2013

FORESTSAFE

CASE STUDY 1

Password and document management in a government department.

ADRIAN OWEN
Entarian Limited
8/24/2013

Table of Contents

The organisation

The customer is a large government department in South East Asia. The department has several thousand staff working on many IT based projects.

Staff log on daily via Windows XP or Windows 7 computers; members of a Windows Domain. Hundreds of Windows 2003 and 2008 Servers are also domain members running IT services. They also have many non-domain windows computers and AIX servers.

Their computer management team are experts in infrastructure security and understand the importance of managing all ‘unmanaged’ computer accounts. They had gone some way to putting their own manual local password management in place, but it was expensive and problematic.

Entarian are unable to give details of the customers identity, at their request. But the issues and challenges they faced are common to any department.

All their account passwords are now managed automatically by ForestSafe. Streamlined password free audited approved access to all computer systems is available to their support teams. Configuring ForestSafe resulted in a saving to their departmental budget and resources.

The Issues

Main Issue

The main issue was managing the passwords of all local Administrator accounts on every Windows computer.

All their systems are ‘imaged’, Security Access Manages (SAMS) get copied, and so all local account passwords are identical.

This high risk security issue is common to all organisations.

Before ForestSafe was installed the department was forced to carry out a complex manual procedure

The manual procedure

- Every local Administrator password of several thousand computers had been individually set by a non-staff member.
- The non-staff member, from another department and building was escorted on site by security guards to a secure room to set the passwords.
- Passwords were written on paper, placed in envelopes and sealed in a safe.
- When support staff needed a password; e.g. changing a network card, they’d apply to their manager. If approved, they’d request the envelope from the safe to reveal it.
- When work was complete, the external staff would return and repeat the procedure.
- Same procedure existed for UNIX root accounts.

Secondary Issues

- They had Windows Services running as privileged domain accounts. These account passwords need to be synchronised, which is difficult and problematic.
- They had database accounts and Lotus Notes Administrator ID files passwords that needed managing.
- They had important digital documents and files spread over many different computers, and wished to make them accessible based on approved requests. To create a secure, central documents store, with the security and cost benefits that would bring.

The Solution

Entarian helped them write a detailed implementation document, describing the ForestSafe configuration required to manage the system. They implemented on a 3 tier configuration, locally on Hyper-V Windows 2008 R2 servers.

Challenges

Decommissioning the manual system

ForestSafe now manages every local Administrator accounts of ALL their legacy computers, domain, workgroup and root account on their AIX servers and Lous Notes Administrator ID passwords It is fully automated, and monitors for new computers discovering and managing them. The manual system has been decommissioned

Value Additions

Support staff no longer retrieve passwords, but prefer to login automatically via a ForestSafe Remote Terminal session. UNIX staff launch SSH sessions with X-Term, without any password required. All access is audited and managed.

Improving and securing the support procedures

The department wished to keep projects computers and support staff accounts, segregated by project, for safe controlled access by the support teams. Before ForestSafe this was impossible to achieve.

They use ForestSafe by creating an Active Directory group for every project. They incorporate the project name in the group name, and make all project domain computers members of this group. They also make the domain account of the staff that will support the projects members of this group. Users and Computes all managed by an AD group.

Value Additions

After logging into ForestSafe, support staff chose the project they wish to manage. The system shows only computers and account for the selected project. Moreover some project computers are in the test lab, and do not require approval before logon, these are put in a separate AD group. Dozens of teams with differing support requirement are all mapped in this way, completely segregated.

Non windows domain computers have also been joined to AD groups ‘virtually’ through the ForestSafe container system. A container is an access list of computers or group or ipaddress or OU both UNIX and Windows mixed if necessary. Containers can contain other containers so that powerful access hierarchies can be configured.

Remote Access Approval process

If a support person applies for approval to remote control a live server, they require that email alerts are sent to all interested parties, at every stage of the process.

> *Value Additions*
>
> *Following the approver granting approval, the support user receives their final 'granted' email confirmation. They click a link in the email and log in directly to the remote system, no password is required. A minute after logon, ForestSafe changes the password. It automatically closes the session after the required time. Password free logon to AIX through X-Term is supported in the same manner.*

Central Digital Document Store

They are importing critical digital files into the ForestSafe Binary Large Object (BLOB) store. These file were spread over many desktops and servers.

> *Value Additions*
>
> *Every file import, export and removal requires approval by a manger. Documents are removed from disk after import, for security. Some team only have import and removal access. Other end-user teams have export only.*

Conclusion

For more information, please visit our web site http://www.eesm.com ,

UK government departments can logon to the Cloud Store portal http://govstore.service.gov.uk/cloudstore/ and search for ForestSafe.

Government Procurement Service supplier