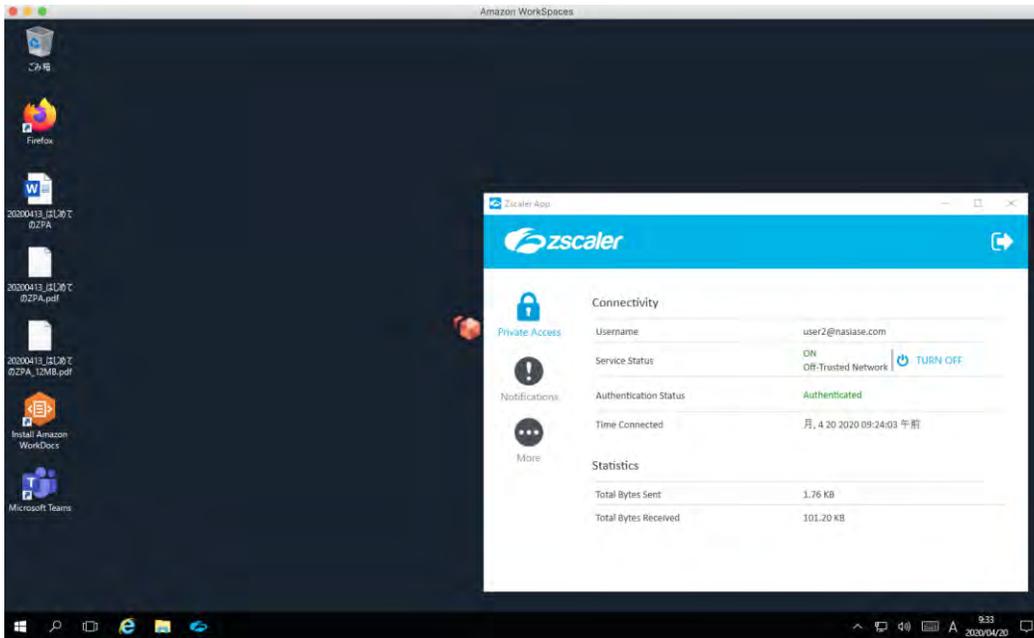


はじめての ZPA



はじめての ZPA

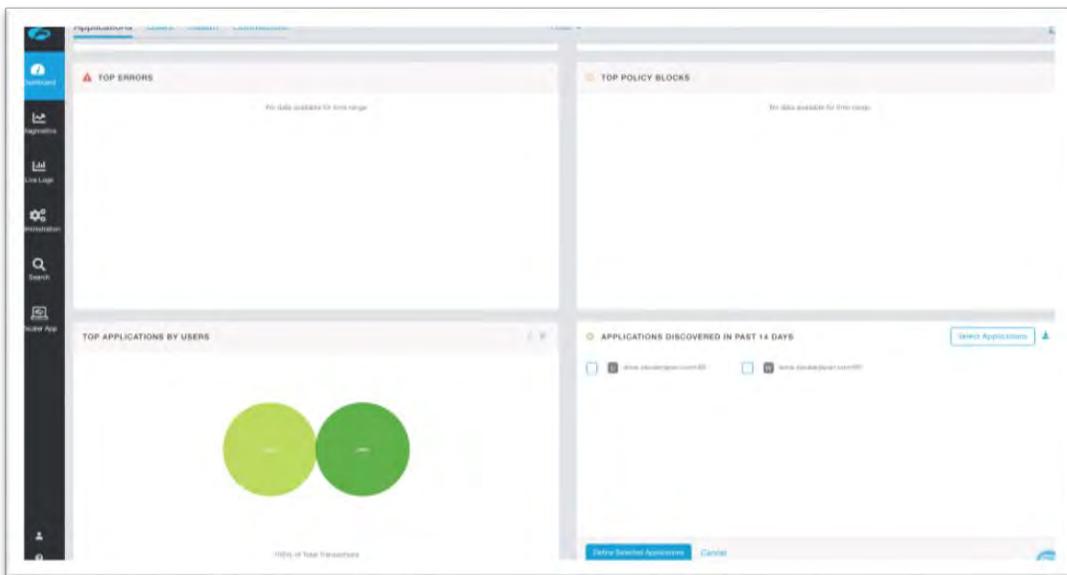
user2（営業部門）で RDP をすると、ポリシーに基づきアクセスが失敗します。



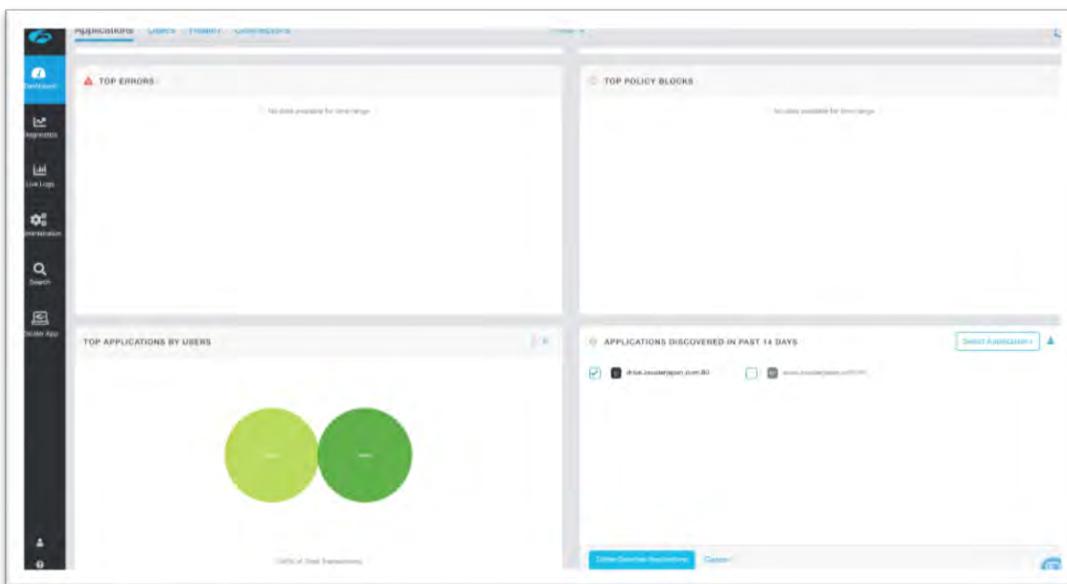
Dynamic Server Discovery を使用した場合でも、想定通りのポリシーで動作していることが確認できます。

Step3. アプリケーションの可視化

Dashboard -> Applications の APPLICATIONS DISCOVERED IN PAST 14 DAYS に * (ワイルドカード) や指定したサブネットにマッチするアプリケーションが表示されますので、どのようなアプリケーションが使用されているのか可視化することが可能です。



[Define Selected Applications]をクリックすることで、個別にアプリケーションを定義し、より柔軟にポリシーを作成することも可能です。



はじめての ZPA

Add Application Segment ✕

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

GENERAL INFORMATION

Name Status Enabled Disabled

Description

APPLICATIONS

Browser Access Add More

ZSCALER APP ACCESS

TCP Port Ranges

Add More

HTTP Port Ranges

Add More

Next Previous Cancel

6. その他の設定

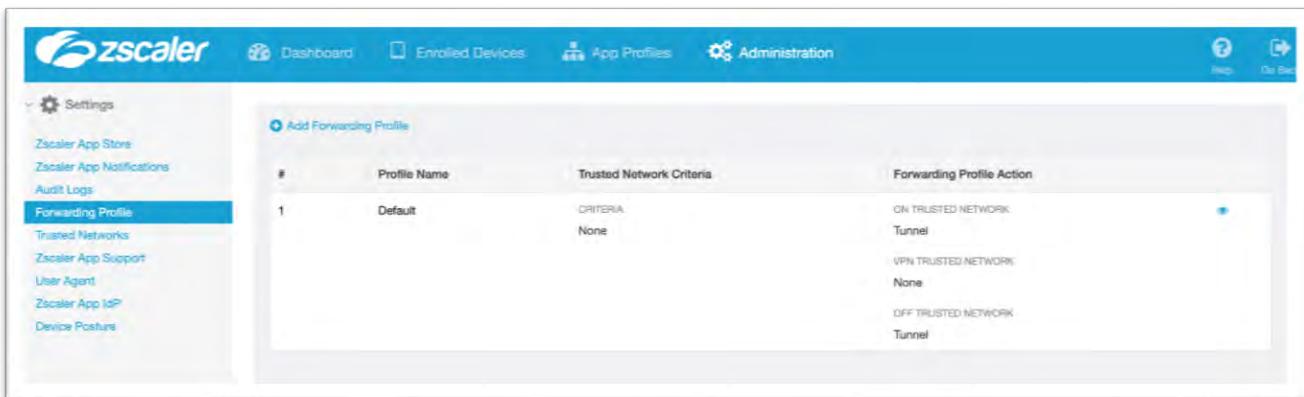
5-1. Forwarding Profile, App Profile の設定

Forwarding Profile について

Forwarding Profile では、接続しているネットワークの種類に応じてアクション (Tunnel or None) を設定することが可能です。

例) Trust NW (社内 NW) に接続している場合にはアクションを Tunnel しない、社外 NW に接続している場合にはアクションを Tunnel する

Zscaler App Portal -> Administration -> Forwarding Profile より[Add Forwarding Profile]をクリックすることで作成が可能です。



必要事項を記入、設定し [Save] をクリックします。

+++++

Profile Name: 任意の名前

TRUSTED NETWORK CRITERIA: 任意の設定 (※1)

FORWARDING PROFILE FOR ZPA: 任意の設定 (※2)

+++++

はじめての ZPA

※1 下図では、DNS Server が 192.168.1.100 の場合

※2 On Trusted Network (TRUSTED NETWORK CRITERIA にマッチ)、Off Trusted Network (Trusted Network 以外) の Action を設定、VPN Trusted Network は、None を設定

Add Forwarding Profile

PROFILE DEFINITION

Profile Name [?]

Mac

TRUSTED NETWORK CRITERIA

Add Condition [?]

Select Add Condition

Condition Match

Any

DNS Servers [?]

192.168.1.100

WINDOWS DRIVER SELECTION

Tunnel Driver Type [?]

Route Based Packet Filter Based

FORWARDING PROFILE ACTION FOR ZPA

On Trusted Network

Tunnel None

VPN Trusted Network

Same as "On Trusted Network"

Tunnel None

Off Trusted Network

Same as "On Trusted Network"

Tunnel None

Save Cancel

App Profile について

App Profile では、各端末に対して主に以下の制御設定をすることができます。

- ユーザが ZPA のサービスを log out や disable にできないように強制
- Forwarding Profile 設定の紐付け

Zscaler App Portal -> Administration -> App Profile より[Add macOS Policy]をクリックすることで作成が可能です（左のサイドバーから OS を選択）。



必要事項を記入、設定し [Save] をクリックします。

+++++

Name: 任意の名前

Rule Order: ポリシー設計を考慮

Groups: 任意のグループ（※1）

Logout Password: 任意の文字列（※2）

Disable Password: 任意の文字列（※3）

Forwarding Profile: 紐づける Forwarding Profile

+++++

※1 ZIA（Zscaler Internet Access）で設定しているグループ名

※2 ユーザが Zscaler App をログアウトする際のパスワードを設定

※3 ユーザが Zscaler App の ZPA を disable にする際のパスワードを設定

Add macOS Policy ✕

DEFINE POLICY AND SCOPE

Name ?
Mac

GENERAL

Rule Order 2	Enable <input type="checkbox"/>
Groups ALL	Logout Password 👁
Disable Password 👁	Custom PAC URL ? Optional
Forwarding Profile Mac	Install Zscaler SSL Certificate <input type="checkbox"/>
Log Mode Debug	Log File Size in MB ? 100

HOSTNAME OR IP ADDRESS BYPASS FOR VPN GATEWAY ?

Use Enter to Add Multiple Hostnames or IP Addresses +

MACOS POLICY DESCRIPTION

Optional

Save Cancel

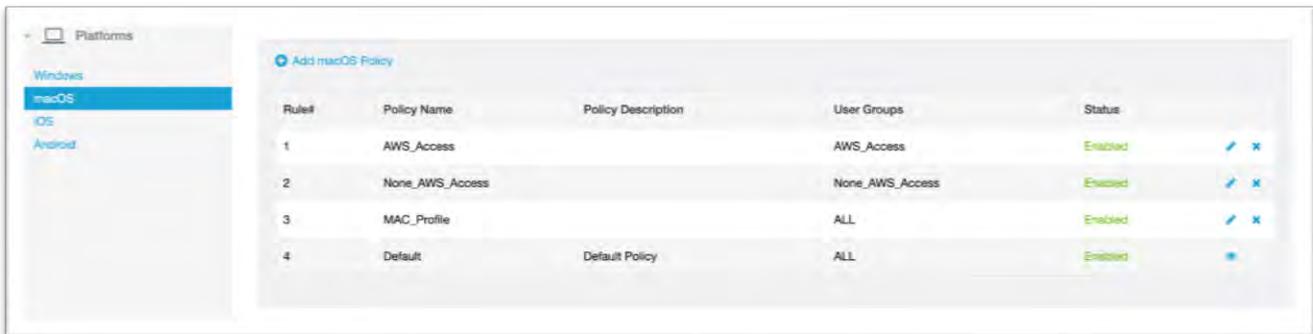
はじめての ZPA

App Profile のポリシーの精査は上から順に評価され、マッチした App Profile が適応されます。

その後のポリシーの評価はされません。

このため、各OSに対して想定した動作のためには、Group条件とポリシーの順番を考慮する必要があります。

例えば、下図では None_AWS_Access の Group に所属する macOS ユーザは、ポリシー 2 にヒットします。



Rule#	Policy Name	Policy Description	User Groups	Status
1	AWS_Access		AWS_Access	Enabled
2	None_AWS_Access		None_AWS_Access	Enabled
3	MAC_Profile		ALL	Enabled
4	Default	Default Policy	ALL	Enabled

5-2. Device Posture の設定

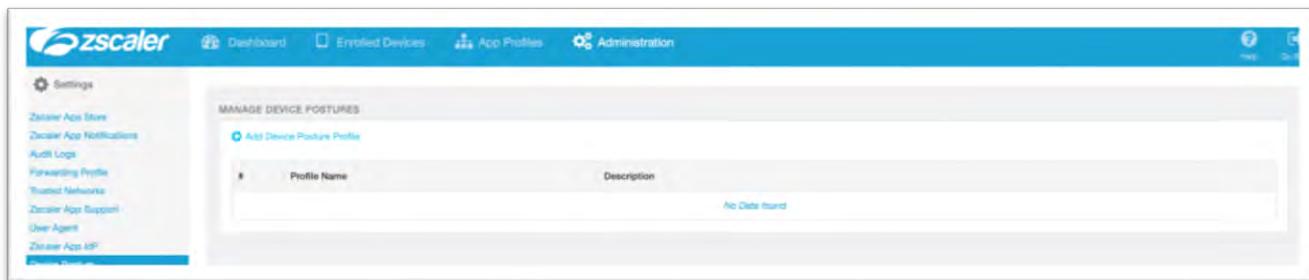
Device Posture は、Access Policy のマッチ条件に使用できる Criteria の一つです。使用できる Device Posture は OS によって異なりますが、例として以下のような Device Posture を作成できます。

- Certificate Trust
特定の CA 証明書を信頼しているかどうか
- File Path
特定の Path に特定のファイルが存在するかどうか
- Detect Carbon Black/CrowdStrike/SentinelOne
特定のエンドポイントセキュリティソフトがインストールされているかどうか

本章では、例として「Certificate Trust」の Device Posture を使用して、Access Policy を作成します。

Step1. Device Posture の作成

Administration -> Settings -> Device Posture より、[Add Device Posture Profile] をクリックします。



はじめての ZPA

必要事項を記入、設定し [Save] をクリックします。

+++++

Name: 任意の名前

PLATFORM: 任意の OS

Posture Type: Certificate Trust (環境に応じて適切な Posture を設定)

Certificate: [Upload]をクリックして、CA 証明書をアップロード

+++++

#	Profile Name	Description
1	Tech_Div	

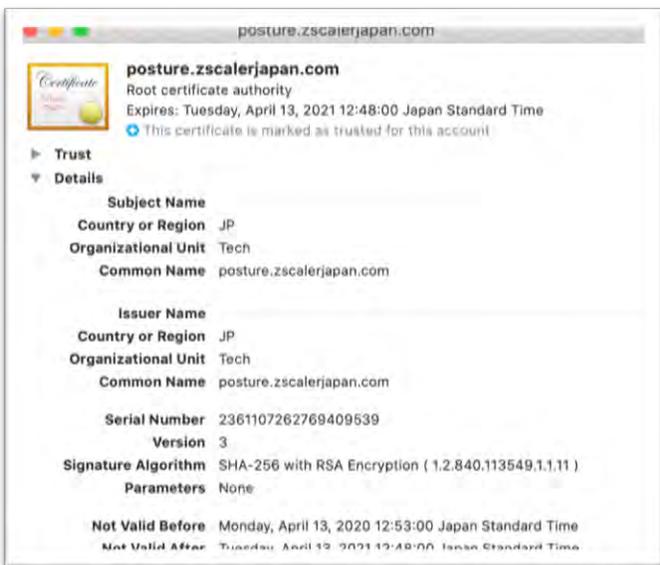
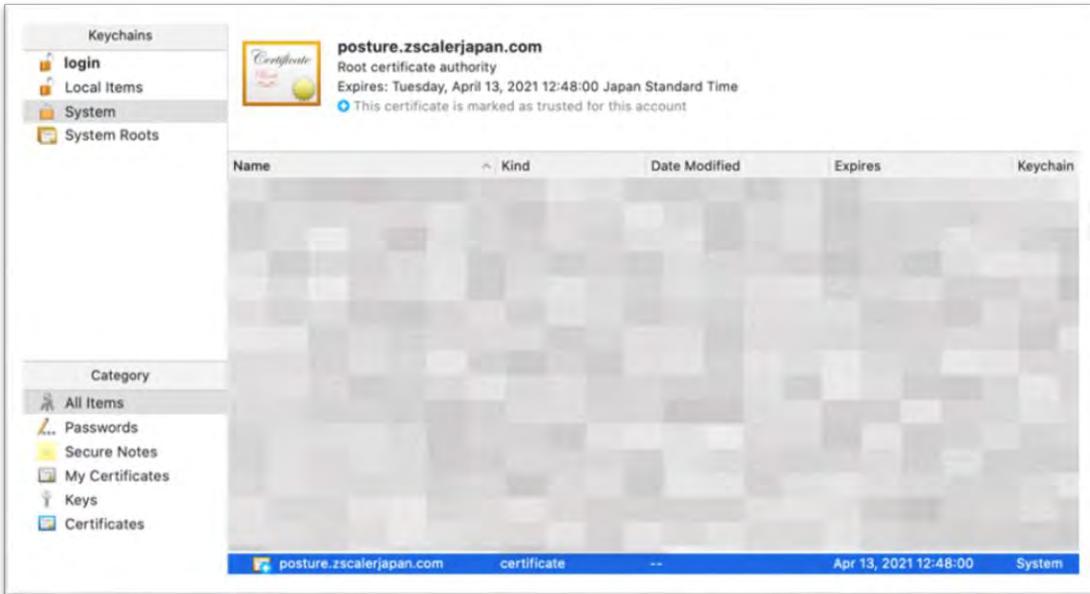
Step2. Access Policy の設定

Zscaler App Posture Profiles に、Step1 で作成した、Device Posture を選択し VERIFIED を設定します。

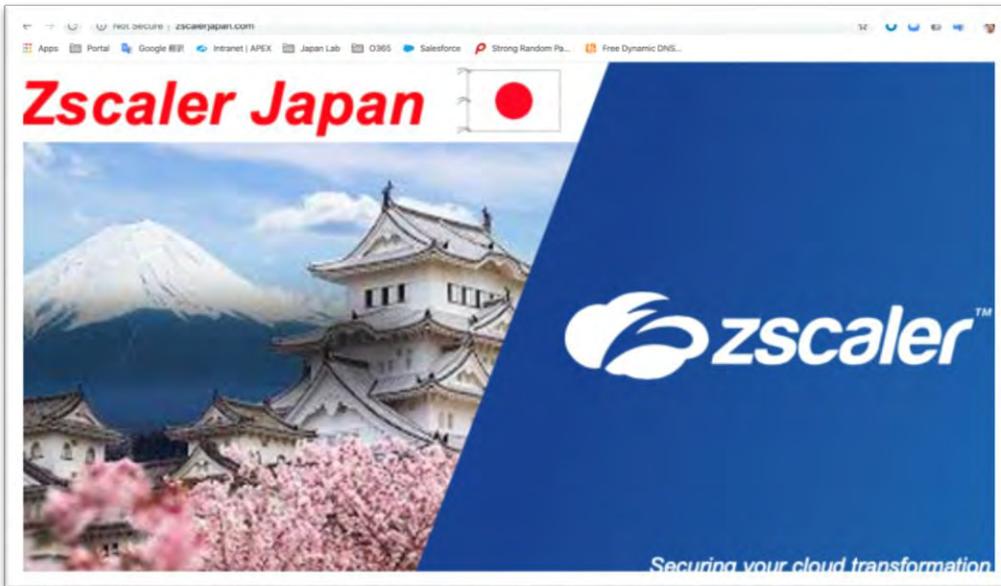
The screenshot shows the 'Edit Access Policy' configuration window. The 'ACTION' section is set to 'Allow Access'. The 'CRITERIA' section includes 'Application Segments' (zscalerjapan, Tech Windows Server2019), 'Segment Groups', 'SAML Attributes' (Any SAML attribute from any IdP), 'Client Types' (Any client type), 'Zscaler App Posture Profiles' (Tech_Div, VERIFIED), and 'Zscaler App Trusted Networks'. The 'Save' and 'Cancel' buttons are at the bottom.

Step3. 動作確認

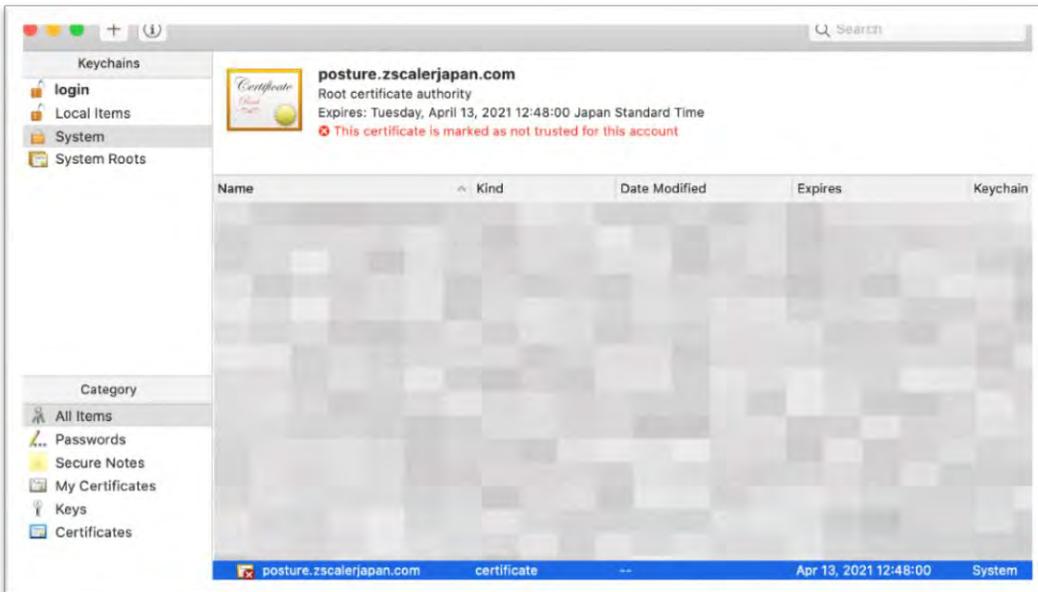
端末が Device Posture で設定した証明書を信頼している状態で、アクセスを実施します。



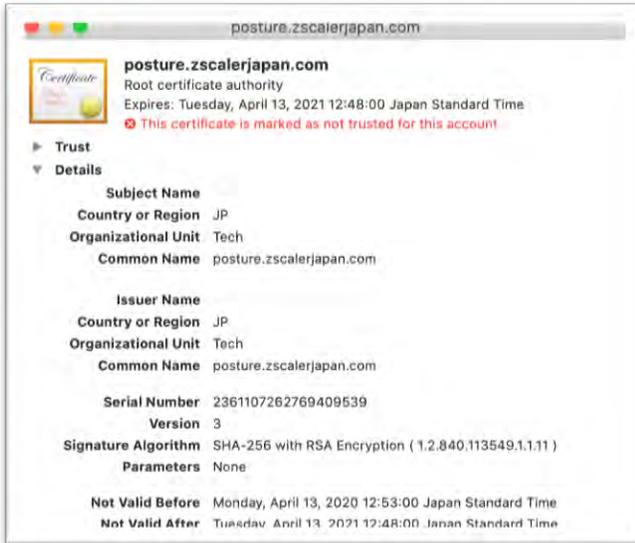
Access Policy の条件にマッチするのでアクセスが成功します。



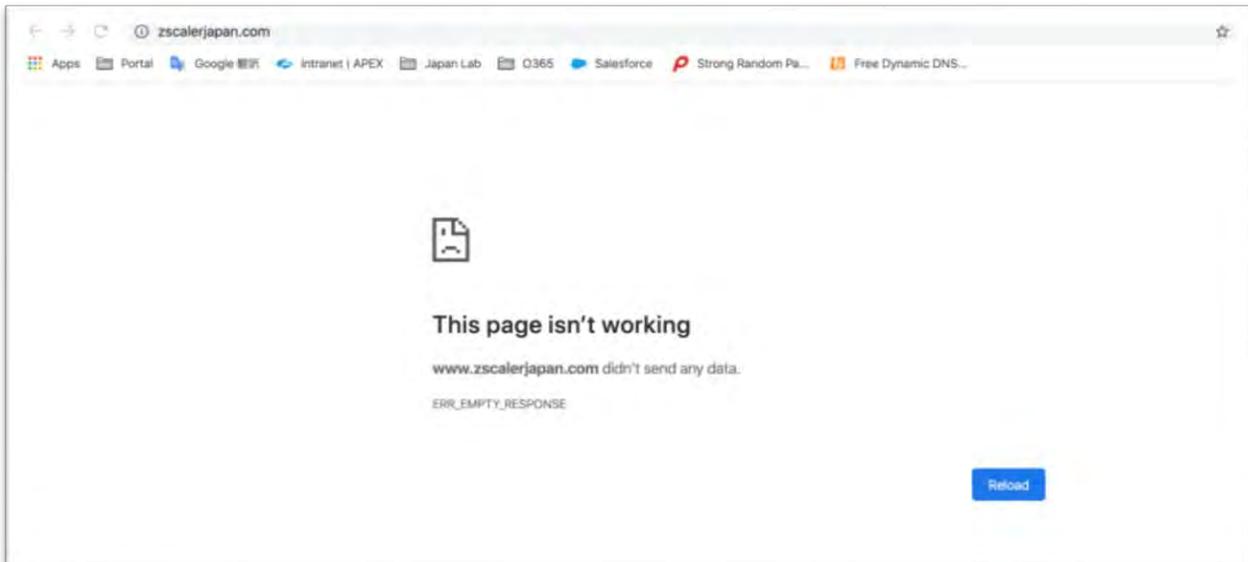
端末が Device Posture で設定した証明書を信頼していない状態で、アクセスを実施します。



はじめての ZPA



Access Policy の条件にマッチしないのでアクセスが失敗します。



以上