Install and Update SFTP Agent - SADOCS-533

Overview

This topic tells you how to download the **RSA Security Analytics Secure FTP Agent** and make the appropriate modifications for log collection.

Context

You must use the SFTP protocol to upload events from File event sources to the Log Collector.

RSA recommends that you use **RSA Security Analytics Secure FTP Agent**, which you can download from the RSA SecurCare Online (SCOL) Customer Support website. The SFTP Agent on SCOL consists of the binaries to install the SFTP Agent. You configure these binaries as described here, in this document. As part of the install process, you generate a public/private keypair.

You need to create a user account for the file transfer on each Windows event source that sends data to the Log Collector. The accounts can have any name, but the documentation assumes the accounts are named **sftp**.

Goal

After completing this how-to you will have...

- Installed and Updated the Security Analytics (SA) SFTP Agent.
- Reviewed the SA SFTP Agent Troubleshooting recommendations.

Return to Log Collection Configuration Checklist

Install and Update the SA SFTP Agent

Complete the following steps to configure the SA SFTP agent on the event source:

1. Run Microsoft Visual C++ 2005 Redistributable Package on Event Source
2. Install SA SFTP Agent on Event Source.
3. Set Up SA SFTP Agent on Event Source.
4. Generate Key Pair on Event Source and Import Public Key to Log Collector.

5. Select User Account to Run SA SFTP Agent Service.
6. Cache Keys for Connection.
7. Configure the SA Upload directories
8. Start SA SFTP Agent Service from Windows Services Control Panel.

Run Microsoft Visual C++ 2005 Redistributable Package

To run the Microsoft Visual C++ 2005 redistributable package

1. Download either of the following packages to the event source:
   - Microsoft Visual C++ 2005 Redistributable Package (x86) -http://www.microsoft.com/downloads/details.aspx?familyid=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en
   - Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) -http://www.microsoft.com/downloads/details.aspx?familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en
2. Click **Download** and run **vcredist_x86.exe**.

Install SA SFTP Agent on the Event Source

Caution: You must use the **RSA Security Analytics Secure FTP Agent.**

To install the SA SFTP Agent on the event source:

1. Search for the **RSA Security Analytics Secure FTP Agent** on SecurCare Online (SCOL).
2. For:
   - Windows client, click **Secure FTP Agent** to download the binaries.
   - UNIX client, click **Unix Secure FTP Agent** to download the binaries.
3. Complete the instructions to install the SFTP Agent onto the event source.

Set Up the SA SFTP Agent on the Event Source

To set up the SA SFTP agent on the event source:

1. Go to the SA SFTP agent install directory (default directory is **C:\sasftpagent**).
2. Use a text editor to open the **sftpagent.conf** file.
3. Make the following edits and keep all other lines commented:

```
agent.logginghost=ngc-ip
dir0=C:\test
dir0.filespec=*.log
dir0.interval=60
```

dir0.has_header=false
dir0.compression=false
dir0.enabled=true
dir0.ftp=ngc-ip,sftp,sftp,*publickey*,//upload/event-source-type/file-dir
dir0.delete_after_read=true

See Parameters for the table that describes all of the available parameters.

Note: You can add dir<n> sections (such as dir1, dir2, and so on) to set parameters for additional directories.

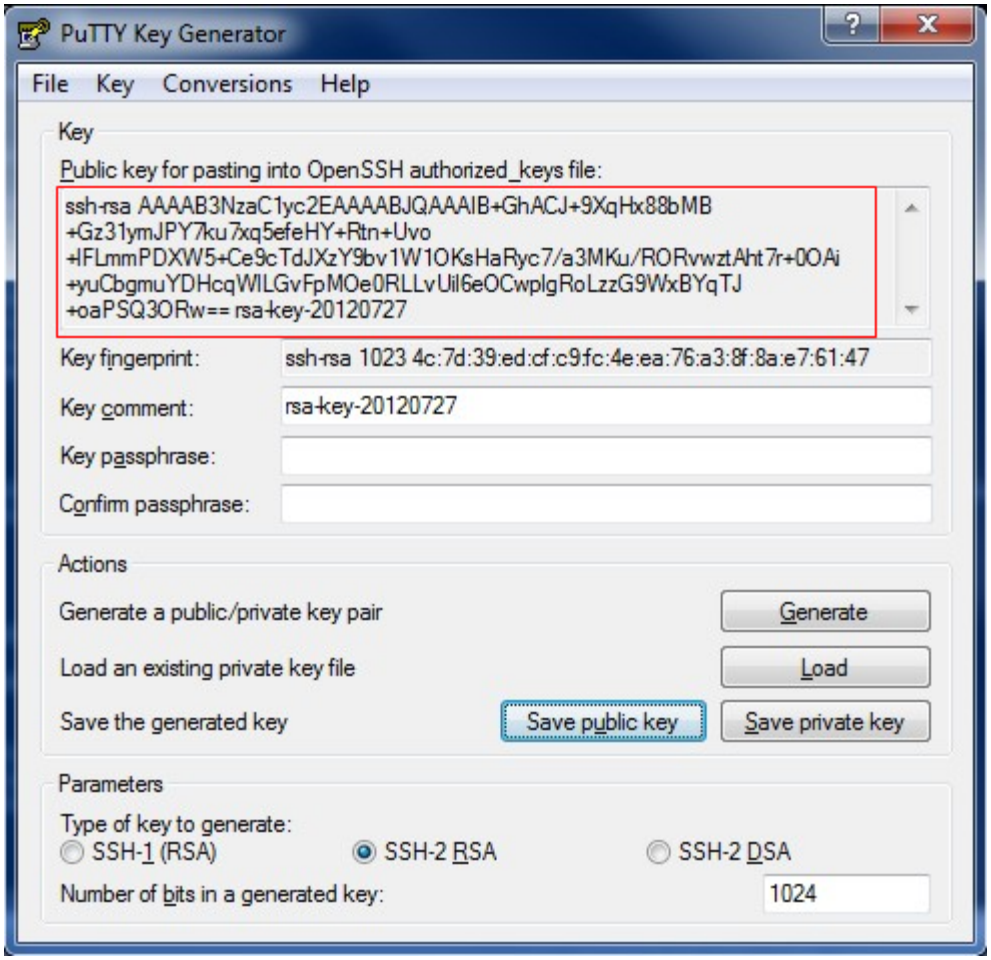
4. Save the file.

Generate Key Pair on Event Source and Import Public Key to Log Collector

To generate the key pair on the event source and import the public key to Log Collector:

1. Double-click **puttygen.exe** in the **C:\sasftpagent** directory. The PuTTY Key Generator starts.
2. Select **SSH2 RSA** as the type of key to generate.
3. Click **Generate**. and move the mouse in the PuTTY Key Generator window until the key is generated.
4. Save the private key:
   a. Click **Save private key**.
   b. Select **Yes** to not use a passphrase.
   c. Save the file as **private.ppk** in the **C:\sasftpagent** directory.
5. Add the public key to the Log Collector:
   a. Copy the public key into your buffer so that you can paste it into the parameter in Security Analytics as described in step 5b.

In the following example, the public key is enclosed in a red box.



b. Paste the public from your buffer into Security Analytics:
   - v10.4 and later, paste the key into the Eventsource SSH Key parameter (see **Configure File Event Sources in Security Analytics** in the SA Help).
   - v10.3.x and earlier:
     1. go to the **Explore** view for a Log Collector service.
     2. Click **logcollection > file**, right-click **eventsources**, and click **Properties**.
     3. Select the **keys**, specify **op=add key="*public-key*"**, and click **Send**.
        where ***public-key*** is the key that you have saved in your buffer.

6. Close the **puttygen.**

Select User Account to Run SFTP Agent Service

After you import the public key to the Log Collector, you must:

- Select either an existing user account, or
- Create a user account on the event source to run the SFTP Agent Service.

To create a user account on the event source:

1. In the Windows **Start** menu, click **Programs** > **Administrator Tools** > **ActiveDirectory users and computers**.

2. Click **Action** > **New** > **User** and create a new user under which you want the service to run.

   Note: The user account should be a member of the local admin group. The account must also have access to the files that are sent to Log Collector.

3. Modify the SA SFTP Agent Service to use this user account:
   a. Right-click SA SFTP Agent and select Properties.
   b. Click the **Log On** tab.
   c. Select **This account**.
   d. Type the user name and password for the account that you are using to run the SFTP Agent Service.
   e. Click **OK**.
4. Log off the event source and log back on using the new user account.

   Note: The user account that runs these steps must be the same user that runs the service.

5. Cache the keys for the connection.

Cache Keys for Connection

After you create the user account that runs the SA SFTP Agent service, you must cache the keys to connect the event source to the Log Collector.

To cache the keys on the event source:

1. Log on the machine with the account you selected for the SA SFTP Agent Service.
2. Run the following command from the **C:\sasftpagent** directory:

   psftp -i *private.ppk* -l sftp -v *ngc-ip*

   where:

   - ***private.ppk*** is the file containing the private key.
   - ***ngc-ip*** is the IP address of the Log Collector.

   The system displays a prompt and some choices.
3. At the prompt, you can enter any of the following options:

   - **g**: Global. If you enter 'g', the fingerprint is installed in the system environment, which is visible to all users. Note that if you enter the global value, you do not need to run the SFTP service as the user that installed the agent: any user can run the SFTP service.
   - **l**: Local. If you enter 'l', the fingerprint is stored in the HKEY_LOCAL_USER registry hive, visible only to the currently logged-in user (and Admins).
   - **n**: Cancel. Cancels the registration procedure.
4. At the **psftp** prompt, type **quit**, and press ENTER.

Configure the SA Upload Directories

After you have added and configured the event source using the Security Analytics GUI, you must configure the upload directories correctly.

1. Change to the /var/netwitness/logcollector directory.
2. Change the owner of the upload directory to the **sftp** user:
   `chown stfp upload`
3. Change the group for the upload directory to the **sftp** user:
   `chgrp -R sftp upload`
4. Ensure the /upload directory has the correct permissions:
   `chmod -R 775 /var/netwitness/logcollector/upload`
5. **Optional:** Set up a cron job to run the script at the time intervals that you wish. If you set up a cron job, make sure to run it as that **sftp** user.

Start SA SFTP Agent Service from Windows Services Control Panel

1. Type **services.msc** on the command line.
2. Start the SA SFTP Agent service.

Parameters

The following parameters are available in the SFTP configuration file.

Parameter	Description
agent.logginghost	Hostname or IP address of the Log Collector to which the logs will be sent.
dir0	Location of the log files for the event sources on your local Windows system.
dir0.filespec	Files that you want to send to the Log Collector from the above location. In this example, any file with the ***.log** extension is sent to the Log Collector.
dir0.interval	Amount of time between file transfers. You can modify this value.
dir0.has_header	If the log has a header at the top of the log file, set this to **true**. If the log file does not have a header, set it to **false**.

Parameter	Description
dir0.compression	Value can be **true** or **false**. If **true**, the system compresses the log files before sending them in a **.gz** format to the Log Collector.
dir0.enabled	Value must be **true**. If you set this value to **false**, the agent does not send any log files to the Log Collector.
dir0.ftp	***Log Collector-ip-address*,sftp,sftp,*publickey*,*//upload/event-source-type/*filedirectory**
dir0.delete_after_read	Value can be **true** or **false**. **true** deletes the files after the agent sends the logs to destination.
dir0.removeemptylines	Set to **true** to strip extra line delimiters before they are passed to the collector. The default is **false**. Windows DNS records contain blank line spaces. Currently, the Log Collector does not strip these but rather, creates a new event with an empty header.
dir0.exclusionfile	Discards any records that contain a specified string (case sensitive). Some log files, such as the Microsoft DHCP log, can add a lot of unneeded records. Set the value to the name of the file that contains the string to exclude. Syntax: **dir0.exclusionfile=*filename*** where ***filename*** is a plain text file. Save the file in the SA SFTP Agent installation directory. The file should contain a list of strings, one per line, to be excluded. **Caution:** The exclusion file strings must not be ambiguous, and the final line of the file must be blank.

Note: The parameters, **removeemptylines** and **exclusionfile** incur additional CPU overhead on the client side, thus we recommend that you use them only when needed. However neither incur any additional memory usage on the client.

Troubleshoot the SA SFTP Agent

The SA SFTP agent installation directory contains an executable file, **AgentLogger.exe**. You can run AgentLogger from the command line. It logs everything passing through localhost port 600 (the default logging port for the SA SFTP agent). This is useful for debugging the agent without the need to stop the service.

Alternatively, you can first stop the service, and then run a command to view debugging messages.

To troubleshoot the SA SFTP Agent by stopping the service:

1. Stop the SA SFTP Agent Service from the Windows Services window.
2. Open a new command shell and change directories to the **SA SFTP Agent** installation directory.
3. Type:

   sasftpagent -v
4. Review the debug messages that are displayed.

   The following sections describe some possible messages and how to fix the corresponding issues.

Error Opening SFTP Agent Configuration File

If the SFTP configuration file is missing, you get the following error:

Error opening file: sftpagent.conf

To resolve the issue, find or recreate the file and move it to the SA SFTP Agent installation directory.

Private Key Issues

If there is a problem with the generation of the key files, you may receive a message similar to the following:

Reading private key file "private.ppk"
Unable to use this key file (unable to open file)
Unable to use key file "private.ppk" (unable to open file)

Or, you may receive a message like the following if there is a key issue:

Offered public key
Server refused our key
Server refused public key

To resolve the issue, regenerate the key pairs and push the key to the Log Collector.