



Cisco Intersight 実践編：

Intersight の初期設定から、Ansible / ServiceNow 連携まで、まるっと具体的な使い方をお見せします！

シスコシステムズ合同会社
データセンター / 仮想化事業部

相園 沙貴

2020年12月16日

アジェンダ

- Intersight 概要
- Intersight 初期設定
- Intersight によるサーバ運用管理
- Ansible 自動化
- Connected TAC
- ServiceNow 連携
- Intersight Workload Optimizer (IWO)

Intersight 概要

Cisco Intersight

Cisco データセンター製品である、UCS、HyperFlex、コンバードインフラ、
3rd Party 製品のインテリジェントなライフサイクル管理

直感的



エンハンス
サポート



プロアクティブ
ガイダンス



セキュリティ
スケーラビリティ



SaaS または
Appliance



SaaS による提供
シンプルなツール

サーバ管理アクション
インテリジェンス

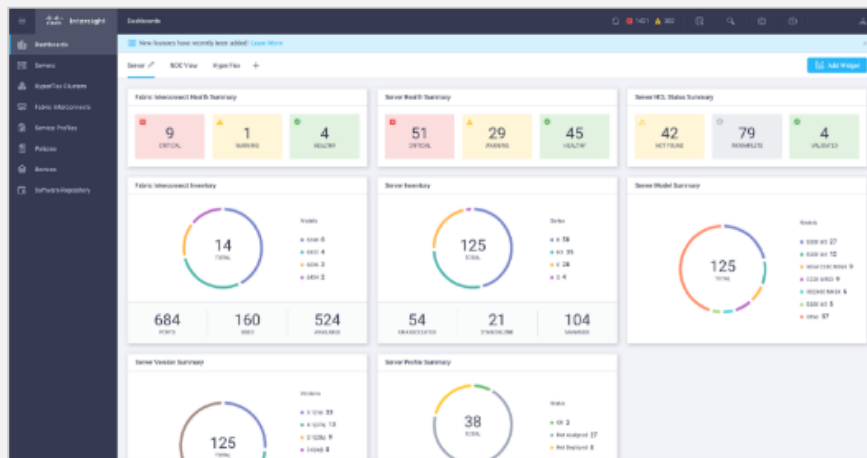


管理を Intersight 一つに統合し、シンプルに。

Operations



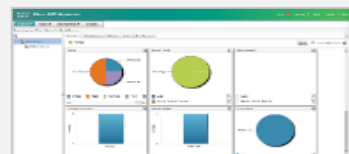
Single Interface / Single API



Automation / Orchestration



Remote/ Branch/ Edge



Multi-Site



Performance



Hyperconverged



Intersight 初期設定

- ・ アカウント作成
- ・ デバイス登録
- ・ ユーザ、ロール設定

Intersight 初期設定

- ・ アカウント作成
- ・ デバイス登録
- ・ ユーザ、ロール設定

Intersight アカウント作成に必要なもの

• シスコ ID

- シスコ ID をお持ちでない場合は、こちらから作成します。
https://www.cisco.com/c/m/ja_jp/partners/tools/how-to-make-ccoid.html
- 現在は、シスコ ID があればまずはアカウントの作成が可能です。

• Intersight に登録するシスコデバイス

- デバイスとは UCSM/IMC/HX Connect 等を指します。
- デバイスは Intersight に通信出来る状態にしておく必要があります。
- サーバ、ファブリックインターコネクトは管理 IP アドレス、DNS 設定を済ませておきます。
- アカウントが作成されたら、デバイスを登録します。

1. Intersight ポータルにアクセスし、“アカウントの作成” をクリック

<https://intersight.com>

日本語

CISCO

INTERSIGHT

シスコID

シスコIDをお持ちでない場合は [ここ](#)

シスコIDでサインイン

シングルサインオン(SSO) ①

メールアドレスの入力

SSOでサインインする

Intersightアカウントを持っていない場合 [アカウントの作成](#)

Cisco Intersightの詳細はこちら：[ヘルプセンター](#)

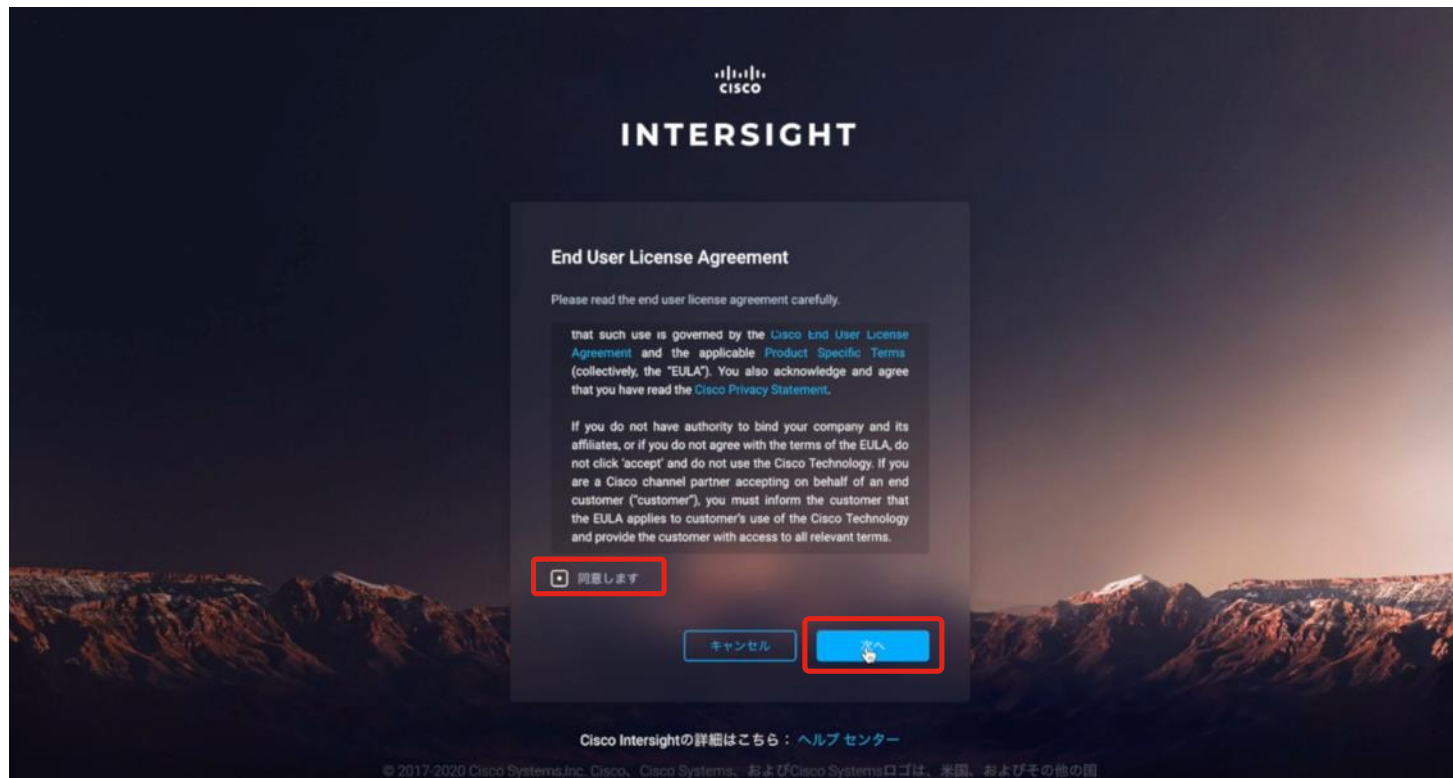
© 2017-2020 Cisco Systems, Inc. Cisco、Cisco Systems、およびCisco Systemsロゴは、米国、およびその他の国におけるCisco Systems, Inc.、およびその関連会社の登録商標です。

2. シスコ ID を入力してサインイン



The image shows a login page for Cisco OneID. At the top right, there is a globe icon with 'JP' and 'JA' labels. The Cisco logo is centered at the top. Below it, the text 'サインイン' (Sign In) is displayed. A label 'ユーザ名または電子メール' (Username or email) is positioned above a horizontal input field. Below the input field is a grey button with the text '次へ' (Next). Further down, the text 'シスコを初めてご利用のお客様向けの情報' (Information for first-time users) is shown above a blue button with the text 'アカウントの作成' (Create account). A small blue circle with a white question mark is located to the right of the 'アカウントの作成' button. At the bottom center, it says 'powered by CISCO OneID'. At the very bottom, there are links for '条件 | プライバシー | フィードバック | Cookie | 商標'.

3. サービス内容をよく読み、同意した後に“次へ”をクリック



4. アカウント名を入力してアカウントを作成

Account Creation

アカウント名*

固有の名前を設定

キャンセル 作成

Cisco Intersightの詳細はこちら：[ヘルプセンター](#)

© 2017-2020 Cisco Systems, Inc. Cisco, Cisco Systems, およびCisco Systemsロゴは、米国、およびその他の国

5. アカウント名・デバイスID・要求コードを入力してアカウントを作成

ターゲットからデバイス登録
(次の章で解説)

Cisco Intersight

Welcome to Cisco Intersight! A software-as-a-service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. Bridge the gap between infrastructure and applications.

Cisco Intersight Overview
INTER-SIGHT

Learn How to...

- サイトツアーを実施
- 新しいデバイスの登録
- Enable License

Intersight Free Trial

Gain hands-on experience using the free Intersight trial.

Start Free Intersight Trial

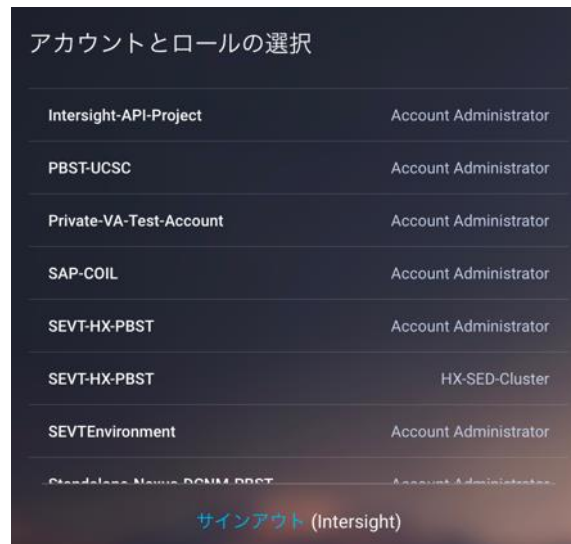
Simplify Application Resource Management For Hybrid Cloud

次回以降は、シスコ ID でログイン可能

ログイン画面にて、シスコ ID を選択



自身のアカウントに紐づく Intersight アカウントが表示される。

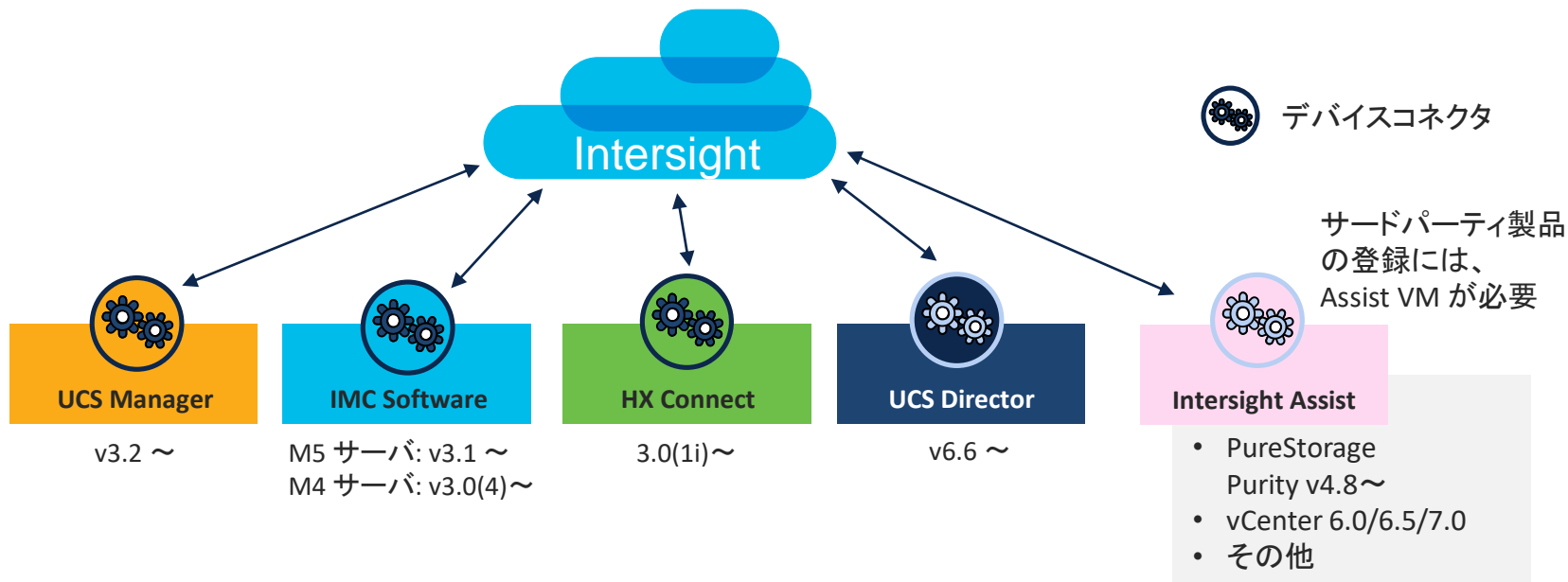


Intersight 初期設定

- ・ アカウント作成
- ・ デバイス登録
- ・ ユーザ、ロール設定

Intersight へのデバイス登録 (デバイスクレーム)

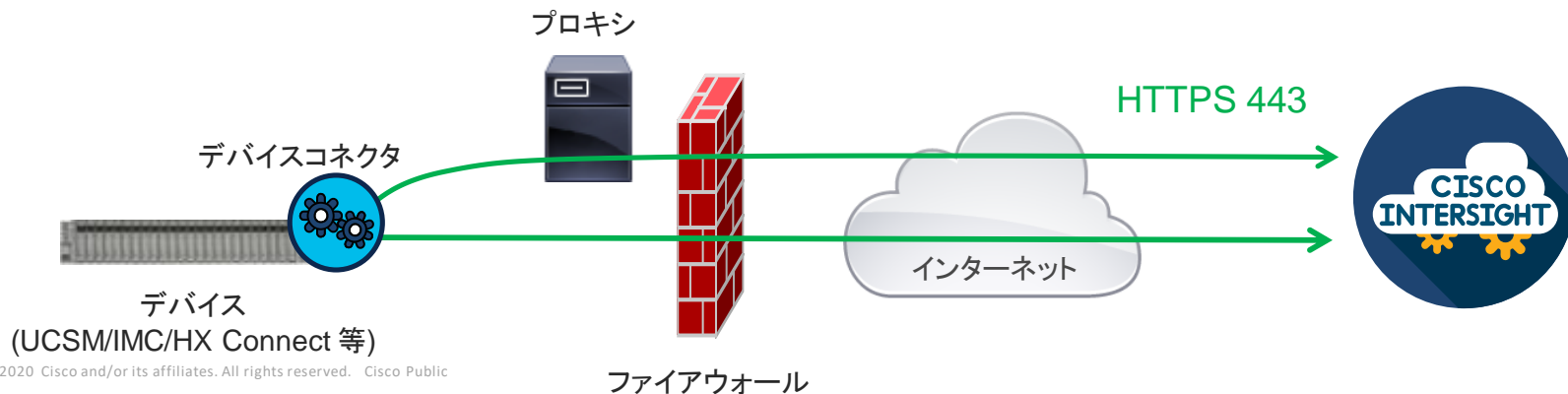
シスコデータセンター製品の管理ソフトウェアにプラグインされる“デバイスコネクタ”機能により Intersight と通信



サポート詳細: https://www.intersight.com/help/supported_systems#supported_hardware_systems_and_software_versions

デバイス通信要件

- Long Lived Web Socket (HTTPS 443)
- デバイス側から開始する通信のみ
- HTTPS Proxy 環境もサポート
- DNS 必須
'svc.intersight.com' (推奨) もしくは 'svc.ucs-connect.com' (将来非推奨となる予定) の解決が必要



デバイス ID・要求コードの取得方法 (Cisco IMC)

管理者 > Device Connector



The screenshot shows the Cisco Integrated Management Controller (IMC) interface. The left sidebar contains a navigation menu with the following items: シャーシ, コンピューティング, ネットワーキング, ストレージ, 管理者 (expanded), ユーザ管理, ネットワーキング, 通信サービス, セキュリティ管理, イベント管理, ファームウェア管理, ユーティリティ, and **デバイス コネクタ** (highlighted with a red box). The main content area is titled 'Device Connector' and includes a sub-header 'ACCESS MODE 制御の許可'. Below this is a diagram showing the connection path: Device Connector (represented by a monitor icon) connected via a dotted green line to Internet (represented by a globe icon), which is then connected via a dotted yellow line with a warning triangle to Intersight (represented by a cloud icon). A yellow banner below the diagram reads '▲ Not Claimed'. On the right side of the page, there is a configuration panel with two fields: 'デバイスID' and '要求コード', both of which are currently set to '省略' (Omission) and are highlighted with a red box. The top of the page shows the Cisco logo, the text 'Cisco Integrated Management Controller', and user information 'admin@192.168.11.236 - C220-WZP2205056R'.

デバイスコネクタの設定項目 - Cisco IMC

管理者 > Device Connector

設定

全般

DNSの構成

NTP設定

プロキシ設定

証明書マネージャ

このオプションをオンにすると、このシステムを要求(請求)して、Cisco Intersightの機能を活用できます。オフになっている場合、Cisco Intersightへの通信は許可されません。 [Learn More](#)

デバイスコネクタ

有効化とアクセス設定

アクセスモード

- 読み取り専用
- 制御を許可
- Intersightだけからの設定
- Tunneled vKVM

● IMCソフトウェアのDNS設定の構成

ドメイン名

DNSサーバ

DNS サーバ

DNS サーバ

● IMCソフトウェアのNTP設定の構成

NTPサーバ

NTP サーバ

NTP サーバ

● プロキシ設定の構成

Enable Proxy

プロキシホスト名/IP*

プロキシポート*

プロキシホスト名

8080

認証

プロキシ

デバイス ID・要求コードの取得方法 (UCS Manager)

管理者アイコン>Device Connector

UCS Manager

All / Device Connector

デバイスコネクタは、クラウドベース管理プラットフォームであるCisco Intersightの機能を実現する組み込み管理コントローラです。デバイスコネクタ設定の詳細については、次を参照してください
[ヘルプセンター](#)

デバイスコネクタ

アクセスモード 制御を許可

Device Connector — Internet — Intersight

Not Claimed

Cisco Intersightポータルへの接続は成功しましたが、デバイスがまだ要求されていません。デバイスでCisco Intersightを開くように要求するには、新しいアカウントを作成してガイダンスに従うか、[デバイス]ページに移動し、既存のアカウントで[新しいデバイスを要求]をクリックします。 [Intersightを開く](#)

1.0.9-3200

デバイスID
省略

登録コード
省略

Logged in as admin@192.168.255.70

System Time: 2020-06-11T16:21

1. ターゲットメニューから“新しいターゲットの要求”をクリック

The screenshot shows the Cisco Intersight management console. On the left sidebar, the '管理' (Management) menu is expanded, and the 'ターゲット' (Targets) option is highlighted with a red box. In the main content area, a notification banner at the top right contains a button labeled '新しいターゲットの要求' (Request new target), which is also highlighted with a red box. Below the notification, a summary card shows '12' connections, with a breakdown: HX 5, UCS F1 3, Intersight アプライ... 2, Intersight Assist 1, and その他 1. At the bottom, a table lists the connections with columns for Name, Status, Type, Requested Time, and User.

[名前 (Name)]	ステータス	タイプ	請求された時間	登録者
hx-intersight.hx.local	接続中	Intersight Appliance	2020年4月6日 14:20	yokashim@cisco.com
hx1-intersight.hx.local	接続中	Intersight Appliance	2020年6月4日 11:39	yokashim@cisco.com
FIA	未接続	UCS Domain	2020年10月29日 14:16	yokashim@cisco.com
172.16.10.43	接続中	VMware vCenter	2020年6月2日 13:00	yokashim@cisco.com
c240M5	接続中	HyperFlex Cluster	2020年11月16日 16:01	yokashim@cisco.com
HX-SED-Cluster	接続中	HyperFlex Cluster	2020年11月30日 12:28	sanomura@cisco.com
hx2-intersight.hx.local	接続中	Intersight Assist	2020年6月2日 11:31	yokashim@cisco.com
Fl6332-16UP	接続中	UCS Domain	2020年4月7日 15:35	yokashim@cisco.com
Fl6454	接続中	UCS Domain	2020年11月24日 12:58	sanomura@cisco.com
HXSYSTEM	未接続	HyperFlex Cluster	2020年10月29日 14:19	yokashim@cisco.com

2. ターゲットタイプを選択し、デバイス ID と要求コードを入力

ターゲットタイプの選択

フィルタ

要求可能

カテゴリ

- すべて
- Compute / Fabric
- Platform Services
- オーケストレータ
- クラウド
- クラウド ネイティブ
- ゲスト OS プロセス/APM
- ストレージ
- ハイパーコンバージド
- ハイパーバイザ

Search

Compute / Fabric

- Cisco UCS Server (Standalone)
- Cisco UCS Domain (Intersight Managed)
- Cisco UCS Domain (UCSM Managed)

Platform Services

- Cisco Intersight Appliance
- Cisco Intersight Assist

ゲスト OS プロセス/APM

- Cisco AppDynamics

クラウド

キャンセル

デバイスコネクタによる登録の例

 **Cisco UCS Server (Standalone)**
To claim your target, you must have the Device ID and Claim Code.

デバイスID * 要求コード *

Intersight Assist による登録の例 (Intersight Assist 登録後に利用可能)

 **Vmware Vcenter**
To claim any on-premises target an Intersight Assist Appliance is required. Deploy and claim an Assist Appliance if needed before claiming the target

Intersight Assist * 管理アドレス *

Port

ユーザ名 * パスワード *

セキュア

データストア参照有効

ターゲットタイプから該当するものを選択

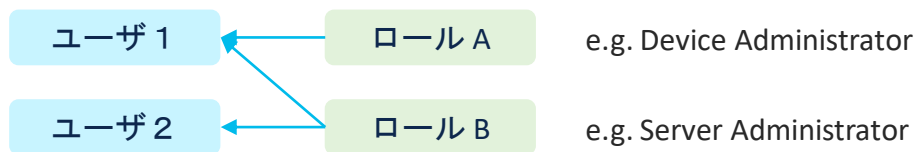
Intersight 初期設定

- ・ アカウント作成
- ・ デバイス登録
- ・ ユーザ、ロール設定

ユーザーとロール

- Intersight では、ロールベースアクセス制御 (RBAC) をサポート
- ID プロバイダ (IdP) を利用してユーザ、グループの追加が可能
- 外部 ID プロバイダの利用も可能 (SSO)
- ユーザおよびグループには、複数ロールを設定可能
- システム定義のロールに加え、ユーザがカスタムロールを作成可能

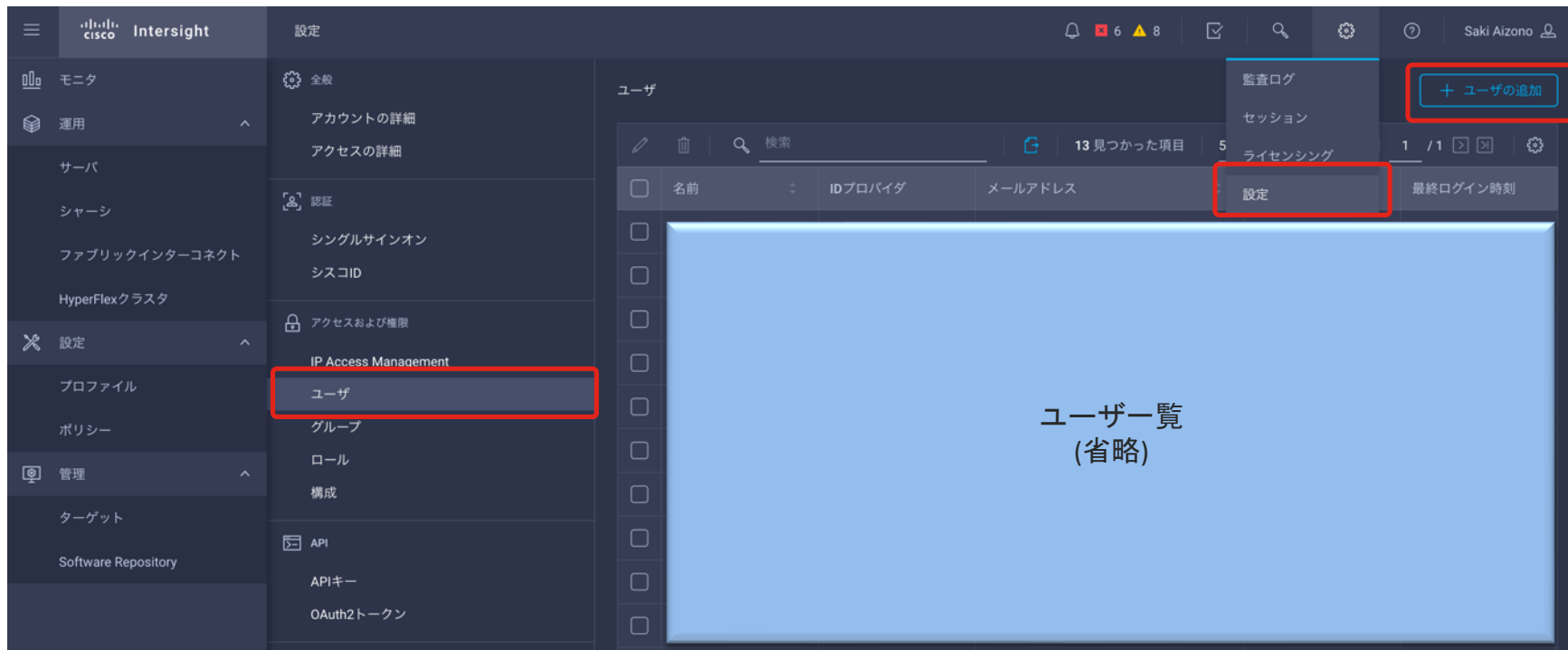
ロールベースアクセス制御 (RBAC) イメージ:



(参考) システム定義ロール一覧

ロール	説明
Account Administrator	Intersight アカウント内の全てのサービスとリソースへの完全なアクセスが可能。
Device Administrator	デバイスクレームとアンクレーム、デバイス詳細やライセンス状態、クレームされたデバイスリストの閲覧、API キーの生成が可能。その他の管理や管理者タスクは出来ない。
User Access Administrator	ユーザとグループの追加管理が可能。アカウント詳細や Audit ログの閲覧、Identity Provider、ロール、セッション、Account Administrator 以外のユーザ向け API キーの管理が可能。デバイスクレームや運用管理タスクは実行できない。また、Account Administrator ロールのユーザの追加、管理は出来ない。
Server Administrator	サーバと Fabric Interconnect の管理および閲覧、サーバと FI に関するダッシュボードウィジェットの閲覧、サーバアクションの実行、サーバ詳細の閲覧、管理コンソールおよび CLI の起動、サーバポリシーとプロファイルの作成と展開、API キーの管理が可能。デバイスクレームは出来ない。
HyperFlex Cluster Administrator	HyperFlex ポリシー、プロファイルの作成、クラスタの展開や管理、HX クラスタダッシュボードウィジェットの閲覧、HX Connect の起動が可能。デバイスクレームは出来ない。
Device Technician	デバイスクレーム、デバイス詳細やライセンス状態、クレームされたデバイスリストの閲覧、API キーの生成が可能。その他の管理や管理者タスクは出来ない。
Read-Only	ダッシュボード、管理対象デバイスのテーブル閲覧、ユーザ設定の変更、API キーの生成が可能。デバイスクレーム、ユーザの追加・削除、Identity Provider の設定やサーバアクションは出来ない。

ユーザの追加手順（1） 設定 > ユーザ 画面から、“ユーザの追加” を選択



The screenshot shows the Cisco Intersight interface. The left sidebar contains a navigation menu with categories like 'Monitor', 'Operate', 'Servers', 'Shares', 'Fabric Interconnects', 'HyperFlex Clusters', 'Settings', 'Profiles', 'Policies', 'Management', and 'Targets'. The 'Settings' menu is expanded, showing options like 'General', 'Authentication', 'Access and Permissions', 'IP Access Management', 'Groups', 'Roles', 'Composition', 'API', and 'API Keys'. The 'Users' option under 'IP Access Management' is highlighted with a red box. The main content area is titled 'ユーザー' (Users) and contains a table with columns for '名前' (Name), 'IDプロバイダ' (ID Provider), 'メールアドレス' (Email Address), '設定' (Settings), and '最終ログイン時刻' (Last Login Time). A red box highlights the '+ ユーザの追加' (Add User) button in the top right corner. The table content is obscured by a large blue box with the text 'ユーザー一覧 (省略)' (User List (Omitted)).

ユーザの追加手順（２） ID プロバイダ、メールアドレス、付与したいロールを選んで保存

ユーザの追加

IDプロバイダ*

Cisco

メールアドレス*

役割*

Device Administrator

役割*

Server Administrator

キャンセル 保存

ID プロバイダをドロップダウンより選択

- デフォルトでは Cisco が設定されているので、シスコ ID を持ったユーザのみが登録可能
- 外部の ID プロバイダの追加も可能 (次ページ参照)

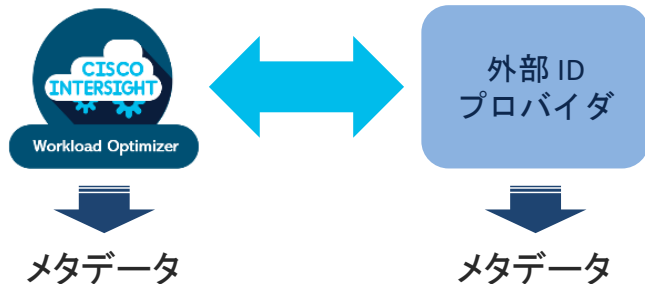
追加したいユーザのメールアドレスを入力

割り当てたいロールを設定

- 複数のロールを割り当てることが可能

外部の ID プロバイダの追加 (SSO)

- SAML 2.0 をサポートする ID プロバイダを Intersight に登録可能
- [Video demo of SSO setup](#) および intersight.com/help をご確認ください。



IDプロバイダの追加

名前 *

ドメイン名 *

Enable Single Logout

組織のIdPメタデータ *

[参照](#) ファイルが選択されていません

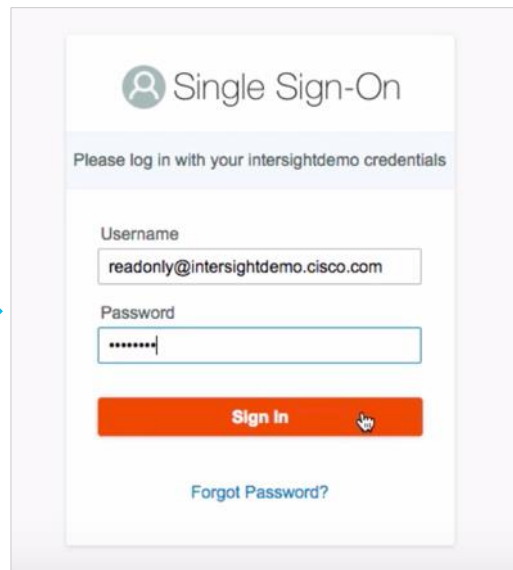
[キャンセル](#) [保存](#)

外部の ID プロバイダを利用した Intersight へのログイン

ログイン画面にて、シングルサインオン (SSO) を選択



外部 ID プロバイダを利用して認証が行われる。

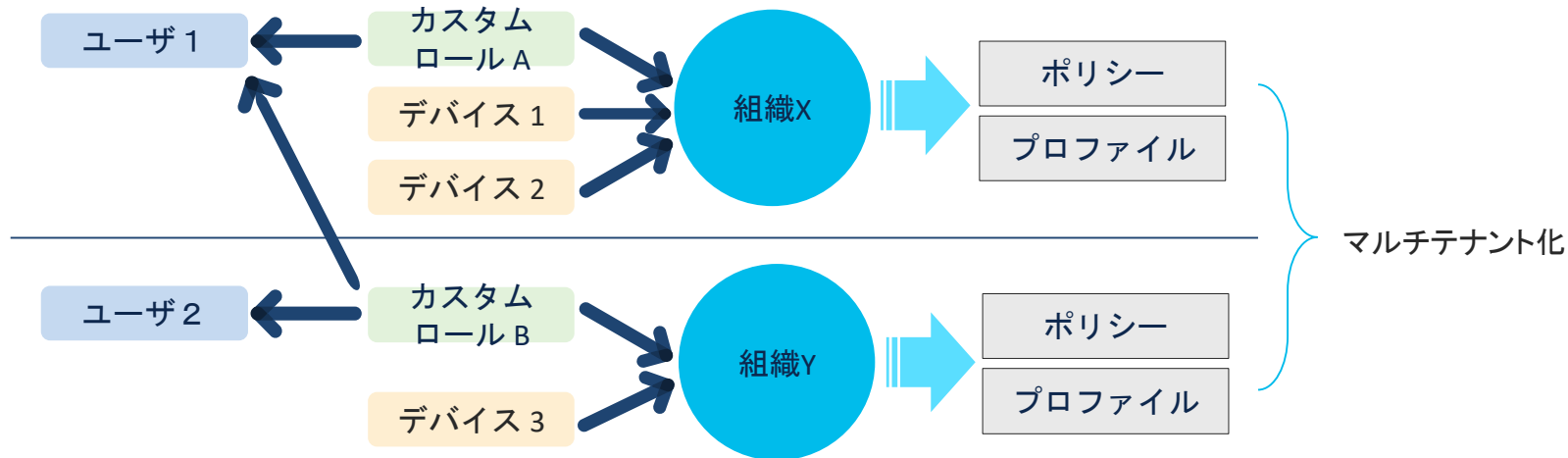


(AWS SSO サービスの例)

組織によるアクセス制御

- デバイスを論理的なグループ内に配置し、マルチテナント化
- デバイスへのアクセスだけでなく、ポリシーやプロファイルも制限
- "default" の組織には、全てのリソースが紐付いている。

組織とユーザ、ロール、デバイスの関係イメージ



組織設定方法

① 組織を作成し、デバイスを紐付ける

設定 > アクセスおよび権限 > 構成 > Create Organization

組織の編集
組織を編集して、論理リソースと物理リソースへのアクセスを管理します。

全般

組織の名前

Name *
HX-SED-Cluster

Description

メンバーシップ

カスタム すべて

デバイスを組織に紐付け

デバイスを選擇して、カスタム組織を作成します。カスタム組織内に作成されたプロフィールとポリシーは、同じ組織内のデバイスにのみ適用されます。

検索

12 見つかった項目 10 ページごと 1 / 2

[名前 (Name...]	ステータス	タイプ	デバイスIPア...	デバイスID
<input type="checkbox"/> hx-intersight.hx.lo...	Connected	IntersightApplia...	172.16.10.52	91512612-b04e-4892-9...
<input checked="" type="checkbox"/> F16332-16UP	Connected	UCSFI	172.16.10.124,172...	FDO221406HZ,FDO221...
<input type="checkbox"/> hx2-intersight.hx.l...	Connected	IntersightApplia...	172.16.10.54	7501bbcd-7bb7-43b5-8...

② カスタムロールを作成し、組織に紐付ける

設定 > アクセスおよび権限 > ロール > ロールを作成する

ステップ 2
Configuration
Select a Scope to delegate the user access to resources in the account.

スコープ

[すべて]を選択すると、アカウントまたは'組織'内のすべてのリソースにアクセスでき、選択したリソースグループにアクセスできます

すべて 組織

ロールを組織に紐付け

アクセス制御

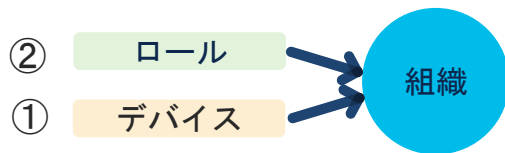
オーガナイゼーション*

HX-SED-Cluster

default
hyperflex
HX-SED-Cluster

権限*

HyperFlex Cluster Administrator × Server Administrator ×
Virtualization Administrator × UCS Domain Administrator ×



Intersight による サーバ運用管理

- ・ Firmware アップグレード
- ・ ポリシーベース設定

Intersight による サーバ運用管理

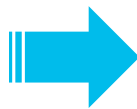
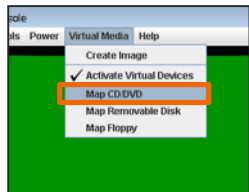
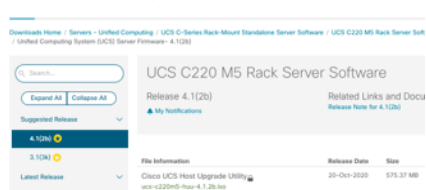
- Firmware アップグレード
- ポリシーベース設定

Intersight によるファームウェアアップグレード

- 従来手動で行っていた以下の作業を自動化し、作業手順を簡素化
 - Cisco Software Central からのファームウェアイメージをダウンロード、およびデバイスへのアップロード
 - ファームウェアイメージのサーバへのマウント

Cisco IMC でのファームウェアアップグレードイメージ

Software Download



Intersight による自動化



イメージ
ダウンロード

自動マウント



イメージダウンロード



Cisco IMC - KVM
CD/DVD Mapping



Boot 制御

分離された複雑なステップ、手動での実施



定義されたワークフローにより簡単に実施

Standalone UCS のファームウェアアップグレード

・ Utility Storage がない場合

1. データセンター内にファイルサーバを用意し、HUU イメージを置いておく
2. Intersight にイメージへのアクセス情報を登録
3. Intersight からアップグレードを実行

ファイルサーバ
(手動でイメージ用意)

NFS
CIFS
HTTPS



自動でマウント

イメージの場所を登録

ファームウェアアップグレード



・ Utility Storage がある場合

1. Intersight からアップグレードを実行

Utility Storage

メンテナンスのための組み込みストレージ領域
M5 : FlexUtil (microSD)
M4 : FlexFlash (SD)

Cisco.com
HUU イメージ

利用

イメージダウンロード
ファームウェアアップグレード

Utility Storage

HUU

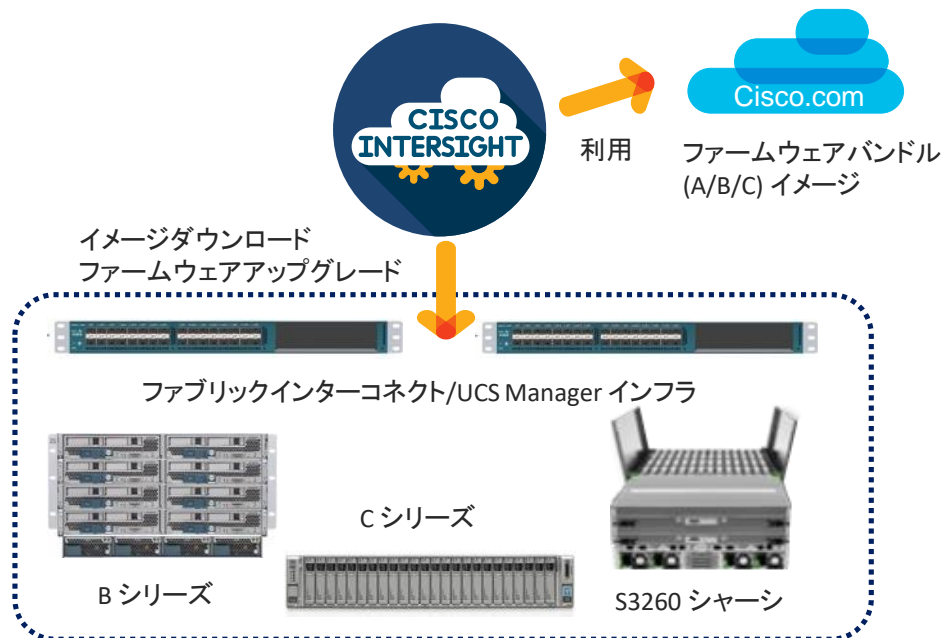


自動でマウント

サーバ規模、環境に合わせて選択

FI Integrated UCS のファームウェアアップグレード

- FI にイメージをダウンロードし、自動でアップグレード



- FI およびサーバのファームウェアをアップグレード
- デフォルトで Fabric Evacuation を選択
- Associated 状態のサーバのみサポート
- アップデートテンプレート利用サーバは非サポート

FI / UCSM インフラのファームウェアアップグレードフロー（1）

ファブリックインターコネクトのメニューから Upgrade Firmware を選択

The screenshot displays the Cisco Intersight interface for managing Fabric Interconnects. The left sidebar shows the navigation menu with 'ファブリックインターコネクト' (Fabric Interconnect) selected. The main content area shows a summary of device health and status, with a table listing two FI-6332-16UP devices. A dropdown menu is open over the table, highlighting the 'Upgrade Firmware' option.

Health: 2 (クリティ... 2)

Connection: Connected 2

ファームウェアバージョン: 2 (4.0(4c) 2)

モデル: 2 (6332-16... 2)

契約ステータス: Not Covered 2

検索: エクスポート 2見つかった項目 12 ページごと 1 / 1

名前	ヘルス	契約ステータス	管理IP	モデル	搭載拡...	合計	ポート数 使用済み	残り使...	ファーム...
FI-6332-16UP	Critical	Not Covered	192.168.255....	UCS-FI-6332-...	0	46	8	38	4.0(4c)
FI-6332-16UP	Critical	Not Covered	192.168.255....	UCS-FI-6332-...	0	46	8	38	4.0(4c)

- Launch UCS Manager
- Launch CLI
- Open TAC Case
- Upgrade Firmware

FI / UCSM インフラのファームウェアアップグレードフロー（2）

ファームウェアアップグレードのフローを確認して開始

The screenshot displays the Cisco Intersight interface for upgrading firmware. The top navigation bar shows 'Fabric Interconnects > Upgrade Firmware' and the user 'Saki Aizono'. A notification banner at the top states '新機能が最近追加されました。詳細はこちら' (New features have been recently added. See details here). The main content area is titled 'ファームウェアのアップグレード' (Firmware Upgrade) and contains two sequential steps:

- Version**: Select a firmware version to upgrade the fabric interconnects to.
- Summary & Firmware Upgrade**: Confirm configuration and initiate the upgrade.

Below the steps is a link for 'About Firmware Upgrade' and a prominent blue 'Start >' button. A 'キャンセル' (Cancel) button is located at the bottom left of the page.

FI / UCSM インフラのファームウェアアップグレードフロー（3）

アップグレードしたいファブリックインターコネクトを選択

新機能が最近追加されました。 [詳細はこちら](#)

進捗ステータス

- 1 General
- 2 Version
- 3 Summary

手順1/3
General
Ensure selected fabric interconnects meet requirements for firmware upgrade.

Confirm Fabric Interconnects Selection 1 Selected

Infrastructure firmware upgrade can be performed only on a pair of fabric interconnects at once

1 見つかった項目 | 10 ページごと | 1 / 1

検索

Domain Name	Fabric Interconnect A			Fabric Interconnect B		
	モデル	シリアル	ファーム...	モデル	シリアル	ファーム...
<input checked="" type="checkbox"/> FI-6332-16UP	UCS-FI-63...	FDO2223...	4.0(4c)	UCS-FI-63...	FDO2216...	4.0(4c)

選択日時 1 / 1 | [選択内容を表示](#) | [選択をすべて解除](#) | 1 / 1

< 戻る | キャンセル | 次へ >

FI / UCSM インフラのファームウェアアップグレードフロー（４）

アップグレード先のファームウェアバージョンを選択

新機能が最近追加されました。 [詳細はこちら](#)

進捗ステータス

- 1 General
- 2 Version
- 3 Summary

手順2/3
Version
Select a firmware version to upgrade the fabric interconnects to.

Select Firmware Bundle

The selected firmware bundle will be downloaded from intersight.com

35見つかった項目 | 10 ページごと

検索

	Version	Size	Release Date	Description	
<input type="radio"/>	4.1(1d)	1.16 GiB	2020年7月10日 09:00	The UCS Infrastructure Soft...	👁
<input checked="" type="radio"/>	4.1(1c)	1.16 GiB	2020年4月20日 09:00	The UCS Infrastructure Soft...	👁
<input type="radio"/>	4.1(1b)	1.16 GiB	2020年3月12日 09:00	The UCS Infrastructure Soft...	👁
<input type="radio"/>	4.1(1a)	1.16 GiB	2020年2月20日 09:00	The UCS Infrastructure Soft...	👁
<input type="radio"/>	4.0(4i)	1.17 GiB	2020年7月6日 09:00	The UCS Infrastructure Soft...	👁
<input type="radio"/>	4.0(4h)	1.17 GiB	2020年3月23日 09:00	The UCS Infrastructure Soft...	👁
<input type="radio"/>	4.0(4n)	1.17 GiB	2019年12月0日 09:00	The UCS Infrastructure Soft...	👁

View Firmware Details

Version 4.1(1c)
Image Name ucs-6300-k9-bundle-infra.4.1.1c.A.bin
Release Date 2020年4月20日 09:00
Size 1.16 GiB
Supported Models UCS-FI-6332, UCS-FI-6332-16UP(2)
Description The UCS Infrastructure Software Bundle contains: - NX-OS software for the UCS 6332 Fabric Interconnects - Firmware for the fabric extenders and I/O modules - UCS Manager - Chassis Management Controller - UCSM Capability Catalog. [View Release Notes](#)

OK

ファームウェア詳細情報の確認

< 戻る | キャンセル | 次へ >

FI / UCSM インフラのファームウェアアップグレードフロー（5）

アップグレードのサマリを確認し、問題なければアップグレードボタンをクリック

新機能が最近追加されました。 [詳細はこちら](#)

進捗ステータス

手順3/3
Summary
Confirm configuration and initiate the upgrade.

1 Selected firmware bundle will be downloaded to the fabric interconnects and upgraded. Click on Requests to monitor the progress of the firmware upgrade.

Firmware

Version	4.1(1c)	Size	1.16 GiB
---------	---------	------	----------

Fabric Interconnects to be Upgraded

1 見つかった項目 | 10 ページごと | 1 / 1

検索

Domain Name	Fabric Interconnect A			Fabric Interconnect B		
	Model	Serial	Firmware V...	Model	Serial	Firmware V...
FI-6332-16UP	UCS-FI-633...	FD022232...	4.0(4c)	UCS-FI-633...	FD022160...	4.0(4c)

< 戻る キャンセル Upgrade >

FI / UCSM インフラのファームウェアアップグレードフロー（6）

本当にアップグレードするかどうかの確認

新機能が最近追加されました。 [詳細はこちら](#)

進捗ステータス

手順3/3
Summary
Confirm configuration and initiate the upgrade.

Selected firmware bundle will be downloaded to the fabric interconnects and upgraded. Click on Requests to monitor the progress of the firmware upgrade.

ファームウェアのアップグレード

Firmware will be installed on the selected fabric interconnects. Are you sure you want to upgrade firmware?

キャンセル Upgrade

Domain Name	Fabric Interconnect A			Fabric Interconnect B		
	Model	Serial	Firmware V...	Model	Serial	Firmware V...
FI-6332-16UP	UCS-FI-633...	FDO22232...	4.0(4c)	UCS-FI-633...	FDO22160...	4.0(4c)

< 戻る キャンセル Upgrade >

FI / UCSM インフラのファームウェアアップグレードフロー（7）

Intersight がソフトウェアを Cisco 側から引き出すために、Cisco ID とパスワードを提供

The screenshot shows the Cisco Intersight interface during a firmware upgrade process. A modal dialog box is open, titled "Setup Software Download Service". The dialog contains the following text:

To upgrade firmware from Cisco Repository, Intersight must be enabled for Cisco Software Download Services. Learn more at [Help Center](#).

Provide your user credentials to get security token which is required to get access to cloud firmware image library.

Security token will be valid for next 24 hours.

シスコID *

パスワード *

Buttons: キャンセル (Cancel), 送信 (Submit)

The background interface shows the "Upgrade Firmware" page for "Fabric Interconnects". The left sidebar has sections for "OPERATE" (サーバ, シャーシ, ファブリックインターコネクタ, HyperFlexクラスタ) and "ADMIN" (デバイス, Software Repository). The main content area has a progress indicator with three steps: 1. General, 2. Version, and 3. Summary (highlighted). A table below shows details for "Fabric Interconnect B", including columns for Firmware V..., Model, Serial, and Firmware V... with values like UCS-FI-633... and FDO22160....

FI / UCSM インフラのファームウェアアップグレードフロー（8）

ライセンス契約の条項に同意すると、インストールが始まる

The screenshot shows the Cisco Intersight interface for upgrading firmware on Fabric Interconnects. A modal dialog box titled "Cisco End User License Agreement" is displayed in the center. The dialog contains the following text:

Cisco End User License Agreement

エンドユーザライセンス契約書をよくお読みください。

In order to download software, Please confirm that you have read and agree to be bound by the terms of the [Cisco End User License Agreement](#) and any [Supplemental Terms](#), if applicable.

ライセンス契約の条項に同意する

Buttons: キャンセル (Cancel), 送信 (Submit)

The background interface shows the "Upgrade Firmware" page for Fabric Interconnects. The left sidebar includes sections for "ダッシュボード", "OPERATE", "設定", and "ADMIN". The main content area shows a progress indicator with three steps: 1. General, 2. Version, and 3. Summary (highlighted). Below the dialog, a table lists the devices to be upgraded:

Firmware V...	Model	Serial	Firmware V...
4c) (↓)	UCS-FI-633...	FDO22160...	4.0(4c) (↓)

At the bottom of the page, there are navigation buttons: "< 戻る" (Back), "キャンセル" (Cancel), and "Upgrade >" (Upgrade).

FI / UCSM インフラファームウェアアップグレード成功時の実行フロー

Intersight 上で進行中の実行フローを確認

The screenshot displays the Cisco Intersight interface for a 'Firmware Infra Upgrade' request. The status is 'Success'. The execution flow is as follows:

Step	Timestamp
Wait for infra upgrade to complete.	Jun 22, 2020 10:20 PM
Wait for user acknowledgement.	Jun 22, 2020 9:52 PM
Wait for user acknowledgement on fabric interconnect - A.	Jun 22, 2020 9:52 PM
Check if user acknowledgement is required.	Jun 22, 2020 8:35 PM
Wait for peer fabric interconnect activation to complete. <i>Waiting for User acknowledgement</i>	Jun 22, 2020 8:35 PM
Activate peer fabric interconnect.	Jun 22, 2020 7:55 PM
Validate if any upgrade is running in fabric interconnect.	Jun 22, 2020 7:55 PM
Validate if image is present in fabric interconnects. <i>ucs-k9-bundle-infra-4.1.1b.A.bin is present in UCSM</i>	Jun 22, 2020 7:55 PM
Validate the space availability prerequisite in the fabric interconnects. <i>Validation of pre-upgrade space availability completed successfully.</i>	Jun 22, 2020 7:55 PM

Intersight による サーバ運用管理

- Firmware アップグレード
- ポリシーベース設定

UCS Manager - サービスプロファイルによる設定抽象化

- UUID・WWN・MAC・BIOS 設定などハードウェア固有情報を抽象化
- サーバに依存した設定をなくすことでサーバ移行を簡単にできる

サーバ管理者のメリット

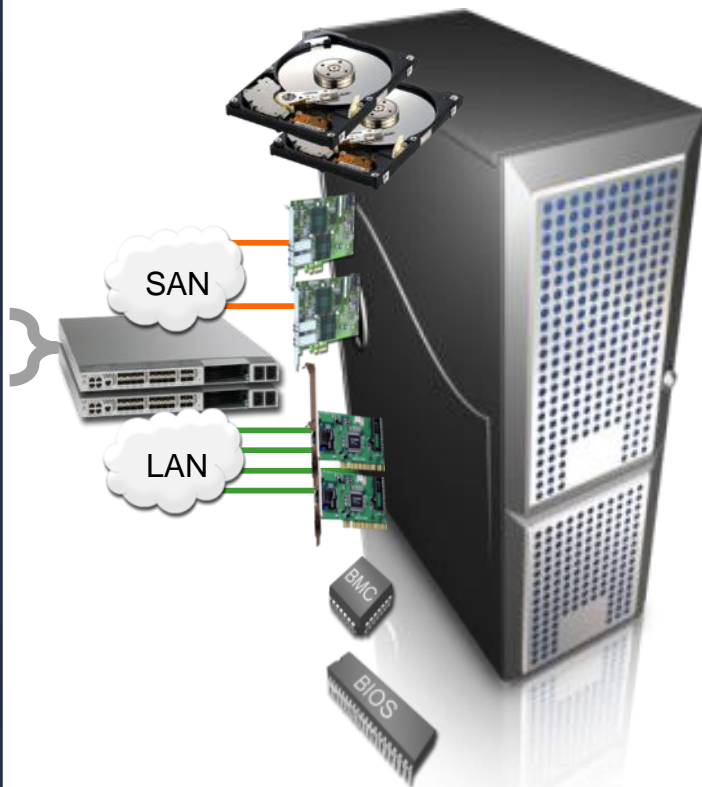
サーバ機種変更に伴うスイッチ・ストレージ変更依頼を一切行うことなく、既存環境を新規サーバに容易に移行可能

ストレージ管理者のメリット

ストレージの初期設定変更を行うことなくサーバ移行することが可能

Cisco UCS サービスプロファイル

NIC Existence
NIC MACs
HBA Existence
HBA WWPNs
Server UUID
BIOS Settings
RAID Settings
SED/KMIP Settings
VLAN Assignments
VLAN Tagging
FC Fabrics Assign.
FC/iSCSI Boot Settings
Boot order
PXE settings
IPMI Settings
QoS
Template Association
Org & Sub Org Assoc.
Server Pool Assoc.
Statistic Thresholds
BIOS scrub actions
Disk scrub actions
BIOS firmware
Adapter firmware
BMC firmware
Advanced NIC settings
Serial over LAN settings



Intersight による UCS サーバのポリシーベース設定

- Standalone UCS は Intersight に接続することで、ポリシーベース設定が可能
- FI Integrated UCS は、現在は UCS Manager でポリシーの管理が可能だが、将来的に Intersight から管理が可能になる

Now: CIMC

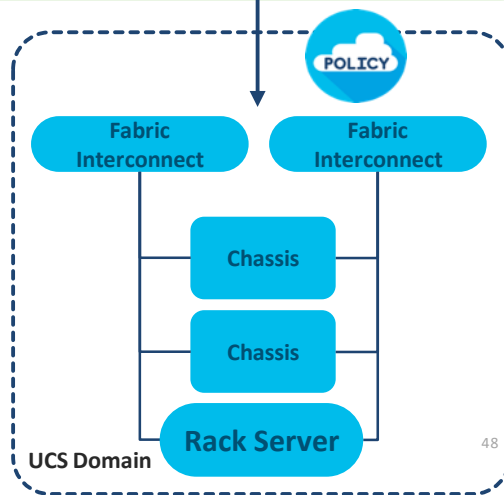
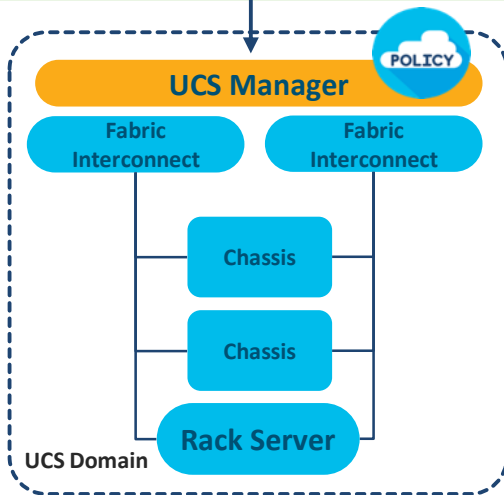
Now: UCS Manager

Future: Intersight Managed Mode

Intersight



Rack Server



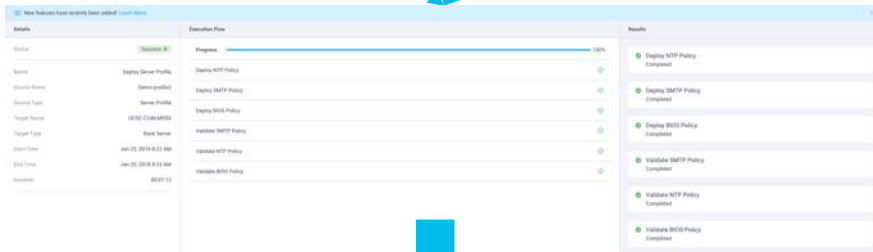
スタンドアロン UCS のポリシーベース設定



サーバポリシー

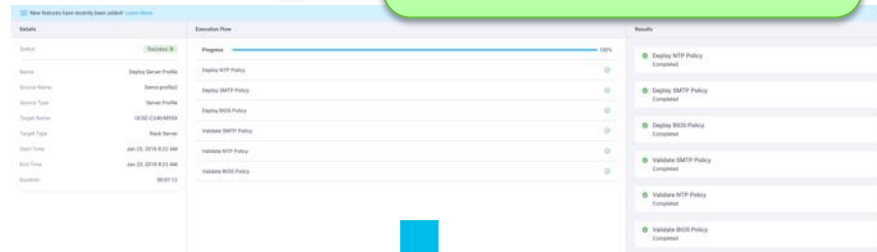
- ✓ NTP 設定
- ✓ Disk Group 設定
- ✓ DNS 設定
- ✓ DHCP 設定
- ✓ vKVM 設定
- ✓ SMTP 設定
- ✓ SNMP 設定
- ✓ SSH 設定
- ✓ Local User 設定
- ✓ Boot Order 設定

プロフィール1



物理サーバ1に適用

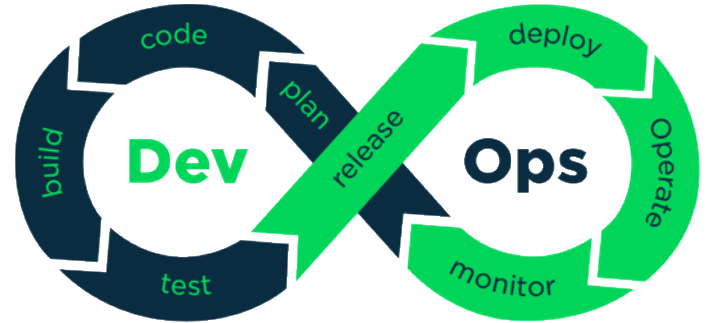
プロフィール2



物理サーバ2に適用

複数のサーバに同じポリシーを適用して、ベースラインのコンフィグが可能。

Ansible 自動化



“Infrastructure as code (IaC) is the process of managing and provisioning computer through machine-readable definition files [...].”

Wikipedia - https://en.wikipedia.org/wiki/Infrastructure_as_Code

Infrastructure as code を実現する様々なツール



Tail-f is now
part of Cisco.



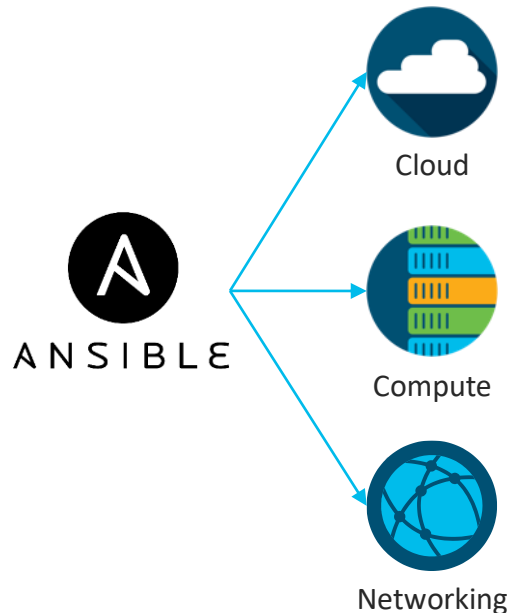
SALTSTACK



ANSIBLE

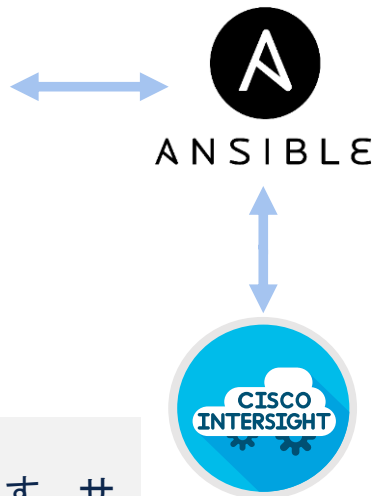
Ansible 紹介

- シンプルな IT 自動化プラットフォーム
- 多くの種類のタスクを処理可能：
 - システムの構成 / 構成管理
 - ソフトウェアの展開 / ソフトウェアパッケージの管理
 - 様々なシステムのプロビジョニング
 - オーケストレーション
- 完全なオープンソース (開発元は Red Hat)



Ansible Collection

- ベンダーモジュールは Ansible に含まれなくなる
 - Ansible 2.10 では Ansible Collection のインストールが必要
 - ベンダーモジュールの追加・アップデートは Ansible Core リリースに依存しない
- ベンダーモジュールは Ansible Galaxy より入手可能
 - 必要なモジュールのみのインストール
 - 必要なモジュールのバージョンをインストール
- Intersight Ansible Collection
 - <https://galaxy.ansible.com/cisco/intersight>



免責事項:

Cisco は利便性と情報提供のみを目的として Ansible モジュールの提供を行っています。サポートについては提供しておりませんので、予めご了承ください。

Ansible Intersight Collection の使い方概要

- Python, Ansible 実行環境を準備
- Ansible Galaxy より Intersight Collection をインストール
- Intersight API キーの生成
- インベントリファイル、Playbook を編集して利用



今回利用した実行環境

- MacOS
- Python 3.7.5

```
$ python --version  
Python 3.7.5
```

- Ansible 2.10.3

```
$ ansible --version  
ansible 2.10.3  
  config file = None  
  configured module search path = ['/Users/sanomura/.ansible/plugins/modules',  
'/usr/share/ansible/plugins/modules']  
  ansible python module location =  
/Users/sanomura/dev/20201209_intersight_ansible_webinar/test/lib/python3.7/site-packages/ansible  
  executable location = /Users/sanomura/dev/20201209_intersight_ansible_webinar/test/bin/ansible  
  python version = 3.7.5 (v3.7.5:5c02a39a0b, Oct 14 2019, 18:49:57) [Clang 6.0 (clang-600.0.57)]
```


Intersight Collection のインストール by Ansible Galaxy

- Cisco Intersight Collection in Ansible Galaxy

<https://galaxy.ansible.com/cisco/intersight>

- ansible-galaxy コマンドによる Collection のインストール

```
$ ansible-galaxy collection install cisco.intersight
Process install dependency map
Starting collection install process
Installing 'cisco.intersight:1.0.8' to
'/Users/sanomura/.ansible/collections/ansible_collections/cisco/intersight'
```

Intersight Collection のインストールコンテンツ確認

- インストール先のディレクトリのコンテンツを確認

```
$ cd /Users/sanomura/.ansible/collections/ansible_collections/cisco/intersight
```

```
$ ls
```

```
Development.md  LICENSE.txt      README.md  misc  plugins  roles  
FILES.json     MANIFEST.json   docs      playbooks
```

module, module_units,
documentationが含まれる

- Playbook ディレクトリの内容

サンプル Playbook が含まれる

```
$ cd playbooks/
```

```
$ ls
```

```
claim_device.yml          intersight_ntp_policy.yml  
cos_server_policies_and_profiles.yml intersight_server_profile.yml  
deploy_server_profiles.yml intersight_virtual_media_policy.yml  
devnet_inventory         ova_workflow.yml  
example_inventory        roles  
firmware_direct_download.yml server_actions.yml  
hcl_status.yml           server_firmware.yml  
intersight_boot_order_policy.yml staging_inventory  
intersight_imc_access_policy.yml update_all_inventory.yml  
intersight_local_user_policy.yml update_standalone_inventory.yml
```

Intersight API キー取得方法（1）



The screenshot shows the Cisco Intersight web interface. The left sidebar contains navigation options: モニタ (Monitor), 運用 (Operate), 設定 (Configure), 最適化 (Optimize), and 管理 (Manage). The main content area is titled 'アカウントの詳細' (Account Details) and displays the following information:

アカウント名	PBST-UCSC
アカウントID	5d12271f7564612d30acdfdd
アクセスリンク	https://5d12271f7564612d30acdfdd.intersight.com/
ライセンス	Premier
作成時刻	2019年6月25日 22:52
Default Idle Timeout	30m
Maximum Concurrent Sessions per User	32 sessions
Default Session Timeout	16h

A dropdown menu is open over the '設定' (Settings) link in the left sidebar. The menu items are: 監査ログ (Audit Log), セッション (Sessions), ライセンシング (Licensing), and 設定 (Settings). The '設定' item is highlighted with a red box.

Intersight API キー取得方法（2）

The screenshot shows the Cisco Intersight management console. The left sidebar contains a navigation menu with categories: モニタ (Monitor), 運用 (Operate), 設定 (Configure), 最適化 (Optimize), and 管理 (Manage). Under the 設定 (Configure) category, the API Key option is highlighted with a red box. The main content area displays the 'API Key' management page. At the top right of this page, the 'APIキーの生成' (Generate API Key) button is highlighted with a red box. Below this, there is a table listing API keys. The table has columns for '説明' (Description), 'APIキーID', 'Purpose', '作成...' (Created...), 'メール...' (Email...), and '役割' (Role). A single row is visible with the text '生成済みの API キー (省略)' (Generated API Key (omitted)), indicating that the key has been successfully created.

Intersight API キー取得方法（3）

APIキーの生成

説明
Ansible for Webinar

API Key Purpose

- API key for OpenAPI schema version 2 Use RSA keys with 2048 bits, RSA SSA PKCS1 v1.5 signature algorithm, and SHA256 cryptographic hash
- API key for OpenAPI schema version 3 (This is a feature in preview and for SDK developer use only)

閉じる 生成

	Purpose	作成...	メール...	役割
見つかった項目				
226e97564612d30ac...	Legac...	2020年1...	sano...	Accou...

Intersight API キー取得方法（４）

APIキーの生成

秘密鍵を表示またはダウンロードできるのは1回だけです。後で秘密鍵を回復することはできません。ただし、いつでも新しいアクセスキーを作成できます。

APIキーID

API キー ID (省略)

秘密キー

----BEGIN RSA PRIVATE KEY----

秘密鍵 (省略)

閉じる

秘密鍵はテキストに保存

	Purpose	作成...	メール...	役割
226e97564612d30ac...	Legac...	2020年1...	sano...	Accou...
226e97564612d30ac...	Legac...	数秒前	sano...	Accou...

Intersight API キー取得方法 (5)

The screenshot displays the Cisco Intersight user interface for managing API keys. The left sidebar contains navigation menus for 'モニタ', '運用', '設定', '最適化', and '管理'. The main area shows the 'APIキー' (API Keys) section with a table of existing keys. A red box highlights the 'API キー ID (省略)' (API Key ID (omitted)) in the table. A callout box below the table states: 'API キー ID は後からでも確認可能' (API Key ID can be confirmed even after).

説明	APIキーID	Purpose	作成...	メール...	役割
	生成済みの API キー (省略)				
Ansible for Webinar	API キー ID (省略)	Legac...	1時間前	sano...	Accou...

インベントリファイル内 API 変数のカスタマイズ

- Intersight Collection Playbook ディレクトリの 'example_inventory' ファイルに API キー情報が含まれており、今回はこれを利用する。
- example_inventory をコピーして新しいインベントリファイルを作成

```
$ cp example_inventory inventory
```

- インベントリファイル内の [Intersight:vars] セクションが、API キー認証を含んでおり、これを Playbook から参照する形をとる。

インベントリファイル内 API 変数のカスタマイズ

- 生成した API キーを利用するようインベントリファイルを編集

example_inventory ファイル :

```
[Intersight_HX]
# Note: at least one host (e.g., sjc07-r13-501) must be present for
update*_inventory.yml to work
sjc07-r13-501
sjc07-r13-503

[Intersight_Servers]

[Intersight:children]
Intersight_HX
Intersight_Servers

[Intersight:vars]
api_private_key=~/.Downloads/SecretKey.txt
api_key_id=596cc79e5d91b400010d15ad/5f0ce0ad7564612d3311a1f3/5f0ea8eb7564612d334ccb5a
```

前段はマニュアルでの
修正は不要

保存した秘密鍵のパスを指定

API キー ID を入力

インベントリ情報をアップデートする

- Playbook “update_standalone_inventory.yml” を利用して Intersight から情報を取得し、スタンドアロンサーバのインベントリファイルをアップデートする。

```
$ ansible-playbook -i inventory update_standalone_inventory.yml
[WARNING]: running playbook inside collection cisco.intersight

PLAY [Intersight] *****

TASK [cisco.intersight.intersight_rest_api] *****(snip)
```

実行結果例:

通常は将来的な Collection のアップデートによる
上書き等を考慮して Collection ディレクトリ外に
Playbook を配置するが、ラボ環境ではOK

```
$ ansible-playbook -i inventory update_standalone_inventory.yml
[WARNING]: running playbook inside collection cisco.intersight

PLAY [Intersight] *****

TASK [cisco.intersight.intersight_rest_api] *****
ok: [sjc07-r13-501]

TASK [debug] *****
ok: [sjc07-r13-501] => {
  "msg": "Inventory filepath
  ¥"/Users/sanomura/.ansible/collections/ansible_collections/cisco/intersight/playbooks/inventory¥"
}

TASK [lineinfile] *****
ok: [sjc07-r13-501]

TASK [lineinfile] *****
changed: [sjc07-r13-501] => (item=UCS-PBST-C-C220M4-3)
changed: [sjc07-r13-501] => (item=UCS-PBST-C-C220M4-4)
changed: [sjc07-r13-501] => (item=UCS-PBST-C-C220M4-2)
changed: [sjc07-r13-501] => (item=UCS-PBST-C-C220M4-1)

PLAY RECAP *****
sjc07-r13-501      : ok=4    changed=1    unreachable=0    failed=0    skipped=0
rescued=0         ignored=0
```

インベントリファイルが自動的にアップデートされる。

実行前：

```
[Intersight_Servers]
```

(空白)



実行後：

```
[Intersight_Servers]
```

UCS-PBST-C-C220M4-1	server_moid=5e33c03a6176752d33676f96	model=UCSC-C220-M4S
UCS-PBST-C-C220M4-2	server_moid=5e33be156176752d3366f948	model=UCSC-C220-M4S
UCS-PBST-C-C220M4-4	server_moid=5e18050b6176752d339e56f3	model=UCSC-C220-M4S
UCS-PBST-C-C220M4-3	server_moid=5e16e2966176752d3366afdd	model=UCSC-C220-M4S

サーバ名

サーバの Moid

サーバモデル

※ Moid = Managed Object Identifier
REST リソース (Managed Object) が
作成されたときに割り当てられる固有の ID

Intersight + Ansible を利用した運用例

Scenario1 : サーバのポリシー/プロファイル設定

- Standalone UCS サーバのポリシー/プロファイルを作成し、サーバに展開 (設定) する。



Intersight
モジュール

Playbook:
cos_server_policies_and_profiles.yml

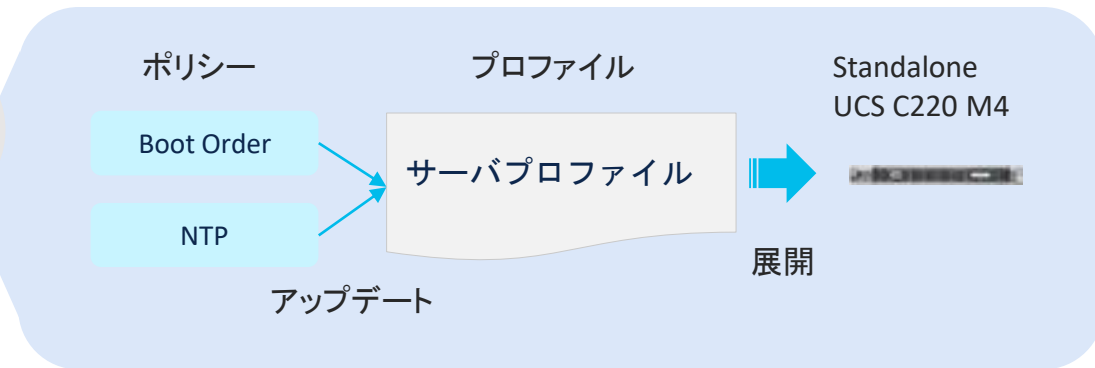
Task:

- プロファイル作成
- ポリシー作成
- プロファイルアップデート

Playbook: deploy_server_profiles.yml

Task:

- サーバプロファイルの展開



Playbook:
cos_server_policies_and_profiles.yml

Playbook:
deploy_server_profiles.yml

ポリシー/プロファイル設定 Playbook

“cos_server_policies_and_profiles.yml” の中身抜粋

```
- hosts: "{{ group | default('Intersight_Servers') }}"
  connection: local
  collections:
    - cisco.intersight
  ...
  tasks:
    # Get the Organization Moid used by all profiles and policies
    - name: "Get Organization {{ org_name }} Moid"
      intersight_rest_api:
        <<: *api_info
        resource_path: /organization/Organizations
        query_params:
          $filter: "Name eq '{{ org_name }}'"
        register: org_resp
        delegate_to: localhost
        tags: always
    #
    # Configure profiles specific to server (run for each server in the inventory)
    # Server Profiles role will register a profile_resp and profile_resp list (from all hosts) can
    # be used by policy tasks
    - name: "Configure {{ profile_name }} Server Profile"
      intersight_rest_api:
```

Collection ステートメント
各タスクでのモジュールの完全修飾が不要

ここからタスクを記載

組織の Moid を取得するタスク

サーバプロファイルを設定するタスク

ポリシー/プロファイル設定 Playbook - Boot Order Policy

“cos_server_policies_and_profiles.yml” - Task > Block 内の Boot Order Policy 設定

```
- block:
  # Boot Order policy
  - import_role:
    name: policies/server_policies
  vars:
    resource_path: /boot/PrecisionPolicies
    api_body: {
      "Name": "COS-Boot",
      "ConfiguredBootMode": "Legacy",
      "BootDevices": [
        {
          "ObjectType": "boot.LocalDisk",
          "Enabled": true,
          "Name": "Disk",
          "Slot": "MRAID"
        },
        {
          "ObjectType": "boot.VirtualMedia",
          "Enabled": true,
          "Name": "VM",
          "Subtype": "cimc-mapped-dvd"
        }
      ],
      "Organization": {
        "Moid": "{{ org_resp.api_response.Moid }}"
      }
    }
  tags: boot_order
```

Boot Order ポリシーの設定値

ポリシー名 : COS-Boot
設定されたブートモード : レガシー
ブートデバイス
- ローカルディスク
有効 : Yes
デバイス名 : Disk
スロット : MRAID
- 仮想メディア
有効 : Yes
デバイス名 : VM
サブタイプ : cimc-mapped-dvd

タグ : Playbook の特定の部分のみ実行できるようになる

ポリシー/プロファイル設定 Playbook - Boot Order Policy

- タグを利用した部分実行 -

```
$ ansible-playbook -i inventory cos_server_policies_and_profiles.yml --tags boot_order
PLAY [Intersight_Servers] *****

TASK [Get Organization default Moid] *****
ok: [UCS-PBST-C-C220M4-1]
ok: [UCS-PBST-C-C220M4-4]
ok: [UCS-PBST-C-C220M4-3]
ok: [UCS-PBST-C-C220M4-2]

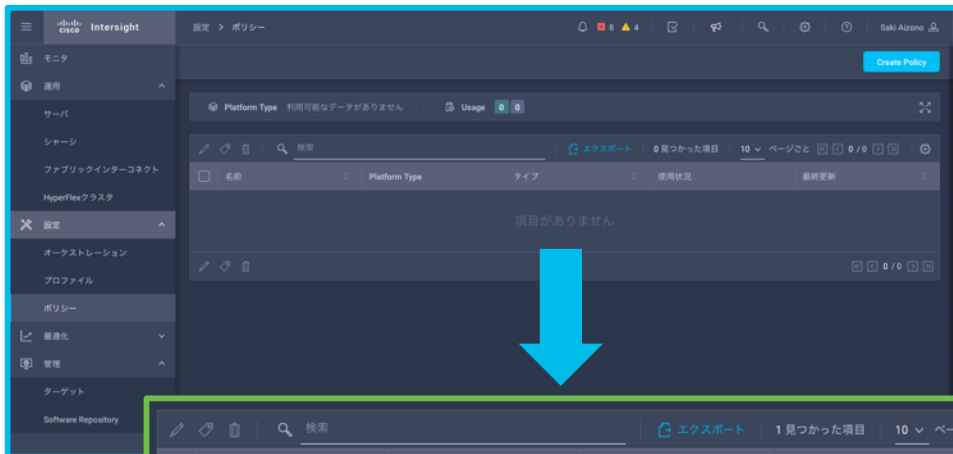
TASK [policies/server_policies : Configure COS-NTP Server Policy] *****
changed: [UCS-PBST-C-C220M4-1]

TASK [policies/server_policies : set_fact] *****
skipping: [UCS-PBST-C-C220M4-1]

TASK [policies/server_policies : Update Server Profiles used by COS-NTP Server Policy (change may always be
reported)] ***
skipping: [UCS-PBST-C-C220M4-1]

PLAY RECAP *****
UCS-PBST-C-C220M4-1      : ok=2    changed=1    unreachable=0    failed=0    skipped=2    rescued=0    ignored=0
UCS-PBST-C-C220M4-2      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-3      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-4      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```


Intersight GUI 結果画面



名前	Platform Type	タイプ	使用状況	最終更新
COS-Boot	UCS Server	Boot Order	0	8分前

Playbook で指定したポリシーが作成される。



ポリシー/プロファイル設定 Playbook - 全体実行

カスタマイズをして実行した

```
$ ansible-playbook -i inventory cos_server_policies_and_profiles.yml
PLAY [Intersight_Servers] *****

TASK [Get Organization default Moid] *****
ok: [UCS-PBST-C-C220M4-2]

TASK [Configure SP-UCS-PBST-C-C220M4-2 Server Profile] *****
ok: [UCS-PBST-C-C220M4-2]

TASK [policies/server_policies : Configure COS-Boot Server Policy] *****
ok: [UCS-PBST-C-C220M4-2]

TASK [policies/server_policies : set_fact] *****
ok: [UCS-PBST-C-C220M4-2]

TASK [policies/server_policies : Update Server Profiles used by COS-Boot Server Policy (change may always be reported)] ***
changed: [UCS-PBST-C-C220M4-2]

TASK [policies/server_policies : Configure COS-NTP Server Policy] *****
ok: [UCS-PBST-C-C220M4-2]
(...snip)

PLAY RECAP *****
UCS-PBST-C-C220M4-2      : ok=16   changed=4   unreachable=0   failed=0   skipped=0   rescued=0   ignored=0
```

Intersight GUI 結果画面

設定 > プロファイル

HyperFlexクラスタプロフィール サーバプロフィール [サーバプロフィールの作成](#)

名前	ステータス	Target Platform	サーバ	最終更新
SP-UCS-PBST-C-C220M4-2	Not Deployed	UCS Server (Standalone)	UCS-PBST-C-C220M4-2	数秒前

All Compute Management Network Storage

NTP COS-NTP

ブート順序 COS-Boot

作成したプロファイルをサーバに展開する

- Playbook “deploy_server_profiles.yml” を利用してサーバにプロファイルを展開する。

```
$ ansible-playbook -i inventory deploy_server_profiles.yml
PLAY [Intersight_Servers] *****

TASK [Deploy (or user defined action) Server Profile] *****
changed: [UCS-PBST-C-C220M4-2]

PLAY RECAP *****
UCS-PBST-C-C220M4-2      : ok=1    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Intersight GUI 結果画面

リクエスト > サーバプロファイルのDeploy

6 3

Saki Aizono

カテゴリ	詳細	実行フロー
モニタ	詳細	
運用	ステータス 成功	
サーバ	名前: サーバプロファイルのDeploy	成功 ブート順序ポリシーの展開 Completed 2020年12月13日 23:13
シャーシ	ID: 5fd6215f696f6e2d30b151d8	成功 NTPポリシーの展開 Completed 2020年12月13日 23:13
ファブリックインターコネク	ターゲットタイプ: ラックサーバ	
HyperFlexクラス	ターゲット名: UCS-PBST-C-C220M4-2	成功 ブート順序ポリシーの検証 Completed 2020年12月13日 23:12
設定	送信元: SP-UCS-PBST-C-C220M4-2 (サーバ...	
オーケストレーション	イニシエータ: sanomura@cisco.com	成功 NTPポリシーの検証 Completed 2020年12月13日 23:12
プロファイル	開始時刻: 2020年12月13日 23:12	
ポリシー	終了時刻: 2020年12月13日 23:13	
最適化	期間: 58 s	
管理	構成: default	

その他の Intersight + Ansible 運用例

Scenario :

2. サーバの HCL - Hardware Compatibility List 情報の取得
3. Intersight へのデバイスの登録 (参考情報リンク)
4. HyperFlex の構築 (参考情報リンク)

Scenario 2 : サーバの HCL 情報の取得

- Ansible Playbook “hcl_status.yml” により、各サーバの HCL リストを取得する。
- 取得した情報は csv 形式でローカルに保存する。

Playbook "hcl_status.yml" タスク内容

tasks:

```
# Get HclStatus
- name: Get HCL Status for Server
  intersight_rest_api:
    <<: *api_info
    resource_path: /cond/HclStatuses
    query_params:
      $filter: "ManagedObject.Moid eq '{{ server_moid }}'"
  delegate_to: localhost
  register: hcl_resp
  when:
    - server_moid is defined
# Create .csv file with version and status information
- copy:
  content: |
    Name, FW version, OS vendor, OS version, HW status, SW status, Overall Status
    {% for host in hostvars %}
      {% set vars = hostvars[host|string] %}
      {% if vars.hcl_resp.api_response is defined %}
        {{ vars.inventory_hostname }}, {{ vars.hcl_resp.api_response.HclFirmwareVersion }}, {{ vars.hcl_resp.api_response.HclOsVendor
}}, {{ vars.hcl_resp.api_response.HclOsVersion }}, {{ vars.hcl_resp.api_response.HardwareStatus }}, {{
vars.hcl_resp.api_response.SoftwareStatus }}, {{ vars.hcl_resp.api_response.Status }} {{ vars.hcl_resp.api_response.ServerReason }}
      {% endif %}
    {% endfor %}
  dest: /tmp/hcl_status.csv
  backup: false
  run_once: true
  delegate_to: localhost
```

← HCL ステータスを取得するタスク

← .csv ファイルを作成するタスク

Playbook "hcl_status.yml" の実行と結果

- Playbook の実行

```
$ ansible-playbook -i inventory hcl_status.yml
PLAY [Intersight_Servers] *****

TASK [Get HCL Status for Server] *****
ok: [UCS-PBST-C-C220M4-3]
ok: [UCS-PBST-C-C220M4-1]
ok: [UCS-PBST-C-C220M4-2]
ok: [UCS-PBST-C-C220M4-4]

TASK [copy] *****
ok: [UCS-PBST-C-C220M4-1]

PLAY RECAP *****
UCS-PBST-C-C220M4-1      : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-2      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-3      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-4      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Playbook "hcl_status.yml" の実行と結果

- Playbook の実行

```
$ ansible-playbook -i inventory hcl_status.yml
PLAY [Intersight_Servers] *****

TASK [Get HCL Status for Server] *****
ok: [UCS-PBST-C-C220M4-3]
ok: [UCS-PBST-C-C220M4-1]
ok: [UCS-PBST-C-C220M4-2]
ok: [UCS-PBST-C-C220M4-4]

TASK [copy] *****
ok: [UCS-PBST-C-C220M4-1]

PLAY RECAP *****
UCS-PBST-C-C220M4-1      : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-2      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-3      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
UCS-PBST-C-C220M4-4      : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

作成された .csv ファイル内容

- “hcl_status.csv” ファイルが作成される。

hcl_status

Name	FW version	OS vendor	OS version	HW status	SW status	Overall Status
UCS-PBST-C-C220M4-1	4.0(2)	VMware	ESXi 6.5 U1	Validated	Validated	Not-Listed Incompatible-Components
UCS-PBST-C-C220M4-2	4.0(1)	VMware	ESXi 6.5 U1	Validated	Validated	Not-Listed Incompatible-Components
UCS-PBST-C-C220M4-3	4.0(2)	VMware	ESXi 6.5 U1	Validated	Validated	Not-Listed Incompatible-Components
UCS-PBST-C-C220M4-4	4.0(1)			Validated	Incomplete	Incomplete Missing-Os-Driver-Info

Scenario 3 : Intersight へのデバイス登録

- Python もしくは Ansible によりデバイススクレームプロセスの自動化が可能
- スクリプトにより、デバイスにアクセスし、デバイス情報と要求コードを自動で取得
- [Video demo of automated device claim](#)

Automated Intersight Device Claim

Cisco Intersight

2700 VIEWS 5 HELPFUL 0 COMMENTS



dsoper

02-17-2018 12:35 PM
Edited On: 03-01-2019 06:07 AM

Cisco Intersight Automated Device Claim and API Usage

This document provides an overview of automated UCS and HyperFlex device claim using the Cisco Intersight API and Python SDK. See the [Intersight API Overview](#) for more information on the Intersight API and how to use API keys for automation with Python and other scripting or programming languages. For general information on Intersight, visit [Cisco Intersight - Cisco](#)

Scenario 4 : HyperFlex の構築

- Intersight API を利用して、HyperFlex のポリシー/プロファイル作成およびクラスタの展開実施可能
- Intersight Ansible モジュールを利用
- 並行して複数のクラスタをインストール可能
- [Video demo of HX automation](#)

Intersight Automated HyperFlex Deployment with Ansible

Cisco Intersight

575 VIEWS 5 HELPFUL 0 COMMENTS



06-07-2018 12:33 PM
Edited On: 03-01-2019 06:08 AM

Intersight Ansible Overview and HyperFlex Deployment Examples

This document provides an overview of the Cisco Intersight Ansible modules which include a complete example of automating HyperFlex cluster deployment. For general information on Intersight, visit [Cisco Intersight - Cisco](#)

Connected TAC

Connected TAC

これまで手動で実施していたプロセスを自動化し、
問題切り分け・障害解析を加速化

Tech Support ファイルを自動で
Cisco® Technical Assistance Center
(TAC) に送信

Cisco TAC と
連携



将来: テレメトリ収集, 問題事象
の証跡, プロアクティブな警告出
力や対処

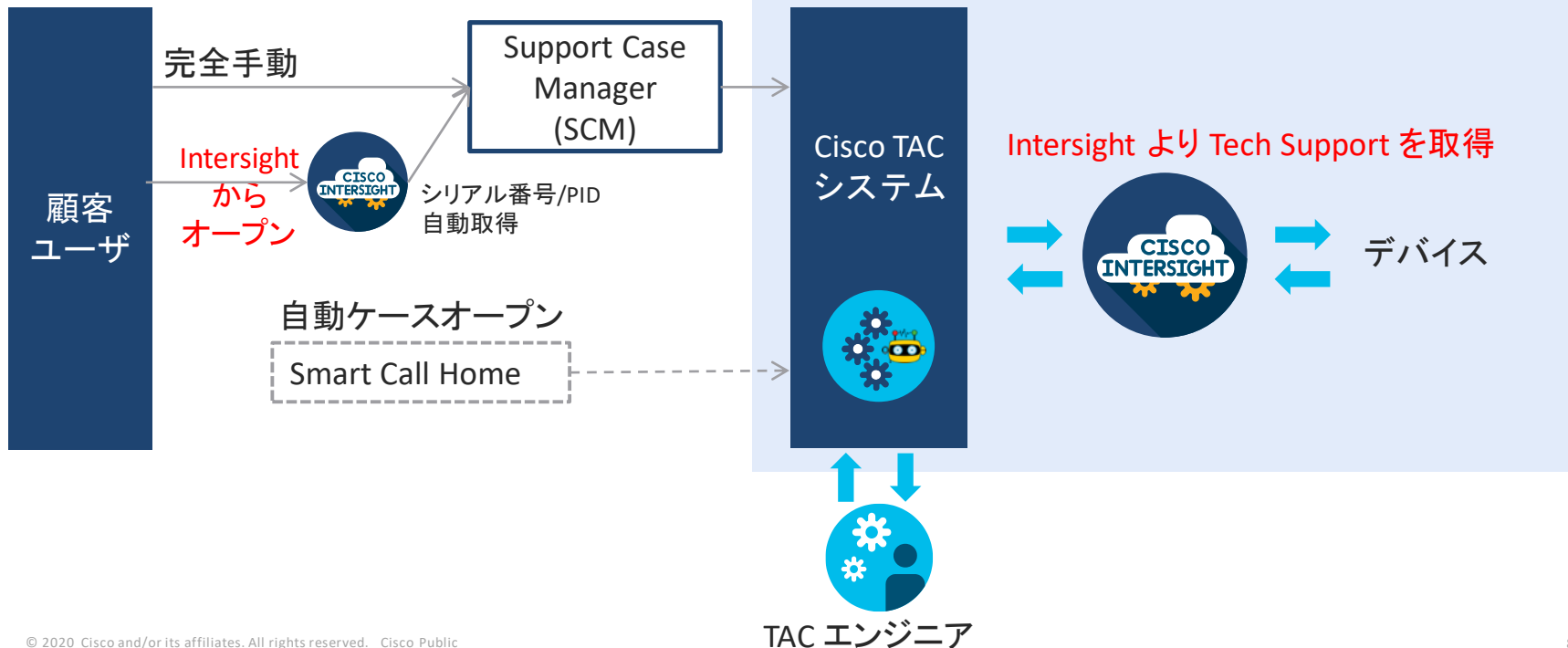


Connected TAC の仕組み

<シリアル番号から Intersight 登録がある場合>

① ケースオープン (手動 or 自動)

② Tech Support ファイルを取得



① Intersight からの TAC ケースオープン

該当デバイスのアクションから「TAC ケースを開く」を選択

- サーバ
- ファブリックインターコネク

<input type="checkbox"/>	名前	ヘルス	管理IP	モデル	
<input type="checkbox"/>	esxi-aci-13.dcv.svpod	● Healthy	10.1.64.74	UCSC-C220-M5SX	...
<input type="checkbox"/>	esxi-aci-10.dcv.svpod	● Healthy	10.1.64.71	UCSC-C220-M5SX	KVMの起動
<input type="checkbox"/>	esxi-aci-11.dcv.svpod	● Healthy	10.1.64.72	UCSC-C220-M5SX	TACケースを開く
<input type="checkbox"/>	esxi-aci-12.dcv.svpod	● Healthy	10.1.64.73	UCSC-C220-M5SX	Cisco IMCの起動



Support Case Manager (SCM) が開かれ、シリアル番号などが自動的に入力される

シリアル番号等を自動的に取得「続ける」を選択

② Intersight からの Tech Support ファイル取得

シリアル番号から Intersight 登録を判断登録があれば、Tech Support を取得



- Tech Support を取得・閲覧できるのは TAC ケースに関する Cisco エンジニアのみ (顧客、パートナーの実施は不可)
- Tech Support 取得は顧客に通知されない

デバイス種別	取得する Tech Support 種別
B-Series Motherboard	Chassis Tech Support
B-Series VIC/Adapter	Chassis Tech Support
IOM	Chassis Tech Support
Chassis	Chassis Tech Support
Fabric Interconnect	UCSM Tech Support
C-Series Motherboard	CIMC Tech Support
C-Series VIC/Adapter	CIMC Tech Support
FEX	FEX Tech Support

Connected TAC の効果 (顧客視点)

実際の TAC ケースの例



TAC ケースオープン:
XXXXXX244



Tech Support ファイルを
自動的に収集



分析結果を
自動的に生成



既知不具合に一致しており、ファームウェアアップグレードとの見解を提供

2018-12-DD 01:25



12 分後



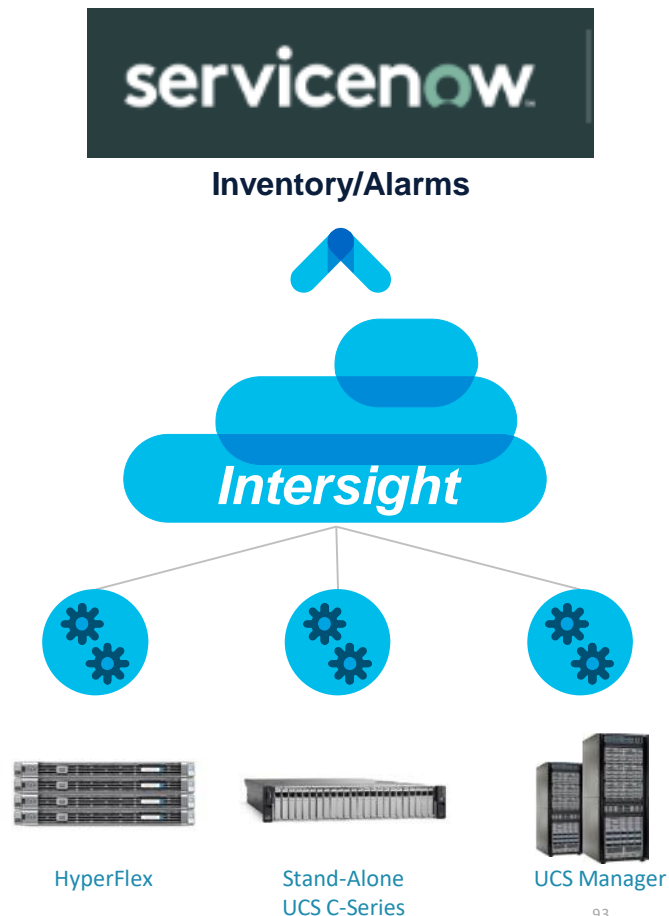
16 分後

問題を診断するまでに要した時間:
合計 28 分

ServiceNow 連携

Intersight - ServiceNow 連携

- ServiceNow プラグインを提供
 - Cisco Intersight ITSM Plugin
- Read-Only の API アクセスで連携可能
- プラグインの機能
 - デバイスインベントリ情報の同期
 - インシデント管理
 - Intersight から取得したアラーム情報を利用
 - ServiceNow による分析レポートとダッシュボード
- Intersight Essentials ライセンス以上が必要



Cisco Intersight ITSM Plugin

https://store.servicenow.com/sn_appstore_store.do#!/store/application/baef2ff5db132300d7b59235ca9619e3



Cisco Intersight ITSM Plugin

Visibility and monitoring for Cisco UCS and HyperFlex.

Cisco Systems Inc

Compatibility: Paris, Orlando | Other App Versions

Pricing
Free

now

Certified App

Get

Contact Seller →

プラグインの入手

Type

Integration

Version

1.3.0

[Other App Versions](#)

Dependencies and Licensing

[View Dependencies and Licensing Requirements](#)

Compatibility

Paris

Orlando

Supporting Links and Docs

[ServiceNow Store Terms Of Use](#)

[Vendor App Subscription Terms and Conditions](#)

[Installation Guide](#)

ドキュメントの入手

[Cisco Intersight](#)

ServiceNow 互換性

☆☆☆☆ No Reviews

Share With

Product Details

Ratings and Reviews

Summary

Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure management platform that is augmented by other intelligent systems. It provides global management of the Cisco Unified Computing System™ (Cisco UCS®) and Cisco HyperFlex® hyperconverged infrastructure anywhere. Intersight provides a holistic approach to managing distributed computing environments from the core to the edge. The Cisco Intersight virtual appliance provides customers with deployment options while still



Cisco Intersight ITSM Plugin リリース

- 1.0.1 : NewYork

- 1.2.0 : Orlando

- 1.3.0 : Paris, Orlando

本日のデモは Paris の developer instance を利用

Cisco Intersight ITSM Plugin インストール手順

1. Performance Analytics and Reporting Plugin のアクティベート
 - Cisco Intersight ITSM Plugin は、ダッシュボードウィジェットを表示するために Performance Analytics and Reporting plugin を利用
2. (Intersight Virtual Appliance 利用の場合) MID サーバの設定
3. Cisco Intersight ITSM Plugin のインストール

Cisco Intersight ITSM Plugin 設定

servicenow Service Management

System Administrator

Intersight Authentication
Intersight - FlashStack

Save & Import Delete

Cisco Intersight

Cisco Intersight Portal

Configuration

Intersight Configuration

Inventory Sync

Servers

HyperFlex Clusters

Fabric Interconnects

Scheduled Jobs

Import Queue

Support

Contact Support

Logs

CISCO

Name Intersight - FlashStack

Hostname intersight.com

URL <https://intersight.com/>

API Key ID

Secret Key

On-Premises

Intersight から取得した API キー ID および秘密鍵情報を入力 (Read-Only)

Intersight Virtual Appliance の場合は、MID サーバの設定

Incidents Others

Incident Assignment Group Application Development

Incident Caller Name Saki Aizono

Alarm Severity Critical, Warning, Info

Advanced

Save & Import Delete

ServiceNow 連携サービスメニュー

The screenshot displays the ServiceNow System Administration dashboard. The top navigation bar includes the ServiceNow logo, the text "Service Management", and the user profile "System Administrator". A search bar contains "intersight", and a dropdown menu shows "System Administration" with an "Open Dashboard Version" button. The main content area is titled "System Administration" and features a grid of management tiles:

- Guided Setup**: Guided Setup tools to help you set up ServiceNow.
- System Security**: Configure and monitor Instance security settings.
- Business Logic**: Manage workflow and behavior of applications.
- Create and Deploy**: Create, modify and deploy applications to your instances.
- Data Management**: Manage the way data is stored and displayed.
- Diagnostics**: Performance, development and debugging tools.
- Email**: Customize behavior of inbound and outbound email.
- Homepages**: Configure homepages for Service Desk and Self Service users.
- Integration**: Integrate with 3rd-party systems and data sources.
- Reporting and Analytics**: Create visual representations of your data.
- User Administration**: Manage users, groups and their roles.
- User Interface**: Control the look and feel of applications.

The left sidebar contains a navigation menu with categories: Configuration, Inventory Sync, Servers, HyperFlex Clusters, Fabric Interconnects, Scheduled Jobs, Import Queue, Support, Contact Support, and Logs. The "Cisco Intersight Portal" link is highlighted with a red box.

Cisco Intersight ITSM Plugin ダッシュボード

CISCO Intersight ITSM Plugin

Dashboard

System Administrator

Dashboard

Alarms

Incidents

Servers

HyperFlex Clusters

Fabric Interconnects

Support

Incidents Open Older than 30 Days

0

Incidents Opened Today

19

Critical Open Incidents

903

Incidents Not Updated for 7 Days

0

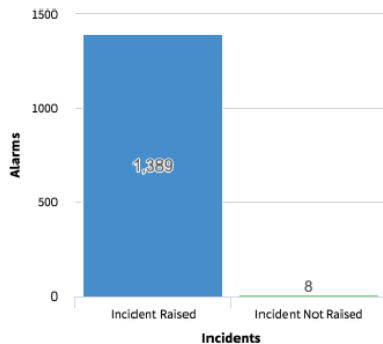
Total Open Incidents

1,389

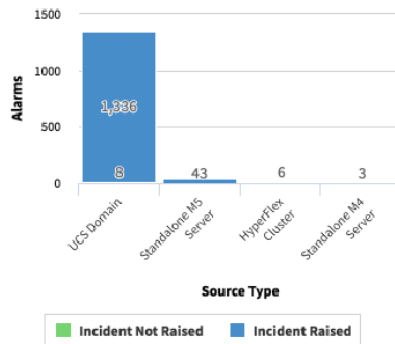
Overdue Incidents

0

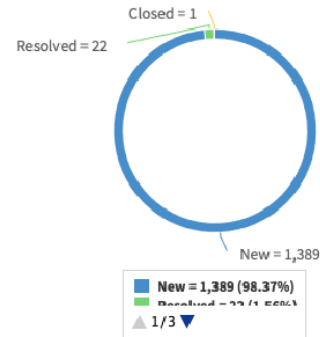
Alarms vs Incidents



Incident Raised by Source Type



Incident States



Cisco Intersight ITSM Plugin アラーム情報

Severity	Code	Source Type	Source Name	Component	Message	Incident	Date/Time
Warning	F1454	UCS Domain	CC7UCS-13	org-root/ls-demo1231/iface-in-band	Vlan 'KVM-817' resolved to unsupporte...	INC0011081	Wed, 17 J
Critical	F0436	UCS Domain	D23-UCS1	org-root/fw-host-pack-3.2.2c/pack-imag...	board-controller image with vendor Cisc...	INC0010324	Wed, 26 S
Critical	F0283	UCS Domain	CC7UCS1	sys/chassis-1/blade-6/fabric-B/path-1/v...	ether VIF 2595 on server 1 / 6 of switch...	INC0011384	Tue, 06 A
Critical	F0436	UCS Domain	D23-UCS1	org-root/fw-host-pack-3.2.2c/pack-imag...	storage-controller image with vendor LS...	INC0010343	Wed, 26 S
Critical	F0479	UCS Domain	CC7UCS1	sys/chassis-1/blade-2/adaptor-1/host-et...	Virtual interface 2610 link state is down	INC0011320	Tue, 06 A
Critical	F0283	UCS Domain	HX29	sys/rack-unit-3/fabric-B/path-1/vc-2891	ether VIF 2891 on server 3 of switch B ...	INC0010570	Thu, 02 M
Critical	F0283	UCS Domain	HX29	sys/chassis-1/blade-8/fabric-A/path-1/v...	ether VIF 2999 on server 1 / 8 of switch...	INC0010651	Wed, 08 M
Critical	F0436	UCS Domain	SAM-QA-108	org-root/org-HX/fw-host-pack-HyperFle...	board-controller image with vendor Cisc...	INC0010866	Tue, 30 A
Critical	F0436	UCS Domain	D23-UCS1	org-root/fw-host-pack-M4Servers/pack-i...	adaptor image with vendor Cisco Syste...	INC0010209	Wed, 26 S
Critical	F0207	UCS Domain	CC7UCS1	sys/chassis-1/blade-1/adaptor-1/host-fo-1	Adaptor for host interface 1/1/1/1 link sta	INC0011119	Fri, 02 A

Cisco Intersight ITSM Plugin インベントリ情報一覧

Intersight ITSM Plugin Servers System Administrator

All

Name	Health	Management IP	Model number	CPU Capacity (GHz)	Memory Capacity (GB)	Firmware
UCSPE-172-28-224-52-1	Healthy ✓	172.28.224.52	UCSC-C220-M4S	9.6	48	3.1(1e)
savbu-qa-modoc-1-bmc	Critical ✗	10.193.197.191	UCSC-C480-M5ML	76.8	192	4.0(4b)
HX29-6	Warning ⚠	10.193.151.180	UCSC-C220-M5SX	20.4	32	4.0(4b)
UCSPE-172-28-224-52-9	Healthy ✓	172.28.224.52	UCSC-C480-M5	20.0	48	3.1(1e)
C220-WZP22040938	Critical ✗	172.28.224.105	HXAF220C-M5SX	44.0	192	3.1(2d)
C220-WZP2231029T	Critical ✗	10.105.219.52	UCSC-C220-M5SX	20.4	64	4.0(4b)
UCSPE-172-28-224-52-13	Healthy ✓	172.28.224.52	UCSC-C220-M5SN	20.0	48	3.1(1e)
CC7UCS-13-1-7	Critical ✗	172.28.225.20	UCSB-B200-M4	52.8	256	4.1(28a)
UCSPE-172-28-224-44-3-1	Healthy ✓	172.28.224.44	UCSB-EX-M4-1	25.0	48	3.1(1e)
UCSPE-172-28-224-44-1	Healthy ✓	172.28.224.44	UCSC-C125	4.6	48	3.1(1e)

Cisco Intersight ITSM Plugin インベントリ情報詳細

The screenshot displays the Cisco Intersight ITSM Plugin interface. The top navigation bar shows 'Servers > C220-WZP22040938' and the user 'System Administrator'. The left sidebar contains navigation options: Dashboard, Alarms, Incidents, Servers (selected), HyperFlex Clusters, Fabric Interconnects, and Support.

The main content area is divided into three panels:

- Details:** A table listing server information.

Name	C220-WZP22040938
Health	Critical ✖
User Label	-
Management IP Address	172.28.224.105
Serial	WZP22040938
PID	HXAF220C-M5SX
Vendor	Cisco Systems Inc
Revision	-
Asset Tag	Unknown
Firmware Version	3.1(2d)
- Properties:** A table listing hardware and system properties.

Power	ON
CPU's	2
Threads	40
CPU Cores	20
CPU Cores Enabled	20
Memory Capacity(GB)	192 GB
CPU Capacity	44.0 GHz
ID	1
Adapters	1
NIC Interfaces	2
HBA Interfaces	2
UUID	D81A3DBE-30B8-49F5-955A-0355616CAC23
- Most Recent Incidents & Alarms:** A section with tabs for 'Incidents' and 'Alarms'. A dropdown menu is set to 'All'. An incident is listed: 'INC0010008' with a 'New' status. The alarm message is: 'Intersight Alarm: PS_RDNDNT_MODE: Power Supply redundancy is lost: Rese...'

アラーム、インベントリインポートジョブ

The screenshot displays the Cisco Intersight interface for managing Scheduled Script Executions. The main content area shows a table with the following data:

	Name	Active	Class	Updated
<input type="checkbox"/>	DeleteProcessQueueData	true	Scheduled Script Execution	2019-05-30 04:09:19
<input checked="" type="checkbox"/>	ImportAlarms	true	Scheduled Script Execution	2019-08-22 05:07:07
<input type="checkbox"/>	ImportInventory	true	Scheduled Script Execution	2019-04-11 05:16:54

The left sidebar contains the following navigation items:

- Intersight
- Cisco Intersight Portal
- Configuration
 - Intersight Configuration
- Inventory Sync
 - Servers
 - HyperFlex Clusters
 - Fabric Interconnects
 - Scheduled Jobs
 - Import Queue
- Support
 - Contact Support
- Logs
 - Logs

Intersight アラームのインポート (実行間隔の設定)

The screenshot displays the ServiceNow interface for configuring a Scheduled Script Execution. The top navigation bar shows 'Service Management' and 'Cisco Intersight'. The left sidebar contains a navigation menu with 'Intersight' selected. The main content area is titled 'Scheduled Script Execution ImportAlarms' and shows the configuration for a script named 'Intersight のスコープで実施'.

Key configuration details:

- Name:** Daily, Weekly, Monthly
- Active:** Periodically (highlighted with a red box)
- Run:** On Demand
- Application:** Cisco Intersight ITSM Plugin
- Conditional:** Checked
- Condition:** `gs.getProperty('x_caci_cisco_inter.start.import') == 'true'`
- Run this script:**

```
1 var snLogger = new Cisco_SNLogger();
2 var appUtil = new Cisco_AppUtil();
3 try{
4     snLogger.debug('Inside Cisco_ImportAlarms Schedule Job for running it periodically.');
```


インシデント管理

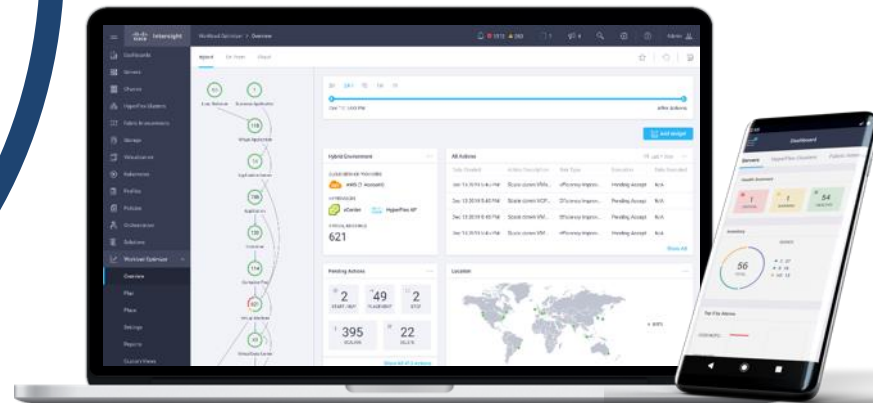
The screenshot displays the ServiceNow interface for incident management. The top navigation bar includes the ServiceNow logo, the user name 'System Administrator', and various utility icons. The main content area is titled 'Incidents [Self Service view]' and features a search bar and a dropdown menu set to 'Opened'. A filter is applied: 'All > Caller = plugin user > Active = true'. The incident list is sorted by 'Number' and 'Opened' date. The first incident, INC0011416, is highlighted with a red box. The list contains several Intersight alarm entries with their respective dates, times, and descriptions.

	Number	Opened	Short description
<input type="checkbox"/>	INC0011416	2019-08-22 05:01:47	Intersight Alarm: storage-controller image with vendor LSI Logic Symbios Logic, model SAS1064E PCI-Express Fusion-MPT SAS and version 01.32.09.00 06.34.00.00
<input type="checkbox"/>	INC0011415	2019-08-22 05:01:47	Intersight Alarm: psu image with vendor Cisco Systems Inc, model UCSB-PSU-2500ACDV-ECD15020029 and version 03.00.00 is deleted
<input type="checkbox"/>	INC0011414	2019-08-22 05:01:44	Intersight Alarm: Server 1/4 (service profile: org-root/lis-DEE-Ctrl-05) vmedia mapping esx-6-5-1 has failed.
<input type="checkbox"/>	INC0011412	2019-08-22 04:47:20	Intersight Alarm: Server 1/1 (service profile: org-root/lis-Server127febtest) vmedia mapping KS has failed.
<input type="checkbox"/>	INC0011413	2019-08-22 04:47:20	Intersight Alarm: Server 1/1 (service profile: org-root/lis-Server127febtest) vmedia mapping CentOS7 has failed.
<input type="checkbox"/>	INC0011411	2019-08-22 04:47:19	Intersight Alarm: Server 1/7 (service profile: org-root/lis-esx-6-5-0-2-ip-224) vmedia mapping esx-sp-nfs has failed.
<input type="checkbox"/>	INC0011410	2019-08-22 04:47:18	Intersight Alarm: Server 1/2 (service profile: org-root/lis-OCP-Master-01) vmedia mapping RHEL74 has failed.
<input type="checkbox"/>	INC0011409	2019-08-22 04:47:17	Intersight Alarm: Server 1/3 (service profile: org-root/lis-OCP-Infra-02) vmedia mapping RHEL74 has failed.

Intersight Workload Optimizer (IWO)

Cisco Intersight の開発コンセプトの拡大

クラウド運用モデル



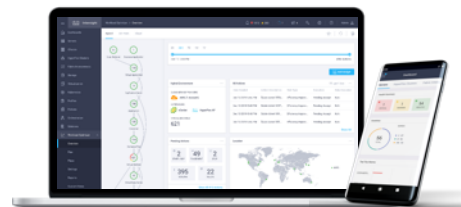
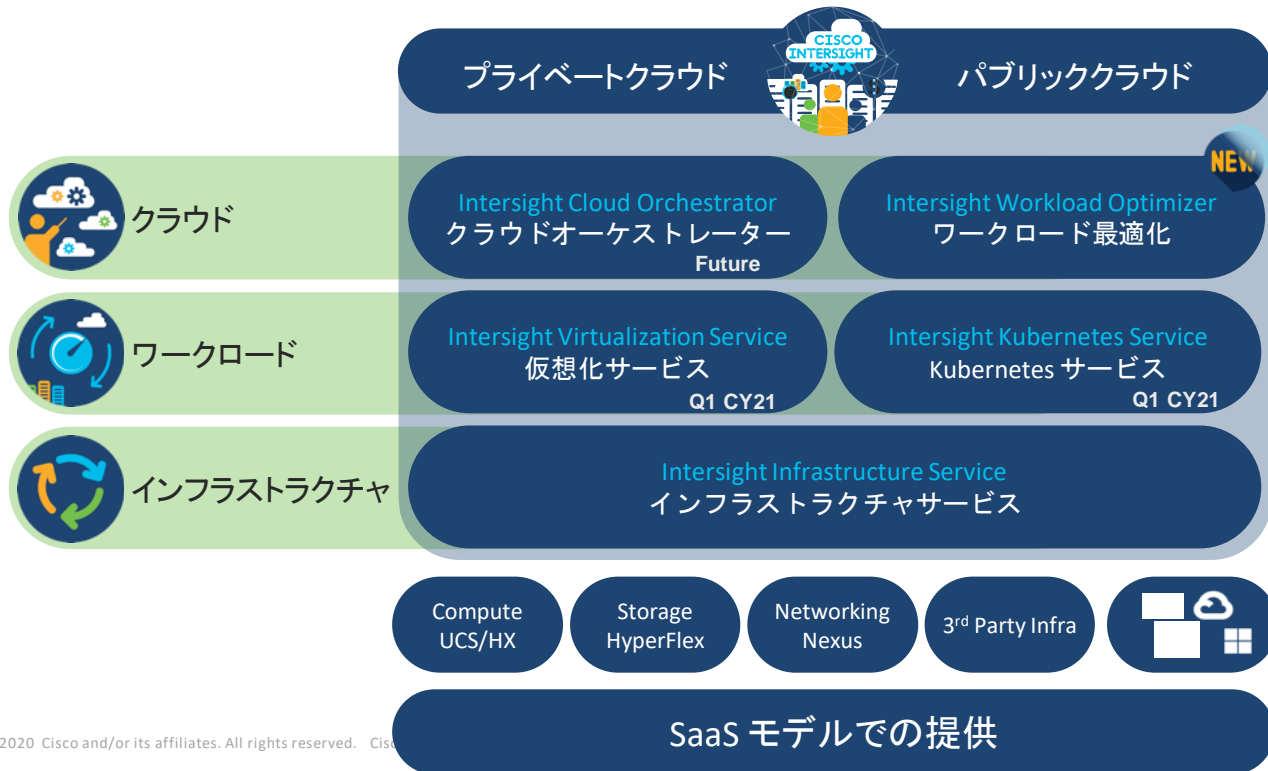
シンプルな運用

継続的な最適化

アジャイルによる提供

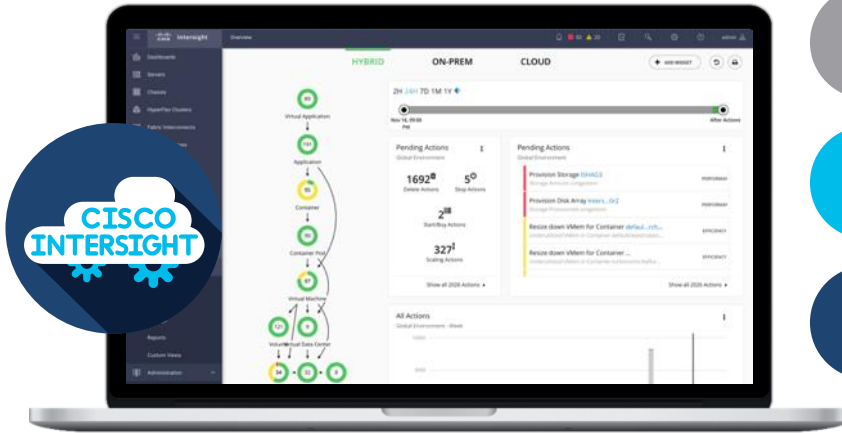
Cisco Intersight の機能モジュール

インフラストラクチャサービスに加えて、ワークロード、クラウドにも機能を拡張





Intersight Workload Optimizer (IWO)



ハイブリッドクラウド環境を完全に視覚化
アプリケーションとインフラの依存関係をマッピング

リソースの需要と供給をリアルタイムに分析
パフォーマンス、コスト、コンプライアンス

具体的なアクションを推奨
様々なターゲットタイプに対し、アクションをトリガー



マシンインテリジェンスを用いた
アプリケーションリソース管理の簡素化

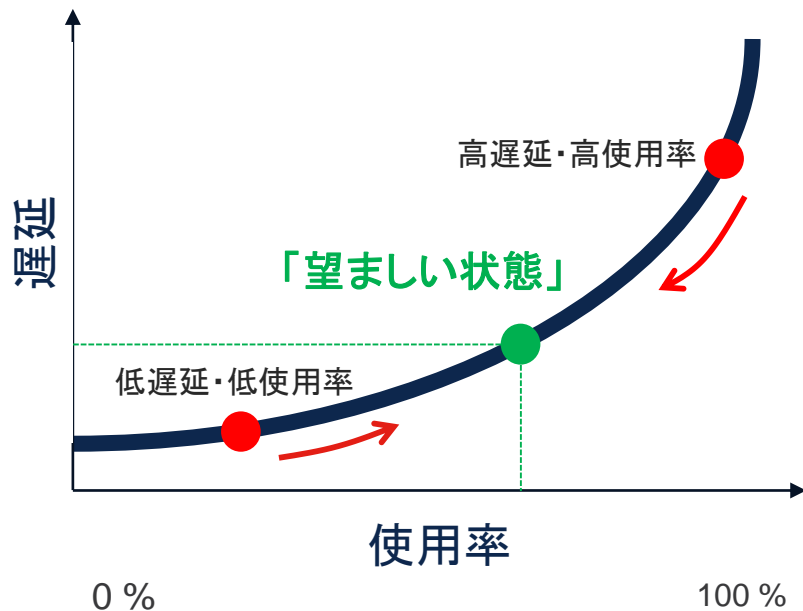


オーバプロビジョニングを排する
ことによる投資保護と運用費の削減



アクション実行の即時性とキャパシテ計画
のシナリオモデル化によるリスク低減

IWO が定義するリソースの「望ましい状態」



- ・ 低遅延・低使用率=リソースの非効率的な使用状態、リソース過多
 - リソース利用率の最適化
- ・ 高遅延・高使用率=パフォーマンスが確保出来ない状態、リソース不足
 - パフォーマンスの最適化

「望ましい状態」とは、インフラを効率的に利用しながらパフォーマンスを確保している状態

IWOは「望ましい状態」に向かって運転する

パフォーマンスの保証

リソースを最も必要とするワークロードに自動的にリソースを割り当てることでパフォーマンスを最適化する

コンプライアンスの確保

ポリシーを常に遵守しながら、自動的にワークロードを配置、サイジング、移行する



コストの削減

ワークロード密度とリソース使用率を自動的に最大化し、インフラストラクチャ/クラウドコストを最小限に抑える

常時バランスをとりながら同時に解決する

1. パフォーマンスの向上
2. コンプライアンスの向上
3. コストの削減

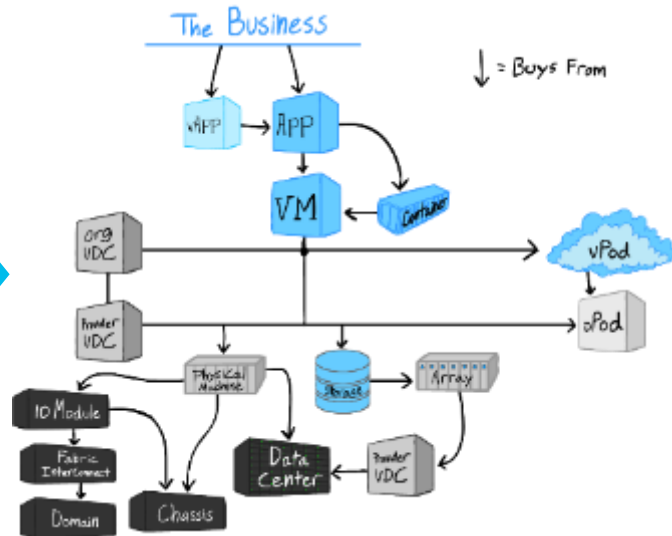
DC 内のフルスタックのリソース関係を把握

登録ターゲット
(管理ソフトウェア)

- APPLICATION PERFORMANCE MANAGEMENT
- PROVISIONING & ORCHESTRATION
- CONFIGURATION & MIGRATION
- CONTAINERS
- APPLICATION SERVERS
- DATABASES
- VIRTUALIZATION
- HYPERCONVERGED
- NETWORK
- STORAGE
- COMPUTE

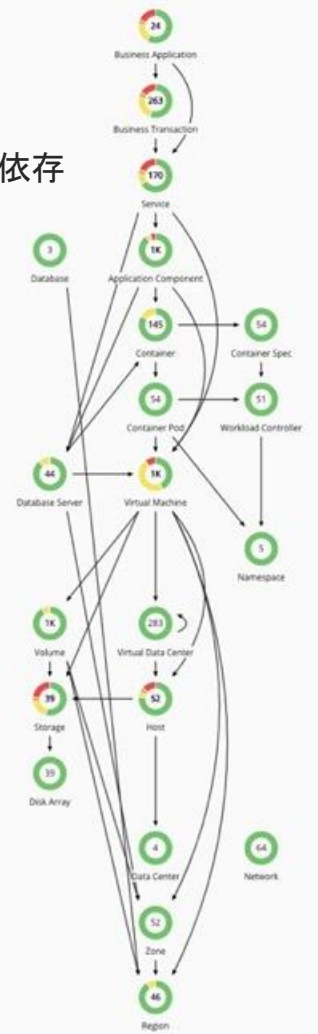


管理ソフトウェアから
情報を収集



1時間以内でリソース依存
関係を GUI に表示
(サプライチェーン)

データ・センター内のすべてを
リソース (CPU、メモリ、IO 等) を売買する
サプライチェーン市場に抽象化



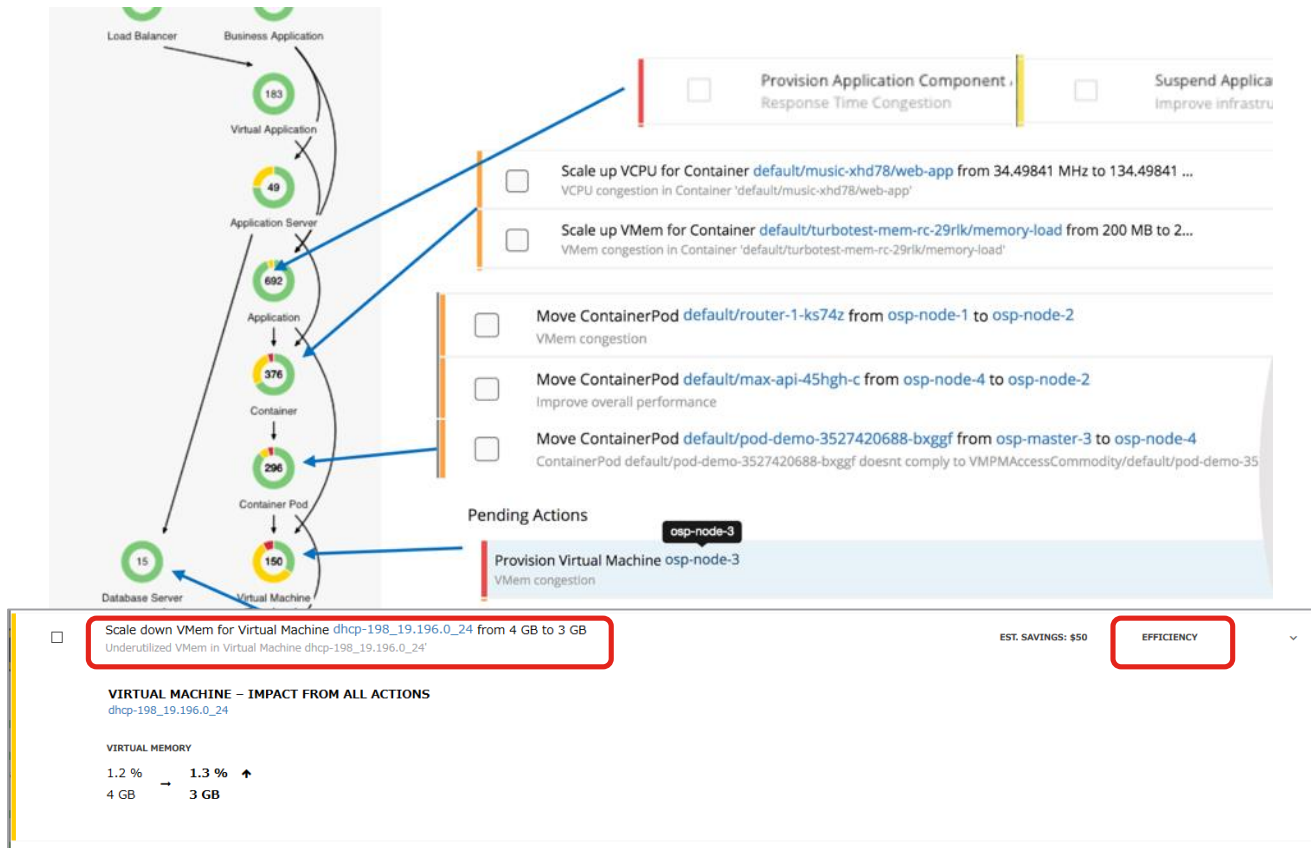
登録可能なターゲット (2020/12/16 現在)

Category	Target Name	Minimum License Tier Required for Intersight Workload Optimizer	Intersight Assist Required
Cloud	Amazon Web Services	Intersight Workload Optimizer Essentials	No
	Amazon Web Services Billing	Intersight Workload Optimizer Essentials	No
	Microsoft Azure Enterprise Agreement	Intersight Workload Optimizer Essentials	No
	Microsoft Azure Service Principal	Intersight Workload Optimizer Essentials	No
Cloud Native	Kubernetes	Intersight Workload Optimizer Advantage	No
Compute / Fabric	Cisco UCS Server (Standalone)	Intersight Workload Optimizer Essentials	No
	Cisco UCS Domain (UCSM Managed)	Intersight Workload Optimizer Essentials	No
Application Performance Management (APM)	Cisco AppDynamics	Intersight Workload Optimizer Advantage	Yes
Hyperconverged	Cisco HyperFlex	Intersight Workload Optimizer Essentials	No
Hypervisor	VMware vCenter	Intersight Workload Optimizer Essentials	Yes
Storage	EMC VMAX	Intersight Workload Optimizer Essentials	Yes
	EMC XtremIO	Intersight Workload Optimizer Essentials	Yes
	EMC ScaleIO	Intersight Workload Optimizer Essentials	Yes
	EMC VPLEX	Intersight Workload Optimizer Essentials	Yes
	NetApp	Intersight Workload Optimizer Essentials	Yes
	Pure Storage FlashArray	Intersight Workload Optimizer Essentials	Yes

- Intersight Assist VM
 - オンプレミスの Third Party 製品を接続する場合に必要
 - Cisco データセンター製品の場合は、デバイスコネクタで直接接続が可能なために不要
 - パブリッククラウドおよび Kubernetes 環境は不要
- GA 後追加ソフトウェアをサポート予定

リアルタイム分析により IWO が提示するアクション

- ・アクションの種類
 - ・リソースの再配置
 - ・リソースの拡張・縮小
 - ・リソースの追加
 - ・リソースの停止・起動
- ・アクションによる効果
 - ・パフォーマンスの最適化
 - ・リソース利用の効率化
 - ・コンプライアンス遵守
- ・アクションの実行
 - ・推奨するのみ
 - ・手動
 - ・自動 (ソフトウェアによる)



参考情報

Cisco Intersight 情報

- Intersight Online Help
<https://intersight.com/help>
- Intersight How To (日本語のシスココミュニティサイト)
<https://community.cisco.com/t5/-/-/ta-p/4072043>

Cisco dCloud デモ環境

- Getting Started with Cisco Intersight v1
<https://dcloud2-rtp.cisco.com/content/instantdemo/getting-started-with-cisco-intersight-v1?returnPathTitleKey=content-view>
- Cisco UCS Management with Intersight v1
<https://dcloud2-rtp.cisco.com/content/demo/467125?returnPathTitleKey=content-view>
- Cisco Intersight Workload Optimizer (Preview) v1
<https://dcloud2-sng.cisco.com/content/instantdemo/cisco-intersight-workload-optimizer-tech-preview-v1?returnPathTitleKey=content-view>

