https://linkedin.com/in/yahya-abd-el-azim

اهم اسئلة انترفيو MCSA

1) الفرق بين Domain, AD, DC
2) إيه هي Group Policy؟
3) إيه الفرق بين Local Group Policy وDomain Group Policy؟
4) إيه هي الـ OU؟
5) مراحل عمل DHCP
6) يعني إيه DNS وRecords بتاعته و Zones
7) إيه الفرق بين Workgroup و Domain ؟
8) ما الفرق بين Forest و Domain و Tree ؟
9) الفرق بين Roaming Profile و Local Profile ؟
10) إيه الفرق بين Mandatory Profile و Roaming Profile ؟
11) إزاي تفرق بين Primary DNS و Secondary DNS ؟
12) إزاي تعمل Migration من Server 2012 لـ 2019 ؟
13) اشرح الفرق بين FSMO Roles كلها
14) اشرح Trust Relationships في Active Directory
15) عايز تعمل Trust بين شركتين كل واحدة لها دومين مختلف ..تبدأ بإيه؟
16) إيه وظيفة الـ SYSVOL؟
17) إيه هي الـ Sites and Subnets في AD؟ وليه نستخدمها؟
18) الفرق بين PDC Emulator وRID Master ؟
19) إزاي تعمل Domain Rename؟
20) إيه هي Default Password Policy في AD؟
21) إيه الفرق بين SID Filtering وSID History ؟
22) إمتى تستخدم Demote لـ DC؟
23) اشرح إيه هو الـ Kerberos؟ وكيف يعمل في بيئة Active Directory
24) إيه هو الفرق بين Backup Types (Full, Incremental, Differential) ؟
25) ايه الفرق بين GPO Link وInheritance و Enforcement؟
26) ايه الفرق بين Security Filtering وWMI Filtering في GPO؟
27) إزاي تتعامل مع كرت شبكة Virtual مش بياخد IP من DHCP؟
28) إزاي تعرف مين آخر حد عمل Logon بـ Domain Admin كـ يحيى مثلا
29) إزاي تمنع الكتابة على الفلاشة لكن تسمح بالقراءة فقط؟
30) إزاي تمنع استخدام الـ CMD للمستخدمين العاديين؟
31) إزاي تهيأ DHCP Failover Cluster ؟
32) إزاي تعمل Restore لـ Deleted OU؟
33) إزاي تعمل تنبيه لو Service معينة وقفت في السيرفر؟
34) إزاي تمنع كل السيرفرات من الوصول للإنترنت لكن تسمح ببعض الـ IPs؟
35) معنى DNS Forwarder وConditional Forwarder؟
36) إيه هو الـ Account Lockout Policy؟
37) إزاي تعمل Sync تلقائي بين الـ File Shares في فرعين مختلفين؟
38) إزاي تجهز سياسة مسح تلقائي للملفات اللي في Desktop بعد 7أيام؟
39) إزاي تمنع استخدام الـ WiFi نهائيًا من GPO؟
40) إزاي تعمل سياسات Timeout للـ Remote Desktop؟
41) إزاي تتبع Service Account بيتم استخدامه من أكتر من جهاز؟
42) إزاي تعمل Audit لمحاولات الدخول الفاشلة؟

مشاكل

قاعدة ال mcsa (اي مصيبة تحصل معاك اول حاجه تفكر فيها ال dns حرفيا العمود بتاع MCSA)

43) فيهGPO بتمنع المستخدمين من تغيير الباسورد، بس يوزر معين لسه قادر يغيرها ..إزاي؟
44) فيه GPO مش بتطبق على OUمعينة؟ تبدأ تحل منين؟
45) جهاز متضاف على الدومين مش ظاهر في DNS..تبدأ تحل منين؟
46) حصل انقطاع في الشبكة والسيرفر رجع يشتغل، بس بعض الخدمات مش بتشتغل ..هتشوف إيه؟
47) يوزر مش قادر يطبع على الطابعة الشبكية، بس الطابعة شغالة لباقي الموظفين ..تحل المشكلة إزاي؟
48) السيرفر بطيء جداً فجأة ..إزاي تعمل له تشخيص مبدئي؟
49) يوزر بيشتكي إنه مش قادر يعمل Log in على الجهاز، لكن الشبكة شغالة ..تبدأ منين؟
50) فيه DC حصل له Crash..هترجعه إزاي من Backup ولا Restore؟إمتى تستخدم Authoritative vs Non-Authoritative؟
51) جالك Alertإن فيه مشاكل في Replicationبين DCs..هتعمل إيه؟
52) إزاي تهاجر DHCP من Server قديم لآخر جديد بدون فقد الإعدادات؟
53) جهاز بيعمل Logon ببطء جدًا ..ازاي تحدد إذا كانت المشكلة من الـ DNSأو GPO؟
54) عايز تمنع بعض اليوزرز من استخدام متصفح معين ..تطبق ده إزاي؟
55) عملت Join لجهاز على الدومين بس مش ظاهر في Active Directory..ليه؟
56) لما بتعمل Logoff للمستخدم، بيتم مسح كل حاجة من Profile..السبب؟
57) عايز توزع الـ Network Printers باستخدام GPO..تعمل ده إزاي؟
58) عايز تمنع Domain Users من الوصول لـ Task Manager..تعمل ده إزاي؟
59) فيه Conflict في الـ IPs رغم إن DHCP شغال ..تبدأ تحل منين؟
60) جهاز عليه Event ID بيوضح إنه مش قادر يعمل Replication..تتصرف إزاي؟
61) إزاي تكتشف إذا كان فيه Loop في الشبكة بسبب جهاز معين؟
62) يوزر بيحصل له Logoff تلقائي بعد 15دقيقة ..تبدأ تحقق منين؟
63) عندك جهاز Virtual مش قادر يتواصل مع ADرغم إن النود شغالة ..تحل منين؟
64) عايز تمنع USB storage انها تشتغل عند كل المستخدمين ..تعمل ده إزاي؟
65) جهاز كل ما يعمل Restart بيرجع IP Static بدل ما يكون DHCP..السبب؟
66) عندك GPO بتتطبق على الكل ماعدا مجموعة معينة من المستخدمين ..السبب؟
67) إزاي تعمل Delegation لـ OU معينة عشان Admin Junior يقدر يضيف يوزرز بس؟
68) جهاز بيظهر Event ID 5719..تتصرف إزاي؟
69) إزاي تمنع المستخدمين من الوصول لـ Control Panel؟
70) إزاي تمنع تشغيل برامج معينة باستخدام GPO؟
71) إزاي تراقب التعديلات على Group Membership؟
72) إزاي تعمل Logon Script باستخدام GPO؟
73) إزاي تعمل Map لـ Network Drive تلقائيًا؟
74) إزاي تعمل Export لكل اليوزرز الموجودين في OUمعينة؟
75) إزاي تعمل Resetلـ DNS Zone؟
76) إزاي تتابع Logsبتاعة Group Policy؟
77) عندك GPO بتطبق على الكل رغم إنها Unlinked..ليه؟
78) إزاي تعرف الأجهزة اللي Out of Domain؟
79) إزاي تعرف GPO اللي مسببة بطء في Logon؟
80) إزاي تعمل Wake on LAN من السيرفر؟
81) إزاي تعرف الأجهزة اللي مش بتاخد IPمن DHCP؟
82) إزاي تمنع أي exe غير موقع Digital Signatureمن التشغيل؟
83) إزاي تعمل تحديد لسرعة الإنترنت من Group Policy؟
84) إزاي تعرف أي GPO عامل Disable لـ USB لكن بـ WMI Filtering؟

85) جهاز بيطلع Error أثناء عملية Join للدومين .."The specified domain does not exist or could not be contacted"تتصرف إزاي؟
86) جهاز بيشتغل بكفاءة في الشبكة، لكن فجأة كل الجروبات اختفت من الـ ..ADUCتبدأ منين؟
87) جهاز بيظهر إنه Online في AD بس هو مطفي بقاله شهر ..السبب؟
88) إزاي تمنع الـ Ransomware من الانتشار في File Server؟
89) إزاي تمنع يوزرز من حذف الملفات من Shared Folder معين؟
90) إزاي تمنع المستخدمين من نسخ ملفات من Shared Folder؟
91) إزاي تعرف مين آخر حد عمل Logonبـ Domain Admin؟
92) ايه الفرق بين NTFS Permissions و Share Permissions؟
93) ايه هو ال Loopback Processing في Group Policy ؟

أسئلة CLIوأوامر مهمة في Windows Server

94) أمر تشوف بيه الـ Replication Statusبين الـ DCs؟
95) أمر تضيف بيه يوزر جديد من CMD؟
96) أمر تعمل بيه Ping لاسم دومين وتشوف الـ DNSاللي بيرد؟
97) أمر تعمل بيه Reset لحساب الكمبيوتر؟
98) أمر تعرض بيه كل اليوزرز الموجودين؟
99) أمر تنقل بيه FSMO Roles ؟
100) أمر تعرض بيه IP Configuration بالجهاز؟
101) أمر تشوف بيه آخر Logon Date للمستخدمين؟
102) أمر تعمل بيه Force GP Update؟
103) أمر تتحقق بيه من مشاكل الـ DNS من CMD؟

1. الفرق بين Domain, AD, DC

Domain: هو مجموعة من الأجهزة (أجهزة كمبيوتر، مستخدمين، طابعات) بتدار بشكل مركزي تحت اسم واحد زي .example.com

Active Directory (AD): هي خدمة من مايكروسوفت لإدارة الدومين، بتخزن معلومات عن الأجهزة والمستخدمين والسياسات.

Domain Controller (DC): هو السيرفر اللي عليه الـ Active Directoryوبيتحكم في الدخول والصلاحيات وكل شيء داخل الـ .Domain

2. إيه هي Group Policy؟

هي ميزة في الـ ADبتستخدم لفرض إعدادات معينة على المستخدمين أو الأجهزة زي تعطيل الـ USB، إعداد الـ wallpaper، أو منع الوصول لحاجات معينة.

3. إيه الفرق بين Local Group Policyو Domain Group Policy؟

Local GPO :بيأثر على الجهاز فقط

Domain GPO :بيتم تطبيقه من خلال الـ ADعلى مستوى الدومين كله

4. إيه هي الـ OU؟

Organizational Unit هي وحدة تنظيمية داخل الـ ADبنستخدمها لتنظيم الأجهزة أو المستخدمين، وممكن نطبق عليها GPOبشكل منفصل.

5. مراحل عمل DHCP

Discover الجهاز بيبعت رسالة عشان يدور على DHCP

Offer السيرفر بيرد بعنوان IP

Request الجهاز بيطلب الـ IPاللي اتعرض عليه

Acknowledge السيرفر بيأكد التخصيص

6. يعني إيه DNSو Recordsبتاعته و Zones

DNS هو النظام اللي بيترجم أسماء المواقع زي (google.comلـ IP والعكس)

طب ايه ال Records بتاعته

A دا يربط اسم بـ IP

CNAME اسم مستعار زي ربط اسم باسم يعني مثلا ريدهات اشترتCentos فتروح رابطه بينهم ب CNAME

MX دا لتوجيه البريد

PTR (عكس A record) من IP لاسم

NS لتحديد السيرفرات المسؤولة عن الـ zone

طب و ال Zones (عندك نوعين)

Forward Lookup Zone ترجمة الاسم لـ IP

Reverse Lookup Zone ترجمة الـ IPلاسم

7. إيه الفرق بين Workgroup و Domain ؟

Workgroup :كل جهاز بيشتغل بشكل مستقل.

Domain :الإدارة مركزية باستخدام AD

8. ما الفرق بين Forest و Domain و Tree ؟

Domain :مجموعة من الكائنات (يوزرات، أجهزة، جروبات) بتشارك في قاعدة بيانات واحدة.

Tree : مجموعة من الدومينات المرتبطة ببعض في هيكل هرمي.

Forest :أعلى مستوى، بيحتوي على مجموعة من الـ Treesوبيمثل حدود الثقة (Trust Boundary)

9. الفرق بين Roaming Profileو Local Profile ؟

Local Profile:

البروفايل بتاع اليوزر بيتخزن على الجهاز نفسه، يعني لو دخل من جهاز تاني، مش هيلاقي الداتا بتاعته.

Roaming Profile:

البروفايل بيتخزن على السيرفر، يعني أي جهاز يدخل منه، هياخد نفس الداتا والإعدادات.

لكن خلي بالك، الـ Roamingممكن يبطأ الـ Log inلو فيه داتا كتير.

10. إيه الفرق بين Mandatory Profileو Roaming Profile ؟

Roaming Profile :بيتنقل مع المستخدم بين الأجهزة اي تعديل بيسمع ع السيرفر

Mandatory Profile :نسخة ثابتة لا تقبل التعديل، أي تغيير بيتم ما بيتسجلش بمجرد تسجيل الخروج يعود الى النسخه الاصليه

11. إزاي تفرق بين Primary DNS وSecondary DNS ؟

Primary DNS: بيحتوي على نسخة أصلية وقابلة للتعديل من الـ zone.

Secondary DNS: نسخة للقراءة فقط، بتاخد نسخة من الـ Primary.

12. إزاي تعمل Migration من Server 2012 لـ 2019 ؟

Add the new server كـ DC جديد ==> Replicate AD ==> Transfer FSMO Roles ==> Demote القديم

13. اشرح الفرق بين FSMO Roles كلها

بص ال roles خمسه بس متقسمين مجموعتين مجموعه ع مستوى ال forest ومجموعه ع مستوى ال domain

Forest-wide (2 Roles)

بتطبق ع ال forest بالكامل ويوجد واحد فقط من كل نوع في Forest (يعني كل forest فيها schema,domain naming master)

==> Schema Master:

تعديل ال schema بتاع ال AD

==> Domain Naming Master:

مسؤول عن اضافة وحذف ال domains

Domain-wide (3 Roles)

تطبق ع كل domain داخل forest يعني لو عندك مثلا تلاته دومين يبقى كدا عندك تلاته FSMO

==> RID Master:

بيدي ال Relative IDs من ال DCs ranges توزيع الـ RID للـ DCs

==> PDC Emulator:

مهم جدًا ومسؤول عن الـ Time Sync وGPO وPassword Changes

==> Infrastructure Master:

تعديل الـ SID references

14. اشرح Trust Relationships في Active Directory

Trust Relationships هي علاقات ثقة بين دومينات مختلفة بتسمح للمستخدمين في دومين معين بالوصول لموارد في دومين تاني

فيه أنواع مختلفة زي:

- **One-way Trust**: ثقة من اتجاه او طرف واحد
- **Two-way Trust**: ثقة متبادلة بين الدومينين
- **External Trust**: ثقة بين دومين في Forest ودومين خارجي
- **Forest Trust**: ثقة بين Forests مختلفة

15. عايز تعمل Trust بين شركتين كل واحدة لها دومين مختلف ..تبدأ بإيه؟

لازم تتاكد من:

- **Network Connectivity**
- **Name Resolution (DNS forwarders)**
- **تتأكد إن الوقت بينهم متزامن.**
- **بعد كده تعمل Trust من AD Domains and Trusts**
- **تختار نوع ال Trust هل هو External او Forest حسب العلاقه**

16. إيه وظيفة الـ SYSVOL؟

ده فولدر بيحتوي على الـ GPOs و Scripts الخاصة باللوجين.

بيتعمله Replication بين الـ DCs باستخدام DFS

17. إيه هي الـ Sites and Subnets في AD؟ وليه نستخدمها؟

بتستخدمها لو عندك مثلا فروع مختلفه في أماكن جغرافية مختلفة

Sites تخلي كل فرع يشتغل على أقرب DC ليه عشان تقلل الـ Traffic وتسرّع الـ Logon

18. الفرق بين PDC Emulator وRID Master ؟

PDC Emulator :مسؤول عن الباسوردات، الـ GPOs، و الوقت.

RID Master :بيوزع الـ RID Pool علشان إنشاء الـ SIDsالجديدة .

19. إزاي تعمل Domain Rename؟

عملية صعبة ونادرة الحدوث ولازم تتحضر لها كويس
لازم تستخدم:
rendom tool
وتاخد Backup
وتراجع الـ DNS
وتعرف إن الـ Renameمش بيشتغل لو فيه Exchange Server

20. إيه هي Default Password Policy في AD؟

هي الاعدادات الاساسية للباسورد الي بتطبق ع اي باسورد بيتم انشائها

Minimum Password Length: 7 Password History: 24 Maximum Password Age: 42 days

Minimum Password Age: 1 day Complexity: ON

21. إيه الفرق بين SID Filteringو SID History ؟

SID History:

لما تنقل يوزر من دومين لدومين، بياخد الـ SIDالقديم عشان صلاحياته القديمة تشتغل.

SID Filtering:

أمان إضافي .يمنع SID Historyمن إنه يتستخدم بشكل خبيث في .Trust Relationships

22. إمتى تستخدم Demoteلـ DC؟

لما تحب تشيل الـ DCمن الشبكة
أو الجهاز بقى قديم
أو بقيت مش محتاجهDC
تستخدم:
dcpromo أو Server Manager > Remove AD DS Role

23. اشرح إيه هو الـ Kerberos؟ وكيف يعمل في بيئة Active Directory

Kerberos هو بروتوكول توثيق (Authentication Protocol)، مش برنامج.
وهو اللي بيستخدمه Active Directoryلتأكيد هوية المستخدمين.
وظيفته انه بيصدر "تذاكر (tickets) "للمستخدمين، بحيث يقدروا يدخلوا على خدمات متعددة بدون إدخال الباسورد كل مرة.

24. إيه هو الفرق بين Backup Types (Full, Incremental, Differential)؟

Full Backup :

بتاخد نسخة كامله من كل الملفات

Differential Backup:

بياخد الي اتغير من اخر Full Backup

Incremental Backup:

بياخد الي اتغير من اخر backup سواء كان Differential او Full

25. ايه الفرق بين GPO Link و Inheritance و Enforcement؟

GPO Link : ربط GPOبوحدة تنظيمية (OU)أو دومين
Inheritance : الـ OUبتورث السياسات من الـ OUالأعلى منها
Enforcement : إجبار تطبيق GPOحتى لو فيه Block Inheritance

26. ايه الفرق بين Security Filtering و WMI Filtering في GPO؟

Security Filtering : تحديد من يطبق عليه GPOبناءً على صلاحيات الأمان.

WMI Filtering : تطبيق GPOبناءً على خصائص الجهاز (زي نظام التشغيل أو نوع الجهاز)

27. إزاي تتعامل مع كرت شبكة Virtualمش بياخد IPمن DHCP؟

اتأكد إن الكرت مفعّل ومتوصل بـ .Network Adapter

شوف إعدادات DHCPعلى السيرفر.

جرب تعمل ipconfig /releaseوبعدين ipconfig /renew

لو المشكلة مستمرة:

اتأكد من الـ Virtual Switchمتوصل صح.

جرب Manual IPللتأكد إن المشكلة في .DHCP

28. إزاي تعرف مين آخر حد عمل Logonبـ Domain Adminكـ يحيى مثلا

تقدر تستخدم Event Viewerمن السيرفر:

افتح**Security Logs** :

دور على**Event ID 4624** :

شوف الـ Account Nameو Workstation Name

29. إزاي تمنع الكتابة على الفلاشة لكن تسمح بالقراءة فقط؟

من خلال :GPO

Computer Configuration → Admin Templates → System → Removable Storage Access

فعل:

“Removable Disks: Deny write access” → Enabled

“Removable Disks: Allow read access” → Enabled

30. إزاي تمنع استخدام الـ CMD للمستخدمين العاديين؟

من :GPO

User Configuration → Admin Templates → System

فعل:

“Prevent access to the command prompt” → Enabled

وممكن كمان تمنع PowerShell بنفس الطريقة.

31. إزاي تهيأ DHCP Failover Cluster ؟

من :DHCP Console

اختار الـ Scope <== كليك يمين Configure Failover

دخل السيرفر التاني

اختار Load balance أو Hot standby

كمّل الإعدادات وفعّل الـ Failover

32. إزاي تعمل Restore لـ Deleted OU؟

لاسترجاع Organizational Unit (OU) تم حذفها، لازم تكون مفعّل ميزة اسمها Active Directory Recycle Bin

ولو مش مفعّلة، ساعتها هتحتاج تستخدم طريقة تانية زي Authoritative Restore من.Backup

استخدم :PowerShell

Get-ADObject -Filter 'IsDeleted -eq $true -and ObjectClass -eq "organizationalUnit"' -IncludeDeletedObjects

33. إزاي تعمل تنبيه لو Serviceمعينة وقفت في السيرفر؟

من :Task Scheduler

Create Task → Triggers: Event ID 7036 أو7031

Actions: Send email أو Show Message أو Run script

أو باستخدام

PowerShell script + Task Scheduler.

34. إزاي تمنع كل السيرفرات من الوصول للإنترنت لكن تسمح ببعض الـ IPs؟

استخدم GPO لعمل Firewall Rule
أو استخدم Proxy أو NAT Rule على الـ Gateway
Block الكل
Allow بعض الـ IPs باستخدام Access Control List (ACL)

35. معنى DNS Forwarder و Conditional Forwarder؟

==> **DNS Forwarder** لما الـ DNS مش عارف يحل اسم، يبعته لسيرفر خارجي.

==> **Conditional Forwarder** يحوّل استفسارات دومين معين فقط لسيرفر DNS محدد (مثلاً دومين الشركة التانية في Trust)

36. إيه هو الـ Account Lockout Policy؟

==> سياسة بتحدد:

كام محاولة فاشلة تقفل الأكاونت ومدة القفل ووقت إعادة المحاولات

من GPO:

Computer Configuration → Windows Settings → Security Settings → Account Lockout Policy

37. إزاي تعمل Sync تلقائي بين الـFile Shares في فرعين مختلفين؟

استخدم DFS Replication
فعّل DFS ==> أنشئ Namespace ==> أضف الـ Shared Folders ==> فعل Replication Group بين الفرعين

38. إزاي تجهز سياسة مسح تلقائي للملفات اللي في Desktop بعد 7أيام؟

Script + GPO:
PowerShell script يحذف ملفات أقدم من 7أيام
اربطه بـ GPO كـ Logon/Logoff Script
مثال:

```
Get-ChildItem "C:\Users\*\Desktop\*" -Recurse | Where-Object { $_.LastWriteTime -lt (Get-Date).AddDays(-7) } | Remove-Item -Force
```

39. إزاي تمنع استخدام الـWiFi نهائيًا من GPO؟

<-- GPO

Computer Configuration → Windows Settings → Security Settings → Wireless Network (IEEE 802.11) Policies

عمل سياسة تمنع الاتصال بأي شبكة

أو Disable Wi-Fi Adapter بـ: Script أو Device Installation Restriction

40. إزاي تعمل سياسات Timeout للـ Remote Desktop؟

عن طريق GPO:

Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits

فعّل السياسات مثل:

Set time limit for active but idle RDS sessions

Set time limit for disconnected sessions

41. إزاي تتبع Service Account بيتم استخدامه من أكتر من جهاز؟

فعّل Audit Logon Events وراقب الـ Security Logs في الـ Event Viewer،
أو استخدم أدوات زي **Logon Tracker** أو **SIEM** لمراقبة الـ logon من أكتر من Host

42. إزاي تعمل Audit لمحاولات الدخول الفاشلة؟

من GPO:
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy
فعّل:
Audit logon events واختر "Failure"
راجع بعدها Event ID: **4625** في Security Logs.

43. **فيه GPO بتمنع المستخدمين من تغيير الباسورد، بس يوزر معين لسه قادر يغيرها ..إزاي؟**

راجع الـ **Password settings** المطبقة على اليوزر.

ممكن يكون فيه **Fine-Grained Password Policy** معمول عليه أو إنه عضو في Groupمستثناة.

44. **فيه GPO مش بتطبق على OUمعينة؟ تبدأ تحل منين؟**

اتأكد إن الـ GPO Linkedلـ OU

افحص بالـ {gpresult /h report.html}

شوف هل فيه Block Inheritance أو WMI filter أو Security Filtering

45. **جهاز متضاف على الدومين مش ظاهر في ..DNSتبدأ تحل منين؟**

اتأكد إن DNS Dynamic Update Enabled

استخدم الأمر {ipconfig /registerdns}

افحص Service: **DNS Client**

افحص Event Viewerعلى الجهاز.

46. **حصل انقطاع في الشبكة والسيرفر رجع يشتغل، بس بعض الخدمات مش بتشتغل ..هتشوف إيه؟**

شوف Event Viewer

افحص إن كل الـ Dependenciesشغالة

استخدم services.mscوتابع الحالة

تأكد من الاتصال بالدومين و.DNS

47. **يوزر مش قادر يطبع على الطابعة الشبكية، بس الطابعة شغالة لباقي الموظفين ..تحل المشكلة إزاي؟**

احذف وأعد إضافة الطابعة

افحص الـ Print Spooler

جرب من جهاز تاني بنفس الحساب

افحص Permissionsأو Policyتمنعه.

48. **السيرفر بطيء جداً فجأة ..إزاي تعمل له تشخيص مبدئي؟**

Task Managerأو Resource Monitor

شوف الـ CPU/RAM/Disk/Network

افحص Event Viewer

شوف لو فيه Updateأو Malware

perfmonلمراقبة الأداء.

49. **يوزر بيشتكي إنه مش قادر يعمل Log in على الجهاز، لكن الشبكة شغالة ..تبدأ منين؟**

افحص رسالة الخطأ

شوف اذا فيه lockout او مشكله ف ال password (هل الباس الي بيدخلها صح)

جرب login محلي

شوف Event ID في ال Security Logs

50. **فيه DCحصل له ..Crashهترجعه إزاي من Backup ولا Restore؟إمتى تستخدم Authoritative vs Non-Authoritative؟**

Non-Authoritative Restore بيرجع من Backup ويتزامن مع باقي الـ DCs

Authoritative Restore تستخدمه لو عايز تفرض الـ Objectsمن النسخة دي (زي حذف OU بالغلط)

استخدم ntdsutil لتحديد النوع.

51. **جالك Alertإن فيه مشاكل في Replicationبين ..DCsهتعمل إيه؟**

استخدم repadmin /replsummary أو repadmin /showrepl

شوف الـ Event Viewer

افحص DNSو Connectivity

شوف لو فيه Time Syncمشكلة

52. **إزاي تهاجر DHCP من Server قديم لآخر جديد بدون فقد الإعدادات؟**

على القديم : {netsh dhcp server export C:\dhcp.txt all}

على الجديد: {netsh dhcp server import C:\dhcp.txt}

53. **جهاز بيعمل Logon ببطء جدًا ..ازاي تحدد إذا كانت المشكلة من الـ DNSأو GPO؟**

جرب{gpresult /h gpreport.html}

Pingالـ DCبالاسم وشوف سرعة الاستجابة

افحص Event Viewerلـ Group Policyو.DNS Errors

54. **عايز تمنع بعض اليوزرز من استخدام متصفح معين ..تطبق ده إزاي؟**

باستخدام :GPO

Software Restriction Policiesأو AppLocker

حدد المتصفح بالـ pathأو الـ hash

55. **عملت Joinلجهاز على الدومين بس مش ظاهر في ..Active Directoryليه؟**

ممكن الجهاز اتضاف بس لسه ما تسجلش كويس في AD

افحص DNS registration

تأكد من OUاللي الجهاز انضم ليها

جرب {net computer \\PCNAME /add}

56. **لما بتعمل Logoff للمستخدم، بيتم مسح كل حاجة من ..Profile السبب؟**

ممكن يكون شغال :GPO

Delete user profiles on logoff

أو المستخدم بيستخدم .**Mandatory Profile**

57. **عايز توزع الـ Network Printers باستخدام ..GPO تعمل ده إزاي؟**

من :Print Management

Right-click printer → Deploy with Group Policy

أو من :GPO

User Configuration > Preferences > Control Panel Settings > Printers

58. **عايز تمنع Domain Users من الوصول لـ ..Task Manager تعمل ده إزاي؟**

من :GPO <== {User Configuration > Administrative Templates > System > Ctrl+Alt+Del Options}

فعّل **Remove Task Manager**

59. **فيه Conflict في الـ IPs رغم إن DHCP شغال ..تبدأ تحل منين؟**

شوف إذا فيه جهاز واخد IP Static

افحص الـ DHCP Scopeو Leases

استخدم arp -aو ping -a

افصل الأجهزة المشكوك فيها واختبر.

60. **جهاز عليه Event ID بيوضح إنه مش قادر يعمل ..Replication تتصرف إزاي؟**

راجع الحدث بالتفصيل

استخدم repadmin /showrepl

افحص DNSو Connectivity

افحص Time Sync.

61. **إزاي تكتشف إذا كان فيه Loop في الشبكة بسبب جهاز معين؟**

راقب الـ Switches: Loop Detectionأو STP Logs

استخدم أدوات زي **Wireshark**لملاحظة الـ Broadcast storms

افصل الأجهزة تدريجياً واختبر.

62. يوزر بيحصل له Logoff تلقائي بعد 15دقيقة ..تبدأ تحقق منين؟

GPO:

Computer/User Configuration > Windows Settings > Security Settings > Local Policies > Security Options

افحص Screen Saver Policiesأو Session Timeouts.

63. عندك جهاز Virtual مش قادر يتواصل مع AD رغم إن النود شغالة ..تحل منين؟

افحص Network Adapter (NAT/Bridge)

Ping الـ DC

DNS settings

افحص الجدار الناري

64. عايز تمنع USB storageانها تشتغل عند كل المستخدمين ..تعمل ده إزاي؟

من GPO:

Computer Configuration > Administrative Templates > System > Removable Storage Access

فعل**All Removable Storage classes: Deny all access** :

65. جهاز كل ما يعمل Restartبيرجع IP Staticبدل ما يكون DHCP..السبب؟

ممكن يكون فيه GPOأو Scriptبيحدد IP

أو Snapshot بيرجعه لحالة سابقة

أو إعداد محفوظ في Task Scheduler.

66. عندك GPO بتتطبق على الكل ماعدا مجموعة معينة من المستخدمين ..السبب؟

افحص Security Filteringو Permissions

ممكن المجموعة دي عليها Deny أو مش ضمن الـ Scope

تحقق من WMI Filter.

67. إزاي تعمل Delegation لـ OUمعينة عشان Admin Junior يقدر يضيف يوزرز بس؟

من Active Directory Users and Computers

Right-clickعلى الـ {OU > Delegate Control}

Add اليوزر واختر المهام **Create, delete, and manage user accounts** :

68. جهاز بيظهر Event ID 5719..تتصرف إزاي؟

الحدث معناه "No domain controller available"

افحص Network/DNS

جرب {nltest /dsgetdc:<domain>}

شوف الـ Secure Channelباستخدام {Test-ComputerSecureChannel -Verbose}

69. إزاي تمنع المستخدمين من الوصول لـ Control Panel؟

من GPO:

User Configuration > Administrative Templates > Control Panel

فعّل**Prohibit access to Control Panel and PC settings** :

70. إزاي تمنع تشغيل برامج معينة باستخدام GPO؟

من GPO:

User Configuration > Administrative Templates > System

فعّل**Don't run specified Windows applications** :

أو استخدم **AppLocker**أو **Software Restriction Policies**لتحديد البرامج بالاسم أو path

71. **إزاي تراقب التعديلات على Group Membership؟**

فعّل Auditing:

GPO > Advanced Audit Policy Configuration > DS Access > Audit Directory Service Changes

راجع Event Viewer: Event ID **4728, 4729, 4732, 4733, 4756, 4757**

72. **إزاي تعمل Logon Scriptباستخدام GPO؟**

من GPO:

User Configuration > Windows Settings > Scripts (Logon/Logoff)

أضف سكريبت bat.أو ps1.في المسار المشترك أو المحلي.

73. **إزاي تعمل Mapلـ Network Driveتلقائيًا؟**

من GPO:

User Configuration > Preferences > Windows Settings > Drive Maps

اختَر "New → Mapped Drive"

حدد الـ Path، واختر طريقة الربط (Replace / Update / Create)

74. **إزاي تعمل Exportلكل اليوزرز الموجودين في OUمعينة؟**

باستخدام PowerShell:

```
Get-ADUser -Filter * -SearchBase "OU=Users,DC=domain,DC=com" | Export-Csv users.csv -NoTypeInformation
```

75. **إزاي تعمل Resetلـ DNS Zone؟**

من DNS Manager: احذف الـ Zoneوأعد إنشائها.

أو

احذف ملفات الـ zoneمن %systemroot%\system32\dns(بحذر)

ثم أعد تحميلها من Backupأو Createمن جديد.

76. **إزاي تتابع Logsبتاعة Group Policy؟**

افتح Event Viewer →

Applications and Services Logs > Microsoft > Windows > GroupPolicy > Operational

تلاقي كل خطوات تطبيق الـ GPOهناك.

77. **عندك GPOبتطبق على الكل رغم إنها Unlinked..ليه؟**

ممكن تكون **WMI Filter**في GPOتانية مرتبطة

أو GPO معمولة **Enforced** من مستوى أعلى (Domain level)

أو **Security Filtering**موجهة لمجموعة معينة.

78. **إزاي تعرف الأجهزة اللي Out of Domain؟**

استخدم PowerShellأو Endpoint Management Tool

أو سكريبت يتحقق من:

```
(Get-WmiObject Win32_ComputerSystem).PartOfDomain
```

79. **إزاي تعرف GPOاللي مسببة بطء في Logon؟**

استخدم gpresult /h report.html

أو راجع Event Viewer → GroupPolicy Logs

أو استخدم Performance Logsمع GP timings.

80. **إزاي تعمل Wake on LANمن السيرفر؟**

شغّل WOLفي BIOS + NIC

استخدم أداة مثل:

```
Send-WOL -mac "xx:xx:xx:xx:xx:xx"
```

أو أدوات مثل SolarWinds Wake-on-LAN.

81. إزاي تعرف الأجهزة اللي مش بتاخد IP من DHCP؟

راجع DHCP Server: Scope > Address Leases

استخدم arp -a أو ping

أو شوف الأجهزة اللي بـ APIPA IP (169.254.x.x)

82. إزاي تمنع أي exe غير موقع Digital Signature من التشغيل؟

استخدم **AppLocker** من GPO

Application Control Policies > AppLocker > Executable Rules

اسمح بتشغيل البرامج ذات التوقيع الرقمي فقط.

83. إزاي تعمل تحديد لسرعة الإنترنت من Group Policy؟

GPO نفسها لا تتحكم في الباندويث مباشرة

لكن:

Computer Configuration > Administrative Templates > Network > QoS Packet Scheduler

استخدم Policy-Based QoS لتحديد Bandwidth لتطبيق أو بروتوكول معين.

84. إزاي تعرف أي GPO عامل Disable لـ USB لكن بـ WMI Filtering؟

راجع GPO Settings

استخدم gpresult /h أو Group Policy Modelling

أو شوف من GPMC: GPO > Scope > WMI Filtering.

85. جهاز بيطلع Error أثناء عملية Join للدومين .. "The specified domain does not exist or could not be contacted" تتصرف إزاي؟

افحص DNS settings (يكون موجّه للـ DC)

Ping ع اسم الدومين

افحص الـ Firewall

اتأكد إن الوقت متزامن مع الـ DC

86. جهاز بيشتغل بكفاءة في الشبكة، لكن فجأة كل الجروبات اختفت من الـ ADUC.. تبدأ منين؟

افحص الـ OU

تأكد إنك مش شغال على Filter معين في ADUC

شوف لو حد عمل حذف للجروبات

راجع الـ Event Logs و Replication Status

87. جهاز بيظهر إنه Online في AD بس هو مطفي بقاله شهر .. السبب؟

AD ما بيعملش Refresh لحالة الأجهزة تلقائيًا

ممكن تستخدم **LastLogonTimestamp**

أو سكريبت PowerShell يتحقق من الأجهزة اللي ما عملتش Logon من فترة

88. إزاي تمنع الـ Ransomware من الانتشار في File Server؟

فعّل Controlled Folder Access

طبق NTFS Permissions بشكل صارم No Full Control (لكل الناس)

افصل المستخدمين عن بعضها

اعمل Endpoint Protection + Backup + Audit.

89. إزاي تمنع المستخدمين من نسخ ملفات من Shared Folder؟

ده مش سهل بالـ NTFS/Share Permissions فقط. ممكن:

استخدام **File Screening** (via FSRM) لمنع نسخ أنواع معينة.

أو استخدم حلول DLP (Data Loss Prevention)

90. إزاي تمنع يوزرز من حذف الملفات من Shared Folder معين؟

من :NTFS Permissions

اعطِ اليوزرRead & Write

لكن بدون Delete أو Modify

وخصوصًا:

Deny Delete

Deny Delete Subfolders and Files

91. إزاي تعرف مين آخر حد عمل Logonبـ Domain Admin؟

راجع :Event Viewer

Security Logs → Event ID 4624

فلتر على الـ Account Name = Domain Admin

أو استخدم :PowerShell

Get-EventLog -LogName Security -InstanceId 4624 | Where-Object {$_.ReplacementStrings[5] -like "*Domain Admins*"}

92. ايه الفرق بين NTFS Permissions و Share Permissions؟

NTFS Permissions : ==> بتطبق ع الملفات والفولدرات المخزنه ع NTFS Partions

Share Permissions : ==> بتطبق فقط لما يتم الوصول للفولدر عبر الشبكه

الاكثر Restrictive من الاتنين هو اللي بيطبق

93. ايه هو ال Loopback Processing في Group Policy ؟

خاصية بتخلي ال Group Policy اللي على الجهاز

تطبق بدل ال GPO الخاصة بالمستخدم

94. أمر تشوف بيه الـ Replication Statusبين الـ DCs؟

repadmin /replsummary

95. أمر تضيف بيه يوزر جديد من CMD؟

net user username password /add

مثال:

net user ahmed 123456 /add

96. أمر تعمل بيه Pingلاسم دومين وتشوف الـ DNSاللي بيرد؟

nslookup domain.name

مثال:

nslookup example.com

97. أمر تعمل بيه Resetلحساب الكمبيوتر؟

netdom reset computername /domain:yourdomain /userd:admin /passwordd:*

أو من Active Directory: Right click on computer > Reset account

98. أمر تعرض بيه كل اليوزرز الموجودين؟

net user

لو عايز تشوف اليوزرز على دومين ==> {net user /domain}

99. أمر تنقل بيه FSMO Roles؟

ntdsutil

ثم تدخل: ==> roles ==>connections <== connect to server YourServer <== transfer <role>

مثلاً: (transfer RID master)

100. أمر تعرض بيه IP Configurationبالجهاز؟

ipconfig /all

101. أمر تشوف بيه آخر Logon Date للمستخدمين؟

net user username /domain

هتلاقي تحت "Last logon"

102. أمر تعمل بيه Force GP Update؟

gpupdate /force

103. أمر تتحقق بيه من مشاكل الـ DNS من CMD؟

nslookup

وتقدر تجرب: {nslookup google.com}

أو اختبار DNS الخاص بالدومين: {dcdiag /test:DNS}