



キャプチャー

Captures





本文の内容は、Capturesのドキュメント(<https://docs.sysdig.com/en/captures.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保存	3
Sysdigキャプチャーの設定	3
キャプチャーファイルを作成する	3
キャプチャーファイルをダウンロードする	4
キャプチャファイルの削除	4
すべてのキャプチャファイルを削除するには :	5
キャプチャファイルの確認	5
キャプチャファイルを探索する	5
キャプチャファイルの調査	5



キャプチャー

Sysdigキャプチャーファイルには、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、キャプチャーファイル名、取得元のホスト、時間枠、およびキャプチャーのサイズを一覧表示するテーブルが含まれています。キャプチャー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、ダウンロードおよび分析に使用できます。

キャプチャーファイルの保存

Sysdigキャプチャーファイルは、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：キャプチャー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。

キャプチャーファイルの作成、構成、分析の詳細については、以下をご覧ください。

- Sysdigキャプチャーの設定
- キャプチャーファイルの確認

Sysdigキャプチャーの設定

キャプチャーファイルを作成する

1. キャプチャーファイルを作成するには：
2. エクスプローラーモジュールから、ホストまたはコンテナを選択します。
3. [Settings（省略記号）]ドロップダウンメニューをクリックし、[Sysdig Capture]を選択します。
Sysdig Captureポップアップウィンドウが開きます。
4. 以下のパラメーターを定義し、「Start Capture」ボタンをクリックします。



パラメーター	説明
Capture path and name	キャプチャーファイルの名前。デフォルト名には、キャプチャーが作成された日付とタイムスタンプが含まれています。
Time frame	キャプチャーされた期間。デフォルトの時間は15秒です。利用可能な最大キャプチャー時間は24時間です。キャプチャーファイルのサイズ制限は100MBです。 注意 Sysdigでは、デフォルトの時間を使用して、キャプチャーを小さく管理しやすいものにするをお勧めします。
Filter	収集されるトレース情報の量を制限します。利用可能なフィルターの例を含む詳細については、 Sysdig Github ページを参照してください。
Storage	キャプチャーファイルの保存場所。デフォルトの保存場所はSysdig Cloud Amazon S3バケットです。カスタムS3ストレージバケットを設定するには、「AWSキャプチャファイルストレージの設定」を参照してください。

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返信するように通知されます。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：

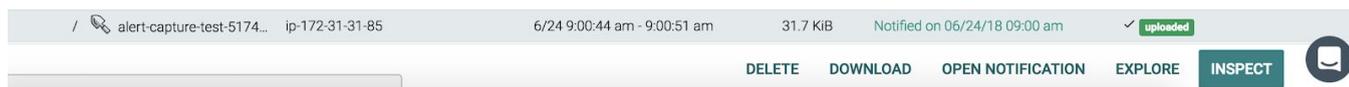
1. **Captures** モジュールから、ターゲットキャプチャファイルに移動します。
2. ターゲットキャプチャーファイルを選択します。
3. ダウンロードボタンをクリックします。キャプチャーファイルがローカルマシンに自動的にダウンロードされます。

キャプチャファイルの削除



1つのキャプチャファイルを削除するには：

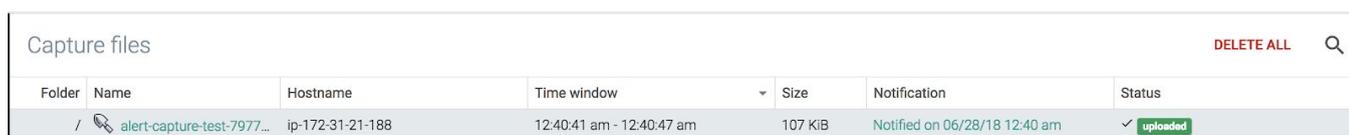
1. **Captures** モジュールから、削除するキャプチャーファイルを選択します。
2. **Captures** モジュールの下部にある **[Delete]** ボタンをクリックします。



3. **[Keep File]** プロンプトで、**[Delete]** ボタンをクリックして確定するか、**[Keep File]** ボタンをクリックしてキャンセルします。

すべてのキャプチャファイルを削除するには：

1. **Captures** モジュールで、**[Delete All]** ボタンをクリックします。



2. **[Yes, Delete Captures]** ボタンをクリックして確定するか、**[Cancel]** ボタンをクリックします。

キャプチャファイルの確認

キャプチャファイルを探索する

1. キャプチャーモジュールから、ターゲットキャプチャーファイルに移動します。
2. ターゲットキャプチャーファイルを選択します。インターフェイスの下部にいくつかのアクションボタンが表示されます。
3. **[Explore]** ボタンをクリックします。キャプチャの **[Explore]** タブビューに移動します。

キャプチャファイルの調査

1. **Captures** モジュールから、ターゲットキャプチャーファイルに移動します。
2. ターゲットキャプチャーファイルを選択します。インターフェイスの下部にいくつかのアクションボタンが表示されます。
3. **Inspect** ボタンをクリックします。キャプチャーの Sysdig Inspect ページに移動します。