

<u>はじめての ZPA</u> (Zscaler Private Access)

ゼットスケーラー株式会社

ZSCALER CONFIDENTIAL INFORMATION

©2020 Zscaler, Inc. All rights reserved.

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	
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。「<u>https://www.okta.com/zscaler/</u>」 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。

Free SSO & Provisioning for Zscaler Water Base of the state of the s	Sign up for OCC 「Get Started」をクリックするの oktaのアクティベーションメール 届きます。 メールの指示に従いテナントが 作成可能です。
	Sel Tayna

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。

ORCO
Sign In
Username
admin@inasiase.com
Password
Remember me
Sign In

Directoryより、 [People] をクリックします。

Editor
ry littlegrations
Masters ch People
Applications
Search Applications

[Add Person]をクリックします。

People				O Help
Add Person	Reset Passwor	ds C Reset Multifactor More Act	tions +	
Q Seenth.				
Everyone	2 Pers	on & Usemame	Primary Email	Status
DNBOARDING	admi umm	n nastase	admin@naslase.com	Active
Succes	Meta	ski Setatri	httpp226/8yahod.co.jp	Active
Pending user action	ō	har of here and here an		
ACTIVE				
Active	2			
Password Reset	0			
Pessword Expired	0			
Locked out	92			
NACTIVE				
Suspended	12			
	~			

下図を参考に必要事項を記入して、user1、user2 を作成します。

		Testame	Laboration of the second secon
lest name	usert	Last marine	Tuttsutsut
ast name	Catalogue .	Usamane	user2dnaslase.com
		Primary email	user2@meslase.com
NETTIOTIE	usertenature.com	Secondary email involution	
rimary email	usertonesiene.com		
econdary email (coprova)		Groups (petic/e)	You haven't added any groups
Poups (retrins)	You haven't addect any groups	Password @	Set by edmin +
	Terretories		
atsword U	Set by admin		User must charge passeors on find locin
	Liser must change password on first login		

Г

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。

E

L People			in the			0
1, Add Person	Roset Pa	sswords	Profile Editor	ns +		
Q Search_			Directory integrations Profile Masters			
Everyone	4	Person & U	semame		Primary Email	Status
ONBOARDING		admin nasia administrias	iase com		admin@nasiase.com	Active
Staged	0	user10nau	He com		user50nasiase.com	Active
Pending user action	0	user2 nasia	se ese com		user2@nasiase.com	Active
ACTIVE	2	Masaki Sata hhrpp226d	ichi yahoo.co.jp		hhrpp226@yahoo.co.jp	Active
Password Reset	ø					

[Add Group]をクリックします。

					O Help
PUNCE.					
AdgGroup				Q, Search	
roe Name		People	Apps	Directories	
Everyone		4	0	0	
All utilities in your 1	ong An IEABoin				
All valers in your i	organization.				
All utilities in your o	onganization		Add Group		
All utiliens in your i Add Group Add groups se you tan que	cirgani@allow		Add Group Add groups so you can	quickly perform actions acro	oss large sets of people.
All utiliers in your o Add Group And groups so you can gain Name	skly perform actions across large sets of people.		Add Group Add groups so you can Name	quickly perform actions acro Sales_Div	oss large sets of people.

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。

Alf	Ne				
AL AD	d Group			Q, Search	
Source	Name	People	Apps	Directories	
0	Everyone: All carrs in your organization	4	C.	0	
0	Sales_DN No description	D.	a.	U.	
0	Tech Div	D	a		

[Manage People]をクリックします。

lech_Div				
INC SHEWPORK				
Manage People	III Manage Apps	Manage Directories	AL Delete Group	
eople Apps	Diversioners			

user1を選択して[save]をクリックします。

Cancel			Save
	Q.]	1.	
Add All 3		C Remove All	
1 Not Members	Showing 1 - 3 of 3	1 Members	Showing 1-1 of 1
Person & Username		Person & Username	
admin naslase admin@naslase.com		usert nasiase Imert@nesiase.com	
user2 nasiase user2@nasiase.com			200 - 200 - 10 - 100
Masaki Satachi hivrpp2260yahoo.co.jp			
Prol	President 1 Faunt Line		

同様の手順で、user2 を Sales_Div に紐付けます。

Add Group				Q, Search	
urce Name		People	Apps	Directories	
All users in your organization		4	D	0	
Salet-Div No description		D	0	o	
Tech_Div No description		1	0	a	
ack to Group Sales_Div No description d or remove people from the	Sales_Div group				
ack to Group Sales_Div No description d or remove people from the Cancel	Sales_Div group			Save	
ack to Group Sales_Div No description d or remove people from the Cancel	Sales_Div group	A Remove Al		Save	
Ack to Group Sales_Div No description d or remove people from the Cancel	Sales_Div group Q. https://www.statics.com/statics/sta	Remove All (Members		Save Showing 1: 1 of 1	
Ack to Group Sales_Div No description d or remove people from the Cancel Acd All 3 Not Members Person & Username admin naslase edmintBrussiege.com	Sales_Div group	Remove All (Remove All (Members Person & Username user2 naslase user2 dansause com		Showing 1: 1 of 1	
Ack to Group Sales_Div No description d or remove people from the Cancel Cancel Acd All 3 Not Members Person & Username admin nasiase edminithresilinge com	Sales_Div group	Remove Al (Members Person & Username User2 nasiase user2 nasiase user2 nasiase		Showing 1: Lot 1	
Ack to Group Sales_Div No description d or remove people from the Cancel Add All () Not Members Person & Username admin nasiase edminothrasilase com user1 nasiase reamtitrivesilase com Masaki Sasachi Ilivrop226/egyshoo.co.jp	Sales_Div group	Remove Al (Members Person & Username user2 timasaase .com		Showing 1:1of1	

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。

okta	Get Started	Directory			
- Back to Gro Sales, No desc	ups _Div		Applications Self Service		

[Add Application]をクリックします。

Applications		0.110
E Add Application		
Q search		
STATUS		
ACTIVE 0		
MALTINE 0		
	Q,	
	No active apps found	
	Add epoteelion and energy eccess to have them appear environ a reason Okda home Page	

Zscaler Private Access を登録します。

Q, zscaler		AI A B C D	EFSHIJKLMNDPQRSTUVWXY
Graceller	Zscaler 2.0 Okta Verfiled SAML Provisioning	Add	only the following apps:
©.zscalar	ZScaler Admin Login Okta Verified	Add	
DISCHER	Zscaler Private Access 2.0	Add	-

 General Settings 		
neral Settings Requir	ed	
		General settings
Application label	Zscaler Private Access 2.0	All fields are required to add this application unime, miniaed optional.
	This label displays under the sop on your home page	
Application Visibility	 Do not display application icon to users 	
	Do not display application icon in the Okta Mobile App	

Step6. ZPAへのuserアサイン

Assign より、[Assign to People]をクリックします。

General Sign On Mobile Import	Assignments	
Assign 👻 🥜 Convert Assignments	Q Search .	People *
Assignto People	Type	
	No users found	

[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。

(DZS	caler	Zscaler H	rivate A	ccess 2.0	
		(<u></u>)			
General	Sign On	Mobile	Am port	Assignments	

ieneral Sign On Mobi	e Import Assignments
App Settings	5ª
Application label	Zscaler Private Access 2.0
Application visibility	Do not display application icon to users Do not display application icon in the Okta Mobile app
Provisioning	Enable on-premises provisioning
Auto-launch	Auto-launch the app when user signs into Okta.
Application notes for end users	
Application notes for admins	

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

General Sign On Mobile	Import Assignments	
App Settings		Cancel
Application label	Zscaler Private Access	
Application visibility	Do not display application icon to users Do not display application icon in the Okta Mobile App	
Provisioning	Enable on-premises provisioning	
Auto-launch	Auto-launch the app when user signs into Okta.	
Application notes for end users		
	This note will be accessible to all end users via their dashboa	ard
Application notes for admins		
	This note will only be accessible to admin on this page	

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。

ilgn On Mobi	le Import Assignments	
	na ningenon ennengenonne mae	
		Edit
THODS nethod determines equire additional co semame is determin	how a user signs into and manages their crede infiguration in the 3rd party application. red by the user profile mapping. Configure pro	ntials for an application. Some sign-
0 ult Relay State		
ble Force Authentic	ation 😨	
ipName	None	
AML 2.0 is not con	ligured until you complete the setup instruction	15.
View Setup Instruct	tions	ynamic configuration.
	THODS nethod determines i equire additional co sername is determin 0 uuit Relay State ble Force Authentic upName GAML 2.0 is not cont View Setup Instruct dentity Provider met	THODS nethod determines how a user signs into and manages their crede equire additional configuration in the 3rd party application. semame is determined by the user profile mapping. Configure pro 0 uit Relay State ble Force Authentication view Setup instructions dentity Provider metadata is available if this application supports d

「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。

Settings		Cancel
SIGN ON METHODS		
The sign-on method determines how a us	ser signs into and manages their credentials for an application in the 3rd party application.	on. Some sign-
Application username is determined by the	he user profile mapping. Configure profile mapping	
SAML 2.0 is the only sign-on optic	on 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 a	until you complete the setup instructions.	
View Setup Instructions		
Identity Provider metadata Is	available if this application supports dynamic configuration.	

ZPA ポータルにログインします。

Admin ID	
zpaadmin@nasiase.com	
Password	
Single Sign-On Usin	g ldP
Remember Me	Two Factor Authenticatio
Language	
English	

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。

dP Centiguater SAUL Atributes Settings				Quere com
Name	Terms AP Liefy (2)		Trap Spice	Actions
		Fair Street, Courts		

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

1 IdP Information	2 SP Metadata	3 Create IdP	
Name			
IdP Config			
Single Sign-On			
Admin 🕑 User			
Domains			
× nasiase.com			~

「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。

IdP Information	3 Create IdP
Configure the Service Provider information in your IdP	
SERVICE PROVIDER SAML METADATA FOR USER SSO	
Service Provider Metadata	Service Provider Certificate
L Download Metadata	🛓 Download Certificate
Service Provider URL	Service Provider Entity ID
https://samisp.private.zscaler.com/auth/72076300767985 753/sso 🚱	https://samisp.private.zscaler.com/auth/metadata/72076 0076/7985753 0

[Save]をクリックします。

Service Provider URL	https://samisp.pr/vate.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 abtain 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.			

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。

O Add	Rule				
Priority	Rule name			Status	Actions
1	Default sign on rule			Active	Not editable
	CONDITIONS		ACTIO	NS	
JL Use	r assigned this app	Allow acces	15		
9 Any	where				

[Next]をクリックし、ZPA 側の設定を続けます。

0	IdP Information	2 SP Metadata	3 Create IdP
Confi	igure the Service Provider i	nformation in your IdP	
SERV	ICE PROVIDER SAML METAD	ATA FOR USER SSO	
Servi	ce Provider Metadata		Service Provider Certificate
± Do	ownload Metadata		A Download Certificate
Servi	ce Provider URL		Service Provider Entity ID
https:/	//samisp.private.zscaler.com/a	uth/72076300767985	https://samisp.private.zscaler.com/auth/metadata/72076. 00767965753 10

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

1 IdP Information	2 SP Metadata	3 Create IdP	
Name			
IdP Config			
Authentication Domains			
× nasiase.com			e.
SAML ATTRIBUTES			
IdP Metadata File			
Upload Metadata File			Select File
IdP Certificate			
Upload the Certificate File			Select File
Single Sign-On URL			

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。

AME ATTRIBUTES	
IdP Metadata File	
netadala.	Change Remove
IdP Certificate	
Upload the Certificate File	Select File
Single Sign-On URL https://yahoo-co-zscaler.okta.com/ap	pp/zscaler_private_epcess/exk41hoy4JmgOZjGM4x6/sso/saml
http://www.okta.com/exk41hoy4Jmg	OZJGM4x6
Status	ZPA (SP) SAML Request
Enabled Disabled	Signed Unsigned
HTTP-Redirect	
Enabled Oisabled	
Pause	

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

lame	Status	MP Entity ID		Single Sign-	On	Actions
♥ ktP Contig	0	http://www.okta.com/ox841hoy4Jmg02j01A	nd.	Utor		1.0
Single Sign-On URL https://pation-on-pacalemonts.com/approxidem_private_access/eekil thoy4.dm	g02)0MMelysusysemi		2PA (SP) SAML Request © Signed		HTTP-Redirect	
Authintication Domains Pression com						
Import SAM, Attributes			SAMI, Attributes			
hasilase.com - O ligger			Simo Ampunis P			
LOWIS PROJECT AND ADDRESS FOR LODGED						
Service Provider Metadata			Service Provider Certificate Description Certificate			
Service Provider LRL, https://www.provider.com/w.itv72076300767885755/vae C			Service Provider Entity ID https://service.prvate.co.ee.com/auth/metadata?	7076300767985758 💆		
ar connecto						
Common Name yahoo-co-cicaler			Serial Number 1583168307958			
Created On Seeday , March 03 2020 1 0x 07 am			Expires On Sunday - March 03 2000 1/2/L07 am			
acont.						
SCIM Byrei						

[Save]をクリックします。

Name	SAM: Annual Stars
Faulture, SP Contig	(entropy)
Lasthians, of Conty.	union .
Proof, MP Davidj	i-m
Engentmentfearen, Lidt Gentig	Doursetsing
Geograms, IP Gong	12 mag house
Bow Comment	
must late store	
and another	
and the second second	
Territorian (
Landon Committee	

P Configuration SAML Attributes Se	dangs	All -		O Had Sittle, America
Name	SAM, Amoute	10 ² Name	Actions	
LastName.mtl Carrig	Lattime	ker Gers	1.1	
Findhame, of Carily	Professor	SP Carty	1.1	
treat tan Corty	trai .	Lat Comp	1.	
Groupfiane_Jaff Contig	(ingliere	ist Carty	1.1	
Dispartmentiliame, MP Contis	Destructione	adminutes	1.	

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。

	\bigcirc	
_	(2)	
T Y	his is the first time you are connecting to $\stackrel{ imes}{}^{ imes}$ ahoo-co-zscaler.okta.com from this browser	
	Sign In	
User	name	
use	r1@nasiase.com	
Pass	word	
R	emember mo	
	Sign In	
	Cigital Cigital	
Need	help signing in?	
	Welcome to zscalerna.com, us	er1!
	Create your zscalema.com account	
	Changes a format incomined months.	
	What is the food you least liked as a child?	•
	Answer	
	zpo test	





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。

			u l	The Farmer
 Creation Date	Bispiny Date	Common Name:	Actory	
	his territy Found			

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

Name		
Root		
Description		
Type Floot CA Intermediate CA	1	
Use for Zscaler App Errollment		

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

[Generate Certificate] をクリックします。

Enrolment Certificates Browne	Access Certificates			O Ligensie Certificate	2. Uplose Centroste Char	Contro Cl
Marra	Canadian Date	Europe Data	Common Name	Letons		Excard
> Root	Turnday, March 17 2020 1:37:18 am	Thursday, March 10 2058 1:37-18 am	nasasi con/Root			

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

Name		
Connector		
Description		
Type	Parent Certificate	
Noch CA Strangediate CA	Root	-
Use for Zscaler App Enrollment		
100 D Ma		

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。

	Creation Date	Exercity Date	Common Same	Actions		
		and a first stress				
Caronettar	Tansing Math 172620 1127 kl an	ilastreiday "Mach 14 2015 1-17-ill am	Nation Conf. C. Immedian			
Parent.	Tamping , March 17 2020 1:17 18 am	Thursday, March 10 2008 110718 am	Automa considerat.		1.1	
						_

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

Name		
Glient		
Description		
Type Root GA 🗢 Intermediate CA	Parent Certificate	
Use for Zscaler App Enrollment		
O Yes No		



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。

-	0-9-9-9-9-9-9-9-9-9-9-9-9-9-9-9-9-9-9-9	Connector Group	Create Provisioning Key	Review	Deploy Connector
Choose an existing prov	visioning key				
Créate a new provisionir	ng key				

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。

Constate May	Signing Certificate	3 Connector Group	Creste Provisioning Key	@ Review	Deploy Connector	
Ótoose a certificate		~				
Envi Loosth string		*0				
O Red. O Climit	Convector					
		Car Secon				
Consister						
Connector						
Connector Choose Key	 Signing Certificate 	Connector Group	Creste Provouaring Key	Review	Deploy Connector	
Connector Choose Key Corrector	Signing Certificate	Connector Group	Create Provisioning Key	Review	Deploy Connector	
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

Choose Key	Signing Certificate	3 Connector Group	Create Provisioning Key	Review	Deploy Connector	
	Select Connector Ges	up -		Add Connect	or Group	
Name AWS Tokyoj						
Description						
Status Cenabled Disuble	0	•				
Connectors						
Connector Software Updat	e Schedule					
Monday		~ e ^{00.00}			~	
Next Periodic Software Updat	er ins dem					
CONNECTOR LOCATIO	N					
Tokyo, Japan						0
						+
			Takyo Japan			-
						-
_						

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

Choose Key	 Signing Certificate 	Connector Group	Create Provisioning Key	G Review	Deploy Connector
lame WS Tokya					
faximum Reuse of Prov	isioning Key				
00					
stances of Provisioning	Key Reuse				

内容を確認して、[Save]をクリックします。

Choose Key	Signing Certificate	3 Connector Group	Create Provisioning Key	B Review	O Deploy Connector
Certificate Name					
Connector					
Connector Group					
AWS Tokyo					
Provisioning Key					
www.iokto					
Review all of the informa	ition before clicking Save				
ve mevious (Hançei				

[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。

	Signing Certhicate	Connector Group	Create Provisioning Key	6 Review	Deploy Connector
opy Provisioning Key 🏮					
UT 192118-YoudgOredAndy JosPoulite vicum gram-Ma Wagaciouspere vicum gram-Ma Wagaciouspere vicum gram-Ma Wagaciouspere vicum gram Wagaciouspere vicum gram Choose Platform	KUSgadow, Klovitwisy (populos) nu-du kistos Stolicka yr Cyfernol 2250,0W (1940, yr TwebGggCA4Las) Cyf leisiw Cauthwigu Prynt (1840, y	Svejblerivk (p.22musłki) Widdaws 20114 postania zaciałan Pros. – wisiesza Astor Istoff Tyckowicz – mistor WP+037253	Novaly Roby 90928		
	vm ware'	9	redhat.	ល្ងំ	amazon webservices
-	ACLE	202	+OF	-	Microsoft

Step2. Connector のインストール

AWS にログインします。

ign in	
O Root user	
Account owne unrestricted ac	r that performs tasks requiring ccess. Learn more
IAM user	
User within an Learn more	account that performs daily tasks
oot user email	address
username@exai	mple.com

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。

Corecalor.	Zscaler Private Access Connector	Pricing Details			
2300101	Connectors can be co-located with your enterprise applications, or they can be deployed in any	Bring Your Own Licen	se (BYOL)		
	location that has connectivity to the applications. Typically, they are deployed on network segments	Hourly Fees			
	that can access secured applications and the ZPA	Instance Type	Software	EC2	Total
	cloud simultaneously, such as in a DMZ.	t3a.medium	\$0.00	\$0.049	\$0.049/hr
	need any inbound	t3a.large	\$0.00	\$0.098	\$0.098/hr
	More info	Cla.xlarge	\$0.00	\$0.196	\$0.196/hr
	View Additional Details in AWS Marketplace	tha.2xiarge	\$0.00	\$0.392	\$0.392/hr
Product Details		t3 medium	\$0.00	\$0.054	\$0.054/hr
		t3.large	\$0.00	\$0.109	\$0.109/hr
Ву	Zscaler	t3.xlarge	\$0.00	\$0.218	\$0.218/hr
Customer Rating	*****(0)	13.2xlarge	\$0.00	\$0.435	\$0.435/hr
Latest Version	ZPA Connector AMI 2019.08	m5a.large	\$0.00	\$0,112	\$0.112/hr
Base Operating System	Linux/Unix, CentOS 7	m5a xlarge	\$0.00	\$0.224	\$0.224/hr
Delivery Method	64-bit (x86) Amazon Machine Image (AMI)	m5a.2xlarge	\$0.00	\$0.448	\$0.448/hr
License Agreement	End User License Agreement	m5a.4xtarpe	\$0.00	\$0.896	\$0.896/hr
On Marketplace Since	8/30/19	m5.large	\$0.00	\$0,124	\$0.124/hr
AWS Services Required	Amazon EC2. Amazon EBS, Amazon VPC	m5 xlarge	\$0.00	\$0.248	\$0.248/hr
Highlights		m5.2xlarge	\$0.00	\$0.496	\$0.496/hr
inginigrica		m5.4xlarge	\$0.00	\$0.992	\$0.992/hr

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

ton 2: (Choose on Instance Tune							
0	General purplete	12.2xtarge			1221.010		Michenty	- 10
2	Centers property	Danes.	2	63	ittes any	- 10	Lights & Riggert	144
ð	Genin's purpose	thirmings	2	- F.	700 ore	70	Lip to 5 Gigathit	90.
8	General purpose	the small	2	7	ITS only	~	Up to 5 Gigent	
	General purpose	the medium	2	4	EBIS only	16	Lip to 5 Gigsbit	10.
	General purpose	thalarge	z	×	EBS only	34	Up to 5 Gigatori	100
	General purpose	thuirge		16	JEBIS only	'96	Up to 5 Gigabit	765
	General purpose	t3a2xtarge		52	EBS only	74	Up to 5-Gigabit	794
5	General purplem	EL-mero	2	-0.5	1251 010	10	Lation 5 Gapacit	- 10
D-	Genes pupper	0.000	2		126.00	-	Up to 3 Gigent	- 14
ð	General Jurgeon	15 invati	2	3	135 ora	70	Lip to 5 Rightet	
	General purpose	S.medum	2	4	1315 only	Tes	Up to 5-Gigabit	Yes
	General purpose	things	2		EBIS only	785	Up to 5 Gigsbit	784
•	Genesi purpose	t3.xiarge		18.	EBS only	94	Up to 5-Gigabit	745
	General purpose	0.2xterps		32	E3/5 only	764	Up to 5-Gapient	785
5	General purpose	etatiop	1		1.4.79.galoj	-	Up to 10 Geptier	141
8	General purposit	reliant storage	4	16.	1 + 152 (502)	24	Lie to 10 General	14.

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。

Carviolas - H	- Lound		P committee and
could AM. / Chosed systems Appr	3.0	Agure Instance 4. Not Demon 1. Act Tap 1. L'Unifigue Decemp Group 1. Novey	
p 3: Configure Instan	ce D	atails	
pure the instance to suit your respute	merce.	co clari laurezh multiple instalezen from the same AMI, request Spot instances to take advantag	a of the lower pricing, assign an access management risk to the instance, and more.
Number of instances	00.5	 Laurott ette Auto Scotting Group (3). 	
Purchaning option	00	Jeper fast emesa-	
Network	00	vpo-latitindasi tische78 (ZPA B) C Owite new VPO	
Subnet	18	Nubmet-0075id29p158h1/h211c Public submet ap-no. Create new submet 246 IP Acdrestes available	
Auto-assign Public IP	00	Use extract setting (Evable) \$	
Placement group	(8) -	C Add entitience to placement group	
Capacity Reservation	ŵ.,	Open. 1 C Desire new Capacity Reserved	han the second se
JAM inde	00	Noine I C Create new PAA now	
CPU options	6	C Specify CPU options	
Shutdown behavior	0	tanp t	
Bruable termination protection	0	Protect agamsI accidental termination	
Monitoring	60	Trable CouldWatch detailed monitoring Additional charges apply	
EB5-optimized instance	0.	- Caurton III EXIS-operation Internal	
Tenancy	9	Shared - Run a stared herdware instance B Additional charger will apply for disclosed tenancy.	
Elastic Inference	90	Add an Easte internet accessition Additional (herges apply)	

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

ume Type ().	Device 1	Sespanot (j)	See (58) ()	Volume Type	IOPS	Throughput (MB/n)	Delete on Termination ()	Encaption ()			
d New Volume	10m/k/dz	snip-lictor/millifieed85	*	General Purpose SSO (gp2)	 via / 3000 	NA	•	nut Emilythed	•		
er ter eligible cust agie hethictoris	temens can get up to 3	0 GB of EBS General Purpose (S	III) or Magnetic store	ps. Livers more about the usage tier el	gibility and						
										C	COLORADO IN

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。

tep 5: Add Tags			
ag consists of a case-nerodive key-value pair. For exemple, you could defi	re a tag with key ,= fairne and value = Verberver. Learn more about tagging your	Amazon (C2) excavors.	
NY 1038 characters teachers)	Value (201-branches insetsure)		
	App Connector	0	
d another tag			

何も変更せずに[Review and Launch]をクリックします。

	Assign a security group: (Charles a new security group Select on existing security group	and the set of the set			
	Security group name: Description:	Zhoaier Phutte Access Connector-JPA Conn This recurity group was generated by AWS M	ector AMI 2019-08-AutogenByAWS Terkerplace and is based on recorm.			
- (i)		Protocol	Port Range	Source	Description	
	0	109	12	Custom 1 = 0.0.00	w.g. Stille for Autom Deviator.	e
Rule						
Rules in	ng eh nazok of 2020 allow a	II P accommons to access your Instances. We reco	erment setting security group rules to slove access true.	krowt P jeżsniani priy		
Rules in	ng ah munic of 2010.05 allow a	II IP inclumines to access your instances. We reco	ennend setting security group rules to allow access trun	krowt P latitetiani oriy		

内容を確認して、[Launch]をクリックします。

p 7: Review	Instance L	aunch	to edit changes for each	n section, Click Launch to assign a k	ey pair to your instance and complete the	iaunch procesa.		
Your instances You can also or	ur instances' si may be accessible pen additional port	ecurity. Your a from any IP at ts in your secur	security group, Zsi idress. We recommend to ity group to facilitate acco	caler Private Access Connect hat you update your security group n sets to the application or service you	dor-ZPA Consector AMI 2019-08 ules to allow access from known IP addres to running, e.g., HTTP (80) for web serving	AutogenByAWSMP-2, is open to the world, eles only. I. Edit security groups		
Your instan To leunch an m	ce configuratio stance that's eligit	in is not eligi de for the free o	ible for the free uses	ge tier A selection, instance type, configurat	ton options, or storage devices. Learn mo	re about free usage for eligibility and usage restrictions.		
							E-to AM	
Detaile							Loss Perce	
I Details Zscaler F	Private Access C	connector						
Al Details Zscaler F fluit Center	Private Access C	Connector						
Al Details Zscaler F Real Device Hourty So Software o By launch End Date	Private Access C Type en Virtualori Rware Fees: \$2.0 charges will begin o charges will begin o charges will begin o	Connector Lie type hus IC per hour on to once you laund ou will be subsc to	Listarge Instance. Addition this AMI and continue u ribed to this software an	nal taxes or fees may apply, and you terminate the instance. It agree that your use of this software	Is subject to the pricing series and the se	ors.		
Al Details Zscaler F fear Over Hourty So Software o By fearch End User stance Type	Private Access C Iger en Undent Rware Fees: \$1.0 charges will begin o ng this product, yo License Agnement	Connector Lia Igar Hus Di per Nour on 10 once you isunct conce you isunct conce you isunct conce you isunct conce you isunct concert	Listarge instance. Additio In this AMI and continue o XBed to this software an	ond taxes of fees may koply, and you terminate the instance. It agree that your use of this software	e is subject to the pricing series and the se	9 7 3	Edit instance type	
Il Details Zscaler F Build Decis Hourty So Software C By Isunch End Liner tance Type Instance Type	Private Access C Inee an Unated Reare Fees: \$0.0 hargen will begin o ng Tila product, yo Lichne Agner ad ECUs	Connector Lie ger hour on to once you laund ou will be subsc e wCPUs	3.xtarga instance. Additio this AMI and continue o stbed to this software an Memory (GRB)	onal taxes or hele may apply, until you seminate the instance. It agree that your use of this software Instance Storage (SBI)	e a subject to the pricing semis and the se EBS-Optimized Available	Ter 1. Network Performance	Edit instance type	
Il Details Zscaler F Hourty So Software C By Ranch End Daar tance Type stance Type	Private Access C Iner en Wouldet Rware Fees: 52.0 charges will begin o charges will begin o charges Agreemen ECUs Versebe	Connector Lin gar has Di per hour on ti once you isund ou wit be subsc tr wCPUs 4	Subarge Instance. Addition him. AMI and continue o protect to this software and Memory (GRB) 18	tral taxes of fees may apply, and you seminate the instance. It agree that your use of this software Instance Storage (SBS) EBS only.	e is subject to the pricing terms and the se EBS-Optimized Available Yes	Network Performance Lip to 3 Gypt	Edit instance type	

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。

o obtain the password used to log into your instance. For Linux AMIs, the private key file allows ecurely SSH into your instance. Note: The selected key pair will be added to the set of keys authorized for this instance. Learn mount bout removing existing key pairs from a public AMI.	you to
ecurely SSH into your instance. Note: The selected key pair will be added to the set of keys authorized for this instance. Learn m nbout removing existing key pairs from a public AMI.	nore
lote: The selected key pair will be added to the set of keys authorized for this instance. Learn m bout removing existing key pairs from a public AMI.	ore
bout removing existing key pairs from a public AMI.	
Choose an existing key pair	\$
Select a key pair	
AWS_Tokyo	•
I acknowledge that I have access to the selected private key file (AWS_Tokyo.pem), and t	hat
without this file, I won't be able to log into my instance.	

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)。

	ch instance	LOP	C ACDONS -												4	0	۰	6
Q,	Filmr by tags and uthilo	ubes (or assect by keyword											0 K K	1 to 1	6 of 6		
	Name		Instance ID +	Instance Type -	Availability Zone -	Instance State -	Status Checks	-	Alarm Status		Public DNS (IPv4) -	IPv4 Public IP	+	IPv6 IPs	+	Key N	ame	
	Ampon Linux		1-0974c01114eb3b348	12 mians	ap-northeast-ta	noning	© 2/2 checks pained		Nonir		ec2-13-114-84-208.ap	13 114 84 208				AWS_	Tokyo.	
	Web/Server2		i-Ocfd00090ebballd2ld	12.19620	ap-notheast-1a	🔵 nunning	2/2 shecks passed		None	2	ec2-13-231-121-48.ap	13.231.121.48				ANS_	fokyo	
	WebServer1&DNS		i-0d56798d4e2eb78	12 micro	ap-northeast-fa	Running	Ø 2/2 checks passed		None	2	ec2-54-250-201-33.ap-	54,250,201.33				ANS_	fokye.	
			1-01876005a84c3d145	t3 slarge	ap-notheast-fa	😝 slopped			Noné	1						AWS_	fokya	
	App Connector		-02abd09a296bb33	t3.xiarge	ap-northeast-fa	 numming 	2/2 checks passed		None	5	ec2-3-113-31-212.ap-n	3.113.31.210				ANS_	Tokyo	
			10c9/38ad6c425be4	13.xiarpe	ap-northeast-1a	beqqola 😜			Nore	5						ANS.	Tokyo	

Connection method	A standalone SSH client Gession Manager EC2 Instance Connect (browser-based SSH connection)
To access your instanc	e:
1. Open an SSH clier	nt. (find out how to connect using PuTTY)
 Locate your privat instance. 	e key file (AWS_Tokyo.pem). The wizard automatically detects the key you used to launch the
3. Your key must not	be publicly viewable for SSH to work. Use this command if needed:
chmod 400 A	WWS_Tokyo.pem
4. Connect to your in	istance using its Public DNS:
ec2-3-113-3	11-210.op-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 tha your AMI usage	It in most cases the username above will be correct, nowever please ensure that you read a instructions to ensure that the AMI owner has not changed the default AMI username.
If you need any assistant	ce connecting to your instance, please see our connection documentation.

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.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。

Connectors Connector Groups	Connector Provisioning Keys				
Name	Maximum # of Connectors	# of Enrolled Connectors	Connector Group	Provisioning Key	Actons
> Auto beyo	-	σ.	AMS Torgs	RED I MET	× ×

-			
C	Copy the key of AWS Tokyo		

api.private.zscaler.com/4G1Z78PmVkl.syzjZVb/1qLjSe/axGddyOZHdBsRpUF7Puf9esSJcUV8JBFOMPDOG9OGxuvZT9ZTiBsYgu3gOn z0A0RgkXJ9qcaocwJ0iovWxrRdYjPpg3KkK0vqblpqVx1pZ2mu4IRVIWMMvcZfTU4hKaVQaVUssFbajl6EvscUW/gw3H+Mutu+QLH6S/hx SNSCA0/yYCyG1WOCpxSMoi4OzGR0nPBG+wBil622ArjScNhGzq7yTrNCqKIdXZe8pEKbYAaK5AmQZ5I0JWv784guyTuwbGgqQxA/Lcz z3Bd9TjjGUpWzx+mbtc6wKFuQ37Zu2dfiOfKZwWYP3yjvXOawhriPin6cthPGYGY1ec8lv/QuL9w6yJrPvy1z1AVUY

x

🖲 📒 D Downloads — admin@ip-10-1-0-113:~ — ssh -i AWS_Tokyo.	pern admin@ec2-3-113-31-210.ap-northeast-1.compute.amazonaws.com - 133x
1 api.private.zscaler.com 46fZ78PmVkLsyzjZVb/1qLjSe/ax0ddy0ZHd xrRdYjPpg3KkK8vqblpqVx1pZzmu41RViWMMvcZfTU4hKaVQaVUssFbajl6Evs q7yTrNCqKIdXZe8pEKbYAaK5AmQZ5I0JWv784guyTuwbGgqQxA/Lczz3Bd9Tjj rPvy1z1AVUY	3sRpUF7Puf9esSJcUV8JBFOMPD0690GxuvZT9ZTIBsYgu3gOnz8A0RgkXJ9qcaocwJ8iovW :UW/gw3H+Mutu+QLH6S/hxSNSCA0/yYCyG1WDCpxSMol40z6R0nPBG+wBi1622ArjScNhGz 3UpWzx+mbtc6wKFuQ37Zu2dli0fKZwWYP3yjvX0awhrIPln6cthPGYGY1ec8lv/QuL9w6yJ
	the second se
3	
:wq	

- 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。

						Eso facand
878	Status	Section	Update Status	Current Software Version	Actions	
auti ingo-i	0	Adventised		18.122.2	1 -	
Convelctor Group		Consistor Platform. Entreprise Unix 7		Last Software Update: Not Available		
2EN: AP-39-8467		Last Connection to 25%: Mar 179, (1157 US7)		Last Disconnect from ZEN: Jan tst. 08:00 (JST)		
Location: Tokyc, Japan		Public IP: 3.113.31.210		Private IP: 10.1.0.113		
Uptime: Stvs Itmes		Signing Certificate:				
Description:						

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

	rue -	Q 2
MINERS	Led James	6 0 6 6
Nat		
COMMESTINS	Name Add Targen 1 Land Optimized View (Proc. 01-07-040-0207)	000



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。

West Server Goups				- 6 gunte
-	Antonio	Domains of IP Addressio	Actions	
		198-Territo Financial		

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

Add Server	
Name	
Windows Server2019	
Description	
Status	
C Enabled Desabled	
Domain or IP Address	
10.1,0.230	
Server Groups	

社内ポータルの設定例

Add Server	×
Name	
Web Server1	
Description	
Enabled Disabled	
Domain or IP Address	
www.zscalerjapan.com	
Server Groups	
No. of the second data and data and	

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

lano.	Reter	Der	nam or IP Address	Actions	
angaa devertiin 🛓	۰		1.139	A 4	
Server Groups				and the second second	Q Add Server Group
					Ego Counci All
Later	Status	Dynamic Server Decovery	Connector Groups	Action	
Servir Girolg	0	0		× *	

社内サーバの設定例

Name	
Tech Windows Server	
Description	
Status Dynamic Server Discovery	
Carlos Enabled On Off	
X Windows Sener2019	
Connector Groups	
× AWS Tokyo	

社内ポータルの設定例

lame	
ntra web site	
Description	
Dynamic Server Discovery On On	
× Web Server1	
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

Application Segments Brow	ser Accesa Segment Groups			even sy same some or P associ	🛞 1943 Sauch Danama 🔒 Add According Segured
					Egg Excent 4
Name	Applications	Satur	Health Reporting	Health Oheck	Actions
5 mismai Application	"missage.com	0	Of Acona	0	0 / *

必要事項を記入し [Next] をクリックします。

社内サーバの設定例

Define Applications Egment Grou	p 🗿 Server Groups	O Servers	O Review	O Policies	
GENERAL INFORMATION					
Name Tech Windows Berver2019		Status Crebied	Disabled		
Description					
APPLICATIONS					
10.1.0.230			8	Browser Access	۰.
					O Auto Marry
EN ZSCALER APP ADDESS					
TCP Port Ranges					
3389	2380				
					O Assistance
UUP Port Hanges	D.,				
					O Add Mary
NUMBER OF STREET, STRE					
Enableo O Courbind	Bypain Litre Che	nt Forwarding Policy			
COMMON COMPOLINATION					
Harite Benedian		Hard Chard			
Continueus On Access		O Default	Nore		

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

Define Applications	Sagment Group	O Server Groups	O Servers	@ Review	O Policies	
	Select Segment Group				Add Segment Group	
Name Rich Windows Server						
Description						
Status Stratbind Onucleud						

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。

 Define Applications 	Segment Group	 Server Groups 	O Servers O Review	Policies	
	Select Server Group			Add Server Group	
Seed a Server Group					~
Europe a sectory corregi					×q
O Intra web site			Server Group		
C Tech Windows Server					
					Cear Selectors

efine Applications	Segment Group	Server Groups	O Servers	O Review	O Policies	
	Select Server Group				Add Server Gener	
	Select Server Group				Add Server Geold	

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

Define Applications	Segment Group	3 Server Groups	O Servers	Review	O Policies	
	Select Server				Add Server	
Windows Server2018						

内容を確認して[Save]をクリックします。

O Desig Performances	Segment Group	Server Groups	O Servers	O Review	O Policies	
Application Sagment			Application Sage	ent Status		
lach Windows Server2013			© Enabled			
Segment Group			Segment Group 5	ama.		
Inch Wooldows Server			© Endered			
			1.1.1.1.1.1.1			
lerver Group Inch Worldway Server			Server Group Bits	6.m		
			1000			
lervers-						
Windows Server2019						
Demestor Groups						
Kitth Tokyos						
ienet2019 Geoups						
sector Groups						
Alb. Tokyo						

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

 Define Applications 	Segment Group	Server Groups	Servers	6 Review	Palicies	
POLICY						Ess Estand
Rule Order	Name		Rule Action			
5 -	Allow Internal Application Group		 Allow Acces 	sis		

社内サーバの設定例

Deliver Applications O Segme	nt Group 3 Server Groups	O Servers	O Review	O Polpes		
CENERAL INFORMATION						
Narie		Status				
www.zsc.ellerjapam.com		© Enabled	Indiated			
Description						
APPLICATIONS						
www.zscolingapan.com			8	Browner Access		
				C. Investigation		
					O Add Maer	
EL ZECALER APP ACCESS						
100 Deel Distant						
80	87					
	40					
					O And Mary	
UDP Port Ranges						
Ferri.						
					O And More	
ADEITRONAL DOMPTILIANTION						
Double Encryption	Bypan	•				
Contract O Description	Ute L	ient Forwarding Policy			<u>~</u>	
COMMON CONTRATION						
Health Reporting		Health Check				
Continues. O On Access		O Default	Norm			

Define Applications	Segment Group	Server Groups	O Servers	@ Rovew	O Polces	
	Smith Segment Droug				Add Sygnent Group	
Name Intra web site						
Description						
Status						
C ENDAG						

O Define Applications	Segment Group	Server Groups	Servers	Review	Policies	
	Select Server Group				And Server Group	
elect a Server Group						
Enter & Search string						

Define Applications	Segment Group	3 Server Groups	 Servers Beview 	O Policies	
	Select Server			Add Serie	
X THED Server1					
Tindo Servier					*

Define Applications	Segment Group	Server Groups	 Servers 	Beview	O Policies	
oplication Segment			Application Segme	nt Status		
www.zscalimjapan.com			 Ensitied 			
Command Conven			Roomant Concer St	all and		
the web site			C Enablert			
ierver Group			Server Group Statu	-		
ntra web site			 Enabled 			
Net Second						
ALL THIAL I						
Connector Groups						
WS Takyo						

Step3. Access Policy の作成

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



coess Policy Timeou	t Policy Client Frewarding Policy			0
Rule Order	Nama		Ruit Actor	Actions
¥ 1	Altre internal Approxities Serval		S Alma Access	a.e. +
Description Net Available		Ruis Action Anno Action Criteria scratarios scratarios Apricator Oracio		

[Add rule]をクリックします。

Access Pisky Time	of Policy Cland Forwarding Policy		C Att Ave
Rule Dear	Name	Ruit Action	Actume
*)	Allow Internal Application George	C Aller Access	
And Annual Annua		Public Active St Allow Access Contents Instead of Sectors of Sectors of Sectors of Sectors of Sectors of Sectors of Sectors	

営業部門の Attribute

Name		
Deny Tech Server for Sales_Div		
Description		
TION		
Rule Action	Message to User	
Allow Access OBlock Access	You don't have a permission to access this site.]	4
DITEDIA		
ALCOMA		
Application Segments X Tech Windows Server2019		-
GR		
Segment Groups		
Select one or more segment groups		÷.
SAML Attributes		O Select IdP
⊶ IdP Config		
GroupName_IdP Config	Sales_Div	0
0		 Add Mone
Client Types		
Any client type		
Zscaler App Posture Profiles		
Select a posture profile	÷	
		O Add More
Zenales Ann Trusted Networks		
Select one or more trusted networks		~

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 Timeou	Policy Client Forwarding Policy		Ana fuir
Rule Order	Name	Rule Action	Actions
• 1	Dary Solt-Server for Sales, Shi	O BROAALCOM	
Description Ret Ausuble		Rule Action Rule Action Cethols Set Around Structures Set Around Structures Action Action Action Cethol Action Cethol Action Cethol Action Cethol Action Actio	
* 1	Allor Hits sets site and Tech Westewe Dever	Attas Access	0.0.0
Description Not Austable		Rule Action Rule Action Rule Action Cohena Arm packed strategy and	

Name	
Allow Intra web site and Tech Windows Server	
Description .	
Description	
CTION	
Rule Action Message to User	
Allow Access Block Access	
RITERIA	
Application Compare	
X Tech Windows Server2019 X www.zscalerjapan.com	
OR	
Segment Groups	
Salart opp or more samplet minutes	~
D	
- SAML Attributes	O Select IdP
Any SAML attribute from any IdP	
D	
- Client Types	
Any client type ~	
D	
Zscaler App Posture Profiles	
Select a posture profile	
	O Add More
D	
Zscaler Ann Trusted Networks	
berect one or more trusted networks	

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

Access Policy (Reena	n manay – Galani Hanisantang Hanay		
Rule Order	Nane	Bule Action	Action
÷ 1	Sleny Tech Server for Sales, Div	O Block Access	01.
Description tetr Available	(<u>-</u>	Nute Action Table Action Tab	
• £	Autor Intra well site and Sech Weddows Server	G Atina Access	
Description Not Augiliphe		Rule Action Alters Access. Ordense Amy Saccess Results of a Amy Saccess Results of a Result Standard Saccess of a second second second second Results Standard Saccess of a second	
	Allow memory Apple allon Group	Altre Access	

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。



Szscaler & Deshboard 🛛 Enrolled Devices	
zscaler App Dashboard	All Users - All States - All OS -
Zscaler App License	Device Model
100	
80	
60	

DATE SETTINGS								
Automatic Rollout								
Aliwayo Littled Version	Specific Version Canad	Renet O Death						
Care Land								
-								
544 5444								
VICE SWAPSHOT								
VICE SNAPSHOT								
Come VICE STUPEHOT Windows					macOS			
Application	Registered	Reisons	Download	Download	macO5 Appleation	Registance	Rainan	Download
VICE SNAPSHOT Windows Application Version	Registered Devices.	Painane Notae	Download, EXE	Download: MSI	macOS Application Version	Registance Devices	Rainater Notes	Download, Link
VICE SHAPSHOT WICKE SHAPSHOT Windows Application Version	Registered Devices.	Painane Notas	Download EXE	Downinad MSI	macOS Application Version	Registered Devices	Roissan Notas	Download Link

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-ggz-2.1.0.190-inst	taller 25.9 MB	Application	Today 2:24	
I Zscaler-osx-2.1installe	r.app.zip 24.9 MB	ZIP archive	Today 2:24	
# AWS_Tokyo.pem	2 KB	printablarchive	Today 1:40	
metadata	2 KB	TextEdit	Today 1:25	

and the second se	
Installing	

Installing	
Installation completed	

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。

Connecting to
okta
Sign In
Geername
Laver (gmanuase.com Paseword
Remardur na
Savine .



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



A	Connectivity	
rivate Access	Usemane	user1@nasiase.com
	Service Status	ON TURN OFF
Ω	Authentication Status	Authenticated
Notifications	Broker	52.198.72.244
_	Time Connected	03/17/2020 02:25AM
•	Statistics	
More	Total Bytes Sent	0 bytes
	Total Bytes Received	0 bytes

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。

Ozscaler	St Derr	Courd Encoded Devices	A App Profile 9% Administratio						2
) Tanima			Al Gara -	tare -	AR 105				-
ta Demen		Share St.	Di Terri	Draine Model		Z App Version	Paring Status		
	1.1	unit/divisioni.com	Windows	tion HMM-parent/		1518	Signature		
		Antilinimum	cae10	Appier Man Brand	Petta	210390	Lipseters	10	

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



0	Connectivity	
ate Access	Username	user1@nasiase.com
	Service Status	ON Off Trusted Network
Ω	Authentication Status	Authenticated
tifications	Broker	165.225.110.251
-	Time Connected	03/18/2020 07:16PM
•	Statistics	
More	Total Bytes Sent	2.84 KB
	Total Bytes Received	1.10 MB

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。

••	Microsoft Remote Desktop	-
888 = 🔅 - + -	PCs Workspaces	Q Search
	/ 8	
k		
10.1.0.230		

 You are connecting to the RDP host "10.1.0.230". The certificate couldn't be verified back to a root certificate. Your connection may not be secure. Do you want to continue?

 Show Certificate
 Cancel

 Configuring remote PC...

 Cancel



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。

リモート デスクトップ 接続		
全般 画面 ローカルリソース エクスペリエンス 詳細設定 ログオン設定		
アノドニック UNINE X ADD COOL アノビニークー(O: 10.1.0.200 ~) リモート・デスクトップ理想 ×		
※ 内部エラーが発生しました。 200		~ D Y
OK 14700 >25	caler	•
度能設定 現在の接続設定をNDPファイボに保存するか、または保存された接続を 聞いてください。 使わたの ののでの のののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでの ののでのの ののののの のののの のののののの	Connectivity	
settin antisticknitche with	Username	user2@naslase.com
**************************************	Service Status	ON Off-Trusted Network
Notifications	Authentication Status	Authenticated
•	Time Connected	末,318202007:15:26 午後
More	Statistics	
	Total Bytes Sent	861 bytes
	Total Bytes Received	550.27 E8 Warning You don't have a permission to access this site.

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。

3 1	0 1	BACK CLOPER	0	4	1048
APPLICATIONS ACCESSED	A 10P	APPLICATIONS BT BAROWIDTH			
		1000 1010 000			
and the second sec	-	and statements and			
C 1.1.1.2.00 (Sate					
			-		
The second		TOP POLICY BLOCKS			
▲ TOP EXERCICE Converting States Agenced Page Converting 2020		TOP POLICY BLOCKS			
A TOP ENROUG Converting Game Cameration (2019) Approximate		TOP POLICY BLOCKS IN POLICY BLOCKS Transat Francy B costs Pracy Blocks			
Tor Encode Converting Galaxy Agrounding Converting 70% Agronomet		TOP POLICY BLOCKS on Pally Books onto Pally Books * Appendix puty Model around			

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。

~						It has to be the the	et loge mate lie mus maint that the best present
	17		0 879000	ACCESS POLICY BLOCKS	THREGUT POLICY BLOCKS	successes. 12	2
	• ha titles taue take sparse						
•;	Appry Cherrie At O Anterna	ġ.					<u>.</u>
a.	Connection 🕞	urc	Policy	Liner ([])	ZEN	Connector	Application
	> Mar tilm, 19.08/07.075.037		Damp from the same dam	user/Wenizer.com	AP-39-6805	No corrector can reach the approacher	10.1.0.200 (0.049 10.24
0	> Mer 189, 16/25/25/407-257		tion the set of an excite	user Planause cont.	NP-3P-8405	Kell Tays 1	environitativgapan com 180 TCP
And And	> Mar 1889, 19 25-35 408		Allow this and allower lot the	une Offension, con	19-39-4862	440.5mp.1	www.cotaletypin.com #010P
	> Mar 1881, 18 (4 15 624 - 5162)		Allow Price and Says and Says Man.	user Dimension Laws	AP. P. 4464	and Search	16.1.0.200 (state TCP
	> Mar 1891, 19:22:51.408.257		Allow this way us and lost (too	uner filteringen zuen	AF-19-4464	And Server 1	www.splainsplan.com; ski2 10P
	3 Mar 186, 1922-11, 486 207		Alow this well signed that this,	user (drawman	4P-3P-8851	Auto Berge 1	serve-bucklegalar, com 145 10P
	> Mar 186, 192243.217 Jat		Allow from even late and fight little	wert Brasses com	41-21-3462	AND TIME I	www.zonietjęca.com Al TOP
	> Mar 189, 1923-45,254 297		Man the set of an inchise	user's Provident costs	10-57-1464	ANNI Taman I	www.coolemiplan.com #0.107

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 🥥	ute.	Policy	One (5	289	Convector	Application
W sthert that: Mar 189, 18,00,07,275,307		ADDES PERCENTANE Desy fact dance for lases (Dr. T	unternante unerfölgangen som T	10001 AF-27-6402	NAME No connector car much this application	MULLING SHE TOP Y
the test Mar New, 1826/07-276, (67		ACTON Deep	18.112.86.175	sizerites Shephy Dhy At	an annual a respective. Unavailable YDP	armunation langeme Sect Minister Security T
алапольских Ардиналог разку поссеня актова Т		POLICE D TOURISOURTHEITE D	Location Tanya.P	POLICE PRODUCTIONS	Location. Unavailable	control principal a recording . United to the TCP
HITTING THE ALLER BURGER OF			CLASHE THEFT Zocame App	neresso cuest 9.8	LINAMOTICA IN LINAMOTICA	Annaciation di Patrimbiane/Weilith @
STRILS Genet Connection			Funturnities	te to convector 0.9	TO AN A CONTRACT OF A CONTRACT	Service at Universite the
Durinition Trea				eta descari conseccione 10.15	construction and in some	Designal desperations Designed
1014, 81100 B				to more and	CONNECTOR LINCLP ID Linuxelistore	
COMECTONIC DisplationBankSTK.Pv.Misslar						
• A C						
> Mar 189, 19,25,20 A07,481		Allow mes was also and face time.	confidences core	AP-37-840	week tangen 1	www.zsiatetapan.com.dl/10 ²
3 Mar 189, 1922-33,406.107		Allow letter well also and Tach 100	contribution com	AF-3P-6465	AND Days 1	www.teislerjapan.com #0.7024
> Marises, Hoseisa kokulat		Allow stres well also and Tech View	unier Menangen John	AP-37-3464	were longer t	10.1.0.200 (3864 TCP)
> Mar 18m, 10:20-01 am .017		Africa series and one and Tach Street	ware between a server	47-37-8464	and have 1	and minimum over that TOP

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。

Name	
All Application in AWS Tokyo	
Description	
	1.
Status Dynamic Server Discovery	
Con Off	
Connector Groups	
× AWS Tokyo	

義が完了します。

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

Add Server Group		×
Name All Application in AWS Korea		
Description		
		le.
Status Carabled Disabled	Dynamic Server Discovery	
Connector Groups		
× AWS Korea		
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

SENERAL INFORMATION	
Name	Status
zscalerjapan	Senabled Disabled
Description	
APPLICATIONS	<i>h</i>
*.zscalerjapan.com	Browser Access
	Add More
S ZSCALER APP ACCESS	
TCP Port Ranges	
80	80
443	443
	Add More
UDP Port Ranges	
From	To
ADDITIONAL CONFIGURATION	
Double Encryption	Bypass
Enabled Oisabled	Use Client Forwarding Policy
COMMON CONFIGURATION	
Health Reporting	Health Check
Continuous On Access	Contraction Default None
Server Groups	Segment Group
X Ali Intra Web Site	- Zscaler -

Name Tech Windows Server2019	Status	a
Description		_
APPLICATIONS		
10.1.0.0/24	Brow Access	Nser
		Add More
S ZSCALER APP ACCESS		
TCP Port Ranges		
3389	3389	O Add More
UDP Port Ranges		
From	To	• Add More
ADDITIONAL CONFIGURATION		
Double Encryption	Bypass	
Enabled Sizebled	Use Client Forwarding Policy	Ť
COMMON CONFIGURATION		
Health Reporting	Health Check	
Continuous On Access	O Default None	
Server Groups X All Application in AWS Tokyo	Segment Group	-

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

ile Order	Name	Rule Action	Actions
(I	Deny Tech Server for Sales_Div	O Block Access	0 / ×
Description Not Available		Rule Action Block Access Criteria AND SAMLATTRIBUTES GroupName_kdP Config = Sakes_Div	
2	Allow lintra web site and Tech Windows Server	Allow Access	0 / x
Description Not Available		Rule Action Allow Access Oriteria APPLCATION SEGMENTS Escamputor of Text Windows Server2019	

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。

	TOP POLICY BLOCKS	
	Sen data and data for free reason	
TOP APPLICATIONS BY USERS	APPLICATIONS DISCOVERED IN PAST 14 DAYS APPLICATIONS DISCOVERED IN PAST 14 DAYS APPLICATIONS DISCOVERED IN PAST 14 DAYS APPLICATIONS DISCOVERED IN PAST 14 DAYS	(tee) Application
104 of has Feasible	Teles Senate Agencies	

[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。

Physical Contents (1999)	and the second se	-		
			TOP POLICY BLOCKS	
	In the events to record		in control processing of the interview of	
тон аркладтова ву шена		19	APPLICATIONS DIRCOVERED IN PAST 14 DAYS	Sense Augustanes s
	and the ferrers.		The Sone Junity, Com-	

Define Applications	Segment Group	3 Server Groups	O Servers	Review O Policie	25
GENERAL INFORMATION					
Name			Status		
-			C ET BELIEVE		
Description					
					4
APPLICATIONS					
drive zacalerjapan.com				Browser Access	
					O Add More
S ZSCALER APP ACCESS					
TCP Port Ranges					
80		BO			1.000

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。

Ozscaler	Dashbo	ard Devic	es 🛔 App Profiles 🗳 Administr	ation	0
Settings Scaler App Store	O Add For	warding Prolite			
scaler App Natifications udit Logs		Profile Name	Trusted Network Criteria	Forwarding Profile Action	
orwarding Profile	1	Default	CRITERIA.	ON TRUSTED NETWORK	
Fusted Networks			None	Tunnel	
scaler App Support				VPN TRUSTED NETWORK	
ser Agent				None	
scaler App IdP				OFF TRUSTED NETWORK	
levice Posture				Tunnel	

 ※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

PROFILE DEFINITION		
Profile Name 🔮		
Mac		
TRUSTED NETWORK CRITI	ERIA	
Add Condition 😢		
Select	Ada Condition	
Condition Match		
Any	*	
DNS Servers		
192.168.1.100	×	
WINDOWS DRIVER SELECT		
WINDOWS DRIVER SELECT Tunnel Driver Type @ Route Based Pa	TION acket Filter Based	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based FORWARDING PROFILE AC	TION acket Filter Based	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Pa FORWARDING PROFILE AC On Trusted Network	TION acket Filter Based	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based FORWARDING PROFILE AC On Trusted Network Tunnel None	TION acket Filter Based	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Par FORWARDING PROFILE AC On Trusted Network Tunnel Notwork VPN Trusted Network	TION acket Filter Based	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Particle FORWARDING PROFILE AC On Trusted Network Tunnel None VPN Trusted Network Same as "On Trusted N	TION acket Filter Based CTION FOR ZPA	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Particle FORWARDING PROFILE AC On Trusted Network Tunnel None VPN Trusted Network Same as "On Trusted None	TION acket Filter Based CTION FOR ZPA	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Parent FORWARDING PROFILE AC On Trusted Network Tunnel None VPN Trusted Network Same as "On Trusted Network Tunnel None Off Trusted Network	TION acket Filter Based CTION FOR ZPA	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Particle FORWARDING PROFILE AC On Trusted Network Tunnel None VPN Trusted Network Same as "On Trusted Network Off Trusted Network Same as "On Trusted Network	TION acket Filter Based CTION FOR ZPA letwork*	
WINDOWS DRIVER SELECT Tunnel Driver Type Route Based Pate FORWARDING PROFILE AC On Trusted Network Tunnel None VPN Trusted Network Same as "On Trusted N Off Trusted Network Same as "On Trusted N None	TION acket Filter Based CTION FOR ZPA Jetwork*	
WINDOWS DRIVER SELECT Tunnel Driver Type PROUTE Based Particle FORWARDING PROFILE AC On Trusted Network Tunnel None Off Trusted Network Same as "On Trusted Network Game as "On Trusted Network None	TION acket Filter Based CTION FOR ZPA Vetwork*	

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)。

Ozscaler	Contrast	C conseit beites de App Profes	Q ² Administra			<u>e</u>
2 Padama	0 in which the					
a08	Rear	Policy Name	Policy Description	User Groups	State	
-		Except Y		ALL	Challent	1.1
	2	Default	Default Psikoy	ALL	(College	

DEEINE POLICY AND SCORE		
DEFINE FOLICY AND SCOPE		
Name 😡		
Mac		
GENERAL		
Rule Order	Enable	
2	*	
Groups	Logout Password ®	
ALL	Y	_
Disable Password (9)	Custom PAC URL	
	Optional	_
Forwarding Profile	Install Zscaler SSL Certificate	
Mac	× 🗌 ×	
Log Mode	Log File Size in MB 🕑	
Debug	✓ 100	
HOSTNAME OR IP ADDRESS BYPAS	S FOR VPN GATEWAY 🕑	
Optional		

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。

indows	O Add macO	35 Policy				
#0\$ 5	Rule#	Policy Name	Policy Description	User Groups	Status	
box	1 t	AWS_Access		AWS_Access	Enabled	1.
	2	None_AWS_Access		None_AWS_Access	Enamed	10
	3	MAC_Profile		ALL	Enabled	1.
	4	Default	Default Policy	ALL	Enisters	

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。

Ozscaler	Destand	Erroled Devices	Aco Profiles	Q ⁶ Administration		0
Settings						
later Age Store	MANAGE DEVICE	POSTURES				
calier Acia Notifications	O Alth Device P	Posture Profile				
di Logi						
and Meteorem	* Pr	ofile Name		Description		
name Aligo Bargoneti					No Dide found	
e Agen						
Tane Acp 10 ²						

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

DEFINE POLICY AND SCOPE			
Name Ø			
Tech_Div			
FLATFORM			
Windows macOS	Android	ios	
DEVICE POSTURE CONFIGURATION			
Posture Type			
Certificate Trust	-		
Certificate:posture.zscalerjapan.com.pem			
Desere Upload			
DEVICE POSTURE DESCRIPTION			
Datima			
-			_

Destort	Enabled Devices	📥 (see Proline	OS Administration	
Lawrences				
MANAGE DEVICE	E POSTUPES			
O Add Device	Posture Profile			
	hofie Name		Description	
t 7	iech_Div			
	MAAAGE DEVIC	Daardouers Li Ensolved Devices MAAAGE Device Posturies Aast Device Posturies Profile Name Tech, Div	Constituent Constit Constituent Constituent Constituent Constituent	

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。

CTION		
0101		
Rule Action	Message to User	
Allow Access Block Access		11
RITERIA		
Application Segments X zscalerjapan X Tech Win	dows Server2019	v
OR		
Segment Groups		
Select one or more segment groups		4
ND		
SAML Attributes		O Select IdP
Any SAME attribute from any IOP		
Client Types		
Amu client turc		
ND CHERT (VDE		
Zensler Ann Posture Profiles		
Zacaler App Postule Promes		
Tech_Div	VERIFIED VERIFICATION FAIL	D
		Add More
٩D		
Zscaler App Trusted Networks		
Select one or more trusted networks		~

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。

Keychains login Local Items System System Roots	Certificate Control Co	ure.zscalerjapan.com certificate authority is: Tuesday, April 13, 2021 12:4 s certificate is marked as trust	18:00 Japan Standard Time ed for this account		
	Name	∧ Kind	Date Modified	Expires	Keychai
Category					
Secure Notes My Certificates Keys Certificates					

	posterescontellabarreetti
posture.zs	calerjapan.com
Root certifica	te authority
Expires: Tues	day, April 13, 2021 12:48:00 Japan Standard Time
O This certif	cale is marked as trusted for this account
Trust	
Details	
Subject Name	
Country or Region	qL
Organizational Unit	Tech
Common Name	posture.zscalerjapan.com
Issuer Name	
Country or Region	JP
Organizational Unit	Tech
Common Name	posture.zscalerjapan.com
Serial Number	2361107262769409539
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Monday, April 13, 2020 12:53:00 Japan Standard Time
Not Valid After	Tuandau Anel 12 2021 12-40-00 Janan Clandard Time

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。

Keychains	nostur	e zscalerianan com			
🖌 login	Certificate Root cer	tificate authority			
Local Items	Expires:	Tuesday, April 13, 2021 12:48	:00 Japan Standard Time		
System	O This c	ertificate is marked as not tru	isted for this account		
🕤 System Roots					
	Name	~ Kind	Date Modified	Expires	Keychair
Category					
All Items					
Passwords					
Secure Notes					
My Certificates					
Keys					
Y Keys Certificates					

	posture.zscalerjapan.com
posture.zs	calerjapan.com
Certificate Root certifica	ate authority
Expires: Tues	day, April 13, 2021 12:48:00 Japan Standard Time
O This certif	icate is marked as not trusted for this account
Trust	
Details	
Subject Name	
Country or Region	JP
Organizational Unit	Tech
Common Name	posture.zscalerjapan.com
Issuer Name	
Country or Region	JP
Organizational Unit	Tech
Common Name	posture.zscalerjapan.com
Serial Number	2361107262769409539
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Monday, April 13, 2020 12:53:00 Japan Standard Time
Not Valid After	Tuesday April 13, 2021 12:48:00 Japan Standard Time

Access Policy の条件にマッチしないのでアクセスが失敗します。

