HowTo LPIC3 300-100
Mixed environments

Curs 2020 - 2021

Documentació / Recursos

LPI-3 Enterprise Mixed Environment (300-100 Exam)

- ❏ https://www.lpi.org/our-certifications/lpic-3-300-overview

Tests de formació:

- ❏ Examtopics
  https://www.examtopics.com/exams/lpi/300-100/
  Disponibles 60 preguntes free.

- ❏ Killtest
  https://www.killtest.com/LPIC-3/300-100.asp

- ❏ Prepare4sure
  https://www.prepare4sure.com/300-100-braindump.html

- ❏ Examdocs
  http://www.examsdocs.com/?option=com_content&view=article&examcode=300-100&gclid=CjwKCAiAzNj9BRBDEiwAPsL0d_1oEBrWHaMNIoxmCUDRZ0VdxCZjNdb0ZmG-ganJSeo5EAqKCPi2sxoCVFAQAvD_BwE

Continguts / Pès:

- ❏ 390 (8) OpenLDAP Configuration
  - ❏ 390.1 (3) OpenLDAP Replication
  - ❏ 390.2 (3) Securing the Directory
  - ❏ 390.3 (2) OpenLDAP Server Performance Tuning

- ❏ 391 (4) OpenLDAP as an Authentication Backend
  - ❏ 391.1 (2) LDAP Integration with PAM and NSS
  - ❏ 391.2 (2) Integrating LDAP with Active Directory and Kerberos

- ❏ 392 (11) Samba Basics
  - ❏ 392.1 (2) Samba Concepts and Architecture
  - ❏ 392.2 (4) Configure Samba
  - ❏ 392.3 (2) Regular Samba Maintenance
  - ❏ 392.4 (2) Troubleshooting Samba
  - ❏ 392.5 (1) Internationalization

- ❏ 393 (9) Samba Share Configuration
  - ❏ 393.1 (4) File Services
  - ❏ 393.2 (3) Linux File System and Share/Service Permissions

  - ❏ 393.3 (2) Print Services
- ❏ 394 (9) Samba User and Group Management
  - ❏ 394.1 (4) Managing User Accounts and Groups
  - ❏ 394.2 (5) Authentication, Authorization and Winbind

- ❏ 395 (9) Samba Domain Integration
  - ❏ 395.1 (3) Samba as a PDC and BDC
  - ❏ 395.2 (3) Samba4 as an AD compatible Domain Controller
  - ❏ 395.3 (3) Configure Samba as a Domain Member Server

- ❏ 396 (5) Samba Name Services
  - ❏ 396.1 (3) NetBIOS and WINS
  - ❏ 396.2 (2) Active Directory Name Resolution

- ❏ 397 (5) Working with Linux and Windows Clients
  - ❏ 397.1 (3) CIFS Integration
  - ❏ 397.2 (2) Working with Windows Clients

390. (8) OpenLDAP Configuration

Contingguts

- ❑ 390 (8) OpenLDAP Configuration
  - ❑ 390.1 (3) OpenLDAP Replication
  - ❑ 390.2 (3) Securing the Directory
  - ❑ 390.3 (2) OpenLDAP Server Performance Tuning

Documentation

- OpenLDAP documentation: Chapter 18 Replication
- Practical LPIC-3 300. Antonio Vazquez. Apress. 2019.
- DockerHub:
  - *docker pull edtasixm06/ldapsyncrepl*
  - *docker pull edtasixm06/ldapdeltasyncrepl*
  - *docker pull edtasixm06/ldapoverlay*
- Apunts edt (Escola del Treball de Barcelona)
  - HowTo-ASIX-2-Ldap
  - HowTo-ASIX-LDAP
  - Mastering OpenLDAP
  - HowTo-ASIX_Certificats_Digitals

390.1 (3) OpenLDAP Replication

Description: Candidates should be familiar with the server replication available with penLDAP.
Weight: 3

Key Knowledge Areas

- Replication concepts
- Configure OpenLDAP replication
- Analyze replication log files
- Understand replica hubs
- LDAP referrals
- LDAP sync replication

The following is a partial list of the used files, terms and utilities

- master / slave server
- multi-master replication
- consumer
- replica hub
- one-shot mode
- referral
- syncrepl
- pull-based / push-based synchronization
- refreshOnly and refreshAndPersist
- replog

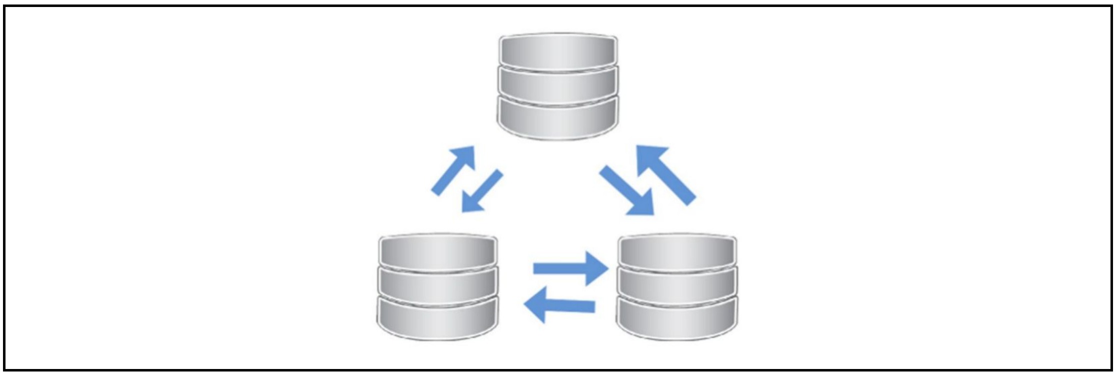
Description

Provider/Multi-provider Consumers

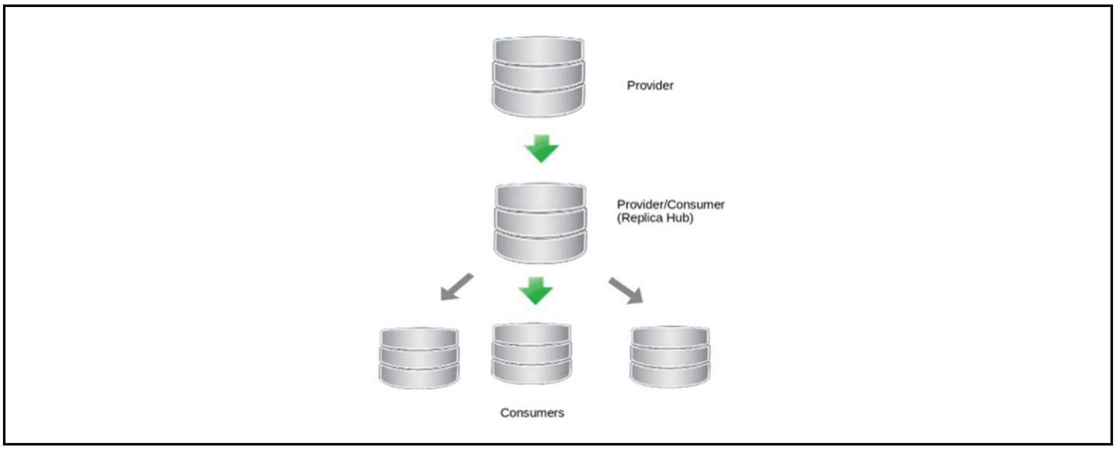
- **provider/multiprovider**: A provider can accept external write operations and make them available for retrieval by consumers. The LDAP Sync provider can be configured as an overlay on any backend.

- **consumers** request replication updates from providers.

- **Multi-Provider** replication is a replication technique using Syncrepl to replicate data to multiple provider ("Provider") Directory servers. If any provider fails, other providers will continue to accept updates. Avoids a single point of failure. Providers can be located in several physical sites i.e. distributed across the network/globe. Good for Automatic failover/High Availability. **Multimaster** replication topology. In this case we have two or more master servers. The changes can be made on any of these servers and they are replicated to the remaining servers.



- **Replica hub**: Unlike the rigidly defined master/slave relationships, provider/consumer roles are quite fluid: replication updates received in a consumer can be further propagated by that consumer to other servers, so **a consumer can also act simultaneously as a provider**. Also, a consumer need not be an actual LDAP server; it may be just an LDAP client.



Syncrepl: The LDAP Sync Replication engine, syncrepl for short,

- is a **consumer-side** replication engine that enables the consumer LDAP server to maintain a shadow copy of a DIT fragment. A syncrepl engine resides at the consumer and executes as one of the slapd(8) threads. It creates and maintains a replica by connecting to the replication provider to perform the initial DIT content load followed either by periodic content polling or by timely updates upon content changes.

- Syncrepl uses the **LDAP Content Synchronization protocol**: LDAP Sync.
- LDAP Sync provides a stateful replication which supports both pull-based and push-based synchronization and does not mandate the use of a history store. In **pull-based** replication the consumer periodically polls the provider for updates. In

push-based replication the consumer listens for updates that are sent by the provider in realtime.

- Since the protocol does not require a history store, the provider does not need to maintain any log of updates it has received.
- Syncrepl keeps track of the status of the replication content by maintaining and exchanging synchronization cookies. Because the syncrepl consumer and provider maintain their content status, the consumer can poll the provider content to perform incremental synchronization by asking for the entries required to make the consumer up-to-date with the provider content. Syncrepl also enables convenient management of consumers by maintaining replication status. The consumer database can be constructed from a consumer-side or a provider-side backup at any synchronization status. Syncrepl can automatically resynchronize the consumer database to be up-to-date with the current provider content.

- With syncrepl, a consumer can create a **replication agreement** without changing the provider's configurations and without restarting the provider server, if the consumer server has appropriate access privileges for the DIT fragment to be replicated. The consumer server can stop the replication also without the need for provider-side changes and restart.

- Syncrepl supports partial, sparse, and fractional replications. The shadow DIT fragment is defined by a general **search criteria** consisting of **base**, **scope**, **filter**, and **attribute list**. The consumer content is also subject to the access privileges of the bind identity of the syncrepl replication connection.

- In the LDAP Sync protocol, entries are uniquely identified by the **entryUUID** attribute value. It can function as a reliable identifier of the entry. The DN of the entry, on the other hand, can be changed over time and hence cannot be considered as the reliable identifier. The entryUUID is attached to each *SearchResultEntry* or *SearchResultReference* as a part of the synchronization control.

- *[deptrecated]* slurpd és l'antic daemon de repliques. Generava fitxers de log anomenats REJECTION amb l'extensiṕ .rej.

refreshOnly synchronization mode,

(provider: pull-based, consumer: polling)

- the provider uses **pull-based** synchronization where the consumer servers need not be tracked and no history information is maintained. The information required for the provider to process periodic polling requests is contained in the synchronization cookie of the request itself. To optimize the pull-based synchronization, syncrepl utilizes the present phase of the LDAP Sync protocol as well as its delete phase, instead of falling back on frequent full reloads. To further optimize the pull-based synchronization, the provider can maintain a per-scope session log as a history store.

- **Polling** is implemented by the refreshOnly operation. The consumer polls the provider using an LDAP Search request with an LDAP Sync control attached. The consumer copy is synchronized to the provider copy at the time of polling using the information returned in the search. The provider finishes the search operation by returning SearchResultDone at the end of the search operation as in the normal search.

❏ At the end of the refreshOnly synchronization, the provider sends a synchronization cookie to the consumer as a state indicator of the consumer copy after the synchronization is completed. The consumer will present the received cookie when it requests the next incremental synchronization to the provider.

refreshAndPersist mode of synchronization,
(provider: push-based, consumer: listening)

❏ the provider uses a **push-based** synchronization. The provider keeps track of the consumer servers that have requested a persistent search and sends them necessary updates as the provider replication content gets modified.

❏ **Listening** is implemented by the *refreshAndPersist* operation. As the name implies, it begins with a search, like refreshOnly. Instead of finishing the search after returning all entries currently matching the search criteria, the synchronization search remains persistent in the provider. Subsequent updates to the synchronization content in the provider cause additional entry updates to be sent to the consumer.

❏ When refreshAndPersist synchronization is used, the provider sends a synchronization cookie at the end of the refresh stage by sending a Sync Info message with refreshDone=TRUE. It also sends a synchronization cookie by attaching it to SearchResultEntry messages generated in the persist stage of the synchronization search. During the persist stage, the provider can also send a Sync Info message containing the synchronization cookie at any time the provider wants to update the consumer-side state indicator.

Phases: Present Phase / delete Phase

❏ The refreshOnly operation and the refresh stage of the refreshAndPersist operation can be performed with a present phase or a delete phase.

❏ In the **present phase**, the provider sends the consumer the entries updated within the search scope since the last synchronization. The provider sends all requested attributes, be they changed or not, of the updated entries. For each unchanged entry which remains in the scope, the provider sends a present message consisting only of the name of the entry and the synchronization control representing state present. The present message does not contain any attributes of the entry. After the consumer receives all update and present entries, it can reliably determine the new consumer copy by adding the entries added to the provider, by replacing the entries modified at the provider, and by deleting entries in the consumer copy which have not been updated nor specified as being present at the provider.

- In the **delete phase** the transmission of the updated entries is the same as in the present phase. The provider sends all the requested attributes of the entries updated within the search scope since the last synchronization to the consumer. In the delete phase, however, the provider sends a delete message for each entry deleted from the search scope, instead of sending present messages. The delete message consists only of the name of the entry and the synchronization control representing state delete. The new consumer copy can be determined by adding, modifying, and removing entries according to the synchronization control attached to the SearchResultEntry message.

- In the case that the LDAP Sync provider **maintains a history** store and can determine which entries are scoped out of the consumer copy since the last synchronization time, **the provider can use the delete phase**. If the provider **does not maintain** any history store, cannot determine the scoped-out entries from the history store, or the history store does not cover the outdated synchronization state of the consumer, the **provider should use the present phase**.

- The use of the **present phase** is much more efficient than a full content reload in terms of the synchronization traffic. To reduce the synchronization traffic further, the LDAP Sync protocol also provides several optimizations such as the transmission of the normalized entryUUIDs and the transmission of multiple entryUUIDs in a single *syncIdSet* message.

Referrals

- Si en les rèpliques només es disposa d'una part de l'arbre DIT les consultres d'aquest subarbre són contestades per la rèplica. Però si es demana per altres branques del DIT que estan al provider i no al consumer la resposta és un error (no update referral).

- Si es tracta d'un ldap delegat (que conté només un subarbre) també passa el mateix quan es demana a un o slatre server les dades que no té en el seu arbre, s'obté una resposta d'error de referral.

- El servidor ldap es pot configurar per amb un referral per proporcionar informació consistent. Ara la resposta del servidor serà indicar el referral (no la informació final). Algunes ordres poden proporcionar la informació final fent *referral chasing*. Per realitzar sempre la resolució final de les dades es pot configurar en el servidor l' *overlay chaining* per tal de que 'segueixi' els referrals.

Configuration

Provider

```
syncprov-checkpoint <ops> <minutes>   #The contextCSN checkpoint <ops> operations or more than <minutes>
syncprov-sessionlog <ops>             # The session log <ops>  maximum session log entries can record
syncprov-reloadhint <TRUE|FALSE>
```

```
syncprov-nopresent <TRUE|FALSE>
```

```
database mdb
    maxsize 85899345920
    suffix dc=example,dc=com
    rootdn dc=example,dc=com
    directory /var/ldap/db
    index objectclass,entryCSN,entryUUID eq

    overlay syncprov
    syncprov-checkpoint 100 10
    syncprov-sessionlog 100
```

Consumer

```
database mdb
    maxsize 85899345920
    suffix dc=example,dc=com
    rootdn dc=example,dc=com
    directory /var/ldap/db
    index objectclass,entryCSN,entryUUID eq

    syncrepl rid=123
        provider=ldap://provider.example.com:389
        type=refreshOnly
        interval=01:00:00:00
        searchbase="dc=example,dc=com"
        filter="(objectClass=organizationalPerson)"
        scope=sub
        attrs="cn,sn,ou,telephoneNumber,title,l"
        schemachecking=off
        bindmethod=simple
        binddn="cn=syncuser,dc=example,dc=com"
        credentials=secret
```

- In this example, the consumer will connect to the provider slapd(8) at port 389 of ldap://provider.example.com to perform a polling (refreshOnly) mode of synchronization once a day. It will bind as cn=syncuser,dc=example,dc=com using simple authentication with password "secret". Note that the access control privilege of cn=syncuser,dc=example,dc=com should be set appropriately in the provider to retrieve the desired replication content. Also the search limits must be high enough on the provider to allow the syncuser to retrieve a complete copy of the requested content. The consumer uses the rootdn to write to its database so it always has full permissions to write all content.

- The synchronization search in the above example will search for the entries whose objectClass is organizationalPerson in the entire subtree rooted at dc=example,dc=com. The requested attributes are cn, sn, ou, telephoneNumber, title, and l. The schema checking is turned off, so that the consumer slapd(8) will not enforce entry schema checking when it processes updates from the provider slapd(8).

Replica example

The following example is for a self-contained push-based replication solution:

```
modulepath  /usr/local/libexec/openldap
      moduleload  back_mdb.la
      moduleload  syncprov.la
      moduleload  back_monitor.la
      moduleload  back_ldap.la

      pidfile     /usr/local/var/slapd.pid
      argsfile    /usr/local/var/slapd.args

      loglevel    sync stats

      database    mdb
      suffix      "dc=suretecsystems,dc=com"
      directory   /usr/local/var/openldap-consumer/data

      maxsize         85899345920
      checkpoint      1024 5
```

```
    index       objectClass eq
    # rest of indexes
    index       default     sub

    rootdn          "cn=admin,dc=suretecsystems,dc=com"
    rootpw          testing

    # Let the replicator DN have limitless searches
    limits dn.exact="cn=replicator,dc=suretecsystems,dc=com" time.soft=unlimited time.hard=unlimited size.soft=unlimited size.hard=unlimited

    updatedn "cn=replicator,dc=suretecsystems,dc=com"

    # Refer updates to the provider
      updateref   ldap://localhost:9011

    database    monitor

    database    config
    rootpw          testing
```

Consumer Proxy that pulls in data via Syncrepl and pushes out via slapd-ldap

```
database        ldap
    # ignore conflicts with other databases, as we need to push out to same suffix
    hidden              on
    suffix          "dc=suretecsystems,dc=com"
    rootdn          "cn=slapd-ldap"
    uri             ldap://localhost:9012/

    lastmod         on

    # We don't need any access to this DSA
    restrict        all

    acl-bind        bindmethod=simple
                    binddn="cn=replicator,dc=suretecsystems,dc=com"
                    credentials=testing

    syncrepl        rid=001
                    provider=ldap://localhost:9011/
                    binddn="cn=replicator,dc=suretecsystems,dc=com"
                    bindmethod=simple
                    credentials=testing
                    searchbase="dc=suretecsystems,dc=com"
                    type=refreshAndPersist
                    retry="5 5 300 5"

    overlay         syncprov
```

390.2 (3) Securing the directory

Description: Candidates should be able to configure encrypted access to the LDAP directory, and restrict access at the firewall level.
Weight: 3

Key Knowledge Areas:

- Securing the directory with SSL and TLS
- Firewall considerations
- Unauthenticated access methods
- User / password authentication methods
- Maintanence of SASL user DB
- Client / server certificates

Terms and Utilities:

- SSL / TLS
- Security Strength Factors (SSF)
- SASL
- proxy authorization
- StartTLS
- iptables

Description

Securing with TLS / SSL

❏ TLS uses **X.509 certificates** to carry client and server identities. All servers are required to have valid certificates, whereas client certificates are optional. Clients must have a valid certificate in order to authenticate via SASL EXTERNAL.

❏ The DN of a **server certificate** must use the CN attribute to name the server, and the CN must carry the server's fully qualified domain name. Additional alias names and wildcards may be present in the subjectAltName certificate extension.

❏ The DN of a **client certificate** can be used directly as an authentication DN. Since X.509 is a part of the X.500 standard and LDAP is also based on X.500, both use the same DN formats and generally the DN in a user's X.509 certificate should be identical to the DN of their LDAP entry. However, sometimes the DNs may not be exactly the same, and so the mapping facility described in Mapping Authentication Identities can be applied to these DNs as well.

ldap / ldaps / starttls

- ❏ Slapd pot escoltar al port 389 LDAP, al port 636 LDAPS i a un socket unix. El servei es configura amb ldap:// ldaps:// ldapi://.

- ❏ The **LDAP Start TLS** operation is used in LDAP to initiate TLS negotiation. All OpenLDAP command line tools support a -Z and -ZZ flag to indicate whether a Start TLS operation is to be issued. The latter flag indicates that the tool is to cease processing if TLS cannot be started while the former allows the command to continue.

- ❏ STARTTLS is an extension to plain text protocols that allows for the encryption of the communication using the same port number as the standard, nonencrypted version of the protocol.

- ❏ In LDAPv2 environments, TLS is normally started using the LDAP Secure URI scheme (ldaps://) instead of the normal LDAP URI scheme (ldap://). OpenLDAP command line tools allow either scheme to used with the -H flag and with the URI ldap.conf(5) option.

Server Configuration

- ❏ **TLSCACertificateFile <filename>**
  This directive specifies the PEM-format file containing certificates for the CA's that slapd will trust. The certificate for the CA that signed the server certificate must be included among these certificates. If the signing CA was not a top-level (root) CA, certificates for the entire sequence of CA's from the signing CA to the top-level CA should be present. Multiple certificates are simply appended to the file; the order is not significant.

- ❏ **TLSCertificateFile <filename>**
  This directive specifies the file that contains the slapd server certificate. Certificates are generally public information and require no special protection.

- ❏ **TLSCertificateKeyFile <filename>**
  This directive specifies the file that contains the private key that matches the certificate stored in the TLSCertificateFile file. Private keys themselves are sensitive data and are usually password encrypted for protection. However, the current implementation doesn't support encrypted keys so the key must not be encrypted and the file itself must be protected carefully.

- ❏ **TLSVerifyClient { never | allow | try | demand }**
  This directive specifies what checks to perform on client certificates in an incoming TLS session, if any.

  - Never: This option is set to never by default, in which case the server never asks the client for a certificate.

- Allow: With a setting of allow the server will ask for a client certificate; if none is provided the session proceeds normally. If a certificate is provided but the server is unable to verify it, the certificate is ignored and the session proceeds normally, as if no certificate had been provided.

- Try: With a setting of try the certificate is requested, and if none is provided, the session proceeds normally. If a certificate is provided and it cannot be verified, the session is immediately terminated. With a setting of demand the certificate is requested and a valid certificate must be provided, otherwise the session is immediately terminated.

❏ The directives go into slapd.conf(5).

Client configuration

❏ Most of the client configuration directives parallel the server directives. The names of the directives are different, and they go into ldap.conf(5) instead of slapd.conf(5). Also, while most of these options may be configured on a system-wide basis, they may all be overridden by individual users in their .ldaprc files.

❏ Una part de les directives client van al ldap.conf però algunes han d'anar per força al fitxer de configuració local de l'usuari .ldaprc. És el cas per exemple de voler autenticar el client.

❏ **TLS_CACERT <filename>**
This directive specifies the PEM-format file containing certificates for the CA's that the client will trust. As noted in the TLS Configuration section, a client typically may need to know about more CAs than a server, but otherwise the same considerations apply.

❏ **TLS_REQCERT { never | allow | try | demand }**
This directive is equivalent to the server's TLSVerifyClient option. However, for clients the default value is demand and there generally is no good reason to change this setting.

❏ TLS_CERT <filename>
This directive specifies the file that contains the client certificate. **This is a user-only directive** and can only be specified in a user's .ldaprc file.

❏ TLS_KEY <filename>
This directive specifies the file that contains the private key that matches the certificate stored in the TLS_CERT file. The same constraints mentioned for TLSCertificateKeyFile apply here. This is also **a user-only directive**.

Security Strength Factors (SSF)

- **Data Integrity and Confidentiality Protection**:
  Transport Layer Security (TLS) can be used to provide data integrity and confidentiality protection in the communication process (TLS / SSL /StartTLS).
  Simple Authentication and Security Layer (SASL) mechanisms, such as DIGEST-MD5 and GSSAPI, also provide data integrity and confidentiality protection.

- The server uses **Security Strength Factors (SSF)** to indicate the relative strength of protection. A SSF of zero (0) indicates no protections are in place. A SSF of one (1) indicates integrity protection are in place. A SSF greater than one (>1) roughly correlates to the effective encryption key length. For example, DES is 56, 3DES is 112, and AES 128, 192, or 256.

- Security controls disallow operations when appropriate protections are not in place.

```
security ssf=1 update_ssf=112
```

  - requires integrity protection for all operations and encryption protection, 3DES equivalent, for update operations (e.g. add, delete, modify, etc.).

Exemple Access control basat en SSF

```
access to dn="cn=example,cn=edu"
        by * ssf=256 read
```

Altres directives slapd.conf basades en SSF

```
transport_ssf=<n>
    tls_ssf=<n>
    sasl_ssf=<n>
```

Firewall Considerations / iptables

- Slapd pot escoltar al port 389 LDAP, al port 636 LDAPS i a un socket unix.

- Exemples d’ordres per obrir ports per sessió o permanentment amb *firewall-cmd*

```
firewall-cmd --add-service=ldap
firewall-cmd --add-service=ldaps
```

```
firewall-cmd --permanent --add-service=ldap
firewall-cmd --permanent --add-service=ldaps
```

- Exemples amb *iptables*

```
iptables -I INPUT -p tcp --dport 389 -j ACCEPT
iptables -I INPUT -p tcp --dport 636 -j ACCEPT
```

- Exemple de selective listening

```
slapd -h ldap://127.0.0.1
slapd -h ldap://127.0.0.1 ldaps://192.168.1.34
```

- By default, slapd(8) will listen on both the IPv4 and IPv6 "any" addresses. It is often desirable to have slapd listen on select address/port pairs.

❑ Exemple de TCP Wrappers

```
slapd: 10.0.0.0/255.0.0.0 127.0.0.1 : ALLOW
slapd: ALL : DENY
```

- slapd(8) supports TCP Wrappers. TCP Wrappers provide a rule-based access control system for controlling TCP/IP access to the server.

Authentication methods: Simple

❑ Authentication methods can be: **Simple**, **SASL**.

❑ Simple authentication can be: **anonymous**, **unauthenticated**, and **user/password authenticated.**

[Anonymous]

❑ **Anonymous** access is requested by providing no name and no password to the "simple" bind operation. An anonymous bind results in an anonymous authorization association. Anonymous bind mechanism is enabled by default, but can be disabled by specifying "*disallow bind_anon*" in slapd.conf.

```
disallow bind_anon
allow bind_anon
```

❑ Disabling the anonymous bind mechanism does not prevent anonymous access to the directory. To require authentication to access the directory, one should instead specify "*require authc*".

[Unauthenticated]

❑ **Unauthenticated** access is requested by providing a name but no password. An unauthenticated bind also results in an anonymous authorization association. Unauthenticated bind mechanism is disabled by default, but can be enabled by specifying "*allow bind_anon_cred*" in slapd.conf.

```
allow bind_anon_cred
disallow bind_anon_cred
```

[Authenticated]

❑ **Authenticated access** (user/password authenticated) is requested by providing a valid name and password. A successful user/password authenticated bind results in a user authorization identity, the provided name, being associated with the session. User/password authenticated bind is enabled by default. The user/password authenticated bind mechanism can be completely disabled by setting "*disallow bind_simple*".

```
disallow bind_simple
allow bind_simple
```

- However, as this mechanism itself offers no eavesdropping protection (e.g., the password is set in the clear), it is recommended that it be used only in tightly controlled systems or when the LDAP session is protected by other means (e.g., TLS, IPsec).

- Using the security directive's *simple_bind option*, provides fine grain control over the level of confidential protection to require for simple user/password authentication. E.g., using *security simple_bind=56* would require simple binds to use encryption of DES equivalent or better (use of SSF).

  ```
  security simple_bind=56
  ```

- An unsuccessful bind always results in the session having an anonymous authorization association.

Authentication methods: SASL

- Authentication methods can be: Simple, **SASL**.

- Simple Authentication and Security Layer (SASL) framework. LDAP attempt to authenticate the user to the LDAP directory server using SASL by default. SASL offers many different authentication mechanisms.

- **PLAIN and LOGIN**, offer no greater security over LDAP simple authentication. Like LDAP simple authentication, such mechanisms should not be used unless you have adequate security protections in place.

- **CRAM-MD5** mechanism is deprecated in favor of DIGEST-MD5.

- **DIGEST-MD5** mechanism is the mandatory-to-implement authentication mechanism for LDAPv3. Prevents chosen plaintext attacks.

- **GSSAPI** mechanism utilizes GSS-API Kerberos V to provide secure authentication services.

- **EXTERNAL** mechanism utilizes authentication services provided by lower level network services such as Transport Layer Security (TLS). EXTERNAL can also be used with the ldapi:/// transport, as Unix-domain sockets can report the UID and GID of the client process.

SASL Proxy Authorization

- **Proxy authorization**, which allows an authenticated user to request that they **act on the behalf of another user**. This step occurs after the user has obtained an authentication DN, and involves sending an authorization identity to the server. This sort of service is useful when one entity needs to act on the behalf of many other users.

❏ The server will then make a decision on whether or not to allow the authorization to occur. If it is allowed, the user's LDAP connection is switched to have a binding DN derived from the authorization identity, and the LDAP session proceeds with the access of the new authorization DN.

❏ The SASL authorization identity is sent to the LDAP server via the -X switch or in the *authzid parameter. The identity can be in one of two forms, either:
u:<username>
dn:<dn>

❏ The decision to allow an authorization to proceed depends on the rules and policies. entries to allow authorization:
authzTo
authzFrom

```
dn: cn=WebUpdate,dc=example,dc=com
authzTo: ldap:///dc=example,dc=com??sub?(objectclass=person)
authzTo: dn.regex:^uid=[^,]*,dc=example,dc=com$
```

Password Storage

❏ LDAP passwords are normally stored in the userPassword attribute. Can be in plain text or hashed. Values of password attributes, regardless of storage scheme used, should be protected as if they were clear text. Hashed passwords are subject to dictionary attacks and brute-force attacks.

❏ The storage scheme is stored as a prefix on the value.The advantage of hashed passwords is that an attacker which discovers the hash does not have direct access to the actual password. Unfortunately, as dictionary and brute force attacks are generally quite easy for attackers to successfully mount, this advantage is marginal at best

❏ The userPassword attribute is allowed to have more than one value, and it is possible for each value to be stored in a different form. During authentication, slapd will iterate through the values until it finds one that matches the offered password or until it runs out of values to inspect.

❏ Schemes examples:

```
userPassword: {SSHA}DkMTwBl+a/3DQTxCYEApdUtNXGgdUac3
userPassword: {CRYPT}aUihad99hmev6
userPassword: {MD5}Xr4ilOzQ4PCOq3aQ0qbuaQ==
userPassword: {SMD5}4QWGWZpj9GCmfuqEvm8HtZhZS6E=
userPassword: {SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=
userPassword: {SASL}user@ad.example.com
```

Pass Through

- slapd has had the ability to delegate password verification to a separate process. so it can use any back-end server that Cyrus SASL supports for checking passwords. The choice is very wide, as one option is to use saslauthd(8) which in turn can use local files, Kerberos, an IMAP server, another LDAP server, or anything supported by the PAM mechanism.

- **Pass-Through** authentication works only with **plaintext passwords**, as used in the "simple bind" and "SASL PLAIN" authentication mechanisms.}}.

```
password-hash   {CLEARTEXT}
```

- Pass-Through authentication is selective: it only affects users whose userPassword attribute has a value marked with the "**{SASL}" scheme**. The format of the attribute is: *userPassword: {SASL}username@realm*

- The username and realm are passed to the SASL authentication mechanism and are used to identify the account whose password is to be verified. This allows arbitrary mapping between entries in OpenLDAP and accounts known to the backend authentication service. It would be wise to use access control to prevent users from changing their passwords through LDAP where they have pass-through authentication enabled (if not, they can become anyone).

- OpenLDAP delegates the whole process of validating that entry's password to Cyrus SASL.

Exemple de configuració a slapd.conf per usar SASL

```
mech_list: plain
 pwcheck_method: saslauthd
 saslauthd_path: /var/run/sasl2/mux
```

Exemple de configuració de saslauthd to delegate some or all authentication to another LDAP server

```
cat /usr/lib/sasl2/slapd.conf

 ldap_servers: ldap://dc1.example.com/ ldap://dc2.example.com/

 ldap_search_base: cn=Users,DC=ad,DC=example,DC=com
 ldap_filter: (userPrincipalName=%u)

 ldap_bind_dn: cn=saslauthd,cn=Users,DC=ad,DC=example,DC=com
 ldap_password: secret
```

```
# test
testsaslauthd -u user@ad.example.com -p userpassword
testsaslauthd -u user@ad.example.com -p wrongpasswor
```

```
#ldap user attribute
 userPassword: {SASL}user@ad.example.com
```

Configuration

Server configuration

```
TLSCACertificateFile <filename>
TLSCACertificatePath <path>

TLSCertificateFile <filename>
TLSCertificateKeyFile <filename>

 TLSVerifyClient { never | allow | try | demand }

TLSCipherSuite <cipher-suite-spec>
TLSRandFile <filename>
TLSDHParamFile <filename>
TLSECName <name>
```

Client configuration

```
TLS_CACERT <filename>
TLS_REQCERT { never | allow | try | demand }

TLS_CACERTDIR <path>

TLS_CERT <filename>
TLS_KEY <filename>

TLS_RANDFILE <filename>
```

Authentication examples

```
security ssf=1 update_ssf=112
access to dn="cn=example,cn=edu" by * ssf=256 read
transport_ssf=<n>
    tls_ssf=<n>
    sasl_ssf=<n>
security simple_bind=56

disallow bind_anon
allow bind_anon

allow bind_anon_cred
disallow bind_anon_cred

disallow bind_simple
allow bind_simple
```

Iptables / firewall

```
iptables -I INPUT -p tcp --dport 389 -j ACCEPT
iptables -I INPUT -p tcp --dport 636 -j ACCEPT

firewall-cmd --add-service=ldap
firewall-cmd --add-service=ldaps

firewall-cmd --permanent --add-service=ldap
firewall-cmd --permanent --add-service=ldaps

slapd -h ldap://127.0.0.1
slapd -h ldap://127.0.0.1 ldaps://192.168.1.34
```

390.3 OpenLDAP Server Performance Tuning

Weight: 2

Description: Candidates should be capable of measuring the performance of an LDAP server, and tuning configuration directives.

Key Knowledge Areas:

- Measure OpenLDAP performance
- Tune software configuration to increase performance
- Understand indexes

Terms and Utilities:

- index
- DB_CONFIG

Description

Indexes

- If you're searching on a filter that has been indexed, then the search reads the index and pulls exactly the entries that are referenced by the index. If the filter term has not been indexed, then the search must read every single entry in the target scope and test to see if each entry matches the filter. Obviously indexing can save a lot of work when it's used correctly.

- You should create indices to match the actual filter terms used in search queries. Each attribute index can be tuned further by selecting the set of index types to generate.

```
index cn,sn,givenname,mail eq
```

```
slapindex
```

- In the log messages pay attention to is:
  "<= bdb_equality_candidates: (foo) index_param failed (18)"
  That means that some application tried to use an equality filter (foo=<somevalue>) and attribute foo does not have an equality index. If you see a lot of these messages, you should add the index. If you see one every month or so, it may be acceptable to ignore it.

- Your slapd(8) should not be running (at least, not in read-write mode) when you do this to ensure consistency of the database.

- If a list of specific attributes is provided on the command line, only the indices for those attributes will be regenerated.

- All files eventually created by slapindex will belong to the identity slapindex is run as, so make sure you either run slapindex with the same identity slapd(8) will be run as (see option -u in slapd(8)), or **change file ownership** before running slapd(8).

Cache

- A cache is a block of memory for temporary storage of data likely to be used again".

- cachesize <integer>
  Specify the size in entries of the in-memory entry cache maintained by the bdb or hdb backend database instance. The default is 1000 entries.

- DB_CONFIG file

```
set_cachesize
set_lg_max

set_data_dir db
set_lg_regionmax 262144
set_lg_bsize 2097152
set_lg_dir logs
```

Questions & Answers

[Replication]

1. Which of the following configuration options enables an OpenLDAP server to act as a syncrepl provider?

   d) overlay syncprov

2. In the example below, what is the missing argument that is required to use secret as the password to authenticate the replication push with a slave directory server?

   ```
   replica uri=ldaps: //slave.example.com: 636
   binddn='cn=Replicator,dc=example,dc=com'
   bindmethod=simple _____________=secret
   ```

   c) credentials

3. In an OpenLDAP masters's slapd.conf configuration file, a replica configuration option is needed to enable a slave OpenLDAP server to replicate. What value is required in the following setting: bindmethod=____________ if using passwords for master/slave authentication? (Only specify the missing value)

   simple

4. It is found that changes made to an OpenLDAP directory are no longer being replicated to the slave server at 192.168.0.3. Tests prove that the slave server is listening on the correct port and changes are being recorded properly to the replication log file. In which file would you find the replication errors?

   c) 192.168.0.3: 389.rej

5. Which of the following parameters is used in the database on a slave server to direct clients that want to make changes to the OpenLDAP database to the master server?

   c) updateref

6. When configuring an OpenLDAP server to act as a proxy to a Microsoft Active Directory server, what is the correct database type for this stanza of the slapd.conf file?

   ```
   database _________
   suffix 'cn=users,dc=testcorp,dc=com'
   subordinate
   rebind-as-user
   uri 'ldap: //dc1.testcorp.com/'
   chase-referrals yes
   ```

   a) ldap

[Securing]

7. Which of the following statements are true regarding pass-through authentication in OpenLDAP? (Choose two.)

a) It only works with plaintext passwords.
c) it is indicated using the (SASL) scheme in a user's userPassword attribute.

8. An administrator has manually migrated local accounts to OpenLDAP, instead of using migration tools. When trying to authenticate as a user, an error is returned about invalid credentials. What is the most likely cause of this?
   a) The password hash type was not included in the user's password attribute.

9. OpenLDAP can be secured by which of these options? (Select THREE correct choices)
   a) TLS (Transport Layer Security)
   b) ACLs (Access Control Lists)
   d) SSL (Secure Sockets Layer)

10. Which of the following values for the option TLSVerifyClient instructs OpenLDAP to request a valid certificate from a client on order to serve the client's request and terminate the connection if the client does not provide a valid certificate?
    d) *demand*

11. In slapd.conf, what keyword will instruct slapd to not ask the client for a certificatE. TLSVerifyClient = ________
    a) never

12. The ________ command, included with OpenLDAP, will generate password hashes suitable for use in slapd.conf. (Enter the command with no options or parameters)
    slappasswd

13. Which of the following procedures will test the TLS configuration of an OpenLDAP server?
    a) Run the ldapsearch command with the -ZZ option, while watching network traffic with a packet analyzer.

14. When configuring OpenLDAP to use certificates, which option should be used with the TLSVerifyClient directive to ask the client for a valid certificate in order to proceed normally?
    d) demand

15. Below is an ACL entry from a slapd.conf file. Fill in the access control level setting to prevent users from retrieving passwords.
    none

[Performance]

16. Which of the following commands regenerates slapd indices based on the current database?
    c) slapindex

17. After modifying the indexes for a database in slapd.conf and running slapindex, the slapd daemon refuses to start when its init script is called. What is the most likely cause of this?

    a) The init script is starting slapd as an ordinary user, and the index files are owned by root.

18. Which of the following properties does the configuration option cachesize in slapd.conf refer to?

    a) The number of entries to be cached.

19. Which of the following parameters can be used in the file DB_CONFIG? (Select TWO correct answers.)

    a) set_cachesize
    e) set_lg_max

20. What does cachesize 1000000 represent in the slapd.conf file?

    a) The number of entries to be cached.

391. (4) OpenLDAP as an Authentication Backend

Contingut

Documentation

- Practical LPIC-3 300. Antonio Vazquez. Apress. 2019.
- Mastering Pluggable Authentication modules. Packt Publishing.
- DockerHub:
  - *Docker Hub edtasixm06/pam20*
  - *Docker Hub edtasixm11/k19*
- Apunts edt (Escola del Treball de Barcelona)
  - HowTo-ASIX-PAM
  - HowTo-ASIX-Kerberos

391.1 (2) LDAP Integration with PAM and NSS

Weight: 2

Description: Candidates should be able to configure PAM and NSS to retrieve information from an LDAP directory.

Key Knowledge Areas:

- Configure PAM to use LDAP for authentication
- Configure NSS to retrieve information from LDAP
- Configure PAM modules in various Unix environments

Terms and Utilities:

- PAM
- NSS
- /etc/pam.d/
- /etc/nsswitch.conf

PAM / NSS

❏ **pam_ldap.so** és el mòdul PAM per autenticar usuaris LDAP.

❏ Cal configurar nsswitch per permetre també la resolució de noms d’usuaris i grups LDAP afegint a l’entrada ldap.

```
passwd:    files ldap
shadow:    files
group:     files ldap
```

```
hosts winbind wins bcast host
```

❏ **authconfig** permet configurar l'autenticació d’usuaris del sistema i establir els paràmetres necessaris per accedir al servei LDAP.

```
authconfig  --enableshadow  --enablelocauthorize
            --enableldap --enableldapauth --ldapserver='ldap.edt.org' --ldapbase='dc=edt,dc=org'
             --enablemkhomedir --updateall
```

❏ També es pot utilitzar sssd com a supra servei que s'encarrega de gestionar tots els serveis implicats en l'autenticació.

```
cat /etc/sssd/sssd.conf
[domain/default]
autofs_provider = ldap
cache_credentials = True
ldap_search_base = ou=users,dc=linuxaholics,dc=com
id_provider = ldap
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldap://alpha.linuxaholics.com/
ldap_id_use_start_tls = True
```

```
ldap_tls_cacertdir = /etc/openldap/cacerts
[sssd]
config_file_version = 2
services = nss, pam, autofs
```

391.2 (2) Integrating LDAP with Active Directory and Kerberos

Weight: 2
Description: Candidates should be able to integrate LDAP with Active Directory Services.

Key Knowledge Areas:

- Kerberos integration with LDAP
- Cross platform authentication
- Single sign-on concepts
- Integration and compatibility limitations between OpenLDAP and Active Directory

Terms and Utilities:

- Kerberos
- Active Directory
- single sign-on
- DNS

Kerberos

❏ kinit / kadmin / kdb_util.

❏ authconfig inclement ldap i kerberos.

```
authconfig  --enableldap --enablekrb5 --ldapserver=alpha.linuxaholics.com
            --ldapbasedn="ou=users,dc=linuxaholics,dc=com"
            --enableldaptls --krb5adminserver="alpha.linuxaholics.com"
            --krb5kdc="alpha.linuxaholics.com" --krb5realm="EXAMPLE.COM" –update
```

❏ /etc/krb5.conf

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = EDT.ORG
# default_ccache_name = KEYRING:persistent:%{uid}

[realms]
EDT.ORG = {
  kdc = kserver.edt.org
  admin_server = kserver.edt.org
 }

[domain_realm]
.edt.org = EDT.ORG
edt.org = EDT.ORG
```

❏ Kerberos port 88.

- One of the most used **SSO** implementations is based on the use of Kerberos. After being granted a TGT, the user will be able to access any Kerberized application without needing to reauthenticate.

- **Single sign-on (SSO)** is an authentication procedure that grants or denies access to a series of related but independent software systems. The obvious advantage is that the users don’t need to authenticate against each and every software system they connect to; instead they authenticate against a common centralized authentication server.

DNS

- Windows Active Directory utilitza obligatòriament DNS per descobrir els serveis de kerberos i ldap. Tots els hosts han d’estar configurats per usar el servidor DNS del domini (el servidor ADS o una rèplica seva).

- El servidor pot tenir configurada la directiva forwarder per poder accedir a un servidor extern que realitzi la resolució de noms externs.

- El servei DNS ha de tenir dues entrades de tipus SRV que permeten identificar el host que ofereix el servei kerberos i el servei ldap.

```
_ldap._tcp.edt.org
_kerberos._udp.edt.org
```

- nmblookup

- samba-tool dns

Integration Windows

- A **domain** could be defined as a group of users, computers, and other network resources that are centrally managed.

- In Windows NT every domain controller kept a local copy of every network resource in the domain. This copy was replicated to every domain controller, but there could only be a single domain controller with write access to the domain registry. This domain controller was called the primary domain controller (PDC). The other domain controllers had read-only copies and they were called backup domain controllers (BDCs). When a client needed to read data from a domain controller, it could contact either the PDC or the BDC, but every time that a change was to be performed the PDC had to be contacted

Questions & Answers

[General]

1. When integrating Samba and OpenLDAP, what schema needs to be included in the OpenLDAP slapd.conf?

   a) samba.schema

2. How can the risk of UID/GID inconsistencies be avoided across UNIX/Linux systems that are sharing information over protocols other than SMB/CIFS (eg: NFS)?

   a) Specify a common OpenLDAP idmap backend in smb.conf.

3. A Samba server is configured to use the OpenLDAP password backend. The root DN for the LDAP directory is defined in slapd.conf. In order to define an alternative account used by the Samba administrator, which steps are necessary? (Select THREE correct answers.)

4. Which option for the pam_ldap module specifies a file from which the module's global settings can be read?

   a) config

5. A server is authenticating users using the pam_ldap module. Only users who are members of a certain group should be allowed to login. In which parameter in ldap.conf can a filter string be specified, that is ANDed with the login attribute when validating a user? (Enter only the parameter, without any options or values)

   a) pam_filter

[Integration]

6. By configuring Pluggable Authentication Module (PAM) and Name Service Switch (NSS) technologies to use OpenLDAP, what authentication service can be replaced?

   c) Network Information Service (NIS)

7. When configuring an OpenLDAP system for integration with PAM and NSS the /etc/nsswitch.conf file needs to be modified. Which of the following parameters completes this line from the /etc/nsswitch.conf file?

   b) ldap

8. Which mechanism of a Linux system is used by Samba to permit identity resolution within a domain?

   b) Name Service Switch (NSS)

9. Which of the following commands show all user accounts as they are currently available to the Linux operating system no matter of their source?

    b) getent

392. (11) Samba Basics

Continguts

- 392. (11) Samba Basics
  - 392.1 (2) Samba Concepts and Architecture
  - 392.2 (4) Configure Samba
  - 392.3 (2) Regular Samba Maintenance
  - 392.4 (2) Troubleshooting Samba
  - 392.5 (1) Internationalization

Documentació

- Samba wiki
- Using Samba, 3rd, O'Reilly & Associates (2007)
- DockerHub
  - DockerHub edtasixm06/samba19
- Apunts edt
  - HowTo-ASIX-Samba

392.1 (2) Samba Concepts and Architecture

Description: Candidates should understand the essential concepts of Samba. As well, the major differences between Samba3 and Samba4 should be known.
Weight: 2

Key Knowledge Areas:

- Understand the roles of the Samba daemons and components
- Understand key issues regarding heterogeneous networks
- Identify key TCP/UDP ports used with SMB/CIFS
- Knowledge of Samba3 and Samba4 differences

The following is a partial list of the used files, terms and utilities:

- /etc/services
- Samba daemons: smbd, nmbd, samba, winbindd

Samba daemons and components

- ❏ The **smbd** service is responsible for providing file sharing and printing services to clients using the SMB/CIFS protocol.

- ❏ The **nmbd** service provides name services based on NetBIOS.

- ❏ Finally, the **winbindd** service is used when we need to get information from Windows servers in a way that can be understood by Linux. This service is not included in a standard Samba server installation, and if we need it we'll have to install the samba-winbindd package with yum.

- ❏ The **smbd** service by default listens on ports TCP **445** and **139**. On the other hand, the **nmbd** service listens on ports UDP **137** and **138**.
  On port UDP 137 the NetBIOS Name Service listens. The NetBIOS Datagram listens on port UDP 138, and the NetBIOS Session Service listens on port TCP 139. Finally port TCP 445 is used by the SMB service.

- ❏ **Samba 3** could emulate a Windows NT BDC. In addition, we could create a member server (a server that is part of the domain but does not store a copy of the domain users database), or a stand-alone server (a server that is not part of a domain and uses only local users). It was not possible at all, however, to emulate an Active Directory domain controller.

- ❏ Samba 4 could emulate an Active Directory domain Controller. To do that, it combines several components:
  - An LDAP server.

- A Kerberos server.
- A dynamic DNS server.
- Remote procedure calls (RPCs).

Roles

- **Stand alone Server**. Server in a workgroup (not member of a domain). Has his own users and groups.
- **Domain member**. Server member of a domain. Obtains users and groups from de Domain Servers. It has to join the domain.
- **PDC** and **BDC**. **Primary Domain Controller** and **Backup Domain Controller**. Domain Controllers (primari and one or more backups) of a domain. Contain de users and groups and directives that rule the domain.
- **Active Directory Domain Controller**. (requires samba4). Primary server controller of a domain using Active Directory (ldap + kerberos + dns).

- **Master Browser**. Un servidor samba actua com a master browser si recull la informació de presencia de xarxa dels altres equips i s’encarrega de fer-la pública. Els controladors de domini **PDC/BDC** han d’actuar com a **master browser** i com a **logon domains**.
- **Wins server**. Un servidor actua com a servidor wins si té aquesta opció activada, i s’encarrega de la resolució de noms wins.

```
# ---------------------- Standalone Server Options -----------------------
# security = the mode Samba runs in. This can be set to user, share (deprecated), or
server (deprecated).
# passdb backend = the backend used to store user information in. New installations
should use either tdbsam or ldapsam. No additional configuration is required for tdbsam.
The "smbpasswd" utility is available for backwards compatibility.
	security = user
	passdb backend = tdbsam
```

```
# ---------------------- Domain Controller Options -----------------------
# security = must be set to user for domain controllers.
# passdb backend = the backend used to store user information in. New installations
should use either tdbsam or ldapsam. No additional configuration is required for tdbsam.
The "smbpasswd" utility is available for backwards compatibility.
# domain master = specifies Samba to be the Domain Master Browser, allowing Samba
to collate browse lists between subnets. Do not use the "domain master" option if you
already have a Windows NT domain controller performing this task.
# domain logons = allows Samba to provide a network logon service for Windows
workstations.
# logon script = specifies a script to run at login time on the client. These scripts must be
provided in a share named NETLOGON.
# logon path = specifies (with a UNC path) where user profiles are stored.
;	security = user
;	passdb backend = tdbsam
;	domain master = yes
;	domain logons = yes
	# the following login script name is determined by the machine name (%m):
```

```
;          logon script = %m.bat
           # the following login script name is determined by the UNIX user used:
;          logon script = %u.bat
;          logon path = \\%L\Profiles\%u
           # use an empty path to disable profile support:
;          logon path =
           # various scripts can be used on a domain controller or a stand-alone
           # machine to add or delete corresponding UNIX accounts:
;          add user script = /usr/sbin/useradd "%u" -n -g users
;          add group script = /usr/sbin/groupadd "%g"
;          add machine script = /usr/sbin/useradd -n -c "Workstation (%u)" -M -d /nohome -s
/bin/false "%u"
;          delete user script = /usr/sbin/userdel "%u"
;          delete user from group script = /usr/sbin/userdel "%u" "%g"
;          delete group script = /usr/sbin/groupdel "%g"
```

```
# ---------------------- Domain Members Options -----------------------
# security = must be set to domain or ads.
# passdb backend = the backend used to store user information in. New installations
should use either tdbsam or ldapsam. No additional configuration is required for tdbsam.
The "smbpasswd" utility is available for backwards compatibility.
# realm = only use the realm option when the "security = ads" option is set. The realm
option specifies the Active Directory realm the host is a part of.
# password server = only use this option when the "security = server" option is set, or if
you cannot use DNS to locate a Domain Controller. The argument list can include
My_PDC_Name, [My_BDC_Name], and [My_Next_BDC_Name]:
# password server = My_PDC_Name [My_BDC_Name] [My_Next_BDC_Name].
# Use "password server = *" to automatically locate Domain Controllers.
;          security = domain
;          passdb backend = tdbsam
;          realm = MY_REALM
;          password server = <NT-Server-Name>
```

```
# ---------------------- Browser Control Options ----------------------------
# local master = when set to no, Samba does not become the master browser on your
network. When set to yes, normal election rules apply.
# os level = determines the precedence the server has in master browser elections. The
default value should be reasonable.
# preferred master = when set to yes, Samba forces a local browser election at start up
(and gives itself a slightly higher chance of winning the election).
;          local master = no
;          os level = 33
;          preferred master = yes
```

```
#---------------------------- Name Resolution ------------------------------
# This section details the support for the Windows Internet Name Service (WINS).
# Note: Samba can be either a WINS server or a WINS client, but not both.
# wins support = when set to yes, the NMBD component of Samba enables its WINS
# server.
# wins server = tells the NMBD component of Samba to be a WINS client.
# wins proxy = when set to yes, Samba answers name resolution queries on behalf of a
non WINS capable client. For this to work, there must be at least one  WINS server on the
network. The default is no.
# dns proxy = when set to yes, Samba attempts to resolve NetBIOS names via DNS
# nslookups.
;	wins support = yes
;	wins server = w.x.y.z
;	wins proxy = yes
;	dns proxy = yes
```

Samba AD DC

```
$ cat /etc/samba/smb.conf
# Global parameters
[global]
	dns forwarder = 172.31.0.2
	netbios name = AD
	realm = EDT.ORG
	server role = active directory domain controller
	workgroup = EDT
	idmap_ldb:use rfc2307 = yes
	winbind enum users = yes
	winbind enum groups = yes
	template shell = /bin/bash
	template homedir = /home/%U

[sysvol]
	path = /var/lib/samba/sysvol
	read only = No

[netlogon]
	path = /var/lib/samba/sysvol/edt.org/scripts
	read only = No
```

Samba AD member

```
workgroup = VENTANAS
password server = yankee.ventanas.local
realm = VENTANAS.LOCAL
security = ads
idmap config * : range = 16777216-33554431
template shell = /bin/false
kerberos method = secrets only
winbind use default domain = false
winbind offline logon = false
```

392.2 (4) Configure Samba

Description: Candidates should be able to configure the Samba daemons for a wide variety of purposes.
Weight: 4

Key Knowledge Areas:

- Knowledge of Samba server configuration file structure
- Knowledge of Samba variables and configuration parameters
- Troubleshoot and debug configuration problems with Samba

Terms and Utilities:

- smb.conf
- smb.conf parameters
- smb.conf variables
- testparm
- secrets.tdb

Configuration structure

- [global] section describes the global configurations options.
- [share] each share has his own section describing his configuration options. There are shares for each file share, printers, etc. Especial shares are:
  - [homes]
  - [netlogons]
  - [profiles]
  - [printers]
- **testparm**. tesparm -v checks the validity of the configuration file **smb.conf**. Also shows the role of the server.

Configuration example [global]

```
[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        idmap config * : backend = tdb
        cups options = raw
```

```
[homes]
      comment = Home Directories
      valid users = %S, %D%w%S
      browseable = No
      read only = No
      inherit acls = Yes
[printers]
      comment = All Printers
      path = /var/tmp
      printable = Yes
```

```
    create mask = 0600
    browseable = No
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = @printadmin root
    force group = @printadmin
    create mask = 0664
    directory mask = 0775
[Docs]
    comment = Public documents
    path = /shared_docs
    public = yes
    writable = yes
    browseable = no
```

Security / Backend

- **Backend** indica el mecanisme a utilitzar per emmagatzemar els passwords. S'utilitza usualment **tdb** o **ldapsdam**.
- The passdb backend parameter specifies where the user information should be stored: either in a local database (tdbsam) or in LDAP (ldapsam).

- **TDB** correspon a la base de dades pròpia amb les eines tdb. **LDAPSAM** desa la informació de la base de dades de samba en una base de dades LDAP (que cal configurar 'populate' amb els elements pertinents necessaris per contenir les dades).

- The user and group information will be stored in the file **passdb.tdb**, located in /var/lib/samba/private.

- In this same location (/var/lib/samba/private) we can also find the **secrets.tdb** file, which stores internal settings such as the machine and domain SID, passwords used with LDAP, and so on.

- We store the LDAP password in secrets.tdb by using the smbpasswd command.

```
security = user
passdb backend = ldapsam:"ldap://alpha.linuxaholics.com"
ldap admin dn = cn=admin,dc=linuxaholics,dc=com

Now we can store the password in secrets.tdb.

[root@hotel ~]# smbpasswd -L -w admin
Setting stored password for "cn=admin,dc=linuxaholics,dc=com" in secrets.tdb
```

- Opcions de configuració de TLS per connectar amb el lDAp de ldapsam

```
ldap ssl = Off
tls enabled = No
tls cafile =
tls certfile =
tls keyfile =
```

- Ordres:
    - smbpasswd
    - pdbedit
    - Net getlocalsid

392.3 (2) Regular Samba Maintenance

Description: Candidates should know about the various tools and utilities that are part of a Samba installation.
Weight: 2

Key Knowledge Areas:

- Monitor and interact with running Samba daemons
- Perform regular backups of Samba configuration and state data

Terms and Utilities:

- smbcontrol
- smbstatus
- tdbbackup

❏ **smbcontrol**. One of the utilities to monitor Samba.

```
# smbcontrol smbd debuglevel
PID 12339: all:0 tdb:0 printdrivers:0 lanman:0 smb:0 rpc_parse:0 rpc_srv:0
rpc_cli:0 passdb:0 sam:0 auth:0 winbind:0 vfs:0 idmap:0 quota:0 acls:0
locking:0 msdfs:0 dmapi:0 registry:0 scavenger:0 dns:0 ldb:0 tevent:0
auth_audit:0 auth_json_audit:0 kerberos:0 drs_repl:0

# smbcontrol smbd debug 3
smbcontrol smbd ping
smbcontrol nmbd ping
smbcontrol winbindd ping
```

❏ **smbstatus**. Shows statistics about the shared resources.

❏ **tdbbackup**. tool to back up Samba TDB files included in the tdb-tools package. Also check the integrity of those files. There are multiple locations with tdb files. Generates a .bak file for each one.

```
# tdbbackup /var/lib/samba/private/passdb.tdb
# tdbbackup -l /var/lib/samba/*.tdb

s /var/lib/samba/private/
msg.sock  passdb.tdb  passdb.tdb.bak  secrets.tdb
```

❏ **tdbrestore**. Restores tdb backup files. Its needed de dumb contents of the backup, not the backup file itself.

```
Usage: tdbrestore dbname < tdbdump_output
tdbrestore passdb.tdb < dumpfile
```

❏ **tdbdump**. dump the contents of the backup file.

```
tdbdump passdb.tdb.bak > dumpfile
```

392.4 (2) Troubleshooting Samba

Weight: 2

Description: Candidates should understand the structure of trivial database files and know how troubleshoot problems.

Key Knowledge Areas:

- Configure Samba logging
- Backup TDB files
- Restore TDB files
- Identify TDB file corruption
- Edit / list TDB file content

Terms and Utilities:

- /var/log/samba/
- log level
- debuglevel
- smbpasswd
- pdbedit
- secrets.tdb
- tdbbackup
- tdbdump
- tdbrestore
- tdbtool

❏ **logging**

```
log file = /var/log/samba/log.%m
max logsize = 50
log level = 4 passdb:5
# debuglevel = 4 passdb:5
syslog = 1 #num of syslog facility
```

❏ **debug**

```
# smbcontrol smbd debuglevel
PID 12339: all:0 tdb:0 printdrivers:0 lanman:0 smb:0 rpc_parse:0 rpc_srv:0
rpc_cli:0 passdb:0 sam:0 auth:0 winbind:0 vfs:0 idmap:0 quota:0 acls:0
locking:0 msdfs:0 dmapi:0 registry:0 scavenger:0 dns:0 ldb:0 tevent:0
auth_audit:0 auth_json_audit:0 kerberos:0 drs_repl:0

# smbcontrol smbd debug 3
smbcontrol smbd ping
smbcontrol nmbd ping
smbcontrol winbindd ping
```

❏ **tdbbackup**. tool to back up Samba TDB files included in the tdb-tools package. Also check the integrity of those files. There are multiple locations with tdb files. Generates a .bak file for each one.

```
# tdbbackup /var/lib/samba/private/passdb.tdb
# tdbbackup -l /var/lib/samba/*.tdb
```

```
s /var/lib/samba/private/
msg.sock  passdb.tdb  passdb.tdb.bak  secrets.tdb
```

- tdbackup also **checks** the validity of the files with the -v option. If there is a corruption and a file backup exists, it regenerates de file.

```
tdbbackup -v passdb.tdb
restoring passdb.tdb
```

- **tdbrestore**. Restores tdb backup files. Its needed de dumb contents of the backup, not the backup file itself.

```
Usage: tdbrestore dbname < tdbdump_output
tdbrestore passdb.tdb < dumpfile
```

- **tdbdump**. dump the contents of the backup file.

```
tdbdump passdb.tdb.bak > dumpfile
```

- **tdbtool**. Utility to tdb files. This utility can be used to create and manipulate the contents of TDB files.

```
tdbtool passdb.tdb dump
tdbtool passdb.tdb info
tdbtool passdb.tdb check
tdbtool passdb.tdb erase
```

392.5 (1) Internationalization

Weight: 1

Description: Candidates should be able to work with internationalization character codes and code pages.

Key Knowledge Areas:

- Understand internationalization character codes and code pages
- Understand the difference in the name space between Windows and Linux/Unix with respect to share, file and directory names in a non-English environment
- Understand the difference in the name space between Windows and Linux/Unix with respect to user and group naming in a non-English environment
- Understand the difference in the name space between Windows and Linux/Unix with respect to computer naming in a non-English environment

Terms and Utilities:

- internationalization
- character codes
- code pages
- smb.conf
- dos charset, display charset and unix charset

Charset

- **dos charset**: This is the charset Samba uses when talking to DOS clients. If the configured value is not available, Samba will fall back to ASCII.

- **unix charset**. This is the charset used by the operating system. In modern versions this is usually UTF-8, which covers all characters in all languages.

```
dos charset = CP850
unix charset = UTF-8
```

- **Unicode**. Starting with Samba 3.0, unicode support was added for filenames and other text containing characters in international character.

- By default, Samba tries to automatically detect the correct character set to use with a connecting client. The *ASCII = yes* parameter in smb.conf forces Samba to use only ASCII.

Questions & Answers

[392.1 Samba Concepts and Architecture]

1. After installing a network with one Samba server and several clients, users are complaining that they receive an Unable to browse the network error when trying to visit a public share. What is the most likely cause of this?

   The nmbd process is not running on the Samba server.

2. Which service unifies Linux/UNIX and Windows NT account management by allowing a UNIX box to become a full member of an NT domain?

   winbind

3. Which mechanism of a Linux system is used by Samba to permit identity resolution within a domain?

   Name Service Switch (NSS)

4. What must be done to ensure the Samba password is kept synchronized when a user changes their Linux password?

   pam_smbpass.so should be added to the password type of the appropriate PAM configuration.

5. What following statement is true about Samba 4?

   Samba 4 can serve as an Active Directory Domain Controller.

6. Which of the following daemons are included in Samba 3? (Select THREE correct answers.)

   winbind
   smbd
   nmbd

[392.2 Configure Samba]

7. Which directive of the smb.conf file will ensure a Samba server will win broadcast elections for the master browser?

   os level = 255

8. By specifying the __________ option in smb.conf and assigning it an appropriate value, Samba will create Machine Trust Accounts automatically when the client joins the domain.

   add machine script

9. In which section of the smb.conf configuration file is the logon script file name specified?

   [global]

10. Which parameter in the smb.conf defines how long the winbind daemon will cache user and group information?

    winbind cache time

11. To minimally configure Samba to publish event logs, the eventlogs to list must be specified in smb.conf. What is the directive in the smb.conf file to enable event logs and list which eventlogs to publish?

    eventlog list

12. Which parameter must be set in the [global] section of smb.conf in order to make Samba use printers managed by CUPS?

    printcap = cups

13. Which of the following are correct values for boolean parameters in smb.conf? (Select THREE correct answers.)

    1
    true
    no

14. In order to restrict access to the SMB (445/tcp) port and stop the use of NetBIOS (139/tcp), what parameter is required in smb.conf in Samba 3?

    smb ports = 445

15. There are multiple network interfaces on a server. Which parameters must you set in smb.conf to limit which interfaces Samba will accept connections? (Choose TWO correct answers.)

    bind interfaces only
    interfaces

16. Specify one of the commands that can be used to check a Samba configuration file for syntactical correctness? (Specify only the command name without any parameters or path.)

    testparm samba-tool

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

    testparm

18. Which parameter in smb.conf defines the directory containing secrets.tdb?

    private dir

19. Which of the following Samba variables must be used to pass the machine name to the script specified in add machine script within a Samba configuration file?

    %u

20. What is stored in the secrets.tdb database file?

    The SID of the local machine.

[392.3 Regular Samba Maintenance]

21. Which commands can be used to terminate all running instances of smbd?

    smbcontrol smbd shutdown

22. Which type of message should be sent to a Samba daemon using smbcontrol in order to change the daemon's debug level? (Specify ONLY the name of the message type without command or options.)

    debug

23. Which command in the Samba suite will list the current connections?

    smbstatus

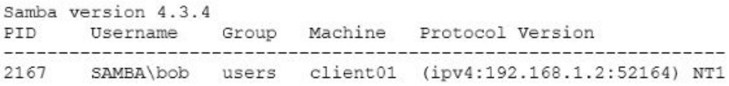
24. Which type of files will be stored inside the directory specified below?
    # smbd -b |grep LOCKDIR
    LOCKDIR: /var/cache/samba

    TDB files

25. Which command can be used to validate and backup a TDB file?

    tdbbackup

26. What samba command generates the following output? (Specify ONLY the command without any path or parameters.)



```
Samba version 4.3.4
PID     Username    Group   Machine   Protocol Version
------------------------------------------------------------------
2167    SAMBA\bob   users   client01  (ipv4:192.168.1.2:52164) NT1
```

smbstatus

[392.4 Troubleshooting Samba]

27. Which command can be used to validate and backup a TDB file?

    tdbbackup

28. Which commands will dump out the contents of a Samba printer driver's TDB file? (Select TWO correct answers.)

    tdbtool dump
    tdbdump

29. Which parameter in smb.conf defines the directory containing secrets.tdb?

    private dir

30. Sending a message of type ________ to a Samba daemon using smbcontrol changes the daemon's debug level. (Only specify the name of the message type without command or options)

    debug

31. In order to generate individual logfiles for machines connecting to Samba, which of the following statements have to be used in the Samba configuration file?

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

32. The log level parameter in smb.conf should normally not be set higher than 2 becausE.

    the server flushes the log file after each operation, which affects overall performance.

33. Which of the following commands converts user accounts from the smbpasswd to the passdb.tdb backend?

    pdbedit --i smbpasswd:smbpasswd --e tdbsam:passdb.tdb

34. Which parameter in the smb.conf defines how long the winbind daemon will cache user and group information?

    winbind cache time

35. To minimally configure Samba to publish event logs, the eventlogs to list must be specified in smb.conf. What is the directive in the smb.conf file to enable event logs and list which eventlogs to publish?

    eventlog list

[392.5 Internationalization]

36. By default Samba tries to recognize correct charsets between server and client. Which parameters can be used in smb.conf to set them manually? (Choose TWO correct answers)

    unix charset

    dos charset

37. By default, Samba tries to automatically detect the correct character set to use with a connecting client. Which parameter in smb.conf forces Samba to use only ASCII?

    ASCII = yes

38. Starting with Samba 3.0, what support was added for filenames and other text containing characters in international character sets?

    unicode

393. (9) Samba Share Configuration

Continguts

393.1 (4) File Services

Description: Candidates should be able to create and configure file shares in a mixed environment.
Weight: 4

Key Knowledge Areas:

- Create and configure file sharing
- Plan file service migration
- Limit access to IPC$
- Create scripts for user and group handling of file shares
- Samba share access configuration parameters

Terms and Utilities:

- smb.conf
- [homes]
- smbcquotas
- smbsh
- browseable, writeable, valid users, write list, read list, read only and guest ok
- IPC$
- mount, smbmount

❏ **smbcquotas**. can be used to manage quotas in a Samba share. For this to work, the file system the share resides on must be mounted with quota support. If that's the case we can list the quotas with the -L parameter.

```
smbcquotas -V
smbcquotas -L
smbcquotas -S UQLIM:root:10000000/20000000 //127.0.0.1/infoquota
smbcquotas -v -L //127.0.0.1/infoquota
```

❏ **IPC$** is a special share used by Windows (and Samba) for inter-process communication with Remote Procedure Call (RPC). The client connecting can perform a series of actions on the server, like listing users, listing shares, and so on. Nevertheless IPC$ can also be used by hackers to create an anonymous connection and get information about the server. To minimize this risk, we can add an [IPC$] entry to the /etc/samba/smb.conf file and add the following access list.

```
[IPC$]
hosts allow = 192.168.1.0/24 127.0.0.1
hosts deny = 0.0.0.0/0
```

Examples

```
path = /dir1/dir2/share
comment = share description
volume = share name
browseable = yes/no
```

```
max connections = #

public = yes/no
guest ok = yes/no
guest account = unix-useraccount
guest only = yes/no

valid users = user1 user2  @group1 @group2 …
invalid users = user1 user2  @group1 @group2 …
auto services = user1 user2  @group1 @group2 …
admin users = user1 user2  @group1 @group2 …

writable = yes/no
read only = yes/no
write list = user1 user2  @group1 @group2 …
read list = user1 user2  @group1 @group2 …

create mode = 0660
directory mode = 0770
```

```
[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        browseable = No
        read only = No
        inherit acls = Yes
```

```
[Docs]
comment = Public documents
path = /shared_docs
public = yes
writable = yes
```

```
[accounting]
    comment = Accounting Department Directory
    writable = yes
    valid users = @account
    path = /home/samba/accounting
    create mode = 0660
    directory mode = 0770
```

```
[global]
    invalid users = root bin daemon adm sync shutdown halt mail news uucp operator
    auto services = dave peter bob

[homes]
    browsable = no
    writable = yes

[sales]
        path = /home/sales
        comment = Sedona Real Estate Sales Data
        writable = yes
        valid users = sofie shelby adilia
        admin users = mike

[salesbis]
        path = /home/sales
        comment = Sedona Real Estate Sales Data
        read only = yes
        write list = sofie shelby
```

```
mount -t cifs -o username=Antonio //hotel.linuxaholics.com/ Docs /mnt/samba_hotel/
```

Migrate

```
net rpc info -S hotel.linuxaholics.com -U avazquez
net rpc share list -S hotel.linuxaholics.com -U avazquez
net rpc share migrate all -S hotel.linuxaholics.com -U avazquez

net user
net localgroup
net share

net rpc rights list privileges SeDiskOperatorPrivilege -U Antonio
net rpc rights grant "Antonio" SeDiskOperatorPrivilege -U "Antonio"
```

Scripts users & groups

- Users must exist in Samba as in the operating system itself. When using the tdbsam back end, if we try to add a Samba user who doesn’t exist in Linux, we get an error. However, if we use the ldapsam back end we could have a Samba user without the corresponding Linux user.

- **add user script**. instruct the samba service to automatically create the Linux user as soon as he or she connects to a Samba share. This can be done with the add user script global parameter, which by default has no value.

```
add user script =
add user script = /usr/local/samba/bin/add_user %u
```

- **add group script**. Idem to create groups.
  add user to group script.

```
add group script = /usr/sbin/groupadd %g
```

Share options...

```
hosts allow = 192.168.1.229
hosts deny = 192.168.1.229

public = yes
writable = yes
browseable = yes
guest ok = yes

read only = no
writable = yes

valid users = Isabel, Rosalia
read list = bob, alice
write list = marta
```

393.2 (3) Linux File System and Share/Service Permissions

Description: Candidates should understand file permissions on a Linux file system in a mixed environment.
Weight: 3

Key Knowledge Areas:

- Knowledge of file / directory permission control
- Understand how Samba interacts with Linux file system permissions and ACLs
- Use Samba VFS to store Windows ACLs

Terms and Utilities:

- smb.conf
- chmod, chown
- create mask, directory mask, force create mode, force directory mode
- smbcacls
- getfacl, setfacl
- vfs_acl_xattr, vfs_acl_tdb and vfs objects

Linux ACLs

- Access lists give us a finer level of control over the permissions. Get its associated access list with the **getfacl** command. the **setfacl** command we can grant permissions.

```
setfacl -m u:rrey:rw example.txt
getfacl example.txt
```

- Samba executes on top of the Linux file system, it relies on Linux file system permissions to work properly.
  És un sistema de dues portes o dos permisos, samba ha de permetre l'accés (sigui lectura, escriptura, execució) però llavors per sota linux també hi ha de permetre.

- **create mask**. **create mode**. If we want to modify the default permissions a file has when it is created from Samba, we'll need to modify the create mask parameter (or its synonym create mode). Als permisos indicats se li aplica la protecció de linux d'eliminar el permís d'execució als fitxers (011). Si es vol forçar que els permisos siguin exactament els indicats cal usar el paràmetre **force create mode**.

```
create mask = 0644

force create mode = 0775
```

- **directory mask**. We can assign new default permissions with the directory mask option. A diferència del que passa amb els fitxers aplica els permisos indicats (sense desactivar la x). També existeix **force create mode**.

```
directory mask = 0744
```

Samba VFS

- **Samba VFS** extends the functionality of Samba in many useful ways. Some of the advantages of using VFS are implementing file auditing or storing Windows ACLs.

- Windows systems allow the sysadmin to audit certain events, such as creating and deleting files or folders, modifying permissions, and so on. We can implement the same functionality with VFS modules.

```
[global]
vfs objects = audit
audit:facility = local3
audit:priority = info
```

- To enable the the support of extended ACL in our Samba server we could use two different VFS modules: **vfs_acl_xattr** and **vfs_acl_tdb**. The first one stores the ACLs in the file extended attributes, whereas the second one keeps that information in the file_ntacls.tdb file. if we're working with a Samba domain controller, these parameters are automatically set.

```
[global]
vfs objects = audit, acl_xattr
map acl inherit = yes
store dos attributes = yes
```

-
- x

393.3 (2) Print Services

Description: Candidates should be able to create and manage print shares in a mixed environment.
Weight: 2

Key Knowledge Areas:

- Create and configure printer sharing
- Configure integration between Samba and CUPS
- Manage Windows print drivers and configure downloading of print drivers
- Configure [print$]
- Understand security concerns with printer sharing
- Uploading printer drivers for Point'n'Print driver installation using 'Add Print Driver Wizard' in Windows

Terms and Utilities:

- smb.conf
- [print$]
- CUPS
- cupsd.conf
- /var/spool/samba/.
- smbspool
- rpcclient
- net

❏ **[printers]**. By default, Samba allows us to share printers with any Samba client. For that purpose, there is a share named [printers] defined in /etc/samba/smb.conf. The option printable = yes means that the clients can open and send files to the spool directory specified in path.

```
[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        guest ok = no
        writable = no
        printable = yes
```

❏ **printing = cups**. Samba can integrate with different printing systems like LPD, which were widely used in Linux before CUPS gradually replaced them. We can determine which printing system to use with the parameter printing. Depending on the value of the parameter **load printers**, the printers defined in CUPS may be shared automatically in Samba.

```
printing = cups
load printers = Yes
```

❑ **Definició propia** d'una impressora. Es poden definir individualment les impressores que es volguin en lloc d'usar el recurs global printers.

```
[Samba_Printer]
    comment = Public printer
    path = /var/spool/samba
    guest ok = Yes
    printable = Yes
    printer name = printer_Canon
```

```
smbcontrol smbd reload-printers
```

❑ The tdb back end we are currently using stores the printer-related information in the /var/lib/samba/printing/ folder, as well as in the /var/lib/samba/printer_list.tdb file. In the /var/lib/samba/printing/ folder we'll see a tdb file for every printer defined in Samba.
The *ntprinters.tdb* and *ntdrivers.tdb* files used in previous versions of Samba are no longer used.

```
ls -l /var/lib/samba/printing/
1 root Antonio 28672 ago 16 05:24 printer_Canon.tdb
1 root root    28672 ago 13 19:40 printers.tdb
1 root Antonio 28672 ago 16 06:15 Samba_Printer.tdb
```

❑ Options

```
printing = CUPS
load printers = yes

cups encrypt = yes

enable spoolss
disable spoolss
```

❑ **[print$]**. Windows printers. What happens when we connect from a Windows client to a shared Windows printer is that the client will try and download the needed drivers to install the new printer. We can mimic this same behavior in our Samba server with a few configuration changes.
Windows clients download the print drivers automatically from a share named print$. This behavior is hard-coded in every Windows box and it cannot be changed.

```
[print$]
    comment = Printer Drivers
    create mask = 0664
    directory mask = 0775
    force group = @printadmin
    path = /var/lib/samba/drivers
    write list = @printadmin root
```

❑ Inside the path of the [print$] share we need to create a series of subfolders (IA64 W32ALPHA W32MIPS W32PPC W32X86 WIN40 x64) **We copy the drivers for each OS in the corresponding folder**. The driver should be uncompressed to be downloaded by the clients.

❑ **Point and Print**. This feature allows a user to create a connection to a remote printer without providing disks or other installation media. All the necessary files and information are downloaded from the print server automatically.

❑ **We need to associate the Samba printer with the right driver**.

❑ **smbspool** is used to send a print file to an SMB printer.

- **rpcclient**. This tool was developed to test MS-RPC functionality in Samba. It is very easy to execute and the only mandatory argument is the NetBIOS of the Samba server to which we are connecting. Nevertheless, if NetBIOS name resolution isn't working properly, we can force the utility to connect to a certain IP by using the -I parameter, in this case the NetBIOS server name is ignored.

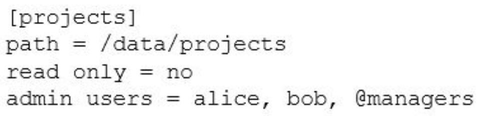
  ```
  rpcclient -I 127.0.0.1  -U Antonio hotel
  rpcclient $> srvinfo
  rpcclient $> netshareenum
  rpcclient $> netsharegetinfo Demo
  rpcclient $> queryuser antonio
  rpcclient $> enumprinters
  ```

Questions & Answers

[393.1 File Services]

1. What is true about the following share's access properties? (Choose TWO correct answers.)
   [projects]
   path = /data/projects
   read only = no
   admin users = timo, taki, @managers
   ** The timo and taki users can manipulate files regardless of the file system permissions.*
   ** @managers will be resolved as a Unix group.*

2. What is the true of the following share's access properties? (Choose two.)



```
[projects]
path = /data/projects
read only = no
admin users = alice, bob, @managers
```

   @managers will be resolved as a Unix group.

3. On Microsoft Windows systems, ACLs on the share are set using tools like the Explorer. For example, in Windows 7, right-click on the shared folder, then select Sharing, then click on Permissions. What Windows group, by default, has full control of the share?
   Everyone

4. Which of the following options can be used to limit access to a share? (Select TWO correct answers)
   write list
   valid users

5. What is true regarding the users listed in the option write list in a share declaration?
   Given sufficient Linux file system permissions, all users listed in the write list are allowed to write to the share.

6. The [homes] section of smb.conf contains the parameter browseable = no. What are the resulting consequences? (Select TWO correct answers)
   ** When browsing the Samba server, there is no visible share called homes.*
   ** The homes share can be directly accessed by specifically opening this share by its UNC path.*

7. What is true about the [homes] section in smb.conf?
   It is a template used for all home directories of users on the Samba server.

8. It is desired to restrict access to the IPC$ share to one specific machine. The setting hosts allow = 192.168.0.3 is added to the share configuration. Later it is discovered that other workstations may still access it. What setting was forgotten in the share configuration?

   hosts deny = 0.0.0.0/0

9. An anonymous user had her access denied while she was trying to access a Samba share using the smbclient command. Assuming that it is necessary for anonymous users to access that share, what must be configured (in the Samba configuration file) to allow access? Please specify the full directive and value.

   guest ok = yes, guest ok=yes, guest ok= yes, guest ok =yes, guest ok = 1, guest ok=1, guest ok =1, guest ok= 1, guest ok = true, guest ok=true, guest ok= true, guest ok =true

10. Which of the following parameters can be used in a Samba configuration in order to execute scripts on the server? (Choose three.)

    add user script
    add group script
    add user to group script

11. Which Samba command allows the management and manipulation of NT Quotas on samba file shares? (Specify ONLY the command without any path or parameters.)

    smbquotas

[393.2 Linux File System and Share/Service Permissions]

12. What is true about the Samba configuration options create mask?

    Each permission bit that is cleared (0) in create mask is always cleared on a file created by Samba even if the client explicit sets the bit.

13. Which of the following Samba VFS modules can be used to store Windows ACLs?

    vfs_acl_tdb
    vfs_acl_xattr

14. In the smb.conf, what is the numeric value for the directory mask directive to ensure directories created within a share will have full permissions for all users?

    0777

15. Which command displays the Unix access control list of the file Company.qbd?

    getfacl Company.qdb

16. The ______________ parameter in the smb.conf file will set hidden files in Linux to also be hidden in windows. (Please specify ONLY the parameter with no value assignment.)

    hide dot files

17. Microsoft file systems are not case sensitive on file names. Linux file systems are case sensitive to file names. Which of the following directives defines how Samba handles file name mapping in this situation?

    case sensitive

[393.3 Print Services]

18. When preparing the delivery of printer drivers from Samba to Windows clients, which of the following requirements have to be fulfilled? (Select TWO correct answers.)

    ** The driver must be associated with the printer either by Samba's rpcclient command or by the Windows Add Printer wizard.*

    ** The driver has to be put on a Samba share called print$.*

19. Which files store printer and driver properties created on the server?

    ntprinters.tdb and ntdrivers.tdb

20. The _________ parameter in smb.conf limits the maximum number of jobs allowed in a Samba printer queue at any given moment.

    max print jobs

21. How is the user user01 from DOMA granted the right to manage printers on a Samba print server?

    net -S server -U domadmin rpc rights grant 'DOMA\user01' SePrintOperatorPrivilege

22. Which of the following sections must exist in a Samba configuration file in order to create dynamic shares for printers?

    [printers]

23. Which parameter must be set in the [global] section of smb.conf in order to make Samba use printers managed by CUPS?

    printcap = cups

394. (9) Samba User and Group Management

Continguts

394.1 (4) Managing User Accounts and Groups

Description: Candidates should be able to manage user and group accounts in a mixed environment.
Weight: 4

Key Knowledge Areas:

- Manager user and group accounts
- Understand user and group mapping
- Knowledge of user account management tools
- Use of the smbpasswd program
- Force ownership of file and directory objects

Terms and Utilities:

- pdbedit
- smb.conf
- samba-tool user (with subcommands)
- samba-tool group (with subcommands)
- smbpasswd
- /etc/passwd
- /etc/group
- force user, force group.
- idmap

smbpasswd

- ❏ **smbpasswd**. create users. It can be executed without parameters by normal users to change their Samba passwords. The command works by connecting to the SMB service, so we must make sure that this one is running; otherwise, the command will fail. It can also be executed on remote systems by providing the -r parameter. We can also specify the remote user whose password we want to change with the -U parameter.

```
smbpasswd -a pere
smbpasswd pere
smbpasswd
smbpasswd -d pere
smbpasswd -x pere

smbpasswd -r 192.168.56.102 -U Antonio
```

- ❏ Usar com a root **-a** per crear (afegir) **-x** per eliminar, **-d** per disable. Sense argument per canviar el passwd.

pdbedit

- **pdbedit**. This tool can only be executed by root.

```
pdbedit -L -v
pdbedit -a -u jdoe
pdbedit -x jdoe

pdbedit -u jdoe -c "[D ]"   # disable user
pdbedit -u jdoe -c "[X ]"   #passwd no expires
pdbedit -u jdoe jdoe -c "[ ]"  # re enable
```

samba-tool

- **samba-tool**. smbpasswd and pdbedit are used to manage local users, but if we want to manage Samba Active Directory users and groups, we'll need to use the samba-tool command.

```
samba-tool user create Jose
samba-tool user edit Jose
samba-tool user disable Jose
samba-tool user enable Jose
samba-tool user delete Jose
```

- Samba-tool can be also used to manage groups.

```
samba-tool group list
samba-tool group listmembers

samba-tool group addmembers group-name user-name...
samba-tool group removemembers group-name user-name…

samba-tool group add "Permanent Staff"
samba-tool group delete "Permanent Staff"
```

Users & Group Mapping

- That is, there is a mapping between the Linux user and the Samba user. By default, a stand-alone Samba server maps any Samba user with the corresponding Linux user of the same name.

If we execute the smbstatus command on the Samba server, we'll see that the user has been mapped to the Linux user avazquez as well.

```
[root@hotel ~]# smbstatus
Samba version 4.1.1
PID     Username      Group     Machine
-------------------------------------------------------------------
16868   avazquez      avazquez   192.168.56.101 (ipv4:192.168.56.101:34886)
```

- If we want to map the Samba user to a specific Linux user we'll create a text file mapping. Then configure the **username map** option.

```
linux -name = samba-name
```

```
[global]
username map = /var/lib/samba/usersmap.txt
```

- Instead of the username map option, we could have used the similar **username map script** option, which points to the full path to a program or script that receives the invoking username as the input value and returns the Linux user it should be mapped to.

- **idmap**. It is the mapping between Windows SIDs and Linux user and group IDs.

```
idmap config * : backend = ldap:"ldap://alpha.linuxaholics.com"
idmap config * : range = 5000-50000
```

```
Deprecated:
  idmap backend = ldap:"ldap://alpha.linuxaholics.com"
  idmap uid = 5000-50000
  idmap gid = 5000-50000
```

- **guest**. A special type of user mapping concerns the Guest user. Historically, Windows systems have included a special account called Guest to grant limited rights to any unknown user. In Samba this account is mapped by default to the Linux account nobody (**guest account = nobody**). It is possible to change this mapping by manually specifying a different user, although is not advisable to do so.

- **map to guest**. Depending on the value of this parameter, Samba will behave differently:
  - Never: In this case any login with an invalid password is rejected.
  - Bad User: User logins with an incorrect password will be rejected, unless the username doesn’t exist, in which case it will be mapped to the guest account.
  - Bad Password: User logins with incorrect passwords are treated as guest logins. This can be confusing, as a user might not be aware of the incorrect password and will probably not understand why they cannot access resources they normally can.
  - Bad uid: Only applicable when Samba is integrated in a domain.

- **net groupmap**. In addition to map users, Samba also maps Linux and Unix group IDs to Windows SIDs. This can be done with the net groupmap command.

Forcing ownership

- Usually when a user uploads a file to a share, this file is owned by that same user, and the same thing happens when creating new subfolders. this default behavior can be changed by adding the parameter **force user** to the share definition.

- An option similar to force user is force group, which forces the default group for new files and folders.

```
[Docs]
  comment = Public documents
  path = /shared_docs
  public = yes
  writable = yes
  force user = avazquez
  force group = users
```

394.2 (5) Authentication, Authorization and Winbind

Description: Candidates should understand the various authentication mechanisms and configure access control. Candidates should be able to install and configure the Winbind service.
Weight: 5

Key Knowledge Areas:

- Setup a local password database
- Perform password synchronization
- Knowledge of different passdb backends
- Convert between Samba passdb backends
- Integrate Samba with LDAP
- Configure Winbind service
- Configure PAM and NSS

Terms and Utilities:

- smb.conf
- smbpasswd, tdbsam, ldapsam
- passdb backend
- libnss_winbind
- libpam_winbind
- libpam_smbpass
- wbinfo
- getent
- SID and foreign SID
- /etc/passwd
- /etc/group

Backends

❏ **smbdpasswd**: This is the first back end used by Samba. It consists of a simple plain text file. At this moment it is still supported, but its use is discouraged, as some Samba features won't work with this back end.

❏ **tdbsam**: Widely used nowadays, it uses Trivial Database (tdb) files to store the information.

❏ **ldapsam**: It uses an LDAP server as a back end.

```
passdb backend = tdbsam

passdb backend = smbpasswd
```

```
security = user
passdb backend = ldapsam:"ldap://alpha.linuxaholics.com"
ldap admin dn = cn=admin,dc=linuxaholics,dc=com
```

```
pdbedit -b tdbsam -L
```

winbind

- **winbind**. It enables a Linux server to become a full member in Windows domains and to use Windows users and group accounts in Linux. The idmap configuration * option tells winbind how to map Windows SIDs and Linux user and group IDs.

```
workgroup = VENTANAS
password server = yankee.ventanas.local
realm = VENTANAS.LOCAL
security = ads
idmap config * : range = 16777216-33554431
template shell = /bin/false
kerberos method = secrets only
winbind use default domain = false
winbind offline logon = false
```

- winbind could use cached credentials to permit a user to log in when the DC is offline

- **wbinfo**.

```
wbinfo -u
wbinfo -g

wbinfo -i jose@ventanas.local  #obtenir info
wbinfo -n jose@ventanas.local  #obtenir el sid
```

NSS & PAM

- **NSS**. When Linux needs to locate a user, group, host, etc it looks at the **/etc/nsswitch.conf**.

```
passwd:    files sss winbind
shadow:    files sss winbind
group:     files sss winbind
```

- **PAM**. However, this is not enough to be able to log in to the system. It is necessary to authenticate the user through the use of a password or other method, check whether that user is authorized to log in to the system, and so on. All these tasks are accomplished by Pluggable Authentication Modules (PAM). PAM module (pam_winbind.so).

- **pam_smbpass.so** module has to be used in order to make sure the Samba password is kept in sync when a user changes his Linux password.

Questions & Answers

[394.1 Managing User Accounts and Groups]

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

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

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

2. Which commands will delete the user account joeuser from a Samba server? (Select TWO correct answers.)

   ** smbpasswd -x joeuser*

   ** pdbedit -x joeuser*

3. The net _________ command is used to manage group mapping. (Specify only the sub command.)

   groupmap

4. Select which groups must map to UNIX GIDs on a Samba server operating as a PDC. (Select TWO correct answers.)

   ** Domain Users*

   ** Domain Guests*

5. Which command will display the groups a user belongs to on a remote SMB server?

   net rpc user info

6. Which of the following statements about the smbpasswd command are true? (Select TWO answers)

   ** The -a <user> parameter adds <user> account to the Samba database. If the account already exists, this parameter is ignored.*

   ** The -x <user> parameter removes the <user> account from the Samba database.*

7. The command ______ -x foo will delete the user foo from the Samba database. (Specify the command only, no path information.)

   pdbedit

   smbpasswd

8. When a Windows domain controller is used, which of the following is assigned a Windows Security Identifier? (Select THREE correct answers.)

   users

   servers

   groups

9. Which of the following Samba 4 commands adds the user candidate to group training?

    samba-tool group addmembers training candidate

[394.2 Authentication, Authorization and Winbind]

10. Which command typed on a Samba server will print out the local SID?

    net getlocalsid

11. What has to be done in order to make sure the Samba password is kept in sync when a user changes his Linux password?

    pam_smbpass.so should be added to the password type of the appropriate PAM configuration.

12. Which mechanism of a Linux system is used by Samba to permit identity resolution within a domain?

    Name Service Switch (NSS)

13. Which of the following commands show all user accounts as they are currently available to the Linux operating system no matter of their source?

    getent

14. An administrator has manually migrated local accounts to OpenLDAP, instead of using migration tools. When trying to authenticate as a user, an error is returned about invalid credentials. What is the most likely cause of this?

    The password hash type was not included in the user's password attribute.

15. Beginning with Windows 2000, by default, Windows requires that passwords on your Samba server:

    are encrypted.

16. How can the risk of UID/GID inconsistencies be avoided across UNIX/Linux systems that are sharing information over protocols other than SMB/CIFS (eg: NFS)?

    Specify a common OpenLDAP idmap backend in smb.conf.

17. A Samba server is configured to use the OpenLDAP password backend. The root DN for the LDAP directory is defined in slapd.conf. In order to define an alternative account used by the Samba administrator, which steps are necessary? (Select THREE correct answers.)

    ** Add a new Samba administrative account to the LDAP directory.*
    ** Make certain that the ldap admin option in smb.conf does not point to the LDAP root DN.*
    ** Change the access attributes in slapd.conf.*

18. Which command can be used to directly query the configured winbind server? (Provide the command without any parameters or options)

    wbinfo

19. After finishing configuring of a Unix client to authenticate with a Microsoft Active Directory server, login attempts are unsuccessful. Which of the following is most likely the cause?

    The PAM library is searching the directory with the default search filter.

20. By configuring Pluggable Authentication Module (PAM) and Name Service Switch (NSS) technologies to use OpenLDAP, what authentication service can be replaced?

    Network Information Service (NIS)

21. When configuring an OpenLDAP system for integration with PAM and NSS the /etc/nsswitch.conf file needs to be modified. Which of the following parameters completes this line from the /etc/nsswitch.conf file?
    passwD. files __________

    ldap

22. A server is authenticating users using the pam_ldap module. Only users who are members of a certain group should be allowed to login. In which parameter in ldap.conf can a filter string be specified, that is ANDed with the login attribute when validating a user? (Enter only the parameter, without any options or values)

    pam_filter

23. The command ________ is used on a Samba server to modify the SID in an existing NT profile.

    profiles

395. (9) Samba Domain Integration

Continguts

395.1 (3) Samba as a PDC and BDC

Description: Candidates should be able to setup and maintain primary and backup domain controllers. Candidates should be able to manage Windows/Linux client access to the NT-Style domains.
Weight: 3

Key Knowledge Areas:

- Understand and configure domain membership and trust relationships
- Create and maintain a primary domain controller with Samba3 and Samba4
- Create and maintain a backup domain controller with Samba3 and Samba4
- Add computers to an existing domain
- Configure logon scripts
- Configure roaming profiles
- Configure system policies

Terms and Utilities:

- smb.conf
- security mode
- server role
- domain logons
- domain master
- logon script
- logon path
- NTConfig.pol
- net
- profiles
- add machine script
- profile acls

Windows model

❏ Samba can act as a domain controller (DC) either in an NT-like domain or in an Active Directory domain. It can also integrate as a member server in both environments.

❏ A Windows **domain** is a group of network resources such as users and computers that are organized according to a centralized security database, as opposed to workgroups, in which every computer holds its own security database. The server, or servers, on which this database is located are called **domain controllers**.

❑ Formerly, in Windows NT, there could be two types of DCs: **PDC** and **BDCs**, the difference being that the PDC could modify and update the information in the database, whereas the BDC had a read-only copy of that same database.

❑ **Trust relationship**. Given two domains DomainA and DomainB, if a user from DomainA wants to access resources from DomainB, that user will need to validate again, providing valid credentials in DomainB. However, there is a way to avoid this by establishing a trust relationship. If DomainB trusts DomainA, then users in DomainA can access resources in DomainB without having to authenticate again. These trust relationships are unidirectional, so DomainA won't trust DomainB unless we specifically create another trust relationship.

Samba PDC

❑ Configuring a samba PDC.

- La directiva *wokgroup* en realitat indica el nom del domain.
- La directiva security indica *user* per a PDC i *ads* per a Acive Directory.
- Cal indicar el backend a usar: *tdbsam* o *ldapsam*.
- In every Windows domain there should be a domain master browser. As the Samba server will be the first server in the domain, we configure it as a domain master browser.
- For the Windows workstations to log in to the domain, we need to provide a network logon service (the directive and the share).

```
workgroup = MY_SAMBA_DOMAIN
security = user
passdb backend = tdbsam
domain master = yes
domain logons = yes

netbios name = JULIET
wins support = yes

[netlogon]
        comment = Network Logon Service
        path = /var/lib/samba/netlogon
        guest ok = yes
        writable = no
        share modes = no
```

- And the configuration parameters for the logon scripts.

```
logon script = %u.bat
logon path = \\%L\Profiles\%u
# use an empty path to disable profile support:
logon path =
add user script = /usr/sbin/useradd "%u" -n -g users
add group script = /usr/sbin/groupadd "%g"
add machine script = /usr/sbin/useradd -n -c "Workstation (%u)" -M -d /nohome -s /bin/false "%u"
delete user script = /usr/sbin/userdel "%u"
delete user from group script = /usr/sbin/userdel "%u" "%g"
delete group script = /usr/sbin/groupdel "%g"
```

- Examples creating groups to map windows groups; **net groupmap**. And granting privileges

```
net groupmap add ntgroup="Domain Admins"
net groupmap list

net rpc rights grant 'MY_SAMBA_DOMAIN\Domain Admins'  SeMachineAccountPrivilege
net rpc rights list -U root
```

- **Logon scripts**. The admin can configure a logon script that will be executed whenever a user logs in. The script location will be set up in the logon script option and it will be a relative path to the [netlogon] share.

```
# cat script.bat
net use y: \\juliet\Soft
```

```
logon script = script.bat
[netlogon]
        comment = Network Logon Service
        path = /var/lib/samba/netlogon
```

- **Roaming profiles**. For users to have the same profile no matter which workstation they are logging in from, we can use roaming profiles. In this case the users' profiles are stored in a central repository instead of the local workstation. To use roaming profiles in Samba we must set a value for the logon path option. If this option is idle it means that roaming profiles are not used.

```
logon path = \\juliet\Profiles\%U
```

```
[Profiles]
        path =/profiles
        writable = Yes
        valid users = @WinUsers
```

```
ls -l /profiles/jane.V2/
```

- **System policies**. The Windows NT Server editions used the program poledit.exe to create policies that could be applied later to all of the users and computers in the domain, or to only a group of them. Unfortunately, Samba does not have a native tool to create system policies in an NT domain environment. We can create those policies in a Windows workstation running poledit.exe, though, and apply them later on the Samba server. Save the new policy with the name NTConfig.pol, then we copy that file to the [netlogon] share of the PDC and to the same location in any BDC we might have. We have to make sure that the file is readable by every user.

```
# ls -lh /var/lib/samba/netlogon
-rw-r--r--. 1 root root 8,0K abr 16 23:42 NTConfig.POL
-rwxr-xr-x. 1 root root   25 abr 15 18:34 script.bat
```

Samba BDC

- The users should be able to log in against the BDC, but the BDC should not be a master browser, as this function is performed by the PDC only. The BDC had a read-only copy of that same database.

- Ha de ser un logon server i er tant definir el [netlogon]. Però no ha de ser un master browser (només ho és el PDC). També configurar el BDC com a client del servidor wins del PDC

```
workgroup = MY_SAMBA_DOMAIN
domain master = no
domain logons = yes
wins server = pdc.fqdn

[netlogon]
   comment = Network Logon Service
   path = /var/lib/samba/netlogon
   guest ok = Yes
```

Add computers to a Domain: Member server

- Afegir hosts al domini permet en aquests hosts usar els usuaris, grups i polítiques definides en el PDC. És a dir, ser administrators centralitzadament.

- When trying to join a Windows workstation to a new Windows (or Samba) NT domain, the client will try to find the **NetBIOS** name associated with the domain. The Samba service in charge of answering any NetBIOS query is **nmb**. El Servidor que es vol unir al domini ha de tenir ben configurada la resolució de noms per tal de poder localitzar el PDC pel seu nom netbios.

- Server Windows: per afegir un windows al domini cal anar a la pestanya de configuració i canviar el workgroup per Domain i indicar el nom del domini al que ha de pertànyer. Llavors cal enregistrar-se al domini. Això el windows ho fa automàticament (no veiem el net join que fa) però per fer-ho cal indicar usuari i password amb privilegis d'admiistrador en el PDC.

- **Machine account**. When adding computers to a domain, every computer must have a machine account. Des d'un client windows que es vol afegir al domini és transparent, només cal un user/passwd amb dret d'administració al PDC.

- Des de un server samba que es vol unir al domini cal crear un compte de màquina. Creating them in Samba is pretty easy. We basically need to add a user account with the NetBIOS name of the computer ending in $.

```
useradd -M -s /sbin/nologin ZULU$
?? smbpasswd -m -a ZULU$
```

- The PDC server is located using his netbios name. So its usual to run alse de wins service allowing the others hosts locate servers by netbios name.

```
netbios name = JULIET
wins support = yes
```

- **Member server**. However, a Samba server can be part of a domain without acting as a DC. In this case, the server plays the role of a member server. When a user tries to access the member server, this one delegates authentication to a DC.

- When adding workstations to the domain, for a workstation (or server) to be a member of any given domain, a machine trust account is needed. This is a security measure used to prevent rogue servers or workstations from getting access to the domain.

- Samba stores a domain security account in the passdb back end configured in the smb.conf file. In addition to this, a corresponding UNIX user account is required. The machine account ends with the character $. After creating the Linux account, we create the associated Samba account.

```
useradd -g machines -d /dev/null -c "servername" -s /bin/false servername$
```

```
smbpasswd -a -m servername
```

❏ Configuració d’un member server. Observar que s’indica qui és el password server (el pDC) i s’indica a la directiva security el valor domain.

```
workgroup = MY_SAMBA_DOMAIN
password server = 192.168.1.226
security = domain
idmap config * : range = 16777216-33554431
template shell = /bin/false
kerberos method = secrets only
winbind use default domain = false
winbind offline logon = false
```

395.2 (3) Samba4 as an AD compatible Domain Controller

Description: Candidates should be able to configure Samba 4 as an AD Domain Controller.
Weight: 3

Key Knowledge Areas:

- Configure and test Samba 4 as an AD DC
- Using smbclient to confirm AD operation
- Understand how Samba integrates with AD services: DNS, Kerberos, NTP, LDAP

Terms and Utilities:

- smb.conf
- server role
- samba-tool domain (with subcommands)
- samba

Active Directory Domain Controller

- Samba 4 uses the service samba to work as a ADDC. Ther daemons smbd, nmbd and winbind are no longer needed.

- **Forest**. For instance, we could have a linuxaholics.com domain, a canada.linuxaholics.com domain, and a us.linuxaholics.com domain. In this case the three domains are part of the same forest and share a common administration.

- **Provisioning** consists of setting up all the infrastructure needed for a Samba Active Directory domain to run such as LDAP, Kerberos, and DNS servers. **samba-tool domain provision** subcommand we can provide the domain.

```
samba-tool domain provision --use-rfc2307 --interactive
```

- Active Directory to work properly, synchronizing the time is mandatory. Samba no incorpora la sincronització de temps, però els hosts han d'estar-ho entre elles (presumiblement pels tickets de kerberos). L'usual és utilitzar NTP.

- Configuració de kerberos: */etc/krb5.conf*.

```
[libdefaults]
  default_realm = LINUXAHOLICS.COM
  dns_lookup_realm = false
  dns_lookup_kdc = true
```

```
kinit administrator@linuxaholics.com
```

Configuració DNS

- **Configuració DNS**. El servidor ADDC ha de ser el servidor DNS del domini. Tots els hosts l'han de tenir com a servidor de DNS. Ell mateix també s'ha de configurar com a servidor DNS i incloure el suffixe del domini.

```
cat /etc/resolv.conf
domain linuxaholics.com
nameserver 192.168.1.234
```

- Per poder resoldre noms de fora del domini caldrà configurar samba amb la directiva de dns forwarder indicant ara si el nom d'un servidor DNS extern que permei la resolució de noms de fora del domini.

- El servei DNS és essencial (i qie el propi AD s'apunti a ell mateix) perquè ha de localitzar els serveis LDAp i Kerberos usant un recurs SRV de DNS.

```
_ldap_._tcp.adsname.fqdn
__kerberos._udp.adsname.fqdn
```

samba-tool

- L'utilitat samba-tool permet la gestió integral d'un Active Dorectory DC.

```
samba-tool user info
samba-tool user list
samba-tool user create Antonio P@ssw0rd Antonio --given-name=Antonio --surname=Vazquez -UAdministrator%P@ssw0rd

samba-tool group list
samba-tool group addmembers "Domain Admins" antonio
samba-tool group listmembers "Domain Admins"
```

- Consultar el domini i la informació de DNS

```
samba-tool dbcheck
samba-tool domain info 192.168.1.234
samba-tool dns query localhost linuxaholics.com mike ALL -U Administrator%Passw0rd
samba-tool gpo listall
```

```
samba-tool dns { add delete query roothints serverinfo update zonecreate zonedelete zoneinfo zonelist }
samba-tool group { add addmembers delete list listmembers move removemembers show stats }
samba-tool user { add create delete disable enable list show move password setexpiry setpassword getpassword syncpasswords }
```

- Afegir un DC adicional, una rèplica del ADDC..

```
samba-tool domain join linuxaholics.com DC --server=mike.linuxaholics.com  -U Administrator --password=Passw0rd
```

- Fer backup de les dades d'un ADDC.

```
samba-tool dbcheck
samba-tool domain backup
samba-tool domain backup restore
```

395.3 (3) Configure Samba as a Domain Member Server

Description: Candidates should be able to integrate Linux servers into an environment where Active Directory is present.
Weight: 3

Key Knowledge Areas:

- Joining Samba to an existing NT4 domain
- Joining Samba to an existing AD domain
- Ability to obtain a TGT from a KDC

Terms and Utilities:

- smb.conf
- server role
- server security
- net command
- kinit, TGT and REALM

PDC Domain Member

- ❏ [mirar capítols anteriors]

AD Domain member

- ❏ A Samba Active Directory domain member is a server that is part of the domain but does not provide domain services.

- ❏ DNS. The first thing we need to do is to change the DNS settings so that the Active Directory domain DNS server is queried first

```
# cat /etc/resolv.conf
search linuxaholics.com
nameserver 192.168.56.107
```

```
getent hosts mike.linuxaholics.com
```

- ❏ We also need to create a /etc/krb5.conf file. We can use the same file we used in the DC.

```
# cat /etc/krb5.conf
[libdefaults]
        default_realm = LINUXAHOLICS.COM
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

- ❏ As domain members must have a synchronized time.

- smb.conf configuration as a AD domain member. La directiva **security = ads** indica que la base de dades d'usuaris és al servidor AD. la diretiva **realm =** nomdomini indica el domini al que pertany, el domini AD.

```
[global]
        security = ADS
        workgroup = LINUXAHOLICS
        realm = LINUXAHOLICS.COM
        log file = /var/log/samba/%m.log
        log level = 1
```

- **Idmap config**. Cal separar els usuaris segons si són locals o del domini per saber quan cal fer el mapping de samba a linux (abans anomenada **idmap range**). every user in a Linux system, whether it is a local user, an LDAP user, and so on, is assigned an ID by the system to uniquely identify it. Usually system users and groups are assigned IDs in the range from 0 to 999, and local users and groups are assigned IDs starting from 1000. With this in mind, it seems pretty reasonable to start assigning IDs to domain users and groups starting from 3000. We should also differentiate between the domain users and groups and the local built-in accounts existing on a member server, such as the local administrator, the local guest, and so on. These two groups must not overlap, so we assign the range 3000 to 7999 to domain built- in user and group accounts.

```
idmap config LINUXAHOLICS:backend = ad
idmap config LINUXAHOLICS:schema_mode = rfc2307
idmap config LINUXAHOLICS:range = 3000-7999

idmap config LINUXAHOLICS:unix_nss_info = yes
template shell = /bin/bash
template homedir = /home/%U
```

- **unix_nss_info = yes**. the back end reads all the information available from Active Directory:
  - Users: Account name, UID, login shell, home directory path, and primary group.
  - Groups: Group name and GID.

- **unix_nss_info = no**. only a subset of the previous information is read. Is the default.
  - Users: Account name, UID, and primary group.
  - Groups: Group name and GID.

- Quan s'obté del backend la informació dels usuaris es pot només obtenir el nom, uid i id (un típic compte d'usuari al ldap de tipus inetorgperson) o es pot obtenir tot (un típic compte de ldap posixuser). Si només s'obté el login, uid i gid el shell i el homedir s'obtenen del valors de les directives **template shell** i **template home**.

- net command. Amb l'ordre net ads join s'afegueix el server al domini AD. Es pot indicar l'usuari i passwd o obtenir prèviament les credencials de kerberos amb kinit.

```
net ads join -U Administrator%P@ssw0rd Using short domain name -- LINUXAHOLICS

kinit Administrator
net ads join
```

```
wbinfo --domain-users
```

Questions & Answers

[395.1 Samba as a PDC and BDC]

1. To properly configure a Samba server to be a Primary Domain Controller (PDC), what configuration option must be set to yes?

   domain master

2. For Samba 3 to be able to work as a PDC, some modifications are needed in its main configuration file. Select the THREE options below that show the required actions for this task.

   ** The Samba server has to be a logon server. This can be configured by the domain logons directive.*
   ** The Samba server must be a Domain Master Browser. To configure this, the domain master directive must be set to yes.*
   ** The security = user directive must be set.*

3. What following statement is true about Samba 4?

   Samba 4 can serve as an Active Directory Domain Controller.

[395.2 Samba4 as an AD compatible Domain Controller]

4. Which of the following ports are open by default on a Samba 4 Active Directory Domain Controller? (Choose three.)

   138/TCP
   389/TCP
   445/TCP

5. After finishing configuring of a Unix client to authenticate with a Microsoft Active Directory server, login attempts are unsuccessful. Which of the following is most likely the cause?

   The PAM library is searching the directory with the default search filter.

6. When upgrading a Samba 3 to a Samba 4 Active Directory domain using samba-tool domain classicupgrade, what is true? (Select THREE correct answers.)

   ** The profiles of the users remain unchanged.*
   ** The user accounts and machine accounts are migrated into the new database.*
   ** A basic set of DNS records required for AD operation is provisioned.*

7. Which of the following steps are performed by the command samba-tool domain provision? (Choose TWO correct answers.)

   ** Samba is configured to serve as an Active Directory Domain Controller, including creation of smb.conf in case it does not exist.*

   ** A basic user database with the accounts required in an Active Directory is provisioned.*

8. Which of the following options must be set in smb.conf in order to configure Samba as Active Directory Domain Controller?

   server role = active directory domain controller

9. Which directive in the smb.conf of a Samba 4 Active Directory Domain Controller specifies the name of the Active Directory Domain? (Specify only the option without any values or parameters)

   realm

10. Which option must be specified in smb.conf in order to make Samba create machine accounts automatically when a client joins the domain?

    kerberos

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

    samba-tool domain provision

12. Which of the following values are valid for the Samba 4 configuration directive server role? (Choose THREE correct answers.)

    ** LEGACY DOMAIN MASTER BROWSER*
    ** ACTIVE DIRECTORY DOMAIN CONTROLLER*
    ** CLASSIC PRIMARY DOMAIN CONTROLLER*

[395.3 Configure Samba as a Domain Member Server]

13. Which port in TCP/IP communication is used for Kerberos v5?

    88

14. Which file stores the global Kerberos configuration needed for OpenLDAP integration with Active Directory and Kerberos? (Specify only the file name without any path.)

    krb5.conf

15. What are benefits of using Single Sign-On (SSO)? (Select THREE correct answers.)

    Reduce IT costs due to lower number of IT help desk calls about passwords.
    Reduce time spent re-entering passwords for the same identity.
    Reduce number of passwords to remember.

16. What are the requirements for configuring a Samba file server to work in Active Directory mode? (Choose THREE correct answers.)

    ** Join a domain using the commanD. net ads join*

** Specify a realm in the smb.conf file.*

** Make sure there is no clock drift between the systems in the AD.*

17. Which command would create a machine account in Active Directory under the Computers/BusinessUnit/Department/Servers organizational unit?

    net ads join createcomputer='Computers/BusinessUnit/Department/Servers'

18. When joining a Samba server to an Microsoft Active Directory domain, what is the correct setting for the security directive of the smb.conf file? (Specify the setting value only without any other keywords)

    ads

19. Which of the following commands are required to join an Active Directory Domain? (Select TWO correct answers)

    ** kinit*

    ** net ads join*

20. Which of the following commands is used to join a properly configured Samba server as member to an Active Directory domain?

    net ads join member

21. When integrating Samba and OpenLDAP, what schema needs to be included in the OpenLDAP slapd.conf?

    samba.schema

396. (5) Samba Name Services

Contingut

396.1 (3) NetBIOS and WINS

Description: Candidates should be familiar with NetBIOS/WINS concepts and understand network browsing.
Weight: 3

Key Knowledge Areas:

- Understand WINS concepts
- Understand NetBIOS concepts
- Understand the role of a local master browser
- Understand the role of a domain master browser
- Understand the role of Samba as a WINS server
- Understand name resolution
- Configure Samba as a WINS server
- Configure WINS replication
- Understand NetBIOS browsing and browser elections
- Understand NETBIOS name types

Terms and Utilities:

- smb.conf
- nmblookup
- smbclient
- name resolve order
- lmhosts
- wins support, wins server, wins proxy, dns proxy
- domain master, os level, preferred master

Netbios

❏ **NetBIOS** works at the session layer of the Open Systems Interconnection (OSI) model. it usually runs over TCP/IP. NetBIOS provides the following services:
• Name service (NetBIOS-NS): This works pretty much like the DNS service, allowing us to register and resolve names.
• Datagram distribution service (NetBIOS-DGM): This is used for connectionless communications.
• Session service (NetBIOS-SSN): This is used for connection-oriented communication.

❏ **nmbd** service that is in charge of the NetBIOS naming services.

❏ The hosts need to register their NetBIOS names. When using NetBIOS over TCP, the name service runs on **UDP port 137**.

- **Datagram Distribution Service**. This is a connectionless service that runs on UDP **port 138**. It works by sending and receiving datagrams and broadcast datagrams.

- **Session Service**. This service runs on TCP port 139, and allows two computers to establish a reliable connection.

- **Netbios name**. NetBIOS names have a length of 16 octets, and the last octets usually designate the type of resource.

```
net view
nbtstat -a juliet_server
```

```
These are the available record types for unique names:
• 00 Workstation Service
• 03 Windows Messenger Service
• 06 Remote Access Service
• 20 File Service
• 21 Remote Access Service
• 1B Domain Master Browser
• 1D Master Browser
```

```
These are the record types for group names:
• 00 Workstation Service
• 1C Domain Controllers
• 1E Browser Service Elections
```

Local master browser

- **Local master browser**. is a computer that keeps a list of every server, workstation, and service available in the network. This role is dynamically assigned to one of the computers in the network segment. However, we can influence this election process by tuning some parameters in the smb.conf file

- **local master = yes** By adding this line to the smb.conf file we tell our Samba server to try and become the local master browser in its network segment.

- **preferred local master = yes**. This will give the Samba server a higher preference when trying to become the master browser.

- **os level = 255**. The higher this value, the higher the chance to become the master browser. If we want to make sure that our Samba server wins every election, we can assign the value 255 to this parameter.

```
local master = yes
preferred local master = yes
os level = 255
```

- En un workgroup sense PDC ni AD els servers / hosts que en formen part escullen un d'ells per fer de master browser. És qui recull la informació de qui forma part de la xarxa. Els equips en engegar anuncien que hi són i el master browser ho anota. Quan volen comunicar-se amb d'altres li pregunten al master browser qui hi ha i com accedir-hi.

Domain browser

- **domain master= yes**. If the computers in our domain span across different subnets, to be able to browse every domain member we need to have in each subnet a domain master server.

nmblookup

- **nmblookup**. can look up NetBIOS names from a Linux computer.

```
nmblookup -M MY_SAMBA_DOMAIN
nmblookup 'MY_SAMBA_DOMAIN#1C'
nmblookup 'MY_SAMBA_DOMAIN#00'
nmblookup -A 192.168.1.236
```

Wins

- WINS was implemented by Microsoft as a name server for NetBIOS computer names. It is analogous to DNS, but it uses NetBIOS names instead of domain names. s soon as a WINS client starts, it registers its NetBIOS name and IP address with the WINS server. In turn, when a WINS client launches a NetBIOS application it will query the WINS server about the destination NetBIOS name. If the WINS server finds the queried name it will respond with the corresponding IP address.

- When we set the value of wins support to yes, the nmbd component of Samba enables its WINS server (en el servidor wins)

```
wins support = yes
wins server = w.x.y.z
wins proxy = yes
```

- En els clients wins cal indicar l'adreça ip del servidor wins. The parameter name resolve order, which determines the order in which the client will resolve the NetBIOS name.

```
wins server = 192.168.56.103
name resolve order = lmhosts, wins, host, bcast
```

```
cat /var/lib/samba/wins.dat
tdbdump /var/lib/samba/wins.tdb
```

396.2 (2)Active Directory Name Resolution

Description: Candidates should be familiar with the internal DNS server with Samba4.
Weight: 2

Key Knowledge Areas:

- Understand and manage DNS for Samba4 as an AD Domain Controller
- DNS forwarding with the internal DNS server of Samba4

Terms and Utilities:

- samba-tool dns (with subcommands)
- smb.conf
- dns forwarder
- /etc/resolv.conf
- dig, host

DNS

❏ When provisioning a Samba Active Directory domain, we can install an internal DNS server or use an existing Bind DNS server. When provisioning the Active Directory domain, we can choose whether to install an internal DNS server (as we did), or use a Bind DNS server instead. If electing to use a Bind DNS server, we would have to choose in turn between using flat files or DLZ Bind.

❏ **samba-tool dns**. Consultar el domini i la informació de DNS.

```
samba-tool dns { add delete query roothints serverinfo update zonecreate zonedelete zoneinfo zonelist }

samba-tool dns zonelist
samba-tool dns roothints mike
samba-tool dns query mike.linuxaholics. com linuxaholics.com mike ALL -U Administrator --password=Passw0rd
samba-tool dns query --additional mike.linuxaholics.com linuxaholics.com @ ALL -U Administrator
samba-tool dns serverinfo mike
samba-tool dns add mike.linuxaholics.com linuxaholics.com dummy A 192.168.1.222 -U Administrator --password=Passw0rd
samba-tool dns delete mike.linuxaholics.com linuxaholics.com dummy A 192.168.1.222 -U Administrator --password=Passw0rd
```

❏ Les utilitats dig i host per examinar recursos dns.

```
dig a @mike.linuxaholics.com mike.linuxaholics.com
host -t a mike.linuxaholics.com
```

❏ **Forwarding**. The internal server was populated with all the records needed for the domain to function properly. However, this server has no knowledge about external records, so if we need to access resources on the Internet the Samba DNS server won't be able to provide the right answers to those queries. To solve this problem we can use DNS forwarding; that is, when the internal DNS server cannot answer a query, it will forward that query to another server.

```
dns forwarder = 192.168.1.1
```

Questions & Answers

[396.1 NetBIOS and WINS]

1. Which command with Samba 3 would be used to search for all available workgroups/domains and NetBIOS names?

    findsmb

    nmblookup

2. What is the NetBIOS equivalent of an /etc/hosts file, equating an IP address to a system NetBIOS name. (Specify only the file name without any path)

    lmhosts

3. Enter the FOUR parameters (in the correct order) to be set in the name resolve order directive to use the following name resolution order? (Enter only the parameter names with space between them)
   1. Use lmhosts file entries
   2. Use a server specified in the 'wins server' directive
   3. Use broadcast
   4. Use default DNS lookup

    lmhosts wins bcast host

4. Which of the following are true when considering NetBIOS browsing? (Choose THREE correct answers)

    ** Servers and workstations register their presence to the network.*

    ** One or more machines on the network collate the local announcements.*

    ** Elections are held to determine the roles of certain servers.*

5. Which of the following statements are true regarding NetBIOS names? (Select TWO correct answers.)

    ** You can use a '.' in a NETBIOS name.*

    ** You can use an '_' (underscore) in a NETBIOS name.*

6. After installing a network with one Samba server and several clients, users are complaining that they receive an Unable to browse the network error when trying to visit a public share. What is the most likely cause of this?

    The nmbd process id not running on the Samba server.

7. What is the effect of the following line within a global section of a Samba configuration file?
   preferred master = yes

    After its start, nmbd forces an election in order to become the master browser.

8. Which parameter must be added to the name resolve order directive in order to use broadcasts in Samba name resolution? (Specify ONLY the parameter name.)

   bcast

[396.2 Active Directory Name Resolution]

9. A Samba 4 server provides DNS information regarding an Active Directory Domain. All other DNS information is provided by another 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?

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

10. Which of the following statements is true about DNS in an Active Directory Domain?

    When resolving DNS names? all domain members must query a domain controller or a DNS server that serves the exact same zone content.

11. Which of the following sub-commands are available for samba-tool dns? (Select TWO correct answers)

    query
    add

12. Which of the following commands add 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?

    samba-tool dns add dc1 samba.private fileserver01 AAAA 2001: db8: : 190 -U Administrator

397. (5) Working with Linux and Windows Clients

Continguts

397.1 (3) CIFS Integration

Description: Candidates should be comfortable working with CIFS in a mixed environment.
Weight: 3

Key Knowledge Areas:

- Understand SMB/CIFS concepts
- Access and mount remote CIFS shares from a Linux client
- Securely storing CIFS credentials
- Understand features and benefits of CIFS
- Understand permissions and file ownership of remote CIFS shares

Terms and Utilities:

- SMB/CIFS
- mount, mount.cifs
- smbclient
- smbget
- smbtar
- smbtree
- findsmb
- smb.conf
- smbcquotas
- /etc/fstab

SMB/CIFS

- **SMB**, also known sometimes as **CIFS**, is the protocol in charge of providing shared access to files and printers on Windows networks. To make things simpler we use both terms interchangeably. This service can run directly over **TCP port 445**.

- **smbclient**. tool to access Windows shares from a Linux workstation. To list the available shares on a Windows server we would use the -L parameter.

```
smbclient -L //192.168.1.129 -U antonio
smbclient //192.168.1.129/public -U antonio
```

- **smbget**. Download files from a Samba share is by using the smbget utility, which is quite similar to wget.

```
smbget smb://192.168.1.129/public/2018feb.txt -U antonio
```

- **smbtar**. allows to download multiple files from a Samba share into a single file or tape.

```
smbtar -s 192.168.1.129 -x public -d . -t fichero.out -u antonio -p antonio -v
```

- **smbtree**. shows every Samba server present in the network and its shares. However, it can be a bit tricky to set up at first. The program needs to be able to resolve NetBIOS names, otherwise it won't show any information.

```
smbtree -s smb_client.conf -U Antonio%antonio
```

```
name resolve order = lmhosts, bcast
```

```
cat /etc/samba/lmhosts
192.168.56.102   HOTEL#20
192.168.56.102   MYGROUP#1D
192.168.56.102   MYGROUP#1B
```

- **smbfind**. show the machines in the network that respond to SMB queries: smbfind. It is really a Perl script that uses nmblookup and smbclient to get the needed information.

```
findsmb
```

- **mount**. mount a Samba shared folder locally with mount or mount.cifs.

```
mount -t cifs -o username=antonio,password=antonio //192.168.1.129/public /mnt/public_docs/
```

- **CIFS credentials**. Mounting SMB/CIFS shares we can specify the username and the password as parameters of the mount command. However, it is more advisable to keep this information stored in a file instead of passing them in plain text as command parameters.

```
cat credentials.txt
  username=antonio
  password=antonio
```

```
mount -t cifs -o credentials=/root/credentials.txt //192.168.1.129/public /mnt/public_docs/
```

- Features CIFS:

  • Integrity and concurrency: CIFS allows concurrent access to the same file, while providing the needed locking mechanisms to prevent conflicts.

  • Optimization for slow links: The CIFS protocol has been optimized over the years to work well even over slow links.

  • Security: A CIFS server allows both anonymous as well as authenticated secure access to the resources.

  • Performance and stability

  • Unicode file names

- **smbacls**. We can list the permissions of a remote Samba share with smbcacls.

```
smbcacls //192.168.1.129/public 2018jan.txt -U antonio
smbcacls //192.168.1.129/public 2018jan.txt -U antonio%antonio -M ACL:Jose:ALLOWED/0/CHANGE
smbcacls //192.168.1.129/public 2018jan.txt -U antonio%antonio
smbcacls //192.168.1.129/public 2018jan.txt -U antonio%antonio -M OWNER:Jose
```

397.2 (2) Working with Windows Clients

Description: Candidates should be able to interact with remote Windows clients, and configure Windows workstations to access file and print services from Linux servers.
Weight: 2

Key Knowledge Areas:

- Knowledge of Windows clients
- Explore browse lists and SMB clients from Windows
- Share file / print resources from Windows
- Use of the smbclient program
- Use of the Windows net utility

Terms and Utilities:

- Windows net command
- smbclient
- control panel
- rdesktop
- workgroup

Windows Clients

❏ **net**.

```
net user
net user /domain

net share

net config workstation
```

❏ **Rdesktop**. Remote administration tool. Before being able to connect, though, we must allow the remote administration on the Windows workstation.

Questions & Answers

[397.1 CIFS Integration]

1. CIFS relies upon which port for direct hosting without requiring NetBIOS?
   445

2. Which of the following are true for CIFS? (Choose TWO correct answers.)
   Filenames can be in any character set.
   Opportunistic Locks are supported.

3. After adding a remote CIFS share to /etc/fstab, the share is mounted to the correct location in the file system. There, all files belong to the user and group root and are not readable or writable by any other users on the system. What should be done in order to permit distinct local user access to the mounted files?
   The user should be added to the local user group smbusers as mount.cifs by default restricts access to all CIFS mounts to members of this group in addition to the root account.

4. After adding a remote CIFS share to /etc/fstab, the share is mounted to the correct place in the file system. There, all files belong to the user and group root and are not read- or writable to any other users in the system. What should be done in order to permit a distinct local user access to the mounted files?
   The mount.cifs options uid, gid, file_mode and dir_mode should be used to specify the ownership and permissions of the mount.

5. Which option to mount.cifs specifies a file that contains the user name, password and domain that should be used for authentication against the server during the mount? (Specify only the option without any values or parameters)
   credentials

6. Which option is used when running smbclient with a file containing user credentials?
   -A

7. Which of the following commands executes a recursive download of the src share located in a Samba server named SOURCES, assuming that this server allows anonymous users?
   smbget -R smB. //sources/src

8. On the Linux command line, which of the following Samba tools lists the available domains, servers and shares?
   smbtree

9. The showmount command will list the available NFS shares on a server. What command will provide the same information on a Samba server named FileSrv1?

   smbclient -L FileSrv1

10. After successfully connecting to a remote CIFS share using smbclient, the command mget MyFiles is issued to retrieve the folder MyFiles, including all of its contents. Instead of transferring the folder, smbclient returns the error:
    NT_STATUS_NO_SUCH_FILE listing \MyFiles
    What should be done in order to download the contents of the folder?

    The server has to support recursion for the given share which, on Samba, is enabled by setting recursion = true.

[397.2 Working with Windows Clients]

11. Which of the following Linux commands can be used to log into a remote Microsoft Windows server using RDP?

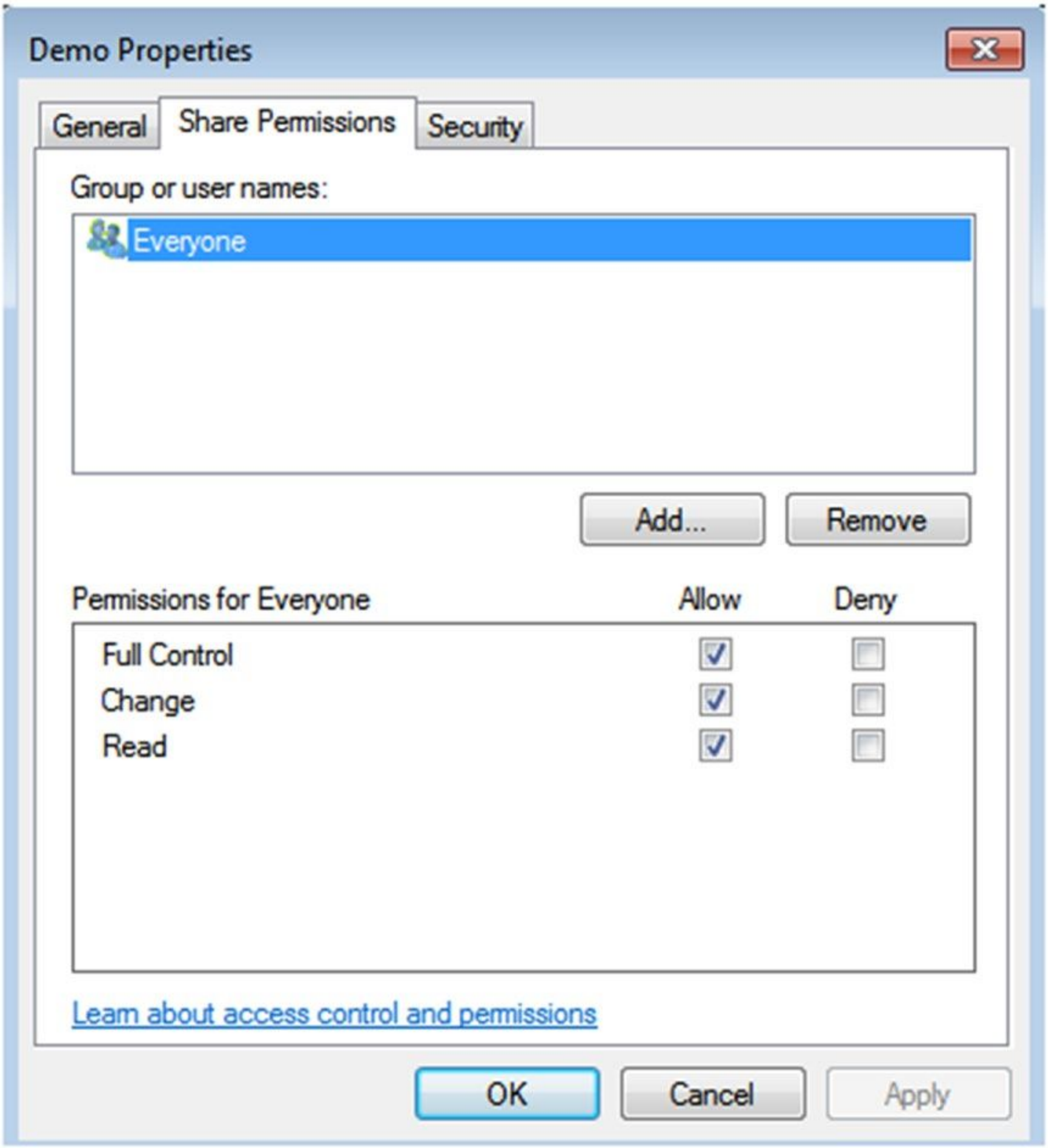
    rdesktop

12. Which port must be open in a firewall to allow access to the Remote Desktop Protocol (RDP) server running on the standard port?

    3389

13. When preparing the delivery of printer drivers from Samba to Windows clients, which of the following requirements have to be fulfilled? (Select TWO correct answers.)

    ** The driver must be associated with the printer either by Samba's rpcclient command or by the Windows Add Printer wizard.*
    ** The driver has to be put on a Samba share called print$.*



Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□