Active Directory Rights Management Services

Tarcísio Rosa Santos[1], Fabricio Alves do Santos[2], Sandro Andrade Monteiro Menezes[3]

Instituto Federal de Educação, Ciência e Tecnologia de Sergipe (IFS), Campus Lagarto
tarcisiorosasantos@hotmail.com, fabricioalves12011@gmail.com,
sandroandrade72@gmail.com

Abstract. *This article will focus the AD-RMS tool (Active Directory Rights Management Services), developed by Microsoft, which is available in both servers, Windows Server. The same provides services that allow users to create persistent use of security policies to protect unauthorized use of information, such as financial reports, customer data, product specifications of a particular company, email, intranet sites, Microsoft office documents (Word, PowerPoint, Excel) etc.*

Resumo. *Este artigo terá como tema a ferramenta AD-RMS (Active Directory Rights Management Services), desenvolvida pela Microsoft, onde está disponível nas versões, Windows Server. A mesma fornece serviços que permitem ao usuário criar diretivas de segurança persistentes para proteger informações do uso não autorizado, como relatórios financeiros, dados de clientes, especificações de produtos de uma determinada empresa, emails, sites de intranet, documentos da Microsoft office (Word, Power Point, Excel) etc.*

Palavras-chave: Windows Server, AD-RMS, Segurança, Diretivas, Criptografia, Banco de Dados.

1. INTRODUÇÃO

Figura 1- AD-RMS. Fonte: http://mvcp.tistory.com/category/%EA%B8%B0%ED%83%80

Atualmente a segurança é de grande necessidade para a sociedade comteporânea, principalmente na área da tecnologia. E nesse contexto, as redes de computadores de certa forma exige uma grande atenção. Ao acessar as redes sociais, emails, sites de relacionamentos, transações bancárias, etc, os usuários, sejam eles iniciantes, intermediários ou avançados, precisam de determinados níveis de segurança.

Existem muitas formas e meios de fazer com que a segurança seja implementada nos diversos tipos de equipamentos em rede, (notebooks, desktops ou até mesmo um smartphones). Nessa necessidade de segurança é que surge a ferramenta AD-RMS/ Active Directory Rights Management Services, que traduzindo para o português ficaria: Serviços de Gerenciamento de Direitos do Active Directory.

O AD-RMS é uma ferramenta disponível nas versões servidores do sistema operacional Windows, o Windows Server, desenvolvido pela Microsoft. Esta ferramenta oferece diversos serviços, que permitem a criação de regras para a proteção de informações de uma determinada organização, por meio da criptografia e por diretivas de uso persistentes, ou seja, independentemente de onde as informações forem movidas, as mesmas irão permanecer com as regras preestabelecidas. Apenas o proprietário do conteúdo poderá alterar ou remover a proteção do documento.

Vale destacar que a ferramenta utiliza um servidor de banco de dados, onde o mesmo fará a gestão do banco de dados do AD-RMS, podendo ser o utilizado o Microsoft SQL Server como opção(que é um dos mais utilizados no mundo). Há uma grande diversidade de conteúdo e informações que podem ser protegidos pelo AD RMS, como relatórios financeiros, dados de clientes e especificações de produtos de uma determinada empresa, emails, sites de intranet, documentos etc.

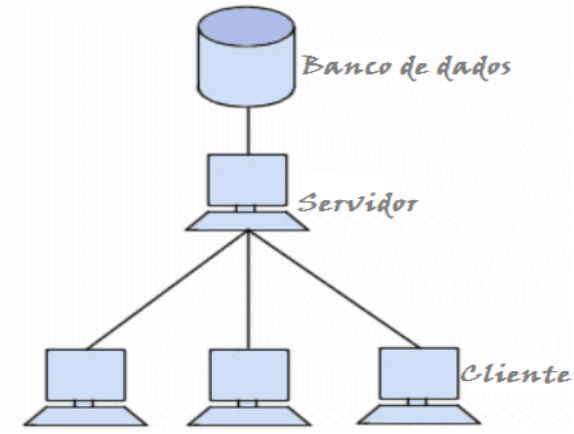
2. AD-RMS

2.1. Visão Geral

O AD RMS inclui:

- Um servidor AD RMS;
- Cliente do AD RMS;
- Um servidor de banco de dados;

1. O BANCO DE DADOS



Fonte: http://br.ccm.net/contents/65-bancos-de-dados-introducao

> Um banco de dados (sua abreviatura é BD, em inglês DB, database) é uma entidade na qual é possível armazenar dados de maneira estruturada e com a menor redundância possível. Estes dados devem poder ser utilizados por programas, por usuários diferentes. Assim, a noção básica de dados é acoplada geralmente a uma rede, a fim de poder pôr, conjuntamente, estas informações, daí o nome banco. (CCM, 2016).

No banco de dados ficarão armazenados informações de configuração, log e serviços de diretório usadas pelo AD RMS.

O servidor AD RMS necessita de um servidor de banco de dados e procedimentos armazenados para executar operações. O mais recomendado neste caso, para quem tiver interesse em fazer a instalação da ferramenta, seria utilizar o Microsoft SQL Server para gerir o banco de dados, porque além de ser um dos mais utilizado no momento, o próprio Windows Server tem a função que permite ao administrador fazer a instalação, porém é possível também, a utilização de outros bancos, como: Oracle, Mysql e etc.

1. CLIENTE AD-RMS

O Windows 7 e o Windows Vista já possuem por padrão o cliente do AD-RMS instalado, mas caso os sistemas operacionais de clientes sejam diferentes dos citados acima, devem ser feitas a instalação do cliente do RMS. Pode-se baixar o cliente do AD-RMS com o Service Pack 2 no Centro de Download da Microsoft.

O cliente do AD-RMS deve ter um navegador ou aplicativo compatível com o AD-RMS para que ambos possam se comunicar, como por exemplo o Microsoft Word ou PowerPoint. Esses aplicativos exigem as versões Enterprise, Professional Plus ou Ultimate do Microsoft Office, para poder criar as diretivas para os arquivos.

2. CRIPTOGRAFIA UTILIZADA

Figura 2 - Simulação de uma criptografia. Fonte: http://cartilha.cert.br/criptografia/

Criptografia corresponde à um conjunto de técnicas de codificação, que tem como objetivo proteger uma determinada informação do acesso não autorizado. Assim, apenas o real destinatário e o emissor poderão ter acesso a informação. E obviamente a ferramenta não deixaria de usar a criptografia em suas operações.

A ferramenta possui dois modos de criptografia, o Modo de Criptografia 1 que é o padrão, e o Modo de criptografia 2 (caso deseje ter um maior nível de segurança), mas o modo 2 requer configuração adicional.

Existem diversos tipos de criptografia atualmente, e com variados níveis de segurança. Algumas das mais conhecidas são as do tipo, chave simétrica e chave assimétrica, que por sinal o AD-RMS tem suporte para ambos tipos.

Chave Simétrica

É o tipo mais simples de criptografia, já que tanto o emissor quanto o receptor da mensagem possuem a mesma chave, ou seja, a mesma chave é usada tanto na codificação quanto

na decodificação. Para ser realizada, basta que o emissor, antes de enviar a mensagem criptografada, envie a chave privada que será utilizada para descriptografá-la. (CASTELLÓ; VAZ, 2016).

Chave Assimétrica

Diferentemente do método de Chave Simétrica, esse tipo utiliza 2 chaves, uma pública e uma privada. O sistema funciona da forma que alguém cria uma chave e envia essa chave à quem quiser mandar informações à ela, essa é a chamada chave pública. Com ela é feita a codificação da mensagem. Para decodificação será necessário utilizar uma outra chave que deve ser criada, a chave privada – que é secreta. (CASTELLÓ; VAZ, 2016).

O AD-RMS suporta o algoritmo RSA 1024 e RSA 2048 para criptografia assimétrica, o algoritmo AES 128 para criptografia simétrica, e o SHA 1 ou SHA 256 para operações de assinatura.

3. VANTAGENS E DESVANTAGENS

3.1. Vantagens:

- Instalação fácil e rápida;
- Maior segurança dos documentos e arquivos;
- Não necessita de alta capacidade de processamento da máquina;
- Tecnologia flexível e personalizável;
- Diretivas persistentes;
- Tolerância a falha;

1.1. Desvantagens:

Não foi observado nenhuma desvantagem no uso da ferramenta. É óbvio que atualmente qualquer organização ou qualquer usuário independentemente do seu nível de conhecimento, irão ficar mais satisfeitos se for possível obter um maior nível de segurança e privacidade no seu dia a dia, ou seja, com o uso da ferramenta só se obtém vantagens.

2. CONSIDERAÇÕES SOBRE HARDWARE E SOFTWARE

2.1. Requisitos de hardware

Requisito	Recomendação
Um processador Pentium 4,3 GHz ou superior	Dois processadores Pentium 4,3 GHz ou superiores
512 MB de RAM	1024 MB de RAM
40 GB de espaço disponível no disco rígido	80 GB de espaço disponível no disco rígido

Tabela 1- Requisitos mínimos e recomendado de hardware para o perfeito funcionamento da ferramenta

2.2. Requisitos de software

Windows Server 2008 ou Windows Server 2012
AD (Active Directory)
IIS (Serviços de Informações da Internet – Servidor Web)

Servidor de Banco de Dados (local ou remoto) - Microsoft SQL Server

Tabela 2 – Requisitos de software para o correto funcionamento da ferramenta

3. FUNCIONAMENTO

O funcionamento da ferramenta pode ser entendido basicamente por alguns passos, os do autor e os do destinatário.

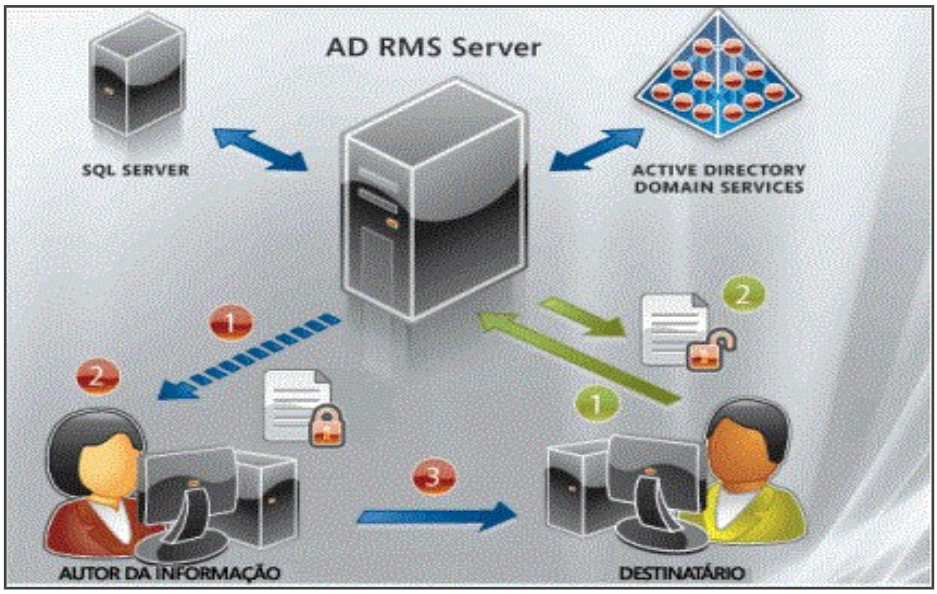


Figura 3 - Esquematização do funcionamento da AD RMS. Fonte: http://www.primesolution.com.-br/ADRMS.php

3.1. Passos do autor (numeração vermelha):

- A primeira vez que o autor protege uma informação ele recebe um certificado.
- O autor define um conjunto de direitos e regras para o arquivo e logo em seguida a aplicação cria uma “licença de publicação” e encripta o arquivo.
- No terceiro passo do autor, despois de o arquivo está encriptado, o mesmo “compartilha” o arquivo.

1.1. Passos do destinatário (numeração verde):

- Quando o destinatário clica no arquivo para abri-lo, a aplicação se comunica com o servidor AD RMS, que valida o usuário e fornece uma “licença de uso”.
- E por último a aplicação compila o arquivo e aplica os direitos.

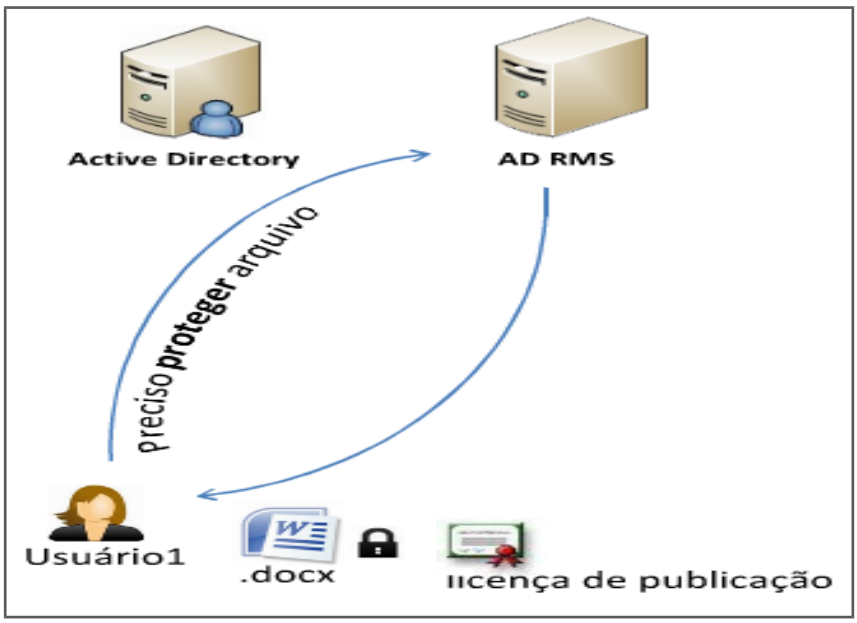


Figura 4 - Solicitação de proteção do arquivo ao AD RMS.

Na figura 2 acontece o seguinte: Primeiramente o usuário 1 solicita ao AD RMS a proteção de um determinado documento e automaticamente recebe um certificado do servidor (deixando bem claro que o documento utilizado no exemplo acima pode ser vários outros tipos de arquivo), e então o usuário 1 irá criar suas diretivas para o arquivo, que ao concluir, a aplicação irá criar uma licença de publicação e logo em seguida encripta o arquivo com as regras definidas pelo usuário e distribui o arquivo. São muitos os tipos de regras e diretivas que você pode criar, como por exemplo: O usuário pode determinar que apenas o usuário poderá alterar o arquivo, ou que apenas pode fazer a leitura do mesmo, mas não poderá modificar o arquivo, ou que pode imprimir, ou que não pode imprimir. O tipo de proteção vai variar de usuário para usuário, vai depender das intenções que os mesmos possuem.

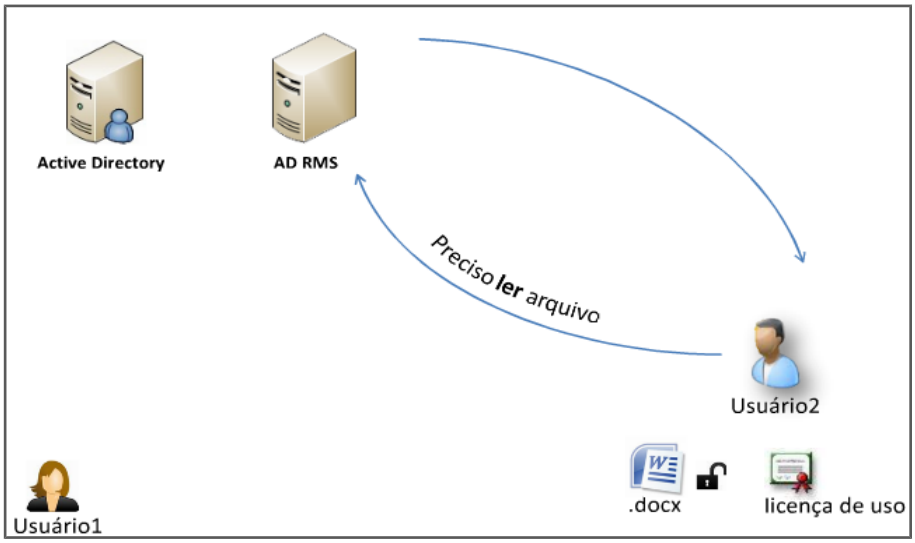


Figura 5 – Solicitação de leitura ao Servidor AD RMS.

Já na figura 3 acontece o seguinte: Quando o usuário 2 clica no arquivo para abri-lo a aplicação solicita a permissão ao AD-RMS para fazer a leitura do arquivo, que foi encriptado segundo as regras criadas pelo usuário1, caso o usuário 1 tenha determinado que o usuário 2 possa fazer a leitura do

documento, o AD RMS irá fornecer uma licença de uso e irá permitir a leitura, caso contrário, a mesma não será permitida.

Vale lembrar que as regras e as diretivas são persistentes, ou seja, mesmo depois de o usuário destinatário ler as informações, imprimir ou fazer qualquer outra ação que tenha a permissão; se ele for acessar o arquivo ou documento novamente, todo o processo será refeito para que o usuário tenha acesso, mesmo que ele envie ou mova o arquivo ou documento para qualquer outro destino, as diretivas de segurança irão permanecer. Tudo isso acontece porque o bloqueio dos direitos acontece no próprio documento depois de encriptado pela aplicação.

1. PÚBLICO ALVO

Atualmente qualquer organização seja ela pública ou privada, de pequeno ou grande porte, irá precisar de segurança na troca de informações entre seus funcionários. Sendo assim toda e qualquer organização que preze pela segurança das suas informações seriam “alvo” da ferramenta. Porque uma empresa não usaria uma ferramenta, sendo que a mesma iria lhe proporcionar uma maior segurança e privacidade na rede? Sendo que a além de sua instalação ser rápido, fácil e ter tolerância a falha, não teria um alto custo financeiro algum, caso na rede da organização já se tenha o Windows Server funcionando, pois assim não teria de adquirir o sistema da Microsoft.

Sua implementação fornece aos funcionários de determinados setores dentro de uma organização, uma maior confiabilidade na manipulação de documentos que precisem de um certo nível de segurança das informações. O uso de suas diretivas promove uma política de segurança voltada a proteção de informações confidenciais, sendo que essas podem ser induzidas a não serem abertas, modificadas, impressas, encaminhadas ou até mesmo, executadas. Um exemplo prático do seu uso pode ser feito com um determinado funcionário de um setor da empresa (Setor 1), onde esse tenha em seu editor de texto informações de pesquisas realizadas sobre a aceitação de um novo produto que será lançado no mercado, por tanto, essas informações não podem ser modificadas nem passadas para terceiros, quando esse funcionário enviar esses dados para o setor gráfico (Setor 2) dessa mesma empresa. Nesse segundo setor, um outro funcionário projetará em gráficos os dados, sendo que o mesmo não pode modificar, encaminhar ou imprimir, apenas poderá abrir e ler as informações. Para que isso seja feito o funcionário do setor 1 estabelecerá regras de segurança através do AD RMS no documento que será enviado ao setor 2.

2. CONCLUSÃO

Embora a ferramenta não seja tão difundida como outras no mercado, ela faz o que promete, é simples e eficiente. Além de oferecer serviços que possibilitam ao usuário criar diretivas e regras de uso persistente aos documentos de sua autoria utilizando criptografia, a instalação é fácil e rápida, a ferramenta não necessitará de alta capacidade de processamento da máquina, possui tecnologia flexível e personalizável, ou seja, seu uso é bem amplo e variado, ainda possuem tolerância a falha (você pode instalar o AD-RMS em dois servidores distintos, caso um pare de funcionar, ou outro automaticamente irá substitui-lo, não deixando que os serviços da ferramenta parem).

Fica claro que é irrecusável fazer o uso da ferramenta AD-RMS. Qual usuário, não seria adepto a uma ferramenta que só lhe traz vantagens e nenhuma desvantagem? Qual usuário ou organização não quer no seu dia a dia mais segurança?

Logicamente, qualquer usuário que tiver uma noção básica de segurança e privacidade, e conhecer apenas uma pequena parcela de todos os benefícios que o AD-RMS oferece, vai querer fazer a utilização dos serviços da ferramenta.

3. REFERÊNCIAS BIBLIOGRÁFICAS

AD RMS No Windows Server 2008. Disponível em: <https://consultormcse.wordpress.com/2010/02/01/ad-rms-no-windows-server-2008/>. Acesso em: 10 mar. 2016.

CASTELLÓ, Thiago; VAZ, Verônica. **Assinatura Digital**. Disponível em: < http://www.gta.ufrj.br/grad/07_1/ass-dig/TiposdeCriptografia.html>. Acesso em: 03 jul. 2016.

CCM. **Bancos de dados - Introdução**. Disponível em: <http://br.ccm.net/contents/65-bancos-de-dados-introducao>. Acesso em: 02 jul. 2016

MICROSOFT. **Comparando o Azure Rights Management e o AD RMS**. Disponível em: <https://docs.microsoft.com/pt-br/rights-management/understand-explore/compare-azure-rms-ad-rms>. Acesso em: 02 jul. 2016.

MICROSOFT. **Guia Passo a Passo do Windows Server Active Directory Rights Management Services**. Disponível em: <https://technet.microsoft.com/pt-br/library/cc753531%28v=ws.10%29.aspx>. Acesso em: 03 mar. 2016.

MICROSOFT. **Visão geral do Active Directory Rights Management Services**. Disponível em: <https://technet.microsoft.com/pt-BR/library/74272acc-0f2d-4dc2-876f-15b156a0b4e0.aspx>. Acesso em: 03 mar. 2016.

MICROSOFT. **Visão geral do Active Directory Rights Management Services**. Disponível em: <https://www.microsoft.com/brasil/servidores/windowsserver2008/adrms.mspx>. Acesso em: 07 abr. 2016.

MICROSOFT**. Noções básicas sobre os bancos de dados AD RMS.** Disponível em: < https://technet.microsoft.com/pt-br/library/cc771792(v=ws.11).aspx>. Acesso em: 06 jul. 2016.

PATRICIO, Anderson. **Instalando o Active Directory Rights Management Service (RMS) no Windows Server 2008 R2**. Disponível em: <http://www.andersonpatricio.org/instalando-o-active-directory-rights-management-service-rms-no-windows-server-2008-r2/>. Acesso em: 03 mar. 2016.

PRIME SOLUTION SOLUÇÕES EM SOFTWARE. **AD RMS**. Disponível em: < http://www.primesolution.com.br/ADRMS.php>. Acesso em: 04 mar. 2016.

PISA, Pedro. **O que é criptografia**. Disponível em: < http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html >. Acesso em: 03 jul. 2016.

SEGURANÇA DA INFORMAÇÃO. **Criptografia**. Disponível em: < http://seguranca-da-informacao.info/criptografia.html >. Acesso em: 02 jul. 2016.