

Latinoamérica



## Apéndice B: Secuencias de comandos y archivos auxiliares de la solución

Publicado: octubre 11, aaaa | Actualizado: 24/11/04

### En esta página

- ↓ [Introducción](#)
- ↓ [Lista de los archivos de la guía de la solución](#)
- ↓ [Estructura de las secuencias de comandos](#)
- ↓ [Descripción de las secuencias de comandos y archivos auxiliares](#)

- [Seguridad en LAN inalámbricas con Servicios de Certificate Server](#)
- [Contenido de la solución](#)
- [Guía de planeamiento](#)
- [Guía de generación](#)
- [Guía de operaciones](#)
- [Guía de prueba](#)
- [Apéndices](#)

### Introducción

En este apéndice se incluye una breve descripción de las secuencias de comandos y otros archivos auxiliares suministrados con la solución para *Seguridad en LAN inalámbricas con Servicios de Certificate Server*. Aunque son funcionales y se han probado, las secuencias de comandos y los archivos auxiliares se proporcionan como ayuda para crear secuencias de comandos administrativas propias. No están diseñados para servir de código con calidad de producción.

### Condiciones de uso

Las secuencias de comandos y los archivos auxiliares proporcionados con esta solución están sujetos a las CONDICIONES DE USO estándar de Microsoft. Las condiciones se encuentran en la página [Microsoft: información acerca de las condiciones de uso](#) en <http://www.microsoft.com/info/copyright.htm>.

**Nota:** asegúrese de probar exhaustivamente estas secuencias de comandos y herramientas en un entorno de prueba antes de implementarlas en un entorno de producción.

↑ [Principio de la página](#)

### Lista de los archivos de la guía de la solución

#### Secuencias de comandos comunes

- constants.vbs
- helper.vbs

#### Secuencias de comandos de Servicios de Certificate Server

- pkiparams.vbs
- ca\_monitor.vbs
- ca\_monitor.wsf
- ca\_operations.vbs
- ca\_operations.wsf
- ca\_setup.vbs
- ca\_setup.wsf

## Secuencias de comandos de IAS y WLAN

- ias\_tools.vbs
- ias\_tools.wsf
- wl\_tools.vbs
- wl\_tools.wsf
- IASClientExport.bat
- IASClientImport.bat
- IASExport.bat
- IASImport.bat
- IAS\_Data.bat

## Archivo auxiliar de IAS y WLAN

- IASAccessPrep.txt

## Archivos desatendidos de componentes opcionales

- OC\_AddIAS.txt
- OC\_AddIIS.txt
- OC\_RemoveRootUpdate.txt

[↑ Principio de la página](#)

## Estructura de las secuencias de comandos

Los archivos por lotes son relativamente simples de seguir, pero los archivos de Microsoft® Visual Basic® Scripting Edition (VBScript) requieren explicación para comprender el modo en que funcionan conjuntamente. A diferencia de muchos ejemplos de VBScript, estas secuencias de comandos son multifuncionales. Para proporcionar acceso a las distintas funciones, las secuencias de comandos aprovechan la funcionalidad de "trabajo" de Microsoft Windows® Scripting Host (WSH). Esto permite varias funciones de programa independientes mediante la especificación de un nombre de trabajo como parámetro para la secuencia de comandos.

Las secuencias de comandos normalmente van por parejas: un archivo .wsf y otro .vbs. El archivo WSF contiene la "interfaz de usuario" para distintas operaciones de la secuencia de comandos. El archivo VBS contiene todo el código que hace que el trabajo del programa.

Todos los archivos de secuencias de comandos utilizan la sintaxis donde *NombreTrabajo* es el nombre de la operación requerida y *ArchivoSecuenciaComandosW* es el nombre del archivo de interfaz XML de la secuencia de comandos como en el siguiente ejemplo:

cscript //job:*NombreTrabajo* *ArchivoSecuenciaComandosW.wsf*

Un extracto de uno de los archivos WSF incluye la siguiente información:

```
<?xml version="1.0" encoding="utf-8" ?>
<package xmlns="Windows Script Host
  <job id="GetCacerts ">
    <comment></comment>
    <script language="VBScript" src="constants.vbs" />
    <script language="VBScript" src="pkiparams.vbs" />
    <script language="VBScript" src="helper.vbs" />
```

```
<script language="VBScript" src="ca_operations.vbs" />
<script language="VBScript"
<![CDATA[
    GetCaCerts
]]>
</script>
</job>
<job id="PublishRootCertstoIIS ">
    <comment></comment>
    <script language="VBScript" src="constants.vbs" />
    <script language="VBScript" src="pkiparams.vbs" />
    <script language="VBScript" src="helper.vbs" />
    <script language="VBScript" src="ca_operations.vbs" />
    <script>
    <![CDATA[
        PublishCertstoIIS ROOT_CERT_SOURCE, WWW_LOCAL_PUB_PATH
    ]]>
    </script>
</job>
```

El primer trabajo es GetCACerts. La definición de este trabajo especifica que se carguen los archivos VBS constants.vbs, pkiparams.vbs, helper.vbs y ca\_operations.vbs, que contienen funciones o subrutinas que necesita el trabajo. La sección final del ejemplo de código especifica la función de nivel superior que se ejecutará para iniciar el trabajo; en este caso, GetCACerts. (Este ejemplo tiene el mismo nombre que el trabajo, pero no es necesario que sea así.) Observe que el segundo trabajo, PublishRootCertstoIIS, proporciona parámetros a la función llamada.

Los archivos VBS se encargan del trabajo real y hay tres tipos principales:

- Archivos de secuencias de comandos específicos de la operación que contienen funciones relacionadas únicamente con dicho tipo de operación. (Por ejemplo, ca\_operations.vbs contiene funciones relacionadas con las operaciones de entidad emisora de certificados, o CA.)
- Archivos de secuencias de comandos genéricos que contienen funciones más generales de las que utilizan las secuencias de comandos más específicas de la operación. Helper.vbs es la única de estas secuencias de comandos y contiene funciones como crear cuentas de usuario y comprobar errores.
- Archivos de secuencias de comandos de parámetros que contienen constantes de VBScript que definen el modo de ejecución de las secuencias de comandos operativas. Se han recopilado para que resulte más fácil modificarlas en un solo lugar en vez de incrustarlas en las funciones de secuencias de comandos. En esta categoría se encuentran los archivos constants.vbs, que contiene parámetros globales, y pkiparams.vbs, que contiene parámetros específicos a la configuración y operaciones de la infraestructura de claves públicas (PKI).

[↑ Principio de la página](#)

## Descripción de las secuencias de comandos y archivos auxiliares

En esta sección se describe cada una de las secuencias de comandos y los archivos auxiliares enumerados anteriormente.

### Secuencias de comandos comunes

Hay dos tipos de archivos de secuencias de comandos comunes.

#### Constants.vbs

Esta secuencia de comandos contiene valores comunes que los usuarios pueden establecer para que los utilicen los demás archivos VBS y WSF. (Por ejemplo, los valores de las alertas SMTP y de registro de sucesos se establecen en esta secuencia de comandos.)

#### Helper.vbs

Esta secuencia de comandos contiene rutinas auxiliares que utilizan numerosas secuencias de comandos VBS (por ejemplo, creación de usuarios y grupos, rutinas de alertas y otras funciones de utilidad).

## Secuencias de comandos de Servicios de Certificate Server

En esta sección se describen las secuencias de comandos de Servicios de Certificate Server.

### **pkiparams.vbs**

Esta secuencia de comandos contiene valores específicos de PKI y de entidad emisora que el usuario puede cambiar. Algunos de estos valores se *deben* cambiar para poder utilizarlos (con el fin de reflejar la configuración correcta del entorno); otros no se tienen que cambiar a menos que se deseé que el comportamiento de la secuencia de comandos sea distinto. En los capítulos principales de la guía (los capítulos 7, "Implementación de la infraestructura de claves públicas", y 11, "Administración de la infraestructura de claves públicas") se proporciona información acerca de dónde se debe o puede cambiar un valor en estos procedimientos.

Todas las demás secuencias de comandos hacen referencia a PKIParams.vbs con el prefijo "CA\_".

### **ca\_setup.vbs y ca\_setup.wsf**

Estas secuencias de comandos contienen funciones para configurar los parámetros de línea de base de las entidades emisoras que se utilizan para crear grupos de seguridad y usuarios. Hay rutinas de configuración para las CA raíz y emisoras. La mayoría de los valores configurados realmente se controlan desde el archivo pkiparams.vbs. Consulte el capítulo 7, "Implementación de la infraestructura de claves públicas", para obtener más información acerca de este archivo.

Los trabajos que contienen estas secuencias de comandos son los siguientes:

- CertLocalGroups: este trabajo crea grupos de seguridad locales (se utilizan en la entidad emisora raíz) para la administración de entidades emisoras. La función de creación de grupos se llama varias veces como parte del trabajo, cada vez con un nombre de grupo distinto.
- CertDomainGroups: este trabajo crea grupos de seguridad del dominio para la administración de CA y PKI. Contiene varias llamadas para crear grupos distintos. El tipo de grupo (local, global o universal) se especifica como un parámetro en la definición de trabajo.
- CertLocalTestAccts: este trabajo crea cuentas de usuario de prueba para la administración de la entidad emisora raíz.
- CertDomainTestAccts: este trabajo crea cuentas de dominio de prueba para la administración de la entidad emisora en línea.
- RootCACConfig: este trabajo configura parámetros de la entidad emisora raíz con llamadas a certutil.
- IssCACConfig: este trabajo configura parámetros de la entidad emisora con llamadas a certutil.

### **ca\_monitor.vbs y ca\_monitor.wsf**

Estas secuencias de comandos contienen funciones para comprobar el estado de la entidad emisora y la PKI. Estas secuencias de comandos comprueban específicamente que la entidad emisora puede responder y que los certificados de CA y las listas de revocación de certificados (CRL) están actualizados. Las secuencias de comandos generan entradas del registro de sucesos, alertas SMTP (protocolo simple de transferencia de correo) o ambas. Están diseñadas para que las ejecute un agente de Microsoft Operations Manager (MOM) (o un agente de administración similar que se ejecute en el servidor) o el programador de tareas de Windows en una entidad emisora en línea. Este procedimiento de secuencias de comandos se utiliza únicamente en el capítulo 11, "Administración de la infraestructura de claves públicas".

Los trabajos que contienen estas secuencias de comandos son los siguientes:

- IsCAAlive: este trabajo comprueba si responden las llamadas a procedimiento remoto (RPC) de Servicios de Certificate Server.
- CheckCRLs: este trabajo comprueba las listas CRL de la entidad emisora en la que se ejecuta la secuencia de comandos y las listas CRL de todas las entidades emisoras principales hasta la raíz. Las alertas se emiten si una lista CRL ha caducado, está a punto de caducar y cuando se debe emitir una nueva lista CRL.
- CheckCACerts: este trabajo comprueba el certificado de la entidad emisora en la que se ejecuta la secuencia de comandos y los certificados de todas las entidades emisoras principales hasta la raíz. Las alertas se

emiten si un certificado ha caducado, cuando un certificado está a un mes de caducar y si se tiene que renovar un certificado (normalmente a la mitad de su duración).

- **SetupSMTPAlerts:** este trabajo configura la entidad emisora para que genere alertas de correo electrónico cuando en la entidad emisora se ha puesto en cola una solicitud de certificado pendiente (en espera de la aprobación del administrador de certificados).

#### **ca\_operations.vbs y ca\_operations.wsf**

Estas secuencias de comandos contienen funciones pertinentes para las operaciones continuas en la entidad emisora, como la publicación certificados y listas CRL, así como la copia de seguridad de las claves y la base de datos de la entidad emisora. Estas secuencias de comandos se utilizan principalmente en el capítulo 11, "Administración de la infraestructura de claves públicas", pero también en algunos procedimientos del capítulo 7, "Implementación de la infraestructura de claves públicas".

Los trabajos que contienen estas secuencias de comandos son los siguientes:

- **GetCaCerts:** este trabajo recupera los certificados de la entidad emisora raíz y los almacena en un disco.
- **GetCRLs:** este trabajo recupera las listas CRL de la entidad emisora raíz y las almacena en un disco.
- **PublishCertstoAD:** este trabajo publica el certificado de la entidad emisora raíz (recuperado con GetCaCerts) en el servicio de directorio Microsoft Active Directory®.
- **PublishCRLstoAD:** este trabajo publica las listas CRL de la entidad emisora raíz (recuperadas con GetCRLs) en Active Directory.
- **PublishRootCertstoIIS:** este trabajo publica el certificado de la entidad emisora raíz (recuperado con GetCaCerts) en el servidor Web de Servicios de Internet Information Server (IIS).
- **PublishRootCRLstoIIS:** este trabajo publica las listas CRL de la entidad emisora raíz (recuperadas con GetCRLs) en el servidor Web de IIS.
- **PublishIssCertstoIIS:** este trabajo publica el certificado de la entidad emisora (recuperado con GetCaCerts) en el servidor Web de IIS.
- **PublishIssCRLstoIIS:** este trabajo publica las listas CRL de la entidad emisora (recuperadas con GetCRLs) en el servidor Web de IIS.
- **BackupCaKeys:** este trabajo realiza una copia de seguridad de los certificados y las claves de la entidad emisora en un disco.
- **BackupCaDatabase:** este trabajo ejecuta NTBackup.exe para realizar una copia de seguridad del estado del sistema (incluida la base de datos y los registros) de la entidad emisora.

#### **Secuencias de comandos de IAS y WLAN**

En esta sección se describen las secuencias de comandos de IAS y WLAN.

#### **ias\_tools.vbs e ias\_tools.wsf**

Estas secuencias de comandos contienen trabajos que sirven de ayuda en la configuración de usuarios para Servicio de autenticación de Internet (IAS) de Microsoft. Estas secuencias de comandos se utilizan en el capítulo 8, "Implementación de la estructura de RADIUS", y el capítulo 9, "Implementación de la infraestructura de seguridad para LAN inalámbricas".

Los trabajos que contienen estas secuencias de comandos son los siguientes:

- **CreateIasGroups:** este trabajo crea los grupos de seguridad de dominio que necesita la solución para administrar IAS.
- **UpdateUsersRAP:** este trabajo edita las propiedades de acceso telefónico de usuario para habilitar el acceso telefónico. (No se ha utilizado en la solución, pero se ha incluido por si se necesita.) Al utilizar esta secuencia de comandos, *sólo* se actualizan los objetos de usuario del contenedor USUARIOS; si desea actualizar objetos

de otras partes, utilice la secuencia como plantilla y modifíquela según le interese.

#### **wl\_tools.vbs y wl\_tools.wsf**

Estas secuencias de comandos crean grupos de seguridad que se utilizan para administrar usuarios de red de área local inalámbrica (WLAN) y contienen una rutina para generar secretos de RADIUS/puntos de acceso inalámbricos. Estas secuencias de comandos se utilizan en el capítulo 9, "Implementación de la infraestructura de seguridad para LAN inalámbricas".

Los trabajos que contienen estas secuencias de comandos son los siguientes:

- CreateWirelessGroups: este trabajo crea grupos de seguridad que se utilizan para administrar la autorización de usuarios y equipos, la inscripción de certificados y la aplicación de las directivas inalámbricas.
- GenPWD: este trabajo genera criptográficamente contraseñas aleatorias para los puntos de acceso inalámbricos y los servidores IAS. El trabajo utiliza CAPICOM para generar las cadenas aleatorias.

#### **Secuencias de comandos de administración de IAS**

En esta sección se describen las secuencias de comandos de administración de IAS.

- IASClientExport.bat e IASClientImport.bat: estos archivos por lotes permiten exportar la información de cliente RADIUS del servidor IAS a un disco para su almacenamiento seguro. La secuencia de comandos de importación importa la información de cliente RADIUS del servidor IAS desde un disco y la vuelve a cargar en el servidor IAS. Estas secuencias de comandos se utilizan en el capítulo 12, "Administración de la infraestructura de seguridad de LAN inalámbrica y RADIUS".
- IASExport.bat e IASImport.bat: la secuencia de comandos IASExport exporta el estado de configuración de IAS común (menos la información de clientes RADIUS) en archivos de texto de configuración que se encuentran en D:\IASConfig. Esta secuencia de comandos se ejecuta como un suceso nocturno mediante Programador de tareas y se utiliza para exportar la configuración de servidor RADIUS de IAS principal.

El archivo por lotes IASImport importa el estado de configuración de IAS exportado anteriormente de los archivos de texto de configuración que se encuentran en D:\IASConfig. Este archivo se utiliza para la recuperación de desastres y para generar los servidores IAS secundario y terciario descritos en el capítulo 8, "Implementación de la infraestructura de RADIUS" de la guía de generación. Estos archivos por lotes también se utilizan en el capítulo 12, "Administración de la infraestructura de seguridad de LAN inalámbrica y RADIUS".

- IAS\_Data.bat: este archivo por lotes crea, establece permisos y comparte las carpetas de IAS. Este archivo está configurado para ejecutarse desde el mismo dominio que los grupos empleados para aplicar permisos a las carpetas. Si no es el caso, edite la secuencia de comandos para utilizar el nombre de dominio explícito. Este archivo se utiliza en el capítulo 8, "Implementación de la infraestructura de RADIUS".

#### **Archivo complementario de IAS**

En esta sección se describe el archivo complementario de IAS.

- IASAccessPrep.txt: este archivo de texto contiene la línea de encabezado y los tipos de los datos de registro de solicitudes de RADIUS, que los auditores de seguridad de IAS los importan en Microsoft Access. Las instrucciones para utilizar este archivo se encuentran en el capítulo 12, "Administración de la infraestructura de seguridad de LAN inalámbrica y RADIUS".

#### **Archivos de instalación de componentes opcionales**

- OC\_AddIIS.txt y OC\_RemoveRootUpdate.txt: puede utilizar estos archivos de texto con el administrador de componentes opcionales de Windows (administrador OC) para especificar los componentes que se instalarán y quitarán. Estos archivos permiten la instalación automatizada de IIS y la eliminación del servicio de actualización de raíces. Estos archivos de texto se utilizan en el capítulo 7, "Implementación de la infraestructura de claves públicas".
- OC\_AddIAS.txt: puede utilizar este archivo de texto con el administrador OC para especificar los componentes que se instalarán con el fin de automatizar la instalación de IAS. Este archivo de texto se utiliza

en el capítulo 8, "Implementación de la infraestructura de RADIUS".

---

[↑ Principio de la página](#)

[Administre su perfil](#)

©2008 Microsoft Corporation. Todos los derechos reservados. [Póngase en contacto con nosotros](#) |  
[Aviso Legal](#) | [Marcas registradas](#) | [Privacidad](#)

