**Please demonstrate Skills architecting and administering Oracle Database Links, SFTP transfer of flat files and other integration techniques**

**Oracle Database Links:**

Oracle provides the concept of Database Links to allow for a source Database to interact and manipulate data stored within a remote Database source. Database Links are stored as Schema objects and their use can be restricted through the configuration of Database Users and Roles. With correct configuration, data can be restricted to Read Only, or provide the ability to INSERT, UPDATE and DELETE, depending on the requirement.

The architecting of Database Links requires a strong understanding of Oracle Database security concepts and principles (System and Object privileges), as well as the utilities available to restrict access and enhance security. Poorly architected Database Links can pose a significant security concern by opening up the underlying Database system to unwanted threats by unknown actors.

Once an optimal configuration of Database Users & Roles has been achieved through the implementation of a minimum access policy, the Oracle Net Listener should be further configured with Transport Layer Security (TLS) encryption, securing all connections and communication between the Oracle Client and the Oracle Listener. The coupling of strict Database User and Role Database configuration along with TLS enabled traffic will provide optimal security inline with Oracle’s best practices.

From Oracle Database 18c and above, encrypted Database Link passwords are implemented by default; therefore, if older Oracle releases are employed, PwC advises upgrading the databases to the latest Oracle release to take advantage of the enhanced security features. PwC would always recommend the deployment of Private Database Links where possible, coupled with a regularly scheduled audit review of ALL granted Database permissions, both at User and Role level.

The implementation of secure Database Links would typically follow the below high level steps:

1. Configure SSL/TLS for Oracle Net.
2. Create a Wallet for Certificate.
3. Store Certificates in Wallet.
4. Create and Configure Private Database Link(s) (Public if required).
5. Configure Database Permissions (Users & Roles).
6. Test the Encrypted Database Link(s).
7. Monitor and Maintain Database Link(s).
8. Secure Wallet.
9. Update Documentation.

**SFTP and Network hardening for Flat File transfers:**

Flat files are typically transferred between two host machines across a network via the SFTP protocol. There are numerous implementation techniques that should be considered to provide hardening of the underlying SSH and SFTP protocols. The correct approach is typically a mix of file and traffic encryption, authentication mechanisms and overall Operating System security.

SFTP makes use of the SSH protocol to secure and authenticate connections, and uses the same methods for SSH authentication. SSH2 is the second-generation SSH protocol which utilises the AES algorithm, and is significantly more secure than its predecessor, SSH1.

To harden the security of the SFTP server, PwC recommends the following configuration concepts as the absolute minimum to securing the SSH / SFTP protocols.

1. Password complexity is not sufficient enough to avoid brute force attacks. Therefore, User Passwords should be disabled.
2. SSH access must be key-based, using a 4096-byte key length, and rotated on a scheduled basis to avoid being compromised.
3. Root access via SSH should be disabled as default to avoid a remote breach at Super User level.
4. Failed Login Attempts should be limited to protect against brute force attacks.
5. Empty Passwords should be forbidden by default.
6. The lesser secure FTP protocol should be disabled by default.
7. Allowlists should be configured on the Network Layer to restrict connections on a per-IP basis, allowing only connections originating from trusted sources.
8. GNU Privacy Guard (GPG) should be deployed to encrypt files and make use of symmetric and asymmetric encryption to secure files at rest on the SFTP server.

an ad-hoc basis.

**Case Study 1:**

PwC deploys, administers and monitors Oracle Database Links for a large number of Client Oracle databases, spanning across all industries and sectors, including the Public Sector where an elevated Security Clearance is required for administration due to the sensitive nature of the underlying data.

One of the larger and more complex Oracle estates under PwC’s management consists of 30+ Oracle Databases, of varying major releases and functionality, including Oracle E-Business Suite, Hyperion Essbase, Oracle Business Intelligence and WebLogic Servers, with custom interfaces and Database Links used as the constructs to interlink systems and provide reporting functionality and integration with Non-Oracle database storage. AES 256 Native Network Encryption is used to encrypt the network traffic.

The on-going management and audit of these Database Links and their associated permissions plays an important role in ensuring the integrity of the underlying Database systems, and monthly audit activities are carried out by PwC to minimise any threat to security. All Databases under the support of PwC are inclusive of the latest in Oracle Critical Update (CPU) patches to address recently found security vulnerabilities, along with regular monitoring of Vendor releases to remain compliant.

With communication between each Database being absolutely critical to the overall solution architecture, and running of the business, the efficiency of the monitoring solution is paramount and therefore configured to report on issues relating to all components within the Oracle Technology Stack on a 24x7 basis.

**Case Study 2:**

PwC has designed, created and deployed automated file transfer solutions across a wide range of Clients' Oracle systems running on various Operating System platforms. We have designed a solution for a global financial services client to transfer files from the UK to Japan. Trial Balance and general ledger data is extracted from the client's Oracle ERP application via a PwC-written custom program to SAMBA storage. The extract is then transferred to Japan via an SSH-hardened SFTP and transformed using an ETL tool. To ensure files are transferred, PwC has deployed a comprehensive monitoring solution. The solution consists of custom PwC scripts designed to monitor OS, application and database performance, health, growth and storage. Monitoring is automated and linked into the PwC Application Managed Services (AMS) service desk.