DISTRIBUTED ACCESS TO DB2: MUST KNOW!

The Db2 Night Show – Nov 2020

Cristian Molaro
The Mindbridge
cmolaro@themindbridge.com

AGENDA

- Introduction
- Why remote access to db2?
- Distributed configurations
- Security
- Best practices
- Workload management
- Summary and conclusions

THEMIND BRIDGE

ABOUT THE SPEAKER

- **Cristian Molaro**, The Mindbridge
  - Independent DB2 specialist and IBM Gold Consultant
  - Recognized by IBM as Information Champion since 2009
  - Recognized by IBM as "TOP" EMEA Consultant in 2011, 2013 and 2016
  - Co-author of 10 Redbooks related to DB2. Holder of the merit badge "Platinum IBM Redbook Author"
  - 13 books published about DB2 for z/OS and DB2 for LUW
- Reachable at
  - cmolaro@themindbridge.com
 - be.linkedin.com/in/cristianmolaro/

DISCLAIMER

- PLEASE BE AWARE THAT THE ACTUAL PROGRAMMING TECHNIQUES, ALGORITHMS AND ALL NUMERICAL PARAMETERS USED IN EXAMPLES GIVEN IN THIS PRESENTATION ARE SUBJECT TO CHANGE AT SOME FUTURE DATE EITHER BY A NEW VERSION OF DB2, A NEW RELEASE, A SMALL PROGRAMMING ENHANCEMENT (SPE) OR A PROGRAMMING TEMPORARY FIX (PTF).

- THE INFORMATION CONTAINED IN THIS PRESENTATION HAS NOT BEEN SUBMITTED TO ANY FORMAL REVIEW AND IS DISTRIBUTED ON AN "AS IS" BASIS WITHOUT ANY WARRANTY EITHER EXPRESS OR IMPLIED. THE USE OF THIS INFORMATION OR THE IMPLEMENTATION OF ANY OF THESE TECHNIQUES IS A CUSTOMER RESPONSIBILITY AND DEPENDS ON THE CUSTOMER'S ABILITY TO EVALUATE AND INTEGRATE THEM INTO THE CUSTOMER'S OPERATIONAL ENVIRONMENT. WHILE EACH ITEM MAY HAVE BEEN REVIEWED FOR ACCURACY IN A SPECIFIC SITUATION, THERE IS NO GUARANTEE THAT THE SAME OR SIMILAR RESULTS WILL BE OBTAINED ELSEWHERE. CUSTOMERS ATTEMPTING TO ADAPT THESE TECHNIQUES TO THEIR OWN ENVIRONMENTS DO SO AT THEIR OWN RISK.

- DB2 IS A TRADEMARK OF INTERNATIONAL BUSINESS MACHINE CORPORATION. THIS PRESENTATION USES MANY TERMS THAT ARE TRADEMARKS. WHEREVER WE ARE AWARE OF TRADEMARKS THE NAME HAS BEEN SPELLED IN CAPITALS.
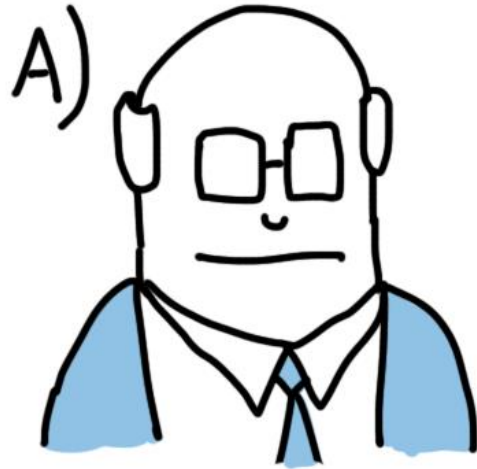
INTRODUCTION

Where are we today?

SPANISH FLU WAVES 1918–1919
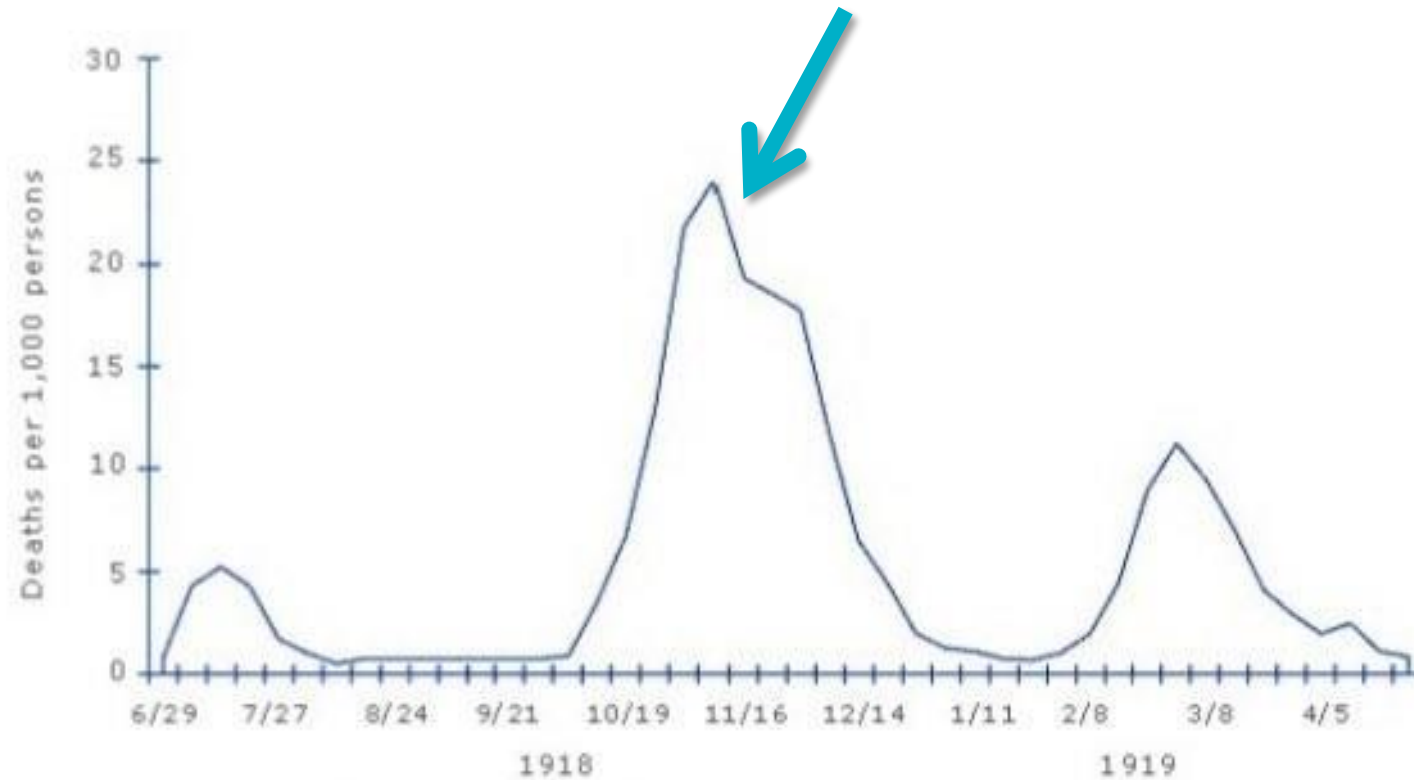
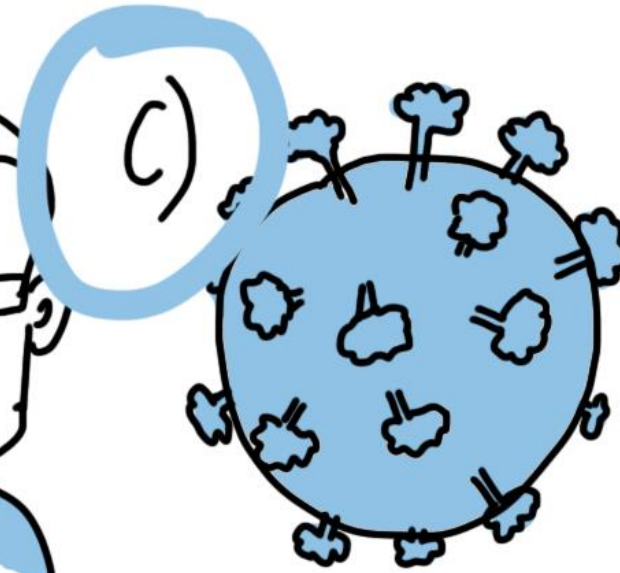Source: CDC Emerging Infectious Diseases · Vol. 12, No. 1, January 2006
Link: http://www.cdc.gov/ncidod/EID/vol12no01/05-0979.htm

INDUSTRY TRENDS

- Online survey of 2,569 enterprise decision-makers in June 2020 – Twilio
  - COVID-19 was the digital accelerant of the decade
    - <u>Accelerated</u> companies' digital communications strategy *by a global average of 6 years*
    - Greatest acceleration in digital communications: construction (8.1 years) and energy (7.2 years)
  - Previous inhibitors to innovation have been broken down
    - 77% respondents say that COVID-19 *increased their budget for digital transformation*
  - COVID-19 propelled some industries further than others
    - Tech companies 78%, energy 77%, healthcare 74%, construction 71% and retail 70%
  - Digital technologies have opened 'definite' future remote work opportunities
    - 99% agreed that digital technologies will open a future of continued remote work
  - Digital communication is the new lifeblood for business
    - 95% are seeking new ways of engaging customers

THE MIND BRIDGE

BUSINESS IMPACT

- Three fundamental business changes brought on by COVID-19
  - New customer behavior and needs
  - Unpredictable demand
  - Huge spike in working remotely
- Results on rapid migration to digital technologies in all industries and sectors
  - The speed of this change is unprecedented
- Digital will be key to thriving during the economic recovery and the next normal that will follow

WHY REMOTE ACCESS TO DB2?

Why it matters so much?

DB2 FOCUS AREAS

- Important growth of distributed transactions
- Security of distributed / remote access to Db2
- Infrastructure performance and capacity
- Workload classification and management
- Cloud
- Federated Db2 systems
- Large quantities of data
- Performance and capacity planning
- Db2 autonomics and AI
- Agile Db2

CASE STUDY: DIGITAL PAYMENTS

- *"Contact-free payments accelerated with Covid-19 crisis"* - Sunday, 11 October 2020
  - More and more people in Belgium have been opting for contact-free payments due to the novel Coronavirus (COVID-19) crisis
  - Since January, the percentage of no-contact payments has almost tripled
  - From 5% in January 2019, and 13% in January 2020, they now represent 37% of all electronic transactions
  - Between January and September, 262 million Bancontact payments were made, a 216% increase on the corresponding period of last year
  - *"Over 50% of transactions in Europe are already contact-free, and a similar rate of adoption can be expected in Belgium by the end of the year" - Worldline BE*
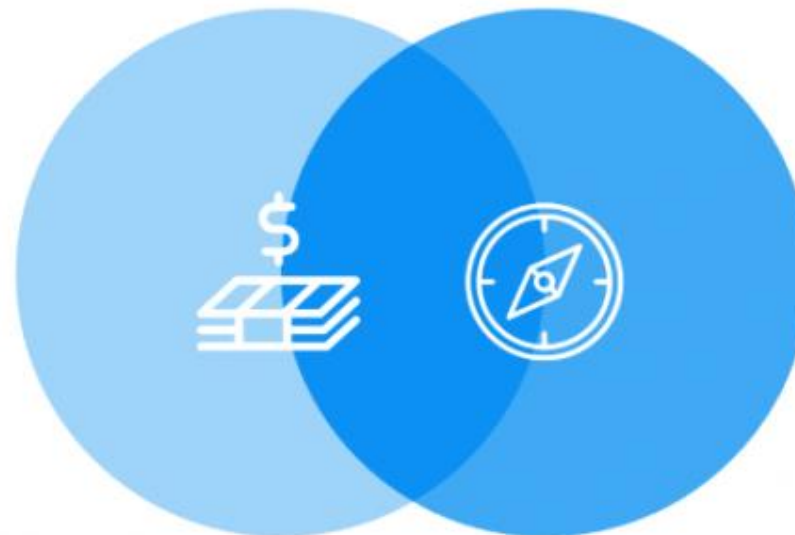
The Brussels Times

ACCELERATION OF CLOUD ADOPTION

Why Cloud Computing?

FINANCIAL BENEFITS

Cost Reductions: Pay per Use, Elasticity and IT Rationalization.

Operation Reduction and Simplification

Avoid complex IT Capacity Planning processes

BUSINESS STRATEGY

Immediate Access to IT Resources: Systems, Platforms, Applications

Quicker Implementations and Time to Value

Significant Improvement of Enterprise Agility

DB2 AND THE CLOUD

- Yes, you can
  - Db2 engine
  - Db2 applications
- Need for speed would accelerate cloud adoption
- Many solutions available
  - AWS, Azure, IBM
  - Paas, Saas, ?
  - On-premises cloud?
  - Security and complaint concerns
  - Very dynamic offering
- Re-platforming is a very hot trend
- Hybrid architectures are possible
  - I.e. Operational on premises + DWH on the cloud
  - Federation, CDC, HADR, etc
  - Performance concerns
  - Pricing not always clear

DB2 on
IBM Cloud Pak for Data

An integrated multicloud data
platform built on Red Hat OpenShift
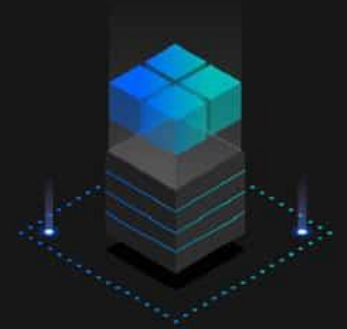
IBM Hybrid Data Management

IBM.

DB2 FEDERATION

- Access remote tables as if they were local
  - Great option for moving small quantities of data
  - Integrate z/OS, LUW, Cloud data sources
- Definition
  - All data sources are federated and linked together from heterogeneous DBMSs, different locations, relevant/irrelevant and structure/non-structure data, into a unified system
- Characteristics of federated DBMS
  - Transparency
  - Heterogeneity
  - A high degree of function
  - Extensibility
  - Openness
  - Autonomy
  - Optimized performance
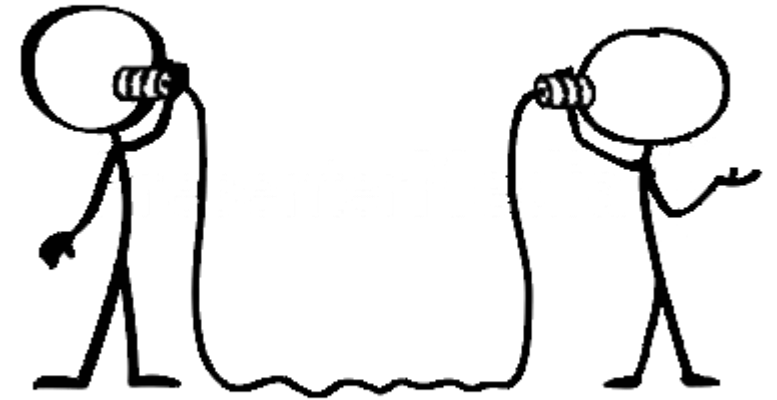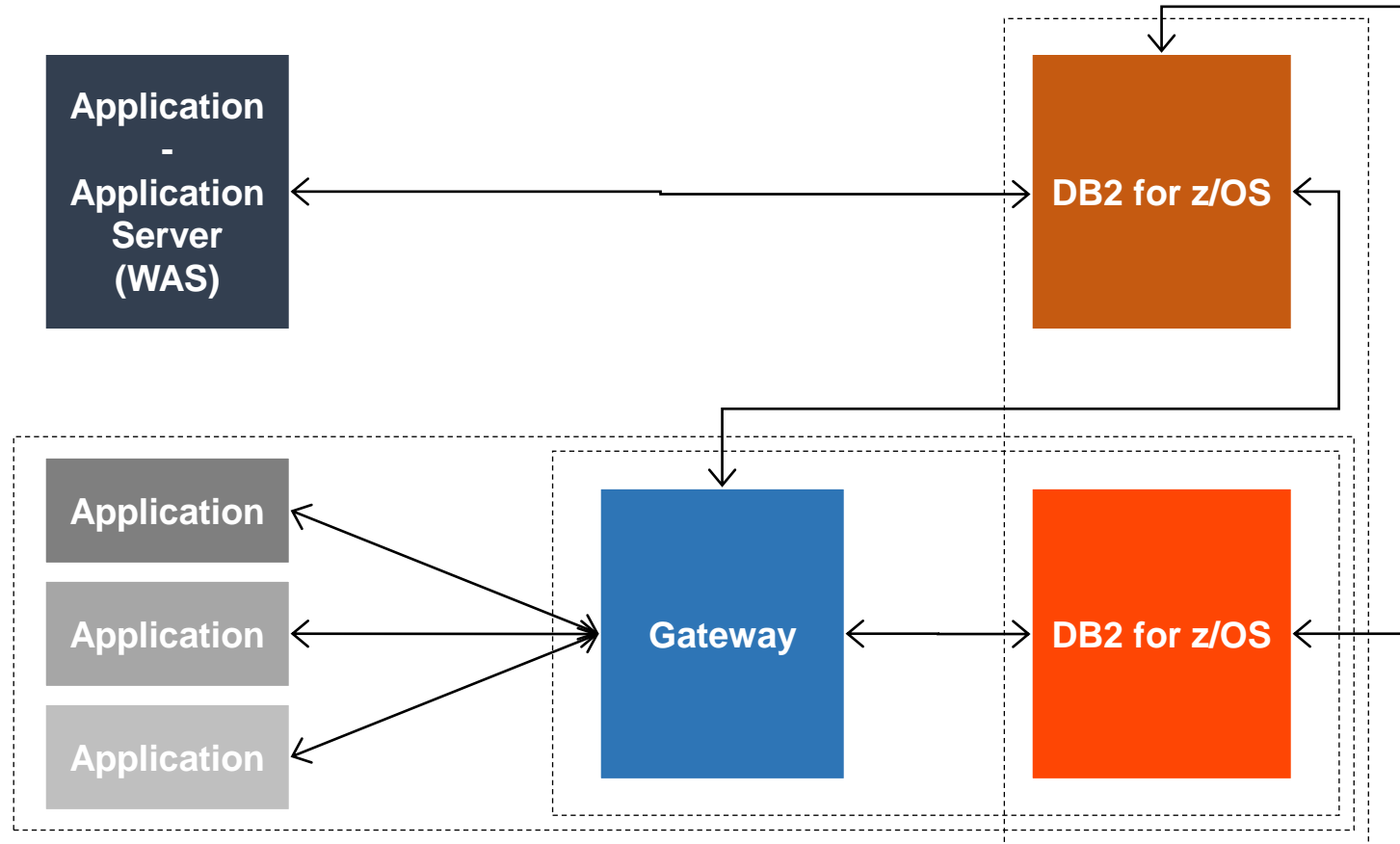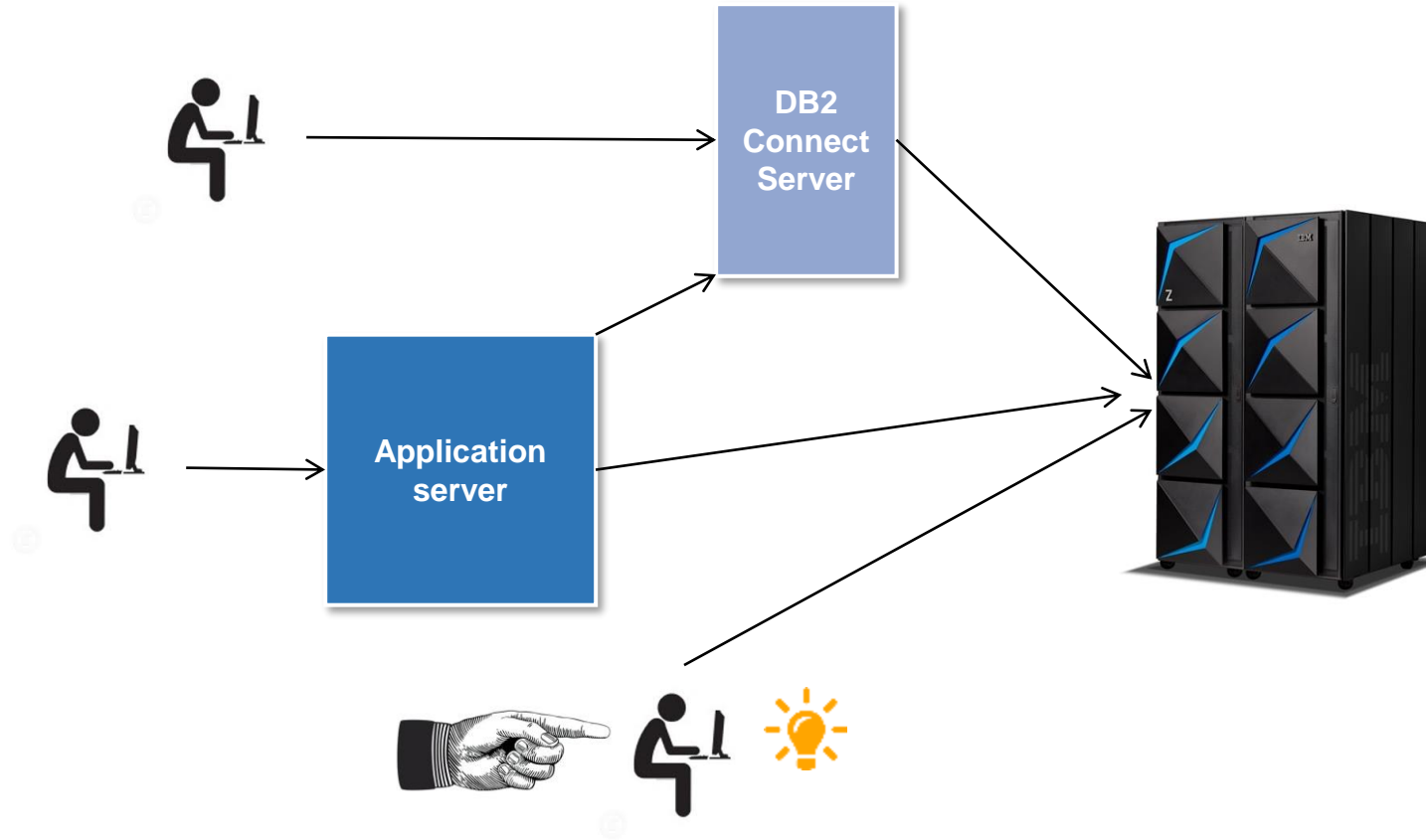
DISTRIBUTED CONFIGURATIONS

Architecture options and must know

DISTRIBUTED ACCESS TO DB2

- Increase in digital transactions results on more distributed access to Db2
- Review, understand, and optimize the distributed access to Db2

DB2 CONNECT CONFIGURATIONS

DB2 Connect Server

Application server

IMPORTANT: DB2 Connect licensing is required in all configurations

DISTRIBUTED RELATIONAL DATABASE ARCHITECTURE

- **Levels**: communication will be done using the lowest DRDA level supported by the Client / Server

- Working with down-level clients?
  - An old client will work but probably with a subset of the DRDA capabilities of the DB2 server
  - Clients and servers are supported independently

- **BUT:** feedback from IBM DDF Level 2 Support area shows:
  - Typical problem: distribution protocol with certain DDM code points
  - Special register settings not taking effect after connection reuse
  - Many (sometimes undetermined) problems solved after updating clients
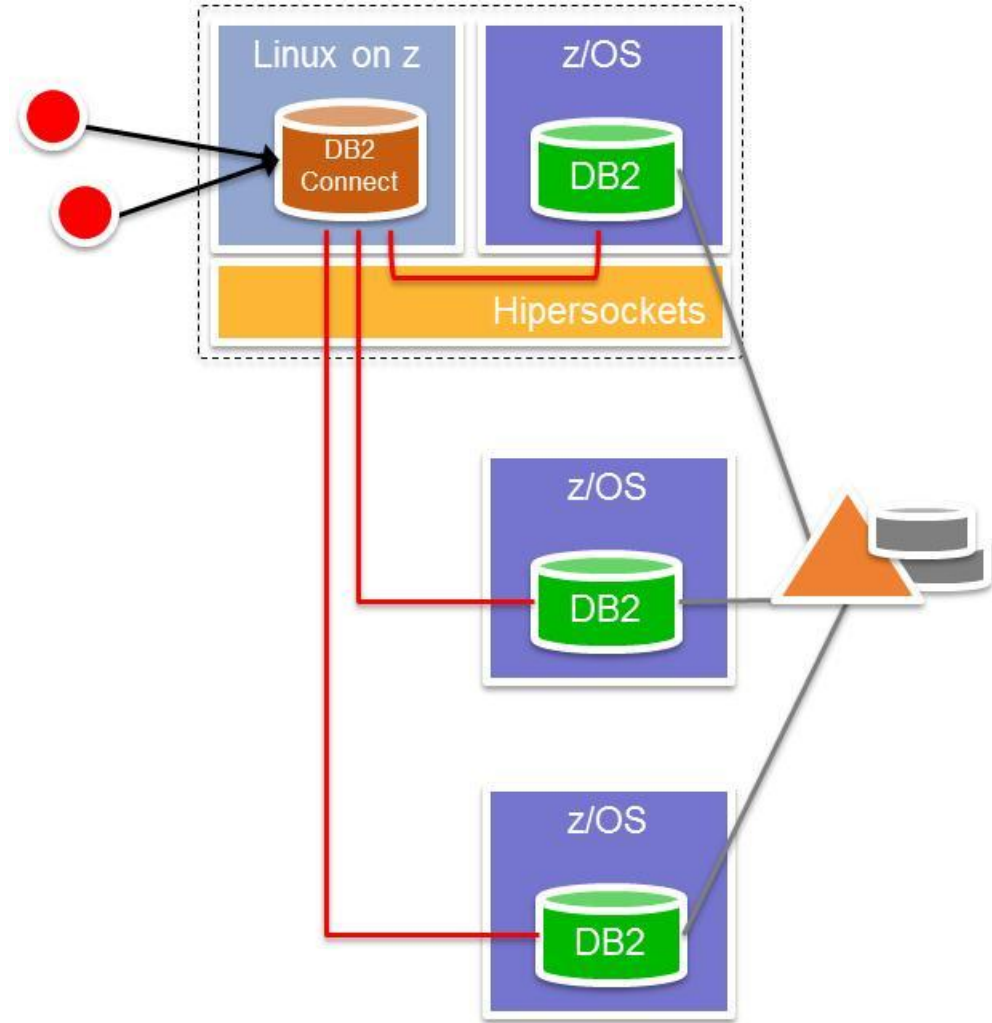
IMPORTANT: Keep clients up to date

AVOID TECHNOLOGICAL DEBT

DB2 CONNECT AND HIPERSOCKETS

- Memory-only network
  - Very good performance
- Only for enabled partitions
- Only for partitions in same CEC
- Also applies for Linux on z

LINUXONE

- Technical details at a glance:
    - Specialty engines: IFL, LPAR, Systems Assistant Processo
    - Encryption: EAL5+, ECC Digital signature, Smart Cards, C
    - I/O: FICON, FCP, zHyperLink, Open Sys Adpt, HiperSock
    - Channels: OSA-Express6S, OSA-Express7S 25 GbE SR
    - NVMe boot support
    - 16U reserved space hardware configuration flexibility
- Supported operating systems:
    - Red Hat Enterprise Linux 7.7, Red Hat Enterprise Linux 8.2, SUSE Linux Enterprise Server 12 SP5, SUSE Linux Enterprise Server 15 SP2, Ubuntu 20.04 LTS
- Supported virtualization:
    - IBM z/VM 6.4, IBM z/VM 7.1, IBM z/VM 7.2, KVM as offered with Linux

SYSPLEX SUPPORT: OVERVIEW
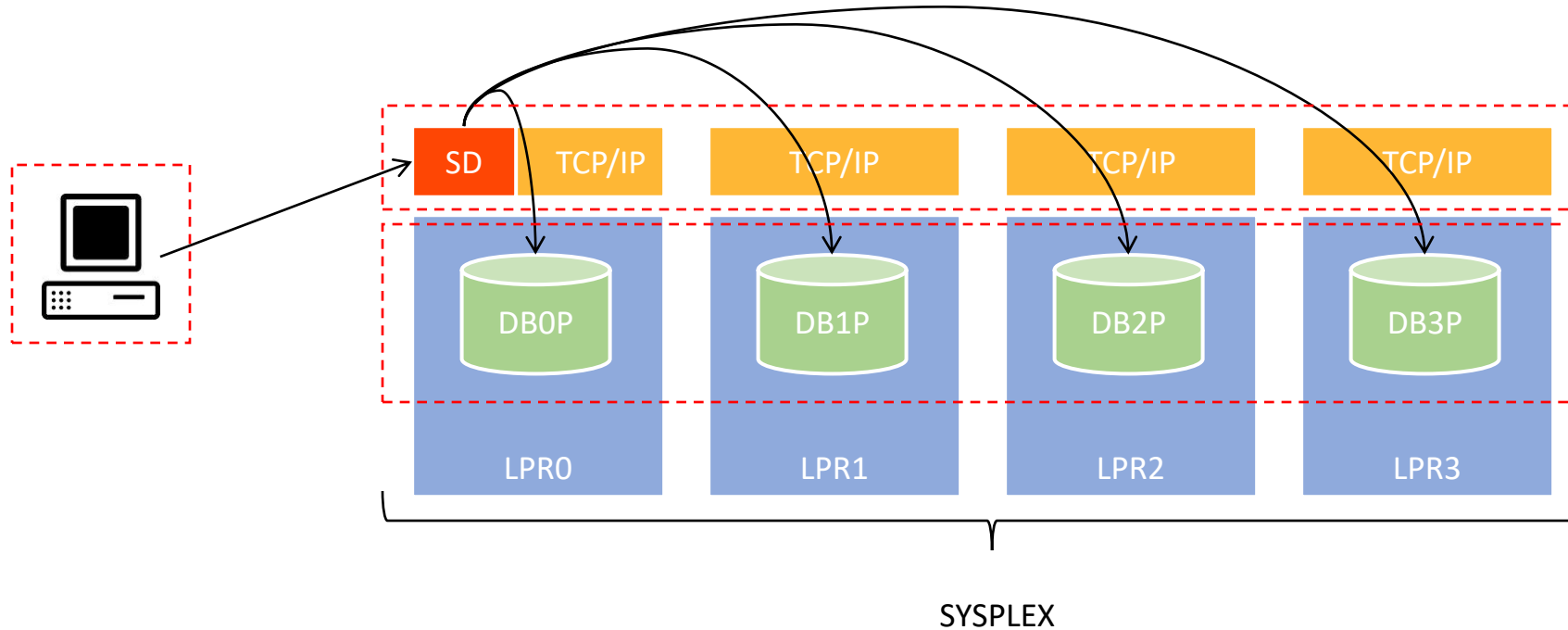
SYSPLEX

- Sysplex Support is based on:
  - TCP/IP Sysplex Distributor configured with Dynamic Virtual IP address (DVIPA) and automatic VIPA takeover
  - DB2 for z/OS Data Sharing Members
  - DB2 Sysplex WLB functions supported by DB2 Connect, Clients and Drivers

SYSPLEX SUPPORT

- **Sysplex Distributor** balances *connections*
- The **WLB** connection concentrator capability balances **transactions** across the group
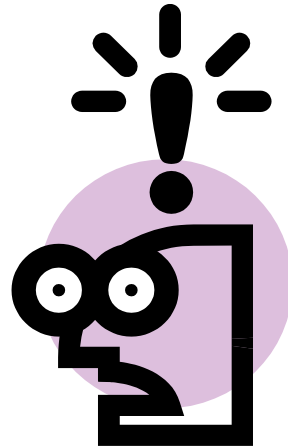
- *Is there any additional benefit in using Sysplex WLB at the application server or DB2 Connect if using DVIPA and Sysplex Distributor on z/OS?*
  - **YES!** Both need to be enabled to ensure highest availability

SECURITY

Securing access and infrastructure

DISTRIBUTED ACCESS TO DB2: SECURITY STRATEGIES

- Plan and apply strategies to improve the security of:
  - The Client
  - The Network
  - The Server

- Create a Security Plan
  - Continuous minimum monitoring and periodic auditing

- Plan and apply security best practices
  - Contextualize access with Trusted Contexts and Roles
  - Rationalize privileges, do not over GRANT

CLIENT ←——— NETWORK ———→ DB2

EFFECTIVE DB2 SECURITY IS MULTI-LAYERED

- Data servers are not protected by a security perimeter anymore
  - Application distributed access is clearly the trend
  - Remote work accessing Db2 for administration
- Apply the principle of least privilege
- Systems are built and used in layers
  - Security must be implemented in each layer
    - Physical Security
    - Network Security
    - Host Security
    - Data Security
  - Complexity increases security risks
- Db2 for z/OS: migrate Db2 security to RACF

RACF PASSTICKETS

- Cryptographically generated alternative to the RACF password
- Unlike a RACF password, the PassTicket applies to only one application
  - It is valid for ten minutes
  - Cannot be replayed, being then inherently more secure than passwords
- PassTicket generation is based on:
  - The client user Id
  - The application Id
  - A secured sign on application key known to both sides
  - A time and date stamp

TIP: Saves the need to send RACF passwords across the network

TRUSTED CONTEXTS AND ROLES: BENEFITS

- Contextualization of access rights
  - Improved control of the use of administrative authorities
- Removes the need for a user to own objects
  - You can use a ROLE as the OWNER
- Manage objects owned by other users
- Improved auditing and accountability of remote end users
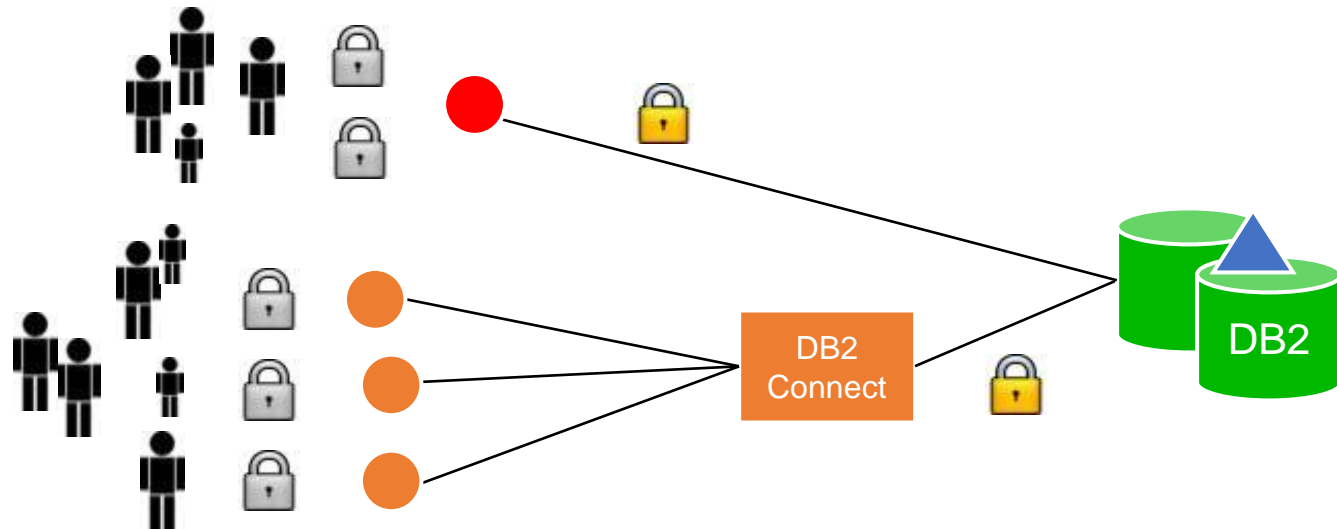
TRUSTED CONTEXTS

- Allows a unique set of privileges to be associated with an application
  - Prevents the use of privileges when not accessing through the trusted context
- It is a database entity that you create based on:
  - System authorization ID – SYSTEM AUTHID
    - DB2 primary authorization ID used to establish the trusted connection
  - Connection trust attributes
    - ADDRESS, SERVAUTH, ENCRYPTION and JOBNAME
- It can be:
  - Remote
  - Local
    - TSO, BATCH, RRSAF
    - No IMS, No CICS

ROLES

- A Role is a database entity that is created in DB2
  - It is an object that can be granted any authority or privilege
- A Role groups the privileges together so that they can be simultaneously granted to and revoked from multiple users
  - A Role **is not the same** than a Group
    - A Group is a set of users
    - A Role is a set of privileges
- A Role can be defined as the default for a Trusted Context
  - Optionally: assign a Role to a user in the Trusted Context
- A Role can provide privileges that are an addition to the current set of privileges of the user's authorization ID
- It is defined through the SQL CREATE ROLE statement
 - It is associated with an authorization ID in a Trusted Context definition

```
CREATE ROLE FINAPP_REM_DBA ;
```

BEST PRACTICES

Getting it done in the most efficient way

DISTRIBUTED ACCESS TO DB2, BEST PRACTICES

- Upgrade Db2 clients, drivers, and Db2 connect
  - Better performance and reliability
- Review and optimize Db2 Connect licenses
- End to end monitoring + performance warehouse
- Verify and update your DRDA specific parameters
- Db2 for z/OS
  - Use INACTIVE threads
  - DataSharing
    - Enable Sysplex Support (WLB + ACR) + Sysplex Distributor + DVIPAs
  - Test and implement High Performance DBATs
  - Exploit Hipersockets and ZIIPs
  - Use Db2 profile tables, System Profiling
  - Classify workload using WLB special registers + WLM

THEMIND BRIDGE
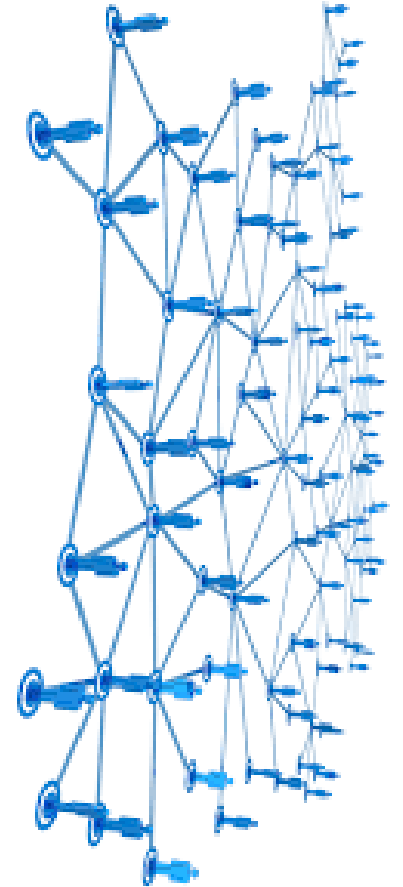
DISTRIBUTED ACCESS TO DB2, BEST PRACTICES

- Enforce Application Development Guidelines and Best Practices
  - Db2 (Native) Stored Procedures should become very popular
- Monitor network performance
- Security options
  - Enforce multilayer security strategies
  - RACF PassTickets / SSL
- Trusted Context and Roles
  - Great feature and easy to implement
  - Contextualization of access rights
  - Improved control of the use of administrative authorities
  - Manage objects owned by other users
  - Improved auditing and accountability of remote end users

THE MIND BRIDGE

USE INACTIVE THREADS

- Enable inactive thread support
  - **CMSTAT=INACTIVE**
  - Allows DB2 for z/OS pooling:
    - Reduction in CPU utilization
    - Reduction in Memory utilization

- To allow DDF threads to become **INACTIVE**
  - Avoid holding resources
    - WITH HOLD cursors not closed
    - DTT not dropped
    - Application using packages bound using KEEPDYNAMIC

IMPORTANT: Resources held across a COMMIT would prevent the connection and associated DB2 thread from being **POOLED**

DIS DDF COMMAND

```
DSNL080I  -DB2P DSNLTDDF DISPLAY DDF REPORT FOLLOWS:
DSNL081I STATUS=STARTD
DSNL082I LOCATION              LUNAME              GENERICLU
DSNL083I DB2P                  DB2P.LU1            -NONE
DSNL084I TCPPORT=5136  SECPORT=5137  RESPORT=5138  IPNAME=-NONE
DSNL085I IPADDR=::192.168.1.1
DSNL086I SQL    DOMAIN=WWW.HELLOWORLD.BE
DSNL090I DT=I   CONDBAT=    1000 MDBAT=  200
DSNL092I ADBAT=     2 QUEDBAT=       0 INADBAT=      0 CONQUED=       0
DSNL093I DSCDBAT=       0 INACONN=      0
DSNL099I DSNLTDDF DISPLAY DDF REPORT COMPLETE
***
```

- DT=I   --> DDF configured with INACTIVE threads
- CONDBAT --> MAX REMOTE CONNECTED
- MDBAT   --> MAX REMOTE ACTIVE
- ADBAT   --> Current # of DBATs, active and disconnected
- QUEDBAT --> Count # times MDBAT was reached, only reset at restart
- INADBAT --> Current # of inactive DBATs, DISPLAY THREAD TYPE(INACTIVE)
- CONQUED --> Current # of queued connections
- DSCDBAT --> Current # of disconnected DBATs= DBAT pool threads
- INACONN --> Current # of inactive connections

BENEFITS OF HP DBAT + RELEASE(DEALLOCATE)

- DB2 High Performance DBAT support reduces CPU consumption by:
  - Supporting RELEASE(DEALLOCATE)
  - Avoid repeated package allocation/de-allocation
  - Avoids acquiring and releasing parent (IS, IX) locks frequently
  - Avoids the processing necessary to go INACTIVE and then back to ACTIVE
  - More noticeable CPU reduction for short transactions

- Behavior
  - DBAT will stay associated with connection at UOW boundaries if there is at least one RELEASE(DEALLOCATE) package allocated
  - DBAT will be terminated after 200 uses
  - Normal idle thread time-out IDTHTOIN detection will be applied to these DBATs

TIP: No benefit and not support for ACTIVE threads (CMSTATS=ACTIVE)

TIP: No benefit for KEEPDYNAMIC YES

IMPLEMENT GRADUALLY OR SELECTIVELY

- BIND a new set of packages with RELEASE(DEALLOCATE)

- SYS**S**Hxyy
  - **S**: Represents a small package (65 sections)
  - **H**: Represents WITH HOLD
  - **x**: Indicates the isolation level
    - 1=UR, 2=CS, 3=RS, 4=RR
  - **yy**: The package iteration, 00 through FF

```
BIND PACKAGE(DRDADEALLOC)
         QUAL(DB2R1)
         OWNER(DB2R1)
         COPY(NULLID.SYSSH200)
         SQLERROR(NOPACKAGE)
         ISOL(CS)
         REL(D)
         CURRENTD(N)
         ACTION(REPLACE)
         KEEPDYNAMIC(N)
```

```
                                                V I V O Quali-   R E D
    S  Collection        Name     Owner    Bind Timestamp    D S A P fier    L X R
    -- ----------------- -------- -------- ---------------- - - - - --------- - - -
       DRDADEALLOC       SYSSH200 DB2R1    2011-02-25-15.01 R S Y Y DB2R1     D N R
       NULLID            SYSSH200 DB2R1    2011-02-22-20.35 R S Y Y DB2R1     C N R
    *********************************** END OF DB2 DATA ***********************************
```

WORKLOAD MANAGEMENT

Protecting the workload that matter

WLM CLIENT INFORMATION

- DB2 server systems have implemented the concepts of:
  - End user IDs
  - End user workstation names
  - End user application names
  - Accounting data

- Much of this information is externalized in various forms:
  - The **DSNV437I** message of the DISPLAY THREAD command
  - THREAD-INFO data in various messages such as **DSNT375I**
  - DB2 accounting records

```
DSNL027I  -PRD1 SERVER DISTRIBUTED AGENT WITH 778
              LUWID=C9DE5919.F7D7.C5C2D6F15029=636
              THREAD-INFO=CRIS:TotoMac:Toto:TestFromMac:*:*:*
              RECEIVED ABEND=04E
              FOR REASON=00D3003B
DSNL028I  -PRD1 C9DE5919.F7D7.C5C2D6F15029=636 779
              ACCESSING DATA FOR
                LOCATION ::10.50.1.12
                IPADDR ::10.50.1.12
```

WLM CLIENT INFORMATION

- Cannot use SQL for setting values
- Can use SQL for inquiring values:

```
SELECT
SUBSTR(CURRENT CLIENT_ACCTNG,1,15),
SUBSTR(CURRENT CLIENT_APPLNAME,1,15),
SUBSTR(CURRENT CLIENT_USERID,1,15),
SUBSTR(CURRENT CLIENT_WRKSTNNAME,1,15)
FROM SYSIBM.SYSDUMMY1;
```

- The value of these special register can be changed by using:
  - SQLE_CLIENT_INFO_USERID (sqleseti)
  - DB2Connection.setDB2ClientUser(String info)
  - The RRS DSNRLI SIGNON, AUTH SIGNON, CONTEXT SIGNON, or SET_CLIENT_ID function
  - The **WLM_SET_CLIENT_INFO** stored procedure

PROTECTING THE WORK THAT MATTERS

- WLM can help to
  - Protect critical workloads
  - Provide consistent response times
- Example:

New DDF vs. Clasiffy DDF Scenarios : CPU profiles compared
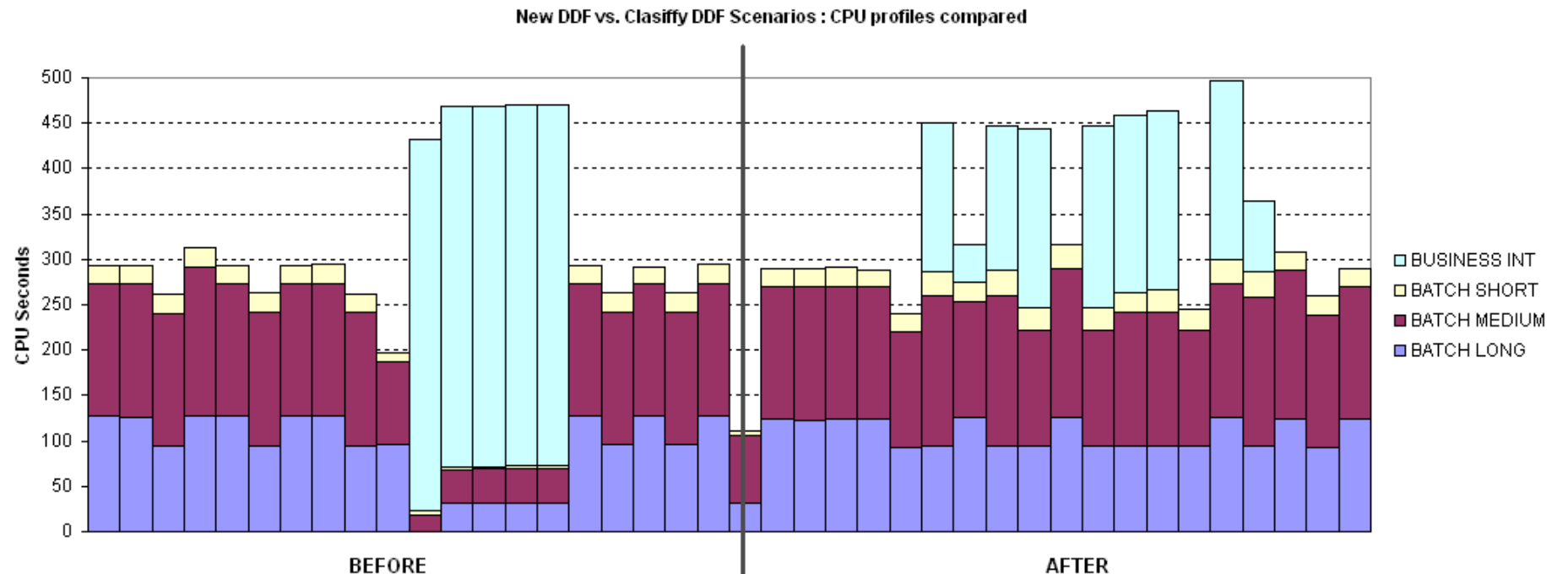
WLM WORKLOAD CLASSIFICATION
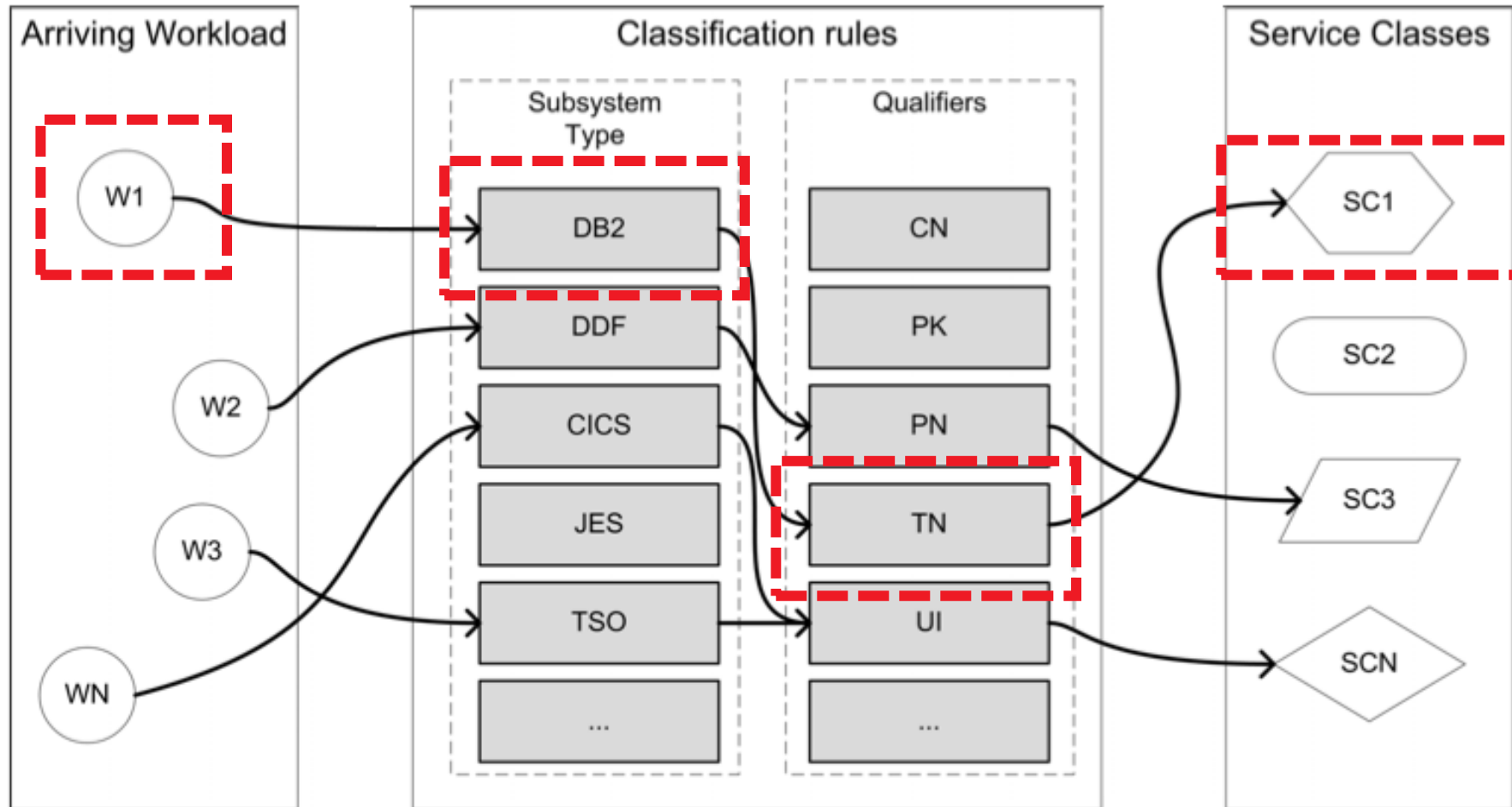
DDF AND CLASSIFICATION RULES

- Classification rules used to assign the incoming work to a
  - Service Class
  - Reporting Class (optional)
- If you do not implement classification rules for DDF
  - All DDF workload is classified and executed under the service class…

SYSOTHER

- System provided service class for all work not associated with a service class
- It is assigned a *discretionary goal*
- ***Discretionary work is run using any system resources not required to meet the goals of other work***

WORKLOAD BALANCING AND WLM

- WLM provides relative weights via a **server list**
  - Returned whenever a connection is established or reused
- DB2 calls WLM to request a weighted list of servers
  - List of servers associated with the DB2 location or alias are returned along with a relative weighting for each member
  - Server drops off list when no capacity
- WLM Weights based
  - Displaceable capacity of system where member resides
  - Performance index that indicates the achievement of the WLM-defined goals of the service classes used by the enclaves of the server
  - Queue delays waiting for a DB2 thread to process a unit-of-work is considered

THEMIND BRIDGE

SUMMARY AND CONCLUSIONS

KEY TAKEAWAYS

THERE IS MORE THAT YOU MUST KNOW!

- Automatic client reroute and workload balancing
- Stored procedures
- Autocommit implications
- Tracing distributed applications
- Application development best practices
- Security topics
- Profile tables
- Invest into Trusted contexts and Roles

THEMIND BRIDGE
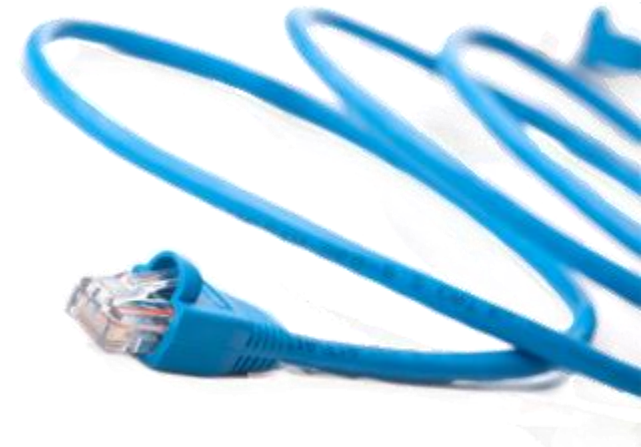
THIS WAS OUR AGENDA

- Introduction
- Why remote access to db2?
- Distributed configurations
- Security
- Best practices
- Workload management
- Summary and conclusions

THE MIND BRIDGE

KEY MESSAGES

- The pandemic is accelerating the digital transformation
  - This is a non-reversible change
  - Do not fail to adapt
- Focus on the Db2 areas that enable unpredictable, high volume, transactions
  - Best performance for distributed access
  - Best security
  - Best performance and scalability
- Focus on the human factor, and keep healthy!

THANKS!

Cristian Molaro
The Mindbridge
cmolaro@themindbridge.com

THE**MIND**BRIDGE