Questions for Design Walkthrough

Wednesday, December 1, 2021

Attendees:

Machine generated alternative text:
Oluwaseyi Mafi 
Host, me 
Ann Marie 
Bianca Moon 
James Rose 
Joseph Rocha 
Nicole 
Terri Ann Quiambao 
Tyrell Jarrett 

Location: Webex

Date: 12/1/2021

AGENDA:

Machine generated alternative text:
Active Directory Enterprise Domain Structure 
Blue = One-way to each 
Pdchs.local 
CVTY.COM 
Healthds.com Bswift.net 
Meritain.com 
Additional Supported AD Forests 
AETDMZ.com 
HealthEHost.com 
Omnicare.com 
Heath 
AETH.aetna.com 
Forest trust 
Red = Two-way 
Blue = One-way 
Retail 
CORP.cvscaremark.com 
Minclinic.local 
CVS.com 
CaremarkRX.net 
PCARE.Ltd 

Jim: Yes it is most recent domain structure. Within forests, there are domains. If you want to have a trust. If there is an agreement and a trust created, then a two way trust relationship is created. (100% trust each other) With Miniclinic and caremarkrx - means caremarkrx trusts miniclimic but miniclinic does not trust caremarkrx for a two way relationship to occur. I can find out the reason why. There are some restrictions between the businesses.

AETH is the core domain. We have one way trust with the domains on the left side. AETH computers are trusted, but the inverse is not the case. After the acqusition of aetna, We implemented a 2 way trust between all CVS domains and the Aeth domain.

**Can you show a configuration file for CaremarkRx and Minclinic?**

A lot of Aetna employees have multiple IDs. Still a discrepancies. Sometime people have accounts in caremarkerx and also have corp.cvscaremark accounts.

The forest on the left sides of image above, these are companies that Aetna had purchased over the years. (Lines of business) They are still active. Payflex is an example. The decision was to do only one way trust, only do two ways trust if integrating all domains. When there is a one way trust, If ever we sold that part of the business, it is a lot easier.

**Who makes the decision whether domains are two way trusted or one way trusted?**

Jim: It was driven by our team. Our goal was to have fully integrated company. We go through a full security review. Discuss what we want to do, how we want to do, risk assessment before final sign off.

Jim: I can provide that information that shows the relationship that was established.

Jim: The relationship between Aeth and CVS happened last year

There were some IP conflicts. There are networks that are not routable. We had to wait for a network team, and firewall team to remediate that before it was established.

Two way relationships go through global security review. Our group (Jim) is responsible for authentication. Inclusive of networks. There cannot be conflicting networks. Second part is, firewall rules that went into place. 700 domain controllers. Making sure each one can talk to each other. Network, global security, firewall and the AD team came together prior to implementation.

**Are these all the structures?**

Jim: Believe there is omnicare domain. A standalone domain. We have ATDMZ, that's another domain that allows to externals - Buffer with internal and outside of our internal domain.

Jim: I can provide diagram of additional domains. There are no trust with them. For ATDMZ, you will need to have active accounts in those domains to get access. We are mainly concerns with the internal domains as shown in the image above. We also have pre-production domain, but not captured in the domain structure image.

Machine generated alternative text:
Domains 
users 
groups 
computer obj 
forestgpos 
HCB — includes qa/test 
forests 
domains 
aetna.com 
Domains 
users 
groups 
computer obj 
forestgpos 
enterprise 
enterprise dcs 
users 
groups 
computers 
gpos 
232044 
153286 
171449 
110 
349,531 
119867 
581,575 
273153 
2159 

There are subdomains.

Jim: I can call them out in a different document.

Majority of the DCs are in Cvscaremakr and CaremakrRX.

HCB - All pre-production account.

Aetna - 4 domains There are 3 sub-domains. We are going to decommission one domain soon.

**What is a subdomain used for?**

When you create a new forest. The recommendation is to create a route forest. Where it is empty, you can create sub-domain for lines of business. Any devices that are not windows based, we put into. We deploy Dcs and we have segregation. It is for structuring/isolation. You can create a one way trust. We do not do one way trust in sub domains however. It gets it complicated.

There is a project where we are shutting down the non-essential domains. As we migrate users, once done, we are able to remove the domain. Saving complexity, time, money.

Once the third party domains users are move from CVTY.com, they are rerouted to AETH.aetna. They inherently already have accounts with Aetna. Struggle we have is apps are configured a long time ago. We haven't had a requirement for new domain in a while. Inherently you don't build new domain, try to establish what is already existing.

**What happens to data hosted in Deactivated domain?**

All of that is moved over to AETH, and ensure everyone has proper access. The data is beyond the scope of this team knowledge.

**Understanding the Group policy Management - What are the default GPOs, GPOs created for specific domains/domain controllers?**

Ann Marie: It is per domain. We try to keep them consist simple and unified. There are password settings which are same across all domain,. There are specific GPOs across servers. Etc. We are working to simplify. Settings that are domain wide and platform.

**What are the driving forces to differentiating domains?**

Those are the same across the board. There might be different settings for specific devices, that is not applied across the board.

**Password setting**

Defined by global security, and we configure then in GPO in the domain.

**How often do they change?**

They are set for every 90 days. User is required to change password. 8 password in length, Can't reset to the same password used. Upper case, lower case, idle timeout. Account will lock after 5 invalid. And lockout will be after 30mins. 10 mins idle timeout.

Ann Marie: We can provide screenshots of this settings

Jim: Most of our admin account are in the password vault. They have a 8 hour duration by default. We have another tools that manages admin accounts. 15 password length, a lot more restrictive.

**Does each member of your team have an admin account?**

Jim: Yes

**Any restrictions, make changes to any domain?**

Jim: Currently we are not using cross domain account. Domain admin account is the highest account. Only people that have access is our team. In Aetna we only had one account to manage. You can have one account to manage all domains but we do not have that set up that way.

Jim: We can share the configuration password settings for the admin accounts.

**Review the domain trust relationships**.

Jim: I can prove this information. Some of these were done via email. We will submit in Auditboard. Our team handles this.

**Understanding how segregation of duties is structured for Critical Active directory Functions.**

Jim: You have to be in a specific group to manage access. We (Jim) have the highest account to manage anything.

**Any of these changes? Are they logged?**

We do not make any changes that does not go through change process. The testing environment is made for standing things up, and if it breaks, doesn’t matter. Any infrastructure, we put in a change to see if it works. All changes that go in QA, we send change notifications account. Active directory changes, mostly active directory changes. We support the exchange team, and we do updates in the active directory. Some are changes we do, and some are requested of us. Any major change, GPO changes, update (high impact) we do in QA.

Jim: We will be able to provide. It is multi-tiered. Fully documented.

**Are there any standards for defining these group policies or is it a custom fit based on business needs?**

Ann Marie: Yes. Defined by global security. Product owner, business owner may have a different requirement, We help to implement and track those updates for the platform owners. Sometimes, we may suggest an alternative. We work with Global security, if anything that might not be going down the right road, we work with them to get a solution.

**Any concerns?**

Ann Marie - No. We are still working to do clean up on the retail side. A massive review and cleanup effort. We continue to unify our group policy across board and simplifying is the key.