Risk Reduction Lab

Joshua Main-Smith

2020-11-09

Contents

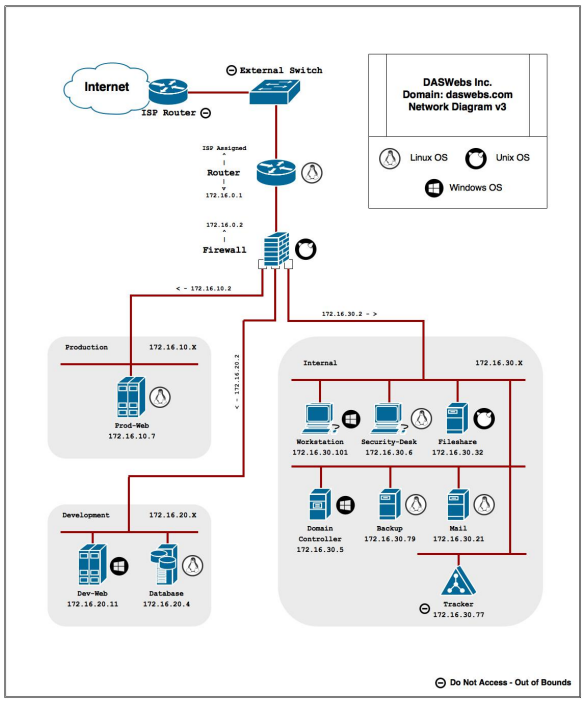
Risk Reduction

Introduction

After a few contractors came in and inspected the Active Directory configuration and security policies for DASWebs Inc., Thanh Akasaka contacted our organization with a few tasks needing to be done. This included:

1. Creating an Accounting and Human Resource organizational unit
2. Creating Accounting and Human Resource Security Groups
3. Move appropriate employees to these organizational units and security groups
4. Group policies for basic removable media threats and logged in user information leak
5. Restrict Accounting and HR from reading/writing to shared folders

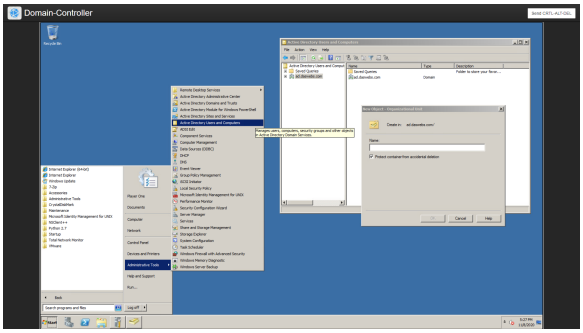
These tasks are to be performed on the Domain Controller which is running Microsoft Windows Server 2008 R2 Standard. The hierarchy of the company infrastructure can be seen in the image below.



Creating Organizational Units

An organizational unit (OU) is a container that can hold objects, such as security principles.These objects, located in directories, are classified to differentiate between objects to mitigate name collision or to manage a hierarchical authorisation structure (Source).

Here, we are tasked with creating an accounting and human resource OU. Adding an OU can be accomplished by selecting **Start ->Administrative Tools ->Active Directory Users and Computers**. Then, right-click **ad.daswebs.com** and select **New ->Organizational Unit**. This will open a popup that will ask for the name of the new organizational unit. Add two OU's, named **Accounting** and **Human Resources**. Keep the default setting **Protect container from accidental deletion**.



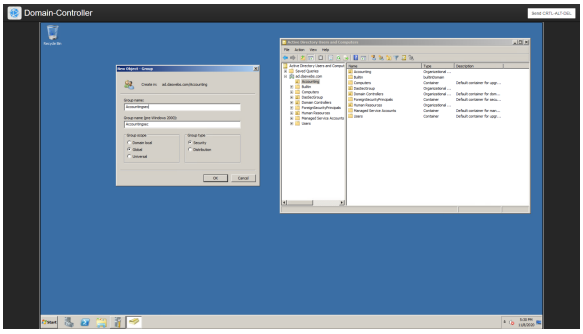
The only users we need to add to each of these OU's are Brimlock Stones for accounting and Sergio Chanel to human resources. To do this, we go to the **Users** directory under **ad.daswebs.com** and right-click the respective user and select **Move**. On the popup window, we select the location we want the user to be moved to (**Accounting** for Brimlock Stones and **Human Resources** for Sergio Chanel) then click **OK**. This will move each user to their respective OU.

Creating Security Groups

Groups are one of the containers within an OU, organizing its resources to match its business structure (such as users). Security groups are used to manage user rights, defining what a user is allowed to do within the scope of their domain. It also manages user permissions, defining their capability in relation to a given resource (Source).

We are tasked with adding two security groups: **Accountingsec** and **HRsec**. With the new OU's we created above, we are able to see their respective directories under **ad.daswebs.com**. For each new OU, right-click then select **New ->Group**. A window will popup and ask for the name of the group to add. The two groups, **Accountingsec** and **HRsec** will be added this way. **Group**

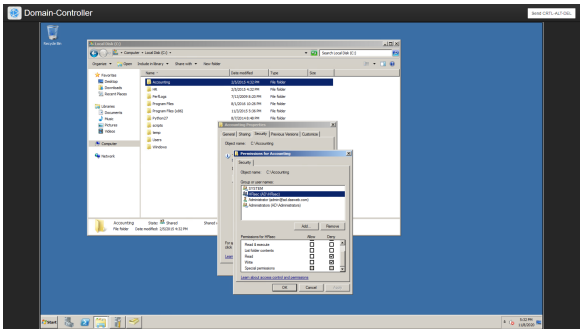
scope will be set to **Global** and **Group type** will be set to **Security**. Pressing **OK** will create the two security groups.



Adding each user to their appropriate group can be accomplished by navigating to the user's OU (**Accounting** for Brimlock Stones and **Human Resources** for Sergio Chanel) then right-clicking on the user and selecting **Add to a group**. Under **Enter the object names to select** input the name of the group each user is to be added to (**Accountingsec** for Brimlock Stones and **HRsec** for Sergio Chanel).

Configure Read/Write Access

By default, users are able to view and write to the contents of shared folders between OU's. This functionality should be limited to those who are only on a need to know basis. So, the accounting security group need not have read or write access to the HR security group. Likewise, the HR security group need not have read or write access to the accouting security group. What we do is add each security group to the other so that we can deny read/write privileges. The reason we do this is because each security group is only on a need to know basis within the scope of their own OU.

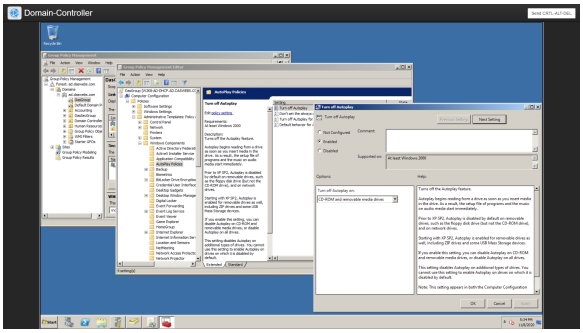


Configuring the read/write privileges of each group can be accomplished by first opening **File Explorer** then navigating the the C:\drive. For each group (Accounting and HR) right-click then select **Properties** from the dropdown

menu. Navigate to the **Security** tab. Under **Group or user names** click the **Add** button. Under the window that pops up, we can add the other security group (add HRsec for Accounting and Accountingsec for HR). Once we do this, select the newly added security group. Under the **Permissions** pane select the box under **Deny** for **Read** and **Write**. Then, click **Apply** and **OK**.

Disabling Removable Media Autoplay

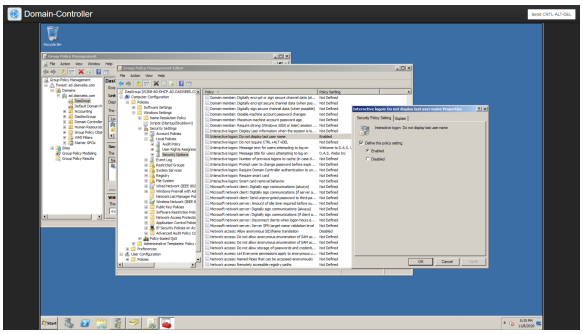
It may be a good idea to prevent autoplay on the CD-ROM and removable devices (such as USB) to prevent the propogation of malicious and potentially unwanted programs. AutoRun is a vector that some malware writers use to aid in spreading to other hosts. For instance, a removable device infected with malware will insert itself onto a host when inserted. Likewise, malware already infected on a host will detect a removable device being inserted and infect it (if not infected already) in the hopes that the removable device will be inserted into a host that's not currently infected (Source).



To disable autoplay, open **Start ->Administrative Tools ->Group Policy Management**. Then, right-click **Forest ->Domains ->ad.daswebs.com ->DasGroup** and select **Edit** from the dropdown. Under the new window that pops up, go to **Computer Configuration ->Policies ->Administrative Templates ->Windows Components ->AutoPlay Policies** then open **Turn off Autoplay**. Now, toggle **Enabled** and set **Turn off Autoplay on** to **CD-ROM and removable media drives**. Then select **Apply** and **OK**.

Handling Login Information Leak

Showing the username of the last user that succesfully logged in may be convenient, especially for users that regularly use the same work station, it could present the risk of unauthorized users attempting to log in. Limiting the view of available users on a given workstation can mitigate an attackers attempt in brute forcing (Source).



A group policy can be put into place under the **Group Policy Management Editor** by going to **Computer Configuration ->Policies ->Windows Settings ->Security Settings ->local policies ->Security Options** then open **Interactive logon: Do not display last user name**. With the window that opens, select **Define this policy setting** then toggle **Enabled**. Select **Apply** then **OK**.