

アドミニストレーション 設定



本文の内容は、Administration Settingsのドキュメント

(<u>https://docs.sysdig.com/en/administration-settings.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。

アドミニストレーション設定	10
アクセス設定パネル	10
設定パネル:管理者とユーザー	10
ユーザープロファイルとパスワード	11
[ユーザープロファイル]ページにアクセス	11
ユーザーのメール、役割、現在のチームを確認する	12
管理者設定の変更(管理者のみに表示)	13
Sysdig APIトークンを取得する	13
パスワードの変更	14
SysdigLabsのベータ機能を有効にする	14
ユーザーとチームの管理	15
Sysdigユーザーについて	15
システムベースの特権	15
Sysdigチームについて	16
チームの目的	16
運用チームとデフォルトチーム	18
チームベースの役割と特権	18
チームメンバーシップがUIのユーザーエクスペリエンスに与える影響	21
UIでのチームの切り替え	21



オンボーディングのベストプラクティス:	22
デフォルトでの新しいユーザー権限の制限	23
APIを介したユーザーとチームの統合	23
ユーザーの役割	23
チームの役割	23
ユーザー管理	24
ユーザーを作成する	24
ユーザー情報を編集	25
ユーザーを削除する	26
チームと役割の管理	26
チームを作成する	27
表1:チーム設定	27
チームのエントリページまたはダッシュボードを設定する	29
チームメンバーの追加と設定	29
チームにユーザーを割り当てる	30
ユーザーにチームベースの役割を割り当てる	31
チーム設定の編集	33
チームを削除する	33
通知管理	33
通知チャネルを追加する	34
通知チャネルを編集する	35
通知チャネルをテストする	36
Amazon SNS通知	37





メール通知	39
PagerDuty通知	40
前提条件	40
PagerDutyの設定	41
既知の問題	44
Slack通知	45
VictorOps通知	46
OpsGenie通知	48
Webhookチャネルを設定する	49
前提条件	49
UIで機能を有効にする	49
オプション:カスタムヘッダーまたはデータを設定する	50
ユースケースの例	50
標準アラート出力	52
POSTデータの説明:	52
POSTデータの例:	52
失敗の例	53
成功例	53
ServiceNowを設定する	54
ServiceNowSetup	54
前提条件	54
ServiceNow GUIでScripted Rest APIの詳細を作成する	54
新しいスクリプトAPIにコードを追加する	55





Sysdig Webhookセットアップ	56
統合テスト	57
通知チャネルを無効化または削除する	58
通知チャネルを一時的に無効にする	58
ダウンタイム中の通知のミュート	58
通知チャネルを削除する	59
アラートの起動遅延を設定する(オンプレミスのみ)	60
AWS:AWSアカウントとCloudWatchメトリクスを統合する(オプション)	61
Sysdig UIの2つのエントリポイント	61
ウェルカムウィザードからのアクセス	61
設定メニューからのアクセス	62
AWSアカウントを手動で統合する	64
AWSでは	64
Sysdigアクセス用のIAMポリシーを作成する	64
IAMユーザーを作成し、プログラムによるアクセスを許可する	65
SysdigモニターUI	65
アクセスと秘密鍵を入力してください	66
CloudWatch統合を有効にする	67
資格情報を再取得	67
Implicit Keyを使用してAWSアカウントを統合する(オンプレミスのみ)	67
Implicit Keyを使用	67
前提条件	67
Kubernetes	68





Replicated	69
ポーリングされるAWSサービスの変更	70
セキュリティグループ	70
特定のAWSリージョンのCloudWatchデータを取得する	70
関連情報	71
使用するIAMポリシーコード	71
AWSロールの委任と統合する	72
前提条件とガイドライン	73
APIでAWSロールの委任を有効にする	73
SaaSの手順	73
オンプレミスの手順	73
External IDを取得する	74
役割の委任を設定する	74
ロールARNを取得	75
AWSアカウントを追加する	76
オンプレミスの追加構成	77
例 : Kubernetesインストールで環境変数を設定する	78
リソースディスカバリのセットアップ	79
ストレージ : キャプチャーファイルのオプションの設定	79
AWS S3ストレージを設定する	80
前提条件	80
Sysdigモニター側	80
テストするには:SysdigモニターUIでトレースファイルをキャプチャーします。	80





カスタムS3エンドポイントを設定する	81
前提条件	81
インストーラーの設定	81
Customer Numberを見つける	84
エージェントのインストール:概要とキー	85
エージェントアクセスキーを取得する	85
サブスクリプション:ライセンスされたエージェントの数の変更	87
ライセンスの仕組み	89
予約済みエージェントとオンデマンドエージェント	89
エージェントをバックエンドに接続する	89
技術的な詳細	90
AWSサービスのライセンス	90
AWSサービスタイプの優先順位と制限	91
ユースケースの例	91
認証と承認(SaaS)	92
ワークフロー	94
Google OAuth(SaaS)	95
Google OAuthを有効にする	95
ユーザー体験	96
SAML (SaaS)	97
基本的な有効化ワークフロー	99
管理者の手順	100
IdPを設定する	100





設定でSAMLを有効にする	101
SAML接続設定を入力	101
SSOにSAMLを選択	102
ユーザー体験	102
注意事項	104
Okta (SAML)	104
Okta設定におけるSysdig固有の手順	104
Oktaステップ6	104
オクタステップ7	104
オクタステップ8	105
Oktaステップ10	105
メタデータのテスト(オプション)	105
OneLogin (SAML)	106
OneLogin構成におけるSysdig固有の手順	106
SAMLテストコネクタの追加	106
テストコネクタ設定ページの設定	106
発行者のURL	108
メタデータのテスト(オプション)	108
ADFS (SAML)	108
サービスプロバイダーが開始するログインフローの場合	109
IdPによって開始されるログインフローの場合(オプション)	122
メタデータのテスト(オプション)	125
OpenID Connect (SaaS)	126





概要	127
SysdigのOpenID機能の概要	127
基本的な有効化ワークフロー	127
管理者の手順	129
IdPを設定する	129
設定でOpenIDを有効にする	129
OpenID基本接続設定を入力してください	129
OpenIDの追加設定を入力します(必要な場合)	130
ユーザー体験	132
Okta (OpenID)	133
OktaのOpenIDプロバイダーの設定	133
OneLogin (OpenID)	134
OneLoginのOpenIDプロバイダーの設定	134
Keycloak (OpenID)	135
KeycloakのOpenIDプロバイダーの設定	136





アドミニストレーション設定

[設定]パネルには、Sysdig MonitorとSysdig Secure UIの両方から、および管理者ユーザーと非管理者 ユーザーの両方がアクセスできます。

アクセス設定パネル

Sysdig MonitorまたはSysdig Secureナビゲーションバーの左下隅からパネルにアクセスします。



設定パネル:管理者とユーザー

Sysdigプラットフォームの管理タスクには、設定パネルからアクセスします。管理者以外のユーザー は、一部のページにアクセスできます。管理者は、ユーザー、チームを管理し、ライセンスを追加す る追加の権限を持っています。

管理者としてログインすると、[設定]パネルに追加のリンクが表示されます。





管理者設定	管理者以外のユーザー設定
Settings	Settings
C User Profile	(User Profile
LUSers	Subscription Non-admins can view but not
Teams	change license count
Notification Channels	AWS
AWS	Agent Installation Can be hidden at
Sysdig Storage	Sysdig Storage
Subscription	
Agent Installation	
Authentication	

ユーザープロファイルとパスワード

ユーザープロファイルページにアクセスして、必要なアクションを確認および実行します。

[ユーザープロファイル]ページにアクセス

1. Sysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



2. [User Profile]を選択します。





User Profile	User profile	
Subscription	Account Name	@sysdig.com
Notifications	Role	Admin
AWS	Current Team	Monitor Operations
Agent Installation		
Sysdig Storage	Admin Settings	
Users	Hide Agent Install	() B
Teams	Allow od hos kierowkies in	Enabling this feature hides the Access Key and Agent Installation page for non-admin users.
	grouping	By enabling this you will be allowing grouping configurations to be formed in ad hoc orders. This may le inaccurate data in your dashboards, alerts and other parts of the application. This capability is available April 30th 2018. Please alter your groupings to follow the right hierarchies to avoid losing data at the en this period.
	Sysdig Monitor API	
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needed your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP AI custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needed your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password New password (confirm)	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needed your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password New password (confirm)	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website. CC RESET T DISCARD CHANCE PASS
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password New password (confirm) Sysdig Labs	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website. RESET T DISCARD CHANGE PASS
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password New password (confirm) Sysdig Labs Here you can find new functionali	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needed your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password New password New password (confirm) Sysdig Labs Here you can find new functionalities h the functionalities until they will b	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needed your current team. To retrieve your API token for another team, please switch to that team. Idig Monitor API, functions and use, refer to the Sysdig Monitor support website.
	Sysdig Monitor offers an HTTP Al custom scripts or programs, you Note, this API token is specific to For further information about Sys Sysdig Monitor API Token Password management Current password New password New password New password (confirm) Sysdig Labs Here you can find new functionalit Note: All the beta functionalities in the functionalities until they will b	PI to help easily access and automate routine tasks and monitor notifications. When accessing the API from y will need to supply the API security token below. Use the <i>Reset</i> token button to generate a new token if needer your current team. To retrieve your API token for another team, please switch to that team. dig Monitor API, functions and use, refer to the Sysdig Monitor support website.

3. 以下の設定を確認し、アクションを実行します。

ユーザーのメール、役割、現在のチームを確認する

現在のユーザーのログイン用メールアドレス、現在のチーム、およびそのチームでの役割が[ユーザー プロファイル]セクションに表示されます。





管理者設定の変更(管理者のみに表示)

管理者としてログオンしている場合は、このページの管理設定にグローバルに適用できます。

エージェントのインストールを非表示にする:このスライダーを切り替えて、設定メニューの
 エージェントのインストールリンクを管理者以外のユーザーから非表示にします。

設定パネルのナビゲート:管理者vsユーザーと<u>エージェントのインストール:概要とキ</u>ーも参 照してください。

Sysdig APIトークンを取得する

カスタムスクリプトまたはアプリケーションでSysdig APIを使用する場合、APIセキュリティトークン (各チームに固有)を提供する必要があります。

1. Sysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



 User Profileを選択します。SysdigモニターまたはSysdigセキュアAPIトークンが表示されます (ログインしたインターフェースとチームによって異なります)。

Sysdig Monitor API

Sysdig Monitor offers an HTTP API to help easily access and automate routine tasks and monitor notifications. When accessing the API from your custom scripts or programs, you will need to supply the API security token below. Use the *Reset* token button to generate a new token if needed. Note, this API token is specific to your current team. To retrieve your API token for another team, please switch to that team. For further information about Sysdig Monitor API, functions and use, refer to the Sysdig Monitor support website.

Sysdig Monitor API Token

eda3

COPY

RESET TOKEN

3. トークンを_{Copy}して使用するか、[Reset Token]ボタンをクリックして新しいトークンを生成でき ます。





注意

リセットすると、発行された以前のトークンはすぐに無効になり、プログラムまたはスクリプ トに適切な変更を加える必要があります。

パスワードの変更

[パスワード管理]フィールドを使用して、このユーザーのパスワードを変更します。

必須:最後に使用したパスワードではなく、8文字以上。連続する特殊文字を使用しないでください (例:&*()_は推奨されませんが、&a1*2S(は問題ありません)。

推奨:長さと一意性に重点を置いて、NISTの最新の推奨事項に従うことをお勧めします。

Sysdig Labsのベータ機能を有効にする

Sysdig Labsの下にリストされている機能設定を切り替えて、インストールに対する特定のベータ機能 を有効/無効にします。すでに保存されているデータは、ベータトグルの影響を受けません。

(ベータ機能がない場合、Sysdig Labsは表示されません。)





ユーザーとチームの管理

このページでは、Sysdigのユーザー、チーム、役割の権限の背後にある概念について説明します。

Sysdigユーザーについて

Sysdigのユーザーは、ユーザー名、電子メールアドレス、パスワード、またはサードパーティの認証オ プションで識別されます。

ユーザーは次のいずれかです。

- 管理者がSysdig UIを介して手動で招待する、または
- サードパーティのシステムを通じて認証されている、または
- 必要に応じて招待プロセスをバイパスできるAdmin APIを介してSysdigデータベースに直接入力します。

招待されると、新しいユーザーは、Sysdig UIへのユーザーの最初の正常なログイン時にSysdigデータ ベースに作成されます。ユーザーが招待を受け入れ、パスワードを入力してログインする前は、「保 留中」のステータスになっています。

システムベースの特権

最初から、Sysdig環境のユーザーは、3つのタイプのシステム特権のいずれかを持っています。

- (スーパー)管理者:これは、電子メールアドレスがSysdig請求先アカウントに関連付けられている管理者です。このユーザーは、すべてに対する管理者アクセス権を持っています。オンプレミスのインストールに最も関連しています。
- 管理者:すべての管理者は、すべてのユーザーに管理者システム権限を付与できます。管理者 は自動的にすべてのチームのメンバーになります。

管理者はユーザーを作成/削除できます。チームの作成/設定/削除;通知チャネルの作成/削除。 ライセンスを管理する。非管理者から非表示になっている[設定]メニューのリンクからエージェ ントを構成します。





ユーザー(非管理者):デフォルトでは、新しいユーザーはSysdigインターフェースでコンテンツを作成、削除、および編集するための読み取り/書き込み特権を持っています。管理者に制限されている設定メニューのオプションは表示されません。

ユーザー権限は、以下で説明するように、チームとチームの役割の割り当てに基づいてさらに 調整されます。

ユーザーが作成されると、デフォルトのチームに自動的に割り当てられます(下記を参照)。

警告

このデフォルトのワークフローでは、すべての新しいユーザーに編集アクセスが許可されています。

Sysdigチームについて

チームはサービスベースのアクセス制御と考えることができます。チームは、Sysdig MonitorとSysdig Secureで個別に作成および割り当てられます。

チームの目的

ユーザーをチームに編成すると、ユーザーのワークフローを改善しながら、データアクセスセキュリ ティポリシーを適用できます。さまざまなチームの役割があり、それぞれにアプリのさまざまな側面 への読み取り/書き込みアクセス権があります。

これにより、実際にデータを必要とする人だけにデータを公開することが制限され、関連するデータ に集中することでユーザーの生産性も向上します。







チームの潜在的な使用例を以下に示します。

- 「Dev」vs「Prod」:多くの組織は、本番データへのアクセスを制限することを好みます。物理インフラストラクチャとアプリケーションを分離することを許可します。
- マイクロサービス:個々の開発チームが独自のダッシュボードを表示し、独自のアラートに対応するためのデータのスコープ。Sysdig Monitorのオーケストレーションまたは構成管理メタデータを使用した論理的な分離に基づくチームの作成を許可します。
- サービスとしてのプラットフォーム:運用チームがプラットフォーム全体を確認する必要がある場所。特定の人がすべてのサービスのすべてのデータと基盤となるハードウェアを見ることができるようにします。これは、マルチテナント環境を管理しているマネージドサービスプロバイダーや、組織内の同様のモデルを使用してチームを開発するのに最適です。
- 制限された環境:セキュリティとコンプライアンスのためにデータアクセスを制限します。認証や請求などの特定のサービスには、それらへのアクセスを許可された非常に特定の個人のセットが含まれる場合があります。
- 効率化のためにモニタリングをセグメント化する必要がある組織:チームを形成してアクセス を簡素化する非常に大規模な組織から、一時的なトラブルシューティングチームを作成する小 さな組織まで、システムデータへのQAおよびサポートアクセスを最適化するために形成された チームまで、幅広いユースケース。





運用チームとデフォルトチーム

デフォルトテンプレートで、Sysdigプラットフォームには、製品ごとに1つの不変のチームがありま す。ライセンスに応じて、組織は次のいずれかまたは両方を使用できます。

- Monitor Operationsチーム
- Secure Operationsチーム

不変のオペレーションチームの主な特徴:

- チームは削除できません
- Operationsチームのユーザーは、その製品のすべてのリソースを完全に可視化できます
- 管理者は、チームの構成設定を変更する前にオペレーションチームに切り替える必要があります

管理者は追加のチームを作成し、任意のチームを指定してその製品のデフォルトチームにすることが できます。環境で許可されるチームの数は、ライセンスによって決まります。

SysdigモニターUIに入力されたユーザーは、モニターのデフォルトチームに自動的に割り当てられま す。SysdigセキュアUIに入力されたユーザーは、セキュアデフォルトチームに自動的に割り当てられ ます。

チームベースの役割と特権

ユーザーには、チームごとに基本的なシステム権限を拡張または制限する役割を割り当てることがで きます。

 システム
 チームの役割

 の役割
 チームの割り当てに関係なく、すべての権限を持つすべてのチームのメン

 Admin
 チームの割り当てに関係なく、すべての権限を持つすべてのチームのメン

 バー。
 すべてのユーザーを作成/削除/構成できます。

 すべてのチームを作成/削除/構成できます。



	Team Manager (Monitor)	Advanced User (Monitor)	Standard User (Monitor)	View Only (Monitor)
Non-Adm	ダッシュボード、ア	ダッシュボード、ア	エクスプロー	チームスコー
in (Sysdig	ラート、またはその	ラート、またはその	ラページにア	プ内の環境へ
Monitor)	他のコンテンツを作	他のコンテンツを作	クセスできな	の読み取りア
	成/編集/削除できま	成/編集/削除できま	い上級ユー	クセス権。た
	す+チームメンバー	す。	ザーに相当し	だし、ダッ
	を追加/削除した		ます(たとえ	シュボード、
	り、チームメンバー		ば、監視情報	アラート、ま
	の権限を変更したり		に興味がない	たはその他の
	できます。		開発者向	コンテンツを
	注:チームマネー		け)。	作成、編集、
	ジャーは、自分がマ			または削除す
	ネージャーとして指			ることはでき
	定されている特定の			ません
	チーム内でのみユー			
	ザー管理権限を持ち			
	ます。			



	Team Manager (Secure)	Advanced User (Secure)	Standard User (Secure)	View Only (Secure)
Non-Adm in (Sysdig Secure)	上級ユーザーと同じ 権限+チームメン バーの追加/削除、 またはチームメン バーの権限の変更。 注:チームマネー ジャーは、自分がマ ネージャーとして指 定されている特定の チーム内でのみユー ザー管理権限を持ち ます	読み取りおよび書き 込みモードで、チー ムスコープ内のすべ てのセキュア機能に アクセスできます。 上級ユーザーは、ラ ンタイムポリシー、 イメージスキャンポ リのコンテンツを作 成、できます。上級 ユーザーはユーザー を管理できません。	コメキにしスをチプイテをすザチク監シたキの込クサンーャプ、キ表一内ムィ表。一マテ査一はュ特みセイテジンッイャ示ムのセイ示標は一ィ、定他ア定機スナをキシメンしスラキベで準、クビポ義の機の能です。 シスート結 コンユンきユベ、テリ、セ能書にきてま しょりトまーンアィ ま 内きアま	チームスコークの能り権ラリメンまのをとんのキーのため、シシーポたコ変は、シシージリはン更では、ポイキー、他ツこせん。
			-	

詳細については、<u>チームメンバーシップがUIのユーザーエクスペリエンスに与える影響</u>を参照してく ださい。





チームメンバーシップがUIのユーザーエクスペリエンスに与える影響

チームメンバーシップは、Sysdig MonitorまたはSysdig Secure UIのユーザーエクスペリエンスにさまざ まな方法で影響します。

最上位レベルでは、表示されるダッシュボード、アラート、およびポリシーイベントは、切り替え先のチームの設定によって制限されます。

より詳細には、チーム設定は以下に影響します。

- デフォルトのランディングページ: UIエントリポイントはチームごとに設定されます。
- [Explore]タブとダッシュボード:これらはチームごと、ユーザーごとに設定され、チームと共有できます。

最初のログイン時に、すべてのチームメンバーに同じ[自分に割り当てられたダッシュボード] ビューが表示されます。ユーザーがそれらのダッシュボードを変更すると、そのユーザーのみ が変更を確認できます。

チームの一部として作成されたダッシュボードは、そのチームにログインしているときにのみ ユーザーに表示され、共有されている場合、他のチームメンバーにのみ表示されます。

- 可視データ:チームのスコープ設定により、チームメンバーがチームに切り替えられている 間、ユーザーが追加のデータを公開する異なる設定を持つ他のチームに属している場合でも、 チームメンバーに表示されるデータが制限されます。たとえば、Sysdig Secureでは、スコープ 内で発生したポリシーイベントのみが表示されます。
- アラートとイベント:これらの設定はチーム全体です。チームのメンバーは誰でもチームのア ラート設定を変更でき、追加や編集はチームのすべてのメンバーに表示されます。
- キャプチャ:チームメンバーに表示されるホスト/コンテナでのみ取得でき、メンバーは現在の チームに切り替えられた他のメンバーによって開始されたキャプチャのリストのみを表示しま す。
- APIトークン: [Settings]> [User Profile]にあるSysdigモニターAPIトークンは、ユーザーごと、チームごとに一意であることに注意してください。(「ユーザープロファイルとパスワー」)
 ド」を参照してください。これは、特定のチームを対象とするAPIを介したカスタムイベントの生成を有効にするために必要です。)





UIでのチームの切り替え

ユーザーは割り当てられているすべてのチームを切り替えることができ、管理者は作成されているす べてのチームを切り替えることができます。

そうするには:

1. ナビゲーションバーの左下隅にあるセレクタボタンをクリックします。

このユーザーに割り当てられたチームは、[Switch Teams]の下に表示されます。



2. 別のチーム名をクリックします。

ポップアップウィンドウに、新しいチームベースの環境ビューの概要が表示されます。UIはチームの設定に応じて変化します。

オンボーディングのベストプラクティス:

チームと役割を戦略的に計画して、データへのアクセスを分離し、インターフェースをカスタマイズ し、ワークフローを合理化します。

一般に、管理者は次のことを行う必要があります。





- 計画的にチームを作成し、ユーザーを招待し、役割を設定する
- 特定のチームが開始するためのいくつかのダッシュボードとアラートから始めます

注:ユーザーが初めてチームにログインすると、そのチームに固有のダッシュボードやアラートなど を紹介するウィザードが表示されます。

デフォルトでの新しいユーザー権限の制限

デフォルトでは、新しいユーザー(手動またはサードパーティのオーセンティケーターを介して追加 されたユーザー)には、上級ユーザー権限が割り当てられています。管理者が新しいユーザーの権限 をさらに制限したい場合は、いくつかの方法があります。

 招待状の送信からユーザーの最初のログインまでの間に、デフォルトの監視チームでのユー ザーの役割を「ユーザーの読み取り」に変更します。

理論的には、ユーザーが一時的に「編集」ステータスになるラグが生じる可能性があることに 注意してください。

- Admin APIを介してユーザーをSysdigに統合し、インポート時に読み取り専用権限を定義します。
- Sysdig MonitorまたはSysdig Secureで、スコープと可視性が非常に制限されたデフォルトのチームを作成します。必要に応じて、より広い権限を持つ追加のチームにユーザーを手動で割り当てます。

APIを介したユーザーとチームの統合

Sysdigサポートエンジニアと協力してSysdig APIを介してユーザーとチームをプロビジョニングする場合は、UI内のユーザーとチームの役割名がAPI ROLE名にどのようにマッピングされるかに注意してください。

ユーザーの役割

通常(管理者以外)=ROLE_USER

管理者= ROLE_CUSTOMER





チームの役割

上級ユーザー= ROLE_TEAM_EDIT

標準ユーザー= ROLE_TEAM_STANDARD

- 表示専用ユーザー= ROLE_TEAM_READ
- チームマネージャー= ROLE_TEAM_MANAGER

ユーザー管理

このページでは、Sysdig MonitorまたはSysdig Secure UI内からユーザー情報を追加、削除、および設定 する方法について説明します。

注意

ユーザーアカウント情報を構成できるのは、管理ユーザーのみです。

警告

Sysdig Monitorに追加されたユーザーは、両方の製品が使用されている場合、Sysdig Monitorと Sysdig Secureの両方のユーザーの完全なリストに表示されます。ただし、ユーザーは、Sysdig Secureチームに追加されるまで、Sysdig Secureへのログインアクセス権を持ちません。





ユーザーを作成する

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。

0	🏟 Settings
	E Logout

- 2. Usersを選択します。
- 3. [Add User]リンクをクリックします。
- 4. ユーザーのメールアドレス、姓名を入力します。

New User		
Email		
Name	First	Last

(i) Admin rights can be configure once the user activates the account

5. [Save]をクリックしてユーザーを招待するか、[Cancel]をクリックしてユーザーを破棄します。

新しいユーザーがユーザー管理テーブルに追加されます。招待が承認されるまで、ステータスは[保留 中]として表示されます。

注意

招待が受け入れられ、ユーザーが初めてインターフェースにログインするまで、管理者権限を割り 当てることはできません。ただし、他のチームに追加したり、チームベースの役割を割り当てるこ とができます。チームの役割の構成の詳細については、チームと役割の管理のドキュメントを参照 してください。





ユーザー情報を編集

既存のユーザーを編集するには:

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Usersを選択します。
- 3. [User Management]テーブルからユーザーを選択します。
- 4. オプション: 名/姓を編集します。
- 5. オプション:管理スイッチを切り替えて、管理者権限を有効/無効にします。
- 6. [Save]をクリックして変更を保存するか、[Cancel]をクリックして未保存の変更を元に戻します。

注意

ユーザーのメールは読み取り専用であり、変更できません。

ユーザーを削除する

既存のユーザーを削除するには:

警告

ユーザーの削除は元に戻せません。ユーザーが任意のチーム用に作成したダッシュボードまたはエ クスプローラグループは完全に削除されます。

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Usersを選択します。
- 3. [User Management]テーブルからユーザーを選択します。
- 4. Delete Userをクリックします。
- 5. [Yes, delete]をクリックして変更を確認します。





チームと役割の管理

チームを使用すると、組織の必要に応じて、グループを編成したり、ワークフローを合理化したり、 データを保護したりするための戦略的な方法が提供されます。 チームの設計と実装を行う管理者は、 組織のインフラストラクチャーと目標に関する深い知識が必要です。

注意

チームの権限を設定できるのは、上級ユーザーのみです。 チームと役割は、Sysdig Monitorと Sysdig Secureで個別に割り当てる必要があります。

基本的な概念を含む詳細については、「<u>ユーザーとチームの管理</u>」を参照してください。

チームを作成する

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Select Teamsを選択します。
- 3. [Add Team]をクリックします。
- 4. チームオプションを設定し、[Save]をクリックします。

注意

各構成オプションの詳細については、表1:チーム設定を参照してください。





表1:チーム設定

設定	必須	説明
Color	Yes	チームに色を割り当てて、リストですばやく識別しやすくし ます。
Name	Yes	[Switch to]ドロップダウンセレクターやその他のメニューに表 示されるチームの名前。
Description	No	チームの長い説明。
Default Team	No	ユーザーがどのチームにも割り当てられていない場合、ユー ザーがオンになっていると、自動的にそのチームの一部にな ります。
Default Entry Point	Yes	デフォルトは「Explore」ページです。必要に応じて別のエン トリを選択します
Scope by	No	チームメンバーが表示できるデータの最高レベルを決定しま す。「ホスト」に設定されている場合、チームメンバーはす べてのホストレベルおよびコンテナレベルの情報を見ること ができます。「コンテナ」に設定されている場合、チームメ ンバーはコンテナレベルの情報のみを表示できます
Scope	Yes	メトリクスのタグ/値式を指定することにより、チームメン バーが表示できるデータをさらに制限します。プルダウンセ レクタのデフォルトは「is」ですが、「is not」、「in」、「 contains」などに変更できます。「Add another」をクリック して複数の式のANDチェーンを作成することで、複雑なポリ シーを作成できます。 スコープ設定を変更すると、すでに構成されているチームの ダッシュボードに表示される内容に劇的な影響を与える可能 性があるため、変更の前後にこれらを注意深く確認すること をお勧めします。



Additional Permissions		Sysdig Capture-このチェックボックスをオンにすると、この チームがSysdig Capturesを取得できるようになります。キャ プチャはこのチームのメンバーにのみ表示されます。 警告:キャプチャには、チームのスコープに関係なく、ホス ト上のすべてのコンテナからの詳細情報が含まれます。 インフラストラクチャイベント-このチェックボックスをオン にすると、このチームはすべてのユーザーとエージェントか らのすべてのインフラストラクチャーイベントとカスタムイ ベントを表示できます。それ以外の場合、このチームには、 このチームに特別に送信されたインフラストラクチャイベン トのみが表示されます。 AWSデータ-このボックスをオンにして、このチームがAWS のメトリクスとタグにアクセスできるようにします。チーム のスコープに関係なく、すべてのAWSデータが利用可能にな ります。
Team Users	No	このチームにすぐに追加する管理者以外のユーザーをクリッ クして選択します。 管理者は自動的にすべてのチームのメン

チームのエントリページまたはダッシュボードを設定する

詳細な監視情報を必要としないユーザーは、Sysdig Monitorをより効率的にオンボードしてナビゲート できるため、一部のSysdig Monitorチームは、通常の[Explore]ページ以外のデフォルトのエントリポイ ントを使用することでメリットを得ます。

バーであるため、デフォルトでは除外されます。

チームの作成で示すように、[Team]ページの[Default Entry Point]設定を使用します。

注:ダッシュボードを選択する場合は、2番目の[Dashboard]ドロップダウンメニューを開くか、ダッ シュボードの名前を入力して選択します。

(ドロップダウンには、チームの誰もがアクセスできる共有ダッシュボードのみが表示されます。)

チームメンバーの追加と設定

ユーザーは複数のチームに割り当てることができます。チームの割り当ては、[User]ページではなく [Team]ページから行い、管理者またはチームマネージャーが行う必要があります。





警告

Sysdig Monitorに追加されたユーザーは、両方の製品が使用されている場合、Sysdig Monitorと Sysdig Secureの両方のユーザーの完全なリストに表示されます。ただし、ユーザーは、Sysdig Secureチームに追加されるまで、Sysdig Secureへのログインアクセス権を持ちません。

チームにユーザーを割り当てる

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[settings]を選択します。
- 2. Teamsを選択します。
- 3. リストから関連するチームを選択するか、検索ボックスで検索してから、関連するチームを選択し ます。
- 4. [Team Users]セクションで、[Assign User]ボタンをクリックします。
- 5. ドロップダウンリストからユーザーを選択するか、ユーザーを検索して選択します。
- 6. [Role]ドロップダウンメニューをクリックして、ユーザーの役割を選択します。

Team Users Assign User Name Role luca@sysdig.com Advanced user X maarten+permissiontest@sysdig.com X Advanced user 0 View only 0 (i) Current Team cannot be deleted Save Team manager 0 Standard user 0

- 7. オプション:追加のユーザーごとにステップ3から5を繰り返します。
- 8. <mark>Save</mark>をクリックします。





ユーザーにチームベースの役割を割り当てる

概要については、<u>チームベースの役割と権限</u>を確認してください。

上級ユーザーの権限は、表示専用ユーザーまたはチームマネージャーにさらに絞り込むことができます。

マネージャーは、チームのメンバーを追加または削除したり、メンバーの権限を編集、読み取り、マ ネージャー間で切り替えたりできます。

管理者にはユニバーサル権限があり、チームマネージャー、上級ユーザー、表示専用ユーザー、また は標準ユーザーとして指定されていないことに注意してください。

マネージャーまたは上級ユーザーの権限は、保留中のユーザーにも割り当てることができます。管理 者は、ユーザーの最初のログインを待ってこれらのロールを設定する必要はありません。

チームのユーザーに役割を割り当てるには:

- 1. Sysdig MonitorまたはSysdig Secureに管理者としてログインし、チームを作成するか、編集する チームを選択します。
- 2. ユーザーを追加するか、チームメンバーのリストからユーザーを選択します。
- 3. ドロップダウンメニューから適切な役割を選択します。

Additional Permissions	Sysdig Captures Infrastructure Events AWS Data	
Default Entry Point	Explore	
Default Team		
Users (show Admins (2))	ADD USER	
	User	Role
	andrew.paul+kube@sysdig.com	Advanced user
		Advanced user 💿
Delete Team	DELETE TEAM	View only 📀
		Team manager 💿
		Standard user OVE EDITS





役割の特権の注意:

管理者:すべての権限を持つすべてのチームのメンバー。すべてのユーザーとチームを作成/削除/構成 できます。

上級ユーザー:Sysdig Monitorの場合:チームが使用できるアプリケーションのコンポーネントへの読 み取り/書き込みアクセス。ダッシュボード、アラート、またはその他のコンテンツを作成/編集/削除 できます。

Sysdig Secureの場合:チームが利用できるアプリケーションのコンポーネントへの読み取り/書き込み アクセス。ランタイムポリシー、画像スキャンポリシー、またはその他のコンテンツを作成、削除、 または更新できます。

チームマネージャー:高度なユーザー権限+チームメンバーの追加/削除、またはチームメンバーの権限の変更。

表示のみ:

Sysdig Monitorの場合:チームスコープ内の環境への読み取りアクセス権。ただし、ダッシュボード、 アラート、またはその他のコンテンツを作成、編集、または削除することはできません。

Sysdig Secureの場合:チームスコープのすべてのSecure機能への読み取りアクセス権。ただし、ラン タイムポリシー、イメージスキャンポリシー、またはその他のコンテンツを変更することはできません。

標準ユーザー:

Sysdig Monitorの場合: Exploreページにアクセスできない上級ユーザー(たとえば、監視情報に興味 がない開発者向け)。

Sysdig Secureの場合:コンテナイメージをスキャンキューに送信し、イメージスキャン結果を表示 し、チームスコープ内のランタイムセキュリティイベントを表示できます。標準ユーザーは、ベンチ マーク、アクティビティ監査、ポリシー定義、または他のセキュア機能内の特定の書き込み機能にア クセスできません。

4. 編集をsaveします。





チーム設定の編集

既存のチームを構成するには:

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Teams を選択します。
- 3. リストから関連するチームを選択するか、検索ボックスで検索してから、関連するチームを選択し ます。
- 必要に応じて編集し、[save]をクリックします。構成オプションの詳細については、表1:チーム 設定を参照してください。

チームを削除する

チームが削除されると、一部のユーザーはチームのメンバーではなくなったため、「孤児」になる場 合があります。これらのユーザーはデフォルトチームに移動されます。

デフォルトのチームは削除できません。古いデフォルトチームを削除する前に、新しいデフォルト チームを選択する必要があります。

作成したチームを削除するには:

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Teamsを選択します。
- リストから関連するチームを選択するか、検索ボックスで検索してから、関連するチームを選択し ます。
- 4. [Delete team]をクリックし、[Yes, delete]をクリックして変更を確認します。





通知管理

<u>アラート</u>は、イベントしきい値を超えた場合はSysdig Monitorで使用され、ポリシー違反が発生した場合はSysdig Secureで使用されます。 アラートは、サポートされているさまざまな通知チャネルを介し て送信できます。

通知管理では、さまざまな通知チャネルタイプを追加、編集、または削除する方法と、スケジュール されたダウンタイム中など、通知が不要な場合に通知を無効または削除する方法について説明します

通知チャネルを追加する

新しい通知チャネルを追加するには:

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Notification Channelsを選択します。

通知のメインページが表示されます。

Settings		
User Profile	Notifications	
Lusers	Downtime Temporarily disable alerts events and me	ute all notifications
Teams	Notification Channels	
Notification Channels	Notification channels	
AWS	Q Search channel	Add Notification Channel
Sysdig Storage	Enabled Channel	
Subscription	To: claudio+admin@sysdig.com	1
Agent Installation	Email Channel (test@sysdig.com)	I
OT Authentication		





3. [Add Notification Channel +]をクリックし、目的の通知チャネルを選択します。



- 4. チャネル固有の手順に従って、設定プロセスを完了します。
 - Amazon SNS通知
 - メール通知
 - PagerDuty通知
 - Slack通知
 - VictorOps通知
 - OpsGenie通知
 - Webhookチャネルを構成する

注意

通知チャネルを設定すると、アラートを追加するときに割り当て可能なオプションとして表示され ます。

通知チャネルを編集する

通知チャネルを編集するには:





1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[settings]を選択します。

?	🏚 Settings
	3 Logout

- 2. Notification Channelsを選択します。
- 3. ターゲットチャネルを見つけて、[Edit]ボタンをクリックします。
- 4. 編集を行い、[Done Editing]をクリックして変更を保存します。

通知チャネルをテストする

通知チャネルをテストするには:

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



2. Notification Channelsを選択します。

New Constant Observate

3. 作成した通知チャネルの横にある3つのドットを選択し、[Test Channel]をクリックします。

Search char	nel	Add Notification Channel
Enabled	Channel	
٠	Sdc-qa-test-notify-email To: franco.nonne+test1@sysdig.com, franco.nor	nne+test2@sysdig.com, franco
	CLAUDIO	Test Channel




注意

通知が10分以内に受信されない場合、通知チャネルは機能していないため、設定を確認する必要が あります。

Amazon SNS通知

Sysdig Monitorは、AWS Simple Notification Service (SNS)と簡単に統合できます。

AWS側:

- 1. Sysdig Monitor アラートを選択したSNSトピックに自動的にプッシュするには:
- 2. AWSコンソールから、SNS管理コンソールを開きます
- 3. 新しいトピックを作成する(必要な場合)
- 4. リストからトピックを選択します
- 5. 上部の[すべてのトピックアクション]メニューから、[トピックポリシーの表示/編集]を開きます
- 6. [**Publishers**]セクションで、[これらのAWSユーザーのみ]を選択し、Sysdig MonitorアカウントID を入力します: ex) 273107874544
- 7. トピックの詳細ページから、トピックARNをコピーしてここに貼り付けます

AWSSNSの詳細については、AWSのドキュメントを参照してください。

SNS通知の場合、「ヘルプ」ボタンをクリックして、SNSトピックの設定に関するヒントを表示できます。

Sysdig MonitorアカウントID: ex) 273107874544への公開権限を許可する必要があります。これ は、以下の画像に示すように、AWSコンソールでSNSトピックに新しいポリシーを作成すること で実行できます。





「その他のトピックアクション」から、以下に示す「トピックポリシーの編集」を選択します。
 Topic details: sysdig-sns-notification

Publish to topic	Other topic actions -		
Topic ARN	Edit topic display name	36418888567:sysdig-sns-notification	
Topic owne	Edit topic policy		
Regior	Edit topic delivery policy		
Display name	Delivery status		
	Delete topic		
Subscriptions			
Create subscription	Request confirmation	Confirm subscription	

 [トピックポリシーの編集]ダイアログの[基本ビュー]タブで、発行元のリストから[これらのAWS ユーザーのみ]を選択し、Sysdig IDを入力します。

Au Au	vanced view			
Allow these users	to publish message	es to this topic		
Only me (topic or	wner)			
Everyone	_			
Only these AWS	users 273	107874544		
Allow those users	to subscribe to this	tonic		
Allow these users	to subscribe to triis	topic		
Only me (topic of Everyone)	wner)			
 Only these AWS 	users	mma-senarated list of AWS	account IDs	
		and separated list of Arro	account hos.	
Only users with e	endpoints that match	examples: "*@exam	ple.com" or "http://example.	com/*"
		HTTP	HTTPS	🖌 Email
Using the	se delivery protocols		CMC	Amazon SQS
Using the	se delivery protocols	Email-JSON	9 3113	6.6.0 C

SysdigモニターUI:





1. 通知チャネルの設定の手順1~3を完了してSysdig UIにログインし、[Amazon SNS Topic]を選択し ます。

New Amazon SNS Topic Channel				
Channel Type	Amazon SNS Topic			
Topics	E.g. arn:aws:sns:us-east-1:273107874544:my-alerts			
Channel Name	Channel name			
Enabled				
Notify when Resolved	Send a new notification when the alert condition is no longer triggered			
Notify when Acknowledged	Send a new notification when the alert is manually acknowledged by a user			
Test notification	Send a test notification when saving changes			
	Cancel	ve		

- AWS側で作成されたトピックを入力し、必要に応じてチャネル名、有効化、および通知トグルを 入力します。
- 3. <mark>Save</mark>をクリックします。

メール通知

メールでアラート通知を送信するには、まずメール通知チャネルを設定する必要があります。

そのためには、通知チャネルの設定の手順1~3を完了してから、次の手順を実行します。

1. Email を選択します。





2. 電子メール通知に関連する詳細を入力します。

User Profile	New Notification Channel		
L Users	Channel Type	🔛 Email	
Teams	Recipients	List of comma separated e-mails	
Notification Channels	Channel Name	Channel name	
AWS	Enabled	•	
Sysdig Storage	Notify when Resolved	Send a new notification when the alert condition is no longer triggered	
Subscription	Notify when Acknowledged	Send a new notification when the alert is manually acknowledged by a user	
Agent Installation	Test notification	Send a test notification when saving changes	
Authentication			

3. Saveをクリックします。

Sottingo

テスト通知を有効にすると、テストメールが送信されます。

電子メール通知を使用するようにアラートを設定できるようになりました。



PagerDuty通知

PagerDutyを介してアラート通知を送信するには、最初にPagerDuty通知チャネルを設定する必要があります。

前提条件





- PagerDuty.comでアカウントを設定します。
- PagerDutyの認証情報(アカウント、パスワード、サービス)を用意します。

注意 ManagerのPagerDuty基本ユーザーロールを使用すると、Sysdig/PagerDuty統合プロセス中にサー ビス情報を自動フェッチできます。 PagerDutyチームの権限がマネージャーであるが、基本ユーザーの権限がレスポンダー以下の場 合、Sysdig UIIこ必要なデータを手動で入力できます。					
Invite your team			×		
Name	Email	Base Role			
First Last	user@domain.com	Manager •	Add		
	Add user(s) above to get sta	Global Admin Manager Responder Team Responder Observer			
Send Invitations Cancel Send Invitations Cancel Stakeholder Restricted Access Learn more about user roles					

PagerDuty UIの基本ユーザーロール

PagerDutyの設定

- 1. Sysdig UIからプロセスを起動するには、通知チャネルのセットアップのステップ1から3を完了 し、PagerDutyを選択します。
- 2. プロンプトが表示されたら[Auto-fetch]を選択します(PagerDutyでマネージャー以上の基本ユー ザーロールが必要です)。





(手動を選択した場合は、手順5に進みます。) PagerDutyの統合画面が表示されます。

Authorize Sysdig to integrate with your account?

Sysdig will be able to **Trigger**, Acknowledge, and Resolve incidents in PagerDuty.

Email					
Password					
Forgot your password?					
Authorize Integration No, Thanks					
If your account uses a Single S Enter the subdomain of your accoun	ign-on Provider t				
subdomain	.pagerduty.com				
Sign In Using Your Identity Provider					
Once authorized, you'll be able to sel	lect the escalation policy to use for				

Once authorized, you'll be able to select the escalation policy to use for Sysdig incidents. You can disable any integration at any time from the Services tab in your PagerDuty account.

3. PagerDutyアカウントに関連付けられているメールアドレスとパスワードを入力し、[Authorize Integration]をクリックします。

または

シングルサインオンとサインインに適切なPagerDutyサブドメインを入力します。

4. PagerDutyサービス選択画面が表示されます。

オプション1:以前に統合したことがない場合は、PagerDuty Servicename名とEscalation policyを選択するように求められます。



- 7	

pagerduty	
	Configure the Sysdig integration.
	To create incidents from Sysdig, you'll need an integration for Sysdig on a PagerDuty service. You can use an integration on an existing service, or create a new service with a Sysdig integration.
	Service name
	Sysdig
	Escalation policy
	Default \$
	Finish Integration or cancel
	You can update services and integrations in your PagerDuty account. Services can have multiple integrations that monitor the various layers of your systems.

オプション2:少なくとも1つのサービスがすでに統合されている場合は、そのサービスを選択するか、別のサービスを作成できます。

Configure the Sysdig integration.		
To create incidents from Sysdig, you'll need an integration for Sysdig on a PagerDuty service. You can use an integration on an existing service, or create a new service with a Sysdig integration.		
 One service has an integration with Sysdig: Use an integration on an existing service 		
Sysdig Service (Sysdig)		
 Create a new service with an integration for Sysdig Finish Integration or cancel 		
You can update services and integrations in your PagerDuty account. Services can have multiple integrations that monitor the various layers of your systems.		

5. [Finish Integration]をクリックします。





統合が承認されると、新しいPagerDuty通知チャネルのSysdigページが表示され、情報が自動入力され

ます。						
	Set	tings				
0		User Profile	New PagerDuty Channel			0
EXPLORE	:	Users	Channel Type	PagerDuty		
	*	Teams	Account	Your Account Name		
		Notification Channels	Service Key	Your Service Key		
ALERTS		AWS	Service Name	Your Service Name		
EVENTS	0	Sysdig Storage	Channel Name	Your Channel Name		
63		Subscription	Enabled	•		
CAPTURES	Ţ	Agent Installation	Notify when Resolved	Send a new notification when the alert condition is no longer triggered		
	07	Authentication	Notify when Acknowledged	Send a new notification when the alert is manually acknowledged by a user		
			Test notification	Send a test notification when saving changes		
D R						
۲						
0						
				[Cancel	ave

6. 自動入力された情報を確認し、[Save]をクリックします。または

手順2で[手動入力]を選択した場合は、情報を入力して[Save]をクリックします。

PagerDuty通知を使用するアラートを追加できるようになりました。

既知の問題

注意

通知を「Acknowledged」から「Unacknowledged」に変更すると、PagerDutyで正しく更新され ないという既知の問題があります。





発生すること:

- イベントによって通知がトリガーされ、通知がPagerDutyに送信されます。
- イベントを開き、Sysdigの[Acknowledge]ボタンをクリックします。
- 通知がPagerDutyに送信され、ステータスが「確認済み」に変更されます。
- イベントを開き、Sysdigの[UnAcknowledge]ボタンをクリックします。

PagerDutyではステータスは変更されません。PagerDutyで「Triggered」に変更されるのではな く、「Acknowledged」のままです。

Slack通知

Slack経由でアラート通知を送信するには、まずSlack通知チャネルを設定する必要があります。

そうするために:

前提条件:

Slack.comでSlackアカウントを構成し、通知に使用する通知チャネルを確認します。

Sysdig UIからプロセスを起動するには、通知チャネルのセットアップのステップ1から3を完了し、Slackを選択します。

Slackアカウントにログインするように求められます。

2. 通知に使用するSlackチャネルをドロップダウンリストから選択し、[Authorize]をクリックします。





3. 必要に応じて構成を完了し、「Done」をクリックします。

New Slack Channel				
All done!				
You can now custor	nize the channel and close.			
Channel	@slackbot			
Name	Enter an optional name			
Notify when OK	Send a new notification when the alert condition is no longer triggered			
Notify when Resolved	Send a new notification when the alert is manually resolved by a user			
Test notification	Send a test notification. If you do not receive a test notification in 10 minutes, your notification channel is not working.			
	DONE			

4. [Test]をクリックして、新しい機能を確認します。

Slack通知を使用するようにアラートを構成できるようになりました。

VictorOps通知

VictorOpsと統合するには

- 1. VictorOpsにログインします。
- 2. VictorOpsインターフェースの[Settings]> [Alert Behavior]> [Integrations]に移動します。



3. 統合機能のリストからRESTを選択します。



4. 通知チャネルの設定の手順1~3を実行してSysdig UIにログインし、VictorOpsを選択します。

Set	Settings					
٢	User Profile	New Notification Channel				
•	Users	Channel Type	VictorOps			
*	Teams	API Key	АРІ Кеу			
	Notification Channels	Routing Key	Routing Key			
•	AWS	Channel Name	Channel name			
0	Sysdig Storage	Enabled	•			
	Subscription	Notify when Resolved	Send a new notification when the alert condition is no longer triggered			
Ţ	Agent Installation	Notify when Acknowledged	C Send a new notification when the alert is manually acknowledged by a user			
07	Authentication	Test notification	Send a test notification when saving changes			
			Cancel Save			

- 5. 次のように、Sysdig Notification ChannelフィールドにVictorOpsパラメータを入力します。
 - a. **API Key**: REST URLの「/alert/」と「/\$routing_key」の間のすべて
 - b. **Routing Key**: アラートを適切なチームにルーティングするVictoOpsの方法。必要に応じて、ルーティングキーのドキュメントで詳細を確認してください。
 - c. Channel Name:「VictorOps」などのわかりやすい名前を選択します。





d. チャネルと目的の通知タイプを有効にします。6. saveをクリックします。

OpsGenie通知

1. OpsGenie統合ページを直接開いて、OpsGenie側の統合を構成します。

OpsGenieは、Sysdig製品(以前はSysdig Cloudと呼ばれていました)との統合方法に関するド キュメントを<u>ここ</u>に保持しています。

2. 通知チャネルの設定の手順1~3を実行してSysdig UIにログインし、OpsGenieを選択します。

New OpsGenie Channel		?
Channel Type	SpsGenie	
API Key	API Key	
Channel Name	Channel name	
Enabled		
Notify when Resolved	Send a new notification when the alert condition is no longer triggered	
Notify when Acknowledged	Send a new notification when the alert is manually acknowledged by a user	
Test notification	Send a test notification when saving changes	
	Cancel	е

- 3. OpsGenie統合APIキーをコピーして貼り付け、必要に応じてチャネル名、有効化、通知の切り 替えを追加します。
- 4. Saveをクリックします。





Webhookチャネルを設定する

Sysdig MonitorとSysdig Secureは、Sysdigがネイティブに統合されていない宛先(Webサイト、カスタ ムアプリケーションなど)にアラート通知を送信することをサポートしています。これを行うには、 カスタムWebhookチャネルを使用します。

前提条件

- HTTPS経由のWebhookは、署名済み/有効な証明書が使用されている場合にのみ機能します。
- 目的のリンク先URLを手元に用意します。

UIで機能を有効にする

1. 通知チャネルの設定の手順1~3を完了し、Webhookを選択します。

New WebHook Channel					
Channel Type	🔏 WebHook				
URL	E.g. https://some.callback.url?apiKey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx				
Channel Name	Channel name				
Enabled					
Notify when Resolved	Send a new notification when the alert condition is no longer triggered				
Notify when Acknowledged	Send a new notification when the alert is manually acknowledged by a user				
Test notification	Send a test notification when saving changes				
	Cancel	ive			

2. Webhookチャネル設定成オプションを入力します。

URL:通知の送信先URLチャネル名:「Ansible」、「Webhook.Site」などのわかりやすい名前を追加します。





有効化:通知オプションのオン/オフを切り替え:アラートが解決または確認されたときの通知 を切り替えます。

テスト通知:設定したURLが機能していることを通知するように切り替えます。

3. Saveをクリックします。

チャネルが作成されると、作成したすべてのアラートで使用できます。

次に、アラートが発生すると、通知がJSON形式のPOSTとしてWebhookエンドポイントに送信されま す。(下記のアラート出力を参照してください。)

テスト目的で、サードパーティのサイトを使用して一時的なエンドポイントを作成し、Sysdigアラート が特定の通知で送信する内容を正確に確認できます。

オプション:カスタムヘッダーまたはデータを設定する

デフォルトでは、アラート通知は標準形式に従います(以下のPOSTデータの説明を参照)。

ただし、一部の統合では追加のヘッダーまたはデータ、あるいはその両方が必要であり、カスタム ヘッダーまたはカスタムデータエントリを使用してアラート形式に追加できます。

たとえば、Ansibleはトークンベースの認証を使用します。これには、署名なしトークンのエントリが 必要です。このエントリは、Sysdigに組み込まれているデフォルトのアラートテンプレートには含まれ ていませんが、カスタムヘッダーを使用して追加できます。

これは、以下で説明するように、コマンドラインから実行する必要があります。

注意

- additionalHeadersは通常、認証に使用されます
- customDataは、アラートに値を追加するために使用されます





ユースケースの例

この例では、2つのカスタムヘッダーを追加し、追加のカスタムデータとそのデータの形式を定義します。

1. curlコマンドを使用して、構成されているすべての通知チャネルを取得します。

```
curl -X GET https://app.sysdigcloud.com/api/notificationChannels -H 'Authorization:
Bearer API-KEY'
```

2. カスタムヘッダーを追加し、リクエストを実行します。

```
curl -X PUT https://app.sysdigcloud.com/api/notificationChannels/1 -H 'Authorization:
Bearer API-KEY' -H 'Content-Type: application/json' -d '{
  "notificationChannel": {
    "id": 1,
    "version": 1,
    "type": "WEBHOOK",
    "enabled": true,
    "name": "Test-Sysdig",
    "options": {
      "notifyOnOk": true,
      "url": "https://hookb.in/v95r78No",
      "notifyOnResolve": true,
      "customData": {
        "String-key": "String-value",
        "Double-key": 2.3,
        "Int-key": 23,
        "Null-key": null,
        "Boolean-key": true
      },
      "additionalHeaders": {
        "Header-1": "Header-Value-1",
        "Header-2": "Header-Value-2"
      }
    }
  }
} '
```





標準アラート出力

通知にカスタムWebhookを使用するアラートは、次のデータを含むJSON形式を送信します。

POSTデータの説明:

"timestamp": Unix timestamp of when notification fired
"timespan": alert duration in seconds
"alert": info on the alert that generated the event triggering the notification
"severity": 0 - 7 int value
"editUrl": URL to edit the alert
"scope": scope as defined in the alert
"name": alert name
"description": alert description
"id": alert id
"event": info on the event that triggered the notification
"id": event id
"url": URL to view the event
"state": ACTIVE (alert condition is met) or OK (alert condition no longer met)
"resolved": false (alert has not been manually resolved) or true (it has)
"entities": array of nodes within the alert scope that triggered the notification
"entity": metadata to identify the node
"metricValues": array of metrics that triggered the notification
"metric": metric name
"aggregation": time aggregation method used to calculate the metric
"groupAggregation": group aggregation method used to calculate the metric
"value": metric value
"additionalInfo": array of additional metadata about the entity
"metric": metadata key
"value": metadata value
"condition": alert condition

POSTデータの例:

```
"timestamp": 1471457820000000,
"timespan": 6000000,
"alert": {
 "severity": 4,
 "editUrl": "http://app.sysdigcloud.com/#/alerting/alerts/1/edit",
 "scope": "host.mac = \"00:0c:29:04:07:c1\"",
 "name": "alertName",
  "description": "alertDescription",
  "id": 1
},
"event": {
 "id": 1,
 "url": "http://app.sysdigcloud.com/#/alerting/notifications/1:604800/1/details"
},
"state": "ACTIVE",
"resolved": false,
```





```
"entities": [{
    "entity": "host.mac = '00:0c:29:04:07:c1'",
    "metricValues": [{
        "metric": "cpu.used.percent",
        "aggregation": "timeAvg",
        "groupAggregation": "none",
        "value": 100.0
    }],
    "additionalInfo": [{
        "metric": "host.hostName",
        "value": "sergio-virtual-machine"
    }]
}],
    "condition": "timeAvg(cpu.used.percent) > 10"
}
```

失敗の例

```
$ curl -X GET https://app.sysdigcloud.com/api/notificationChannels -H 'authorization:
Bearer dcla42cc-2a5a-4661-b4d9-4ba835fxxxxx''
{"timestamp":1543419336542,"status":401,"error":"Unauthorized","message":"Bad
credentials","path":"/api/notificationChannels"}
```

成功例

```
$ curl -X GET https://app.sysdigcloud.com/api/notificationChannels -H 'Authorization:
Bearer dcla42cc-2a5a-4661-b4d9-4ba835fxxxxx'
{"notificationChannels":[{"id":18968,"version":2,"createdOn":1543418691000,"modifiedOn":154
3419020000,"type":"WEBHOOK","enabled":true,"sendTestNotification":false,"name":"robin-webho
ok-test","options":{"notifyOnOk":true,"url":"https://postb.in/6dtwzz71","notifyOnResolve":t
rue}]]}
$
```

Webhook機能は、次のチャネルを統合するために使用されます。

ServiceNowを設定する





ServiceNowを設定する

Sysdigは、カスタムWebhookを使用してServiceNowと統合できます。

ServiceNowSetup

前提条件

- ServiceNowアカウントを設定して機能させます。
- 必要に応じて、ServiceNow開発者用ドキュメントを参照してください。

ServiceNow GUIでScripted Rest APIの詳細を作成する

1. ServiceNow (開発者エントリ) にログインし、スクリプトREST APIを作成します。



2. [New]をクリックして、次の情報を含むフォームを送信します。

名前:SysdigAlert API ID:sysdigalert

3. Scripted REST APIsに戻り、作成したリソースを開きます。

関連リスト領域までスクロールし、[Resources]を選択して、[New]をクリックします。これにより、新しいスクリプトREST APIリソースが作成されます。





4. [Name]フィールドに入力します。例、Demo.

Resourc	es (1)	Request Headers	Query Parameters				
	Resourc	ces New Go to	HTTP method V Sea	rch		\$ ◄ ◄	1 to 1 of 1 🕨 🍉 🖻
P	Image: Provide a state of the state of t						
<u>کې</u>	Q	≡ Name		▲ ■ Relative path	Resource path	API version	Active
	Q (j)	E Name	E HTTP method	Relative path	Resource path	■ API version	E Active

5. [Security]までスクロールして、認証が必要なチェックボックスをオフにします。

Security	Content Negotiation	Documentation						
Resource	Resources can specify security settings that override the parent settings.							
By defau access th	By default resources 'Require authentication' but do not 'Require ACL authorization'. To make a resource public, meaning no authentication is required to access the resource, uncheck 'Requires authentication'.							
To requir from the	To require authorization, select the 'Requires ACL authorization' check box and select an ACL record(s). Leave the 'ACL' field blank to enforce the 'Default ACLs' from the parent API. Access is granted if at least one matching ACL record is found.							
More info	More info							
	Pequires .							
authe	Requires authentication							

6. HTTP method をGETからPOSTに変更します。

リソースが作成されます。

新しいスクリプトAPIにコードを追加する

次に、リソースに実行するコードを指定します。

スクリプトREST APIリソースで使用するデフォルトのオブジェクトは、responseとrequestです。

リクエストとレスポンスの詳細については、<u>Scripted REST Request API</u>および <u>Scripted REST Response API</u>を参照してください

作成されたリソースには、すでにいくつかのサンプルコードが含まれています。

```
(function process(/*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {
    // implement resource here
})(request, response);
```





1. このデフォルトコードを次のように変更します。

(function process(/*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {

gs.info(request.body.dataString);

})(request, response);

 この新しく作成されたリソースへの次のリソースパスが表示されるようになりました: /api/snc/sysdigalert

このリソースのURLは、https://yourInstance.service-now.com/ <resource_Path>または https://yourInstance.service-now.com/api/snc/sysdigalertになります。

Resource path

/api/snc/sysdigalert

3. このリソースで[Submit/Update]をクリックします。

Sysdig Webhookセットアップ

ServiceNowのカスタムAPIエンドポイントが作成されたので、カスタムWebhookを使用して ServiceNow統合をトリガーするようにSysdigアラートを設定できます。

API URL:インスタンス名URL

Name: ServiceNow(またはこのSysdigアラートWebhookに付ける任意の名前)

Notify when OK:オプション

Notify when Resolved:オプション





Test Notification:このトグルを使用するか、次のセクションで説明するようにテストアラートを設定します。

Add custom data ar	nd headers using our API. Please refer to our docs.		
Push Sysdig Monito below, including the	ir alerts via webhook: when a notification fires to this channel, a POST will be sent to the URL endpoint given data specified here.		
WebHook Url	https:/YOURINSTANCENAME/api/ <u>snc/sysdigalert</u>		
Name	Enter a name		
Notify when Resolved	Field must be present.		
Notify when Acknowledged	Send a new notification when the alert is manually acknowledged by a user		
Test notification Send a test notification. If you do not receive a test notification in 10 minutes, your notif channel is not working.			

統合テスト

このServiceNow統合がセットアップされて正しく機能しているかどうかをテストするために、トリ ガーするテストアラートをセットアップできます。たとえば、CPU使用率のアラートを作成します:

×

Define		1		
(a) Metric (a)				
Average 👻 of	cpu.used.percent		•	→←
b Scope 💿				
container.image	▼ is		t and	\otimes
container.name	▼ is	▼ sysdig-agen	t	0
	-			
c Trigger				
If metric > + 99	% for the las	t 10 minute(s)	▼ on average	
Simple Alert 👻				
Trigger a single alert	- when the trigger cor	ndition is met across you	ir scope	





ServiceNowで、System Log > Allに移動して、サンプルのトリガーされたWebhookを表示します。

serv							
		8	Created 2016-12-20 08:55:34				
	*	\bigcirc	Level	Information			
Sybase Service Cata	alog		Source	*** Script			
Catalogs			Created	2016-12-20 08:55:34			
▼ Catalog	Definitions		Message	{"timestamp":1482252360000000,"timespan":600000000,"alert":{"severity":4,"editUrl":"https://app.sysdigcloud.com/#/alerting/alerts/904656/edit";"scope":"container.image =			
My Cata	logs			\"luca3m/node-example\" and container.name = \"distracted_ptolemy\" and container.id = \"e286470898dd\"","name"."Down Container.","description".null,"id".904656),"event":			
Maintai	n Catalogs			["entry": container.image = 'luca3m/node-example' and container.name = 'distracted_ptolemy' and container.id = 'e256470598d4";"metricValues":			
^a erformance	e Analytics			[{"metric":"uptime";"aggregation":"timeAvg";"groupAggregation":"none";"value":0];"additionalInfo":null]];"condition":"timeAvg(uptime) = 0";"source":"Sysdig Cloud"}			
V Data Co	lloctor						

通知チャネルを無効化または削除する

通知チャネルを一時的に無効にする

通知チャネルを一時的に無効にするには:

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



- 2. Notification Channels を選択します。
- 3. [Enabled]スライダーをオフに切り替えます。

ダウンタイム中の通知のミュート

管理者は、スケジュールされたシステムのダウンタイム中など、必要に応じてすべてのアラートイベ ントと通知をオフにすることを選択できます。

通知をミュートすると、すべてのチャネルにグローバルに影響します。ミューティングがオンになっている場合、設定されたチャネルを通じて通知は送信されません。通知が一時的に無効になっている





ことを特定のチャネルに通知するかどうかを選択できます。通知のミュートと再有効化は手動のプロ セスです。

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



- 2. Notification Channelsを選択します。
- 3. [Downtime]トグルを選択します。

オプション:プロンプトが表示されたら「<u>ves</u>」ボックスをオンにしてチャネルに通知し、目的のチャネルを選択します。

現時点では、ダウンタイムの開始/停止時に通知できるのは、EメールおよびSlackチャネルのみです。

Activate D	Downtime				
Temporarily dis	able alert events a	nd mute all noti	ifications?		
Notify via e	e-mail or Slack				
				No	Yes

通知チャネルを削除する

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。
- 2. Notification Channelsを選択します。
- 3. 作成したチャネルの横にある3つのドットを選択し、[Delete Channel]をクリックします。





Notification	Channels		
Q Search char	inel	 Add Notification Channel 	
Enabled	Channel		
sdc-qa-test-notify To: franco.nonne+te		fy-email test1@sysdig.com, franco.nonne+test2@sysdig.com, franco	
	CLAUDIO To: claudio@sysdig.c	om Test Channel Delete Channel	
	ar ann an a		

アラートの起動遅延を設定する(オンプレミスのみ)

Sysdigアラートジョブは、起動直後に開始されます。ただし、Sysdigが予期せずに停止した場合、また は適切なシャットダウン/起動手順が実装されていない場合、データが欠落してアラート通知がトリ ガーされることがあります。

draios.alerts.startupDelayパラメーターを設定することにより、オンプレミス環境でアラートジョブの 起動遅延を設定できます。パラメータには期間値が必要です。以下の例は、10分の継続時間を示して います。

draios.alerts.startupDelay = 10m

このパラメーターは、Replicated環境またはKubernetes環境のいずれかに構成できます。

- Replicated環境の場合、SysdigアプリケーションのJVMオプションリストにパラメーターを追加 します。詳細については、Sysdig Install with Replicatedのドキュメントを参照してください。
- Kubernetes環境の場合、configmapのsysdigcloud.jvm.worker.optionsパラメーターにパラメー ターを追加します。configmapの編集の詳細については、Sysdig Install with Kubernetes 1.9+ を参照してください。





AWS:AWSアカウントとCloudWatchメトリクス を統合する(オプション)

SysdigエージェントがAWS環境にインストールされている場合、Sysdigプラットフォームは、一般的な メタデータとさまざまなタイプのCloudWatchメトリクスの両方を収集できます。

AWSアカウントをSysdigに統合するには3つの方法があります。

- AWSアクセスキーとシークレットキーを手動で入力し、必要に応じて手動で管理/ローテーションする
- SysdigがAWS ECSロールとそのアクセス許可を自動検出できるようにするパラメーターを渡し、「implicit key」を渡す(オンプレミスのみ)。

implicitオプションでは、AWSがバックグラウンドでこれらのアクセス許可を処理するため、手動のキーローテーションは必要ありません。

 AWS Role delegationの使用。役割の委任は、アクセスキーを使用する既存の統合方法の代替 手段です。Amazonは開発者のアクセスキーをサードパーティと共有することを推奨していない ため、この方法は安全であると考えられています。

SysdigモニターUIには、以下で説明するように、CloudWatchメトリクスをSysdigモニターに簡単に統 合するのに役立つリンクが含まれています。

Sysdig UIの2つのエントリポイント

Sysdigインターフェースは、2つの異なる場所(ウェルカムウィザードまたは管理者の[Settings]メ ニュー)からこの統合を実行するように求めます。

ウェルカムウィザードからのアクセス

最初にSysdigモニターUIにログインするとき、ウェルカムウィザードにはAWSアカウントを統合して CloudWatchメトリクススを収集するオプションが含まれています。





注意

implicit keyを使用する場合は、ウィザードのこのページをスキップする必要があります。詳細については、Implicit Key Optionを参照してください。

an illen Efennen	Hiter Binn Q Jam & Hit Xing California	+ III Other Beatman
0	being income and income and income	
Integrat	e with AWS	Veenu III
tiyadig Mantor offen RDS within Dynitig M	deep magratum with AHD, allowing you to monitor service mitor and alloc pull your tags and other AHD metadata.	seath as TCC, 118 and
To enable the integ account, See here	ndon you just real to provide Spady Monter with read or to specific remainters in how to present the receivery K	ly access to your ays
Access Key ID:	E & AKARDIFICORRECKAMPLE	
Secret Access Kay	Please, event a cold key of	
	Plasmi, Indust a vehiclikely	
CloudWatch Inte	pration Status	
Coudmit integri	ne	
Note: Drok you provi feature is anabled, fo small additional (har	In the recenterly laye, CloudWatch Integration will be intelli- why thready will poin the CloudWatch Aff yoary 1 minutes, a ge from ART does Analysi CloudReady Truing)	et by default, when this, disch will generate a
Theire not using a ch	and provider? Don't worry, Syndry Microsof will still work west	for your infrastructure.
autr.	-	-

設定メニューからのアクセス

エージェントがインストールされたら、管理者としてSysdig MonitorまたはSysdig Secureにログインして、統合手順を実行するか、既存のAWS設定を確認/変更します。

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。







2. AWSを選択します。

٢	User Profile	AWS accounts		
	Subscription	Credentials		Status
	Notifications			✓ OK
٠	AWS			
Ţ	Agent Installation			
0	Sysdig Storage			REFETCH NOW ADD
•	Users			
*	Teams	Add a new AWS account		
		See instructions here to grant the p	roper access.	
		Access Key ID:	E.g	
			Please, insert a valid key id	
		Secret Access Key:		
			Please, insert a valid key	
				CANCEL SAVE
		Amazon CloudWatch Integration		
		Sysdig Monitor can integrate Cloud alongside your existing Sysdig Mor	Watch metrics into your dashboards, allowing you to explore data fro litor data.	m AWS services like RDS, EC2 and ELB
		CloudWatch can be selected in the	data source menu in the Explore page.	
		Warning: When this feature is enab AWS (see Amazon CloudWatch Price	led, Sysdig Monitor will poll the CloudWatch API every 5 minutes, whi cing).	ch will generate a small additional charge from
		CloudWatch Integration Stat	us	
		Disabled Constant Enabled		

アクセスキーとシークレットキーのフィールドが表示された手動キー統合を示すAWSページ。

注: AWS統合がまだない場合は、[ADD YOUR AWS ACCOUNT]をクリックして、アクセスキーとシーク レットキーを入力してください"





AWSアカウントを手動で統合する

AWS EC2アカウントの詳細を用意します。統合はAWS側で始まり、SysdigモニターUIで完了します。

AWSでは

Sysdigアクセス用のIAMポリシーを作成する

注意

代わりに既存のIAMReadOnlyポリシーを使用することもできますが、Sysdig固有のポリシーを作成 すると、より詳細なアクセス制御が提供され、CloudTrailでアクティビティを簡単に区別できるた め、ベストプラクティスと見なされます。

- AWSで、IAMを選択し、Sysdigに使用するポリシーを作成します。 (サンプルポリシー名: SysdigMonitorPolicy。)
- JSONエディタービューを使用して、Sysdig固有のポリシーコードをコピーして新しいポリシーに 貼り付け、保存します。
- 3. ビジュアルエディタでポリシーを確認できます。





完成したポリシーをビジュアルエディターで確認すると、次のように表示されます。

- Policies > SysdigMonitorPolicy
- Summary

	Policy ARN arn:aws:iam:: Description Policy to allow	:policy/SysdigMonitorPolicy 《신 AWS integration and Cloudwatch polling	
ermissions Attache	ed entities (0) Policy versions	Access Advisor	
Policy summary {]	JSON Edit policy		
Q Filter			
Service 👻	Access level	Resource	Request condit
Allow (10 of 139 servic	es) Show remaining 129		
Auto Scaling	Full: List, Read	All resources	None
CloudWatch	Full: List, Read	All resources	None
DynamoDB	Limited: List	All resources	None
EC2	Full: List Limited: Read	All resources	None
EC2 Container Service	Full: List, Read	All resources	None
ElastiCache	Full: Read Limited: List	All resources	None
ELB	Full: List, Read	All resources	None
ELB v2	Full: Read	All resources	None
RDS	Full: List Limited: Read	All resources	None
SQS	Full: List Limited: Read	All resources	None

IAMユーザーを作成し、プログラムによるアクセスを許可する

既存のIAMユーザーを使用するか、または(ベストプラクティス)Sysdigバックエンドがプログラムで CloudWatchにアクセスしてそのデータを使用するための特定のIAMユーザーを作成します。

- 1. IAMコンソールで、<u>ユーザーを追加</u>します。
- 2. 「AWSアクセスタイプ:プログラムによるアクセス」を選択します。
- 3. 「既存のポリシーを直接アタッチ」を選択し、検索して、新しく作成したポリシーを選択します (サンプルポリシー名: SysdigMonitorPolicy)
- 4. 「ユーザーの作成」オプションを選択します。
- 生成されたアクセスキーとシークレットキーをコピーして保存します(注:シークレットは1回し か表示されないため、資格情報ファイルをダウンロードするか、キーを安全に保管して、再度参照 できるようにします)。





SysdigモニターUI

アクセスと秘密鍵を入力してください

- 1. Sysdig MonitorまたはSysdig Secureに管理者としてログインし、[Settings]を選択します。
- 2. AWSを選択します。

G User Profile	AWS accounts			
Subscription	Credentials	Status		
A Notifications		~ OK		
AWS				
Agent Installation				
Sysdig Storage		REFETCH NOW ADD		
L Users				
Teams	Add a new AWS account			
	See instructions here to gra	ant the proper access.		
	Access Key ID:	E.g. the second contract of the second contract		
		Please, insert a valid key id		
	Secret Access Key:			
		Please, insert a valid key		
		CANCEL SAVE		
	Amazon CloudWatch Integration			
	Sysdig Monitor can integrate CloudWatch metrics into your dashboards, allowing you to explore data from AWS services like RDS, EC2 and ELB alongside your existing Sysdig Monitor data.			
	CloudWatch can be selecte	ed in the 🕮 data source menu in the Explore page.		
	Warning: When this feature AWS (see Amazon CloudW	e is enabled, Sysdig Monitor will poll the CloudWatch API every 5 minutes, which will generate a small additional charge from /atch Pricing).		
	CloudWatch Integratio	on Status		
	Disabled Enabled			

3. ユーザーアクセスキーとシークレットキーを入力し、[save]をクリックして、アカウントを追加し ます。

資格情報は[OK]のステータスがチェックされた状態で表示されます。

注意

代わりにエラーが発生した場合は、入力した資格情報を再確認してください。入力ミスは、エラー の最も一般的な原因です。





CloudWatch統合を有効にする

- 1. まだ開いていない場合は、Sysdig Monitor UIのAWSページに移動します。
- 2. CloudWatch統合ステータスを有効に切り替えます。

Sysdig Monitorは5分ごとにCloudWatch APIをポーリングします。これにはAWSからの追加料 金が発生することに注意してください。

資格情報を再取得

統合されたAWSアカウントがAWS側で変更されると、[Settings]>[AWS]ページの[Credentials Status]にエラーが表示されます。

統合を再確立するには、「Refetch Now」ボタンを使用します。

Implicit Keyを使用してAWSアカウントを統合する(オンプレ ミスのみ)

SysdigがEC2インスタンスにインストールされている場合、そのインスタンスの既存のEC2 IAMロール を利用できます。これにより、Sysdigバックエンドに提供される公開鍵と秘密鍵を手動でローテーショ ンする必要がないため、管理が簡単になります。

Implicit Keyを使用

前提条件

適切なIAMロールを持つAWS EC2インスタンスにオンプレミスのSysdigプラットフォームをインス トールします。

注意

このオプションでは、ウェルカムウィザードのAWS統合ステップを使用できません。

暗黙的なキーを有効にするには、次のパラメータを設定する必要があります。





-Ddraios.providers.aws.implicitProvider=true

注意

初期インストール時、またはすでに手動でキーを入力している場合は、implicit keyに切り替えるためにこのパラメーターを使用します。

切り替える場合は、バックエンドでAPI、ワーカー、コレクターのコンポーネントを再起動する必要 があります。

[Settings]>[AWS]ページで、以前の認証情報は上書きされ、implicit keyが表示されます。

有効化の手順は、オーケストレーターとしてKubernetesを使用しているか、Replicatedを使用しているかによって異なります。

Kubernetes

1. config.yamlを編集して、次のエントリ(config.yamlのDataセクション内)に追加します。

sysdigcloud.jvm.api.options: sysdigcloud.jvm.worker.options: sysdigcloud.jvm.collector.options:







2. 手動キーからimplicit keyに切り替える場合は、API、ワーカー、コレクターのコンポーネントも再 起動する必要があります。

詳細については、<u>設定を変更する</u>を参照してください。

3. Sysdig UIでCloudwatch統合を有効にします。

Replicated

- Replicated管理コンソールで、Sysdig CloudアプリケーションのJVMオプションに
 -Ddraios.providers.aws.implicitProvider = trueと入力します。
- そのフィールドに他の設定がある場合は、エントリをスペースで区切ります。

Advanced Setting	5
Show Advanced Settings]
Leave empty to use defaults	
Cassandra JVM options	
-Xms m -Xmx m	
We HIGHLY recommend you explici	tly set Java -Xmx and -Xms parameters for this component.
Elasticsearch JVM options	
-Xms m -Xmx m	
We HIGHLY recommend you explici	tly set Java -Xmx and -Xms parameters for this component.
Sysdig Cloud application JVM o	ptions
-Xms m -Xmx m	
We HIGHLY recommend you explici	tly set Java -Xmx and -Xms parameters for this component.

<u>Replicated詳細設定</u>も参照してください。

- 手動キーから切り替える場合は、Replicated管理コンソールからバックエンドコンポーネントを再 起動する必要があります。
- 3. SysdigモニターUIでCloudWatch統合を有効にします。





ポーリングされるAWSサービスの変更

Sysdigは、IAMポリシーコードに反映される特定のAWSサービスのメタデータを収集するように設計 されています。

サービスは次のとおりです。

- DynamoDB
- EC2ホスト
- ECS
- Elasticache
- RDS
- SQS

上記のコードと統合手順を実装すると、2種類の収集がトリガーされます。最初に各サービスのメタ データが収集され、次にSysdigが返されたメタデータに関するメトリクスをポーリングします。そのた め、環境でサービスが有効になっていない場合、メタデータ(およびメトリクス)は収集されませ ん。有効になっているが、メトリクスをポーリングしたくない場合は、そのサービスに関連するコー ド行をIAMポリシーから削除します。これにより、潜在的な不要なAWS APIリクエストと潜在的な AWS料金が回避されます。

メトリクススディクショナリーの<u>AWS</u>も参照してください。

セキュリティグループ

オンプレミスのSysdigバックエンドがあり、送信セキュリティグループが制限されている場合、Sysdig バックエンドコンポーネントがAmazon APIに接続するために、HTTPSおよびDNSアクセスを許可する 必要がある場合があります。Amazon APIエンドポイントは名前で参照され、多数のIPがあるため、こ れはHTTPSおよびDNSの完全な0.0.0.0/0アウトバウンドアクセスである必要がある場合があります。

Amazon IP範囲のみをフィルタリングする必要がある場合は、以下をガイドとして使用できます。 https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html

特定のAWSリージョンのCloudWatchデータを取得する





環境内の特定のAWSリージョンのみからメトリクス収集を有効にするには、Sysdigサポートでチケットを開く必要があります。詳細については、サポートに連絡してください。

関連情報

Sysdigモニターに表示される結果のAWSサービスの詳細については、メトリクスディクショナリの AWS関連情報を参照してください(SysdigモニターUI内からも利用可能)。

ライセンスがAWSサービスビューに与える影響については、「<u>AWSサービスのライセンス</u>」を参照し てください。

使用するIAMポリシーコード

ベストプラクティス:Sysdigへのプログラムによるアクセスを許可するために使用するSysdig固有の IAMポリシーを作成します。以下のコードスニペットをコピーしてこのポリシーに貼り付けます。 Sysdigは、環境に応じて、次のサービスからメタデータとCloudWatchメトリクスを収集できます。

- Dynamodb
- EC2ホスト
- ECS
- Elasticache
- RDS
- SQS

注意

独自のAWS S3バケットを使用してSysdigキャプチャファイルを保存する場合は、これらのコードス ニペットをこのIAMポリシーに追加することもできます。詳細については、「ストレージ:AWS キャプチャファイルストレージの構成(オプション)」を参照してください。





詳細については、ポーリングされるAWSサービスの変更を参照してください。

AWSロールの委任と統合する

このセクションでは、Amazon Webサービス(AWS)AssumeRole機能を利用するようにSysdigモニ ターを設定し、Sysdigモニターがクラウドアセットを検出し、AWSアカウントからCloudWatchメトリ クススを取得し、キャプチャを格納するためにカスタムS3バケットを利用することを承認する方法に ついて説明します。AWSロールと統合すると、Sysdig AWSアカウントに関連付けられていないAWSリ ソースへのアクセスを委任できます。




ロールを介してクロスアカウントアクセスを設定すると、各アカウントで個別のIAMユーザーを作成す る必要がなくなります。さらに、ユーザーは、別のAWSアカウントのリソースにアクセスするため に、1つのアカウントからサインアウトして別のアカウントにサインインする必要はありません。

役割の委任は、アクセスキーを使用する既存の統合方法の代替手段です。Amazonは開発者のアクセス キーをサードパーティと共有することを推奨していないため、この方法は安全であると考えられてい ます。

前提条件とガイドライン

このトピックは、次の準備が整っており、AWSに精通していることを前提としています。

- SysdigモニターAPIトークン
- External ID
- APIエンドポイント。このトピックでは、{{host}}として参照されます
 - SaaS:エンドポイントは、モニターの場合はhttps://app.sysdigcloud.com、セキュアの場合はhttps://secure.sysdig.comです。
 - オンプレミス:オンプレミスのデプロイメントに依存します。
- AWS統合を構成するための管理者権限
- APIクライアント。このトピックの例ではcurlを使用しています
- AWSアカウントID
 - SaaS: AWSアカウントID例は273107874544です
 - オンプレミス: 顧客固有

APIでAWSロールの委任を有効にする

このセクションでは、APIを使用してAWSロールの委任を有効にする方法について説明します。

SaaSの手順

- <u>External IDを取得</u>します。
- <u>役割の委任を設定</u>します。
- <u>ロールARNを取得</u>します。
- <u>AWSアカウントを追加</u>します。





オンプレミスの手順

- <u>External IDを取得</u>します。
- <u>役割の委任を設定</u>します。
- <u>ロールARNを取得</u>します。
- <u>AWSアカウントを追加</u>します。
- オンプレミスの追加設定に従います。

External IDを取得する

次のようにExternal IDを取得します。

curl -k --request GET \ --url {{host}}/api/users/me \ --header 'authorization: Bearer e71d7c0f-501e-47d4-a159-39da8b716f44' | jq '.[] | .customer | .externalId'

応答のExternal IDの例は、04acdd59-4c98-4d11-8ee5-424326248161です。

役割の委任を設定する

Sysdigプラットフォームとアマゾンウェブサービスを統合するには、AWS IAMを使用してロールの委 任を設定する必要があります。

1. AWS IAMコンソールで新しいロールを作成します。

Create role		
Select type of trusted entity		
AWS service EC2, Lambda and others Allows entities in other accounts to perform actions	Web identity Cognito or any OpenID provider SAML 2.0 federation Your corporate directory sin this account. Learn more Same Second Sec	
Specify accounts that can use th	nis role	
Account ID*	059797578166	
Options	 Require external ID (Best practice when a third party will assume this role) 	
	You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more	
	External ID p4acdd59-4c98-4d11-8ee5-	





- a. ロールタイプとして、「別のAWSアカウント」を選択します。
- b. (SaaS) アカウントIDにSysdigアカウントIDを入力します。

これは、AWSデータへの読み取り専用アクセスを許可していることを意味します。

- c. [Require external ID]を選択し、前の手順で取得したものを入力します。 MFAを無効 のままにします。
- 2. 次へ:権限をクリックします。
- 3. 次のポリシーを作成します。
 - sysdig_cloudwatch:リストへのアクセスを提供し、サポートされるAWSリソースを記述し、それらのCloudWatchメトリクスを取得します。
 - sysdig_s3:キャプチャを保存するバケット名を定義します

ポリシーの詳細については、<u>使用するIAMポリシーコード</u>を参照してください。

ポリシーの作成方法の詳細な手順については、「<u>AWSアカウントを手動で統合する</u>」を参照してくだ さい。

- a. ポリシーがすでに作成されている場合は、このページでポリシーを検索して選択し、手順にスキップしてください。それ以外の場合は、[Create Policy]をクリックすると、新しいウィンドウが開きます。
- b. [ポリシーの確認]をクリックします。
- c. ポリシーに名前を付け、適切な説明を入力します。たとえば、sysdig_cloudwatch。
- d. 「ポリシーの作成」をクリックします。

このウィンドウを閉じることができます。

- 4. [ロールの作成]ウィンドウで、ポリシーのリストを更新し、作成したポリシーを選択します。
- 5. [次へ]をクリックします。
- 6. ロールに名前と適切な説明を付けます。たとえば、sysdig_roleです。
- 7. 「役割の作成」をクリックします。





ロールARNを取得

1. Roles> sysdig-roleを選択します。

Roles > sysdig-role

Role ARN	arn:aws:iam: B:role/sysdig-role
Role description	Edit
Instance Profile ARNs	42
Path	/
Creation time	2020-01-14 17:56 UTC+0100
Last activity	2020-01-14 18:31 UTC+0100 (9 days ago)
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=sysdig-role&account=4

Permissions Trust relationships Tags Access Advisor Revoke sessions

- Permissions policies (2 policies applied)

2. ロールARNをコピーします。

AWSアカウントを追加する

作成したロールを使用して、Sysdigモニター側にAWSアカウントを追加します。 次のAPI呼び出しを使 用します。

```
curl --request POST \
    --url {{host}}/api/providers \
    --header 'authorization: Bearer e71d7c0f-501e-47d4-a159-39da8b716f44' \
    --header 'content-type: application/json' \
    --data '{"name": "aws","credentials": {"role": "<Role_ARN>"},"alias": "role_delegation"}'
```

<Role_ARN>を前のセクションでコピーしたものに置き換えます。 応答には、すべてのプロバイダーがリストされます。応答の例を以下に示します。





```
"provider": {
    "id": 7,
    "name": "aws",
    "credentials": {
      "id": "role delegation",
     "role": "arn:aws:iam::485365068658:role/sysdig-access3"
    },
    "tags": [],
    "status": {
      "status": "configured",
     "lastUpdate": null,
     "percentage": 0,
      "lastProviderMessages": []
    },
    "alias": "role delegation"
 }
}
```

役割の委任が作成されていることを確認します。

- 1. 管理者としてSysdig MonitorまたはSysdig Secureにログインします。
- 2. [Settings]>[AWS]を選択します。

{

- 3. 作成したロールがAWSアカウントのリストに追加されます。
- 4. CloudWatchとAWS S3バケットの有効化に進みます。

詳細については、<u>AWS:AWSアカウントとCloudWatchメトリクススの統合(オプション)</u>を 参照してください。





オンプレミスの追加構成

- 1. 一時的な認証情報を取得するために使用されるAWSユーザーを作成します。
- 2. AssumeRoleを許可するポリシーをユーザーに割り当てます。例えば:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::{ACCOUNT-ID}:role/{ROLE_NAME}*"
}
```

- 3. 次のいずれかのソースからユーザーがアクセスキーを利用できるようにします。
 - 環境変数
 - Javaシステムプロパティ
 - Amazon EC2メタデータサービスを通じて配信されるインスタンスプロファイルの認証情報。

インストールがAWS上にある場合は、EC2メタデータサービスをお勧めします。

- 例:Kubernetesインストールで環境変数を設定する
- 1. シークレットを作成:

```
apiVersion: v1
kind: Secret
metadata:
   name: aws-credentials
type: Opaque
data:
   aws.accessKey: {{BASE64_ENCODED_ACCESS_KEY_ID}}
   aws.secretKey: {{BASE64_ENCODED_ACCESS_KEY_SECRET}}
```

 デプロイメント記述子(sysdigcloud-collector、sysdigcloud-worker、sysdigcloud-api)の変数と、 新しく作成されたシークレットの参照値を公開します。

```
    name: AWS_ACCESS_KEY_ID
    valueFrom:
    secretKeyRef:
    key: aws.accessKey
    name: aws-credentials
    name: AWS_SECRET_ACCESS_KEY
```





```
valueFrom:
secretKeyRef:
    key: aws.secretKey
    name: aws-credentials
```

新しい変数がインストーラーの一部になるまで、各プラットフォームアップデートの記述子に 変数を追加します。

リソースディスカバリのセットアップ

サポートされるAWSは、EC2、RDS、Elastic Load Balancer(ELB)、ElastiCache、SQS、DynamoDB 、およびApplication Load Balancer(ALB)です。

デフォルトでは、AWSがサポートするすべてのリージョンのすべてのリソースがフェッチされます。 これは、API経由でプロバイダーキーを作成するときにリージョンをホワイトリストに登録することで 回避できます。 リージョンをホワイトリストに登録するときのプロバイダーキーリクエストの本文の 例:

```
{
    "name": "aws",
    "credentials": {
        "role": "arn:aws:iam::676966947806:role/test-assume-role"
    },
    "additionalOptions": "{\"regions\":[\"US_EAST_1\",\"US_EAST_2\"]}"
}
```

ストレージ : キャプチャーファイルのオプション の設定

Sysdigキャプチャー機能を使用すると、エージェントがインストールされたホストからリモート接続を 介して詳細なシステムトレースデータを記録できます。SaaSのインストールでは、デフォルトで、こ のデータはSysdigのセキュア Amazon S3ストレージロケーションの、アカウント用の別のパーティショ





ンに保存されます。オンプレミスインストールでは、デフォルトで、データはCassandraデータベース に保存されます。

このページでは、AWS S3バケットの使用(SaaSおよびオンプレミスで利用可能)とカスタムS3スト レージの使用(オンプレミスのみ)の2つのカスタム代替案について説明します。

AWS S3ストレージを設定する

このオプションを設定するには、Sysdig設定UIのフィールドを使用して、Sysdig統合用にAWSで作成したIAMポリシーにコードを追加します。

前提条件

- AWSアカウントはSysdigと統合する必要がありますが、CloudWatch機能を有効にする必要はありません。
- <u>AWS:AWSアカウントとCloudWatchメトリクススの統合(オプション)</u>を参照してください
- S3バケット名を用意します。

Sysdigモニター側

Settings

- 1. 管理者としてSysdig Monitorにログインします。
- 2. 左下のナビゲーションのセレクタボタンから、[Settings]>[Sysdig Storage]を選択します。

Q Use Pole	Syndy Monge			
Babacrytics.	Configure your SD bucket to intern systely bace files.			
hethoatons	Use a custom to burner.			
Art Art	APRI 13 Judiet rate			
Apert musilation	Next of the control of the section of the factor make to provide any site on the section of the			
O Tyrofig Romage	To do so, open the AMS identity and Access Management (IAM) page and poll the following policy (expand)			
± liters	(
	*Artuer's (*Artuer's (*Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet's *Silvet			
	where BREKET, MARKE is the name of the Stitubater you configure.			

3. Use a custom S3 bucket を有効にして、AWSS3バケット名を入力します。

テストするには:SysdigモニターUIでトレースファイルをキャプチャーします。





有効にすると、ファイルキャプチャーを設定するときに、「Sysdig Monitor Storage」または独自のストレージバケットを選択するオプションが表示されます。Sysdigキャプチャファイルの作成を参照してください。

カスタムS3エンドポイントを設定する

Sysdigオンプレミス展開にキャプチャを保存するために、<u>MinioやIBM Cloud Object Storage</u>などのカス タムAmazon-S3互換ストレージを設定できます。キャプチャーの保存場所は、Sysdig MonitorとSysdig Secureの両方に使用できます。これはAPIのみの機能であり、現在、UIサポートは利用できません。

この設定を機能させるには、Sysdigインストールに対応するvalues.yamlを構成する必要があります。

前提条件

- オンプレミスインストールはインストーラーベースです。Sysdigプラットフォームを手動でインストールし、キャプチャーファイルを保存するようにカスタムS3バケットを設定する場合は、Sysdigの担当者にお問い合わせください。
- 認証に使用されるAWSクライアント互換の認証情報が環境に存在することを確認します。
- リスト、取得、および書き込み操作が、使用するS3バケットで機能していることを確認してく ださい。これを確認するには、たとえば、<u>IBM CloudのAWS CLI</u>で説明されているように、S3 ネイティブツールを使用します。

インストーラーの設定

コレクター、ワーカー、およびAPIサーバーがカスタムエンドポイント構成を認識するように、 values.yamlファイルで以下のパラメーターを構成します。

```
• sysdig.s3.enabled
```

```
Required: true
Description: Specifies if storing Sysdig Captures in S3 or S3-compatible storage
is enabled or not.
Options:true|false
Default:false
```

```
例:
sysdig:
s3:
```

enabled: true





sysdig.s3.endpoint

Required: true

Description: Specifies if storing Sysdig Captures in S3 or S3-compatible storage is enabled or not. Options:true|false Default:false

例:

```
sysdig:
s3:
enabled: true
```

sysdig.s3.bucketName

Required: true Description: The name of the S3 or S3-compatible bucket to be used for captures. This option is ignored if sysdig.s3.enabled is not configured

例:

sysdig:

s3: endpoint: <Name of the S3-compatible bucket to be used for captures>

sysdig.accessKey

Required: true Description: The AWS or AWS-compatible access key to be used by Sysdig components to write captures in the S3 bucket.

例:

sysdig: accessKey: BASE64_ENCODED_ACCESS_KEY_ID

sysdig.secretKey

Required: true Description: The AWS or AWS-compatible secret key to be used by Sysdig components to write captures in the s3 bucket.





例: sysdig: secretKey: BASE64_ENCODED_ACCESS_KEY_SECRET

たとえば、次のAWS CLIコマンドは、SysdigキャプチャーファイルをMinioバケットにアップロードします。

aws --profile minio --endpoint http://10.101.140.1:9000 s3 cp <Sysdig Capture filename>
s3://test/

この例では、エンドポイントはhttp://10.101.140.1:9000/であり、バケットの名前はtestです。

S3設定が完了したら、インストーラーを使用したオンプレミスインストールの手順に進みます。





Customer Numberを見つける

SysdigのSaaS顧客は、Sysdig環境が最初にプロビジョニングされたときに電子メールで提供される一意の顧客番号で識別できます。通常、顧客番号を知る必要はなく、ユーザーインターフェイスに目立つように表示されませんが、一部の構成設定では必要になる場合があります。番号を取得するには:

- 1. Sysdigインターフェースにログインします。
- 2. URLエンドポイント/api/user/me? product=SDCに移動します。
- 3. JSONのcustomer:id部分を見つけて、Customer Numberを特定します。



注意

オンプレミス環境の場合、お客様番号は通常1になります。





エージェントのインストール:概要とキー

[エージェントインストール]ページには、さまざまな種類のエージェントインストールに必要なコード 行をコピー/貼り付けるためのショートカットがあります。

エージェントアクセスキーを取得することもできます(コピー/貼り付け)。

管理者が選択した場合、このページは非管理者から非表示にすることができます。[ユーザープロファ イル]ページの[管理者設定の変更]も参照してください。

エージェントアクセスキーを取得する

キーを取得するか、エージェントインストールコードスニペットを使用するには

1. Sysdig MonitorまたはSysdig Secure (例えば管理者として) にログインし、[Settings]を選択しま す。



- 2. Agent Installation を選択します。
- 3. オプション: [Copy]ボタンを使用して、ページの上部にあるアクセスキーをコピーします。



オプション:リストにあるように、サンプルコードを確認して使用し、エージェントをインストー ルします。

 User Profile Subscription 	Access Key COPY	
Notifications	Agent Installation	
AWS	Tagging your machines is highly recommended! Replace example_tag:example_value in the commands with a comma-separated list of tags (eg.	
Sysdig Storage	Note: tags will also be created automatically from your infrastructure's metadata, including AWS, Docker, Mesos, Kubernetes, etc	
Users	If you have any issues, please refer to the full installation instructions and FAQ pages. And do not hesitate to contact us at support@sysdig.com!	
	Install in a Docker container	
	The Sysdig Monitor agent is available to run inside a single Docker container to report on the entire host. 1. First, install kernel headers on the host:	
	Debian-like distributions: apt-get -y install linux-headers-\$(uname -r) COPY	
	2. Now install the Sysdig Monitor container on the host:	
	<pre>docker run -dname sysdig-agentrestart alwaysprivilegednet hostpid host -e ACCESS_KEY= TAGS=example_tag:examp -v /var/run/docker.sock:/host/var/run/docker.sock -v /dev:/host/dev -v /proc:/hos o -v /boot:/host/boot:ro -v /lib/modules:/host/lib/modules:ro -v /usr:/host/usr:ro ize=350m sysdig/agent</pre>	
	Note, this will run the container in detached mode. To see the container's output, remove the "-d".	
	Install on Linux	
	Run this single command to install the agent automatically.	
	<pre>curl -s https://s3.amazonaws.com/download.draios.com/stable/install-agent sudo bash COPY -saccess_keytags example_tag:example_value</pre>	
	Install on Kubernetes	
	Complete instructions for installing and configuring Systig Monitor on Kubernetes can be found on the support page	



P

//



サブスクリプション:ライセンスされたエージェ ントの数の変更

管理者は、[Settings]>[Subscription]タブで、Sysdigからライセンスを取得した予約済みエージェント とオンデマンドエージェントの数を変更できます。

非管理者はエージェントの数を表示できますが、エージェントを追加または削除する計画をカスタマ イズすることはできません。

エージェントサブスクリプションプランを表示または変更するには:

- 1. Sysdig MonitorまたはSysdig Secureに管理者としてログインします。
- 2. 左側のナビゲーションの[セレクタ]ボタンから、[Settings]> [Subscription]を選択します。



4. 年間プランをアップグレードするか、ライセンスを取得したエージェントの数を調整するには、
 [プランのカスタマイズ]を選択します。





て調整し、[Ch o	e <mark>ckout</mark>]をクリックします。
Customi	ze your plan
Agents increase the number of Reserved A	gents to monitor.
# of Reserved Agents \$0 each / month 15 € ✓ Billed Annually	Total recurring charge \$0 per month Upgrade to an annual subscription for a 20% discount
d Agents iemand Agents to surge your capac nable On-demand Agents	ity and only pay for what you use.
of On-demand Agents S0 each / hour	For example: if you used an On-demand Agent for 4 hours each day, then your On-demand bill would be about \$0.00/month. 4 hrs × 30 days × \$0 = \$0.00
	C調整し、[Che Customi Agents @ increase the number of Reserved A # of Reserved Agents S0 each / month 15 章 イ Billed Annually d Agents @ demand Agents to surge your capace nable On-demand Agents of On-demand Agents S0 each / hour

以下も参照してください。

- <u>ライセンスの仕組み</u>
- <u>AWSサービスのライセンス</u>





ライセンスの仕組み

購入したエージェントライセンスの数は、Sysdigの使用方法に2つの異なる影響を及ぼします。

- エージェント数は、デプロイできるエージェントの最大数を定義します。たとえば、100個のライ センスを購入すると、100個のエージェントをインストールできます。エージェントは、予約済み エージェントとオンデマンドエージェントに分割される可能性があります。
- AWSでは、Sysdig Monitorダッシュボードで表示できるAWSオブジェクトの数も決定します(実際にインストールされているエージェントの数とは関係ありません)。つまり、100個のライセンスを購入した場合、リージョンごと、サービスタイプごとに100個のAWSオブジェクトしか表示できません。詳細については、AWSサービスライセンスを参照してください。

AWS環境で許可されているライセンス(およびオブジェクトビュー)の数を確認するには、Settings >Subscriptionページを確認してください。

エージェントがインストールされているホストの正確なビューを取得するには、許可された最小の時 間間隔を使用して、Agent Summary dashboardを適用します(履歴データが表示されないようにしま す)。

予約済みエージェントとオンデマンドエージェント

予約されたエージェントは購入され、継続的に毎月使用されます。オンデマンドエージェントは、短期間のニーズに応じて1時間ごとにライセンスを取得できます。たとえば、組織が2日間のスケールテ ストをスケジュールし、その時間枠で追加の500のオンデマンドエージェントにライセンスを付与する 場合があります。予約エージェントとオンデマンドエージェントの違いは、技術的なものではなく、 財務的なものです。オンデマンドエージェントを使用すると、予約済みエージェントとまったく同じ ように動作します。

エージェントをバックエンドに接続する

Sysdigプラットフォームは、同時使用ライセンスモデルを使用して、インストールされたエージェント がバックエンドサーバーに接続し、ホストメトリクスに関するレポートをいつ許可するかを決定しま す。つまり、Sysdigエージェントを任意の数のインスタンスにインストールできます。ただし、ライセ ンスされた数のエージェントのみが接続して、記録とレポートのためのメトリクスを送信できます。





エージェントは「先着順」で接続し、オーバーサブスクリプション(ライセンスを必要とするよりも 多くのエージェントが通信を希望する)が発生した場合、エージェントは定期的に再接続を試みま す。既存の通信インスタンスがダウンして切断されると、接続を試みる次のエージェントが許可され ます。

オーバーサブスクリプションが原因でエージェントが接続を拒否するのを防ぐには、確立され、許可 された接続の数を監視します。使用中のライセンスの数を確認するには、[Settings]>[Subscription] ページを参照してください。この情報を使用して、UIから追加のライセンス容量を購入するか、通常 のオーケストレーションおよびシステム管理手段を介して優先度の低いエージェントをシャットダウ ンします。

技術的な詳細

複数のインストール:エージェントは基本的にソフトウェアの「インストール」です。システムが外 部IPアドレスを変更した場合、またはVMイメージをシャットダウンして別の場所に戻した場合、これ は同じエージェント接続のままです。ただし、同時にデータを送信している同一のインストール(通 常は事故)は、2つの接続と見なされます。MACアドレスは、ライセンスの目的でホストを識別する ために使用されます。

ライセンスリリースのタイムラグ:なんらかの理由でホストをシャットダウンした場合、エージェントのライセンスはすぐにはリリースされません。これにより、エージェントは短時間の停止または再 起動のためにライセンススロットを保持できます。タイムアウト間隔には最大20分かかる場合があり、その間隔内に接続が再確立されない場合、接続を待機している次のホストが使用できるようにラ イセンスが解放されます。





AWSサービスのライセンス

[Explore]タブまたはSysdigモニターのダッシュボードで、AWSサービスごとに表示されるメトリクスの数は、リージョンごとに購入または使用されたエージェントライセンスの数によって制限されます。

ライセンス数:

- 予約済みエージェントとオンデマンドエージェントが含まれます(使用されていない場合でも)。
- 各リージョンの各サービスに表示されるAWSリソースの数を決定するために使用されます。
- 異なるAWSサービス間で転送できません。

<u>ライセンスの仕組み</u>もご覧ください。

AWSサービスタイプの優先順位と制限

AWSサービスタイプごとに、サービスは次の優先順位で表示されます。

- EC2:エージェントがインストールされているインスタンスを選択すると、ECSに属するインス タンスがインスタンスの前に、インスタンスIDのアルファベット順に、ライセンス数まで起動 されます。
- RDS: ライセンス数まで、最も古いインスタンスを最初に作成時間で選択します。
- ELB:バランスのとれたインスタンスの数(大きいほうのELBが最初)で選択し、次に作成時間 で古いものから、ライセンス数まで選択します。
- ElastiCache:名前で並べ替え、最大ライセンス数のアイテムを表示します。
- SQS:キューを名前で並べ替え、フェッチするキューの数をライセンス数まで取得します。
 データは、メトリクスを報告しているキューについてのみ表示されます。
- DynamoDB:名前で並べ替え、ライセンス数まで表示します。
- ALB:名前で並べ替え、最大ライセンス数の項目を表示します。

AWSメトリクススの詳細については、メトリクススディクショナリのAWSを参照してください。





ユースケースの例

200個のAWSインスタンスがあり、100個のSysdigエージェントライセンスを購入し、実際に50個の エージェントをインストールしたとします。

AWSサービスのビューには、リージョンごとに次の制限が適用されます。

- EC2:エージェントがインストールされた50のインスタンスが最初に表示され、次にEC50から、次にECSから、さらに稼働時間ごとに50のインスタンスが表示されます。
- RDS:最も古いものから100個のRDSリストが表示されます。
- ELB: 100個のELBが表示され(最初に大きい)、次に作成時間順に表示されます。
- ElastiCache: 100のElastiCacheオブジェクトが、名前のアルファベット順に表示されます。
- SQS:メトリクスを報告している100個のSQSキューが表示されます。
- DynamoDB: 100のDynamoDBが名前のアルファベット順に表示されます。
- ALB: 100のALBが名前のアルファベット順に表示されます。

AWSサービスビューの項目の制限を増やすには、Sysdigセールスに連絡して、ライセンス契約に応じ て追加のリソースを有効にします。「<u>サブスクリプション:ライセンスされたエージェントの数の変</u> 更」も参照してください。





認証と承認(SaaS)

Sysdig MonitorとSysdig Secureは、いくつかのユーザー認証/承認方法で機能するように設計されています。

タイプ	デフォルトで有効	統合手順が必要
User email/password	Yes	No
Google OAuth	No	No
SAML	No	Yes
OpenID Connect	No	Yes

ユーザーのビュー:



このセクションのページでは、SAMLまたはOpenID Connectに必要な統合と有効化の手順、および Okta、OneLogin、Keycloakなどのこれらのプロトコルをサポートする<u>IDプロバイダー(IdP)サービ</u> <u>ス</u>について説明します。SaaS環境では、簡単なドロップダウン選択でGoogleログインを有効にできま す。統合はすでに実行されています。





注意

SAMLまたはOpenID ConnectをSysdig MonitorとSysdig Secureの両方と統合するには、統合ステップを2回(各Sysdig製品に対して1回)実行する必要があります。

ワークフロー

新しい承認UIでは、シングルサインオン(SSO)オプションを有効にする基本的なプロセスは次のとおりです。

- 企業で使用しているSSOオプション(GoogleOAuth、SAML、OpenID)と、使用しているIdPサービス(Okta、OneLoginなど)を確認します(ある場合)。
- 2. 適切な[認証]タブで、選択したSSOに必要な接続設定を入力します。(注:Googleの場合、設定は すでに入力されています。)
- 3. IdP側で関連するIdP設定を構成します。
- (有効なシングルサインオン)ドロップダウンからSSOオプションを選択し、[認証を保存]をクリックします。
- 5. Sysdig MonitorとSysdig Secureの両方を有効にする場合は、2番目のアプリケーションでプロセス を繰り返します。

Set	tings		
٢	User Profile	Authentication	
•	Users	Enabled Single Sign-On Google Gauth 🗸	
	Teams		Enable Authentication
	Notification Channels		
•	AWS	Connection Settings	
0	Sysdig Storage	OpenID SAML Google Oauth	
	Subscription	Application ID	
Ţ	Agent Installation	Application Secret	
04	Authentication	URL Redirect	

SaaS環境でのGoogle OAuthの認証ページの表示。





Google OAuth (SaaS)

注意

SAMLまたはOpenID ConnectをSysdig MonitorとSysdig Secureの両方と統合するには、統合ステップを2回(各Sysdig製品に対して1回)実行する必要があります。

SaaS環境では、GoogleユーザーはGoogle OAuth経由でログインすることができます。

SaaSプラットフォームはこのようなログインを許可するように事前設定されているため、すでに Googleサービス(G Suiteなど)を使用している環境では、これがログインを簡略化するための最も便 利なアプローチであると考えられます。

Google OAuthを有効にする

Google OAuthはSysdigによって事前に設定されているため、管理者はそれを有効にするために、選択した認証オプションとしてそれを選択するだけで済みます。

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



2. Authenticationを選択します。





(事前設定された(編集できない)設定を表示する場合は、[Google OAuth]タブを選択します。)

Sett	tings		
٢	User Profile	Authentication	
:	Users	Enabled Single Sign-On Gcogle Gauth 🗸	
	Teams	Enable Aut	hentication
۰	Notification Channels		
٠	AWS	Connection Settings	
0	Sysdig Storage	OpenID SAML Google Oauth	
目	Subscription	Application ID	
Ţ	Agent Installation	Application Secret	
07	Authentication	URL Redirect	

- 3. [Enabled Single Sign-On]ドロップダウンから[Google OAuth]を選択し、[Save Authentication] をクリックします。
- 4. 両方のアプリケーションで有効にする場合は、Sysdig MonitorまたはSysdig Secureについて繰り返します。

ユーザー体験

Google OAuthログインを成功させるには、次の要件に注意してください。

警告

ユーザーは、環境に少なくとも一度は正常にログインしている必要があります(電子メールベースの招待を介して、初期パスワードを設定しているなど)。

Sysdigプラットフォームでのユーザーのログインユーザー名は、ユーザーのGoogleメールアドレス と正確に一致する必要があります(つまり、短縮/変更されたGoogleメールエイリアスにすることは できません)。

このようなユーザーがGoogle OAuth経由でログインするには、[Log in with Google]ボタンをクリックします。





itor
d *OpenID



ユーザーのブラウザーがGoogleによる認証にまだ成功していないか、ブラウザーが認識している複数のGoogleプロファイルを持っている場合、Sysdig環境にリダイレクトされる前に、プロファイルを選択してパスワードを入力するためのGoogleページが表示されます(必要な場合)。

ユーザーの作成については、<u>ユーザーとチームの管理</u>も参照してください。





SAML (SaaS)

注意

このガイドは、クラウドベース(SaaS) Sysdig環境に固有です。オンプレミスのSysdig環境を構成す る場合は、代わりにSAML(オンプレミス)を参照してください。

SysdigプラットフォームでのSAMLサポートにより、選択したアイデンティティプロバイダー (IdP) による認証が可能になります。

Sysdigプラットフォームは通常、独自のユーザーデータベースを維持して、ユーザー名とパスワードの ハッシュを保持します。代わりにSAMLを使用すると、組織のIdPにリダイレクトして、ユーザー名/パ スワード、およびSysdigアプリケーションへのアクセスを許可するために必要なその他のポリシーを検 証できます。SAMLによる認証が成功すると、Sysdigプラットフォームのユーザーデータベースに対応 するユーザーレコードが自動的に作成されますが、IdPに送信されたパスワードは、Sysdigプラット フォームによって見られたり保存されたりすることはありません。

このセクションでは、SAMLをSysdig MonitorとSysdig Secureの両方と統合して有効にする方法について説明します。

特定のIdP統合情報については、以下を参照してください。

- Okta (SAML)
- OneLogin (SAML)
- ADFS (SAML)

<u>警告</u>も参照してください





基本的な有効化ワークフロー

ステップ	オプション	注意
1.会社が使用し、構 成するldPを把握し ます。	 Okta (SAML) OneLogin (SAML) ADFS (SAML) 	これらは、Sysdigが詳細な相互運用性テストを実行 し、標準のドキュメントを使用して統合する方法を 確認したIdPです。 IDPがリストにない場合でも、Sysdigプラットフォー ムで動作する可能性があります。Sysdigサポートに お問い合わせください。
2コーザーに休験さ	SAMIボタンをクリッ	ann sysdigcloud comまたはsecure sysdig com>ページ

2.ユーザーに体験さ SAMLボタンをクリッ app.sysdigcloud.comまたはsecure.sysdig.com>ページ せるログインフ クし、会社名を入力し から、会社名を入力します。 ローを決定します ます (3つのオプション から選択しま す)。

ブラウザでURLを入力 /ブックマーク	Monitor: https://app.sysdigcloud.com/api/saml/ <pre>company_name Secure: https://secure.sysdig.com/api/saml/ company_name?product=SDS</pre>
ldPインターフェース からログイン	個々のIdP統合ページでは、SysdigをIdPインター フェースに追加する方法について説明しています。 手元にSysdig customer numberが必要です。





3. IdPインター フェースで構成手 順を実行し、結果 の構成属性を収集 します。 • Okta (SAML)

OneLogin

(SAML)

• ADFS (SAML)

メタデータURL(またはXML)を収集してテストし ます。

IDPによって開始されるログインフローを設定する場

合は、SysdigのCustomer numberを手元に用意して

ください。後の構成ステップで次のように参照され ます

CUSTOMER_ID_NUMBER.

4 a, Sysdig Monitorまたは Sysdig Secure Settingsに (管理 者として) ログイ ンし、UIに必要な 構成情報を入力し ます。SSOとして SAMLを有効にし ます。 4b. Monitorと Secureの両方を使 用している場合 は、 他の Sysdig 製 品に対してプロセ スを繰り返します

管理者の手順

IdPを設定する 以下のリストから適切なIdPを選択し、指示に従ってください。

- Okta (SAML)
- OneLogin (SAML)





• ADFS (SAML)

設定でSAMLを有効にする

ベースラインSAML機能を有効にするには:

SAML接続設定を入力

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



- 2. Authenticationを選択します。
- 3. [SAML]タブを選択します。

User Profile	Authentication	
Users	Enabled Single Sign-On	None ~
t eams		Enable Authentication
Notification Channels	Connection Settin	gs
AWS	LDAP OpenID	SAML Google Oauth
Sysdig Storage	Metadata	
Subscription		Enter Metadata URL
Agent Installation	Signed Assertion	SysdigCloud app should verify that every single assertion is signed
+ Authentication	Email Parameter	Enter Email Parameter
	Validate Signature	Sysdig app should verify that the response is signed
	Verify Destination	Flag to control whether Sysdig should check the "destination" field in the SAML Response. This should ensure that the SAML Response was intended for the receiving SP. it may be disabled if the IDP is not sending on it, or in special cases where the destination is not the one set in the IDP configuration(e.g. proxy in front of sysdig app)

4. 関連するパラメータを入力し(下の表を参照)、[save]をクリックします。

接続設定	オプション	説明	サンプル エントリ
Metadata	URL	IdP構成手順の最後に提供されるURL	





	XML	URLによるメタデータXMLの抽出をサ ポートしないIdPに使用できるオプショ ン	
Signed Assertion	off/on	Sysdigは、応答に署名されたアサーショ ンをチェックする必要があります(正し いIdPの検証を支援するため)	ON
Email Parameter	email	ユーザーEメールIDのSAML応答のパラ メーターの名前。Sysdigはこれを使用し て、応答からユーザーのEメールを抽出 します	email
Validate Signature	off/on	Sysdigバックエンドは、応答が署名され ていることを確認する必要があります	ON
Verify Destination	off/on	SysdigがSAMLResponseの「宛先」 フィールドをチェックするかどうかを制 御するフラグ。セキュリティ対策として ONを推奨します。Sysdigバックエンド の前にあるプロキシーなど、特殊なケー スではオフになる場合があります。	ON

SSOにSAMLを選択

- 1. [Enabled Single Sign-On]ドロップダウンから[SAML]を選択します
- 2. [Save Authentication] をクリックします。
- 3. 両方のアプリケーションで有効にする場合は、Sysdig MonitorまたはSysdig Secureの有効化プロセ ス全体を繰り返します。

ユーザー体験

上記の基本的な有効化ワークフローで述べたように、SAML構成を使用してログインする3つの方法を ユーザーに提供できます。

• Sysdig SaaS URLから開始して、SAMLボタンをクリックできます。

モニター: app.sysdigcloud.comまたはセキュア: secure.sysdig.com

彼らは会社名の入力を求められるので、Sysdigプラットフォームは認証のためにブラウザーを IdPにリダイレクトできます。







● ユーザーが会社名を次の形式で入力する必要がないように、代替URLを提供できます。

Sysdig Monitor: https://app.sysdigcloud.com/api/saml/ COMPANY_NAME

Sysdig Secure: https://secure.sysdig.com/api/saml/ COMPANY NAME?product=SDS

 IdPを構成するときに、IdPによって開始されるログインフローを構成できます。次に、ユー ザーはIDPのアプリディレクトリからSysdigアプリケーションを選択し、SysdigアプリケーションのURLを直接参照しません。

注意

Sysdig Secureへの最初の成功したSAMLログインを完了するユーザーは、「ユーザーにSysdig Secure にログインする権限がありません」というエラーメッセージを受け取る場合があります。これは、 Secure OperationsチームのメンバーのみがSysdig Secureへのアクセスを許可されており、新しく作 成されたログインは、デフォルトではこのチームに存在しないためです。そのようなユーザーは、 Sysdig環境をSecure Operationsチームに追加するために管理者に連絡する必要があります。

すべてのユーザーにデフォルトでSecureへのアクセスを許可する環境では、この<u>サンプルPythonス</u> <u>クリプト</u>を使用して、チームメンバーシップを頻繁に「同期」できます。





Sysdigが提供するサンプルPythonスクリプトの使用に関するヒントについては、開発者用ドキュメントを参照してください。

ユーザーの作成については、<u>ユーザーとチームの管理</u>も参照してください。

注意事項

- SAMLアサーションの暗号化/復号化は現在サポートされていません。
- <u>SAMLシングルログアウト</u>はサポートされていません。したがって、ユーザーはSysdigアプリ ケーションから直接ログアウトするように注意する必要があります。

Okta (SAML)

開始する前に<u>SAML(SaaS)</u>を確認してください。

OktaでのSAMLアプリケーションの設定に関するOktaのドキュメントを使用して、Sysdig Monitorや Sysdig SecureをSAMLアプリケーションとして設定します。以下の注記は、追加のアクションが必要な 特定のステップを示しています。

Okta設定におけるSysdig固有の手順

Oktaステップ6

ステップ#6で、IDPによって開始されるログインフローを設定しない場合は、[ユーザーにアプリケー ションアイコンを表示しない]および[Oktaモバイルアプリにアプリケーションアイコンを表示しない] のチェックボックスをオンにします。

オクタステップ7

手順7で、次の表に示す値を入力します。IDPによって開始されるログインフローを設定する場合は、 CUSTOMER-ID-NUMBERを、「Find Your Customer Number」の説明に従って取得した番号に置き 換えます。





設定	Value for Sysdig Monitor	Value for Sysdig Secure
Single sign on URL	https://app.sysdigcloud.com/api/ saml/auth	https://secure.sysdig.com/api/saml/sec ureAuth
Audience URI (SP Entity ID)	https://app.sysdigcloud.com/api/ saml/metadata	https://app.sysdigcloud.com/api/saml/m etadata
Default RelayState	#/&customer= CUSTOMER-ID-NUMBER	#/&customer= CUSTOMER-ID-NUMBER
(optional - only configure if you intend to use IDP-initiated login		

flow)

オクタステップ8

ステップ#8では、Oktaの例に示されているものの代わりに、値を追加します。

Name	Value
email	user.email
first name	user.firstName
last name	user.lastName

属性では大文字と小文字が区別されるため、属性を入力するときは注意してください。

メールのみが必要です。ただし、新しいユーザーが初めてSAML経由で正常にログインしたときに、 Sysdigプラットフォームのデータベースで作成されたレコードにこれらの値が含まれるようになるため、姓/名を含めることをお勧めします。

Oktaステップ10

ステップ#10で、URLをコピーし、SAML接続設定の[SAML設定]ページのメタデータエントリに貼り 付けます。





メタデータのテスト(オプション)

IDP構成手順の最後にコピーするメタデータURLが正しいことを確認するには、ブラウザーから直接ア クセスしてメタデータURLをテストできます。

URLにアクセスすると、ブラウザーは、以下に示す例のように始まるXMLファイルをすぐにダウン ロードする必要があります。それを正常にダウンロードするために、資格情報の入力やその他のセ キュリティ対策は必要ありません。これが当てはまらない場合は、IDP構成手順に再度アクセスしてく ださい。

<?xml version= "1.0" ?><EntityDescriptor xmlns= "urn:oasis:names:tc:SAML:2.0:metadata"
entityID= "https://app.onelogin.com/saml/metadata/680358" ><IDPSSODescriptor xmlns:ds=
"http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
"urn:oasis:names:tc:SAML:2.0:protocol">names:tc:SAML:2.0:metadata"
https://app.onelogin.com/saml/metadata/ 680358 ">...

OneLogin (SAML)

開始する前に<u>SAML(SaaS)</u>を確認してください。

<u>OneLogin SAML Test Connectorを使用する</u>というタイトルのOneLoginの記事を使用して、Sysdig MonitorやSysdig SecureをSAMLアプリケーションとして設定します。以下の注記は、追加のアクションが必要な特定のステップを示しています。

OneLogin構成におけるSysdig固有の手順

SAMLテストコネクタの追加

「SAMLテストコネクタの追加」のステップで、SAMLテストコネクタ(IdPw/attrw/sign response) を選択します。 IDPによって開始されるログインフローを構成しない場合は、スライダーをオフにし て、「ポータルで表示」されないようにします。

テストコネクタ設定ページの設定





[テストコネクタ設定ページ]で、次の表に示す値を入力します。IDPによって開始されるログインフ ローを構成する場合は、CUSTOMER-ID-NUMBERを、<u>お客様番号の検索に関する説明</u>に従って取得し た番号に置き換えます。

フィールド	Value for Sysdig Monitor	Value for Sysdig Secure
RelayState	#/&customer=	#/&customer= CUSTOMER-ID-NUMBER
(オプション-IDPによって 開始されるログインフロー を使用する場合にのみ構成 します)	CUSTOMER-ID-NUMBER	
Recipient	https://app.sysdigcloud.co m/api/saml/auth	https://secure.sysdig.com/api/saml/secu reAuth
ACS (Consumer) URL Validator	https://app.sysdigcloud.co m	https://secure.sysdig.com
ACS (Consumer) URL	https://app.sysdigcloud.co m/api/saml/auth	https://secure.sysdig.com/api/saml/secu reAuth

(オプション)新規ユーザーが初めてSAML経由で正常にログインしたときに、Sysdigプラットフォー ムのデータベースに作成されたレコードにユーザーの名と姓を含める場合は、[パラメーター]タブをク リックします。[パラメーターを追加]をクリックし、2つの新しいフィールドをそれぞれ作成します。 SAMLアサーションに含めるには、毎回ボックスをオンにします。次に、各フィールドをクリックして 編集し、ドロップダウンメニューから表示される値を選択してから、[保存]をクリックします。

Field Name	Value
first name	First Name
last name	Last Name

フィールド名では大文字と小文字が区別されるため、すべて小文字で入力するように注意してください。





以下は、名の正しく構成されたフィールドの例を示しています。

	Edit Field First Name
Name	first name
Value	First Name 🔹
Flags	Include in SAML assertion
	CANCEL DELETE SAVE

発行者のURL

[SSO]タブをクリックし、発行者のURLをコピーして、SAML接続設定の[SAML設定]ページの[メタデー タ]エントリに貼り付けます。

メタデータのテスト(オプション)

IDP構成手順の最後にコピーするメタデータURLが正しいことを確認するには、ブラウザーから直接ア クセスしてメタデータURLをテストできます。

URLにアクセスすると、ブラウザーは、以下に示す例のように始まるXMLファイルをすぐにダウン ロードする必要があります。それを正常にダウンロードするために、資格情報の入力やその他のセ キュリティ対策は必要ありません。これが当てはまらない場合は、IDP構成手順に再度アクセスしてく ださい。

<?xml version= "1.0" ?> <EntityDescriptor xmlns= "urn:oasis:names:tc:SAML:2.0:metadata"
entityID= "https://app.onelogin.com/saml/metadata/680358" > <IDPSSODescriptor xmlns:ds=
"http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
"urn:oasis:names:tc:SAML:2.0:protocol" >names:tc:SAML: 2.0 :metadata " entityID="
https://app.onelogin.com/saml/metadata/ 680358 "> ...




ADFS (SAML)

開始する前に<u>SAML(SaaS)</u>を確認してください。

これらの手順では、インターネットにアクセス可能なADFS(Active Directoryフェデレーションサービス)サーバーがすでに動作していることを前提としています。相互運用性テストは、特にWindows Server 2012 R2上のADFSで実行されました。

以下の手順に従って、Windows Server ManagerのADFS管理ツールでADFSを構成します。

サービスプロバイダーが開始するログインフローの場合

 [サービス]>[フェデレーションサービスプロパティの編集]を右クリックします。フェデレーション サービス識別子のホスト名に注意してください。これは、Sysdig認証設定の[SAML構成]ページの [メタデータ]エントリに貼り付けるメタデータURLで使用されるためです。具体的には、メタデー タURLの形式はhttps://HOSTNAME/FederationMetadata/2007-06/FederationMetadata.xmlです。 また、SysdigプラットフォームがこのURLに直接アクセスできるように、このホストはDNSで解決 し、有効な(自己署名されていない) SSL/TLS証明書を持っている必要があります。





	Federation Service Properties
General	Organization Events
Federat	ion Service display name:
adfstest	local
Example	e: Fabrikam Federation Service
Federat	ion Service name:
fs1.adfs	test.local
Example	e: fs.fabrikam.com
Federat	ion Service identifier:
http://fs	s1.adfstest.local/adfs/services/trust
Example Web S	e: http://fs.fabrikam.com/adfs/services/trust 50 lifetime: 480
	OK Cancel Apply

- 2. Sysdigアプリケーションの証明書利用者信頼構成を追加します。
 - a. [証明書利用者信頼]>[証明書利用者信頼の追加]を右クリックし、[開始]をクリックしてウィ ザードを開始します。

91		AD F	S	_ _ X
🎲 File Action View 🕅	Window Help			_ 6
ad FS		Relying Party Trusts		Actions
Service Grust Relationships Claims Provider 1 Rehimp Party True	Trusts	Display Name Device Registration Service	Enabled 1 Yes V	Relying Party Trusts
Attribute Store Add Relying Party Trucke Add Relying Party Authentication Pc Add Non-Clain View	Party Trust ims-Aware Relying Party Trust		View New Window from Here	
	New Window Refresh	from Here		Ci. Refresh
	Help			Device Registration Service
Contains commands for cust	tomizing this win	<	5	



- b. [データソースの選択]ステップで、証明書利用者に関するデータを手動で入力するボタ ンをクリックし、[次へ]をクリックします。

Ŷ .	Add Relying Party Trust Wizard
Select Data Source	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authoritation Rules Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network: Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Ederation metadata address (host name or URL): Ederation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Impgrt data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported to the relying party from a file. Use this option to import the necessary data and certificates from a relying party organization that has exported to the file. Federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Enverse (e) Enter data about the relying party manually: Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

c. 選択した表示名(「Sysdig Monitor」または「Sysdig Secure」など)を入力し、[次へ]を クリックします

\$	Add Relying Party Trust Wizard
Specify Display Nar	ne
Steps Welcome Select Data Source	Enter the display name and any optional notes for this relying party. Display name: Sysdig Monitor
 Specify Display Name Choose Profile Configure Certificate Configure URL Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	Ngtes:





d. [次へ]をクリックして、ADFSプロファイルを使用するデフォルトのオプションを受け入 れます

Q	Add Relying Party Trust Wizard
Choose Profile	
Choose Profile Steps Welcome Select Data Source Choose Profile Configure Cettificate Configure UtIL Configure Identifiers Configure Multi factor Authentication Now? Concose Issuance Authonization Rules Ready to Add Trust Finish	 This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust. AD ES profile This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol. △ AD FS 1.0 and 1.1 profile This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.
	< Previous Next > Cancel

e. [次へ]をクリックして、オプションのトークン暗号化証明書の選択をスキップします(Sysdigはこのオプションをサポートしていません)

\$ 1	Add Relying Party Trust Wizard
Configure Certificate	9
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Cetificate Configure URL Configure Identifiers Configure Multi Actor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to it. To specify the certificate, click Browse Issuer: Subject: Brective date: Eprintion date: Image: Image: Image: Image:





f. [SAML 2.0 Web SSOプロトコルのサポートを有効にする]チェックボックスをオンにして、証明書利用者のSAML 2.0 SSOサービスURLに次のいずれかの値を入力します。

Sysdig Monitorを構成する場合は、https://app.sysdigcloud.com/api/saml/authと入力します。

Sysdig Secureを構成する場合は、https://secure.sysdig.com/api/saml/secureAuthと入 カします。

次に「次へ」をクリックします。

\$	Add Relying Party Trust Wizard
Configure URL	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party. ☐ Enable support for the WS-Federation Passive protocol The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL: Relying party <u>W</u> S-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/ls/ ✓ Engble support for the SAML 2.0 WebSSO protocol The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 webSSO protocol. Relying party <u>SAML 2.0 SSO</u> service URL: https://app.sysdigcloud.com/api/saml/auth] Example: https://www.contoso.com/adfs/ls/
-	< Previous Next > Cancel

g. 証明書利用者信頼識別子には、次のいずれかの値を入力します。

Sysdig Monitorを構成する場合は、https://app.sysdigcloud.comと入力します。

Sysdig Secureを構成する場合は、https://secure.sysdig.comと入力します。





次に[追加]をクリックし、	[次へ]をクリックします。

Add Relying Party Trust Wizard	x
Relying parties may be identified by one or more unique identifier strings. Specify the identifiers f party trust. Relying party trust identifier:	or this relying
https://app.sysdigcloud.com	Add
Example: https://fs.contoso.com/adfs/services/trust	
Relying party trust identifiers:	
	Remove
< Previous Next >	Cancel
	Add Relying Party Trust Wizard Relying parties may be identified by one or more unique identifier strings. Specify the identifiers party trust. Relying party trust identifier: Interst/facor.org/adis/services/trust Relying party trust identifiers:

h. [次へ]をクリックして、多要素認証の構成をスキップします

Ŷ.	Add Relying Party Trust Wizar	d 2
Steps Welcome Select Data Source	Configure multi-factor authentication settings for this relyin there is a match for any of the specified requirements.	g party trust. Multi-factor authentication is required if
Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Identifiers	Multi-factor Authentication Requirements Users/Groups Not config Device Not config Location Not config	Global Settings pured pured
Athentication Now? Choose Issuance Authonization Rules Ready to Add Trust Finish	I do not want to configure multi-factor authentication s Configure multi-factor authentication settings for this re You can also configure multi-factor authentication setti Authentication Policies node. For more information, set	ettings for this relying party trust at this time. alying party trust. Ings for this relying party trust by navigating to the e <u>Configuring Authentication Policies</u> .
		< Previous Next > Cancel



- ユーザーにSysdigアプリケーションへのログインを許可するかどうかのポリシーを選択します。デフォルトでは、すべてのユーザーに証明書利用者へのアクセスを許可するというデフォルトの設定が許容されます。次へをクリックします。

\$	Add Relying Party Trust Wizard
Choose Issuance Au	thorization Rules
Choose Issuance Au Steps • Welcome • Select Data Source • Choose Profile • Configure Cettificate • Configure URL • Configure Multi-factor • Configure Multi-factor • Configure Multi-factor • Configure Multi-factor • Choose Issuance Authonization Now? • Ready to Add Trust • Finish	thorization Rules Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. • Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. O Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next > Cancel

j. 概要を確認し、[次へ]をクリックして証明書利用者信頼の構成を完了します

Ŷ	Add Relying Party Trust Wizard				
Ready to Add Trust					
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Cetificate Configure URL Configure URL Configure Multifactor Authonization Now? Choose Issuance Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Not(< Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL: Monitor relying party Automatically update relying party This relying party's federation metadata data was last checked on: <never> This relying party was last updated from federation metadata on: <never></never></never>				
	< Previous Next > Cancel				





k. 次のステップでは、クレームルールを追加する必要があります。チェックボックスをオンのままにして[クレームルールの編集]ダイアログを開き、[閉じる]ボタンをクリックして、クレームルールエディターにすぐに移動できます。

\$	Add Relying Party Trust Wizard
Finish	
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. ✓ Open the Edt Claim Rules dialog for this relying party trust when the wizard closes
	Close

- 3. SamlResponseSignatureオプションがSysdig認証構成と一致していることを確認してください。
 - a. PowerShell経由でSet-AdfsRelyingPartyTrust/Get-AdfsRelyingPartyTrustコマンドレットを 使用して、SamlResponseSignatureを構成します。

-SamlResponseSignature

依存パーティが期待する応答署名を指定します。このパラメーターの許容値は次のとお りです。

AssertionOnly

 ${\it MessageAndAssertion}$

MessageOnly

詳細については、「<u>Set-AdfsRelyingPartyTrust</u>」を参照してください。

b. Sysdigアプリで[設定]>[認証]に移動し、Sysdig認証設定がSamlResponseSignatureにマッ プされていることを確認します。



User Profile	Authentication	
Users	Enable Single Sign On	None
Teams		Set Authentication
Notification Channels	Connection Cotting	
AWS	Connection Setting	gs General and the second
Sysdig Storage	LDAP OpenID	SAML Google Dauth AssertionOr
Agent Installation	Metadata	● URL ○ XML
	1 million 1	Enter Metadata URL
Authentication	Signed Assertion	SysdigCloud app should verify that every single assertion is signed
	Email Parameter	Enter Email Parameter
	Validate Signature	Sysdig app should verify that the response is signed MessageOr
	Verify Destination	Flag to control whether Sysdig should check the "destination" field in the SAML Response. This should
		ensure that the SAML Response was intended for the receiving SP. It may be disabled if the IDP is not
		sending on it, or in special cases where the destination is not the one set in the IDP configuration(e.g.
		proxy in ironi or sysdig app)
	Create user on login	Flag to enable/disable create user on login

MessageAndAssertionで、両方のオプションを有効にします。

- 次に、クレームルールを使用して、必要に応じてログインデータがSysdigプラットフォームに送信 されるようにします。Sysdigプラットフォームへのユーザーのログインは電子メールアドレスに基 づいており、デフォルトのADFS構成では必要に応じて電子メールアドレスを送信しません。次の 構成により、Active Directoryの正しいフィールドがクレームで配信されるようになります。
 - a. 前の手順のクレームルールエディターにまだない場合は、作成した証明書利用者信頼を右ク リックして[クレームルールの編集]を選択し、エディターに移動します。





R	AD) FS		- x
🎲 File Action View Window Help				- 8 ×
AD FS	Relying Party Trusts		Actions	_
Service Service Trust Relationships Cleims Provider Trusts Relying Party Trusts Authenticute Stores Authentication Policies	Contract Name Device Registration Service Update from Federati Edit Claim Rules Digable Properties Delete Help	Enabled T Yes V ion Metadata	Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying Party Trust View New Window from Here Refresh Help Sysdig Monitor Update from Federation Metadata Edit Claim Rules Disable Properties Velete Help	

ssuance Transform Rule	S les anne Authorization R	des Delegation & thoriz	ation Rides
The following transform	rules specify the claims that	will be sent to the relying ;	party.
Order Rule Name		Issued Claims	
			*
Add Rule Ed	Rule Remove Rule		
		OK Cancel	Apply

b. Add Ruleをクリックします。次の画面で、デフォルトのルールテンプレートを受け入れて LDAP属性をクレームとして送信し、[次へ]をクリックします。



Фр	Add Transform Claim Rule Wizard
Select Rule Templat	e e
Steps	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Choose Hule Type Configure Claim Rule	Claim rule template:
	Send LDAP Attributes as Claims v Claim rule template description:
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > Cancel

c. ルールの名前を入力し、属性ストアとしてActive Directoryを選択してから、プルダウンセレ クターを使用して、LDAP属性と送信クレームタイプの両方として電子メールアドレスを選択 し、同様に、名と姓のプルダウン選択を行います。。これらの選択が完了したら、[完了]をク リックします。



which	to extract LDAP attributes. Specify how I from the rule.	the a	attributes will map to the outgoing claim types that will b	be
laim I	rule name:			
bysdig	g Monitor Username			
Rule t	emplate: Send LDAP Attributes as Claim	ıs		
ttribu	te store:			
Active	a Directory			
NCLIVE	e Directory		•	
Nappi	ing of LDAP attributes to outgoing claim	types	3:	
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)	
	E-Mail-Addresses		E-Mail Address	Y
•	Given-Name	Y	Given Name	~
	Sumame	~	Sumame	Y
8		¥		Y

d. ここでもう一度[ルールの追加]をクリックします。今度は、着信クレームを変換するためのテ ンプレートを選択します

Q 0	Add Transform Claim Rule Wizard
Select Rule Templa	te
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Transform an Incoming Claim
	Claim rule template description:
	Using the Transform an Incoming Claim rule template you can use this inicoming claim, change its claim type, and optionally change its claim value. For example, you can use this line template to create a rule that will send a role claim with the same claim value of an incoming group claim. Wu can also use this nule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim. With a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.





e. ルールの名前を入力し、プルダウンを使用して、電子メールアドレスの受信クレームタイプ、 名前IDの送信クレームタイプ、および電子メールの送信名ID形式を選択し、[完了]をクリック します。

Q 0	Add Transf	orm Claim Rule Wizard		×
Configure Rule				
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to also map an incoming claim v outgoing claim type and whe Claim rule name:	map an incoming claim type to an outgoing of alue to an outgoing claim value. Specify the ther the claim value should be mapped to a n	claim type. As an option, you can incoming claim type to map to the ew claim value.	5
	Translate Email to Name ID			
	Rule template: Transform an	Incoming Claim		
	Incoming claim type:	E-Mail Address	~	
	Incoming name ID format:	Unspecified	~	
	Outgoing claim type:	Name ID	*	
	Outgoing name ID format:	Emei	~	
	 Pass through all claim val Replace an incoming claim value: 	ues n value with a different outgoing claim value	1	
	Outgoing claim value:		Browse	
	O Replace incoming e-mail	suffix claims with a new e-mail suffix		
	New e-mail suffix:			
		Example: fabrikam.com		
		< Previous	Finish Cancel	-

f. (オプション)新規ユーザーが初めてSAML経由で正常にログインしたときに、Sysdigプラットフォームデータベースで作成されたレコードにユーザーの名と姓を含める場合は、追加の変換ルールも作成する必要があります。メールベースのユーザー名のみが必須であり、このためのルールはすでに作成されているため、この手順はオプションです。

これを行う場合は、[ルールの追加]をクリックし、もう一度、受信クレームを変換するための テンプレートを選択します。ルールの名前を入力し、プルダウンを使用して、受信クレームの 種類として名を選択します。送信クレームの種類については、フィールドに名前を直接入力し ます。[完了]をクリックした後、[ルールの追加]をクリックし、同様のルールを作成して、姓 の受信クレームタイプを姓の送信クレームタイプに変換します。



	9	

Configure Rule			
Steps	You can configure this rule to	n man an incoming claim type to an outgoing cla	im type. As an option, you can
Choose Rule Type	also map an incoming claim v	value to an outgoing claim value. Specify the inc	coming claim type to map to the
Configure Claim Rule	outgoing claim type and whe	ther the claim value should be mapped to a new	/ claim value.
	Claim rule name:		
	Pula tamplata: Transform an	Lassening Claim	
	Hule template: Transform an	incoming Claim	
	Incoming claim type:	Given Name	~
	Incoming name ID format:	Unspecified	~
	Outgoing claim type:	first name	~
	Outgoing name ID format:	Unspecified	v
	Pass through all claim val	lies	
	Replace an incoming clai	in value with a different outgoing claim value	
	Incoming claim values		
	incoming claim value.		
	Outgoing claim value:		Browse
	O Replace incoming e-mail	suffix claims with a new e-mail suffix	
	New e-mail suffix:		
		Example : fabrikam.com	
0 Configure Rule	Add Trans	form Claim Rule Wizard	
Configure Rule Steps Choose Rule Type	Add Trans You can configure this rule f also map an incoming claim	form Claim Rule Wizard	laim type. As an option, you can coming claim type to map to the
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans You can configure this rule t also map an incoming claim outgoing claim type and wh Claim rule name.	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne	laim type. As an option, you can coming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame	laim type. As an option, you can coming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans You can configure this rule t also map an incoming claim outgoing claim type and wh Claim rule name: Translate Sumame to last n Rule template: Transform an	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame n incoming Claim	laim type. As an option, you can coming claim type to map to the w claim value.
Configure Rule Reps 0 Choose Rule Type 0 Configure Claim Rule	Add Trans You can configure this rule t also map an incoming claim outgoing claim type and wh Claim rule name : Irranslate Sumame to last n Rule template: Transform an	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame In Incoming Claim	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps 0 Choose Rule Type 0 Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame Incoming Claim Sumame	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps 0 Choose Rule Type 0 Configure Claim Rule	Add Trans You can configure this rule f also map an incoming data outgoing claim type and wh Claim rule name: Translate Sumame to last n Rule template: Transform an Incoming claim type: Incoming name ID format:	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame n Incoming Claim Sumame Unspecified	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps 0 Choose Rule Type 0 Configure Claim Rule	Add Trans Yeu can configure this rule also map an incoming claim outgoing claim type and wh Claim rule name: Translate Sumame to last n Rule template: Transform ar Incoming claim type: Incoming name ID format: Outgoing claim type:	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame n Incoming Claim Sumame Unspecified last name	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans You can configure this rule i autoping claim type and wh Claim rule name: Translate Sumame to last n Rule template: Transform ar Incoming claim type: Incoming name ID format: Outgoing claim type:	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified Iast name Unspecified	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified Iast name Unspecified alues	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir ether the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified last name Unspecified alues aim value with a different outgoing claim value	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified last name Unspecified alues aim value with a different outgoing claim value	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified last name Unspecified alues aim value with a different outgoing claim value	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame ame Unspecified last name Unspecified alues aim value with a different outgoing claim value	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Steps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified last name Unspecified alues aim value with a different outgoing claim value I suffix claims with a new e-mail suffix	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Steps Choose Rule Type Configure Caim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified last name Unspecified alues aim value with a different outgoing claim value I suffix claims with a new e-mail suffix	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Steps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified last name Unspecified alues aim value with a different outgoing claim value sum value with a different outgoing claim value sum value with a new e-mail suffix Example: fabrikam.com	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Sumame Unspecified Iast name Unspecified alues aim value with a different outgoing claim value I suffix claims with a new e-mail suffix Example: fabrikam.com	laim type. As an option, you can nooming claim type to map to the w claim value.
Configure Rule Reps Choose Rule Type Configure Claim Rule	Add Trans	form Claim Rule Wizard to map an incoming claim type to an outgoing cl value to an outgoing claim value. Specify the ir either the claim value should be mapped to a ne ame ame In Incoming Claim Unspecified Iast name Unspecified alues aim value with a different outgoing claim value I suffix claims with a new e-mail suffix Example: fabrikam.com	laim type. As an option, you can nooming claim type to map to the w claim value.

g. 最後のルールを作成した後に[完了]をクリックすると、エディターにすべてのルールが表示されます。[OK]をクリックすると、SysdigアプリケーションのADFS構成が完了します。Sysdig サポートがサポートリクエストで送信するメタデータURLを使用して構成の側面を完了する と、テストできます。





suance	Transform Rules	Issuance Authorization Rules	Delegation Authorization Ru	les
The follo	owing transform n	ules specify the claims that will	be sent to the relying party.	
Order	Rule Name		Issued Claims	
1	Sysdig Monitor	Usemame	E-Mail Address, Given Na	
2	Translate Emai	to Name ID	Name ID	
3	Translate Give	n Name to first name	first name	
4	Translate Sum	ame to last name	last name	
			2	
		Rule Remove Rule		

IdPによって開始されるログインフローの場合(オプション)

(オプション)上記の手順は、サービスプロバイダーが開始するSAML構成を表しています。 IdPに よって開始されるSAML構成を希望する場合、これはADFSでも可能ですが、以下で説明する追加の手 順が必要です。

 Sysdigプラットフォームでは、IdPによって開始されるログインフローを受け入れるために、 RelayStateの特定の設定が必要です。テストされたADFSバージョンでは、このRelayStateの使用 はデフォルトで無効になっていることがわかりました。Microsoftの記事でこのトピックについて 詳しく説明しています。これを有効にするには、Microsoftフォーラムスレッドで説明されている ように、ADFSホストで %systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.configを編集し、

systemPools(ADD)(APPOSITE Control of the anticyperver.bervice and the anticyperver.bervice anticyperver.bervice and the anticyperver.bervice and the anticyperver.bervice anticyperver.ber





- 2. <u>顧客番号の検索に関する説明</u>に従って、Sysdig Customer numberを取得する必要があります。
- 3. 次に、IdPによって開始されるログインURLを生成する必要があります。

正しい設定に加えて、適切にURLエンコードされている必要があります。この構成を簡単にするには、この<u>ADFS RelayState Generatorツール</u>を使用します。起動したら、以下の値を入力し、[URLの生成]ボタンをクリックします。

- IDP URL文字列には、https://YOUR_ADFS_SERVER/adfs/ls/idpinitiatedsignon.aspxと入力し ます
- 証明書利用者識別子には、次のいずれかの値を入力します。
- Sysdig Monitorを構成する場合は、https://app.sysdigcloud.comと入力します
- Sysdig Secureを構成する場合は、https://secure.sysdig.comと入力します。
- リレー状態/ターゲットアプリの場合は、#/&customer=CUSTOMER-ID-NUMBERを入力し、前のステップで取得したCUSTOMER-ID-NUMBERを置き換えます

ADFS RelayState Generator

AD FS 2.0 (Rollup 2 and Greater) RelayState Generator for IDP Initiated Signon

IDP URL String

https://fs1.example.local/adfs/ls/idpinitiatedsignon.aspx

Relying Party Identifier

https://app.sysdigcloud.com

Relay State / Target App

#/&customer=5551212

Generate URL

Results:

https://fs1.example.local/adfs/ls/idpinitiatedsignon.aspx? RelayState=RPID%3Dhttps%253A%252F%252Fapp.sysdigcloud.com%26RelayState%3D%25 23%252F%2526customer%253D5551212





注意

この結果URLは、SAML接続設定のメタデータエントリに貼り付けるメタデータURLで使用 されます。

4. ツールの結果URLを使用して、IdPで開始されたログインをテストします。この<u>Microsoft</u> フォーラムスレッドでは、ユーザーが

https://YOUR_ADFS_SERVER/adfs/ls/idpinitiatedsignon.aspxのプルダウンメニューからアプリ ケーションを選択したときに、そのようなURLを使用するようにADFSを構成することは明らか に不可能であることに注意してください。ただし、URLをカスタムポータルまたはブックマー クリストに埋め込むことができます。

5. これで、電子メールアドレスが構成されたActive Directoryユーザーを使用してログインをテストできます。

Published (Certificates	Member Of	Passwon	d Replication	n Dia	l-in	Object
Security Environmen		nvironment	Sessions		Remote control		ntrol
Remote Desktop S		ervices Profile CO		-MC +MC		ute Editor	
General	Address	Account	Profile	Telephone	es (Organ	nization
Seed come	John Doe						
rirst name		John					
Last name	r:	Doe					
Display na	ime:	John Doe					
Descriptio	n:						
Office:							
Telephone	e number:				Ot	her	
E-mail:		idoe@adfstes	t.local				
Web page) :				Ot	her	





メタデータのテスト(オプション)

IDP構成手順の最後にコピーするメタデータURLが正しいことを確認するには、ブラウザーから直接ア クセスしてメタデータURLをテストできます。

URLにアクセスすると、ブラウザーは、以下に示す例のように始まるXMLファイルをすぐにダウン ロードする必要があります。それを正常にダウンロードするために、資格情報の入力やその他のセ キュリティ対策は必要ありません。これが当てはまらない場合は、IDP設定手順に再度アクセスしてく ださい。

<?xml version= "1.0" ?> <EntityDescriptor xmlns=
"urn:oasis:names:tc:SAML:2.0:metadata" entityID=
"https://app.onelogin.com/saml/metadata/680358" > <IDPSSODescriptor xmlns:ds=
"http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
"urn:oasis:names:tc:SAML:2.0:protocol" >names:tc:SAML: 2.0 :metadata " entityID="
https://app.onelogin.com/saml/metadata/ 680358 "> ...

OpenID Connect (SaaS)

注意

このガイドは、クラウドベース(SaaS) Sysdig環境に固有です。オンプレミスのSysdig環境を構成 する場合は、代わりに<u>OpenID Connect (On-Prem)</u>を参照してください。

Sysdigプラットフォームの<u>OpenID</u>サポートにより、選択した<u>アイデンティティプロバイダー(IdP)</u>を 介した認証が可能になります。 このセクションでは、OpenID ConnectをSysdig MonitorとSysdig Secureの両方と統合して有効にする方法について説明します。







SysdigのOpenID機能の概要

Sysdigプラットフォームは通常、独自のユーザーデータベースを維持して、ユーザー名とパスワードの ハッシュを保持します。代わりにOpenIDを使用すると、組織のIdPにリダイレクトして、ユーザー名/ パスワード、およびSysdigアプリケーションへのアクセスを許可するために必要なその他のポリシーを 検証できます。OpenIDによる認証が成功すると、Sysdigプラットフォームのユーザーデータベースに 対応するユーザーレコードが自動的に作成されますが、IdPに送信されたパスワードは、Sysdigプラッ トフォームによって見られたり保存されたりすることはありません。

ステップ	オプション	注意
1.会社が使用し、設定 するldPを把握しま す。	 Okta (OpenID) OneLogin (OpenID) Keycloak (OpenID) 	これらは、Sysdigが詳細な相互運用性テストを実行し、標準のドキュ メントを使用して統合する方法を確認したOpenIDプロバイダーです。 OpenIDプロバイダーがリストされていない場合(<u>OpenID Connect</u> <u>Discovery</u> をサポートしていないものを含む)、それでもSysdigプラッ トフォームで動作する可能性があります。Sysdigサポートにお問い合 わせください。
2.ユーザーに体験して もらいたいログインフ ローを決定する:3つ のオプション	OpenIDボタンをク リックし、会社名を入 力します	app.sysdigcloud.comまたはsecure.sysdig.com>ページから、会社名を入 カします。

基本的な有効化ワークフロー







	ブラウザでURLを入力/ ブックマーク	Monitor: https://app.sysdigcloud.com/api/oauth/openid/CompanyName Secure: https://secure.sysdig.com/api/oauth/openid/CompanyName?product=S DS
	ldPインターフェース からログイン	個々のIdP統合ページでは、SysdigをIdPインターフェースに追加する 方法について説明しています。 Sysdig customer numberが必要になります。
3. IdPインターフェー スで設定手順を実行 し、結果の構成属性を 収集します。	 Okta (OpenID) OneLogin (OpenID) Keycloak (OpenID) 	メタデータURL(またはXML)を収集してテストします。 IDPによって開始されるログインフローを構成する場合は、Customer Numberを見つけて手元に用意してください。後の構成手順では CUSTOMER_ID_NUMBERとして参照されます。





4 a, Sysdig Monitorま たはSysdig Secure Settings (スーパー管 理者として) にログイ ンし、UIに必要な設 定情報を入力します。 OpenIDをSSOとして 保存して有効にしま す。 4 b, MonitorとSecure の両方を使用している 場合は、他のSysdig製 品に対してプロセスを 繰り返します。 各製品のIdPに個別のリダイレクトURLを入力しま す。それ以外の場合、統合プロセスは同じです。



IdPを設定する

以下の適切なIdPリンクを選択し、指示に従ってください:

- Okta (OpenID)
- OneLogin (OpenID)
- Keycloak (OpenID)

設定でOpenIDを有効にする

ベースラインOpenID機能を有効にするには:

OpenID基本接続設定を入力してください

1. 管理者としてSysdig MonitorまたはSysdig Secureにログインし、[Settings]を選択します。



2. Authenticationを選択します。





3. OpenID タブを選択します。

Settings		
User Profile	Authentication	
LUSERS	Enabled Single Sign-On None 🗸	
Teams	Enable Authentica	tion
Notification Channels		
AWS	Connection Settings	
Sysdig Storage	LDAP OpenID SAML Google Oauth	
Subscription	Client ID 0abc1defghiJ2K3LMNo4	
Agent Installation	Client Secret	
Or Authentication	Issuer URL Supported IDPs are Okta, Onelogin and Keycloak	
	Metadata Discovery Discovery is supported by the Issuer	
	Delete Settings S	ave

4. 関連するパラメータを入力し(下の表を参照)、[save]をクリックします。

接続設定	説明
Client ID	IdPによって提供されるID
Client Secret	IdPが提供するシークレット
Issuer URL	ldPから提供されたURL: <u>https://YOUR-ONELOGIN-DOMAIN.onelogin.com/oidc</u>

注意
Okta、OneLogin、Keycloakはメタデータの自動検出をサポートしているため、これらのIdPにはこ れらの設定で十分です。

OpenIDの追加設定を入力します(必要な場合)

OpenID IdPがメタデータの自動検出をサポートしていない場合があり、追加の構成設定を手動で入力 する必要があります。





この場合:

1. OpenIDタブで、Metadata Discoveryボタンをオフに切り替えて、ページに追加のエントリを表示します。

OpenID SAML G	loogle Oauth
lient ID	andrea@sysdig.com
lient Secret	······
suer URL	
Metadata Discovery	Discovery is supported by the Issuer
ase Issuer	
uthorization Endpoint	
oken Endpoint	
son Web Key Set Endpoint	

2. IdPから派生した関連パラメーターを入力し(下の表を参照)、[Save]をクリックします。

接続設定	説明
Base Issuer	必須。多くの場合、同じ発行者URLですが、個別の一般的なドメイン とユーザー固有のドメインを持つプロバイダーでは異なる場合があり ます (たとえば、一般的なドメイン: <u>https://openid-connect.onelogin.com/oidc、</u> ユーザー固有のドメイン: https://sysdig-phil-dev.onelogin.com/oidc)
Authorization Endpoint	必須。承認リクエストのエンドポイント
Token Endpoint	必須。 トークン交換エンドポイント
JSON Web Key Set Endpoint	必須。 トークン署名検証のための鍵資格情報を含むエンドポイント





Token Auth認証方法Methodサポートされている値:
client_secret_basic
client_secret_post (大文字小文字を区別しません)

SSOのOpenIDを選択

- 1. [Enabled Single Sign-On]ドロップダウンから[OpenID]を選択します。
- 2. 「Save Authentication」をクリックします。
- 両方のアプリケーションで有効にする場合は、Sysdig MonitorまたはSysdig Secureの有効化プロ セス全体を繰り返します。

ユーザー体験

上記の基本的な有効化ワークフローで述べたように、OpenID構成でログインする3つの方法をユー ザーに提供できます。

• Sysdig SaaS URLから開始して、OpenIDボタンをクリックできます。

モニター: app.sysdigcloud.comまたはセキュア: secure.sysdig.com

会社名の入力を求められるので、Sysdigプラットフォームは認証のためにブラウザーをIdPにリ ダイレクトできます。







• ユーザーが会社名を次の形式で入力する必要がないように、代替URLを提供できます。

モニター: https://app.sysdigcloud.com/api/oauth/openid/ _{CompanyName} Secure: https://secure.sysdig.com/api/oauth/openid/ _{CompanyName}?product=SDS

 IdPを設定するときに、IdPによって開始されるログインフローを設定できます。次に、ユー ザーはIDPのアプリディレクトリからSysdigアプリケーションを選択し、SysdigアプリケーションのURLを直接参照しません。

注意

ユーザーの作成については、<u>ユーザーとチームの管理</u>も参照してください。

Okta (OpenID)

OktaのOpenIDプロバイダーの設定

開始する前に、<u>OpenID Connect(SaaS)</u>を確認してください。

以下のメモでは、Oktaで実行する最小限の手順について説明します。環境の詳細に基づいて手順を調 整する必要がある場合があります。

- 1. 管理者権限を持つユーザーとしてOkta組織にログインし、管理ダッシュボードをクリックします
- [アプリケーションの追加]ショートカットをクリックし、[新しいアプリケーションの作成]ボタン をクリックします
- 3. プラットフォームタイプとして[Web]を選択し、サインオンメソッドとして[OpenID Connect]をクリックして、「作成]をクリックします。
- 4. 新しいアプリケーションを作成する
 - 選択した一般設定を入力してください
 - ログインリダイレクトURIの場合は、次のいずれかの値を入力します。





- Sysdigモニターを構成する場合は、
 https://app.sysdigcloud.com/api/oauth/openid/authと入力します。
- Sysdig Secureを構成する場合は、
 https://secure.sysdig.com/api/oauth/openid/secureAuthと入力します。
- 保存ボタンをクリックします
- 5. 次に、[全般]タブに移動します。表示されているクライアントIDとクライアントシークレットをメ モします。
- 6. これらは、Sysdig認証設定のOpenID構成ページに入力します。
- [サインオン]タブをクリックします。表示されている発行者のURLをメモします。Sysdigサポート に送信する必要があるためです。
- 8. OpenID設定のOpenID設定ページに入力します。

OneLogin (OpenID)

OneLoginのOpenIDプロバイダーの設定

開始する前に、<u>OpenID Connect(SaaS)</u>を確認してください。

以下のメモでは、OneLoginで実行する必要のある最小限の手順について説明します。環境の詳細に基 づいて手順を調整する必要がある場合があります。

- 1. 管理者権限を持つユーザーとしてOneLogin組織にログインし、[アプリ]>[カスタムコネクタ]をク リックして、[新しいコネクタ]ボタンをクリックします。
- 2. 新しいコネクタを作成する
 - 選択したコネクタ名を入力してください
 - OpenID Connectのサインオン方法を選択します
 - リダイレクトURIには、次のいずれかの値を入力します。
 - Sysdigモニターを構成する場合は、
 https://app.sysdigcloud.com/api/oauth/openid/authと入力します。
 - Sydig Secureを構成する場合は、
 https://secure.sysdig.com/api/oauth/openid/secureAuthと入力します。
 - 保存ボタンをクリックします

3. [その他のアクション]プルダウンメニューから、[アプリをコネクタに追加]を選択します





- [保存]をクリックして、アプリをカタログに追加します。クリックすると、追加のタブが表示されます。
- 5. [SSO]タブをクリックします。[トークンエンドポイント]ドロップダウンの設定をPOSTに変更し、 [保存]をクリックします。

Token Endpoint	Authentication Method		
	POST	•	

 まだ[SSO]タブで、表示されているクライアントIDとクライアントシークレットをメモします([ク ライアントシークレットを表示]をクリックして表示します)。

それらをOpenID設定に入力します。

7. 発行者のURLはhttps://YOUR-ONELOGIN-DOMAIN.onelogin.com/oidcで設定されることに注意してください

それらをOpenID設定に入力します。

注意

テスト中に、OneLoginがOpenIDプロバイダー設定で行われた変更を保持しないことがあることが わかりました。OneLogin設定を変更し、Sysdigアプリケーションにログインしようとしたときに HTTP 400 Bad Requestなどの問題が発生した場合は、OneLoginのカスタムコネクタとアプリ設定を 削除して、最初から再作成する必要がある場合があります。





Keycloak (OpenID)

KeycloakのOpenIDプロバイダーの設定

開始する前に、<u>OpenID Connect(SaaS)</u>を確認してください。

以下のメモでは、Keycloakで実行する必要のある最小限の手順について説明します。環境の詳細に基 づいて手順を調整する必要がある場合があります。

- 1. Keycloakサーバーの管理コンソールにログインします。
- 2. レルムを選択するか、新しいレルムを作成します。
- 3. [クライアント]をクリックし、[作成]ボタンをクリックします。
- 4. 選択したクライアントID(「SysdigMonitor」など)を入力し、メモします。

これは、Sysdig認証設定のOpenID構成ページに入力します。

- 5. [クライアントプロトコル]ドロップダウンでopenid-connectが選択されていることを確認します。 保存ボタンをクリックします。
- 6. OpenID Connect クライアントを構成する
 - Authorization EnabledのトグルをクリックしてONにします。
 - 有効なリダイレクトURIには、次のいずれかの値を入力します。
 - Sysdigモニターを構成する場合は、https://app.sysdigcloud.com/api/oauth/openid/auth と入力します。
 - Sysdig Secureを構成する場合は、 https://secure.sysdig.com/api/oauth/openid/secureAuthと入力します。
 - 保存ボタンをクリックします
- 7. [認証情報]タブをクリックします。表示される秘密に注意してください。
- 8. OpenID設定に入力します
- 発行者URLは、https://KEYCLOAK_SERVER_ADDRESS/auth/realms/REALM_NAMEで設定されま す。KEYCLOAK_SERVER_ADDRESSおよびREALM_NAMEは、設定を作成した環境から派生したも のです。OpenID設定に入力します。

