



APIUS
technologies

Introduction

Main goal of Apius SSHFS Helper is to provide easy way to access and monitor files without using SplunkForwarder on remote, production servers. SSHFS Helper requires only user account with read rights to log files on remote servers and of course ssh daemon running. After you set up connection, the only thing you need to do, is to configure file monitor input as you would do on local file system.

Apius SSHFS Helper does not require Splunk to be run on root account. It takes care on all mount points be restored as soon as you restart Splunk or reboot server.

Prerequisites

Apius SSHFS Helper requires following packages on a server, where you plan to install it:

- Linux 2.6 (product was tested on Ubuntu Server, but all distributions should also work OK)
- OpenSSH client including: ssh, ssh-keyscan and ssg-keygen,
- fusefs support in kernel,
- fusermount tool,
- sshfs package installed

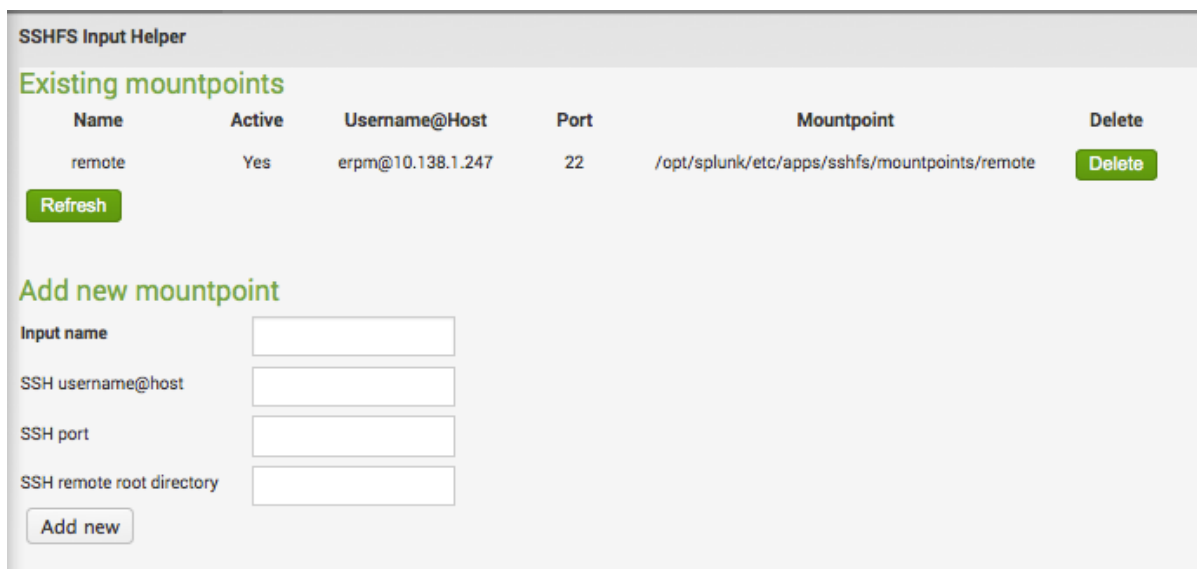
Apius SSHFS Helper can not be installed in Splunk Universal Forwarder, but you may use it with Heavy Forwarder.

Usage

Apius SSHFS Helper may be configured using application's user interfaces, as standard input (Settings » Data Inputs) or with inputs.conf file. Preferred method is using application's GUI.

SSHFS Helper supports password and private key authentication. Configuration procedure is following:

1. Install application using provided sshfs.spl file and allow Splunk to restart afterwards.
2. Choose Apius SSH Helper app. You will see screen similar to one below:



The screenshot shows the 'SSHFS Input Helper' web interface. It has a title bar 'SSHFS Input Helper'. Below it, the section 'Existing mountpoints' contains a table with columns: Name, Active, Username@Host, Port, Mountpoint, and Delete. There is one row for 'remote' with 'Yes' in the Active column, 'erpm@10.138.1.247' in Username@Host, '22' in Port, and '/opt/splunk/etc/apps/sshfs/mountpoints/remote' in Mountpoint. A 'Delete' button is next to the Mountpoint. Below the table is a 'Refresh' button. The section 'Add new mountpoint' has four input fields: 'Input name', 'SSH username@host', 'SSH port', and 'SSH remote root directory'. An 'Add new' button is at the bottom.

Name	Active	Username@Host	Port	Mountpoint	Delete
remote	Yes	erpm@10.138.1.247	22	/opt/splunk/etc/apps/sshfs/mountpoints/remote	Delete

Refresh

Add new mountpoint

Input name:

SSH username@host:

SSH port:

SSH remote root directory:

Add new

- Enter correct values for all entries and press **Add new** button.
- If everything is correct, you will be presented with next screen, where you have to provide credentials (password or private key). Verify fingerprint of server's key, choose authentication method and then type your password or paste private key in a field. Press **Add this host**.

SSHFS Input Helper

Add a new SSH connection

Enter private key or SSH password

☒ Enter private key
☐ Enter password

Details

Key Type	Fingerprint	Key length
RSA	b5:a5:e1:25:63:fd:b7:fc:b8:a6:58:8d:67:e7:d4:22	2048
DSA	78:bf:d3:5e:70:78:ed:ab:d6:df:da:cf:a5:4a:ed:07	1024
ECDSA	03:f1:9a:05:ca:b7:fe:18:32:be:02:83:07:e2:9e:47	256

Please check these fingerprints. Enter password or private key **only** if they identify host that you want to connect to.
Make sure that you have secure connection with Splunk Web Server

Add this host

- Next screen will show you all your connections. Copy to clipboard **mountpoint** of your connection and proceed as usual to configure file monitor input: **Settings » Data inputs » Files & directories**

Name	Active	Username@Host	Port	Mountpoint	Delete
remote	Yes	erpm@10.138.1.247	22	/opt/splunk/etc/apps/sshfs/mountpoints/remote	Delete
test	Yes	splunk@10.138.1.247	22	/opt/splunk/etc/apps/sshfs/mountpoints/test	Delete

- Path of the data you want to index will start with directory you have in clipboard.

Remarks

If you want to provide private key without using application's GUI (using Settings » Data Inputs menu or directly within inputs.conf) enter it without spaces, newlines and headers. If you have id_rsa, id_dsa or id_ecdsa file, you need to convert it using simple unix command:

```
cat ~/.ssh/id_rsa | grep -v "PRIVATE KEY-----" | tr -d '\n' | sed 's/$/\n/g'
```

Additionally you have to accept server public key in your OS, before saving a new input using account on which splunkd is running. To do so simply connect to the server with 'ssh' command and accept host fingerprint.

Every secret(password or private key) is replaced with '<stored>', after adding/modifying the input. If you want to change stored secret - replace '<stored>' with a new one (it will be encrypted after saving input). Please read <http://blogs.splunk.com/2011/03/15/storing-encrypted-credentials> , to know how does Splunk store credentials.

Activated input will keep remote filesystem mounted. It does not output any events and do not need any index. You can monitor files and directories in remote filesystem, as if they were local.

Limitations

Always enable input before removing it, even when credentials are incorrect. Stored password or private key won't be removed if you delete disabled input.

Inputs.conf

```
[sshfs://<name>]
address = <ip address or host name>
port = <port>

# Enter IP or hostname and port you want connect to.

auth = PASS

#Enter how do you want to authenticate. You have to specify private key
#type if you enter it, otherwise leave this field empty. Allowed values:
#PASS, ECDSA, RSA, DSA. Default value is PASS. Any other value is ignored

dir = <path on remote server>

#Enter the remote directory you want to mount locally. This allows you to
#limit the visible part of a remote filesystem. Defaults to / (whole
#remote filesystem).

user = <username>

#Enter user name on remote server

password = <password>
privkey = <privatekey>

#Enter password or private key for SSH connection here.
#Only one of these fields is required, and you have to provide exactly
#one of them. After saving input (and enabling it) - it will be
#encrypted, and secret (password or private key) will be replaced with
# '<stored>'. Don't enter both private key and password, just one of them!
```

Changelog

v0.9

- Initial public beta release

Support

If you have any problems using our app please contact us on: splunk@apius.pl.