Runbooks

What to do when faced with certain types of incidents or non prod support issues

NTLM is not working for a VM hosted application

What is NTLM? a legacy network authentication protocol that was prominent in the 1990s era (older than some engineers here). https://www.google.com/url?sa=i&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fopenspecs%2Fwindows_protocols%2Fms-apds%2F5bfd942e-7da5-494d-a640-f269a0e3cc5d&psig=AOvVaw0HJHZ6n5W-OCHex4EEvzrs&ust=1626134054097000&source=images&cd=vfe&ved=0CAoQjRxqFwoTCPCS3sib3PECFQAAAAAdAAAAABAD

Why do we need to support this legacy technology? because COTS applications still uses NTLM and vendors are unwilling to support kerberos or openID connect which are much more secure protocols with better interop, or the vendor no longer supports the version of the COTS application and BHP is running the application without support.

Typical network deployment:

1. Single Windows 2019 / 2016 VM hosting IIS web application with NTLM network auth enabled.
2. Internal ingress Azure Application gateway V1 SKU deployed in each paired region proxying DNS round robin with the backend target as the windows VM with a timeout of 30 minutes.

Troubleshooting steps:

1. Ensure the IIS only has the 1 option for network authentication:
    a. In IIS Manager
    b. Select your site
    c. Click on the Authentication module
    d. Select Windows Authentication
    e. Select Providers...
    f. Ensure the only option is windows authentication with NTLM being the only provider selected
2. Check that the NTLM local group policy setting allows all forms of NTLM:
    a. The following image shows what the group policy setting should be:
    b. http://woshub.com/wp-content/uploads/2019/09/network-security-lan-manager-authentication-level.png
3. Restart IIS and get the application users to clear cache and restart browser to see if that fixes the issue
4. In some cases the application gateway v1 instances also need to be restarted to terminate any long running http connections. This can be done using the azure cli (you will need to install this if you haven't already)
    a. az login
    b. az network application-gateway stop --name <name of app gateway v1> --resource-group <resource group name> --subscription BHP-Technology-SharedServices
    c. az network application-gateway start --name <name of app gateway v1> --resource-group --resource-group <resource group name> --subscription BHP-Technology-SharedServices
    d. This will take about 20 minutes, and will impact all applications hosted on this app gateway, if there is more than 1 active application then seek approval from all applications for an outage and update the SNOW incident.