



Intersight Success Community Webinar

やっぱりSplunkでしょ。 IntersightデータをSplunk連携

シスコシステムズ合同会社

Toshiyuki Jimbo
Customer Success Specialist

2025年3月6日



Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

目次

1. SplunkとIntersightの概要
2. Intersightデータ連携のユースケースとメリット
3. デモ
連携方法とダッシュボードご紹介



音声について

イベントが開始されると自動的に音声流れ始めます。

音声が流れない場合は、画面下の [音声ブロードキャスト] をクリックし、表示された画面から [再生] をクリックしてください。

音声接続に関する詳細はこちらをご参照ください。

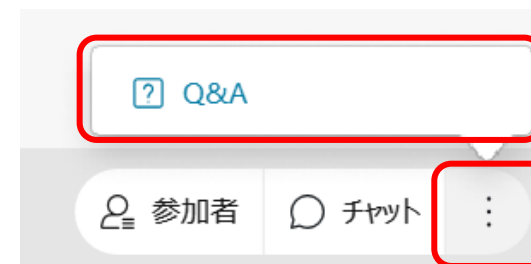
<https://community.cisco.com/t5/-/-/ta-p/3129991>

解決しない場合は、画面右側の Q&A ウィンドウより **[すべてのパネリスト (All Panelist)]** 宛にお知らせください。



ご質問方法

ご質問は、画面右側の Q&A ウィンドウから **[すべてのパネリスト (All Panelist)]** 宛に送信してください。



※ Q&A ウィンドウが画面右側に見つからない場合はここから表示

本日のプレゼンター



Tiffany Guo

カスタマーエクスペリエンス
カスタマーサクセススペシャリスト



Toshiyuki Jimbo

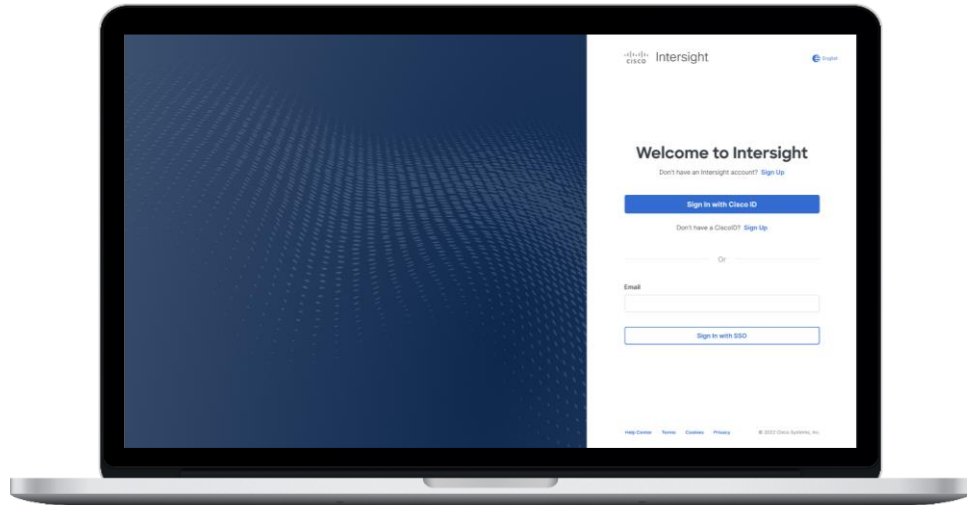
カスタマーエクスペリエンス
カスタマーサクセススペシャリスト

Intersightとは？

クラウドから統合管理する SaaS サービス



CISCO INTERSIGHT



シスコのクラウドオペレーション
プラットフォーム...

ネットワーク、サーバ、ストレージ、
仮想マシンを可視化、運用の自動化

基本的には、SaaSで提供、
(仮想アプライアンス提供も可能)

どこからでも、

**1つのダッシュボードから
全体の運用管理を実現**

Intersightで何が出来る？

クラウドから統合管理する SaaS サービス

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

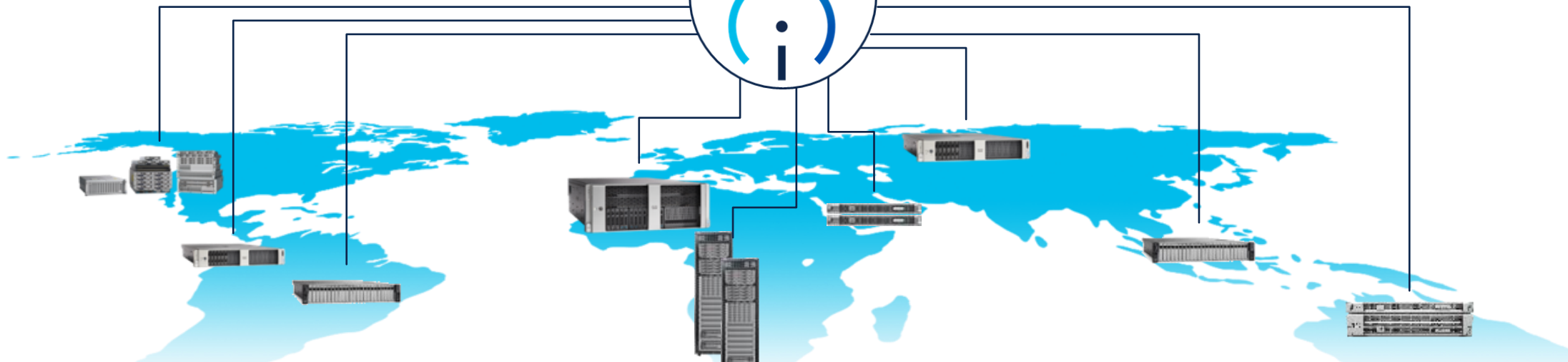


SaaS または
Appliance



SaaS による提供
シンプルなツール

サーバ管理操作
インテリジェンス

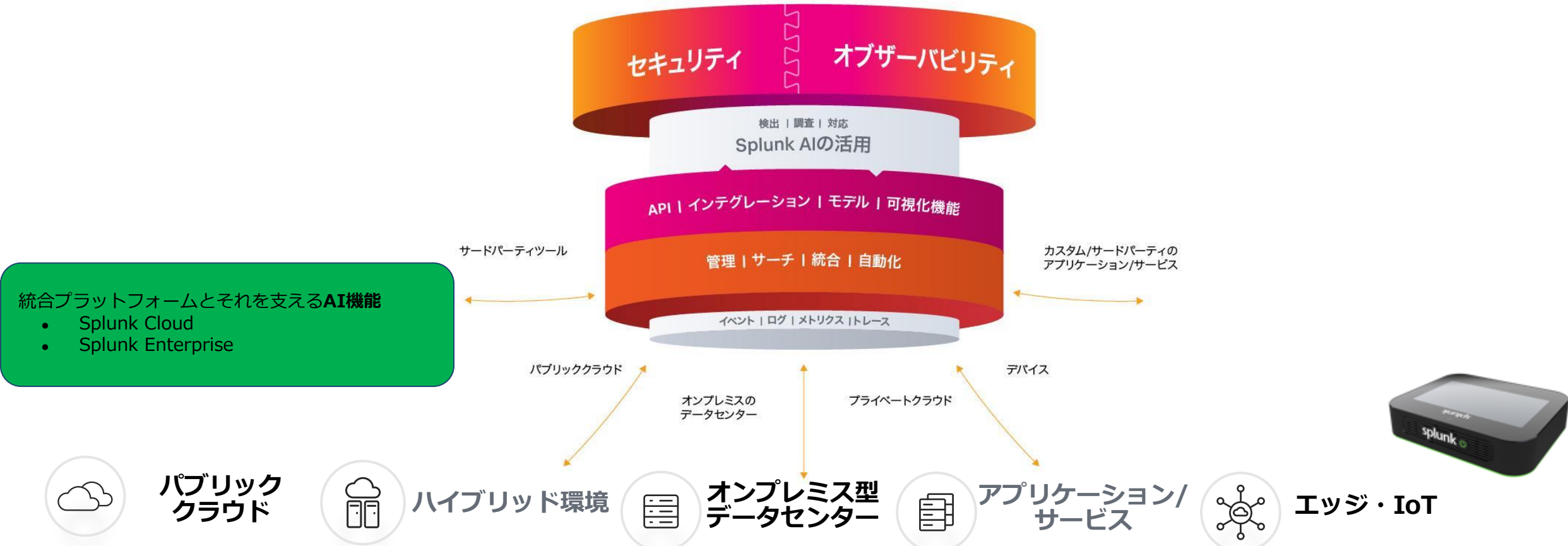


インターネット環境さえあれば、どこからでもアクセス可能

Splunkとは？

セキュリティとオペラビリティ向上のための統合プラットフォーム

- セキュリティとITサービスのデータを集約し、分析・可視化する業務支援を行う
- AI技術（自動化や機械学習）で、予兆や運用効率の向上



統合プラットフォームとそれを支えるAI機能

- Splunk Cloud
- Splunk Enterprise



パブリッククラウド



ハイブリッド環境



オンプレミス型データセンター



アプリケーション/サービス



エッジ・IoT



Splunkで何ができる？

セキュリティとオペラビリティ向上のための統合プラットフォーム

- セキュリティとITサービスのデータを集約し、分析・可視化する業務支援を行う
- AI技術（自動化や機械学習）で、予兆や運用効率の向上

セキュリティ業務をご支援するハットトリック*を達成したセキュリティ製品群

- Enterprise Security (ES)
- SOAR
- UEBA
- Attack Analyzer (フィッシング、マルウェア等)
- Mission Control

* Gartner, IDC, Forrester Wave3社よりリーダー認定

統合プラットフォームとそれを支えるAI機能

- Splunk Cloud
- Splunk Enterprise



ITサービス運用、開発業務をご支援するオペラビリティ製品群 (Gartner, GigaOmにてリーダー評価)

- Observability Cloud / AppDynamics
 - IM : Infrastructure Monitoring (インフラ管理)
 - APM (性能管理)
 - RUM (Real Time User Monitoring)
 - Synthetic (外形監視)
- ITSI : SI for SAP など(機械学習でSAP運用強化)

エコシステム

- 1,800種類を超えるSplunk Baseアプリケーション
- パートナー様



パブリッククラウド



ハイブリッド環境



オンプレミス型データセンター



アプリケーション/サービス



エッジ・IoT

SplunkとIntersight連携 Intersight Add-on

エコシステム
1,800種類を超えるSplunk Base
アプリケーション(Apps)
パートナー様



Welcome to the new Splunkbase! To return to the old Splunkbase, [click here](#).

splunkbase™ Collections Apps [Submit an App](#) [Log In](#)

This app is archived. [Learn more](#)

Cisco Intersight Add-on for Splunk
The Cisco Intersight Add-on for Splunk (TA-intersight-addon) provides a python-based scripted input to retrieve data from Cisco Intersight. SaaS, Connected Virtual Appliance, and Private Virtual Appliance deployments of Intersight are all supported. Data that can be imported from Intersight...
Built by [Karthik Karupasamy](#)

[Login to Download](#) [Share](#) [Alert](#)

Latest Version 1.3.1 August 4, 2022 Release notes	Compatibility Splunk Enterprise Platform Version: 9.3, 9.2, 9.1, 9.0, 8.2, 8.1, 8.0	Rating 5 ★★★★★ (1) Log in to rate this app	Support Not Supported Learn more
--	--	---	---

SplunkとIntersight 連携による可観測性の向上



- Intersight 監査ログ
- Intersight アラーム
- Intersight インベントリ



- ログ保管
- 統計 / 可視化
(ダッシュボード)
- アラート

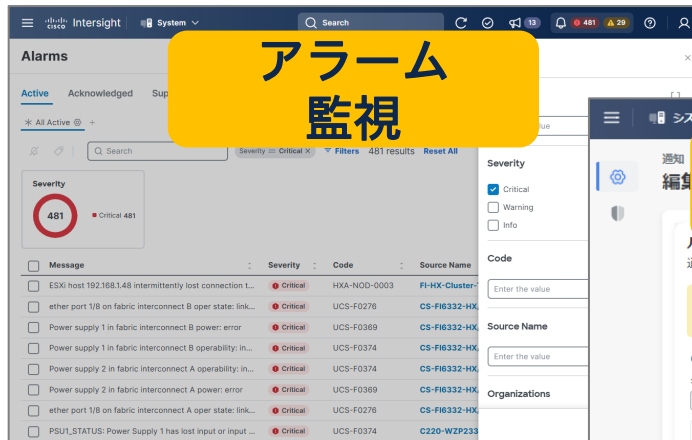


- Intersight でのトラブルシューティングや障害対応の高度化
- Intersight 管理機器の傾向分析とプロアクティブな問題検出
- Intersight の監査ログの可視化と活用

ユースケース1 Intersight でのトラブル シューティング / 障害対応高度化

Intersight でのトラブルシューティング / 障害対応高度化

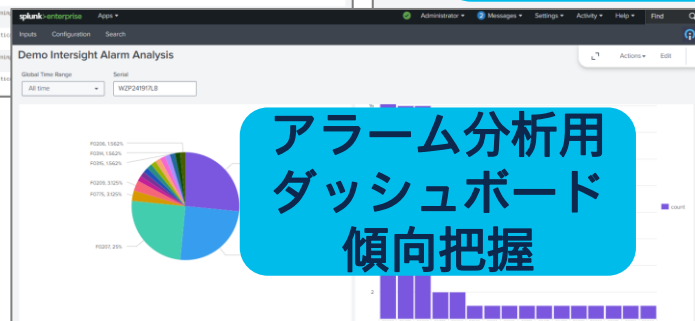
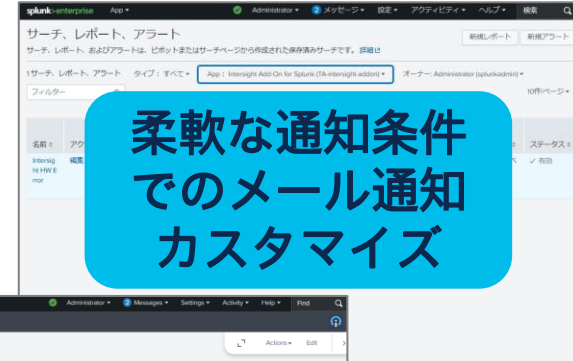
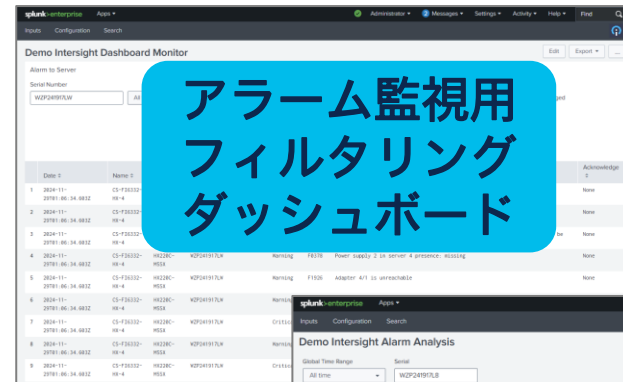
Intersightのアラーム状況を自由なレイアウト & 切り口で可視化・分析・通知



アラーム
監視



管理ポータルで提供される
基本的なモニタリングとメール通知



Intersight管理データを活用した
高度な可視化・分析・監視のカスタマイズ

Intersight でのトラブルシューティング / 障害対応高度化



アラーム 監視

**Intersight管理対象
機器のfault/
アラームを集約**

Severity: 543 (Critical 479, Warning 29, Info 35)

Message	Severity	Code	Source Name
The API key ending with '67184cd3756461330171759...	Critical	IamApiKeyExpired	
ESXi host 192.168.1.48 intermittently lost connection t...	Critical	HXA-NOD-0003	FI-HX-Cluster-Tokyo ...
ether port 1/8 on fabric interconnect B oper state: link...	Critical	UCS-F0276	CS-FI6332-HX/sys/t...
ether port 1/4 on fabric interconnect B oper state: sfp...	Info	UCS-F0279	CS-FI6332-HX/sys/t...
ether port 1/2 on fabric interconnect B oper state: sfp...	Info	UCS-F0279	CS-FI6332-HX/sys/t...
ether port 1/3 on fabric interconnect B oper state: sfp...	Info	UCS-F0279	CS-FI6332-HX/sys/t...
ether port 1/1 on fabric interconnect B oper state: sfp...	Info	UCS-F0279	CS-FI6332-HX/sys/t...
Power supply 1 in fabric interconnect B power: error	Critical	UCS-F0369	CS-FI6332-HX/sys/t...

Severity: 481 (Critical 481)

Filters: Severity = Critical x, 481 results

Message	Severity	Code	Source Name
ESXi host 192.168.1.48 intermittently lost connection t...	Critical	HXA-NOD-0003	FI-HX-Cluster-Tokyo ...
ether port 1/8 on fabric interconnect B oper state: link...	Critical	UCS-F0276	CS-FI6332-HX/sys/t...
Power supply 1 in fabric interconnect B power: error	Critical	UCS-F0369	CS-FI6332-HX/sys/t...

**基本的な
フィルタリング
機能をサポート
アラーム内容
重大度
Fault Code**

Intersight でのトラブルシューティング / 障害対応高度化



アラーム
監視

Demo Intersight Dashboard Monitor

Alarm Monitor

Serial Number: * 全時間 FaultCode (Fxxx): * Description (Free Text): *

重大度: Cleared, Critical, Warning, All

確認済み: Acknowledged, None

	Date	Name	Model	Serial	UserLabel	Severity	Description	Acknowledge
1	2024-11-29T16:05:24.364Z	CS-FI6332-HX-4	HX220C-MSSX	WZP241917LW		Critical	F0314 Server 4 (service profile:) discovery: failed	None
2	2024-11-28T07:19:30.053Z	CS-FI6332-HX-2	HX220C-MSSX	WZP241917L8		Cleared	F0479 Virtual interface 1185 link state is down	None
3	2024-11-28T07:19:30.053Z	CS-FI6332-HX-2	HX220C-MSSX	WZP241917L8		Cleared	F0479 Virtual interface 1184 link state is down	None
4	2024-11-28T07:19:30.053Z	CS-FI6332-HX-2	HX220C-MSSX	WZP241917L8		Cleared	F0479 Virtual interface 1181 link state is down	None

Intersight管理対象
機器のfault/
アラームを集約

Demo Intersight Dashboard Monitor

Alarm Monitor

Serial Number: * 過去24時間 FaultCode (Fxxx): * Description (Free Text): *

重大度: Cleared, Critical, Warning, All

確認済み: Acknowledged, None

	Date	Name	Model	Serial	UserLabel	Severity	Code	Description	Acknowledge
1	2024-11-29T16:05:24.364Z	CS-FI6332-HX-4	HX220C-MSSX	WZP241917LW		Cleared	F0314	Server 4 (service profile:) discovery: failed	None

faultコード、アラーム内容、
重大度に加えて、
アラームの発生日時、シリアル番号
でも絞り込み可能に！

Intersight でのトラブルシューティング / 障害対応高度化



アラーム メール通知

通知 > Alarm
編集

ルールを追加
通知のルールを作成します。

通知メールにはユーザーのアカウントの機密情報が含まれている場合があります。詳細については、ヘルプセンターを参照してください

Enable Rule

名前*
Email-Notification

メールアドレス*
tjimbo@cisco.com

アラーム

重大度
 Critical 警告 情報

Include Cleared Alarms

通知メールの
送信条件として
重大度が
設定可能

アラーム

重大度
 Critical 警告 情報

Include Cleared Alarms



全てのアラーム(12)がメール通知される
例) Critical(8)と警告(4)

Criticalアラーム(8)

HXの論理障害	UCSのH/W障害(CPU/Mem)等
Intersightとの接続切断情報	UCSのH/W(PSUの未給電)
XXX	YYY
ZZZ	Other

警告アラーム(4)

FIのポートダウン	FIのバックアップ失敗
UCSの管理ポートに接続失敗	XXX

Intersight でのトラブルシューティング / 障害対応高度化



柔軟な通知条件
でメール通知
カスタマイズ

splunk>enterprise App Administrator 2 メッセージ 設定 アクティビティ ヘルプ 検索

サーチ、レポート、アラート 新規レポート 新規アラート

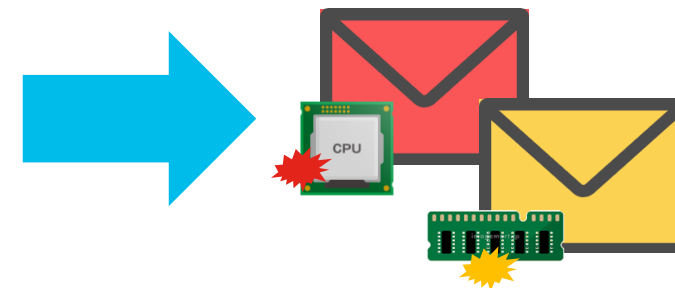
サーチ、レポート、およびアラートは、ピボットまたはサーチページから作成された保存済みサーチです。詳細

1 サーチ、レポート、アラート タイプ: すべて App: Intersight Add-On for Splunk (TA-intersight-addon) オーナー: Administrator (splunkadmin)

フィルター 10件/ページ

名前	アクション	タイプ	次の予定時間	ビューの表示	オーナー	App	アラート	共有中	ステータス
Intersight HWE rror	編集 実行 最新を表示	アラート	2024-11-30 21:15:00 CST	なし	splunkadmin	TA-intersight-addon	0	プライベート	有効

柔軟な絞込みが可能なアラート機能：
特定 H/W Fault に該当する場合のみ
管理者にメール可能

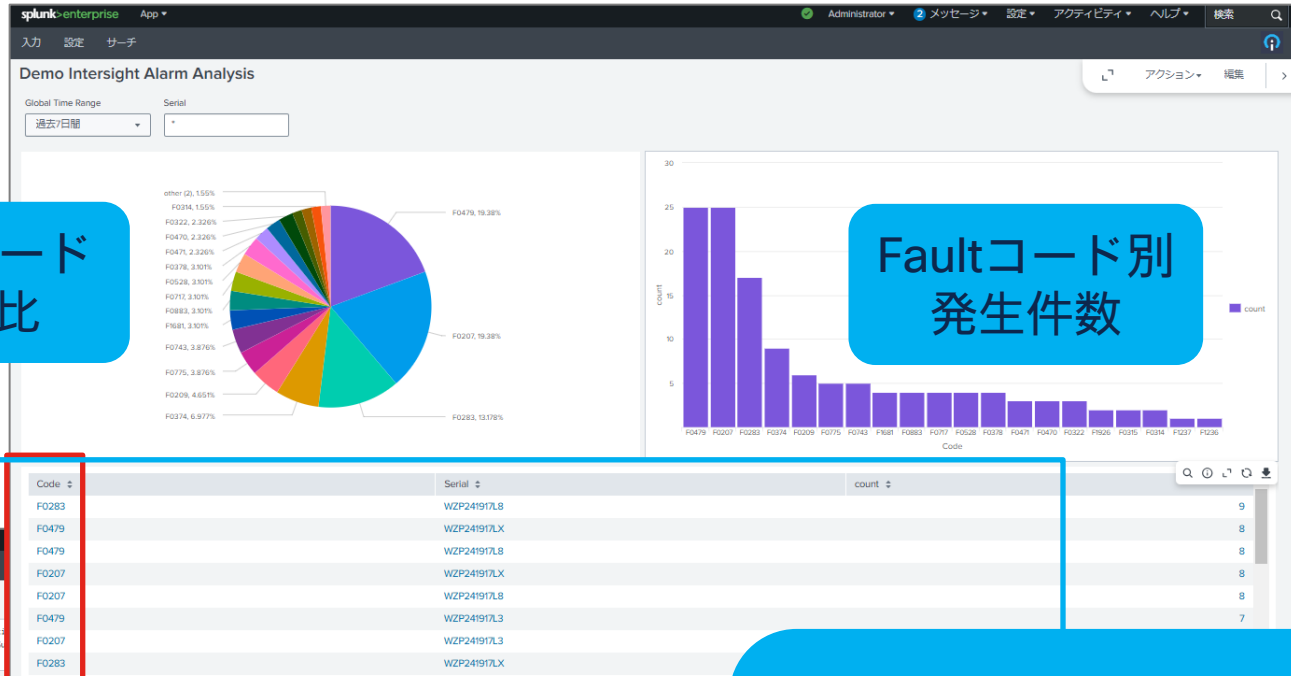


ユースケース 2 Intersight 管理機器の 傾向分析と プロアクティブな 問題検出

Intersight 管理機器の傾向分析とプロアクティブな問題検出

統計情報を整理し、グラフも組み合わせ、より分かりやすくカスタマイズ

Faultコード
構成比



Faultコード別
発生件数

詳細情報を
ドリルダウンして
確認できる

サーバで
特定Faultコード・Fault回数
の発生が多い場合、
故障の予兆を疑う

新規サーチ

```
index=* sourcetype=cisco:intersight:condAlarms Code="F0283*" Severity="*" Acknowledge = "none" Descr:
AncestorMoid as Moid | join Moid[search index=intersight sourcetype=cisco:intersight:computePhysi
,Acknowledge | rename ModTime as Date
```

✓ 17件のイベント (2024/11/23 21:00:00.000~2024/11/30 21:55:45.000) イベントサンプリングを行わない

イベント パターン 統計情報 (7) 視覚エフェクト

20件/ページ / フォーマット プレビュー

Date	Name	Model	Serial	UserLabel	Severity
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T07:19:30.053Z	CS-F16332-HK-2	HX220C-M55X	WZP241917L8		Cleared
2024-11-28T03:03:28.735Z	CS-F16332-HK-3	HX220C-M55X	WZP241917LX		Cleared
2024-11-28T03:03:28.735Z	CS-F16332-HK-3	HX220C-M55X	WZP241917LX		Cleared
2024-11-28T03:03:28.735Z	CS-F16332-HK-3	HX220C-M55X	WZP241917LX		Cleared
2024-11-28T03:03:28.735Z	CS-F16332-HK-3	HX220C-M55X	WZP241917LX		Cleared
2024-11-28T03:03:28.735Z	CS-F16332-HK-3	HX220C-M55X	WZP241917LX		Cleared
2024-11-28T06:48:00.053Z	CS-F16332-HK-1	HX220C-M55X	WZP241917L3		Cleared
2024-11-28T06:48:00.053Z	CS-F16332-HK-1	HX220C-M55X	WZP241917L3		Cleared

ユースケース3 Intersight 監査ログの 可視化と活用

Intersightの監査ログの可視化と活用

```
010101      001!01      #011
00z1:00##   10&&10   0101+=
1>>>01010  10?10!/%  1010*10   01001
1%=01110-  01+010/  1011*0   01<010
010^01000  0110     100#     01001   01
0101110    1010     =011
                                00101
                                0%0
101/010-010#01101
10*10&&01001110++01*0101
%=01110-0101+010/001011*0010
0<<%=001000110101:0100#01101
01110-10:101>0110101001+=01001
10!/%01010*100####10&&101110-1
101010||0100100####010++01010
101^01*010110%00#0110?10!010
0101001--0101####010010##
1001110++*=01001/=0101
10>010111001|0101!010
=010010111001-=01
01101&&0101101
10111010#01>>0
%0++0101>0101
0#0110011*=01
010>010111001
1001+=01001011
0101####10&&1
0!/%01010*100###
101010||0100100##
#01101^01*010110%
101+=0101001--0101
010*10&&01001110++
011*00101<010>0101
100#01101001+=010
101/=0110101%=01
111011<<100001
1^01*01011
```

1. 退職者の利用状況チェック
退職者が出た場合は不正なアクセスや操作をしていないかチェック

2. 不正操作など内部不正への備え
情報漏洩や不正操作などの内部不正をチェック

監査していることを従業員に通知すれば、
内部不正の抑止力としても有効

Intersightの監査ログの可視化と活用

Intersightの監査ログ

Intersight システム

検索 [検索 (Search)]

12 468 36

監査ログ

* All 監査ログ +

検索 Filters 7952 results

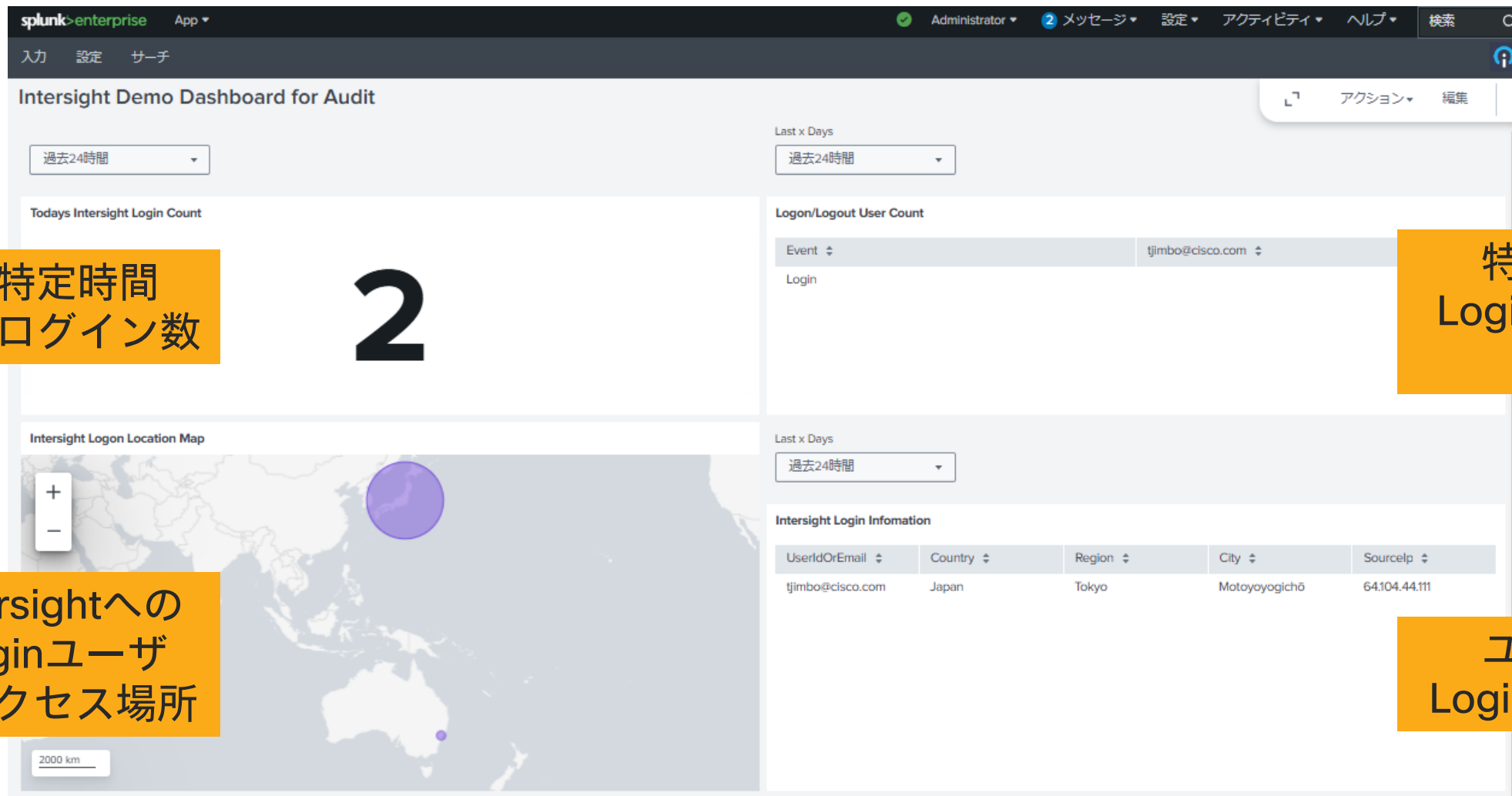
エクスポート

日時	作用されたオブジェクトタイプ	作用されたオブジェクト	イベント	ユーザのEメール	クライアントアドレス
2024年11月4日 10:28:09 午前	顧客操作		Modified	tjimbo@cisco.com	
2024年11月4日 10:26:12 午前	ユーザ	tjimbo@cisco.com	Login	tjimbo@cisco.com	
2024年11月4日 8:44:24 午前	ユーザ	tjimbo@cisco.com	Login	tjimbo@cisco.com	
2024年11月1日 4:27:54 午後	ユーザ	tsumura@cisco.com	Logout	tsumura@cisco.com	
2024年11月1日 3:57:26 午後	ユーザ	tsumura@cisco.com	Login	tsumura@cisco.com	
2024年10月31日 5:07:54 午後	ユーザ	tjimbo@cisco.com	Logout	tjimbo@cisco.com	
2024年10月31日 4:37:23 午後	デバイス要求	2876c075-3c10-43c2-aad1-65cde	Deleted	tjimbo@cisco.com	
2024年10月31日 4:22:40 午後	デバイス要求	FDO23451F9Y&FDO23451FAL	Created	tjimbo@cisco.com	
2024年10月31日 3:53:09 午後	ユーザ	tjimbo@cisco.com	Login	tjimbo@cisco.com	
2024年10月31日 12:21:52 午後	ユーザ	tjimbo@cisco.com	Logout	tjimbo@cisco.com	
2024年10月31日 11:43:50 午前	デバイス要求	2876c075-3c10-43c2-aad1-65cde	Created	tjimbo@cisco.com	
2024年10月31日 11:43:17 午前	ユーザ	tjimbo@cisco.com	Login	tjimbo@cisco.com	

オブジェクト例	イベント例
ユーザ	Login Logout
デバイス登録	Created Modified
APIキー	Created
クラスタプロファイル	Create Modified
Alarm Suppression	Created Deleted
アプリケーションの登録	Created

Intersightの監査ログの可視化と活用

Intersightの監査ログをより分かりやすく



特定時間の
ログイン数

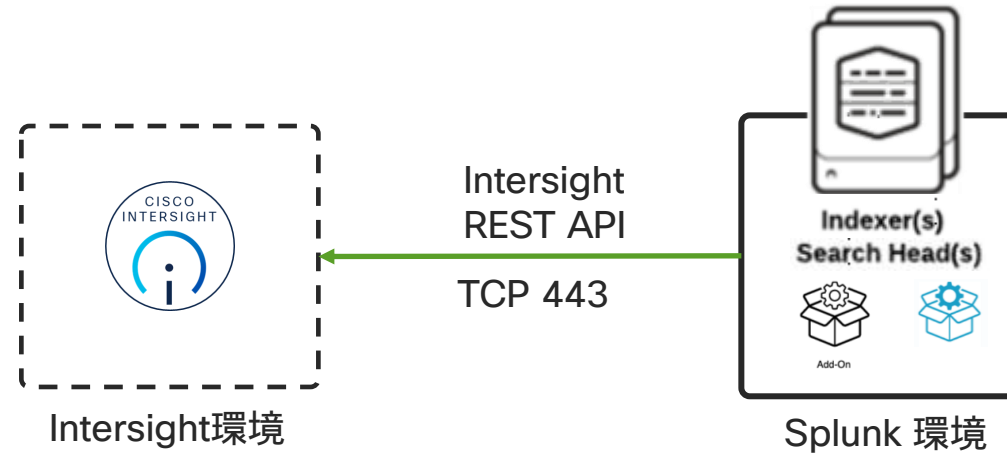
2

特定時間
Login/Logout
情報

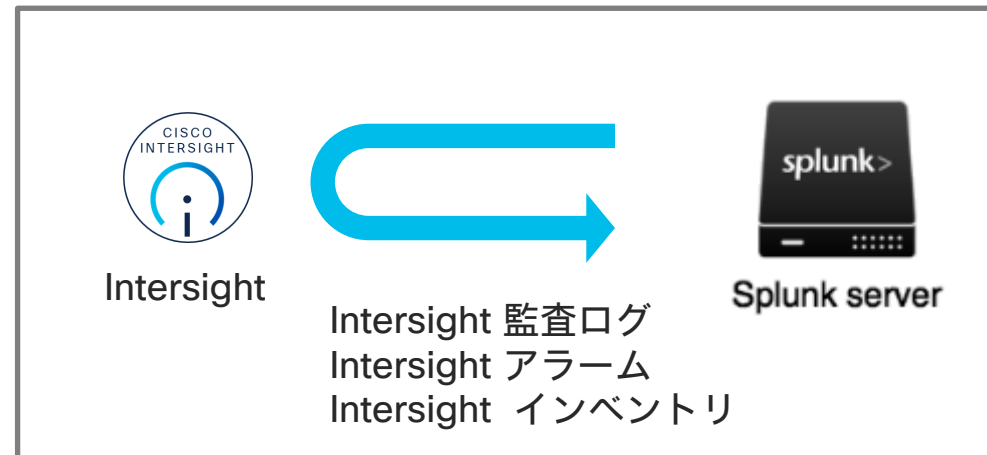
Intersightへの
Loginユーザ
のアクセス場所

ユーザ別
Login詳細情報

Intersight環境から情報収集する仕組み



使用例



Intersight環境から情報収集する仕組み

Welcome to the new Splunkbase! To return to the old Splunkbase, [click here](#).

splunkbase™ Collections Apps [Submit an App](#) [Log In](#)

This app is archived. [Learn more](#)

Cisco Intersight Add-on for Splunk

The Cisco Intersight Add-on for Splunk (TA-intersight-addon) provides a python-based scripted input to retrieve data from Cisco Intersight. SaaS, Connected Virtual Appliance, and Private Virtual Appliance deployments of Intersight are all supported. Data that can be imported from Intersigh...

Built by [Karthik Karupasamy](#)

[Login to Download](#) [Share](#) [Notify](#)

Latest Version 1.3.1
August 4, 2022
[Release notes](#)

Compatibility ⓘ
Splunk Enterprise
Platform Version: 9.3, 9.2, 9.1, 9.0, 8.2, 8.1, 8.0

Rating
5 ★★★★★ (1)
[Log in to rate this app](#)

Support
 Not Supported
[Learn more](#)

本日のデモ

Splunk連携の方法



Step 1
Splunk Enterprise
を構築

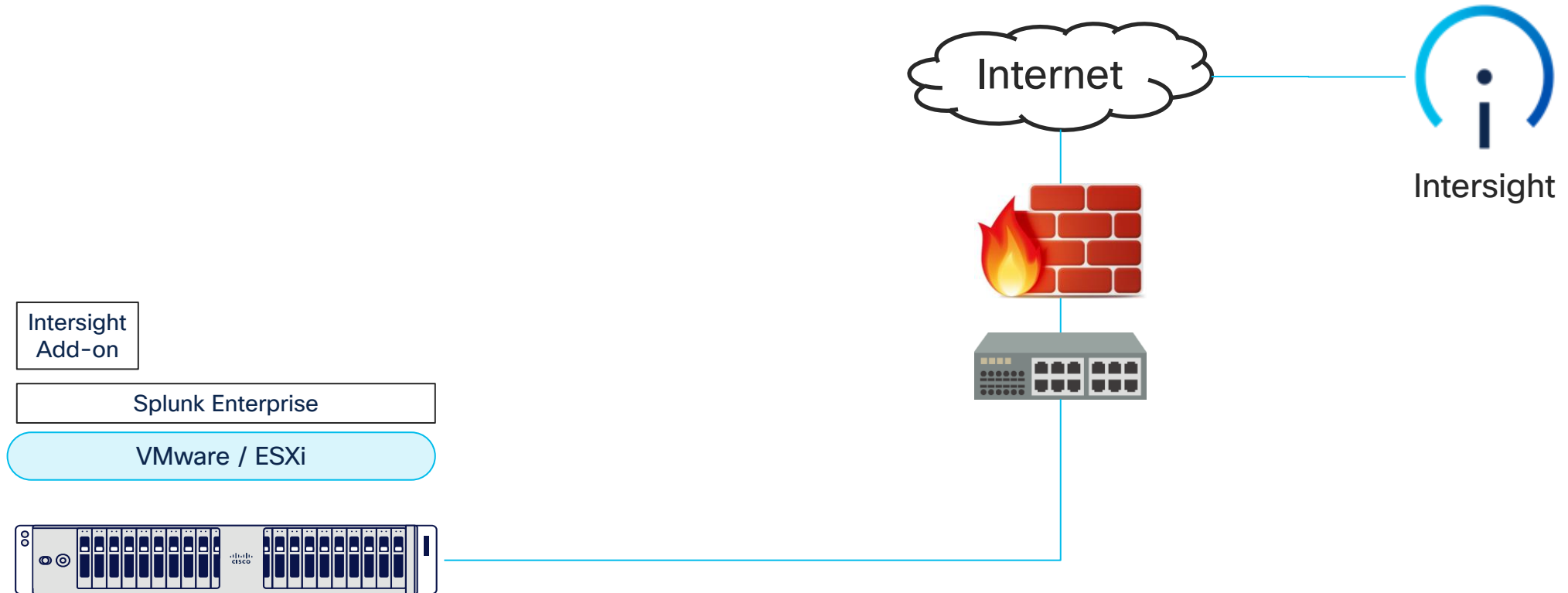
Step 2
Intersight
API Key/Id発行

Step 3
Intersight
Add-on 導入

Step 4
Splunk Add-on
Input設定

Step 5
Splunk Dashboard
作成/インポート

本日のデモ内容 (環境)



App 管理

Appを名前ですearch...

- Intersight Add-On for Splunk
- Search & Reporting
- Splunk Dashboard Examples
- Splunk Secure Gateway
- Upgrade Readiness App

[他のAppの検索](#)

こんにちは, Administrator

- [クイックリンク](#)
- [ダッシュボード](#)
- [最近表示したデータ](#)
- [自分で作成](#)
- [あなたと共有](#)

共通のタスク

データの追加 さまざまな共通のソースからデータを追加します。	データの検索 Splunk検索でデータを行動に変えます。	データの視覚化 データに適したダッシュボードを作成します。	チームメンバーの追加 Splunkプラットフォームにチームメンバーを追加します。
権限の管理 ルールを使用して、アクセスできるユーザーを制御します。	モバイルデバイスの設定 Splunk Secure Gatewayを使用してモバイルデバイスにログインまたはモバイルデバイスを管理します。		

学習およびリソース

プロダクトツアー Splunkは初めてですか？ ツアーに参加して使用方法を確認しましょう。	Splunk Docsで詳しく学ぶ 総合的なガイダンスに従ってSplunkソフトウェアをデプロイ、管理、使用します。	Splunkエキスパートの支援を受ける Splunk Lanternカスタマーサクセスセンターの利用可能なガイダンス。	権限の拡張 Splunkbaseにある何千ものAppを参照します。
Splunkコミュニティに参加する 学び、刺激を受け、知識を共有します。	他のユーザーのSplunkの使用方法を確認する 実際のカスタマーストーリーを参照します。	トレーニングおよび認定 認定Splunk Ninjaになる。	

本日のセッションのまとめ



1

IntersightとSplunkの連携により
可観測性を向上可能

2

トラブルシューティングや障害対応の
迅速化・プロアクティブな問題検出
監査ログの可視化と活用

3

無償トライアル利用可能
Splunk Enterprise (60日)
Splunk Cloud (15日)



Cisco Intersight/UCS サクセスコミュニティ Webinar



Cisco Intersight/UCSユーザー様、運用パートナー様向けに、Webセミナーを実施させていただきます。

開催日時	テーマ
2025年4月10日 (木) 15:30 ~ 16:30	Intersight success community - webinar#4 <非公式> UCS C220 M5+RAID構成にNutanix CE 2.1を入れてみる

- ※ 途中参加、途中退席も可能です。ご自由に参加ください。
- ※ 開催中はQAを受け付けておりますので、お気軽にご質問ください。

