



z/OS Problem Solving Issues addressed by eventACTION

eventACTION and **ussACTION** are comprehensive event tracking 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. 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 steps are taken to resolve a problem without eventACTION?

Using the currently available resources to locate and resolve a problem can be very labour intensive and time consuming. Normally the following steps would need to be taken:

1. Identify the problem – Product, Program, Application or Datasets affected.
2. Try and determine what changes were made in these areas by looking at the “Change Management” information. This, without **eventACTION** is almost certainly an electronic paper driven system that sometimes bears little in common with reality as changes can be made outside of these controls.
3. If the change cannot be identified from the “Change Management” system, then the next step would be to examine the product/application program and parameter datasets to see if any changes were made. Again, this change data may or may not exist. If nothing can be found here, then a further step could be to examine the SMF data to see if any update accesses had been made. Unfortunately, the update access only shows that the dataset was opened for update, not specifically that any changes were made, especially as this information is only recorded on the dataset and not the member level.
4. Having exhausted all these possibilities, the search for the error would have to proceed to asking the various people in the groups who had Update access to these datasets, and
5. in parallel to examine the SYSLOG for any suspicious commands, and
6. also to examine the Dump if one was written.
7. By now there would probably be 2-5 people working on the problem and anywhere from 30 minutes to 2 hours would have passed.

In the end it is clearly not possible to say how many man hours are annually wasted on researching and resolving problems that could have either been prevented, or in the case that the problem still occurred, been resolved in a matter of minutes.

What steps are needed to resolve a problem with eventACTION?

As **eventACTION** tracks and records changes made to datasets etc. that the user has deemed as being critical or important to the running and stability of the system, applications and programs, locating and fixing the problem is relatively easy.

1. Use the SCAN function in **eventACTION** to shows where changes were made in the area affected.
2. Localise the actual change
3. Restore the previous version and restart the program or application

The elapsed time should be in the range of 1 to 10 minutes.

Naturally due to the real-time protection and change controls, most of the problems experienced in the past would never happen, as there would be no changes to critical or important elements that would bypass the "Change Management" controls. Once these controls have been implemented, no further changes are possible to the protected datasets unless the requirements (see below) have been fulfilled. This means that all changes are controlled, recorded and fully documented. There is no longer the risk that a change can be made outside of the "Change Management" system. This is an essential pre-requisite for CobIT, Sarbanes Oxley (SOX) and any other forms of Compliance. Also the tracking and controls result in a complete and accurate audit trail of all changes made, thus simplifying the task of the auditors. In the event that these are external auditors, this should also reduce the cost of the audit.

Please also be aware that tracking of changes will continue even if the **eventACTION** STC (Started Task) is stopped. However, it should be in the auditors interest to implement an alert if this task is stopped and then to determine why this was done.

Potential Problem Solving 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. Im CH-6330 Cham, Switzerland

Tel.: +41 41 748 6266

Fax: +41 41 748 6267

E-Mail: Marketing(at)actionsoftware.ch