

Let's Encrypt: Windows

Julian F. Latorre

22 de noviembre de 2024

Índice

| | |
|--|----------|
| 1. Implementación Detallada de Let's Encrypt | 1 |
| 1.1. Introducción a Let's Encrypt en Windows | 1 |
| 1.2. Conceptos Clave | 1 |
| 1.3. Instalación de win-acme | 2 |
| 1.3.1. Descarga e Instalación | 2 |
| 1.4. Obtención de Certificados con win-acme | 2 |
| 1.4.1. Ejecución de win-acme | 2 |
| 1.4.2. Proceso de Obtención de Certificados | 2 |
| 1.5. Configuración de IIS | 3 |
| 1.6. Renovación Automática de Certificados | 3 |
| 1.7. Solución de Problemas Comunes en Windows | 3 |
| 1.8. Mejores Prácticas para Windows | 3 |
| 1.9. Implementación en Escenarios Específicos de Windows | 4 |
| 1.9.1. Múltiples Sitios en un Solo Servidor IIS | 4 |
| 1.9.2. Integración con Aplicaciones .NET | 4 |
| 1.9.3. Uso con Remote Desktop Services (RDS) | 4 |
| 1.10. Alternativas a win-acme en Windows | 4 |

1. Implementación Detallada de Let's Encrypt

1.1. Introducción a Let's Encrypt en Windows

Aunque Let's Encrypt fue diseñado principalmente para sistemas Unix, es posible implementarlo en Windows con algunas adaptaciones. Este instructivo cubrirá los pasos necesarios para obtener y gestionar certificados Let's Encrypt en un entorno Windows.

1.2. Conceptos Clave

- **ACME (Automatic Certificate Management Environment):** Protocolo utilizado por Let's Encrypt para verificar el control de un dominio y emitir certificados.

- **Certbot**: Cliente ACME de código abierto para automatizar la obtención y renovación de certificados Let's Encrypt.
- **win-acme**: Cliente ACME específico para Windows, alternativa a Certbot.

1.3. Instalación de win-acme

win-acme es una herramienta popular para gestionar certificados Let's Encrypt en Windows.

1.3.1. Descarga e Instalación

1. Visite la página de lanzamientos de win-acme en GitHub:
<https://github.com/win-acme/win-acme/releases>
2. Descargue la última versión (archivo zip)
3. Extraiga el contenido del zip en una carpeta, por ejemplo:
C:\win-acme

1.4. Obtención de Certificados con win-acme

1.4.1. Ejecución de win-acme

Abra PowerShell como administrador y navegue a la carpeta de win-acme:

```
cd C:\win-acme  
.\wacs.exe
```

1.4.2. Proceso de Obtención de Certificados

1. Seleccione "N" para crear un nuevo certificado
2. Elija el tipo de certificado (generalmente, un solo sitio)
3. Seleccione el sitio de IIS para el cual desea el certificado
4. Confirme el dominio o dominios a incluir en el certificado
5. Elija el método de validación (HTTP es el más común)
6. Siga las instrucciones en pantalla para completar el proceso

1.5. Configuración de IIS

win-acme generalmente configura IIS automáticamente, pero es bueno verificar:

1. Abra el Administrador de IIS
2. Seleccione su sitio web
3. En el panel de “Acciones” , haga clic en “Enlaces”
4. Verifique que existe un enlace para HTTPS en el puerto 443 con el nuevo certificado

1.6. Renovación Automática de Certificados

win-acme configura una tarea programada para la renovación automática. Para verificar:

1. Abra el Programador de tareas de Windows
2. Busque una tarea llamada “win-acme renew”
3. Verifique que esté programada para ejecutarse regularmente

Para forzar una renovación manual:

```
cd C:\win-acme  
.\wacs.exe --renew
```

1.7. Solución de Problemas Comunes en Windows

- **Error de acceso denegado:** Asegúrese de ejecutar win-acme como administrador.
- **Fallo en la validación HTTP:** Verifique que el sitio sea accesible públicamente y que el puerto 80 esté abierto.
- **Problemas con IIS:** Asegúrese de que IIS esté correctamente configurado y que el sitio esté en ejecución.
- **Errores de .NET Framework:** Verifique que tiene instalada la versión correcta de .NET Framework.

1.8. Mejores Prácticas para Windows

- Mantenga Windows Server y IIS actualizados.
- Use el Firewall de Windows para controlar el acceso a los puertos 80 y 443.

- Implemente HSTS en IIS para forzar conexiones HTTPS.
- Configure la redirección de HTTP a HTTPS en IIS.
- Realice copias de seguridad regulares de la configuración de IIS y los certificados.

1.9. Implementación en Escenarios Específicos de Windows

1.9.1. Múltiples Sitios en un Solo Servidor IIS

win-acme puede manejar múltiples sitios. Simplemente repita el proceso de obtención de certificados para cada sitio.

1.9.2. Integración con Aplicaciones .NET

Para aplicaciones .NET, asegúrese de que estén configuradas para usar HTTPS en el archivo web.config:

```
<system.webServer>
  <rewrite>
    <rules>
      <rule name="HTTP to HTTPS redirect" stopProcessing="true">
        <match url="(.*)" />
        <conditions>
          <add input="{HTTPS}" pattern="off" ignoreCase="true" />
        </conditions>
        <action type="Redirect" url="https://{HTTP_HOST}/{R:1}"
          redirectType="Permanent" />
      </rule>
    </rules>
  </rewrite>
</system.webServer>
```

1.9.3. Uso con Remote Desktop Services (RDS)

Para servidores RDS, puede usar win-acme para obtener certificados para el Gateway de RDS. Asegúrese de configurar correctamente los nombres de dominio y los puertos en la configuración de RDS.

1.10. Alternativas a win-acme en Windows

- **Certify The Web:** Una GUI para gestionar certificados Let's Encrypt en Windows.
- **PowerShell con Posh-ACME:** Para usuarios avanzados que prefieren scripts de PowerShell.
- **ACMESharp:** Otra implementación de ACME para Windows en PowerShell.