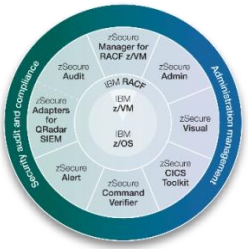


IBM Security zSecure Newsletter – Issue 22, 2015

A very warm welcome to the latest zSecure Newsletter.

We are pleased to announce that the 5th zSecure User Group meeting will run across various countries this year, starting off in London and Frankfurt. Keep reading this newsletter to find out more.

You may have heard that Glinda Cummings retired from IBM at the end of 2014 – many of you know that Glinda was our Worldwide Product Manager for zSecure. I hope you'll join me in wishing Glinda a long and happy retirement, plus a big thank you for all her hard work and dedication to the z business over the years.

So you may be asking who replaced Glinda? I'm pleased to confirm that I have taken on the role. Yes after 18 years of working with zSecure, starting life as a RACF Administrator, I'm the new Worldwide Product Manager for zSecure.

Thanks for reading!

Best wishes

Jamie Pease
Worldwide Product Manager for zSecure

In this edition . . .

zSecure User Group 2015 - Europe

The 5th zSecure User Group will take place on the following dates:-

Frankfurt - 25th & 26th June
London - 30th June & 1st July

You are welcome to attend the event in either City – please click on your preferred City above to find out more about the event.

The User Group is an excellent opportunity to hear first-hand from development about new functions and features, how to get the most from your existing implementation, plus presentations from Business Partners and customers. There is also an opportunity to tell us your requirements for future releases.

zSecure User Group 2015 - Worldwide

We are planning to run the zSecure User Group in the following cities in Q3 and Q4 of 2015:-

Atlanta, US	- 16th November
Canberra, Australia	- 9th September
Los Angeles, US	- 18th November
Melbourne, Australia	- 7th September
New York City, US	- 11th November
Sao Paulo, Brazil	- Date to be confirmed
Singapore	- 18th September
Sydney, Australia	- 14th September
Washington DC, US	- 13th November
Wellington, New Zealand	- 15th September

The agenda and registration details will be made available over the next few weeks.

New release for zSecure Manager for RACF z/VM

If you are running z/VM in your environment, you may be interested to know that a new release of zSecure Manager for RACF z/VM has become generally available. The new release, 1.11.2, is based on IBM Security zSecure Suite 2.1.1 (for z/OS) and introduces the zSecure Audit Compliance Testing Framework to the z/VM operating system.

Our zSecure Development Manager, Jeroen Tiggelman, created a blog about the new release on developerWorks – click here to read it.

New Redbook, Security on the IBM Mainframe ……

A new Redbook is now available to download, titled *Security on the IBM Mainframe, Volume 1 A Holistic Approach to Reduce Risk and Improve Security.* This publication explores how System z hardware is designed to provide integrity, process isolation, and cryptographic capability to help address security requirements. This book highlights the features of IBM z/OS and other operating systems, which offer various customisable security elements under the Security Server and Communication Server components. This book describes z/OS and other operating systems and additional software that leverage the building blocks of System z hardware to provide solutions to business security needs.

Performance improvement for zSecure

A performance improvement was recently made available to speed up processing for CARLa queries using z/OS UNIX file data. If you are using zSecure 2.1.0 or 2.1.1, we recommend you look at the service provided through APAR OA46606. Please check out our zSecure blog area for more details.

What functions and features would you like to see in a future release?

As the Product Manager for zSecure, I'm responsible for reviewing your enhancement requests. So if there are functions and features that you would like to see in a future release of zSecure, here is a gentle reminder to submit a Request for Enhancement (RFE).

IBM z Systems Security Conference

The IBM z Systems Security Conference will be held from 29th September to 2nd October – this will take place at the IBM Client Center in Montpellier, France.

Cloud, Analytics, Mobile and Social all have one thing in common: they need a platform that has a deeply integrated security stack. This is where IBM® z Systems™ excel. To help counter the many threats to your business in the current world, including hackers looking to penetrate your systems and government backed attacks, z Systems offers a platform with layers of defense to protect your data, intellectual property, and your reputation.

Join us in Montpellier to find out more about how to meet these security challenges with z Systems and discover the new z13 machine and the latest version of z/OS in its version 2.2. Like previous years, we expect more than 100 attendees including Customers, Business Partners and IBMers. Security experts from the IBM z Systems community and labs will share their experience and expertise.

There is no charge for attending this event, however attendees need to cover all transport and lodging expenses.

For more details including registration, please click here.

2015 IBM Systems Technical University

The 2015 IBM Systems Technology University Conference will be held from 5th -9th October at the Hilton Orlando, Florida. The 2015 IBM Systems Technical University is a best-in-class event featuring IBM z Systems and IBM Power Systems. This 4.5 day event is designed for technical and professional development in IBM Systems -- allowing you to take a deeper dive into smarter computing implementation, product announcements, and, key topics across the z Systems and Power Systems platforms.

There will be an entire track at the event dedicated to z Systems security with subjects spanning cloud, mobile and data security covering strategic products including encryption, IBM RACF, IBM Security zSecure, IBM Security Guardium, IBM Security QRadar and more. Here is the link to the event website.

GSE Annual UK Conference

The annual GSE UK Conference will take place on the 3rd & 4th November at Whittlebury Hall, Whittlebury, UK. As usual, the Enterprise Security Working Group will have a 2-day security track – the agenda and registration details will be available on the conference website over the next few weeks, so stay tuned.

New white paper: Maximize mainframe security to reduce risk with 10 best practices

A best-practices approach to managing risk can help organizations maximize mainframe security, enforce security policy, enhance security intelligence, detect vulnerabilities, and reduce risk. Read our new white paper to learn how to:

- Establish security policies to better protect sensitive and critical assets
- Comply with industry standards and regulations
- Understand and control potential threats and vulnerabilities

New Video: Best Practices on Risk Management for z Systems Security

IBM z Systems provide the ultimate security platform with 80% of mission critical data originating or residing on mainframes. The mainframe is the workhorse of the enterprise acting as a central processing hub for essential mobile, cloud and data analytic applications. Learn 10 best practices on how organizations can reduce the risk for systems, applications and data residing on the mainframe with IBM Security zSecure, Guardium and QRadar solutions. Watch Jamie in the new video on YouTube: Best Practices on Risk Management for z Systems Security.

zSecure Beta Program

The next release of the IBM Security zSecure suite is currently under development. We would like to invite new and existing zSecure customers interested in getting early experience with this product and providing development their feedback. The Beta Program has just started and will run through to the end of the year.

The Beta participants will experience the following benefits:

- The opportunity to discuss problems and share ideas with product experts from IBM and with other customers, via web conferences and an online web-based Discussion Forum.
- The ability to install, configure and/or evaluate the new product code in their own test environment to validate new functionality and ensure the product works in their environment before the product goes GA.
- Dedicated support provided by Development for the duration of the beta program, via an online web-based Discussion Forum.
- An opportunity to influence the product function and future directions.

What do we expect from the beta participants?

- Download the beta code drops and install them
- Test out the functions that are important to you and post any problems and questions to an online web-based Discussion Forum
- Provide occasional status by submitting an online Feedback form when requested by us
- Consider being a reference at the end of the beta program if your company has a positive experience

Interested? Please submit the online beta program nomination form by clicking here.

Static Security

I recently attended a lecture at the British Computer Society where I heard the term “static security”. Basically the lecturer was talking about those legacy systems/applications that our businesses are still heavily reliant on, where security has not changed since their inception. So for example you may have built an application in the 80s, however the security for it has not been redesigned to factor in the threats of today - so in reality the controls do not align with current policies and standards. Sound familiar?

After the lecture had finished, it was proceeded with a networking event where I got talking to a few security and audit professionals. We all collectively agreed that the term “static security” was probably a good term to use in justification documents, or discussions where we are trying to convince our management to make investments in security.

The word static means lacking in movement, action or change. So if you think about security and the world we live in today, the two words don’t mix. Now, how about using “dynamic security” – dynamic means change, activity or progress – far more positive I’m sure you’ll agree.

So thinking about the critical systems, applications and data you are responsible for securing, are any of these running with static security? A few I suspect. I doubt any security manager would warm to the term “static security” particularly when you explain what it really means, however for you, it might be the next useful term to use in discussions and justification material.

Are you making the most of your investment in zSecure?

It is often said that software you purchase, albeit for personal or business use, on average you use about 25% of the product's capability. In some cases this is acceptable as you may have just a handful of regular tasks that you need to accomplish. Typically in our busy schedules, we don't have the time to exploit the software to see where functions and features can help make our lives just a little bit easier.

So when looking at security software deployment on the mainframe and the expectation that you must build and maintain secure systems, can you really justify utilising only 25% of the software? There are of course some inhibitors, like lack of staff, higher priority projects. However it does make sense to set some time aside on resource planning to research new functions and features that IBM delivers in the hardware and software – so think about security capabilities in z/OS, z/VM, RACF, Commserver, CICS, DB2 . . . oh, and don't forget zSecure! Doing a gap analysis often helps, by comparing what you are using and what you're not (cross referencing with product announcements), then document how these will add value to your organisation and include a priority for implementation. You might want to involve your local IBM Security Technical Specialist to assist with an exploitation workshop.

Setting some time aside to do this as part of continuous improvement efforts, may serve as a return on investment. Remember that some enhancements we deliver may help address some audit concerns that are proving to be costly, or perhaps some productivity features may speed up a particular process.

Perhaps if your management could see a pie-chart showing a percentage of utilisation for each piece of security software you have installed, it might help influence them to kick off a review of deployment.

zSecure Wiki

A quick reminder about the existence of the zSecure Wiki and Blog on developerWorks – this is a valuable resource, which contains a CARLa training guide, presentations, past newsletters and blogs from our zSecure Subject Matter Experts.

Stay tuned to the Wiki as we plan to include some sample solutions in the near future – also the number of CARLa samples will grow over time.

Recent zSecure Technotes

Some Technotes have been recently published by our zSecure Support team – included below are links to the most recent publications, which we encourage you to read:-

After migrating to zSecure 2.1.1 why do I see MQ resource access violations?

How can I compare group connects with zSecure Admin when universal groups are in use?

Why is zSecure Alert not reporting some selected alerts?

zSecure Alert access violations or CKFREEZE size increase running C2PCOLL after maintenance applied

zSecure 1.12 end of support date – Final reminder

If you are running zSecure 1.12, please note that this release goes out of support on **30th September 2015**. The current release is 2.1.1, which is available to download from Shopz. The IBM Software Support lifecycle page can be accessed from here, where you can search for lifecycle dates for IBM software.

zSecure maintenance up to date? Recommended fixes for zSecure

Do you have all the latest zSecure PTFs applied for the products you have installed? You might want to check out the links below to see the recommended fixes. Pay careful attention because some of these introduce new functions and features!

Product	**Link to recommended fixes**
zSecure Admin	http://www.ibm.com/support/docview.wss?uid=swg27010596
zSecure Alert for RACF	http://www.ibm.com/support/docview.wss?uid=swg27010599
zSecure Alert for ACF2	http://www.ibm.com/support/docview.wss?uid=swg27015183
zSecure Audit for RACF, ACF2 and Top Secret	http://www.ibm.com/support/docview.wss?uid=swg27017677
zSecure CICS Toolkit	http://www.ibm.com/support/docview.wss?uid=swg27010602
zSecure Command Verifier	http://www.ibm.com/support/docview.wss?uid=swg27010603
zSecure Visual (Server & Client)	http://www.ibm.com/support/docview.wss?uid=swg27010605
zSecure Manager for RACF z/VM	http://www.ibm.com/support/docview.wss?uid=swg27019173

CARLa Corner – Before and After

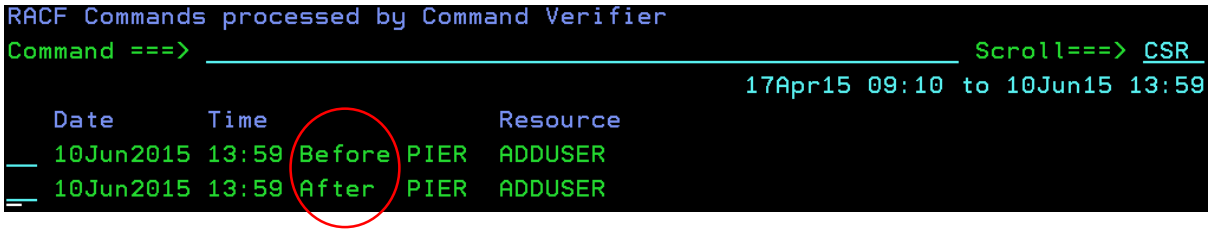
If you are using zSecure Command Verifier, you'll hopefully be aware that in addition to preventing RACF commands and keywords that are not compliant, you can also establish policies that take corrective action.

Suppose you have updated your procedures, which prescribes that user IDs for a given business unit must be defined to RACF with a specific default group and owner. If you established Command Verifier policies to enforce this, one might want to periodically check to see if Command Verifier had to take corrective action on RACF commands. This may reveal Security personnel who are not following your updated procedures.

Well the good news is that you can produce a report using a CARLa query from the sample library. A prerequisite is that you are logging RACF commands, pre and post Command Verifier processing – so you must define XFACILIT profiles C4R.PREAUD.** and C4R.PSTAUD.**. Users who need to be subject to this logging are required to have READ access to the policies.

The sample CARLa (member C4RCNA00) is available in your <your.prefix>.SC4RSMP library. You can run this interactively via zSecure option CO.

Some sample screenshots from an inspection of ADDUSER commands . . .



Please turnover for more screenshots . . . .

Notice in the next screenshot the value of the owner and default group for the ADDUSER command – SYSPROG was specified, which is not appropriate for this prefix of user ID.

```
RACF Commands processed by Command Verifier
Command ===> _____________________________________________ Scroll===> CSR
                                          17Apr15 09:10 to 10Jun15 13:59
  Resource
_ ADDUSER
  System ID                    ZT01 Wed 10 Jun 2015 13:59
_ RACF userid/ACF2 logonid     PEASEJ
  User name                    JAMIE PEASE
  SAF profile key              C4R.PREAUD.**
_ SAF resource name            C4R.PREAUD.ADDUSER
  RACF Command                 ADDUSER  U866HYZ OWN(SYSPROG) DFL(SYSPROG) NAM(
```

In the next screenshot you notice that the owner and default group values are different. This is where Command Verifier has taken corrective action to ensure the values are correct for this prefix of user ID.

```
RACF Commands processed by Command Verifier
Command ===> _____________________________________________ Scroll===> CSR
                                          17Apr15 09:10 to 10Jun15 13:59
  Resource
_ ADDUSER
  System ID                    ZT01 Wed 10 Jun 2015 13:59
_ RACF userid/ACF2 logonid     PEASEJ
  User name                    JAMIE PEASE
  SAF profile key              C4R.PSTAUD.**
_ SAF resource name            C4R.PSTAUD.ADDUSER
  RACF Command                 ADDUSER  U866HYZ OWN(U866) DFL(U866) NAM('#####
```

There are additional samples in the SC4RSMP library. For example, member C4RCNA01 produces a summary of RACF commands that were processed by Command Verifier. In the screenshot below we can see the RACF command that was executed, the number of times it was processed by Command Verifier and whether the command failed due to a policy violation.

```
                RACF Commands processed by Command Verifier      Line 1 of 22
Command ===> _____________________________________________ Scroll===> CSR
                                          17Apr15 09:10 to 11Jun15 17:30
   Resource Count #FAIL
__ ADDGROUP     6     0
__ ADDSD       30     2
__ ADDUSER     28     3
__ ALTDSD      26     2
__ ALTGROUP     4     0
__ ALTUSER     76     2
```

We hope you find this useful. If you have a CARLa sample that you would like to share with the community, why not post it on the zSecure forum on developerWorks.

Useful Links

zSecure home page	http://www.ibm.com/software/security/products/zsecure/
Request for Enhancement Tool (RFE)	https://www.ibm.com/developerworks/rfe/?BRAND_ID=301
zSecure online customer forum	http://www.ibm.com/developerworks/forums/forum.jspa?forumID=1255
zSecure community	https://ibm.biz/Bdx29z
zSecure information centre	https://ibm.biz/BdFqSa
zSecure Wiki	https://ibm.biz/BdRr43
zSecure education – search for classes	https://ibm.biz/BdRUfA
zSecure licensed publications – how to obtain them	https://ibm.biz/BdEer3
Redbook: "z/OS Mainframe Security and Audit Management using the IBM Security zSecure Suite"	http://www.redbooks.ibm.com/redpieces/abstracts/sg247633.html
Redpaper: "Empowering Security and Compliance Management for the z/OS RACF Environment using IBM Tivoli Security Management for z/OS"	http://www.redbooks.ibm.com/abstracts/redp4549.html
Introduction to the New Mainframe: z/OS Basics	http://www.redbooks.ibm.com/abstracts/sg246366.html
Introduction to the New Mainframe: Security	http://www.redbooks.ibm.com/abstracts/sg246776.html
Security on z/VM	http://www.redbooks.ibm.com/abstracts/sg247471.html
Security for Linux on System z	http://www.redbooks.ibm.com/abstracts/sg247728.html
Security on the IBM Mainframe	http://www.redbooks.ibm.com/abstracts/sg247803.html
IBM Institute for Advanced Security	http://www.ibm.com/security/ias/

This newsletter is prepared by the UKI (United Kingdom and Ireland) System z Security Technical Professional team for the IBM Security zSecure suite of products. It is provided for information only and is sent to a selected list of mostly existing users of the suite. If you wish to unsubscribe from the distribution list please click here.

http://www.ibm.com/software/security/products/zsecure/