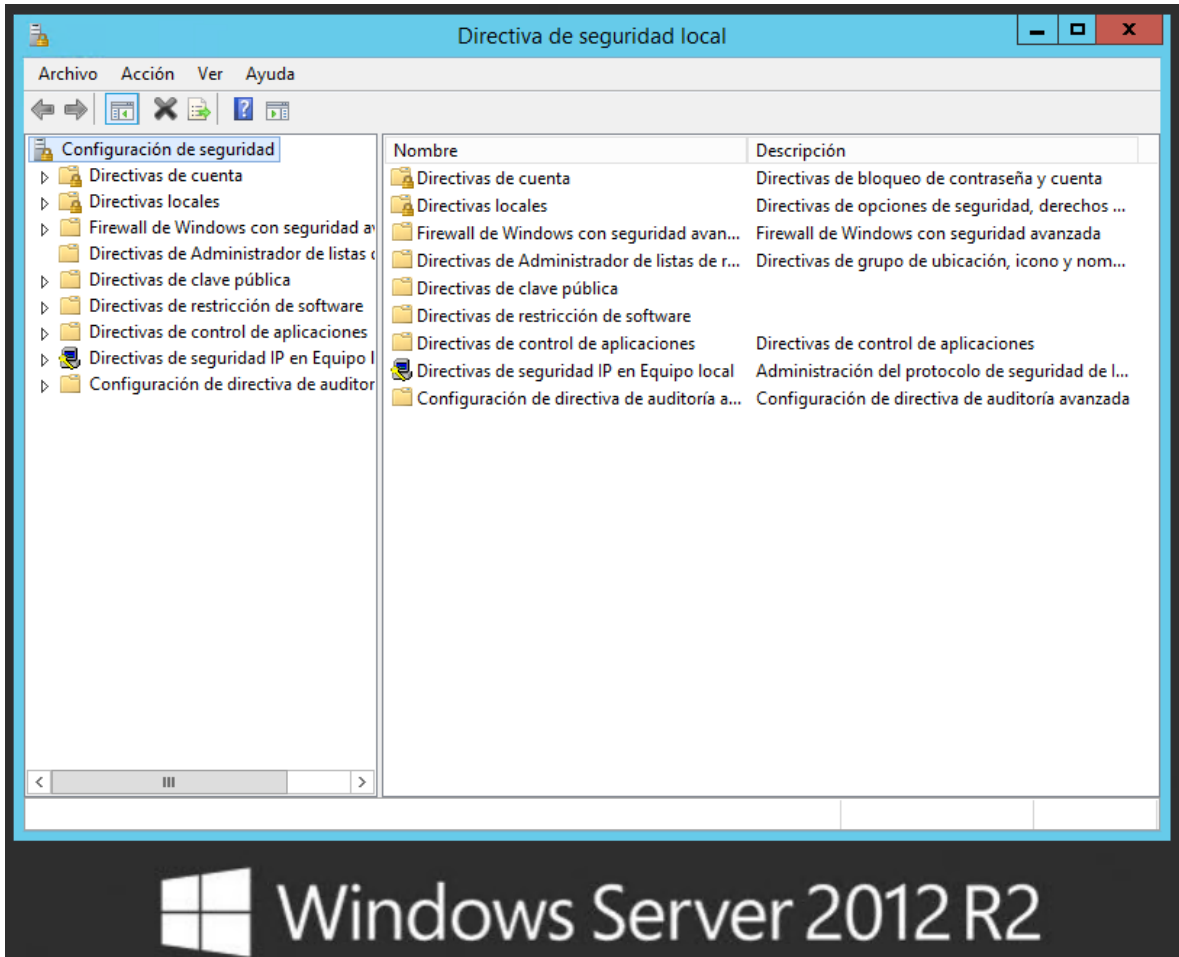


Aplicando y verificando Políticas de Seguridad en Windows

1. Aplicando Políticas de Seguridad

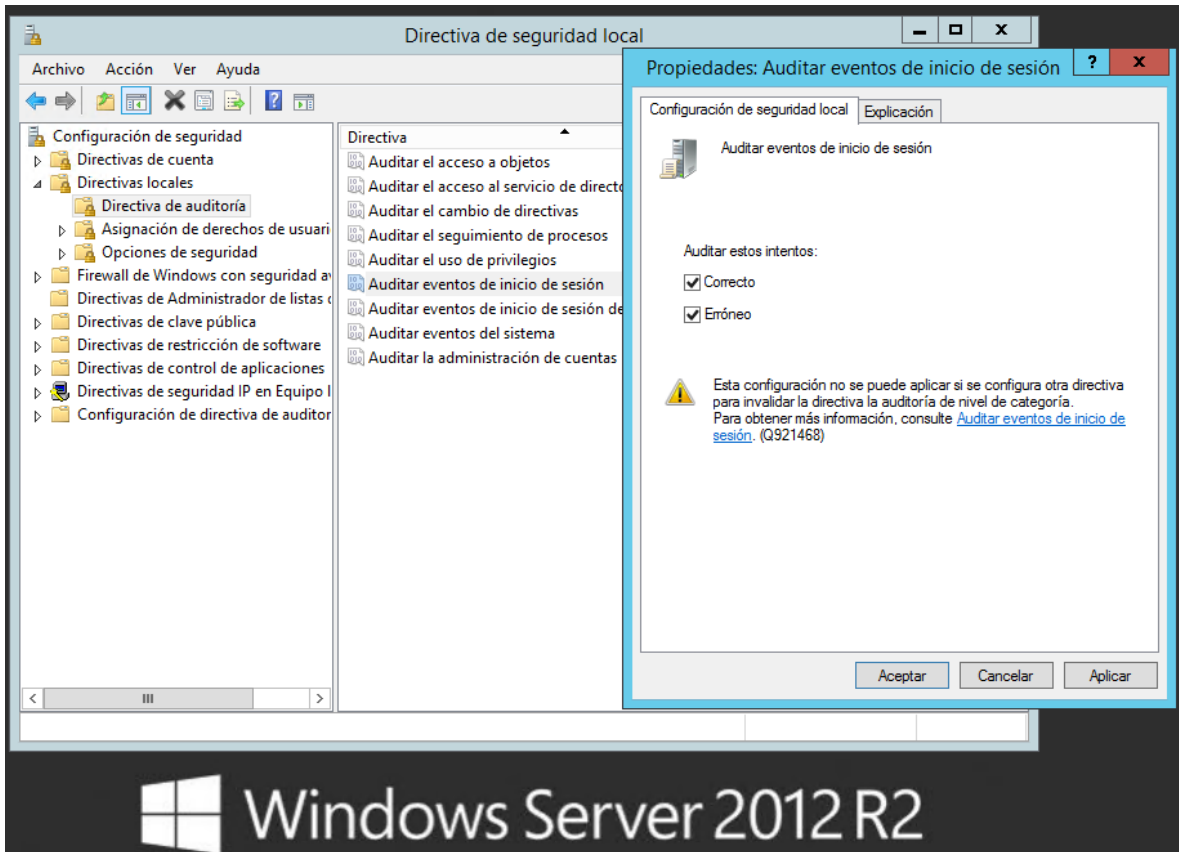
- Abro el Editor de Políticas de Seguridad Local: secpol.msc



2. Configurando la política seleccionada:

- En este caso voy a auditar los intentos de inicio de sesión tanto correctos como erróneos:

Para configurarlo voy a Directivas locales -> Directiva de auditoría -> Auditar eventos de inicio de sesión.



Directiva	Configuración de seguridad...
Auditar el acceso a objetos	Sin auditoría
Auditar el acceso al servicio de directorio	Sin auditoría
Auditar el cambio de directivas	Sin auditoría
Auditar el seguimiento de procesos	Sin auditoría
Auditar el uso de privilegios	Sin auditoría
Auditar eventos de inicio de sesión	Correcto, Erróneo
Auditar eventos de inicio de sesión de cuenta	Sin auditoría
Auditar eventos del sistema	Sin auditoría
Auditar la administración de cuentas	Sin auditoría

3. Verificando las Políticas con el Visor de Eventos:

- Abro el visor de Eventos: eventvwr.msc

Para auditar los registros de lo relacionado a Seguridad voy a -> Registros de Windows -> Seguridad

The screenshot shows the Windows Event Viewer interface. The left pane displays the navigation tree with 'Seguridad' selected. The main pane shows a list of security events under the 'Seguridad' category, with 39,824 total events. The selected event (ID 4625) is expanded to show its details.

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Error de auditoría	28/05/2024 21:55:19	Microsoft Windows security auditing.	4625	Inicio de sesión
Error de auditoría	28/05/2024 21:54:44	Microsoft Windows security auditing.	4625	Inicio de sesión
Error de auditoría	28/05/2024 21:53:52	Microsoft Windows security auditing.	4625	Inicio de sesión
Error de auditoría	28/05/2024 21:53:33	Microsoft Windows security auditing.	4625	Inicio de sesión
Error de auditoría	28/05/2024 21:52:47	Microsoft Windows security auditing.	4625	Inicio de sesión
Error de auditoría	28/05/2024 21:51:52	Microsoft Windows security auditing.	4625	Inicio de sesión

Evento 4625, Microsoft Windows security auditing.

General | Detalles

Error de una cuenta al iniciar sesión.

Sujeto:

- Id. de seguridad: NULL SID
- Nombre de cuenta: -
- Dominio de cuenta: -
- Id. de inicio de sesión: 0x0

Tipo de inicio de sesión: 3

Cuenta con error de inicio de sesión:

- Id. de seguridad: NULL SID
- Nombre de cuenta: PracticaUTN
- Dominio de cuenta: HAZARD-LAPTOP

Información de error:

- Motivo del error: Nombre de usuario desconocido o contraseña incorrecta
- Estado: 0xC000006D
- Subestado: 0xC0000064

En este caso verificamos que hubo un intento de inicio de sesión fallido (id 4625) a las 21:54:44 del 28/05/2024 del usuario "PracticaUTN" y el motivo del error es Usuario o contraseña inválidos.

Rodrigo Vila.-