



2020年11月25日 時点





本文の内容は、ベンチマークのドキュメント(https://docs.sysdig.com/en/benchmarks.html) 2020年11 月25日時点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	4
Sysdigベンチマークテストの仕組み	4
タスクの設定	5
テストの実行	5
レポート結果のレビュー	5
ベンチマークメトリクスのレビュー	5
レポートフィルタを理解する	6
カスタム選択について	7
ベンチマークバージョンについて	7
Kubernetes のバージョンマッピング	8
Linux ベンチバージョン	8
Dockerのバージョンマッピング	9
プロファイルレベルについて	9
ベンチマークタスクの設定	10
自動ベンチマークテストをスケジュールする	10
タスクの作成	10
レポート結果のフィルタリング	12
スケジュールされたタスクの編集	14
スケジュールされたタスクの削除	14
手動ベンチマークテストのトリガー(Run Now)	15





ベンチマークテスト結果のレビュー	16
結果リストの使用	16
結果報告書の利用	17
レメディエーションのヒントをチェックする	18
レポートをCSVファイルでダウンロードする	18
コンプライアンスのダッシュボードとメトリクスを使用する	20
コンプライアンスダッシュボード	20
コンプライアンスメトリクス	21





# ベンチマーク

留意事項

Sysdig Secureの以前のバージョンでは、このモジュールはコンプライアンスと呼ばれていました。

<u>Center for Internet Security (CIS)</u>は、ITシステムと環境の安全性を確保するための標準化されたベンチ マーク、ガイドライン、ベストプラクティスを発行しています。また、RedhatはOpenshift 3.10/3.11 クラスタを実行するためのベストプラクティスの概要をまとめたコンテナセキュリティガイドを発行 しています。

Sysdig Secureには、お客様の環境に対して実行可能な4つのベンチマークの実装が含まれています。

- CIS Docker 1.2
- <u>CIS Kubernetes 1.3/1.4/1.5</u>
- <u>CIS ディストリビューションインデペンデントLinux 1.1.0</u>
- Redhat Container Security Guide 3.10/3.11

これらのベンチマークは、3つの別々のプログラムタイプを介して実行することができます。

- Dockerベンチマーク: CIS Docker用
- Kubernetesベンチマーク: CIS KubernetesとRedhatコンテナセキュリティガイド
- Linux ベンチマーク: CIS ディストリビューションのための独立した Linux

### 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ベストプラクティスです。Sysdigは、 Kubernetes、Linux、Dockerの異なるバージョンに対して、これらの標準化されたコントロールを実装 しています。





### タスクの設定

新しいタスクを使用して、テストの種類、環境スコープ、およびコンプライアンス チェックのスケ ジュールされた頻度を設定します。また、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。

### テストの実行

タスクが設定されると、Sysdig Secure は以下のようになります。

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

### レポート結果のレビュー タスクが実行されると、結果ページに表示され、レポートとして確認することができます。

BENCHMARKS >	Kuberne	etes Cor	npliance (	Check	🚯 Download CSV
MED RISK	16 Fail	3 Warn	4 Pass	Completed on Result Scherna Kubernetes Benchmark 1.5 Host Mac Host Name	
4.1. Worker Node	Configuratio	on Files	4.	1. Worker Node Configuration Files	
4.2. Kubelet			<b>()</b> 4.	1.1 S Ensure that the kubelet service file permissions are set to 644 or more restrictive (Scored)	
			<b>()</b> 4.	1.2 S Ensure that the kubelet service file ownership is set to root:root (Scored)	
			<b>()</b> 4.	1.3 S Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive (Scored)	
			<b>()</b> 4.	1.4 S Ensure that the proxy kubeconfig file ownership is set to root:root (Scored)	
	• 4.1.5 S Ensure that the kubelet.conf file permissions are set to 644 or more restrictive (Scored)				
• 4.1.6 S Ensure that the kubelet.conf file ownership is set to root:root (Scored)					
			<b>(</b> ) 4.	1.7 S Ensure that the certificate authorities file permissions are set to 644 or more restrictive (Scored)	
			<b>9</b> 4.	1.8 S Ensure that the client certificate authorities file ownership is set to rootroot (Scored)	
			<b>A</b> 1	1.0 Convertex that the hybelet configuration file has permissions set to 644 or more restrictive (Scored)	

### ベンチマークメトリクスのレビュー

Consolidated Benchmarkメトリクスは、デフォルトのコンプライアンスダッシュボードまたはカスタ マイズされたコンプライアンスダッシュボードから、Sysdig Monitorでも確認することができます。





#### Explore

Hosts & Containers 🔹	Compliance (Docker)	: ×
Q Search environment	Scope: Entire Infrastructure	
<ul> <li>✓ Entire Infrastructure (1)</li> <li>&gt; ip-172-31-63-204 (23)</li> </ul>	Benchmark Score <b>3</b> No comparable data for <b>1 day ago</b> More options	Benchmark Score Over Time
	Overall Pass % <b>68.3</b> No comparable data for <b>1 day ago</b> Time: Maximum Group: Average Metric: compliance.docker-bench.pass	Pass % Over Time
Back to Explore Table	Pass % By Section	Pass % By Section Over Time

### レポートフィルタを理解する

テストレポートの表示をカスタマイズして、例えば、優先度の高い結果のみを表示したり、選択した コントロールからの結果を表示したりすることができます。

フィルタは、レポートの表示にのみ影響を与えるかもしれませんし(エージェント・バージョン9.7.0 以前)、実際にテストを決定するかもしれないことに注意してください(エージェント・バージョン 9.7.0以降)カスタム選択についても参照してください。

古いバージョンでは、Benchmark TaskページのReportの下で、レポートをフィルタリングします。

- カスタム選択を選択
- ベンチマークのバージョンを選択し
  - プロファイルフィルタを適用する。
  - 個々のコントロールを選択/選択解除します。





Results > Schedu	ule > Kubernetes Compliance Check	Cancel Sa
Name	Kubernetes Compliance Check	
Туре	Kubernetes Benchmark	
Schedule	Twice a day $\checkmark$ 6 am, 6 pm UTC $\checkmark$	
Scope	Everywhere V	
Report	All Tests     Image: Custom Selection       Kubernetes Benchmark 1.4     V	
	2       All       Profile Level         2       >       1         Level 1 Profile       1       Level 2 Profile         2       >       1         2       >       1.4         Configuration Files       2         2       >       1.5         2       >       1.6         General Security Primitives       2         2       >       1.7         Pol Security Primitives       2	

このセクションの情報を使用して、選択の効果を理解してください。

#### カスタム選択について

フィルタリングルールはレポートに適用され、テスト自体には適用されません。

- 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を適用すると、フィルタビューは履歴レポート に遡って適用されます。
- 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やDockerソフトウェアの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、対応するバージョンのベンチマークコントロールを実行します。
- ベンチマークバージョンを指定した場合、レポートフィルタを適用することができます。





### テストバージョンが環境バージョンと一致しない場合、フィルタは無視され、すべてのテスト が表示されます。

#### Kubernetes のパージョンマッピング

#### 注) CIS 1.0、1.1、1.2は非推奨です。

CIS Benchmark Ver.	Kubernetes Ver.	Sysdig Agent	Targets
CIS 1.3	Kubernetes v 1.11-1.12	all	Master control plane, Node, Etcd, Policies
CIS 1.4	Kubernetes v 1.13-1.14	all	Master control plane, Node, Etcd, Policies
CIS 1.5	Kubernetes v 1.15-	all	Master control plane, Node, Etcd, Policies
RH 0.7 Red Hat OpenShift hardening guide	OCP 3.10-3.11	v9.7-	Master node
CIS1.6	Kubernetes v1.16-	v10.6-	Master control plane, Node, Etcd, Policies
GKE 1.0	GKE	v10.6-	Master control plane, Node, Etcd, Policies, Managed services
EKS 1.0	EKS	v.10.6-	Control plane, Node, Policies, Managed services

Sysdigは以下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。

• IBM IKS: IBM Kubernetes Service

注: CIS ベンチマークを IKS に対して実行すると、IBM が特定のコンポーネントを配置する方法 により、一部の失敗や誤検出が発生する可能性があります。<u>IBMからの詳細はこちらをご覧く</u> <u>ださい。</u>

• Rancher RKE: Rancher Kubernetes エンジン

注:RKEに対してCISベンチマークを実行すると、Rancherが特定のコンポーネントをデプロイ する方法により、失敗や偽陽性が発生することがあります。詳しくは<u>Rancherをご覧くださ</u> い。

**Linux ベンチバージョン** Linux Benchmarks (例: 2.0 と 1.1) はどちらも任意の Linux ディストリビューションで動作します。





Dockerのバージョンマッピング

**CIS Benchmark Version** 

Sysdig Report Filter

CIS\_Docker\_Community\_Edition\_Benchmark\_v1.1.0 Docker 1.0

### プロファイルレベルについて

CISでは、以下のように2つのレベルのテストを定義しています。

Sysdig Secureでは、フルベンチマークは常に実行されますが、レポートの表示をフィルタリングして、最優先 (レベル1プロファイル)の結果のみを表示したり、セカンダリ (レベル2優先)の結果のみを 表示したりすることができます。

<u>CISFAQ</u>より:

• レベル1プロファイル:メジャーな問題に限定

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ている基本的 な推奨事項と考えられます。レベル1プロファイルのベンチマークの目的は、マシンの使用可 能性を維持し、ビジネス機能を妨げないようにしながら、組織の攻撃対象を減らすことです。

• レベル2プロファイル:大規模なチェック、より完全なチェック

「防御の深さ」と考えられており、セキュリティが最重要視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する推奨事項は、適切に実施されていない場合、または十分な注意 を払わずに実施した場合、組織に悪影響を及ぼす可能性があります。

#### 注意事項

Sysdig Secure インターフェースで、[All] を選択すると、レベル1とレベル2の両方のコントロールを 含む詳細なレポートが表示されます。

優先度の高いコントロールのみを含むレポートを表示するには、[Level 1]を選択します。





レベル2を選択すると、レベル1から除外された優先度の低いコントロールのみを含むレポートが表示 されます。

# 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定義します。

- 実行するベンチマーク・テストの種類
- チェック対象の環境の範囲
- 予定された試験頻度
- 結果レポートを表示するフォーマットを指定します。

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上で自動的にテストが実行されます。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をトリガーする(Run Now)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

タスクの作成

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

スケジュール一覧(既存のタスクの)が表示されます。

benchmai Resu	rks Its > Schedule		🕀 Add Task
•	Docker Benchmark - Everywhere Entire Infrastructure	Twice a day - 6 am, 6pm UTC docker-bench-security	
	Kubernetes Compliance Check Entire Infrastructure	Twice a day - 6 am, 6pm UTC kube-bench	
	Linux node checks kubernetes.cluster.name = "demo-kube-aws"	Once a day - 6 am UTC linux-bench	
	Store-frontend CIS Docker bench kubernetes.namespace.name in ("store-frontend")	Twice a day - 6 am, 6pm UTC docker-bench-security	

2. [タスクを追加]をクリックし、[新規タスク]ページでタスクのパラメータを定義します。





BENCHMARKS Results > Schedu	le > New Task		Cancel Save
Name	my task		
Туре	Kubernetes Benchmark		
Schedule	Twice a day 🗸	6 am, 6 pm UTC 🗸 🗸	]
Scope	Everywhere	~	
Report	All Tests     O Custom Selection		
	Select 🗸		
	OpenShift Hardening Guide		
	Kubernetes Benchmark 1.3		
	Kubernetes Benchmark 1.4		
	Kubernetes Benchmark 1.5		

- Name: 意味のある名前を作成します。
- Type:タイプを指定します。環境に応じて、Docker Benchmark、Kubernetes Benchmark、Linux Benchmarkのいずれかを選択してください。
- Schedule:スケジュールを設定します。テストを実行する頻度と時間を選択します。
- Scope:スコープを選択します。Everywhereを選択するか、必要に応じてスコープを絞ります。

(メトリクスのグループ化、スコープ、セグメンテーションも参照してください)

- Report: レポートを作成する方法を選択します。レポート:レポートでテスト結果を表示する方法 を選択します。
  - All Tests: レポートにフィルタ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、お客様の環境に合った正しいバージョンのベンチマークテストを自動的に適用します。

Custom Selection: LEGACY: は、レポート結果をフィルタリングすることを意味します。





エージェント9.7.0以降では、カスタム選択は、テストのどの部分が実行されるかも定義 します。レポート フィルタを理解する」も参照してください。

3. 保存をクリックします。

1つのタスク、1つのテスト、1つの環境

Kubernetesのバージョンが異なる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 に別のタスクを作成してください。Sysdigでは、1つのタスクで複数のバージョンのテストを実行する ことはできません。

### レポート結果のフィルタリング

レポート・ビューがフィルタリング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。

1. ベンチマークモジュールから、スケジュールアイコンを選択し、タスクを選択または作成します

タスク設定ページが表示されます。





BENCHMARKS Results > Schedule > New Task				
Name	my task			
Туре	Kubernetes Benchmark	·		
Schedule	Twice a day	6 am, 6 pm UTC V		
Scope	Everywhere	~		
Report	<ul> <li>All Tests</li> <li>Custom Selection</li> <li>Select</li> <li>OpenShift Hardening Guide</li> <li>Kubernetes Benchmark 1.3</li> <li>Kubernetes Benchmark 1.4</li> <li>Kubernetes Benchmark 1.5</li> </ul>			

- 2. レポートについては、「カスタム選択」を選択します。
- 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Typeに基づいて)。

詳細については、「ベンチマークの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。

プロファイル・レベル1を選択すると、高脆弱性の結果のみが表示されます。

プロファイル レベル2を選択すると、レベル1から除外された下位レベルの結果のみが 表示されます。

完全な結果を表示するには、[すべて](プロファイル・フィルタなし)を選択します。

こちらも参照してください。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: [すべて] を選択します。すべてを選択して、以前の選択をクリアしてからや り直します。





5. 保存をクリックします。

### スケジュールされたタスクの編集

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。

#### 注意事項

既に実行済みのタスクのレポート フィルタ設定を変更すると、既存のレポート ビューが遡ってフィル タリングされます。

3. 保存をクリックします。

### スケジュールされたタスクの削除

- 1. Benchmarksモジュールから、Scheduleアイコンを選択します。
- 2. 該当するタスクで、[その他のオプション] (3つの点) アイコンをクリックします。

Results > Schedule					isk
Docker Benchmark - Everywhere Entire Infrastructure			Twice a day - 6 am, 6pm UTC docker-bench-security	0 :	
		Kubernetes Compliance Check Entire Infrastructure	Twice a day - 6 am, 6pm UTC kube-bench	Delete Task	
		Linux node checks kubernetes.cluster.name = "demo-kube-aws"	Once a day - 6 am UTC linux-bench		
		Store-frontend CIS Docker bench kubernetes.namespace.name in ("store-frontend")	Twice a day - 6 am, 6pm UTC docker-bench-security		

3. タスクの削除を選択し、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(Run Now)

ベンチマークテストを実行するために次のスケジュール時間を待つのではなく、ユーザーは手動でベ ンチマークテストを実行することを選択することができます。

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

benchma Resu	rks > Schedule		🕂 Add Task
	Docker Benchmark - Everywhere Entire Infrastructure	Twice a day - 6 am, 6pm UTC docker-bench-security	Run now
	Kubernetes Compliance Check Entire Infrastructure	Twice a day - 6 am, 6pm UTC kube-bench	0:
	Linux node checks kubernetes.cluster.name = "demo-kube-aws"	Once a day - 6 am UTC linux-bench	
	Store-frontend CIS Docker bench kubernetes.namespace.name in ("store-frontend")	Twice a day - 6 am, 6pm UTC docker-bench-security	

テストが正常に実行されたことを示す通知が表示されます。

3. 結果タブに戻り、数分後にページを更新すると結果が表示されます。





# ベンチマークテスト結果のレビュー

テストを実行するようにBenchmarkタスクを設定している場合、各タスクを実行すると、レポートに 関連したリストが作成されます。このページでは、結果リストと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

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

BENCHMAN Resu	ks ts	📥 Sched	dule
Q Ente	r task name Module Name 🗸	Dashboards: Benchmarks (K8s) Docker/Cl	s ø
•	Kubernetes Compliance Check Kubernetes Benchmark 1.5 ip-172-20-40-16	4 hours ago Kubernetes Master   32/65 tests failed	
•	Kubernetes Compliance Check Kubernetes Benchmark 1.5 gke demo-kube-gke default-pool-f141e1d0-zvsn	4 hours ago 16/23 tests failed	
	Kubernetes Compliance Check Kubernetes Benchmark 1.5 gke-demo-kube-gke-default-pool-f141e1d0-5sm1	4 hours ago 16/23 tests failed	
•	Kubernetes Compliance Check Kubernetes Benchmark 1.5 gke demo-kube-gke default-pool-f141e1d0-vsb0	4 hours ago 16/23 tests failed	
	Kubernetes Compliance Check Kubernetes Benchmark 1.5 ip-172-20-46-222	4 hours ago 14/23 tests failed	
•	Kubernetes Compliance Check Kubernetes Benchmark 1.5 ip-172-20-54-228	4 hours ago 14/23 tests failed	
	Kubernetes Compliance Check Kubernetes Benchmark 1.5 ip-172-20-42-99	4 hours ago 14/23 tests failed	
	Kubaratas Complianas Chask		

このページでは、以下のことができます。

- レポートへのアクセス
- スケジュールアイコンからタスクを作成/アクセス
- 検索バーからタスク名でレポートー覧を検索する
- Sysdig Monitorのダッシュボードと関連するメトリクスへのリンク

注意:テストが完全に失敗した場合、レポートリンクの代わりにエラーログが表示されます。





# Kubernetesテストでは、結果リストにはKubernetesマスターノードも表示されるので、識別に役立ちます。



an hour ago Kubernetes Master | 25/67 tests passed

### 結果報告書の利用

結果リストの項目をクリックして、対応する結果レポートを開きます。

以下のことができます:

- 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の結果で改善案を確認する
- 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する

Results > 1	Kuberne	etes Con	npliance	Chec	ck				🚯 Download CSV	
MED RISK	16 Fail	3 Warn	4 Pass		Completed on Host Mac	101.000 T-0.00 011.000 T-0.00	Result Schema Host Name	Kubernetes Benchmark 1.5		
4.1. Worker Node	Configuratic	n Files		4.1. V	Vorker Node Cor	nfiguration Files				
4.2. Kubelet			0	4.1.1 S Ensure that the kubelet service file permissions are set to 644 or more restrictive (Scored)						
			0	4.1.2 🕻	Ensure that the k	ubelet service file owners	hip is set to root:roo	ot (Scored)		
			0	• 4.1.3 S Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive (Scored)						
			0	4.1.4 🕻	Ensure that the p	roxy kubeconfig file owne	rship is set to root:r	oot (Scored)		
			0	4.1.5 🕻	Ensure that the k	ubelet.conf file permissio	ns are set to 644 or	more restrictive (Scored)		
			0	• 4.1.6 S Ensure that the kubelet.conf file ownership is set to root:root (Scored)						
			0	0 4.1.7 S Ensure that the certificate authorities file permissions are set to 644 or more restrictive (Scored)						
			0	4.1.8	Ensure that the c	lient certificate authoritie	s file ownership is s	et to root:root (Scored)		
ro sysdia com/#/	onobmark	-/65701121	f261_4700	410 6	Ensure that the k	ubelet configuration file h	as permissions set	to 644 or more restrictive (Scored)		

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

#### ヒント

注記:情報のサブセットを強調表示するために、レポートビューをフィルタリングすることを選択した 場合があります。



フィルタは、[結果]ページのすべての関連リストに適用されます。詳細は、「レポート結果のフィル ター」を参照してください。

### レメディエーションのヒントをチェックする

対策のヒントは、問題を解決するために通常必要なことの一般的な概要を提供しています。この情報 は環境固有のものではなく、特定の構成手順ではなく、ガイドとして使用する必要があります。

レメディエーションのヒントは、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 アクセスできます。

BENCHMARKS Results > Kubernetes compliance check						
HIGH RISK	43 Fail	22 Warn	23 Pass	Completed on Host Mac	Dec 5, 02:6d:	. 2019 - 12:18 pm :14:9f:bc:52
Kubernetes Master		Remedia Follow the	ation documentation and co	onfigure alternate mechar		
1.1. API Server		/etc/kuberr node and re	netes/manifests/kube emove thebasic-autl	th argument is set to false (Scored)		
1.2. Scheduler			• 1.1.2 S Ensure that thebasic-auth-file argument is not set (Scored)			n-file argument is not set (Scored)
1.3. Controller Manager			1.1.3	1.1.3 Ensure that theinsecure-allow-any-token argument is not set (Scored)		
1.4. Configuration Files			<ul><li>✓ 1.1.4</li></ul>	Ensure that thekubelet-https argument is set to true (Scored)		

ダウンロードしたCSVレポートには、レメディエーション情報も含まれています。

## レポートをCSVファイルでダウンロードする

レポートページから「CSVをダウンロード」をクリックします。











# コンプライアンスの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 Results リストから提供されています。

# 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、コンプライアンス&セキュリティダッシュボードを提供しています。

- Compliance (K8s)
- Compliance (Docker)

Dockerのコンプライアンスダッシュボードのサンプル:

Compliance (Docker) Scope: Entire Infrastructure	1
Benchmark Score <b>3.12</b> No comparable data for <b>1 day ago</b>	Benchmark Score Over Time
Overall Pass %	Pass % Over Time
65.5 No comparable data for 1 day ago	100 50
	Tue 09 Thu 11 Sat 13 Mon 15 Wed 17 Fri 19 Oct 21
Pass % By Section - compliance.docker-bench.1.host-configuration.pass_pct - compliance.docker-bench.2.docker-daemon-configuration.pass_pct	Pass % By Section Over Time

Kubernetesのコンプライアンスダッシュボードのサンプル





:

#### Compliance (K8s)

Scope: Entire Infrastructure

Overall Pass %	Overall Pass % Over Time
13.0	50-
No comparable data for <b>1 day ago</b>	0 Tue 09 Thu 11 Sat 13 Mon 15 Wed 17 Fri 19 Oct 21
Pass % By Section         - compliance.k8s-bench.1.1.gsi-server.pass_pct         - compliance.k8s-bench.1.3.controller-manager.pass_pct         - compliance.k8s-bench.1.3.controller-manager.pass_pct         - compliance.k8s-bench.1.4.configure-files.pass_pct         - compliance.k8s-bench.1.5.etcd.pass_pct         - compliance.k8s-bench.1.6.general-security-primitives.pass_pct         - compliance.k8s-bench.1.5.etcd.pass_pct         - compliance.k8s-bench.2.1.kubelet.pass_pct         - compliance.k8s-bench.2.2.configuration-files.pass_pct         0       2       4       6       8       10       12       14       16       18       20	Pass % By Section Over Time
Test Details (Overall) - compliance.k8s-bench.tests_pass	Test Details (1.1 - API Server)

## 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のダッシュボードで確認することができます。これらのメトリクスは Metrics Dictionary で完全に文書化されており、こちらから入手できます: <u>コンプライアンス</u>

