Contenido

[Capa de Servicios Web 2](#_Toc447728036)

[Capa de Presentación 5](#_Toc447728037)

# Capa de Servicios Web

**Servidores**:

*Balanceador*: BCRSICAD-app, TCP 28000, IP 172.21.16.87

*Nodo 1*: BCR0683ASIC41.

*Nodo 2*: BCR0683ASIC42.

El siguiente proceso de instalación debe realizarse en cada uno de los nodos indicados anteriormente.

1. Instalación

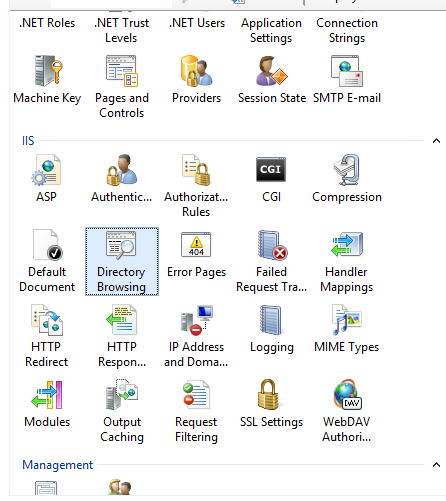
a). Crear el sitio en el IIS del servidor utilizando los compilados correspondientes.

b). En el archivo web.Config modificar las siguientes etiquetas.

|  |  |
| --- | --- |
| Nombre del Tag | Valor |
| **SICAD** | Data Source=BCRSICAD-BD,10000;Initial Catalog=SICAD;User Id=[Credencial asignado];Password=[Credencial asignado]; |
| **SICAD\_BITACORA** | Data Source= BCRSICAD-BD,10000;Initial Catalog=SICAD\_BITACORA;User Id=[Credencial asignado];Password=[Credencial asignado]; |
| **SICAD\_CONSOLIDADO** | Data Source=BCRSICAD-BD,10000;Initial Catalog=SICAD\_CONSOLIDADO;User Id=[Credencial asignado];Password=[Credencial asignado]; |
| **Endpoint BasicHttpBinding\_ISvAdministrarSesiones** | http://bcrServiciosGenerales-app:24001/BCR.ServiciosGenerales.SVL.SvAdministrarSesiones.svc |
| **Endpoint NetTcpBinding\_ISvAdministrarSesiones** | net.tcp://bcrServiciosGenerales-app:24001/BCR.ServiciosGenerales.SVL.SvAdministrarSesiones.svc |
| **decryptionKey** | [Valor según machineKey] |
| **validationKey** | [Valor según machineKey] |

c). Asignar el Application Pool que utiliza el sitio con el valor ApplicationPoolIdentity

d). Habilitar la Búsqueda en el Directorio



e). Verificar que el sitio creado se ejecute satisfactoriamente.

1. Creación de Log de Eventos.

a). Validar en el IIS que el Application Pool que utiliza el sitio este configurado con Identity = ApplicationPoolIdentity

b). Abrir la consola de Windows Powershell con derechos de administrador (Run as Administrator), en caso de no hacerlo así, el script generara error

c). Ejecutar la siguiente línea de comando:

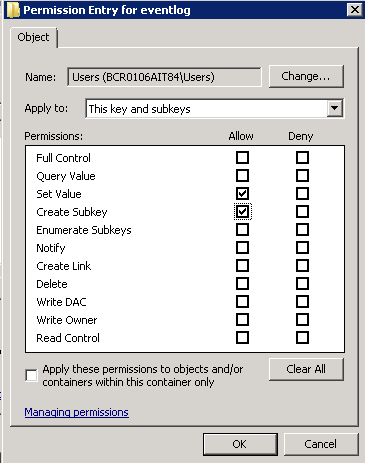
New-Eventlog –logname SICAD –Source SICAD

e). Dar exit a Windows PowerShell

f).En windows abrir el Regedit

g). Ir a la ruta HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\eventlog, clic derecho sobre esta opción y en: “Permissions” Agregar el usuario NETWORK SERVICE con Full Control

h). Agregar “Users” y dar permisos especiales de “Set Value” y “Create Subkey”. Para esto se da clic en Advanced y se edita o agrega el usuario desde la ventana de Advanced Security Settings.



i). Ir a la ruta HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security, clic derecho sobre esta opción y en: “Permissions” Agregar el usuario NETWORK SERVICE con permiso de Lectura, luego el usuario IIS\_IUSRS con Full Control y finalmente el usuario virtual con el nombre del Application Pool que ha sido configurado para la aplicación. Se debe buscar de la siguiente forma: IIS AppPool\”Nombre del Application Pool” con permiso de lectura.

j). Ir a la ruta “HKEY\_LOCAL\_MACHINE” ->”System” -> “CurrentControlSet” -> “Services” -> “EventLog” ->”SICAD”, clic derecho sobre esta opción y en: “Permissions” -> “Advanced” -> “Add” ->Usuario virtual con el nombre del Application Pool que ha sido configurado para la aplicación de SICAD. Se debe buscar de la siguiente forma: IIS AppPool\”Nombre del Application Pool” con permiso Full Control (estos usuarios los crea Windows de forma virtual, no se encuentran a nivel local si se hace una búsqueda general en el servidor).

# Capa de Presentación

**Servidores**:

*Balanceador*: BCRSICAD, TCP 28000, IP 172.21.8.48

*Nodo 1*: BCR0683WSIC21.

*Nodo 2*: BCR0683WSIC22.

El siguiente proceso de instalación debe realizarse en cada uno de los nodos indicados anteriormente.

1. Instalación

a). Crear el sitio en el IIS del servidor utilizando los compilados correspondientes.

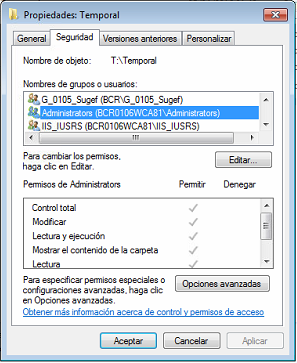
b). En el archivo web.Config modificar las siguientes etiquetas.

|  |  |
| --- | --- |
| Nombre del Tag | Valor |
| **MostrarErrorTecnico** | false |
| **ActiveDirectoryWS** | http://bcrsicad-app:28000/SicadActiveDirectoryWS.asmx |
| **SiteMapWS** | http://bcrsicad-app:28000/SicadSiteMapWS.asmx |
| **SeguridadWS** | http://bcrsicad-app:28000/SicadSeguridadWS.asmx |
| **SesionesWS** | http://bcrsicad-app:28000/SicadSesionesWS.asmx |
| **ConfiguracionWS** | http://bcrsicad-app:28000/SicadConfiguracionWS.asmx |
| **ContenidoWS** | http://bcrsicad-app:28000/SicadContenidoWS.asmx |
| **ListaWS** | http://bcrsicad-app:28000/SicadListasWS.asmx |
| **CatalogosSugefWS** | http://bcrsicad-app:28000/SicadCatalogosSugefWS.asmx |
| **ClasesDatosWS** | http://bcrsicad-app:28000/SicadClasesDatosWS.asmx |
| **HomologacionesWS** | http://bcrsicad-app:28000/SicadHomologacionesWS.asmx |
| **ProcesosWS** | http://bcrsicad-app:28000/SicadProcesosWS.asmx |
| **ServidorReportes** | https://bcrrepotesweb/Reportserver |
| **CarpetaReportes** | [Nombre de Carpeta asignada] |
| **UsuarioDominio** | [Nombre de usuario asignado para el acceso dfs] |
| **PasswordDominio** | [Password de usuario asignado para el acceso dfs] |
| **DescargaArchivosXML** | \\bcr.fi.cr\aplicaciones\0167\SICAD\ArchivosXML |
| **DescargaArchivosDBF** | [\\bcr.fi.cr\aplicaciones\0167\SICAD\ArchivosSalida](file://bcr.fi.cr/aplicaciones/0167/SICAD/ArchivosSalida) |
| **RutaCargaArchivos** | \\bcr.fi.cr\aplicaciones\0167\SICAD |
| **decryptionKey** | [Valor según machineKey] |
| **validationKey** | [Valor según machineKey] |

c). Asignar el Application Pool que utiliza el sitio con el valor ApplicationPoolIdentity

d). Establecer el archivo LogIn.aspx como página por defecto.

e). Asignar a la carpeta con el nombre Temporal (que se encuentra en los archivos compilados) permisos de “Control Total” para el usuario de acceso dfs (tag UsuarioDominio web.Config)



f). Verificar que el sitio creado se ejecute satisfactoriamente.

1. Creación de Log de Eventos.

a). Validar en el IIS que el Application Pool que utiliza el sitio este configurado con Identity = ApplicationPoolIdentity

b). Abrir la consola de Windows Powershell con derechos de administrador (Run as Administrator), en caso de no hacerlo así, el script generara error

c). Ejecutar la siguiente línea de comando:

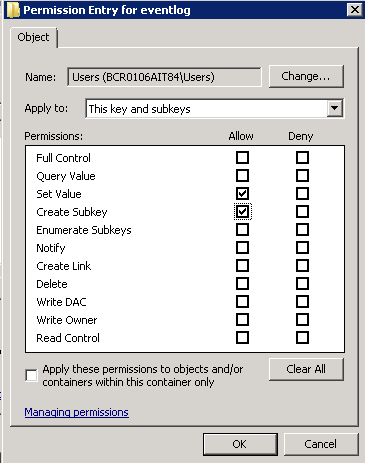
New-Eventlog –logname SICAD –Source SICAD

e). Dar exit a Windows PowerShell

f).En windows abrir el Regedit

g). Ir a la ruta HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\eventlog, clic derecho sobre esta opción y en: “Permissions” Agregar el usuario NETWORK SERVICE con Full Control

h). Agregar “Users” y dar permisos especiales de “Set Value” y “Create Subkey”. Para esto se da clic en Advanced y se edita o agrega el usuario desde la ventana de Advanced Security Settings.



i). Ir a la ruta HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Security, clic derecho sobre esta opción y en: “Permissions” Agregar el usuario NETWORK SERVICE con permiso de Lectura, luego el usuario IIS\_IUSRS con Full Control y finalmente el usuario virtual con el nombre del Application Pool que ha sido configurado para la aplicación. Se debe buscar de la siguiente forma: IIS AppPool\”Nombre del Application Pool” con permiso de lectura.

j). Ir a la ruta “HKEY\_LOCAL\_MACHINE” ->”System” -> “CurrentControlSet” -> “Services” -> “EventLog” ->”SICAD”, clic derecho sobre esta opción y en: “Permissions” -> “Advanced” -> “Add” ->Usuario virtual con el nombre del Application Pool que ha sido configurado para la aplicación de SICAD. Se debe buscar de la siguiente forma: IIS AppPool\”Nombre del Application Pool” con permiso Full Control (estos usuarios los crea Windows de forma virtual, no se encuentran a nivel local si se hace una búsqueda general en el servidor).