Red Hat Advanced Cluster Security for Kubernetes 4.5

アーキテクチャー

システムアーキテクチャー

Last Updated: 2024-09-16

Red Hat Advanced Cluster Security for Kubernetes 4.5 アーキテクチャー

システムアーキテクチャー

法律上の通知

概要

Red Hat Advanced Cluster Security for Kubernetes アーキテクチャーの概要および詳細を説明します。

目次

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャー

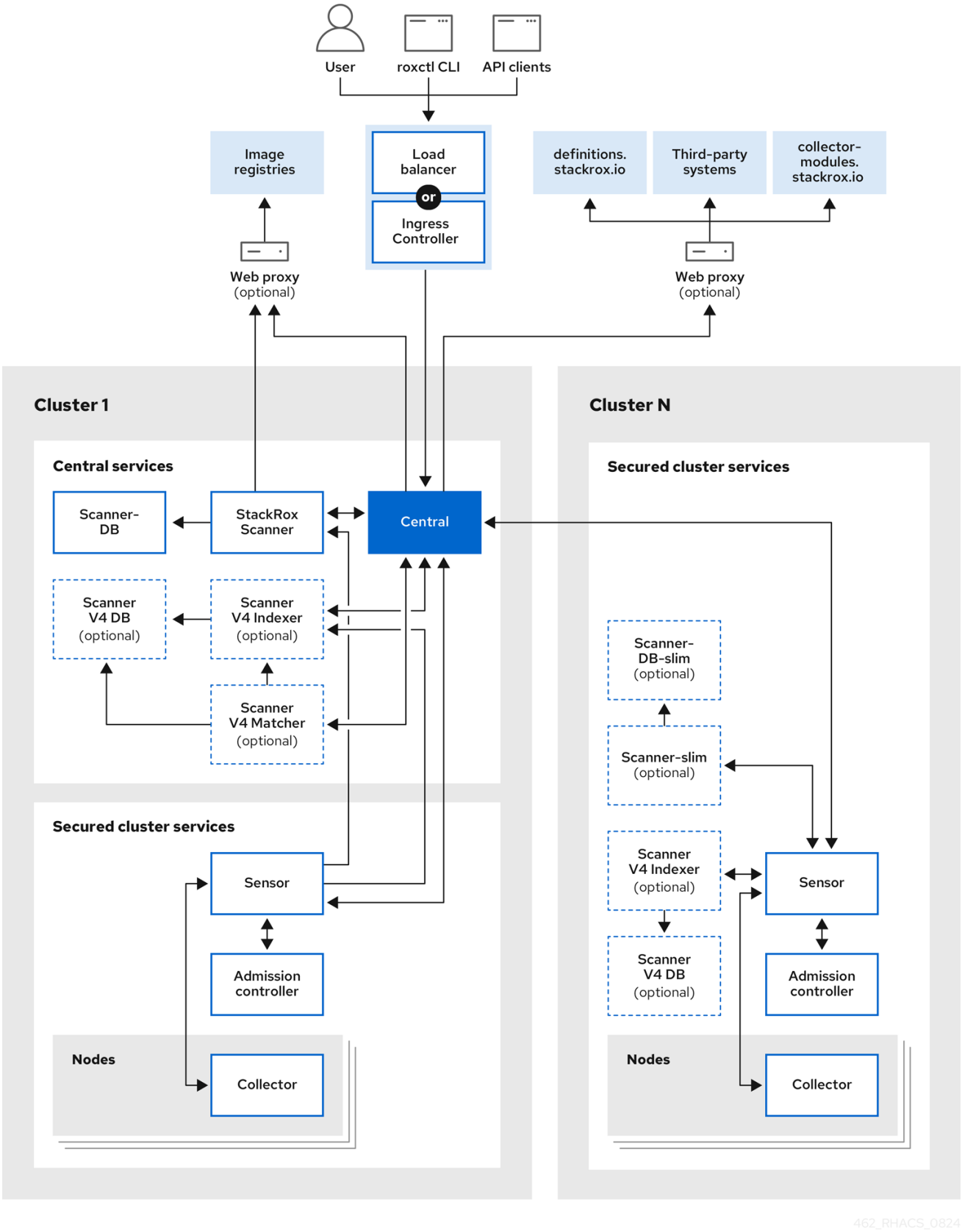
ここでは、Red Hat Advanced Cluster Security for Kubernetes のアーキテクチャーと概念を説明します。

1.1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャーの概要

Red Hat Advanced Cluster Security for Kubernetes (RHACS) は、大規模なデプロイメントに対応した分散アーキテクチャーを使用しており、基盤となる OpenShift Container Platform ノードまたは Kubernetes ノードへの影響を最小限に抑えるように最適化されています。

RHACS アーキテクチャー

次の図は、StackRox Scanner と Scanner V4 を含むアーキテクチャーを示しています。Scanner V4 のインストールは任意ですが、インストールするとさらなる利点が得られます。



OpenShift Container Platform または Kubernetes クラスターにコンテナーセットとして RHACS をインストールします。RHACS には次のサービスが含まれています。

- 1 つのクラスターにインストールする Central サービス
- RHACS の保護対象の各クラスターにインストールするセキュアクラスターサービス

これらの主要サービスに加え、RHACS は他の外部コンポーネントとも対話して、クラスターのセキュリティーを強化します。

インストールの違い
Operator を使用して RHACS を OpenShift Container Platform にインストールすると、RHACS はすべてのセキュアなクラスターに軽量バージョンの Scanner をインストールします。軽量 Scanner は、統合 OpenShift イメージレジストリー内のイメージをスキャンできるようにします。Helm インストールメソッドを **デフォルト** 値で使用して OpenShift Container Platform または Kubernetes に RHACS をインストールすると、軽量バージョンの Scanner はインストールされません。Helm を使用してセキュアなクラスターに軽量 Scanner をインストールするには、**scanner.disable=false** パラメーターを設定する必要があります。**roxctl** インストール方法を使用して、軽量 Scanner をインストールすることはできません。

関連情報

- 外部コンポーネント

1.2. CENTRAL サービス

Central サービスは 1 つのクラスターにインストールします。このサービスには次のコンポーネントが含まれています。

- **Central**: RHACS アプリケーション管理インターフェイスおよびサービスです。API 対話とユーザーインターフェイス (RHACS ポータル) アクセスを処理します。同じ Central インスタンスを使用して、複数の OpenShift Container Platform または Kubernetes クラスターを保護できます。

- **Central DB**: Central DB は RHACS のデータベースで、すべてのデータ永続性を処理します。現在、PostgreSQL 13 をベースにしています。

- **Scanner V4**: バージョン 4.4 以降、RHACS にはコンテナーイメージをスキャンするための Scanner V4 脆弱性スキャナーが含まれています。Scanner V4 は、Clair スキャナーにも利用されている ClairCore 上に構築されています。Scanner V4 は、言語および OS 固有のイメージコンポーネントのスキャンをサポートしています。バージョン 4.4 では、Scanner V4 によってノードおよびプラットフォームのスキャン機能がサポートされるまで、これらの機能を提供するために、この Scanner を StackRox Scanner と組み合わせて使用する必要があります。Scanner V4 には、Indexer、Matcher、および DB コンポーネントが含まれています。

    - **Scanner V4 Indexer**: Scanner V4 Indexer は、以前はイメージ分析と呼ばれていたイメージのインデックス作成を実行します。Indexer は、イメージとレジストリーの認証情報を指定されると、レジストリーからイメージを取得します。ベースオペレーティングシステムを検索し、システムが存在する場合はそのパッケージを検索します。指定されたイメージの結果を含むインデックスレポートを保存および出力します。

    - **Scanner V4 Matcher**: Scanner V4 Matcher は、脆弱性の照合を実行します。Central サービスの Scanner V4 Indexer がイメージにインデックスを作成した場合、Matcher はその Indexer からインデックスレポートを取得し、そのレポートを Scanner V4 データベースに保存されている脆弱性と照合します。セキュアクラスターサービスの Scanner V4 Indexer がインデックス作成を実行した場合、Matcher はその Indexer から送信されたインデックスレポートを使用して、脆弱性と照合します。また、Matcher は脆弱性データを取得し、Scanner V4 データベースを最新の脆弱性データで更新します。Scanner V4 Matcher は、イメージの最終結果を含む脆弱性レポートを出力します。

    - **Scanner V4 DB**: このデータベースには、すべての脆弱性データとインデックスレポートを含む、Scanner V4 の情報が保存されます。Central がインストールされているクラスター上の Scanner V4 DB には、永続ボリューム要求 (PVC) が必要です。

- **StackRox Scanner**: StackRox Scanner は、RHACS のデフォルトのスキャナーです。バージョン 4.4 で、新しいスキャナーである Scanner V4 が追加されました。StackRox Scanner は、Clair v2 オープンソーススキャナーのフォークから生まれました。RHCOS のノードスキャンとプラットフォームスキャンには、このスキャナーを引き続き使用する必要があります。

- **Scanner-DB**: このデータベースには、StackRox Scanner のデータが含まれています。

RHACS のスキャナーは、各イメージレイヤーを分析してベースオペレーティングシステムを特定し、プログラミング言語パッケージとオペレーティングシステムパッケージマネージャーによってインストールされたパッケージを識別します。スキャナーは、さまざまな脆弱性ソースからの既知の脆弱性とスキャン結果を照合します。さらに、StackRox Scanner が、ノードのオペレーティングシステムとプラットフォームの脆弱性を特定します。これらの機能は、今後のリリースで Scanner V4 に追加される予定です。

1.2.1. 脆弱性ソース

RHACS は次の脆弱性ソースを使用します。

- Alpine Security Database
- Amazon Linux Security Center で追跡されるデータ
- Debian Security Tracker
- Oracle OVAL
- Photon OVAL
- Red Hat OVAL
- Red Hat CVE Map : これは、Red Hat Container Catalog に表示されるイメージに使用されます。
- SUSE OVAL
- Ubuntu OVAL
- OSV: Go、Java、Node.js (JavaScript)、Python、Ruby などの言語関連の脆弱性に使用されます。このソースは、脆弱性の CVE 番号ではなく GitHub Security Advisory (GHSA) ID を提供する場合があります。

注記

RHACS Scanner V4 は、こちらのライセンス に基づいて OSV.dev で入手可能な OSV データベースを使用します。

- NVD: ベンダーが情報を提供していない場合に情報のギャップを埋めるなど、さまざまな目的で使用されます。たとえば、Alpine は、詳細、CVSS スコア、重大度、公開日を提供していません。

注記

この製品は、NVD API を使用していますが、NVD による承認や認定を受けていません。

- StackRox: アップストリームの StackRox プロジェクトは、他のソースからのデータのフォーマットやデータの欠如が原因で発見されていない可能性のある一連の脆弱性を管理しています。

Scanner V4 Indexer は次のソースを使用します。

- repository-to-cpe.json: RPM リポジトリーを関連する CPE にマッピングします。これは、RHEL ベースのイメージの脆弱性を照合するために必要です。
- container-name-repos-map.json: コンテナー名と、コンテナーの配布先のリポジトリーを照合します。

1.3. セキュアクラスターサービス

保護対象の各クラスターには、セキュアクラスターサービスを RHACS Cloud Service を使用してインストールします。セキュアクラスターサービスには、次のコンポーネントが含まれています。

- **Sensor**: クラスターの分析と監視を行うサービスです。OpenShift Container Platform または Kubernetes API および Collector イベントをリッスンして、クラスターの現在の状態を報告します。RHACS Cloud Service ポリシーに基づき、デプロイタイムおよびランタイムの違反もトリガーします。さらに、ネットワークポリシーの適用、RHACS Cloud Service ポリシーの再処理の開始、Admission コントローラーとの対話など、すべてのクラスターの対話も担当します。
- **Admission コントローラー**: ユーザーが RHACS Cloud Service のセキュリティーポリシーに違反するワークロードを作成するのを防ぎます。
- **Collector**: クラスターノード上のコンテナーアクティビティーを分析および監視します。コンテナーのランタイムとネットワークアクティビティーの情報を収集し、収集したデータを Sensor に送信します。
- **StackRox Scanner**: Kubernetes では、セキュアクラスターサービスに、オプションのコンポーネントとして Scanner-slim が含まれています。一方、OpenShift Container Platform では、OpenShift Container Platform 統合レジストリーと、必要に応じて他のレジストリー内のイメージをスキャンするために、RHACS Cloud Service によって各セキュアクラスターに Scanner-slim バージョンがインストールされます。
- **Scanner-DB**: このデータベースには、StackRox Scanner のデータが含まれています。
- **Scanner V4**: Scanner V4 が有効な場合、Scanner V4 のコンポーネントがセキュアクラスターにインストールされます。
  - **Scanner V4 Indexer**: Scanner V4 Indexer は、以前はイメージ分析と呼ばれていたイメージのインデックス作成を実行します。Indexer は、イメージとレジストリーの認証情報を指定されると、レジストリーからイメージを取得します。ベースオペレーティングシステムを検索し、システムが存在する場合はそのパッケージを検索します。指定されたイメージの結果を含むインデックスレポートを保存および出力します。
  - **Scanner V4 DB**: このコンポーネントは、Scanner V4 が有効な場合にインストールされます。このデータベースには、インデックスレポートを含む Scanner V4 の情報が格納されます。最適なパフォーマンスを得るには、Scanner V4 DB 用に永続ボリューム要求 (PVC) を設定してください。

注記

セキュアクラスターサービスが Central サービスと同じクラスターにインストールされ、同じ namespace にインストールされている場合、セキュアクラスターサービスは Scanner V4 コンポーネントをデプロイしません。代わりに、Central サービスに Scanner V4 のデプロイメントがすでに含まれているとみなします。

1.4. 外部コンポーネント

Red Hat Advanced Cluster Security for Kubernetes (RHACS) は、以下の外部コンポーネントと対話します。

- **サードパーティーシステム**: RHACS を、CI/CD パイプライン、イベント管理 (SIEM) システム、ロギング、電子メールなどの他のシステムと統合できます。
- **roxctl**: **roxctl** は、RHACS でコマンドを実行するためのコマンドラインインターフェイス (CLI) です。
- **イメージレジストリー**: RHACS をさまざまなイメージレジストリーと統合し、RHACS を使用してイメージをスキャンおよび表示できます。RHACS は、セキュアクラスターで検出されたイメージプルシークレットを使用して、アクティブなイメージのレジストリー統合を自動的に設定します。ただし、非アクティブなイメージをスキャンするには、レジストリー統合を手動で設定する必要があります。
- **definitions.stackrox.io**: RHACS は、**definitions.stackrox.io** エンドポイントでさまざまな脆弱性フィードからのデータを集約し、この情報を Central に渡します。フィードには、一般的な National Vulnerability Database (NVD) データと、Alpine、Debian、Ubuntu などのディストリビューション固有のデータが含まれます。
- **collector-modules.stackrox.io**: Central は、**collector-modules.stackrox.io** にアクセスして、サポートされているカーネルモジュールを取得し、これらのモジュールを Collector に渡します。

1.5. サービス間の対話

このセクションでは、RHACS サービスがどのように対話するかを説明します。

表1.1 RHACS と Scanner V4

コンポーネント	方向	コンポーネント	説明
Central	▮	Scanner V4 Indexer	Central は、特定のイメージをダウンロードしてインデックス作成 (分析) するように Indexer に要求します。このプロセスにより、インデックスレポートが作成されます。Scanner V4 Indexer は、インデックス作成プロセスを支援するマッピングファイルを Central に要求します。

コンポーネント	方向	コンポーネント	説明
Central	▮	Scanner V4 Matcher	Central は、特定のイメージを既知の脆弱性と照合するように Scanner V4 Matcher に要求します。このプロセスにより、最終的なスキャン結果、つまり脆弱性レポートが生成されます。Scanner V4 Matcher は、Central から最新の脆弱性を要求します。
Sensor	▮	Scanner V4 Indexer	Operator を使用してデプロイされた Red Hat OpenShift 環境の場合、またはスキャン委譲が使用されている場合、**SecuredCluster** のスキャンがデフォルトで有効になります。**SecuredCluster** のスキャンが有効になっている場合、Sensor は Scanner V4 にイメージのインデックス作成を要求します。Scanner V4 Indexer は、Central が同じ namespace に存在しない限り、インデックス作成プロセスを支援するマッピングファイルを Sensor に要求します。その場合は、代わりに Central と通信します。
Scanner V4 Indexer	→	Image Registries	Indexer は、レジストリーからイメージのメタデータを取得してイメージのレイヤーを確認し、以前にインデックス作成されていない各レイヤーをダウンロードします。
Scanner V4 Matcher	→	Scanner V4 Indexer	Scanner V4 Matcher は、イメージのインデックス作成の結果、つまりインデックスレポートを Indexer に要求します。次に、レポートを使用して関連する脆弱性を特定します。この対話は、イメージのインデックスが Central クラスターで作成された場合にのみ発生します。この対話は、セキュアクラスターでインデックス作成されたイメージの脆弱性を Scanner V4 が照合する場合には発生しません。
Scanner V4 Indexer	→	Scanner V4 DB	Indexer は、イメージレイヤーのダウンロードとインデックス作成が 1 回だけ行われるように、インデックス作成の結果に関連するデータを保存します。これにより、不必要なネットワークトラフィックやその他のリソースの使用が防止されます。
Scanner V4 Matcher	→	Scanner V4 DB	Scanner V4 Matcher は、すべての脆弱性データをデータベースに保存し、このデータを定期的に更新します。Scanner V4 インデクサーは、脆弱性照合プロセスの一環としてこのデータもクエリーします。

コンポーネント	方向	コンポーネント	説明
Sensor	▮	Central	Central と Sensor 間の双方向通信です。Sensor は、Sensor バンドル設定の更新をダウンロードするために定期的に Central をポーリングします。また、セキュアクラスターで観察されたアクティビティーと観察されたポリシー違反のイベントも送信します。Central は Sensor と通信して、有効なポリシーに対してすべてのデプロイメントの再処理を強制します。
Collector	▮	Sensor	Collector は Sensor と通信し、すべてのイベントをクラスターのそれぞれの Sensor に送信します。サポートされる OpenShift Container Platform クラスターでは、Collector はノードにインストールされているソフトウェアパッケージを分析し、それらを Sensor に送信して、後で脆弱性の有無をスキャンできるようにします。Collector は、不明ドライバーも Sensor に要求します。Sensor は、Collector にコンプライアンススキャン結果を要求します。さらに Sensor は、Central から外部の Classless Inter-Domain Routing 情報を受け取り、それを Collector にプッシュします。
Admission コントローラー	▮	Sensor	Sensor は、適用するセキュリティーポリシーのリストを Admission コントローラーに送信します。Admission コントローラーは、セキュリティーポリシー違反アラートを Sensor に送信します。Admission コントローラーは、必要に応じて Sensor にイメージスキャンを要求することもできます。
Admission コントローラー	→	Central	これは一般的ではありません。ただし、Central エンドポイントが判明しており、かつ Sensor が使用できない場合、Admission コントローラーは Central と直接通信できます。

表1.2 RHACS と StackRox Scanner

コンポーネント	方向	対話先	説明
Central	▮	Scanner	Central と Scanner の間の双方向通信です。Central は Scanner にイメージスキャンを要求し、Scanner は Central に CVE データベースの更新を要求します。
Central	→	**definitions.stackrox.io**	Central は、**definitions.stackrox.io** エンドポイントに接続して、集約された脆弱性情報を受信します。

コンポーネント	方向	対話先	説明
Central	→	**collector-modules.stackrox.io**	Central は、サポートされているカーネルモジュールを **collector-modules.stackrox.io** からダウンロードします。
Central	→	イメージレジストリー	Central はイメージレジストリーにクエリーを実行して、イメージメタデータを取得します。たとえば、RHACS ポータルで Dockerfile の手順を表示します。
Scanner	→	イメージレジストリー	Scanner はイメージレジストリーからイメージをプルして、脆弱性を特定します。
Sensor	▌	Central	Central と Sensor 間の双方向通信です。Sensor は、Sensor バンドル設定の更新をダウンロードするために定期的に Central をポーリングします。また、セキュアクラスターで観察されたアクティビティーと観察されたポリシー違反のイベントも送信します。Central は Sensor と通信して、有効なポリシーに対してすべてのデプロイメントの再処理を強制します。
Sensor	▌	Scanner	Sensor は、セキュアなクラスターにインストールされている軽量 Scanner と通信できます。この接続により、Central がそれらにアクセスできない可能性があるシナリオでは、Sensor がセキュアなクラスターからレジストリーに直接アクセスできます。スキャナーリクエストでは Sensor から更新されたデータを、Sensor はこれらのリクエストを Central に転送し、Central は必要なデータを **definitions.stackrox.io** からダウンロードします。
Collector	▌	Sensor	Collector は Sensor と通信し、すべてのイベントをクラスターのそれぞれの Sensor に送信します。サポートされる OpenShift Container Platform クラスターでは、Collector はノードにインストールされているソフトウェアパッケージを分析し、それらを Sensor に送信して、後で脆弱性の有無をスキャンできるようにします。Collector は、不明ドライバーも Sensor に要求します。Sensor は、Collector にコンプライアンススキャン結果を要求します。さらに Sensor は、Central から外部の Classless Inter-Domain Routing 情報を受け取り、それを Collector にプッシュします。

コンポーネント	方向	対話先	説明
Admission コントローラー	▮	Sensor	Sensor は、適用するセキュリティーポリシーのリストを Admission コントローラーに送信します。Admission コントローラーは、セキュリティーポリシー違反アラートを Sensor に送信します。Admission コントローラーは、必要に応じて Sensor にイメージスキャンを要求することもできます。
Admission コントローラー	→	Central	これは一般的ではありません。ただし、Central エンドポイントが判明しており、かつ Sensor が使用できない場合、Admission コントローラーは Central と直接通信できます。