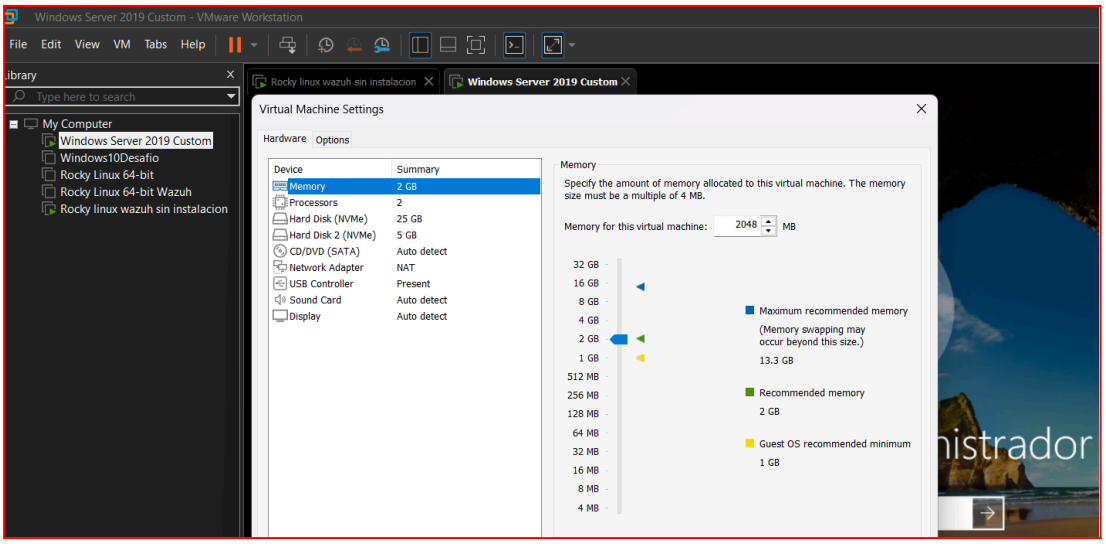
Desafío - Instalación de Wazuh

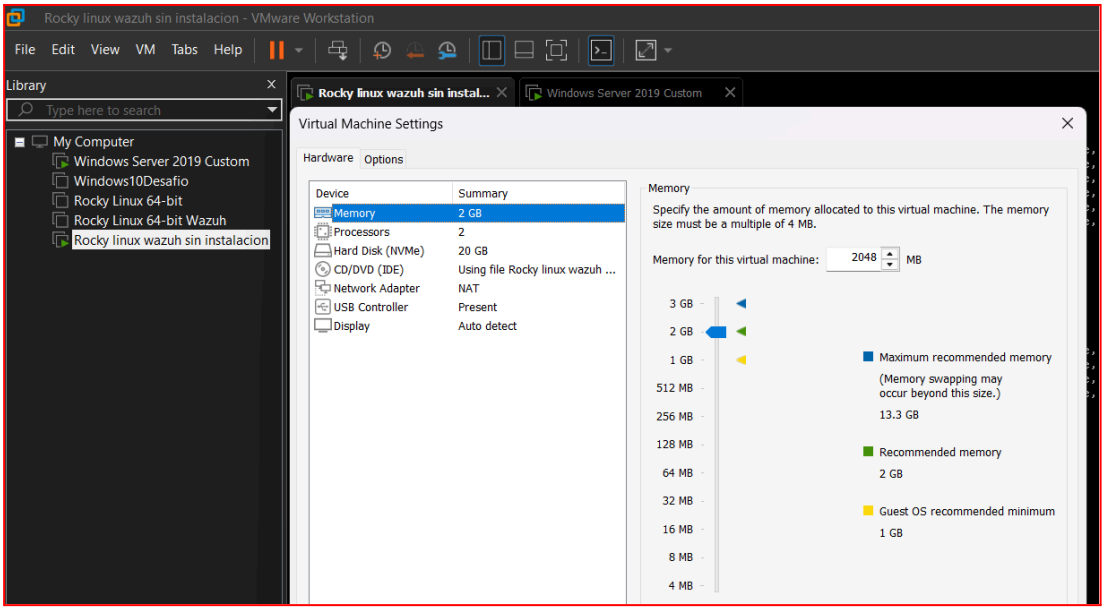
1. **Instalación de una máquina virtual con Sistema Operativo Windows Server. (2 puntos)**

   En este desafío se utilizara una máquina virtual con Windows Server 2019, la cual ya se encuentra previamente configurada y ha sido utilizada durante el desarrollo del curso.



2. **Instalación de una máquina virtual con Sistema Operativo Fedora. (2 puntos)**

   En este desafío se utilizara una máquina virtual con Rocky Linux release 9.5 (Blue Onyx), la cual ya se encuentra previamente configurada y ha sido utilizada durante el desarrollo del curso.

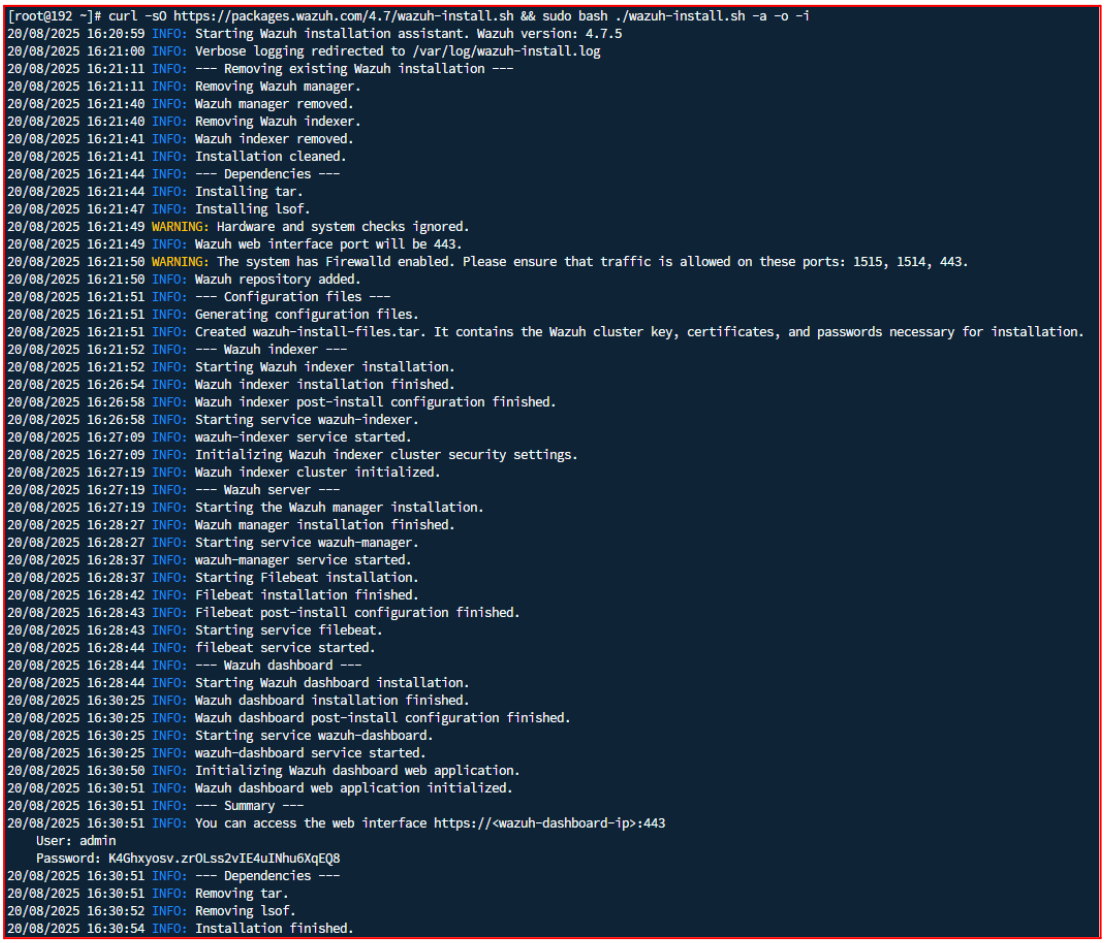


3. **Instalación de Wazuh en el Servidor con Fedora. (2 puntos)**

Se instaló la versión 4.7, la cual no presentó inconvenientes durante el proceso de instalación (ignorando las características del equipo con la opción **-i**), y se utilizó el siguiente comando:

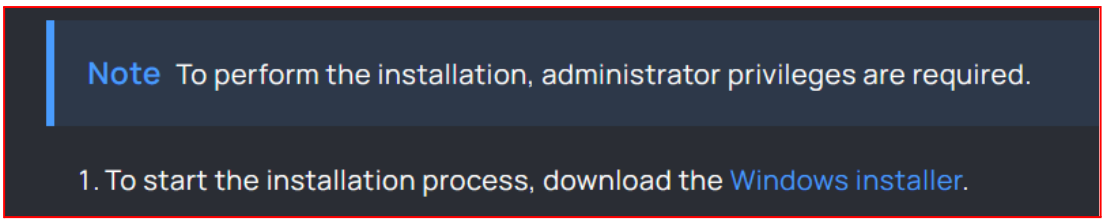
`curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -o -i`

El cual descarga el script de instalación y lo ejecuta.



4. **Instalación de Wazuh Agent en el Servidor Windows Server. (2 puntos)**

Para instalar el agente en el servidor (Windows Server 2019), primero es necesario descargarlo. En este caso, se utilizó la versión 4.7.5-1, la cual es compatible con la versión 4.7 de Wazuh instalada en Rocky Linux. La descarga se realizó desde la página oficial https://documentation.wazuh.com/4.7/installation-guide/wazuh-agent/wazuh-agent-package-windows.html.

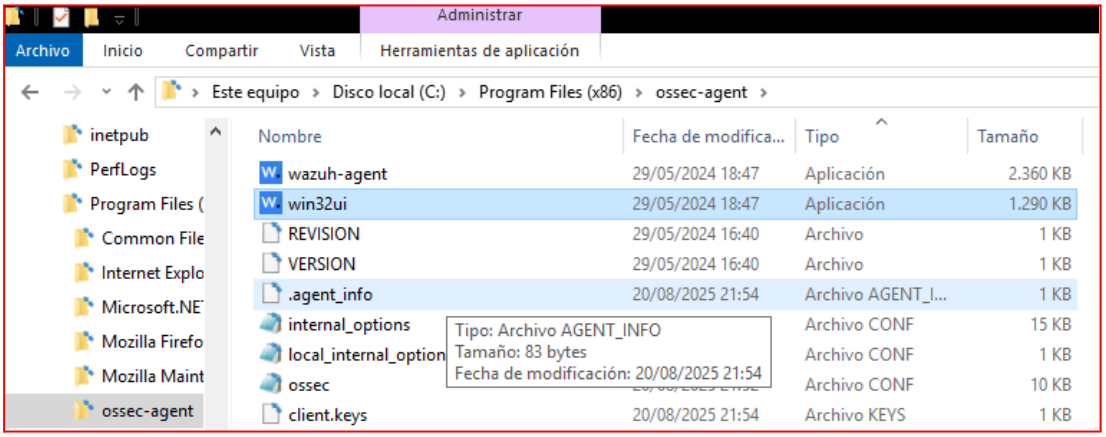


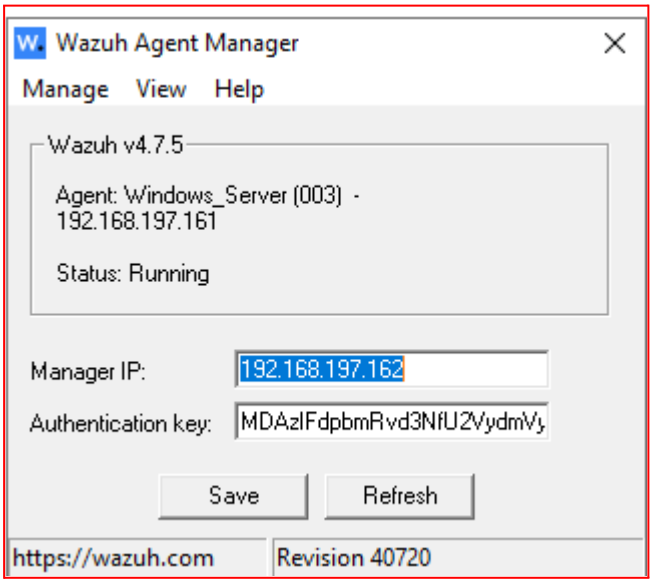
A continuación, se ejecuta el comando de instalacion desde la consola CMD, considerando la dirección IP del servidor en el que se encuentra instalado Wazuh.

```
wazuh-agent-4.7.5-1.msi /q WAZUH_MANAGER=192.168.197.162
```

5. **Configurar Wazuh Agent para que se conecte con el servidor SIEM. (2 puntos)**

Para la configuración del agente, se puede ejecutar la aplicación **`win32ui`**, ubicada en la ruta `C:\Program Files (x86)\ossec-agent`, una vez finalizada la instalación del agente, en el paso anterior.



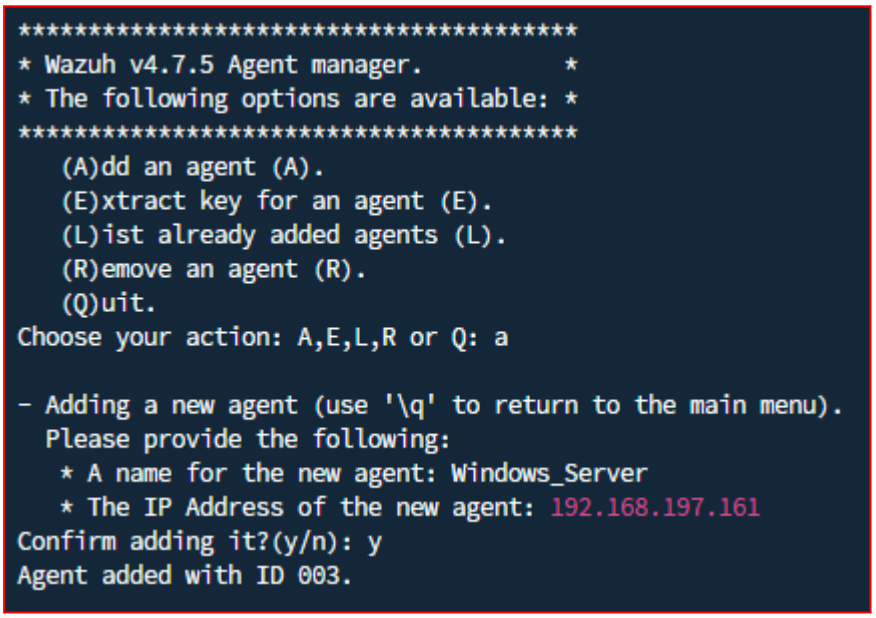


La aplicación solicitará la dirección IP del servidor y la llave de autenticación, la cual debe obtenerse desde el servidor Wazuh.

Para obtener la clave, es necesario que el agente esté registrado con anterioridad. Este proceso se gestiona mediante el siguiente comando:

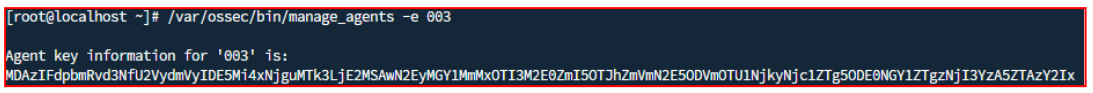
```
/var/ossec/bin/manage_agents
```

Al ejecutar este comando, y tomando la primera opción (`Add an agente`), se solicitará la dirección IP del agente, además de un nombre identificador para el mismo.



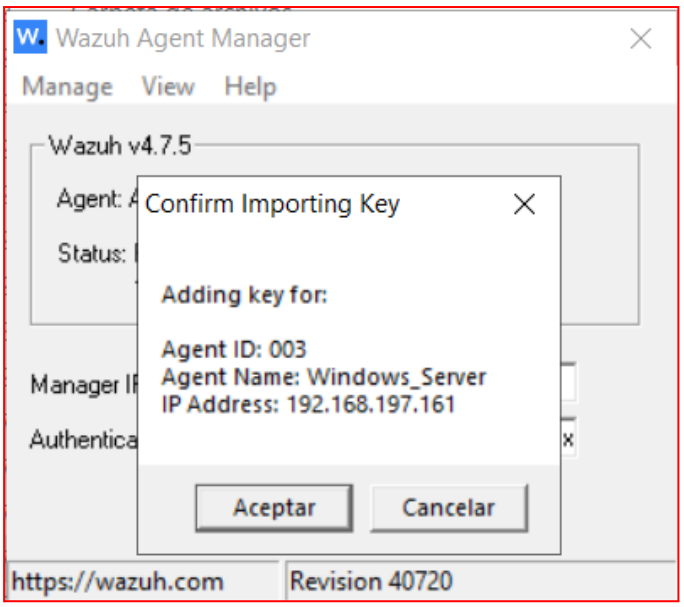
Con el agente registrado, podemos obtener la key de autentificación, con el comando

```
/var/ossec/bin/manage_agents -e 003
```

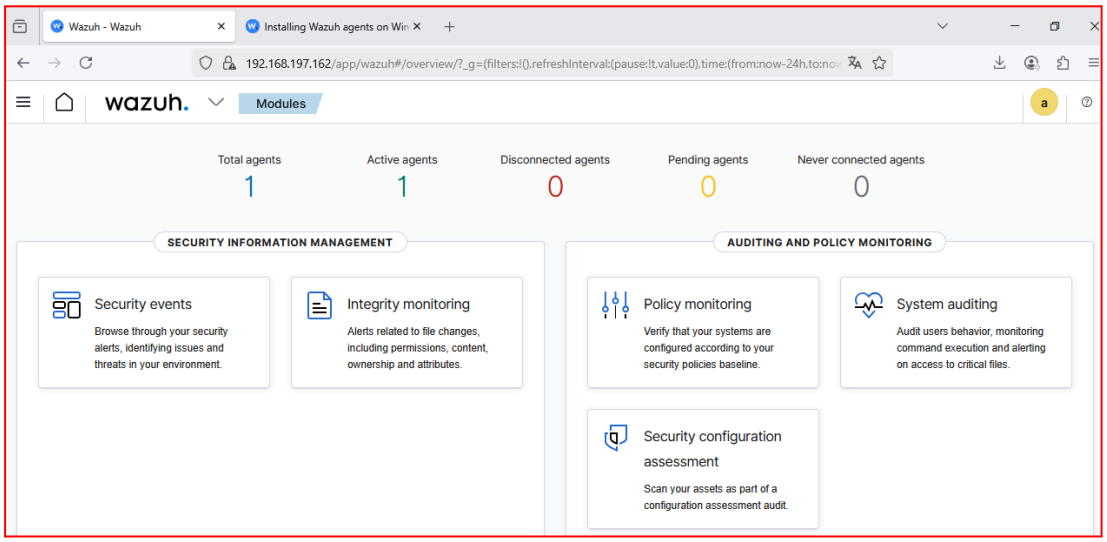


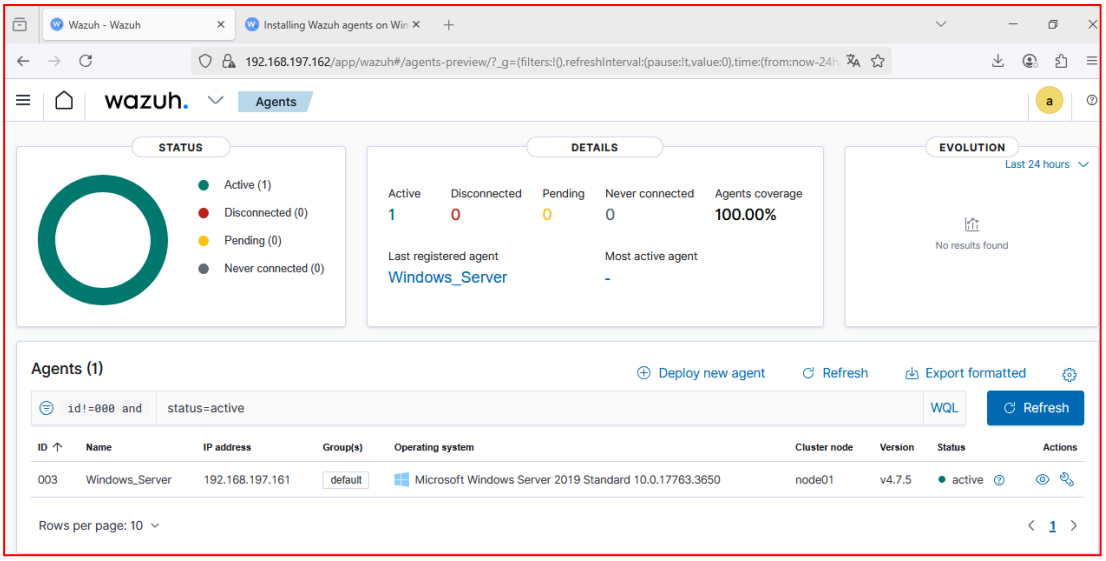
Es importante, tener claro el ID del agente, en mi caso el 003.

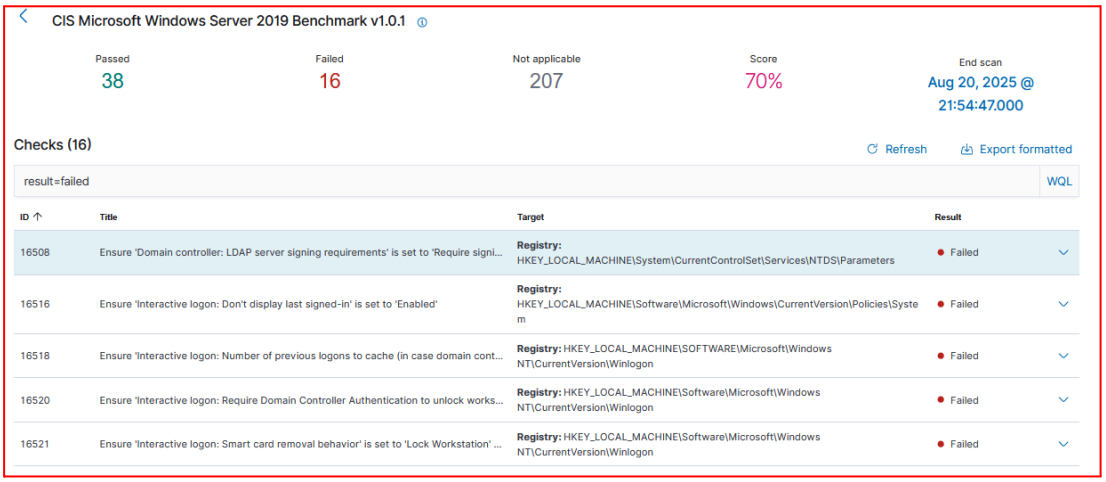
Una vez ingresados la dirección IP del servidor y la clave obtenida en la aplicación del agente en Windows Server, se puede inicializar el agente directamente desde la misma aplicación.



Posteriormente, la validación se realiza accediendo desde el navegador a la dirección del servidor con el puerto 443, en mi caso https://192.168.197.162:443




Wazuh - Wazuh
Installing Wazuh agents on Win
192.168.197.162/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h
wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
0
Pending
0
Never connected
0
Agents coverage
100.00%
Last registered agent
Windows_Server
Most active agent
-
EVOLUTION
Last 24 hours
No results found
Agents (1)
Deploy new agent
Refresh
Export formatted
id!=000 and
status=active
WQL
Refresh
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
003
Windows_Server
192.168.197.161
default
Microsoft Windows Server 2019 Standard 10.0.17763.3650
node01
v4.7.5
active
Rows per page: 10
1


CIS Microsoft Windows Server 2019 Benchmark v1.0.1
Passed
38
Failed
16
Not applicable
207
Score
70%
End scan
Aug 20, 2025 @
21:54:47.000
Checks (16)
Refresh
Export formatted
result=failed
WQL
ID
Title
Target
Result
16508
Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signi...
Registry:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
Failed
16516
Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'
Registry:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Failed
16518
Ensure 'Interactive logon: Number of previous logons to cache (in case domain cont...
Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Failed
16520
Ensure 'Interactive logon: Require Domain Controller Authentication to unlock works...
Registry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Failed
16521
Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' ...
Registry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Failed