

CICS INSIGHT Series



In-depth technical discussions led by CICS experts

Welcome

**Today's session will
begin soon.**

**Thank you for
your patience.**



CICS INSIGHT Series



In-depth technical discussions led by CICS experts

Today's Session:

April 17th

11:00 AM EDT

CICS TS 6.2 Overview

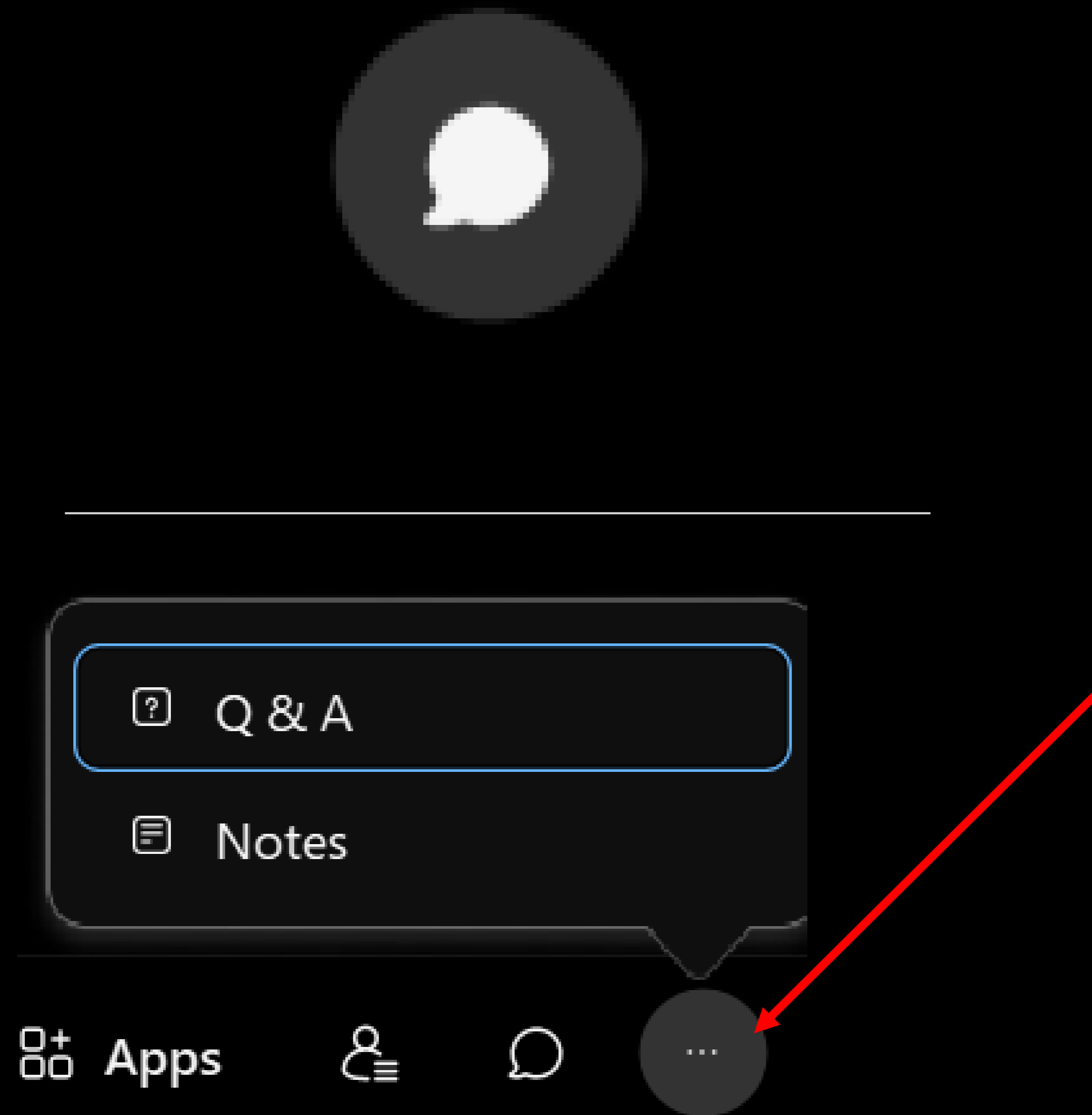
Visit this site for slides, replays and upcoming session announcements:

<https://ibm-zcouncil.com/cics-insight-series-2024/>



*If you have questions
during the session*

**Place them in the chat
or
enter them in the
Q&A section**



IBM® CICS® Transaction Server for z/OS

*Secure and scalable
transaction processing*



Louisa Seers
CICS TS, Product Manager
LOUISASE@uk.ibm.com



Notices and disclaimers

© 2024 International Business Machines Corporation.
All rights reserved.

This document is distributed “as is” without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM.

Not all offerings are available in every country in which IBM operates.

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: www.ibm.com/legal/copytrade.shtml.

Certain comments made in this presentation may be characterized as forward looking under the Private Securities Litigation Reform Act of 1995.

Forward-looking statements are based on the company’s current assumptions regarding future business and financial performance. Those statements by their nature address matters that are uncertain to different degrees and involve a number of factors that could cause actual results to differ materially. Additional information concerning these factors is contained in the Company’s filings with the SEC.

Copies are available from the SEC, from the IBM website, or from IBM Investor Relations.

Any forward-looking statement made during this presentation speaks only as of the date on which it is made. The company assumes no obligation to update or revise any forward-looking statements except as required by law; these charts and the associated remarks and comments are integrally related and are intended to be presented and understood together.

Agenda

CICS TS 6.2

- Application modernization
 - CICS TS vision
 - CICS TS 6.2 dates and themes
-

Management and resiliency

- Threadsafe access to shared data tables
 - Reduced volumes of SMF
 - CICS policies + much more
-

Security and compliance

- Adopting Zero Trust
 - Security discovery and definition capture
 - TLS 1.3, key rings, certificate processing
 - Sign-on, command security checking
 - Defaults, documentation
-

Developer productivity

- Java, Jakarta, Spring Boot, and Node.js
 - CICS containers
 - Ansible and z/OS Cloud Broker
-

Q&A panel



Louisa Seers
CICS TS, Product Manager
LOUISASE@uk.ibm.com



Jenny He
CICS TS, Development Lead, Master Inventor
HEJEN@uk.ibm.com



Colin Penfold
CICS TS, Technical Leader of security
colin_penfold@uk.ibm.com



John Taylor
CICS TS, Software engineer
JTAYLOR1@uk.ibm.com

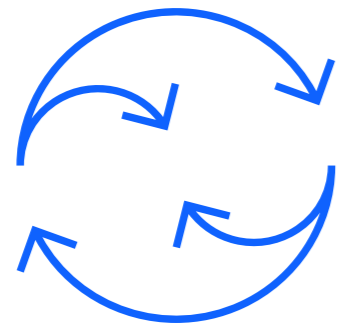


Stew Francis
CICS TS, Architect
stewartfrancis@uk.ibm.com

IBM z16 is built to build

We built a powerful and secure platform for business.
Let's build the future of yours.

Predict and Automate for Increased Decision Velocity



Apply insights at speed and scale
to create new value in every
client interaction

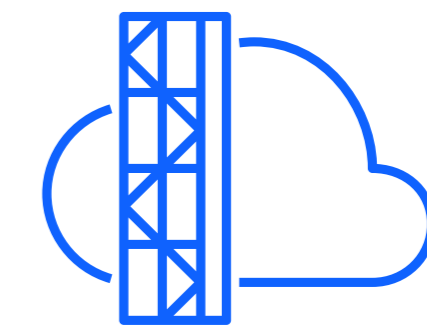
Increase productivity and lower
operational costs with
automation and AIOps

Secure with a Cyber Resilient System



Secure data and systems now and in the
future with quantum-safe protection
Address ever-increasing regulations
with automation for compliance
Plan and mitigate risk of potential
future outages

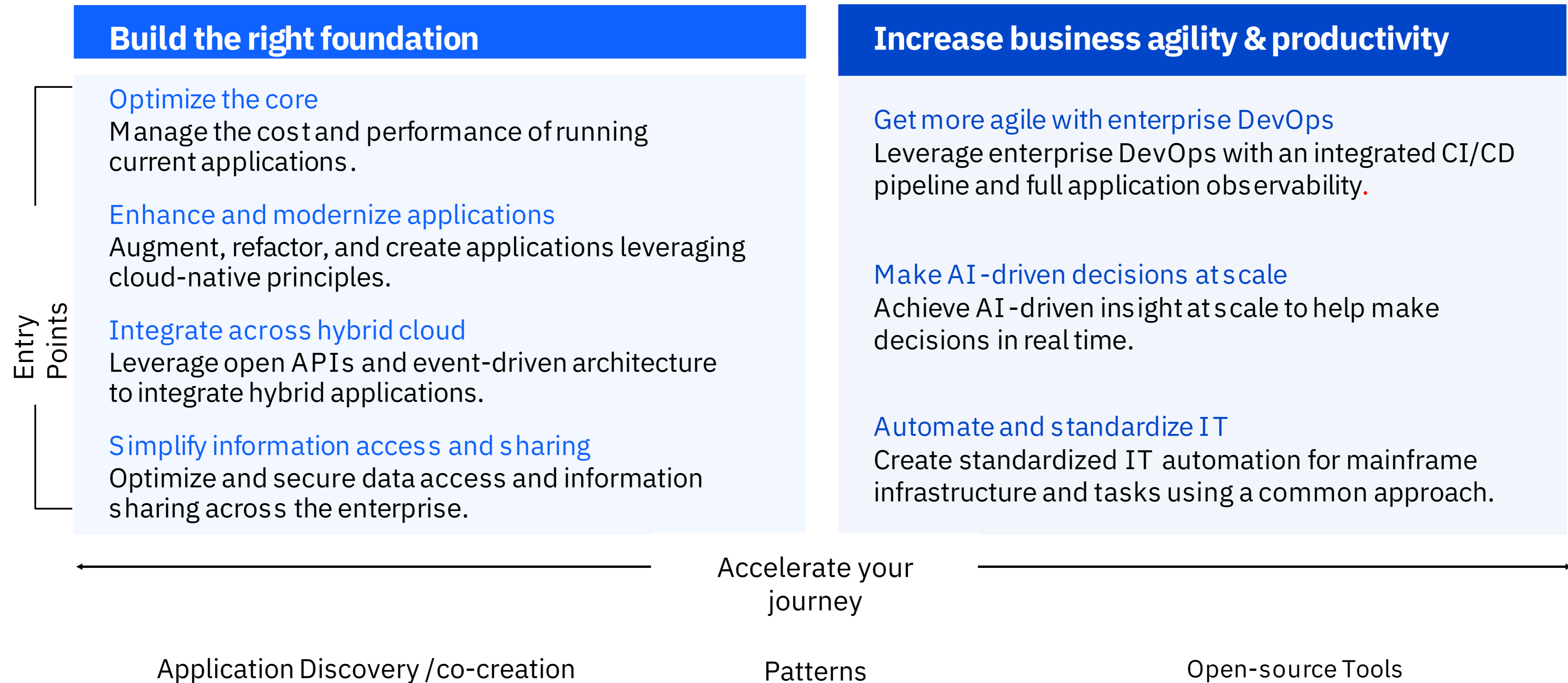
Modernize with Hybrid Cloud



Empower developers with agility to
accelerate modernization of
existing workloads

Enable integration of IBM zSystems
workloads with new digital services
across the hybrid cloud

IBM's approach lets you **continuously modernize** applications & data on IBM zSystems and Cloud



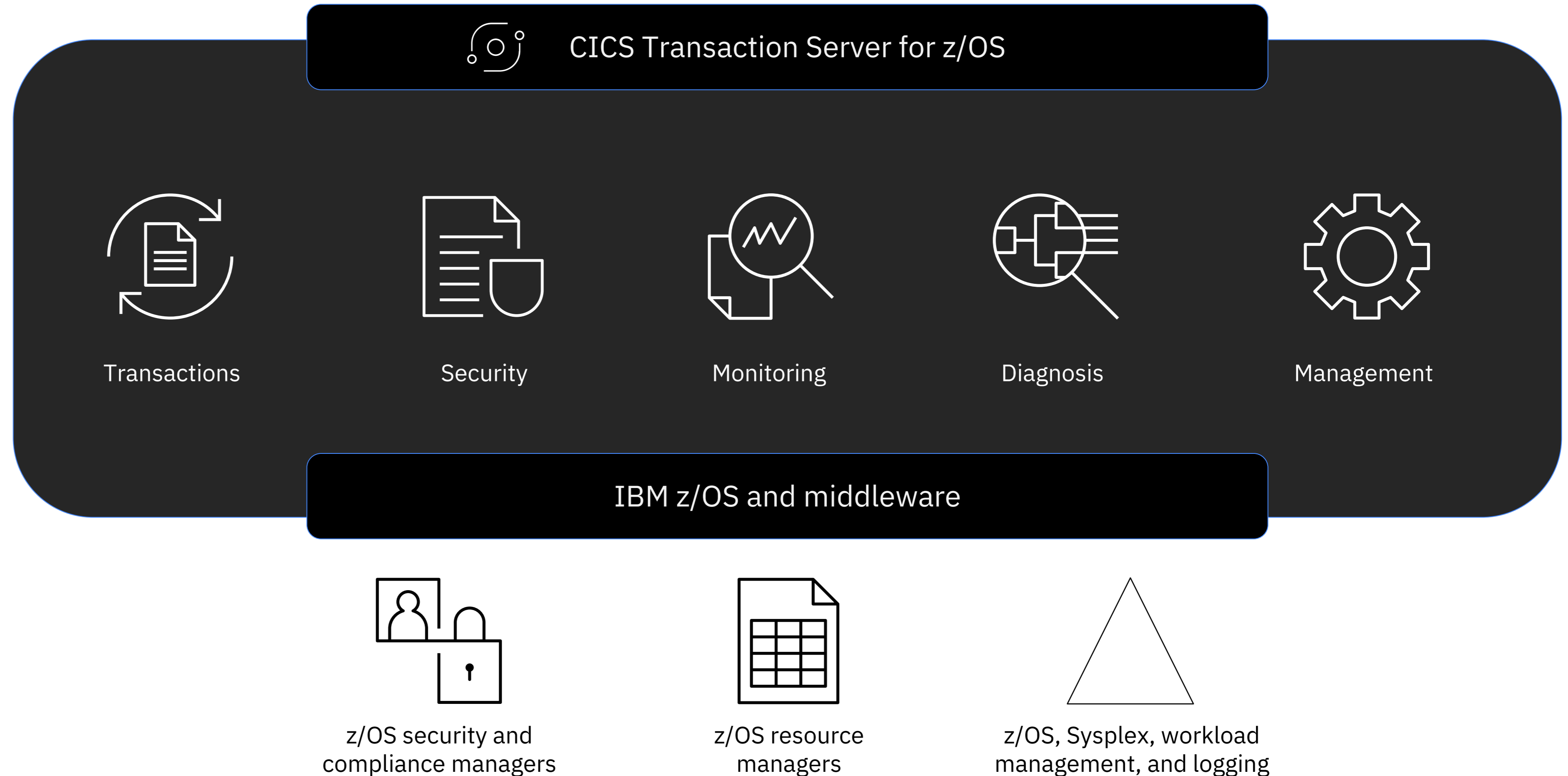
ibm.com/topics/application-modernization

CICS TS is a secure and scalable platform for transactional enterprise applications in hybrid architectures

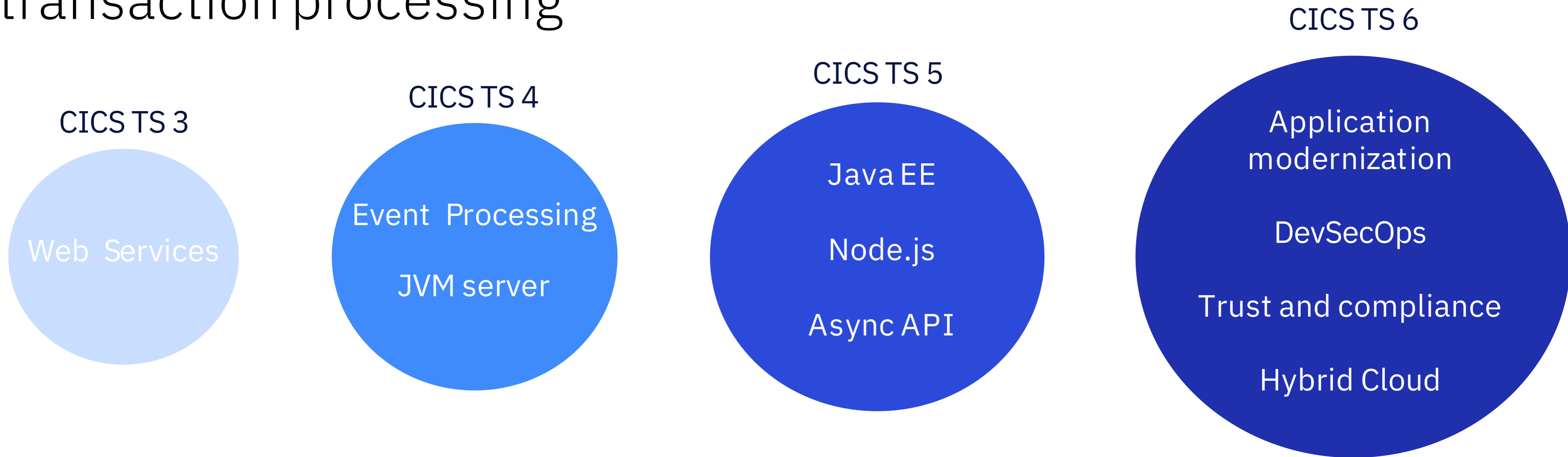
Vision

Applications have access to the full potential of the IBM Z platform

- Easily update multiple data sources with integrity
- Use the right mix of languages to suit developers' skills and business needs, whilst reusing existing apps
- Provides a stepwise, low-risk, high-return approach to application modernization
- Optimized integration with z/OS and middleware to securely update data at scale



55 years of secure and scalable transaction processing

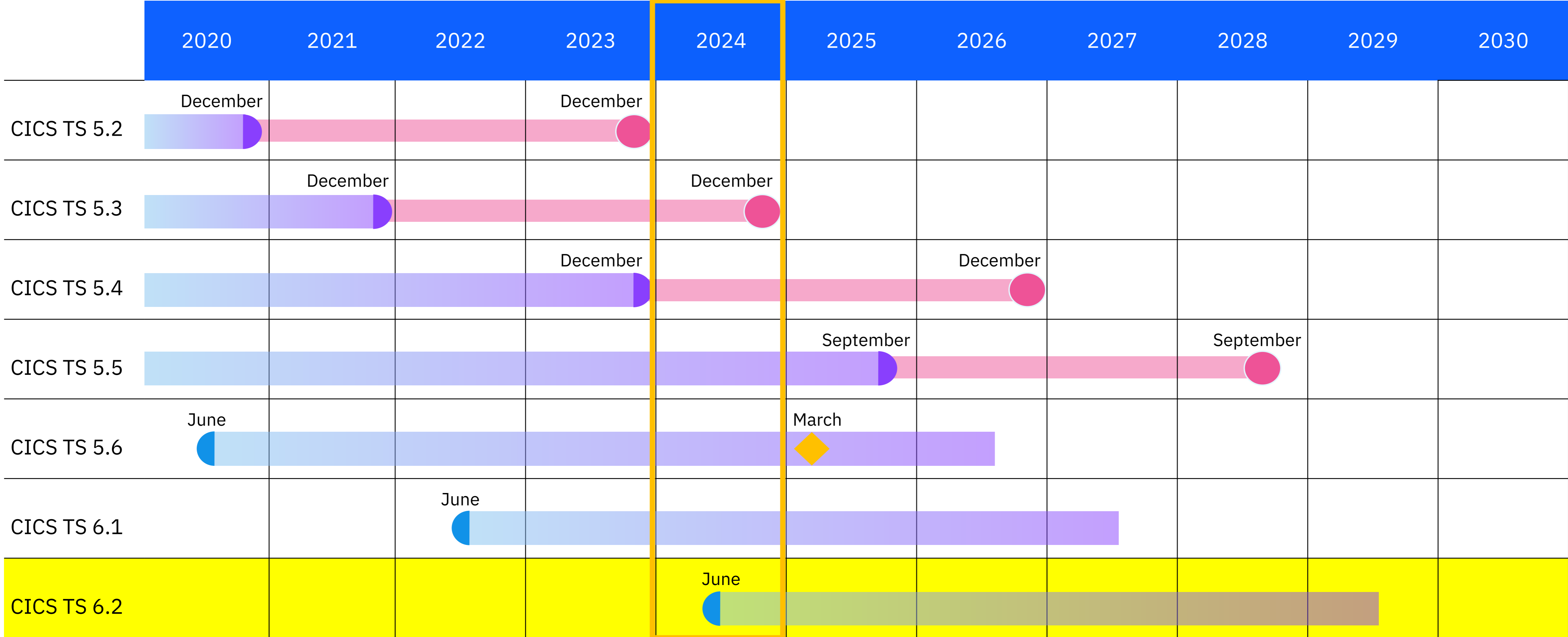


Capabilities added over the years have progressively enhanced CICS from a transaction processor into a general application platform.

Applications running in CICS can securely access IBM Z data and services at scale, using languages, APIs and frameworks that take advantage of the power of IBM Z and z/OS.

In common with other application platforms, CICS applications and development teams can adopt standard industry skills and best practices, including DevSecOps, based on common pipelines and commodity tooling, and automated testing.

CICS TS 6.2 dates



Open beta
 Generally available
 End of marketing
 End of service
 End of service extension

[CICS TS announcements](#). IBM Lifecycle "Extended" = at least 5 years in service + 3 years service extension

CICS TS deliveries

Continuous delivery

- Separate APAR for each feature
- Some flexibility of when to apply APAR or to roll back, until APAR become part of pre-req chain, and in some cases feature toggles used to selectively opt-in to new capabilities
- Focused on latest release, previous releases if there is demand
- CICS Explorer - CD features included with service in CICS Explorer 5.5 update

CICS TS open beta

- Early view of our next version [available now](#)
- Includes CD features and fixes from previous releases
- New features that cannot be made available via service - for example they not complete, or could be disruptive to other products or applications
- Some features may be removed
- [IBM Ideas portal](#) to submit your ideas and vote

New versions

- Every 18 to 24 months
- Upgrade directly from any version to the latest version

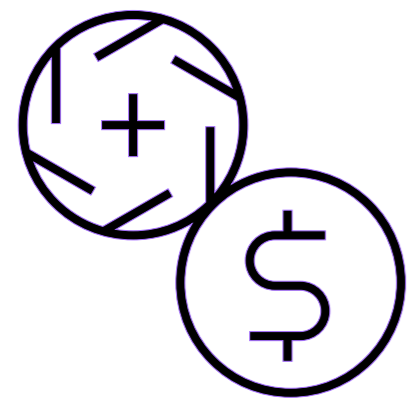
Other

- New capability release elsewhere to improve DevOps and automation scenarios, for example, Ansible CICS Collection and z/OS Cloud Broker, and plug-ins for Maven, Gradle, and UrbanCode Deploy

Announcements

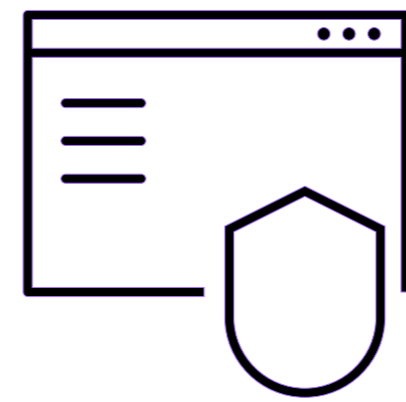
- [Announcements](#) of CD features and open betas at regular intervals

CICS TS 6.2



Reduced cost of management and resiliency

CICS administrators can further optimise apps with threadsafe access to shared data tables, reduced volumes of data written to SMF, automate more with CICS policies and Ansible, and use the power of the IBM Z platform to further improve resilience and scalability.



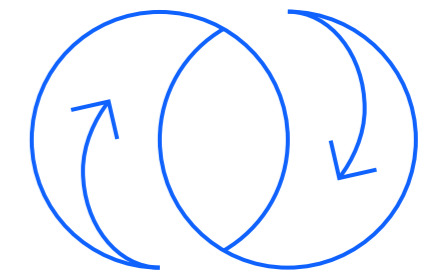
Improved security and compliance management

CICS and Security admins can use new features, tools and workflows to tighten security for valuable transactions and data that is best practice and a requirement when adopting a Zero Trust strategy.



Enhanced developer productivity

Developers can use new features in the latest versions of Java, Jakarta, Spring Boot, and Node.js to modernize and extend applications in CICS.



Increased business agility

Architects can unlock access to CICS applications with API enablement, messaging, event driven architecture, and AI.

CICS TS 6.2

Management and resiliency

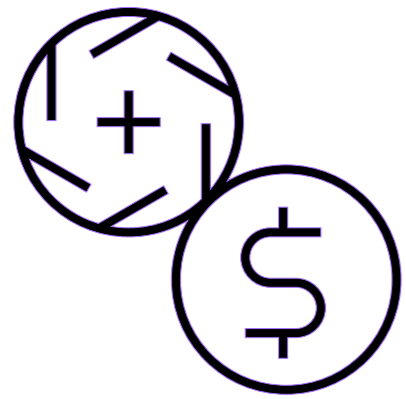


Jenny He

CICS TS, Development Lead, Master Inventor

HEJEN@uk.ibm.com

CICS TS 6.2 - Highlights



Reduced cost of management and resiliency

CICS administrators can further optimise apps with threadsafe access to shared data tables, reduced volumes of data written to SMF, automate more with CICS policies and Ansible, and use the power of the IBM Z platform to further improve resilience and scalability.

- New option to discard transaction requests when TRANCLASS is constrained
- Read and Browse requests to shared data tables are made threadsafe
- New health check on stabilized functions
- Reduced volume of CICS statistics data written to System Management Facilities (SMF)
- New DFHRL messages indicating the result of GRPLIST installation of BUNDLE resources
- Enhanced support for GRPLIST
- Integration of CICS and CICSplex SM shutdowns
- Enhanced on processing type 71 ENF events for a CICSplex
- Enhanced exploitation of Instruction Execution Protection
- Enhanced SOS protection and monitoring of 64-bit MVS storage
- CICS TS now opens TCPIP SERVICE automatically after a TCP/IP restart
- Monitoring CICSplex SM Data Repository usage

Number of tasks in a CICS region

```
TRANClass      : HA11CLAS
Group          : TSTGRP
DEscription    :
CLASS LIMITS
Maxactive      : 002           0-999
Purgethresh    : 0999995     No | 1-1000000
```

MXT (10 - 2000)

- Limit the maximum number of user tasks that can be active in a region at the same time
- For all user transactions

Tranclass Max active (0-999)

- Limit of how many tasks under this tranclass can be active at the same time
- 0 means no task can be active

Tranclass Purge threshold (0 – 1,000,000)

- Limit of how many tasks under this tranclass can queue
- If it is 0, no specified limit
- Queued tasks have task number
- Beyond threshold (>1), tasks are abended with **AKCC**

Total number of tasks in a region can be up to 99998

When lowering the purge threshold for Tranclass:

- CICS releases extra queued tasks and then abend them with AKCC
- Can lead to MAXTASKS condition in the region

Task number allocation has been optimized

When a CICS region has a spike in number of tasks, the region can experience issues:

- High CPU in DFHXMAT when the current number of TRANCLASS'd tasks approaches 99,999
- CICS spends a lot of time during CICS task attach figuring out what task number to assign

CICS TS 6.2 is optimized when finding a range of free task numbers in CICS

Performance tests with over 90,000 queued tasks show:

- ✓ No CPU increase, no response time and throughput degradation on running tasks
- ✓ CICS becomes much more responsive with high number of tasks in the region
- ✓ TRANCLASS-queued tasks no longer impact the performance of running tasks

Discard requests rather than AKCC abend

Instead of turning the request into a task then abend AKCC, CICS provides an alternative behaviour which is to discard the request, when PURGETHRESH is reached

The new behaviour is controlled through tranclass resource definition

Apply to all kinds of ways of starting a task

Note if lowering PURGETHRESH, tasks already in TRANCLASS queue will be AKCC-abended, not discarded. No change to this behavior

TRANCLASS new attribute – PURGEACTION

```
OBJECT CHARACTERISTICS                                CICS RELEASE = 0750
CEDA View TRANClass( HEJCLAS1 )
TRANClass      : HEJCLAS1
Group          : CLASGRP
DEscription    :
CLASS LIMITS
Maxactive      : 002                0-999
PURGEThresh    : 0000001           No | 1-1000000
PURGEAction    : Discard           Abend | Discard
DEFINITION SIGNATURE
DEFinetime     : 13/03/23 15:27:27
CHANGETime     : 17/03/23 08:59:47
CHANGEUsrid    : HEJEN
CHANGEAGent    : CSDApi           CSDApi | CSDBatch
CHANGEAGRel    : 0750
```

- New PURGEACTION attribute is supported in CSD, BAS, inquire, set SPIs
- The default is AKCC Abend to keep the same behavior as previous releases

Complete solution supporting TRANCLASS DISCARD

```
DFHXM0206 25/04/2023 23:00:07 IYCWZCAB  
TRANCLASS HEJCLAS1 has had 2 purges in the  
last 5 minutes.
```

CICS discard the request to start a task according to its TRANCLASS PURGEACTION.

Set response to signal the discard wherever sensible and consistent with the behavior of other errors (e.g. transid is disabled).

New CICS message **DFHXM0206** to show the number of purges in the last 5 minutes.

TRANCLASS statistics to record the purge action of discard, with existing field show the number of purges.

Monitoring field to record number of tasks in a TRANCLASS.

Policy rule to monitor TRANCLASS queue level in real-time.

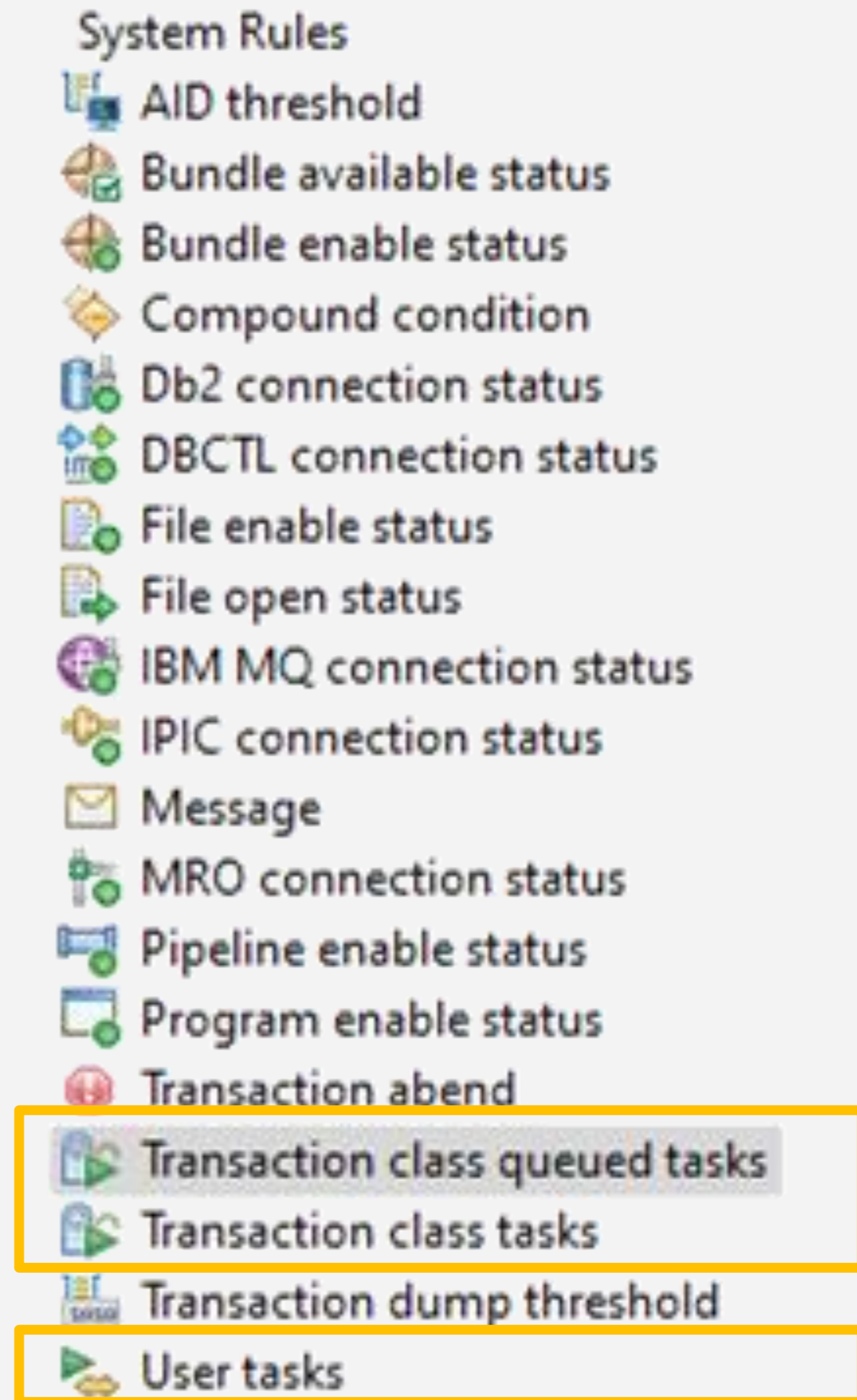
(Existing) Ability for system administrator to get rid of long overdue TRANCLASS-queued tasks.

New system rule – transaction class queued tasks

The new policy rule behaves in much the same way as the **User tasks** and **tranclass tasks** rules


The rule monitors the number of tasks queueing in a TRANCLASS goes above or below a specified threshold:

- Percentage of PURGETHRESH-1 can be chosen from a predefined list of 50%, 60%, 70%, 80%, 90% and 100%
- The rule only applies to TRANCLASS where PURGETHRESH \geq 11



New system rule – transaction class queued tasks

General Information

Rule type:  Transaction class queued tasks

Perform an action when the number of queued tasks in a CICS transaction class crosses a threshold.

Transaction classes are configured with a maximum number of tasks (the value of PURGETHRESH minus 1) that are allowed to queue. This rule triggers an action when the number of queued tasks in a transaction class crosses a defined threshold, which is represented by a percentage of the PURGETHRESH minus 1 value. The threshold is chosen from a predefined list of 50%, 60%, 70%, 80%, 90%, or 100%.

Description:

Conditions

This rule will be restricted to changes in the number of queued transactions within a transaction class that match a set of conditions.

Limit this rule to specific transaction classes:

Transaction class:*

equals

TCL100

Trigger this rule when the number of queued user tasks in a transaction class crosses a threshold:

Percentage of PURGETHRESH:

Goes higher than

100%

60%

70%

80%

90%

100%

Action

What response will the originator get in the DISCARD case?

```
EXEC CICS START ATTACH
EXEC CICS START BREXIT      - for bridge attach
EXEC CICS RUN TRANSID       - Async API
```

- For these APIs, new **RESP(NOSTART) & RESP2(1)** will be returned
- RESP(INVREQ) RESP2(12) for disabled TRANSID

Note that for PURGEACTION AKCCabend case, these originators get normal response

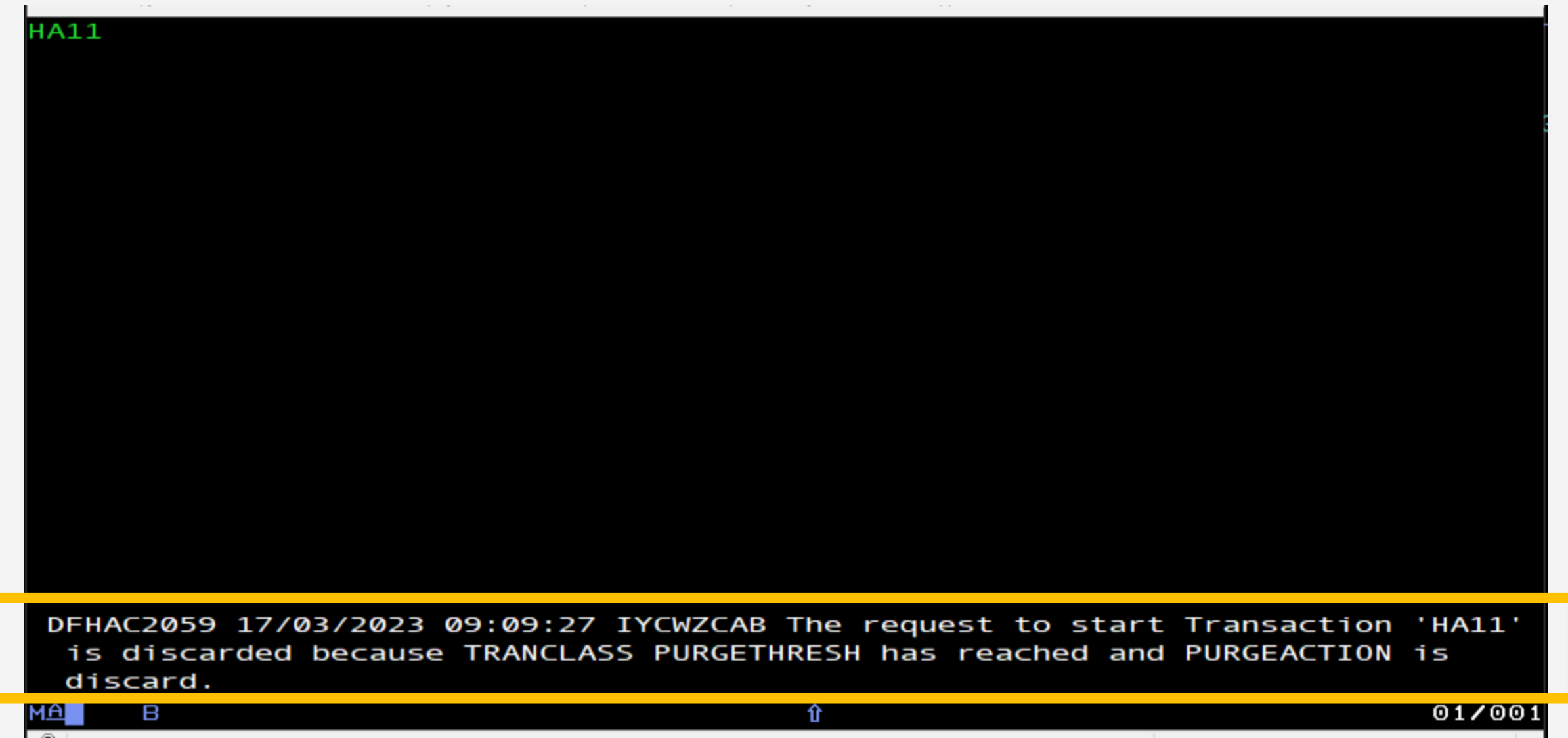
EXEC CICS START without terminal

- The API response will be NORMAL so its callers won't be aware of DISCARD
- Normal RESP for disabled TRANSID

What response will the originator get in the DISCARD case?

Terminal attach local and remote transaction:

- New message DFHAC2059 is issued indicating that the request is discarded
- DFHAC2008 for disabled TRANSID



```
HA11  
DFHAC2059 17/03/2023 09:09:27 IYCWZCAB The request to start Transaction 'HA11'  
is discarded because TRANCLASS PURGETHRESH has reached and PURGEACTION is  
discard.  
MA B 01/001
```


What response will the originator get in the DISCARD case? – Bridges

Web bridge

- Client gets 500 Internal server error

LINK3270 bridge

- Client gets brihrc_request_discarded (88)

CICS-MQ bridge – DPL scenario

- If CKBP or user transaction is discarded, MQ message will be put back to the queue

CICS-MQ bridge – start 3270 transaction scenario

- MQCRC_TRANSID_NOT_AVAILABLE as return code
- New DFHMQ0798 message issued in CICS

CICS-MQ Monitor (aka adapter)

- MQ message will be put back to the queue

What response will the originator get in the DISCARD case?

Alias transaction (CWBA)

- Client gets 503

CWXN

- Connection is reset

CPIH for web service

- Client gets 503
- DFHWB0732 message in CICS

z/OS Connect

- Over IPIC, client gets 500
- DFHIS1025 message in CICS

CICS Transaction Gateway

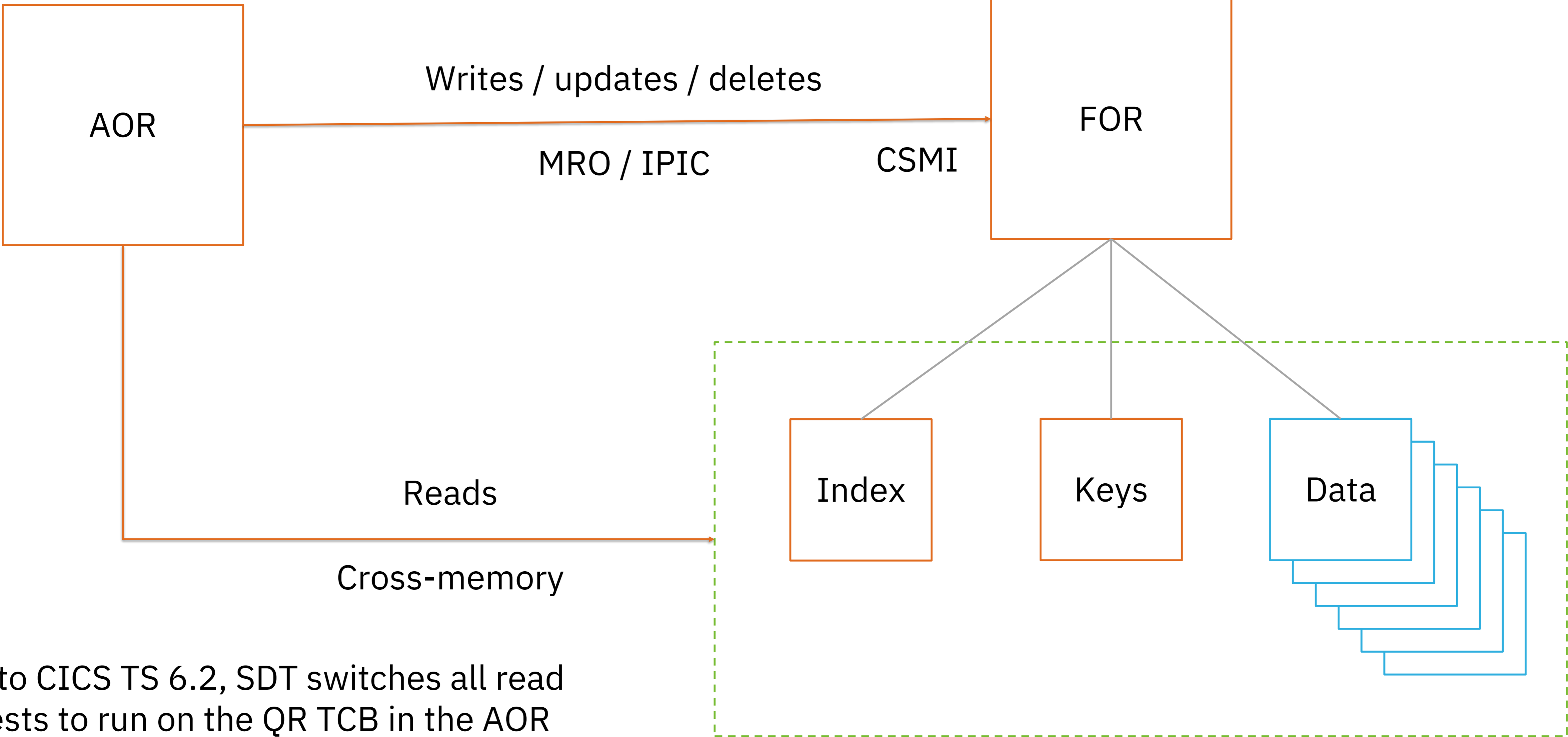
- Over IPIC, client gets -9
- DFHIS1025 message in CICS

Java client

- HTTP 503 Service Unavailable

SDT read and browse
requests thread-safe

Requests to Shared Data Tables



Prior to CICS TS 6.2, SDT switches all read requests to run on the QR TCB in the AOR

CICS TS 6.2 has made SDT read requests threadsafe

- CICS TS 6.2 has changed so removed the TCB-switches in read-only request processing
- SDT read-only requests in the same region can run parallel, so **become threadsafe**
- Also change SDT to use 16-bit LXs so increase the limit from ~2000 to ~32000 per LPAR
- The following **read** and **browse** commands can now run on an open TCB as well as QR TCB on the request region (AoR) when accessing a CMT or UMT SDT
 - READ (without the UPDATE option)
 - STARTBR
 - READNEXT (without the UPDATE option)
 - READPREV (without the UPDATE option)
 - ENDBR
 - RESETBR
- **Update** a shared data table are **not** threadsafe and continue to run on QR TCB only on the FOR region
 - READ with UPDATE
 - REWRITE
 - READNEXT with UPDATE
 - READPREV with UPDATE, DELETE, WRITE
- The loading of shared data tables is also unaffected by this change and executes always on the QR TCB

CICS-maintained Shared Data Table (CMT) is full

- When a user maintained shared data table (UMT) is full, a write/rewrite request fails and a DFHFC0432 message is produced
- But when a CMT is full, the request will not fail because it will be written to the source data set. But there is [no message indicates the CMT table is full](#)
- Accessing those records not in CMT will be through the source data set, so incurs some performance impact

New message in CICS TS 6.2

- [DFHFC0437](#) applid Data table request for file filename has reached the state of CMT {TABLE FULL | STORE FAIL}.

New message indicates the record has not been written to the data table. That could be caused by:

- The data table has reached the maximum number of records defined in the file definition MAXNUMRECS, or
- There is not enough storage to create an entry

The new message is issued only once following the file being loaded

- So it is not re-issued if the number of records have changed until the file is reloaded.

```
16.35.33 JOB58016 +DFHFC0437 IYCWZCAB Data table
request for file FILEA has reached the state of
CMT TABLE FULL.
```

Monitor z/OS storage
expanded to cover 64-bit

New SIT parms for z/OS storage monitoring

If SOS should a task wait for a storage?

- `com.ibm.cics.mvssm.sos.wait={true|false}`

6.2 • `ZOSSOSNEWTCBS=(DELAY|NODELAY)`

Interval in seconds for storage calculations

- `com.ibm.cics.mvssm.mon.interval={0|60,1-60}`

6.2 • `ZOSMONINTERVAL=(60,1-60)`

- The interval of monitoring reduces to 10 seconds if in SOS, zero value is removed from CICS TS 6.2

Size in KB of the remaining storage regarded as SOS for 24-bit storage

- `com.ibm.cics.mvssm.sos24.minavailable.contiguous={32,1-1024}`

- `com.ibm.cics.mvssm.sos24.minavailable.total={64,1-1024}`

6.2 • `ZOSSOS24UNALLOC={(64,1-1024),(32,1-1024)}`

Size in KB of the remaining storage regarded as SOS for 31-bit storage

- `com.ibm.cics.mvssm.sos31.minavailable.total={128,1-16384}`

- `com.ibm.cics.mvssm.sos31.minavailable.contiguous={64,1-16384}`

6.2 • `ZOSSOS31UNALLOC={(128,1-16384),64,1-16384}`

Size in MB of the remaining storage regarded as SOS for 64-bit storage

6.2 • `ZOSSOS64UNALLOC=(64,1-2048)`

- Sets the SOS threshold for the 64-bit storage that is restricted by MEMLIMIT

SOS messages at a glance

| | 24-bit | 31-bit | 64-bit |
|-----------------------|-----------|-----------|-----------|
| SOS | DFHSM0144 | DFHSM0149 | DFHSM0155 |
| No longer SOS | DFHSM0145 | DFHSM0150 | DFHSM0156 |
| Constrained | DFHSM0146 | DFHSM0151 | n/a |
| No longer constrained | DFHSM0147 | DFHSM0152 | n/a |
| Information | DFHSM0148 | DFHSM0153 | DFHSM0154 |

z/OS storage statistics STUP report in CICS TS 6.2

CICS Monitoring field **SMMVSSWT** records the time that the user task waited because MVS user region or extended user region was short on storage.

```
MVS User Region, Extended User Region and MEMLIMIT Storage Monitoring
-----
```

| | User region | | Extended user region | | MEMLIMIT | |
|--|---------------|----------|----------------------|----------|---------------|----------|
| Last monitor sample time.....: | 03/01/2023 | 12:59:59 | 03/01/2023 | 12:59:59 | 03/01/2023 | 12:59:59 |
| State.....: | NORMAL | | NORMAL | | NORMAL | |
| Current unallocated total.....: | 4452K | | 346332K | | 8155M | |
| LWM unallocated total.....: | 4448K | | 345992K | | 0M | |
| Current unallocated largest contiguous area....: | 4420K | | 345912K | | N/A | |
| LWM unallocated largest contiguous area.....: | 4416K | | 345728K | | N/A | |
| Last date and time SOS.....: | | | | | 03/01/2023 | 12:46:41 |
| SOS duration.....: | 00:00:00.0000 | | 00:00:00.0000 | | 00:04:34.4647 | |
| Times SOS.....: | 0 | | 0 | | 1 | |
| Current tasks waiting because SOS.....: | 0 | | 0 | | N/A | |
| Peak tasks waiting because SOS.....: | 0 | | 0 | | N/A | |
| Total waits because SOS.....: | 0 | | 0 | | N/A | |
| Time tasks waited because SOS.....: | 00:00:00.0000 | | 00:00:00.0000 | | N/A | |

IEP is extended to CICS internal storage

- IEP (instruction execution protection) is IBM Z[®] hardware function
- It can help protect certain storage areas from being executed hence protect the system from errors such as stack overflow and malicious attacks
- CICS TS 6.1 can protect dynamic storage areas (DSAs) from instruction execution using IEP

CICS TS 6.2 has extended IEP usage in CICS to protecting z/OS[®] storage requested by CICS for its internal use

New GRPLIST SPI and
processing for bundles

GRPLIST

```
INQUIRE SYSTEM
STATUS: COMMAND EXECUTION COMPLETE
EXEC CICS INQUIRE SYSTEM
+ < EDsalimit( +0838860800 ) >
  < EPCdsasize( +0002097152 ) >
  < EPUdsasize( +0001048576 ) >
  < ERdsasize( +0041943040 ) >
  < ESdsasize( +0001048576 ) >
  < EUdsasize( +0003145728 ) >
  < Forceqr( +0000001054 ) >
  < GCdsasize( 1G ) >
  < GMMText( '**** J. TILLING - CICS TS 6.2 (Emerald) System **' ... )
  GMMLength( +00051 ) >
  < GMMTranid( 'CSGM' ) >
  < GRpllist( 'DFHLIST ,EME ,JOHN ' ) >
  < GSdsasize( 0 ) >
  < GUdsasize( 0 ) >
  < Healthcheck( +0000001241 ) >
  < Initstatus( +0000000628 ) >
+ < Jobname( 'CI13JTD5' ) >

RESPONSE: NORMAL
EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
01/018
```

GRPLIST added to:

- EXEC CICS INQUIRE SYSTEM
- CICS RGN basetable
- CICS Explorer

The screenshot shows the z/OS Explorer interface for a CICS region. The 'Attributes' window is open, displaying a table of system parameters. A yellow box highlights the 'GRPLIST' attribute in the 'SITGroupList' table.

| Name | CICS Name | Value |
|---------------------|--------------|--------------------|
| MVS System ID | MVSSYSID | MV2C |
| Mvssysname | MVSSYSNAME | MV2C |
| OS | OPSYS | X |
| OS Code | CICSSYS | X |
| OS Level | OSLEVEL | 020400 |
| OS Release | OPREL | 24 |
| Page In Count | PAGEIN | 0 |
| Page Out Count | PAGEOUT | 0 |
| Peak Loader Wait Co | LOADHMMW | 1 |
| Peak Task Count | PEAKTASKS | 54 |
| Performance Monito | PERFCLASS | PERF |
| Priority Aging | PRTYAGING | 32,768 |
| Program Remove Co | PRGMRCMP | 0 |
| Program Use Count | PRGMUCNT | 6,146 |
| Rdebrbld | RDEBRBLD | 0 |
| Real Storage | REALSTG | 243,084 |
| Reentrant Program P | REENTPROTECT | REENTPROT |
| Region | EYU_CICSNAME | IYK2Z2G1 |
| Release | RELEASE | 0750 |
| RLS Status | RLSSTATUS | RLSACTIVE |
| Rrmsstat | RRMSSTAT | OPEN |
| Runaway | RUNAWAY | 2,000 |
| Scan Delay | SCANDELAY | 500 |
| SDT Memory Limit | SDTMEMLIMIT | 2,147,483,648 |
| SITGroupList | GRPLIST | DFHLIST ,EME ,JOHN |
| SOS Above Bar | SOSABOVEBAR | NOTSOS |
| SOS Above Line | SOSABOVELINE | NOTSOS |
| SOS Below Bar | SOSSTATUS | NOTSOS |
| SOS Below Line | SOSBELOWLINE | NOTSOS |

Are bundles specified in GRPLIST all ready?

- BUNDLES can be installed via GRPLIST when region does a cold start
 - INSTALLAGENT for these bundles is GRPLIST
- When region warm or emergency starts they are recovered from catalog
- A BUNDLE may contain Java application and many other resources
- Java application can take long time to install
- DFHSI1517 control given to CICS message can be issued seconds or minutes before these bundle resources are ready for business

When all BUNDLES are in an ENABLED state the application is ready for work

- Bundle resources inherit its state from bundle's state
- So safe to issue SET WLMHEALTH OPEN

CICS TS 6.2 checks all bundles installed from GRPLIST

Have all bundles in GRPLIST reached their desired state?

- Yes, DFHRL0137 is issued
- If one or more bundles not reached, DFHRL0138 is issued

Note that if no bundles, DFHRL0137 is still issued to aid automation

This function is also available on CICS TS 6.1 through APAR 58296 (UI95130)

```
22.47.03 JOB40478 +DFHRL0137 I IYCWZCAB 403
403 07/01/2024 22:47:03 IYCWZCAB CJSI All BUNDLE resources with an
403 install agent of GRPLIST are now in their desired target state. Total
403 number of BUNDLE resources are 13.
```

Automating SET WLMHEALTH OPEN in rule action

- CICS region's WLM health is **closed** at region starts up time if setting SIT WLMHEALTH=(0,nn)
 - i.e. increment or decrement WLM health interval value with 0
- **Closed** is the desired status when the region is not ready for business
- However when using policy action to open WLMHEALTH, it will fail with DFHMP3017 message **if interval is 0**
- You can code a program into program list table (PLT) to change to a non-0 e.g. SET WLMHEALTH INTERVAL(5) at second phase PLT
 - But this is not ideal

In CICS TS 6.2, you can specify a non-0 interval when defining the WLMHEALTH policy action

- This value will override the interval in CICS region when the action happens
- So ensure WLM health action will be successful by setting to a non-zero interval
- This function is also available on CICS TS 6.1 through APAR 58295 (UI95014)

Policy rule editor: WLM health interval

Set an interval in WLM open status action

- Value ranges from 1 to 600 seconds
- Selecting “No change” means the current region’s setting will be used when taking the action.

Action

What action should be taken when all of the conditions are met?

Issue a message

Emit an event:

EP Adapter

Event name:

▸ **Static Data (0 items)**

Set z/OS WLM open status to:

OPEN seconds

- Set interval to
- No change to interval
- Set interval to

Reduction in CICS
statistics volume

CICS region resources – what customers say

A CICS region may have many resources installed

- Programs, transactions,
- sessions, connections, etc.

Many of them – sometimes 90% - are not used

- for many intervals
- Or for the entire duration of the region runs

Idea: [Reduce and/or eliminate CICS statistics with zero use count](#)

Idea: [Limit 110 Subtype 2 to active resources only](#)

As a result, the statistics SMF records:

- These unused resources' records have zero counts
- Costing CPU to generate these records
- Occupies SMF storage
- Have to transfer and process them in reporting tool
- Hard to see wood (i.e. those used resources) for the trees so less efficient when identifying problem using statistics

Reduction in CICS statistics volume

Suppress SMF records with zero-counting fields in these types of statistics following stats reset:

- Interval statistics
- Requested statistics
- Requested reset statistics

This design is applied to:

- **Transaction statistics** (DFHXMLRDS)
- **Program statistics** (DFHLDRDS, DFHLDPDS)

Not suppressed in these types of statistics:

- End of day statistics
 - so that zero-count resources will appear in statistics at least once a day
- Unsolicited statistics
- In other types of statistics record just after the resource being created in CICS
 - so recording the changes in stats

More CICS health checks

Stabilized functions

Out-of-date technology inside CICS TS for z/OS is often [stabilized](#) and might be reduced in capability or discontinued in a future release.

Stabilized functions that are still in use might expose CICS to potential risks, reduction of performance, or constraints in capability.

Stabilization notices

Last Updated: 2023-03-16

[Edit online](#)

Out-of-date technology inside CICS® Transaction Server for z/OS® is often stabilized and might be reduced in capability or discontinued in a future release.

Technologies that are discontinued are detailed in [Changes between releases](#). The following technologies are stabilized.

APPC password expiration management (PEM)

Support for APPC PEM is stabilized. The PEM server does not support password phrases. To support authentication with password phrases when using CICS Transaction Gateway with CICS TS, you must migrate from APPC to IP interconnectivity (IPIC) and change your application code to use a current External Security Interface (ESI) API such as **CICS_VerifyPassword** and **CICS_ChangePassword** as described in the [CICS Transaction Gateway for Multiplatforms](#) product documentation.

CICS debugging tools sockets interface

As of Version 14.2, IBM® z/OS Debugger supports only the TCP/IP Socket Interface for CICS; therefore, the debugging tools sockets interface provided by CICS TS is no longer used and thus stabilized.

CICS Service Flow Runtime

[Service Flow Runtime](#) and Service Flow Modeler capability in [IBM Developer for z/OS 14.2.3](#) are stabilized. Consider exposing and orchestrating applications as API services by using [z/OS Connect Enterprise Edition](#), CICS [web services](#), or by writing web applications in [Java](#) or [Node.js](#). Where applications contain a mixture of presentation and business logic, consider using the IBM Developer for z/OS refactoring tools to extract

Topic [Stabilization notices](#)

CICS TS 6.2 checks stabilized functions

S.CK output

```
SDSF HEALTH CHECKER DISPLAY MV2C LINE 1-21 (254)
COMMAND INPUT ==> SCROLL ==> PAGE
NP NAME CheckOwner State Status Result Diag1 Diag2
  ALLOC_ALLC_OFFLN_POLICY IBMALLOC ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ALLOC_SMSHONOR_STATE IBMALLOC ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ALLOC_SPEC_WAIT_POLICY IBMALLOC ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ALLOC_TAPELIB_PREF IBMALLOC ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  ALLOC_TIOT_SIZE IBMALLOC ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ASM_LOCAL_SLOT_USAGE IBMASM ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ASM_NUMBER_LOCAL_DATASETS IBMASM ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ASM_PAGE_ADD IBMASM ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ASM_PLPA_COMMON_SIZE IBMASM ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  ASM_PLPA_COMMON_USAGE IBMASM ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  CATALOG_ATTRIBUTE_CHECK IBMCATALOG ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  CATALOG_IMBED_REPLICATE IBMCATALOG ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  CATALOG_RNLS IBMCATALOG ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  CICS_CAT3_CONFIGURATION IBMCICS ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  CICS_CEDA_ACCESS IBMCICS ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  CICS_JOB SUB_SPOOL IBMCICS ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  CICS_JOB SUB_TDQINTRDR IBMCICS ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
  CICS_REGION_CONFIGURATION IBMCICS ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  CICS_RESOURCE_CONFIGURATION IBMCICS ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  CICS_RESOURCE_SECURITY IBMCICS ACTIVE (ENABLED) EXCEPTION-LOW 4 00000000 00000000
  CICS_STABILIZED_FUNCTIONS IBMCICS ACTIVE (ENABLED) SUCCESSFUL 0 00000000 00000000
```

- New checks are added for stabilized functions
- Each check issues a unique message if certain stabilized function is used
 - Is Extended Recovery Facility (XRF) being used?
 - Is the CICS debugging tool sockets interface in use?
 - Is the CICS service flow runtime in use?
 - Are CICS system events in use?
 - Are JVMSERVER based configuration options for web services in use?
 - Is ONC RPC in use?
 - Is SAML using the CICS security Token Service?
 - Is password expiry management for LU6.2 sessions in use?
 - ...

- DFHH0951 – DFHH0964

- Can use CICS tagging to switch off a specific check
 - Sample cicstags.yaml is provided

TCP/IP enhancements

Eliminate TCB switching for CSOL

For web requests, the socket listener task CSOL needs to peek socket data to see whether to attach user transactions directly

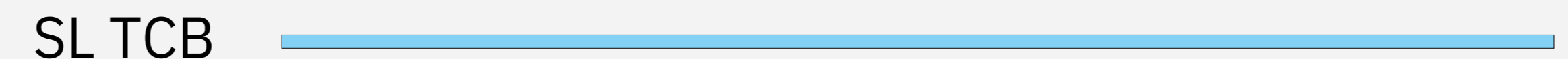
During the peak process, CSOL performs a TCB switching in CICS TS 6.1 and earlier

CICS TS – CSOL is switched to SO TCB to peek



- In CICS TS 6.2 this TCB switching has been eliminated
- As a result, this reduces CPU and response time so gets optimal performance from CICS region

CICS TS 6.2 – CSOL doesn't switch to SO TCB to peek



Automatically restore TCPIPservice following TCP/IP outage

Requirement from Idea CICSTS-I-2031

TCPIPS goes to closed state if any outage in TCP/IP, but it does not open automatically when the TCP/IP is back.

We have to manually open the TCPIPS in CICS using CEMT.

z/OS 2.5 introduced **SRU (Stack Really Up) event** into type 80 ENF

CICS now listens for **SRU ENF 80 event**

Restores TCPIP SERVICE resources to the states they had prior to a TCP/IP outage

- Requires z/OS 2.5

Enhancements in CICS translator

CICS Translator no longer tolerant spelling mistakes

Spelling mistake can happen in user programs

```
EXEC CICS ASSIGN ASRAREG64(ASRAREGS)
```

CICS TS 6.1 and before the Translator substitutes the misspelt option with an assumed one, issues a warning message, and carries on

BUT the substitute may not be what user wanted

The CICS TS 6.2 translator issues an error message & the translate step fails with a return code 8

- Ideally, fix source code and re-compile
- Can continue using translator from previous CICS release

```
MESSAGE NUMBER  SEVERITY  LINE NUMBER  MESSAGE  
DFH7067I        W         00049  'ASRAREG64' IS NOT VALID. 'ASRAREGS' ASSUMED.
```

6.2

```
MESSAGE NUMBER  SEVERITY  LINE NUMBER  MESSAGE  
DFH7053I        C         00046  OPTION 'ASRAREG64' IS NOT VALID AND IS IGNORED.
```

CPSM enhancements

New messages to identify CMAS

In CICS TS 6.1 and earlier, it is not possible to identify CMAS status from job log

- Which one is the maintenance point?
- Which CICSplex is managed by this CMAS?

CICS TS 6.2 will issue new messages in the EYULOG of CMAS:

- EYUCP0034 is issued if the CMAS is the maintenance point
- EYUCP0035 is issued if the CMAS manages a CICSplex
- EYUCP0036 is issued if the CMAS no longer manages a CICSplex

```
09/21/2023 23:17:19 EYUCP0034I JATP3450 This CMAS
is the maintenance point for CICSplex CPLX3450.
```

```
09/21/2023 23:17:23 EYUCP0035I JATP3451 This CMAS
manages CICSplex CPLX3450. The maintenance point
is JATP3450.
```

Integrated CICS & CPSM shutdowns

In CICS TS 6.1 and before, to shutdown a CMAS transaction COSD should be used

COSD shuts down CMAS processing then initiates CICS shutdown

In CICS TS 6.2, EXEC CICS/CEMT PERFORM SHUTDOWN command is enhanced to shut down CMAS as part of the process

EYUDREP space monitoring

- CPSM EYUDREP is a VSAM file defined to CICS
- It contains the CICSplex SM administration definitions applicable to its associated CMAS
- Each CMAS must have a unique EYUDREP data repository associated with it
- It can be very large as it holds CICSplex topology, BAS configuration, CPSM WLM, CICSplex SM monitoring etc.
- When EYUDREP file runs out of space, the CMAS issues EYUXD0011E when no further updates will be processed, and the DREP must be enlarged

New message in CICS TS 6.2

```
11/02/2023 12:17:05 EYUXD1032W JATP3450 EYUDREP  
has exceeded 70% of its extent availability,  
DATA(72%), INDEX(16%).
```

Message is issued if either of its DATA or INDEX components exceeds that

Optimized ENF 71 support in CICSplex environment

- RACF® sends a type 71 ENF signal to listeners when
 - A CONNECT, REMOVE, or REVOKE command changes a user's resource authorization, or
 - A user ID is revoked automatically as a result of too many failed password attempts
- CICS TS 6.1 and earlier region listens for ENF 71 events when SIT parm RACFSYNC(YES) is set
- In a CICSplex environment this can cause system overload when large numbers of MAS regions are listening and reacting to ENF 71 events

CICS TS 6.2 introduced new YES value to SIT parm RACFSYNC

RACFSYNC={YES | NO | CPSM}

RACFSYNC(CPSM) should be specified in MAS and WUI regions

- means MAS gets the ENF71 info from CPSM i.e. its CMAS, when MAS heartbeat happens, currently every 15 seconds
- specifying RACFSYNC(CPSM) for a CMAS is rejected, EYUCI0103E is issued

RACFSYNC(YES) should be specified only in CMAS regions

- The CICS region running as a CMAS will listen for ENF71
- The CMAS will update its own security information as part of reacting to ENF 71, regardless of CPSM SECTIMEOUT setting

It uses existing CPSM functionality to propagate information to MAS regions so less z/OS resources are used

CICS TS 6.2

Security – Trust and Compliance



Colin Penfold

CICS TS, Technical Leader of security

colin_penfold@uk.ibm.com

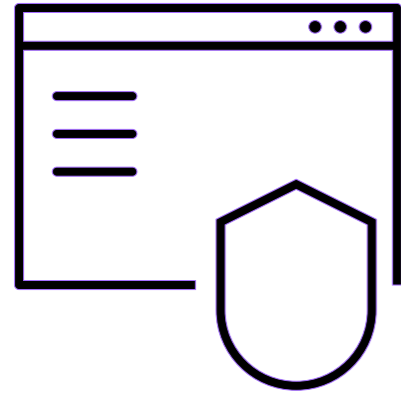


John Taylor

CICS TS, Software engineer

JTAYLOR1@uk.ibm.com

CICS TS 6.2



Improved security and compliance management

CICS and Security admins can use new features, tools and workflows to tighten security for valuable transactions and data that is best practice and a requirement when adopting a Zero Trust strategy.

Zero Trust

- CICS Security Discovery
- Changes to RESSEC and CMDSEC
- Security Definition Capture
- Security Definition Validation

Other security changes

- TLS
- Simplification
- Compliance and Auditability
- Security Doc Restructure

Zero Trust

Zero trust at IBM

” Zero trust isn't something you can buy or implement. It's a philosophy and a strategy. And to be frank, at IBM, we wouldn't even characterize zero trust as a security strategy. It's an IT strategy done securely.

IBM CISO

<https://www.ibm.com/zero-trust>

What is zero trust?

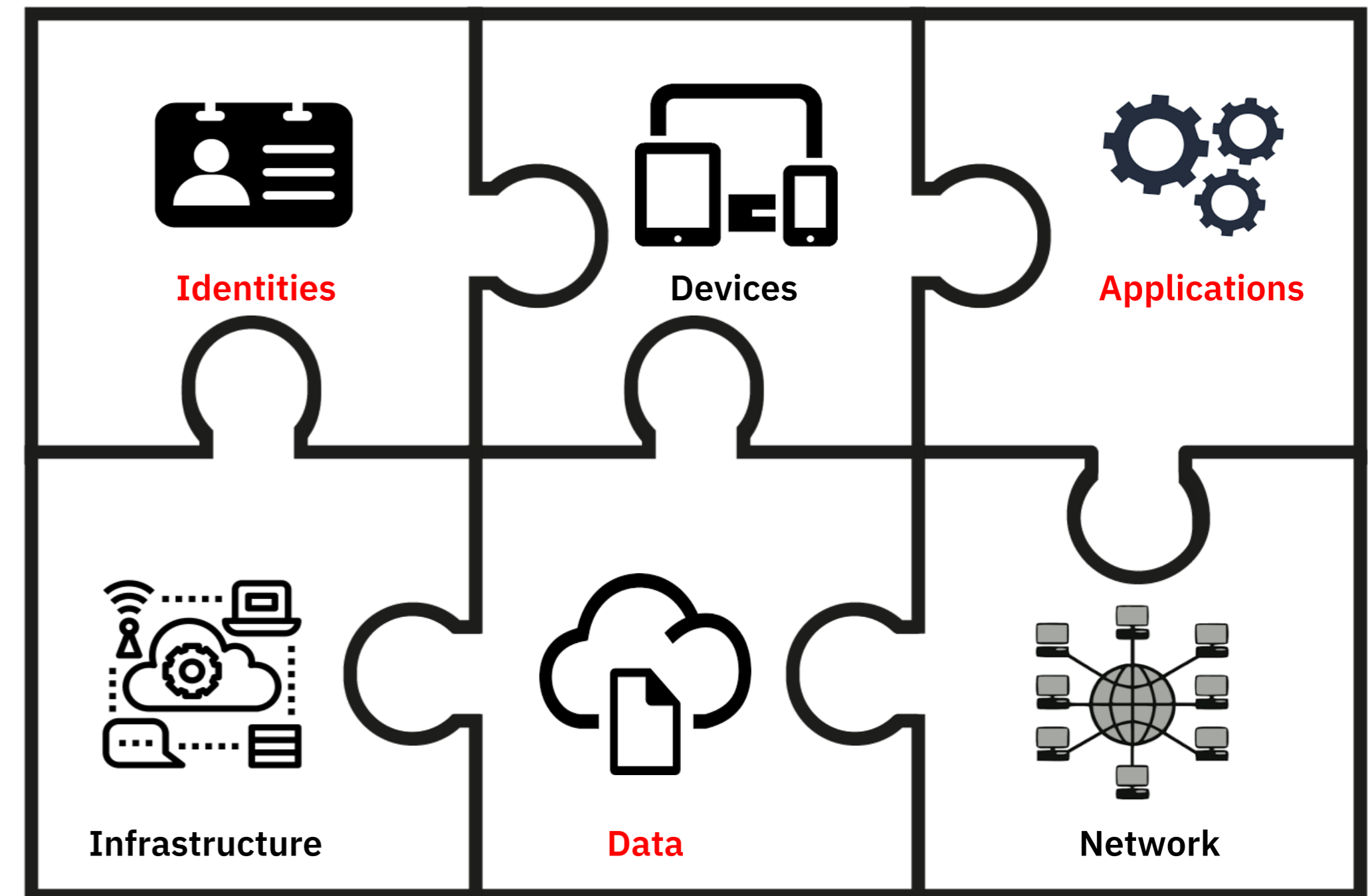
Focus on protecting resources not perimeters

Enable the **right user**,
to have the right **access**,
to the **right data**,
for the **right reasons**

Never trust, always **verify**

Assume the bad actor is already present &
continuously monitor

The key elements of a Zero Trust strategy



This presentation concentrates on the **identities** who need access to **data** used by **applications**

Research

71% increase of attacks using valid credentials

85% of attacks on critical sectors could have been avoided by:

- up-to-date fixes
- MFA
- least-privilege principals

IBM X-Force 2024 report

<https://newsroom.ibm.com/2024-02-21-IBM-Report-Identity-Comes-Under-Attack,-Straining-Enterprises-Recovery-Time-from-Breaches>

CICS TS 6.2 Zero Trust strategy roadmap



CICS Security Discovery

Improve role-based security

Identify resource security definitions in production

Estimate cost of adding resource security

Changes to RESSEC and CMDSEC

Enable customers to set RESSEC=ALWAYS and CMDSEC=ALWAYS

Remove unnecessary security definitions in CICS transactions

Security Definition Capture and Validation

Identify security definitions during development

Framework for automation of this process if tests are automated

See topic [Implementing a zero trust strategy](#)

CICS Security Discovery

Zero Trust and Resource Security

Transaction security is a form of boundary security

- Transactions can access anything on the region
- Transactions can DPL to other connected regions
- You are trusting the developer

It's the data that needs to be secured

Most customers don't have resource security

- Complexity of implementing
- CPU Cost
- Historically transaction security considered to be sufficient

Is application separation sufficient?

- An application is a set of isolated CICS regions
- Only data for the application installed
- Valid, but only if there is just one role

Importance of Roles

“Enable the right user, to have the right access, to the right data, for the **right reasons**”

A user’s access should be related to their **role**

When they leave that role, they must lose access

Some customers don’t use roles or use a mixture of roles & userids

- Hard to maintain
- Unused access often kept
- Difficult to audit

Migrating to Resource Security

Most customers do not have

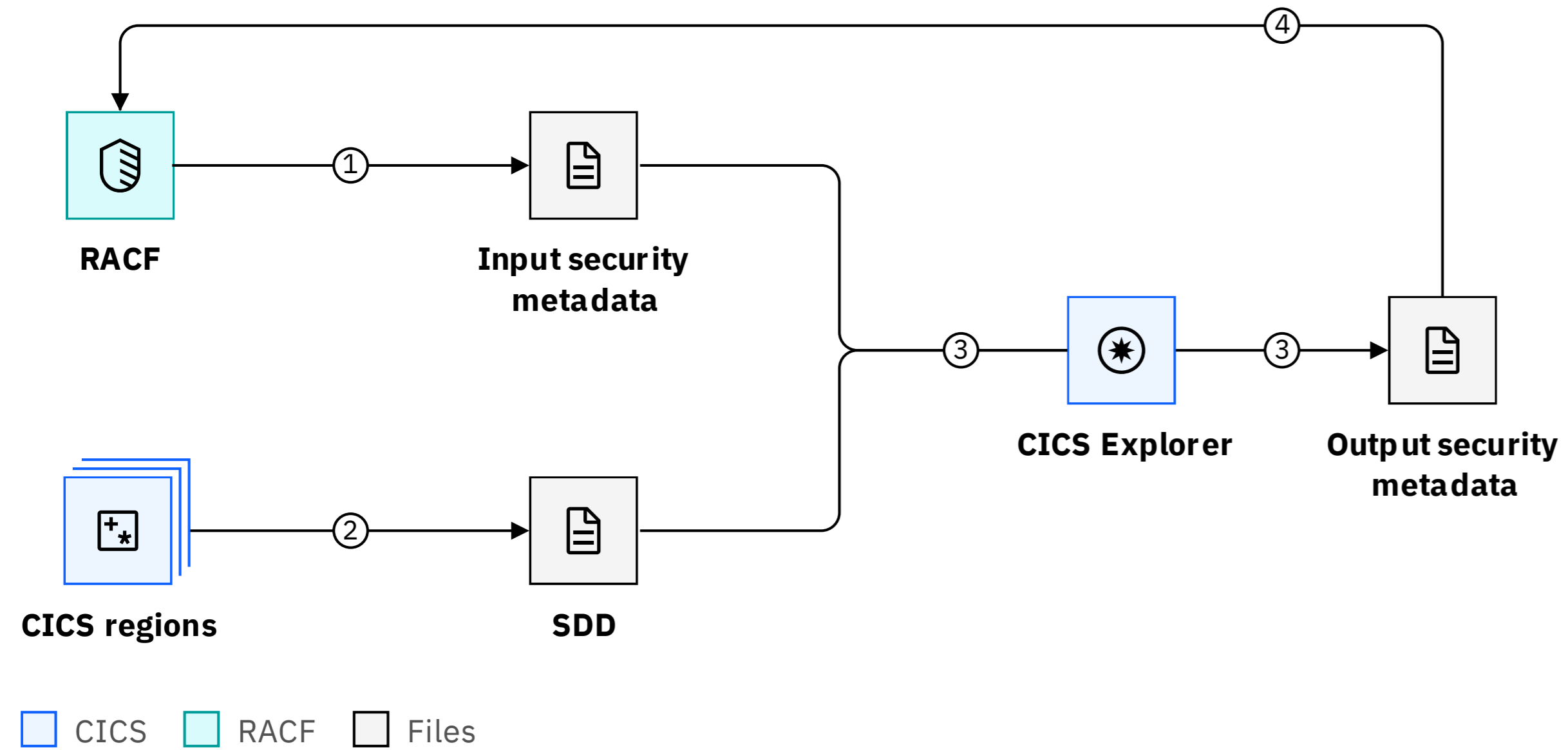
- Fully automated tests
- Good coverage of tests
- Specific security tests

How do you identify

- The roles?
- What resource access is required?

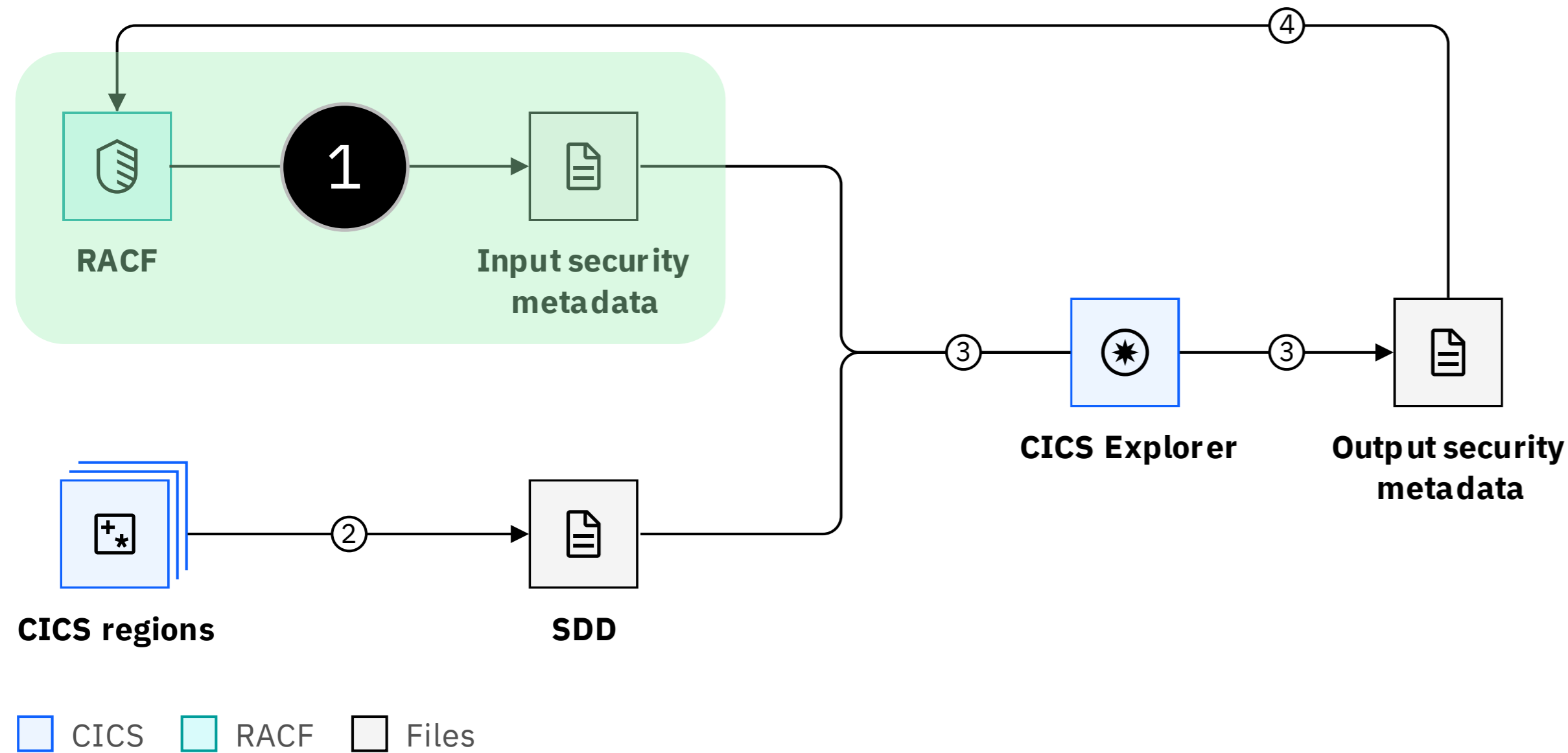
How do you migrate without breaking applications?

CICS Security Discovery



1. Extract RACF definitions
2. Capture security discovery data (SDD)
3. Analyse security definitions in CICS Explorer and export them for review
4. Create RACF commands from reviewed security definitions

Import RACF definitions as security metadata



- Imports transaction class and groups using this class
- Assumes users have good transaction security
- Separate import for each SECPRFX
- Optionally imports other CICS security classes

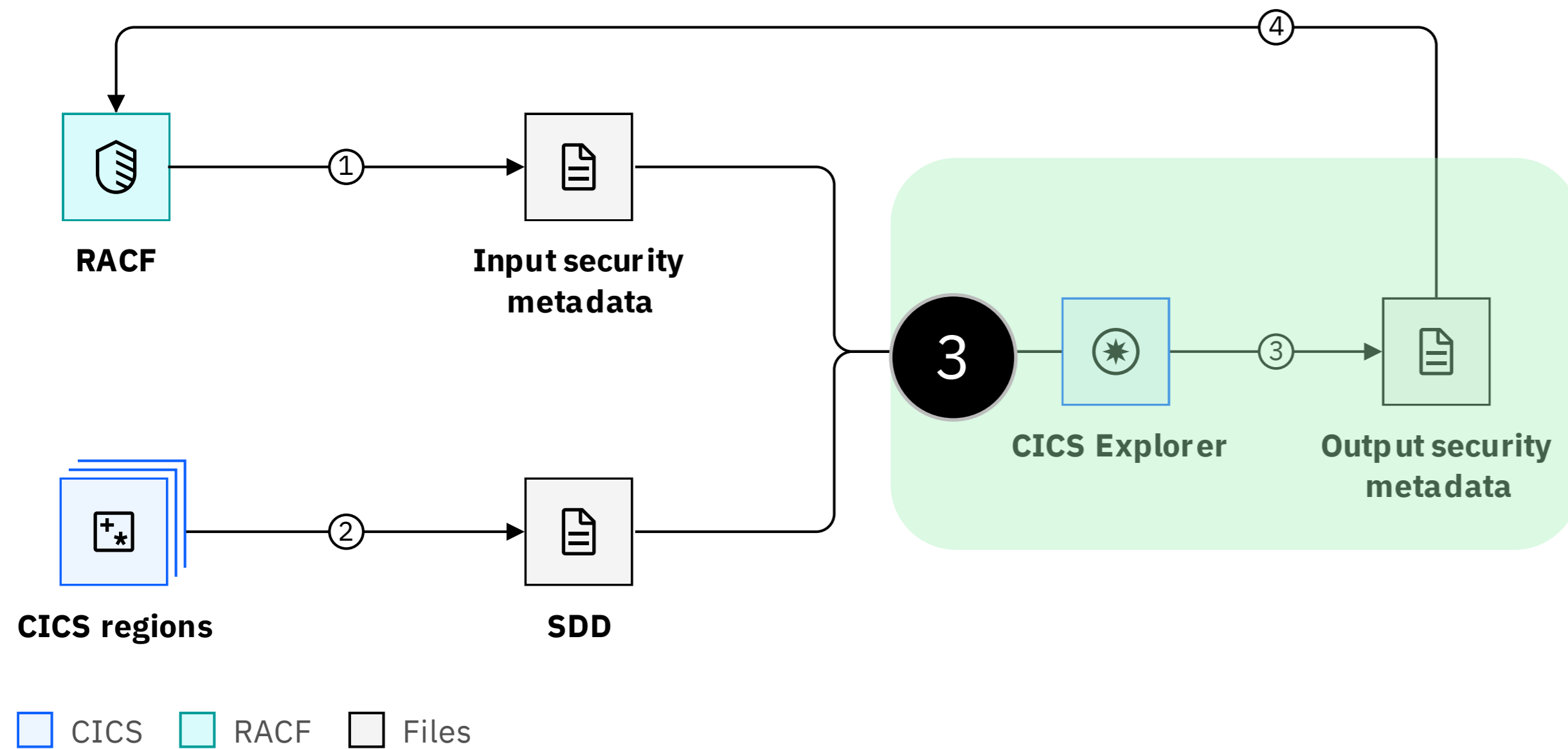
DFH\$R2SM

```
//SECMETA JOB
//SECMETA EXEC DFHXSMET,SAMPLIB=h1q.SDFHSAMP,
//          DIR='/u/userid/cics/', FN='regionsA'
//INPUT.SYSIN DD *
XTRAN=CICSTRN
SECPRFX=NO
//
```

Security metadata

```
--- # Security Metadata ---
version: 2
file_created:
- date: "17 Mar 2023"
- time: "17:27:26"
- user: SUE
group_list:
- name: MANAGER
  users:
  - MAINWRN
- name: TELLER
  users:
  - WILSON
  - PIKE
user_list:
- user: JONES
  username: "Jack Jones"
- user: MAINWRN
  username: "George Mainwaring"
- user: PIKE
  username: "Frank Pike"
- user: WILSON
  username: "Arthur Wilson"
secprfx: NO
classes:
- class: XTRAN
  name: CICSTRN
  profiles:
  - name: BANKING
    members:
    - BNK1
    - BNK2
    access_lists:
    - access: READ
      groups:
      - MANAGER
      - TELLER
      users:
      - JONES
```


Analyse security definitions in CICS Explorer and export them for review



Use security metadata to

- Identify user groups (roles) and their access to transaction member lists

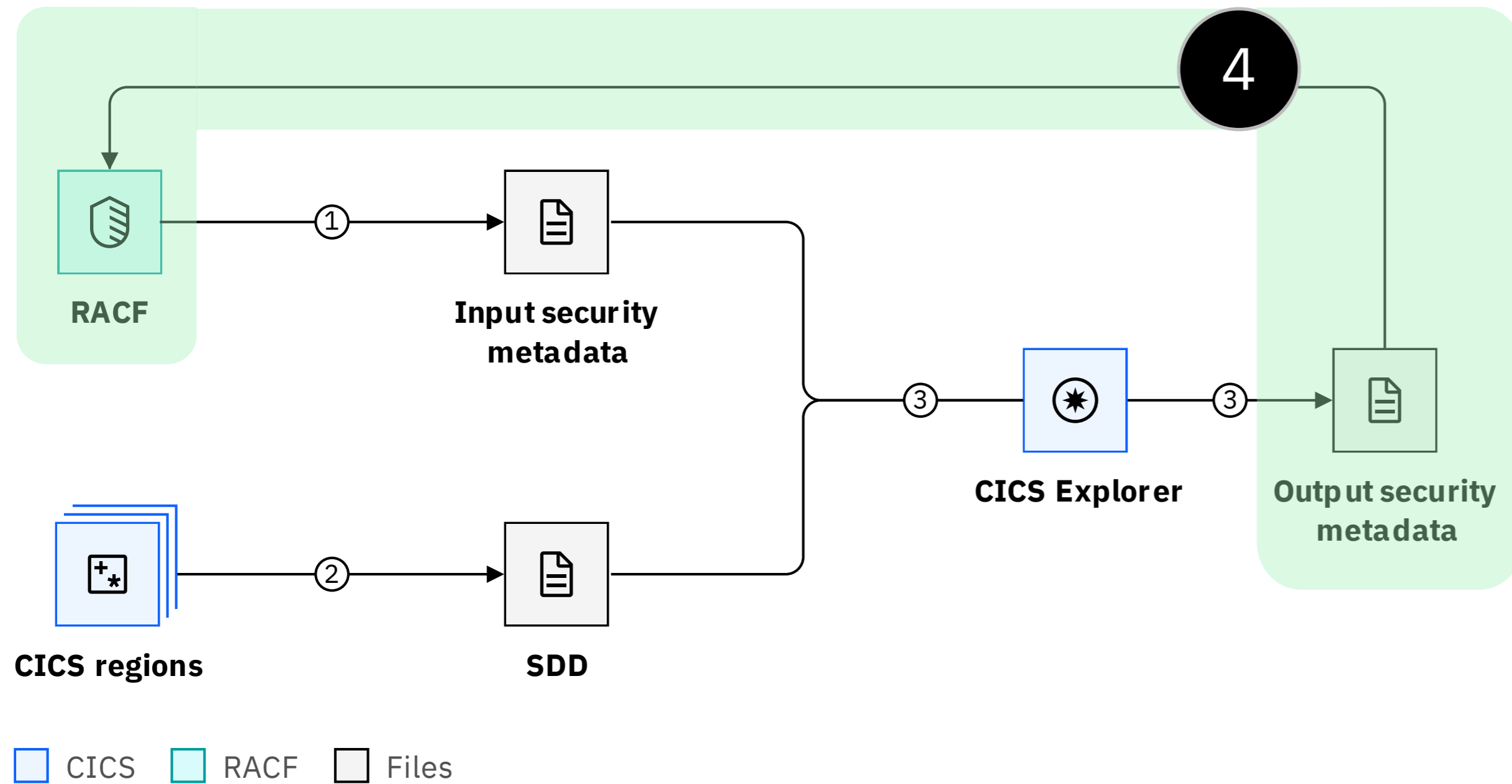
Use Security Discovery Data to

- Refine user groups and transaction member lists
- Identify user groups access to resource member lists

CICS Explorer - Security Discovery Perspective

| | | | 005 | m0000006 | m0000007 | m000... | m000... | | | |
|---|----------|------------------|------|----------|----------|---------|---------|------|------|------|
| | | | T019 | T021 | T049 | T023 | T047 | T025 | T026 | T027 |
| ✓ | HR | | | | | | | R+r | | R+r |
| □ | USR0015 | Dick Pollard | | | | | | Rr | | Rr |
| □ | USR0028 | Callum Ferguson | | | | | | R+ | | R+ |
| □ | USR0064 | Eddie Hemmings | | | | | | Rr | | Rr |
| □ | USR0084 | Norman Gifford | | | | | | Rr | | Rr |
| □ | USR0094 | Tommy Mitchell | | | | | | R | | Rr |
| ✓ | MANAGER | | R | Rr | R | | | | | |
| ✓ | USR0070 | Robin Smith | R | Rr | R | | | | | |
| ✓ | SYSADMIN | | Rr | | | Rr | Rr | | | |
| ✓ | USR0061 | Mark Stoneman | Rr | | | Rr | Rr | | | |
| ✓ | TELLER | | R+r | Rr | Rr | Rr | Rr | | | R+r |
| □ | USR0026 | David Colley | R+ | Rr | Rr | R | Rr | | | Rr |
| □ | USR0076 | Charlie Kelleway | Rr | Rr | Rr | Rr | Rr | | | Rr |
| □ | USR0083 | Len Darling | Rr | Rr | Rr | Rr | Rr | | | R+ |

Create RACF commands from reviewed security definitions



- Create new classes (allows easy migration)
- Configure for selected regions at a time
- Options to customise with WARNING, OWNER etc

DFH\$SM2R

```

//SECMETA JOB REGION=OM
//RACFCMD EXEC PGM=IRXJCL,PARM='DFH$XSR'
//SYSEXEC DD DISP=SHR,DSN=h1q.SDFHSAMP
//YAML DD DISP=SHR,DSN=<<security metadata>>
//XTRAN DD SYSOUT=*
//XFCT DD SYSOUT=*
...
//GROUPS DD SYSOUT=*
//SYSIN DD *
XTRAN=TESTTRN
XFCT=TESTFCT
//
  
```

RACF commands

```

RDEFINE GCIC1TRN TGRP1 +
        UACC(NONE) +
        ADDMEM(TRNA,TRNB,TRNC,TRND)
PERMIT TGRP1 CLASS(GCIC1TRN) +
        ACCESS(READ) +
        ID(UGRP1)
RDEFINE GCIC1TRN TGRP2 +
        UACC(NONE) +
        ADDMEM(TRNE,TRNF)
PERMIT TGRP1 CLASS(GCIC1TRN) +
        ACCESS(READ) +
        ID(UGRP2)
  
```


Capturing Security Discovery Data

Details of the process of capturing the resource data usage in a production region and saving the information as Security Discovery Data

Capturing Security Discovery Data

Discovers following resource access by

- Userid
- Transaction
- Origin transaction

Each access only captured once

- Each level of access recorded

Data captured in 64-bit memory

Small performance overhead

Activated by PLT or CICS Explorer

Captures CICS security accesses

- Ignores Xnnn settings
- Ignores RESSEC/CMDSEC setting

Data written daily to a logstream

- Also at shutdown or on request

Data for sets of regions combined offline

SPI for SECDISCOVERY

Start/stop collecting data for all or selected classes

Status of data collection

- Transaction data always collected
- Information about how much data is being collected

Write data out

```
SET SECDISCOVERY  
  < STATUS() | ON | OFF >  
  < DISCOVERALL | _classes_ >
```

```
INQUIRE SECDISCOVERY  
  < STATUS() >  
  < TRAN() > _classes_  
  < LASTSECDTIME() > < LASTWRITTIME() >  
  < SECDCOUNT() > < NEWSECDCOUNT() >
```

```
PERFORM SECDISCOVERY WRITE
```

```
_classes_ = < CMD() > < DB2() > < DCT() > < FCT() >  
           < HFS() > < JCT() > < PCT() > < PPT() >  
           < PSB() > < RES() > < TST() > < USER() >
```

How much data to capture?

Expect to be left running for an extended period

- Capture normal use and special periods (end of month, year etc)
- Stats to show how much data is being collected
- Data collection should tail off after a few days
- Also available with CICS Explorer and SPI

```
DFHXS1602 date time applid Security  
Discovery is {active|inactive}. Total  
records: recordcount. Records since last  
write: writecount. Last recording:  
mm/dd/yyrecorddate hh:mm:ssrecordtime. Last  
write: mm/dd/yywritedate hh:mm:sswritetime.
```

Statistics

Shows number of resource checks

and

Number which are not currently checked due to XPPT=NO for example.

Can use this information to estimate cost of implementing resource security.

```
Security Discovery records      :      20
Transactions executed          :      24
Successful resource checks     :     179
  Checks that bypassed DFHXSRC :      54
  Checks that called DFHXSRC   :     172
    Exempt resources           :      32
    Resource class not active   :       2
  FASTAUTH calls               :     138
  AUTH calls                    :       0
Resource class counts
  XCMD checks                  :      24
  XDB2 checks (class not active) :       0
  XDCT checks                  :       6
  XFCT checks (class not active) :      47
  XHFS checks (class not active) :       0
  XJCT checks (class not active) :       0
  XPCT checks (class not active) :       0
  XPPT checks                  :     120
  XPSB checks (class not active) :       0
  XRES checks (class not active) :       2
  XTRAN checks                 :      21
  XTST checks (class not active) :       5
```

Statistics

Cost per transaction =

(Num Xnnn checks /
Num XTRAN checks)

* 2 micro second

* CPU Type Scalling

See CICS Performance Report
for details

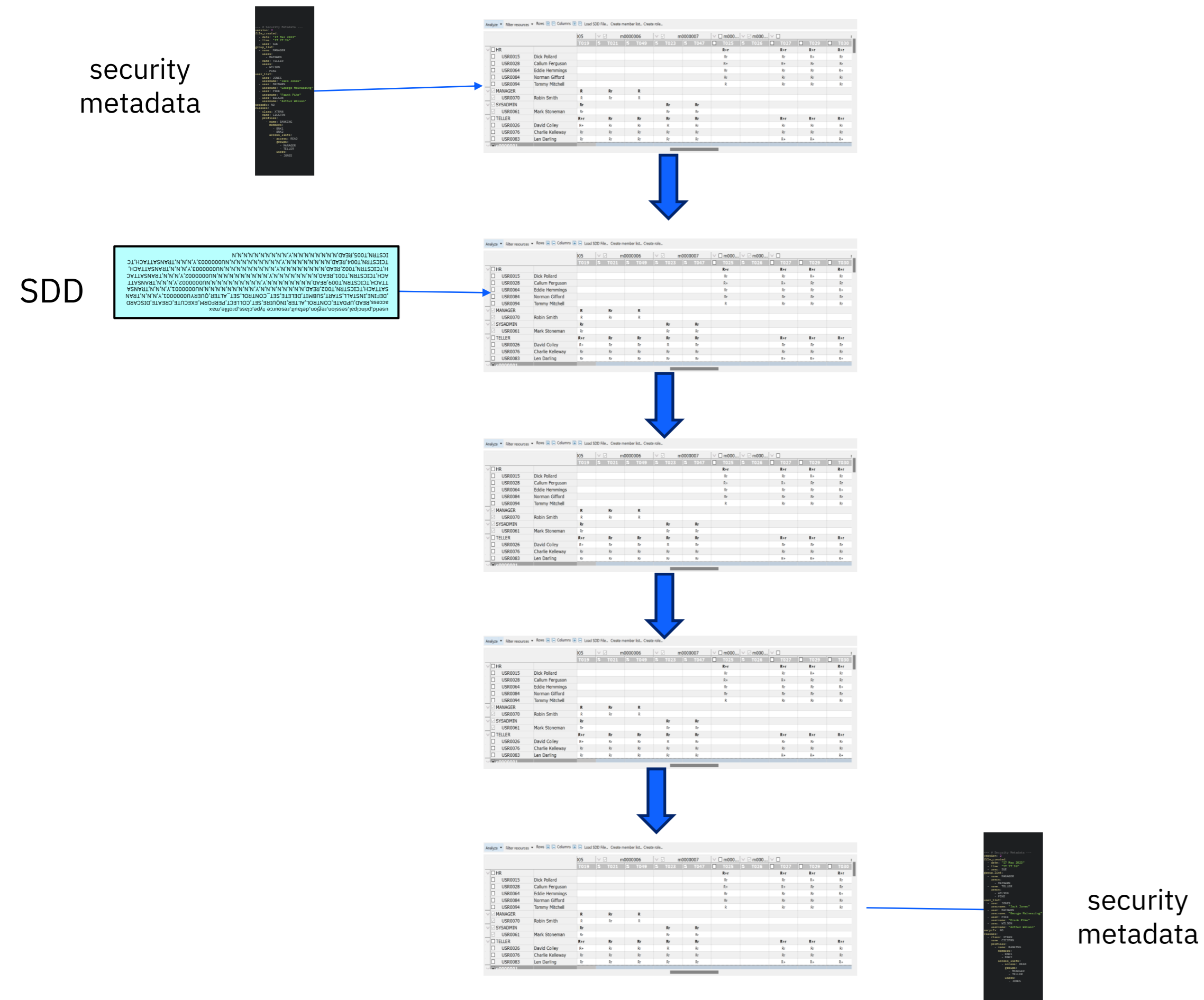
```
Security Discovery records      :      20
Transactions executed          :      24
Successful resource checks     :     179
  Checks that bypassed DFHXSRC :      54
  Checks that called DFHXSRC   :     172
  Exempt resources             :      32
  Resource class not active    :       2
  FASTAUTH calls               :     138
  AUTH calls                   :       0
Resource class counts
  XCMD checks                  :      24
  XDB2 checks (class not active) :       0
  XDCT checks                  :       6
  XFCT checks (class not active) :      47
  XHFS checks (class not active) :       0
  XJCT checks (class not active) :       0
  XPCT checks (class not active) :       0
  XPPT checks                  :     120
  XPSB checks (class not active) :       0
  XRES checks (class not active) :       2
  XTRAN checks                 :      21
  XTST checks (class not active) :       5
```

Analysing the data using CICS Explorer

Details of the process of using the Security Discovery perspective in the CICS Explorer to analyse security metadata and SDD to identify roles and member lists for transactions and resources



Stages of analysis



1. Identify roles and transaction member lists
2. Refine users in roles
3. Define Application Filters
4. Identify resource member lists and refine roles
5. Export security metadata and review applications

RACF definitions imported into the Security Discovery editor

1

Import the security metadata .esm file

Example has transaction definitions by user ID (no groups or member lists)

R indicates that a user ID has READ access to the transaction

Analyze ▾ Filter resources ▾ Rows Columns Load SDD File... Create member list... Create role...

| | | Ungrouped | | | | | | | | | |
|--|---------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | | T001 | T002 | T003 | T004 | T005 | T006 | T007 | T008 | T009 | T00a |
| <input checked="" type="checkbox"/> Unresolved | | | | | | | | | | | |
| <input checked="" type="checkbox"/> U0000001 | Tom Richmond | R | R | R | R | R | | R | R | R | R |
| <input checked="" type="checkbox"/> U0000002 | Bruce Laird | | | R | | | R | R | | | R |
| <input checked="" type="checkbox"/> U0000003 | Paul Jarvis | R | | R | R | | | R | R | R | |
| <input checked="" type="checkbox"/> U0000004 | Jack Wilson | R | R | R | R | R | | R | R | R | R |
| <input checked="" type="checkbox"/> U0000005 | Chris Adams | | | R | | | | R | R | R | |
| <input checked="" type="checkbox"/> U0000006 | Steve Rhodes | | R | | | R | R | R | | | R |
| <input checked="" type="checkbox"/> U0000007 | Paul Parker | | | R | | | | R | R | R | |
| <input checked="" type="checkbox"/> U0000008 | Harry Lee | | R | | | R | R | R | | | R |
| <input checked="" type="checkbox"/> U0000009 | Mark Ealham | | | R | | | R | R | | | R |
| <input checked="" type="checkbox"/> U0000010 | Mark Stoneman | R | | R | R | | | R | R | R | |

Transaction security definitions grouped by similarity

1 Suggests groups and member lists with similar access

Example has transaction definitions by user ID (no groups or member lists)

R+ indicates that if the suggestion is accepted, the user ID will gain access

| Analyze ▾ Filter resources ▾ Rows Columns Load SDD File... Create member list... Create role... | | | | | | | | | | | |
|---|---------------|-------------------------------------|-------------------------------|--|--|--|--|---|---|---|---|
| | | ▼ <input type="checkbox"/> m0000000 | | | | ▼ <input checked="" type="checkbox"/> m0000001 | | ▼ <input checked="" type="checkbox"/> m000... | ▼ <input checked="" type="checkbox"/> m000... | ▼ <input checked="" type="checkbox"/> m000... | ▼ <input checked="" type="checkbox"/> m000... |
| | | <input type="checkbox"/> T001 | <input type="checkbox"/> T004 | <input checked="" type="checkbox"/> T008 | <input checked="" type="checkbox"/> T009 | <input checked="" type="checkbox"/> T002 | <input checked="" type="checkbox"/> T005 | <input checked="" type="checkbox"/> T003 | <input checked="" type="checkbox"/> T006 | <input checked="" type="checkbox"/> T007 | <input checked="" type="checkbox"/> T00a |
| ▼ <input checked="" type="checkbox"/> g0000000 | | R+ | R+ | R | R | | | R | | R | |
| <input checked="" type="checkbox"/> U0000003 | Paul Jarvis | R | R | R | R | | | R | | R | |
| <input type="checkbox"/> U0000005 | Chris Adams | R+ | R+ | R | R | | | R | | R | |
| <input type="checkbox"/> U0000007 | Paul Parker | R+ | R+ | R | R | | | R | | R | |
| <input checked="" type="checkbox"/> U0000010 | Mark Stoneman | R | R | R | R | | | R | | R | |
| ▼ <input checked="" type="checkbox"/> g0000001 | | R | R | R | R | R | R | R | | R | R |
| <input checked="" type="checkbox"/> U0000001 | Tom Richmond | R | R | R | R | R | R | R | | R | R |
| <input checked="" type="checkbox"/> U0000004 | Jack Wilson | R | R | R | R | R | R | R | | R | R |
| ▼ <input checked="" type="checkbox"/> g0000002 | | | | | | R | R | | R | R | R |
| <input checked="" type="checkbox"/> U0000006 | Steve Rhodes | | | | | R | R | | R | R | R |
| <input checked="" type="checkbox"/> U0000008 | Harry Lee | | | | | R | R | | R | R | R |
| ▼ <input checked="" type="checkbox"/> g0000003 | | | | | | | | R | R | R | R |
| <input checked="" type="checkbox"/> U0000002 | Bruce Laird | | | | | | | R | R | R | R |
| <input checked="" type="checkbox"/> U0000009 | Mark Ealham | | | | | | | R | R | R | R |

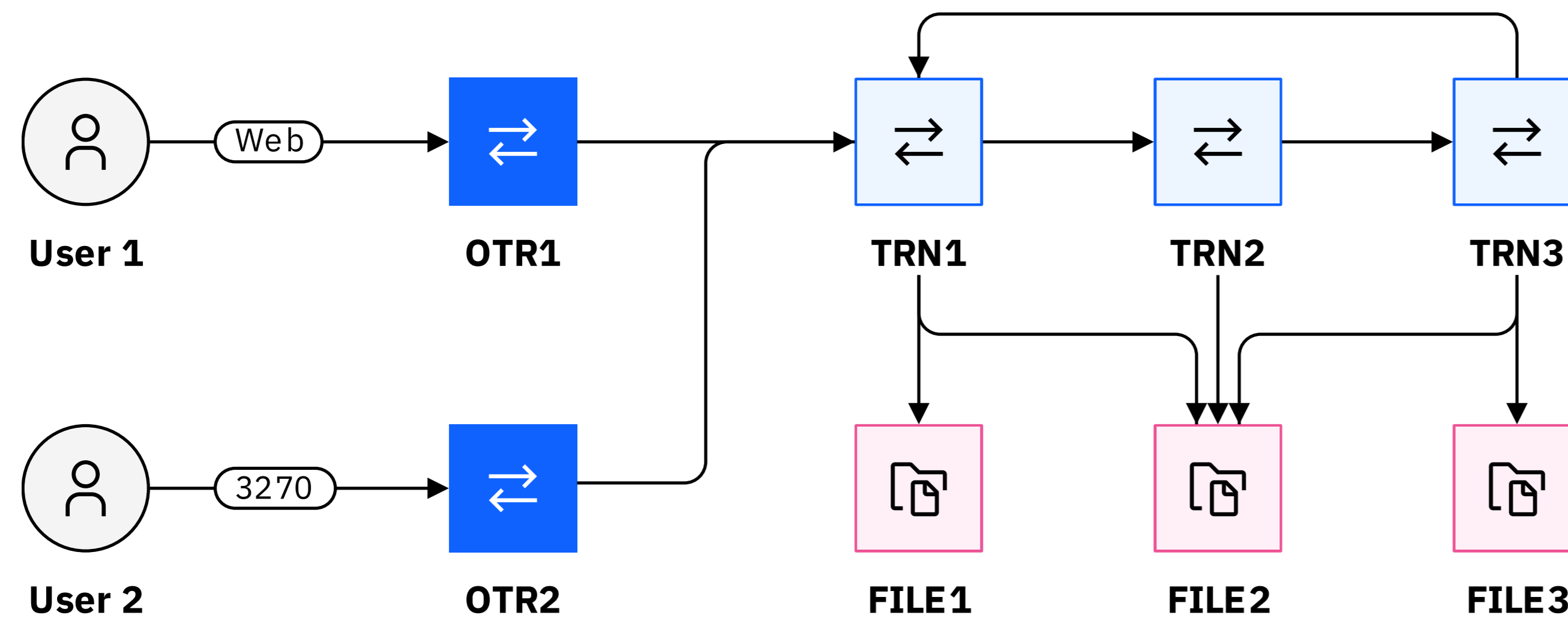
What is an application?

3

User in a role has access to transactions and resources

Access may be through specific entry points, represented by origin transactions

Different users (roles) may have different accesses to transactions and resources



○ Users ■ Origin transactions □ Transactions □ File resources

Selecting origin transactions

3

Select all the origin transaction associated with the application

All transactions associated with these origins will be displayed as pending

All member lists including these transaction will be displayed with # of transactions

The screenshot displays a software interface with four main panels:

- Application filter attributes:** Contains a dropdown menu for 'Filter name' (set to 'Banking'), a text input for 'Description', and another for 'Owner'. Below these are buttons for 'New...', 'Duplicate...', 'Rename...', and 'Delete'.
- Origin transactions:** Features a search filter, a 'Select all' checkbox, and a table with columns 'Select' and 'Origin transacti...'. The table lists transactions T002, T006, T009, T012, and T016. T002 and T006 are checked.
- Transaction member lists:** Includes a search filter, a 'Select all' checkbox, and a table with columns 'Select', 'Member list', and 'Fit'. The table shows 'APP1' with a fit of '5/5' and 'APP2' with a fit of '2/7'. 'APP1' is selected.
- Application transactions:** Shows a search filter and two columns: 'Included' and 'Pending'. The 'Pending' column lists transactions T001, T007, T002, T003, T004, and T005.

Selecting member lists

3

Select all the member list which give access to this application

All user roles for the application will automatically be added when you include member lists

Warning triangles indicate transactions which are not part of the application (need resolving)

Analyze ▾ Filter resources ▾ Rows Columns Load SDD File... Create member list... Create role...

Resource type filter=XTRAN: Application=Banking: Displayed roles=21: Displayed member lists=2

| | | APP2 | | | | | | | | | |
|-------------------------------------|---------|------------------|-------------------------------------|------|-------------------------------------|------|--|--|--|--|--|
| <input checked="" type="checkbox"/> | USR0219 | Chris Read | <input checked="" type="checkbox"/> | T006 | <input checked="" type="checkbox"/> | T007 | <input checked="" type="checkbox"/> ⚠ T044 | <input checked="" type="checkbox"/> ⚠ T045 | <input checked="" type="checkbox"/> ⚠ T046 | <input checked="" type="checkbox"/> ⚠ T047 | <input checked="" type="checkbox"/> ⚠ T048 |
| <input checked="" type="checkbox"/> | USR0267 | Tim Bresnan | | | | | | | | | |
| <input checked="" type="checkbox"/> | VENTUPD | | | | | | | | | | |
| <input checked="" type="checkbox"/> | USR0007 | Sammy Carter | | | | | | | | | |
| <input checked="" type="checkbox"/> | USR0030 | Paul Collingwood | | | | | | | | | |
| <input checked="" type="checkbox"/> | USR0219 | Chris Read | | | | | | | | | |
| <input checked="" type="checkbox"/> | VIEWERS | | Rr | Rr | Rr | Rr | R | Rr | Rr | | |

Application filter attributes

Filter name: Banking

Description:

Owner:

New... Duplicate... Rename... Delete

Origin transactions

Select all

| Select | Origin transacti... |
|-------------------------------------|---------------------|
| <input checked="" type="checkbox"/> | T002 |
| <input checked="" type="checkbox"/> | T006 |
| <input type="checkbox"/> | T009 |
| <input type="checkbox"/> | T012 |

Transaction member lists

Select all

| Select | Member list | Fit |
|-------------------------------------|-------------|-----|
| <input checked="" type="checkbox"/> | APP1 | 5/5 |
| <input checked="" type="checkbox"/> | APP2 | 2/7 |

Application transactions

| Included | Pending |
|----------|---------|
| T001 | |
| T007 | |
| T002 | |
| T003 | |
| T004 | |

Transaction security definitions defined by the Banking application filter

3 Application is now completely defined

This defines all the user roles and transaction member lists for the application

This can be exported into security metadata and reviewed by the application owner

Analyze ▾ Filter resources ▾ Rows Columns Load SDD File... Create member list... Create role...

Resource type filter=XTRAN: Application=[Banking](#): Displayed roles=21: Displayed member lists=14

| | | APP2 | | | | | | |
|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | | T006 | T007 | T044 | T045 | T046 | T047 | T048 |
| <input checked="" type="checkbox"/> | VIEWERS | Rr | Rr | Rr | Rr | R | Rr | Rr |
| <input checked="" type="checkbox"/> | USR0042 George Studd | Rr | Rr | R | R | R | R | R |
| <input checked="" type="checkbox"/> | USR0099 Kurtis Patterson | R | R | R | R | R | R | Rr |
| <input checked="" type="checkbox"/> | USR0243 Bill Johnston | R | R | Rr | Rr | R | Rr | R |
| <input checked="" type="checkbox"/> | USR0256 Ernie Hayes | R | R | R | R | R | R | Rr |
| <input checked="" type="checkbox"/> | USR0293 Tom Hogan | R | R | R | R | R | R | Rr |
| <input checked="" type="checkbox"/> | VIEWERSU | | | | | | | |

Application filter attributes

Filter name: Banking ▾
Description:
Owner:

New... Duplicate... Rename... Delete

Origin transactions

Select all

| Select | Origin transacti... |
|-------------------------------------|---------------------|
| <input checked="" type="checkbox"/> | T002 |
| <input checked="" type="checkbox"/> | T006 |
| <input checked="" type="checkbox"/> | T009 |
| <input checked="" type="checkbox"/> | T012 |

Transaction member lists

Select all

| Select | Member list | Fit |
|-------------------------------------|-------------|-----|
| <input checked="" type="checkbox"/> | APP2 | 7/7 |
| <input checked="" type="checkbox"/> | CURRENT | 6/6 |
| <input checked="" type="checkbox"/> | MCP | 6/8 |

Application transactions

| Included | Pending |
|----------|---------|
| T044 | |
| T022 | |
| T002 | |
| T032 | |
| T009 | |

Transaction security definitions defined by the Banking application filter

3

Review with Application Owner

They are only looking at existing transaction security

If there are any changes go back to CICS Explorer and amend

```
--- # Security Metadata ---
version: 2
file_created:
  - date: "10 Mar 2024"
  - time: "12:33:24"
  - user: SUE
application:
  - name: "Current Account"
  - owner: "Claude Gordon"
  - description: "Front office account application"
origin_transactions:
  - TRN1
  - TRN2
group_list:
  - name: MANAGER
    users:
      - MAINWRN
  - name: TELLER
    users:
      - WILSON
      - PIKE
user_list:
  - user: MAINWRN
    username: "George Mainwaring"
  - user: PIKE
    username: "Frank Pike"
  - user: WILSON
    username: "Arthur Wilson"
secprfx: NO
```

```
classes:
  - class: XTRAN
    name: CICSTRN
    profiles:
      - name: BANKING
        members:
          - BNK1
          - BNK2
        access_lists:
          - access: READ
            groups:
              - MANAGER
              - TELLER
```


Role groups with proposed access to FILE resources for the application

4

Best file analysis will then match these with copies of the existing transaction roles

The roles have +r or +u for example to indicate that all resources are accessed READ or UPDATE

Groups are then merged or renamed

The R+ or U+ indicate the RACF access that will be given, if accepted

Analyze ▾ Filter resources ▾ Rows Columns Load SDD File... Create member list... Create role...

Resource type filter=XFCT: Application=No application: Displayed roles=39: Displayed member lists=31

| | | m000... | m000... | m000... | m000... | m000... | m000... | m000... | m000... |
|-------------------------------------|---------|------------------|------------|------------|------------|------------|------------|------------|------------|
| | | 0017 | FI0028 | FI0030 | FI0031 | FI0032 | FI0034 | FI0035 | FI0037 |
| <input type="checkbox"/> | USR0271 | Rex Sellers | U+u | U+ | U+u | | U+u | U+ | |
| <input checked="" type="checkbox"/> | VENT | | | | | | | | |
| <input checked="" type="checkbox"/> | USR0007 | Sammy Carter | | | | | | | |
| <input checked="" type="checkbox"/> | USR0030 | Paul Collingwood | | | | | | | |
| <input checked="" type="checkbox"/> | USR0219 | Chris Read | | | | | | | |
| <input checked="" type="checkbox"/> | USR0267 | Tim Bresnan | | | | | | | |
| <input type="checkbox"/> | VENT+r | | R+r | R+r | R+r | R+r | R+r | R+r | R+r |
| <input type="checkbox"/> | USR0007 | Sammy Carter | R+r | R+r | R+r | R+r | R+r | R+r | R+r |
| <input type="checkbox"/> | USR0030 | Paul Collingwood | R+ | R+ | R+r | R+r | R+r | R+ | R+r |
| <input type="checkbox"/> | USR0219 | Chris Read | R+r | R+ | R+r | R+r | R+r | R+ | R+r |
| <input type="checkbox"/> | USR0267 | Tim Bresnan | R+r | R+r | R+r | R+r | R+r | R+r | R+r |
| <input type="checkbox"/> | VENT+u | | U+u | U+u | | | | U+u | |
| <input type="checkbox"/> | USR0007 | Sammy Carter | U+u | U+u | | | | U+u | |
| <input type="checkbox"/> | USR0030 | Paul Collingwood | U+u | U+u | | | | U+u | |
| <input type="checkbox"/> | USR0219 | Chris Read | U+ | U+u | | | | U+u | |
| <input checked="" type="checkbox"/> | VIEWERS | | | | | | | | |
| <input checked="" type="checkbox"/> | USR0042 | Georae Studd | | | | | | | |

Export security metadata and review application

5

Review with Application Owner

If there are any changes go back to CICS Explorer and amend.

```
--- # Security Metadata ---
version: 2
file_created:
  - date: "17 Mar 2024"
  - time: "17:27:26"
  - user: SUE
application:
  - name: "Current Account"
  - owner: "Claude Gordon"
  - description: "Front office account application"
  origin_transactions:
    - TRN1
    - TRN2
group_list:
  - name: MANAGER
    users:
      - MAINWRN
  - name: TELLER
    users:
      - WILSON
      - PIKE
user_list:
  - user: MAINWRN
    username: "George Mainwaring"
  - user: PIKE
    username: "Frank Pike"
  - user: WILSON
    username: "Arthur Wilson"
secprfx: NO
```

```
classes:
- class: XTRAN
  name: CICSTRN
  profiles:
    - name: BANKING
      members:
        - BNK1
        - BNK2
      access_lists:
        - access: READ
          groups:
            - MANAGER
            - TELLER
- class: XFCT
  name: CICSFCT
  profiles:
    - name: BANKING
      members:
        - CURRENT
        - SAVING
      access_lists:
        - access: READ
          groups:
            - MANAGER
            - TELLER
        - access: UPDATE
          groups:
            - MANAGER
```

Changes to RESSEC and CMDSEC

Zero Trust and Compliance with PCI-DSS

- It is recommended that customers use resource and command security for production regions to secure sensitive data
- Unfortunately, RESSEC(NO) CMDSEC(NO) was the default
- Simple solution would be to use SIT parameters RESSEC=ALWAYS, CMDSEC=ALWAYS

But ...

- Many CICS transactions are defined with RESSEC(NO) and CMDSEC(NO)
- There are implications for CICS and Customer transactions
- Security definitions may need to be defined

Changing CICS Definitions

All CICS transactions changed to RESSEC(YES) CMDSEC(YES)

- Many don't have resource security checks
- **Some unnecessary security checks removed** (trusted application)
- Where security is required **single table of security documentation**

Existing definitions added to compatibility group DFHCOMPK

Why do some CICS transactions not require command/resource security checking?

*Enable the right user,
to have the right access,
to the right data,
for the right reasons*

CICS code is trusted as long as it's totally encapsulated

Signoff transaction CESF is trusted
Commands issued by CECI are not trusted

CESF write a message to CSMT TDQ

Pointless requiring security definitions for CESF to do this

If users had access for CESF, they'd have it for anything it does

Changing Customer Definitions

*Enable the right user,
to have the right access,
to the right data,
for the right reasons*

RESSEC(YES) and CMDSEC(YES) is the new default for transaction definitions

Existing transactions definitions are **not changed**

Use Security Discovery to implement RACF definitions before changing either the RESSEC or CMDSEC transaction values

After all transaction are changed consider using either

- RESSEC=ALWAYS and CMDSEC=ALWAYS
- Resource builder to ensure new transactions conform

Security Definition Capture

The problem

How do you identify security definitions for a new application?

Or

How do you identify security changes when updating an application?

- Preprod is usually earliest part of security testing
- Developers often go through sysprogs to get security definitions
- Getting security permissions is a slow process

External Research (Jan 2023)

<https://devclass.com/2023/01/26/devsecops-report/>

*“the biggest barrier to DevSecOps being that security teams do not trust developers, identified by 55 percent of organizations as the top issue” **

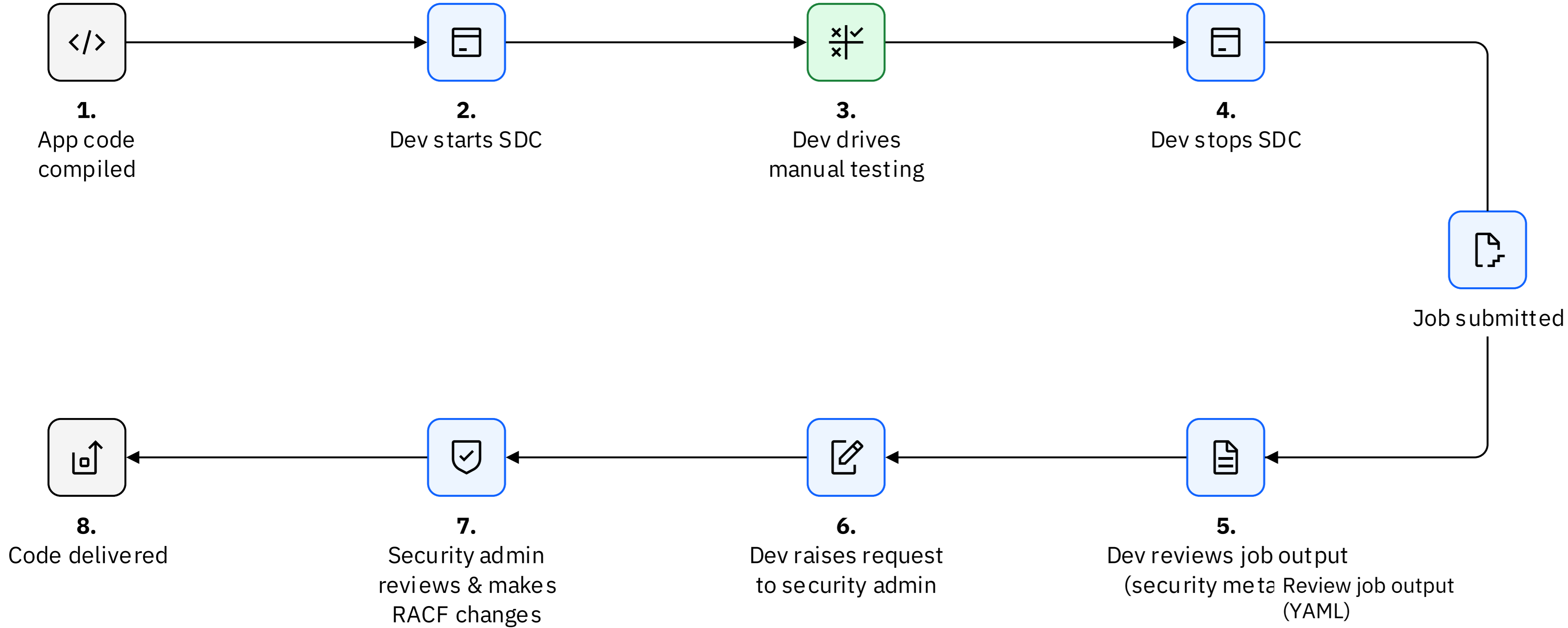
* Based on a survey of 1300 DevOps and Security professionals in large enterprises

Security Definition Capture

- Identify security definitions during testing
- Can use development system with minimal security (SEC=YES)
- No knowledge of security required by developer

- Restful interface and 3270 transaction to switch on/off
- Security metadata automatically created at end of test
- Security metadata can be sent to developer or security admin

Manually identify security definitions



Security Test Other development stages

Starting & Stopping SDC

3270 Process

- Sign on to terminal
- CXSD ON
- Run tests
- CXSD OFF

Captures security definitions originating from this terminal

Non-3270 Process

- HTTP POST to SDC endpoint
 - Supply credentials
- Run tests
- HTTP DELETE to SDEC endpoint

Captures security definitions for this user ID

Security Metadata

The user name is that of the developer/tester

They would represent a user role for the production security definition

```
--- # Security Metadata
version: 2
file_created:
  - date: "15 Mar 2024"
  - time: "09:33:24"
  - user: U000125
classes:
- name: XFCT
  profiles:
    - name: FILEA
      access_lists:
        - access: READ
          users:
            - U000125
    - name: FILEB
      access_lists:
        - access: READ
          users:
            - U000125
- name: XTRAN
  profiles:
    - name: TRNA
      access_lists:
        - access: READ
          users:
            - U000125
```

The resource type (file)

File name

Access level

User name

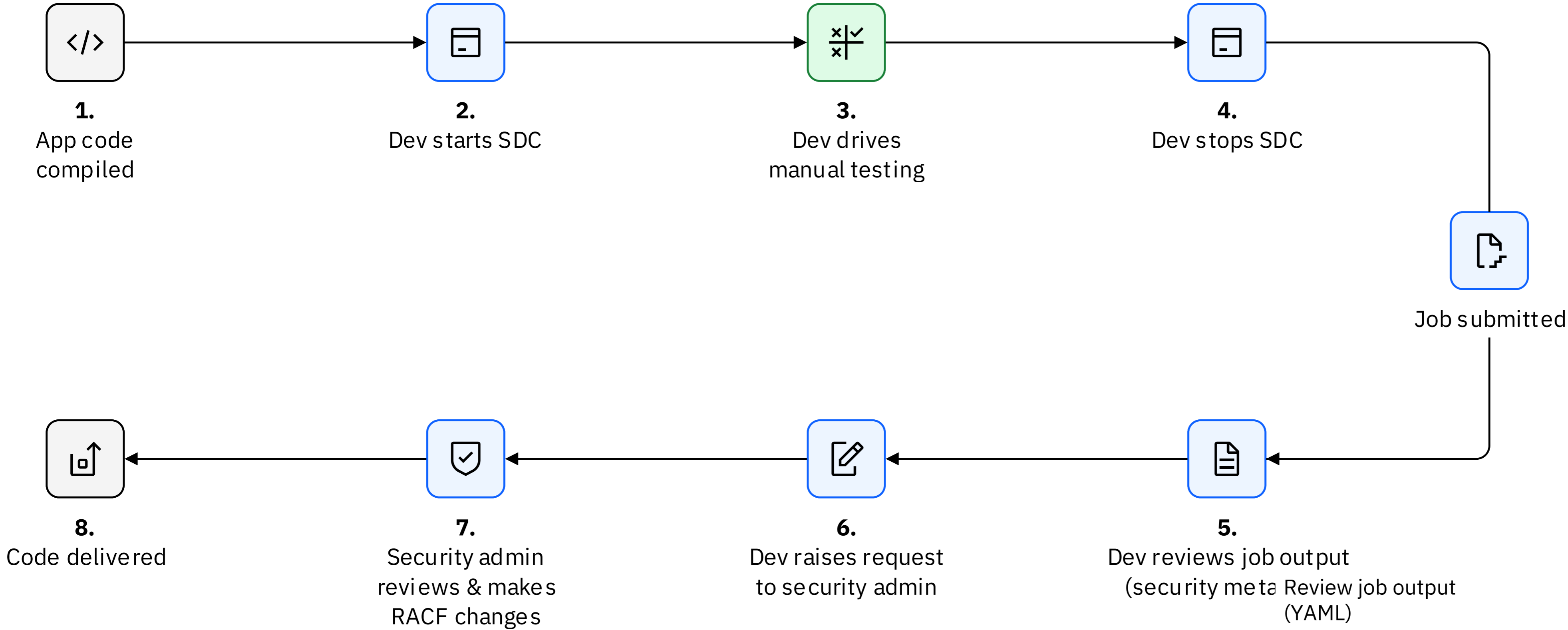
Security Definition Validation

How do we automate this?

- Automated tests are tagged with the test role (e.g. TELLER)
- SDC started and stopped before after the test
- Security metadata changes can be reviewed

Open source example of this process using Galasa will be made available.

Moving towards a DevSecOps process



Security Test Other development stages

Security metadata

Before code change

```
--- # Security Metadata
version: 2
group_list:
  - name: TELLER
classes:
- name: XFCT
  profiles:
    - name: FILEA
      access_lists:
        - access: READ
      groups:
        - TELLER
    - name: FILEB
      access_lists:
        - access: READ
      groups:
        - TELLER
- name: XTRAN
  profiles:
    - name: TRNA
      access_lists:
        - access: READ
      groups:
        - TELLER
```

After code change

```
--- # Security Metadata
version: 2
group_list:
  - name: TELLER
classes:
- name: XFCT
  profiles:
    - name: FILEA
      access_lists:
        - access: READ
      groups:
        - TELLER
    - name: FILEB
      access_lists:
        - access: UPDATE
      groups:
        - TELLER
- name: XTRAN
  profiles:
    - name: TRNA
      access_lists:
        - access: READ
      groups:
        - TELLER
```

The automation specifies the role of the test: TELLER

This replaces the user ID in the security metadata

Security changes required

```
- name: FILEB
  access_lists:
  D - - access: READ
  I - - access: UPDATE
  groups:
    - TELLER
```



TLS Enhancements

TLS Enhancements

Certificate Expiry Detection

Support for virtual and shared keyrings

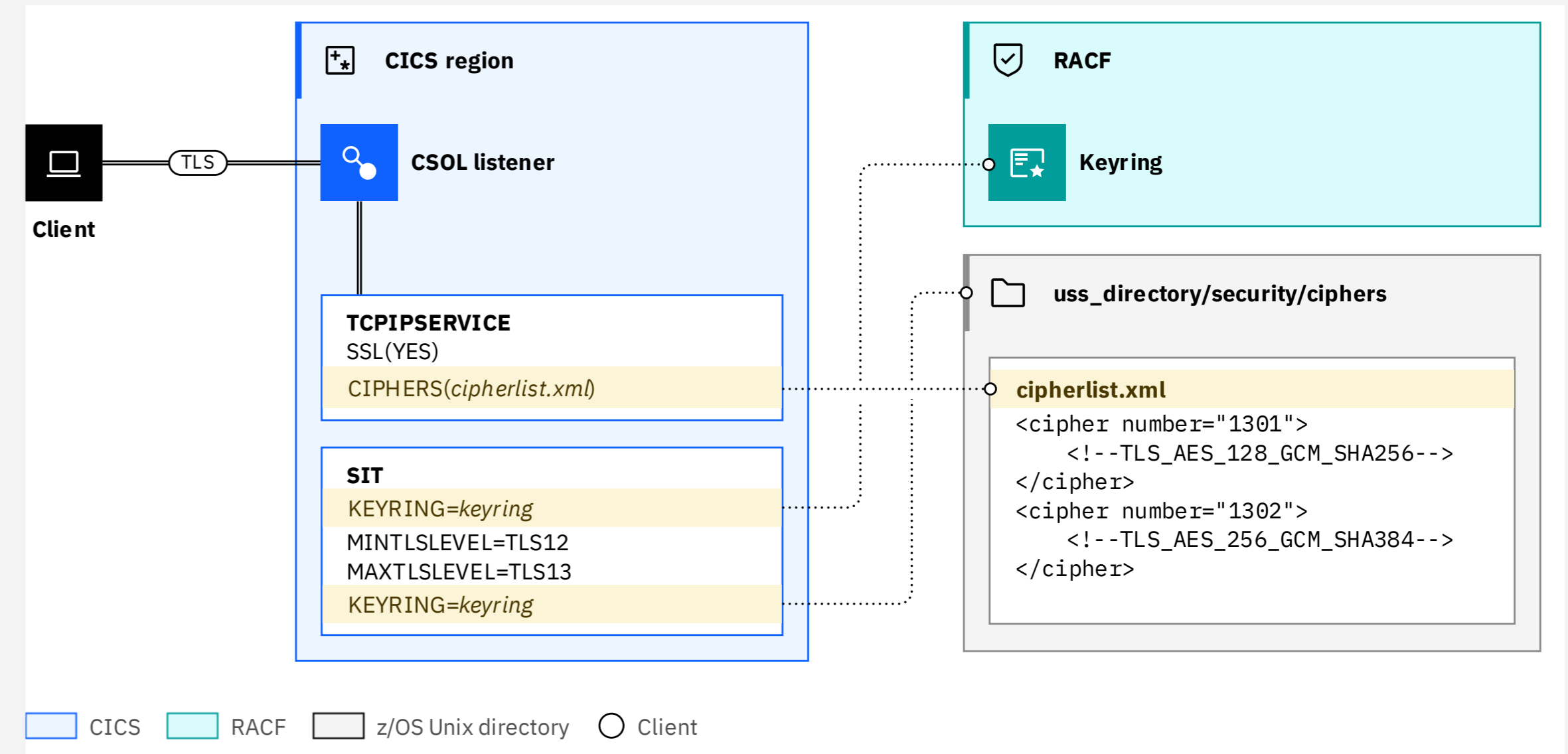
Increase key strength of TLS cipher keys

Sysplex Cache for TLS 1.3

Support for strict transaction security (HSTS)

Certificate Diagnostics

Message for IP Stack Failure



Certificate Expiry Detection

Health Checker for z/OS

```
CHECK(IBMRA CF,RACF_CERTIFICATE_EXPIRATION)
SYSPLEX: PLEX2 SYSTEM: MV2C
START TIME: 11/07/2023 06:02:03.363846
CHECK DATE: 20111010 CHECK SEVERITY: MEDIUM

          Certificates Expiring within 60 Days

S Cert Owner      Certificate Label                End Date  Trust Rings
-----
E ID(USR0843)    GSmith-2048-Certificate          2023-12-17 Yes         1
E ID(USR0512)    Keyring26-Default-Certificate    2023-12-30 No          0
E ID(USR0234)    JBlogg-2048-Certificate          2023-12-31 Yes         0
```

What about certificates not in RACF database

- Client certificates
- External Server certificates
- Signing certificates in certificate chain

New SIT option

```
CERTEXPIRYWARN={NO|expiry_days}
```

Warns if certificates will expire within *expiry_days*

Message DFHS01100 with details of certificate

```
DFHS01100I date time applid SubjectDN: subjectDN,
IssuerDN: issuerDN, Serial Number: serialNumber,
Data Source: dataSource, Not Before: notBefore,
Not After: notAfter
```

Very small performance cost in WOR, see CICS performance report

Support for virtual and shared keyrings

Before the change:

- KEYRING=keyring
- keyring owned by the regionID

1000's of regions require either
shared regionIDs
or multiple keyrings

A **virtual keyring** is a set of all certificates owned by a userid

```
KEYRING=ringowner/*
```

- *ringowner* is the owning userid
- * is all certificates owned by that userid

Shared keyrings used by a different userid to the regionID

```
KEYRING=userid/keyringname
```

There are two special userids that can be used:

- *AUTH* - all CA certificates (used for client only regions)
- *SITE* - server regions that share a SITE certificate

APAR PH49253 for CICS TS 5.5, 5.6

APAR PH49261 for CICS TS 6.1

Increase key strength of TLS cipher keys

New feature toggle:

```
com.ibm.cics.tls.minimumkeystrength={1024|2048}
```

- Set minimum keysize during TLS handshakes
- 2048 for RSA, DSA and Diffie-Hellman
256 for ECC

If 2048 set the System SSL settings will be in effect:

```
GSK_CLIENT_ECURVE_LIST=0025002400230030002  
GSK_SERVER_ALLOWED_KEX_ECURVES=00250024002300300029  
GSK_CLIENT_EPHEMERAL_DH_GROUP_SIZE=2048  
GSK_SERVER_EPHEMERAL_DH_GROUP_SIZE=2048  
GSK_PEER_DH_MIN_KEY_SIZE=2048  
GSK_PEER_DSA_MIN_KEY_SIZE=2048  
GSK_PEER_ECC_MIN_KEY_SIZE=256  
GSK_PEER_RSA_MIN_KEY_SIZE=2048
```

APAR PH50175 for CICS TS 5.4, 5.5, 5.6

APAR PH51719 for CICS TS 6.1

Sysplex Cache for TLS 1.3

- TLS 1.3 is very different to TLS 1.2
- More secure
- No common ciphers with TLS 1.2
- Different performance characteristics
- See CICS performance report

```
SSLCACHE=CICS | SYSPLEX
```

CICS TS 6.1 introduced TLS 1.3

- No support for caching

CICS TS 6.2

- Support for caching using System SSL

z/OS 3.1 or

z/OS 2.5 with APARs OA63252 and OA63164

Support for strict transaction security (HSTS)

- RFC 6797
- Instructs browsers only to interact with servers using HTTPS
- Adds the follow header (for example)

```
Strict-Transport-Security: max-age=86400; includeSubDomains
```

- Doesn't override EXEC CICS WEB WRITE HTTPHEADER
- Doesn't apply to Liberty
 - Separate control in server.xml

Settings for a CICS region

- Activate HSTS for region and sets the max-age time

```
com.ibm.cics.web.hsts.max-age=seconds
```

- Controls HSTS to subdomains in CICS

```
com.ibm.cics.web.hsts.includesubdomains={true|false}
```

Override for a specific TCPIP SERVICE (TCPIPS)

- Set HSTS time for a TCPIP SERVICE (or deactivates -1)

```
com.ibm.cics.web.hsts.max-age.TCPIPS={seconds|-1}
```

- Controls HSTS to subdomains in CICS for TCPIP SERVICE

```
com.ibm.cics.web.hsts.includesubdomains.TCPIPS={true|false}
```

APAR PH55369 for CICS TS 5.5, 5.6

APAR PH55370 for CICS TS 6.1

Certificate Diagnostics

More detailed error messages and diagnostics

- Identifying the certificate chain
- Identifying the certificate in error

Additional trace information

- SO level 2
- Trace full certificate chain

Example of the certificate diagnostics

Certificate Index : 1

```
SubjectDN      : CN=gb1220_chrome,OU=CICS TS,0=IBM,L=Hursley,ST=Hampshire,C=UK
IssuerDN       : CN=CICS TLS 1.3 CA,OU=CICS TS Dev,0=IBM,L=Hursley,ST=hampshire,C=UK
Serial Number  : 0c
Data Source    : Handshake
Not Before     : 230223000000Z
Not After      : 240223000000Z
```

Certificate Index : 2

```
SubjectDN      : CN=CICS TLS 1.3 CA,OU=CICS TS Dev,0=IBM,L=Hursley,ST=hampshire,C=UK
IssuerDN       : CN=CICS TLS 1.3 CA,OU=CICS TS Dev,0=IBM,L=Hursley,ST=hampshire,C=UK
Serial Number  : 00
Data Source    : ChrisP2I
Not Before     : 220427230000Z
Not After      : 230427230000Z
```

Additional TLS configuration

CICS TLS SIT parms

- MINTLSLEVEL
- MAXTLSLEVEL
- SSLCACHE
- KEYRING

USSCONFIG

- Location of cipher files

CICS uses System SSL

- SIT parms set GSK_ parameters

Set other GSK parms

- Globally in PARMLIB(CEEPRMxx)
 - CELQDOPT option
- For a CICS Region
 - PDS member in CEEOPTS DD

```
ENVAR("GSK_parm1=value",  
      "GSK_parm2=value")
```

- Provide by System SSL
- Available on All CICS releases
- CICS TS 6.2 doc lists valid GSK parms
- Cannot override those that CICS sets using SIT parms

Message for IP Stack Failure

If there is an TCP/IP Stack failures

- TCP/IP stack will not be considered to be in the same SYSPLEX
- This results in a generic security violation message (DFHIS2040)
- Not helpful for diagnosis

Client tries to acquire

IPCONN USERAUTH(IDENTIFY)

using unsecured connection from outside the SYSPLEX

New message replaces DFHIS2040

```
DFHIS2041 date time applid Unable to acquire  
IPCONN IPCONNname because USERAUTH(IDENTIFY) is  
not supported for unsecured connections with a  
partner system that is located outside the  
sysplex.
```

Simplification

Terminal security - A powerful command

3270 applications often need to change aspects of their terminal

- e.g. allow mixed case fields in BMS screen

These changes require use of SET TERMINAL

- Requires UPDATE authority for the TERMINAL command
- Required for all users including the transaction
- For user written signon programs, required for default user !

However, SET TERMINAL is a powerful command

- e.g. purge another terminal

Command security checking is removed from

- INQUIRE TERMINAL(termid) ...
- INQUIRE NETNAME(netid) ...
- SET TERMINAL(termid) ...

Exceptions

- Options with system wide impacts ..
- Browses: INQUIRE (START, NEXT, END)
- SET TERMINAL
 - Tracing options: EXITTRACING, TRACING, ZCPTRACING
 - Naming options: OPERID
 - Purging options: PURGETYPE
- SET NETNAME
 - Tracing options: EXITTRACING

Removing this security check makes the system more secure

Security of DPLs

For local transactions the entrypoint is defined on transaction definition

- There is no security check on this program even if XPPT=YES
- Transaction security is therefore the way entrypoints are protected

For mirror transactions the entrypoint is DFHMIRS

- The 1st user program is the 2nd program
- Therefore, transaction security doesn't protect mirror programs

Current solutions (one of the following)

1. Program security on for all programs
 - Recommended if you have sensitive programs in the region
 - However, this is expensive if only the entry needs to be checked
2. Separate mirror transactions for each program
 - Used for load separation, but not really designed as a security solution
3. RYO solutions
 - Difficult to write and maintain – goes against normal security

New DPLONLY option on XPPT SIT parm

DPLONLY

- Performs the security check only on the first program that is linked by the mirror program during distributed program link (DPL).
- It works only when YES or class_name is specified
- ALL
- Existing behavior is maintained with checks on all programs. This is the default

XPPT=({YES|class_name|NO} [, {ALL|DPLONLY}])

Compliance and Auditability

QUERY SECURITY NOLOG

- Main use case is to limit a user's option
- Only display transactions that a user can run
- Improves usability by limiting users' options
- Avoids unnecessary ICH408I security errors

- Could in theory be abused by a rogue developer
- Code should be reviewed before running in CICS
- You can limit what API developers can user

- Need to monitor (ab)usage

New Stats

DFHSTUP name: Failed authorizations NOLOG NOTAUTH

Field name: [XSG_AUTHOR_FAIL_NL_NA](#)

Description: The number of QUERY SECURITY LOGMESSAGE(NOLOG) requests that are successful but returned no authority on READ, UPDATE, CONTROL or ALTER.

Reset characteristic: reset to zero

In summary report

DFHSTUP name: Failed authorizations NOLOG NOTFND

Field name: [XSG_AUTHOR_FAIL_NL_NF](#)

Description: The number of QUERY SECURITY LOGMESSAGE(NOLOG) requests failed with response code 13 NOTFND

Reset characteristic: reset to zero

In summary report

New performance class record fields

Nickname: XSNLNACT

Group: DFHTASK

Field ID: 048

Field Type: A

Field Length: 4 bytes

Nickname: XSNLNFCT

Group: DFHTASK

Field ID: 049

Field Type: A

Field Length: 4 bytes

Last logon information

Best practice requires information about last signon to be available as part of the signon process

Solution

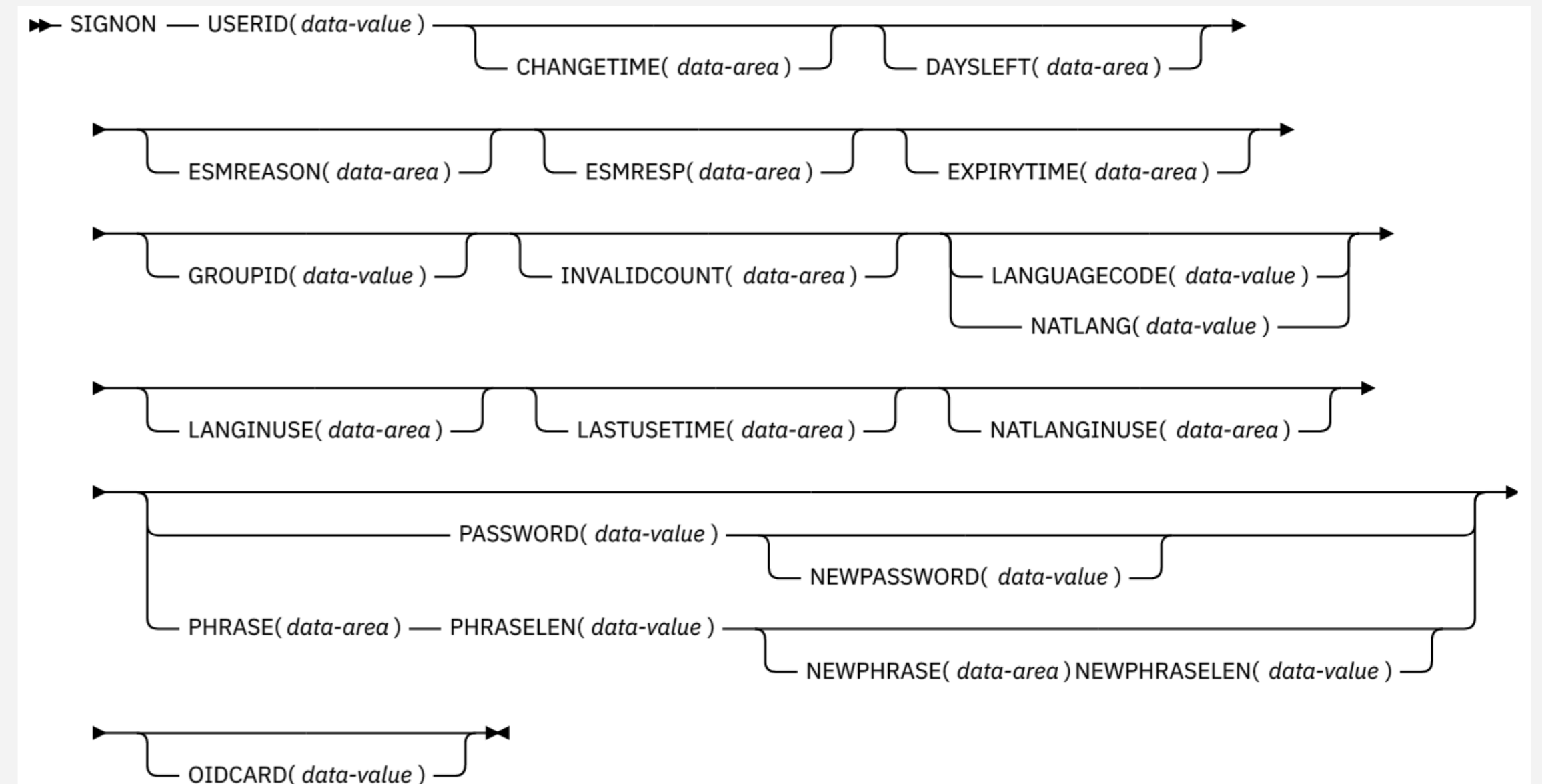
- Changes to SIGNON API
- Changes to messages

Change to SIGNON

New parameters

- CHANGETIME
- EXPIRYTIME
- DAYSLEFT
- INVALIDCOUNT
- LASTUSEDTIME
- Same info as on the VERIFY command

SIGNON



Conditions: INVREQ, LENGERR, NOTAUTH, USERIDERR

Updated Messages

Terminal end user:

DFHCE3549 Sign-on is complete after 2 failed attempts. User ID was last accessed on 15/08/2022 at 122301. (Language ENU).

Destination CSCS

DFHSN1100 15/08/2022 13:48:40 IYK4Z0E3 CESL
Signon at netname IYCXTC05 TN3270 IP Address
9.145.51.223 by user GALLEN in group TSOUSER is
complete after 2 failed attempts. User ID was
last accessed on 15/08/2022 at 12:23:01.

WUI browser:

EYUVC1000I Sign on by user GALLEN successful
after 3 failed attempts. Last access at
13:48:40 on 15/08/22. The password will
expire in 2 days.

EYUVC1001I Sign on by user GALLEN successful
after 0 failed attempts. Last access at
13:58:41 on 16/08/22

Security Doc Restructure

Security documentation restructure

New

- How it works: Zero Trust in CICS
- Implementing a Zero Trust strategy in CICS
- Security for Java applications
- Security for TLS

Updated

- Security for CICS Liberty

The screenshot shows the IBM Documentation website for CICS Transaction Server for z/OS. The page title is "Securing CICS" and it was last updated on 2023-01-05. The left sidebar contains a table of contents with the following items:

- What does security mean for CICS?
 - CICS security is a team sport
 - How it works: identification in CICS
 - How it works: authentication in CICS
 - How it works: authorization in CICS
 - How it works: integrity and confidentiality in CICS
 - How it works: auditing in CICS
 - How it works: Zero trust in CICS
 - How it works: securing CICS with RACF
 - Security through the network layers
 - Security for MRO

The main content area includes the following text:

Use this information to plan and implement security across your CICS® systems.

CICS uses an external security manager (ESM), such as RACF®, to secure CICS systems, and the resources in those systems, against unauthorized access. This documentation assumes that the ESM used is RACF. Example configurations use RACF commands. If you use another ESM, the principles of security are the same but you must use your ESM documentation to find the equivalent configuration details and commands.

This documentation assumes that security is enabled. This is done by setting the SEC system initialization parameter to SEC=YES. For information, see [SEC system initialization parameter](#).

– **What does security mean for CICS?**
CICS Transaction Server itself has security facilities and it also benefits from security capabilities that are integrated into the z/OS operating system and IBM Z hardware. You choose how to apply these facilities, depending on the security objectives for your organization and on the types of CICS environments and applications that you run.

– **CICS security is a team sport**
Whose job is security in CICS? Decisions about security in CICS and its implementation are made by a team of people who fulfill different roles. It's important to understand the different roles and to identify the people who fulfill them in your organization.

– **How it works: identification in CICS**
All CICS tasks are associated with one or more user IDs. The primary user ID is known as the *task user ID*. The task user ID is derived from whoever or whatever started the task - and that can be one of many different things. To differentiate the user ID that comes from each of these starting points, CICS uses different names for them. These names are explained in this document.

– **How it works: authentication in CICS**
CICS handles the authentication process. It requests credentials from a user, decodes the authentication information if necessary, calls RACF or a third-party authentication server to authenticate the supplied credentials, and rejects the request if the authentication fails. It supports different forms of authentication. Your options for authentication depend on the way that you access CICS; see [Which authentication method can I use with which access method?](#) for details.

CICS TS 6.2

Developer productivity

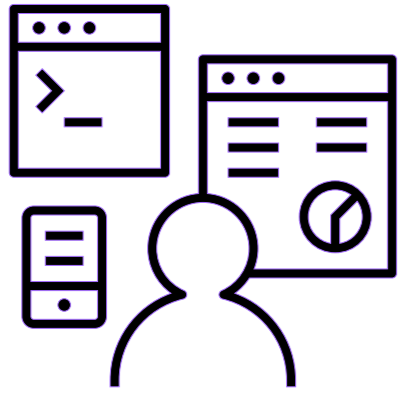


Stew Francis

CICS TS, Architect

stewartfrancis@uk.ibm.com

CICS TS 6.2 - Highlights



Enhanced developer productivity

Developers can use new features in the latest versions of Java, Jakarta, Spring Boot, and Node.js to modernize and extend applications in CICS.

- Support for Java 17
- Support for Jakarta EE 10 and Spring Boot 3
- Support for Node.js 18
- Enhanced CICS container support
- CICS TS resource builder 1.0.4

Java 17

CICS TS 6.2 supports IBM Semeru Runtime Certified Edition for z/OS 17.0.7.0 onwards

Java 8 and Java 11 continue to be supported

Java 17 is an LTS release

Jakarta EE 10 and Spring Boot 3

Jakarta EE 10 is now additionally supported by CICS TS 6.2

Jakarta EE was previously known as Java EE, but was renamed when stewardship was transferred to the Eclipse foundation

A number of updates to included features, including major version updates affecting compatibility

Also introduces support for Spring Boot 3

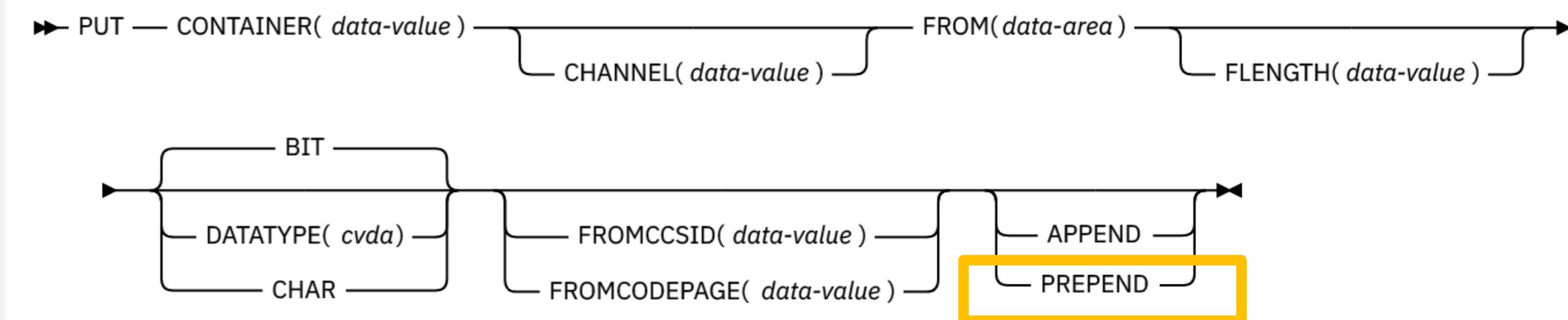
Enhanced CICS containers

CICS TS adds a new PREPEND option to the CONTAINER commands

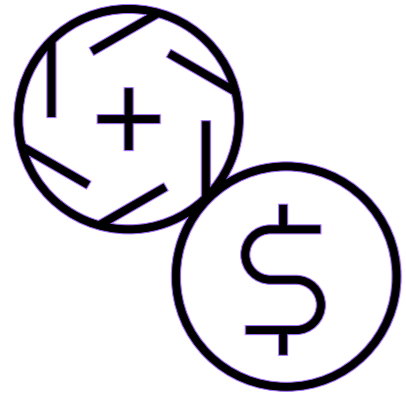
Supported via:

- PUT CONTAINER (CHANNEL)
- PUT64 CONTAINER
- PUT CONTAINER (EXCI)
- JCICS + JCICSX Container API
 - prepend()
 - prependString()

PUT CONTAINER (CHANNEL)



CICS TS 6.2 - Highlights



Reduced cost of
management and resiliency

CICS administrators can further optimise apps with threadsafe access to shared data tables, reduced volumes of data written to SMF, automate more with CICS policies and Ansible, and use the power of the IBM Z platform to further improve resilience and scalability.

- Much expanded CICS TS Ansible collection
- Playbooks for provisioning new CICS regions
- Cloud Broker operator for integration with Red Hat OpenShift

Ansible

Ansible is a general-purpose automation tool

With an extensible architecture, and IBM provides extensions for targeting z/OS and CICS TS (amongst others)

Red Hat's Ansible Automation Platform offering provides enterprise-wide access to automation.

Ansible for z/OS

z/OS is a great candidate for automation with Ansible

ibm_zos_core collection provides foundational support for working with z/OS resources

There are [Ansible collections](#) providing more targeted support for Z, e.g. ibm_zos_ims

Many enhancements to the ibm_zos_cics collection delivered with CICS TS 6.2

```
- name: Create a KSDS data set if it does not exist
zos_data_set:
  name: someds.name.here
  type: ksds
  key_length: 8
  key_offset: 0
```

```
- name: List data sets matching pattern in catalog
zos_mvs_raw:
  program_name: idcams
  auth: true
  dds:
    - dd_input:
      dd_name: sysin
      content: " LISTCAT ENTRIES('SOME.DATASET.*') "
    - dd_output:
      dd_name: sysprint
      return_content:
        type: text
        src_encoding: iso8859-1
        response_encoding: ibm-1047
```


New Modules in the CICS TS Ansible Collection

CICS TS Ansible collection has new modules you can use to provision and manage CICS data sets

auxiliary_temp – DFHTEMP

csd – DFHCSD

global_catalog – DFHGCD

intrapartition – DFHINTRA

local_catalog – DFHLCD

local_request_queue – DFHLRQ

start_cics – Generate CICS JCL

stop_cics – Stop CICS

trace - DFHAUXT, DFHBUXT

transaction_dump – DFHDMPA, DFHDMPB

Don't forget our modules for working with the CICS TS system management API, CMCI!

- name: Run a DFHCSDUP script
ibm.ibm_zos_cics.csd:
state: script
script_src: "USER.DEFS(CSDIN)"
script_location: DATA_SET

- name: Allocate a new Global Catalog
ibm.ibm_zos_cics.global_catalog:
state: initial
cics_data_sets:
sdfhload: CTS620.CICS750.SDFHLOAD
region_data_sets:
dfhgcd:
dsn: MY.REGION.DFHGCD

- name: Stop CICS
ibm.ibm_zos_cics.stop_cics:
job_id: JOB12345

Provisioning CICS TS regions with Ansible

You can use the new Ansible modules to provision, start, stop and deprovision a CICS region

Have a look at our new [samples for provisioning and deprovisioning a CICS region](#) with Ansible on GitHub

```
---
- name: Provision CICS Data sets and start the region
  hosts: all
  gather_facts: false
  vars_files: "{{ playbook_dir }}/host_vars/variables.yml"
  environment: "{{ environment_vars }}"

  vars:
    applid: APPLID

  module_defaults:
    group/ibm.ibm_zos_cics.region_group:
      state: initial
      cics_data_sets:
        template: "CTS610.CICS740.<< lib_name >>"
        sdfhlic: "CTS610.CICS740.LIC.SDFHLIC"
      region_data_sets:
        template: "{{ ansible_user }}.REGIONS.{{ applid }}.<< data_set_name >>"
      le_data_sets:
        template: "CEE.<< lib_name >>"

  tasks:
    - name: Create the auxiliary temporary storage data set (DFHTEMP)
      ibm.ibm_zos_cics.auxiliary_temp:

    - name: Create the auxiliary trace data set (DFHAUXT)
      ibm.ibm_zos_cics.trace:

    - name: Create the second auxiliary trace data set (DFHBUXT)
      ibm.ibm_zos_cics.trace:
        destination: B

    - name: Create the transaction dump data set (DFHDMPA)
      ibm.ibm_zos_cics.transaction_dump:

    - name: Create the second transaction dump data set (DFHDMPB)
      ibm.ibm_zos_cics.transaction_dump:
        destination: B

    - name: Create the CSD data set (DFHCSD)
      ibm.ibm_zos_cics.csd:

    .
    .
    .
```

Provisioning via OpenShift

The CICS TS OpenShift operator, powered by z/OS Cloud Broker can drive our Ansible CICS region provisioning, via the OpenShift UI

The screenshot shows the Red Hat OpenShift console interface for provisioning a CICS region. At the top, the Red Hat OpenShift logo is visible. Below it, the project name is set to 'stewf-dev2'. The main heading is 'Create CICSTSRegion', with a sub-note: 'Create by completing the form. Default values may be provided by the Operator authors.' There are two tabs for configuration: 'Form view' (selected) and 'YAML view'. A blue information box states: 'Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.' The form contains several fields: 'Name' with the value 'sfl'; 'Labels' with the value 'app=frontend'; 'ZosEndpoint Selection' with a dropdown menu showing 'ZE wazi-sandbox' and a note 'The ZosEndpoint to be used for remote execution'; and 'System identifier (SYSID)' with the value 'SF1' and a note: 'Region system identifier. This must be no longer than 3 characters. The region application identifier (APPLID) will be created by prefixing the value of SYSID with 'ZCICS''. At the bottom, there are 'Create' and 'Cancel' buttons.

Project: stewf-dev2

Create CICSTSRegion

Create by completing the form. Default values may be provided by the Operator authors.

Configure via: Form view YAML view

Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.

Name *

sfl

Labels

app=frontend

ZosEndpoint Selection *

ZE wazi-sandbox

The ZosEndpoint to be used for remote execution

System identifier (SYSID) *

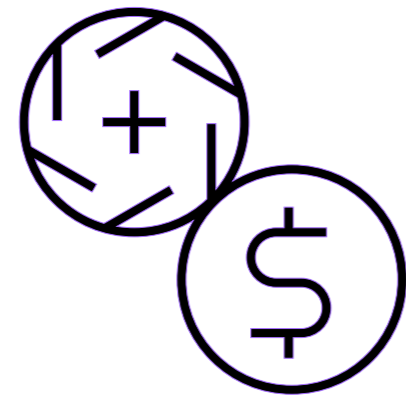
SF1

Region system identifier. This must be no longer than 3 characters. The region application identifier (APPLID) will be created by prefixing the value of SYSID with 'ZCICS'

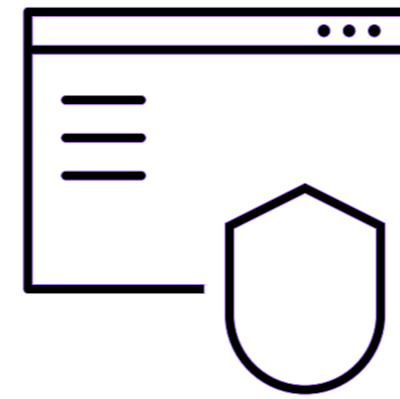
Create **Cancel**

CICS TS 6.2

Questions?



Reduced cost of
management and resiliency



Improved security and
compliance management



Enhanced
developer productivity



Louisa Seers
CICS TS, Product Manager
LOUISASE@uk.ibm.com



Jenny He
CICS TS, Development Lead,
Master Inventor
HEJEN@uk.ibm.com



Colin Penfold
CICS TS, Technical Leader of security
colin_penfold@uk.ibm.com



Mark Cocker
CICS TS, Senior Product Manager
mark_cocker@uk.ibm.com



Stew Francis
CICS TS, Architect
stewartfrancis@uk.ibm.com



John Taylor
CICS TS, Software engineer
JTAYLOR1@uk.ibm.com

CICS INSIGHT Series



Next Session:

May 15th

11:00 AM EDT

Mainframe Modernization with Generative AI

<https://ibm-zcouncil.com/events/insight-may-15/>

In-depth technical discussions led by CICS experts



CICS INSIGHT Series



In-depth technical discussions led by CICS experts

Thank you for attending

Please complete an event survey:

<https://ibm.biz/CICSInsightSurvey>



IBM