SFTP Public Key Authentication Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	ASR 5500 VPC-DI VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide*

Revision History

Note Revision history details are not provided for features introduced before releases 21.2 and N5.5.

Revision Details	Release
Added support for SFTP public key-based authentication. Refer to the *SFTP Public Key Authentication Support* section for more information.	21.24
New functionality was added to replace or supplement the configured bulkstats schema with the option of preserving bulkstats configuration parameters. New functionality was added to collect bulkstats samples in the SSD. Refer to the *Collecting Bulk Statistics Samples in SSD* section for more information. The **bulkstat** Global Configuration Mode command added the **config [schema | supplement]** keywords to enable this functionality. Refer to the *Configuring a Separate Bulkstats Config File* section for more information. **show configuration bulkstats brief** command output was expanded to include all bulkstats configuration details except for schema.	21.3
First introduced.	Pre 21.2

Feature Description

The SFTP supports public key based authentication for bulk statistics transfer in StarOS. To ensure adherence to better security practices, the StarOS based products must not use the password-based mechanism for transferring bulk statistics to external servers. This feature allows the use of SSH keys instead of passwords. The bulk statistics transfer mechanism involves the following steps:

1. Generate the private and public RSA key pair.

   For more information, see the *Configuring SSH Options > SSH Client Login to External Servers > Generating SSH Client Key Pair* section in the *Getting Started* chapter of the *ASR 5500 System Administration Guide*.

2. Push the the public key to an external bulk statistics server.

   For more information, see the *Configuring SSH Options > SSH Client Login to External Servers > Pushing an SSH Client Public Key to an External Server* section in the *Getting Started* chapter of the *ASR 5500 System Administration Guide*.

   Steps 1 and 2 are existing mechanisms and are required only once.

3. Transfer the bulk statistics files using the keys that are exchanged in steps 1 and 2.

   For more information, see the *Configuring SFTP Public Key Authentication* section.

For more information, see the *ASR 5500 System Administration Guide*.

Configuring SFTP Public Key Authentication

To configure the SFTP public key for bulkstats transfer, use the following sample configuration in the Bulk Statistics Configuration mode.

```
config
  bulkstats mode
    receiver { mode { redundant | secondary-on-failure } | ip_address {
primary | secondary } [ mechanism { { ftp login user_name [ encrypted ]
password pwd } | sftp login user_name user_name { public-key | [ encrypted
] password pwd } | tftp } } ] }
    end
```

NOTES:

- **mechanism { { ftp login** *user_name* **[encrypted] password** *pwd* **} | sftp login user_name** *user_name* **{ public-key | [encrypted] password** *pwd* **} | tftp }**
  - **sftp login user_name** *user_name* **{ public-key | [encrypted] password** *pwd* **}**: Specify the SFTP protocol for data file transfer. *user_name* specifies the remote system secure login and must be an alphanumeric string of 1 through 31 characters. *pwd* specifies the password to use for remote system authentication and must be from 1 to 31 characters or 1 to 64 characters if the **encrypted** keyword is also specified. **public-key** enables public-key based authentication for bulk statistics transfer.

For example:

```
[local]laas-setup# configure
[local]laas-setup(config)# bulkstats collection
[local]laas-setup(config)# bulkstats mode
[local]laas-setup(config-bulkstats)# sample-interval 1
[local]laas-setup(config-bulkstats)# transfer-interval 1
[local]laas-setup(config-bulkstats)# receiver 10.84.43.64 primary mechanism
sftp login root public-key
[local]laas-setup(config-bulkstats)# remotefile format
/localdisk/sftpkey/bulkstat_counter%date%%time%.txt
[local]laas-setup(config-bulkstats)# gtpc schema gtpcSch4 format
PPM,%epochtime%,%localdate%,%localtime%,%uptime%,%vpnname%
[local]laas-setup(config-bulkstats)# end
[local]laas-setup#
```

Verifying the Configuration

Use the following show command to verify the configuration.

show configuration bulkstats

For example:

```
[local]laas-setup# show configuration bulkstats
config
  bulkstats collection
  bulkstats mode
    sample-interval 1
    transfer-interval 1
    file 1
      remotefile format /localdisk/sftpkey/bulkstat_counter%date%%time%.txt
      receiver 10.84.43.64 primary mechanism sftp login root public-key
     gtpc schema gtpcSch4 format PPM,%epochtime%,%localdate%,%localtime%,%uptime%,%vpnname%

    #exit
  #exit
end
[local]laas-setup#
```