Configuration Management using Sysgem File Synchronizer (SFiS)

What problem is being addressed?

Computer networks with distributed multi-platform servers can demand a lot of management effort to ensure that they are configured correctly. Often, there are many configuration files on distributed servers that need to be monitored and managed to ensure that the servers perform correctly and that security is maintained.

As the numbers of servers grow, so too does the management effort required. This growth is often exponential and the task of maintaining server integrity and security becomes unsustainable using traditional management techniques.

How does SFiS solve this problem?

Sysgem File Synchronizer (SFiS) keeps a central copy of a file that we call a 'policy source file'. The content of this file is compared to the content of text files held on multiple distributed servers. SFiS produces a report showing whether the distributed files on the target servers match the central policy file. Those files that do not conform may be selected in the report and menu options used to update the target files so that the configuration policy is maintained throughout.

Note that this task is conducted from the one central location. There is no requirement to log in to the remote servers either to verify the correctness of the distributed files, or to update them when they are found to differ from the policy file.

To allow for variations between the different distributed servers, the central policy source file is more than just a text representation of the files on the target servers. It includes a very simple (one character) meta-language definition that describes file differences for different groups of servers. This provides both flexibility and brevity for the centrally held policy source file.

What other software is on the market?

There are two other products available that address the same problem: "CFEngine" and "Puppet". However, both these products are very complex to use (even though they claim to be simple). The origins of SFiS began when a Sysgem customer asked for a new solution because these alternative products were just too complex; didn't maintain an audit trail; didn't allow delegation with varying levels of access control and privileges; and thereby didn't provide enough security to be deployed on a large network for use by multiple people with varying degrees of technical expertise and management responsibility.

What are the key features and benefits of SFiS?

i. Interactive access:

- Central policy files are compared against the content of designated files on target servers and a report on their conformance is produced
- Target files are updated when their content does not conform to the central policy definition
- Simple to use 'pattern matching' shows variances to allow known exceptions

ii. 24/7 Automatic Monitoring:

- Unattended, automated monitoring of target files and automatic raising of alarms when variances are found
- Alarms may be configured to notify via email

iii. Policy files held in a central file cabinet:

- Share central file cabinet drawers between users / private drawers
- Structured folder system for platform variants / policy files / include files / script files

iv. Simple meta-language:

- Define which target servers should be compared / updated
- Define groups of servers for brevity
- Define content of target text files in a central policy file
- Define text variations between servers or groups of servers
- Define text substitution variables for comparison & update
- Simple, single character meta-language clauses
- Validation of policy file format

v. Possibilities for delegation:

- Full Access
- Read-Only Reporting
- Restrict access to nominated servers
- Restrict access to nominated files
- Restrict access to nominated meta-language clauses
- Restrict access to O/S Scripts

vi. Full auditing:

- Source File edits
- Target File Updates
- Who did what; when; with which source files; to which target servers & files

vii. Security:

- Full authentication of users (login via username and password)
- Full authentication of target agent and central console software
- Encrypted communication messages
- SSH or TCP/IP protocols
- SSL in V3.0, plus message certificates
- Proxy server options to protect mission-critical servers
- Agent configuration limits access from defined IP addresses only

viii. Expandability:

- If your requirement is for more than just text file synchronization, the same basic Sysgem software framework that is installed with SFiS can be expanded by the addition of other Sysgem modules for applications such as: User Account Management; Identity Management; Systems Management; Monitoring; etc.