はじめての ZPA (Zscaler Private Access)

ゼットスケーラー 株式会社

ZSCALER CONFIDENTIAL INFORMATION

コンテンツー覧

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。

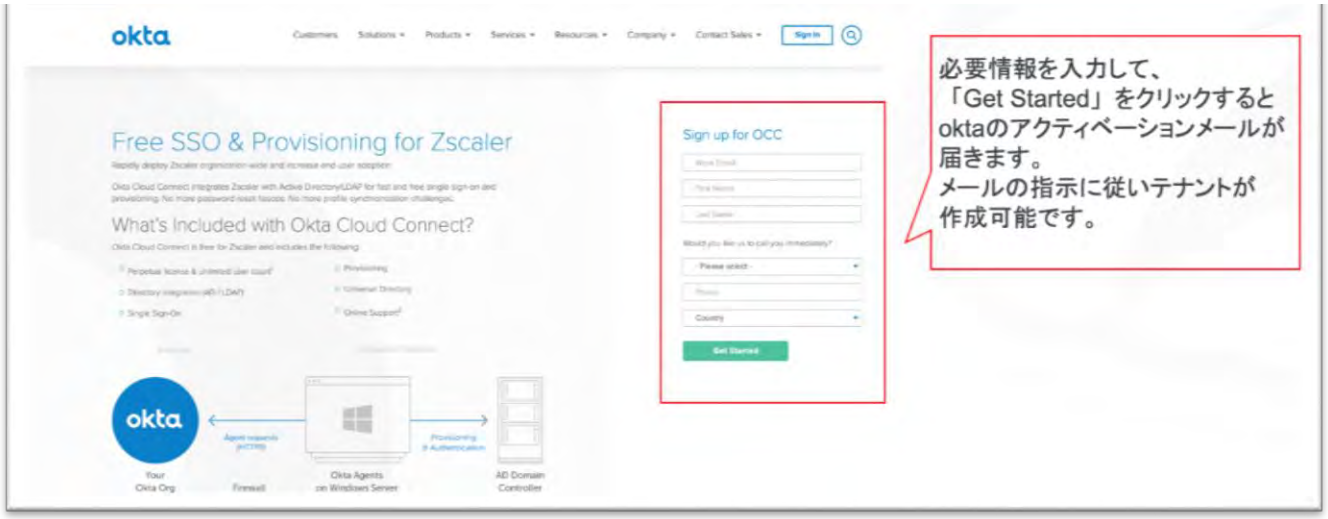
ZPA の導入をご検討の場合には、弊社担当や販売パートナー様にご連絡の上、お客様実環境での動作確認、検証を実施いただくことを強く推奨いたします。

2. 環境について

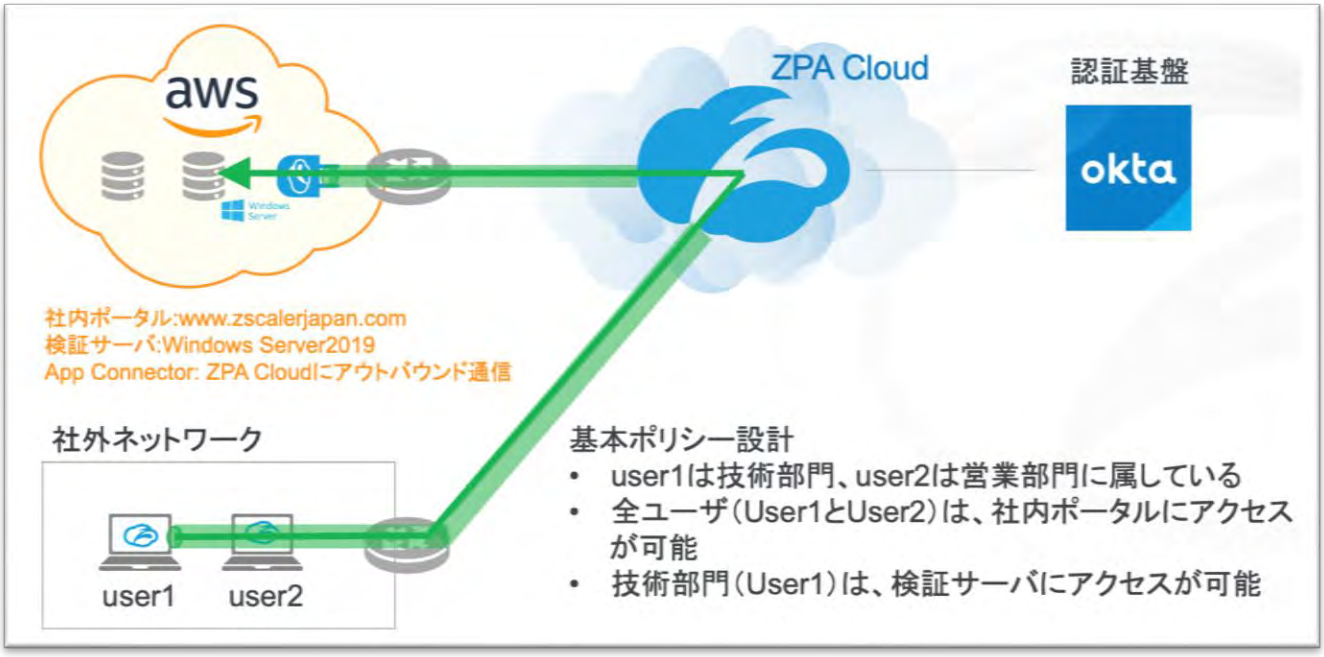
2-1. SAML 認証基板について

ZPA を使用するためには SAML 認証基盤（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 認証基盤として okta を使用します。
SAML 認証基盤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。



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

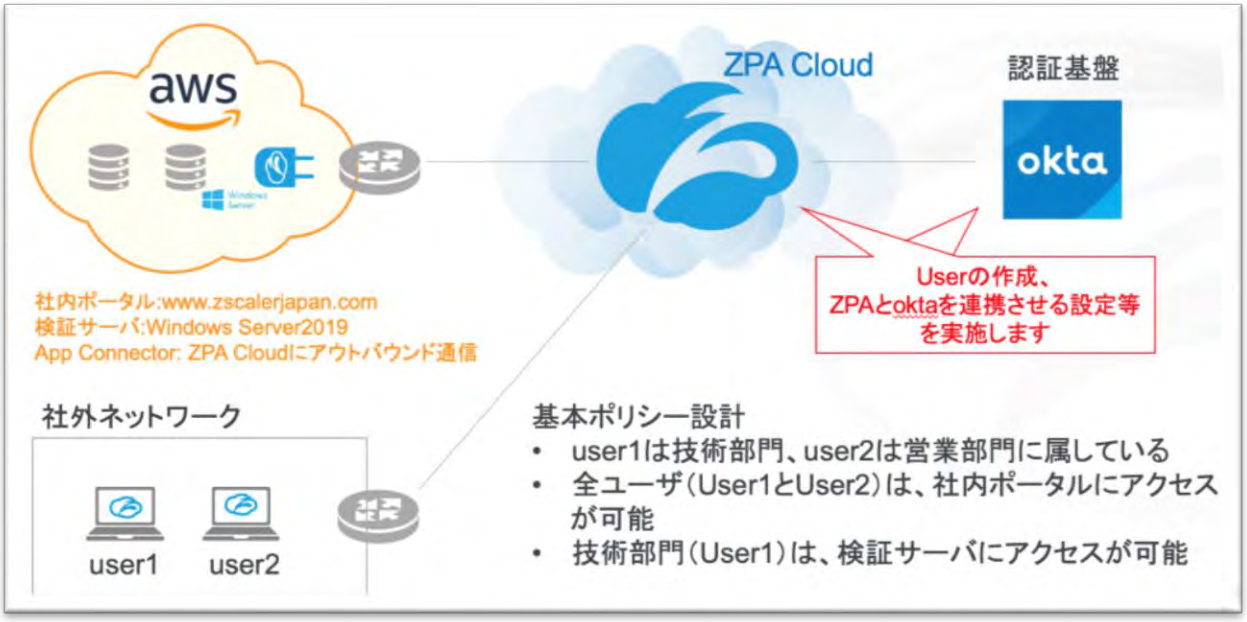
- SP（ZPA）と IdP（okta）の連携
- Zscaler App（user1 のみ）、Connector のインストール

- 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。

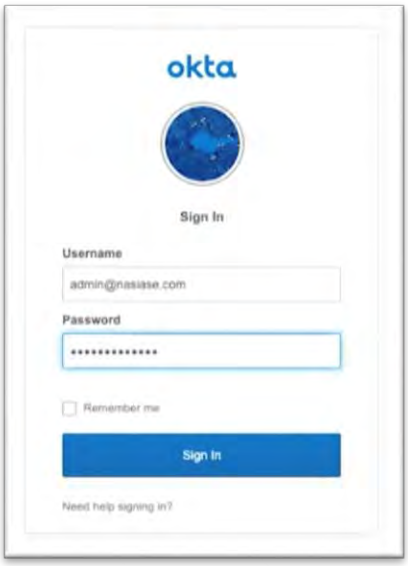
3. 基本設定

3-1. SP（ZPA）と IdP（okta）の SAML 認証連携設定

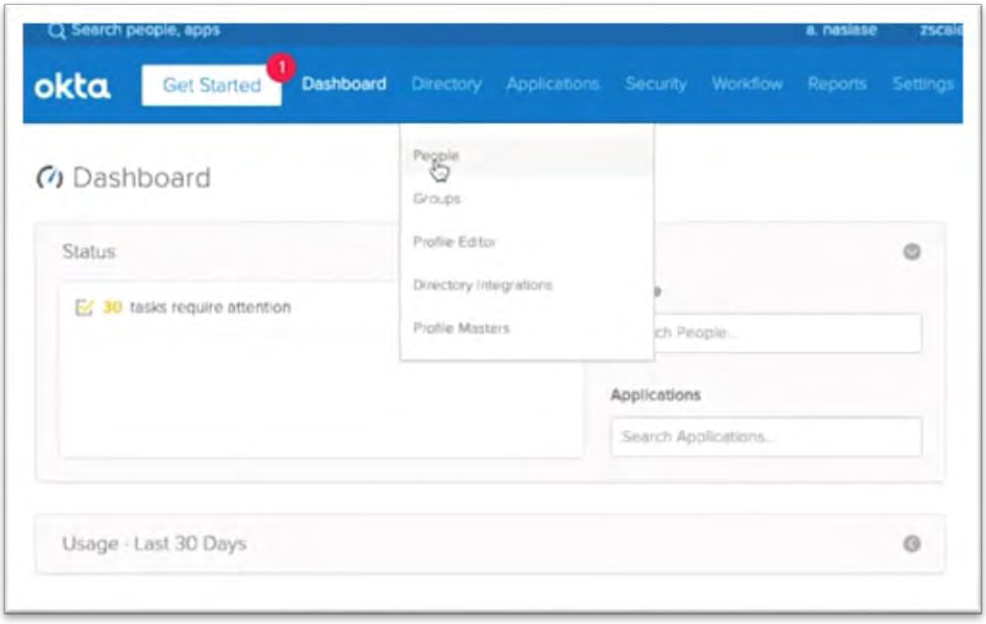


Step1. ユーザ（user1、user2）の作成

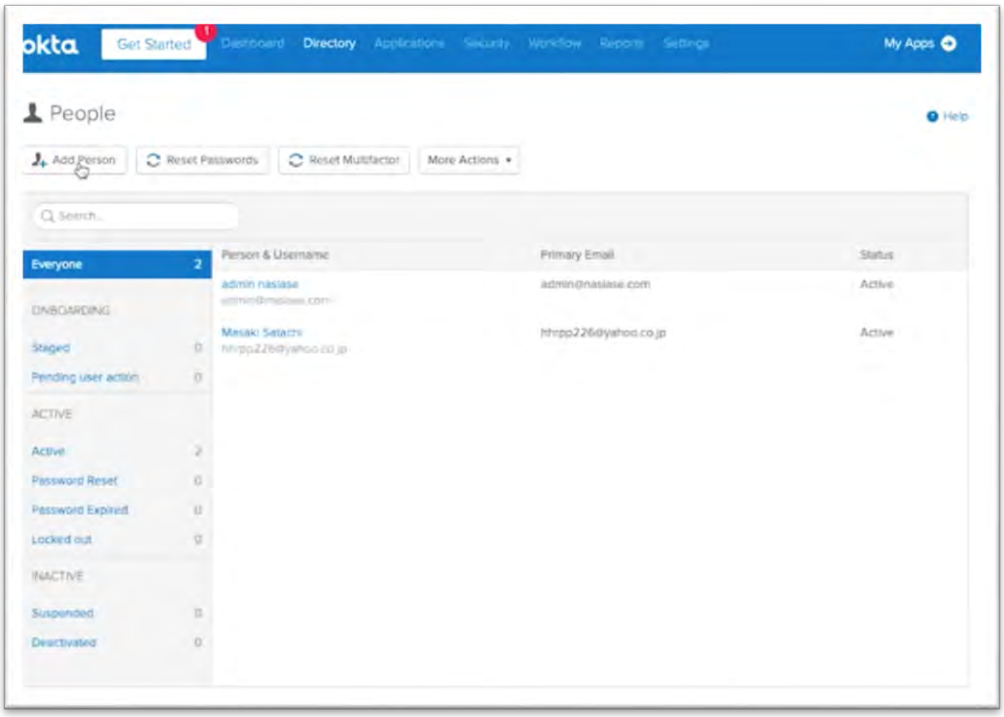
okta に admin アカウントでログインします。



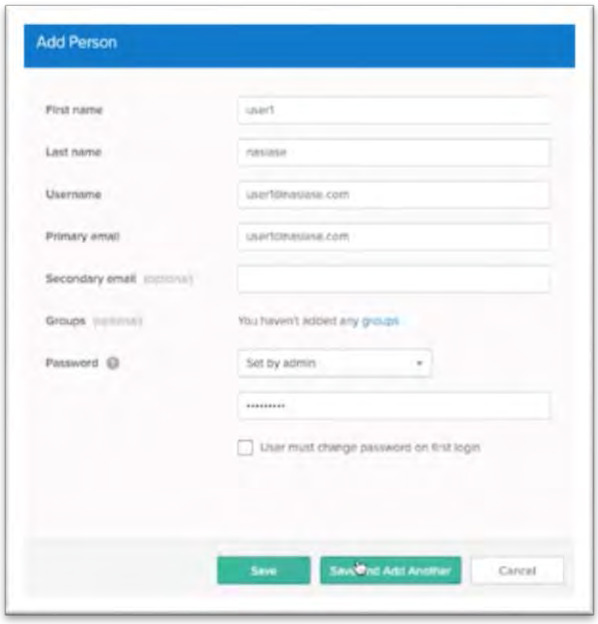
Directoryより、 [People] をクリックします。

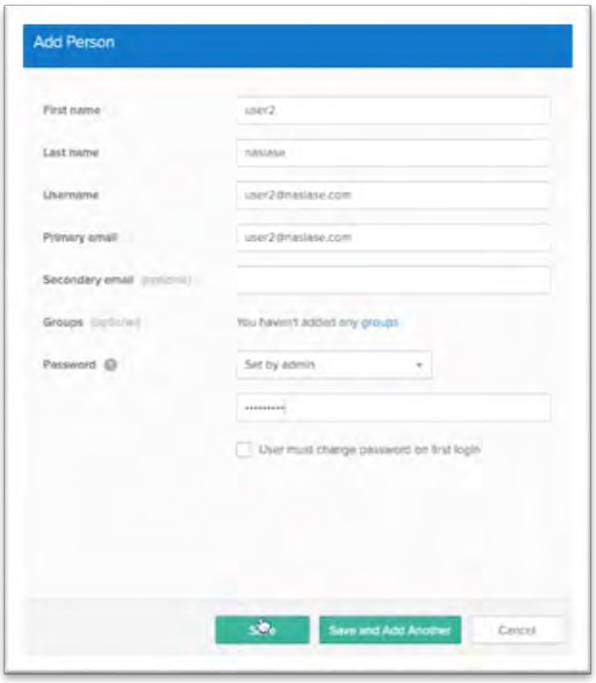


[Add Person]をクリックします。



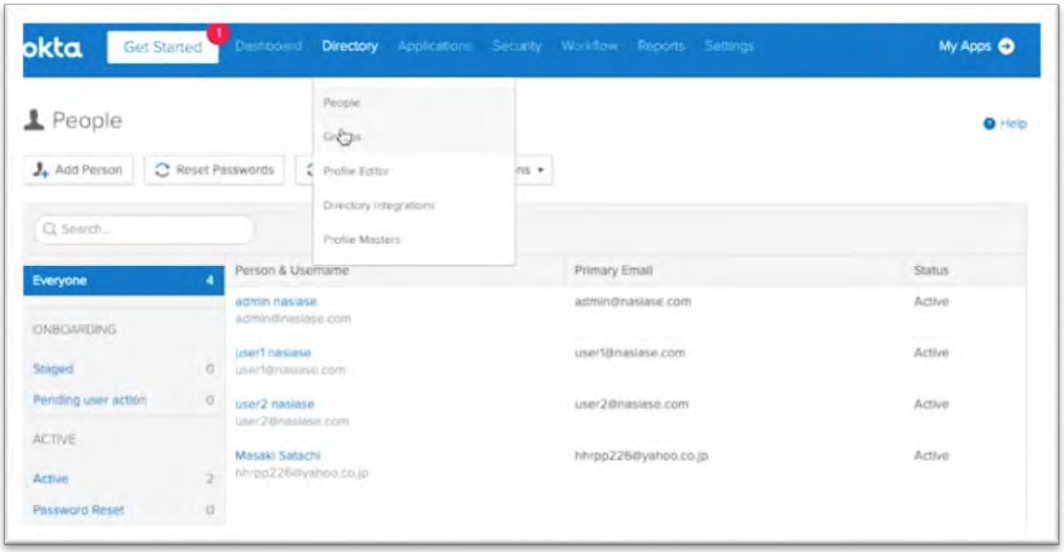
下図を参考に必要事項を記入して、user1、user2 を作成します。



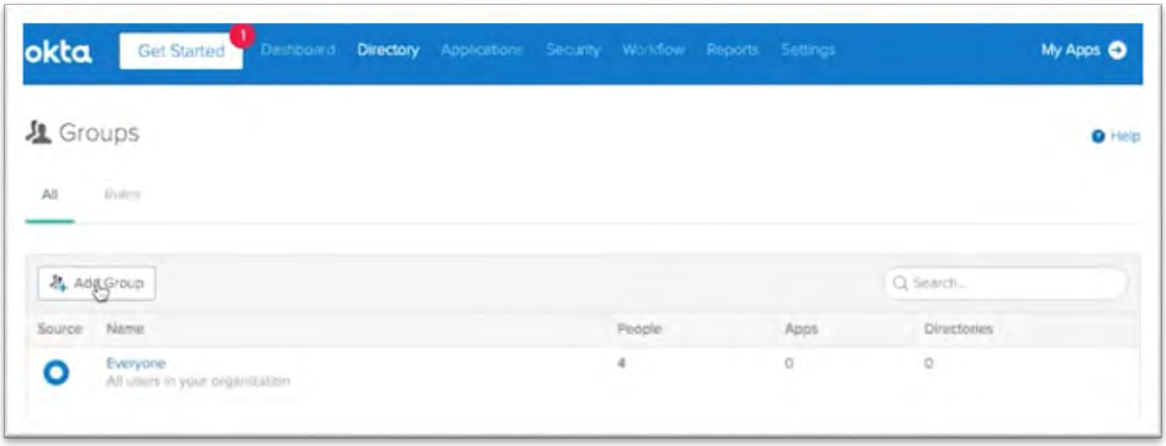


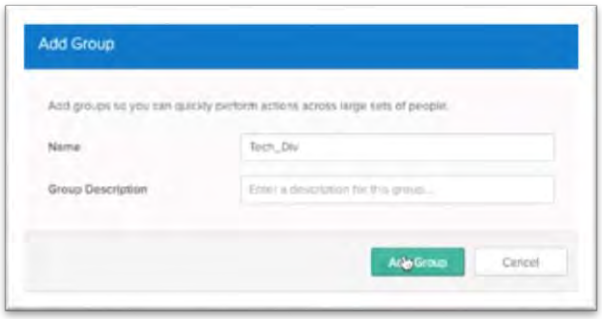
Step2. Tech_Div（技術部門）と Sales_Div（営業部門）のグループの作成

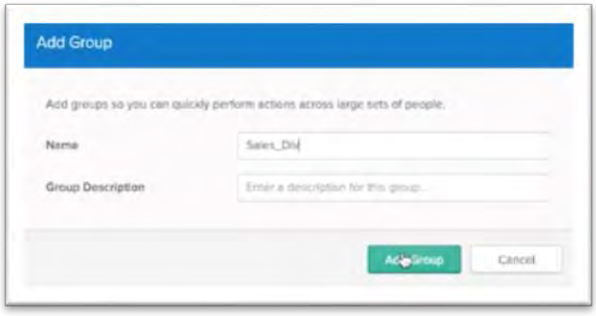
Directory より、[Groups]をクリックします。



[Add Group]をクリックします。

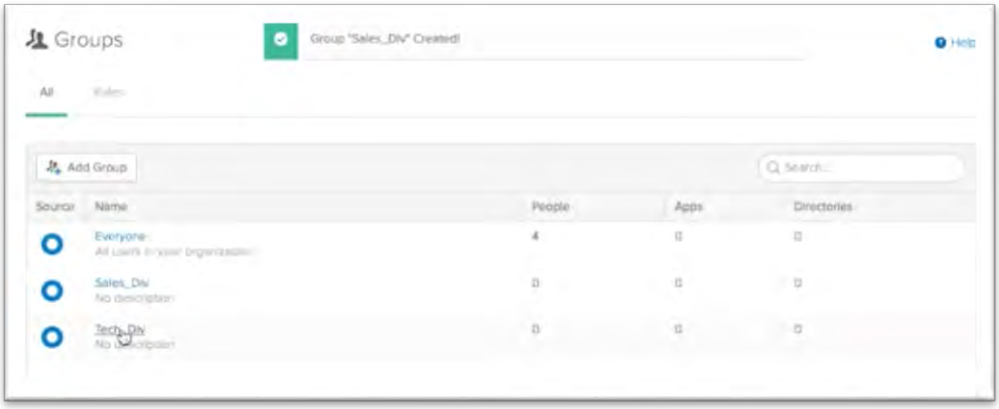




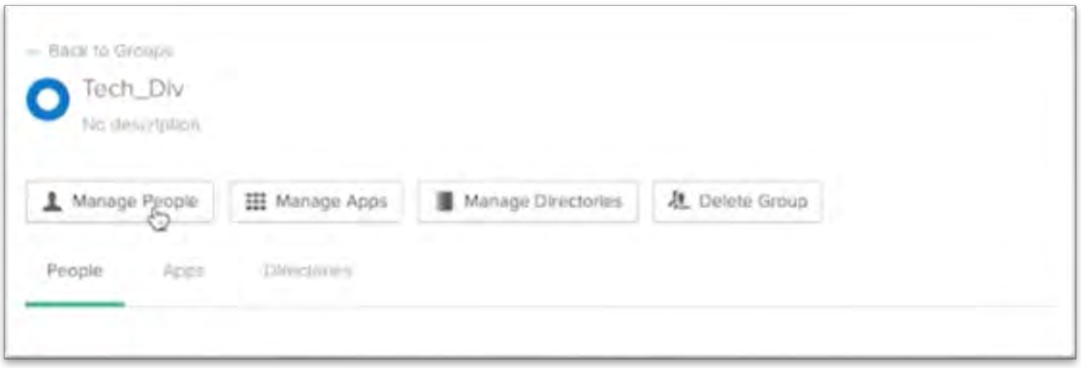


Step4. User のグループ紐付け（user1 に Tech_Div を Sales_Div に user2）

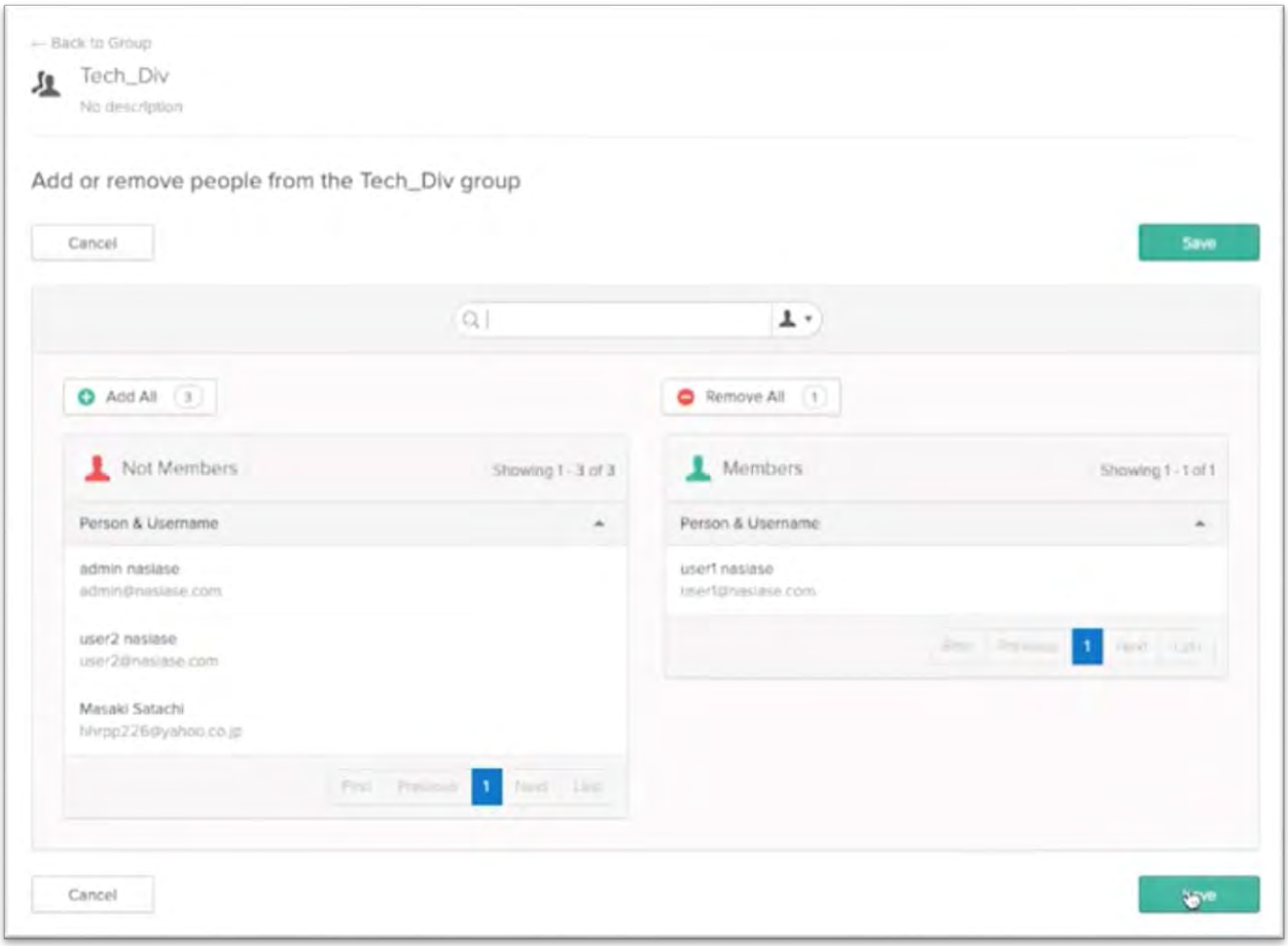
[Tech_Div]をクリックします。



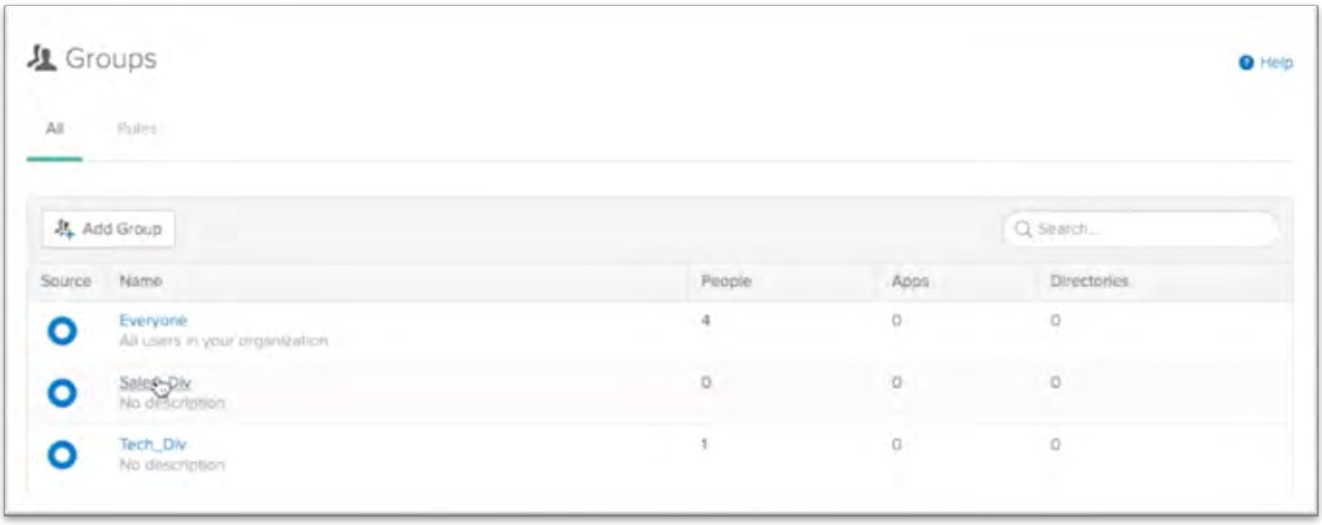
[Manage People]をクリックします。

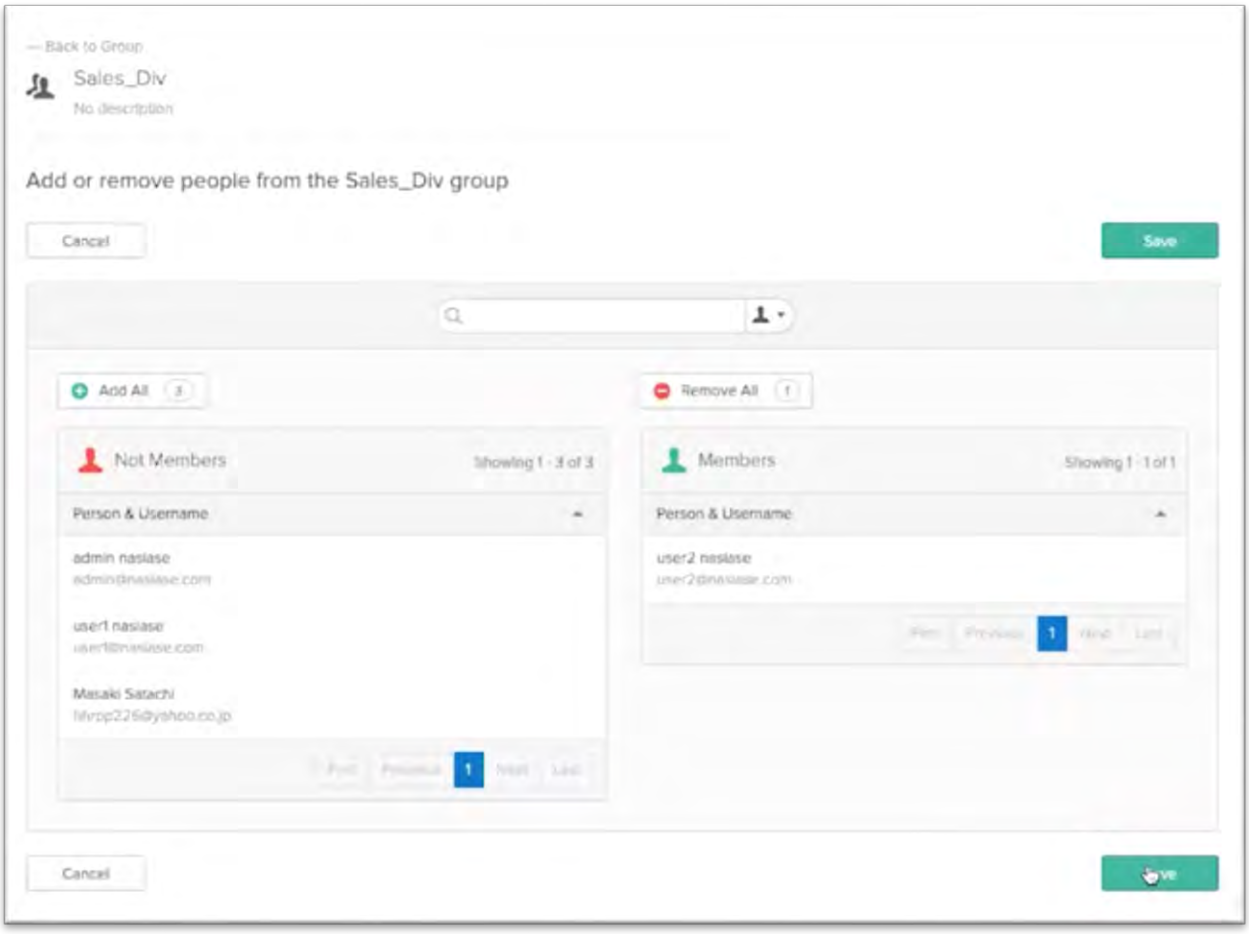


user1 を選択して[save]をクリックします。



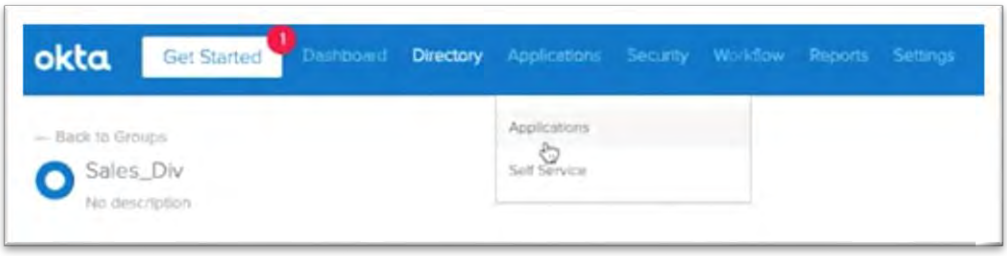
同様の手順で、user2 を Sales_Div に紐付けます。



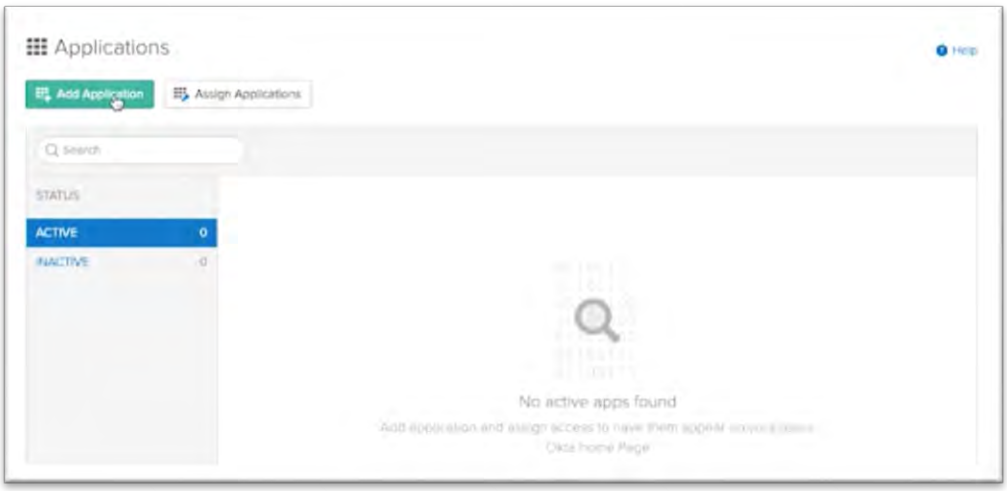


Step5. oktaにアプリケーション（ZPA）の登録

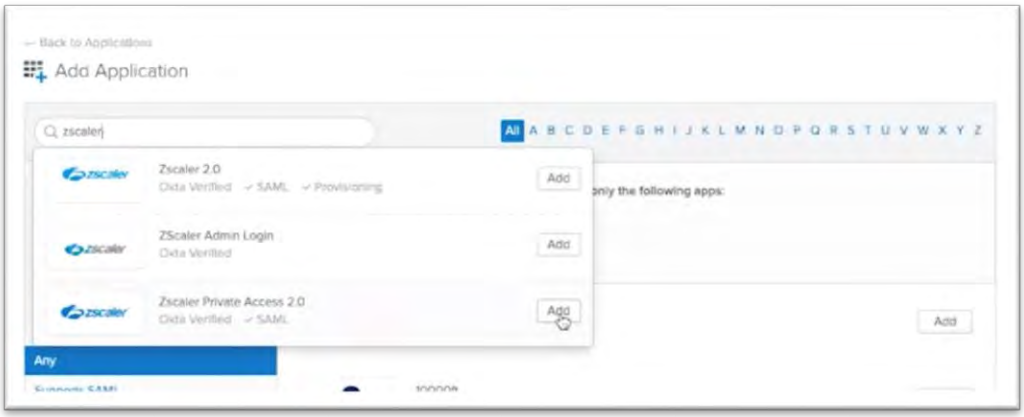
Applications より、[Applications]をクリックします。

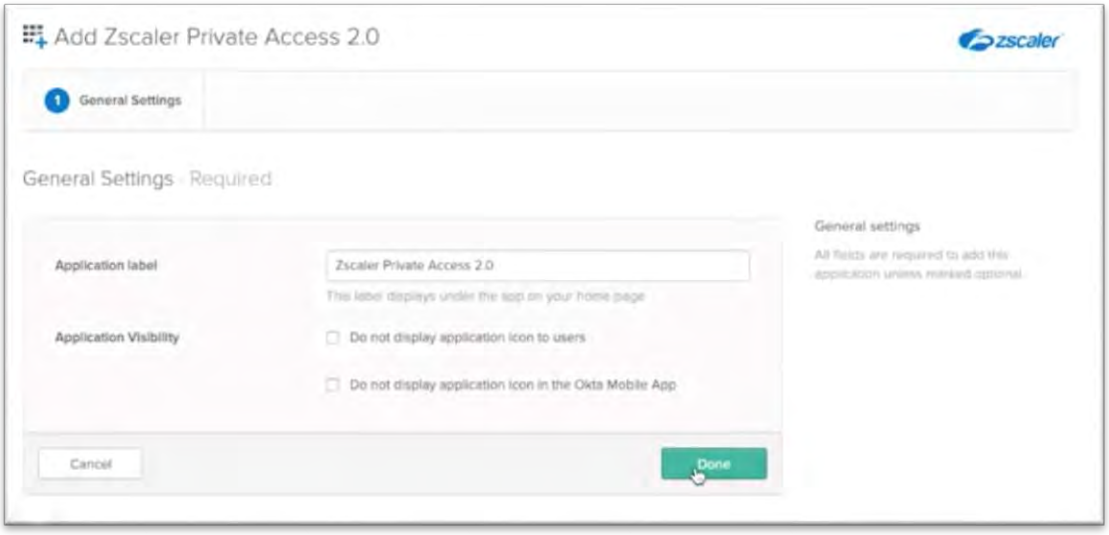


[Add Application]をクリックします。



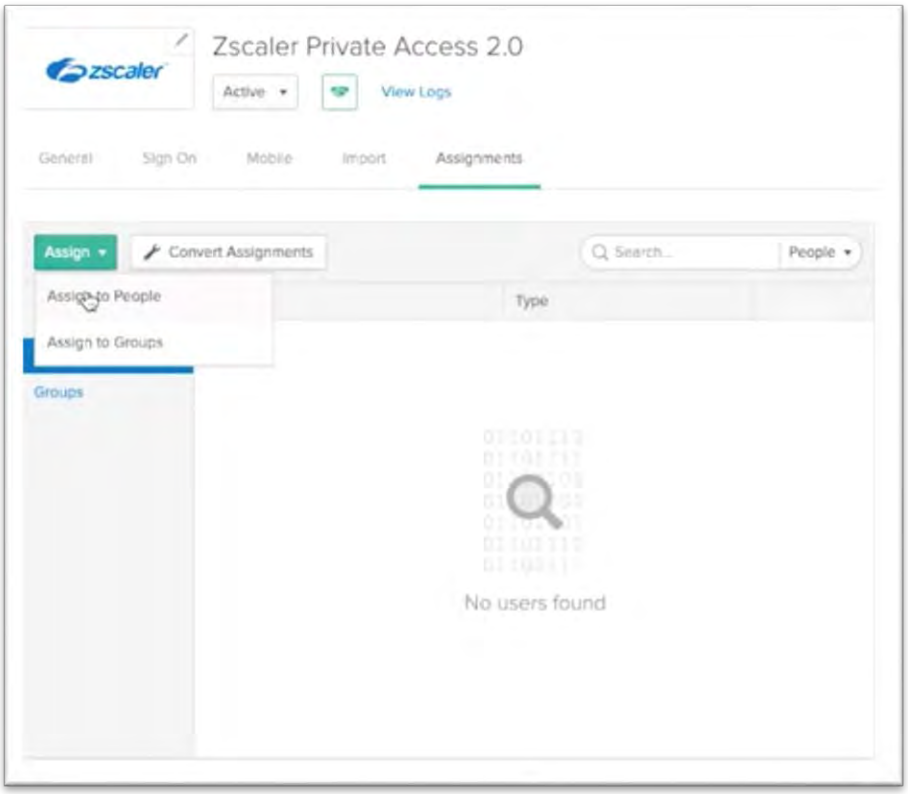
Zscaler Private Access を登録します。





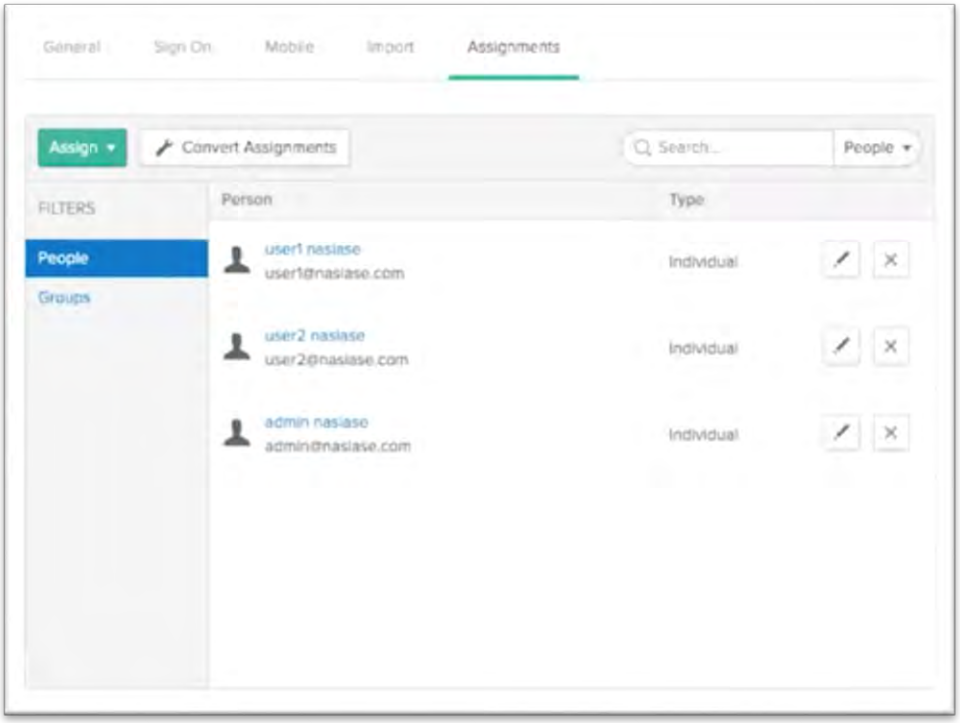
Step6. ZPAへのuserアサイン

Assign より、[Assign to People]をクリックします。



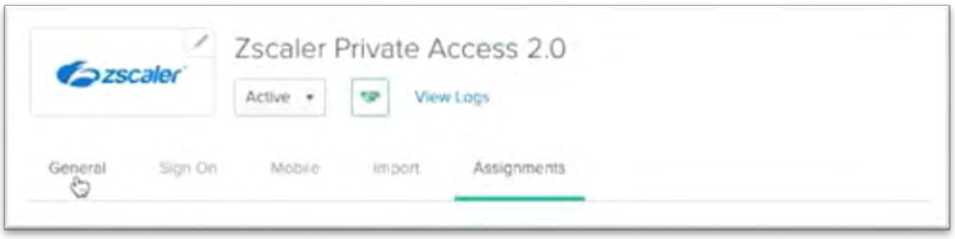
[Assign]をクリックして、user1 をアサインします。

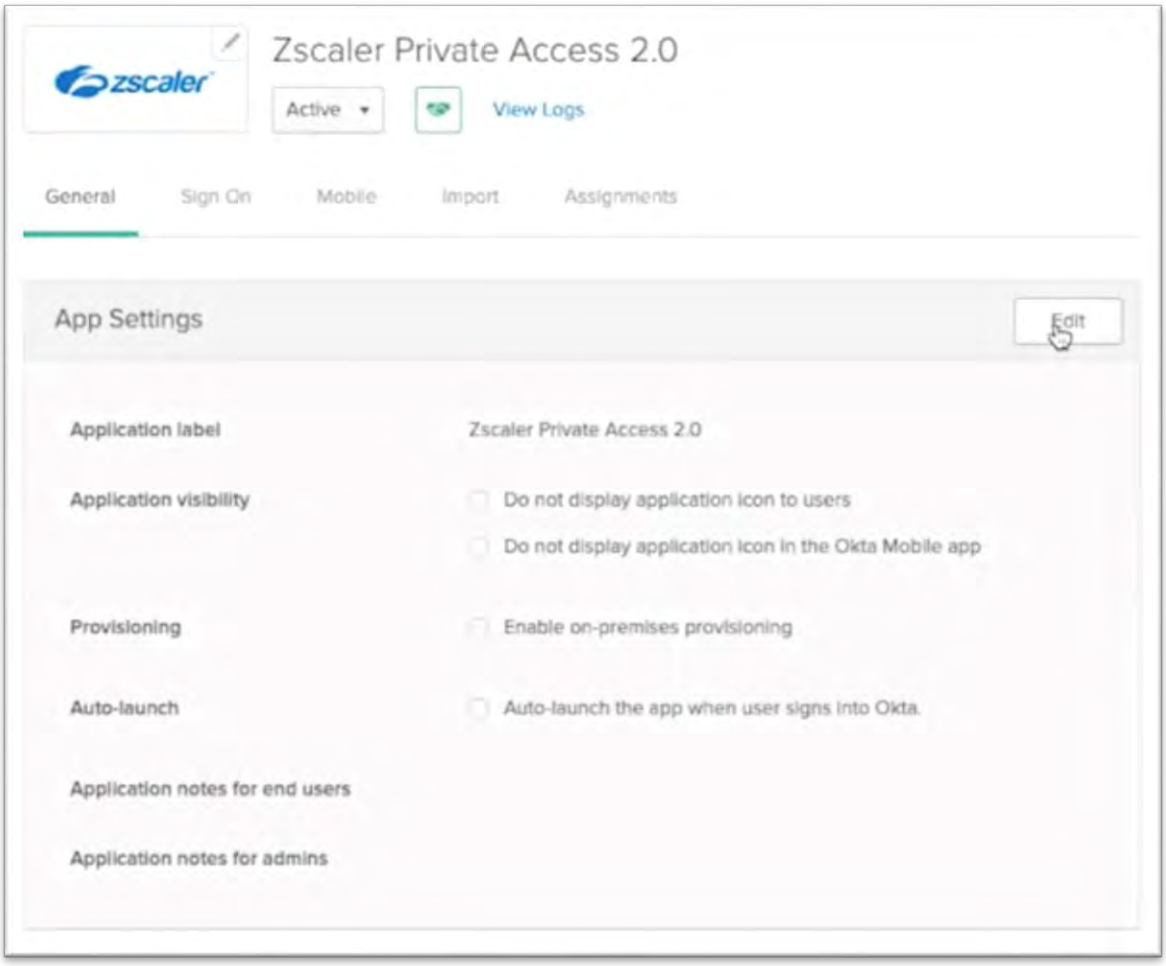
同様の手順で必要な user をアサインします。



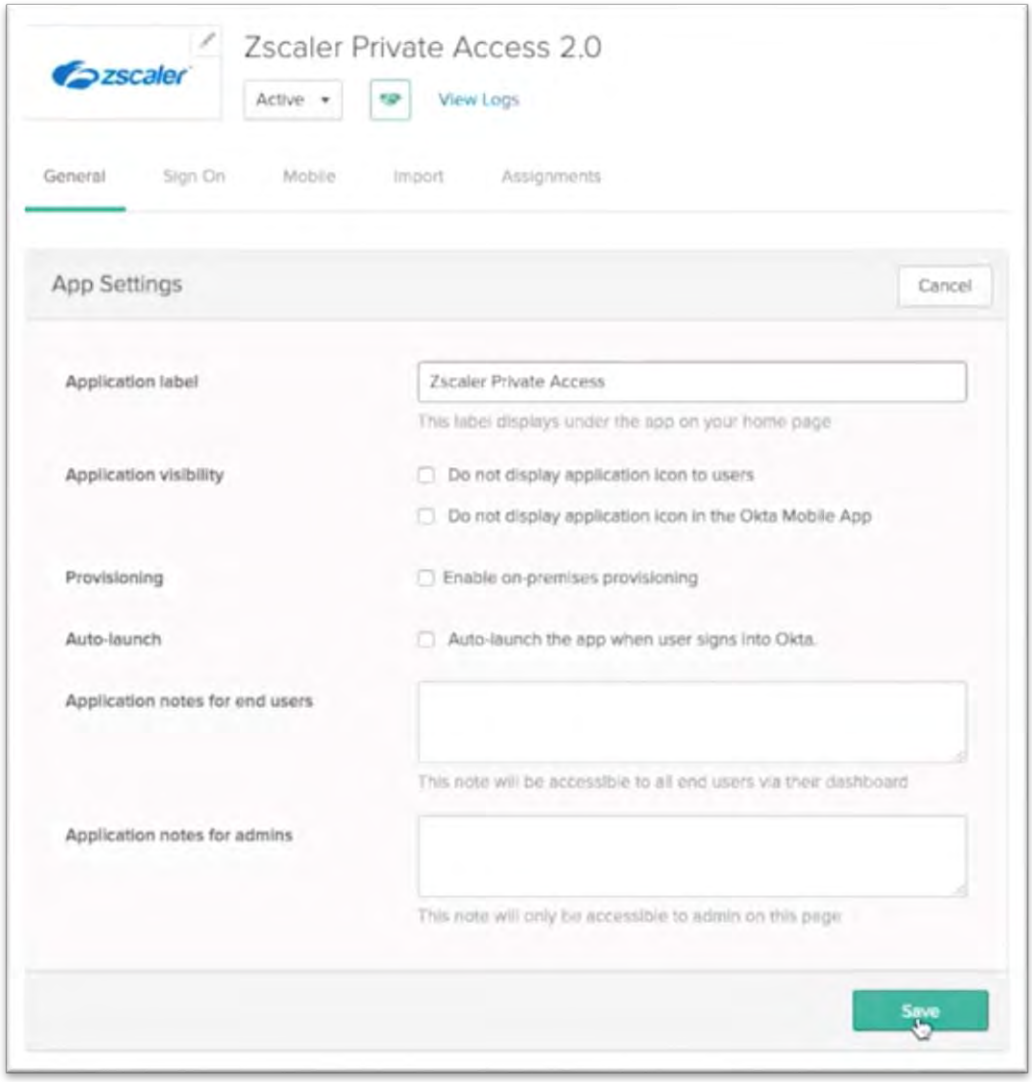
Step7．Applicationラベルの変更

Generalより、[Edit]をクリックします。



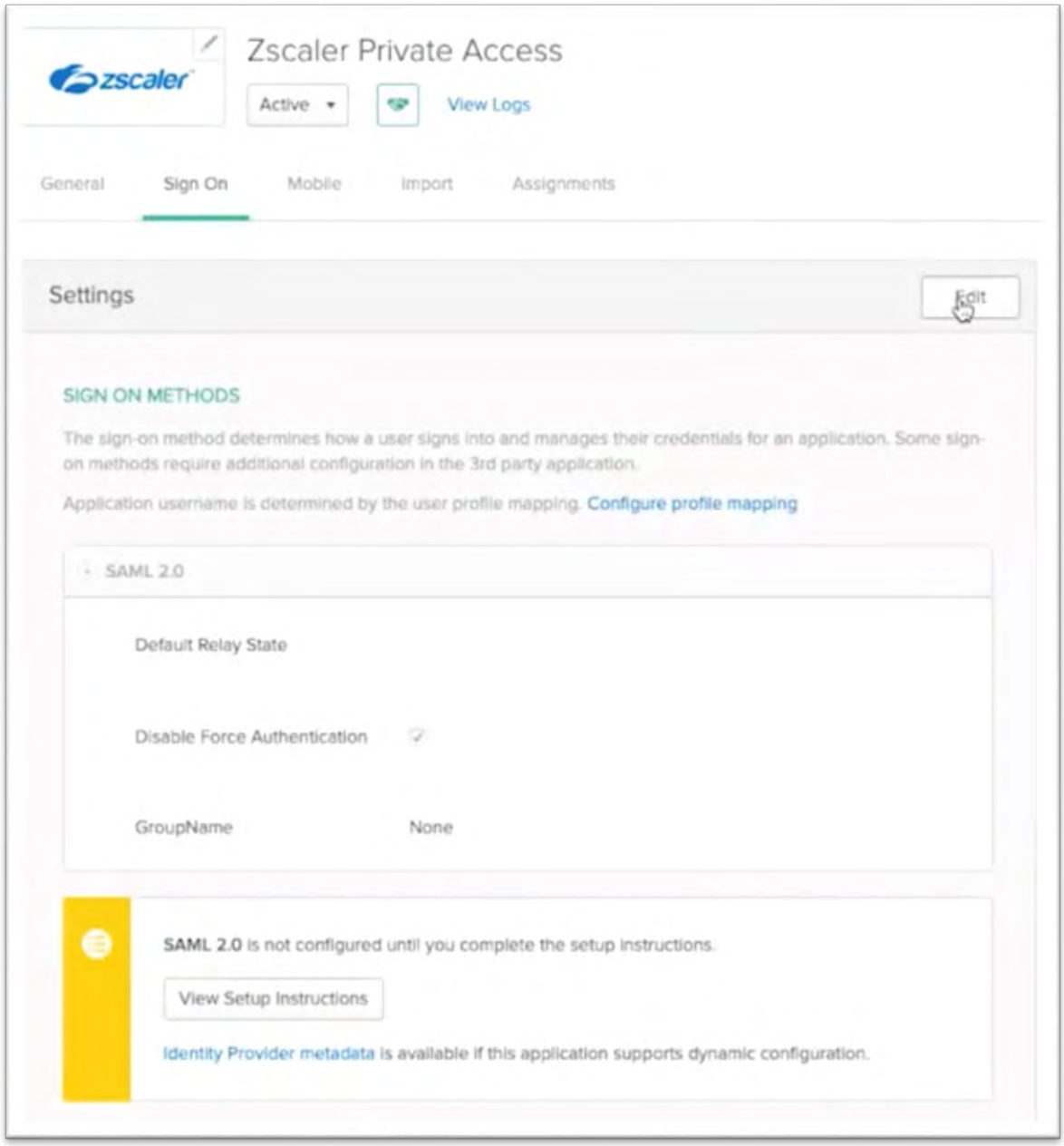


Application label 欄を任意に変更し、[Save]をクリックします。



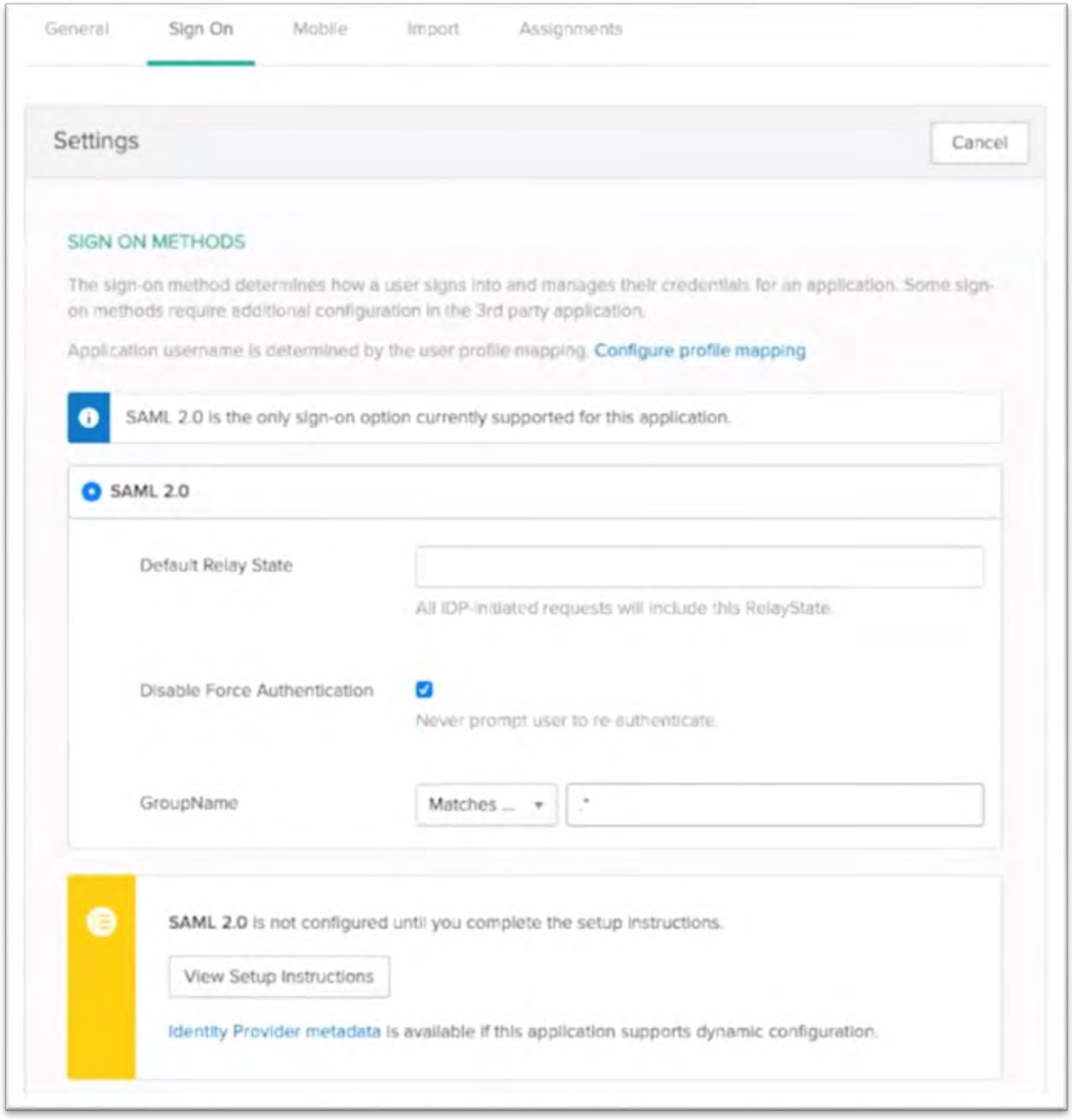
Step8. ZPAとokta間のSAML認証連携設定

Sign On -> Settingsより、[Edit]をクリックします。

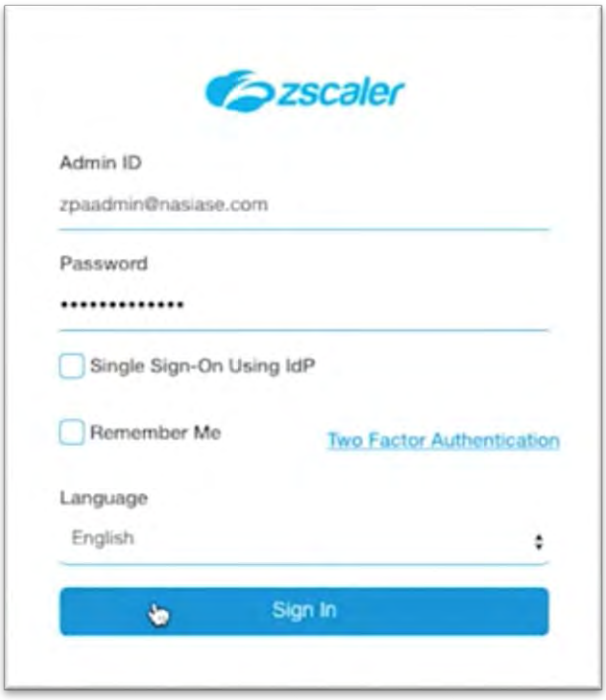


「Disable Force Authentication」にチェックが入っていることを確認し、Group Name を「Matches regex」に変更し「.*」を入力します。

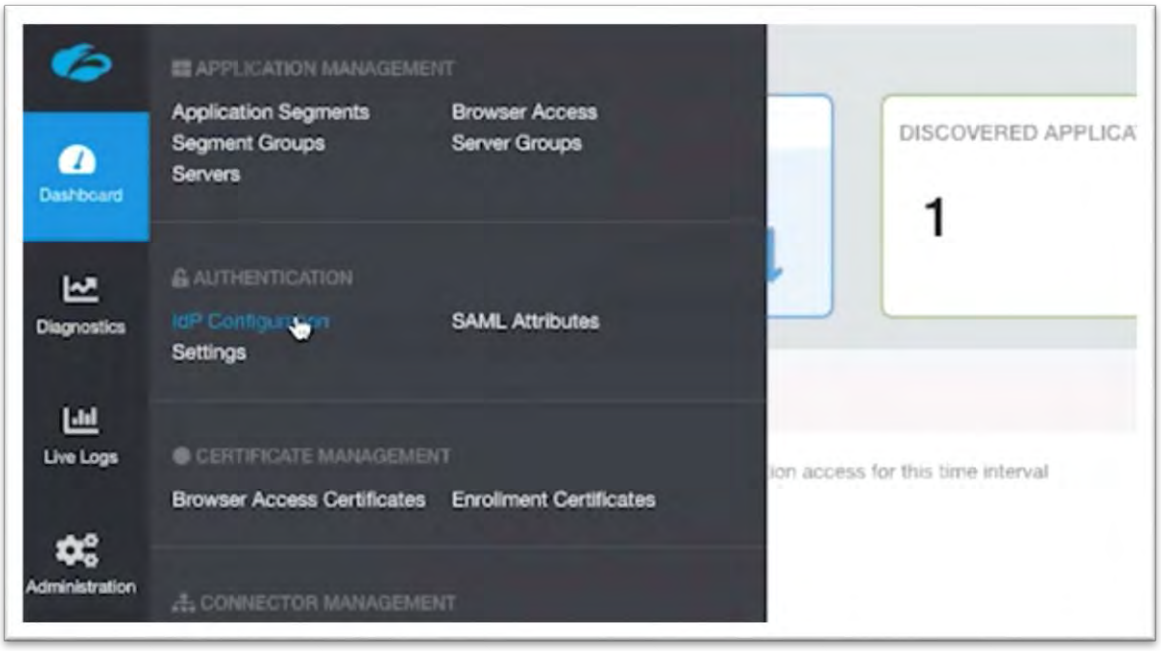
Identity Provider metadata のリンク先のファイル（メタデータ）を PC 保存します。



ZPA ポータルにログインします。



Administration -> AUTHENTICATION -> IdP Configuration より、IdP のプロファイルを作成します。



[Add IdP Configuration]をクリックします。

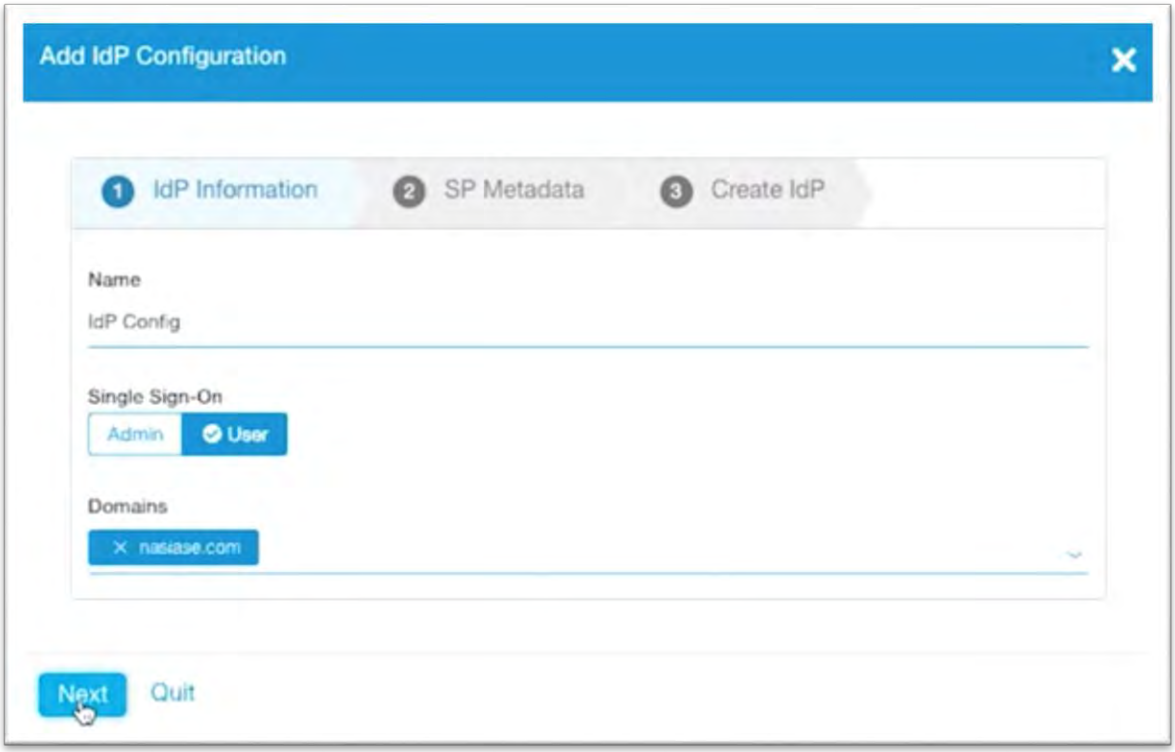
必要事項を記入、設定し [Next] をクリックします。

++

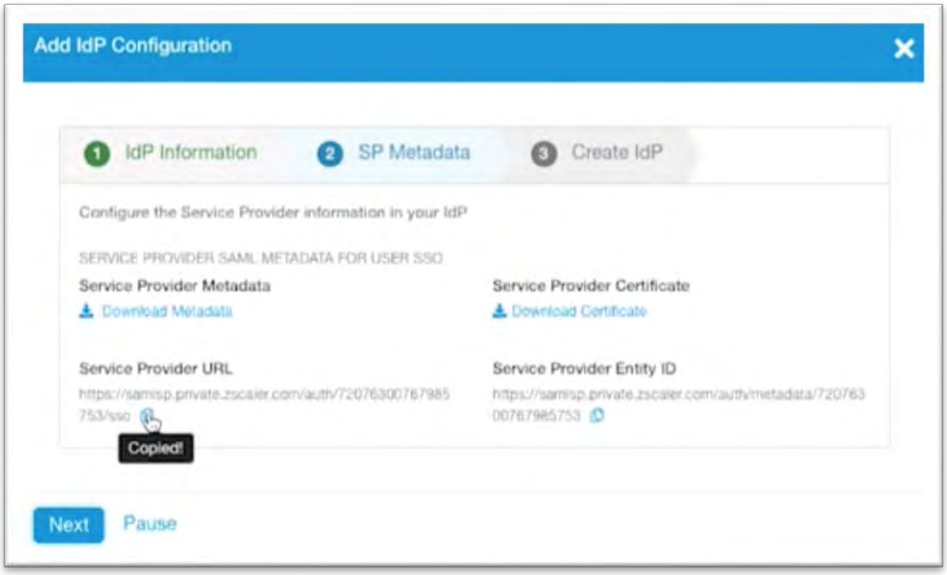
Name: 任意の名前

Domains: 申請いただいたドメイン名

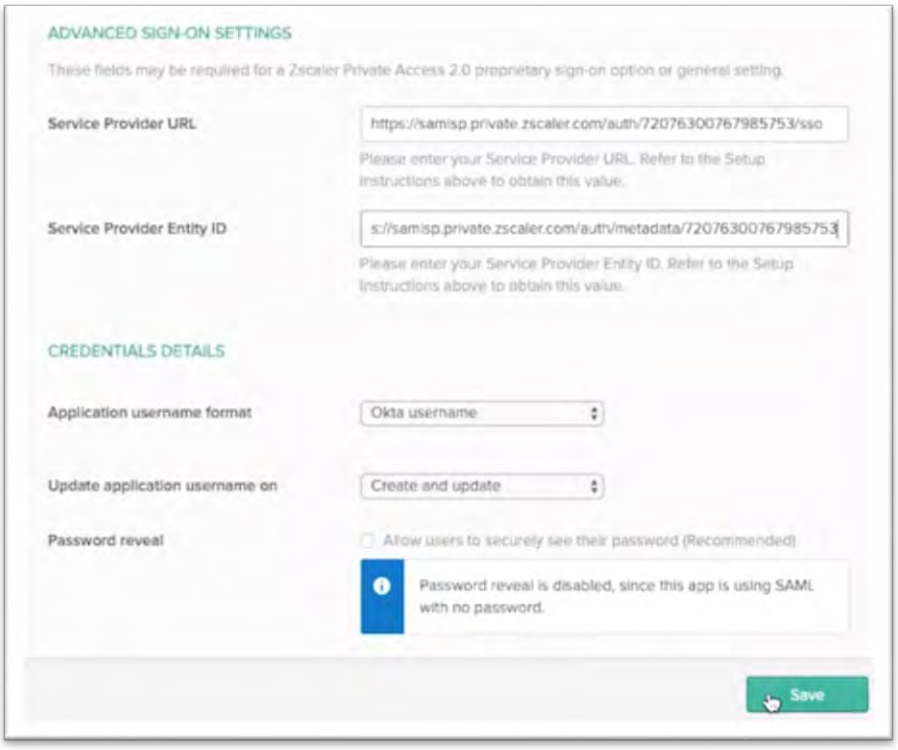
++



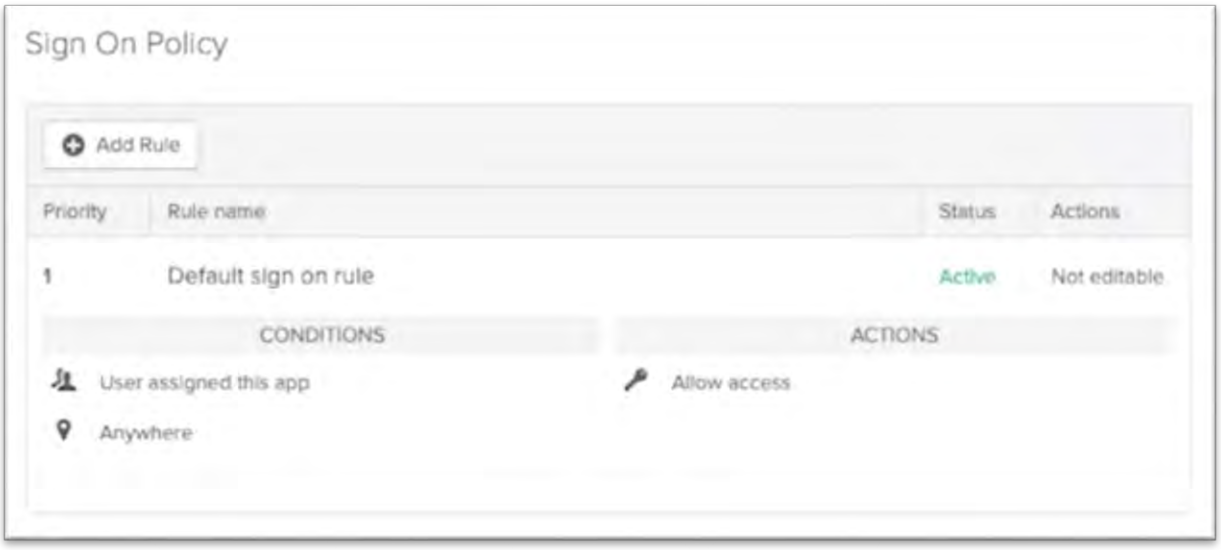
「Service Provider URL」、「Service Provider Entity ID」を okta のポータルにコピーペーストします。



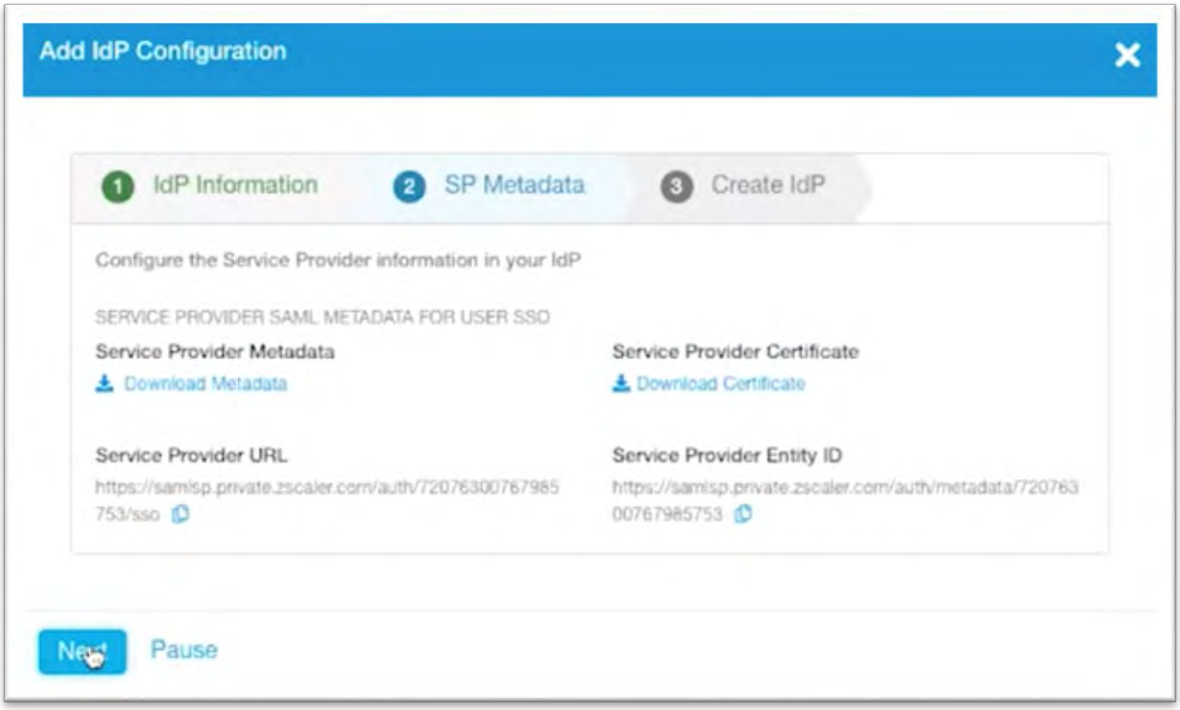
[Save]をクリックします。



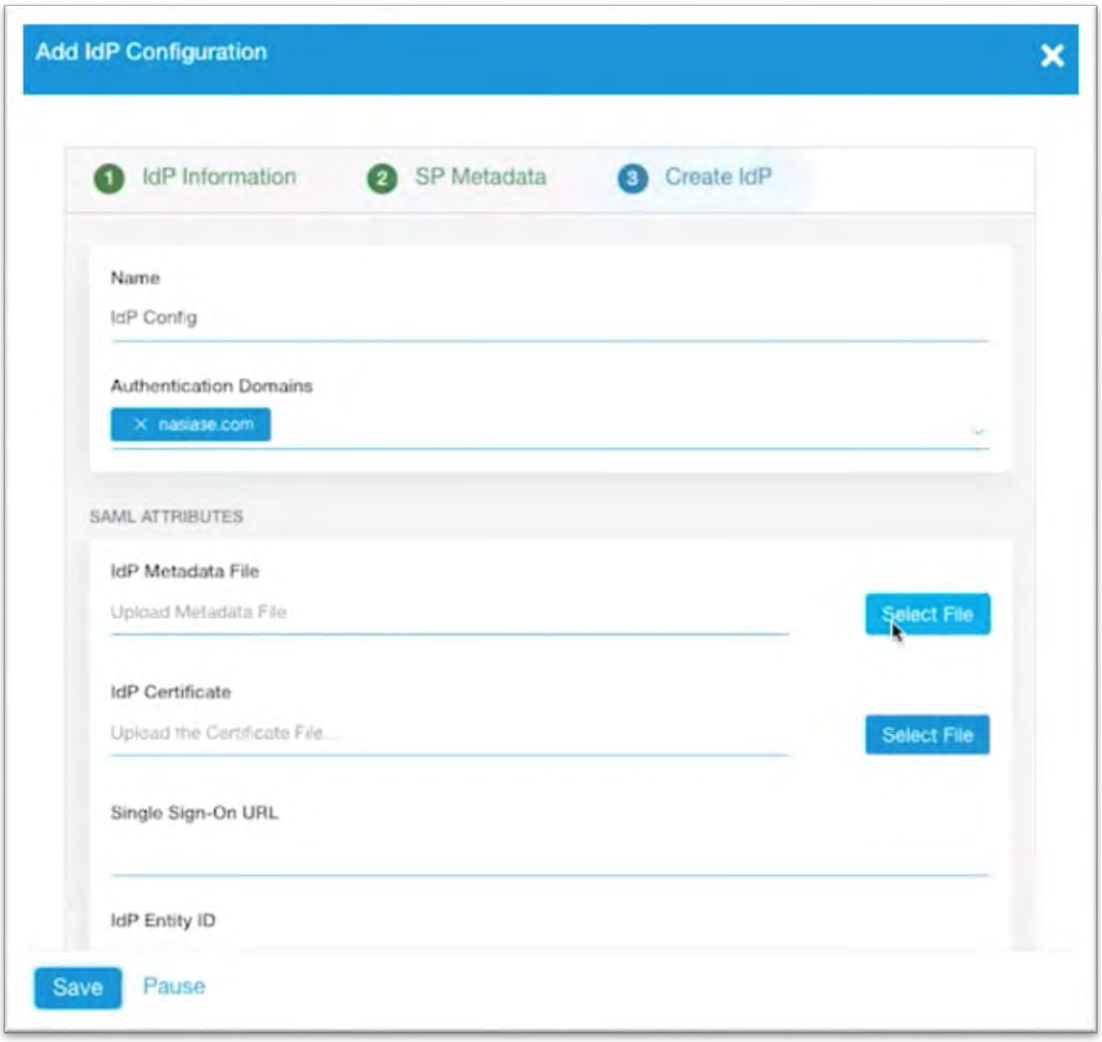
Sign On Policy の内容を確認します、こちらで okta 側の設定は完了です。



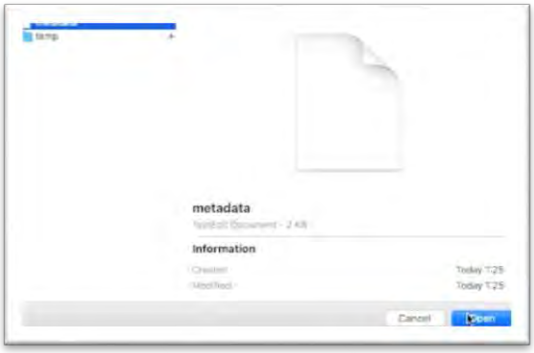
[Next]をクリックし、ZPA 側の設定を続けます。



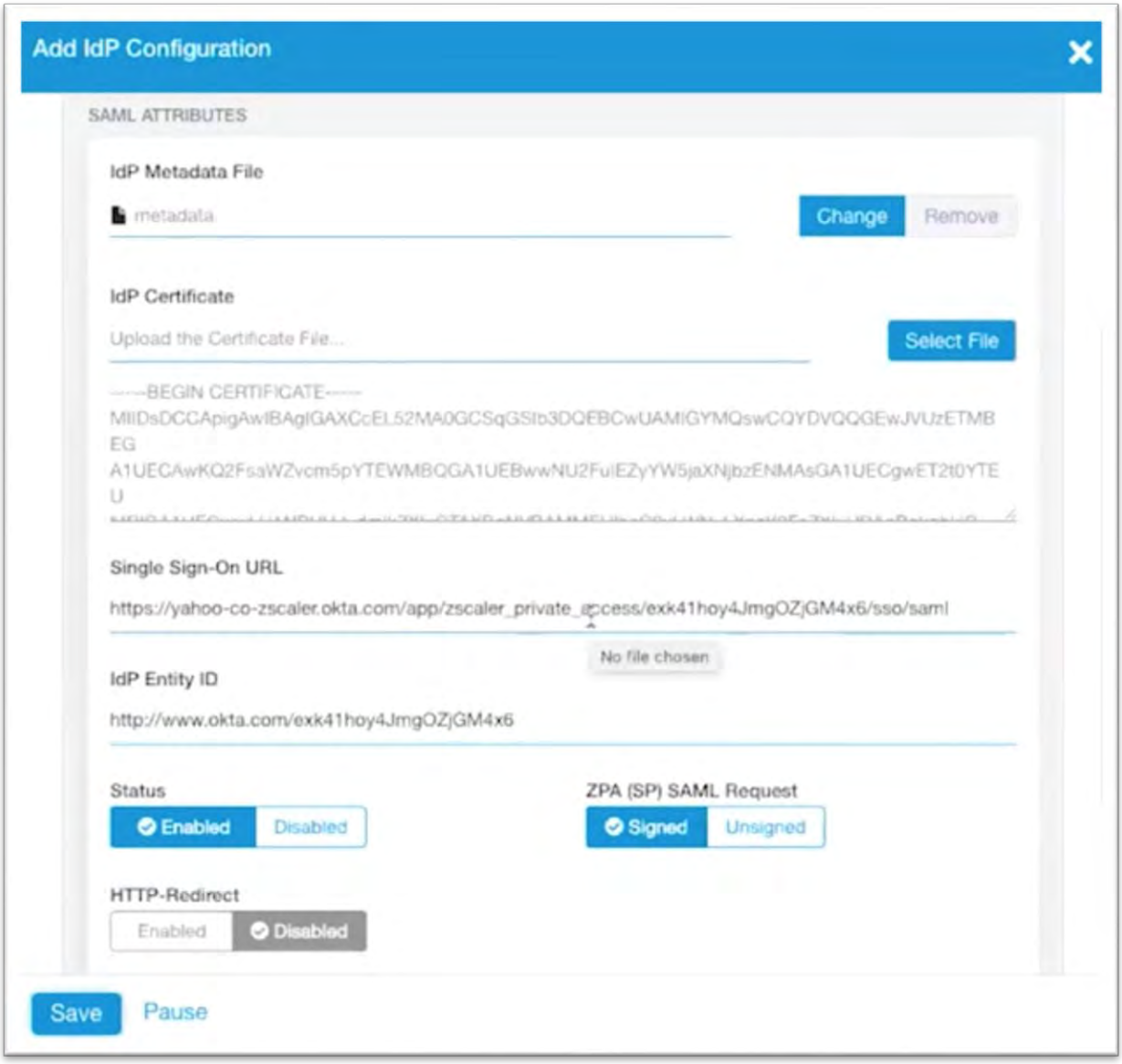
IdP Metadata File より、[Select File]をクリックします。



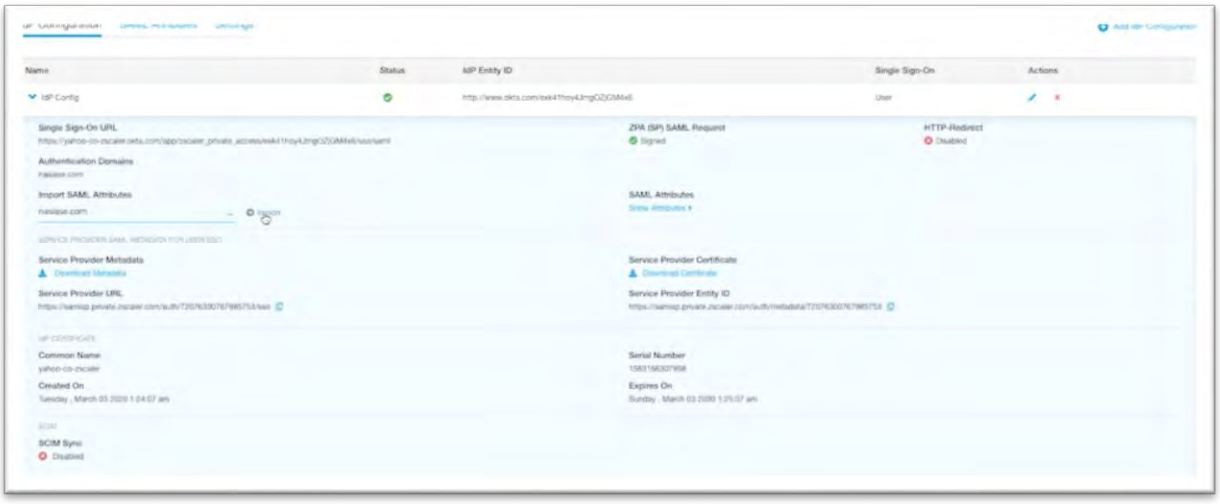
ダウンロードした Metadata File を選択すると、情報が自動でインポートされます。



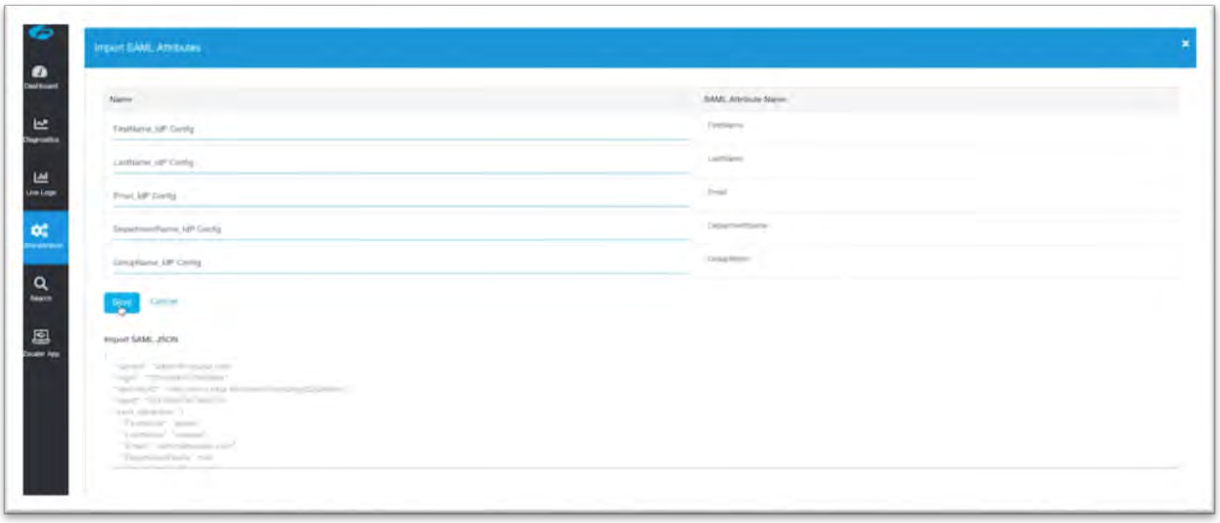
[Save]をクリックします。

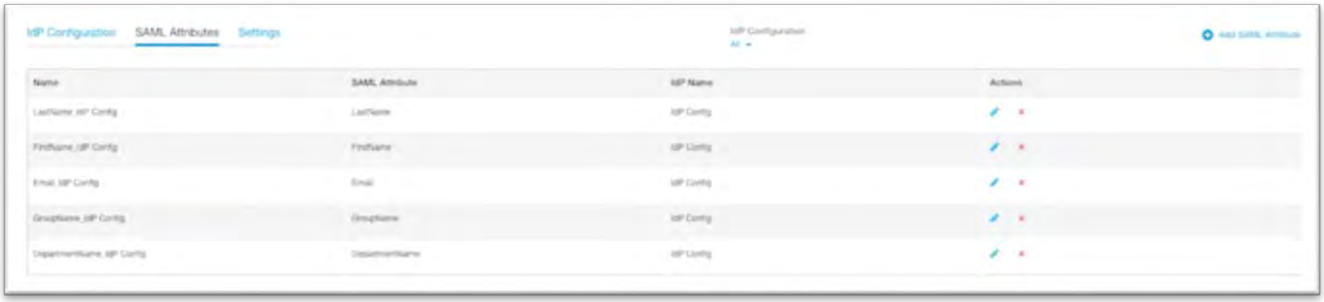


Import SAML Attributes より、[import]をクリックします。

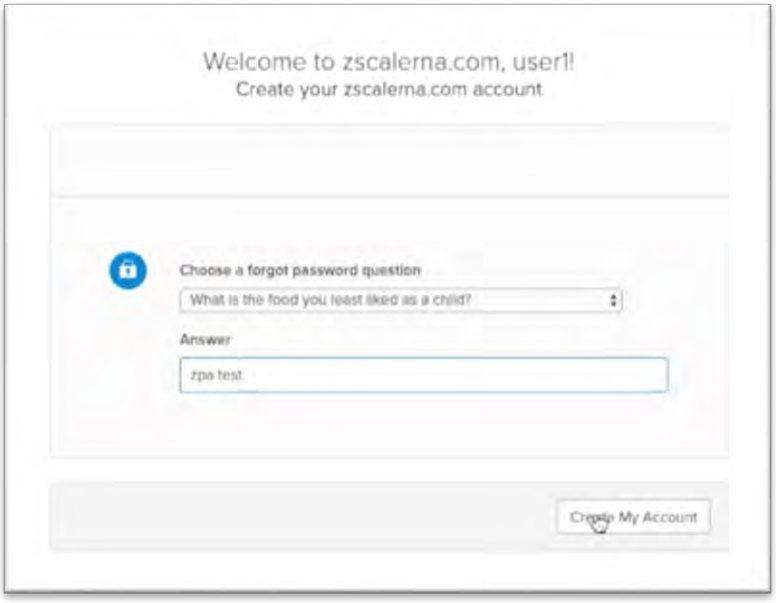


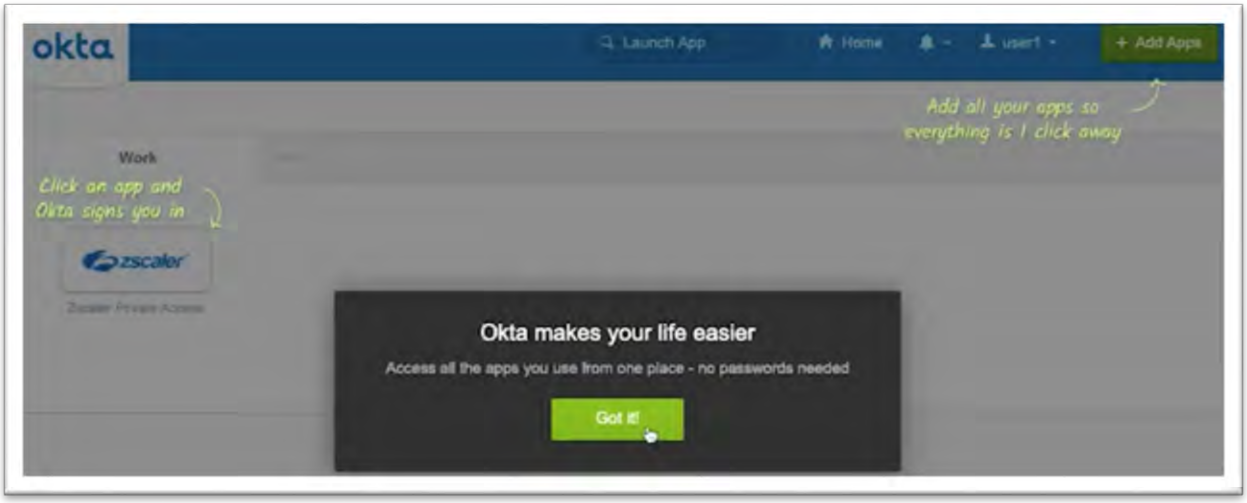
[Save]をクリックします。



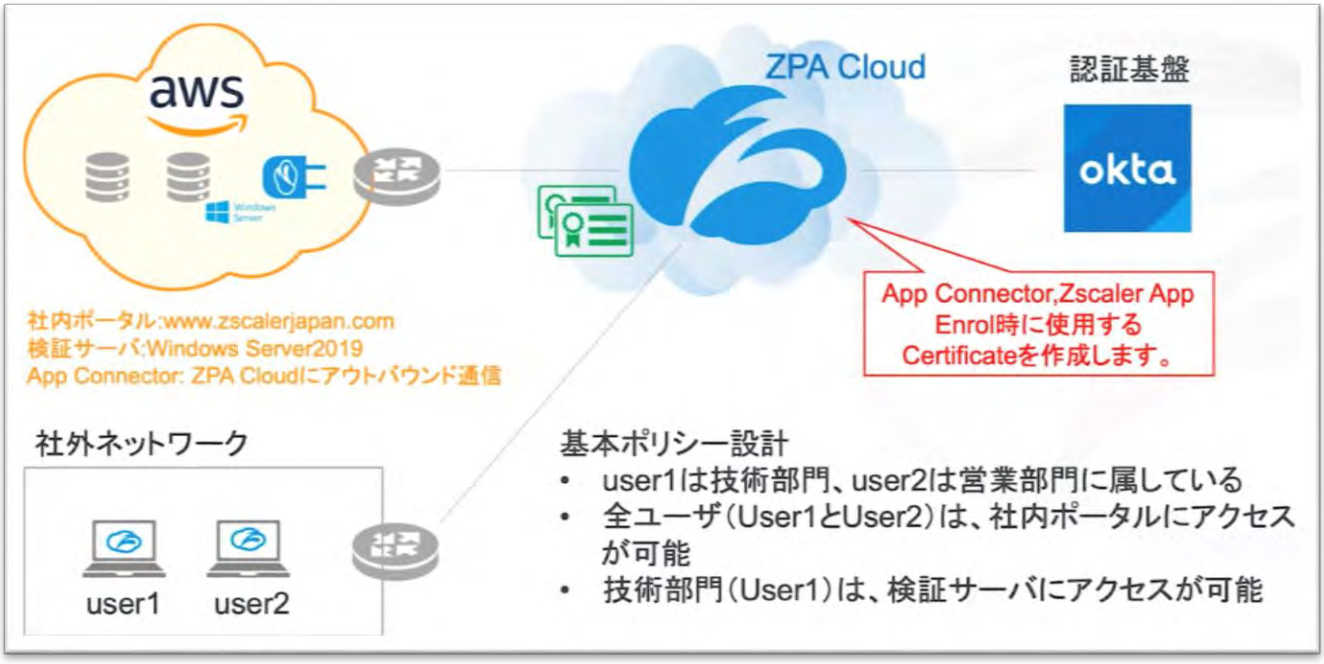


作成した user は、ログインすることでアクティベーションされるので、user1 と user2 でログインします。





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



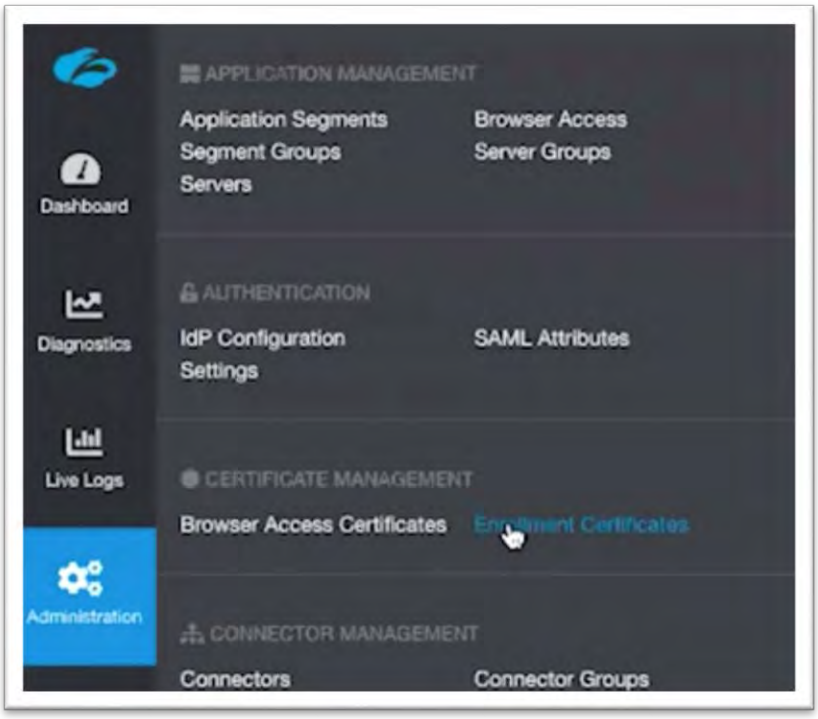
Notes

✓ 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。

必要事項を記入、設定し [Generate] をクリックします。

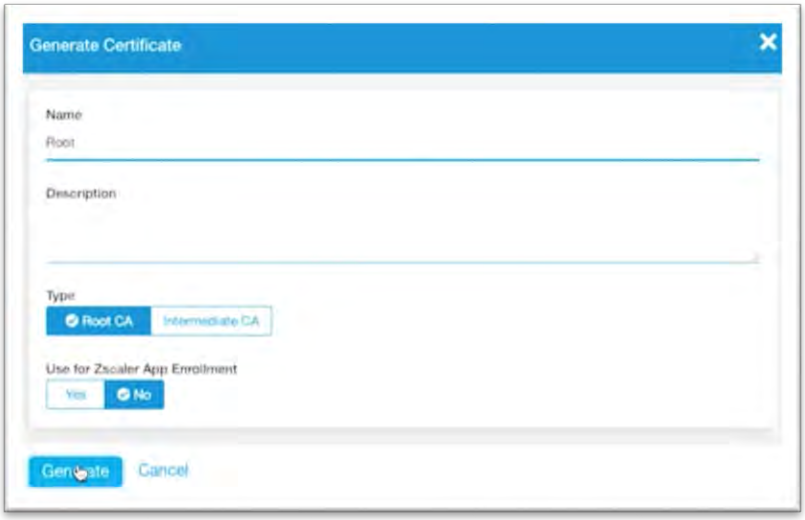
++

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。

必要事項を記入、設定し [Generate] をクリックします。

++

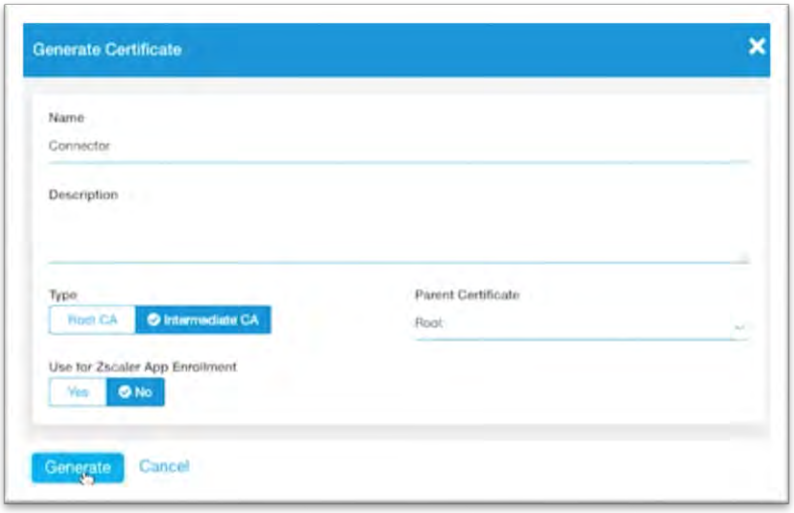
Name: 任意の名前

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。

必要事項を記入、設定し [Generate] をクリックします。

++

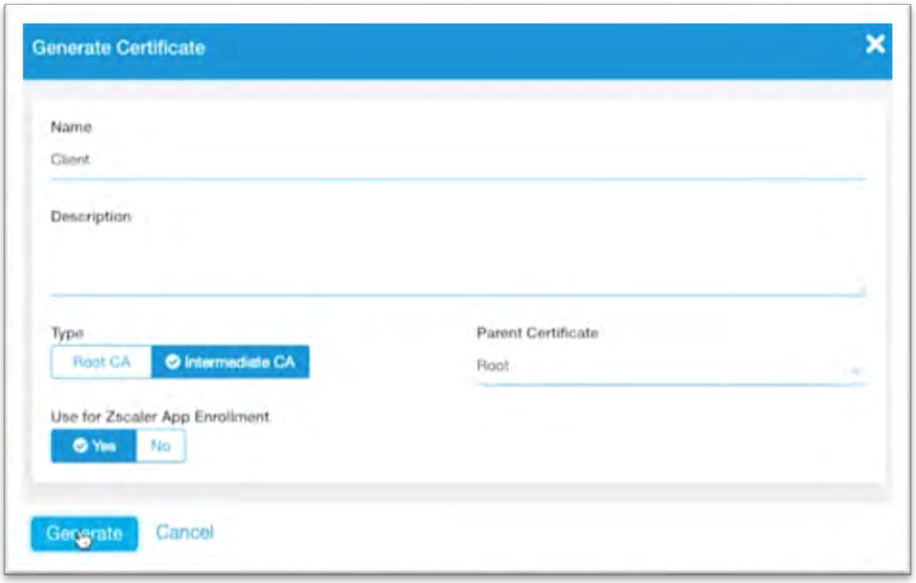
Name: 任意の名前

Type: Intermediate CA

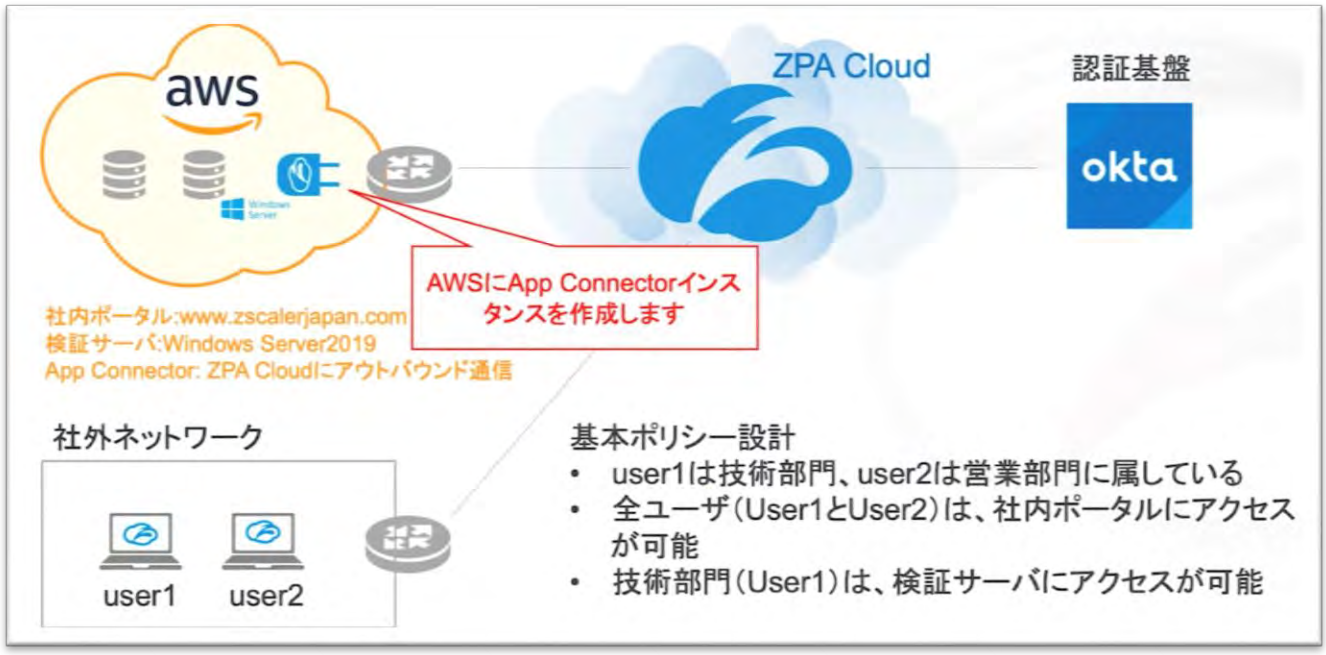
Parent Certificate: Step1 で作成した Root CA 証明書

Use for Zscaler App Enrollment: Yes

++



3-3. Connector のインストール



Note

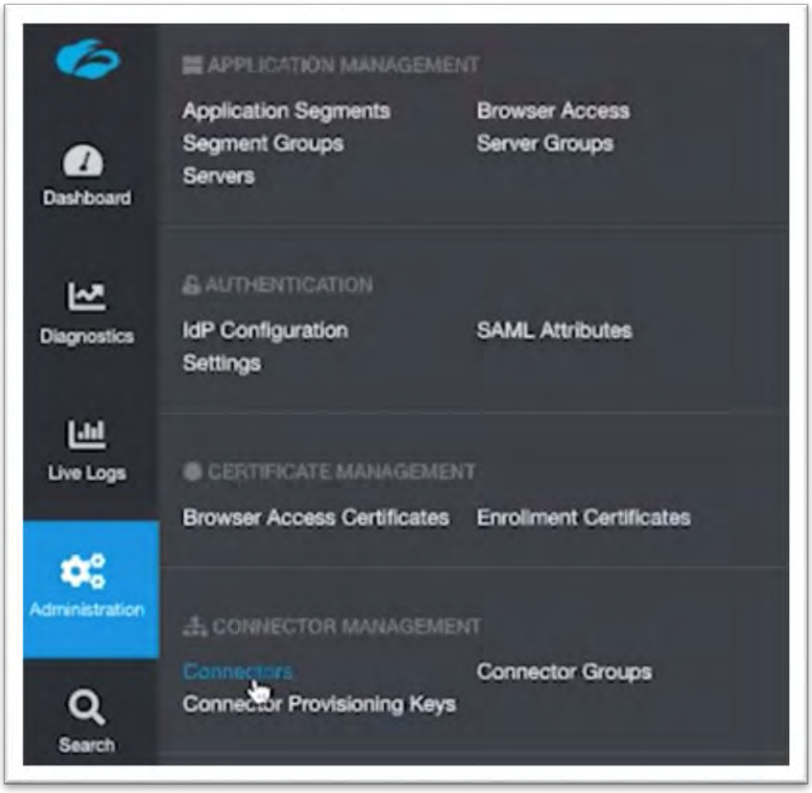
✓ 本ドキュメントでは、AWS でのインストール方法を紹介

✓ 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

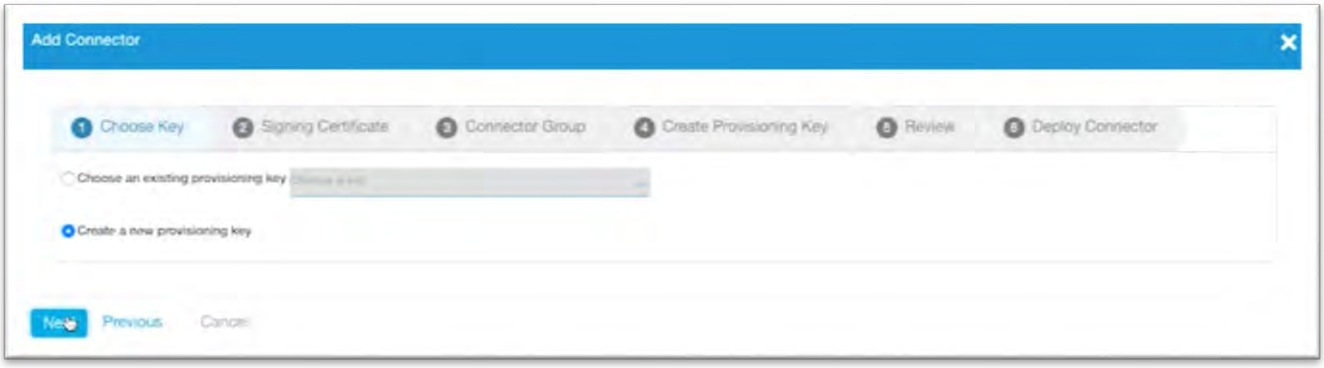
Step1. Connector のプロファイル作成

Administration -> CERTIFICATE MANAGEMENT -> Connectors より、プロファイルを作成します。



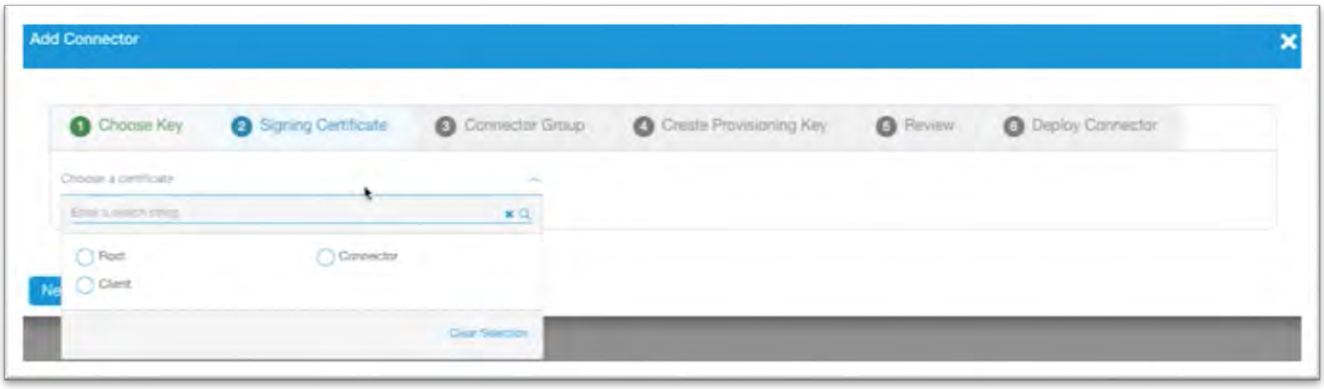
[Add Connector]をクリックします。

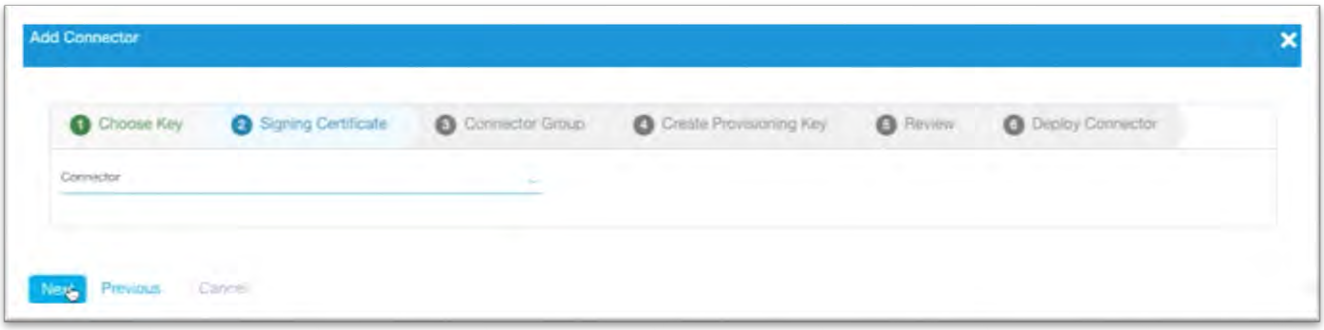
Create a new provisioning key にチェックをつけ、[Next] をクリックします。



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。





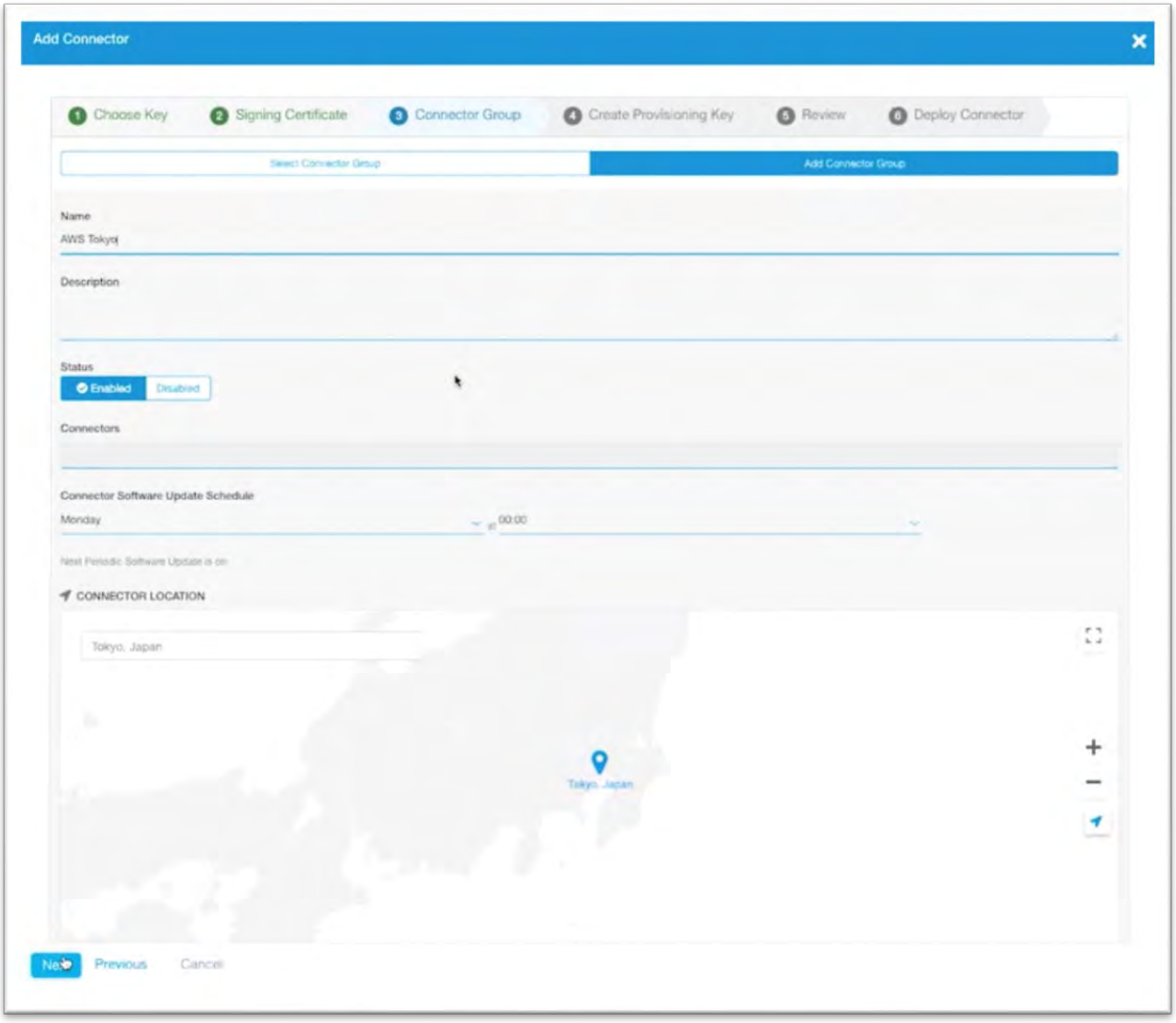
必要事項を記入し [Next] をクリックします。

++

Name: 任意の名前

CONNECTOR LOCATION: Connector の設置場所

++



必要事項を記入し [Next] をクリックします。

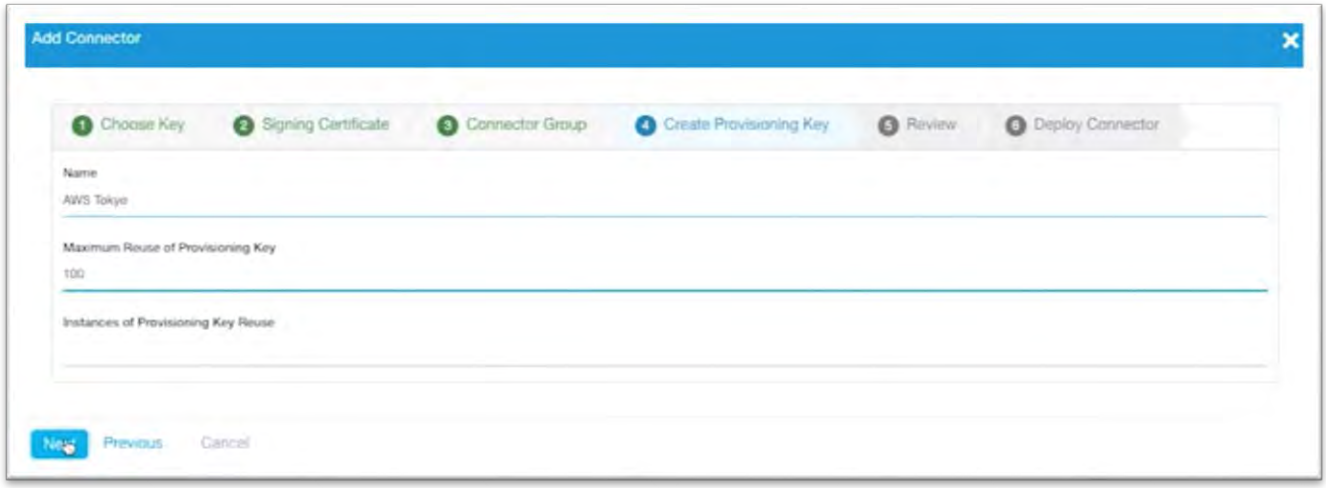
++++++++++

Name: 任意の名前

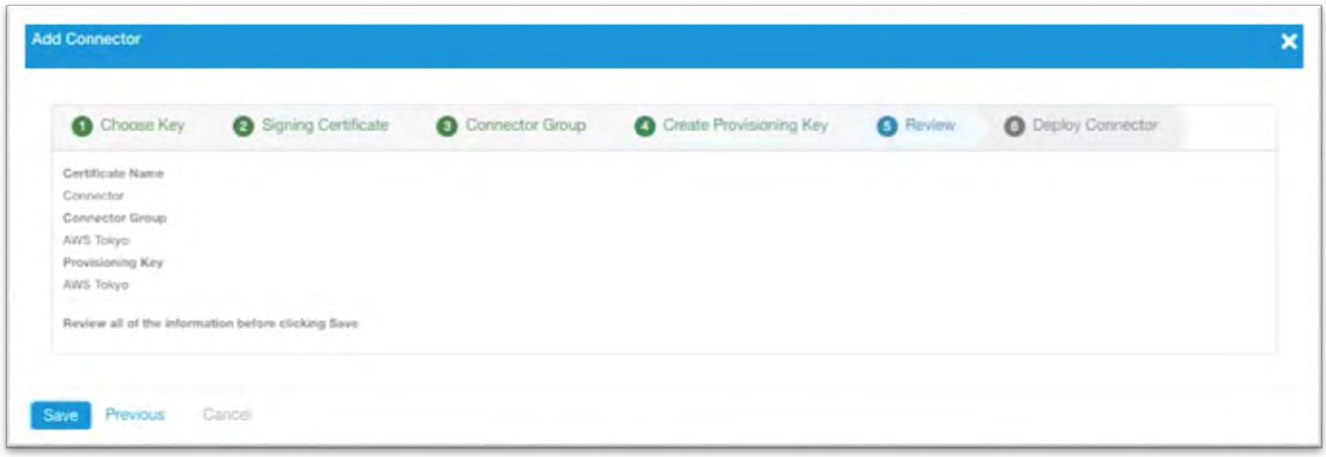
Maximum Reuse of Provisioning Key: 任意の値

Instances of Provisioning Key Reuse: 任意の値

++++++++++

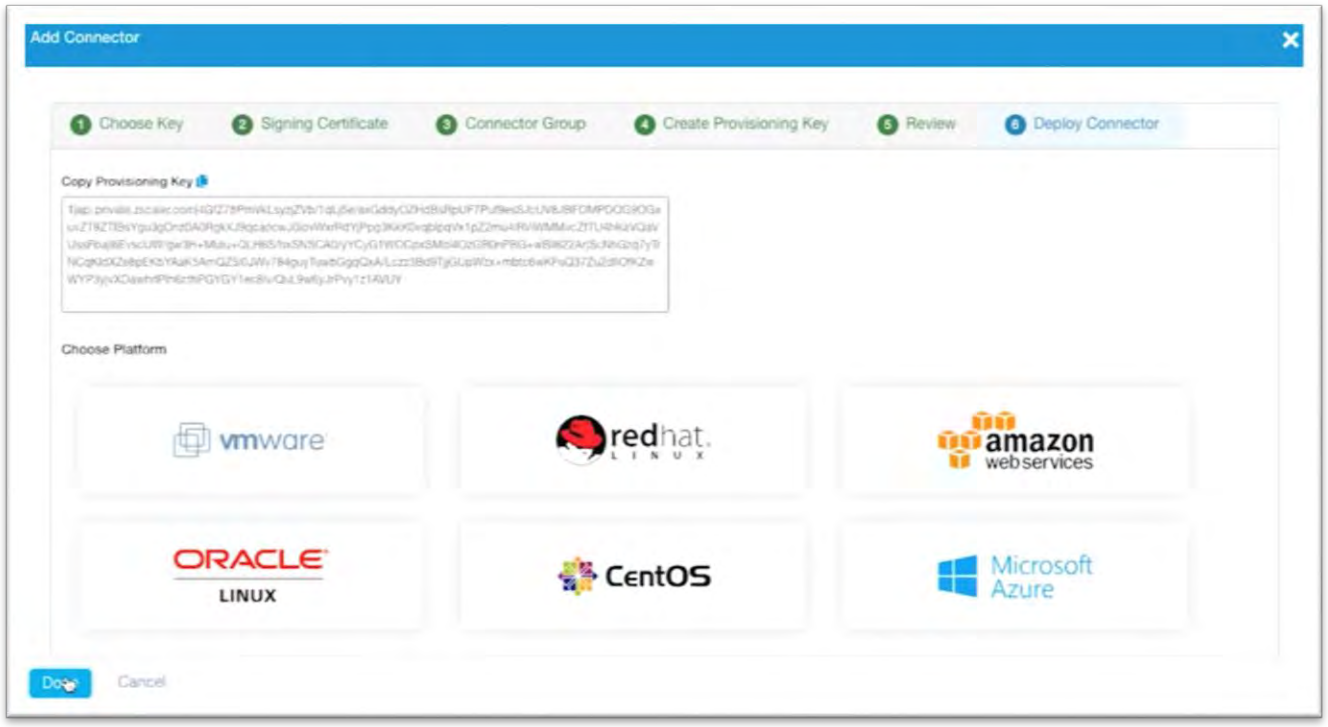


内容を確認して、[Save]をクリックします。



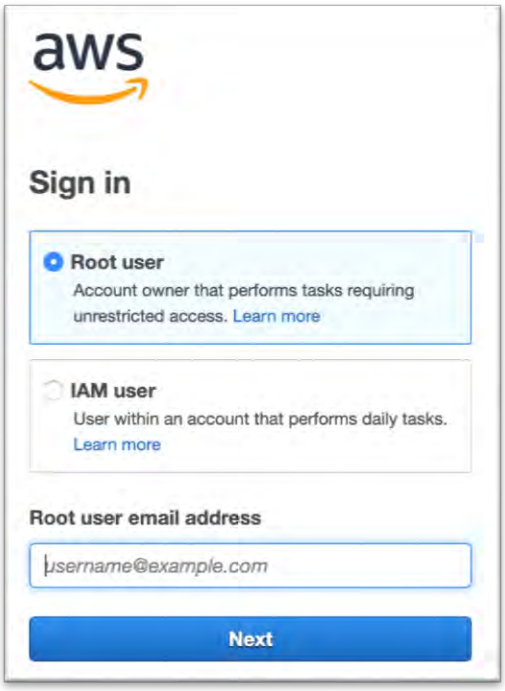
[Done]をクリックします。

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。

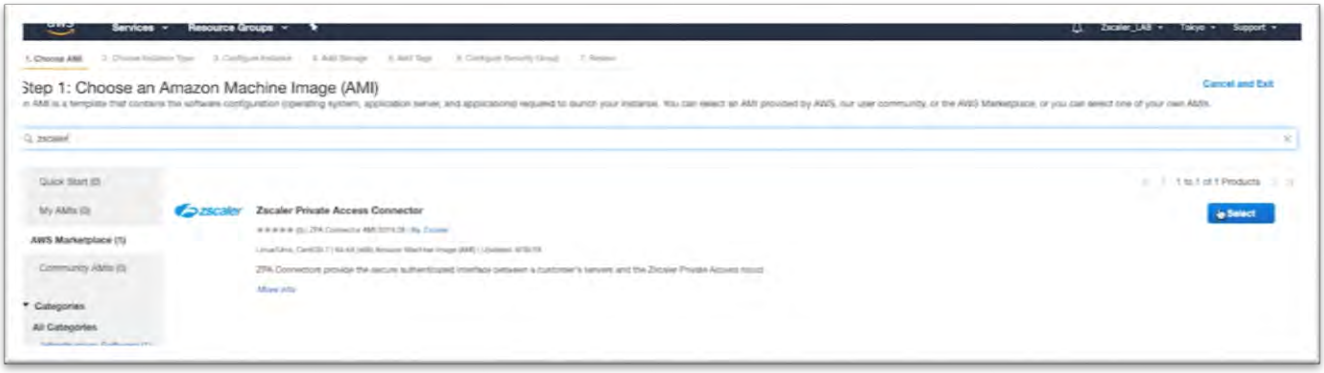


Step2. Connector のインストール

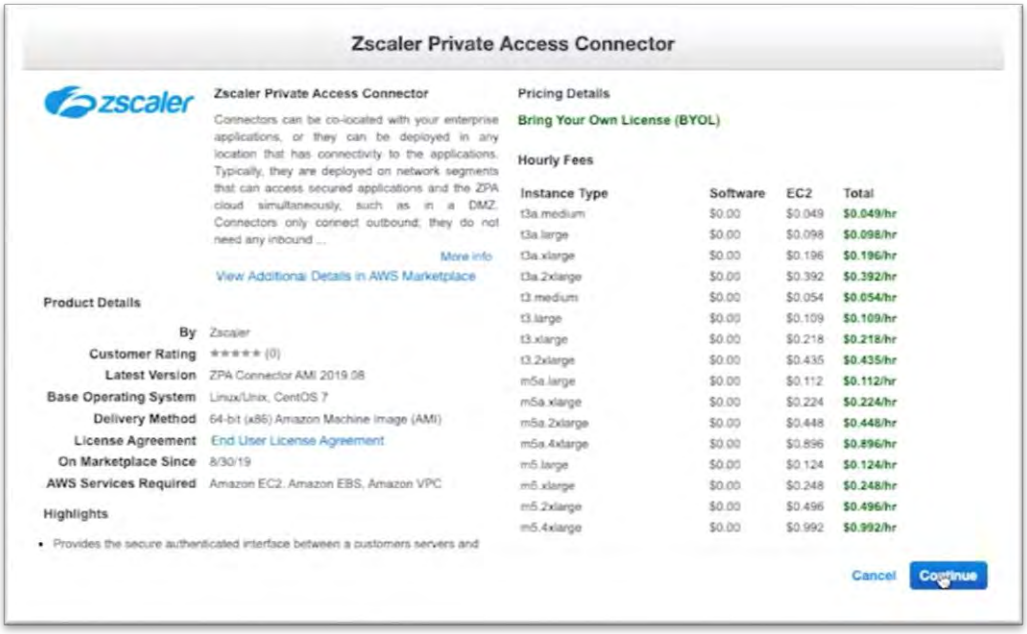
AWS にログインします。



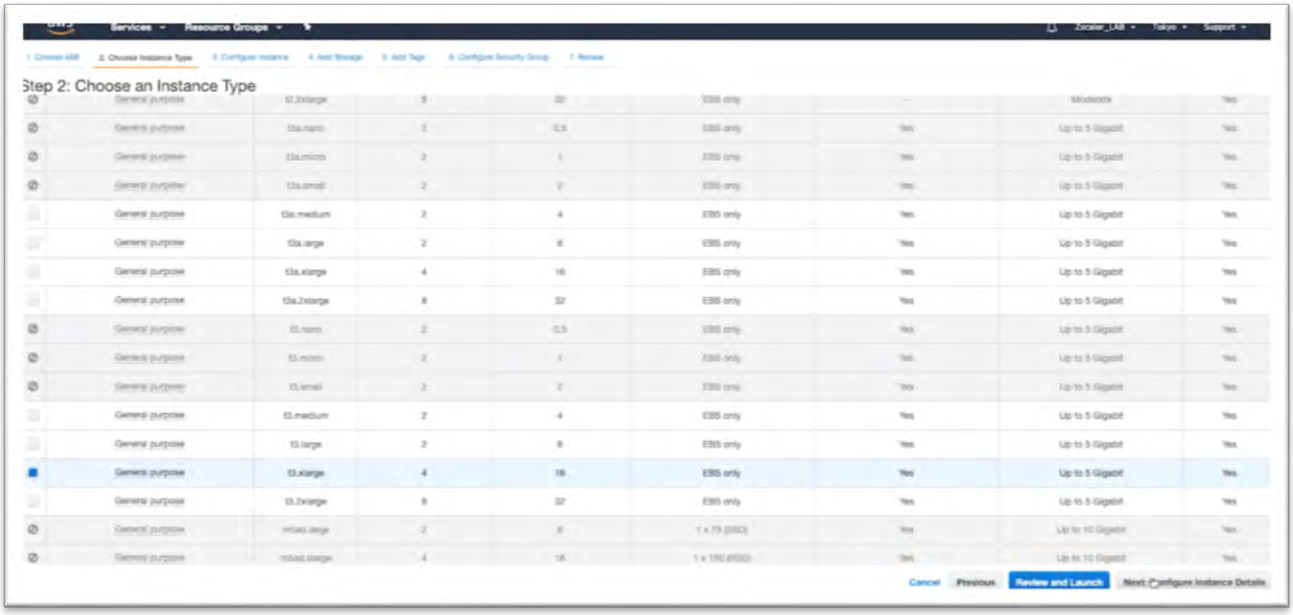
AWS Marketplace より、「Zscaler Private Access Connector」を選択します。



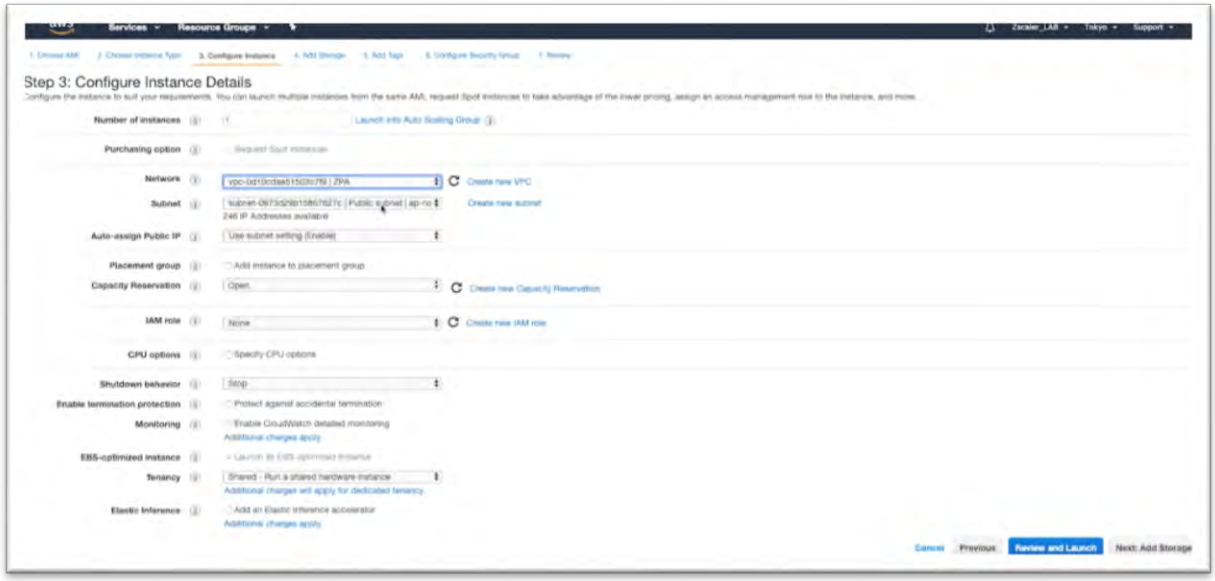
内容を確認して、[Continue] をクリックします。



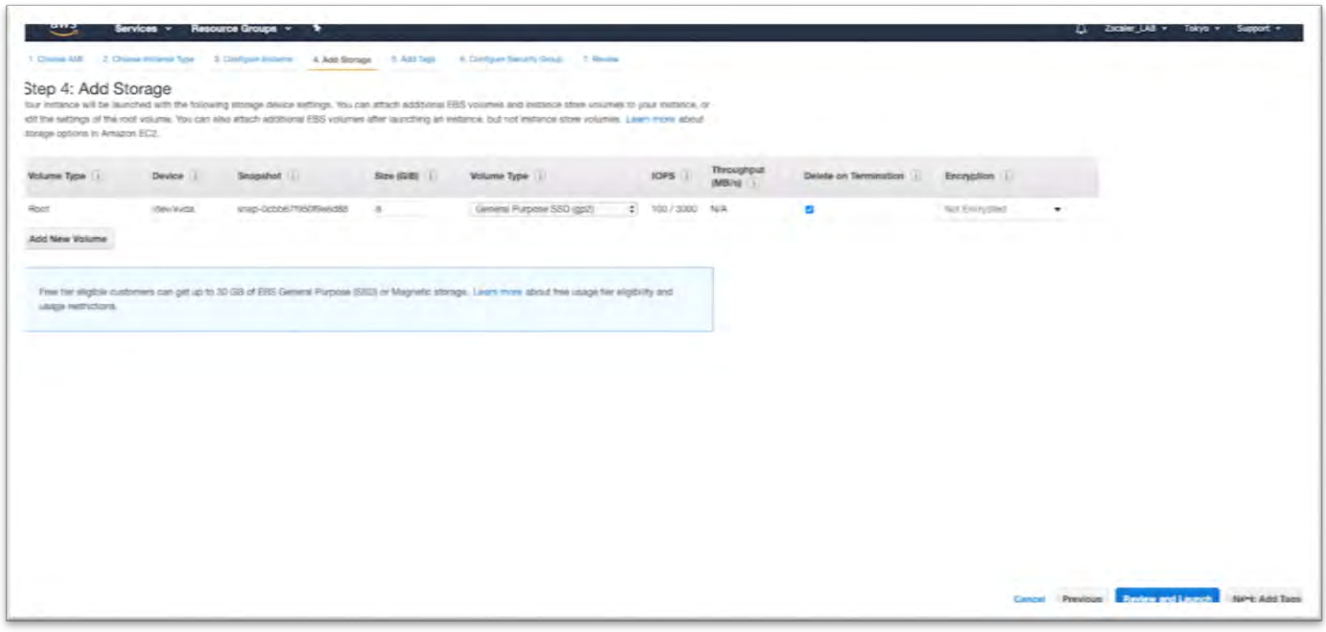
Instance Type は t3.xlarge を選択し、[Next: Configure Instance Details]をクリックします。



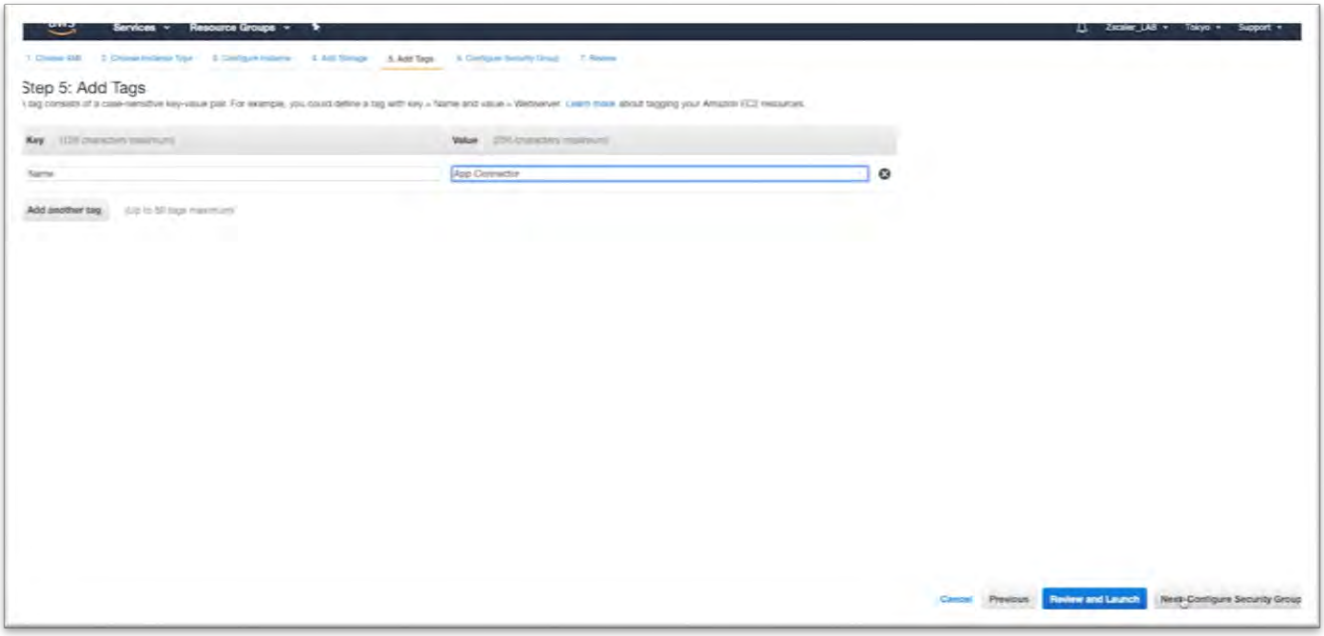
Network を社内リソースがある VPC に変更し、[Next: Add Storage]をクリックします。



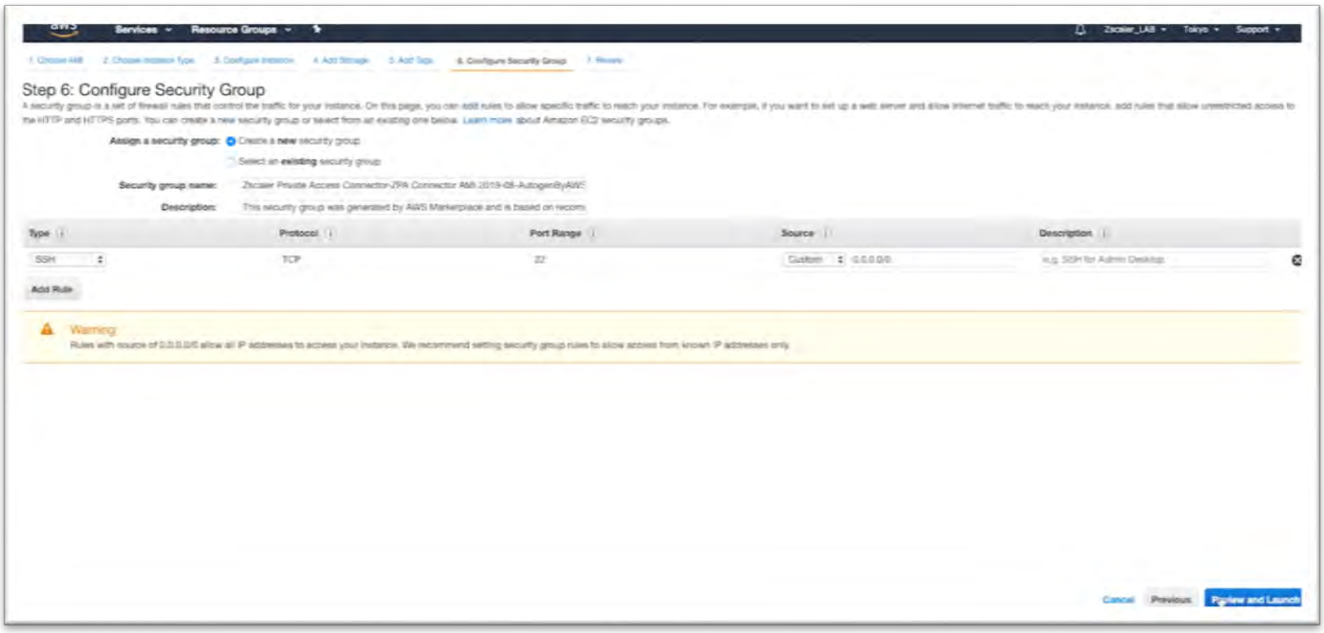
Storage は変更せずに、[Next: Add tags]をクリックします。



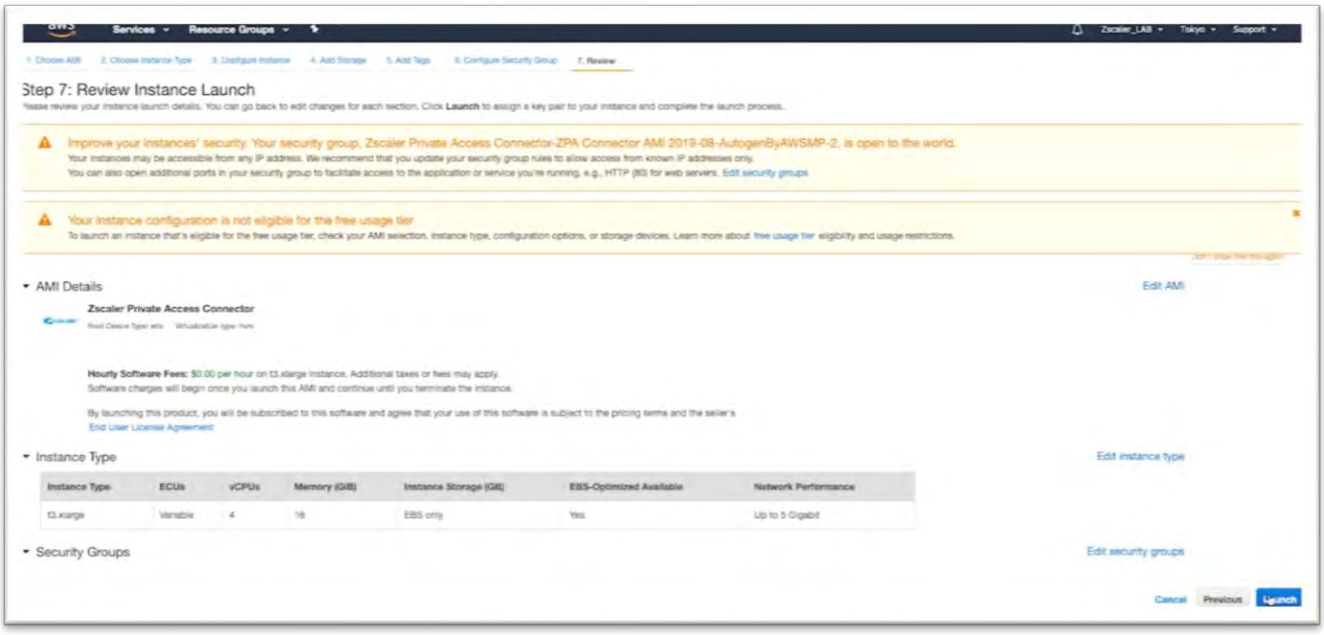
必要に応じてわかりやすいように Tags を作成して、[Next: Configura Security Group] をクリックします。



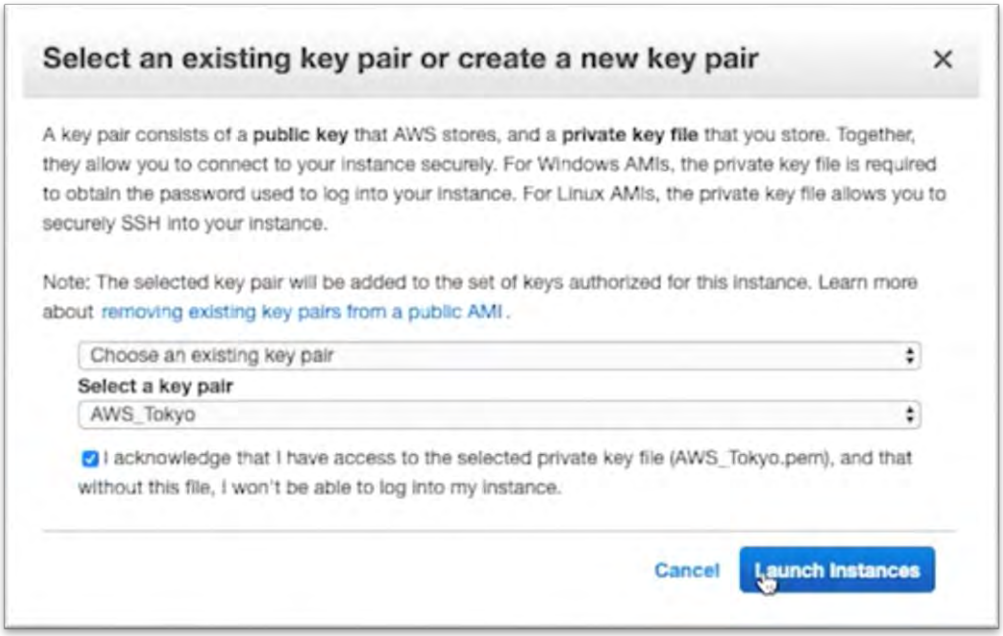
何も変更せずに[Review and Launch]をクリックします。



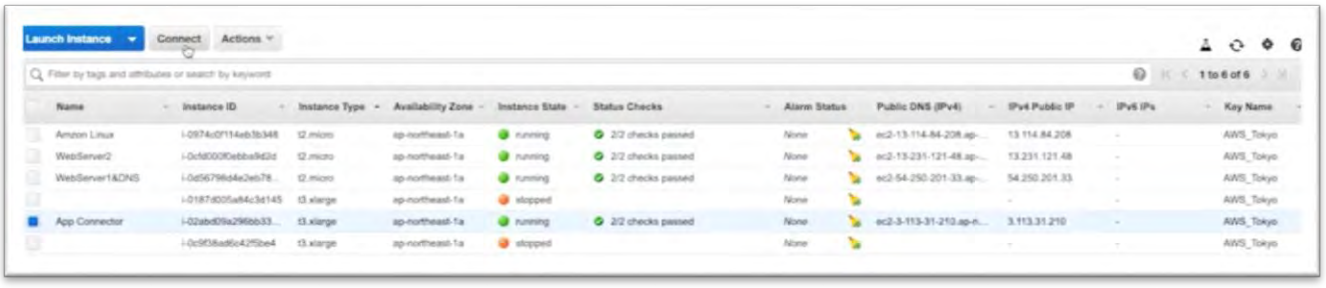
内容を確認して、[Launch]をクリックします。

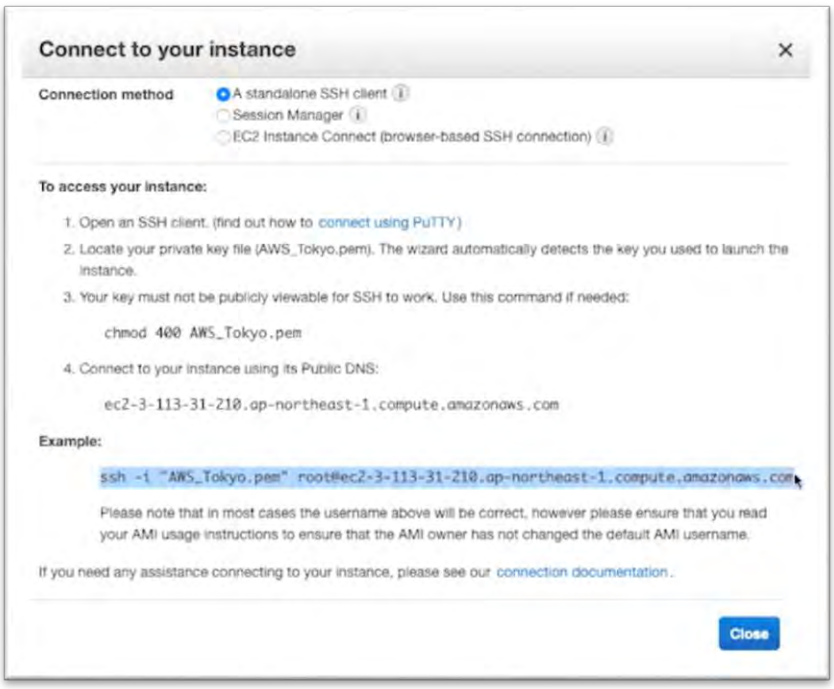


SSH でログインする際に使用する Key Pair を選択し、[launch Instances]をクリックします。



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）。



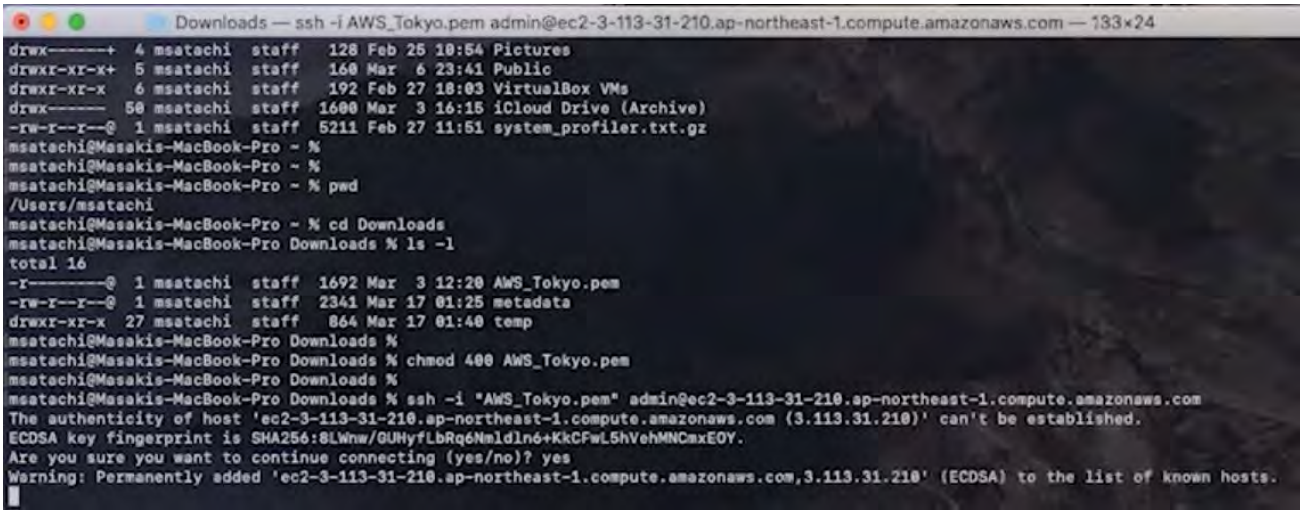


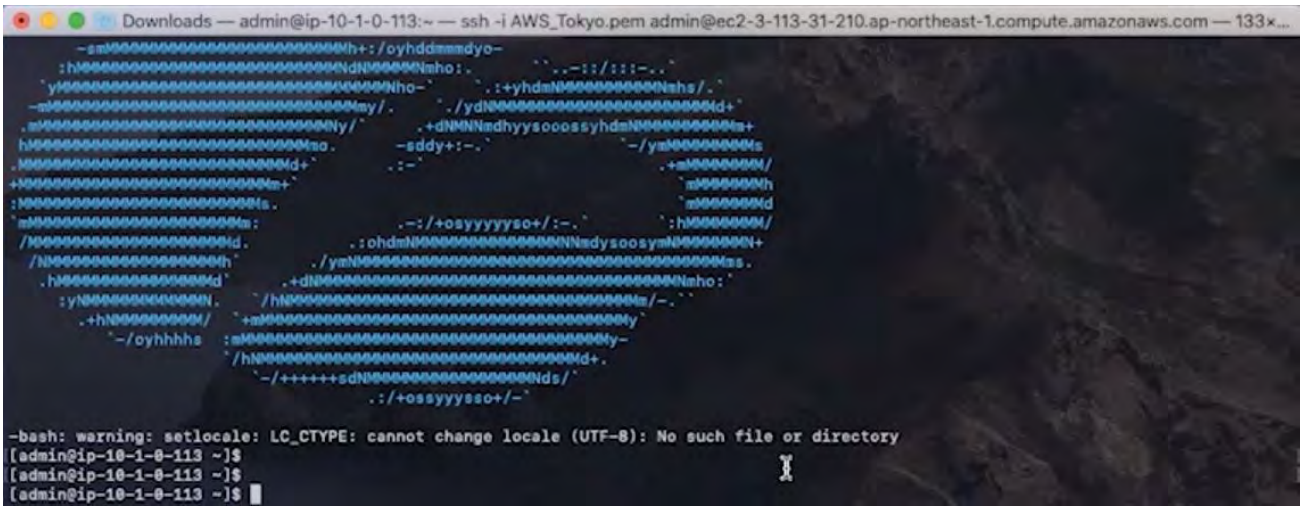
ターミナルソフトより、使用する Key Pair の権限を変更し、SSH で Connector にログインします。

コマンド例）

chmod 400 AWS_Tokyo.pem

ssh -i "AWS_Tokyo.pem" admin@ec2-x-xxx-xx-xx.ap-northeast-1.compute.amazonaws.com





ログインが成功したら、以下のコマンドを実行します。

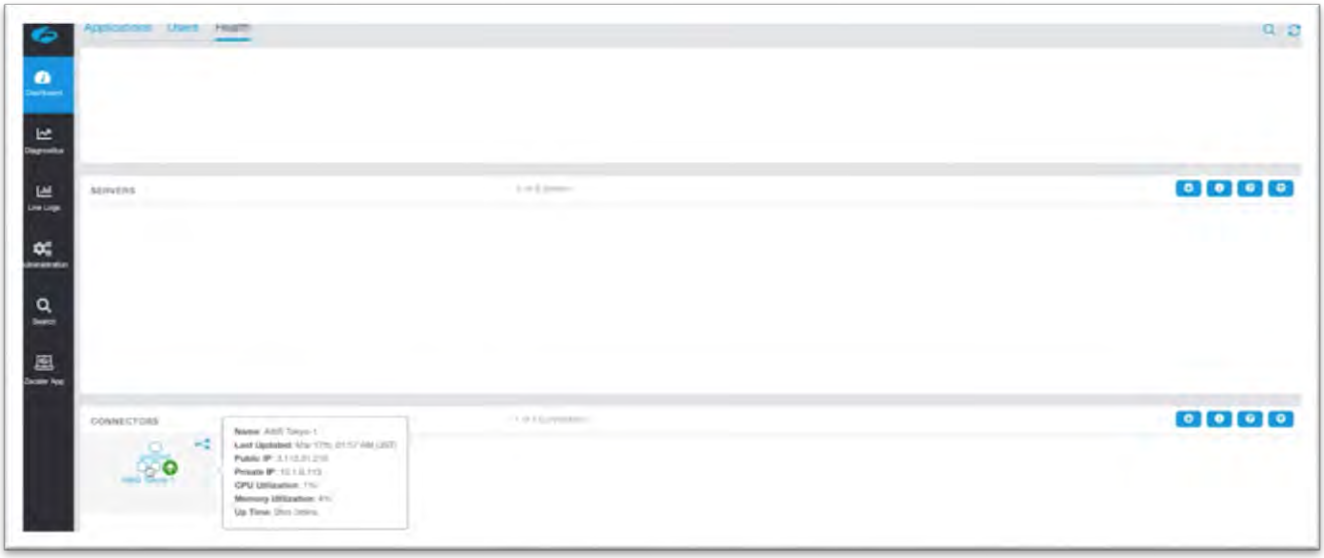
1. sudo systemctl stop zpa-connector
2. sudo touch /opt/zscaler/var/provision_key
3. sudo chmod 644 /opt/zscaler/var/provision_key
4. sudo vi /opt/zscaler/var/provision_key

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。

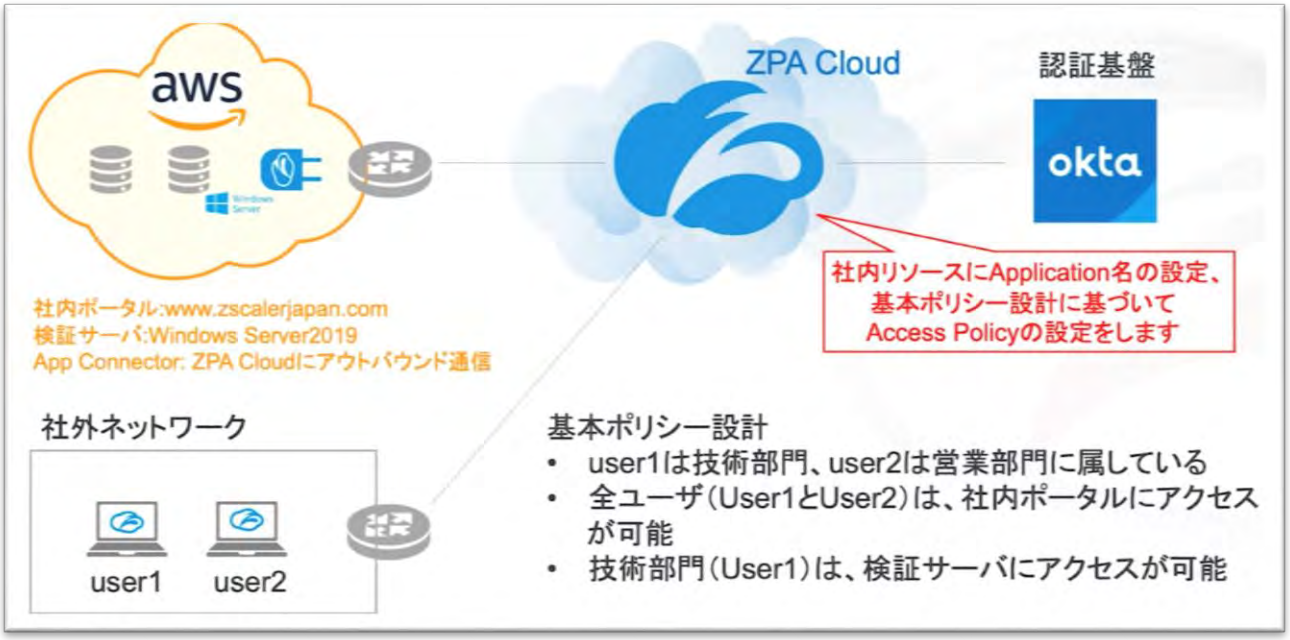
5. sudo cat /opt/zscaler/var/provision_key
6. sudo systemctl start zpa-connector

コマンドの実行が完了したら、Connectors に情報が表示されるようになります。

また、Dashboard -> Health より Connector のワークロードが確認できます。

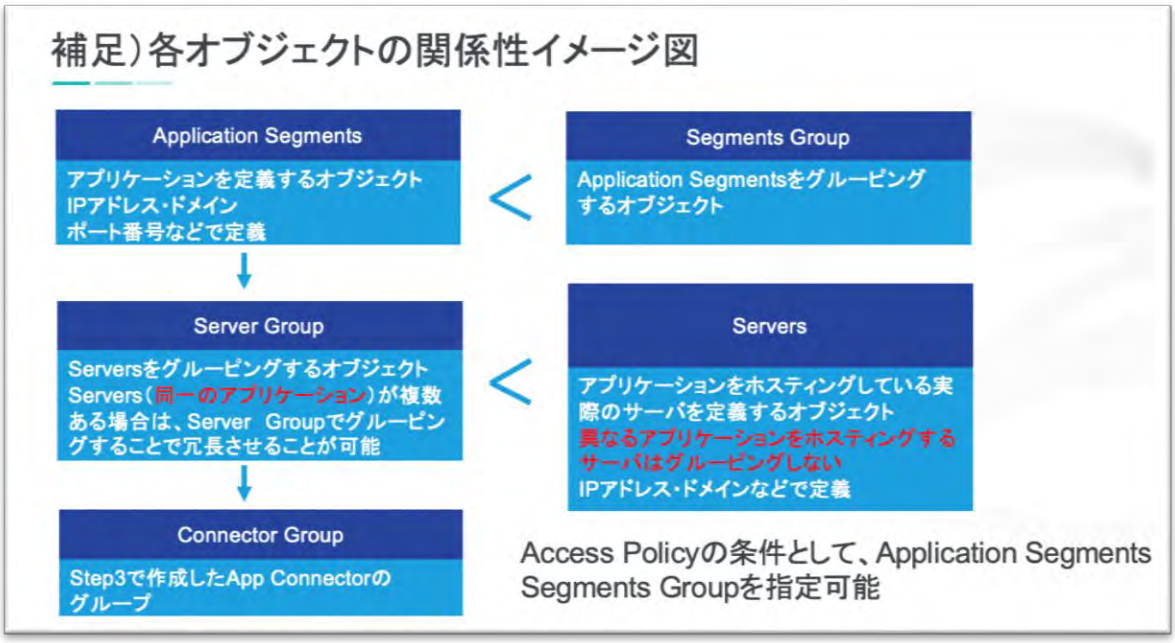


3-4. Application Segmentation / Access Policy の設定



Notes

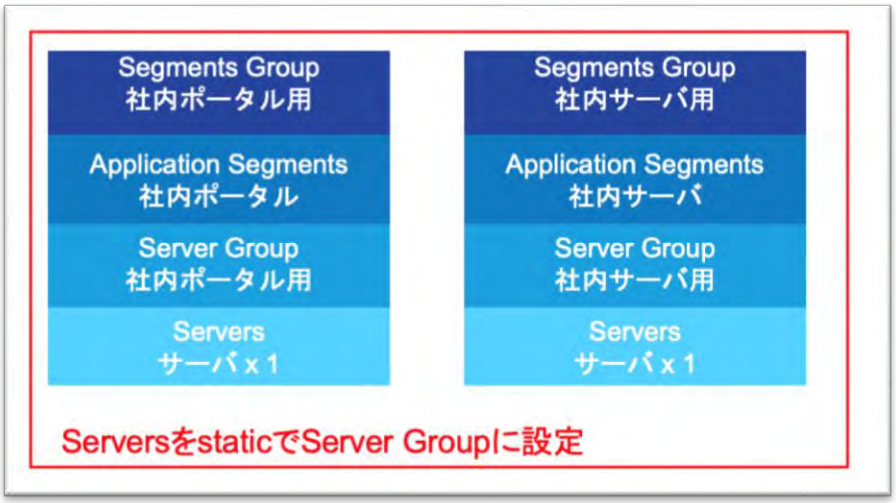
✓ 本手順で作成するオブジェクトの関係性イメージ図



✓ 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

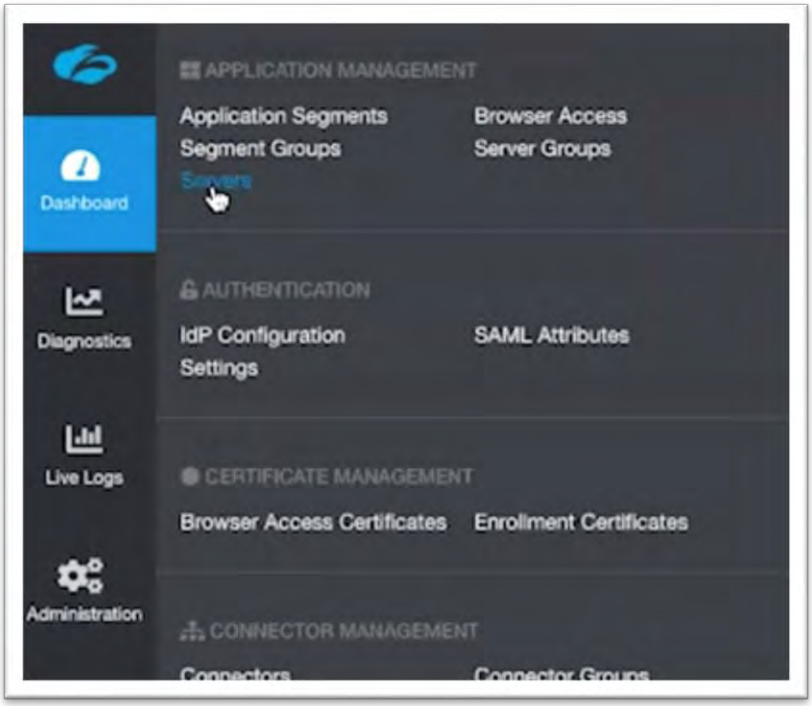


✓ 社内アプリへアクセスが発生した際の内部処理イメージ

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。

必要事項を記入、設定し [Save] をクリックします。

++

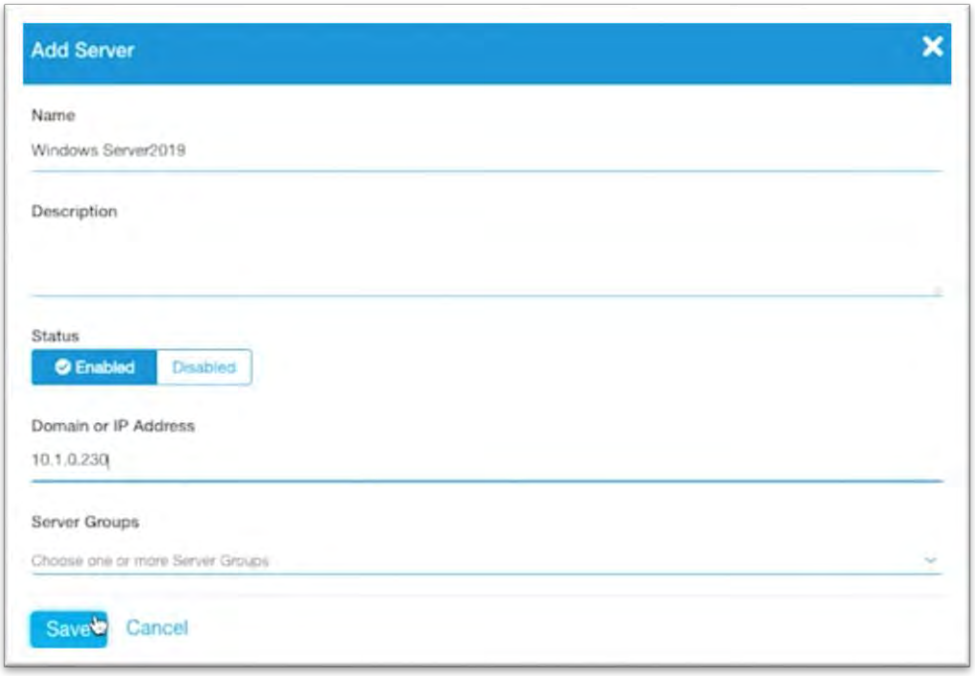
Name: 任意の名前

Status: Enabled

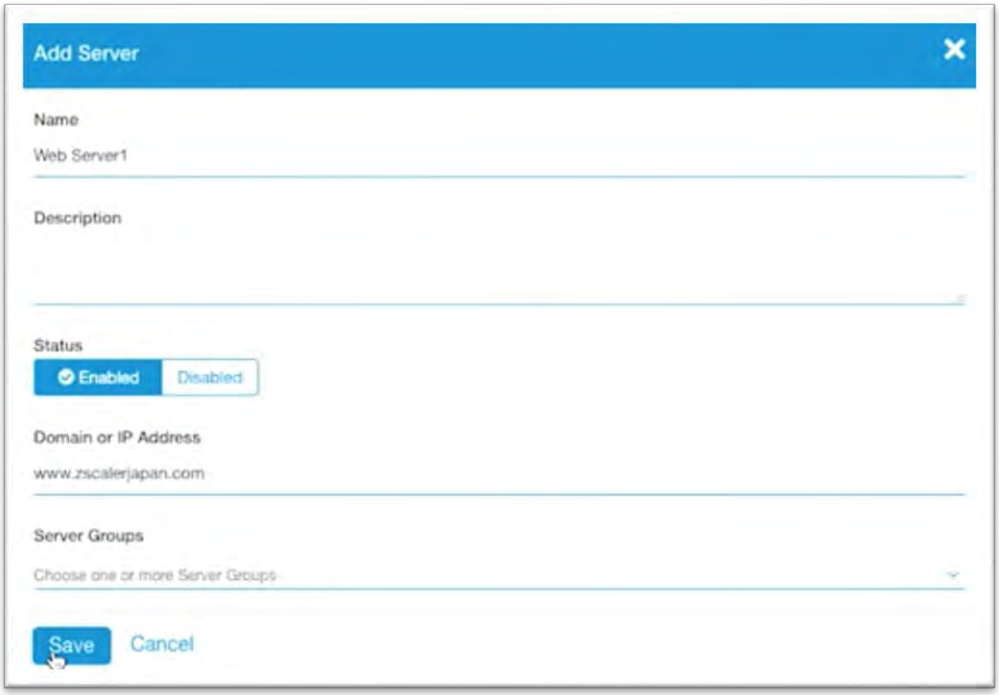
Domain or IP Address: ドメイン名 or IP アドレス

++

社内サーバの設定例



社内ポータルの設定例



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

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

Status: Enabled

Dynamic Server Discovery: Off（※）

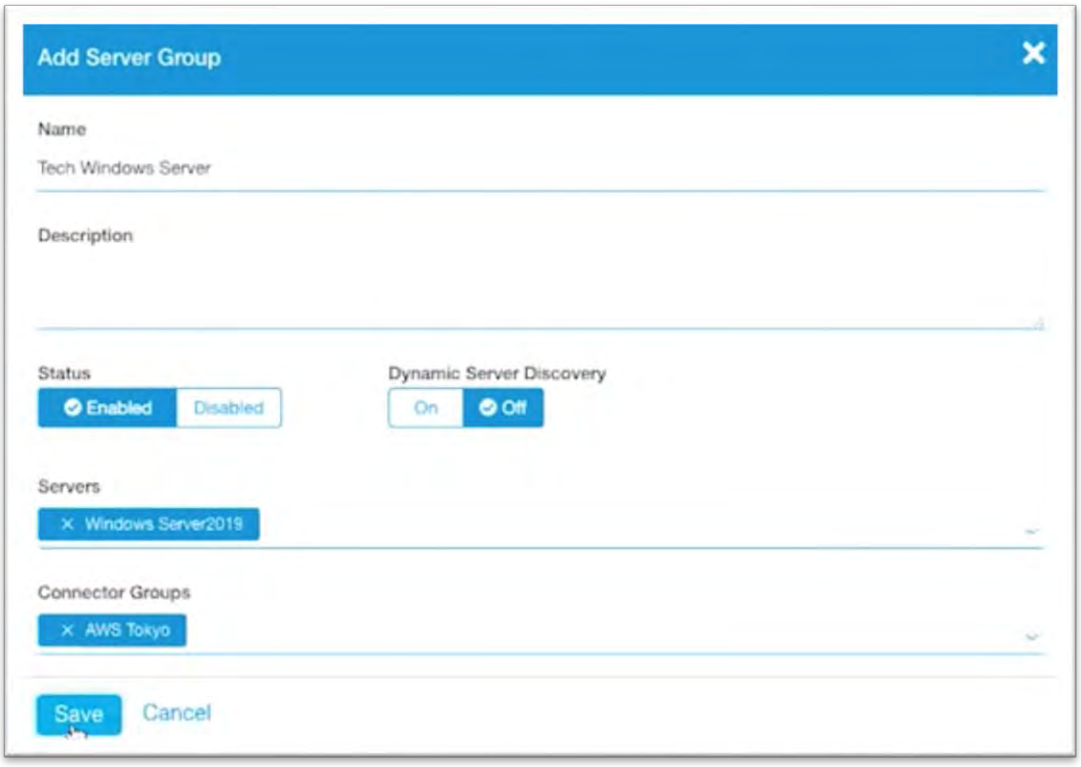
Servers: グルーピングする Servers を選択

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

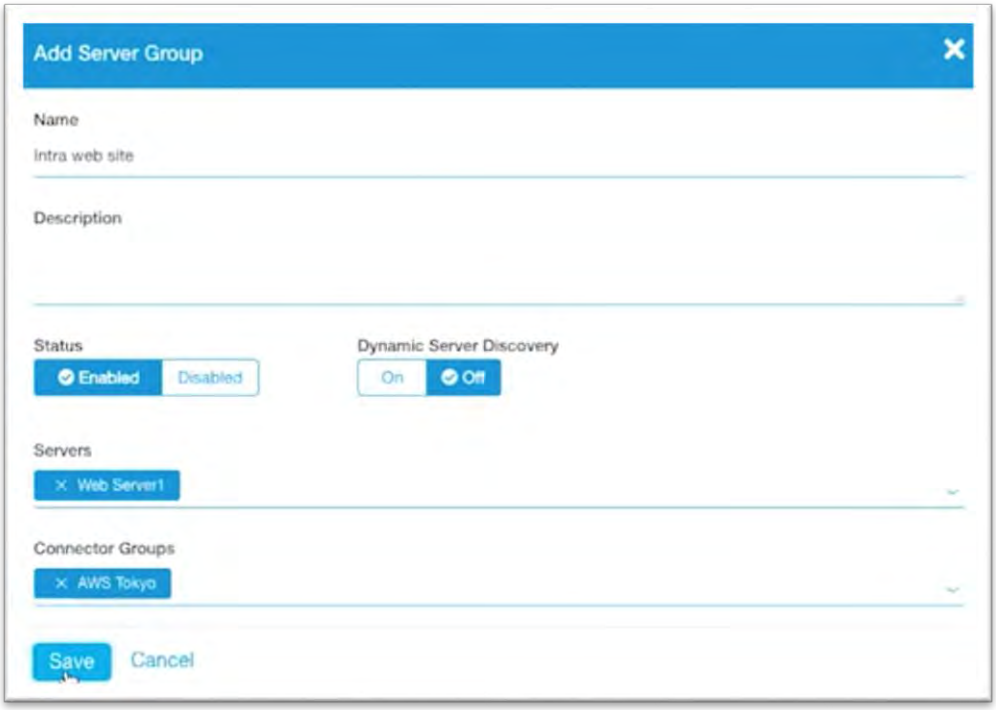
++

※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



社内ポータルの設定例



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。

++

Name: 任意の名前

Status: Enabled

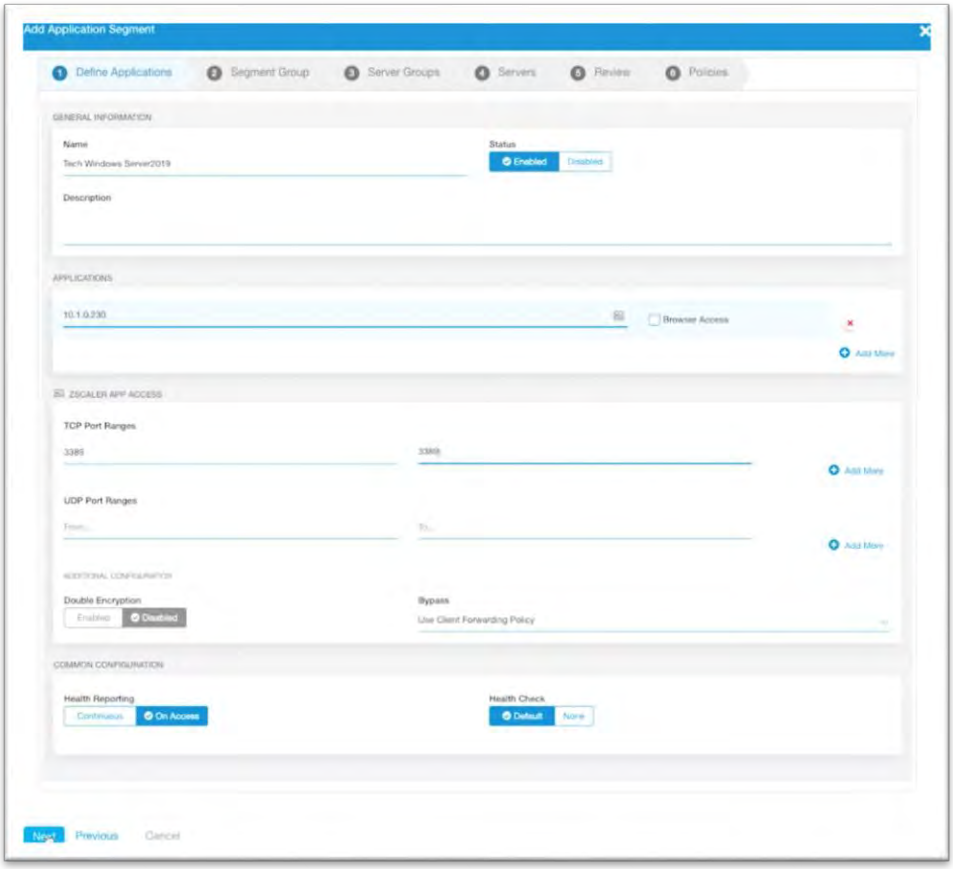
APPLICATIONS: ドメイン名 or IP アドレス

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



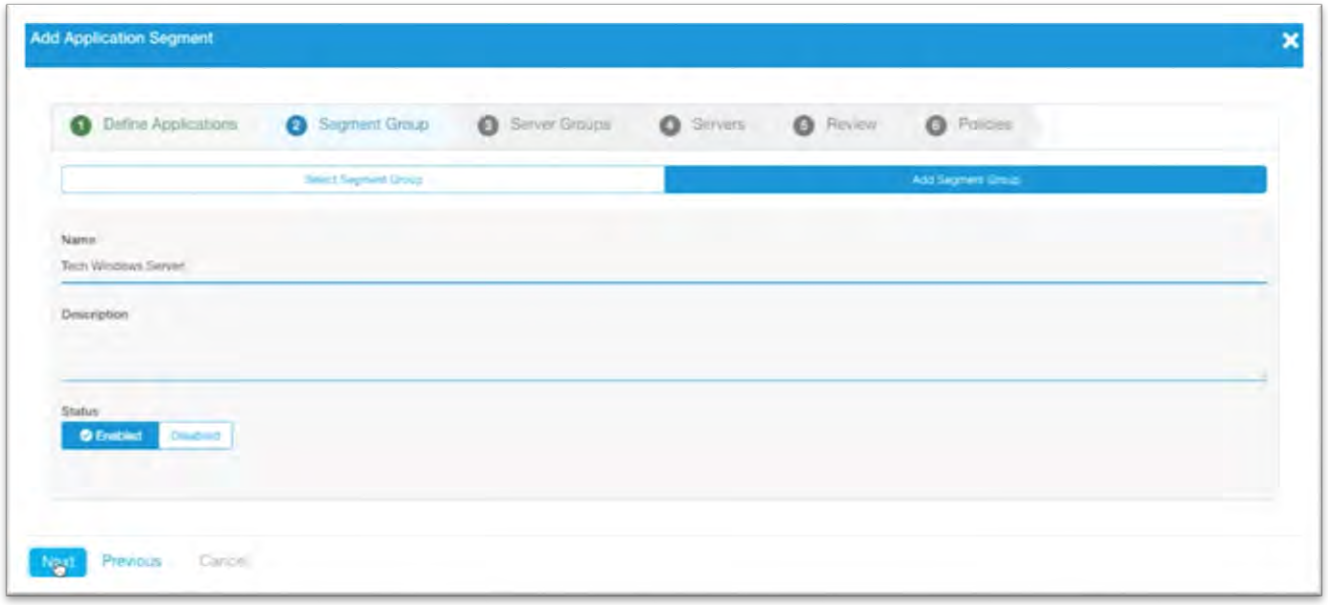
Add Segment Group を選択し、必要事項を記入、設定し [Next] をクリックします。

++

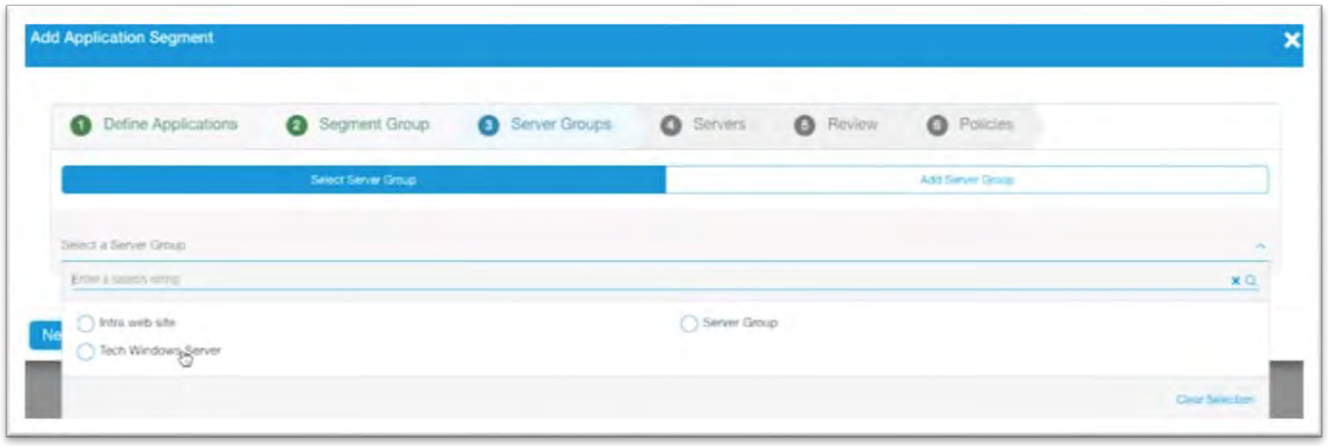
Name: 任意の名前

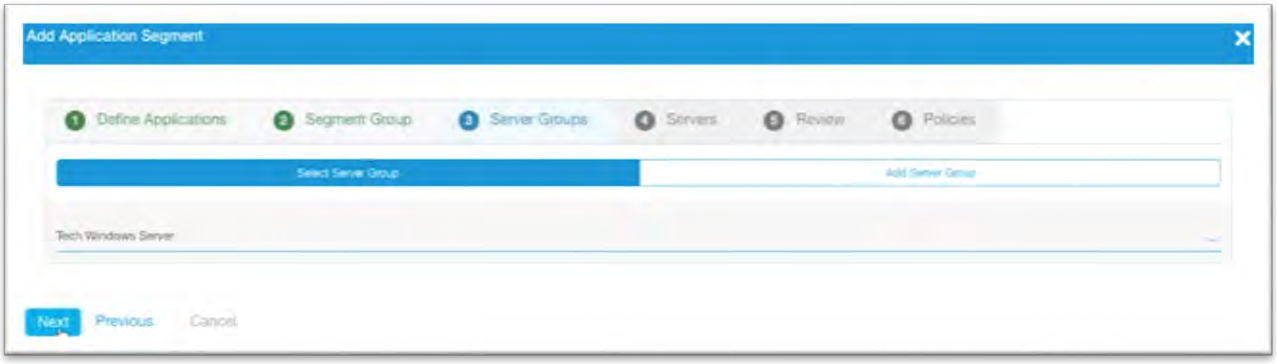
Status: Enabled

++

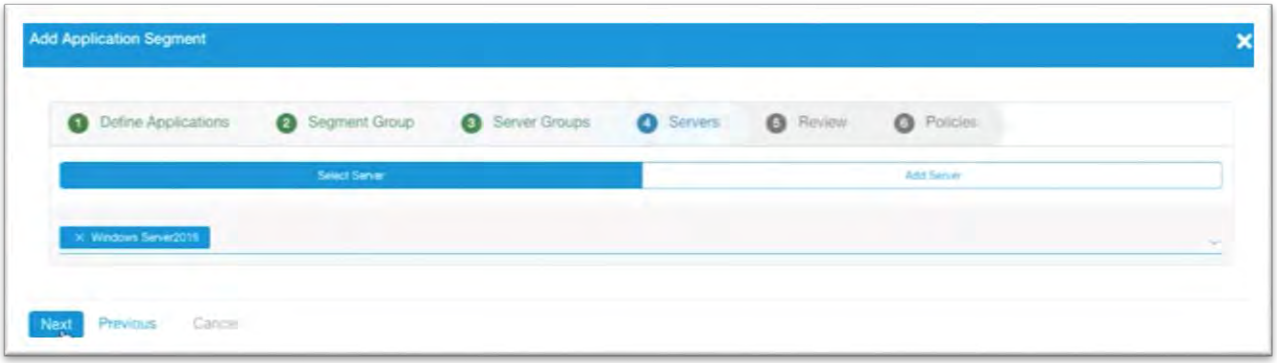


Step1 で作成した Application Segments に対応する Server Group を選択し、[Next]をクリックします。

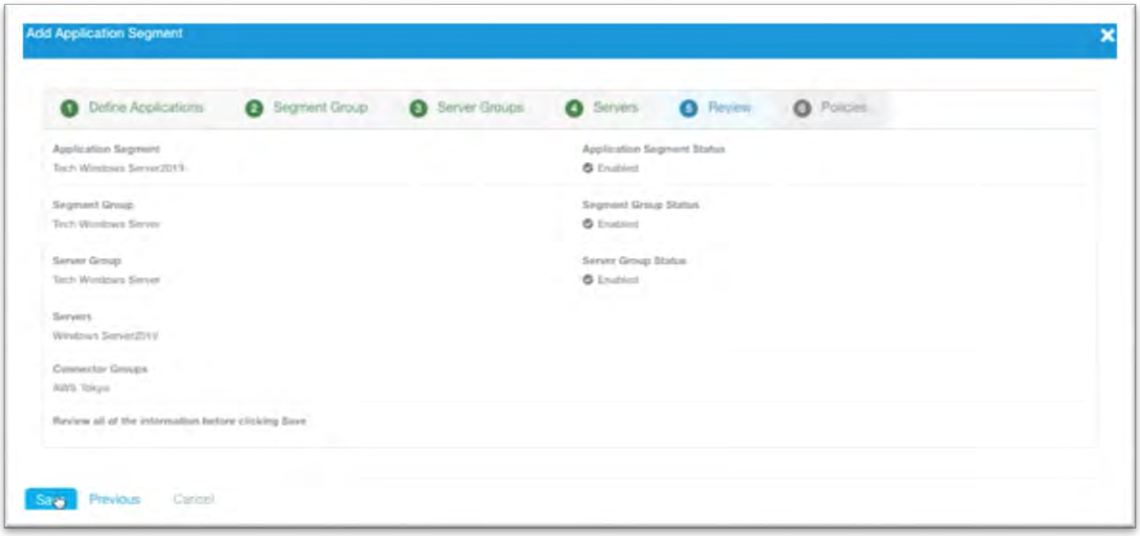




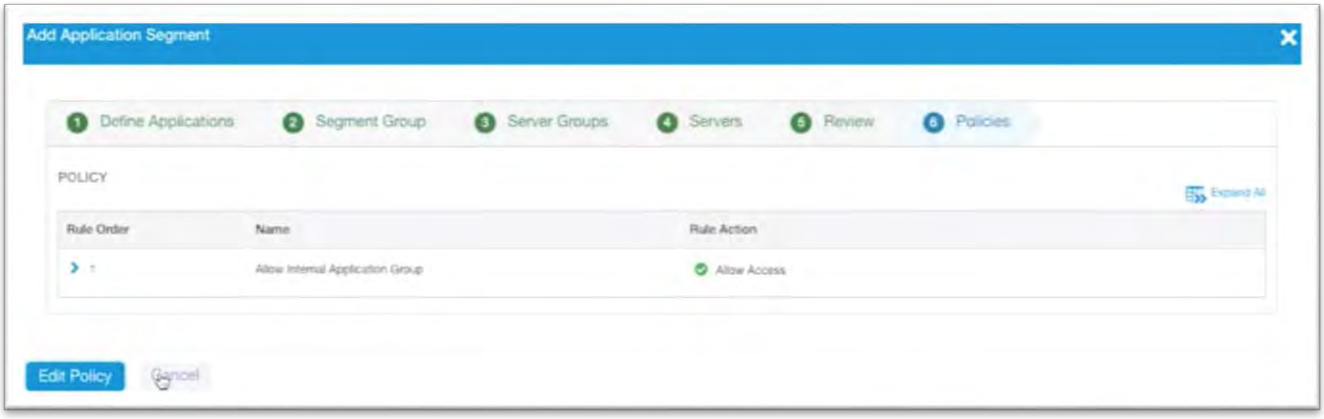
Server Groups に紐づいている Servers を確認して、[Next]をクリックします。



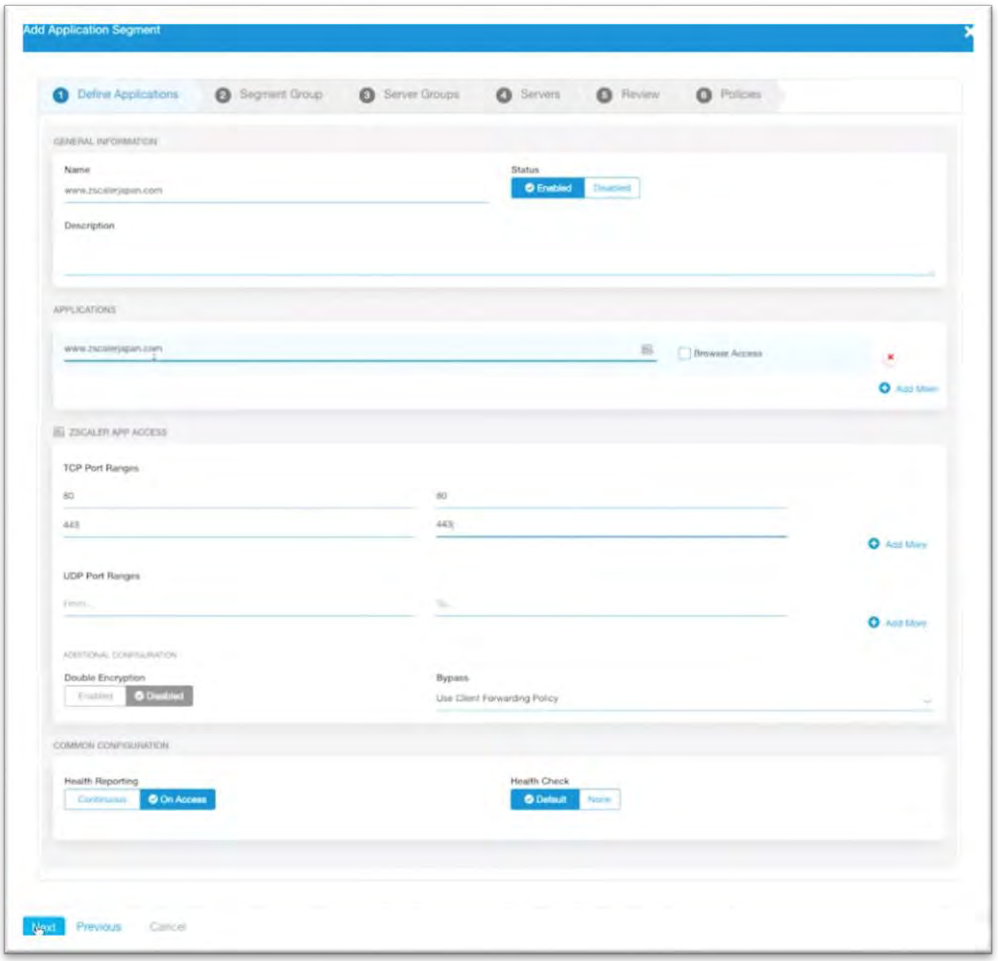
内容を確認して[Save]をクリックします。

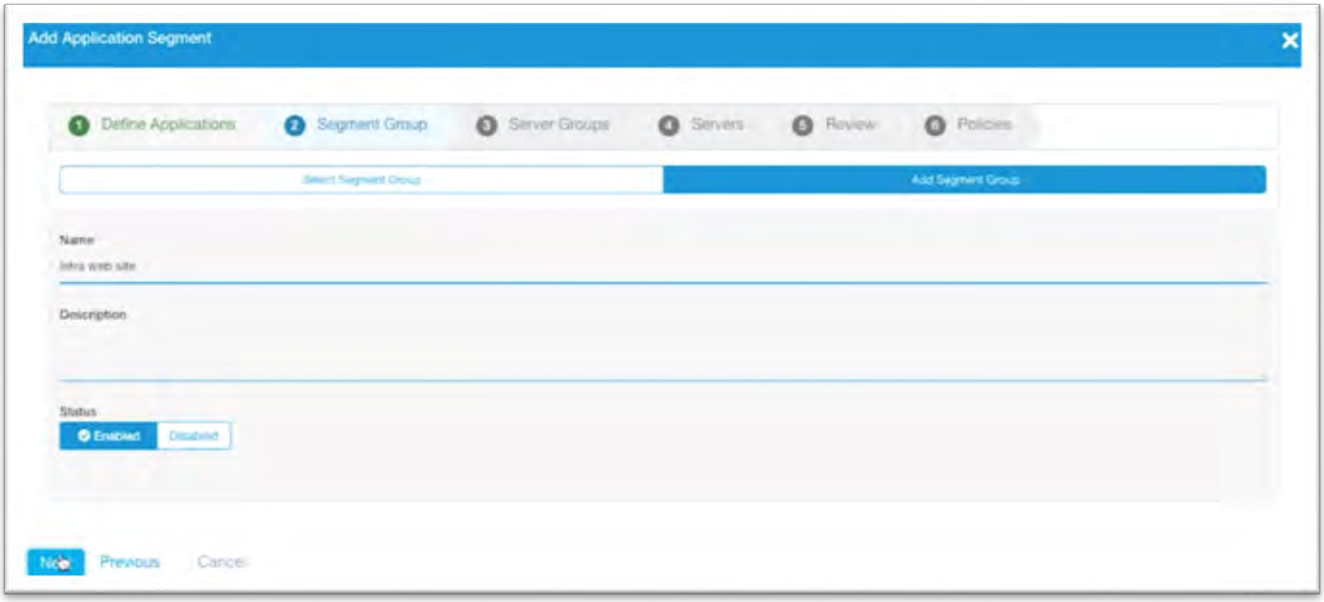


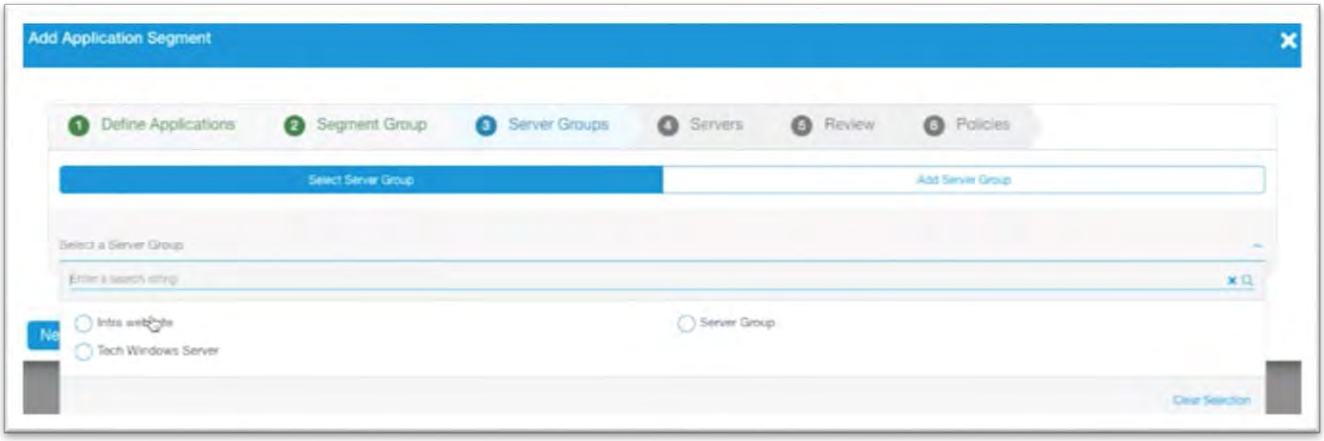
Access Policy は後で設定するので、[Cancel]をクリックします。

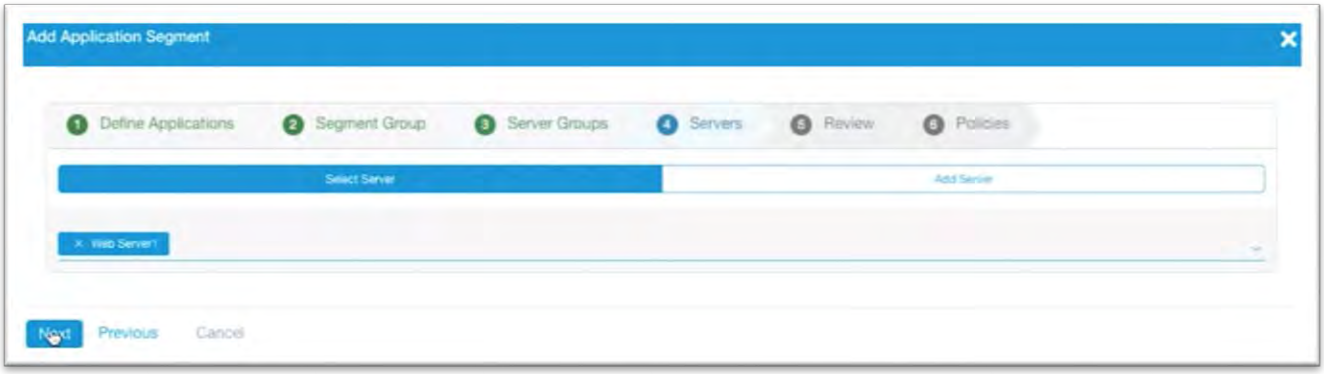


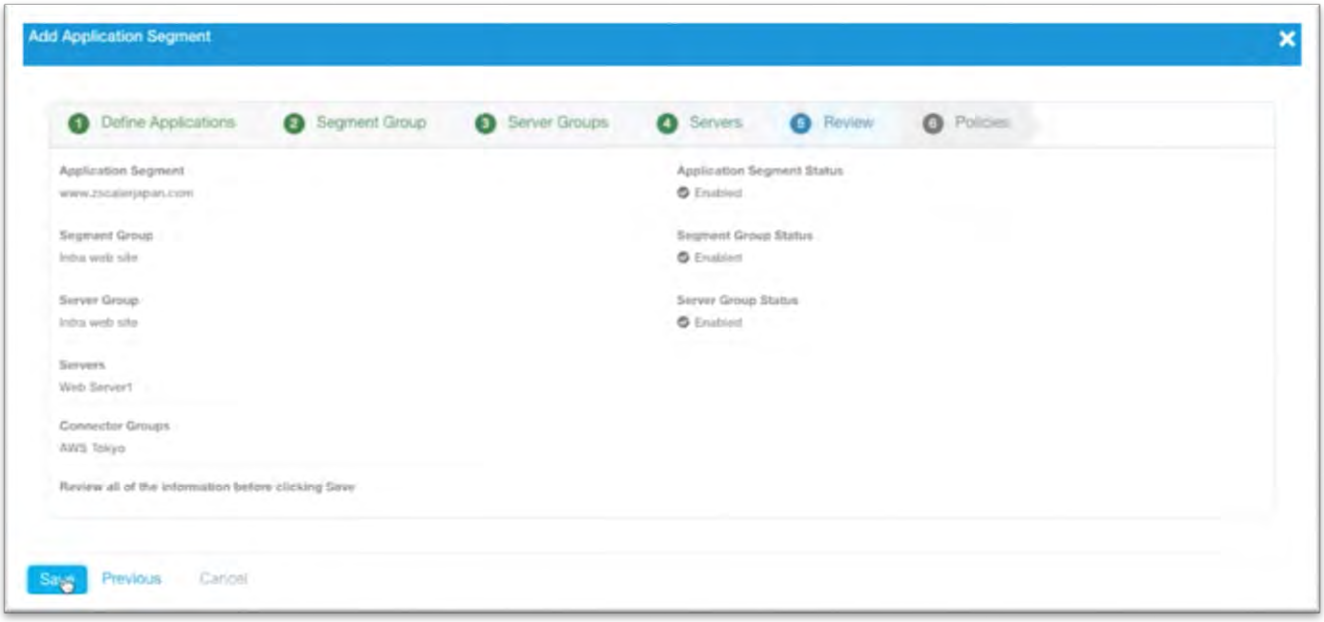
社内サーバの設定例





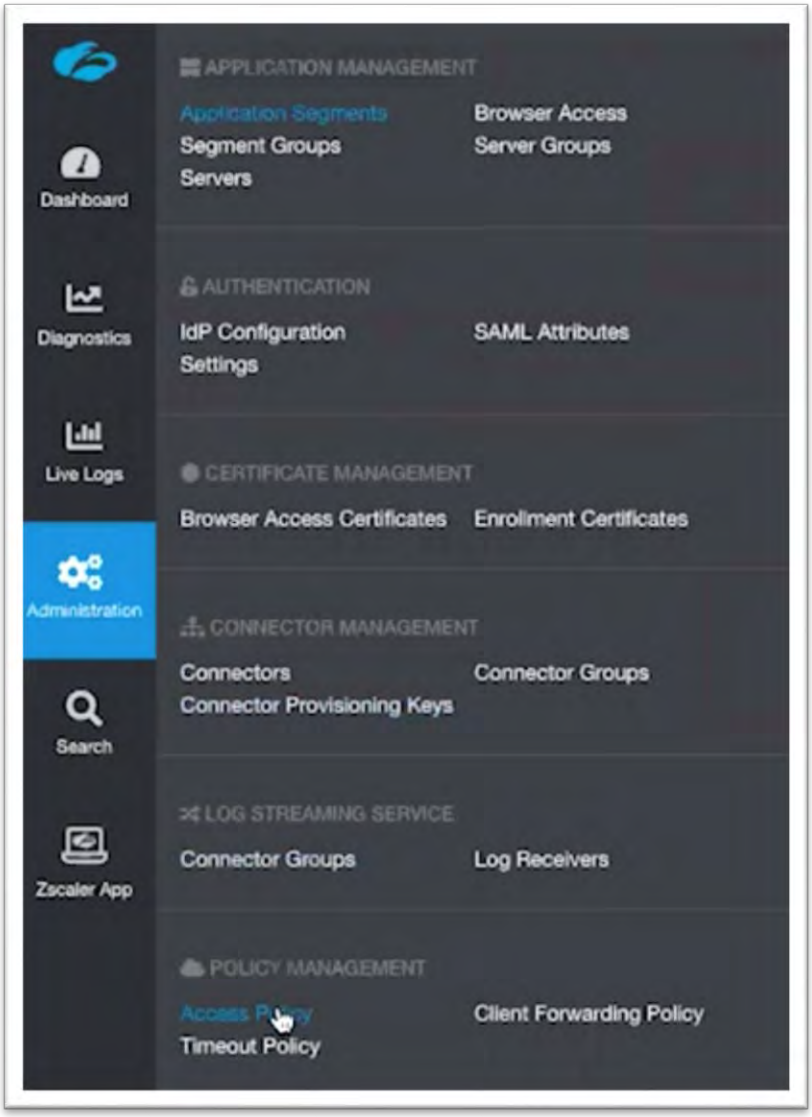


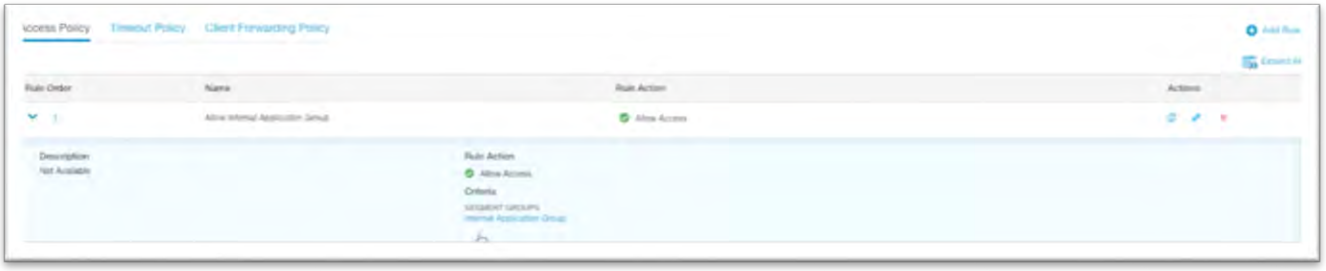




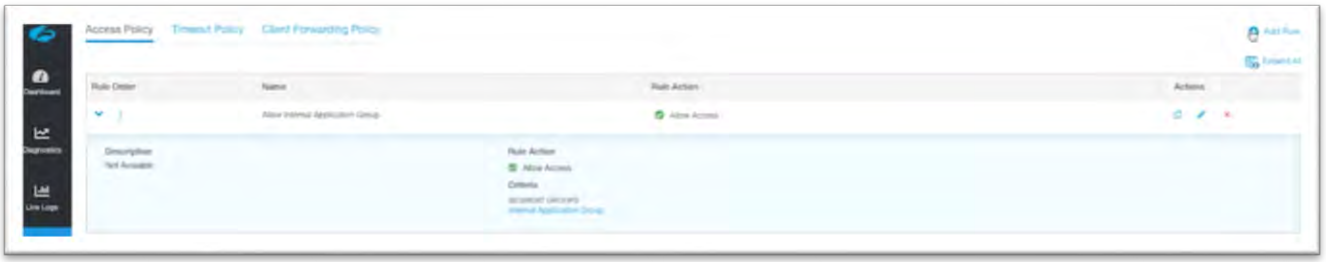
Step3. Access Policy の作成

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





[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

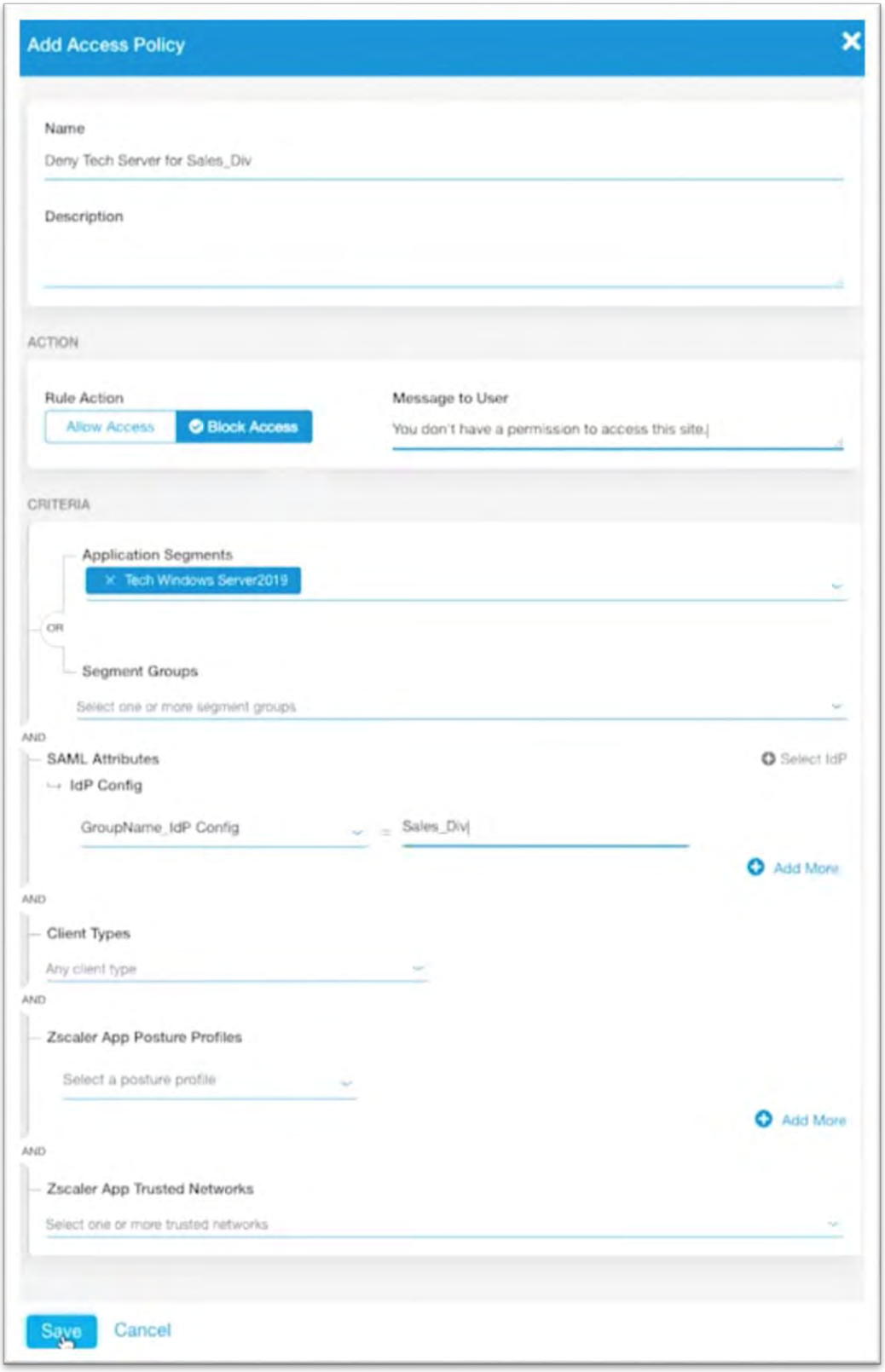
Application Segments: Tech Windows Server2019（※1）

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



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

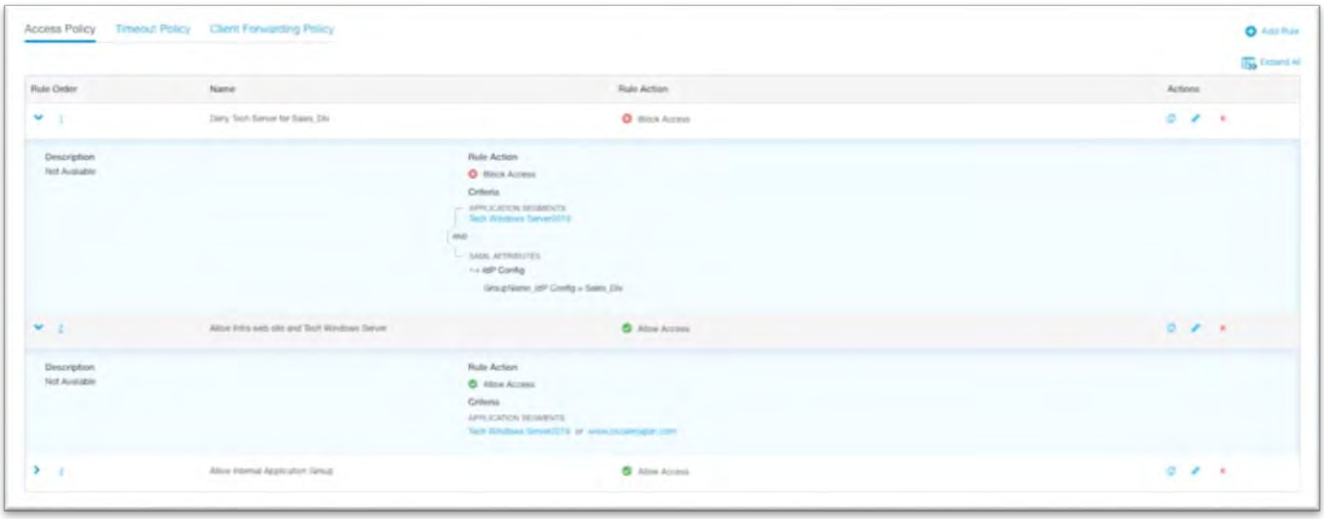
Application Segments: Tech Windows Server2019、www.zscalerjapan.com（※1）

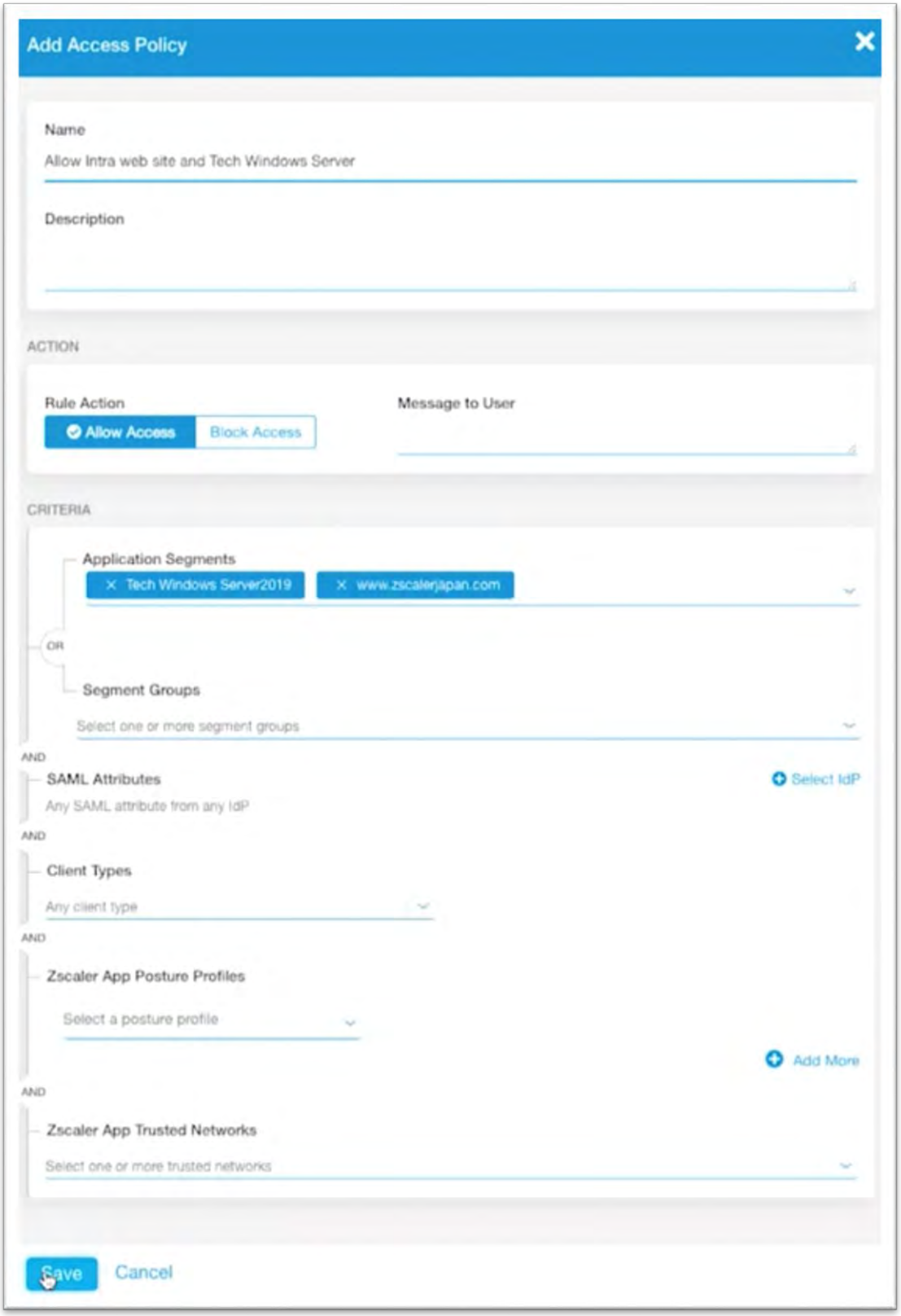
SAML Attributes: なし（※2）

++

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

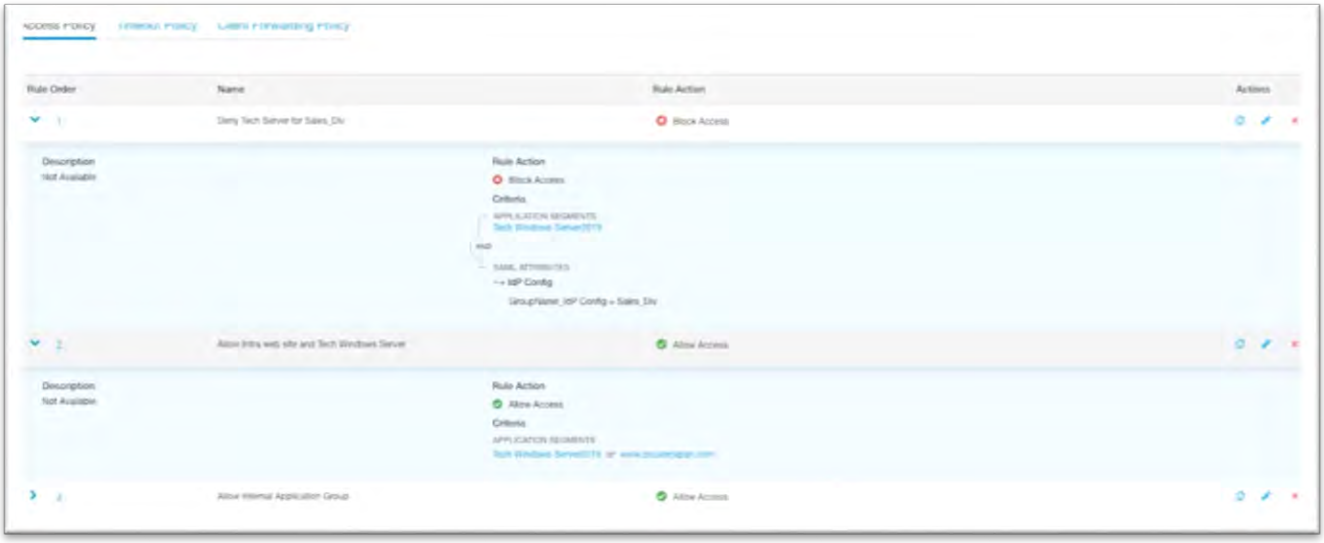
※2　全員（技術部門、営業部門）という条件なので、SAML Attributes は設定しません



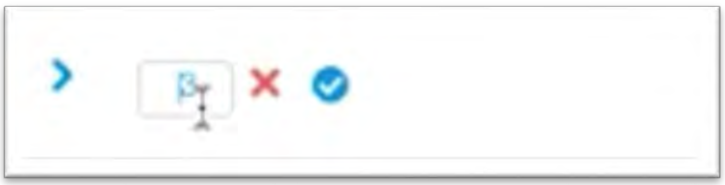


Access Policyの精査は上から順に評価され、マッチしたポリシーが適応されます。
その後のポリシーの評価はされません。
このため、想定した動作のためにはポリシーの順番を考慮する必要があります。
例）

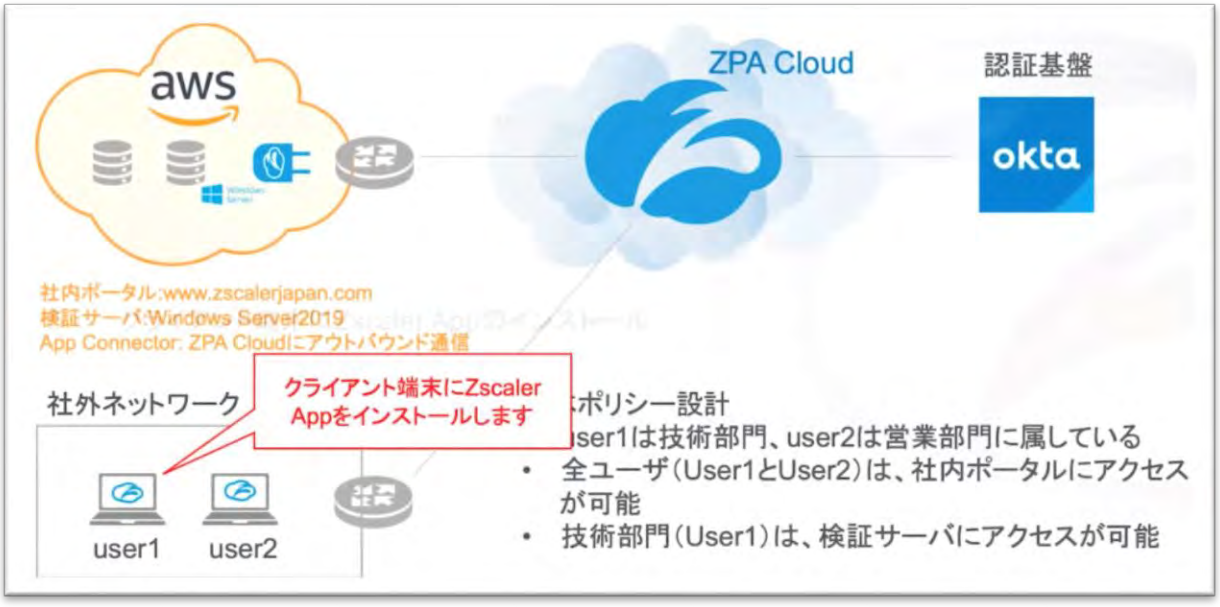
User	アクセス先	適応ポリシー	アクション
営業部門	社内ポータル	No2	Allow
営業部門	社内サーバ	No1	Deny
技術部門	社内ポータル	No2	Allow
技術部門	社内サーバ	No2	Allow



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。

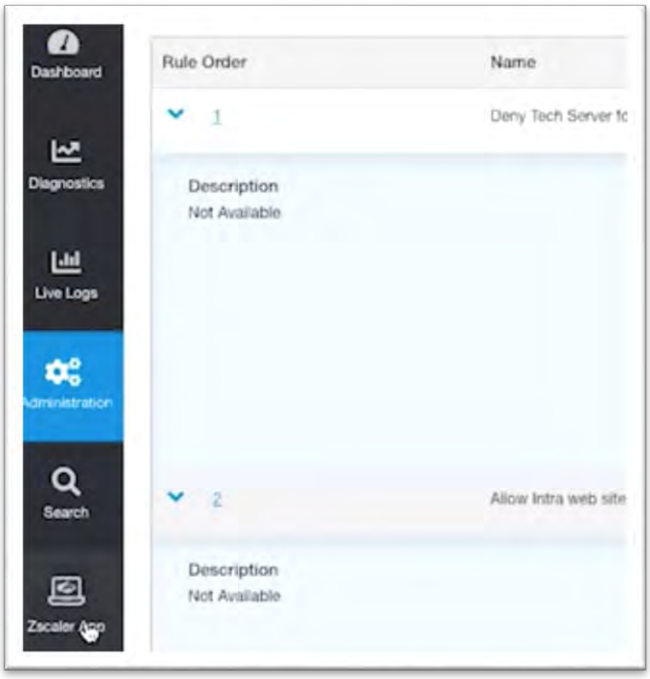


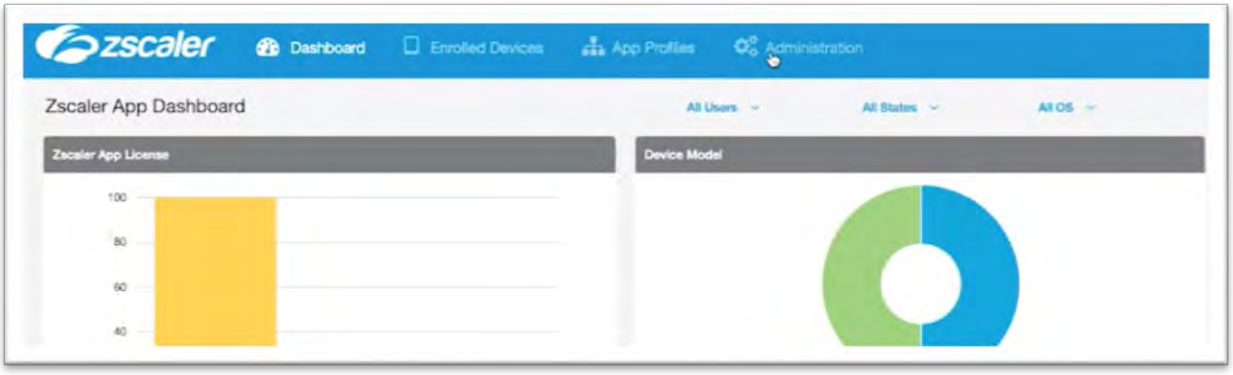
3-5. Zscaler App のインストール

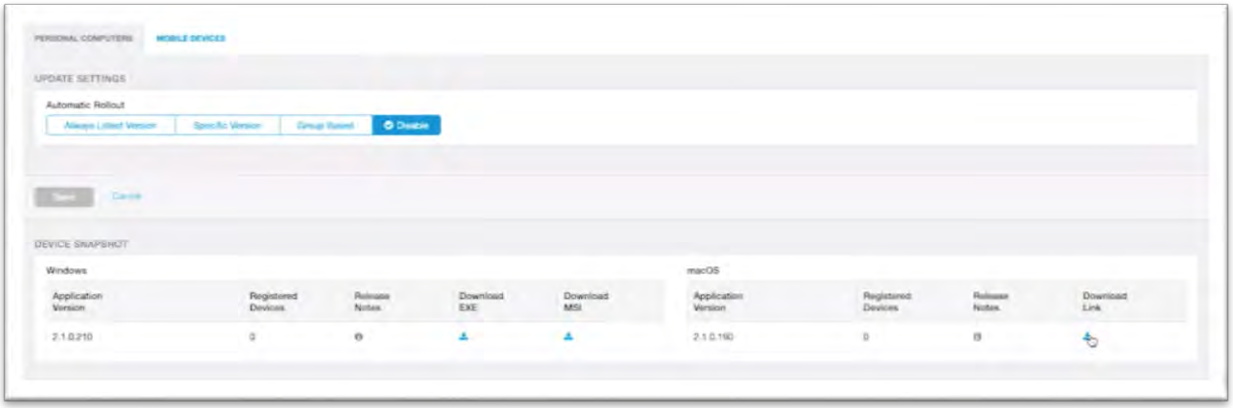


Step1. ZscalerApp のインストーラーダウンロード

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

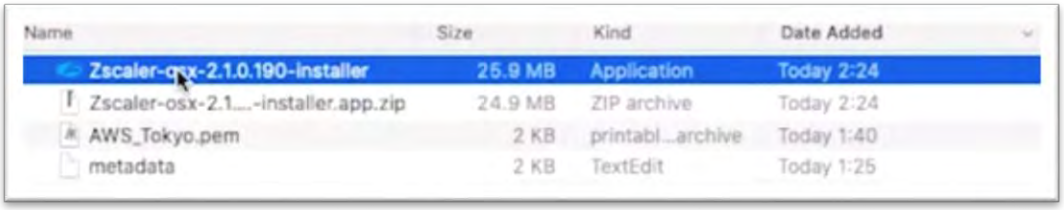


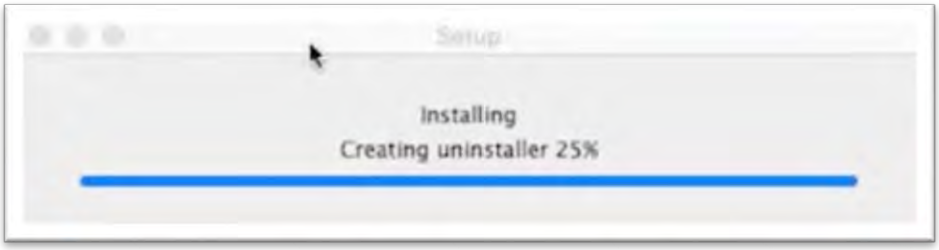


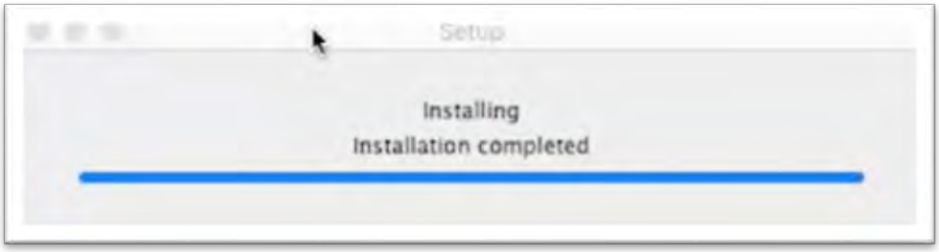


Step2. ZscalerApp のインストール

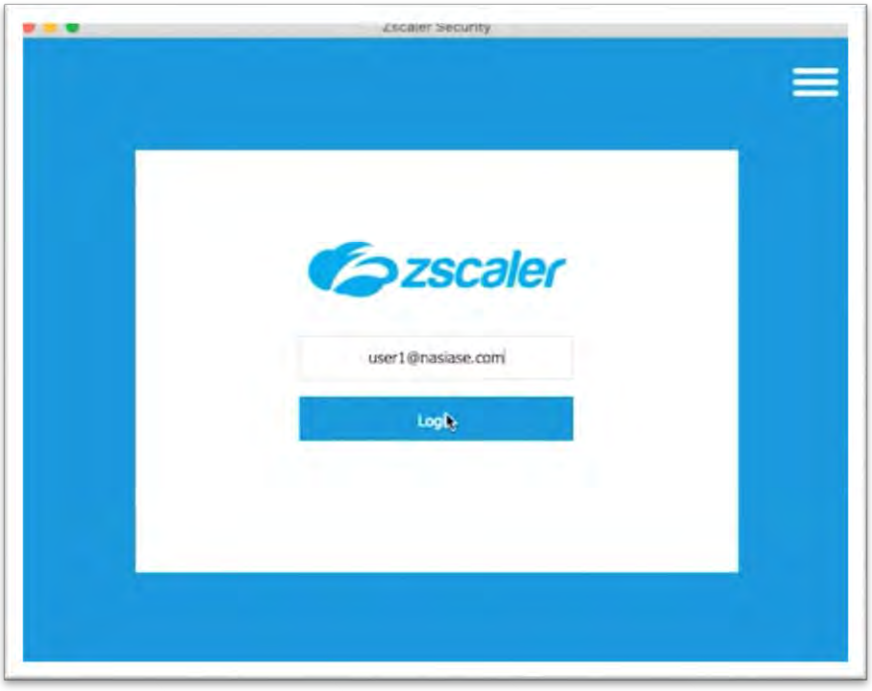
ダウンロードしたインストーラーを PC で実行します。



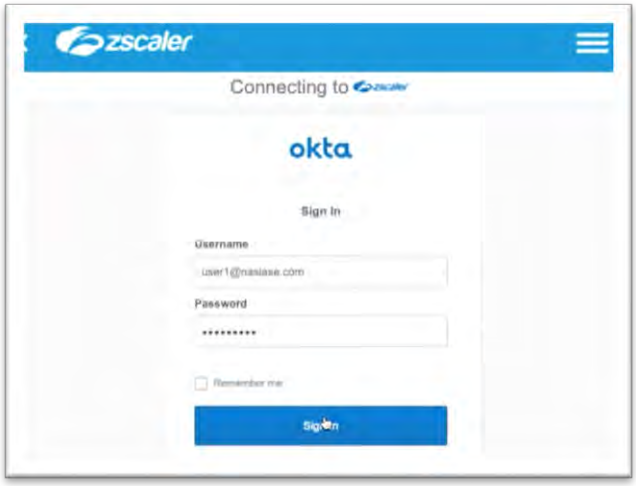




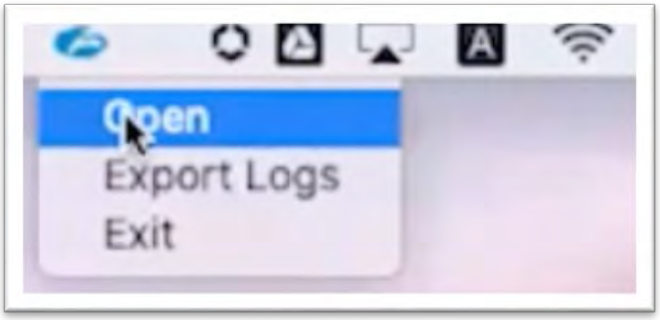
ユーザ名を入力して、[Login]をクリックします。



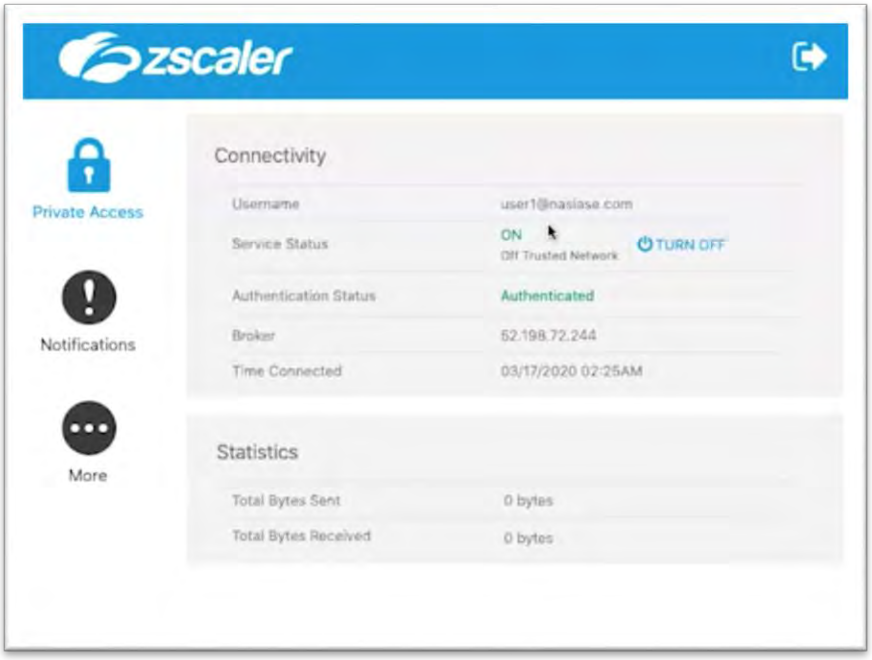
Username、Password を入力して、[Signin]をクリックします。



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

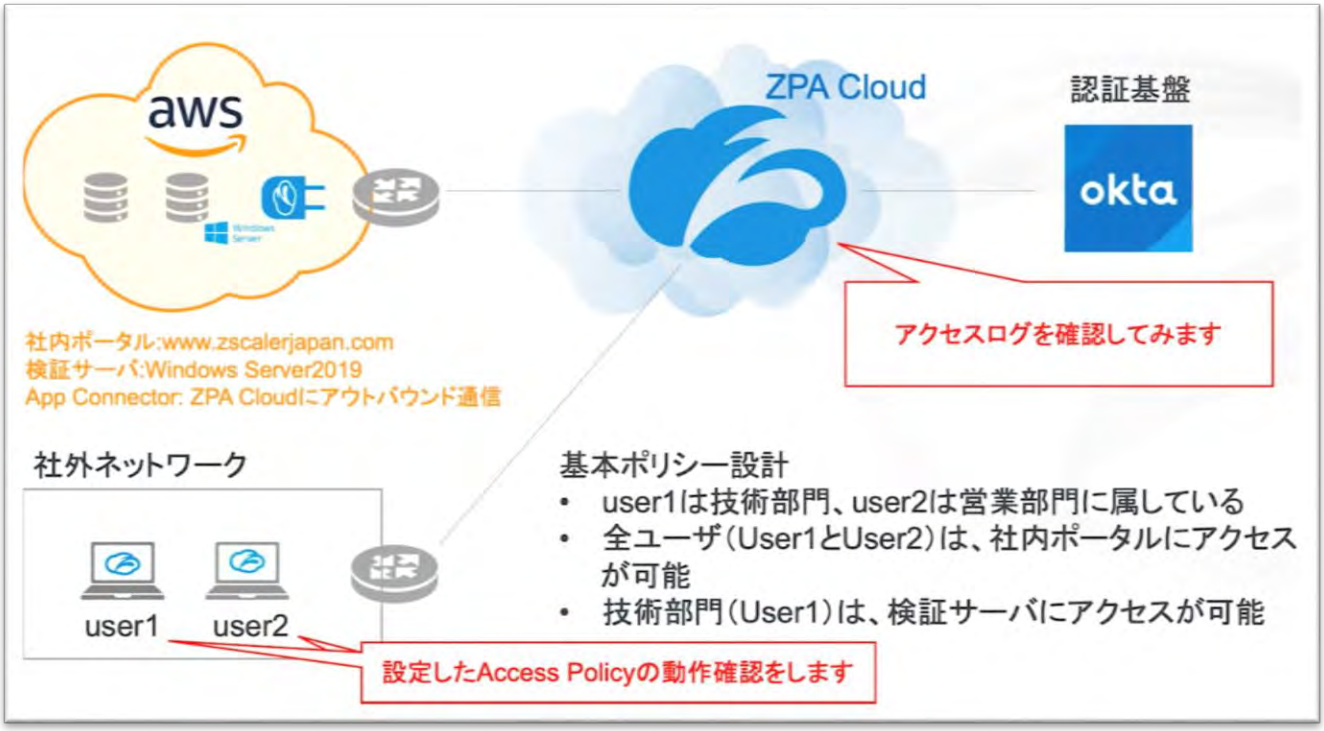


Authenticated Status が Authenticated となっていることを確認します。



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

4. 動作確認

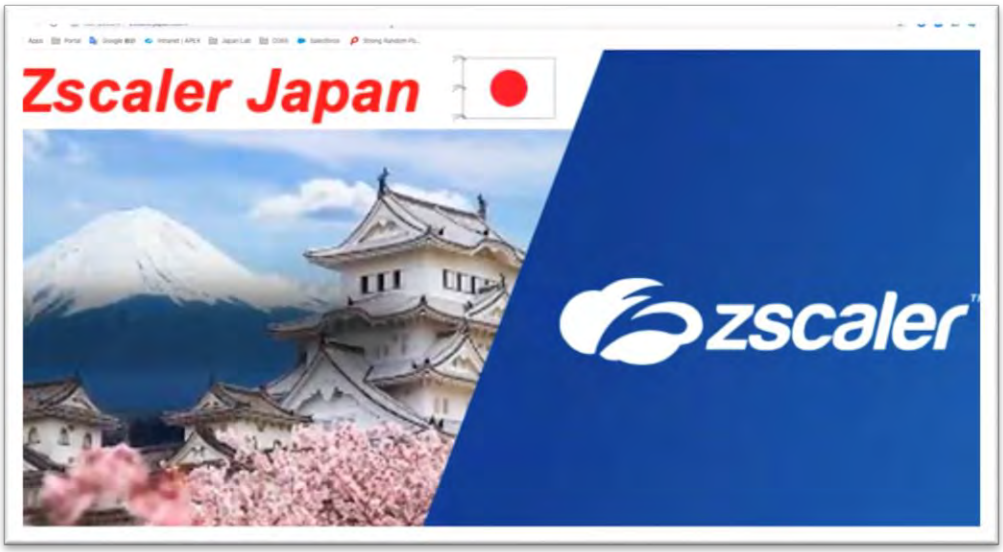


4-1.社内リソースへのアクセス

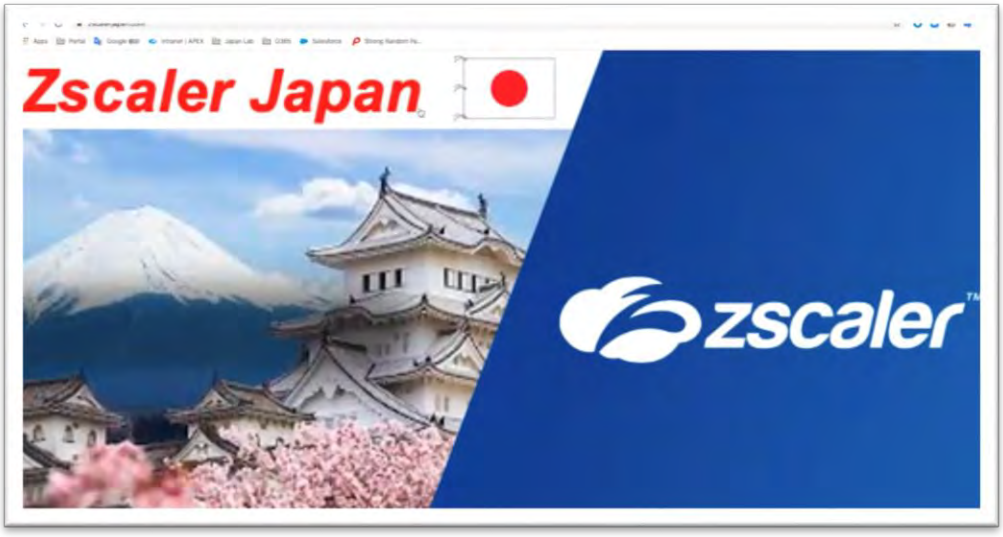
Step1. user1 でのアクセス

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。

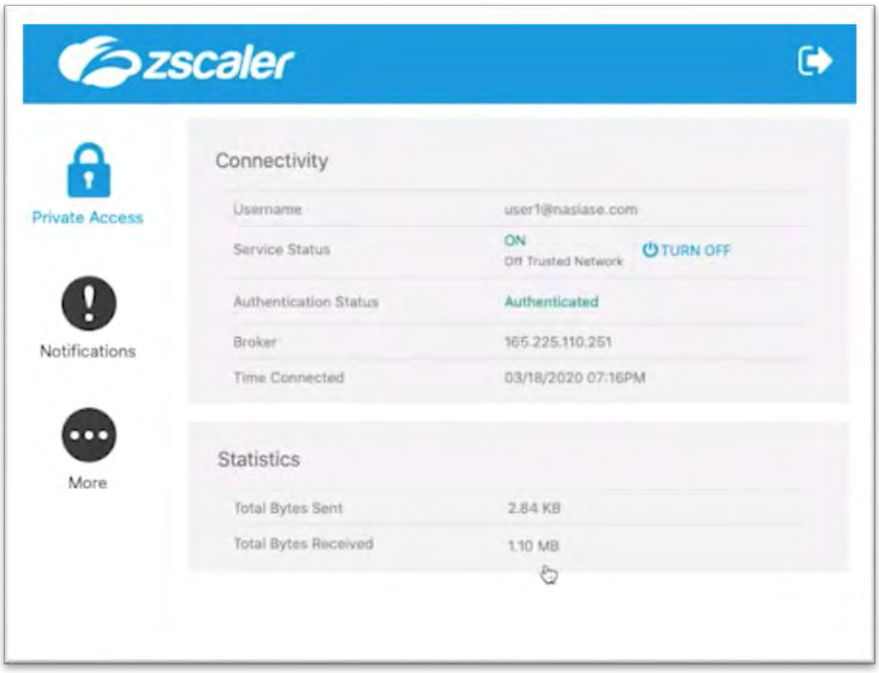
http の場合



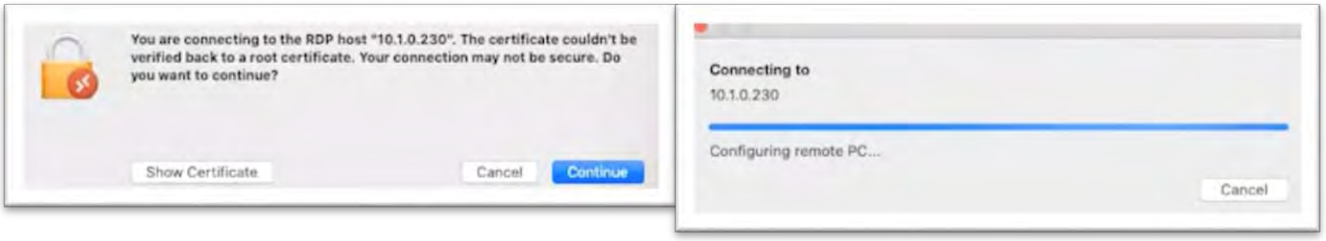
https の場合



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。



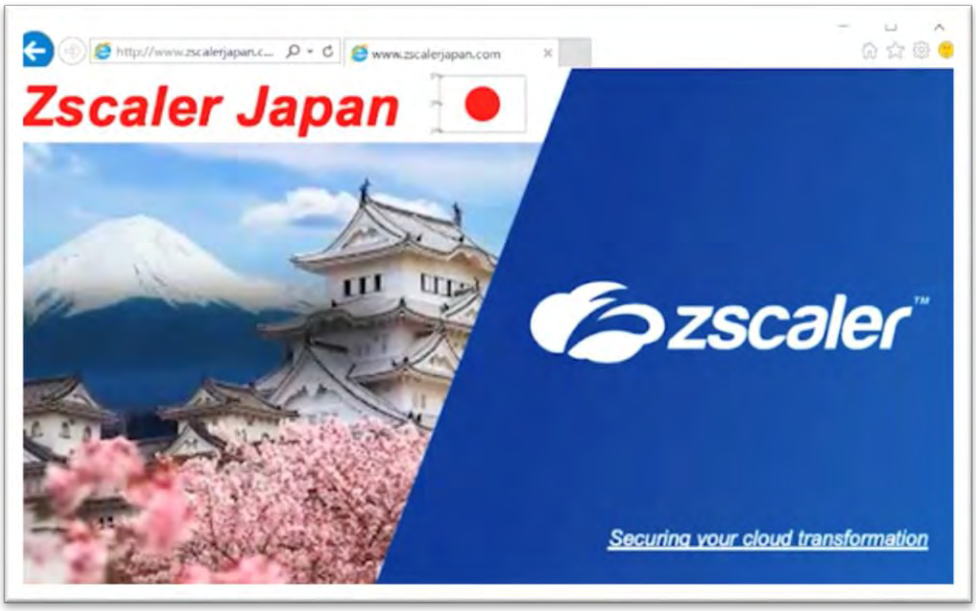
社内サーバへの RDP アクセスも成功します。



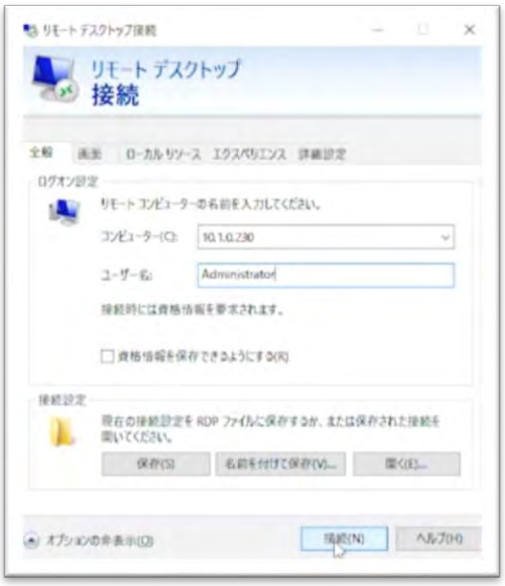
Step2. user2 でのアクセス

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。

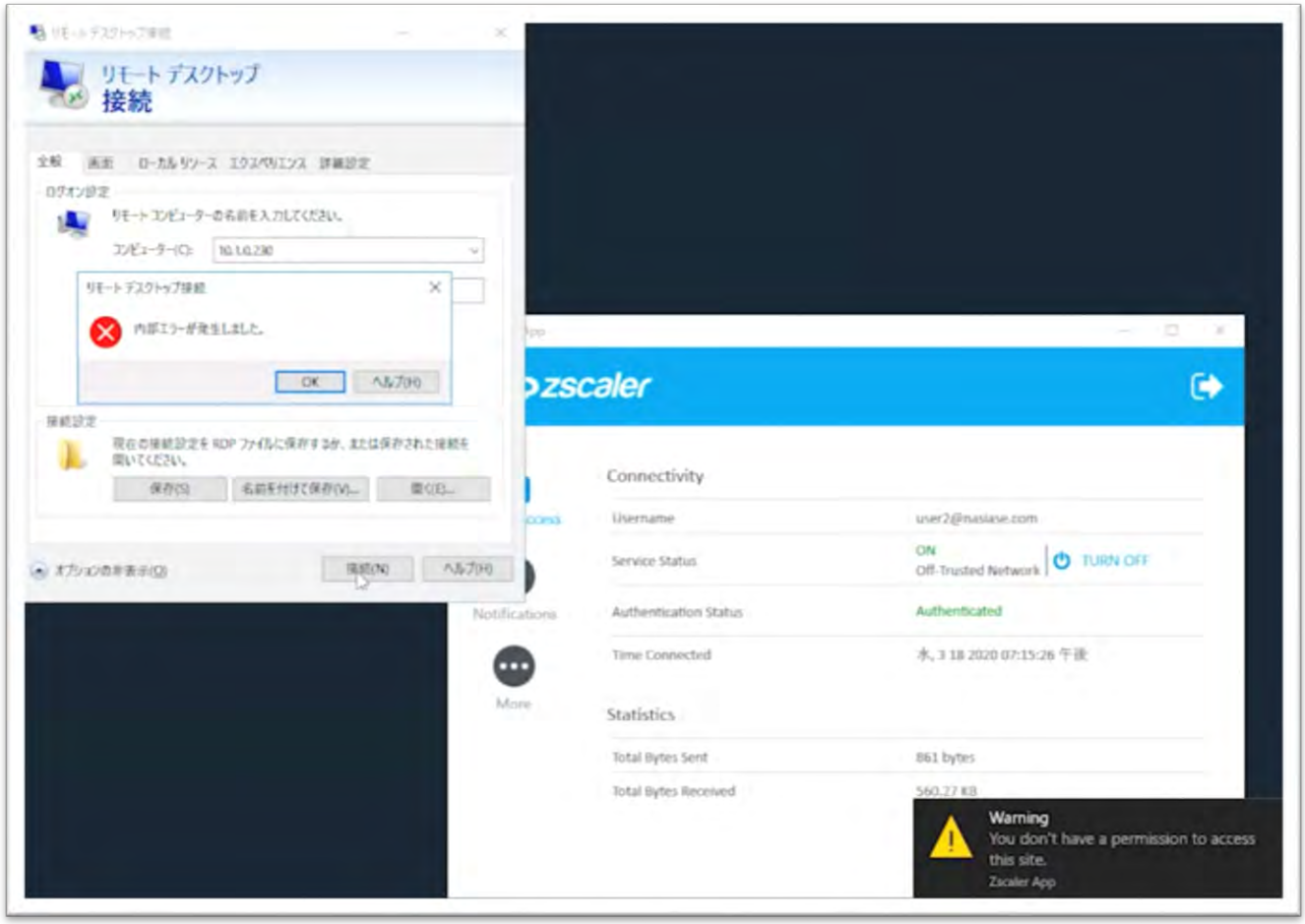
問題なくページが表示されます。



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。



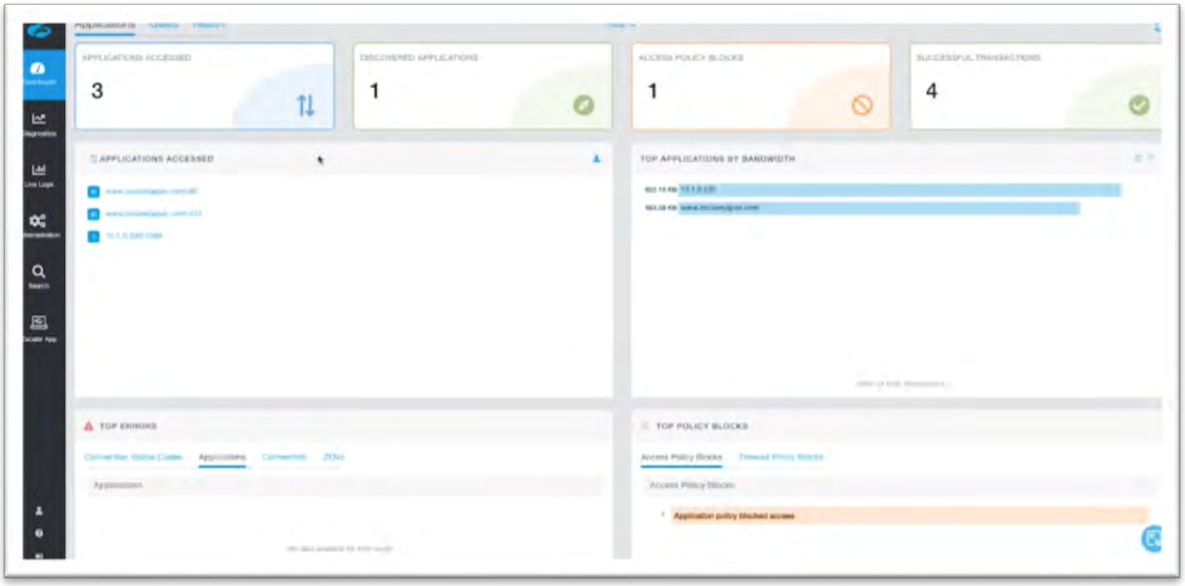
設定した警告メッセージも表示されます。



4-2. ログの確認

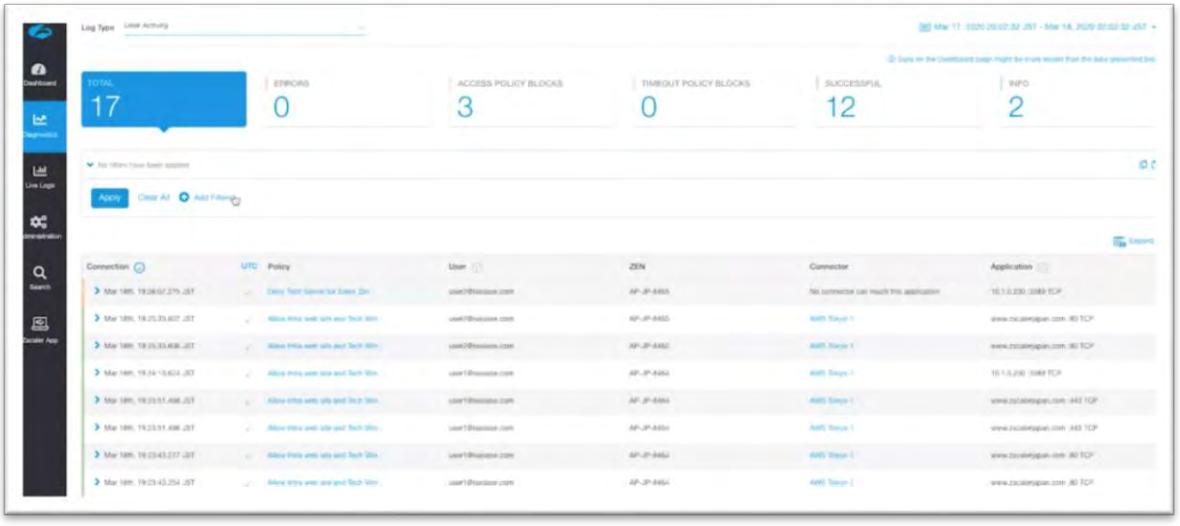
Step1. 統計情報の確認

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

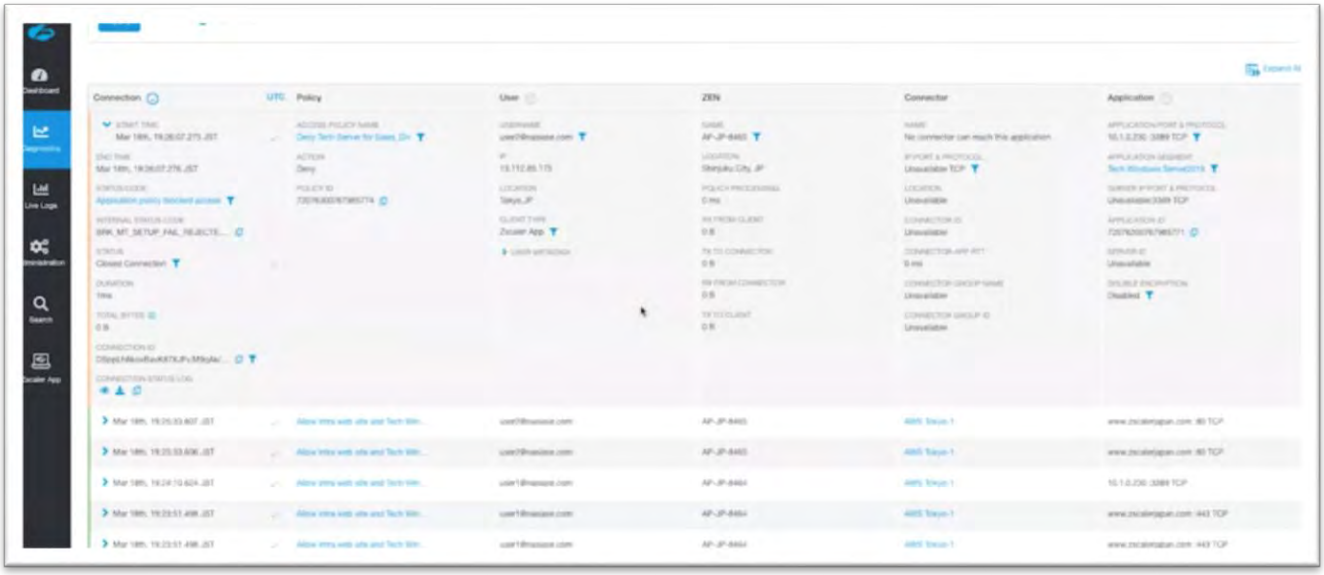


Step２. ログの詳細確認

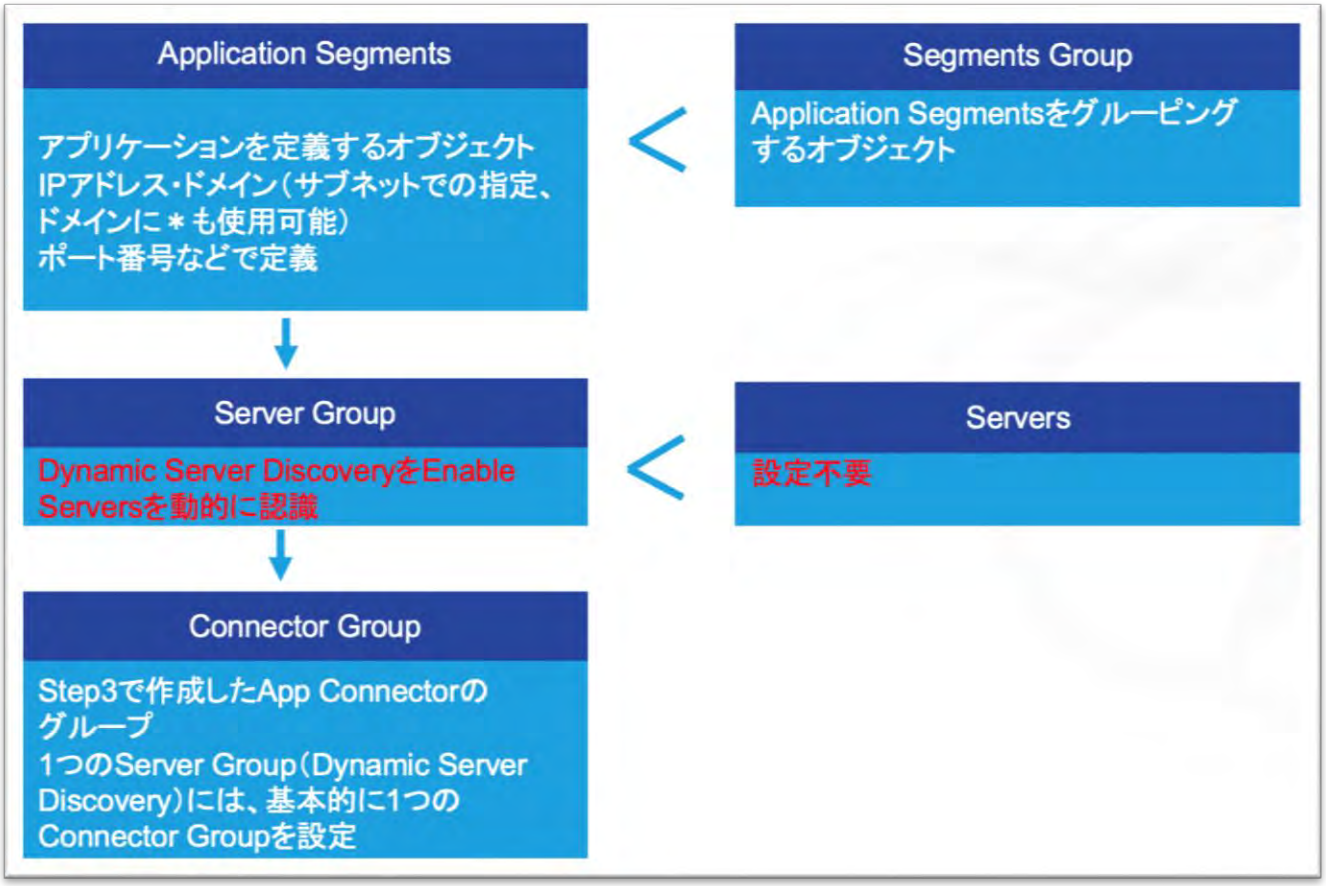
Dashboard -> Diagnostics より、各アクセス毎のログが確認できます。



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。



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

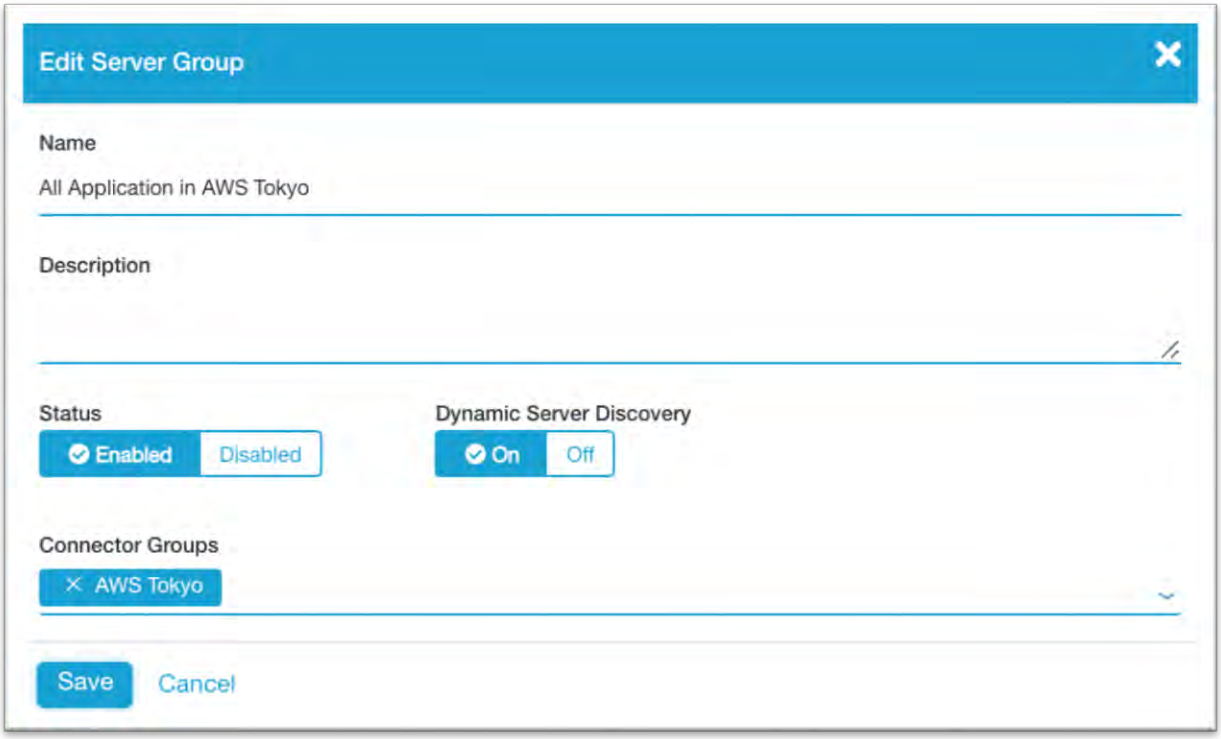
✓ 使用可能な場合、アプリケーションの定義には Dynamic Server Discovery を使用

✓ 基本的には 1 つの Server Group（Dynamic Server Discovery）には 1 つの Connector Group を設定

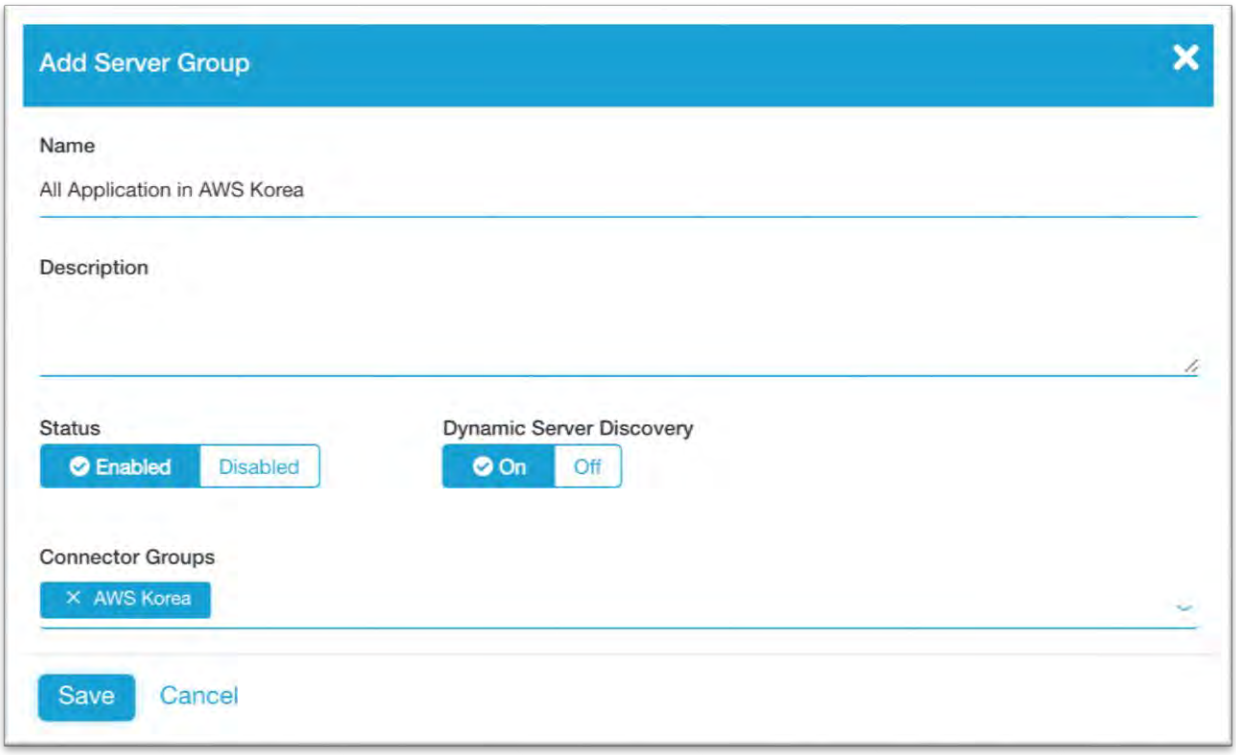
✓ 基本的には 1 つの DC（社内 DC、AWS Tokyo、AWS Korea など）に対しては、1 つの Server Group を設定

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。

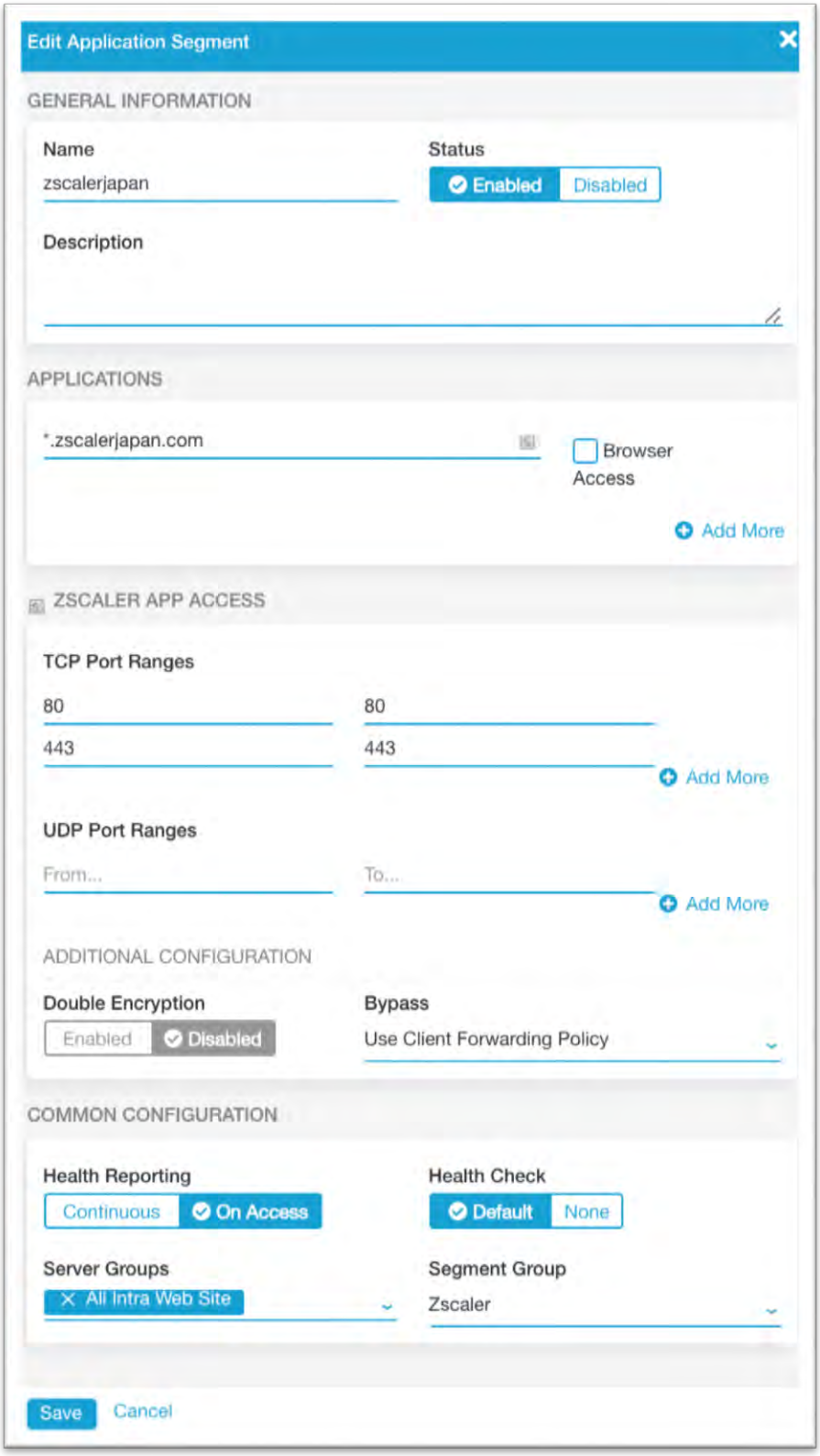


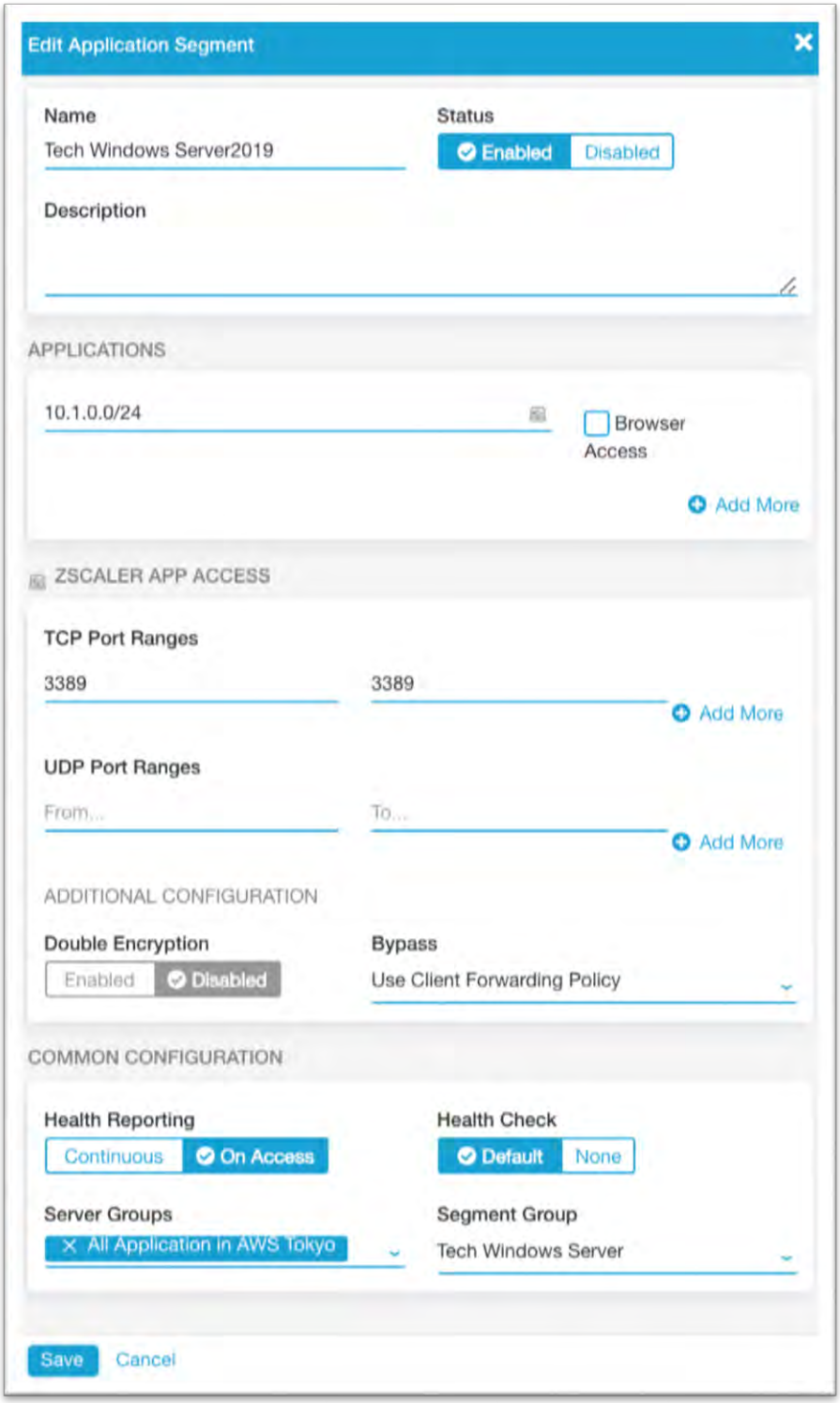
必要に応じて、他 DC 用の Connector group を追加します。



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。

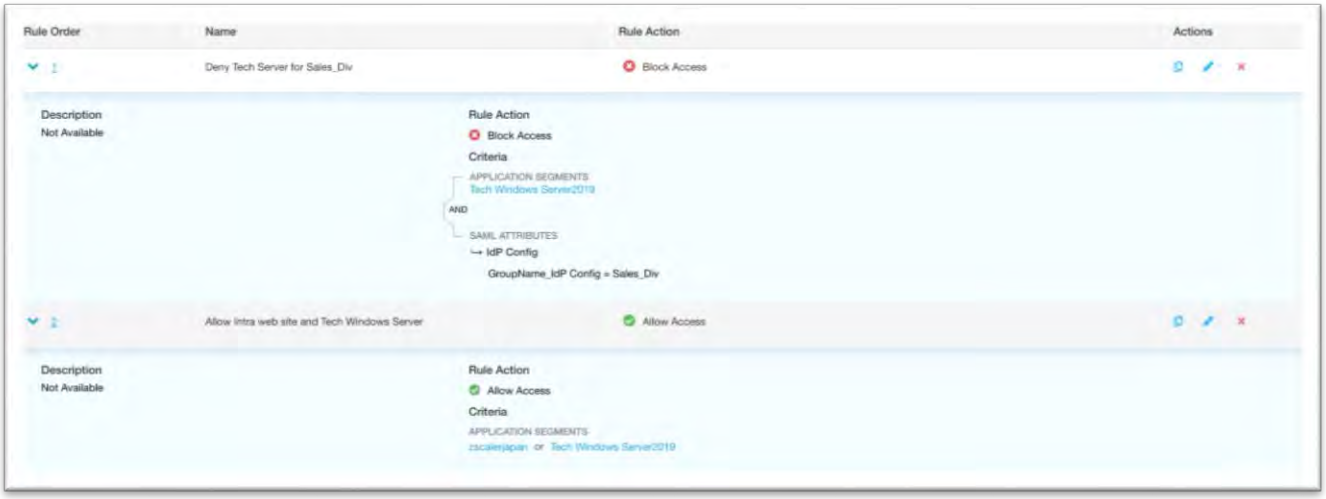




Step2. Access Policy の設定

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

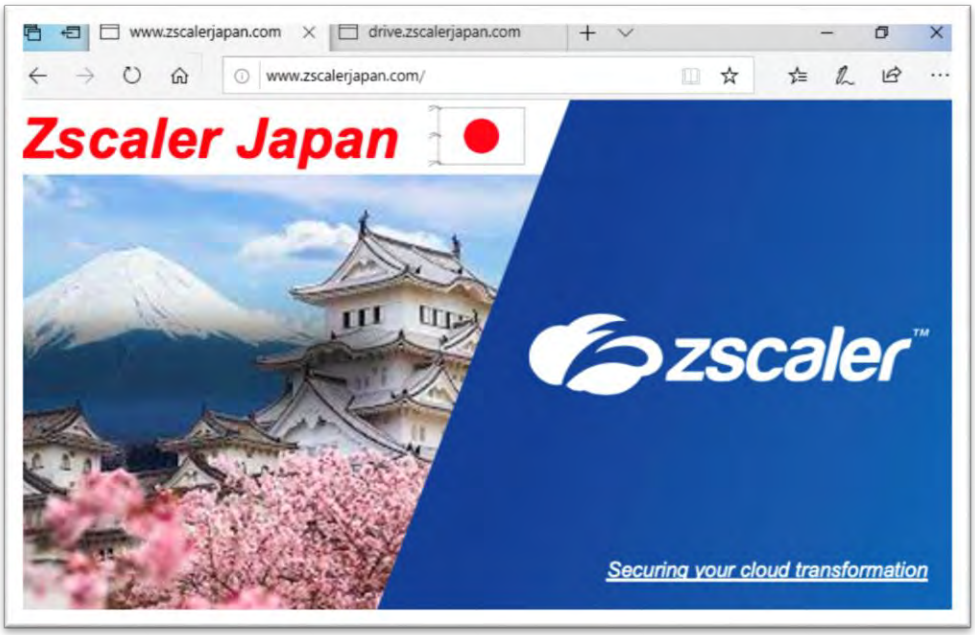
※営業部門は、社内サーバにアクセス禁止

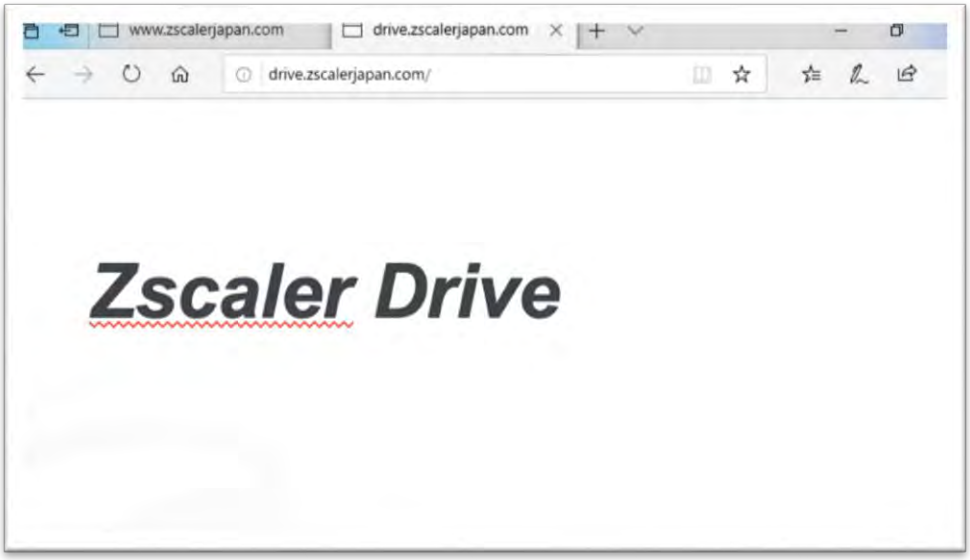


Step3. 動作確認

「www.zscalerjapan.com」と「drive.zscalerjapan.com」へアクセスを実施します。

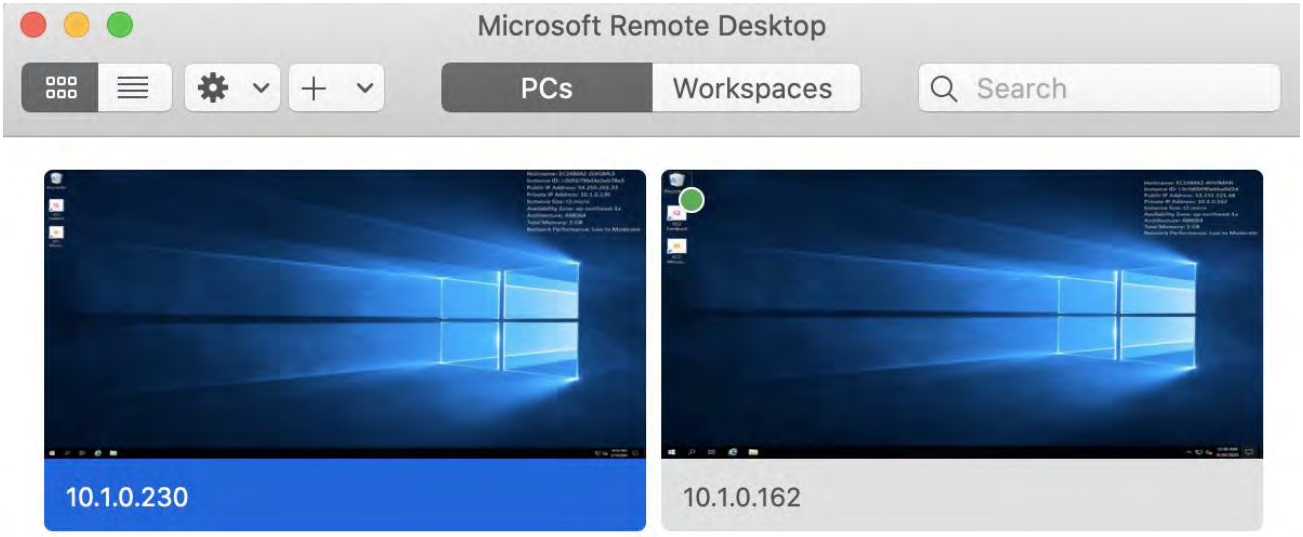
「*.zscalerjapan.com」にマッチするため、ページが表示されます。

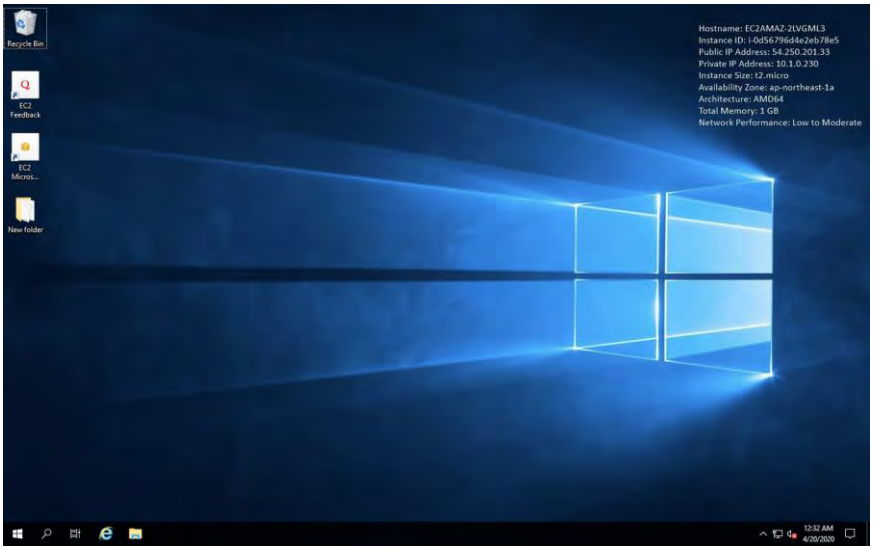


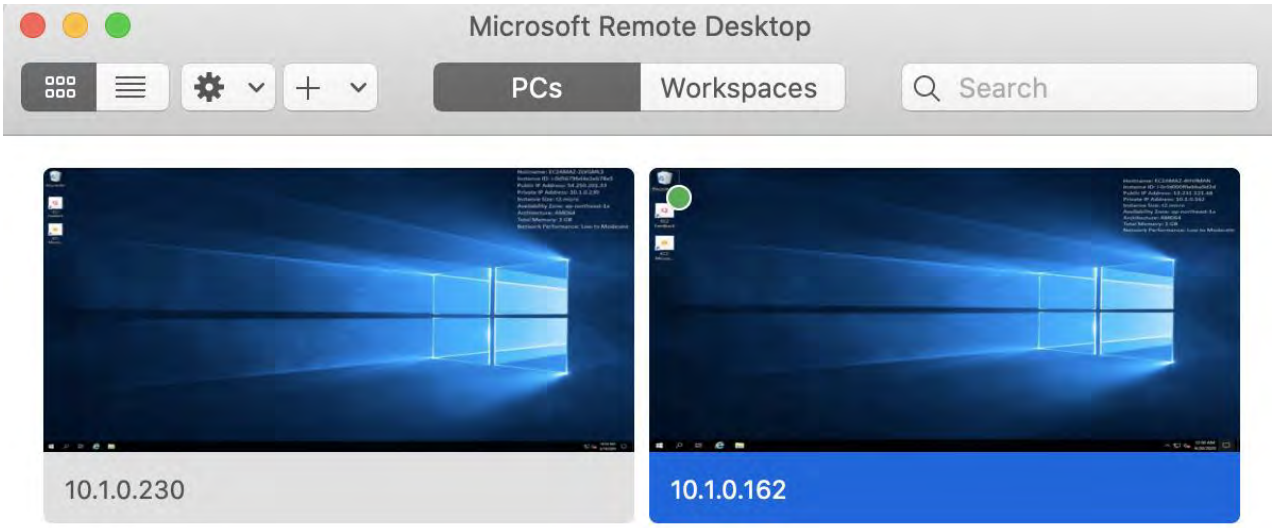


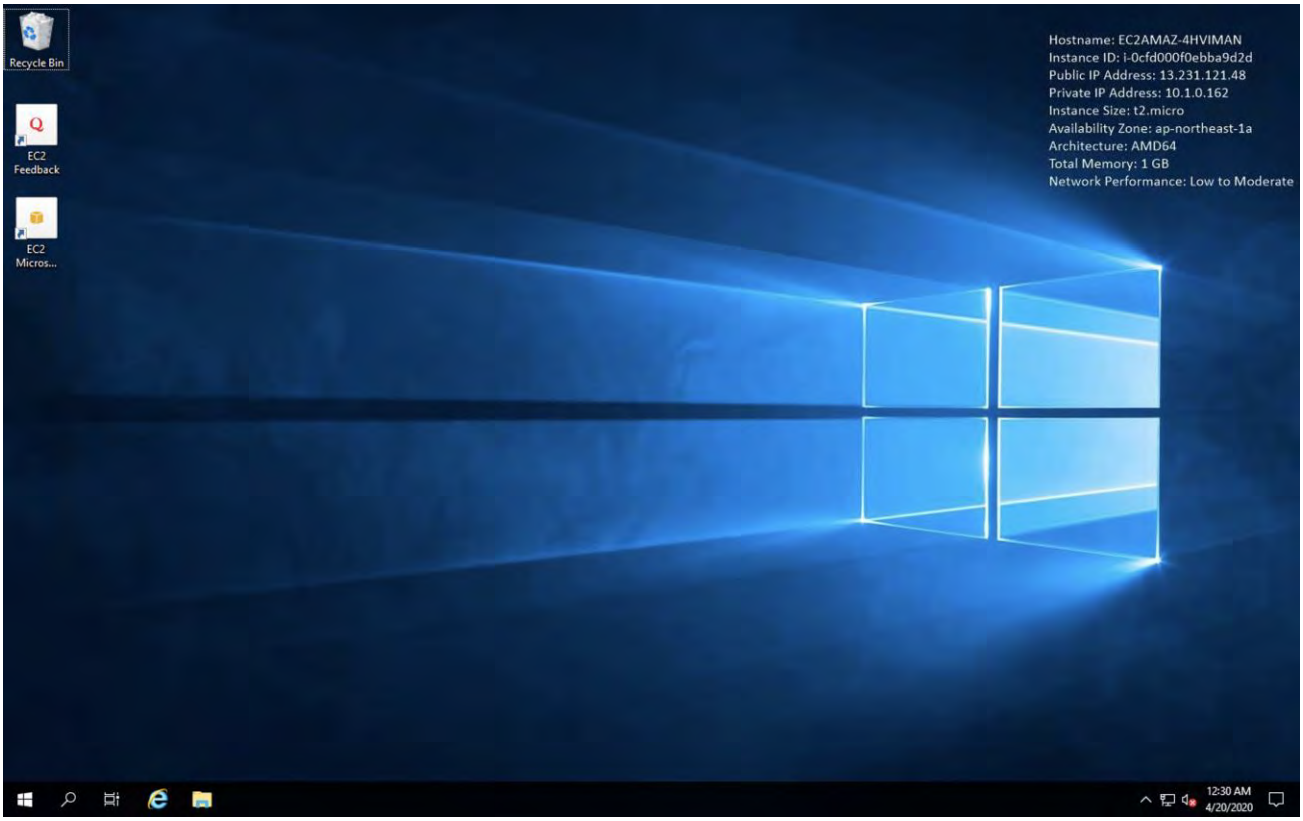
「10.1.0.230」と「10.1.0.162」に RDP でアクセスを実施します。

「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。

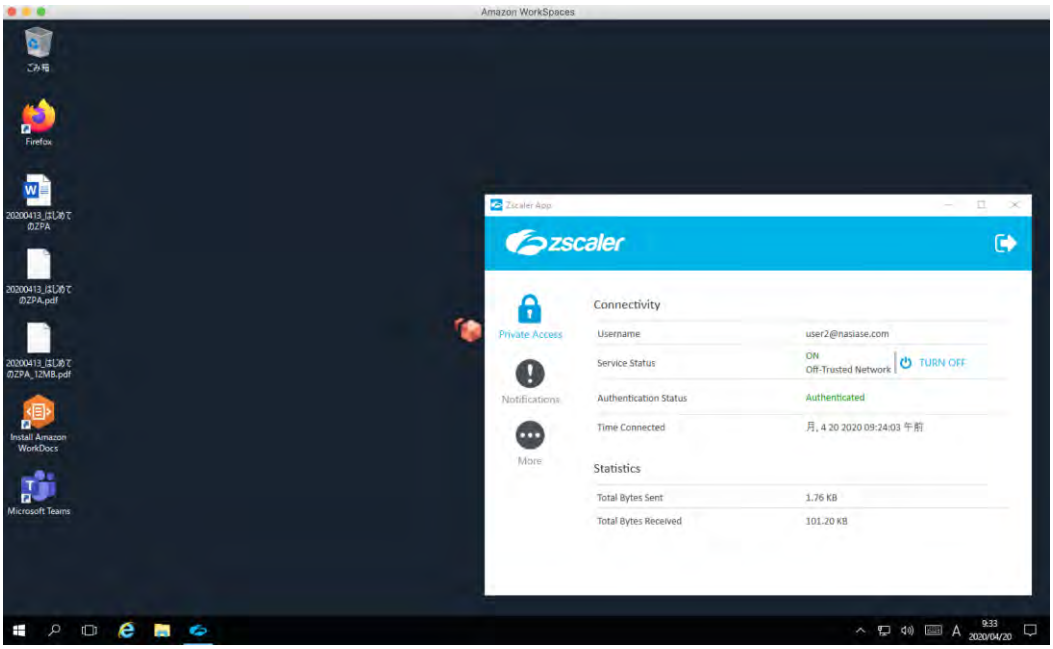


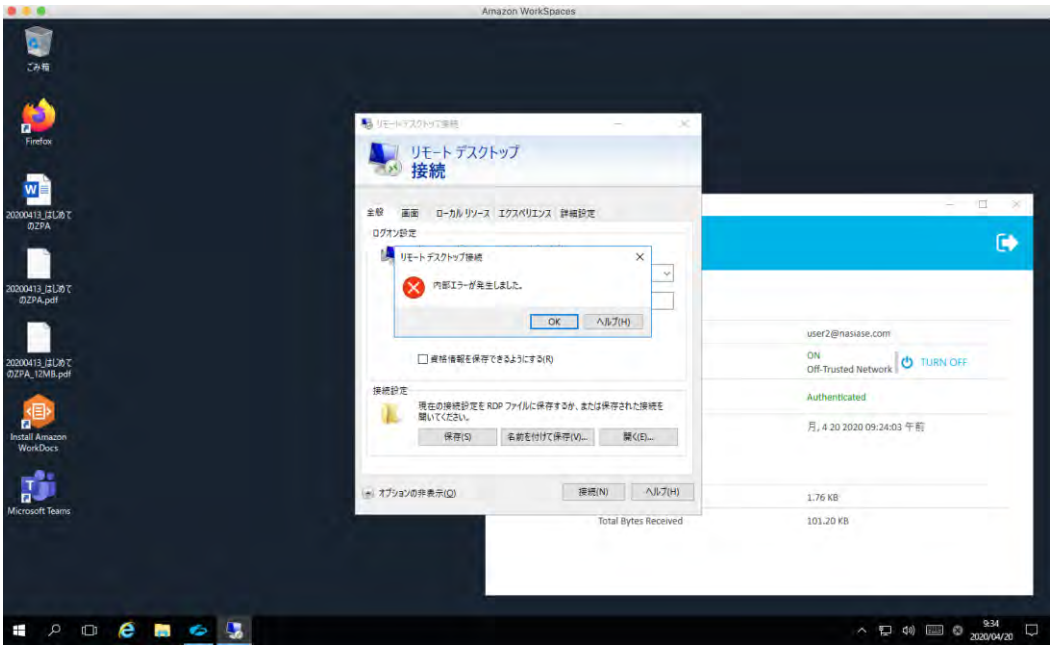






user2（営業部門）で RDP をすると、ポリシーに基づきアクセスが失敗します。

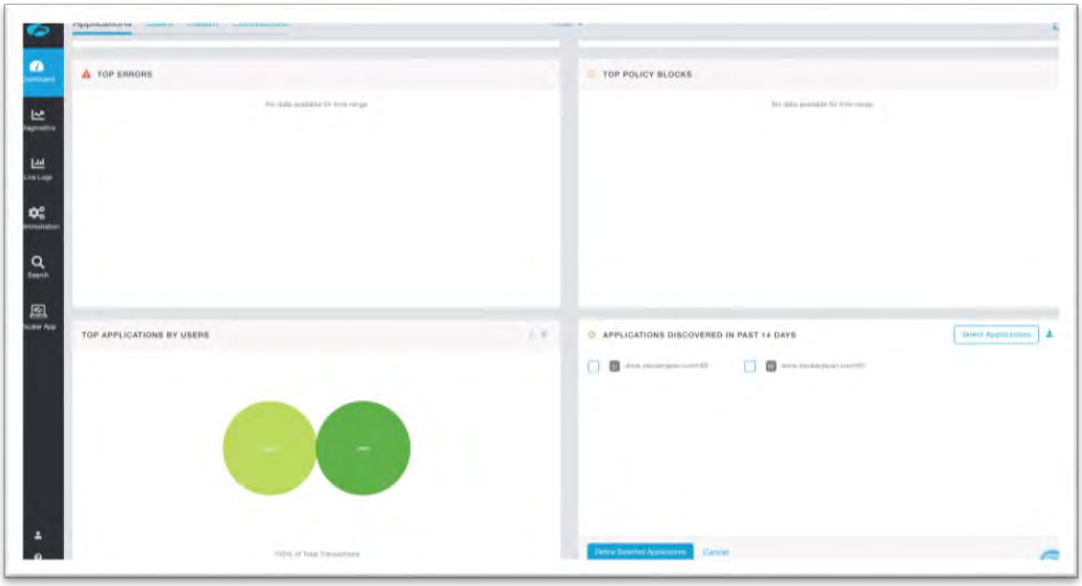




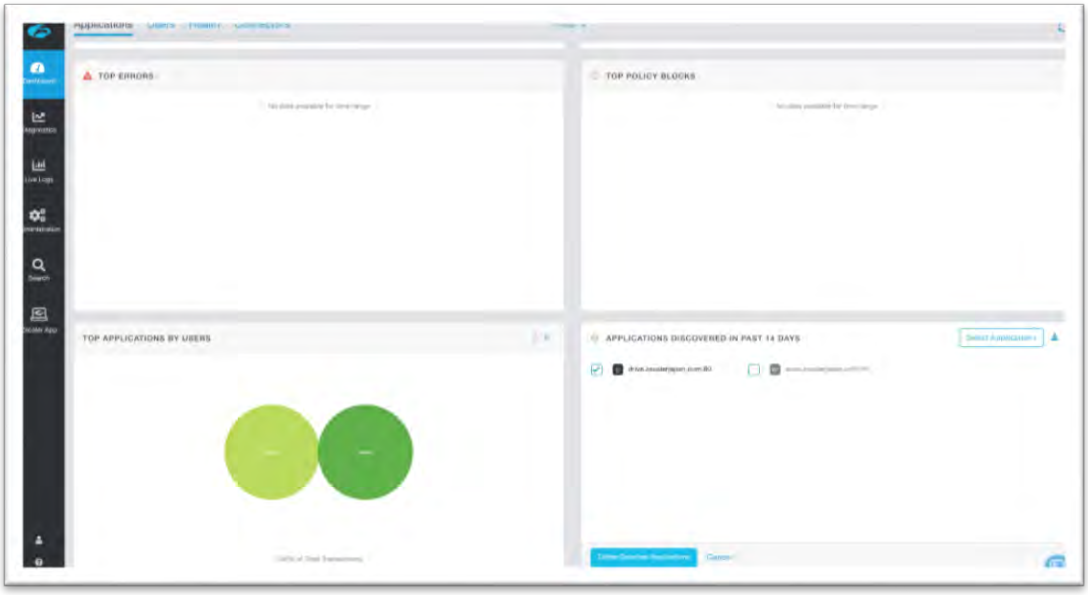
Dynamic Server Discovery を使用した場合でも、想定通りのポリシーで動作していることが確認できます。

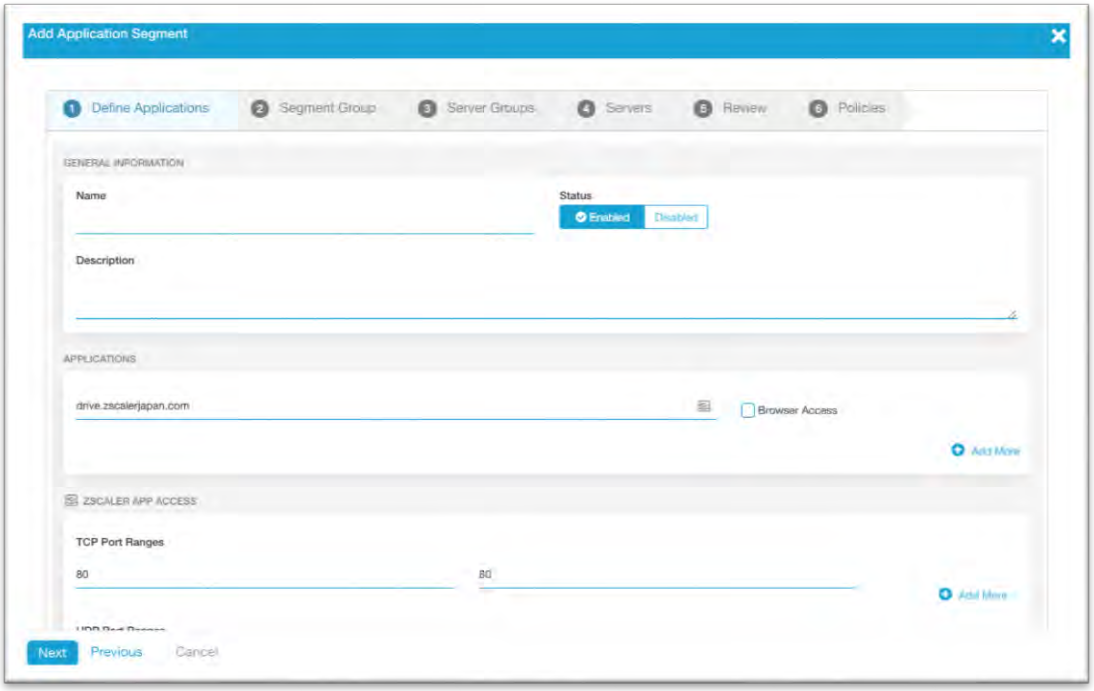
Step3. アプリケーションの可視化

Dashboard -> Applications の APPLICATIONS DISCOVERED IN PAST 14 DAYS に*（ワイルドカート）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。





6. その他の設定

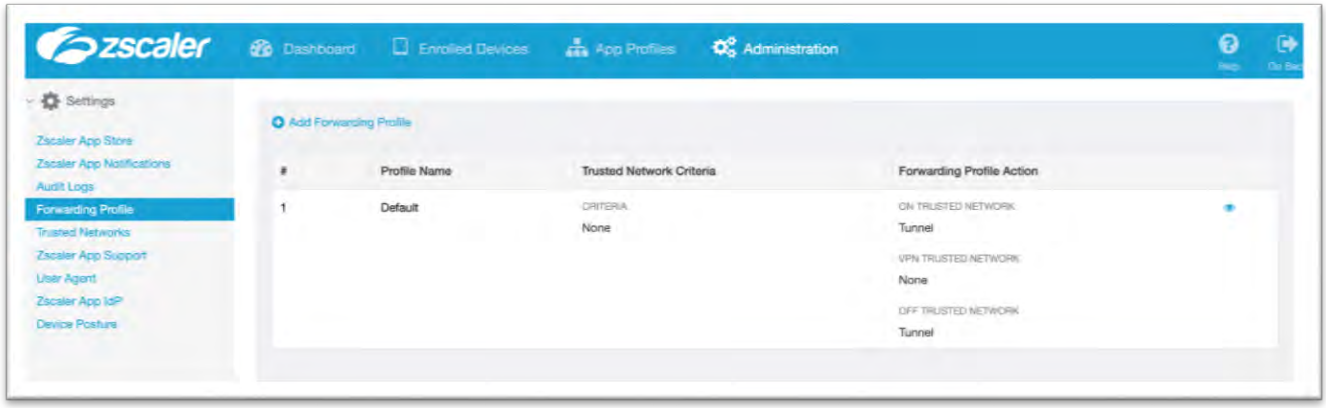
5-1. Forwarding Profile, App Profile の設定

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

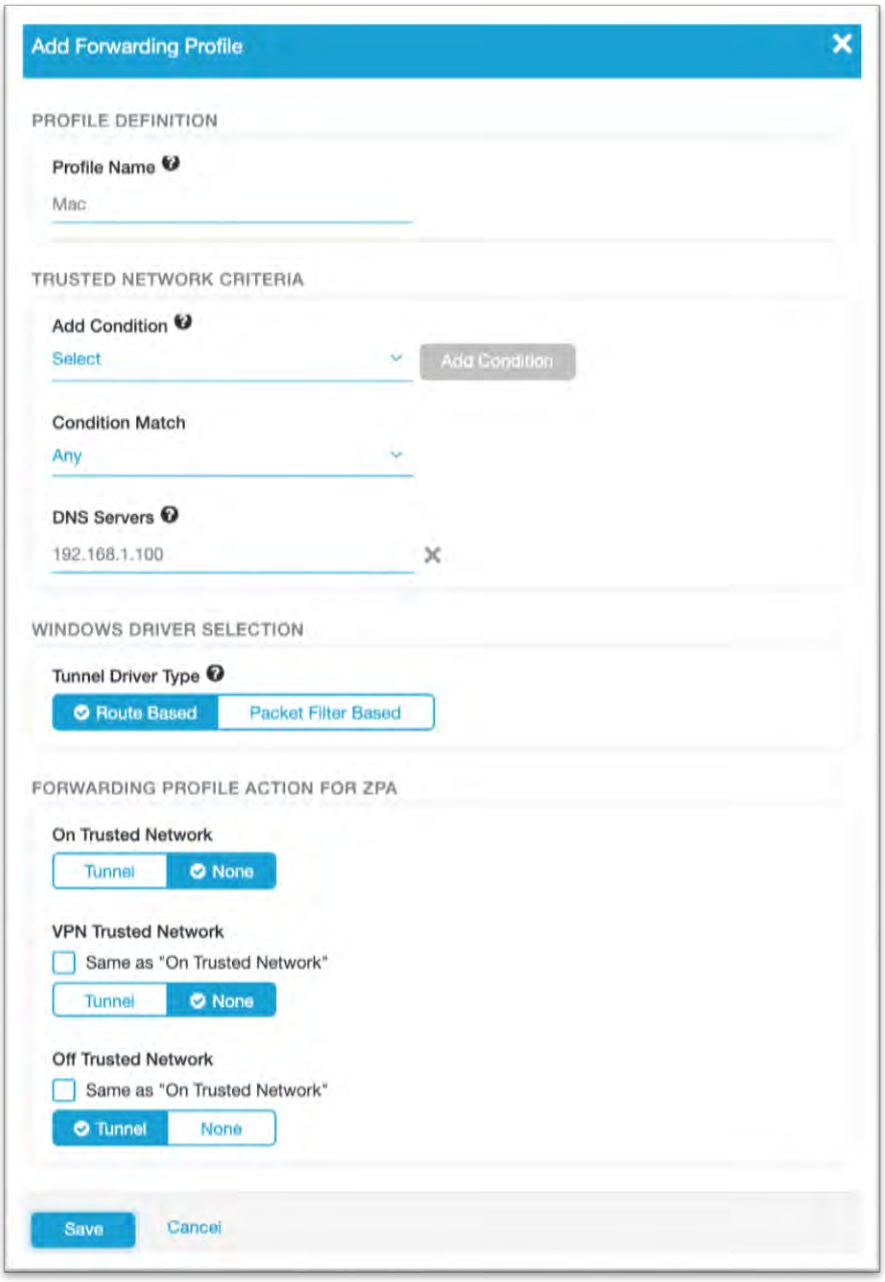
TRUSTED NETWORK CRITERIA: 任意の設定（※1）

FORWARDING PROFILE FOR ZPA: 任意の設定（※2）

++

※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 Netwrok 以外）の Action を設定、VPN Trusted Network は、None を設定



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）

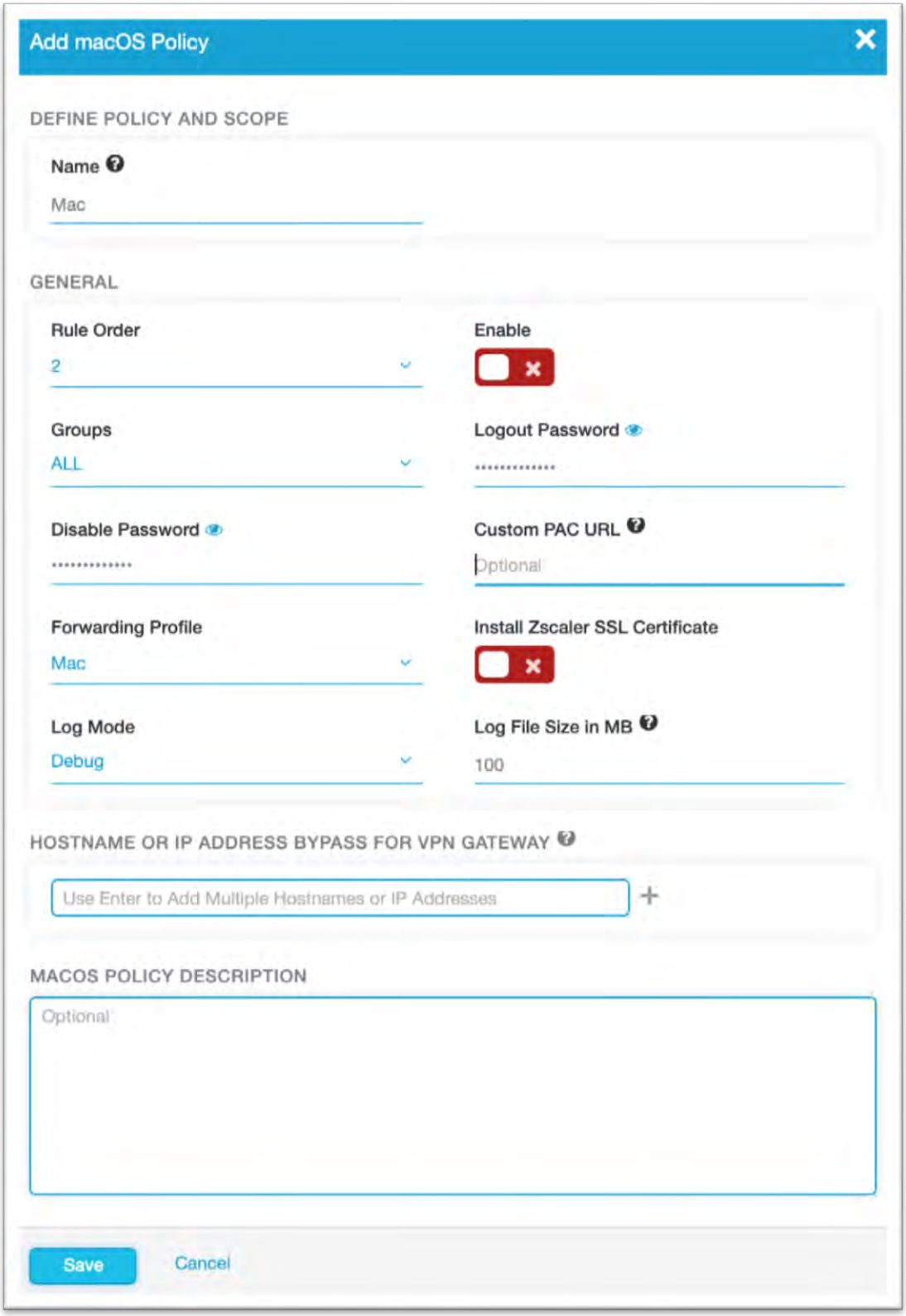
Forwarding Profile: 紐づける Forwarding Profile

++

※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



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。

5-2. Device Posture の設定

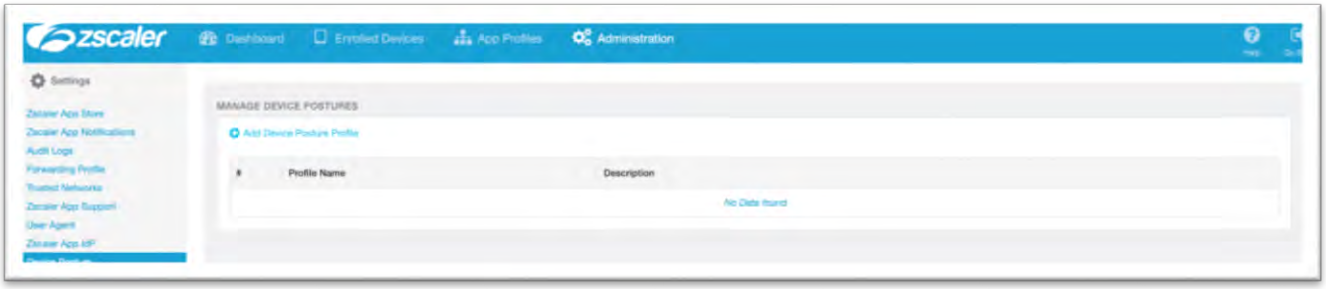
Device Posture は、Access Policy のマッチ条件に使用できる Criteria の一つです。
使用できる Device Posture は OS によって異なりますが、例として以下のような Device Posture を作成できます。

- 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。



必要事項を記入、設定し [Save] をクリックします。

++

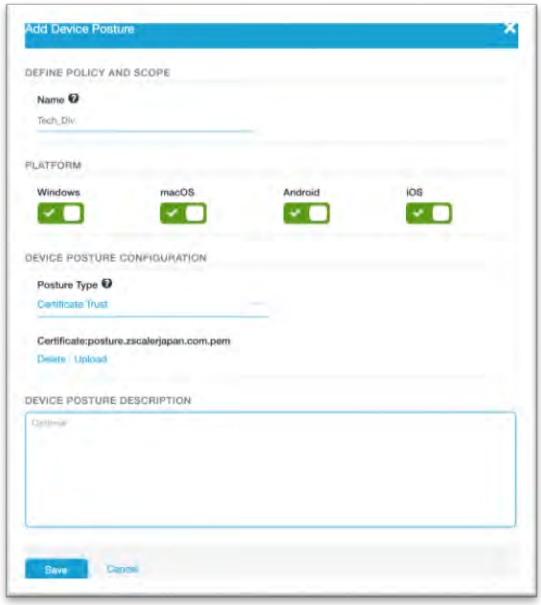
Name: 任意の名前

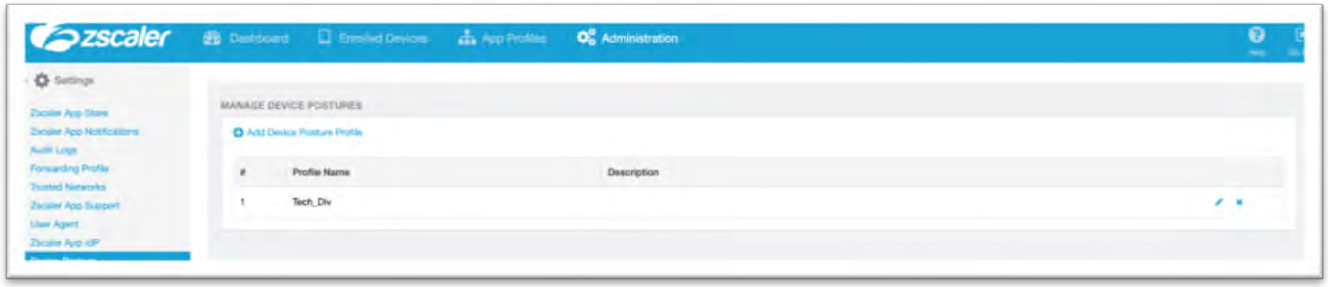
PLATFORM: 任意の OS

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

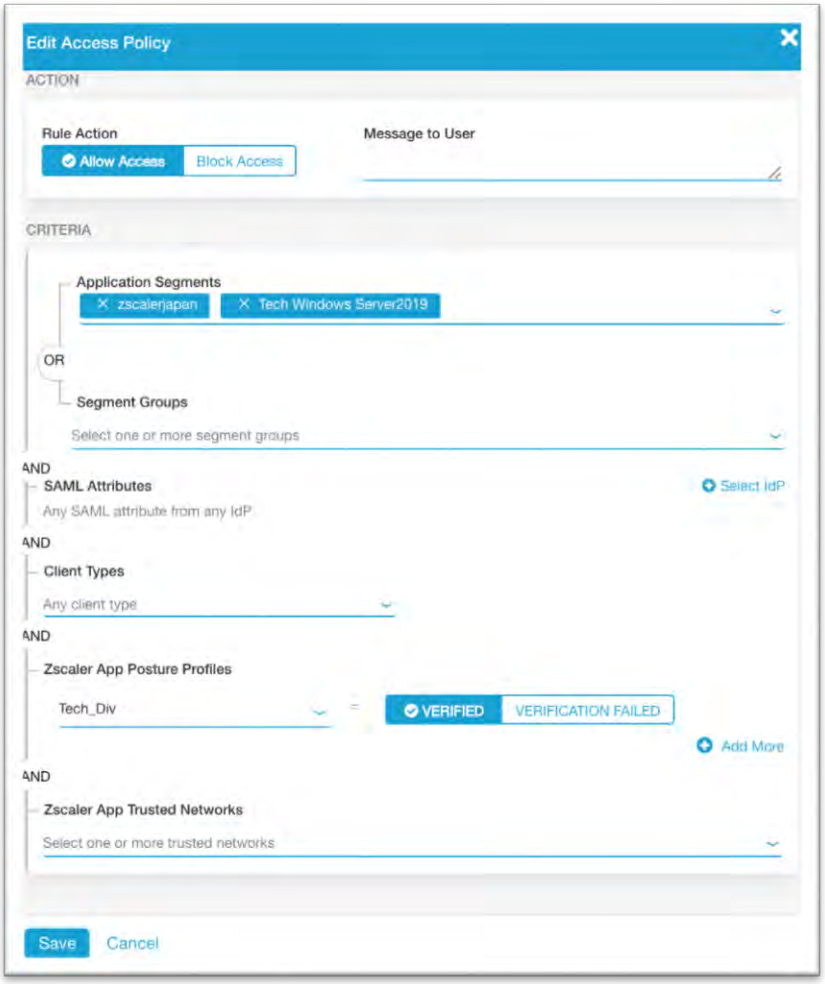
++





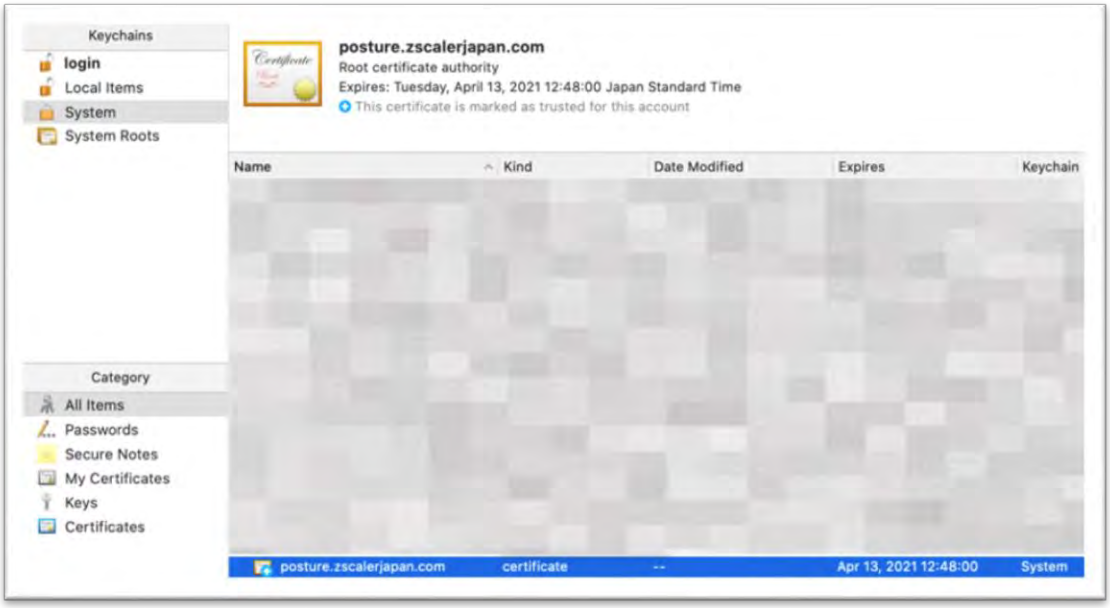
Step2. Access Policy の設定

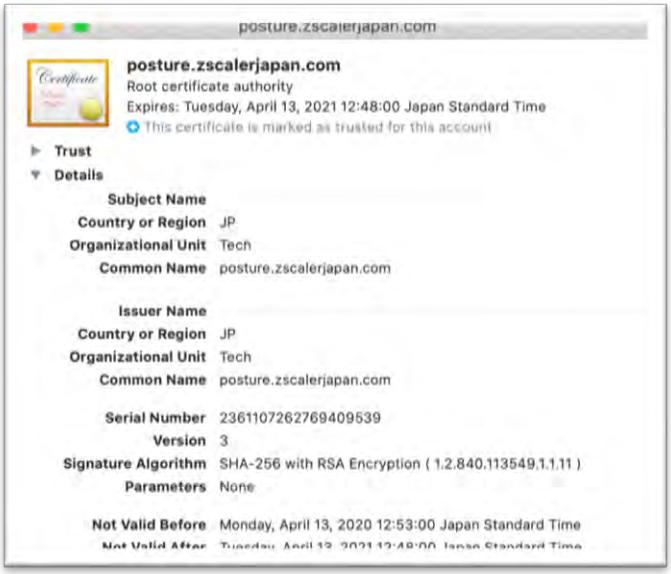
Zscaler App Posture Profiles に、Step1 で作成した、Device Posture を選択し VERIFED を設定します。



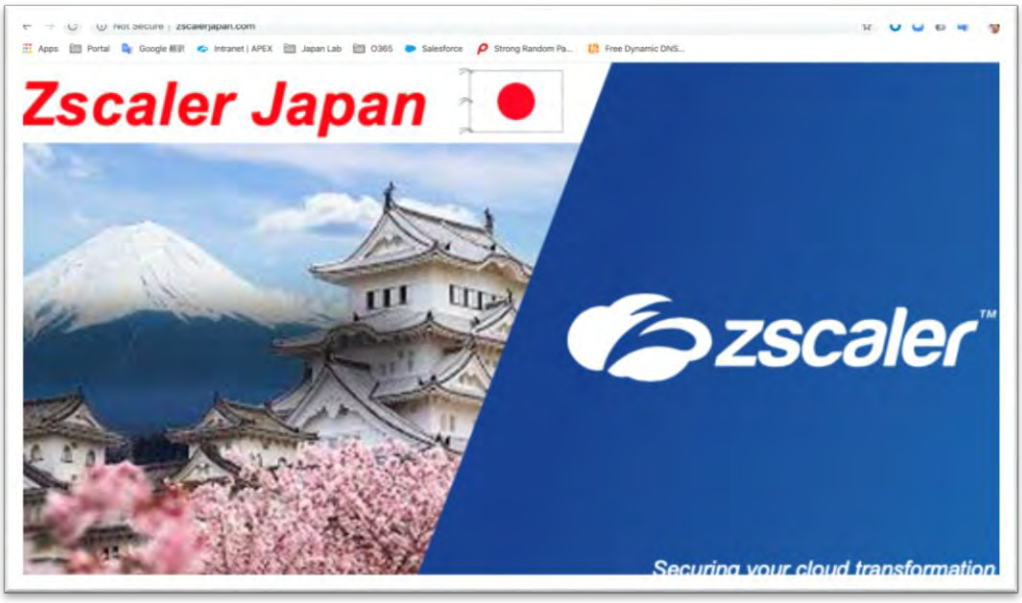
Step3. 動作確認

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。

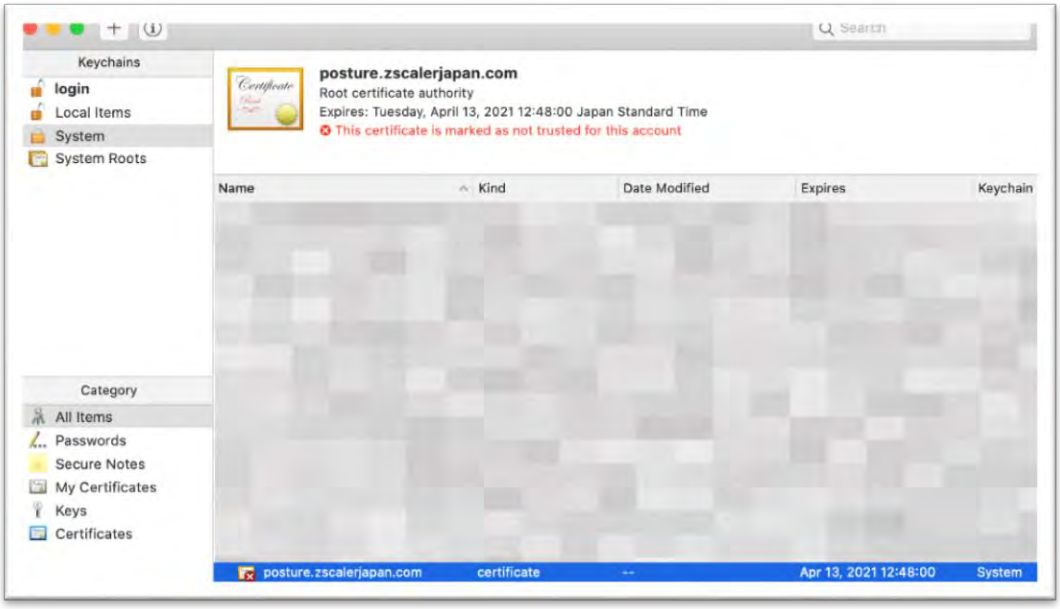


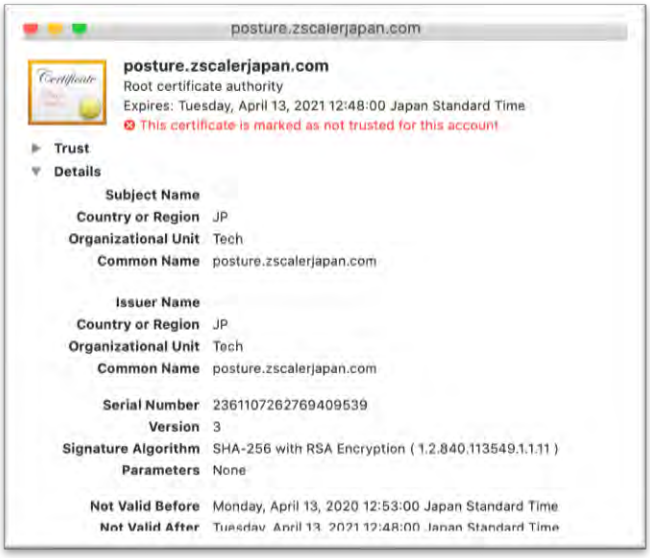


Access Policy の条件にマッチするのでアクセスが成功します。

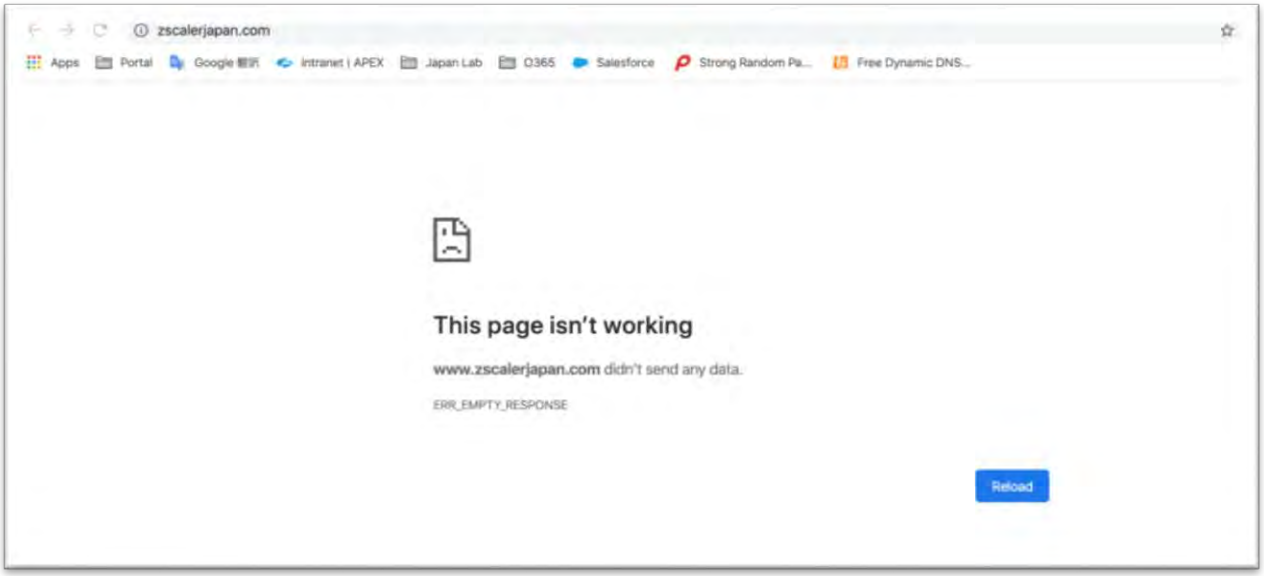


端末が Device Posture で設定した証明書を信頼していない状態で、アクセスを実施します。





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