



Cisco Nexus Dashboard Insights Software Management、リリース 6.5.1 : Cisco ACI の場合

目次

- 新規情報および変更情報 2
- ソフトウェア管理 3
 - ソフトウェア管理 3
 - ソフトウェア管理ジョブの表示 3
 - ソフトウェア管理の作成 4
 - アクティブ バグと影響を受けやすいバグの表示..... 6
 - Cisco APICの事前検証基準 8
- 著作権 16

初版：2024 年 7 月 16 日

米国本社

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

新規情報および変更情報

次の表は、最新リリースまでの主な変更点の概要を示したものです。ただし、本リリースまでの変更点や新機能の一部は表に記載されていません。

Cisco Nexus Dashboard Insightsの新機能と変更された動作

特長	説明	リリース	参照先
技術変更	「サイト」という言葉は「ファブリック」に変更されました。	6.5.1	ドキュメント全体

このドキュメントは、Nexus Dashboard Insights の GUI およびオンラインで www.cisco.com で入手できます。本書の最新バージョンに関しては、「[Cisco Nexus Dashboard Insights](#)」の「[Documentation](#)」を参照してください。

ソフトウェア管理

ソフトウェア管理

アップグレードを実行する前に、複数の検証を実行する必要があります。同様に、アップグレードプロセス後、複数のチェックを実行すると、アップグレード手順の変更と成功を判断するのに役立ちます。

ソフトウェア管理機能は、推奨されるソフトウェア バージョンへのアップグレード パスを提案し、アップグレードの潜在的な影響を判断します。また、アップグレード前後の検証チェックにも役立ちます。

ソフトウェア管理機能には次のようなメリットがあります。

- ・ ネットワークの正常なアップグレードの準備と検証を支援します。
- ・ アップグレード前のチェックに関する可視性を提供します。
- ・ アップグレード後のチェックとアップグレード後のステータスに関する可視性を提供します。
- ・ 実稼働環境への影響を最小限に抑えます。
- ・ アップグレードプロセスが単一のステップであるか複数のステップであるかを可視化します。
- ・ 特定のファームウェアバージョンに該当するバグを表示します。

通常、特定の長期リリースに対応した最新のメンテナンス リリースとパッチにアップグレードすることをお勧めします。そのリリース後に導入された機能が必要な場合、最新のリリースにアップグレードできます。

注意事項と制約事項

アップグレード後の分析を実行する前に、すべてのノードがアップグレード済みであることを確認してください。

ソフトウェア管理ジョブの表示

1. [管理 (Admin)] > [ファブリック ソフトウェア管理 (Fabric Software Management)] に移動します。

Software Management

Software Management Jobs 🕒 Last week

Refresh

New Analysis

Filter

Job Status



Status	Name	Fabric	Node Target Firmware	Devices	Start Time	End Time	
Analysis Failed	test-demo	ndfc129	9.3(12)	ni-dcnm-switch1	Feb 09 2024 09:54:49.457 AM	Feb 09 2024 09:58:33.564 AM	
Analysis Failed	demo1	ndfc129	10.2(6)M	ni-dcnm-switch1	Feb 09 2024 10:09:56.556 AM	Feb 09 2024 10:13:51.061 AM	
Analysis Complete	test-ua-sa	aci130	16.0(4c)	aci-switch-103	Feb 08 2024 11:18:51.663 AM	Feb 08 2024 11:30:30.962 AM	
Analysis Complete	demo	aci130	16.0(4c)	aci-switch-103	Feb 09 2024 10:27:15.766 AM	Feb 09 2024 10:39:17.362 AM	

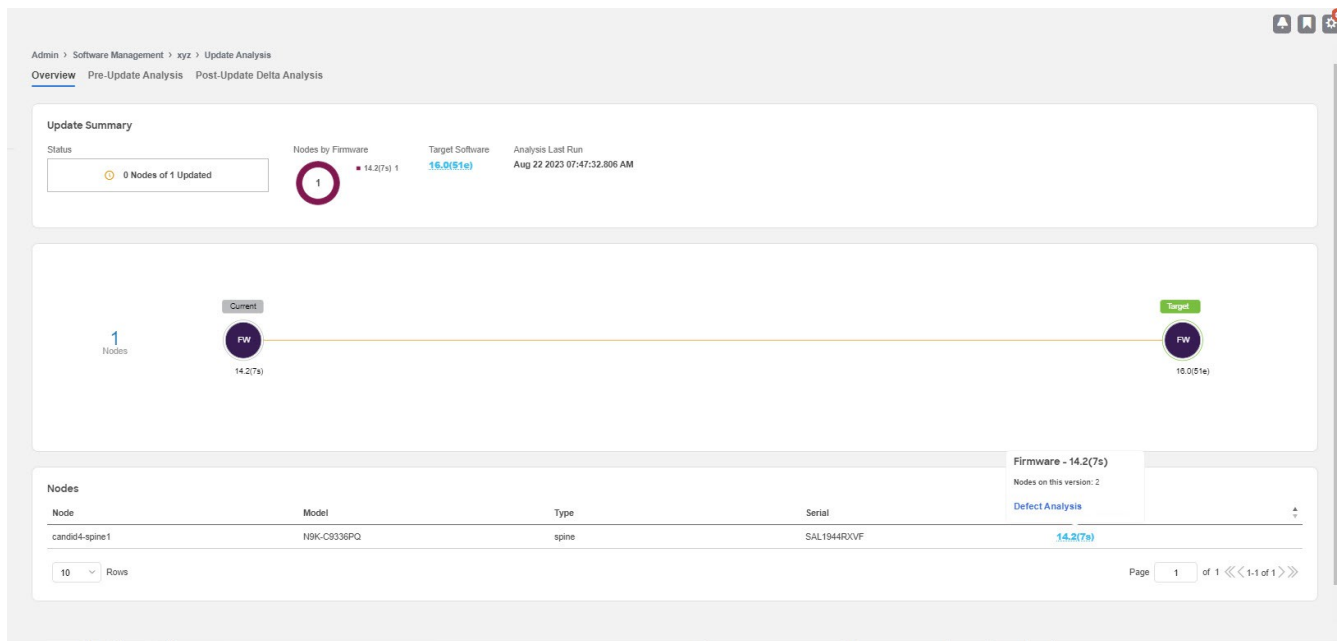
- [時刻 (Time)] セレクタを使用して、時間範囲を選択します。
 - ソフトウェア管理ページでは、選択された時間範囲に基づきファブリックのジョブ ステータスを表示します。
 - フィルタバーを使用して、ステータス別にジョブをフィルタ処理します。
 - [ジョブ ステータス (Job Status)] 円チャートでは、ステータスとともにジョブ数を表示します。
 - [ジョブ (Jobs)] テーブルでは、ステータス、名前、ファブリック、ノード ターゲット ファームウェア、デバイス、開始時間、終了時間などソフトウェア管理ジョブの情報を表示します。
- 歯車アイコンをクリックして、[ジョブ (Jobs)] テーブルの列を構成します。

ソフトウェア管理の作成

- [管理 (Manage)] > [ファブリック ソフトウェア管理 (Fabric Software Management)] > [新しい分析 (New Analysis)] を選択します。
- 分析名を入力します。
- ファブリックを選択します。[次へ (Next)] をクリックします。
- ファームウェアを選択します。シスコ推奨リリースと最新のファームウェアリリースが表示されます。

この手順をスキップすることもできます。

- [ノードの選択 (Select Nodes)] をクリックします。
 - ノードを選択します。更新が必要なノードのみ表示されます。分析ごとに一度に選択できるノードは10個だけです。
 - [追加 (Add)] をクリックします。
- [ジョブの作成 (Create Job)] をクリックします。ジョブは [ソフトウェア管理 (Software Management)] ダッシュボードに表示されます。
- 完了した分析をクリックして、詳細を表示します。



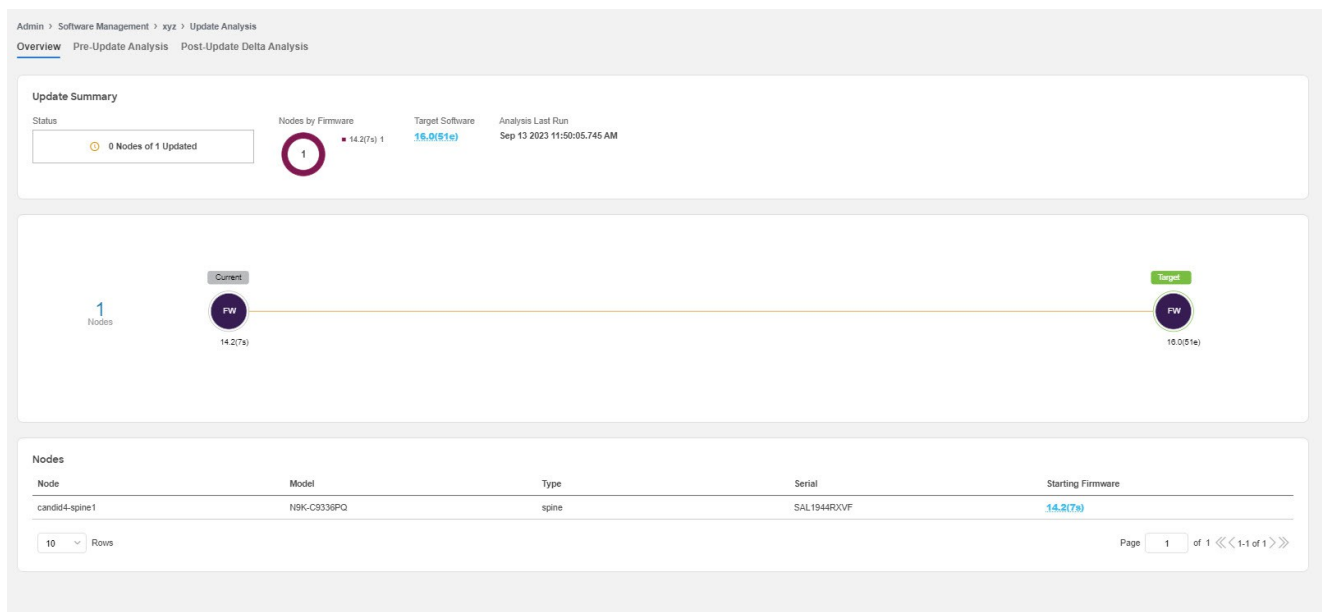
分析の詳細

- ・ [全般 (General)] : ここでは、分析ステータスの場合に表示されます
- ・ [ファームウェアの概要 (Firmware summary)] : ここでは、ファブリック、ファブリック ファームウェア、ファブリック ターゲット ファームウェア、選択されたノード、ノード ファームウェアおよびノード ターゲット ファームウェアが表示されます。
- ・ ファームウェアおよびノードのアップグレード パス。ファームウェアを選択した場合、ファームウェアとノードのアップグレードパスは個別に表示されます。

[**更新の詳細を表示 (View Update Details)**] をクリックして、ファームウェアまたはノードの更新前の分析と更新後の分析を表示します。

概要

ここでは、更新の概要、アップグレード パス、ノードのリストが表形式で表示されます。

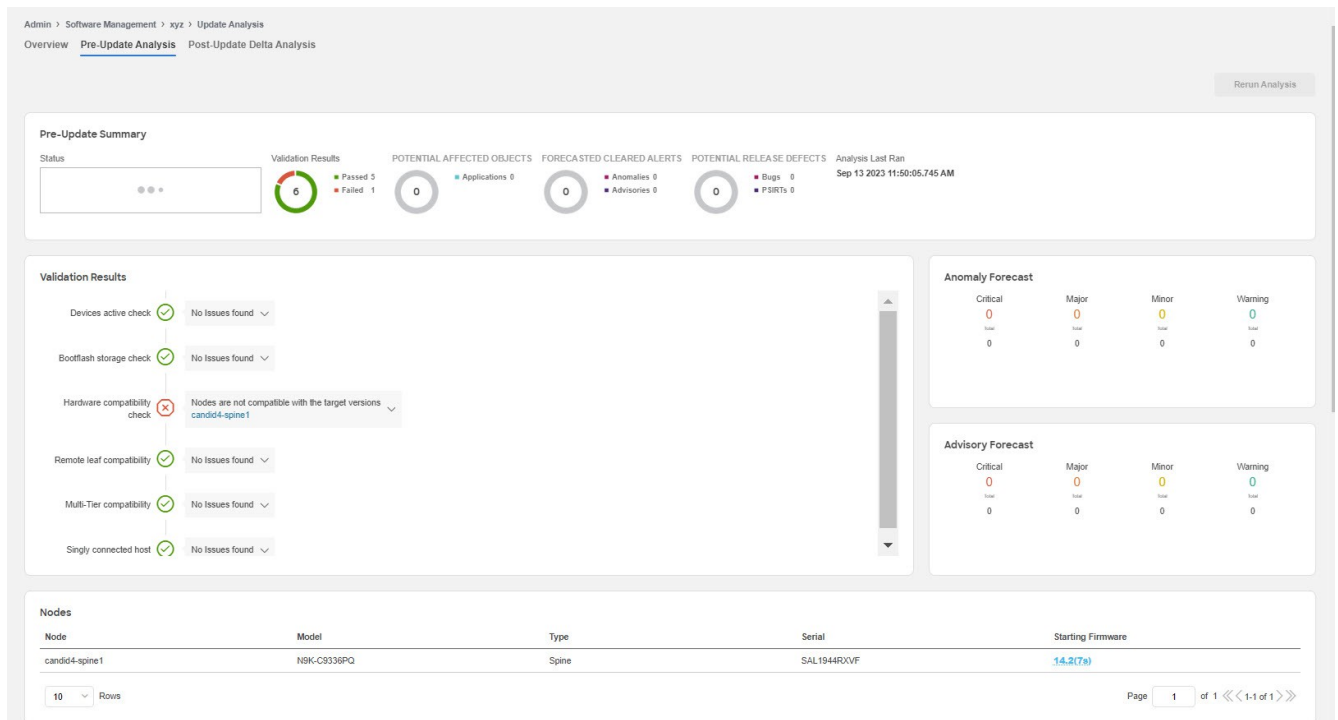


更新前の分析

ここでは、ノード ステータス、検証結果、影響を受ける可能性のあるオブジェクト、アップグレード後に予測されるクリア アラート、アップグレード後に当てはまる潜在的なリリース障害などの詳細を表示します。ここでは、異常性とアドバイザリの予測も示しています。**[検証結果 (Validation Results)]** エリアで強調表示されている問題を修正したら、**[分析を再実行 (Rerun Analysis)]** をクリックします。ドロップダウン ボタンをクリックして、更新前の検証基準と、各基準で検出された問題を表示します。「Cisco APIC の事前検証基準」を参照してください。



アップグレード前の検証に変更が影響したかどうかを確認するために、再度 python スクリプトを実行し、ファイルをアップロードしてからアシュアランス分析を再度実行することをお勧めします。



更新後の分析

ここでは、更新後の分析の詳細を表示します。更新後の概要には、アップグレードのステータスが表示されます。

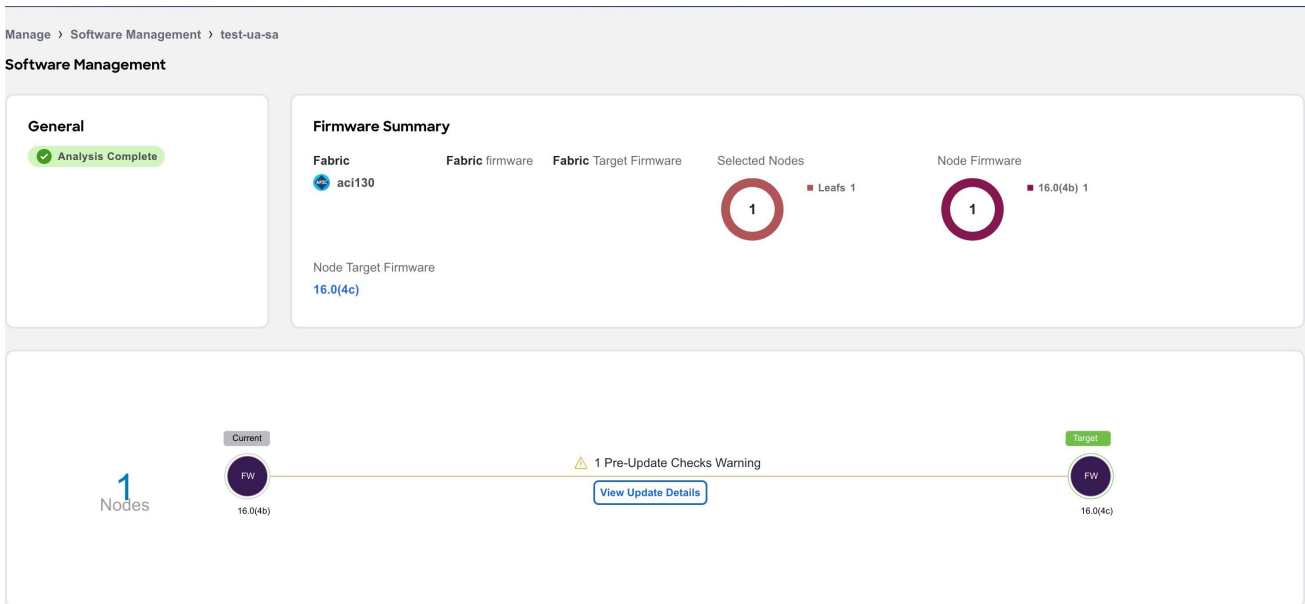
- ・ **[正常性の差分 (Health Delta)]** をクリックして、アップグレード前とアップグレード後の分析間の異常の違いを表示します。
- ・ **[運用の差分 (Operational Delta)]** をクリックして、アップグレード前とアップグレード後の分析間の運用リソースの違いを表示します。
- ・ **[ポリシーの差分 (Policy Delta)]** をクリックして、アップグレード前とアップグレード後の分析が実行されたときのポリシーの違いを表示します。これは、ACI ファブリックにのみ適用されます。
- ・ **[分析を再実行 (Rerun Analysis)]** をクリックします。

アクティブ バグと影響を受けやすいバグの表示

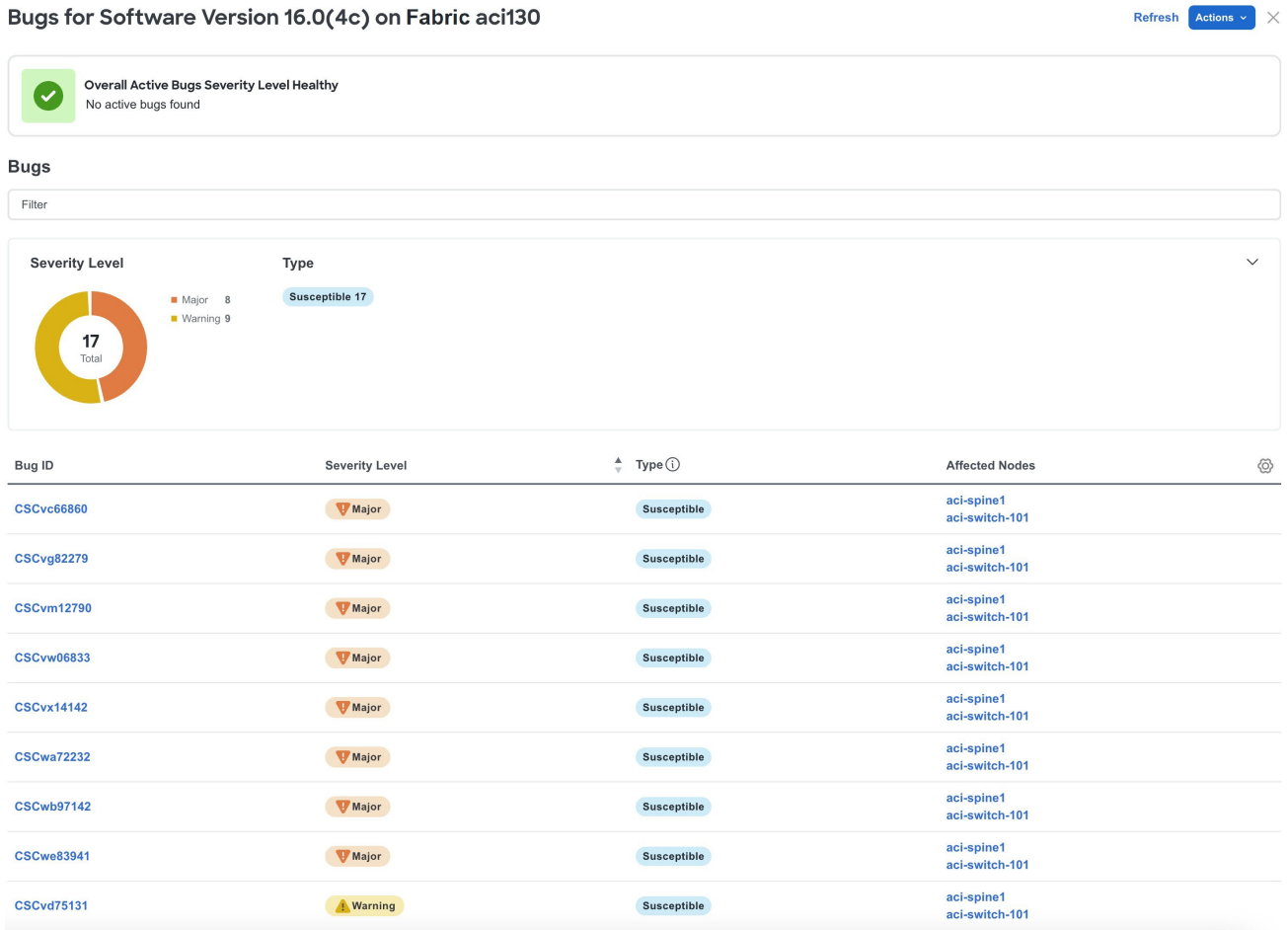


すべてのファブリックでバグ スキャンが有効になっていることを確認してください。

1. [管理 (Admin)] > [ファブリック ソフトウェア管理 (Fabric Software Management)] に移動します。
2. [ソフトウェア管理ジョブ (Software Management Jobs)] テーブルで、分析をクリックします。



[ファームウェアの概要 (Firmware Summary)] エリアで、ノード ターゲット ファームウェアにカーソルを合わせ、[バグの表示 (View Bugs)] をクリックして、そのファブリックのアクティブ バグと影響を受けやすいバグを表示します。「バグスキャン」を参照してください。



3. [アクション (Actions)] ドロップダウン メニューから、[バグ スキャンの実行 (Run Bug Scan)] をクリックして、オンデマンドのバグ スキャンを実行します。

Cisco APICの事前検証基準

事前検証基準	説明	リリース
非アクティブなデバイスが見つかりました	この検証では、すべてのデバイスがアクティブかどうかを確認します。	6.0.1
互換性のあるターゲットバージョンを選択してください	この検証では、ターゲットのファームウェアバージョンが現在実行中のバージョンと互換性があるかどうかを確認します。	6.0.1
リモートリーフの互換性	この検証では、ターゲットのファームウェアバージョンでリモートリーフ機能がサポートされているか、ファブリックがリモートリーフ機能を使用しているかどうかを確認します。	6.0.1
多層互換性	この検証は、ターゲットのファームウェアバージョンで多層トポロジがサポートされているか、ファブリックにTier-2リーフノードがあるかどうかを確認します。	6.0.1
ファブリックにアクティブなクリティカルな設定障害が4つあります	この検証では、ファームウェアの更新に影響を与える可能性があるクリティカルな設定障害または特定の障害の存在を確認します。	6.0.1
ポッドにあるインフラ MP-BGP用のルートリフレクタが2つ未満	この検証では、各ポッドに、インフラMP-BGPのルートリフレクタとして設定されたスパインノードが少なくとも2つあるかどうかを確認します。	6.0.1
ノードがvPCにありません	この検証では、ファームウェアの更新中に冗長性/高可用性を確保するために、リーフノードがvPCで設定されているかどうかを確認します。	6.0.1
ノードにアウトオブバンド管理IPがありません	この検証では、OOB (アウトオブバンド) 管理IP設定のないノードの存在を確認して、常にすべてのノードにアクセスできるようにします。	6.0.1
NTPが設定されていません	この検証では、Network Time Protocol (NTP)がCisco APICに設定されているかどうかを確認します。	6.0.1
スイッチ アップグレード メンテナンス グループ チェック	この検証では、APICにメンテナンスグループとファームウェアグループがあるかどうかを確認します。	6.0.1
ルールを検証できませんでした	この検証では、ターゲットのファームウェアバージョンが現在実行中のCIMCバージョンと互換性があるかどうかを確認します。	6.0.1

事前検証基準	説明	リリース
クラスタ内のCisco APICに異なるインフラVLAN IDが設定されています	この検証では、クラスタ内のAPICに同じインフラVLAN IDが設定されているかどうかを確認します	6.0.1
Cisco APICクラスタのステータスが、すべてのAPICノードに完全には適合していません	この検証では、APICクラスタのステータスがすべてのAPICノードに完全に適合しているかどうかを確認します。	6.0.1
ファブリックリカバリが進行中です	この検証では、進行中のファブリックリカバリがあるかどうかを確認します。	6.0.1
設定されたSNMPv3ユーザー認証やプライバシータイプは、ターゲットのCisco APICファームウェアバージョンでサポートされていません	この検証は、設定されたSNMPv3ユーザー認証やプライバシータイプがターゲットのAPICファームウェアバージョンでサポートされているかどうかを確認します。	6.0.1
エンドポイントネットワークの冗長性	この検証では、ノードの再起動中のトラフィック損失を避けるために、ノードに非冗長エンドポイントがあるかどうかを確認します。	6.0.2
APIC クラスタ ステータス	この検証では、APICクラスタのステータスがすべてのAPICノードに完全に適合しているかどうかを確認します。 データレイヤが部分的に分岐しているか、または完全に適合していない場合は、APIC とスイッチのファームウェア更新を実行しないでください。	6.3.1
APIC クラスタ ステータス	この検証では、APICクラスタのステータスがすべてのAPICノードに完全に適合しているかどうかを確認します。 データレイヤが部分的に分岐しているか、または完全に適合していない場合は、APIC とスイッチのファームウェア更新を実行しないでください。	6.3.1

事前検証基準	説明	リリース
APIC ディスク容量	この検証では、APIC のディスク領域が不足していることを警告する障害があるかどうかを確認します。 これにより、APIC のアップグレードが失敗する可能性があります。APIC は、残りのディスク領域の量に応じて 3 つの異なる障害を発生させますこれらの障害のいずれかがシステムで発生した場合は、アップグレードを実行する前に問題を解決する必要があります。	6.3.1
スイッチのブート フラッシュの使用	この検証では、スイッチ ノードを正常にアップグレードするのに十分なブートフラッシュ ストレージがあるかどうかを確認します。	6.3.1
APIC SSD の正常性	この検証では、APIC SSD の正常性ステータスを警告する障害があるかどうかを確認します。	6.3.1
スイッチ SSD の正常性	この検証では、スイッチ SSD の正常性ステータスを警告する障害があるかどうかを確認します。	6.3.1
日次構成バックアップ	この検証では、過去 24 時間に取得された有効な構成バックアップがあるかどうかを確認します。	6.3.1
NTP設定	この検証では、APIC に Network Time Protocol (NTP) が設定されているかどうかを確認します。	6.3.1
NTPステータス	この検証では、Network Time Protocol (NTP) がファブリック内の APIC とスイッチで同期されているかどうかを確認します。	6.3.1
OOB 管理 IP	この検証では、OOB (アウトオブバンド) 管理 IP 設定なしでノードの存在をチェックし、すべてのノードに常にアクセスできることを確認します。 アップグレード/ダウングレード中に、ACI インフラ経由でノードに到達できない場合があります。念のため、各ノードへのコンソールアクセスを準備することをお勧めします。	6.3.1

事前検証基準	説明	リリース
進行中のファブリックの復旧	この検証では、進行中のファブリックリカバリがあるかどうかを確認します。	6.3.1
アクティブなアプリケーション	この検証では、無効にする必要があるアクティブなアプリケーションが APIC にあるかどうかを確認します。	6.3.1
構成ゾーン	この検証では、アップグレード前に無効化または削除する必要がある構成ゾーンがあるかどうかを確認します。	6.3.1
スイッチのハイ アベイラビリティ (vPC リーフ)	この検証では、ファームウェア更新中に冗長性とハイアベイラビリティを確保するために、リーフ ノードにvPCが設定されているかどうかチェックされます。 ファブリックが ECMP などの他の手段によって冗長性を提供している場合、または意図的にシングル ホーム サーバがある場合は、このチェックを無視します。	6.3.1
スイッチのハイ アベイラビリティ (スパイン ルート リフレクタ)	この検証では、各ポッドに、インフラMP-BGPのルートリフレクタとして設定されたスパインノードが少なくとも2つあるかどうかを確認します。 すべてのルート リフレクタ スパイン ノードが同時に使用できない場合、ファブリックは L3Outs からの外部ルートへの到達可能性を失います。	6.3.1
アップグレード グループ (スパイン HA)	メンテナンス グループが見つかった場合、この検証では以下を確認します 1) 同じポッド内のすべてのスパインが同じグループでアップグレードされるわけではありません。 2) すべての BGP ルート リフレクタ スパインが同じグループでアップグレードされるわけではありません。 3) すべての IPN/ISN スパインが同じグループでアップグレードされるわけではありません。	6.3.1
アップグレード グループ (vPC HA)	この検証では、同じ vPC ペアの両方のリーフ ノードが同じアップグレード グループにないことを確認します。	6.3.1

事前検証基準	説明	リリース
アップグレード グループ (APIC リーフ HA)	これにより、同じ APIC に接続されている両方のリーフ ノードが同じアップグレードグループに属していないことが確認されます。	6.3.1
重大な構成違反	この検証では、ファームウェアの更新に影響を与える可能性がある重大な構成障害または特定の障害の存在を確認します。	6.3.1
コントローラ ポートの構成の競合	この検証では、APIC 接続ポートに展開されているために拒否されている構成があることを警告する障害があるかどうかを確認します。	6.3.1
L3 インターフェイス展開の競合	この検証では、すでに L2 モードで動作しているポートで L3 構成が拒否されていることを警告する障害があるかどうかを確認します。	6.3.1
L2 インターフェイス展開の競合	この検証では、すでに L3 モードで動作しているポートで L2 設定が拒否されていることを警告する障害があるかどうかを確認します。	6.3.1
BD サブネットの重複	この検証では、BD サブネットが同じではなく、同じ VRF 内で重複していることを警告する障害があるかどうかを確認します。 一度に有効になるのは、これらの構成の 1 つだけです。 したがって、アップグレード後に、以前とは異なる BD サブネットが有効になる場合があります。	6.3.1
重複する BD サブネット	この検証では、同じ VRF 内の外部ブリッジドメインに重複するプレフィックスがあることを警告する障害があるかどうかを確認します。	6.3.1
外部 EPG プレフィックスの重複	この検証では、同じ VRF 内の外部 EPG に重複するプレフィックスがあることを警告する障害があるかどうかを確認します。	6.3.1

事前検証基準	説明	リリース
HW プログラミングの失敗 (L3Out プレフィックス、コントラクト)	この検証では、L3Out プレフィックスから pcTag へのマッピング エントリまたはコントラクトのプログラミングに失敗したことを警告する障害があるかどうかを確認します。	6.3.1
スケーラビリティ (キャパシティ ダッシュボードに関連する障害)	この検証では、APIC GUI の [キャパシティ ダッシュボード (Capacity Dashboard)] で確認できるオブジェクト eqptcapacityEntity の警告スケーラビリティの問題に関連する統計障害 (TCA : Threshold Crossing Alert) があるかどうかを確認します。 デフォルトでは、キャパシティ ダッシュボードのすべての統計に障害を発生させるしきい値が構成されているわけではありません。これは、[ファブリック (Fabric)] > [ファブリック ポリシー (Fabric Policies)] > [ポリシー (Policies)] > [モニタリング (Monitoring)] > [デフォルト (default)] > [統計収集ポリシー (Stats Collection Policies)] > [モニタリング オブジェクト (Monitoring Object)] > [機器 キャパシティ エンティティ (eqptcapacityEntity) (Equipment Capacity Entity (eqptcapacityEntity))] > [統計タイプ (Stats Type)] で確認および構成できます。	6.3.1
重複する VLAN プール	これにより、同じ EPG 上で VLAN ID が重複している VLAN プールが検出されます。 このような構成は、この構成が意図的であり、VNID がどのように割り当てられ、ACI で動作するかを理解している場合を除き、アップグレード後またはアップグレード中にトラフィックに影響を与える可能性があります。	6.3.1
マルチポッド/マルチサイトの ISIS 再配布メトリック	これにより、マルチポッドおよびマルチサイトの ISIS 再配布メトリックがチェックされます。	6.3.1

事前検証基準	説明	リリース
L3Out MTU サイズ	この検証では、ファブリック内のすべてのレイヤ 3 Out に構成されている MTU サイズをチェックします。 ACI L3Out 側と接続されたデバイスの MTU サイズが一致しない場合、アップグレード前にすべてが機能していた場合でも、アップグレード後のルート交換が失敗する可能性があります。	6.3.1
LLDP を介した異なるインフラ VLAN	この検証では、障害があるかどうかを確認します。2 つの異なる ACI ファブリック間でバックツーバック接続されたインターフェイスがある場合は、アップグレードの前にこれらのインターフェイスで LLDP を無効にする必要があります。 これは、アップグレード後にスイッチが復歸すると、別のインフラ VLAN を使用している可能性がある他のファブリックから LLDP パケットを受信して処理する可能性があるためです。その場合、スイッチは誤って他のファブリックのインフラ VLAN を介して検出され、正しいファブリックでは検出されません。	6.3.1
オフライン VMM ドメイン	この検証では、VMM ドメインにオフラインのコントローラがあるかどうかを確認します。	6.3.1
VMM ドメイン LLDP/CDP 隣接関係	この検証では、APIC が VMM DVS 統合の vCenter を介して vSwitch の LLDP/CDP 情報を見つけられない場合に、障害警告があるかどうかを確認します。 LLDP/CDP 情報は、VLAN を動的に展開する ACI スイッチのインターフェイスを検出するために使用されます。	6.3.1

事前検証基準	説明	リリース
CIMC 互換性	この検証では、ターゲット ファームウェアバージョンが現在実行中の CIMC バージョンと互換性があるかどうかを確認します。	6.3.1
バージョンの互換性	この検証では、ターゲットのファームウェアバージョンが現在実行中のバージョンと互換性があるかどうかを確認します。	6.3.1
リモート リーフの互換性	この検証では、ファブリックがリモート リーフ機能を使用している場合、ターゲット ファームウェア バージョンでリモート リーフ機能がサポートされているかどうかを確認します。このチェックは、主にダウングレード シナリオ用です。	6.3.1
多層互換性	この検証では、ファブリックに Tier-2 リーフ ノードがある場合、ターゲット ファームウェア バージョンで多層トポロジがサポートされているかどうかを確認します。このチェックは、主にダウングレード シナリオ用です。	6.3.1
スイッチ アップグレード メンテナンス グループ チェック	この検証では、4.0 以前のリリースから 4.0 以降のリリースにアップグレードする前に、APIC にメンテナンスとファームウェア グループが存在するかどうかを確認します。	6.3.1
インフラ VLAN ID の検証	この検証では、クラスタ内の APIC に同じインフラVLAN ID が設定されているかどうかを確認します。	6.3.1
SNMPv3 認証の互換性	この検証は、設定されたSNMPv3ユーザー認証やプライバシータイプがターゲットの APICファームウェアバージョンでサポートされているかどうかを確認します。	6.3.1

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『INFORMATION PACKET』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または黙示のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。商標または登録商標です。シスコの商標の一覧は、<http://www.cisco.com/go/trademarks> でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。(1110R)。

© 2017-2024 Cisco Systems, Inc. All rights reserved.