
IDUG
Leading the DB2 User Community since 1988
IDUG Db2 Tech Conference NA
Philadelphia, PA | April 29 - May 3, 2018
#IDUGDb2
Db2 in the Cloud – A Perfect Match!
Philip Gunning
Gunning Technology Solutions, LLC
Session code: C02
2:00 – 3:00 PM. April 30, 2018
Db2 LUW
1

Agenda

- Db2 inherently cloud-capable architecture
- Standards and Regulations compliance
- Built-in Multi-tenacy
- DB2 Architecture is cloud friendly
- Multiple Editions
- Bare-metal or Virtulization
- High level architecture overview

Phil Gunning is an author or three books on Db2 LUW and has been providing consulting services for Db2 for 28 years, the last 15 as the principal of Gunning Technology Solutions, LLC. Phil was the former list owner and admin of the DB2-L listserver and is a member of the DB2-L Hall of Fame. Phil has presented for the last 20 years at IDUG North America, Db2 Tech Conference, IDUG EMEA and Db2 user groups in North America. He is a member and regular sponsor of the Central Pa Db2 User Group. Phil provides Db2 consulting in the areas of performanc and tuning, SQL tuning, HADR, TSAMP and upgrades and migrations. He has re-platformed many applications to Db2 LUW with high success. He consults with FORTUNE 100 companies and mid-range and small enterprises throughout the world. His current clients include an entertainment company which has outsourced all Db2 support to him and the seventh largest school district in the US. He is regularly sought out by companies with Db2 LUW for consultations and advice.

Agenda

- Db2's architecture makes it a Perfect Match "Built-in multi-tenancy"
- Multiple schemas
- Support for many virtualization techniques
- Workload Management per distinct application workload with priorities assigned
- Multi-temperature storage
  - Separation of client data

As we progress through the presentation you will see how DB2 is architected for rapid implementation and perfectly capable of multi-tenancy.

Agenda

- Data and Network Encryption
- Scalability within and between Db2 Editions
- Multiple DB2 copies

Standards and Regulations

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- NIST
- FIPS
- Federal Privacy Act
- Graham-Leach-Bliley Act (GLBA)
- Data Protection Act (DPA) in UK

When considering moving to the Cloud companies need to perform their due diligence and consider all the regulations and standards that govern their line of business and ensure that the Cloud provider can meet their requirements.

Standards and Regulations

- Health Information Technology for Economic and Clinical Health Act (HITECH)
- International Standards Organization (ISO)
- Import/Export Controls
- Trans-border data flow
- Data Breaches
- Privacy

Standards and Regulations

- Public Key Cryptography Standard #11 (PKCS#11) – DB2 11.1 Secure Local Key management with Native Encryption
- Advanced Encryption Standard
- EU General Data Protection Regulation (GDPR)*
- Cloud Security Alliance
- Clouds Standards Customer Council (ISO)

The GDPR goes into effect May 25, 2018. The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

DB2 11.1 Regulatory and Standards Compliance

- Federal Information Processing Standards (FIPS)
  - Publicly announced US Government standards
  - ANSI
  - IEEE
  - ISO
- PCI DSS
- NIST
- AES
- TLS

Db2 Instance

- Think of a Db2 instance as being at the highest level
- It can be stopped and started
- Each instance has an instance owner with associated privileges
- It can house single or multiple databases

Although many of you may be quite familiar with DB2 instances we will go over the Db2 structures and focus in on what enables them to inherently provide and support multi-tenancy. Multi-tenancy is a "sweet spot" that enables cloud providers to make maximum use of hardware and software resources while providing users with separation of their data from others. We will see how this can be done with schemas, tablespaces, storage groups, buffer pools, workload management and RCAC where even the same table can be shared across tenants.

Db2 Database

- Resides in an single instance
- Consists of bufferpools, tablespaces, tables, logs, application objects, shared memory areas
- Consists of default tablespaces
- Database can be made highly available via HADR

Db2 Tablespace

- Contains table or multiple table data
- Storage assigned via STOGROUP and STORAGE PATHS
- Extentsize and Prefetchsize defined or can use automatic
- Index and Data
- Assigned to same or different bufferpools
- Can be backed up individually
- Can be used to restore and rebuild a database

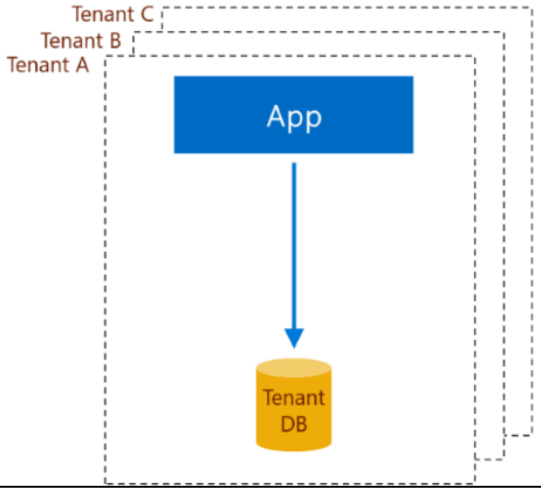
Db2 Multi-tenancy

- Single tenant single instance
- Multiple tenants each with own Db2 instance
- Multiple tenants sharing Db2 instance
  - Single database
  - Multiple schemas
  - Dedicated tablespaces
  - Dedicated bufferpools
  - Dedicated storage
- Workload Management

Typically on premises DB2 is installed using a single instance or maybe a few instances on the same server but most common is single instance single server and even single schema. However, with the shortage of DBA skills and IT skills in general we are seeing more examples of multiple databases per instance and multiple schemas per database. And the best thing is that the way DB2 was designed, handles this very well.

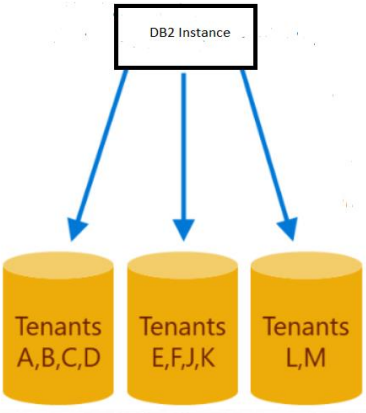
Db2 Single Tenant

- Db2 architecture uniquely positioned to support single or multi-tenancy



In the single tenant application, each tenet has their own Db2 instance and database. They could run multiple different applications against the same database. There can be one schema or multiple schemas. Of course, each tenant or instance has their own code and database and there are no dependencies between tenants or instances.

Db2 Multi-tenant



With Db2 multi-tenancy, there are many combinations of Db2 objects that can be used in multi-tenancy. Is this example we have one Db2 instance with multiple tenet databases. Similarly, we could have one Db2 instance and one database with multiple tenant schemas. This would be the ultimate in multi-tenancy! Each tenant could have their own tablespaces, buffer pools, and storage space. Many other areas have to be considered when deciding on a multi-tenant cloud solution.

Db2 in Cloud Multi-tenant Considerations

- Scalability
- Number of tenants
- Aggregate storage
- Disaster Recovery
- Regulatory Requirements
- Security – cyber and physical security
- Workload
- Tenant Isolation

Db2 in Cloud Multi-tenant Considerations

- Per tenant costs
- Recoverabilty
- Backup considerations
- Performance monitoring
- Database Security
- VPN
- TSL
- Schema Management

Db2 in Cloud Multi-tenant Considerations

- Per tenant costs
- Workload management
- Litigation
- Customizations

Db2 Supports Strong Cyber Security

- TSL/SSL for secure communication between clients and DB2 Servers
- Key Management Interoperabiltiy Protocol (KMIP) Ver 1.1 or higher
- PKCS #11 compliant key store
- Data Encryption of data at rest through DB2 Native Encryption
  - Included with all editions of DB2
- Row and Column Access Control (RCAC)
- Label-based Access Control (for Defense and Intelligence companies)
- Data Security controlled by a Security Administrator
- Logon Proc

Transport Layer Security (Formerly SSL)

- Complies with IETF
- Implement and Control with IBM Global Security Kit
- DBM DBCOMM registry variable
- Configuration File
- Support for applications via the Db2 JDBC Driver
- As of DB2 11.1.3.3 support for TLS encryption of HADR logs (non-pureScale)

DB2 Native Encryption Overview

- DB2 Native Encryption provided in DB2 10.5 FP5
  - Available to all Editions of DB2
- Supports DPF and pureScale
- Requires no hardware, software, application or schema changes
- Not enabled by **DEFAULT**
- Provides transparent and secure key management
- For many database implementations, encryption is now mandatory for compliance with many government regulations and industry standards
- Two-tier model for key management (Envelope Encryption)

DB2 Native Encryption Overview

- DB2 Native Encryption is **transparent** to **applications** and **database schemas**
- DB2 uses symmetric encryption for encrypting the database and backups
- Both Advanced Encryption Standard (AES) and 3DES are supported
  - AES with 256 bit key length is the default
- Can be seen via DB CFG parameter -- Encryption Options for Backup (ENCROPTS) = CIPHER=AES:MODE=CBC:KEY LENGTH=256

DB2 Native Encryption Overview

- **DB2 Native Encryption is implemented by the DB2 Kernel which encrypts the data before calling the underlying file system to write the data to disk**
  - **Via encryption algorithm and encryption key**
- Current data is protected, any new tablespaces or any that are added in the future
- DB2 Native encryption exploits processer technology improvements
  - Intel AES-NI
  - Automatically detected and exploited
  - POWER8 Hardware Assisted Encryption

NOTES:

Db2 High Availability

- Db2 High Availability Disaster Recovery (HADR)
- Provided with all editions of Db2 except DB2 Express-C
- Easy to configure and setup
- Db2 provided built-in monitoring
- Compatible with TSAMP and Microsoft Cluster Services
  - Other clustering software
- Standby server or multiple standby servers

Db2 High Availability

- IBM Tivoli Systems Automation for Multiplatforms (TSAMP)
  - Provided with all editions of DB2 except DB2 Express-C
- Clustering
- Failover
  - Can be used for clustering and automatic failure detection and takeover/failover

TSAMP comes with most editions of DB2 except as noted. For IBM Db2 on Cloud Managed Database as a Service, Compose Governor is used instead. TSAMP provides automated failover using a floating or virtual IP address.

Db2 HADR Overview

- Standby Database
- Multiple Standby databases
  - Principal Standby
  - Auxiliary Standby
- Co-location
- Multiple locations
- DR location in Cloud or private via LAN/WAN
- WAN for georgraphical dispersal

HADR is available for use in private clouds, IBM Cloud or on premises.

DB2 HADR Disaster Recovery

- Cross-cloud (data center) Disaster Recovery

Compose Governor for HA

- HA software developed in conjunction with Compose(an IBM company) (IBM Managed Database as a Service offering)
- Prevents split brain
- Tiebreaker node

DB2 Workload Manager

- Not available with Express-C and can be purchased as part of IBM Db2 Performance Management Offering for WSE, ESE, and Direct Standard, included with other editions
- Priortize and isolate different workloads
- Service classes and thresholds
- Separate application tenants into distinct workload classes and CPU usage
- Workload Balancing

The SYSDEFAULTWORKLOAD user workload and the SYSDEFAULTUSERCLASS are created by default for each database. These can be used to investigate the workload management features without having to create any user-defined workloads or service classes. All work is associated with these if no user defined workloads and service classes are created.

DB2 Workload Manager

- Work Identification
  - Connection, transaction level using session attributes
  - Application name
  - Authorization Id that submitted the work
- Work Class
  - Identify workload of interest
  - Insert, Update, Delete statements, etc
- Data tags for Storage Groups and Table spaces
- Monitoring and Intervention

DB2 Workload Manager

- Prevent work from running
  - Timerons
- Lower priority of work running
- Cancel work
- Track and collect data for work activities
- Identification of long running queries
- Input to Design Advisor and Data Studio
- Detailed historical analysis and reporting

DB2 Workload Manager also integrates with Operating System workload managers on AIX and LINUX. This is done by mapping a Db2service class to an Operating System Workload Manager class on the CREATE or ALTER SERVICE CLASS statement. I see the ability to discretely manage workloads as a key enabler to DB2 in cloud and multi-tenancy. For those used to this robust capability on Db2 for z/OS, you will find that this Db2 offering brings many of those capabilities to the distributed environment. The capability could be a differentiator in selecting a cloud offering or service.

Multi-Temperature Storage

- Create separate Storage Groups per entity (customer) and map those Storage Groups to separate file systems and disk to separate client data on disk
- Can be used to control temperature of client access (fast versus standard versus slow) based on SLA or other considerations
- Enhances multi-tenancy
- Use ALTER Tablespace using STOGROUP to adjust storage isolation as needed

Moving to the Cloud

- Due diligence
  - Basic services
  - Determine your CPU, RAM, DISK capacity and requirements
  - Cloud provider reputation and track record
  - Compliance with regulatory and legal requirements
  - Security compliance (cyber and physical)
    - Security Controls
- High Availabiltiy
- Disaster Recovery
- Service level agreement

Db2 Premise to Cloud Movement

- Db2look
- Db2 export/import
- Db2 load
- Db2 Federation
- MQ
- IBM Lift CLI
  - Uses high speed Aspera Technology

33

Aspera is a very fast data transport software that is up to 100x faster than FTP and HTTP. High speed transfer of large amounts of data is imperative when moving to the Cloud.

Data Movement – Network Considerations

- Basic mechanism for small amounts of data is TCP/IP
- Amount of data is limited by TCP/IP inherent flow rate control mechanism
- Makes use of TCP/IP for large amounts of data difficult or unworkable
- Workarounds
  - Bulk data transer
  - Aspera
  - Mass storage devices used to move data to and send to cloud site

Support for Myriad Data Access Types

- SQL
- JSON
  - Storage and manipulation
- Rest
  - OData standards based access to data
- pureXML
  - Storage and manipulation of XML documents
- SQL Procedural Language (SQL PL)
- PL/SQL for enabling existing PL/SQL applications to with with Db2
- RDF Graph Store
  - Native support for graph triples

Db2 on Premises

- DB2 Software Installed
- Typical install type for most organizations
- You install and manage on your hardware on your premises

You may have heard of Db2 installs as being on premises or on the Cloud. There can be a lot of confusion with the various Db2 installs nowadays. Think of Db2 on premises as how you would typically have Db2 installed in the past. On your premises and on your hardware. This includes all editions available. For information on the Db2 editions available always refer to the product announcement letters.

IBM Db2 on Cloud Offerings

- DB2 Hosted (not fully managed by IBM)
  - Virtual environment
  - Managed by user
  - Database as a Service (DBaaS)
  - Either DB2 Workgroup Server Edition or DB2 Advanced Enterprise Server Edition
  - Control
- DB2 on Cloud – (fully IBM managed services)
  - Managed Database as a Service
  - Adminsistered mainly via BlueMix Web Console
  - Simplicity

The purpose of this slide is to only make you aware of the Db2 Cloud offerings. For details concerning current offerings and descriptions refer to your IBM representative. Db2 hosted offers a virtual environment administered by the user. The use maintains CONTROL of the environment and data.

IBM Db2 on Cloud Offerings

- Db2 Warehouse on Cloud – IBM‘s Data Warehousing and analytics solution in the cloud
- Flex Plans for Db2 Hosted, on Cloud and Data Warehousing
  - Scale CPU and Storage
    - Sliderbar
- Flex on virtual environment
- Precise Performance Plan
  - Bare Metal

DB2 on Cloud Lite!

- Totally free*
- Great for development and evaluation
- Shared multitenant system
- 100MB of storage
- 5 simultaneous connections
- Extend service every 30 days via email
  - This helps provide free resources for all

*as per IBM Cloud pricing, https://www.ibm.com/cloud/db2-on-cloud/pricing.

Keeping Encrypted Data Encrypted during Movement

- Unloaded data from DB2 Native Encrypted database becomes unencrypted
- Once it leaves the server unloaded from it is no longer considered secure
- Person doing the move must be only one with access to the unecrypted data

Keeping Encrypted Data Encrypted during Movement

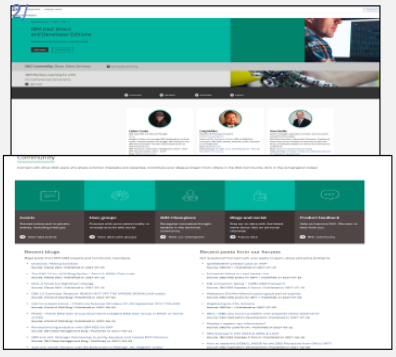
- One workaround is to establish a secure connection between on-premise database server and cloud server using TSL and then use EXPORT/IMPORT/INGEST
- Other disk encryption technologies
- Secure File Transfer

References

The Db2 Developer Community

Db2 samples, expertise and community access for deep collaboration

https://developer.ibm.com/data/db

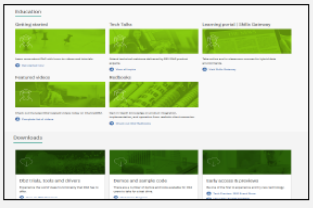


Launched in June 2017

Enhancements ongoing

- Add Db2 Tech Day recordings
- Integrate and aggregate forums and dW Answers
- Dynamic content posted from blogs forums social media.
- Links to training, download and sample code included

Db2 community links from dW communities, product pages



Db2 in the Cloud -- References

- http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf
- https://www.idug.org/p/bl/ar/blogaid=701
- https://www.ibm.com/support/knowledgecenter/en/SS6NHC/com.ibm.swg.im.dashdb.doc/learn_how/loaddata_overview.html
- Move to cloud sample script: https://www.ibm.com/support/knowledgecenter/SS6NHC/com.ibm.swg.im.dashdb.doc/learn_how/loaddata_movetocloud.html

Db2 in the Cloud -- References

- Aspera: http://asperasoft.com/technology/transport/fasp/
- Db2 on Cloud Overview https://tinyurl.com/y7aytye5
- https://www.ibm.com/cloud/bluemix
- DB2 on Cloud Announcement Letter: https://www-01.ibm.com/common/ssi/rep_ca/5/897/ENUS218-145/ENUS218-145.PDF
- DB2 Developer Works: https://www.ibm.com/developerworks/data/library/techarticle/dm-1201dbdesigncloud/

Db2 in the Cloud -- References

- DB2 Functionality by Edition: https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.licensing.doc/doc/r0053238.html
- DB2 Tech Talk, DB2 on #Cloud: https://t.co/OE288Kye4n

Thank You!

IDUG
Leading the DB2 User Community since 1988

IDUG Db2 Tech Conference NA
Philadelphia, PA | April 29 - May 3, 2018

#IDUGDb2

Philip K. Gunning
Gunning Technology Solutions, LLC
topgun@gts1consulting.com

Session code: C02

Please fill out your session evaluation before leaving!