

エクスプローラー Explore

•



本文の内容は、Exploreのドキュメント(<u>https://docs.sysdig.com/en/explore.html</u>)を 元に日本語に翻訳・再構成した内容となっております。





エクスプローラー

Sysdig モニター Webインターフェースは、インフラストラクチャー監視操作の大部分をエクスプロー ラーモジュールを中心に行う事ができます。エクスプローラーを使用すると、インフラストラク チャースタックの主要なメトリクスとエンティティを表示およびトラブルシューティングを行えま す。Sysdig モニターは自動的にスタックを検出し、エクスプローラーに事前に作成されたビューを表 示します。インフラストラクチャー階層の任意のレイヤーにドリルダウンして、詳細なレベルのデー タを表示できます。グループ化は、エクスプローラーにおいてエンティティの編成方法をコントロー ルできます。グループ化は、コンテナ、Kubernetesクラスター、サービスなどの論理レイヤーによっ て完全にカスタマイズを行う事が可能です。

次のセクションで、エクスプローラーの使用方法について詳しく学習していきます。

- エクスプローラーインターフェース
- エクスプローラーテーブル
- タイムウインドウ
- エクスプローラーワークフロー

エクスプローラーインターフェース

以下のセクションでは、インターフェースの主要な領域の概要と基本的なナビゲーション手順の詳細 について説明します。

Cーフレーム構造







以下の画像は、SysdigモニターのC-フレームスタイルのインターフェースの全体像を示しています。

上の画像で強調表示されているいくつかの重要なエリアがあります:

セクション	説明
Product Selector	ユーザーがSysdig プロダクトを切り替えられるようにします。
Modules	主なSysdigモニターモジュール(エクスプローラー、ダッシュボード、 アラート、イベント、キャプチャ)のクイックリンク。
Management	Sysdig Spotlight、ヘルプ/追加資料、およびユーザープロファイル構成 設定のクイックリンク。
Page	インターフェースのメインセクション。
Time Navigation	ユーザーがデータの表示に使用される時間枠をカスタマイズできるよう にします。





共有コンテンツの設定

Sysdig Monitorは、データ、ダッシュボード、および構成設定を共有することにより、ユーザーが個々 のレベルで、またはより大きなチーム内で作業できるようにする幅広い機能を提供します。Sysdig Monitorの各コンポーネントへの影響は異なります。

エクスプローラーモジュール

エクスプローラーモジュールは、ユーザーごと、チームごとにコンテンツを表示します。ユーザーが より広い範囲の権限を持つ他のチームに属している場合でも、エクスプローラーモジュール内に表示 されるデータのセットは、チーム設定で許可されている範囲に制限されます。列の順序など、エクス プローラーテーブルの設定に対する変更は、現在のユーザーに対してのみ保持され、他のチームメン バーの設定は変更されません。

エクスプローラで個々の行をクリックすると、対応するダッシュボードビューが表示されます。[ダッ シュボード]ビューには、選択されたエンティティのリソース使用量に関する健全性が要約されていま す。

ダッシュボードモジュール

ダッシュボードモジュールは、ユーザーごと、チームごとにコンテンツを表示します。初めて新しい チームに切り替えた後、初期設定は既存のチームメンバーの設定と一致します。これは、たとえば、 自分と共有されている各ダッシュボードの初期特性は、ダッシュボードの所有者の初期特性と同じに なることを意味します。

ダッシュボードを使用するときは、次のガイドラインを考慮してください。

- 特定のチームに切り替えられている間にユーザーが作成したダッシュボードは、ユーザーがそのチームに切り替えられている間のみ表示されます。ダッシュボードが共有されている場合、その特定のチームのメンバーにのみ表示されます。
- ダッシュボード内に表示されるデータのセットは、ユーザーがより広いスコープ権限を持つ他のチームに属している場合でも、チームのスコープ設定で許可されているものに制限されます。





共有ダッシュボードに加えられた変更は、現在のユーザーに対してのみ保持され、他のチーム
 メンバーのダッシュボードは変更されません。

イベントモジュール

イベントデータはアクティブなチーム固有になります。カスタムイベントセクションは、少なくと も、アクティブなチームのメンバーのAPIトークンによって生成されたイベントで構成されます。ただ し、チームの設定により、Sysdigモニター環境内で収集されたすべてのカスタムイベントをチームにも 表示できる場合があります。チームの設定を確認するには、管理ユーザーに連絡してください。

アラートモジュール

アラート設定はチーム全体です。チームメンバーは誰でもチームのアラート設定を変更でき、それらの変更はチームの他のすべてのメンバーにすぐに表示されます。

キャプチャモジュール

キャプチャは、アクティブなチームのスコープ設定内に表示されているホスト/コンテナでのみ実行で きます。キャプチャーモジュールに表示される既存のキャプチャーのリストも、アクティブなチーム に切り替えられているときにチームメンバーによって開始されたものに制限されます。

APIトークン

Sysdig モニター APIトークンはチームごとに固有であり、APIを介して生成されたカスタムイベントが 特定のチームを対象とすることを可能にします。

グローバル設定

ー部の構成設定は、すべてのチームにわたってグローバルです。ユーザーによるこれらの設定の変更 は、チームのステータスに関係なく、すべてのユーザーに影響します。これらには、通知チャネル、 エージェントインストールのデフォルト、Sysdigストレージの設定が含まれます。





エクスプローラーテーブル

このセクションは、SysdigモニターUIのエクスプローラーテーブルをナビゲートに関して説明を行います。。

データソース

データソースの切り替え 使用可能なデータソースを切り替えるには:

1. [Explore]タブで、[On the Explore tab, click the Data Source (2つの四角形)]ドロップダウンメ ニューをクリックします。

HOSIS & C	Jontainers		
SWITCH DATA SOURCE	▲ Insta		
🗞 Sysdig Agents	0)		
🚏 AWS Services	41d4b-11k		
EC2	141d4b-40r		
RDS	41d4b-kh1		
ELB			
ALB	5)		
ElastiCache			
SQS	1)		
DynamoDB			

2. ドロップダウンリストから目的のデータソースを選択します。

グルーピング

グループはタグの階層構造であり、ユーザーはインフラストラクチャービューをエクスプローラタブ で論理階層に編成できます。 グループ化の詳細については、メトリクスのグループ化、スコープ、お よびセグメント化を参照してください。

テーブルサーチ





エクスプローラーテーブルの検索バーを使用すると、部分的または完全な名前の文字列に基づいて、 インフラストラクチャーオブジェクトの現在のグループを検索できます。

たとえば、以下の検索では、gke-を含むすべての結果が表示されます:

Exp	lore							
	Hosts & Containers	•	host.hostName 💌 🗙	container.id 🔻 🗙	Ð	Q	gke ×	\$
Name		• c	loudProvider.insta	cpu.used.perce	memory.used.p	net.bytes.total	net.request.cou	fs.roo
~	Entire Infrastructure (44)			8.7	11.2	86.9	21.3	
	> gke-overview-test-default-pool-e6.	2		16.3	25.5	135.7	22.3	
	> gke-overview-test-default-pool-e6.	~		27.9	33.3	124.1	13.7	
	> gke-overview-test-default-pool-e6.			22.3	22.9	237.4	135.5	

上記の各結果は、検索パラメーターから始まります。ただし、以下の例では、正確な名前の知識は必 要ないことを示しています。

= • 🚹	Hosts & Containers 🔹 host.hostN	ame 🔻 🗙 contai	ner.id 🔻 🗙 🕀			Q 1-	×
Name	 Instance Type 	CPU % %	Memory Us	Network Byt	Requests In	FS Root Usa	FS Largest
∽ Entire In	frastructure (10)	32.6	6.5	15.3	0.2	29.0	29.0
> gke-	dev-pool-1-14a41d4b	41.5	9.5	17.1	0.5	9.1	9.1
> gke-	dev-pool-1-14a41d4b	70.2	11.5	28.2	0.5	9.7	9.7
> gke-	dev-pool-1-14a41d4b	99.5	11.1	39.3	0.5	9.1	9.1
> ip-1	72-31-17-37 (1)	78.1	4.2	18.1	0	56.4	56.4
> ip-1	72-31-21-188 (5)	0	1.8	<0.1	0	100.0	100.0
> ip-12	72-31-22-60 (1)	0.3	4.2	3.6	0	37.5	37.5
> ip-12	72-31-29-177 (1)	0.5	4.0	3.7	0	36.4	36.4
> ip-1	72-31-30-9 (1)	3.1	4.5	22.7	0	55.9	55.9
> ip-1	72-31-31-85 (1) 🏚	0.3	4.2	3.7	0	37.5	37.5

上記の結果には、名前のどこにあるかに関係なく、名前に1-を含むすべてのインスタンスが含まれます。

テーブルの列

エクスプローラーテーブルの列には、それぞれ異なるメトリクスが表示されます。これらの列は、イ ンフラストラクチャーに必要な正確な情報を表示するように構成できます。





注意

既存の列の順序への変更は、列が追加または削除されない限り、グループ間で永続的ですが、ログ イン間では永続的ではありません。

テーブル列の並べ替え

テーブルの列を並べ替えるには:

1. [Explore]タブで、マウスカーソルを関連する列ヘッダーの上に移動し、左ボタンを押したままに します。 左側に太い壁の境界線が表示されます。

Expl	ore	Met	ric: cpu.used.percent	1				
	Hosts & Containers	→ ho Grou	e: Rate Ip: Average	ntainer.id 🔻 🗙	\oplus			
Name		Network B	¢ / ≑ / ^{℃PU °} CPU %	% Memory U	Requests I	FS Root Us	F	File Bytes
~	Entire Infrastructure (9)	25.0	38.7	21.9	1.6	26.0	26.0	0.5
>	→ gke-dev-pool-1-14a41d	17.3	41.8	9.6	0.5	9.1	9.1	0.1
>	→ gke-dev-pool-1-14a41d	28.5	70.2	11.6	0.5	9.7	9.7	0.2
>	→ gke-dev-pool-1-14a41d	39.5	99.3	11.1	0.5	9.1	9.1	0.5
>	ip-10-0-1-139.ec2.intern	41.2	1.2	24.7	10.2	73.2	73.2	0.1
>	ip-10-0-1-152.ec2.intern	18.4	7.0	16.9	0	36.6	36.6	0.3
>	ip-10-0-2-240.ec2.intern	34.6	79.9	30.5	2.2	32.7	32.7	2.2
>	ip-10-0-3-74.ec2.interna	39.9	53.0	83.8	0.8	27.8	27.8	1.6
>	ip-172-31-21-188 (1)	3.7	0.3	4.0	0	31.8	31.8	<0.1
	localhost.localdomain	2.7	0.2	5.6	0	4.6	4.6	<0.1

2. ボーダーマーカーが目的の場所に来るまで列をドラッグし、左ボタンを放して変更を確定しま す。

テーブル列の設定

列は、テーブル構成チェックリストで追加/削除できます:



チェックリストに加えられた変更は、ログイン間で保持されます。





メトリクステーブルの列を構成するには:

- 1. 「Explore」タブで、Settings (歯車) アイコンをクリックして、テーブル設定パネルを開きま す。
- メトリクスドロップダウンメニューを開いてメトリクスを追加または変更し、集約ドロップダウン メニューを開いて関連する時間とグループの集約を構成します。

Configure Table Columns

cloudProvider.instance.type	•	CONCAT -	\times
cpu.used.percent	•	RATE -	×
memory.used.percent	•	RATE -	×
net.bytes.total	•	RATE -	×
net.request.time.in	•	AVG -	×
fs.root.used.percent	•	AVG -	×
fs.largest.used.percent	•	AVG -	×
file.bytes.total	•	RATE -	×
net.request.count.in	×	RATE -	×
net.request.count.out	•	RATE -	×
net.http.error.count	•	AVG -	×
cpu.stolen.percent	•	RATE -	×
	-		



3. [save]ボタンをクリックして変更を保存します。

色分けを設定する





テーブルの列は、色を使用して値を強調表示し、エクスプローラーテーブルの読みやすさを向上させるように設定できます。

列の色分けを設定するには:

1. エクスプローラモジュールで、目的の列のEdit (鉛筆)アイコンをクリックします。

Metr Time Grou	ric: net.bytes.total e: Rate up: Average	
¢ /	net.bytes.total B/s	•
	29.3	
	4.7	
	<0.1	
	71.2	

2. 有効化スイッチを切り替えます。



3. 必要に応じてカラー値を設定します。変更は自動的に行われます。





テーブルの列をデフォルトに戻す

デフォルトのメトリクステーブルの列を復元するには:

- 1. エクスプローラーモジュールで、Settings定(歯車)アイコンをクリックして、テーブル設定 パネルを開きます。
- 2. [Restore Defaults]ボタンをクリックします。
- 3. [save]ボタンをクリックして変更を保存します。

ドリルダウンメニュー

Sysdig モニターユーザーは、エクスプローラーテーブルに表示できる多数のダッシュボードとメトリ クスを使用して、インフラストラクチャーヘドリルダウンできます。これらの表示は、インフラスト ラクチャーオブジェクトを選択し、ドリルダウンメニューを開くと見つけられます。

注意

Sysdigモニターは、選択したインフラストラクチャーオブジェクトに関連するメトリクスとダッシュ ボードのみを表示します。

ドリルダウンメニューの固定/固定解除 ドリルダウンメニューを[Explore]タブに固定するには:

1. 「Explore」タブで、インフラストラクチャオブジェクトを選択します。







2. ドリルダウンメニューを開きます。



3. [Pin Menu]リンクをクリックして、メニューを[Explore]タブに固定します。

メニューの固定を解除するには、メニューの下部にある[Unpin Menu]リンクをクリックします。





>	Recently Used	
~	🖬 Default Dashboards	
	> Applications	
	> Hosts & Containers	
	> Network	
	> Services	
	> Topology	
>	📰 My Dashboards	
~	Metrics	
	> Containers (16)	
	> File (24)	
	> Network (76)	
	> Process (4)	
	> System (40)	
	Unpin Menu	

ダッシュボード

ドリルダウンメニューには、選択したインフラストラクチャオブジェクトに関連する使用可能なすべてのダッシュボードが表示されます。これらのダッシュボードは2つのセクションに分かれています。

- Default Dashboardsは、Sysdigモニターによって事前定義されたものです。
- My Dashboardsは、現在のユーザーによって作成された、または現在のユーザーと共有されているダッシュボードです。

ダッシュボードを表示するには:

- 1. [Explore]タブで、インフラストラクチャーオブジェクトを選択します。
- 2. ドリルダウンメニューを開きます。
- 3. [Default Dashboards]または[My Dashboards]ドロップダウンメニューから目的のダッシュボード を見つけて選択します。



Hosts & Cont 🔻	E Container Limits	: ×
Q Search environment	Scope: host.hostName = 'gke-dev-pool-1-14a41d4b-40rc'	
 Entire Infrastructure (9) > gke-dev-pool-1-14a41d4b-11kz 	CPU Shares Used	CPU Quota Used
 > gke-dev-pool-1-14a41d4b-40rc > gke-dev-pool-1-14a41d4b-kh1 > ip-10-0-1-139.ec2.internal (10) > ip-10-0-1-152.ec2.internal (> ip-10-0-2-240.ec2.internal (113) 	100 % 0 11:45 Thu 28 12:15 12:30	100 % 0 11:45 Thu 28 12:15 12:30
 ip-10-0-3-74.ec2.internal (85) ip-172-31-21-188 (1) 	Memory Limit Used	Memory Limit
localhost.localdomain	100 % 0 11/45 Tu 28 12/15 12/20	954 MB

これで、ユーザーがナビゲートするまで、エクスプローラーテーブルの代わりにダッシュボードが表 示されます。

注意

ダッシュボードのスコープは、ドリルダウンメニューで表示される場合、エクスプローラーテーブ ルから選択されたインフラストラクチャーオブジェクトに設定されます。

メトリクス

Sysdig Monitorユーザーは、ドリルダウンメニューをナビゲートすることにより、インフラストラク チャオーブジェクトの特定のメトリクスを表示できます。

- 1. [Explore]タブで、インフラストラクチャオブジェクトを選択します。
- 2. ドリルダウンメニューを開きます。
- 3. [Metrics]ドロップダウンメニューを移動し、目的の指標を選択します。





Hosts & Cont 🔻	✓ container.count ▲
Q Search environment	Q Search Metrics and Dashboards
✓ Entire Infrastructure (9)	> 🕓 Recently Used
> gke-dev-pool-1-14a41d4b-11kz	> E Default Dashboards
> gke-dev-pool-1-14a41d4b-40rc	> 📰 My Dashboards
> gke-dev-pool-1-14a41d4b-kh1	✓ ✓ Metrics
> ip-10-0-1-139.ec2.internal (10)	> App Checks
> ip-10-0-1-152.ec2.internal (18)	✓ Containers
> ip-10-0-2-240.ec2.internal (109)	container.count
> ip-10-0-3-74.ec2.internal (89)	cpu.quota.used.percent
> ip-172-31-21-188 (5)	cpu.shares.count
localhost.localdomain	cpu.shares.used.percent
	memory.limit.bytes
	memory.limit.used.percent
	swap.limit.bytes
	swap.limit.used.percent
	> Docker Orchestration
	> File
	> Host
Back to Explore Table	Pin Menu

これで、ユーザーがナビゲートするまで、Exploreテーブルの代わりにメトリクスが表示されます。







注意

メトリクスのスコープは、ドリルダウンメニューを介して表示される場合、エクスプローラーテー ブルから選択されたインフラストラクチャーオブジェクトに設定されます。

タイムウインドウ

デフォルトでは、Sysdigモニターはライブモードで情報を表示します。 つまり、ダッシュボード、パ ネル、エクスプローラーテーブルは、時間の経過とともに新しいデータで自動的に更新され、設定さ れた時間枠で使用可能な最新のデータが表示されます。

注意

デフォルトでは、タイムナビゲーションは2時間の時間枠でライブモードに入ります。

タイムウィンドウナビゲーションバーは、一般的なタイムウィンドウへのクイックリンクのほか、履 歴データを確認するためにカスタム期間を設定する機能をユーザーに提供します。

LIVE: 1:00 pm - 2:00 pm (1 H) JST 10 S 1 M 10 M 1 H 6 H 1 D 2 W CUSTOM II II - ZOOM 2x +

上の図に示すように、ナビゲーションバーにはいくつかの情報が表示されます。

- データの状態(ライブまたは過去)
- 現在の時間枠
- 設定されたタイムゾーン

さらに、ナビゲーションバーには次の機能があります。

一般的なタイムウィンドウのクイックリンク(10秒、1分、10分、1時間、6時間、1日、2週
 間)





- カスタムの時間枠構成オプション
- 一時停止/再生ボタン。ライブモードを終了し、データをタイムウィンドウに固定し、ライブ モードに戻ります
- 前後のボタンに移動して、フリーズした時間枠をジャンプして履歴データを確認します
- タイムウィンドウを拡大/縮小するためのズームイン/アウトボタン

カスタム期間を構成する

タイムナビゲーションドロップダウンパネルを使用して、特定の時間範囲を構成できます。手動範囲 を構成するには:

- 1. [Explore]タブまたは[Dashboards]タブで、時間ナビゲーションバーのカスタムリンクをクリック します。
- 2. 開始点と終了点を設定し、[Adjust Time]ボタンをクリックして変更を保存します。



カスタムタイムウィンドウにはいくつかの制限が適用されます。詳細については、「時間枠の制限」 セクションを参照してください。

時間枠の制限

一部の時間枠構成は、特定の状況では使用できない場合があります。これらのインスタンスでは、時間枠の変更が自動的に適用され、警告通知が表示されます。

Time modification applied. 2 ×





時間枠が利用できない主な理由は2つあります。どちらもデータの粒度と特異性に関連しています。

- 時間枠は、有効期限が切れて使用できなくなったデータの粒度を指定します。たとえば、6か月前から1時間の時間範囲を指定する時間枠は使用できず、その結果、時間枠は少なくとも1日の時間範囲に変更されます。
- グラフは特定の数のデータポイントしか処理できないため、タイムウィンドウは、ウィンドウのサイズを考えると高すぎるデータの粒度を指定します。たとえば、複数時間の時間範囲には、1分単位のデータポイントが多すぎて、10分単位に自動的に変更されます。

