Cisco Catalyst Center のバナーメッセージ

バナーの概要

ご使用のネットワークで常に最新のベストプラクティスの利点を活用できるように、Catalyst Center はリリースごとに機能設定を自動的に最適化します。

改善された設定がアップグレードに含まれる場合は、明確なバナー通知が表示されます。クリックするだけで更新をすぐに適用できます。機能を再設定したり、手動の手順を実行したりする必要はありません。Catalyst Center がプロセスを処理します。

一部のバナー通知は、特定の IOS-XE バージョンに依存します。必要な IOS-XE バージョンをネットワークデバイスが実行するまで、これらのバナーは非アクティブのままであり、180 日間のタイマーにはカウントされません。

すべてのバナー通知がお客様に適用されるわけではありません。機能の使用状況に基づき、導入された更新に関するバナーのみ表示されます。したがって、ご使用の展開に関連する設定変更についてのみ通知されます。

その他の注意事項については、個々の Catalyst Center リリースノートを参照してください。

バナーの動作：

注： 既存のファブリックは影響を受けません。新しいファブリック プロビジョニングのみがブロックされます。

ワークフロー

1. リリースのアップグレード後、必要な CLI の変更がバナーメッセージで通知されます。
2. 変更を適用するまでの期間は 180 日です。
3. バナーの変更が適用されていない場合、すべてのファブリック プロビジョニング操作は 180 日後にブロックされます。

各バナーの説明

このセクションでは、各 Catalyst Center バナーとその影響について説明します。

クラスター IP の変更

表 1. バナータイトル：クラスター IP の変更

値	説明
追加されたリリース	3.1.3
バナー全文	Catalyst Center の IP アドレスが変更されました。新しい IP アドレスを許可するには、サプリカントベースの拡張ノードのオンボーディング ACL を更新する必要があります。この更新は、新しいサプリカントベースの拡張ノードをオンボーディングする前に必要です。この更新が実稼働ネットワークのトラフィックに影響を与えることはありません。
概要	バックアップおよび復元操作後に、Catalyst Center の IP アドレスが変更され、サプリカントベースの拡張ノード（SBEN）のオンボーディングがファブリックで有効になっている場合に、このバナーが表示されます。 このバナーは、SBEN ACL 設定を新しい Catalyst Center IP アドレスで更新する必要があることを示しています。

値	説明
設定の詳細	ip access-list extended SBEN_MAB_ACL no 10 permit ip any host <IP_address> no 20 permit tcp any host <IP_address> eq www no 30 permit tcp any host <IP_address> eq 443 10 permit ip any host <IP_address> 20 permit tcp any host <IP_address> eq www 30 permit tcp any host <IP_address> eq 443 exit
影響	サプリカントベースの拡張ノードのオンボーディングは、このバナーが適用されるまで機能しません。実稼働ネットワークのトラフィックには影響しません。

ファブリック内の自動化された iBGP の削除

表 2. バナータイトル：ファブリック内の自動化された iBGP の削除

値	説明
追加されたリリース	2.3.7.9
バナー全文	ボーダーノードとコントロールプレーンノード間の自動化された iBGP セッションは、ファブリック操作で不要になるため、設定の簡素化の一環として削除されます。この変更は、レイヤ 3 ハンドオフの自動化された eBGP ネイバーや、手動で設定またはテンプレート化された BGP ネイバーには影響しません。
概要	このバナーは、LISP/PubSub サイトのファブリック内の iBGP 設定を削除します。 このバナーにより、LISP から BGP（内部ボーダー）にインポートされたルートが、SDA-トランジットを使用して接続されているサイトのボーダーといったその他のボーダーで BGP に再配布されます。

値	説明

設定の詳細	SDA トランジットを使用した外部コロケーションボーダー（CP + B）の設定例：
	no ip community-list 84
	no ip community-list 84 permit 844888
	route-map LISP_TO_BGP permit 10
	 match tag 955999
	route-map LISP_TO_BGP permit 15
	 description Set the BGP AS Path to AS Number of BGP Handoff Neighbor
	 set as-path tag
	router bgp 64001
	 address-family ipv4
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX out
	  no neighbor <IP_address> send-community both
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX out
	  no neighbor <IP_address> send-community both
	  exit
	 address-family vpnv4
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX out
	  no neighbor <IP_address> send-community both
	  no neighbor <*IP_address*> route-map DENY_0_FABRIC_PREFIX out
	  no neighbor <*IP_address*> send-community both
	  exit
	 address-family ipv6
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out
	  no neighbor <IP_address> send-community both
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out
	  no neighbor <IP_address> send-community both
	  exit
	 address-family vpnv6
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out
	  no neighbor <IP_address> send-community both
	  no neighbor <IP_address> route-map DENY_0_FABRIC_PREFIX_V6 out
	  no neighbor <IP_address> send-community both
	  exit
	 no neighbor <IP_address> remote-as 64001
	 no neighbor <IP_address> remote-as 64001
	router lisp
	 instance-id 4097
	  service ipv4
	  database-mapping <IP_address>/24 locator-set rloc_537529e3-d852-4475-861a-468c66d0ec25 route-tag 955999 proxy
	 instance-id 4098

値	説明
影響	バナーが実行されると、トラフィックの転送に影響があります。このバナーは、メンテナンス期間中にのみ実行することを推奨します。

サプリカントベースの拡張ノードに対するグループベースのポリシー適用の更新

表 3. バナータイトル：サプリカントベースの拡張ノードに対するグループベースのポリシー適用の更新

値	説明
追加されたリリース	2.3.7.6
バナー全文	サプリカントベースの拡張ノードに対する設定標準が見直され、アップリンク インターフェイスでのグループベースのポリシー適用が明示的に無効になりました。この変更により、これらのノードに対するオンボーディングプロセスの信頼性が向上します。
概要	サプリカントベースの拡張ノード（SBEN）および AP のアップリンクインターフェイスでグループベースのポリシーの適用を明示的に無効にすることにより、SBEN のオンボーディングの信頼性が向上します。
設定の詳細	デイジーチェーン接続された展開におけるファブリックエッジまたは認証済み拡張ノード： template SWITCH_SBEN_FULL_ACCESS_TEMPLATE no cts role-based enforcement exit 認証済み拡張ノード： interface GigabitEthernet1/0/1 no cts role-based enforcement exit
影響	サプリカントベースの拡張ノードをオンボーディングするために、インターフェイス テンプレートに追加します。

AAA サーバーがオンラインに戻るときにクライアントがオープン認証で再認証されない

表 4. バナータイトル：AAA サーバーがオンラインに戻るときにクライアントがオープン認証で再認証されない

値	説明
追加されたリリース	2.3.5.4
バナー全文	AAA サーバーが到達不能になると、一部のエンドポイントは SD-Access ファブリックで認証できません。AAA サーバーが到達可能になっても、認証に失敗したエンドポイントは再認証できません。再認証を有効にするには、すべてのエッジノードと拡張ノードに新しい認証テンプレートを適用する必要があります。新しい認証テンプレートを適用すると、アクティブなクライアントセッションがリセットされることがあります。
概要	AAA サーバーが到達不能になるか、サーバーとの接続をデバイスが失った場合、デバイスはクリティカル音声およびクリティカル VLAN モードになります。AAA サーバーがオンラインに戻ると、クリティカル認証クラスマップに対して、クリティカル音声 VLAN のサービステンプレートのみがアクティブ化されます。データクライアントを再認証できるようにするには、データ用のクリティカル VLAN も設定する必要があります。このバナーは、ファブリックサイトにエッジまたは拡張ノードデバイスが含まれている場合に表示されます。

値	説明
設定の詳細	作業前： class-map type control subscriber match-any IN_CRITICAL_AUTH match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE ! class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE 作業後： class-map type control subscriber match-any IN_CRITICAL_AUTH match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE <<<< After banner application class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE <<<< After banner application match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
影響	このバナーを適用すると、アクティブなクライアントセッションがリセットされる場合があります。

エッジノードおよび拡張ノードの明示的なデバイスプロビジョニング機能オンラインカード追加イベント

表 5. バナータイトル：エッジノードおよび拡張ノードの明示的なデバイスプロビジョニング機能オンラインカード追加イベント

値	説明
追加されたリリース	2.3.4.3
バナー全文	1 つ以上のスタックメンバーまたはラインカードが既存のスイッチに追加されています。追加された新しいスタックメンバーやラインカードで、サイト認証テンプレートを設定する必要があります。
概要	このバナーは、新しいメンバースタックまたはラインカードがファブリックエッジまたは拡張ノードに追加され、明示的なプロビジョニングが必要な場合に表示されます。このバナーを手動で適用して、追加されたポートのデバイスプロビジョニングを開始する必要があります。これは、ファブリック認証が [閉じた（Closed）]、[オープン（Open）]、または [低影響（Low Impact）] に設定されている場合に適用されます。 このバナーは、ポート割り当てまたはポートチャネル用に以前使用されていたポートがあり、インターフェイスが想定されるアクセスモードではなくダイナミック自動に設定されているようなラインカードが検出された場合にも表示されます。このバナーは、新しく追加されたポートが検出されると再表示されることがあります。

値	説明
設定の詳細	認証テンプレートが [閉じた認証（Closed Auth）] の場合： interface Forty1/1/1 no load-interval no switchport voice vlan no switchport access vlan switchport mode access source template DefaultWiredDot1xClosedAuth spanning-tree portfast spanning-tree bpduguard enable dot1x timeout tx-period 7 dot1x max-reauth-req 3 認証テンプレートが [オープン認証（Open Auth）] の場合： interface Forty1/1/1 no load-interval no switchport voice vlan no switchport access vlan switchport mode access source template DefaultWiredDot1xOpenAuth spanning-tree portfast spanning-tree bpduguard enable dot1x timeout tx-period 7 dot1x max-reauth-req 3 認証テンプレートが [低影響（Low Impact）] の場合： interface Forty1/1/1 no load-interval no switchport voice vlan no switchport access vlan switchport mode access source template DefaultWiredDot1xLowImpactAuth spanning-tree portfast spanning-tree bpduguard enable ipv6 traffic-filter IPV6_PRE_AUTH_ACL in ip access-group IPV4_PRE_AUTH_ACL in dot1x timeout tx-period 7 dot1x max-reauth-req 3
影響	この設定変更は、新しく追加されたラインカードまたはスタックメンバーとそのポートに影響があります。

拡張ノードのデイジーチェーン接続の機能強化

表 6. バナータイトル：拡張ノードのデイジーチェーン接続の機能強化

値	説明
追加されたリリース	2.3.3.0
バナー全文	このリリースでは、ポリシー拡張ノードとして動作するサプリカントベースの拡張ノードと Catalyst 9000 シリーズスイッチをデイジーチェーン接続する機能が導入されています。この機能をサポートするために、新しいアクセスコントロールリストとインターフェイス テンプレートが既存のポリシー拡張ノードデバイス上にプロビジョニングされます。
概要	このバナーを使用すると、Catalyst 9000 シリーズのサプリカントベースの拡張ノードをデイジーチェーントポロジでオンボーディングできます。バナーは、サプリカントベースの拡張ノードが有効で、ファブリック内に既存のポリシー拡張ノードが存在する場合に、2.3.3.0 にアップグレードすると使用できます。

値	説明

設定の詳細	template SWITCH_AEN_MAB_TEMPLATE
	  switchport access vlan {en_vlan}
	  switchport mode access
	
	template SWITCH_AEN_FULL_ACCESS_TEMPLATE
	  cts manual
	  policy static sgt 8000 trusted
	  switchport mode trunk
	  access-session host-mode multi-host peer
	
	template SWITCH_AEN_BPDU_TEMPLATE
	  spanning-tree bpduguard enable
	
	ip access-list extended AEN_DHCP_ACL
	  permit udp any any eq 67
	  permit udp any any eq 68
	  deny ip any any
	
	ip access-list extended AEN_MAB_ACL
	  permit ip any host {DNAC_IP}
	  permit ip any host {EN_Subnet_Gateway}
	  permit ip any host {DHCP_Server}
	  permit ip any host {DNS_Server}
	  permit tcp any host {DNAC_IP} eq 80
	  permit tcp any host {DNAC_IP} eq 443
	  permit tcp any host {DNAC_IP} eq 2222
	  permit udp any any eq 67
	  permit udp any any eq 68
	  deny ip any any

影響	影響なし。新機能。

ストリーミングテレメトリの NETCONF 要件を示す SD-Access アシュアランスバナー

表 7. バナータイトル：ストリーミングテレメトリの NETCONF 要件を示す SD-Access アシュアランスバナー

値	説明
追加されたリリース	2.3.3.x
バナー全文	SD-Access アシュアランスは、リアルタイムのアシュアランスデータを収集するために、ファブリックノードのテレメトリサブスクリプションに登録します。これには、ネットワークデバイスを NETCONF で設定し、重要業績評価指標（KPI）をプロビジョニングするテレメトリを有効にする必要があります。 注：NETCONF を有効にするには、[プロビジョニング（Provision）] > [ネットワークデバイス（Network Devices）] > [インベントリ（Inventory）] > [FOCUS：インベントリ（FOCUS: Inventory）] の順に選択して、デバイスを選択し、[アクション（Actions）] > [インベントリ（Inventory）] > [デバイスの編集（Edit Device）] の順に選択して、ネットワークデバイスに Netconf を設定します。 テレメトリ サブスクリプションをプロビジョニングするには、[プロビジョニング（Provision）] > [ネットワークデバイス（Network Devices）] > [インベントリ（Inventory）] > [FOCUS：インベントリ（FOCUS: Inventory）] の順に選択して、デバイスを選択し、[アクション（Actions）] > [テレメトリ（Telemetry）] > [テレメトリ設定の更新（Update Telemetry Settings）] の順に選択します。
概要	SD-Access アシュアランスの場合、ストリーミングテレメトリに登録するには、ファブリックノードが NETCONF でプロビジョニングされている必要があります。 このバナーは、ファブリックアシュアランスでデータを取得するために、すべてのファブリックノードの NETCONF とストリーミングテレメトリを有効にするようにネットワーク管理者に警告します。
設定の詳細	ありません（このバナーは読むだけのバナーです）。
影響	ありません（このバナーは読むだけのバナーです）。

ルートマップ TAG_LOCAL_EIDS の更新

表 8. バナータイトル：ルートマップ TAG_LOCAL_EIDS の更新

値	説明
追加されたリリース	2.3.2.0
バナー全文	特定の展開トポロジでは、ボーダーノードとサイトローカル コントロール プレーン ノード間またはボーダーノードとトランジット コントロール プレーン ノードの間の到達可能性のフラップにより、ルーティングループが作成される場合があります。この可能性に対処するために、ボーダーノード上とサイトローカル コントロール プレーン ノード上にプロビジョニングされた既存のルートマップに additive キーワードが適用されます。additive キーワードを使用すると、BGP コミュニティ値は、単に置き換えられるのではなく、既存のコミュニティ値に追加されます。 SD-Access ファブリックを 2 つ以上の外部 BGP ドメイン間の BGP のトランジットとして使用する展開の場合、このキーワードにより、ファブリックをトランジットとして使用するこれらのドメイン間の既存のルーティングポリシーの動作が変更される可能性があります。
概要	スタンドアロン コントロール プレーンを備えたファブリックサイトでは、サイトボーダーは BGP コミュニティタグのあるトランジット CP からルートを学習します。同じルートが、BGP コミュニティタグのないローカル CP からも学習されます。したがって、リモートサイトボーダーが到達不能になってその後に到達可能になると、ルーティングループが作成されて、トラフィックがドロップされる可能性があります。
設定の詳細	route-map tag_local_eids permit 5 set community 655370 additive
影響	この変更はトラフィックに影響を与えます。

サプリカントベースの拡張ノードの機能

表 9. バナータイトル：サプリカントベースの拡張ノードの機能

値	説明
追加されたリリース	2.3.2.0
バナー全文	このリリースでは、ポリシー拡張ノードとして動作する Catalyst 9000 シリーズスイッチをオプションで認証するための拡張機能が提供されています。この機能を使用するには、ポリシー拡張ノードと関連するエッジノードを IOS XE 17.7.1 以降にアップグレードする必要があります。Identity Service Engine（ISE）は、バージョン 3.1.0 以降にアップグレードする必要があります。 このリリースでは、接続されたエンドポイントをプロファイリングするために ISE に属性を送信するのに役立つ拡張ノードの設定を更新することにより、さらなる機能強化が提供されます。
概要	サプリカントベースの拡張ノードのオンボーディングで、より安全なオプションが使用できるようになりました。これにより、Cisco ISE を介して拡張ノードが認証および承認されます。
設定の詳細	エッジノード： device-sensor filter-list dhcp list iseDHCP option name v-i-vendor-class <---------- 新しい設定 ! <AP プールがファブリックでプロビジョニングされている場合> template ApAutzTemplate access-session interface-template sticky timer 60 <---- 10 から 60 に更新 既存の拡張ノードの場合： ip dhcp snooping <---------- 新しい設定 ip dhcp snooping vlan <vlan-list> <------- 新しい設定 ip dhcp snooping glean <---------- 新しい設定 ! <エッジノードまたは他の拡張ノードに接続しているインターフェイス> ip dhcp snooping trust <---------- 新しい設定 device-sensor filter-list dhcp list iseDHCP option name v-i-vendor-class <---------- 新しい設定 ! <AP プールがファブリックでプロビジョニングされている場合> template ApAutzTemplate access-session interface-template sticky timer 60 <-- 10 から 60 に更新
影響	影響なし。新機能。

SVL ボーダーでの CLI「bgp nopeerup-delay nsf-switchover 1」のサポート

表 10. バナータイトル：SVL ボーダーでの CLI「bgp nopeerup-delay nsf-switchover 1」のサポート

値	説明
追加されたリリース	2.3.2.0
バナー全文	このリリースでは、BGP 設定が更新され、StackWise Virtual メンバースイッチのスイッチオーバー中のコンバージェンス時間が改善されます。この変更は、レイヤ 3 ハンドオフの自動化を使用して設定された StackWise Virtual で動作するボーダーノードに適用されます。
概要	SVL スイッチオーバーが発生すると、組織の内部と外部間のトラフィックのコンバージェンスに 31 秒かかります。ただし、「router bgp <ASN>」の下に「bgp nopeerup-delay nsf-switchover 1」コマンドを追加すると、スイッチオーバー後の組織の内部と外部間のトラフィックのコンバージェンスが 250 ミリ秒以内に短縮されます。
設定の詳細	router bgp <bgp-as> bgp nopeerup-delay nsf-switchover 1
影響	このバナーは、ボーダーで SVL が設定されているファブリックで 2.3.2.0 にアップグレードされると表示されます。 この設定変更は、トラフィックの転送に影響します。このバナーは、メンテナンス期間中にのみ実行することを推奨します。

NETCONF のないデバイスで設定するためのメッセージ

表 11. バナータイトル：NETCONF のないデバイスで設定するためのメッセージ

値	説明
追加されたリリース	2.2.2.x
バナー全文	NETCONF で検出されていないデバイスにサブスクリプションをプロビジョニングするには、NETCONF でデバイスを再検出し、[設定のプッシュを強制（Force Configuration Push）] オプションでテレメトリ設定を更新します。
概要	このバナーは、サイトに割り当てられた一部のデバイスに NETCONF が設定されておらず、必要なすべてのストリーミング テレメトリ サブスクリプションの設定ができないことを警告します。バナーが適用されると、Catalyst Center はこれらのデバイスで必要なテレメトリ サブスクリプションを有効にします。これらのサブスクリプションは、アシュアランスに関する洞察を提供するために必要です。

値	説明
設定の詳細	Catalyst 9500 にプッシュする単一のサブスクリプションの設定例： telemetry ietf subscription 550 encoding encode-tdl filter tdl-uri /services;serviceName=smevent/sessionevent receiver-type protocol source-address <IP_address> stream native update-policy on-change receiver name DNAC_ASSURANCE_RECEIVER
影響	このバナーでは、該当するデバイスの関連するすべてのストリーミング テレメトリ サブスクリプションが設定されます。これらのサブスクリプションは、アシュアランスに関する洞察を提供するために必要です。

RADIUS サーバー稼働状況テスター

表 12. バナータイトル：RADIUS サーバー稼働状況テスター

値	説明
追加されたリリース	2.2.2.x
バナー全文	トランザクションを処理するための RADIUS サーバーの稼働状況と可用性を判断するために、RADIUS の自動化されたテスターは、テストユーザー ID を使用してサーバーに定期的に要求を送信します。このリリースでは、この自動テスト機能のサポートが追加されています。この設定では、デバイスは定期的なテスト認証メッセージを RADIUS サーバーに送信して稼働状態をテストします。この設定は、ポリシー拡張ノードとエッジノード機能で動作するすべてのデバイスに適用されます。この変更を適用すると、RADIUS サーバー設定が更新され、アクティブなクライアントセッションがリセットされる可能性があります。
概要	このバナーは、ファブリックデバイスで RADIUS サーバーがプロビジョニングされている 2.2.2.x より前のリリースからアップグレードすると表示されます。
設定の詳細	radius server dnac-radius_2.2.2.2 address ipv4 2.2.2.2 auth-port 1812 acct-port 1813 timeout 2 retransmit 1 automate-tester username dummy ignore-acct-port probe-on pac key 7 0011100F
影響	バナーを適用すると、アクティブなクライアントセッションがリセットされる場合があります。

スイッチ仮想インターフェイス ファブリック DHCP の更新

表 13. バナータイトル スイッチ仮想インターフェイス ファブリック DHCP の更新

値	説明

値	説明
追加されたリリース	2.1.2.3
バナー全文	VLAN に割り当てられたレイヤ 2 ポートに、関連付けられたクライアントがない場合、スイッチのスイッチ仮想インターフェイス（SVI）は「ダウン」状態のままになります。ファブリックインアボックスや、同じ場所に配置されたボーダーノードおよびエッジノードの展開時に、ファブリック DHCP 機能が正しく動作するためには、SVI が「アップ」状態のままである必要があります。このリリースでは、ファブリックの一部として自動化された SVI の下で適用される「no autostate」コマンドを使用して、この機能を有効にします。これらの変更によって、ダウンタイムが発生することも、ネットワークやクライアントに影響を及ぼすこともありません。
概要	FiAB + FE の展開では、FiAB の SVI がダウンしているため（接続されているクライアントが存在しないため）、DHCP パケットは FE の背後にあるクライアントに到達しません。 これを解決するために、Catalyst Center は、FiAB およびボーダーとエッジデバイスで「no autostate」コマンドを設定します。これにより、SVI が起動して、DHCP パケットを転送できるようになります。
設定の詳細	interface Vlan1021 no autostate
影響	影響なし

エッジノード上の IPv6 対応スイッチ仮想インターフェイスの self-ping

表 14. バナータイトル：エッジノード上の IPv6 対応スイッチ仮想インターフェイスの self-ping

値	説明
追加されたリリース	2.1.2.3
バナー全文	このリリースでは、ファブリックの一部として自動化された IPv6 対応スイッチ仮想インターフェイス（SVI）に対して、エッジノードが self-ping する機能が提供されます。
概要	異なるエッジノードのエニーキャストゲートウェイには同じ IPv6 アドレスが割り当てられます。重複したアドレスが検出されるため、Catalyst Center はエニーキャストゲートウェイの IPv6 アドレスに ping できません。 このバナーを適用すると、Catalyst Center は IPv6 エニーキャストゲートウェイに ping できます。
設定の詳細	interface vlan <vlan> ipv6 nd dad attempts 0
影響	影響なし

アップグレード時のテレメトリ サブスクリプションの設定

表 15. バナータイトル：アップグレード時のテレメトリ サブスクリプションの設定

値	説明
追加されたリリース	1.3.3.x

値	説明
バナー全文	IOS-XE デバイスがネットワークで検出されました。これには、アシュアランスデータの新しいテレメトリ サブスクリプションを有効にし、既存のサブスクリプションの一部をパフォーマンスのために最適化する必要があります。これらのデバイスは、グループベースのポリシー モニタリング テレメトリの新しいサブスクリプションを受信することに注意してください。これらのサブスクリプションをプロビジョニングするためのアクションを実行しますか？
概要	Catalyst Center リリースで新しいテレメトリ機能が導入された場合、このバナーにより、不足しているテレメトリ更新をデバイスに適用するように求められます。デバイス上のテレメトリ サブスクリプションと、現在の Catalyst Center リリースに必要なテレメトリ サブスクリプションが一致しない場合に、このバナーが表示されます。正しいテレメトリが適用されると、バナーが非表示になります。
設定の詳細	<mdt-config-data xmlns=" http://cisco.com/ns/yang/Cisco-IOS-XE-mdt-cfg" > <mdt-named-protocol-rcvrs> <mdt-named-protocol-rcvr> <name>ASSURANCE_RECEIVER</name> <host> <address> <IP_address></address> </host> <protocol>tls-native</protocol> <profile>sdn-network-infra-iwan</profile> <port>25103</port> </mdt-named-protocol-rcvr> </mdt-named-protocol-rcvrs> </mdt-config-data>
影響	このバナーは、デバイスのテレメトリ サブスクリプションを更新します。

エッジノード マルチキャスト スタブ ルーティング（MULTICAST_PIM）

表 16. バナータイトル：エッジノード マルチキャスト スタブ ルーティング（MULTICAST_PIM）

値	説明
追加されたリリース	1.3.3.1
バナー全文	このリリースでは、ファブリックの一部として自動化されているスイッチ仮想インターフェイス（SVI）のマルチキャスト スタブ ルーティングを有効にすることで、エッジノードのマルチキャスト設定が強化されます。エッジノードと対象の受信者の間にマルチキャスト スタブ ルーティングを実装すると、IGMP トラフィックを引き続き通過および転送させながら、PIM 制御トラフィックの全体的な処理が削減されるため、効率が向上します。

値	説明
概要	1.3.3.1 より前の Catalyst Center リリースから新しいリリースにアップグレードするときに、ファブリックの VN でマルチキャストが有効になっていて、同じ VN 内のサブネットでレイヤ 2 フラッディングがアクティブになっている場合に、このバナーが表示されます。 1.3.3.1 より前では、プロトコル独立マルチキャスト - スパースモード（PIM-SM）がエッジノードで使用されていました。このバナーを適用すると、代わりに PIM-Passive がエッジノードに設定されます。 ルーテッドインターフェイスで PIM-Passive を使用すると、インターフェイスで PIM 制御トラフィックは処理も転送もされず、IGMP トラフィックのみが処理または転送されます。これにより、エッジノードは受信側に直接接続されるため、不要な PIM 制御処理が削減されます。
設定の詳細	interface Vlan101 no ip pim sparse-mode ip pim passive
影響	この設定の変更は、マルチキャストトラフィックに影響を与えます。

802.1x オーセンティケータスイッチとしての従来の拡張ノードおよびクリティカル VLAN 認証テンプレートの更新

表 17. バナータイトル：802.1x オーセンティケータスイッチとしての従来の拡張ノードおよびクリティカル VLAN 認証テンプレートの更新

値	説明
追加されたリリース	1.3.3.1
バナー全文	このリリースでは、クリティカル VLAN のエッジノードの認証テンプレートが更新されています。この機能強化の一環として、以前にプロビジョニングされた SGT 値 3999 が認証テンプレートから削除されました。 現在、展開でクリティカル VLAN に SGT 値 3999 を使用している場合、ホスト オンボーディング ワークフロー中にこの値をクリティカル VLAN セグメントに割り当てる必要があります。 このリリースでは、接続されたエンドポイントの 802.1x オーセンティケータとして実行される機能を提供する従来の拡張ノードの設定を更新することにより、さらなる機能強化が提供されます。これらの再設定プロセスが開始されると、有線および無線エンドポイントが完了するまでダウンタイムが発生します。クライアントセッションが中断され、デバイスは AAA サーバーで再認証する必要があります。
概要	Catalyst Center 1.3.3.1 では、クリティカル VLAN の認証プロファイル（IBNS）と、拡張ノードでの認証が機能強化されました。このリリース以降にアップグレードする場合、デフォルトではこれらの機能強化は有効になりません。バナーを使用して手動で有効にする必要があります。 Catalyst Center は、ファブリックエッジデバイスと拡張ノードデバイスの両方の認証テンプレートでクリティカル VLAN 設定を更新します。Catalyst Center は、関連する認証テンプレートを含む拡張ノードの認証設定も更新します。 結果として、クライアントデバイスは拡張ノードで直接認証されるようになります。

値	説明
設定の詳細	SWITCH_INTERFACE_TEMPLATE no switchport mode trunk no access-session host-mode multi-host LAP_INTERFACE_TEMPLATE no switchport mode trunk no access-session host-mode multi-host ApAutzTemplate no switchport mode trunk no access-session host-mode multi-host service-template DefaultCriticalAuthVlan_SRV_TEMPLATE vlan <critical_vlan_id>
影響	認証テンプレートの更新により、ネットワークトラフィックが影響を受けます。この変更によりクライアントセッションがリセットされる可能性があるため、それらのクライアントは Cisco ISE で再認証される必要があります。

ファブリック認証キー - 再試行

表 18. バナータイトル：ファブリック認証キー - 再試行

値	説明
追加されたリリース	1.3.1.7
バナー全文	ファブリック認証キーの更新が正常に完了しませんでした。ファブリックサイトで他の操作を実行する前に、この更新を正常に完了させる必要があります。
概要	ファブリック認証キーの更新に失敗した場合に、操作を再試行するようにこのバナーで通知されます。
設定の詳細	service ipv4 . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- 変更されたキー . . exit-service-ipv4 ! service ethernet . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- 変更されたキー . exit-service-ethernet !
影響	この再設定プロセスが完了するまでは、有線および無線エンドポイントでダウンタイムが発生します。完了したら、ファブリックロールで動作している AireOS ベースの WLC デバイスをすべて再起動します。

ファブリック認証キーの更新

表 19. バナータイトル：ファブリック認証キーの更新

値	説明
追加されたリリース	1.3.0

値	説明
バナー全文	ボーダーノード、エッジノード、およびワイヤレス LAN コントローラ（WLC）がコントロールプレーンノードにプレフィックスを登録する場合、その登録プロセスで認証キーが使用されます。このファブリック認証キーを更新する必要があります。この再設定プロセスが開始されると、完了するまで有線および無線エンドポイントでダウンタイムが発生します。AireOS ベースの WLC デバイスがファブリックロールで動作している場合は、プロセスの完了後にそれらを再起動してください。ワイヤレスの停止を回避するために、バナープッシュを試行する前に、デバイスレベルおよびファブリックレベルでこのファブリック内のすべての WLC を個別に再プロビジョニングして、WLC プロビジョニングにエラーがないことを確認してください。
概要	このバナーにより、ファブリック認証キーを更新するように求められます。以前は、キーに一定の文字列が設定されていました。このバナーを適用すると、ランダムに生成された一意のキーが各ファブリックに設定されます。このバナーは、1.2.x から 1.3.x 以降に移行する際に表示されます。
設定の詳細	service ipv4 . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- 変更されたキー . . exit-service-ipv4 ! service ethernet . . etr map-server <IP_address> key 7 0357020E030C2715175D41554F46595E02 <--- 変更されたキー . exit-service-ethernet !
影響	この処理中、有線エンドポイントおよび無線エンドポイントはダウンタイムになります。

関連技術情報

Catalyst Center に関するその他のドキュメントについては、「Cisco Catalyst Center Documentation」を参照してください。

法的情報

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。マニュアル内の例、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。

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。

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。