EKRAN

CASE STUDY

Featured story

Bastion Host

Organize secure access of the third-party administrators to the bank’s infrastructure with the complete activity monitoring

Problem

One of the bank’s project required involvement of third-party providers for administrating several databases. In order to protect themselves from unauthorized access to other critical infrastructure components, bank’s security department decided to implement advanced security system for administrator access control.

Bank’s specialists expected that no more than two third-party experts would have access to their systems. Both of them can have simultaneous privileged access to the bank's systems.

Needless to say that any session of the third-party provider’s employees should be monitored for security compliance and logged to enable post-audit activities.

The question was whether Ekran System could solve this task of organizing and monitoring remote service provider access. The bank representatives requested a proposal with price estimation for Ekran System components needed according to their specific requirements.

Details

Ekran System specialists asked the client a few clarifying questions:

1. How many systems with databases need to be monitored?
2. What are the versions of those databases?
3. What are the operating systems?
4. How will administrators have access to databases? Directly or via software (TOAD, SQL Management Studio, SQL Developer, etc.)?

The bank's team answered all of them:

1. 116 systems with Oracle databases - administrators can use Grid Control to access them; 6 DB2 databases - administrators can access them via command line
2. RHEl 5.x, 6.x, AIX 6.x, 7.x OS
3. Oracle 11g, 12c
4. DB2 9.7, 10.5

Solution

Ekran System team suggested solving this problem via **Bastion host architecture**. It requires installing terminal server that has protected access both to the internal network and to the external one by RDP. All tools needed for Oracle databases administration should be installed on it.

Ekran System agent that monitors all user actions and all user sessions should be installed on the Bastion server. All access rules should be set, and Ekran System Secondary Authentication option should be enabled. In addition, rules for instant alerts should be defined in order to notify security personnel about the beginning of work with the database.

Thus, the work of all third-party providers will be under control and each their session will be available for audit with any action recorded. Secondary authentication will provide clear information about who exactly accessed the infrastructure under the admin credentials.

After providing price estimation, Ekran System team was hired for this project and successfully deployed described Bastion solution.