Capítulo 11

Requisitos previos

☒Tener conocimientos básicos de la administración de Windows Server 2016.

☒Tener nociones básicas de la gestión de permisos NTFS.

☒Saber gestionar una infraestructura AD CS.

Objetivos

☒Comprender la gestión de derechos AD RMS.

☒Conocer los diferentes componentes de una infraestructura AD RMS.

☒Saber instalar una infraestructura AD RMS.

☒Saber configurar una infraestructura AD RMS.

☒Saber implementar una infraestructura AD RMS.

☒Saber proteger la integridad de los datos.

A. Servicios de gestión de derechos

A partir de Windows Server 2008, los servicios de gestión de derechos digitales se presentan bajo la forma de un rol de servidor llamado AD RMS (*Active Directory Rights Management Services*). AD RMS permite extender los permisos de seguridad NTFS para aportar una seguridad complementaria pensada para proteger la integridad de los datos. En comparación, los servicios de administración de derechos en Windows Server realizan las mismas funciones que la gestión de derechos digitales para el contenido de audio o vídeo (DRM, *Digital Rights Management*).

1. Presentación de AD RMS

AD RMS es un rol de servidor que permite proteger la integridad de los datos generados en su empresa. Este rol permite, en particular, preservar la propiedad intelectual, así como el contenido de datos hospedados o intercambiados con otros asociados. La protección de un servidor de archivos con los permisos tradicionales NTFS pueden verse limitados en un proceso de gestión de derechos digitales. AD RMS permite extender la seguridad de NTFS para proteger, por ejemplo, el contenido de los archivos de Office. Cuando un usuario accede a un recurso compartido de red para abrir un documento de Word, el sistema verifica las ACL para comprobar que el usuario está autorizado a leer o modificar el contenido. Sin embargo, una vez que se abra el documento, la seguridad NTFS no puede impedir que el contenido se conserve. De este modo, el usuario que abra el archivo también puede imprimir los datos visualizados o copiarlos para modificarlos más tarde. AD RMS permite responder a esta necesidad de seguridad implementando una capa adicional a través de una nueva tecnología que puede basarse en los componentes AD DS (Servicios de dominio de Active Directory), AD CS (Servicios de certificados) y AD FS (Servicios de federación). Mediante la implementación del rol de servidor AD RMS, es posible proteger el contenido de sus datos tanto en el interior de su red empresarial como en el exterior. Este rol de servidor es, en cierta medida, una evolución del servicio de administración de derechos de Microsoft (RM: *Rights Management*), disponible con el sistema operativo Windows Server 2003 en la forma de un servicio de Windows llamado RMS (*Rights Management Services*).

a. Funcionamiento de AD RMS

Para proteger los datos confidenciales de su empresa, una infraestructura de gestión de derechos Active Directory se basa en un conjunto de servidores AD RMS que gestionan el conjunto de reglas de protección de los datos, así como el intercambio de certificados y licencias de acceso al servicio. La configuración de la infraestructura, así como los registros de actividad, se almacenan en una base de datos. Los usuarios acceden al contenido protegido y cifrado mediante un cliente AD RMS que se autentica automáticamente en un directorio Active Directory con objeto de garantizar que el usuario está habilitado para utilizar el contenido protegido. El usuario obtiene, a continuación, un certificado que le permite descifrar los datos protegidos. Los servicios de gestión de derechos se basan a su vez en los servicios web IIS. El conjunto de usuarios o grupos que deben tener acceso a los servicios de administración de derechos Active Directory deben poseer una dirección de correo electrónico configurada en su perfil Active Directory.

AD RMS es compatible en particular con las siguientes aplicaciones:

- Pack Office 2007 / 2010 / 2013 y posteriores.
- Microsoft SharePoint 2003 / 2007 / 2013 y posteriores.
- Microsoft Exchange Server 2007 / 2010 / 2013 y posteriores.
- XPS Viewer.
- Internet Explorer (requiere la instalación de un módulo complementario).
- Adobe Acrobat Reader.

La instalación de una infraestructura de este tipo requiere la formación de los usuarios, ya que son ellos los que deben definir los elementos que se han de securizar indicando si el documento puede ser sobreescrito, copiado, impreso, etc. Estos datos se almacenan directamente en el documento, de manera que puede intercambiarse fuera de la infraestructura de red empresarial. Solo los usuarios autenticados o que dispongan de un certificado válido pueden acceder a los datos protegidos. Cuando un usuario securiza un documento empleando los servicios de administración de derechos, la infraestructura AD RMS genera una licencia de uso que se almacena dentro del documento. Si el usuario forma parte de su organización, o de una entidad aprobada por los servicios de federación, el cliente AD RMS instalado en la máquina cliente solicita automáticamente una licencia de uso a la infraestructura AD RMS.

Para facilitar la gestión de los derechos cuando un usuario genera contenido, un administrador de la infraestructura AD RMS puede, a su vez, desplegar plantillas de directivas de permisos. En función del uso del contenido, un usuario podrá aplicar la plantilla de directiva directamente sin tener que preocuparse de los elementos que es preciso configurar para proteger eficazmente su contenido.

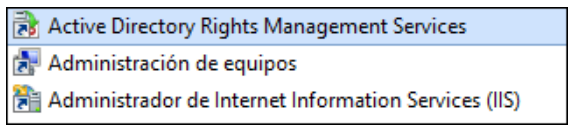
La instalación de un servidor AD RMS crea un primer servidor en un clúster raíz. Este clúster no necesita contar con las tecnologías de clustering de Microsoft o de equilibrio de carga de red. Un clúster raíz AD RMS aporta simplemente una solución de alta disponibilidad para las peticiones de los usuarios utilizando una tecnología propia de los servicios de gestión de derechos de Active Directory. Si la infraestructura AD RMS va a trabajar con un solo servidor de gestión de derechos, es posible utilizar una base de datos interna llamada WID (*Windows Internal Database*), que está integrada en el sistema operativo. Esta instancia de base de datos solo permite la creación de un único servidor en el clúster AD RMS raíz. Una infraestructura AD RMS soporta como mínimo la utilización de una base de datos Microsoft SQL Server 2008.

La instalación del primer servidor del clúster raíz AD RMS necesita la creación de una clave de cifrado. Esta clave debe asignarse a todos los servidores que se unan al clúster para que estos puedan, a su vez, cifrar los certificados o las licencias que se han de transmitir a los usuarios. Existen dos métodos de almacenamiento de esta clave de cifrado:

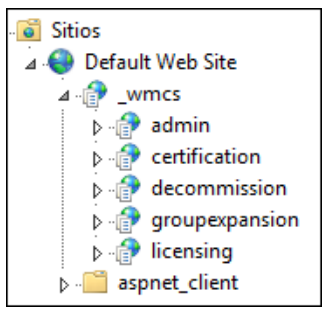
- **Almacenamiento centralizado**: permite almacenar la clave de cifrado en la base de datos del clúster AD RMS. De esta forma, cada servidor que se una al clúster puede recuperar automáticamente la clave de cifrado sin intervención del administrador.
- **Almacenamiento manual**: obliga a seleccionar un proveedor de servicios criptográfico para cifrar la clave, que debe almacenarse, posteriormente, de forma manual. Cada servidor que solicite unirse al clúster debe recuperar esta clave de cifrado antes de integrarse en el clúster raíz AD RMS.

b. Administración de AD RMS

La administración del rol de servidor AD RMS se realiza mediante un complemento ubicado en la siguiente ruta: **%SYSTEMROOT%\system32\AdRmsAdmin.msc**

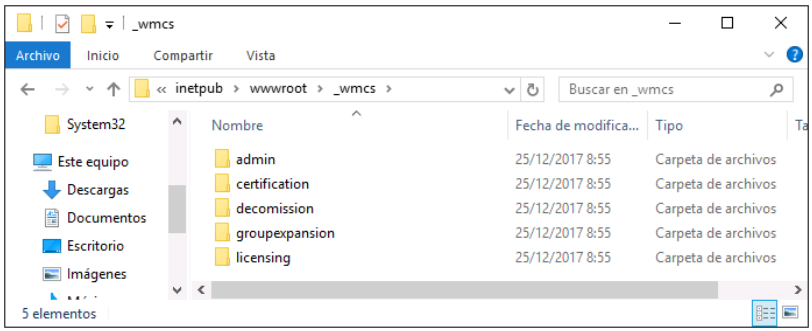


El clúster AD RMS raíz es accesible a través de una URL que es preferible asociar a un alias DNS declarado previamente en el servidor de nombres de su organización. El clúster AD RMS raíz utiliza las carpetas virtuales siguientes en el árbol del sitio web predeterminado:



Estas carpetas virtuales albergan los servicios web utilizados por la gestión del clúster AD RMS. La consola de administración está configurada para apuntar a la URL del clúster AD RMS utilizando los protocolos HTTP o HTTPS según la configuración del administrador de servicios de Internet (IIS). En entornos de producción, es preferible securizar el acceso al clúster AD RMS implementando la autenticación SSL, con lo que se ofrece así una protección mediante un certificado.

Las carpetas virtuales dedicadas a la administración de los servicios de gestión de derechos se almacenan de manera local en la carpeta siguiente: **C:\inetpub\wwwroot_wmcs**

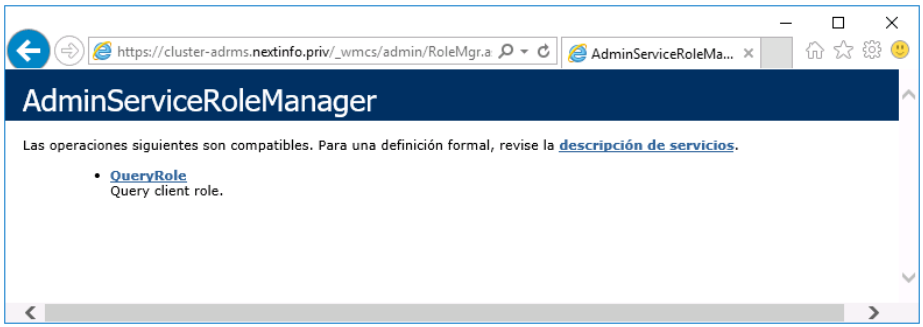


Para verificar si el servicio web administrador de roles AD RMS está operativo, basta con acceder a la URL siguiente:

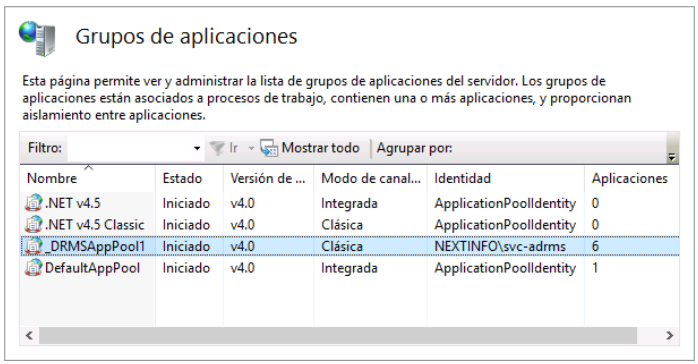
http://<Alias DNS del clúster>/_wmcs/admin/RoleMgr.asmx

o bien

https://<Alias DNS del clúster>/_wmcs/admin/RoleMgr.asmx



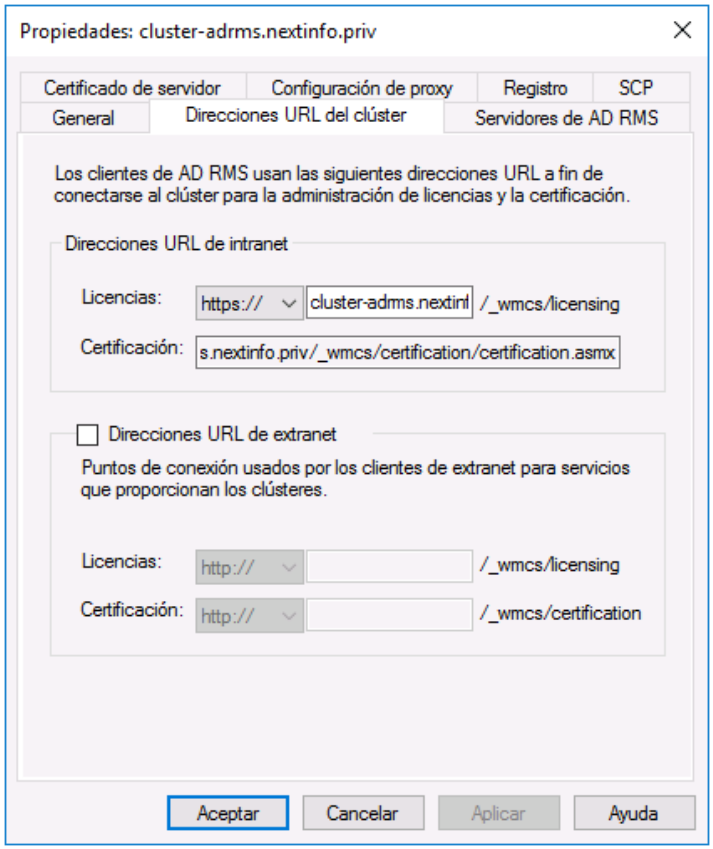
Los servicios web AD RMS se gestionan a través de un grupo de aplicaciones llamado **_DRMSAppPool1**. Este grupo de aplicaciones utiliza la cuenta de servicio introducida durante la instalación del rol de servidor AD RMS basándose en el **Framework .NET 4.0.30319**.



El administrador de licencias AD RMS está accesible en la URL siguiente:

https://cluster-adrms.<dominio DNS>/_wmcs/licensing

Es posible, no obstante, modificar en cualquier momento la URL del administrador de licencias a través de las propiedades del clúster AD RMS, haciendo clic en la pestaña **Direcciones URL del clúster**. En esta misma pestaña, es posible configurar las URL de la extranet, para hacer que AD RMS esté disponible desde el exterior de la red empresarial:



El administrador de certificados AD RMS está disponible en la URL siguiente:

https://cluster-adrms.<dominio DNS>/_wmcs/certification/certification.asmx