Security of Domain Controllers Walkthrough

Friday, December 3, 2021

1:01 PM

Attendees:

0" Oluwaseyi Mafi 
Host, me 
Ann Marie 
David Kaemmerer 
c) Grant Gilliam 
James Rose 
Joseph Rocha 
Michael Shanahan 
Sarah Kubiak 
Saurabh Dilip Saxena 
c) Steve Barrett 
Terri Ann Quiambao 
C) Tyrell Jarrett 

Location: Webex

AGENDA:

**What does the domain controller contain? What information is contained.**

Any resource that is in the company. All user account, computer accounts. Service account that run application. All information is stored. We are employed to make sure everything is secure. The IAM team oversees provisioning. We hold the information. We do not facilitate.

Our team. We set privilege access. System account, access needed. Within access directory, there are some built in role. Domain administrative roles restricted to our team. Configuration, server builds. The next most utilized role. Account operator role. Manages computers in the environment. You can create account, delete user. What we have done in the past, is we create and delegate information. Have ability to go in AD, and set specific permission. You want to add computer into windows 10 OU. (Add, update, and Delete) that is one OU. We put account operators group, and restrict access. There are several Ous. If SQL server team wants permission. We work with them to delegate permissions. Compartmentalizing their access. Privileges are delegated to a subset.

We have archer polices, enterprise configuration, change control. We hold everything.

Those are the baseline tools.

In all the servers, there are console access. It is restricted by group. You can look at the server, restart and reboot it. Even with the local console, one still needs credentials, elevated rights.

**Are there antivirus in the domain controller?**

Jim: I can get a list of things installed on that.

There are certain containers within active directory that are restricted. Have to be domain access level.

Semantic and crowd.

**Service packs for Microsoft?**

SCCM. That's the tool we use for deploying. We have a testing QA in the HCB side. On the CVS side, we have crest. We schedule every 7 days.

Grant - We have vulnerability scanning that are done. The MSB program is validated monthly to show the security baselines are in check. This goes in line with the batching. PSS. Not HCB. For the vulnerability scanning.

Scanning is weekly, and MSB is monthly.

Grant: If it is a high severity, the repair time is faster. If it is a medium or low, the time is extended. If there is an exception, but in place, it will be documented, to identify any of these venerability.

Domain controller, there are many copies of it. All the changes in domain are replicated. Designed by default.

**Why do we have the amounts of domain controllers?**

Instead of backup, we build redundancies. In Azure we have central. We build Domain controllers in each region. Built in pairs for redundancy. If one patch has a problem, the other will pick it up - Patches are for the servers, not the AD. Never patched a data center. One data center one night. The patching cycles within CVS health is robust. 7 day patch cycle. Pushing things out pretty quickly. Patching is done by global security (Standard Microsoft patches). We have a whole team that looks at the Microsoft patches. HCB is different from PSS and retail. Start with lower patch (least impactful) and move to the higher one. It is well defined.

In data center, if there is a high load situation, we try to balance it.

**How do you know which domain controllers are active?**

Jim: Sites and services. Say HCB. A certain data center has IP ranges. Within active directory, we take a physical model, we take the networks in the data center site and map them directly to that site. Any of the machines covered in that site, it will cover them. It is IP based with workload. The master slave configuration does not work anymore.

**Have you ever had to implement an emergency patch?**

If there is anything critical, we have meetings. We can possibly do it a quicker than we do now.

**Is the process of patching defined? SOP**

Yes, we do. If something does not get patched. We look back and check. We have other teams who look into this for us as well.

**What is your ticketing system for change management?**

Service now

There are enterprise changes that covered everything. There are times when there are freezes - point in time when we don't do anything for some time. For instance, during enrollment, informational updates are sent to us.

When we decommission. Everything goes through change control. Say we need new capacity, we build. We continuously upgrade our domain controllers to the latest. We have 2016 and 2019, coming from our 2012 to a supported newer version.

When we decommission, we don't do as much. When we decommission, we can remove active directory. It ignores it and leaves as a basic server. Either we shut it down or leave it.

We have always leased our hardware. The physical server have a 3 year lease cycle. Inclusive of any new OS version. The VM environment, it is the same. We order new servers, and prep for the replacement.

Windows operating system - 2019, 2019.

Linux, Mainframe system, Mac. They all have other teams. We are only responsible for the windows operating system.

**Peak Performance**

There are redundancies to handle peak load. We have built new data center over the years specifically to address this.