NetWitness® Platform XDR

Install and Update the SFTP Agent

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

November, 2022

Contents

Overview

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

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

RSA recommends that you use **RSA NetWitness Secure FTP Agent**, which you can download from the RSA Link Customer Support website. The SFTP Agent on RSA Link 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**.

Install and Update the SA SFTP Agent

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

I. Install SA SFTP Agent on Event Source.

II. Set Up SA SFTP Agent on Event Source.

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

IV. Select User Account to Run SA SFTP Agent Service.

V. Cache Keys for Connection.

VI. Start SA SFTP Agent Service from Windows Services Control Panel.

Install SA SFTP Agent on the Event Source

Caution: You must use the RSA NetWitness Secure FTP Agent.

To install silently from the command line, see below.

To install the SA SFTP Agent on the event source:

1. Navigate directly to the RSA NetWitness SFTP Agent Downloads URL on RSA Link: https://community.netwitness.com//t5/netwitness-platform-downloads/rsa-netwitness-sftp-agent-downloads/ta-p/565267

   Note: You need to log on with credentials supplied to you by RSA.

2. Choose your OS:
   - For a Windows client, click **RSA NetWitness SFTP Agent** to download the binaries.
   - For a UNIX client, click **RSA NetWitness Unix SFTP Agent** to download the binaries.
3. Complete the rest of these instructions to install the SFTP Agent onto the event source.

Note: If the installation fails, try manually downloading the Microsoft Visual C++ 2013 Redistributable Package from http://download.microsoft.com/download/2/E/6/2E61CFA4-993B-4DD4-91DA-3737CD5CD6E3/vcredist_x86.exe, and installing it.

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. Sample configuration files are located within the sasftpagent directory. These samples are named according to the corresponding event source. For example the Microsoft IIS event source sample SFTP configuration file is named **sftpagent.conf.microsoftiis**.
3. Create the file `C:\sasftpagent\sftpagent.conf`, and use the appropriate sample file, setting the following values:

```
agent.logginghost=log_collector_IP_address
dir0=C:\test
dir0.filespec=*.log
dir0.interval=60
dir0.has_header=false
dir0.compression=false
dir0.enabled=true
dir0.ftp=log_collector_IP_address,sftp,sftp,publickey,//upload/event-source-type/file-dir
dir0.delete_after_read=true
```

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

4. Save the file, making sure the file name stays the same (that is, make sure not to append a **.txt** extension to the file).

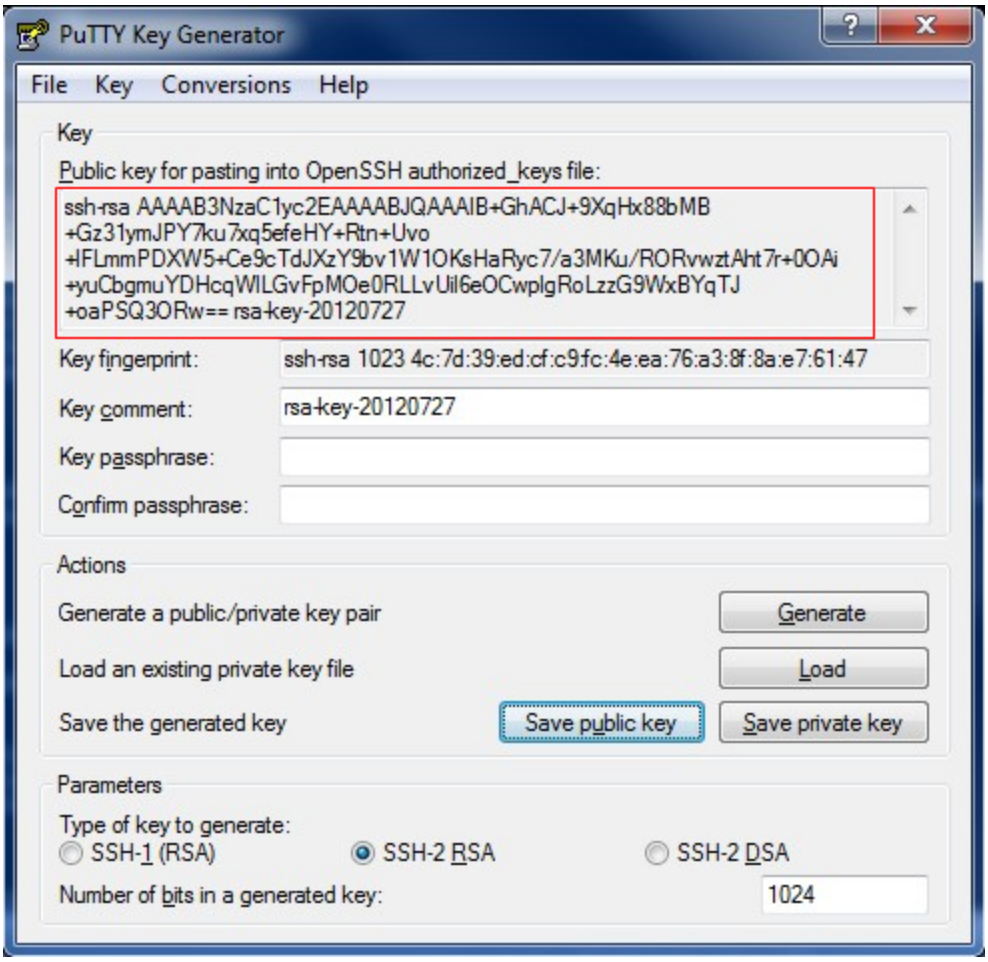
> **Note:**
> - For more information about the parameters, see SFTP Parameters.
> - To view the examples, go to Example Configuration Files.

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 RSA NetWitness Platform as described in step 5b.

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



b. Paste the public key from your buffer into the Eventsource SSH Key parameter in RSA NetWitness Platform. For details, see the **Configure File Event Sources** topic in the *RSA NetWitness Platform Log Collection Guide*.

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 ***log_collector_IP_address***`

   where:

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

   The system displays a prompt and some choices.
3. After the prompt, you can enter any of the following options:
   - **y**: To start the registration procedure: another prompt is displayed.
     - **y**: Global install: If you enter 'y', the fingerprint is installed in the system environment, which is visible to all users.

       Note: 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.

     - **n**: Local install. If you enter 'n', the fingerprint is stored in the `HKEY_CURRENT_USER` registry hive, visible only to the currently logged-in user (and Administrators).
   - **n**: Cancels the registration procedure.

IMPORTANT: If you do not see these options, then you might be running an outdated version of the SFTP Agent: the most recent agent is available on RSA Link on the RSA NetWitness SFTP Agent Downloads page.

4. At the `psftp` prompt, type **quit**, and press ENTER.

The key is now cached in the registry of the event source.

Note: If you encounter the error message `No supported authentication methods available (server sent : publickey)`, see https://community.netwitness.com/t5/netwitness-knowledge-base/problems-with-sftp-agent-certificate-exchange-on-windows-for-rsa/ta-p/677135.

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.

Example Configuration Files

The following are examples of the sftpagent.conf file for various event sources.

An example configuration file for setting up a Microsoft IIS server:

```
agent.logginghost=log_collector_IP_address
dir0=C:\inetpub\logs\LogFiles\W3SVC1
dir0.filespec=*.log
dir0.interval=60
dir0.has_header=false
dir0.compression=false
dir0.enabled=true
dir0.ftp=log_collector_IP_address,sftp,sftp,publickey,//upload/iis_tvm/IIS
dir0.delete_after_read=true
```

An example configuration file for setting up an Apache event source:

```
dir0=C:\Program Files\Apache Group\Apache2\logs
dir0.filespec=access_log*
dir0.interval=60
dir0.has_header=false
dir0.compression=true
dir0.enabled=true
dir0.ftp=10.100.229.182,nic_sshd,publickey,APACHE_10.10.31.155
```

SFTP Parameters

The following table describes all of the available parameters.

Parameter	Description
agent.logginghost	Hostname or IP address where the SFTP agent is installed. When this setting is enabled with the Log Collector IP address, the Log Collector collects the agent's debug logs on port 514. The debug logs collected are displayed in the NetWitness **Investigate** Page for a different device type. **Note:** - You must disable this setting to avoid debug logs collection. - Enable this setting only if you encounter any issues.
dir0	Location of the logs files for the event sources on your local windows system.
dir0.compression	Value can be **true** or **false**. • Set to **true** to use compression. Log files are compressed and then sent in a **.gz** format to the Log Collector. • Set to **false** to not use file compression.
dir0.delete_after_read	Value is either **true** or **false**. Value of **true** deletes the files after the agent sends the logs to destination.
dir0.enabled	Value is set to **true**. Do not modify this value because if you change it to **false**, you do not send any log files to the Log Collector.
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.
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.

Parameter	Description
dir0.ftp	***Log Collector-ip-address***,sftp,sftp,***publickey***,***//upload/event-source-type/filedirectory*** This path can be found on the Log Collector within the following path: /var/netwitness/logcollector/upload/ Appended to the end of that path is the value you enter for the **File Directory** parameter when you create the event source in the RSA NetWitness Platform User Interface.
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**.
dir0.interval	Amount of time between file transfers. You can modify this value.
dir0.psftptimeout	This value is the time, in seconds, for the psftp process to timeout. By default, there is no timeout. RSA recommends that you not set this to less than 5 seconds. If you need to set it, 30 seconds is recommended.
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.

The **removeemptylines** and **exclusionfile** parameters 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

To troubleshoot, you must first stop the service, and then run a command to view debugging messages.

To troubleshoot the SA SFTP Agent:

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.