CHAPTER 12

アラームの管理

ACS のモニタリング機能では、クリティカルなシステム条件を通知するアラームが生成されます。モニタリング コンポーネントでは、データが ACS から取得されます。このデータにしきい値と規則を設定して、アラームを管理できます。

アラーム通知は Web インターフェイスに表示され、電子メールおよび Syslog メッセージを通じてイベントの通知を取得できます。ACS は、重複するアラームをデフォルトでフィルタリングします。

この章の内容は、次のとおりです。

アラームについて

ACS には 2 種類のアラームがあります。

しきい値アラーム

しきい値アラームは、特定のイベントを通知する ACS サーバから収集されたログ データに定義されます。たとえば、ACS システムの健全性、ACS プロセスのステータス、認証がアクティブかどうかなどを通知するようにしきい値アラームを設定できます。

これらのデータ セットに対してしきい値条件を定義します。しきい値条件が満たされると、アラームがトリガーされます。しきい値を定義するときには、しきい値をいつ適用する必要があるか（期間）、アラームの重大度、および通知の送信方法も定義します。

使用可能なアラームしきい値の 15 個のカテゴリを使用すると、ACS システムの動作の多くの異なる側面を監視できます。しきい値アラームの詳細については、「アラームしきい値の作成、編集、および複製」（P.12-11）を参照してください。

システム アラーム

システム アラームは、ACS Monitoring & Reporting Viewer の実行中に検出されたクリティカル条件を通知します。システム アラームは、データ削除イベントや、ログ コレクタによる View データベースへのデータ入力の失敗など、システム アクティビティの情報ステータスも提供します。

システム アラームは定義済みであり、設定できません。ただし、システム アラームをディセーブルにしたり、イネーブルにした場合の通知方法を決定したりするオプションはあります。

ここでは、次の内容について説明します。

- 「アラームしきい値の評価」（P.12-2）
- 「ユーザへのイベントの通知」（P.12-3）

アラームしきい値の評価

ACS は、スケジュールに基づいてしきい値条件を評価します。これらのスケジュールを定義し、しきい値の作成時にしきい値にスケジュールを割り当てます。スケジュールは、週の中の 1 つ以上の連続または不連続期間で構成されます。

たとえば、月曜日から金曜日までの午前 8:00 から ～午後 5 時 00 分、月曜日～金曜日。詳細については、「アラーム スケジュールについて」（P.12-9）を参照してください。このスケジュールをしきい値に割り当てると、ACS によってしきい値が評価され、アクティブな期間中にだけアラームが生成されます。

ACS は、現在イネーブルになっているしきい値の数に応じてしきい値を定期的に評価します。

表 12-1 に、特定のしきい値数の評価サイクルの長さを示します。

表 12-1　アラームしきい値の評価サイクル

イネーブルになっているしきい値の数	評価サイクル[1]
1 ～ 20	2 分ごと
21 ～ 50	3 分ごと
51 ～ 100	5 分ごと

1. しきい値の評価にかかる時間が長くなると、評価サイクルが 2 分から 3 分、3 分から 5 分、5 分から 15 分に増加します。評価サイクル時間は、12 時間ごとに 2、3、および 5 分にリセットされます。

評価サイクルが開始されると、ACS はイネーブルになっている各しきい値を次々に評価します。しきい値に関連付けられているスケジュールでしきい値の実行が許可されている場合、ACS はしきい値条件を評価します。条件が満たされるとアラームがトリガーされます。詳細については、「アラームしきい値の作成、編集、および複製」（P.12-11）を参照してください。

（注）　システム アラームには関連付けられているスケジュールがなく、発生後即時に送信されます。システム アラームは全体としてだけイネーブルまたはディセーブルにすることができます。

ユーザへのイベントの通知

しきい値に達するかシステム アラームが生成されると、アラームが Web インターフェイスの [Alarms Inbox] に表示されます。このページから、アラームの詳細を表示したり、アラームに関するコメントを追加したりできます。また、ステータスを変更して、[Acknowledged] または [Closed] であることを示すことができます。

アラームをトリガーしたイベントを調査するときに役立つ関連レポートが 1 つ以上ある場合は、このページのアラーム詳細に、それらのレポートへのリンクが表示されます。

ダッシュボードには、最新の 5 つのアラームも表示されます。確認または終了したアラームは、ダッシュボードのこのリストから削除されます。

ACS では、次の形式で通知を受信するオプションが提供されています。

- 電子メール：アラーム詳細ページに表示されるすべての情報が含まれます。この電子メールを送信する必要がある受信者のリストを設定できます。ACS 5.4 には、HTML 形式の電子メールを介してイベントの通知を受信するオプションがあります。
- Syslog メッセージ：アラーム syslog ターゲットとして設定した Linux または Windows マシンに送信されます。最大 2 つのアラーム syslog ターゲットを設定できます。

受信ボックスでのアラームの表示および編集

ACS サーバから収集されたデータのセットに対するしきい値設定または規則に基づいて ACS が生成するアラームを表示できます。設定されたしきい値を満たしたアラームは、受信ボックスに送信されます。アラームを表示したあとで、アラームのステータスの編集、管理者へのアラームの割り当て、およびイベントをトラッキングするためのメモの追加を行うことができます。

受信ボックスのアラームを表示するには、[Monitoring and Reports] > [Alarms] > [Inbox] を選択します。

ACS によってトリガーされたアラームのリストがある [Inbox] ページが表示されます。表 12-2 に、[Alarms] ページのフィールドを示します。表 12-3 に、ACS 5.4 のシステム アラームと、その重大度を示します。

表 12-2　[Alarms] ページ

オプション	説明
Severity	*表示のみ*。関連付けられているアラームの重大度を示します。次のオプションがあります。 • Critical • Warning • Info
Name	アラームの名前を示します。クリックして [Alarms: Properties] ページを表示し、アラームを編集できます。

表 12-2　[Alarms] ページ （続き）

オプション	説明
Time	*表示のみ*。関連付けられているアラーム生成時刻を *Ddd Mmm dd hh:mm:ss timezone yyyy* 形式で示します。ここで、 • Ddd = Sun、Mon、Tue、Wed、Thu、Fri、Sat。 • Mmm = Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • dd = 日を表す 2 桁の数字。01 ～ 31。 • hh = 時間を表す 2 桁の数字。00 ～ 23。 • mm = 分を表す 2 桁の数字。00 ～ 59。 • ss = 秒を表す 2 桁の数字。00 ～ 59。 • *timezone* = タイムゾーン。 • yyyy = 年を表す 4 桁の数字。
Cause	*表示のみ*。アラームの原因を示します。
Assigned To	*表示のみ*。アラームを調査する担当者を示します。
Status	*表示のみ*。アラームのステータスが表示されます。次のオプションがあります。 • New：アラームは新規です。 • Acknowledged：アラームは既知です。 • Closed：アラームは終了しました。
Edit	編集するアラームの隣にあるチェックボックスをオンにし、[Edit] をクリックしてアラームのステータスを編集し、対応するレポートを表示します。
Close	終了するアラームの隣にあるチェックボックスをオンにし、[Close] をクリックしてアラームを終了します。アラームを終了する前に終了メモを入力できます。 アラームを終了すると、アラームがダッシュボードからだけ削除されます。アラーム自体は削除されません。
Delete	削除するアラームの隣にあるチェックボックスをオンにし、[Delete] をクリックしてアラームを削除します。

表 12-3　ACS 5.4 のシステム アラーム

アラーム	重大度
パージ関連のアラーム	
バックアップが失敗しました。データベースのパージの前に、バックアップが失敗しました。	Critical
バックアップが正常に行われました。データベースのパージの前に、バックアップが失敗しました。	Info
日次テーブルのデータベースの削除が失敗しました。例外で詳細が示されます。	Critical
月次テーブルのデータベースの削除が失敗しました。例外で詳細が示されます。	Critical
年次テーブルのデータベースの削除が失敗しました。例外で詳細が示されます。	Critical

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
増分バックアップが設定されていません。データベースのパージを正常に行うには、増分バックアップを設定する必要があります。これによってディスク領域の問題を回避できます。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actual db size GB です。	Warning
増分バックアップ データ リポジトリをリモート リポジトリとして設定してください。そうしないと、バックアップが失敗し、増分バックアップ モードがオフに変更されます。	Warning
パージの前に、データをバックアップするために使用するリモート リポジトリをパージ設定で設定します。	Warning
View データベース サイズが上限の maxlimit GB を超えています。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actualDBSize GB です。View データベース サイズが上限の maxLimit GB を超えています。	Critical
View データベース サイズが上限の upperLimit GB を超えています。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actualDBSize GB です。View データベース サイズが上限の upperLimit GB を超えています。	Critical
ACS View DB のサイズが下限の lowerLimit GB を超えています。View データベースのサイズは filesize GB で、ハード ディスク上で占有されるサイズは actualDBSize GB です。View データベース サイズが下限の lowerLimit GB を超えています。	Warning
DB の削除。データベースが削除を開始します。	Info
ディスク容量の制限の超過 - 次のウィンドウ：ディスク容量制限が、1 か月のデータで推奨されるしきい値を超過しました。下限に達するまで週次データを削除します。	Warning
ACS View アプリケーションが、許可された最大ディスク サイズを超えました。ディスク領域が推奨されるしきい値を超えました。余分な monthsinnumber か月のデータを削除します。	Warning
ACS View アプリケーションが、許可された最大ディスク サイズを超えました。ディスク領域が推奨されるしきい値を超えました。monthsinnumber か月のデータを削除します。	Info
削除が成功しました。View データベースに存在するレコードのサイズは actualsizeinGB GB です。ディスク上の View データベースの物理サイズは sizeinGB GB です。View データベースの物理サイズを減らす場合は、コマンドラインで ACS コンフィギュレーション モードから acsview-db-compress コマンドを実行します。	Warning
下限に達するまでパージ プロセスによって week 週のデータが削除されました。	Info
パージ プロセスが直前 3 週間のデータを削除して、下限に達するまで最大データを削除しようとしましたが、acsview データベース サイズが下限よりも大きいままです。現在、直前 1 週間のデータしか保管されていません。	Warning
入力ログ メッセージの数がしきい値（GB）に近づいています。メッセージの重要なカテゴリだけをログ コレクタに送信するように ACS を設定してください。	Warning
増分バックアップ	
オンデマンド完全バックアップが失敗しました。例外で詳細が示されます。	Critical
データベースの完全バックアップが失敗しました。例外で詳細が示されます。	Critical

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
データベース削除の完全バックアップが失敗しました。例外で詳細が示されます。	Critical
増分バックアップが失敗しました。例外で詳細が示されます。	Critical
増分リストアが成功しました。	Info
増分リストアが失敗しました。理由：例外で詳細が示されます。	Critical
オンデマンド完全バックアップが失敗しました。例外で詳細が示されます。	Critical
データベースの完全バックアップが失敗しました。例外で詳細が示されます。	Critical
データベース削除の完全バックアップが失敗しました。例外で詳細が示されます。	Critical
増分バックアップが失敗しました。例外で詳細が示されます。	Critical
ログのリカバリ	
ログ メッセージのリカバリが失敗しました。例外で詳細が示されます。	Critical
View の圧縮	
データベースの再構築操作が開始されました。ログ コレクタ サービスはこの操作中にシャット ダウンされ、再構築処理が完了した後で構成されます。ログのリカバリ オプションがすでにイネーブルの場合、再構築処理中に受信したログ メッセージがあれば、ログ コレクタ サービスの起動後にリカバリされます。	Critical
データベースのリロード操作が完了しました。	Info
システムがデータベースの圧縮の必要性を検出しました。メンテナンス ウィンドウで View データベースの圧縮操作を手動で実行してください。実行しない場合、ディスク領域の問題を避けるため、データベースの自動再構築がトリガーされます。	Warning
データベースの自動再構築操作が開始されました。ログ コレクタ サービスはこの操作中にシャット ダウンされ、再構築処理が完了した後で構成されます。ログのリカバリ オプションがすでにイネーブルの場合、再構築処理中に受信したログ メッセージがあれば、ログ コレクタ サービスの起動後にリカバリされます。	Critical
データベースのリロード操作が完了しました。	Info
データベースの自動再構築処理は、ディスク領域の問題を避けるために、データベースのサイズが上限を超えるとトリガーされます。ログ リカバリ機能をイネーブルにすると、データベースの再構築中に失われたログ メッセージをリカバリできます。データベースの再構築操作はログ リカバリ機能を有効にするまで継続しません。	Warning
しきい値のエグゼキュータ	
割り当てられた thresholdEvaluationInterval 分のインターバルで、すべてのしきい値の実行を完了できませんでした。しきい値は、次のインターバルで再度評価されます。このエラーは、次の場合に発生する可能性があります。システムに重い負荷がかかっている（例：パージなど）。現時点でアクティブなしきい値が多すぎる。	Info
セッション モニタ	
アクティブなセッションが制限値を超えています。セッションが 250000 を超えています。	Warning
Syslog Collector の失敗	

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
詳細についてはコレクタ ログを参照してください。	Critical
ACS のスケジュール バックアップ	
ACS 設定データベースのスケジュール バックアップは、バックアップ名に無効な文字があるために開始されませんでした。	Critical
ACS 設定データベースのスケジュール バックアップは、リポジトリが無効であるために開始できませんでした。リポジトリがあることを確認してください。	Critical
ホスト名を取得できません。ACS 設定データベースのスケジュール バックアップは失敗しました。詳細については、ADE.log を参照してください。	Critical
バックアップ ライブラリをロードできませんでした。ACS 設定データベースのスケジュール バックアップは失敗しました。詳細については、ADE.log を参照してください。	Critical
シンボル ルックアップのエラー。ACS 設定データベースのスケジュール バックアップは失敗しました。詳細については、ADE.log を参照してください。	Critical
内部エラーのため、ACS バックアップを実行できませんでした。詳細については、ADE.log を参照してください。	Critical
ディスク サイズの確認	
バックアップ サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、バックアップ プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
パッチ サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、パッチのインストール プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
サポート バンドル サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、サポート バンドル収集プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
バックアップ サイズの directorySize M が、許可されているクォータの MaxSize M を超えています。十分なディスク領域がある限り、復元プロセスは禁止されません。よりディスク領域が多いマシンに ACS を移動することを検討する必要があります。	Critical
ディスク クォータ	
ACS DB のサイズが許可されているクォータを超えました。	Critical
ACS View DB のサイズが許可されているクォータを超えました。	Critical
View データのアップグレード	
データベースの変換が正常に完了しました。View の newVersion データベースが installedVersion にアップグレードされ、アクティブ化する準備が整いました。	Warning
データベースの変換が正常に完了しませんでした。View の newVersion のアップグレード プロセスでエラーが発生し、完了できませんでした。アップグレード ログに詳細情報が含まれます。	Critical
その他	
アグリゲータがビジーです。Syslog はドロップされます。	Critical

表 12-3　ACS 5.4 のシステム アラーム （続き）

アラーム	重大度
コレクタがビジーです。Syslog はドロップされます。	Critical
登録解除された ACS サーバのサーバ名です。	Warning
不明なメッセージ コードを受信しました。	Critical

（注）　クォータを超える ACS データベースのアラームは、ACS データベースの合計サイズがクォータを超えた場合にだけ送信されます。ACS データベースの合計サイズ = acs*.log + acs.db で、acs*.log は ACS データベース ログ ファイルです。acs*.log および acs.db ファイルは、どちらも /opt/CSCOacs/db にあります。

（注）　ACS は、リモート syslog サーバとして使用できません。ただし、syslog サーバとして外部サーバを使用できます。syslog サーバとして外部サーバを使用する場合、syslog メッセージが外部の syslog サーバに送信されるため、ACS ビューではアラームを生成できません。ACS ビューでアラームを生成するには、CLI を使用してロギング オプションを localhost に設定します。

アラームを編集するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Inbox] を選択します。

ACS によってトリガーされたアラームのリストがある [Inbox] ページが表示されます。

ステップ 2　編集するアラームの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

次のタブがある [Inbox - Edit] ページが表示されます。

- [Alarm]：このタブは、アラームをトリガーしたイベントに関する詳細情報を示します。表 12-4 に、[Alarm] タブのフィールドを示します。[Alarm] タブのフィールドは編集できません。

表 12-4　[Inbox - Alarm] タブ

オプション	説明
Occurred At	アラームがトリガーされた日時。
Cause	アラームをトリガーしたイベント。
Detail	アラームをトリガーしたイベントに関する詳細情報。通常、ACS では、指定したしきい値を超過した項目のカウントがリストされます。
Report Links	イベントをさらに調査するための関連レポートがある場合は、それらのレポートへの 1 つ以上のハイパーリンクが表示されます。
Threshold	しきい値設定に関する情報。

- [Status]：このタブでは、アラームのステータスを編集したり、イベントをトラッキングするための説明を追加したりできます。

ステップ 3　必要に応じて、[Status] タブのフィールドを変更します。表 12-5 に、各フィールドを示します。

表 12-5　[Inbox - Status] タブ

オプション	説明
Status	アラームのステータス。アラームの生成時のステータスは [New] です。アラームを表示したあとで、アラームのステータスを [Acknowledged] または [Closed] に変更してアラームの現在のステータスを示します。
Assigned To	（任意）このアラームが割り当てられるユーザの名前を指定します。
Notes	（任意）記録するアラームに関する追加情報を入力します。

ステップ 4　[Submit] をクリックして変更を保存します。

変更が反映された [Alarms] ページが表示されます。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「アラームしきい値の削除」（P.12-33）

アラーム スケジュールについて

アラーム スケジュールを作成して、特定のアラームしきい値をいつ実行するかを指定できます。アラーム スケジュールを作成、編集、および削除できます。週 7 日のさまざまな時刻に実行するアラーム スケジュールを作成できます。

デフォルトでは、ACS には non-stop アラーム スケジュールが付属しています。このスケジュールは、1 日 24 時間、週 7 日にわたってイベントを監視します。

アラーム スケジュールのリストを表示するには、[Monitoring and Reports] > [Alarms] > [Schedules] を選択します。[Alarm Schedules] ページが表示されます。表 12-6 に、[Alarm Schedules] ページのフィールドを示します。

表 12-6　[Alarm Schedules] ページ

オプション	説明
Filter	検索基準に基づいてアラーム スケジュールをフィルタリングするための検索基準を入力します。
Go	検索を開始するには [Go] をクリックします。
Clear Filter	検索結果をクリアし、すべてのアラーム スケジュールをリストするには、[Clear Filter] をクリックします。
Name	アラーム スケジュールの名前。
Description	（任意）アラーム スケジュールの簡単な説明。

ここでは、次の内容について説明します。

- 「アラーム スケジュールの作成と編集」（P.12-10）
- 「しきい値へのアラーム スケジュールの割り当て」（P.12-10）
- 「アラーム スケジュールの削除」（P.12-11）

アラーム スケジュールの作成と編集

アラーム スケジュールを作成または編集するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Schedules] を選択します。

[Alarm Schedules] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 編集するアラーム スケジュールの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Alarm Schedules - Create or Edit] ページが表示されます。表 12-7 に、[Alarm Schedules - Create or Edit] ページのフィールドを示します。

表 12-7　[Alarm Schedules - Create or Edit] ページ

オプション	説明
ID	
Name	アラーム スケジュールの名前。名前は最大 64 文字です。
Description	アラーム スケジュールの簡単な説明。最大 255 文字です。
Schedule	
四角をクリックして、その時間を選択または選択解除します。前回の選択から開始するブロックを選択または選択解除するには、Shift キーを使用します。スケジュール ボックスの詳細については、「スケジュール ボックス」（P.5-17）を参照してください。	
Select All	1 日 24 時間、週 7 日にわたってイベントを監視するスケジュールを作成するには、[Select All] をクリックします。
Clear All	すべての選択を解除するには、[Clear All] をクリックします。
Undo All	スケジュールの編集時に、[Undo All] をクリックすると直前のスケジュールに戻ります。

ステップ 3　[Submit] をクリックしてアラーム スケジュールを保存します。

作成したスケジュールが [Threshold] ページの [Schedule] リスト ボックスに追加されます。

しきい値へのアラーム スケジュールの割り当て

アラームしきい値を作成する場合は、しきい値のアラーム スケジュールを割り当てる必要があります。アラーム スケジュールを割り当てるには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択します。

[Thresholds] ページが表示されます。

（注）　この手順では、しきい値にスケジュールを割り当てる方法についてだけ説明します。しきい値の作成、編集、または複製方法の詳細については、「アラームしきい値の作成、編集、および複製」（P.12-11）を参照してください。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 編集するしきい値の隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- 複製するしきい値の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

ステップ 3　[General] タブで、目的のスケジュールを [Schedule] ドロップダウン リスト ボックスから選択します。

ステップ 4　[Submit] をクリックしてしきい値にスケジュールを割り当てます。

アラーム スケジュールの削除

（注）　アラーム スケジュールを削除する前に、ACS で定義されているしきい値によって参照されていないことを確認します。デフォルトのスケジュール（nonstop）またはしきい値によって参照されているスケジュールは削除できません。

アラーム スケジュールを削除するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Schedules] を選択します。

[Alarm Schedules] ページが表示されます。

ステップ 2　削除するアラーム スケジュールの隣にあるチェックボックスをオンにし、[Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item(s)?
```

ステップ 3　アラーム スケジュールを削除するには [Yes] をクリックします。

アラーム スケジュール ページが表示されます。このとき、削除したスケジュールは表示されません。

アラームしきい値の作成、編集、および複製

このページは、各アラーム カテゴリのしきい値を設定する場合に使用します。最大 100 個のしきい値を設定できます。

アラーム カテゴリのしきい値を設定するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択します。

表 12-8 で説明する [Alarms Thresholds] ページが表示されます。

表 12-8　[Alarm Thresholds] ページ

オプション	説明
Name	アラームしきい値の名前。
Description	アラームしきい値の説明。
Category	アラームしきい値のカテゴリ。オプションは次のとおりです。 • Passed Authentications • Failed Authentications • Authentication Inactivity • TACACS Command Accounting • TACACS Command Authorization • ACS Configuration Changes • ACS System Diagnostics • ACS Process Status • ACS System Health • ACS AAA Health • RADIUS Sessions • Unknown NAD • External DB Unavailable • RBACL Drops • NAD-reported AAA Down
Last Modified Time	アラームしきい値がユーザによって最後に変更された時刻。
Last Alarm	関連付けられているアラームしきい値によってアラームが最後に生成された時刻。
Alarm Count	関連付けられているアラームが生成された回数。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するアラームの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するアラーム名をクリックします。または、変更するアラームの隣にあるチェックボックスをオンにして [Edit] をクリックします。
- イネーブルにするアラームの隣にあるチェックボックスをオンにし、[Enable] をクリックします。
- ディセーブルにするアラームの隣にあるチェックボックスをオンにし、[Disable] をクリックします。

ステップ 3　必要に応じて、[Thresholds] ページのフィールドを変更します。有効なフィールド オプションに関する情報については、以降のページを参照してください。

- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値基準の設定」（P.12-14）
- 「しきい値通知の設定」（P.12-32）

ステップ 4　[Submit] をクリックして設定を保存します。

アラームしきい値設定が保存されます。新しい設定を示す [Threshold] ページが表示されます。

関連トピック

- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値基準の設定」（P.12-14）
- 「しきい値通知の設定」（P.12-32）

一般的なしきい値情報の設定

一般的なしきい値情報を設定するには、[Thresholds] ページの [General] タブのフィールドに入力します。表 12-9 に、各フィールドを示します。

表 12-9　[General] タブ

オプション	説明
Name	しきい値の名前。
Description	（任意）しきい値の説明。
Enabled	このしきい値の実行を許可する場合に、このチェックボックスをオンにします。
Schedule	ドロップダウン リスト ボックスを使用して、しきい値を実行するスケジュールを選択します。使用可能なスケジュールのリストが表示されます。

関連トピック

- 「しきい値基準の設定」（P.12-14）
- 「しきい値通知の設定」（P.12-32）

しきい値基準の設定

ACS 5.4 には、異なるしきい値基準を定義するための次のしきい値カテゴリがあります。

Passed Authentications

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の成功した認証が調べられます。

これらの認証レコードは、ACS Instance、User、Identity Group などの共通属性によってグループ化されています。これらの各グループ内のレコード数が計算されます。これらのグループのいずれかで計算されたカウントが、指定したしきい値を超えた場合、アラームがトリガーされます。

たとえば、Passed authentications greater than 1000 in the past 20 minutes for an ACS instance というしきい値を設定するとします。ACS がこのしきい値を評価したときに、3 つの ACS インスタンスが成功した認証を次のように処理していたとします。

ACS インスタンス	成功した認証のカウント
New York ACS	1543
Chicago ACS	879
Los Angeles	2096

この場合、過去 20 分間に少なくとも 1 つの ACS インスタンスで成功した認証が 1000 を超えているため、アラームがトリガーされます。

（注）　1 つ以上のフィルタを指定して、しきい値評価の対象となる成功した認証を制限できます。各フィルタは認証レコード内の特定の属性に関連付けられており、フィルタ値が指定した値と一致したレコードだけがカウントされます。複数のフィルタを指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

表 12-10 の説明に従って、[Criteria] タブのフィールドを変更し、成功した認証の基準を持つしきい値を作成します。

表 12-10　Passed Authentications

オプション	説明
Passed Authentications	次のようにデータを入力します。 greater than *count* > **occurrences** |**%**> in the past *time* > Minutes | Hours for a *object*。ここで、 • *count* 値は、発生の絶対数またはパーセントです。次の値が有効です。 – *count* は、greater than に対して 0 ～ 99 の範囲である必要があります。 – *count* は、lesser than に対して 1 ～ 100 の範囲である必要があります。 • **occurrences** | **%**> 値は、occurrences（発生）または % です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel 分散展開では、2 つの ACS インスタンスがある場合、カウントはインスタンスごとに絶対数またはパーセンテージとして計算されます。ACS インスタンスのいずれかの個別のカウントが、指定したしきい値を超えた場合にだけ、ACS によってアラームがトリガーされます。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。
Identity Store	[Select] をクリックして、しきい値を設定する有効な ID ストア名を選択します。
Access Service	[Select] をクリックして、しきい値を設定する有効なアクセス サービス名を選択します。
MAC Address	[Select] をクリックして、しきい値を設定する有効な MAC アドレスを選択または入力します。このフィルタは、RADIUS 認証だけに使用できます。

表 12-10　Passed Authentications （続き）

オプション	説明
NAD Port	[Select] をクリックして、しきい値を設定するネットワーク デバイスのポートを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthZ Profile	[Select] をクリックして、しきい値を設定する認可プロファイルを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthN Method	[Select] をクリックして、しきい値を設定する認証方式を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP AuthN	[Select] をクリックして、しきい値を設定する EAP 認証値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP Tunnel	[Select] をクリックして、しきい値を設定する EAP トンネル値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

Failed Authentications

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の失敗した認証が調べられます。これらの認証レコードは、ACS Instance、User、Identity Group などの共通属性によってグループ化されています。

これらの各グループ内のレコード数が計算されます。これらのグループのいずれかで計算されたカウントが、指定したしきい値を超えた場合、アラームがトリガーされます。

たとえば、Failed authentications greater than 10 in the past 2 hours for Device IP というしきい値を設定するとします。ACS がこのしきい値を評価したときに、過去 2 時間に 4 つの IP アドレスに対して失敗した認証が次のように発生していたとします。

デバイス IP	失敗した認証のカウント
a.b.c.d	13
e.f.g.h	8
i.j.k.l	1
m.n.o.p	1

この場合、過去 2 時間に少なくとも 1 つのデバイス IP で失敗した認証が 10 を超えているため、アラームがトリガーされます。

（注）　1 つ以上のフィルタを指定して、しきい値評価の対象となる失敗した認証を制限できます。各フィルタは認証レコード内の特定の属性に関連付けられており、フィルタ値が指定した値と一致したレコードだけがカウントされます。複数のフィルタを指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

表 12-11 の説明に従って、[Criteria] タブのフィールドを変更し、失敗した認証の基準を持つしきい値を作成します。

表 12-11　Failed Authentications

オプション	説明
Failed Authentications	次のようにデータを入力します。 greater than *count* > **occurrences** | **%**> in the past *time*> *Minutes*|*Hours* for a *object*。ここで、 • *count* 値は、発生の絶対数またはパーセントです。有効な値は 0 ～ 99 の範囲です。 • **occurrences** | **%**> 値は、occurrences（発生）または % です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel 分散展開では、2 つの ACS インスタンスがある場合、カウントはインスタンスごとに絶対数またはパーセンテージとして計算されます。ACS インスタンスのいずれかの個別のカウントが、指定したしきい値を超えた場合にだけ、ACS によってアラームがトリガーされます。
フィルタ	
Failure Reason	[Select] をクリックして、しきい値を設定する有効な失敗理由名を入力します。
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

表 12-11　Failed Authentications （続き）

オプション	説明
Identity Store	[Select] をクリックして、しきい値を設定する有効な ID ストア名を選択します。
Access Service	[Select] をクリックして、しきい値を設定する有効なアクセス サービス名を選択します。
MAC Address	[Select] をクリックして、しきい値を設定する有効な MAC アドレスを選択または入力します。このフィルタは、RADIUS 認証だけに使用できます。
NAD Port	[Select] をクリックして、しきい値を設定するネットワーク デバイスのポートを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthZ Profile	[Select] をクリックして、しきい値を設定する認可プロファイルを選択します。このフィルタは、RADIUS 認証だけに使用できます。
AuthN Method	[Select] をクリックして、しきい値を設定する認証方式を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP AuthN	[Select] をクリックして、しきい値を設定する EAP 認証値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
EAP Tunnel	[Select] をクリックして、しきい値を設定する EAP トンネル値を選択します。このフィルタは、RADIUS 認証だけに使用できます。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

Authentication Inactivity

このしきい値が ACS で評価される場合、過去 31 日間までの指定した時間間隔中に発生した RADIUS または TACACS+ の認証が調べられます。指定した時間間隔中に認証が行われなかった場合、アラームがトリガーされます。

指定した時間間隔中に特定の ACS インスタンスまたはデバイス IP アドレスで認証が行われなかった場合にアラームを生成するフィルタを指定できます。

認証の非アクティブしきい値で指定した時間間隔が、継続的に実行されている集約ジョブの完了にかかった時間よりも短い場合は、このアラームが抑制されます。

集約ジョブは、毎日 00:05 に開始されます。23:50 から集約ジョブが完了するまで、認証の非アクティブ アラームは抑制されます。

たとえば、本日の 01:00 に集約ジョブが完了した場合、認証の非アクティブ アラームは 23:50 から 01:00 まで抑制されます。

（注）　00:05 から 05:00 までの間に ACS をインストールした場合、または 00:05 にメンテナンスのためにアプライアンスをシャットダウンしていた場合は、認証の非アクティブ アラームが 05:00 まで抑制されます。

このカテゴリを選択して、非アクティブな認証に基づくしきい値基準を定義します。表 12-12 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-12　Authentication Inactivity

オプション	説明
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device	[Select] をクリックして、しきい値を設定する有効なデバイスを選択します。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+
Inactive for	ドロップダウン リスト ボックスを使用して、次のいずれかの有効なオプションを選択します。 • [Hours]：1 ～ 744 の範囲の時間数を指定します。 • [Days]：1 ～ 31 の範囲の日数を指定します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

TACACS Command Accounting

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信した TACACS+ アカウンティング レコードが調べられます。

1 つ以上の TACACS+ アカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は前回と今回のアラーム評価サイクルの間に受信した TACACS+ アカウンティング レコードを調べます。I

1 つ以上の TACACS+ アカウンティング レコードが、指定したコマンドまたは特権レベルと一致した場合、アラームがトリガーされます。

1 つ以上のフィルタを指定して、しきい値評価の対象となるアカウンティング レコードを制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、TACACS コマンドに基づくしきい値基準を定義します。表 12-13 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-13　TACACS Command Accounting

オプション	説明
Command	しきい値を設定する TACACS コマンドを入力します。
Privilege	ドロップダウン リスト ボックスを使用して、しきい値を設定する特権レベルを選択します。有効なオプションは次のとおりです。 • Any • 0 ～ 15 の数字。
フィルタ	
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

TACACS Command Authorization

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信した TACACS+ アカウンティング レコードが調べられます。

1 つ以上の TACACS+ アカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は前回と今回のアラーム評価サイクルの間に受信した TACACS+ 認可レコードを調べます。

1 つ以上の TACACS+ 認可レコードが、指定したコマンド、特権レベル、および成功または失敗した結果と一致した場合、アラームがトリガーされます。

1 つ以上のフィルタを指定して、しきい値評価の対象となる認可レコードを制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、TACACS コマンド認可プロファイルに基づくしきい値基準を定義します。表 12-14 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-14　TACACS Command Authorization

オプション	説明
Command	しきい値を設定する TACACS コマンドを入力します。
Privilege	ドロップダウン リスト ボックスを使用して、しきい値を設定する特権レベルを選択します。有効なオプションは次のとおりです。 • Any • 0 ～ 15 の数字。

表 12-14　TACACS Command Authorization （続き）

オプション	説明
Authorization Result	ドロップダウン リスト ボックスを使用して、しきい値を設定する認可結果を選択します。有効なオプションは次のとおりです。 • Passed • Failed
フィルタ	
User	[Select] をクリックして、しきい値を設定する有効なユーザ名を選択または入力します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Device Name	[Select] をクリックして、しきい値を設定する有効なデバイス名を選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS Configuration Changes

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信したアカウンティング レコードが調べられます。

1 つ以上のアカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は前回と今回のアラーム評価サイクルの間に行われた ACS 設定変更を調べます。1 つ以上の変更が行われていた場合、アラームがトリガーされます。

1 つ以上のフィルタを指定して、しきい値評価の対象となる設定変更を制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ACS インスタンスで行われた設定変更に基づくしきい値基準を定義します。表 12-15 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-15　ACS Configuration Changes

オプション	説明
Administrator	[Select] をクリックして、しきい値を設定する有効な管理者ユーザ名を選択します。
Object Name	しきい値を設定するオブジェクトの名前を入力します。
Object Type	[Select] をクリックして、しきい値を設定する有効なオブジェクト タイプを選択します。

表 12-15　ACS Configuration Changes （続き）

オプション	説明
Change	ドロップダウン リスト ボックスを使用して、しきい値を設定する管理変更を選択します。有効なオプションは次のとおりです。 • Any • [Create] :「複製」および「編集」管理アクションを含みます。 • Update • Delete
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS System Diagnostics

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信したアカウンティング レコードが調べられます。

1 つ以上のアカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS は時間間隔中に監視対象の ACS が生成したシステム診断レコードを調べます。

1 つ以上の診断が指定したセキュリティ レベル以上で生成されていた場合、アラームがトリガーされます。1 つ以上のフィルタを指定して、しきい値評価の対象となるシステム診断レコードを制限できます。

各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ACS インスタンスのシステム診断に基づくしきい値基準を定義します。表 12-16 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-16　ACS System Diagnostics

オプション	説明
Severity at and above	ドロップダウン リスト ボックスを使用して、しきい値を設定する重大度レベルを選択します。この設定により、しきい値で指定した重大度レベルおよびそれよりも上の重大度レベルが取得されます。有効なオプションは次のとおりです。 • Fatal • Error • Warning • Info • Debug
Message Text	しきい値を設定するメッセージ テキストを入力します。最大文字数は 1024 文字です。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS Process Status

このしきい値が ACS で評価される場合、前回と今回のアラーム評価サイクルの間に受信したアカウンティング レコードが調べられます。

1 つ以上のアカウンティング レコードが一致した場合、前回のアラーム評価サイクルからの経過時間が計算されます。アクティブなしきい値の数に応じて、経過時間が 2、3、または 5 分に達した場合、ACS はその時間中にいずれかの ACS プロセスが失敗したかどうかを調べます。

ACS が 1 つ以上の失敗を検出した場合、アラームがトリガーされます。特定のプロセス、特定の ACS インスタンス、またはその両方のチェックに制限できます。

このカテゴリを選択して、ACS プロセス ステータスに基づくしきい値基準を定義します。表 12-17 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-17　ACS Process Status

オプション	説明
Monitor Processes	
ACS Database	ACS データベースをしきい値設定に追加する場合に、このチェックボックスをオンにします。
ACS Management	ACS 管理をしきい値設定に追加する場合に、このチェックボックスをオンにします。
ACS Runtime	ACS ランタイムをしきい値設定に追加する場合に、このチェックボックスをオンにします。
Monitoring and Reporting Database	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。

表 12-17　ACS Process Status （続き）

オプション	説明
Monitoring and Reporting Collector	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
Monitoring and Reporting Alarm Manager	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
Monitoring and Reporting Job Manager	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
Monitoring and Reporting Log Processor	このプロセスを監視する場合に、このチェックボックスをオンにします。このプロセスがダウンすると、アラームが生成されます。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS System Health

このしきい値が ACS で評価される場合、いずれかのシステム健全性パラメータが、過去 60 分間までの指定した時間間隔中に、指定したしきい値を超えたかどうかが調べられます。これらの健全性パラメータには、CPU 使用率やメモリ消費率などが含まれます。

パラメータのいずれかが指定したしきい値を超えた場合、アラームがトリガーされます。デフォルトでは、しきい値は展開されているすべての ACS インスタンスに適用されます。必要に応じて、1 つの ACS インスタンスだけにチェックを制限できます。

このカテゴリを選択して、ACS のシステム健全性に基づくしきい値基準を定義します。表 12-18 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-18　ACS System Health

オプション	説明
Average over the past	ドロップダウン リスト ボックスを使用して、設定に対して設定する時間を選択します。<min> は分で、次のいずれかです。 • 15 • 30 • 45 • 60
CPU	しきい値設定に対して設定する CPU 使用率を入力します。有効な範囲は 1 ～ 100 です。
Memory	しきい値設定に対して設定するメモリ使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk I/O	しきい値設定に対して設定するディスク使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。

表 12-18　ACS System Health （続き）

オプション	説明
Disk Space Used/opt	しきい値設定に対して設定する /opt ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk Space Used/local disk	しきい値設定に対して設定するローカル ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk Space Used/	しきい値設定に対して設定する / ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
Disk Space Used/tmp	しきい値設定に対して設定する一時ディスク領域の使用率（指定した値以上）を入力します。有効な範囲は 1 ～ 100 です。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

ACS AAA Health

このしきい値が ACS で評価される場合、いずれかの ACS 健全性パラメータが、過去 60 分間までの指定した時間間隔中に、指定したしきい値を超えたかどうかが調べられます。ACS は次のパラメータを監視します。

- RADIUS Throughput
- TACACS Throughput
- RADIUS Latency
- TACACS Latency

パラメータのいずれかが指定したしきい値を超えた場合、アラームがトリガーされます。デフォルトでは、しきい値は展開されているすべての監視対象 ACS インスタンスに適用されます。必要に応じて、1 つの ACS インスタンスだけにチェックを制限できます。

表 12-19 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-19　ACS AAA Health

オプション	説明
Average over the past	ドロップダウン リスト ボックスを使用して、設定に対して設定する時間を選択します。<min> は分で、次のいずれかです。 • 15 • 30 • 45 • 60
RADIUS Throughput	しきい値設定に対して設定する 1 秒あたりの RADIUS トランザクション数（指定した値以下）を入力します。有効な範囲は 1 ～ 999999 です。
TACACS Throughput	しきい値設定に対して設定する 1 秒あたりの TACACS トランザクション数（指定した値以下）を入力します。有効な範囲は 1 ～ 999999 です。
RADIUS Latency	しきい値設定に対して設定する RADIUS 遅延（指定した値以上）をミリ秒単位で入力します。有効な範囲は 1 ～ 999999 です。
TACACS Latency	しきい値設定に対して設定する TACACS+ 遅延（指定した値以上）をミリ秒単位で入力します。有効な範囲は 1 ～ 999999 です。
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

RADIUS Sessions

このしきい値が ACS で評価される場合、セッションのアカウンティング開始イベントが受信されていない認証済み RADIUS セッションが過去 15 分間に発生したかどうかが判断されます。これらのイベントは、デバイス IP アドレスでグループ化され、いずれかのデバイス IP に対する発生カウントが指定したしきい値を超過した場合にアラームがトリガーされます。フィルタを設定して、評価を 1 つのデバイス IP に制限できます。

このカテゴリを選択して、RADIUS セッションに基づくしきい値基準を定義します。表 12-20 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-20　RADIUS Sessions

オプション	説明
More than *num* authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	*num*：過去 15 分間の認証済みセッションの数。

表 12-20　RADIUS Sessions （続き）

オプション	説明
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。

Unknown NAD

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の失敗した認証が調べられます。これらの失敗した認証から、ACS は失敗理由が [Unknown NAD] である認証を識別します。

未知のネットワーク アクセス デバイス（NAD）認証レコードは、ACS インスタンス、ユーザなどの共通属性によってグループ化され、各グループ内のレコード カウントが計算されます。いずれかのグループのレコード カウントが指定したしきい値を超えた場合、アラームがトリガーされます。これは、たとえば、しきい値を次のように設定した場合に発生します。

Unknown NAD count greater than 5 in the past 1 hour for a Device IP

過去 1 時間に未知の NAD の失敗理由で失敗した認証が 2 つの異なるデバイス IP アドレスに対して次の表のように発生した場合は、少なくとも 1 つのデバイス IP アドレスのカウントが 5 を超えているためアラームがトリガーされます。

デバイス IP	未知の NAD 認証レコードのカウント
a.b.c.d	6
e.f.g.h	1

1 つ以上のフィルタを指定して、しきい値評価の対象となる失敗した認証を制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、未知の NAD により失敗した認証に基づくしきい値基準を定義します。表 12-21 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-21　Unknown NAD

オプション	説明
Unknown NAD count	greater than *num* in the past *time Minutes|Hours* for a *object*。ここで、 • *num* 値は、ゼロ（0）以上の 5 桁の任意の数字です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – Device IP
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

External DB Unavailable

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した RADIUS または TACACS+ の失敗した認証が調べられます。

これらの失敗した認証から、ACS は失敗理由が [External DB unavailable] である認証を識別します。この失敗理由を持つ認証レコードは、ACS インスタンス、ユーザなどの共通属性によってグループ化され、各グループ内のレコード カウントが計算されます。

いずれかのグループのレコード カウントが指定したしきい値を超えた場合、アラームがトリガーされます。これは、たとえば、しきい値を次のように設定した場合に発生します。

デバイス IP の過去 1 時間の [External DB Unavailable] 数が 5 よりも大きい

過去 1 時間に [External DB Unavailable] の失敗理由で失敗した認証が 2 つの異なるデバイス IP アドレスに対して次の表のように発生した場合は、少なくとも 1 つのデバイス IP アドレスのカウントが 5 を超えているためアラームがトリガーされます。

デバイス IP	外部 DB が使用不能な認証レコードのカウント
a.b.c.d	6
e.f.g.h	1

1 つ以上のフィルタを指定して、しきい値評価の対象となる失敗した認証を制限できます。各フィルタはレコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ACS が接続できない外部データベースに基づくしきい値基準を定義します。表 12-22 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-22　External DB Unavailable

オプション	説明
External DB Unavailable	*percent*|*count* greater than *num* in the past *time Minutes*|*Hours* for a *object*。ここで、 • Percent|Count 値は Percent（パーセント）または Count（カウント）です。 • *num* 値は次のいずれかです。 – パーセントの場合は 0 ～ 99 – カウントの場合は 0 ～ 99999 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – ACS Instance – Identity Store
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Identity Group	[Select] をクリックして、しきい値を設定する有効な ID グループ名を選択します。
Identity Store	[Select] をクリックして、しきい値を設定する有効な ID ストア名を選択します。
Access Service	[Select] をクリックして、しきい値を設定する有効なアクセス サービス名を選択します。
Protocol	ドロップダウン リスト ボックスを使用して、しきい値に対して使用するプロトコルを設定します。有効なオプションは次のとおりです。 • RADIUS • TACACS+

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

RBACL Drops

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した Cisco Security Group Access RBACL ドロップが調べられます。RBACL ドロップ レコードは、NAD、SGT などの特定の共通属性によってグループ化されます。

これらの各グループ内のこのようなレコードのカウントが計算されます。いずれかのグループのカウントが指定したしきい値を超えた場合、アラームがトリガーされます。たとえば、次のしきい値設定について考えます。

SGT による過去 4 時間の [RBACL Drops] が 10 よりも大きい

過去 4 時間に RBACL ドロップが 2 つの異なる送信元グループ タグに対して次の表のように発生した場合は、少なくとも 1 つの SGT のカウントが 10 を超えているためアラームがトリガーされます。

SGT	RBACL ドロップのカウント
1	17
3	14

1 つ以上のフィルタを指定して、しきい値評価の対象となる RBACL ドロップ レコードを制限できます。各フィルタは RBACL ドロップ レコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

表 12-23 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-23　RBACL Drops

オプション	説明
RBACL drops	greater than *num* in the past *time Minutes|Hours* by a *object*。ここで、 • *num* 値は、ゼロ（0）以上の 5 桁の任意の数字です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – NAD – SGT – DGT – DST_IP
フィルタ	
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
SGT	[Select] をクリックして、しきい値を設定する有効な送信元グループ タグを選択または入力します。
DGT	[Select] をクリックして、しきい値を設定する有効な宛先グループ タグを選択または入力します。
Destination IP	[Select] をクリックして、しきい値を設定する有効な宛先 IP アドレスを選択または入力します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

NAD-Reported AAA Downtime

このしきい値が ACS で評価される場合、過去 24 時間までの指定した時間間隔中に発生した NAD レポート AAA ダウン イベントが調べられます。AAA ダウン レコードは、IP アドレスやデバイス グループなどの特定の共通属性によってグループ化され、各グループ内のレコード カウントが計算されます。

いずれかのグループのカウントが指定したしきい値を超えた場合、アラームがトリガーされます。たとえば、次のしきい値設定について考えます。

AAA Down count greater than 10 in the past 4 hours by a Device IP

過去 4 時間に NAD レポート AAA ダウン イベントが 3 つの異なるデバイス IP アドレスに対して次の表のように発生した場合は、少なくとも 1 つのデバイス IP アドレスのカウントが 10 を超えているためアラームがトリガーされます。

デバイス IP	NAD レポート AAA ダウン イベントのカウント
a.b.c.d	15
e.f.g.h	3
i.j.k.l	9

1 つ以上のフィルタを指定して、しきい値評価の対象となる AAA ダウン レコードを制限できます。各フィルタは AAA ダウン レコード内の特定の属性に関連付けられており、フィルタ条件と一致したレコードだけがカウントされます。複数のフィルタ値を指定した場合は、すべてのフィルタ条件と一致したレコードだけがカウントされます。

このカテゴリを選択して、ネットワーク アクセス デバイスがレポートする AAA ダウンタイムに基づくしきい値基準を定義します。表 12-24 の説明に従って、[Criteria] タブのフィールドを変更します。

表 12-24　NAD-Reported AAA Downtime

オプション	説明
AAA down	greater than *num* in the past *time Minutes|Hours* by a *object*。ここで、 • *num* 値は、ゼロ（0）以上の 5 桁の任意の数字です。 • *time* 値は、1 ～ 1440 分、つまり 1 ～ 24 時間です。 • Minutes|Hours 値は、Minutes（分）または Hours（時間）です。 • *object* 値は、次のいずれかです。 – Device IP – Device Group

表 12-24　NAD-Reported AAA Downtime （続き）

オプション	説明
フィルタ	
ACS Instance	[Select] をクリックして、しきい値を設定する有効な ACS インスタンスを選択します。
Device IP	[Select] をクリックして、しきい値を設定する有効なデバイス IP アドレスを選択または入力します。
Device Group	[Select] をクリックして、しきい値を設定する有効なデバイス グループ名を選択します。

関連トピック

- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「一般的なしきい値情報の設定」（P.12-13）
- 「しきい値通知の設定」（P.12-32）

しきい値通知の設定

このページは、アラームしきい値通知を設定する場合に使用します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択し、次のいずれかを実行します。

- [Create] をクリックして、新しいアラームしきい値を作成します。
- アラームしきい値の名前をクリックするか、既存のアラームしきい値の隣にあるチェックボックスをオンにし、[Edit] をクリックして、選択したアラームしきい値を編集します。
- アラームしきい値の名前をクリックするか、既存のアラームしきい値の隣にあるチェックボックスをオンにし、[Duplicate] をクリックして、選択したアラームしきい値を複製します。

ステップ 2　[Notifications] タブをクリックします。

表 12-25 で説明する [Thresholds: Notifications] ページが表示されます。

表 12-25　[Thresholds: Notifications] ページ

オプション	説明
Severity	ドロップダウン リスト ボックスを使用して、アラームしきい値の重大度レベルを選択します。有効なオプションは次のとおりです。 • Critical • Warning • Info
Send Duplicate Notifications	重複するアラームを通知する場合に、このチェックボックスをオンにします。同じしきい値に対して以前に生成されたアラームが現在のアラームに対して指定された時間枠内に発生した場合は、アラームが重複と見なされます。

表 12-25　[Thresholds: Notifications] ページ （続き）

オプション	説明
Email Notification	
Email Notification User List	電子メール アドレスまたは ACS 管理者名あるいはその両方のカンマ区切りリストを入力します。次のいずれかを実行します。 • 電子メール アドレスを入力します。 • [Select] をクリックして、有効な ACS 管理者名を入力します。管理者設定に電子メール識別情報が指定されている場合にだけ、関連付けられた管理者に電子メールで通知されます。詳細については、「管理者アカウントの作成、複製、編集、および削除」（P.16-7）を参照してください。 しきい値アラームが発生した場合は、[Email Notification User List] 内のすべての受信者に電子メールが送信されます。 このフィールドをクリアするには、[Clear] をクリックします。
Email in HTML Format	電子メール通知を HTML 形式で送信する場合は、このチェックボックスをオンにします。電子メール通知をプレーン テキストで送信する場合は、このチェックボックスをオフにします。
Custom Text	アラームしきい値に関連付けるカスタム テキスト メッセージを入力します。
Syslog Notification	
Send Syslog Message	ACS で生成される各システム アラームの syslog メッセージを送信する場合に、このチェックボックスをオンにします。 （注）　ACS で syslog メッセージを正常に送信するには、[Alarm Syslog Targets] を設定する必要があります。これは、syslog メッセージの宛先です。詳細については、「アラーム Syslog ターゲットについて」（P.12-35）を参照してください。

関連トピック

- 「受信ボックスでのアラームの表示および編集」（P.12-3）
- 「アラームしきい値の作成、編集、および複製」（P.12-11）
- 「アラームしきい値の削除」（P.12-33）

アラームしきい値の削除

アラームしきい値を削除するには、次の手順を実行します。

ステップ 1　[Monitoring and Reports] > [Alarms] > [Thresholds] を選択します。

[Alarms Thresholds] ページが表示されます。

ステップ 2　削除するしきい値の隣にあるチェックボックスを 1 つ以上オンにして、[Delete] をクリックします。

ステップ 3　[OK] をクリックして、選択したアラームを削除することを確認します。

[Alarms Thresholds] ページが表示されます。このとき、削除されたしきい値は表示されません。

システム アラーム設定の設定

システム アラームは、次の情報をユーザに通知するために使用されます。

- Monitoring and Reporting サービスで発生したエラー
- データの削除に関する情報

このページは、システム アラームをイネーブルにしたり、アラーム通知の送信先を指定したりする場合に使用します。システム アラームをイネーブルにした場合は、アラームが [Alarms Inbox] に送信されます。また、選択した受信者にアラーム通知を電子メールで送信することや、アラーム syslog ターゲットとして指定された宛先に syslog メッセージとして送信することを選択できます。

Monitoring and Report Viewer から、[Monitoring Configuration] > [System Configuration] > [System Alarm Settings] を選択します。

表 12-26　[System Alarm Settings] ページ

オプション	説明
System Alarm Settings	
Notify System Alarms	システム アラーム通知をイネーブルにする場合に、このチェックボックスをオンにします。
System Alarms Suppress Duplicates	ドロップダウン リスト ボックスを使用して、重複するシステム アラームが [Email Notification User List] に送信されないようにする時間数を指定します。有効なオプションは、1、2、4、6、8、12、および 24 です。
Email Notification	
Email Notification User List	電子メール アドレスまたは ACS 管理者名あるいはその両方のカンマ区切りリストを入力します。次のいずれかを実行します。 • 電子メール アドレスを入力します。 • [Select] をクリックして、有効な ACS 管理者名を入力します。管理者設定に電子メール識別情報が指定されている場合にだけ、関連付けられた管理者に電子メールで通知されます。詳細については、「管理者アカウントの作成、複製、編集、および削除」（P.16-7）を参照してください。 システム アラームが発生した場合は、[Email Notification User List] 内のすべての受信者に電子メールが送信されます。 このフィールドをクリアするには、[Clear] をクリックします。
Email in HTML Format	電子メール通知を HTML 形式で送信する場合は、このチェックボックスをオンにします。電子メール通知をプレーン テキストで送信する場合は、このチェックボックスをオフにします。
Syslog Notification	
Send Syslog Message	ACS で生成される各システム アラームの syslog メッセージを送信する場合に、このチェックボックスをオンにします。 ACS で syslog メッセージを正常に送信するには、[Alarm Syslog Targets] を設定する必要があります。これは、syslog メッセージの宛先です。詳細については、「アラーム Syslog ターゲットについて」（P.12-35）を参照してください。

ここでは、次の内容について説明します。

- 「アラーム Syslog ターゲットの作成と編集」（P.12-35）
- 「アラーム Syslog ターゲットの削除」（P.12-36）

アラーム Syslog ターゲットについて

アラーム syslog ターゲットは、アラーム syslog メッセージが送信される宛先です。Monitoring and Report Viewer は、syslog メッセージの形式でアラーム通知を送信します。これらの syslog メッセージを受信するように、syslog サーバを実行するマシンを設定する必要があります。

設定した syslog ターゲットのリストを表示するには、[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets] を選択します。

（注）　Monitoring and Report Viewer で、最大 2 つの syslog ターゲットを設定できます。

ここでは、次の内容について説明します。

- 「アラーム Syslog ターゲットの作成と編集」（P.12-35）
- 「アラーム Syslog ターゲットの削除」（P.12-36）

アラーム Syslog ターゲットの作成と編集

アラーム syslog ターゲットを作成または編集するには、次の手順を実行します。

ステップ 1　[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets] を選択します。

[Alarm Syslog Targets] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 編集するアラーム syslog ターゲットの隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Alarm Syslog Targets Create or Edit] ページが表示されます。

ステップ 3　表 12-27 で説明されているフィールドを変更します。

表 12-27　[Alarm Syslog Targets Create or Edit] ページ

オプション	説明
ID	
Name	アラーム syslog ターゲットの名前。名前は最大 255 文字です。
Description	（任意）作成するアラームの簡単な説明。説明は最大 255 文字です。
Configuration	
IP Address	syslog メッセージを受信するマシンの IP アドレス。このマシンでは、syslog サーバを実行している必要があります。Windows または Linux マシンを使用して syslog メッセージを受信することを推奨します。

表 12-27　[Alarm Syslog Targets Create or Edit] ページ （続き）

オプション	説明
Use Advanced Syslog Options	
Port	リモート syslog サーバが受信するポート。デフォルトでは、514 に設定されます。有効なオプションは 1 ～ 65535 です。
Facility Code	ロギングに使用する Syslog ファシリティ コード。有効なオプションは、Local0 ～ Local7 です。

ステップ 4　[Submit] をクリックします。

関連トピック

- 「アラーム Syslog ターゲットについて」（P.12-35）
- 「アラーム Syslog ターゲットの削除」（P.12-36）

アラーム Syslog ターゲットの削除

（注）　デフォルトの *nonstop* スケジュールは削除できません。

アラーム syslog ターゲットを削除するには、次の手順を実行します。

ステップ 1　[Monitoring Configuration] > [System Configuration] > [Alarm Syslog Targets] を選択します。

[Alarm Syslog Targets] ページが表示されます。

ステップ 2　削除するアラーム syslog ターゲットの隣にあるチェックボックスをオンにし、[Delete] をクリックします。

次のメッセージが表示されます。

```
Do you want to delete the selected item(s)?
```

ステップ 3　[Yes] をクリックします。

[Alarm Syslog Targets] ページが表示されます。このとき、削除したアラーム syslog ターゲットは表示されません。