CCN-CERT

# BP/23

# Security recommendations for DB2 databases

GOOD PRACTICE REPORT

OCTOBER **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edit

Paseo de la Castellana 109, 28046 Madrid, Spain



Date of edition: February 2022

Sidertia Solutions S.L. has participated in the creation and modification of this document and its annexes.

## Foreword

In an increasingly complex and globalised world, in which information and communication technologies (ICTs) play an extremely important role, we must be aware that the proper management of cybersecurity is a collective challenge that we must necessarily face. It is necessary to ensure the protection of our country's economic, technological and political capacity, especially when the proliferation of targeted attacks and the theft of sensitive information is an undeniable reality.

It is therefore essential to keep abreast of the threats and vulnerabilities associated with the use of new technologies. Knowledge of the risks that loom over cyberspace must serve to implement with guarantees the measures, both procedural and technical and organisational, that allow for a safe and reliable environment.

Law 11/2002, of 6 May 2002, regulating the National Intelligence Centre (CNI), entrusts the National Intelligence Centre with the exercise of functions relating to the security of information technologies and the protection of classified information, while conferring on its Secretary of State Director the responsibility of directing the National Cryptologic Centre (CCN).

Based on the CNI's knowledge and experience of threats and vulnerabilities in terms of emerging risks, the Centre carries out, through the National Cryptologic Centre, regulated by Royal Decree 421/2004 of 12 March, various activities directly related to ICT security, aimed at training expert personnel, the use of appropriate security technologies and the application of security policies and procedures.

Precisely, this series of CCN-STIC documents is a clear reflection of the work that this body carries out in terms of security implementation, enabling the application of policies and procedures, as the guides have been drawn up with a clear objective: to improve the degree of cybersecurity of organisations, aware of the importance of establishing a reference framework in this area to support government staff in carrying out the difficult task of providing security for the ICT systems under their responsibility.

With this series of documents, the National Cryptologic Centre, in compliance with its tasks and with what is reflected in Royal Decree 3/2010 regulating the National Security Scheme in the field of electronic administration, contributes to improving Spanish cybersecurity and maintaining the infrastructures and information systems of all public administrations with optimal levels of security. The aim is to generate confidence and guarantees in the use of these technologies, protecting the confidentiality of data and guaranteeing its authenticity, integrity and availability.

February 2022

**Paz Esteban López**
Secretary of State
Director of the National Cryptologic Centre

# Index

# 1. About CCN-CERT, National Governmental Cert

The CCN-CERT is the Information Security Incident Response Team of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

**The CCN-CERT is the Information Security Incident Response Team of the National Cryptologic Centre**

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, by being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centres.

Its ultimate aim is to make cyberspace more secure and reliable, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

# 2. Fundamentals of database security

Database management systems run on specific platforms and operating systems that provide them with the fundamental elements of communication and access.

The security model of a database management system, therefore, from a simplified point of view, can be said to be divided into these two areas of action:

1. The scope of the platform where the service runs.
2. The environment and capabilities provided by the database manager itself.

The IBM DB2 product is a generalist relational database manager, which means that it can be used in multiple environments and applications, and can be deployed on Unix, Linux and Microsoft Windows servers.

In all cases, it will be important not to lose sight of the security aspects that are configured at the operating system level, such as users, services, communications and protocols, as well as those that are configured in the DB2 environment, such as authorisation processes and access control to the data residing in the different databases.

**Database management systems run on specific platforms and operating systems that provide them with the fundamental elements of communication and access**

Authentication is the process by which a system verifies the identity of a user. In DB2, this process is performed outside the application environment, through an authentication module. By means of different modules that DB2 incorporates, it is possible to make use of authentication protocols such as LDAP and Kerberos. User authentication is usually performed by the operating system or by an external server.

**Authentication is the process by which a system verifies the identity of a user**

Authorisation is the process of determining whether an authenticated user has access to the information and permissions they are requesting. This process is carried out entirely within IBM DB2, consulting the permissions associated with a specific identity. In this sense, there are different types of permissions that can be granted.

A. **Primary permissions:** Those that are granted directly to the authorisation identifier.

B. **Secondary permissions:** Those that are granted to groups and roles of which an authorisation identifier is a member.

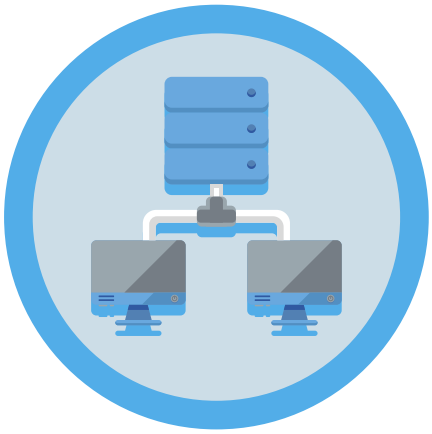
C. **Public permits:** Those that are granted to the entity PUBLIC.

D. **Context-based permissions:** Those that are granted to a trusted context role.

These permissions can be granted to users at various levels or categories:

E. **System-level authorisation:** The system administrator (SYSADM), system control (SYSCTRL), system maintenance (SYSMAINT) and system supervisor (SYSMON) authorities provide varying degrees of control over instance-level functions. This is a way to group privileges and control actions such as maintenance operations and other tasks for instances, databases and database objects.

F. **Database level authorisation:** The authorities security administrator (SECADM), database administrator (DBADM), access control (ACCESSCTRL), data access (DATAACCESS), SQL administrator (SQLADM), workload management administrator (WLMADM), loading data into a table (LOAD) and connecting to a database (CONNECT), provide varying degrees of control within the database.



G. **Object level authorisation:** Object level authorisation involves the checking of privileges when a specific operation is performed on a specific object.

H. **Content-based authorisation:** One way to authorise content-based access is through views. Views allow you to control which columns or rows in a table can be read by specific users. Label-based access control (LBAC), on the other hand, determines which users have permissions to read and write individual rows and columns.

Another important component in defining the security of a database manager is encryption, both of data in transit and data at rest. BD2 offers different data encryption options.

For encryption of data at rest, the following options are available:

- DB2 native encryption to encrypt databases and backup images.
- IBM InfoSphere Guardium Data Encryption solution to encrypt underlying operating system data and backup files.
- The AIX Encrypted File System (EFS) to encrypt operating system data and backup files.

To encrypt data in transit between DB2 clients and databases, it is recommended to make use of the native TLS support included in DB2 for inter-database communications:

- DB2 clients and servers.
- Primary and standby nodes in a DB2 HADR environment
- DB2 clients and a DB2 federation server.

**NOTE:**

**The DATA_ENCRYPT authentication type is deprecated and may be removed in a future release. To encrypt data in transit between clients and DB2 databases, it is recommended to use DB2 database system support for TLS (Transport Layer Security). In addition, DATA_ENCRYPT and SERVER_ENCRYPT use weak algorithms that are not compatible with CCN-STIC guidelines and should not be used.**

# 3. Secure database implementation

During the DB2 database installation process, a user ID, a group and a password are created. These values are created by default if they are not changed during the installation. Depending on the platform where DB2 is installed, different values are created:

A. **UNIX and Linux operating systems:** The installation wizard creates, by default, the user "dasusr" for the DAS, "db2inst" for the instance owner and "db2fenc" as the fenced user. It is recommended to specify different user names than those created by default.
If a default user already exists, the installation wizard adds a number from 1 to 99 to the default name, until a user ID that does not yet exist can be created.

B. **Microsoft Windows operating systems:** By default, the installation wizard creates a single user name the user (db2admin) for the DAS user, the instance owner, and the delimited users. It is recommended to change this default setting and specify different user names for each role. Unlike Linux and UNIX operating systems, no numeric value is added to the user ID.

**During the DB2 database installation process, a user ID, a group and a password are created**

As noted above, DB2 can use the operating system's own authentication mechanisms to authenticate users. Therefore, it is highly recommended to specify strong authentication requirements at the operating system level.

On Linux and UNIX operating systems, undefined passwords are treated as NULL and any user without a password will be considered to have a NULL password. From the operating system's perspective, this is a match and the user will be validated and will be able to connect to the database.

By default, the communication method of command execution in partitioned database environments on Linux and UNIX operating systems is based on the "rsh" tool. This tool transmits passwords in unencrypted text over the network, which may represent a security risk.

It is recommended to configure the registry variable DB2RSHCMD to set the path to the SSH executable to improve security in any type of environment

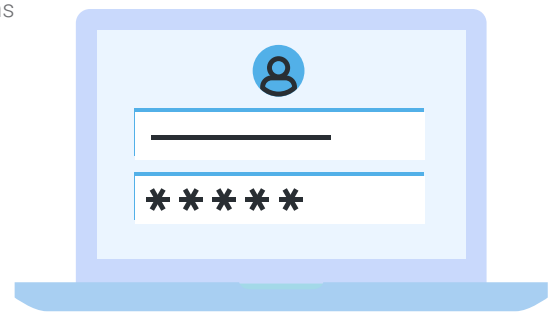
```
# db2set DB2RSHCMD=/usr/bin/ssh -i
```

It is also advisable to review and modify the default privileges that have been granted to users during installation. By default, the installation process grants system administration privileges (SYSADM) to the following users on each operating system:

A. **On Linux and UNIX operating systems,** SYSADM privileges are granted to any valid user belonging to the instance owner's primary group.

B. **On Microsoft Windows systems,** SYSADM privileges are granted to members of the Local Administrators group and the LocalSystem account.

If group enumeration has been configured (LOCAL or DOMAIN), then SYSADM privileges will also be applied to the administrators group on the domain controller where the users are defined. The DB2_GRP_LOOKUP environment variable allows you to control how DB2 performs group enumeration on Windows systems.



It is recommended to create instance-specific instance owner user identifiers for each instance, adding it only as a member of the group that owns the instance and not using it in any other group. This allows for more control over the number of users and groups that can modify the instance.

By default, during installation, extended security is enabled on all DB2 products installed on Windows. In this case, the installer creates two new groups DB2ADMNS and DB2USERS. Members of the DB2ADMNS group are also granted SYSADM privileges.

The privileges assigned to each user group when using Windows extended security are shown below.

| PRIVILEGE | DB2ADMNS | DB2USERS | MOTIVE |
|---|---|---|---|
| **Create a token object (SeCreateTokenPrivilege)** | Y | N | Token Manipulation (required for certain token manipulation operations and used in authentication and authorisation) |
| **Replace a process level token (SeAssignPrimaryTokenPrivilege)** | Y | N | Create process as another user |
| **Increase quotas (SeIncreaseQuotaPrivilege)** | Y | N | Create process as another user |
| **Act as part of the operating system (SeTcbPrivilege)** | Y | N | User login |
| **Generate security audits (SeSecurityPrivilege)** | Y | N | Manipulating audit and security logs |
| **Take ownership of files or other objects (SeTakeOwnershipPrivilege)** | Y | N | Modify object ACLs |
| **Increase scheduling priority (SeIncreaseBasePriorityPrivilege)** | Y | N | Modify the working memory of processes |
| **Backup files and directories (SeBackupPrivilege)** | Y | N | Profile and registry manipulation (required to perform certain registry and user profile manipulation routines: LoadUserProfile, RegSaveKey(Ex), RegRestoreKey, RegReplaceKey, RegLoadKey(Ex)) |

| PRIVILEGE | DB2ADMNS | DB2USERS | MOTIVE |
|---|---|---|---|
| Restore files and directories (SeRestorePrivilege) | Y | N | Profile and registry manipulation (required to perform certain registry and user profile manipulation routines: LoadUserProfile, RegSaveKey(Ex), RegRestoreKey, RegReplaceKey, RegLoadKey(Ex)) |
| Debug programs (SeDebugPrivilege) | Y | N | Token Manipulation (required for certain token manipulation operations and used in authentication and authorisation) |
| Manage auditing and security log (SeAuditPrivilege) | Y | N | Generate audit entries |
| Log on as a service (SeServiceLogonRight) | Y | N | Running DB2 as a service |
| Access this computer from the network (SeNetworkLogonRight) | Y | Y | Allow network credentials (allows DB2 database administrator to use the LOGON32_LOGON_NETWORK option to authenticate, which has performance implications) |
| Impersonate a client after authentication (SeImpersonatePrivilege) | Y | N | Client impersonation (required for Windows to allow the use of certain APIs to impersonate DB2 clients: ImpersonateLoggedOnUser, ImpersonateSelf, RevertToSelf, etc.) |
| Lock pages in memory (SeLockMemoryPrivilege) | Y | N | Support for large memory pages |
| Create global objects (SeCreateGlobalPrivilege) | Y | Y | Privilege to create global objects in a Terminal Services session (required on Windows) |

Finally, in all cases during installation, it is recommended to make use of strong passwords that comply with the organisation's security policies.

# 4. Secure database configuration

**The following are recommendations to strengthen the security of the DB2 database after the installation process has been completed.**

## 4.1 Access control

Designing appropriate access controls tailored to the needs of data exploitation by users and tools is essential to reduce the risks of exfiltration or unauthorised access. Most threats fall into this category and are minimised or eliminated by maintaining strict controls.

Access to an instance or a database requires the user to authenticate. DB2 provides different types of authentication. The type of authentication used is stored in the configuration file on the server and is configured when the instance is created. Each instance can have its own authentication type to access the server and the databases running on that instance.

- It is recommended to use strong authentication mechanisms such as SERVER, LDAP or Kerberos and to avoid using CLIENT authentication, especially in environments where client security cannot be guaranteed.

- It is recommended to follow the principle of least privilege, where only users are allowed to access the information and do the actions they really need to do, minimising the exposure surface.
- It is recommended to review and, if necessary, revoke permissions of users or groups that do not need them.
- In scenarios where sensitive data is stored, it is recommended, in addition to reviewing privileges, to establish granular access controls such as Row and Column Access Control (RCAC) and Label Based Access Control (LBAC), in order to prevent access to sensitive roles from untrusted environments.
- By default, a DBA has access to any table in his or her database instance. This is a risk, especially if the account has been breached or if these privileges are abused. It is recommended to revoke the DBA's data access privileges if he/she has no real need to access the data.
- It is recommended to check that PUBLIC access has not been granted to any database.
- An unauthorised user can access information residing in system tables if they have not been properly protected. It is recommended to review and protect important system tables such as Staging, Exception, SQL Replicated, Clone and Materialised Query Tables (MQTs).
- It is recommended to assign privileges through a role model, avoiding direct assignment to users.
- It is recommended to use operating system controls to prevent operating system administrators from gaining too much access.
- It is recommended to assign DBA permissions only through a role, and to control access to this role through trusted contexts. This allows you to restrict access only to connections originating from trusted computers.
- It is recommended to revoke the privilege to create databases for all users except the DBA user.

**It is recommended to check that PUBLIC access has not been granted to any database**

# 4.2 Audit

Auditing is a fundamental component in strengthening the security of an IT environment, especially in multi-user environments, where there is a need to know the actions performed by each of the users.

Logging of unwanted actions or unauthorised access to data and subsequent analysis improves the levels of data access control and the prevention of unauthorised access, malicious access or misconfiguration.

Monitoring of individual user and application access, including system administration actions, can provide a historical record of activity on your database systems.

DB2 auditing generates and maintains audit evidence for a series of pre-defined database events. The logs generated are stored in an audit log file and their analysis can reveal patterns of usage that would identify system misuse. Once identified, actions can be taken to reduce or eliminate such system misuse.

The audit function allows auditing at instance level as well as at individual database level, with all activities being recorded independently in separate logs for each.

The system administrator (who has the SYSADM authorisation) can use the "db2audit" tool to configure the auditing at instance level, as well as to control when such auditing information is collected.

The "db2audit" tool can also be used to archive database and instance audit logs, as well as to extract audit data from archived logs of any type.

**Auditing is a fundamental component in strengthening the security of an IT environment, especially in multi-user environments**

The security administrator (who has SECADM authority within a database) can use auditing policies in addition to the SQL AUDIT function to configure and control the auditing requirements for an individual database.

The security administrator can use the following audit routines to perform the specified tasks:

- **The stored procedure SYSPROC.AUDIT_ARCHIVE archives the audit records.**
- **The SYSPROC.AUDIT_LIST_LOGS table function allows you to locate records of interest.**
- **The stored procedure SYSPROC.AUDIT_DELIM_EXTRACT extracts data into delimited files for analysis.**

From the point of view of the audit information generated, DB2 identifies the different events in different categories:

A. **Audit (AUDIT).** Generates logs when the audit configuration is changed or when the audit log is accessed.

B. **Authorisation checking (CHECKING).** Generates logs during the authorisation check of attempts to access or manipulate DB2 database objects or functions.

C. **Object Maintenance (OBJMAINT).** Generates records when creating or releasing data objects and when altering certain objects.

D. **Security maintenance (SECMAINT).** Generates records when:

1. Object privileges or database authorisations are granted or revoked.
2. Security labels or exemptions are granted or revoked.
3. Group authorisation, role authorisation or overriding or restricting attributes of an LBAC security policy is altered.
4. SETSESSIONUSER privilege is granted or revoked.
5. You modify any of the configuration parameters: SYSADM_GROUP, SYSCTRL_GROUP, SYSMAINT_GROUP or SYSMON_GROUP

E. **System Administration (SYSADMIN).** Generates logs when operations requiring SYSADM, SYSMAINT or SYSCTRL authorisation are performed.

F. **User validation (VALIDATE).** Generates logs when authenticating users or retrieving security information from the system.

G. **Context of operation (CONTEXT).** Generates records to show the context of the operation when a database operation is performed. This category allows a better interpretation of the audit log file.

H. **EXECUTE.** Generates logs during the execution of SQL statements.

For each category, audit policies can be generated to record failures, successes or both. Enabling all categories and all events can lead to over-reporting and a high number of records.

- It is recommended to review the audit event logging needs and to select only those events that are important for the organisation or those that are related to the security of the system.
- It is recommended to create an AUDITOR role and grant the necessary privileges to read and manage audit events.
- It is recommended to control access to the AUDITOR role through trusted contexts. This allows restricting access only to connections originating from trusted computers.
- It is recommended that the generated audit files should not be copied, modified or deleted directly by the operating system administrator or by any other unauthorised user of the platform.
- It is recommended to make use of a centralised audit trail service.
- It is recommended to encrypt the authoring records stored on disk (data at rest), both on the database server and on the log centraliser service, if one is available.
- It is recommended to audit all DBA actions.
- It is recommended to audit user access, in particular those who have access to sensitive data.
- It is recommended to audit all accesses to important tables.
- If direct access to MQT (Materialised Query Tables) tables is required, it is recommended to enable granular auditing of all SQL accesses to these tables.
- It is recommended to audit all attempts to create databases.

**For each category, audit policies can be generated to record failures, successes or both**

# 4.3 Communications protection measures

Db2 uses the TLS (Transport Layer Security) protocol to securely transmit data between servers and clients.

To protect data in transit with the highest degree of reliability on all networks using TCP/IP, it is recommended to enable the use of TLS 1.2 or higher and to restrict the use of SSL, TLS 1.0 or TLS 1.1.

It is recommended to use robust cipher algorithm sets endorsed by the National Cryptologic Centre.

During TLS protocol negotiation, the client and server negotiate which cipher suite to use to exchange data. A cipher suite is a set of algorithms that are used to provide authentication, encryption and data integrity.

Db2 uses GSKit running in FIPS mode to provide TLS support. GSKit supports the following cipher suites:

| SETS OF ALGORITHMS SUPPORTED BY GSKIT | |
|---|---|
| TLS_RSA_WITH_AES_256_CBC_SHA | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA |
| TLS_RSA_WITH_AES_128_CBC_SHA | TLS_RSA_WITH_AES_128_GCM_SHA256 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_RSA_WITH_AES_128_CBC_SHA256 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA |

During negotiation DB2 automatically selects the strongest cipher set supported by both the client and the server.

If the server is required to accept only one or more specific cipher sets, the configuration parameter "ssl_cipherspecs" can be set:

- Any of the above values.
- A combination of values, separating each value by a comma, without spaces.
- Null. In this case, the strongest available algorithm would be selected.

It is recommended to verify that you have a recent version of DB2 where 3DES-based encryption algorithms have been disabled. If not, it is recommended to remove the following algorithm sets from the list of values in "ssl_cipherspecs":

- TLS_RSA_WITH_3DES_EDE_CBC_SHA.
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA.
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA.

**NOTE:**

**These algorithms are disabled as of the following versions: Db2 V10.5 FP9, Db2 V11.1.2.2 and Db2 V11.5.0.0.**

To enable TLS 1.2 in DB2, it is recommended to use certificates issued by a trusted certificate authority.

The DB2 database uses port 523 for the DB2 Administration Server (DAS), which is used by the DB2 database tools. It is recommended that you review and configure the ports used by all server instances by using the services file to map the service name in the server's database administrator configuration file to its port number.

In addition, for partitioned database environments and Db2 pureScale environments, if the registry variable DB2_FIREWALL_PORT_RANGE is set, it is recommended to only allow connections in the specified port range between members of the same DB2 instance.

If this registry variable is not set, connections must be allowed on all unprivileged ports between members of the same DB2 instance. Unprivileged ports have port numbers greater than or equal to 1024.

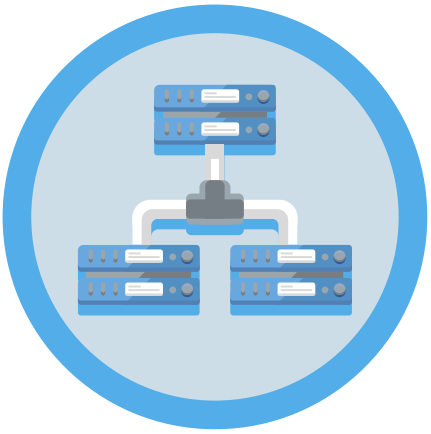
# 4.4 Information protection measures

**Information protection measures include both those that are configured or implemented in the database server environment as well as in the operating system environment running the server.**

## 4.4.1 Row and Column Access Control (RCAC)

Starting with DB2 version 10.1, support for configuring row and column access control (RCAC) is added as an additional layer of data security. RCAC controls access to a table at the row level, column level or both and can be used to complement the table privilege model.

With this feature, you can ensure that information is adequately protected and that users only have access to the subset of data they require to perform their work tasks and comply with specific rules and regulations.



Advantages of RCAC:

**A.** RCAC complies with the "need to know" principle.

**B.** No database user is inherently exempt from row and column access control rules.

**C.** Even higher level authorities, such as users with DATAACCESS authority, are not exempted from these rules.

**D.** Only users with security administrator (SECADM) authority can administer access controls to rows and columns within a database.

**E.** Table data is protected regardless of how a table is accessed via SQL.

**F.** Applications, makeshift query tools and reporting tools are all subject to RCAC rules. The application is data-centric.

**G.** g) No application changes are required to take advantage of this additional layer of data security.

The RCAC-based security model focuses on who accesses what information, not on a static set of permissions. The result sets for the same query change depending on the context in which the query was requested and no warnings or errors are returned.

It is recommended to design and make use of RCAC policies in environments where there are regulations or standards to comply with and access to data has to be made according to the context of the requester.

**The RCAC-based security model focuses on who accesses what information, not on a static set of permissions**

### 4.4.2 Label-Based Access Control (LBAC)

Label-based access control (LBAC) is a security model that is primarily intended for government applications or applications with known classification grades, as it requires data and users to be classified with a fixed set of rules that are implemented.

LBAC greatly increases the control you have over who can access the data, allowing you to decide exactly who has write access and who has read access to individual rows and columns.

In contrast, RCAC is a general-purpose security model intended primarily for commercial customers. Any organisation can use RCAC to create its own security rules, which in turn allows for greater flexibility.

An LBAC security policy includes this information:

**A.** Which security label components are used in the security labels that are part of the policy

**B.** What rules are used when comparing the components of the security label

**C.** Which of certain optional behaviours are used when accessing data protected by the policy

**D.** What additional security labels and exceptions should be considered when enforcing access to data protected by the security policy.

Each protected table must have one and only one security policy associated with it. The rows and columns of that table can only be protected with security labels that are part of that security policy and all access to the protected data follows the rules of that policy.

**Label-based access control (LBAC) is a security model that is primarily intended for government applications or applications with known classification grades**

You can have multiple security policies on a single database, but you cannot have more than one security policy protecting a given table.

LBAC is recommended at the registry level when handling sensitive or classified information related to government entities.

LBAC at registry level is recommended when the following statements are true:

**A.** The degree of classification of the data is known.

**B.** The classification of the data can be represented by one or more LBAC security labels.

**C.** Authorisation rules can be linked to the components of the security label.

LBAC at spinal level is recommended when:

**A.** It is required to protect sensitive columns from unauthorised access to the table owners or even the DBA.

**B.** It is required to protect entire tables from unauthorised access to the table owners or even the DBA. In this case, you will assign a security label to all columns of the table, then assign the security label to a role and assign that role only to users who require access to the table information.

The following should be considered before implementing an LBAC-based security model:

**A.** LBAC will never allow access to data that is prohibited by discretionary access control.

**B.** LBAC policies only limit access to protected data. They have no effect on unprotected data.

**C.** LBAC policies are not checked when you remove a table or database, even if the table or database contains protected data.

**D.** LBAC policies are not checked when backing up data. If a user can run a backup of a table, the rows that are backed up are not limited in any way by LBAC protection of the data. In addition, the data on the backup media is not LBAC protected. Only the data in the database is protected.

**E.** LBAC cannot be used to protect any of the following types of tables:

1. A staging table.
2. A table on which a staging table depends.
3. A typed table.

Regardless of the access controls implemented, it is recommended to make use of encryption at rest mechanisms for data, tables, audit files and backup files at the operating system level.

# 4.5 Backup policies

Sometimes a poor backup protection policy allows unauthorised access to data that is no longer protected by server security.

If data stored in backups are left unprotected, they can be accessed directly from the backup service.

It is recommended to encrypt all backup files and archive images, regardless of the medium on which they are stored.

It is recommended to ensure that the restoration of any backup should require controlled access to the encryption key and should be audited, both the access and the restoration itself.

# 5. Glossary

**Authentication:** is the process by which a system verifies the identity of a user. In DB2, this process is performed outside the application environment, through an authentication module. By means of different modules that DB2 incorporates, it is possible to make use of authentication protocols such as LDAP and Kerberos. User authentication is usually performed by the operating system or by an external server.

**Authorisation:** is the process of determining whether an authenticated user has access to the information and permissions being requested. This process is carried out entirely within IBM DB2, consulting the permissions associated with a specific identity

**DB2 Native Encryption:** Db2 Native Encryption provides built-in encryption capability to protect database backup images and key database files from unauthorised access while on external storage media. Encryption is a key component of offline data protection.

**TLS:** Transport Layer Security is a communications protocol whose main purpose is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS registration protocol and the TLS handshake protocol. During TLS negotiation, a public key algorithm is used to securely exchange digital signatures and encryption keys between a client and a server. The identity information and the key are used to establish a secure connection for the session between the client and the server. Once the secure session is established, the data transmission between the client and the server is encrypted using a symmetric algorithm, such as AES.

**HADR:** High Availability Disaster Recovery. DB2 on Red Hat OpenShift supports High Availability Disaster Recovery (HADR) to protect the database against data loss. HADR provides a high-availability solution to partial and complete site failures by replicating changes from a source database, called the primary database, to target databases, called standby databases.

**DB2 Federation Server:** A federated system is a special type of distributed database management system (DBMS) that consists of a database instance acting as a federated server, a database acting as a federated database, one or more data sources, and clients (users and applications) accessing the database and data sources. A federated system serves as a foundation upon which one or more data virtualisation solutions can be built. Within a federated system, a single SQL statement can access data that is distributed across multiple data sources.

**Fenced user:** the fenced user is a user type used to execute user-defined functions (UDFs) and stored procedures outside the address space used by the DB2 database. The default user is db2fenc1 and the default group is db2fadm1.

**DAS:** DB2 Administration Server. The DB2 Administration Server (DAS) is a control point that is used solely to assist with tasks on DB2 database instances. You must have a running DAS if you want to use tools such as the Replication Center or the Developer Center. DB2 Administration Server (DAS) has been deprecated and may be removed in a future release. DAS is not supported in Db2 pureScale environments.

**RSH:** protocol for remote execution of console commands for administration of a DB2 database. The use of rsh is not recommended due to its use of weak encryption algorithms.

**SSH:** Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. SSH can be used as the basis for a number of secure network services as it provides robust encryption, server authentication and integrity protection. It also provides data compression.

**Extended Security:** installation option that is enabled by default when DB2 is installed on Windows operating systems. This installation option creates two security groups (DB2ADMNS and DB2USERS) at the operating system level and grants them controlled privileges.

**RCAC:** Row and Column Access Control. It allows access to a table to be controlled at row level, column level or both and can be used to complement the table privilege model, ensuring that information is adequately protected and that users only have access to the subset of data that is required to perform their job tasks and comply with specific rules and regulations.

**LBAC:** Label Based Access Control. It is a security model that is primarily intended for government applications or applications with known classification grades, as it requires data and users to be classified with a fixed set of rules that are implemented.

**DBA:** Database Administrator.

**MQT:** Materialized Query Tables. Materialised Query Tables (MQTs) are tables whose definition is based on the result of a query. MTQ tables cache the results of a query and when the query is re-executed, the database engine can return data from the materialised query table to improve performance. The data consists of pre-computed results from the tables specified in the materialised lookup table definition.

**GSKit:** Global Security Kit. DB2 uses the Global Security Kit (GSKit) cryptographic capabilities to encrypt both data at rest (native encryption) and data in transit. The GSKit is used to implement the SSL and TLS protocols that enable secure DB2 communications over the network.

**FIPS:** Federal Information Processing Standards. Federal Information Processing Standards (FIPS) Publication 140-2 is a U.S. government standard that defines the minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

**DB2 pureScale:** a set of IBM technologies that help reduce the risk and cost associated with distributed database solution growth by providing extreme capacity and application transparency. The Db2 pureScale environment is designed for continuous availability and combines several integrated software components into a highly available database solution. These components are automatically installed and configured when DB2 pureScale Feature is deployed.

# 6. Summary table of security enhancement measures

| FIELD | NUM. | MEASURE | MOTIVE |
|---|---|---|---|
| **SECURE IMPLEMENTATION** | 1. | On Unix or Linux systems, it is recommended to specify different user names than those created by default. | Avoid using default names to plan attacks on the database. |
| | 2. | On Windows systems, it is recommended to change this default setting and specify different user names for each role. | Avoid using default names to plan attacks on the database. |
| | 3. | It is recommended to configure the registry variable DB2RSHCMD to set the path to the SSH executable to improve security in this type of environment. | By default, on Linux and UNIX operating systems, DB2 uses the rsh tool. This tool transmits passwords in clear text over the network, which can pose a security risk. |
| | 4. | It is recommended to create instance-specific instance owner user IDs for each instance, adding it only as a member of the instance owner group and not using it in any other group. | It allows greater control over the number of users and groups that can modify the instance. |
| | 5. | During installation, it is recommended to use strong passwords that comply with the organisation's security policies. | Minimises the possibility of brute force attacks. |

| FIELD | NUM. | MEASURE | MOTIVE |
|---|---|---|---|
| **ACCES CONTROL** | 6. | It is recommended to use strong authentication mechanisms such as SERVER, LDAP or Kerberos and to avoid using CLIENT authentication, especially in environments where client security cannot be guaranteed. | Improve the security and reliability of authentication mechanisms. |
| | 7. | It is recommended to follow the principle of least privilege, where only users are allowed to access the information and do the actions they really need. | Minimise the exposure surface. |
| | 8. | It is recommended to review and, if necessary, revoke permissions of users or groups that do not need them. | Minimise the exposure surface. |
| | 9. | In scenarios where sensitive data is stored, it is recommended, in addition to reviewing privileges, to establish granular access controls. | Prevent access to sensitive roles from untrusted environments. |
| | 10. | It is recommended to revoke the DBA's data access privileges if he/she has no real need to access the data. | By default, a DBA has access to any table in his or her database instance. This poses a risk, especially if the account has been breached or if these privileges are abused. |
| | 11. | It is recommended to check that PUBLIC access has not been granted to any database. | Minimise the exposure surface. |
| | 12. | It is recommended to review and protect important system tables such as Staging, Exception, SQL Replicated, Clone and Materialized Query Tables (MQTs). | An unauthorised user can access information residing in system tables if they have not been adequately protected. |
| | 13. | It is recommended to assign privileges through a role model, avoiding direct assignment to users. | Improve control and maintenance of access privileges. |
| | 14. | It is recommended to use the access controls of the operating system. | Prevent operating system administrators from gaining too much access. |

| FIELD | NUM. | MEASURE | MOTIVE |
|---|---|---|---|
| **ACCES CONTROL** | 15. | It is recommended to assign DBA permissions only through a role, and to control access to this role through trust contexts. | Allows to restrict access only to connections originating from trusted computers. |
| | 16. | It is recommended to revoke the privilege to create databases for all users except the DBA. | Minimise the exposure surface. |
| **AUDIT** | 17. | It is recommended to review the audit event logging needs and to select only those events that are important for the organisation or those that are related to the security of the system. | Control the audit information generated, avoiding irrelevant data and storage problems that may lead to loss of relevant evidence. |
| | 18. | It is recommended to create an AUDITOR role and grant the necessary privileges to read and manage audit events. | Control who can access audit information and how. |
| | 19. | It is recommended to control access to the AUDITOR role through trusted contexts. | Allows to restrict access only to connections originating from trusted computers. |
| | 20. | It is recommended that the generated audit files should not be copied, modified or deleted directly by the operating system administrator or by any other unauthorised user of the platform. | Prevent exfiltration of data or access to sensitive audit information by bypassing database security mechanisms. |
| | 21. | It is recommended to make use of a centralised audit trail service. | Unification of different audit sources, facilitating log correlation and avoiding loss or manipulation of evidence. |
| | 22. | It is recommended to encrypt the authoring records stored on disk (data at rest), both on the database server and on the log centraliser service, if one is available. | Prevent exfiltration of data or access to sensitive audit information by bypassing database security mechanisms. |
| | 23. | It is recommended to audit all DBA actions. | Maintain an audit trail of administrative actions that may compromise the system. |

| FIELD | NUM. | MEASURE | MOTIVE |
|---|---|---|---|
| **AUDIT** | 24. | It is recommended to audit user access, in particular those who have access to sensitive data. | Maintain an audit trail of user actions. |
| | 25. | It is recommended to audit all accesses to important tables. | Maintain an audit trail of actions that may compromise the system. |
| | 26. | If direct access to MQT (Materialised Query Tables) tables is required, it is recommended to enable granular auditing of all SQL accesses to these tables. | Maintain an audit trail of actions that may compromise the system. |
| | 27. | It is recommended to audit all attempts to create databases. | Maintain an audit trail of administrative actions that may compromise the system. |
| **COMMUNICATIONS PROTECTION** | 28. | It is recommended to make use of the native TLS support included in DB2 for communications between:<br>· DB2 clients and servers.<br>· Primary and standby nodes in a DB2 HADR environment.<br>· DB2 clients and a DB2 federation server. | Prevent data capture in transit through the network. |
| | 29. | To encrypt data in transit between clients and DB2 databases, it is recommended to use the DB2 database system support for TLS (Transport Layer Security). | The DATA_ENCRYPT authentication type is deprecated and may be removed in a future version. DATA_ENCRYPT and SERVER_ENCRYPT use weak algorithms that are not compatible with CCN-STIC guidelines and should not be used. |
| | 30. | It is recommended to use robust cipher algorithm sets endorsed by the National Cryptologic Centre. | Prevent exploitation of vulnerabilities in weak or obsolete algorithms. |
| | 31. | It is recommended to verify that you have a recent version of DB2 where 3DES-based encryption algorithms have been disabled. | Older versions make use of weak or vulnerable encryption algorithms that should not be used. |
| | 32. | It is recommended to remove the following algorithm sets from the list of values in "ssl_cipherspecs":<br>· TLS_RSA_WITH_3DES_EDE_CBC_SHA.<br>· TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA.<br>· TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA. | Algorithm sets that make use of 3DES or SHA1 are considered weak or vulnerable and should not be used. |

| FIELD | NUM. | MEASURE | MOTIVE |
|---|---|---|---|
| **COMMUNICATIONS PROTECTION** | 33. | To enable TLS 1.2 in DB2, it is recommended to use certificates issued by a trusted certificate authority. | It allows to correctly validate the certificate issuing chain and therefore its trust. |
| | 34. | It is recommended to review and configure the ports used by all server instances by using the services file to map the service name in the server's database administrator configuration file to its port number. | Minimise the exposure surface, enabling only the necessary communication ports. |
| | 35. | For partitioned database environments and Db2 pureScale environments, if the registry variable DB2_FIREWALL_ PORT_RANGE is set, it is recommended to only allow connections in the specified port range between members of the same DB2 instance. | Minimise the exposure surface, enabling only the necessary communication ports. |
| | 36. | It is recommended to design and make use of RCAC policies in environments where there are regulations or standards to comply with and access to data has to be made according to the context of the requester. | Comply with the "need to know" principle. |
| | 37. | It is recommended to use LBAC at the registry level when handling sensitive or classified information related to government entities. | Comply with the "need to know" principle. |
| | 38. | It is recommended to use LBAC at registry level when the following statements are true:<br>· The degree of classification of the data is known.<br>· The classification of the data can be represented by one or more LBAC security labels.<br>· Authorisation rules can be linked to the components of the security label. | Comply with the "need to know" principle. |
| | 39. | LBAC at spinal level is recommended when:<br>· It is required to protect sensitive columns from unauthorised access to the table owners or even the DBA.<br>· It is required to protect entire tables from unauthorised access to the table owners or even the DBA. | Comply with the "need to know" principle. |

| FIELD | NUM | MEASURE | MOTIVE |
|---|---|---|---|
| **COMMUNICATIONS PROTECTION** | **40.** | Regardless of the access controls implemented, it is recommended to make use of encryption at rest mechanisms for data, tables, audit files and backup files at the operating system level. | Prevent unauthorised access to sensitive information outside the scope of protection of the database. |
| **BACKUP** | **41.** | It is recommended to encrypt all backup files and archive images, regardless of the medium on which they are stored. | Prevent unauthorised access to backups. |
| | **42.** | It is recommended to ensure that the restoration of any backup should require controlled access to the encryption key and should be audited, both the access and the restoration itself. | Prevent unauthorised access to backups and log any access through auditing. |

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


ccn-cert
centro criptológico nacional
CCN
centro criptológico nacional