White paper

Do you still need your database?

Two-factor authentication makes bloated databases superfluous

Table of contents

Introduction

Big data, sensitive data, data protection – these keywords appear increasingly often in the media. As a result of the increased digitisation of processes, more flexible working hours and locations, as well as improved internet connections, all kinds of information circulate within and between companies, government agencies, organisations, associations, hospitals, medical practices, etc. And special database systems are generally used for the storage, management and processing of electronic data. But it is not always necessary to make new purchases in this respect. This white paper explains how two-factor authentication solutions can use existing infrastructures for data storage.

Databases today

These days, big data trends often result in database solutions being designed to store terabytes of data. However, in most cases, these are not the most efficient answer. Only a few such systems are "filled to the brim" with data. And such resource-hungry infrastructure consumes a lot of disk space. Companies and organisations therefore invest heavily in the necessary hardware, servers or virtual environments, including suitable applications, which in turn can cause performance and availability issues. Any company implementing a database solution should first look at the "worst case" scenarios, such as security encroachments in the form of SQL injections and the like. These digital attacks involve cybercriminals exploiting vulnerabilities in an SQL database by injecting their own commands via the application that provides access to the database. This can result in data being spied upon or changed, or the entire server being hijacked. And upgrades need to be carefully managed especially if the software vendor has decided to change to a different database manufacturer.

Big data – little data

The boom in big data is underlined by a recent study carried out by market research firm IDC: by 2018, global investment in this sector is expected to amount to 41.5 billion dollars. This equates to six times greater growth than in the rest of the IT sector. With regard to the specific storage of user data for a two-factor authentication system (short 2FA) to ensure secure remote access to a corporate network, conventional solutions also tend to rely on the use of large database infrastructures. The disadvantages here are the very high installation costs and, in most cases, costs involved in the purchase of separate dedicated servers as the very high memory and disk needs of databases do not lend themselves well to virtualisation. Furthermore, the addition to the infrastructure of a further component that needs to be managed means additional work for the IT department. And these systems must also be included in the security measures. Nevertheless, they may still fail and cause delays.

Curiously though, common 2FA solutions involve only very small amounts of data, so the use of big data structures for storage is excessive. Generally, the login user ID along with the first name and surname of the user, PIN and passcodes or seed records (special algorithms for creating the one-time numerical passcodes used for authentication) and last login time are stored. In cases involving about 10,000 users, companies usually require about 200 bytes per user. It is therefore not particularly efficient to store such small volumes in environments that are designed for considerably larger amounts of data - so investment in major infrastructure is also unnecessary.

Data synchronisation risks

If IT teams are making entries of personal details in a database system for the first time, they must enter a large amount of information manually. This includes, for example, first names and surnames. In the case of a change of name, for example as a result of getting married, it should be ensured that this change is made in the database. This is particularly important if the information is to be synchronised. If an error occurs in this respect and user files are insufficiently synchronised, a database may, over time, contain several records with different information for a single user, rather than a single correct record per user.

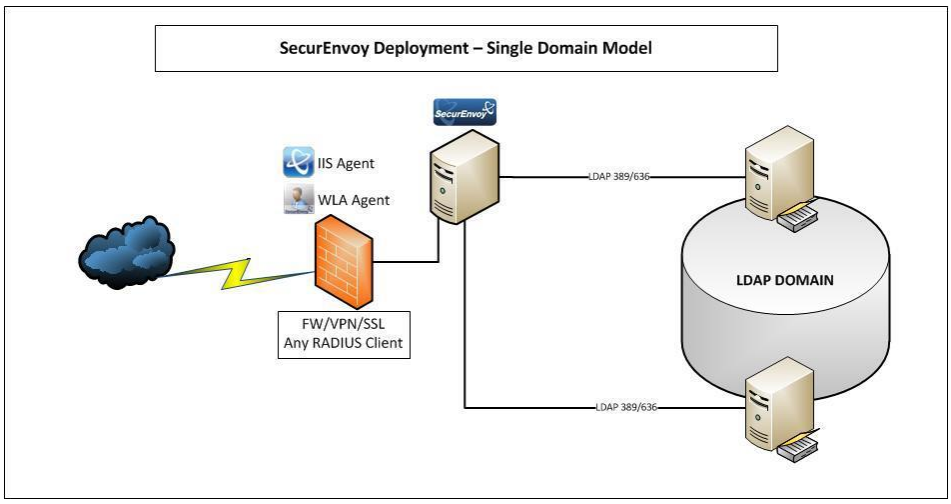
The set up and management and administration of the database system can in general be time-consuming and labour-intensive. Each database needs to replicate changes to other copies on other servers. This may require network ports opening on firewalls between servers and regular checking that replication is working and up to date. If a user authenticates, for example, when a server crashes, the database may become unusable until the last transaction is rolled back. This normally requires manual administrator interaction and help from the software vendor. System downtime can also often result in financial losses.

Option: using an existing LDAP server

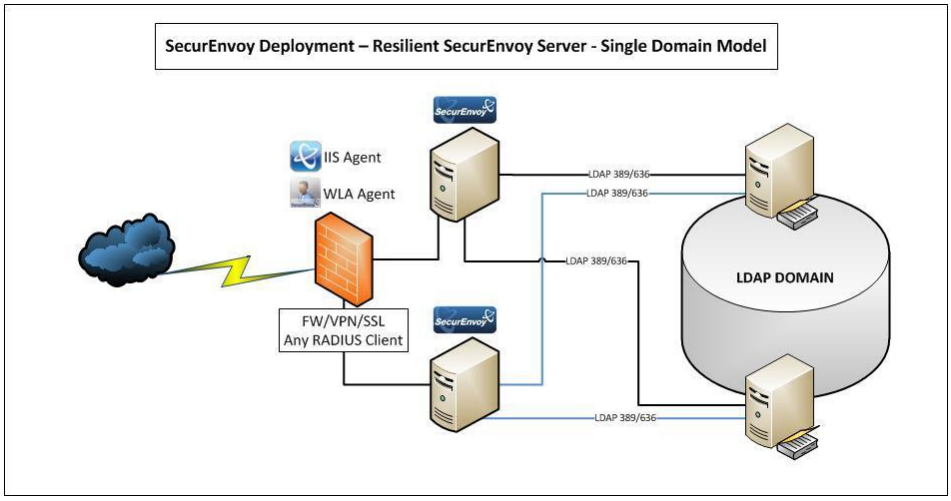
In the area of 2FA, the method developed by SecurEnvoy offers a good alternative. Based on the principle of "reusing existing infrastructure", the technology is tokenless i.e. instead of expensive dedicated hardware tokens, existing smartphones and other mobile devices are used as the authentication token. Furthermore, the method makes use of existing LDAP servers for the database, so that no new (big data) structures are required. The solutions instead integrate seamlessly with Microsoft Active Directory, Microsoft AD LDS (Active Directory Lightweight Directory Services), Novell eDir, Oracle Directory Server and OpenLDAP, without the need for additional databases or hardware.

No schema change is required as SecurEnvoy use existing attributes defined for telex machines that are no longer used but must exist to be compliant with LDAP standards, this data being secured via FIPS 140-2 approved AES encryption. In addition, the technology is able to support a heterogeneous environment consisting of LDAP servers from different manufacturers and can be managed via a single SecurEnvoy server. IT departments can choose between three installation methods:

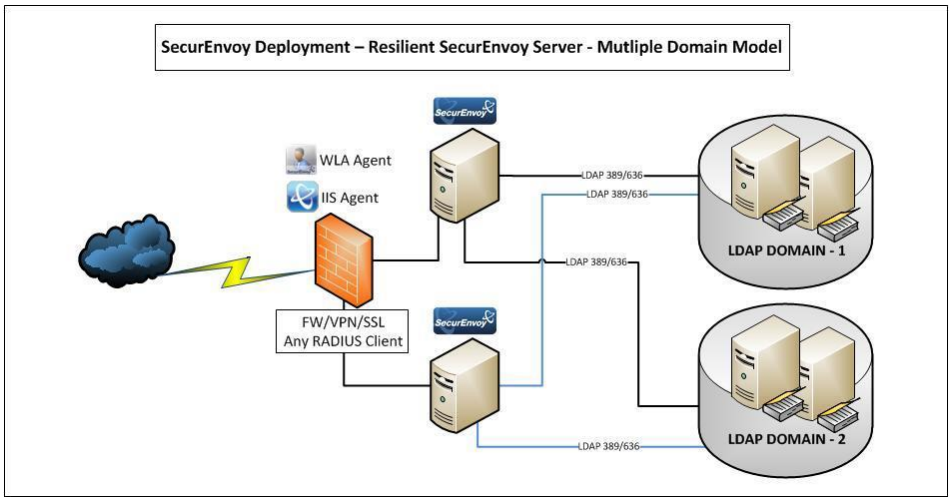
1) Single Security Server:



2) Multiple Security Servers:



3) or the Multiple Domain Model:



As a result of the integration into existing LDAP environments, companies and organisations benefit from reduced backup, management, administration and synchronisation workloads, as no additional hardware needs to be maintained. Moreover, they are leveraging the scalability and redundancy already in place by utilising, in the case of Windows, all the domain controllers already deployed. This also guarantees faultless functioning of the 2FA solution. In addition, the existing infrastructure includes all the important information such as name, e-mail and mobile number which can be used in real time from the same single LDAP source. The latter is important if the 2FA is carried out via SMS. In this context, SecurEnvoy provides a connection via over 30 Internet SMS gateway providers or via a Wavecom or Siemens modems. Via existing LDAP administration tools, the IT team is able to register new users for 2FA by joining them to a group, manage mobile numbers and e-mail addresses. The Windows (or other LDAP) passwords that already exist, which the staff previously used in order to log in, are also stored in the Active Directory. Unless otherwise requested, these passwords can simply be integrated into the SecurEnvoy technology and reinforced with passcodes. Thus users are not obliged to also remember a PIN or separate password and they can reuse their existing password. This means upgrades are very convenient too, as all the user data is controlled and preserved by your existing LDAP system.

Explanatory note: what are passcodes?

Passcodes allow users to confirm their identity when using the tokenless SecurEnvoy 2FA solutions. A passcode, which is a sequence of numbers, is entered in addition to a username and password when logging in. This allows the user to provide verification of his/her identity twice: once using something that he/she knows (user ID and password) and once using something that he/she possesses (smartphone etc.) and which receives the passcode. The patented tokenless SecurEnvoy method permits the receiving of the passcode via SMS, e-mail, soft token app, as input using a voice call or using "One Swipe". The latter involves a one-time QR code being read using the webcam on a laptop in order to prove the identity of the user.

Summary

It is undoubtedly the case that the amount of data handled by companies and organisations is constantly increasing. But dedicated databases are only required if considerable amounts of data are being handled. Otherwise, it is always advisable to make use of already existing infrastructure rather than further increasing the effort/expense of maintenance and administration. With 2FA, there is definitely no requirement for extravagant solutions, which means companies can save the money, time and effort that would otherwise be needed to set up new hardware or similar. One option is the approach offered by SecurEnvoy, which can be integrated into existing LDAP infrastructures, leveraging the existing scalability and resilience of these multi-server, multi-domain LDAP systems.