



キャプチャー





本文の内容は、Sysdig Secure キャプチャーのドキュメント

(<https://docs.sysdig.com/en/captures-122718.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。

キャプチャー	3
キャプチャファイルの設定	3
キャプチャファイルの保存	3
キャプチャファイルを作成する	3
キャプチャファイルを削除する	5
キャプチャファイルの確認	5
Sysdig Inspectでキャプチャファイルを確認する	5
キャプチャーファイルをダウンロードする	6
キャプチャ機能を無効にする	6

キャプチャー

Sysdigキャプチャファイルには、オープンソースのsysdigまたはcsysdig（cursesベースの）ユーティリティで分析できるシステムコールおよびその他のOSイベントが含まれておりキャプチャーモジュールに表示されます。

キャプチャーモジュールには、キャプチャファイル名、取得元のホスト、時間枠、キャプチャのサイズをリストするテーブルが含まれています。キャプチャファイルのステータスがアップロードされると、ファイルはSysdigエージェントからストレージバケットに正常に送信され、ダウンロードと分析に使用できます。

このセクションでは、Sysdig Secureでキャプチャファイルを作成する方法について説明します。

キャプチャファイルの設定

キャプチャファイルの保存

Sysdigキャプチャファイルは、デフォルトでSysdigのAWS S3ストレージ（SaaS環境の場合）またはCassandra DB（オンプレミス環境の場合）に保存されます。

- 自身のAWS S3ストレージバケットを使用するには、「ストレージ：キャプチャファイルのオプションの設定」を参照してください。
- オンプレミスのインストールには、MinioやIBM Cloud Object StorageなどのAWS互換のカスタムストレージを使用するオプションもあります。カスタムS3エンドポイントの設定を参照してください

キャプチャファイルを作成する

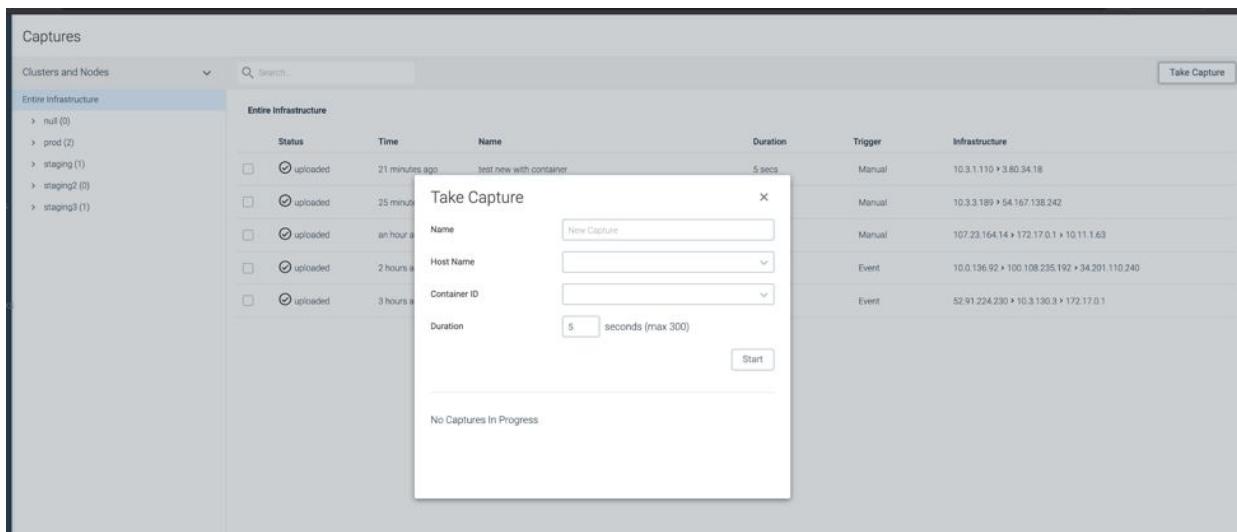
キャプチャファイルは、ポリシーの一部として設定するか、キャプチャーモジュールから手動で作成することにより、Sysdig Secureで作成できます。

注意

ポリシーの一部としてキャプチャを作成する方法の詳細については、「ポリシーの管理」を参照してください。

キャプチャファイルを手動で作成するには：

1. [Captures]モジュールから[Take Capture]ボタンをクリックして、キャプチャ作成ウィンドウを開きます。



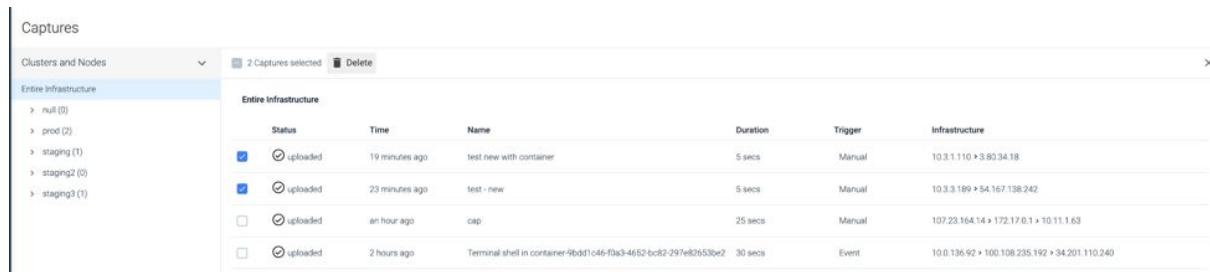
2. キャプチャの名前を定義します。
3. キャプチャーファイルがシステムコールを記録するホストとコンテナを構成します。
4. キャプチャの期間を定義します。最大長は300秒（5分）です。

5. [Start]ボタンをクリックします。

Sysdigエージェントは、キャプチャーを開始し、結果のトレースファイルを送り返すように通知されます。その後、ファイルはキャプチャーモジュールに表示されます。

キャプチャファイルを削除する

1. [Captures]モジュールから、削除するキャプチャーファイルを選択します。
2. [Delete] (ゴミ箱) アイコンをクリックします。



Status	Time	Name	Duration	Trigger	Infrastructure
<input checked="" type="checkbox"/> uploaded	19 minutes ago	test new with container	5 secs	Manual	10.3.1.110 > 3.80.34.18
<input checked="" type="checkbox"/> uploaded	23 minutes ago	test - new	5 secs	Manual	10.3.3.189 > 54.167.138.242
<input type="checkbox"/> uploaded	an hour ago	cap	25 secs	Manual	107.23.164.14 > 172.17.0.1 > 10.11.1.63
<input type="checkbox"/> uploaded	2 hours ago	Terminal shell in container-9bdd1c46-f0a3-4652-bc82-297e82653be2	30 secs	Event	10.0.136.92 > 100.108.235.192 > 34.201.110.240

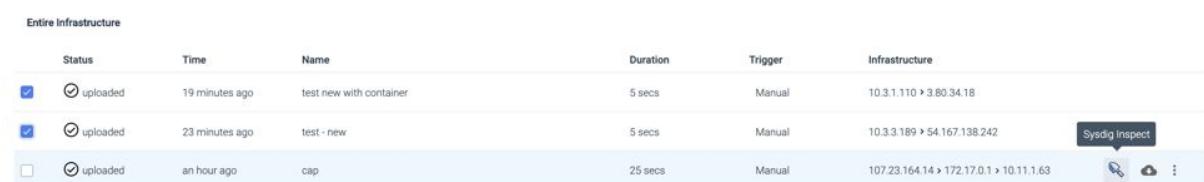
3. [Yes] (チェック) アイコンをクリックしてキャプチャの削除を確認するか、[No] (クロス) アイコンをクリックしてキャンセルします。

キャプチャファイルの確認

Sysdig Inspectでキャプチャファイルを確認する

Sysdig Inspectでキャプチャファイルを確認するには：

1. [Captures]モジュールから、削除するキャプチャーファイルを選択します。
2. Inspect (Sysdigロゴ) アイコンをクリックして、新しいブラウザタブでSysdig Inspectを開きます。



Status	Time	Name	Duration	Trigger	Infrastructure
<input checked="" type="checkbox"/> uploaded	19 minutes ago	test new with container	5 secs	Manual	10.3.1.110 > 3.80.34.18
<input checked="" type="checkbox"/> uploaded	23 minutes ago	test - new	5 secs	Manual	10.3.3.189 > 54.167.138.242
<input type="checkbox"/> uploaded	an hour ago	cap	25 secs	Manual	107.23.164.14 > 172.17.0.1 > 10.11.1.63

キャプチャーファイルをダウンロードする

キャプチャーファイルをダウンロードするには：

1. [Captures](#) モジュールから、ターゲットキャプチャーファイルを選択します。
2. [Download] アイコンをクリックして、キャプチャーファイルをダウンロードします。

Entire Infrastructure						
Status	Time	Name	Duration	Trigger	Infrastructure	
<input checked="" type="checkbox"/>	⌚ uploaded	19 minutes ago	test new with container	5 secs	Manual	10.3.1.110 ➤ 3.80.34.18
<input checked="" type="checkbox"/>	⌚ uploaded	23 minutes ago	test - new	5 secs	Manual	10.3.3.189 ➤ 54.167.138.242
<input type="checkbox"/>	⌚ uploaded	an hour ago	cap	25 secs	Manual	107.23.164.14 ➤ 172.17.0.1 ➤ 10.11.1.63

これで、キャプチャーファイルがローカルマシンにダウンロードされます。

キャプチャ機能を無効にする

セキュリティ要件により、キャプチャ機能をまったくトリガーしないように指示される場合があります（支払い情報におけるPCIコンプライアンスなど）。

キャプチャを完全に無効にするには、「[キャプチャの無効化](#)」の説明に従ってエージェント設定ファイルを編集します。