WGET ERROR: The certificate of 'app.dominio.lan' is not trusted.

root@server:/home# wget https://app.dominio.lan/api/public/dl/mFwz/installers/agent-13.2.24.deb Resolving app.dominio.lan (app.dominio.lan)... 192.168.100.10 Connecting to app.dominio.lan (app.dominio.lan)|192.168.100.10|:443... connected. ERROR: The certificate of 'app.dominio.lan' is not trusted. ERROR: The certificate of 'app.dominio.lan' doesn't have a known issuer. root@server:/home#

Descripcion

El mensaje de error que encontró indica que su sistema no confía en el certificado SSL utilizado por el servidor filebrowser.scuarmander.lan. Esto suele ocurrir cuando el certificado está autofirmado, la autoridad certificadora que lo emitió no es de confianza o el certificado no está instalado correctamente.

Soluciones para Resolver Problemas de Certificados SSL

1. **Instalar el Certificado de la Autoridad Certificadora (CA):** Si tienes el certificado de la CA que firmó `app.dominio.lan`, puedes instalarlo en el almacén de certificados confiables de tu sistema. Esto varía dependiendo del sistema operativo.

2. **Ignorar la Validación del Certificado SSL:** Para usos no críticos, puedes omitir la verificación del certificado. Con `wget`, puedes ignorar la verificación del certificado SSL con la opción `--no-check-certificate`. Aquí te muestro cómo puedes modificar tu comando: `wget --no-check-certificate https://app.dominio.lan/api/public/dl/mFwz/installers/agent-13.2.24.deb`

   Advertencia: Este enfoque hace que la conexión sea vulnerable a ataques de

intermediarios. Úsalo solo si estás seguro de la integridad de tu red.

3. **Actualizar los Certificados CA del Sistema:** A veces, simplemente actualizar los certificados CA de tu sistema puede resolver este tipo de problemas. Para un sistema basado en Debian, puedes actualizarlos con:
   `sudo apt-get update`
   `sudo apt-get install ca-certificates`

4. **Verificar la Configuración del Servidor:** Asegúrate de que el servidor esté configurado correctamente con los certificados SSL/TLS adecuados, incluidos los certificados intermedios. Esto es crucial para que los clientes puedan verificar la identidad del servidor.

Elige el enfoque que mejor se adapte a tus políticas y requisitos de seguridad. Para entornos de producción, generalmente es mejor asegurarse de que todos los certificados sean válidos y estén confiados para evitar riesgos de seguridad.

Revisión #1
Creado 7 mayo 2024 19:48:47 por Greivin
Actualizado 7 mayo 2024 19:57:18 por Greivin