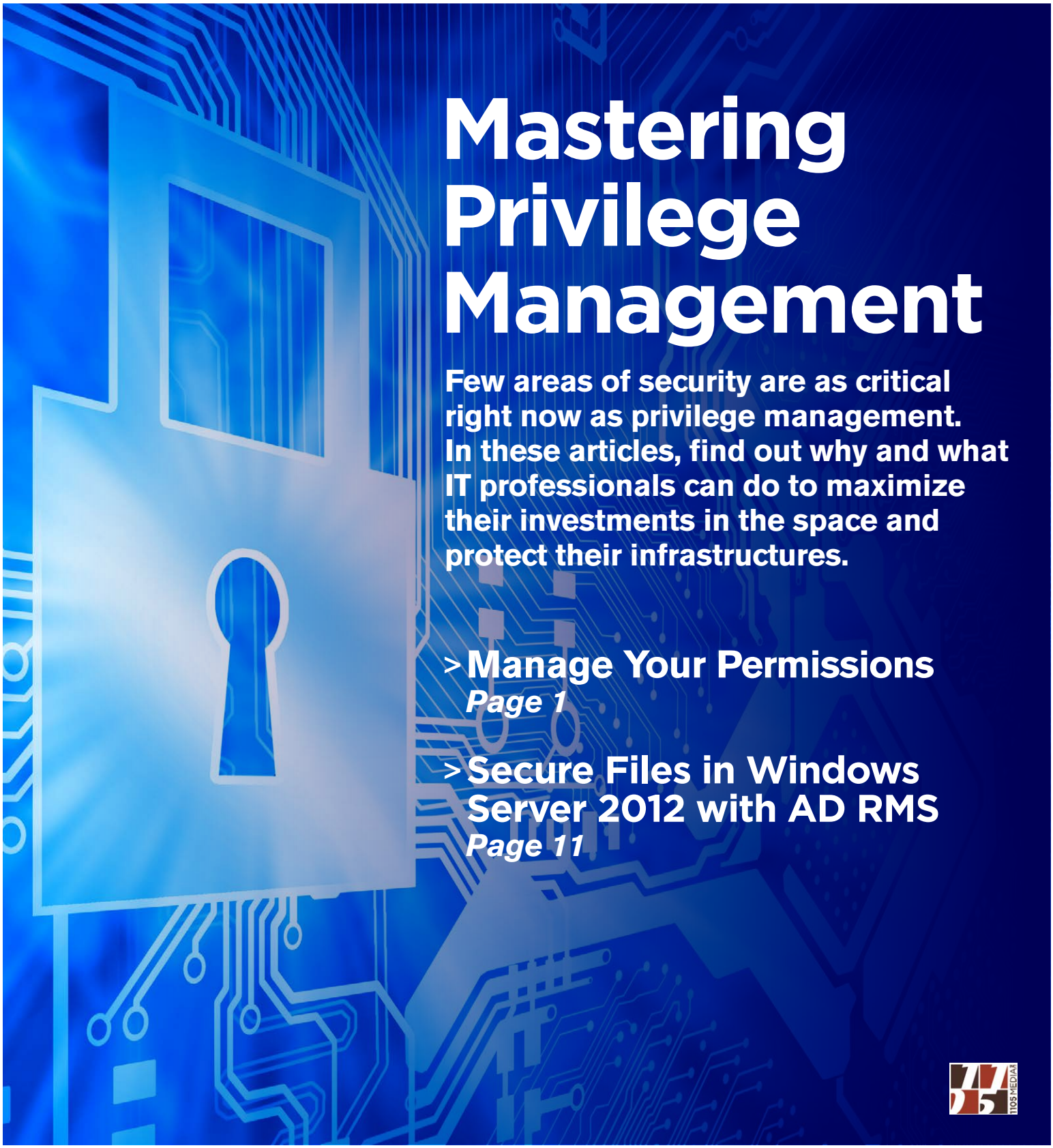
CONTENT PROVIDED BY

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

SPONSORED BY

VIEWFINITY



Mastering Privilege Management

Few areas of security are as critical right now as privilege management. In these articles, find out why and what IT professionals can do to maximize their investments in the space and protect their infrastructures.

1105 MEDIA

VIEWFINITY

A Fortune 500 Energy and Utilities Company

"We started our research by reaching out to other Energy & Utility companies that had implemented or were in the process of planning to migrate to Windows 7 and asked if they were also taking the initiative to remove administrator rights…

While other companies were using different methods and had different requirements and goals, it appeared the majority of Energy companies we spoke with were using Viewfinity and having success with it. This was a big driver."

IT Professional on the IT Infrastructure team

This prominent Energy and Utilities Company is a Fortune 500 company with assets over $20 billion. The company ranks as one of the largest electric power providers and also ranks as the largest natural gas distribution operation in total number of customers.

This prominent Energy and Utilities Company is a Fortune 500 company with assets over $20 billion. The company ranks as one of the largest electric power providers and also ranks as the largest natural gas distribution operation in total number of customers.

The Company's corporate-wide vision of "leading the way to a secure energy future" is also the vision of its IT organization, which translates into securing its IT environment. One such fundamental IT security charter was to reduce exposure to malware and virus threats. With a Windows 7 deployment project a year into planning, part of the project scope was to reduce exposure to cyber attacks by removing administrator rights from desktops. This was a proactive approach that was investigated previously during an XP migration but the security features in Windows XP weren't robust enough and at the time, there were no 3rd party tools to bridge the gap.

Fast Facts

Project Scope: Remove administrator rights during Windows 7 rollout

- 8500 desktops concerned with this project
- Managing ~250 applications that corporate IT delivers
- Between 6-8K unmanaged applications that end users install on their own. Ultimately the IT team supports the unmanaged to some extent but not on the service level of the corporate applications.
- Laptops / mobile workers constitute ~25% of the user base
- There are over 100 remote offices spread over Missouri and Illinois

The Challenge:

With a goal of reducing exposure to malware and virus threats by removing administrator rights during the Windows 7 rollout, the IT team realized there would be additional management involved because business processes and application functionality required administrator level access to the operating system. From previous attempts to remove local admin rights, the IT team knew they would need a tool to manage end user desktop privileges on a granular scale. This is where they are leveraging the Viewfinity solution.

The Solution:

The company started its research by contacting other Energy and Utility companies that had implemented or were in the process of planning Windows 7 migration projects and asked if they were also taking the initiative to remove administrator rights. The Company heard about Viewfinity through these peer companies. Their research also encompassed online data, and they looked to Gartner reports and analysts to help further qualify the Privilege Management space. Once they understood the possible solutions, they did their due diligence and had discussions with all vendors.

While the other Energy companies that this company spoke with had different requirements and goals, it appeared the majority were using Viewfinity and having success with it. This was a big driver. Cost was another driver but pricing was comparable with some of the other vendors. The Viewfinity solution was fairly straightforward. The Viewfinity sales and professional services team came onsite and had conversations about the solution, product roadmap and the level of effort to implement and support post implementation– which was informative and helpful. Viewfinity Professional Services were engaged to assist with the Viewfinity product

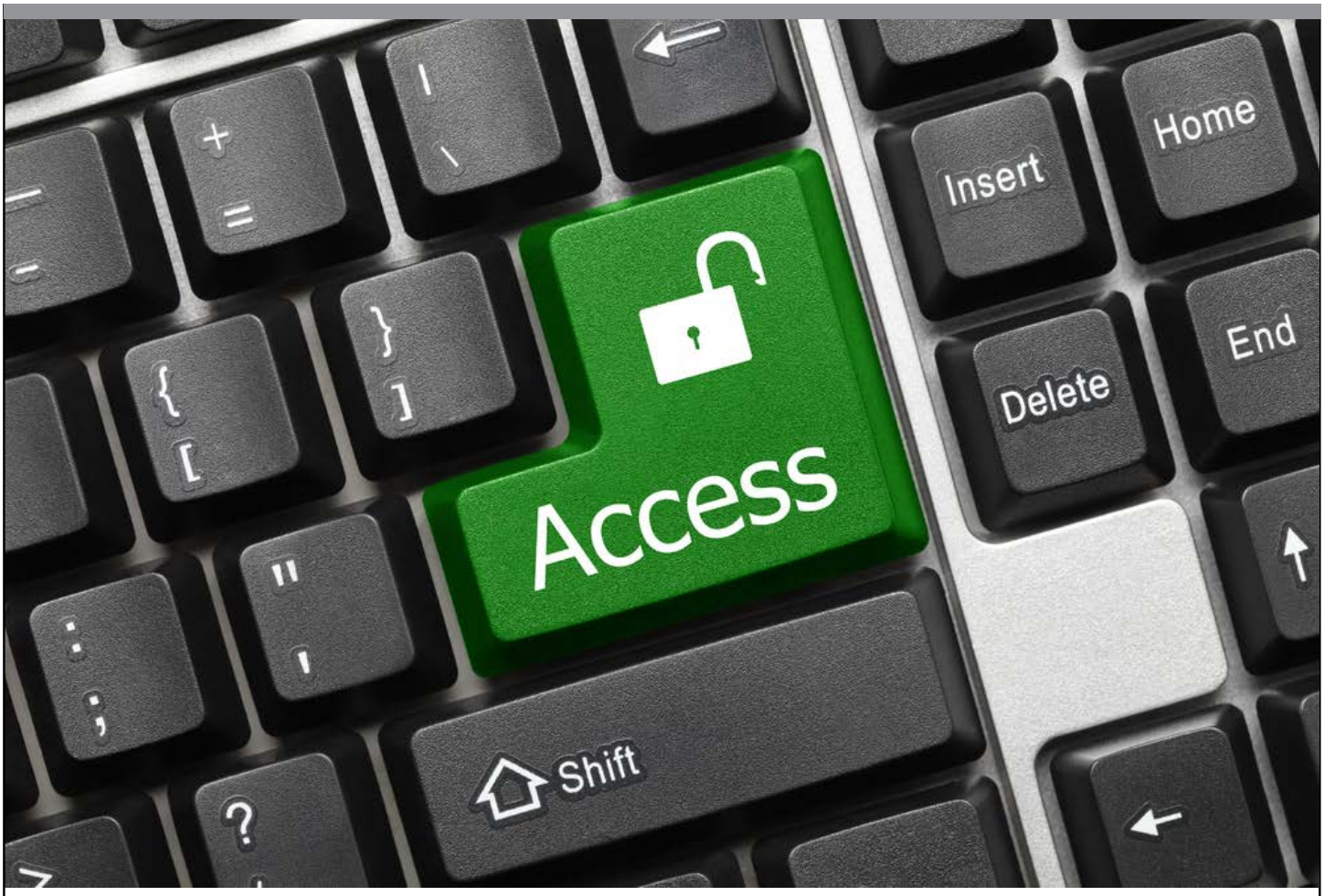
implementation and the Windows 7 rollout, which was critical as these two projects happened simultaneously. The ability to include the Viewfinity agent as part of the deployment image was instrumental to the project since the scope included rolling out Windows 7 machines and removing administrator rights at the same time.

The Results:

The Energy and Utilities company is continuously improving its cyber security posture with a bonus of greater visibility into its end user client computing environment. The Viewfinity product gives the company the ability to quickly update and push policy changes to client endpoints. The company can be proactive and respond to cyber threats without impacting business processes and applications. At the same time, they continue to reduce complexity in their client computing environment, and over time that will reduce costs. The company is managing more in terms of Viewfinity policy but this allows them to work more closely with end users to understand their needs. By having this increased visibility through working closely with their end users, the company will have increased awareness to the applications that exist across the organization, who owns them and how they are used.

Taking away functionality that the Energy and Utility company's end users were used to having was a challenging cultural change. However, the end users will see benefit from less configuration drift and a desktop that will perform better over its useful life. The possibility of a cyber attack is a constant threat. Removing administrator privileges from end users is a big step in protecting the company from these threats. Just this reduction in vulnerability to cyber attack makes it feasible to reduce the company's exposure. Without the automation component from Viewfinity, this would not be do-able for this prominent Energy and Utilities company.

> "With a goal of reducing exposure to malware and virus threats by removing administrator rights during our Windows 7 rollout, we realized there would be additional management involved because we would be taking back functionality that users needed…
>
> This is where the Viewfinity solution stepped in to help out."
>
> IT Professional on the IT Infrastructure team



Manage Your Permissions

A look at four tools that help control access to files and shares.

BY DEREK SCHAULAND

To say Windows is a huge platform is an understatement. At a high level it seems so large because everything tends to work together in a way that makes sense for both administrators and employees alike. But when securing information becomes the task at hand, it can quickly become a daunting exercise in futility.

But now, thanks to the latest iteration of Active Directory Rights Management Services (AD RMS) in Windows Server 2012 (see

"Secure Files in Windows Server 2012 with AD RMS," p. 11), it's a much easier endeavor. If you're an IT manager considering privilege management suites, you might want to consider those that allow you to control who has access to files and folders. In this article, I'll look at four privilege management tools that give such control over permissions.

First, it's important to understand Windows file system permissions. Everyone who's managed Windows has dealt with or has come across permissions. But what are permissions? Permissions on files and folders are just like permissions to things around the house I recall as a child. Some things I was allowed to use whenever I wanted, while others needed supervision. Then there were those that were off limits completely. Windows can do the same thing for files and folders.

Windows permissions can work in conjunction with privileges but the two are distinctly different.

Think of Windows permissions as toy chest permissions. If I have three folders–C:\Boss, C:\Derek and C:\Project–they can represent different work items for me. For C:\Boss, I would have no access because those are my boss's files and are none of my business. For C:\Derek I would have full control: I can write to and delete from anything inside that folder with no trouble. And the C:\Project folder might contain files I can read but not modify, items I can modify and, still, other items I can delete. These folders are much like items around my house growing up. Things in my bedroom were pretty much available for me to use whenever and however I wanted (like C:\Derek). Things in the kitchen might have been OK to use depending on the level of supervision that was around and what my goal was (C:\Project). And things in the living room were generally considered off limits (C:\Boss). When you look at it with simple real-world comparisons, it isn't quite so bad.

Windows permissions can work in conjunction with privileges but the two are distinctly different. Privilege allows a user to perform an action (such as accessing a file) and can override permissions. Permissions are lists of controls placed on a file or folder; they tell Windows which users and groups are able to see or use the data and nothing more.

Managing Shares

Shares are another "object" that you can control and manage in Windows. There are fewer options available for shares in terms of security available, but whichever permission is most restrictive wins,

especially if both share permissions and NTFS permissions are in play. When you access the Boss folder on a network share (\\server\Boss), you'll encounter both share permissions and NTFS permissions. The share permissions determine if the shared object is visible over the network. This could be similar to a cookie jar in the way the permissions are applied. Read share access might happen when the cookie jar is on the top of the fridge: I can see it but I can't access it. Modify permissions might work like supervised access to the cookies–when Mom is watching, I'm allowed two cookies. Full control access would be that I can have as many of the cookies as I like. NTFS permissions can be applied to specific accounts or the built-in group "Everyone," which mostly disables them. NTFS permissions can be far more granular in allowing or denying access, but if your login can't get past the share permissions you'll be restricted right away. Because of the more granular functionality, I tend to rely on NTFS permissions and set share permissions to be less restrictive, if restrictive at all. How you handle this will be determined by requirements in your organization.

Because of the nature of working with permissions and their depth within Windows, these four privilege management applications might help you manage permissions within your Windows environment.

Because of the nature of working with permissions and their depth within Windows, these four privilege management applications might help you manage permissions within your Windows environment.

Dell Software: Security Explorer

Licensing: Starts at $649 per server

The NTFS Security navigation option with Dell Software Security Explorer will help with NTFS permissions. The application manages security of other applications including Exchange, SharePoint and SQL Server, allowing one interface to work on any and all security in the environment. Here, NTFS will be the focus. There are two types of tasks available: Basic and Advanced. Some of the basic tasks used for general permissions management let you view permissions, manage computers, grant or revoke permissions from a selected resource, and search permissions.

The advanced permissions allow functions such as reducing a user or group access to read only or changing the owner. They can be quite useful, but as with any application working in NTFS security,

getting the hang of how the basic tasks work before getting too far into the advanced techniques is advised.

Granting Permissions: To grant a permission, select the grant task. You'll then need to select a path (or resource) against which to grant a permission, as well as the permission to assign. When you select the permission you'll choose the type of permission and if it's allowed or denied, the user or group getting the permission, where it applies (to this folder only or to this folder and subfolders and files, for example) and whether the permission set will be appended to existing permissions or replace them. After completing this information and clicking OK, Security Explorer will add permissions to the resources as requested.

Security Explorer includes many features to ease permissions management for both share and NTFS.

Standout Features: Security Explorer includes many features to ease permissions management for both share and NTFS. Some of the most useful include:

- Reporting–the ability to see what permissions are applied where in a few clicks.
- Backup/Restore–make sure the security settings you need can be reapplied with ease should something go wrong.
- Windows PowerShell support–the ability to use Security Explorer features from the command line in Windows PowerShell helps automate permissions management.

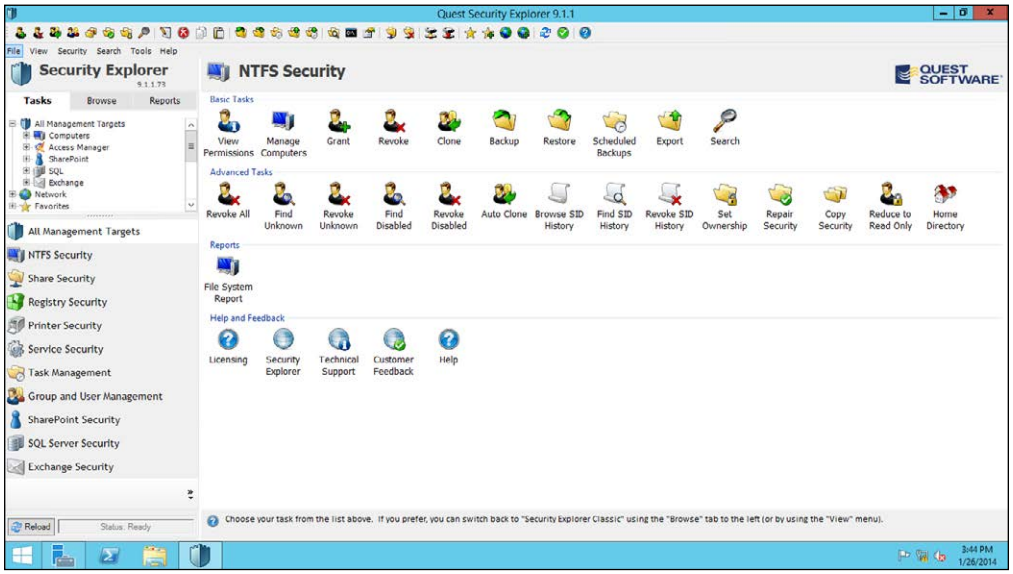


Figure 1: *The main window in Security Explorer lets you view, manage, grant and revoke NTFS permissions.*

BeyondTrust: PowerBroker for Windows

Licensing: Starts at $39/active user

Power Broker for Windows from BeyondTrust Inc. uses privilege identity rules to determine which users or groups are able to access resources and file integrity management rules to track the usage of assigned privilege. I'll focus on the first type of rule, but note that monitoring access is something included with this tool.

Power Broker for Windows uses privilege identity rules to determine which users or groups are able to access resources and file integrity management rules to track the usage of assigned privilege.

Managing Permissions with PowerBroker: Permissions to access resources are managed with Privilege Identity rules. To create a rule within PowerBroker, expand the user configuration, policies and BeyondTrust PowerBroker for Windows inside the Group Policy Management Console. From here a rules wizard helps you select the users (or groups) to which the rule should apply, as well as the folders (and files) the rule will be used to control. Once the initial rule is created, its properties can be modified to further tweak how the rule behaves. PowerBroker also has rules for file integrity management, which work to provide information about access to resources. Using these rule types together can provide a clear picture of what's happening in your environment as well as provide data for compliance, if needed.

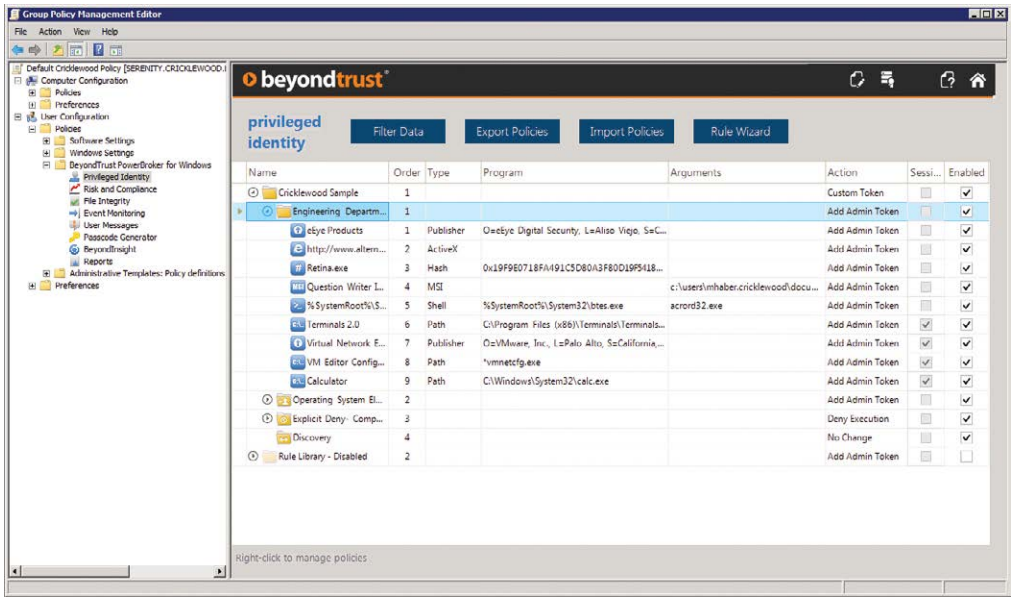


Figure 2: *You can provide access to files in PowerBroker for Windows by invoking the Rules Wizard.*

Standout Features: PowerBroker for Windows has regulatory considerations built-in that compare configuration elements to regulatory compliance standards. For example, the rules created can be compared against things such as PCI-DSS, and trigger event capture based on compliance.

Any action can be captured by logging. When a user account accesses a file or folder, this action is logged regardless of outcome (success or failure). Because all this information is logged within the application, which filters relevant Windows event logs for easier viewing, you can see what's going on and understand where changes are needed.

Using agents, even computers that aren't in a specific Active Directory domain can be managed.

Using agents, even computers that aren't in a specific Active Directory domain can be managed. The agents apply rules to these computers and track their usage for reporting. This allows computers within a DMZ or off the network for PCI compliance to be monitored without much additional effort. In conjunction with agents, screen captures can be taken any time a screen changes where an agent is installed. This will give you an idea of what an account is doing with permissions granted to it. Note that his feature can be made visible or invisible to the user, depending on laws in the region or on company policy.

Viewfinity: Application Control

Licensing: Perpetual licensing begins at $35/managed desktop; Software as a Service managed installation starts at $20/managed desktop—both have a 25 percent cost for maintenance and support

Application Control from VIewfinity Inc. has several flavors, two of which are Group Policy and Standalone. I chose to use the Group Policy application because many of the Microsoft environments used in organizations today rely on Active Directory. When installed, the application snaps directly into the Group Policy Management Console (GPMC).

This snap-in manages files and folders, as well as other items that might be useful in an enterprise.

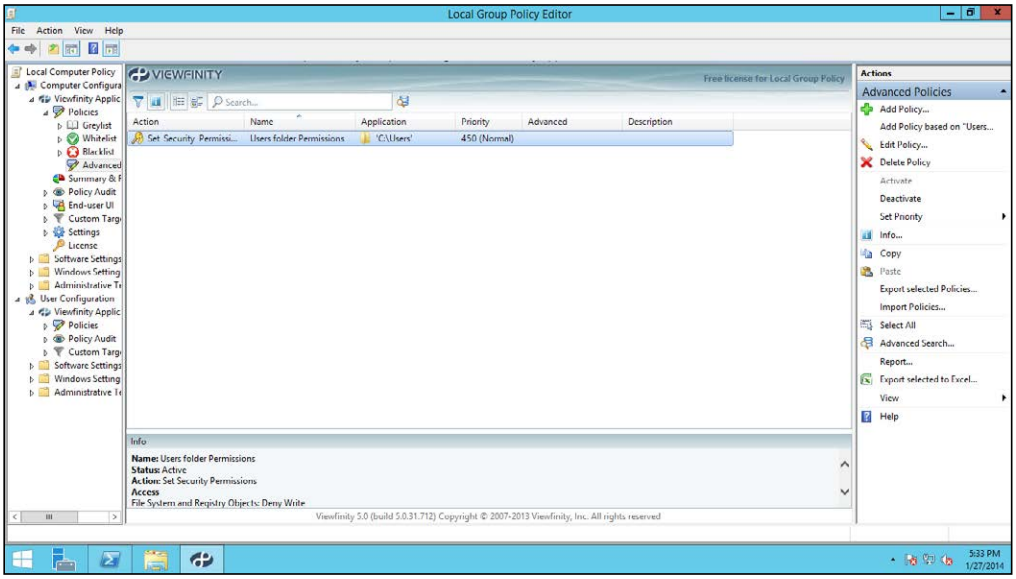


Figure 3: *Application Control snaps into Group Policy Management.*

Note that just like other items within the GPMC, the policies configured by Application Control can be configured for user or computer objects.

Managing Permissions with Policies: Permissions are managed using policies, which behave similarly to (and can be managed like) group policies in Active Directory. This minimizes the number of agents and extra management needed.

The application provides a wizard-style interface to help you create policies to manage permissions, including:

- Access–manages permissions on files and folders
- Services–manages permissions on services
- Removable–sets permissions for all items on removable media

Selecting Access and choosing an access type, allow read, allow full control, deny write, or deny any access will allow that permission to be used. For example, select Allow read.

Once the type of policy is defined the next thing to do is select the folders or files where the policy should be applied. Then the more granular settings can be applied based on the needs of your environment.

Note that just like other items within the GPMC, the policies configured by Application Control can be configured for user or computer objects. The settings are similar within the configuration element for permissions, but the computer configuration object has more types of settings.

Standout Features: One of the first features I noticed when configuring Application Control was the snap-in to the Group Policy environment. While this is not a "feature" of the software necessarily, I like it for its usability. When snapped into Group Policy, you don't have to work with another interface to use the product.

The policy creation is wizard-based to help get you off and running. This is not like traditional Group Policy management where most explanation is text-based and requires you to know where to find the right elements. Settings within the application, however, are configured like traditional Group Policy items having a state of Enabled, Disabled or Not Configured. Granular configuration allows dynamic items like RAM and CPU and other hardware or environment items to thin down where a policy might be applied.

One of the first features I noticed when configuring Application Control was the snap-in to the Group Policy environment.

Revision history allows each policy to log its modification/revision history. This will help keep track of changes to policies within the application.

Arellia: Security Analysis Solution

Licensing: Starts at $75/endpoint

Like the other products covered here, Security Analysis Solution from Arellia Inc. has features that are beyond the scope of managing permissions to files. I mention this because the tool is extremely modular and features can be added to the management framework once they're licensed.

Security Analysis Solution requires the Symantec Installation Manager (SIM) platform to be installed and configured before installing the product. Arellia and Symantec Corp. are partners in this arrangement and Arellia is planning a standalone application in a future release.

The initial configuration of the SIM and Arellia add-ins was a bit cumbersome, but the capabilities of the product once configured are definitely worthwhile. The Local Security Solution allows permissions management in both Active Directory and non-Active Directory environments using rules to define which security principals are allowed permissions on a resource and what those permissions

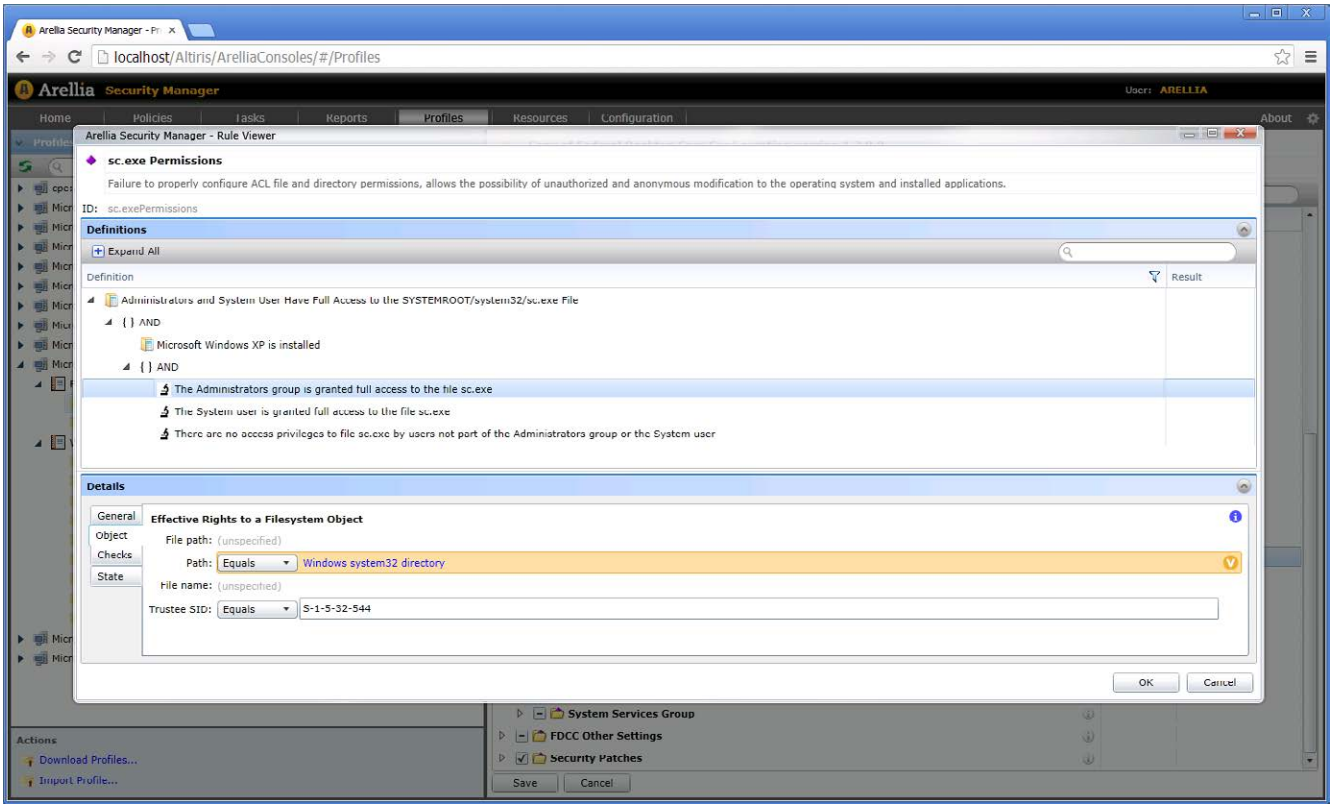


Figure 4: *You can manage permissions from the Profiles tab.*

should be. In addition to being rule/task list based, the changes are fully auditable for accounting and regulatory purposes.

On a specific resource, you can select the administrators full control descriptor to apply full control on this file for members of the Administrators group.

Managing Permissions: To create rules, open the Arellia Security Manager from the start menu. This will open a focused Web application for working with Arellia products. Select the Tasks tab and expand the Arellia | Client Tasks | Security Analysis | Remediation tasks | Remediation Pack | File Security. This will list all preexisting file permissions tasks. Right-click File Security, select New and then Task to create a new task. In the new task dialog, select File Security as the type of task to create in the left pane.

Select Add Item to add a new resource to secure. Specifying the path to the item to be secured and the security descriptor to apply. For example, on a specific resource (C:\new.txt) you can select the administrators full control descriptor to apply full control on this file for members of the Administrators group. Enter a name for the task (descriptive names are better) and Click OK to save the task.

Tasks can also be grouped into collections (or profiles) to allow the assignment of multiple configurations to a given set of resources or users.

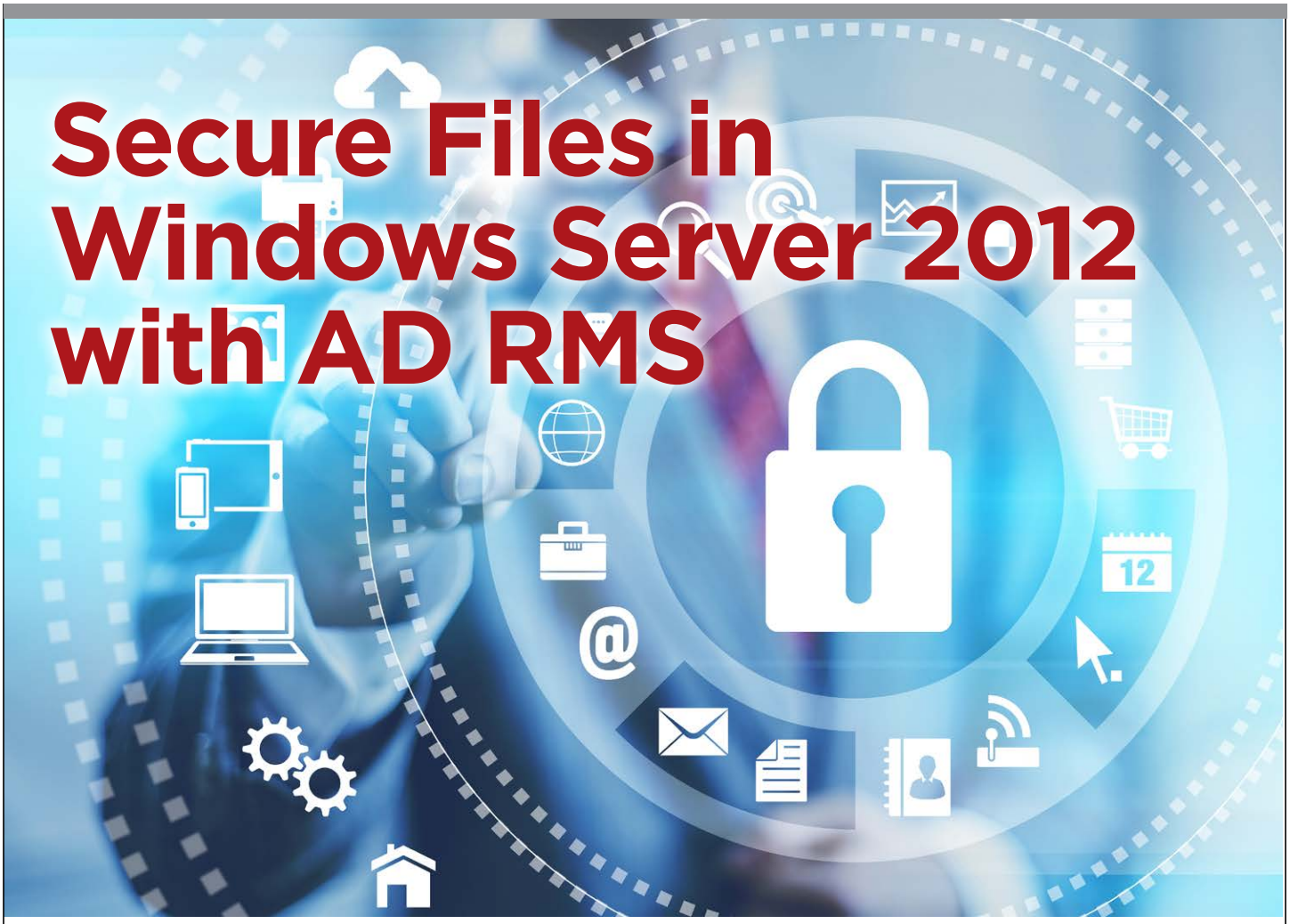
Tasks can be scheduled to run at intervals to ensure the security settings are applied as needed to ensure security compliance is maintained on files within an organization. Tasks can also be grouped into collections (or profiles) to allow the assignment of multiple configurations to a given set of resources or users.

Standout Features: You can start rules from compliance listings created by top-level security organizations. For example, if your organization is required to meet PCI DSS regulations, there are lists available within Arellia Security Manager to configure matching rules. This way, you can apply them to your organization to ensure these requirements are met with regard to the files and folders being managed. The solution isn't limited to regulatory rules—organizations can create their own rules based on internal needs to ensure files and folders are secured appropriately.

Rule scheduling to ensure that resources remain compliant with the security settings of an organization is a great feature. Using rules will possibly allow a file or folder to be created in a location and then ensure security gets applied as outlined in a policy. This helps ensure no files or resources are missed. R

Derek Schauland has worked in technology for 15 years in everything from a help desk role to Windows systems administration. He's also worked as a freelance writer for the past 10 years. Reach him at derek@derekschauland.com.

Secure Files in Windows Server 2012 with AD RMS



How to install and configure Active Directory Rights Management Services to lock down your organization's files and shares.

BY GARY OLSEN

As locking down information becomes a more critical priority for IT organizations, securing individual files or shares is completely dependent on effectively setting up security groups. Because security is tied to the user, an individual can open a file from within the intranet or a public kiosk. This causes the infamous security group bloat from which many organizations suffer, in an attempt to get granular permissions on file shares.

Microsoft has added some nice features in the file system of Windows Server 2012 and using Active Directory Rights Management Services (AD RMS) with other features, you can apply file classification so the file carries the rights without

having to apply security groups. Windows Server 2012 includes a new security wizard as well as new device permissions.

In this article, I'll examine the new security permissions wizard in Windows Server 2012. I'll also explore AD RMS, including installation and configuration.

Windows Server 2012 Security Permissions Wizard

Unlike configuring central access policies with the new Windows Server 2012 Dynamic Access Control (DAC) (see my August 2013 article, "Implement the New Windows Server 2012 DAC," Redmondmag.com/OlsenDAC), AD RMS is an additional component to more effectively secure files in Windows Server. Note that AD RMS was introduced in Windows Server 2008 and the file classification features and other components of DAC have existed for some time now. Windows Server 2012 puts them all together for an extremely granular application of permissions.

One of the new features in AD RMS is the conditional security permissions that add Boolean conditions to security principal permissions.

One of the new features in AD RMS is the conditional security permissions that add Boolean conditions to security principal permissions. While the options in Windows Server 2008 and Windows Server 2012 are the same—Folder/Share Properties | Security Tab | Advanced | Add (to add a user or group) | Edit (to edit permissions on a user or group)—the last screen on Windows Server 2012 is different. You can select the principal to edit at the top of the screen and set advanced permissions similar to Windows Server 2008 and previous versions. The big difference is the conditional statement at the bottom in Windows Server 2012 (see **Figure 1**, p. 13).

The conditions available depend on what you've already configured. Out of the box you can set User and Device permissions and apply them to a single user or group. One new feature, Device permissions, will permit access to a share only if the user connects from a computer in the group granted the permissions. However, I haven't been successful in getting this feature to actually work.

When I examined DAC, I configured it to have additional resources such as country and department to add additional filtering (see **Figure 2**, p. 14). In addition, you can define multiple conditions for a single principal (also shown in **Figure 2**). The Effective Access tab

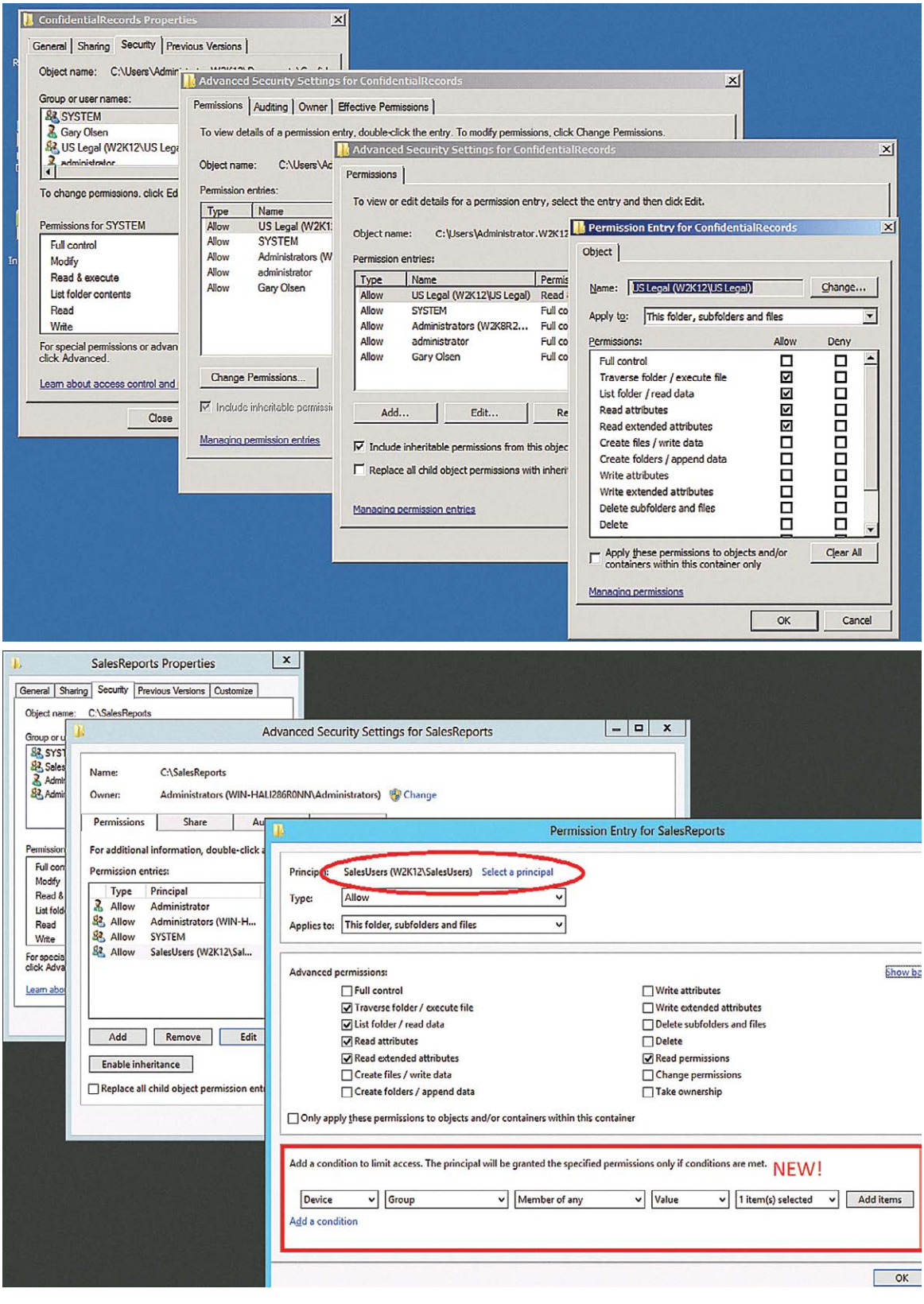


Figure 1. *Advanced permissions in Windows Server 2008 are shown on top, while the newer advanced permissions in Windows Server 2012 are shown on bottom.*

is a new take on the old Effective Permissions in previous Windows Server versions. By setting a Device permission you can restrict a user to access a share only when logged in to computers in certain group. As shown in **Figure 3** (p. 15), Caroline (the user) is being added to a group membership and the device selected is the Windows 8 PC ALF-WIN8. The Effective Access tab shows the permissions she'll be granted if logged on to ALF-WIN8, which is a member of the SalesPC group that was given the permission restriction. This makes it easy to do what-if testing for users on various machines.

AD RMS is an important component to secure sensitive information such as health records.

It's important to note that these new permission features can only be set on shares, folders and files on Windows Server 2012, though the permissions will apply to all users. DAC also requires a Windows Server 2012 domain controller, though there's no requirement for a specific Domain or Forest Functional Level to be set. Again, some of these features are available in Windows Server 2008, but Windows Server 2012 is the ideal environment to put it all together.

AD RMS is an important component to secure sensitive information such as health records. Any company that handles and stores health information should be aware of the severe penalties provided in HIPAA. Obviously, other data such as personnel records and finance

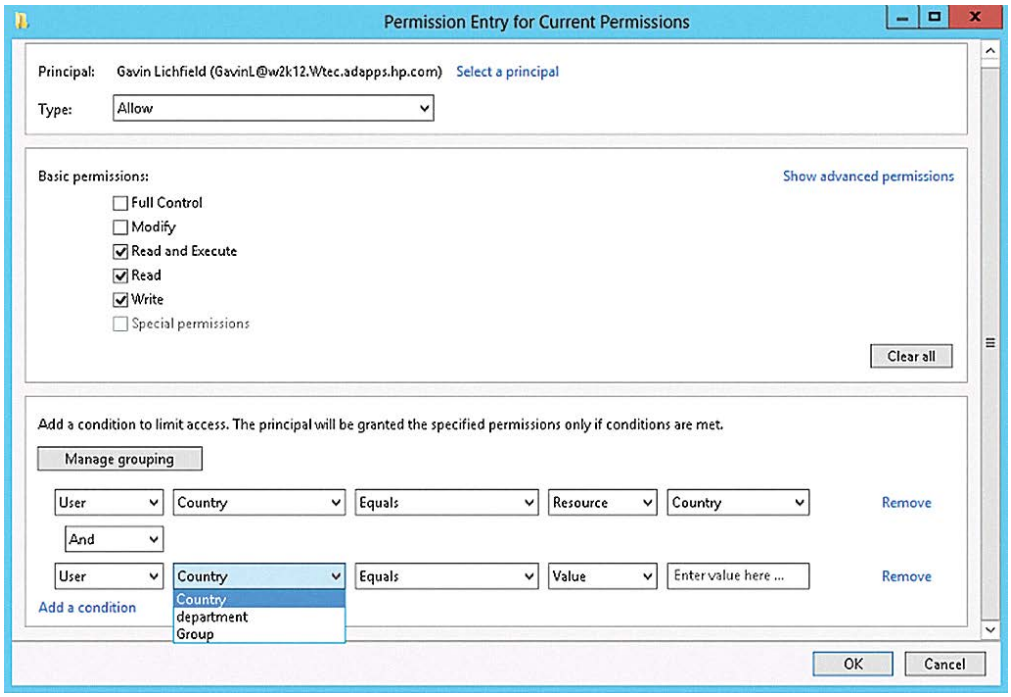


Figure 2. *You can select the level of permissions granted to a user.*

AD RMS can protect information produced by word processors, e-mail and other applications.

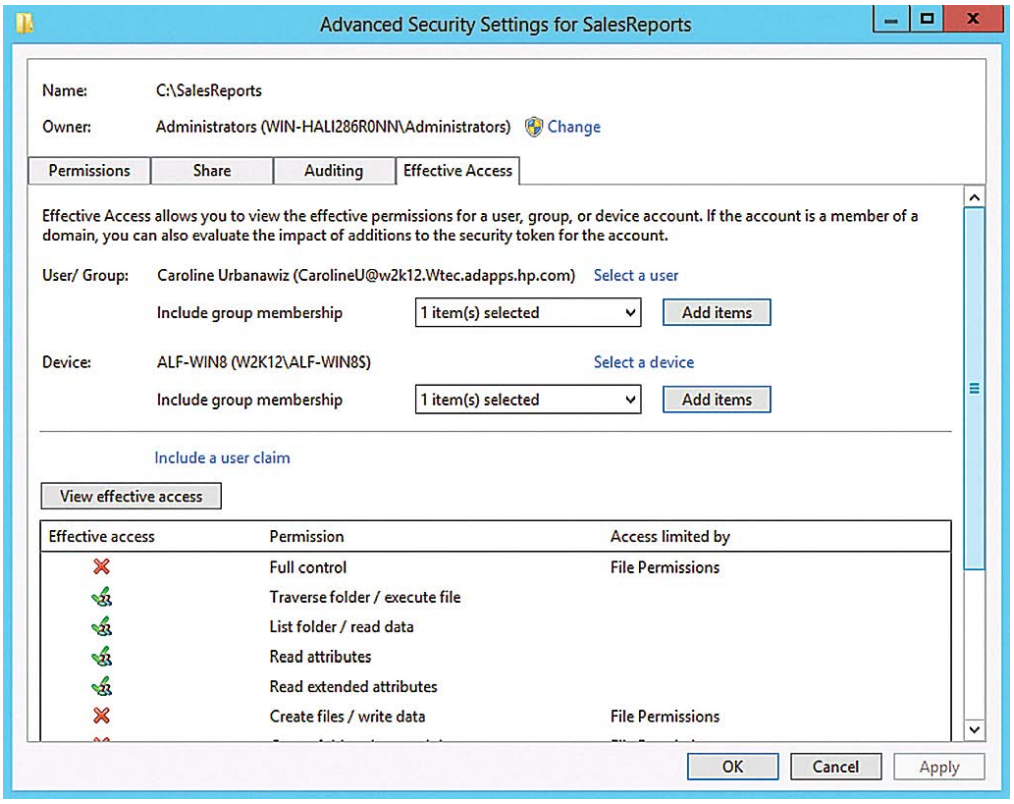


Figure 3. *You can restrict how a user can access a share.*

data including credit card information has similar requirements for protection. AD RMS can protect information produced by word processors, e-mail and other applications. Using AD RMS, users can define access to the files that remains with the data no matter where it's moved. This is a significant improvement over the old default Windows file security, and it's more flexible. Custom usage policies can be created to force compliance with company policy.

AD RMS Requirements

AD RMS requires a Windows Server 2008 or Windows Server 2012 system with the AD RMS server role installed. In addition, AD RMS requires IIS, a database such as Microsoft SQL Server and it must be run on a member of an Active Directory Domain Services forest. The AD RMS installation will install a single instance of a Microsoft SQL database if there's no SQL database available.

Note that AD RMS installation makes reference to an AD RMS cluster being required. This is not a Windows cluster as you might assume, but simply a term that refers to one or more AD RMS

Computer Name	OS	Role
W2k12-DC1	Windows Server 2012	Domain controller
Win2012Svr1	Windows Server 2012	AD RMS server, DB host
Alf-Win8	Windows 8 client	client

Table 1. *Machines, OSes and roles used for deploying Active Directory Rights Management Services*

servers and a single-node cluster is permitted. You don't need to install this on a Windows cluster.

AD RMS Installation and Configuration

Prerequisites to installing AD RMS include:

- Domain user account to be used for AD RMS service account (no special permissions needed). In this example I used ADRMSsvc and added it to the local administrators group.
- Domain user account to be used for AD RMS installation (different from the service account). My account is ADRMSAdmin and is a member of the domain administrators group. This account must have access to the SQL database if an external database is used. (In this example AD RMS will create the database.)
- URL (FQDN) for the AD RMS cluster to be used during AD RMS installation. This URL is not the same as the computer name.
- If you're upgrading from RMS to AD RMS, see considerations noted on the TechNet Library page at **bit.ly/1iHaL5y**.

For this example, the machines listed in **Table 1** are used.

This is not a Windows cluster as you might assume, but simply a term that refers to one or more AD RMS servers and a single-node cluster is permitted.

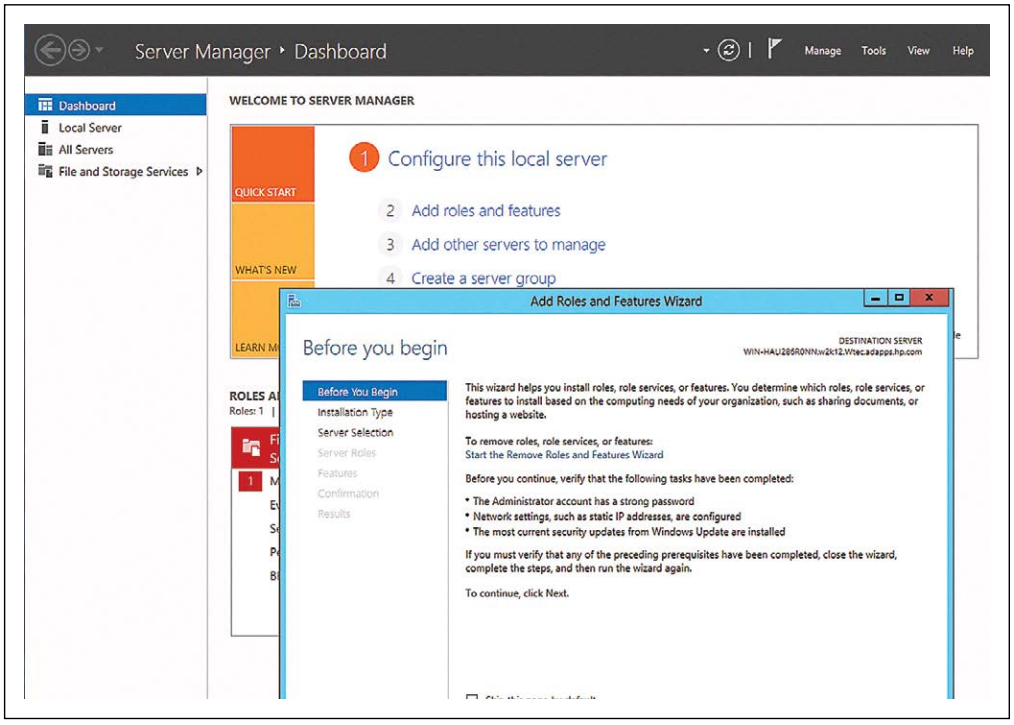


Figure 4. *The Windows Server 2012 Server Manager wizard enables you to create or add server roles.*

The Windows Server 2012 Server Manager is a bit different than the one in Windows Server 2008.

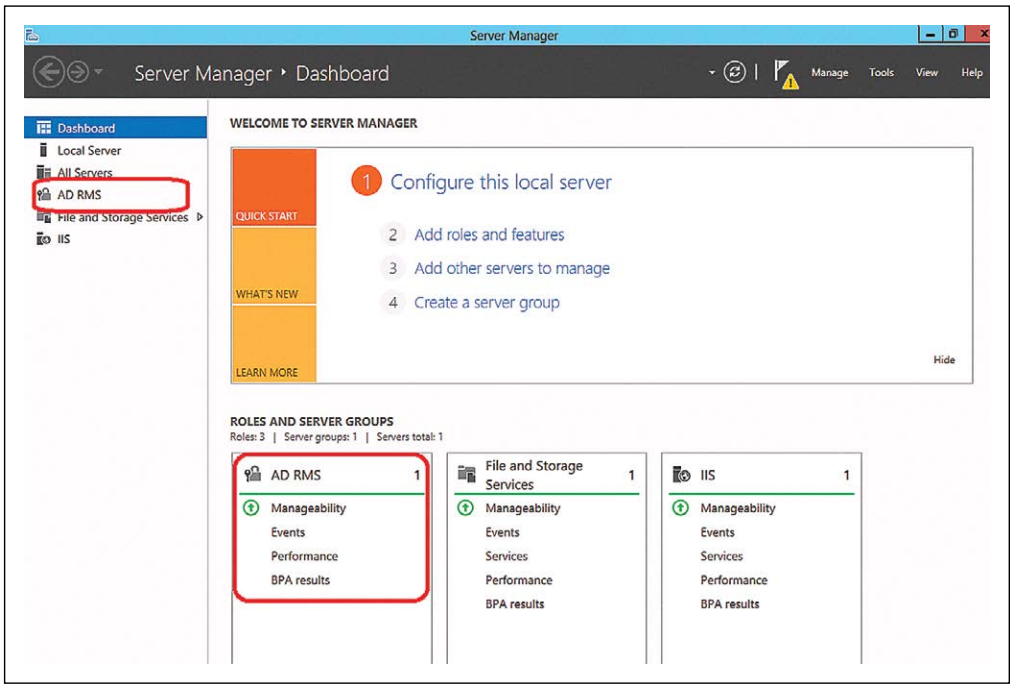


Figure 5. *The Windows Server 2012 Server Manager Menu showing AD RMS available for selection.*

AD RMS was available for Windows Server 2008, but the setup is much improved in Windows Server 2012. Therefore, this example is based on using Windows Server 2012.

Install AD RMS Role

The Windows Server 2012 Server Manager is a bit different than the one in Windows Server 2008 (see **Figure 4**). Choose Add roles and features from the Dashboard or from the Tools dropdown menu.

- Skip past the intro screen and select Role-based or feature based installation.
- Select Destination Server (select the VHD or server to which you want to install).
- Select Server Roles | Select Active Directory Rights Management. This will pop up a list of prerequisite services to install (.NET 4.5, IIS and so on). Click the Add Features button, then click Next.
- Select Features | Select Windows Internal Database. Click Next.
- Web Server Role (information only). Click Next.
- Role Services (AD RMS is selected) Click Next.
- Confirmation (click Install). No need to check the box to restart the server automatically as AD RMS does not require a reboot for installation or removal.

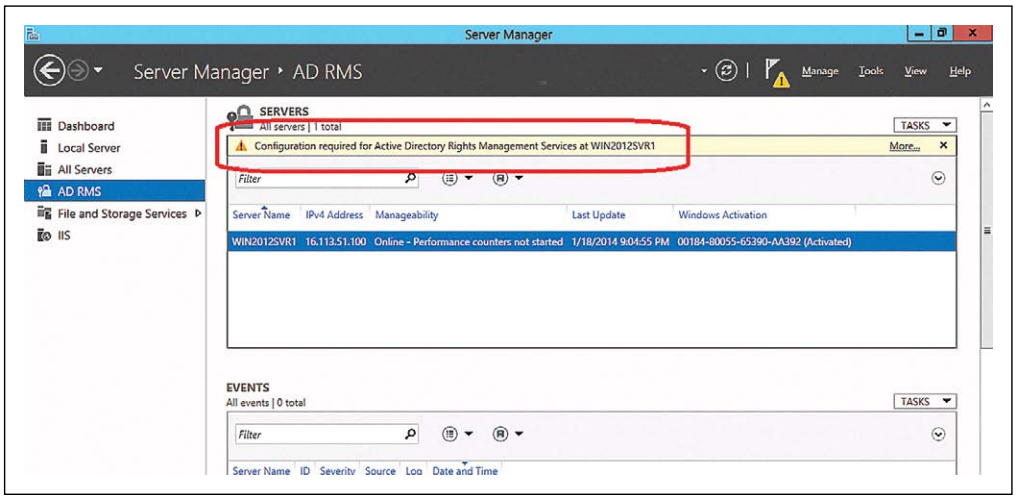


Figure 6. *The Windows Server 2012 Server Manager alerting that additional configuration is needed.*

Initially you must create a new AD RMS root cluster for certification and licensing, then you can join others to it or create other clusters for licensing only.

Following the installation, Server Manager will show AD RMS in the menu (see **Figure 5**, p. 17). Once you select it, you'll notice it needs configuration (see **Figure 6**).

Configure AD RMS Role

In the yellow notification box "Configuration required for Active Directory Rights Management Services at WIN2012SVR1" click More and the All Servers Task Details window will appear. Click the Perform Additional Configuration link (see **Figure 7**, p. 19).

- AD RMS Intro Page: click Next.
- Select Create or join an AD RMS Cluster. Note: There's a lot of information about the AD RMS Cluster that's beyond the scope of this article. Suffice it to say this is not a Windows Failover Cluster as you might assume, but a cluster of AD RMS servers. Initially you must create a new AD RMS root cluster for certification and licensing, then you can join others to it or create other clusters for licensing only.
- Select Create a new AD RMS root cluster. Note: In my testing I initially put AD RMS role on my Windows Server 2012 DC, but didn't configure it. Later I decided to create a server to use for AD RMS. I uninstalled AD RMS from the DC but when I installed it on the server (Win2012svr1) and tried to configure it, this step failed. The Create a new AD RMS root cluster was greyed out and an error appeared: "The SCP is registered but the root cluster cannot be contacted." Following a suggestion from the AD RMS forum (**bit.ly/1b1g37h**), I deleted the SCP attribute from the AD RMS

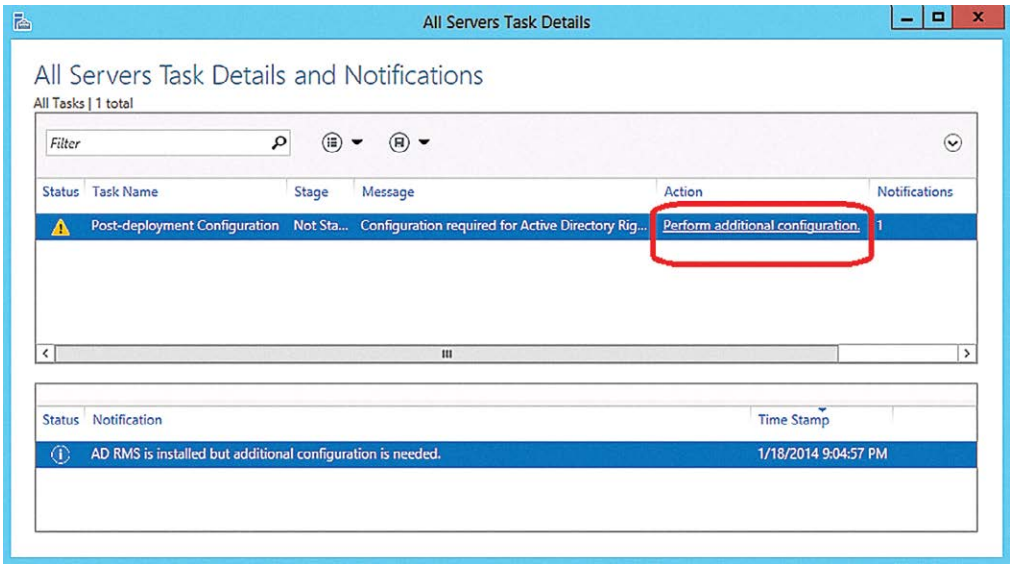


Figure 7. *The Windows Server 2012 Server Manager post-deployment configuration alert.*

This key is used to sign certificates and licenses the cluster issues.

object, then re-ran the configuration for AD RMS and the option was available.

- Configuration the AD RMS Cluster Database. If you have a SQL instance, specify it here. But this is just a lab so I'm going for the easy way and selecting Use Windows Internal Database on this server. (See **Figure 8**, p. 20). Click Next. Note: Windows Internal Database was installed as a role when the AD RMS role was installed.
- Service Account. Enter the username and password of the previously created service account (I'm using ADRMSsvc), which is a member of the Administrators group. Click Next.
- Specify Cryptographic Mode. I accepted the default, Cryptographic Mode 2. Click Next.
- Cluster Key Storage. This key is used to sign certificates and licenses the cluster issues. Because this is just a lab, I used the default AD RMS centrally managed key storage. If you have a CSP in production you can opt for that. Click Next.
- Cluster Key Password. This password is used to encrypt the cluster key. This is required to join other AD RMS servers to this cluster or to restore the cluster from backup. Note: this password isn't stored in AD RMS and is unrecoverable. Keep it somewhere you can find when needed. Enter the password and confirm. Click Next.
- Cluster Web Site. Select a Web site for the virtual directory. For this exercise I just used the Default Web Site but in production

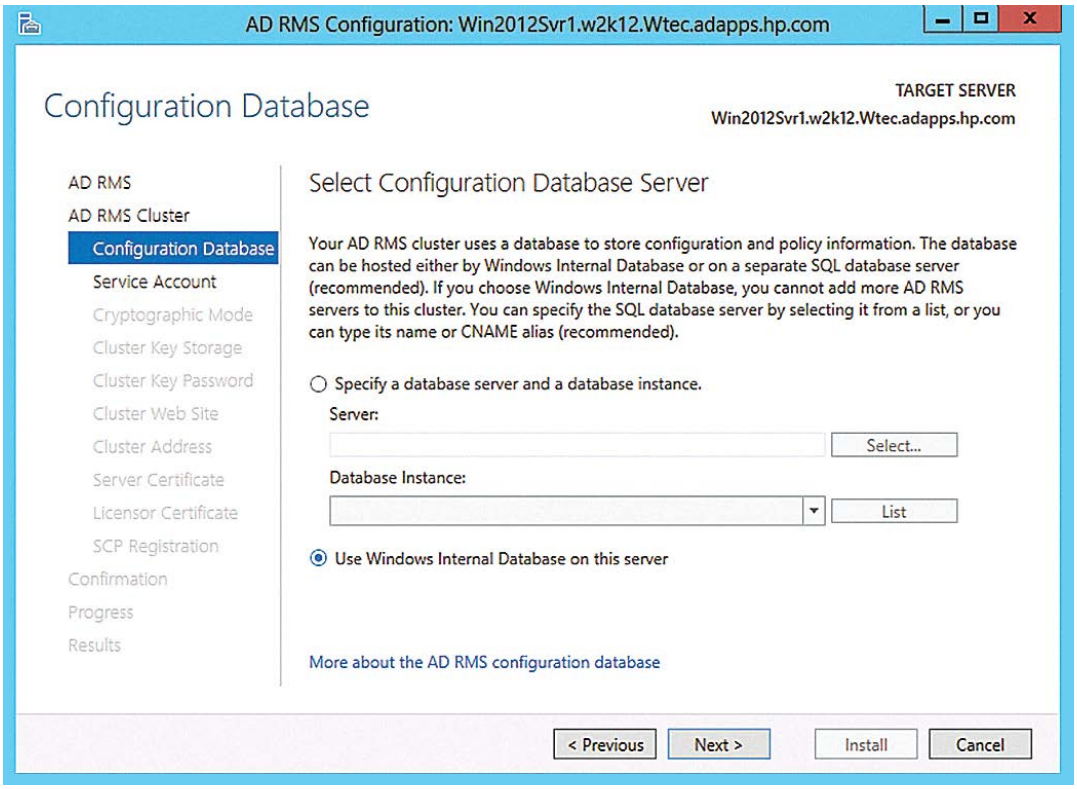


Figure 8. *Configuring the database system for the AD RMS cluster.*

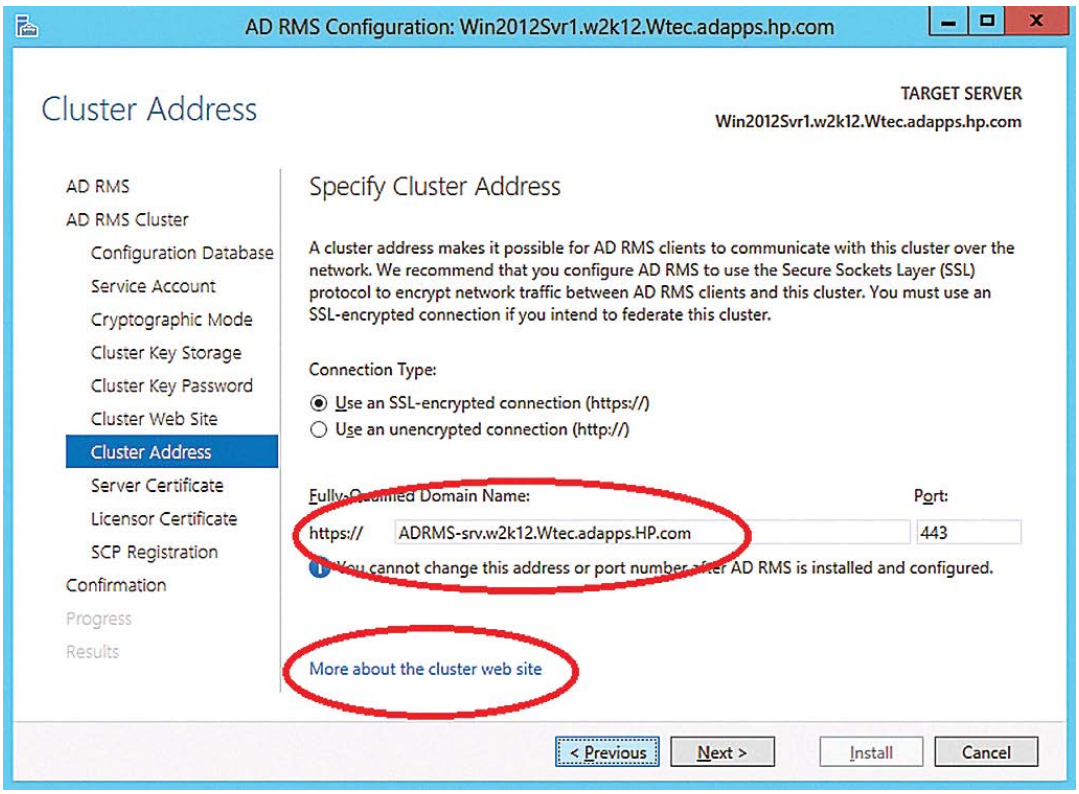


Figure 9. *You can specify a cluster address, which lets AD RMS clients link to the cluster.*

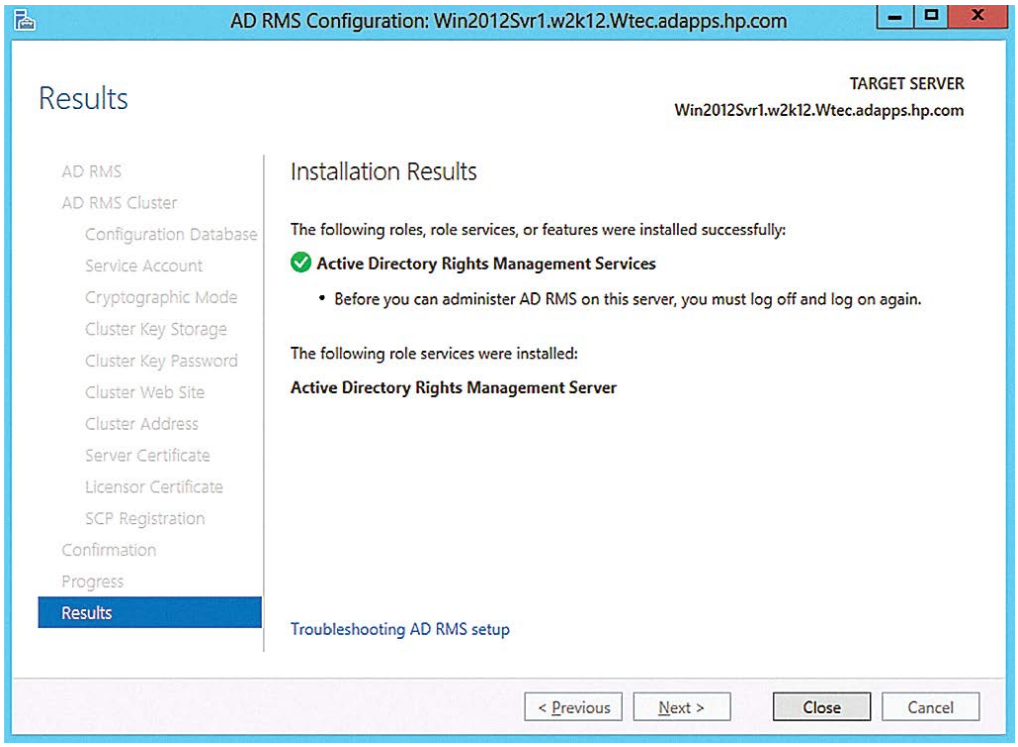


Figure 10. *The results of the installation, success or fail, appear and enable troubleshooting if necessary.*

Like any cluster, you must have a cluster address to permit communication among nodes.

you could create an original site to use. Click Next.

- Cluster Address. Like any cluster, you must have a cluster address to permit communication among nodes. Enter an FQDN in the box (see **Figure 9**, p. 20)—make it unique and easy to remember because you cannot change the FQDN or the port. My domain is W2K12.Wtec.adapps.HP.com. Click Next. Note that at the bottom of the screen on each of these dialog pages, there's a link to additional information on each step.
- Server Certificate. For this exercise I have no certificate authority set up so I'll use the self-signed option. Click Next. Note: Do not use the self-signed certificate for production for obvious security reasons.
- Licensor Certificate. Use the default name (or change it if you want). Click Next.
- SCP Registration. As noted previously, this is an Active Directory attribute on the RMS object in Active Directory. Choose the Register the SCP now option. Note: This page states the account you're using must be a member of the Enterprise Admins (EA) domain. If your account isn't an EA account, just continue. You can go into the AD RMS console and created the SCP later.
- Confirmation. Review the answers and Click Install.

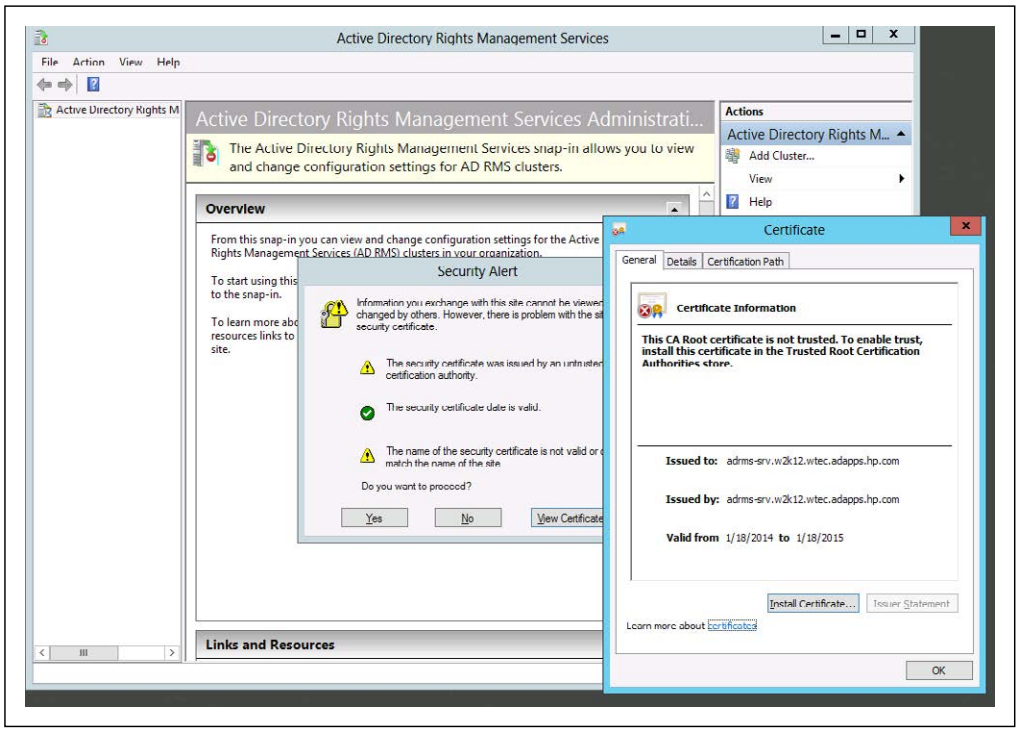


Figure 11. *This security alert is typical upon installation and lets you install a certificate.*

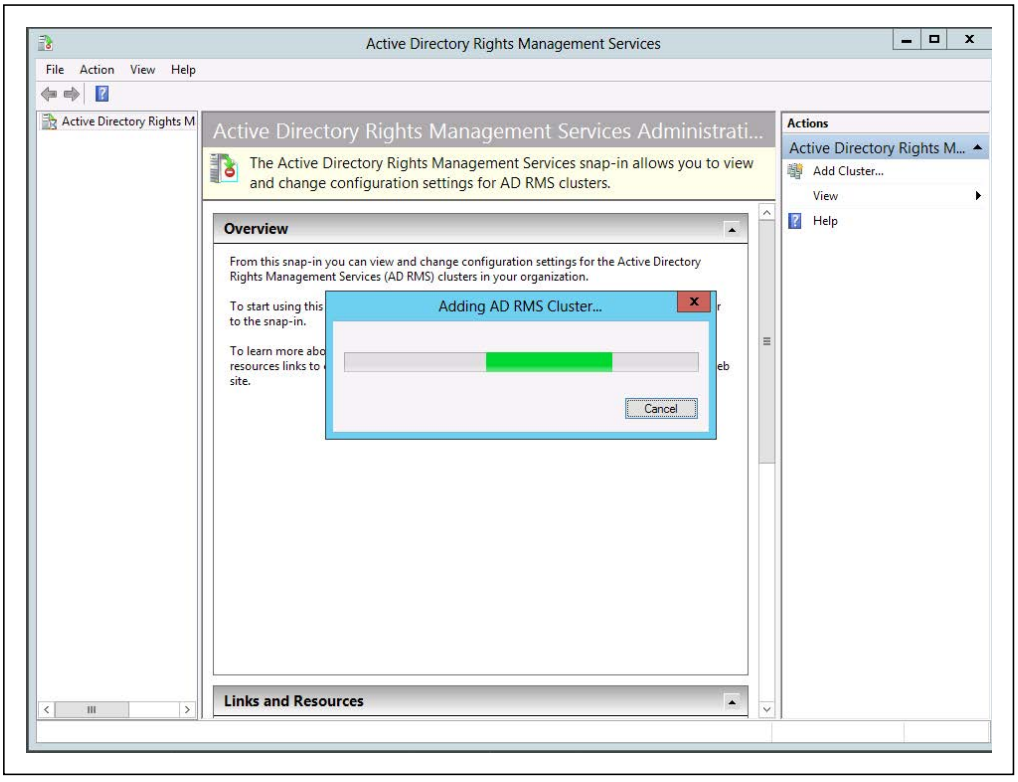


Figure 12. *A view of the AD RMS cluster being added.*

- Results. Success or failure of AD RMS configuration will be indicated here. Click Close. Note the Troubleshooting AD RMS setup link at the bottom of the Installation Results screen (see **Figure 10**, p. 21).
- Close the All Servers Task Details dialog. In the Server Manager, Click AD RMS. Note AD RMS is online and there are no errors.

The Active Directory Rights Management Console is now available from Server Manager. Opening this console you can see an expected security alert due to the self-signed certificate that was used. Select Yes to continue and the cluster will be added.

Using AD RMS

Windows Server 2012 has vastly improved many aspects of file security and management, including advanced security permissions and improved setup of AD RMS.

Of course, AD RMS is just the security engine that can be used in conjunction with applications as noted previously. Each application—Word, SharePoint, Exchange and others—each require configuration, which is beyond the scope of this article. Permissions can be set on a Word document by a user to restrict access to users or groups.

Windows Server 2012 has vastly improved many aspects of file security and management, including advanced security permissions and improved setup of AD RMS. Dynamic Access Control ties into these two features to make significant improvements in file security and removing the old clunky method of building security groups. Security can now be set by users on the file itself without an administrator creating specialized security groups and managing access. This is done on a granular level and allows the security to follow the file. While this is generally viewed as being the future in Windows, it's quite complicated and will take some effort to understand how to apply it in any enterprise. Now is the time to see how these new features can be implemented to make your enterprise and your files more secure. R

Gary Olsen is a Microsoft Directory Services MVP and a solution architect in the Technology Services organization of Hewlett-Packard Co. He is the founder and president of the Atlanta Active Directory Users Group (aadug.org).