

# Cisco Network Insights for DCNM/ NX-OS v1



最終更新日 : 08-May-2020

## このサンドピットについて

一般的に、dCloud サンドピットにはデモガイドは含まれていません。このドキュメントは、詳細なガイドが利用可能になるまで一時的に提供されます。

この環境の使用方法については、付属のビデオを参照してください。

## 要件

次の表に、このデモンストレーションの要件の概要を示します。

必須	オプション
ラップトップ	

## このソリューションについて

Cisco Network Insights Advisor (Cisco NIA) アプリケーションは、データセンターネットワークを監視し、対処可能な問題を特定して、可用性の維持と突発的な停止回数の軽減を実現します。Cisco NIA はお客様のネットワークの状況を把握することで、可用性を維持し、アップタイムに影響を与える可能性がある潜在的な問題について警告することに重点を置いた、プロアクティブなアドバイスを提供できます。

Cisco Network Insights for Resources (Cisco NIR) アプリケーションは、データ収集を通じて情報を収集し、Cisco Data Center Network Manager (Cisco DCNM) 全体で利用可能なリソースとアクティブなプロセスおよび設定の概要を提供します。

## はじめに

### プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

**プレゼンテーションを成功させるには入念な準備が不可欠です**

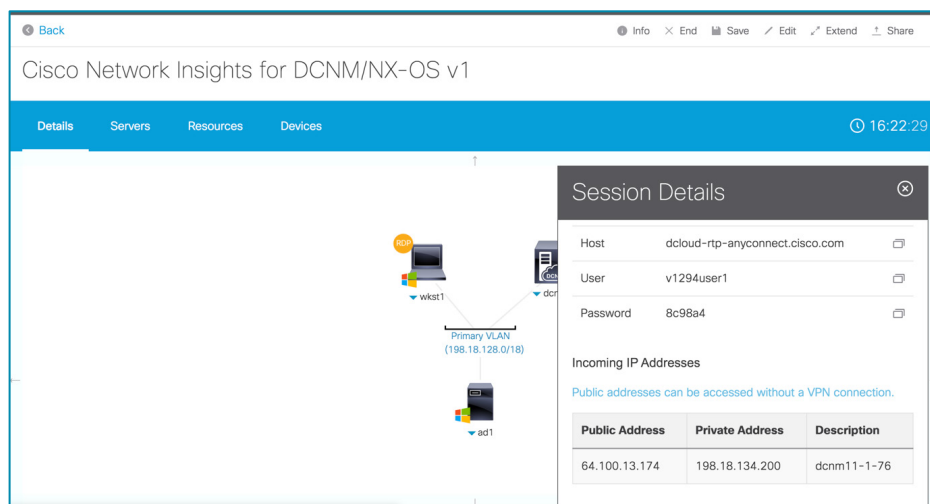
次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[[手順を見る](#)] [英語]

**注：**セッションがアクティブになるまで最長で 20 分かかることがあります。

2. 次に示す使用可能な接続方法のいずれかにより、DCNM に接続します。

- Cisco dCloud リモート デスクトップ クライアント [[手順を見る](#)] デスクトップから DCNM を起動します。
- ブラウザから DCNM に直接接続して、デモセッションに割り当てられたパブリック IP を使用します。パブリックアドレスは、セッションの詳細ペインで確認できます。



The screenshot shows the Cisco Network Insights for DCNM/NX-OS v1 interface. The main area displays a network topology with a 'Primary VLAN (198.18.128.0/18)' and devices 'wkst1' and 'ad1'. A 'Session Details' panel is open on the right, showing the following information:

Host	User	Password
dcloud-rtp-anyconnect.cisco.com	v1294user1	8c98a4

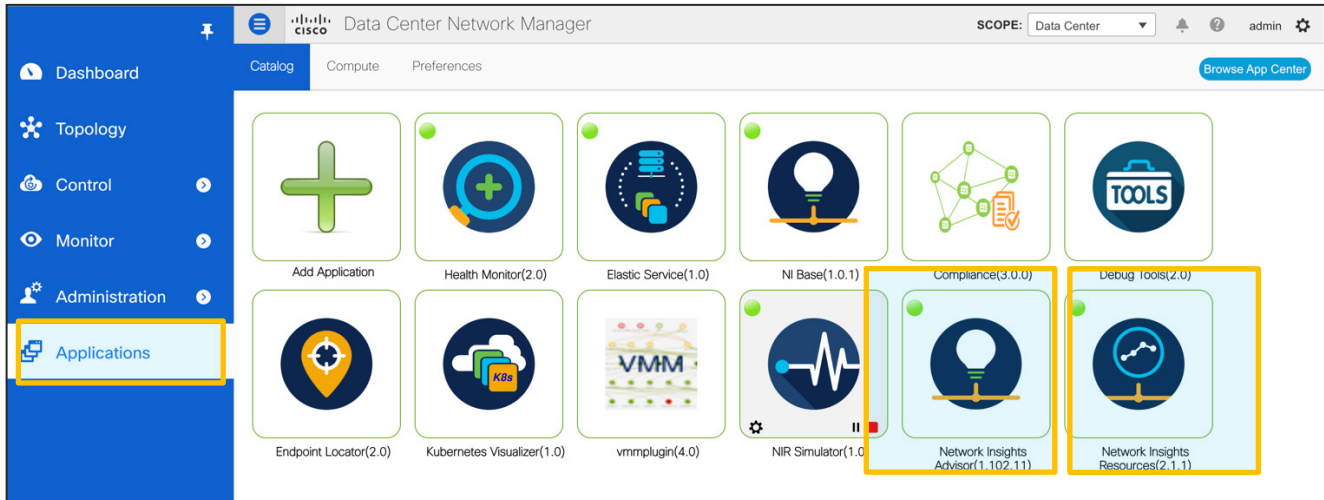
Below the session details, there is a section for 'Incoming IP Addresses' with a note: 'Public addresses can be accessed without a VPN connection.'

Public Address	Private Address	Description
64.100.13.174	198.18.134.200	dcnm11-1-76

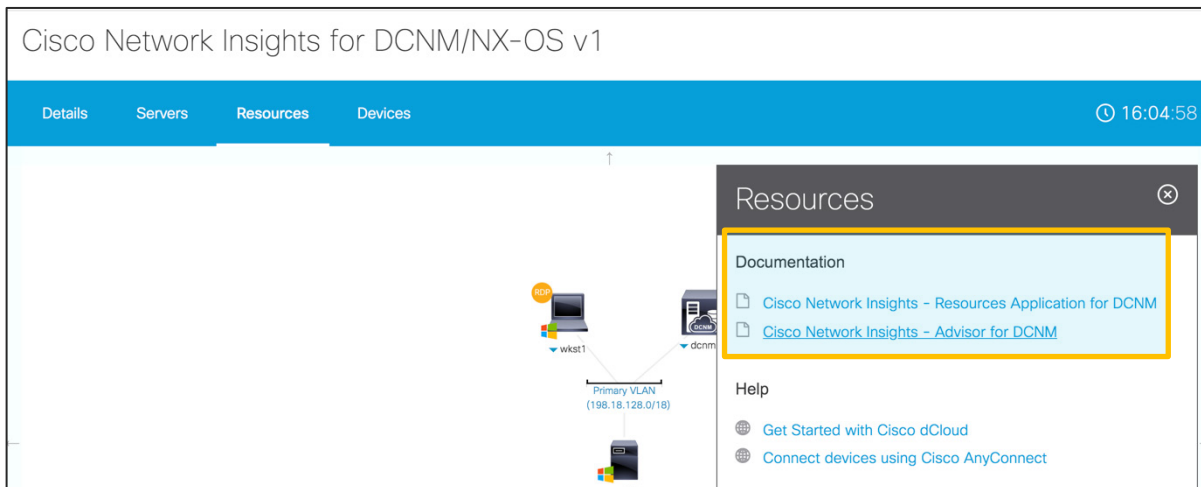
3. 次のクレデンシャルを使用して DCNM にログインします。

- Admin / C1sco12345

4. アプリケーションにアクセスするには、上記の IP アドレスとクレデンシャルを使用して GUI にログインします。[アプリケーション (Applications)] タブにスクロールし、Network Insights Resources (NIR) と Network Insights Advisor (NIA) を探します。アプリケーションをクリックして、参照します。

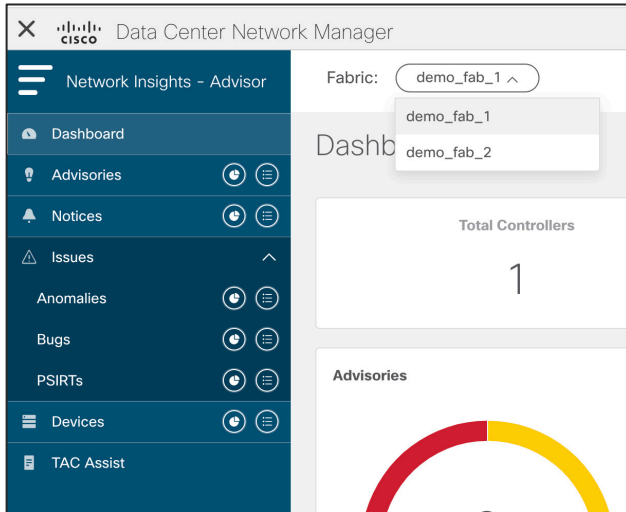


5. アプリケーションと使用例の詳細については、dCloud セッション「リソース」にあるビデオ（吹替版）をご覧ください。

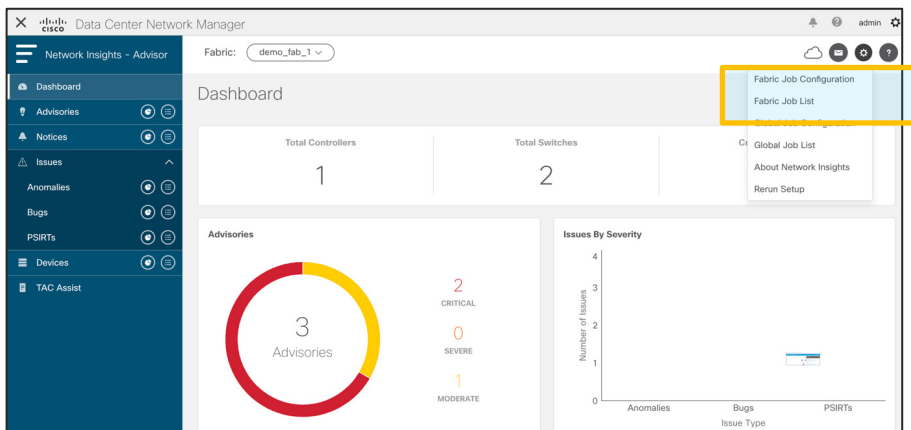


## Network Insights Advisor

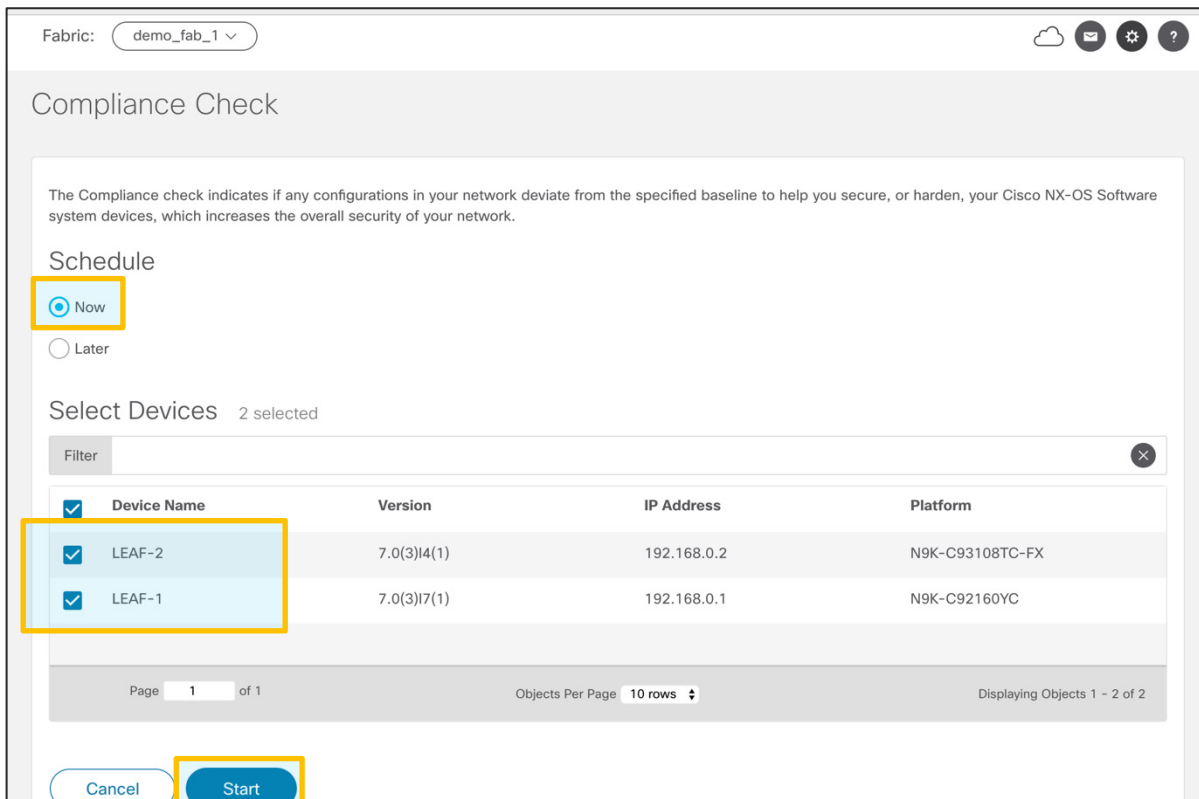
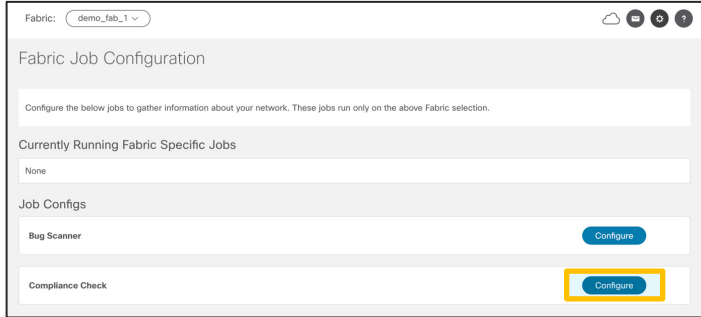
Network Insights Advisor (NIA) の場合は、以下のジョブを実行して、バグ/PSIRT/異常にある関連するデータを確認してください。これは Demo\_Fabric\_1 と Demo\_Fabric\_2 の両方に対して実行できます。



[設定 (Settings) ] の下にある [ファブリックジョブ設定 (Fabric Job Configurations) ] までスクロールして、バグスキャンジョブとコンプライアンスジョブを実行し、関連するバグ/PSIRT と、ファブリック内のハードニングに関する違反を確認します。



コンプライアンスジョブを実行してファブリック内のハードニングに関する違反を確認するには、[コンプライアンスチェック (Compliance Check) ] ジョブの [設定 (Configure) ] を選択し、スケジュールおよび関連するデバイスを選択してジョブを実行します。



コンプライアンスジョブを実行すると、次に示すように、関連するハードニングに関する違反がスイッチに表示されます（通常は完了までに数分かかります）。

The screenshot shows the Cisco Data Center Network Manager interface. The left sidebar is titled 'Network Insights - Advisor' and contains several menu items: Dashboard, Advisories, Notices, Issues, Anomalies (highlighted with a yellow box), Bugs, PSIRTs, Devices, and TAC Assist. The main content area is titled 'Anomalies' and shows a donut chart with the number '8' in the center, indicating the total number of anomalies. To the right of the chart, there are three categories of anomalies: CRITICAL (0), SEVERE (0), and MODERATE (8). Below the chart is a table with the following columns: Severity, Type, Title, and Devices Affected.

Severity	Type	Title	Devices Affected
Moderate	Management Plane	Enable strong password checking	2
Moderate	Management Plane	Use AAA for accounting	2
Moderate	Management Plane	Use AAA (TACACS+) for command authorization	2

ファブリック内のスイッチに影響を与えるバグと PSIRT を確認するには、「バグスキャナ」ジョブを設定して、スケジュールおよび関連するデバイスを選択して、ジョブを実行します。

The screenshot shows the 'Fabric Job Configuration' page in Cisco Data Center Network Manager. The page title is 'Fabric Job Configuration' and it includes a sub-header 'Currently Running Fabric Specific Jobs' with the value 'None'. Below this, there is a section for 'Job Configs' which lists two jobs: 'Bug Scanner' and 'Compliance Check'. The 'Bug Scanner' job has a 'Configure' button highlighted with a yellow box. The 'Compliance Check' job also has a 'Configure' button.

Bug Scanner

The Bug Scan provides actionable intelligence for security threats and vulnerabilities. The Bug Scan will Analyze Known Bugs on your network.

**Schedule**

Now  
 Later

Select Devices 2 selected

Filter

<input checked="" type="checkbox"/>	Device Name	Version	IP Address	Platform
<input checked="" type="checkbox"/>	LEAF-2	7.0(3)14(1)	192.168.0.2	N9K-C93108TC-FX
<input checked="" type="checkbox"/>	LEAF-1	7.0(3)17(1)	192.168.0.1	N9K-C92160YC

Page 1 of 1      Objects Per Page 10 rows      Displaying Objects 1 - 2 of 2

Cancel      Start

このバグスキャンジョブを実行すると、関連するバグと PSIRT が次のように表示されます（通常は完了までに数分かかります）。

Network Insights - Advisor      Fabric: demo\_fab\_1

Bugs

Filter

Bugs

2 Bugs

0 CRITICAL  
1 SEVERE  
1 MODERATE

Severity	Bug	Title	Devices Affected
Severe	CSCvi87166	Nexus 3500 crashes with "spm hap reset" due to memory leak in libspm.so or only SPM process crashes.	2
Moderate	CSCvj96082	Inconsist Higig interface number	2



The screenshot shows the Cisco Data Center Network Manager interface. The left sidebar contains navigation items: Advisories, Notices, Issues, Anomalies, Bugs, PSIRTs (highlighted with a yellow box), Devices, and TAC Assist. The main content area is titled 'PSIRTs' and features a donut chart showing 53 total PSIRTs, broken down into 0 Critical, 42 Severe, and 11 Moderate. Below the chart is a table with columns for Severity, PSIRT ID, Title, and Devices Affected.

Severity	PSIRT	Title	Devices Affected
Severe	CSCve41590	Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability	2
Moderate	CSCvf31232	Evaluation of n9k-standalone-sw for gSOAP June-July 2017	2
Severe	CSCvh20027	Cisco FXOS NX-OS Software Command Injection Vulnerabilities (CVE-2019-1781, CVE-2019-1782)	2