

IBM QRadar Security Intelligence

バージョン 7.2.6

オフボード・ストレージ・ガイド

IBM

注記

本書および本書で紹介する製品をご使用になる前に、39 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。

原典： IBM QRadar Security Intelligence
Version 7.2.6
Offboard Storage 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

© Copyright IBM Corporation 2012, 2015.

目次

QRadar 製品でのオフボード・ストレージ・デバイスの概要	v
第 1 章 オフボード・ストレージの概要	1
オフボード・ストレージのファイル・システム・オプション	2
オフボード・ストレージ・ソリューションのパフォーマンスへの影響	2
ストレージ拡張	3
外部ストレージ・オプション	3
外部ストレージの制限	4
HA 環境でのオフボード・ストレージ	5
第 2 章 iSCSI 外部ストレージ・デバイス	7
HA 環境での iSCSI 構成オプション	7
セカンダリー・ネットワーク・インターフェース	7
標準的な QRadar デプロイメント環境での iSCSI 構成	8
iSCSI ボリュームの構成	9
iSCSI ストレージ・ソリューションへの /store/ariel ファイル・システムの移動	11
iSCSI ストレージ・ソリューションへの /store ファイル・システムの移動	12
iSCSI ボリュームの自動マウント	14
HA デプロイメント環境での iSCSI の構成	15
HA デプロイメント環境でのセカンダリー・インターフェースの制御の構成	17
iSCSI 接続の検証	18
iSCSI に関する問題のトラブルシューティング	19
第 3 章 ファイバー・チャネル・ストレージ	23
ファイバー・チャネル・ストレージの構成の概要	23
Emulex アダプターのインストールの検証	23
ファイバー・チャネル接続の検証	24
ファイバー・チャネル・ソリューションへの /store ファイル・システムの移動	26
ファイバー・チャネル・ソリューションへの /store/ariel ファイル・システムの移動	28
ファイバー・チャネル・マウント・ポイントの検証	29
標準的な QRadar デプロイメント環境でのファイバー・チャネルの構成	29
HA デプロイメント環境でのファイバー・チャネルの構成	31
セカンダリー HA ホストのマウント・ポイントの構成	32
第 4 章 NFS オフボード・ストレージ・デバイス	35
NFS へのバックアップの移動	35
新しいバックアップの場所の構成	37
セカンダリー HA ホストのマウント・ポイントの構成	37
特記事項	39
商標	40
プライバシー・ポリシーに関する考慮事項	41
索引	43

QRadar 製品でのオフボード・ストレージ・デバイスの概要

本書には、IBM® Security QRadar® 製品の /store ファイル・システムまたは /store/ariel ファイル・システムを外部ストレージ・デバイスに移動する方法に関する情報が記載されています。

対象読者

オフボード・ストレージ・デバイスの構成を担当するシステム管理者には、QRadar システムへの管理アクセス権限、およびネットワーク・デバイスとファイアウォールへの管理アクセス権限が必要です。システム管理者は、企業ネットワークとネットワークキング・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 (すべての翻訳資料を含む) を Web 上で探すには、IBM Knowledge Center (<http://www.ibm.com/support/knowledgecenter/SS42VS/welcome>) にアクセスしてください。

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。ライセンサーは、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 オフボード・ストレージの概要

アプライアンスのストレージ容量を増やすために、データの一部をオフボード・ストレージ・デバイスに移動できます。/store、/store/ariel、または /store/backup の各ファイル・システムを移動できます。

外部ストレージの追加に複数の方式 (iSCSI、ファイバー・チャネル、NFS (ネットワーク・ファイル・システム) など) を使用できます。UI からアクセス可能で検索可能なデータ (/store/ariel ディレクトリーなど) を保管するには、iSCSI またはファイバー・チャネルを使用する必要があります。

重要: NFS の用途は日次バックアップ・データに限定されます (/store/backup/ディレクトリーなど)。

オフボード・ストレージ・ソリューションを任意の管理対象ホストまたはコンソールに対して使用できます (高可用性システム (HA) の場合を含む)。HA で iSCSI またはファイバー・チャネルを使用する場合、アクティブ HA ノードが外部ストレージ・デバイスをマウントし、HA で障害が発生してもデータの整合性が保障されます。HA で外部ストレージを使用する場合、プライマリー HA ホストおよびセカンダリー HA ホストに対してそれらのデバイスを構成する必要があります。

オフボード・ストレージ・ソリューションを実装する前に、ローカル・ストレージ・オプション、既存のハードウェア・インフラストラクチャー、データ保存要件、およびフォールト・トレランス要件を検討してください。

ローカル・ストレージ

QRadar アプライアンス上にローカルに保管したデータ (最大で 40 TB のデータまでサポート) には、外部ストレージより短い待ち時間でアクセスできます。可能な場合は、外部ストレージ・デバイスの代わりにローカル・ストレージおよびデータ・ノード・アプライアンスを使用してください。

複数のアプライアンス

QRadar デプロイメントでより多くのストレージ容量が必要な場合、複数のアプライアンスを使用します。

複数のアプライアンスを使用できない場合、または既存のデプロイメントで外部ストレージを使用して容量を増加できる場合、ご使用のデプロイメントには外部ストレージが適している可能性があります。

ハードウェアおよびインフラストラクチャー

オフボード・ストレージ・ソリューションを使用するかどうか決定する場合、既存のインフラストラクチャーおよびストレージ・エリア・ネットワークに関する経験が重要な要素となります。

特定のオフボード・デバイスでは、構成をそれほど行う必要がなく、既存のネットワーク・インフラストラクチャーを使用できる場合があります。例えば、iSCSI で

は、既存のイーサネット・ネットワークを使用し、一方、ファイバー・チャンネルでは、より特殊なハードウェアを使用します。

データ保存およびフォールト・トレランス

オフボード・ストレージ・ソリューションを検討する際に、QRadar データ保存ポリシーが重要です。データ保存設定が既存のストレージの容量を超えている場合、または既存のデプロイ済みアプライアンスの保存容量の拡張を計画している場合、オフボード・ストレージ・ソリューションが必要になる可能性があります。

オフボード・ストレージ・ソリューションを使用すると、フォールト・トレランス機能および災害復旧機能を向上できます。

オフボード・ストレージのファイル・システム・オプション

オフボード・ストレージ・ソリューションを使用して、/store ファイル・システムまたは特定のサブディレクトリー (/store/ariel ディレクトリーなど) を移動します。

IBM Security QRadar デプロイメントでフォールト・トレランス・レベルを向上させたい場合、/store ファイル・システムを移動できます。各オプションは QRadar のパフォーマンスに影響します。

/store ファイル・システムを外部デバイスに移動することにより、高可用性システムの実装に代わる方法を利用できます。

/store/ariel ディレクトリーは、オフボード・ストレージ・ソリューションに移動する最も一般的なファイル・システムです。/store/ariel ファイル・システムを移動すると、収集されるログおよびネットワーク・アクティビティー・データを外部ストレージに移動できます。ローカル・ディスクは、引き続き PostgreSQL データベースおよび一時検索結果に使用されます。

管理者は、以下のタイプの QRadar データをオフボード・ストレージ・デバイスに移動できます。

- PostgreSQL メタデータおよび構成情報
- ログ・アクティビティー、ペイロード (生データ)、正規化されたデータ、および索引
- ネットワーク・アクティビティー、ペイロード、正規化されたデータ、および索引
- 時系列グラフ (グローバル・ビューおよび集約)

オフボード・ストレージ・ソリューションのパフォーマンスへの影響

/store ファイル・システムを外部デバイスに移動すると、QRadar のパフォーマンスに影響を及ぼす可能性があります。

マイグレーション後、/store ファイル・システムとのすべてのデータの I/O は、ローカル・ディスク上では実行されなくなります。QRadar データを外部ストレージ・デバイスに移動する前に、以下の情報を考慮する必要があります。

- 使用されていない /store ファイル・パーティションに /store/transient ファイル・システムをマウントすることで、ご使用のローカル・ディスクでのログ・アクティビティーおよびネットワーク・アクティビティーの検索を維持してください。
- 保存済みのマークが付けられている検索は、/store/transient ディレクトリー内にもあります。ローカル・ディスクで障害が発生した場合、これらの検索は保存されません。

ストレージ拡張

複数のボリュームを作成し、/store/ariel/events と /store/ariel/flows をマウントすることにより、QRadar でサポートされるファイル・システムの限界である 16 TB を超えてストレージ容量を拡張することができます。

/store ファイル・システム内の任意のサブディレクトリーを、外部ストレージ・デバイスのマウント・ポイントとして使用できます。

専用のイベント・データまたはフロー・データを移動する場合には、限定的な追加のマウント・ポイントを構成する可能性があります。例えば、/store/ariel/events/records と /store/ariel/events/payloads をマウント・ポイントとして構成できます。限定的なマウント・ポイントは、ログ・アクティビティー・データまたはネットワーク・アクティビティー・データ用として最大 32 TB のストレージを用意することができます。

外部ストレージ・オプション

iSCSI、ファイバー・チャネル、または NFS を使用してオフボード・ストレージ・ソリューションを提供できます。

オンボード・ディスクは、オフボード・ストレージ・デバイスよりも高速なソリューションを提供します。アプライアンスのローカル・ディスク・ストレージは、IBM Security QRadar の 200 から 400 MBps の読み取り速度および約 200 MBps の書き込み速度をサポートしています。複数のアプライアンスをデプロイすると、パフォーマンスとキャパシティーが同じ比率で上昇します。

ファイバー・チャネル

ファイバー・チャネルでは、ネットワークの構成に基づいて、200 MBps から 3200 MBps のストレージ・エリア・ネットワーク (SAN) 速度を使用することで、最も高速なオフボード・パフォーマンスを実現します。

ファイバー・チャネルのパフォーマンスは、以下の要因など、SAN 実装内の要因に影響を受ける場合があります。

- ボリュームあたりのディスク数またはスピンドル数
- 並行セッションの数
- SAN コントローラーのキャッシュ容量

iSCSI iSCSI では、専用 SAN ネットワークではなく、標準イーサネット・インフラストラクチャーで専用ストレージ・チャネルが使用されます。このため、iSCSI は、最大のコスト効率および最大の利便性を最も簡単に実現できます。

iSCSI ソリューションを実装する場合、外部ストレージ・アクセスと管理インターフェース I/O の間でネットワーク容量が共有されます。このソリューションでは、個別ストレージ・ネットワークでセカンダリー・ネットワーク・インターフェースを構成できます。

専用インターフェースを使用しても、1 Gbps に制限され、200 MBps から 400 MBps の速度しか実現できない場合があります。iSCSI ストレージ・デバイスでは、25 MBps から 50 MBps の I/O パフォーマンスしか実現できない場合があります。

NFS アクティブな QRadar データを保管するために、ネットワーク・ファイル・システム (NFS) ソリューションは使用しないでください。/store/backup ファイル・システムを外部 NFS に移動できます。

/store ファイル・システムを NFS ソリューションにマウントすると、PostgreSQL データが破損する可能性があります。/store/ariel ファイル・システムを NFS にマウントすると、QRadar でパフォーマンスの問題が発生します。

オフピーク時間中のタスク、バッチ・ファイルの書き込みがあるタスク、およびファイル I/O の量が限られているタスクに対して NFS を使用します。例えば、毎日の構成およびデータ・バックアップに NFS を使用します。

NFS ストレージは、既存の管理イーサネット・ネットワーク上で作動し、パフォーマンス・レベルは 20 MBps から 50 MBps に制限されます。NFS プロトコルは、ファイル・アクセス、ロック、およびネットワーク許可のパフォーマンスに影響する場合があります。専用ネットワーク・インターフェースを使用することで、パフォーマンスへの影響を軽減してください。

NFS をバックアップにのみ使用する場合、各ホストに対し同じ NFS 共有を使用できます。バックアップ・ファイルにシステム・ホスト名が含まれているため、各バックアップ・ファイルを識別できます。NFS 共有で長期データを保管する場合、デプロイメント内のアプライアンスごとに個別の共有またはエクスポートを検討します。

外部ストレージの制限

複数のシステムは、IBM Security QRadar デプロイメントの同じブロック・デバイスにアクセスすることができません。

HA 環境で iSCSI を構成する場合、プライマリー・ホストがボリュームにアクセスしている間に、セカンダリー・ホストに iSCSI ボリュームまたはファイバー・チャネル・ボリュームをマウントしないでください。

外部ストレージ・デバイスでは、100 MBps から 200 MBps の一貫した読み取りおよび書き込み能力を提供できる必要があります。一貫した読み取りおよび書き込み能力を提供できない場合、以下の問題が発生する場合があります。

- データ書き込みのパフォーマンスが影響を受ける。
- 検索のパフォーマンスが影響を受ける。

パフォーマンスの低下が続くと、処理のパイプラインがブロック状態になる場合があります。QRadar で警告メッセージが表示され、イベントおよびフローがドロップする可能性があります。

HA 環境でのオフボード・ストレージ

高可用性 (HA) 環境で /store ファイル・システムを移動した場合、/store ファイル・システムはディスク複製ブロック・デバイスを使用して複製されません。

/store/ariel ファイル・システムをオフボード・ストレージ・デバイスに移動し、ローカル・ディスクで /store ファイル・システムを保持する場合、/store ファイル・システムとセカンダリー HA ホストが同期されます。デフォルトでは、環境が HA 対応として構成されている場合、ディスク複製ブロック・デバイスは使用可能です。

第 2 章 iSCSI 外部ストレージ・デバイス

管理者は、標準または高可用性 (HA) IBM Security QRadar デプロイメントで iSCSI ストレージ・デバイスを構成できます。

iSCSI 外部ストレージ・デバイスを構成する場合、/store ファイル・システムまたは /store/ariel ファイル・システムで維持されている QRadar データをマイグレーションし、その後、/store ファイル・システムまたは /store/ariel ファイル・システムを iSCSI デバイス・ボリュームのパーティションにマウントする必要があります。

デバイス構成によっては、ファイバー・チャネル・ディスクのボリュームにパーティションを作成しなければならない可能性があります。

HA デプロイメントで iSCSI を構成し、プライマリー HA ホストで障害が発生した場合には、セカンダリー HA ホストとのデータの整合性を維持するために iSCSI デバイスを使用できます。

HA 環境での iSCSI 構成オプション

iSCSI の構成は、プライマリー HA ホストとセカンダリー HA ホストで異なります。iSCSI を構成する場合、HA クラスター内でプライマリー HA ホストとセカンダリー HA ホストを接続しないようにする必要があります。

HA 環境で /var/log/messages ファイルを確認し、iSCSI ストレージ構成のエラーがないか調べます。

必ず、プライマリー HA ホストとセカンダリー HA ホストで異なる **initiatorname** を使用してください。各 **initiatorname** が iSCSI デバイスの同じボリュームにアクセスできるように iSCSI デバイスを構成する必要があります。

/etc/iscsi/initiatorname.iscsi ファイルで **initiatorname** を構成します。QRadar は、これを使用して、/store ファイル・システムまたは /store/ariel ファイル・システムのマウント先の iSCSI デバイス・ボリュームを識別します。

関連タスク:

15 ページの『HA デプロイメント環境での iSCSI の構成』
高可用性 (HA) 環境で iSCSI デバイスを使用するには、同じ iSCSI 外部ストレージ・デバイスを使用するようにプライマリー HA ホストとセカンダリー HA ホストを構成する必要があります。

セカンダリー・ネットワーク・インターフェース

iSCSI ストレージ・エリア・ネットワーク (SAN) に接続するための専用 IP アドレスを持つセカンダリー・ネットワーク・インターフェースを構成できます。

セカンダリー・ネットワーク・インターフェースを使用すると、パフォーマンスが向上します。セカンダリー・ネットワーク・インターフェースを構成する場合、

SAN ネットワーク・マネージャーからのアドレス情報が必要です。ネットワーク・インターフェースの構成方法について詳しくは、「管理ガイド」を参照してください。

iSCSI デプロイメントでの HA システム

iSCSI ストレージ・ネットワークへの専用アクセスのために、以下の順番で高可用性 (HA)、iSCSI、およびネットワーク・インターフェースをセットアップします。

1. プライマリー・アプライアンスおよびセカンダリー・アプライアンスを構成します。
2. 両方のホストで外部 iSCSI ストレージをセットアップします。
3. プライマリー・ホストおよびセカンダリー・ホストで HA を構成します。

IBM Security QRadar の HA プロセスにより、すべてのネットワーク・インターフェースが制御されます。HA アプライアンスがアクティブ・モードの場合、HA プロセスによりこれらのインターフェースが使用可能になります。HA がスタンバイ・モードの場合、HA プロセスによりこれらのインターフェースが使用不可になります。ストレージの専用ネットワーク・インターフェースが使用不可で、HA システムがフェイルオーバーに移行すると、スタンバイ・ホストがアクティブ・モードに移行しようとしています。HA システムがスタンバイ・モードの場合、iSCSI ストレージ・システムにはアクセスできません。HA ノードがスタンバイからアクティブに移行する間、アクセスの問題が発生します。HA プロセスによりセカンダリー・インターフェースがオンラインに移行されますが、iSCSI システムのマウント時にネットワークが使用不可であり、フェイルオーバー・プロセスが失敗します。スタンバイ HA ホストをアクティブ・モードに変更することができません。

この問題を解決するには、ネットワーク・インターフェースが常にアクティブになるように、iSCSI ネットワーク・インターフェースの制御を HA システムから解除する必要があります。HA ノードの状況に対するネットワーク・インターフェースの依存関係を削除します。HA のプライマリー・ホストおよびセカンダリー・ホストには、これらのセカンダリー・ネットワーク・インターフェースの固有 IP アドレスが必要です。

関連タスク:

17 ページの『HA デプロイメント環境でのセカンダリー・インターフェースの制御の構成』

高可用性 (HA) デプロイメント環境で iSCSI および専用のネットワーク・インターフェースを使用する場合は、セカンダリー・インターフェースが HA プロセスを通じて管理されることのないようにする必要があります。セカンダリー HA ホストへのフェイルオーバーが発生した場合に、セカンダリー・インターフェースが常にアクティブな状態を維持するように、そのインターフェースの管理を構成します。

標準的な QRadar デプロイメント環境での iSCSI 構成

標準的なデプロイメント環境で QRadar コンソール を使用して iSCSI を構成します。

管理者は、以下のタスクをこの順番で実行する必要があります。

1. iSCSI ボリュームを構成します。

2. ファイル・システムを iSCSI ストレージ・ソリューションにマイグレーションします。
 - /store/ariel ファイル・システムを iSCSI ストレージ・ソリューションに移動します。
 - /store ファイル・システムを iSCSI ストレージ・ソリューションに移動します。
 - iSCSI ボリュームを自動的にマウントします。
3. iSCSI の接続を検証します。

iSCSI ボリュームの構成

iSCSI は、スタンドアロンの QRadar コンソール用にも、あるいは高可用性 (HA) デプロイメント環境におけるプライマリー HA ホストの QRadar コンソール用にも構成できます。

このタスクについて

オプションで、外部の iSCSI ストレージ・デバイスのボリューム上にパーティションを作成できます。

IBM Security QRadar V7.2.1 以降では、XFS ファイル・システムが使用されています。使用されているファイル・システムが ext4 と XFS のいずれであっても、iSCSI デバイスにパーティションを作成することができます。

ディスクのパーティションは、GUID パーティション・テーブル (GPT) を使用して作成されます。新しいデバイス・パーティションを、マイグレーションする /store や /store/ariel などのファイル・システム用のマウント・ポイントとして使用することができます。

重要: iSCSI デバイス・パーティションまたはファイバー・チャネル・デバイス・パーティションを外部デバイス上に作成して QRadar データを保管している場合には、パーティションを作成することも、ボリューム上のパーティションを再フォーマットすることもできません。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. /etc/iscsi/initiatorname.iscsi ファイルを編集して、ご使用のホストの iSCSI 修飾名を組み込みます。

```
InitiatorName=iqn.yyyy-mm.{reversed domain name}:hostname
```

例: InitiatorName=iqn.2014-11.com.qradar:pl13

3. コマンド `service iscsi restart` を入力して、iSCSI サーバーとのセッションを開きます。
4. iSCSI サーバー上のボリュームを検出するため、以下のコマンドを入力します。

```
iscsiadm -m discovery --type sendtargets --portal IP address:[port]
```

IP address オプションは、iSCSI サーバーの IP アドレスです。 *port* はオプションです。 イニシエーター名を記録します。

5. iSCSI サーバーにログインするため、次のコマンドを入力します。

```
iscsiadm -m node --targetname <Initiator name from step 4> --portal <IP address:[port]> --login
```

6. iSCSI デバイス・ボリューム名を検索するために、以下のコマンドを入力します。

```
dmesg | grep "Attached SCSI disk"
```

7. オプション: パーティションを作成する場合は、GNU の以下の `parted` コマンドを使用します。

```
parted /dev/volume
```

8. 以下のコマンドを入力して、GPT を使用するようにパーティション・ラベルを構成します。

```
mklabel gpt
```

9. 以下のメッセージが表示された場合は、Yes と入力します。

```
警告: /dev/volume 上の既存のディスク・ラベルが破棄され、  
このディスク上のすべてのデータが失われます。続行しますか?  
(Warning: The existing disk label on /dev/volume will be  
destroyed and all data on this disk will be lost. Do you want to  
continue?)
```

10. iSCSI ディスク・ボリューム上にパーティションを作成します。

- a. パーティションを作成するために、以下のコマンドを入力します。

```
mkpart primary 0% 100%
```

- b. 以下のコマンドを入力して、デフォルト単位を TB に設定します。

```
unit TB
```

- c. 以下のコマンドを入力して、パーティションが作成されていることを検証します。

```
print
```

- d. 以下のコマンドを入力して、GNU の `parted` を終了します。

```
quit
```

- e. 以下のコマンドを入力して、新しいパーティションのデータでカーネルを更新します。

```
partprobe /dev/volume
```

アプライアンスを再起動するように指示するプロンプトが表示される場合があります。

- f. パーティションが作成されていることを検証するために、以下のコマンドを入力します。

```
cat /proc/partitions
```

- パーティションを再フォーマットしてファイル・システムを作成します。
 - XFS ファイル・システムを作成するには、以下のコマンドを入力します。

```
mkfs.xfs -f /dev/partition
```
 - ext4 ファイル・システムの場合は、以下のコマンドを入力します。

```
mkfs.ext4 /dev/partition
```

次のタスク

『iSCSI ストレージ・ソリューションへの /store/ariel ファイル・システムの移動』または 12 ページの『iSCSI ストレージ・ソリューションへの /store ファイル・システムの移動』を参照してください。

関連タスク:

19 ページの『iSCSI に関する問題のトラブルシューティング』
iSCSI のディスクおよび通信に関する問題を防止するには、QRadar、iSCSI サーバー、およびネットワーク・スイッチを、無停電電源装置 (UPS) に接続する必要があります。ネットワーク・スイッチで電源障害が発生すると、iSCSI ボリュームでディスク・エラーが報告されたり、あるいはこのボリュームが読み取り専用の状態のままになったりする可能性があります。

iSCSI ストレージ・ソリューションへの /store/ariel ファイル・システムの移動

/store/ariel ファイル・システムで維持されている IBM Security QRadar データをマイグレーションして、/store/ariel ファイル・システムを iSCSI デバイス・パーティションにマウントすることができます。

始める前に

iSCSI ボリュームを構成します。

手順

- 以下のコマンドを入力して、hostcontext サービスを停止します。

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```
- 以下のコマンドを入力して、既存のマウント・ポイントを移動します。

```
cd /store
mv ariel ariel_old
```
- 以下のコマンドを入力して、iSCSI デバイス・パーティションの Universally Unique Identifier (UUID) を検証します。

```
blkid /dev/partition
```
- 以下のテキストを /etc/fstab ファイルに追加して、/store/ariel ファイル・システム用のマウント・ポイントを追加します。
 - ファイル・システムが ext4 の場合、次のテキストを追加します。

```
UUID=uuid /store/ariel ext4 noatime,noauto,nobarrier 0 0
```

- ファイル・システムが XFS の場合、次のテキストをテキスト・エディターにコピーし、改行を削除して、単一の行として貼り付けます。

```
UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,  
noauto,noatime 0 0
```

5. 以下のコマンドを入力して、マウント・ポイント用の `ariel` ディレクトリーを作成します。

```
mkdir ariel
```

6. 以下のコマンドを入力して、iSCSI デバイス・パーティションに `/store/ariel` をマウントします。

```
mount /store/ariel
```

7. 以下のコマンドを入力して、`/store/ariel` が正しくマウントされていることを検証します。

```
df -h
```

8. 以下のコマンドを入力して、ローカル・ディスクのデータを iSCSI ストレージ・デバイスに移動します。

```
mv /store/ariel_old/* /store/ariel
```

9. 以下のコマンドを入力して `/store/ariel_old` ディレクトリーを削除します。

```
rmdir /store/ariel_old
```

10. 以下のコマンドを入力して、`hostcontext` サービスを始動します。

```
service crond start  
service systemStabMon start  
service hostservices start  
service tomcat start  
service hostcontext start
```

次のタスク

14 ページの『iSCSI ボリュームの自動マウント』を参照してください。

関連タスク:

『iSCSI ストレージ・ソリューションへの `/store` ファイル・システムの移動』

`/store` ファイル・システムで維持されている IBM Security QRadar データをマイグレーションして、`/store` ファイル・システムを iSCSI デバイス・パーティションにマウントすることができます。

iSCSI ストレージ・ソリューションへの `/store` ファイル・システムの移動

`/store` ファイル・システムで維持されている IBM Security QRadar データをマイグレーションして、`/store` ファイル・システムを iSCSI デバイス・パーティションにマウントすることができます。

オフボード・ストレージ・デバイスへの `/store` ファイル・システムのマイグレーションには、長時間かかる可能性があります。

始める前に

iSCSI ボリュームを構成します。

手順

1. 以下のコマンドを入力して、`hostcontext` サービスを停止します。

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

2. 以下のコマンドを入力して、ファイル・システムをアンマウントします。

```
umount /store/tmp
umount /store/transient
umount /store
```

3. 以下のコマンドを入力して `/store_old` ディレクトリーを作成します。

```
mkdir /store_old
```

4. 以下のコマンドを入力して、iSCSI デバイス・パーティションの `Universal Unique Identifier (UUID)` を取得します。

```
blkid /dev/partition
```

5. `/etc/fstab` ファイルを編集して、既存の `/store` ファイル・システムのマウント・ポイントを、`/store_old` に更新します。

6. 以下のテキストを `/etc/fstab` ファイルに追加して、`/store` ファイル・システム用の新しいマウント・ポイントを追加します。

- ファイル・システムが `ext4` の場合、次のテキストを追加します。

```
UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
```

- ファイル・システムが `XFS` の場合、次のテキストを追加します。

```
UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- a. 以下のファイル・システム・オプションを使用するように `/store/tmp` のマウント行を変更します。

```
noatime,noauto,nobarrier 0 0
```

- b. `/store/transient` が `fstab` ファイル内にリストされている場合は、次のファイル・システム・オプションを入力します。

```
xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- c. ファイルを保存して閉じます。

7. 以下のコマンドを入力して、iSCSI デバイス・パーティションに `/store` ファイル・システムをマウントします。

```
mount /store
```

8. 以下のコマンドを入力して、ローカル・ディスクに `/store_old` ファイル・システムをマウントします。

```
mount /store_old
```

9. 以下のコマンドを入力して、ローカル・ディスクのデータを iSCSI ストレージ・デバイスに移動します。

```
mv -f /store_old/* /store
```

10. 以下のコマンドを入力して、ファイル・システムを再マウントします。

```
mount /store/tmp  
mount /store/transient
```

11. 以下のコマンドを入力して、/store_old をアンマウントします。

```
umount /store_old
```

12. 以下のコマンドを入力して、/store_old ディレクトリーを /etc/fstab ファイルから削除します。

```
rmdir /store_old
```

13. 以下のコマンドを入力して、hostcontext サービスを始動します。

```
service crond start  
service systemStabMon start  
service hostservices start  
service tomcat start  
service hostcontext start
```

次のタスク

『iSCSI ボリュームの自動マウント』を参照してください。

関連タスク:

11 ページの『iSCSI ストレージ・ソリューションへの /store/ariel ファイル・システムの移動』

/store/ariel ファイル・システムで維持されている IBM Security QRadar データをマイグレーションして、/store/ariel ファイル・システムを iSCSI デバイス・パーティションにマウントすることができます。

iSCSI ボリュームの自動マウント

iSCSI ボリュームを自動的にマウントするように IBM Security QRadar を構成する必要があります。

始める前に

/store/ariel と /store の各ファイル・システムを iSCSI ストレージ・ソリューションに移動してあることを確認してください。

手順

1. 以下のコマンドを入力して、iSCSI スクリプトを始動情報に追加します。

```
chkconfig --add iscsi  
chkconfig --level 345 iscsi on
```

2. 以下のコマンドを入力して、iSCSI ストレージ・ソリューションをマウントするスクリプトへのシンボリック・リンクを作成します。

```
ln -s /opt/qradar/init/iscsi-mount /etc/init.d
```

3. 以下のコマンドを入力して、マウント・スクリプトを始動情報に追加します。

```
chkconfig --add iscsi-mount  
chkconfig --level 345 iscsi-mount on
```

4. システムを再始動して、iSCSI デバイスが正常にマウントされていることを検証します。
 - a. 以下のコマンドを入力して、システムを再始動します。reboot
 - b. コマンド `df -h` を入力して、iSCSI マウント・ポイントが保持されていることを確認します。

次のタスク

高可用性 (HA) 環境を構成する場合は、プライマリー HA ホストに使用したものと同一 iSCSI 接続を使用してセカンダリー HA ホストをセットアップする必要があります。詳しくは、『HA デプロイメント環境での iSCSI の構成』を参照してください。

関連タスク:

『HA デプロイメント環境での iSCSI の構成』

高可用性 (HA) 環境で iSCSI デバイスを使用するには、同じ iSCSI 外部ストレージ・デバイスを使用するようにプライマリー HA ホストとセカンダリー HA ホストを構成する必要があります。

HA デプロイメント環境での iSCSI の構成

高可用性 (HA) 環境で iSCSI デバイスを使用するには、同じ iSCSI 外部ストレージ・デバイスを使用するようにプライマリー HA ホストとセカンダリー HA ホストを構成する必要があります。

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。
2. iSCSI デバイス・ボリュームを識別するようにセカンダリー HA ホストを構成するため、ホストの iSCSI 修飾名を `/etc/iscsi/initiatorname.iscsi` ファイルに追加します。

```
Initiatorname=iqn.yyyy-mm.{reversed domain name}:hostname
```

例: `InitiatorName=iqn.2008-11.com.qradar:p113`

3. 以下のコマンドを入力することにより、iSCSI サービスを再始動してサーバーとのセッションを開きます。

```
service iscsi restart
```

4. iSCSI サーバー上のボリュームを検出するため、以下のコマンドを入力します。

```
iscsiadm -m discovery --type sendtargets --portal IP address:[port]
```

注: `port` はオプションです。

5. 以下のコマンドを入力して、iSCSI サーバーへのログインを検証します。

```
iscsiadm -m node -l
```

6. iSCSI デバイス・ボリューム名を検索するために、以下のコマンドを入力します。

```
dmesg | grep "Attached SCSI disk"
```

7. オプション: パーティションを作成する場合は、GNU の以下の `parted` コマンドを使用します。

```
parted /dev/volume
```

8. セカンダリー HA ホストのマウント・ポイントを構成します。
 - a. ファイル・システムをアンマウントするために、以下のコマンドを入力します。

```
umount /store/tmp  
umount /store/transient  
umount /store
```

- b. 以下のコマンドを入力して、iSCSI デバイス・パーティションの UUID を識別します。

```
blkid /dev/partition
```

- c. `/store` ファイル・システムを移動する場合、`/etc/fstab` ファイル内のファイル設定を、プライマリー HA ホスト上の `/etc/fstab` ファイルにリストされているマウント・ポイントと同一になるように編集します。

- `/store`
- `/store/temp`
- `/store/transient`

- d. `/store/ariel` ファイル・システムを移動する場合、`/etc/fstab` ファイル内の設定を、`/store/ariel` に対して、プライマリー HA ホスト上の `/etc/fstab` ファイルにリストされているマウント・ポイントと同一になるように編集します。

9. iSCSI ボリュームを自動的にマウントするようにセカンダリー HA ホストを構成します。

- a. 以下のコマンドを入力して、iSCSI スクリプトを始動情報に追加します。

```
chkconfig --add iscsi  
chkconfig --level 345 iscsi on
```

- b. 以下のコマンドを入力して、マウント・スクリプトへのシンボリック・リンクを作成します。

```
ln -s /opt/qradar/init/iscsi-mount /etc/init.d
```

- c. 以下のコマンドを入力して、マウント・スクリプトを始動情報に追加します。

```
chkconfig --add iscsi-mount  
chkconfig --level 345 iscsi-mount on
```

次のタスク

18 ページの『iSCSI 接続の検証』を参照してください。

関連概念:

7 ページの『HA 環境での iSCSI 構成オプション』

iSCSI の構成は、プライマリー HA ホストとセカンダリー HA ホストで異なります。iSCSI を構成する場合、HA クラスタ内でプライマリー HA ホストとセカンダリー HA ホストを接続しないようにする必要があります。

HA デプロイメント環境でのセカンダリー・インターフェースの制御の構成

高可用性 (HA) デプロイメント環境で iSCSI および専用のネットワーク・インターフェースを使用する場合は、セカンダリー・インターフェースが HA プロセスを通じて管理されることのないようにする必要があります。セカンダリー HA ホストへのフェイルオーバーが発生した場合に、セカンダリー・インターフェースが常にアクティブな状態を維持するように、そのインターフェースの管理を構成します。

始める前に

以下の条件が満たされていることを確認してください。

- 各 HA サーバー上の専用の iSCSI ネットワーク・インターフェースに対して、それぞれ別の IP アドレスが設定されている。

それぞれ別の IP アドレスを設定することで、ネットワーク・インターフェースが両方の HA ホスト上で同時にアクティブになっている場合に、IP アドレスの競合が回避されます。iSCSI ソフトウェアおよびドライバーは、始動時と HA フェイルオーバー中に外部ストレージにアクセスできます。HA ノードがスタンバイからアクティブに切り替わる時に、外部ボリュームを正常にマウントできるようにもなります。

- プライマリーとセカンダリーのアプライアンスが構成されている。

詳しくは、「IBM Security QRadar 高可用性ガイド」を参照してください。

- iSCSI ストレージが構成されている。

手順

1. プライマリー・ホスト上で、SSH を使用し root ユーザーとして QRadar コンソール にログインします。
2. ネットワーク・インターフェースの QRadar HA サービスの制御を無効にします。
 - a. `/opt/qradar/ha/interfaces/` ディレクトリーに移動します。

このディレクトリーには、`ifcfg-ethN` という名前のファイルのリストが格納されています。QRadar HA プロセスで制御されるインターフェースのそれぞれに対し、1 つのファイルが存在します。

- b. iSCSI ストレージ・ネットワークへのアクセスに使用されるファイルを削除します。

このファイルを削除すると、インターフェースの制御が HA プロセスから解除されます。

3. ネットワーク・インターフェースのオペレーティング・システム・レベルでの制御を再び有効にします。
 - a. `/etc/sysconfig/network-scripts/ifcfg-ethN` ディレクトリーに移動します。
 - b. iSCSI ネットワークに接続するインターフェースの `ifcfg-ethN` ファイルを開きます。
 - c. ネットワーク・インターフェースを常にアクティブな状態にするために、ONBOOT パラメーターの値を `ONBOOT=yes` に変更します。

- 、以下のコマンドを実行して、iSCSI サービスを再始動します。

```
/etc/init.d/iscsid restart
```

- これらのステップを、セカンダリー HA アプライアンスに対して繰り返します。
- オプション: セカンダリー・アプライアンスからの iSCSI ストレージへのアクセスをテストする場合は、以下の ping コマンドを使用します。

```
ping iscsi_server_ip_address
```

関連概念:

7 ページの『セカンダリー・ネットワーク・インターフェース』

iSCSI ストレージ・エリア・ネットワーク (SAN) に接続するための専用 IP アドレスを持つセカンダリー・ネットワーク・インターフェースを構成できます。

iSCSI 接続の検証

プライマリー HA ホスト (またはセカンダリー HA ホスト) と iSCSI デバイスとの間の接続が作動可能であることを検証します。

手順

- SSH を使用して、プライマリー HA ホストまたはセカンダリー HA ホストに root ユーザーとしてログインします。
- iSCSI ストレージ・デバイスへの接続をテストするため、以下のコマンドを入力します。

```
ping iSCSI_Storage_IP_Address
```

- 以下のコマンドを入力して、iSCSI サービスが実行されていること、および iSCSI ポートが使用可能であることを検証します。

```
telnet iSCSI_Storage_IP_Address 3260
```

注: デフォルト・ポートは 3260 です。

- 以下のコマンドを入力して、iSCSI デバイスへの接続が作動可能であることを検証します。

```
iscsiadm -m node
```

iSCSI デバイスが正しく構成されていることを検証するには、プライマリー HA ホストについて表示される出力が、セカンダリー HA ホストについて表示される出力と一致することを確認する必要があります。

iSCSI ボリュームへの接続が作動可能ではない場合には、以下のメッセージが表示されます。

```
iscsiadm: レコードが見つかりません (iscsiadm: No records found)
```

- iSCSI ボリュームへの接続が作動可能ではない場合には、以下のトラブルシューティング・オプションを検討してください。
 - 外部の iSCSI ストレージ・デバイスが作動可能であることを検証します。

- /var/log/messages ファイルにアクセスし、このファイルの内容を確認して、iSCSI ストレージ構成が原因の固有のエラーがあるかどうかを調べます。
- /etc/iscsi/initiatornames.iscsi ファイルを使用して iSCSI の **initiatornames** の値が正しく構成されていることを確認します。
- エラー・ログでエラーを見つけることができず、iSCSI 接続が無効な状態が続いている場合は、ネットワーク管理者に連絡して、iSCSI サーバーが動作しているか、あるいは、ネットワーク構成に変更がなかったかを確認します。
- ネットワーク構成が変更されている場合は、iSCSI 接続を再構成する必要があります。

次のタスク

HA クラスタを確立します。QRadar ユーザー・インターフェースを使用して、プライマリー HA ホストをセカンダリー HA ホストと接続する必要があります。HA クラスタの作成について詳しくは、「*IBM Security QRadar 高可用性ガイド*」を参照してください。

iSCSI に関する問題のトラブルシューティング

iSCSI のディスクおよび通信に関する問題を防止するには、QRadar、iSCSI サーバー、およびネットワーク・スイッチを、無停電電源装置 (UPS) に接続する必要があります。ネットワーク・スイッチで電源障害が発生すると、iSCSI ボリュームでディスク・エラーが報告されたり、あるいはこのボリュームが読み取り専用の状態のままになったりする可能性があります。

.

このタスクについて

高可用性 (HA) 環境では、プライマリー・ホストで障害が発生した場合、プライマリー・ホストに対する iSCSI 構成を復元する必要があります。この場合、/store または /store/ariel のデータは、iSCSI 共有外部ストレージ・デバイスへと既にマイグレーションされています。従って、プライマリー・ホストの iSCSI 構成を復元するために、セカンダリー HA ホストを必ず構成してください。詳しくは、15 ページの『HA デプロイメント環境での iSCSI の構成』を参照してください。

手順

1. ディスク・エラーの有無を判別します。
 - a. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
 - b. 以下のいずれかのコマンドを入力して、iSCSI ボリューム上に filename.txt という名前の空のファイルを作成します。
 - touch /store/ariel/filename.txt
 - touch /store/filename.txt

iSCSI ボリュームが正しくマウントされていて、そのボリュームに対する書き込み権限をユーザーが持っている場合は、`touch` コマンドにより、`filename.txt` という名前の空のファイルが iSCSI ボリューム上に作成されます。

エラー・メッセージが表示された場合は、iSCSI ボリュームをアンマウントしてから再マウントします。

2. IBM Security QRadar サービスを停止します。

- `/store` ファイル・システムをマイグレーションした場合は、以下の各コマンドを指定の順序で入力します。
 - `service hostcontext stop`
 - `service tomcat stop`
 - `service hostservices stop`
 - `service systemStabMon stop`
 - `service crond stop`

- `/store/ariel` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
service hostcontext stop
```

3. iSCSI ボリュームをアンマウントします。

- `/store` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
– umount /store/tmp
```

```
– umount /store
```

- `/store/ariel` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
umount /store/ariel
```

4. iSCSI ボリュームをマウントします。

- `/store` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
mount /store
```

```
mount /store/tmp
```

- `/store/ariel` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
mount /store/ariel
```

5. マウント・ポイントをテストします。

- `/store` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
touch /store/filename.txt
```

- `/store/ariel` ファイル・システムをマイグレーションした場合は、以下のコマンドを入力します。

```
mount /store/ariel/filename.txt
```

ディスクの再マウント後に読み取り専用のエラー・メッセージが引き続き表示される場合は、iSCSI ボリュームを再構成します。

別の方法として、ファイル・システムを再度アンマウントし、コマンド `fsck /dev/partition` を使用して、手動でのファイル・システム・チェックを実行することもできます。

6. QRadar サービスを始動します。

- `/store` ファイル・システムをマイグレーションした場合は、以下の各コマンドを指定の順序で入力します。
 - `service crond start`
 - `service systemStabMon start`
 - `service hostservices start`
 - `service tomcat start`
 - `service hostcontext start`
- `/store/ariel` ファイル・システムをマイグレーションした場合は、コマンド `service hostcontext start` を入力します。

関連タスク:

9 ページの『iSCSI ボリュームの構成』

iSCSI は、スタンドアロンの QRadar コンソール用にも、あるいは高可用性 (HA) デプロイメント環境におけるプライマリー HA ホストの QRadar コンソール用にも構成できます。

第 3 章 ファイバー・チャネル・ストレージ

標準的な QRadar デプロイメント環境または高可用性 (HA) 環境で、ファイバー・チャネル (FC) を構成できます。また、FC スイッチで障害が発生した場合の冗長性を確保するために、FC マルチパスを構成することができます。

FC デバイスを構成する場合、IBM Security QRadar データを /store ファイル・システムまたは /store/ariel ファイル・システムに移動できます。その後、/store ファイル・システムまたは /store/ariel ファイル・システムを FC デバイスのパーティションにマウントします。

デバイス構成によっては、FC ディスクのボリュームにパーティションを作成しなければならない可能性があります。

HA デプロイメントで FC を構成し、プライマリー HA ホストで障害が発生した場合には、セカンダリー HA ホストとのデータの整合性を維持するために FC デバイスを使用できます。HA 環境でのデータの整合性および共有ストレージについて詳しくは、「IBM Security QRadar 高可用性ガイド」を参照してください。

ファイバー・チャネル・ストレージの構成の概要

ファイバー・チャネル (FC) の構成は、プライマリー高可用性 (HA) ホストとセカンダリー HA ホストで異なります。FC を構成する場合、HA クラスター内でプライマリー HA ホストとセカンダリー HA ホストを接続しないようにする必要があります。

頻繁に検索されるデータは、より高速なディスクに移動する必要があります。例えば、最新のデータや、セキュリティー・インシデントの調査のために使用されるデータは移動します。ただし、高性能のオフボード・ディスク・ストレージを導入するとコストがかかる場合があります。可能な場合は、古いデータの移動、アーカイブなどのアクティビティーや、レポート作成の目的では、性能と価格が低いオフボード・ストレージを使用します。

アーカイブの目的でのみ FC を使用する場合、すべてのアプライアンスに対し同じマウント・ポイントを使用し、それらのマウント・ポイントが各固有 FC ボリュームに対応するように構成します。

複数のアプライアンスを使用するデプロイメントでは、個別の FC ボリュームを使用するように各アプライアンスを構成する必要があります。個別ボリュームを使用しないと、2 つのデバイスが同じブロック・デバイスをマウントするという状況を招く可能性があります。これにより、ブロック・デバイス・ファイル・システムが破損する可能性があります。

Emulex アダプターのインストールの検証

Emulex LPe12002 ホスト・バス・アダプターが接続されており、さらに、正しいファームウェアとドライバーのバージョンを使用してインストールされていることを検証する必要があります。

始める前に

ファイバー・チャンネル・プロトコルを使用するには、Emulex LPe12002 ホスト・バス・アダプターを IBM Security QRadar アプライアンスにインストールする必要があります。高可用性 (HA) デプロイメント環境では、Emulex LPe12002 カードを、プライマリーとセカンダリーの HA ホストにインストールする必要があります。

Emulex LPe ホスト・バス・アダプターが使用するドライバーとファームウェアは、それぞれ以下のバージョンである必要があります。

- ドライバー・バージョン: 8.3.5.68.5p
- ファームウェア・バージョン: 1.10A5(U3D1.10A5),sli-3

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. 以下のコマンドを入力して、Emulex LPe12002 カードが接続されていることを検証します。

```
hbacmd listhbas
```

結果が表示されない場合には、システム管理者に連絡してください。

3. 以下のコマンドを入力して、Emulex カードが正しいファームウェアとドライバーのバージョンを使用していることを検証します。

```
hbacmd HBAAttrib
```

device id は、前のステップで表示されたポート WWN です。

関連タスク:

『ファイバー・チャンネル接続の検証』

外部のファイバー・チャンネル・デバイスのディスク・ボリュームを識別する必要があります。必要に応じて、ボリューム上にパーティションを作成する必要もあります。

ファイバー・チャンネル接続の検証

外部のファイバー・チャンネル・デバイスのディスク・ボリュームを識別する必要があります。必要に応じて、ボリューム上にパーティションを作成する必要もあります。

始める前に

Emulex アダプターのインストールを検証します。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. 以下のコマンドを入力して、ファイバー・チャンネルのボリュームを識別します。

```
ls -l /dev/disk/by-path/*-fc-*
```

複数のファイバー・チャンネル・デバイスが接続されていて、正しいファイバー・チャンネルのボリュームを識別できない場合は、システム管理者に連絡してください。

3. オプション: ファイバー・チャンネルのボリューム上にパーティションがない場合は、ファイバー・チャンネル・デバイスのボリューム上にパーティションを作成します。

- a. オプション: パーティションを作成する場合は、GNU の以下の `parted` コマンドを使用します。

```
parted /dev/volume
```

- b. 以下のコマンドを入力して、GPT を使用するようにパーティション・ラベルを構成します。

```
mklabel gpt
```

- c. 以下のメッセージが表示された場合は、Yes と入力します。

```
警告: /dev/volume 上の既存のディスク・ラベルが破棄され、  
このディスク上のすべてのデータが失われます。続行しますか?  
(Warning: The existing disk label on /dev/volume will be  
destroyed and all data on this disk will be lost. Do you want to  
continue?)
```

- d. パーティションを作成するために、以下のコマンドを入力します。

```
mkpart primary 0% 100%
```

- e. 以下のコマンドを入力して、デフォルト単位を TB に設定します。

```
unit TB
```

- f. 以下のコマンドを入力して、パーティションが作成されていることを検証します。

```
print
```

- g. 以下のコマンドを入力して、GNU の `parted` を終了します。

```
quit
```

- h. 以下のコマンドを入力して、新しいパーティションのデータでカーネルを更新します。

```
partprobe /dev/volume
```

アプライアンスを再起動するように指示するプロンプトが表示される場合があります。

- i. パーティションが作成されていることを検証するために、以下のコマンドを入力します。

```
cat /proc/partitions
```

4. パーティションを再フォーマットしてファイル・システムを作成します。

- XFS ファイル・システムを作成するには、以下のコマンドを入力します。

```
mkfs.xfs -f /dev/partition
```

- ext4 ファイル・システムの場合は、以下のコマンドを入力します。

```
mkfs.ext4 /dev/partition
```

関連タスク:

23 ページの『Emulex アダプターのインストールの検証』

Emulex LPe12002 ホスト・バス・アダプターが接続されており、さらに、正しいファームウェアとドライバーのバージョンを使用してインストールされていることを検証する必要があります。

ファイバー・チャネル・ソリューションへの /store ファイル・システムの移動

/store ファイル・システムで維持されている IBM Security QRadar データを移動して、/store ファイル・システムをファイバー・チャネル (FC) デバイス・パーティションにマウントすることができます。

始める前に

24 ページの『ファイバー・チャネル接続の検証』

手順

1. QRadar のインストール後、QRadar をファイバー・チャネルと接続し、再始動します。
2. 以下のコマンドを入力して、hostcontext サービスを停止します。

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

3. 以下のコマンドを入力して、ファイル・システムをアンマウントします。

```
umount /store/tmp
umount /store/transient
umount /store
```

/store/transient ファイル・システムがマウントされているのは、/store ファイル・システムが XFS であるときのみです。

4. 以下のコマンドを入力して /store_old ディレクトリーを作成します。

```
mkdir /store_old
```

5. 以下のコマンドを入力して、デバイス・パーティションの Universal Unique Identifier (UUID) を取得します。

```
blkid /dev/partition
```

6. /etc/fstab ファイルを編集して、既存の /store ファイル・システムのマウント・ポイントを、/store_old に更新します。

7. 以下のテキストを /etc/fstab ファイルに追加して、/store ファイル・システム用のマウント・ポイントを追加します。

- ファイル・システムが ext4 の場合、次のテキストを追加します。

```
UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
```

- ファイル・システムが XFS の場合、次のテキストを追加します。

```
UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- a. 以下のファイル・システム・オプションを使用するように /store/tmp のマウント行を変更します。

```
noatime,noauto,nobarrier 0 0
```

- b. /store/transient が fstab ファイル内にリストされている場合は、次のファイル・システム・オプションを入力します。

```
xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- c. ファイルを保存して閉じます。

8. 以下のコマンドを入力して、FC デバイス・パーティションに /store ファイル・システムをマウントします。

```
mount /store
```

9. 以下のコマンドを入力して、ローカル・ディスクに /store_old ファイル・システムをマウントします。

```
mount /store_old
```

10. 以下のコマンドを入力して、ファイバー・チャンネル・パーティションにデータをコピーします。

```
cp -af /store_old/* /store
```

11. 以下のコマンドを入力して、ファイル・システムをマウントします。

```
mount /store/tmp  
mount /store/transient
```

/store/transient ファイル・システムがマウントされているのは、/store ファイル・システムが XFS であるときのみです。

12. 以下のコマンドを入力して、/store_old をアンマウントします。

```
umount /store_old
```

13. /store_old ディレクトリーを /etc/fstab ファイルから削除します。

14. 以下のコマンドを入力して、hostcontext サービスを始動します。

```
service crond start  
service systemStabMon start  
service hostservices start  
service tomcat start  
service hostcontext start
```

次のタスク

29 ページの『ファイバー・チャンネル・マウント・ポイントの検証』を参照してください。

関連タスク:

28 ページの『ファイバー・チャンネル・ソリューションへの /store/ariel ファイル・システムの移動』

/store/ariel ファイル・システムで維持されている IBM Security QRadar データを移動して、/store/ariel ファイル・システムをファイバー・チャンネル (FC) デバイス・パーティションにマウントすることができます。

ファイバー・チャンネル・ソリューションへの /store/ariel ファイル・システムの移動

/store/ariel ファイル・システムで維持されている IBM Security QRadar データを移動して、/store/ariel ファイル・システムをファイバー・チャンネル (FC) デバイス・パーティションにマウントすることができます。

始める前に

24 ページの『ファイバー・チャンネル接続の検証』を参照してください。

手順

1. QRadar のインストール後、QRadar をファイバー・チャンネルと接続し、再始動します。
2. 以下の各コマンドを入力して、QRadar サービスを停止します。

```
service systemStabMon stop
service hostcontext stop
service tomcat stop
service hostservices stop
service crond stop
```

3. 以下のコマンドを入力して、一時ディレクトリーを作成します。

```
mkdir /tmp/fcdata
```

4. 以下のコマンドを入力して、ファイバー・チャンネル・ストレージ・パーティションを一時ディレクトリーにマウントします。

```
mount /dev/<partition> /tmp/fcdata
```

<partition> は、デバイス・パーティションの名前です。例えば、sdb1 などです。

5. 以下のコマンドを入力して、ファイバー・チャンネル・デバイスにデータをコピーします。

```
cp -af /store/ariel/* /tmp/fcdata
```

6. 以下のコマンドを入力して、ファイバー・チャンネル・パーティションをアンマウントします。

```
umount /tmp/fcdata
```

7. 以下のコマンドを入力して、iSCSI デバイス・パーティションの Universally Unique Identifier (UUID) を検証します。

```
blkid /dev/<partition>
```

<partition> は、デバイス・パーティションの名前です。例えば、sdb1 などです。

8. 以下のコマンドを入力して、fstab ファイルを編集します。 vi /etc/fstab

9. 以下のテキストを /etc/fstab ファイルに追加して、/store/ariel ファイル・システム用のマウント・ポイントを追加します。

ファイル・システムが ext4 の場合:

```
UUID=uuid /store/ariel ext4 defaults,noatime,nobarrier 1 2
```

ファイル・システムが XFS の場合:

```
UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,nobarrier 0
```

uuid は、ファイバー・チャンネル・デバイス・パーティションの UUID です。

10. ファイルを保存して閉じます。
11. 以下のコマンドを入力して、FC デバイス・パーティションに /store/ariel ファイル・システムをマウントします。

```
mount /store/ariel
```

12. 以下の各コマンドを入力して、QRadar サービスを開始します。

```
service crond start
service hostservices start
service tomcat start
service hostcontext start
service systemStabMon start
```

次のタスク

『ファイバー・チャンネル・マウント・ポイントの検証』.

関連タスク:

26 ページの『ファイバー・チャンネル・ソリューションへの /store ファイル・システムの移動』

/store ファイル・システムで維持されている IBM Security QRadar データを移動して、/store ファイル・システムをファイバー・チャンネル (FC) デバイス・パーティションにマウントすることができます。

ファイバー・チャンネル・マウント・ポイントの検証

プライマリー・ホスト上で、移動したファイル・システムがファイバー・チャンネル・デバイス・パーティションに正しくマウントされていることを検証します。

このタスクについて

手順

1. 以下のコマンドを入力します。

```
df -h
```

2. /store ファイル・システムまたは /store/ariel ファイル・システムが、ファイバー・チャンネル・デバイス・パーティションに正しくマウントされていることを検証します。

標準的な QRadar デプロイメント環境でのファイバー・チャンネルの構成

IBM Security QRadar では、マルチパス・ファイバー・チャンネルを実装できます。マルチパスを使用すると、ストレージ・エリア・ネットワーク (SAN) スイッチで問題が発生した場合に、フロー・データおよびイベント・データが中断されないように追加の冗長度が提供されます。

始める前に

以下のタスクが完了していることを確認します。

- Emulex アダプターのインストールの検証。
- ファイバー・チャンネル接続の検証。

手順

1. ご使用の QRadar コンソール アプライアンス上で、両方のファイバー・チャンネルのケーブルを Emulex LPe12002 ホスト・バス・アダプターに接続します。
2. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
3. 以下のコマンドを入力して、ストレージ・エリア・ネットワーク (SAN) パーティションを識別します。

```
blkid -o list
```

4. パーティションをフォーマットします。
 - ご使用のファイル・システムが ext4 の場合は、コマンド `mkfs.ext4 -L multiPath /dev/partition` を入力します。
 - ご使用のファイル・システムが XFS 場合は、コマンド `mkfs.xfs -L multiPath /dev/partition` を入力します。
5. 以下の各コマンドを指定の順序で入力して、QRadar サービスを停止します。

```
service systemStabMon stop  
service hostcontext stop  
service tomcat stop  
service imq stop  
service postgresql stop  
service hostservices stop
```

6. 以下のコマンドを入力して、ファイル・システムをアンマウントします。

```
umount /store/tmp  
umount /store/transient  
umount /store
```

7. 以下のコマンドを入力して、/store_old ディレクトリーを作成します。

```
mkdir /store_old
```

8. 以下のコマンドを入力して、デバイス・パーティションの Universally Unique Identifier (UUID) を判別します。

```
blkid /dev/partition
```

9. /etc/fstab ファイルを編集します。
 - a. 既存の /store ファイル・システム項目を /store_old システムへと置き換えます。
 - b. ファイル・システムが ext4 の場合は、次のテキストを追加します。

```
UUID=uuid /store ext4 defaults,noatime,nobarrier 1 2
```
 - c. ファイル・システムが XFS の場合は、次のテキストを追加します。

```
UUID=uuid /store xfs defaults,noatime,nobarrier 1 2
```

10. 以下のコマンドを入力して、ファイル・システムをマウントし、データをデバイスにコピーします。

```
mount /store
mount /store_old
cp -af /store_old/* /store
mount /store/tmp
umount /store_old
```

11. 以下の各コマンドを指定の順序で入力して、QRadar サービスを始動します。

```
service hostservices restart
service postgresql restart
service imq restart
service tomcat restart
service hostcontext restart
service systemStabMon restart
```

12. 以下のコマンドを入力して、ファイバー・チャンネルのマルチパスを使用可能にします。

```
mpathconf --enable
```

13. 以下のコマンドを入力して、マルチパス・デーモンを始動します。

```
service multipathd start
```

14. 以下のコマンドを入力して、システムを再始動します。

```
reboot
```

HA デプロイメント環境でのファイバー・チャンネルの構成

高可用性 (HA) 環境でファイバー・チャンネル・ストレージまたはマルチパスを使用する場合、管理者は、同じストレージ・パーティションを使用するようにプライマリー HA ホストとセカンダリー HA ホストを構成する必要があります。

このタスクについて

重要: HA の同期を開始する前に、プライマリー HA ホストとセカンダリー HA ホストの両方でマルチパスを構成する必要があります。

手順

1. 正しいファイバー・チャンネル・ハードウェアがセカンダリー HA にインストールされていることを検証します。詳しくは、23 ページの『Emulex アダプターのインストールの検証』を参照してください。
2. プライマリー HA ホスト上でファイバー・チャンネルを構成します。詳しくは、29 ページの『標準的な QRadar デプロイメント環境でのファイバー・チャンネルの構成』を参照してください。
3. HA ファイバー・チャンネル接続を検証します。詳しくは、24 ページの『ファイバー・チャンネル接続の検証』を参照してください。
4. セカンダリー HA ホストのファイル・システム・マウント・ポイントを構成します。
5. ファイバー・チャンネルにマルチパスが構成されている場合、ファイバー・チャンネルのマルチパス・サービスを有効にします。詳しくは、29 ページの『標準的な QRadar デプロイメント環境でのファイバー・チャンネルの構成』を参照してください。

重要: HA をファイバー・チャンネル構成に追加する前に、`/store/backup/` がローカルであることを確認してください。`/store/backup` へのリンクは、HA を追加した後にのみ作成してください。

セカンダリー HA ホストのマウント・ポイントの構成

マウント・ポイントを、ファイバー・チャンネル・ストレージ・デバイスに移動するファイル・システムのセカンダリー高可用性 (HA) ホスト上に構成する必要があります。

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。
2. 以下のコマンドを入力して UUID を取得します。

```
blkid /dev/partition
```

3. コマンド `partprobe` を入力して、ファイバー・チャンネル・パーティションのデータでカーネルを更新します。

トラブルシューティング: カーネルがパーティション・テーブルを読み取ることができないことを警告するエラー・メッセージが表示された場合は、コマンド `ls -l /dev/disk/by-uuid/UUID` を入力します。出力が表示されない場合には、`reboot` を入力してセカンダリー HA ホストを再始動します。

4. 以下のコマンドを入力して、ファイル・システムをアンマウントします。

```
umount /store/tmp
umount /store/transient
umount /store
```

`/store/transient` ファイル・システムがマウントされているのは、`/store` ファイル・システムが XFS であるときのみです。

5. `/store` ファイル・システムをオフボード・デバイスにリダイレクトしていた場合は、次のいずれかのオプションを選択して `/etc/fstab` ファイルを編集します。

- `/store` ファイル・システムが XFS ファイル・システムの場合、次の行を更新します。各行について、テキストをテキスト・エディターにコピーし、改行を削除して、単一の行として貼り付けます。

```
UUID=uuid /store xfs inode64,logbsize=256k,noatime,
noauto,nobarrier 0 0
```

```
UUID=uuid /store/transient xfs inode64,logbsize=256k,noatime
,noauto,nobarrier 0 0
```

```
UUID=uuid /store/tmp ext4 noatime,noauto,nobarrier 0 0
```

- `/store` ファイル・システムが ext4 の場合は、以下の行を更新します。

```
UUID=uuid /store ext4 defaults,noatime,noauto,nobarrier 1 2
```

6. `/store/ariel` ファイル・システムをオフボード・デバイスに移動する場合は、次のいずれかのオプションを選択して `/etc/fstab` ファイルを編集します。

- `/store/ariel` ファイル・システムが XFS ファイル・システムの場合、次の行を更新します。各行について、テキストをテキスト・エディターにコピーし、改行を削除して、単一の行として貼り付けます。

```
UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,  
noauto,nobarrier 0 0
```

```
UUID=uuid /store/transient xfs inode64,logbsize=256k,noatime  
,noauto,nobarrier 0 0
```

- /store/ariel ファイル・システムが ext4 の場合は、以下の行を更新します。

```
UUID=uuid /store/ariel ext4 defaults,noatime,noauto,nobarrier 1 2
```

次のタスク

HA クラスターを作成します。詳しくは、「*IBM Security QRadar 高可用性ガイド*」を参照してください。

第 4 章 NFS オフボード・ストレージ・デバイス

IBM Security QRadar データを外部ネットワーク・ファイル・システム (NFS) にバックアップできます。

PostgreSQL データベース、Ariel データベースなど、アクティブ・データを保管するために NFS は使用できません。NFS を使用すると、それが原因でデータベースが破損する場合やパフォーマンスの問題が発生する場合があります。

高可用性 (HA) デプロイメントによっては、QRadar バックアップ・ファイルの場所を変更し、この新しい場所で NFS 共有を構成する必要があります。

スタンドアロンの QRadar コンソールから NFS にバックアップ・ファイルを移動し、新しい HA デプロイメントを構成できます。また、バックアップ・ファイルを NFS に移動することや、既存の QRadar HA デプロイメントからバックアップ・ファイルを移動することができます。

NFS へのバックアップの移動

ネットワーク・ファイル・システム (NFS) は、スタンドアロンの QRadar コンソール、新規 QRadar HA デプロイメント環境、および既存の QRadar HA デプロイメント環境のそれぞれに合わせて構成できます。

このタスクについて

以下のいずれかのシチュエーションが該当する場合は、NFS サーバーへの接続を有効にする必要があります。

- スタンドアロンの QRadar コンソールから NFS に /store/backup ファイル・システムをマイグレーションする場合
- 新規 HA デプロイメント環境と既存の HA デプロイメント環境がある場合

以下のいずれかのシチュエーションが該当する場合は、NFS マウントを構成する必要があります。

- スタンドアロンの QRadar コンソールから NFS に /store/backup ファイル・システムをマイグレーションする場合。
- HA デプロイメント環境を初めて構成する場合、プライマリーとセカンダリーの HA ホスト上に /store/backup ファイル・システム用の NFS マウント・ポイントを構成する必要があります。

HA 環境で NFS ストレージを使用するには、同じ NFS 構成を使用してプライマリー HA ホストとセカンダリー HA ホストを構成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 にログインします。
2. ご使用の NFS サーバーを以下の形式で /etc/hosts ファイルに追加します。

IP address hostname

3. 以下の行を `/opt/qradar/conf/iptables.pre` ファイルに追加します。

```
-A INPUT -i interface -s IP address -j ACCEPT
```

専用の NFS ネットワークがある場合、*interface* は `ETH0` または `ETH1` です。

IP address は、ご使用の NFS サーバーの IP アドレスです。

4. 以下のコマンドを入力して、ファイアウォールの設定を更新します。

```
/opt/qradar/bin/iptables_update.pl
```

5. 以下のコマンドを入力し、NFS を始動ルーチンに追加してその構成の一部にします。

```
cd /etc/rc3.d  
chkconfig --level 3 nfs on  
chkconfig --level 3 nfslock on
```

6. 以下のコマンドを入力して、NFS サービスを開始します。

```
service nfslock start  
service nfs start
```

7. 以下の行を `/etc/fstab` ファイルに追加します。

```
hostname:shared_directory/store/backup nfs  
soft,intr,rw,clientaddr=IP address 0 0
```

ご使用の構成に合わせて NFS マウント・ポイントの設定を調整することが必要な場合があります。

例:

```
hostname:shared_directory/store/backup  
nfs soft,intr,rw,noac 0 0
```

8. 以下のコマンドを入力して、バックアップ・ファイルを既存のディレクトリーから一時的な場所に移動します。

```
cd /store/  
mv backup backup.local
```

9. 以下のコマンドを入力して、新しいバックアップ・ディレクトリーを作成します。

```
mkdir /store/backup
```

10. 以下のコマンドを入力して、NFS ボリュームに対する権限を設定します。

```
chown nobody:nobody /store/backup
```

11. 以下のコマンドを入力して、NFS ボリュームをマウントします。

```
mount /store/backup
```

`hostcontext` プロセスは `root` ユーザーとして実行されるため、マウントされている NFS ボリュームに対する読み取りアクセス権限と書き込みアクセス権限を `root` ユーザーが持っている必要があります。

12. 以下のコマンドを入力して、`/store/backup` がマウントされていることを検証します。

```
df- h
```

13. 以下のコマンドを入力して、バックアップ・ファイルを一時的な場所から NFS ボリュームに移動します。

```
mv /store/backup.local/* /store/backupHost/inbound/
```

14. 以下のコマンドを入力して backup.local ディレクトリーを削除します。

```
cd /store  
rm -rf backup.local
```

新しいバックアップの場所の構成

既存の高可用性クラスターがある場合には、プライマリー HA ホスト上の IBM Security QRadar のバックアップの場所を変更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 コンソールにログインします。
2. QRadar のバックアップを保管するためのファイルの場所を作成します。

制約事項: この新しいバックアップの場所は、/store ファイル・システムの下には作成しないでください。

3. 以下の行を /etc/fstab ファイルに追加します。

```
hostname:shared_directory backup location nfs  
soft,intr,rw,clientaddr=IP address 0 0
```

4. 以下のコマンドを入力して、この新しいバックアップ・ファイルの場所を NFS 共有にマウントします。

```
mount backup location
```

5. 以下のコマンドを入力して、既存のバックアップ・データを NFS 共有にコピーします。

```
mv /store/backup/* backup location
```

6. QRadar にログインします。
7. 「管理」タブをクリックします。
8. 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。
9. 「バックアップおよびリカバリー」をクリックします。
10. ツールバーで、「構成」をクリックします。
11. 「バックアップ・リポジトリー・パス」フィールドに QRadar V7.2.2 のバックアップ・ファイルを保管する場所を入力し、「保存」をクリックします。
12. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

セカンダリー HA ホストのマウント・ポイントの構成

既存のセカンダリー高可用性 (HA) ホスト上で、IBM Security QRadar のバックアップ・ファイル用の代替の場所のための NFS マウント・ポイントを構成する必要があります。

手順

1. SSH を使用して、QRadar のセカンダリー HA ホストに root ユーザーとしてログインします。
2. プライマリー HA ホスト上のバックアップ・ファイルの場所に対応するバックアップ・ファイルの場所を作成します。

詳しくは、37 ページの『新しいバックアップの場所の構成』を参照してください。

制約事項: この新しいバックアップの場所は、/store ファイル・システムの下には作成しないでください。

3. 以下の行を /etc/fstab ファイルに追加します。

```
hostname:shared_directory backup location nfs  
soft,intr,rw,clientaddr=IP address 0 0
```

4. 以下のコマンドを入力して、QRadar のバックアップ・ファイル用のこの新しい場所をマウントします。

```
mount backup location
```

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を提供し、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。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認できません。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をお願いします。

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ます、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](http://www.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。

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]

お客様サポート
連絡先情報 v

[カ行]

技術ライブラリー
場所 v

[サ行]

資料
技術ライブラリー v
ストレージ
オプション 3
拡張 3
制限 4
セカンダリー・ネットワーク・インターフェース
概要 7

[ナ行]

ネットワーク管理者
説明 v
ネットワーク・インターフェース
セカンダリー 7
ネットワーク・ファイル・システム
参照: NFS

[ハ行]

パフォーマンス
影響 2
標準的なデプロイメント環境
ファイバー・チャネル構成 30
iSCSI の構成 8
ファイバー・チャネル
概要 23
構成の概要 23
接続の検証 24
マウント・ポイントの検証 29
HA デプロイメント環境の概要 31

ファイル・システム
オフボード・ストレージへ移動 2
iSCSI ストレージ・ソリューションへの移動 11

[マ行]

マイグレーション
参照: 移動

E

Emulex アダプター
インストール 24

H

HA デプロイメント環境
ファイバー・チャネル 32
マウント・ポイントの構成 38

I

iSCSI
オフボード・ストレージ・オプション 7
接続の検証 18
標準的なデプロイメント環境の構成 8
ボリュームの構成 9
マウント 14
HA 環境での構成オプション 7
/store/ariel ファイル・システムの移動 28

N

NFS
新しいバックアップの場所の構成 37

[特殊文字]

/store ファイル・システム
iSCSI ストレージ・ソリューションへの移動 13



Printed in Japan