ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

Which of the following statements is true about raw printing with Samba?

A. Print jobs are submitted as vector files, including font files, which are rendered and printed by Samba.
B. Printing jobs are always submitted to Samba in raw postscript.
C. Any printed file, e.g. an office document, is submitted to the printer without any further processing in exactly the same bit sequence as it is stored on disk.
D. Samba converts printer-specific jobs to raw data to make them printable on an arbitrary printer.
E. Printing jobs are rendered on the client and passed on to the printer by Samba.

Answer: E

Explanation:

Client-Side Rendering: In Samba, raw printing means that the client machine renders the print job, which includes converting it to a printer-ready format.
Transmission to Printer: This rendered print job is then sent to the Samba server without further processing or alteration. Samba acts merely as a pass-through, sending the job directly to the printer. Advantages: This method offloads the rendering process from the server to the client, which can be beneficial in environments with diverse printer types and models, reducing the processing load on the server.
Conclusion: Thus, the correct answer is that printing jobs are rendered on the client and passed on to the printer by Samba.
Reference:
Samba Printing Documentation

Question: 2

The configuration of a Samba share contains the following line:
force directory mode = 0555
If a client creates a new directory with the permissions 0750, which permissions will the resulting directory have in the Samba server's file system?

A. 0755
B. 0750
C. 0750
D. 0555
E. 0777

Answer: D

Explanation:

force directory mode = 0555: This setting in Samba forces the permissions of any newly created directories to be 0555 regardless of what the client requests.
Client Request: If a client creates a directory with permissions 0750, Samba will override this and set the directory's permissions to 0555.
Permissions Breakdown:
0: No permissions for owner.

5: Read and execute permissions for the group.
6: Read and execute permissions for others.
Enforcement: Samba applies this mode strictly to ensure consistency and security as defined by the administrator.
Reference:
Samba Force Directory Mode Documentation

Question: 3

Which of the following smb.conf options turns a regular file share into a DFS share?

A. msdfs root = yes
B. addfs support = yes
C. dfs forward = yes
D. follow symlinks = yes
E. proxy share = yes

Answer: A

Explanation:

DFS (Distributed File System): This allows for the organization of shared files on multiple servers in a distributed file system.
msdfs root = yes: This option in the Samba configuration file (smb.conf) enables a share to be a DFS root. This means the share can provide access to multiple other shares possibly located on different servers, creating a single point of access.
Functionality: When enabled, users accessing this DFS root can be redirected transparently to the actual location of the shared files, which might be spread across different servers.
Setup: To configure a DFS root, add msdfs root = yes to the specific share definition in smb.conf. Reference:
Samba DFS Configuration

Question: 4

FILL BLANK
What option in sms.conf defines where the data of a file share is stored? (Specify ONLY the option name without any values.)

Answer: path

Explanation:

path Option: This parameter in smb.conf specifies the directory on the server where the shared data is stored.
Usage: Within a share definition, the path option points to the actual location on the filesystem that Samba will share.
Example Configuration:
[example_share] path = /srv/samba/share
Importance: Defining the correct path is crucial for ensuring that the share points to the intended directory with the appropriate data and permissions.

Reference:
Samba smb.conf man page

Question: 5

Which parameter within a share definition in the Samba configuration makes Samba only show files and directories on a file share which a user can access?

A. hide unreadable = yes
B. valid files = read,write
C. browse mask = 000
D. browseable = readable
E. display mode = 100

Answer: A

Explanation:

hide unreadable: This smb.conf option ensures that only files and directories that the user has permissions to access are visible in the file share.
Functionality: When set to yes, files and directories that the user cannot read (due to permissions) will be hidden from their view.
Security and Usability: This helps in enhancing both security and usability by preventing users from seeing files they cannot access, reducing clutter and potential confusion.
Example Configuration:
[example_share] hide unreadable = yes
Reference:
Samba smb.conf Documentation

Question: 6

Which of the following lines is missing in the given [printers] share definition?

```
[printers]
        path = /var/spool/samba quest ok = yes
```

A. printcap name = cups
B. printable = yes
C. print script = /usr/bin/lp -d %P %s
D. print admin = Administrator, root, @lpadmin
E. load printers = yes

Answer: B

Explanation:

In the context of a Samba configuration for printer shares, the [printers] section usually requires the printable = yes directive to indicate that the share is meant for printing. Without this directive, Samba would not treat the share as a printer share, even if other settings like path are configured properly.
The given snippet is:
The line printable = yes is missing and is essential for defining a printer share.

Reference:
Samba Official Documentation - Printer Sharing

Question: 7

The [homes] section of smb.conf contains the parameter browseable = no. What are the resulting consequences? (Choose two.)

A. When browsing the Samba server, there is no visible share named after the current user.
B. If the Samba server is part of an Active Director/ Domain, only users in the qroup Se3rowsingUsers can browse the homes share.
C. When browsing the Samba server, users can open the homes share but they cannot see the content of their home directories.
D. The homes share can be directly accessed by specifically opening this share by its UNC path.
E. When browsing the Samba server, there is no visible share called homes.

Answer: A, D

Explanation:

When browseable = no is set in the [homes] section of smb.conf, it prevents the share from appearing in the list of available shares when users browse the server. However, users can still access their home directories if they specify the correct UNC path directly.
A . When browsing the Samba server, there is no visible share named after the current user.
The share will not appear in the list of shares visible to the user during browsing.
D . The homes share can be directly accessed by specifically opening this share by its UNC path. Users can still access the share by directly typing the path in the form \\servername\username. Reference:
Samba Official Documentation - Home Directories

Question: 8

Which Samba utility, when launched with the appropriate parameters, generates the following output?

```
REVISION:1
CONTROL:0x8004
OWNER:3-1-5-21-3621094050-2160514158-817190072-500
GROUP:S-l-22-2-0
ACL:S-l-5-21-3621094050-2160514158-817190072-500:0/0x0/0x001f019f
ACL:3-1-22-2-0:0/0x0/0x00120089
ACL:3-1-1-0:0/0x0/0x00120089
```

A. smbcacls
B. smbclient
C. getfacl
D. smbxattr
E. smbfacl

Answer: A

Explanation:

The smbcacls utility is used to manage Windows ACLs on Samba shares. The output format shown in the image suggests it relates to detailed ACL information, which is typically generated by smbcacls. Reference: Samba smbcacls man page

Question: 9

Which of the following options can be used to limit access to a Samba share? (Choose two.)

A. untrusted users
B. write list
C. valid groups
D. valid users
E. accept list

Answer: C, D

Explanation:

To limit access to a Samba share, the valid users and valid groups options can be used. These directives specify which users or groups are allowed to access the share.

C . valid groups

This option restricts access to members of specified Unix groups.

D . valid users

This option restricts access to specified Unix users. Reference: Samba smb.conf man page

Question: 10

In case the following parameters are set in a Samba file share configuration: create mask = 711 force create mode = 750

What are the effective permissions of a file created with the permissions 777?

A. 066
B. 027
C. 777
D. 761
E. 751

Answer: E

Explanation:

The effective permissions of a file created with the permissions 777 can be calculated considering the create mask and force create mode.

create mask = 711 implies that the permission bits are ANDed with 0711, i.e., only the owner can read, write, and execute.

force create mode = 750 implies that certain permission bits are always set, specifically 0750, i.e., read, write, and execute for the owner, and read and execute for the group.

The create mask reduces the permissions to 0711, and then force create mode adds the 0750 mask to the result.

Original permission: 777 AND with create mask (711): 711 OR with force create mode (750): 751

Thus, the effective permission is 751.

Reference:

Samba smb.conf man page - create mask

Question: 11

Which of the following are valid Samba backends to store user and group information? (Choose two.)

A. sdb
B. smbpasswd
C. ldapsam
D. krb
E. smb

Answer: B, C

Explanation:

smbpasswd: This backend uses the smbpasswd file to store user and group information. It is a simple plaintext file format that holds password hashes and other account information.

ldapsam: This backend utilizes LDAP (Lightweight Directory Access Protocol) to store user and group information. LDAP is a more scalable and flexible option suitable for larger environments.

Other Options:

sdb, krb, smb: These are not valid Samba backends for storing user and group information.

Reference:

Samba User and Group Database Backends

Question: 12

How is the Global Catalog of an Active Directory domain accessed?

A. Through LDAP queries to the ports 3268 (plain text) and 3269 (TLS encrypted).
B. Through the share GCS SMB which is available on each domain controller.
C. Through GCS records in the DNS sub zone _gc in the domain's DNS zone.
D. Through LDAP queries to the base dn CN=GC in the standard LDAP directory.
E. Through SRV records in the DNS sub zone _msgc in the domain's DNS zone.

Answer: A

Explanation:

Global Catalog: The Global Catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multi-domain Active Directory forest.

Access Method: It is accessed through LDAP queries to specific ports:

Port 3268: For plain text (unencrypted) LDAP queries.

Port 3269: For LDAP queries encrypted with TLS.

Other Options:

GCS SMB share, GCS records, SRV records, CN=GC in LDAP: These do not provide the correct method to access the Global Catalog.

Reference:

Microsoft Documentation on Active Directory Global Catalog

Question: 13

Which of the following Samba commands provides comprehensive information and status flags on the user candidate?

A. smbpasswd -l -u candidate
B. net sam show candidate
C. pdbedit -v -u candidate
D. samba-tool user list
E. getent smbpasswd candidate

Answer: C

Explanation:

pdbedit: This Samba command is used to manage the user accounts stored in the Samba password database.
-v: The verbose option provides detailed information.
-u candidate: Specifies the user for which to display the information.

Other Commands:

smbpasswd, net sam show, samba-tool user list, getent smbpasswd: These commands do not provide the same comprehensive information and status flags as pdbedit.

Reference:

Samba pdbedit Documentation

Question: 14

Which service unifies Linux and Windows account management by allowing a Linux system to include Windows domain users in the Linux user database?

A. smbpasswdd
B. sudo
C. NIS
D. Winbind
E. OpenLDAP

Answer: D

Explanation:

Winbind: This service is used to unify Linux and Windows account management by allowing a Linux system to include Windows domain users in the Linux user database.
Functionality: Winbind enables Linux systems to retrieve user and group information from a Windows NT-based domain or Active Directory.

Other Services:

smbpasswdd, sudo, NIS, OpenLDAP: These services do not provide the same functionality for unifying account management between Linux and Windows.

Reference:

Samba Winbind Documentation

Question: 15

Which group of commands manages the directory replication in an active directory domain?

A. samba-tool repl
B. samba-tool directory
C. samba-tool drs
D. samba-tool domain
E. samba-tool sync

Answer: C

Explanation:

samba-tool drs: This set of commands is used to manage directory replication in an Active Directory domain. DRS stands for Directory Replication Service.

Functionality: It provides various subcommands to monitor, manage, and troubleshoot replication issues.

Other Commands:

samba-tool repl, directory, domain, sync: These do not specifically manage directory replication in the same way as samba-tool drs.

Reference:

Samba DRS Command Documentation

Question: 16

FILL BLANK

Which sub command of net groups commands related to an AD membership, as in the following example? (Specify ONLY the subcommand without any path or parameters.)

net join

Answer: ads

Explanation:

The net command is used to administer Samba and Windows servers. The subcommand ads is used in conjunction with the join command to join a Samba server to an Active Directory domain. The correct subcommand that fits the pattern net join is ads.

Reference:

Samba net command man page

Question: 17

Which option in smb.conf defines the domain of which the server is a member?

A. ad
B. member domain
C. basedn
D. domain

E. realm

Answer: E

Explanation:

In smb.conf, the realm option specifies the Kerberos realm for the Active Directory of which the server is a member. This option is crucial for integrating the Samba server into an AD environment. Reference: Samba smb.conf man page - realm

Question: 18

Which of the following groups exists by default in an Active Directory domain?

A. Domain Administrators
B. Domain Users
C. Domain 31aclclisc
D. Domain Update Role Accounts
E. Unassigned Users

Answer: B

Explanation:

In an Active Directory domain, the Domain Users group exists by default. This group includes all user accounts created in the domain and is commonly used for assigning permissions and rights to all users.

Reference:

Microsoft Docs - Active Directory Default Groups

Question: 19

Which of the following FSMO roles exist? (Choose two.)

A. File Server
B. Directory Server
C. PDC Emulator
D. RID Master
E. Global Catalog

Answer: C

Explanation:

Flexible Single Master Operations (FSMO) roles, also known as operations master roles, are specialized domain controller tasks in an Active Directory environment. The FSMO roles include: C . PDC Emulator

The Primary Domain Controller (PDC) Emulator is responsible for synchronizing time and managing password changes.

D . RID Master

The Relative ID (RID) Master allocates blocks of RIDs to each domain controller in the domain. Reference:

Microsoft Docs - FSMO Roles

Question: 20

When using rsync to synchronize the SYSVOL share's contents between multiple Samba servers, which of the following precautions should be taken? (Choose three.)

A. Synchronize from the domain controller which is the PDC emulator to the other domain controllers.
B. Overwrite the permissions of all files in the SYSVOL directory to be readable by root only after each sync.
C. Make the SYSVOL share read only on all domain controllers but the one used as synchronization source.
D. Make sure that the SYSVOL share is active on only one domain controller.
E. Make sure to make all changes to GPOs on the domain controller which is the replication source.

Answer: A, C, E

Explanation:

When using rsync to synchronize the SYSVOL share's contents between multiple Samba servers, it's essential to ensure data consistency and avoid conflicts. The following precautions should be taken: A . Synchronize from the domain controller which is the PDC emulator to the other domain controllers.

The PDC emulator is typically the authoritative source for certain domain-wide operations, making it the best source for SYSVOL synchronization.

C . Make the SYSVOL share read only on all domain controllers but the one used as synchronization source. This prevents changes on other domain controllers that could cause inconsistencies.

E . Make sure to make all changes to GPOs on the domain controller which is the replication source. Ensuring that all Group Policy Objects (GPOs) changes are made on the source controller prevents conflicts and ensures that all controllers have the latest configuration.

Reference:

Samba Documentation - SYSVOL Replication

Question: 21

Which of the following commands adds a forward DNS record named fileserver01 pointing to the IPv6 address 2001:db8::190 into the DNS zone samba.private on the Samba 4 server dc1?

A. net dns -S dc1 -U Administrator addrecord fileserver01.samba.private AAAA 2001:db8::190
B. dnstool -f dns.tdb add fileserver01.samba.private AAAA 2001:db8::190 -U Administrator
C. samba-dns dynupdate -S dc1 -U Administrator -h fileserver01.samba.private -t AAAA -V 2001:db8::190
D. nsupdatesmb -U Administrator //dc1/samba.private/fileserver01 add AAAA 2001:db8::190
E. samba-tool dns add dc1 samba.private fileserver01 AAAA 2001:db8::190 -U Administrator

Answer: E

Explanation:

Command The samba-tool dns add command is used to add DNS records in Samba. Parameters:
dc1: Specifies the Samba DNS server.
samba.private: The DNS zone.
fileserver01: The hostname for the new DNS record.
AAAA: Specifies that the record is for an IPv6 address.
2001:db8::190: The IPv6 address to be assigned to the hostname.
-U Administrator: Specifies the user performing the operation, in this case, the Administrator.

Usage: This command properly adds a forward DNS record for fileserver01 with the specified IPv6 address into the samba.private zone on the server dc1.

Reference:

Samba DNS Administration

Question: 22

A Samba 4 server provides DNS information regarding an Active Directory Domain. All other DNS information is provided by an additional DNS server. Which of the following solutions ensures that the clients of the Samba server can look up all DNS records including those from the domain?

A. The additional DNS server is configured in the file /etc/resolv.conf on the Samba server and the option dns forwarder = yes is set in smb.conf.

B. The search domain of all clients is set to the Active Directory domain name. All clients query only the additional DNS server and not a domain controller.

C. Both the Samba server and the additional DNS server are configured on the clients. This ensures that the Samba server is listed first in each client's resolv.conf.

D. All clients are configured to send DNS queries to the additional DNS server only. The Samba server's smb.conf contains the option wins dns proxy = yes to provide all domain-related naming information via the NetBIOS name service independently from DNS.

E. The additional DNS server is configured in the option dns forwarder in smb.conf. All clients query the Samba server for any DNS information.

Answer: E

Explanation:

dns forwarder: This smb.conf option specifies the DNS server to which queries should be forwarded if they cannot be resolved locally by the Samba server.

Configuration:

Add dns forwarder = <additional_DNS_server_IP> to smb.conf on the Samba server.

Ensure all clients are configured to query the Samba server for DNS information.

Process:

Clients send all DNS queries to the Samba server.

If the Samba server cannot resolve a query locally, it forwards the request to the additional DNS server.

Benefit: This ensures that all DNS records, including those from the Active Directory domain and other DNS information, can be resolved by the clients.

Reference:

Samba DNS Forwarding

Question: 23

Which of the following commands sets up Samba 4 as an Active Domain Directory Controller for a new domain?

A. samldap-domainadd
B. net ads prepare domain
C. samba-tool domain provision
D. smbcontrol dcpromo

E. samba-dcpromo

Answer: C

Explanation:

samba-tool domain provision: This command sets up Samba 4 as an Active Directory Domain Controller.

Process:

Run samba-tool domain provision to start the setup.

Follow the prompts to specify the domain name, administrator password, and other required information.

Outcome: This command initializes the Samba server as a new domain controller for a new domain, configuring the necessary services and databases.

Reference:

Samba Active Directory Domain Controller

Question: 24

What is true about the container CN=Users in an Active Directory LDAP tree? (Choose two.)

A. GPOs cannot be assigned to this container.
B. Users outside of this container cannot log into any member computer of the domain.
C. The container can only contain user object but no user groups.
D. New users are created here and must be moved to another container before they can log in.
E. New users are by default created in this container.

Answer: A, E

Explanation:

CN=Users Container:

GPOs: Group Policy Objects (GPOs) cannot be linked to this container because it is not an Organizational Unit (OU). GPOs can only be applied to OUs.

Default Location: New users are created in the CN=Users container by default when using standard Active Directory tools unless specified otherwise.

Other Options:

Users outside this container can log in.

The container can contain both user objects and user groups.

Users created here do not need to be moved to log in.

Reference:

Active Directory Containers and OUs

Question: 25

Which of the following statements are true regarding the smbpasswd command? (Choose two.)

A. The -x parameter removes an account from the Samba database.

B. The -a parameter adds an account to the Samba database. If the account already exists, this parameter is ignored.

C. The -d parameter deletes an account from the Samba database.

D. The -e parameter excludes an account from the Samba database.

E. smbpasswd changes only passwords on Samba domain controllers while DCs running Windows keep the

old passwords.

Answer: A, B

Explanation:

- x Parameter: This parameter is used to remove (delete) an account from the Samba database. Example: smbpasswd -x username
- a Parameter: This parameter adds a new account to the Samba database. If the account already exists, it will update the account.

Example: smbpasswd -a username

Other Options:

- d Parameter: Disables (not deletes) an account.
- e Parameter: Enables a previously disabled account.

Password Synchronization: The smbpasswd command does not affect Windows domain controllers; it manages Samba-specific passwords.

Reference:

smbpasswd Command Documentation

Question: 26

Which of the following commands can be used to join the local Samba server as a member to the domain samba.private?

A. samba-tool member add samba.private
B. samba-tool domjoin samba.private
C. samba-tool domain join samba.private member
D. samba-tool join samba.private member
E. samba-tool node set-domain samba.private

Answer: C

Explanation:

Understanding Samba Domain Join: Joining a Samba server to a domain allows it to authenticate and provide resources to users of that domain.

Command Breakdown: The correct command format for joining a Samba server as a member of a domain involves the "domain join" action followed by the domain name and the role. In this case, "samba.private" is the domain name, and "member" specifies the role.

Command

samba-tool domain join samba.private member: samba-tool: A command-line utility for managing Samba. domain join: Specifies the action of joining a domain. samba.private: The domain to join. member: The role within the domain.

Reference:

Samba Wiki - Samba Tool

Question: 27

Which parameters are available for samba-tool group add? (Choose two.)

A. --default-gpo
B. --groupou
C. --login-script
D. --sid
E. --group-type

Answer: D, E

Explanation:

The samba-tool group add command is used to add a new group to the Samba Active Directory. This command has several parameters to customize the group creation process. Two of the available parameters are --sid and --group-type.

--sid:

The --sid parameter allows you to specify a Security Identifier (SID) for the new group.

Example usage:

samba-tool group add mygroup --sid=S-1-5-21-1234567890-123456789-1234567890-1234

This command will create a new group named mygroup with the specified SID.

--group-type:

The --group-type parameter allows you to specify the type of the group being created. This can be a security group or a distribution group.

Example usage:

samba-tool group add mygroup --group-type=security

This command will create a new security group named mygroup.

Reference:

Samba Official Documentation: samba-tool

Samba Active Directory Management: Managing Groups

Question: 28

FILL BLANK

What command checks the Samba configuration file for syntactical correctness? (Specify ONLY the command without any path or parameters.)

Answer: testparm

Explanation:

Purpose of the Command: testparm is used to check the Samba configuration file (smb.conf) for syntax errors.

Command

Running testparm will read the smb.conf file, parse it, and display any syntax errors or warnings. This helps ensure that the configuration is valid before restarting the Samba service.

Usage Example:

Simply execute testparm in the terminal, and it will automatically check the default configuration file.

Reference:

Samba.org - testparm

Question: 29

Which of the following statements is true regarding Samba 4?

A. Samba 4 is only a minor update to Samba 3, which fixes smaller bugs and contains no new features.
B. Microsoft Windows clients cannot connect to Samba 4 servers.
C. Samba 4 can serve as an Active Directory Domain Controller.
D. Samba 4 includes an own file system, sambafs, to format block devices.
E. Integration of Samba 4 in an existing Active Directory Domain is not possible.

Answer: C

Explanation:

Samba 4 Features: Samba 4 introduces major enhancements over Samba 3, including the ability to function as an Active Directory (AD) Domain Controller.

Capability as AD Controller:

Samba 4 includes support for AD protocols, allowing it to manage domain users and computers similar to a Windows AD server.

Incorrect Statements Clarified:

Samba 4 is a significant update with new features.

Windows clients can connect to Samba 4 servers.

Samba 4 does not include a proprietary file system called sambafs.

Samba 4 can integrate with existing AD domains.

Reference:

Samba Wiki - Samba4

Question: 30

How is Samba instructed to read its entire configuration from the registry?

A. By starting all Samba processes with the option --regconf.
B. By putting config backend = registry in the [global] section of smb.conf.
C. By starting the regd service in addition to the other Samba services.
D. By replacing private.tdb with a plain text registry file holding the server's configuration.
E. By creating a symbolic link from smb.conf to the .reg file holding the configuration.

Answer: B

Explanation:

Configuration Backend: Samba can be configured to read its settings from various backends, including the Windows registry.

Setting the Backend:

Adding config backend = registry in the [global] section of smb.conf instructs Samba to use the registry for its configuration.

Implementation Steps:

Open the smb.conf file.

Add the line config backend = registry under the [global] section.

Restart the Samba services to apply the changes.

Reference:

Question: 31

Which of the following commands terminates all running instances of the Samba daemon handling for SMB shares?

A. smbcontrol samba shutdown
B. smbcontrol nmbd shutdown
C. smbcontrol shutdown
D. smbcontrol smbd shutdown
E. smbcontrol cifs stop

Answer: D

Explanation:

Samba is a suite of programs that allows SMB/CIFS clients to interact with file and print services on a Linux/UNIX server.
smbd is the Samba daemon responsible for handling SMB/CIFS requests.
The smbcontrol utility is used to send messages to running Samba daemons.
The correct way to terminate all running instances of the Samba daemon handling SMB shares is to send a shutdown message to smbd using the command smbcontrol smbd shutdown.
This command ensures that only the smbd processes, which are responsible for handling SMB shares, are terminated without affecting other Samba components like nmbd (NetBIOS name server daemon).

Reference:
Samba documentation: https://www.samba.org/samba/docs/current/man-html/smbcontrol.1.html

Question: 32

Which of the following TCP ports is used to provide the SMB protocol without NetBIOS?

A. 133
B. 138
C. 139
D. 386
E. 445

Answer: E

Explanation:

The SMB protocol (Server Message Block) is used for providing shared access to files and printers.
Historically, SMB ran on top of NetBIOS over TCP/IP using port 139.
SMB can also run directly over TCP/IP without the NetBIOS layer, which uses port 445.
Therefore, TCP port 445 is used to provide the SMB protocol without NetBIOS.

Reference:
Official IANA port numbers: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
Microsoft documentation on SMB: https://docs.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview

Question: 33

FILL BLANK
What attribute starts the declaration of an object in an LDIF file? (Specify ONLY the attribute name without any values.)

Answer: dn

Explanation:

An LDIF (LDAP Data Interchange Format) file is used to represent directory entries in LDAP (Lightweight Directory Access Protocol).
Each entry in an LDIF file starts with the dn (Distinguished Name) attribute, which uniquely identifies the entry in the directory.
The dn attribute is mandatory and specifies the path to the entry within the LDAP directory. Reference:
LDAP documentation: https://ldap.com/ldap-data-interchange-format-ldif/
OpenLDAP LDIF documentation: https://www.openldap.org/doc/admin24/ldif.html

Question: 34

In an LDIF file using changetype: modify, which of the following options can be used? (Choose two.)

A. patch
B. overwrite
C. add
D. replace
E. generate

Answer: C, D

Explanation:

In an LDIF file, changetype: modify is used to specify modifications to an existing LDAP entry.
The add option is used to add new attributes or values to an existing attribute.
The replace option is used to replace existing attribute values with new ones.
These options are used to update the directory information according to the LDAP protocol.
Reference:
LDAP modification operations: https://ldap.com/the-ldif-format/
OpenLDAP modify documentation: https://www.openldap.org/doc/admin24/modify.html

Question: 35

In a Samba configuration file, which of the following variables represents the domain of the current user?

A. %D
B. %r
C. %d
D. %G
E. %w

Answer: A

Explanation:

In a Samba configuration file, variables can be used to represent dynamic values.
The %D variable represents the domain of the current user.
This variable can be used in various configuration directives to customize the behavior of Samba services based on the user's domain.

Reference:
Samba variables documentation: https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

Question: 36

What are benefits of registry based Samba configuration compared to file based configuration? (Choose three.)

A. The registry can be edited remotely without logging into the server.
B. Registry based configuration supports advanced options which do not exist in smb.conf.
C. Server processes require less time to start because they do not have to parse the configuration file.
D. Configuration changes become effective immediately without a daemon reload.
E. Specific attributes of LDAP objects in Active Directory can be overwritten in the configuration registry.

Answer: A, C, D

Explanation:

Remote Editing:
A . The registry can be edited remotely without logging into the server: One of the benefits of registry-based Samba configuration is that the registry can be edited remotely. This means administrators can make changes without needing to log into the server directly, facilitating easier and more flexible management.
Improved Startup Time:
C . Server processes require less time to start because they do not have to parse the configuration file: Registry-based configurations can reduce startup time because the Samba server processes do not need to parse a potentially complex smb.conf file. Instead, they access the configuration directly from the registry, which can be faster.
Immediate Effect of Configuration Changes:
D . Configuration changes become effective immediately without a daemon reload: Changes made in the registry are applied immediately and do not require a daemon reload. This can be very advantageous for administrators who need to make quick adjustments without interrupting the service.

Reference:
Samba documentation
Various Samba configuration tutorials and best practice guides

Question: 37

In order to generate an individual log file for each of the machines connecting to a Samba server, which of the following statements must be used in the Samba configuration file?

A. log file = /var/log/samba/log.%m

B. log file = /var/log/samba/log.%M
C. log file = /var/log/samba/log.%r
D. log file = /var/log/samba/log.%I
E. log file = /var/log/samba/log.%c

Answer: A

Explanation:

Individual Log Files:

A . log file = /var/log/samba/log.%m: To generate an individual log file for each machine connecting to a Samba server, the %m variable is used in the log file path. This variable represents the machine name of the connecting client. Thus, the configuration line log file = /var/log/samba/log.%m creates a unique log file for each client machine.

Reference:

Samba smb.conf manual

Logging configurations in Samba

Question: 38

Which command creates a consistent copy of LDB files?

A. tdbbackup
B. samba-backup
C. ldbbackup
D. smbbackup
E. ldbsync

Answer: C

Explanation:

Consistent Copy of LDB Files:

C . ldbbackup: The ldbbackup command is used to create a consistent copy of LDB files. LDB files are used by Samba to store data in a database format. The ldbbackup utility ensures that the data is copied in a consistent state, which is crucial for backup and recovery processes.

Reference:

Samba documentation on ldbbackup

General LDB management guides

Question: 39

FILL BLANK

What service name must be added to a database entry in /etc/nsswitch.conf to include SSSD as a source of information? (Specify ONLY the service name without any parameters.)

Answer: sss

Explanation:

Adding SSSD to /etc/nsswitch.conf:

To include SSSD (System Security Services Daemon) as a source of information in the /etc/nsswitch.conf file, the service name sss must be added. This is specified without any parameters. The sss service allows the system to retrieve information from various sources, such as LDAP, Kerberos, and others, as configured in SSSD.

Reference:

SSSD documentation

nsswitch.conf configuration guidelines

Question: 40

Which of the following Group Policy Objects exist by default in an Active Directory domain? (Choose two.)

A. Default Domain Policy
B. Default Domain Controllers Policy
C. Default Domain File Access Policy
D. Default Domain Firewall Policy
E. Default Domain Print Driver Policy

Answer: A, B

Explanation:

Default Group Policy Objects in AD:

A . Default Domain Policy: This is a built-in GPO that is applied to all users and computers in the domain. It contains security settings, password policies, and other domain-wide configurations. B . Default Domain Controllers Policy: This GPO is specifically applied to the Domain Controllers organizational unit (OU). It contains settings relevant to domain controllers, such as security settings and audit policies.

Reference:

Active Directory Group Policy documentation

Best practices for managing Group Policy in Active Directory

Question: 41

Which of the following keywords are module types for PAM? (Choose three.)

A. cache
B. authentication
C. password
D. session
E. account

Answer: C, D, E

Explanation:

Pluggable Authentication Modules (PAM) provides a system of libraries that handle the authentication tasks of applications (services) on a Linux system. These libraries are loaded dynamically and can be configured in the /etc/pam.d directory or in /etc/pam.conf. The PAM modules are divided into four types:

auth (authentication): This module type is responsible for authenticating the user, setting up user credentials, and initiating a session.

account: This module type manages account policies such as password expiration, access restrictions, and

checking user permissions.
password: This module type handles the updating of authentication tokens, such as passwords. session: This module type manages tasks that need to be performed at the beginning and end of a session, like mounting directories or logging.
Reference:
Linux PAM Documentation
Understanding PAM

Question: 42
FILL BLANK

Which command line option instructs smbclient to authenticate using an existing Kerberos token? (Specify ONLY the option name without any values or parameters.)

Answer: -k

Explanation:

The smbclient command is used to access shared resources on a server running the SMB/CIFS protocol. To authenticate using an existing Kerberos token, the -k option is used. This instructs smbclient to use Kerberos for authentication, assuming that the user already has a valid Kerberos ticket (usually obtained via the kinit command).
Example:
smbclient //server/share -k
Reference:
smbclient man page
Kerberos Authentication with Samba

Question: 43
Which of the following sections is always present in sssd.conf?

A. [krb5]
B. [ad]
C. [autn]
D. [sssd]
E. [local]

Answer: D

Explanation:

The sssd.conf file is the configuration file for the System Security Services Daemon (SSSD). SSSD provides access to different identity and authentication providers. The configuration file typically contains multiple sections, but the [sssd] section is always present. This section provides global options that apply to all other sections of the file.
Example:

[sssd] config_file_version = 2 services = nss, pam domains = LDAP

Reference:

SSSD Configuration

SSSD Man Pages

Question: 44

Which of the following sections in the Kerberos configuration file may contain the option default_realm?

A. defaults
B. krb5
C. libdefaults
D. global
E. realms

Answer: C

Explanation:

The Kerberos configuration file, typically located at /etc/krb5.conf, contains several sections, each with different settings that control the behavior of Kerberos. The libdefaults section is where default settings for Kerberos libraries are defined, and it may include the default_realm option.

Example:

[libdefaults] default_realm = EXAMPLE.COM dns_lookup_realm = false dns_lookup_kdc = true

Reference:

Kerberos Configuration

Red Hat Kerberos Configuration

Question: 45

Which of the following names identify services within a SSSD configuration file? (Choose three.)

A. kerberos
B. ssh
C. smb
D. nss
E. sudo

Answer: A, D, E

Explanation:

In the SSSD (System Security Services Daemon) configuration file, various services can be defined to handle different types of access and authentication. The services listed in the SSSD configuration file under the [sssd] section can include:

kerberos: This service allows SSSD to handle Kerberos authentication.

nss (Name Service Switch): This service provides name resolution and manages user and group information.

sudo: This service enables SSSD to provide sudo rules based on the identity provider.

These services are specified in the services attribute of the [sssd] section of the sssd.conf file.

Example:

[sssd] services = nss, pam, sudo domains = LDAP [nss] filter_users = root filter_groups = root [sudo]
sudo_provider = ldap

Reference:
SSSD Services
SSSD Man Pages

Question: 46

Which smbclient invocation displays a list of the available SMB shares on the remote Samba server FileSrv1?

A. smbcontrol -L FileSrv1
B. smbshares --server FileSrv1
C. smbstatus -S FileSrv1
D. smbmount -L FileSrv1
E. smbclient -L FileSrv1

Answer: E

Explanation:

The smbclient command is used to access shared resources on a network that uses the SMB (Server Message Block) protocol. To list the available SMB shares on a remote Samba server, the correct invocation is smbclient -L <server_name>. Here, -L stands for "list" and <server_name> is the name of the Samba server. Therefore, smbclient -L FileSrv1 will list all the available SMB shares on the server named FileSrv1.

Reference:
smbclient man page
Samba: smbclient Command

Question: 47

Which parameter in a user object defines on which share the user's roaming profile is stored?

A. autoMount
B. logonDrive
C. profilePath
D. homePath
E. driveMap

Answer: C

Explanation:

The profilePath parameter in a user object specifies the path to the user's roaming profile. A roaming profile is a feature in Windows that allows user profile data to be stored on a network share so that users can access their profiles from any workstation within the network. By setting the profilePath, administrators can define where on the network the profile data is stored.

Reference:
Roaming User Profiles
User Account Properties

Question: 48

Which of the following commands connects to the share Share on the Windows Server 2012 R2 server fs1 using the SMB3 protocol?

A. smb3client //fs1/Share
B. smbclient --max-protocol SMB3 //fs1/Share
C. smbclient --w2k12 //fs1/share
D. smbclient -p 3 //fs1/Share
E. cifsclient //fs1/Share

Answer: B

Explanation:

To connect to a share on a Windows server using the SMB3 protocol, the smbclient command with the --max-protocol option should be used. The --max-protocol option allows you to specify the highest SMB protocol version that should be used. Therefore, the correct command is smbclient -max-protocol SMB3 //fs1/Share.

Reference:

smbclient man page

Samba: smbclient Command Options

Question: 49

When logging into a windows workstation which is member of an Active Directory domain, which of the following user names refers to the local account bob instead of the domain-wide account bob?

A. bob@local
B. %bob%
C. .\bob
D. "bob"
E. bob$

Answer: C

Explanation:

When logging into a Windows workstation that is a member of an Active Directory domain, the .\ prefix is used to specify a local user account rather than a domain account. Therefore, to refer to the local account bob, you would use .\bob.

Reference:

How to Log On to Your Computer if You Are a Domain User

Windows Logon Naming Conventions

Question: 50

What is a correct statement about FreeIPA ID views?

A. ID views are used to modify sudo rules on a per host base.

B. ID views are the FreeIPA equivalent to Active Directory SIDs.
C. ID views specify new values for attributes of a POSIX user or group.
D. ID views provide a consecutive numberspace of UIDs and GIDs for FreeIPA users and groups.
E. ID views always manage IDs from 32768 to 65536.

Answer: C

Explanation:

In FreeIPA, ID views allow administrators to override default POSIX attributes for users and groups. This feature is useful when integrating with other identity management systems, enabling specific attribute values to be used on a per-host basis. This way, different POSIX attributes can be set for the same user or group in different contexts.

Reference:
FreeIPA: ID Views
FreeIPA Documentation

Question: 51

Given a proper network and name resolution setup, which of the following commands establishes a trust between a FreeIPA domain and an Active Directory domain?

A. trustmanager add --domain ad://addom --user Administrator -w
B. ipa-ad --add-trust --account ADDOM\Administrator --query-password
C. net ad ipajoin addom -U Administrator -p
D. ipa trust-add --type ad addom --admin Administrator --password
E. ipa ad join addom -U Administrator -W

Answer: D

Explanation:

To establish a trust between a FreeIPA domain and an Active Directory domain, the correct command is ipa trust-add. This command is used to add a trust relationship with an Active Directory (AD) domain. The --type ad specifies the type of the trust, addom is the domain name, --admin Administrator specifies the AD administrator account, and --password prompts for the administrator's password.

The complete command looks like this:
a trust-add --type ad addom --admin Administrator --password
This command will initiate the trust creation process, which involves providing the credentials of the AD administrator.

Reference:
FreeIPA Trusts
FreeIPA Trust Management

Question: 52

Which of the following commands open NFSv4 ACLs in an editor? (Choose two.)

A. nfs4_setfacl -e
B. nfs4_editfacl

C. nfs4_stat -e --acl
D. nfs4_chmod -i
E. nfs4_conf

Answer: A, B

Explanation:

To open NFSv4 ACLs in an editor, the following commands can be used: nfs4_setfacl -e: This command is used to set NFSv4 ACLs, and the -e option opens the ACLs in an editor for modification. The command usage is: This opens the ACL editor where the user can modify the ACLs for the specified file. nfs4_editfacl: This command is a more intuitive way to edit NFSv4 ACLs directly in an editor. It provides a user-friendly interface for managing ACLs.

Reference:

NFSv4 ACL Tools Documentation

NFSv4 ACLs

Question: 53

Which of the following statements about automount in a FreeIPA domain are true? (Choose two.)

A. In a FreeIPA domain, mount points for automount are always directories.
B. The command ipa automount up mounts all file systems handled by automount on a FreeIPA client.
C. The base configuration file for automount is /etc/auto.master.
D. In a FreeIPA domain, automount requires SSSD to be installed on each client.
E. In a FreeIPA domain, automount can only mount NFS shares from FreeIPA servers.

Answer: C, D

Explanation:

Automounting in a FreeIPA domain involves several key aspects:

Base Configuration File (/etc/auto.master): The auto.master file is the main configuration file for the automounter. It contains the master map which defines mount points and their corresponding maps. This file is crucial for setting up automount points.

Example entry in /etc/auto.master:

plaintext

Copy code

/home /etc/auto.home

SSSD Requirement: In a FreeIPA domain, automount requires the System Security Services Daemon (SSSD) to be installed and configured on each client. SSSD is used to retrieve automount maps from the FreeIPA server, enabling the automount feature to function correctly.

Example configuration in /etc/sssd/sssd.conf:

[sssd] services = nss, pam, autofs config_file_version = 2 domains = example.com [domain/example.com] autofs_provider = ipa ipa_server = _srv_

Reference:

Automount Configuration

FreeIPA SSSD Integration