**PowerShell scripting/Jenkins-Debug**

**Question #1:** PowerShell scripting

Get the path of the first .log file on your C:\ drive that has no characters on the first line of the file.

Code:

cd C:\

Get-ChildItem -path \*.log -Recurse | ForEach-Object {

[pscustomobject] @{

Name = $\_.Name

Status =

('1stLine\_Empty', 'NotEmpty')[([string]::IsNullOrEmpty((Get-Content $\_.Name -First 1)))]

}

}

##########################################################################################################################################################################

**Question #2:** Jenkins troubleshooting

You log into Jenkins to start the work day and see multiple pipelines are failing with the following error, what happened / how do you resolve it?

"Failed to connect to repository : sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target"

**\* Failed to connect to repository**

Problem-Description:

This error generally occurs while there is any connectivity issue happen between the Jenkins and the repository tool like github or any.

Debug/resolution:

In such scenario, need to debug where the connection is blocked, we can try telnet and ping from jenkins serevr to the respective target repository.

* In the manage jenkins we can check the respective git-api path.
* We can check the git-functional user credentials.
* Set git-executable path in manage jenkins.
* If there is ssh connectivity between jenkins and git then check the respective ssh keys permissions and owner, it should be owned by jenkins user.

**\* sun.security.validator.ValidatorException: PKIX path building failed**

Problem-Description:

Attempting to access applications or websites that are encrypted with SSL (for example HTTPS, LDAPS, IMAPS) throws an exception and the connection is refused. This can happen when attempting to establish a secure connection.

The way trust is handled in Java is that you have a truststore (typically $JAVA\_HOME/lib/security/cacerts). The truststore contains a list of all known Certificate Authority (CA) certificates, and Java will only trust certificates that are signed by one of those CAs or public certificates that exist within that truststore.

Resolution:

* Make sure you have imported the public certificate of the target instance into the truststore according to the Connecting to SSL Services instructions.
* Make sure any certificates have been imported into the correct truststore; you may have multiple JRE/JDKs. See Installing Java for this.
* Check to see that the correct truststore is in use. If -Djavax.net.ssl.trustStore has been configured, it will override the location of the default truststore, which will need to be checked.
* If this error results while integrating with an LDAP server over LDAPS and there is more than one LDAP server, then deselect the Follow referrals option within the LDAP user directory configuration per Connecting to and LDAP Directory. Optionally, import the SSL certificates from the other LDAP servers into the Confluence truststore.
* Check if your Anti Virus tool has "SSL Scanning" blocking SSL/TLS. If it does, disable this feature or set exceptions for the target addresses (check the product documentation to see if this is possible.)
* If connecting to a mail server, such as Exchange, ensure authentication allows plain text.
* Verify that the target server is configured to serve SSL correctly. This can be done with the SSL Server Test tool.
* If all else fails, your truststore might be out of date. Upgrade Java to the latest version supported by your application.

**\* sun.security.provider.certpath.SunCertPathBuilderException**

Problem-Description

This is caused when the Java environment does not have information about the HTTPS server to verify that it is a valid website. Sometimes the certificate is provided by an internal Root CA or is a Self-Signed Certificate. This sometimes can confuse the JVM as it is not one of the ones on the Java “trusted” list who can provide these certificates.

Resolution

* you’ll find two commonly recommended solutions. The first, which is both the most onerous and the most technically correct is to update the security certificate catalog used by the embedded Jetty web container and the underlying JDK.
* If security is not a core concern in this box, you may in Jenkins web UI go to Manage Jenkins > Manage Plugins > tab Available and search for "skip-certificate-check" plugin.

**\* unable to find valid certification path to requested target**

This error message seems the same with previous statement i.e "sun.security.provider.certpath.SunCertPathBuilderException"