Juniper.JN0-480.v2024-06-28.q22

試験コード:	JN0-480
試験名称:	Data Center, Specialist (JNCIS-DC)
認定資格:	Juniper
無料問題数:	22
バージョン:	v2024-06-28
アクセス数:	241
ページビュー数:	220
https://www.jpnpdf.com/Juniper.JN0-480.v2024-06-28.q22-mondaishu.html	

最新問題: **1**
新しいスイッチを Juniper Apstra ソフトウェアに追加しています。[管理対象デバイス] ページには、「OS 隔離済み」ステータスが表示されます。デバイスをブループリントで使用できるようにするための適切な次のステップは何ですか?
A. デバイスを認識します。
B. デバイスをメンテナンス モードから解除します。
C. デバイスのエージェントをインストールします。
D. デバイスをドレイン状態から解除します。
Answer: A (メーッセージを残す**)**
新しいスイッチが Juniper Apstra ソフトウェアに追加されると、最初は「OS-Quarantined」ステータスが表示されます。これは、デバイスがまだ Apstra によって管理されておらず、どのブループリントにも割り当てられていないことを意味します。デバイスをブループリントで使用できるようにするための適切な次のステップは、デバイスを承認することです。これは、デバイスの ID と所有権を確認する手動のアクションです。デバイスを認識すると、ステータスが次のように変わります。
「OOS-Ready」。デバイスをブループリントに割り当てて展開する準備ができていることを意味します12。参考文献
:
* デバイスの管理
* AOS デバイス構成ライフサイクル

最新問題: **2**
Juniper Apstra ZTP サーバーを使用してジュニパーネットワークス デバイスをオンボードする場合、正しいのはどれですか?
A. 使用するデバイス キーは、ZTP サーバー上の dhcpd.conf ファイルで設定できます。
B. 状態は、ZTP サーバー上の ztp.Json ファイルで設定できます。

C. 管理 IP アドレスを事前に決定できません。
D. ホスト名はデバイスのシリアル番号になります。
Answer: B (メーッセージを残す**)**
Apstra ZTP サーバー上の ztp.Json ファイルには、ZTP を使用してオンボードされる各デバイスの構成パラメーターが含まれています。パラメータの 1 つは状態
で、init、ready、in_progress、done、error、disabled のいずれかの値になります。State は、ZTP プロセスにおけるデバイスの現在のステータスを示します。たとえば、状態が準備完了の場合、デバイスが Apstra ZTP サーバーにオンボードされる準備ができていることを意味します。状態が「done」の場合、デバイスが ZTP プロセスを完了し、Apstra サーバーによって管理されていることを意味します。ztp.Json ファイルで状態を手動で設定または変更して、ZTP 中のデバイスの動作を制御できます。詳細については、「Apstra ZTP 設定ファイル」を参照してください。参考文献:
* Apstra ZTP 設定ファイル
* アプストラ ZTP の紹介
* Apstra ZTP を構成する

最新問題**: 3**
Juniper Apstra が単一のサーバー インスタンスで数千のデバイスを拡張および管理できるようにする属性はどれですか?
A. Apstra はクラウド リソースとしてインストールされます。
B. Apstra は NGINX に基づいています。
C. アプストラは OVA として利用可能です。
D. Apstra は分散状態システムです。
Answer: D (メーッセージを残す**)**
Juniper Apstra が単一のサーバー インスタンスで数千のデバイスを拡張および管理できる特徴は、Apstra が分散状態システムであることです。これは、Apstra がグラフ データベースを使用して、ネットワーク トポロジと構成データを複数のサーバー ノード間で分散および複製された方法で保存することを意味します。
これにより、Apstra は高いパフォーマンス、信頼性、可用性を備えた大規模ネットワークを処理できるようになります。Apstra はステートフル オーケストレーション エンジンも使用しており、ネットワークの状態がネットワークの設計と動作の論理表現であるブループリントの意図と常に一致していることを保証します。Apstra は、望ましいネットワーク状態と実際のネットワーク状態の間の不一致を自動的に検出して解決し、ネットワーク内の変更や障害を処理できます。他のオプションは次の理由で正しくありません。
* A. Apstra はクラウド リソースとしてもオンプレミス リソースとしてもインストールできるため、Apstra をクラウド リソースとしてインストールするのは間違いです。Apstra は、VMware ESXi、QEMU/KVM、Microsoft Hyper-V、Oracle VirtualBox などのさまざまなハイパーバイザーに展開できる仮想マシン イメージとして利用できます。Apstra は、アマゾン ウェブ サービス (AWS) や Microsoft Azure などのパブリック クラウド プラットフォームにも導入できます。ただ

し、インストール方法は、分散状態システムのアーキテクチャによって決定される Apstra のスケーラビリティには影響しません。
* B. Apstra は NGINX に基づいているという間違いは、Apstra は NGINX に基づいておらず、Python と Django に基づいているためです。NGINX は、Apstra が Web ユーザー インターフェイスと REST API を提供するために使用する Web サーバーおよびリバース プロキシです。ただし、NGINX は Apstra のコア コンポーネントではなく、分散状態システム アーキテクチャによって決定される Apstra のスケーラビリティには影響しません。
* C. Apstra は OVA として利用可能ですが、Apstra は OVA ではなく OVF として利用可能であるため、誤りです。アン
* OVF (Open Virtualization Format) は、仮想マシン イメージをパッケージ化して配布するための標準フォーマットです。OVA (Open Virtual Appliance) は、OVF と仮想ディスク イメージを含む単一のファイルです。Apstra は、VMware ESXi、QEMU/KVM、Microsoft Hyper-V、Oracle VirtualBox などのさまざまなハイパーバイザーにインポートできる OVF ファイルを提供します。ただし、Apstra を OVF として利用できるかどうかは、分散状態システム アーキテクチャによって決定される Apstra のスケーラビリティには影響しません。参考文献:
* ジュニパー アプストラ アーキテクチャ
* Apstra サーバーの要件/リファレンス
* ジュニパーネットワークス Apstra 4.0 はユーザーとオペレーターのエクスペリエンスを向上させます

最新問題: **4**
5 段階のクロを作成するには、テンプレートでどの生地の種類を選択する必要がありますか?
A. 折りたたまれています
B. 回線交換
C. ラックベース
D. ポッドベース
Answer: D (メーッセージを残す**)**
Juniper のドキュメント 1 によると、5 段階の Clos アーキテクチャにより、複数のポッドを単一のファブリックに相互接続する追加の集約層を備えた大規模なトポロジが可能になります。ポッドは、同じスパイン デバイスを共有するラックのグループです。ラックは、同じサーバーに接続するリーフ デバイスのグループです。Juniper Apstra を使用して 5 段階の Clos ネットワークを作成するには、テンプレート作成ウィザードでポッドベースのファブリック タイプを選択する必要があります。これにより、ネットワーク設計のポッド、プレーン、スパイン、リーフの数を指定できるようになります。したがって、正解は D.pod ベースです。参考資料: 5 段階 Clos アーキテクチャ | アプストラ 4.1 | ジュニパーネットワークス

最新問題: **5**
ジュニパーアプストラを使用。テンプレートで定義されているコンポーネントはどれですか?
A. リーフからスパインへの相互接続
B. スパイン デバイスとリーフ デバイス間のリンクの速度

C. トポロジ内のスパイン デバイスの数
D. IP プールの定義
Answer: (解答を表示する**)**
Juniper のドキュメント 1 によると、テンプレートはネットワークのポリシーの意図と構造を定義する構成テンプレートです。テンプレートは、ネットワーク設計内のラックとポッドのタイプと数に応じて、ラックベースまたはポッドベースのいずれかになります。テンプレートには次の詳細が含まれます。
* ポリシー: オーバーレイ制御プロトコル、ASN 割り当てスキーム、アンダーレイ タイプなど、ネットワーク全体に適用されるパラメーターです。
* 構造: ラック、ポッド、スパイン、リーフの種類と数など、ネットワークの物理的なレイアウトです。この構造は、リーフとスパインの相互接続 (リーフ デバイスとスパイン デバイス間のリンクの数とタイプ) も定義します。リーフからスパインへの相互接続は、冗長性と帯域幅の要件に応じてシングルまたはデュアルにすることができます。
したがって、正解は A. リーフとスパインの相互接続です。これは、ネットワークの物理接続を決定するため、テンプレートで定義されるコンポーネントです。リンクの速度、スパイン デバイスの数、および IP プールの定義は、デバイス プロファイル、リソース プール、またはブループリント設定から派生するため、テンプレートで定義されるコンポーネントではありません。参考資料: テンプレートの紹介 | アプストラ 4.2 | ジュニパーネットワークス

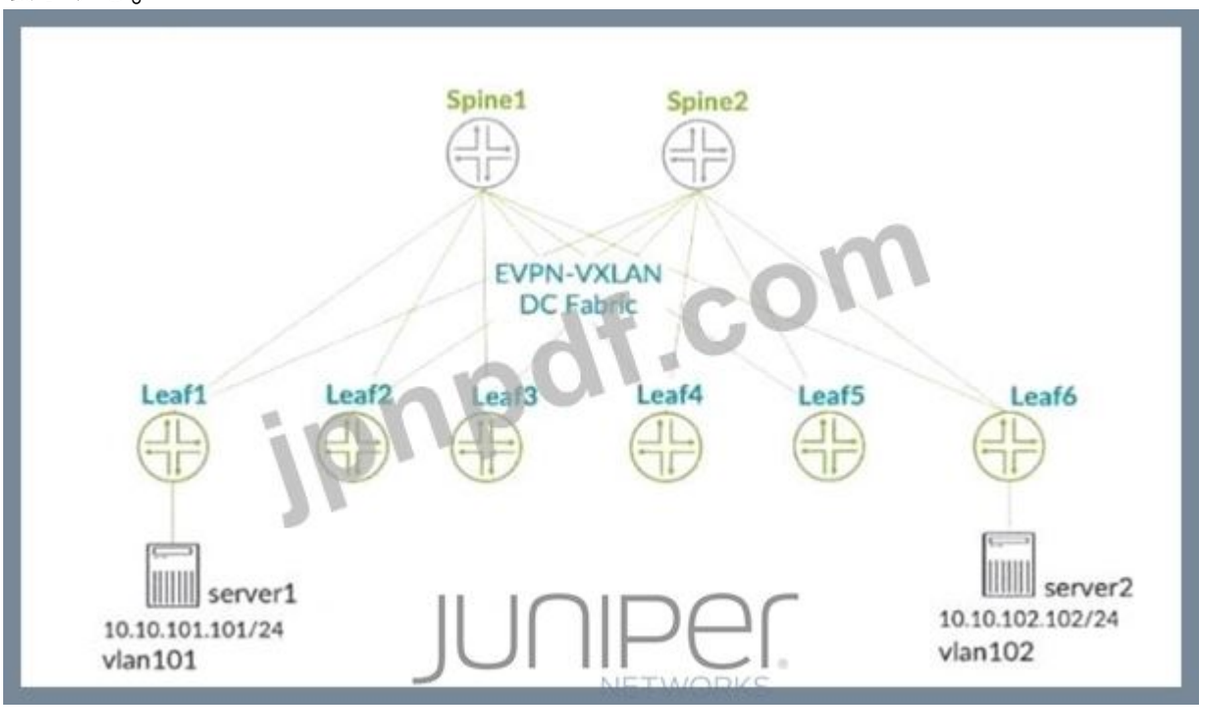
最新問題**: 6**
Juniper Apstra を使用して特定のデバイスにコンフィグレットを適用したいと考えています。このタスクを実行するには、どの 2 つのパラメータを使用しますか? (2つお選びください。)
A. フォームファクター
B. ホスト名
C. ポートグループ
D. タグ
Answer: B,D (メーッセージを残す**)**
Juniper Apstra を使用して特定のデバイスにコンフィグレットを適用するには、デバイスのホスト名とタグを指定する必要があります。ホスト名は、Apstra システム内のデバイスの一意の識別子であり、タグは、同じ特性を共有する他のデバイスとグループ化するためにデバイスに割り当てることができるラベルです。ホスト名とタグを使用して、ブループリント カタログでコンフィグレットを適用するデバイスをフィルタリングできます12。
参考文献:
* コンフィグレットの概要
* Terraform レジストリ

最新問題**: 7**
データセンターに Juniper Apstra サーバーをインストールしています。データセンター内で運用タスクを構成、管理、実行することが期待される複数のユーザーがいます。Apstra サーバーのロールベースのアクセス制御にリモート ユーザー認証を実装することにしました。

このシナリオでは、どの 3 つの方法がサポートされていますか? 3つお選びください。）
A. TACACS+
B. LDAP
C. 半径
D. SAML
E. 認証0
Answer: A,B,C (メーッセージを残す**)**
Apstra サーバーのロールベースのアクセス制御にリモート ユーザー認証を実装するには、TACACS+、LDAP、または RADIUS のいずれかの方法を使用できます。これらは、企業内の個々のユーザーに割り当てられたロールに基づいてユーザーを認証および認可するために Juniper Apstra がサポートするプロトコルです。
これらのプロトコルの 1 つ以上を認証ソースとして使用し、優先順位を指定するように Apstra サーバーを設定できます。リモート認証が失敗した場合に、フォールバック オプションとしてローカル ユーザー アカウントを使用するように Apstra サーバーを設定することもできます。他のオプションは次の理由で正しくありません。
* D. SAML (Security Assertion Markup Language) は、Apstra サーバーのロールベースのアクセス制御のリモート ユーザー認証でサポートされているプロトコルではないため、SAML は間違っています。SAML は、アイデンティティ プロバイダーやサービス プロバイダーなど、さまざまな当事者間で認証および認可データを交換するための XML ベースの標準です。SAML は Web ベースのシングル サインオン (SSO) シナリオでよく使用されますが、Apstra サーバーとは互換性がありません。
* E. Auth0 は誤りです。Auth0 はプロトコルではなく、Web およびモバイル アプリケーションに認証および認可ソリューションを提供するサービスです。Auth0 は、OAuth、OpenID Connect、SAML、JWT などのさまざまなプロトコルと標準をサポートするプラットフォームです。Auth0 は、Apstra サーバーのロールベースのアクセス制御のためのリモート ユーザー認証としてサポートされているサービスではありません。
参考文献:
* ユーザー認証の概要
* [Juniper Apstra] 認証と認可のデバッグ1
* ユーザー認証(API)
* アプストラサーバーを構成する

最新問題**: 8**
5 段階のクロを作成するには、テンプレートでどの生地の種類を選択する必要がありますか?
A. 回線交換
B. ラックベース
C. ポッドベース
D. 折りたたまれています
Answer: (解答を表示する**)**

最新問題: **9**
展示する。



展示に示すように、Juniper Apstra を使用して 2 つのシングルホーム サーバーを接続します。共通のルーティング ゾーン内の 2 つの仮想ネットワークで ERB 設計ブループリントを使用しています。
このシナリオでは、EVPN コントロール プレーンによって自動的に作成される 2 種類の VXLAN トンネルはどれですか? (2つお選びください。)
A. EVPN 信号ルート タイプ 8 VXLAN トンネル
B. EVPN 信号ルート タイプ 3 VXLAN トンネル
C. EVPN 信号ルート タイプ 6 VXLAN トンネル
D. EVPN 信号ルート タイプ 2 VXLAN トンネル
Answer: B,D (メーッセージを残す**)**
Juniper のドキュメント 1 によると、EVPN ルート タイプ 3 は、VTEP の IP アドレスと、それがサポートする VNI をアドバタイズするために使用されます。これにより、VTEP が相互に検出し、共通する VNI の VXLAN トンネルを形成できるようになります。EVPN ルート タイプ 2 は、VTEP に接続されているホストの MAC アドレスと IP アドレスをアドバタイズするために使用されます。これにより、VTEP は、同じ VNI 内のホストの MAC から IP へのバインディングと MAC から VTEP へのマッピングを学習できるようになります。したがって、ERB 設計ブループリントと共通のルーティング ゾーン内の 2 つの仮想ネットワークを備えた Juniper Apstra を使用する場合、これら 2 種類の VXLAN トンネルは EVPN コントロール プレーンによって自動的に作成されます。参考資料: 例: EVPN-VXLAN 中央ルーティング ブリッジング ファブリックの構成

最新問題: **10**

Juniper Apstra UI の管理対象デバイス内で、いくつかのデバイスが OOS 隔離ステータスになっていることがわかります。デバイスをブループリントに追加することはできません。どのアクションがこの問題を解決するでしょうか?
A. デバイスを認識します。
B. 隔離されたデバイスのハードウェアの問題を修正します。
C. 接続が確立されている場合でも、エージェントをインストールします。
D. 新しい初期設定をアップロードします。
Answer: A (メーッセージを残す**)**
エージェントのインストールが成功すると、Juniper Apstra UI を使用して、デバイスはサービス外検疫 (OOS-QUARANTINED) 状態になります。この状態は、デバイスがまだ Apstra によって管理されておらず、どのブループリントにも割り当てられていないことを意味します。この時点のデバイス構成は Pristine Config と呼ばれます。デバイスをブループリントで使用できるようにするには、デバイスを承認する必要があります。これは、デバイスの ID と所有権を確認する手動のアクションです。デバイスを認識すると、ステータスが Out of Service Ready (OOS-READY) に変わります12。参考文献:
* デバイスの管理
* AOS デバイス構成ライフサイクル

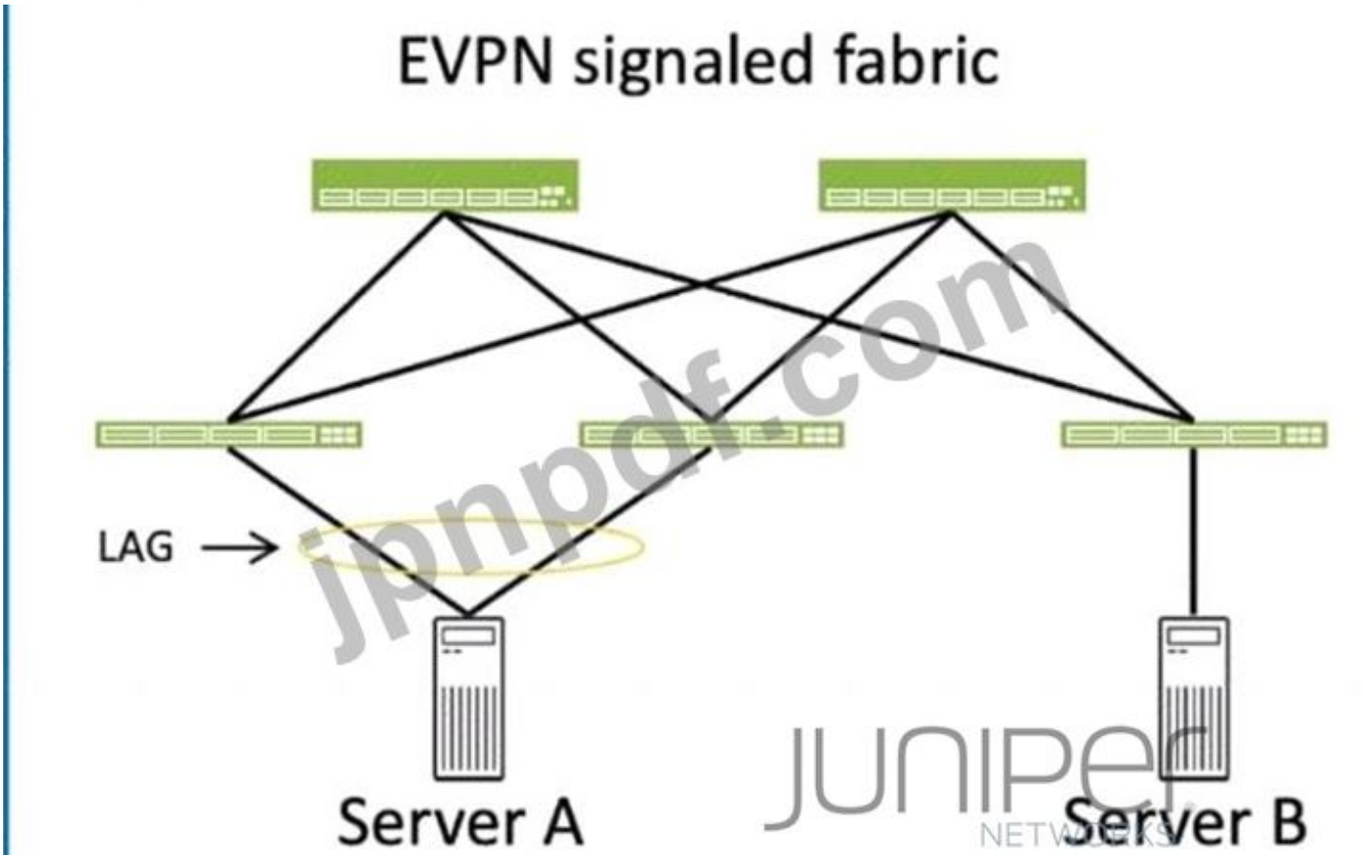
最新問題**: 11**
Juniper Apstra で使用できる 2 つのシステム定義のユーザー ロールは何ですか? (2つお選びください。)
A. 許可されています
B. ルート
C. ビューア
D. ユーザー
Answer: C,D (メーッセージを残す**)**
Juniper Apstra は、Apstra GUI 環境で使用できる 4 つのシステム定義のユーザー ロールを提供します。これらは、administrator、device_ztp、viewer、および user1 です。Web 検索結果に基づいて、次のようなことが推測できます。
* ビューア: このロールには、ブループリント、デバイス、デザイン、リソース、外部システム、プラットフォームなど、Apstra システム内のさまざまな要素を表示するだけの権限が含まれます。この役割を持つユーザーは、要素を作成、編集、削除することはできません12。
* ユーザー: このロールには、ブループリント、デバイス、デザイン、リソース、外部システム、プラットフォームなど、Apstra システム内のさまざまな要素を表示および編集する権限が含まれます。この役割を持つユーザーは、要素を作成または削除することはできません12。
* 承認済み: これは、Juniper Apstra のシステム定義のユーザー ロールではありません。これは、LDAP、Active Directory、TACACS+、RADIUS3 などの外部システムによって認証されたユーザーを表すために使用される用語です。

* root: これは、Juniper Apstra のシステム定義のユーザー ロールではありません。これは、Linux システム上のスーパーユーザー アカウントを表すために使用される用語であり、すべてのコマンドとファイルへの完全なアクセス権を持ちます。Apstra GUI でユーザーを作成しても、そのユーザーは SSH 経由で Apstra プラットフォームにアクセスできません。SSH 経由で Apstra プラットフォームにアクセスするには、ローカル Linux システム ユーザー 4 を作成する必要があります。参考文献:
* ユーザー/ロール管理の概要
* ユーザー/ロール管理 (プラットフォーム)
* AAA プロバイダー
* ユーザープロファイル管理

最新問題**: 12**
Juniper Apstra のロールベースのアクセス制御に関する記述はどれが正しいですか?
A. 閲覧者の役割は事前に定義されており、削除できます。
B. 管理者ロールはすべての権限を表示できます。
C. ユーザー ロールはロールを作成できます。
D. 管理者ロールは、事前定義された唯一のロールです。
Answer: (解答を表示する**)**
Juniper Apstra ロールベースのアクセス制御 (RBAC) は、さまざまなユーザーのロールに基づいてアクセス許可を指定できる機能です。RBAC サーバーは、企業内の個々のユーザーに割り当てられた役割に基づいてネットワーク アクセスを認証および許可するリモート ネットワーク サーバーです1。Juniper Apstra には、管理者、device_ztp、user、viewer2 という 4 つの事前定義されたユーザー ロールがあります。管理者ロールは最も強力なロールであり、Apstra ソフトウェア アプリケーション内のすべての権限を確認し、すべてのアクションを実行できます。管理者ロールは、変更できない 4 つの事前定義されたユーザー ロールを除き、ユーザー ロールを作成、複製、編集、および削除することもできます2。したがって、管理者ロールがすべての権限を参照できるという記述は正しいです。
このシナリオでは、次の 3 つのステートメントは正しくありません。
※閲覧者の役割はあらかじめ定義されており、削除することができます。これは当てはまりません。閲覧者の役割は 4 つの事前定義されたユーザー 役割の 1 つであり、削除できないからです。閲覧者の役割は最も制限された役割であり、ネットワーク情報と構成の表示のみが可能ですが、変更はできません2。
※ユーザーロールはロールを作成できます。ユーザー ロールは 4 つの事前定義されたユーザー ロールの 1 つであり、ロールを作成できないため、これは当てはまりません。ユーザー役割は、ネットワーク構成および管理タスクのほとんどを実行できますが、プラットフォーム設定やユーザー管理機能にはアクセスできません2。
* 管理者ロールは、事前に定義されている唯一のロールです。これは真実ではありません。事前定義されたユーザー ロールは 1 つではなく 4 つあるからです。他の 3 つの事前定義されたユーザー ロールは、device_ztp、user、viewer2 です。

参考文献:
* プロバイダー - Apstra 3.3.0 ドキュメント
* ユーザー/ロール管理 (プラットフォーム)

最新問題: **13**
展示する。



ESI 値に関する 2 つの記述は、展示物に示されているファブリックへのサーバー接続に関して正しいものはどれですか? (2つお選びください。)
A. サーバー A の有効な ESI 値は 0x00.00.00.00.00.00.00.00.00.00 です。
B. サーバー B の有効な ESI 値は 0x00.20.20.20.20.20.20.20.20.20 です。
C. サーバー A の有効な ESI 値は 0x00.10.10.10.10.10.10.10.10.10 です。
D. サーバー B の有効な ESI 値は 0x00.00.00.00.00.00.00.00.00.00 です。
Answer: (解答を表示する**)**
この質問に答えるには、EVPN LAG の ESI 値の概念を理解する必要があります。ESI は、イーサネット セグメントを識別する 10 バイトの値です。イーサネット セグメントは、マルチホーム デバイス (サーバーなど) を EVPN ネットワーク内の 1 つ以上の PE デバイス (リーフ スイッチなど) に接続するリンクのセットです。同じイーサネット セグメントに接続するすべての PE デバイスで同じ ESI 値を設定する必要があります。これにより、PE デバイスが EVPN LAG を形成できるようになり、デバイスのアクティブ/アクティブまたはアクティブ/スタンバイ マルチホーミングがサポートされます。ESI 値は手動で設定することも (タイプ 0)、LACP (タイプ 1) またはその他の方法から自動的に取得することもできます。展示品では、サーバー A は、LACP が有効になった LAG を使用して 2 つのリーフ スイッチ (QFX 5210) に接続されています。サーバー B

は、LACP が有効になっている LAG を使用して 3 つのリーフ スイッチ (QFX 5120) に接続されています。この情報に基づくと、ファブリックへのサーバー接続の ESI 値に関する次の記述は正しいと言えます。
* C. サーバー A の有効な ESI 値は 0x00.10.10.10.10.10.10.10.10.10 です。この ESI 値は QFX 5210 デバイスの LACP 設定から自動的に導出できるため、これは当てはまります。LACP システム ID は通常、デバイスの MAC アドレスに基づいており、LACP 管理キーは
LAGを識別する2バイトの値。たとえば、QFX 5210 デバイスの MAC アドレスが 00:10:10:10:10:10 で LAG ID が 10 の場合、LACP システム ID は 00:10:10:10:10:10 で、LACP 管理キーは 00:0A です。ESI 値は、LACP システム ID と LACP 管理キーを連結することによって導出され、00:10:10:10:10:10:00:0A となります。この ESI 値は、16 進数表記で
0x00.10.10.10.10.10.00.0A として表すことも、ゼロを埋め込んで次のように表すこともできます。
0x00.10.10.10.10.10.00.0A.00.00。この ESI 値は、サーバー A に接続する両方の QFX 5210 デバイスで構成する必要があります。
* D. サーバー B の有効な ESI 値は 0x00.00.00.00.00.00.00.00.00.00 です。この ESI 値はシングルホーム デバイスを示す予約値であるため、これは当てはまります。サーバー B は LAG を使用して 3 つのリーフ スイッチ (QFX 5120) に接続されていますが、どのリーフ スイッチにもマルチホーム化されていません。これは、サーバー B がリーフ スイッチと EVPN LAG を形成するために ESI 値を必要としないことを意味します。代わりに、サーバー B は予約された ESI 値 0x00.00.00.00.00.00.00.00.00.00 を使用できます。これは、サーバー B がシングルホーム デバイスであり、EVPN LAG に参加していないことを示します。この ESI 値は 3 つの QFX すべてで設定する必要があります
サーバー B に接続する 5120 デバイス。ファブリックへのサーバー接続の ESI 値に関する次の記述は正しくありません。
* A. サーバー A の有効な ESI 値は 0x00.00.00.00.00.00.00.00.00.00 です。この ESI 値はシングルホーム デバイスを示す予約値であるため、これは false です。サーバー A は、LACP が有効になっている LAG を使用して 2 つのリーフ スイッチ (QFX 5210) に接続されています。これは、サーバー A が両方に対してマルチホームであることを意味します。これは、サーバー A がリーフ スイッチと EVPN LAG を形成するには ESI 値が必要であることを意味します。ESI 値はイーサネット セグメントごとに一意でゼロ以外である必要があるため、予約されている ESI 値は 0x00.00.00.00.00.00.00.00.00.00 はサーバー A では無効です。
* B. サーバー B の有効な ESI 値は 0x00.20.20.20.20.20.20.20.20.20 です。この ESI 値は QFX 5120 デバイスの LACP 設定から派生したものではないため、これは false です。サーバー B は、LACP が有効になった LAG を使用して 3 つのリーフ スイッチ (QFX 5120) に接続されていますが、どのリーフ スイッチにもマルチホーム化されていません。これは、サーバー B がリーフ スイッチと EVPN LAG を形成するために ESI 値を必要としないことを意味します。代わりに、サーバー B は予約された ESI 値 0x00.00.00.00.00.00.00.00.00.00 を使用できます。これは、サーバー B がシングルホーム デバイスであり、EVPN LAG に参加していないことを示します。ESI値は

0x00.20.20.20.20.20.20.20.20.20 はサーバー B では無効であり、同じ ESI 値を使用する他のイーサネット セグメントと競合する可能性があります。参考文献:
* EVPN LAG のイーサネット セグメント識別子、ESI タイプ、および LACP
* EVPN ネットワークで自動生成された ESI について
* EVPN のイーサネット セグメント: 知っておくべきことすべて

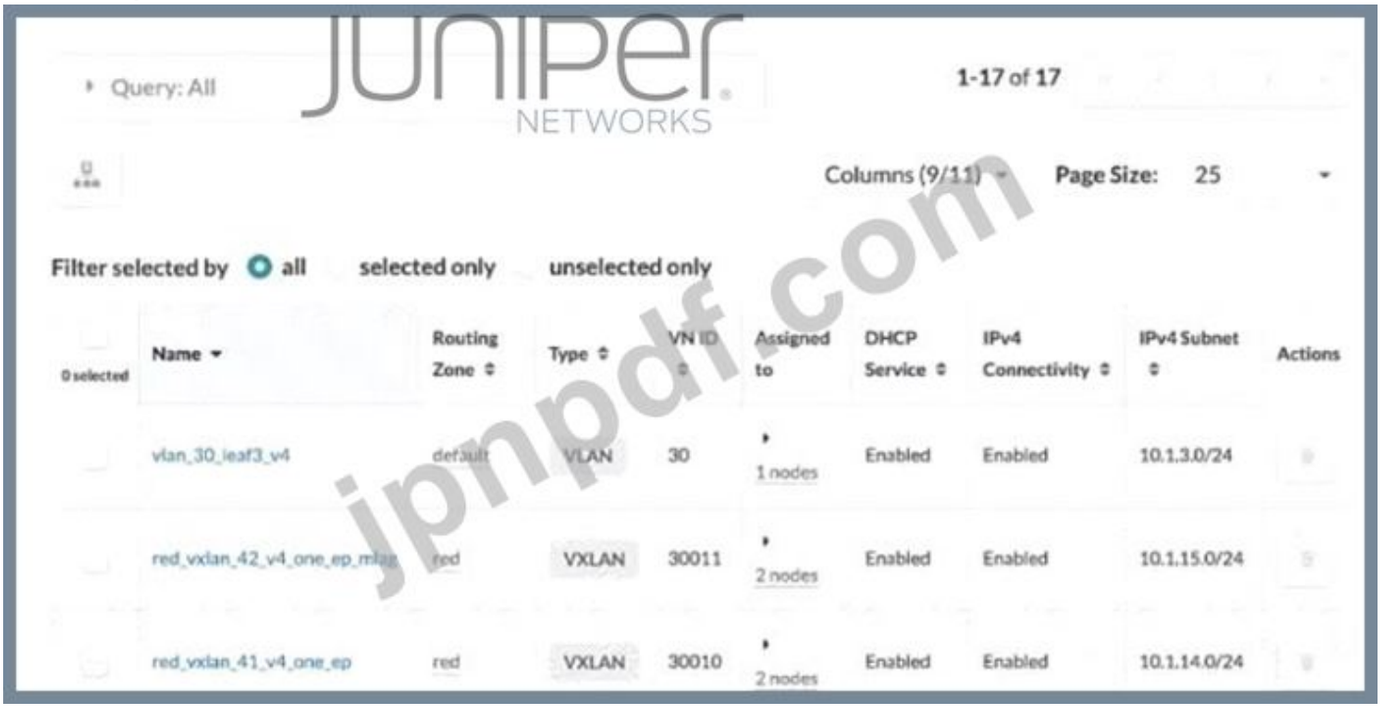
最新問題**: 14**
最近、Juniper Apstra で新しいブループリントを作成した後、変更をコミットしました。メイン ダッシュボードには、BGR に関連する多数の異常が表示されます。これらの異常の考えられる原因は何ですか?
A. ASN の構成が間違っています。
B. ファブリックはまだ収束していません。
C. スパインとリーフのリンクが正しく設定されていません。
D. 汎用システムが構成されていません。
Answer: B (メーッセージを残す**)**
Juniper Apstra では、ブループリントはネットワークの設計と構成を論理的に表現したものです。新しいブループリントを作成するときは、変更をコミットしてネットワーク デバイスに適用する必要があります。ただし、変更をコミットしても、ネットワークがすぐに更新されて動作可能になるわけではありません。ネットワークが収束し、ブループリントの新しい状態が反映されるまでに時間がかかる場合があります。この間、メイン ダッシュボードに BGP に関連する異常が表示される場合があります。これは、BGP セッションがデバイス間で確立されていないか、安定していないことを示します。これらの異常は通常は一時的なもので、ネットワークが収束し、BGP セッションが稼働すると解消されます。したがって、このシナリオではステートメント B がこれらの異常の原因である可能性が最も高くなります。
このシナリオでは、次の 3 つのステートメントがこれらの異常の原因である可能性は低くなります。
* ASN の設定が間違っています。Juniper Apstra は、デバイスの役割に基づいてデバイスに自動的に割り当てることができる ASN プールを提供しているため、これは可能ですが、可能性は非常に低いです。デバイスの ASN を手動で指定することもできますが、ASN が一意であり、ネットワーク設計と一致していることを確認する必要があります。ASN の構成が間違っている場合は、BGP に関連する異常が発生する可能性がありますが、ネットワークが収束した後も異常は消えません。異常を解決するには、ASN を修正し、変更を再度コミットする必要があります。
* スパインとリーフのリンクが正しく設定されていません。Juniper Apstra は、インターフェイス マップに基づいてスパインとリーフのリンクを定義するために使用できる接続テンプレートを提供しているため、これは可能ですが、可能性は非常に低いです。スパインとリーフのリンクを手動で指定することもできますが、それらが正しく、物理的なケーブル配線と一致していることを確認する必要があります。スパイン/リーフ リンクを誤って設定した場合、BGP に関連する異常が発生する可能性がありますが、ネットワークが収束した後も異常は消えません。異常を解決するには、スパインとリーフのリンクを修正し、変更を再度コミットする必要があります。

※汎用システムは構築されていません。汎用システムは Juniper Apstra によって管理されないデバイスですが、ネットワークに接続されているため、これは関係ありません。汎用システムは、Juniper Apstra によって管理されるデバイス間の BGP セッションには影響しません。ネットワーク内に汎用システムがある場合は、それを手動で構成し、ネットワーク設計と互換性があることを確認する必要があります。汎用システムでは、メイン ダッシュボードの BGP に関連する異常は発生しません。
参考文献:
* ブループリントの概要とダッシュボード
* BGP セッション フラッピング プローブ
* プローブ: BGP セッション監視

最新問題**: 15**
EVPN ルートをアドバタイズするためにどのプロトコルが使用されますか?
A. OSPF
B. BGP
C. IS-IS
D. RIP
Answer: B (メーッセージを残す**)**
BGP は、EVPN ルートをアドバタイズするために使用されるプロトコルです。EVPN ルートは、イーサネット VPN の MAC アドレスと IP プレフィックス情報を伝送する新しいタイプの BGP ネットワーク層到達可能性情報 (NLRI) です。EVPN ルートは、MPLS、VXLAN、SR、または SRv6 トンネル上の BGP マルチプロトコル拡張 (MP-BGP) を使用して PE 間で交換されます。EVPN ルートにより、PE は同じ EVPN インスタンス内の異なるサイトの MAC アドレスと IP プレフィックスの到達可能性を学習できます。EVPN ルートは、高速コンバージェンス、冗長性、エイリアシング、サブネット間ルーティングなどのさまざまな機能もサポートしています。他のオプションは次の理由で正しくありません。
* A. OSPF は誤りです。OSPF は自律システム内の IP ルートをアドバタイズするために使用される内部ゲートウェイ プロトコル (IGP) であるためです。OSPF は、イーサネット VPN の MAC アドレスと IP プレフィックス情報を伝送する BGP NLRI の一種である EVPN ルートをアドバタイズするためには使用されません。
* C. IS-IS は誤りです。IS-IS は、自律システム内で IP ルートと MPLS ラベルをアドバタイズするために使用される内部ゲートウェイ プロトコル (IGP) であるためです。IS-IS は、イーサネット VPN の MAC アドレスと IP プレフィックス情報を伝送する BGP NLRI の一種である EVPN ルートをアドバタイズするためには使用されません。
* D. RIP は誤りです。RIP は、自律システム内の IP ルートをアドバタイズするために使用される内部ゲートウェイ プロトコル (IGP) であるためです。RIP は、イーサネット VPN の MAC アドレスと IP プレフィックス情報を伝送する BGP NLRI の一種である EVPN ルートをアドバタイズするためには使用されません。参考文献:
* EVPN の基礎
* RFC 9136 - イーサネット VPN (EVPN) における IP プレフィックス アドバタイズメント

* EVPN タイプ 5 ルート: IP プレフィックス アドバタイズメント
* EVPN Pure Type 5 ルートについて

最新問題: **16**
展示する。



展示を参照して、リストされているすべての VXLAN の IPv6 サブネットを表示するにはどうすればよいですか?
A. 各 VXLAN が個別に選択されている場合に、IPv6 サブネットが表示されます。
B. [列] を選択してから、[IPv6 サブネット] を選択します。
C. すべての VXLAN を選択します。[IPv6 サブネット] 列が表示されます。
D. [IPv6 サブネット] 列は表示されず、IPv6 サブネットが割り当てられている VXLAN がないことを示します。
Answer: B (メーッセージを残す**)**
展示品を参照すると、画像はネットワーク管理と構成に使用される Juniper Apstra ソフトウェア アプリケーションのユーザー インターフェイスを示しています。この図は、[リソース] メニューの [仮想ネットワーク] テーブルを示しています。ここには、ネットワーク内の VLAN と VXLAN の詳細が表示されます。テーブルには 11 列がありますが、画像には 9 列だけが表示されています。他の 2 つの列は IPv6 接続と IPv6 サブネットで、デフォルトでは非表示になっています。リストされたすべての VXLAN の IPv6 サブネットを表示するには、ユーザーは [列] を選択してから、[IPv6 サブネット] を選択する必要があります。これにより、テーブルに IPv6 サブネット列が表示され、IPv6 プールから VXLAN に割り当てられた IPv6 アドレスが表示されます。詳細については、「仮想ネットワーク (リソース)」を参照してください。参考文献:
* 仮想ネットワーク (リソース)
* IPv6 プール (リソース)
* Apstra ユーザーガイド

最新問題: **17**
エージェントのインストールが成功すると、Juniper Apstra UI を使用してデバイスはどの状態になりますか?
A. IS-MAINT
B. OOS 対応
C. OOS 隔離済み
D. アクティブです
Answer: C (メーッセージを残す**)**
エージェントのインストールが成功すると、Juniper Apstra UI を使用して、デバイスはサービス外検疫 (OOS-QUARANTINED) 状態になります。この状態は、デバイスがまだ Apstra によって管理されておらず、どのブループリントにも割り当てられていないことを意味します。この時点のデバイス構成は Pristine Config と呼ばれます。デバイスをブループリントで使用できるようにするには、デバイスを承認する必要があります。これにより、状態が Out of Service Ready (OOS-READY)12 に変わります。参考文献:
* デバイスの管理
* AOS デバイス構成ライフサイクル

最新問題: **18**
組織のメンバーが、Juniper Apstra を使用して事前定義されたインターフェイス マップを変更しました。
このシナリオで正しい 2 つの記述はどれですか? (2つお選びください。)
A. 事前定義されたインターフェイス マップに加えられた変更は、Apstra ソフトウェアには影響しません。
B. グローバル カタログ内のインターフェイス マップを変更すると、次のコミット時に対処する必要がある異常が発生する可能性があります。
C. Apstra がアップグレードされると、事前定義されたインターフェイス マップに加えられた変更はすべて破棄されます。
D. グローバル カタログ内のインターフェイス マップへの変更は、既にブループリント カタログにインポートされているインターフェイス マップには影響しません。
Answer: C,D (メーッセージを残す**)**

Juniper のドキュメント 1 によると、インターフェイス マップは、ベンダー仕様に準拠しながら、論理デバイスと物理ハードウェア デバイス (デバイス プロファイルで表される) の間のインターフェイスをマップする構成テンプレートです。インターフェイス マップは、事前定義またはカスタムのいずれかです。事前定義されたインターフェイス マップは、Apstra ソフトウェアに同梱されており、ほとんどの認定された Juniper デバイスをサポートします。カスタム インターフェイス マップは、特定の要件を満たすためにユーザーによって作成されるマップです。インターフェイス マップは、グローバル カタログまたはブループリント カタログに保存できます。グローバル カタログには、ブループリントで使用できるすべてのインターフェイス マップが含まれています。ブループリント カタログには、グローバル カタログからインポートされ、特定のブループリントで使用されるインターフェイス マップが含まれています。
組織のメンバーが事前定義されたインターフェイス マップを変更する場合、次の記述は正しいです。
* グローバル カタログ内のインターフェイス マップに対する変更は、既にブループリント カタログにインポートされているインターフェイス マップには影響しません。これは、元のバージョンのインターフェイス マップを使用する既存のブループリントが変更の影響を受けないことを意味します。ただし、インターフェイス マップの更新バージョンを新規または既存のブループリントで使用する場合は、グローバル カタログから再度インポートする必要があります。
* 事前定義されたインターフェイス マップに加えられた変更は、Apstra がアップグレードされると破棄されます。これは、変更が Apstra ソフトウェアの異なるバージョン間では保持されないことを意味します。Apstra のアップグレードを通じてカスタマイズされたインターフェイス マップを保持したい場合は、事前定義されたインターフェイス マップを直接変更するのではなく、事前定義されたインターフェイス マップを複製し、一意の名前を付けてカスタマイズする必要があります。
したがって、正解は A と B です。グローバル カタログ内のインターフェイス マップへの変更は、既にブループリント カタログにインポートされているインターフェイス マップには影響せず、事前定義されたインターフェイス マップに加えられた変更は Apstra のアップグレード時に破棄されます。参考資料: インターフェイス マップの編集 | アプストラ 4.2 | ジュニパーネットワークス

最新問題**: 19**
ジュニパー ･アプストラで。どちらの発言が正しいでしょうか？
A. VMware の異常検出はデフォルトでオンになっています。
B. VMware 異常検出には、外部システムで構成された vCenter サーバーが必要です
C. VMware 異常検出には、エクスポートが有効になっている VMware ハイパーバイザーが必要です。
D. VMware の異常検出には、VMware 上で実行されている Apstra サーバーが必要です。
Answer: B (メーッセージを残す**)**
VMware 異常検出は、VMware vSphere 環境の仮想ネットワーク設定と物理ネットワーク設定の可視性と検証を提供する Apstra の機能です。この機能を有効にするには、Apstra は、ESX/ESXi ホストおよび Apstra 管理のリーフ スイッチに接続されている VM を管理する vCenter サーバー

への接続を必要とします。vCenter サーバーは、Apstra Web インターフェイスの外部システムで構成する必要があり、vCenter 統合をブループリントでステージングしてコミットする必要があります。これにより、Apstra は VM、ESX/ESXi ホスト、ポート グループ、および VDS に関する情報を収集し、VM の接続に影響を与える可能性のある不一致や不一致にフラグを立てることができます。他のオプションは次の理由で正しくありません。
* VMware 異常検出はデフォルトではオンになっていません。これを有効にするには、外部システムで vCenter サーバーを構成し、ブループリントに仮想インフラを追加する必要があります。
* VMware 異常検出には、エクスポートが有効になっている VMware ハイパーバイザーは必要ありません。必要なのは、ホスト インターフェイスをリーフ インターフェイスに関連付けるために、VMware 分散仮想スイッチ上で LLDP 送信を有効にすることだけです。
* VMware の異常検出には、VMware 上で実行されている Apstra サーバーは必要ありません。Linux、Windows、Docker など、サポートされているプラットフォーム上で実行できます。参考文献:
* VMware vCenter/vSphere 仮想インフラ
* 異常 (サービス)
* より良いエクスペリエンス: VMware + Juniper Apstra

最新問題**: 20**
ジュニパーアプストラ。デバイスで使用できる 3 つのモードはどれですか? 3つお選びください。）
A. デプロイ
B. アクティブ
C. 停止しました
D. ドレイン
E. 準備完了
Answer: (解答を表示する**)**
Juniper Apstra は、デバイスの 3 つの展開モード (Deploy、Drain、Ready) をサポートしています。これらのモードは、データセンター ファブリック 12 内のデバイスの構成と状態を決定します。
* デプロイ: このモードは、Apstra リファレンス デザインに従って、Apstra でレンダリングされた完全な構成をデバイスに適用します。デバイスの状態は IS-ACTIVE になり、デバイスはファブリック 12 でトラフィックを伝送できる状態になります。
* ドレイン: このモードはデバイスに 「ドレイン」構成を追加し、新しいトラフィックがデバイスに入るのを防ぎます。デバイスの状態は IS-READY になり、デバイスはメンテナンスまたは廃止の準備が整います12。
* Ready: このモードでは、Apstra でレンダリングされた構成がデバイスから削除され、デバイスのホスト名、インターフェイスの説明、ポート速度/ブレークアウトなどの基本構成のみが残ります。デバイスの状態は IS-READY になり、デバイスはファブリック 12 の一部ではありません。参考文献:
* デバイス構成のライフサイクル

* デプロイモードの設定 (データセンター)

最新問題: **21**
デバイス構成を編集して手動による変更をインストールする場合、どの手順に従う必要がありますか?
A. CLI を使用してデバイスの設定を直接編集します。変更は Juniper Apstra 構成で自動的に調整されます
B. デバイスの初期設定を編集します。
C. コンフィグレットを使用してデバイス構成に永続的な変更を追加します。
D. Juniper Apstra システムからデバイスを削除し、構成を変更してから、デバイスを再インポートします。
Answer: (解答を表示する**)**
コンフィグレットは、デバイスまたはデバイスのグループに適用して、Apstra によって上書きされない永続的な変更を加えることができる小さな構成です。コンフィグレットを使用すると、カスタム コマンド、スクリプト、機能など、Apstra レンダリングされた構成の一部ではない手動の変更をインストールできます。コンフィグレットは、Apstra GUI または CLI12 から作成、編集、削除できます。参考文献:
* コンフィグレットの概要
* コンフィグレット ユーザー ガイド

最新問題: **22**
Juniper Apstra は、ケーブル配線に関する異常を指摘しました。
問題を修復する 2 つの方法は何ですか? (2つお選びください。)
A. ケーブル配線マップを手動で編集します。
B. エラーのあるデバイスを再展開します。
C. 無効なポートを無効な状態に設定します。
D. Apstra に LLDP を使用してケーブル マップを自動修復させます。
Answer: A,D (メーッセージを残す**)**
ケーブル配線の異常は、データセンター ファブリック内のデバイス間の物理接続が、Apstra リファレンス デザインに基づいた予期される接続と一致しない場合に発生する問題です。ケーブル配線の異常により、誤ったルーティング、最適ではないトラフィック フロー、デバイスの分離などの問題が発生する可能性があります。この問題を解決するには、次の方法のいずれかまたは両方を使用できます。
* ケーブル配線マップを手動で編集します。これにより、Apstra で生成されたケーブル配線をオーバーライドし、デバイス間の正しい接続を指定できます。Apstra UI または Apstra CLI を使用して、ケーブル配線マップを編集し、変更をファブリック 12 に適用できます。
* Apstra に LLDP を使用してケーブル マップを自動修復させます。これにより、Apstra はデバイスから LLDP データを収集し、それを使用してケーブル マップを自動的に更新できるようになります。LLDP は、デバイスがその ID、機能、および近隣デバイスに関する情報を交換できるように

するプロトコルです。Apstra は、LLDP データを使用して、ファブリック内のケーブル接続エラーを検出および修正できます34。参考文献:
* ケーブル配線マップの編集 (データセンター)
* ケーブル配線マップのインポート/エクスポート (データセンター)
* LLDP の概要
* 異常 (サービス)