[SFTP] Invalid Sftp credential provided for 'SshPublicKey' authentication type

Last updated by | Jackie Huang | Jan 4, 2022 at 12:24 AM PST

201030- [SFTP] Invalid Sftp credential provided for 'SshPublicKey' authentication type		ASC Onboard	

Monday, December 18, 2017
11:22 AM

SME	
Symptoms	Customer is using SshPublicKey auth but hit Invalid Sftp credential provided for 'SshPublicKey' authentication type.
Cause	There are three possible root causes could lead this error 1. Private key content is set from AKV/SDK but they are not encoded correctly 2. Wrong key content format 3. Invalid credential or private key content

Resolution	Please follow below steps to figure out the right solution
	
	1. If private key content is from AKV and original key file can work if customer upload it directly to SFTP linked service
	As described in https://docs.microsoft.com/en-us/azure/data-factory/connector-sftp#using-ssh-public-key-authentication , the privateKeyContent is a Base64 encoded SSH private key content.
	You should encode the **whole content of original private key file** with base64 encoding and store the encoded string to AKV. We have some customers decode their key content and then encode the key content again, that is wrong, don't do anything to the original private key file, treat it as a black box and encode all content of this file. Original private key file means the one that can work on SFTP linked service if you click on upload from file.
	
	To generate such string, customer can use below 2 ways:
	● Using C# code
	  byte[] keyContentBytes = File.ReadAllBytes(privateKeyPath);
	  string keyContent = Convert.ToBase64String(keyContentBytes, Base64FormattingOptions.None);
	● Using Python code
	  import base64
	  rfd = open(r'{Your private key file}', 'rb')
	  keyContent = rfd.read()
	  rfd.close()
	  print base64.b64encode(keyContent)
	● Using 3rd party base64 convert tool
	  Paste the whole private key content to such tool (like https://www.base64encode.org/) and encode to a base64 format string. Paste this string to key vault
	
	2. If customer's key is using PKCS#8 format ssh private key
	Customer is using PKCS#8 format SSH private key to access SFTP server, but this format is not supported in ADF. ADF supports the traditional SSH Key format. In detail, the difference between PKCS#8 format and traditional Key format is PKCS#8 key content starts with "-----BEGIN ENCRYPTED PRIVATE KEY-----" while traditional key format starts with "-----BEGIN RSA PRIVATE KEY-----".
	
	please let customer run below commands to convert the key to traditional key format:
	
	openssl pkcs8 -in pkcs8_format_key_file -out traditional_format_key_file // decrypt the pkcs8 key and convert the format to traditional key format
	chmod 600 traditional_format_key_file
	ssh-keygen -f traditional_format_key_file -p // re-encrypte the key file using passphrase
	
	(Above commands should be conposed in one line)
	3. Elsewise
	Suggest customer to double check if their key file or password is correct using other tools (like winscp) and get back to us if other tool can succeed

More Information	
Tags	SFTP

How good have you found this content?