THE EUROPEAN BANK SAFEGUARDS ITS ORACLE APPLICATIONS WITH CLAREMONT'S SECURITY SOLUTION

THE CLIENT

Established in 1991, the European Bank for Reconstruction and Development (EBRD) offers project financing to public and private sector organisations.

Providing loan and equity finance, guarantees, leasing facilities and trade finance for projects, the bank invests only in projects that could not otherwise attract financing on similar terms. It is funded by sixty-four countries and two inter-governmental organisations and works across thirty-four countries.

The Business Challenge

The EBRD makes extensive use of Oracle technology – this includes the use of over three hundred separate databases. A security audit identified that changes were required to ensure these Oracle-based systems were kept secure and better processes were needed to manage security.

In particular, password maintenance had become a burden for end-users and support personnel. Several legacy applications did not have the ability to change passwords, which made security hard to uphold.

The EBRD needed to address these safety issues with a technology solution that would not create its own management or administration headaches. The solution had to be robust but still cost-effective. It could not add unjustified cost to the business since these changes aimed to enforce security on existing systems rather than provide any new functionality.

Benefits

The issues identified in the security audit were wholly resolved through a single, central system that integrated the Oracle databases with the corporate authentication platform. Claremont's robust and cost-effective solution delivered the following business benefits:

- Oracle Fusion Middleware enabled all Oracle-based systems to be integrated with EBRD's corporate security and authentication platform, Microsoft AD.

- Additional support and administration costs were minimised.

- All password maintenance is now centralised with the corporate network logon policy.
- All Oracle systems are now single sign-on. Each user has only one user name and password for multiple applications.

- The entire solution was achieved using standard, off-the-shelf Oracle functionality without any customisations being required.

- No changes or new developments were required to legacy applications for them to be part of this solution.

European Bank
for Reconstruction and Development

The Solution

The EBRD engaged Claremont to deliver a solution that would tackle these evident security threats. Claremont's experienced team designed and implemented a vigorous solution that would connect all of the ERBD's Oracle databases to its corporate identity solution – Microsoft Active Directory (AD) – where its users' network logons are stored. This would ensure that:

- All its Oracle users were authenticated against AD
- Password maintenance was enforced through the corporate network logon policy
- Each user required only one user name and password was for multiple applications

System Configuration

A fully fault-tolerant infrastructure was configured using two Oracle Fusion Middleware components from the 11g Identity Management Suite: Oracle Internet Directory (OID) and Oracle Virtual Directory (OVD).

Oracle databases were registered with OID using the Enterprise User Security option in the database software. OID and OVD were configured to communicate with Microsoft AD and pass through credential checking for all users connecting to the Oracle databases that were registered with OID.

Data Replication

Fault tolerance was provided by configuring identical OID and OVD infrastructures at both a primary and secondary site, enabling OID data replication between them to ensure both sites had a copy of all the database registration details.

In addition, OVD was configured to communicate with multiple AD servers to prevent the loss of a single AD server affecting the whole solution. Similarly, end user applications were aware of both the primary and secondary OID and OVD sites, so if one was unavailable, they could continue to authenticate against AD, seamlessly. Full redundancy made this a fully fault tolerant, high availability security solution.

Test Environments

Claremont configured the solution in development and test environments where it could be tested by the EBRD. This enabled full end-to-end testing of the disaster recovery (DR) solution with simulated failover tests to ensure the fault

tolerant DR solution worked as intended. When testing was complete and signed-off by the EBRD, the solution was then implemented in primary and secondary live environments.

Pro-Active Support

Having designed and implemented the solution, Claremont put provisions in place to support EBRD's internal technical team in future. A comprehensive handover was performed, including one-to-one training for the EBRD Database Administration (DBA) team and detailed guidance was produced.

No changes were required to legacy applications to make this solution work. The whole exercise was completed in an elapsed period of six weeks.

Business Benefits

The issues identified in the security audit were wholly resolved through a single, central system that integrated the Oracle databases with the corporate authentication platform. Claremont's robust and cost-effective solution delivered the following business benefits:

- Oracle Fusion Middleware enabled all Oracle-based systems to be integrated with EBRD's corporate security and authentication platform, Microsoft AD.
- Additional support and administration costs were minimised.
- All password maintenance is now centralised with the corporate network logon policy.
- All Oracle systems are now single sign-on. Each user has only one user name and password for multiple applications.
- The entire solution was achieved using standard, off-the-shelf Oracle functionality without any customisations being required.
- No changes or new developments were required to legacy applications for them to be part of this solution.

Choosing The Right Managed Services Provider

If you are looking for an Oracle partner who can help you with your Security, goes about it the right way and can back up the talk, then contact us.