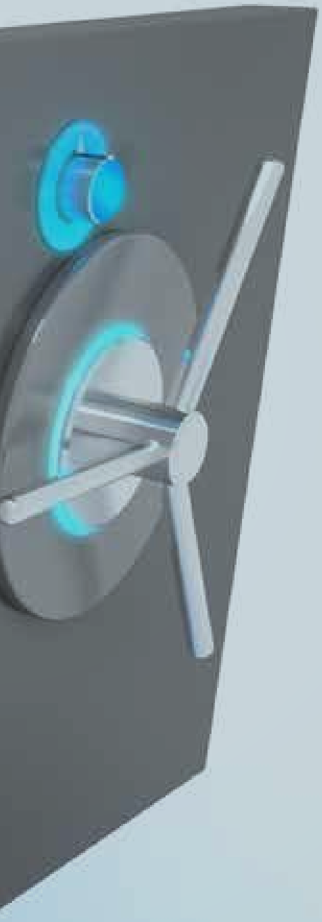
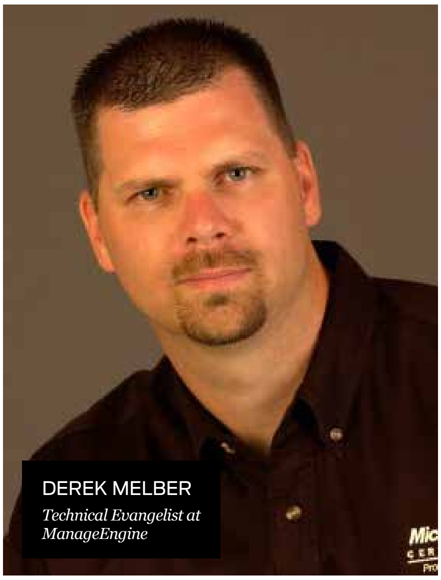


REINFORCING SECURITY BY REDUCING PRIVILEGED ACCESS

As I tour the world helping Active Directory administrators, security professionals, and auditors secure their Windows environment, I often get questions about privileged access, states Derek Melber, Technical Evangelist at ManageEngine. The questions usually are about how privileges are granted and how an organisation can know if its privileges are correct. These are great questions considering the onset of so many attacks on Windows in the past five to seven years. It is important to see that privileged access is usually at the core of these attacks.

> **THE MOST COMPLEX CONCEPT WITH REPORTING ON GROUPS IS TO GET THE RECURSIVE GROUP MEMBERS, I.E., THE USERS WHO ARE LOCATED IN NESTED GROUPS OF THE MAIN GROUP AND WHO NEED TO BE REPORTED AS WELL.THERE ARE PLENTY OF REPORTING TOOLS THAT CAN GET GROUP MEMBERSHIP RECURSIVELY, THOUGH. POWERSHELL BY MICROSOFT AND ADMANAGER PLUS BY MANAGEENGINE ARE TWO OPTIONS**



DEREK MELBER

Technical Evangelist at ManageEngine

There are many ways to grant privileges in a Windows environment. Granting privileges is rather easy. Reporting and analysing the current privileged access, however, can be a bit harder as there is no centralised location that shows an administrator or auditor the current privileged access. Understanding the different technologies and features that grant privileged access is the first step. Then, for each area where privileges can be granted, there are five steps that should be taken to ensure ongoing privileged access security. Those steps include:

- Reporting on the current settings;
- Analysing the settings to understand who has privileged access;
- Configuring the correct privileged access;
- Monitoring for changes to privileged access;
- Alerting, in real time, for key privileged access changes

The technologies and features in a Windows environment that grant privileged access include:

- Group membership
- User rights
- Delegation
- Access control lists or permissions
- Group membership

Depending on how the group is configured in the environment, it can have the highest level of privileges or just a few privileges. For example, the Domain Admins group has nearly the highest level of privileges in the entire Active Directory domain. Just adding a user to this group grants this level of privilege. However, the most complex concept with reporting on groups is to get the recursive group members, i.e., the users who are located in nested groups of the main group and who need to be reported as well.

There are plenty of reporting tools that can get group membership recursively, though. PowerShell by Microsoft and ADManager Plus by ManageEngine are two options.

User rights

User rights control global access over different aspects of a domain controller, server, or workstation. User rights are configured using Group Policy, giving granular control of each computer individually. Therefore, each computer could have a unique set of user rights, making the reporting and configuration of these settings difficult and time consuming.

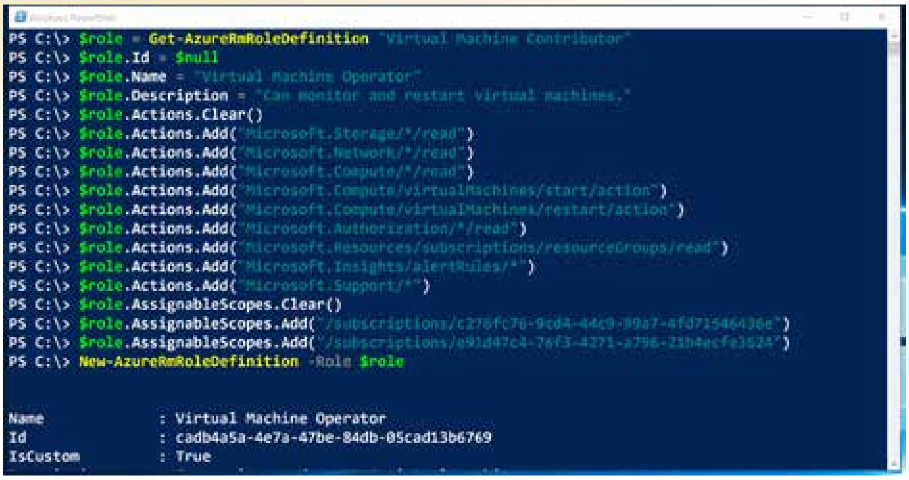
Every Windows computer comes with a built-in tool," secpol.msc", which can report the current user rights on each computer. The tool must be run locally, but it is extremely powerful and gives precise configurations. Since each user right provides some level of privilege over the computer, each and every user right should be evaluated and configured to meet the minimum requirements for server access.

Access control lists

Controlling access to files and folders is essential for assuring the security of data within any organisation. You need to properly configure the access control lists for your key data and ensure that they only provide access to the appropriate people. The wrong privileges granted to a file or folder could severely hurt, or even destroy, a company.

Reporting on who has access to a file or folder is a monumental task, due to the volume of files and folders on a typical network. Therefore, selection of the most important data must occur, and then those selected files and folders can be the focus of the security hardening. There are many tools that can help report on data access control lists, but if you do not want to purchase a tool you

USER RIGHTS CONTROL GLOBAL ACCESS OVER DIFFERENT ASPECTS OF A DOMAIN CONTROLLER, SERVER, OR WORKSTATION. USER RIGHTS ARE CONFIGURED USING GROUP POLICY, GIVING GRANULAR CONTROL OF EACH COMPUTER INDIVIDUALLY



```
PS C:\> $role = Get-AzureRmRoleDefinition "Virtual Machine Contributor"
PS C:\> $role.Id = $null
PS C:\> $role.Name = "Virtual Machine Operator"
PS C:\> $role.Description = "Can monitor and restart virtual machines."
PS C:\> $role.Actions.Clear()
PS C:\> $role.Actions.Add("Microsoft.Storage/*/read")
PS C:\> $role.Actions.Add("Microsoft.Network/*/read")
PS C:\> $role.Actions.Add("Microsoft.Compute/*/read")
PS C:\> $role.Actions.Add("Microsoft.Compute/virtualMachines/start/action")
PS C:\> $role.Actions.Add("Microsoft.Compute/virtualMachines/restart/action")
PS C:\> $role.Actions.Add("Microsoft.Authorization/*/read")
PS C:\> $role.Actions.Add("Microsoft.Resources/subscriptions/resourceGroups/read")
PS C:\> $role.Actions.Add("Microsoft.Insights/alertRules/*")
PS C:\> $role.Actions.Add("Microsoft.Support/*")
PS C:\> $role.AssignableScopes.Clear()
PS C:\> $role.AssignableScopes.Add("/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e")
PS C:\> $role.AssignableScopes.Add("/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624")
PS C:\> New-AzureRmRoleDefinition -Role $role


Name             : Virtual Machine Operator
Id               : cadb4a5a-4e7a-47be-84db-05cad13b6769
IsCustom         : True
```

can always use the built-in "xcacls.exe" tool, which comes with all Windows computers.

Delegation

The concept of delegation falls under the category of access control lists, but it is a specific term used for Active Directory and Group Policy management. Due to the complexity of Active Directory delegation, the configuration of the delegation is typically done through the Delegate Control Wizard. This wizard is located on the drop down menu for the domain node for each Organisational Unit in the Active Directory Users and Computers tool. The wizard defines which account (user or group) is granted a specific task. The most common tasks are resetting passwords for users and modifying group membership, both of which have a potential impressive security impact if the wrong account is granted the delegation.

The Delegate Control Wizard can only configure the delegations—it can't report or remove delegations. Therefore, a different tool must be used for each task. The built-in "dsacls.exe" tool is ideal for reporting on delegations for each Active Directory node. As for modifications to existing delegations, that is typically left up to manual efforts performed on the Security tab located on the object's Property page.