IBM Security QRadar
バージョン **7.2.6**

システム通知のトラブルシューティング

IBM

注記

本書および本書で紹介する製品を使用する前に、 47 ページの『特記事項』に記載されている情報をお読みください。

この資料は、IBM QRadar Security Intelligence Platform V7.2.6 に適用されます。また、この資料の更新版が公開されない限り、これ以降のリリースにも適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar
Version 7.2.6
Troubleshooting System Notifications

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

システム通知の概要

「IBM® Security QRadar® システム通知のトラブルシューティング」では、QRadar コンソールに表示されるシステム通知をトラブルシューティングおよび解決する方法について説明します。コンソールに表示されるシステム通知は、デプロイメント内のすべてのアプライアンスまたは QRadar 製品に適用できます。

特に明記されていない限り、QRadar を参照しているすべての箇所は、以下の製品を参照していることがあります。

- IBM Security QRadar SIEM
- IBM Security QRadar Log Manager

対象読者

QRadar システムのインストールと構成を担当するネットワーク管理者は、ネットワーク・セキュリティーの概念および Linux オペレーティング・システムを十分に理解している必要があります。

技術資料

IBM Security QRadar の製品資料を Web で入手するには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。各言語に翻訳された資料もすべて用意されています。

QRadar 製品ライブラリーでより技術的な資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせ方法については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、

製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意:

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar システム通知のトラブルシューティング

IBM Security QRadar によって生成されたシステム通知を使用して、システムの状況および正常性をモニターします。ソフトウェアおよびハードウェアのツールとプロセスは、継続的に QRadar アプライアンスをモニターし、ユーザーおよび管理者に情報、警告、エラー・メッセージを配信します。

関連概念:

3 ページの『第 2 章 QRadar アプライアンスのエラー通知』
IBM Security QRadar 製品のエラー通知には、ユーザーまたは管理者の応答が必要です。

19 ページの『第 3 章 QRadar アプライアンスの警告通知』
IBM Security QRadar システム正常性の通知は、ソフトウェアまたはハードウェアの実際の障害または切迫した障害のプロアクティブなメッセージです。

43 ページの『第 4 章 QRadar アプライアンスの情報通知』
IBM Security QRadar は、プロセスまたはアクションの状況または結果に関する情報メッセージを提供します。

第 2 章 QRadar アプライアンスのエラー通知

IBM Security QRadar 製品のエラー通知には、ユーザーまたは管理者の応答が必要です。

メモリー不足エラー

38750004 - アプリケーションのメモリーが不足しています。

説明

システムで、これ以上メモリーまたはスワップ・スペースが使用できないことが検出されると、アプリケーションまたはサービスが動作を停止する場合があります。メモリー不足という問題は、ソフトウェアまたはユーザー定義の、多量の使用可能メモリーを消費する照会や操作によって発生します。

ユーザー応答

/var/log/qradar.log ファイルに書き込まれたエラー・メッセージを確認してください。サービスを再開することで、害を与えているアプリケーションまたはサービスが停止され、リソースが再配分される可能性があります。

Java™ Database Connectivity (JDBC) またはログ・ファイル・プロトコルを使用してログ・ソースから多くのレコードをインポートすると、システムがリソースを使い果たす場合があります。複数の大規模データのインポートが同時に発生する場合、開始時刻の間隔をずらすという方法が考えられます。

ディスク使用率がしきい値を超えた

38750038 - ディスク監視機能: ディスク使用量が最大しきい値を超えました。

説明

システム上の少なくとも 1 つのディスクの使用率が 95% になっています。

システムでのデータ破損を防止するために、プロセスがシャットダウンされます。

ユーザー応答

ファイルを手動で削除するか、イベントまたはフローのデータ保存ポリシーを変更することで、ディスク・スペースを解放してください。容量の 92% というしきい値を下回るのに十分なディスク・スペースを解放すると、システムはプロセスを自動的に再開します。

プロセス・モニター・アプリケーションの開始に複数回失敗した

38750043 - プロセス・モニター: アプリケーションの開始に複数回失敗しました。

説明

システムが、システム上でアプリケーションまたはプロセスを開始できません。

ユーザー応答

フロー・ソースを調べて、デバイスがフロー・データの送信を停止したかどうか、ユーザーがフロー・ソースを削除したかどうかを確認してください。

デプロイメント・エディターを使用してフロー・プロセスを削除するか、フロー・ソースをフロー・データに割り当ててください。「管理」タブで、「フロー・ソース」をクリックします。

プロセス・モニターのディスク使用量を下げる必要がある

38750045 - プロセス・モニター: ディスク使用量を削減する必要があります。

説明

プロセス・モニターは、システム・リソースが不足しているため、プロセスを開始できません。システム上のストレージ区画は、ほぼ 95% 以上です。

ユーザー応答

ファイルを手動で削除するか、イベントまたはフローのデータ保存ポリシーを変更することで、ディスク・スペースを解放してください。使用されているディスク・スペースが容量の 92% というしきい値を下回ると、システムはシステム・プロセスを自動的に再開します。

イベント・パイプラインによってイベントが除去された

38750060 - イベント・パイプラインによってイベント/フローが除去されました。

説明

イベント・パイプラインに問題があるか、ライセンス制限を超えた場合、イベントまたはフローが除去される可能性があります。

除去されたイベントおよびフローは、復旧できません。

ユーザー応答

以下の選択肢を確認してください。

- システム上の受信イベントとフローの速度を確認してください。イベント・パイプラインがイベントを除去している場合、より多くのデータを扱うようにライセンス内容を拡張してください。
- ルールやカスタム・プロパティーに対する最近の変更を確認してください。ルールやカスタム・プロパティーの変更によって、イベントやフローの速度が変わることがあり、システム・パフォーマンスに影響する可能性があります。

- 問題が SAR 通知に関連しているかどうかを判別してください。SAR 通知が、キューに入れられたイベントおよびフローがイベント・パイプラインにあることを示している可能性があります。システムは、通常、イベントを除去する代わりにストレージにルーティングします。
- イベント・パイプラインに入るイベントとフローの量を削減するようにシステムをチューニングしてください。

イベント・パイプラインによって接続が除去された

38750061 - イベント・パイプラインによって接続が除去されました。

説明

TCP ベースのプロトコルによって、システムに対して確立された接続が除去されました。

接続の確立とイベントの転送を確実に行うために、TCP ベースのプロトコルによって確立できる接続の数は制限されています。イベント・コレクション・サーバー (ECS) では、最大 15,000 個のファイル・ハンドルが許可され、各 TCP 接続は 3 個のファイル・ハンドルを使用します。

接続除去の通知を発行する TCP プロトコルには、次のプロトコルがあります。

- TCP syslog プロトコル
- TLS syslog プロトコル
- TCP 複数行プロトコル

ユーザー応答

以下の選択肢を確認してください。

- より価格のアプライアンスにイベントを分散させてください。他のイベント・プロセッサーおよびフロー・プロセッサーへの接続により、コンソールからの作業負荷が分散されます。
- 低い優先順位の TCP ログ・ソース・イベントは、UDP ネットワーク・プロトコルを使用するように構成してください。
- イベント・パイプラインに入るイベントとフローの量を削減するようにシステムをチューニングしてください。

自動更新エラー

38750066 - 自動更新はインストールを完了できませんでした。詳しくは、「自動更新ログ」を参照してください。

説明

更新プロセスでエラーが発生し、更新サーバーに接続できません。システムは更新されません。

ユーザー応答

次のオプションのいずれかを選択します。

- 自動更新履歴を調べて、インストール・エラーの原因を判別してください。

  「管理」タブで、「自動更新」アイコンをクリックし、「ログの表示」を選択します。
- コンソールが更新サーバーに接続できることを確認してください。

  「更新」ウィンドウで、「設定の変更」を選択し、「拡張」タブをクリックして、 tab 自動更新構成を表示します。「**Web** サーバー」フィールドのアドレスを調べて、自動更新サーバーにアクセスできることを確認してください。

自動更新はインストールされたが、エラーが発生した

38750067 - 自動更新はインストールされましたが、エラーが発生しました。詳しくは、「自動更新ログ」を参照してください。

説明

自動更新エラーの最も一般的な理由は、DSM、プロトコル、またはスキャナー更新用のソフトウェア依存関係が欠落していることです。

ユーザー応答

次のオプションのいずれかを選択します。

- 「管理」タブで、「自動更新」アイコンをクリックし、「更新履歴の表示」を選択します。失敗した RPM の表示、選択、および再インストールを実行できます。
- 自動更新がユーザー・インターフェース経由で再インストールを実行できない場合は、欠落している依存関係を手動でコンソールにダウンロードし、インストールしてください。コンソールによって、インストールされたファイルがすべての管理対象ホストに複製されます。

スタンバイ HA システム障害

38750080 - スタンバイ HA システム障害。

説明

セカンダリー・アプライアンスの状況が「失敗」に切り替わり、システムに HA 保護がなくなっています。

ユーザー応答

以下の解決策を確認してください。

- セカンダリー・システムをリストアしてください。

  「管理」タブをクリックし、「システムおよびライセンス管理」をクリックして、「システムのリストア」をクリックします。

- セカンダリー HA アプライアンスを調べて、電源が遮断されたか、ハードウェア障害が発生したかを判別してください。
- **ping** コマンドを使用して、プライマリー・システムとスタンバイ・システムとの通信を確認してください。
- プライマリー HA アプライアンスとセカンダリー HA アプライアンスを接続するスイッチを確認してください。

  プライマリー・アプライアンスおよびセカンダリー・アプライアンス上で IPtables を確認してください。
- スタンバイ・アプライアンスの /var/log/qradar.log ファイルを調べて、障害の原因を判別してください。

アクティブ高可用性 (HA) システム障害

38750081 - アクティブ HA システム障害。

説明

アクティブ・システムが応答しないか、障害が発生しているため、アクティブ・システムがスタンバイ・システムと通信できません。スタンバイ・システムが、障害が発生しているアクティブ・システムから運用をテークオーバーします。

ユーザー応答

以下の解決策を確認してください。

- アクティブ HA アプライアンスを調べて、電源が遮断されたか、ハードウェア障害が発生したかを判別してください。
- アクティブ・システムが HA プライマリーの場合、アクティブ・システムをリストアします。

  「管理」タブをクリックし、「システムおよびライセンス管理」をクリックします。「高可用性」メニューから、「システムのリストア」オプションを選択します。
- スタンバイ・アプライアンスの /var/log/qradar.log ファイルを調べて、障害の原因を判別してください。
- **ping** コマンドを使用して、アクティブ・システムとスタンバイ・システムとの通信を確認してください。
- アクティブ HA アプライアンスとスタンバイ HA アプライアンスを接続するスイッチを確認してください。

  アクティブ・アプライアンスおよびスタンバイ・アプライアンス上で IPtables を確認してください。

高可用性のインストールに失敗した

38750086 - クラスターに高可用性をインストール中に問題が発生しました。

説明

高可用性 (HA) アプライアンスをインストールするときに、インストール・プロセスは、プライマリー・アプライアンスおよびセカンダリー・アプライアンスをリンクします。構成プロセスおよびインストール・プロセスには、インストールでいつ注意を喚起する必要があるかを決定する時間間隔があります。ハイ・アベイラビリティーのインストールが、6 時間という制限時間を超えました。

HA 保護は、問題が解決されるまで利用できません。

ユーザー応答

お客様サポートにお問い合わせください。

HA アプライアンスのアンインストールに失敗した

38750087 - クラスターから高可用性を削除中に問題が発生しました。

説明

高可用性 (HA) アプライアンスを削除するときに、インストール・プロセスは、プライマリー・アプライアンスとセカンダリー・アプライアンスとの間の接続とデータ複製プロセスを削除します。インストール・プロセスが HA アプライアンスをクラスターから正しく削除できない場合、プライマリー・システムは正常な動作を続行します。

ユーザー応答

もう 1 度、高可用性アプライアンスを削除してみてください。

スキャナー初期化エラー

38750089 - スキャナーが初期化に失敗しました。

説明

スケジュールされた脆弱性スキャンが、スキャンのインポート・プロセスを開始するために外部のスキャナーに接続できません。

スキャン初期化の問題は、通常、資格情報の問題、またはリモート・スキャナーへの接続の問題によって発生します。初期化に失敗したスキャナーは、状況が失敗であるスケジュールされたスキャンのホバー・テキストに詳細なエラー・メッセージを表示します。

ユーザー応答

次の手順を実行します。

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「**VA** スキャナーのスケジュール」アイコンをクリックします。

4. スキャナー・リストで、任意のスキャナーの「状況」列にカーソルを移動して、正常終了または失敗の詳細なメッセージを表示します。

スキャン障害エラー

38750090 - スキャナーが失敗しました。

説明

スケジュールされた脆弱性スキャンが、脆弱性データのインポートに失敗しました。スキャン障害は、通常、インポートするデータが大容量であることによる構成上の問題またはパフォーマンス上の問題が原因で発生します。スキャン障害は、システムによってダウンロードされたスキャン・レポートが読めない形式であるときにも発生する場合があります。

ユーザー応答

次の手順を実行します。

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「**VA** スキャナーのスケジュール」をクリックします。
4. スキャナー・リストで、任意のスキャナーの「状況」列にカーソルを移動して、正常終了または失敗の詳細なメッセージを表示します。

フィルターの初期化に失敗した

38750091 - トラフィック分析フィルターが初期化に失敗しました。

説明

構成が正しく保存されていない場合、または構成ファイルが破損している場合、イベント・コレクション・サーバー (ECS) の初期化に失敗する可能性があります。トラフィック分析プロセスが開始されていない場合、新しいログ・ソースは自動的にはディスカバーされません。

ユーザー応答

次のオプションのいずれかを選択してください。

- すべての新しいアプライアンスまたはイベント・ソースについて、トラフィック分析プロセスが動作するまで、ログ・ソースを手動で作成してください。

  新しいイベント・ソースはすべて、ログ・ソースにマップされるまだ、SIM 汎用として分類されます。
- 自動更新エラーが表示された場合は、自動更新ログを調べて、DSM またはプロトコルがインストールされたときにエラーが発生したかどうかを判別してください。

ディスク・ストレージを使用できない

38750092 - ディスク監視機能は 1 つ以上のストレージ区画がアクセス不能であることを検出しました。

説明

ディスク監視機能が、30 秒以内に応答を受信しませんでした。ストレージ区画の問題が存在するか、システムに過剰な負荷がかかっていて 30 秒というしきい値内に応答できない可能性があります。

ユーザー応答

次のオプションのいずれかを選択します。

- **touch** コマンドを使用することで、/store 区画の状況を確認してください。

システムが **touch** コマンドに応答する場合、ディスク・ストレージを使用できないのはシステム負荷による可能性が高いと思われます。

- 通知が除去されたイベントに対応するものかどうかを判別してください。

イベントが除去され、イベントおよびディスク・ストレージが使用できない場合は、イベントとフローのキューがいっぱいになっている可能性があります。ストレージ区画の状況を調べてください。

データをエクスポートするにはディスク・スペースが不足

38750096 - ディスク・スペースが不足しているため、データ・エクスポート要求を完了できません。

説明

エクスポート・ディレクトリーに十分なスペースがない場合、イベント、フロー、およびオフェンスのデータのエクスポートは、取り消されます。

ユーザー応答

次のオプションのいずれかを選択します。

- /store/exports ディレクトリーのディスク・スペースを解放してください。
- 「システム設定」ウィンドウの「エクスポート・ディレクトリー」プロパティーを、十分なディスク・スペースがある区画を使用するように構成してください。
- オフボードのストレージ・デバイスを構成してください。

アキュムレーターに時間がかかっている

38750099 - アキュムレーターが、この間隔のすべてのイベント/フローを集計できませんでした。

説明

このメッセージは、システムが 60 秒の間隔内にデータの集計を集約できなかったときに表示されます。

QRadar は、集約された各検索のデータの集計を毎分作成します。データの集計は、時系列グラフおよびレポートで使用されるもので、60 秒の間隔内に完了する必要があります。検索の数および検索内の固有値の数が大きすぎる場合、集計の処理に必要な時間が 60 秒を超える可能性があります。集計が 60 秒以内に完了できないとき、その集計間隔は除去されます。問題が発生したときの期間の列が、時系列グラフおよびレポートから欠落する可能性があります。

この問題が発生してもデータは欠落しません。生のデータ、イベント、およびフローは、ディスクに書き込まれたままです。格納されているデータから生成されるデータ・セットである集計が不完全になるだけです。

ユーザー応答

アキュムレーターのパフォーマンス劣化の原因であるワークロードの増大に影響する可能性がある要因は次のとおりです。

不完全な集計の頻度
: 集計の失敗が日に 1、2 回の場合、欠落の原因は、大規模な検索、データ圧縮のサイクル、またはデータ・バックアップによって増大したシステム負荷である可能性があります。

  失敗が頻繁ではない場合は無視してかまいません。失敗が日に複数回で、常時発生する場合は、詳しく調べることをお勧めします。

高いシステム負荷
: 他のプロセスが多くのシステム・リソースを使用する場合、増大したシステム負荷により、集計が遅くなることがあります。システム負荷が増大した原因を調べて、可能な場合はその原因に対応してください。

  例えば、完了までに長時間かかる大規模なデータ検索中に集計の失敗が発生した場合、保存済み検索のサイズを削減することで、アキュムレーターでの欠落を防止できる可能性があります。

アキュムレーターの大規模な要求
: アキュムレーター間隔が頻繁に欠落する場合は、ワークロードの削減が必要になることがあります。

  アキュムレーターのワークロードは、集計の数とそれらの集計内の固有オブジェクトの数によって決まります。集計内の固有オブジェクトの数は、検索に適用されるグループ化基準パラメーターおよびフィルターによって変わります。

  例えば、検索がサービスを集約し、ローカル・ネットワーク階層項目 (DMZ 領域など) を使用してデータをフィルターに掛け、IP アドレスを基準にしてグループ化する場合、その検索には、最大 200 個の固有オブジェクトが含まれる可能性があります。検索に宛先ポートを追加し、各サーバーがさまざまなポートで 5 個から 10 個のサービスをホストする場合、`destination.ip + destination.port` の新しい集計では、固有オブジェクトの数が 2000 に増大する可能性があります。集計に送信元 IP アドレスを追加するときに、各サービスにヒットするリモート IP アドレスが何千個もある場合、集約ビューは、何十万個もの固有値を持つ可能性があります。この検索では、アキュムレーターへの要求が多大になると考えられます。

アキュムレーターへの要求が最も高い集約ビューを確認するには、次のようにします。

1. 「管理」タブで、「集約データ管理」をクリックします。
2. 「書き込まれたデータ」列をクリックして、降順にソートし、最大のビューを表示します。
3. 最大になっている各集計のビジネス・ケースを調べて、それらがまだ必要であるかどうかを検討します。

CRE がルールの読み取りに失敗した

38750107 - ルール読み取りの前回の試行が (通常はルールの変更により) 失敗しました。これを解決する方法については、メッセージの詳細とエラー・ログを参照してください。

説明

イベント・プロセッサーのカスタム・ルール・エンジン (CRE) は、受信イベントを相互に関連付けるためのルールを読み取ることができません。通知には、次のいずれかのメッセージが含まれる場合があります。

- CRE が単一のルールを読み取ることができなかったときは、ほとんどの場合、最近のルールの変更が原因です。通知メッセージのペイロードには、該当するルールまたはルール・チェーンが表示されます。
- まれに、データ破損により、ルール・セット全体に障害が発生していることがあります。アプリケーション・エラーが表示され、ルール・エディター・インターフェースが応答しなくなるか、より多くのエラーを生成します。

ユーザー応答

単一のルール読み取りエラーの場合は、以下の選択肢を確認してください。

- 通知を発生させているルールを見つけるために、一時的にルールを無効にしてください。
- ルールを編集して、最近の変更を元に戻してください。
- エラーを発生させているルールを削除し、再作成してください。

CRE がルールの読み取りに失敗するアプリケーション・エラーの場合は、お客様サポートにお問い合わせください。

アキュムレーターが集約データのビュー定義を読み取ることができない

38750108 - アキュムレーター: 同期が取れなくなる問題を防止するため、集約データのビュー定義を読み取ることができません。集約データ・ビューは、もう作成もロードもできません。時系列グラフ、およびレポート作成も機能しなくなりました。

説明

同期の問題が発生しました。メモリー内の集約データ・ビュー構成が誤ったデータをデータベースに書き込みました。

データ破損を防止するため、システムは集約データ・ビューを無効にします。集約データ・ビューが無効なときは、時系列グラフ、保存済み検索、およびスケジュールされたレポート作成で空のグラフが表示されます。

ユーザー応答

お客様サポートにお問い合わせください。

ストア・アンド・フォワード・スケジュールがすべてのイベントを転送しなかった

38750109 - イベントがディスクに残っている間にストア・アンド・フォワードのスケジュールが終了しました。これらのイベントは、次のフォワード・セッションが開始されるまで、ローカル・イベント・コレクターに保管されます。

説明

スケジュールの開始時刻と終了時刻の間が短い場合や、スケジュールに転送対象のイベントが多数ある場合、キューに入れられたイベントをイベント・コレクター・アプライアンスが転送する時間が不足する可能性があります。イベントは、次のイベント転送機会まで保管されます。次のストア・アンド・フォワード間隔になったときに、イベントがイベント・プロセッサーに転送されます。

ユーザー応答

イベント・コレクター・アプライアンスのイベント転送速度を上げるか、イベントの転送に対して構成されている時間間隔を増やしてください。

ディスク障害

38750110 - ディスク障害: ハードウェア・モニターにより、ディスクが障害状態になっていることが検出されました。

説明

オンボードのシステム・ツールにより、ディスクに障害が発生していることが検出されました。この通知メッセージには、障害が発生したディスク、および障害のスロットまたはベイの場所についての情報が表示されます。

ユーザー応答

通知が解決しない場合は、お客様サポートにお問い合わせいただくか、部品を交換してください。

予測されるディスク障害

38750111 - 予測されるディスク障害: ハードウェア・モニターにより、ディスクで障害が発生する可能性があることが検出されました。

説明

システムは、毎時、ハードウェアの状況をモニターして、アプライアンスでハードウェア・サポートが必要なときを判別します。

オンボードのシステム・ツールにより、ディスクが障害、または耐用年数の終了に近づいていることが検出されました。障害のスロットまたはベイの場所が特定されます。

ユーザー応答

障害状態が予測されているディスクの保守をスケジュールしてください。

スキャン・ツール障害

38750118 - スキャンが予期せずに停止しました。これにより、スキャンが停止する場合があります。

説明

システムは脆弱性スキャンを初期化できないため、アセット・スキャン結果を外部のスキャナーからインポートできません。スキャン・ツールが予期せずに停止した場合、システムは外部のスキャナーと通信できません。システムは、30 秒間隔で 5 回、外部のスキャナーとの接続を試行します。

まれに、ディスカバリー・ツールで未テストのホストまたはネットワーク構成が検出されます。

ユーザー応答

次のオプションのいずれかを選択します。

- デプロイメント・エディターで、外部のスキャナーの構成を調べて、ゲートウェイの IP アドレスが正しいことを確認してください。
- 外部のスキャナーが、構成されている IP アドレス経由で通信できることを確認してください。
- DMZ のファイアウォール・ルールによって、アプライアンスとスキャン対象のアセットとの間の通信がブロックされていないことを確認してください。

外部スキャンのゲートウェイ障害

38750119 - 外部 IBM ホスト・スキャナーに対し、無効または不明なゲートウェイ IP アドレスが指定されたため、スキャンが停止しました。

説明

外部のスキャナーが追加されるときは、ゲートウェイの IP アドレスが必須です。デプロイメント・エディターでスキャナーに対して構成されているアドレスが正しくない場合、スキャナーは外部のネットワークにアクセスできません。

ユーザー応答

次のオプションのいずれかを選択してください。

- デプロイメント・エディターで、構成されている外部のスキャナーの構成を調べて、ゲートウェイの IP アドレスが正しいことを確認してください。
- 外部のスキャナーが、構成されている IP アドレス経由で通信できることを確認してください。
- DMZ のファイアウォール・ルールによって、アプライアンスとスキャン対象のアセットとの間の通信がブロックされていないことを確認してください。

自動更新のためのユーザー認証が失敗した

38750127 - 自動更新のユーザー認証が失敗しました。有効な個別の IBM ID が必要です。

説明

更新サーバーからの自動ダウンロードを許可するには、有効な資格情報が必要です。

ユーザー応答

次のオプションのいずれかを選択してください。

- IBM サポート Web サイト (http://www.ibm.com/support/) で管理者がアカウントを登録する必要があります。
- 自動更新設定を表示するには、「管理」タブで「自動更新」アイコンをクリックし、「設定の変更」 > 「拡張」を選択します。管理者は、「設定」ウィンドウのユーザー名およびパスワードが正しいことを確認できます。

集約データ制限に到達した

38750130 - 集合的な制限により、集合データ・ビューを作成できませんでした。

説明

アキュムレーターは、検索、グラフの表示、およびレポートのパフォーマンスを支援するためにデータ集計でイベントとフローをカウントおよび準備する QRadar プロセスです。アキュムレーター・プロセスは、定義済みの期間でデータを集計し、集合データ・ビューを作成します。集合データ・ビュー は、時系列グラフを描画したり、スケジュールされたレポートを作成したり、アノマリ検出ルールをトリガーしたりするために使用するデータ・セットです。

コンソールでは、アクティブな集合データ・ビューの数が 130 に制限されています。

以下のユーザー・アクションによって、新規の集合データ・ビューが作成される可能性があります。

- 新規のアノマリ検出ルール。
- 新規のレポート。

- 時系列データを使用する新規の保存済み検索。

集合データ・ビューの限度に達すると、通知が生成されます。ユーザーが新規のアノマリ・ルール、レポート、または保存済み検索を作成しようとすると、システムが限度に達していることがユーザー・インターフェースでプロンプト表示されます。

ユーザー応答

管理者は、この問題を解決するために、「管理」タブの「集約データ管理」ウィンドウで、アクティブな集合データ・ビューを確認することができます。集約データ管理機能によって、それぞれの集合データ・ビューで使用中のレポート、検索、およびアノマリ検出ルールに関する情報が表示されます。管理者は、集合データ・ビューのリストを確認し、ユーザーにとって最も重要なデータを判別できます。集合データ・ビューを無効にして、集合データ・ビューを必要とする新規のルール、レポート、または保存済みの検索をユーザーが作成できるようにすることが可能です。

管理者が集合データ・ビューを削除することを決定した場合、サマリーに、影響を受ける検索、ルール、またはレポートの概要が示されます。管理者は、検索、アノマリ・ルール、またはレポートを再度有効にするか、再作成するだけで、削除された集合データ・ビューを再作成することができます。必要なデータに基づいて、システムによって集合データ・ビューが自動的に作成されます。

判定機能でオフェンスの更新を続行できない

38750147 - 判定機能で重大なエラーが検出されました。これにより、オフェンスの更新が妨げられる可能性があります。

説明

オフェンスの更新をデータベースに書き込み中に、システムが例外を検出しました。

イベントは処理されて保管されますが、オフェンスには反映されません。

ユーザー応答

「オフェンスを非アクティブにする」のチェック・マークを外して、SIM データ・モデルのソフト・クリーンを実行します。

1. 「管理」タブをクリックします。
2. ツールバーで「拡張」 > 「**SIM** モデルのクリーンアップ」をクリックします。
3. 「ソフト・クリーン」をクリックして、オフェンスを非アクティブに設定します。
4. 「オフェンスを非アクティブにする」にチェック・マークが付いていないことを確認します。
5. 「データ・モデルをリセットしますか**?**」チェック・ボックスをクリックして、「次へ進む」をクリックします。

SIM モデルをクリーンアップすると、既存のオフェンスはすべてクローズされます。SIM モデルをクリーンアップしても、既存のイベントおよびフローには影響しません。

第 3 章 QRadar アプライアンスの警告通知

IBM Security QRadar システム正常性の通知は、ソフトウェアまたはハードウェアの実際の障害または切迫した障害のプロアクティブなメッセージです。

最大センサー・デバイス数がモニターされた

38750006 - トラフィック分析は、既に最大数のログ・ソースをモニターしています。

説明

システムでは、トラフィック分析によって自動ディスカバリーするようにキューに入れることができるログ・ソースの数に制限があります。キューのログ・ソースの最大数に到達すると、新しいログ・ソースを追加できなくなります。

ログ・ソースについてのイベントは、SIM 汎用として分類され、不明なイベント・ログというラベルが付けられます。

ユーザー応答

次のオプションのいずれかを選択してください。

- 「ログ・アクティビティー」タブで、SIM 汎用ログ・ソースを確認して、イベント・ペイロードからアプライアンスのタイプを判別してください。
- 自動更新により、最新の DSM 更新をダウンロードできるようにして、ログ・ソース・イベントを正しく識別し、解析してください。
- ログ・ソースが公式にサポートされていることを確認してください。

  アプライアンスがサポートされている場合、自動的にディスカバーされなかったイベントのログ・ソースを手動で作成してください。
- アプライアンスが公式にサポートされていない場合、イベントを識別し、分類するためのユニバーサル DSM を作成してください。
- デバイスが 1,000 件のイベントを発生させるのをお待ちください。

  1,000 件のイベントが発生してもシステムによってログ・ソースが自動ディスカバーされない場合、そのソースはトラフィック分析キューから削除されます。スペースは、自動ディスカバーの対象になる別のログ・ソースが使用できるようになります。

関連付けられているログ・ソースを判別できない

38750007 - IP アドレス <IP address> に関連付けられているログ・ソースを自動的に検出できません。

説明

ログ・ソースを識別するには、少なくとも 25 件のイベントが必要です。1,000 件のイベントが発生してもログ・ソースが識別されない場合、システムは自動ディスカバリー・プロセスを中止します。

トラフィック分析プロセスが自動ディスカバリーの最大しきい値を超えたときに、システムはそのログ・ソースを SIM 汎用として分類し、イベントに**不明なイベント・ログ**というラベルをつけます。

ユーザー処置

以下の選択肢を確認してください。

- ログ・ソースを特定する IP アドレスを確認してください。
- 低速でイベントを転送するログ・ソースをすべて確認してください。イベント速度が遅いログ・ソースでは、通常、この通知が発生します。
- システムのイベントを正しく解析するために、自動更新によって最新の DSM がダウンロードされるようにしてください。
- 中央のログ・サーバー経由でイベントを発生させるログ・ソースをすべて確認してください。中央のログ・サーバーまたは管理コンソールから提供されるログ・ソースでは、ログ・ソースを手動で作成することが必要な場合があります。
- 「ログ・アクティビティー」タブを確認して、通知メッセージ内の IP アドレスからアプライアンスのタイプを判別し、次にログ・ソースを手動で作成してください。
- ログ・ソースが公式にサポートされていることを確認してください。アプライアンスがサポートされている場合、イベントのログ・ソースを手動で作成してください。
- アプライアンスが公式にサポートされていない場合、イベントを識別し、分類するためのユニバーサル DSM を作成してください。

最大イベント数に到達した

38750008 - 過去 1 時間に間隔あたりのイベント数のしきい値を超えました。

説明

各アプライアンスには、特定の量のイベントおよびフロー・データを処理するライセンスがあります。

ライセンスの制限を超え続けると、システムは、イベントとフローをキューに入れたり、バックアップ・キューがいっぱいになったときには、データを除去したりする可能性があります。

ユーザー応答

イベント・パイプラインに入るイベントとフローの量を削減するようにシステムをチューニングしてください。

フロー・コレクターが初回の同期を確立できない

38750009 - フロー・コレクターが初回の同期を確立できませんでした。

説明

QFlow プロセスには、時刻を同期するためにサーバー IP アドレスを構成する拡張機能が含まれています。ほとんどのケースでは、値を構成しないでください。構成すると、QFlow プロセスは、1 時間ごとに IP アドレスのタイム・サーバーを同期しようとします。

ユーザー応答

デプロイメント・エディターで、QFlow プロセスを選択します。「アクション」 > 「構成」をクリックし、「拡張」をクリックします。「時刻同期サーバー **IP** アドレス」フィールドの値をクリアし、「保存」をクリックします。

バックアップで要求を完了できない

38750033 - バックアップ: 空きディスク・スペースが不足しているためバックアップを実行できません。

説明

この通知は、バックアップを実行するのに十分な空きスペースがないときに発生します。

ディスク監視機能は、システム・ディスクのストレージの問題のモニターを担当します。バックアップを開始する前、ディスク監視機能は使用可能なディスク・スペースを検査して、バックアップを正常に完了できるかどうかを判別します。バックアップ・データを格納する区画で 90% というしきい値をディスク・スペースが超えている場合、バックアップはキャンセルされます。空きディスク・スペースが、最後のバックアップのサイズの 2 倍より少ない場合、バックアップはキャンセルされます。デフォルトでは、バックアップは `/store/backup` に格納されます。

ユーザー応答

この問題を解決するには、次のオプションのいずれか 1 つを選択します。

- `/store/backup` でバックアップが完了するのに十分なスペースを確保できるように、アプライアンス上のディスク・スペースを解放します。
- 空きディスク・スペースがある区画を使用するように既存のバックアップを構成します。
- アプライアンスに対して追加ストレージを構成します。詳しくは、「オフボード・ストレージ・ガイド」を参照してください。

バックアップで要求を実行できない

38750035 - バックアップ: バックアップ要求を実行できません。

説明

次のいずれかの理由で、バックアップを開始または完了できません。

- システムが、バックアップ複製同期テーブルをクリーンアップできない。
- システムが削除要求を実行できない。
- システムが、ディスク上のファイルを使用してバックアップを同期できない。
- NFS がマウントされているバックアップ・ディレクトリーが使用できないか、正しくない NFS エクスポート・オプション (no_root_squash) が指定されている。
- システムがオンデマンド・バックアップを初期化できない。
- システムが、選択したバックアップ・タイプ用の構成を取得できない。
- スケジュールされたバックアップを初期化できない。

ユーザー応答

バックアップを手動で開始して、失敗が再発するかどうかを判別してください。バックアップの開始に複数回失敗した場合は、お客様サポートにお問い合わせください。

プロセス・モニターのライセンスが期限切れ、または無効

38750044 - プロセス・モニター: プロセスを開始できません: ライセンスが期限切れ、または無効です。

説明

管理対象ホストのライセンスが期限切れになりました。アプライアンス上のすべてのデータ収集プロセスが停止します。

ユーザー応答

営業担当員に連絡して、ライセンスを更新してください。

実行時間の長いトランザクションを発生させている非管理対象プロセスが見つかった

38750048 - トランザクション監視機能: システムの安定度を低下させる異常に実行時間の長いトランザクションを発生させている非管理対象プロセスが見つかりました。

説明

トランザクション監視機能は、外部プロセス (データベースの複製問題、保守スクリプト、自動更新、コマンド・ライン・プロセスなど) またはトランザクションが、データベース・ロックを発生させていると判別しました。

ユーザー応答

次のオプションのいずれかを選択します。

- /var/log/qradar.log ファイルで TxSentry という語を探して、トランザクションの問題を発生させているプロセスの ID を調べます。
- プロセスがトランザクションを完了し、データベース・ロックを解放するかどうかを確認するために待ちます。
- データベース・ロックを手動で解放します。

ハングしたトランザクションの取り消しによってシステム・ヘルスが回復した

38750049 - トランザクション監視機能: ハングしたトランザクションまたはデッドロックを取り消すことにより、システム・ヘルスが回復しました

説明

トランザクション監視機能が、中断状態のデータベース・トランザクションを取り消すか、データベース・ロックを削除することで、システムを正常なシステム・ヘルスに回復させました。エラーを発生させたプロセスを判別するために、qradar.log ファイルで TxSentry という語を探します。

ユーザー応答

アクションは不要です。

アクティブなオフェンスの最大数に到達した

38750050 - MPC: 新しいオフェンスを作成できません。アクティブなオフェンスの最大数に達しています。

説明

システムは、オフェンスを作成できず、休止オフェンスをアクティブなオフェンスに変更することもできません。システムでオープンにできるデフォルトのアクティブなオフェンスの数は、2500 に制限されています。アクティブなオフェンスとは、過去 5 日以内に、更新されたイベント数を受信しつづけているオフェンスです。

ユーザー応答

次のオプションのいずれかを選択してください。

- 低いセキュリティーのオフェンスをオープン(アクティブ) からクローズ、または保護されたクローズに変更します。
- オフェンスを生成するイベントの数を削減するようにシステムをチューニングしてください。

  クローズしたオフェンスがデータ保存ポリシーによって削除されるのを防止するために、クローズしたオフェンスを保護してください。

オフェンスの合計の最大数に到達した

38750051 - MPC: オフェンスを処理できません。オフェンスの合計の最大数に到達しました。

説明

デフォルトでは、プロセスの制限は、2,500 件のアクティブなオフェンスと、100,000 件の全体のオフェンスです。

アクティブなオフェンスが、30 分間イベント更新を受信しない場合、オフェンスの状況は「休止」に変わります。イベント更新が発生すると、休止オフェンスはアクティブに変わる場合があります。5 日後、イベント更新がない休止オフェンスは「非アクティブ」に変わります。

ユーザー応答

次のオプションのいずれかを選択してください。

- オフェンスを生成するイベントの数を削減するようにシステムをチューニングしてください。
- オフェンスの保存ポリシーを、データの保存ポリシーが非アクティブなオフェンスを削除できる間隔に調整してください。

  クローズしたオフェンスがデータ保存ポリシーによって削除されるのを防止するために、クローズしたオフェンスを保護してください。
- 重要であるアクティブなオフェンスのためのディスク・スペースを解放するために、オフェンスを「アクティブ」から「休止」に変更してください。

長時間実行のレポートが停止した

38750054 - 構成されている最大しきい値よりも長い時間実行されていたことが検出されたレポートを終了しています。

説明

システムは、制限時間を超えたレポートを取り消します。次のデフォルトの制限時間より長い時間実行されたレポートは取り消されます。

表 *1.* レポートの頻度ごとのデフォルトの制限時間

レポートの頻度	デフォルトの制限時間 **(**時**)**
毎時	2
毎日	12
手動	12
毎週	24
毎月	24

ユーザーが実行する必要がある作業

次のオプションのいずれかを選択してください。

- レポートの時間を削減してください。ただし、より頻繁に実行するようにスケジュールしてください。
- スケジュールどおりに生成されるように、手動レポートを編集してください。

手動レポートは、Raw data に依存してかまいませんが、累積データにはアクセスできません。手動レポートを編集して、レポートが毎時、毎月、または毎週のスケジュールを使用するように変更してください。

メモリー不足エラーになり、エラーが発生したアプリケーションが再始動された

38750055 - メモリー不足：システムが復元され、エラーが発生したアプリケーションが再始動されました。

説明

アプリケーションまたはサービスがメモリー不足になり、再始動されました。メモリー不足という問題は、通常、ソフトウェアまたはユーザー定義の照会によって発生します。

ユーザー応答

/var/log/qradar.log ファイルを確認して、サービスの再始動が必要かどうかを判別してください。

大規模な脆弱性スキャン、または大容量のデータのインポートがエラーの原因になっているかどうかを判別してください。例えば、システムがイベントや脆弱性データを通知タイム・スタンプ付きでシステムにインポートした時刻を比較してください。必要な場合、データのインポートの時間間隔をずらしてください。

管理対象プロセスの長時間のトランザクション

38750056 - トランザクション監視機能：システムの安定度を低下させる異常に実行時間の長いトランザクションを発生させている管理対象プロセスが見つかりました。

説明

トランザクション監視機能では、Tomcat、イベント・コレクション・サーバー (ECS) などの管理対象プロセスがデータベース・ロックの原因であることを判別します。

管理対象プロセスは、強制的に再始動されます。

ユーザー応答

エラーを発生させたプロセスを判別するために、qradar.log で TxSentry という語を探します。

プロトコル・ソース構成が正しくない

38750057 - プロトコル・ソース構成により、イベントの収集が停止される可能性があります。

説明

システムは、ログ・ソースについて正しくないプロトコル構成を検出しました。リモート・ソースからのイベントの取得にプロトコルを使用するログ・ソースは、プロトコルに構成上の問題が検出されたときに初期化エラーを生成する可能性があります。

ユーザー応答

プロトコル構成の問題を解決するには、次のようにします。

- ログ・ソースを調べて、プロトコル構成が正しいことを確認してください。

  認証フィールド、ファイル・パス、JDBC のデータベース名を確認し、システムがリモート・サーバーと通信できることを確認してください。ログ・ソースにマウス・ポインターを移動して、より詳細なエラー情報を表示してください。
- /var/log/qradar.log ファイルで、プロトコル構成エラーに関する詳細情報を確認してください。

MPC: プロセスが正常にシャットダウンされない

38750058 - MPC: サーバーが正常にシャットダウンされませんでした。再同期を実行し、システムの安定度を確保するために、オフェンスが閉じられます。

説明

判定機能プロセスでエラーが発生しました。アクティブなオフェンスが閉じられ、サービスが再開され、必要な場合は、データベース表が検査および再作成されます。

システムは、データ破損を防止するために同期を実行します。判定機能コンポーネントが破損状態を検出した場合、データベース表およびファイルは再作成されます。

ユーザー応答

判定機能コンポーネントは、自己修復できます。エラーが続行する場合は、お客様サポートにお問い合わせください。

前回のバックアップが許可されている制限時間を超えた

38750059 - バックアップ: 前回スケジュールされたバックアップが実行しきい値を超えました。

説明

制限時間は、構成時に割り当てるバックアップの優先順位によって決定されます。

ユーザー応答

次のオプションのいずれかを選択してください。

- バックアップ構成を編集して、バックアップの完了について構成されている制限時間を延長してください。24 時間を超える延長はしないでください。
- 失敗したバックアップを編集して、優先順位をより高い値に変更してください。高い優先順位では、バックアップの完了に対してより多くのシステム・リソースが割り振られます。

ログ・ソースのライセンス制限

38750062 - 構成済みログ・ソースの数が、ライセンス交付を受けた制限に近づいているか、この制限に到達しました。

説明

すべてのアプライアンスは、特定の数のログ・ソースからイベントを収集するライセンスとともに販売されます。このライセンス制限に近づいたか、この制限を超えました。

これ以上追加されるログ・ソースは、デフォルトで無効になります。無効にされたログ・ソースには、イベントが収集されません。

ユーザー応答

以下の選択肢を確認してください。

- 「管理」タブで、「ログ・ソース」アイコンをクリックし、優先順位が低いか、非アクティブなイベント・ソースがあるログ・ソースをすべて無効にするか、削除してください。無効にされたログ・ソースは、ログ・ソースのライセンス数に含められません。ただし、無効にされたログ・ソースによって収集されたイベント・データは、引き続き使用も検索もできます。
- 削除したログ・ソースが自動的に再ディスカバーされないことを確認してください。ログ・ソースが再ディスカバーされた場合は、そのログ・ソースを無効にできます。ログ・ソースを無効にすることで、自動ディスカバリーが防止されます。
- ログ・ソースを一括で追加するときは、ライセンス制限を超えないことを確認してください。

自動更新のデプロイ

38750069 - 自動更新が正常にインストールされました。「管理」タブで、「変更のデプロイ」をクリックしてください。

説明

RPM 更新などの自動更新がダウンロードされました。このインストール・プロセスを終了するには、ユーザーが変更をデプロイする必要があります。

ユーザー応答

「管理」タブで、「変更のデプロイ」をクリックしてください。

ログ・ソースが無効な状態で作成された

38750071 - ライセンス制限により、ログ・ソースが無効な状態で作成されました。

説明

トラフィック分析とは、イベントからログ・ソースを自動的にディスカバーし、作成するプロセスです。現在のログ・ソースのライセンス制限に到達した場合、トラフィック分析プロセスは、ログ・ソースを無効な状態で作成する可能性があります。無効にされたログ・ソースは、イベントを収集せず、ログ・ソースの制限に含められません。

ユーザー応答

以下の選択肢を確認してください。

- 「管理」タブで、「ログ・ソース」アイコンをクリックし、優先順位が低いログ・ソースを無効にするか、削除してください。無効にされたログ・ソースは、ログ・ソースのライセンス数に含められません。
- 削除したログ・ソースが自動的に再ディスカバーされないことを確認してください。ログ・ソースを無効にして、自動ディスカバリーを防止できます。
- ログ・ソースを一括で追加するときは、ライセンス制限を超えないことを確認してください。
- より多くのログ・ソースを含めるために拡張ライセンスが必要な場合は、営業担当員にお問い合わせください。

SAR 標識しきい値を超えた

38750073 - SAR 標識: しきい値を超えました。

説明

システム・アクティビティー・レポーター (SAR) ユーティリティーで、システム負荷がしきい値を超えていることが検出されました。システムのパフォーマンスが低下する可能性があります。

ユーザー応答

以下の選択肢を確認してください。

- ほとんどのケースでは、解決は必要ありません。

  例えば、CPU の使用率が 90% を超えると、システムが、自動的に正常な動作に戻そうとします。
- この通知が繰り返し発生する場合は、SAR 標識のデフォルト値を増やしてください。

  「管理」タブをクリックし、「グローバル・システム通知」をクリックします。通知のしきい値を増やしてください。
- システム負荷の通知については、同時に実行するプロセスの数を減らしてください。

ログ・ソースに対するレポート、脆弱性スキャン、データのインポートの開始時刻をずらしてください。システム負荷を低減させるために、バックアップとシステム・プロセスとは、異なる時刻に開始するようにスケジュールしてください。

ユーザーが存在しないか未定義である

38750075 - ユーザーが存在しないか、未定義のロールを割り当てられています。

説明

システムが、より多くの権限を持つようにユーザー・アカウントを更新しようとしましたが、そのユーザー・アカウントまたはユーザー・ロールが存在しません。

ユーザー応答

「管理」タブで、「変更のデプロイ」をクリックしてください。ユーザー・アカウントまたはユーザー・ロールを更新するには、変更をデプロイする必要があります。

ディスク使用率の警告

38750076 - ディスク監視機能: ディスク使用量が警告しきい値を超えました。

説明

ディスク監視機能で、システムのディスク使用率が 90% より大きいことが検出されました。

システム上のディスク・スペースが 95% に到達すると、システムは、データ破損を防止するためにプロセスを無効にし始めます。

ユーザー応答

ファイルを削除するか、データ保存ポリシーを変更することで、ディスク・スペースを解放する必要があります。ディスク・スペースの使用率が容量の 92% というしきい値を下回ると、システムはプロセスを自動的に再開できます。

インフラストラクチャー・コンポーネントが破損しているか、開始しなかった

38750083 - インフラストラクチャー・コンポーネントが破損しています。

説明

メッセージング・サービス (IMQ) または PostgreSQL データベースが開始できないか、再作成できないときは、管理対象ホストは正しく動作したり、コンソールと通信したりできません。

ユーザー応答

お客様サポートにお問い合わせください。

データ複製障害

38750085 - データ複製で障害が発生しています。

説明

管理対象ホストがダウンロードしたデータを複製しようとしたときに、障害が発生しました。データ複製により、コンソールが使用できなくなっても管理対象ホストがデータの収集を続行できるようになります。管理対象ホスト上のダウンロード・データの複製で繰り返し障害が発生する場合は、システムにパフォーマンス上の問題または通信上の問題が発生している可能性があります。

ユーザー応答

管理対象ホストが複製の問題を自力で解決しない場合は、カスタマー・サポートにお問い合わせください。

イベントは直接ストレージに経路指定された

38750088 - イベント・パイプラインでパフォーマンスの低下が検出されました。イベントは直接ストレージに経路指定されました。

説明

キューがいっぱいになるのを防止し、システムがイベントを除去するのを防止するため、イベント・コレクション・サーバー (ECS) はデータをストレージに経路指定します。受信イベントとフローは、分類されません。ただし、生のイベントとフロー・データは、収集され、検索できます。

ユーザー応答

以下の選択肢を確認してください。

- 受信イベントとフローの速度を確認してください。イベント・パイプラインがイベントをキューに入れている場合、より多くのデータを保持するようにライセンス内容を拡張してください。
- ルールやカスタム・プロパティーに対する最近の変更を確認してください。ルールやカスタム・プロパティーの変更によって、イベントやフローの速度が変わることがあります。変更により、パフォーマンスに影響が及んだり、システムがイベントをストレージに経路指定したりする可能性があります。
- DSM 解析の問題により、イベント・データがストレージに経路指定される可能性があります。ログ・ソースが公式にサポートされていることを確認してください。
- SAR 通知が、キューに入れられたイベントおよびフローがイベント・パイプラインにあることを示す場合があります。
- イベント・パイプラインに入るイベントとフローの量を削減するようにシステムをチューニングしてください。

カスタム・プロパティーが無効になっている

38750097 - カスタム・プロパティーが無効になっています。

説明

カスタム・プロパティーの処理で問題が発生したため、カスタム・プロパティーが無効になっています。この無効になっているカスタム・プロパティーを使用するルール、レポート、検索は、正しい動作を停止します。

ユーザー応答

次のオプションのいずれかを選択してください。

- 無効になっているカスタム・プロパティーを調べて、正規表現のパターンを修正してください。無効になっているカスタム・プロパティーを、まず正規表現のパターンまたは計算を見直して最適化することなく、再有効化しないでください。
- カスタム・プロパティーがカスタムのルールまたはレポートに使用されている場合、「ルール、レポート、および検索の構文解析を最適化」チェック・ボックスを選択していることを確認してください。

装置バックアップ障害

38750098 - 装置のバックアップ試行中に障害が発生したか、バックアップが取り消されました。

説明

このエラーは、通常、ソース構成管理 (CSM) での構成エラー、またはユーザーによるバックアップの取り消しにより発生します。

ユーザー応答

次のオプションのいずれかを選択してください。

- CSM の資格情報とアドレスのセットを調べて、アプライアンスがログインできることを確認してください。
- ネットワーク・デバイスに接続するために構成されているプロトコルが有効であることを確認してください。
- ネットワーク・デバイスおよびバージョンがサポートされていることを確認してください。
- ネットワーク・デバイスとアプライアンスとの間に接続があることを確認してください。
- 最新のアダプターがインストールされていることを確認してください。

アキュムレーターに時間がかかっている

38750099 - アキュムレーターが、この間隔のすべてのイベント/フローを集計できませんでした。

説明

このメッセージは、システムが 60 秒の間隔内にデータの集計を集約できなかったときに表示されます。

QRadar は、集約された各検索のデータの集計を毎分作成します。データの集計は、時系列グラフおよびレポートで使用されるもので、60 秒の間隔内に完了する必要があります。検索の数および検索内の固有値の数が大きすぎる場合、集計の処理に必要な時間が 60 秒を超える可能性があります。集計が 60 秒以内に完了できないとき、その集計間隔は除去されます。問題が発生したときの期間の列が、時系列グラフおよびレポートから欠落する可能性があります。

この問題が発生してもデータは欠落しません。生のデータ、イベント、およびフローは、ディスクに書き込まれたままです。格納されているデータから生成されるデータ・セットである集計が不完全になるだけです。

ユーザー応答

アキュムレーターのパフォーマンス劣化の原因であるワークロードの増大に影響する可能性がある要因は次のとおりです。

不完全な集計の頻度
: 集計の失敗が日に 1、2 回の場合、欠落の原因は、大規模な検索、データ圧縮のサイクル、またはデータ・バックアップによって増大したシステム負荷である可能性があります。

  失敗が頻繁ではない場合は無視してかまいません。失敗が日に複数回で、常時発生する場合は、詳しく調べることをお勧めします。

高いシステム負荷
: 他のプロセスが多くのシステム・リソースを使用する場合、増大したシステム負荷により、集計が遅くなることがあります。システム負荷が増大した原因を調べて、可能な場合はその原因に対応してください。

  例えば、完了までに長時間かかる大規模なデータ検索中に集計の失敗が発生した場合、保存済み検索のサイズを削減することで、アキュムレーターでの欠落を防止できる可能性があります。

アキュムレーターの大規模な要求
: アキュムレーター間隔が頻繁に欠落する場合は、ワークロードの削減が必要になることがあります。

  アキュムレーターのワークロードは、集計の数とそれらの集計内の固有オブジェクトの数によって決まります。集計内の固有オブジェクトの数は、検索に適用されるグループ化基準パラメーターおよびフィルターによって変わります。

  例えば、検索がサービスを集約し、ローカル・ネットワーク階層項目 (DMZ 領域など) を使用してデータをフィルターに掛け、IP アドレスを基準にしてグループ化する場合、その検索には、最大 200 個の固有オブジェクトが含まれる可能性があります。検索に宛先ポートを追加し、各サーバーがさまざまなポートで 5 個から 10 個のサービスをホストする場合、`destination.ip + destination.port` の新しい集計では、固有オブジェクトの数が 2000 に増大する可能性があります。集計に送信元 IP アドレスを追加するときに、各サービスにヒットするリモート IP アドレスが何千個もある場合、集約ビューは、何十万個もの固有値を持つ可能性があります。この検索では、アキュムレーターへの要求が多大になると考えられます。

アキュムレーターへの要求が最も高い集約ビューを確認するには、次のようにします。

1. 「管理」タブで、「集約データ管理」をクリックします。
2. 「書き込まれたデータ」列をクリックして、降順にソートし、最大のビューを表示します。
3. 最大になっている各集計のビジネス・ケースを調べて、それらがまだ必要であるかどうかを検討します。

イベントまたはフローのデータに索引が付けられていない

38750101 - イベント/フローのデータに間隔用の索引が付けられていません。

説明

有効になっている索引が多すぎるか、システムの負荷が過剰な場合、システムは、索引部分からイベントまたはフローを除去する可能性があります。

ユーザー応答

次のオプションのいずれかを選択します。

- 索引の除去間隔が SAR 標識通知で発生する場合、問題の原因はシステム負荷または低ディスク・スペースである可能性が高いと考えられます。
- システム負荷を削減するために一部の索引を一時的に無効にするには、「管理」タブで、「索引管理」アイコンをクリックします。

応答アクションのしきい値に到達した

38750102 - 応答アクション: しきい値に到達しました。

説明

応答のしきい値に到達しているため、カスタム・ルール・エンジン (CRE) がルールに応答できません。

汎用ルールやチューニングされているシステムでは、多くの応答アクションを生成する可能性があります。特に、**IF-MAP** オプションが有効なシステムでは多くなります。応答アクションはキューに入れられます。キューが 2000 (イベント・コレクション・サーバー (ECS) の場合) または 1000 (Tomcat の場合) の応答アクションを超過した場合、応答アクションは削除されることがあります。

ユーザー応答

- **IF-MAP** オプションが有効な場合、**IF-MAP** サーバーへの接続が存在することと、帯域幅の問題によってルールへの応答が Tomcat のキューに入れられていないことを確認してください。
- トリガーするルールの数を削減するようにシステムをチューニングしてください。

ディスクの複製に時間がかかっている

38750103 - DRBD 標識: ディスクの複製に時間がかかっています。詳細はログを参照してください。

説明

プライマリー・アプライアンスの複製キューがいっぱいになった場合、プライマリーのシステム負荷が増大している可能性があります。複製の問題は、通常、プライマリー・システムのパフォーマンスの問題、セカンダリー・システムのストレージの問題、またはアプライアンス間の帯域幅の問題によって発生します。

ユーザー応答

次のオプションのいずれかを選択してください。

- 保存済み検索「ログ・アクティビティー」タブから「**MGMT: Bandwidth Manager**」をロードすることで、帯域幅アクティビティーを確認してください。この検索により、コンソールとホストとの間の帯域幅使用量が表示されます。
- SAR 標識通知がプライマリー・アプライアンスで繰り返し発生している場合、プライマリー・システムで Distributed Replicated Block Device キューがいっぱいになっている可能性があります。
- SSH および `cat /proc/drbd` コマンドを使用して、プライマリー・ホストまたはセカンダリー・ホストの Distributed Replicated Block Device の状況をモニターしてください。

アセットの変更が破棄された

38750106 - アセットの変更が中止されました。

説明

アセットの変更が、変更のしきい値を超えたため、アセット・プロファイル・マネージャーはアセットの変更要求を無視します。

アセット・プロファイル・マネージャーには、アセットのプロファイル情報を更新する、アセット永続というプロセスが含まれています。このプロセスは、新しいアセット・データを収集し、その情報をアセット・モデルを更新する前にキューに入れます。ユーザーがアセットの追加または編集をしようとしたとき、データは一時ストレージに格納され、変更キューの末尾に追加されます。変更キューが大きい場合は、アセットの変更がタイムアウトになり、一時ストレージが削除される可能性があります。

ユーザー応答

次のオプションのいずれかを選択してください。

- もう 1 度、アセットを追加または編集してください。
- 脆弱性スキャンの開始時刻を調整したりずらしたりするか、スキャンのサイズを削減してください。

アセット永続キューのディスクがいっぱい

38750113 - アセット永続キューのディスクがいっぱいです。

説明

アセット永続キューに割り当てられているスピルオーバー・ディスク・スペースがいっぱいになっていることをシステムが検出しました。アセット永続の更新は、ディスク・スペースが使用できるようになるまでブロックされます。情報は除去されません。

ユーザー応答

スキャンのサイズを削減してください。スキャンのサイズを削減すると、アセット永続キューのオーバーフローを防止できます。

アセット更新リゾルバー・キューのディスクがいっぱい

38750115 - アセット更新リゾルバー・キューのディスクがいっぱいです。

説明

アセット・リゾルバー・キューに割り当てられているスピルオーバー・ディスク・スペースがいっぱいになっていることをシステムが検出しました。

システムは、データ損失を防止するために、ディスクへのデータの書き込みを続行します。ただし、システムにディスク・スペースがない場合、スキャン・データは除去されます。ディスク・スペースが使用できるようになるまで、システムは、受信アセット・スキャン・データを扱うことができません。

ユーザー応答

以下の選択肢を確認してください。

- システムに空きディスク・スペースがあることを確認してください。この通知には、潜在的なディスク・スペースの問題を通知するための SAR 標識通知が付属していることがあります。
- スキャンのサイズを削減してください。
- スキャンの頻度を減らしてください。

アセット変更キューのディスクがいっぱい

38750117 - アセット変更リスナーのキューのディスクがいっぱいです。

説明

アセット・プロファイル・マネージャーには、アセットの CVSS スコアを更新するために統計を計算する、変更リスナーというプロセスが含まれています。システムは、ディスクにデータを書き込むため、保留中のアセットの統計のデータ損失は防止されます。ただし、ディスク・スペースがいっぱいの場合、スキャン・データはシステムによって除去されます。

ディスク・スペースが使用できるようになるまで、システムは、受信アセット・スキャン・データを処理できません。

ユーザー応答

次のオプションのいずれかを選択してください。

- システムに十分な空きディスク・スペースがあることを確認してください。
- スキャンのサイズを削減してください。
- スキャンの頻度を減らしてください。

高負荷のカスタム・ルールが見つかった

38750120 - 高負荷のカスタム・ルールが CRE に見つかりました: イベント・パイプラインでパフォーマンスの低下が検出されました。CRE で高負荷のカスタム・ルールが検出されました。

説明

カスタム・ルール・エンジン (CRE) は、イベントがルール・セットに一致しているかどうかを検証して、アラート、オフェンス、または通知をトリガーするプロセスです。

広い範囲を持つカスタム・ルール、または最適化されていない正規表現パターンを使用するカスタム・ルールをユーザーが作成すると、そのカスタム・ルールはパフォーマンスに影響する場合があります。

ユーザー応答

以下の選択肢を確認してください。

- 「オフェンス」タブで、「ルール」をクリックし、検索ウィンドウを使用して高負荷のルールを編集するか、無効にしてください。
- 高負荷のルール通知で SAR 標識通知が繰り返し発生する場合は、そのルールを調べてください。

アノマリ検出エンジンに対して集計が無効にされている

38750121 - アノマリ検出エンジンに対して集計が無効にされています。

説明

集約データ・ビューが無効にされているか、使用できないか、新しいルールが使用できないデータを必要としています。

集計が除去されたからといって、アノマリ・データが失われたわけではありません。集計は、格納されているデータから生成されるデータ・セットであるため、元のアノマリ・データは維持されています。通知には、除去された集計インターバルに関する詳細情報が含まれています。

アノマリ検出エンジンには、集計作業のためにそのアノマリ・データの間隔を参照することができません。

ユーザー応答

より小さいデータ・セットを使用するようにアノマリ・ルールを更新してください。

通知で SAR 標識エラーが繰り返し発生する場合は、システム・パフォーマンスが問題の原因である可能性があります。

プロセスが許可されている実行時間を超えた

38750122 - プロセスの実行時間が長すぎます。デフォルトの最大時間は 3,600 秒です。

説明

個々のプロセスでタスクを完了するデフォルトの制限時間である 1 時間を超えました。

ユーザー応答

実行中のプロセスを調べて、タスクが続行してかまわないプロセスであるか、停止する必要があるかを判別してください。

ライセンスの有効期限が切れた

38750123 - 割り振られたライセンスの有効期限が切れたため、無効になっています。

説明

コンソールでライセンスの有効期限が切れるときは、新しいライセンスを適用する必要があります。管理対象ホストでライセンスの有効期限が切れるときは、管理対象ホスト上でホスト・コンテキストが無効になります。ホスト・コンテキストが無効になると、有効期限が切れたライセンスのアプライアンスは、イベントやフローのデータを処理できません。

ユーザー応答

有効期限が切れたライセンスのアプライアンスを判別するために、「管理」タブをクリックし、「システムおよびライセンス管理」をクリックします。有効期限が切れたライセンスを持つシステムは、「ライセンスの状況」列に無効な状況が表示されます。

無許可の IP アドレスまたは範囲の外部スキャン

38750126 - 外部スキャンの実行で、無許可の IP アドレスまたはアドレス範囲をスキャンしようとしました。

説明

スキャン・プロファイルに定義されているアセット・リスト外の CIDR 範囲または IP アドレスが含まれているとき、スキャンは続行します。ただし、外部のスキャナ

ー・リストに含まれていないアセットの CIDR 範囲または IP アドレスは無視されます。

ユーザー応答

外部のスキャナーによってスキャンされるアセットについて、許可されている CIDR 範囲または IP アドレスのリストを更新してください。スキャン・プロファイルを調べて、外部のネットワーク・リストに含まれているアセットに対して、スキャンが構成されていることを確認してください。

時刻の同期に失敗した

38750129 - プライマリーまたはコンソールとの時刻の同期が失敗しました。

説明

管理対象ホストがコンソールと同期できないか、セカンダリー HA アプライアンスがプライマリー・アプライアンスと同期できません。

管理者は、ポート 37 上の **rdate** 通信を許可する必要があります。時刻の同期が正しくないと、データがコンソールに正しく報告されません。システムが同期せずに動作する時間が長くなるほど、データ、レポート、またはオフェンスの検索で正しくない結果が返されるリスクが高くなります。時刻の同期は、管理対象ホストおよびアプライアンスからの要求の正常な実行に不可欠です。

ユーザー応答

お客様サポートにお問い合わせください。

循環しているカスタム・ルール依存チェーンが検出された

38750131 - カスタム・ルールの循環依存チェーンが検出されました。

説明

単一のルールが自分を直接参照しているか、一連の他のルールやビルディング・ブロックを経由して参照しています。このエラーは、すべての構成をデプロイしたときに発生します。ルール・セットはロードされません。

ユーザー応答

循環依存を生成しているルールを編集してください。システム通知が繰り返し発生するのを防止するために、ルール・チェーンが破損されている可能性があります。ルール・チェーンを修正すると、保存により自動的にルールが再ロードされ、問題が解決されます。

ブラックリスト通知

38750136 - アセット調整除外ルールにより、新しいアセット・データがアセットのブラックリストに追加されました。

説明

IP アドレス、ホスト名、MAC アドレスなどの 1 つのアセット・データが、アセットの増加状況の逸脱にあたる振る舞いを示しています。

アセットのブラックリスト とは、アセット調整除外の CRE ルールによって信用できないとみなされたアセット・データの集合です。ルールは、アセット・データの整合性および保全性をモニターします。1 つのアセット・データが疑わしい振る舞いを 2 時間以内に 2 回以上示した場合、そのデータはアセットのブラックリストに追加されます。ブラックリストに登録されたアセット・データが含まれている更新はそれ以降、アセット・データベースに適用されません。

ユーザー応答

- 通知の説明で、「アセット調整除外ルール **(Asset Reconciliation Exclusion rules)**」をクリックして、アセット・データのモニターに使用されているルールを表示します。
- 通知の説明で、「ログ・ソースによってアセットの逸脱を確認 **(Asset deviations by log source)**」をクリックして、過去 24 時間に発生したアセットの逸脱レポートを表示します。
- ブラックリストへのデータ追加の頻度が高すぎる場合は、ブラックリストにデータを追加するアセット調整除外ルールをチューニングできます。
- 該当のアセット・データをアセット・データベースに追加する場合は、ブラックリストからそのアセット・データを削除して、対応するアセットのホワイトリストに追加します。ホワイトリストにアセット・データを追加すると、それらのデータがブラックリストに誤って再表示されることがなくなります。
- アセット調整の資料を参照してください。

アセットの増加状況の逸脱が検出された

38750137 - システムにより、通常サイズのしきい値を超えるアセット・プロファイルが検出されました。

説明

システムにより、アセット・データベース内で、逸脱した増加や異常な増加を示す 1 つ以上のアセット・プロファイルが検出されました。逸脱した増加は、システムしきい値で許可されている数よりも多くの IP アドレス、DNS ホスト名、NetBIOS 名、または MAC アドレスを単一のアセットが累積したときに発生します。増加の逸脱が検出されると、システムは、それらのアセット・プロファイルに対する以降の着信更新をすべて中断します。

ユーザー応答

次のようにしてアセットの増加状況の逸脱の原因を判別します。

- マウスのポインターを通知の説明の上に移動して、通知のペイロードを確認します。ペイロードによって、最も頻繁に逸脱するアセットの上位 5 件のリストが表示されます。システムが各アセットに増加状況の逸脱のマークを付けた理由、およびアセットがアセットのサイズしきい値を超えて増加しようとした回数に関する情報も表示されます。

- 通知の説明で、「これらのアセットのレポートを確認 **(Review a report of these assets)**」をクリックして、過去 24 時間に発生したアセットの増加状況の逸脱の完全レポートを表示します。
- アセットの増加状況の逸脱に関する資料を参照してください。

高負荷のカスタム・プロパティーが見つかった

38750138 - イベント・パイプラインでパフォーマンスの低下が検出されました。高負荷のカスタム・プロパティーが見つかりました。

説明

通常の処理中、最適化済みとマーク付けされているカスタム・イベントおよびカスタム・フローのプロパティーは、パイプライン内で抽出されます。これらの値はただちにカスタム・ルール・エンジン (CRE) で使用可能になり、直接ストレージに経路指定されます。

形式の正しくない正規表現 (regex) ステートメントは、イベントが誤って直接ストレージに経路指定される原因になることがあります。

ユーザー応答

次のオプションのいずれかを選択してください。

- 通知のペイロードを確認します。必要な場合は、カスタム・プロパティーに関連付けられている regex ステートメントを改善します。
- プロパティーが突き合わせを試行するカテゴリーの範囲を絞り込むために、カスタム・プロパティー定義を変更します。
- イベント解析の不要な試行を避けるために、カスタム・プロパティー定義には単一のイベント名を指定してください。

RAID コントローラー構成の誤り

38750140 - RAID コントローラーの構成の誤り: ハードウェア・モニターにより、仮想ドライブの構成に誤りがあることが検出されました。

説明

パフォーマンスを最大限に高めるには、RAID コントローラー・キャッシュおよびバッテリー・バックアップ装置 (BBU) がライトバック・キャッシュ・ポリシーを使用するように構成する必要があります。ライトスルー・キャッシュ・ポリシーを使用すると、ストレージ・パフォーマンスが低下してシステムが不安定になることがあります。

ユーザー応答

バッテリー・バックアップ装置の正常性を確認します。バッテリー・バックアップ装置が正しく作動している場合、キャッシュ・ポリシーをライトバックに変更します。

ログ・ファイルの収集時にエラーが発生した

38750141 - 必要なサポート・ログの収集がエラーで失敗しました。「システムおよびライセンス管理」を参照してください。

説明

ログ・ファイルの収集中にエラーが発生しました。ログ・ファイルの収集は失敗しました。

ユーザー応答

収集が失敗した原因について情報を確認するには、次の手順を実行します。

1. 通知メッセージの「システムおよびライセンス管理」をクリックします。
2. 「システム・サポート・アクティビティー・メッセージ」を展開します。
3. ログ・ファイルの収集が失敗した原因について詳細情報を確認します。

高負荷の DSM 拡張が見つかった

38750143 - イベント・パイプラインでパフォーマンスの低下が検出されました。高負荷の DSM 拡張が見つかりました。

説明

ログ・ソース拡張とは、イベント・ペイロードからのイベントを識別し分類するために必要な正規表現パターンをすべて格納している XML ファイルです。ログ・ソース拡張は、エラー・ログや一部のシステム通知では、デバイス拡張 と呼ばれる場合があります。

通常の処理では、ログ・ソース拡張はイベント・パイプライン内で実行されます。これらの値はただちにカスタム・ルール・エンジン (CRE) で使用可能になり、ディスクに保管されます。

形式の正しくない正規表現 (regex) は、イベントが直接ストレージに経路指定される原因になることがあります。

ユーザー応答

次のオプションのいずれかを選択してください。

- 通知のペイロードを確認します。可能な場合は、デバイス拡張に関連付けられている regex ステートメントを改良します。
- ログ・ソース拡張が正しいログ・ソースにのみ適用されていることを確認します。

  「管理」タブで、「システム構成」 > 「データ・ソース」 > 「ログ・ソース」をクリックします。各ログ・ソースを選択し、「編集」をクリックして、ログ・ソースの詳細を確認します。
- バッチ・ログ・ソースを使用している場合は、イベント・スロットルを変更して、イベントがディスクのバッファーに入れられないようにします。イベント・スロットル設定は、ログ・ソースに対するプロトコル構成の一部です。

第 4 章 QRadar アプライアンスの情報通知

IBM Security QRadar は、プロセスまたはアクションの状況または結果に関する情報メッセージを提供します。

自動更新が正常にダウンロードされた

38750068 - 自動更新が正常にダウンロードされました。詳しくは、「自動更新ログ」を参照してください。

説明

ソフトウェア更新が自動的にダウンロードされました。

ユーザー応答

通知内のリンクをクリックして、ダウンロードされた更新をインストールする必要があるかどうかを判別してください。

自動更新が正常に完了した

38750070 - 自動更新が正常に完了しました。

説明

自動ソフトウェア更新が正常にダウンロードおよびインストールされました。

ユーザー応答

アクションは不要です。

SAR 標識動作の復元

38750072 - SAR 標識: 通常の動作が復元されました。

説明

システム・アクティビティー・レポーター (SAR) ユーティリティーで、システム負荷が受容できるレベルに戻ったことが検出されました。

ユーザー応答

アクションは不要です。

ディスク使用率が正常に戻る

38750077 - ディスク監視機能: システムのディスク使用量が通常レベルに戻りました。

説明

ディスク監視機能で、ディスク使用率が全容量の 90% を下回っていることが検出されました。

ユーザー応答

アクションは不要です。

インフラストラクチャー・コンポーネントが修復された

38750084 - 破損したインフラストラクチャー・コンポーネントが修復されました。

説明

管理対象ホスト上のホスト・サービスを担当している破損したコンポーネントが修復されました。

ユーザー応答

アクションは不要です。

ディスク・ストレージを使用できる

38750093 - 以前はアクセス不能であった 1 つ以上のストレージ区画がアクセス可能になりました。

説明

ディスク監視機能で、ストレージ区画を使用できることが検出されました。

ユーザー応答

アクションは不要です。

ライセンスの有効期限が近づいている

38750124 - ライセンスの有効期限がもうすぐ切れます。期限までに置き換える必要があります。

説明

アプライアンスのライセンスの有効期限が 35 日以内に切れることをシステムが検出しました。

ユーザー応答

アクションは不要です。

ライセンス割り振りの猶予期間の期限

38750125 - 割り振られているライセンスの猶予期間がもうすぐ終了します。まもなくロックされます。

説明

アプライアンスのライセンス変更がライセンスの猶予期間内であることをシステムが検出しました。

管理者は、ロックされていないライセンスを移動したり、未使用のイベントまたはフローのライセンスを、デプロイメント内の他のアプライアンスに適用したりできます。ライセンスをホストに割り振るときに、14 日間というライセンスの猶予期間が開始します。猶予期間の有効期限が切れると、ライセンスを移動できなくなります。

ユーザー応答

アクションは不要です。

ログ・ファイルが正常に収集された

38750142 - 必要なサポート・ログが正常に収集されました。「システムおよびライセンス管理」を参照してください。

説明

ログ・ファイルが正常に収集されました。

ユーザー応答

収集したログ・ファイルをダウンロードするには、次の手順を実行します。

1. 通知メッセージの「システムおよびライセンス管理」をクリックします。
2. 「システム・サポート・アクティビティー・メッセージ」を展開します。
3. 「ファイルをダウンロードするには、ここをクリックしてください」をクリックします。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様になんら義務も負わせない適切な方法で、使用もしくは配布することがあります。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、 IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

［マ行］

［ラ行］

H

R

S

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21