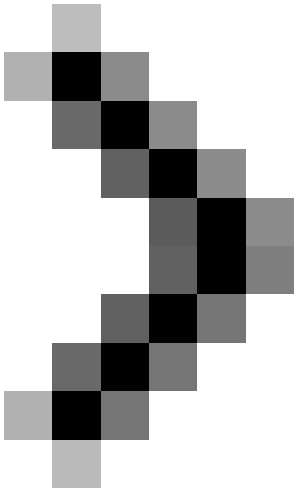
Configure Hyper-V security using Authorization Manager - Part 2

In this article, I will show you how to secure virtual machines when running on Hyper-V.



Configuring Hyper-V security with Authorization Manager - Part 1
Network administration - Securing virtual machines running on Hyper-V is an important task. Therefore, in Part 2, I will show you how to secure virtual machines when running on Hyper-V. Authorization Manager is a component in Windows. Hyper-V uses its repository to secure the Hyper-V parent partition and the virtual machines running on it. The policy settings for Hyper-V are stored in an XML file. By default, Local Administrator can manage all aspects of Hyper-V.

This section will focus on the following topics:

- Secure Hyper-V resources by using Authorization Manager

- Step by step in using Authorization Manager
- Hyper-V tasks (Task), Operation (Operation) and categories
- Simple example of using Authorization Manager

Hyper-V uses Authorization Manager to secure Hyper-V's Parent Partition and VMs. Before implementing them, you must be familiar with the basic terms used in Authorization Manager, starting with the following terms:

Authorization Manager uses the role access control model (RBAC). In this model, roles are allowed to access activities or tasks to perform an action listed in the activity list. Figure 1 defines the following terms:

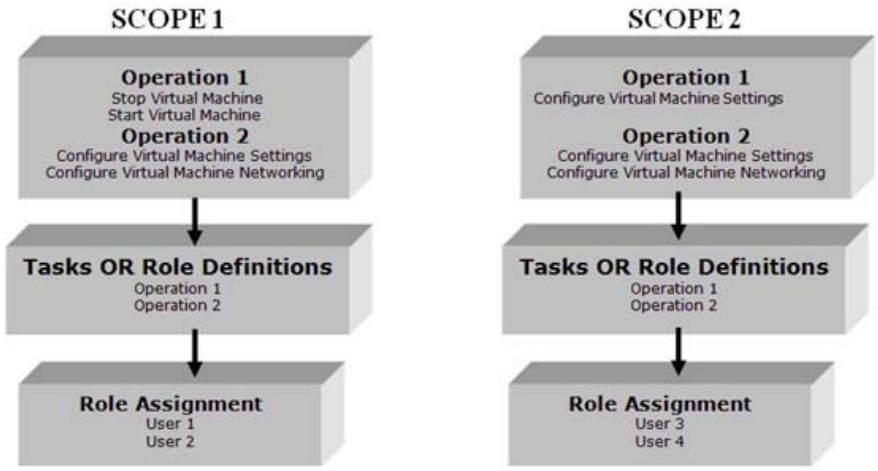


Figure 1: Authorization Manager RABC model

Scope - Scope: Scope is the boundary for a Role. You can create a Scope by right-clicking on the Hyper-V Services in Authorization Manager or by using a small script. When creating a new scope, there are three things related to each scope that you create in Authorization Manager as shown in Figure 2:

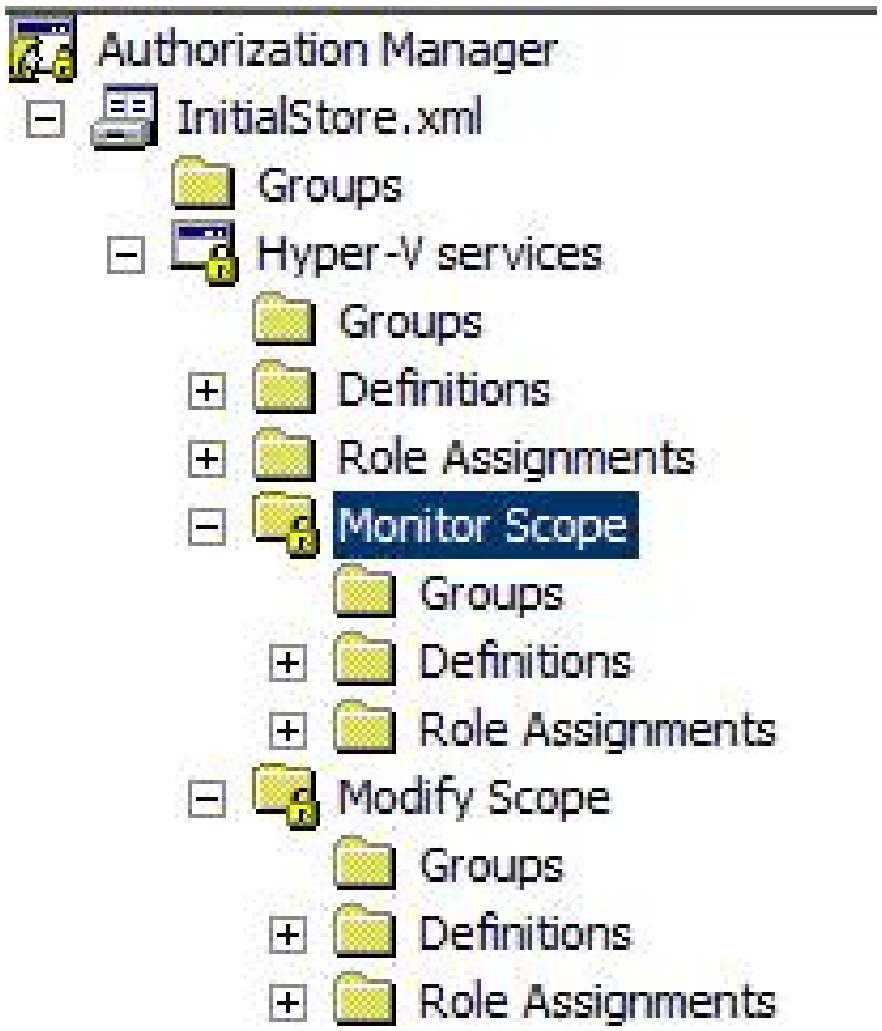


Figure 2: Screen of Authorization Manager

1. Groups
2. Definitions
3. Role Assignments

Operation - Operation: Operation is the basic licensing block. For example, stop and start a VM.

Task - Task and Role Assignment - **Role Definition:** Task is a set of activities, while Role **Definition** is a license assigned to Role Assignment.

Role role - Role Assignment: Role Assignment consists of multiple users assigned certain tasks or activities.

As shown in Figure 1, two scopes are created: SCOPE 1 and SCOPE 2. Both scopes include Operation, Tasks and Roles, but the permissions are different. The role defined in Scope 1 is User 1 and User 2, and Operation assigned to these Roles is "Start Virtual Machine" and "Stop Virtual Machine". Similarly, you can see in SCOPE 2, Roles here are completely different: User 3 and User 4. Scope 2 only has one Operation defined for User 3 and User 4: "Configure Virtual Machine Settings".

Operations, Tasks and Roles are defined in an XML file.

```
% SystemRoot% ProgramDataMicrosoftWindowsHyper-VInitialStore.XML
```

Note : The ProgramData folder is hidden by default on Windows Server 2008. You may need to show this folder to view the path above.

Hyper-V Server uses this repository. If the file is lost, the Hyper-V services will fail when starting. Hyper-V will initially read this file to get the permissions assigned to the VM. It then queries a registry entry shown below to get the path of the InitialStore.XML file:

```
HKLMSoftwareMicrosoftWindows NTCurrentVersionVirtualization
```

The above key saves two registry entries: StoreLocation and ServiceApplication. The StoreLocation entry defines the path of InitialStore.XML file and ServiceApplication entry defines which application in the policy the InitialStore.XML file is used. In this case, it is Hyper-V Services.

Tip : The InitialStore.XML file is installed only when you enable Hyper-V Role. If this file is lost or corrupted, you have the following two options:

- Copy files from a working Hyper-V Server

Or

- Install Install.WIM from Windows Server 2008 ISO, then search for InitialStore.XML. Copy this file to Hyper-V Server.

The scope of this article is limited to Hyper-V security, so we won't explain much about Authorization Manager and its features.

By default, Hyper-V Server defines a Scope, 33 Operation and a Role, all of which are stored in an XML file mentioned above. By default, Local Administrator on the parent partition is configured as the Default Role and all are granted privileges to configure Hyper-V and VMs running on it. You can view and configure them using the Authorization Manager MMC. The name MMC is AzMan.MSC. The user must be a member of the local admin group on the parent partition to be able to use Authorization Manager.

Step by step instructions for Authorization Manager

1. Go to Start Menu> type "AzMan.MSC"
2. Right-click Red Cross> click "Open Authorization Store"
3. Point to% SystemRoot% ProgramDataMicrosoftWindowsHyper-VInitialStore.XML> click Ok.
4. When clicking OK, Authorization Manager will read the InitialStore.XML file and load the content from this file to display in the snap-in as shown below:

Three main categories are defined in Authorization Manager to control Hyper-V Server and VM virtual machines. These items include:

- Hyper-V Services Operations
- Hyper-V Network Operations
- Hyper-V Virtual Machine Operations

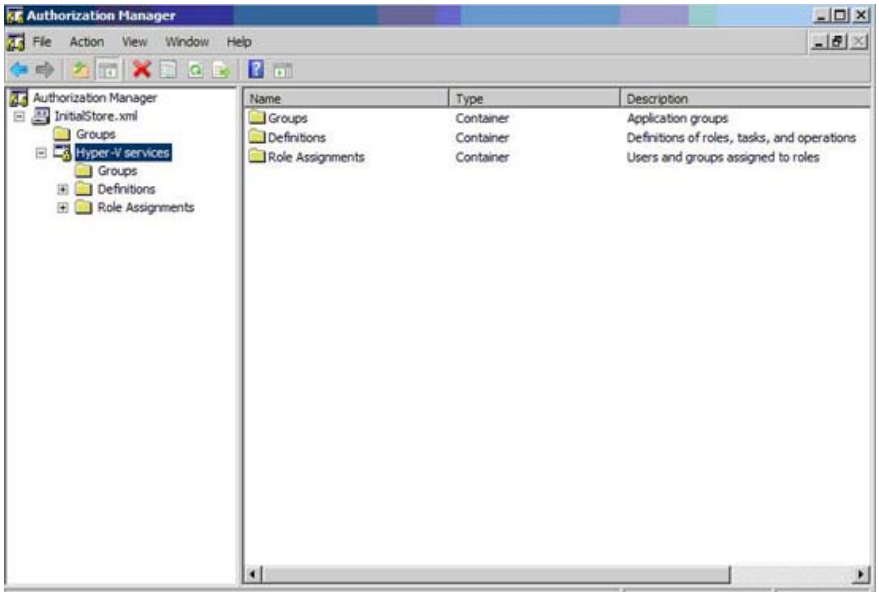


Figure 3: Authorization Manager Snap-in

As introduced before, there are 33 Operation activities. These activities are divided into the above categories. The table below shows the activities included in these categories:

As shown in Figure 4, by using Authorization Manager, you can delegate two types of operations to Hyper-V and VMs Configuration. These operations are: Modify or Read. These credentials are required in a large organization, where a team is responsible for changing the Hyper-V Configuration and a group responsible for checking Hyper-V VMs and others.

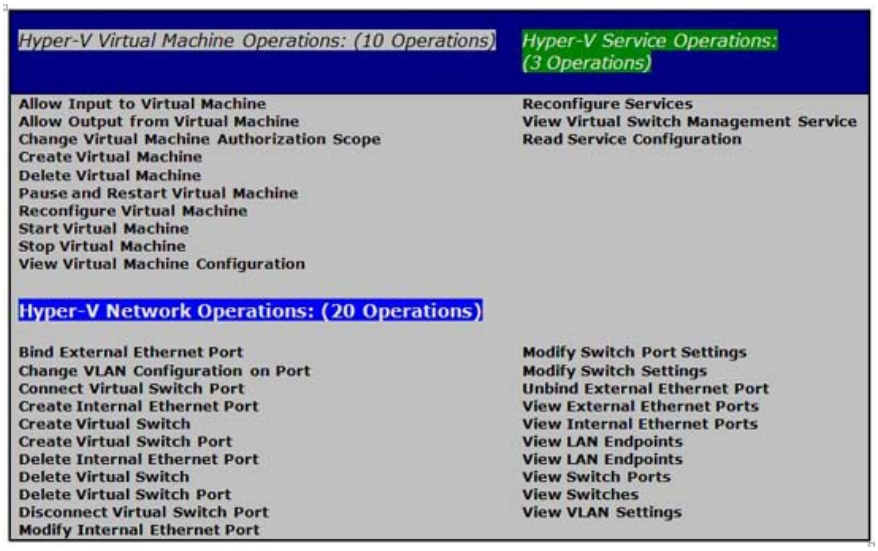


Figure 4: Items of Operation in Authorization Manager

Administrator Role is a role defined in Authorization Manager, including 33 default activities. This role fully controls the Hyper-V aspects, including virtual machines and its configuration.

The example will allow non-local administrators to manage Hyper-V servers and virtual machines.

By default, the local administrator on the Hyper-V server is allowed to control the Hyper-V Server and all virtual machines running on it. You can delegate this control to a user who is a member of the Active Directory domain. This is an example that allows someone in your organization to control the Hyper-V Server and VM instead of using a Local Administrator account on the Hyper-V Server. You can use Authorization Manager's Local Store for this example.

1. Open AzMan.MSC
2. Right-click "Open Authorization Store"> select the XML file from this location: ProgramDataMicrosoftWindowsHyper-VInitialStore.XML.
3. Click OK to open InitialStore.XML policy settings in Authorization Manager.
4. Expand Microsoft Hyper-V Services> Role Assignments section.
5. In the right pane, click "Administrator" and select "Assign Users and Groups" then select "From Windows and Active Directory".
6. Enter the name of the User or the Security Group you want to allow them to control Hyper-V and VM.
7. Click OK, then close Authorization Manager snap-in.

In the above example, users in the Active Directory domain can control the Hyper-V server and VM virtual machines running on it.

In the next part of this article series, I will show you the control on Hyper-V and the virtual machines running on it.

Conclude

In this section, we have introduced Authorization Model that can provide security for virtual machines running on Hyper-V Server. In addition, we also introduced some of the tasks available with Authorization Manager, providing a simple example of how to configure users outside of the administrator to be able to control Hyper-V Server and virtual machines.