



# Integrate RSA Malware Analysis with Cuckoo Sandbox



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

## **Trademarks**

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm](http://www.emc.com/legal/emc-corporation-trademarks.htm).

## **License Agreement**

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

## **Third-Party Licenses**

This product may include software developed by parties other than RSA.

## **Note on Encryption Technologies**

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## **Distribution**

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

March 2019

# Contents

---

<b>How to Integrate RSA Malware Analysis with Cuckoo Sandbox .....</b>	<b>4</b>
Enable the File Sharing Protocol .....	4
Change the Share Name .....	4
Configure the Cuckoo Sandbox .....	5
Run the Script Periodically .....	6
Script Contents .....	7

# How to Integrate RSA Malware Analysis with Cuckoo Sandbox

Users would like to integrate RSA Malware Analysis with sandbox solutions, so they can:

- Automatically submit malicious artifacts to these other solutions, and
- See the results from RSA Malware Analysis and a sandbox solution together.

This document is based on work presented by Luiz Borges [luiz.borges@techbiz.com.br](mailto:luiz.borges@techbiz.com.br) at the 2016 RSA Techfest.


In this document, we consider the Cuckoo Sandbox, and describe how to integrate this solution with RSA Malware Analysis.

You will need:

- RSA NetWitness for Packets, with the Malware Analysis module.
- Cuckoo Sandbox

## Enable the File Sharing Protocol

The first step is to enable the File Sharing Protocol on the RSA Malware Analysis Service.

1. In the RSA NetWitness UI, navigate to **ADMIN > Services**.
2. Select a Malware Analysis service, and click  **View > Config**.
3. In the **General** tab, in the **Repository Configuration** section, enter **SAMBA** for the **File Sharing Protocol**.

### Repository Configuration

Name	Config Value
Directory Path	/var/lib/netwitness/rsamalware/spectrum
<b>File Sharing Protocol</b>	<b>SAMBA</b>
Retention (in days)	60

## Change the Share Name

Next, you need to change the share name on the Malware Analysis service.

1. Connect to the RSA Malware Analysis service through SSH.
2. Change the share name from **File Store** to **repository**.

```
root@sa:~  
# rsa malware smb configuration, guest and read only  
[global]  
workgroup = NWSPCTRM  
netbios name = SPCTRMFS  
local master = no  
server string = RSA Malware File Share  
security = share  
syslog only = yes  
max log size = 5120  
[repository]  
comment = RSA Malware File Store Content  
path = /var/lib/netwitness/rsamalware/spectrum/repository/files  
read only = Yes  
guest only = Yes
```

3. Restart the **smb** service.

```
/etc/init.d/smb restart
```

## Configure the Cuckoo Sandbox

On the Cuckoo Sandbox, you need to create a script file.

1. Connect to the Cuckoo Sandbox through SSH.
2. Create a directory named **/mnt/rsamalware**.
3. Create a script file named **rsamalware.sh** in Cuckoo's **utils** directory, and set executable permission for the file.
4. Enter the following code into the script file using a text editor (replace *your\_rsa\_malware* with the IP

address for your RSA Malware Analysis service):

```

1  #!/bin/bash
2
3  df -h | grep -i malware
4  RESULT=$?
5
6  if [ $RESULT -eq 1 ]; then
7
8      echo Not mounted.
9      echo Mounting...
10     mount -t cifs //your_rsa_malware/repository /mnt/rsamalware/ -o guest
11     RESULT=$?
12
13     if [ $RESULT -eq 0 ]; then
14
15         df -h | grep -i malware
16         echo Mounted successfully
17
18         find /mnt/rsamalware/ -mmin -5 -type f | while read line; do
19
20             python submit.py $line
21             sleep 30
22
23         done
24     fi
25
26
27     else echo Is mounted.
28
29     find /mnt/rsamalware/ -mmin -5 -type f | while read line; do
30
31         python submit.py $line
32         sleep 30
33
34     done
35
36 fi

```

## Run the Script Periodically

Finally, add a cron job to run the script periodically, for example every 5 minutes. You can change the period based on the demands of your installation.

In the following procedure, we set the frequency so the script runs every 5 minutes.

1. Open a terminal on your Cuckoo sandbox.
2. Run the following command:

```
crontab -e
```

This opens crontab in a vim editor.

3. Press ‘i’ to enter edit mode, and navigate to the final line in the file.

4. Copy the following line into the editor:

```
*/5 * * * * /utils/rsamalware.sh
```

This runs the script every 5 minutes.

5. Press the Escape key, then enter **:wq!** to save your work and close the vim editor.

The following message is displayed, indicating that the job is installing correctly:

```
crontab: installing new crontab
```

The job will run every 5 minutes.

## Script Contents

Below is the text version of the **rsamalware.sh** script. You can copy this code when you are editing your file.

**Note:** Replace the example IP address, **10.100.255.255**, with the IP address of your RSA Malware Analysis service.

```
#!/bin/bash
df -h | grep -i malware
RESULT=$?
if [ RESULT -eq 1 ]; then
    echo Not mounted.
    echo Mounting...
    mount -t cifs //10.100.255.255/repository /mnt/rsamalware/ -o guest
    RESULT=$?
    if [ $RESULT -eq 0 ]; then
        df -h | grep -i malware
        echo Mounted successfully
        find /mnt/rsamalware/ -mmin -5 -type f | while read line; do
            python submit.py $line
            sleep 30
        done
    fi
    else echo Is mounted.
    find /mnt/rsamalware/ -mmin -5 -type f | while read line; do
        python submit.py $line
        sleep 30
    done
fi
```