

RSA NetWitness Platform

Event Source Log Configuration Guide



Check Point Security Suite, IPS-1

Last Modified: Wednesday, February 19, 2020

Event Source Product Information:

Vendor: [Check Point](#)

Event Source: Check Point Security Suite, IPS-1

Versions: R76, R77.x, R80.x

Note: For version R77.30 & R80.10 and going forward, the only collection method we support is syslog collected via log exporter tool. This is by recommendation from Checkpoint.

Supported Platforms:

Check Point Appliances, SecuredBy Check Point partner appliances, Check Point SecurePlatform running on Open Servers, and Check Point software running on supported Operating Systems (such as Windows, Red Hat and Solaris)

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: checkpointfw1, cef

Collection Method:

- Check Point LEA API
- Log Exporter (R77.30 and R80.10)

Event Source Class.Subclass: Security.Firewall

To configure the Check Point Security Suite to work with RSA NetWitness Platform, perform the following tasks:

- I. [Introduction to the Check Point Security Suite](#)
- II. [Verify the Functionality of the Existing Check Point Security System](#)
- III. [Configure Check Point to Accept Connections](#)
 - To use Check Point Lea API collection, choose either of the following procedures, based on your version:
 - [Configure version R80](#)
 - [Configure version R76 or 77.x](#)
 - To use Log Exporter, [Configure the Log Exporter tool to send CEF format syslog to RSA NetWitness Platform](#)
- IV. Configure RSA NetWitness Platform
 - [Configure NetWitness Platform for Check Point Collection](#)
 - Or, if using Log Exporter, [Configure RSA NetWitness Platform for Syslog](#)

Introduction to the Check Point Security Suite

This section discusses security tightening done for some versions of Check Point, and provides an overview of the event source.

Log Exporter Tool

Checkpoint configuration requires the Log Exporter tool be installed on the Checkpoint event source. This tool is not included by default in certain Checkpoint versions.

Checkpoint Version	Comments
80.20	Log Exporter is included in this version.
80.10 77.30	Install Log Exporter using Check Point Log Exporter Portal .

Check Point Security Tightening

For the newer versions of the Check Point Security Suite, security to access Check Point Management Console has been hardened. Note the following:

- For version R61 and newer, you cannot use the **no authentication** method to connect to the console. You need to use **auth_OPSEC** or **SSLCA** as the authentication method.
- For version R71 and newer, you cannot use the **no authentication** nor the **auth_OPSEC** method to connect to the console. You need to use **SSLCA** as the authentication method.

RSA recommends that customers use **SSLCA** as the authentication method whenever possible. If not, you may see errors in the *checkpoint servername_opsec_output.log* file such as **connection reset by peer** or **unable to connect**.

Check Point Configuration Overview

Note the following:

- The Check Point product has several feature packs that run on numerous operating systems or platforms. The naming conventions, menu selections, and entry fields may vary slightly between versions. The basic flow for any of them is nearly identical. These configuration instructions are for NG and later running in a Windows environment.
- By default, Check Point logs are sent from the Check Point event sources to the management server. Alternatively, logs can be sent to a centralized log module (CLM). In this document, the term "log server" refers to either the management server or a CLM, whichever you are using.

Verify the Functionality of the Existing Check Point Security System

Note: If an enforcement point sends logs to the management server, an enforcement point does not store the logs locally in the **fw.log** file. Therefore, an LEA connection between RSA NetWitness Platform and the enforcement point does not see any messages, except for the messages that are stored locally.

To verify the functionality of the Check Point Security System:

1. Open the Check Point SmartView Tracker, and ensure that the log server is receiving events.

Warning: Do not proceed until the Check Point log server is receiving events. If the log server does not display logs, RSA NetWitness Platform will not receive any events.

2. To ensure that RSA NetWitness Platform communicates with the Check Point management server, confirm that:
 - Event sources have been configured for all communication between Check Point and RSA NetWitness Platform.
 - Proper routing is available.

Warning: The following ports must be open on any firewall between RSA NetWitness Platform and the Check Point Management Station.

Port	Use
FW_lea (18184)	Required for non- authenticated or authenticated connections.
FW_ica_Pull (18210)	Required for sending the certificate file to the appliance.

To ensure that the LEA server component sends LEA events for Check Point versions earlier than R60:

1. To verify that the dictionary log file has no more than 1000 rows, follow these steps:
 - a. Open the `%FWDIR%\log\fw.logtrack` file with a text editor to calculate the number of rows in this file.
 - b. If there are more than 1000 rows in the file, back up the `fw.logtrack` file, and type:

```
fw logswitch
```

Note: The LEA server component on the log server fails to send LEA events if the dictionary log file has more than 1000 rows.

2. Verify that the number of network objects does not exceed the 64 K OPSEC buffer.

Warning: If the number of network objects exceeds the 64 K OPSEC buffer, go to the Check Point web site, and download the fix associated with **ID sk23634**.

Configure Check Point to Accept Connections

To change directories to the installation directory of your firewall, in a command prompt, run one of the following commands, depending on your operating system:

- On a Windows system, type `cd %FWDIR%`
- On a Linux or Unix system, type `cd $FWDIR`

Configure version R80

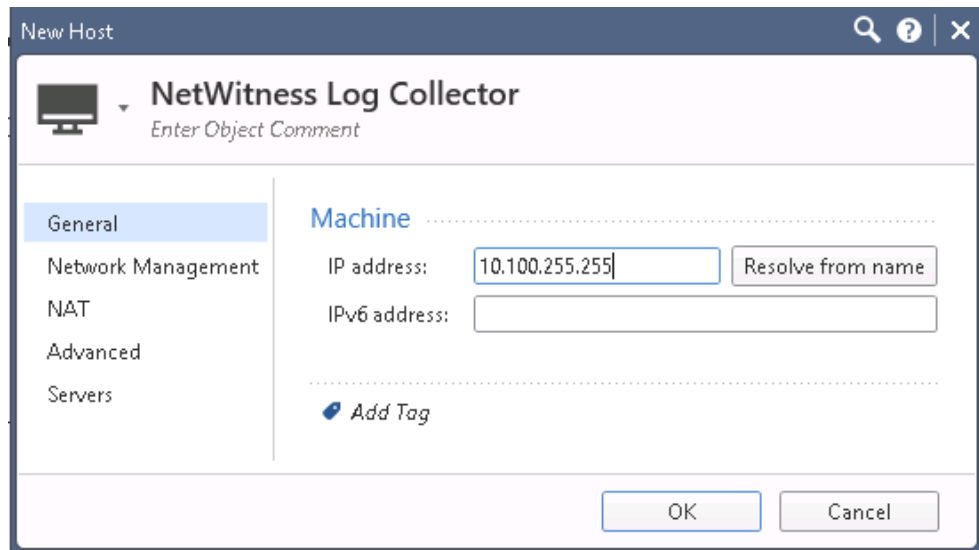
Note: To configure version R80, you need to have RSA NetWitness Platform version 10.6.2.1 or later to configure Check Point version R80.

Depending on your version, you may need to install the Log Exporter tool be installed on the Checkpoint event source.

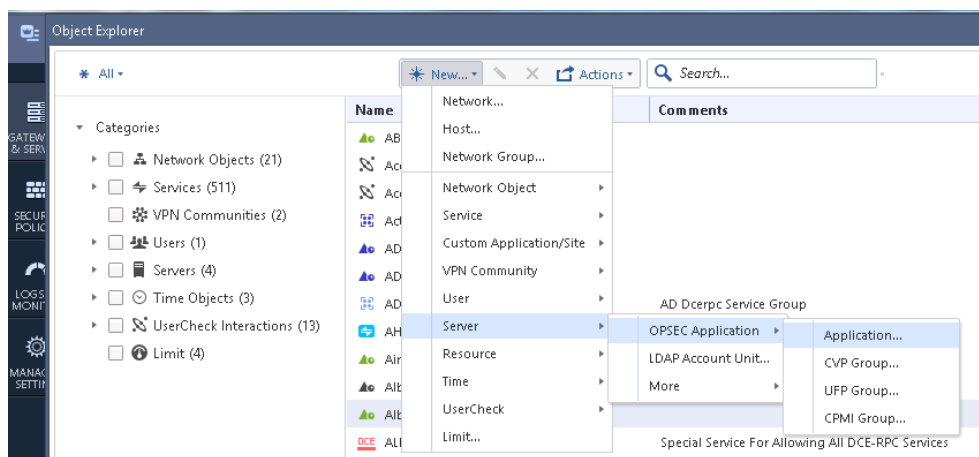
Checkpoint Version	Comments
80.20	Log Exporter is included in this version.
80.10	Install Log Exporter using Check Point Log Exporter Portal .

To configure Check Point to accept connections from RSA NetWitness Platform:

1. Follow these steps to define a network object:
 - a. Connect to the Check Point Management Server with the SmartDashboard client.
 - b. From the Check Point SmartDashboard menu, click **Objects > Object Explorer**.
 - c. In the Network Object window, click **New > Host**.
 - d. Enter a name for the Host, and enter the IP address of the RSA NetWitness Log Collector.



- e. Click **OK**.
2. Follow these steps to add an OPSEC application to represent RSA NetWitness Platform:
 - a. From the Check Point SmartDashboard menu, click **Objects > Object Explorer**.
 - b. From the menu, select **New > Server > OPSEC Application > Application**.



- c. In the OPSEC Application Properties window, complete the fields as follows.

Field	Action
Name	Type SA_OPSEC .
	<div style="border: 1px solid green; padding: 5px;"> <p>Note: This value is used to obtain the SSL certificate for SSLCA authentication.</p> </div>

Field	Action
Host	Select the Check Point network object that you defined in step 1.
Vendor	Select RSA. The Product field is auto-filled with enVision: accept this value.
Client Entities	Ensure the LEA value is selected.

- d. Click **Communication**.
- e. Enter a password to act as the activation key. Enter the activation key again.
- f. Click **Initialize**.
- g. Click **Close**.

Note: You need to enter the DN string that is displayed in this step as the Client SIC name when you add the LEA Client Service.

3. Follow these steps to add an access rule that permits RSA NetWitness Platform to collect events:
 - a. On the Check Point Smart Dashboard menu, click **Rule > Add a Rule**.
 - b. Complete the fields as follows to add the access rule.

Source	Destination	Service	Action	Track
Enter the host name of the RSA NetWitness Platform Log Collector.	Enter the host name of the Check Point log server.	Type: FW1_ica_Pull FW_lea	Type: Accept	Type: Log
Enter the host name of the Check Point log server.	Enter the host name of the RSA NetWitness Platform Log Collector.			

- c. Click **File > Save**.
- d. Click **Policy > Install**.

Warning: If you encounter an interpretation problem or a conflict among rules, move this rule to the top of the list.

Configure version R76 or 77.x

Checkpoint configuration requires the Log Exporter tool be installed on the Checkpoint event source. For details on how to install the tool, see [Check Point Log Exporter Portal](#).

To configure Check Point to accept connections from RSA NetWitness Platform:

1. Follow these steps to define a network object:
 - a. Connect to the Check Point Management Server with the SmartDashboard client.
 - b. From the Check Point SmartDashboard menu, click **Manage > Network Object**.
 - c. In the Network Object window, click **New > Node > Host**.
 - d. Enter the appropriate values to represent the RSA NetWitness Platform Log Collector service.
 - e. Click **OK**.
2. Follow these steps to add an OPSEC application to represent RSA NetWitness Platform:
 - a. From the Check Point SmartDashboard menu, click **Manage > Servers and OPSEC Applications**.
 - b. In the Servers and OPSEC Applications window, select **New > OPSEC Application**.
 - c. In the OPSEC Application Properties window, complete the fields as follows.

Field	Action
Name	Type SA_OPSEC . <div style="border: 1px solid green; padding: 5px; margin-top: 5px;"> Note: This value is used to obtain the SSL certificate for SSLCA authentication. </div>
Host	Select the Check Point network object that you defined in step 1.

- d. Click **Communication**.
- e. Enter a password to act as the activation key. Enter the activation key again.
- f. Click **Initialize**.
- g. Click **Close**.

Note: You will need to enter the string that is displayed in this step as the **Client Distinguished** name when you add Check Point Source in RSA NetWitness Platform.

3. Follow these steps to add an access rule that permits RSA NetWitness Platform to collect events:

- a. On the Check Point Smart Dashboard menu, click **Rule > Add a Rule**.
- b. Complete the fields as follows to add the access rule.

Source	Destination	Service	Action	Track
Enter the host name of the RSA NetWitness Platform Log Collector.	Enter the host name of the Check Point log server.	Type: FW1_ica_Pull FW_lea	Type: Accept	Type: Log
Enter the host name of the Check Point log server.	Enter the host name of the RSA NetWitness Platform Log Collector.			

- c. Click **File > Save**.
- d. Click **Policy > Install**.

Warning: If you encounter an interpretation problem or a conflict among rules, move this rule to the top of the list.

Configure the Log Exporter tool to send CEF format syslog to RSA NetWitness Platform

Log Exporter is a multi-threaded daemon service, running on a log server. Each log that is written on the log server is read by the log exporter daemon, transformed into the desired format and mapping, and then sent to the end target.

On MDS/MLM, if log exporter is deployed on several domains, each domain server has its own log exporter daemon service. If exporting the logs to several targets, each target has its own log exporter daemon.

- **Extract:** Reads incoming logs from the GW
- **Transform:** Changes the logs according to the configuration
- **Load:** Sends the logs to the configured target server

Run Log Exporter Commands

Once you have installed the log exporter on the Check Point log server, you need to run the following command:

```
cp_log_export add name <unique name of the log export session> target-server <Decoder IP> target-port <the port on which the target is listening> protocol <protocol to use> format CEF
```

If you are on a Multi Domain environment, run the following command to specify the domain name or IP:

```
cp_log_export add name <unique name of the log export session> domain-server <MDS/MLM domain name or IP> target-server <Decoder IP> target-port <the port on which the target is listening> protocol <protocol to use> format CEF
```

Examples

SmartCenter/Log Server

```
cp_log_export add name test-session-1 target-server 10.10.10.10 target-port 514 protocol tcp format cef
```

MDS/MLM

```
cp_log_export add name test-session domain-server 20.20.20.20 target-server 10.10.10.10 target-port 514 protocol tcp format cef
```

Configure NetWitness Platform for Check Point Collection

This section contains instructions for configuring Check Point collection on the RSA NetWitness Platform log collector, as well as details about setting some of the parameters.

Configure the Log Collector for Check Point Collection

You should configure the Log Collector for Check Point collection.

To configure the Log Collector for Check Point collection:

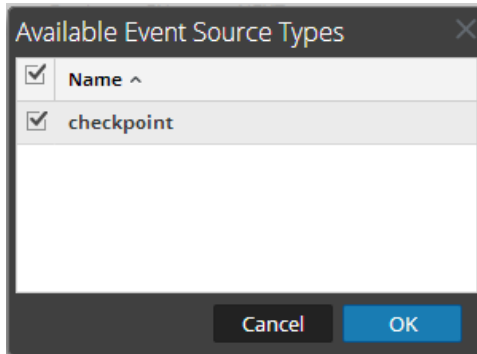
1. In the RSA NetWitness Platform menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Check Point/Config** from the drop-down menu.

The Event Categories panel displays the Check Point event sources that are configured, if any.

4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

5. Select **checkpoint** from the list, and click **OK**.



The newly added event source type is displayed in the Event Categories panel.

6. Select the **checkpoint** type in the Event Categories panel and select **Pull Cert** in the Sources panel toolbar.
7. Enter the **Server Address**, **Client Entity Name**, and **Password**, then click **OK**.

Note: The entity name and password must match the values you entered when you created the OPSEC application on the Check Point server.

8. Click **+** in the Sources panel toolbar, and enter the parameter values in the Add Source dialog box, then Click **OK**.

Parameter	Description
Name*	Enter the name of the OPSEC Application that you created when configuring Check Point earlier.

Parameter	Description
Address*	IP Address of the Check Point server.
Server Name*	Enter the name of the Check Point server.
Certificate Name	Select a certificate from the drop-down list.
Client Distinguished	Enter the Client Distinguished Name from the Check Point server. This is the string that was displayed when you created the OPSEC application in the Check Point server earlier.
Client Entity Name	Enter the OPSEC Application name you entered on the Check Point server.
Server Distinguished	This should be the Client Distinguished name, without the first section of that string. See the example screen below for details.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.

This is an example of the Check Point Add/Edit Source dialog box:

The screenshot shows the 'Edit Source' dialog box with the following fields and values:

- Name ***: SA_OPSEC
- Address ***: 10.100.33.5
- Server Name ***: cp-R80secmgt
- Certificate Name**: checkpoint_SA_OPSEC
- Client Distinguished**: CN=SA_OPSEC,O=cp-R80secmgt.asoc54.lab.qr9yr9
- Client Entity Name**: SA_OPSEC
- Server Distinguished**: cn=cp_mgmt,O=cp-R80secmgt.asoc54.lab.qr9yr9
- Enabled**:
- Pull Certificate**:
- Certificate Server Address**: 10.100.33.5
- Password**: *****

At the bottom, there is an 'Advanced' section (collapsed), 'Cancel' and 'OK' buttons.

Parameters are defined in the next section.

Check Point Parameters

The Add Source dialog and the Edit Source dialog contain the same information.

Basic Parameters

Parameter	Description
Name*	Name of the event source.
Address*	IP Address of the Check Point server.
Server Name*	Name of the Check Point server.

Parameter	Description
Certificate Name	<p>Certificate name for secure connections to use when the transport mode is https. If set, the certificate must exist in the certificate trust store that you created using the Settings tab.</p> <p>Select a certificate from the drop-down list. The file naming convention for Check Point event source certificates is checkpoint_name-of-event-source.</p>
Client Distinguished	Enter the Client Distinguished Name from the Check Point server.
Client Entity Name	Enter the Client Entity Name from the Check Point server.
Server Distinguished	Enter the Server Distinguished Name from the Check Point server.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Pull Certificate	Select the checkbox to pull a certificate for first time. Pulling a certificate makes it available from the trust store.
Certificate Server Address	IP Address of the server on which the certificate resides. Defaults to the event source address.
Password	Only active when you select the Pull Certificate checkbox for first time. Password required to pull the certificate. The password is the activation key created when adding an OPSEC application to Check Point on the Check Point server.

Determine Advanced Parameter Values for Check Point Collection

You use less system resources when you configure a Check Point event source connection to stay open for a specific time and specific event volume (transient connection). RSA NetWitness Platform defaults to the following connection parameters that establish a transient connection:

- Polling Interval = **180** (3 minutes)
- Max Duration Poll = **120** (2 minutes)
- Max Events Poll = **5000** (5000 events per polling interval)
- Max Idle Time Poll = **0**

For very active Check Point event sources, it is a good practice to set up a connection that stays open until you stop collection (persistent connection). This ensures that Check Point collection maintains the pace of the events generated by these active event sources. The persistent connection avoids restart and connection delays and prevents Check Point collection from lagging behind event generation.

To establish a persistent connection for a Check Point event source, set the following parameters to the following values:

- Polling Interval = **-1**
- Max Duration Poll = **0**
- Max Events Poll = **0**
- Max Idle Time Poll = **0**

Parameter	Description
Event Filter	<p>Enter a regular expression to filter events.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: See the topic "Configure Event Filters for Log Collector" in the <i>Log Collection Guide</i> for details on how to create more detailed rules for event filtering.</p> </div>
Port	Port on the Check Point server that Log Collector connects to. Default value is 18184.
Collect Log Type	<p>Type of logs that you want to collect: Valid values are:</p> <ul style="list-style-type: none"> • Audit - collects audit events. • Security - collects security events. <p>If you want to collect both audit and security events, you must create a duplicate event source. For example, first you would create an event source with Audit selected pulling a certificate into the trust store for this event source. Next you would create another event source with the same values except that you would select Security for the Collect Log Type and</p>

Parameter	Description
	you would select the same certificate in Certificate Name that you pulled when you set up the first set of parameters for this event source and you would make sure that Pull Certificate was not selected.
Collect Logs From	<p>When you set up a Check Point event source, Security Analytics collects events from the current log file. Valid values are:</p> <ul style="list-style-type: none"> • Now - Start collecting logs now (at this point in time in the current log file). • Start of Log - Collect logs from the beginning of the current log file. <p>If you choose "Beginning of Time" for this parameter value, you may collect a very large amount of data depending on how long the current log file has been collecting events. Note that this option is effective only for the first collection session.</p>
Polling Interval	<p>Interval (amount of time in seconds) between each poll. The default value is 180.</p> <p>For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.</p>
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.> 300 is the default value.
Forwarder	Enables or disables the Check Point server as a forwarder. By default it is disabled.
Log Type (Name Value Pair)	Logs from the event source in Name Value format. By default it is disabled.

Parameter	Description
Debug	<p>Caution: Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector.</p> <p>Enables and disables debug logging for the event source.</p> <p>Valid values are:</p> <ul style="list-style-type: none">• Off = (default) disabled• On = enabled• Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p> <p>If you change this value, the change takes effect immediately (no restart required).</p>

Configure RSA NetWitness Platform for Syslog

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **cef**.



Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:

- If you see  **Start Capture**, click the icon to start capturing Syslog.
- If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.
The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click **+**.
The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.
The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.
Click **OK** to accept your changes and close the dialog box.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.