ベンチマーク

Sysdig Secureの以前のバージョンでは、このモジュールをコンプライアンスと呼んでいました。

本文の内容は、Sysdig Secure ベンチマークのドキュメント (https://docs.sysdig.com/en/benchmarks.html) を元に日本語に翻訳・再構成した内容となっております。

ベンチマーク

Center for Internet Security（CIS）は、ITシステムと環境を保護するための標準化されたベンチマーク、ガイドライン、およびベストプラクティスを発行しています。

Sysdig Secureのベンチマークモジュールを使用して、KubernetesおよびDocker CISベンチマークを環境に対して実行します。

Sysdigベンチマークテストの仕組み

CISベンチマークは、ターゲットシステムの安全な構成のためのベストプラクティスです。 Sysdigは、KubernetesとDockerのさまざまなバージョンにこれらの標準化されたコントロールを実装しています。

タスクを設定する

新しいタスクを使用して、テストの種類、環境スコープ、コンプライアンスチェックのスケジュールされた頻度を構成します。結果レポートの表示方法をフィルタリングすることもできます。ベンチマークタスクの構成も参照してください。

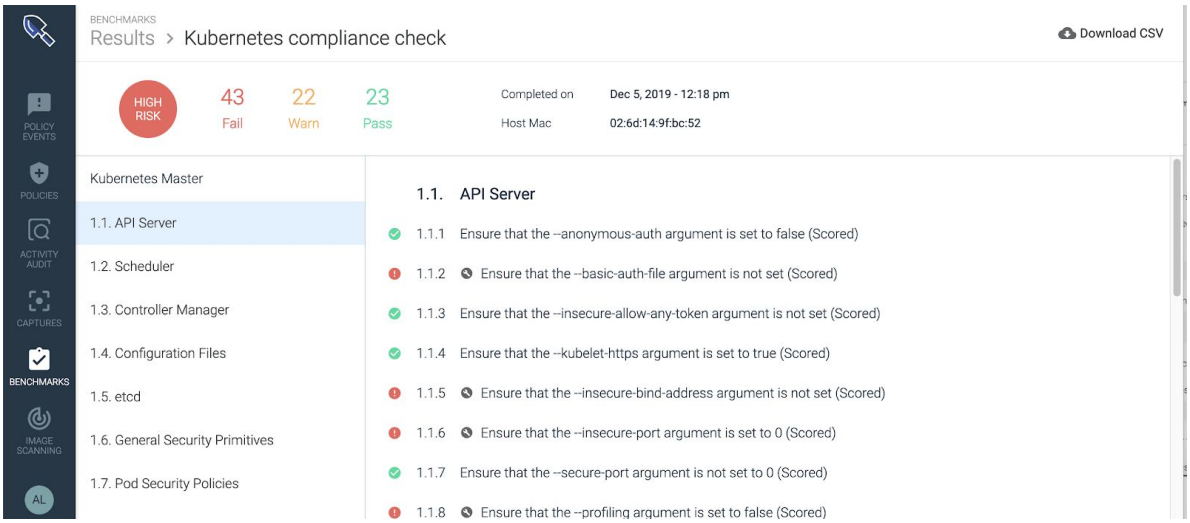
テストを実行する

タスクが設定されると、Sysdig Secureは次のことを行います。

- エージェントのチェックを開始して、CISベストプラクティスに対するシステム構成を分析します
- このタスクの結果を保存する

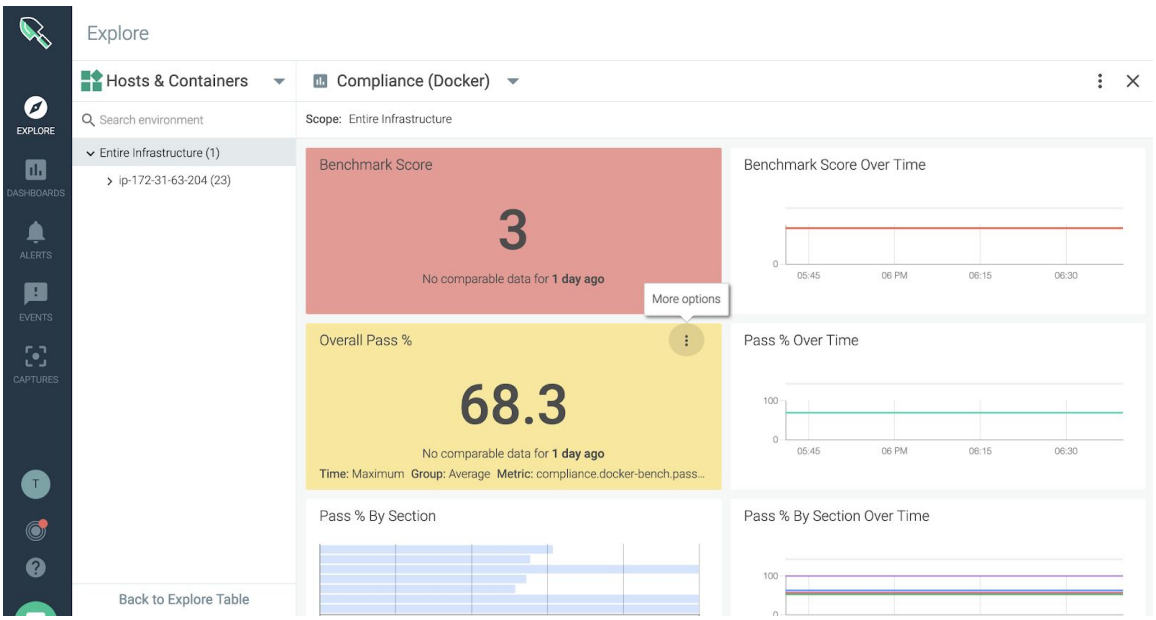
レポート結果の確認

タスクが実行されると、結果ページにリストされ、レポートとして表示できます。



ベンチマークメトリクスの確認

統合されたベンチマークメトリクスは、デフォルトまたはカスタマイズされたベンチマークダッシュボードからSysdig Monitorで表示することもできます。

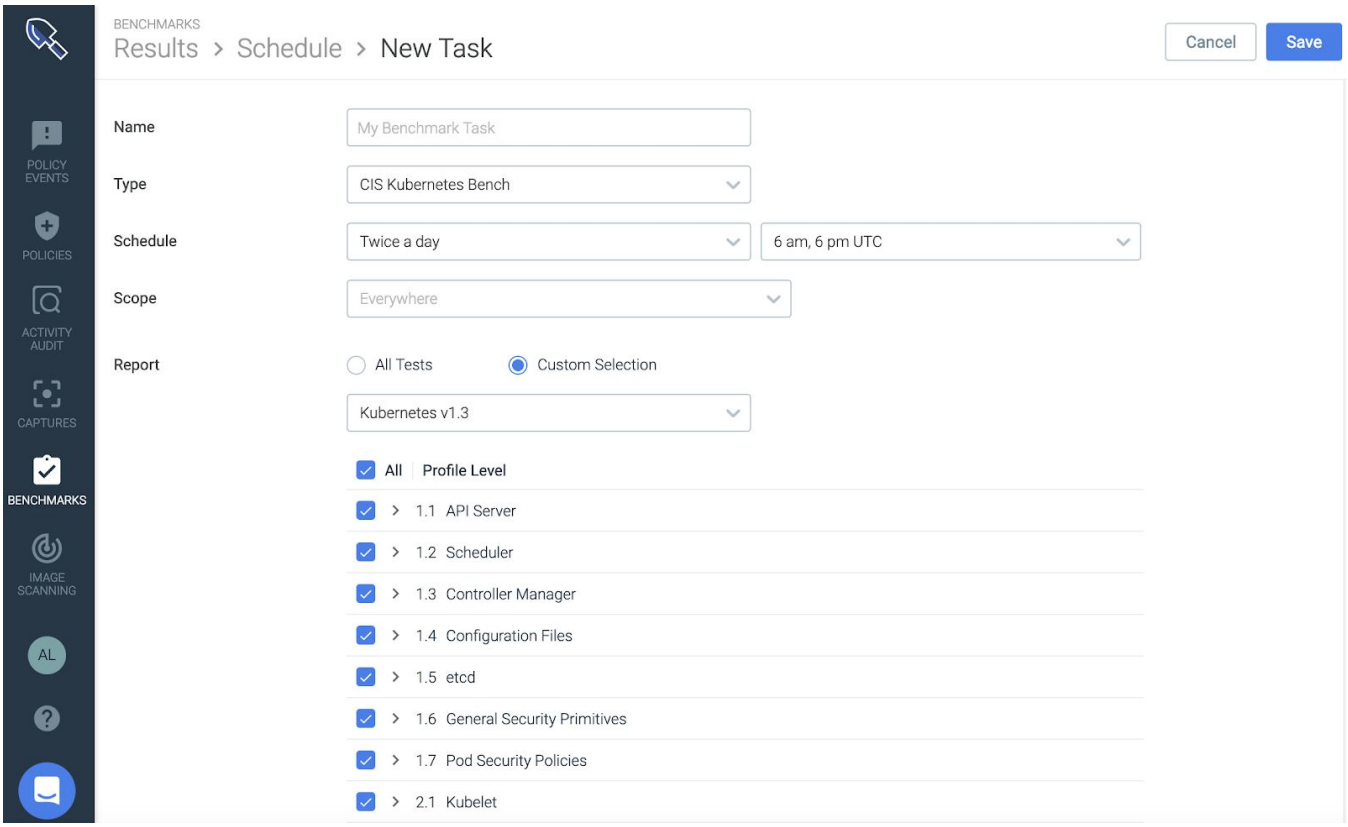


レポートフィルターについて

テストレポートの表示をカスタマイズします。たとえば、優先度の高い結果または選択したコントロールの結果のみを表示します。（テストスイート全体は引き続き実行されます。レポートの内容のみがフィルターされます。）

レポートフィルターの設定は簡単です。`Benchmark Task`ページの**`Report`**の下で：

- `Custom Selection`を選択
- `Benchmark version`を選択して、
    - `Profile`フィルターを適用する、および/または
    - 個々のコントロールを選択/選択解除します。



このセクションの情報を使用して、選択の効果を理解します。

カスタム選択について

フィルタリングルールは、テスト自体ではなくレポートに適用されます。

フィルタリング規則
レポートビューをフィルタリングしても、テスト実行の範囲は変わりません。

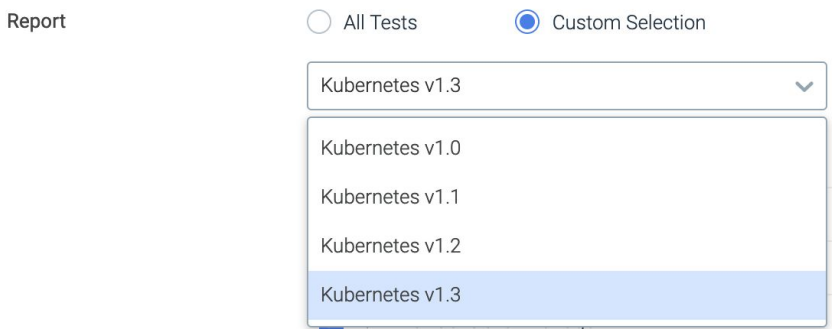
- 完全なテストは実行されますが、結果ビューは編集されます。
- すでに実行されている既存のタスクにフィルターを適用すると、フィルタービューが履歴レポートにさかのぼって適用されます。
- フィルタの選択を解除すると、完全な結果が再び表示されます。

ベンチマークバージョンについて

CISは、KubernetesまたはDockerソフトウェアバージョンに対応する（ただし、同一ではない）ベンチマークバージョンを発行します。 以下のマッピング表を参照してください。

バージョンルール
- レポートをカスタマイズ/フィルタリングしない場合、Sysdigエージェントは環境バージョンを自動検出し、ベンチマークコントロールの対応するバージョンを実行します。
- ベンチマークバージョンを指定した場合、レポートフィルターを適用できます。
- テストバージョンが環境バージョンと一致しない場合、フィルターは無視され、すべてのテストが表示されます。

KUBERNETESバージョンマッピング



Sysdigは、次のディストリビューションのKubernetesベンチマークテストもサポートしています。

- EKS：Kubernetes用のAmazon Elastic Container Service、デフォルトのクラスターバージョン
- GKE：Google Kubernetes Engine（GKE）、デフォルトのクラスターバージョン
- IKS：IBM Kubernetesサービス
- OpenShiftバージョン3.10、3.11
- Rancher

DOCKERバージョンマッピング

CISベンチマークバージョン: CIS_Docker_Community_Edition_Benchmark_v1.1.0

Sysdigレポートフィルター: Docker 1.0

プロファイルレベルについて

以下のように、CISは2つのレベルのテストを定義しています。

Sysdig Secureでは、完全なベンチマークが常に実行されますが、レポートのビューをフィルター処理して、最優先（レベル1プロファイル）のみまたは二次（レベル2優先）結果のみを表示できます。

CIS FAQから：

- レベル1プロファイル：主要な問題に限定
  かなり迅速に実装でき、パフォーマンスに大きな影響を与えないように設計された基本的な推奨事項を検討しました。レベル1プロファイルベンチマークの目的は、ビジネスの機能を妨げずにマシンを使用可能な状態に保ちながら、組織の攻撃対象領域を低くすることです。
- レベル2プロファイル：広範なチェック、より完全
  「多層防御」と見なされ、セキュリティが最優先される環境を対象としています。レベル2プロファイルに関連付けられた推奨事項は、適切に実装されない場合、または十分な注意を払わない場合、組織に悪影響を与える可能性があります。

注意
Sysdig Secureインターフェースで、「`All`」を選択して、レベル1およびレベル2の両方のコントロールを含む詳細なレポートを表示します。

`Level 1`を選択して、優先度の高いコントロールのみを含むレポートを表示します。
`Level 2`を選択して、レベル1から除外されている優先度の低いコントロールのみを含むレポートを表示します。

ベンチマークタスクの設定も参照してください。

ベンチマークタスクの設定

ベンチマークタスクを使用して以下を定義します。

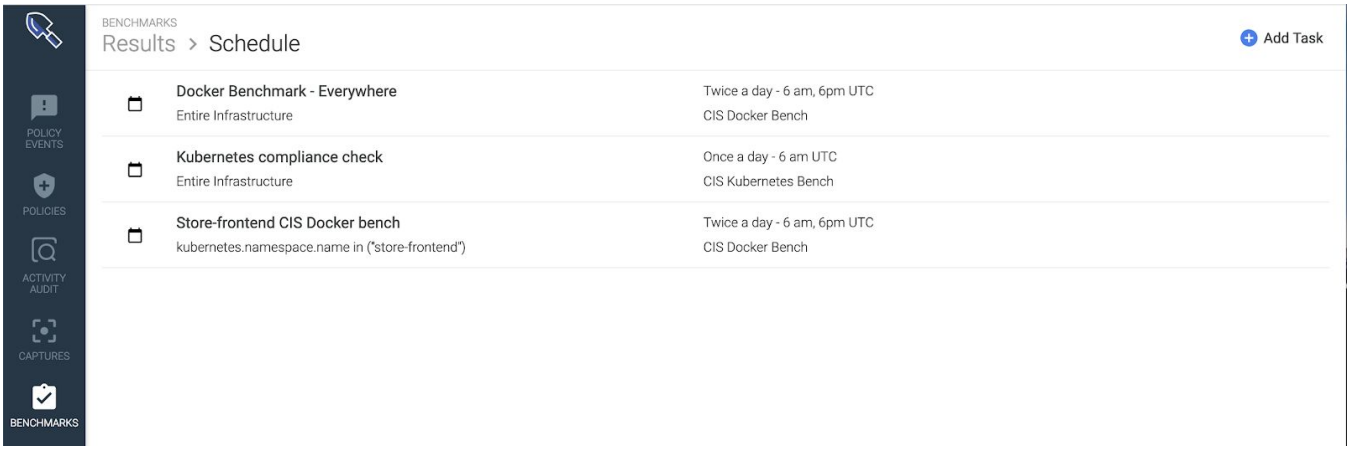
- 実行するベンチマークテストのタイプ
- チェックする環境の範囲
- スケジュールされたテスト頻度
- 結果レポートを表示する形式

タスクが設定されると、スケジュールされたタイムラインでテストが自動的に実行されます。タスクを手動でトリガーすることもできます。 手動ベンチマークテストのトリガー（今すぐ実行）を参照してください。

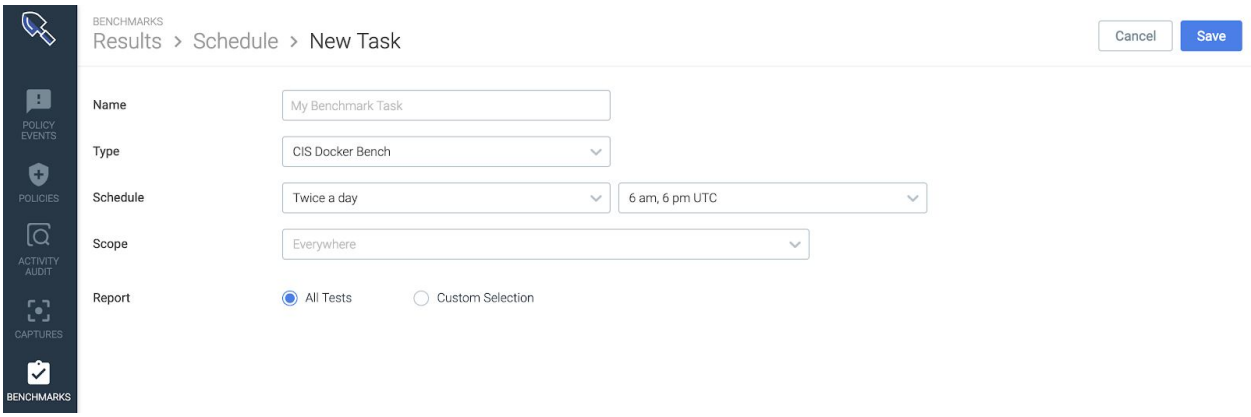
自動ベンチマークテストをスケジュールする

タスクを作成する

1. [`Benchmarks`]モジュールから、[`Schedule`]アイコンを選択します。
   （既存のタスクの）`Schedule list`が表示されます。



2. [+`Add Task`]をクリックし、[`New Task`]ページでタスクパラメーターを定義します。



- `Name`：意味のある名前を作成します。
- `Type`：CIS Docker BenchまたはCIS Kubernetes Benchを選択します。
- `Schedule`：テストを実行する頻度と時間を選択します。
- `Scope`：`Everywhere`選択するか、必要に応じてスコープを絞り込みます。
  （メトリクスのグループ化、スコープ、およびセグメント化も参照してください。）
- `Report`：レポートでのテスト結果の表示方法を選択します。
- `All Tests`：レポートにフィルターが適用されないことを意味します。
  Sysdigは、エージェントがインストールされているKubernetesまたはDockerのバージョンに基づいて、環境のベンチマークテストの正しいバージョンを自動的に適用します。
- `Custom Selection`：レポート結果をフィルタリングすることを意味します。

3. `Save`をクリックします。

1つのタスク、1つのテスト、1つの環境

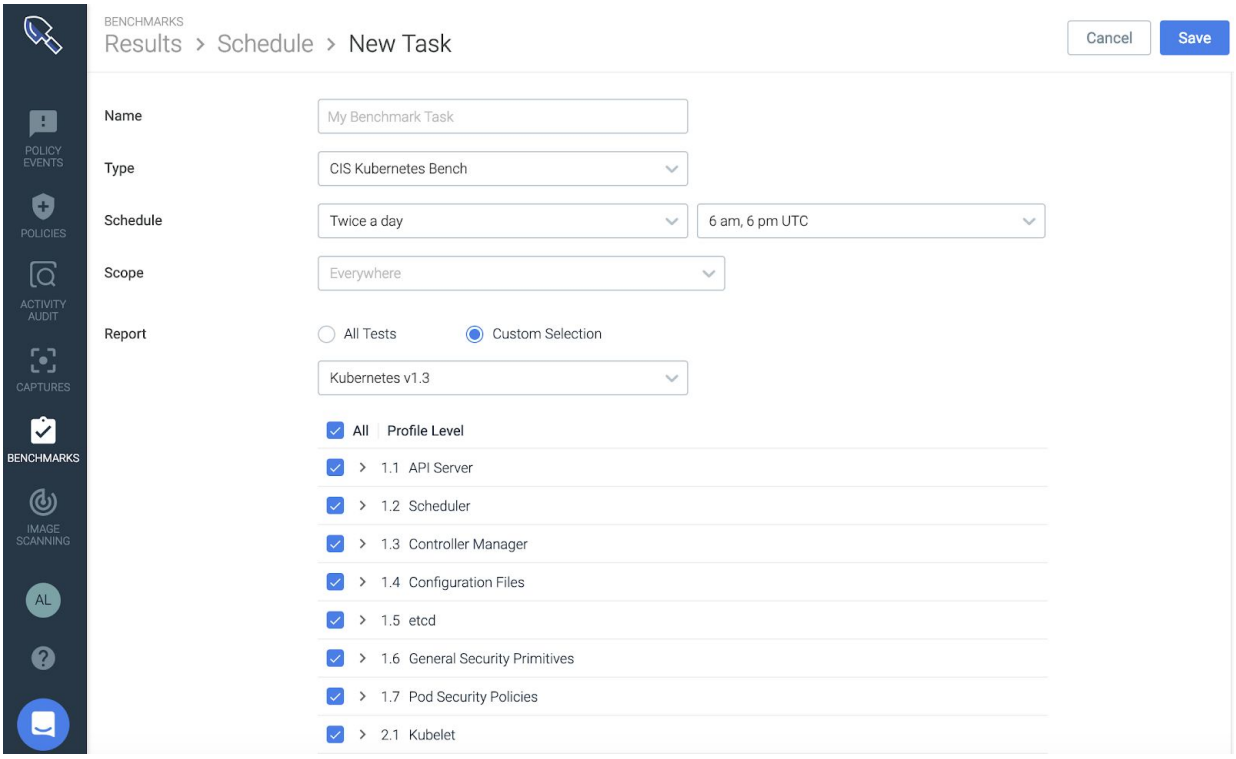
異なるKubernetesバージョンの環境でベンチマークを実行するには、そのスコープとバージョン用に個別のタスクを作成します。 Sysdigは、単一のタスクで複数のバージョンのテストを実行できません。

レポート結果のフィルタリング

レポートビューがフィルター処理されている場合でも、完全なCISベンチマークテストが実行されることに注意してください。 詳細については、レポートフィルターについてを参照してください。

1. `Benchmarks`モジュールから、`Schedule`アイコンを選択し、`Task`を選択または作成します。

   [`Task Configuration`]ページが表示されます。



2. [レポート]で、[`Custom Selection`]を選択します。
3. ドロップダウンメニューから適切なCISbenchmarkバージョンを選択します（選択したタイプに基づいて）。

   詳細については、ベンチマークバージョンについてを参照してください。

4. 必要に応じて結果をフィルタリングします。
   a. オプション：プロファイルレベル（1または2）を選択します。

高脆弱性の結果のみを表示するには、`Profile Level 1`を選択します。

レベル1から除外された下位レベルの結果のみを表示するには、`Profile Level 2`2を選択します。

`All`（プロファイルフィルターなし）を選択して、完全な結果を表示します。

参照：プロファイルレベルについて。

b. オプション：必要に応じて個々のコントロールを選択/選択解除します。
c. オプション：[`All`]を選択して、以前の選択をクリアし、再度開始します。

5. `Save`をクリックします。

スケジュールされたタスクを編集する

1. [`Benchmarks`]モジュールから、[`Schedule`]アイコンを選択します。

   スケジュールされたタスクのリストが表示されます。

2. リストからタスクを選択して編集します

   注意

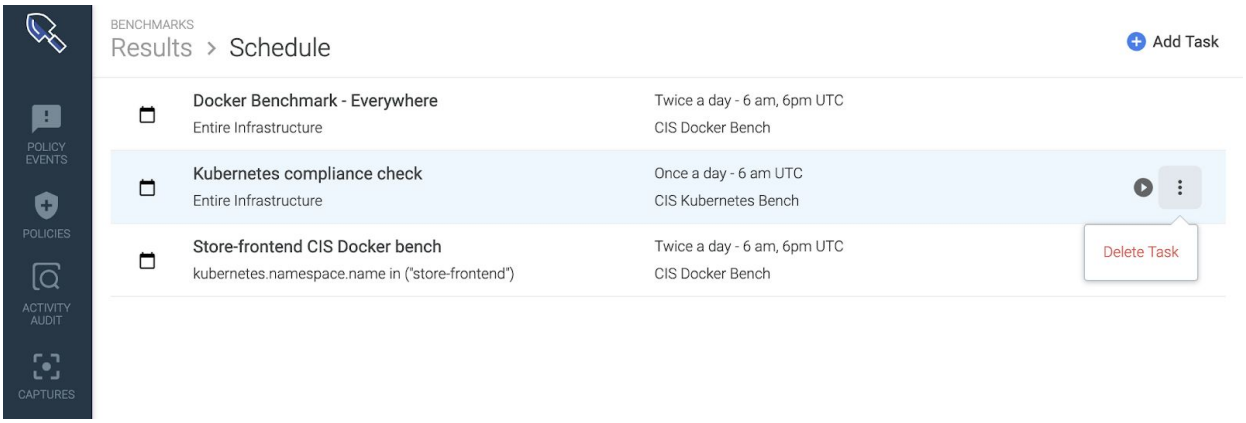
   既に実行されたタスクのレポートフィルター設定を変更すると、既存のレポートビューがさかのぼってフィルターされます。

3. `Save`をクリックします。

スケジュールされたタスクを削除する

1. [`Benchmarks`]モジュールから、[`Schedule`]アイコンを選択します。

2. 関連するタスクで、[More Options]（3つのドット）アイコンをクリックします。

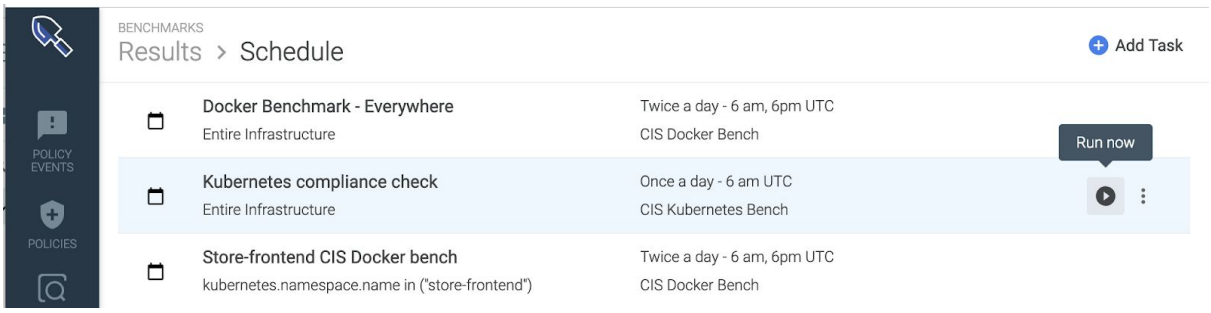


3. [Delete task]を選択し、[Yes]をクリックして確認します（または[No]をクリックして変更を元に戻します）。

手動ベンチマークテストのトリガー（今すぐ実行）

ユーザーは、ベンチマークテストが実行される次の予定時間を待つのではなく、ベンチマークテストを手動で実行することを選択できます。

1. [Benchmarks]モジュールから、[Schedule]アイコンを選択します。
2. 関連するタスクで、[Run Now]（矢印）アイコンをクリックします。



通知は、テストが正常に実行されたことを示します。

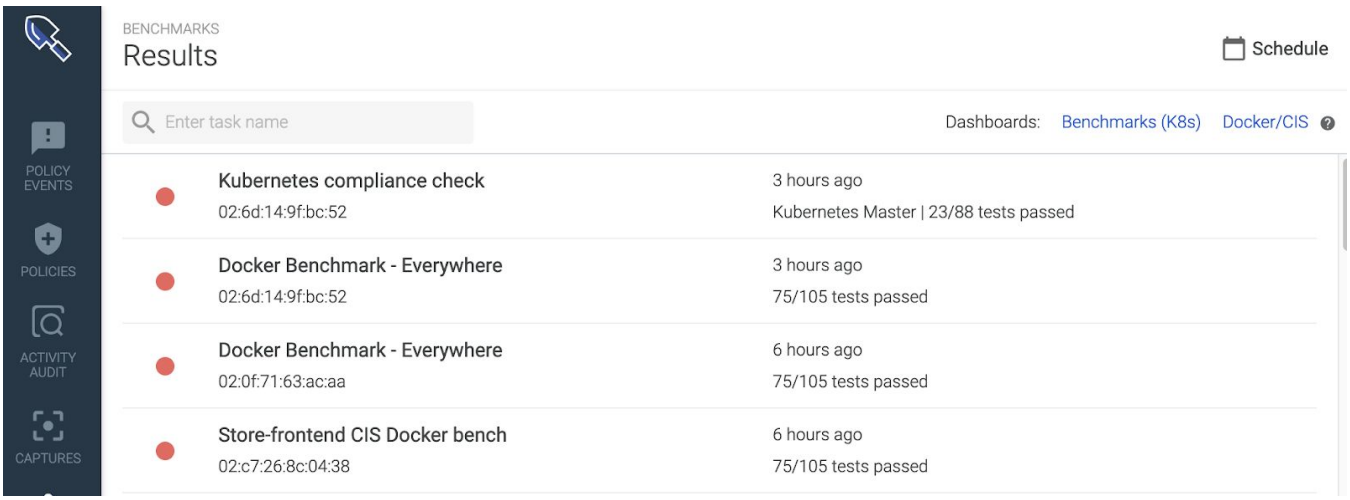
3. [Results]タブに戻り、数分後にページを更新して結果を確認します。

ベンチマークテスト結果の確認

テストを実行するようにベンチマークタスクを設定すると、各タスクを実行すると、レポートに関連付けられたリストが生成されます。 このページでは、結果リストおよび関連するレポートページに関連する機能について説明します。

結果リストの使用

ベンチマークランディングページは結果リストでもあり、完了した各結果レポートがリンクされています。



このページから次のことができます。

- `Reports`へアクセス
- スケジュールアイコンから`Tasks`を作成/アクセスする
- 検索バーから`Task`名で`Report`リストを検索する
- Sysdig Monitorの`Dashboards`とそれに関連するメトリクスへのリンク

注：テストがすべて失敗すると、レポートリンクの代わりにエラーログが一覧表示されます。

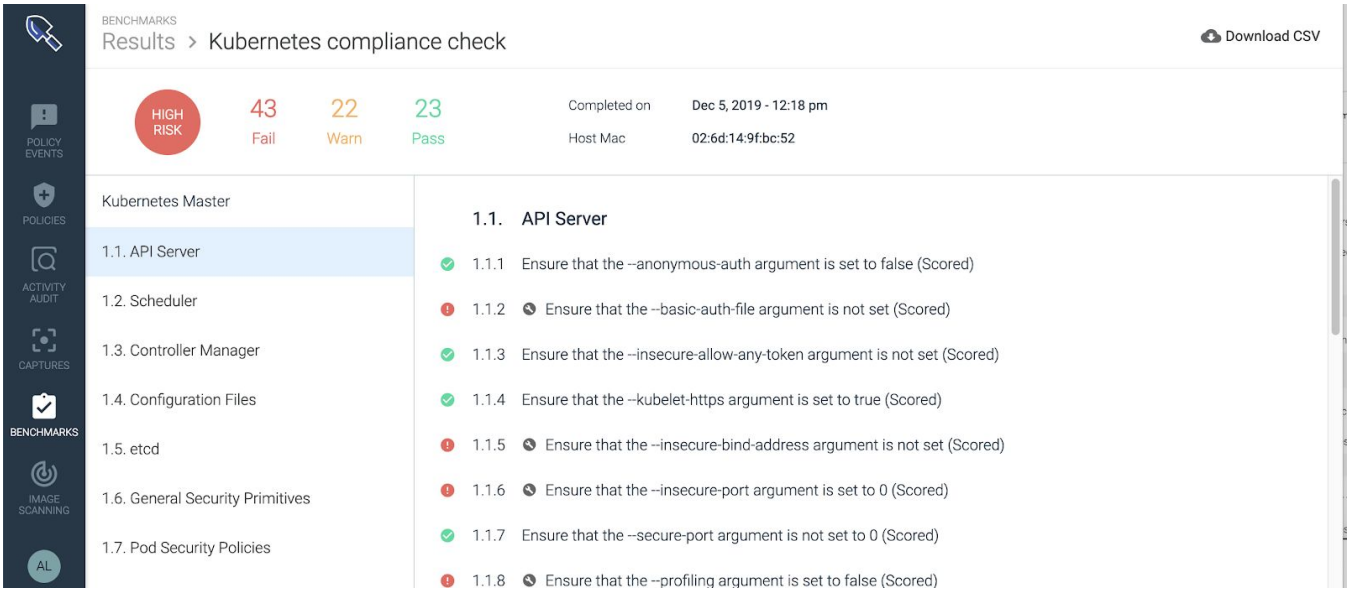
Kubernetesテストでは、結果リストにKubernetesマスターノードも表示されます。これは、識別に役立ちます。

結果レポートの使用

[`Results`]リストのエントリをクリックして、対応する`Results Report`を開きます。

できる事：

- 各コンプライアンスコントロールの`Pass/Fail/Warn`結果を確認する
- `Warn/Fail`結果の修復提案を確認します
- 必要に応じてレポートをCSVファイルとしてダウンロードします



Kubernetesレポートのサンプル。（参照：https://www.cisecurity.org/benchmark/kubernetes/)

ヒント

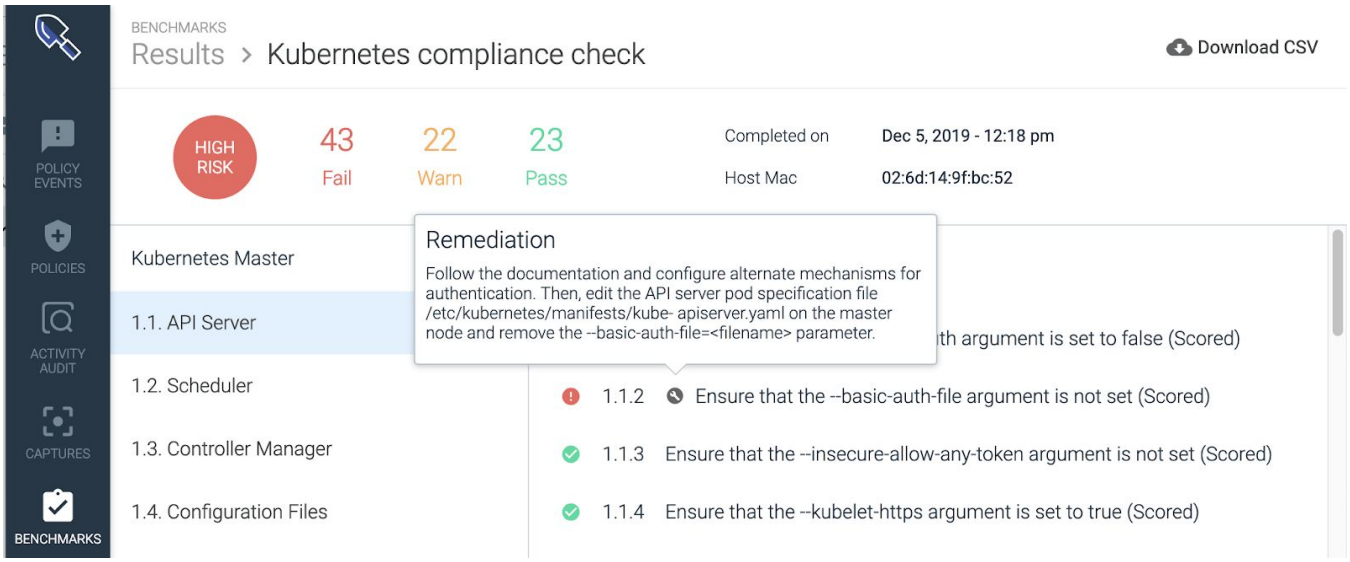
要確認：レポートビューをフィルターして、情報のサブセットを強調表示することを選択した可能性があります。

[結果]ページのすべての関連リストにフィルターが適用されます。 フィルターを削除して、テスト結果全体を表示します。 レポート結果のフィルターを参照してください。

修復のヒントを確認する

修復のヒントは、問題を解決するために通常必要なものの一般的な概要を提供します。 この情報は環境固有ではないため、特定の設定手順ではなくガイドとして使用する必要があります。

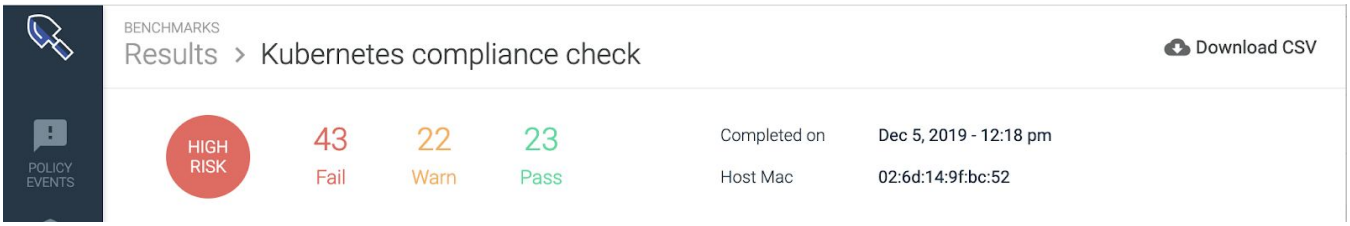
レポートの`Warn`または`Fail`エントリの横にあるレンチアイコンから修復のヒントにアクセスします。



修復情報は、ダウンロードされたCSVレポートにも含まれています。

レポートをCSVファイルとしてダウンロードする

[`Report`]ページで、[`Download CSV`]をクリックします。



コンプライアンスダッシュボードとメトリクスを使用する

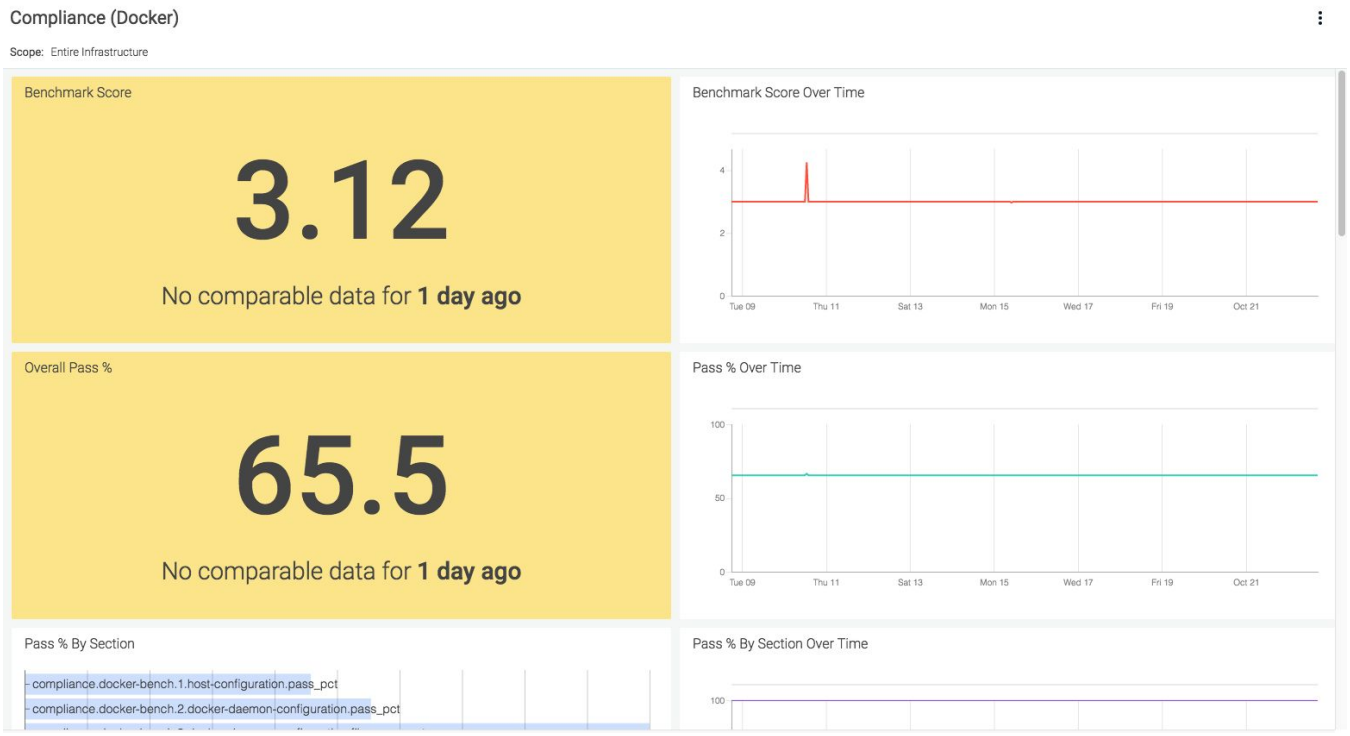
Sysdig MonitorのComplianceDashboardsへのリンクは、Sysdig Secure Benchmarksモジュールの結果リストから提供されます。

コンプライアンスダッシュボード

Sysdigは、Sysdig Monitorの一部として2つの事前構築済みコンプライアンスダッシュボードを提供します。

- コンプライアンス（K8s）
- コンプライアンス（Docker）

サンプルDockerコンプライアンスダッシュボード：



Kubernetesコンプライアンスダッシュボードのサンプル：

コンプライアンスメトリクス

KubernetesとDockerの両方のコンプライアンスメトリクスは、Sysdig Monitorダッシュボードで表示できます。 これらのメトリクスは、メトリクスディクショナリに完全に文書化されており、次の場所から入手できます。(https://docs.sysdig.com/en/benchmarks-and-compliance.html)