sysdig

アドミニストレーション
設定

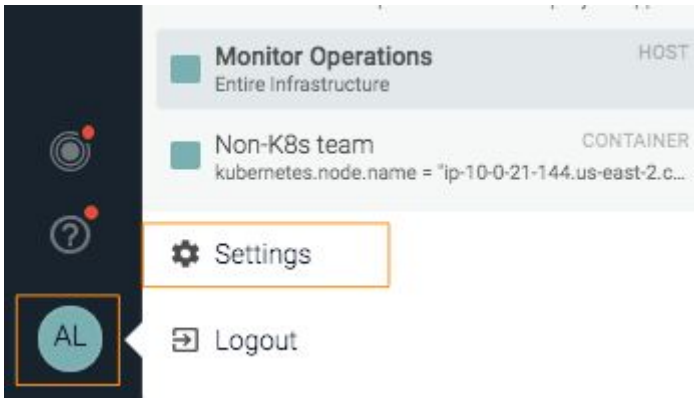
本文の内容は、Administration Settingsのドキュメント(https://docs.sysdig.com/en/administration-settings.html)を元に日本語に翻訳・再構成した内容となっております。

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

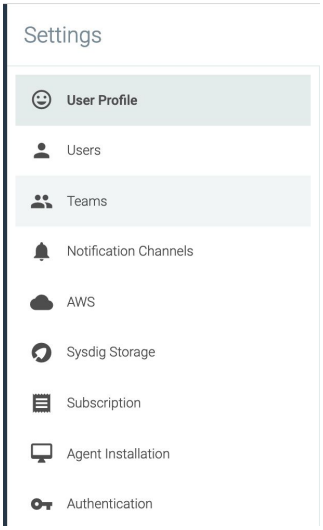
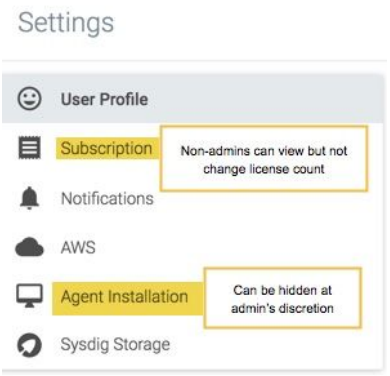
Sysdig MonitorまたはSysdig Secureナビゲーションバーの左下隅からパネルにアクセスします。



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
	

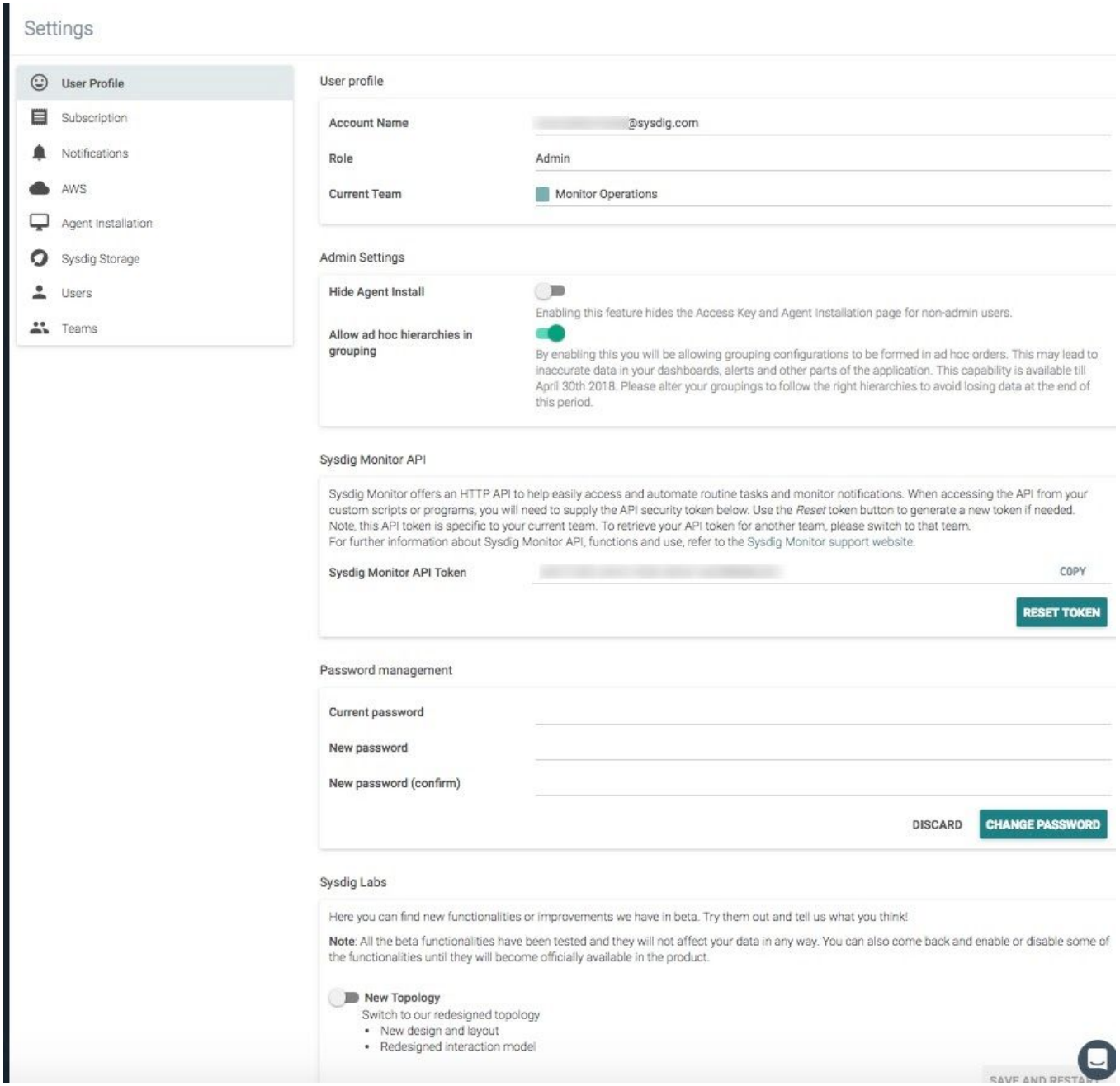
ユーザープロファイルとパスワード

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。



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。

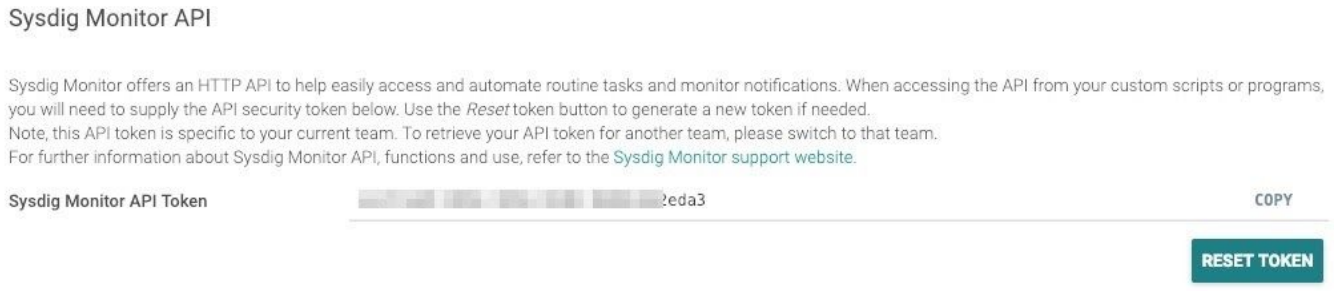
  設定パネルのナビゲート：管理者vsユーザーとエージェントのインストール：概要とキーも参照してください。

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。

2. `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）。



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。

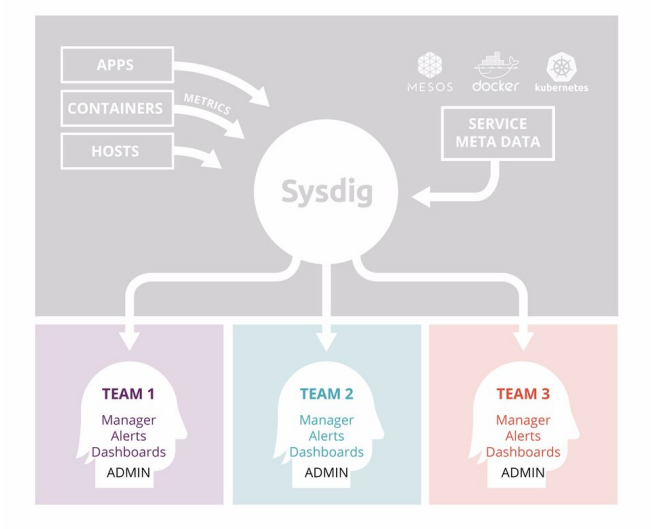
Sysdigチームについて

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。

システムの役割	チームの役割
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-Admin (Sysdig Monitor)	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+チームメンバーを追加/削除したり、チームメンバーの権限を変更したりできます。 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。	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。	エクスプローラページにアクセスできない上級ユーザーに相当します（たとえば、監視情報に興味がない開発者向け）。	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

	Team Manager (Secure)	Advanced User (Secure)	Standard User (Secure)	View Only (Secure)
Non-Admin (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。 上級ユーザーはユーザーを管理できません。	コンテナーイメージをスキャンキューにプッシュし、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。	チームスコープ内のすべてのセキュア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。

詳細については、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。）

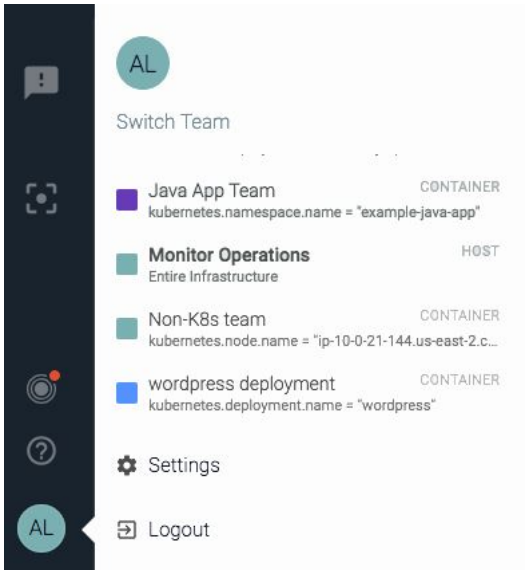
UIでのチームの切り替え

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。

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。

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、「ユーザーとチームの管理」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バーであるため、デフォルトでは除外されます。

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。

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

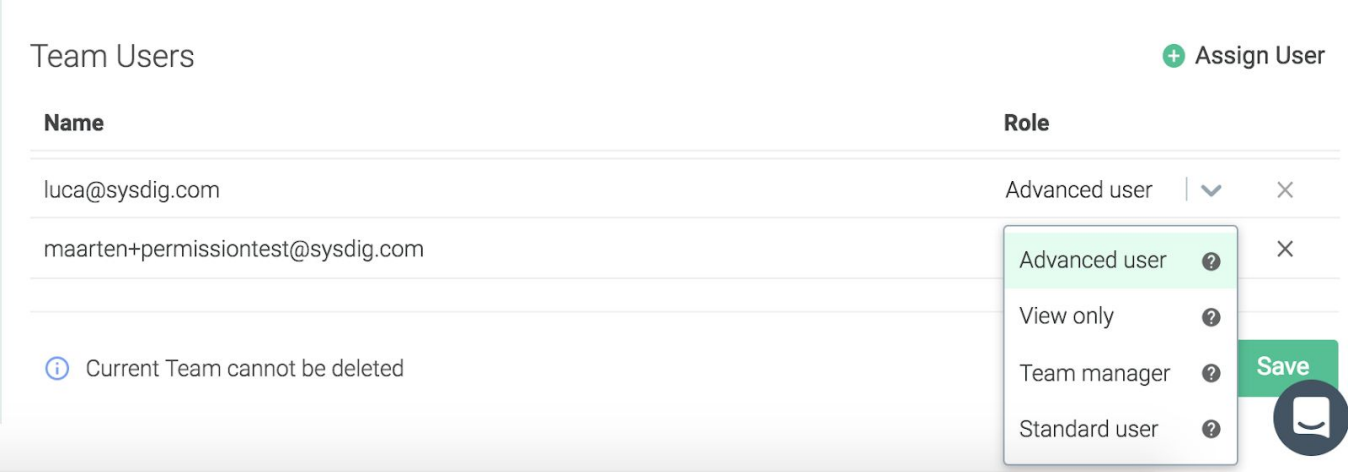
ユーザーは複数のチームに割り当てることができます。チームの割り当ては、[User]ページではなく[Team]ページから行い、管理者またはチームマネージャーが行う必要があります。

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。



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. `Save`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、チームベースの役割と権限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。

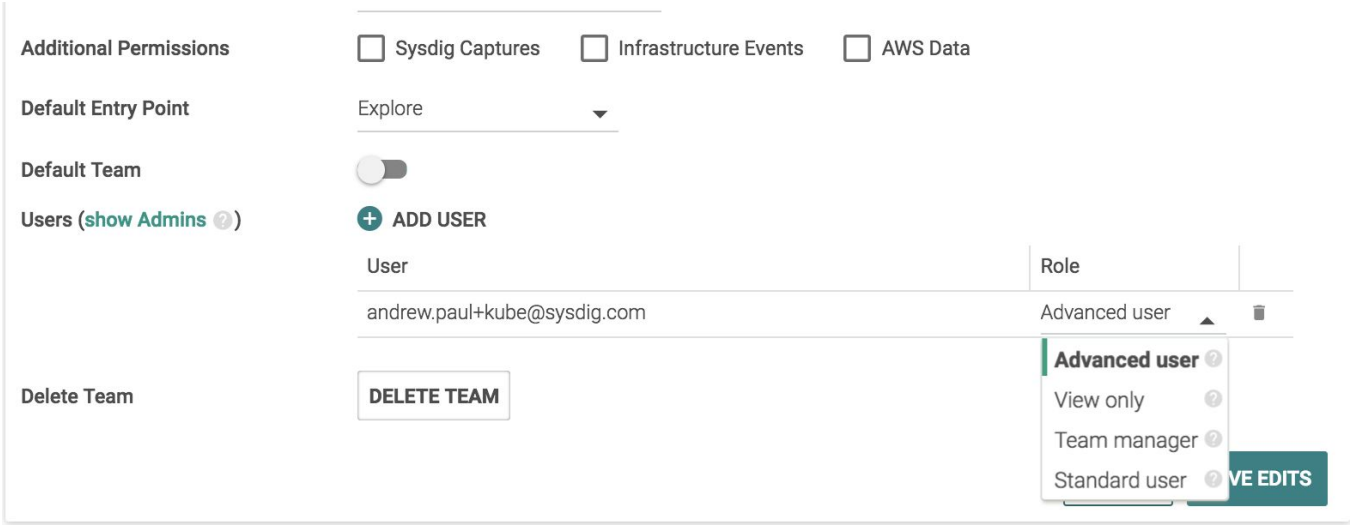
マネージャーは、チームのメンバーを追加または削除したり、メンバーの権限を編集、読み取り、マネージャー間で切り替えたりできます。

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。



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。
4. 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。
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. [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

アラートは、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。

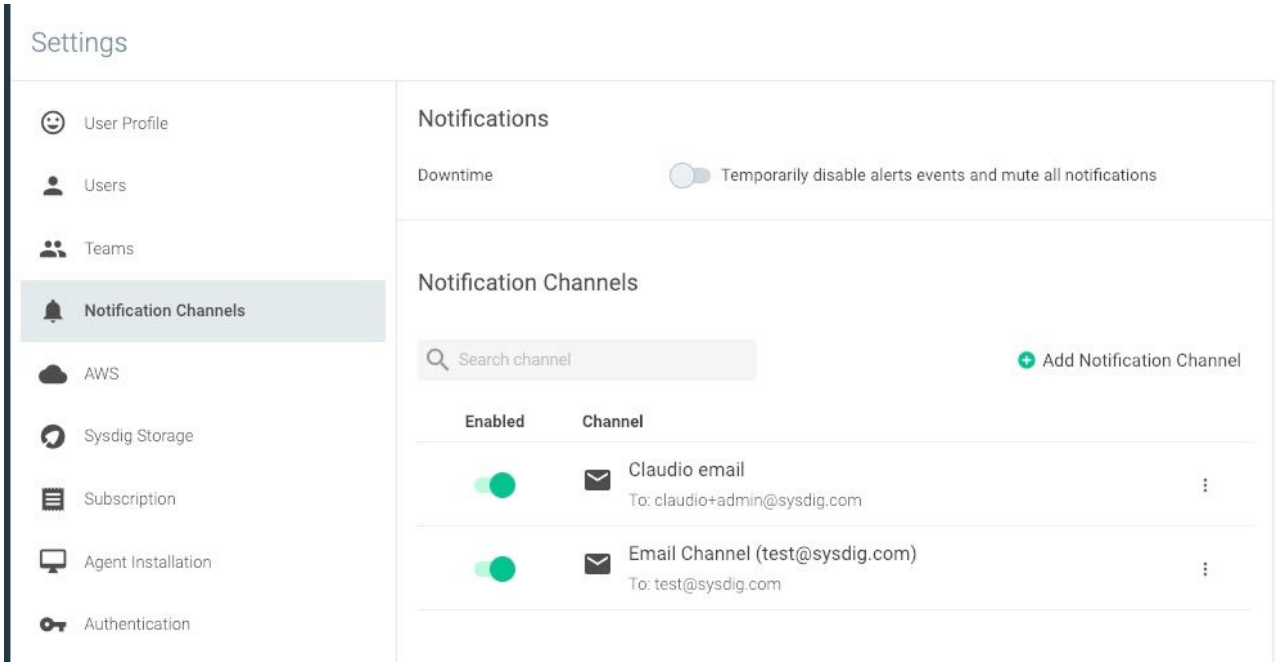
通知管理では、さまざまな通知チャネルタイプを追加、編集、または削除する方法と、スケジュールされたダウンタイム中など、通知が不要な場合に通知を無効または削除する方法について説明します

通知チャネルを追加する

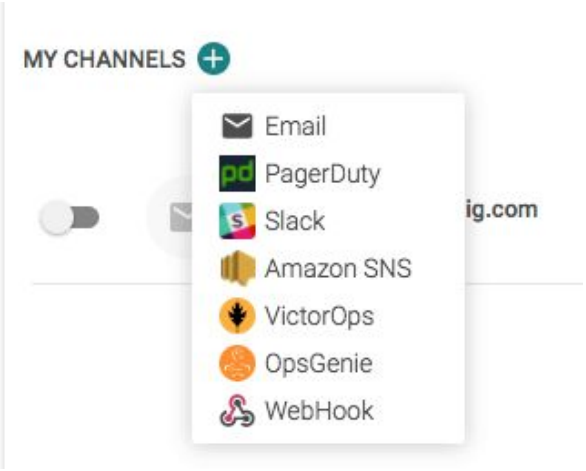
新しい通知チャネルを追加するには：

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。



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。

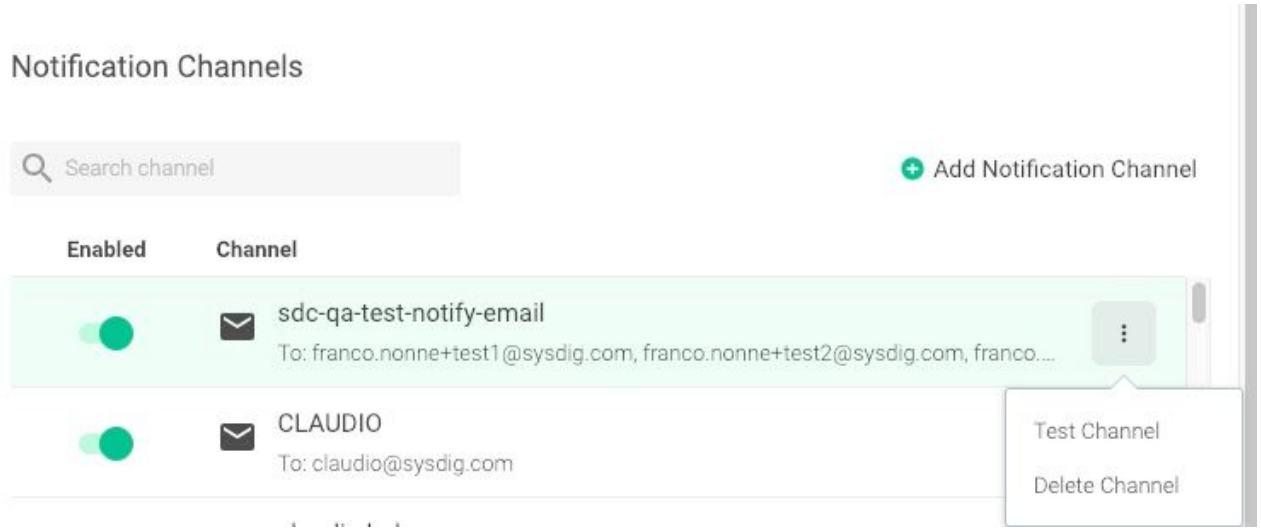
2. `Notification Channels`を選択します。
3. ターゲットチャネルを見つけて、[`Edit`]ボタンをクリックします。
4. 編集を行い、[`Done Editing`]をクリックして変更を保存します。

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。
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。



4.

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：

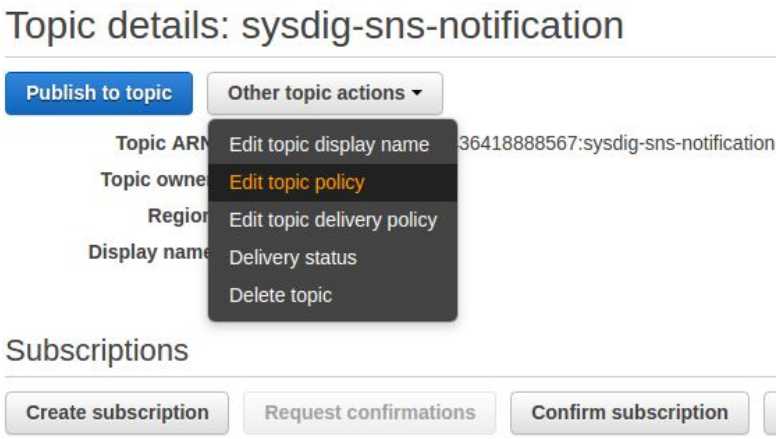
1. Sysdig Monitorアラートを選択したSNSトピックに自動的にプッシュするには：
2. AWSコンソールから、SNS管理コンソールを開きます
3. 新しいトピックを作成する（必要な場合）
4. リストからトピックを選択します
5. 上部の[すべてのトピックアクション]メニューから、[トピックポリシーの表示/編集]を開きます
6. [**Publishers**]セクションで、[これらのAWSユーザーのみ]を選択し、Sysdig MonitorアカウントIDを入力します：ex) 273107874544
7. トピックの詳細ページから、トピックARNをコピーしてここに貼り付けます

   AWS SNS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。

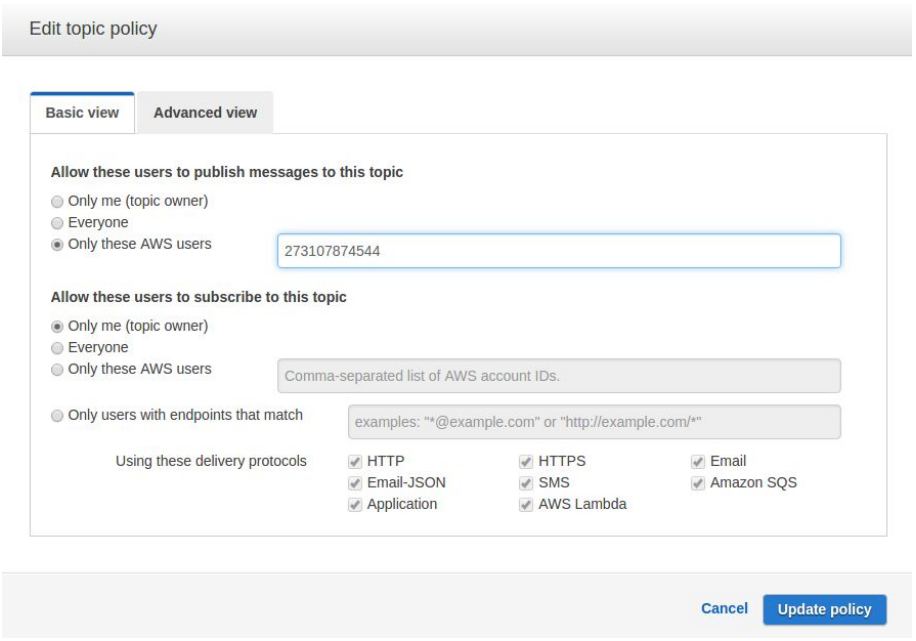
   SNS通知の場合、「ヘルプ」ボタンをクリックして、SNSトピックの設定に関するヒントを表示できます。

   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。

1. 「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。

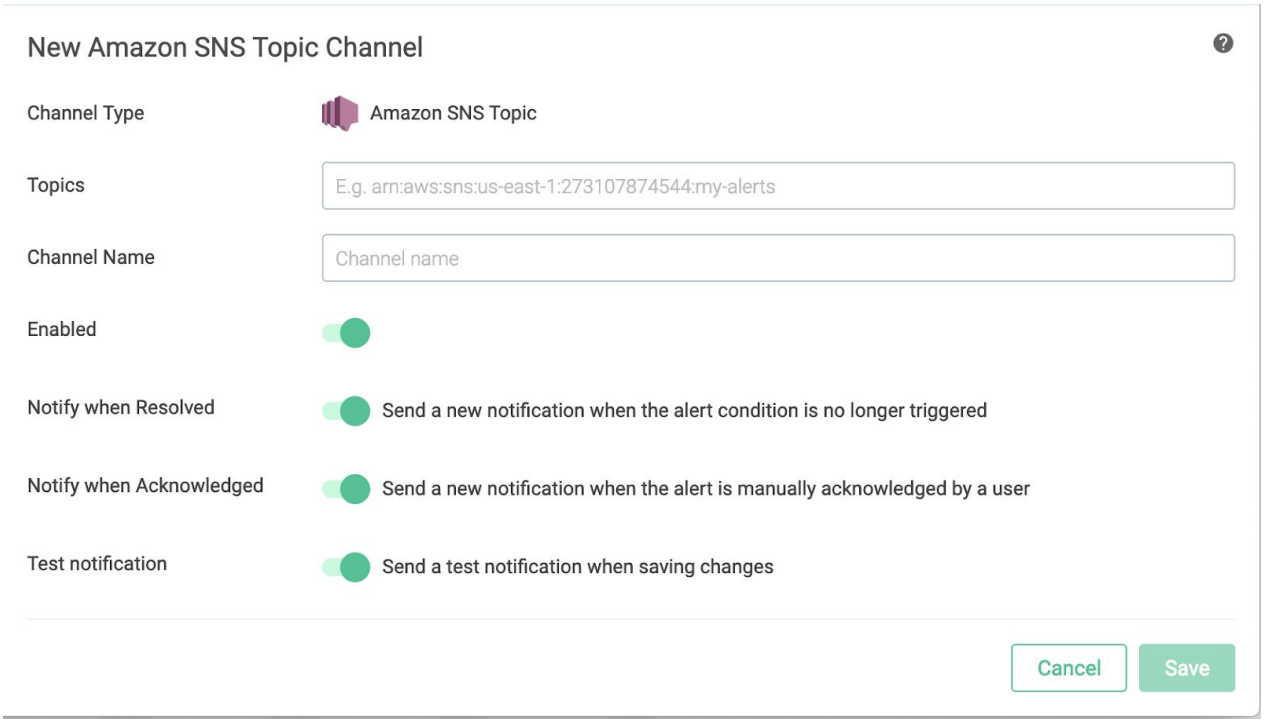


2. [トピックポリシーの編集]ダイアログの[基本ビュー]タブで、発行元のリストから[これらのAWSユーザーのみ]を選択し、Sysdig IDを入力します。



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。



2. 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. `Save`をクリックします。

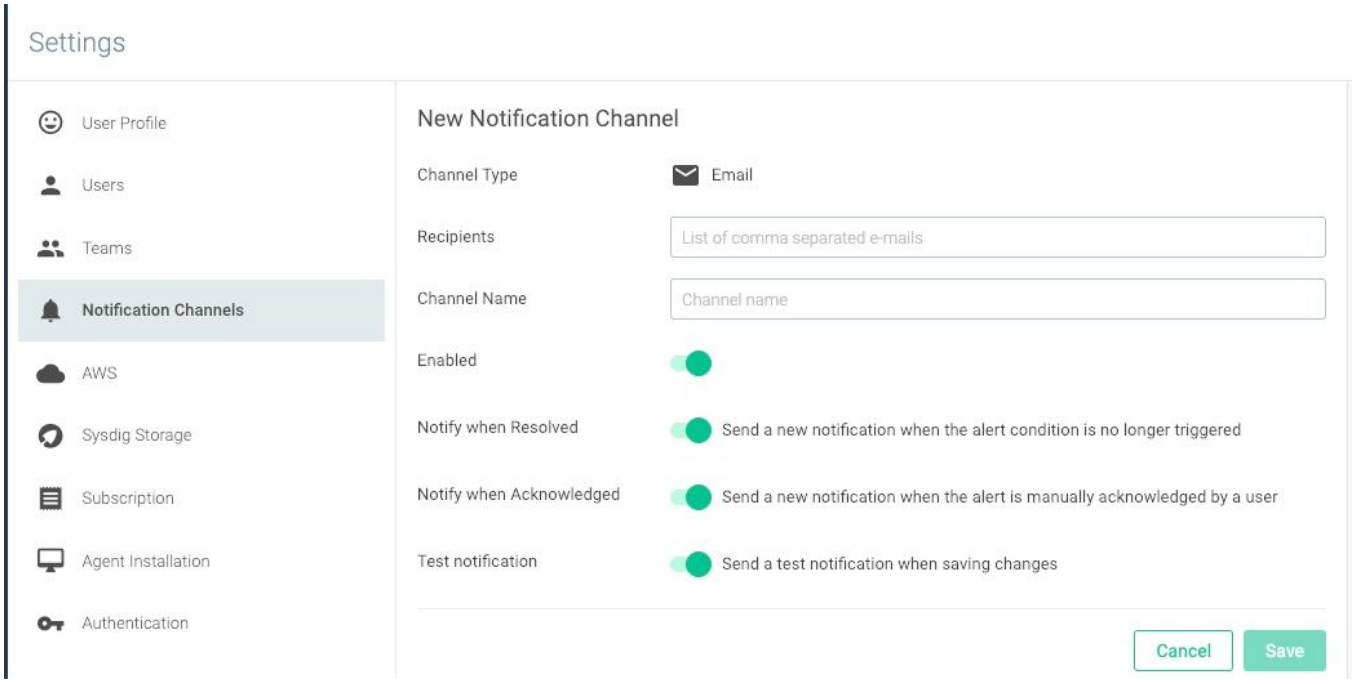
メール通知

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。



3. `Save`をクリックします。

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。

注意

オンプレミス環境の場合、RepricatedまたはKubernetesインストール configmapでSMTPパラメーターを事前に構成しておく必要がある場合があります。

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。

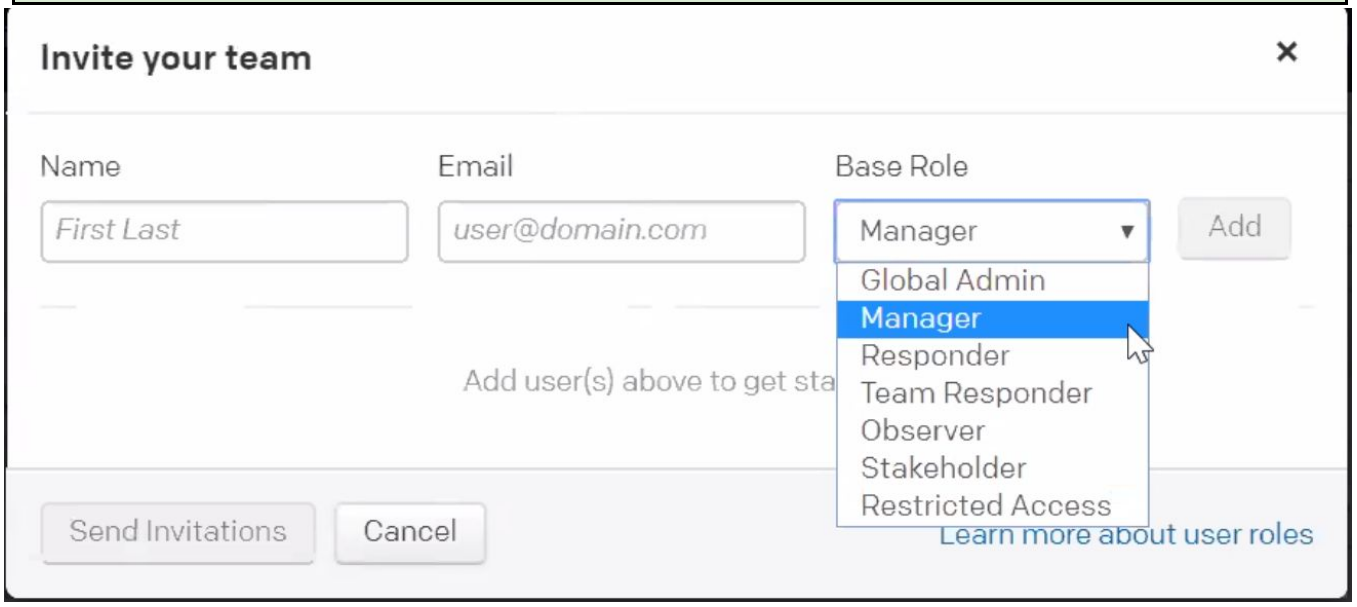
前提条件

- 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 UIに必要なデータを手動で入力できます。

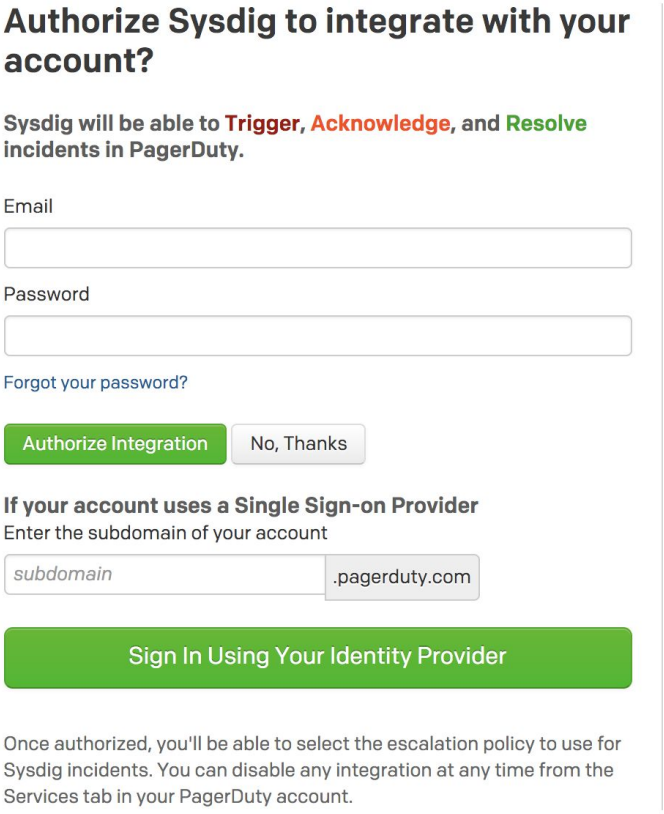


PagerDuty UIの基本ユーザーロール

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。



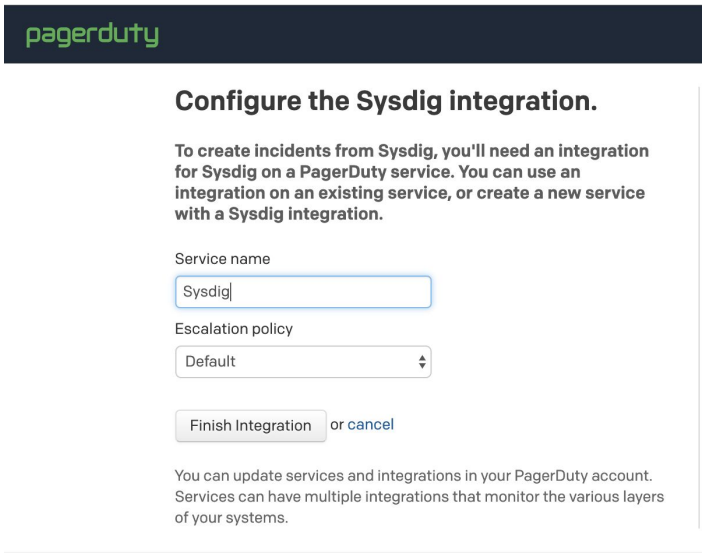
3. PagerDutyアカウントに関連付けられているメールアドレスとパスワードを入力し、[`Authorize Integration`]をクリックします。

   または

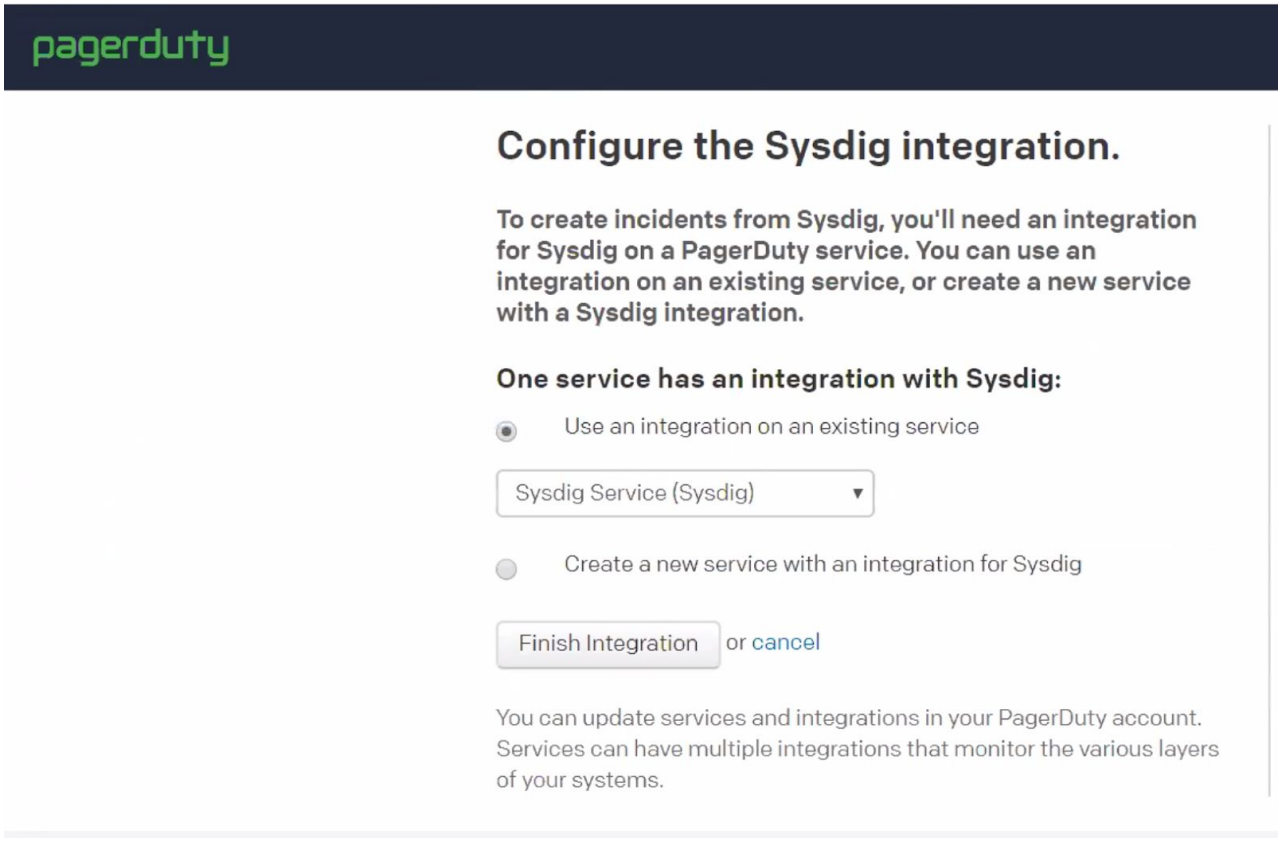
   シングルサインオンとサインインに適切なPagerDutyサブドメインを入力します。

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。

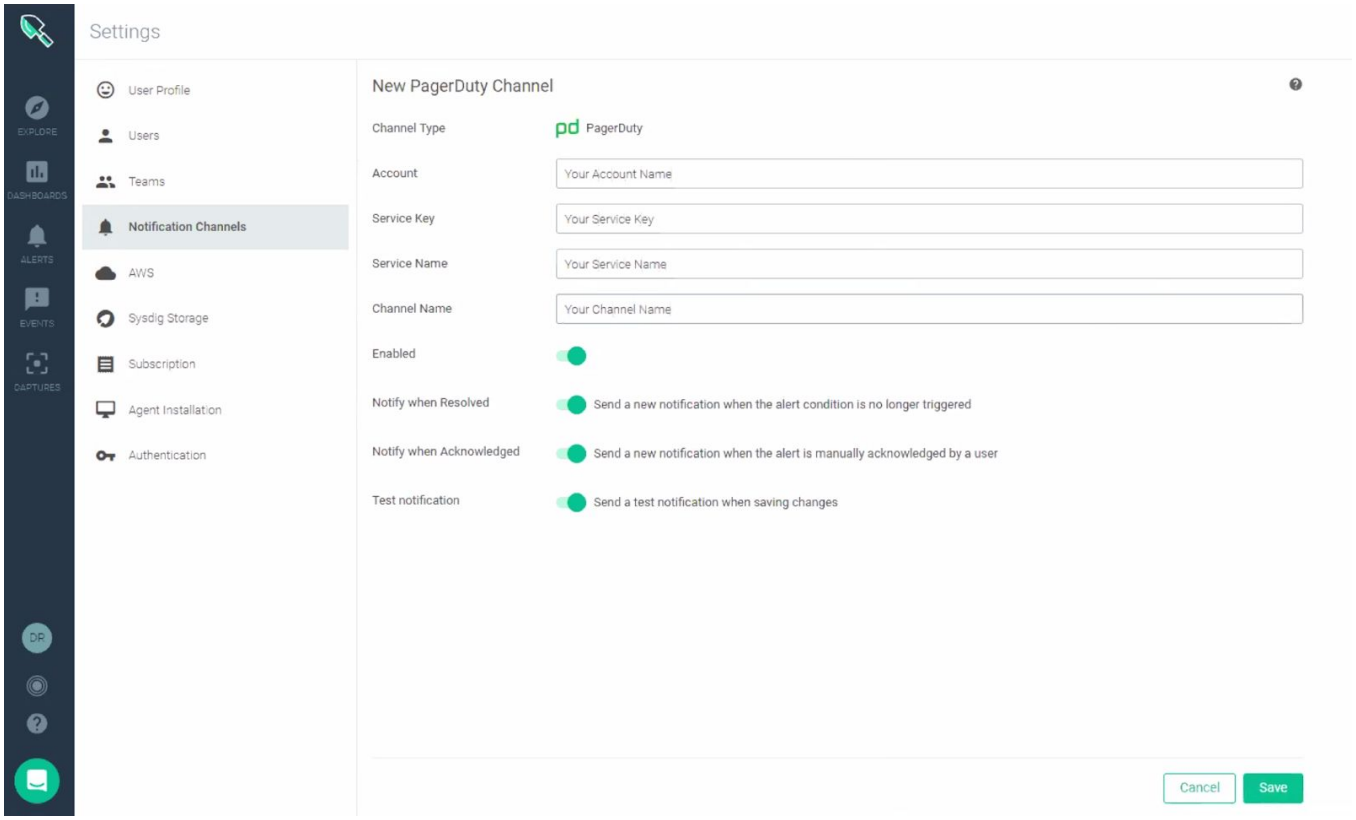


オプション2：少なくとも1つのサービスがすでに統合されている場合は、そのサービスを選択するか、別のサービスを作成できます。



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。



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：

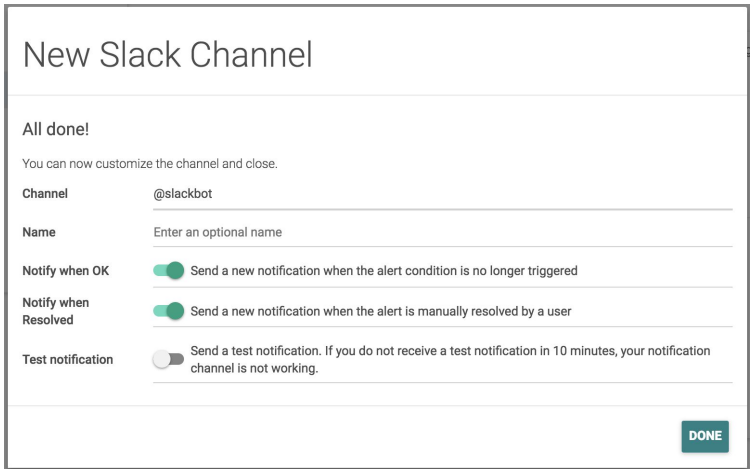
Slack.comでSlackアカウントを構成し、通知に使用する通知チャネルを確認します。

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、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。



4. [**Test**]をクリックして、新しい機能を確認します。

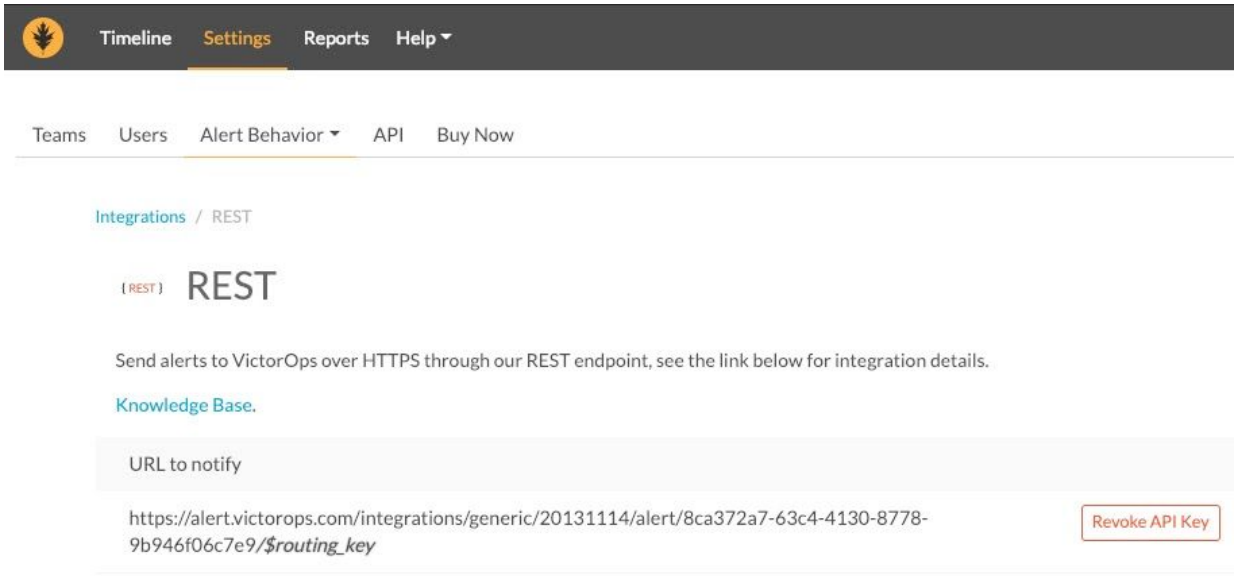
Slack通知を使用するようにアラートを構成できるようになりました。

VictorOps通知

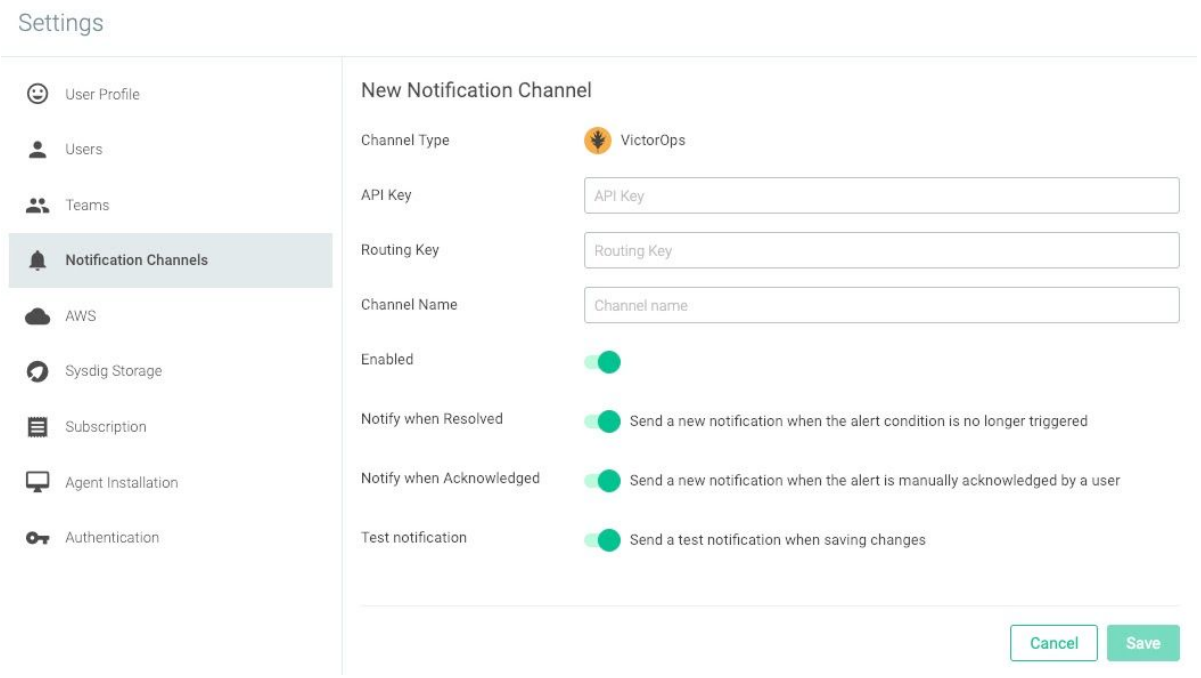
VictorOpsと統合するには

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。



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。

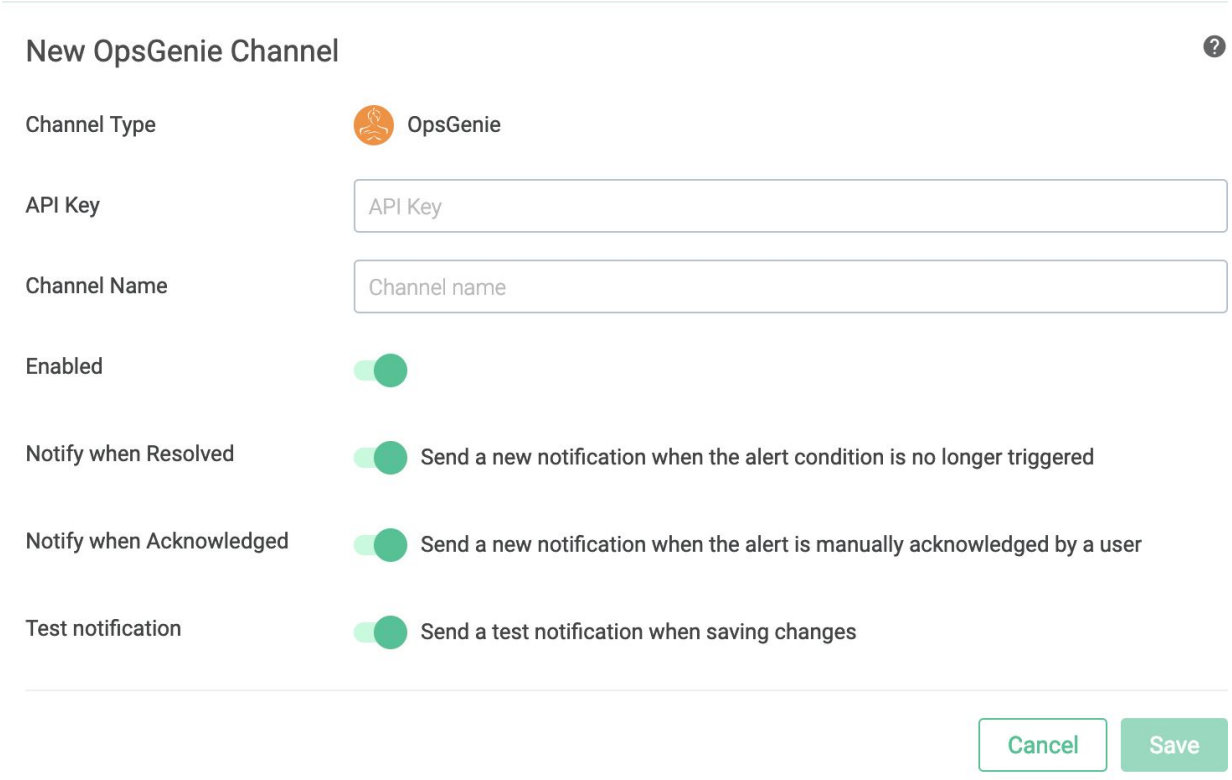
6. `Save`をクリックします。

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ここに保持しています。

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。



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

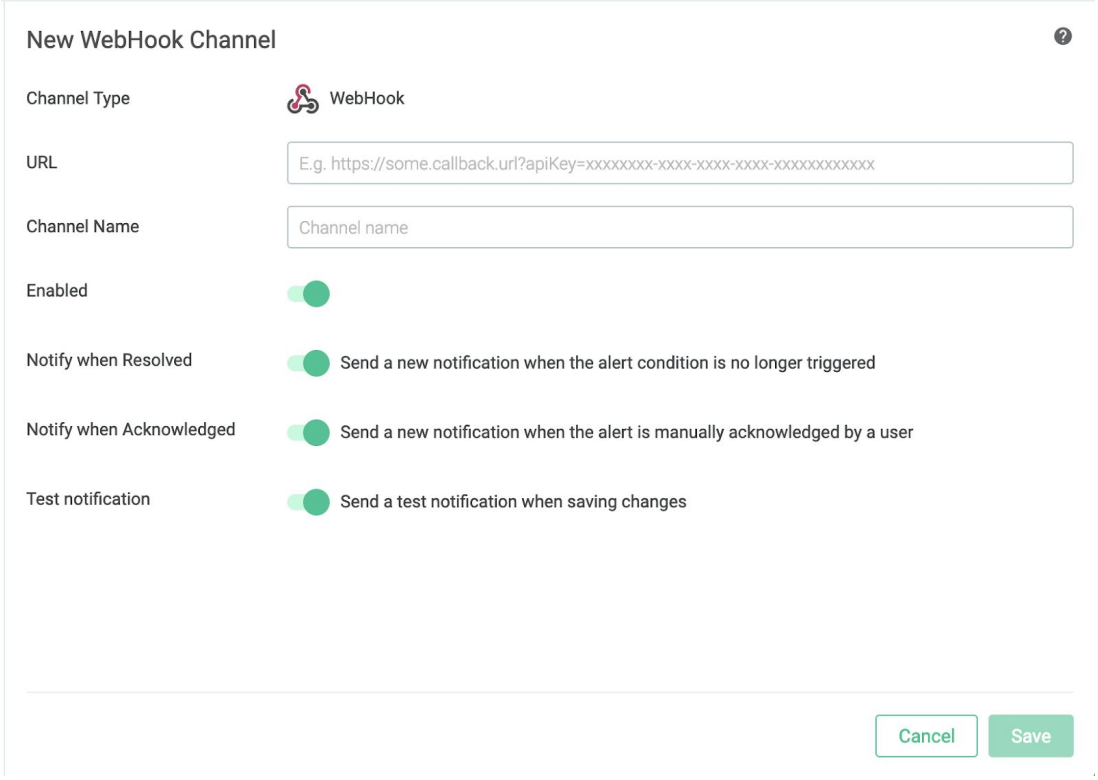
Sysdig MonitorとSysdig Secureは、Sysdigがネイティブに統合されていない宛先（Webサイト、カスタムアプリケーションなど）にアラート通知を送信することをサポートしています。これを行うには、カスタムWebhookチャネルを使用します。

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。



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": 60000000,
 "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 dc1a42cc-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 dc1a42cc-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/6dtwzz7l","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。

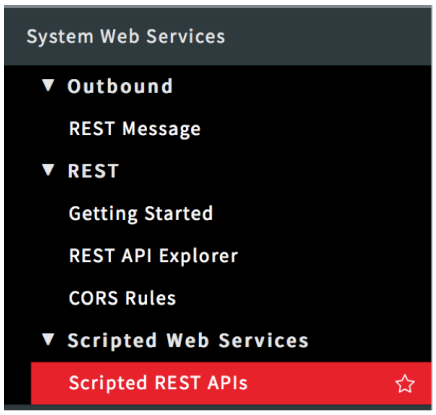
ServiceNowSetup

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。

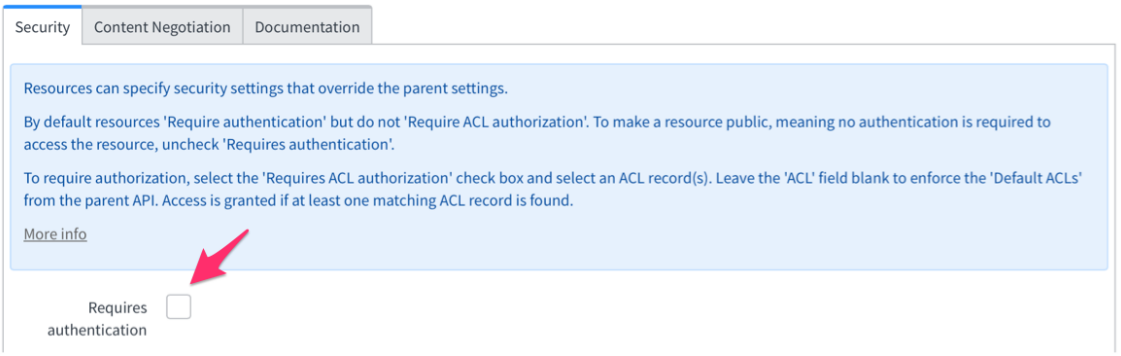
   名前：SysdigAlert API ID：sysdigalert

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.

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。



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、Scripted REST Request APIおよびScripted REST Response API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。

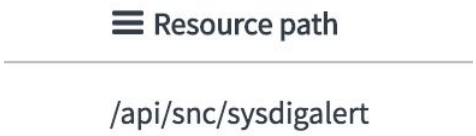
```
(function process(/*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {

  gs.info(request.body.dataString);

})(request, response);
```

2. 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。



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。

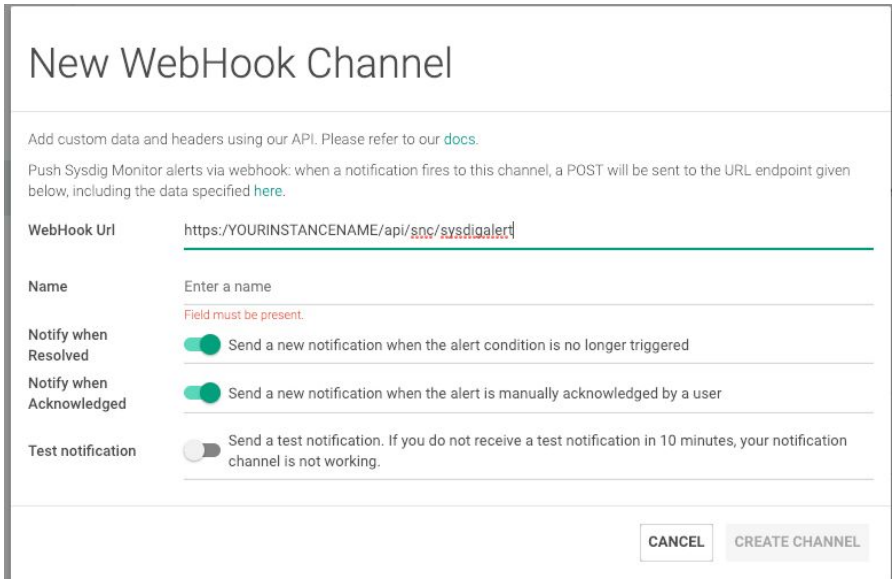
API URL：インスタンス名URL

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

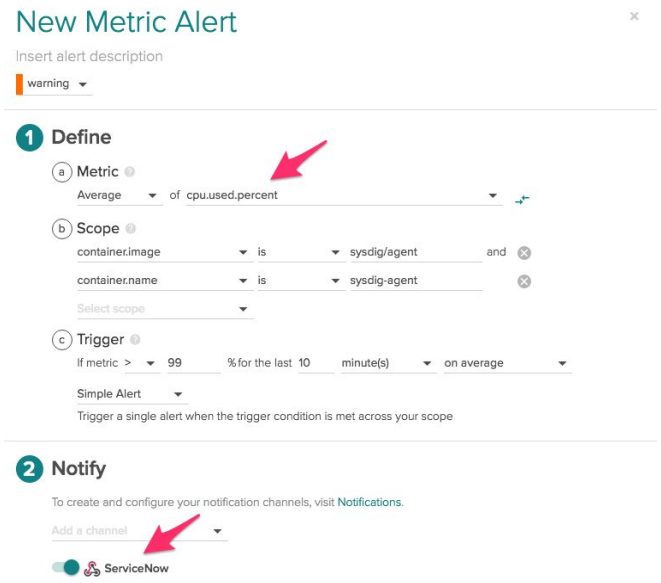
Notify when Resolved：オプション

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。



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：



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。

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

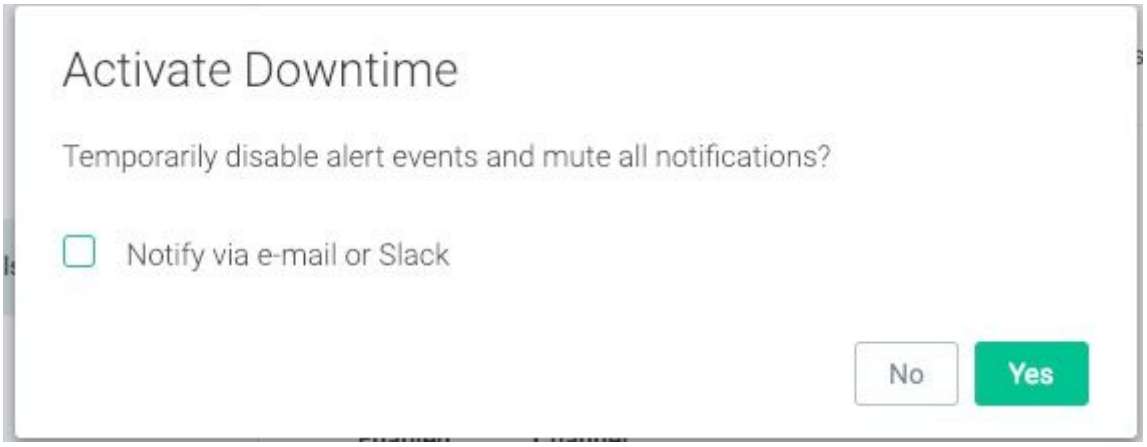
ことを特定のチャネルに通知するかどうかを選択できます。通知のミュートと再有効化は手動のプロセスです。

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。

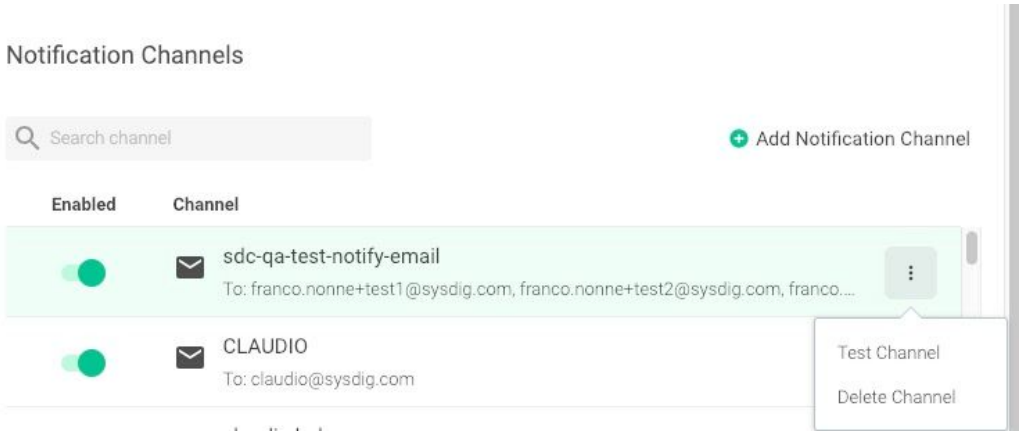
    オプション：プロンプトが表示されたら「**`Yes`**」ボックスをオンにしてチャネルに通知し、目的のチャネルを選択します。

    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。



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。



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

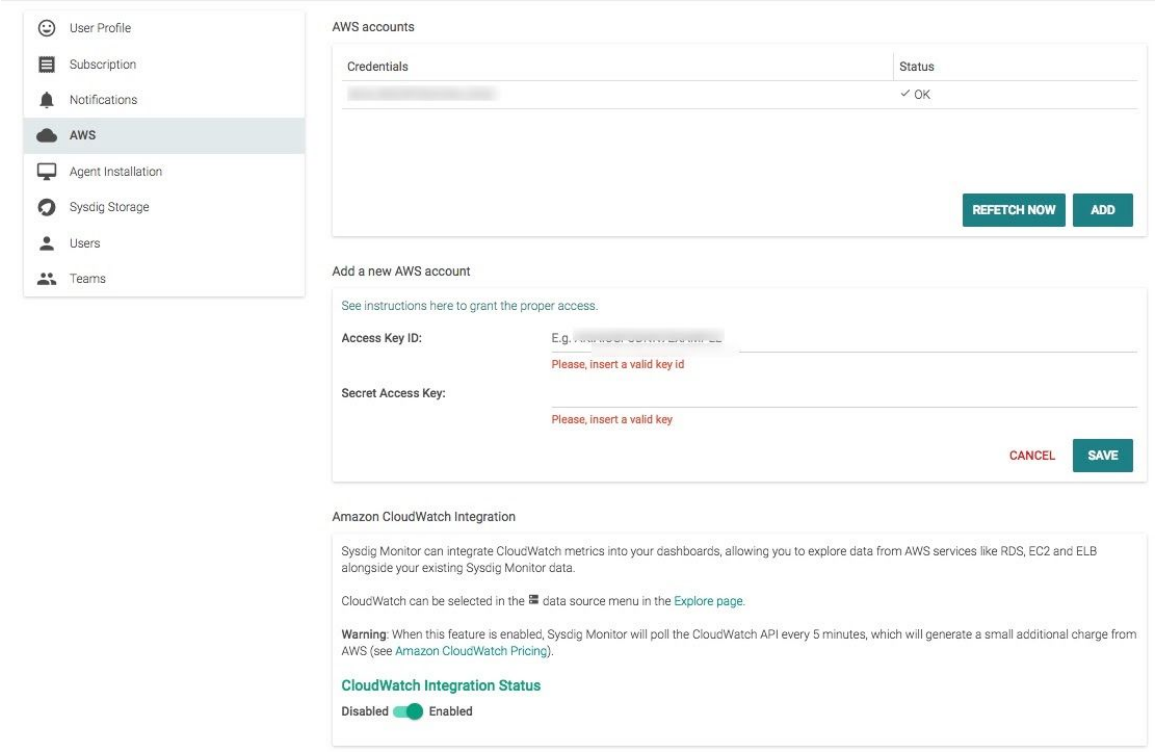
implicit keyを使用する場合は、ウィザードのこのページをスキップする必要があります。詳細については、Implicit Key Optionを参照してください。

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。



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

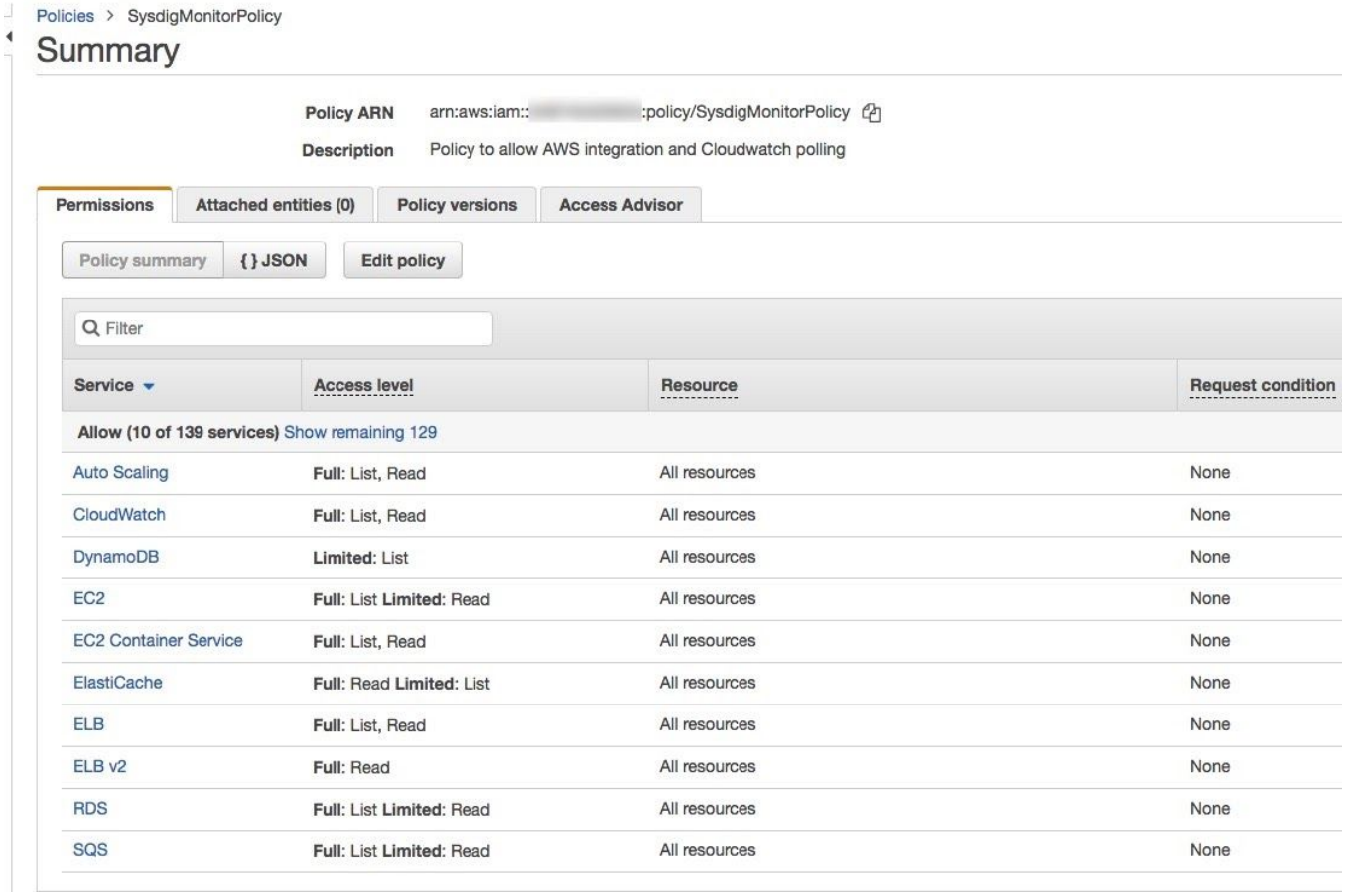
Sysdigアクセス用のIAMポリシーを作成する

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。

1. 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。）
2. 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。



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

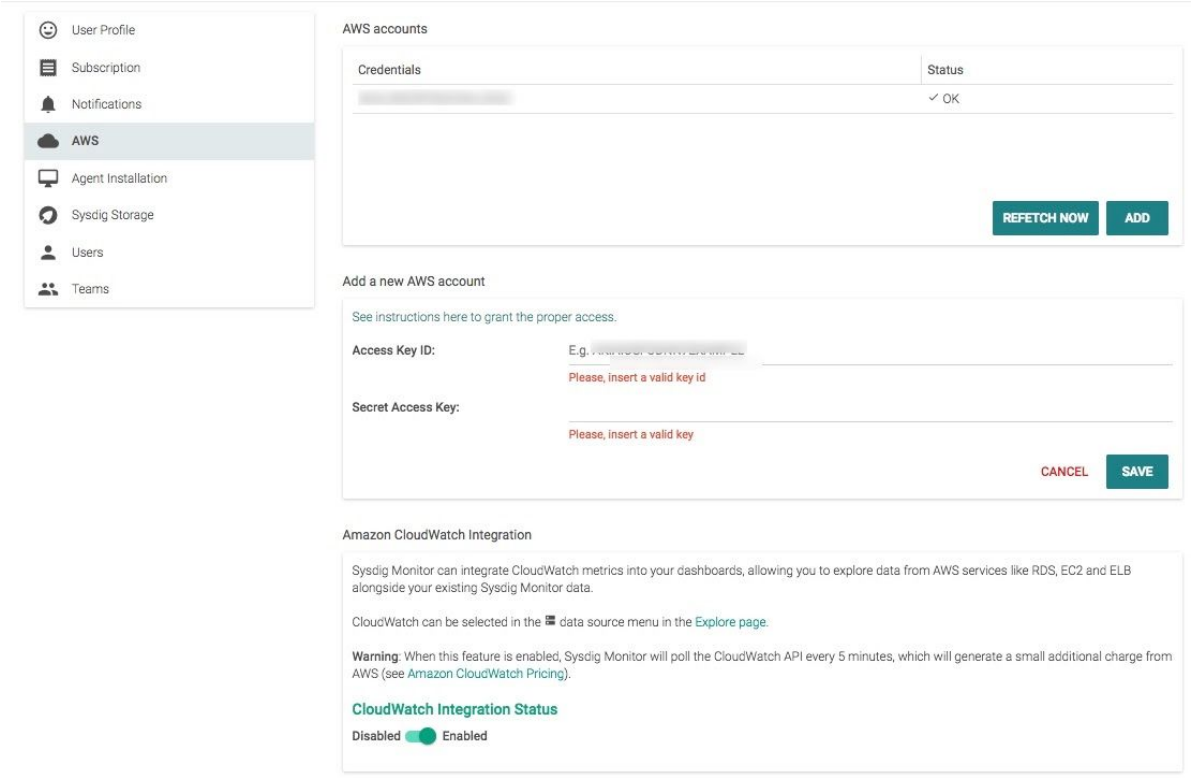
既存のIAMユーザーを使用するか、または（ベストプラクティス）Sysdigバックエンドがプログラムで CloudWatchにアクセスしてそのデータを使用するための特定のIAMユーザーを作成します。

1. IAMコンソールで、ユーザーを追加します。
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。
5. 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。



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:
```

```
sysdigcloud.jvm.api.options: "-Ddraios.providers.aws.implicitProvider=true"
sysdigcloud.jvm.worker.options: "-Ddraios.providers.aws.implicitProvider=true"
sysdigcloud.jvm.collector.options: "-Ddraios.providers.aws.implicitProvider=true"
# JVM GC options for the collectors
sysdigcloud.jvmgc.collector.options: "-XX:+PrintFlagsFinal -Xverify:none -XX:+UseG1GC -XX:MaxGCPauseMillis=
# Required: Sysdig Cloud license
sysdigcloud.license: ""
# Optional: OAuth allowed domains (comma separated list of domains)
sysdigcloud.oauth.allowed.domains.list: ""
# Optional: Sysdig Cloud Google OAuth Client ID
sysdigcloud.google.oauth.client.id: ""
# Optional: Sysdig Cloud Google OAuth Client Secret
sysdigcloud.google.oauth.client.secret: ""
###################################
# ======= BEGIN DEPRECATED LDAP 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。

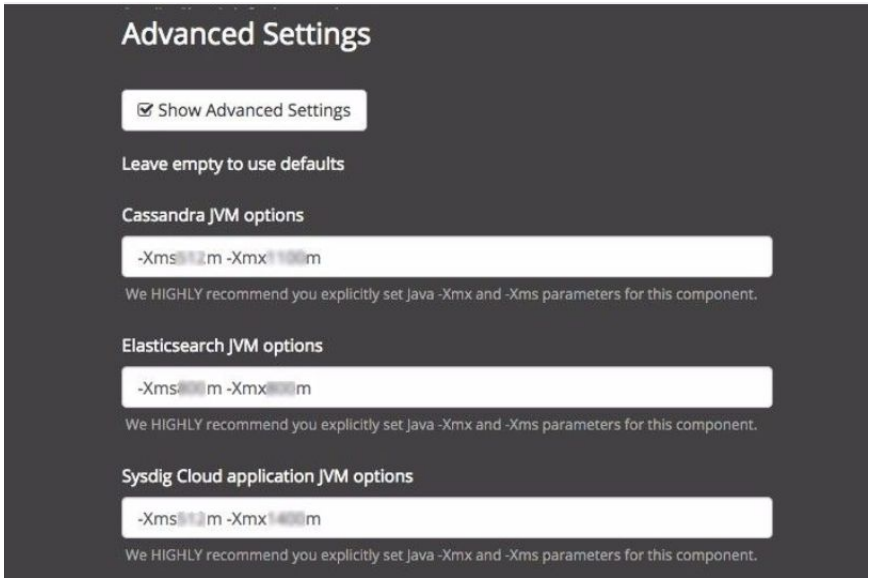
   詳細については、設定を変更するを参照してください。

3. Sysdig UIでCloudwatch統合を有効にします。

Replicated

1. 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。



Replicated詳細設定も参照してください。

2. 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AWS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、「AWSサービスのライセンス」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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "autoscaling:Describe*",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*",
                "dynamodb:ListTables",
                                "dynamodb:Describe*",
                "ec2:Describe*",
                "ecs:Describe*",
                "ecs:List*",
                "elasticache:DescribeCacheClusters",
                "elasticache:ListTagsForResource",
                "elasticloadbalancing:Describe*",
                "rds:Describe*",
                "rds:ListTagsForResource",
                "sqs:ListQueues",
                "sqs:GetQueueAttributes",
                "sqs:ReceiveMessage"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

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

- External IDを取得します。
- 役割の委任を設定します。
- ロールARNを取得します。
- AWSアカウントを追加します。

オンプレミスの手順

- External IDを取得します。
- 役割の委任を設定します。
- ロールARNを取得します。
- AWSアカウントを追加します。
- 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。

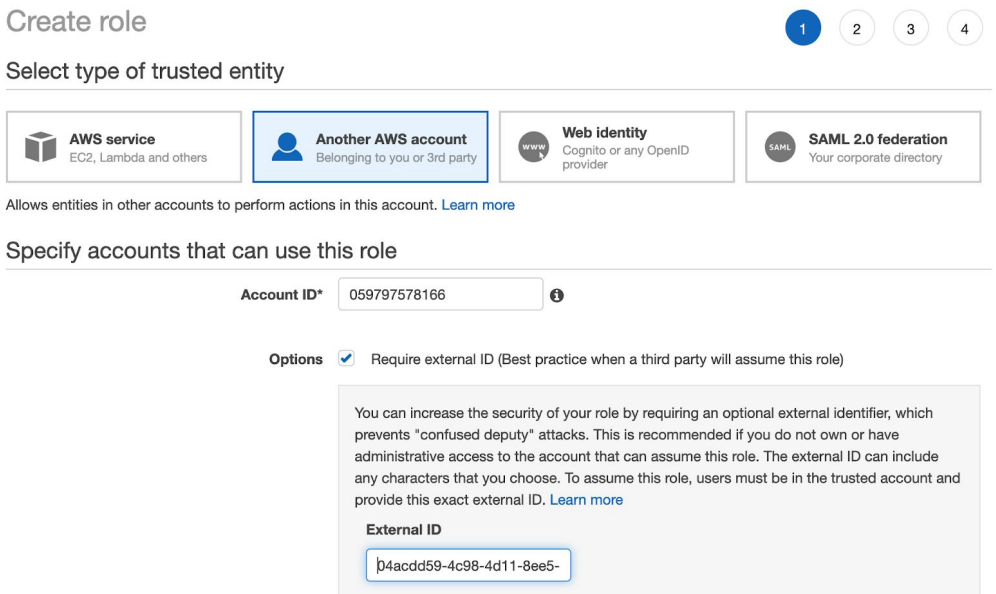
```
curl -k --request GET \ --url {{host}}/api/users/me \ --header 'authorization: Bearer e71d7c0f-501e-47d4-a159-39da8b716f44' | jq '.[] | .customer | .externalId'
```

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。



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、使用するIAMポリシーコード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、「AWSアカウントを手動で統合する」を参照してください。

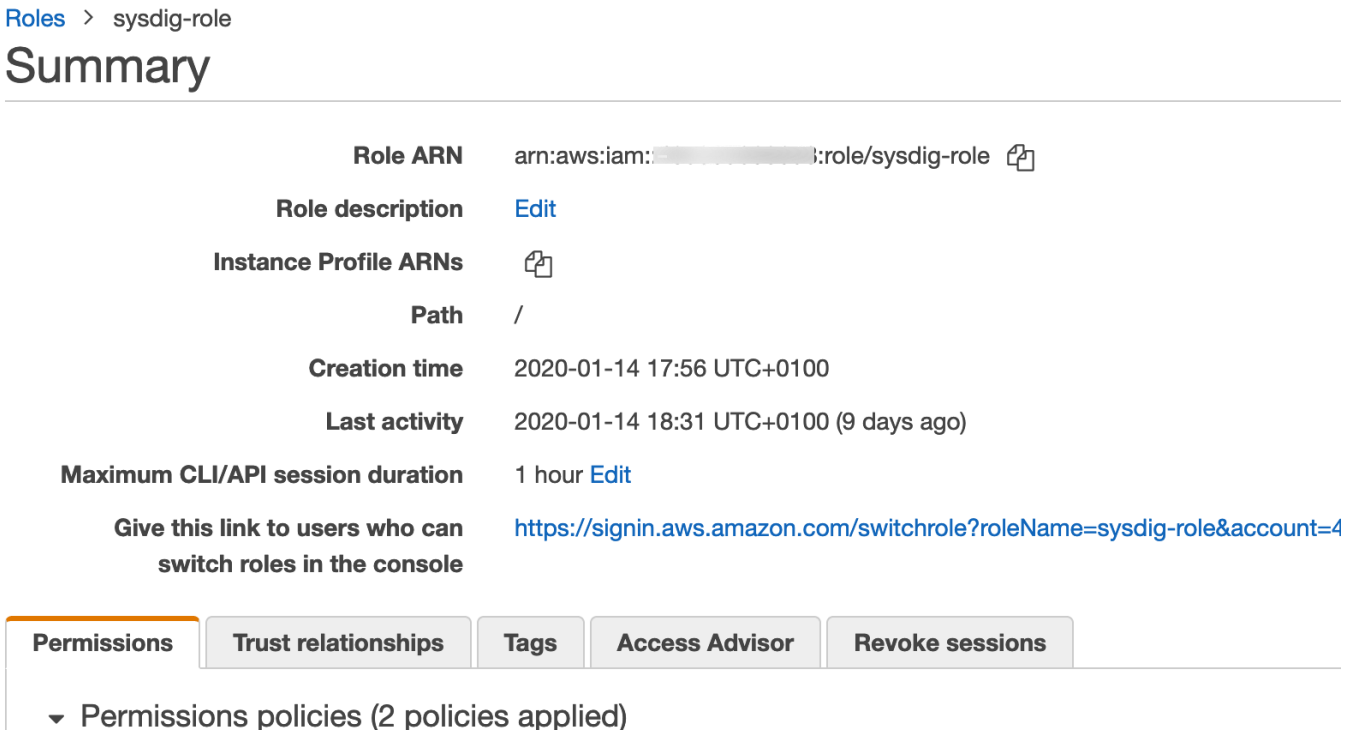
a. ポリシーがすでに作成されている場合は、このページでポリシーを検索して選択し、手順にスキップしてください。それ以外の場合は、[Create Policy]をクリックすると、新しいウィンドウが開きます。
b. [ポリシーの確認]をクリックします。
c. ポリシーに名前を付け、適切な説明を入力します。たとえば、sysdig_cloudwatch。
d. 「ポリシーの作成」をクリックします。

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。



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、AWS：AWSアカウントとCloudWatchメトリクススの統合（オプション）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}}
```

2. 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。
- AWS：AWSアカウントとCloudWatchメトリクススの統合（オプション）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

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。

3. `Use a custom S3 bucket`を有効にして、AWS S3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、MinioやIBM Cloud Object Storage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、IBM CloudのAWS CLI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/
```

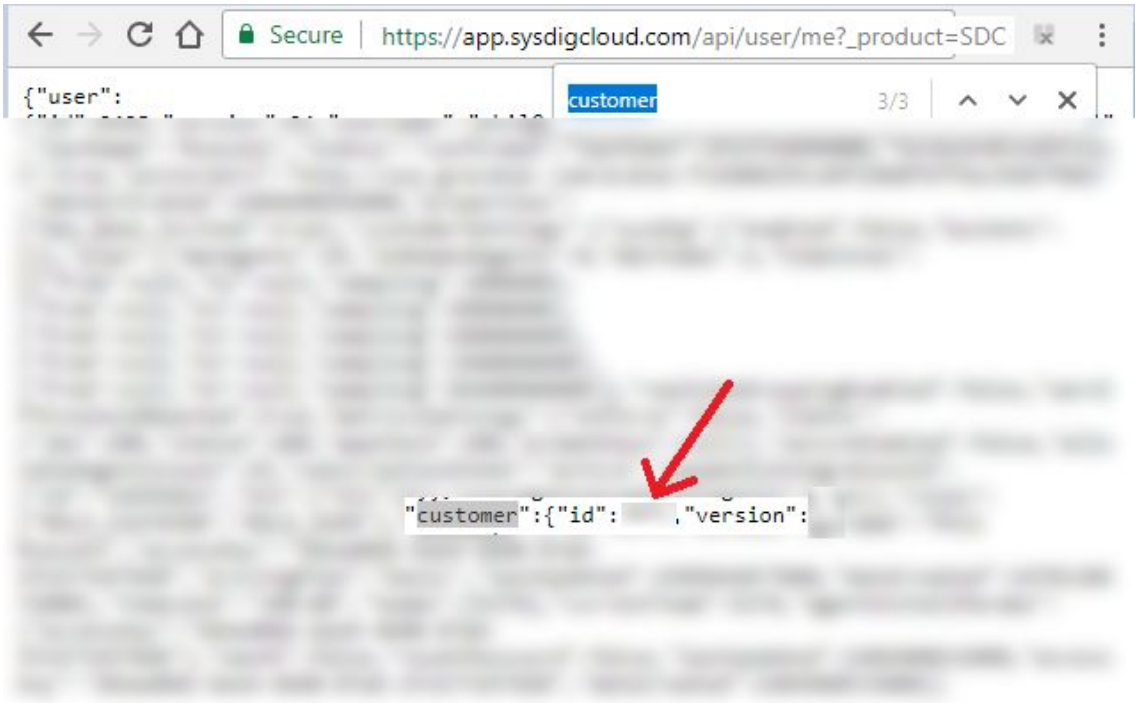
この例では、エンドポイントはhttp://10.101.140.1:9000/であり、バケットの名前はtestです。

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。

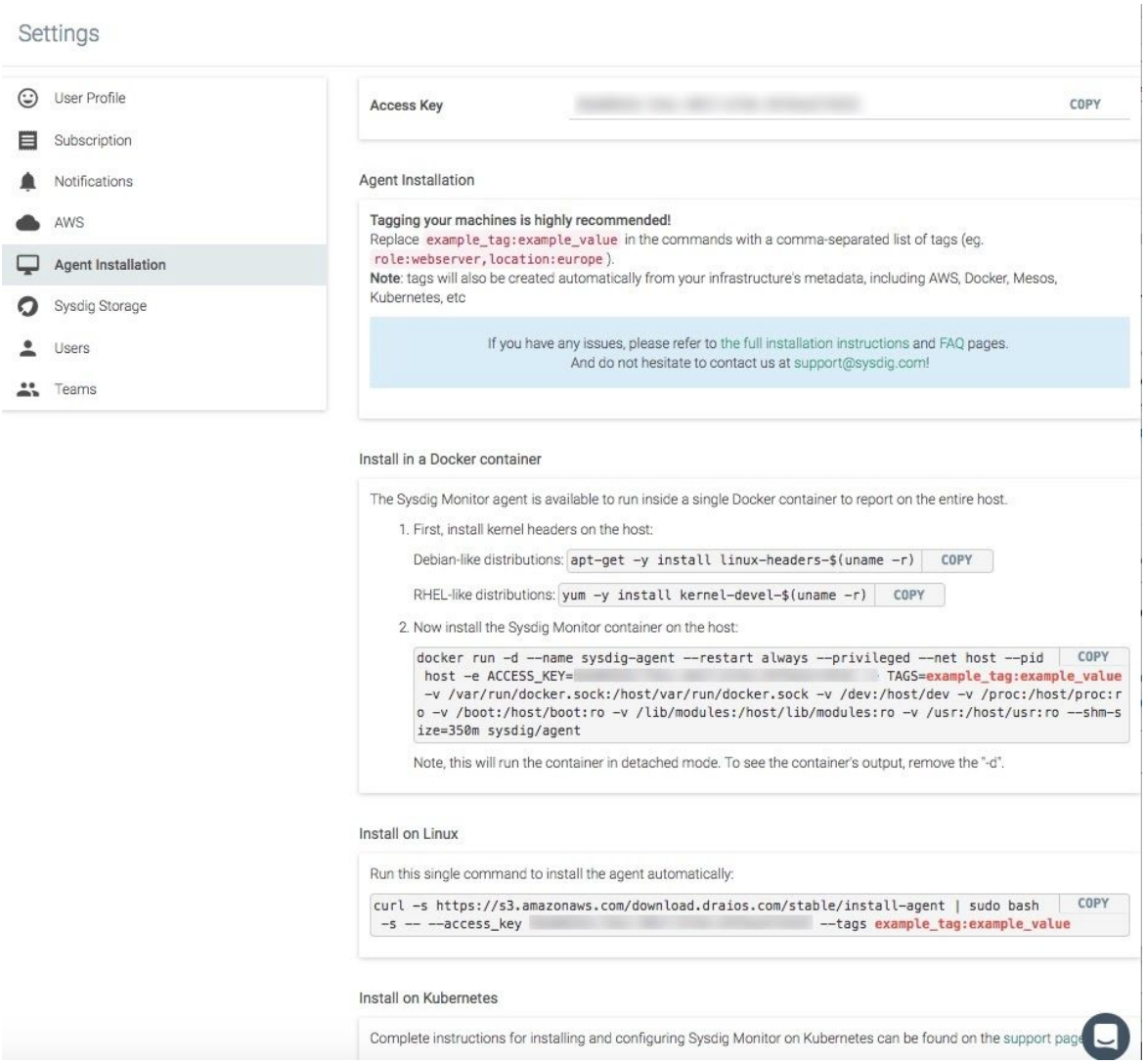
エージェントアクセスキーを取得する

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。



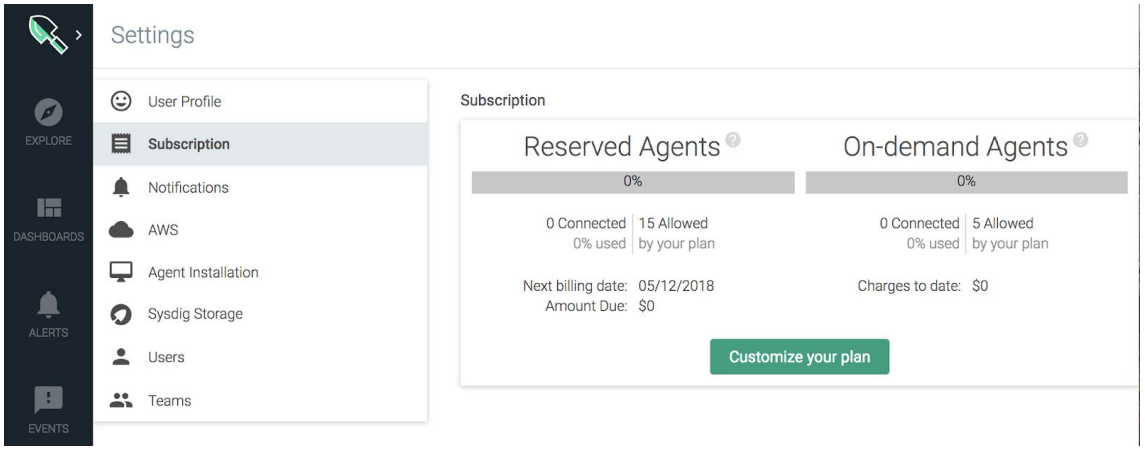
サブスクリプション：ライセンスされたエージェントの数の変更

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。

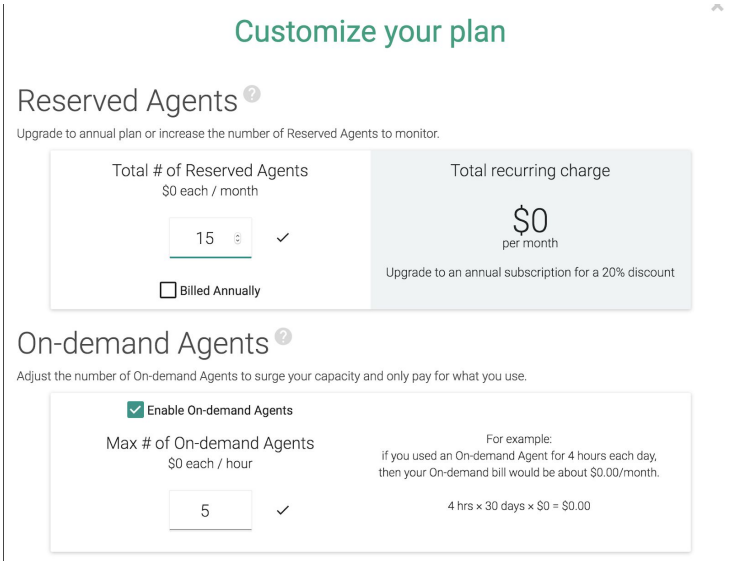
エージェントサブスクリプションプランを表示または変更するには：

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。



3. 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。

必要に応じて調整し、[**Checkout**]をクリックします。



以下も参照してください。

- ライセンスの仕組み
- AWSサービスのライセンス

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。

1. 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。
2. 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。

ライセンスの仕組みもご覧ください。

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。

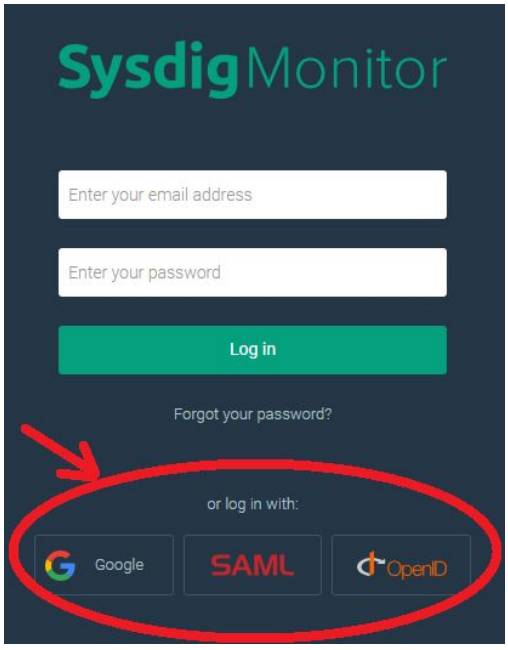
AWSサービスビューの項目の制限を増やすには、Sysdigセールスに連絡して、ライセンス契約に応じて追加のリソースを有効にします。「サブスクリプション：ライセンスされたエージェントの数の変更」も参照してください。

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[IDプロバイダー（IdP）サービス]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。

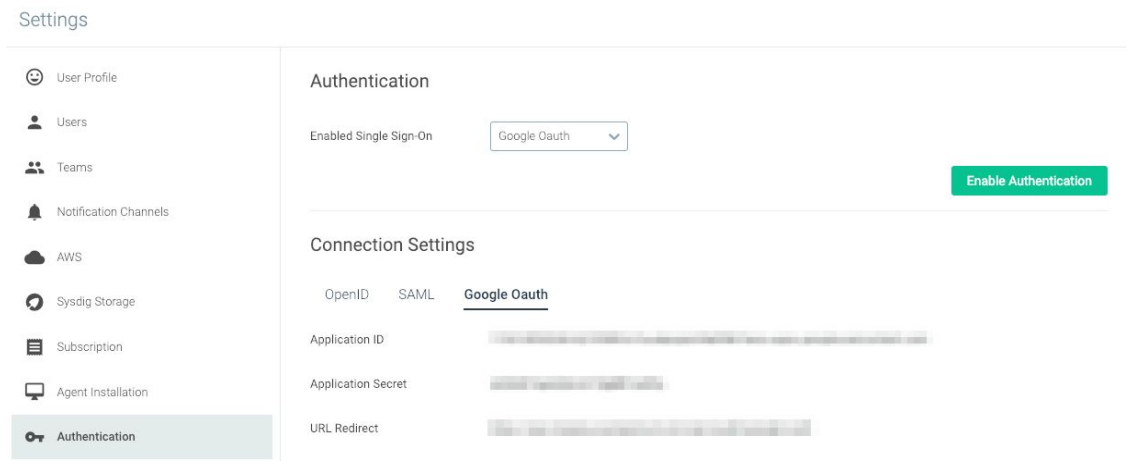
注意

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。

1. 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。
4. [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。



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。

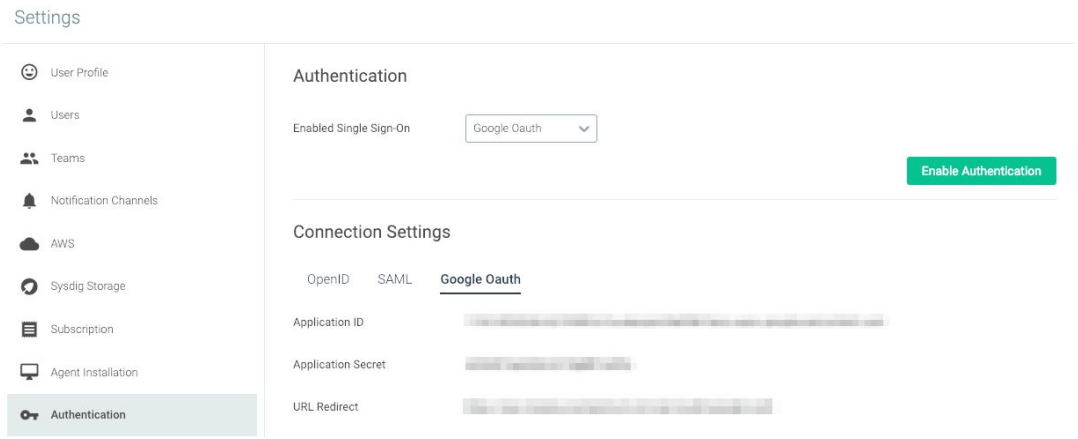
Google OAuthを有効にする

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。）



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

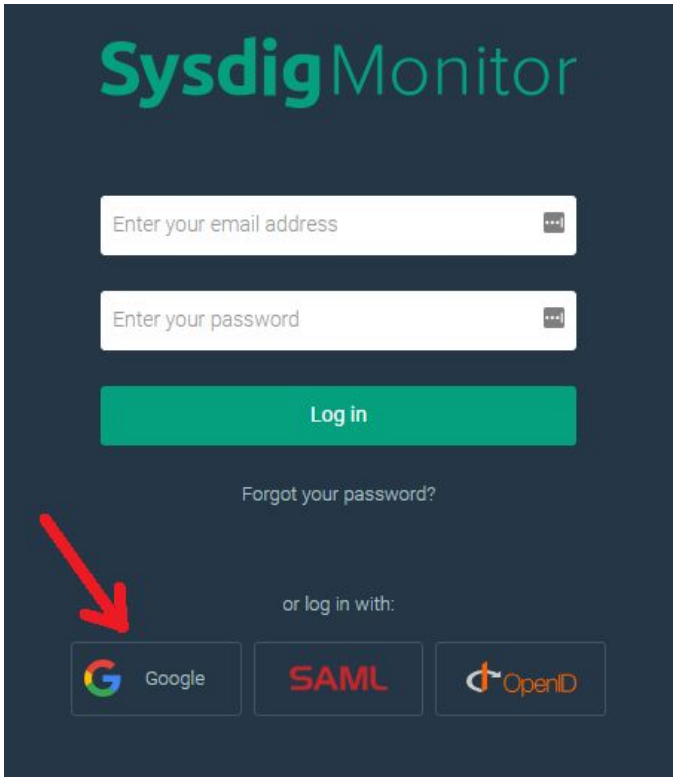
Google OAuthログインを成功させるには、次の要件に注意してください。

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。



注意

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、ユーザーとチームの管理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。

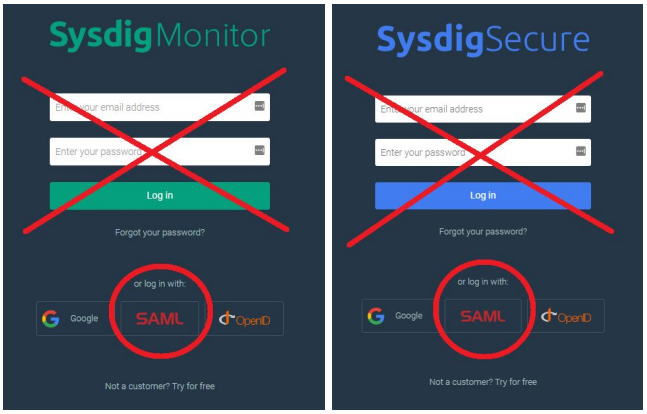
このセクションでは、SAMLをSysdig MonitorとSysdig Secureの両方と統合して有効にする方法について説明します。

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）

警告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IdP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.ユーザーに体験させるログインフローを決定します（3つのオプションから選択します）。	SAML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、会社名を入力します。 
	ブラウザでURLを入力/ブックマーク	**Monitor:** https://app.sysdigcloud.com/api/saml/`COMPANY_NAME` **Secure:** https://secure.sysdig.com/api/saml/`COMPANY_NAME`?product=SDS
	IdP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。 **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**		

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）

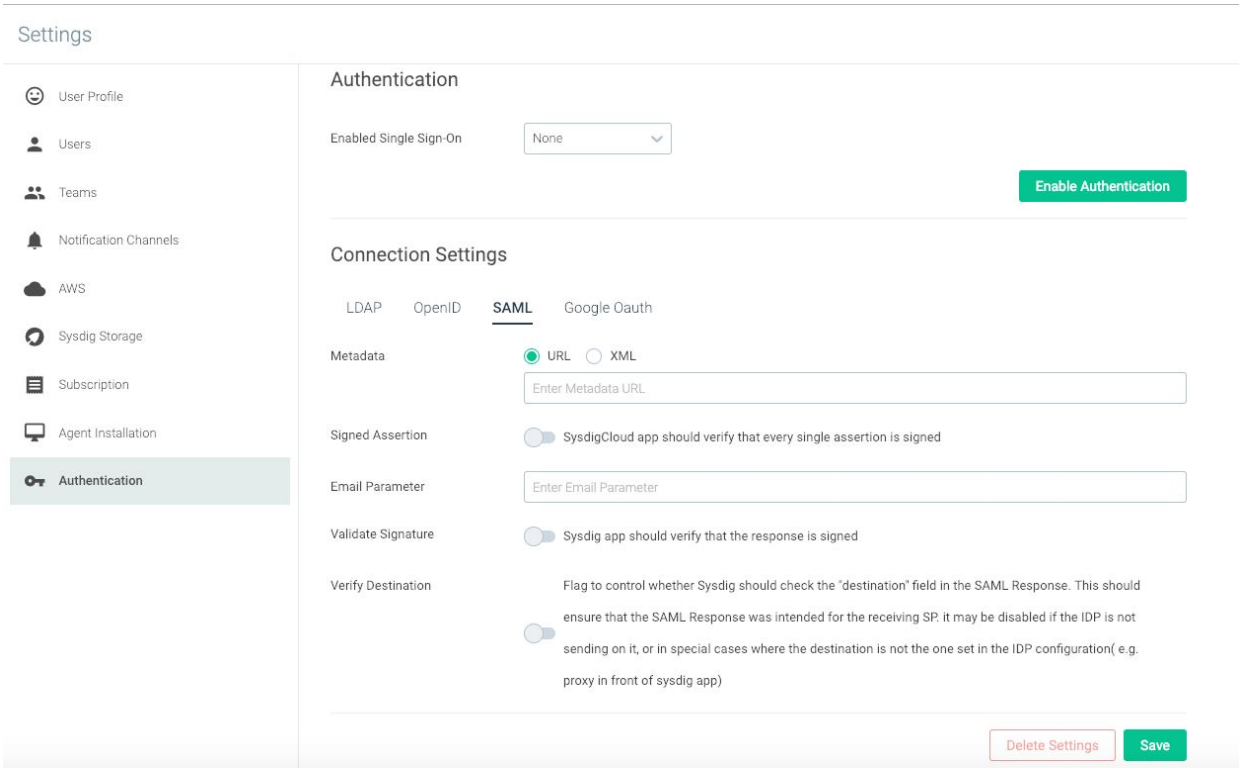
設定でSAMLを有効にする

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。



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。

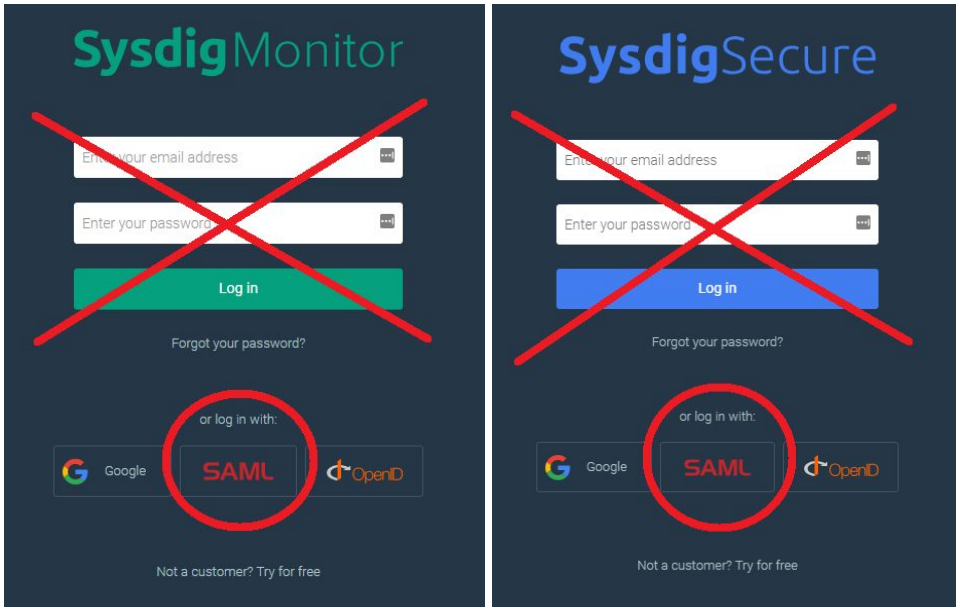
ユーザー体験

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、このサンプルPythonスクリプトを使用して、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、ユーザーとチームの管理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。
- SAMLシングルログアウト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SAML（SaaS）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/secureAuth`
Audience URI (SP Entity ID)	`https://app.sysdigcloud.com/api/saml/metadata`	`https://app.sysdigcloud.com/api/saml/metadata`
Default RelayState (optional - only configure if you intend to use IDP-initiated login flow)	#/&customer= `CUSTOMER-ID-NUMBER`	#/&customer= `CUSTOMER-ID-NUMBER`

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" entityID="
https://app.onelogin.com/saml/metadata/ 680358">...
```

OneLogin（SAML）

開始する前にSAML（SaaS）を確認してください。

OneLogin SAML Test Connectorを使用するというタイトルの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（IdP w / attr w / 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、お客様番号の検索に関する説明に従って取得した番号に置き換えます。

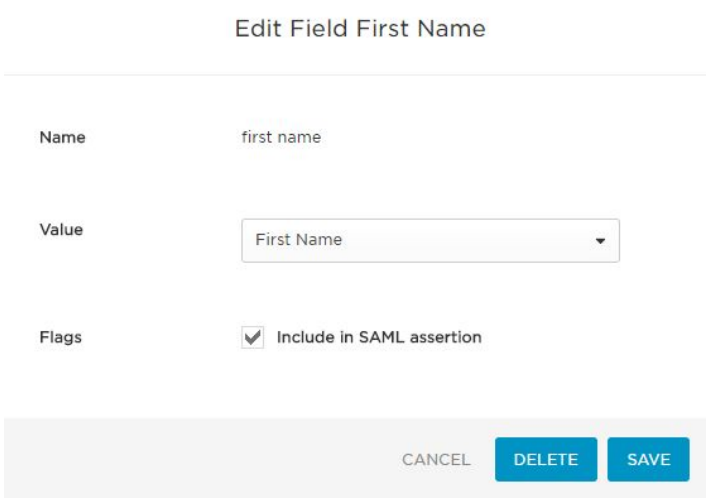
フィールド	Value for Sysdig Monitor	Value for Sysdig Secure
RelayState （オプション-IDPによって開始されるログインフローを使用する場合にのみ構成します）	#/&customer=`CUSTOMER-ID-NUMBER`	#/&customer=`CUSTOMER-ID-NUMBER`
Recipient	`https://app.sysdigcloud.com/api/saml/auth`	`https://secure.sysdig.com/api/saml/secureAuth`
ACS (Consumer) URL Validator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

（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。



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）

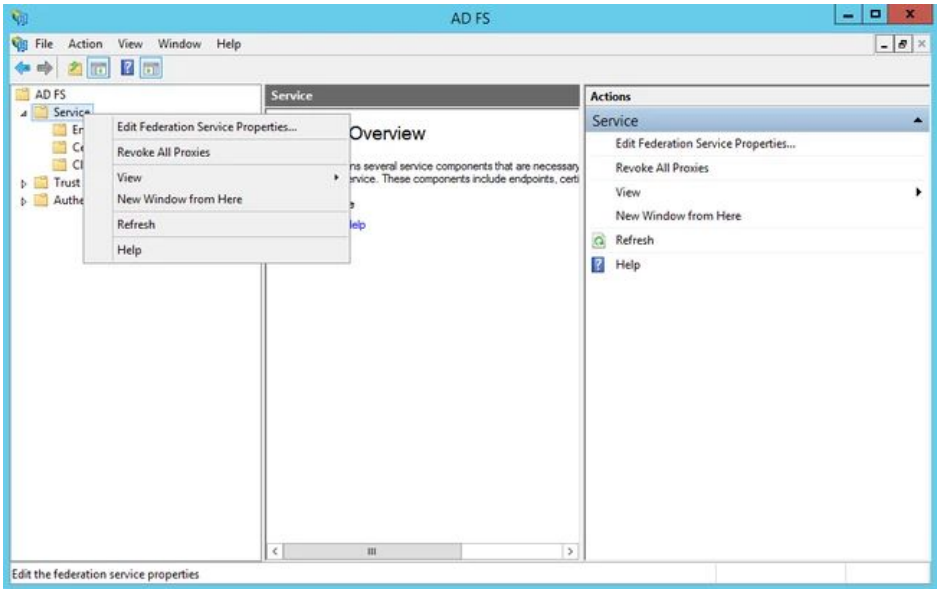
開始する前にSAML（SaaS）を確認してください。

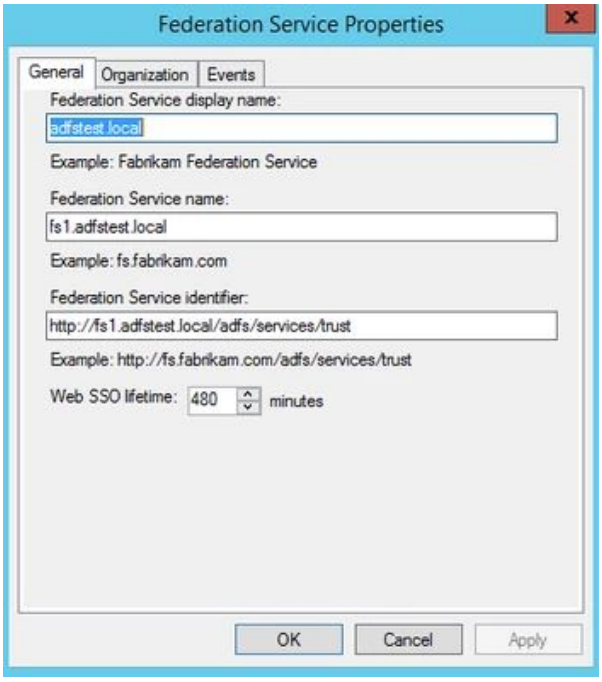
これらの手順では、インターネットにアクセス可能なADFS（Active Directoryフェデレーションサービス）サーバーがすでに動作していることを前提としています。相互運用性テストは、特にWindows Server 2012 R2上のADFSで実行されました。

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。

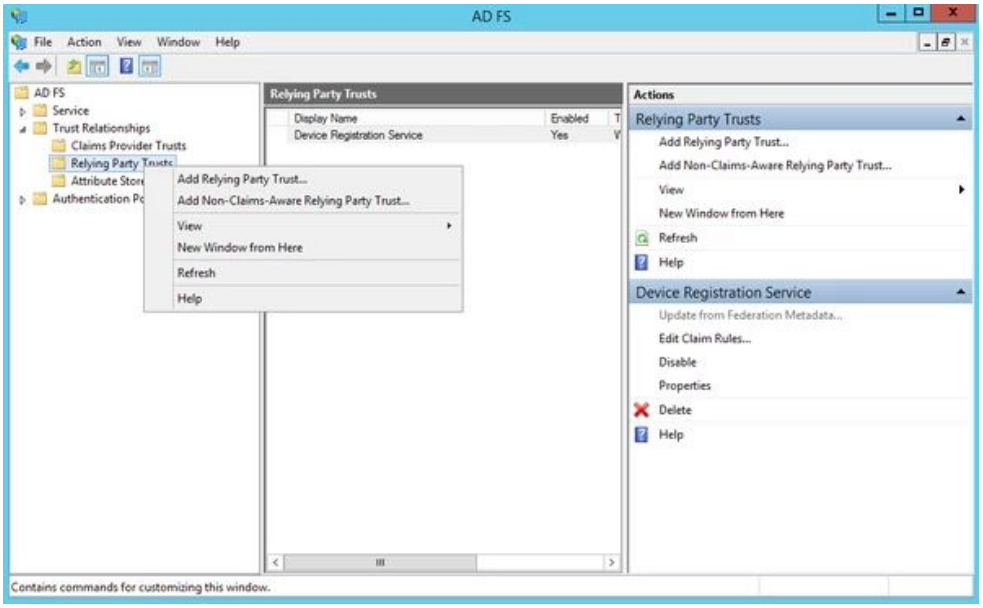
サービスプロバイダーが開始するログインフローの場合

1. [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。

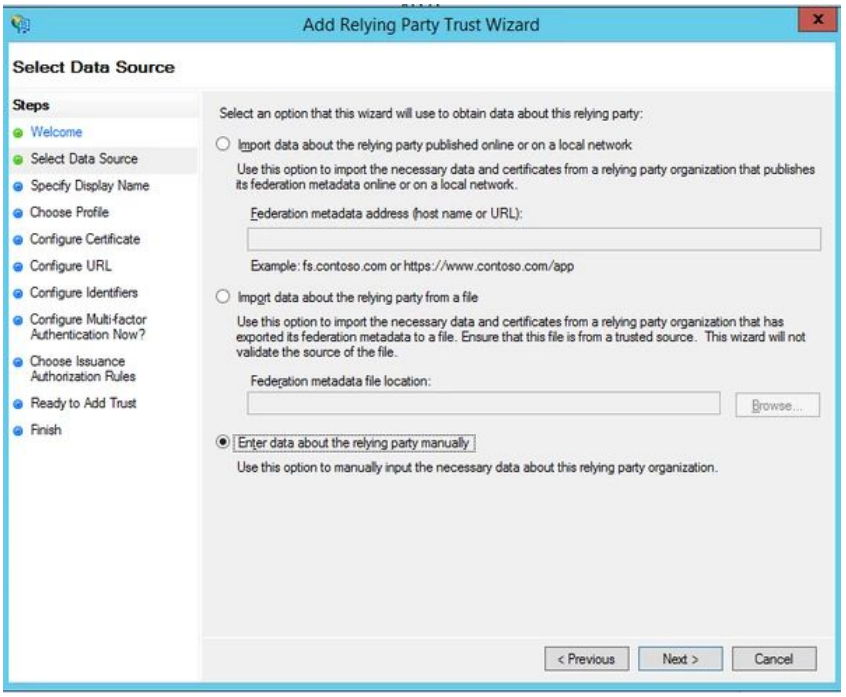




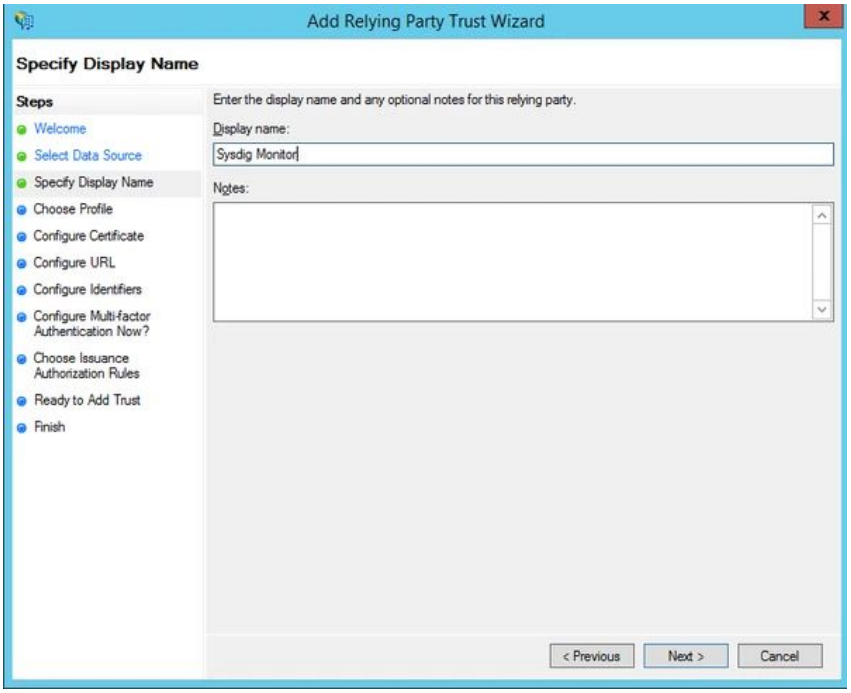
2. Sysdigアプリケーションの証明書利用者信頼構成を追加します。
    a. [証明書利用者信頼]> [証明書利用者信頼の追加]を右クリックし、[開始]をクリックしてウィザードを開始します。



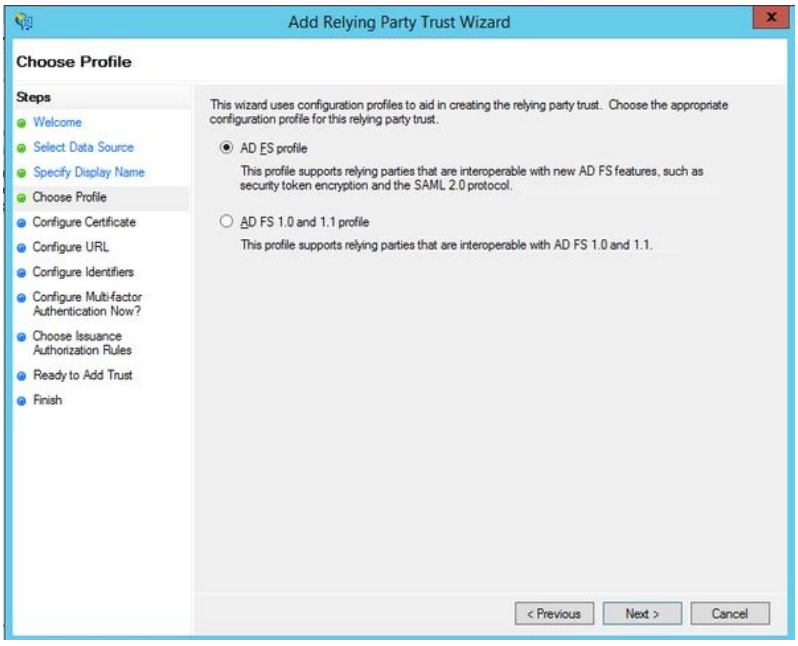
b. [データソースの選択]ステップで、証明書利用者に関するデータを手動で入力するボタンをクリックし、[次へ]をクリックします。



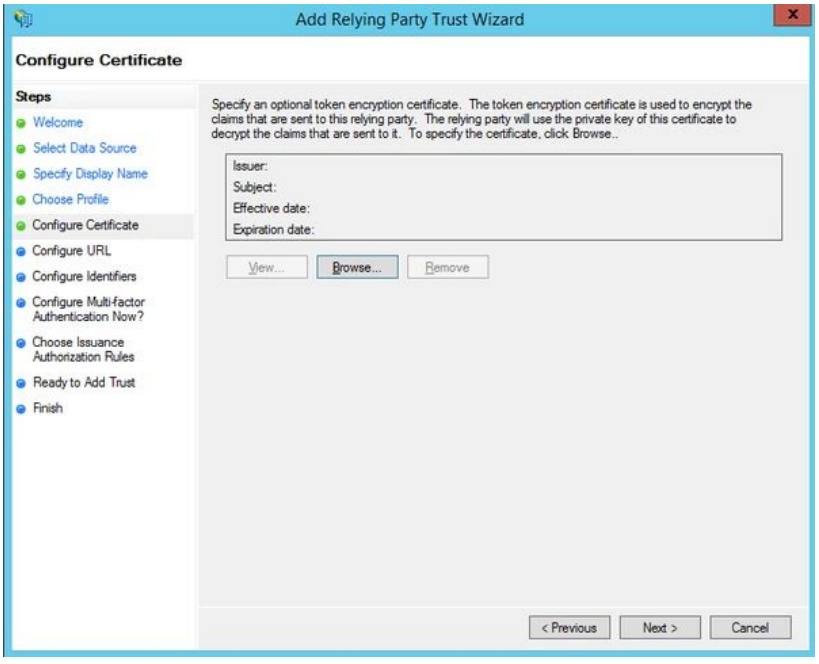
c. 選択した表示名（「Sysdig Monitor」または「Sysdig Secure」など）を入力し、[次へ]をクリックします



d. [次へ]をクリックして、AD FS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



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）

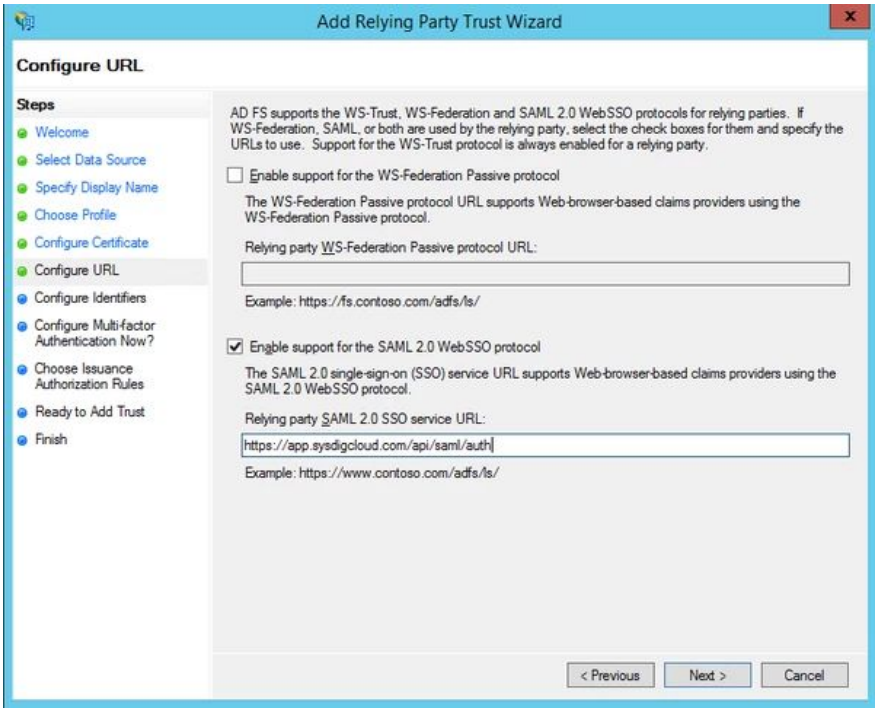


f. [SAML 2.0 Web SSOプロトコルのサポートを有効にする]チェックボックスをオンにして、証明書利用者のSAML 2.0 SSOサービスURLに次のいずれかの値を入力します。

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と入力します。

次に「次へ」をクリックします。

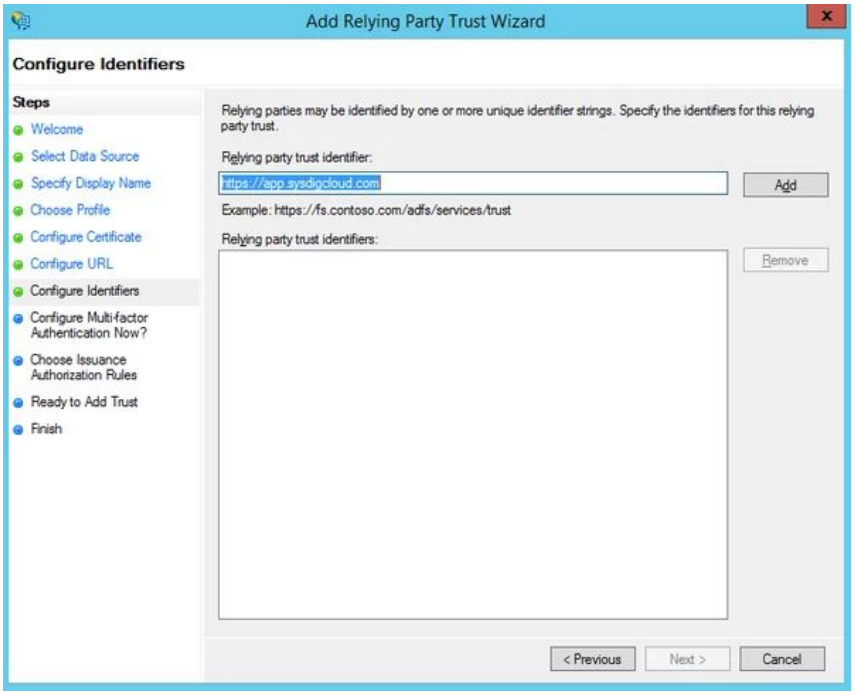


g. 証明書利用者信頼識別子には、次のいずれかの値を入力します。

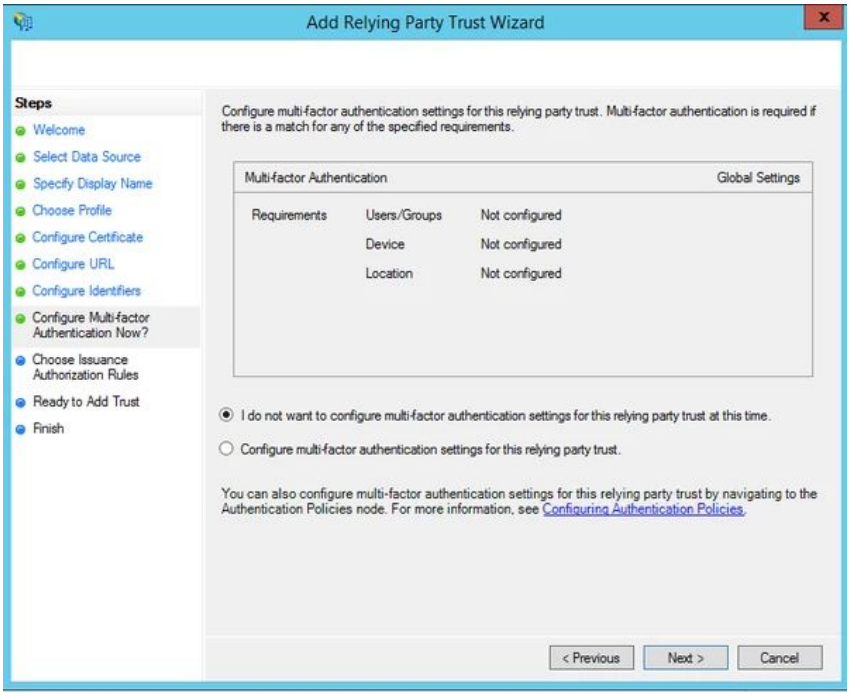
Sysdig Monitorを構成する場合は、https：//app.sysdigcloud.comと入力します。

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

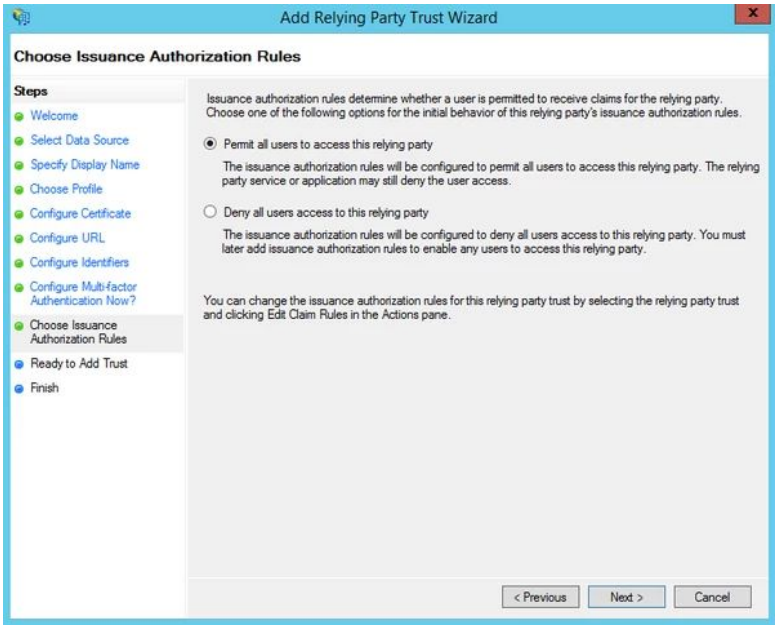
次に[追加]をクリックし、[次へ]をクリックします。



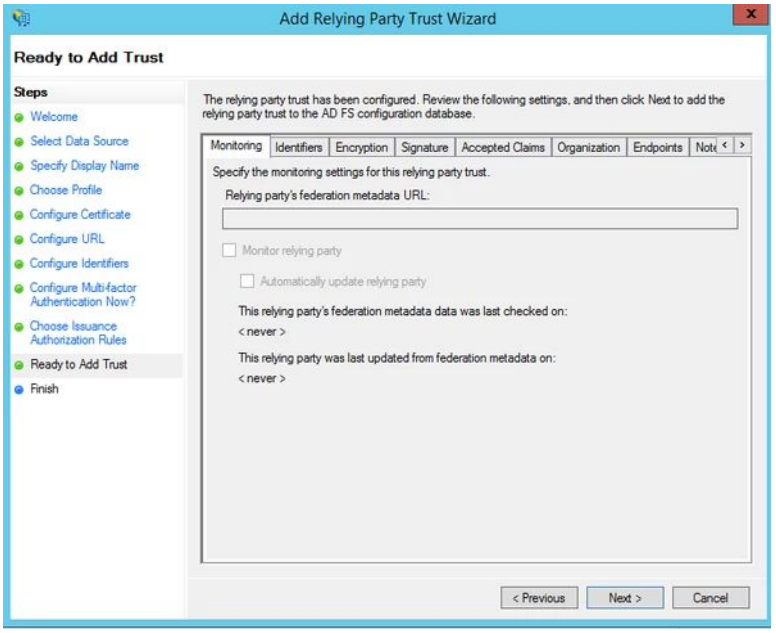
h. [次へ]をクリックして、多要素認証の構成をスキップします



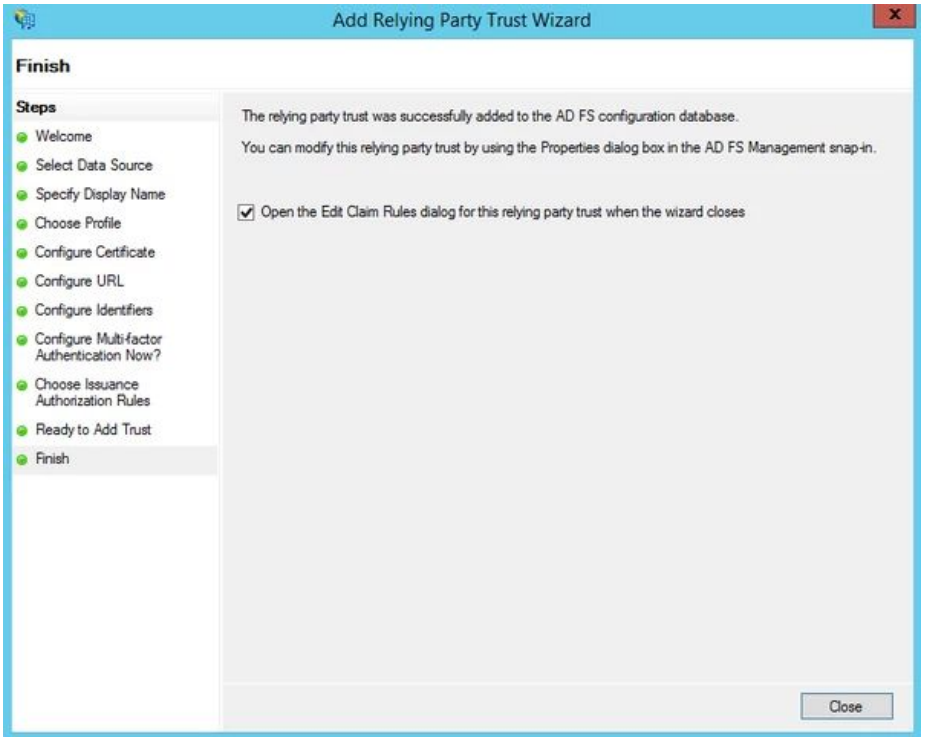
i. ユーザーにSysdigアプリケーションへのログインを許可するかどうかのポリシーを選択します。デフォルトでは、すべてのユーザーに証明書利用者へのアクセスを許可するというデフォルトの設定が許容されます。次へをクリックします。



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

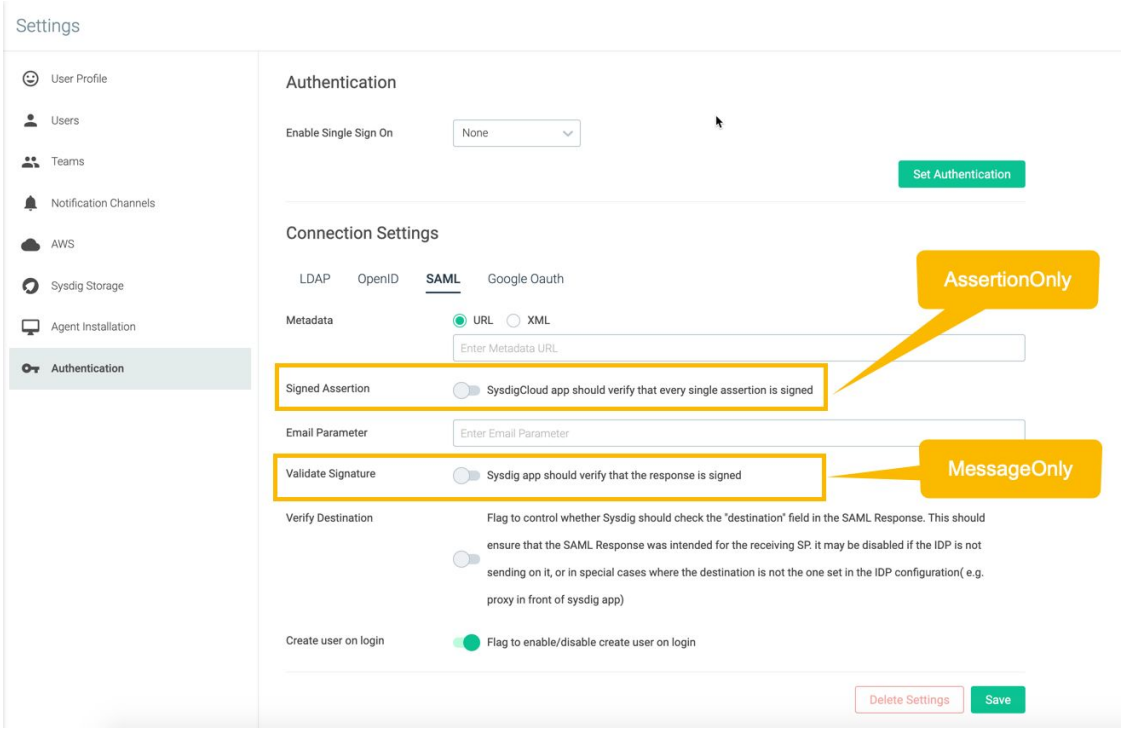


k. 次のステップでは、クレームルールを追加する必要があります。チェックボックスをオンのままにして[クレームルールの編集]ダイアログを開き、[閉じる]ボタンをクリックして、クレームルールエディターにすぐに移動できます。



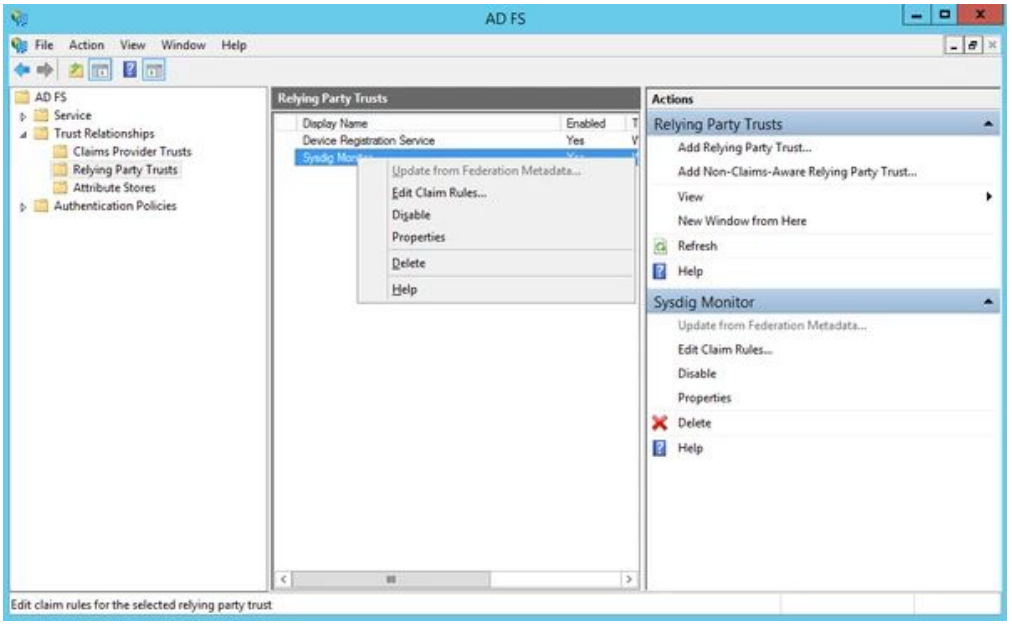
3. SamlResponseSignatureオプションがSysdig認証構成と一致していることを確認してください。
   a. PowerShell経由でSet-AdfsRelyingPartyTrust / Get-AdfsRelyingPartyTrustコマンドレットを使用して、SamlResponseSignatureを構成します。

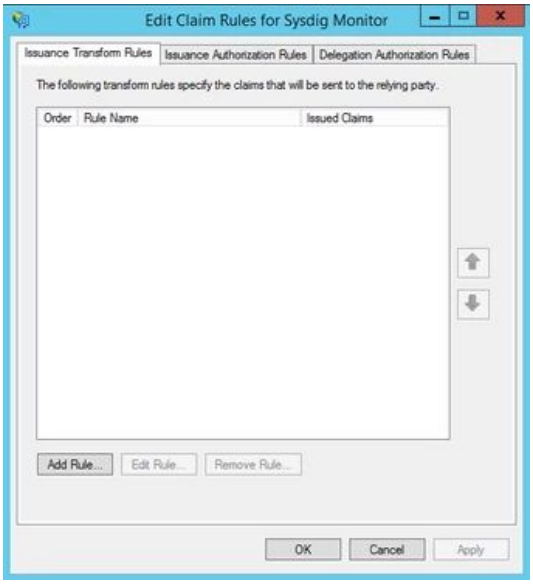
      -SamlResponseSignature
      依存パーティが期待する応答署名を指定します。このパラメーターの許容値は次のとおりです。
      AssertionOnly
      MessageAndAssertion
      MessageOnly
      詳細については、「Set-AdfsRelyingPartyTrust」を参照してください。
   b. Sysdigアプリで[設定]> [認証]に移動し、Sysdig認証設定がSamlResponseSignatureにマップされていることを確認します。



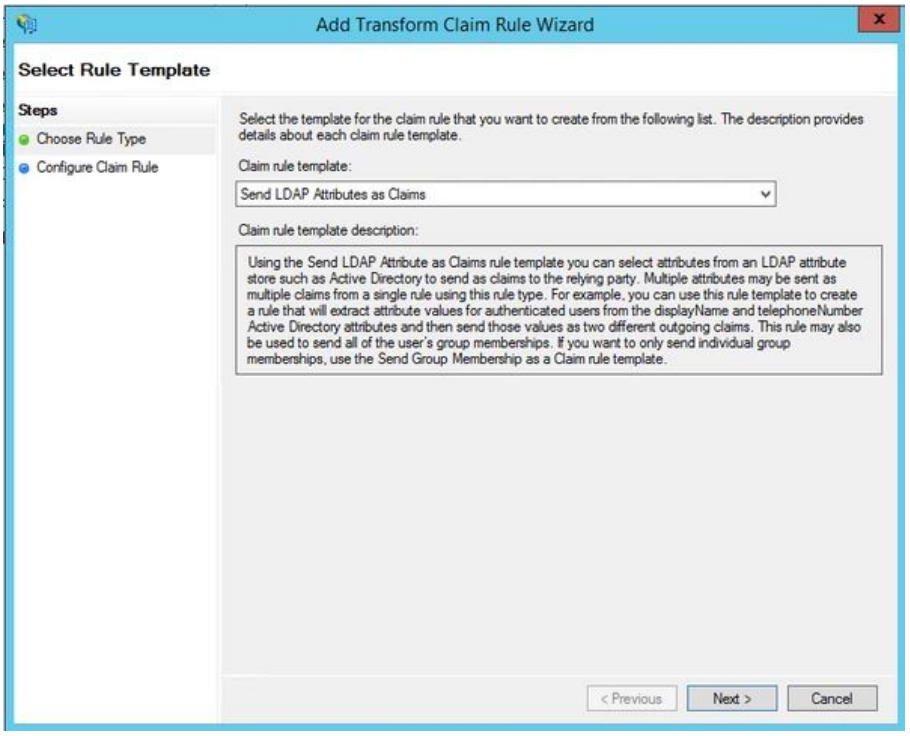
MessageAndAssertionで、両方のオプションを有効にします。

4. 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。

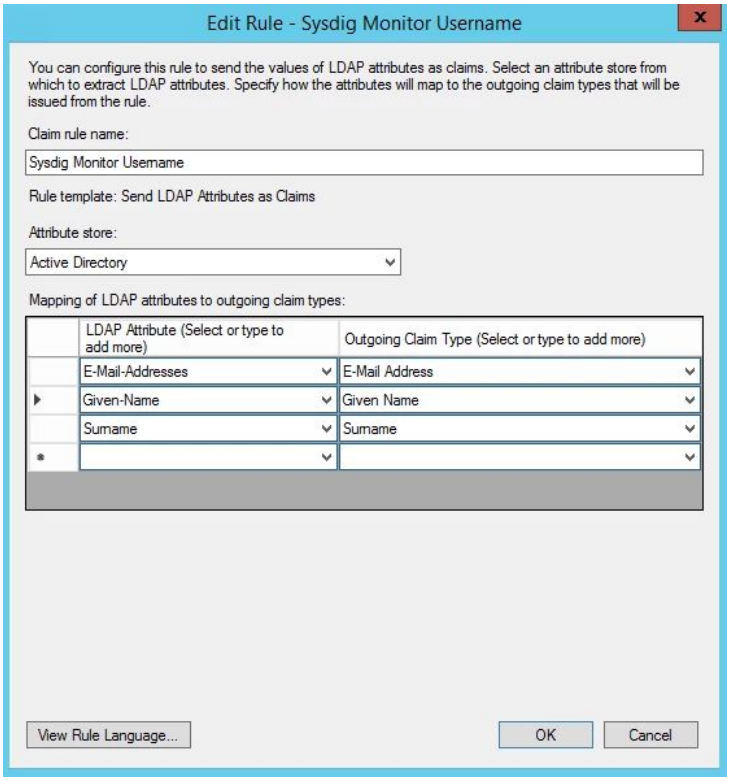




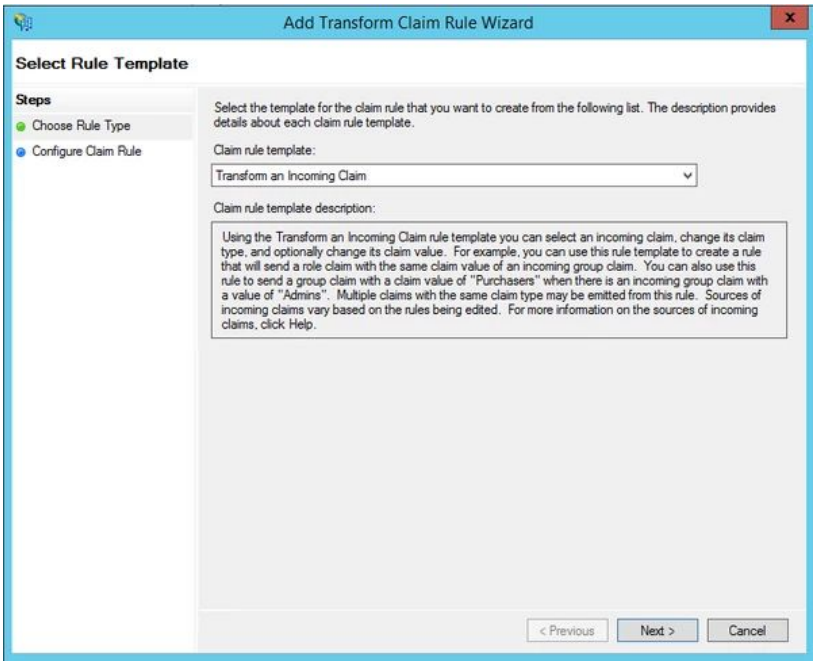
b. Add Ruleをクリックします。次の画面で、デフォルトのルールテンプレートを受け入れてLDAP属性をクレームとして送信し、[次へ]をクリックします。



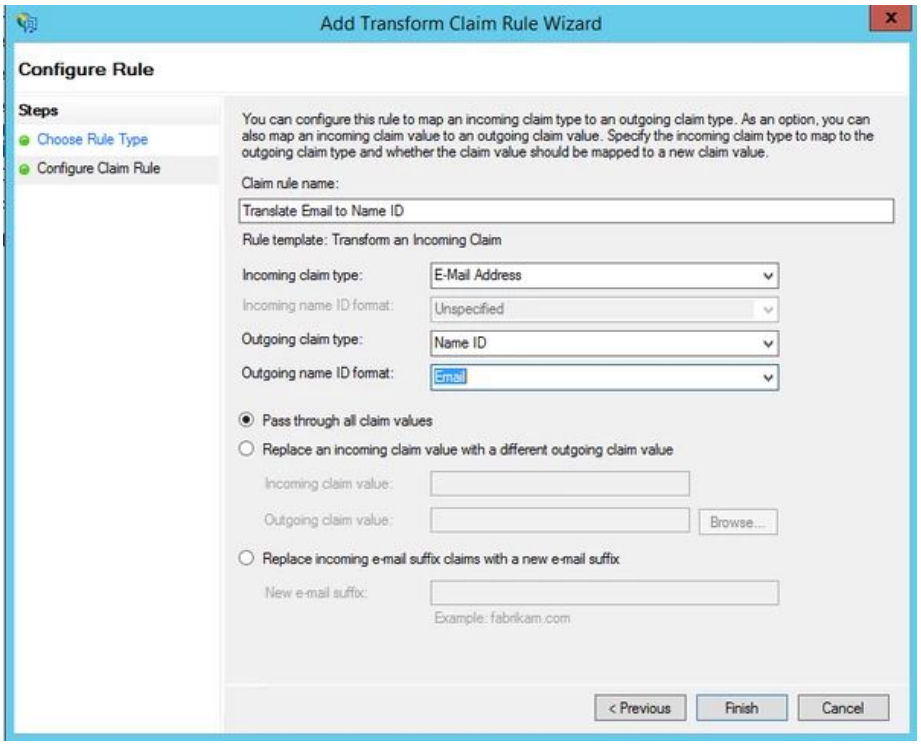
c. ルールの名前を入力し、属性ストアとしてActive Directoryを選択してから、プルダウンセレクターを使用して、LDAP属性と送信クレームタイプの両方として電子メールアドレスを選択し、同様に、名と姓のプルダウン選択を行います。 。これらの選択が完了したら、[完了]をクリックします。



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

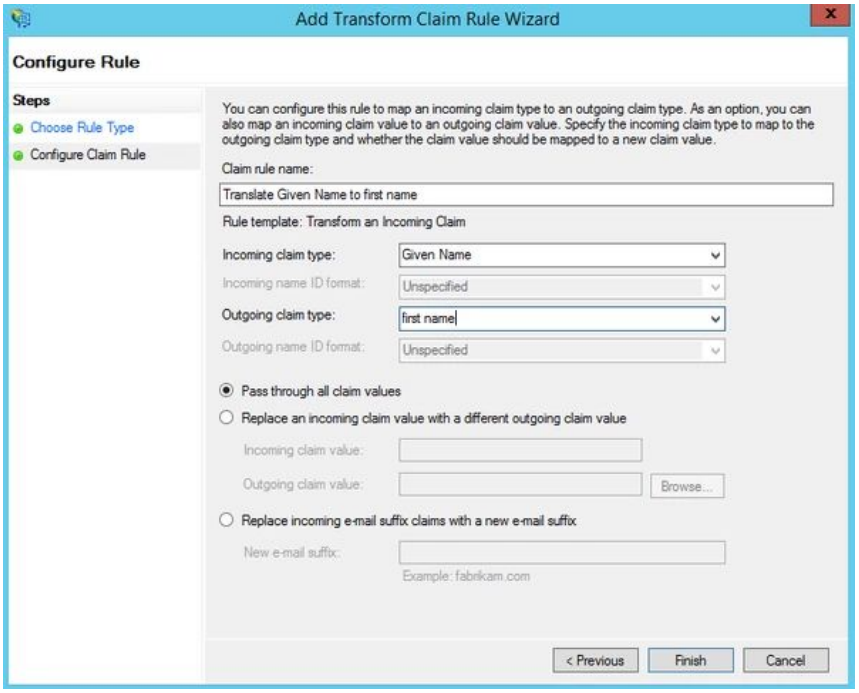


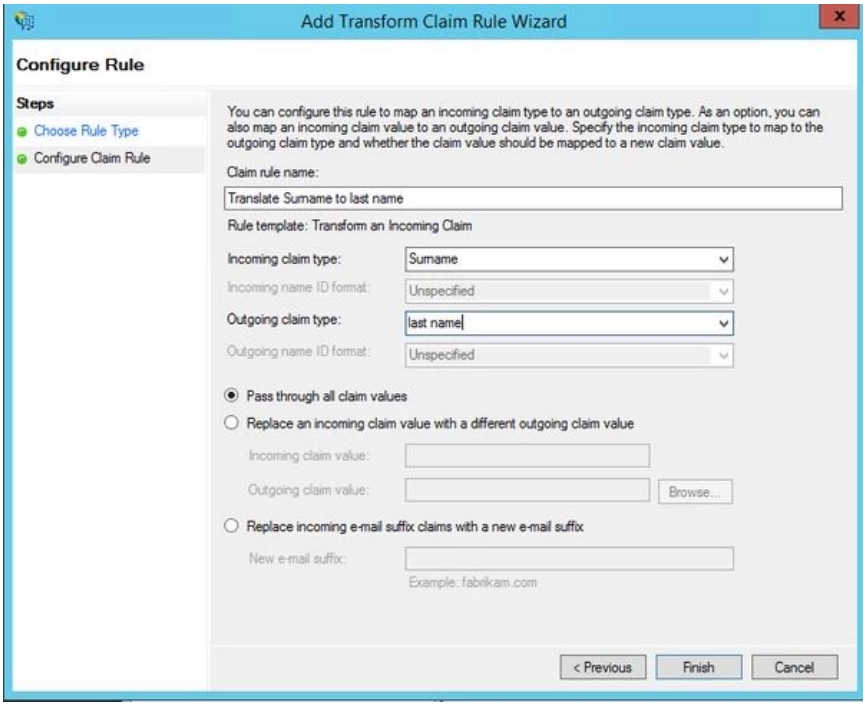
e. ルールの名前を入力し、プルダウンを使用して、電子メールアドレスの受信クレームタイプ、名前IDの送信クレームタイプ、および電子メールの送信名ID形式を選択し、[完了]をクリックします。



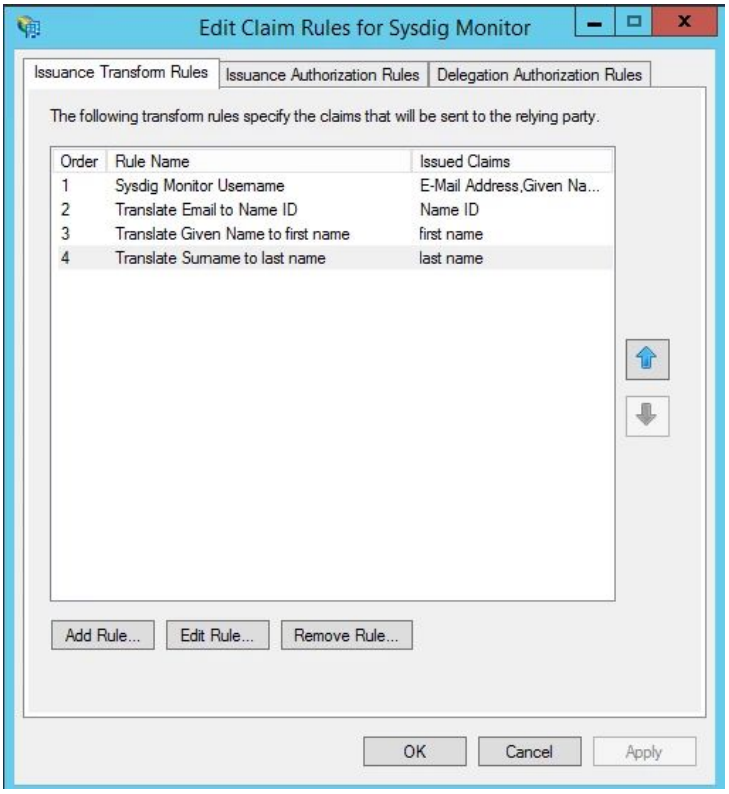
f. （オプション）新規ユーザーが初めてSAML経由で正常にログインしたときに、Sysdigプラットフォームデータベースで作成されたレコードにユーザーの名と姓を含める場合は、追加の変換ルールも作成する必要があります。メールベースのユーザー名のみが必須であり、このためのルールはすでに作成されているため、この手順はオプションです。

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。





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。



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）

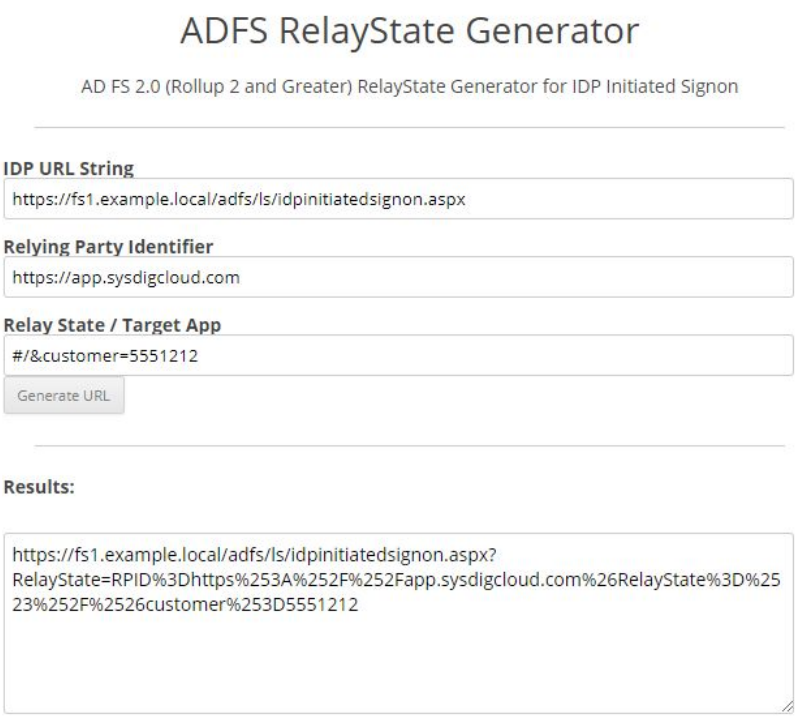
（オプション）上記の手順は、サービスプロバイダーが開始するSAML構成を表しています。 IdPによって開始されるSAML構成を希望する場合、これはADFSでも可能ですが、以下で説明する追加の手順が必要です。

1. 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、`<microsoft.identityserver.web>`セクションに`<useRelayStateForIdpInitiatedSignOn enabled="true" />`を追加します。変更を保存したら、ADFSサービスを再起動して変更を有効にします。

2. 顧客番号の検索に関する説明に従って、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ADFS RelayState Generatorツールを使用します。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。

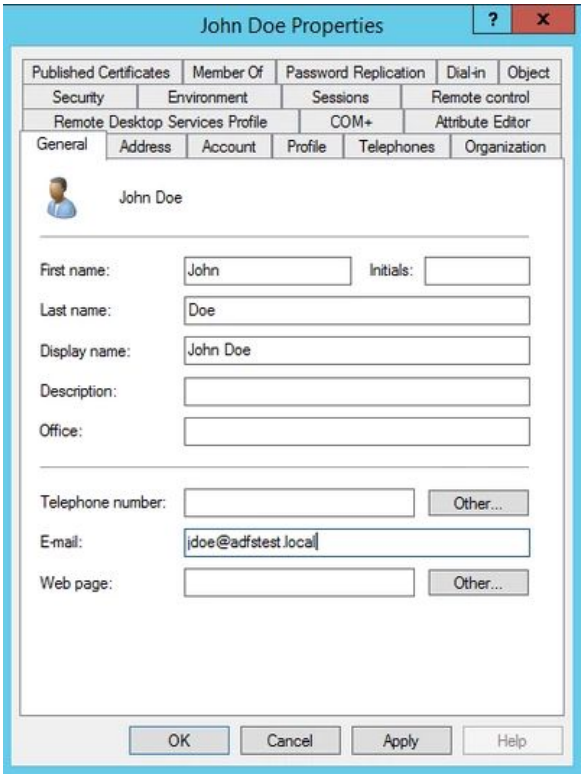
   - IDP URL文字列には、https://YOUR_ADFS_SERVER/adfs/ls/idpinitiatedsignon.aspxと入力します
   - 証明書利用者識別子には、次のいずれかの値を入力します。
   - Sysdig Monitorを構成する場合は、https://app.sysdigcloud.comと入力します
   - Sysdig Secureを構成する場合は、https://secure.sysdig.comと入力します。
   - リレー状態/ターゲットアプリの場合は、`#/&customer=CUSTOMER-ID-NUMBER`を入力し、前のステップ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



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Microsoft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。



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OpenID Connect（On-Prem）を参照してください。

Sysdigプラットフォームの OpenID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）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。

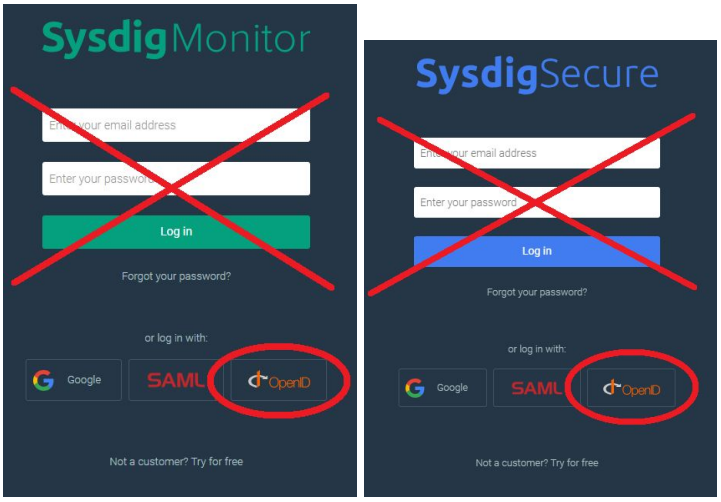
概要

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。

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、設定するIdP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（OpenID Connect Discovery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、会社名を入力します。

		
	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=SDS
	IdP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。

管理者の手順

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

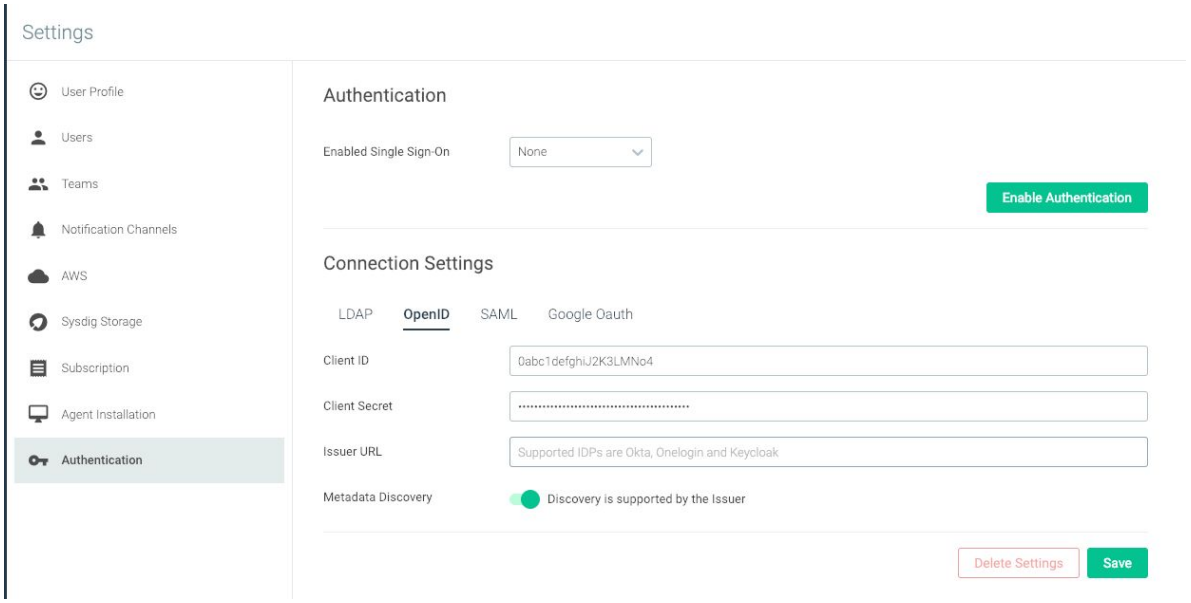
ベースラインOpenID機能を有効にするには：

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。



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	IdPから提供されたURL: https://YOUR-ONELOGIN-DOMAIN.onelogin.com/oidc

注意

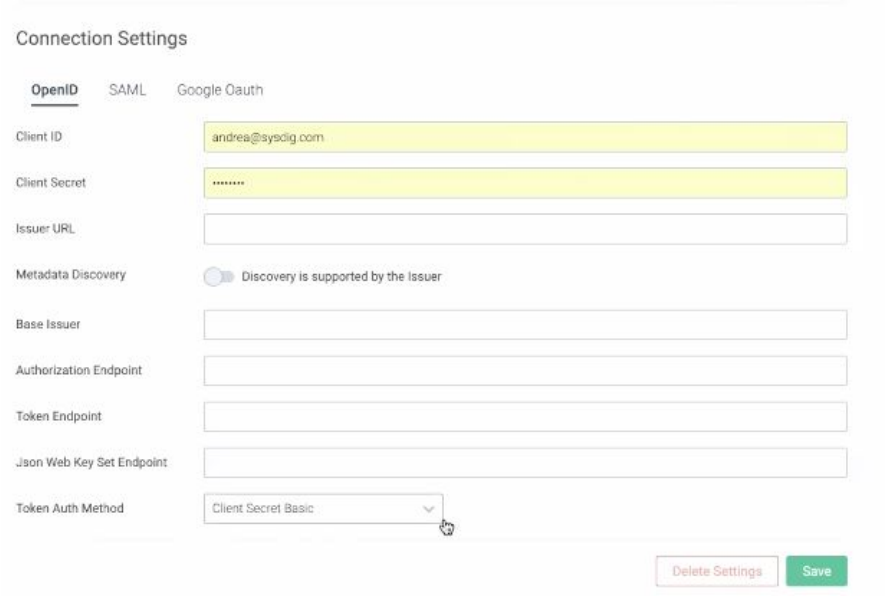
Okta、OneLogin、Keycloakはメタデータの自動検出をサポートしているため、これらのIdPにはこれらの設定で十分です。

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。



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: https://openid-connect.onelogin.com/oidc、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 Method	認証方法 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。
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。

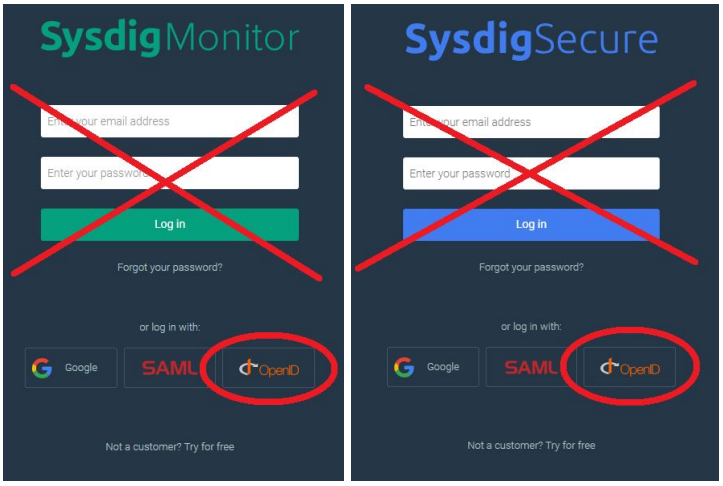
ユーザー体験

上記の基本的な有効化ワークフローで述べたように、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、ユーザーとチームの管理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、OpenID Connect（SaaS）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
2. [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。
7. [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）

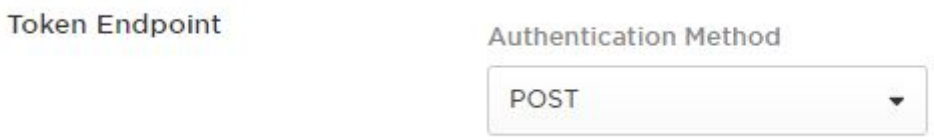
OneLoginのOpenIDプロバイダーの設定

開始する前に、OpenID Connect（SaaS）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

4. [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。



6. 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、OpenID Connect（SaaS）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
9. 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。