PUBLIC
Document Version: 1.0 – 2026-03-17

SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Security Guide

Content

1 SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Security Guide

This guide focuses on the new security features and enhancements that are specific to SAP Adaptive Server Enterprise, cloud edition by IBM Cloud.

For an in-depth introduction of security implementation and administration for SAP ASE, see SAP Adaptive Server Enterprise Security Administration Guide.

2 Secure Your SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Instance

Learn how to ensure secure access control and secure setup and configuration of your SAP Adaptive Server Enterprise, cloud edition by IBM Cloud instance.

Essential Security Tasks

After your SAP ASE instance is provisioned, perform the following essential security tasks:

1. Create at least one user with database administration privileges.
   See User Management [page 6].
2. Lock the login `aseadmin`.
   The default cloud administration user `aseadmin` is not intended for day-to-day activities. Once you have used this user to create dedicated database users for administration tasks and assign privileges to these users, deactivate `aseadmin`.
3. Create audit policies.
   See Auditing [page 68].

Recommended Security Tasks

Keep your SAP ASE instance secure by following these general recommendations:

- Develop a security concept for your SAP ASE scenario and implement it as soon as possible.
- Define and implement a concept for user roles and privilege.
- Define and implement a concept for auditing operations.
- Configure a strong password policy.

3 Network and Communication Security

Encryption of data-in-transit ensures that the network communication to SAP Adaptive Server Enterprise, cloud edition by IBM Cloud is secured using TLS/SSL.

The network communication channels used by the SAP ASE cloud edition are always encrypted by using TLS/SSL. Any attempts to connect to the SAP ASE cloud edition without TLS/SSL are not allowed.

Network password encryption is enabled by default for all `isql` connection attempts to the SAP ASE cloud edition.

4 User Management

Every user who wants to work directly with SAP Adaptive Server Enterprise, cloud edition by IBM Cloud must have a login account into server and be a database user with the necessary privileges. Depending on the scenario, the user accessing the SAP ASE cloud edition may either be a technical system user, or an individual end user.

After successfully logging in, the user's authorization to perform the requested operations on the requested objects is verified. This is determined by the privileges that the user has been granted. Privileges can be granted to database users either directly, or indirectly through roles. For more information about the authorization model of the SAP ASE cloud edition, see Authorization [page 14].

4.1 Predefined Logins

A number of predefined logins (hereinafter referred to as SAP logins) are required to operate an SAP ASE cloud edition database. The following sections describe the logins that are available by default in the SAP ASE cloud edition.

aseadmin

Login	`aseadmin`
Description	All SAP ASE cloud edition instances have an administration user named `aseadmin`. The `aseadmin` login is used only by SAP ASE cloud edition service customers. → Tip **Don't** use the `aseadmin` login for routine tasks. Use `aseadmin` to create logins and database users for specific administrative tasks and assign them the privileges required. Then, deactivate the `aseadmin` login. ⓘ Note It is not possible to delete the `aseadmin` login.
Password Specification	The password for `aseadmin` is specified when an SAP ASE cloud edition instance is created. The password is expired 180 days later by default. It is not recommended to modify it to a value greater than 180.
System User IDs	-6

Default Granted Roles	`cust_sa_role`
	`cust_sso_role`
	`replication_maint_role_gp`
	`mon_role`
	`replication_role`
	`js_user_role`
	Note
	`sybase_ts_role` is not granted to `aseadmin` by default. But `aseadmin` can grant this role to any user if needed.

saptu

Login	`saptu`
Description	`saptu` is a technical database user that performs the setup of SAP ASE cloud edition instance and used by tooling for the server infrastructure work. This account would never be used by humans. `saptu` is the owner of master key and default database encryption key in the master database and has the `own database` privilege in system databases.
Password Specification	Not applicable This is a technical database user. It is not possible to log on with this user. Its password is stored in vault.
System User IDs	-4

Default Granted Roles	`saptu_role`
	`sa_serverprivs_role`
	`oper_role`
	`mon_role`
	`sybase_ts_role`
	`js_admin_role`
	`js_user_role`

sapsupport

Login	`sapsupport`

Description	`sapsupport` is for SAP human operators who use this account to diagnose customer issues and perform administrative tasks.
Password Specification	Not applicable This account is used by technical support and cloud operations teams. Its password will be stored in a vault.
System User IDs	-5

Default Granted Roles	`sapsupport_role`
	`sybase_ts_role`
	`js_admin_role`

sappr

Login	`sappr`
Description	`sappr` is responsible for password rotation. It rotates the passwords of `saptu`, `sapsupport` and `sappr`.
Password Specification	Not applicable This is a technical database user. It is not possible to log on with this user. Its password is stored in a vault.
System User IDs	-7
Default Granted Privileges	`change password` `allow exceptional login`

The `sa` login is locked automatically after provision is done.

You cannot lock, unlock, or modify the `sa`, `saptu`, `sappr`, and `sapsupport` logins.

Additional Logins

The following predefined logins are used by various SAP ASE components and users. All the password policy defined by customers are bypassed for these logins.

Separate pool of login connections are reserved for these technical users so that these users can login to perform the SAP ASE cloud edition service related functionality even if maximum number of user connection limit is reached.

User/Component	Logins	Privilege/Role	SUID
Ping agent	`sapping`	`allow exceptional login`	-8

User/Component	Logins	Privilege/Role	SUID

Telemetry	`sapexporter`	`mon_role` with the following privileges:
		`allow exceptional login`
		`map external file`
		`manage dump configuration`
		`own database on tempdb`
			-9

Audit log service	`sapaudlog`	`select any audit table` in the `sybsecurity` database `allow exceptional login`	-10
AMC Admin for IBM human user	`sapamcadmin`		-11

DR Admin login of HADR in IBM setup	`sapdradmin`	`own any database`
		`own database on master`
		`manage server`
		`manage hadr`
		`manage replication`
		`use any database`
		`MANAGE ANY LOGIN`
		`MANAGE CUSTOMER SERVER CONFIGURATION`
			-12

DR Maintenance login of HADR in IBM setup	`sapdrmaint`	Alias as dbo of the user database with the following roles granted:
		`sybase_ts_role`
		`replication_role`
		`replication_maint_role_gp`
		`sap_maint_user_role`
			-13

Only `sa` or users with `saptu_role` can modify and drop login attributes of all SAP logins.

5 Authentication

The identity of logins accessing SAP Adaptive Server Enterprise, cloud edition by IBM Cloud is verified through a process called authentication. The mechanisms used to authenticate individual users are specified as part of the login creation.

> **Note**
>
> For JDBC and ODBC client connections, user passwords are always transmitted in encrypted form during the user authentication process, never in plain text.

`aseadmin` is created with `ANY` authentication mechanism. See more details in the `create login` command. You can change the authentication mechanism with the `alter login` command.

5.1 Password Policy

The passwords of logins are subject to certain rules. These rules are defined in the password policy.

SAP defines password policy for SAP logins and uses the policy to generate passwords for these logins during their creation. You can define the password policy using `sp_passwordpolicy` for your logins according to the business needs. Your password policy is not applicable to all predefined SAP logins.

The following table shows whether or not the user in the row can change the password of the user in the column. For example, you can see from the table that `aseadmin` can change the password for `aseadmin` only.

	`sappr`	`saptu`	`sapsupport`	`sa`	`aseadmin`	**sapping**	**sapexporter**	**sapaudlog**	**sapamcadmin**	**sapdradmin**	**sapdrmaint**
`sappr`	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
`saptu`	No	No	No	No	No	No	No	No	No	No	No

	sappr	saptu	sapsupport	sa	aseadmin	sapping	sapex-porter	sapau-dlog	sapam-cadmin	sap-drad-min	sapdr-maint
sapsupport	No	No	No **Note** sapsupport is a shared login used by technical support and cloud operation teams.	No	No	No	No	No	No	No	No
sa	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
aseadmin	No	No	No	No	Yes	No	No	No	No	No	No
sapping	No	No	No	No	No	No	No	No	No	No	No
sapex-porter	No	No	No	No	No	No	No	No	No	No	No
sapau-dlog	No	No	No	No	No	No	No	No	No	No	No
sapam-cadmin	No	No	No	No	No	No	No	No	No	No	No
sap-dradmin	No	No	No	No	No	No	No	No	No	No	No

	sappr	saptu	sapsupport	sa	aseadmin	sapping	sapex-porter	sapau-dlog	sapam-cadmin	sap-drad-min	sapdr-maint
sapdr-maint	No	No	No	No	No	No	No	No	No	No	No

The `password exp warn interval` parameter which reminds you the password expiration is set to 7 (seven days before) by default. You can modify the parameter when needed. See the `sp_passwordpolicy` stored procedure for more details.

Enable Custom Password Checks

The owner of `sp_extrapwdchecks` and `sp_cleanpwdchecks` is changed from `dbo` to `aseadmin`. To set the custom password check properly, use `aseadmin` to create `master.aseadmin.sp_extrapwdchecks` and `master.aseadmin.sp_cleanpwdchecks` in the master database.

The owner of `pwdhistory` is changed from `dbo` to `aseadmin`. `aseadmin.pwdhistory` can be created in user database, but one of the following steps needs to be done to avoid the error when executing `sp_password` or `sp_addlogin`:

- Add the guest user into this user database.
- Add the user who is executing `sp_password` or `sp_addlogin` into this user database.

6 Authorization

When you access the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud database using a client interface, your ability to perform operations on database objects is determined by the privileges that you have.

All the privileges granted to your user account, either directly or indirectly through roles, are combined. This means that whenever you try to access an object, the system performs an authorization check on the user account, the user's roles, and directly granted privileges. The system does not need to check all the user's privileges. As soon as all requested privileges have been found, the system skips further checks and grants access.

> **Note**
>
> The `enable granular permissions` is set to 1 by default during the provisioning. The logins `aseadmin` and `sapsupport` are forbidden to change the value of this configuration parameter.

To check if you have the privilege to execute a statement, check your granted privileges in the `cust_sa_role` and `cust_sso_role` firstly. And then check in the following topics if the statement is in the authorized operations list of your granted privileges:

- Server-Wide Privileges [page 34]
- Database-Wide Privileges [page 58]

In addition, you can use `sp_helprotect` to verify if you have the required privileges for executing the statement.

6.1 System Roles

SAP Adaptive Server Enterprise, cloud edition by IBM Cloud creates several new system-defined roles.

`saptu_role` – contains a set of system privileges required by `saptu` login. Only `saptu` can inherit privileges from this system defined role.

`sapsupport_role` – contains a set of system privileges required by `sapsupport` login. All SAP Cloud Operation users can inherit privileges from this system-defined role.

`cust_sa_role` – contains a set of privileges required by customer admin for their business administrative work. The `aseadmin` login inherits this system-defined role by default and is able to grant or revoke this role to any SAP ASE cloud edition service user.

`cust_sso_role` – contains a set of privileges required by customer system security officer for the security related work. The login `aseadmin` inherits this system-defined role by default and is able to grant or revoke this role to any SAP ASE cloud edition service user.

`cust_sa_role` and `cust_sso_role` are created with the principle of separation of duties (SoD) for the customer.

SAP restricted roles:

- `sa_role`
- `sso_role`
- `saptu_role`
- `sapsupport_role`
- `navigator_role`
- `dtm_tm_role`
- `ha_role`
- `keycustodian_role`
- `hadr_admin_role_gp`
- `sa_serverprivs_role`
- `oper_role`

Use `sp_restore_system_role` (which requires `manage customer security permissions` privileges) to restore a role or database owner to the default role privilege configuration. `sp_restore_system_role` cannot be used to restore sap restricted roles.

6.1.1 Privileges Granted to saptu_role

This topic lists the server-wide privileges granted to `saptu_role` by default.

ALLOW EXCEPTIONAL LOGIN
CONNECT
CREATE DATABASE
DBCC CHECKALLOC ANY DATABASE
DBCC CHECKCATALOG ANY DATABASE
DBCC CHECKDB ANY DATABASE
DBCC CHECKINDEX ANY DATABASE
DBCC CHECKSTORAGE ANY DATABASE
DBCC CHECKTABLE ANY DATABASE
DBCC CHECKVERIFY ANY DATABASE
DBCC FIX_TEXT ANY DATABASE
DBCC INDEXALLOC ANY DATABASE
DBCC MONITOR
DBCC REINDEX ANY DATABASE
DBCC TABLEALLOC ANY DATABASE
DBCC TEXTALLOC ANY DATABASE
DBCC TUNE

DUMP ANY DATABASE
DUMP DATABASE ON master
KILL
KILL ANY PROCESS
LOAD ANY DATABASE
LOAD DATABASE ON master
MANAGE ANY AUTOTUNING RULE
MANAGE ANY ESP
MANAGE ANY LOGIN
MANAGE ANY REMOTE LOGIN
MANAGE ANY THREAD POOL
MANAGE AUDITING
MANAGE CUSTOMER SECURITY CONFIGURATION
MANAGE CUSTOMER SECURITY PERMISSIONS
MANAGE CUSTOMER SERVER CONFIGURATION
MANAGE CUSTOMER SERVER PERMISSIONS
MANAGE DATA CACHE
MANAGE DISK
MANAGE DUMP CONFIGURATION
MANAGE INTERNAL CONFIGURATION
MANAGE OPT GOAL
MANAGE RESOURCE LIMIT
MANAGE SAP ROLES
MANAGE SECURITY CONFIGURATION
MANAGE SECURITY PERMISSIONS
MANAGE SERVER
MANAGE SERVER CONFIGURATION
MANAGE SERVER PERMISSIONS
MANAGE TRACEFILE
MAP EXTERNAL FILE
MONITOR SERVER REPLICATION
MOUNT ANY DATABASE
ONLINE ANY DATABASE
ONLINE DATABASE ON master

OWN DATABASE ON master
OWN DATABASE ON model
OWN DATABASE ON sybsystemdb
OWN DATABASE ON sybsystemprocs
OWN DATABASE ON tempdb
QUIESCE ANY DATABASE
SELECT ON GET_APPCONTEXT
SELECT ON LIST_APPCONTEXT
SELECT ON RM_APPCONTEXT
SELECT ON SET_APPCONTEXT
SET SWITCH
SET TRACING
SET TRACING ANY PROCESS
SHOW SWITCH
SHUTDOWN
TRACE AUDITING
UNMOUNT ANY DATABASE
USE DATABASE ON sybsecurity

Database-wide privileges granted to saptu_role by default

`saptu_role` applies only on the `master` and `sybsecurity` databases and doesn't have database-wide privileges on any of the customer created databases.

create encryption key
manage any encryption key
manage column encryption key
manage database encryption key
manage master key
manage service key
select dbo.syslogininfo
select dbo.sysloginroles
select dbo.syslogins
select dbo.syssrvroles

`select any system catalog`
`select dbo.sysdatabases`
`select dbo.sysencryptkeys`
`select dbo.syslisteners`
`select dbo.sysobjects`

6.1.2 Privileges Granted to sapsupport_role

This topic lists the privileges granted to `sapsupport_role` by default.

Server-Wide Privileges

`ALLOW EXCEPTIONAL LOGIN`
`CHECKPOINT ANY DATABASE`
`CHECKPOINT ON master`
`CONNECT`
`DBCC CHECKALLOC ANY DATABASE`
`DBCC CHECKCATALOG ANY DATABASE`
`DBCC CHECKDB ANY DATABASE`
`DBCC CHECKINDEX ANY DATABASE`
`DBCC CHECKSTORAGE ANY DATABASE`
`DBCC CHECKTABLE ANY DATABASE`
`DBCC CHECKVERIFY ANY DATABASE`
`DBCC FIX_TEXT ANY DATABASE`
`DBCC INDEXALLOC ANY DATABASE`
`DBCC MONITOR`
`DBCC REINDEX ANY DATABASE`
`DBCC TABLEALLOC ANY DATABASE`
`DBCC TEXTALLOC ANY DATABASE`
`DBCC TUNE`
`DUMP ANY DATABASE`
`DUMP DATABASE ON master`

DUMP DATABASE ON model
DUMP DATABASE ON sybsystemdb
DUMP DATABASE ON sybsystemprocs
DUMP DATABASE ON tempdb
LOAD ANY DATABASE
LOAD DATABASE ON master
LOAD DATABASE ON model
LOAD DATABASE ON sybsystemdb
LOAD DATABASE ON sybsystemprocs
LOAD DATABASE ON tempdb
MANAGE ANY THREAD POOL
MANAGE INTERNAL CONFIGURATION
MONITOR QP PERFORMANCE
MONITOR SERVER REPLICATION
ONLINE ANY DATABASE
ONLINE DATABASE ON master
SELECT ON ASEHOSTNAME
SELECT ON GET_APPCONTEXT
SELECT ON LIST_APPCONTEXT
SET SWITCH
SET TRACING
SET TRACING ANY PROCESS
SHOW SWITCH
SHUTDOWN
TRACE AUDITING

Database-Wide Privileges

No database-wide privileges granted on any customer created databases by default. You can grant proper database-wide privileges to `sapsupport_role` accordingly.

The privileges in the following table applied on the `master` database and the `sybsecurity` database

references any table
reorg any table

`select any system catalog`
`select any table`

> **Note**
>
> `select any audit table` is not in the list because only `saptu` can access audit records.

6.1.3 Privileges Granted to cust_sa_role

This topic lists the server-wide and database-wide privileges granted to `cust_sa_role` by default.

The server-wide privileges granted to `cust_sa_role` by default:

`ALLOW EXCEPTIONAL LOGIN`
`CHECKPOINT ANY DATABASE`
`CHECKPOINT ON master`
`CONNECT`
`CREATE DATABASE`
`DBCC CHECKALLOC ANY DATABASE`
`DBCC CHECKCATALOG ANY DATABASE`
`DBCC CHECKDB ANY DATABASE`
`DBCC CHECKINDEX ANY DATABASE`
`DBCC CHECKSTORAGE ANY DATABASE`
`DBCC CHECKTABLE ANY DATABASE`
`DBCC CHECKVERIFY ANY DATABASE`
`DBCC FIX_TEXT ANY DATABASE`
`DBCC INDEXALLOC ANY DATABASE`
`DBCC MONITOR`
`DBCC REINDEX ANY DATABASE`
`DBCC TABLEALLOC ANY DATABASE`
`DBCC TEXTALLOC ANY DATABASE`
`DBCC TUNE`
`DUMP ANY DATABASE`
`KILL`
`KILL ANY PROCESS`
`LOAD ANY DATABASE`

MANAGE ANY AUTOTUNING RULE
MANAGE ANY DATABASE
MANAGE ANY ESP
MANAGE ANY EXECUTION CLASS
MANAGE ANY THREAD POOL
MANAGE CUSTOMER SERVER CONFIGURATION
MANAGE CUSTOMER SERVER PERMISSIONS
MANAGE DATA CACHE
MANAGE DISK
MANAGE LOCK PROMOTION THRESHOLD
MANAGE OPT GOAL
MANAGE RESOURCE LIMIT
MANAGE ROW CACHE
MANAGE SERVER
MANAGE TRACEFILE
MAP EXTERNAL FILE
MONITOR QP PERFORMANCE
MONITOR SERVER REPLICATION
ONLINE ANY DATABASE
ONLINE DATABASE ON master
OWN ANY DATABASE
OWN DATABASE ON model
SELECT ON GET_APPCONTEXT
SELECT ON LIST_APPCONTEXT
SELECT ON RM_APPCONTEXT
SELECT ON SET_APPCONTEXT
SET SWITCH
SET TRACING
SET TRACING ANY PROCESS
SHOW SWITCH
USE ANY DATABASE

The database-wide privileges granted to `cust_sa_role` by default on system databases:

`alter any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any default`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any function`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any index`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any object`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any procedure`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any rule`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any trigger`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any view`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`dbcc checkalloc`

`dbcc checkcatalog`

`dbcc checkdb`

`dbcc checkindex`

`dbcc checkstorage`

`dbcc checktable`

`dbcc checkverify`

`dbcc fix_text`

`dbcc indexalloc`

`dbcc reindex`

`dbcc tablealloc`

`dbcc textalloc`

`delete any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any default`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any function`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any object`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any procedure`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any rule`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any trigger`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any view`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`execute any function`

`execute any procedure`

`identity_insert any table`

`identity_update any table`

`insert any table`

> **Note**
>
> Not applicable in the `master` database.

`manage abstract plans`

`manage any statistics`

`manage any user`

`manage checkstorage`

`manage database`

`manage replication`

`references any table`

> **Note**
>
> Not applicable in the `master` database.

`reorg any table`

> **Note**
>
> Not applicable in the `master` database.

`report checkstorage`

`select any system catalog`

`select any table`

`transfer any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`truncate any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`update any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create table`

> **Note**
>
> Not applicable in the `master` database.

`create view`

> **Note**
>
> Not applicable in the `master` database.

`create trigger`

> **Note**
>
> Not applicable in the `master` database.

`create procedure`

`create default` **Note** Not applicable in the `master` database.
`create rule` **Note** Not applicable in the `master` database.
`create function` **Note** Not applicable in the `master` database.
`create schema` **Note** Not applicable in the `master` database.

6.1.4 Privileges Granted to cust_sso_role

This topic lists the server-wide and database-wide privileges granted to `cust_sso_role` by default.

Server-wide privileges granted to `cust_sso_role` by default:

`manage customer security permissions`
`manage customer security configuration`
`change password` **Note** Changing password for predefined SAP logins is not supported.
`manage any login`
`manage any login profile`
`manage any remote login`
`manage auditing`
`trace auditing`

`manage roles`

> **Note**
>
> Managing SAP restricted roles is not supported. For more information, see System Roles [page 14].

`set proxy`

`use database`

> **Note**
>
> In the `sybsecurity` database.

`use any database`

Database-wide privileges granted to `cust_sso_role` by default on the `master` database and the `sybsecurity` database:

`manage database encryption key`

> **Note**
>
> Only in the master database.

`manage service key`

`decrypt any table`

`manage column encryption key`

`create encryption key`

`select any audit table`

> **Note**
>
> Only in the `sybsecurity` database.

`truncate any audit table`

> **Note**
>
> Only in the `sybsecurity` database.

6.1.5 Restrictions to Customer Users

Customer users have some restrictions in the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service.

Customer users cannot:

- apply `sp_locklogin` on system predefined logins.

- set proxy to system predefined logins.
- apply `alter login…modify password` on system predefined logins.
- `alter login` and `drop login` for system predefined logins.
- `alter role` and `drop role` on `saptu_role` or `sapsupport_role`.
- apply `sp_autoconnect` on system predefined logins.
- apply `sp_addexternlogin` on system predefined logins.
- apply `sp_dropexternlogin` on system predefined logins.
- apply `sp_addremotelogin` on system predefined logins.
- apply `sp_dropremotelogin` on system predefined logins.
- apply `sp_defaultdb` on system predefined logins.
- `alter master key` in the master database.
- apply `sp_add_resource_limit` on system predefined logins.
- apply `sp_addalias` on system predefined logins.
- apply `sp_clearstats` on system predefined logins.
- apply `sp_drop_resource_limit` on system predefined logins.
- apply `sp_dropserver <server_name>, droplogins` on system predefined logins.
- change error log path via `sp_errorlog`.
- execute any deprecated system stored procedures to change attribute on sap logins, such as `sp_addlogin`, `sp_droplogin`, `sp_modifylogin`, `sp_password`, `sp_addengine`, `sp_dropengine`, and so on.

6.2 Permissions

In the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, the duties related to SAP administrative responsibilities and customer administrative responsibilities are separated using granular permission management. Several new permissions are developed accordingly.

In on-premises SAP ASE, all system privileges are managed by users with `manage server permissions`, `manage security permissions`, or `manage database permissions` privileges. In the SAP ASE cloud edition service, two more privileges are added to manage all system privileges:

- `manage customer server permissions` – users with this privilege can grant or revoke server-wide privileges for customer's business purpose. User with `manage customer server permissions` can grant or revoke this privilege. `aseadmin` (with `cust_sa_role`) has this privilege by default and can grant or revoke it to any SAP ASE cloud edition service user.
  For more information, see manage customer server permissions [page 29].
- `manage customer security permissions` – users with this privilege can grant or revoke security related server-wide privileges and database-wide privileges for customers' business purposes. User with the `manage customer security permissions` privilege can grant or revoke this privilege. The login `aseadmin` (with `cust_sso_role`) has this privilege by default and can grant or revoke it to any SAP ASE cloud edition service user.
  For more information, see manage customer security permissions [page 32].

6.2.1 manage customer server permissions

Users with `manage customer server permissions` can grant or revoke server-wide privileges managed by it.

The `manage customer server permissions` privilege is:

1. Initially explicitly granted to `cust_sa_role` on a newly deployed SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service.
2. Initially granted to `sa_role` and `saptu_role` for provision work.

Some of the privileges that were managed by `manage server permissions` are managed by `manage customer server permissions` in the SAP ASE cloud edition service. In other words, the set of privileges managed by `manage server permissions` in on-premises SAP ASE are split into two parts in the SAP ASE cloud edition service. One part is managed by `manage customer server permissions` and the other part is managed by `manage server permissions`.

Server-wide privileges managed by manage customer server permissions

`checkpoint`
`checkpoint any database`
`connect`
`create database`
`dbcc checkalloc any database`
`dbcc checkcatalog any database`
`dbcc checkdb any database`
`dbcc checkindex any database`
`dbcc checkstorage any database`
`dbcc checktable any database`
`dbcc checkverify any database`
`dump any database`
`kill`
`kill any process`
`load any database`
`manage any autotuning rule`
`manage any database`
`manage any ESP`
`manage any execution class`
`manage any thread pool`
`manage cache device`
`manage customer server configuration`

`manage data cache`
`manage resource limit`
`manage row cache`
`manage server`
`manage tracefile`
`map external file`
`monitor qp performance`
`online any database`
`online database` **Note** On any databases except `sybsecurity`.
`own any database` **Note** On any databases except system databases.
`own database` **Note** On any databases except system databases.
`set switch`
`set tracing`
`set tracing any process`
`show switch`
`use any database`

Database-wide privileges managed by manage customer server permissions

`alter any object owner`
`alter any table`
`create any default`
`create any function`
`create any index`
`create any object`
`create any procedure`
`create any rule`

create any table
create any trigger
create any view
create default
create function
create procedure
create rule
create schema
create table
create trigger
create view
delete any table
drop any default
drop any function
drop any object
drop any procedure
drop any rule
drop any table
drop any trigger
drop any view
execute any function
execute any procedure
identity_insert any table
identity_update any table
insert any table
manage any object permission
manage any statistics
manage any user
references any table
reorg any table
select any audit table
select any system catalog
select any table
transfer any table

`truncate any audit table`
`truncate any table`
`update any table`

6.2.2 manage customer security permissions

Users with the `manage customer security permissions` privilege can grant or revoke security related server-wide and database-wide privileges for the customer business purpose.

The `manage customer security permissions` privilege is:

1. Initially explicitly granted to `cust_sa_role` on a newly deployed SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service.
2. Initially granted to `sa_role` and `saptu_role` for provision work.

Server-wide privileges managed by the manage customer security permissions privilege

`change password` **Note** For any users except the predefined SAP logins.
`checkpoint` **Note** On the `sybsecurity` database.
`manage any login`
`manage any login profile`
`manage any remote login`
`manage auditing`
`manage certificates`
`manage customer security configuration`
`manage jwt provider`
`manage roles` **Note** For any roles except SAP restricted roles.

`online database`

> **Note**
>
> On the `sybsecurity` database.

`set proxy`

`setuser`

> **Note**
>
> On any databases except the master and `sybsecurity` database.

`trace auditing`

`use database`

> **Note**
>
> On the `sybsecurity` database.

Database-wide privileges managed by the manage customer security permissions privilege

`create encryption key`

> **Note**
>
> On non-system databases.

`decrypt any table`

`manage any encryption key`

`manage column encryption key`

`manage database encryption key`

`manage master key`

> **Note**
>
> On non-system databases.

`manage service key`

`select any audit table`

`select any system catalog`

`truncate any audit table`

6.3 Server-Wide Privileges

In the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, the duties related to IBM Cloud landscape administrative responsibilities and customer administrative responsibilities are separated with more granularity using granular permission management. Several new server-wide privileges are developed and some existing server-wide privileges are enhanced.

Server-Wide Privileges Developed for the SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Service

Privilege Name	Managed By
`manage customer server configuration`	`manage customer server permissions`
`manage customer security configuration`	`manage customer security permissions`
`manage internal configuration`	`manage server permissions`
`manage row storage cache`	`manage customer server permissions`
`manage tracefile`	`manage customer server permissions`
`trace auditing`	`manage customer security permissions`
`manage sap roles`	`manage security permissions`
`manage cache device`	`manage customer server permissions`

In on-premise SAP ASE, all server configuration options are managed by users with privilege `manage server configuration` and `manage security configuration`. In the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, three more privileges are added to manage all the server configuration options:

- `manage security configuration`
- `manage customer server configuration` – users with this privilege can modify the server configuration values for customer business purposes. Users with `manage customer server permissions` can grant or revoke this privilege to any SAP ASE cloud edition service user.
- `manage customer security configuration` – users with this privilege can modify the security-related server configuration values for customer business purposes. Users with `manage customer security permissions` can grant or revoke this privilege to any SAP ASE cloud edition service user.
- manage internal configuration – users with this privilege can modify the server configuration values for internal maintenance purposes.

Server-Wide Privileges for SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Service

While introducing new server-wide privileges in SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, some of the existing privileges need to remove some commands or stored procedures out of their control. The following table lists all the grantable server-wide privileges.

Privileges marked with an asterisk (*) may be granted or revoked when enable granular permissions is disabled.

Privilege name	Operations the privilege authorizes
Privileges management	
`manage security permissions`	Granting and revoking security privileges for internal maintenance purposes.
`manage server permissions`	Granting and revoking non-security server-wide privileges for internal maintenance purposes.
`manage customer security permissions`	Granting and revoking security privileges for customer business purposes. See manage customer security permissions [page 32] for more details. Built-in functions: • `set_appcontext()` • `list_appcontext()` • `get_appcontext()` • `rm_appcontext()`
`manage customer server permissions`	Granting and revoking nonsecurity server-wide privileges for customer business purposes. See manage customer server permissions [page 29] for more details. Built-in functions: • `authmech()` • `asehostname()`
Audit management	

Privilege name	Operations the privilege authorizes
`manage auditing`	Managed by `manage customer security permissions` TSQL commands: • `truncate table` – audit tables • `alter database sybsecurity` System stored procedures: • `sp_addaudittable` • `sp_audit` • `sp_confighistory` – change the option state of configuration history auditing
`trace auditing`	Managed by `manage customer security permissions` TSQL commands: • `set switch (7601)` DBCC commands: • `dbcc traceon (7601)` • `dbcc traceoff (7601)` • `sp_displayaudit`
Login and role management	
`allow exceptional login`	Granting login to the server when: • Server maximum connection limit exceeded • Master database is in restore mode • Server is in shutdown • Recovery is in progress (during server restart)
`change password`	Executing this command: • `alter login ... change password` Executing these system store procedure: `sp_locklogin` (unlock any login account which was locked because the user exceeded the limit of maximum failed logins)

Privilege name	Operations the privilege authorizes
`manage any login`	Executing these commands: • `create login` • `alter login` • `drop login` Executing these system procedures: • `sp_autoconnect` • `sp_defaultdb` • `sp_displaylogin` • `sp_grantlogin` (Windows only) • `sp_helpmaplogin` • `sp_logininfo` (Windows only) • `sp_locklogin` • `sp_maplogin` • `sp_revokelogin` (Windows only) Executing this function: • `valid_user`
`manage any login profile`	Executing these commands: • `create login profile` • `alter login profile` • `drop login profile` Executing this system procedure: • `sp_securityprofile`
`manage any remote login`	Executing these system procedures: • `sp_addexternlogin` • `sp_addremotelogin` • `sp_dropexternlogin` • `sp_dropremotelogin` • `sp_dropserver` • `sp_remoteoption`

Privilege name	Operations the privilege authorizes
`manage roles`	Managed by `manage customer security permissions` Executing these commands: • `create role` • `alter role` • `drop role` • `grant role` – apply on non-SAP restricted roles • `revoke role` – apply on non-SAP restricted roles Executing these system procedures: • `sp_displayroles` • `sp_grantlogin` • `sp_logininfo` • `sp_revokelogin`
`manage sap roles`	Managed by `manage security permissions` Executing these commands: • `grant role` – apply on SAP restricted roles • `revoke role` – apply on SAP restricted roles
Database Management	
`checkpoint`	Executing the `checkpoint` command for a specified database
`checkpoint any database`	Executing the `checkpoint` command for any database. Executing these system procedures: • `sp_fixindex`
`create database`*	Executing the `create database` command
`dump any database`	Executing these commands for any user database: • `dump database` • `dump transaction`
`dump database`	Executing these commands for a specified database: • `dump database` • `dump transaction`
`load any database`	Executing these commands for any user database: • `load database` • `load transaction`

Privilege name	Operations the privilege authorizes
`load database`	Executing these commands for a specified database: • `load database` • `load transaction`

Privilege name	Operations the privilege authorizes
`manage any database`	Managed by `manage customer server permissions` Perform database maintenance operations in any customer created database. Executing these commands: • `install jar` • `remove jar class` Executing these system procedures: • `sp_addmessage` • `sp_addobjectdef` • `sp_addsegment` • `sp_addthreshold` `sp_altermessage` • `sp_checksource` • `sp_dbextend 'simulate'` • `sp_dbextend 'execute'` • `sp_dbextend 'clear','threshold'` • `sp_dbextend 'check'` • `sp_dbextend 'set','threshold'` • `sp_dbextend 'modify', 'database'` • `sp_dbextend 'set','database'` • `sp_dbextend 'set', 'threshold'` • `sp_dropmessage` • `sp_dropobjectdef` • `sp_dropsegment` • `sp_dropthreshold` • `sp_droptype` • `sp_extendsegment` • `sp_forceonline_db` • `sp_forceonline_object` • `sp_forceonline_page` • `sp_hidetext` • `sp_modifthreshold` • `sp_placeobject` • `sp_procxmode` • `sp_rename` • `sp_rebuild_text` • `sp_spaceusage` (for some parameters)

Privilege name	Operations the privilege authorizes
`manage any database` (continued)	Executing these `dbcc` commands: • `dbcc dbrepair(remap)` • `dbcc dbrepair(newthreshold)` • `dbcc dbrepair(findstranded)` • `dbcc dbrepair(fixlogfreespace)` • `dbr_remap` • `dbcc dbrepair(ltmignore)` • `dbcc dbrepair(upd_usg)` • `dbcc dbrepair(auinit)` • `dbcc dbrepair(dmap_unlock)` • `dbcc rebuild_text` • `dbcc refreshids (placeobject)` • `dbcc refreshpdes` • `dbcc update_tmode` • `dbcc upgrade_obj` Executing these functions: • `derived_stat` • `identity_burn_max`
`mount any database`	Executing the `mount database` command for any database
`online any database`	Executing the `online database` command for any database
`online database`	Executing the `online database` command for a specified database
`own any database`	Managed by `manage customer server permissions` Act as `dbo` for any customer created database. See `own database` for a list of operations the privilege is authorized to perform.

Privilege name	Operations the privilege authorizes
`own database`	Acting as database owner for any database. Executing these commands: • `drop database` • `grant` (default) • `revoke` (default) • `checkpoint` • `dump database` • `dump transaction` • `load database` • `load transaction` • `online database` • `use database`
`own database` (continued)	Executing these system procedures: • `sp_addmessage` • `sp_altermessage` • `sp_dboption` • `sp_dbremap` • `sp_dropmessage` • `sp_fixindex` • `sp_forceonline_db` • `sp_forceonline_page` • `sp_helptext` • `sp_logdevice` • `sp_post_xpload` • `sp_renamedb` • `sp_setsuspect_granularity` • `sp_tempdb_markdrop` • `sp_version` • `xp_cmdshell` • `xp_enumgroups` • `xp_logevent` Executing these dbcc commands: • `dbcc addtempdb` • `dbcc dbrepair` • `dbcc reindex`

Privilege name	Operations the privilege authorizes
`quiesce any database`	Executing the `quiesce database` command for any database
`unmount any database`	Executing the `unmount database` command for any database
Server Maintenance	
`manage any thread pool`	Executing these commands: • `create thread pool` • `alter thread pool` • `drop thread pool`
`manage disk`	Executing these commands: • `disk init` • `disk refit` • `disk reinit` • `disk mirror` • `disk unmirror` • `disk remirror` Executing these system procedures: • `sp_addumpdevice` • `sp_diskdefault` • `sp_deviceattr` • `sp_dropdevice` • `sp_refit_admin` • `sp_dbextend` (required by some options)
`manage security configuration`	Enable or disable security related configurations. Executing these system procedures: • `sp_configure` (to set security-related configuration options) • `sp_encryption` • `sp_ssladmin [addcert] | [dropcert] | [refreshcert]`

Privilege name	Operations the privilege authorizes
`manage customer security configuration`	Enable or disable security related configurations. For more information, see manage customer security configuration [page 57]. Executing these system procedures: • `sp_configure` (to set security-related configuration options) • `sp_ldapadmin` • `sp_logintrigger` • `sp_passwordpolicy` • `sp_ssladmin`

Privilege name	Operations the privilege authorizes
`manage server`	Manage server maintenance operations Executing these system procedures: • `sp_addlanguage` • `sp_addserver` (current security system officer) • `sp_clearstats` • `sp_countmetadata` • `sp_dbrecovery_order` • `sp_displaylogin` • `sp_displayroles` • `sp_droplanguage` • `sp_dropserver` (current security system officer) • `sp_engine` • `sp_extengine` • `sp_helpapptrace` • `sp_metrics` • `sp_monitorconfig` • `sp_object_stats` • `sp_reportstats` • `sp_serveroption` • `sp_setlangalias` • `sp_tempdb` Executing these `dbcc` commands: • `dbcc complete_xact` • `dbcc engine` • `dbcc forget_xact` • `dbcc traceflags` Executing these functions: • `passinfo` • `valid_user`
`manage server configuration`	Enable or disable server configurations not related to security Executing these system procedures: • `sp_configure` (set security related configuration options) • `sp_jreconfig` • `sp_lmconfig`

Privilege name	Operations the privilege authorizes
`manage customer server configuration`	Enable or disable server configurations not related to security. For more information, see manage customer server configuration [page 51]. Executing these system procedures: • `sp_configure` (set security related configuration options) • `sp_displaylevel` • `sp_pciconfig` • `sp_shmdumpconfig`
`shutdown`	Shutting down the: • Server • Cluster (also requires `manage cluster` privilege) • Instance • Backup Server Execute the `shutdown` command.
`manage cache device`	Managed by `manage customer server permissions` Executing these commands: • `disk init …. type = 'inmemory'`
dbcc	
`dbcc checkalloc any database`	Executing `dbcc checkalloc` in any database
`dbcc checkcatalog any database`	Executing `dbcc checkcatalog` in any database
`dbcc checkdb any database`	Executing `dbcc checkdb` in any database
`dbcc check index any database`	Executing `dbcc checkindex` in any database
`dbcc checkstorage any database`	Executing `dbcc checkstorage` in any database
`dbcc checktable any database`	Executing `dbcc checktable` in any database
`dbcc checkverify any database`	Executing `dbcc checkverify` in any database
`dbcc fix_text any database`	Executing `dbcc fix_text` in any database
`dbcc indexalloc any database`	Executing `dbcc indexalloc` in any database
`dbcc reindex any database`	Executing `dbcc reindex` in any database
`dbcc tablealloc any database`	Executing `dbcc tablealloc` in any database
`dbcc textalloc any database`	Executing `dbcc textalloc` in any database

Privilege name	Operations the privilege authorizes
`dbcc tune`	Executing `dbcc tune`
Application Management	
`manage any execution class`	Executing these system procedures: • `sp_addengine` • `sp_addexeclass` • `sp_bindexeclass` • `sp_clearpsexe` • `sp_dropengine` • `sp_dropexeclass` • `sp_setpsexe` • `sp_unbindexeclass`
`manage any ESP`	Executing these system procedures: • `sp_addextendedproc` • `sp_dropextendedproc` • `sp_freedll` • `sp_helpextendedproc`
`manage data cache`	Managed by `manage customer server permissions` System stored procedures: • `sp_bindcache` • `sp_cacheconfig` • `sp_cachestrategy` • `sp_poolconfig` • `sp_unbindcache` • `sp_unbindcache_all` DBCC commands: • `dbcc refreshides`

Privilege name	Operations the privilege authorizes
`manage row cache`	Managed by `manage customer server permissions` TSQL commands: • `alter table (row_caching)` • `create table` – use row storage cache for row caching or snapshot isolation • `create global temporary table` – use row storage cache for row caching or snapshot isolation System stored procedure: • `sp_logiosize`
`manage dump configuration`	Managing dump configuration for a backup server Executing these commands: • `dump configuration` Executing these system procedures: • `sp_config dump` • `sp_dump history @operation = { 'purge' |'purgefiles' |'delete' | 'upgrade' | 'downgrade' | 'create_table'}`
`manage lock promotion threshold`	Executing these system procedures: • `sp_dropglockpromote` • `sp_droprowlockpromote` • `sp_setpglockpromote` • `sp_setrowlockpromote`

Privilege name	Operations the privilege authorizes
`monitor qp performance`	Managed by `manage customer server permissions` TSQL commands: • `set switch (3604, 3605)` • `set plan for plan_list` • `set option <optimizer_show_option> {value | on | off}` System stored procedures: • `sp_cmp_all_qplans` • `sp_cmp_qplans` • `sp_find_qplans` • `sp_flush_query_tuning` • `sp_flushmetrics` • `sp_flushstats` • `sp_metrics (for 'filter', 'show', 'help')` • `sp_showplan` DBCC commands: • `dbcc traceoff (3604, 3605)` • `dbcc traceon (3604, 3605)` • `dbcc nodetraceoff (3604, 3605)` • `dbcc nodetraceon (3604, 3605)`
`manage resource limit`	Executing these system procedures: • `sp_add_resource_limit` • `sp_add_time_range` • `sp_drop_resource_limit` • `sp_drop_time_range` • `sp_help_resource_limit` • `sp_modify_resource_limit` • `sp_modify_time_range`
Others	
`connect*`	Connecting to any server using the `connect` command
`kill`	Killing processes owned by the privilege holder
`kill any process`	Killing any process owned by any user
map external file	Mapping a proxy table to a directory or file on a remote server

Privilege name	Operations the privilege authorizes
`monitor server replication`	Displaying replication status Executing these system procedures: • `sp_config_rep_agent` (no configure value specified, with or without database name specified) • `sp_help_rep_agent` (with or without the database name specified)
`set proxy`	Executing `set proxy` to change the identity to another user
`set tracing*`	Managed by `manage customer server permissions` TSQL commands: • `set plan for <plan_list> on|off` • `set option <optimizer_show_option> on|off` DBCC commands: • `dbcc traceoff (3604, 3605)` • `dbcc traceon (3604, 3605)` • `dbcc nodetraceoff (3604, 3605)` • `dbcc nodetraceon (3604, 3605)`
`manage tracefile`	Managed by `manage customer server permissions` • `set tracefile (for any session)` • `set tracefile (for own session)`
`set tracing any process`	Managed by `manage customer server permissions` Executing these commands: • `set plan for <plan_list> on|off` • `set option <optimizer_show_option> on|off` Executing these dbcc commands: • `dbcc traceoff (3604, 3605)` • `dbcc traceon (3604, 3605)` • `dbcc nodetraceoff (3604, 3605)` • `dbcc nodetraceon (3604, 3605)`

Privilege name	Operations the privilege authorizes
`set switch`	Enabling or disabling any trace flag Executing these commands: • `set switch` • `show switch` Executing these `dbcc` commands: • `dbcc traceon` • `dbcc traceoff` • `dbcc nodetraceon` • `dbcc nodetraceoff` Executing this stored procedure: • `sp_dbextend 'trace'`
`show switch`	Displays trace flags that are on Execute the `show switch` command
`use any database`	Accessing any database when the privilege holder is not a valid user of the database and there is no "guest" account in the database Execute the `use database` command
`use database`	Accessing the specified database when the privilege holder is not a valid user of the database and there is no guest account in the database Execute the `use database` command

6.3.1 manage customer server configuration

Users with the `manage customer server configuration` privilege can modify the server configuration values for customer business purposes.

In the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, you need to have the `manage customer server configuration` privilege to execute `sp_configure` with the following configuration parameters:

- `abstract plan cache`
- `abstract plan dump`
- `abstract plan dynamic replace`
- `abstract plan load`
- `abstract plan replace`
- `abstract plan sharing`
- `additional network memory`

- allocate max shared memory
- allow backward scans
- allow nested triggers
- allow resource limits
- allow statement rollback
- builtin date strings
- capture compression statistics
- capture missing statistics
- cis bulk insert array size
- cis bulk insert batch size
- cis connect timeout
- cis cursor rows
- cis idle connection timeout
- cis packet size
- cis rpc handling
- column default cache size
- compression info pool size
- cost of a logical io
- cost of a physical io
- cost of a cpu unit
- deadlock checking period
- deadlock pipe active
- deadlock pipe max messages
- deadlock retries
- decompression row threshold
- default database size
- default exp_row_size percent
- default fill factor percent
- default language id
- default network packet size
- deferred name resolution
- disable character set conversions
- disable varbinary truncation
- disk i/o structures
- dtm detach timeout period
- dtm lock timeout period
- dynamic allocation on demand
- dynamic SQL plan pinning
- early row send increment
- enable async database init
- enable bulk inserts
- enable compression

- enable concurrent dump tran
- enable deferred parallel
- enable DTM
- enable functionality group
- enable HCB index
- enable housekeeper GC
- enable inline default sharing
- enable job scheduler
- enable js restart logging
- enable large chunk elc
- enable large pool for load
- enable LFB index
- enable lightweight rvm
- enable literal autoparam
- enable logins during recovery
- enable permissive unicode
- enable query tuning mem limit
- enable query tuning time limit
- enable real time messaging
- statement pipe max messages
- stream rep msg channel timeout
- enable rep agent threads
- enable resolve as owner
- enable select into in tran
- enable semantic partitioning
- enable sort-merge join and JTC
- enable sql debugger
- enable sticky statistics
- enable stmt cache monitoring
- enable streamlined parallel
- enable surrogate processing
- enable unicode conversion
- enable unicode normalization
- enable utility lvl 0 scan wait
- enable workload analyzer
- enable xact coordination
- enable xml
- engine local cache percent
- errorlog pipe active
- errorlog pipe max messages
- errorlog size
- event log computer name(windows only)

- event logging (windows only)
- extended cache size
- extend implicit conversion
- global async prefetch limit
- global cache partition number
- heap memory per user
- histogram tuning factor
- housekeeper free write percent
- identify burning set factor
- identity grab size
- identity reservation size
- inline table functions
- job scheduler interval
- job scheduler memory
- job scheduler tasks
- js heartbeat interval
- js job output width
- js restart delay
- large allocation auto tune
- LFB memory size
- lock hashtable size
- lock scheme
- lock shared memory
- lock spinlock ratio
- lock table spinlock ratio
- lock timeout pipe active
- lock timeout pipe max message
- lock wait period
- max buffers per lava operator
- max cis remote connections
- max js restart attempts
- max nesting level
- max network packet size
- max number of IN elements
- max parallel degree
- max query parallel degree
- max repartition degree
- max resource granularity
- max scan parallel degree
- max SQL text monitored
- max transfer history
- max utility parallel degree

- maximum job output
- memory alignment boundary
- memory dump compression level
- memory per worker process
- messaging memory
- metrics elap max
- metrics exec max
- metrics lio max
- metrics pio max
- min pages for parallel scan
- mnc_full_index_filter
- nonpushdown pipe active
- nonpushdown pipe max messages
- number of alarms
- number of aux scan descriptors
- number of checkpoint tasks
- number of disk tasks
- number of dtx participants
- number of dump threads
- number of histogram steps
- number of index trips
- number of locks
- number of oam trips
- number of open databases
- number of open indexes
- number of open objects
- number of open partitions
- number of pre-allocated extents
- number of reexecutions
- number of remote connections
- number of remote logins
- number of remote sites
- number of sort buffers
- number of user connections
- number of worker processes
- object lockwait timing
- open index hash spinlock ratio
- open index spinlock ratio
- open object spinlock ratio
- optimization goal
- optimize temp table resolution
- optimization timeout limit

- optimizer level
- page lock promotion HWM
- page lock promotion LWM
- page lock promotion PCT
- page utilization percent
- partition groups
- partition spinlock ratio
- pci memory size
- per object statistics active
- percent database for history
- percent database for output
- percent history free
- percent output free
- performance monitoring option
- permission cache entries
- plan text pipe active
- plan text pipe max messages
- print deadlock information
- print recovery information
- procedure cache size
- procedure deferred compilation
- process wait events
- prod-consumer overlap factor
- quoted identifier enhancements
- rapidlog buffer size
- rapidlog max files
- read committed with lock
- replication agent memory size
- row lock promotion HWM
- row lock promotion LWM
- row lock promotion PCT
- rtm thread idle wait period
- sampling percent
- scavenge temp objects
- select for update
- session tempdb log cache size
- show deferred compilation text
- size of auto identity column
- size of unilib cache
- sproc optimize timeout limit
- SQL batch capture
- sql text pipe active

- `sql text pipe max messages`
- `statement cache size`
- `statement pipe active`
- `statement statistics active`
- `streamlined dynamic SQL`
- `suppress js max task message`
- `sysstatistics flush interval`
- `text prefetch size`
- `threshold event max messages`
- `threshold event monitoring`
- `time slice`
- `transfer utility memory size`
- `update statistics hashing`
- `user log cache queue size`
- `user log cache size`
- `user log cache spinlock ratio`
- `wait event timing`
- `wait on uncommitted insert`
- `execution time monitoring`
- `enable spinlock monitoring`
- `lock timeout pipe max messages`

6.3.2 manage customer security configuration

Users with the `manage customer security configuration` privilege can modify the security-related server configuration values for customer business purposes.

In the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, you need to have the `manage customer security configuration` privilege to execute `sp_configure` with the following configuration parameters:

- `allow procedure grouping`
- `audit queue size`
- `check password for digit`
- `current audit table`
- `enable ldap user auth`
- `enable merge join`
- `enable metrics capture`
- `enable predicated privileges`
- `enable row level access (control)**`
- `external keystore`
- `log audit logon failure`

- `log audit logon success`
- `maximum failed logins`
- `minimum password length`
- `restricted decrypt permission`
- `secure default login`
- `select on syscomments.text`
- `suspend audit when device full`
- `systemwide password expiration`

6.3.3 manage internal configuration

Users with `manage internal configuration` can modify the following server configurations.

- `aggressive task stealing`
- `cpu accounting flush interval`
- `cpu grace time`
- `enable rapidlog`
- `enable rapidtimer`
- `engine memory log size`
- `i/o accounting flush interval`
- `i/o batch size`
- `max async i/os per engine`
- `max async i/os per server`
- `number of large i/o buffers`
- `number of network tasks`
- `sigstack csmd min size`
- `sigstack min size`
- `stack guard size`
- `stack size`

6.4 Database-Wide Privileges

The `manage database permissions` privilege is authorized to manage database-wide privileges except `manage database permissions`, `create encryption key`, `manage any encryption key`, and `manage master key`. Those exceptional privileges are managed by either `manage security permissions`, or `manage customer security permissions`.

The set of privileges managed by `manage database permissions` remains the same in the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service as that of on-premises SAP ASE. However, who owns this permission depends on the database.

User Database

Within all customer created databases, `manage database permissions` is managed by `manage customer security permissions` and would be implicitly granted to dbo in-box. Customer user with `manage database permissions` can manage all database wide privileges freely as per need.

`create encryption key`, `manage any encryption key`, and `manage master key` are all managed by `manage customer security permissions` within customer created databases.

System Database

Within system databases, `manage database permissions` is managed by `manage security permissions` and would be implicitly granted to dbo in-box. In addition, `saptu` would grant some proper database wide privileges on system databases to `aseadmin(via cust_sa_role)` explicitly during the provision of the SAP ASE cloud edition instance.

`create encryption key`, `manage any encryption key`, and `manage master key` are all managed by `manage security permissions` within system databases.

Database-wide privileges on system databases granted to `aseadmin` (via `cust_sa_role`):

`alter any table`

> ⓘ Note
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any default`

> ⓘ Note
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any function`

> ⓘ Note
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any index`

> ⓘ Note
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any object`

> ⓘ Note
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create any procedure` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.
`create any rule` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.
`create any table` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.
`create any trigger` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.
`create any view` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.
`dbcc checkalloc`
`dbcc checkcatalog`
`dbcc checkdb`
`dbcc checkindex`
`dbcc checkstorage`
`dbcc checktable`
`dbcc checkverify`
`dbcc fix_text`
`dbcc indexalloc`
`dbcc reindex`
`dbcc tablealloc`
`dbcc textalloc`

`delete any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any default`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any function`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any object`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any procedure`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any rule`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any trigger`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`drop any view`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`execute any function`
`execute any procedure`
`identity_insert any table`
`identity_update any table`
`insert any table` **Note** Not applicable in the `master` database.
`manage abstract plans`
`manage any statistics`
`manage any user`
`manage checkstorage`
`manage database`
`manage replication`
`references any table` **Note** Not applicable in the `master` database.
`reorg any table` **Note** Not applicable in the `master` database.
`report checkstorage`
`select any system catalog`
`select any table`
`transfer any table` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.
`truncate any table` **Note** Not applicable in the `master` database or the `sybsystemprocs` database.

`update any table`

> **Note**
>
> Not applicable in the `master` database or the `sybsystemprocs` database.

`create table`

> **Note**
>
> Not applicable in the `master` database.

`create view`

> **Note**
>
> Not applicable in the `master` database.

`create trigger`

> **Note**
>
> Not applicable in the `master` database.

`create procedure`

`create default`

> **Note**
>
> Not applicable in the `master` database.

`create rule`

> **Note**
>
> Not applicable in the `master` database.

`create function`

> **Note**
>
> Not applicable in the `master` database.

`create schema`

> **Note**
>
> Not applicable in the `master` database.

Database-wide privileges on the `sybsecurity` database granted to `aseadmin` (via `cust_sso_role`):

`manage database encryption key`

> **Note**
>
> Only in the master database.

`manage service key`

`decrypt any table`

`manage column encryption key`

`create encryption key`

`select any audit table`

> **Note**
>
> Only in the `sybsecurity` database.

`truncate any audit table`

> **Note**
>
> Only in the `sybsecurity` database.

> **Note**
>
> SAP recommends that you do not create tables, views, stored procedures, or other objects in the master database because the space in the master database is important for some operations.

7 Key Management

The SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service supports a key hierarchy by using a master key as a root key. The master key is used to encrypt other keys and can be created for each database.

There are several types of master keys:

- The master key in the master database is used to encrypt the database encryption key (DEK), the column encryption key (CEK) and the service key.
- Master keys in non-master databases are used to encrypt the CEK and the service key.
- A dual master key is owned by another user and used to encrypt keys along with the master key.

7.1 Key Management for a Master Database

In the SAP Adaptive Server Enterprise, cloud edition by IBM Cloud service, the master key in the master database is created and owned by the `saptu` login. Only `saptu` can create, alter, and drop the master key. Other users are not allowed to modify the master key.

The password of the master key follows the same password policy as that of the SAP ASE cloud edition service out-of-the-box logins. The password of the master key is stored in the landscape vault. During the SAP ASE cloud edition instance start up, the password of the master key is retrieved from the vault and supplied to the SAP ASE cloud edition instance.

The SAP ASE cloud edition service provides a new command syntax for creating a default database encryption key (DEK). This default DEK is used to encrypt the system database `sybsecurity` and user databases when the `encrypt with <dek>` clause is not specified during database creation. You are allowed to change the default DEK and hence this default DEK is owned by yourself. Only one default database encryption can exist in the SAP ASE cloud edition instance. You can also create your own DEK encrypted with the master key to encrypt your databases.

Syntax

```
create encryption key <keyname>
[as default]
[for <algorithm_name>]
for database encryption
[with
{[master key]
[keylength 256]
[init_vector random]
[[no] dual_control]}
alter encryption key <key_name>
[as [not] default]
for database encryption
```

Parameter

as [not] default

indicates whether or not the default property should be assigned to this database encryption key.

Usage

`sp_encryption helpkey` shows the key type as the `symmetric default database encryption key` for the default database encryption key.

Example

Create the default database encryption key `dek1`:

```
create encryption key dek1 as default for database encryption
```

Display the information about `dek1`:

```
sp_encryption helpkey,'dek1'
```

The returned result is:

```
Key Name Key Owner       Key Length Key Algorithm Key
Type
-------- --------------- ---------- -------------
----------------------------------------
dek1     manage_db_login 256        AES           symmetric default database
encryption key

Pad Initialization Vector Protected By Key Recovery # of Key Copies
--- --------------------- ------------ ------------ ---------------
0   1                      master key   0            0
```

Alter the existing database encryption key `dek2` as the default database encryption key.

```
alter encryption key dek2 as default for database encryption
```

8 Database Encryption

SAP Adaptive Server Enterprise, cloud edition by IBM Cloud supports the creation of encrypted databases only. SAP ASE cloud edition does not support the creation of clear-text user databases.

`sybsecurity` Database

The `sybsecurity` system database is used to store auditing information and is encrypted with the default DEK during provisioning.

User Database

You can create encrypted databases by either using your own DEK or with the default DEK.

When creating a database, use the `encrypt with <dek>` parameter to specify the DEK that is used to encrypt the database. If you don't specify this parameter when creating the database, the SAP ASE cloud edition service uses the default DEK instead.

To change the DEK of any database, decrypt the database and then encrypt it with a different DEK. However, SAP ASE cloud edition doesn't allow you to decrypt a database with the `alter database` command. Therefore, you cannot change the DEK of your database.

You can also create a database using an encrypted template database.

Other System Databases

The other system databases, except `tempdb`, are not encrypted.

The `sybmgmtdb` and `saptools` databases are also created in clear-text. Additional databases created during SAP ASE instance creation and configuration, `sysibm` and `auditarchive`, are encrypted.

9 Auditing

In SAP Adaptive Server Enterprise, cloud edition by IBM Cloud, auditing is always enabled, and it is not allowed to be turned off.

The SAP ASE cloud edition service provides configured auditing mechanism and pre-configured audit options for you. You can further configure audit option as per your business need for customer-created users, objects, databases, and so on. The SAP ASE cloud edition service provides the configuration of different audit events, which you can use to satisfy the data protection and privacy (DPP) requirement.

SAP Audit Logging Service periodically captures all the audit events of all predefined SAP logins and login events of all logins.

Default Server Configurations

The server configuration options that are already configured are listed as follows:

- Enable auditing:

  ```
  sp_configure ‘auditing’,1
  ```

  > ⓘ Note
  >
  > It is not allowed to turn this feature off.

- Set the number of records in the audit queue in memory to 300:

  ```
  sp_configure "audit queue size", 300
  ```

- Suspend the audit process if the current audit table becomes completely full. The full condition occurs only if the threshold procedure attached to the current table segment is not functioning properly:

  ```
  sp_configure "suspend audit when device full",1
  ```

- Enable the trunc log on chkpt option for the `sybsecurity` database to prevent the transaction log from becoming full:

  ```
  sp_dboption sybsecurity, "trunc log on chkpt", true
  ```

- Configure the `current audit table` parameter to use `sysaudits_01` by default:

  ```
  sp_configure "current audit table",1
  ```

Default Audit Options

It is not allowed to turn off the default audit options listed below:

- `sp_audit ‘all’,’sa’,’all’,’on’`
- `sp_audit ‘all’,’saptu’,’all’,’on’`
- `sp_audit ‘all’,’sapsupport’,’all’,’on’`
- `sp_audit ‘all’,’sappr’,’all’,’on’`
- `sp_audit ‘all’,’sapping’,’all’,’on’`
- `sp_audit ‘all’,’sapexporter’,’all’,’on’`
- `sp_audit ‘all’,’sapaudlog’,’all’,’on’`
- `sp_audit ‘truncate’,’all’,’sybsecurity’,’on’`
- `sp_audit ‘login’,’all’,’all’,’on’`

Audit Table Mechanism

There are three audit tables created by default after provisioning. The thresholds are created for each audit table. The default threshold is triggered when the audit table is 75% full. When the threshold procedure is triggered, it does the truncation for the next table and switches to use it. You can modify the threshold according to your own requirement.

The default threshold procedure does not back up the audit records, you need to rewrite this procedure and back up your data before the truncation happens. The currently configured threshold procedure is `aseadmin.sp_audit_thresh`. Follow the example below to update this procedure and back up your audit records from the audit table in `sybsecurity` database into another user database, such as the `audit_data` table in the `sybsecurityarch` database.

1. Create a database to archive the audit records:

```
create database sybsecurityarch
go
exec sp_dboption 'sybsecurityarch','select into/bulkcopy',true
go
```

2. Create the threshold procedure to copy audit records from `sybsecurity..sysaudits_01` to the user database. A similar threshold procedure can be created for each audit table.

```
use sybsecurity
go
create or replace proc aseadmin.sp_audit_thresh01
@dbname varchar(30),
@segname varchar(30),
@space int,
@status int
as
begin
        print "Background: threshold crossed %1! db, %2! segment, %3! space",
@dbname, @segname, @space
        --switch to the next audit table.
        exec sp_configure "current audit table", 0,"with truncate"
        --Copy the audit records from previous table to user database
        if not exists (select name from sybsecurityarch..sysobjects where
name="audit_data")
                select * into sybsecurityarch.dbo.audit_data from
sybsecurity..sysaudits_01
        else
                insert into sybsecurityarch.dbo.audit_data select * from
sybsecurity..sysaudits_01
end
```

```
go
```

3. Check the existing threshold value that is set for `sybsecurity..sysaudits_01`. This value is used to update the threshold. For example:

   ```
   sp_helpthreshold aud_seg_01
   go
   ```

   The returned result is:

   ```
   segment name   free pages   last chance    threshold procedure
   -------------- ------------ -------------- --------------------
   aud_seg_01     47616        0              aseadmin.sp_audit_thresh
   ```

   In this example, the threshold value is 47616.
   The thresholds defined for other audit tables can be checked in a similar way.
4. Update the threshold to use the procedure associated with `sybsecurity..sysaudits_01`. Similarly, the thresholds set for other audit tables can be updated accordingly. For example:

   ```
   sp_modifythreshold sybsecurity, aud_seg_01, 47616,
   ‘aseadmin.sp_audit_thresh01’
   go
   ```

> ### Note
>
> To add a system audit table, you must indicate the device name of the audit table by executing `sp_addaudittable <devname>`, the value "default" is not allowed to be used. See sp_addaudittable for more details.

10 Data Protection and Privacy

SAP Adaptive Server Enterprise, cloud edition by IBM Cloud provides the technical enablement and infrastructure to allow you to run applications on SAP ASE cloud edition instances to conform to the legal requirements of data protection in the different scenarios in which SAP ASE cloud edition service is used.

Un-encrypted system databases (including master database) contain customer logins or user names that are not encrypted.

Operation logs such as error logs are not encrypted and may contain customer information like login names.

For more details about data protection in SAP ASE cloud edition, see Data Protection in SAP ASE.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap