**Working with Certificate and Local Configuration**

Before you begin the tasks, review the following articles:

* [Boot diagnostics](https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/boot-diagnostics)
* [SSL/TLS Certificate File Types](https://blogs.msdn.microsoft.com/kaushal/2010/11/04/various-ssltls-certificate-file-typesextensions/)
* [Service Accounts](https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts)

1. Via PowerShell script get Azure VM **Boot Diagnostics** and filter some string to print out to the console.
2. Write a firewall rule to open port 443 in the deployed Windows VM.
3. Create PowerShell script to import pfx certificate with a password to the 'cert:\LocalMachine\My' location and get thumbprint for this certificate. You may have to create the starting certificate from which to import pfx.
4. Download 7z with PowerShell script and use the 7z.exe file to extract any zip archive file.
5. Write a function which will change any parts of the strings inside of this function.
6. Write a function that takes the first parameter as the path to the file, the second and third parameters as a string and changes certain lines within this file with the value of the second and third parameters.
7. Create a PowerShell script to create a new local user with a password in the Windows virtual machine.
8. Create a PowerShell script to create a new local user with a password in the Windows virtual machine and give ‘Logon As Service’ permission for this user.
9. Create a PowerShell script to create a new folder and give ‘Full Control’ access to the user that was created in task 7.
10. (disabled) Create a PowerShell script to give ‘Service Control’ access to the user that was created in task 7 [Grant Users Rights to Manage Services](https://social.technet.microsoft.com/wiki/contents/articles/5752.how-to-grant-users-rights-to-manage-services-start-stop-etc.aspx) .