AD Management Walkthrough

Monday, November 29, 2021

Attendees:

Machine generated alternative text:
Oluwaseyi Mafi 
Host. me 
qo Ann Marie 
David Kaemmerer 
K) Gary Francis 
O James Rose 
c) Joseph Rocha 
Julie Gonzalez 
c) Nicole 
Saurabh Dilip Saxena 
Terri Ann Quiambao 
Tyrell Jarrett 

Location: Webex

AGENDA

* 1. Understand the active directory environment – Multiple Servers / OS managed through Active Directory
  2. All teams involved in the management of AD and their responsibilities, POC for each of those teams
  3. Understanding the policies and procedures leveraged
  4. Gain an understanding of any Management Reporting on KPI’s / KRI’s
  5. Get an understanding of any defined SLAs related to AD Management Incidents

------------------------------------------------------------------------------------------

**The team involved in Active directory, roles and responsibilities in managing active directory?**

Julie: Two sides. Administration - Julie, Jim Rose, Ann Marie. Take care of infrastructure supporting active directory. Policies and standards are owned by security department. Split is between data and infrastructure. Infrastructure support is owned and governed by WCS workstation and core services (Under Julie) Specific team is authentication services.

**Setting up a new domain, is that under infrastructure?**

Julie - Correct, WCS is responsible for that.

**How is active directory used to store and manage several services?**

Jim: We try to keep up to the most current version. Enforces tightening security constraints. All of our domains are 2016, not quite 2019. Can double check.

**Using 2016 console?**

Believe in HBC side, majority are hosted in 2019. Basically, from a user perspective, you won’t know the difference, however tooling is the same. The differences however are noticeable on the back end infrastructure that AD works on. It can be managed by tools that are backward compatible.

**With WCS, any segregation of duties? Someone responsible for different task?**

Involves group services. The only people that manage the environment are the people in the infrastructure team. Environment is restricted.

**Your team responsible for any configuration related changes?**

Yes, specifically our team. We manage that (James Rose)

**How do you make decision on logging information change? How is that managed by your team?**

Those decision of config, upgrades, stays with our team. We work out as team or call on Microsoft to help us out for logging, if it is a security requirement, that is a policy we have to abide by, usually by audit team, or global security. Requires a multi-team.

**Any control standards that you follow? Any documented standard for your team?**

James: When it comes to domain controller and setting up, we have a documented process of what is required. When we are done, we do a server post check to make sure the server meets expectation. It is tailored to enterprise. The process is documented. A bit different on HCB side. They have different tooling in CVS vs HCB. But same security. Performing same functions, just different approach.

**Who owns the standard and procedure document?**

We do. Doesn’t change much. If tools change, whoever builds the server will update it accordingly.

**While managing the whole infrastructure, do not need to involve any outside WCS group?**

Depends. We have domain DNS, and the engineering team support. Other than that, hard to determine who manages different aspect. We put a request for piece of hardware, and then that's when we take it. Mainly the WCS team or James team is responsible. Highly managed environment.

**Who is the POC?**

James Rose. Confined to his team.

DNS - Domain Name Services.

James - Active directory SME. About 12 people (engineers) Not sure how many server we have, couple hundreds. It is a large infrastructure.

For example - Want to get into a SharePoint site - that's managed by IAM (Administrative) Managed by group access, held in the active directory.

There are no third-party tool. It's all managed by the Microsoft Azure environment. Certain tools you can use with lesser privileges. You can search for users in a domain (as a trusted user) given it is a read information. The private information is restricted by Domain level access.

Machine generated alternative text:
AutoSave 
File Home Insert 
Calibri 
Paste 
Clipboard 
A14 
CVS 
Nov 2012 VAD _ St 
Formulas Data 
- Read-Only • 
Review 
Page Layout 
Font 
Alignment 
2 
3 
4 
13 
14 
Domains 
OCS 
users 
groups 
omputer 
f orestgpo 
136 
171449 
1379 
HCB — includes qa/test 
t orests 
domains 
aetna.com 
15 1 Domains 
16 OCS 
17 users 
18 : groups 
19 1 computer 
20 forestgpo 
110 
349,531 
119867 
228673 

James: To be honest, hasn't changed much. This looks like the monthly statistics. Should be Nov 2021. Next week, there will be December stats pooled. They are due by the 10th of month. Next Friday.

James will provide Query used to generate Stats.

Is there segregation by organization unit?

There is domain, then work station, under that, different operating systems. Mostly Windows 10.

Machine generated alternative text:
Active Computers 
File V. 
.nd Computers 
M.eosx 
M. ged 
Ops 
O bj«ts 
Org 
SCI 
M.•wqed Aæts 
OSK 
Def "H 

Sometimes we have requirements to separate some of the servers. We have default GPO. 2016, there is a specific GPO applied, and focused on what they are applied to.

Machine generated alternative text:
OSx 
AWS 
OAC 
201s 
NTDSQuot„ 

Each server is owned by a specific group - application based. Server owners and application owners are the ones in charge.

The Domain controllers are owned by James team.

**What happens when a domain controller goes down?**

We are responsible for replicating changes. Once a password changes for instance, should be in minutes be able to use that password and get access into the different environment.

Machine generated alternative text:
A dive Md A 
Swe 
M„osx 
A OOwte 
Cire 
, QNXT 
ART p. AETH.m1 
C 01 
& MAzp.AETV4.ox 
IVMlOP-AETH.t5 
EMIop.AETH*02 
Mv'lop-AETH.u:. 
p ocp 
AZURE • 
uK.s 
AZURE. us. E2 
AzuRE.us.c 
AZURE -us. €2 
OH 
CA DC 
G, mbM0 NC 
00 m 
00 m. n 
Cow 

Domain controllers - These are mostly default - only James's team can go in and make changes.

**Are there any KPI/KRI. Any management reporting done?**

Availability is a big think for us. Closely monitored. Services level are monitored for availability, and continuous. Exceeding SLA for 2021, currently 99.9%. Haven't had a widespread outage. Logging and monitoring is continuous, and doesn’t not fall into management reporting.

We will utilize Auditboard for all our requests.

James: We can share the policies and procedure document with IA, given no proprietary information included confirmed.

**If you are not meeting SLAs, what will be next steps/action to address unfavorable results?**

Service level are managed by Joe. They track all those service level, enterprise wide, Tier 1 and 2 app. Reporting is done during any down time and outages, enterprise wide. Applies to our platform. Root case analysis, any remediation requires as part of outage. Reported up through management. Ownership will be only within our platform. Whoever owns the root cause, will be responsible. In order for AD to have these outages, there will have to be an intracultural failure. Users can't authenticate anything.