アラート送信先/SIEM

Datadog

設定が完了すると、定義済みのアラートサービスプロファイルとアラートルールを使用して、Multicloud Defense アラートが Datadog に送信されます。

アラート プロファイル サービスの作成

始める前に

Datadog にアラートを送信するには、次の情報が必要です。

- Datadog アカウント
- API Key

ヒント

- Datadog アカウントにサインアップするには、Datadog アカウント（https://www.datadoghq.com/）を参照してください。
- Datadog API キーを作成するには、Datadog API キー（https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api）を参照してください。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。例 `Multicloud Defense：-Datadog-profile`。
ステップ 4 [説明（Description）]（任意）：アラート統合の説明を入力します。
ステップ 5 [タイプ（Type）]：プルダウンを使用して、[Datadog] を選択します。
ステップ 6 [APIキー（API Key）]：通信の認証に使用する Datadog API キーを指定します。
ステップ 7 [保存（Save）] をクリックします。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

アラートルールの作成

始める前に

Datadog にアラートを送信するには、次の情報が必要です。

- Datadog アカウント
- API Key

ヒント

- Datadog アカウントにサインアップするには、Datadog アカウント（https://www.datadoghq.com/）を参照してください。
- Datadog API キーを作成するには、Datadog API キー（https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api）を参照してください。

手順

ステップ 1 **[設定（Settings）]** > **[アラートプロファイル（Alert Profiles）]** > **[アラートルール（Alert Rules）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。例：`Multicloud Defense-Datadog-alert-rule`。

ステップ 4 [説明（Description）]（任意）：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、[PagerDutyアラートプロファイル（PagerDuty Alert Profile）] を選択します。例として、上で作成した `Multicloud Defense-Datadog-profile` プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）]：[システムログ（System Logs）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。[検出（Discovery）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [インサイトルール（Insights Rule）] です。

ステップ 8 [重大度（Severity）]：[システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、重大度レベルを [情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。[検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] のいずれかのオプションから重大度レベルを選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

Microsoft Sentinel

設定が完了すると、定義済みのアラートサービスプロファイルとアラートルールを使用して、Multicloud Defense アラートが Microsoft Sentinel に送信されます。

アラート プロファイル サービスの作成

始める前に

Microsoft Sentinel にアラートを送信するには、次の情報が必要です。

- Azure ログ分析ワークスペースを作成します。
- Azure ログテーブルを定義します。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。例：`mcd-mssentinel-profile`。

ステップ 4 [説明（Description）]（任意）：アラート統合の説明を入力します。

ステップ 5 [タイプ（Type）]：プルダウンを使用して、[Microsoft Sentinel] を選択します。

ステップ 6 [APIキー（API Key）]：Azure ログ分析ワークスペース用に Azure で作成された共有キーを指定します。

ステップ 7 [Azureログテーブル名（Azure Log Table Name）]：Azure ログ分析ワークスペースの作成時に定義された Azure ログの名前を指定します。

ステップ 8 [Azureログ分析ワークスペースID（Azure Log Analytics Workspace ID）]：Azure ログ分析ワークスペースの ID を指定します。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

アラートルールの作成

始める前に

Microsoft Sentinel にアラートを送信するには、次の情報が必要です。

- Azure ログ分析ワークスペースを作成します。
- Azure ログテーブルを定義します。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[アラート（Alert）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。例：`mcd-mssentinel-alert-rule`。

ステップ 4 [説明（Description）]（任意）：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、以前に作成した適切なプロファイルを選択します。例として、上で作成した `mcd-mssentinel-profile` プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）]：[システムログ（System Logs）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。[検出（Discovery）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [インサイトルール（Insights Rule）] です。

ステップ 8 [重大度（Severity）]：[システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、重大度レベルを [情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。[検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] のいずれかのオプションから重大度レベルを選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

PagerDuty

設定が完了すると、定義済みのアラートサービスプロファイルとアラートルールを使用して、Multicloud Defense アラートが PagerDuty API ゲートウェイに送信されます。

アラート プロファイル サービスの作成

始める前に

このガイドの手順を完了するには、以下が必要です。

- API キーが設定された PagerDuty アカウント。

ヒント

- PagerDuty アカウント（https://www.servicenow.com/my-account/sign-up.html）にサインアップします。
- API キー（https://developer.pagerduty.com/api-reference）を設定します。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。例：`mcd-pagerduty-profile`。

ステップ 4 [説明（Description）]（任意）：アラート統合の説明を入力します。

ステップ 5 [タイプ（Type）]：プルダウンを使用して、[PagerDuty] を選択します。

ステップ 6 [APIキー（API Key）]：上で生成した PagerDuty API キー、または必要に応じて他の PagerDuty API キーをコピーします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

アラートルールの作成

始める前に

このガイドの手順を完了するには、以下が必要です。

API キーが設定された PagerDuty アカウント。

ヒント

- PagerDuty アカウント（https://www.servicenow.com/my-account/sign-up.html）にサインアップします。
- API キー（https://developer.pagerduty.com/api-reference）を設定します。

手順

ステップ 1 **[管理（Administration）] > [アラートプロファイル（Alert Profiles）] > [アラートルール（Alert Rules）]** に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。例：`mcd-pagerduty-alert-rule`。

ステップ 4 [説明（Description）]（任意）：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、[PagerDutyアラートプロファイル（PagerDuty Alert Profile）] を選択します。例として、上で作成した `mcd-pagerduty-profile` プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）]：[システムログ（System Logs）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。[検出（Discovery）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [インサイトルール（Insights Rule）] です。

ステップ 8 [重大度（Severity）]：[システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、重大度レベルを [情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。[検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] のいずれかのオプションから重大度レベルを選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

ServiceNow

設定が完了すると、定義済みのアラートサービスプロファイルとアラートルールを使用して、Multicloud Defense アラートが ServiceNow API ゲートウェイに送信されます。

アラート プロファイル サービスの作成

始める前に

このガイドの手順を完了するには、以下が必要です。

- 着信ウェブフック URL を持つ ServiceNow アカウント。
- 設定済みの API キー。

ヒント

- ServiceNow アカウントへのサインアップ（https://www.servicenow.com/my-account/sign-up.html）
- ウェブフックと API キーの設定（https://docs.servicenow.com/search?q=setup%20webhook）

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。例：`mcd-servicenow-profile`。

ステップ 4 [説明（Description）]（任意）：アラート統合の説明を入力します。

ステップ 5 [タイプ（Type）]：プルダウンを使用して、[ServiceNow] を選択します。

ステップ 6 [APIキー（API Key）]：上記で生成した ServiceNow API キー、または必要に応じて他の ServiceNow API キーを指定します。

ステップ 7 [API URL]：上で生成された ServiceNow ウェブフック URL を指定するか、必要に応じて他の ServiceNow ウェブフック URL を指定します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

アラートルールの作成

始める前に

このガイドの手順を完了するには、以下が必要です。

- 着信ウェブフック URL を持つ ServiceNow アカウント。
- 設定済みの API キー。

ヒント

- ServiceNow アカウントへのサインアップ（https://www.servicenow.com/my-account/sign-up.html）
- ウェブフックと API キーの設定（https://docs.servicenow.com/search?q=setup%20webhook）

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[アラートルール（Alert Rules）]** に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。例：`mcd-servicenow-alert-rule`。

ステップ 4 [説明（Description）]（任意）：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、[ServiceNowアラートプロファイル（ServiceNow Alert Profile）] を選択します。例として、上で作成した `mcd-servicenow-profile` プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）] を選択します。

- [システムログ（System Logs）] タイプの場合、オプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。
- [検出（Discovery）] タイプの場合、オプションは [インサイトルール（Insights Rule）] のみです。

ステップ 8 [重大度（Severity）] を選択します。

- [システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、重大度レベルを [情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。
- [検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] から選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

Slack

設定が完了すると、Multicloud Defense アラートは、定義済みのアラート サービス プロファイルとルールを使用して Slack 着信ウェブフック URL に送信されます。

アラート プロファイル サービスの作成

始める前に

このガイドの手順を完了するには、以下が必要です。

- 着信ウェブフック URL が設定された Slack アカウント。

ヒント

1. Slack アカウント（https://slack.com/get-started#/create）を作成します。
2. 着信ウェブフック（https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks）を作成します。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。例：`mcd-slack-profile`。

ステップ 4 [説明（Description）]（任意）：アラート統合の説明を入力します。

ステップ 5 [タイプ（Type）]：プルダウンを使用して、[Slack] を選択します。

ステップ 6 [API URL]：上で生成された Slack ウェブフック URL を指定するか、必要に応じて他の Slack ウェブフック URL を指定します。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

アラートルールの作成

始める前に

このガイドの手順を完了するには、以下が必要です。

着信ウェブフック URL が設定された Slack アカウント。

ヒント

1. Slack アカウント（https://slack.com/get-started#/create）を作成します。
2. 着信ウェブフック（https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks）を作成します。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[アラートルール（Alert Rules）]** に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。例：`mcd-slack-alert-rule`。

ステップ 4 [説明（Description）]（任意）：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、[Slackアラートプロファイル（Slack Alert Profile）] を選択します。例として、上で作成した `mcd-slack-profile` プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）]：[システムログ（System Logs）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。[検出（Discovery）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [インサイトルール（Insights Rule）] です。

ステップ 8 [重大度（Severity）]：[システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、重大度レベルを [情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。[検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] のいずれかのオプションから重大度レベルを選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

Webex

設定が完了すると、定義済みのアラートサービスプロファイルとアラートルールを使用して、Multicloud Defense アラートが Webex API ゲートウェイに送信されます。

アラート プロファイル サービスの作成

Webex サービスのアラートプロファイルを作成するには、次の手順を実行します。

始める前に

このガイドの手順を完了するには、以下が必要です。

- 着信ウェブフック URL を持つ Webex アカウント。
- 設定済みの API キー。

（注）

1. Webex アカウントを作成するか、アカウントにアクセスします。
2. Webex 着信ウェブフックを作成します。
3. 着信ウェブフックの権限を受け入れます。
4. 名前を入力し、Webex スペースを選択します。
5. アラート サービス プロファイルの設定で使用する Webex ウェブフック URL をコピーします。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。

ステップ 4 （任意）[説明（Description）]：アラート統合の説明を入力します。

ステップ 5 [タイプ（Type）]：プルダウンを使用して、[Webex] を選択します。

ステップ 6 [API URL]：前提条件の一部として生成された Webex ウェブフック URL、または必要に応じて他の Webex ウェブフック URL を指定します。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

アラートルールの作成

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[アラートルール（Alert Rules）]** に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。たとえば、`mcd-servicenow-alert-rule` などです。

ステップ 4 （任意）[説明（Description）]：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、[Webexアラートプロファイル（Webex Alert Profile）] を選択します。例として、上で作成した mcd-servicenow-profile プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）] を選択します。

- [システムログ（System Logs）] タイプの場合、オプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。
- [検出（Discovery）] タイプの場合、オプションは [インサイトルール（Insights Rule）] のみです。

ステップ 8 [重大度（Severity）] を選択します。

- [システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、[情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。
- [検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] から選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

スプランク

設定が完了すると、定義済みのアラートサービスプロファイルとアラートルールを使用して、Multicloud Defense アラートが API ゲートウェイに送信されます。

Splunk プロファイルサービスの作成

Splunk サービスのアラートプロファイルを作成するには、次の手順を実行します。

始める前に

次のように設定し、準備しておく必要があります。

- Multicloud Defense で API キーを作成し、キーとシークレットの両方を保存します。詳細については、Multicloud Defense での API キーの作成を参照してください。
- Splunk Web で HTTP Event Collector（HEC）を設定します。詳細については、「Splunk Cloud での HTTP Event Collector の設定」を参照してください。
- Splunk HEC で次のように設定する必要があります。
  - HEC を**有効**にする必要があります。
  - 少なくとも 1 つのアクティブな HEC トークンを使用できる必要があります。
  - アクティブなトークンを使用して HEC に認証する必要があります。
  - HEC に送信するデータを適切にフォーマットする必要があります。「HTTP Event Collector 向けのイベントのフォーマット」を参照してください。

手順

ステップ 1 **[管理（Administration）]** > **[アラートプロファイル（Alert Profiles）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [名前（Name）]：アラート統合の一意の名前を入力します。

ステップ 4 [説明（Description）]（任意）：アラート統合の説明を入力します。

ステップ 5 [タイプ（Type）]：プルダウンを使用して、[Splunk] を選択します。

ステップ 6 [APIキー（API Key）]：上で生成した Splunk API キー、または必要に応じて他の PagerDuty API キーをコピーします。

ステップ 7 SAN フィールドがドメインと一致する証明書がサーバーにない場合は、[証明書の検証をスキップ（Skip Verify Certificate）] チェックボックスをオンにします。SAN フィールドがドメインに一致する証明書がサーバーにある場合は、このチェックボックスをオフのままにします。

ステップ 8 [インデックス（デフォルト-メイン）（Index(default - main)）] は、処理されたすべてのデータが保存される Splunk のデフォルトのインデックスです。これは、Splunk HEC を設定するときに提供されます。

ステップ 9 Splunk HTTP Event Collector の [API URL] を入力します。次の URL が推奨されます：`https://<host>:<port>/services/collector` 。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

この新しいプロファイルを使用してアラートルールを作成します。

Splunk ルールの作成

Splunk アラートサービスを含むルールを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [アラートプロファイル（Alert Profiles）] > [アラート（Alert）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [プロファイル名（Profile Name）]：統合の一意の名前を入力します。例：`mcd-mssentinel-alert-rule`。

ステップ 4 [説明（Description）]（任意）：アラートルールの説明を入力します。

ステップ 5 [アラートプロファイル（Alert Profile）]：プルダウンを使用して、以前に作成した適切なプロファイルを選択します。例として、上で作成した `mcd-splunk-rule` プロファイルを選択します。

ステップ 6 [タイプ（Type）]：プルダウンを使用して、[システムログ（System Logs）] または [検出（Discovery）] を選択します。

ステップ 7 [サブタイプ（Sub Type）]：[システムログ（System Logs）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [ゲートウェイ（Gateway）] または [アカウント（Account）] のいずれかになります。[検出（Discovery）] タイプの場合、[サブタイプ（Sub Type）] プルダウンオプションは [インサイトルール（Insights Rule）] です。

ステップ 8 [重大度（Severity）]：[システムログ（System Logs）] タイプを選択した場合、プルダウンを使用して、重大度レベルを [情報（Info）]、[警告（Warning）]、[中（Medium）]、[高（High）] または [重大（Critical）] のオプションから選択します。[検出（Discovery）] タイプの場合、[情報（Info）]、[中（Medium）]、[重大（Critical）] のいずれかのオプションから重大度レベルを選択します。

ステップ 9 [有効（Enabled）]：チェックボックスをオンにして、このアラートプロファイルを有効にします。

ステップ 10 [保存（Save）] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。