Hewlett Packard Enterprise

NonStop Technical Boot Camp 2023 TBC23-TB53 Enable Zero Trust Security with NonStop SQL

Roland Lemoine, Product Manager

September 2023

Forward-looking statements

This is a rolling (up to three year) Roadmap and is subject to change without notice

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard Enterprise's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett Packard Enterprise may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.

Agenda

- CIA, a security model for data security
- Top 10 security features for Nonstop SQL
- Implementing zero trust security
- Futures
- Conclusion

CIA, a security model for data security

Confidentiality	Integrity	Availability
Access control Privacy of data	Prevent and detect alteration of data	Protection of components providing access to data
Authentication and authorization	Encryption and auditing	Fault-tolerance and disaster recovery

Security threat modeling

- Examples of threats classified using the STRIDE model
- Data threats encompass more than protecting the database

Threat example	Class	Possible counter measure
Password attack of privileged user	E	Disabling privileged account and let regular user achieve daily tasks
Hacked DBA account	R	Implement auditing, disable account when user leaves
SQL Injection	S,T,I	Typically enforced at the application. Specific DB features can help
Denial of Service attacks	D	DB not in DMZ, firewall rules, limit resource usage at 80%,
Backdoor (default passwords)	S	Change default passwords at installation
physical access attacks	S,T,I,E	Disk encryption, tape encryption, locked server rooms, CCTV,...
Eavesdropping	S,I	Data in transit encryption
Privilege escalation using OS vulnerability	E	Principle of least privileges, role-based access, patch OS vulnerabilities

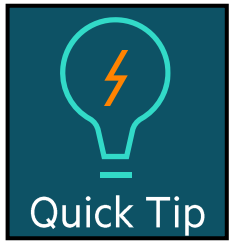
Threat classes
Spoofing
Tampering
Repudiation
Information disclosure
Denial of Service
Elevation of Privilege

Top 10 security features for Nonstop SQL

No need for a super powered DBA

C Access Control

- Don't use "SUPER.SUPER", use regular users as DBAs
  - The catalog or database owner is implicitly granted the ability to create and delete schemas
  - The schema owner is implicitly granted the ability to create and delete objects
  - Even if super.super is used, ownership stays with the existing owner
  - Catalog and schema ownership can be transferred
- Use Security Admin for security administration
- Use MXCS operator role for network security administration
- Use Tenant.admin for DBS tenant administration
- As last resort, use "sudo" rather than SUPER.SUPER
  (See securing SQL/MX in OSS)



You can freeze the SUPER.SUPER user in Safeguard to make sure it is not used (See security hardening guide).

SQL/MX built-in

Benefit examples

Avoid access to unnecessary privileges to reduce the attack surface in case of a DBA activity being hacked

NonStop SQL does not have a specific super powered user such as "sa" in SQL server or SYSDBA in Oracle, a primary target for hackers, so the only effort is to make sure to not use SUPER.SUPER for DBA tasks.

ANSI Grant/Revoke security

C | Access Control

- Provides ANSI standard ACL (Access Control List) capability to NonStop SQL
  - You can grant/revoke access to objects to specific users
  - You can grant/revoke access to objects to privileges groups
  - You can grant/revoke permission to grant
  - Access may apply to SQL objects such as tables, views, … and include schemas
- Showddl, MXDM or SQLXPress can be used to review default and custom privileges

SQL/MX

Benefit examples

ACL based security allows to better apply the principle of least privilege where users are given permissions only for the tasks they are expected to carry and nothing more

Privilege groups

- Defines a named group including a set of privileges to be shared by members of the group
- This helps significantly on addressing scalability of implementing ACLs
- Similar to roles in allowing to decouple users from being assigned low level object permissions
- Instead, the security administrator only manages a small set of privilege groups
- New users or departing users can just join or depart the privilege group
- It is a first step towards Role-Based Access Control

SQL/MX 3.5 & later

Benefit examples

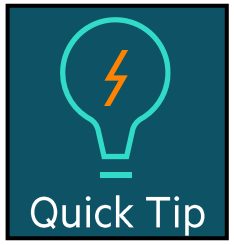
Most common and primary RBAC benefit

Combines benefits of ANSI Grant/Revoke ACLs with named functions in the enterprise

Secure SQL/MX in OSS

C	Access Control	I	Prevent data tampering

- Secure SQL/MX programs in OSS
- Secure user modules
- Turn on Safeguard OSS auditing
- Use OSS ACLs for SQL programs such as mxci
- If you absolutely must use SUPER.SUPER in OSS, you may use sudo instead but:
  - Don't use a default configuration without enforcing any ACLs
    - Commonly seen: *root ALL=(ALL) ALL*
    - Which basically gives you same powers as SUPER.SUPER
  - Leverage sudo security features
    - Use sudo RBAC features
    - Auditing of commands is built-in with sudo AND on NonStop the events are automatically forwarded to EMS and XMA



See list of manuals for each task at the end of this presentation

SQL/MX built-in

Benefit examples

Prevent elevation of privileges

Detect suspicious patterns

Reduce situations requiring to communicate the SUPER.SUPER password

Data at rest encryption

I Prevent data tampering

- Data at rest includes disk and tape encryption
- For disk: NonStop Volume Level Encryption (NS VLE)
- For tape: BackBox VTC and/or NonStop SecurTape
- BackBox VTC (Virtual Tape Controller)
  - Requires to purchase NonStop VLE and Utimaco ESKM
  - But also supports externally provided encryption (SecurTape or physical encryption)
  - In the case of SecurTape no external ESKM is required
- BackBox further leverages the QoreStor technology adding support for cloud-based storage options as well as optimized and integrated use of compression, deduplication and encryption at once
- **New with SQL/MX 3.8.2**
  - **Application level encryption (DBMS_CRYPTO package)**

Combination of NS VLE, BackBox VTC, NS SecurTape and ESKM

Benefit examples

Prevent data access via physical attack

Use RBAC for DBA activities

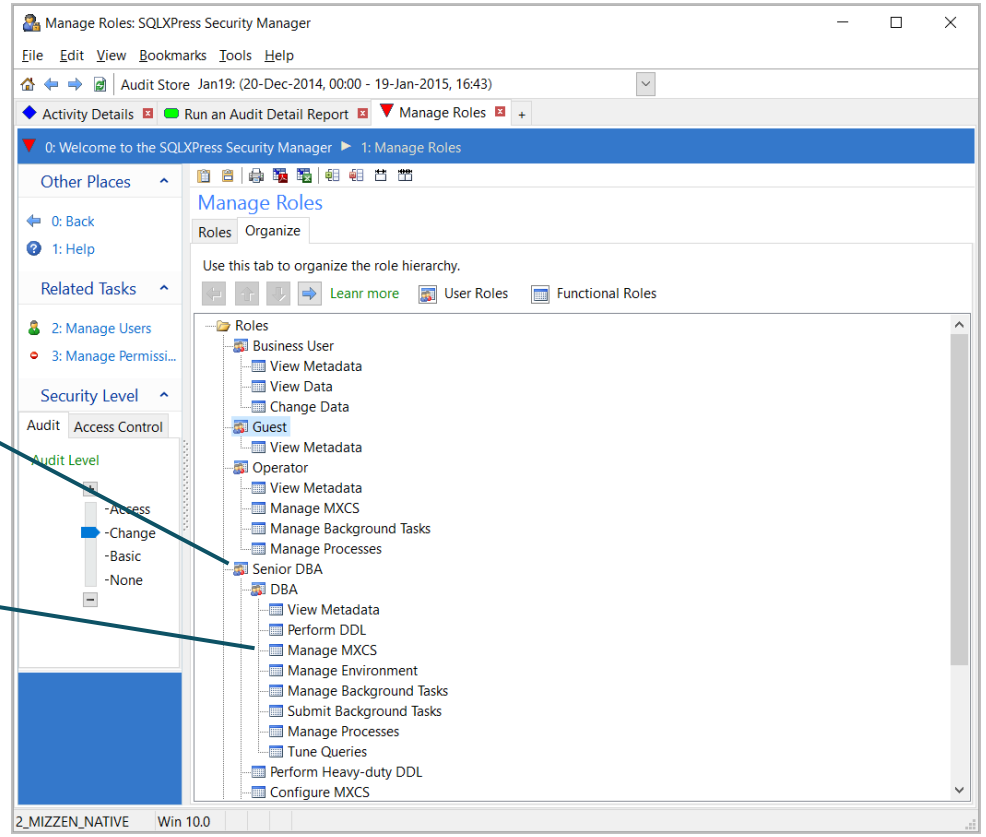
C | Access Control

- SQLXPress includes an extensive role-based access control implementation
- Includes roles hierarchy
- Includes concepts of user roles and function roles

SQLXPress 3.7 & later

User role
"Senior DBA"

Function role
"Manage MXCS"



Benefit examples

Fine grained roles and functions to prevent elevation of privilege
Easier security management than raw ACLs

Demo

Multi-factor authentication

C Access Control

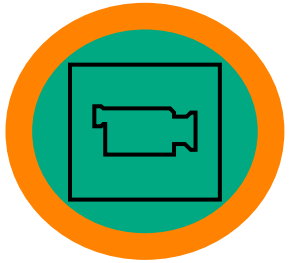
- SQLXPress is the most comprehensive GUI based administration solution for SQL/MX (as well as SQL/MP) and comes with MFA capability
- No configuration required for SQLXPress:
  - SQLXPress detects if XUA is setup for MFA
  - If enabled SQLXPress will use MFA
- MFA setup in XUA
  - Requires RSA SecurID or Radius Authentication server
  - In a UAGROUP element define the types of authentication required by a given user (other criteria available)
  - NonStop user IDs are mapped to external user IDs (i.e. RSA SecurID ID)

SQLXPress 3.7 & later

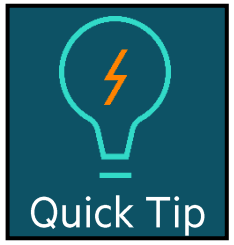
Benefit examples

Prevents brute force password attack

Prevents elevation of privilege



Demo



Access to mxci in OSS can also be protected using MFA. This can be enforced at the user level when using SSH with the attribute REQUIRED-AUTHENTICATIONS

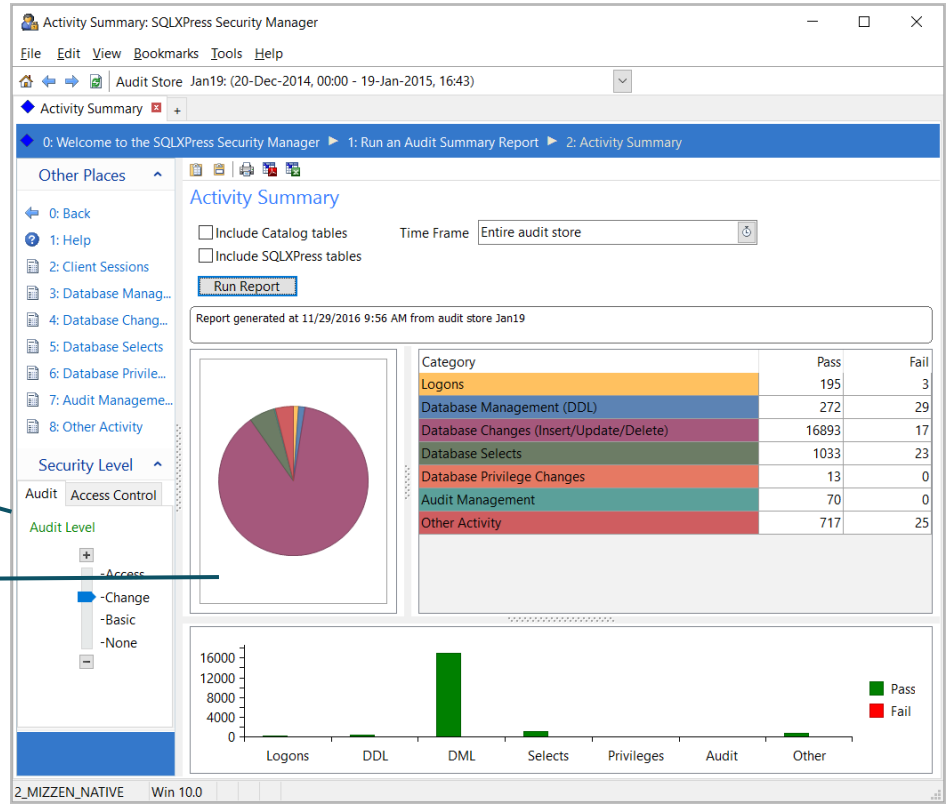
Enable auditing of DBA activities

I Prevent data tampering

- Audit activity of SQLXPress users
- Audits logons, SQL statements, scripts
- Includes audit levels
- Include audit reports

Set audit level

Get instant report



Quick Tip

With SQL/MX 3.8 we introduce a new DDL auditing feature native to SQL/MX that can be leveraged by 3rd party tools

SQLXPress 3.7 & later

Benefit examples

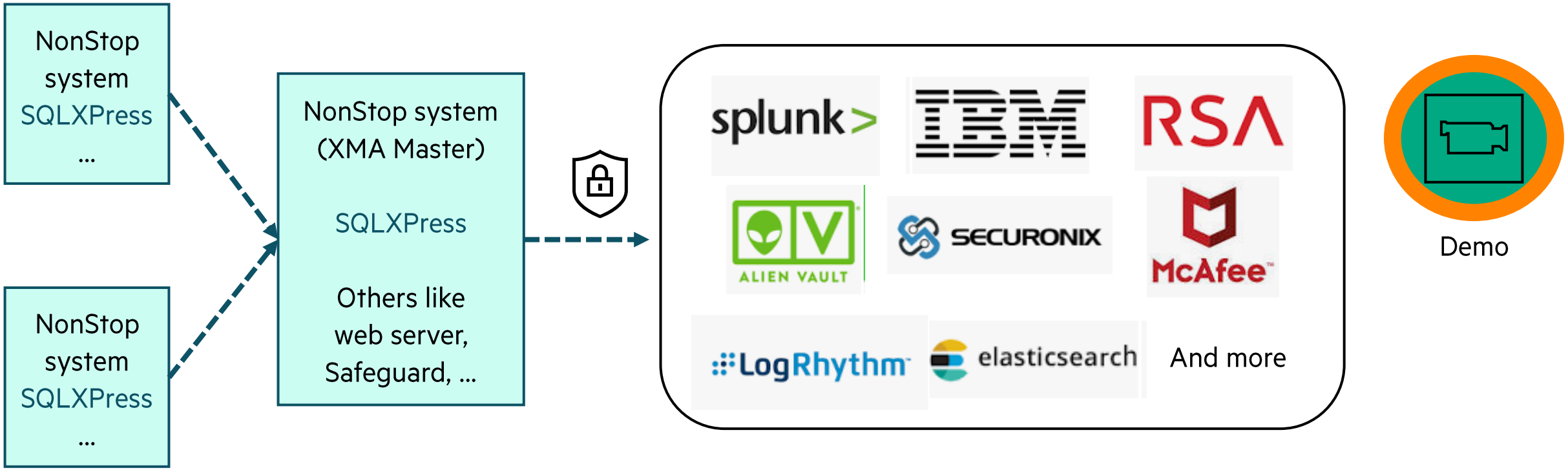
Non-repudiation

Detect security breach attempts

Demo

Security information and event management (SIEM)

- SQLXPress security events are forwarded to a NonStop XMA (Xygate Merged Audit) Master node
- For reasons that include security compliance, such acquired data needs to be sent off platform in a repository (aka SIEM) such as Splunk, ElasticSearch or others…
- XMA is part of the OS and provides filters for both incoming data into the XMA database and what is sent to a SIEM



Use parameterized queries

I Prevent data tampering

- SQL injection takes place using valid SQL syntax
  - For example, instead of a query with “emp=111”
  - The query is replaced with “emp=111 or 1=1”, still a valid syntax
- To protect against such attack, use prepared statements with parameterized queries
- Use input validation lists (Allow/Deny)
- Escape using input with single quotes
- Abstraction language layers such as JPA may add controls

SQL/MX built-in

Benefit examples

Avoid SQL Injection attacks

Quick Tip

You can use Open Source SQLMap to test your application resistance to SQL injection

Implementing zero trust security with NonStop SQL

A simplified architecture is easier to secure

Security complexity increases exponentially with the number of different pieces to secure

Security Tip

88% of security breaches happen because of human error (*)

Simple to secure

HPE NonStop SQL

One RDBMS to manage

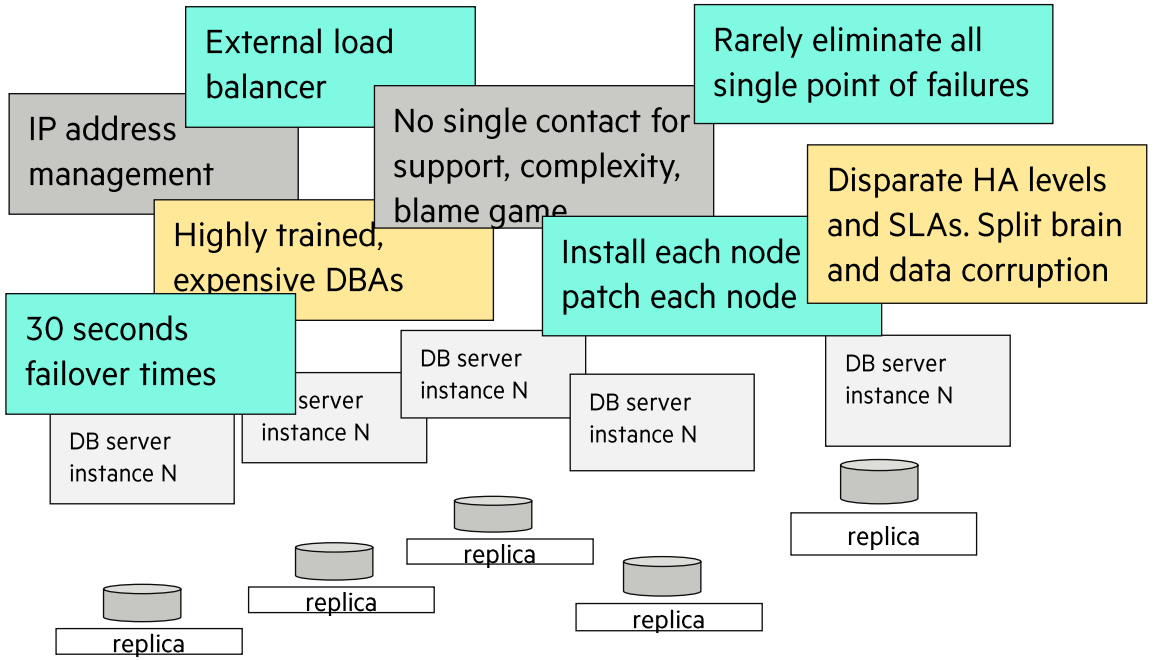
One OS to manage

Kernel-level SSI management

Kernel-level SSI management is the most desirable solution to manage clusters (*)

Complicated to secure

Other “assembled” DBMS clusters



(*) Gregory F. Pfister “In search of clusters” (1998).

(*) Stanford research 2021: https://www.influencive.com/human-error-is-still-the-number-one-cause-of-most-data-breaches-in-2021/

SQLXPress: simplify, accelerate and keep everything secured!

Simplify

One tool instead of 10 for basic DBA functions

Tasks	Tools required
Database objects creation/update/deletes ; Query whiteboard; MXCS management; View/update data in a table; Import csv data into a table; Export data into a csv table; Show Graphical Query plans (Embedded SQL); Capture runtime statistics (Embedded SQL); Partition management; Lock analysis, scripting; process and transaction information; task manager	MXDM, mxci, rmxci, DB Visualizer, OSS import, VQP, FUP, pstate, tmfcom, netbatch

Accelerate

Only in SQLXPress

Tasks
Visual Query tuner (w/ metadata acquisition); Partition analysis and management; Create queries graphically; Histograms management ; Compare tables and DDL ; Disk space management; Database report

Secure

Zero trust ready

Tasks
MFA authentication, full RBAC capabilities, auditing, signed code, native encryption, security admin, SIEM integration

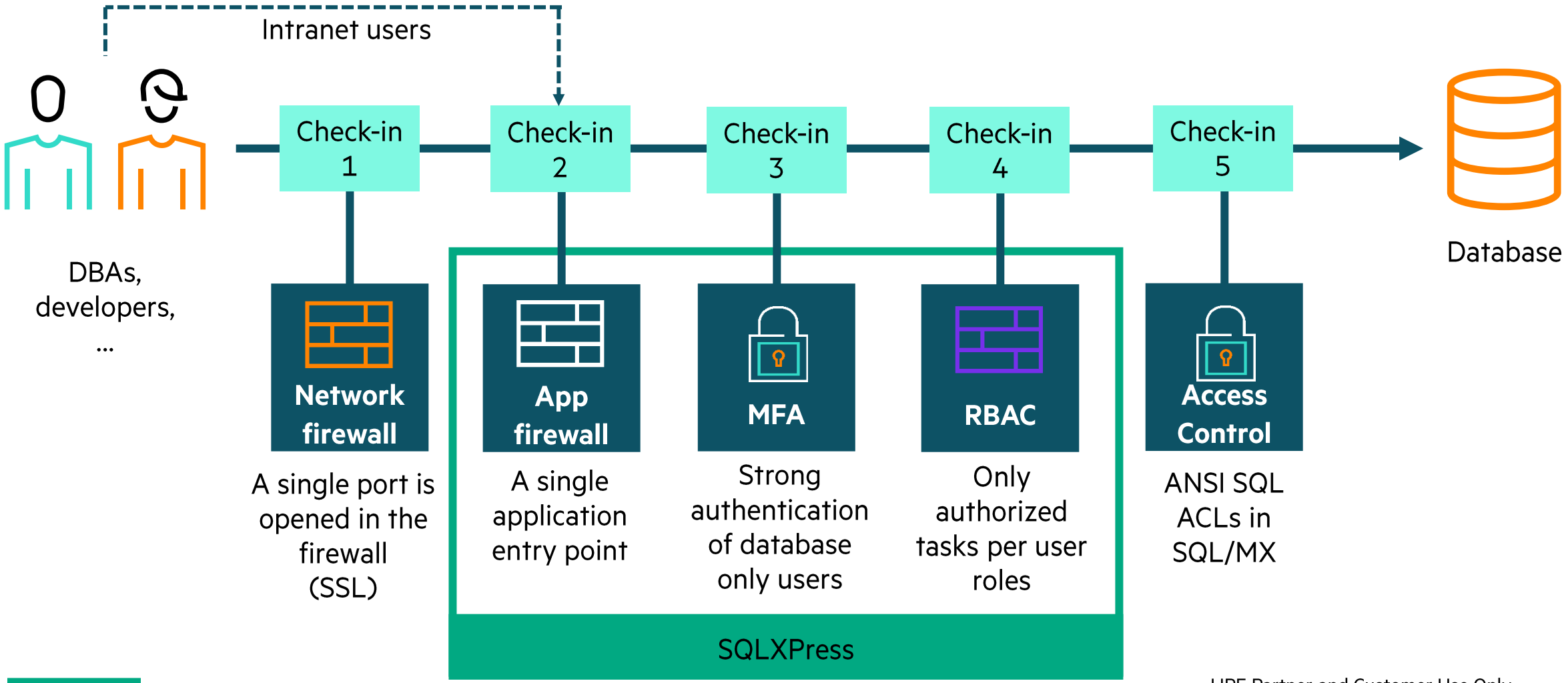
NonStop SQL out of the box security features

	NonStop SQL/MP	NonStop SQL/MX	NonStop SQL Cloud Edition
SQL memory protection	✓	✓	✓
Guardian RWEP	✓	N/A	N/A
Posix read, write, execute	N/A	✓	✓
ANSI Grant/Revoke	-	✓	✓
Privilege groups	- (can use RBAC Optional [1])	✓	✓
Security admin	- (or use Optional [1])	✓	✓
SSL (odbc/jdbc)	- (or use Optional [1])	✓	✓
PL/MX SQL governance	-	✓	✓
DBS reduced attack surface	-	✓	✓
Role-Based Access Control	Optional [1]	Optional [1]	✓
DBA MFA authentication	Optional [2]	Optional [2]	✓
DBA auditing	Optional [1]	Optional [1]	✓
Enterprise security integration	Optional [3]	Optional [3]	✓

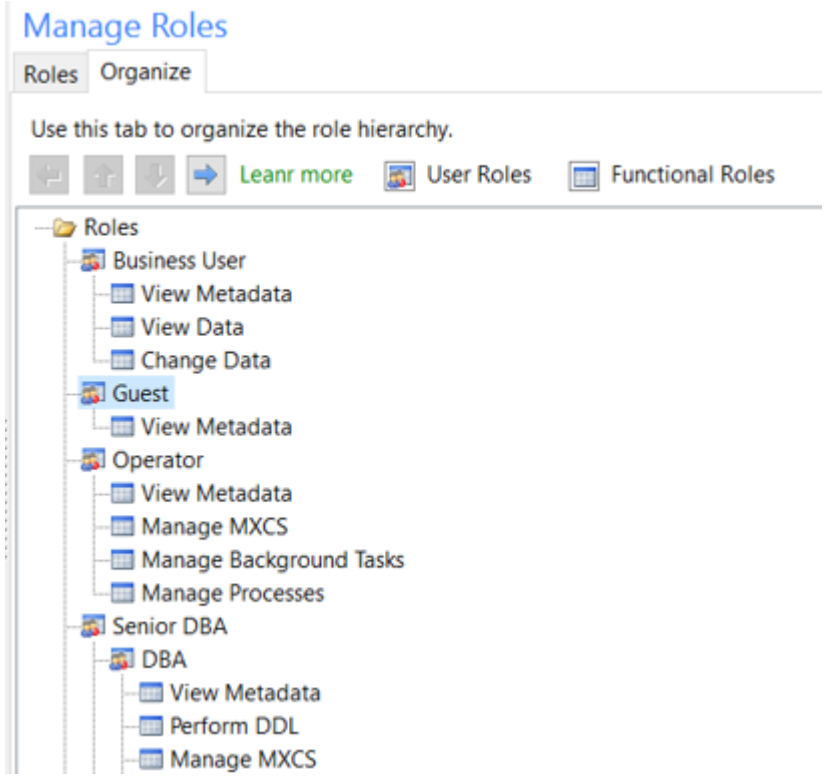
[1] SQLXPress ; [2] SQLXPress (via XUA); [3] SQLXPress (via XMA)

Zero trust security

Even once authenticated in the network and in the system, we still validate that each task execution is authorized



SQLXPress streamlines RBAC deployment in DBaaS



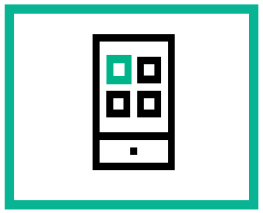
- Using SQLXPress roles, you streamline the creation of different SQL user profiles:
  - Managed database service provider
  - DBaaS tenant, tenant DBA, …
- At the same time, you ensure they are assigned with the appropriate level of security, for example taking a “Deny all by default” approach to support a zero-trust security strategy.
- You decide what that security level should be for your organization.
- And because SQLXPress includes the most comprehensive collection all the database functions, it allows you to centralize all the activities through that single tool, meaning you have only one entry point to secure.

SQLXPress with NonStop SQL Cloud Edition at no extra charge

HPE NonStop SQL Cloud Edition

A single database s/w bundle that includes everything you need to run a database server in your data fabric infrastructure

HPE NonStop SQL/MX



The complete HPE NonStop SQL/MX Software product with all features such as high-availability, scale and multi-tenancy already included that let you **focus on the application**

HPE NonStop SQLXPress

HPE NonStop SQLXPress, a management solution that makes every DBA task **easy** while maintaining the **highest level of security**

HPE NonStop Database Analyzer

HPE NonStop Database Analyzer (NSDA), an advanced real-time monitoring of your database workload that does not require any DBA skills and shows business metrics to drive **insights** and **optimize** your workloads

Futures (subject to change)

- Adding **Transparent Data Encryption** (TDE) to SQL/MX
  - TDE is well known in the industry as a compromise between complexity/constraints of user level encryption yet providing a strong and easily deployed encryption for data at rest
- **Administrative privileges**
  - Extends the model of ANSI SQL privileges beyond data access to administrative functions
  - Better separation of duties, granular security and removing requirements for highly privileged user
- **DBaaS**
  - Admin privileges, platform management integration, SSL support, enhanced resource management functions
- **SQLXPress**
  - SQL/MX 3.8: Full DML support for native LOBs, runtime stats, row count, built-in functions & expressions
  - WMS API support: RTS/WMS performance monitoring
  - Extended PL/MX package support
  - SQL/MX DBS: SQLXPress as a DBS client, SQLXPress as DBS administration
- Others:
  - Lob and Binary support for Linux and Windows ODBC drivers
  - Performance improvements

Conclusion

Secure database management: conclusion

At TBC 2023

- Visit the HPE NonStop booth for a quick demo

Confidentiality

Strong authentication mechanisms diminish password breaking
Granular ACLs and RBAC features help implement **zero trust security**
Principle of least privileges leads to **reduced attack surface**

Integrity

Data integrity can be preserved with a uniquely protected environment, **encryption** and **auditing** for immediate detection of breaches and trace back

Availability

The NonStop **availability** and multi-tenant capabilities can be leveraged to **reduce the impact** and attack surface to fewer components of the system yet in a **simple and centralized way**

Library and HPE Manuals references

Task	Manual(s)
Introduction	HPE NonStop Security Hardening Guide
Securing SQL/MX programs in OSS	Securing HP NonStop Servers in an Open Systems World XYPRO ISBN 978-1-55558-344-6
Securing User Modules	HPE NonStop SQL/MX Release x.y Management Guide
Turn on Safeguard OSS auditing	OSS Management and Operations Guide
SQL/MX Security Administrator	SQL/MX 3.x Reference Manual
Privilege groups	SQL/MX 3.x Reference Manual
General database security	Implementing Database Security and Auditing Ron Ben Natan ISBN 1-5558-334-2
Multi-factor Authentication	HPE NonStop Security Hardening Guide and XUA reference manual
System security	Safeguard Reference Manual

NonStop Partnership– It's a Beautiful Thing!

Thank you for attending this talk TBC23-TB53 Enable Zero Trust Security with NonStop SQL

Roland.lemoine@hpe.com

HPE Slides and Materials Usage

This content is protected

This presentation is the property of Hewlett Packard Enterprise and protected by copyright laws of the United States. The material in this presentation is provided to attendees of the NonStop TBC 2023 as part of their registration and attendance at the event. Attendees are free to use this material and share it with others within their own company.

This material may not be quoted, copied, communicated or shared with third parties or mutual customers without permission from HPE. To request permission to share material in this presentation outside of your company, send an email to roland.lemoine@hpe.com explaining the usage you are intending and your request will be considered.