

Maquetación de carpetas y Logs con Event Viewer.

Paso 1: Crear dos carpetas en el disco local C: "C:\", la primera de ellas llamada "Splunk", la segunda "Kaspersky-ESC".

Splunk	9/18/2023 10:40 AM	File folder
Kaspersky-ESC	9/18/2023 9:56 AM	File folder

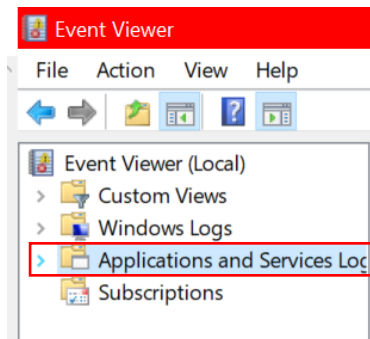
Paso 2: Instalar el archivo ZIP de Splunk y extraerlo en la carpeta creada con su nombre correspondiente "C:\Splunk".

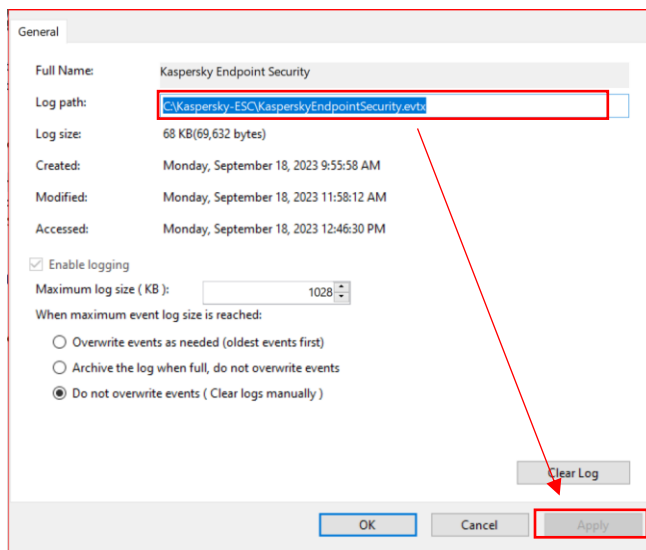
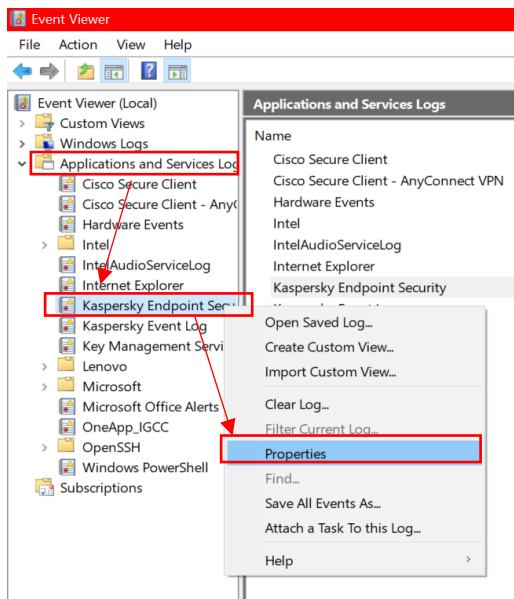
También instalar el driver "splunkclouduf.spl" y enviarlo a esta misma carpeta. Eliminar el archivo adicional de Splunk destinado a la plataforma Linux.


splunkclouduf.spl	9/18/2023 9:11 AM	SPL File	7 KB
splunkforwarder-9.1.1-64e843ea36b1-x64-release.msi	9/4/2023 6:19 PM	Windows Installer Package	82,232 KB

Paso 3: Abrir "Event viewer", desplegar el menu "Applications and services logs", click derecho en "Kaspersky Endpoint Security", "Properties", cambiar el Log path por la siguiente dirección.

"C:\Kaspersky-ESC\KasperskyEndpointSecurity.evtx" presionar "Apply" y cerrar esta ventana. Al terminar este paso se debera crear automáticamente un archivo .evtx en la carpeta creada "Kaspersky-ESC".

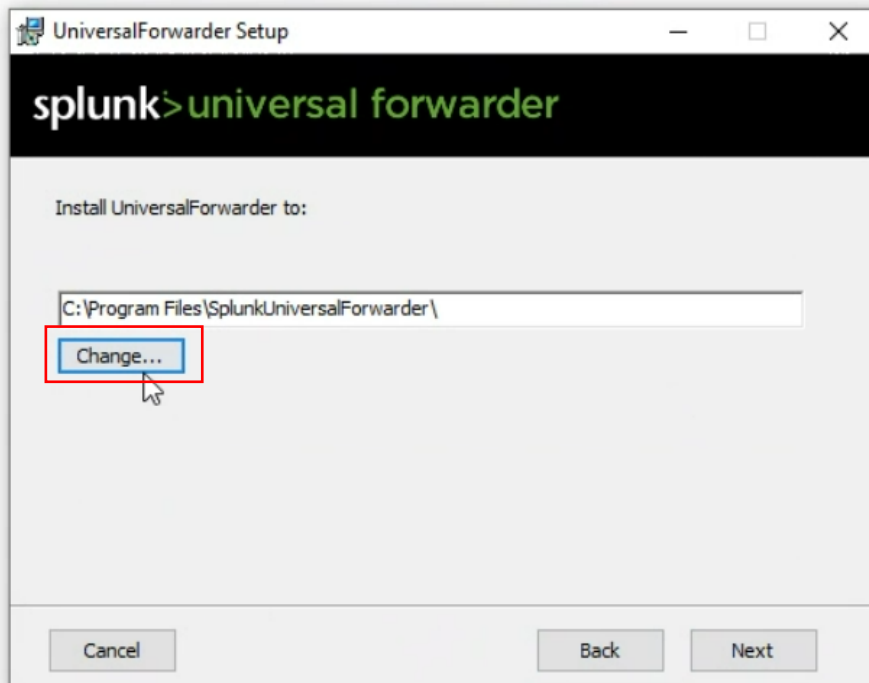
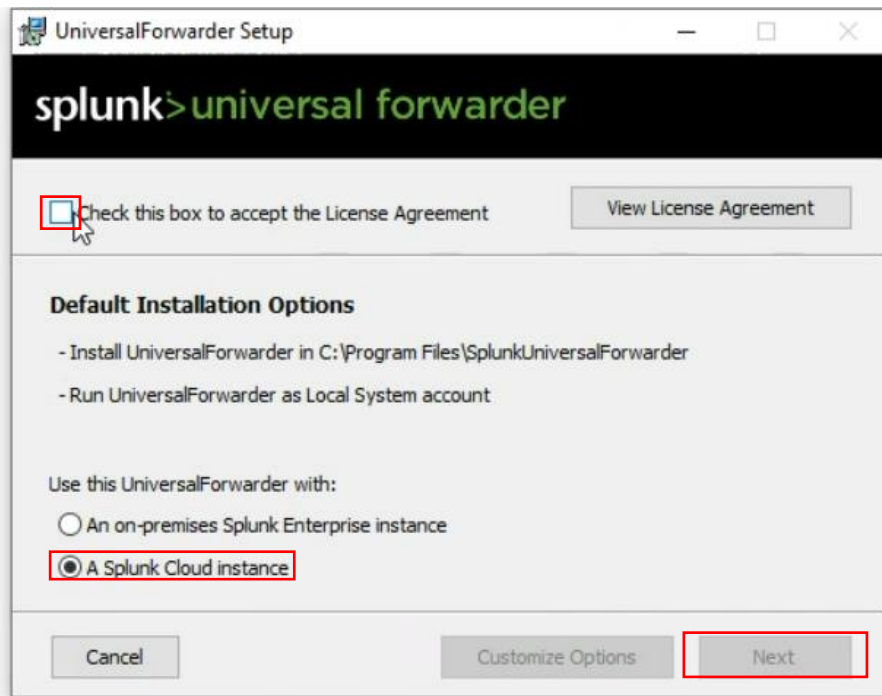


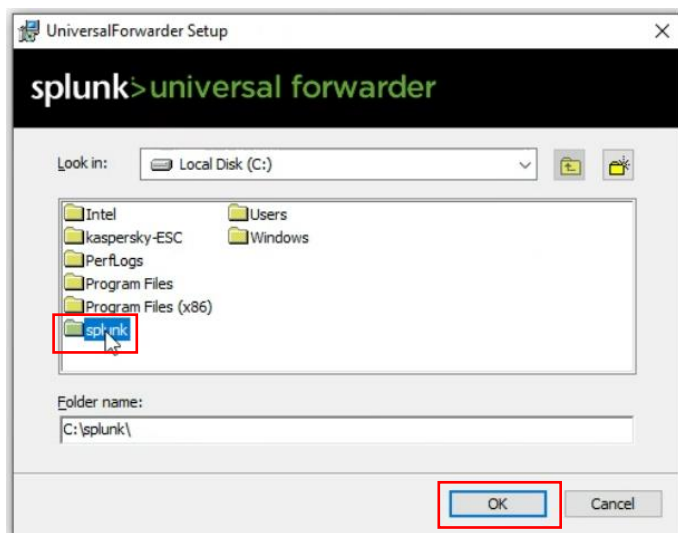
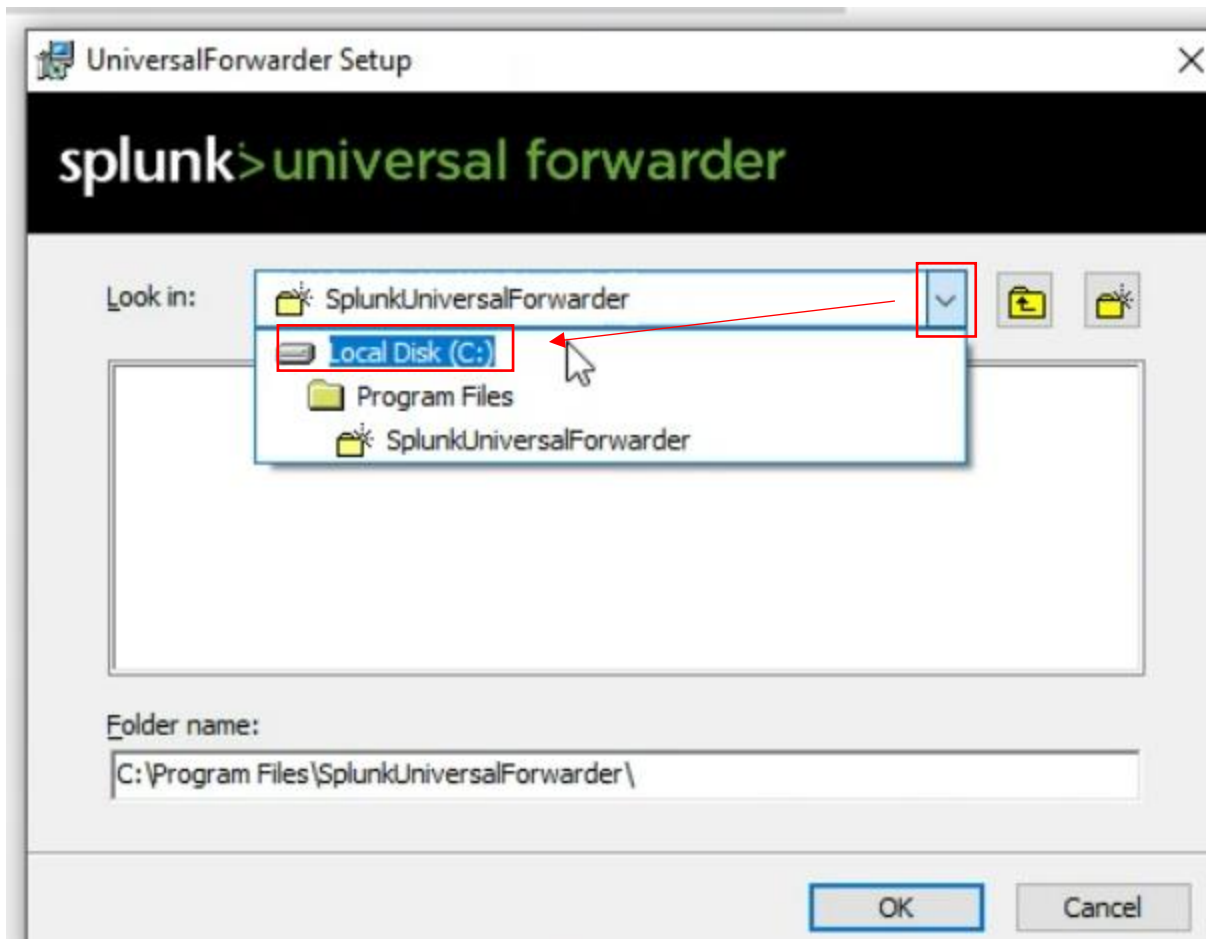


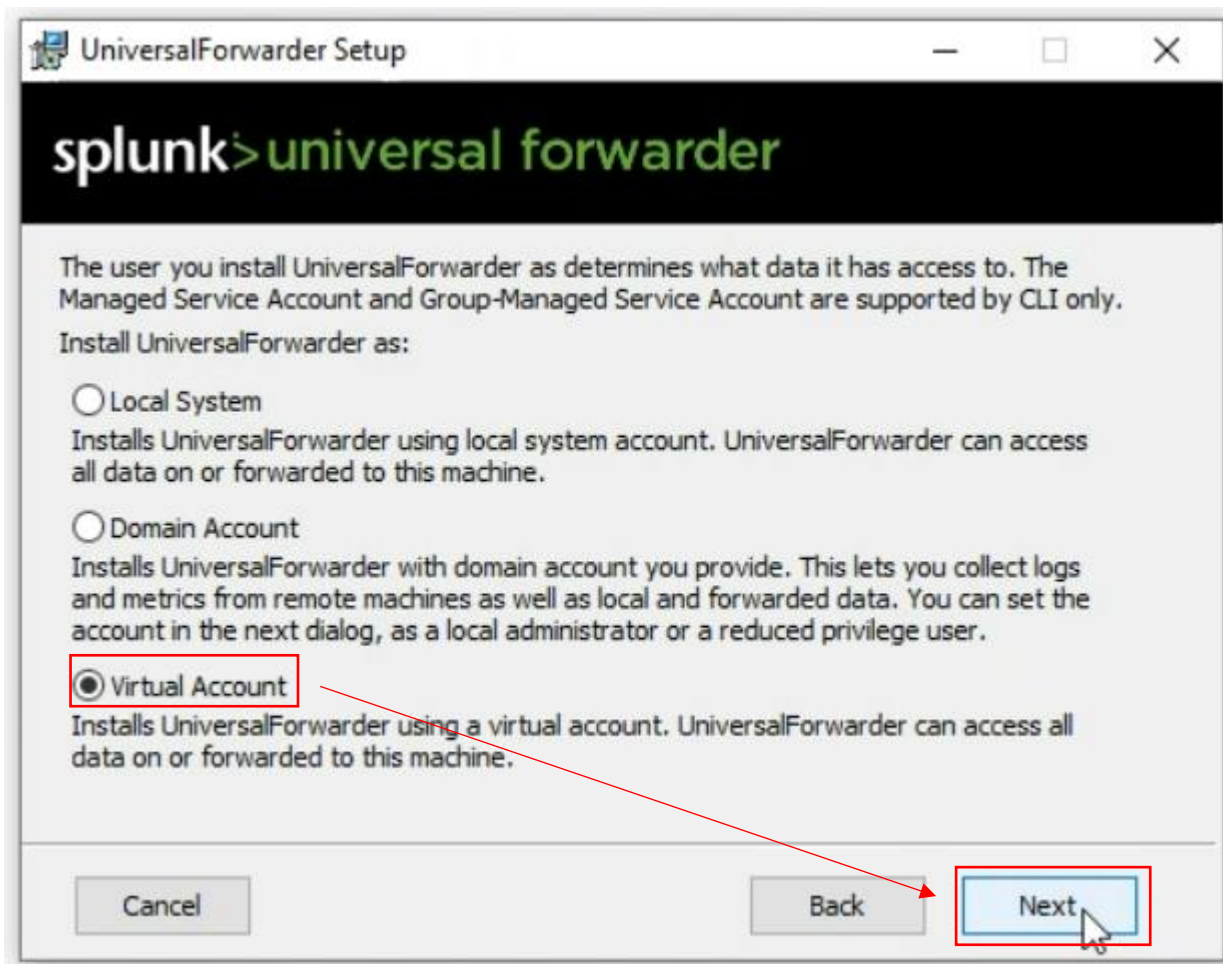
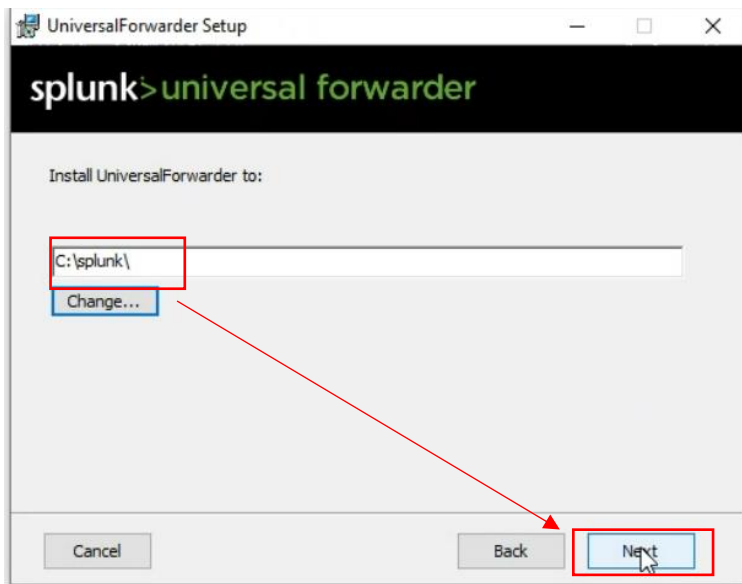
> Local Disk (C:) > Kaspersky-ESC			
Name	Date modified	Type	Size
 KasperskyEndpointSecurity.evtx	9/18/2023 11:58 AM	Event Log	68 KB

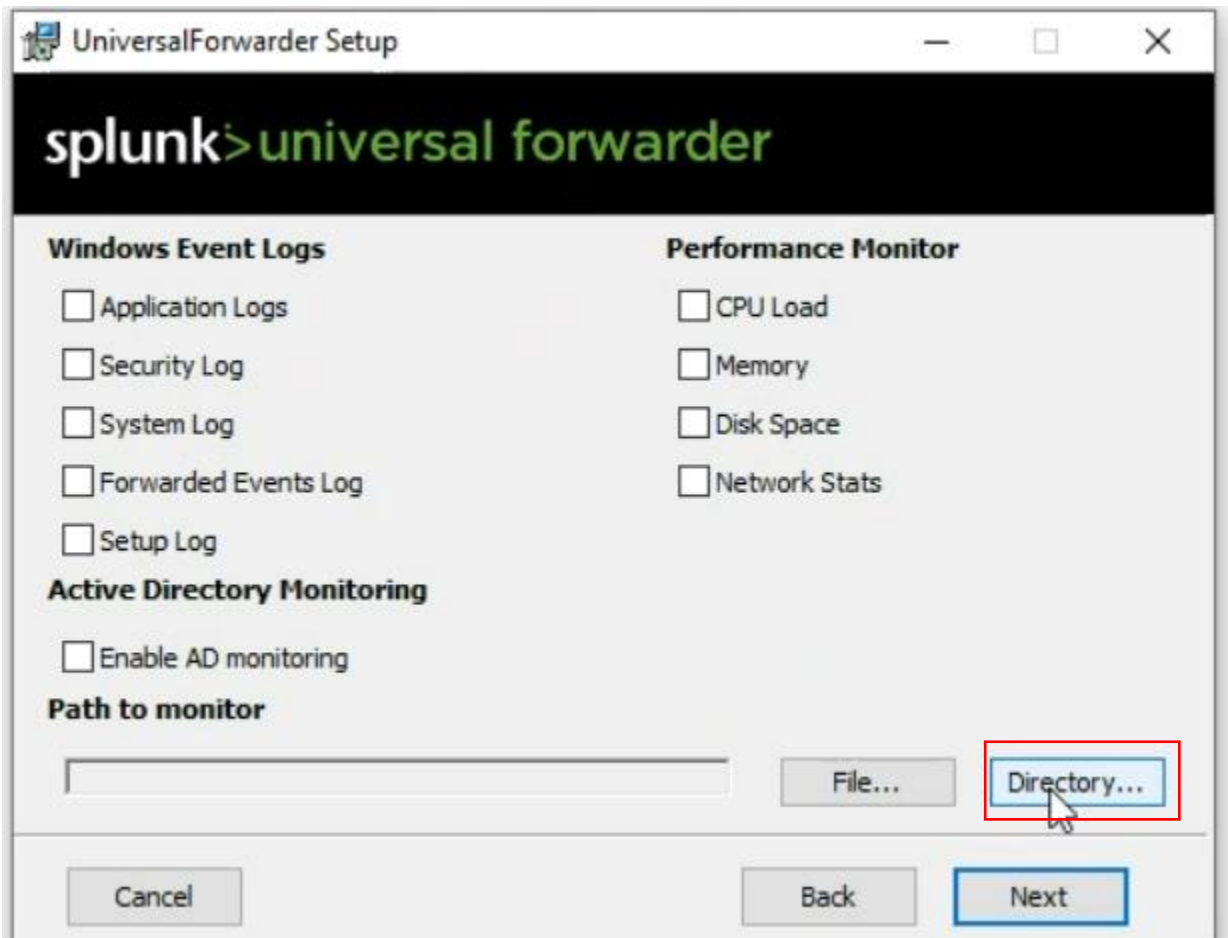
Instalación del Forwarder Universal Splunk

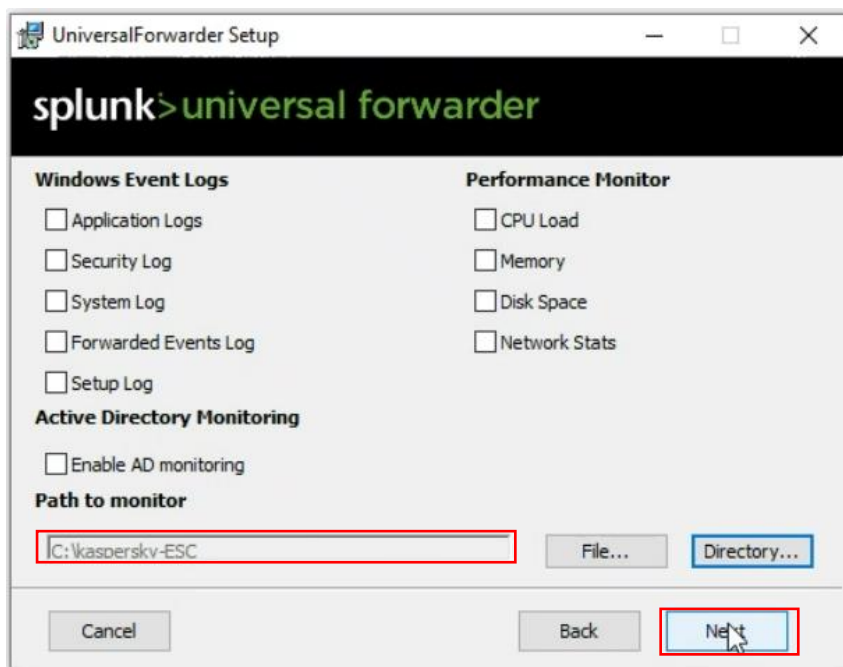
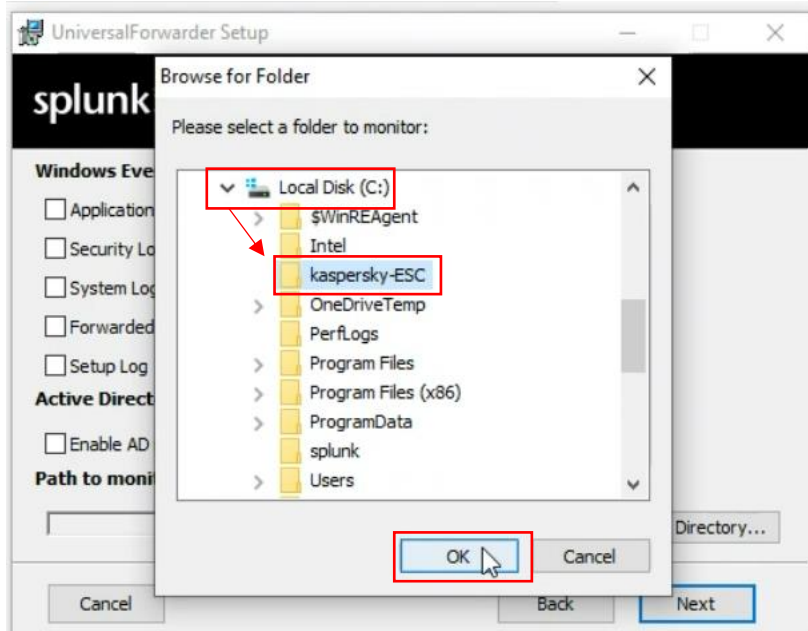
Ejecutar el instalador de Splunk y seguir el paso a paso.



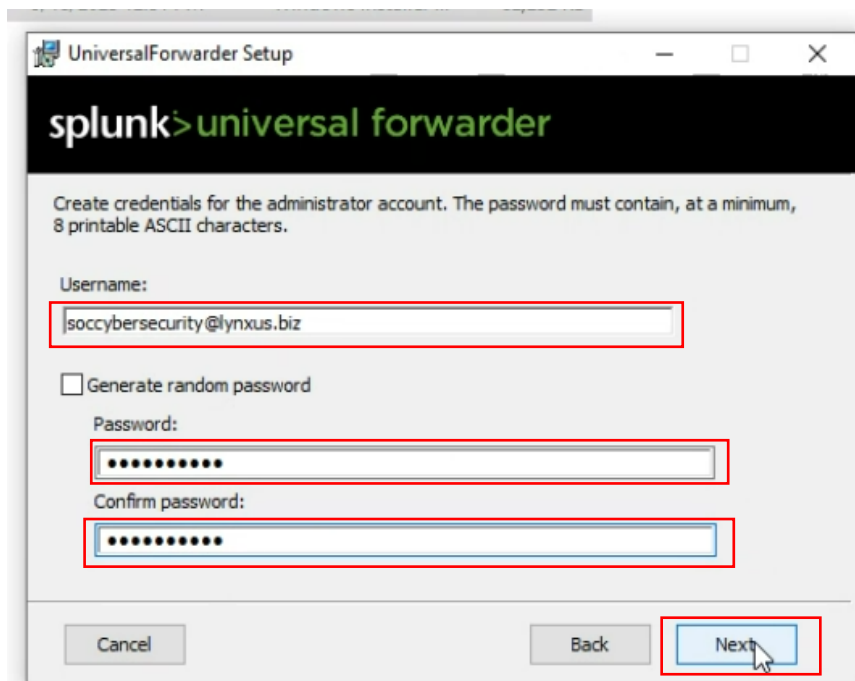






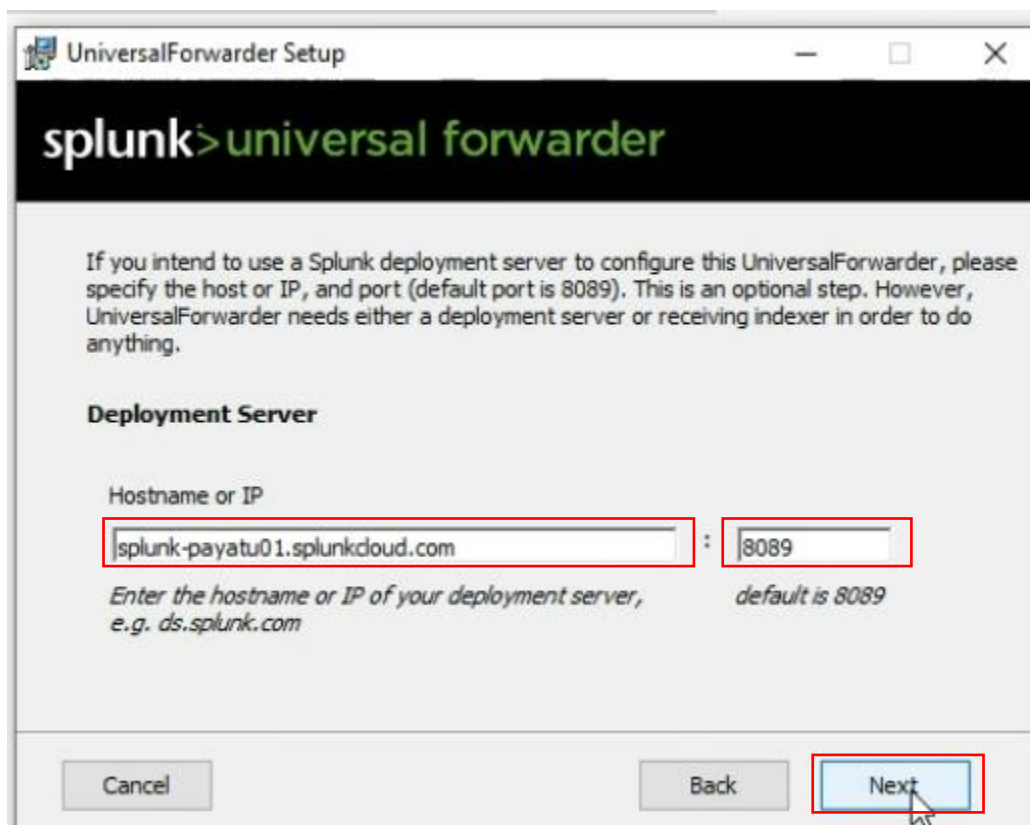


Completar los campos con el Username: "soccybersecurity@lynxus.biz" y Password: "Lynxus@SOC"



The screenshot shows the 'UniversalForwarder Setup' window. The title bar says 'UniversalForwarder Setup'. The main header is 'splunk>universal forwarder'. Below the header, it says 'Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.' There are three input fields: 'Username:' with the value 'soccybersecurity@lynxus.biz', 'Password:' with masked characters, and 'Confirm password:' with masked characters. There is a checkbox 'Generate random password' which is unchecked. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button is highlighted with a red box and a mouse cursor.

Al igual que el Hostname: "payatu01.splunkcloud.com" y el Port:"8089"



The screenshot shows the 'UniversalForwarder Setup' window. The title bar says 'UniversalForwarder Setup'. The main header is 'splunk>universal forwarder'. Below the header, it says 'If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.' There is a section titled 'Deployment Server'. Below it, there are two input fields: 'Hostname or IP' with the value 'splunk-payatu01.splunkcloud.com' and 'Port' with the value '8089'. There is a colon between the two fields. Below the input fields, there is a note: 'Enter the hostname or IP of your deployment server, e.g. ds.splunk.com' and 'default is 8089'. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button is highlighted with a red box and a mouse cursor.

Configuración desde PowerShell

Paso 1: Ejecutar PowerShell como administrador. Ubicarnos sobre la ruta que deseamos modificar en PowerShell, en este caso se hace con el comando "Set-location "C:\Splunk""

```
PS C:\Windows\system32> Set-Location "C:\Splunk"
```

Paso 2: Ingresar a la sub-carpeta "bin" dentro de la carpeta Splunk, con el siguiente comando "cd .\bin\".

```
PS C:\Splunk> cd .\bin\  
PS C:\Splunk\bin>
```

Paso 3: A continuación vamos a realizar la integración del Software principal con el driver instalado anteriormente, para ello se utiliza el siguiente comando: ".\Splunk.exe install app ..\splunkclouduf.spl"

```
PS C:\Splunk\bin> .\splunk.exe install app ..\splunkclouduf.spl
```

Paso 4: Tendremos que iniciar sesión con el usuario y contraseña utilizados anteriormente. Username: soccybersecurity@lyxus.biz, Password: Lynxus@SOC.

```
Splunk username: soccybersecurity@lynxus.biz  
Password:  
App 'C:\Splunk\splunkclouduf.spl' installed  
You need to restart the Splunk Server (splunkd) for your changes to take effect.
```

Paso 5: La aplicación deberá de ser reiniciada para aplicar sus cambios, esto con el siguiente comando : ".\Splunk.exe restart"

```
PS C:\Splunk\bin> .\splunk.exe restart
```

Comprobar conexión

Paso 1: Una vez terminados los siguientes pasos pasaremos a comprobar la conexión de la aplicación tanto con la Nube como con Kaspersky Endpoint Security. Ejecutar el siguiente comando ".\Splunk.exe list forward-server"

```
PS C:\Splunk\bin> .\splunk.exe list forward-server
```

Paso 2: Iniciar nuevamente sesión con las mismas credenciales;

Paso 3: Si todos los pasos fueron correctos allí se encontrará el Driver instalado y su ruta host.

```

Splunk username: soccybersecurity@lynxus.biz
Password:
Active forwards:
    inputs1.splunk-payatu01.splunkcloud.com:9997 (ssl)
Configured but inactive forwards:
    inputs10.splunk-payatu01.splunkcloud.com:9997
    inputs11.splunk-payatu01.splunkcloud.com:9997
    inputs12.splunk-payatu01.splunkcloud.com:9997
    inputs13.splunk-payatu01.splunkcloud.com:9997
    inputs14.splunk-payatu01.splunkcloud.com:9997
    inputs15.splunk-payatu01.splunkcloud.com:9997
    inputs2.splunk-payatu01.splunkcloud.com:9997
    inputs3.splunk-payatu01.splunkcloud.com:9997
    inputs4.splunk-payatu01.splunkcloud.com:9997
    inputs5.splunk-payatu01.splunkcloud.com:9997
    inputs6.splunk-payatu01.splunkcloud.com:9997
    inputs7.splunk-payatu01.splunkcloud.com:9997
    inputs8.splunk-payatu01.splunkcloud.com:9997
    inputs9.splunk-payatu01.splunkcloud.com:9997
PS C:\Splunk\bin>

```

Paso 4: Para comprobar la vinculación con Kaspersky deberás ejecutar el siguiente comando de monitoreo: `.\Splunk.exe list monitor`

```

PS C:\Splunk\bin> .\splunk.exe list monitor
Monitored Directories:
    $SPLUNK_HOME\var\log\splunk
        C:\splunk\var\log\splunk\audit.log
        C:\splunk\var\log\splunk\btool.log
        C:\splunk\var\log\splunk\conf.log
        C:\splunk\var\log\splunk\first_install.log
        C:\splunk\var\log\splunk\health.log
        C:\splunk\var\log\splunk\license_usage.log
        C:\splunk\var\log\splunk\mergebuckets.log
        C:\splunk\var\log\splunk\mongod.log
        C:\splunk\var\log\splunk\remote_searches.log
        C:\splunk\var\log\splunk\scheduler.log
        C:\splunk\var\log\splunk\search_messages.log
        C:\splunk\var\log\splunk\searchhistory.log
        C:\splunk\var\log\splunk\splunkd-utility.log
        C:\splunk\var\log\splunk\splunkd_access.log
        C:\splunk\var\log\splunk\splunkd_ui_access.log
        C:\splunk\var\log\splunk\wlm_monitor.log
    $SPLUNK_HOME\var\log\splunk\configuration_change.log
        C:\splunk\var\log\splunk\configuration_change.log
    $SPLUNK_HOME\var\log\splunk\license_usage_summary.log
        C:\splunk\var\log\splunk\license_usage_summary.log
    $SPLUNK_HOME\var\log\splunk\metrics.log
        C:\splunk\var\log\splunk\metrics.log
    $SPLUNK_HOME\var\log\splunk\splunk_instrumentation_cloud.log*
        C:\splunk\var\log\splunk\splunk_instrumentation_cloud.log
    $SPLUNK_HOME\var\log\splunk\splunkd.log
        C:\splunk\var\log\splunk\splunkd.log
    $SPLUNK_HOME\var\log\watchdog\watchdog.log*
        C:\splunk\var\log\watchdog\watchdog.log
    $SPLUNK_HOME\var\run\splunk\search_telemetry\*search_telemetry.json
    $SPLUNK_HOME\var\spool\splunk\tracker.log*
    C:\kaspersky-ESC
        C:\kaspersky-ESC\KasperskyEndpointSecurity.evtx
Monitored Files:
    $SPLUNK_HOME\etc\splunk.version
PS C:\Splunk\bin>

```

Comprobar funcionalidad de los Logs.

Paso 1: Dirígete a tu navegador Edge y ingresa el siguiente link: secure.eicar.org/eicar.com.



Paso 2: Abrir la aplicación “Event Viewer”, en el apartado de Kaspersky Endpoint Security, deberán de quedar registrados los Logs realizados por el antivirus, así funcionando correctamente.

