



## 付録 B クエリーの作成

この付録では、MARS の長期クエリーを作成および表示する方法について説明します。MARS では長期クエリーを 2 つの方法で実行できます。

### 1. 既存レポートを変更します。

*利点:*

- ・ レポートが比較的短時間でコンパイルされます。
- ・ 長期間にわたり収集されたデータをコンパイルできます。

*欠点:*

このタイプのクエリーを使用できるのは、時間範囲以外のクエリー基準が変更されていない場合のみです。また、併用できるのは、次のレポートに限られます。

- ・ Activity:All - Top Destination Ports
- ・ Activity:All - Top Destinations
- ・ Activity:All - Top Event Types
- ・ Activity:All - Top Reporting Devices
- ・ Activity:All - Top Sources
- ・ Activity:Attacks Seen - Top Reporting Devices
- ・ Activity:Denies - Top Destination Ports
- ・ Activity:P2P Filesharing/Chat - Top Event Types
- ・ Activity:Scans - Top Destination Ports
- ・ Activity:Scans - Top Destinations
- ・ Activity:Unknown Events - All Events
- ・ Activity:Web Usage - Top Destinations by Sessions
- ・ Activity:Web Usage - Top Sources
- ・ Attacks:All - Top Rules Fired
- ・ Attacks:All - Top Sources

### 2. バッチ クエリーを実行します。

*利点:*

- ・ どのクエリー基準でも変更できます。
- ・ 短期間のデータに最適です。

*欠点:*

- ・ このタイプのクエリーは低速であり、完了までかなりの時間がかかることがあります。
- ・ バッチ クエリーを実行できるのは管理ユーザのみです。

この付録では、両方の長期クエリー方式について説明します。

## レポートを使用した長期クエリーの実行

MARS のアクティビティを長期間観察する場合は、定期的に行われる既存レポートの期間(1 時間ごと、1 日ごとなど)を変更する必要があります。レポートが出荷時に MARS に付属していたか、あるいはユーザが作成したかには関係しません。



**注** 「オンデマンド」でのみ動作するレポートを使用して長期クエリーを実行しようとすると、クエリーを実行した場合と同じ効果になります。長期クエリーではデータをコンパイルする必要があるため、処理に時間がかかることがあります。一方、定期実行レポートのデータは継続的に事前コンパイルされます。

レポートを使用してクエリーを実行する手順は、次のとおりです。

**ステップ 1** QUERY / REPORTS タブで、**Reports** タブをクリックしてメイン レポート ウィンドウを取得します。

図 B-1 メイン レポート ウィンドウ

Report Selection

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
<input type="radio"/> Activity: All - NAT Connections	Run on demand only	Normal	None	Query Type: NAT connections ranked by Time Time: May 1, 2004 8:21:50 PM PDT - Jun 6, 2004 8:31:50 PM PDT	This report lists Network Address Translations performed on non-denied sessions as reported to MARS.	Finished: Jun 16, 2004 4:40:36 AM PDT	Jun 15, 2004 8:32:09 PM PDT	May 1, 2004 8:21:50 PM PDT - Jun 6, 2004 8:31:50 PM PDT
<input type="radio"/> Activity: All - Top Destination Ports	Run on demand only	Trend	None	Query Type: Destination Ports ranked by Sessions Time: 1hh:0mm:0ss	This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 10, 2004 4:17:02 PM PDT	Jun 10, 2004 4:16:58 PM PDT	Jun 10, 2004 3:16:58 PM PDT - Jun 10, 2004 4:16:58 PM PDT
<input checked="" type="radio"/> Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 17, 2004 2:15:52 PM PDT	Jun 17, 2004 2:15:52 PM PDT	Nov 30, 2003 1:05:52 PM PST - Jun 17, 2004 2:15:52 PM PDT

143798

**ステップ 2** 変更する定期レポートの横にあるオプション ボタンにナビゲートして、クリックします(この例では、**Activity:All - Top Destinations** を使用します)。Query カラムをクリックして、レポートを編集します。Build Report ウィンドウが表示されます。

## 図 B-2 Build Report ウィンドウ

## Build Report

Click the cells below to define the report:

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 16, 2004 7:15:42 PM PDT	Jun 16, 2004 7:15:42 PM PDT	Nov 29, 2003 6:05:42 PM PST - Jun 16, 2004 7:15:42 PM PDT

**Time Range:**

Last: 200 Days 0 Hrs 10 Mins

Start: 2004 June 16 19 Hrs 42 Mins  
 End: 2004 June 16 19 Hrs 52 Mins

143686

**ステップ 3** Build Report ウィンドウの下部で、レポート (**Activity:All - Top Destinations**) の対象となる **Time Range** を、目的の期間に変更します。

**ステップ 4** **Submit** ボタンをクリックしてレポートを実行し、メイン レポート ウィンドウに戻ります。

## Report タブでのクエリー結果の表示

Report タブにクエリーを表示する手順は、次のとおりです。

## 図 B-3 メイン レポート ウィンドウ (下部)

<input checked="" type="radio"/>	Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 17, 2004 2:15:52 PM PDT	Jun 17, 2004 2:15:52 PM PDT	Nov 30, 2003 1:05:52 PM PST - Jun 17, 2004 2:15:52 PM PDT
<input type="radio"/>	Activity: All Events and Netflow - Top Destination Ports	Run on demand only	Trend	None	Query Type: Destination Ports ranked by Sessions Time: 1hh:0mm:0ss	This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 8, 2004 9:28:51 PM PDT	Jun 8, 2004 9:29:03 PM PDT	Jun 8, 2004 8:28:51 PM PDT - Jun 8, 2004 9:28:51 PM PDT
<input type="radio"/>	Activity: All Sessions - Top Destination Ports by Bytes	Run on demand only	Normal	None	Event type: Info/AllSession, Query Type: Destination Ports ranked by Bytes Transmitted Time: 0hh:10mm:0ss	This report ranks all destination ports by bytes transferred.	Not Run	Jun 8, 2004 9:29:20 PM PDT	Jun 8, 2004 9:19:20 PM PDT - Jun 8, 2004 9:29:20 PM PDT
<input type="radio"/>	Activity: All Sessions - Top Destinations by Bytes	Run on demand only	Normal	None	Event type: Info/AllSession, Query Type: Destination IPs ranked by Bytes Transmitted Time: 0hh:10mm:0ss	This report ranks all destinations by bytes transferred.	Not Run	Jun 8, 2004 9:29:57 PM PDT	Jun 8, 2004 9:19:57 PM PDT - Jun 8, 2004 9:29:57 PM PDT

143789

**ステップ 1** メイン レポート ウィンドウの下部で、レポート (**Activity:All - Top Destinations**) の横にあるオプション ボタンをクリックします。



図 B-5 Query Event Data ウィンドウ

Query Event Data

Click the cells below to change query criteria:

Query type: *Sessions ranked by Time, 0hh:10mm:0ss*

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
H-10.1.252.250	H-65.54.153.118	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	ANY

Keywords: [ None ]

Result Format: All Matching Sessions

Order/Rank By: Time

Filter by Time:

Last: 0 Days 0 Hrs 10 Mins

Start: 2004 June 22 18 Hrs 38 Mins  
End: 2004 June 22 18 Hrs 48 Mins

Real Time

Use Only Firing Events:

Maximum rank returned: 100

143795

**ステップ 3** Query Event Data ウィンドウで、クエリー基準を変更できます(クエリー基準の詳細については、「[インシデントの調査](#)」を参照)。各パラメータをクリックすると、クエリーの性質を変更できます。この場合は、送信元 IP アドレスを **10.1.1.6**、保存済みの宛先 IP アドレス範囲を **mygroup** として指定し、クエリー期間を過去 2 日間に設定します。いずれかの **Apply** ボタンをクリックして、変更をクエリーに適用します。Query Save/Submit ウィンドウが表示されます。

図 B-6 Query Save/Submit ウィンドウ

Query Event Data

Click the cells below to change query criteria:

Query type: *Event Types ranked by Sessions, 2dd:0hh:0mm:0ss*

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
[10.1.1.6] 10.1.1.6	my group [10.0.0.0 / 255.0.0.0] n-10.0.0.0/8	BackOrifice (src port: ANY, dst port: 31337, proto: TCP), BackOrifice (src port: ANY, dst port: 31338, proto: TCP)	ANY	ANY	ANY	ANY	None	ANY	ANY	ANY

Keywords: [ None ]

143794

**ステップ 4** Query Save/Submit ウィンドウに、**Save as Rule**、**Save as Report**、または **Submit Batch** のオプションから選択するように求めるメッセージが表示されます。クエリーをバッチ クエリーとして送信するには、**Submit Batch** をクリックします。クエリーが送信され、Batch Query タブに自動的に移動します。

## 図 B-7 Batch Query タブ

Page Refresh Rate

1 minute

Batch Query Selection

Owner	Query	Status	Submitted	Time Range
<input checked="" type="radio"/> Administrator, Administrator (pnadmin)	Query Type: Event Types ranked by Sessions Time: 0hh:10mm:0ss	Finished: Jun 21, 2004 8:07:08 PM PDT	Jun 21, 2004 8:07:02 PM PDT	Jun 21, 2004 7:57:02 PM PDT - Jun 21, 2004 8:07:02 PM PDT
<input type="radio"/> Administrator, Administrator (pnadmin)	Query Type: Event Types ranked by Sessions Time: 4ww:2dd:0hh:10mm:0ss	Not Run	Never	May 5, 2004 11:52:25 AM PDT - Jun 4, 2004 12:02:25 PM PDT
<input type="radio"/> Administrator, Administrator (pnadmin)	Query Type: Event Types ranked by Sessions Time: 2ww:0dd:0hh:0mm:0ss	Finished: Jun 13, 2004 2:17:43 PM PDT	Jun 13, 2004 12:58:32 PM PDT	May 30, 2004 12:58:32 PM PDT - Jun 13, 2004 12:58:32 PM PDT
<input type="radio"/> Administrator, Administrator (pnadmin)	Event type: != Built/teardown/permitted IP connection, Query Type: Event Types ranked by Sessions Time: 4ww:2dd:0hh:10mm:0ss	Stopped: 16%	Jun 13, 2004 12:42:35 PM PDT	May 14, 2004 12:32:35 PM PDT - Jun 13, 2004 12:42:35 PM PDT
<input type="radio"/> Administrator, Administrator (pnadmin)	Query Type: Event Types ranked by Sessions Time: 1ww:6dd:0hh:10mm:0ss	Finished: Jun 13, 2004 1:37:15 PM PDT	Jun 13, 2004 12:40:35 PM PDT	May 31, 2004 12:30:35 PM PDT - Jun 13, 2004 12:40:35 PM PDT

View HTML View HTML View CSV View Results Resubmit Stop Delete

143785

**ステップ 5** クエリーのステータスをリアルタイムで表示するには、Batch Query タブのドロップダウン リストを使用して、**Page Refresh Rate** を **Never** (デフォルト) から 1、3、5、10、15、または 30 分に変更します。

**ステップ 6** 動作中のバッチ クエリーの結果を表示するには、目的のクエリーの横にあるオプション ボタン (グリーンに強調表示) をクリックして、**View Results** をクリックします。この処理は、クエリーの進行中に実行できます。

MARS のユーザ プロファイル内の電子メール アドレスが有効な場合は、クエリーが完了すると、バッチ クエリーの結果がユーザに電子メールで送信されます。また、**QUERY / REPORTS > Batch Query > View Results** の順にクリックして、バッチ クエリーの結果を表示できます。



**注** クエリーの進行中に、**View Results** をクリックすると、その時点までにコンパイルされた結果が再計算されます。この処理を実行すると、結果をコンパイルした場合よりも、表示に時間がかかることがあります。