UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE SOLUCIONES DE SEGURIDAD INFORMÁTICA EN PLATAFORMAS WINDOWS Y UNIX

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

P R E S E N T A

RICARDO ANDRÉS CARMONA DOMÍNGUEZ

ASESOR DE INFORME

M.I. NORMA ELVA CHÁVEZ RODRÍGUEZ

Ciudad Universitaria, Cd. Mx., 2016

Implementación de soluciones de seguridad informática en plataformas Windows y UNIX

Nombre de la Organización: Coordinación de Seguridad de la Información/UNAM-CERT, perteneciente a la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

CONTENIDO

ÍNDICE DE IMÁGENES

CAPÍTULO I

CAPÍTULO III

ÍNDICE DE TABLAS

CAPÍTULO II

CAPÍTULO III

Introducción

INTRODUCCIÓN

En este documento describo las actividades que he realizado en la Coordinación de Seguridad de la Información/UNAM-CERT para obtener el título de Ingeniero en Computación por parte de la Facultad de Ingeniería, haciendo uso de la modalidad de titulación por Trabajo Profesional.

La Coordinación de Seguridad de la Información/UNAM-CERT es una organización que busca contribuir con la comunidad universitaria a través de la divulgación y fomento de la cultura de seguridad informática. Así mismo, ofrece servicios de seguridad a las diversas entidades de la Universidad Nacional Autónoma de México y externas que los requieran.

Durante mi instancia en la Coordinación he participado en diversos proyectos, de los cuales he retomado los dos que considero más relevantes para presentarlos en este trabajo.

Muchas organizaciones se fundamentan en el valor de su propiedad intelectual. La pérdida de esta propiedad, el mal uso, la realización de copias no autorizadas o el robo, pueden causar daños incuantificables a sus operaciones. No es necesario tener una empresa muy grande para beneficiarse de alguna forma de la gestión de derechos.

Para esto, he contribuido con la CSI/UNAM-CERT en aspectos de protección de propiedad intelectual mediante la implementación del rol Active Directory Rights Management Services, para aumentar la estrategia de seguridad al proteger información mediante directivas de uso persistentes, que permanecen con la información, independientemente del lugar en donde se encuentre.

El otro proyecto que abordo se deriva del Convenio de Colaboración con el Instituto Nacional Electoral (INE), en el cual la CSI/UNAM-CERT a través de la Dirección General de Cómputo y de Tecnologías de la Información y Comunicación (DGTIC) de la UNAM llevó a cabo la revisión de configuraciones de seguridad a la infraestructura de Tecnologías de Información que sería utilizada para el Programa de Resultados Electorales Preliminares (PREP) 2015.

Destaco las actividades en las que participé, las cuales incluyen el análisis de la información de configuraciones de los dispositivos de la infraestructura de Tecnologías de Información del “PREP 2015” con base en buenas prácticas de seguridad informática para identificar oportunidades de mejora y emitir recomendaciones orientadas al fortalecimiento de la misma.

CAPÍTULO I - DESCRIPCIÓN DE LA COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN/UNAM-CERT

CAPÍTULO I - DESCRIPCIÓN DE LA COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN/UNAM-CERT

La Coordinación de Seguridad de la Información (CSI) /UNAM-CERT es "un punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesorías y servicios de seguridad; así como para intercambiar experiencias y puntos de vista, logrando con ello, establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad y difundir la cultura de la seguridad en cómputo." [1]

A continuación muestro un breve panorama de la CSI/UNAM-CERT con el fin de contextualizar al lector sobre la organización e indicar la importancia de la misma en la Universidad Nacional Autónoma de México y en el país.

I.1 MISIÓN

Contribuir al desarrollo de la UNAM, a través de la prestación de servicios especializados, la formación de capital humano y el fomento de la cultura de seguridad de la información.

I.2 VISIÓN

Consolidar a la UNAM como la entidad líder en materia de Seguridad de la Información en el país.

I.3 OBJETIVOS

- Proporcionar servicios de seguridad de la información para la UNAM y otras organizaciones.
- Promover la cultura de seguridad de la información.
- Formar especialistas que desarrollen y apliquen estrategias de protección de la información.
- Difundir contenidos especializados en seguridad de la información.
- Colaborar con instituciones nacionales e internacionales en materia de detección y respuesta a incidentes.
- Elaborar políticas y lineamientos de seguridad de la información para las dependencias y entidades académicas universitarias.

[1] Coordinación de Seguridad de la Información. Principios. Recuperado el 3 de marzo de 2016, de http://www.seguridad.unam.mx/acerca/principios.dsc

I.4 HISTORIA

La seguridad de la información no es un tema que haya surgido recientemente. Me atrevo a decir que desde el momento en que los seres humanos fuimos capaces de almacenar y transmitir información surgió la necesidad de protegerla de aquellos a quienes no estaba destinada. Para esto surgieron diferentes técnicas de protección, que van desde su almacenamiento custodiado hasta el uso de algoritmos criptográficos.

La seguridad de la información, entonces, debe adaptarse a las nuevas técnicas y tecnologías con el fin de garantizar que la información se mantenga confidencial, íntegra y esté disponible para aquellas personas destinadas a hacer uso de ella.

Hoy en día, debido a la gran expansión de los equipos de cómputo y su uso a lo largo del planeta, grandes cantidades de información comenzaron a ser almacenadas de forma digital dado que este formato ofrece ventajas como facilidad de administración, flexibilidad, eficiencia, entre otras. Nuevamente, la seguridad de la información tuvo que adoptar las nuevas tecnologías y generar nuevos métodos para la protección de los datos.

Muchas organizaciones entre las que destacan gobiernos, industrias y universidades han estado preocupadas por la protección de la información, la UNAM no es la excepción.

Según la tesis del Ingeniero Diego Martín Zamboni:

> *'Desde 1975 se tenían problemas de seguridad en cómputo. Estos eran con los sistemas Burroughs. Ya había en ese entonces en la Universidad gente con la capacidad y el interés de romper las barreras de seguridad impuestas por el sistema, por "el simple gusto de hacerlo". Contra estas violaciones de seguridad nunca fue posible tomar alguna acción formal debido a la falta de legislación al respecto, así como las fricciones y conveniencias políticas que, desgraciadamente, siempre han invadido los ámbitos académico y científicos en nuestra Universidad.'*[2]

Para solventar este problema surgió el Área de Seguridad en Cómputo, que con paso de los años ha evolucionado a la par del avance tecnológico y del surgimiento de nuevas amenazas a los sistemas informáticos hasta convertirse en la Coordinación de Seguridad de la Información. A continuación presento los acontecimientos que considero más relevantes en la historia de UNAM-CERT.

[2] Martín, D. Junio 1995. Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix. Recuperado el 10 de diciembre de 2015, de http://homes.cerias.purdue.edu/~zamboni/pubs/thesis-bs.pdf

1993
Dadas las deficiencias mencionadas por el Ingeniero Martín Zamboni en su tesis y diversos incidentes de seguridad, en 1993 se realizó el primer contacto con el Coordination Center de Carnellie Mellon de Estados Unidos o Computer Emergency Response Team (CERT/CC). El CERT/CC es el primer equipo de respuesta a incidentes de todo el mundo y ha realizado varias contribuciones al área de seguridad de la información.

Ese mismo año, en Ingeniero Martín Zamboni creó el Equipo de Respuesta a Incidentes en Seguridad en Cómputo, perteneciente a la entonces Dirección General de Servicios de Cómputo Académico (DGSCA), hoy DGTIC.

1994
El Área de Seguridad en Cómputo organizó la primera edición del Día Internacional de la Seguridad en Cómputo en México, que en años posteriores se utilizó para ofrecer pláticas de concientización de seguridad.

1998
Las pláticas del DISC fueron ofrecidas por ponentes de organizaciones especializadas en seguridad, de México y del extranjero. Esta edición del DISC es considerada como la primera edición del Congreso de Seguridad en Cómputo de UNAM-CERT.

1999
El Lic. Juan Carlos Guel López toma la jefatura del Área de Seguridad en Cómputo y bajo su liderazgo se convierte en el Departamento de Seguridad en Cómputo (DSC), se aumentan los recursos asignados a la organización, tanto humanos como materiales, lo que permitió que se ampliara el ámbito de acción del DSC a otras dependencias de la UNAM.

1999 – 2001
En México no existía ningún equipo de respuesta a incidentes que fuera reconocido internacionalmente, por lo que se vio la necesidad de ubicarse como punto de contacto internacional para atender incidentes no sólo en RED-UNAM, sino en México, por esa razón se inició el trámite y se obtuvo la acreditación ante el Forum of Incident Response Security Teams (FIRST). Al mismo tiempo, la acreditación le permitió a UNAM-CERT obtener visibilidad internacional para lograr acuerdos con grupos nacionales e internacionales.

2003
Mediante la colaboración de la ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior), se crea la Red Nacional de Seguridad en Cómputo (RENASEC), con el objetivo de albergar y compartir las iniciativas, acuerdos y noticias en materia de seguridad informática, a más de 145 Instituciones de Educación Superior del país.

2005
UNAM-CERT se une al Proyecto Honeynet mediante Honeynet UNAM-CHAPTER. La participación de UNAM-CERT en el Proyecto Honeynet le permitió establecer nuevos vínculos

con organizaciones internacionales y estar a la vanguardia de nuevas tecnologías de detección de intrusos, análisis de malware, respuesta a incidentes y cómputo forense.

2010
El Departamento de Seguridad en Cómputo se convierte en Subdirección de Seguridad de la Información. Se obtiene la certificación ISO 27001:2005 para el proceso de respuesta y atención a incidentes de seguridad.

2014
La Subdirección cambia su nombre a Coordinación de Seguridad de la Información (CSI), con lo que se actualiza el alcance y el ámbito de acción de la organización.

2015
Se llevó a cabo la transición de la certificación ISO 27001:2005 a su versión 2013.

I.5 SERVICIOS

Para lograr sus objetivos la CSI ofrece una serie de servicios, organiza diversos eventos, imparte cursos, seminarios, pláticas, difunde información y realiza investigaciones.

Los servicios de Seguridad en Tecnologías de la Información ofrecidos a organizaciones internas y externas son:

- Implementación de ISMS de acuerdo al estándar ISO 27001
- Auditoría informática
- Análisis forense
- Análisis de vulnerabilidades y pruebas de penetración
- Análisis de tráfico de red
- Análisis de riesgos
- Respuesta a incidentes de seguridad de la información
- Revisión de configuraciones
- Creación de políticas de seguridad de la información
- Auditoría de código
- Programas de capacitación

Uno de los servicios de mayor valor que proporciona la CSI/UNAM-CERT es la transferencia de conocimiento. Este servicio se proporciona a través de sus programas de capacitación, ya sea por medio de cursos a la medida o de sus líneas de especialización.

I.5.1 PROGRAMA DE BECAS DE FORMACIÓN EN SEGURIDAD INFORMÁTICA

La Coordinación de Seguridad de la Información cuenta con un plan de becarios desde 1995 en dónde busca especializar a los asistentes en temas de seguridad y otras áreas, como programación, bases de datos, buenas prácticas de administración de sistemas, legislación, administración de proyectos, entre otros.

Actualmente, este plan de becarios está dividido en 5 módulos:

1. Especialista en Seguridad en redes y sistemas operativos
2. Especialista en Seguridad en Sistemas
3. Especialista en análisis de vulnerabilidades y hacking ético
4. Especialista en respuesta a incidentes
5. Gestión de la seguridad de la información

Actualmente, alumnos de la Universidad y de otras instituciones pueden participar en el programa, con lo que la Coordinación busca cumplir su objetivo de formar especialistas que desarrollen y apliquen estrategias de protección de la información.

I.5.2 CONGRESO DE SEGURIDAD EN CÓMPUTO

Como mencioné en la sección de Historia, el Congreso de Seguridad en Cómputo tuvo su primera edición en el año de 1998 en el marco del Día Internacional de Seguridad en Cómputo (DISC).

Durante este evento se imparten cursos de alta especialización sobre seguridad de la información y se desarrollan conferencias con la participación de destacados especialistas nacionales e internacionales.

I.6 ESTRUCTURA ORGANIZACIONAL

I.6.1 DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

La Dirección General de Cómputo y de Tecnologías de la Información (DGTIC) es la entidad de la UNAM que gestiona los asuntos relacionados con seguridad de la información, cómputo de alto rendimiento, redes avanzadas, visualización científica asistida por computadora, realidad virtual, entre otros.

En la DGTIC se desarrollan soluciones que "requieren una visión integral y estratégica, así como la aplicación de las Tecnologías de Información y Comunicación." [3]

DGTIC "contribuye al logro de los objetivos de la UNAM como punto de unión de la comunidad universitaria para aprovechar los beneficios que las tecnologías de la información y las comunicaciones pueden aportar a la docencia, la investigación, la difusión de la cultura y la administración universitaria." [4]

I.6.1.1 ORGANIGRAMA – DGTIC

La DGTIC está dividida en diez áreas, como podemos ver en la *Imagen I.1*, se cuentan con dos Coordinaciones, cinco Direcciones, una Subdirección y una Unidad Administrativa, todos bajo la Dirección General del Dr. Felipe Bracho Carpizo.

Dentro del organigrama mostrado, destaco a la Dirección de Sistemas y Servicios Institucionales (DSSI) a cargo del Act. José Fabián Romo Zamudio. Bajo esta dirección se encuentran Departamentos y Coordinaciones entre los que destacan:

- **Coordinación de Seguridad de la Información**
- Supercómputo
- Departamento de Visualización y Realidad Virtual
- Departamento de Firma Electrónica Avanzada
- Departamento de Administración de Servidores
- Servicios del Centro de Datos

[3] Universidad Nacional Autónoma de México. Marzo 2014. *Iniciativas de Colaboración y vinculación.* Recuperado el 3 de Marzo de 2016, de http://colaboracion-vinculacion.tic.unam.mx/

[4] Universidad Nacional Autónoma de México. 19 de Abril de 2012. *¿Quiénes somos?* Recuperado el 3 de Marzo de 2016, de http://www.tic.unam.mx/mision.html

IMAGEN I. 1 - ORGANIGRAMA DGTIC[5]

I.6.2 COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN

La CSI apoya a la Dirección de Sistemas y Servicios Institucionales a cumplir con sus objetivos, capacitando a los administradores de TI para operar bajo estándares de seguridad en cómputo, respondiendo a incidentes de seguridad de la información, realizando auditorías informáticas, revisión de configuraciones, análisis forense y pruebas de penetración.

Para solventar los servicios que la CSI ofrece a la Universidad y entidades externas es necesario contar con personal capacitado en diferentes áreas de seguridad de la información.

[5] Universidad Nacional Autónoma de México. 2015. *Organigrama*. Recuperado el 3 de Marzo de 2016, de http://www.tic.unam.mx/imgs/tic/organigrama_dgtic_2015.png

I.6.2.1 ORGANIGRAMA – CSI/UNAM-CERT

Como se observa en la *Imagen I.2,* la Coordinación de Seguridad de la Información está dividida en 5 departamentos bajo el cargo del Coordinador de Seguridad de la Información, el Mtro. José Roberto Sánchez Soledad. En el organigrama mostrado destaco al Departamento de Operación Interna. Este Departamento cuenta con cuatro puestos cuyos nombres y funciones listo a continuación:

- **Especialista en Seguridad en Windows:** Aplicación de los principios de seguridad, buenas prácticas administrativas y herramientas de seguridad para los sistemas operativos Windows.
- **Administrador de Aplicaciones:** Administración de la infraestructura Windows y plantillas de auditoría.
- **Especialista en Seguridad en UNIX:** Implementación de seguridad en aplicaciones, servicios y servidores sobre sistemas operativos UNIX.
- **Especialista en Seguridad en Red:** Implementación de procesos y dispositivos para la protección perimetral y monitoreo de redes.

Actualmente me desempeño en el puesto de Especialista en Seguridad en Windows, que describo más a detalle en el siguiente capítulo.

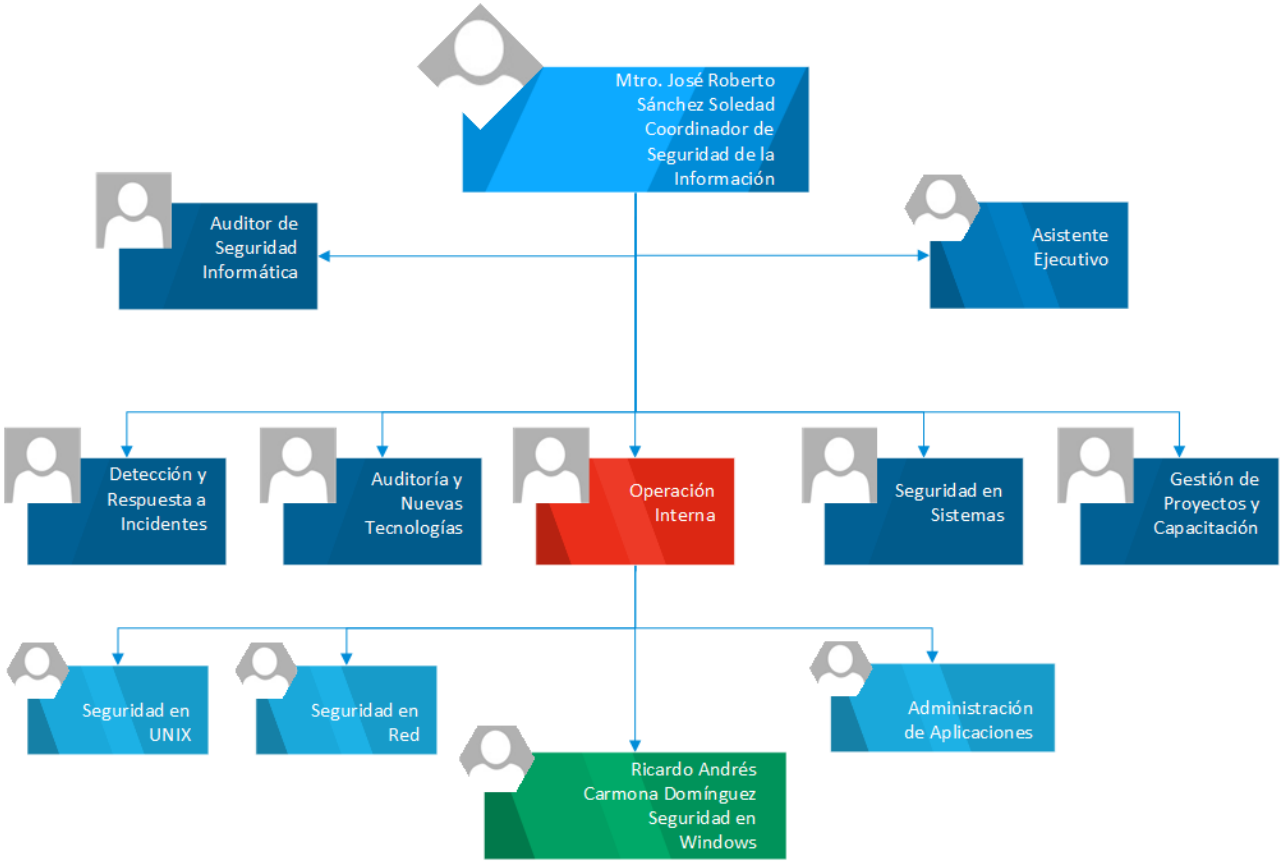


IMAGEN I. 2 - ORGANIGRAMA UNAM-CERT

CAPÍTULO II - PUESTO DE TRABAJO

CAPÍTULO II - PUESTO DE TRABAJO

II.1 INGRESO AL PUESTO DE TRABAJO

En mi último semestre en la Facultad de Ingeniería (2014-1), estando registrado en el módulo de Redes y Seguridad, apliqué para el Programa de Becas de Formación en Seguridad Informática impartido por la CSI y del que ya hablé brevemente en el capítulo anterior.

El proceso de selección consiste en una serie de exámenes psicométricos, psicológicos, de conocimientos y entrevistas con los miembros de la Coordinación.

El examen de conocimientos aborda temas como programación, sistemas operativos, redes, bases de datos, matemáticas y lógica, temas que la Facultad de Ingeniería cubre con su plan de estudios, lo que me proporcionó los conocimientos necesarios para afrontar estas pruebas y obtener un resultado aprobatorio para continuar con la fase de selección.

Al terminar dicho proceso fui seleccionado entre más de 100 aspirantes para formar parte de los 30 que tomarían la capacitación en seguridad informática y formarían a la octava generación de becarios, la cual dio inicio en agosto de 2013.

Durante el primer módulo (Agosto – Diciembre 2013) me capacité como Especialista en seguridad en redes y sistemas operativos. Los cursos de este módulo me sirvieron para reforzar los conocimientos de redes, sistemas operativos y seguridad de la información adquiridos durante dichas materias en la facultad. Fue en los cursos de Administración y seguridad en Windows y Unix donde adquirí los conocimientos adicionales que me permiten desempeñar mi puesto de trabajo óptimamente.

En este primer módulo participé en proyectos de administración e implementación de infraestructura tecnológica, dichos proyectos sirvieron como base para implementaciones que la Coordinación de Seguridad de la Información retomó tiempo después.

En 2014, debido a la rotación de personal en la CSI, surgió la oportunidad de ingresar al puesto de Especialista en Seguridad en Windows a cargo del Departamento de Operación Interna. Durante el proceso de selección se evaluaron mis habilidades, se me realizaron exámenes de conocimientos, donde nuevamente la Facultad de Ingeniería me preparó para afrontar las pruebas.

Una vez aprobados los exámenes de conocimientos logré obtener el puesto, en el cual he laborado desde mayo de 2014.

II.2 ESPECIALISTA EN SEGURIDAD EN WINDOWS

El puesto de Especialista en Seguridad en Windows se desempeña bajo el departamento de Operación Interna como muestro en el organigrama de la Coordinación de Seguridad de la Información del capítulo anterior (*IMAGEN I.2*), y está pensado para personas que hayan estudiado una licenciatura o sean estudiantes de los últimos semestres en ingeniería en computación, ingeniería en telecomunicaciones o carreras afines.

Las habilidades requeridas para el desempeño del puesto son:

- Capacidad de aplicación de los conocimientos de seguridad en sistemas y redes Microsoft.
- Habilidades para el desarrollo y elaboración de guías, manuales.
- Conocimientos para proporcionar asesorías y apoyo a entidades internas y externas a la UNAM.

Estas habilidades son necesarias para cumplir con las funciones del puesto y desarrollar las actividades de manera óptima.

II.3 – ACTIVIDADES DEL PUESTO DE TRABAJO

Mis actividades en la Coordinación de Seguridad de la Información están enfocadas en la administración y aplicación de principios de seguridad en servicios y servidores que funcionen bajo el sistema operativo Windows. De manera adicional, he trabajado con sistemas operativos GNU/Linux con la finalidad de proporcionar compatibilidad de servicios entre ambos sistemas operativos.

Las actividades que realizo de forma recurrente en la Coordinación son las siguientes:

- Gestión, monitoreo y mantenimiento
- Apoyo en incidentes de seguridad informática
- Publicación de noticias de seguridad informática
- Traducción y publicación de boletines de Microsoft

II.3.1 GESTIÓN, MONITOREO Y MANTENIMIENTO

Esta actividad la muestro en 7 actividades secundarias con la finalidad de ofrecer un panorama más específico de mis labores. De no realizarse, la Coordinación de Seguridad de la Información incumpliría con los controles del Anexo A del estándar ISO 27001:2013 listados a continuación:

- A.8.1.1 Inventario de Activos
- A.9.2 Gestión de acceso de usuarios
- A.11.2.4 Mantenimiento de equipos
- A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
- A.12.6.2 Control de software operacional

OBJETIVO GENERAL

Mantener en funcionamiento óptimo los servicios internos ofrecidos por la Coordinación de Seguridad de la Información para apegarse al cumplimiento del estándar ISO 27001:2013.

DESARROLLO

Las siguientes tablas (de la Tabla II. 1 a la Tabla II. 7) muestran las actividades realizadas para el cumplimiento de los controles mencionados anteriormente, el periodo de tiempo en que se realizan y los resultados obtenidos.

TABLA II. 1 - ADMINISTRACIÓN DE LOS USUARIOS Y EQUIPOS DEL DOMINIO

Actividad	**Administración de los usuarios y equipos del dominio**
Objetivo	Mantener actualizada la base de datos de equipos y usuarios activos.
Periodicidad	Quincenal - La actividad se realiza una vez cada 15 días, en caso de algún cambio extraordinario la actualización de la base de datos se hace de forma inmediata.
Desarrollo	Haciendo uso de la consola *"Users And Computers"* del rol *"Active Directory Domain Services"* [1] de Windows puedo verificar qué usuarios continúan activos en el sistema y deshabilitar las cuentas que estás hayan sido comprometidas o que ya no estén en uso. Los equipos que se den de baja por obsolescencia también deben ser dados de baja en la base de datos de Active Directory. Al cambiar la membresía de un usuario a un grupo en específico garantizo que las políticas de seguridad asociadas a este apliquen de igual forma al usuario, permitiendo crear una separación de roles y privilegios.
Resultados	La base de datos de Active Directory con los usuarios, equipos y privilegios de los mismos se encuentra actualizada constantemente, garantizando el cumplimiento de los controles A.8.1.1 y A.9.2 del ISO 27001:2013.

TABLA II. 2 - INVENTARIO DE EQUIPOS

Actividad	**Inventario de equipos**
Objetivo	Mantener actualizado el inventario de equipos asignados por la DGTIC a la Coordinación de Seguridad de la Información.
Periodicidad	La actividad se realiza en conjunto con el área de Bienes y Suministros de la DGTIC en caso de algún cambio en la lista de bienes asignados.
Desarrollo	La DGTIC a través del Área de Bienes y Suministros asigna a los diferentes departamentos y coordinaciones equipos de cómputo y mobiliario para el desarrollo de las actividades. Estos equipos al ser propiedad de la UNAM deben ser inventariados y cualquier cambio (altas y bajas) en las listas de asignación por departamento debe ser notificado. Mi trabajo consiste en ubicar los equipos nuevos o que estén en proceso de baja y verificar que los datos de los mismos corresponden con los publicados en las listas de inventario para evitar inconsistencias.
Resultados	Las listas de inventario se encuentran actualizadas, sin inconsistencias y han sido verificadas con el área de Bienes y Suministros. El desarrollo de esta actividad garantiza el cumplimiento del control A.8.1.1 del Anexo A del estándar ISO 27001:2013.

TABLA II. 3 - MONITOREO DE EQUIPOS

Actividad	**Monitoreo de equipos**
Objetivo	Identificar riesgos o fallas en los servidores a cargo del Departamento de Operación Interna derivados del uso de recursos y carga de trabajo.
Periodicidad	La actividad se realiza semanalmente. En caso de algún evento extraordinario la actividad se realiza cuando se presenta una alerta.
Desarrollo	Cada viernes antes de finalizar la jornada laboral, verifico el estado de los servidores con la finalidad de identificar riesgos de operación. El Departamento de Operación Interna cuenta con servicios de monitoreo de infraestructura de TI que envían alertas por correo electrónico cuando los activos críticos asociados al departamento pasen el umbral de seguridad referente al uso de recursos (disco duro, CPU, memoria, entre otros). En caso de que se presente alguna anomalía, debo identificar que la está causando y solucionarlo manteniendo la disponibilidad de los servicios.
Resultados	Los equipos monitoreados cuentan siempre con recursos suficientes para su funcionamiento óptimo. Cuando se presenta una anomalía esta es atendida a la brevedad.

TABLA II. 4 - MANTENIMIENTO PERIÓDICO A LOS EQUIPOS

Actividad	**Mantenimiento periódico a los equipos cliente y servidores**
Objetivo	Extender la vida útil de los equipos de cómputo de la Coordinación. Es necesario que los equipos sean revisados para asegurar su disponibilidad e integridad, de tal forma que las operaciones no se vean afectadas.
Periodicidad	Mensual
Desarrollo	Mensualmente, estoy a cargo de realizar mantenimiento físico a los servidores y equipos clientes. Este mantenimiento incluye limpieza y reacomodo de cableado para evitar accidentes. De igual forma, el mantenimiento contempla la actualización de hardware, como discos duros y memoria RAM. Para realizarlo acuerdo una ventana de mantenimiento con los administradores del sistema en caso de que los servicios sean críticos y no puedan estar fuera de línea por mucho tiempo.
Resultados	Los equipos cliente de la Coordinación contaron con un aumento de memoria principal. Los servidores se encuentran en un estado óptimo y factores como el polvo acumulado no afectan su funcionamiento. El desarrollo de esta actividad garantiza el cumplimiento del control A.11.2.4 del Anexo A del estándar ISO 27001:2013.

TABLA II. 5 - INSTALACIÓN DE ACTUALIZACIONES

Actividad	**Instalación de actualizaciones**
Objetivo	Verificar que las actualizaciones liberadas para los servidores Windows no afecten la disponibilidad de los servicios.
Periodicidad	Mensual
Desarrollo	Una vez al mes, al liberarse las actualizaciones de seguridad de Microsoft, debo verificar en un ambiente de pruebas que estas no afecten el funcionamiento de los servicios ofrecidos. En caso de que no haya alguna afectación, instalo las actualizaciones en los servidores y programo una ventana de mantenimiento para reiniciar los equipos si es necesario. Cuando las actualizaciones afectan de forma considerable a los equipos notifico a mi jefe inmediato para que él evalúe la acción a tomar.
Resultados	Los servidores cuentan con las últimas actualizaciones de seguridad y mantienen los servicios disponibles. El desarrollo de esta actividad garantiza el cumplimiento del control A.11.2.4 del Anexo A del estándar ISO 27001:2013.

TABLA II. 6 - GESTIÓN DE SOFTWARE

Actividad	Gestión y distribución de software de licencia
Objetivo	Garantizar que el software utilizado por los miembros de la Coordinación de Seguridad de la Información haya sido adquirido legalmente y se cuente con licencia de uso.
Periodicidad	Mensual
Desarrollo	A través de una plataforma web de administración de inventarios y de un agente instalado en los equipos cliente y servidores, verifico el software que ha sido instalado en los mismos. Si ese software no se encuentra en un listado de software con licencias adquirido por la Coordinación, notifico a los usuarios del mismo el incidente y procedo con la desinstalación. En caso de que los usuarios comprueben que adquirieron legalmente el software, notifico a mi jefe inmediato para que autorice la instalación y uso del mismo.
Resultados	Los equipos cliente y servidores cuentan únicamente con software autorizado. El desarrollo de esta actividad garantiza el cumplimiento del control A.12.6.2 del Anexo A del estándar ISO 27001:2013.

TABLA II. 7 - CREACIÓN Y CONFIGURACIÓN DE AMBIENTES DE PRUEBAS

Actividad	Creación y configuración de ambientes de pruebas
Objetivo	Contar con ambientes separados de la infraestructura operacional para realizar pruebas a soluciones de seguridad y nuevas implementaciones.
Periodicidad	N/A
Desarrollo	Cuando la Coordinación de seguridad deba evaluar nuevas soluciones de seguridad (antimalware, firewall, UTM, entre otros), o el Departamento de Operación Interna busque implementar nuevos roles de servidores Windows, debo implementar ambientes de prueba separados de la infraestructura operacional, ya sea mediante la creación de máquinas virtuales o haciendo uso de equipos físicos dedicados. La creación y configuración de los ambientes incluye la instalación del sistema operativo, configuración de red e instalación de software adicional.
Resultados	Se han evaluado 5 soluciones de seguridad (antimalware, IPS, IDS, UTM) durante mi instancia en la Coordinación. Se ha implementado un nuevo rol de Windows (ADRMS) [2]. El desarrollo de esta actividad garantiza el cumplimiento del control A.12.1.4 del Anexo A del estándar ISO 27001:2013.

II.3.2 APOYO EN INCIDENTES DE SEGURIDAD INFORMÁTICA

La actividad principal de la Coordinación de Seguridad de la Información y por la cual cuenta con la certificación ISO 27001:2013 es atender incidentes de seguridad en cómputo que se presenten en las dependencias de la Universidad o alguna entidad externa. Como parte de mis funciones debo atender aquellos incidentes relacionados con los sistemas operativos Windows.

Cuando se presenta un incidente que debo atender, debo buscar el qué lo causa y una vez identificado, emitir recomendaciones de solución y de configuración para que no se presenten de nuevo o para mitigar el impacto en caso de reincidencia.

El desarrollo de esta actividad ayuda al cumplimiento de los objetivos de la CSI y garantiza el cumplimiento de los controles del dominio A.16 del Anexo A del estándar ISO 27001:2013.

II.3.3 PUBLICACIÓN DE NOTICIAS DE SEGURIDAD INFORMÁTICA

La Coordinación de Seguridad de la Información / UNAM-CERT publica noticias relacionadas con seguridad de la información de forma cotidiana en su portal *www.seguridad.unam.mx*.

Esta actividad consiste en apoyar en la traducción y publicación de noticias, verificando el contenido de las noticias y la redacción, adaptándolas para que puedan ser leídas y comprendidas por personas que no estén familiarizadas con temas de seguridad y computación.

El desarrollo de esta actividad ayuda al cumplimiento de los objetivos de la Coordinación promoviendo la cultura de seguridad de la información.

II.3.4 TRADUCCIÓN Y PUBLICACIÓN DE BOLETINES DE MICROSOFT

El segundo martes de cada mes, Microsoft libera un boletín de seguridad en donde describe las vulnerabilidades encontradas en sus productos (sistemas operativos, aplicaciones, complementos, entre otros), los sistemas afectados, el impacto de la vulnerabilidad y un parche o proceso para solucionarla.

Cada que se publica el boletín de Microsoft me dedico a traducirlo y publicarlo en el portal de la Coordinación. Durante la traducción que realizo cuido que no se pierda el sentido de la publicación, que quede especificado de forma clara qué sistemas son afectados por las vulnerabilidades y cuál es el proceso de solución.

CAPÍTULO III – PROYECTOS PRINCIPALES EN LA COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO III – PROYECTOS PRINCIPALES EN LA COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Durante mi instancia en la Coordinación de Seguridad de la Información/UNAM-CERT he participado en diversos proyectos dentro de la misma Coordinación y con entidades externas.

Dos de los proyectos principales y de los cuales aprendí más fueron la implementación de Active Directory Rights Management Services para la protección de recursos informáticos (documentos, presentaciones, material para cursos) de la CSI.

El segundo consistió en mi participación en el proyecto "Auditoría y Apoyo Técnico en Materia de Tecnologías de Información y Comunicación al Programa de Resultados Electorales Preliminares para las Elecciones Federales 2015", en el cual colaboré en la revisión de configuraciones de la infraestructura tecnológica.

III.1 ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES

III.1.1 ANTECEDENTES DEL PROYECTO

La Coordinación de Seguridad de la Información genera material didáctico que es almacenado y distribuido en formato digital.

Parte de las actividades organizadas por UNAM-CERT incluyen el Congreso de Seguridad en Cómputo que se realiza anualmente, los planes de capacitación a becarios y los cursos impartidos a los administradores de TI en el marco del AdminUNAM. Los asistentes a dichos cursos que imparte la CSI pueden tener cualquier procedencia (dentro o fuera de la UNAM, particulares, iniciativa privada).

Dadas estas circunstancias es importante contar con infraestructura que permita lidiar de manera efectiva y centralizada con los permisos que los usuarios finales tienen sobre el material, como copiar, imprimir, visualizar, editar, entre otros.

Active Directory Rights Management Services (AD RMS) es un rol que puede ser instalado en un servidor Windows y que permite administrar permisos a archivos de manera individual, a través de plantillas, y que facilita la restricción de usos (copiar, imprimir, visualizar, editar) que se les dan a estos.

El proyecto tuvo como finalidad implementar AD RMS para la distribución y restricción de permisos en el material desarrollado por la CSI, que permita centralizarlo, y al mismo tiempo, que siga permitiendo a los usuarios la lectura de su material, sin que sea difundido o distribuido a terceros no autorizados.

III.1.2 OBJETIVO DEL PROYECTO

Proteger el uso de material generado por la Coordinación de Seguridad de la Información, utilizando la herramienta Rights Management Services (RMS) como plataforma de Data Leak Protection (DLP).

III.1.3 INTRODUCCIÓN

Mediante Active Directory Rights Management Services (AD RMS) y el cliente de AD RMS, la Coordinación de Seguridad de la Información busca aumentar la estrategia de seguridad al proteger información mediante directivas de uso persistentes, que permanecen con esta, independientemente del lugar a donde se mueva. AD RMS ayuda a impedir que información confidencial, como informes, datos de clientes y mensajes de correo electrónico confidenciales, caigan en manos equivocadas, ya sea por accidente o de forma intencionada.

Muchas organizaciones se fundamentan en el valor de su propiedad intelectual. La pérdida de esta propiedad, el mal uso, la realización de copias no autorizadas o el robo, pueden causar daños incuantificables a sus operaciones. No es necesario tener una empresa muy grande para beneficiarse de alguna forma de la gestión de derechos.

III.1.4 DESARROLLO DEL PROYECTO

Para desarrollar este proyecto lo primero que tuve que hacer fue familiarizarme con el funcionamiento de los servicios a implementar.

Mi investigación consistió en buscar qué son y cómo funcionan los servicios de Active Directory Domain Services (ADDS) [1], Active Directory Certificate Services (ADCS) [2], SQL Server y AD RMS en conjunto.

Active Directory Domain Services (ADDS)
El requisito principal para la implementación de AD RMS es la existencia de un dominio para su implementación. ADDS es un rol de los servidores Windows que me permitió crear una infraestructura escalable y segura para la administración de usuarios y recursos.

Gracias a la instalación de este rol pude crear Unidades Organizacionales, lo que me permitió administrar de forma más eficiente a los usuarios y equipos con los que estuve trabajando.

Otro de los servicios de los que hice uso fue el servicio de Domain Name System (DNS). El servicio de DNS lo utilicé para poder identificar a los equipos en mi dominio más fácilmente, adicionalmente lo utilice para crear una URL que fue utilizada posteriormente por RMS.

Active Directory Certificate Services (ADCS)
ADCS es un rol de servidor que me permitió crear una Infraestructura de Clave Pública (PKI) con la finalidad de generar los certificados que AD RMS puede integrar en documentos.

A pesar de no ser obligatorio su uso para la implementación de RMS, decidí usarlo ya que provee una infraestructura de criptografía de clave pública, certificados digitales y la capacidad de firma digital que puede ser aprovechada por la Coordinación de Seguridad de la Información y brinda un nivel mayor de seguridad a los documentos protegidos y a los sitios web utilizados (HTTPS).

SQL Server
Uno de los componentes más activos en una infraestructura RMS es la base de datos. RMS puede funcionar con una base de datos interna (WID), pero dada la característica del proyecto decidí hacer uso de la versión 2014 de SQL Server.

SQL Server me permitió tener un mejor control de las bases de datos utilizadas por RMS, ya que su mantenimiento, depuración y respaldo es mucho más fácil que con una base de datos interna (WID); Además, la documentación oficial recomienda hacer uso de la base de datos interna únicamente en ambientes de pruebas.

RMS hace uso de tres bases de datos:

- **BD de Configuración:** almacena, comparte y recupera toda la información de configuración y otros datos que el servicio necesita para administrar la certificación de cuentas, el licenciamiento y los servicios de publicación de todo el clúster.

- **BD de Servicios de Directorio:** contiene información acerca de usuarios, identificadores (como correos electrónicos), ID de seguridad (SID), membresías a grupos y otros identificadores. Esta información es un cache de la información del servicio de directorio utilizado por ADRMS y obtenido mediante solicitudes LDAP al catálogo global de ADDS. Es utilizada para mejorar el rendimiento y reducir la carga de trabajo del controlador de Dominio.

- **BD de Bitácoras:** almacena los eventos presentados en la infraestructura de AD RMS.

III.1.5 FUNCIONAMIENTO DE RMS

Una vez que terminé la investigación de los servicios necesarios para la implementación de AD RMS lo siguiente fue investigar cómo funciona RMS, con la finalidad de comprender el proceso de protección de datos, emisión de licencias y certificados, consumo de contenido y uso de Windows ID.

Estos procesos están descritos en la documentación oficial de Microsoft, por lo que aquí los describo de forma resumida con fines ilustrativos, ya que no es necesario conocer estos

procesos para implementar el servicio. Como muchos servicios Web, AD RMS funciona basado en una arquitectura Cliente/Servidor.

Cliente RMS

El cliente de AD RMS es un programa que permite a los usuarios crear, publicar y consumir contenido protegido (cifrado). Específicamente, una aplicación con soporte para AD RMS puede hacer uso del cliente para llevar a cabo las siguientes tareas:

- Enviar peticiones al servicio de activación de RMS para obtener un certificado de máquina que permita identificar a los equipos cliente.
- Enviar peticiones al servicio de activación de RMS para obtener un certificado de privilegios de usuario (RAC) para identificar a un usuario y asociarlo a un equipo específico.
- Crear una licencia de publicación que indica que usuarios puede descifrar el contenido protegido y que permisos tendrán sobre el mismo.
- Cifrar contenido y hacerlo disponible para usuarios autenticados.
- Adquirir licencias de usuario final para un usuario específico, con el fin de descifrar el contenido y forzar la aplicación de los permisos asociados a éste en la licencia de publicación.

El cliente está instalado por defecto en equipos Windows con SO Server 2008, Vista, Server 2008 R2, Server 2012 [3] [4] y Windows 8. En caso de que no esté disponible es posible descargarlo desde el sitio oficial de Microsoft.

La recomendación que hago aquí es que se descargue la versión más reciente del cliente, ya que la que se incluye en los sistemas operativos puede no ser la más actual.

Servidor RMS

El servidor RMS está basado en un conjunto de servicios web ejecutados sobre Internet Information Services (IIS). Los siguientes servicios son las más importantes para el funcionamiento e implementación de AD RMS:

- **Administration:** Aloja el sitio web de administración para manejar AD RMS a través de MMC.
- **Account Certification:** Crea certificados de equipo y de derechos de cuenta permitiendo identificar usuarios y equipos.
- **Licensing:** Expide licencias de usuario final.
- **Publishing:** Crea licencias de publicación definidas en las políticas, que se enumeran en una licencia de usuario final.
- **Precertification:** Permite a un servidor solicitar un certificado RAC en nombre del usuario.
- **Service Locator:** Provee la URL de las cuentas de certificación y servicios de publicación, así como el licenciamiento, permitiendo a los clientes descubrir los servidores AD RMS.

Funcionamiento

Una vez que explique las funciones tanto del cliente como del servidor, diseñé un diagrama (*Imagen III.1*) para ejemplificar de forma más clara cómo es que estos dos interactúan durante el proceso de creación y consumo de contenido

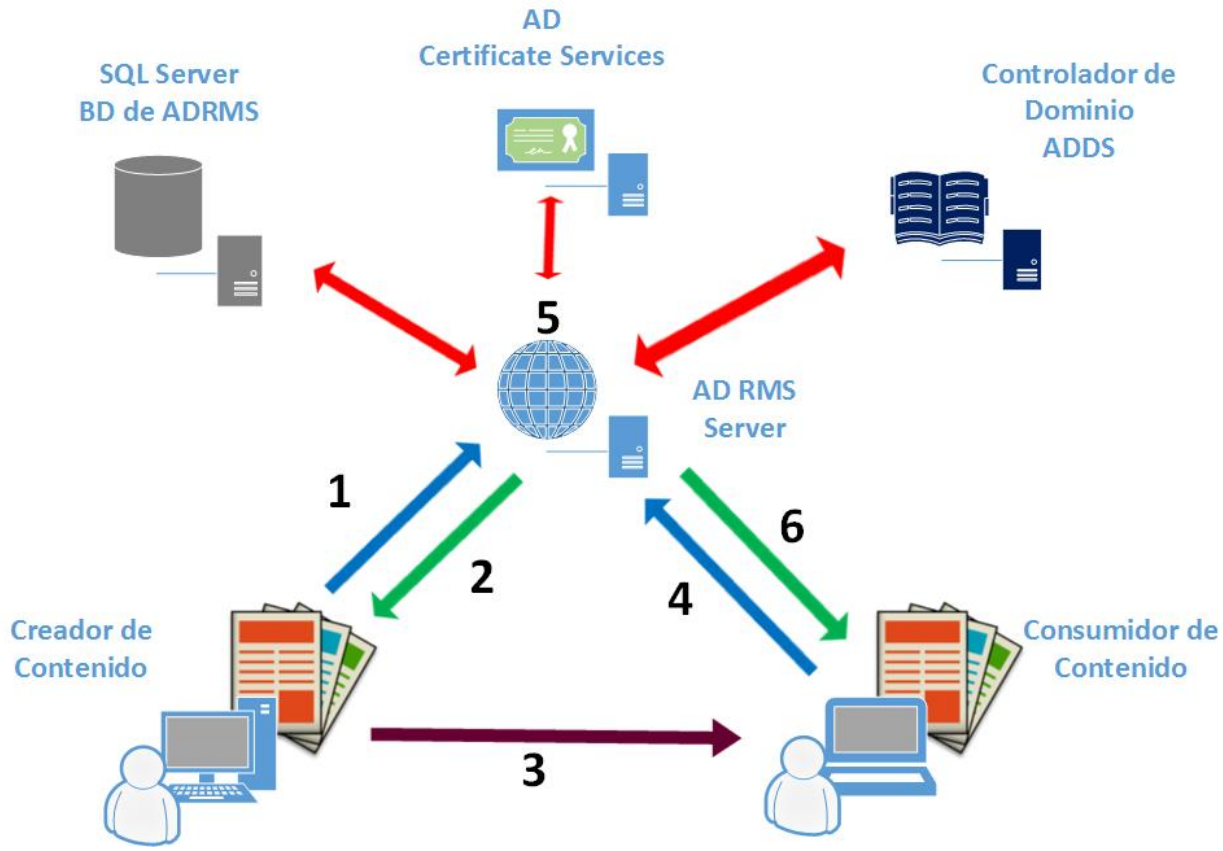


IMAGEN III. 1 - FUNCIONAMIENTO AD RMS

1. Se aplican las restricciones al documento, el cliente ADRMS lanza e inicializa una petición de servicio al servidor AD RMS

2. El servidor AD RMS regresa un CLC (Client Licensor Certificate) al cliente instalado en el equipo que hizo la solicitud. El cliente entonces permite al creador guardar el documento y cifrarlo con el nivel deseado de protección.

3. Se envían los documentos a las personas correspondientes.

4. Al abrir el documento, el cliente RMS en el equipo receptor contacta al servidor AD RMS para adquirir una licencia de usuario final.

5. El servidor únicamente va a expedir CLC a los usuarios del Dominio. Solo los usuarios del dominio pueden proteger documentos. La base de datos almacena la configuración de RMS y un cache de usuarios para los que el servidor ha expedido algún tipo de licencia, permitiendo así hacer consultas más rápidas y disminuir la carga de trabajo para el controlador de dominio.

6. El cliente en el equipo receptor recibe la licencia de usuario final, lo que indica que el receptor tiene permitido ver el documento. El cliente descifra el documento y aplica las restricciones de acuerdo a las indicaciones del creador de contenido.

Tipos de Certificados

El rol AD RMS funciona a base de certificados. Estos certificados juegan diferentes roles, los cuales muestro en la *Tabla III.1*.

TABLA III. 1 - TIPOS DE CERTIFICADOS

Certificado o Licencia	Propósito
Server Licensor Certificate (SLC)	Creado cuando el rol de ADRMS es instalado y configurado por primera vez. Permite identificar al servidor.
Client Licensor Certificate (CLC)	Creado por el clúster RMS en respuesta a una petición del cliente. Otorga al usuario privilegios para proteger contenido.
Machine Certificate	Creado en el equipo cliente cuando se hace uso por primera vez de una aplicación con soporte para RMS. Identifica un equipo o dispositivo que está correlacionado con el usuario que ha iniciado sesión.
Rights Account Certificate (RAC)	Establece la identidad de un usuario en el sistema AD RMS. Es creado la primera vez que el usuario intenta consumir contenido protegido. Puede tener una validez de un año o un para un certificado temporal de 15 minutos.
Publishing License	Creado por el cliente cuando el contenido protegido es guardado. Especifica qué usuarios pueden abrir el contenido protegido y los privilegios que cada uno tiene sobre el mismo.
Use License	Especifica los privilegios que aplican al contenido protegido en el contexto del usuario actual. Está ligado al RAC, por lo que si éste no está presente no se puede abrir el contenido protegido.

III.1.6 PROPUESTA DE INFRAESTRUCTURA

Una vez que adquirí el conocimiento necesario respecto a los servicios necesarios y su funcionamiento para la implementación de RMS el siguiente paso fue diseñar una propuesta de infraestructura indicando los requisitos mínimos de los equipos que harían la función de servidores para la infraestructura de RMS.

Hice llegar esta propuesta de infraestructura a mi jefe de proyecto, quien a su vez la escaló al Coordinador de Seguridad de la Información con el fin de obtener la aprobación de uso de recursos, determinando que todo se implementaría en un ambiente virtualizado en uno de los servidores de la Coordinación.

A continuación presento el diagrama de la infraestructura propuesta *(Imagen III.2)*, junto con una tabla de requisitos mínimos y deseables para su funcionamiento y una justificación de uso *(Tabla III.2).*

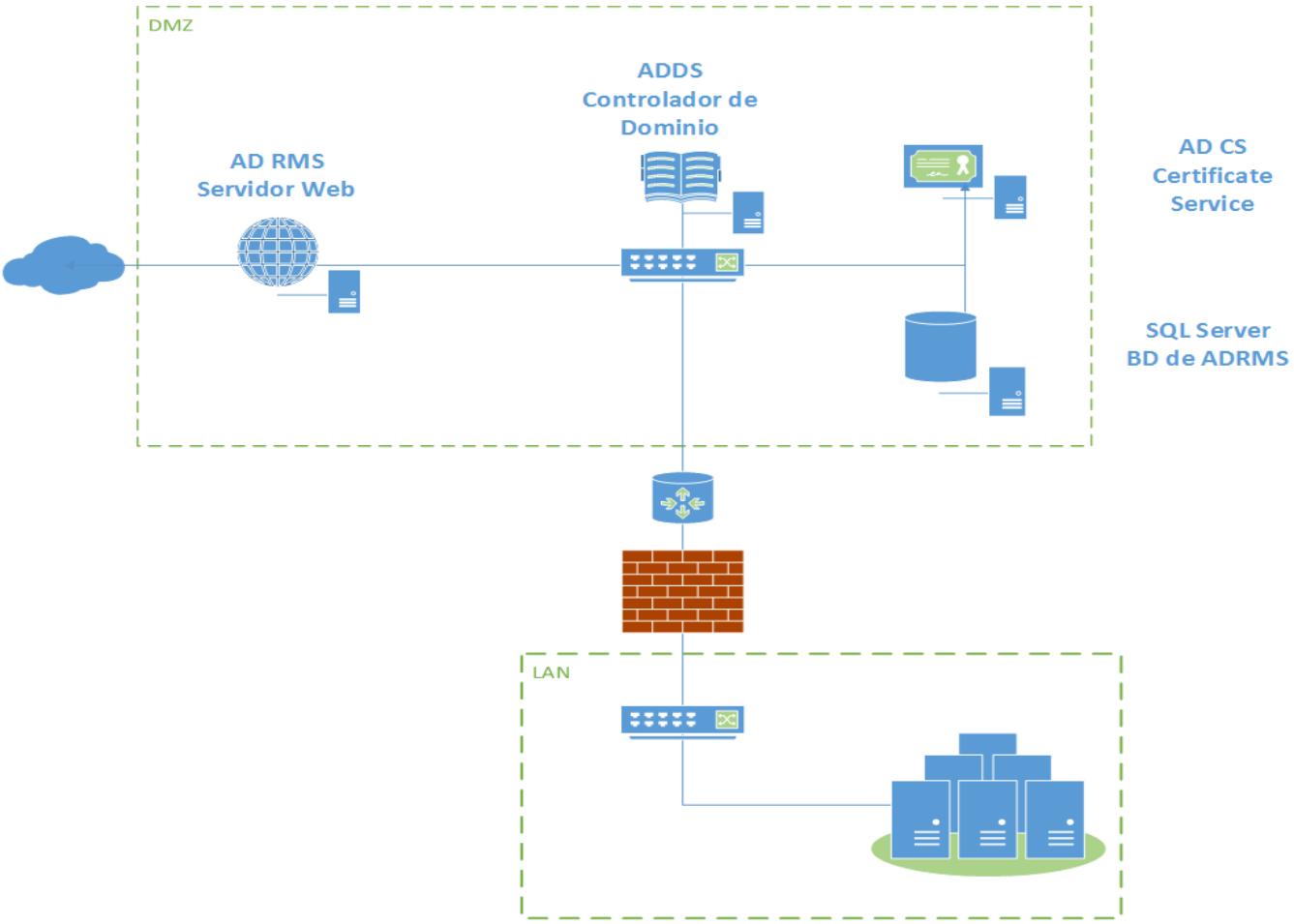


IMAGEN III. 2 - PROPUESTA DE INFRAESTRUCTURA

TABLA III. 2 - REQUISITOS DE INFRAESTRUCTURA

Servidor	Requisito	Mínimo	Deseado
Controlador de Dominio ADDS	Memoria RAM	512 MB	2048 MB
	Disco Duro	32 GB	50 GB
	Procesador	64 bits a 1,4 GHz	64 bits a 2 GHz o superior
	Software	Windows Server 2012	Windows Server 2012 R2
Autoridad Certificadora ADCS	Memoria RAM	512 MB	2048 MB
	Disco Duro	40 GB	50 GB
	Procesador	64 bits a 1,4 GHz	64 bits a 2 GHz o superior
	Software	Windows Server 2012	Windows Server 2012 R2
Base de Datos SQL Server 2014	Memoria RAM	1024 MB	4096 MB
	Disco Duro	40 GB	50 GB
	Procesador	64 bits a 1,4 GHz	64 bits a 2 GHz o superior
	Software	Windows Server 2012	Windows Server 2012 R2
		.NET Framework 3.5	.NET Framework 4.0
		Powershell 2.0 [3]	Powershell 2.0
Active Directory Rights Management Services AD RMS	Memoria RAM	512 MB	2048 MB
	Disco Duro	80 GB	100 GB
	Procesador	64 bits a 3 GHz	Dos procesadores de 64 bits a 3 GHz
	Software	Windows Server 2012	Windows Server 2012 R2
		.NET Framework 3.5	.NET Framework 3.5
	Red	Dos interfaces de red	Dos interfaces de red

Otros requisitos fueron:

- Una dirección IPv4 pública
- Un nombre de dominio (Registro A) asociado a esa dirección IP pública.

Un vez que obtuve respuesta por parte del Coordinador de Seguridad de la Información, adecué mi propuesta a los recursos que me asignaron, donde debo destacar dos cosas importantes:

1. La autoridad certificadora (ADCS) propuesta no fue implementada, en su lugar se decidió utilizar la CA con la que cuenta la Coordinación actualmente.
2. Todos los servidores necesarios para la implementación del rol AD RMS se virtualizaron en un equipo dedicado con Hyper-V.

III.1.7 INFRAESTRUCTURA A IMPLEMENTAR

La siguiente tabla muestra las características de los servidores aprobados, junto con el diagrama final de la infraestructura a implementar *(Imagen III.3)*.

TABLA III. 3 - CARACTERÍSTICAS FINALES DE INFRAESTRUCTURA

Servidor	Requisito	Asignado
Controlador de Dominio ADDS	Memoria RAM	1024 MB
	Disco Duro	50 GB
	Procesador	64 bits a 2 GHz
	Software	Windows Server 2012 R2
Base de Datos SQL Server 2014	Memoria RAM	2048 MB
	Disco Duro	50 GB
	Procesador	64 bits a 2 GHz
	Software	Windows Server 2012 R2
		.NET Framework 3.5
		Powershell 2.0
Active Directory Rights Management Services AD RMS	Memoria RAM	2048 MB
	Disco Duro	100 GB
	Procesador	64 bits a 3 GHz
	Software	Windows Server 2012 R2
		.NET Framework 3.5
	Red	Dos interfaces de red

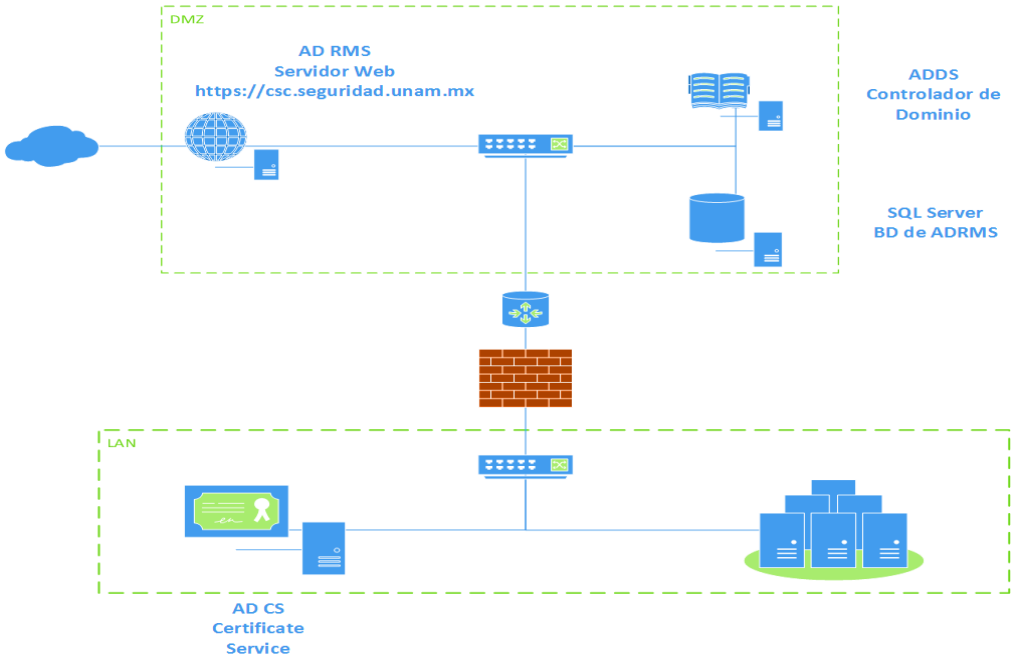


IMAGEN III. 3 - INFRAESTRUCTURA A IMPLEMENTAR

El trabajar con equipos virtualizados me permitió crear una red virtual mediante el administrador de Switch de Hyper-V. Esta red virtual está aislada del resto de los equipos de la red. Para la implementación hice uso del segmento de red 172.16.16.0/29, el cual me permite hacer uso de 6 direcciones IP en caso de ser requeridas.

Para esta implementación solo fueron necesarias 3 direcciones IP privadas del segmento 172.16.16.0/29 y una dirección IP pública.

TABLA III. 4 - RELACIÓN DE SERVICIOS Y DIRECCIONES IP

Servicio	Dirección IP Privada	Dirección IP pública
ADDS	172.16.16.1	N/A
SQL Server	172.16.16.2	N/A
AD RMS	172.16.16.3	132.248.X.Y

III.1.8 MONTAJE DE INFRAESTRUCTURA DE PRUEBAS

Una vez diseñada la infraestructura a implementar, el siguiente paso fue crear un ambiente de pruebas en un servidor dedicado con el fin de generar documentación de implementación, solucionar los errores durante la implementación, crear un protocolo de pruebas de funcionamiento y modificar las especificaciones dependiendo de los resultados de las pruebas.

El ambiente de pruebas se montó en 4 etapas:

1. Creación de switch virtual
2. Creación de máquinas virtuales
3. Configuración de red y nombres de equipos
4. Instalación y configuración de roles

Creación de switch virtual

La creación de un switch virtual fue importante para este proyecto para contar con medio que permita la comunicación entre las máquinas virtuales y a su vez las aísle de la red, impidiendo que otros equipos que no estén conectados a ese switch virtual puedan comunicarse con ellos. La siguiente serie de imágenes muestran el proceso de creación de un switch virtual.

El primer paso es abrir el Administrador de Switch Virtual (Imagen III.4):

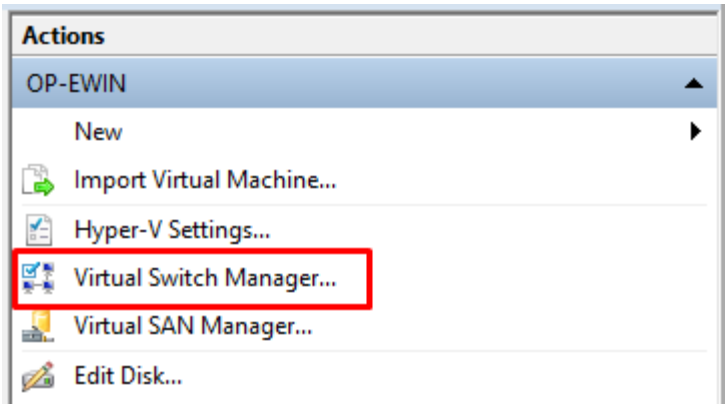


IMAGEN III. 4 - VIRTUAL SWITCH MANAGER

Selecciono el tipo de switch requerido como se observa en la Imagen III.5:

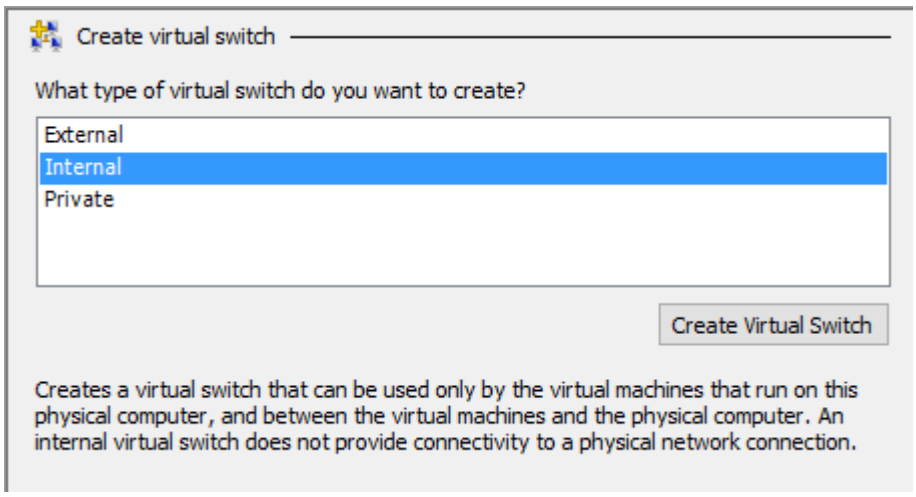


IMAGEN III. 5 - SWITCH VIRTUAL INTERNO

Es importante asignar un nombre que permita la identificación del switch a usar en todos los equipos de la infraestructura como se muestra en la imagen III.6:

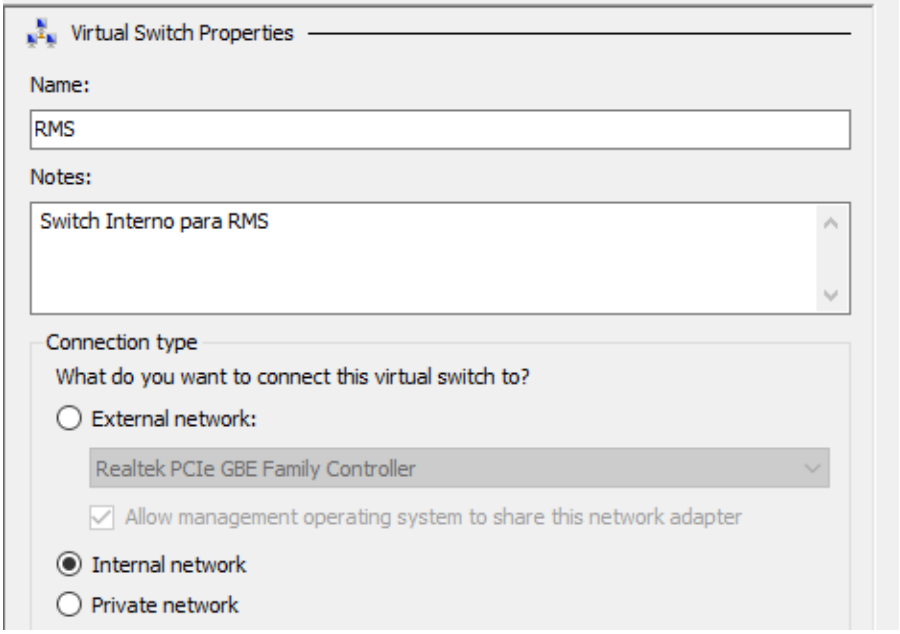


IMAGEN III. 6 - NOMBRE Y DESCRIPCIÓN DEL SWITCH INTERNO

Creación de Máquinas Virtuales

Se crearon las 4 máquinas virtuales en la plataforma Hyper-V mostradas en la Tabla III.5:

TABLA III. 5 - RELACIÓN SERVIDORES, SERVICIOS Y DIRECCIONES IP

Nombre de la máquina	Servicio que proporciona	Dirección IP
CSC	Active Directory Rights Management Service	172.16.16.3 132.248.X.Y
rmsdom	Active Directory Domain Services	172.16.16.1
rmsbd	Base de Datos SQL Server SQL 2014	172.16.16.2
clienterms	Office 2013 para protección de contenidos	172.16.16.4

En Hyper-V, en en panel de acciones, seleccionar New -> Virtual Machine (Imagen III.7)

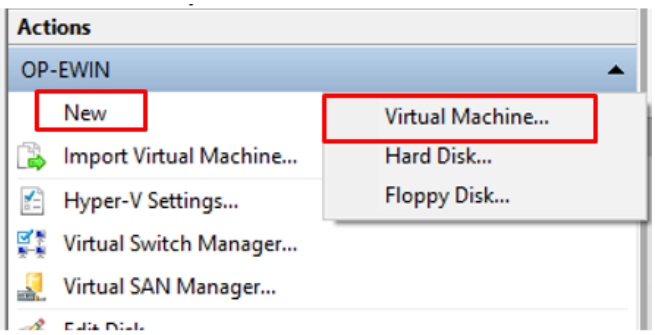


IMAGEN III. 7 - CREACIÓN DE MÁQUINAS VIRTUALES

El nombre de la máquina me permitió identificarla más fácilmente en la infraestructura (Imagen III.8).

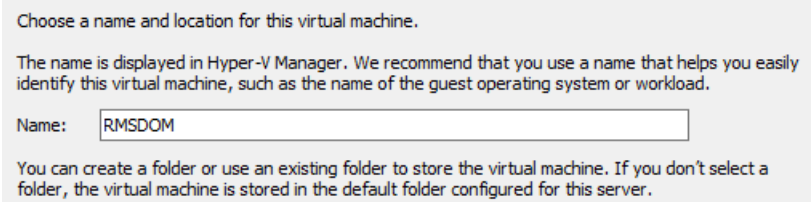


IMAGEN III. 8 - NOMBRE DE LA MÁQUINA VIRTUAL

La generación configura al equipo para trabajar bajo un soporte de virtualización de características como UEFI (Imagen III.9)

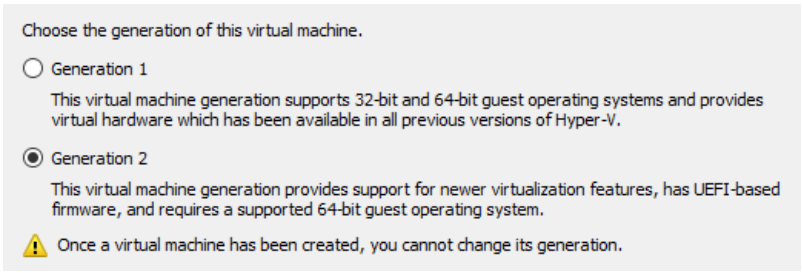


IMAGEN III. 9 - GENERACIÓN DE LA MÁQUINA VIRTUAL

Los recursos como memoria RAM y procesador son configurables desde las opciones de la máquina virtual (Imagen III.10).

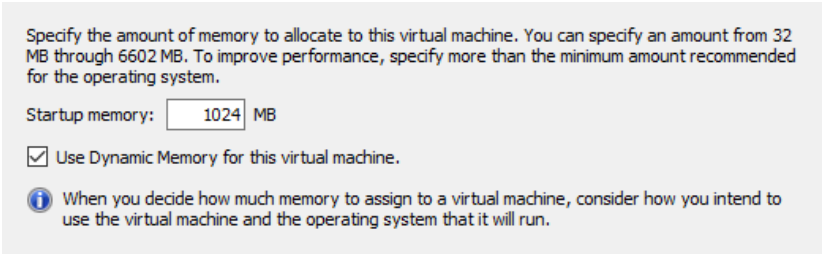


IMAGEN III. 10 - ASIGNACIÓN DE RAM

Para brindar conectividad de red, es necesario seleccionar el switch virtual creado anteriormente (Imagen III.11).

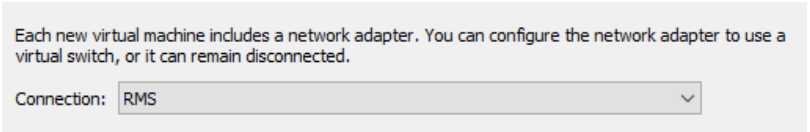


IMAGEN III. 11 - CONEXIÓN A SWITCH VIRTUAL

La asignación de disco duro (Imagen III.12) se pudo hacer dinámica gracias a los discos VHDX. Estos discos permitieron establecer un tamaño "máximo" pero del cual solo se ocupara lo necesario para la máquina virtual, este tamaño puede aumentar o disminuir dependiendo las necesidades del equipo.

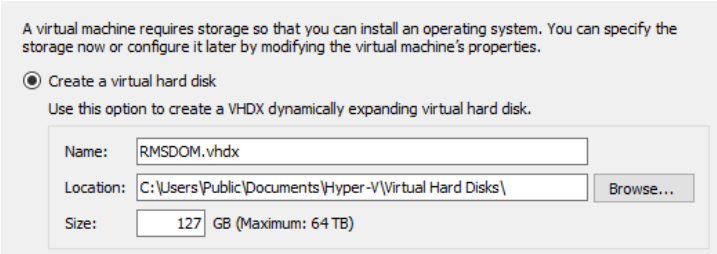


IMAGEN III. 12 - ASIGNACIÓN DE ESPACIO DE DISCO DURO

Configuración de red y nombres de equipos

Lo siguiente realizado fue cambiar el nombre de los equipos y colocar su dirección IP asignada (Imagen III.13), considerando como DNS al servidor que servirá como Controlador de Dominio (ADDS).

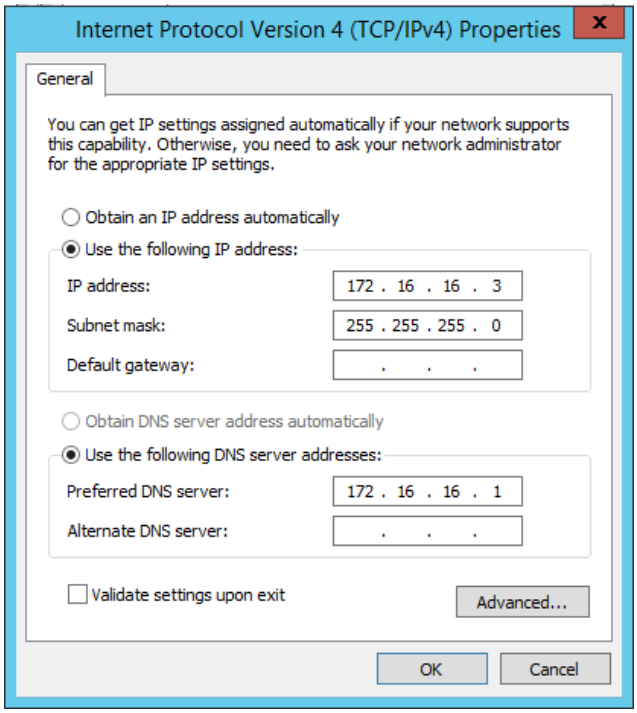


IMAGEN III. 13 - CONFIGURACIÓN DE RED

Instalación y configuración de roles

Dominio

El primer paso en la instalación de roles fue la instalación del dominio seguridad.unam.mx en el equipo rmsdom. El rol necesario para esto es Active Directory Domain Services [2], el cual instala y configura a su vez al servidor DNS a ocupar.

Una vez instalado, el resto de los equipos se unieron al dominio para poder trabajar bajo el mismo directorio.

Dentro de "Active Directory Users and Computers", desplegué las opciones del dominio y creé una Unidad Organizacional, dentro de esa OU creé los usuarios listados en la tabla III.6:

TABLA III. 6 - CUENTAS DE USUARIO

Nombre de Usuario	Cuenta de Usuario	Dirección E-mail	Grupo
ADRMSSRV Cuenta de Servicio RMS	ADRMSSRV		
ADRMSADMIN	ADRMSADMIN	adrmsadmin@seguridad.unam.mx	Enterprise Admins
Coordinación de Seguridad de la Información	ADRMSCSI	adrmscsi@seguridad.unam.mx	

El primero usuario es una cuenta de servicio necesaria para la conexión entre el clúster de RMS y otros equipos, no debe contar con ningún privilegio extra.

La segunda cuenta es con la que se hizo la instalación y administración del rol AD RMS. Esta cuente debe pertenecer al grupo Enterprise Admins con la finalidad de que tenga privilegios suficientes para instalar los roles y características necesarias.

La cuenta de la Coordinación fue creada con la finalidad de proteger contenido, por lo que no requiere privilegios especiales.

Dentro del mismo equipo, se creó un registro A en el DNS asociado a la IP del equipo con el nombre de csc.seguridad.unam.mx. Este registro A permitió configurar más adelante el sitio web en el servidor IIS.

SQL Server 2014 (Base de Datos)

Con los equipos en el dominio se hizo la instalación del servidor de base de Datos SQL Server. Este servidor requirió configuraciones adicionales para trabajar en conjunto con RMS. Estas configuraciones fueron las descritas a continuación.

El primer paso es asignar permisos de administrador del sistema a la cuenta ADRMSADMIN en la instancia de SQL Server para poder crear las bases de datos necesarias durante la instalación de AD RMS.

En el servidor SQL inicié sesión con una cuenta de administrador que esté en el dominio. En el menú inicio, abrir SQL Server presionando el icono del servicio mostrado en la Imagen III.14 (o bien, presionar la combinación de teclas Win+R y escribir “ssms.exe”):

IMAGEN III. 14 - ICONO DE SQL SERVER

Con el servicio de SQL en ejecución el siguiente paso fue conectarme al servidor con la finalidad de agregar al usuario (Imagen III.15).

IMAGEN III. 15 - CONEXIÓN AL SERVIDOR SQL

Una vez conectado, en el explorador de objetos, navegue hasta la opción deseada a través de las siguientes opciones (Imagen III.16):

"Servidor_SQL" > "Security", clic derecho en "Logins" y "New Login…".

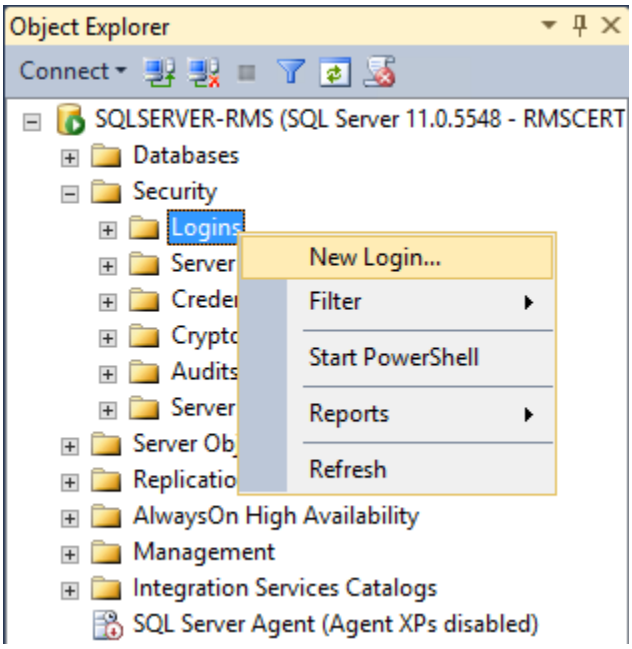


IMAGEN III. 16 - NEW LOGIN EN SQL SERVER

En la ventana que se abrió di clic en el botón Search, ahí escribí el nombre del usuario administrador de RMS creado en el dominio (Imagen III.17).

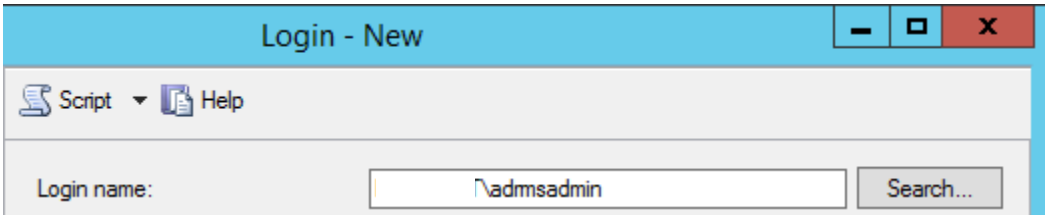


IMAGEN III. 17 - NUEVO LOGIN ASOCIADO A CUENTA DE DOMINIO

En esa misma ventana, en el panel del lado izquierdo, seleccioné “Server Roles” y marque la casilla “sysadmin” (Imagen III.18). Al finalizar se debe cerrar SQL Server.

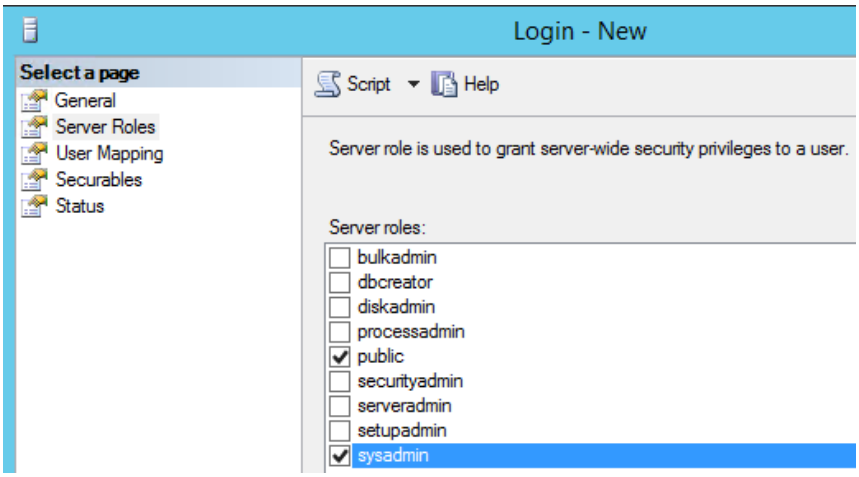


IMAGEN III. 18 - ASIGNACIÓN DE ROLES EN EL SERVIDOR SQL

Para el funcionamiento de RMS es necesario habilitar el servicio “SQL Server Browser”, esto se hace desde la consola de administración de servicios de Windows (Imagen III.19)

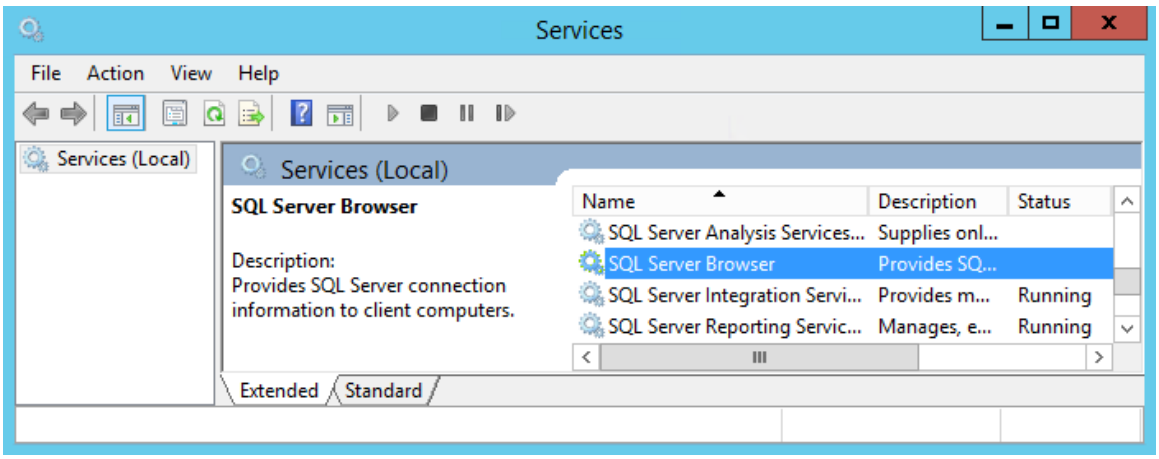


IMAGEN III. 19 - SERVICIO SQL SERVER BROWSER

Una vez ubicado “SQL Server Browser”, modifiqué sus propiedades con la finalidad de que iniciara de forma automática al encender el equipo (Imagen III.20).

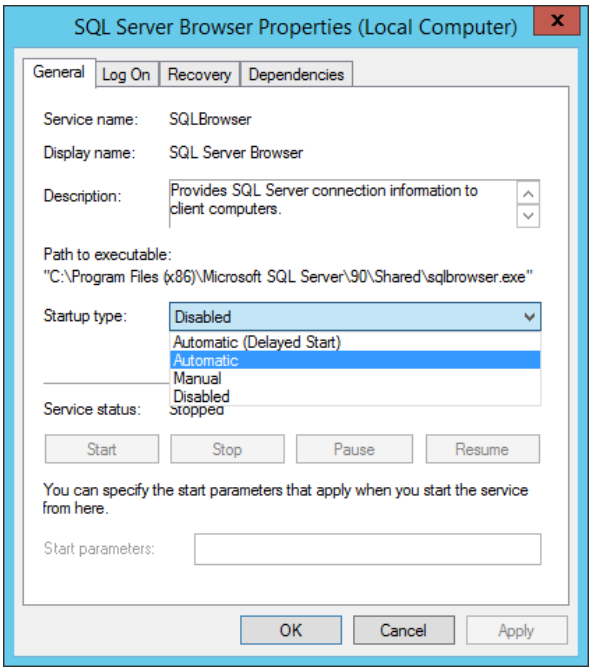


IMAGEN III. 20 - CONFIGURACIÓN DE ARRANQUE DEL SERVICIO SQL

Por último di clic en el botón “Start” y después en “OK”.

Dado que se van a realizar conexiones al servidor de base de datos para hacer consultas, se deben crear reglas de firewall para permitir dicho tráfico. En el panel de administración del firewall de Windows, en el panel del lado izquierdo, seleccioné “Inbound Rules” y en el panel derecho abrí la opción de “New Rule” para crear una regla de entrada (Imagen III.21).

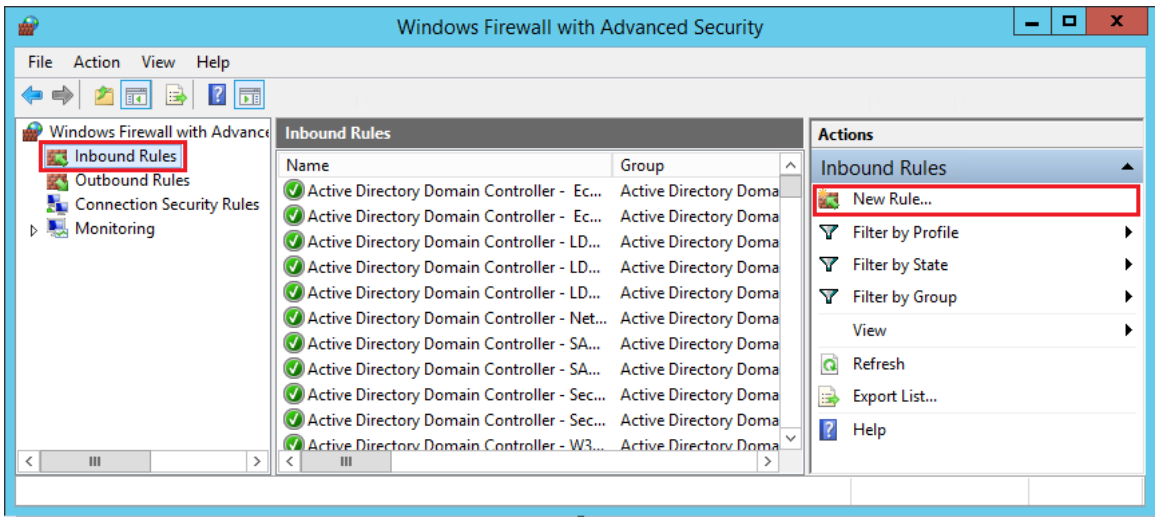


IMAGEN III. 21 - NUEVA REGLA DE ENTRADA EN EL FIREWALL DE WINDOWS

Es necesario permitir las conexiones entrantes desde los puertos 1433,1434, 445 y 11435 tanto en TCP como en UDP, para esto se debe seleccionar lo siguiente como se muestra en la Imagen III.22:

- Rule Type: Port
- Protocols and Ports: TCP
- Specific local ports: 1433
- Action: Allow the connection
- Profile: Domain, Private y Public
- Name: SQL_1433

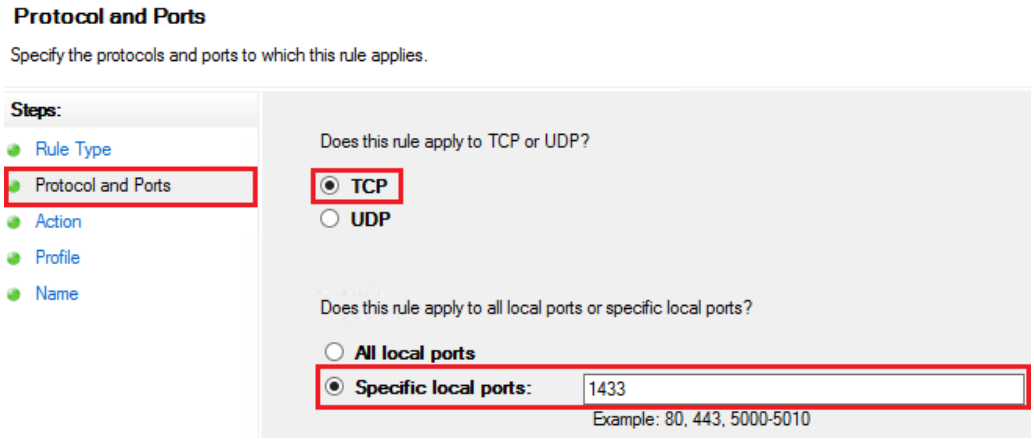


IMAGEN III. 22 - PROTOCOLO Y PUERTO DE LA REGLA DE FIREWALL

Se crearon tres reglas más de entrada (inbound) modificando únicamente las siguientes características:

Regla: Protocols and Ports: UDP
Specific local ports: 1434
Name: SQL_1434

Regla: Protocols and Ports: TCP
Specific local ports: 445
Name: SQL Server Named Pipes

Regla: Protocols and Ports: TCP
Specific local ports: 11435
Name: SQL Server Cloud Adapter (TCP-in)

AD RMS

Con los usuarios listos en el controlador de dominio y con el servidor de base de datos instalado y configurado adecuadamente el siguiente paso fue instalar el rol de AD RMS.

Para esto lo primero que hice fue instalar la versión 3.5 de .NET Framework de Windows, ya que es un requisito indispensable para la instalación de RMS y sin el cual ésta no puede ser llevada a cabo (Imagen III.23).

Para esta instalación de .NET Framework 3.5 es necesario contar con el disco de instalación de Windows Server 2012 R2, ya que en el disco se encuentran los archivos necesarios para agregar la característica (Imagen III.24).

Desde la consola de Server Manager se hizo la instalación, seleccionando la característica deseada e indicando la ruta de los archivos adicionales cuando se solicitó.

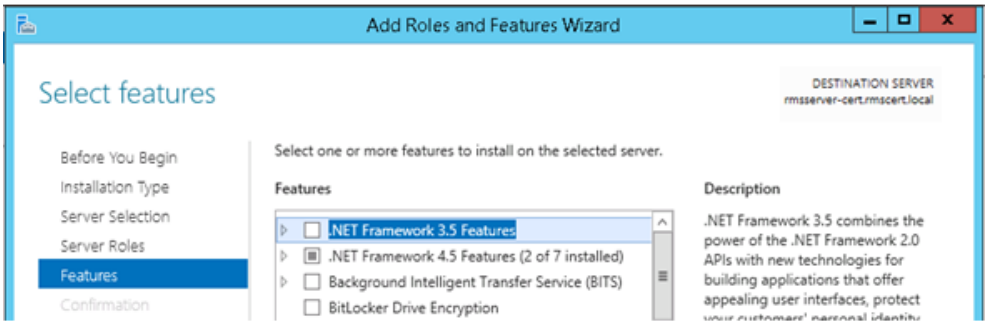


IMAGEN III. 23 - CARACTERÍSTICA .NET FRAMEWORK

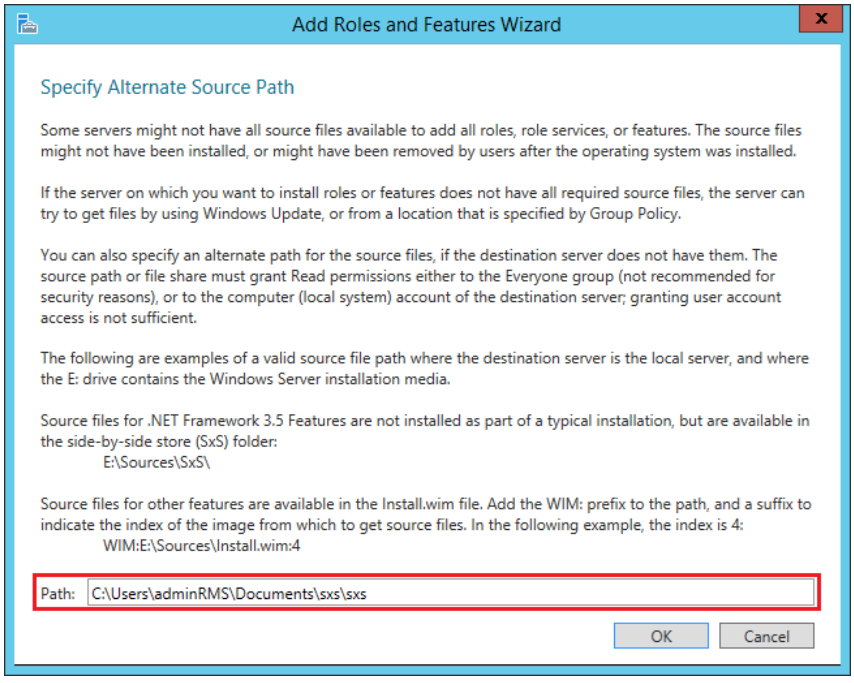


IMAGEN III. 24 - RUTA ALTERNATIVA

Con .NET Framework instalado, el siguiente paso fue instalar el rol de servidor web Internet Information Services o IIS.

Este rol también se instaló desde el Server Manager del servidor CSC. La instalación realizada fue una instalación por defecto, sin agregar ninguna característica adicional (Imagen III.25).

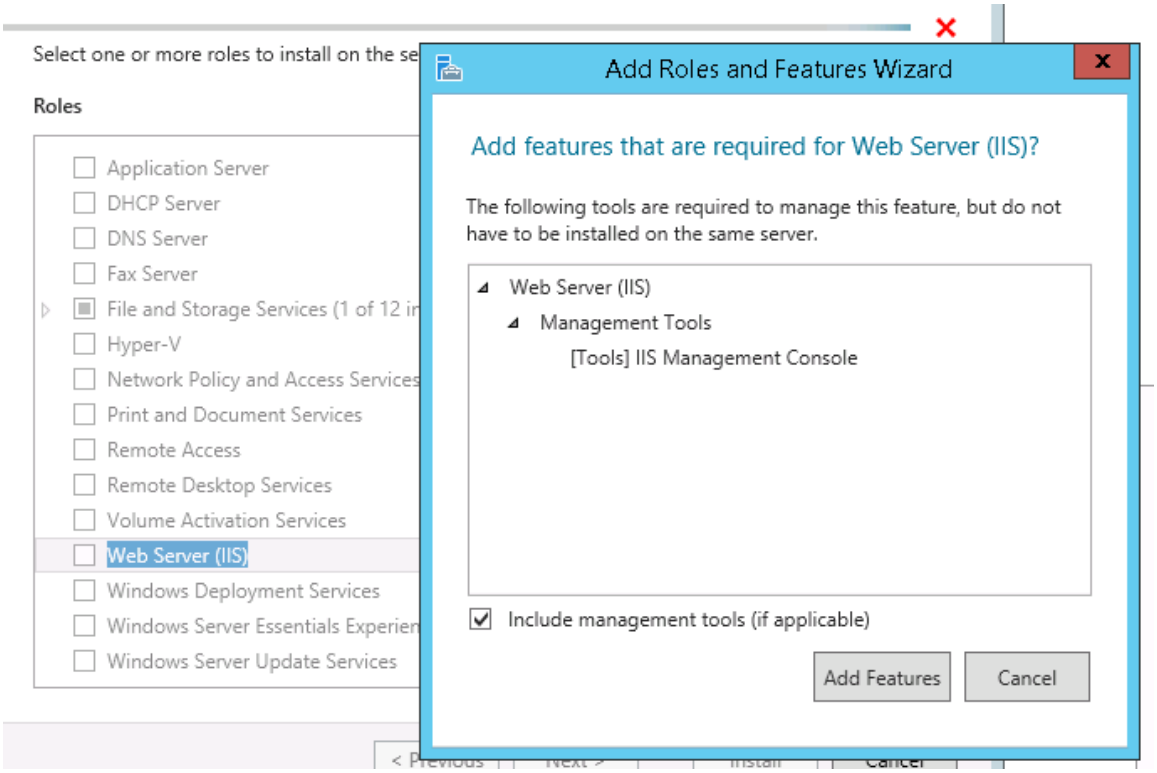


IMAGEN III. 25 - ROL DE SERVIDOR WEB IIS

Una vez instalado IIS, lo que hice fue abrir la consola de administración del servidor Web y crear una solicitud de certificado digital con la finalidad de poder hacer uso del protocolo HTTPS en el sitio web de licenciamiento y certificación de RMS (Imagen III.26).

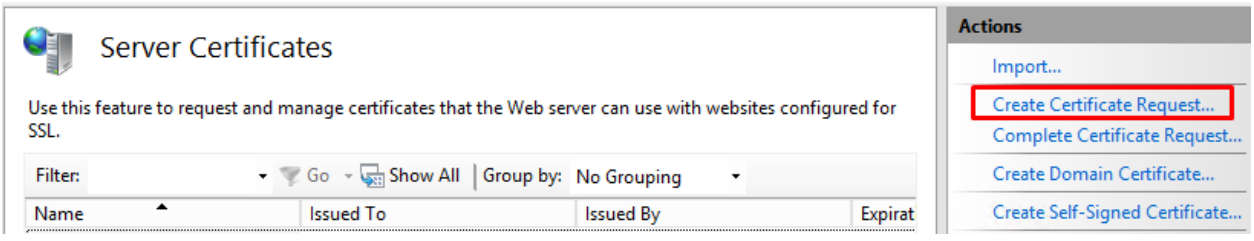


IMAGEN III. 26 - CREACIÓN DE SOLICITUD DE CERTIFICADO DIGITAL

La solicitud se llenó con los datos mostrados en la Imagen III.27, cabe destacar que el campo "Common Name" debe coincidir con la URL del sitio, ya que de no ser así los navegadores web podrían detectar que se trata de un sitio malicioso o que no es de confianza y esto afectaría el funcionamiento de RMS.

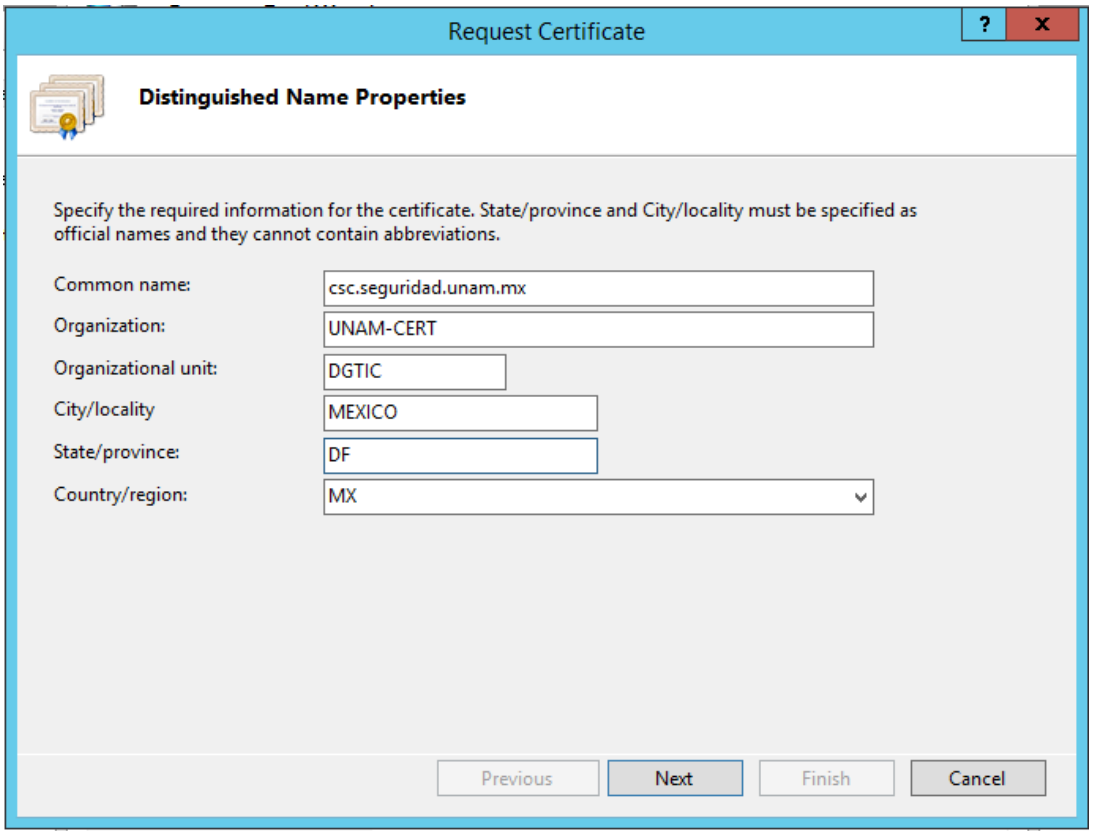


IMAGEN III. 27 - PROPIEDADES DEL CERTIFICADO

Teniendo la solicitud del certificado digital, contacté al administrador de la Autoridad Certificadora de la Coordinación de Seguridad de la Información con la finalidad de obtener la firma y de la solicitud y así contar con un certificado digital para servidor web válido y de confianza (Imagen III.28).

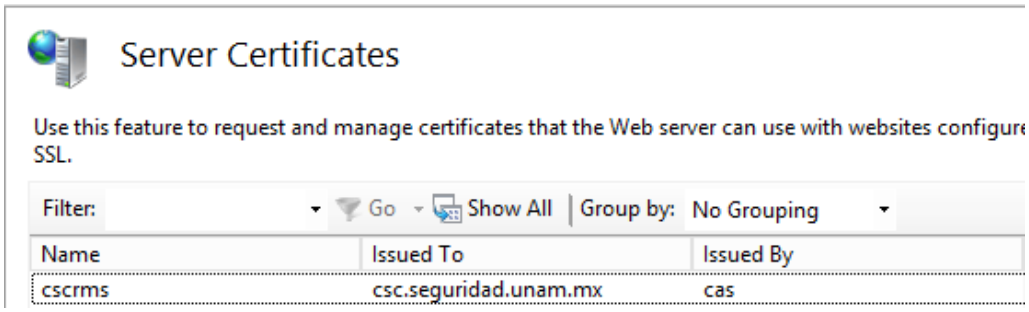


IMAGEN III. 28 - CERTIFICADOS DISPONIBLES PARA IIS

Con IIS listo para su uso, el siguiente paso fue instalar el rol de AD RMS desde el Server Manager de Windows (Imagen III.29), seleccionando únicamente la opción de servidor de AD RMS como se muestra en la Imagen III.30.

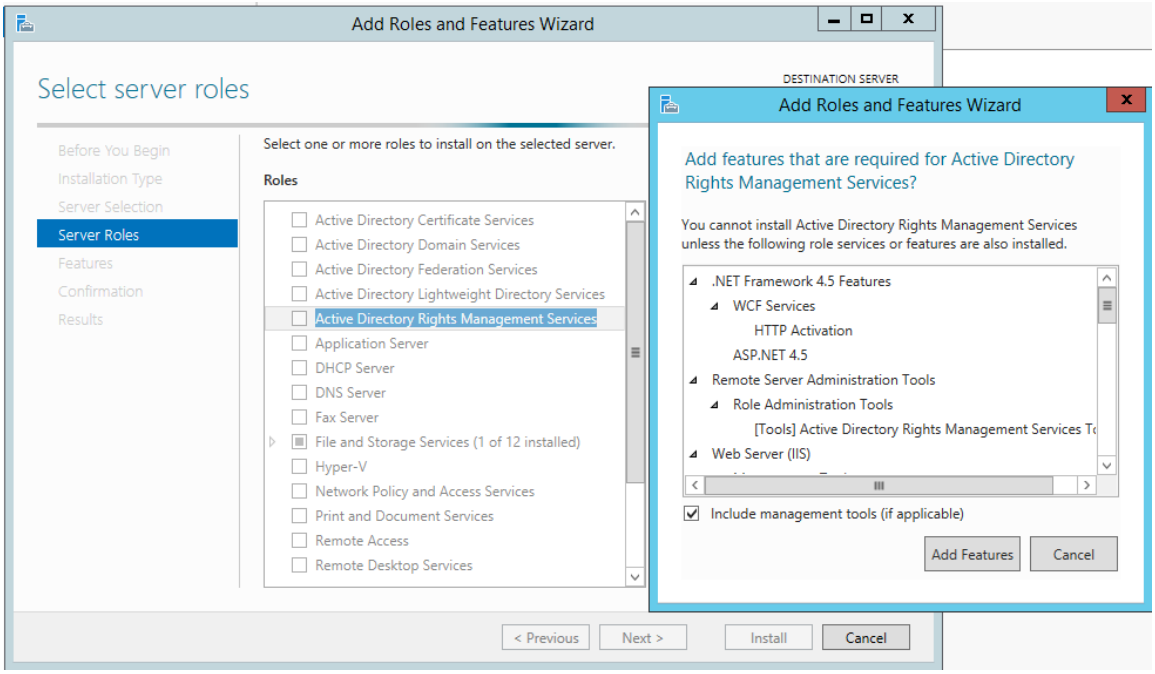


IMAGEN III. 29 - ROL DE ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES

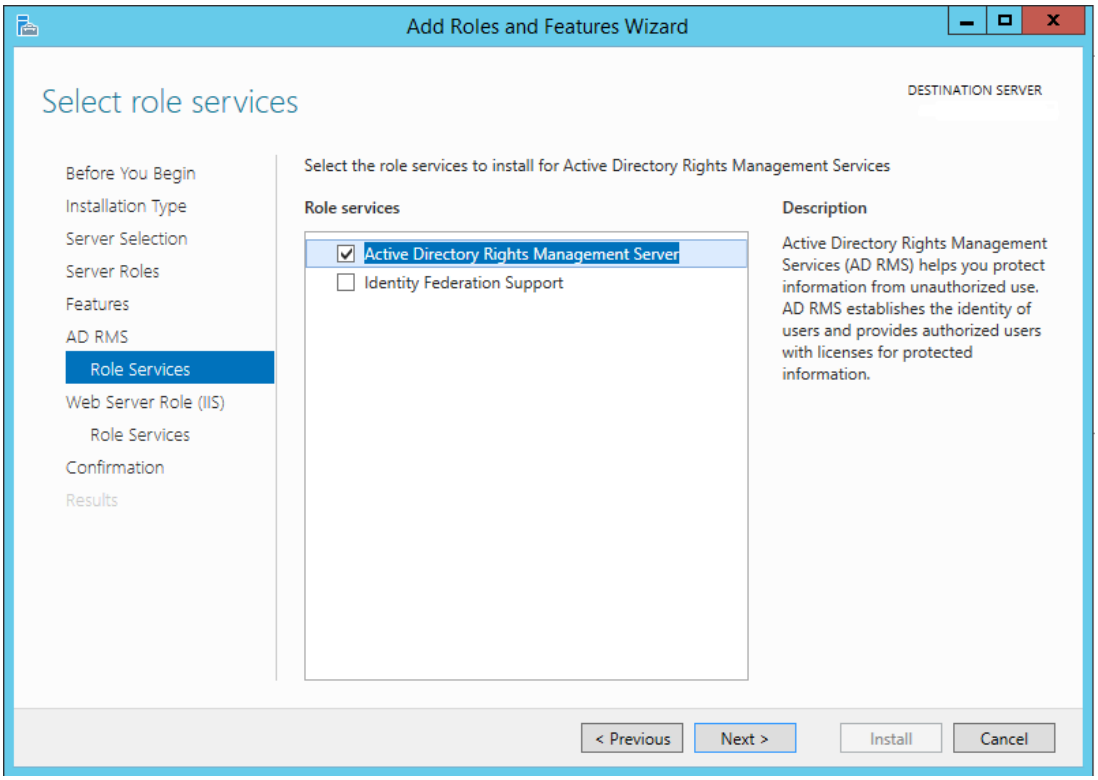


IMAGEN III. 30 - SELECCIÓN DEL ROL A INSTALAR

Cuando finalizó la instalación fue necesario realizar una configuración adicional (Imagen III.31).

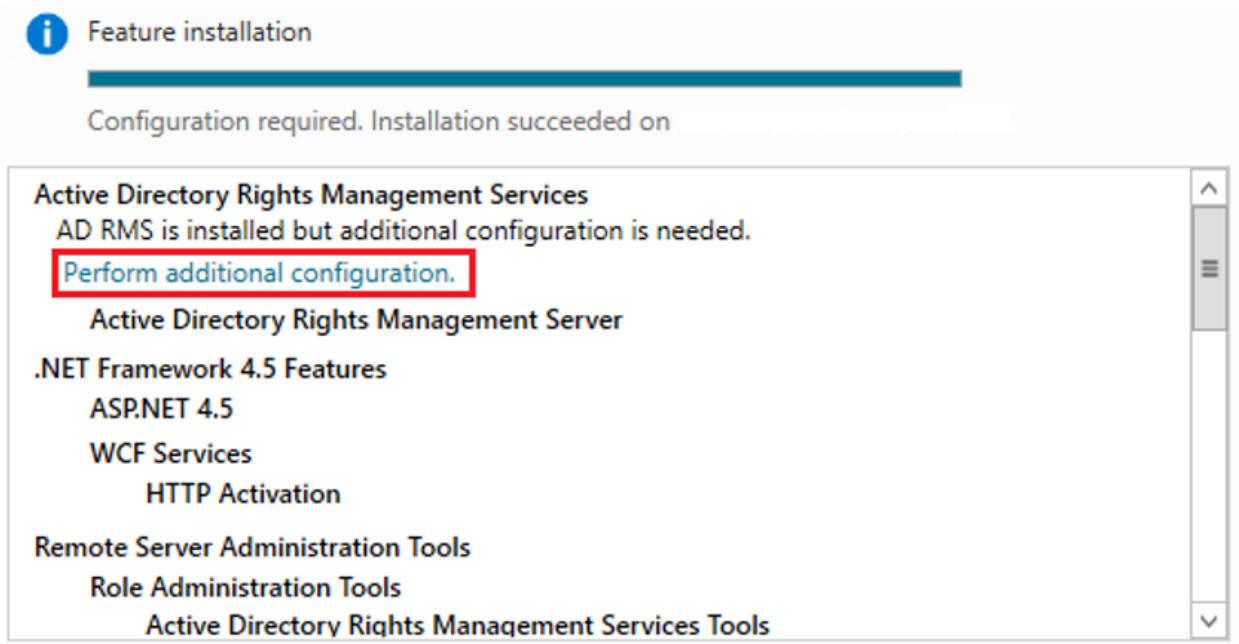


IMAGEN III. 31 - FIN DE LA INSTALACIÓN DE AD RMS

La configuración se realizó con los datos mostrados en la imagen III.32:

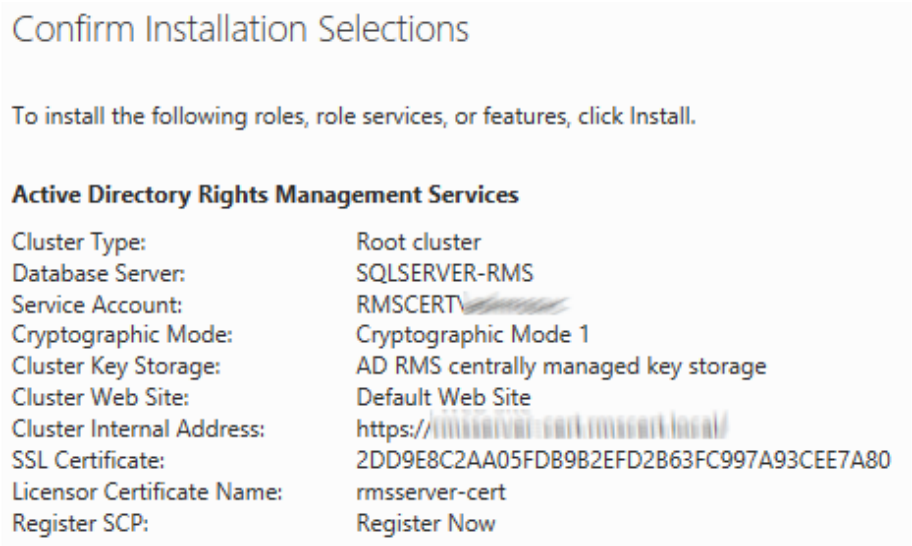


IMAGEN III. 32 - CONFIGURACIÓN ADICIONAL

- El tipo de clúster se seleccionó como Root, ya que es el único que trabajara en el dominio seleccionado. Debemos indicar la base de datos a utilizar y el servidor que la aloja.
- La cuenta de servicio a utilizar es la misma que creamos cuando configuramos el dominio.

- El modo criptográfico fue el 1, ya que es el único modo en que puede hacerse uso de una relación de confianza con Microsoft para trabajar con Windows ID.
- Especifiqué la URL del sitio que vamos a utilizar, indicando también el certificado que la Autoridad Certificadora emitió. Por ultimo tuve que indicar que debía registrarse el Service Connection Point (SCP) en el dominio con la finalidad de validar al servidor RMS.

Al finalizar la instalación se muestra una pantalla de resultados (Imagen III.33)

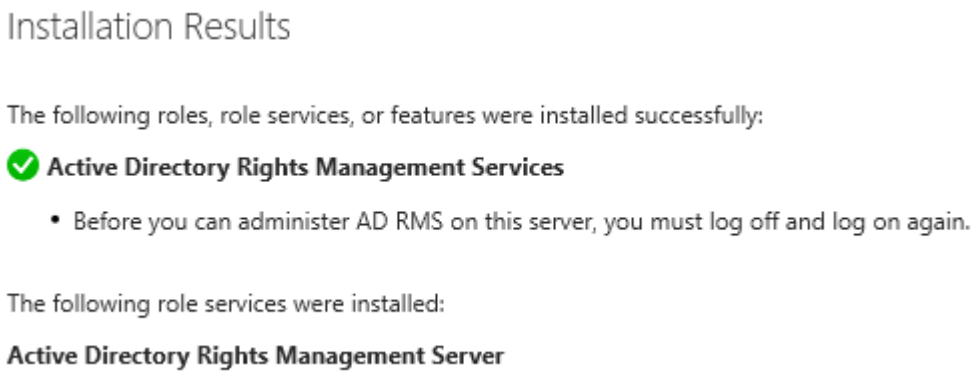


IMAGEN III. 33 - INSTALACIÓN EXITOSA DE AD RMS

Para contar con RMS funcional con cuentas Windows ID se debe configurar IIS para que permita la autenticación anónima a los sitios requeridos por RMS. Dentro de la consola de administración de IIS se expandieron las características de los subsitios “Licensing” y “Certification” (Imagen III.34), en ambos sitios existe un archivo al cual al que habilitar la autenticación anónima, estos archivos son license.asmx y certificate.asmx respectivamente (Imagen III.36)

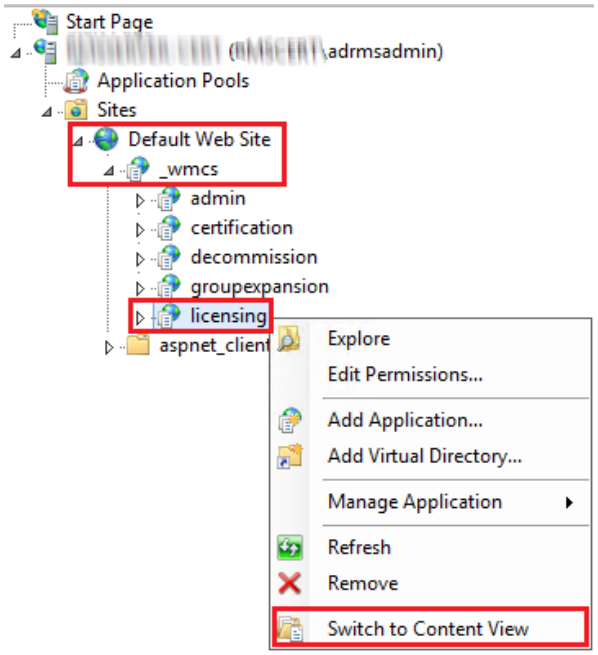


IMAGEN III. 34 - VISTA DE CONTENIDO DEL SITIO WEB

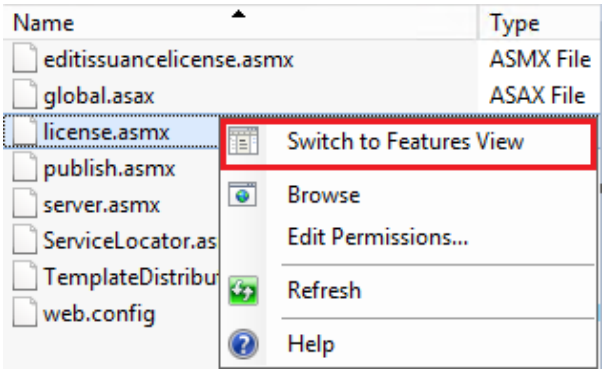


IMAGEN III. 35 - VISTA DE CARACTERÍSTICAS DEL SITIO WEB

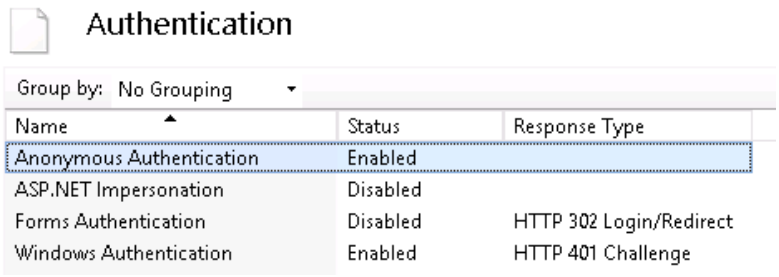


IMAGEN III. 36 - HABILITACIÓN DE AUTENTICACIÓN ANÓNIMA

Con la autenticación anónima habilitada, lo siguiente fue solicitar una relación con Microsoft para confiar en las cuentas proporcionadas por ellos, conocidas como Windows Live ID. Esto se hace desde la consola de administración de AD RMS, expandiendo el árbol de opciones hasta "Trusted Users Domains" (Imagen III.37) y dar clic en "Trust Microsoft accounts", lo que agrega una nueva relación de confianza al servidor (Imagen III.38)

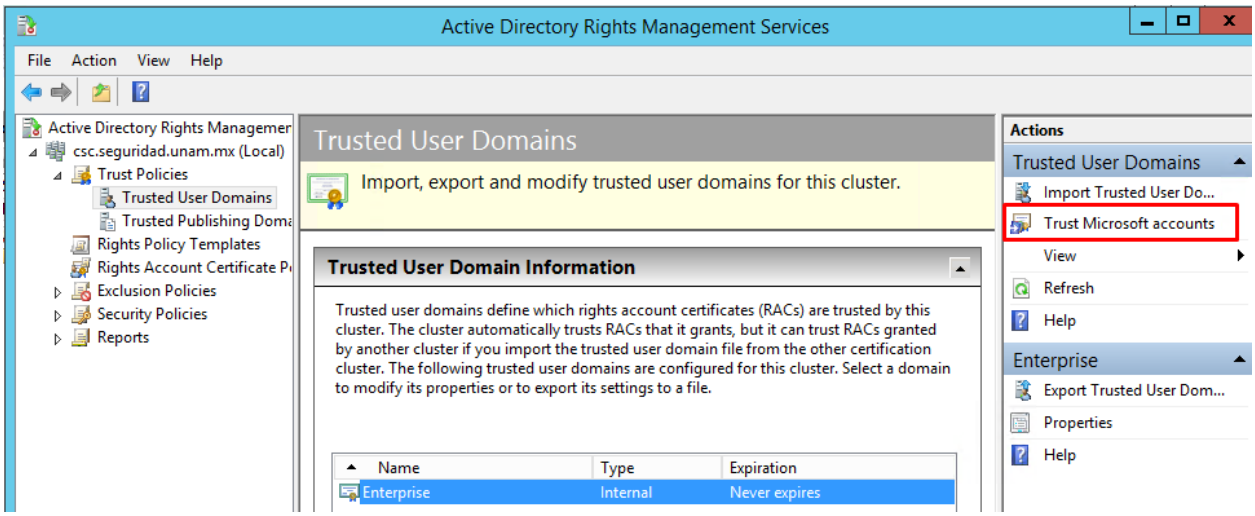


IMAGEN III. 37 - CONFIANZA EN CUENTAS MICROSOFT

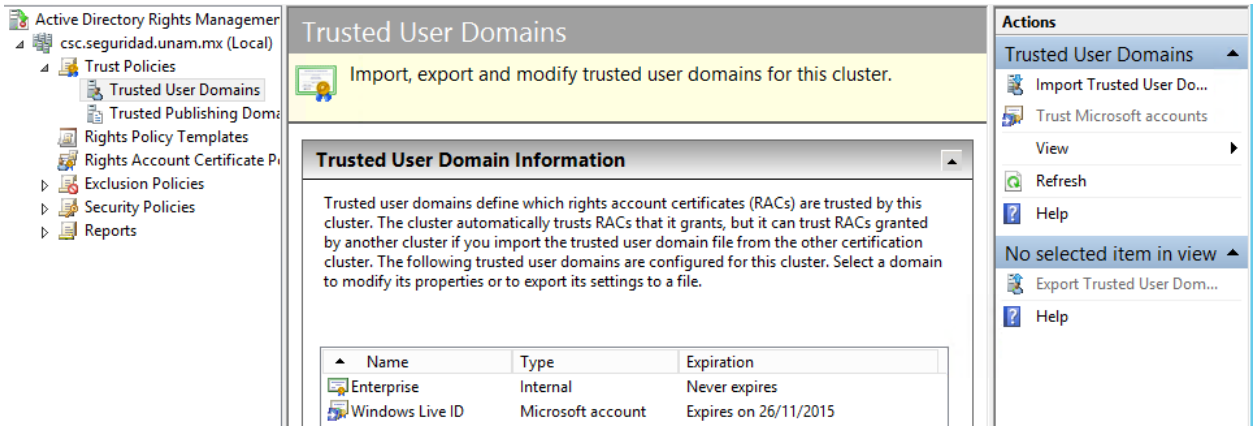


IMAGEN III. 38 - DOMINIOS DE CONFIANZA

Para que usuarios fuera del dominio puedan hacer uso de AD RMS es necesario configurar una URL extranet, es decir, URL desde donde nuestro servicio web de licencias puede ser visitado por Internet. Esto se hizo desde las propiedades del clúster en la consola de administración de AD RMS. Ahí se indicaron las URL a utilizar, correspondientes al registro DNS creado y asociado a la dirección IP pública (Imagen III.39)

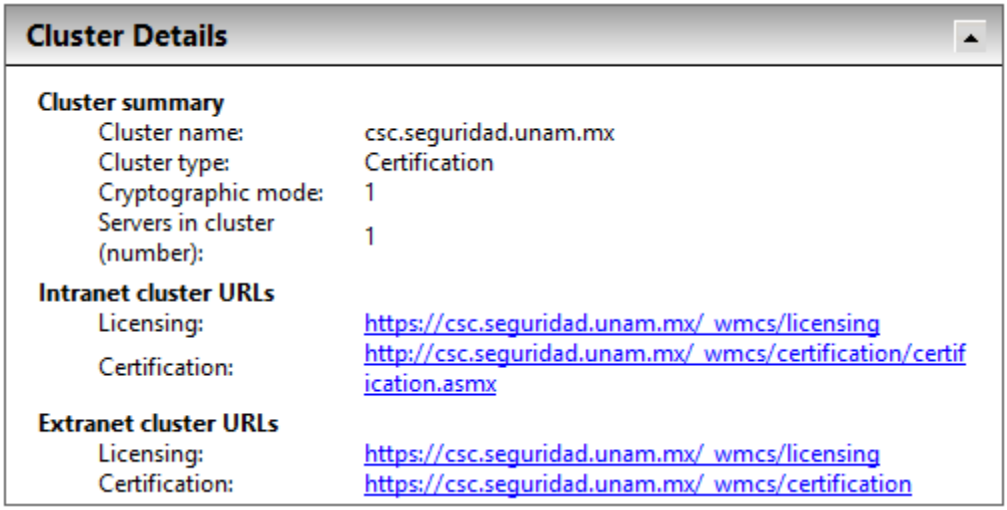


IMAGEN III. 39 - URLS DEL SERVICIO RMS

Con esto se terminó de instalar el ambiente de pruebas. Se configuró adicionalmente un cliente Windows (Windows 8.1) unido al dominio con Office 2013 instalado.

Se protegieron documentos para probar la funcionalidad del ambiente, tanto en el dominio como en una red externa con el fin de probar la conexión desde Internet. Los resultados obtenidos fueron los esperados, por lo que se decidió replicar el proceso de instalación para el ambiente de producción.

III.1.9 IMPLEMENTACIÓN EN UN AMBIENTE DE PRODUCCIÓN

Para la implementación del ambiente de producción se replicó el proceso de instalación y configuración usado en el ambiente de pruebas debido a que este ambiente resultó funcional y no hubo errores de diseño a corregir.

Como se mencionó anteriormente, el ambiente de producción se instaló en la DMZ de la Coordinación de Seguridad de la Información, quedando como se muestra en la imagen III.40.

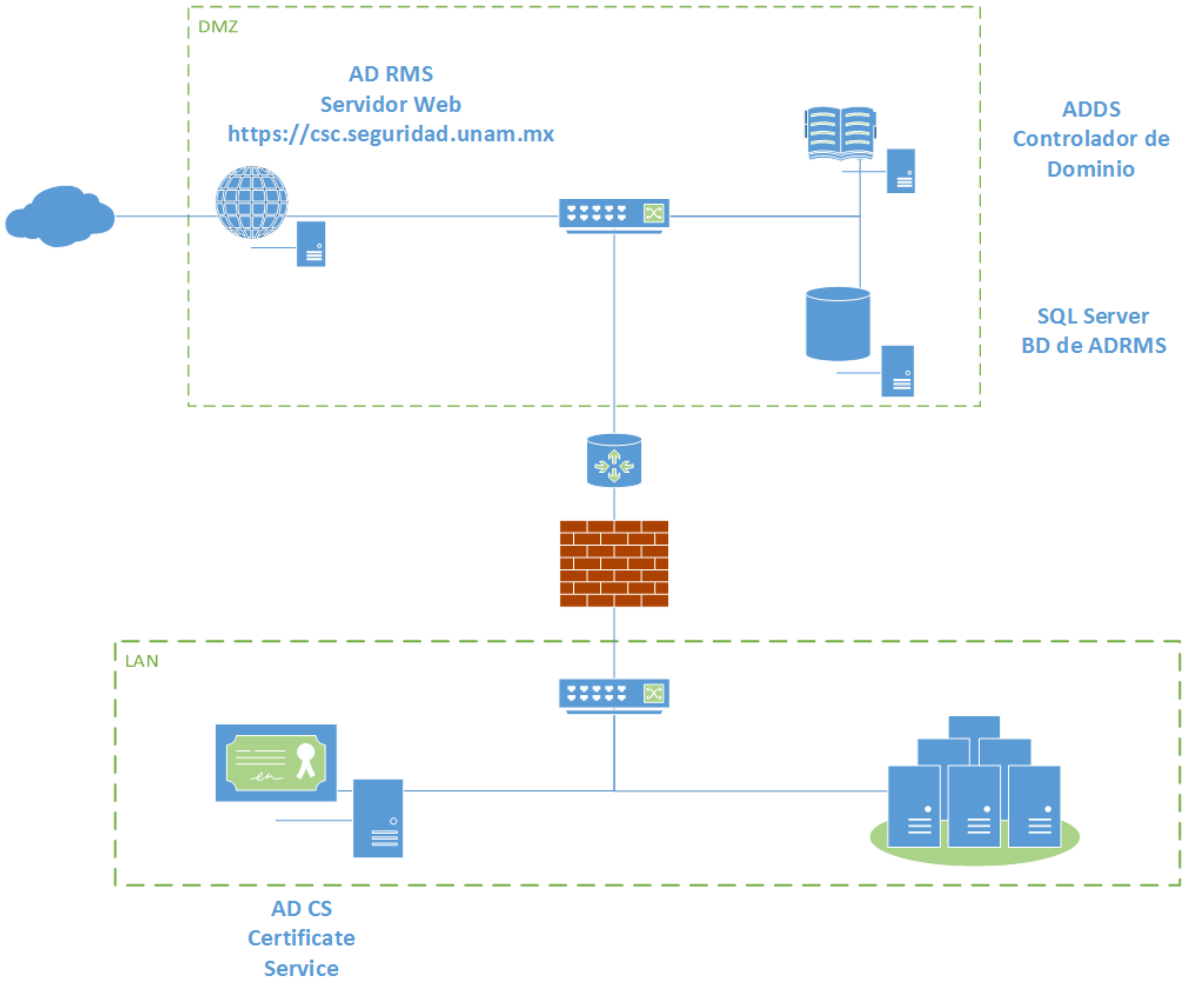


IMAGEN III. 40 - INFRAESTRUCTURA IMPLEMENTADA

Las URL que el cliente de RMS visitará tanto desde el dominio como desde Internet son:

- **https://csc.seguridad.unam.mx/_wmcs/licensing/license.asmx**
- **https://csc.seguridad.unam.mx/_wmcs/certfication/certification.asmx**

III.1.10 PRUEBAS FUNCIONALES

Las pruebas funcionales se realizaron creando un documento de Word para que solo el usuario *rmspruebas@outlook.com* pudiera ver el documento. Esto se hizo de dos formas, con una plantilla de RMS y con protección individual desde Office. La plantilla se genera en el servidor RMS, ahí se le añadió una descripción y una lista de usuarios (Imagen III.41 e Imagen III.42).

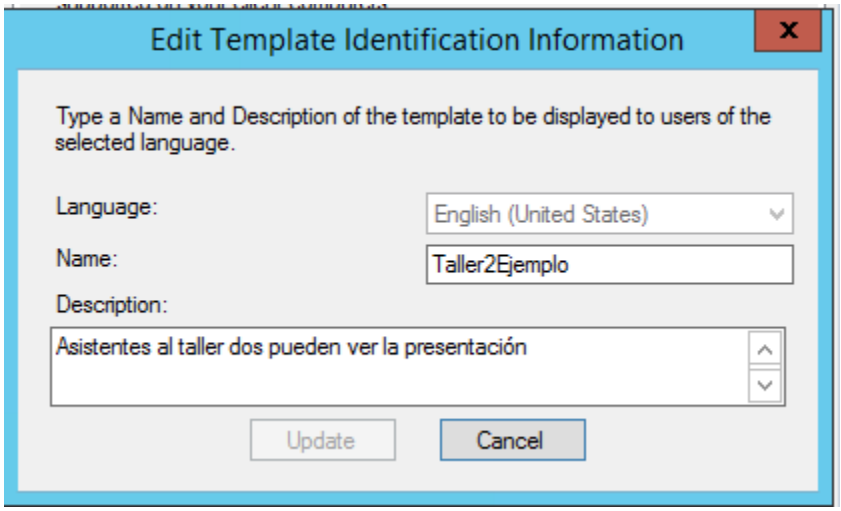


IMAGEN III. 41 - DATOS DE LA PLANTILLA RMS

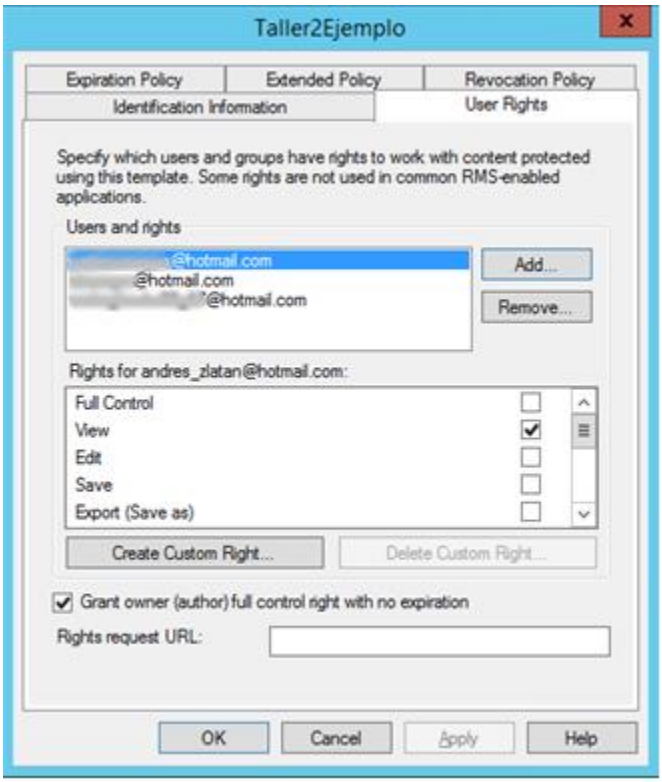


IMAGEN III. 42 - PERMISOS DE USUARIO EN LA PLANTILLA

Al abrir el Word y crear un documento, en el menú tenemos la opción de proteger dicho archivo, ahí podremos contactar al servidor RMS y descargar las plantillas de seguridad creadas (Imagen III.43).

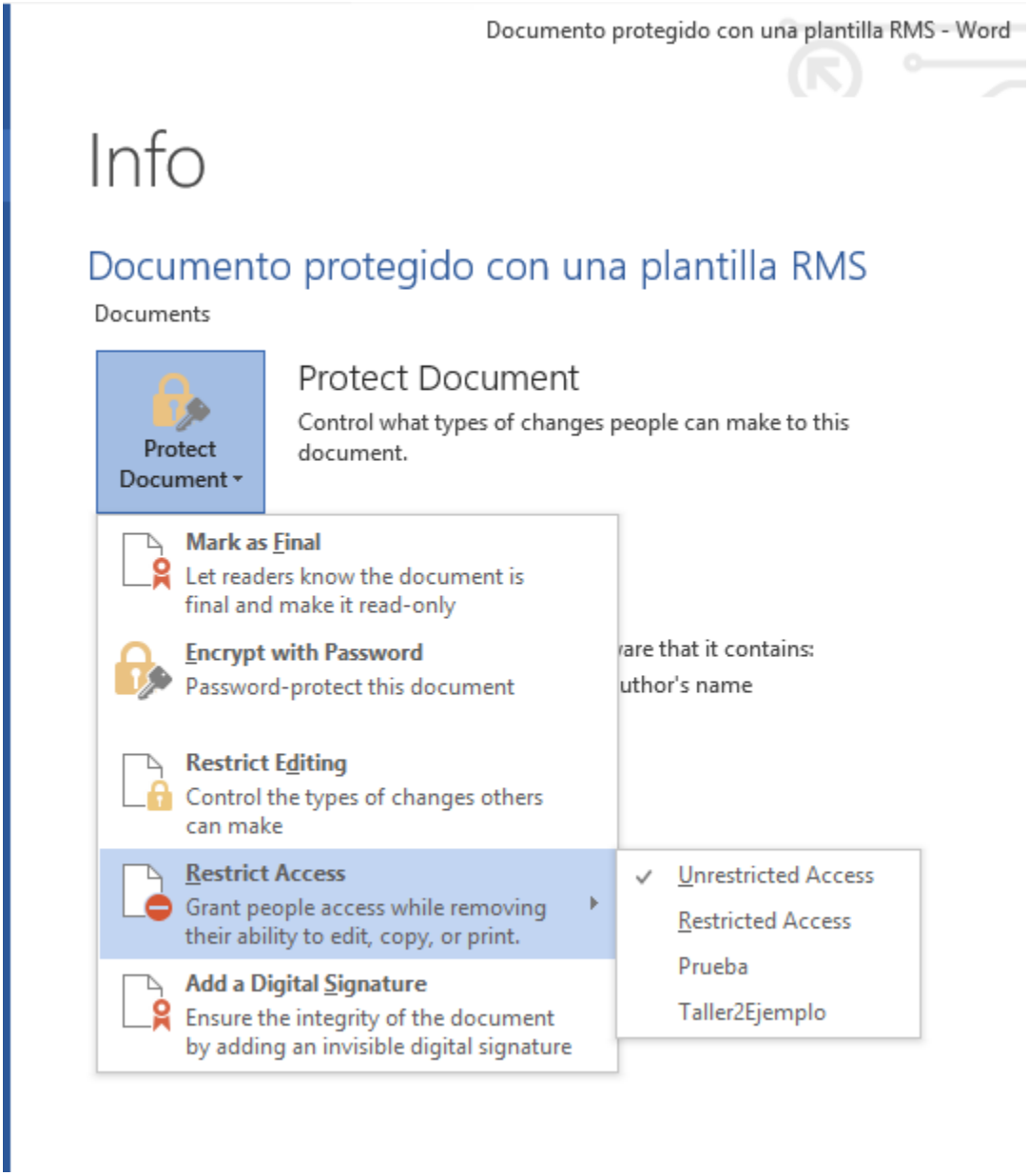


IMAGEN III. 43 - RESTRICCIÓN DE ACCESO A UN DOCUMENTO DE WORD

Al seleccionar una plantilla, el documento desplegará una banda en la que se pueden revisar los permisos asociados a la plantilla (Imagen III.44)

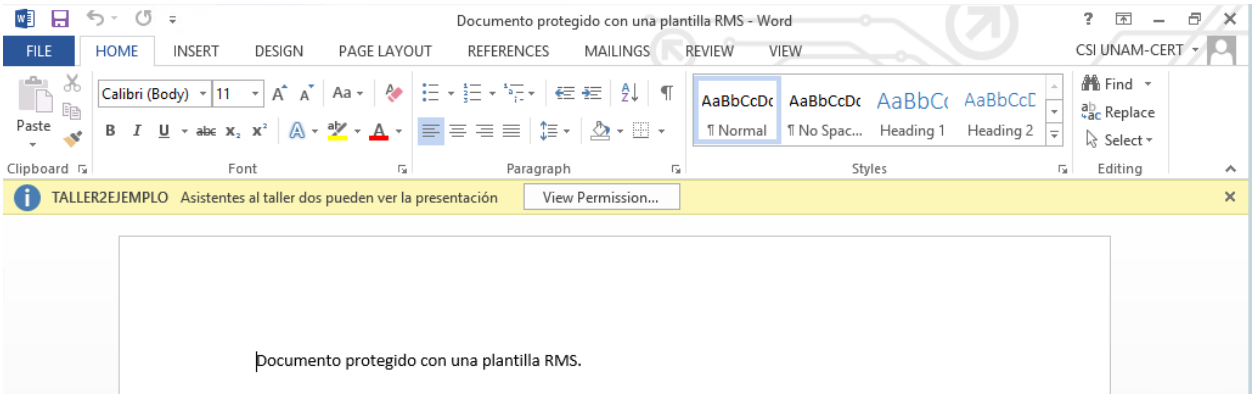


IMAGEN III. 44 - DOCUMENTO PROTEGIDO (VISTO POR EL CREADOR)

Una vez que se protegió el documento se puso al alcance de uno de los usuarios destinados a verlo. Al abrir el documento, el cliente instalado en el equipo del usuario contactó al servidor RMS con la finalidad de obtener la información necesaria para poder visualizar el documento (Imagen III.45).

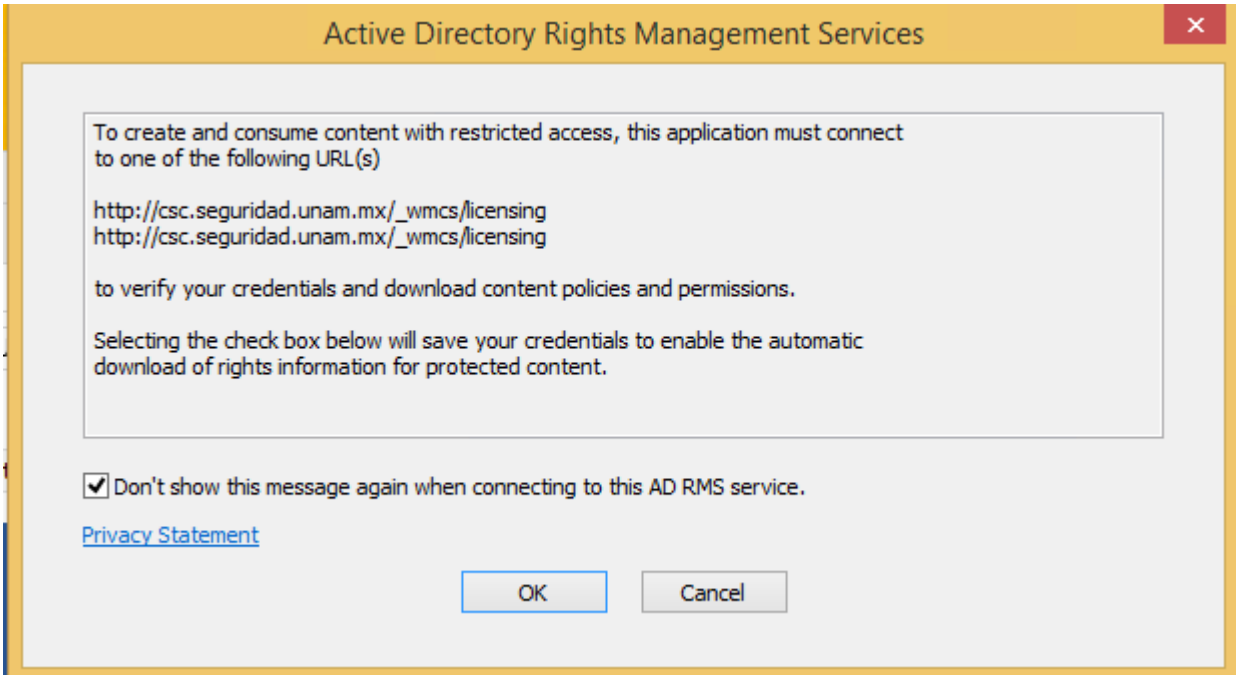


IMAGEN III. 45 - CONEXIÓN AL SERVIDOR RMS

Al no tratarse de un usuario del dominio en donde se encuentra instalado el servidor RMS, el cliente solicitó al usuario un correo electrónico para poder abrir el archivo (Imagen III.46 e Imagen III.47).

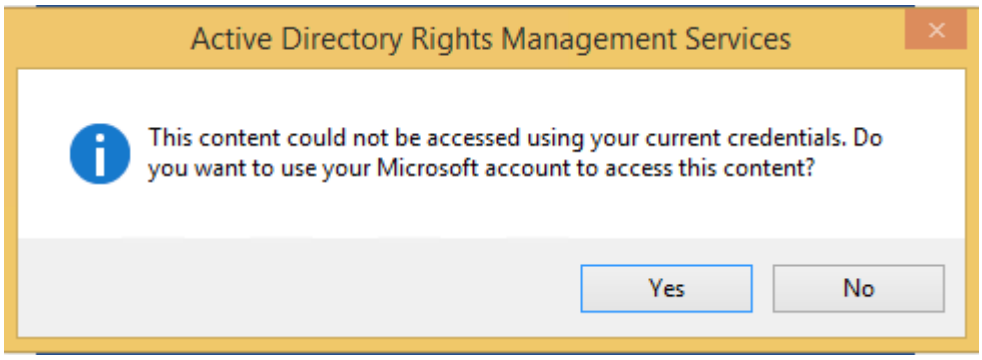


IMAGEN III. 46 - ACCESO CON CUENTA MICROSOFT

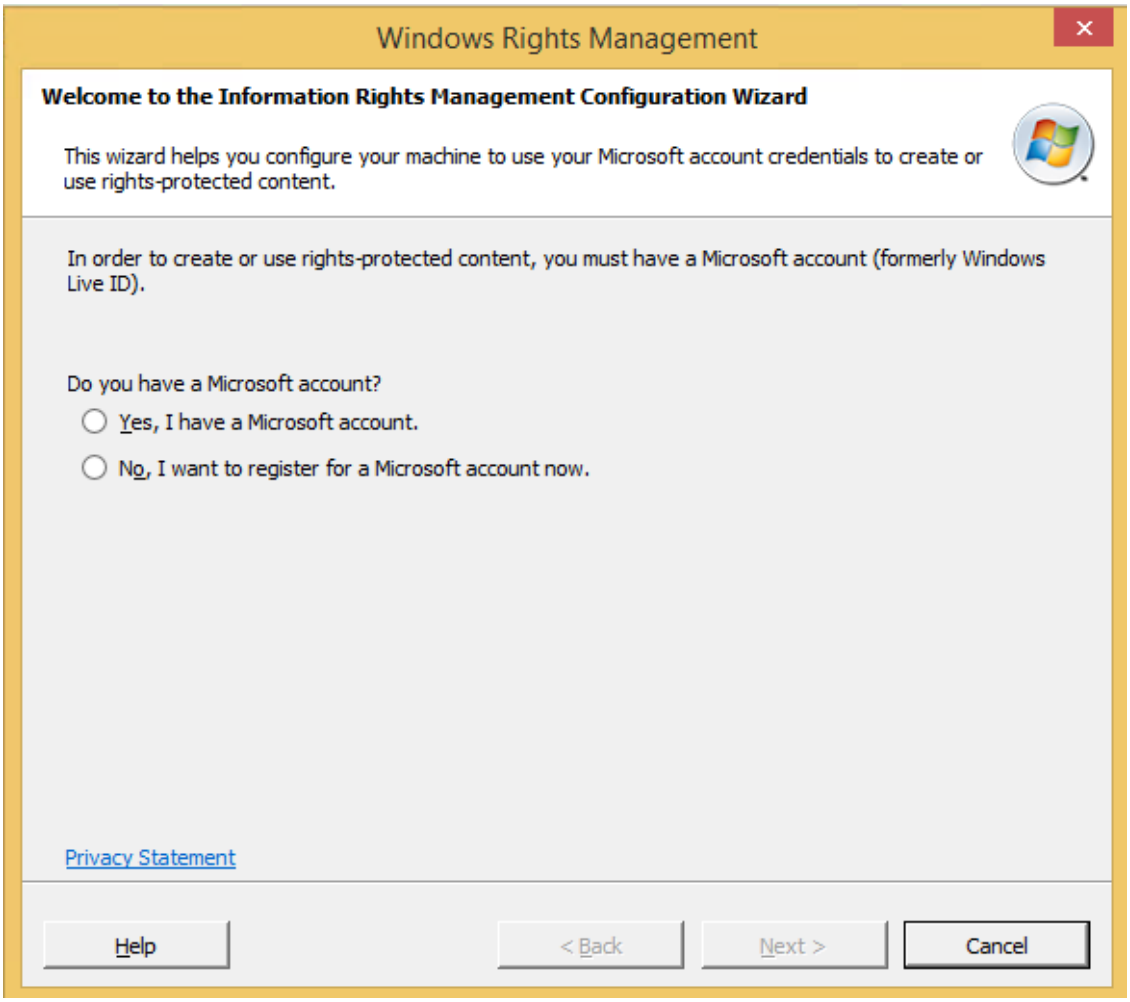


IMAGEN III. 47 - SOLICITUD DE ACCESO CON CUENTA MICROSOFT

El usuario entonces inició sesión con la cuenta de correo rmspruebas@outlook.com (Imagen III.48 e Imagen III.49).

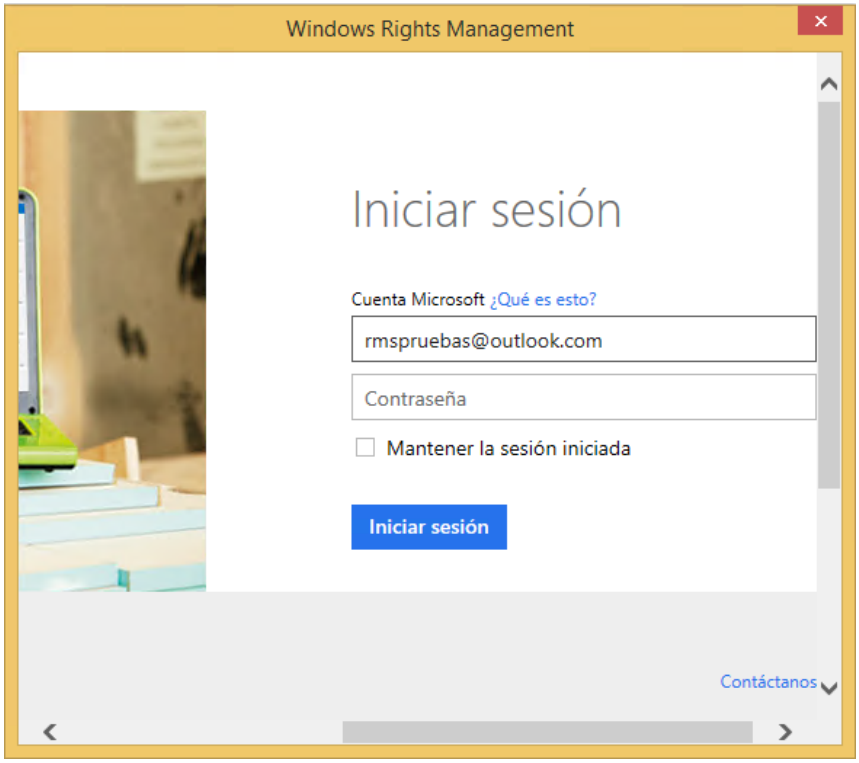


IMAGEN III. 48 - SOLICITUD DE CREDENCIALES

IMAGEN III. 49 - SELECCIÓN DE TIPO DE COMPUTADORA

Al verificarse la identidad del usuario, el servidor RMS otorgó una licencia de uso por un periodo de tiempo definido (Imagen III.50).

IMAGEN III. 50 - CONFIRMACIÓN DE ELECCIÓN

Es entonces cuando el cliente RMS de manera automática aplicó los permisos y restricciones al documento asociados al usuario autenticado (Imagen III.51).

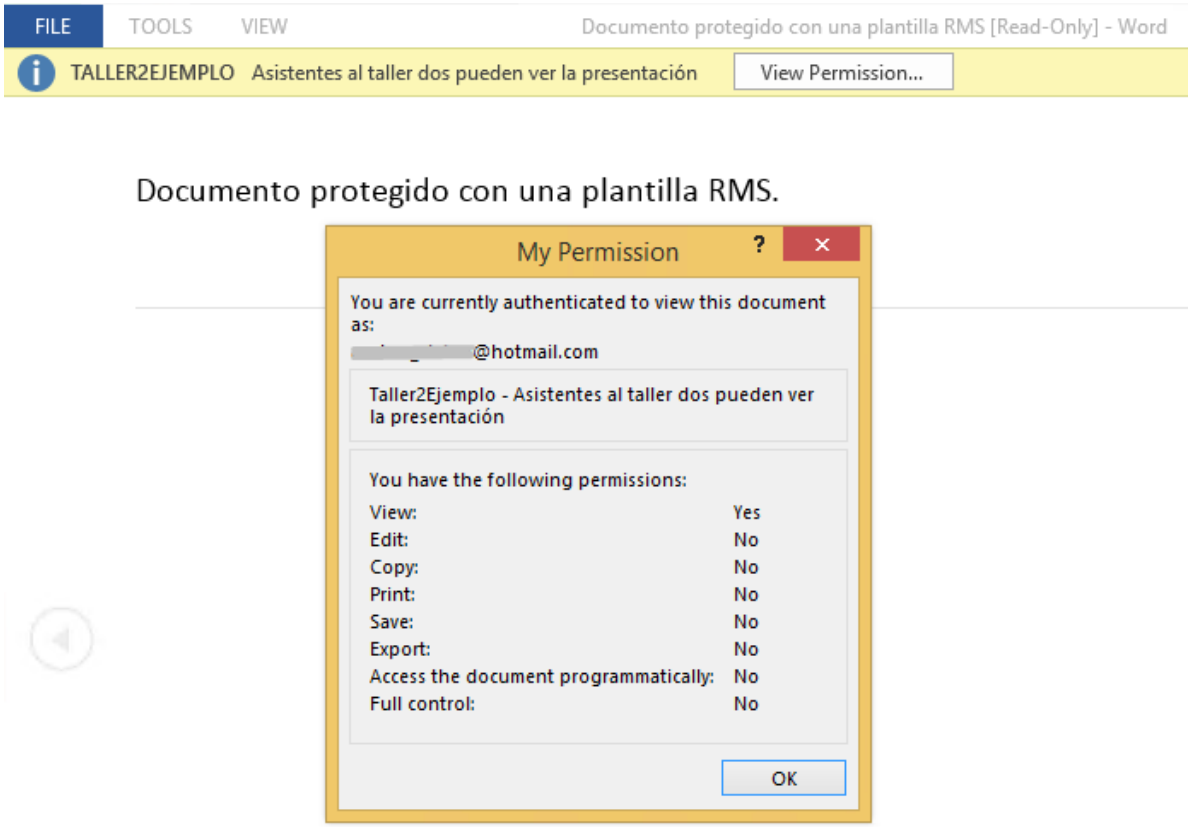


IMAGEN III. 51 - DOCUMENTO PROTEGIDO Y PERMISOS

III.1.11 RESULTADOS OBTENIDOS

Al finalizar este proyecto, se obtuvieron como resultados un ambiente de pruebas y un ambiente en producción. De forma adicional se generó un documento (Ver Anexo 1) en donde se detalló el proceso de instalación, tanto del ambiente de pruebas como de producción, adicionalmente se generó documentación para la implementación del proyecto en una infraestructura alojada en la nube haciendo uso de la plataforma Windows Azure.

A continuación presento la tabla de contenido del documento generado con la descripción anterior:

1. Introducción
2. Objetivo del Proyecto
3. Descripción del Proyecto
4. CREACIÓN DE SERVICIOS EN MICROSOFT AZURE
   - 4.1 Cuenta de almacenamiento
   - 4.2 Red Virtual
   - 4.3 Máquinas virtuales
     - 4.3.1 Creación de la máquina virtual para el servidor SQL
     - 4.3.2 Creación de la máquina virtual para el servidor RMS
     - 4.3.3 Conexión a las máquinas virtuales por escritorio remoto
     - 4.3.4 Establecer IP estática para las máquinas virtuales del proyecto
5. INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS EN EL SERVIDOR SQL
   - 5.1 Active Directory
     - 5.1.1 Instalación del servicio de dominio de Active Directory
     - 5.1.2 Configuración del servicio de dominio de Active Directory
   - 5.2 Verificación de instalación de .NET Framework 3.5
   - 5.3 Permitir conexiones remotas utilizando políticas de grupo
     - 5.3.1 Creación del grupo de seguridad para usuarios de escritorio remoto
     - 5.3.2 Creación de GPO (Group Policy Object) [4]
   - 5.4 Creación de usuarios
   - 5.5 Autoridad Certificadora (Opcional)
     - 5.5.1 Instalación
   - 5.6 Configuración de SQL Server
     - 5.6.1 Añadir el usuario ADRMSADMIN como cuenta de inicio de sesión a SQL
     - 5.6.2 Iniciar el servicio SQL Server Browser
     - 5.6.3 Añadir excepciones en el firewall para los puertos usados por SQL Server
6. INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS EN EL SERVIDOR RMS
   - 6.1 Unión del servidor RMS al dominio
   - 6.2 Apertura de puertos en el portal de Microsoft Azure
   - 6.3 .NET Framework 3.5
   - 6.4 Instalación IIS
   - 6.5 Solicitud de certificado
   - 6.6 Instalación y configuración de AD RMS

III.2 AUDITORÍA Y APOYO TÉCNICO EN MATERIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN AL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES PARA LAS ELECCIONES FEDERALES 2015

III.2.1 ANTECEDENTES DEL PROYECTO

Como parte del Convenio de Colaboración con el Instituto Nacional Electoral (INE), la Coordinación de Seguridad de la Información/UNAM-CERT a través de la Dirección General de Cómputo y de Tecnologías de la Información y Comunicación (DGTIC) de la UNAM llevó a cabo la revisión de configuraciones de seguridad a la infraestructura de Tecnologías de Información que sería utilizada para el Programa de Resultados Electorales Preliminares (PREP) 2015.

III.2.2 OBJETIVO

Analizar información de configuraciones de los dispositivos que conforman la infraestructura de Tecnologías de Información del "PREP 2015" con base en buenas prácticas de seguridad informática para identificar oportunidades de mejora y emitir recomendaciones orientadas al fortalecimiento de la misma.

III.2.3 INTRODUCCIÓN

El proyecto a cargo de la UNAM se dividió en dos líneas principales:

1. Auditoría de Software y Pruebas de Calidad
2. Auditoría de Seguridad a la Infraestructura Tecnológica

Auditoría de Software y Pruebas de Calidad
Tiene como objetivo "analizar el aplicativo del Programa de Resultados Electorales Preliminares, (PREP 2015), mediante la revisión de código fuente y la realización de pruebas funcionales de caja negra, que permitan evaluar la integridad en el procesamiento de la información de las Actas de Escrutinio y Cómputo para la elección de Diputados Federales y la generación de resultados preliminares conforme a la normativa aplicable y vigente".[6]

Está Línea a su vez se dividió en 3 sublíneas de trabajo:

a. Revisión de Código Fuente
b. Pruebas de Calidad
c. Validación de programas

[6] Universidad Nacional Autónoma de México. 2015. *Auditoría y apoyo técnico al Programa de Resultados Electorales Preliminares para las Elecciones Federales 2015*. Recuperado el 10 de Enero de 2016, de http://www.auditoriaprep2015.unam.mx/consiste.html

Auditoría de Seguridad a la Infraestructura Tecnológica
La auditoría de seguridad a la infraestructura tecnológica del PREP 2015 y RedINE comprende cuatro fases. Las tres primeras fases se realizan de forma previa a la jornada electoral y consisten en ejecutar pruebas de penetración, revisión de configuraciones y pruebas de denegación de servicio (DoS, por sus siglas en inglés). Tienen por objetivo identificar posibles vulnerabilidades en la infraestructura tecnológica del PREP y la RedINE, para emitir recomendaciones que permitan subsanarlas oportunamente. A partir de esta información, el INE toma medidas pertinentes. Posteriormente, la UNAM verifica que las medidas implementadas por el INE hayan corregido los hallazgos reportados. En la última etapa se realiza el monitoreo de seguridad en la infraestructura del PREP 2015 durante su operación.[7]

De forma resumida, esta línea está dividida en cuatro etapas:
1. Pruebas de Penetración
2. Revisión de Configuraciones
3. Pruebas de Denegación
4. Monitoreo de Seguridad

III.2.4 ACTIVIDADES REALIZADAS DURANTE EL PROYECTO

La descripción de las actividades que realicé durante de mi participación en este convenio se apega a la décima tercera cláusula del Convenio de Colaboración entre el Instituto Nacional Electoral y la Universidad Nacional Autónoma de México, por lo que no se revelará información considerada como confidencial o reservada, haciendo uso únicamente de la información de carácter público.

Las actividades que realicé fueron parte de la línea de *Auditoría de Seguridad a la Infraestructura Tecnológica* en la fase de Revisión de Configuraciones.

La revisión de configuraciones de seguridad consistió en una serie de pruebas que buscaban analizar las configuraciones de una muestra de dispositivos que conforman la infraestructura tecnológica, comparándolas con buenas prácticas internacionales de seguridad informática.

Para esta fase, mi primera actividad fue actualizar la lista de configuraciones de seguridad recomendadas perteneciente a la Coordinación de Seguridad de la información/UNAM-CERT y adaptarla a la infraestructura tecnológica del INE, principalmente para los equipos con sistema operativo UNIX.

Está lista la actualicé y la comparé con recomendaciones de seguridad emitidas por organizaciones como Red Hat, National Institute of Standards and Technology (NIST), SysAdmin Audit, Networking an Security Institute (SANS) y la National Security Agency (NSA).

[7] Ídem

Una vez actualizada la lista de recomendaciones, lo siguiente que hice fue revisar los equipos con sistema operativo UNIX de la infraestructura del INE y comprobar cada uno de los elementos de dicha lista verificando su cumplimento. Terminada la revisión, realicé un análisis de resultados obtenidos en los que seleccione los elementos de la lista de recomendaciones de seguridad que no cumplieron con los valores esperados. Estos elementos fueron puestos en un informe que se le entro al Instituto Nacional Electoral, detallando cada uno de los hallazgos, el impacto que tenían sobre la infraestructura y una recomendación de solución.

El INE entonces se encargó de corregir dichos hallazgos para mitigar los riesgos que estos conllevaban. Una vez corregidos, mi siguiente actividad fue realizar una segunda revisión y verificar que se realizaron las correcciones pertinentes o bien, que se expusieron razones por las cuales la corrección no se hizo, justificando por qué y aceptando el riesgo que esto conllevaba. Terminando la segunda revisión redacté un informe en dónde indiqué los hallazgos obtenidos durante la primera y segunda revisión, las fortalezas encontradas respecto a buenas prácticas y un resumen del estado final de la infraestructura. Este informe formó parte de un informe general en donde se conjuntaron los resultados de las pruebas de penetración, de denegación y monitoreo.

III.2.5 RESULTADOS OBTENIDOS

Generales

Los resultados de la auditoría mostraron que el PREP se encontraba listo para recabar, procesar y publicar, de forma íntegra y confiable, la información de las Actas de Escrutinio y Cómputo del día 7 de junio. El día de la jornada electoral, antes de que el PREP iniciara operaciones, la UNAM comprobó ante notario público que los programas que fueron auditados fuesen los mismos que el INE operó en esa elección federal y que la base de datos de los resultados preliminares iniciara en ceros. [8]

Revisión de Configuraciones

La UNAM analizó los parámetros de configuración de una muestra conformada por al menos un elemento de cada tipo de los que integraban la infraestructura tecnológica del PREP de las elecciones de Diputados federales 2015. A partir del análisis, se identificaron fortalezas y áreas de oportunidad respecto a las buenas prácticas de seguridad de la información, a partir de las cuales se presentaron recomendaciones. Las sugerencias fueron debidamente atendidas por el INE y verificadas por la Universidad. [9]

---

[8] Instituto Nacional Electoral. 5 de Junio de 2015. *La UNAM concluye la auditoría al PREP de las Elecciones Federales 2015.* Recuperado el 10 de Enero de 2016, de http://www.ine.mx/archivos3/portal/historico/contenido/comunicados/2015/06/20150605.html

[9] Universidad Nacional Autónoma de México. Junio 2015. *Informe final de la auditoría de seguridad a la infraestructura tecnológica del PREP 2015.*Recuperado el 11 de Enero de 2016, de http://www.auditoriaprep2015.unam.mx/docs/resultados_auditoriadeseguridad.pdf

CONCLUSIONES

Durante mi instancia en la Facultad de Ingeniería adquirí los conocimientos de redes, sistemas operativos, hardware, software y seguridad de la información que me permitieron desempeñar mis actividades laborales. Adicionalmente mi participación en la Coordinación de Seguridad de la Información/UNAM-CERT como becario y trabajando me permitió adquirir conocimientos adicionales que facilitaron la realización de los proyectos en los que participé.

El primer proyecto referente a Active Directory Rights Management Services (AD RMS) fue el primer proyecto a mi cargo en la Coordinación y el primer proyecto que sería implementado para su uso en una dependencia de la Universidad.

Considero que cumplí los objetivos planteados para el proyecto, ya que logre implementar una infraestructura funcional de AD RMS para su uso en los Congresos de Seguridad en Cómputo, AdminUNAM, plan de becarios y demás proyectos de UNAM-CERT que requieran distribuir materiales a los participantes. Este proyecto permite a la Coordinación proteger estos documentos y garantizar que sólo las personas autorizadas tengan acceso a estos, sean o no miembros de la comunidad universitaria.

Como aportación adicional, la documentación del proceso de instalación, pruebas funcionales y solución de errores permitirán a la Coordinación realizar una nueva instalación en caso de que sea requerida, o bien, implementarlo en otras dependencias de la Universidad.

Respecto al segundo proyecto, Auditoría y Apoyo Técnico en Materia de Tecnologías de Información y Comunicación al Programa de Resultados Electorales Preliminares para las Elecciones Federales 2015, los objetivos planteados por la Universidad y por el INE se cumplieron, dando como resultado una elecciones federales en las cuales la infraestructura tecnología funcionó de la mejor manera bajo las buenas prácticas de seguridad de la información.

Este proyecto fue el primer proyecto con repercusión nacional en el que he participado activamente, y en el que nuevamente gracias a los conocimientos obtenidos en la Facultad de Ingeniería y en UNAM-CERT pude desempeñarme de forma eficiente cumpliendo con las expectativas tanto de la Universidad como del Instituto Nacional Electoral.

REFERENCIAS BIBLIOGRÁFICAS

[1] B. Svidergol y R. Allen, Active Directory Cookbook, Estados Unidos de América: O'Reilly, 2013.

[2] B. Desmond, J. Richards, R. Allen y A. Lowe-Norris, Active Directory: Desingning, Deploying and Running, Estados Unidos de América: O'Reilly, 2013.

[3] B. Payatte, Windows Powershell In Action, Second Edition, Estados Unidos de América: Manning, 2011.

[4] J. Moskowitz, Group Policy: Fundamentals, Security and Troubleshooting, Estados Unidos de América: SYBEX, 2008.

[5] B. Smith and B. Komar, Microsoft Windows Security Resource Kit, Estados Unidos de América: Microsoft Press, 2003.

[6] C. Russel and C. Zacker, Windows Server 2008 R2, Estados Unidos de América: Microsoft Press, 2010.

[7] C. Russel, Administering Windows Server 2012 R2, Estados Unidos de América: Microsoft Press, 2014.

[8] D. Bernal, «Adaptación del proyecto de software libre para la implementación de servidor WHOIS, Actividades realizadas por SSI/UNAM-CERT de la DGTIC de la UNAM,» Universidad Nacional Autónoma de México, México D.F., 2011.

[9] D. Martín, «Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix,» Universidad Nacional Autónoma de México, México, D.F., 1995.

[10] J. Johansson, Windows Server 2008 Security Resource Kit, Estados Unidos de América: Microsoft Press, 2008.

[11] K. Schaefer, J. Cochran, S. Forsyth, R. Baugh y et al., Professional IIS 7, Estados Unidos de América: Wiley Publishing Inc., 2008.

[12] M. Minasi y et al, Mastering Windows Server 2012 R2, Estados Unidos de América: SYBEX, 2014.

[13] R. Morimoto, Windows Server 2012 Unleashed, Estados Unidos de América: Pearson Education, 2012.

[14] R. Peña, L. Balart, J. Cuartero y J. Orbegozo, Paso a paso Office 2013. Manual práctico para todos, México: Alfaomega, 2013.

[15] S. Reimer y M. Mulcare, Active Directory Resource Kit, Estados Unidos de América: Microsoft Press, 2008.

REFERENCIAS ELECTRÓNICAS

Classon, D. 10 de Septiembre de 2010. *How to install .NET Framework 3.5 on Windows Server 2012 and Windows Server 2012 R2*. Recuperado el 5 de Noviembre de 2014, de http://www.danielclasson.com/install-net-framework-35-server-2012/

Coordinación de Seguridad de la Información. 2015. *Congreso Seguridad en Cómputo*. Recuperado el 5 de diciembre de 2015, de https://congreso.seguridad.unam.mx/2015/

Coordinación de Seguridad de la Información. 2015. *Programa de Becas de Formación en Seguridad Informática*. Recuperado el 9 de Diciembre de 2015, de http://www.seguridad.unam.mx/plan-becarios/cursos.dsc

Delprato, G. 31 de Mayo de 2011. *Demostración Rights Management Services (RMS) en Ambiente de Prueba*. Recuperado el 15 de Noviembre de 2014, de https://windowserver.wordpress.com/2011/05/31/demostracin-rights-management-services-rms-en-ambiente-de-prueba/

Eckes, D. J. 5 de Octubre de 2013. *Server 2012 Enable Remote Desktop (RDP) through Group Policy (GPO)*. Recuperado el 23 de Octubre de 2014, de http://www.dannyeckes.com/server-2012-enable-remote-desktop-rdp-group-policy-gpo/

Gao, R. 5 de Agosto de 2013. *Troubleshooting AD RMS client authentication error.* Recuperado el 28 de Noviembre de 2014, de http://www.rickygao.com/category/adrms/

Jacops, A. 1 de Septiembre de 2014. *Disable strict name checking with PowerShell*. Recuperado el 25 de Noviembre de 2014, de https://4sysops.com/archives/disable-strict-name-checking-with-powershell/

Kam Wah, Y. 24 de Agosto de 2014. *Windows 2012 R2 RMS with Windows Live ID*. Recuperado el 6 de Noviembre de 2014, de http://monsterbean.com/2014/08/24/windows-2012-r2-rms-with-windows-live-id/

Microsoft Corporation. 1 de Julio de 2009. *Using Windows Live ID to Establish RACs for Users*. Recuperado el 17 de Noviembre de 2014, de https://technet.microsoft.com/es-mx/library/ee221037(v=ws.10).aspx

Microsoft Corporation. 13 de Julio de 2013. *Plan Information Rights Management in Office 2013*. Recuperado el 30 de Octubre de 2014, de https://technet.microsoft.com/en-us/library/cc179103(v=office.15).aspx

Microsoft Corporation. 14 de Enero de 2010. *AD RMS Firewall Considerations*. Recuperado el 5 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/dd941596(v=ws.10).aspx

Microsoft Corporation. 15 de Febrero de 2011. *Pre-installation Information for Active Directory Rights Management Services*. Recuperado el 5 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/cc771789.aspx

Microsoft Corporation. 16 de Agosto de 2012. *Configuring Custom Templates for Azure Rights Management.* Recuperado el 17 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/dn642472.aspx

Microsoft Corporation. 2 de Abril de 2009. *Cómo solucionar problemas de configuración de IIS en SQL Server 2005 Reporting Services*. Recuperado el 26 de Noviembre de 2014, de https://support.microsoft.com/es-es/kb/958998

Microsoft Corporation. 2 de Julio de 2012. *Test Lab Guide: Deploying an AD RMS Cluster*. Recuperado el 30 de Octubre de 2014, de https://technet.microsoft.com/en-us/library/jj134037.aspx

Microsoft Corporation. 2013. *Requisitos del sistema e información de instalación de Windows Server 2012 R2*. Recuperado el 15 de Diciembre de 2015, de https://technet.microsoft.com/es-MX/library/dn303418.aspx

Microsoft Corporation. 30 de Diciembre de 2007. *Understanding AD RMS Certificates*. Recuperado el 16 de Diciembre de 2015, de https://technet.microsoft.com/en-us/library/cc753886.aspx

Microsoft Corporation. 31 de Marzo de 2008. *Step 2: Configuring the AD RMS client*. Recuperado el 15 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/cc771971(v=ws.10).aspx

Microsoft Corporation. 7 de Agosto de 2013*. Active Directory Domain Services Overview*. Recuperado el 20 de Noviembre de 2015, de https://technet.microsoft.com/en-us/library/hh831484.aspx

Microsoft Corporation. 9 de Noviembre de 2006. *La conexión a un recurso compartido SMB en un equipo basado en Windows 2000 o en Windows Server 2003 puede no funcionar con un nombre de alias.* Recuperado el 25 de Noviembre de 2014, de https://support.microsoft.com/es-es/kb/281308

Microsoft Technet Forums. 27 de Julio de 2011. *Client can't connect to AD RMS Server*. Recuperado el 27 de Noviembre de 2014, de https://social.technet.microsoft.com/Forums/en-US/b28b335f-4cde-48ad-b682-d81039565e25/client-cant-connect-to-ad-rms-server?forum=rms

Schmarr, A. 14 de Noviembre de 2013. *Installing AD Rights Management Services (ADRMS) on Windows Server 2012 R2.* Recuperado el 6 de Noviembre de 2014, de http://www.schmarr.com/Blog/Post/16/Installing-AD-Rights-Management-Services-%28ADRMS%29-on-Windows-Server-2012-R2

Siddiqui, M. O. 9 de Junio de 2014. *ADRMS Error - The operation being requested was not performed because the user has not been authenticated*. Recuperado el 28 de Noviembre de 2014, de http://blogs.technet.com/b/omers/archive/2014/06/09/adrms-error-the-operation-being-requested-was-not-performed-because-the-user-has-not-been-authenticated.aspx

UNAM. 1998. *Día Internacional de la Seguridad en Cómputo*. Recuperado el 6 de diciembre de 2015, de http://www.disc.unam.mx/1998/

Vilcinskas, M. 16 de Julio de 2013. *Install a new Active Directory forest on an Azure virtual network*. Recuperado el 13 de Agosto de 2015, de https://azure.microsoft.com/en-us/documentation/articles/active-directory-new-forest-virtual-machine/

ANEXO 1

El siguiente documento fue generado para la Coordinación de Seguridad de la Información/UNAM-CERT con la finalidad de contar con una guía de implementación del rol Active Directory Rights Management Services en equipos con sistema operativo Windows Server 2012 R2 para la protección de documentos digitales.

Dicha guía ofrece escenarios de pruebas e implementación, así como una metodología de solución de posibles errores que se puedan presentar durante la instalación del rol.

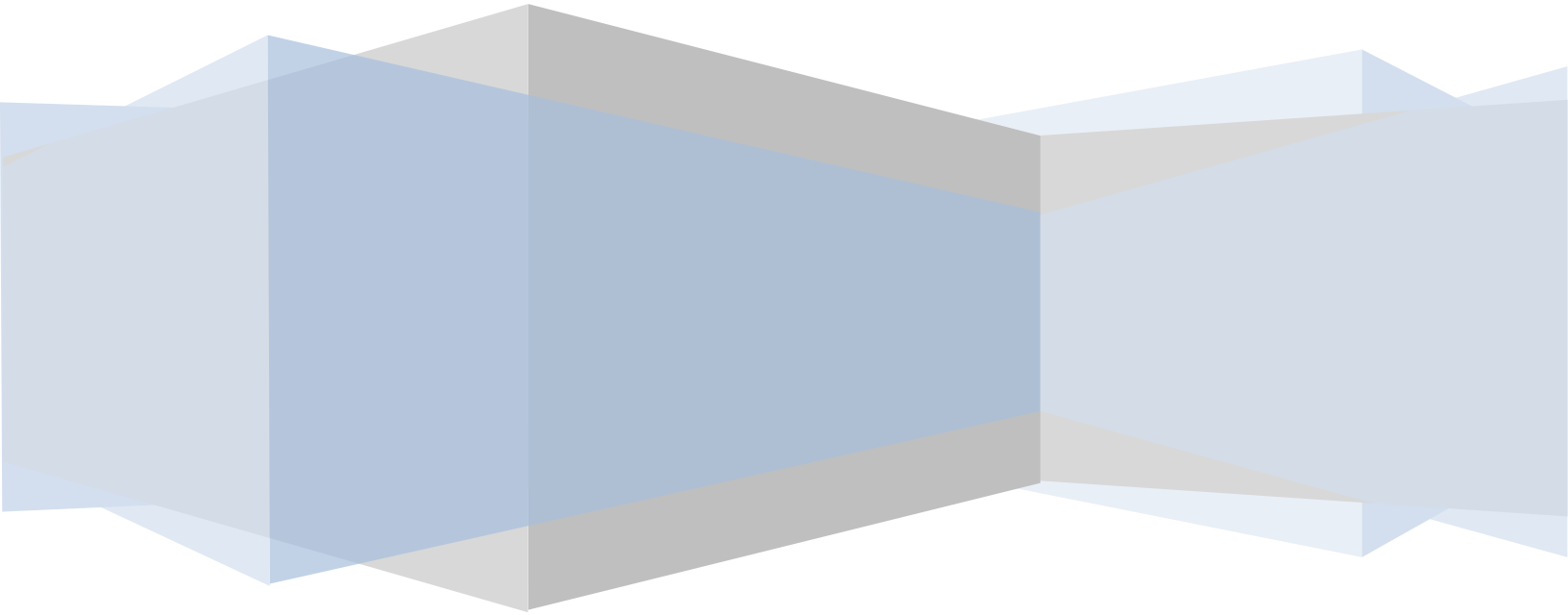
Nota: Debido a que el Anexo 1 es un documento generado para otra institución la edición del mismo está restringida y el formato difiere del presentado en este informe.

CSI / UNAM-CERT

Active Directory Rights Management Services

Implementación

Ricardo Andrés Carmona Domínguez



Contenido

Introducción

La coordinación de Seguridad de la Información genera material didáctico que es distribuido en formato digital a los diferentes participantes. Los asistentes a los cursos pueden tener cualquier procedencia (dentro o fuera de la UNAM, particulares, iniciativa privada). Sin embargo, actualmente no se cuenta con una infraestructura que permita lidiar de manera efectiva y centralizada las acciones sobre el material, como copiar, imprimir, visualizar, editar, entre otros.

Active Directory Rights Management Services (AD RMS) es un rol que puede ser instalado en un servidor Windows y que permite administrar permisos a archivos de manera individual, a través de plantillas, y que facilita la restricción de usos (copiar, imprimir, visualizar, editar) que se les dan a estos.

El proyecto tiene como finalidad implementar AD RMS para la distribución y restricción de permisos en el material desarrollado por la CSI, que permita centralizarlo, y al mismo tiempo, que siga permitiendo a los usuarios la lectura de su material, sin que sea difundido o distribuido a terceros no autorizados.

Objetivo del Proyecto

Proteger el uso de material generado por la CSI, utilizando la herramienta Rights Management Services (RMS) como plataforma de Data Leak Protection (DLP).

Descripción del Proyecto

Se generó una infraestructura que permite asegurar archivos creados por la CSI, independientemente de donde se encuentren estos.

1. CREACIÓN DE SERVICIOS EN MICROSOFT AZURE

Windows Azure permite la creación de redes virtuales las cuales pueden utilizarse para permitir la comunicación de un conjunto de máquinas virtuales creadas en la plataforma. El proceso de creación es sencillo, lo que facilitará al administrador de la cuenta en Azure la creación de redes y subredes en diferentes segmentos de direcciones IP privadas.

1.1 Cuenta de almacenamiento

Una cuenta de almacenamiento es el espacio en el cual los servicios tales como máquinas virtuales, sitios web y bases de datos se encontrarán alojados. Antes de la creación de alguno de estos servicios es recomendable, más no forzoso, crear el servicio de almacenamiento.

1) Dar clic en el símbolo **"+"** del menú inferior del sitio de administración de Azure.

2) Seleccionar **"Data Services"** > **"Storage"** > **"Quick Create"**.

3) Asignar un nombre al servicio de almacenamiento y elegir la ubicación de preferencia, dejando la replicación "Geográficamente redundante".

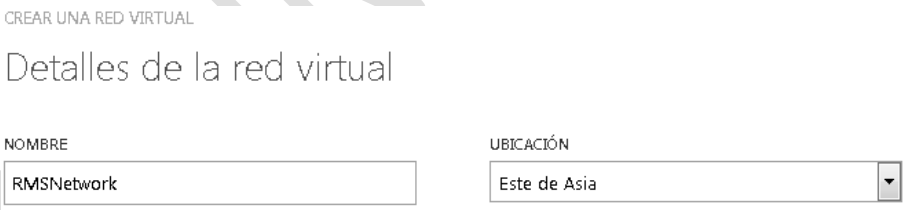
1.2 Red Virtual

Las redes virtuales permiten la comunicación directa entre equipos virtuales. Su creación implica la selección de un segmento de direcciones IP privado en el cual se podrán especificar diversas subredes y números de host variables.

1) Dar clic en el símbolo **"+"** (Nuevo) del menú inferior del sitio de administración de Azure.

2) Seleccionar **"Servicios de Red"** > **"Red Virtual"** > **"Creación Personalizada"**.

3) En la pantalla que se muestra, indicar el nombre de la red y la ubicación.



4) Dar clic en la flecha de la esquina inferior derecha para pasar a la siguiente parte de la configuración. En caso de requerirse, indicar los servidores DNS y la configuración de la VPN, si no serán utilizados dejar los valores por defecto.

5) En la siguiente ventana elegir el segmento de direcciones IP privado y el número de direcciones que se piensa utilizar. A su vez, se pueden crear subredes dentro del segmento elegido.

6) Finalizar dando clic en el símbolo **"✓"**. Verificar que la red se haya creado de forma correcta.

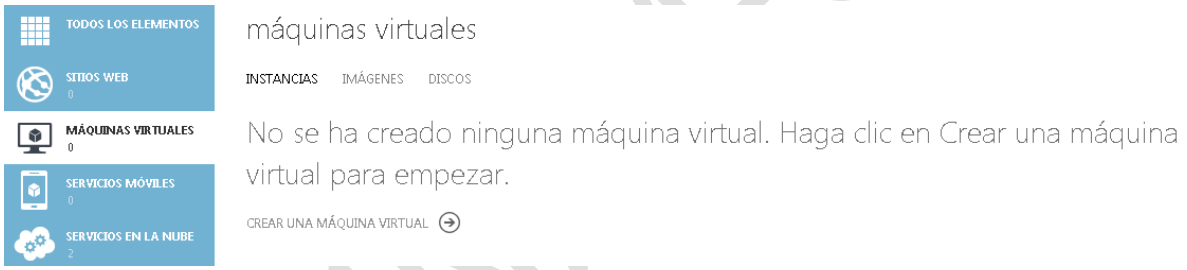
1.3 Máquinas virtuales

Windows Azure permite la creación de máquinas virtuales que se ejecutarán como un servicio en la nube, permitiendo su administración mediante conexión a escritorio remoto. Para que dos máquinas virtuales creadas en Windows Azure tengan comunicación entre sí es necesario que se encuentren conectadas a la misma red virtual. La creación personalizada de máquinas virtuales permite seleccionar la red virtual y la cuenta de almacenamiento asociadas a la máquina, por lo que es recomendable la creación de estos dos servicios antes de crear cualquier máquina virtual.

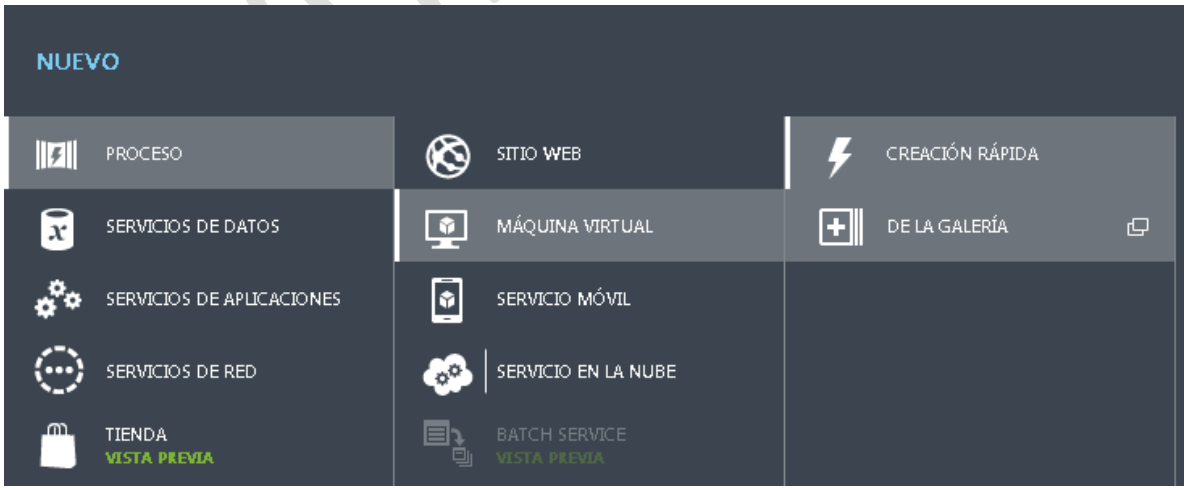
Es necesario crear dos máquinas virtuales:

- SQL Server 2012 SP2 Standard: Con la configuración del dominio, la CA raíz y de la base de datos SQL.
- Windows 2012 R2 Datacenter: Con la configuración del RMS y el IIS.

1) En el menú del lado izquierdo dar clic en **"Máquinas Virtuales"** y en **"Crear una máquina virtual"**.



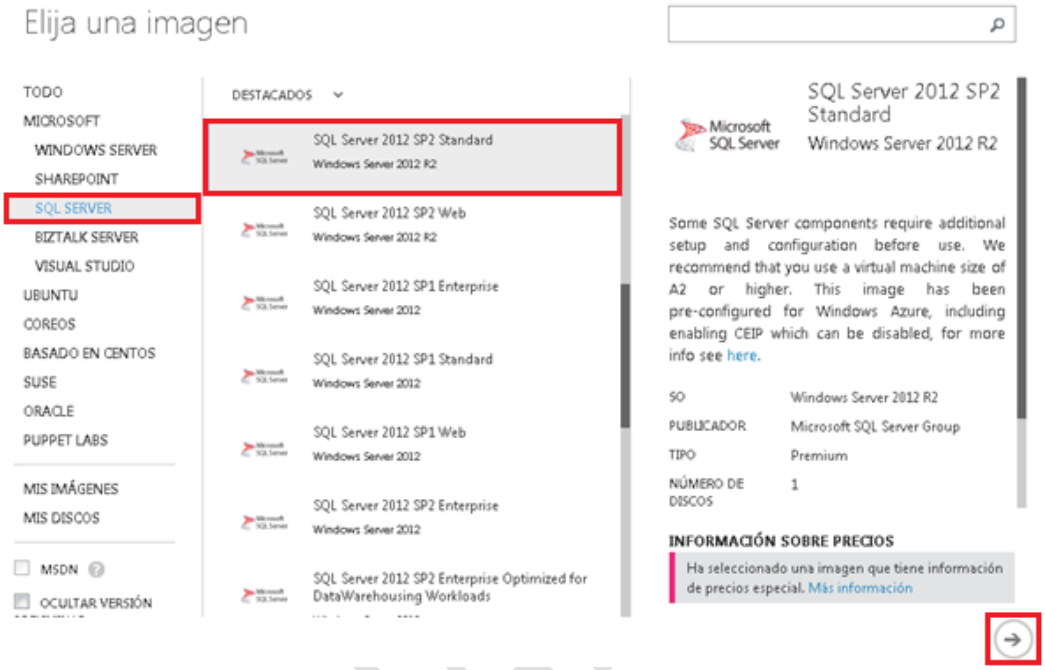
2) Del menú que se despliega seleccionar **"Proceso"** > **"Máquina virtual"** > **"De la galería"**.



3) En la ventana que se muestra, seleccionar la imagen del sistema operativo que se desee instalar en la máquina virtual.

- **Creación de la máquina virtual para el servidor SQL**

4) En el menú de imágenes, que se encuentra del lado izquierdo, seleccionar **"SQL Server"** y **"SQL Server 2012 SP2 Standard"**. Presionar la flecha en la esquina inferior derecha para continuar con el proceso de creación de la máquina virtual.



5) En la siguiente sección llenar los campos con los valores solicitados. Es importante recordar el usuario y la contraseña ya que será la cuenta que nos dará acceso a la máquina virtual.

6) En la siguiente sección indicar el nombre del servicio en la nube, el cual proporcionará una URL que será utilizada para realizar la conexión a la máquina virtual vía escritorio remoto. Se debe seleccionar la creación de un nuevo servicio en la nube e indicar un nombre disponible. Si el nombre elegido está en uso, el asistente de Azure nos lo indicará con una marca roja.

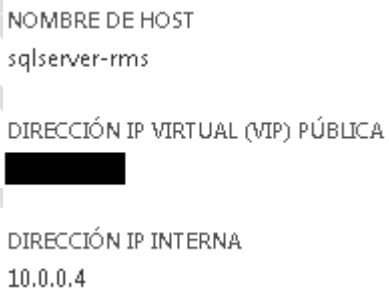
7) En la lista de Región/Grupo de Afinidad/Red Virtual se debe seleccionar la red virtual a la cual la maquina estará conectada. En caso de que no se desee conectar la maquina a una red virtual se debe escoger una región.

8) Al escoger una red virtual, se debe elegir alguna de las subredes creadas dentro de la red elegida.

9) Seleccionar la cuenta de almacenamiento donde se alojará la máquina virtual.

10) En la siguiente sección, verificar que se encuentre seleccionada la opción de instalación del agente de máquina virtual. Dar clic en el símbolo **"✓"** y esperar a que la máquina se cree y se encuentre en ejecución, esto puede tardar varios minutos.

11) Al ingresar a la sección de administración de la máquina virtual se puede ver la dirección IP de la red virtual asociada que le fue asignada a la máquina.



- **Creación de la máquina virtual para el servidor RMS**

1) Dar clic en el símbolo **"+"** del menú inferior del sitio de administración de Azure.

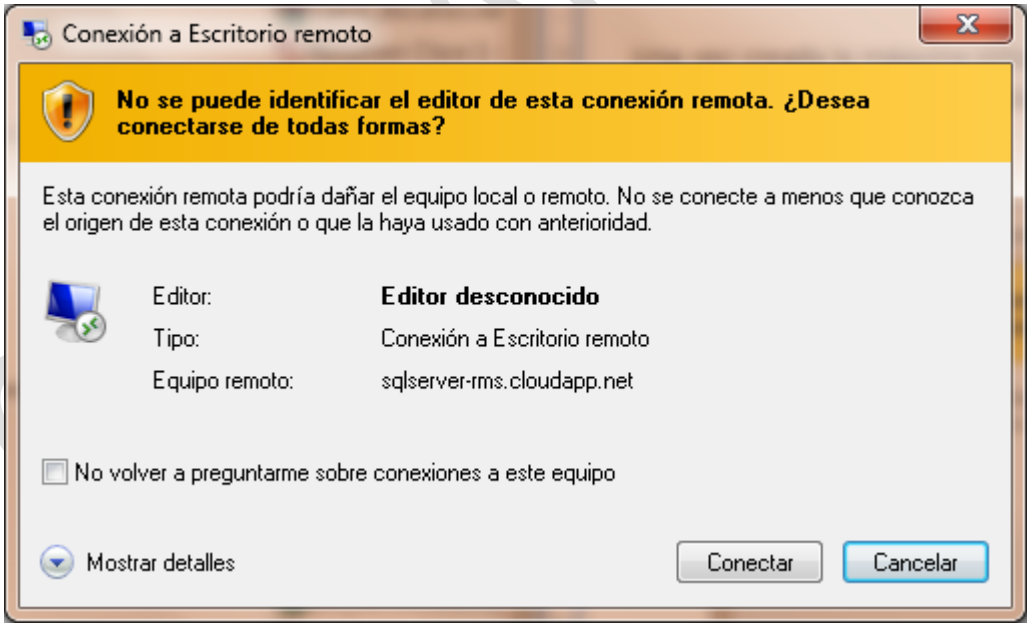
2) Seleccionar **"Proceso"** > **"Virtual Machine"** > **"Custom Create"**.

3) En el menú de imágenes, que se encuentra del lado izquierdo, seleccionar **"Windows 2012 R2 Datacenter"**. Presionar la flecha en la esquina inferior derecha para continuar con el proceso de creación de la máquina virtual.

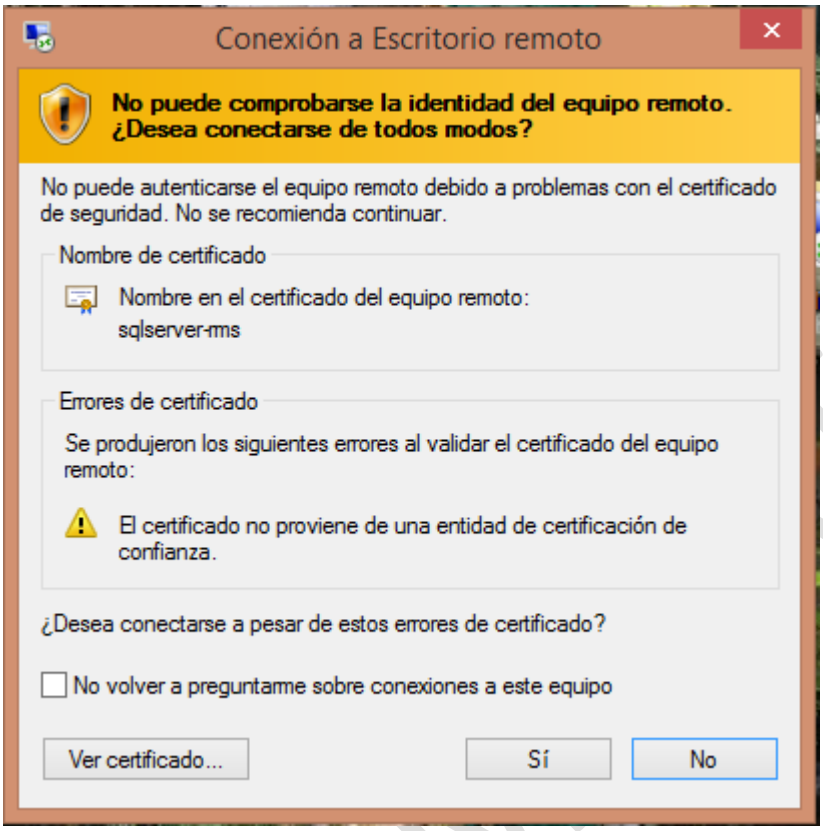
4) Seguir los pasos 5 al 10 de la sección anterior. Tomar en cuenta que, para que puedan comunicarse, las máquinas virtuales deben estar en la misma red virtual.

- **Conexión a las máquinas virtuales por escritorio remoto**

Una vez creada la máquina virtual se puede acceder a ella por medio del archivo con extensión "rdp" que se descarga dando clic en la opción **"Conectar"**, localizada en el área inferior izquierda del panel de Microsoft Azure.

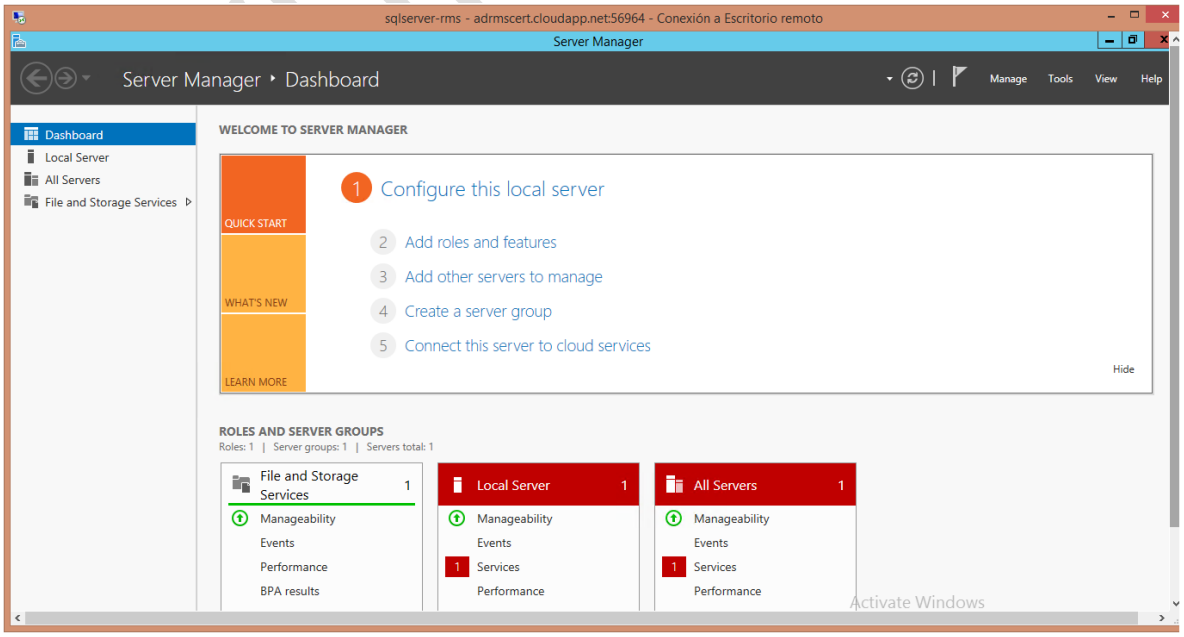


Al dar doble clic en el archivo .rdp descargado, se muestra una ventana como la que se muestra a continuación. Dar clic en el botón **"Si"**.



La conexión con el escritorio remoto debe hacerse utilizando el usuario y el dominio separados por una arroba "@", por ejemplo: rdccert@rmscert.local.

Ya se tiene acceso a la máquina virtual con SQL Server 2012 SP2 Standard instalado.

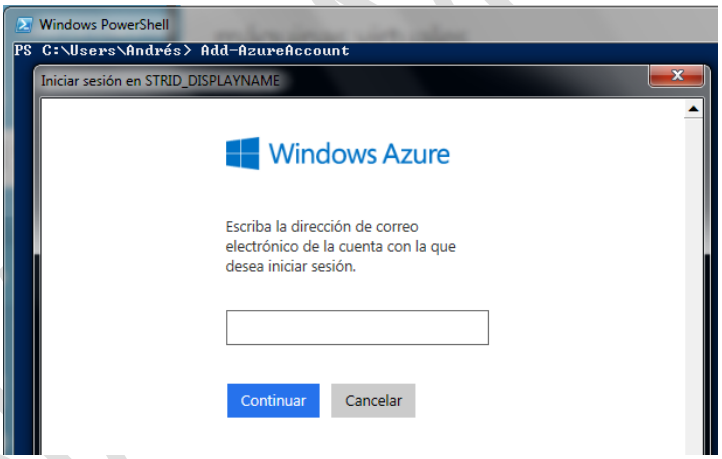


- **Establecer IP estática para las máquinas virtuales del proyecto**

Debido a que se requiere utilizar una máquina virtual en la que se implementará un dominio con Active Directory, es necesario establecer una IP estática en esa máquina ya que, de no hacerlo, al momento de reiniciar la máquina la plataforma de Microsoft Azure podría asignarle una IP diferente a la configurada para el dominio, ocasionando fallas de comunicación entre servicios y equipos.

Azure permite asignar direcciones IP estáticas a las máquinas virtuales mediante PowerShell, cabe destacar que estas direcciones no son realmente estáticas, es decir, Azure hace uso de un DHCP para asignar direcciones a las máquinas dentro de una VNet. Con PowerShell es posible hacer solicitud para que la máquina virtual obtenga siempre la misma dirección IP. Cabe destacar que esto no es una reservación, asignar una IP estática de una VNET a una máquina virtual asegura que Azure tratará de asignar la IP indicada a la máquina pero no es una garantía de que esto ocurra siempre.

Para la asignación es necesario contar con Azure PowerShell, disponible para su descarga en el siguiente enlace: http://go.microsoft.com/fwlink/p/?linkid=320376&clcid=0x409. Una vez instalado se debe añadir la cuenta en donde están alojadas nuestras máquinas virtuales.



Teniendo la cuenta agregada a PowerShell, debemos ejecutar el siguiente comando:

```
PS C:\Users\Andrés> Get-AzureVM -ServiceName sqlserver-rms -Name sqlserver-rms | Set-AzureStaticVNetIP -IPAddress 10.0.0.4
| Update-AzureVM

OperationDescription                OperationId                          OperationStatus
--------------------                -----------                          ---------------
Update-AzureVM                      c26583a6-30ab-5d47-b2b8-6686ea13b559 Succeeded
```

Donde:

- ServiceName: Nombre del Cloud Service donde está almacenada la máquina virtual.
- Name: Nombre de la máquina virtual.
- IPAddress: Dirección IPv4 que se desea asignar a la máquina virtual.
- Update-AzureVM: Reinicia el servicio de la máquina virtual para aplicar los cambios hechos.

2. INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS EN EL SERVIDOR SQL

2.1 Active Directory

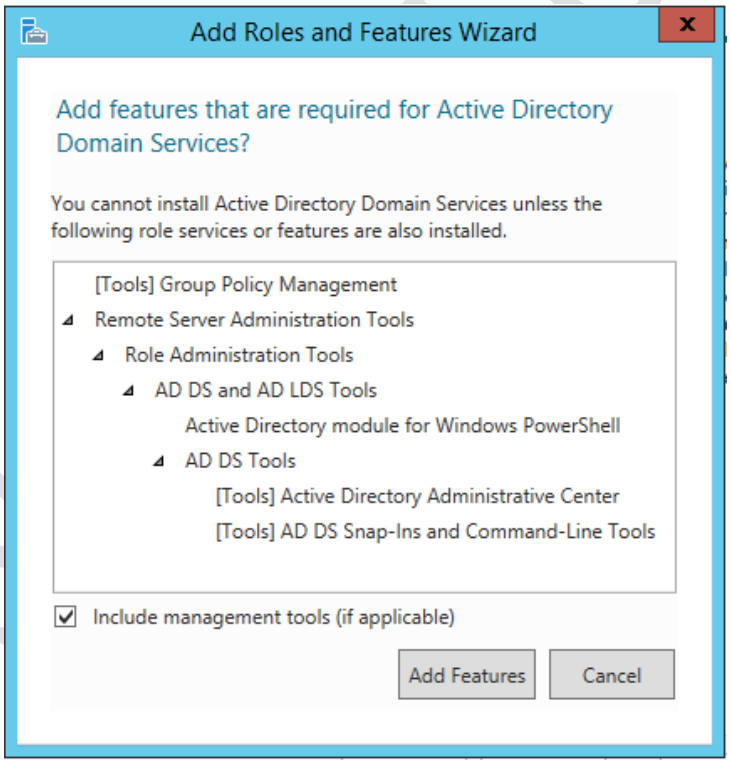
- **Instalación del servicio de dominio de Active Directory**

La instalación de la característica Active Directory Domain Services se puede hacer de dos formas:

- Dando clic a **"Add roles and features"** en el menú de inicio rápido del panel.
- Dando clic en **"Manage"**, que se localiza en la esquina superior derecha del panel, y eligiendo **"Add roles and features"**.

En la ventana del asistente **"Add roles and features"** seleccionar las siguientes opciones:

- Role-based or feature-based installation
- Select a server from the server pool
- Active Directory Domain Services

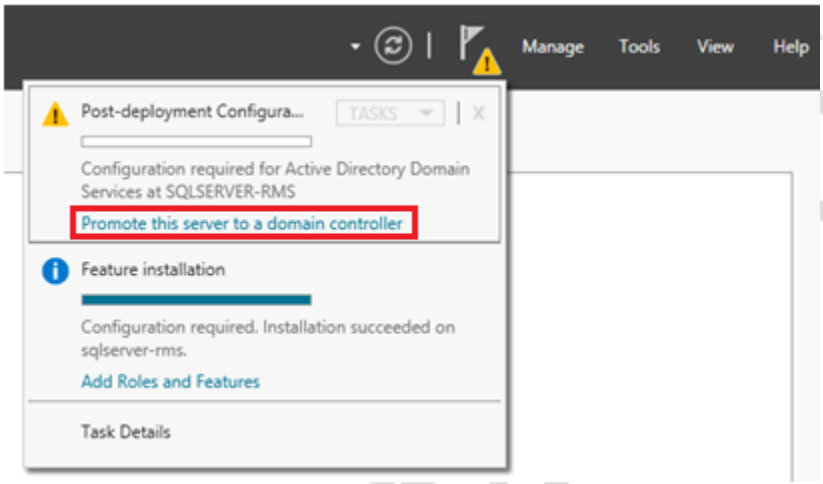


Dar clic en el botón **"Add Features"**. Para terminar con la instalación dar clic en el botón **"Install"** que se encuentra el final del asistente.

- **Configuración del servicio de dominio de Active Directory**

Una vez que se haya instalado el rol de Active Directory, dar clic en el ícono de bandera que se encuentra en la esquina superior derecha. El signo de precaución indica que aún falta configurar el servicio.

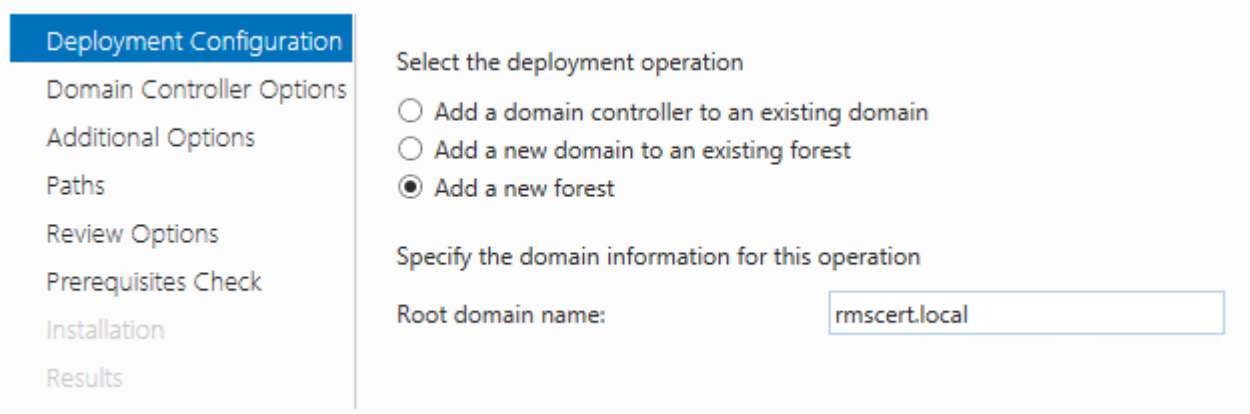
1) Dar clic en **"Promote this server to a domain controller"**.



2) En el asistente de configuración seleccionar las siguientes opciones de configuración:

Domain Controller Options

Forest functional level: Windows Server 2012 R2
Domain functional level: Windows Server 2012 R2
Marcar las casillas de "Domain Name System (DNS) server" y Global "Catalog (GC)".
Establecer una contraseña segura.



3) Dejar las opciones restantes sin modificar y, después de pasar la validación de los prerrequisitos, presionar el botón **"Install"**. La instalación se habrá completado después de reiniciar el equipo.

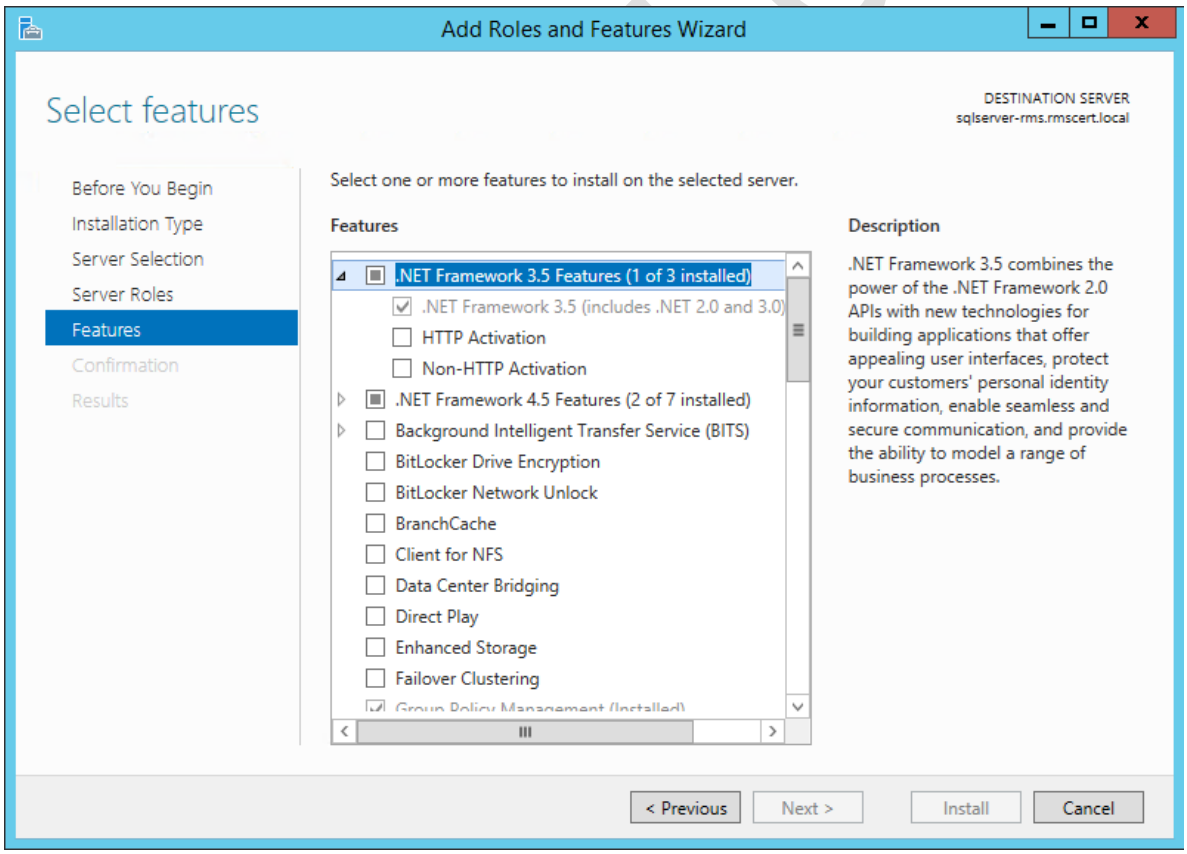
2.2 Verificación de instalación de .NET Framework 3.5

SQL Server 2012 requiere que estén instaladas las características de .NET Framework 3.5. SQL Server 2012 SP2 Standard ya tiene instalado .NET Framework 3.5; sin embargo, una forma de comprobar esto es haciendo uso de PowerShell:

```
PS C:\Users\adadmin> Get-WindowsFeature * | where name -like *Framework*

Display Name                                            Name                    Install State
------------                                            ----                    -------------
    [ ] .NET Framework 4.5                              AS-NET-Framework            Available
[X] .NET Framework 3.5 Features                         NET-Framework-Features      Installed
    [X] .NET Framework 3.5 (includes .NET 2.0 and 3.0)  NET-Framework-Core          Installed
[X] .NET Framework 4.5 Features                         NET-Framework-45-Fea...     Installed
    [X] .NET Framework 4.5                              NET-Framework-45-Core       Installed
    [ ] ASP.NET 4.5                                     NET-Framework-45-ASPNET     Available
[ ] Windows Biometric Framework                         Biometric-Framework         Available
```

O bien, haciendo uso del server manager, verificando que la característica esté marcada. Si aparece marcada la característica **".NET Framework 3.5 Features"** significa que ya está instalada, de lo contrario se debe marcar y continuar en el asistente dando clic en el botón **"Install"**.

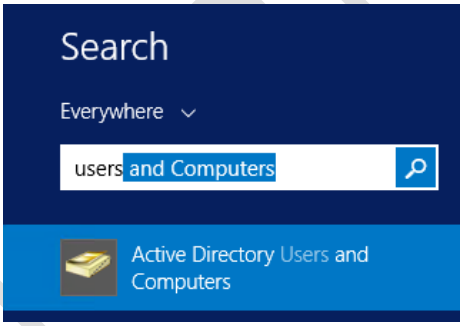


2.3 Permitir conexiones remotas utilizando políticas de grupo

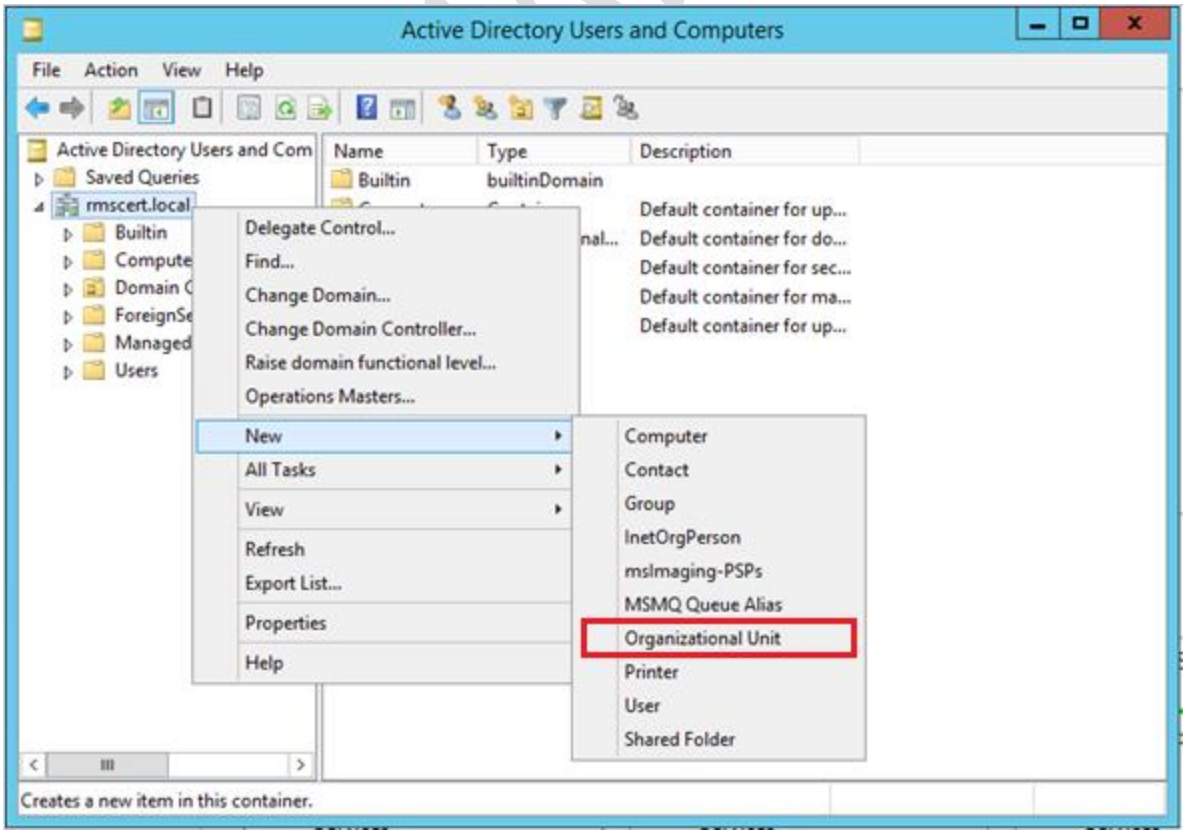
Puesto que los dos servidores empleados son remotos, se debe configurar el servicio de escritorio remoto para facilitar su manejo, limitando el acceso de los usuarios para garantizar la seguridad de los servidores. Esto se hace utilizando políticas de grupo [1], como se explica a continuación.

- **Creación del grupo de seguridad para usuarios de escritorio remoto**

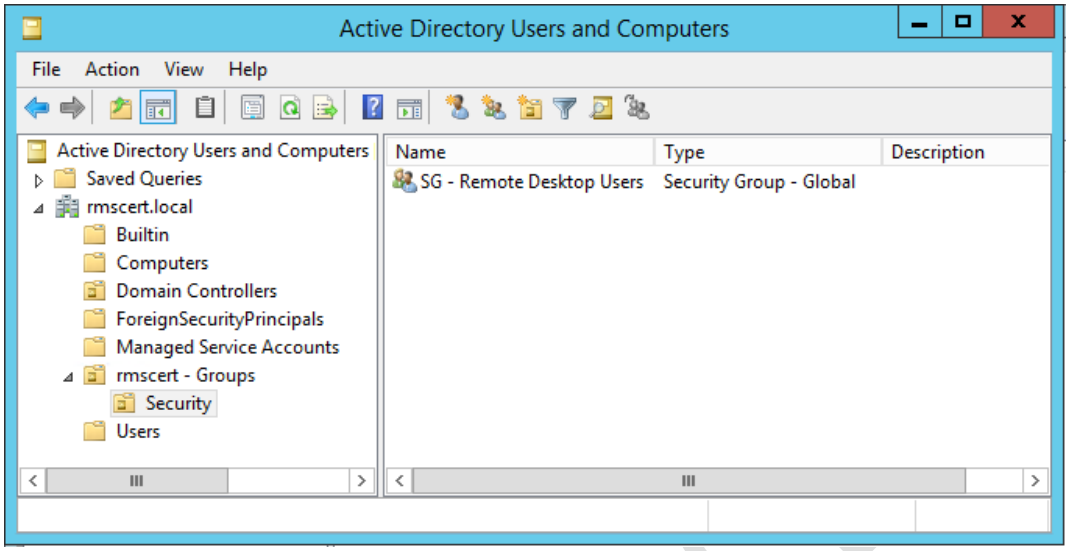
Dar clic en el botón de inicio, que se encuentra en la esquina inferior izquierda, buscar y abrir la aplicación **"Active Directory Users and Computers"**.



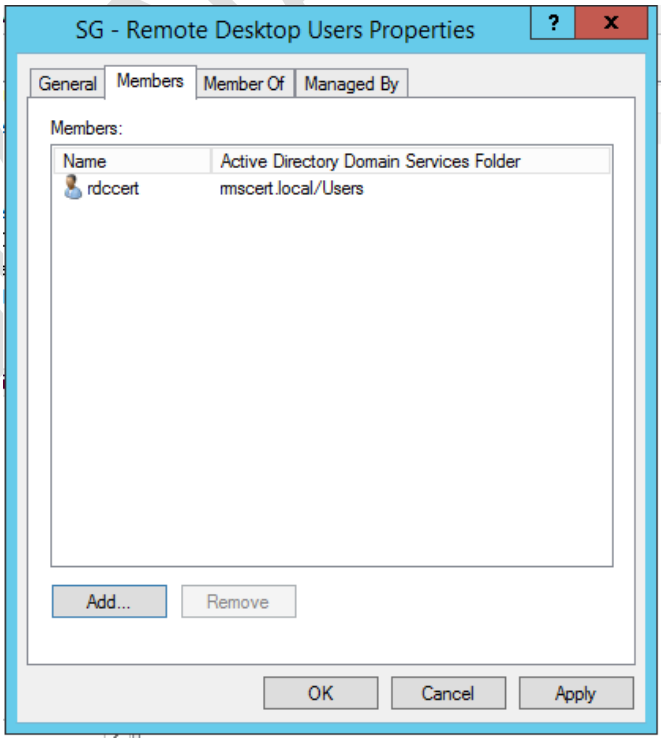
Dar clic derecho sobre el nombre del dominio, seleccionar **"New"** y **"Organizational Unit"** para crear una unidad organizacional llamada "<Nombre_del_Dominio> - Groups".



Dentro de ésta, crear otra unidad organizacional llamada **"Security"** y dentro crear un grupo llamado **"Remote Desktop Users"**, con alcance (scope) **"Global"** y de tipo (type) **"Security"**.

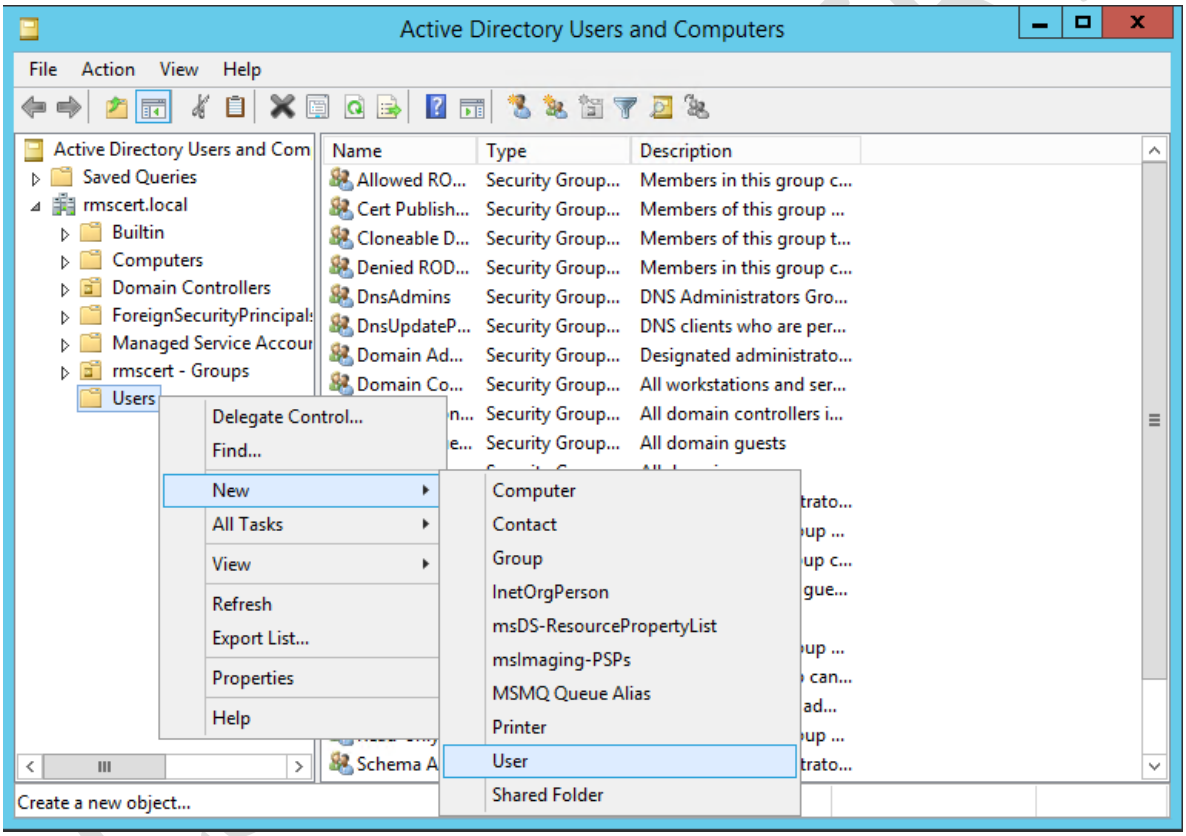


Es importante añadir el nombre de al menos un usuario administrador para que sea posible seguir accediendo al servidor por medio del servicio de Escritorio Remoto. Dar doble clic al nombre del grupo de seguridad y seleccionar la pestaña **"Members"** en la ventana que se abre. Dar clic en el botón **"Add…"**, escribir el nombre del usuario y presionar el botón **"Check Names"** para comprobar el nombre del usuario. Dar clic en el botón "OK" de ambas ventanas para guardar los cambios.



Posteriormente crear un usuario para iniciar sesión en el servidor RMS una vez que éste se haya unido al dominio. Dar clic derecho en **"Users"**, seleccionar **"New"** y **"User"**. Asignar un nombre (first name) y un nombre de inicio de sesión (user logon name) y presionar el botón **"Next"**. Escribir una contraseña para el usuario. Las otras opciones se dejan a su consideración; en este manual se optó por desmarcar la casilla **"User must change password at next logon"**, para que el servidor no solicite cambiar la contraseña del usuario después de iniciar sesión por primera vez, y marcar la casilla **"Password never expires"**, para que la contraseña que se le asigne al usuario al momento de ser creado no expire. Volver a presionar el botón **"Next"** y por último dar clic en **"Finish"**.

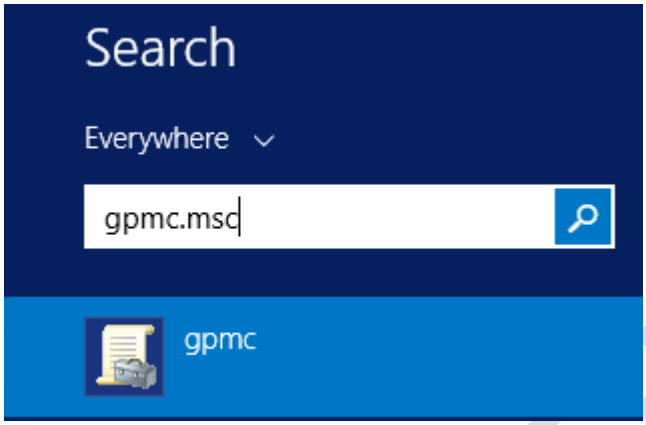
Añadir este usuario al grupo **"Domain Admins"** para poder instalar y configurar AD RMS en el servidor.



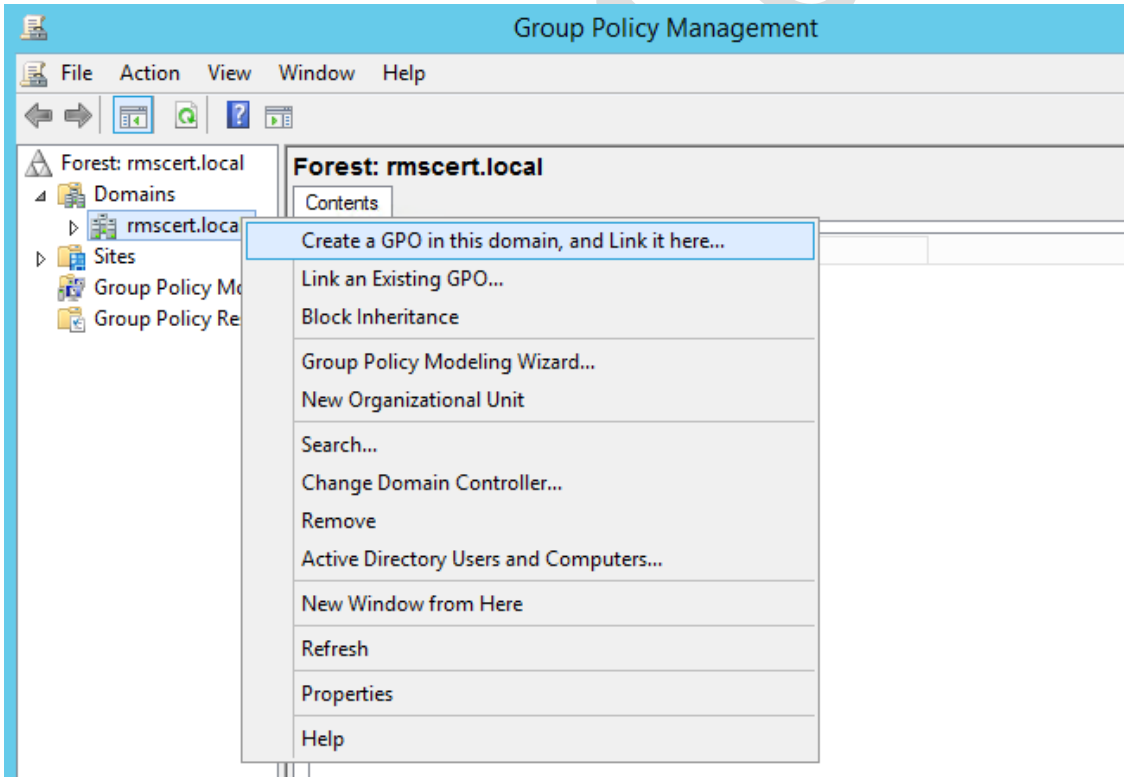
- **Creación de GPO (Group Policy Object)**

Una vez creado el grupo de seguridad, se debe habilitar el Protocolo de Escritorio Remoto (RDP, por sus siglas en inglés) y añadir sólo a los usuarios que deben tener permiso de conectarse al servidor.

En la pantalla de inicio escribir gpmc.msc y, una vez encontrado, abrir la Consola de Administración de Directivas de Grupo (GPMC, por sus siglas en inglés).

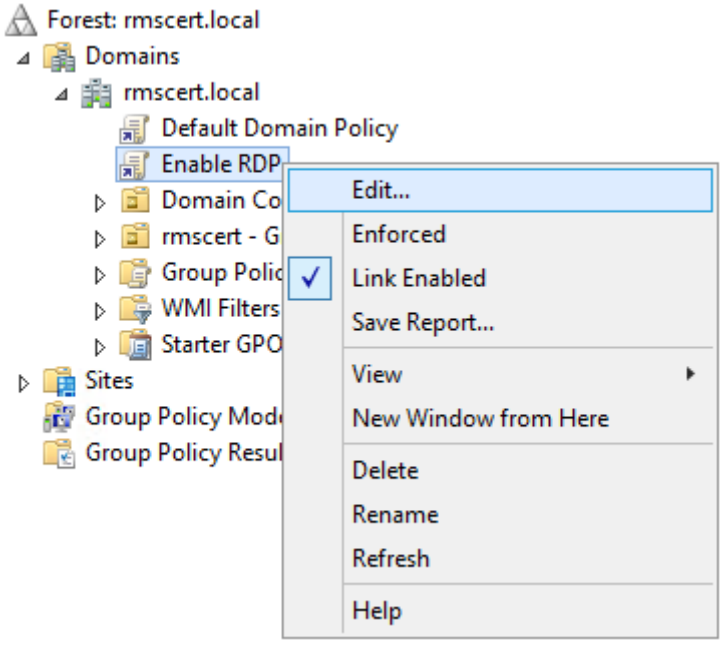


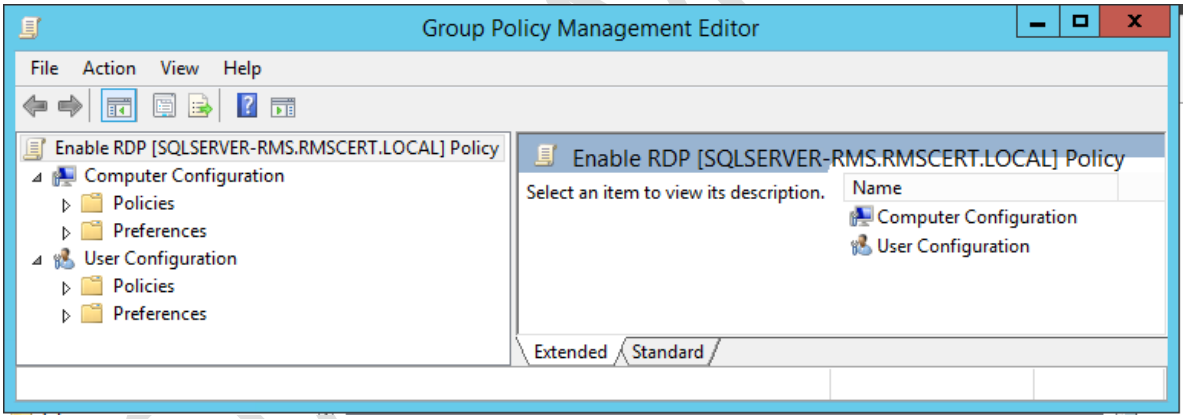
En la ventana de GPMC, dar doble clic en el nombre del bosque (forest), desplegar el campo de dominios, dar clic derecho en el nombre del dominio y seleccionar **"Create a GPO in this domain, and Link it here…"**.



Al crear el objeto de directiva de grupo (GPO, por sus siglas en inglés) en la raíz del dominio para tenga efecto en todos los equipos que se encuentren unidos al dominio. Nombrar la política, en este caso el nombre es **"Enable RDP"**, y dar clic en **"OK"**.

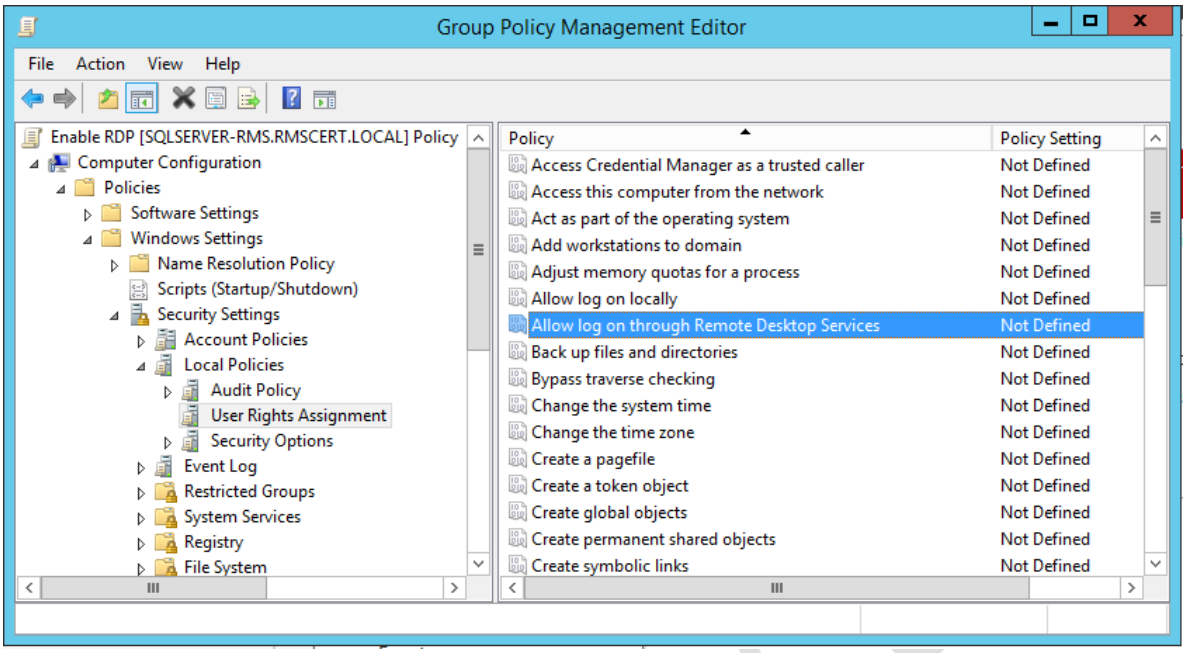
Al principio la política está vacía, para personalizarla se debe dar clic derecho sobre su nombre y seleccionar la opción **"Edit…"**, esto abrirá la ventana del Editor de Políticas de Grupo.



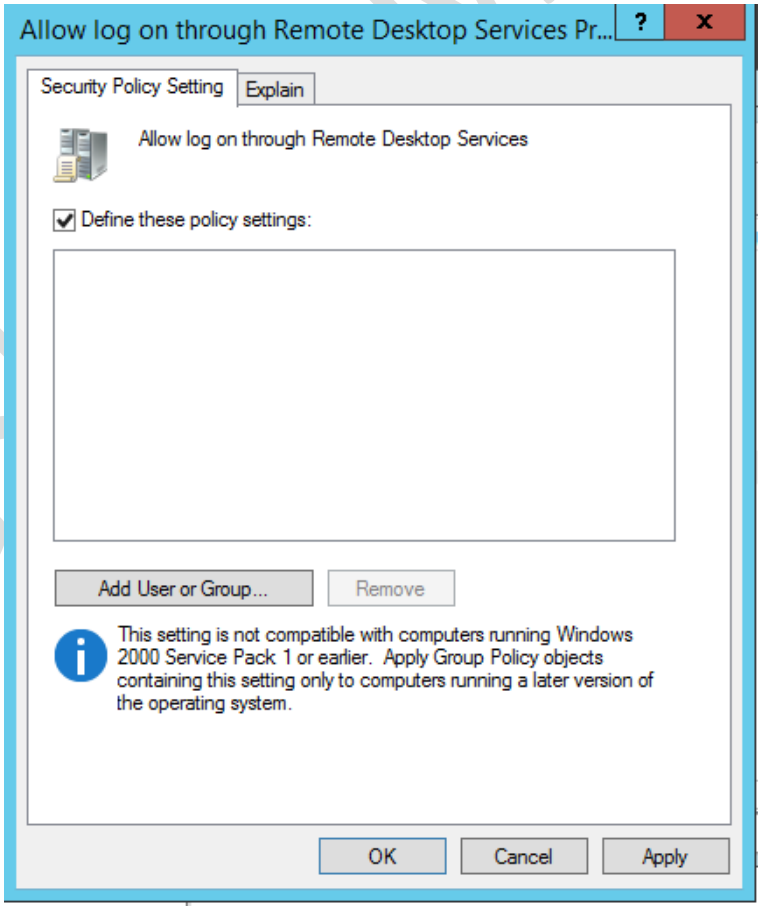


En la ventana del Editor de Políticas de Grupo modificar la configuración de la computadora para habilitar RDP, abrir el Firewall y añadir usuarios al grupo de seguridad siguiendo los pasos descritos a continuación:

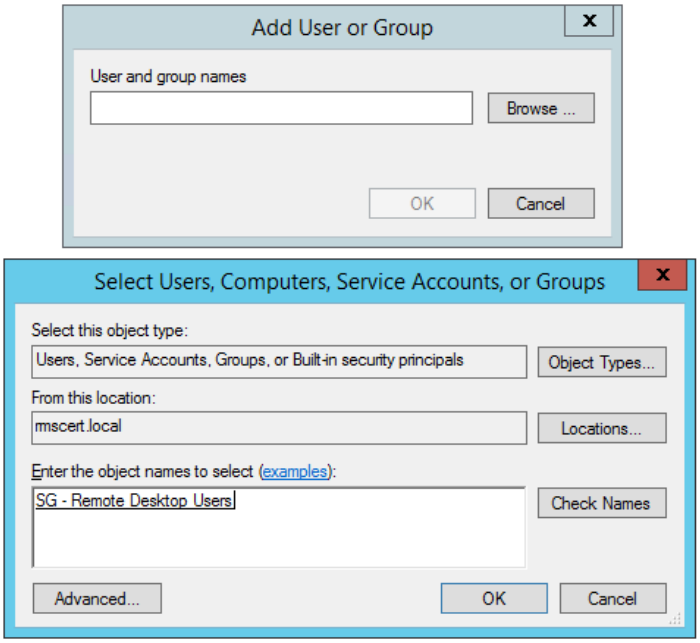
1) Habilitar RDP. Desplegar las opciones del editor de Políticas de Grupo en el siguiente orden: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment.



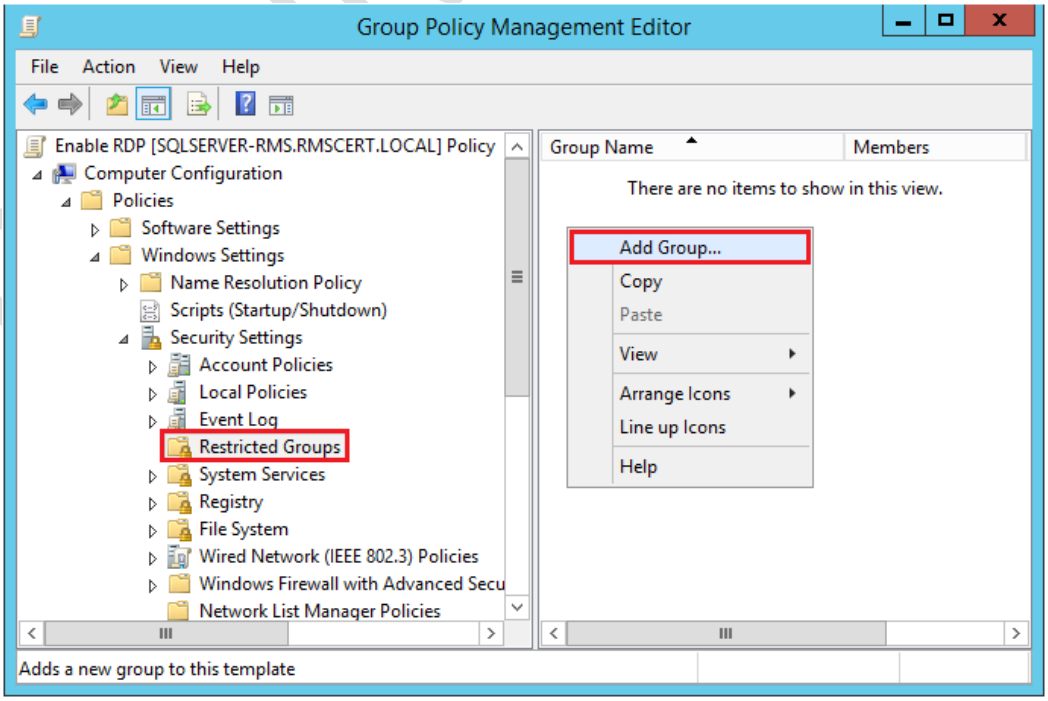
2) Seleccionar User Rights Assignment y, del lado derecho, dar doble clic en la política **"Allow log through Remote Desktop Services"**. En la ventana de la política, marcar la casilla **"Define these policy settings"** y dar clic en el botón **"Add user or group"**.



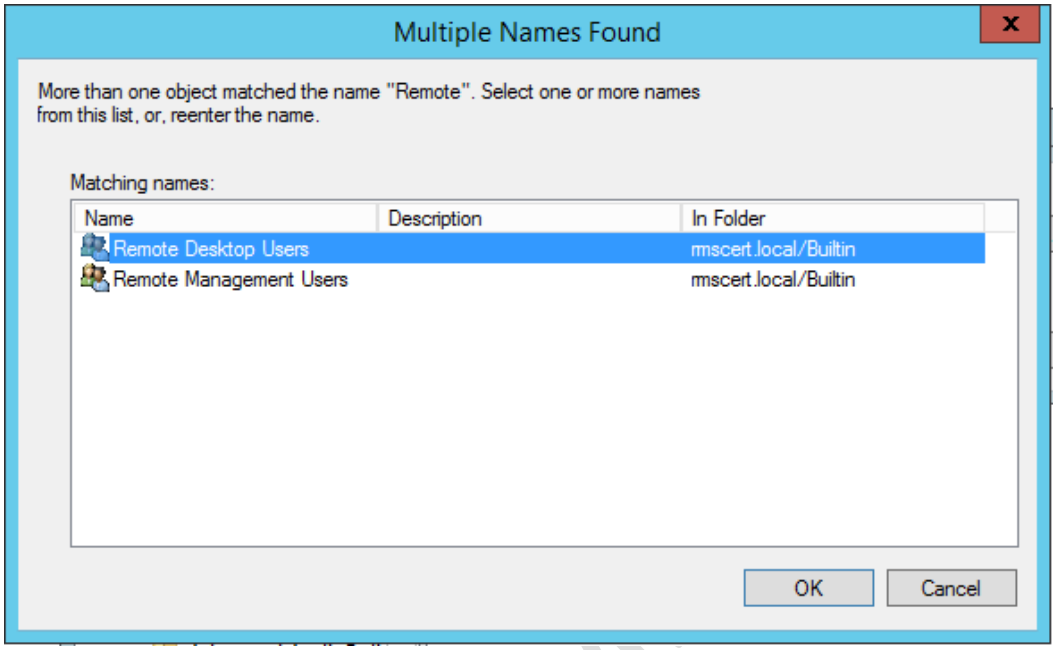
3) Dar clic en el botón **"Browse…"** y en la ventana que se abre escribir el nombre, o parte del nombre, del grupo de seguridad que se creó en el Active Directory. Si el nombre del grupo existe y fue escrito correctamente, se mostrará subrayado al presionar el botón **"Check Names"**. Presionar **"OK"** en las tres ventanas para cerrarlas y aplicar el cambio.



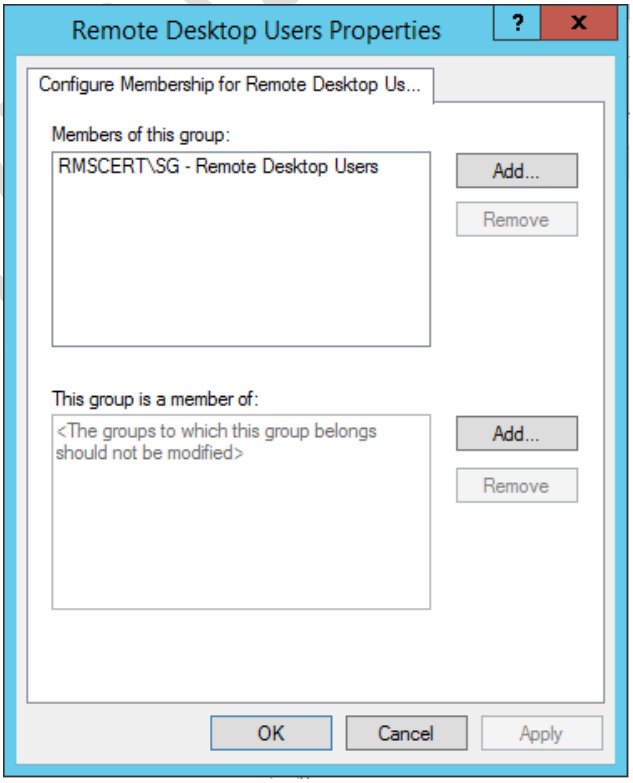
4) Modificar la política Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups, dando clic derecho en el espacio en blanco y seleccionando la opción **"Add Group"**.



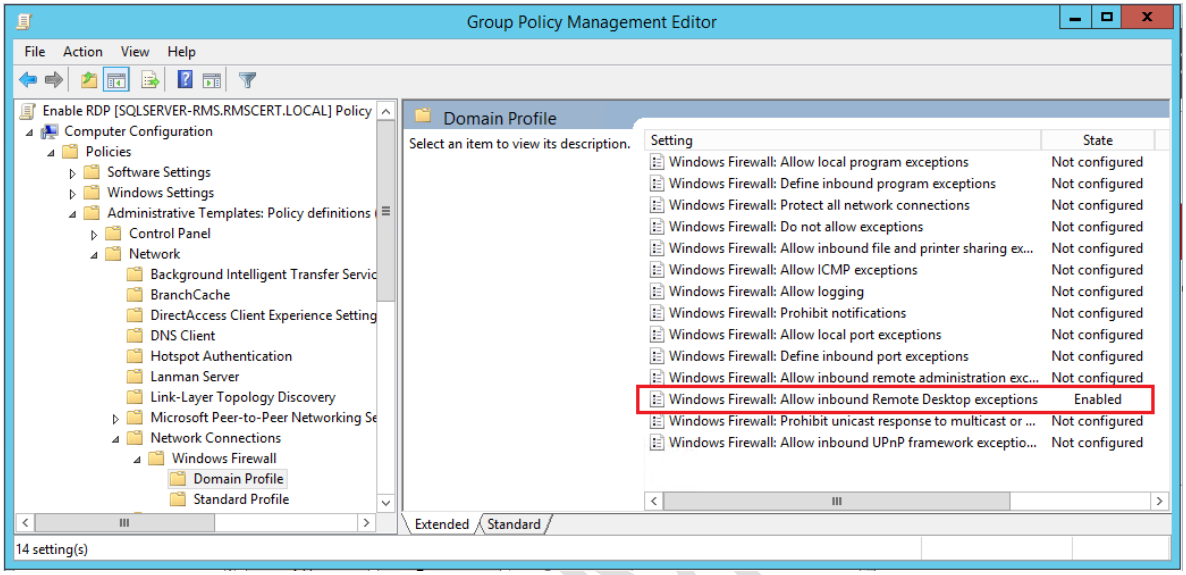
5) En la nueva ventana dar clic en el botón **"Browse…"**, buscar **"Remote Desktop Users"** como se vio en pasos anteriores y dar clic en el botón **"OK"** de las tres ventanas.



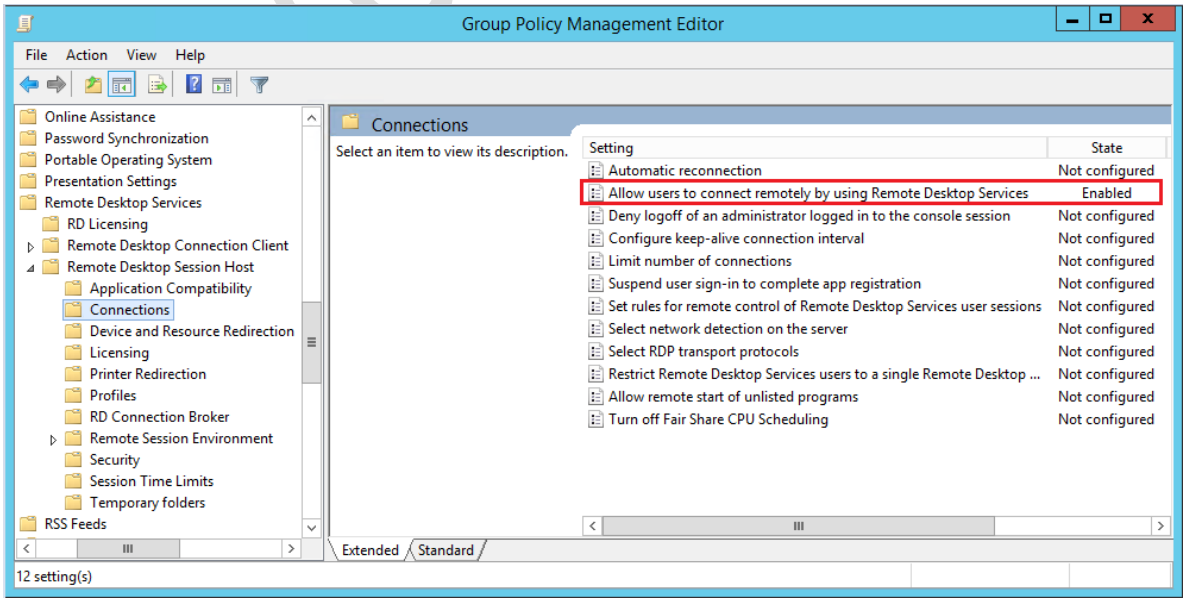
6) En la ventana "**Remote Desktop Users Properties"** que se abre al dar doble clic en el nombre del grupo, ir al área **"Members of this Group"** y dar clic en el botón **"Add…"**, seleccionar el grupo de seguridad y aplicar los cambios.



7) Habilitar la política Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Allow Inbound Remote Desktop exceptions, dando doble clic y seleccionando la opción "**Enabled"**. Esto permite que el servidor reciba conexiones de escritorio remoto, abriendo el puerto TCP 3389 en el Firewall de Windows.

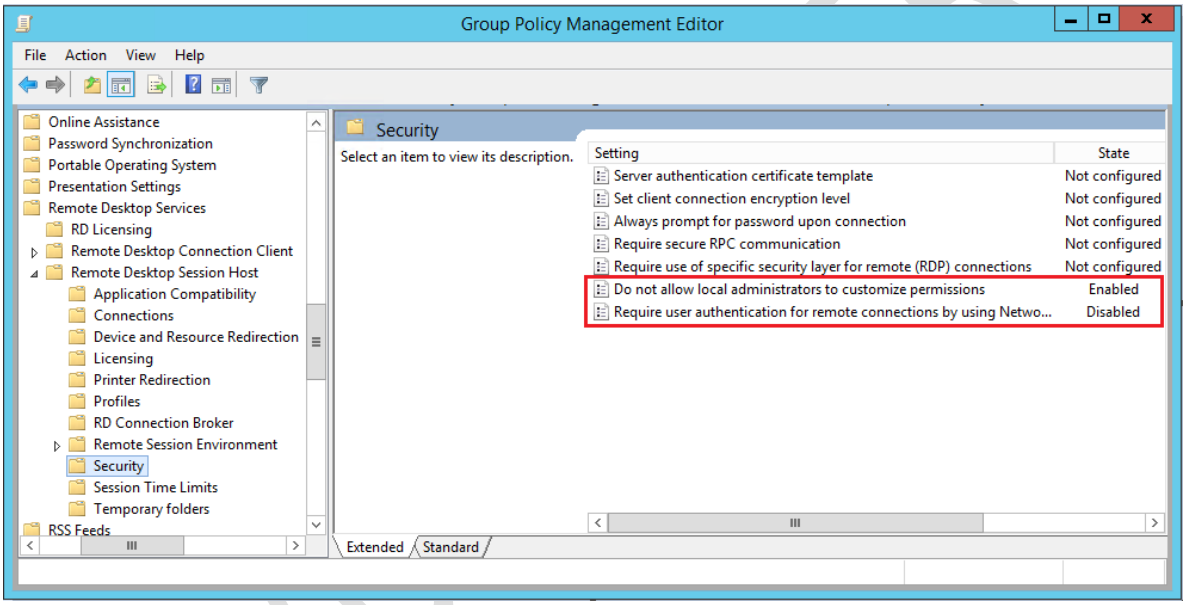


8) Habilitar la política Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Allow user to connect remotely by using Remote Desktop Services, dando doble clic y seleccionando la opción "**Enabled**". Esta política permite que los miembros del grupo **"Remote Desktop Users"** se puedan conectar de forma remota a otros equipos.



9) Habilitar la política Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Do not allow local administrators to customize permissions, dando doble clic y seleccionando la opción "**Enabled**". Esta política previene que los administradores locales modifiquen los permisos de seguridad relacionados con los grupos de usuarios que pueden conectarse remotamente.

10) Deshabilitar la política Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using NLA, dando doble clic y seleccionando la opción "**Disabled".** Esta configuración indica que no es necesaria la autenticación a nivel de red para las conexiones remotas, que es importante debido a que algunos sistemas operativos, como Windows 7 Home Premium, no soportan la autenticación a nivel de red.



2.4 Creación de usuarios

En la máquina virtual con Active Directory instalado, que en este caso es el servidor SQL crear los siguientes usuarios necesarios para la instalación de RMS [2]. Abrir **"Active Directory Users and Computers"**, desplegar las opciones del dominio, dar clic derecho en **"Users"** y seleccionar **"New"** > **"Users"**.

Nombre de Usuario	Cuenta de Usuario	Dirección E-mail	Grupo
ADRMSSRV Cuenta de Servicio RMS	ADRMSSRV		
ADRMSADMIN	ADRMSADMIN	adrmsadmin@rmscert.local	Enterprise Admins

Agregar al usuario **adrmsadmin** al grupo creado anteriormente para que pueda iniciar sesión mediante escritorio remoto en los equipos.

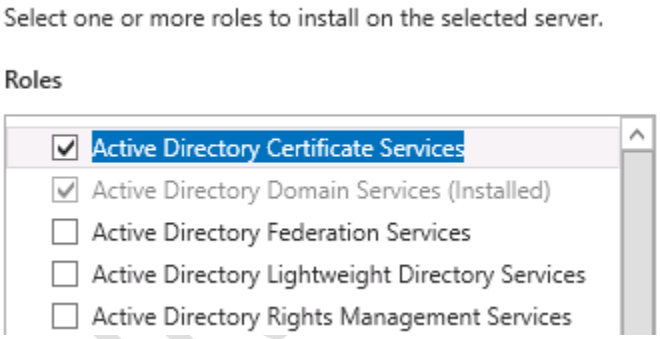
2.5 Autoridad Certificadora (Opcional)

Debido a que el sitio utilizado por RMS requiere el uso de un certificado para cifrar la comunicación, es preferible contar con una Autoridad Certificadora en el dominio. Se puede hacer uso de un certificado autofirmado o del certificado creado automáticamente por Azure para el equipo virtual, aunque esto es recomendado sólo para entornos de pruebas.

- **Instalación**

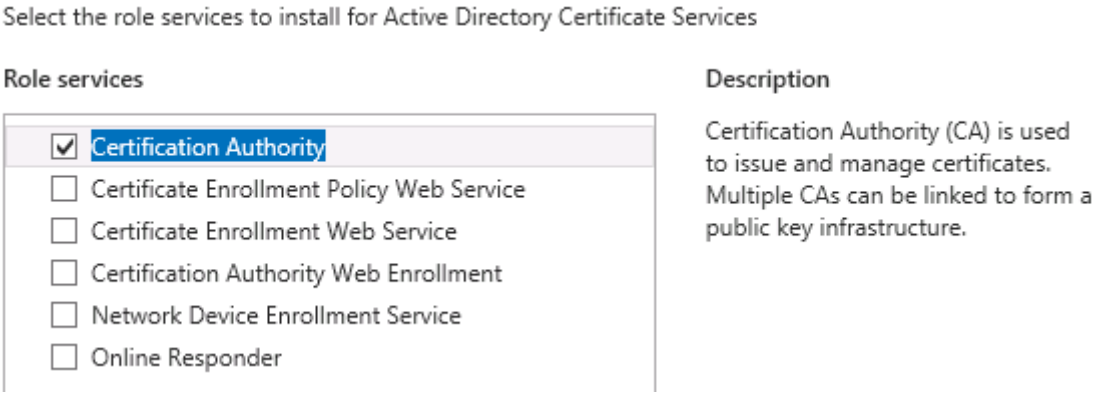
1) Iniciar sesión, con una cuenta de administrador, en el servidor donde se halla instalado Active Directory Domain Services.

2) En la ventana **"Server Manager"** dar clic en "**Add Roles and Features"**. Cuando el asistente se encuentre en **"Server Roles"**, seleccionar e instalar el rol para la Autoridad Certificadora: **"Active Directory Certificate Services"**.

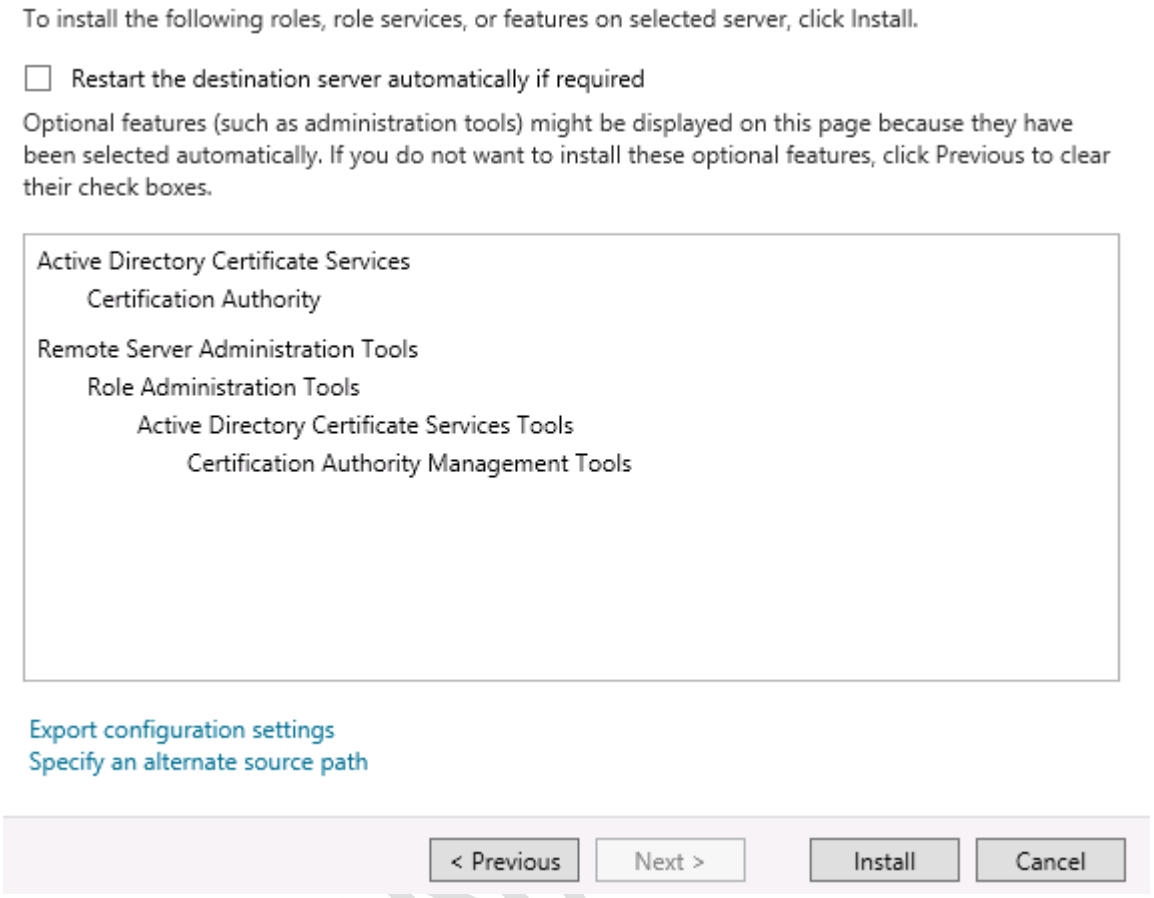


3) Avanzar en el asistente dando clic en **"Next"** hasta llegar a **"Role Services"**.

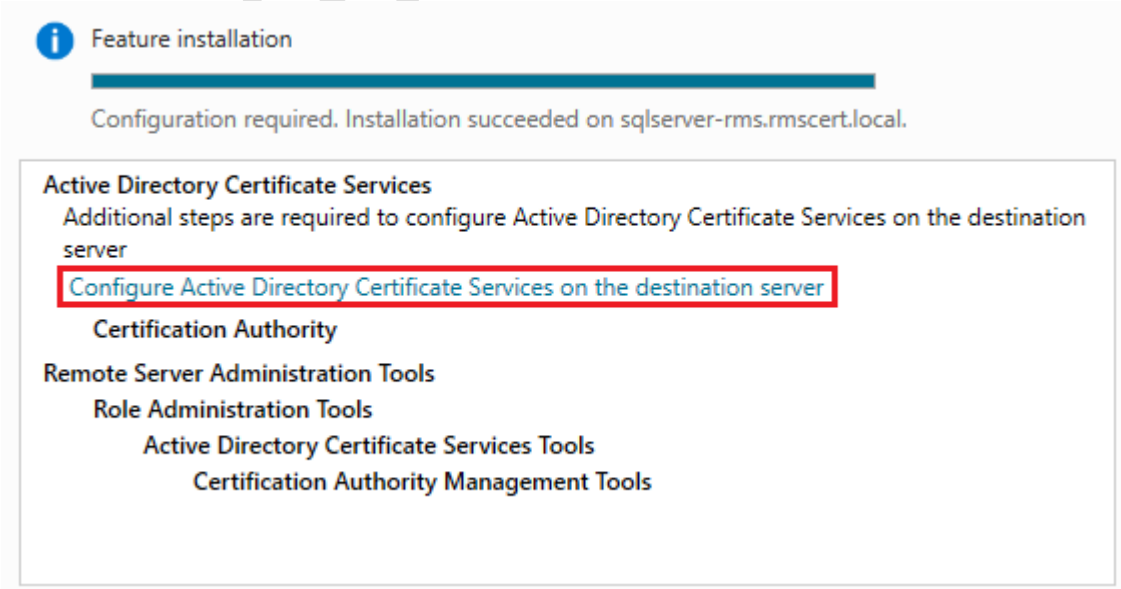
4) Verificar que se encuentre marcada la casilla **"Certification Authority"** y dar clic en **"Next"**.



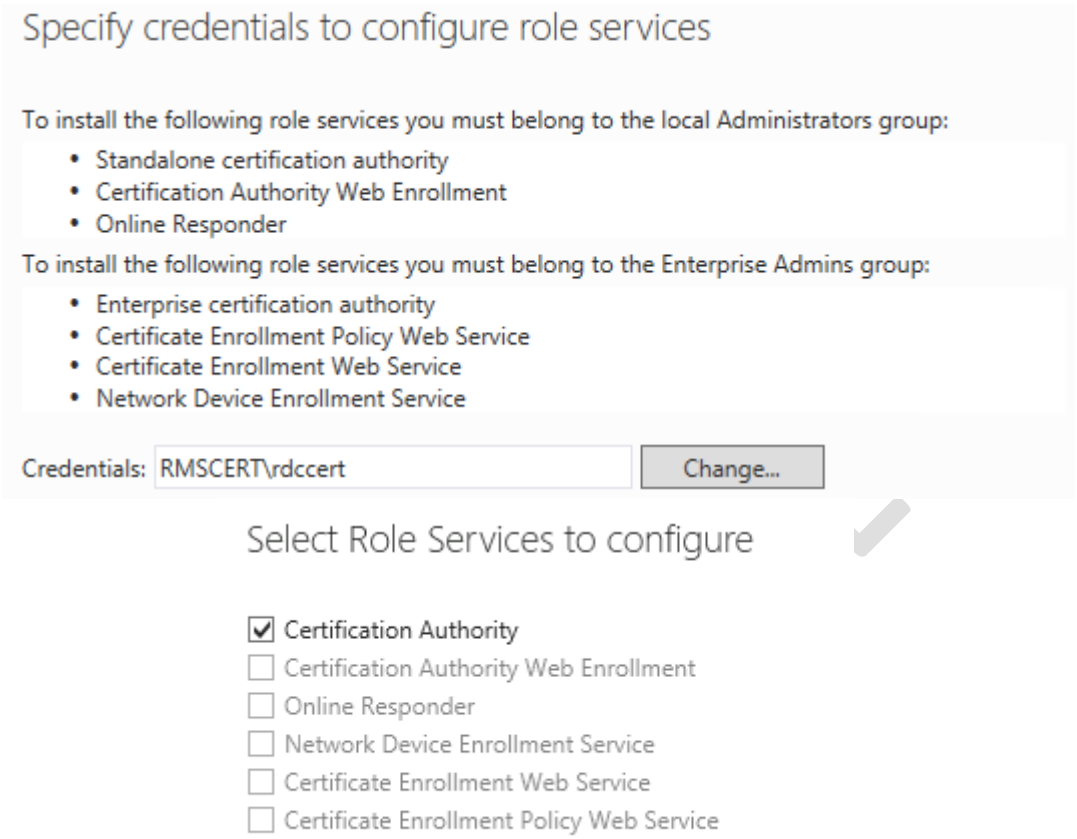
5) Si las características seleccionadas corresponden a las que se muestran en la siguiente imagen, dar clic en **"Install"**.



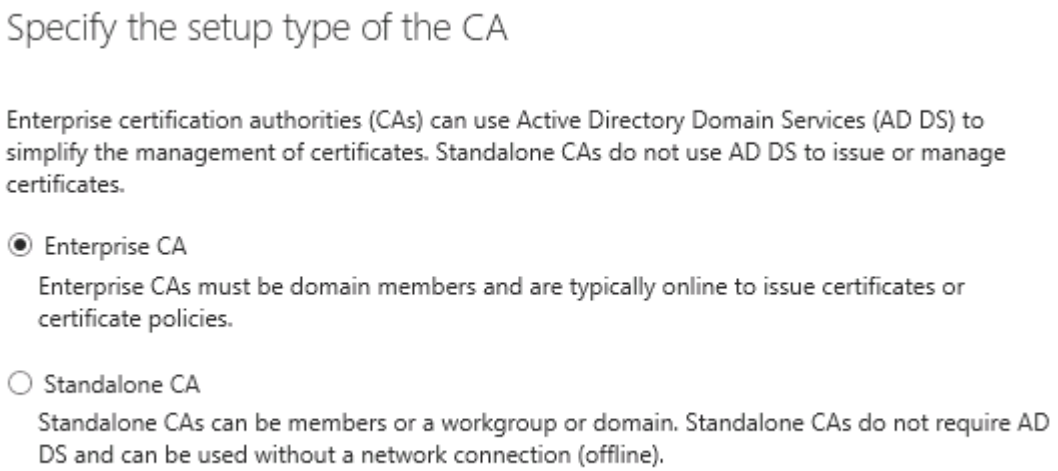
6) Una vez instalada esta característica, es necesario configurarla dando clic en el texto en color azul, señalado en la imagen:

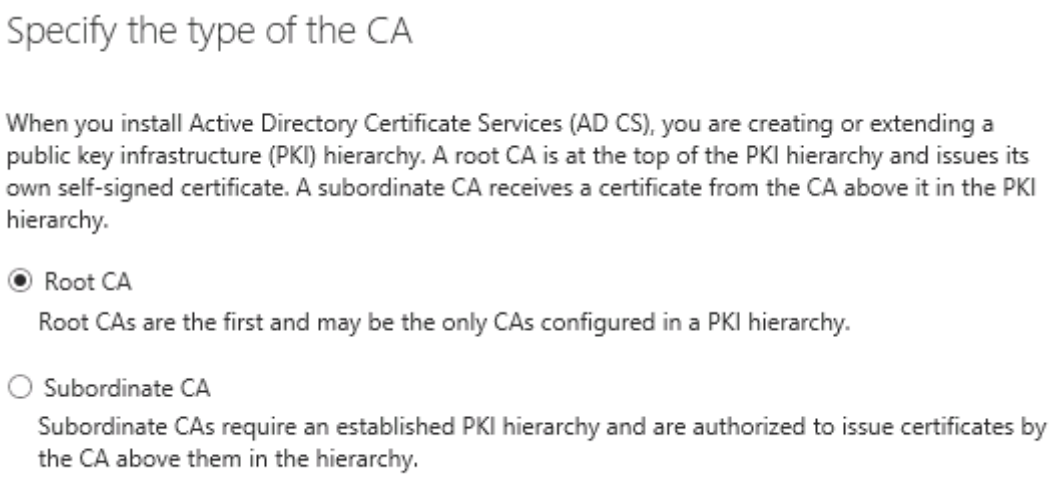


7) Puesto que únicamente se instaló el rol de Autoridad Certificadora, éste es el único que se podrá configurar después de especificar las credenciales del administrador del dominio.

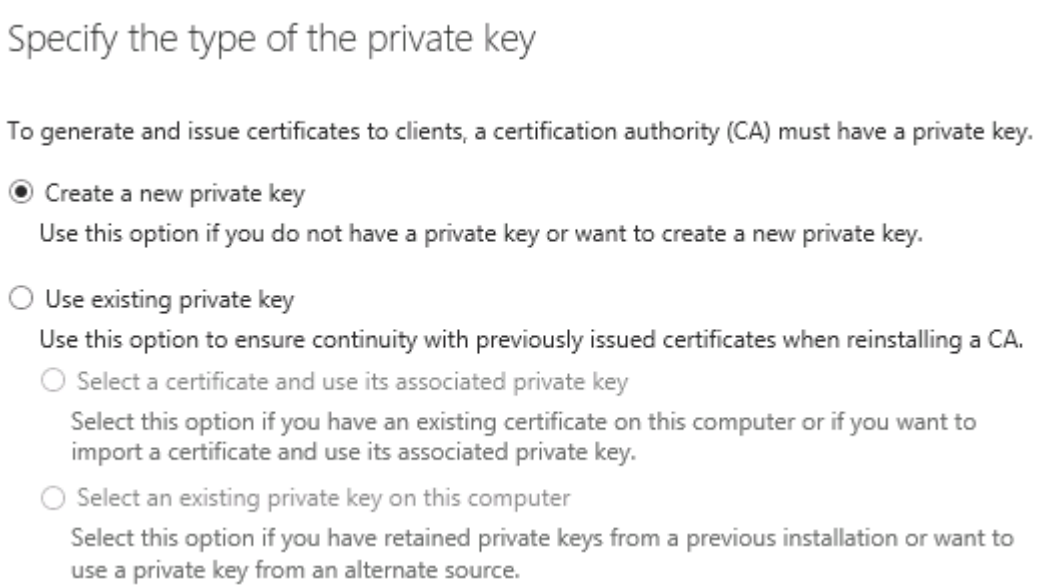


8) Para nuestro entorno contaremos con una CA Enterprise que será a su vez una CA raíz. Seleccionar las opciones **"Enterprise CA"** y **"Root CA"**.

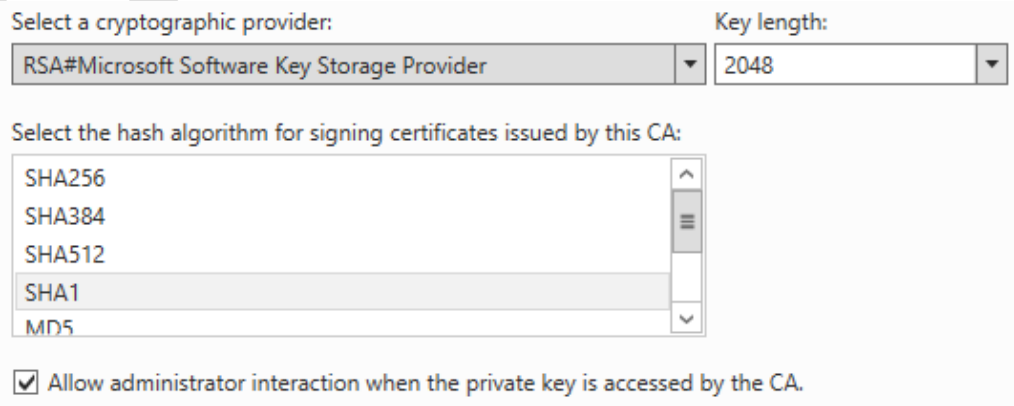




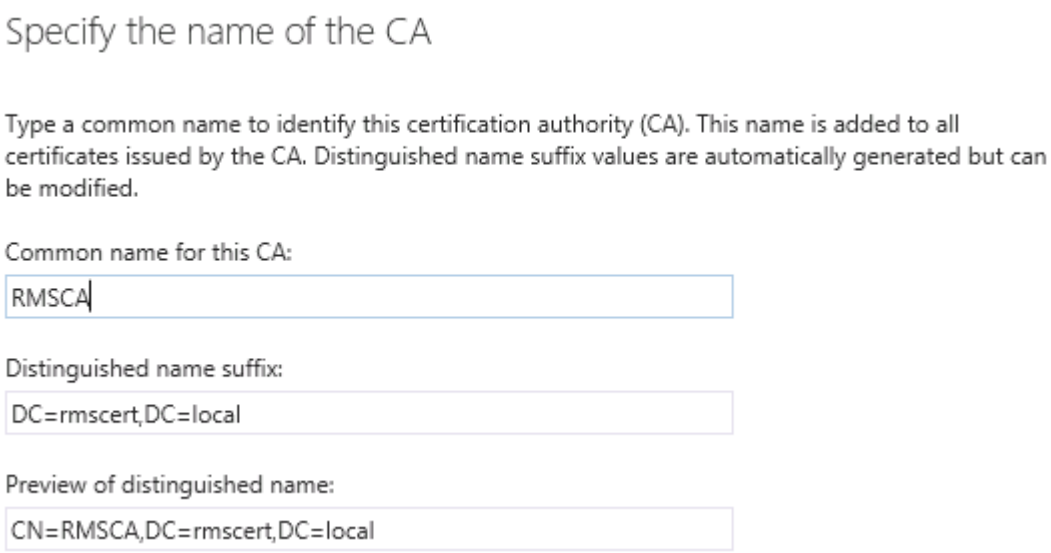
9) Se debe crear una nueva llave privada para la CA, seleccionar **"Create new private key"**.



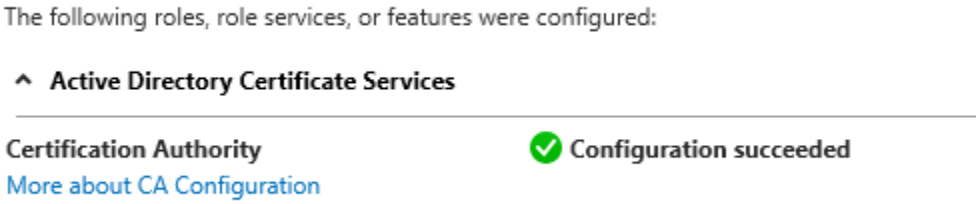
10) Elegir las opciones criptográficas convenientes y dar clic en **"Next"**. Durante el desarrollo de este manual se mantuvieron las opciones predeterminadas para la CA.



11) Configurar un nombre para que pueda ser vista en el dominio.



12) Dar clic en el botón **"Next"** hasta llegar al final del asistente. Dar clic en **"Configure"** para terminar la configuración.



2.6 Configuración de SQL Server

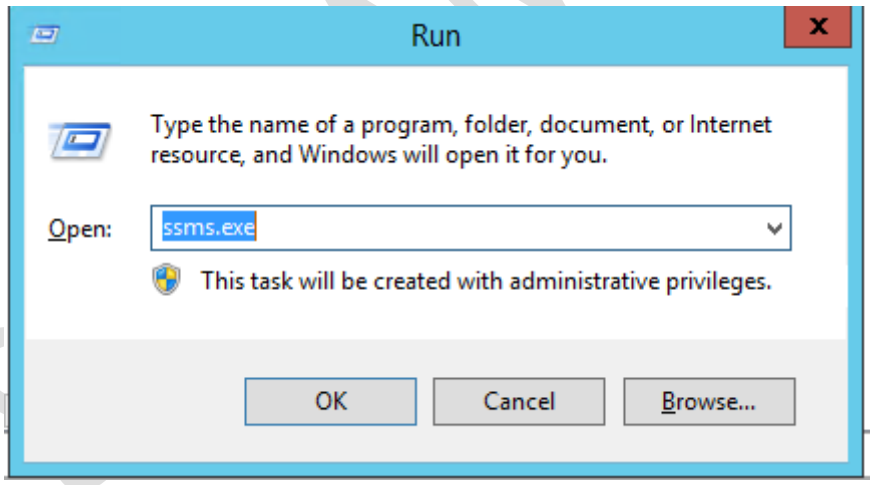
En los siguientes puntos se describen los pasos para realizar las modificaciones necesarias que permitan que AD RMS tenga acceso a SQL Server.

- **Añadir el usuario ADRMSADMIN como cuenta de inicio de sesión a SQL**

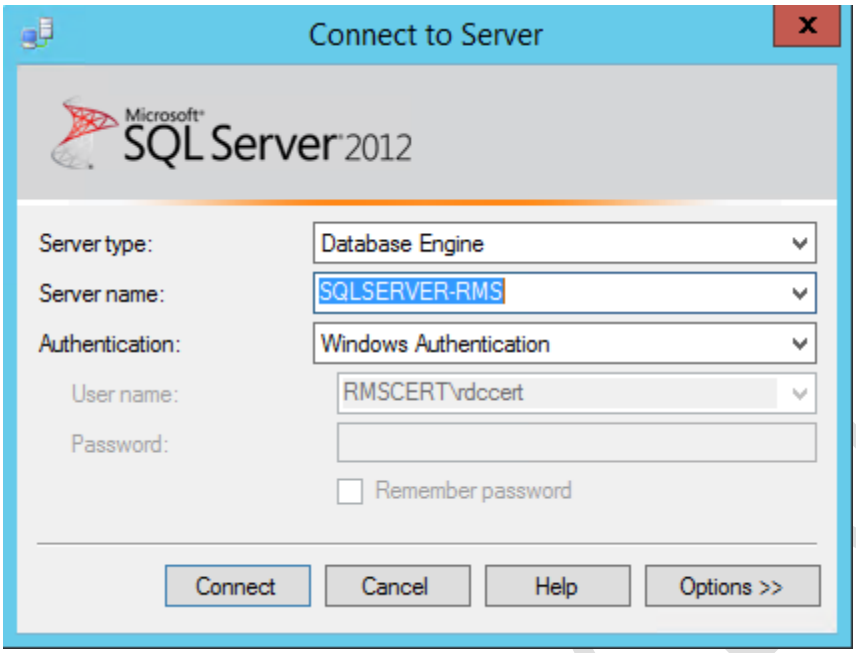
El primer paso es asignar permisos de administrador del sistema a la cuenta ADRMSADMIN en la instancia de SQL Server para poder crear las bases de datos necesarias durante la instalación de AD RMS.

1) En el servidor SQL iniciar sesión con una cuenta de administrador que esté en el dominio. En el menú inicio, escribir SQL Server y dar clic en el icono verde correspondiente a la figura:

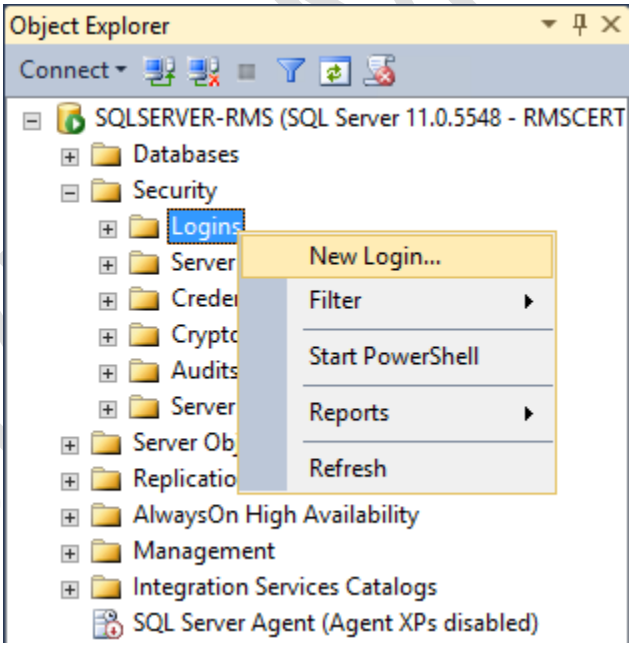
2) O bien, presionar la combinación de teclas **Win+R** y escribir **"ssms.exe"**.



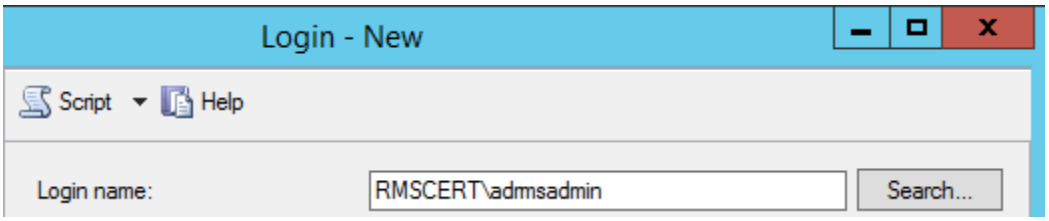
3) En la ventana **"Connect to server"** de "Microsoft SQL Server Management Studio" dar clic en **"Connect"**.



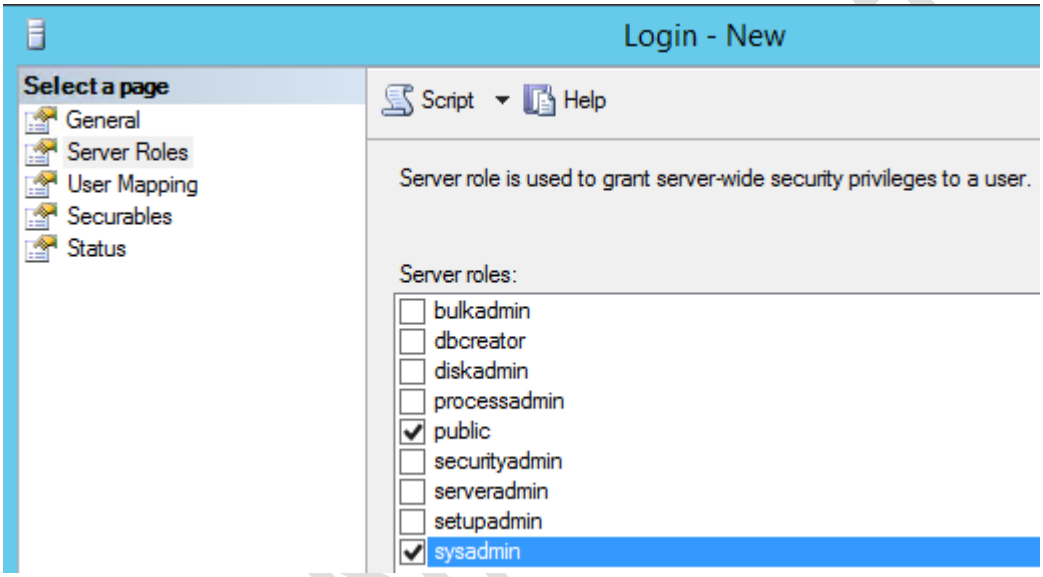
4) En el explorador de objetos, expandir **"Servidor_SQL"** > **"Security"**, dar clic derecho en **"Logins"** y seleccionar **"New Login…"**.



5) En la ventana **"Login - New"** dar clic en **"Search"**. En la ventana que se abre, escribir **"ADRMSADMIN"**, dar clic en **"Check Names"** y después en **"OK"**.

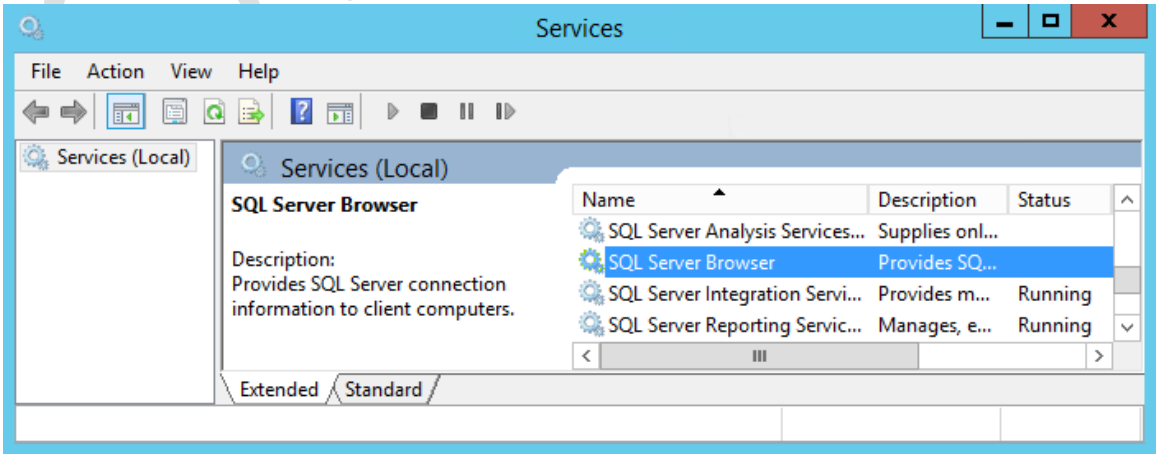


6) Aún en la ventana **"Login – New"**, en el panel del lado izquierdo, seleccionar **"Server Roles"** y marcar la casilla **"sysadmin"**. Aceptar los cambios dando clic en **"OK"** y cerrar SQL Server Management Studio.



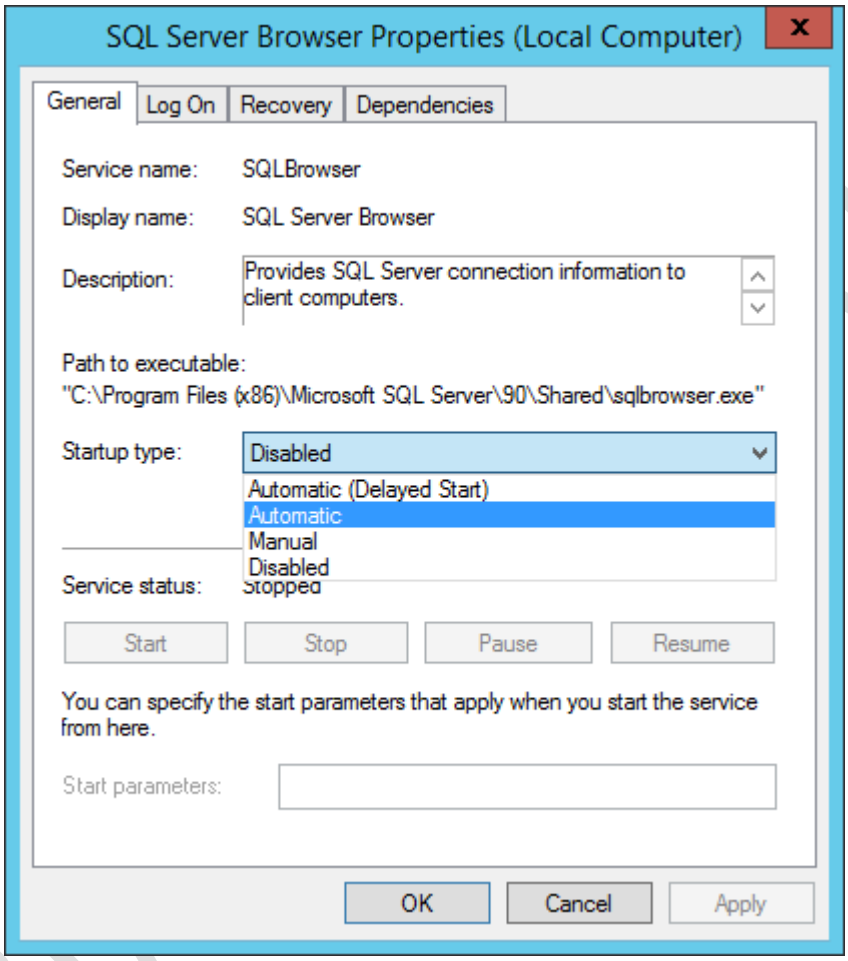
- **Iniciar el servicio SQL Server Browser**

7) Abrir de nuevo **"Task Manager"**, ya sea presionando las teclas **CTRL + ALT + DEL** o dando clic derecho sobre la barra de tareas, y dar clic en **"File"** > **"Run new task"**. En la ventana que se abre escribir **"Services.msc"** y dar clic en **"OK"** para abrir la consola de servicios.



8) Desplazarse sobre la lista de servicios hasta encontrar **"SQL Server Browser"**. Dar derecho sobre el nombre del servicio y seleccionar **"Properties"**.

9) En la ventana **"SQL Server Properties"**, seleccionar **"Automatic"** para el campo **"Startup type"** y dar clic en **"Apply"** para aplicar los cambios.

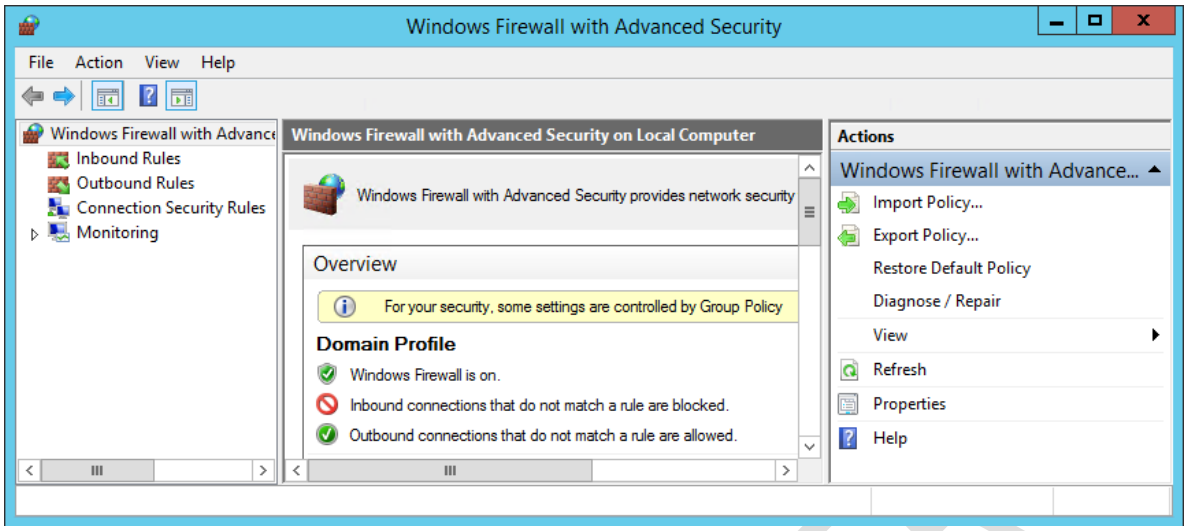


10) Por último dar clic en el botón **"Start"** y después en **"OK"**. Cerrar la consola de servicios.

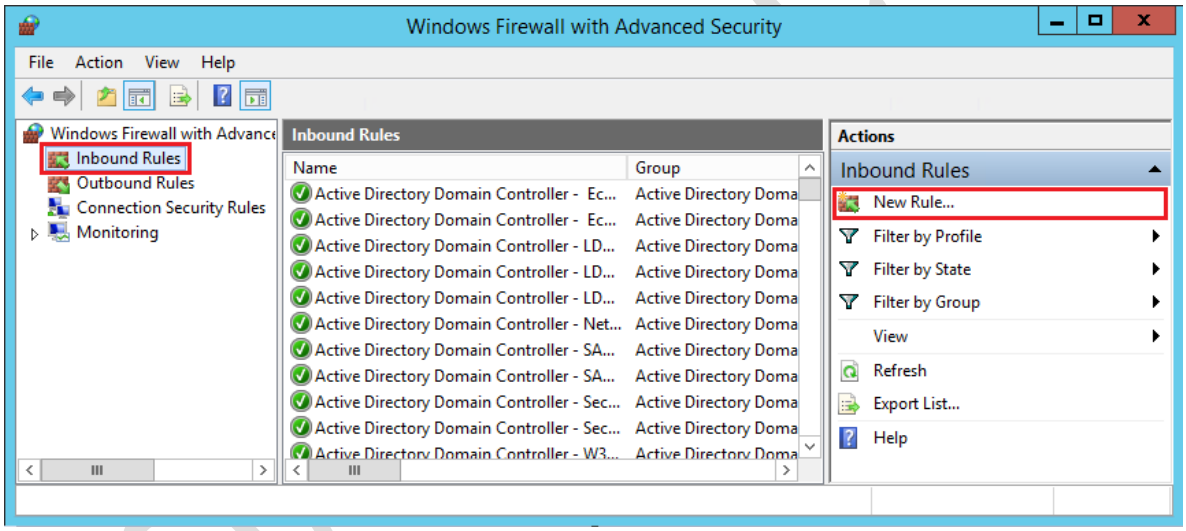
- **Añadir excepciones en el firewall para los puertos usados por SQL Server**

11) Abrir el manejador de tareas presionando las teclas **CTRL + ATL + DEL** o dando clic derecho sobre la barra de tareas.

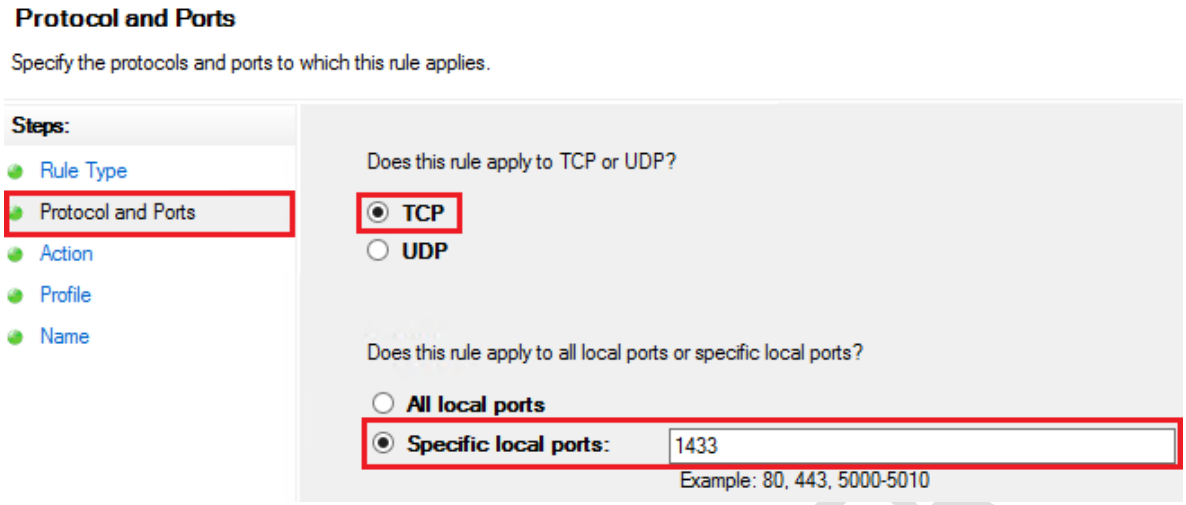
12) Del menú **"File"**, seleccionar **"Run new task"** y escribir **"Wf.msc"** para abrir la consola del firewall de Windows con seguridad avanzada. Dar clic en **"OK"**.



13) En el panel del lado izquierdo, dar clic sobre **"Inbound Rules"** y en el panel derecho dar clic sobre **"New Rule"** para crear una regla de entrada.



14) Es necesario permitir las conexiones entrantes desde el puerto 1433 tanto en TCP como en UDP, para esto se debe seleccionar lo siguiente:
Rule Type: Port
Protocols and Ports: TCP
Specific local ports: 1433
Action: Allow the connection
Profile: Domain, Private y Public
Name: SQL_1433



15) Crear tres reglas más de entrada (inbound) modificando únicamente las siguientes características [3]:

Regla: Protocols and Ports: UDP
Specific local ports: 1434
Name: SQL_1434

Regla: Protocols and Ports: TCP
Specific local ports: 445
Name: SQL Server Named Pipes

Regla: Protocols and Ports: TCP
Specific local ports: 11435
Name: SQL Server Cloud Adapter (TCP-in)

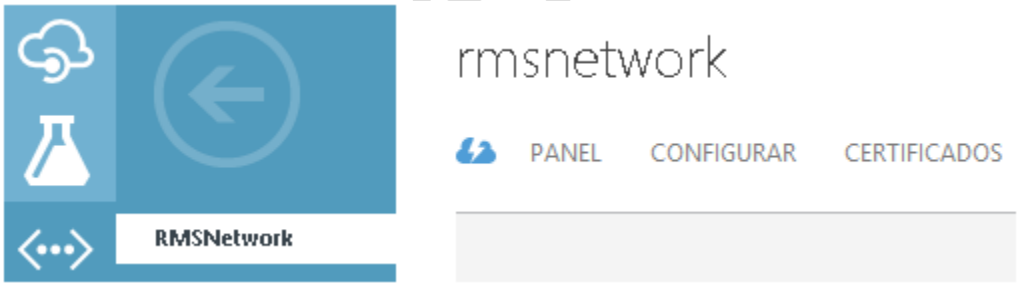
16) Cerrar la consola del firewall de Windows con seguridad avanzada.

3. INSTALACIÓN Y CONFIGURACIÓN DE SERVICIOS EN EL SERVIDOR RMS

3.1 Unión del servidor RMS al dominio

Antes de poder unir un equipo al dominio es necesario configurar el servidor DNS para la red virtual en el portal de Microsoft Azure [4].

1) Dar clic en **"Redes"** para abrir el panel de configuración de las redes virtuales. Al dar doble clic en el nombre de la red virtual, creada en pasos anteriores, se muestran las opciones para su manejo. Dar clic en **"Configurar"**.

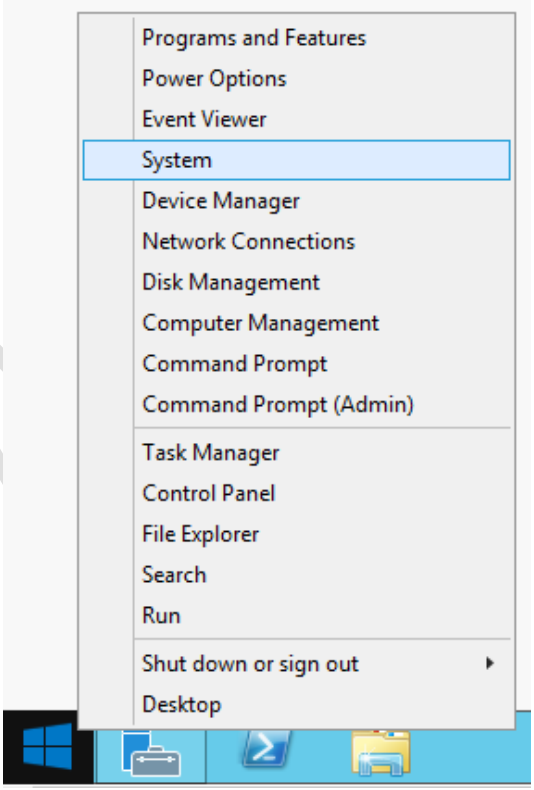


2) En **"Servidores DNS"** seleccionar un DNS (como no se especificó ninguno al crear la red virtual la única opción que aparece es "dns") y automáticamente se mostrará la dirección IP del servidor con Active Directory instalado, en la imagen del ejemplo se observa la dirección IP 10.0.0.4 del servidor sqlserver-rms.

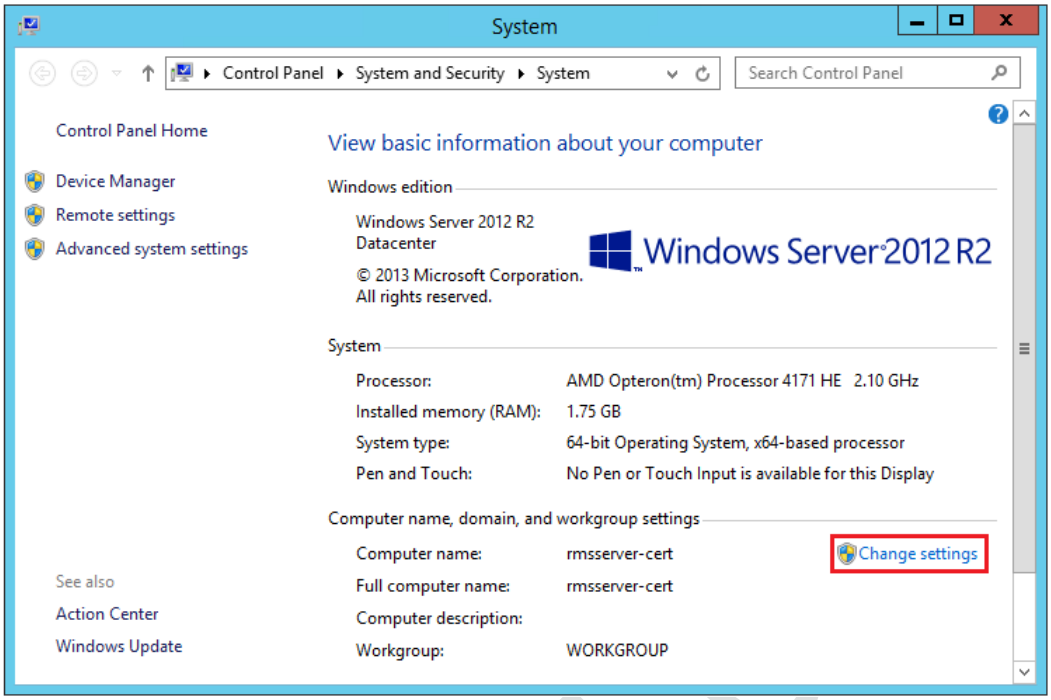
3) Para que las máquinas puedan tener salida a Internet se puede agregar la dirección IP 168.63.129.16 como DNS alternativo.

4) Dar clic en **"Guardar"**, que se encuentra en la parte inferior del portal y elegir **"Si"** cuando se muestre el mensaje de advertencia que indica que se interrumpirá la conexión con la máquina virtual. Reiniciar ambos servidores para que las máquinas virtuales actualicen sus configuraciones de DNS [4].

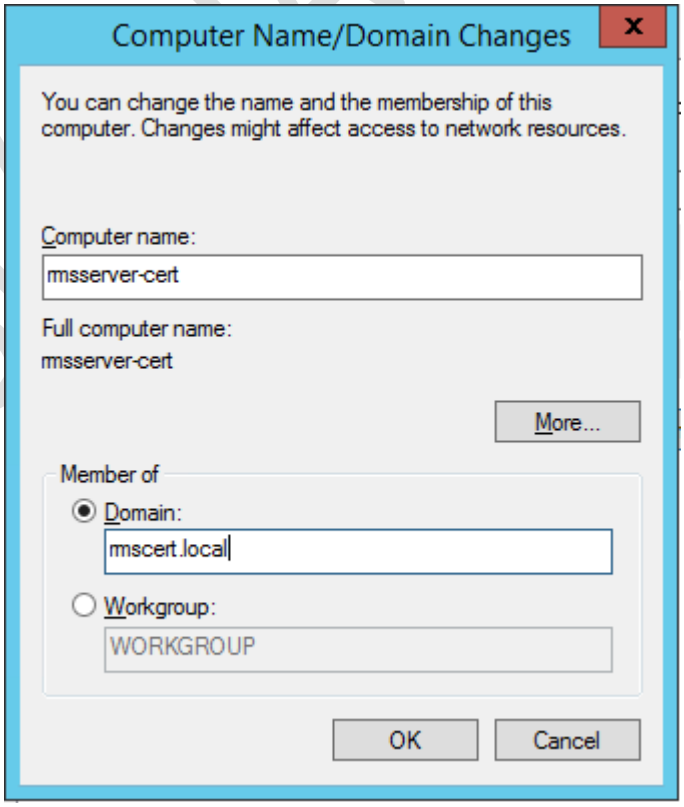
5) A continuación, iniciar sesión con el dominio y el usuario creado en la máquina virtual con el servidor RMS.



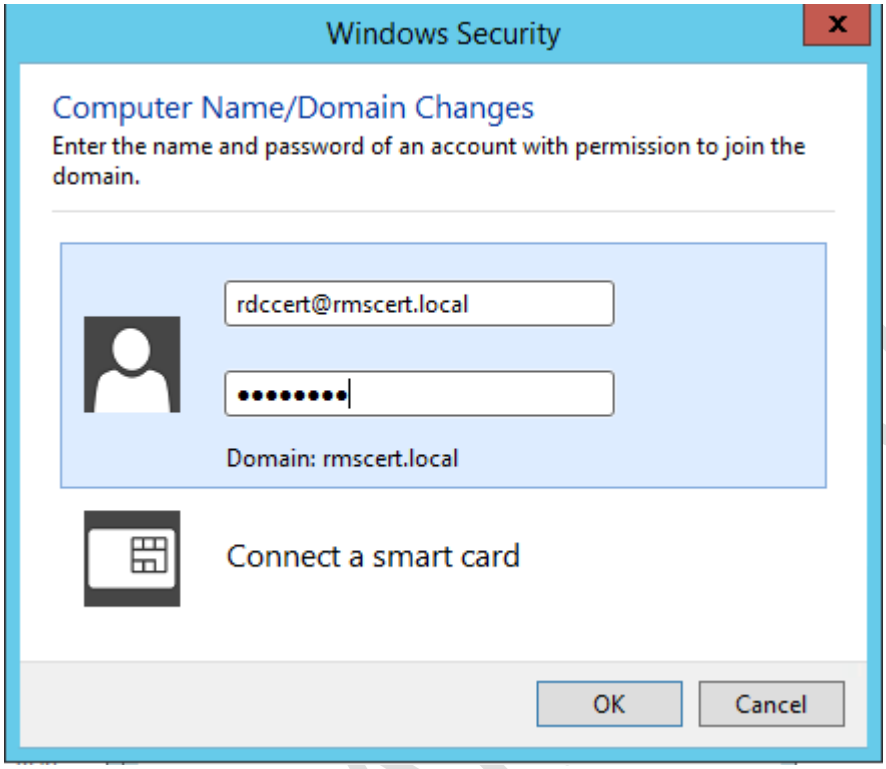
6) Dar clic derecho en el ícono de Windows que se encuentra en la esquina inferior izquierda y seleccionar **"System"**.



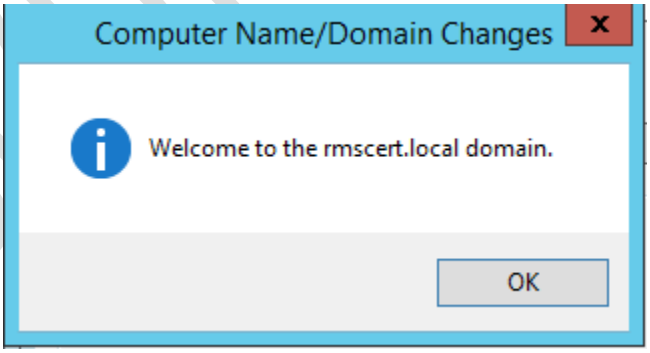
7) Dar clic en **"Change Settings"** y después en el botón **"Change…"** de la ventana **"System Properties"**. De forma predeterminada el servidor es miembro del grupo de trabajo **"Workgroup"**, para unir el equipo al dominio se debe seleccionar **"Domain"** y escribir el nombre del dominio en la caja de texto que se habilita.



8) Para que el equipo pueda unirse al dominio es necesario autenticarse con una cuenta de administración, como se muestra en la siguiente imagen.



9) Si la unión al dominio se lleva a cabo sin problemas, se mostrará una ventana con un mensaje de bienvenida. Reiniciar el servidor RMS para que los cambios hagan efecto.



3.2 Apertura de puertos en el portal de Microsoft Azure

Antes de continuar con la configuración del servidor RMS es necesario abrir los puertos 80 y 443 en el portal de Microsoft Azure. En el panel de máquinas virtuales dar doble clic en el nombre asignado al servidor RMS y elegir **"Extremos"**.

Dar clic en el botón **"Agregar"** que se encuentra en la parte inferior del portal. En el asistente de configuración seleccionar las siguientes opciones:

Agregar un extremo independiente.

Detalles del extremo

- Nombre: HTTP
- Protocolo: TCP
- Puerto público: 80
- Puerto privado: 80

Y seguir los dos pasos para el puerto 443 (HTTPS).

3.3 .Net Framework 3.5

.NET Framework es una tecnología que admite la compilación y ejecución de aplicaciones y servicios Web XML. El diseño de .NET Framework está enfocado a cumplir los siguientes objetivos:

- Proporcionar un entorno coherente de programación orientada a objetos, en el que el código de los objetos se pueda almacenar y ejecutar de forma local, ejecutar de forma local pero distribuida en Internet o ejecutar de forma remota.
- Proporcionar un entorno de ejecución de código que minimiza los conflictos en el despliegue y versionado de software.
- Proporcionar un entorno de ejecución de código que elimine los problemas de rendimiento de los entornos en los que se utilizan scripts o intérpretes de comandos.
- Ofrecer al programador una experiencia coherente entre tipos de aplicaciones muy diferentes, como las basadas en Windows o en Web.

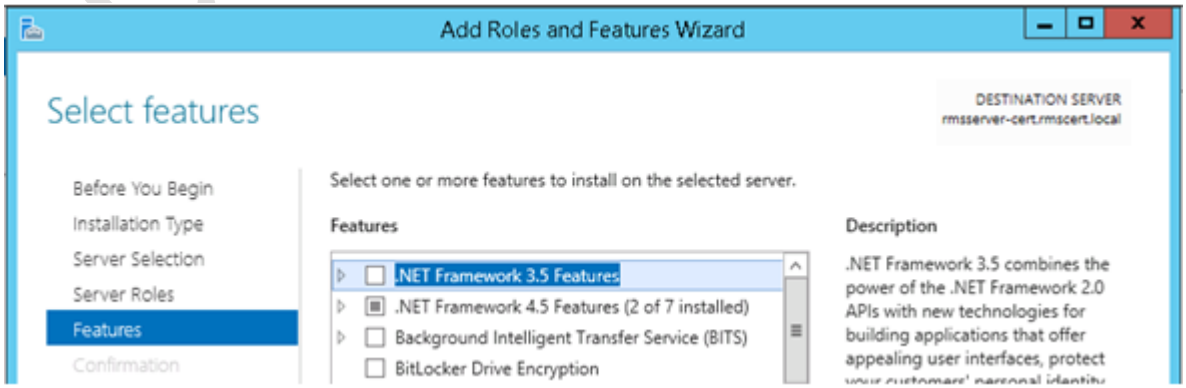
Para hacer uso de AD RMS es necesario contar con .Net Framework 3.5 instalado en el equipo. Su instalación se realiza de la misma forma que cualquier otra característica, pero con la diferencia de que se debe indicar la ruta de la fuente donde estén los archivos necesarios.

Esta fuente alternativa puede ser un disco de instalación de Windows Server 2012 R2, pero debido a que la máquina virtual se encuentra alojada en la nube no es posible insertar un disco. Eso nos deja con dos opciones, descargar un disco de instalación y montarlo en el servidor o descargar únicamente los archivos necesarios.

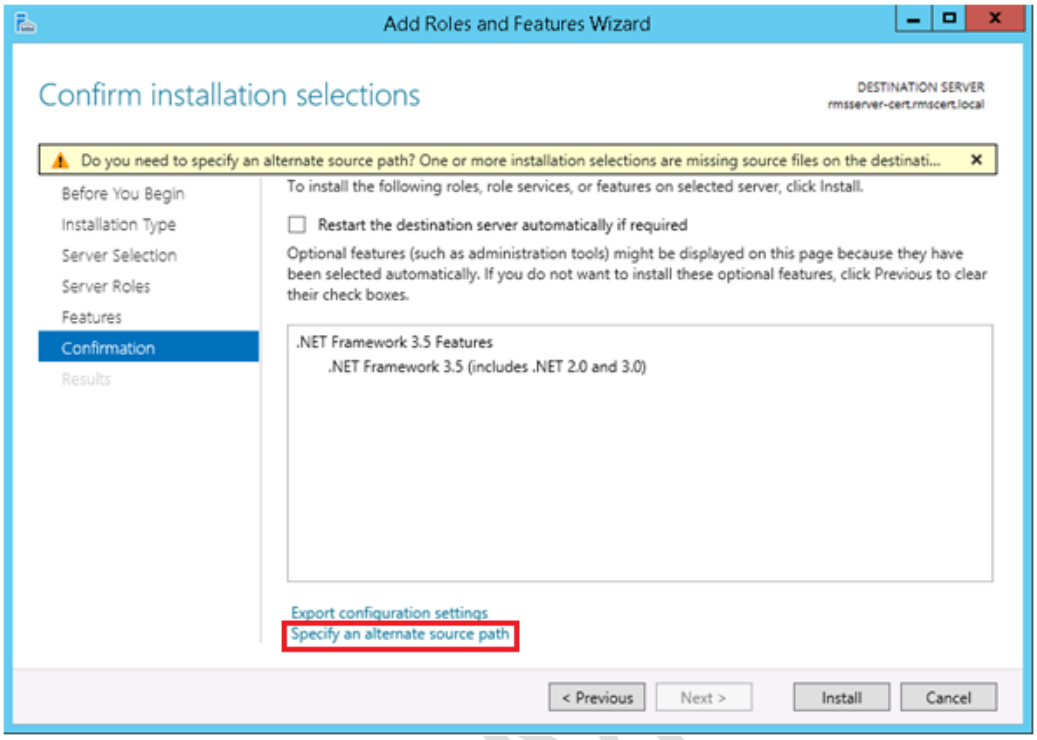
Debido a que es más eficiente descargar solo los archivos necesarios, estos se extrajeron de un disco de instalación y se pusieron disponibles para su descarga en el siguiente enlace: http://bit.ly/1I57rZT

Una vez descargados, se puede instalar .Net Framework de forma normal en el equipo donde se ejecutará AD RMS [5].

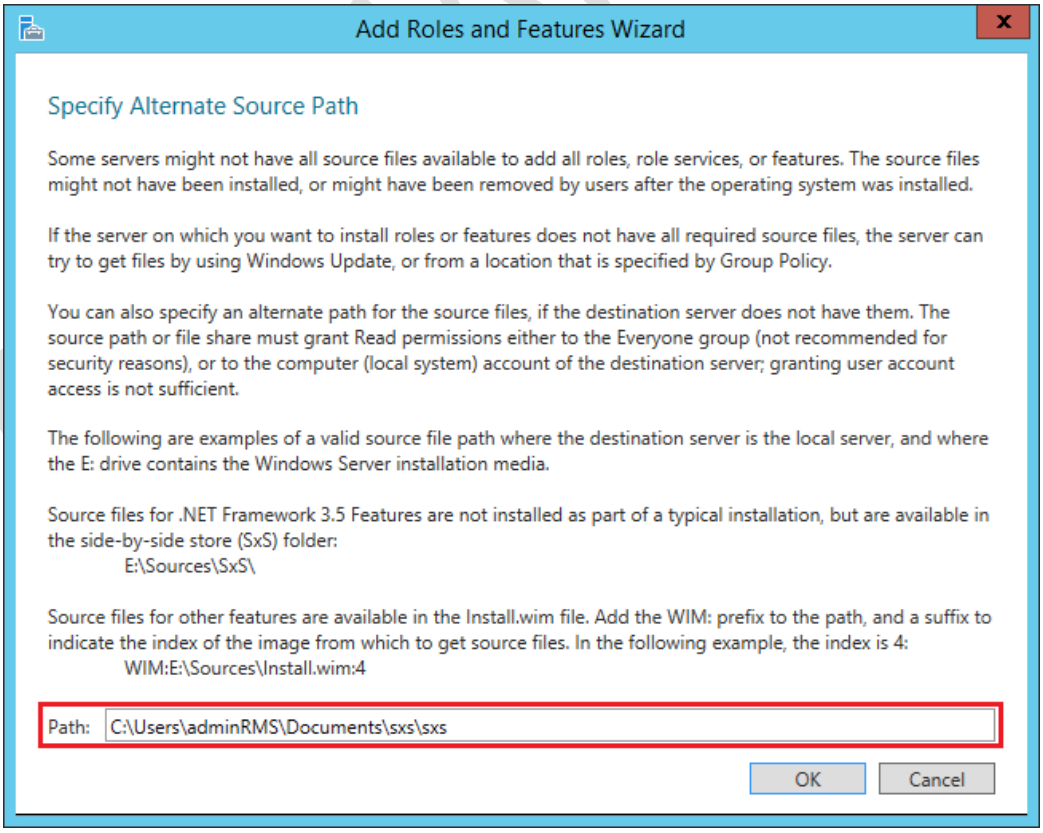
1) En la ventana de **"Server Manager"** dar clic en **"Add Roles and Features"** y seleccionar **".NET Framework 3.5 Features"**.



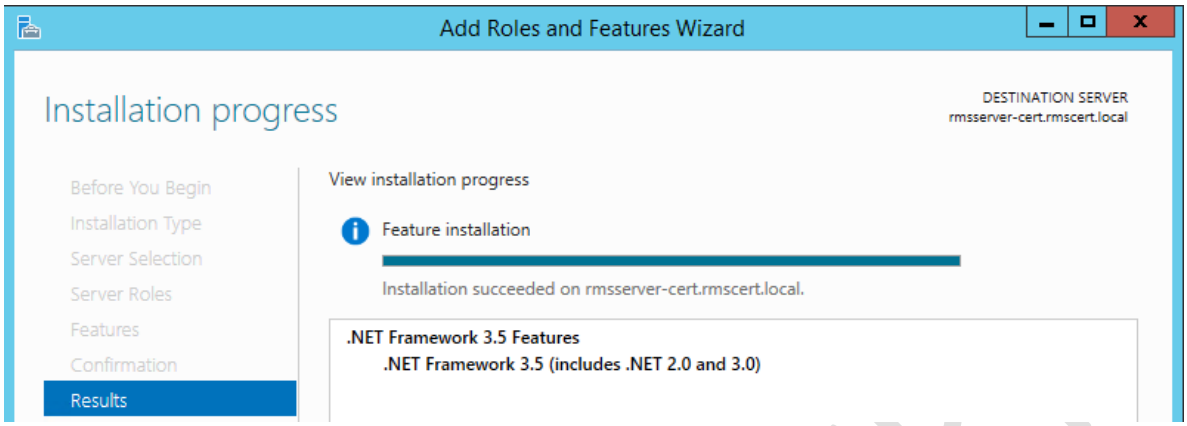
2) En el panel de confirmación dar clic en **"Specify an alternate source path"**.



3) Indicar la ruta completa de la carpeta con los archivos fuente.



4) Comenzar la instalación dando clic en el botón **“Install”**.



3.4 Instalación IIS

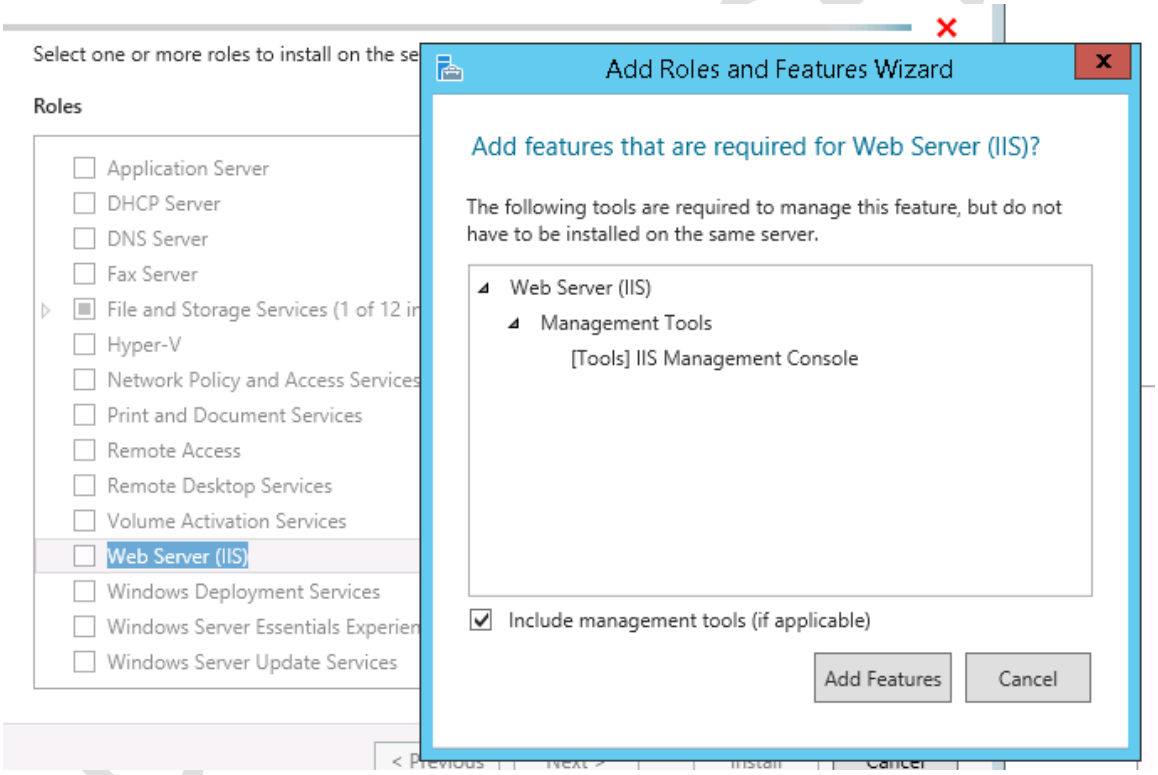
Teniendo la Autoridad Certificadora funcionando en el dominio se procede a instalar el rol Web Service para poder configurar el sitio web utilizado por AD RMS.

La instalación de IIS no requiere ninguna característica extra, basta con hacer una instalación por defecto, esto debido a que RMS es el encargado de configurar el sitio Web para su funcionamiento.

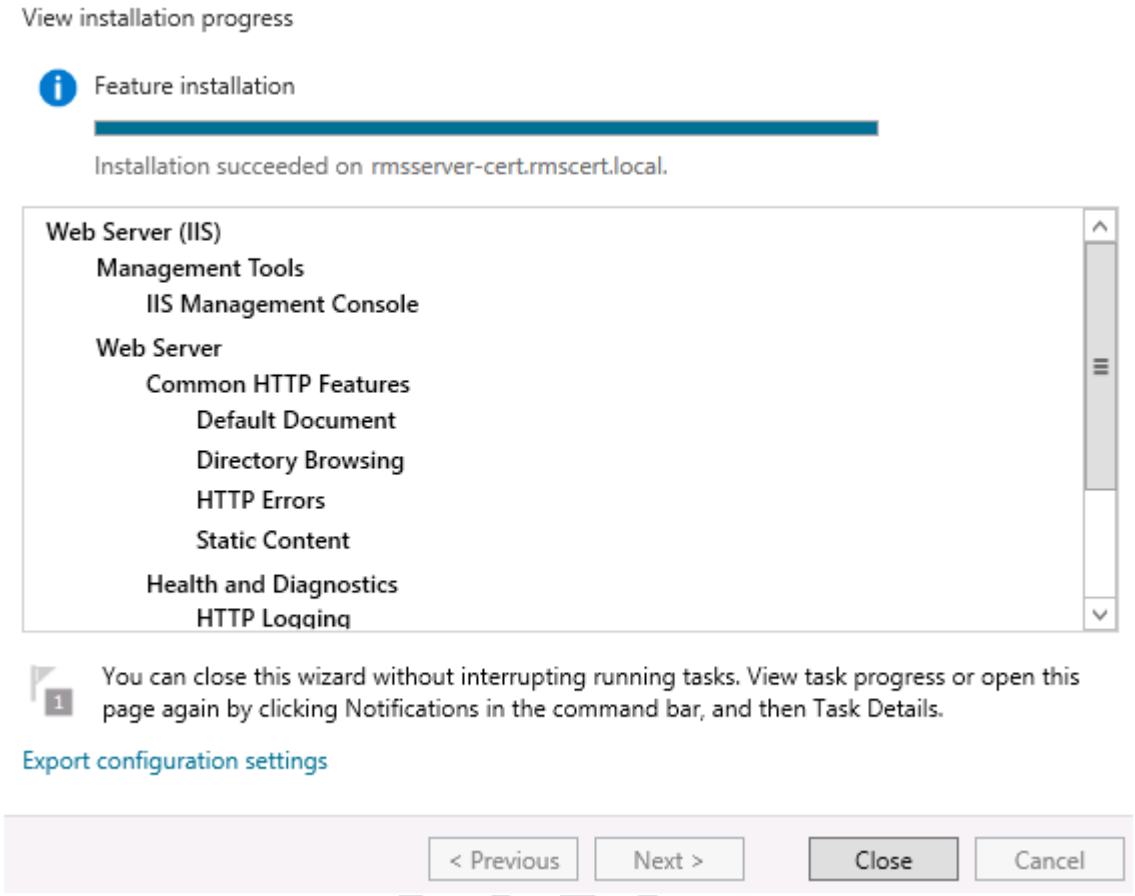
1) En la ventana de **"Server Manager"** dar clic en **"Add Roles and Features"**.

2) Dar clic en el botón **"Next"** hasta llegar a **"Server Roles"**.

3) Marcar la casilla **"Web Server (IIS)"** y dar clic en **"Add Features"**.



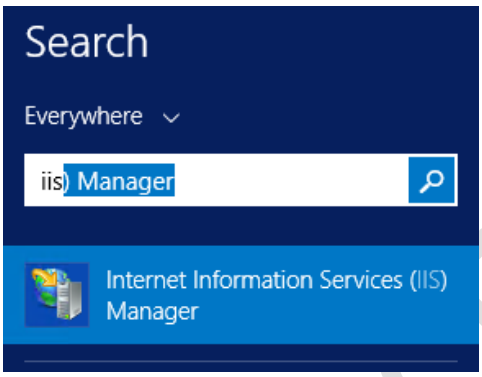
4) Dar clic en **"Next"** hasta que se muestre el botón **"Install"**. Terminar la instalación.


View installation progress
Feature installation
Installation succeeded on rmsserver-cert.rmscert.local.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

3.5 Solicitud de certificado

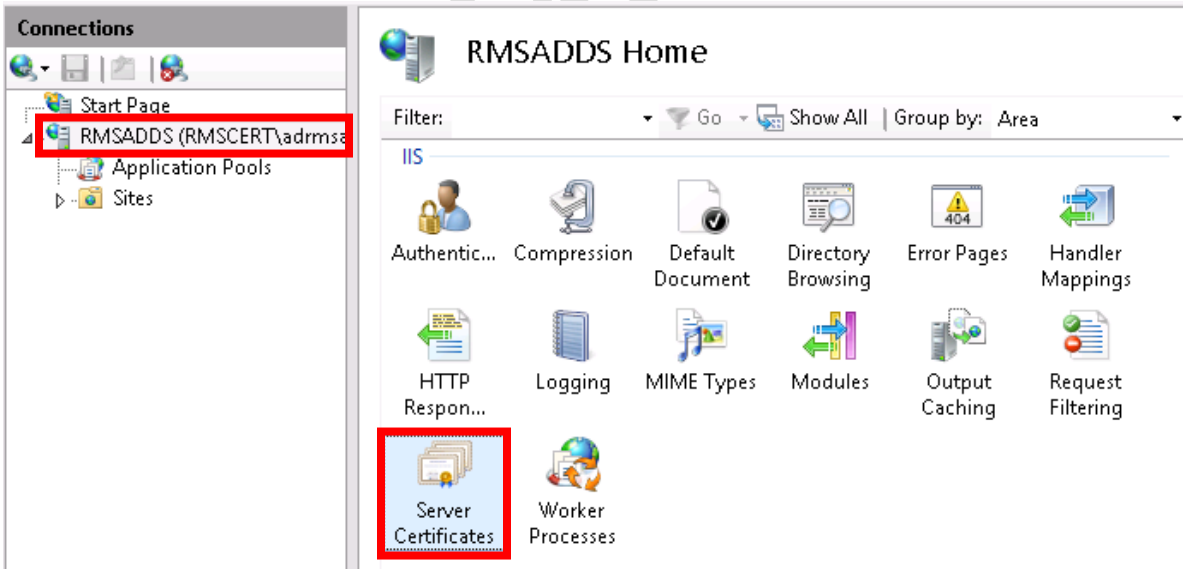
Teniendo IIS instalado, se debe solicitar un certificado para que pueda ser utilizado en el sitio web de RMS.

1) Buscar **"IIS"** en el menú de Inicio.

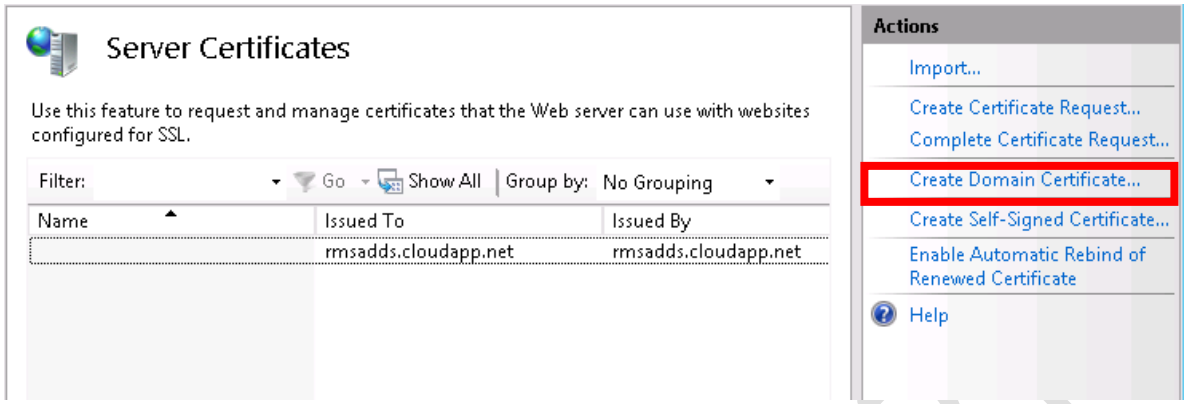


2) Abrir la aplicación dando doble clic sobre el ícono de **"Internet Information Services (IIS) Manager"**.

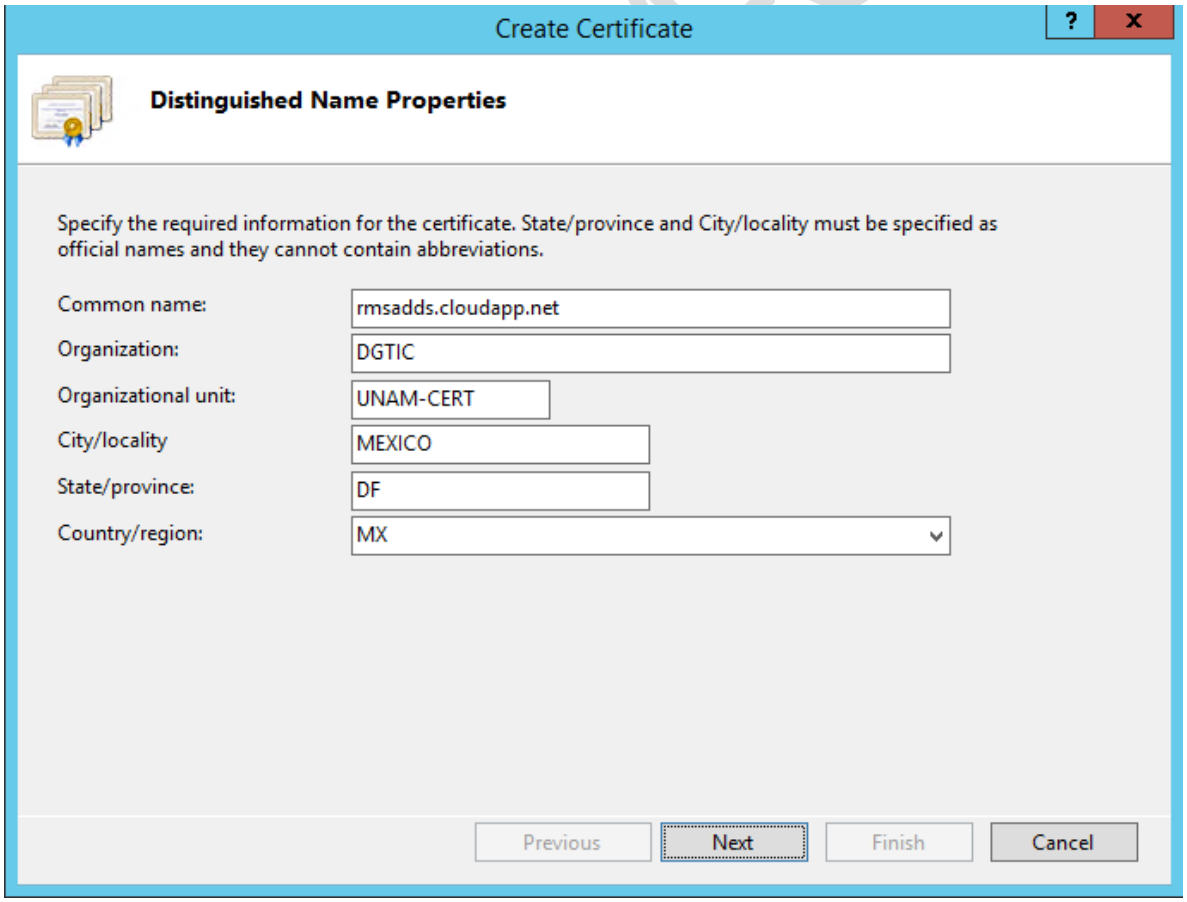
3) A nivel de servidor, dar doble clic en el ícono correspondiente a los servicios de certificados.



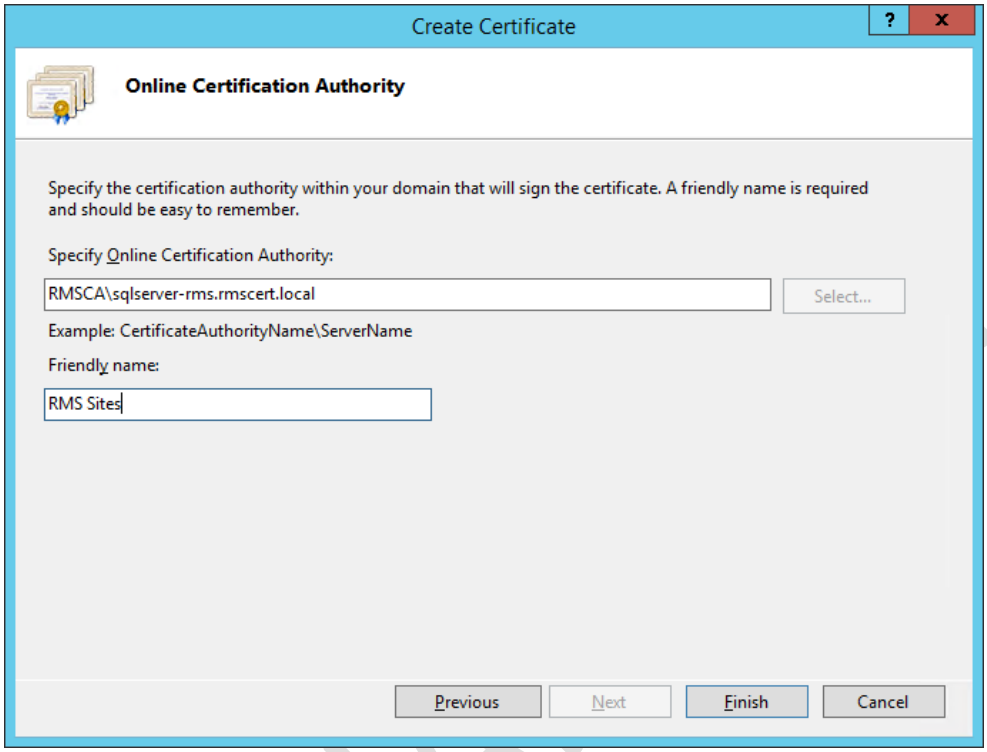
4) Solicitar un nuevo certificado de dominio dando clic en **“Create Domain Certificate”**.



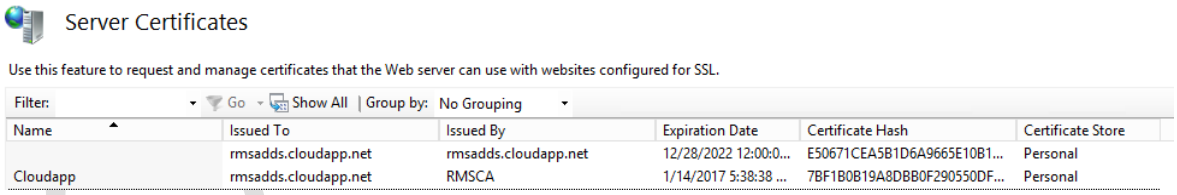
5) Llenar los datos del formulario como se observa en la imagen; cabe destacar que **“Common Name”** debe coincidir con el nombre del sitio público en el que se usará el certificado.



6) Al dar clic en **"Next"** se debe seleccionar la Autoridad Certificadora a la cual se le solicitará el certificado. En caso de que la autoridad certificadora no se pueda listar, se deben actualizar las políticas de grupo haciendo uso del comando **"gpupdate /force"** en PowerShell o en un cmd.



7) Después de dar clic en el botón **"Finish"** para terminar de crear el certificado, se debe ver lo siguiente en **"Server Certificates"**:



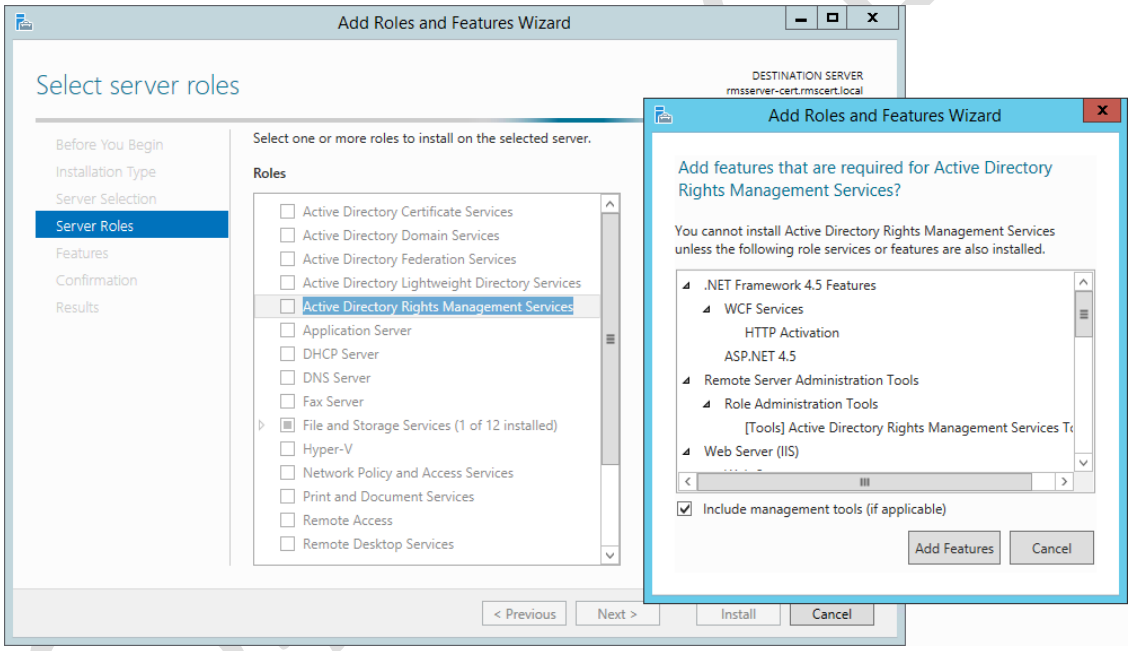
3.6 Instalación y configuración de AD RMS

En Windows Server 2012 se puede instalar y configurar el rol de AD RMS a través del Server Manager.

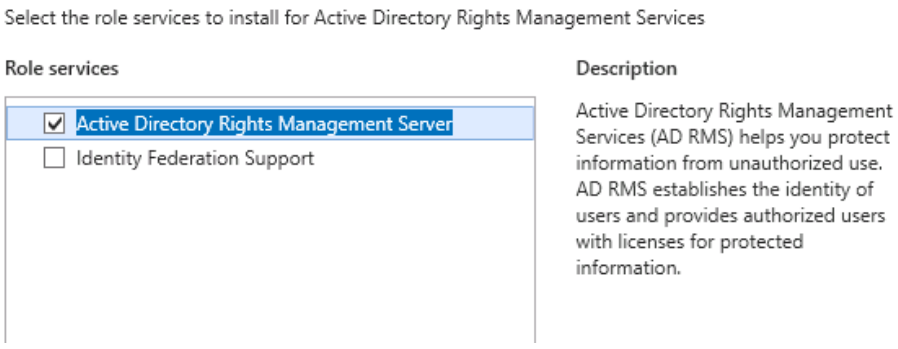
- **Instalar el rol AD RMS**

1) Iniciar sesión en el servidor RMS con la cuenta ADRMSADMIN, que pertenece al grupo **"Enterprise Admins"** y cuyo propósito es encargarse de la instalación e implementación del servidor AD RMS.

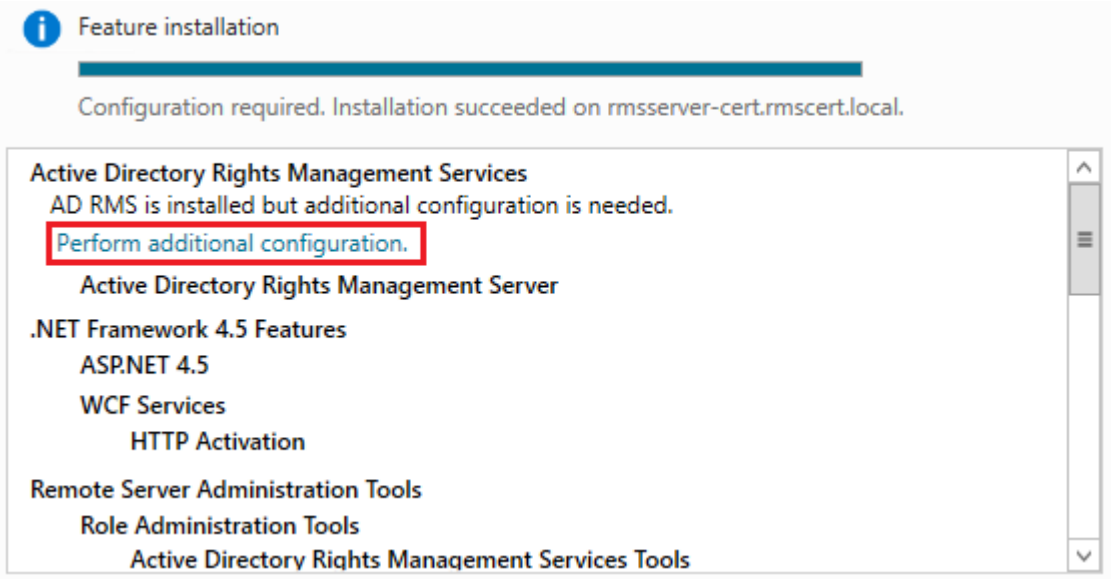
2) En la ventana de **"Server Manager"** dar clic en **"Add roles and features"**. Al llegar a **"Server Roles"** se debe marcar el rol **"Active Directory Rights Management Services"**, al hacerlo observamos que se añadirán características extras a nuestro IIS. Dar clic en **"Add Features"**.



3) Seleccionar únicamente el rol de Servidor de RMS y comenzar la instalación.

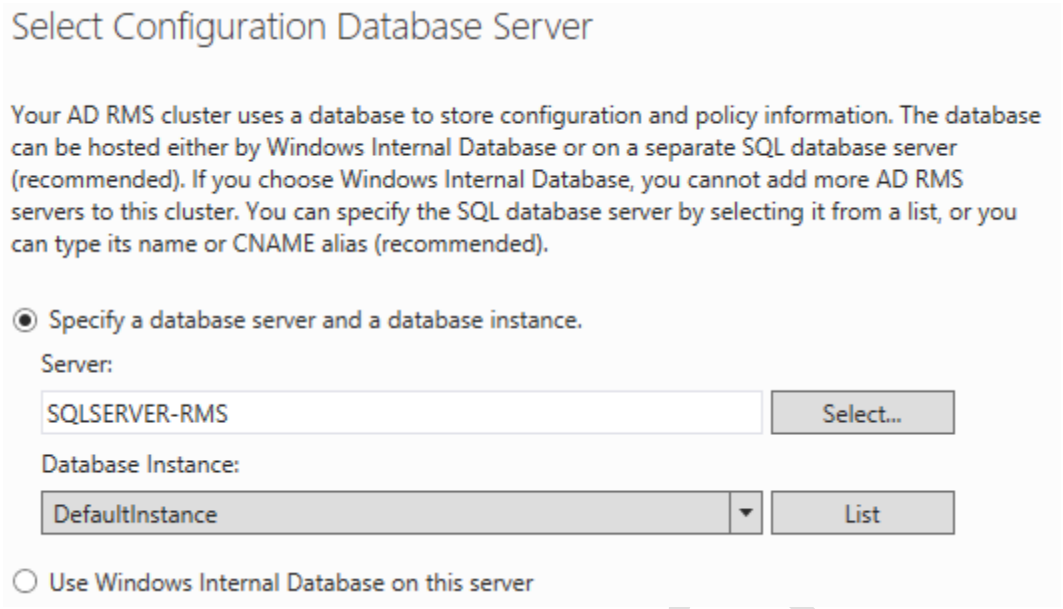


4) Configurar AD RMS dando clic en el enlace color azul, señalado en la imagen siguiente, y seguir el asistente.

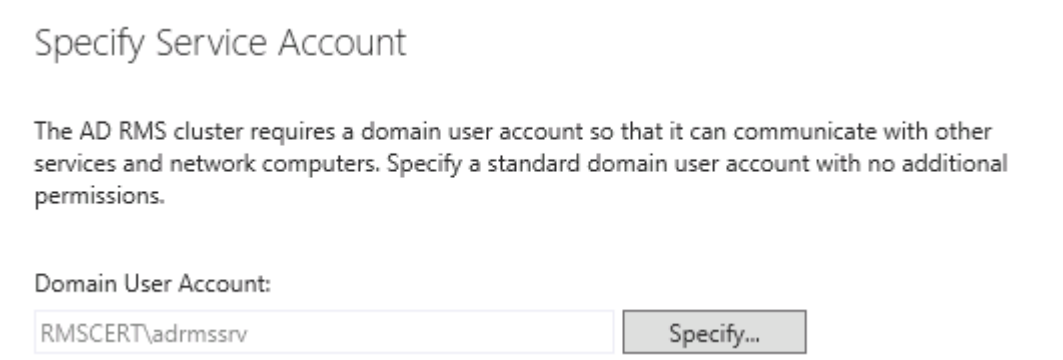


5) Al ser un servicio nuevo en el dominio, debemos crear un clúster AD RMS. Este clúster raíz es el que se encarga de la certificación y del licenciamiento. Seleccionar **"Create a new AD RMS root cluster"** y continuar.

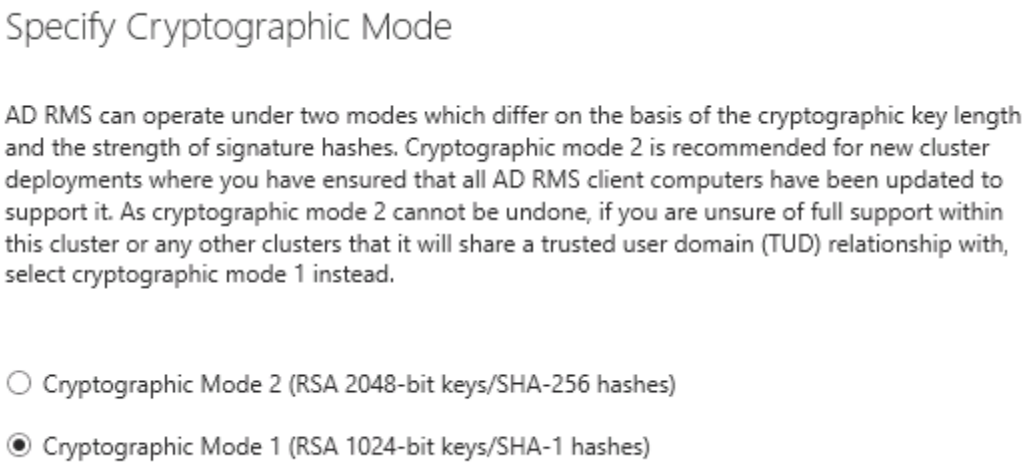
6) Debemos indicar el servidor en el que se encuentra alojada nuestra base de datos, una vez seleccionado debemos dar clic en el botón **"Select"** y después desplegar la lista de instancias de bases de datos dando clic en **"List"**. Seleccionar la instancia por defecto (DefaultInstance).



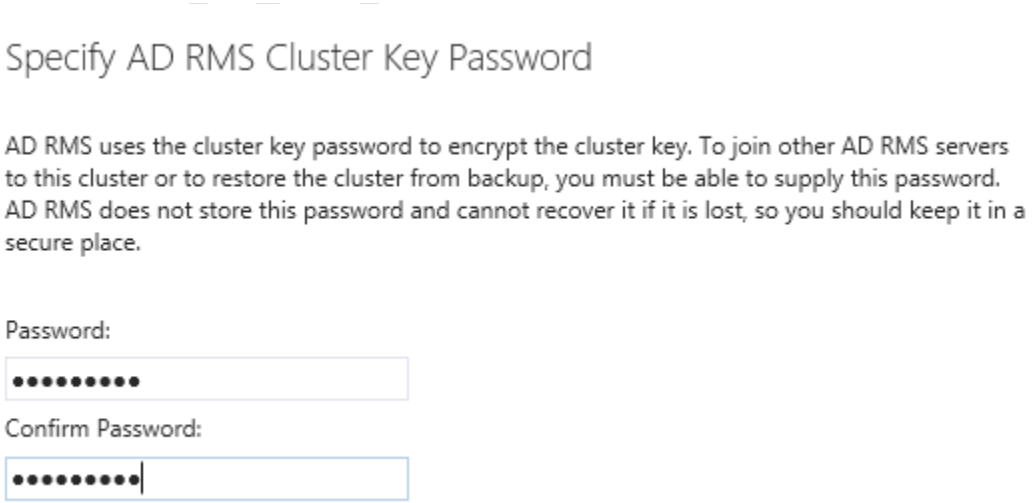
7) Es necesario contar con una cuenta de usuario sin ningún privilegio extra únicamente para poder comunicar AD RMS con otros equipos o servicios. Al tenerla hay que especificarla en la configuración de AD RMS. En este caso la cuenta es ADRMSSRV, creada en pasos anteriores.



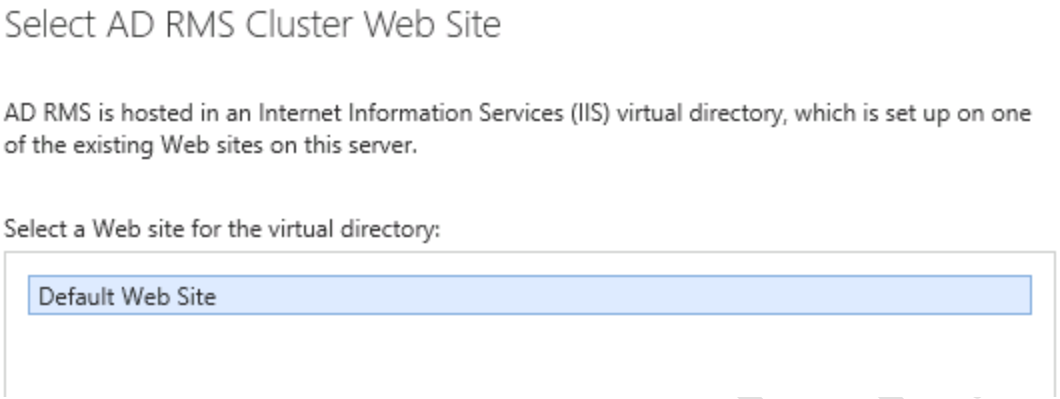
8) Como la descripción lo indica, AD RMS puede operar en dos modos criptográficos, debido a que es necesario hacer uso de Windows ID debemos elegir el modo 1, ya que el modo 2 no ofrece soporte para el manejo de Windows ID [6].



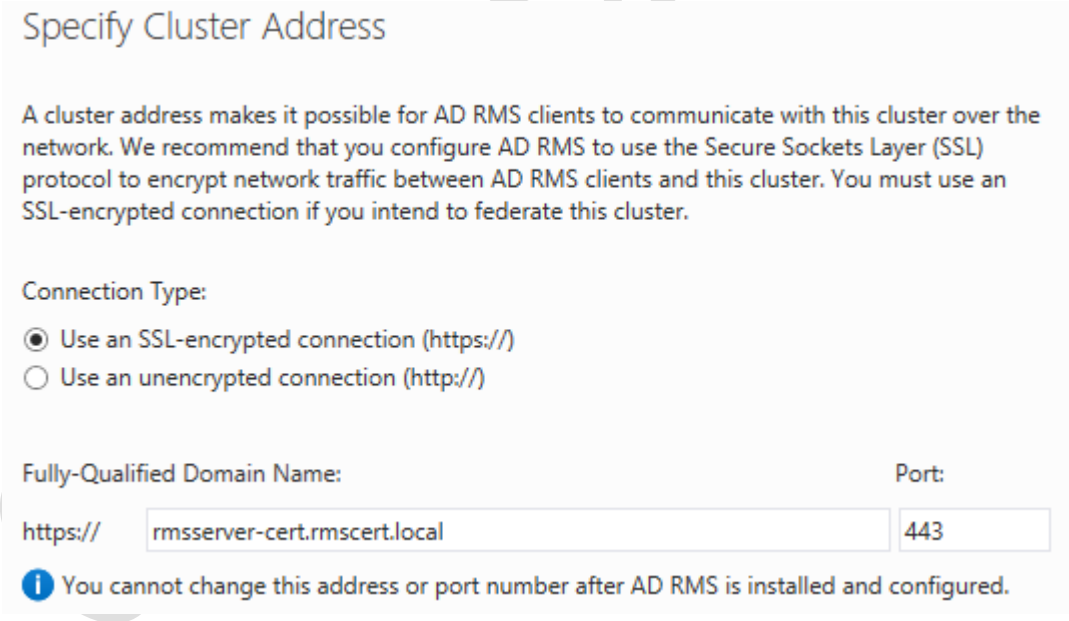
9) Continuar con el asistente como se muestra en las siguientes imágenes.



10) Al no tener otro sitio web creado en IIS mas que el sitio por defecto, debemos seleccionarlo para que AD RMS haga uso de él.

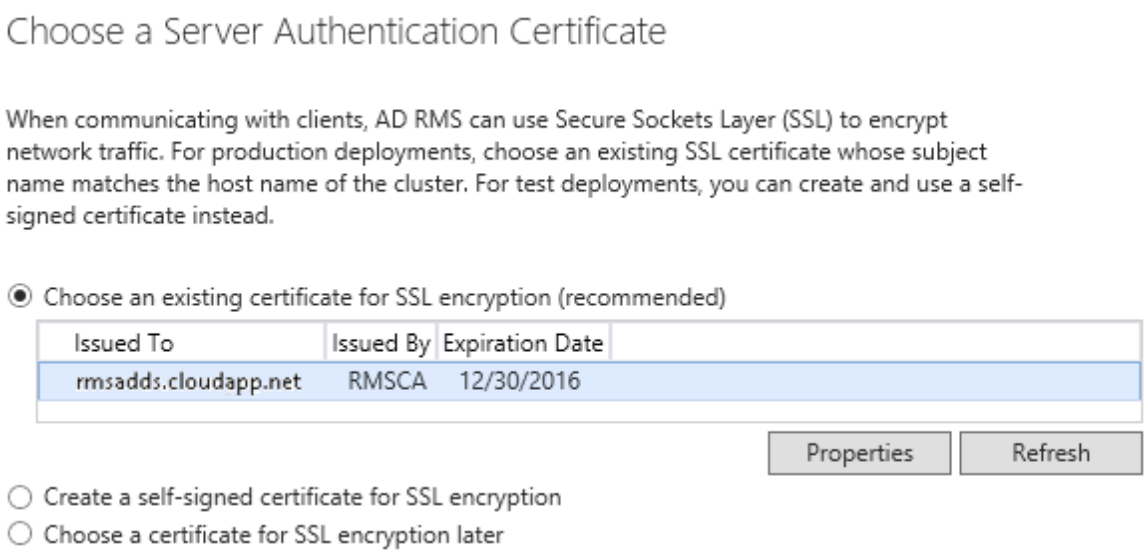


11) Seleccionar la opción de conexión mediante HTTPS e indicar la dirección que utilizará RMS para que los clientes puedan comunicarse con el servicio. Esta dirección no podrá ser cambiada una vez configurado el servicio.



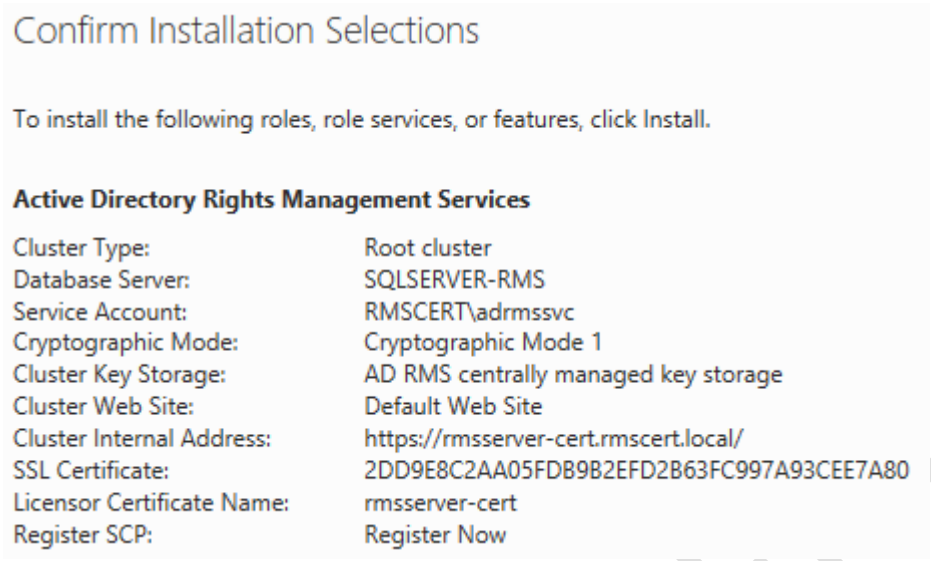
La URL para el clúster AD RMS debe ser distinta al nombre del equipo [7].

12) Seleccionar el certificado creado anteriormente, en caso de no contar con un certificado se puede crear y dar clic en **"Refresh"**, o bien, utilizar un certificado autofirmado (esto no es recomendado).

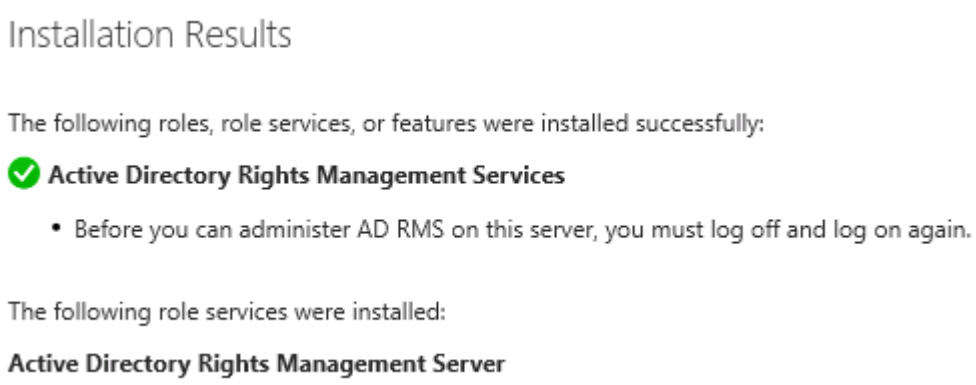


13) Registrar el SCP del servidor en Active Directory.

14) Revisar y confirmar la configuración dando clic en el botón **“Install”**.



15) Después de unos minutos se debe ver el siguiente mensaje:



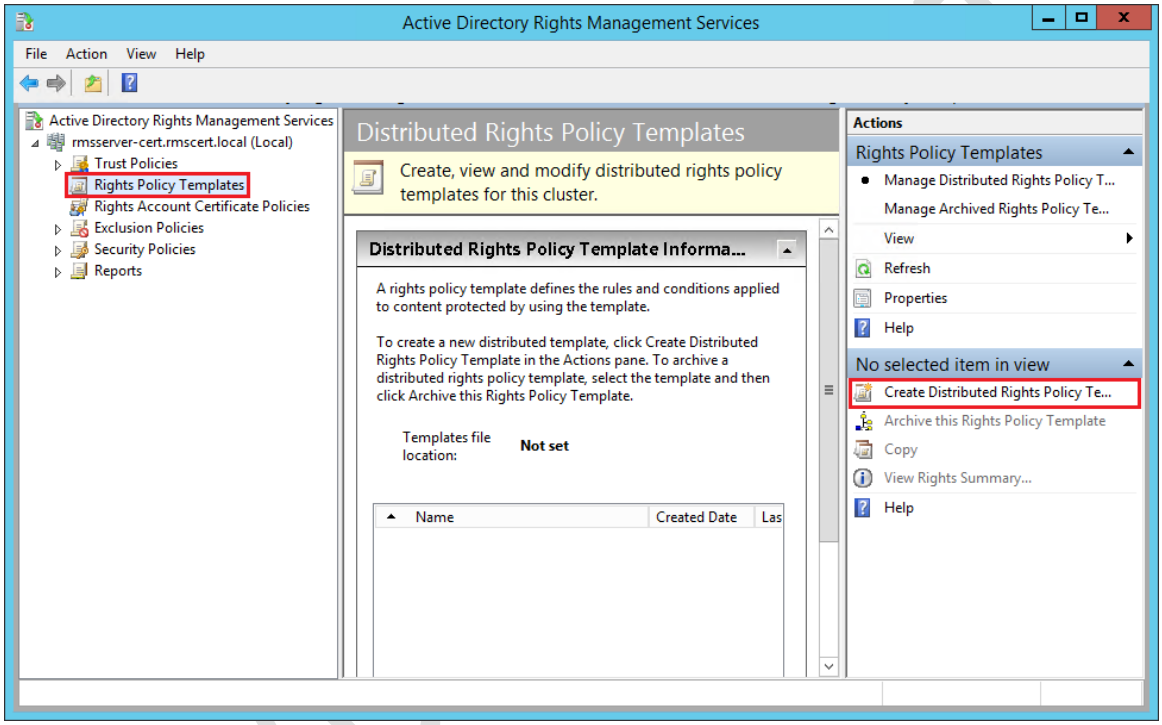
16) Es necesario cerrar sesión y volver a iniciarla para poder hacer uso de AD RMS por primera vez.

3.7 Creación de plantillas en RMS

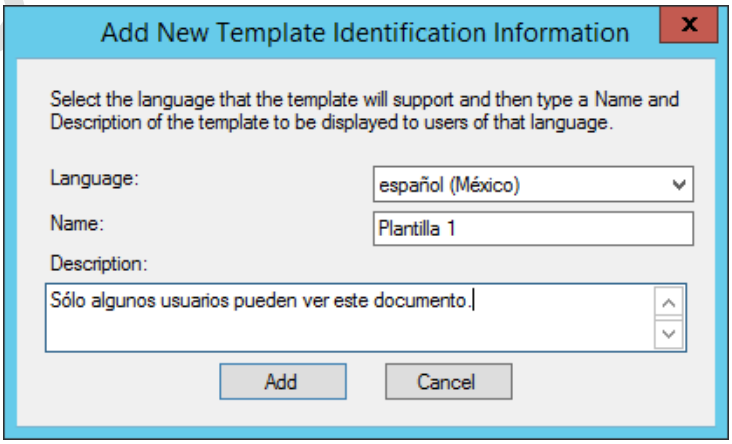
1) Abrir la consola de configuración de RMS.

2) En el panel izquierdo, desplegar las opciones del servidor RMS y seleccionar **"Rights Policy Templates"**.

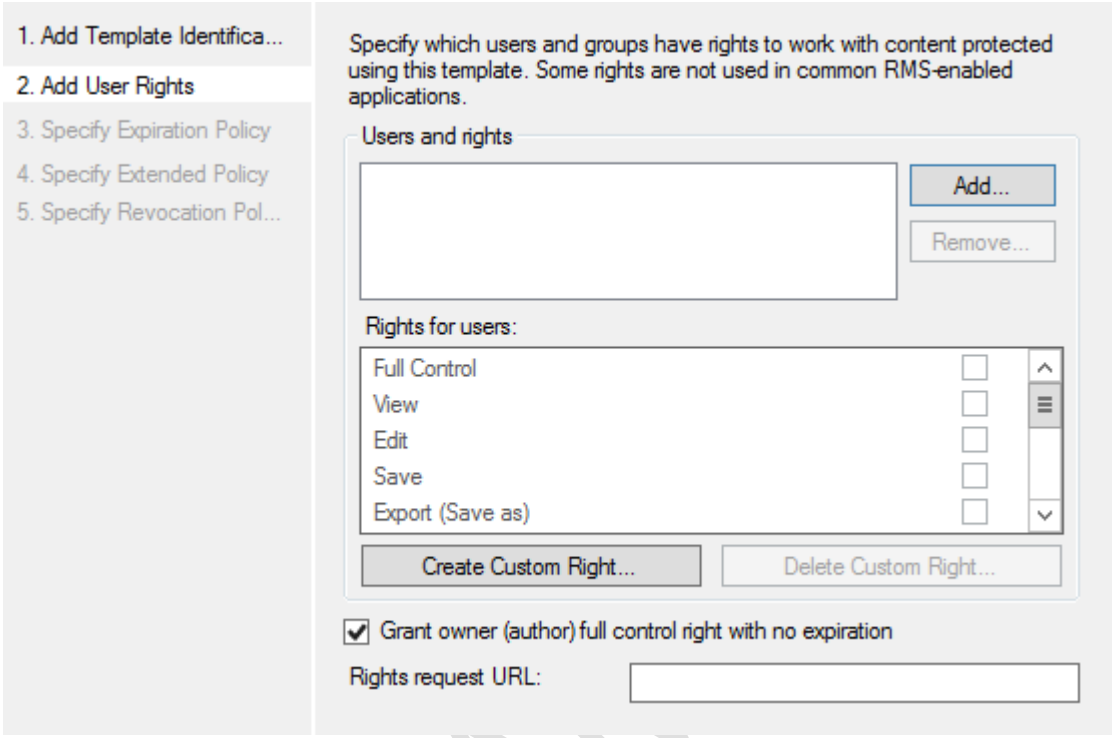
3) Del lado derecho, en el panel **"Actions"**, dar clic en **"Create Distributed Rights Policy Templates"** [8].



4) El primer paso en el asistente es seleccionar el idioma que se usa en los equipos cliente. Dar clic en el botón **"Add"**. Y en la ventana que se abre elegir el idioma deseado y añadir un nombre y una descripción para la plantilla.

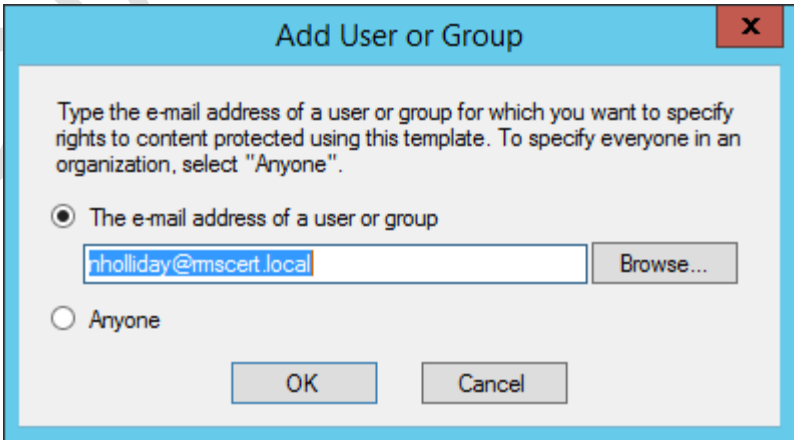


5) El segundo paso es elegir los usuarios o grupos de usuarios que pueden acceder al documento y los permisos que se les otorgan.



6) Al dar clic en **"Add…"** se abre otra ventana con dos opciones: dar permiso a cualquier usuario (Anyone) o especificar la dirección de correo electrónico de los usuarios o grupos con permiso.

7) Elegir la opción **"The e-mail address of a user or group"** y escribir el correo de un usuario, en el ejemplo se muestra el correo del usuario ficticio "Nicole Holliday".



8) En los permisos se tienen las siguientes opciones: Control total, vista, editar, guardar, exportar, imprimir, permitir macros, entre otros. En este ejemplo sólo se eligió el permiso **"View"**, para que el usuario pueda ver el contenido del documento.

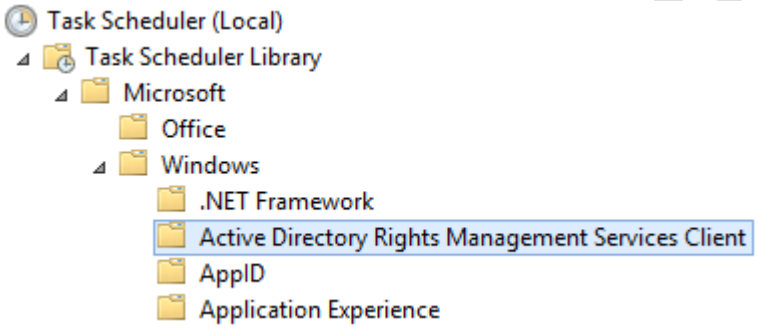
9) Terminar la plantilla con el botón **"Finish"**. También se puede establecer un periodo de expiración, entre otras opciones.

En este punto, la plantilla ha sido creada pero no está configurada y por lo tanto no ha sido publicada, por lo que aún no será visible.

3.8 Publicación de plantillas

AD RMS tiene dos tareas definidas en el programador: automatizada y manual. La automatizada está configurada para ejecutarse después de que un usuario inicia sesión y cada mañana a las 3 a.m., aunque está deshabilitada por defecto. Cabe mencionar que esta tarea sólo funciona en computadoras que están unidas al dominio [9].

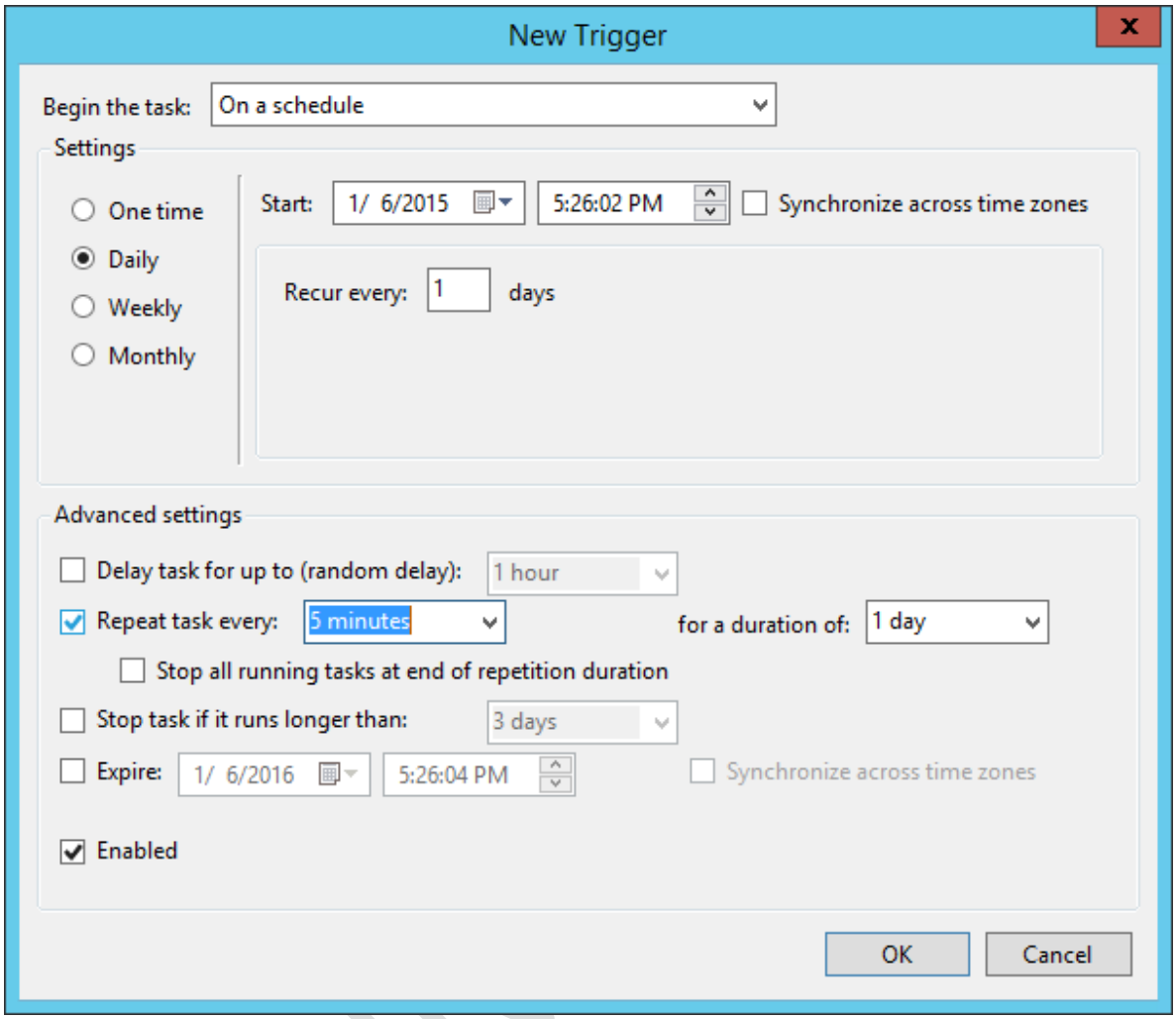
1) Abrir el programador de tareas escribiendo **"Task Scheduler"** en el menú de inicio. Navegar por las opciones del panel izquierdo de esta forma: **"Task Scheduler"** > **"Task Scheduler Library"** > **"Windows"** > **"Active Directory Rights Management Services Client"**.



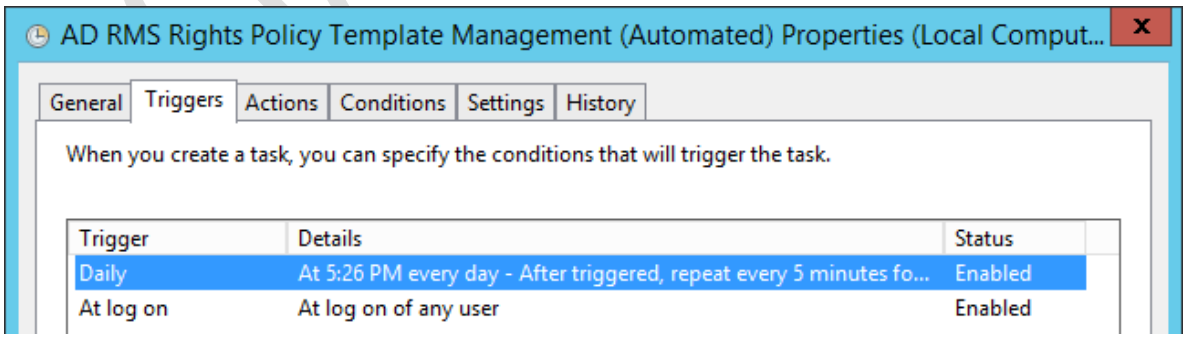
2) En el área central dar doble clic en la tarea **"AD RMS Rights Policy Template Management (Automated)"** y en la ventana que se abre seleccionar la pestaña **"Triggers"** y dar clic en el botón **"New…".** También se puede modificar el trigger ya existente para que actualice las plantillas, no sólo a las 3 a.m., sino constantemente durante el día.

El propósito de este paso es acelerar la actualización de plantillas, de tal forma que sean procesadas y almacenadas en C:\Users\adrmsadmin\AppData\Local\Microsoft\DRM\Templates, de donde pueden ser copiadas a la carpeta de plantillas de Microsoft Office. De lo contrario se tendría que esperar 7 días para que el directorio de plantillas de Office se actualizara [10].

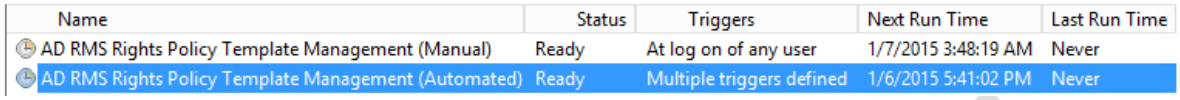
3) En la ventana de creación (o edición) de un trigger seleccionar está configuración:
   Begin the task: On a schedule
   Settings: Daily
   Start: Indicar la fecha y la hora en la que se debe iniciar la tarea. Si el trigger se está creando, de forma predeterminada aparece la fecha y la hora actual del servidor.
   Advanced Settings: Repeat task every 5 minutes (que es el tiempo mínimo que se puede seleccionar para que una tarea se repita).
   Enabled



4) En la pestaña **"Triggers"** debe aparecer habilitado el trigger que se acaba de crear, es decir, la columna **"status"** debe tener el valor **"Enabled"**. Dar clic en **"OK"**.

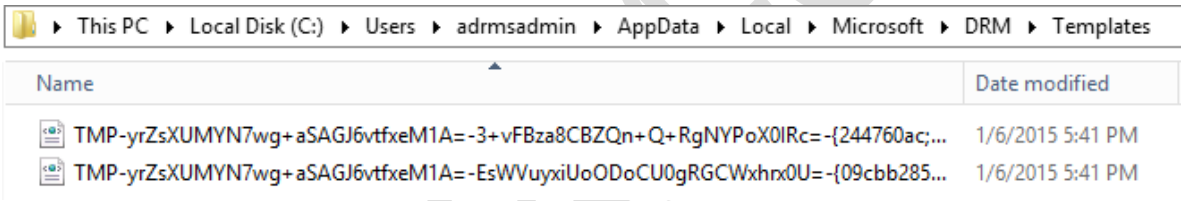


5) En la ventana del programador de tareas dar clic derecho sobre la tarea **"AD RMS Rights Policy Template Management (Automated)"**, y seleccionar **"Enable"**. La tarea debe aparecer como lista **"ready"** y tener en el campo **"Next Run Time"** la fecha y hora de su creación con cinco minutos más, que es el momento en el que se ejecutará por primera vez la tarea, en este caso se ejecutará a las 5:41pm.

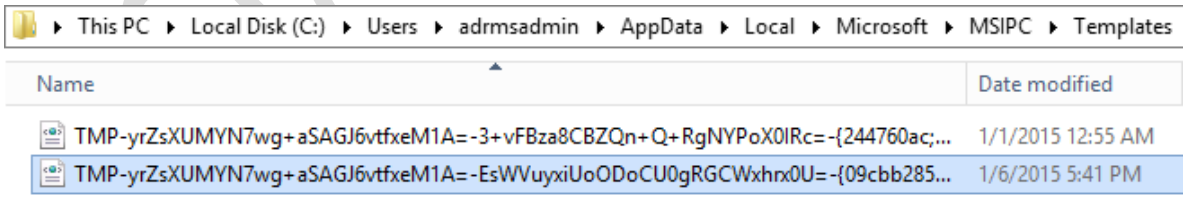


También es posible forzar la actualización de plantillas al dar clic derecho sobre la tarea y seleccionar **"Run"** para que ésta se ejecute inmediatamente.

6) A la hora indicada, 5:41, la tarea de actualización de plantillas se llevó a cabo, como se puede observar en la fecha de modificación de los archivos, generando un archivo XML para cada plantilla.



7) Copiar el archivo de la plantilla al directorio C:\Users\adrmsadmin\AppData\Local\Microsoft\MSIP\Templates, que Office revisará al abrir Word, PowerPoint o Excel. De esta forma ya no es necesario esperar 7 días para la actualización.



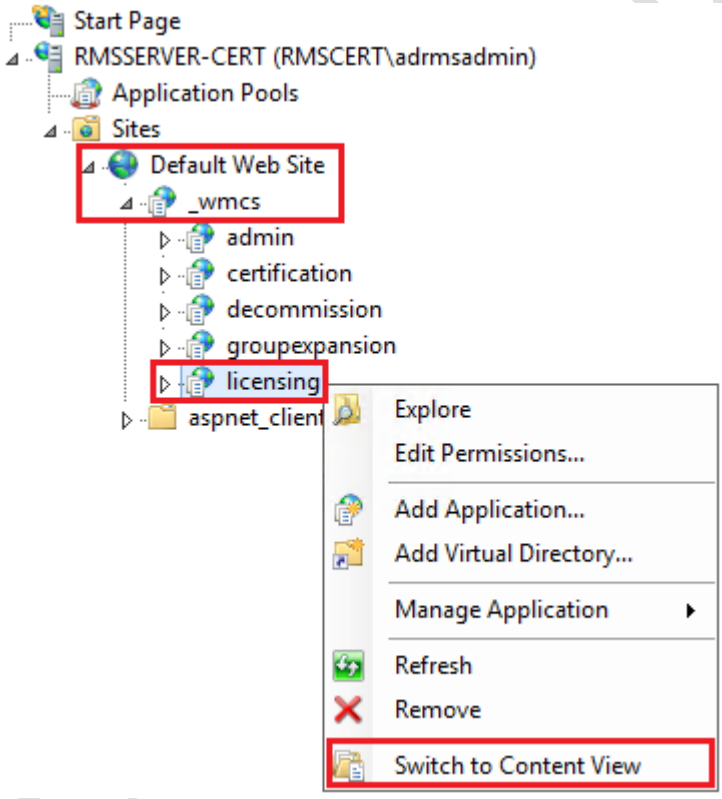
8) Ahora, al tratar de proteger un archivo de Word, PowerPoint o Excel, se observará también la plantilla recién creada.

3.9 Configuración de IIS para Windows ID

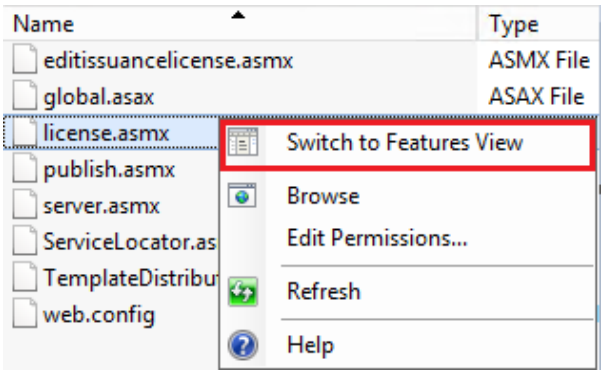
Por defecto, el sitio de RMS solicita autenticación Windows para poder hacer uso de los servicios. Ya que los usuarios con un Windows ID (correo de Hotmail, Windows Live, Outlook) no tienen una cuenta del dominio es necesario habilitar la autenticación anónima en el servicio de licencias para que puedan ver contenido protegido por RMS [11]. Para esto se deben seguir los siguientes pasos:

1) Abrir la consola de IIS. Del lado izquierdo, expandir el sitio web por defecto de la forma **"<Servidor>/Sites/Default Web Site/_wmcs/licensing"**.

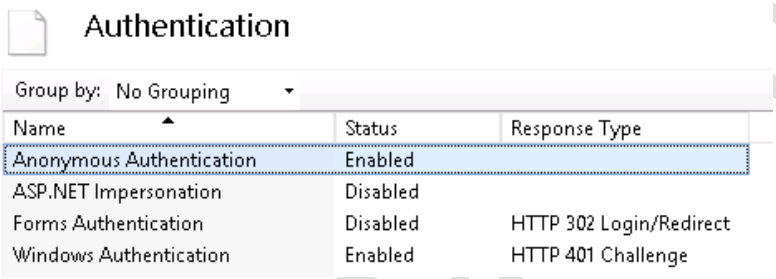
2) Dar clic derecho sobre **"licensing"** y seleccionar la opción **"Switch to Content View"**.



3) Seleccionar el archivo **"license.asmx"**, dar clic derecho sobre su nombre y seleccionar **"Switch to Feature View"**.



4) Dar doble clic en el icono **"Authentication"** y habilitar la autenticación anónima dando clic derecho y seleccionando **"Enable"**.



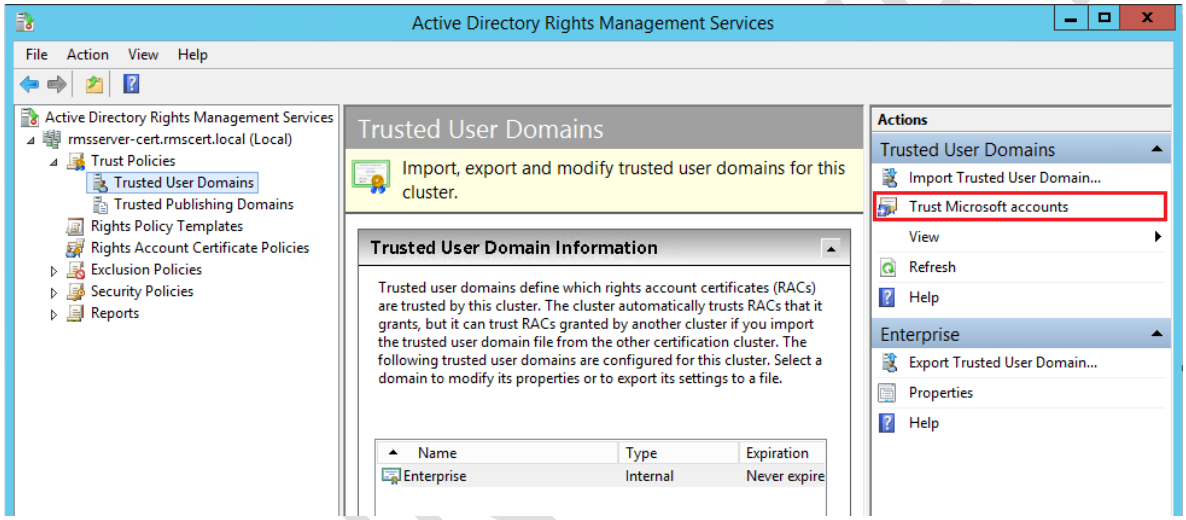
3.10 Configuración de cuentas de Microsoft en RMS

Una vez que se tiene el sitio web configurado para aceptar solicitudes de clientes sin cuenta del dominio se debe configurar AD RMS para que funcione con cuentas Microsoft o Windows ID. Para esto basta con agregar la confianza a ese tipo de cuentas.

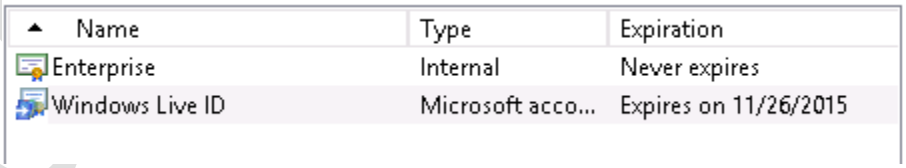
1) Abrir la consola de administración de AD RMS.

2) Ir a **"<Servidor>/Trust Policies/Trusted User Domains"**.

3) En el panel **"Actions"**, dar clic en **"Trust Microsoft accounts"**.



4) En el área de **"Trusted User Domains"**, verificar que aparece Windows Live ID como una entidad de confianza.

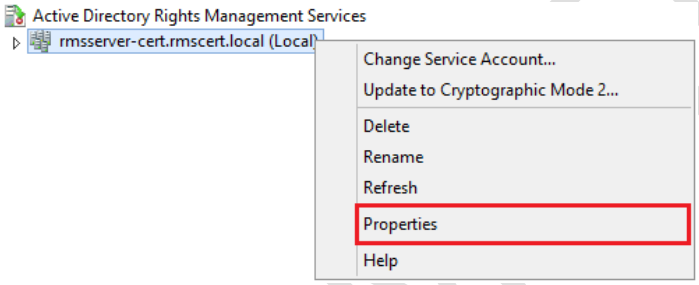


3.11 Configuración de Extranet

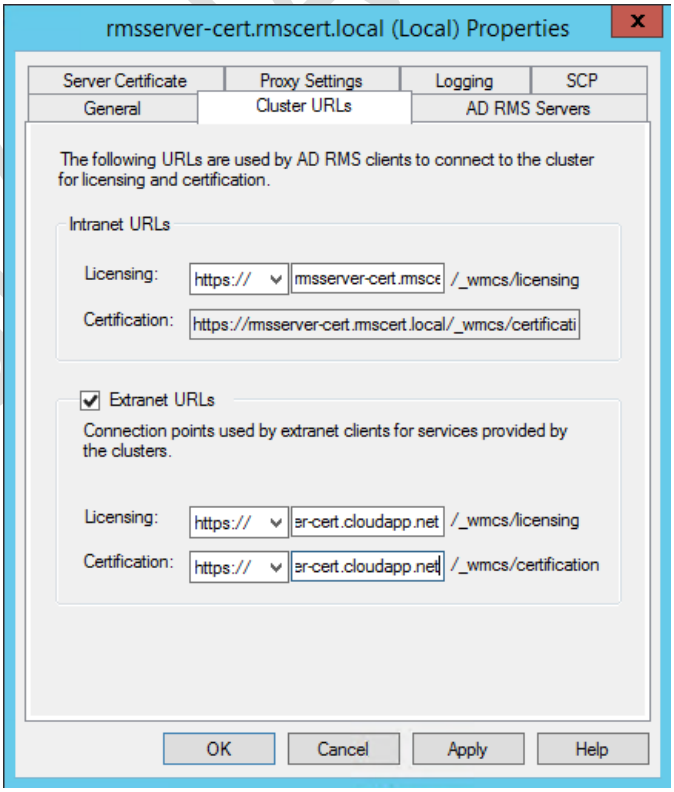
Para que usuarios fuera del dominio puedan hacer uso de AD RMS es necesario configurar una URL extranet, es decir, URLs desde donde nuestro servicio web de licencias puede ser visitado por Internet.

Debido a que nuestra máquina virtual está alojada en la nube es mucho más fácil habilitar el servicio de extranet, basta solo con indicar la URL asociada a la máquina virtual donde se ejecuta AD RMS. Es necesario que estén abiertos los puertos 443 y 80 de la máquina virtual en Azure.

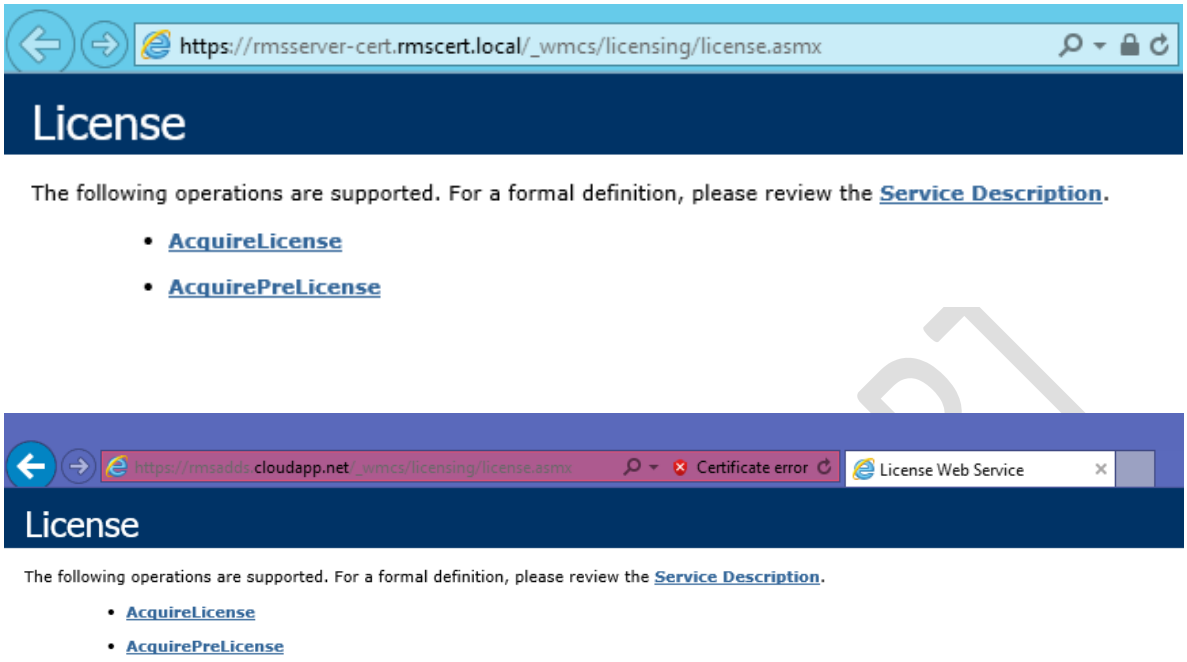
1) Dar clic derecho sobre el nombre del servidor RMS y después dar clic en **"Properties"** para abrir la ventana de propiedades.



2) Seleccionar la pestaña **"Cluster URLs"**, habilitar la opción **"Extranet URLs"**, indicar el protocolo HTTPS y la URL de Azure asociada a la máquina virtual. Dar clic en **"Apply"** y en **"OK"**.



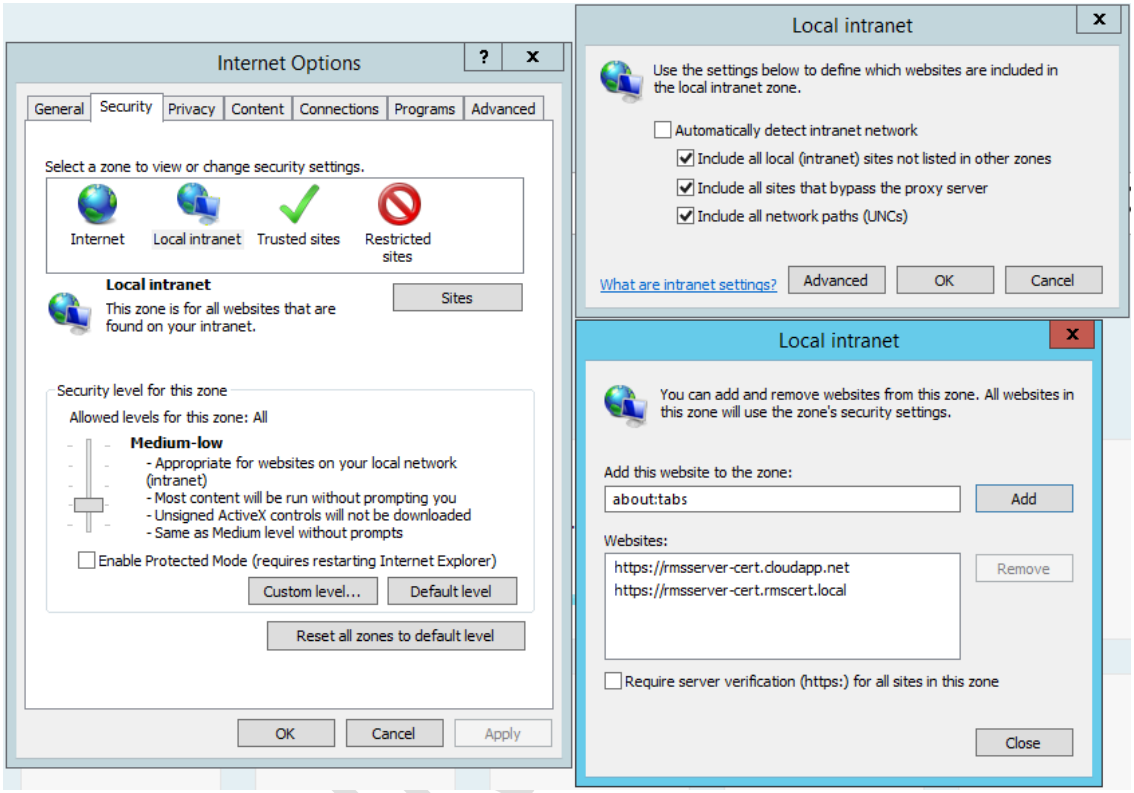
3) Verificar que ambas URLs pueden ser accedidas en el navegador.



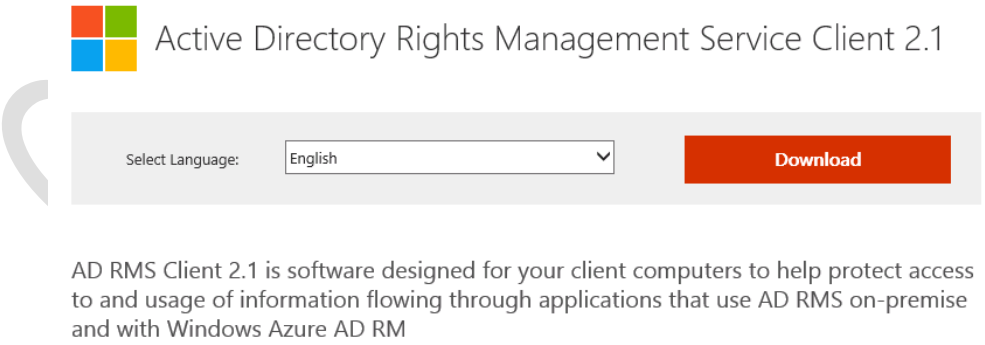
El mensaje de advertencia sobre el certificado se debe a que éste fue autofirmado cuando AD RMS se configuró. Para un servidor en producción se recomienda utilizar certificados firmados por una autoridad certificadora reconocida y, con esto, el mensaje de advertencia dejará de aparecer.

3.12 Configuración de AD RMS en equipos cliente del dominio

1) Se requiere agregar el sitio de RMS en la lista de sitios de la Zona de Intranet, esto puede hacerse desde las opciones de Internet Explorer: **"Tools"** > **"Internet Options"** > **"Security"** > **"Local Intranet"** > **"Sites"** > **"Advanced"** y se agrega el sitio.



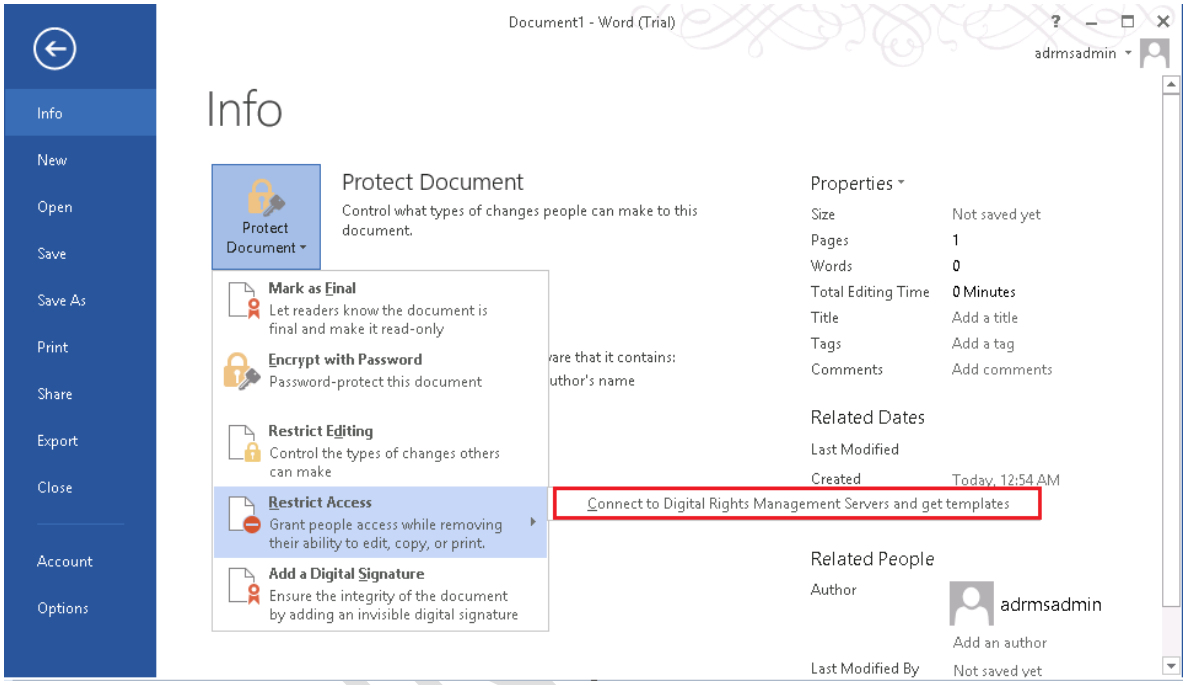
2) Instalar el cliente de AD RMS versión 2.1 en el equipo



3) Teniendo el cliente instalado y el sitio de RMS en la zona de intranet, se puede hacer uso del servidor. Se debe conectar el producto de Office con el servidor para que el cliente AD RMS descargue las plantillas y que éstas puedan ser utilizadas para proteger el contenido del archivo.

3.13 Establecer restricciones RMS en un archivo

Abrir una aplicación de Microsoft Office, por ejemplo Word 2013 [12]. En **"Info"**, hacer clic en **"Proteger documento"** (Protect Document) y, a continuación, hacer clic en **"Acceso restringido"** (Restricted Access) y después en **"Connect to Digital Rights Management Servers and get Templates"**.



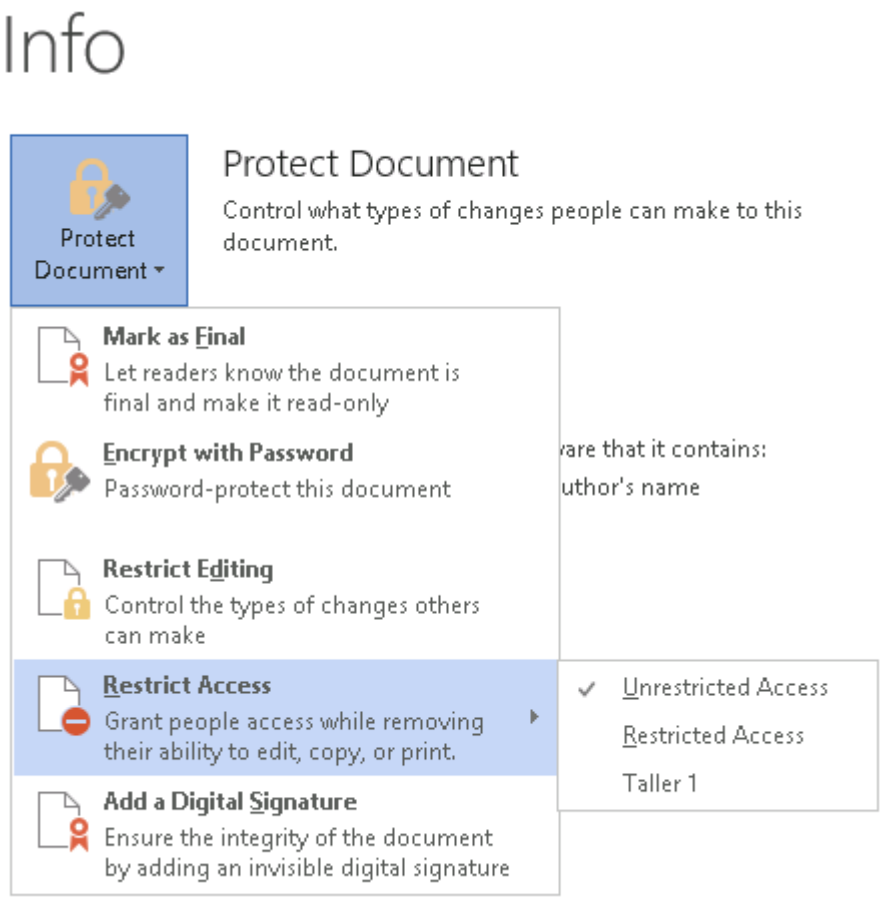
Al finalizar esta operación ya se podrá utilizar la funcionalidad de IRM (Information Rights Management) para proteger documentos y compartirlos con otros usuarios.

Para aplicar una plantilla a un archivo, abrir el documento de Word y continuar el manual según la versión de Office [13] [14].

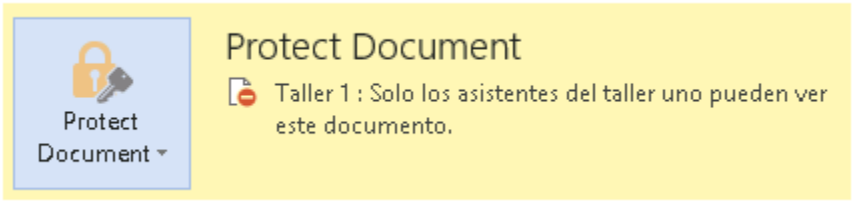
Microsoft Office 2013

1) Ir a **"File"** > **"Info"** > **"Protected Document"** > **"Restrict Access"** > **"Restricted Access"**.

2) En la ventana de permisos que se abre verificar que esté marcada la opción **"Restrict permission to this document"**. Escribir la(s) dirección(es) de correo electrónico de los usuarios que puedan leer o modificar el documento. Dar clic en **"OK"**.



3) Una vez que el documento esté protegido con la plantilla seleccionada, se mostrará un mensaje como el siguiente:



Microsoft Office 2010

4) Ir a **"File"** > **"Info"** > **"Protected Document/Workbook/Presentation"** > **"Restrict Permission by People > Restricted Access"**.

5) En la ventana de permisos que se abre verificar que esté marcada la opción **"Restrict permission to this document"**. Escribir la(s) dirección(es) de correo electrónico de los usuarios que puedan leer o modificar el documento. Dar clic en **"OK"**.

Microsoft Office 2007

6) Ir a **"File**" > **"Prepare"** > **"Restrict Permission"** > **"Restricted Access"**.

7) En la ventana de permisos que se abre verificar que esté marcada la opción **"Restrict permission to this document"**. Escribir la(s) dirección(es) de correo electrónico de los usuarios que puedan leer o modificar el documento. Dar clic en **"OK"**.

Se puede guardar el documento protegido en la carpeta compartida **"Public"** que se creó en pasos anteriores para que pueda ser accedido por otros usuarios.

4 PROTOCOLO DE PRUEBAS DE AD RMS

A continuación se ejemplifica paso a paso la creación de una plantilla donde se asignan permisos específicos a algunos usuarios, la protección de un documento de Word y el funcionamiento del servidor en dos casos: cuando el documento es abierto por un usuario con permisos y cuando es abierto por un usuario sin permisos. A grandes rasgos, los pasos son los siguientes:

1) Creación de usuarios y grupos de prueba. Ver sección 2.4.
2) Creación de un directorio compartido de red
3) Creación de plantilla. Ver sección 3.7.
4) Publicación de plantilla. Ver sección 3.8.
5) Configuración de equipos cliente en el dominio. Ver sección 3.12.
6) Establecer restricciones RMS en un archivo. Ver sección 3.13.

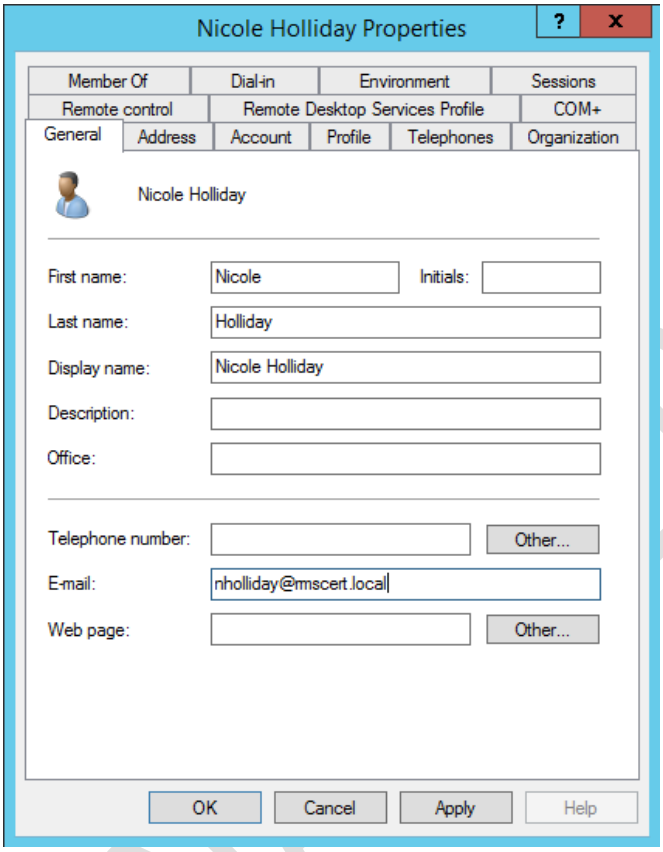
4.1 Creación de usuarios y grupos de prueba

En la máquina virtual con Active Directory instalado, que en este caso es el servidor SQL crear los siguientes usuarios y grupos para realizar pruebas una vez que la instalación de RMS haya finalizado [2]. Abrir **"Active Directory Users and Computers"**, desplegar las opciones del dominio, dar clic derecho en **"Users"** y seleccionar **"New"** > **"Users"**. Para crear los grupos Employees, Marketing, Engineering y Finance, dar clic derecho en **"Users"** y seleccionar **"New"** > **"Group"**.

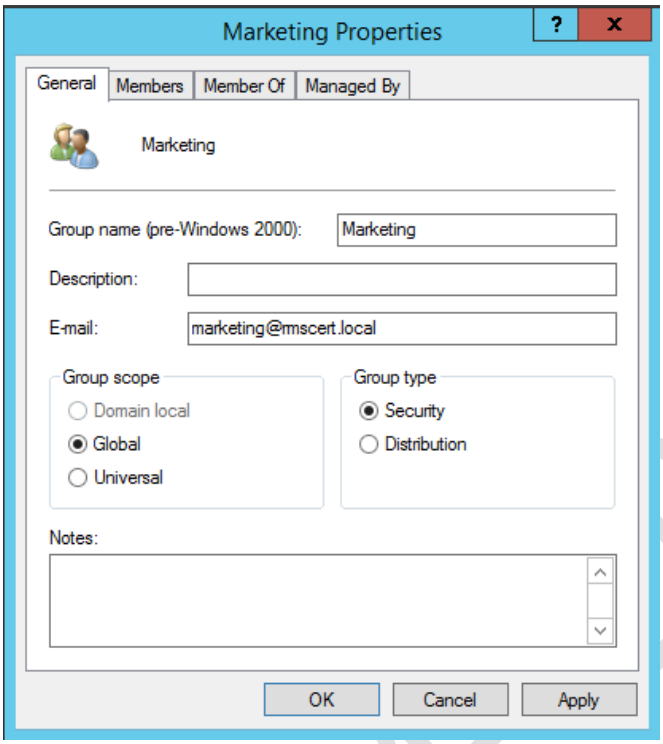
Para agregar usuarios a un grupo, dar doble clic en el nombre del grupo, seleccionar la pestaña **"Members"**, dar clic en el botón **"Add…"**, escribir el nombre del usuario que se desee agregar, dar clic en **"Check Names"** y aplicar los cambios. No es necesario agregar un usuario a la vez a un grupo, en la ventana **"Select Users, Contacts, Computers, Service Accounts, or Groups"** es posible escribir varios nombres, separados por **";"** y dar clic al botón **"Check names"** para validarlos al mismo tiempo.

Nombre de Usuario	Cuenta de Usuario	Dirección E-mail	Grupo
Nicole Holliday	NHOLLIDA	nholliday@rmscert.local	Employees, Finance
Limor Henig	LHENIG	usuario_lhenig@outlook.com	Employees, Marketing
Stuart Railson	SRAILSON	cert@outlook.com	Employees, Engineering

Para añadir una dirección de correo electrónico a un usuarios, dar doble clic en su nombre y escribir el correo en el campo **"E-mail"** de la pestaña **"General"**.



Los grupos también deben tener dirección de correo electrónico. Para añadirla, dar doble clic sobre el nombre del grupo escribir el correo en el campo **"E-mail"** de la pestaña **"General"**.



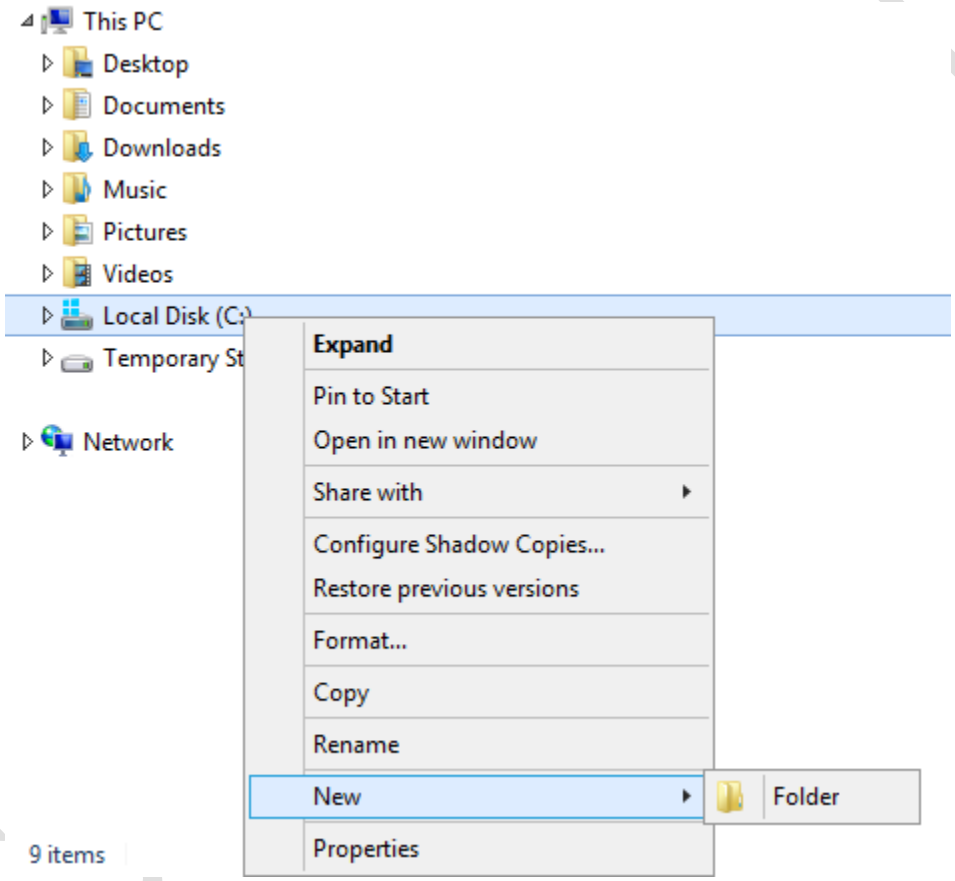
La siguiente tabla contiene las direcciones de correo electrónico de cada grupo.

Grupo	Dirección E-mail
Finance	finance@rmscert.local
Marketing	marketing@rmscert.local
Engineering	engineering@rmscert.local
Employees	employees@rmscert.local

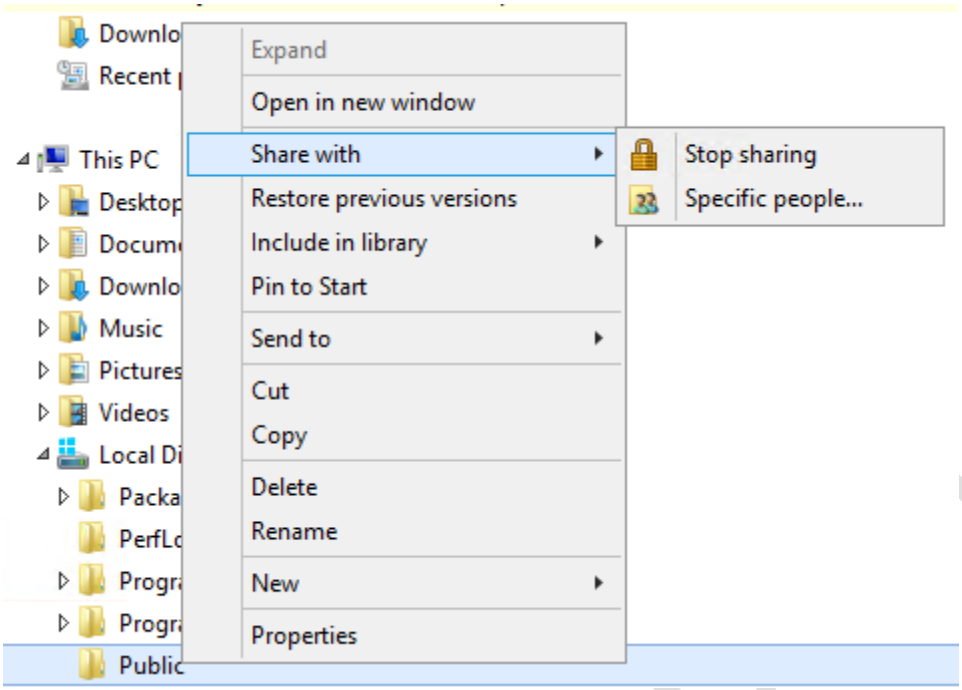
4.2 Creación de un directorio compartido de red

En el servidor SQL crear un directorio compartido de red donde los usuarios que sean parte del dominio puedan tener acceso a los documentos guardados.

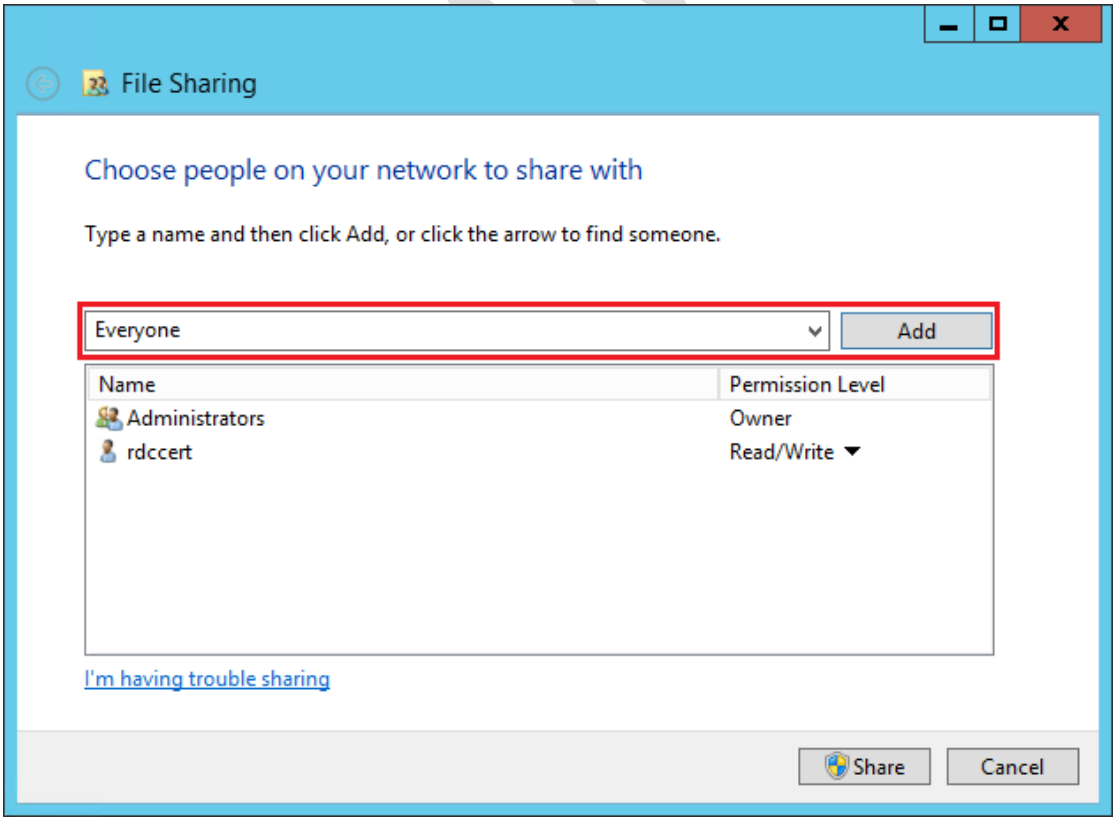
1) Iniciar sesión con una cuenta que tenga permisos de administrador y que sea parte del dominio.
2) Abrir el Explorador de Windows y dar clic derecho sobre el disco local C, seleccionar **"New"** > **"Folder"**.
3) Nombrar el nuevo directorio como **"Public"**.



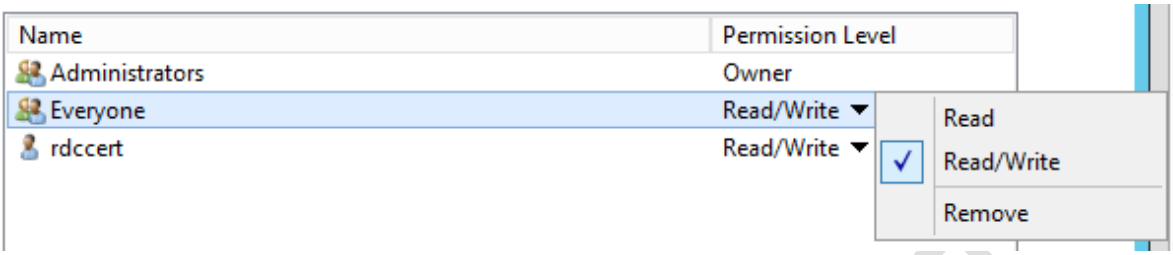
4) Dar clic derecho sobre el fólder **"Public"** y seleccionar **"Share with"** > **"Specific people"** para compartirlo con los usuarios que se especifiquen en los siguientes pasos.



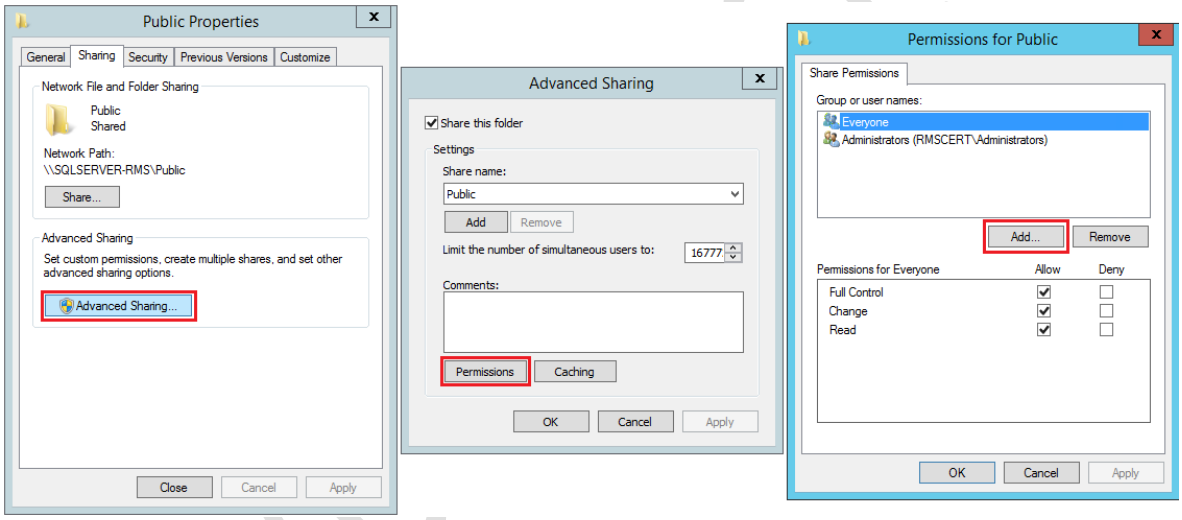
5) A continuación se abre el asistente para compartir archivos. Dar clic en la flecha de la caja de selección y elegir **"Everyone"**. Dar clic en el botón **"Add"**.



6) De la lista de usuarios y dar clic en la flecha del nivel de permisos (permission level) para el grupo **"Everyone"**. Seleccionar **"Read/Write"**, dar clic en **"Share"** y por último en el botón **"Done"**.



7) En el Explorar de Windows, dar clic derecho sobre la carpeta **"Public"** y seleccionar **"Properties"**. En la pestaña **"Sharing"**, dar clic en **"Advanced Sharing"** > **"Permissions"** > **"Add"**.



8) En la ventana "**Select Users, Computers, Service Accounts, or Groups**" escribir **"Domain Users"**, dar clic en **"Check Names"** y al final en **"OK"**.

9) En la ventana **"Permissions for Public"** seleccionar **"Domain Users"** y marcar la casilla **"Full Control"** en la columna **"Allow"** para que los usuarios del dominio tengan todo el control del contenido de la carpeta **"Public"**.

10) Clic en **"OK"** para cerrar las dos ventanas superiores y **"Close"** para cerrar el asistente de configuración de los archivos compartidos.

4.3 Crear plantilla

En la consola de RMS, en el panel del lado izquierdo, desplegar las opciones en el nombre del servidor y dar clic en **"Rights Policy Templates"**. En el panel de acciones, del lado derecho, dar clic en **"Create Distributed Rights Policy Template"**.

En el asistente seleccionar las siguientes opciones o añadir los siguientes datos, según corresponda:

- Add Template Identification Information
  - Language: Spanish (Mexico)
  - Name: Plantilla para asistentes al congreso
  - Description: Los documentos sólo pueden leerse
- Add User Rights. En este paso agregar el correo del usuario lhenig creado en pasos anteriores.
  - E-mail: usuario_lhenig@outlook.com
  - Rights for cert@outlook.com: View
- Specify Expiration Policy
  - Content expires: Never expires
  - Use license expiration. Expires after the following duration (days): 3
- Finish

4.4 Publicar la plantilla

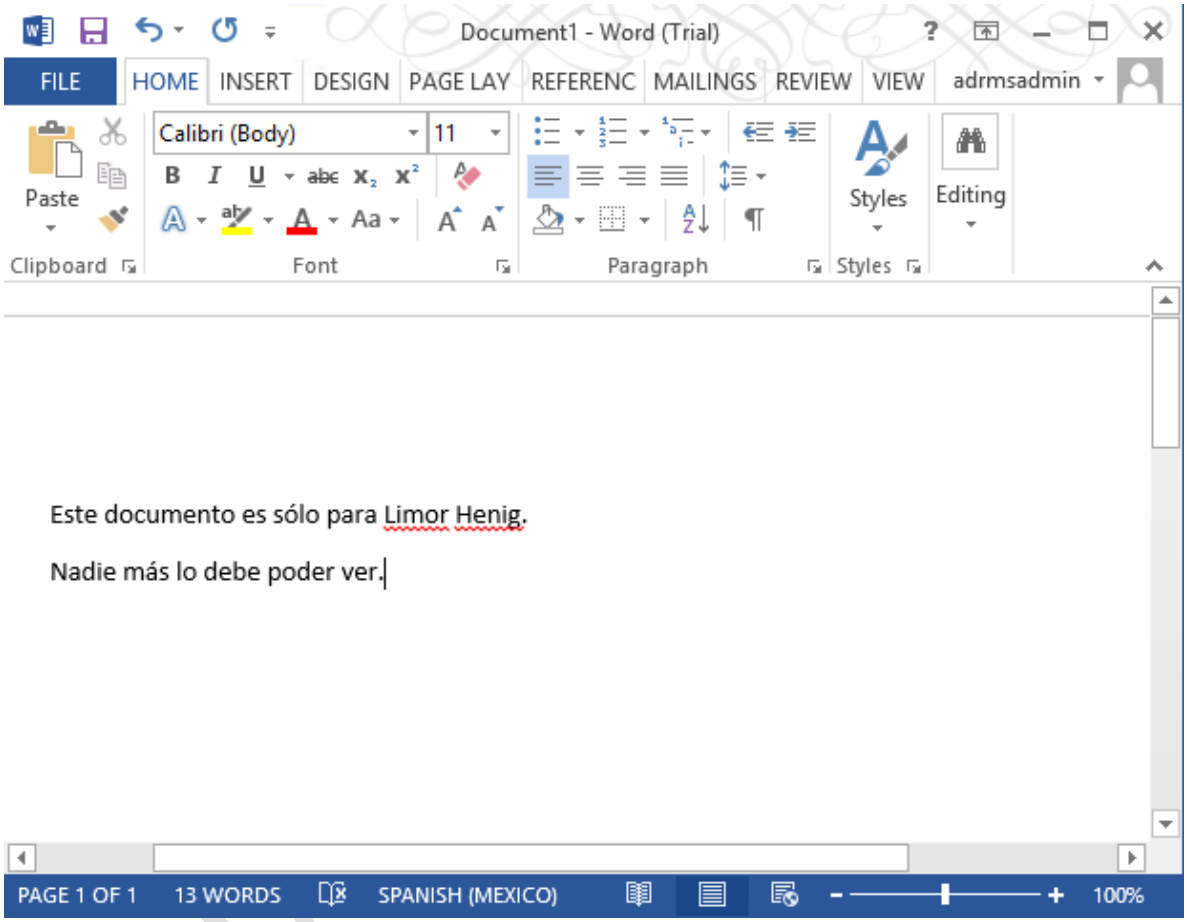
En pasos anteriores se vio cómo modificar la tarea de actualización de plantillas en el programador de tareas para que la carpeta se actualizara de forma automática en el menor tiempo posible. Esto significa que, una vez creada la plantilla, el usuario puede esperar 5 minutos, o menos, para que su plantilla aparezca configurada y publicada en el directorio **C:\Users\adrmsadmin\AppData\Local\Microsoft\DRM\Templates**.

Una vez allí, simplemente debe copiar el archivo de su plantilla al directorio **C:\Users\adrmsadmin\AppData\Local\Microsoft\MSIP\Templates**, donde se guardan las plantillas de permisos para los archivos de Microsoft Office. O esperar 7 días a que se actualice la carpeta automáticamente.

4.5 Protección de documento de Word

1) Abrir Word 2013 y crear un nuevo documento.

2) Escribir algunas líneas y guardar.



3) Si es la primera vez que se habilita la funcionalidad de IRM, dar clic en **"File"** > **"Info"** > **"Protect Document"** > **"Restrict Access"** > **"Restricted Access"**. Marcar la casilla **"Restricted permission to this document"**.

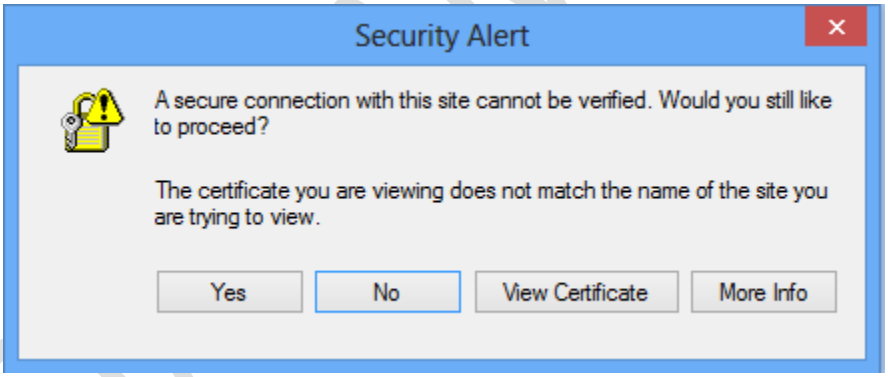
   De lo contrario, dar clic en **"File"** > **"Info"** > **"Restrict Access"** y seleccionar una plantilla. Para este ejemplo se eligió **"Plantilla para asistentes al congreso"**, creada en el punto 5.1.

4) A partir de ahora el archivo estará protegido con los permisos especificados en la plantilla.

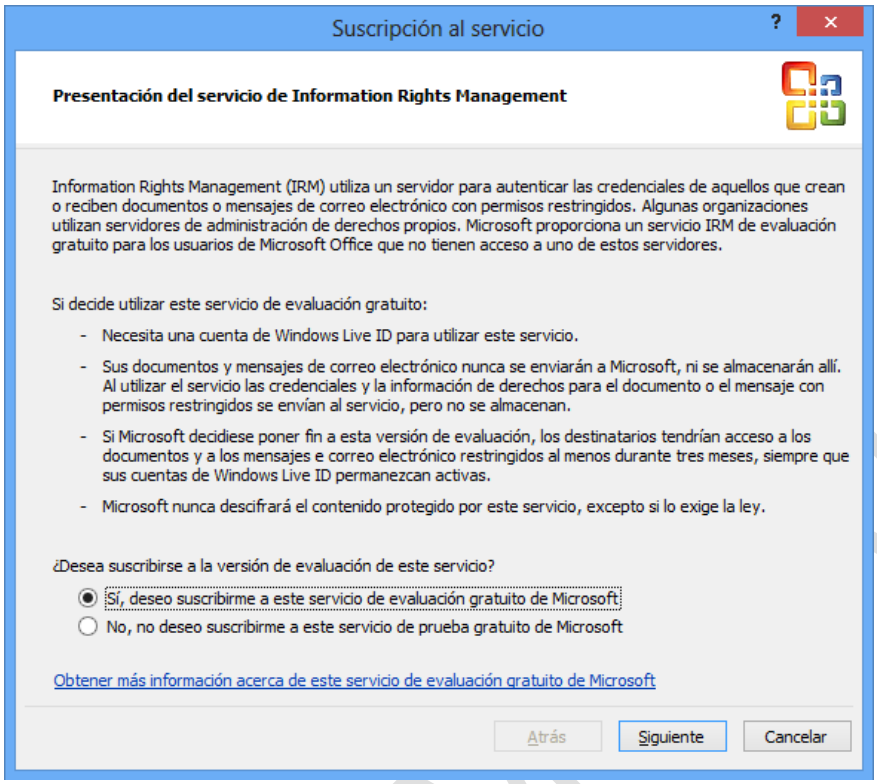
4.6 Apertura de archivo protegido

Al abrir el archivo se muestra una alerta de seguridad indicando que se necesita una conexión segura con autenticación a un servidor. También indica que no se confía en el emisor del certificado, esto debido a que el certificado es autofirmado.

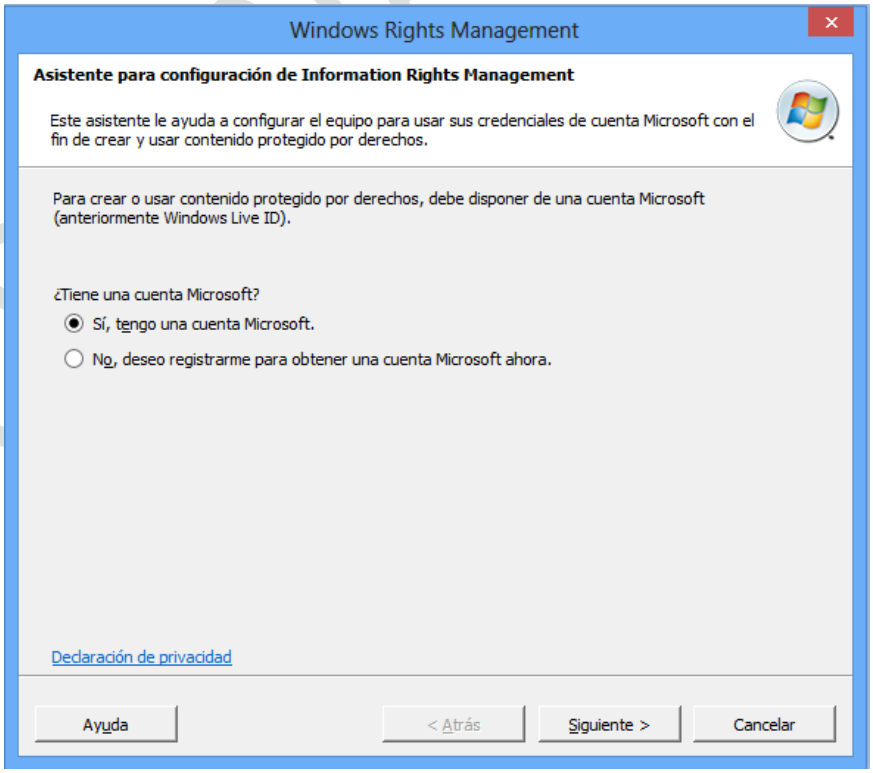
Al presionar **"Sí"**, se muestra otro mensaje de advertencia preguntando al usuario si desea abrir el archivo aún cuando no se puede comprobar que se estableció una conexión segura con el servidor.



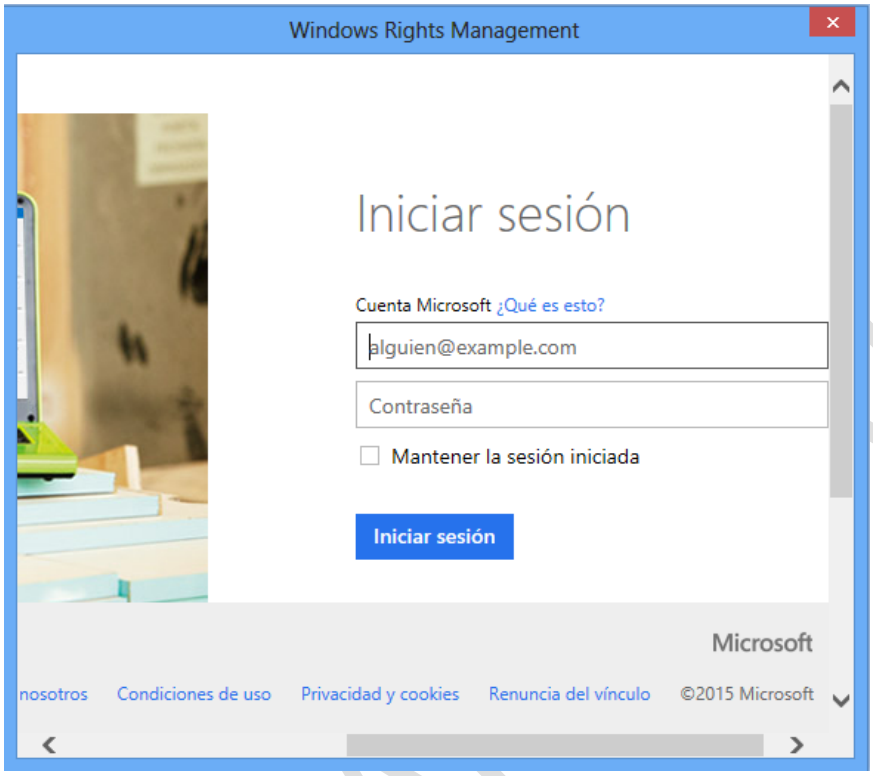
Posteriormente se muestra una ventana de suscripción al servicio gratuito de IRM para poder autenticar las credenciales de los usuarios que reciben documentos protegidos. Seleccionar **"Si, deseo suscribirme a este servicio de evaluación gratuito de Microsoft"**. Dar clic en el botón **"Siguiente"**.

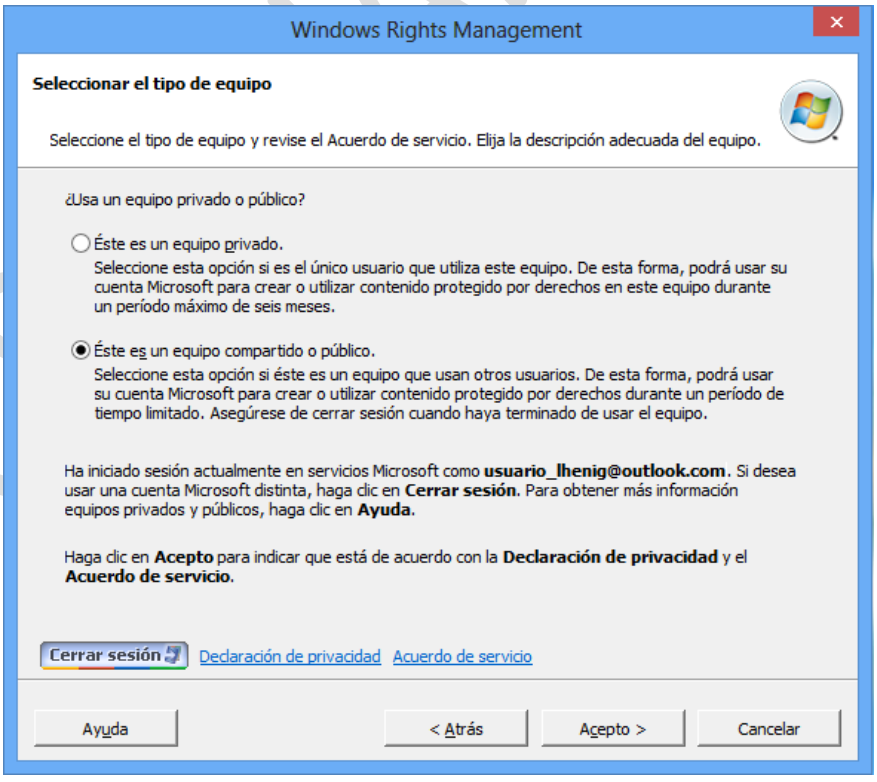


El asistente pregunta al usuario si ya cuenta con una cuenta de Microsoft. En este caso, el usuario Limor Henig ya tiene una cuenta de Outlook, por lo que se selecciona la opción **"Si, tengo una cuenta Microsoft"**. Dar clic en **"Siguiente"**.



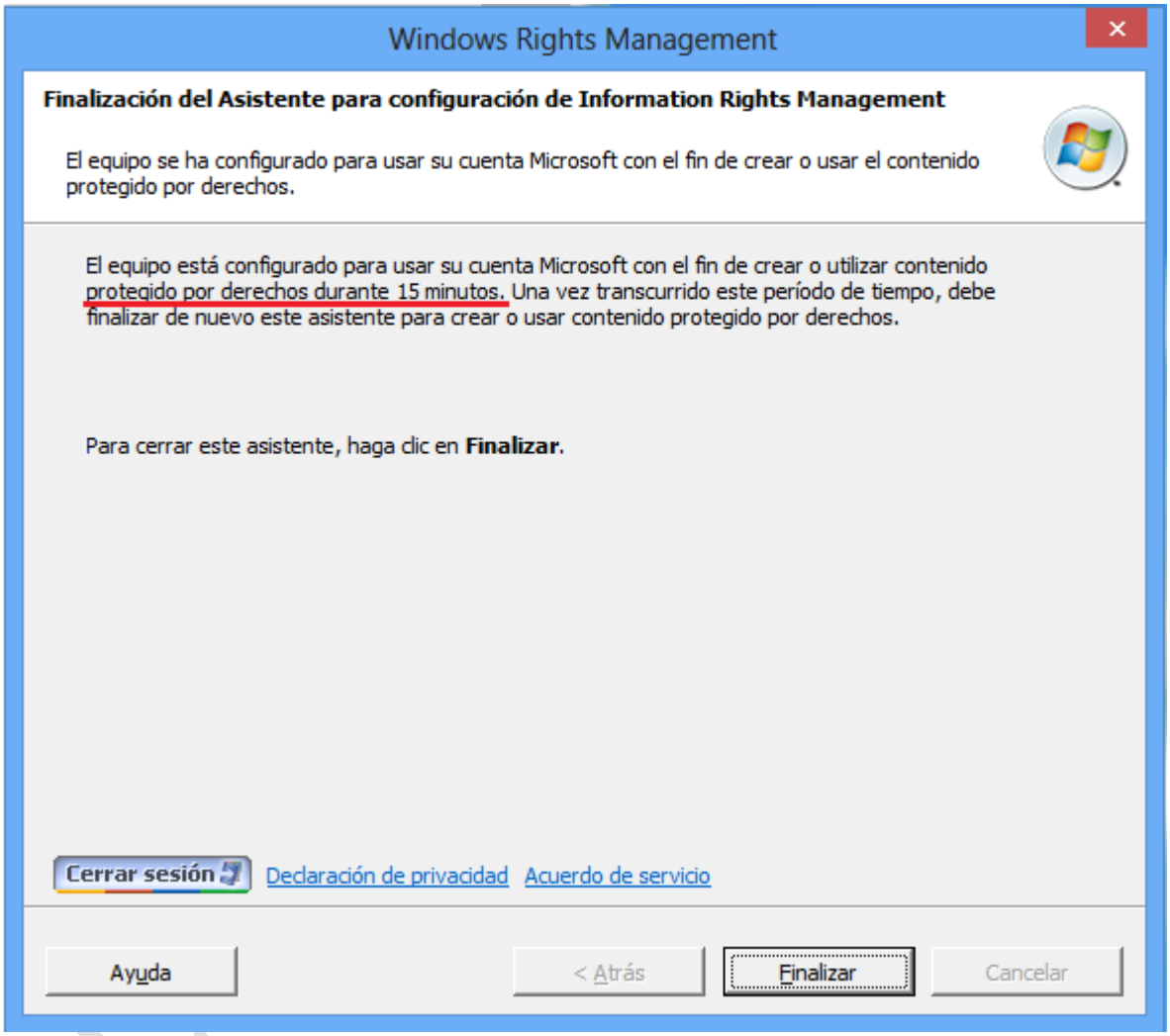
Iniciar sesión con la cuenta de Microsoft y su contraseña. En este ejemplo la cuenta del usuario Limor Henig es usuario_lhenig@outlook.com.





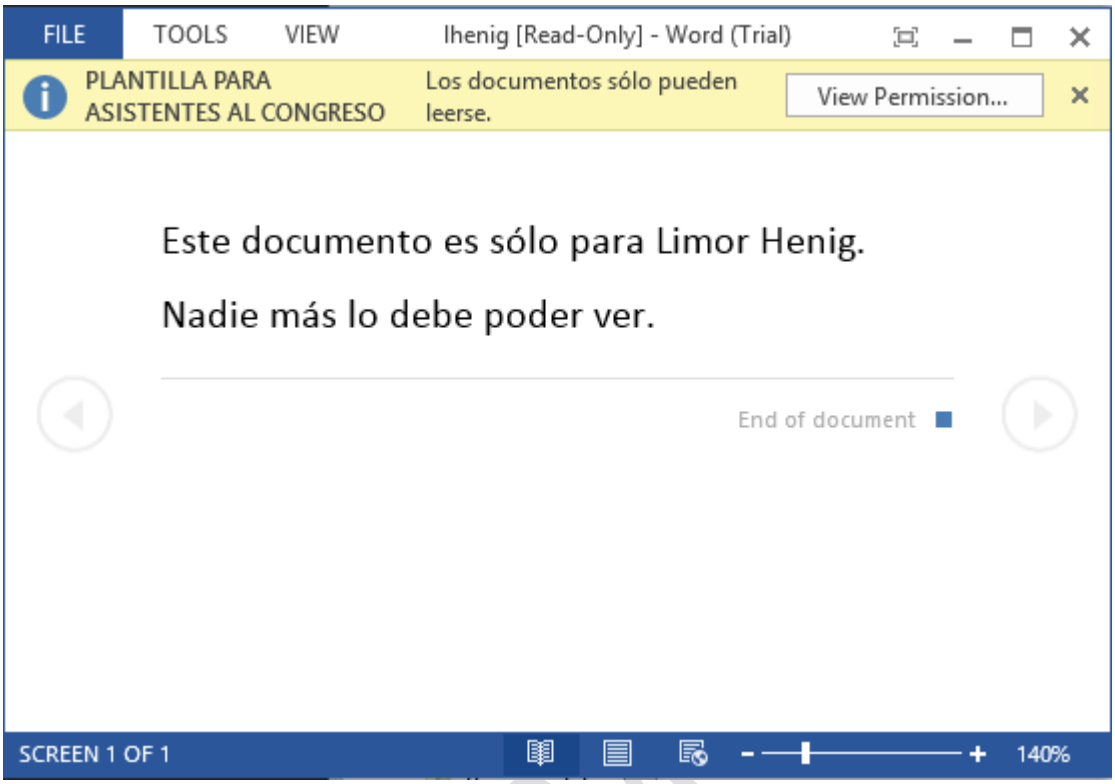
A continuación pregunta si el equipo es público o privado. Es importante tener en cuenta que si se elige la opción "privado", el certificado se va a almacenar en el equipo y va a seguir autenticando con las mismas credenciales proporcionadas, es decir, no se puede desasociar el equipo.

Por el contrario, si se elige la opción "público", el documento funcionará con esa sesión de autenticación durante 15 min, después tendrá que volver a escribir las credenciales de su cuenta Microsoft.

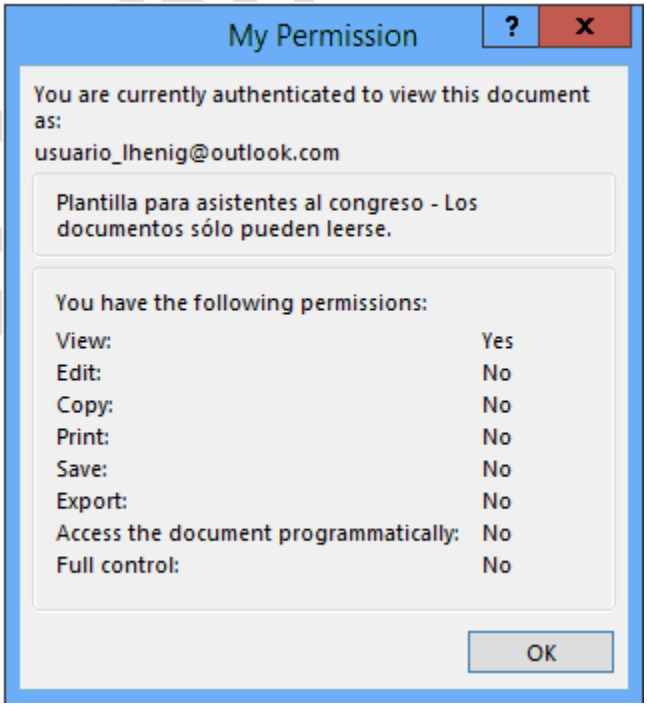


Una vez que el usuario se autentique exitosamente, podrá acceder al contenido del archivo, como se muestra en la siguiente imagen.

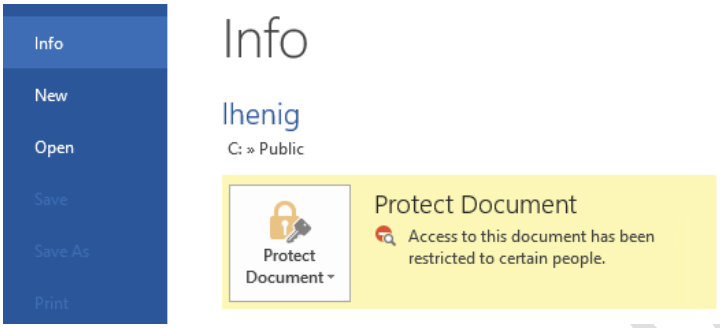
En la parte superior de la ventana se muestra un mensaje donde se menciona el nombre de la plantilla y los permisos que el usuario tiene. Puesto que en la plantilla sólo se asignaron permisos para ver el documento, el mensaje dice "Los documentos sólo pueden leerse".



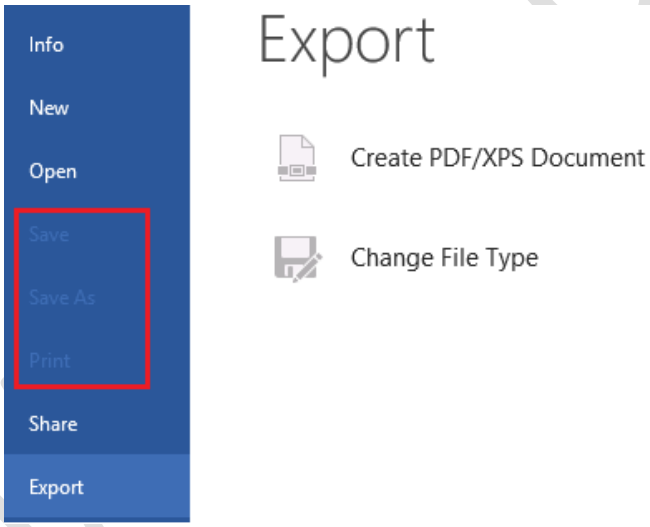
Al dar clic en el botón **"View permission"** se abre una ventana donde se especifica la cuenta con la que se autenticó el usuario, el nombre de la plantilla y las acciones que tiene permitidas.



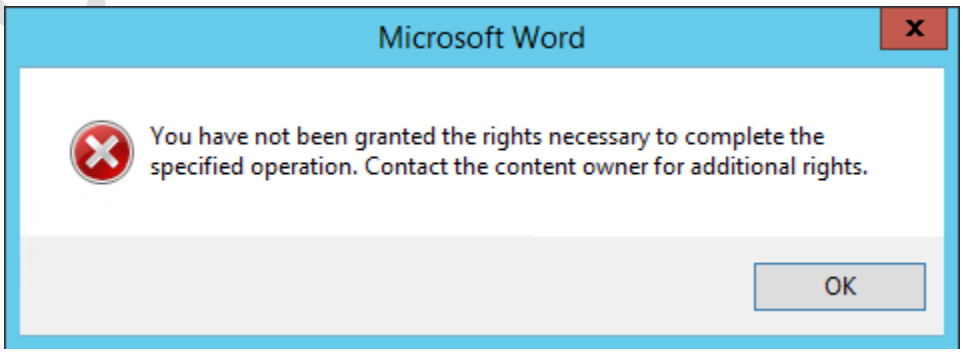
Para confirmar que el archivo está protegido contra acciones como guardar, imprimir o exportar el documento, dar clic en **"File"**. Al seleccionar **"Info"** debe mostrarse el mensaje de documento protegido, como se muestra en la siguiente imagen:



Las opciones "Save" y "Save As" para guardar los cambios en el archivo, "Print" para imprimirlo, así como "Create PDF/XPS Document" y "Change File Type" para exportar el archivo, deben estar deshabilitadas.



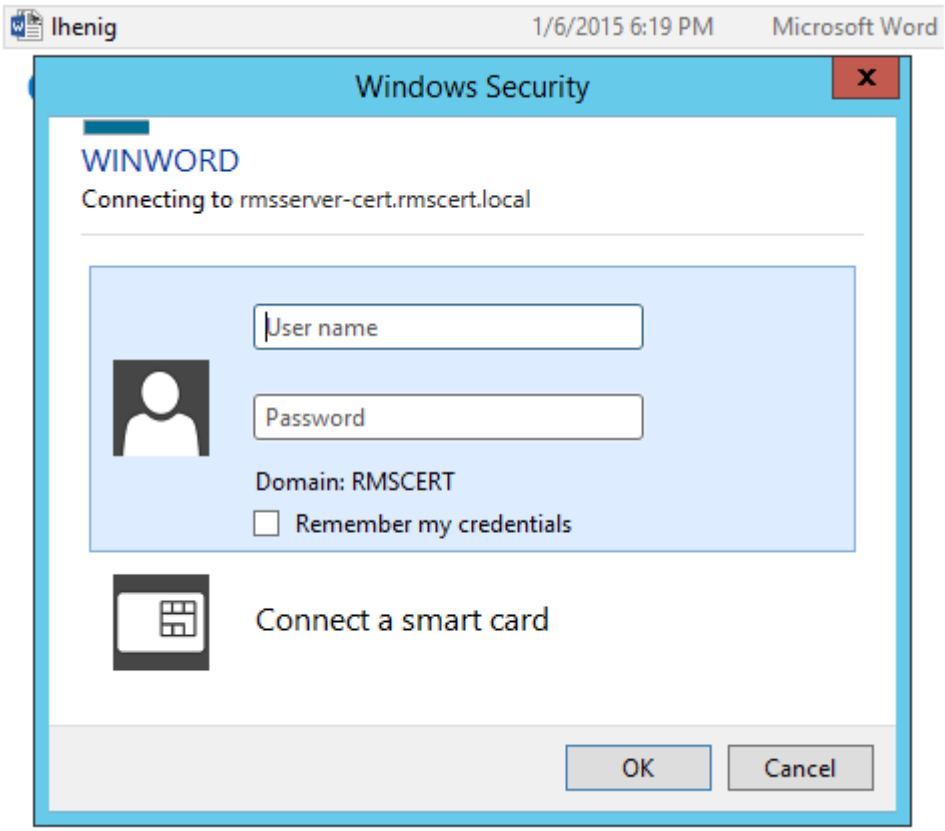
Por otro lado, si un usuario, cuyo nombre o correo electrónico no está en la lista de permisos de la plantilla, trata de abrir el archivo, se muestra el siguiente mensaje:



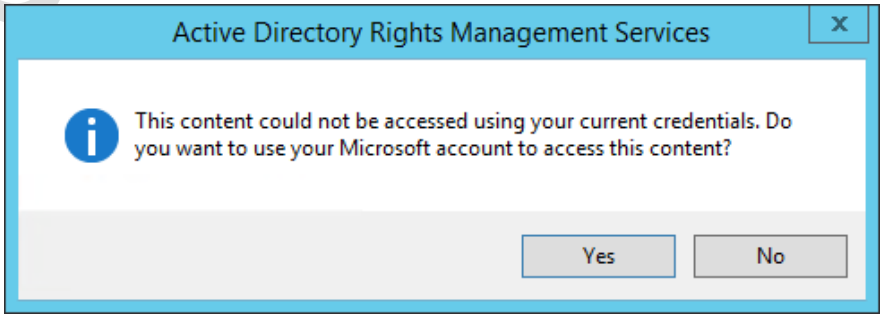
- **Autenticación como usuario del dominio**

En el caso de equipos unidos al dominio, es posible iniciar sesión con las credenciales de la cuenta, siempre que ésta se encuentre en la lista de usuarios o grupos permitidos.

Si el equipo no está en el dominio y al tratar de abrir el documento de Word se muestra una ventana que pide credenciales para autenticarse en éste, basta con dar clic en el botón **"Cancel"** para poder iniciar sesión con un correo electrónico de Microsoft.



Al hacerlo se abre otra ventana con el siguiente mensaje, donde le preguntan al usuario si quiere utilizar su cuenta de Microsoft para tener acceso al contenido. Dar clic en **"Yes"**.



4.7 Problemas de conexión al servidor RMS desde un equipo cliente

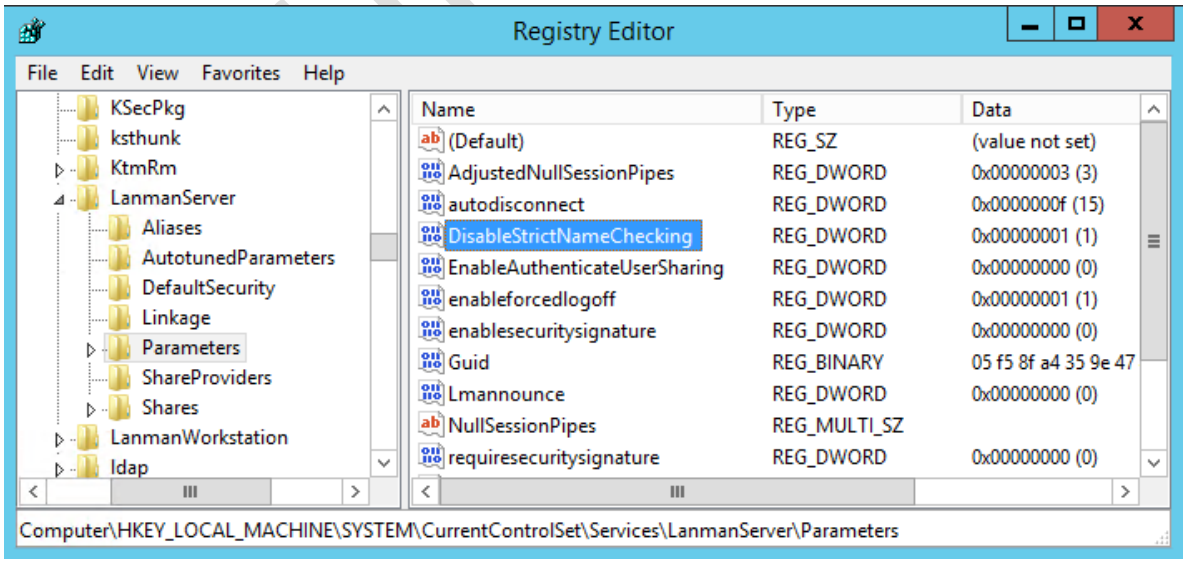
A continuación se mencionan algunos procedimientos que se pueden seguir si en un equipo cliente, no unido al dominio, se muestra un mensaje de error indicando que la conexión al servidor RMS no fue posible: “This service is temporarily unavailable. Ensure that you have connectivity to this server. This error could be because you are working offline, your proxy settings are preventing your connection, or you are experiencing intermittent network issues”.

- **Solución 1**

“Strict name checking” es el nombre que se le da a la medida de seguridad implementada por Microsoft para permitir a un servidor responder sólo a su nombre de equipo. Al deshabilitar esta opción, los servicios e instancias responden al servidor aún cuando el nombre del equipo es distinto al configurado inicialmente. En este caso, la URL de IIS no coincide con el nombre del servidor, lo que causa conflictos con el servicio.

Para solucionar esto se recomienda agregar el siguiente valor a la llave de registro **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters** [15] [16] [17]:

Nombre del valor (Name): DisableStrictNameChecking
Tipo de datos (Type): REG_DWORD
Base: Decimal
Valor (Data): 1



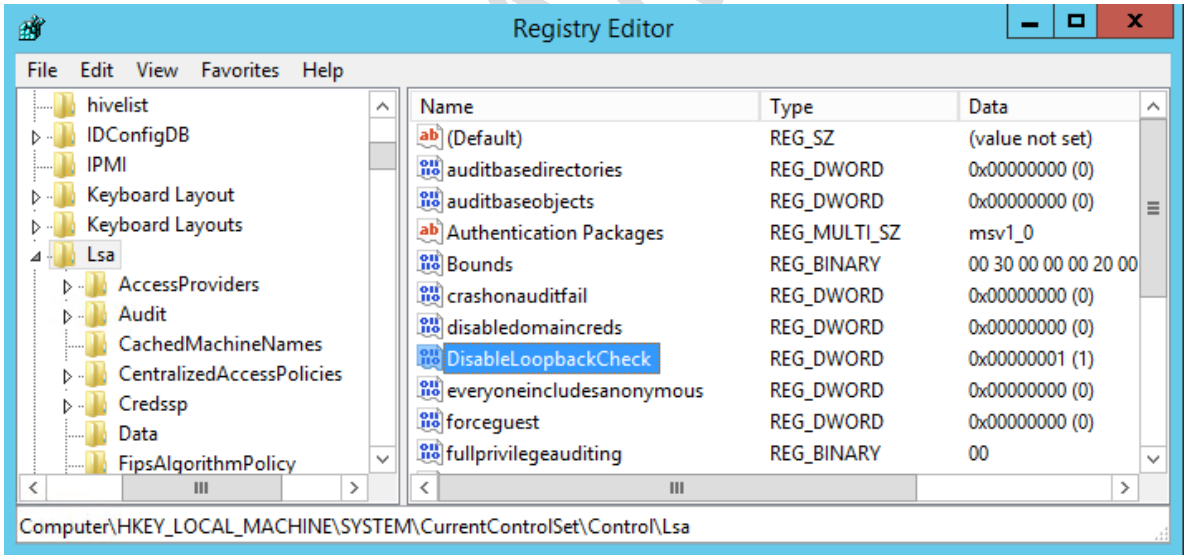
Para que los cambios tengan efecto es necesario reiniciar el equipo.

- **Solución 2**

De forma predeterminada IIS sólo permite autenticar usuarios en los sitios web que aloja de forma local si el sitio tiene el mismo nombre que el equipo, por lo que si un sitio alojado en IIS requiere autenticación y se trata de acceder a él directamente en el servidor IIS, el servicio entra en un bucle, deja de aceptar conexiones y los usuarios no se pueden autenticar [18].

Esto debido a que Windows Server 2012 contiene una característica de seguridad de comprobación de bucles invertidos [19] diseñada para ayudar a evitar los ataques de reflexión del equipo; que consiste en enviar a un equipo una gran cantidad de mensajes como si procedieran de otro equipo y fueran legítimos [20]. Por tanto, se producen errores en la autenticación si el FQDN (Fully Qualified Domain Name) o el encabezado del host no coinciden con el nombre del equipo local.

Para solucionar esto se puede modificar la llave de registro que verifica desde dónde se está accediendo al sitio. Abrir regedit y en el editor del registro buscar la siguiente clave: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**. Dar clic derecho sobre **"Lsa"**, seleccionar **"New"** > **"DWORD"**. Escribir **"DisableLoopbackCheck"**. Por último dar clic derecho en el valor recién creado y seleccionar **"Modify"**. En "Base" seleccionar **"Decimal"** y en "Value data" escribir **1**.



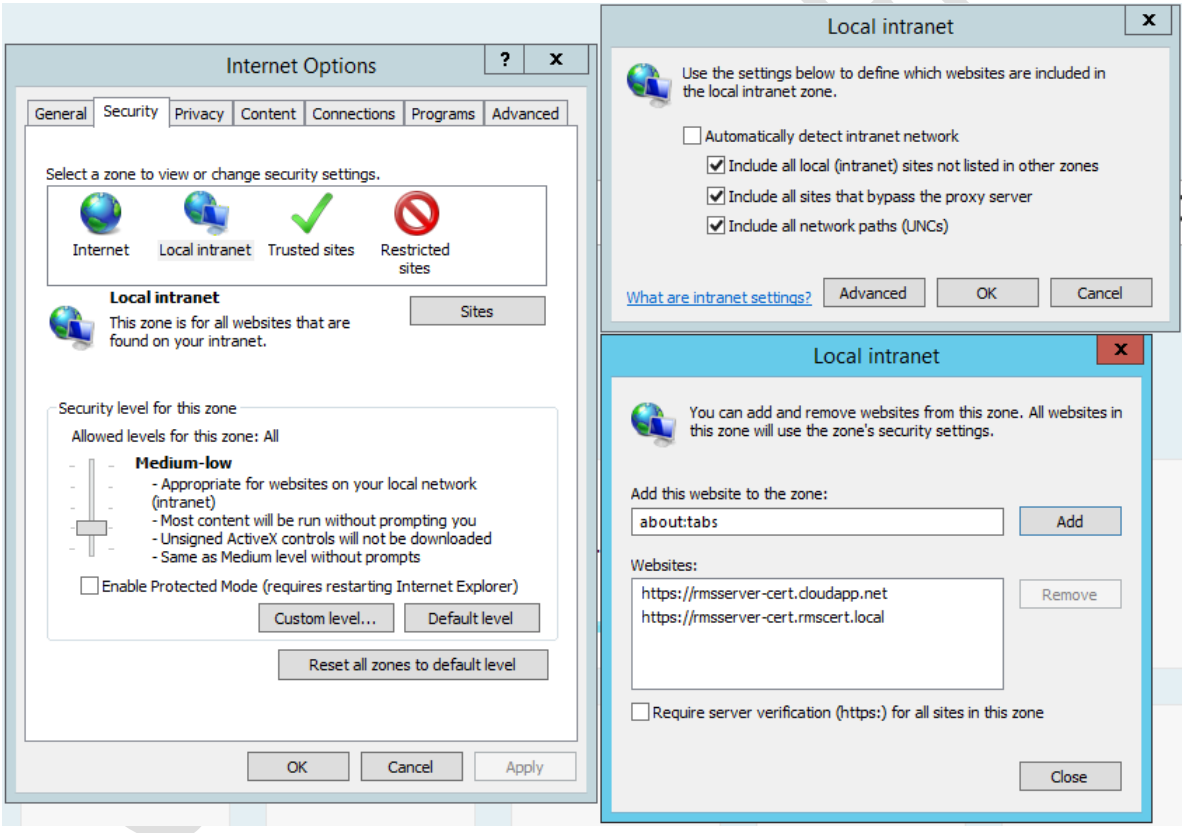
Para que los cambios tengan efecto es necesario reiniciar el equipo.

- **Solución 3**

En ocasiones el problema puede estar relacionado con la intranet y la configuración de ésta en Internet Explorer [21] [22].

Abrir el navegador y presionar **Ctrl + H** o dar clic en el ícono de herramientas  y después en **"Internet Options"**. Seleccionar **"Security"** > **"Local Intranet"** y dar clic en el botón **"Sites"**. Verificar lo siguiente:

- El nivel de seguridad en **"Local intranet"** debe estar en **"Medium-low"**.
- La opción **"Include all sites that bypass the proxy server"** en la ventana de sitios de Intranet debe estar seleccionada.
- En la ventana **"Local Intranet"** dar clic al botón **"Advanced"** y verificar que en la lista se encuentre la URL del servidor AD RMS. De lo contrario, agregarla a la lista. [22]



Referencias Bibliográficas

[1] B. Svidergol y R. Allen, Active Directory Cookbook, Estados Unidos de América: O'Reilly, 2013.

[2] B. Desmond, J. Richards, R. Allen y A. Lowe-Norris, Active Directory: Desingning, Deploying and Running, Estados Unidos de América: O'Reilly, 2013.

[3] B. Payatte, Windows Powershell In Action, Second Edition, Estados Unidos de América: Manning, 2011.

[4] J. Moskowitz, Group Policy: Fundamentals, Security and Troubleshooting, Estados Unidos de América: SYBEX, 2008.

[5] B. Smith and B. Komar, Microsoft Windows Security Resource Kit, Estados Unidos de América: Microsoft Press, 2003.

[6] C. Russel and C. Zacker, Windows Server 2008 R2, Estados Unidos de América: Microsoft Press, 2010.

[7] C. Russel, Administering Windows Server 2012 R2, Estados Unidos de América: Microsoft Press, 2014.

[8] D. Bernal, «Adaptación del proyecto de software libre para la implementación de servidor WHOIS, Actividades realizadas por SSI/UNAM-CERT de la DGTIC de la UNAM,» Universidad Nacional Autónoma de México, México D.F., 2011.

[9] D. Martín, «Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix,» Universidad Nacional Autónoma de México, México, D.F., 1995.

[10] J. Johansson, Windows Server 2008 Security Resource Kit, Estados Unidos de América: Microsoft Press, 2008.

[11] K. Schaefer, J. Cochran, S. Forsyth, R. Baugh y et al., Professional IIS 7, Estados Unidos de América: Wiley Publishing Inc., 2008.

[12] M. Minasi y et al, Mastering Windows Server 2012 R2, Estados Unidos de América: SYBEX, 2014.

[13] R. Morimoto, Windows Server 2012 Unleashed, Estados Unidos de América: Pearson Education, 2012.

[14] R. Peña, L. Balart, J. Cuartero y J. Orbegozo, Paso a paso Office 2013. Manual práctico para todos, México: Alfaomega, 2013.

[15] S. Reimer y M. Mulcare, Active Directory Resource Kit, Estados Unidos de América: Microsoft Press, 2008.

Referencias Electrónicas

Classon, D. 10 de Septiembre de 2010. *How to install .NET Framework 3.5 on Windows Server 2012 and Windows Server 2012 R2*. Recuperado el 5 de Noviembre de 2014, de http://www.danielclasson.com/install-net-framework-35-server-2012/

Coordinación de Seguridad de la Información. 2015. *Congreso Seguridad en Cómputo*. Recuperado el 5 de diciembre de 2015, de https://congreso.seguridad.unam.mx/2015/

Coordinación de Seguridad de la Información. 2015. *Programa de Becas de Formación en Seguridad Informática*. Recuperado el 9 de Diciembre de 2015, de http://www.seguridad.unam.mx/plan-becarios/cursos.dsc

Delprato, G. 31 de Mayo de 2011. *Demostración Rights Management Services (RMS) en Ambiente de Prueba*. Recuperado el 15 de Noviembre de 2014, de https://windowserver.wordpress.com/2011/05/31/demostracin-rights-management-services-rms-en-ambiente-de-prueba/

Eckes, D. J. 5 de Octubre de 2013. *Server 2012 Enable Remote Desktop (RDP) through Group Policy (GPO)*. Recuperado el 23 de Octubre de 2014, de http://www.dannyeckes.com/server-2012-enable-remote-desktop-rdp-group-policy-gpo/

Gao, R. 5 de Agosto de 2013. *Troubleshooting AD RMS client authentication error.* Recuperado el 28 de Noviembre de 2014, de http://www.rickygao.com/category/adrms/

Jacops, A. 1 de Septiembre de 2014. *Disable strict name checking with PowerShell*. Recuperado el 25 de Noviembre de 2014, de https://4sysops.com/archives/disable-strict-name-checking-with-powershell/

Kam Wah, Y. 24 de Agosto de 2014. *Windows 2012 R2 RMS with Windows Live ID*. Recuperado el 6 de Noviembre de 2014, de http://monsterbean.com/2014/08/24/windows-2012-r2-rms-with-windows-live-id/

Microsoft Corporation. 1 de Julio de 2009. *Using Windows Live ID to Establish RACs for Users*. Recuperado el 17 de Noviembre de 2014, de https://technet.microsoft.com/es-mx/library/ee221037(v=ws.10).aspx

Microsoft Corporation. 13 de Julio de 2013. *Plan Information Rights Management in Office 2013*. Recuperado el 30 de Octubre de 2014, de https://technet.microsoft.com/en-us/library/cc179103(v=office.15).aspx

Microsoft Corporation. 14 de Enero de 2010. *AD RMS Firewall Considerations*. Recuperado el 5 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/dd941596(v=ws.10).aspx

Microsoft Corporation. 15 de Febrero de 2011. *Pre-installation Information for Active Directory Rights Management Services*. Recuperado el 5 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/cc771789.aspx

Microsoft Corporation. 16 de Agosto de 2012. *Configuring Custom Templates for Azure Rights Management.* Recuperado el 17 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/dn642472.aspx

Microsoft Corporation. 2 de Abril de 2009. *Cómo solucionar problemas de configuración de IIS en SQL Server 2005 Reporting Services*. Recuperado el 26 de Noviembre de 2014, de https://support.microsoft.com/es-es/kb/958998

Microsoft Corporation. 2 de Julio de 2012. *Test Lab Guide: Deploying an AD RMS Cluster*. Recuperado el 30 de Octubre de 2014, de https://technet.microsoft.com/en-us/library/jj134037.aspx

Microsoft Corporation. 2013. *Requisitos del sistema e información de instalación de Windows Server 2012 R2*. Recuperado el 15 de Diciembre de 2015, de https://technet.microsoft.com/es-MX/library/dn303418.aspx

Microsoft Corporation. 30 de Diciembre de 2007. *Understanding AD RMS Certificates*. Recuperado el 16 de Diciembre de 2015, de https://technet.microsoft.com/en-us/library/cc753886.aspx

Microsoft Corporation. 31 de Marzo de 2008. *Step 2: Configuring the AD RMS client*. Recuperado el 15 de Noviembre de 2014, de https://technet.microsoft.com/en-us/library/cc771971(v=ws.10).aspx

Microsoft Corporation. 7 de Agosto de 2013*. Active Directory Domain Services Overview*. Recuperado el 20 de Noviembre de 2015, de https://technet.microsoft.com/en-us/library/hh831484.aspx

Microsoft Corporation. 9 de Noviembre de 2006. *La conexión a un recurso compartido SMB en un equipo basado en Windows 2000 o en Windows Server 2003 puede no funcionar con un nombre de alias.* Recuperado el 25 de Noviembre de 2014, de https://support.microsoft.com/es-es/kb/281308

Microsoft Technet Forums. 27 de Julio de 2011. *Client can't connect to AD RMS Server*. Recuperado el 27 de Noviembre de 2014, de https://social.technet.microsoft.com/Forums/en-

US/b28b335f-4cde-48ad-b682-d81039565e25/client-cant-connect-to-ad-rms-server?forum=rms

Schmarr, A. 14 de Noviembre de 2013. *Installing AD Rights Management Services (ADRMS) on Windows Server 2012 R2.* Recuperado el 6 de Noviembre de 2014, de http://www.schmarr.com/Blog/Post/16/Installing-AD-Rights-Management-Services-%28ADRMS%29-on-Windows-Server-2012-R2

Siddiqui, M. O. 9 de Junio de 2014. *ADRMS Error - The operation being requested was not performed because the user has not been authenticated*. Recuperado el 28 de Noviembre de 2014, de http://blogs.technet.com/b/omers/archive/2014/06/09/adrms-error-the-operation-being-requested-was-not-performed-because-the-user-has-not-been-authenticated.aspx

UNAM. 1998. *Día Internacional de la Seguridad en Cómputo*. Recuperado el 6 de diciembre de 2015, de http://www.disc.unam.mx/1998/

Vilcinskas, M. 16 de Julio de 2013. *Install a new Active Directory forest on an Azure virtual network*. Recuperado el 13 de Agosto de 2015, de https://azure.microsoft.com/en-us/documentation/articles/active-directory-new-forest-virtual-machine/