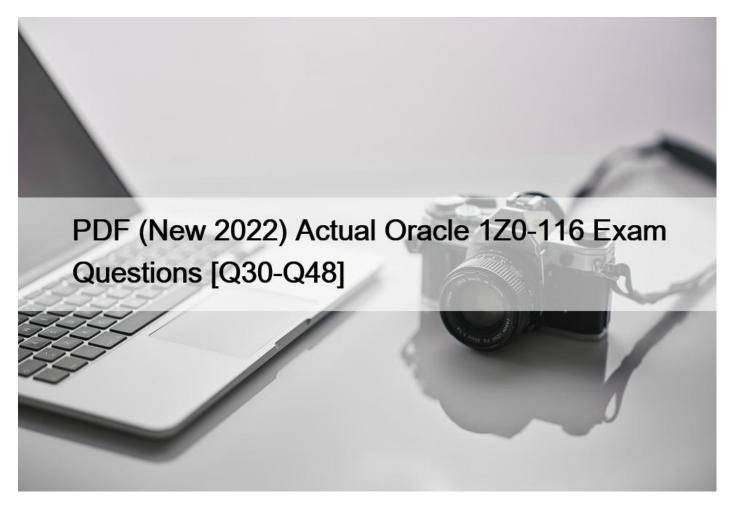# PDF (New 2022) Actual Oracle 1Z0-116 Exam Questions [Q30-Q48

PDF (New 2022) Actual Oracle 1Z0-116 Exam Questions
Dumps Moneyack Guarantee - 1Z0-116 Dumps UpTo 90% Off

NO.30 Which two statements are true about column-level transparent data encryption?
* It can bo used for tables in encrypted tablcspaces.
* encrypted columns cannot have an Index.
* All encrypted columns of a table use the same encryption key.
* Column level encrypted data remains encrypted in the buffer cache.
* Column-level encryption keys are not encrypted by the master key.

NO.31 Which two privileges can be restricted at the column level?
* SELECT
* INSERT
* REVOKE
* UPDATE
* GRANT
* DELETE

NO.32 Examine these commands and responses:

```
SQL> connect mary
Enter password:
Connected.
SQL> exec U1.PROC2('Code')
BEGIN U1.PROC2('Code'); END;

*
ERROR at line 1:
ORA-06598: insufficient INHERIT PRIVILEGES privilege
ORA-06512: at "U1.PROC2", line 1
ORA-06512: at line 1
```

Which object privilege must be granted to allow execution of the stored procedure?
* grant EXECUTE ON MARY.PBOC2 Co U1;
* grant INHERIT PRIVILEGES ON USER U1 TO MARY;
* grant INHERIT PRIVILEGES ON USER MARY TO U1 ;
* grant EXECUTE ON U1.PROC2 TO MARY;

NO.33 When creating labels using Oracle Label Security, which is required?
* level and group
* level, compartment, and group
* compartment
* group
* level
* compartment and group
* level and compartment

NO.34 Examine this command:

```
emcli list_masking_definitions -definition_name=credit -target_name=test%
```

What masking definitions does it list?
* All with the name credit and the commands to deploy them on all databases with names starting with test.
* All with names starting with credit and created on databases with names starting with test.
* All with the name credit and created on databases with name starting with teat.
* All with names starting with credit and created on any database.
* All with the name credit and the commands to deploy them on a database with the name test.

NO.35 Which three authentication methods are available with Centrally Managed Users (CMU)?
* remote Access Services authentication
* smart key authentication
* public key Infrastructure (PKT) authentication
* kerberos authentication
* username/password authentication
* SSH authentication

NO.36 What Is the first step when analyzing security within a database?
* Encrypt tablespaces using Transparent Data Encryption

* Configure and enable Database Vault
* Execute Database Security Assessment Tool (DBSAT)
* Mask nonproduction data using Data Masking & Subsetting
* Deploy Oracle Key Vault
* Create a Data Redaction Policy for your most sensitive tables

NO.37 Which statement can be used to force password complexity in the password file?
* orapwd file=orapwORCL format=12 force-yes
* orapwd file=orapwORCL force=yes format=legacy
* orapwd file=orapwOPCL forcaat=12
* orapwd file=orapwOBCL forroat=12.2

NO.38 Examine this query:

```
SELECT username, account_status
FROM    dba_users
WHERE   username IN ('JANE','TOM','MARK');

USERNAME ACCOUNT_STATUS
-------- ----------------
JANE     LOCKED(TIMED)
```

Why is this account in this status?
* The account uses a global authentication.
* The user exceeded the value of FAILED_LOGIN _ATTEMPTS and its password has not been reset yet.
* The account has the SYSDBA privilege granted.
* The user exceeded the value of PASSWORD_LIFE_TIME and Its password has not been reset yet
* The ACCOUNTS_ STATUS column is not updated until the user attempts to log in.

NO.39 Database Vault is not used in your installation.

Why is a conventional secure application role more secure than a normal role?
* It Is In effect only when configured as a default role for the user.
* It requires a password to be set.
* It can be set only by a package or procedure that is created with deflner's rights.
* It can be set only by users with the grant any bole privilege.
* It can be set only by a package or procedure associated with the role definition.

NO.40 While upgrading your Oracle database server from 10g to 19c, you want to ensure that the users can still connect with their current passwords after the upgrade.

What do you need to set explicitly for this purpose?
* SQLNET.ALLOWED_LOGON_VERSION_SERVER = 12a in the sqlnet.ora of the new database home
* Client net. allowed_lLOGON_VERSION_client must be set to a lower value than the server SQLNET.ALLOWED LOGON. VEBSION .SERVER.
* SQLNET.ALLOWED_LOGON_VERSION_client = 8 in the sqlnec.ora file of the client application.
* SQLNET.ALLOWED_LOGON_VERSION_sebveb = 8 In the aqlnec.ora of the new database homo.

NO.41 Database Vault Is configured and enabled In the Oracle database.

Three users are granted the dba, dv_omneb, and dv_acctmgb roles.

There is a requirement to create a user who can:

1. Connect to the database Instance

2. Select from dictionary views

Which users can complete the operation to meet the requirement?
* users granted DV_ACCTMGR and DV_OWNER roles
* users granted DV_OWNER role
* users granted DBA and DV_OWNER roles
* users granted DV_ACCTMGR and DBA roles

NO.42 The utl_http package is used to invoke REST API's to manage Oracle GoldenGate Microservlces Architecture components on host1.

You must use dbms__network_acl_admin to specify a range of ports to be used when connecting to host01.

What three requirements must you consider?
* The lower_port may be null but the upper_port must specify a value.
* The port range must not overlap with any other port ranges for host01.
* upper_port must be greater than or equal to lower_port.
* The port range may not include values larger than or equal to 1024.
* Both lower_port and upper_port must not be NULL
* The upper_port may be null but the lower_port must specify a value.

NO.43 You grant user JANE the SYSDBA administrative privilege. Which two are true?
* User JANE must always connect as SYSDBA to the database instance.
* User JANE can grant SYSDBA privilege to roles.
* User JANE must use operating system authentication.
* User JANE can create objects In sys schema only when connected as SYSDBA.
* User JANE acquires the DBA role by default.
* User JANE can backup and recover the database.

NO.44 Examine this sqlnet.ora file used by a client application:

```
SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS)
SSL_VERSION = 1.2
SSL_CLIENT_AUTHENTICATION = TRUE

WALLET_LOCATION =
    (SOURCE =
      (METHOD = FILE)
      (METHOD_DATA =
        (DIRECTORY = /etc/oracle/client/wallet)
      )
    )
```

Which three are found in the wallet specified by the directory parameter?
* the private key of the database service
* the trusted certificates of the database service
* the user certificate used to uniquely Identify the database service
* the private key of the client application

* the username, password, and service name required to connect to the database
* the user certificate used to uniquely Identify the client application
* the trusted certificates of the Certification Authority

NO.45 What is true about the client identifier?
* The client Identifier is automatically included In the audit trail.
* The client Identifier is automatically set by the SQL-Net layer.
* A session can have multiple client Identifier values set simultaneously.
* The client Identifier cannot be changed during the session.

NO.46 Which two are true about Database Privilege Analysis?
* It can be used after you install the Oracle Database without any additional database configuration steps.
* It must have the Database Vault option enabled.
* Privilege analysis data for dropped objects are kept.
* If a privilege is captured during run time, it is saved under the run-time capture name.
* It shows the grant paths to the privileges and suggests which grant path to keep.
* It cannot be used to capture the privileges that have been exercised on precompiled database objects.

NO.47 Examine this parameter In sqinet.ora:

SQLNET.ADTHENTICATION_SEBVICES=(NONE)

For which two cases do you need a password file?
* to authenticate externally Identified users locally
* to authenticate nonprivllegcd database users locally
* to authenticate administrative privileged users remotely
* to authenticate externally Identified users remotely
* to authenticate nonprivileged database users remotely
* to authenticate administrative privileged users locally

NO.48 When querying the database view, VSECRYPTION_WALLET, the status Is OPEN_NO_MASTER _KEY. What does this mean?
* You do not have select privileges on this database view.
* The master key has been corrupted.
* The key store is not open.
* The master key has not been created.
* This is expected behavior for this view.

Understanding functional and technical aspects of Oracle Database Security Administration Exam Number: 1Z0-116
The following will be discussed in the **ORACLE 1Z0-116 exam dumps**:

- Survey security needs (hazard decrease, administrative consistence)- Send the Maximum Security Architecture- Survey the normal assault focuses for a data set **Updated Jun-2022 Pass 1Z0-116 Exam - Real Practice Test Questions:** https://www.topexamcollection.com/1Z0-116-vce-collection.html]