



z/OS Change Management Issues addressed by eventACTION

eventACTION and **ussACTION** are comprehensive event tracking and control products that can help you pro-actively manage and audit your z/OS environment with real time capture of any change, reference, or execution to any system level data. Due to the manner in which the controls are implemented system datasets can be protected against unauthorised and undocumented changes. In fact once a dataset is placed under **eventACTION** controls, it is no longer possible to change this dataset or any of its members unless the relevant change request exists and has been authorised. The reporting tools provide a complete and accurate picture of all changes made to the structure of the system, both for MVS and UNIX System Services changes.

What are the risks and exposures in other Change Management products?

The majority of Change Management products are really only electronic paper systems that rely heavily on ITIL and of course that the personnel stick to these guidelines implicitly. Unfortunately guidelines provide no guarantee that changes are not made outside of the stated guidelines. In fact some experts estimate that the number of unauthorised and undocumented changes is as high as 30%. One single unauthorised or undocumented change can lead to a complete outage of a system, which in turn can cost millions of Euro per hour, not to mention the damage to the customer base and the corporation's image.

If we take a look at this potential 30% of unauthorised or undocumented changes, then we can immediately see that there are more far reaching effects, such as:

1. The increased risk of system outages, application outages, product crashes and incorrectly working batch processes. All these can lead to a loss or corruption of data, loss in confidence of the customers and loss of revenue.
2. The information required by both the internal and external auditors is wholly inadequate, incomplete and requires an enormous amount of resources to attempt to provide a complete and accurate picture. This however would in any case prove to be impossible as many of the changes have not been tracked or recorded. Of course such audits, whether internal or external, will account for a huge amount of resources in time, manpower and costs.
3. As these products neither track all the changes nor prevent unauthorised or undocumented changes, they are open to malicious manipulation. A clever programmer can make changes in the system that would allow him to destroy all backups over a period of time before destroying the current systems. The result would be that the organisation would lose all its computing power, all of its systems and probably all of its data. The logical result of this would be – Bankruptcy.
4. Relying on ITIL procedures and the threat of dismissal for abuse of the Change Management processes only has any real effect when you are in the position to identify these abuses. In reality unearthing these abuses will only happen when it is too late and the systems and applications have already been impacted. In other words these processes are at the best retro-active and not real-time or pro-active.
5. As these systems can be bypassed there is absolutely no guarantee that the data gathered and approved by quality assurance represent the actual state of the programs and applications. This opens another avenue of manipulation that can lead to theft of customer data and even to theft of real money.

What improvements are provided by **eventACTION**?

As **eventACTION** tracks and records changes made to datasets etc. and works pro-actively in real-time it has the ability not only to record but to block any potential changes. This real-time control has the following advantages:

1. Once datasets/members or directories/files have been defined to **eventACTION** they can be tracked and controlled at various levels:
 - a. The lowest level of tracking is just to record a STATistic record whenever a dataset or member is either changed or referenced.
 - b. The next level would be to take Backups of the changed data, which at a later point in time will allow older versions to be restored.
 - c. The next level is to force the users to provide a Change Request. Once this level has been activated, no further changes can be made to this resource without the Change Request being present.
 - d. Next we add authorisation, single or multiple, to the Change Request. Now the Change Request has to have been authorised before the change can be made.
 - e. Finally the Change Request can be coordinated by the Change Coordinator. This ensures that changes to critical applications or Batch programs are made at a time when they cannot impact these applications or batch suites. These changes cannot then be made outside the scheduled window.
2. Trusted programs that track their own changes can be excluded from **eventACTION** allowing the user to define whether statistics or backups should be taken and if the change controls should be bypassed. In other words programs such as SMP/E or CA-Endevor can monitor their own changes, but the target production datasets can still be monitored by **eventACTION** for changes made by other means. Naturally all this tracking and change information can also be recorded by **eventACTION**.
3. Once all the datasets/member or directories/files that are critical or important to the running of the system, applications, products or programs (including CLISTs, REXX EXECs, JCL, Parameters etc.) have been defined with their various levels of control (Change Request, Authorisation, Coordination) and their tracking options (Statistics, Backups or References), the system should be vastly more stable.
4. The risk of manipulation should be greatly reduced as each form of manipulation, if not already prevented, will leave tracks that can easily be located. Knowing this will almost certainly persuade the potential manipulator to cease.
5. Now that all the critical and important changes are being tracked and backups are being taken, if a problem does occur it is easy to revert to a previous state by backing out the changes to a version that works. Also should a dataset or member become damaged or lost, then this can be recovered back to the point of impact, rather than the point in time when the last full backup of the dataset was made.
6. Auditing now becomes very fast and simple due to the fact that all the changes are recorded with or without backups as defined either by the auditors or the organisation itself. There are now no more undocumented changes to critical or important elements, unless of course these have been omitted from **eventACTION**'s controls.
7. Despite the fact that the change controls are inactive when the started task is stopped, recording of these changes continues. Thus the major method of manipulation – Stop the task, manipulate the system, start the task – no longer works as all the changes will be recorded, thus unmasking the manipulator.
8. **eventACTION** provides real-time pro-active protection, reducing outages and problems, providing more stability and availability, improved security with controls at the member level, reduced risk of manipulation and an improved customer satisfaction and corporate image.

Potential Savings through **eventACTION.**

Reduced Outages: With the implementation of the Change Controls no unknown or undocumented changes can be made to the datasets that are critical to the well being of the system, products, applications or batch programs. As the changes are all known, documented and have been controlled by the Approvers, errors leading to potential outages are avoided or at least greatly reduced. Unlike electronic paper driven Change Management systems that cannot prevent unauthorised and undocumented changes **eventACTION** assures that all changes are recorded and backups are taken where required. Through real time controls and proper checking of changes by the Approvers, outages and problems can be reduced to an absolute minimum. Each outage has the potential, of costing an organisation millions of Euro per hour, of alienating its customers and finally of damaging the corporate image.

Faster Problem Resolution: Because **eventACTION** tracks and optionally records all changes in the system, this information is immediately available if and when a problem occurs. Using the SCAN function the potential cause of the problem can be quickly identified and through the stored backups immediately be reversed out to the previous working version. Whereas before just the process of locating the source of a problem could have taken hours or even days with many people working on resolving the issue, now the identification and repair of the problem can be handled by one person in minutes. Though the man hours saved do not actively represent a saving to the organisation, unless of course the headcount is reduced, the saved man hours can be put to good use on other projects.

Compare Utility: The Compare Utility has a unique side-by-side display facility for pointing out differences between files. This side-by-side display allows changes to be identified much faster than previous types of compare output. Just the compare utility can save hundreds of man hours each year. It can be used online to compare members of libraries or **eventACTION** backups of members. It can compare all or a subset of the members of two different libraries to indicate which members are the same or different. This utility can be used to investigate problems, to see how something was last changed, or to see how one system library may differ from another. In batch mode, entire volumes may be compared or sets of datasets via the Catalog. This is an absolutely essential tool for auditors when they are trying to track down what changes were made that led to a system and/or application outage.

Restore: Any organisation that has experienced the loss of a dataset or even a whole disk knows that recovering the data without RAID Disks or Mirroring is virtually impossible and the recovery of what can be saved is hugely time consuming and labour intensive. With **eventACTION** this problem is literally eliminated as all the backups up to the point of impact can be restored over the last valid disk or dataset backups. To restore the contents of a dataset to the point of impact once the last valid dataset backup has been restored can be achieved in a matter of minutes. Prior to **eventACTION** one would have tried to reconstruct what changes had been made and to manually re-apply these changes. However, this reconstruction would be done without any certainty that all, especially the undocumented, changes had been re-applied. This could again lead to further problems and outages.

Manipulation: The dangers of manipulation and subsequent destruction of systems or parts of systems are mostly perpetrated by insiders. A well versed systems specialist can, without the presence of **eventACTION**, manipulate datasets or members of datasets without leaving any recognisable traces or can implement SVCs on a temporary basis to bypass security or other controls. As **eventACTION** tracks all these changes, the risk of manipulation is greatly reduced as the perpetrator must assume that the traces left behind can and will be identified thus resulting in his or her identification. Manipulative attacks can be many times more serious than a system outage as this could well lead not only to the loss of the system but to the backups as well. In end effect the system would need to be re-built from scratch. The monetary losses here are incalculable and could easily lead to failure and bankruptcy of the entire organisation.

eventACTION includes the following:

Change Tracker automatically and transparently tracks and records all changes to defined data sets down to a member level, regardless of what program was used to make the changes.

Change Manager is used to control changes, according to criteria specified by you; ensures that any changes are logged / documented in a change request, and optionally, approved.

Unlike other change management products, **eventACTION** does not require the use of specific tools to make changes. It works transparently regardless of the tools used, so that all changes made are tracked, providing a comprehensive picture.

Command Manager allows an installation to track and/or control operator commands; provides capabilities similar to Change Tracker / Manager for operator commands. Since an operator command can implement a change, this is an important control point.

Reference Tracker allows an installation to track all references to defined data sets and PDS members; and can be used for library cleanup, program usage measurement and product execution control.

ussACTION provides the **Change Tracker**, **Change Manager** and **Reference Tracker** in the same form as **eventACTION** for z/OS UNIX System Services.

With its numerous other features (such as a unique side-by-side compare utility, automatic batch job scheduling, extensive reporting functions, and flexible backup/recovery options) **eventACTION** is a self-contained and fully integrated management solution to provide dynamic change tracking, control, and distribution for single or multiple site MVS systems.

Summary:

At the end of the day **eventACTION** provides:

- System controls to assist in z/OS compliance
- Complete / secure audit trail
- Basis for software asset management
- Assure Software providers that their products only run on licensed systems
- Powerful compare facility
- Reporting for all data thru online, batch, email, scheduled
- Investigate 'incidents' real-time (changes, program usage, operations)
- Repository for z/OS system data
- Interfaces to your current processes & procedures



Copyright © 2010 Action Software GmbH
May not be reproduced without permission.
All rights reserved.

If you want more information about **eventACTION** please contact:

Action Software GmbH
Alte Steinhäuserstr. 1m CH-6330 Cham, Switzerland

Tel.: +41 41 748 6266

Fax: +41 41 748 6267

E-Mail: Marketing(at)actionsoftware.ch