IBM Security QRadar SIEM
バージョン **7.2.6**

高可用性ガイド

注記

本書および本書で紹介する製品を使用する前に、 53 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。

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.2.6 および以降のリリースに適用されます。

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。

本書は下記原典を翻訳したものです。

原典： IBM Security QRadar SIEM
Version 7.2.6
High Availability Guide

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

IQRadar の高可用性デプロイメントの概要

管理者は、高可用性 (HA) ソリューションを実装することにより、IBM® Security QRadar® データを保護することができます。

対象読者

QRadar SIEM 製品のインストールとデプロイを行う管理者は、自社のネットワーク・インフラストラクチャー、Linux オペレーティング・システム、およびネットワーク・テクノロジーについて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については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) 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 HA 概要

ハードウェアやネットワークで障害が発生した場合でも、IBM Security QRadar は高可用性 (HA) アプライアンスを使用することで、イベント・データとフロー・データの収集、保管、および処理を継続できます。

HA を有効にするため、QRadar はプライマリー HA ホストとセカンダリー HA ホストを接続して HA クラスターを作成します。

プライマリー HA ホストで障害が発生した場合、セカンダリー HA ホストはデータ同期機能または共有外部ストレージを使用して、プライマリー HA ホストと同じデータへのアクセスを維持します。

セカンダリー HA ホストは、プライマリー HA ホストからライセンスを継承します。セカンダリー・ホストに別のライセンスを適用する必要はありません。

iSCSI、ファイバー・チャネル、NFS などの共有外部ストレージを HA で使用する方法について詳しくは、「*IBM Security QRadar Offboard Storage Guide*」を参照してください。

特に断りがない限り、QRadar は QRadar SIEM and IBM Security QRadar Log Manager のことを指します。

関連概念:

3 ページの『HA クラスター』
高可用性 (HA) クラスターは、プライマリー HA ホスト、セカンダリー HA ホスト、クラスター仮想 IP アドレスから構成されます。

『HA のデータの整合性』
HA フェイルオーバーが発生すると、IBM Security QRadar によってデータの整合性が確保されます。

HA のデータの整合性

HA フェイルオーバーが発生すると、IBM Security QRadar によってデータの整合性が確保されます。

使用するストレージのタイプにより、HA データの整合性を保守する方法が決まります。外部ストレージを持つ HA を構成した場合、iSCSI やファイバー・チャネルなどの外部ストレージ・デバイス・コンポーネントを使用して、データの整合性が保守されます。 14 ページの『HA のためのオフボード・ストレージ要件』を参照してください。

外部のストレージ・デバイスを使用しない場合、QRadar HA は Distributed Replicated Block Device を使用して、プライマリー HA ホストとセカンダリー HA ホスト間のデータの整合性を保守します。

デフォルトでは、IBM Security QRadar QFlow コレクター に対して Distributed Replicated Block Device は有効になっていません。 QRadar QFlow データを同期

化するには、QRadar QFlow データを収集するコンソールまたは管理対象ホストを使用して、HA クラスターを構成する必要があります。

データの同期は、以下の場合に HA 環境内で実行されます。

- HA クラスターを初めて構成した場合。
- フェイルオーバー後にプライマリー HA ホストをリストアした場合。
- 通常の HA 操作を実行すると、プライマリー・ホストとセカンダリー・ホスト間でリアルタイムにデータが同期化されます。

関連概念:

1 ページの『第 1 章 HA 概要』
ハードウェアやネットワークで障害が発生した場合でも、IBM Security QRadar は高可用性 (HA) アプライアンスを使用することで、イベント・データとフロー・データの収集、保管、および処理を継続できます。

14 ページの『リンク帯域幅と待ち時間』
高可用性 (HA) を構成するには、プライマリー HA ホストとセカンダリー HA ホスト間の帯域幅と待ち時間を考慮する必要があります。

17 ページの『HA ホストの状況』
高可用性 (HA) クラスター内のプライマリー・ホストとセカンダリー・ホストの状況を確認できます。

リアルタイムのデータ同期

HA クラスターを構成すると、プライマリー HA ホスト上の /store ファイル・システムが、セカンダリー HA ホスト上の /store パーティションと自動的に同期化されます。

プライマリー HA ホストでフェイルオーバーが発生すると、セカンダリー HA ホスト上の /store ファイル・システムがローカル・ディスクに自動的にマウントされ、フェイルオーバーの発生前にプライマリー HA ホストが受信したデータに対して、読み取り操作と書き込み操作が引き続き実行されます。

データの同期が完了すると、セカンダリー HA ホストの状況が「スタンバイ」になります。

プライマリーの /store パーティションのサイズとパフォーマンスに応じて、ディスクの同期にかかる時間が長くなることがあります。プライマリー HA ホストとセカンダリー HA ホスト間の接続の帯域幅が、1 Gbps 以上であることを確認してください。

関連概念:

17 ページの『HA ホストの状況』
高可用性 (HA) クラスター内のプライマリー・ホストとセカンダリー・ホストの状況を確認できます。

フェイルオーバー後のデータ同期

プライマリー高可用性 (HA) ホストによってフェイルオーバーの発生時点まで収集されたデータは、セカンダリー HA ホスト上で実質的にリアルタイムに維持されます。

フェイルオーバーからリストアされると、プライマリー HA ホストの状況はオフラインになります。このプライマリー HA ホストをアクティブなホストにするには、オンライン状態に設定する必要があります。プライマリー HA ホストがオフラインになっている間は、セカンダリー HA ホストによるディスク複製が有効になります。

プライマリー HA ホストがリストアされると、フェイルオーバー中にセカンダリー HA ホストによって収集されたデータだけが、プライマリー HA ホストのデータと同期化されます。そのため、ホストを手動で修復するときに、プライマリー HA ホスト上のディスクを交換したり再フォーマットしない限り、フェイルオーバー後のディスク同期は、初期のディスク同期よりも短時間で終了します。

関連タスク:

24 ページの『HA ホストをオンラインに設定する』
プライマリー HA ホストまたはセカンダリー HA ホストをオンラインに設定することができます。

HA クラスター

高可用性 (HA) クラスターは、プライマリー HA ホスト、セカンダリー HA ホスト、クラスター仮想 IP アドレスから構成されます。

プライマリー HA ホスト

プライマリー HA ホストとは、障害の発生時にデータ損失を防ぐ必要がある IBM Security QRadar SIEM のデプロイメント環境内の任意のコンソールまたは管理対象ホストのことです。

HA クラスターを作成すると、プライマリー HA ホストの IP アドレスがクラスター仮想 IP アドレスに自動的に再割り当てされます。そのため、使用されていない IP アドレスをプライマリー HA ホストに割り当てる必要があります。

プライマリー HA ホストは、セカンダリー HA ホストに代わってスタンバイ・システムとして機能することがあります。例えば、フェイルオーバー後にプライマリー HA ホストを修復した場合、状況はスタンバイに変更されます。

セカンダリー HA ホスト

セカンダリー HA ホストは、プライマリー HA ホストのスタンバイ・システムです。

プライマリー HA ホストで障害が発生した場合、セカンダリー HA ホストがプライマリー HA ホストのすべての処理を自動的にテークオーバーします。

仮想 IP アドレス

HA クラスターを作成すると、クラスター仮想 IP アドレスがプライマリー HA ホストの IP アドレスを引き継ぎます。

クラスターの構成

HA ウィザードを使用して、プライマリー・ホスト、セカンダリー・ホスト、およびクラスターの仮想 IP アドレスを構成します。

HA ウィザードを使用して構成するときに、次の項目が検証されます。

- セカンダリー HA ホストに有効な HA アクティベーション・キーがあるかどうか。
- セカンダリー HA ホストが別の HA クラスターの一部になっていないかどうか。
- プライマリー HA ホストとセカンダリー HA ホスト上のソフトウェアのバージョンが同じかどうか。
- プライマリー HA ホストで外部のストレージ・デバイスが構成されている場合、セカンダリー HA ホストが同じ外部のストレージ・デバイスにアクセスするように構成されているかどうか。
- プライマリー HA ホストとセカンダリー HA ホストで、同じデバイス・サポート・モジュール (DSM)、スキャナー、およびプロトコル RPM がサポートされているかどうか。

関連概念:

1 ページの『第 1 章 HA 概要』
ハードウェアやネットワークで障害が発生した場合でも、IBM Security QRadar は高可用性 (HA) アプライアンスを使用することで、イベント・データとフロー・データの収集、保管、および処理を継続できます。

5 ページの『プライマリー HA ホストでの障害』
セカンダリー高可用性 (HA) ホストがプライマリー HA ホストでの障害を検出すると、セカンダリー HA ホストが自動的にプライマリー HA ホストの処理をテークオーバーしてアクティブなシステムになります。

17 ページの『HA ホストの状況』
高可用性 (HA) クラスター内のプライマリー・ホストとセカンダリー・ホストの状況を確認できます。

13 ページの『IP アドレスとサブネット』
高可用性 (HA) を構成するには、セカンダリー HA ホストで使用されるサブネットと、仮想 IP アドレスを考慮する必要があります。

関連タスク:

20 ページの『HA クラスターの作成』
IBM Security QRadar を使用して、プライマリー・ホスト、セカンダリー高可用性 (HA) ホスト、仮想 IP アドレスの組み合わせを作成すると、HA クラスターが作成されます。

フェイルオーバー

プライマリーまたはセカンダリーの高可用性 (HA) ホストで障害が発生した場合、IBM Security QRadar によってデータの整合性が維持されます。

以下の場合にフェイルオーバーが発生します。

- 電源装置で障害が発生した場合。

- ネットワーク接続テストでネットワーク障害が検出された場合。
- オペレーティング・システムの問題により、ハートビート ping テストが遅延または停止した場合。
- プライマリー HA ホスト上の Redundant Array of Independent Disks (RAID) がまったく機能しなくなった場合。
- 手動フェイルオーバーが実行された場合
- プライマリー HA ホスト上の管理インターフェースで障害が発生した場合。

プライマリー HA ホストでの障害

セカンダリー高可用性 (HA) ホストがプライマリー HA ホストでの障害を検出すると、セカンダリー HA ホストが自動的にプライマリー HA ホストの処理をテークオーバーしてアクティブなシステムになります。

プライマリー HA ホストがフェイルオーバーからリカバリーされても、HA クラスター内で自動的にアクティブな状況をテークオーバーするわけではありません。この場合、セカンダリー HA ホストがアクティブ・システムのままになり、プライマリー・ホストはスタンバイ・システムとして機能します。

プライマリー・ホストでの障害が正常にリカバリーされたら、プライマリー・ホストの状況を「アクティブ」に戻す必要があります。

関連概念:

3 ページの『HA クラスター』
高可用性 (HA) クラスターは、プライマリー HA ホスト、セカンダリー HA ホスト、クラスター仮想 IP アドレスから構成されます。

関連タスク:

25 ページの『プライマリー HA ホストをアクティブ・システムに切り替える』
プライマリー高可用性 (HA) ホストをアクティブなシステムに設定することができます。

セカンダリー HA ホストでの障害

プライマリー高可用性 (HA) ホストがセカンダリー HA ホストでの障害を検出すると、プライマリー HA ホストが自動的にセカンダリー HA ホストの処理を引き継いでアクティブなシステムになります。

プライマリー高可用性 (HA) ホストがセカンダリー HA ホストでの障害を検出すると、プライマリー HA ホストが自動的にセカンダリー HA ホストの処理を引き継いでアクティブなシステムになります。

フェイルオーバーが発生しないシナリオ

IBM Security QRadar がソフトウェア・エラーやディスク容量の問題を検出しても、HA フェイルオーバーが発生しません。

次の問題では、HA の自動フェイルオーバーは発生しません。

- QRadar プロセスでエラーが発生した場合、機能が停止するか、プロセスが停止してエラーが出力されます。

- プライマリー HA ホスト上のディスク使用率が 95% に達した場合、QRadar のデータ収集が停止しますが、プライマリー HA ホストは引き続き稼働します。

HA フェイルオーバー・イベントの順序

IBM Security QRadar は、プライマリー高可用性 (HA) ホストで障害が発生した場合に、一連のイベントを開始します。

フェイルオーバーが発生すると、セカンダリー HA ホストがプライマリー HA ホストの処理を引き継ぎます。次の一連のアクションが、順に実行されます。

1. 外部の共有ストレージ・デバイスが検出され (構成されている場合)、ファイル・システムがマウントされます。詳しくは、「IBM Security オフボード・ストレージ・ガイド」を参照してください。
2. 管理インターフェースのネットワーク別名が作成されます。例えば、eth0 のネットワーク別名は eth0:0 になります。
3. クラスター仮想 IP アドレスが上記のネットワーク別名に割り当てられます。
4. すべての QRadar サービスが開始されます。
5. セカンダリー HA ホストがコンソールに接続され、構成ファイルがダウンロードされます。

ネットワーク接続テスト

ネットワーク接続をテストするために、プライマリー高可用性 (HA) ホストは、IBM Security QRadar のデプロイメントのすべての管理対象ホストに対して、自動的に ping を実行します。

プライマリー HA ホストから管理対象ホストへのネットワーク接続が失われた場合であっても、セカンダリー HA ホストへの接続は維持されます。セカンダリー HA ホストは、管理対象ホストを使用して、別のネットワーク接続テストを実行します。このテストが成功した場合、プライマリー HA ホストは、セカンダリー HA ホストへの制御フェイルオーバーを実行します。テストが失敗した場合、2 次 HA ホストでもネットワーク接続の問題が発生している可能性があるため、HA フェイルオーバーは実行されません。

関連タスク:

20 ページの『HA クラスターの作成』

IBM Security QRadar を使用して、プライマリー・ホスト、セカンダリー高可用性 (HA) ホスト、仮想 IP アドレスの組み合わせを作成すると、HA クラスターが作成されます。

ハートビート ping テスト

ハートビート ping テストの時間間隔を構成することにより、プライマリー高可用性 (HA) ホストの動作をテストできます。

事前に構成された時間内にプライマリー HA ホストからの応答をセカンダリー HA ホストが受信しなかった場合、セカンダリー HA ホストに対する自動フェイルオーバーが実行されます。

関連タスク:

20 ページの『HA クラスターの作成』
IBM Security QRadar を使用して、プライマリー・ホスト、セカンダリー高可用性 (HA) ホスト、仮想 IP アドレスの組み合わせを作成すると、HA クラスターが作成されます。

プライマリー・ディスク障害

RAID がまったく機能しなくなり、すべてのディスクが使用できなくなった場合、プライマリー HA ホストはシャットダウンを実行し、セカンダリー HA ホストにフェイルオーバーします。

フェイルオーバーが発生すると、プライマリー HA ホストの状況が「失敗」になります。

関連概念:

17 ページの『HA ホストの状況』
高可用性 (HA) クラスター内のプライマリー・ホストとセカンダリー・ホストの状況を確認できます。

手動フェイルオーバー

プライマリー高可用性 (HA) ホストからセカンダリー HA ホストに対して、フェイルオーバーを手動で強制的に実行できます。

手動フェイルオーバーは、コンソールや管理対象ホスト上で計画的なハードウェア保守を行う場合に便利です。手動フェイルオーバーを実行する前に、以下の事項を確認してください。

- プライマリー HA ホストとセカンダリー HA ホストが同期化されていること。
- セカンダリー HA ホストの状況が「スタンバイ」になっていること。

プライマリー HA ホストでハードウェア保守を行うには、プライマリー・システムをオフラインに設定して、セカンダリー HA ホストをアクティブにします。セカンダリー・ホストがアクティブになった後、プライマリー・ホストをシャットダウンできます。

セカンダリー HA ホストでハードウェア保守を行う場合は、セカンダリー HA ホストをオフラインに設定し、セカンダリー HA ホストをパワーオフします。

手動フェイルオーバーについて詳しくは、 24 ページの『HA ホストをオフラインに設定する』を参照してください。

パッチやソフトウェア・アップグレードをインストールする場合は、プライマリー HA ホスト上で手動フェイルオーバーを実行しないでください。詳しくは、「*IBM Security QRadar Upgrade Guide*」を参照してください。

関連タスク:

24 ページの『HA ホストをオフラインに設定する』
プライマリーまたはセカンダリーの高可用性 (HA) ホストの状況を、「アクティブ」または「スタンバイ」から「オフライン」に設定することができます。

第 2 章 HA デプロイメントの計画

高可用性デプロイメントを計画します。

高可用性 (HA) を実装する前に、IBM Security QRadar デプロイメントを理解して準備するために、すべての要件を確認してください。

ファームウェア更新

QRadar アプライアンスの内部ハードウェア・コンポーネントについての追加機能と更新を活用するために、IBM Security QRadar アプライアンスのファームウェアを更新します。

ファームウェアの更新方法について詳しくは、Firmware update for QRadar (http://www-01.ibm.com/support/docview.wss?uid=swg27047121) を参照してください。

アプライアンス要件

IBM Security QRadar SIEM コンソール にセカンダリー・ホストを追加する前に、プライマリー・アプライアンスとセカンダリー・アプライアンス間で異なっているハードウェア構成を確認する必要があります。

プライマリー HA とセカンダリー HA のペアとして配置された各アプライアンスは、互換性を確保するためにすべて一致しています。ただし、いずれかのアプライアンスを交換したり、異なるハードウェアが構成されている古いコンソールに HA を追加したりすると、データの複製に関する問題が発生する可能性があります。データの複製に関する問題は、耐用年数を超えたハードウェアを交換した場合や、異なる製造元のアプライアンスが搭載されたプライマリー HA とセカンダリー HA のペアを作成した場合に発生する可能性があります。

/Store パーティションの要件

- /store パーティションのファイル・システムは、プライマリー・ホストとセカンダリー・ホストで一致している必要があります。

  例: プライマリー・ホスト上の /store パーティションで ext-3 がファイル・システムとして使用されている場合、セカンダリー・ホスト上の /store パーティションでも ext-3 を使用する必要があります。/store パーティションでのファイル・システムの不一致は許可されていません。
- セカンダリー・ホスト上の /store パーティションのサイズは、プライマリー・ホスト上の /store パーティションのサイズ以上でなければなりません。

例えば、3 TB の /store パーティションを使用するプライマリー・ホストと、2 TB の /store パーティションを使用するセカンダリー・ホストをペアにすることはできません。

ストレージ要件

アプライアンスを交換するときは、次のストレージ要件に従ってください。

- 新しく交換するアプライアンスに、元のハードウェア以上のストレージ容量があることを確認してください。
- 交換するセカンダリー・アプライアンスのストレージ容量が、プライマリー・アプライアンスのストレージ容量よりも大きい場合があります。その場合は、HA のペアを構成する際に、プライマリー・アプライアンス上のストレージ容量に一致するようにセカンダリー・アプライアンス上のパーティションのサイズが変更されます。
- 交換するプライマリー・アプライアンスのストレージ容量が、セカンダリー・アプライアンスのストレージ容量よりも大きい場合があります。その場合は、HA のペアを構成する際に、セカンダリー・アプライアンス上のストレージ容量に一致するようにプライマリー・アプライアンス上のパーティションのサイズが変更されます。
- プライマリー・アプライアンスとセカンダリー・アプライアンスの両方を交換する場合、最も小さいストレージ容量を持つアプライアンスに合わせて、ストレージ・パーティションのサイズが変更されます。

管理対象インターフェース

- プライマリー・ホストが、セカンダリー・ホストよりも多くの物理インターフェースを持つことはありません。

  フェイルオーバーが発生した場合、プライマリー・ホストのネットワーク構成がセカンダリー・ホストに複製されます。セカンダリー・ホストよりも多くの物理インターフェースを持つようにプライマリー・ホストが構成されている場合、フェイルオーバー時に、それらの追加のインターフェースをセカンダリー・ホストに複製することはできません。
- セカンダリー HA ホストでは、プライマリー HA ホストと同じ管理インターフェースを使用する必要があります。

  プライマリー HA ホストで、例えば管理インターフェースとして eth0 を使用している場合、セカンダリー HA ホストでも eth0 を使用する必要があります。
- 管理インターフェースでは、1 つのクラスター仮想 IP アドレスがサポートされます。
- TCP ポート 7789 を開き、Distributed Replicated Block Device トラフィック用に、プライマリーとセカンダリー間の通信を許可する必要があります。

  Distributed Replicated Block Device トラフィックはディスクの複製を行い、プライマリー・ホストとセカンダリー・ホスト間を双方向に流れていきます。
- プライマリー・アプライアンスとセカンダリー・アプライアンスのペアを初めて作成する前に、プライマリー・ホストとセカンダリー・ホストで QRadar ソフトウェアのバージョンが一致していることを確認する必要があります。

QRadar のバージョンがプライマリー・ホストとセカンダリー・ホストで異なっている場合、プライマリー・アプライアンスとセカンダリー・アプライアンスのいずれかにパッチを適用し、両方のアプライアンスで同じバージョンのソフトウェアを使用する必要があります。

プライマリー ・アプライアンスとセカンダリー・アプライアンスのペアを作成すると、ディスク複製機能により、追加のソフトウェア更新も確実にセカンダリー・アプライアンスに適用されるようになります。

- セカンダリー・ホストに正しい HA アクティベーション・キーが設定されていることを確認してください。

ソフトウェアと仮想アプライアンスの要件

ハードウェアに IBM Security QRadar SIEM ソフトウェアをインストールする場合や、仮想アプライアンスを使用する場合は、高可用性 (HA) を構成する前に、以下の要件を確認してください。

仮想アプライアンスのシステム要件

IBM Security QRadar が正しく動作するようにするため、使用する仮想アプライアンスが最小のソフトウェア要件およびハードウェア要件を満たしていることを確認します。

仮想アプライアンスをインストール前に、次の最小要件を満たしていることを確認します。

表 1. 仮想アプライアンスの要件

要件	説明
VMware クライアント	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 VMWare クライアントについて詳しくは、VMware の Web サイト (www.vmware.com) を参照してください。
QRadar VFlow コレクター、QRadar イベント・コレクター (Event Collector)、QRadar イベント・プロセッサー (Event Processor)、QRadar フロー・プロセッサー、QRadar オールインワン、および QRadar Log Manager の各アプライアンス上の仮想ディスク・サイズ	最小: 256 GB **重要:** パフォーマンスを最適化するには、最小ディスク・スペースの 2 から 3 倍の追加スペースを使用できるようにしてください。
QRadar QFlow コレクター・アプライアンスの仮想ディスク・サイズ	最小: 70 GB

表 1. 仮想アプライアンスの要件 (続き)

要件	説明
QRadar Risk Manager アプライアンスの仮想ディスク・サイズ	1 万件までの構成ソースの実装に推奨される仮想ディスク・サイズ: 1 TB
QRadar Vulnerability Manager プロセッサー・アプライアンスの仮想ディスク・サイズ	50000 個の IP アドレス - 500 GB 150000 個の IP アドレス - 750 GB 300000 個の IP アドレス - 1 TB
QRadar Vulnerability Manager スキャナー・アプライアンスの仮想ディスク・サイズ	20000 個の IP アドレス - 150 GB

仮想アプライアンスの最小メモリー所要量を次の表に示します。

表 2. *QRadar* 仮想アプライアンスの最小およびオプションのメモリー所要量

アプライアンス	最小メモリー所要量	推奨されるメモリー所要量
QRadar VFlow Collector 1299	6 GB	6 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1699	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3199	24 GB	48 GB
QRadar Log Manager Virtual 8090	24 GB	48 GB
QRadar Risk Manager	24 GB	48 GB
QRadar Vulnerability Manager プロセッサー	8 GB	16 GB
QRadar Vulnerability Manager スキャナー	2 GB	4 GB

表 3. 「**CPU**」ページの設定例

プロセッサーの数	**QRadar** アプライアンスに基づくパフォーマンス
4	ログ・マネージャー 3190: 2500 イベント/秒以下。 ログ・マネージャー・イベント・プロセッサー 1690、または SIEM イベント・プロセッサー 1690: 2500 イベント/秒以下。 オールインワン 3190: 25000 フロー/分以下、500 イベント/秒以下。 フロー・プロセッサー 1790: 150,000 フロー/分。 専用コンソール 3190
8	ログ・マネージャー 3190: 5000 イベント/秒以下。 ログ・マネージャー・イベント・プロセッサー 1690、または SIEM イベント・プロセッサー 1690: 5000 イベント/秒以下。 オールインワン 3190: 50000 フロー/分以下、1000 イベント/秒以下。 フロー・プロセッサー 1790: 300,000 フロー/分。
12	オールインワン 3190: 100,000 フロー/分以下、1000 イベント/秒以下。
16	ログ・マネージャー・イベント・プロセッサー 1690、または SIEM イベント・プロセッサー 1690: 20,000 イベント/秒以下。 オールインワン 3190: 200,000 フロー/分以下、5000 イベント/秒以下。

IP アドレスとサブネット

高可用性 (HA) を構成するには、セカンダリー HA ホストで使用されるサブネットと、仮想 IP アドレスを考慮する必要があります。

管理者は、以下の条件が満たされていることを確認する必要があります。

- セカンダリー・ホストは、プライマリー・ホストと同じサブネット内に存在している必要があります。
- プライマリー・ホストの IP アドレスをクラスター仮想 IP アドレスとして再割り当てする場合、その新しい IP アドレスは同じサブネット内に存在している必要があります。
- HA クラスターに追加するセカンダリー HA ホストは、別の HA クラスター内のコンポーネントであってはなりません。

関連概念:

3 ページの『HA クラスター』
高可用性 (HA) クラスターは、プライマリー HA ホスト、セカンダリー HA ホスト、クラスター仮想 IP アドレスから構成されます。

リンク帯域幅と待ち時間

高可用性 (HA) を構成するには、プライマリー HA ホストとセカンダリー HA ホスト間の帯域幅と待ち時間を考慮する必要があります。

HA クラスターでディスク同期機能を使用する場合は、以下の条件を満たす必要があります。

- プライマリー HA ホストとセカンダリー HA ホスト間の接続用に 1 ギガビット/秒 (Gbps) 以上の帯域幅が確保されていること。
- プライマリー HA ホストとセカンダリー HA ホスト間の待ち時間が 2 ミリ秒 (ms) 未満であること。

注**:** HA ソリューションで広域ネットワーク (WAN) を使用してクラスター内の各ホストを地理的に分散させた場合、そのホストまでの距離に従って待ち時間が長くなります。待ち時間が 2 ミリ秒を超えると、システムのパフォーマンスが影響を受けます。

関連概念:

1 ページの『HA のデータの整合性』
HA フェイルオーバーが発生すると、IBM Security QRadar によってデータの整合性が確保されます。

データのバックアップ要件

高可用性 (HA) のホストを構成する前に、データのバックアップについていくつかの事項を考慮する必要があります。

バックアップ・アーカイブの作成元が HA クラスターの場合は、リストアの完了後に「すべての構成のデプロイ」をクリックして、HA クラスター構成をリストアします。ディスク複製が有効になっている場合、システムのリストア後、セカンダリー HA ホストによって即時にデータが同期されます。

バックアップの完了後にセカンダリー HA ホストをデプロイメント環境から削除すると、「システムおよびライセンス管理」ウィンドウで、セカンダリー HA ホストの状況が「失敗」と表示されます。

HA 環境でのバックアップ・アーカイブのリストアについては、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

HA のためのオフボード・ストレージ要件

IBM Security QRadar の `/store` パーティションが iSCSI デバイスやファイバー・チャネル・デバイスなどの外部ストレージ・ソリューションにマウントされているときに、高可用性 (HA) を実装できます。

外部のストレージ・ソリューションを実装すると、プライマリー HA ホストが受信したデータは、自動的にその外部デバイスに転送されます。このデータには、検索やレポート作成用にアクセスすることができます。

フェイルオーバーが発生した場合は、セカンダリー HA ホスト上の `/store` パーティションが自動的に外部デバイスにマウントされます。外部デバイス上では、フェ

イルオーバーが発生する前にプライマリー HA ホストが受信したデータに対して、引き続き読み取り操作と書き込み操作が実行されます。

HA が実装された共有外部ストレージの構成については、「IBM Security QRadar オフボード・ストレージ・ガイド」を参照してください。

管理者は、オフボードのストレージ・デバイスを実装する前に、以下の HA 要件について確認する必要があります。

- 外部デバイスと通信するようにプライマリー HA ホストを構成する必要があります。ローカル・ディスク上の `/store` パーティション内のデータは、外部ストレージ・デバイスに移動する必要があります。
- 外部デバイスと通信するようにセカンダリー HA ホストを構成する必要があります。これにより、プライマリー HA ホストでフェイルオーバーが発生した場合に、セカンダリー HA ホストで外部ストレージ・デバイスを検出できるようになります。
- HA クラスターを作成するには、同じ外部ストレージ・デバイスにアクセスするようにセカンダリー HA ホストを構成しておく必要があります。
- 外部ストレージ・デバイスまたは HA クラスターの設定を再構成する場合は、プライマリー HA ホストとセカンダリー HA ホスト間の HA クラスターを削除する必要があります。詳しくは、『*HA クラスターの切断*』を参照してください。
- 各 HA ホストと外部デバイスとの間に 1 Gbps 以上の接続が確立されていることを確認してください。

重要**:** QRadar へのアップグレード時に、HA クラスター内のホストに対する外部ストレージ・デバイスの接続を再構成する必要があります。詳しくは、「*Reconfiguring Offboard Storage During a QRadar Upgrade Technical Note*」を参照してください。

第 3 章 HA 管理

高可用性 (HA) 設定のチューニング、トラブルシューティング、更新を行う必要がある場合は、IBM Security QRadar SIEM の「管理」タブの「システムおよびライセンス管理」ウィンドウを使用します。

管理者は、「システムおよびライセンス管理」ウィンドウを使用して、HA に関する以下のタスクを実行することができます。

- HA クラスターの状態をモニターする。
- プライマリー HA ホストの手動フェイルオーバーを実行して、プライマリー・ホスト上で保守作業を行う。
- HA クラスターを切断して、プライマリー HA ホストとセカンダリー HA ホストのパーティションを変更する。
- ping テストの時間間隔を構成する (この時間が経過すると、セカンダリー HA ホストに対する自動フェイルオーバーが発生する)。
- ネットワーク接続のテストを制御するための HA クラスター設定を変更する。

HA ホストの状況

高可用性 (HA) クラスター内のプライマリー・ホストとセカンダリー・ホストの状況を確認できます。

以下の表に、「システムおよびライセンス管理」ウィンドウに表示される各ホストの状況を示します。

表 4. *HA* 状況の説明

状況	説明
アクティブ	このホストがアクティブなシステムで、すべてのサービスが正常に稼働していることを示します。プライマリー HA ホストまたはセカンダリー HA ホストのいずれかの状況が「アクティブ」として表示されます。 **注:** セカンダリー HA ホストの状況が「アクティブ」として表示されている場合は、プライマリー HA ホストで障害が発生しています。
スタンバイ	このホストがスタンバイ・システムとして動作していることを示します。スタンバイ状態の場合、サービスは何も実行されませんが、ディスクの複製が有効になっている場合は、データの同期化が実行されます。プライマリー HA ホストまたはセカンダリー HA ホストのいずれかで障害が発生した場合、スタンバイ・システムが自動的にアクティブ・システムになります。

表 4. *HA* 状況の説明 (続き)

状況	説明
失敗	プライマリー・ホストまたはセカンダリー・ホストで障害が発生したことを示します。 プライマリー HA ホストの状況が「失敗」と表示されている場合は、プライマリー HA ホストの処理をセカンダリー HA ホストが引き継ぎ、セカンダリー HA ホストの状況が「アクティブ」として表示されます。 セカンダリー HA ホストの状況が「失敗」と表示されている場合、プライマリー HA ホストはアクティブなままですが、プライマリー・ホストが HA によって保護されることはありません。 「失敗」状態になっているシステムは、手動で修復または交換を行ってからリストアする必要があります。ネットワークで障害が発生した場合は、物理的なアプライアンスにアクセスしなければならないことがあります。
同期中	ホスト間でデータの同期が実行されていることを示します。 **注:** この状況が表示されるのは、ディスクの複製が有効になっている場合のみです。
オンライン	ホストがオンライン状態になっていることを示します。
オフライン	管理者が HA ホストを手動でオフラインに設定したことを示します。オフライン・モードは、通常はアプライアンスの保守を行うために使用される状況を示します。 アプライアンスの状況が「オフライン」になっている場合は、以下のような動作になります。 アクティブな HA ホストとオフラインの HA ホストとの間でデータの複製が実行されます。 オフラインの HA ホストの場合、イベント、フロー、オフェンス、ハートビート ping テストを処理するサービスが停止します。 管理者が HA ホストをオンラインに設定するまで、フェイルオーバーを実行することはできません。
リストア中	ホストがリストア中であることを示します。詳しくは、 41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』を参照してください。
ライセンスが必要	HA クラスターに対してライセンス・キーが必要であることを示します。この状況の場合、プロセスは何も実行されません。 ライセンス・キーの適用について詳しくは、「管理ガイド」を参照してください。
オフラインに設定中	管理者が HA ホストの状況をオフラインに変更していることを示します。
オンラインに設定中	管理者が HA ホストの状況をオンラインに変更していることを示します。

表 4. HA 状況の説明 (続き)

状況	説明
アップグレードが必要	セカンダリー HA ホストでソフトウェアのアップグレードが必要であることを示します。 「アップグレードが必要」状況が表示されているときは、プライマリー・ホストはアクティブなままですが、プライマリー・ホストがフェイルオーバーに対して保護されることはありません。イベントとフローのディスク複製は、プライマリー HA ホストとセカンダリー HA ホスト間で続行されます。
アップグレード中	プライマリー HA ホストによってセカンダリー HA ホストがアップグレードされていることを示します。 セカンダリー HA ホストの状況が「アップグレード中」と表示されている場合、プライマリー HA ホストはアクティブなままですが、プライマリー・ホストが HA によって保護されることはありません。ハートビートのモニターとディスクの複製は、引き続き機能します (有効に設定されている場合)。 DSM またはプロトコルをコンソールにインストールしてデプロイすると、そのコンソールにより、DSM とプロトコルの更新内容が管理対象ホストに複製されます。プライマリー HA ホストとセカンダリー HA ホストが同期化されると、DSM とプロトコルの更新内容がセカンダリー HA ホストにインストールされます。 「アップグレード中」状況が表示される可能性があるのは、セカンダリー HA ホストだけです。

関連概念:

2 ページの『リアルタイムのデータ同期』
HA クラスターを構成すると、プライマリー HA ホスト上の /store ファイル・システムが、セカンダリー HA ホスト上の /store パーティションと自動的に同期化されます。

3 ページの『HA クラスター』
高可用性 (HA) クラスターは、プライマリー HA ホスト、セカンダリー HA ホスト、クラスター仮想 IP アドレスから構成されます。

7 ページの『プライマリー・ディスク障害』
RAID がまったく機能しなくなり、すべてのディスクが使用できなくなった場合、プライマリー HA ホストはシャットダウンを実行し、セカンダリー HA ホストにフェイルオーバーします。

1 ページの『HA のデータの整合性』
HA フェイルオーバーが発生すると、IBM Security QRadar によってデータの整合性が確保されます。

関連タスク:

41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』
プライマリー HA ホストとセカンダリー HA ホストが作動可能な状態になっているかどうかを確認する必要があります。

HA クラスターの IP アドレスの表示

高可用性 (HA) クラスター内のすべてのコンポーネントの IP アドレスを表示することができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. QRadar のプライマリー・コンソールを特定します。
5. マウスを「ホスト名」フィールドにポイントします。

HA クラスターの作成

IBM Security QRadar を使用して、プライマリー・ホスト、セカンダリー高可用性 (HA) ホスト、仮想 IP アドレスの組み合わせを作成すると、HA クラスターが作成されます。

始める前に

プライマリー HA ホストで外部ストレージが構成されている場合は、同じ外部ストレージ・オプションを使用するようにセカンダリー HA ホストを構成する必要があります。詳しくは、「QRadar オフボード・ストレージ・ガイド」を参照してください。

このタスクについて

ディスクの同期機能が有効になっている場合は、プライマリー HA ホストの `/store` パーティション内のデータがセカンダリー HA ホスト上のデータと最初に同期化されるまで、24 時間以上かかることがあります。

プライマリー HA ホストで障害が発生し、セカンダリー HA ホストがアクティブになった場合、クラスター仮想 IP アドレスがセカンダリー HA ホストに割り当てられます。

HA デプロイメント環境の場合、プライマリー HA ホストとセカンダリー HA ホストの両方のインターフェースが飽和状態になる可能性があります。パフォーマンスが影響を受ける場合は、プライマリー HA ホストとセカンダリー HA ホストで別のインターフェースのペアを使用して、HA とデータ複製を管理することができます。これらのインターフェースに接続するには、クロスケーブルを使用します。

手順

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「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. HA を構成する対象ホストを選択します。
5. 「アクション」メニューで「**HA** ホストの追加」を選択して「**OK**」をクリックします。

6. 説明テキストを読み、「次へ」をクリックします。
7. 以下のパラメーターの値を入力します。

オプション	説明
プライマリー・ホスト **IP** アドレス	プライマリー HA ホストの新しい IP アドレス。新しい IP アドレスにより、以前の IP アドレスが置き換えられます。プライマリー HA ホストの現在の IP アドレスは、クラスター仮想 IP アドレスになります。 プライマリー HA ホストの新しい IP アドレスは、仮想ホストの IP アドレスと同じサブネット上に存在している必要があります。 IPv6 については、インストール時に IPv6 に対して QRadar を自動構成するオプションに「はい」を選択した場合、記録した IP アドレスを入力します。
セカンダリー **HA** ホスト **IP** アドレス	セカンダリー HA ホストの IP アドレス。セカンダリー HA ホストは、プライマリー HA ホストと同じサブネット上に存在している必要があります。
ホストの **root** パスワードの入力 **(Enter the root password of the host)**	セカンダリー HA ホストの root パスワード。このパスワードで特殊文字を使用することはできません。
ホストの **root** パスワードの確認 **(Confirm the root password of the host)**	確認のため、セカンダリー HA ホストの root パスワードをもう一度入力します。

8. 拡張パラメーターを構成するには、「拡張オプションを表示」の横に表示されている矢印をクリックして、パラメーターの値を入力します。

オプション	説明
ハートビート間隔 **(秒)**	ハートビート ping を実行する間隔を秒数で指定します。デフォルト値は 10 秒です。 ハートビート ping について詳しくは、 6 ページの『ハートビート ping テスト』を参照してください。
ハートビート・タイムアウト **(秒)**	ハートビートが検出されない場合に、プライマリー HA ホストが使用不可の状態になっているとみなすまでの時間を秒数で指定します。デフォルト値は 30 秒です。

オプション	説明
ネットワーク接続テストでピア **IP** アドレスをリストする **(**コンマ区切り**) (Network Connectivity Test List peer IP addresses (comma delimited))**	セカンダリー HA ホストが ping を実行する対象ホストの IP アドレス。デフォルトでは、QRadar のデプロイメント環境内の他のすべての管理対象ホストが ping されます。 ネットワーク接続テストについて詳しくは、 6 ページの『ネットワーク接続テスト』を参照してください。
ディスクの同期速度 **(MB/秒) (Disk Synchronization Rate (MB/s))**	ディスクの同期速度。デフォルト値は 100 MB/秒 です。
ディスク複製の無効化	このオプションが表示されるのは、管理対象ホストを使用して HA クラスターを構成する場合だけです。
クロスケーブルの構成	クロスケーブルは、QRadar が複製トラフィックをその他すべての QRadar トラフィック (イベント、フロー、照会など) から分離できるようにします。
クロス・インターフェース	プライマリー HA ホストに接続するインターフェースを選択します。アクティブなリンクが存在するインターフェースのみ、リストに表示されます。
クロス詳細オプション	プロパティー値の入力、編集、表示を行うには、「クロス詳細オプションの表示」を選択します。

9. 「次へ」をクリックしてから「終了」をクリックします。

重要**:** HA クラスターが構成されると、その HA クラスター内で使用される IP アドレスを表示できるようになります。「システムおよびライセンス管理」ウィンドウの「ホスト名」フィールドにマウスをポイントしてください。

関連概念:

3 ページの『HA クラスター』
高可用性 (HA) クラスターは、プライマリー HA ホスト、セカンダリー HA ホスト、クラスター仮想 IP アドレスから構成されます。

6 ページの『ネットワーク接続テスト』
ネットワーク接続をテストするために、プライマリー高可用性 (HA) ホストは、IBM Security QRadar のデプロイメントのすべての管理対象ホストに対して、自動的に ping を実行します。

6 ページの『ハートビート ping テスト』
ハートビート ping テストの時間間隔を構成することにより、プライマリー高可用性 (HA) ホストの動作をテストできます。

関連タスク:

28 ページの『セカンダリー HA コンソールまたは非コンソールのリカバリー』
セカンダリー高可用性 (HA) IBM Security QRadar または非コンソール (管理対象ホスト) アプライアンスのインストールやリカバリーを実行することができます。

35 ページの『障害が発生したプライマリー HA コンソールまたは非コンソール上での IBM Security QRadar のリカバリー』
障害が発生したプライマリー HA ホスト上の IBM Security QRadar コンソールまたは非コンソール (管理対象ホスト) ソフトウェアをリカバリーすることができます。

HA クラスターの切断

HA クラスターを切断すると、プライマリー HA コンソールまたは管理対象ホスト上のデータは、ネットワークやハードウェアの障害に対して保護されなくなります。

始める前に

/store ファイル・システムをファイバー・チャネル・デバイスにマイグレーションした場合、HA クラスターを切断する前に、/etc/fstab ファイルを変更する必要があります。詳しくは、『/etc/fstab ファイルの更新』を参照してください。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. 削除する HA ホストを選択します。
5. ツールバーで「高可用性」 > 「**HA** ホストの削除」を選択します。
6. 「**OK**」をクリックします。

注**:** クラスターから HA ホストを削除すると、そのホストが再始動します。

/etc/fstab ファイルの更新

ファイバー・チャネルの HA クラスターを切断する前に、 /etc/fstab ファイルの /store マウント情報と /store/tmp マウント情報を変更する必要があります。

このタスクについて

プライマリー HA ホストとセカンダリー HA ホストの /etc/fstab ファイルを更新する必要があります。

手順

1. SSH を使用して、root ユーザーとして QRadar ホストにログインします。
2. etc/fstab ファイルを変更します。
   a. /store ファイル・システムおよび /store/tmp ファイル・システムの既存のマウント情報を見つけます。
   b. /store ファイル・システムおよび /store/tmp ファイル・システムの **noauto** オプションを削除します。
3. ファイルを保存して閉じます。

次のタスク

HA クラスターを切断します。

HA クラスターの編集

HA クラスターの拡張オプションを編集することができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. 編集したい HA クラスターの行を選択します。
5. ツールバーで、「高可用性」 > 「**HA** ホストの編集」を選択します。
6. 拡張オプション・セクションの表でパラメーターを編集します。
7. 「次へ」をクリックします。
8. 情報を確認します。
9. 「終了」をクリックします。

HA ホストをオフラインに設定する

プライマリーまたはセカンダリーの高可用性 (HA) ホストの状況を、「アクティブ」または「スタンバイ」から「オフライン」に設定することができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. オフラインに設定する HA ホストを選択します。
5. ツールバーで、「高可用性」 > 「システムをオフラインに設定」を選択します。

関連概念:

7 ページの『手動フェイルオーバー』

プライマリー高可用性 (HA) ホストからセカンダリー HA ホストに対して、フェイルオーバーを手動で強制的に実行できます。

HA ホストをオンラインに設定する

プライマリー HA ホストまたはセカンダリー HA ホストをオンラインに設定することができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。

4. オンラインに設定したいオフラインの HA ホストを選択します。
5. ツールバーで、「高可用性」 > 「システムをオンラインに設定」を選択します。

次のタスク

「システムおよびライセンス管理」ウィンドウで、HA ホストの状況を確認します。以下のいずれかの処理を実行してください。

- プライマリー HA ホストの状況が「アクティブ」と表示されている場合、このホストはリストアされています。
- 問題が発生した場合は、プライマリー HA ホストまたはセカンダリー HA ホストをリストアしてください。詳しくは、『障害が発生したセカンダリー *HA* ホストのリストア』または『障害が発生したプライマリー *HA* ホストのリストア』を参照してください。

関連概念:

2 ページの『フェイルオーバー後のデータ同期』
プライマリー高可用性 (HA) ホストによってフェイルオーバーの発生時点まで収集されたデータは、セカンダリー HA ホスト上で実質的にリアルタイムに維持されます。

プライマリー HA ホストをアクティブ・システムに切り替える

プライマリー高可用性 (HA) ホストをアクティブなシステムに設定することができます。

始める前に

プライマリー HA ホストがスタンバイ・システムになっていて、セカンダリー HA ホストがアクティブなシステムになっている必要があります。

このタスクについて

障害が発生したプライマリー・ホストをリカバリーすると、そのホストは HA クラスター内で自動的にスタンバイ・システムとして割り当てられます。プライマリー HA ホストをアクティブ・システムにするには、セカンダリー HA ホストを手動でオフラインに切り替える必要があります。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. 「システムおよびライセンス管理」ウィンドウで「プライマリー **HA** ホスト」を選択します。
5. ツールバーで、「高可用性」 > 「システムをオフラインに設定」を選択します。

   注**:** この間、IBM Security QRadar SIEM ユーザー・インターフェースにアクセスできなくなる可能性があります。

次のタスク

「システムおよびライセンス管理」ウィンドウにアクセスし、「状況」列を確認します。この列で、プライマリー HA ホストがアクティブなシステムになっていて、セカンダリー HA ホストがスタンバイ・システムになっていることを確認します。

関連概念:

5 ページの『プライマリー HA ホストでの障害』
セカンダリー高可用性 (HA) ホストがプライマリー HA ホストでの障害を検出すると、セカンダリー HA ホストが自動的にプライマリー HA ホストの処理をテークオーバーしてアクティブなシステムになります。

第 4 章 HA アプライアンスのリカバリー・オプション

IBM Security QRadar 高可用性 (HA) アプライアンスの再インストールまたはリカバリーを行うことができます。

HA クラスターで共有ストレージを使用している場合は、外部のストレージ・デバイスを手動で構成してください。詳しくは、「IBM Security QRadar オフボード・ストレージ・ガイド」を参照してください。

ノートブックのハイパーターミナル接続

IBM Security QRadar アプライアンスをリカバリーする際に、ノートブックを使用してインストールの進行状況をモニターすることができます。

HyperTerminal を使用して QRadar の再インストールやリカバリーをモニターする場合は、次の表にリストされている接続パラメーターから選択してください。

表 5. ハイパーターミナル接続パラメーター

パラメーター	説明
以下を使用して接続 (Connect Using)	シリアル・コネクターの適切な COM ポートを選択します。
ビット/秒	タイプ 9600
ストップ・ビット	タイプ 1
データ・ビット	タイプ 8
タイプ 8	タイプなし

関連タスク:

28 ページの『セカンダリー HA コンソールまたは非コンソールのリカバリー』
セカンダリー高可用性 (HA) IBM Security QRadar または非コンソール (管理対象ホスト) アプライアンスのインストールやリカバリーを実行することができます。

ネットワーク接続

IBM Security QRadar アプライアンスのリカバリーまたは再インストールを行う際に、ネットワーク接続設定を指定することができます。

QRadar アプライアンスのリカバリーや再インストールを行う場合は、以下の表を参照してください。

表 6. QRadar のネットワーク設定パラメーター

パラメーター	説明
ホスト名	システムのホスト名として、完全修飾ドメイン名を入力します。

表 6. *QRadar* のネットワーク設定パラメーター (続き)

パラメーター	説明
IP アドレス	システムの IP アドレスを入力します。 **注:** HA アプライアンスのリカバリーを行う場合は、ここで入力する IP アドレスがプライマリー HA ホストの IP アドレスになります。「システムおよびライセンス管理」ウィンドウで IP アドレスを確認することができます。
ネットワーク・マスク	システムのネットワーク・マスク・アドレスを入力します。
ゲートウェイ	**オプション:** サーバーのパブリック **IP** アドレスを入力します。パブリック **IP** アドレスは、 サーバーへのアクセスで使用されるセカンダリー IP アドレスです。通常は、異なるネットワークやインターネットからサーバーにアクセスします。このアクセスは、ネットワーク管理者によって管理されます。パブリック **IP** アドレスは、多くの場合、ネットワーク上のネットワーク・アドレス変換 (NAT) サービスまたはファイアウォール設定を使用して構成されます。
E メール・サーバー	E メール・サーバーを入力します。E メール・サーバーを使用しない場合は、このフィールドに `localhost` と入力します。

セカンダリー HA コンソールまたは非コンソールのリカバリー

セカンダリー高可用性 (HA) IBM Security QRadar または非コンソール (管理対象ホスト) アプライアンスのインストールやリカバリーを実行することができます。

始める前に

プライマリーまたはセカンダリーのコンソールや非コンソールの HA コンソールをリカバリーする場合、または QRadar ソフトウェアを再インストールする場合は、有効なアクティベーション・キーが必要になります。

アクティベーション・キーは 24 桁の英数字で、4 つの部分に分かれています。アクティベーション・キーは以下の場所にあります。

- ステッカーに印刷され、コンソールに物理的に添付されています。
- 納品書に記載されています。関連するキーとともに、すべてのコンソールがリストされています。

注: 文字の「I」と数字の「1」は同じ値として処理され、文字の「O」と数字の「0」も同じ値として処理されます。

プライマリー HA ホストのビルド・バージョンは、セカンダリー HA ホストにインストールされている QRadar のビルド・バージョンと一致している必要があります。

HA クラスターを構成する前に、セカンダリー HA ホストまたはプライマリー HA ホストにパッチを適用して、正しいビルド・バージョンにする必要があります。

手順

1. アプライアンスを準備します。
   a. 必要なすべてのハードウェアをインストールします。
   b. ノートブックをアプライアンスの背面のシリアル・ポートに接続するか、キーボードおよびモニターをそれぞれのポートに接続します。

      QRadar アプライアンスとアプライアンスのポートについては、「*IBM Security QRadar Hardware Guide*」を参照してください。
   c. システムの電源をオンにし、「ユーザー名」に `root` と入力してログインします。

      注**:** ユーザー名では大/小文字を区別します。
   d. Enter を押します。
   e. スペース・バーを押して各ウィンドウを進み、「yes」と入力してご使用条件に同意して**Enter** キーを押します。
   f. アクティベーション・キーを入力して、Enter キーを押します。
2. ウィザードの説明に従います。
3. QRadar のネットワーク設定を構成します。
4. 「次へ」を選択して、Enter キーを押します。

   注**:** `qchange_netsetup` を使用してネットワーク設定を変更する場合は、「終了」を選択して Enter キーを押します。ネットワーク設定の変更については、「*IBM Security QRadar SIEM* インストール・ガイド」または「*IBM Security QRadar Log Manager Installation Guide*」を参照してください。
5. 以下のように、QRadar の root パスワードを構成します。
   a. パスワードを入力し、「次へ」を選択して Enter キーを押します。
   b. 新しいパスワードをもう一度入力します。「終了」を選択して、Enter キーを押します。

      注**:** このプロセスには数分かかることがあります。
   c. Enter キーを押して、「OK」を選択します。
6. QRadar ユーザー・インターフェースにログインします。

次のタスク

HA クラスターを構成します。

関連概念:

27 ページの『ノートブックのハイパーターミナル接続』

IBM Security QRadar アプライアンスをリカバリーする際に、ノートブックを使用してインストールの進行状況をモニターすることができます。

関連タスク:

20 ページの『HA クラスターの作成』
IBM Security QRadar を使用して、プライマリー・ホスト、セカンダリー高可用性 (HA) ホスト、仮想 IP アドレスの組み合わせを作成すると、HA クラスターが作成されます。

障害が発生したプライマリー HA ホストのリカバリー

障害が発生したプライマリー高可用性 (HA) IBM Security QRadar ホストをリカバリーできます。

始める前に

障害が発生したプライマリー高可用性 (HA) ホスト上に QRadar を再インストールする場合、セカンダリー HA ホストのビルド・バージョンを考慮する必要があります。

プライマリーまたはセカンダリーのコンソールや非コンソールの HA コンソールをリカバリーする場合、または QRadar ソフトウェアを再インストールする場合は、有効なアクティベーション・キーが必要になります。

アクティベーション・キーは 24 桁の英数字で、4 つの部分に分かれています。アクティベーション・キーは以下の場所にあります。

- ステッカーに印刷され、コンソールに物理的に添付されています。
- 納品書に記載されています。関連するキーとともに、すべてのコンソールがリストされています。

注**:** 文字の「I」と数字の「1」は同じ値として処理され、文字の「O」と数字の「0」も同じ値として処理されます。

プライマリー HA ホストのビルド・バージョンは、セカンダリー HA ホストにインストールされている QRadar のビルド・バージョンと一致している必要があります。

HA クラスターを構成する前に、セカンダリー HA ホストまたはプライマリー HA ホストにパッチを適用して、正しいビルド・バージョンにする必要があります。

手順

1. 必要なすべてのハードウェアをインストールします。
2. 以下のいずれかのオプションを選択します。
   - ノートブックをアプライアンスの背面のシリアル・ポートに接続します。詳しくは、 27 ページの『ノートブックのハイパーターミナル接続』を参照してください。
   - キーボードとモニターをそれぞれのポートに接続します。
3. システムの電源をオンにし、「ユーザー名」に `root` と入力してログインします。
4. Enter を押します。

5. スペース・バーを押して各ウィンドウを進み、「yes」と入力してご使用条件に同意して Enter キーを押します。
6. アクティベーション・キーを入力して、Enter キーを押します。
7. 「**HA** リカバリーのセットアップ **(HA Recovery Setup)**」を選択し、「次へ」を選択して Enter キーを押します。
8. ウィザードの説明に従います。
9. QRadar のネットワーク設定を構成します。
10. 「次へ」を選択して、Enter キーを押します。
11. QRadar のルート・パスワードを構成します。
12. QRadar ユーザー・インターフェースにログインします。
13. 障害が発生したプライマリー HA ホストをリストアします。詳しくは、41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』を参照してください。

障害が発生したセカンダリー HA ホストを IBM Security QRadar SIEM 7.1 にリカバリーする

障害が発生したセカンダリー高可用性 (HA) ホストを IBM Security QRadar SIEM v7.1 にリカバリーすることができます。

このタスクについて

古いバージョンの QRadar を使用しているセカンダリー HA ホストで障害が発生し、このホストをリカバリーする場合は、更新されたリカバリー・パーティションから QRadar 7.1 をインストールすることができます。

インストーラーにより、ハード・ディスクの再パーティション化と再フォーマットが実行され、オペレーティング・システムがインストールされます。その後、QRadar が再インストールされます。フラット化プロセスが完了するまで待ってください。このプロセスには数分かかることがあります。

セカンダリー HA ホストのインストールについて詳しくは、「*IBM Security QRadar* インストール・ガイド」または「*IBM Security QRadar Log Manager Administration Guide*」を参照してください。

手順

1. SSH を使用して、セカンダリー HA ホストに root ユーザーとしてログインします。
   a. ユーザー名: `root`
   b. パスワード: **<パスワード>**
2. https://www.ibm.com/support で、QRadar ソフトウェアを入手します。
3. **`scp <iso ファイル名> root@<IP アドレス>:/root`** コマンドを入力して、QRadar 7.1 ISO をセカンダリー HA ホストにコピーします。

   重要: バージョン 7.0 以降の QRadar をインストールする場合は、ステップ 4 とステップ 5 を実行する必要はありません。リカバリー・スクリプトは、インストール時に `/opt/qradar/bin` に格納されます。

4. **mount -o loop <iso ファイル名> /media/cdrom/** コマンドを入力して、ISO をマウントします。
5. **cp /media/cdrom/post/recovery.py /root** コマンドを入力して、リカバリー・スクリプトをルート・ディレクトリーにコピーします。
6. **umount /media/cdrom/** コマンドを入力して、ISO をアンマウントします。
7. ホストが非コンソールの場合は、セキュア・コピー (SCP) が実行できるように、**IPTables** サービスを停止するために次のコマンドを入力します。

   service iptables stop
8. **./recovery.py -r --default --reboot <iso ファイル名>** コマンドを入力して、抽出されたリカバリー・スクリプトを開始します。
9. プロンプトが表示されたら、Enter キーを押してアプライアンスを再始動します。
10. プロンプトが表示されたら、flatten と入力して Enter キーを押します。
11. インストールが完了したら、SETUP と入力して root ユーザーとしてシステムにログインします。

障害が発生したセカンダリー HA ホストを IBM Security QRadar SIEM 7.1 (MR2) にリカバリーする

古いバージョンの IBM Security QRadar SIEM を使用している障害が発生したセカンダリー高可用性 (HA) ホストをリカバリーするときに、更新されたリカバリー・パーティションから QRadar 7.1 をインストールできます。

手順

1. SSH を使用して、セカンダリー HA ホストに root ユーザーとしてログインします。
   a. ユーザー名:root
   b. パスワード: <パスワード>
2. https://www.ibm.com/support で、QRadar ソフトウェアを入手します。
3. **scp <iso ファイル名> root@<IP アドレス>:/root** コマンドを入力して、QRadar 7.1 ISO をセカンダリー HA ホストにコピーします。
4. ホストが非コンソールの場合は、セキュア・コピー (SCP) が実行できるように、**IPTables** サービスを停止するために次のコマンドを入力します。

   service iptables stop
5. **./recovery.py -r --default --reboot <iso ファイル名>** コマンドを入力して、抽出されたリカバリー・スクリプトを開始します。
6. プロンプトが表示されたら、Enter キーを押してアプライアンスを再始動します。
7. プロンプトが表示されたら、flatten と入力して Enter キーを押します。

タスクの結果

インストーラーにより、ハード・ディスクの再パーティション化と再フォーマットが実行され、オペレーティング・システムがインストールされます。その後、

QRadar SIEM が再インストールされます。フラット化プロセスが完了するまで待ってください。このプロセスは、システムによっては数分かかることがあります。このプロセスが完了すると、通常のインストール・プロセスが実行されます。

障害が発生したプライマリー高可用性 (HA) QFlow アプライアンスのリカバリー

障害が発生したプライマリー高可用性 (HA) IBM Security QRadar QFlow コレクター をリカバリーすることができます。

手順

1. 必要なすべてのハードウェアをインストールします。
2. 以下のいずれかのオプションを選択します。
   - ノートブックをアプライアンスの背面のシリアル・ポートに接続します。詳しくは、 27 ページの『ノートブックのハイパーターミナル接続』を参照してください。
   - キーボードとモニターをそれぞれのポートに接続します。
3. システムの電源をオンにし、「ユーザー名」に `root` と入力してログインします。
4. Enter を押します。
5. スペース・バーを押して各ウィンドウを進み、「`yes`」と入力してご使用条件に同意して Enter キーを押します。
6. アクティベーション・キーを入力して、Enter キーを押します。
7. 「**HA** リカバリーのセットアップ **(HA Recovery Setup)**」を選択します。「次へ」を選択して、Enter キーを押します。
8. タイム・ゾーンの大陸または領域を選択します。「次へ」を選択して、Enter キーを押します。
9. タイム・ゾーンの地域を選択します。「次へ」を選択して、Enter キーを押します。
10. 「**IPv4**」を選択します。「次へ」を選択して、Enter キーを押します。

    注**:** 物理リンクのある各インターフェースはプラス (+) 記号付きで表示されます。
11. 管理インターフェースを選択します。「次へ」を選択して、Enter キーを押します。
12. 「クラスター仮想 **IP** アドレス」を入力し、「次へ」を選択して Enter キーを押します。詳しくは、 20 ページの『HA クラスターの IP アドレスの表示』を参照してください。
13. QRadar のネットワーク設定を構成します。.
14. 「次へ」を選択して、Enter キーを押します。
15. QRadar のルート・パスワードを構成します。
16. QRadar ユーザー・インターフェースにログインします。

17. 障害が発生したプライマリー HA ホストをリストアします。障害が発生したプライマリー HA ホストのリストア方法については、 41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』を参照してください。

セカンダリー高可用性 (HA) コンソールまたは非コンソール・システム上での QRadar のリカバリー

セカンダリー高可用性 (HA) システム上で、QRadar コンソール または非コンソール (管理対象ホスト) ソフトウェアのインストールやリカバリーを実行することができます。

始める前に

以下の手順は、QRadar コンソール と非コンソールのインストールまたはリカバリーを行う場合の手順です。インストールやリカバリーを行うアプライアンスに応じて、異なるオプションを選択する必要があります。

QRadar のアクティベーション・キーを持っていることを確認してください。詳しくは、『QRadar のアクティベーション・キー』を参照してください。

手順

1. 必要なハードウェアをインストールします。
2. Red Hat Enterprise Linux オペレーティング・システムを入手してハードウェアにインストールします。

   注**:** Red Hat Enterprise Linux オペレーティング・システムのインストール方法と構成方法については、「*IBM Security QRadar* インストール・ガイド」を参照してください。
3. root としてログインします。
4. コマンド `mkdir /media/cdrom` を入力して、`/media/cdrom` ディレクトリーを作成します。
5. https://www.ibm.com/support で、QRadar ソフトウェアを入手します。
6. コマンド `mount -o loop <QRadar ISO のパス> /media/cdrom` を入力して、QRadar ISO をマウントします。
7. コマンド `./media/cdrom/setup` を入力して、インストールを開始します。
8. スペース・バーを押して各ウィンドウを進み、「**yes**」と入力してご使用条件に同意して Enter キーを押します。
9. アクティベーション・キーを入力して、Enter キーを押します。
10. ウィザードの説明に従います。
11. QRadar のネットワーク設定を構成します。
12. 「次へ」を選択して、Enter キーを押します。

    注**:** **`qchange_netsetup`** を使用してネットワーク設定を変更する場合は、「終了」を選択して Enter キーを押します。詳しくは、「*IBM Security QRadar* インストール・ガイド」を参照してください。
13. QRadar のルート・パスワードを構成します。
14. QRadar ユーザー・インターフェースにログインします。

次のタスク

HA クラスターを構成します。

障害が発生したプライマリー HA コンソールまたは非コンソール上での IBM Security QRadar のリカバリー

障害が発生したプライマリー HA ホスト上の IBM Security QRadar コンソールまたは非コンソール (管理対象ホスト) ソフトウェアをリカバリーすることができます。

始める前に

以下の手順は、プライマリー・コンソールと非コンソール上で QRadar のインストールまたはリカバリーを行う場合の手順です。インストールやリカバリーを行うアプライアンスに応じて、異なるオプションを選択する必要があります。

QRadar のアクティベーション・キーを持っていることを確認してください。詳しくは、『QRadar のアクティベーション・キー』を参照してください。

手順

1. 必要なハードウェアをインストールします。
2. Red Hat Enterprise Linux オペレーティング・システムを入手してハードウェアにインストールします。

   注**:** Red Hat Enterprise Linux オペレーティング・システムのインストール方法と構成方法については、「*IBM Security QRadar* インストール・ガイド」を参照してください。
3. root としてログインします。
4. コマンド `mkdir /media/cdrom` を入力して、`/media/cdrom` ディレクトリーを作成します。
5. https://www.ibm.com/support で、QRadar ソフトウェアを入手します。
6. コマンド `mount -o loop <QRadar ISO のパス> /media/cdrom` を入力して、QRadar ISO をマウントします。
7. コマンド `./media/cdrom/setup` を入力して、インストールを開始します。

   注**:** QRadar は MD5 sum を確認することにより、インストールの前にメディアの整合性を検証します。MD5 チェックサムが失敗したことを示す警告メッセージが表示された場合は、QRadar をもう一度ダウンロードしてください。さらに支援が必要な場合は、お客様サポートに連絡してください。
8. スペース・バーを押して各ウィンドウを進み、「`yes`」と入力してご使用条件に同意して Enter キーを押します。
9. アクティベーション・キーを入力して、Enter キーを押します。
10. ウィザードの説明に従います。
11. QRadar のネットワーク設定を構成します。
12. 「次へ」を選択して、Enter キーを押します。
13. QRadar のルート・パスワードを構成します。

14. QRadar にログインします。

次のタスク

障害が発生したプライマリー HA ホストをリストアします。 41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』を参照してください。

関連タスク:

20 ページの『HA クラスターの作成』
IBM Security QRadar を使用して、プライマリー・ホスト、セカンダリー高可用性 (HA) ホスト、仮想 IP アドレスの組み合わせを作成すると、HA クラスターが作成されます。

セカンダリー HA ホストを以前のバージョンまたは出荷時のデフォルト値に戻す

IBM Security QRadar のセカンダリー高可用性 (HA) ホストを前のバージョンにリカバリーしたり、出荷時のデフォルト値に戻したりできます。

このタスクについて

リカバリー・パーティションや USB ポートがない、障害が発生した QRadar のセカンダリー HA ホストを前のバージョンにリカバリーできます。また、システムを出荷時のデフォルト値に戻すこともできます。障害が発生したセカンダリー HA ホストをリカバリーすると、ホスト上のすべてのデータが削除され、出荷時のデフォルト値に戻ります。

手順

1. SSH を使用して、root ユーザーとしてコンソールにログインします。
2. IBM SmartCloud Provisioning を使用して、コンソールの `recovery.py` スクリプトを、障害が発生したセカンダリー HA ホストにコピーします。

   注: 場所を指定しなかった場合、`recovery.py` スクリプトはデフォルトで `/root` ディレクトリーにダウンロードされます。
3. https://www.ibm.com./support で、QRadar ISO を入手します。
4. セキュア・コピー (SCP) を使用して、ISO ファイルを QRadar ターゲット・ホストにコピーします。

   `scp <iso_file_name> root@<TargetIP_address>:/root`
5. SSH を使用してセカンダリー HA ホストにログインします。
6. 以下のコマンドを入力します。

   ```
   chmod 755 recovery.py
   ./recovery.py -r --default --reboot <iso_file_name>
   ```
7. システムを再始動するためのプロンプトが表示されたら Enter キーを押します。
8. プロンプトが表示されたら、`flatten` と入力して Enter キーを押します。

タスクの結果

インストーラーにより、ハード・ディスクの再パーティション化と再フォーマットが実行され、オペレーティング・システムがインストールされます。その後、QRadar がインストールされます。 **フラット化**プロセスが完了するまで待ってください。このプロセスの完了までに数分かかることがあります。このプロセスが完了すると、通常のインストール・プロセスが続行されます。

第 5 章 QRadar HA のデプロイメントに関する問題のトラブルシューティング

トラブルシューティングを行う場合は、「システムおよびライセンス管理」ウィンドウで HA ホストの状況を参照すると便利です。

状況の組み合わせと考えられる解決策

以下の表は、プライマリー HA ホストとセカンダリー HA ホストで考えられる状況の組み合わせを示したものです。それぞれの組み合わせについて、異なるトラブルシューティングのアプローチが必要になります。

表 7. 「システムおよびライセンス管理」ウィンドウに表示されるホストの状況：

プライマリー **HA** ホストの状況	セカンダリー **HA** ホストの状況	可能な処置
アクティブ	「失敗」または「不明」	セカンダリー・ホストがオンになっているかどうか、SSH を使用して root ユーザーとしてセカンダリー・ホストにログオンできるかどうかを確認してください。接続できる場合は、 40 ページの『障害が発生したセカンダリー HA ホストのリストア』を参照してください。
「失敗」または「不明」	アクティブ	プライマリー・ホストがオンになっているかどうか、SSH を使用して root ユーザーとしてプライマリー・ホストにログオンできるかどうかを確認してください。接続できる場合は、 41 ページの『障害が発生したプライマリー HA ホストのリストア』を参照してください。
不明	不明	SSH を使用してプライマリー HA ホストとセカンダリー HA ホストのいずれにも接続できない場合は、ネットワークとハードウェアの構成が作動可能な状態になっているかどうかを確認してください。
オフライン	アクティブ	プライマリー・ホストをオンラインに設定します。その方法については、『プライマリー HA ホストをオンラインに設定する』を参照してください。

アクティブなホストを特定する

SSH を使用して、HA クラスター内で直前までアクティブだったホストを特定することができます。

1. HA クラスター構成を表示するには、次のコマンドを入力します。

   ```
   cat /proc/drbd
   ```

2. 出力結果で以下の行を確認します。

   ```
   0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate
   ```

   - この行に cs:Connected というテキストが表示されていない場合は、HA クラスター内で直前までアクティブだった HA ホストを判別します。
   - 出力に Secondary/Primary というテキストが表示されている場合は、セカンダリー HA ホストがアクティブなシステムになっています。
   - 出力に ro:Primary/Secondary というテキストが表示されている場合は、プライマリー HA ホストがアクティブなシステムになっています。

3. 上記の行に ro:Secondary/Secondary というテキストが表示されている場合は、出力結果の以下の行を確認します。

   ```
   0: cs:Connected ro:Secondary/Secondary
   ```

   - 出力に ds:< >/UpToDate というテキストが表示されている場合、セカンダリー HA ホストがアクティブなシステムになっています。
   - 出力に ds:UpToDate/< > というテキストが表示されている場合、プライマリー HA ホストがアクティブなシステムになっています。
   - 出力に ds:< >/< > というテキストが表示されている場合、HA クラスター内で直前までアクティブだった HA ホストを判別します。
   - 出力に ds:UpToDate/UpToDate というテキストが表示されている場合、HA クラスター内で直前までアクティブだった HA ホストを判別します。

障害が発生したセカンダリー HA ホストのリストア

障害が発生したセカンダリー HA ホストをリストアすることができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」をクリックします。
4. リストアするセカンダリー HA ホストを選択します。
5. 「高可用性」メニューで、「システムのリストア」をクリックします。
6. 「システムおよびライセンス管理」ウィンドウで、セカンダリー HA ホストの状況が「失敗」または「不明」と表示されている場合は、SSH を使用して root ユーザーとしてセカンダリー HA ホストにログインし、ホストが作動可能な状態になっているかどうかを確認します。
7. reboot と入力してセカンダリー HA ホストを再始動します。
8. システムの再始動後も、セカンダリー HA ホストの状況が「失敗」または「不明」と表示される場合は、「高可用性」メニューで「システムのリストア」をクリックします。

関連タスク:

41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』

プライマリー HA ホストとセカンダリー HA ホストが作動可能な状態になってい

るかどうかを確認する必要があります。

障害が発生したプライマリー HA ホストのリストア

障害が発生したプライマリー HA ホストをリストアすることができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」をクリックします。
4. リストアするプライマリー HA ホストを選択します。
5. 「高可用性」メニューで、「システムのリストア」をクリックします。
6. プライマリー HA ホストの状況を確認します。
7. 「システムおよびライセンス管理」ウィンドウで、プライマリー HA ホストの状況が「オフライン」と表示されている場合は、「高可用性」 > 「システムをオンラインに設定」をクリックします。
8. 「システムおよびライセンス管理」ウィンドウで、プライマリー HA ホストの状況が「失敗」または「不明」と表示されている場合は、SSH を使用して root ユーザーとしてプライマリー HA ホストにログインし、ホストが作動可能な状態になっているかどうかを確認します。
9. **reboot** コマンドを入力して、プライマリー HA ホストを再始動します。

関連タスク:

42 ページの『プライマリー HA ホストの状況をオンラインに設定する』
プライマリー HA ホストの状況が「オフライン」と表示されている場合、この状況を「オンライン」にリセットすることができます。

プライマリー・ホストとセカンダリー・ホストの状況の確認

プライマリー HA ホストとセカンダリー HA ホストが作動可能な状態になっているかどうかを確認する必要があります。

手順

1. プライマリー HA ホストがコンソールとして構成されているか、または管理対象ホストとして構成されているかを確認します。
2. プライマリー HA ホストがコンソールとして構成されている場合は、SSH を使用して、root ユーザーとしてクラスター仮想 IP アドレスにログインします。
   - クラスター仮想 IP アドレスに接続できる場合は、QRadar へのアクセスをリストアしてください。詳しくは、「*IBM SecurityQRadar SIEM Troubleshooting Guide*」を参照してください。
   - クラスター仮想 IP アドレスに接続できない場合は、SSH を使用して root ユーザーとしてセカンダリー HA ホストにログインし、セカンダリー HA ホストが作動可能な状態になっていることを確認してください。
3. セカンダリー・ホストが管理対象ホストとして構成されている場合は、SSH を使用して、root ユーザーとしてセカンダリー HA ホストにログインします。

- SSH を使用してプライマリー HA ホストとセカンダリー HA ホストのいずれにも接続できない場合は、ネットワークとハードウェアの構成が作動可能な状態になっているかどうかを確認してください。
- プライマリー HA ホストとセカンダリー HA ホストに接続できる場合は、HA クラスター内で直前までアクティブだった HA ホストを特定してください。

関連概念:

17 ページの『HA ホストの状況』
高可用性 (HA) クラスター内のプライマリー・ホストとセカンダリー・ホストの状況を確認できます。

関連タスク:

41 ページの『プライマリー・ホストとセカンダリー・ホストの状況の確認』
プライマリー HA ホストとセカンダリー HA ホストが作動可能な状態になっているかどうかを確認する必要があります。

プライマリー HA ホストの状況をオンラインに設定する

プライマリー HA ホストの状況が「オフライン」と表示されている場合、この状況を「オンライン」にリセットすることができます。

手順

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、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」をクリックします。
4. リストアするプライマリー HA ホストを選択します。
5. 「システムおよびライセンス管理」ウィンドウで、プライマリー HA ホストの状況が「オフライン」と表示されている場合は、プライマリー HA ホストをリストアする必要があります。

関連タスク:

41 ページの『障害が発生したプライマリー HA ホストのリストア』
障害が発生したプライマリー HA ホストをリストアすることができます。

第 6 章 QRadar デプロイメントにおける災害復旧

データを別の同じ QRadar システムにミラーリングすることで、災害復旧 (DR) を実装し、IBM Security QRadar 構成およびデータを保護します。災害復旧は、相互にミラーリングする 2 つの同じ QRadar システムが、地理的に離れた環境に設置されていて、両方のサイトでデータが収集される場合に可能です。

実データを転送する際 (例えば、プライマリー QRadar システムのフローおよびイベントを別のサイトの並行システムに転送する場合など) に、災害復旧 (DR) を有効にします。データの転送には、オフサイト転送 を使用します。これは、プライマリーとセカンダリーの両方のデプロイメント環境でセットアップされます。災害復旧は、地理的に異なる場所にあるデプロイメント環境でセットアップできます。

以下のいずれかの災害復旧デプロイメント・シナリオを選択してください。

プライマリー **QRadar** コンソールおよびバックアップ・コンソール
: バックアップ・コンソールがプライマリー・サーバーのコピーであり、両方の構成は同じだが、バックアップ・コンソールの電源はオフのままになっているハードウェア障害ソリューション。操作可能なコンソールは常に 1 つのみです。プライマリー・コンソールに障害が発生した場合、バックアップ・コンソールの電源を手動でオンにして、プライマリー構成バックアップを適用し、プライマリー・コンソールの IP アドレスを使用します。プライマリー・サーバーをリストアした後、それをオンにする前に、バックアップ・サーバーを手動でオフにします。長期間システムが停止している場合は、バックアップ・コンソールの構成バックアップをプライマリー・サーバーに適用します。

イベントおよびフローの転送
: イベントおよびフローがプライマリー・サイトからセカンダリー・サイトに転送されます。2 つの別個のデータ・センターのアーキテクチャーが同一である必要があります。

プライマリー・サイトおよびセカンダリー・サイトへの同じイベントおよびフローの配布
: ロード・バランサーなどの手法を使用して、ミラーリングされたアプライアンスに同じデータを送信することにより、同じイベント・データとフロー・データを 2 つのライブ・サイトに配布します。各サイトは、送信されるログ・データのレコードを保持します。

プライマリー QRadar コンソールおよびバックアップ QRadar コンソール

プライマリー QRadar コンソールに障害が発生した場合に、バックアップ QRadar コンソールでプライマリー・コンソールの役割を引き継ぐようにしたい場合、バックアップ・コンソールの電源を手動でオンにして、構成バックアップおよびプライマリー・コンソールの IP アドレスを適用します。QRadar QFlow コレクターやイベント・コレクター (Event Collector)など、その他のアプライアンスについて同様の切り替え方式を使用します。この場合、各アプライアンスはコールド・バックアップ、または同一アプライアンスであるスペアを備えています。

バックアップ・コンソールは、アクティブ化された時点以降、プライマリー QRadar コンソールの役割を引き継ぎ、元のプライマリー QRadar コンソールからの過去のイベント、フロー、あるいはオフェンスは保管しません。ハードウェア障害が発生した場合、ダウン時間を最小化するために、ご使用のアプライアンスでこのタイプのデプロイメントを使用します。

プライマリー・コンソールで障害が発生した場合、以下の手順を実行して、バックアップ・コンソールをプライマリー QRadar コンソールとしてセットアップします。

1. バックアップ・コンソールの電源をオンにします。
2. プライマリー・コンソールの IP アドレスを追加します。
3. プライマリー・コンソールからバックアップ・コンソールに構成バックアップ・データをリストアします。

バックアップ・コンソールは、プライマリー・コンソールがオンラインに戻るまで、プライマリー・コンソールとして機能します。両方のサーバーが同時にオンラインにならないようにしてください。

バックアップ・コンソールでの IP アドレスの構成

プライマリー QRadar コンソールに障害が発生した場合に、プライマリー・コンソールの役割を引き受けるようにセカンダリー・バックアップ・コンソールを構成します。障害が発生した QRadar コンソールの IP アドレスをバックアップ・コンソールに追加して、QRadar システムが継続して機能するようにします。

始める前に

バックアップ・コンソールの電源をオンにします。

手順

1. SSH を使用して、root ユーザーとしてログインします。
2. バックアップ・コンソールで IP アドレスを構成するには、以下の手順を実行します。
   a. 次のコマンドを入力します。

      ```
      qchange_netsetup
      ```

   b. ウィザードの指示に従って、構成パラメーターを入力します。

      要求した変更が処理されると、QRadar システムは自動的にシャットダウンして再始動します。

バックアップおよびリカバリー

システム障害やデータ損失からリカバリーできるように、IBM Security QRadar の構成情報およびデータをバックアップします。

データをバックアップするには、QRadar に組み込まれているバックアップおよびリカバリーを使用します。ただし、データを手動でリストアする必要があります。

デフォルトでは、QRadar は真夜中に構成情報の日次バックアップ・アーカイブを作成します。バックアップ・アーカイブには、その前日の構成情報または生成データ、あるいはその両方が含まれます。

以下のタイプのバックアップを作成できます。

- 構成バックアップ。このバックアップには、例えば、QRadar デプロイメント内のアセットおよびログ・ソースなど、システム構成データが含まれています。
- データ・バックアップ。このバックアップには、例えば、ログ情報やイベント日付など、処理を実行中の QRadar デプロイメントによって生成される情報が含まれています。

データのバックアップおよびリカバリーについて詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

プライマリー・データ・センターから別のデータ・センターへのイベントおよびフローの転送

イベント、フロー、およびオフェンス用の冗長データ・ストアが用意され、2 つの別個のデータ・センターに同一のアーキテクチャーが存在するようにするために、イベント・データおよびフロー・データをサイト 1 からサイト 2 に転送します。

このシナリオは、サイト 1 がアクティブのままになっているかどうかに依存します。サイト 1 で障害が発生すると、データはサイト 2 に送信されませんが、障害発生時点までデータは現行データです。サイト 1 で障害が発生した場合、IP アドレスを手動で変更して災害復旧 (DR) を実装し、バックアップとリストアを使用してサイト 1 からサイト 2 にフェイルオーバーし、すべての QRadar ホストについてサイト 2 に切り替えます。

以下のリストで、プライマリー・サイトからセカンダリー・サイトにイベントおよびフローを転送するためのセットアップ方法について説明します。

- プライマリー・データ・センターとセカンダリー・データ・センターからなる 2 つの別個のデータ・センターに、分散された同一のアーキテクチャーが存在する。
- プライマリー QRadar コンソールがアクティブであり、ログ・ソースからすべてのイベントおよびフローを収集し、相関するオフェンスを生成している。
- プライマリー・データ・センターのイベント・データおよびフロー・データをもう 1 つのデータ・センターのイベント・プロセッサーおよびフロー・プロセッサーに転送できるように、プライマリー QRadar コンソールにオフサイト・ターゲットを構成する。

  ファースト・パス: セットアップが簡単なため、オフサイト・ターゲットではなく、ルーティング・ルールを使用します。
- コンテンツ・マネジメント・ツールを定期的に使用して、プライマリー QRadar コンソールからセカンダリー QRadar コンソールへの転送内容を更新する。

転送宛先およびルーティング・ルールの詳細については、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

サイト 1 で障害が発生した場合、高可用性 (HA) デプロイメントを使用して、サイト 2 への自動フェイルオーバーをトリガーできます。サイト 2 のセカンダリー HA ホストは、サイト 1 のプライマリー HA ホストの役割を引き継ぎます。サイト 2 では、イベント・データとフロー・データを引き続き収集、保管、および処理します。スタンバイ状態のセカンダリー HA ホストには実行中のサービスはありませんが、ディスクの複製が有効になっている場合は、データが同期化されます。HA デプロイメントの計画について詳しくは、 9 ページの『第 2 章 HA デプロイメントの計画』を参照してください。

注: ロード・バランサーを使用することにより、イベントの分割、および NetFlow、 J-Flow、sFlow などのフローの分割を行うことができます。しかし、ロード・バランサーを使用して QFlows を分割することはできません。QFlow を分割し、バックアップ・サイトに送信するには、再生タップなどの外部テクノロジーを使用してください。

以下の図は、サイト 1 の冗長データ・ストアとしてサイト 2 を使用する方法を示しています。イベント・データとフロー・データがサイト 1 からサイト 2 に転送されます。

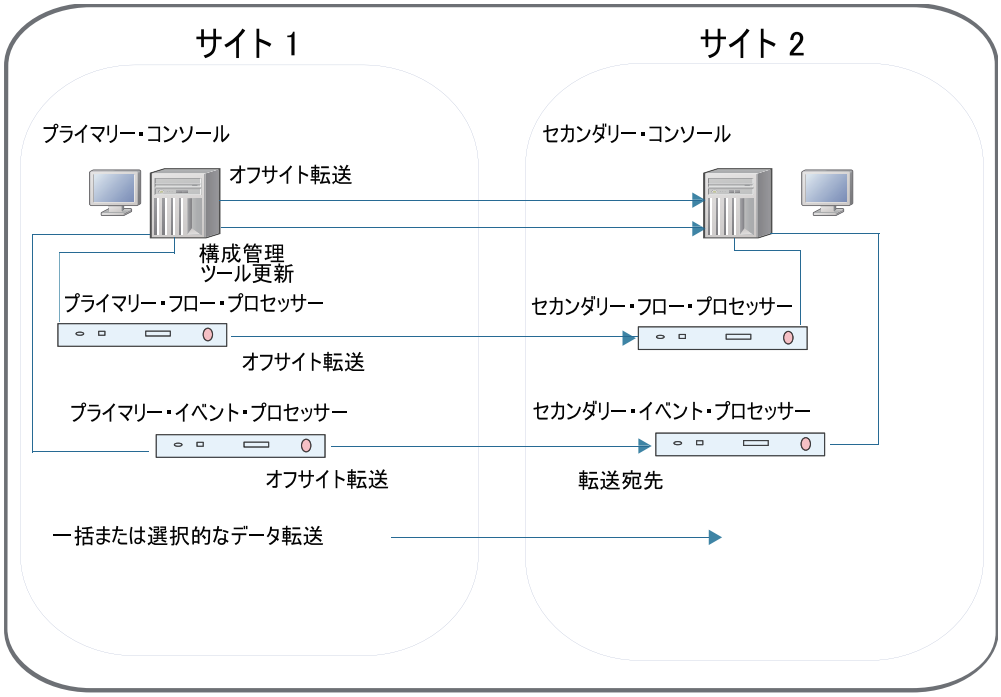

図 *1.* 災害復旧のためのサイト *1* からサイト *2* へのイベントおよびフローの転送

イベントおよびフローの転送構成

データの冗長性を実現するために、あるサイトからバックアップ・サイトにデータを転送するように IBM Security QRadar システムを構成します。

QRadar からデータを受け取るターゲット・システムを、「転送宛先」と呼びます。QRadar システムにより、データはすべて、変更されずに転送されます。新し

いバージョンの QRadar システムは、それより前のバージョンの QRadar システムからのデータを受信することができます。ただし、前のバージョンがそれより新しいバージョンからのデータを受信することはできません。互換性の問題を回避するために、データを送信する QRadar システムをアップグレードする前にすべての受信側をアップグレードしてください。転送をセットアップするには、以下の手順を実行します。

1. 1 つ以上の転送宛先を構成します。

   転送宛先とは、IBM Security QRadar プライマリー・コンソールからイベント・データとフロー・データを受け取るターゲット・システムのことです。一括または選択的なデータ転送を構成するには、転送宛先を追加する必要があります。転送宛先の詳細については、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。
2. ルーティング・ルールまたはカスタム・ルール、あるいはその両方を構成します。

   イベント・データとフロー・データ用の 1 つ以上の転送宛先を追加したら、フィルター・ベースのルーティング・ルールを作成することで、大容量のデータを転送できます。ルーティング・ルールについて詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。
3. データのエクスポート、インポート、および更新を構成します。

   コンテンツ・マネジメント・ツールを使用して、プライマリー QRadar コンソールからセカンダリー QRadar コンソールにデータを移動します。セキュリティーおよび構成の内容を IBM Security QRadar から外部のポータブルな形式にエクスポートします。コンテンツ・マネジメント・ツールを使用してデータを転送する方法について詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

2 つのサイト間でのイベントおよびフローのロード・バランシング

2 つのライブ IBM Security QRadar デプロイメントをプライマリー・サイトとセカンダリー・サイトの両方で稼働している場合、イベント・データおよびフロー・データを両方のサイトに送信します。各サイトは、送信されるログ・データのレコードを保持します。コンテンツ・マネジメント・ツールを使用して、デプロイメント間でデータの同期状態を維持します。

以下の図は、2 つのライブ・サイトを示しており、各サイトのデータがもう一方のサイトに複製されています。

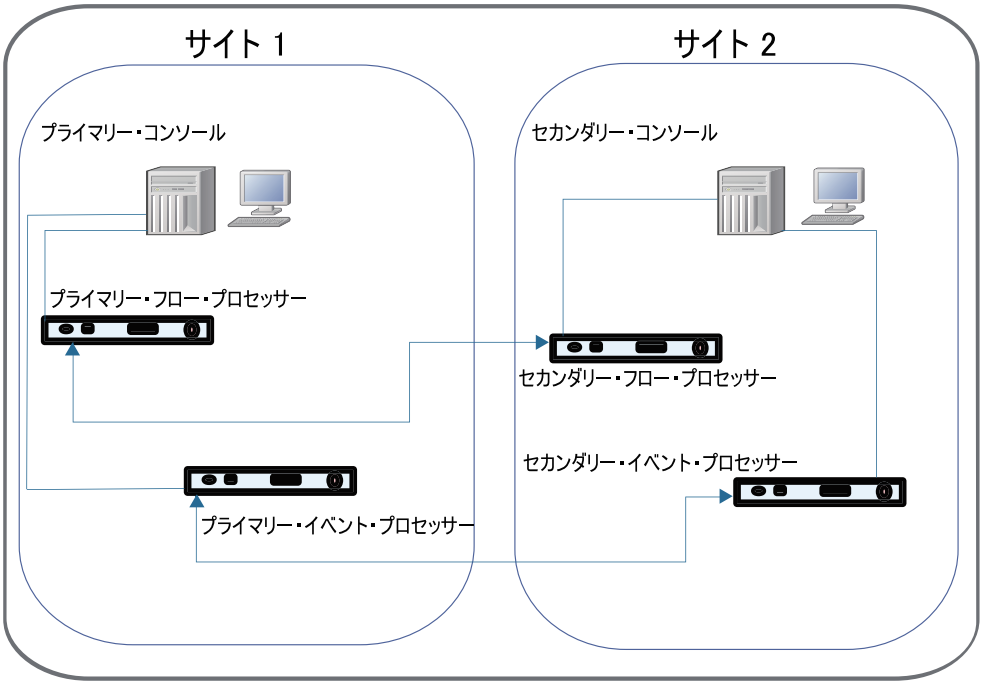

図 2. 2 つのサイト間でのイベントおよびフローのロード・バランシング

関連概念:

49 ページの『イベント・データとフロー・データの冗長性』
ロード・バランサーなどの手法を使用して、ミラーリングされたアプライアンスに同じデータを送信することにより、同じイベントおよびフローを別のデータ・センターまたは地理的に離れたサイトに送信し、データの冗長性を可能にします。

プライマリー QRadar コンソールからセカンダリー QRadar コンソールへの構成データのリストア

セカンダリー QRadar コンソールをログの宛先としてセットアップしたら、プライマリー QRadar コンソールからバックアップ・アーカイブを追加またはインポートします。別の QRadar ホストで作成されたバックアップ・アーカイブをリストアすることができます。セカンダリー QRadar コンソールにログインし、このセカンダリー QRadar コンソールに対してプライマリー・コンソール・バックアップ・アーカイブの完全リストアを実行します。

始める前に

このタスクを実行するには、プライマリー・コンソールからのデータ・バックアップが必要になります。

手順

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、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー」アイコンをクリックします。
4. 「アーカイブのアップロード」フィールドで、「参照」をクリックします。

5. アップロードするアーカイブ・ファイルを見つけて選択します。

   ヒント: QRadar バックアップ・アーカイブ・ファイルがコンソール・サーバーの `/store/backupHost/inbound` ディレクトリーにある場合、バックアップ・アーカイブ・ファイルは自動的にインポートされます。

   アーカイブ・ファイル名には `.tgz` 拡張子が付いている必要があります。
6. 「開く」をクリックします。
7. 「アップロード」をクリックします。
8. アップロードしたアーカイブを選択し、「リストア」をクリックします。

   リストアが完了すると、セカンダリー QRadar コンソールがプライマリー・コンソールになります。

イベント・データとフロー・データの冗長性

ロード・バランサーなどの手法を使用して、ミラーリングされたアプライアンスに同じデータを送信することにより、同じイベントおよびフローを別のデータ・センターまたは地理的に離れたサイトに送信し、データの冗長性を可能にします。

データの冗長性を実現するために、ログ・ソースおよびフロー・ソースの配布を以下のとおり構成します。

- セカンダリー・サイトのイベント・プロセッサー (Event Processor)にログ・ソース・データを送信する。
- セカンダリー・サイトのフロー・プロセッサーにフロー・ソース・データを送信する。

  ログ・ソースの構成について詳しくは、「*IBM Security QRadar Log Sources Configuration Guide*」を参照してください。

  フロー・ソースの詳細については、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

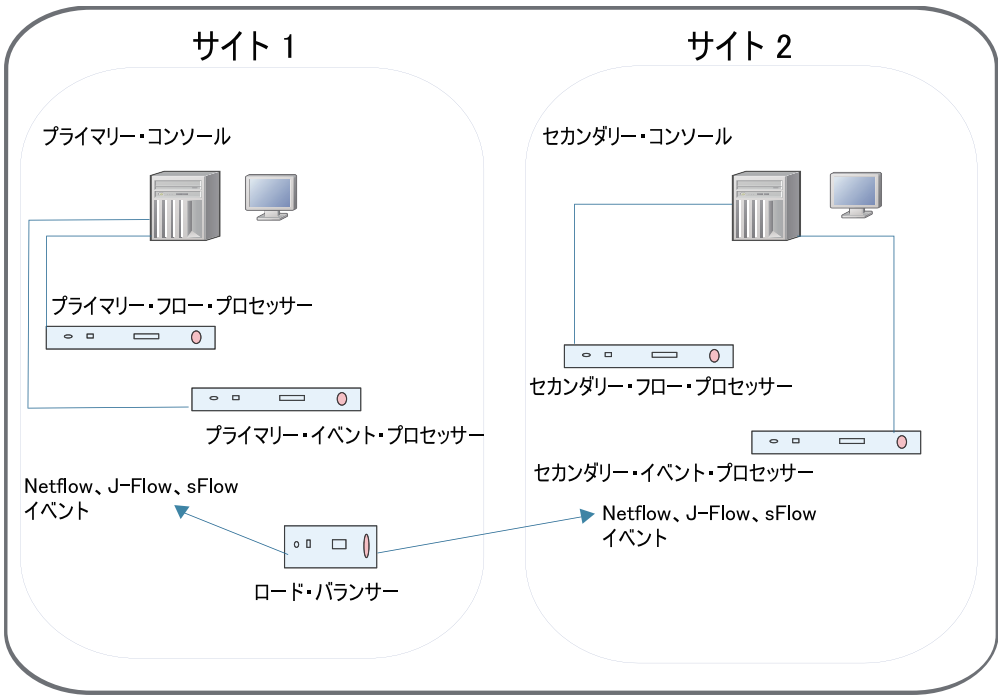

図 3. 2 つのサイトへのイベントおよびフローの送信

イベントを受信するように **QRadar** を構成する

QRadar は、デプロイメント内で Syslog メッセージを送信する多数のログ・ソースを自動的に検出します。QRadar で自動的に検出されたログ・ソースは、「ログ・ソース」ウィンドウに表示されます。

イベント・コレクター (Event Collector)構成の**「自動検出が有効」**設定を使用して、イベント・コレクター (Event Collector)ごとにログ・ソースの自動ディスカバリーを構成します。ログ・ソースのイベント ID をプライマリー・イベント・コレクター (Event Collector)と同期したままにする場合は、**「自動検出 (Autodetection)」**設定を無効にします。この状態の場合、コンテンツ・マネジメント・ツールを使用して、ログ・ソース構成を同期化するか、構成バックアップをサイトにリストアします。

自動ディスカバー済みログ・ソース、およびご使用のデバイスまたはアプライアンスに固有の構成について詳しくは、「*IBM Security QRadar DSM Configuration Guide*」および「*IBM Security QRadar Log Sources Configuration Guide*」を参照してください。

フローを受信するように **QRadar** を構成する

フローのデータ冗長性を可能にするには、NetFlow、J-Flow、および sFlow を QFlow 収集のために両方のサイトに送信する必要があります。

SPAN またはタップからフローを収集し、バックアップの場所にパケットを送信するか、外部テクノロジーを使用して、SPAN またはタップをバックアップの場所でミラーリングすることができます。ロード・バランサーは、NetFlow、J-Flow、および sFlow などのフローを分割しますが、QFlow は分割できません。

フロー・ソースの詳細については、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

コンテンツ・マネジメント・ツール **(CMT)** を使用する

サイト 1 のプライマリー QRadar コンソールとサイト 2 のセカンダリー QRadar コンソールの構成が同一になるようにしたい場合は、コンテンツ・マネジメント・ツールを使用して、サイト 1 の構成でサイト 2 を更新します。

コンテンツ・マネジメント・ツールの使用について詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

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、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

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。

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。

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