Benji Gifford | David Thomsen | Micah Kezar
Team "Snyder Cut"

SYS255 Final: Subdomains

DESCRIPTION

Team Snyder Cut will research, plan, deploy and test our own subdomain. We aim to create a domain and then give it a subdomain in Microsoft Active Directory, featuring a private file share that uses one-way trust.

OVERVIEW

We are going to be using David's Virtual Machines (mostly just AD02-david, AD03-david and WKS05-david (as well as BLOG01 and FW02)) in order to create a new domain (dota.local) and create a subdomain (dotatwo.dota.local) and setting up a one way file share system on that subdomain.

REFERENCES

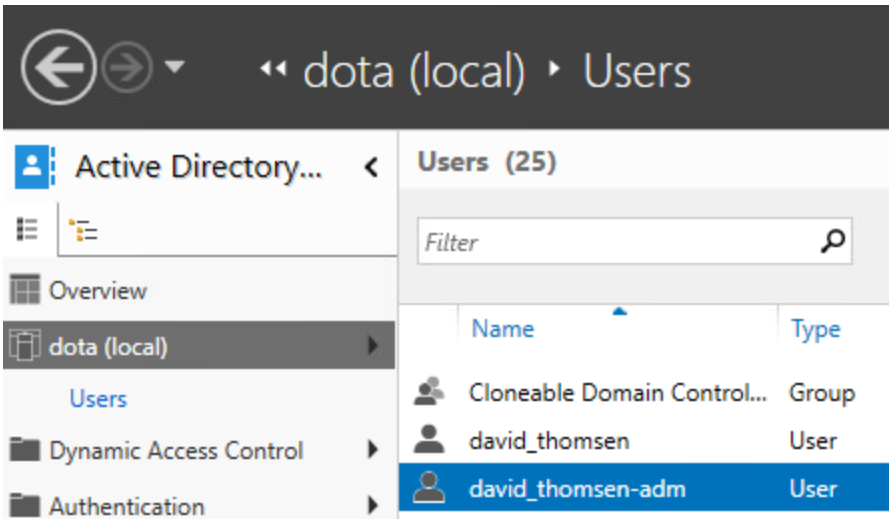
https://www.manageengine.com/products/active-directory-audit/kb/how-to/how-to-create-child-domain-in-windows-server-2012-r2.html

A LOT of trial and error troubleshooting that can be read down below and screaming at AD which I have not included as I'm sure you do not want to hear it.

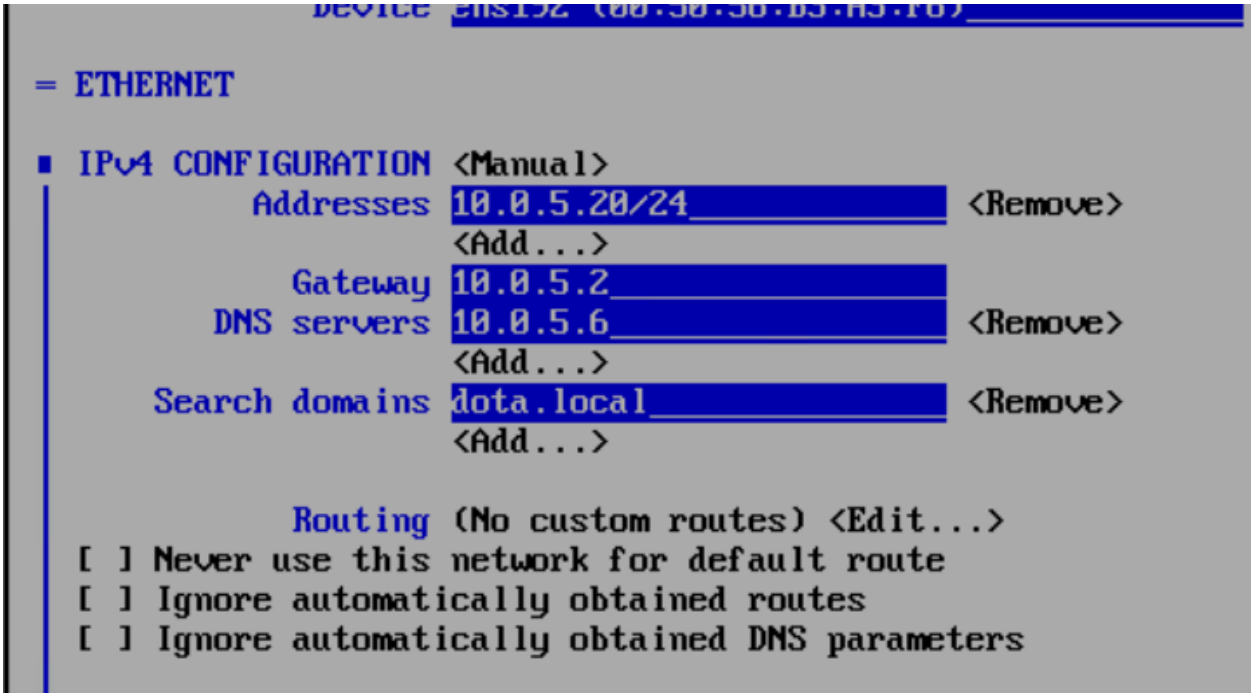
BUILD DOCUMENTATION

1. First off, we had to remove the current domain we had on our domain to compensate for our new domain, because you can't have two domains running at the same time and on the same AD.
2. Once we deleted the old domain, we then created "dota.local," and created an admin account and a standard user.
3. We then added in the local admin account as well as the regular local account.
4. Connected WKS05, BLOG01& FW02 to the new domain. Configured this on the individual machines and add them to the host and pointer records in Server Manager.
5. Made AD03 and created the local accounts same as on AD02
6. Created the subdomain (dotatwo.dota.local)
7. Did this all over again on AD03
    a. Needed a second AD in order to control the subdomain
        i. This was an issue that we had to struggle through as we were not aware that this was a necessary step to this process and tried to do it all on the one AD
            1. This did not work well to no one's surprise.
8. Made sure all the computers could communicate with each other
    a. This was by far the most tedious step and took days of troubleshooting and clicking the same things again and again until they worked properly
        i. Testing and reconfiguring DNS, FW, BLOG, and, Both ADS
        ii. Getting stuck with permissions and file shares
        iii. Giving the right users the right permissions
        iv. Getting locked out of the WKS due to an error we saw 100 times trying to fix.
            1. "The security database on the server does not have a computer account for this workstation trust"
        v. Figuring out this trust issue

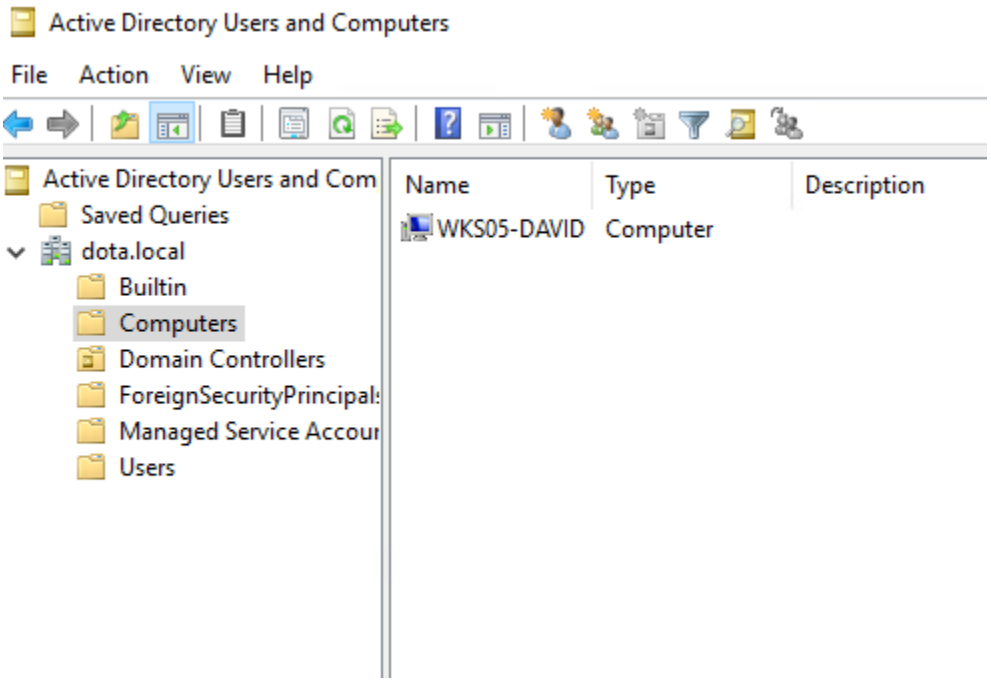
        1. Ended up being solved by logging in as champuser and connecting to the domain so that the other users could be accessed.
9. Create the file share
    a. On AD03, in the "All Servers" list in Server manager, right-click on AD03 and click "Computer Management"
    b. Shared Folders > Shares > New Share > "share-name" (ours is named "Shares")
    c. Configure the permissions so that the admin account has full control over the share, but the admin account on WKS05 and AD02 can only read it.
        i. This was actually surprisingly easier than the setup to make this possible.
10. Test the file share from both the WKS as well as the AD03
11. Make this write-up
12. Film the test video
13. Submit



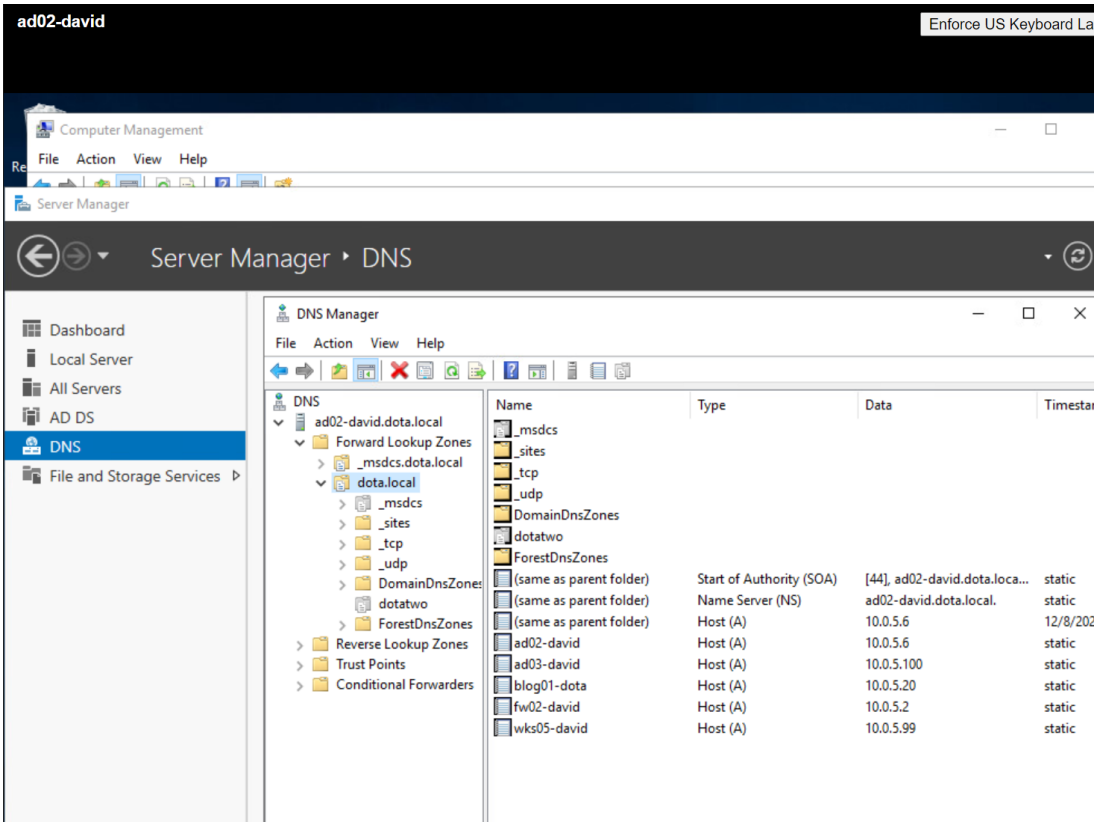
Creating the new users and setting up the AD for dota.local.



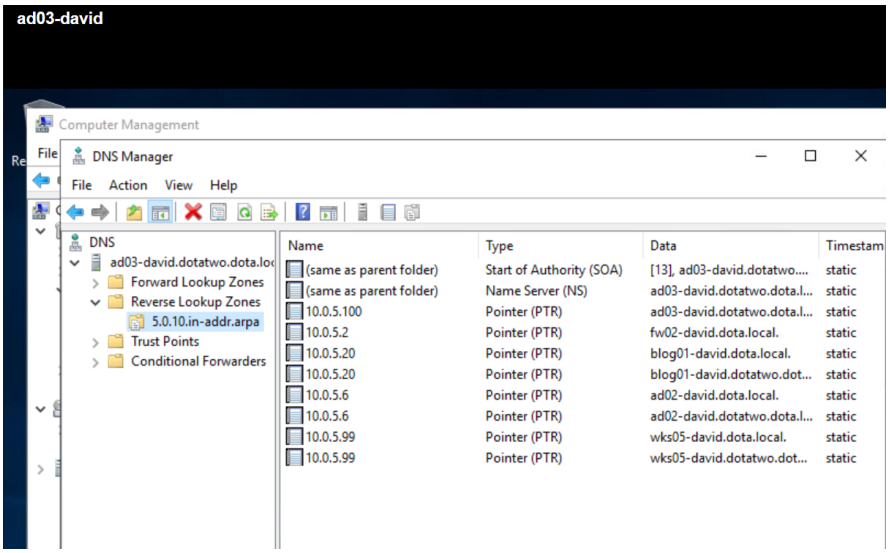
First, we had to switch all of the domains on all of the computers from david.local, to dota.local. This assured that all of the devices were properly connected to the new domain we created for this final.



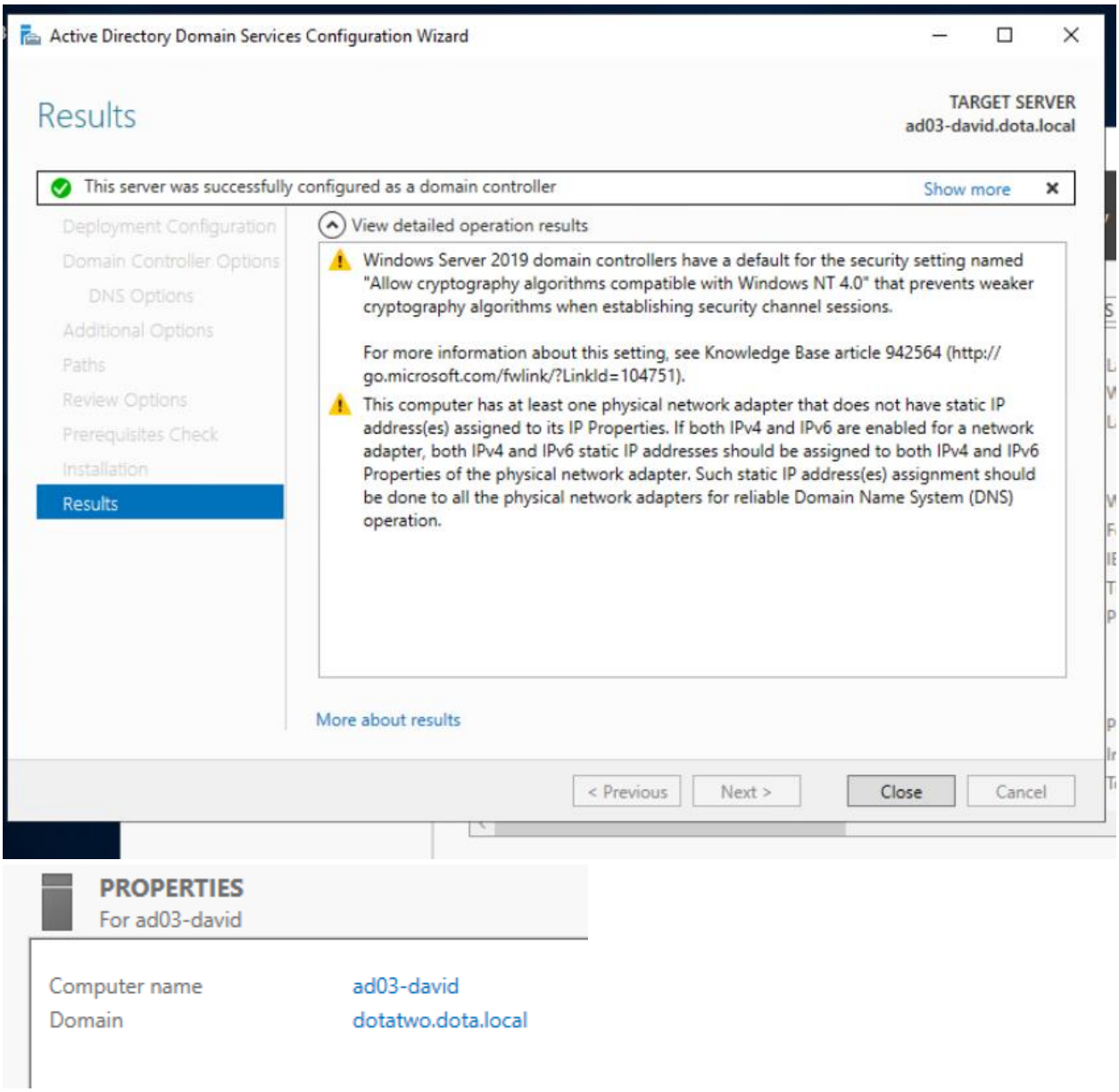
Connecting the Workstation to the dota.local domain



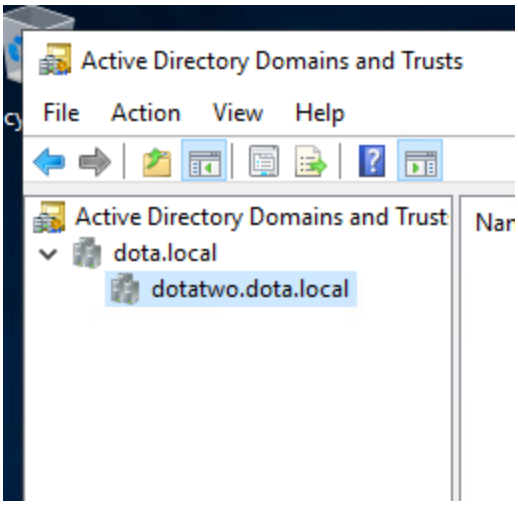
We had a big conflict with our A and PTR records, but once we resolved all of them, the devices were able to communicate with each other without error.



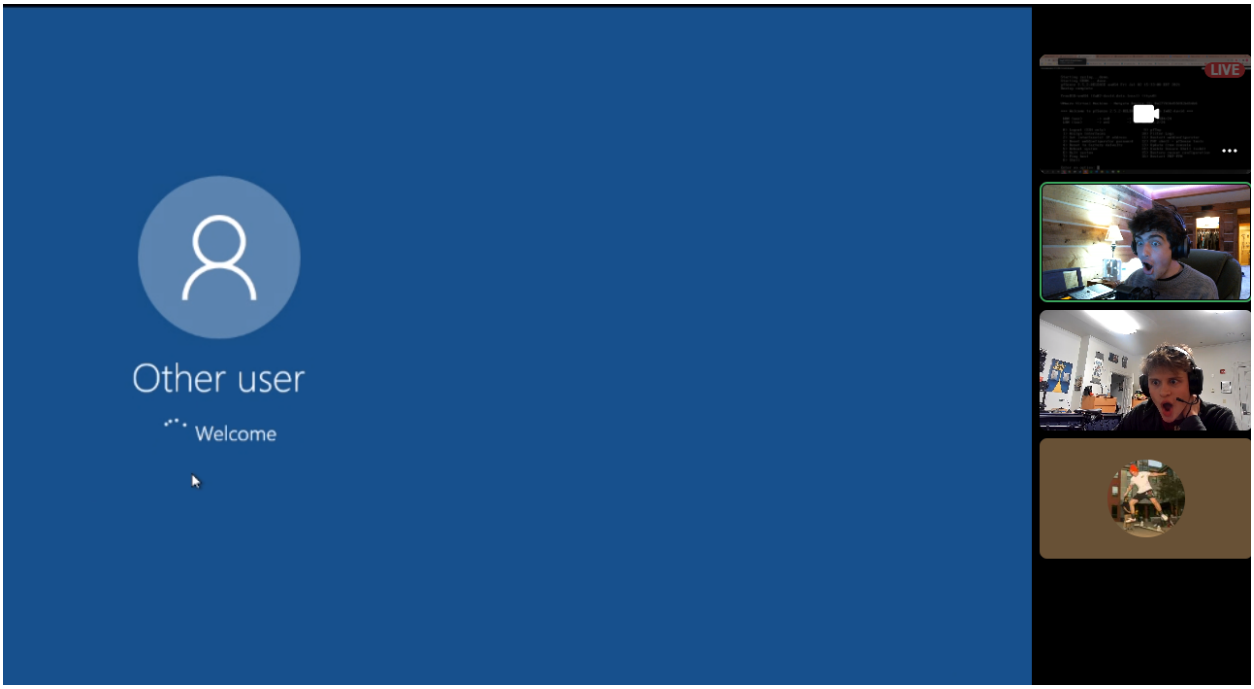
Setting up of the DNS on the Domains so they can connect to all the other machines.



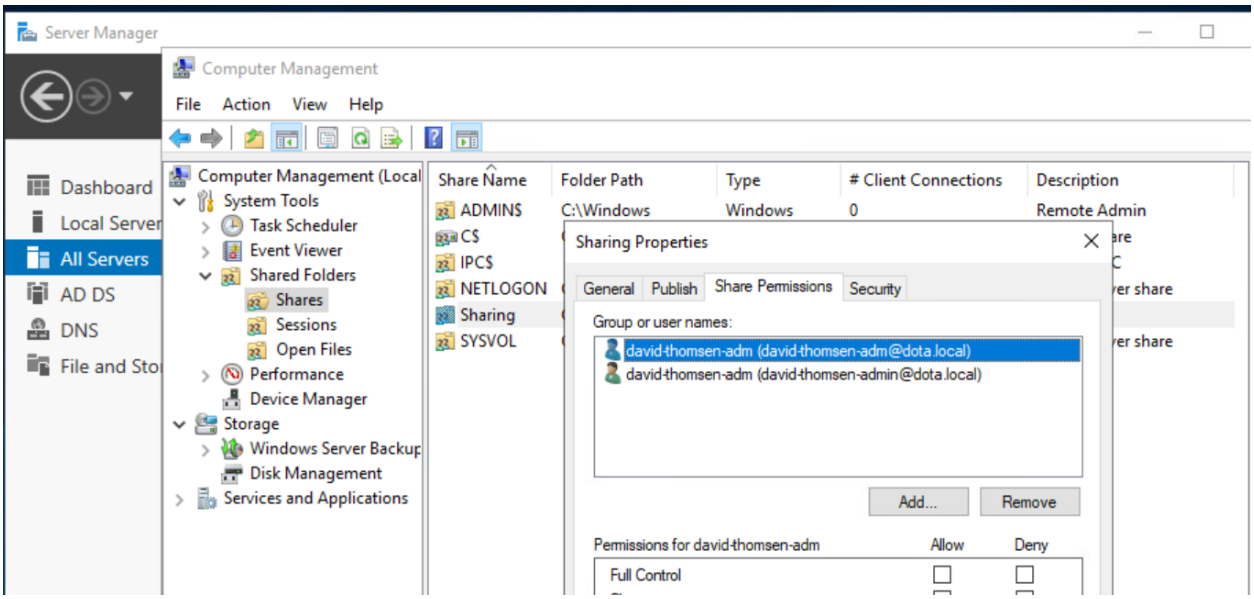
The creation of dotatwo.dota.local as well as the promotion to Domain Controller on AD-03



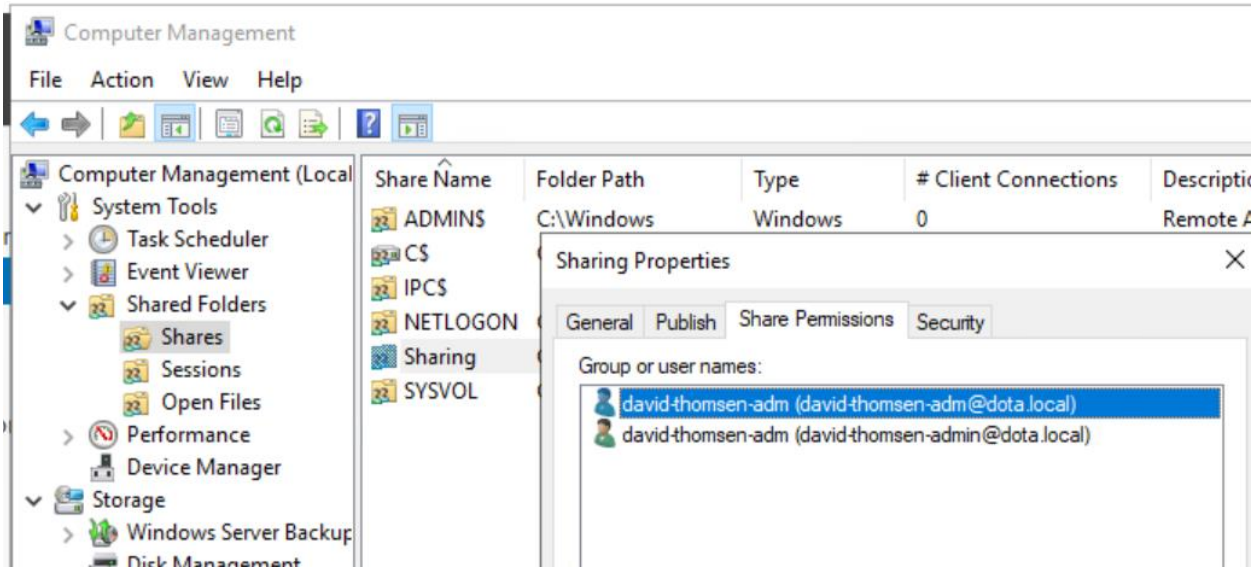
This screenshot shows the successful addition of dotatwo being added as a child domain to the dota.local main domain.



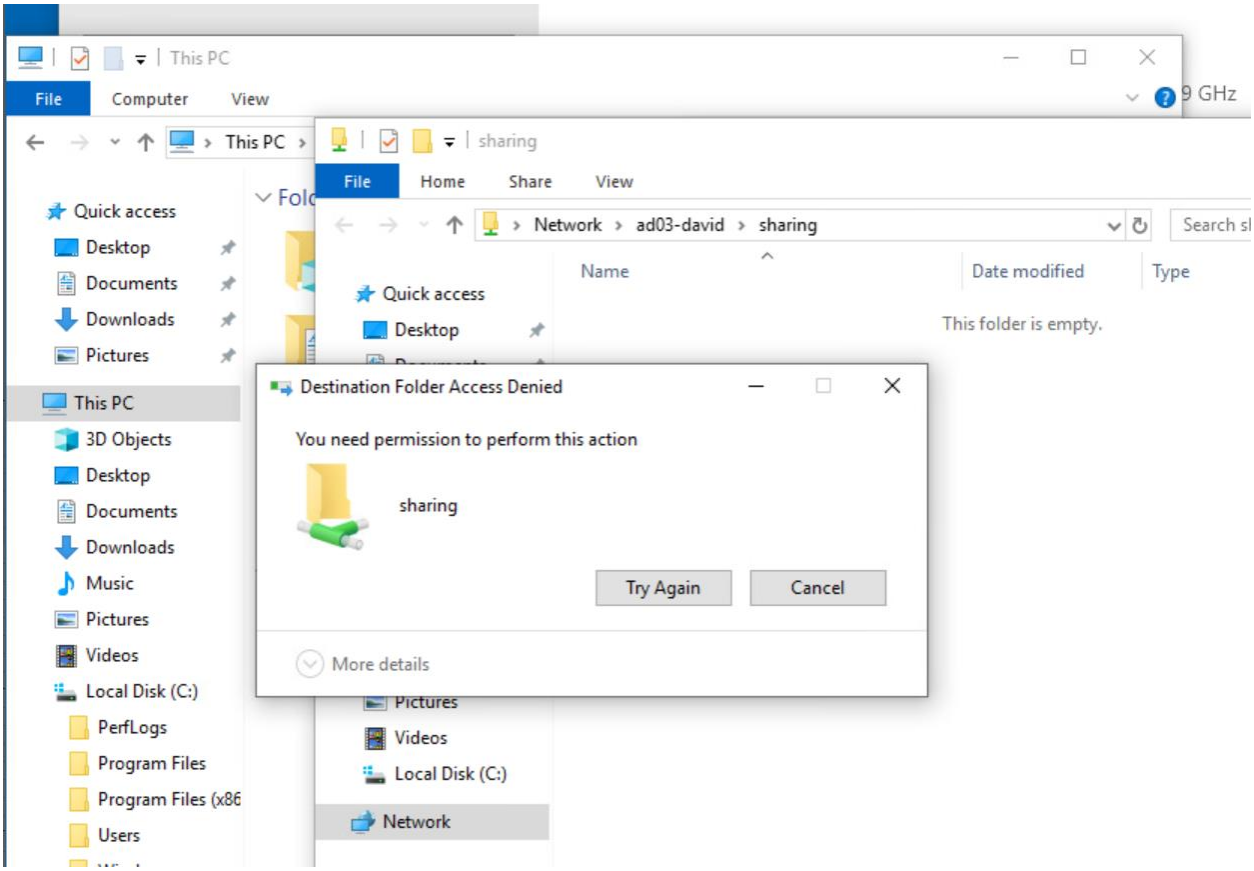
We accidentally forgot to change the WKS to be a part of the new domain, so logging in to WKS was a pain. The local administrator account got disabled, and we couldn't log in with any of our domain admin accounts. After 30 minutes, we finally got in by using the champuser account and the Ch@mpl@1n!21 password. We had our jaws on the floor when we had seen the screen say welcome and not give us an immediate error, only to get the same error again.



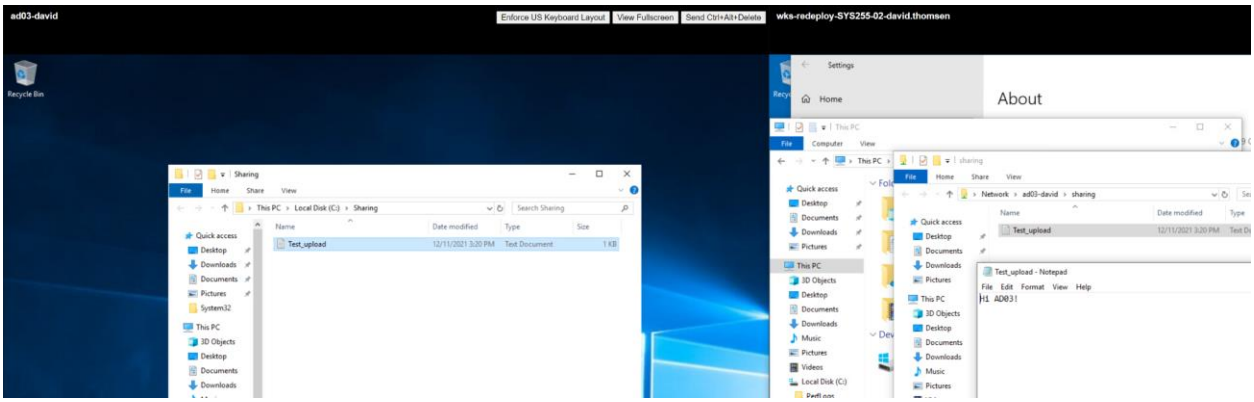
First, we shared the Sharing folder (\\AD02-david\Sharing) with the admin account first to make sure it could only read, and then we started to set up other permissions (david-thomsen-adm is AD02/WKS05, david-thomsen-admin is AD03).



These are the further permissions so that **adm** account can read, but not write. But the **admin** account had full control.



As you can see, WKS does not have permissions to do anything other than reading.



A successful upload from the AD03 that was able to be read on the Workstation.

TEST VIDEO - https://drive.google.com/file/d/1U1m0OHP3nOkMO2RmXg9qpXkihPIH1eNj/view?usp=sharing

Corrections on the video because I don't know how to edit footage:

- 0:20 Virtual Machines*
  - Not "the workstations and stuff"
- 0:32 AD03*
  - Technically AD is right but forgot I had to be a bit more specific with it now that I have two AD boxes.
- 1:50 AD03*
  - Not FS03, I don't even have a device called that so I'm not sure why I said it.

DISCUSSION

1. To start our troubleshooting process, we first had to start by deleting david.local. Once this was done, we replaced the old david.local with a new domain called dota.local.
2. The next step of creating the subdomain is where a lot of the trouble sets in. There was no definite tutorial to really explain how subdomains work, so it made things very tough. We spent a long time trying to figure out how to create the subdomain on the same device as the main domain, just to find out that it's not possible. We had to get a secondary AD server dedicated to the subdomain we wanted to create.
3. After we had the third AD and two domains, it was a pain in the neck trying to get all the devices to communicate with each other for no reason other than our own idiocy
   a. Was not able to ping WKS for hours only to find out that the windows firewall was on and blocked ICMP packets.
4. Once we got the second AD up and running as well as communicating, then created the child domain, it was a piece of cake.