Cisco Nexus Dashboard リリース 4.3.1 のリリース ノート

©2026 Cisco and/or its affiliates. All rights reserved.

はじめに

インサイトから影響まで、 Cisco Nexus Dashboard 4.3.1 は、統合された可視性、よりスマートな自動化、シームレスな統より、ネットワークの処理量を増やし、より高速にスマートに強化します。

Cisco Nexus Dashboard 4.3.1 は、可視性、オーケストレーション、自動化などの複数の機能を、データセンター運用のための単一のシームレスなプラットフォームに統合します。ダッシュボードは最新のネットワークの統合管理ペインとして機能し、 ACI、 VXLAN EVPN、クラシック LAN、AI、ルーテッド、外部およびファブリック間、メディア ファブリック、 SAN ファブリックなどの異なるアーキテクチャ間でのシームレスな運用を可能にします。ネットワークのリアルタイム分析、優れた可視性、および堅牢なアシュアランスを提供し、組織がパフォーマンスを最適化して信頼性を強化できるようにします。

詳細については、このドキュメントの最後にある「関連コンテンツ」を参照してください。

表1 新機能および変更された情報

日付	説明
2026 年 8 月 22 日	リリース 4.3.1.175 が利用可能になりました。

新しいソフトウェア機能

Prime Infrastructure の機能

表 2 新しいインフラストラクチャの機能

製品への影響	特長	説明
使いやすさ	VMware ESXi 9.0.2 デプロイメントのサポート	VMware ESXi 9.0.2 のサポートが追加された、サポートされている最新の VMware インフラストラクチャに Nexus Dashboard を展開することで、チームは Nexus Dashboard を現在の仮想化標準に合わせることができるようになります。 詳細については、『*Cisco Nexus Dashboard Fabric Controller Deployment Guide*』を参照してください。
使いやすさ	KVM 環境の合理化された QCOW2 デプロイメント	RHEL や Nutanix を含む KVM ベースの環境全体でNexus Dashboard をより一貫して展開できるようになります。QCOW2 イメージに、セットアップを簡素化し、互換性を検証し、サポートされているプラットフォーム間で一貫したデプロイメントを促進する、デプロイメントの検証とオーケストレーションスクリプトが含まれるようになりました。 詳細については、『*Cisco Nexus Dashboard Fabric Controller Deployment Guide*』を参照してください。
使いやすさ	拡張された Connected TACによる迅速なサポート	拡張された Connected TACにより、LAN およびSAN環境全体での問題解決を拡張。このエクスペリエンスは、アクティブなソフトウェアテレメトリに依存せず、システム設定- ファブリック管理 から一元管理でき、 Nexusダッシュボードプロキシを介した Cisco N9000 スイッチでのターゲットを絞った診断収集と安全な読み取り専用コマンド実行をサポートします。 詳細については、 *「Cisco テクニカル サポートの操作」* の「接続されたTAC」の項を参照してください。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
使いやすさ	接続シューティングを迅速化するための詳細な LLDP 診断	acs lldp show コマンドを介して LLDP ネイバー、インターフェイス、設定、および統計データに rescue-user アクセスすることで、ノード接続の問題を迅速にトラブルシュートします。テクニカルサポートコレクションには、NDノード管理およびデータ インターフェイスからの LLDP ネイバー情報も含まれ、診断のためのより完全な証拠が提供されるようになりました。 詳細については、 *「Cisco Nexus Dashboard のトラブルシューティング」の* 記事の「 システムと接続のトラブルシューティング」 セクションを参照してください。
セットアップの容易さ	委任デバイスアップグレード管理	より広範な管理アクセス権を付与せずに、ファブリック ソフトウェアのアップグレードを委任します。Nexus Dashboard 4.3.1 では、デバイス アップグレード ワークフローに対して、以前は NDFC デバイス アップグレード管理者として使用可能だったデバイス アップグレード管理者ロールが再導入されています。 詳細については、 *「ユーザー、ロール、およびSecurityの構成* 」の記事の 「統合リリースのロールと権限」 セクションを参照してください。
使いやすさ	自律テンプレートでの同名ポリシーの確実なインポート	ファブリック間で同一のオブジェクト名が存在する場合、オーケストレータ関連の自律テンプレート ポリシーをより高い信頼性でインポートできます。Nexus Dashboardは、送信元ファブリック内でのみリレーションシップの参照を解決し、インポート中に他のファブリックの同じ名前のオブジェクトが誤って使用されるのを防ぎます。 詳細については、「*ACI ファブリックのスキーマとアプリケーション テンプレート*」を参照してください。
ライセンス取得プロセス	ACI ライセンス階層レポート	ACIライセンスの消費に関してより信頼性の高いの高い可視性を取得します。Nexus Dashboard は、ND にオンボードされている APIC のオンボードされたスイッチの数と使用中のライセンス階層（Essentials、 Advantage、または Premier）を報告するようになりました。 詳細については、 *「ライセンスの構成 」の* 記事の 「ACIファブリックのサポート」の 項を参照してください。
使いやすさ	ケルベロスによるエンタープライズ プロキシ認証	Nexus Dashboard をエンタープライズ認証プロキシ環境と統合します。Nexus Dashboard は、ケルベロス クライアントとして機能し、構成されたキー発行局（KDC）からチケットを取得し、アウトバウンド HTTPS が HTTP との接続を認証できるようになりました。機能タイトルは、このリリース用に文書化された NTLM ベースのプロキシ認証のサポートも反映しています。 詳細については、「*システム設定の操作* 」の「プロキシ設定」セクションを参照してください。
使いやすさ	Nexus Dashboard MCP サーバによるセキュアな AI 統合	ネイティブのモデル コンテキスト プロトコル（MCP）サーバー統合により、Nexus Dashboard を Cisco Cloud Control およびお客様が管理する大規模言語モデルに安全に接続します。この基盤により、AI 支援のネットワーク運用とカスタム AI ワークフローが可能になり、組織は企業データと AI モデルを独自の環境内に維持できます。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
		詳細については、「*モデル コンテキスト プロトコル（MCP）サーバー統合*」の記事を参照してください。
使いやすさ	柔軟な初回ログイン パスワード ポリシー	組織のポリシーまたは自動アカウント プロビジョニングで必要な場合に、最初のログイン時にパスワードの変更が必須であることを無効にすると、スーパー管理者はユーザー オンボーディング ワークフローをより詳細に制御できます。 詳細については、「*ユーザー、ロール、およびセキュリティの設定*」の記事の「違反アクション」の項を参照してください。

表 3 新しい LAN 自動化機能

製品への影響	特長	説明
使いやすさ	VXLAN 全体の統合された可視性とトラブルシューティング：ACI ファブリック グループ	VXLAN および ACI ドメインを 1 つの接続された環境として動作させます。VXLAN-ACI ファブリック グループは、EPG から ESG への移行、ルート サーバーを使用した集中型 VXLAN EVPN マルチサイト ピアリング、すべてのセキュリティグループ タイプ、接続分析、およびトラフィック分析をサポートするようになりました。検索と探索がすべてのファブリックグループ タイプで利用できるため、ドメイン間のエンドポイント、ポリシー、および接続の調査も容易になります。 詳細については、これらの記事を参照してください： • 「*ネットワークの分析とトラブルシューティング*」 • *ファブリック グループのファブリック設定の編集* • *Nexus Dashboard の検索と探索* • *ファブリック グループについて*
使いやすさ	メディア向け IP ファブリックのマルチキャスト送信元検出の高速化	PIM フラッディング メカニズム ソース ディスカバリ（PFM-SD）を使用した IP Fabric for Media（IPFM）環境でのマルチキャスト送信元検出を拡張します。ファーストホップ ルータは、ランデブー ポイント、MSDP、または BSR に依存せずに、ファブリック全体にアクティブな送信元をアナウンスできます。サポートには、単一サイトおよびマルチサイト展開、デフォルトおよびデフォルト以外の VRF、ファブリック間境界制御が含まれます。 詳細については、「*メディア（IPFM）ファブリック設定の IP ファブリックの編集*」項目の送信元検出の PIM フラッディング メカニズム」および「非デフォルト VRF およびマルチサイト展開の PFM-SD ポリシー」セクションを参照してください。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
使いやすさ	Hypershield 統合による VXLAN EVPN ファブリックでのスマートスイッチのサポート	トップオブラックおよびゾーンベースのセグメンテーション展開のための分散セキュリティを簡素化します。Nexus Dashboard は、Cisco Hyper Shield コントローラ をオンボードして、Cisco N9324C-SE1U および N9348Y2C6D スマート スイッチでのセキュリティ ポリシーの適用、ゾーンセグメンテーション、およびトラフィック ステアリングを自動化できます。 詳細については、「*Hypershield 統合*」項を参照してください。
使いやすさ	マルチクラスタ展開全体での柔軟な ACI オンボーディング	マルチクラスタ デプロイメントの Nexus Dashboard クラスタから ACI ファブリックを導入準備て管理します。このリリースでは、マルチクラスタ環境での APIC のセカンダリクラスタのオンボーディングと登録解除が追加されています。このリリースでは、マルチクラスタ環境での APIC のセカンダリクラスタのオンボーディングと登録解除が追加されています。 詳細については、「*クラスタの接続*」の記事の次のセクションを参照してください： • Nexus Dashboard 内のマルチクラスタ接続の理解 • ACI クラスターを接続 • ACI クラスターの切断 • ACI ファブリックからのセカンダリ クラスタの登録解除
使いやすさ	自動リモート ファブリック バックアップ	リモート ストレージへのスケジュール済みバックアップでファブリック設定を保護します。Nexus Dashboard は、スイッチの実行構成のバックアップに構成されたリモート ストレージの場所を使用できるようになりました。これにより、チームがリカバリ データを一元化し、ファブリックの状態を一貫してキャプチャできるようになりました。この機能は、外部およびクラシック LAN ファブリックでサポートされています。 詳細については、「*Nexus Dashboard のバックアップと復元*」を参照してください。
使いやすさ	モニタ対象の NX-OS ファブリックのファブリック エージェントの更新	スタンドアロン NX-OS ファブリックをモニタ モードから移行することなく、接続性分析の準備を整えます。Nexus Dashboard は、必要なテレメトリ、ライセンス、メタデータ、およびイメージ管理の前提条件が満たされている場合に、ファブリック エージェント パッケージを更新できます。 詳細については、*「網の分析とトラブルシューティング」の* 記事の 「接続分析の作成」 セクションを参照してください。
セットアップの容易さ	レイヤ 2 ToR をサポートするキャンパス ファブリックでのゼロタッチ インバンド デプロイメント	VXLAN EVPN Campus ファブリックを、インバンド プラグアンドプレイ（PnP）を使用してブートストラップできるようになりました。さらに、インバンド プラグ アンド プレイを使用して、外部ファブリックでレイヤ 2 トップオブラック スイッチとして Catalyst 9200-CX スイッチをブ

©2026 Cisco and/or its affiliates. All rights reserved.

製品への影響	特長	説明
		ートストラップ、管理します。これにより、ゼロタッチデプロイメントがインバンド管理対象キャンパスファブリックの Catalyst 9000 リーフに接続されたアクセス スイッチに拡張されます。 詳細については、*「インバンド管理およびアウトオブバンド PnP の設定」*の「Catalyst 9200-CX ToR スイッチのインバンド PnP」セクションを参照してください。
セットアップの容易さ	Nexus Dashboard ML2 プラグインを使用したハードウェア アクセラ OpenStack ネットワーキング	クラウド オーケストレーションとファブリック自動化を、強化された OpenStack ML2 統合とともに実現します。 新しい Nexus Dashboard ネットワーク タイプは、ハードウェア アクセラレーションによるレイヤ 3 転送を可能にします。階層型ポート バインディングにより、VLAN セグメントが動的に割り当てられます。アドレス範囲が VRF にマッピングされ、より詳細な分離が可能です。そして nd-status 拡張は、自動デプロイメントの再試行とリアルタイムのステータスを提供します。追加の制御により、VLAN ネットワークとボーダー リーフ スイッチのレイヤ 3 転送が有効になります。 詳細については、『*Cisco OpenStack Integration Installation Guide for Nexus Dashboard*』を参照してください。
使いやすさ	Cisco Nexus E100 プラットフォームの自動化とアシュアランスの拡張	トランク インターフェイス ポリシーおよび選択された Nexus Dashboard Insights 機能での VLAN マッピングをサポートする、NX- OS 10.6（4）を実行する追加の Cisco Nexus E100 ベースのプラットフォーム。 これらのプラットフォームでは、 Nexus Dashboard は、トランクインターフェイス ポリシーでの VLAN マッピングを介してポート VLAN 変換をサポートしています。 Nexus Dashboard Insights は、トポロジ、ルートテレメトリ、インターフェイス分析、リソース分析、アシュアランス関連のワークフローなど、これらのプラットフォームの選択された機能をサポートします。トラフィック分析は、E100 プラットフォームのコンパクト モードでのみサポートされますが、フロー テレメトリおよびトラフィック分析フルモードはサポートされません。 注： Cisco NX-OS リリース 10.6（3） 以前を実行しているCisco Nexus E100 ベースのプラットフォームは、AI ファブリックでの QoS をサポートしていません。これらのプラットフォームのいずれかが AI ファブリックに追加されると、再計算操作は失敗し、ユーザーにはエラーが表示されます。
使いやすさ	AI と外部ファブリックの Cisco N9164E-NS4-O のサポート	NX-OS 10.6.2（N）を実行している Cisco N9164E-NS4-O を、AI ルーテッド、AI VXLAN、および外部ファブリックに展開します。このプラットフォームでは、ダイナミック ロード バランシングはパケット単位モードでのみサポートされます。
使いやすさ	より強力なファブリック セキュリティとより細かいプロトコル制御	SHA-512 ハッシュ、スイッチユーザー ポリシーのタイプ 8 およびタイプ 9 パスワード暗号化、 NTP 用の AES-128-CMAC 認証、ルーティング プロトコル キーチェーン管理、および拡張 OSPF および BFD タイマー制御によってファブリック操作を強化します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
		詳細については、「*Data Center VXLAN ファブリック設定の編集*」の「認証」の 項を参照してください。
使いやすさ	多層 VXLAN のスケーラブルなボーダー接続とルーティング分離	スーパー スパインを使用した 3 層トポロジのボーダーおよびボーダーゲートウェイ接続を強化することで、より大規模で耐障害性の高い VXLAN ファブリックを構築します。新しい機能には、適用可能なボーダー スイッチ上の一意の ASN、VRF 単位および VTEP 単位のループバック自動プロビジョニング、および Data Center と AI VXLAN eBGP ファブリックの自動 EVPN オーバーレイ ピアリング ポリシーが含まれます。 詳細については、*「Data CenterVXLAN ファブリック設定の編集*」の「ファブリック管理（eBGP オーバーレイルーティングプロトコルを使用するファブリックの場合）」セクションを参照してください。
使いやすさ	Campus VXLAN EVPN の拡張された設計の柔軟性	ルーティングとトポロジの柔軟性を高めるキャンパス VXLAN EVPN ファブリックを設計します。拡張機能には、4 バイトの BGP ASN、BGP 高速コンバージェンス、より大きなループバックID 範囲、 IP VRF のカスタム ルート識別子、 SVI ベースの IOS XE VRF-Lite 接続、ボーダー スパイン ロール、およびボーダーゲートウェイ スーパー スパインを使用した 3 層トポロジの強化されたボーダー接続が含まれます。 詳細については、「*Campus VXLAN ファブリック設定の編集*」の記事を参照してください。
使いやすさ	ファブリックグループ全体の分析、アドバイザリ、および接続の可視性	単一のファブリック グループ コンテキストから接続されたファブリックをモニターおよびトラブルシュートします。オペレータは、分析とアドバイザリを表示し、接続とファブリックのバグをレビューし、接続分析を起動し、メンバー ファブリック全体のエンドポイントを調べ、サポートされているすべてのファブリック グループ タイプのファブリック間接続の正常性を監視できます。 詳細については、これらの記事を参照してください： • 「*ネットワークの分析とトラブルシューティング*」 • *Nexus Dashboard での異常の検出* • *Nexus Dashboard でのアドバイザリの識別* • *ファブリック グループについて*
セットアップの容易さ	モニタ モードでのイメージ管理	外部およびクラシック LAN ファブリックのソフトウェア イメージをモニター モードのままで準備および管理し、アップグレード計画中のモードの変更と運用上の負担を軽減します。 詳細については、「*ファブリック ソフトウェアの管理*」の「モニタ モードでのイメージ管理」セクションを参照してください。
使いやすさ	Nexus H1 および H2 プラットフォームのファブリック レベルの NetFlow 自動化	Nexus Dashboard からファブリック レベルの NetFlow 構成を生成して、Nexus H1 および H2 スイッチのフローの可視性を拡張します。 詳細については、*[ファブリックとファブリック グループの作成（Creating Fabrics and Fabric Groups）]* 項目の [ネットフロー サポートの構成（Configuring Netflow support）] セクションを参照してください。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
使いやすさ	Catalyst センター アシュアランスで共存	Nexus Dashboard を使用して、Catalyst 9000 ベースのキャンパス ファブリックで VXLAN EVPN 構成をプロビジョニングできると同時に、スイッチがテレメトリおよびアシュアランス データを Catalyst Center にストリーミングできます。NetFlow およびデバイストラッキングに関連するアシュアランス関連の設定ポリシーは、これらの環境の Catalyst Center から Catalyst 9000 スイッチにプッシュできます。Nexus Dashboard には、アシュアランス ポリシー関連のインテントを更新して、スイッチの実行コンフィギュレーションとの同期を保つ機能があります。 これにより、Catalyst Center のワイヤレス アシュアランス関連機能は、キャンパス EVPN ファブリックを管理する Nexus Dashboard と引き続き共存できます。 詳細については、「*Nexus Dashboard LAN ファブリックの接続の操作*」の「インターフェイスの編集」セクションおよび「*キャンパス VXLAN ファブリック設定の編集*」の記事の「Catalyst Center Assurance インターフェイス フィールド」の項を参照してください。

新しい SAN 自動化機能

表 4 新しい SAN 自動化機能

製品への影響	特長	説明
使いやすさ	SAN 向け CyberArk 資格情報の管理	企業ログイン情報の統治を SAN 運用に拡張します。Nexus Dashboard は、Credential-Store キーを使用して CyberArk から Cisco MDS ファブリック検出とデバイスのログイン情報を取得できます。これにより、ローカルに保存されたログイン情報が削減され、SAN ワークフローのログイン情報のローテーションが簡素化されます。 詳細については、「*SAN ファブリックの作成と編集*」の記事の「SAN スイッチ のデバイスログイン情報の編集」セクションおよび「*システム設定の操作*」の 記事の「SAN ファブリックの AAA リモート認証パススルー」の項を参照してください。

新しいオーケストレーション機能

表 5 新しいオーケストレーション機能

製品への影響	特長	説明
使いやすさ	構成のばらつきの検出と調整の拡張 アプリケーション テンプレートの構成のばらつきへのサポート	より多くの Orchestrator テンプレートのプロパティでアプリケーションのインテントを保護します。Nexus Dashboard は、EPG とブリッジドメイン サブネット、ブリッジドメイン DHCP ラベル、EPG 静的ポート、コントラクト関係、および uSeg 属性のばらつきを検出して調整するようになりました。 詳細については、「*ACI ファブリックのテンプレートの概要と操作*」の「ACI ファブリックのテンプレートの概要と操作」 の「構成のばらつきと アプリケーション テンプレートのばらつきの調整」 セクションを参照してください。
	同じ名前ポリシーおよび自律テンプレートの関連ポリシーのインポートとデプロイメントのサポート	カテゴリベースのフィルタリングにより、適切な設定ポリシーテンプレートを迅速に見つけ、統合された show running-config のようなビューで結果のインテントを確認します。関連する親ポリシーと子ポリシーが一緒に表示されるため、生成された設定のデプロイメント前の理解と検証が容易になります。 詳細については、「*Nexus Dashboard LAN または IPFM ファブリックの構成ポリシーの操作*」の「簡素化されたポリシーテンプレートの選択と複合構成ビュー」セクションを参照してください。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明

新しいモニタリングおよびオブザーバビリティ機能

表 6 新しいモニタリングおよびオブザーバビリティ機能

製品への影響	特長	説明
使いやすさ	実用的な異常抑制とアップグレード対応の相関	アラート疲れを減らし、根本原因の分析を迅速化します。 環境に関連しない異常を抑制し、ファブリック全体にルールを適用し、異常から直接ルールを作成します。ACI ソフトウェアの更新中に、関連付けによって、コントローラまたはスイッチの更新イベントを関連する異常の根本イベントとして識別できます。 詳細については、「*Nexus Dashboard の異常の検出の*」記事の「異常から異常のルールを作成する」、「異常のルール」、および「異常相関について」セクションを参照してください。
使いやすさ	VXLAN ファブリックのエンドツーエンドのマルチキャストパスの可視性	最初のホップルータからラストホップ ルータまでの完全なビューを使用して、マルチキャスト配信のトラブルシュートを行います。 テナント ルーテッド マルチキャスト（TRM）を使用する VXLAN EVPN データ センター ファブリックでは、 Nexus ダッシュボードは Cisco N9000 スイッチからのマルチキャストルートと状態を可視化し、送信元と受信者の統計情報を提供し、トラフィックと受信者の数による上位のマルチキャストグループを識別します。 詳細については、「Nexus Dashboard LAN ファブリックの接続の操作」の「マルチキャスト トラフィック モニタリングの概要」の項を参照してください。
使いやすさ	Live Protect の強化	セキュリティ態勢と保護ステータスを 1 か所で確認します。デバイス セキュリティ ページの新しい概要タブには、セキュリティ アドバイザリ、Live Protect デプロイメント ステータス、ヒット数、および過去の傾向が統合されているため、オペレータはリスクを特定し、保護を検証し、アクションの優先順位付けことができます。 詳細については、「*Nexus Dashboard を使用したセクション アドバイザリの管理*」の「概要」セクションの記事を参照してください。
使いやすさ	プロアクティブなスケール コンプライアンス モニタリング	運用に影響を与える前にキャパシティ リスクを特定できます。 Nexus Dashboard は、ファブリック テレメトリ リソースがクラスタ プロファイルの検証済み制限に近づくか、または超えると異常を発生させ、影響を受けるリソース、現在の使用状況、検証済みの制限、使用率、影響、および推奨される修復を提供します。 詳細については、「*Nexus Dashboard のシステム ステータスの確認*」の記事の「スケール規則遵守の異常」セクションを参照してください。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
使いやすさ	サーバー NIC テレメトリによるエンドツーエンドの AI ジョブの可視性	ネットワーク ファブリックを介して GPU とサーバー NIC からの AI ワークロードのパフォーマンスを関連付けます。 AI ジョブのモニタリングは、外部 AI ファブリックをサポートし、GPU およびスイッチ インターフェイスのデータとともに CRC エラー、破棄、帯域幅、NACKs、CNP、動作状態、リンク速度などのサーバー NIC メトリックを追加します。 詳細については、「*人工知能ファブリックの拡張分析の理解*」を参照してください。
使いやすさ	トラフィック分析互換モードの sFlow のサポート	サポートされているプラットフォームでトラフィック分析互換モードを有効にする場合は、NetFlow に加えて sFlowを使用して異種ファブリック間でトラフィックの可視性を拡張します。 詳細については、*「Silicon One（S1）プラットフォームのトラフィック分析サポート」*を参照してください。
使いやすさ	Cisco Silicon One プラットフォームのトラフィック分析	サポートされている Cisco Silicon One プラットフォームに対してトラフィックの可視性を拡張します。 Nexus Dashboard は、NX- OS 10.6（3） 以降を実行している Silicon One ベースの Cisco N9000 スイッチで NetFlow 互換モードをサポートし、Cisco N9000 -C9804、Cisco N9000 -C9808、および G200 スイッチで sFlow をサポートします。サポートされるモードは、スイッチ プラットフォームによって異なります。Cloud スケール専用の従来のファブリックは、引き続き Netflow 互換モードを使用します。 詳細については、*「Silicon One（S1）プラットフォームのトラフィック分析サポート」*を参照してください。

新しいハードウェア機能

次に、このリリースでサポートされる新しいハードウェアのリストを示します。

表 7 新しいハードウェア機能

製品への影響	特長	説明
ハードウェアサポート	Cisco N9164E-NS4-O サポート	AI ルーテッド、外部、およびクラシック LAN ファブリックで NX-OS 10.6（2n）リリースを実行している Cisco Nexus N9164E-NS4-O を管理します。 サポートはレイヤ 3 操作に限定されます。 SVI、vPC、ポートチャネル、マルチキャスト、 VLAN、PACL、VACL、 VXLAN、接続性分析、NetFlow、sFlow、トラフィック分析、およびフローテレメトリは、このプラットフォームではサポートされていません。
	Cisco Nexusプラットフォームの SONiC サポート	Nexus Dashboard の操作を SONiC を実行している Cisco N9164E-NS4-O および Cisco N93108TC-FX3 スイッチに拡張します。これらのプラットフォームは、ルーテッド、AI ルーテッド、および外部ファブリックでサポートされています。 詳細については、これらの記事を参照してください： • *ファブリックとファブリック グループの作成* • *AI データ センター ルーテッド ファブリック設定の編集* • *ルーテッド ファブリック設定の編集* • *外部ファブリック設定の編集*
	統合されたイメージ管理による拡張された Catalyst プラットフォームのサポート	キャンパス VXLAN および外部ファブリック操作を Catalyst C9300L-24P-4G、C9300L-48P-4G、C9200CX-12P-2X2G-E スイッチ、および Cisco Secure Router 8475-G2 および 8455-G2 プラットフォームに拡張します。サポートには、ソフトウェアイメージ管理（SWIM）

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

製品への影響	特長	説明
		と、サポートされているすべての Catalyst switch のロールが含まれます。
	LAN ファブリック全体でのCisco Nexus N9348Y12C-SE1 のサポート	すべての Nexus Dashboard LAN ファブリック タイプで NX- OS 10.6（4）を実行している Cisco Nexus N9348Y12C-SE1 を展開して管理します。 詳細については、これらの記事を参照してください： • *AI データ センター ルーテッド ファブリック設定の編集* • *AI データ センター VXLAN ファブリック設定の編集* • *キャンパス VXLAN ファブリック設定の編集* • *クラシック LAN ファブリック設定の編集* • *データセンター VXLAN ファブリック設定の編集* • *外部ファブリック設定の編集* • *メディア用 IP ファブリック（IPFM）ファブリック設定の編集* • *ルーテッド ファブリック設定の編集*

注： Cisco Nexus 9000 シリーズは Cisco N9000 シリーズになりました：

- N9200（以前の名前は、Nexus 9200 です）
- N9300（以前の名前は、Nexus 9300 です）
- N9400（以前の名前は、Nexus 9400 です）
- N9500（以前の名前は、Nexus 9500 です）
- N9800（以前の名前は、Nexus 9800 です）
- N9300 スマート スイッチ

3 ノード vND 大規模および 5 ノード vND アプリケーション小規模/大規模展開のサポート終了

これらのクラスタは、 Nexus Dashboard リリース 4.3.1 でのグリーンフィールド展開としてはサポートされていませんが、リリース 4.3.1 にアップグレードする場合は次がサポートされます：

- 3 ノード仮想クラスタ アプリケーション大規模（1.5 TB ストレージのアプリ ノード）
- 5 ノード仮想クラスタ アプリケーション大規模（1.5 TB ストレージのアプリ ノード）
- 5 ノード仮想クラスタ 大規模（500 G ストレージのアプリ ノード）

これらのクラスタ タイプは、次のリリースのアップグレード オプションとしてはサポートされません。*展開およびアップグレード Cisco Nexus Dashboard* に記載されている手順を使用して、新しいクラスタ タイプの 3 ノードリモート対応クラスタ（データ ノード）または 3 ノード物理クラスタに移行することを推奨します。

ガイドラインと制約事項

- Nexus Dashboard 機能のガイドラインと制限については、機能の記事を参照してください。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

- 互換性の詳細については、「互換性情報」を参照してください。

サポートされているアップグレード パス

プラットフォームとその個々のサービスが 1 つの製品に現在統合されました。その結果、サービスの展開、構成、アップグレードを個別に行う必要がなくなり、すべての管理が統合プラットフォームを通じてまとめて処理されます。

詳細については、『*Cisco Nexus Dashboard展開およびアップグレード ガイド*』の「3.2.2 からの ND のアップグレードで サポートされているアップグレード パス」 または「4.1.1 からの ND のアップグレードで サポートされているアップグレード パス」セクションを参照してください。

動作における変更

Nexus Dashboard 4.3.1 の動作の変更

これらのセクションでは、 Nexus Dashboard 4.2.1 と比較して、 Cisco Nexus Dashboard 4.3.1 で導入された動作の変更のカテゴリについて説明します。

システム レベルの統合された変更

表 8 システム レベルの統合機能の動作変更

動作変更カテゴリ	説明
システム レベルの統合機能	バックアップと復元への変更 バックアップの復元時にクラスタ名が変更された • Nexus Dashboard リリース 4.2.1 では、クラスタ名はバックアップと一致するように変更されませんでした。 • Nexus Dashboard リリース 4.3.1 では、フェデレーテッド クラスタとスタンドアロン クラスタの両方で、バックアップを復元するときに、ローカル クラスタ名がバックアップと一致するように変更されるようになりました。バックアップを作成したクラスタの名前は、復元が実行されるときに使用される名前です。詳細については、「*Nexus Dashboard のバックアップと復元*」を参照してください。
	API スキーマ検証 Nexus Dashboard（ND）リリース 4.3.1 以降、システムはバックエンド処理の前に、公開された API スキーマに対してすべての API 要求を検証します。主な変更点と要件は次のとおりです： • 検証動作：スキーマに準拠しない要求は拒否されるようになりました。以前のリリースでは、システムが準拠していないデータを受け入れたり、無視したり、正規化したりしている場合があります。 • 検証範囲：スキーマ検証は、要求ペイロード、クエリ パラメータ、パス パラメータ、フィールド タイプ、必須フィールド、サポートされている列挙値、およびオブジェクト構造に適用されます。 • アップグレードの影響：統合または自動化ワークフローが誤ったデータ型、必要な属性の欠落、またはスキーマに準拠していない値を送信する場合、リリース 4.3.1 以降へのアップグレード後に検証エラーが発生する場合があります。 推奨アクション： API クライアントと自動化ワークフローを調べて、すべての要求がターゲットNexus Dashboard リリースの API スキーマと一致することを確認します。文書化されたフィールドのみを使用し、必須の属性を指定し、値が期待されるタイプと形式を使用するようにする必要があります。
	セカンダリ クラスタでの ACI のオンボーディングと可視性のサポート

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	• Nexus Dashboard 4.2.1 では、フェデレーションでは、プライマリ クラスタのみが新しい APIC クラスタをオンボードできます。そうしないと、オーケストレーションやテレメトリなどの機能を有効にするためにセカンダリ クラスタで使用できるようになります。 • Nexus Dashboard 4.3.1 では、フェデレーションで、セカンダリ クラスタは、プライマリ クラスタでの明示的なオンボーディングを必要とせずに、APIC を直接オンボーディングできるようになりました。これにより、 ACI ファブリックのマルチクラスタ エクスペリエンスがより合理化されます。
	変更制御が有効になっている場合、自由形式のインターフェイス構成がブロックされる • Nexus Dashboard 4.2.1 では、変更制御が有効になっている間、自由形式のインターフェイス構成が許可されていました。ロールバックおよびプレビュー操作では、提供されるステータスの詳細が制限されており、より狭いロール セットがサポートされています。 • Nexus Dashboard 4.3.1 では、オーバーライド プロパティが設定されていない限り、変更制御が有効になっている場合、インターフェイス構成がデフォルトでブロックされるようになりました。このリリースでは、ワークフローの前に重複または制限された編集をブロックするためのより厳密な検証が導入されています。さらに、ロールバックおよびプレビュー操作により、より明示的なステータス情報と更新されたロールベースのアクセス制御が提供されるようになりました。
	LAN ファブリック テンプレート、検証、および PTP 構成の変更 • Nexus Dashboard 4.2.1 では、LAN ファブリック テンプレートのワークフローは古いフィールド名と列挙値を使用し、一部の省略された設定を空白のままにし、PTP 送信元 IPとインターフェイスをより狭いモデルでプログラムしました。 • Nexus Dashboard 4.3.1 では、LAN ファブリック テンプレート フィールドの名前と値（列挙型）が正規化され、テンプレートは自動的にデフォルト値を適用して、設定が空白にならないようにし、PTP 送信元 IP の派生を自動化します。既存のテンプレート、 API ペイロード、および PTP 設定を見直して一貫性を確保する必要があります。これらの変更は、生成された構成や受け入れられる入力値に影響を与える可能性があるためです。 モニター モードでのスイッチの選択とアップグレード グループの作成 • Nexus Dashboard 4.2.1 で、デバイスまたはファブリックがモニタ モードまたは移行モードの場合、 **ファブリック ソフトウェア デバイス** タブはスイッチの選択を無効にし、更新グループの作成をブロックしました。 • Nexus Dashboard 4.3.1 では、スイッチは選択可能なままであり、モニター モードのファブリックに対して更新グループを作成できます。
	デバイス アップグレードの管理者ロール権限の変更。 • Nexus Dashboard 4.2.1 では、device-upgrade-admin ロールを持つリモート TACACS ユーザーが ND fabric-admin ロールにマッピングされていました。したがって、設定の変更などのすべてのファブリック管理関連の操作は、そのロールを持つユーザーが利用できました。 • Nexus Dashboard 4.3.1 では、device-upgrade-admin ロールを持つリモート TACACS ユーザーは、スイッチのアップグレードの実行のみを許可する新しく導入された ND device-upgrade ロールにマッピングされます。このロールを持つユーザーが実行できる設定変更はありません。
	オーケストレーション テンプレートのテナントベースの RBAC • Nexus Dashboard 4.2.1 では、ロール ベース アクセス コントロール（RBAC）およびユーザーとテナントの関連付けルールにかかわらず、変更が許可されなかったテナントのテンプレートを削除、タグ付けする、送信する、または承認できます。 • Nexus Dashboard 4.3.1 では、そのテナントの権限を持っていない限り、変更が許可されていないテナントのテンプレートを削除、タグ付けする、承認のために送信する、または承認することはできません。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	「デフォルト」という名前のテナントのアップグレード サポート • Nexus Dashboard リリース 4.2 では、テナントはプラットフォーム全体の構造になりました。システムによって作成されたデフォルトのテナントには、以前はテナントをサポートしていなかったアプリケーションのポリシーが含まれます。デフォルトという名前の既存の NDO テナントは、システムが作成したテナントと競合し、リリース 4.2 へのアップグレードが失敗する可能性があります。 • Nexus Dashboard リリース 4.3 では、この競合は、orch-default、ndo-default、tenant-default、または migrated-default のいずれかの名前で既存のオーケストレータ テナントを移行することで解決されます。 APIC のテナント名は引き続き「デフォルト」であり、新しく名前が付けられたデフォルトのテナント（orch-default など）に関連付けられたテンプレートのすべてのポリシーは、 APIC の「デフォルト」という名前のテナントに展開されます。
	分析プロキシには TLS 証明書の検証が必要です • Nexus Dashboard 4.2.1 では、 DCNM ACI 分析プロキシは TLS 証明書の検証を適用せずに接続できます。 • Nexus Dashboard 4.3.1 では、 DCNM ACI 分析プロキシ接続パスは証明書の検証を適用します。信頼されていない、または誤って設定された証明書を持つ展開では、信頼を正しく設定する必要があります。 証明書の管理には RBAC 権限が必要 • Nexus Dashboard 4.2.1 では、より広範なロールを持つ一部の認証済みユーザーが、証明書のアップロード、変更、添付、または削除を実行できます。 • Nexus Dashboard 4.3.1 では、これらの証明書管理アクションには、より具体的な RBAC 権限が必要です。許可されたユーザーが証明書の管理を続行できるようにするには、必要に応じてユーザー ロールを更新する必要があります。
	SMTP 電子メール サーバー ホストのアップグレード検証 • Nexus Dashboard 4.2.1 では、アップグレードの検証で、smtpHost 値が OpenAPI ホスト名スキーマに従っていない SMTP 電子メール サーバー構成がブロックされませんでした。このような設定は、続行され、アップグレード後にホスト名検証エラーで失敗する場合があります。 • Nexus Dashboard 4.3.1 では、構成された SMTP 電子メール サーバーに空のまたは無効な smtpHost がある場合、 のアップグレードはブロックされます。アップグレードを続行するには、ホストが有効な RFC 1123 のホスト名または IP アドレスである必要があります。
	vND OVF デプロイメントの構成 • Nexus Dashboard 4.2.1 では、 IP とサブネット マスクの両方を取得する管理ネットワーク フィールドは 1 つだけです。例：192.168.1.100/24。 • Nexus Dashboard 4.3.1 には、2 つの独立したフィールドがあります。1 つは「管理ネットワーク IP アドレス」用、もう 1 つは「管理ネットワーク マスク」用です。これにより、VMware OVF テンプレートの制限を超えて、より適切な検証処理が可能になります。

自動化

表 9 自動化機能の動作の変更

動作変更カテゴリ	説明
自動化	Nexus Dashboard GUI への変更 モニタ対象ファブリックのファブリック管理の変更 • Nexus Dashboard 4.2.1 では、これらのファブリックに対して一部のアクションが非表示またはブロックされ、新しいファブリックは古いモニタ モードのデフォルトを使用し、モニタされたファブリックは管理ed-state 成功ステータスを表示する場合があります。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	• Nexus Dashboard 4.3.1 では、新しいファブリックはデフォルトでモニター モードにデフォルト、モニター対象のステータスは非該当として表示され、スイッチの選択または更新グループの作成はモニター モードまたは移行モードのファブリックで使用できます。 変更前の検証レポートと結果 変更前検証（PCV）の送信と結果は、要求を再送信するより厳格な入力および結果ルールに従います。 • Nexus Dashboard 4.2.1 では、一部の PCV の送信が受け入れられ、結果はそれほど厳格でないルールで返されていました。 • Nexus Dashboard 4.3.1 では、PCV 送信の要件と結果の処理はより厳しいルールに従います。要求を再送信する前に、PCV 入力を検証し、報告されたすべての入力エラーを修正します。 OpenShift 統合では OpenShift 固有のツールを使用します OpenShift 統合によって生成された証明書のセットアップは、OpenShift 固有のツールに従うようになりました。 • Nexus Dashboard 4.2.1 では、Kubernetes 指向のエンドポイントを介して OpenShift 統合で生成された証明書ツールとコマンドを追加します。 • Nexus Dashboard 4.3.1 では、生成されたワークフローはOpenShift 固有の証明書のエンドポイントとツールを使用します。OpenShift 統合を追加するときに、生成された OpenShift 固有の証明書のコマンドと手順を使用します。 ユーザー設定を保存する前にタイムゾーンを手動で選択する必要があります **ユーザー設定** での手動タイムゾーン制御は、値が選択されるまで保存をブロックするようになりました。 • Nexus Dashboard 4.2.1 では、手動モードでタイム ゾーンを選択せずに **[保存（Save）]** し、選択をクリアするとリストを再度開くことができます。 • Nexus Dashboard 4.3.1 では、タイムゾーンが選択されるまで **[保存（Save）]** は、無効のままになり、値をクリアすると、再度開かずに制御がリセットされます。ユーザー設定を保存する前に手動タイムゾーンを選択 ユーザーに警告するバックアップが進行中です バックアップのアクティブ中に構成が試行され、警告バナーがトリガーされるようになりました。 • Nexus Dashboard 4.2.1 では、ユーザーが変更を試みたときに、構成ワークフローでバックアップが進行中であるという警告が表示されませんでした。 • Nexus Dashboard 4.3.1 では、アクティブなバックアップ中に構成を変更しようとするユーザーに対して、明示的な警告バナーが表示されます。 ファブリックそして全般に追加された設定オプション ファブリックの新しい「設定」オプションがファブリックの全般カードに追加され、ドロワーにファブリック設定が表示されるようになりました。 • Nexus Dashboard 4.2.1 では、設定オプションは使用できません。 • Nexus Dashboard 4.3.1 では、ファブリックの **[全般（General）]** カードに新しい設定オプションが追加され、ファブリック設定がドロワーに表示されます。これは、可視性のみを目的としています。 フィルタ処理可能なテーブルの完全に折りたたみ可能な内訳パネル

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	チャートでフィルタ処理されたすべてのテーブルの内訳パネルが完全に折りたたまれ、展開できなくなります。 • Nexus Dashboard 4.2.1 では、内訳パネルは折りたためませんでした。 • Nexus Dashboard 4.3.1 では、チャートを含むすべてのフィルタ可能なテーブルの内訳パネルが完全に折りたたまれ、展開できなくなっています。 ファブリックグループのジャーニーの実装 • Nexus Dashboard 4.2.1 では、ファブリック グループ ジャーニー ページは Nexus Dashboard UI で使用できません。 • Nexus Dashboard 4.3.1 では、ジャーニー ページがファブリック グループに追加され、ファブリック グループの構成プロセスに従いやすくなりました。 デフォルトの ログイン情報エラー ポップアップ • Nexus Dashboard4.2.1 では、デフォルト ログイン情報を持つユーザーのログイン中に警告は表示されません。 • Nexus Dashboard 4.3.1 では、デフォルト ドメインに関係なく、テナントのログイン情報を持つユーザーのログイン時に警告が表示されるようになりました。これにより、以前の DCNM および NDFC のリリースと一致する従来の動作が復元されます。この検証チェックは、オーケストレーションが有効になっており（Orchestrator のみ）、すべての SAN ファブリック構成の場合、vND-app small に対してバイパスされます。
	Nexus Data Broker（NDB） 接続作成ページでの Redirect-all オプションのサポート • Nexus Dashboard 4.2.1 には、 ACE プログラミングで redirect-all コマンドをプログラムするオプションがありません。 • Nexus Dashboard 4.3.1 では、 Redirect-all チェックボックス オプションが接続作成ページに導入されています。デフォルトでは、このオプションは無効になっています。 入力ポートおよび ISL ポートに導入された新しい CDP 許可ルール • Nexus Dashboard 4.2.1 には、CDP 許可ルールはプログラムされていませんでした。 • Nexus Dashboard 4.3.1 では、CDP 許可 ACE ルールは、デフォルトで ISL ポートと入力ポートでプログラムされます。 PTP 機能の変更 • Nexus Dashboard 4.2.1 では、NDB コントローラが PTP 機能、送信元 IP アドレス、およびインターフェイス構成をプログラムします。 • Nexus Dashboard 4.3.1 では、NDB コントローラは、外部グランド マスターまたはピア ネイバーのいずれかのデバイス接続に基づいて、PTP 機能、送信元 IP アドレスをプログラムします。 ドメインを構成するオプションも提供します。 NDB ファブリックでの実稼働デバイスとしての LAN ファブリックのサポート • Nexus Dashboard 4.2.1 では、ACI ファブリックのみがデータ ブローカ ファブリックにオンボーディングできました。 • Nexus Dashboard 4.3.1 では、LAN ファブリック（Classic LAN、Enhanced Classic LAN、VXLAN、Campus VXLAN、VXLANibgp）がサポートされており、データ ブローカ ファブリックにオンボードできます。 Data Broker ファブリックの概要ページで、「コントローラ」タブの名前が「実稼働ファブリック」に変更されました。これらのファブリックは、SPAN 接続先とセッションを作成するために使用できます。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	レガシーコントローラ API は、テナントに関連付けられた VXLAN ファブリックおよびファブリックグループでの CRUD 操作をサポートしなくなりました • Nexus Dashboard 4.2.1 では、テナントが関連付けられている （CRUD） VXLAN ファブリックおよびファブリック グループへのアクセスに、レガシー コントローラ（NDFC）API を使用しないでください。テナントに関連付けられたファブリックへのアクセスには、新しく公開されたオープン API を使用します。 • Nexus Dashboard 4.3.1 では、レガシー コントローラ（NDFC） API は、テナントが関連付けられている VXLAN ファブリックおよびファブリック グループにアクセスしたり、CRUD 操作を実行したりできません。テナントに関連付けられたファブリックへのアクセスには、新しく公開されたオープン API を使用します。
	変更管理を使用した自由形式のインターフェイス構成 変更制御が有効になっているときに、インターフェイス設定をフリーフォーム ポリシーに追加する動作が変更されました。 • Nexus Dashboard 4.2.1 では、変更制御が有効になっている場合、インターフェイス構成をスイッチ、ファブリック、またはブートストラップ フリーフォーム ポリシーに追加できませんでした。 • Nexus Dashboard 4.3.1 では、[管理（Admin）] > [システム設定（System Settings）] > [ファブリック管理（Fabric Management）] > [詳細設定（Advanced Settings）] > [LAN ファブリック（LAN-Fabric）] の配下に、変更管理が有効な場合でもフリーフォームポリシー内でのインターフェイス設定を許可するという新しいフラグが追加されました。これを有効にすることで、フリーフォーム ポリシー内でインターフェイス設定を行うことが可能になります。このフラグはデフォルトでは無効になっています。この設定は、 TAC サポートの詳細設定およびオプションの表示オプションが有効になっている場合にのみ使用できます。
	アップグレード後のレイヤ 4（L4）からレイヤ 7（L7）へのルート ピアリング スタティックルートに複数のネクスト ホップがある場合、L4 から L7 のルート ピアリングがアップグレード中に再編成されます。 • Nexus Dashboard 4.2.1 では、ネクスト ホップを一緒に表すことができました。 • Nexus Dashboard 4.3.1 では、 Nexus Dashboard 4.3.1 にアップグレードすると、ネクスト ホップごとに個別のルート ピアリング構成が作成され、そのツール チップはそのネクスト ホップを識別します。 アップグレード後に、生成されたルートピアリングを確認します。
	デフォルトテナント リソースのレイヤ 4（L4）~レイヤ 7（L7）サービス テナント対応ファブリックのデフォルトテナント リソースに対して L4~L7 サービスを設定できるようになりました。 • Nexus Dashboard 4.2.1 では、L4-L7 サービスはテナント対応ファブリックでは使用できませんでした。 • Nexus Dashboard 4.3.1 では、リソースがデフォルトのテナントに属し、アカウントが all-tenant-domain アクセス権を持っている場合、ワークフローが許可されます。 デフォルトのテナントリソースと、all-tenant-domain アクセス権を持つアカウントを使用します。
	プッシュ ポリシー後のスイッチ ステータス • Nexus Dashboard 4.2.1 では、結果がスイッチの完全な構成状態を表していなくても、スイッチ構成の同期ステータスがプッシュ ポリシー デプロイメントの成功または失敗の結果に誤って設定される場合があります。 • Nexus Dashboard 4.3.1 では、既存の構成同期ステータスはプッシュ ポリシー操作後も保持されます。スイッチにはすでに他の保留中の設定変更がある可能性があるため、ポリシー デプロイメントの結果によって同期ステータスが上書きはありません。 完全な構成を評価し、同期ステータスを更新するには、次の手順を実行します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	ポリシーをプッシュした後、 **設定のプレビュー** または **再同期** を実行する。 プッシュ ポリシー機能自体は変更されていません。構成同期ステータスの処理のみが修正されました。
	AI Monitoredは、ファブリック タイプとして使用できます • Nexus Dashboard 4.2.1 では、モニタ対象の AI はファブリック タイプとして使用できませんでした。 • Nexus Dashboard 4.3.1 では、モニタ対象の をファブリック タイプとして使用できます。 移行アクションは必要ありません。
	ボーダー ゲートウェイ（BGW）のループバック 100 の説明 • Nexus Dashboard 4.2.1 では、BGW ループバック100 の説明はグリーンフィールド展開では利用できませんでした。 • Nexus Dashboard 4.3.1 では、グリーンフィールド展開で ボーダー ゲートウェイ Loopback100 インターフェイスに説明が自動的に追加されます。
	ACI および NX-OS （Nexus One）ファブリック グループ ファブリックおよびネットワーク API 間でアドレス、サブネット、ゲートウェイ、およびスイッチ IP 形式が変更された ファブリック サブネット、ゲートウェイ、 SVI、およびスイッチ IP フィールドは、改訂されたアドレス形式を使用します。 • Nexus Dashboard 4.2.1 では、影響を受けるフィールドでは IPv4 のみ、 CIDR のみ、または cidrv4 および cidrv6 形式が使用されていました。 ◦ サブネットおよびゲートウェイ IP のインポートが受け入れられた /32 および /128 IP 以降の値については、展開時に拒否された。 ◦ トランクとトランクネイティブの 2 種類のポートモードのみがサポートされています。 ◦ テナント名はネットワークを正確に識別するために使用されません。 • Nexus Dashboard 4.3.1 では、フィールドは ipv4WithSubnet、ipv6WithSubnet、またはより広範な IP 形式を使用し、以前は IPv4 のみがサポートされていた IPv6 値を受け入れたり返すことができます。影響を受けるファブリック サブネット、ゲートウェイ、 SVI、およびスイッチ IP フィールドの検証ツールとパーサーを更新します。 ◦ サブネットおよびゲートウェイ IP のインポートは /32 および /128 Ips を受け入れず、これらの値は互換性レポートでフラグが付けられます。 ◦ トランクおよびトランク ネイティブの他に、新しいポート モード「access」が追加されています。 ◦ テナント名は、ネットワークを正確に識別するために使用されます。 セキュリティ グループおよびコントラクト API は、ご利用条件チェックと改訂された要求および応答ルールを適用します。 • Nexus Dashboard 4.2.1 では、一部のセキュリティ グループおよびコントラクトの操作が新しいご利用条件チェックなしで続行され、古い削除応答フィールドまたは TCP フラグ制約が使用されていました。 • Nexus Dashboard 4.3.1 では、影響を受ける API によってご利用条件チェックが適用され、削除応答フィールドが変更され、TCP フラグとステータスの動作が修正されます。 ご利用条件の障害を処理するためのセキュリティ グループおよびコントラクト API コールの更新、フィールドの削除、新しい TCP フラグの動作。 ACI 添付ファイル ワークフローでポート モードを明示的に保持および公開するようになった ACI 添付ファイルの作成、編集、および展開ワークフローでは、ポート モードが明示的に保持されます。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	• Nexus Dashboard 4.2.1 では、影響を受ける添付ファイルはトランク モードを効果的に想定し、ネイティブまたはアクセス インテントを一貫して保持しませんでした。 • Nexus Dashboard 4.3.1 では、添付ファイル モードが明示的に公開され、トランク、トランク ネイティブ、および アクセスの動作はエンド ツー エンドで保持されます。 暗黙的なトランクの動作に依存するのではなく、作成および編集操作中に添付ファイル モードを検証します。 保存/デフォルトの max-PATHS を 1 から 64 に変更し、アップグレード/メタデバイスのケースを修正します。通常の有効な設定は、多くの場合 64/32 のままですが、誤った最大パス 1 と保留中の差分は削除されます。ACI-ISN リンクには影響しません。
	外部ファブリックの選択とホスト ポートの再同期の変更 外部ファブリック添付ファイルとホストポートの再同期により、スイッチのロールがフィルタリングされ、変更された vPC 状態が異なる方法で回復するようになりました。 • Nexus Dashboard 4.2.1 では、スパイン スイッチがマルチアタッチの選択で表示され、vPC 構成のアウトオブバンド削除後にホスト ポートの再同期が失敗する場合があります。 • Nexus Dashboard 4.3.1 では、スパイン スイッチは選択からフィルタ処理され、再同期により、影響を受ける vPC ピアのペアリングを自動的に解除し、スタンドアロン スイッチとしてレンダリングできます。
	外部サービスのIP検証と IPv6 プールのデフォルトが変更された 管理プールの到達可能性の検証と IPv6 リソースプールのシーケンシングで、より厳密なデフォルトが使用されるようになりました。 • Nexus Dashboard 4.2.1 では、 IP 検証はアドレスごとに 3 秒間のタイムアウトで 5 回の ping を使用し、IPv6 自動割り当ては .0 で開始できます。 • Nexus Dashboard 4.3.1 では、検証は1 秒間のタイムアウトと SIM 到達可能性チェックで 2 つの ping を使用し、IPv6 自動割り当ては .1 で開始されます。.0 で始まる IPv6 プールの前提を置き換え、より短い ping および SIM 到達可能性チェックに合格するアドレスを選択します。
	SNMP 検証およびデフォルト 動作の変更 SNMP コミュニティとユーザーテンプレートのワークフローにより、より厳密な検証と改訂されたプライバシーのデフォルトが適用されます。 • Nexus Dashboard 4.2.1 では、一部のコミュニティ文字列とテンプレート フィールドは緩やかに検証され、authNoPriv は具体的なプライバシー プロトコルのデフォルトを割り当てることができます。 • Nexus Dashboard 4.3.1 では、無効なコミュニティ値とテンプレート値が以前に拒否され、authNoPriv はプライバシー プロトコルのデフォルトを割り当てなくなりました。無効な SNMP入力を修正し、authNoPriv の暗黙的なプライバシー プロトコル値への依存を停止します。

テレメトリ（Telemetry）

表 10 テレメトリ機能の動作の変更

動作変更カテゴリ	説明
テレメトリ（Telemetry）	デフォルト ファブリック設定パラメータの変更：AI QoS および Queuing - RoCEv2 • Nexus Dashboard 4.2.1 では、RoCEv2 DSCP のデフォルト値：26 • Nexus Dashboard 4.3.1 では、RoCEv2 DSCP のデフォルト値：24 ~ 31 この変更は、アップグレード シナリオには影響しません。Nexus Dashboard を以前のリリースからアップグレードし、 QoS ポリシーがすでに構成されている場合、Nexus Dashboard 4.3 は既存の RoCEv2 DSCP 値を保持します。

©2026 Cisco and/or its affiliates. All rights reserved.

動作変更カテゴリ	説明
	トラフィック分析互換モードでの NTP の必要性 トラフィック分析互換モードの時刻同期の前提条件が変更された • Nexus Dashboard 4.2.1 では、トラフィック分析互換性モードで PTP を有効にする必要がありました。 • Nexus Dashboard 4.3.1 では、 NTP を設定する必要があり、PTP は必要なくなりました。トラフィック分析互換モードを有効にする前に、 NTP を設定して確認します。
	接続された TAC の変更 • Nexus Dashboard 4.2.1 では、Connected TAC （faststart）フローを無効にできません。使用される管理者ユーザーとテレメトリクラスタが必要であり、Intersight に要求されました。 • Nexus Dashboard 4.3.1 では、Nexus Dashboard の UI 上で「Connected TAC（faststart）」フローを無効にしたり、Nexus Dashboard ユーザー（showtechの収集に使用されるデバイス認証情報に対応）を設定したりすることが可能です。また、コロケーションでのデプロイメントにおいては、（NX-OS) コントローラ クラスタを Intersight に接続し、要求しておく必要があります。
	接続された TAC アクションにより、有効化、権限、およびより厳密なコマンド チェックが適用されるようになります 接続された TAC、callhome、およびプロキシ アクションにより、イネーブルメント、ビジー状態、ロール、コマンド、およびクレデンシャルのチェックが適用されます。 • Nexus Dashboard4.2.1 では、これらのワークフローはより回数変更可能で、広範なロール アクセスで、厳密ではない検証でした。 • Nexus Dashboard 4.3.1 では、無効またはビジー要求を拒否できます。接続された TAC エンドポイントにはスーパー管理者ロールが必要で、コマンドとログイン情報はより厳密に検証されます。 アクションを再試行する前に、「ネットワーク管理者」アカウントを活用、Connected TAC を有効にし、アクティブな操作をクリアし、コマンドまたはログイン情報の失敗を修正します。
	削除または廃止システム異常 システム異常とテレメトリ プラットフォーム カバレッジの低下。 • Nexus Dashboard 4.2.1 では、影響を受けるシステム異常が生成され、C9200CX がテレメトリ収集のためにサポートされていました。 • Nexus Dashboard 4.3.1 では、影響を受けるシステム異常が削除または廃止、C9200CX のテレメトリ サポートが削除されています。 廃止された異常と C9200CX テレメトリ データのモニタリング依存関係を削除することをお勧めします。
	トラフィック分析の互換性により、サポートされていないスイッチがスキップされる サポートされていないスイッチで、トラフィック分析の互換性の有効化が失敗したように見えなくなりました。 • Nexus Dashboard 4.2.1 では、サポートされていないスイッチはイネーブルメントの失敗として表される場合があります。 • Nexus Dashboard 4.3.1 では、サポートされていないスイッチは、互換性の有効化中に「失敗」としてマークされるのではなく、スキップされます。
	中断を伴う NX-OS または ACI バグの影響を受けるスイッチでのバグ スキャンおよびログ収集の変更 • Nexus Dashboard 4.2.1 では、影響を受けるスイッチでオンデマンドのログ収集またはバグ スキャン ジョブを実行しても警告は表示されず、スケジュールされたバグ スキャンは自動的に実行されました。 • Nexus Dashboard 4.3.1 では、影響を受けるスイッチのスケジュールされたバグ スキャン ジョブは自動的にスキップされます。これらのスイッチのオンデマンド バグ スキャンまたはログ収集ジョブを開始する前に、システムにより警告が表示され、明示的なユーザー確認が必要になります。スケジュールされたバグ スキャン中にスキップされたスイッチは、**[システム ステータス（System Status）] > [テレメトリ（Telemetry）]** ページに「スキップ」ステータスで

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	表示されます。 注： Nexus Dashboardは、show techの収集が原因で中断が発生する可能性のある潜在的なスイッチを特定できます。この ID では、これらのデバイスで show tech を実行する必要はありません。
	サポートされていないハードウェアの組み合わせが既存のワークフローで早期にブロックされるようになりました PTP およびデバイス アドミッション ワークフローは、サポートされていないハードウェアとイメージの組み合わせを早期にブロックします。 • Nexus Dashboard 4.2.1 では、一部のサポートされていないスイッチ モデルまたはイメージは、PTP の有効化またはデバイス アドミッションを介して続行される可能性があります。 • Nexus Dashboard 4.3.1 では、C9200CX キャンパスの追加とサポートされていない PTP モデルまたはバージョンの組み合わせが、より明確な検証ガイダンスとともに拒否されます。 PTP を有効にするか、デバイスを承認する前に、影響を受けるキャンパスの追加から C9200CX を削除し、サポートされていないスイッチイメージをアップグレードします。
	レガシー クラシック LAN ファブリックは、policy-cam ワークフローから除外されます ポリシー CAM の資格は、手動とスケジュールされた両方の再同期からレガシー クラシック LAN ファブリックを除外するようになりました。 • Nexus Dashboard 4.2.1 では、ワークフローが適用されない場合でも、ファブリックが policy-cam の選択に表示される場合があります。 • Nexus Dashboard 4.3.1 では、レガシー クラシック LAN ファブリックは選択から除外され、定期的なポリシー CAM 再同期は試行されません。ポリシー CAM 再同期およびスケジュール済み同期の手順から、レガシー クラシック LAN ファブリックを削除します。
	AI ファブリックでは、必要なサービスが実行されていない場合、フリート コレクション スクリプトがコレクションをブロックする • Nexus Dashboard 4.2.1 では、必要なサービス（DCGM Exporter、NVIDIA DOCA Telemetry Service（DTS）、または Fluent Bit）のいずれかが実行されていない場合、スクリプトは収集をブロックしません。 • Nexus Dashboard 4.3.1 では、必要なサービス（DCGM Exporter、NVIDIA DOCA Telemetry Service（DTS）、または Fluent Bit）のいずれかが実行されていない場合、スクリプトは収集をブロックします。 GPU/ NICトポロジ フリート コレクタ スクリプトを実行する前に、次のサービスがターゲット GPU サーバーで実行されていることを確認します。 ◦ Data CenterGPU マネージャ（DCGM）エクスポータ ◦ NVIDIA Data Center Infrastructure on a China Architecture（DOCA）テレメトリ サービス（DTS） ◦ Fluent Bit

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

動作変更カテゴリ	説明
	外部異常イベントでは正しい頭字語大文字が使用されます。 外部の syslog と Kafka にエクスポートされた異常イベントの略語が正しい大文字を保持するようになりました。 • Nexus Dashboard 4.2.1 では、頭字語テキストは外部の syslog および Kafka 接続先にエクスポートされる前に小文字に強制されていました。 • Nexus Dashboard 4.3.1 では、頭字語テキストは小文字に変換されなくなり、エクスポートされたイベントで正しい頭字語の文字列が保持されます。大文字と小文字を区別する syslog および Kafka パーサーを更新して、修正された頭字語の大文字を受け入れるようにします。
	トポロジのインポートとビューは、より厳密なファブリック RBAC と更新されたリンク処理に従います トポロジのインポートとトポロジ ビューは、ファブリック RBAC を適用し、BGP 中心のリンクデータを返します。 • Nexus Dashboard 4.2.1 では、参照されるすべてのファブリックに対してファブリック スコープの承認なしでインポートを続行でき、トポロジの結果に LLDP ベースのリンクが含まれる可能性があります。 • Nexus Dashboard 4.3.1 では、アップロードされたコンテンツはインポート前にファブリック レベルの承認についてチェックされ、影響を受けるトポロジ ビューから LLDP リンクがフィルタリングされます。 すべての参照ファブリックに対して承認されたアカウントを活用、それらのビューの LLDP リンクに依存するコンシューマを更新します。
	エンドポイント、VRF、およびネットワークの EPL スナップショット サマリーのカウント間隔の変更 • Nexus Dashboard 4.1 および 4.2.1 では、エンドポイント、VRF、およびリモート対応クラスタ上のネットワークの EPL スナップショットのサマリー数が 1 時間ごとに更新されていました。 • Nexus Dashboard 4.3.1 では、これらの数は 6 時間ごとに更新され、スナップショットの比較は 6 時間の精度で行われます。詳細については、「ネットワークの分析とトラブルシューティング」 項目を参照してください。

オーケストレーション

表 11 オーケストレーション機能の動作の変更

	説明
オーケストレーション	テナントの作成で空の説明が拒否される tenant-create 要求は、明示的な空の説明を拒否するようになりました。 • Nexus Dashboard 4.2.1 では、説明フィールドが空のテナントを作成できます。 • Nexus Dashboard 4.3.1 では、明示的に空の説明は拒否されますが、省略された説明は引き続き有効です。テナントの **[説明（description）]** フィールドを省略するか、すべての作成要求で空でない値を指定します。
	テナントのアップグレードで、 デフォルトという名前のテナントが異なるように処理される

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

	説明
	「デフォルト」という名前のテナントを昇格させると、ローカル名とグローバル名が個別に割り当てられます。 • Nexus Dashboard 4.2.1 では、「デフォルト」という名前のテナントは 3.2.2 から昇格されませんでした。 • Nexus Dashboard 4.3.1 では、「デフォルト」がローカル名として保持され、起動時にグローバル テナント名が割り当てられます。 割り当て後の手順と自動化を更新して、割り当てられたグローバル名を使用し、ローカル名として「デフォルト」を保持します。
	ファブリック ポリシー テンプレートの応答で、機密キーがユーザーに公開されなくなりました。 オブザーバに表示されるファブリック ポリシー テンプレートのGET ペイロードで、NTP、MCP、および MACsec 認証キーが除外されるようになりました。 • Nexus Dashboard 4.2.1 では、オブザーバ ロールの応答にこれらの認証キーが含まれている場合があります。 • Nexus Dashboard 4.3.1 では、ユーザーは応答で NTP、MCP、および MACsec 認証キーの値を表示できなくなりました。
	スケール制限が適用され、スケール制限の異常が報告されるようになりました スケール チェックで、ポリシー オブジェクト、サブネット、EPG、および IP L3Out がカバーされるようになりました。 • Nexus Dashboard 4.2.1 では、サポートされているスケール番号は適用されませんでした。 • Nexus Dashboard 4.3.1 では、 Nexus Dashboard は、テナント、ファブリック、またはモニタリング テンプレートごとに 500 個のポリシー オブジェクト、8000 個のサブネット、6000 個の EPG、およびテンプレートごとに 100 個の IP L3Out で制限違反を報告します。 サポートされている制限を超えるポリシー オブジェクト、サブネット、EPG、およびIP L3Out を削減または再配布します。
	異なるサイトの移行では、最初にソース テンプレートをデプロイメント必要がある 別のサイトの移行でのターゲットのデプロイメントは、以前のソース テンプレートのデプロイメントに依存するようになりました。 • Nexus Dashboard 4.2.1 では、ソース テンプレートとターゲット テンプレート間のデプロイメント順序は適用されませんでした。 • Nexus Dashboard 4.3.1 では、最初にターゲット テンプレートを展開すると、ソース テンプレートを展開するようにユーザーに指示する検証エラーが返されます。 異なるサイトの移行のたびに、ターゲット テンプレートの前にソース テンプレートを展開します。
	設定のばらつきの検出に子ポリシーが含まれるようになりました。 設定のばらつきのモニタリングには、 Nexus Dashboard が所有する親ポリシーの子が含まれるようになりました。 • Nexus Dashboard 4.2.1 では、既存の子ポリシーまたは新しく作成された子ポリシーに対する直接 APIC の変更は、親が Nexus Dashboard で所有されている場合、構成のばらつきとして検出されませんでした。 • Nexus Dashboard 4.3.1 では、既存の子ポリシーまたは新しく作成された子ポリシーに対する直接の APIC 変更が構成のばらつきとして検出され、確認と調整に使用できます。

解決済みの問題

その問題点に関する追加情報を表示するには、バグ ID をクリックして、バグ検索ツール（BST）にアクセスします。表の「固定」列は、問題が存在する特定のパッチを示します。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

シスコの製品ドキュメント内のバグ ID を検索するには、 Web ブラウザのアドレス バーに次を入力します：
<*bug_number*> site:cisco.com

例：**CSCwo61222 site:cisco.com**

表 12 Nexus Dashboard の解決済みの問題

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt93725	テンプレートを使用して設定コンプライアンス ルールを作成する場合、「選択したオブジェクトの表示」機能を使用しようとすると、プレビューが失敗することがあります。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCws51848	Nexus Dashboard GUI の ACI ファブリック インベントリにおいて、**[ファブリック サマリ（Fabric Summary）] > [接続（Connectivity）] > [インターフェイス（Interfaces）] >[サブインターフェイス インターフェイス詳細（Sub-Interface Interfaces Details）] > [トレンドと統計（Trends and Statistics）] > [エラー（Errors）] > [エラー詳細（Errors Details）]** と進み、**[エラー詳細（Error Details）]** をクリックし、メインのインターフェース詳細ページにはエラーが存在していることが確認できても GUI 上にデータが表示されません。	4.3.1.175 以降	自動化
CSCwb07730	Nexus Dashboard VXLAN-ACI ファブリック グループのデプロイメントでは、ボーダー ゲートウェイ（BGW）を介してファブリック間でブリッジされるトラフィックが誤ったセキュリティ グループ タグ（SGT）の割り当てで発生する場合があります。この問題は、特に L2VNI に関連付けられた SVI がシャットダウン状態になっている NX-OS BGW をトラフィックが通過する場合に発生します。この設定では、送信元 SGT が誤って「0」とタグ付けされているため、拡張されたネットワーク全体でポリシーの適用に一貫性がありません。	4.3.1.175 以降	自動化
CSCwv16926	同じ場所に配置された Nexus Dashboard デプロイメントでは、Live Protect が有効になっている場合、Live Protect 保護ポリシーの更新は影響を受けるスイッチに適用できず、モニタ モード オプションは Nexus Dashboard に表示されません。その結果、ポリシーの変更は有効にならず、 Nexus Dashboard UI からモニタリングを設定または検証できません。この問題は、共同ホストされたデプロイメントでは発生しません。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt08695	Nexus Dashboard（ND）クラスタのセットアップの復元後に Slack 統合設定が欠落する。	4.3.1.175 以降	一般
CSCwt22977	ACIファブリックのファブリック テレメトリ（FT）およびテレメトリ分析（TA）のテーブルに、間違ったエンドポイント セキュリティ グループ（ESG）名が表示されます。この問題は、ESG が構成された ACI ファブリックが Nexus Dashboard（ND）にオンボードされ、テレメトリが有効になっている場合に発生します。次のシーケンスでは問題が発生します： • ユーザーはテレメトリを無効にしてから、エンドポイント グループ（EPG）、ESG、およびレイヤ 3 出力（L3OUT）を再設定します。 • 再プロビジョニング後、ユーザーはテレメトリを再度有効にします。	4.3.1.175 以降	モニタリング/オブザーバビリティ

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt11065	ユーザーが Nexus Dashboard（ND）でプロトコル定義を作成し、いくつかの DSCP 値を使用してACI にプッシュすると、ND は DSCP プロパティの値をデフォルトで「未指定」としてプッシュします。この問題では、ND が DSCP プロパティの指定されていない値をプッシュしないように、モデルとデータベースを変更する必要があります。	4.3.1.175 以降	一般
CSCwt17198	テナントのデプロイメントは、 Nexus Dashboard UI の NX1、NX2、および ACI ファブリック間で順番に進行しているように見えます。各ファブリックのステータス バーは、同時にではなく、順次完了に移行します。バックエンドの展開が並行して行われる場合でも、順次表示される視覚的なフィードバックにより、ユーザーは展開に時間がかかるように感じる場合があります。	4.3.1.175 以降	自動化
CSCwb33814	Nexus Dashboard のアップグレード時に後方互換性をサポートするために、接続グループ API を使用する場合は、128 文字を超える名前を持つ更新グループが許可されます。ただし、作成または編集時に更新グループ名が最大 128 文字に制限されるように、UI に検証が追加されました。	4.3.1.175 以降	自動化
CSCwt52799	ACI ファブリックでソフトウェア アップグレード分析を実行しようとすると、対応するファブリックにロック記号が表示されます。回避策については、バグ検索ツールの詳細を参照してください。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCwt49667	セキュリティ グループ名には特殊文字を使用できません。 バージョン 4.2 で、システムは次の特殊文字のいずれかを含むセキュリティ グループ名の処理に失敗します： !@#$^=+{} 。これにより、更新プロセス中にエラーが発生し、ユーザー インターフェイスにエラーが表示されます。	4.3.1.175 以降	自動化
（CSC）78591	トラフィック分析インターフェイス フィルタ フロー ルールが構成され、バックアップと復元が試行されると、インターフェイス フィルタがファブリック テレメトリ設定の UI に表示されますが、Nexus Dashboard の構成の復元後にフィルタ構成はデバイスにプッシュされません。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt34011	Kafka コンシューマは、まれな Kafka 再調整イベント中にスタック状態になる可能性があります。この場合、オンデマンド/トリガーされたバグ スキャン要求は処理されず、その後の要求はブロックされます。これにより、手動リカバリが実行されるまで、オンデマンド/トリガーされたワークフローが機能停止します。	4.3.1.175 以降	一般
CSCwt40431	GPU メモリ使用率の異常で、メモリ使用率の値が正しく表示されない。	4.3.1.175 以降	一般
CSCwt41931	クラスタでのバックアップの復元/再設定後、またはテレメトリの一時停止/再開後に、エンドポイント テーブルに内部ファブリック ネットワークのリンクが EP として（ファブリック内に）表示されます。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt42224	シングル ノード クラスタで「acs reboot clean」を使用してクリーンリブートを実行すると、ノードがアクティブに戻らないため、クラスタが破損する可能性があります。	4.3.1.175 以降	一般
CSCwt42921	Nexus Dashboard 3.2 から 4.2 にアップグレードした後、エンドポイントの vCenter エンリッチメント情報はエンドポイント テーブルに表示されません。	4.3.1.175 以降	一般

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt43518	サブ コマンドを使用してデバイスのアウトオブバンドで VLAN が設定されている場合、異なるビューと保留中の構成の並列ビューの VLAN 範囲 CLI には VLAN は含まれません。サブコマンドを持つ VLAN 行のブロックのみが表示され、Device show run で表示されても VLAN CLI のリストは表示されません。	4.3.1.175 以降	自動化
CSCwt46057	v3.2x から v4.1 または v4.2 にアップグレードした後、自動作成されたマルチサイト アンダーレイ リンクを持つマルチ クラスタ ファブリック グループ（MCFG）で、セカンダリ クラスタの管理対象メンバー ファブリックが、ボーダーゲートウェイのインターフェイスを追加します。 これは、アップグレード前にアンダーレイ リンクがデフォルト以外の最大パス値を使用するように手動で更新されなかった場合に発生します。	4.3.1.175 以降	自動化
CSCwt52763	テナントの展開が成功し、展開する保留中のインテントがない場合でも、スイッチの設定同期ステータスが「Pending」と表示されます。	4.3.1.175 以降	自動化
CSCwt46809	ToR スイッチがブラウンフィールド インポートを使用して VxLAN ファブリックに追加された後、ネットワークは ToR スイッチのホスト インターフェイスとアップリンク アクセス ポート チャネルから切断されます。	4.3.1.175 以降	自動化
CSCwt49616	マルチクラスタ ファブリック グループにセキュリティ グループが有効になっており、ND 4.1 のネットワーク ポート セレクタを持つセキュリティ グループがあった場合、プライマリ クラスターが ND 4.2 にアップグレードされると、ネットワーク ポート セレクタは ND 4.2 で失われます。 また、デフォルトセキュリティ グループに関連するコントラクト数は入力されません。	4.3.1.175 以降	自動化
CSCwt51427	ND 3.2 または 4.1 から 4.2 へのアップグレード後、 接続 、仮想インフラストラクチャを介してセキュリティ グループ（SG）を VM に関連付けると、その後の展開中に、同じ VRF 内の他の SG の既存の VM 派生セレクタが無効になる可能性があります。	4.3.1.175 以降	自動化
CSCwb08868	基盤となる VPC がダウンした場合、BGP ダウン異常は生成されません。	4.3.1.175 以降	自動化
CSCws90654	IPv4 スタックのない Nexus Dashboard クラスタでネイティブSplunk を使用して Splunk UI を起動し、管理およびデータ ネットワーク アドレスにのみ IPv6 を使用しても機能しません。	4.3.1.175 以降	一般
CSCwt07507	Nexus Dashboard からテレメトリが有効になっている場合、nxsecure 機能がスイッチで無効になっていても、クエリnxsecure ポリシーへのセンサー パスは存在し続けます。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCws35228	「セキュリティ グループ ESG1 は ESG2 と通信できるか」といった検索と探索でのクエリは、たとえ実際にはそれらの間にトラフィックをブロッキングする直接的な拒否コントラクトが存在していたとしても、両者が同じ優先グループに属しているという理由から、通信可能であると示される場合があります。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCws98701	ACI ファブリックから VXLAN へのテナント ポリシーのインポート：ACI ファブリック グループがネットワーク作成エラーで失敗する。	4.3.1.175 以降	自動化

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt25921	ループバック インターフェイスの IP アドレスは、Cisco IOS-XE Catalyst デバイスのテレメトリ データでストリーミングされません。その結果、これらの IP は Nexus ダッシュボードに表示されません。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt25919	Cisco IOS-XE Catalyst デバイス のNexus Dashboard に OSPF ルータ ID が表示されません。	4.3.1.175 以降	自動化
CSCwt04861	Nexus Dashboard のテナント名が対応する ACI のテナント名と一致しない場合、「Tenant <ND_TenantName> not found on fabric」というエラー メッセージが表示され、インポートが失敗します。	4.3.1.175 以降	自動化
CSCwt11065	ユーザーが Nexus Dashboard（ND）でプロトコル定義を作成し、いくつかの DSCP 値を使用してACI にプッシュすると、ND は DSCP プロパティの値をデフォルトで「未指定」としてプッシュします。この問題では、ND が DSCP プロパティの指定されていない値をプッシュしないように、モデルとデータベースを変更する必要があります。	4.3.1.175 以降	一般
CSCwt14341	VXLAN-ACI ファブリック グループを使用した ACI サイトへの展開は、デプロイメント履歴に表示されません。展開の監査ログのみが使用可能ですが、ACI 展開のデプロイメント履歴は表示されません。	4.3.1.175 以降	自動化
CSCwt17198	テナントのデプロイメントは、 Nexus Dashboard UI の NX1、NX2、および ACI ファブリック間で順番に進行しているように見えます。各ファブリックのステータス バーは、同時にではなく、順次完了に移行します。バックエンドの展開が並行して行われる場合でも、順次表示される視覚的なフィードバックにより、ユーザーは展開に時間がかかるように感じる場合があります。	4.3.1.175 以降	自動化
CSCws26984	VXLAN-ACI のオブジェクトの場合、リリース 4.2 の ACI ファブリックでは「構成同期」機能を使用できず、ステータスの更新は定期ではありません。 ACI オブジェクトは、N/A（作成時）から PENDING（アタッチまたはアタッチ解除された場合）に移行します。PENDING 状態をクリアして、ステータスを N/A に戻すには、「展開」アクションを実行する必要があります。	4.3.1.175 以降	自動化
CSCwb33814	Nexus Dashboard のアップグレード時に後方互換性をサポートするために、接続グループ API を使用する場合は、128 文字を超える名前を持つ更新グループが許可されます。ただし、作成または編集時に更新グループ名が最大 128 文字に制限されるように、UI に検証が追加されました。	4.3.1.175 以降	自動化
CSCwt52799	ACI ファブリックでソフトウェア アップグレード分析を実行しようとすると、対応するファブリックにロック記号が表示されます。回避策については、バグ検索ツールの詳細を参照してください。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCwt49667	セキュリティ グループ名には特殊文字を使用できません。 バージョン 4.2 で、システムは次の特殊文字のいずれかを含むセキュリティ グループ名の処理に失敗します： **!@#$^=+{}** 。これにより、更新プロセス中にエラーが発生し、ユーザー インターフェイスにエラーが表示されます。	4.3.1.175 以降	自動化

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt29261	マルチクラスタ環境で、メンバー クラスタがまだバージョン 4.1 を実行している場合、下位互換性がない特定の 4.2 機能はマルチクラスタ ファブリック グループ（MCFG）では使用できません。 バージョン（4.2 と 4.1）が混在するクラスタが存在する場合、次の制限が適用されます。 • VRF を使用したレイヤ 2 ネットワーク：サポートされていません。UI と API 応答の両方にエラー メッセージが表示されます。 • ファブリック グループのバックアップと復元：サポートされていません。UI と API 応答の両方にエラー メッセージが表示されます。 • セキュリティ ポリシーの更新：セキュリティ グループ、契約、関連付け、およびプロトコルの特定のプロパティに対する変更は許可されません。 • MCFG 構成プレビュー：構成数の追加/削除：UI と API 応答の両方で、4.1 クラスタのスイッチでは構成数の追加/削除は使用できません。 • MCFG 監査レコード：4.1 のすべてのクラスタ ビューから MCFG 監査レコードへのアクセスはサポートされていません。 • srcSecurityGroup または dstSecurityGroup がデフォルトのUNWARE グループ（SG_DEFAULT~GPO_UNAARE、SG_DEFAULT~MyVRF_50001 など）である場合、MCFGSecurityアソシエーションの作成はサポートされません。 • 編集フローでの MCFGSecurityアソシエーションの接続/切断はサポートされていません。接続/切断は、アクションの接続/切断で使用できます。 • ユーザーが MCCFG の説明で Swagger を介して securityGroup/securityContract/securityAssociation/securityProtocol をすでに作成している場合、MCFG 4.1.1g ファブリックのファブリック グループ メンバーの追加はサポートされません。 ネットワーク接続のパフォーマンス：ネットワーク添付ファイルのクエリと更新で、パフォーマンスが低下する場合がある	4.3.1.175 以降	自動化
CSCwr95624	ACI ファブリックとテナントの関連付けを解除しても、テナントはリモート APIC から削除されません。	4.3.1.175 以降	一般
（CSC）78591	トラフィック分析インターフェイス フィルタ フロー ルールが構成され、バックアップと復元が試行されると、インターフェイス フィルタがファブリック テレメトリ設定の UI に表示されますが、Nexus Dashboard の構成の復元後にフィルタ構成はデバイスにプッシュされません。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt34011	Kafka コンシューマは、まれな Kafka 再調整イベント中にスタック状態になる可能性があります。この場合、オンデマンド/トリガーされたバグ スキャン要求は処理されず、その後の要求はブロックされます。これにより、手動リカバリが実行されるまで、オンデマンド/トリガーされたワークフローが機能停止します。	4.3.1.175 以降	一般
CSCwt40431	GPU メモリ使用率の異常で、メモリ使用率の値が正しく表示されない。	4.3.1.175 以降	一般
CSCwt41931	クラスタでのバックアップの復元/再設定後、またはテレメトリの一時停止/再開後に、エンドポイント テーブルに内部ファブリック ネットワークのリンクが EP として（ファブリック内に）表示されます。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt42224	シングル ノード クラスタで「acs reboot clean」を使用してクリーン リブートを実行すると、ノードがアクティブに戻らないため、クラスタが破損する可能性があります。	4.3.1.175 以降	一般

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt42921	Nexus Dashboard 3.2 から 4.2 にアップグレードした後、エンドポイントの vCenter エンリッチメント情報はエンドポイント テーブルに表示されません。	4.3.1.175 以降	一般
CSCwt43518	サブ コマンドを使用してデバイスのアウトオブバンドで VLAN が設定されている場合、異なるビューと保留中の構成の並列ビューの VLAN 範囲 CLI には VLAN は含まれません。サブコマンドを持つ VLAN 行のブロックのみが表示され、Device show run で表示されても VLAN CLI のリストは表示されません。	4.3.1.175 以降	自動化
CSCwt45228	ACI ファブリックから VXLAN ファブリック グループに ポリシーを再インポートすると、同じ名前のブリッジ ドメインがユーザー テナントと共通テナントの両方で再インポートされる場合、重複インターフェイス添付ファイル エラーが発生します。	4.3.1.175 以降	自動化
CSCwt46057	v3.2x から v4.1 または v4.2 にアップグレードした後、自動作成されたマルチサイト アンダーレイ リンクを持つマルチ クラスタ ファブリック グループ（MCFG）で、セカンダリ クラスタの管理対象メンバー ファブリックが、ボーダーゲートウェイのインターフェイスを追加します。 これは、アップグレード前にアンダーレイ リンクがデフォルト以外の最大パス値を使用するように手動で更新されなかった場合に発生します。	4.3.1.175 以降	自動化
CSCwt46630	Colo ファブリックの場合のみ、VM 名とハイパーバイザのリダイレクトはエンドポイント テーブルから機能しません。 • NDFC クラスタで、 vCenter 統合によって学習されたエンドポイントのエンドポイント テーブル内の VM 名またはハイパーバイザリンクをクリックすると、400 エラーで失敗します。 • NDI クラスタで、 vCenter 統合がローカル クラスタで構成されていない場合、エンドポイント テーブルのハイパーバイザリンクをクリックすると、400 エラーで失敗します。 vCenter統合がリモート クラスタで設定されている場合、エンドポイントテーブルの VM 名をクリックすると、「No Data」ページにリダイレクトされます。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwt52763	テナントの展開が成功し、展開する保留中のインテントがない場合でも、スイッチの設定同期ステータスが「Pending」と表示されます。	4.3.1.175 以降	自動化
CSCwt46809	ToR スイッチがブラウンフィールド インポートを使用して VxLAN ファブリックに追加された後、ネットワークは ToR スイッチのホスト インターフェイスとアップリンク アクセス ポート チャネルから切断されます。	4.3.1.175 以降	自動化
CSCwt49616	マルチクラスタ ファブリック グループにセキュリティ グループが有効になっており、ND 4.1 のネットワーク ポート セレクタを持つセキュリティ グループがあった場合、プライマリ クラスターが ND 4.2 にアップグレードされると、ネットワーク ポート セレクタは ND 4.2 で失われます。 また、デフォルトセキュリティ グループに関連するコントラクト数は入力されません。	4.3.1.175 以降	自動化

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	修正 済み	影響を受ける機能
CSCwt51427	ND 3.2 または 4.1 から 4.2 へのアップグレード後、 接続 、仮想インフラストラクチャを介してセキュリティ グループ（SG）を VM に関連付けると、その後の展開中に、同じ VRF 内の他の SG の既存の VM 派生セレクタが無効になる可能性があります。	4.3.1.175 以降	自動化
CSCwt53079	L2 ネットワークの作成およびファブリック/ファブリック グループの追加に関するカスタム ネットワーク テンプレートの問題。 • マルチクラスタ ファブリック グループ（MCFG）では、ユーザー定義のネットワーク テンプレートを使用して L2 ネットワークが作成されると、API 応答は「layer」：「layer2」ではなく「layer」：「layer3」を返します。 • ユーザー定義タイプのネットワークを含むファブリックまたはファブリック グループを MCFG に追加しようとすると、追加操作が失敗し、着信ファブリックは拒否されます。	4.3.1.175 以降	自動化
CSCwt46375	L4 ~ L7 サービスのワークフローから開始されたネットワークの作成がエラーで失敗します。これは、ターゲットのファブリック グループの名前が親のマルチクラスタ ファブリック グループ名と一致しない場合、ワークフローがターゲットのファブリック グループを解決できないために発生します。	4.3.1.175 以降	自動化

未解決の問題

その問題点に関する追加情報を表示するには、バグ ID をクリックして、バグ検索ツール（BST）にアクセスします。表の「存在する場所」列は、問題が存在する特定のパッチを示します。

シスコの製品ドキュメント内のバグ ID を検索するには、 Web ブラウザのアドレス バーに次を入力します：
<*bug_number*> site:cisco.com

例：**CSCwo61222 site:cisco.com**

テーブル 13 Nexus Dashboard の未解決の問題

不具合 ID	説明	存在 する場所	影響を受ける機能
CSCwt47732	設定されたストレージ クォータのしきい値を超える NAS から復元が試行されると、実際の復元を開始する前に Nexus Dashboard の復元が中止されます。	4.3.1.175 以降	自動化
CSCwv82709	Catalyst 9000（Cat9k）スイッチは、不正なパスワード（Base64 形式）で外部ファブリックでのブートストラップ中にトップオブラック（TOR）スイッチとしてプロビジョニングされると、到達不能になります。	4.3.1.175 以降	自動化
CSCwv89975	**[異常（Anomalies）]** ページに表示される行数をデフォルトの（10）から 100 行に増やすと、ページ上の行の選択性が低下し、最大 5 秒間遅れる可能性があります。この遅延は、特に Windows 仮想デスクトップ インフラストラクチャ（VDI）環境で観察されます。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCwww00810	バックアップからNexus Dashboard（共同ホストまたは同じ場所に配置されている）を復元した後、Live Protect Shield ステータスが Nexus Dashboard ファブリック間で一貫して表示されません。	4.3.1.175 以降	一般

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

不具合 ID	説明	存在 する場所	影響を受ける機能
CSCww05274	NX-OS のアップグレードとその後のダウングレード後、Nexus Dashboard に表示される Live Protect 保護ステータスは、スイッチの実際の保護モードと一致しません。保護ポリシーは **モニター** モードのスイッチで正しく復元されますが、 Nexus Dashboard には、アドバイザリ/保護のステータスが誤って「アクティブ/使用可能」と表示されます。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCwv75308	スイッチのクロックが 60 秒を超えるずれから回復している間に、スイッチのタイムゾーンが非 UTC のタイムゾーンから UTC に変更されると、スイッチが必要なタイムゾーン変更通知を送信できない場合があります。その結果、 Nexus Dashboard Insights（NDI）は以前のクロック オフセット状態を保持し、スイッチが同期に戻っても PTP クロックを「非同期」として報告し続けます。	4.3.1.175 以降	モニタリング/オブザーバビリティ
CSCww05954	Nexus Dashboard 3.2 から 4.3.1 にアップグレードした後、既存のファブリックが PolicyCAM スケジュールを作成するために必要な構成イベントを自動的に受信しない場合があります。この問題は、NX-OS PolicyCAM 機能のないリリースからその機能を含むリリースにアップグレードするとき、特にアップグレード前に保証分析の設定が有効になっている場合に発生する可能性があります。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCwv73261	Nexus ダッシュボードからルーテッド ファブリックの SONiC FX3 スイッチをアップグレードした後、アップグレードされたスイッチで 、**管理（Manage）** ページの「SSH Key Mismatch」エラーが表示されます。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCwv33170	特定のファブリックを範囲とするファブリック管理者ロールとセキュリティ ドメインを持つユーザーは、アラート ルール設定を表示できません。	4.3.1.175 以降	自動化
CSCwv25969	スイッチを追加する複数のセッションが異なるファブリック間で並行して開始されると、スイッチの追加が失敗します。REST API を使用してスイッチを追加した場合、スイッチの追加操作が失敗した場合でも、誤ってHTTP 200（成功）を返します。	4.3.1.175 以降	自動化
CSCwv81908	Nexus Dashboard で、有効な IP アドレスに先頭または末尾の空白が含まれている場合、インターフェイス構成の保存は一般的な要求検証エラーで失敗します。インターフェイスは作成または更新されず、エラー メッセージでは障害の原因となったフィールドは特定されません。	4.3.1.175 以降	自動化
CSCww01224	テレメトリが有効なクラスタがブートストラップ後にワーカー ノードを追加するように展開されている場合、4.3.1 へのアップグレードが失敗します。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCww14559	VXLAN-ACI ファブリック グループでは、ルート サーバはオーバーレイ EVPN セッションを Loopback0 から送信する必要があり、他のループバック ID はこのリリースではサポートされていません。	4.3.1.175 以降	自動化

既知の問題

その問題点に関する追加情報を表示するには、バグ ID をクリックして、バグ検索ツール（BST）にアクセスします。表の「存在する場所」列は、問題が存在する特定のパッチを示します。

シスコの製品ドキュメント内のバグ ID を検索するには、 Web ブラウザのアドレス バーに次を入力します：
<*bug_number*> site:cisco.com

©2026 Cisco and/or its affiliates. All rights reserved.

例：**CSCwo61222 site:cisco.com**

表 14 Nexus Dashboard の既知の問題

不具合 ID	説明	存在 する場所	影響を受ける機能
CSCwv20271	ブラウンフィールド ファブリックでは、Live Protect または NX-Secure がスイッチですでに有効になっている場合でも、Nexus Dashboard ではセキュリティ アドバイザリを展開するデバイスを選択できません。 この問題は、ファブリックを Nexus Dashboard にオンボーディングする前に、Live Protect、NX-Secure、または必要なシールドをスイッチで直接設定した場合に発生します。Nexus Dashboard は、既存の Live Protect 設定を自動的に検出または採用しません。セキュリティ アドバイザリを展開するには、Live Protect または NX-Secure を有効にし、 Nexus Dashboard を介して必要なシールドを展開します。	4.3.1.175 以降	自動化
CSCwv67802	3.2.2m から Nexus Dashboard 4.3.1 にアップグレードすると、最大パスと最大 BGP パスが保留中の構成として表示されます。	4.3.1.175 以降	自動化
CSCwv47593	デフォルトの前方誤り訂正（FEC）設定を使用した場合、FX3-SONiC および NX-OS デバイス間の 25G リンクは、互換性がないため確立できません。この問題は、SONiC と NX-OS のデフォルトの FEC モードが一致しないために発生します。	4.3.1.175 以降	自動化
CSCwv93995	L4-L7 サービス構成のカスタム テンプレートを使用してNexus Dashboard リリース 3.2.2m からアップグレードした後、サービス機能への編集操作を行うと、「テンプレートの実行中に予期しないエラーが発生しました」というエラーが発生する場合があります。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード
CSCwv05468	Nexus Dashboard のアップグレードの検証中に、次のようなエラーで検証状態でアップグレードが失敗する場合があります：「有効なホスト名が設定されていない SMTP メール サーバー：<server-name>。アップグレードを続行する前に設定を更新してください。」この問題は、Nexus Dashboard 4.3.1 にアップグレードし、 SMTP 電子メール サーバーが空のまたは無効な SMTP ホスト値で設定されている場合に発生します。	4.3.1.175 以降	ファブリック ソフトウェアのアップグレード

互換性情報

Nexus ダッシュボード クラスタのサイジングの注意事項については、「Nexus ダッシュボード キャパシティ プランニング」ツールを参照してください。

物理 Nexus Dashboard ノードは、次のサーバーをサポートします。

- Cisco UCS-220-M5（SE-NODE-G2）、
- Cisco UCS-225-M6（ND-NODE-L4）、および
- Cisco UCS-C225-M8（ND-NODE-G5S および ND-NODE-G5L）

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

物理的な Nexus Dashboard ノードは、サポートされているバージョンの UCS サーバー ファームウェア（CIMC、BIOS、RAID コントローラ、ディスクおよび NIC アダプタ ファームウェアを含む）を実行している必要があります。

表 15 サポートされている UCS サーバー ファームウェア ()

製品 ID	サポートされているリリース
Cisco UCS-220-M5（SE-NODE-G2）	• 4.2(3b) • 4.2(3e) • 4.3(2.230207) • 4.3(2.250037) • 4.3(2.250045) • 4.3(2.260007) • 4.3(2.260020)
Cisco UCS-225-M6 （ND-NODE-L4）	• 4.3(4.240152) • 4.3(4.242066) • 4.3(5.250001) • 4.3(5.250030) • 4.3(6.250040) • 4.3(6.250053) • 4.3(6.260017) • 4.3（6.260054）
Cisco UCS-C225-M8 （ND-NODE-G5S）	• 6.0(1.250127) • 6.0(1.250131) • 6.0（2.260143）
Cisco UCS-C225-M8（ND-NODE-G5L）	• 6.0(1.250127) • 6.0(1.250131) • 6.0（2.260143）

注：

- 4.3（2.240009）および 4.3（2.240077）リリースは、Cisco UCS-220-M5（SE-NODE-G2）でサポートされているリリースとしてリストされなくなりました。CSCwn56294 に関連する問題により、推奨されません。
- 上記以外のファームウェア バージョンは、標準規格の UCS C220/C225 サーバーでサポートされている可能性がありますが、 Nexus Dashboard アプライアンスではサポートされていないため、問題が発生する可能性があります。
- サポートされている UCS サーバー ファームウェアの詳細については、次を参照してください：
  - 4.3(2) 用ファームウェア ファイル
  - 4.3(6) のファームウェア ファイル
  - 6.0(2) のファームウェア ファイル

VMware ESX で展開された Nexus ダッシュボード仮想ノードでは、VMware vMotion はサポートされていません。

Nexus Dashboard は、Intersight 米国リージョン（「us-east-1」）または EU 地域（「eu-central-1」）で要求できます。

©2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

ブラウザの互換性

Cisco Nexus Dashboard のUI は、 Chrome、 Firefox、 Edge、Safari など、最も一般的なブラウザの最新のデスクトップ バージョンと互換性を持つように設計されています。ほとんどの場合、互換性は最新のリリースより後のバージョンまで拡張されます。

モバイル デバイスとの互換性を保つように設計されていませんが、ほとんどのモバイル ブラウザは Nexus Dashboard UI の大部分をレンダリングできます。ただし、デスクトップまたはラップトップで上記のブラウザを使用することをお勧めします。モバイル ブラウザは、 Cisco Nexus Dashboard で正式にサポートされていません。

検証済みスケーラビリティの制限値

検証済みの拡張性の制限については、『 *Cisco Nexus Dashboard 検証済み拡張性ガイド、リリース 4.3.1*』を参照してください。該当するドキュメントは、 CCO ポータルから直接入手できます。

関連コンテンツ

リリース 4.3.1 の場合、すべてのマニュアルの内容は製品の GUI に直接表示され、ヘルプ センターのリンクからアクセスできます。

ND 4.3.1 のすべてのユーザー コンテンツを検索して表示するには、次の URL に移動します：
https://www.cisco.com/c/en/us/td/docs/dcn/nd/4x/collections/nd-user-content-431.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、ciscodcnapps-docfeedback@cisco.com までご意見をお寄せください。

法的情報

シスコおよびシスコのロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、https://www.cisco.com/c/ja_jp/about/legal/trademarks.html をご覧ください。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）。

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。

© 2026 Cisco Systems, Inc. All rights reserved.

米国本社
Cisco Systems, Inc.
カリフォルニア州サンノゼ

アジア太平洋本社
Cisco Systems (USA), Pte. Ltd.
シンガポール

ヨーロッパ本社
Cisco Systems International BV
Amsterdam, The Netherlands

2023 年 11 月発行

© 2023 Cisco and/or its affiliates. All rights reserved.
Cisco および Cisco ロゴは、Cisco Systems, Inc. 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。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。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」または「partner」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シップ関係が存在することを意味するものではありません。1175152207 10/23

Printed in USA Cxx-xxxxxx-xx 01/20

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。