



IT Automation Terraform Driver 【座学編】

※本書では「Exastro IT Automation」を「ITA」として記載します。

Exastro IT Automation ver 1.8
Exastro developer

目次

1. はじめに

2. Terraform Driverとは

2.1 Terraform Driverとは

2.2 登録するファイルと動作

2.3 Policyファイルについて

3. ITA×Terraform運用例

3.1 ITAと連携可能なTerraform

3.2 Terraform Enterpriseを利用する場合

3.3 Terraform Cloudを利用する場合

4. Terraform Driverメニュー

4.1 Terraform Driverメニュー概要

4.2 Terraformの連携

4.3 Organizationsの連携

4.4 Workspacesの連携

4.5 Moduleの適用

4.6 Policyの適用

4.6 Terraform Driverの作業フロー

1. はじめに

1. はじめに

メインメニュー

- 本書では、メニューグループの「**Terraform**」についての機能説明を目的としております。
- 実習編ではITAの画面を用いて説明しておりますので合わせてご覧ください。

The screenshot displays the Exastro IT Automation dashboard. The top navigation bar includes the Exastro logo, a user login status for 'ようこそ[システム管理者]さん' (Welcome [System Administrator]), and links for 'パスワード変更' (Change Password) and 'ログアウト' (Logout). The main content area is divided into a left sidebar and a central dashboard. The sidebar shows a 'Menu' button and a 'DASHBOARD' tab. The central dashboard features a 'メニューグループ' (Menu Group) section with a grid of icons. The 'Terraform' icon, located at the bottom left of the grid, is highlighted with a red rectangle. To the right of the menu group are three large circular gauges labeled 'Movement', 'Status', and 'Result', each showing a 'Total' value of 0. Below these gauges are three tables: 'Movement', 'Status', and 'Result', each with columns for 'CON', 'SYN', and 'SUM'. The 'Movement' table lists 'Ansible Legacy', 'Ansible Pioneer', 'Ansible Legacy Role', and 'Terraform'. The 'Status' table lists '実行中' (Running), '未実行(予約)' (Not executed (Reserved)), and '未実行' (Not executed). The 'Result' table lists '正常終了' (Normal completion), '異常終了' (Abnormal completion), '想定外エラー' (Unexpected error), '緊急停止' (Emergency stop), and '予約取消' (Reservation cancellation).

Exastro IT Automation

ようこそ[システム管理者]さん
ログインID [administrator]
パスワード変更 ログアウト

Menu DASHBOARD

メインメニュー

メニューグループ

管理コンソール 基本コンソール エクスポートノイ... Symphony Conductor メニュー作成

比較 ホストグループ管理 Ansible共通 Ansible-Legacy Ansible-Pioneer Ansible-LegacyR...

Terraform

Movement

Movement
0
Total

作業状況

Status
0
Total

作業結果

Result
0
Total

Movement	SUM
Ansible Legacy	0
Ansible Pioneer	0
Ansible Legacy Role	0
Terraform	0

Status	CON	SYN	SUM
実行中	0	0	0
未実行(予約)	0	0	0
未実行	0	0	0

Result	CON	SYN	SUM
正常終了	0	0	0
異常終了	0	0	0
想定外エラー	0	0	0
緊急停止	0	0	0
予約取消	0	0	0

作業履歴

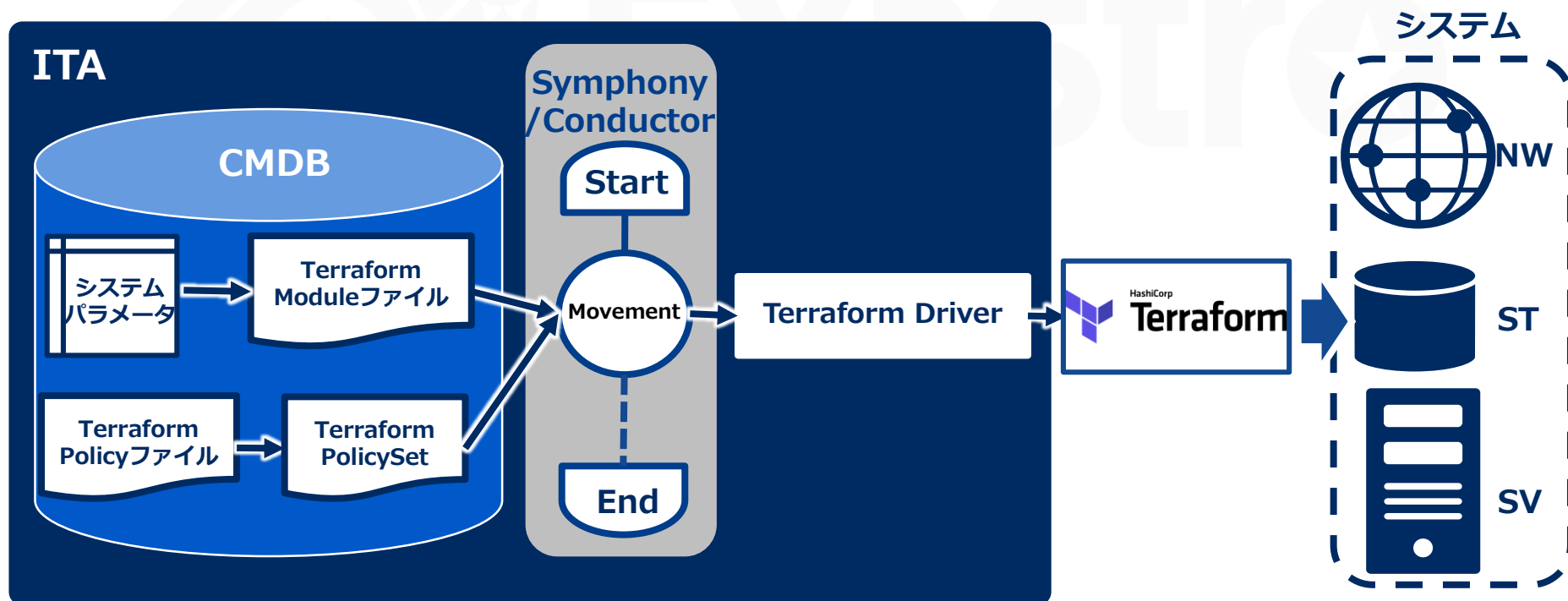
管理者に連絡

2. Terraform Driverとは

2.1 Terraform Driverとは

Terraform DriverはITAが一元管理するシステムパラメータとIaC(Module)の変数を紐づけてTerraformに連携実行させることが可能です。

- ITAシステムに連携したTerraform EnterpriseまたはTerraform Cloudに対し、Organization・Workspaceの作成、作業の実行(Plan/PolicyCheck/Apply)及び作業ログの取得を行うことが可能です。
※ITAとTerraform Enterprise・Terraform Cloudの使い分けについては「3. ITA×Terraform運用例」で解説しております。
- 作業実行に利用するModuleファイルや、PolicyCheckを行うためのPolicyファイルをITAシステム上で部品化し、再利用することができます。



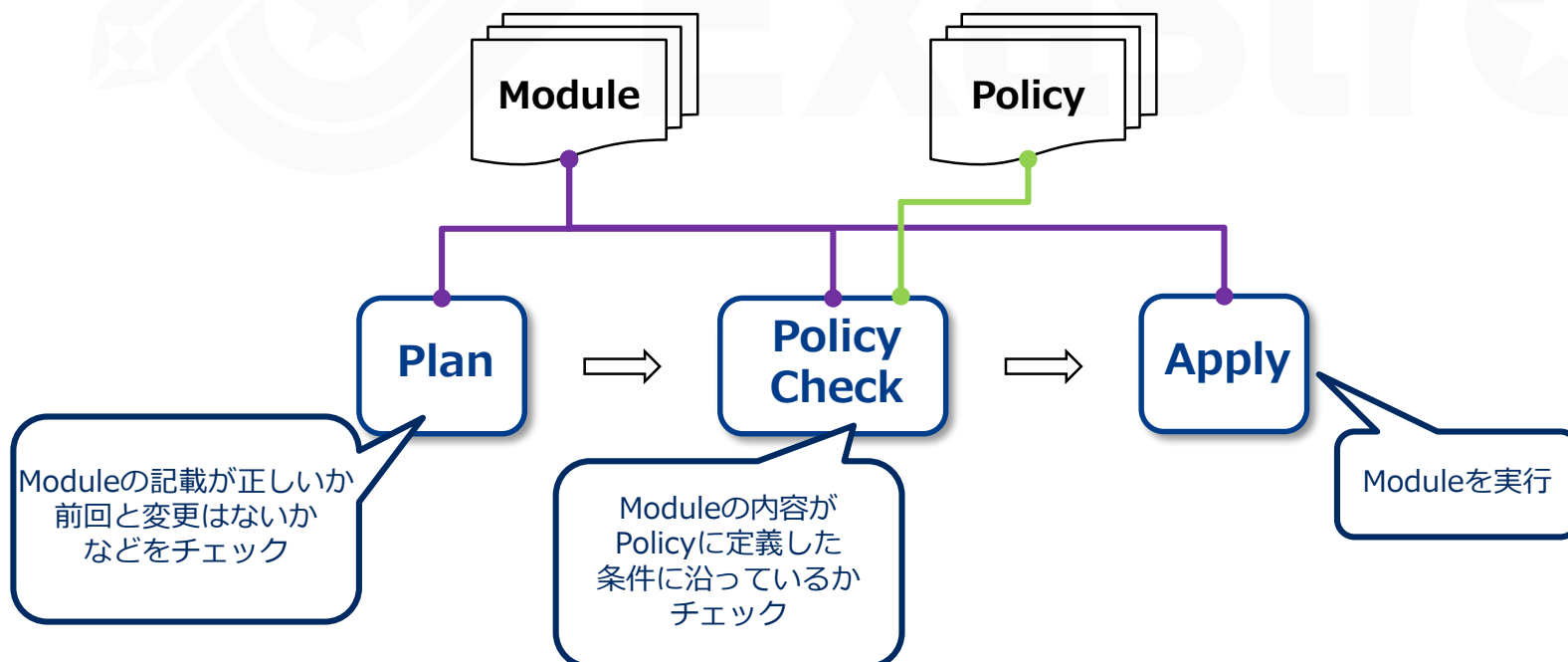
2.2 登録するファイルと動作

登録するファイルの種類と動作について

- Terraform Driverに登録するファイルは「**Module**」と「**Policy**」の二種類があります。
- 「**Module**」はTerraformのメインの実行ファイルです。**HCL** (Hashicorp Config Language) 言語で書かれ、Azure,AWS,GCP,VMwareなどあらゆる環境で同一の言語を用いてプロビジョニングすることができます。
- 「**Policy**」は実行におけるポリシーを定義するファイルです。

※Policyについての詳細は「2.3 Policyファイルについて」で解説しております。

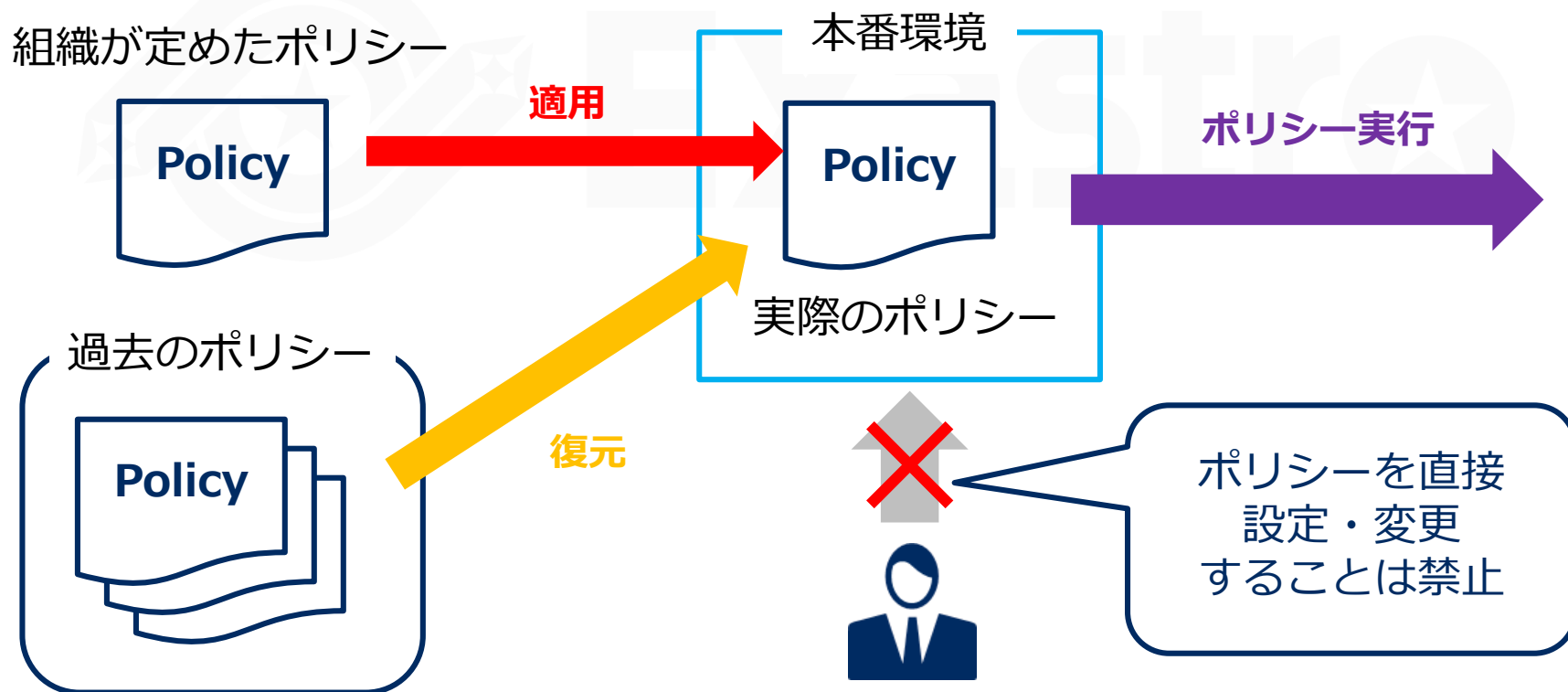
- Terraform は[**Plan**]>[**PolicyCheck**]>[**Apply**]の順番で動作します。



2.3 Policyファイルについて

Policyファイル(PaC)

- PaC(Policy as Code)はポリシーをコード化し管理することを指し、Terraformでは **Sentinel** が使用されます。
- コード化したポリシーを環境に適用して変更範囲を制限することで、組織が定めたポリシー(予算・コーポレートガバナンス・セキュリティ・法律等)と実際のポリシーが一致し、権限などの設定漏れ・誤りを防ぐことが可能です。また、過去のポリシーを適用することで復元も容易です。

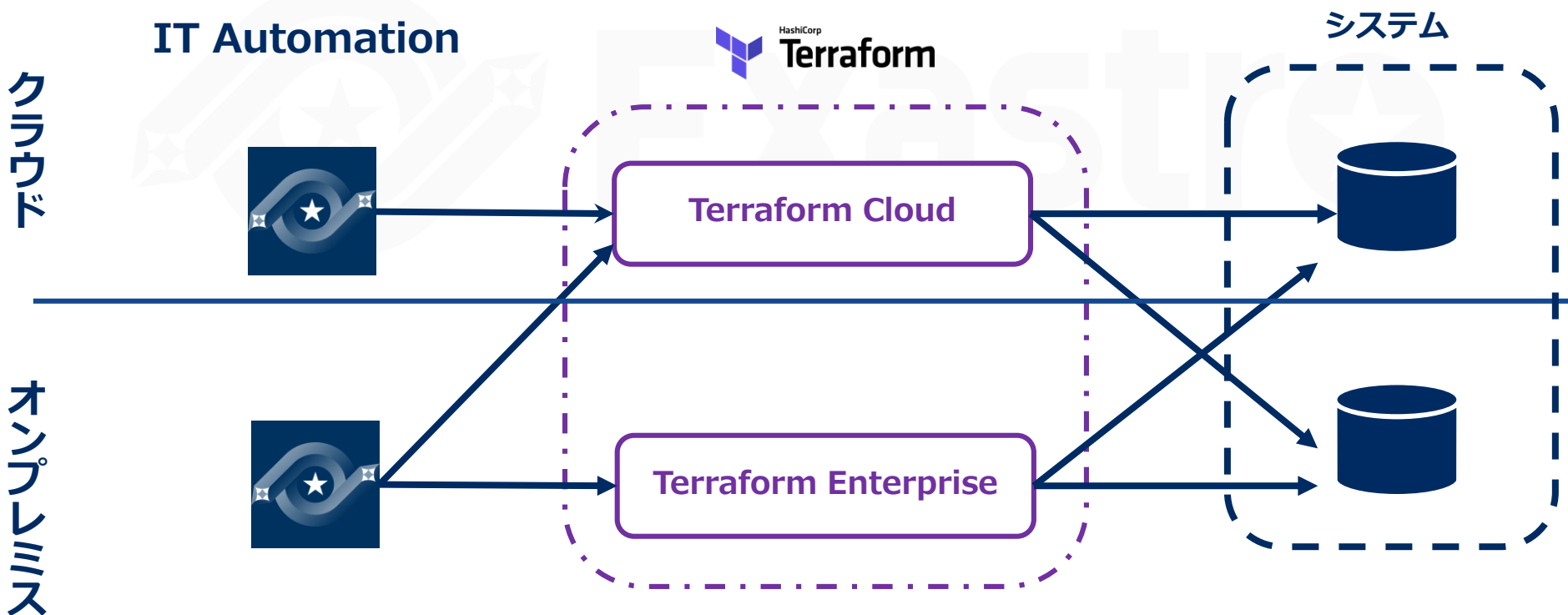


3. ITA×Terraform運用例

3.1 ITAと連携可能なTerraform

ITAと連携可能なTerraformについて

- ITAは「Terraform Enterprise」、または「Terraform Cloud」との連携が可能です。
- 本章では、ITAと「Terraform Enterprise」・「Terraform Cloud」を組み合わせ、オンプレミスまたはクラウド上にシステムを構築する運用例を記述しております。



3.2 Terraform Enterpriseを利用する場合

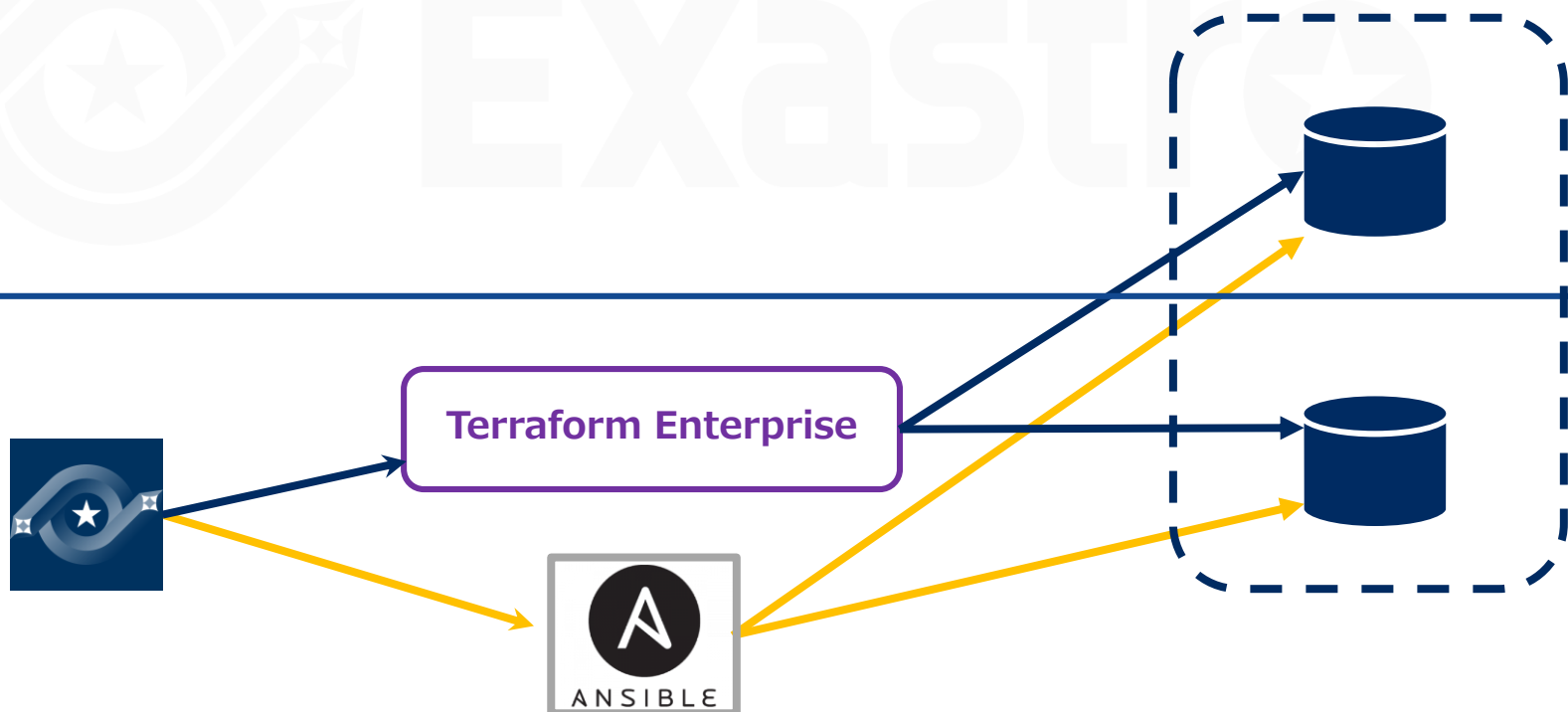
- Terraform Enterpriseを利用する場合は、オンプレミスにITAサーバを構築することでオンプレミス・クラウド上のシステムにプロビジョニングが行うことができます。
- さらにオンプレミスにAnsibleを導入することで、構築したオンプレミス・クラウド上のシステムに対して様々な設定をすることができます。

※Ansibleの利用方法等の詳細については「Exastro-ITA_利用手順マニュアル_Ansible-driver」をご参照ください

システム

クラウド

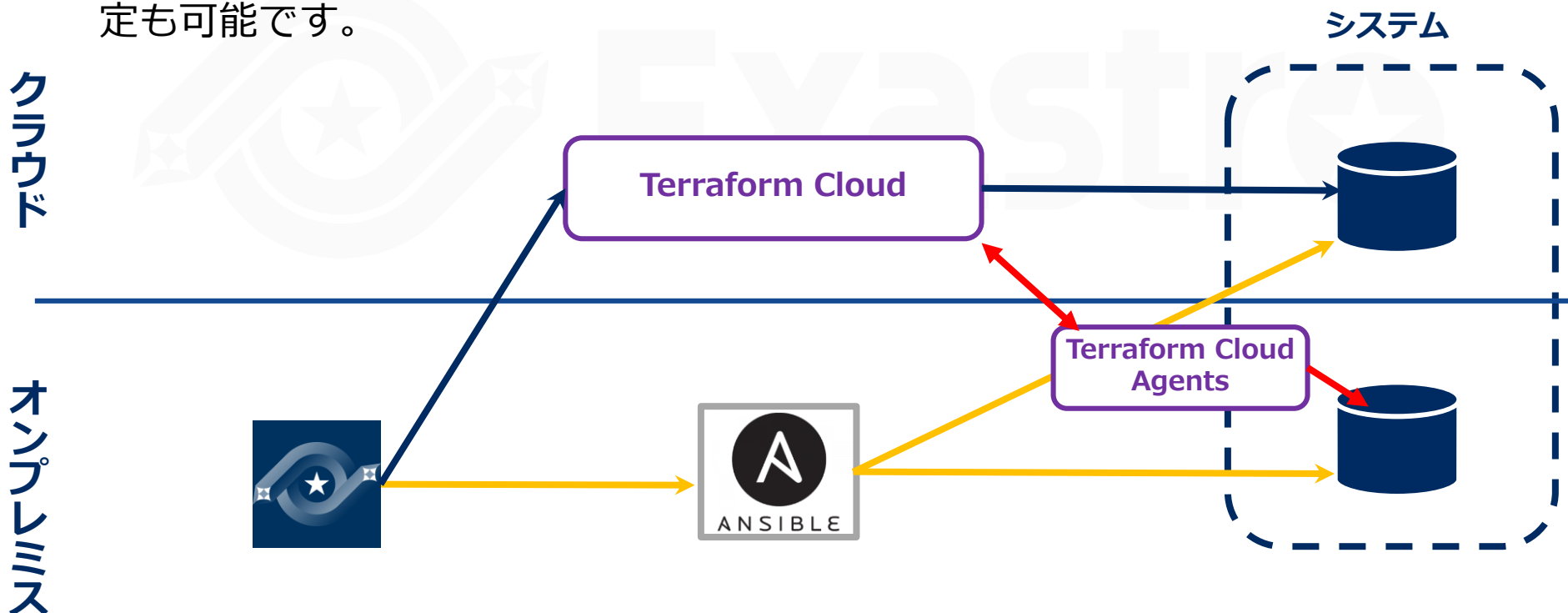
オンプレミス



3.3 Terraform Cloudを利用する場合(1/3)

ITAサーバをオンプレミスに建てる

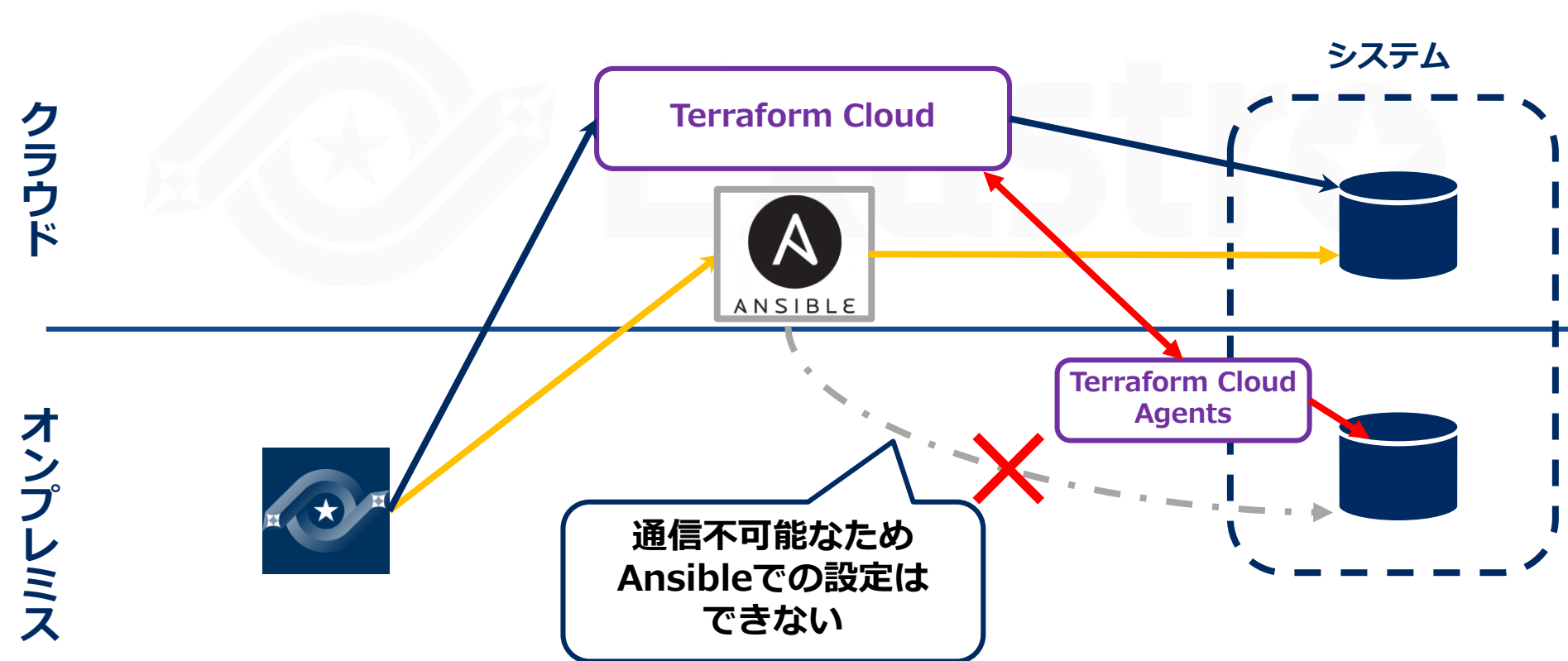
- ITAサーバをオンプレミスに建てる場合Terraform Cloudを利用してクラウドのシステムのプロビジョニングを行うことができます。
- Terraform Cloud Agentsを導入することでオンプレミス上のシステムのプロビジョニングも可能です。
- オンプレミス上のAnsibleから、構築したオンプレミス・クラウドのシステムの設定も可能です。



3.3 Terraform Cloudを利用する場合(2/3)

ITAサーバをオンプレミスに建てる

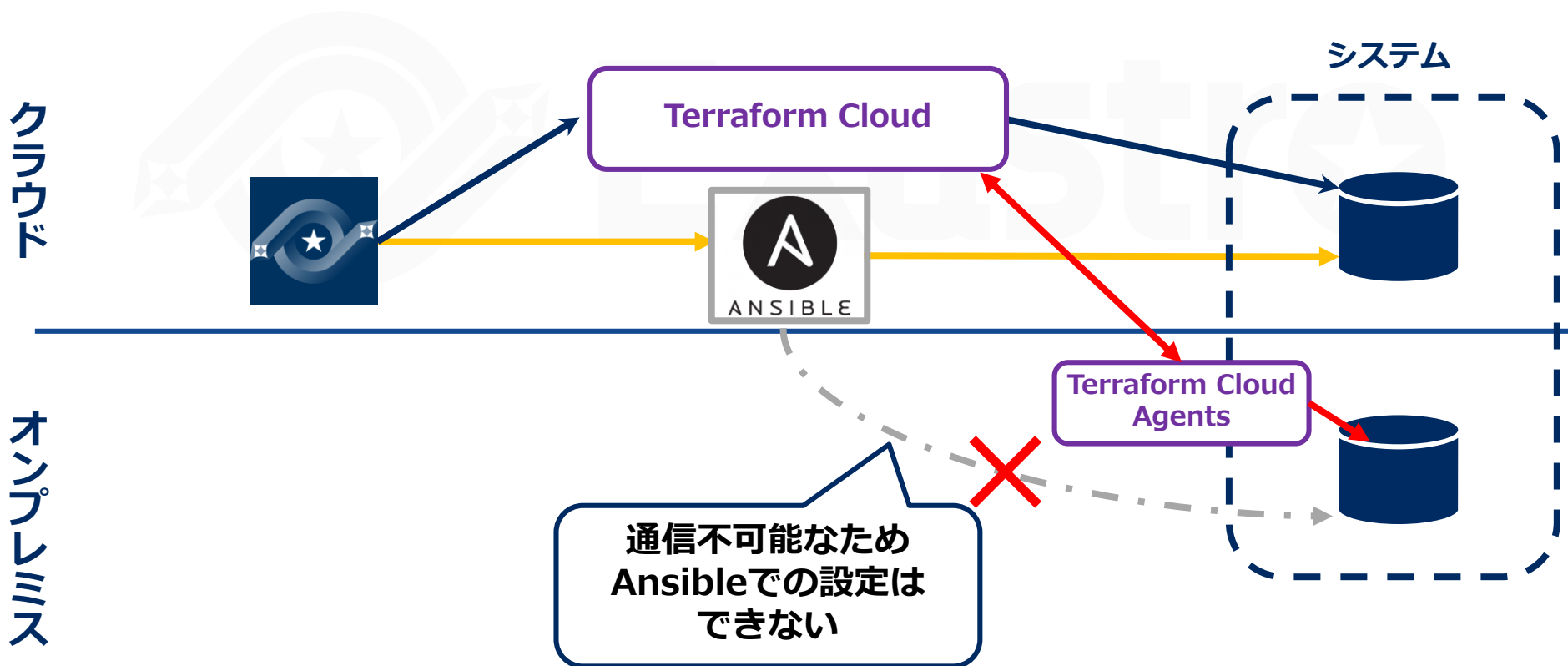
- Ansibleをクラウドシステム側に導入した場合、クラウド上のシステムにプロビジョニングと設定が行うことができます。
- Terraform Cloud Agentsを導入することでオンプレミス上のシステムのプロビジョニングも可能です。



3.3 Terraform Cloudを利用する場合(3/3)

ITAサーバをクラウドに建てる

- ITAサーバをクラウド建てる場合Terraform Cloudを利用して、クラウド上のシステムに対してプロビジョニングを行うことができます。
- Terraform Cloud Agentsを導入することでオンプレミス上のシステムのプロビジョニングも可能です。



4. Terraform Driverメニュー

4.1 Terraform Driverメニュー概要(1/2)

メニュー機能説明

- インターフェース情報

ITAと連携するTerraformの情報を管理します。

- Organizations管理

Terraformで利用するOrganizationの情報を管理します。

- Workspaces管理

Terraformで利用するWorkspacesの情報を管理します。

- Movement一覧

Symphony/Conductorに登録するMovementの一覧を管理します。

- Module素材集

Moduleファイルを管理します。

- Policies管理

Policyファイルを管理します。

- Policy Sets管理

Policy Setを管理します。

Policy SetはPolicyおよびWorkspaceと紐付けることで、作業実行時に対象のWorkspaceに対してPolicyを有効にします。

- PolicySet-Policy紐付管理

PolicySetとPolicyの紐付けを管理します。

Menu

メインメニュー

インターフェース情報

Organizations管理

Workspaces管理

Movement一覧

Module素材集

Policies管理

Policy Sets管理

PolicySet-Policy紐付管理

4.1 Terraform Driverメニュー概要(2/2)

メニュー機能説明

- **PolicySet-Workspace紐付管理**

PolicySetとWorkspaceの紐付けを管理します。

- **Movement-Module紐付**

MovementとModule素材の関連付けを管理します。

- **代入値自動登録**

パラメータシートのメニューに登録されているオペレーション毎の項目や値を紐付けるMovementと変数を管理します。

- **代入値管理**

変数の代入値を管理します。

- **作業実行**

作業実行するMovementとオペレーションを選択し実行を指示します。

- **作業状態確認**

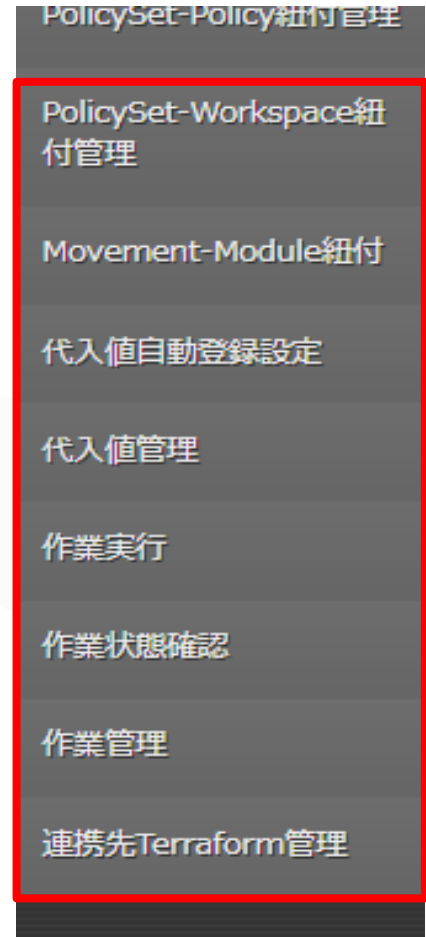
作業実行状態を確認します。

- **作業管理**

作業実行履歴を管理します。

- **連携先Terraform管理**

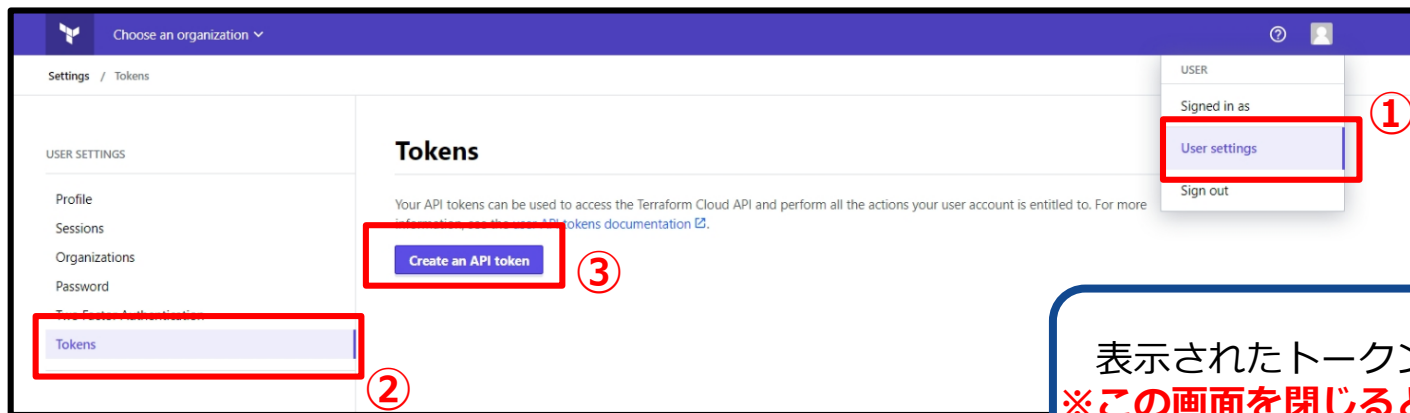
Terraformに登録されているOrganization,Workspace,Policy,PolicySetの一覧表示および削除することができます。



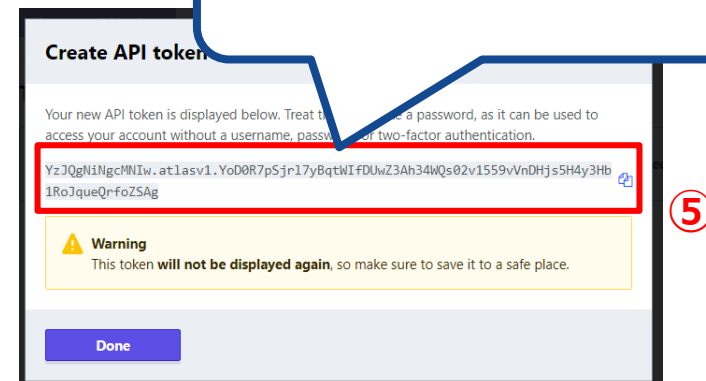
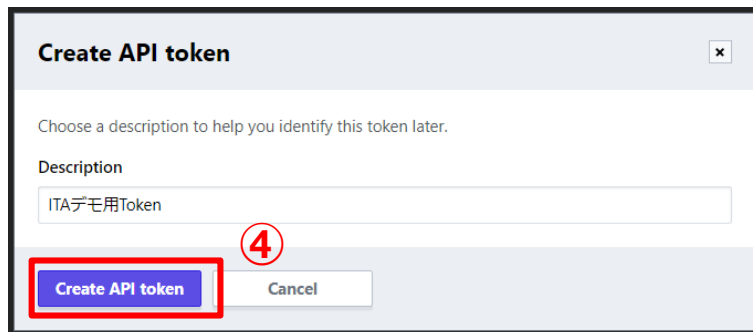
4.2 Terraformの連携(1/2)

■ インターフェース情報に登録するUser Tokenの発行

- Terraform DriverをTerraformと連携するために、Terraformからユーザートークンを発行する必要があります。
- ブラウザよりTerraformにログインし、[User Setting]→[Tokens]→[Creat an API token]の順に押下することで発行することができます。



表示されたトークンをメモしておく
※この画面を閉じると再表示できません



4.2 Terraformの連携(2/2)

■ インターフェース情報

- 連携するTerraformのHostnameと、発行したUserTokenを入力します

※ITAに連携できるTerraformは1つのみなので、インストール時に最初からある項目を「更新」して値を入力する必要があります。

The screenshot shows the ITA interface with the 'インターフェース情報' (Interface Information) section selected in the left sidebar. The main content area displays a table for Terraform integration. A callout points to the 'Hostname' field, stating '連携するTerraformのHostnameを記入' (Enter the Hostname of the Terraform to be integrated). Another callout points to the 'User Token' field, stating 'Terraformで発行したUserToken' (UserToken issued by Terraform). The table has columns for No., Hostname, User Token, Proxy (Address, Port), Status Monitoring Period (unit: milliseconds), Progress Status Display Count, and NULL. The first row is for the existing Terraform instance, with a status of 'Terraformのホスト名を記載' (Enter the Terraform hostname) and a status of '更新' (Update). The '更新' button is highlighted with a red box. Below the table, there is a note '※*は必須項目です。' (※* is a required item.) and two buttons: '戻る' (Back) and '更新' (Update).

No.	Hostname*	User Token	Proxy	状態監視周期(単位ミリ秒)*	進行状態表示行数*	NULL連携	
			Address	Port			
1				3000	1000	無効

※*は必須項目です。

戻る 更新

4.3 Organizationsの連携

Organizations管理

- Organization管理からOrganizationの項目を作成した後、
[連携状態チェック]で対象のTerraformに追加したOrganizationがあるかどうかをチェックすることができます。
- 「登録なし」であれば[登録]を押下することで対象のTerraformにOrganizationを作成できます。

The screenshot displays the Terraform Organizations management interface. The top section shows a table of organizations with columns for Organization ID, Organization Name, Email address, and Terraform連携 (Terraform Integration). The 'Terraform連携' section includes buttons for 状態チェック (Status Check), 連携状態 (Integration Status), 登録 (Register), 更新 (Update), and 削除 (Delete). The '登録' button is highlighted with a red box.

履歴	複製	更新	廃止	Organization ID	Organization Name	Email address	Terraform連携				Workspaces管理	
履歴	複製	更新	廃止				状態チェック	連携状態	登録	更新	削除	Workspaces管理
履歴	複製	更新	廃止	1	ITAllearn_org	test@example.com	連携状態チェック	登録なし	登録	更新	削除	Workspaces管理

フィルタ結果件数: 1

Excel出力

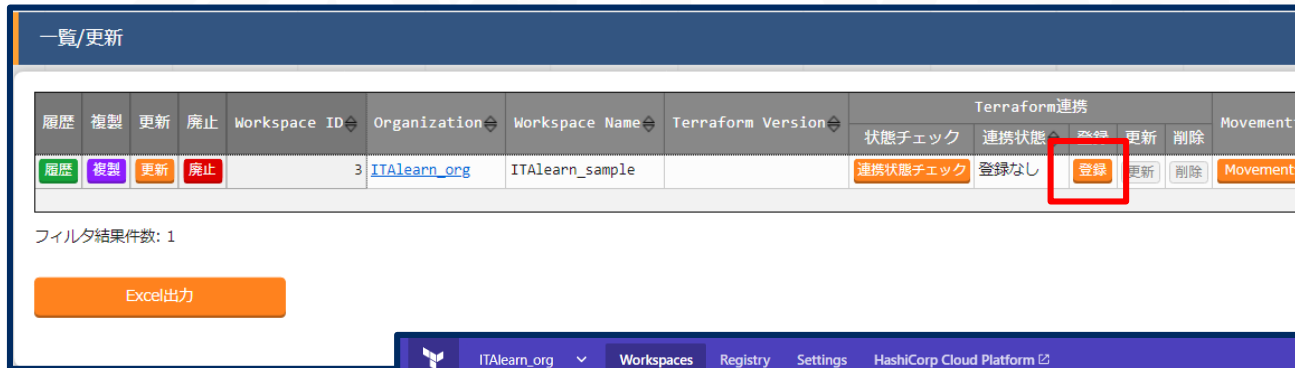
The bottom section shows the 'Organizations' page in the Terraform console. It displays the organization 'ITAllearn_org' with the role 'OWNER'. The organization name and role are highlighted with a red box.

4.4 Workspacesの連携

Workspaces管理

- Workspaces管理からWorkspaceの項目を作成した後、
[連携状態チェック]で対象のTerraformに追加したWorkspaceがあるかどうかをチェックすることができます。
- 「登録なし」であれば[登録]を押下することで対象のTerraformにWorkspaceを作成できます。

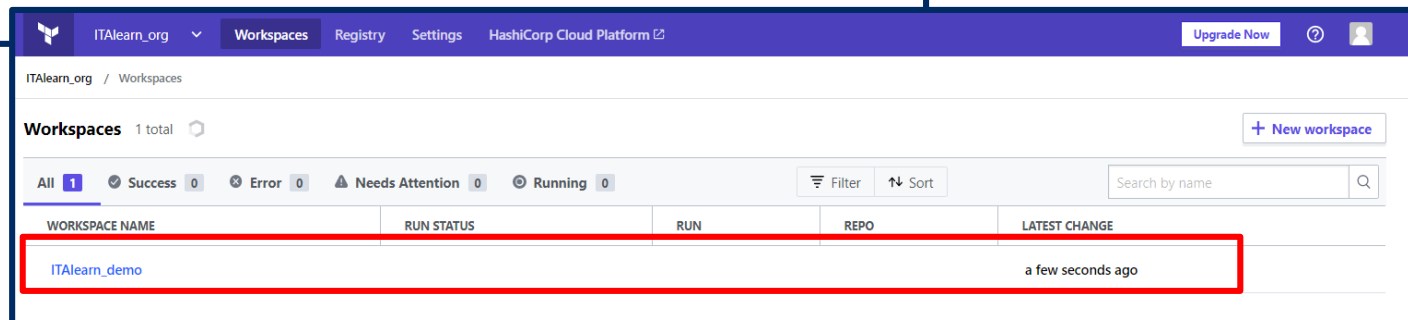
※WorkspaceはいずれかのOrganizationに所属する必要があるため、
必ず先に所属させるOrganizationを対象のTerraformに作成しておく必要があります



履歴	複製	更新	廃止	Workspace ID	Organization	Workspace Name	Terraform Version	Terraform連携				Movement	
履歴	複製	更新	廃止					状態チェック	連携状態	登録	更新	削除	
				3	ITAllearn_org	ITAllearn_sample		連携状態チェック	登録なし	登録	更新	削除	Movement

フィルタ結果件数: 1

Excel出力



ITAllearn_org / Workspaces

Workspaces 1 total

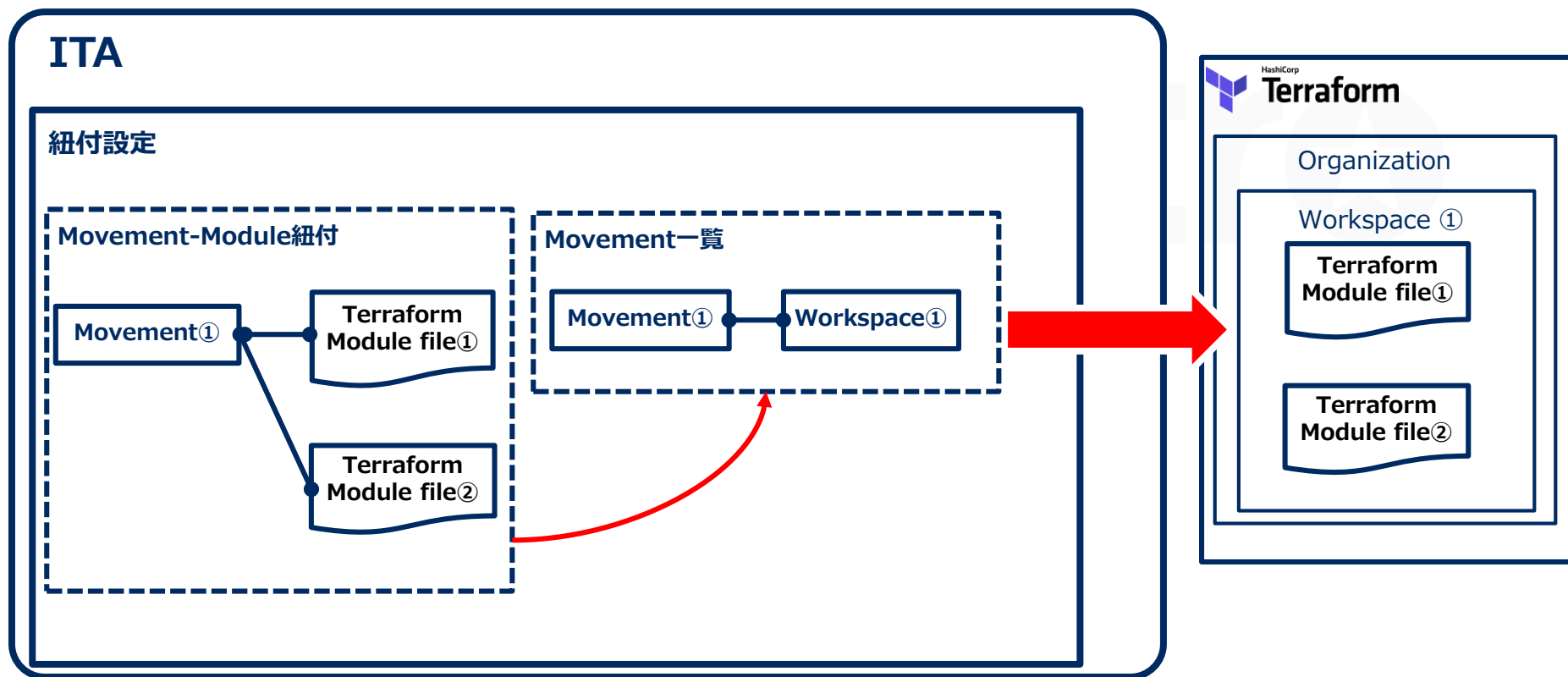
All 1 Success 0 Error 0 Needs Attention 0 Running 0

WORKSPACE NAME	RUN STATUS	RUN	REPO	LATEST CHANGE
ITAllearn_demo				a few seconds ago

4.5 Moduleの適用

Moduleの適用について

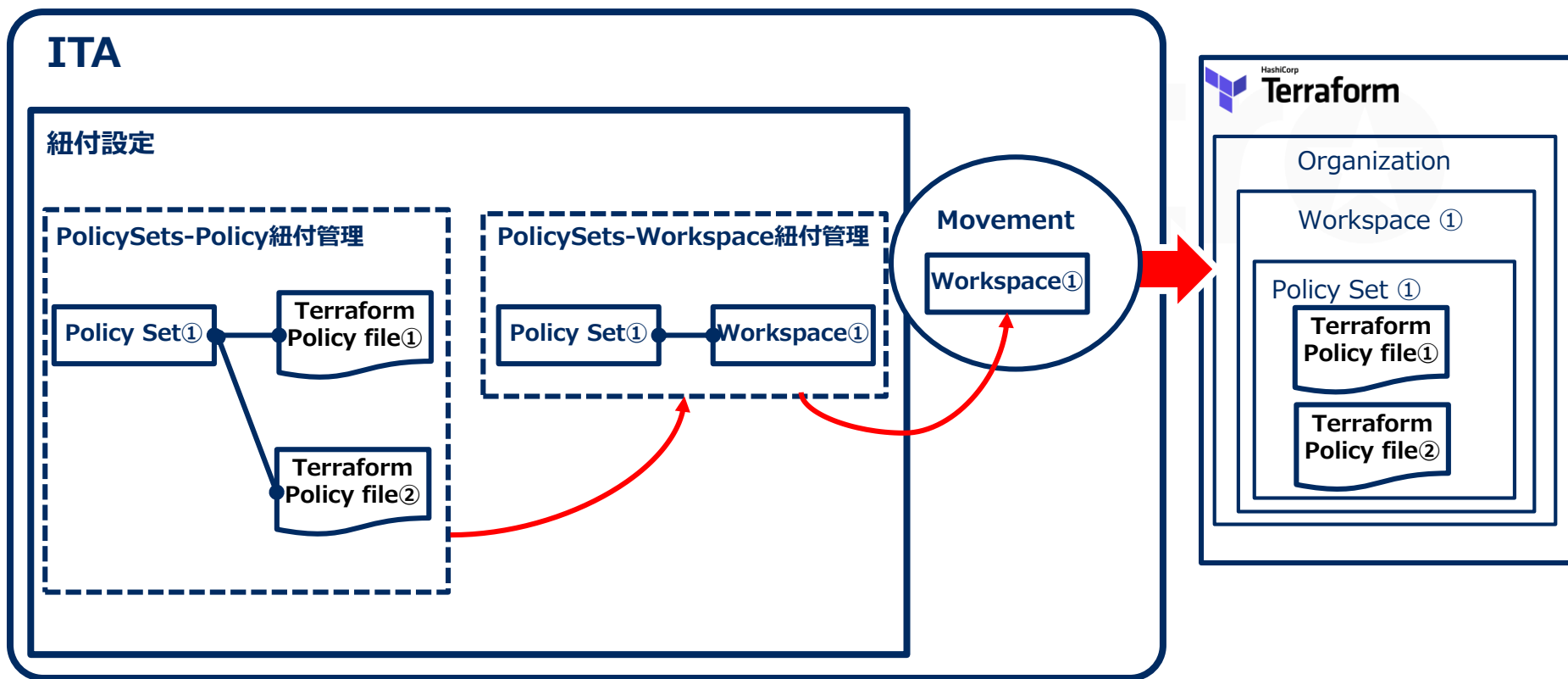
- 作業実行に対してModuleを適用させるために、各種紐付設定を行う必要があります。
- 作業実行時にMovementに紐付いたWorkspaceに対し、実行するModuleが適用されます。



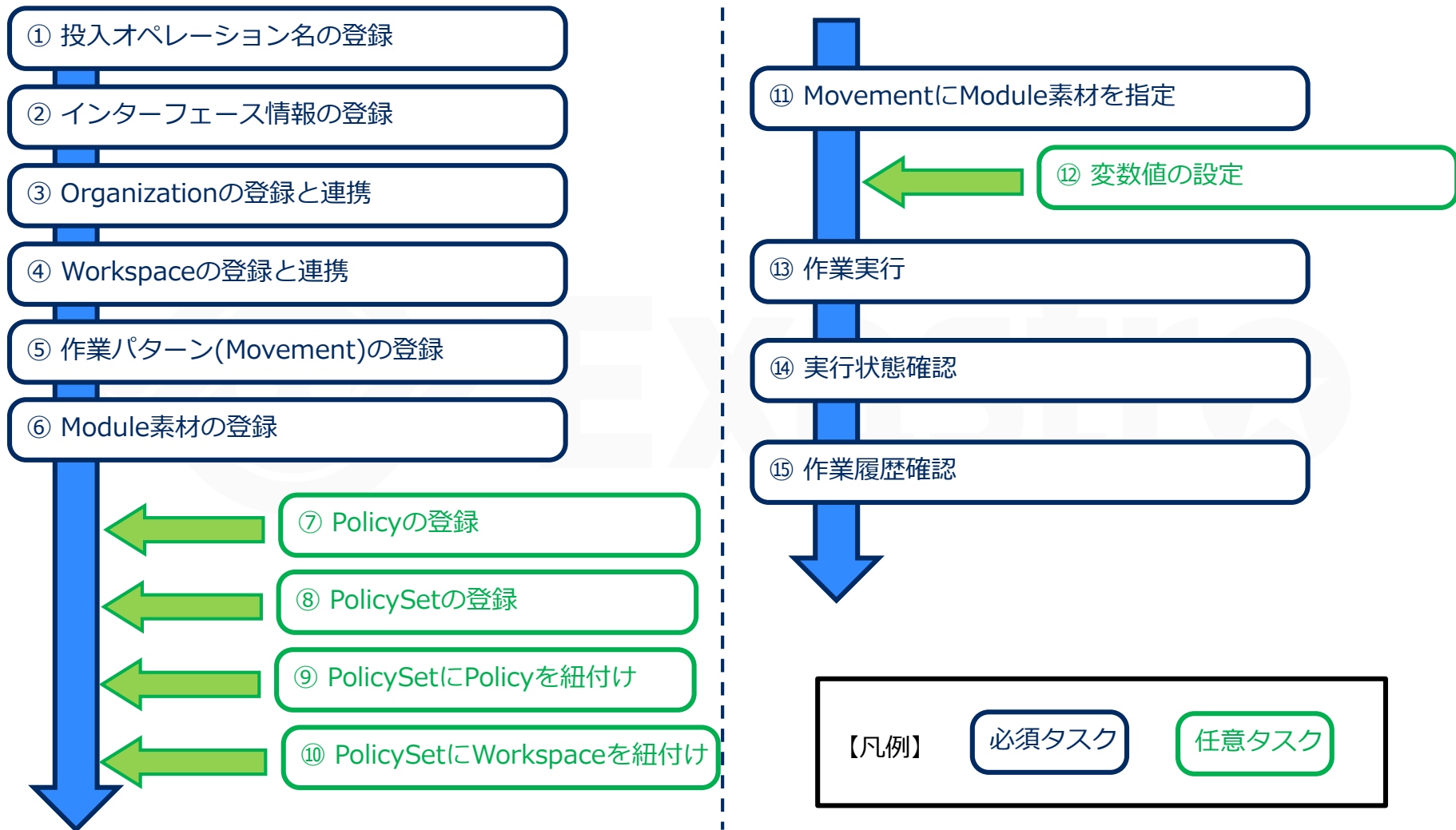
4.6 Policyの適用

Policyの適用について

- 作業実行に対してPolicyを適用させるために、Policyに関する各設定登録をした後にそれぞれ紐付け設定をする必要があります。
- 作業実行時にMovementに紐付いたWorkspaceに対し、Policysetとそれに紐付けられたPolicyが適用されます。



4.6 Terraform Driverの作業フロー





Exastro