IBM Security QRadar Incident Forensics
バージョン 7.2.8

IBM QRadar Network Packet Capture 管理ガイド

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、 29 ページの『特記事項』に記載されている情報をお読みください。

この資料は、IBM QRadar Security Intelligence Platform V7.2.8 に適用されます。また、この資料の更新版が公開されない限り、これ以降のリリースにも適用されます。

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

原典： IBM Security QRadar Incident Forensics
Version 7.2.8
IBM QRadar Network Packet Capture Administration 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

QRadar Network Packet Capture 製品管理の概要

管理者は、IBM® QRadar® Network Packet Capture を使用してダッシュボードを管理します。

対象読者

このガイドは、ネットワーク・セキュリティーの調査と管理を担当するすべての QRadar Network Packet Capture ユーザーを対象としています。このガイドは、QRadar Network Packet Capture へのアクセス権限とご使用の企業ネットワークとネットワーキング・テクノロジーに関する知識をお持ちの方を想定して記述されています。

テクニカル・ドキュメント

QRadar 製品ライブラリーで IBM Security QRadar 製品資料を見つけるには、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

お客様サポートへのお問い合わせ

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

適切なセキュリティーの実践に関する注意事項

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

注意**:**

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポ

リシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar Network Packet Capture の管理

パケット・キャプチャーのタスクを実行するときは、管理者としてログインする必要があります。

QRadar Network Packet Capture ユーザー・アカウントおよび認証のセットアップ

IBM QRadar Network Packet Capture アプライアンスでのユーザー認証は 2 段階で行われます。ユーザーがログインするときには、ローカル環境で認証が実行されます。ユーザーは認証に失敗すると、構成済みの Active Directory または LDAP (Lightweight Directory Access Protocol) サーバーに照らして認証されます。両方のタイプの認証に失敗した場合、ユーザーにアクセス権限は付与されません。

注**:** QRadar Network Packet Capture アプライアンスが QRadar Network Packet Capture グループのメンバーである場合は、ユーザー・アカウントおよび認証の構成が自動的にグループ全体に同期されます。

新規ローカル・ユーザーの作成

ユーザー・ベースが小規模であり、認証プロバイダー (Active Directory や LDAP サーバーなど) が不要な場合は、IBM QRadar Network Packet Capture アプライアンスにアクセスする必要がある各ユーザーに対して、ローカル・ログイン・アカウントを作成します。

始める前に

管理者として QRadar Network Packet Capture アプライアンスにログインします。

QRadar Network Packet Capture ユニットは、Microsoft® Active Directory または LDAP サービスで指定されたユーザー認証も完全にサポートします (2 ページの『ユーザー認証のための Active Directory や LDAP サーバーの構成』を参照)。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「アカウント (ACCOUNTS)」ウィジェットに移動し、「ユーザー」フィールドおよび「パスワード」フィールドに新規ユーザーの値を入力します。
3. ユーザーのレベルを選択します。
   - 最も高いアクセス・レベルを必要とし、かつすべての構成を変更できる管理者の場合は、「管理者」を選択します。
   - 検索や照会などの操作で QRadar Network Packet Capture アプライアンスを使用する必要があるユーザーの場合は、「オペレーター (Operator)」を選択します。

- QRadar Network Packet Capture アプライアンスからの結果のモニターのみが必要なユーザーの場合は、「モニター」を選択します。

必要なユーザー・レベルを決定するには、以下の情報を使用してください。

操作	モニター・レベル	オペレーター・レベル	管理者レベル
デバイスから統計情報を取得する	X	X	X
現在のグループ設定に関する情報を取得する	X	X	X
ユニットからのデータの検索および照会を開始する		X	X
実行中の検索を取り消す		X	X
デバイスの構成 (ユーザー・アカウントの追加や削除など) を変更する			X
ユニットの統計情報をリセットまたは消去する			X
ログやサポート・アーカイブなどのサポート情報をデバイスから取得する			X
データのキャプチャーを開始および停止する			X
グループ設定を変更する			X

4. 「アカウントの追加 **(Add account)**」をクリックします。

ローカル・ユーザー・パスワードの変更

セキュリティー上の理由で、「アカウント (ACCOUNTS)」ウィジェットを使用して任意のユーザーのパスワードを変更することができます。

このタスクについて

パスワードを変更すると、ローカル・ユーザーを自動的にログアウトします。ユーザーは、新しいパスワードを使用して再度ログインする必要があります。管理者が自身のパスワードを変更するときも、再度ログインする必要があります。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「アカウント (ACCOUNTS)」ウィジェットに移動し、該当するユーザー名を「ユーザー」フィールドに入力します。
3. 新しいパスワードを「パスワード」フィールドに入力し、「アカウントの更新 **(Update Account)**」をクリックします。 確認メッセージが表示され、新しいパスワードが直ちに有効になります。

ユーザー認証のための Active Directory や LDAP サーバーの構成

既存の認証プロバイダーを使用することによって、IBM QRadar Network Packet Capture がご使用のセキュリティー・インフラストラクチャーに統合します。「認

証および許可 (AUTHENTICATION AND AUTHORIZATION)」ウィジェットを使用して、Active Directory および LDAP を構成します。QRadar Network Packet Capture は、Microsoft® Active Directory サービスまたは LDAP サーバーで指定されたユーザー認証を完全にサポートします。デフォルトでは、認証ソースとしての Microsoft® Active Directory サーバーおよび LDAP サーバーは無効になっています。

始める前に

管理者として QRadar Network Packet Capture ユニットにログインします。

手順

1. 「管理」タブをクリックして「認証および許可 (AUTHENTICATION AND AUTHORIZATION)」ウィジェットに移動します。
2. 該当する「サーバー・タイプ」を選択して「適用」をクリックします。 構成するパラメーターは、認証サーバーのタイプによって異なります。

   注**:** ユーザーが認証を要求したときにプライマリーの認証および許可サーバーにアクセスできない場合は、DNS 名に照らしてサービス・レコード (SRV) ルックアップが実行されます。解決された SRV IP アドレスのリストはセカンダリー認証サーバーとして使用されます。

   重要**:** 「Active Directory」を有効にする場合は、ユーザー名を完全修飾ドメイン名にしなければなりません (¥¥[domain]¥[user name] や [user name]@[domain] など)。

   以下の表を使用して、適切な「サーバー・タイプ」を選択して構成してください。

パラメーター	サーバー・タイプ	説明	デフォルト
Active Directory または LDAP サーバーと通信するためのプロトコル (Protocol for communicating with the Active Directory or LDAP server)	すべて	プロトコルおよび暗号化方式。指定可能な値: • LDAP • LDAP + TLS • LDAP + SSL	LDAP
Active Directory または LDAP サーバーのホスト名または IP アドレス (Host name or IP address of the Active Directory or LDAP server)	すべて		N/A

パラメーター	サーバー・タイプ	説明	デフォルト
Active Directory または LDAP サーバーに接続するポート番号 (Port number to connect to on the Active Directory or LDAP server)	すべて		389
Active Directory または LDAP サーバーへの接続のタイムアウト (秒) (Timeout in seconds of the connection to the Active Directory or LDAP server)	すべて		25 秒
基本ドメイン名 (Base Domain Name)	すべて	照会を開始する場所の識別名。	N/A
管理者レベルのグループ (Administrator level group)	すべて	管理者レベルの特権を識別するために使用するグループの名前	N/A
オペレーター・レベルのグループ (Operator level group)	すべて	オペレーター・レベルの特権を識別するために使用するグループの名前	N/A
モニター・レベルのグループ (Monitor level group)	すべて	モニター・レベルの特権を識別するために使用するグループの名前	N/A
フィルター	LDAP	項目が満たさなければならない条件	N/A
フィルターの有効範囲 (Scope of the filter)	LDAP	指定可能な値: • ベース • 1 レベル (One Level) • サブツリー (Subtree)	サブツリー (Subtree)
ユーザーへのグループの割り当てに使用する属性名 (Attribute name used for assigning groups to users)	LDAP	グループ名を含む、返されるオブジェクト属性の名前。	

始動時のデータ整合性検査

IBM QRadar Network Packet Capture アプライアンスの始動時に、保管されているデータの完全性および整合性が検査されます。

QRadar Network Packet Capture にログインすると、サービスの初期化中であることを示すメッセージが表示されます。ウィンドウ上部のステータス・バーに初期化の進行状況が表示されます。

整合性検査の所要時間は、QRadar Network Packet Capture アプライアンスに保管されているデータの量によって異なります。

日時の構成 (NTP)

キャプチャーされたデータに正しいタイム・スタンプが設定されるように、QRadar Network Packet Capture が使用する日時を構成する必要があります。QRadar Network Packet Capture に対してローカル日時を構成するか、NTP (Network Time Protocol) や PTP (Precision Time protocol) によって外部ソースの日時と同期させることができます。

始める前に

PTP ケーブルが QRadar Network Packet Capture ユニットに接続されていないことを確認してください。

手順

1. 「管理」タブをクリックして「NTP セットアップ (NTP SETUP)」ウィジェットに移動します。

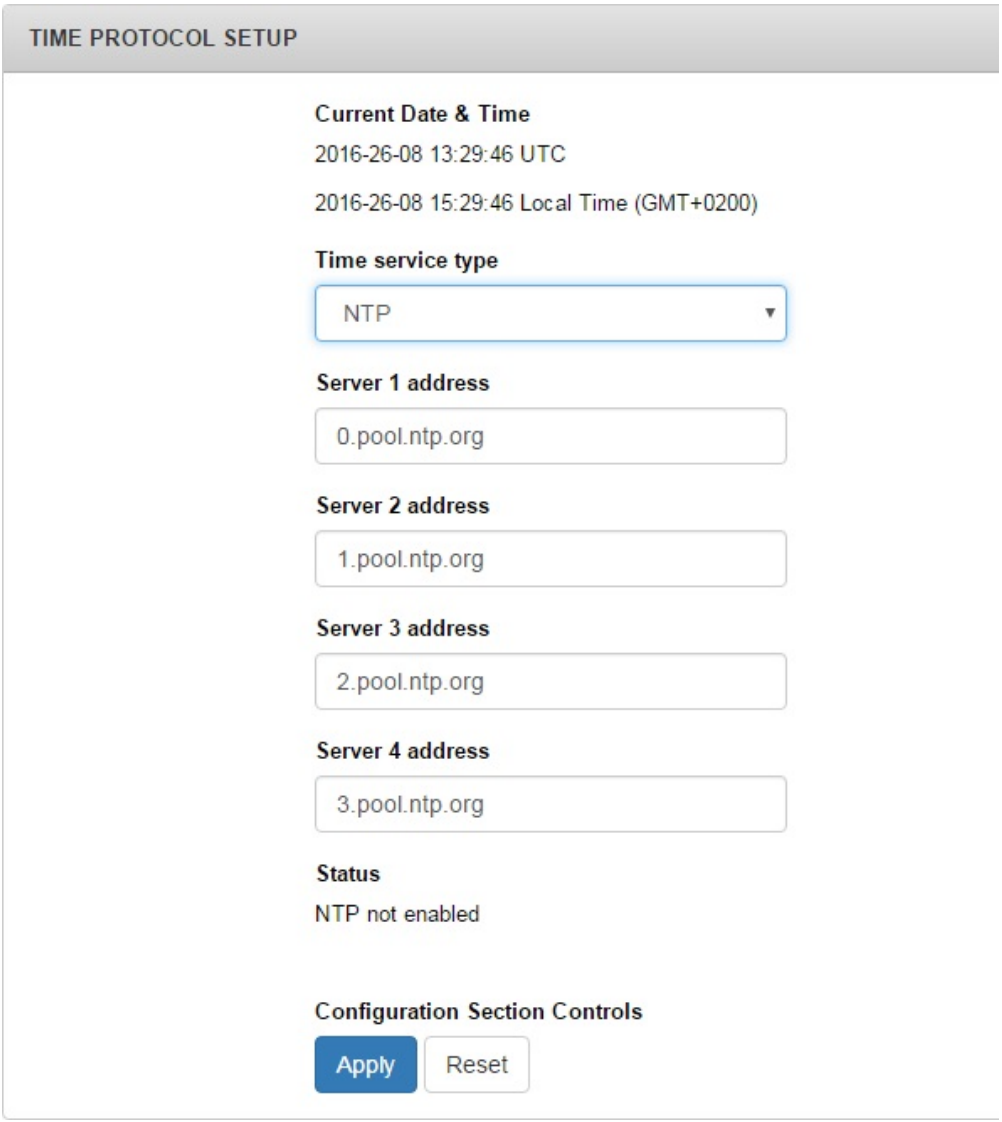


図 *1.* 「時刻プロトコルのセットアップ *(Time Protocol Setup)*」ウィジェット

2. ローカル日時を構成するには、「日時 **(Date & Time)**」フィールドに示されている形式で日時を入力します。
3. 日時を外部サーバーと同期させるには、「**NTP** 対応 **(NTP enabled)**」のデバイスを選択し、日時ソースとして適切なサーバー・アドレスを選択します。
4. 「適用」をクリックして完了します。

タスクの結果

QRadar Network Packet Capture のアクセラレーターの時刻が自動的にオペレーティング・システムの時刻に同期します。

ロケーション名および連絡先の構成

QRadar Network Packet Capture アプライアンスを識別しやすくするために、認識可能な名前を付けてください。

手順

1. 「管理」タブをクリックします。
2. 「一般設定 (GENERAL SETUP)」ウィジェット (以下の図) までスクロールダウンします。

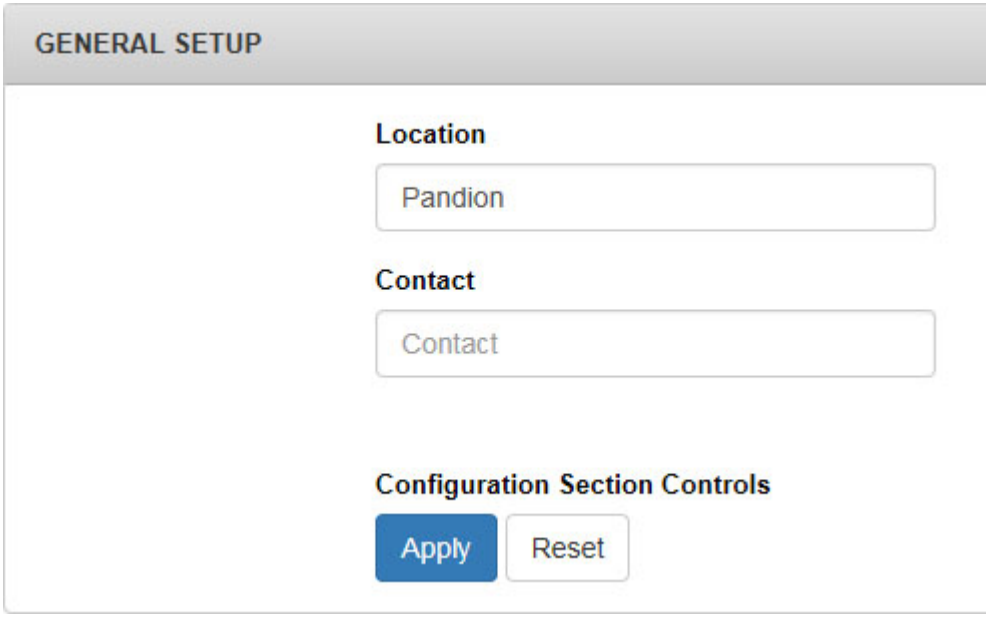


図 2. 「一般設定 *(General Setup)*」ウィジェット

3. ロケーション名を入力し、オプションで連絡先担当者の名前を入力します。
4. 「**Apply**」をクリックします。

パケット・キャプチャーの開始または停止

アプライアンス・キャプチャーの記録数を制御できます。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「制御 (CONTROL)」ウィジェットに移動します。
3. 「トラフィックのキャプチャー **(Traffic Capture)**」を「オンにする **(Turn On)**」または「オフにする **(Turn Off)**」に設定します。

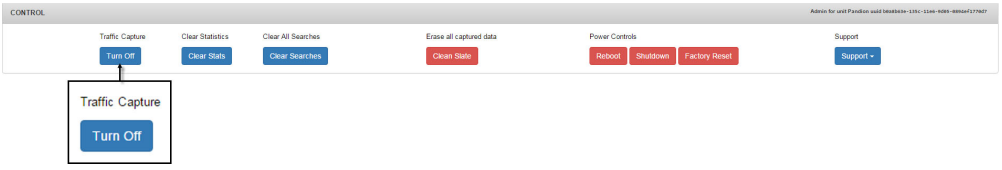


図 3. トラフィックのキャプチャー *(Traffic Capture)*

デフォルトではパケットのキャプチャーがオンになっています。QRadar Network Packet Capture がパケットをキャプチャーしていない場合は、「トラフィックのキャプチャー **(Traffic Capture)**」が「オンにする **(Turn On)**」に設

定されています。QRadar Network Packet Capture がパケットをキャプチャーしている場合は、「トラフィックのキャプチャー **(Traffic Capture)**」が「オフにする **(Turn Off)**」に設定されています。

リモート syslog 設定の構成

リモート・システムのロギングを有効にしてプロトコルの詳細を構成するには、「リモート Syslog の設定 (REMOTE SYSLOG SETUP」ウィジェットを使用します。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「リモート Syslog の設定 (REMOTE SYSLOG SETUP)」ウィジェットに移動します。
3. 「リモート **Syslog** が有効 **(Remote Syslog Enabled)**」チェック・ボックスを選択してシステム・ロギングを有効にします。

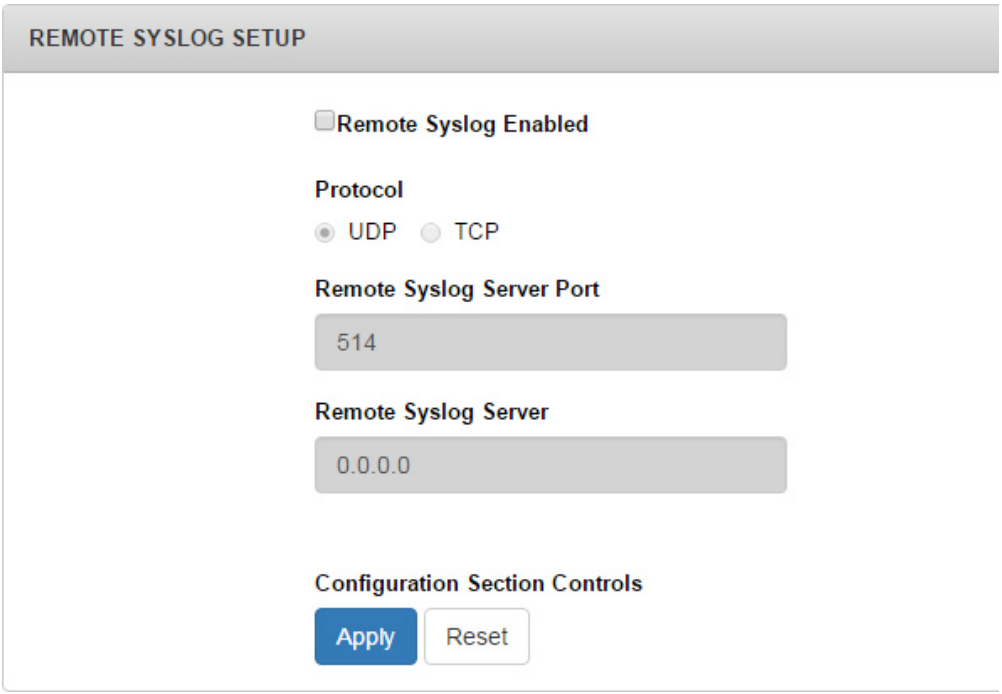


図 4. リモート *Syslog* の設定 *(Remote Syslog Setup)*

4. 使用する設定に応じて「**UDP**」または「**TCP**」のプロトコルにチェック・マークを付けます。
5. 「リモート **Syslog** サーバーのポート **(Remote Syslog Server Port)**」フィールドにポート番号を指定し、「リモート **Syslog** サーバー **(Remote Syslog Server)**」フィールドに IP アドレスを指定します。
6. 「**Apply**」をクリックします。

syslog の表示

デバイスのトラブルシューティングを行うには「syslog (SYSLOGS)」を使用します。

デフォルトでは、IBM QRadar Network Packet Capture アプライアンスの syslog のうち最後の 500 行が「syslog (SYSLOGS)」ウィジェットに表示されます。

表示する行をフィルターに掛けたり行数を調整したりするには、「**syslog** のレベル **(Syslog Level)**」および「ログ行数 **(Log Lines)**」のコントロールを使用します。

X509 の構成

「X509 セットアップ (X509 SETUP)」ウィジェットを使用して、新しい X509 証明書をインストールします。この証明書は、HTTPS で IBM QRadar Network Packet Capture アプライアンスを認証するために使用されます。

ユーザーによってインストールされた証明書が存在しない場合は、出荷時にインストール済みの、デバイスごとに固有の証明書が使用されます。この証明書は自己署名されます。

アクセラレーターの構成

「アクセラレーターのセットアップ (ACCELERATOR SETUP)」ウィジェットを使用して、アクセラレーターのポート設定、パケット処理、およびプレフィルターを構成します。

ポートの設定

ポートに SFP モジュールまたは SFP+ モジュールがインストールされている場合、このモジュールはデフォルトで有効になっています。「アクセラレーターのセットアップ (ACCELERATOR SETUP)」ウィジェットで、このモジュールを手動で無効にすることができます。デフォルトでは、各ポートがモジュールの速度を自動的に検出します。ただし、デュアル・レート・モジュールを使用している場合、ラジオ・ボタンを使用して手動で速度を 1G または 10G に設定できます。

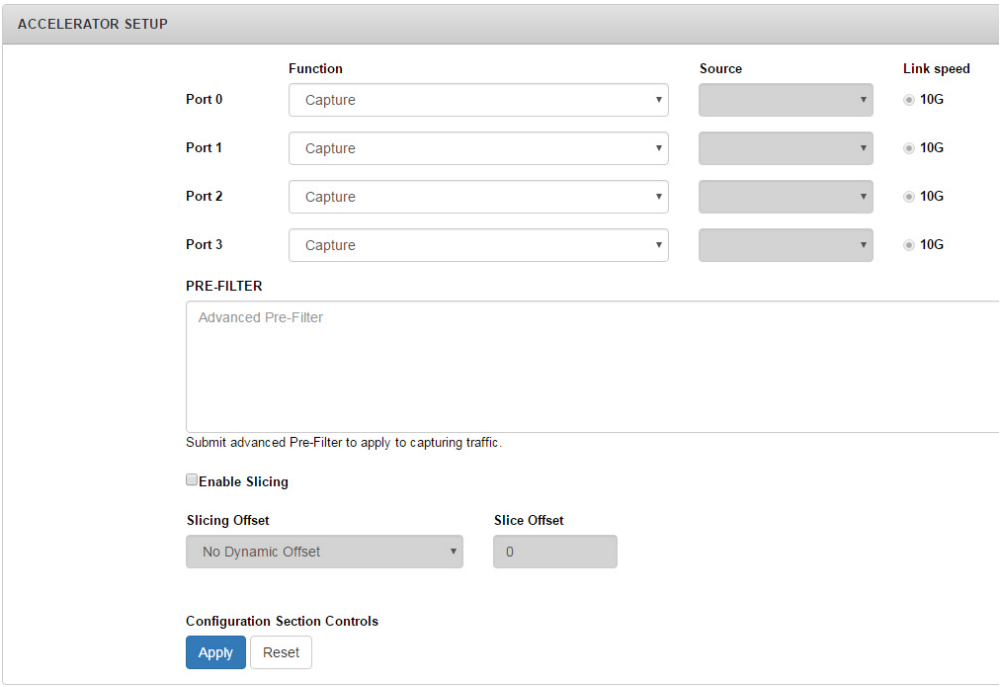


図 5. アクセラレーターのセットアップ *(Accelerator Setup)*

プレフィルターの構成

キャプチャーして保管するパケットのサイズを削減するために、「アクセラレーターのセットアップ (ACCELERATOR SETUP)」ウィジェットを使用して、キャプチャーするパケットをフィルターに掛けます。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「アクセラレーターのセットアップ (ACCELERATOR SETUP)」ウィジェットに移動します。
3. プレフィルターの構成:
   a. 「プレフィルター **(PRE-FILTER)**」フィールドにステートメントを入力します。
   b. 「**Apply**」をクリックします。
4. パケット処理のセットアップ:
   a. 「プレフィルター **(PRE-FILTER)**」フィールドにステートメントを入力します。
   b. 「スライス処理の有効化 **(Enable Slicing)**」を選択し、オフセットを設定してスライス処理を有効にします。 スライス処理のオフセットは、動的なオフセットと静的なオフセットの和として、すべてのパケットがスライスされるように構成します。
   c. 「**Apply**」をクリックします。

統計や検索の消去

実行中およびキューに入れられたすべての検索を消去するには、「制御 (CONTROL)」ウィジェットを使用します。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「制御 (CONTROL)」ウィジェットに移動します。
3. ヒストリカル・データを消去する場合は、「統計の消去 **(Clear Statistics)**」を「統計情報の消去 **(Clear Stats)**」に設定します。
4. 最近の検索をすべて消去する場合は、「検索をすべて消去 **(Clear All Searches)**」を「検索の消去 **(Clear Searches)**」に設定します。

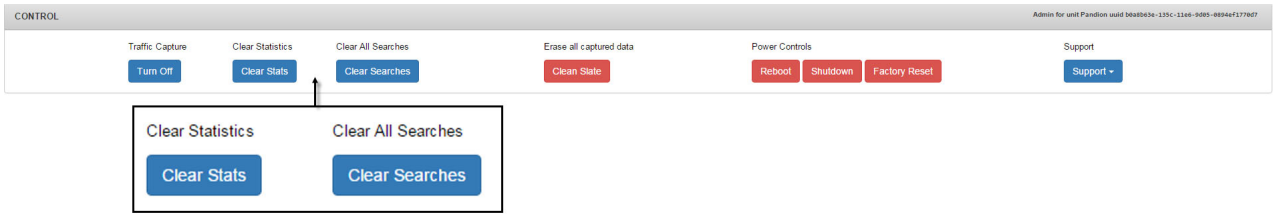


図 *6.* 統計または検索を消去します。

QRadar Network Packet Capture の再始動と工場出荷時の状態へのリセット

「制御 **(CONTROL)**」ウィジェットを使用して、IBM QRadar Network Packet Capture の電源設定にアクセスします。

手順

1. QRadar Network Packet Capture アプライアンスを再始動またはシャットダウンするには、以下のようにします。
   a. QRadar Network Packet Capture の「管理」タブをクリックします。
   b. 「制御 (CONTROL)」ウィジェットに移動します。
   c. 「電源制御 **(Power Controls)**」を「リブート **(Reboot)**」または「シャットダウン」に設定します。

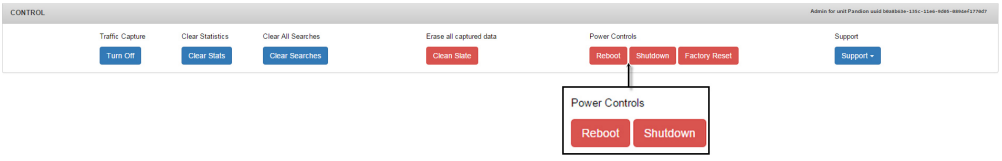


図 *7.* 電源制御 *(Power Controls)*

2. パケットをすべて消去して工場出荷時の状態にリセットするには、以下のようにします。

a. QRadar Network Packet Capture の「管理」タブをクリックします。
b. 「制御 (CONTROL)」ウィジェットに移動します。
c. ディスクを消去する場合は、「キャプチャーしたデータをすべて消去 **(Clear all captured data)**」を「完全消去 **(Clean Slate)**」に設定します。QRadar Network Packet Captureアプライアンスをリセットする場合は、「電源制御 **(Power controls)**」を「工場出荷時の状態にリセット **(Factory Reset)**」に設定します。

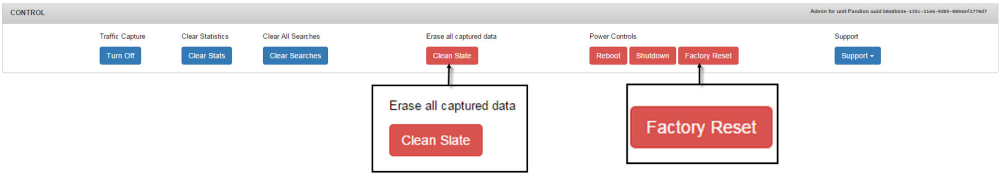


図 *8.* 電源制御 *(Power Controls)*

注**:** 「工場出荷時の状態にリセット **(Factory Reset)**」を実行すると、ネットワーク構成以外のすべての設定がリセットされます。キャプチャーされたデータはすべて消去されます。

第 2 章 QRadar Network Packet Capture およびパケット・キャプチャーのモニター

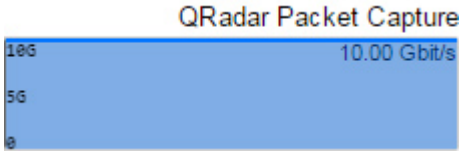
グループ内の 1 つ以上の IBM QRadar Network Packet Capture アプライアンスの全体的な状況を確認するには、「ダッシュボード」の「モニター (Monitoring)」ウィジェットを使用します。

QRadar Network Packet Capture グループは物理的に個別のアプライアンスから構成され、各アプライアンスが個別のネットワーク・タップからデータをキャプチャーします。グループ化の機能を使用して 1 つの論理エンティティーを形成すると、管理や検索が容易になります。1 つのグループには最大で 8 つの QRadar Network Packet Capture アプライアンスを組み込むことができます。

グループ・ビュー (GROUP VIEW)

各 QRadar Network Packet Capture アプライアンスは以下のモニター・コンポーネントから構成されています。

表 1. モニター・コンポーネント

アイコン	説明
	アクセラレーター
	システム
	ストレージ
	トラフィック

コンポーネントの状態は色 (明るいグレー、黄色、および赤) によって示されます。

グループ・リスト・ビュー (GROUP LIST VIEW)

グループ内の各 QRadar Network Packet Capture アプライアンスの正常性をモニターする際は、「グループ・リスト・ビュー (GROUP LIST VIEW)」ウィジェットを使用します。

ユニット・ビュー (UNIT VIEW)

「グループ・ビュー (GROUP VIEW)」ウィジェットで選択した IBM QRadar Network Packet Capture アプライアンスに関する詳細情報を表示する際は、「ユニット・ビュー (UNIT VIEW)」を使用します。

「ユニット・ビュー (UNIT VIEW)」は、QRadar Network Packet Capture アプライアンスの保有期間および正常性に関する概要情報を表示します。

アクセラレーター、システム、およびストレージについての詳細情報が表示されます。

CPU 使用率 (CPU UTILIZATION)

各ハイパースレッド・コアの CPU 使用率を個別にモニターする際は、「CPU 使用率 (CPU UTILIZATION)」ウィジェットを使用します。表示される CPU モデルおよび速度を使用して CPU を識別します。

トラフィック

QRadar Network Packet Capture アプライアンスによって受信されたパケット・キャプチャー・トラフィックの履歴をモニターする際は、「トラフィック」ウィジェットを使用します。

グラフは定期的に更新されます。ヒストリカル・データの最後の期間のみを表示するには、右にスクロールしてください。

パケットの分布 (PACKET DISTRIBUTION)

最後に統計データをリセットしてから IBM QRadar Network Packet Capture アプライアンスによって受信されたブロードキャスト・フレーム、マルチキャスト・フレーム、およびユニキャスト・フレームの分布をモニターする際は、「パケットの分布 (PACKET DISTRIBUTION)」ウィジェットを使用します。

パケット・サイズの分布 (PACKET SIZE DISTRIBUTION)

最後に統計データをリセットしてから QRadar Network Packet Capture アプライアンスによって受信されたフレームのパケット・サイズの分布をモニターする際は、「パケット・サイズの分布 (PACKET SIZE DISTRIBUTION)」ウィジェットを使用します。

第 3 章 QRadar Network Packet Capture の検索と照会

特定の時刻範囲内かつ特定のポートからの特定のパケットを検索するには、「検索」タブを使用します。送信元 IP、宛先 IP、ソース・ポート、宛先ポート、またはプロトコルの各フィールドを組み合わせて指定すると、QRadar Network Packet Capture 照会言語 (NTQL) ストリングが生成されます。NTQL ストリングを変更したり、独自の NTQL 式を新規に作成したりすることができます。

検索結果の制限

検索結果を制限して検索の結果が配信されるまでの時間を短縮するには、以下のいずれかのフィルターを使用して検索に有効範囲を追加します。

- 時間間隔 (Time Interval)
- 受信ポート (Receive Ports) (選択済みのポート)

QRadar Network Packet Capture アプライアンスのグループに対して検索を実行する場合は、必ずローカル・アプライアンスにログオンしているときにのみ、検索照会を実行するようにしてください。そうしないと、検索結果の取得パフォーマンスが低下します。

検索出力の形式は標準の PCAP 形式または PCAP-NG 形式です。QRadar Network Packet Capture アプライアンスのグループ全体にわたって検索するときであっても、PCAP-NG 形式の場合はポート番号の情報が入ります。トラフィックを検索する際は、グループ内のサーバーごとに受信ポートを指定することもできます。

検索を送信する前に検索エンジンがビジー状態である場合は、その検索をキューに入れることができます。検索が完了したらすぐに出力を自動的にダウンロードするかどうかを選択できるほか、複数の検索に優先順位を付けることができます。

NTQL と BPF の違い

キャプチャー時に作成された索引に基づいて検索を高速化するには、NTQL を使用します。

NTQL フィルターの動作は BPF (Berkeley Packet Filters) とは異なります。NTQL フィルターの動作を以下の例に示します。

- IP アドレスを検索する場合は、VLAN、MPLS、ISL のタグ付けやカプセル化にかかわらず、その IP アドレスを持つすべてのパケットが返されます。
- 特定の TCP ポートまたは UDP ポートを検索したときに返される結果には、拡張ヘッダーを持つ IPv6 パケットが含まれます。

BPF ポストフィルターは、完全な BPF 構文に基づいています。BPF 式を作成すると、指定された NTQL フィルターを通過したパケットのみを BPF ポストフィルターがフィルターに掛けます。

BPF フィルターの動作は NTQL とは異なるため、NTQL フィルターによって検出されたパケットが削除される可能性があります。

関連概念:

19 ページの『NTQL』

23 ページの『第 4 章 グループ化した QRadar Network Packet Capture アプライアンス』

キュー待機検索

実行する検索が複数ある場合は、キュー待機検索を使用します。

処理される検索は一度に 1 つだけですが、複数の検索を実行することができます。この場合は検索がキューに入れられ、優先順位に従って実行されます。キューに入れられた検索は「検索キュー (SEARCH QUEUE)」ウィジェットに表示されます。

以下の図は、キューに入れられた状態にあり、優先順位に従って実行される検索照会を示しています。

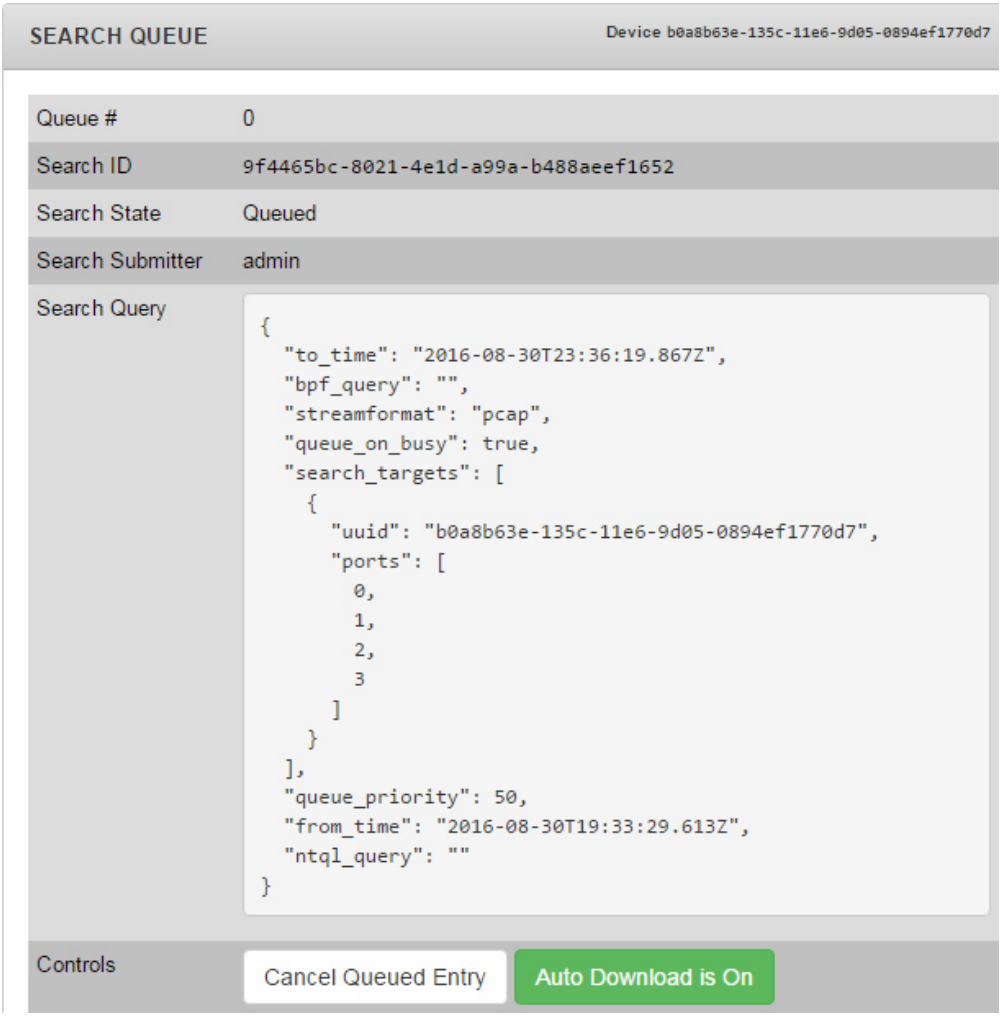


図 9. 「検索キュー *(SEARCH QUEUE)*」ウィジェット。

検索を送信する前に「ストリームの準備ができたら自動的にダウンロード **(Auto-download when ready to stream)**」オプションにチェック・マークを付けます。検索が完了すると、自動的に検索結果がダウンロードされます。「自動ダウンロードがオン **(Auto Download is On)**」をクリックすると、この動作を変更できます。

アクティブな検索

アクティブかつ処理中の検索をすべて表示するには、「アクティブな検索 (ACTIVE SEARCH)」ウィジェットを使用します。

アクティブな検索の照会を以下の図に示します。

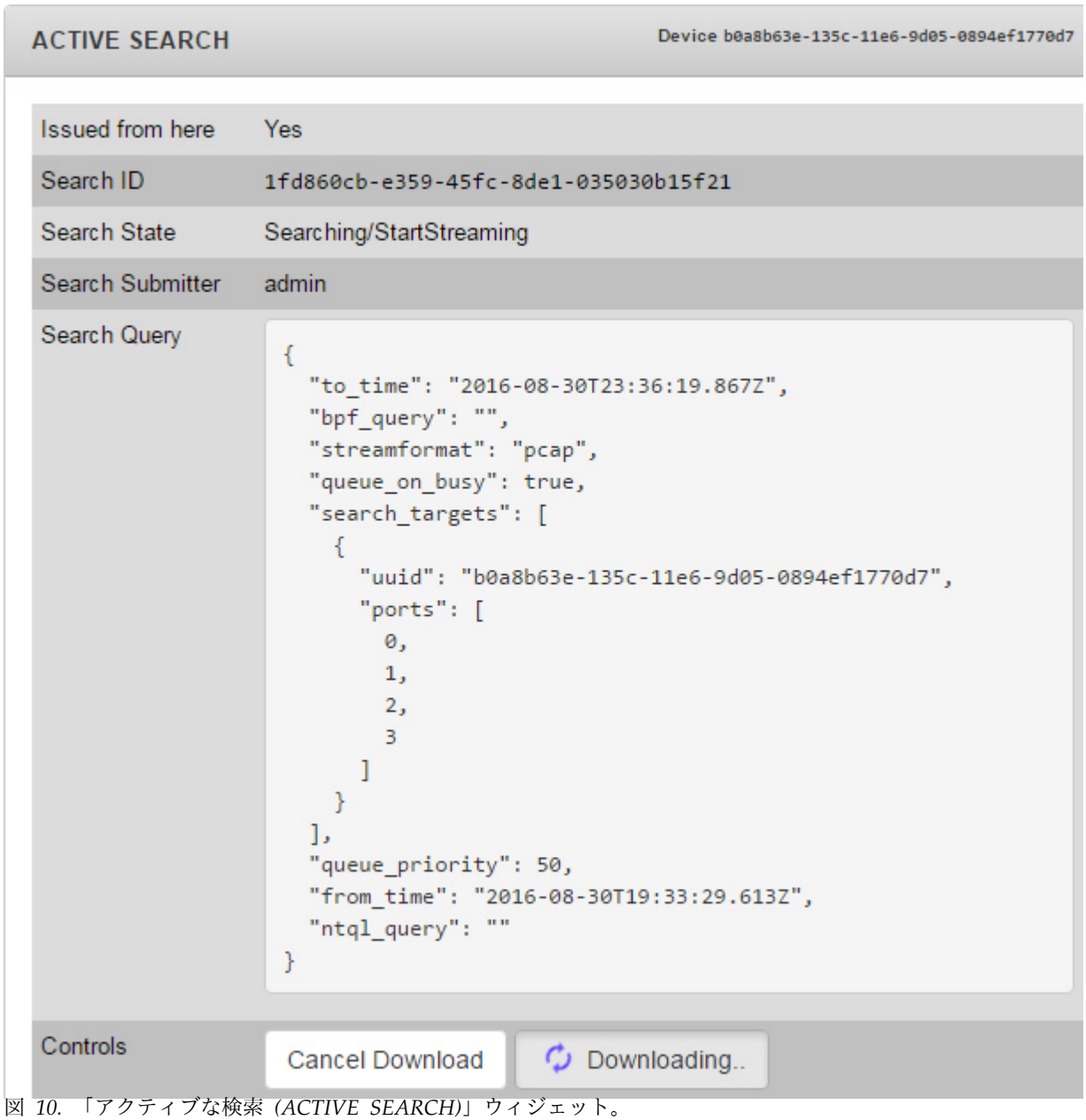


図 *10.* 「アクティブな検索 *(ACTIVE SEARCH)*」ウィジェット。

検索履歴 (SEARCH HISTORY)

IBM QRadar Network Packet Capture アプライアンスでの検索履歴を表示するには、「検索履歴 (SEARCH HISTORY)」ウィジェットを使用します。

完了した検索照会の検索履歴を以下の図に示します。

図 *11.* 「検索履歴 *(SEARCH HISTORY)*」ウィジェット。

検索テンプレート

「検索履歴 (SEARCH HISTORY)」ウィジェットを使用すると、以前に実行した検索を次の検索のテンプレートとして使用できます。「検索テンプレートとして使用 **(Use as Search Template)**」をクリックしてから「検索」ウィジェットに移動し、テンプレートに必要な変更を加えます。

検索の削除

アクティブな検索を停止したり、キューに入っている検索を削除したりするには、「検索キュー (SEARCH QUEUE)」ウィジェットまたは「アクティブな検索 (ACTIVE SEARCH)」ウィジェットで「チケットの削除 **(Delete ticket)**」をクリックします。

NTQL

キャプチャーしたパケットからデータを取り出すには、QRadar Network Packet Capture 照会言語 (NTQL) を使用します。例えば、以下の種類の情報に NTQL を使用できます。

- IPv4 ホスト・アドレス (送信元、宛先、または両方)
- IPv6 ホスト・アドレス (送信元、宛先、または両方)
- TCP ポート番号または UDP ポート番号 (送信元、宛先、または両方)
- イーサネット・フレームによって使用されるレイヤー 3 プロトコル
- IP パッケージによって使用されるレイヤー 4 プロトコル
- 上記のものを論理 AND および OR で組み合わせたもの

全件一致

空の NTQL ストリングはすべてのパケットに一致するため、一致件数が制限される場合に便利です。

ホスト・アドレスの検索

特定のホストとの間で送受信されたパケットを検索するには、以下のストリングを入力します。

```
src host <IP_address>
```

ホストに送信されたパケットを検索するには、以下のストリングを入力します。

```
dst host <IP_address>
```

ポート番号の検索

TCP ポートまたは UDP ポートとの間で送受信されたパケットを検索するには、以下のストリングを入力します。

```
port <number>
```

ポート番号のないプロトコルを使用して送信されたパケットは、この検索では破棄されます。

検索結果を特定のポートから送信されたパケットに絞り込むには、以下のストリングを入力します。

```
src port <number>
```

特定のポートに送信されたパケットを検索するには、以下のストリングを入力します。

```
dst port <number>
```

レイヤー 3 プロトコルの検索

特定のレイヤー 3 プロトコルを使用したパケットを検索するには、以下のストリングを入力します。

`l3proto <protocol>`

ここで、*<protocol>* はプロトコルの番号または名前です。サポートされているプロトコル名は以下のとおりです。

- `ip`
- `ip4`
- `ipv4`
- `arp`
- `ip6`
- `ipv6`
- `lldp`
- `ptp`

プロトコルとして `ip` を指定すると、IPv4 が使用されます。

レイヤー 4 プロトコルの検索

特定のレイヤー 4 プロトコルを使用したパケットを検索するには、以下のストリングを入力します。

`l4proto <protocol>`

ここで、*<protocol>* はプロトコルの番号または名前です。サポートされている名前は以下のとおりです。

3pc、ah、argus、aris、ax.25、bbn-rcc-mon、bna、br-sat-mon、cbt、cftp、chaos
compaq-peer、cphb、cpnx、crtp、crudp、dccp、dcn-
meas、ddp、ddx、dgp、egp、eigrp
emcon、encap、esp、etherip、fc、fire、ggp、gmtp、gre、hip、hmp、hopopt、i-
nlsp、iatp icmp、idpr、idpr-cmtp、idrp、ifmp、igmp、igp、il、ip-in-
ip、ipcomp、ipcu、ipip、iplt、ippc、iptm、ipv6、ipv6-frag、ipv6-icmp、ipv6-
nonxt、ipv6-opts、ipv6-route、ipx-in-ip、irtp、iso-ip、iso-
tp4、kryptolan、l2tp、larp、leaf-1、leaf-2、manet、merit-inp、mfe-nsp
mhrp、micp、mobile、mobility header、mpls-in-
ip、mtp、mux、narp、netblt、nsfnet-igp、nvp-ii
ospf、pgm、pim、pipe、pnni、prm、ptp、pup、pvp、qnx、rdp、rohc、rsvp、rsvp-
e2e-ignore、rvd、sat-expak、sat-mon、scc-sp、scps、sctp、sdrp、secure-
vmtp、shim6、skip、sm、smp、snp、sprite-rpc
sps、srp、sscopmce、st、stp、sun-nd、swipe、tcf、tcp、tlsp、trunk-1、trunk-
2、ttp、udp、udplite uti、vines、visa、vmtp、vrrp、wb-expak、wb-
mon、wesp、wsn、xnet、xns-idp

検索語の結合

検索語を AND および OR のキーワードで結合すると、より複雑な式を記述できます。例えば、1.1.1.1 または 2.2.2.2 との間で送受信されたパケットを検索するには、以下のストリングを入力します。

```
host 1.1.1.1 or host 2.2.2.2
```

1.1.1.1 または 2.2.2.2 との間で送受信されたパケットを検索するには、以下のストリングを入力します。

```
host 1.1.1.1 and host 2.2.2.2
```

これらのキーワードは左結合です。例として以下の構文について考えます。

```
port 42 and host 1.1.1.1 or host 2.2.2.2
```

この式は以下のように評価されます。

- ポート 42 との間かつホスト 1.1.1.1 との間で送受信された、または
- ポート番号にかかわらずホスト 2.2.2.2 との間で送受信されたパケット

以下の例に示すように、括弧を使用してこの左結合を変更することができます。

```
port 42 and (host 1.1.1.1 or host 2.2.2.2)
```

この式を評価させると、ポート 42 との間で送受信され、かつホスト 1.1.1.1 または 2.2.2.2 との間で送受信されたパケットが検索されます。

関連概念:

15 ページの『第 3 章 QRadar Network Packet Capture の検索と照会』

第 4 章 グループ化した QRadar Network Packet Capture アプライアンス

管理や検索操作のために、複数の物理アプライアンスをグループ化して単一の論理エンティティーを形成するには、IBM QRadar Network Packet Capture のグループ化機能を使用します。グループ化機能を使用すると、複数のタップ・ポイントおよび複数の QRadar Network Packet Capture アプライアンスに対して、1 つのアプライアンスであるかのようにアクセスおよび操作できます。

QRadar Network Packet Capture グループは、個別のネットワーク・タップからデータをキャプチャーできます。管理ネットワーク・インターフェースで、すべての QRadar Network Packet Capture グループ・メンバーにアクセスするように、すべての QRadar Network Packet Capture アプライアンスを構成する必要があります。また、ネットワークに DNS サーバーを用意する必要があります。

QRadar Network Packet Capture アプライアンスをグループ化すると、1 回のデータ照会でグループ・メンバーのすべてのデータを検索できるようになります。検索結果は単一の PCAP ファイルであり、すべてのグループ・メンバーからのデータがマージされて格納されます。

いずれかのメンバーにログインするだけでグループ全体にアクセスできます。この 1 個所でのログインから、QRadar Network Packet Capture グループの他のすべてのメンバーとプロキシーによって通信できます。

プロキシー機能は、主にリモート・アプライアンスの管理、構成、およびデバッグを目的としています。ユーザーがプロキシー方式を介してリモートの QRadar Network Packet Capture 上にいるときにグループ全体にわたる検索を開始すると、冗長なトラフィックが管理ネットワーク全体で大量に送信されます。管理ネットワークの帯域幅や待ち時間によっては、このことが検索のパフォーマンスに影響します。したがって、QRadar Network Packet Capture グループにわたる検索は、ハブやプロキシーを使用せずに、必ずプライマリー・マシンまたはローカル・マシンで開始してください。

関連概念:

15 ページの『第 3 章 QRadar Network Packet Capture の検索と照会』

グループ・アクセス

グループ内の IBM QRadar Network Packet Capture アプライアンスにアクセスしているときに、一部の機能の動作が異なります。相違点は以下のとおりです。

- 「ダッシュボード」タブの「グループ・ビュー (GROUP VIEW)」ウィジェットに複数の QRadar Network Packet Capture アプライアンス (グループ) が表示されます。
- 「切り替え先」ボタンは、「ダッシュボード」の「グループ・ビュー (GROUP VIEW)」におけるアプライアンス切り替えに対応します。

- ユーザー・アカウントを変更して Active Directory をセットアップすると、更新内容が自動的にすべてのグループ・メンバーに伝搬します。

グループの作成および変更

初期ピアツーピア・グループ

IBM QRadar Network Packet Capture アプライアンスでグループ化要求を開始するには、GUI または REST API のいずれかを使用します。

以下の例では、グループの作成を要求する QRadar Network Packet Capture アプライアンスをアプライアンス A とし、グループ化要求を受け取るアプライアンスをアプライアンス B とします。

例えば、QRadar Network Packet Capture グループを 2 つのメンバーで構成するとします。以下の処理が発生します。

- グループ化要求の一環として、アプライアンス B のための管理者レベルのアクセス権限を持つユーザー名およびパスワードを用意する必要があります。
- ローカル・アカウントのリストおよび Active Directory の構成をアプライアンス A からアプライアンス B にエクスポートします。アプライアンス B の以前のアカウントの構成および Active Directory 構成はすべて上書きされます。
- アプライアンス A とアプライアンス B の両方のキャプチャー・データはすべて保持され、どちらのアプライアンスからも検索できます。

既存のグループへの組み込み

スタンドアロンの QRadar Network Packet Capture アプライアンスを既存のグループに組み込むための要求は、そのグループのメンバーであるスタンドアロン・アプライアンスで開始できます。以下の例では、グループに組み込むスタンドアロンの QRadar Network Packet Capture アプライアンスをアプライアンス C とします。

例えば、QRadar Network Packet Capture アプライアンスを既存のグループに組み込む際は、以下の処理が発生します。

- グループのローカル・アカウントおよび Active Directory の構成をアプライアンス C にエクスポートします。アプライアンス C の以前のアカウントおよび Active Directory 構成は上書きされます。

グループからの解除

QRadar Network Packet Capture アプライアンスをグループから解除するときに、ローカル・アカウントおよび Active Directory 構成が状態のスナップショットとして保持されます。以後はグループとの同期が行われません。

QRadar Network Packet Capture グループのセットアップ

複数の QRadar Network Packet Capture アプライアンスを 1 つのグループに構成します。

始める前に

- 確実に、IBM QRadar Network Packet Capture アプライアンスのグループ化について理解するために、『グループ化した QRadar Network Packet Capture アプライアンス』を参照してください。
- 管理者として QRadar Network Packet Capture アプライアンスにログインします。

このタスクについて

グループ全体、選択したメンバー、または単一のメンバーを検索できます。検索結果は、タイム・スタンプの順に 1 つのストリームにマージして配信されます。各パケットには、PCAP/NG 形式で送信元デバイスの UUID および受信ポートのアノテーションが付きます。

手順

1. 「管理」タブをクリックして「グループ・メンバーシップ (GROUP MEMBERSHIP)」ウィジェットに移動します。
2. リモート QRadar Network Packet Capture アプライアンスの DNS または IP アドレスを入力します。
3. リモート QRadar Network Packet Capture アプライアンスへの管理者ユーザーのログイン情報を入力します。
4. 「ホストの追加」をクリックします。

タスクの結果

現在ログインしているアプライアンスとリモート QRadar Network Packet Capture アプライアンスがグループ化されます。

次のタスク

「削除」をクリックすると、QRadar Network Packet Capture アプライアンスがグループから削除されます。

第 5 章 外面 LED のトラブルシューティング

外面 LED の状態や色を確認すると、IBM QRadar Network Packet Capture アプライアンスのトラブルシューティングに役立ちます。

各種の外面 LED を特定したり問題のトラブルシューティングを行ったりする際は、以下の図表を参照してください。

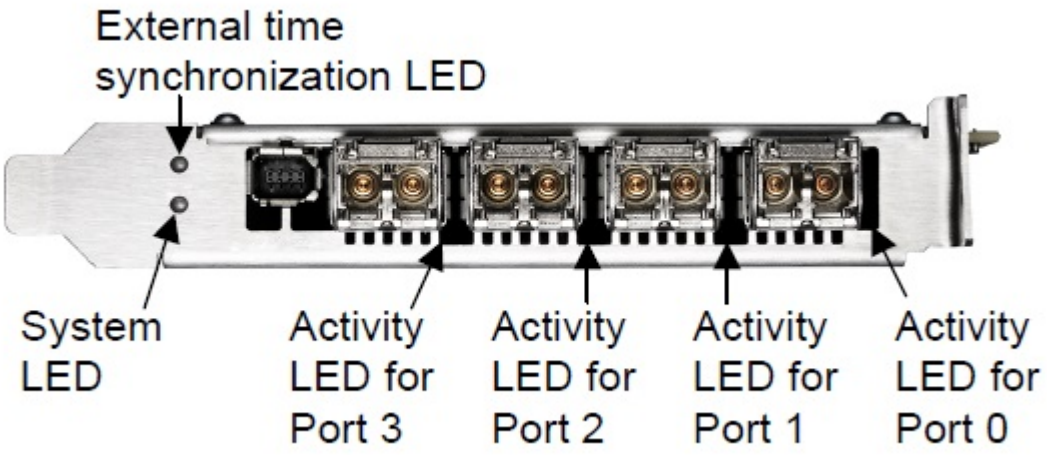


図 *12.* 外面 *LED* の位置。

アクティビティー LED

アクティビティー LED の色が示す一般的な状態を以下の表に示します。

表 *2.* アクティビティー *LED* とアプライアンスの動作状況。

状態および色	状況
オフ	ドライバーがロードされていません。イーサネット・リンクが停止しているか、ポートが切断されています。
緑点灯	ドライバーがロードされ、イーサネット・リンクが稼動していますが、トラフィックがありません。
緑点滅	ドライバーがロードされており、イーサネット・リンクにトラフィックがあります。

システム LED

システム LED の色が示す一般的な状態を以下の表に示します。

表 *3.* システム *LED* とアプライアンスの動作状況。

状態および色	状況
オフ	電源が入っていません。

表 3. システム *LED* とアプライアンスの動作状況。 (続き)

状態および色	状況
赤点灯	始動中であり、電源が入っています。アクセラレーターが電源装置を検査しています。
赤点滅	始動後であり、電源が入っています。重大なハードウェア・エラーが発生しました。
黄点灯	始動中であり、電源が入っています。電源装置が稼動しています。
黄点滅	ハードウェア・ログに新しい項目があります。
緑点灯	FPGA がロードされ、システムが稼動しています。

外部時刻同期 LED

外部時刻同期 LED の色が示す一般的な状態を以下の表に示します。

表 4. 外部時刻同期 *LED* とアプライアンスの動作状況。

状態および色	状況
オフ	ドライバーがロードされていないか、PTP (Precision Time Protocol) ポートのイーサネット・リンクが停止しています。
黄点灯	PTP ポートのイーサネット・リンクが稼動しています。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

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

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

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。

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。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、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なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

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