Need to know details for Administrators

Essential knowledge: Creating an Active Directory Test Lab

Author

Bob Bobel

Cayosoft | Need2Know

About the Author

As a Product Management Director, Bob is responsible for driving innovation and strategy for Security, Compliance and Identity products. Bobel combines his twenty+ years of IT management and enterprise software experience to provide strategic vision to high-performance teams through times of growth and change. Bobel previously held Product Management roles at enterprise software companies Netwrix Software and Quest Software Inc. (Acquired by Dell in 2012) While at Quest, Bobel's role included creating the first true Active Directory centric Identity Management platform – ActiveRoles Server®. A frequent traveler, Bob resides in Ohio with his wife and two children.

Email: bob@cayosoft.com
LinkedIn: linkedin.com/in/robertbobel
Twitter: @rbobel

Overview

There are two primary methods used by administrators to implement Dev/Test environments to protect Active Directory from errors while they try out administrative changes. There are numerous options for creating an Active Directory test lab. The first method is to **clone** the directory and the second is to **recreate** the directory. Each has benefits and drawbacks that should be considered before choosing the method that meets your organizations requirements. Cloning keeps all object Security IDs (SIDs) identical to the production while Recreating will new SIDs for the objects. Both methods should keep the object names the same and that is typically the important part. Cloning may be seen by some as a security problem as well since you end up with a duplicate Active Directory with password hashes intact. I prefer Recreation of the directory because it is simpler, safer, more secure and can be extended to pull additional changes from production into test.

Cloning Active Directory (Keep SIDs intact)

Cloning is more accurate yet the more difficult of the two methods. Cloning is a one-time event the result of which must forever be disconnected from you production environment so that there is no chance of improper replication. There are two general ways people clone Active Directory. Both methods will require you implement changes to Active Directory such as seizing FISMO roles and potentially re-implementing services such as DNS, but with a lot of work it can be done. The result of cloning is that you very accurate clone of AD at that moment in time.

Option 1: Create a backup of an active directory domain controller then restore that backup new computer (VM or Physical Host) on a disconnected or sandboxed network. This method can get messy because of the restored OS will detect the hardware changed and you will need to repair the OS. In addition to fixing the OS you will need to update AD by seizing the FISMO roles with NTDSUTIL as well as configure a new DNS to work with this new environment.

Option 2: Create a computer on the production network (VM or Physical Host) and promote it to a domain controller. After it fully replicates, move the domain controller to a completely isolated network so that it has no chance of replicating with the source directory.

Recreation (Copy object without SIDs)

Recreating is less accurate it is vastly simpler and safer. Recreated directories are usually just as useful as a cloned directory and there is no fear of accidental replication back into production.

Option 1: Setup a new Windows Server (VM or physical host) and install DNS and Active Directory; this will be the home of your dev/test directory. When you configure AD choose a domain name that is similar, but not the same as your production domain. For example, if my domain name is bobbobel.com, make the test environment domain name bobbobel.devtest. On a domain controller

your existing production directory use either the LDIFDE or CSVDE utilities to export the data in Active Directory. (Technet article on using CSVDE) I prefer CSVDE because the resulting file can be opened and modified in Microsoft Excel allowing you to find/replace names. Using LDIFDE or CSVDE import the file into your new domain.

Option 2: Writing a PowerShell script that copies the most important objects from production to a dev/test environment is actually very simple. In this case you create a new host with a new dev/test domain as you would with option 1, but instead of using LDIFDE or CSVDE you write a PowerShell script that will copy the OU structure, user objects, group objects, group memberships etc… until you have enough detail to meet your requirements. I like this approach, because the scripting that is required is typically one or two lines per object type and examples are easily found on the Internet. I also like this option because you get ultimate control over what you copy into dev/test and you delete your dev/test objects and re-run the scripts to get an up-to-date picture of your current production environment.

Conclusion

Having used both cloning and recreating, I have rarely run into a situation where re-creating the directory did not meet my requirements. For dev/test I almost never need the SIDs or passwords to be identical to production and I never enjoy dealing with FISMO role transfers or repairing the OS. So in my mind I would always choose re-creating the directory using PowerShell until I ran into some situation that would force me to consider cloning.

Cayo | Software™

To get additional practical whitepapers from Cayo | Software, please visit www.cayosoft.com.

WARRANTY

The information contained in this document is subject to change without notice. Cayo|Software makes no warranty of any kind with respect to this information.

Cayo | SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Cayo | Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

Cayo | and Cayo | Software are trademarks of Cayo | Software, LLC. in the United States of America and other countries. Other trademarks and registered trademarks used in this document are property of their respective owners.

For additional information please see our web site at (www.cayosoft.com)

This page intentionally left blank