GFS SOFTWARE

SYSchange®

Compliancy and Deployment Management

Technical Datasheet

Higher demands for security and compliance in data centers require the process of deploying changes to be managed, controlled and verified. SYSchange provides a sustainable compliance and deployment capability, including change and configuration management integrated into the day-to-day operations of the z/OS mainframe data centers.
With a comprehensive set of process driven change management tools, organizations are able to comply with strict industry mandates and audit requirements more efficiently, while being enabled to deliver developed enhancements and required maintenance quickly and safely.

The SYSchange Solution

SYSchange is a System Software Change Control and Management solution for the z/OS designed to address three specific areas of a data center operation, i.e. **Compliancy Management, Deployment Management, and Application Lifecycle Management.**

SYSchange eliminates risks, improves systems availability, achieves maximum compliance and accelerates software change distribution. It is designed to help data centers implementing an automated, integrated and transparent solution to centrally monitor, control, and manage changes. It also packages and deploys authorized software changes across systems, LPARs and SYSPLEXes.

"SYSchange is versatile, automated, proactive and transparent by design," according to Michael Madani, Pristine Software's President and Chief Architect of SYSchange. "Data centers seek super-fast, reliable, repeatable and verifiable technologies which can cut costs, increase productivity, enhance operational efficiency, and provide management with a birds-eye view of system-wide changes. Our solutions have been used by major financial and other corporate institutes world-wide since 1992."

SYSchange Integrated Components

SYSchange has two integrated components in the areas of systems software and application software change control and management:
The Compliancy and Deployment Component and The Developers Workspace.

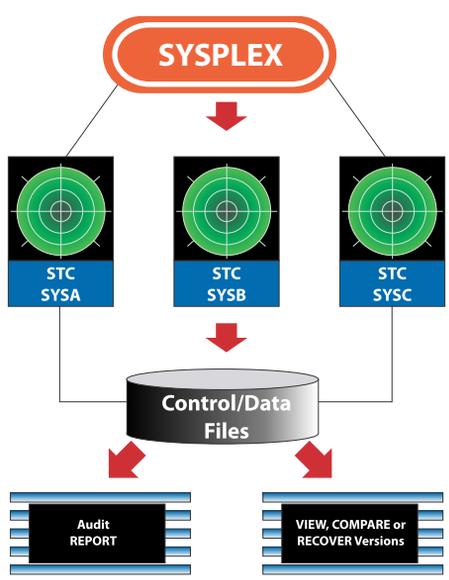
Never miss any changes with Automated "Packaging and Deployment"

Pristine Software

The Compliancy and Deployment Management

The ***Compliancy Management*** enables data centers to protect their critical systems libraries. Once a library is "protected", every time a library member is updated, the SYSchange Started Task (STC) automatically captures the changed member and stores it in the SYSchange repository.

The diagram below depicts a SYSPLEX environment with three systems. The SYSchange STC is set up on each system, controlling the changes to the libraries in its protection list.



By capturing member-level changes automatically, and in real time, users will be able to revert to a prior member version by recovering it from the SYSchange online repository. Collected member versions are displayed online, where users can compare any two versions to see the change details to determine the desired version for recovery. With a single click, the selected version is recovered.

SYSchange provides systems administrators a non-intrusive process to effortlessly document their work just prior to saving an edited member of a protected library. The user-supplied notes for the introduced changes are automatically augmented to the created member version, which is stored in the SYSchange repository, viewable at any time in the future.

The Configuration and Change Control feature in this component of SYSchange enable systems administrators and operations control managers to grant authorization to update to certain library members while blocking other members in the library from update access.

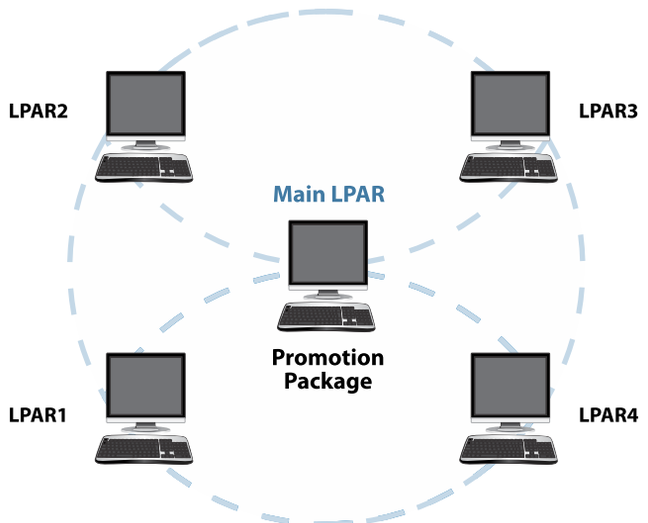
A summary of the functions in the compliancy management include:

- Member-level change activities are recorded by the SYSchange Started Task on a constant basis
- Automatic backup of changed members; no changed version is ever lost whether the change is introduced using ISPF or batch functions (source and load modules)
- Ability to document changes online as the change is introduced
- Online view of contents of member versions enables users to recover the right version with certainty and without any guesswork
- Member-level protection against unauthorized change; by using the LOCK feature for certain critical libraries, only authorized users will be allowed to introduce changes

The ***Deployment Management Component*** provides a central approach for developing changes, and packaging and distributing the software changes to multiple environments. One of the biggest challenges for today's z/OS data centers is adopting a deployment tool, offering consistent and reliable processes for distributing software changes to multiple systems from a central location.

Whether the changes are occurring in ISV products, in-house developed products, or IBM delivered software maintenance (PTFs), the tool must be capable of handling all such changes without discrimination.

A practical deployment solution must be auditable, repeatable, and reversible if things go wrong. SYSchange's advanced deployment functions offer a practical and cost effective way to meet all these challenges and more.



The SYSchange Deployment Management enables data centers to automatically identify and package the changed components introduced in a software environment. Using this technology, environments of any size and configuration (multiple systems, multiple LPARs, and SYSPLEXes) are synchronized. Automated synchronization of software environments is important to protect the state of production environments and ensure that changes are correctly and consistently deployed.

"At Rabobank we use SYSchange Advanced Deployment as a standard tool for our software distribution. SYSchange also complements our full volume copy and our other home-grown tools by effectively controlling and preventing regressions."

Top 3 Uses of the SYSchange Compliance Management

1. Automatic Member-level Backup and Recovery of Critical Systems and Application Libraries

Once a critical library has become protected by the SYSchange Started Task (STC), SYSchange automatically and transparently backs up the changed member to its repository every time a change is introduced, regardless of the method of introducing the change (ISPF or batch). Thus, users are enabled to recover from an undesired change online.

2. Auditing of All Real-time Changes and Verifying Software Integrity

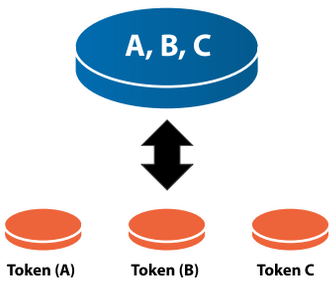
The SYSchange Started Task monitors real-time change activities for protected libraries. SYSchange provides two approaches to auditing.

1) In the first approach, users protect critical libraries using the SYSchange "protect a resource" function, thereby requesting the STC to record member-level changes in real time and back up the changed members to its repository. This approach is recommended for volatile systems libraries, such as your PARMLIB, PROCLIB, JCLLIB, LINKLIB, etc. Real-time tracking allows you to audit your critical z/OS libraries by identifying who has made the change.

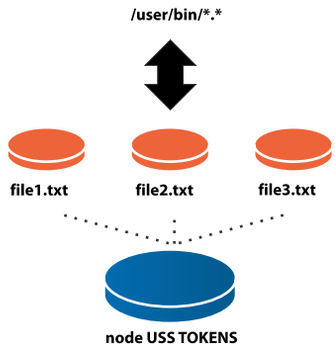
2) The second approach to auditing software changes can be used both within and between environments. Using the SYSchange tokenization technology, patterns of datasets or patterns of USS directories are tokenized to establish "content reference tokens" for each library member or the USS file, or to establish one token for the entire file (such as a physical sequential file).

These reference tokens representing the contents of the files at the exact time of tokenization are stored either in the SYSchange control file, or on an external file referred to as a "token file".

Tokenize a PDS or PDSE



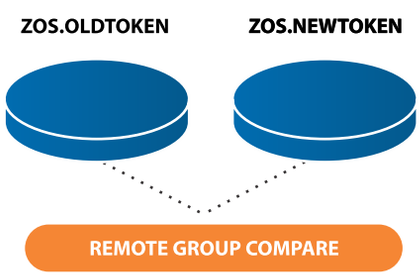
Tokenize USS Directories



- **Compare:** Referring to these token files, installations may run the SYSchange "group compare" function, or the "Path Compare" function to identify and report any changes introduced in the entire z/OS environment, or the entire USS environment since the environment has first been tokenized.

- **Verify Integrity:** The same process can be used to verify the integrity of a z/OS software environment, or a USS environment over time. By re-tokenizing an environment, creating a current token file, and comparing it with its original token file, any changes are identified and reported. Lack of change in the report guarantees the integrity of the software environment.

Comparison of z/OS environment



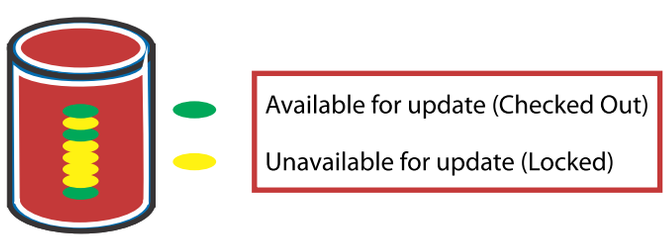
3. Configuration and Change Control Using the Locking Mechanism

LOCK=NO: When a resource is protected using the LOCK=NO parameter, all members of that library remain available for update by any user. Once the change is made, upon pressing PF3 or issuing the SAVE command, optionally prompted to document that change. Using the "Check Out" function, however, the SYSchange Global Administrator may grant exclusive ownership over certain members or member groups in this library. Such members will only be available for updates by pre-designated users or a RACF group. The benefit of this approach is that it provides the freedom to selectively freeze certain library members.

LOCK=YES: In this type of protection, all members of the library become unavailable for update except the ones explicitly "checked out." To enable users to update the library, the SYSchange Global Administrator may grant *exclusive ownership* over certain members or member groups. The following diagram shows the opposite of the previous case.

PDS with LOCK=YES

All members are locked except the ones "Checked out"



"The high number of LPARs coupled with the constant changes being introduced to those systems, make the tasks of security and change control a daunting one at best. This is because traditional products do not offer an automated and transparent process for tracking changes that take place in every corner of our data center. Inherent to this challenge are the enormous resources that are ordinarily required to achieve such ends."

"At Rabobank, one of our imperatives was to acquire a solution offering a comprehensive set of change management technologies that would help us gain control of change and keep us at the helm."

"SYSchange has provided us the assurance that all system-wide activities are centrally monitored, backed up for recovery purposes, and quickly reported."

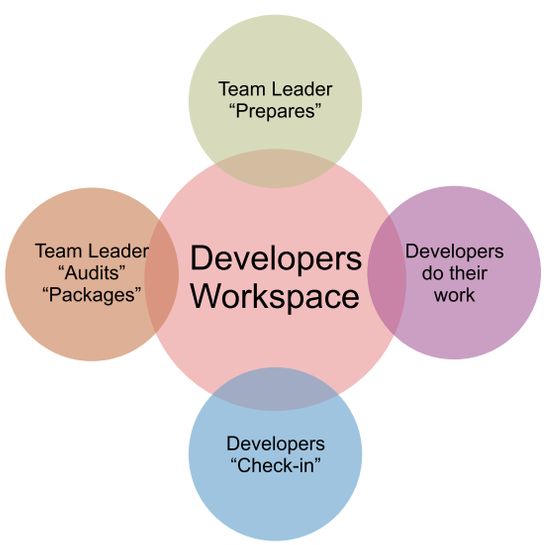
The SYSchange Developers Workspace Component

This component of SYSchange enables application developers to develop code in a secured environment, and then deliver the developed application to multiple environments via the SYSchange "Packaging" and "Promotion Processes".

First, a team leader "Prepares" an application providing exclusive ownership to the components to be developed. Then, the developers start their development work while they have exclusive control over the components being developed. When finished, they "Check-in" their developed work and notify the team leader. Finally, the team leader "Audits" the changes and automatically creates the SYSchange "Promotion Package" for the application.

These packages, containing only the changed components must be approved are transferred to the TEST system for testing purposes. Once, the testing is complete, the same package is sent to the QA system and finally to the production system.

This component is used by medium size mainframe development shops who seek replacements for their CA/Librarian, CA/Panvalet, CA/Endevor, their home-grown Change Management solutions, and other ALM products.



VSAM Change Manager Component (Release 4.2.0)

The "VSAM Change Manager" component of SYSchange enables data centers to identify and report record-level changes in VSAM clusters. Users can create a "full" backup for all VSAM types (KSDS, RRDS, ESDS and LDS) and "differential" backups for KSDS and RRDS. Once the backups are created, they can be "packaged" and "promoted" to synchronize similar VSAM files on local or remote systems.

This component is recommended for data centers that require transfer of their VSAM record-level changes to distributed environments, or to other VSAM files on z/OS to synchronize. Transferring or downloading only the changes in VSAM files dramatically saves time and resources as well as meeting auditor's requirements to identify record-level changes in VSAM files.

As an additional feature for auditing and security, administrators can set up an Email Alert to notify select contacts of changes made to highly critical libraries.

GFS Software Company Overview

GFS Software is an Advanced-level IBM Business Partner and a leading developer of tape management software for the IBM z/OS environment. Founded in 1988, GFS has over 25 years of experience in developing quality software solutions that produce measurable cost savings while increasing software efficiency.

Some of the largest z/OS installations, with the largest tape storage-environments, rely on GFS solutions to maintain and improve operational optimization, including financial services, telecommunications, and governmental organizations.

GFS Software, Inc. is an authorized distributor of SYSchange.
SYSchange is a product of Pristine Software Company LLC.

www.gfssoftware.com

GFS Software, Inc.

1133 Broadway, Suite 310
New York, NY 10010
Phone +1 212 659-2220
Fax +1 646 786-4174

e-mail: gfs@gfssoftware.com
www.gfssoftware.com

December 2015