SplunkUF via GPO

Sunday, August 18, 2024 11:38 PM

1. Create a software deployment share on your DC
    a. Create a folder on the desktop of your DC, name it software
        i. Rclick > properties > sharing
        ii. Click Share > share to authenticated users and administrators
        iii. apply
    b. Create a folder in the share for the splunk UF and drop necessary files
        i. Rclick > New Folder > Rename: SplunkUF
        ii. Drop files in the new SplunkUF folder
            1) inputs.conf
            2) DeploySplunk.bat
            3) SplunkUninstall.bat
            4) splunkuniversalforwarder.msi (rename the UF to this filename or the .bat files won't work)

        iii. Edit the DeploySplunk.bat file to match your infrastructure
            1) @echo off
            SET FLAG=C:\SplunkFlag.txt
            IF EXIST %FLAG% GOTO END
            echo "SplunkUF Installed" > %FLAG%
            msiexec.exe /i "\\DC01\Software\SplunkUF\splunkuniversalforwarder.msi" DEPLOYMENT_SERVER="192.168.5.20:8089"
            RECEIVING_INDEXER="192.168.5.20:9997" AGREETOLICENSE=Yes SERVICESTARTTYPE=AUTO LAUNCHSPLUNK=1
            SPLUNKUSERNAME=splunk GENRANDOMPASSWORD=1 WINEVENTLOG_APP_ENABLE=1 WINEVENTLOG_SEC_ENABLE=1
            WINEVENTLOG_SYS_ENABLE=1 WINEVENTLOG_FWD_ENABLE=1 WINEVENTLOG_SET_ENABLE=1 PERFMON=network ENABLEADMON=1
            /passive
            copy "\\DC01\Software\SplunkUF\inputs.conf" "C:\Program Files\SplunkUniversalForwarder\etc\system\local\"
            :END

            2) The highlighted portions must be changed or else the file will not work. All filepaths must me changed to your share. all IP addresses must match your infrastructure.

2. Create an OU for the workstations you wish to add the UF to
    a. open the Server Manager
        i. Click Tools
            1) Click the Active Directory Computers and Users
                a) rclick your ad (example doge.AD in this instance)
                    i) Create a new Organizational Unit (OU) for your splunk Deployment (example RedDev)
                b) Open the computers tab to view the AD computers on your domain
                    i) select the computers you want to add to this OU and drag/drop them into the OU

    b. Open to Group Policy Management via the search bar
        i. Navigate to your domain (doge.AD example) and view your OU (RedDev example) that you just created
            1) Rclick > Create a GPO in this domain and link it here… (example SUF Installer)
                a) Rclick the new GPO and edit
                    i) Computer Configuration > Policies > Windows Settings > Scripts > Startup (these scripts must be in this order)
                        1- Add > Name: [Full filepath to the share we made in step 1 (ex. \\DC01\Software\SplunkUF\SplunkUninstall.bat)]
                        2- Add > Name: [Full filepath to the share we made in step 1 (ex. \\DC01\Software\SplunkUF\DeploySplunk.bat)]

    c. run this command in cmd (administrator)
        i. `gpupdate /force`

    d. restart the computers in your OU to apply the GPO

3. OPTIONAL ********** Sysmon install
    a. In your share make a new folder called SYSMON
    b. put sysmon.exe in the folder as well as the DeploySysmon.bat
        @echo off
        SET FLAG=C:\SysmonFlag.txt
        IF EXIST %FLAG% GOTO END
        echo "Sysmon Installed" > %FLAG%
        \\DC01\Software\Sysmon\sysmon.exe -i -accepteula

        :END

    c. change the filepath to point to your share and the sysmon.exe file

d. follow step 2b. but create a SYSMON installer with it as well
e. follow step 2c.