Vidisolve

Seen it. Solved it.

Application Auditing Made Easy

Simon L. Prinsloo

simon@vidisolve.com

PUG CHALLENGE EXCHANGE AMERICAS

Introduction

Simon Prinsloo

Vidisolve in Pretoria

Working with Progress since v.7 in 1996

Worked on various commercial systems

Mostly focused on CASE tools and implementing new functionality in legacy projects

Agenda

Why Auditing?

About this case study

Preparation for auditing

Deployment of auditing

Audit context

AUDIT-CONTROL System Handle

Reporting

Examples

PUG CHALLENGE EXCHANGE AMERICAS

Why Auditing?

- Business requirements
- Legal requirements

About this case study

- Replace traditional auditing
- Replace traditional record history tracking
- Enhance visibility with context

PUG CHALLENGE EXCHANGE AMERICAS

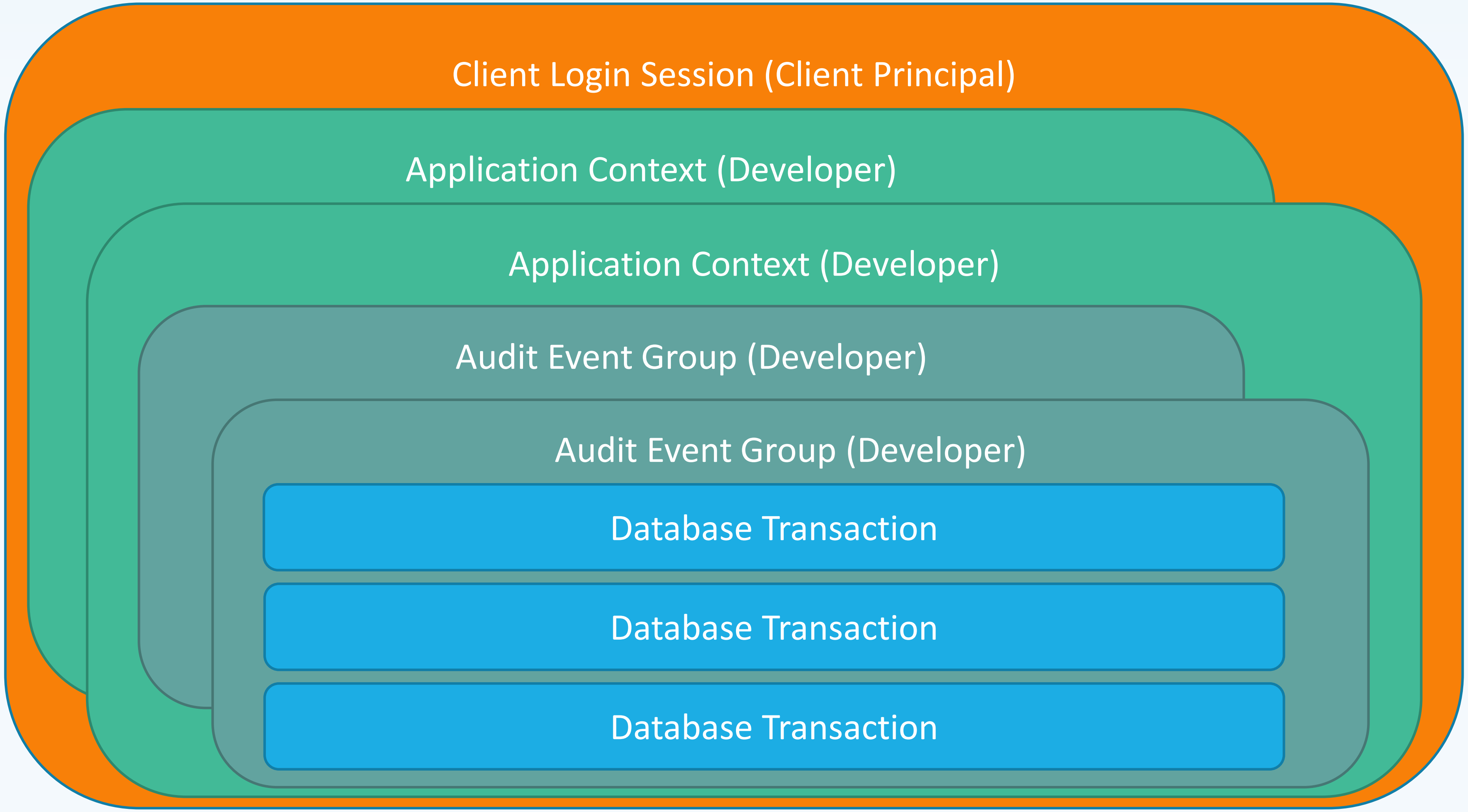
Preparation for auditing

1. Implement user authentication
   - Preferably using CLIENT-PRINCIPAL
2. Add audit areas to database(s)
3. Enable auditing with proutil
   - Offline ☹
4. Set up audit security
5. Setup audit policies
6. Add audit context and events (Optional)
7. Create audit reports

Deployment of auditing

1. Add audit areas to database(s)
2. Enable auditing with proutil
   - Offline ☹
3. Set database identification
4. Set up audit security
5. Import audit policies
6. Periodically archive audit data

Audit Context



Client Login Session (Client Principal)

Application Context (Developer)

Application Context (Developer)

Audit Event Group (Developer)

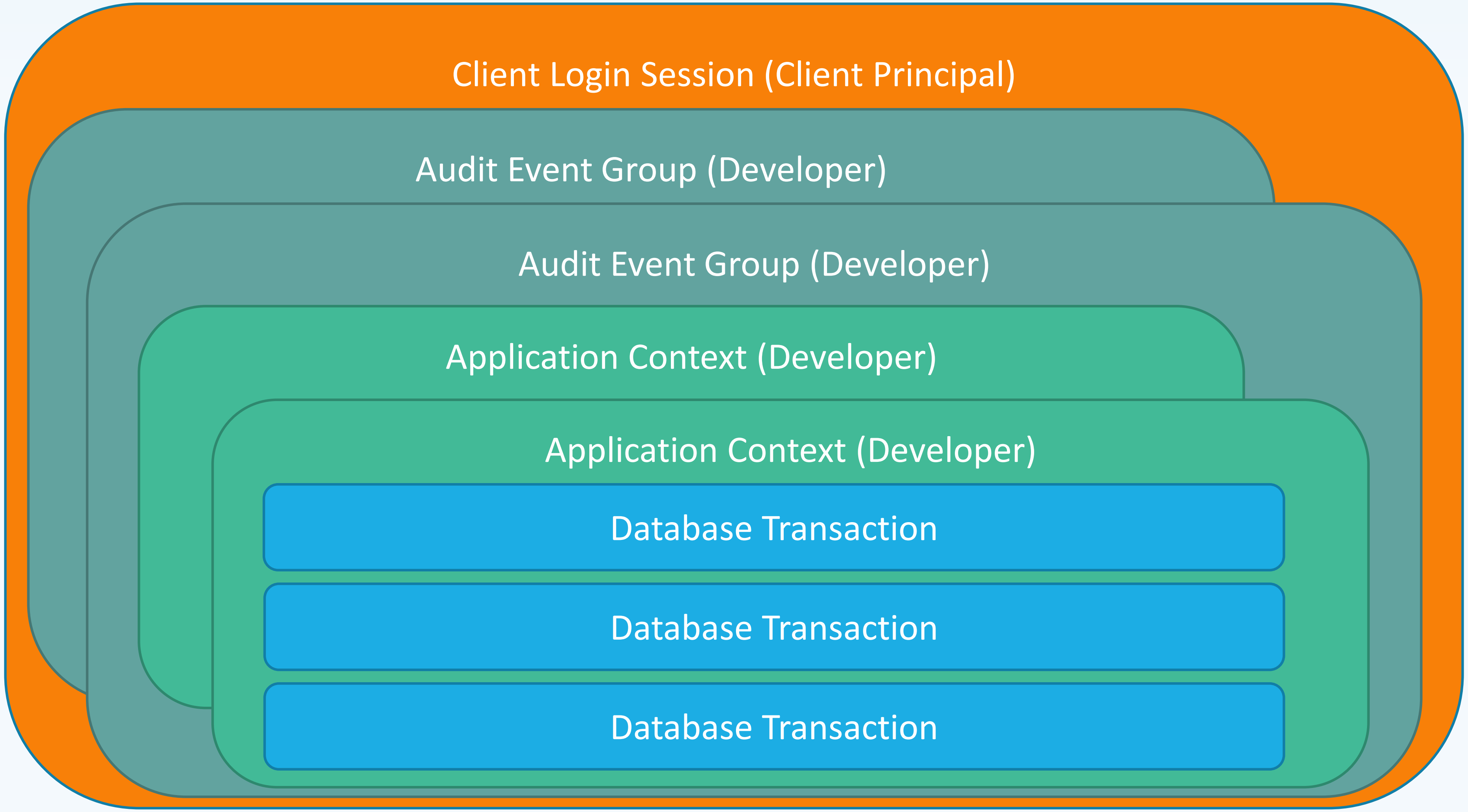
Audit Event Group (Developer)

Database Transaction

Database Transaction

Database Transaction

Audit Context



Client Login Session (Client Principal)
Audit Event Group (Developer)
Audit Event Group (Developer)
Application Context (Developer)
Application Context (Developer)
Database Transaction
Database Transaction
Database Transaction

AUDIT-CONTROL system handle

METHODS

- SET-APPL-CONTEXT( )
- CLEAR-APPL-CONTEXT( )

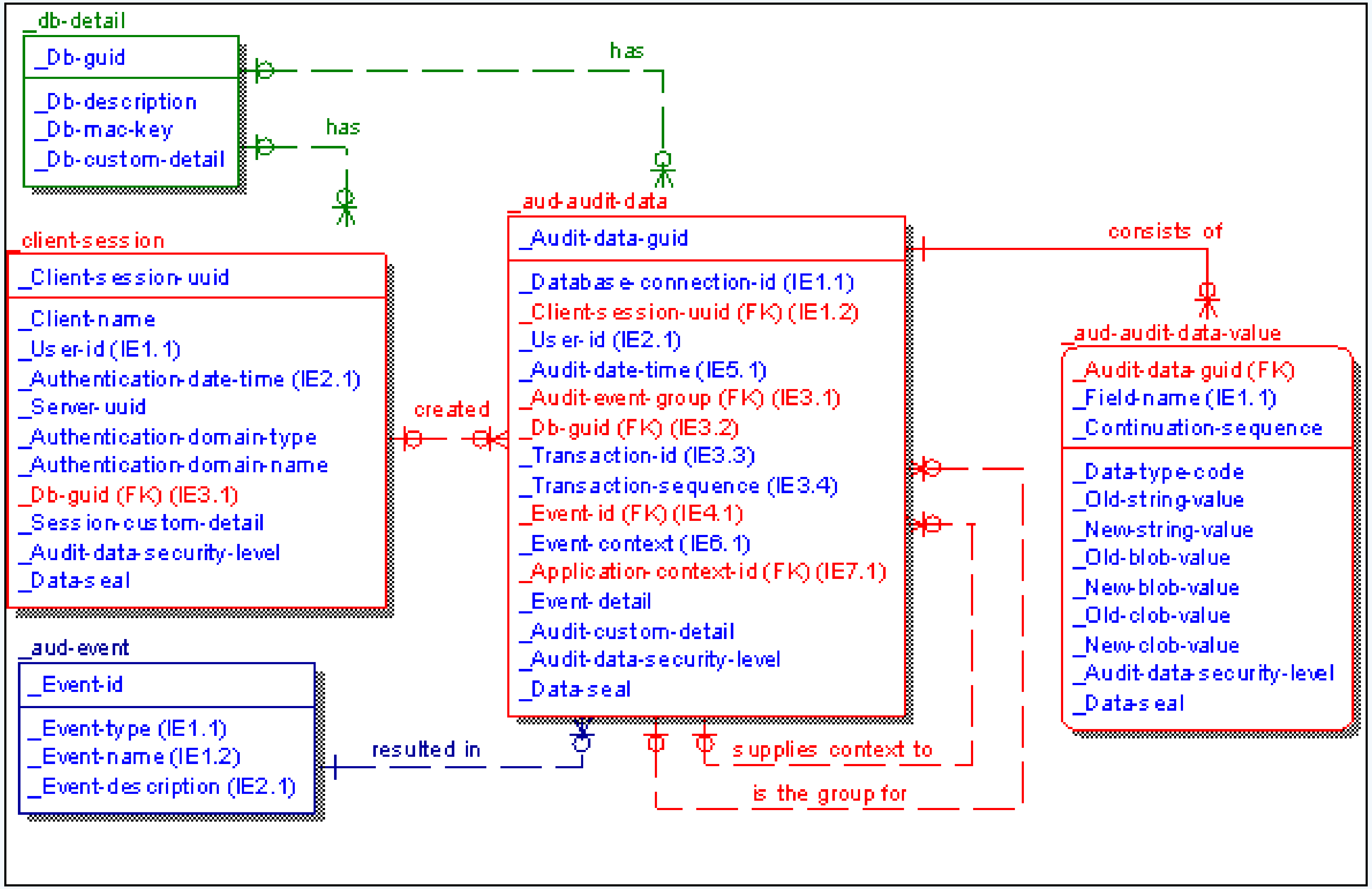
- BEGIN-EVENT-GROUP( )
- END-EVENT-GROUP( )

- LOG-AUDIT-EVENT( )

PROPERTIES

- APPL-CONTEXT-ID
- EVENT-GROUP-ID

Reporting



_db-detail
- _Db-guid
- _Db-description
- _Db-mac-key
- _Db-custom-detail

client-session
- _Client-session-uuid
- _Client-name
- _User-id (IE1.1)
- _Authentication-date-time (IE2.1)
- _Server-uuid
- _Authentication-domain-type
- _Authentication-domain-name
- _Db-guid (FK) (IE3.1)
- _Session-custom-detail
- _Audit-data-security-level
- _Data-seal

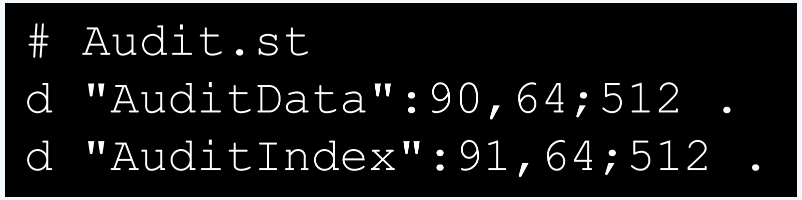
_aud-event
- _Event-id
- _Event-type (IE1.1)
- _Event-name (IE1.2)
- _Event-description (IE2.1)

_aud-audit-data
- _Audit-data-guid
- _Database-connection-id (IE1.1)
- _Client-session-uuid (FK) (IE1.2)
- _User-id (IE2.1)
- _Audit-date-time (IE5.1)
- _Audit-event-group (FK) (IE3.1)
- _Db-guid (FK) (IE3.2)
- _Transaction-id (IE3.3)
- _Transaction-sequence (IE3.4)
- _Event-id (FK) (IE4.1)
- _Event-context (IE6.1)
- _Application-context-id (FK) (IE7.1)
- _Event-detail
- _Audit-custom-detail
- _Audit-data-security-level
- _Data-seal

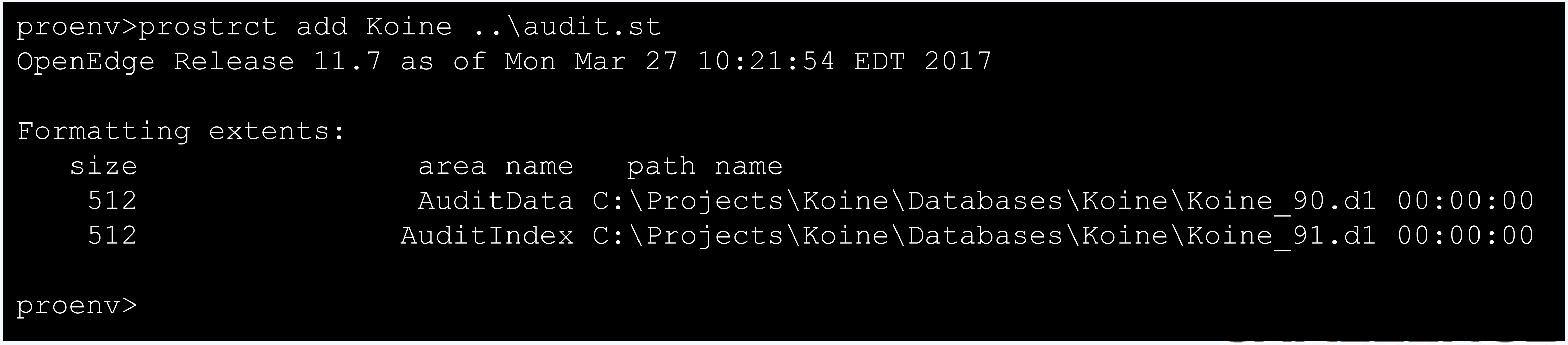
_aud-audit-data-value
- _Audit-data-guid (FK)
- _Field-name (IE1.1)
- _Continuation-sequence
- _Data-type-code
- _Old-string-value
- _New-string-value
- _Old-blob-value
- _New-blob-value
- _Old-clob-value
- _New-clob-value
- _Audit-data-security-level
- _Data-seal

Examples

1. Add audit areas to database(s)



```
# Audit.st
d "AuditData":90,64;512 .
d "AuditIndex":91,64;512 .
```



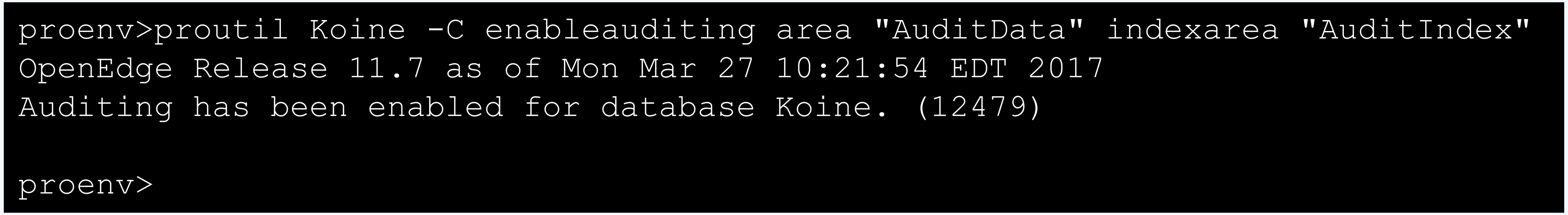
```
proenv>prostrct add Koine ..\audit.st
OpenEdge Release 11.7 as of Mon Mar 27 10:21:54 EDT 2017

Formatting extents:
   size                area name   path name
    512                AuditData C:\Projects\Koine\Databases\Koine\Koine_90.d1 00:00:00
    512               AuditIndex C:\Projects\Koine\Databases\Koine\Koine_91.d1 00:00:00

proenv>
```

Examples

2. Enable auditing with proutil

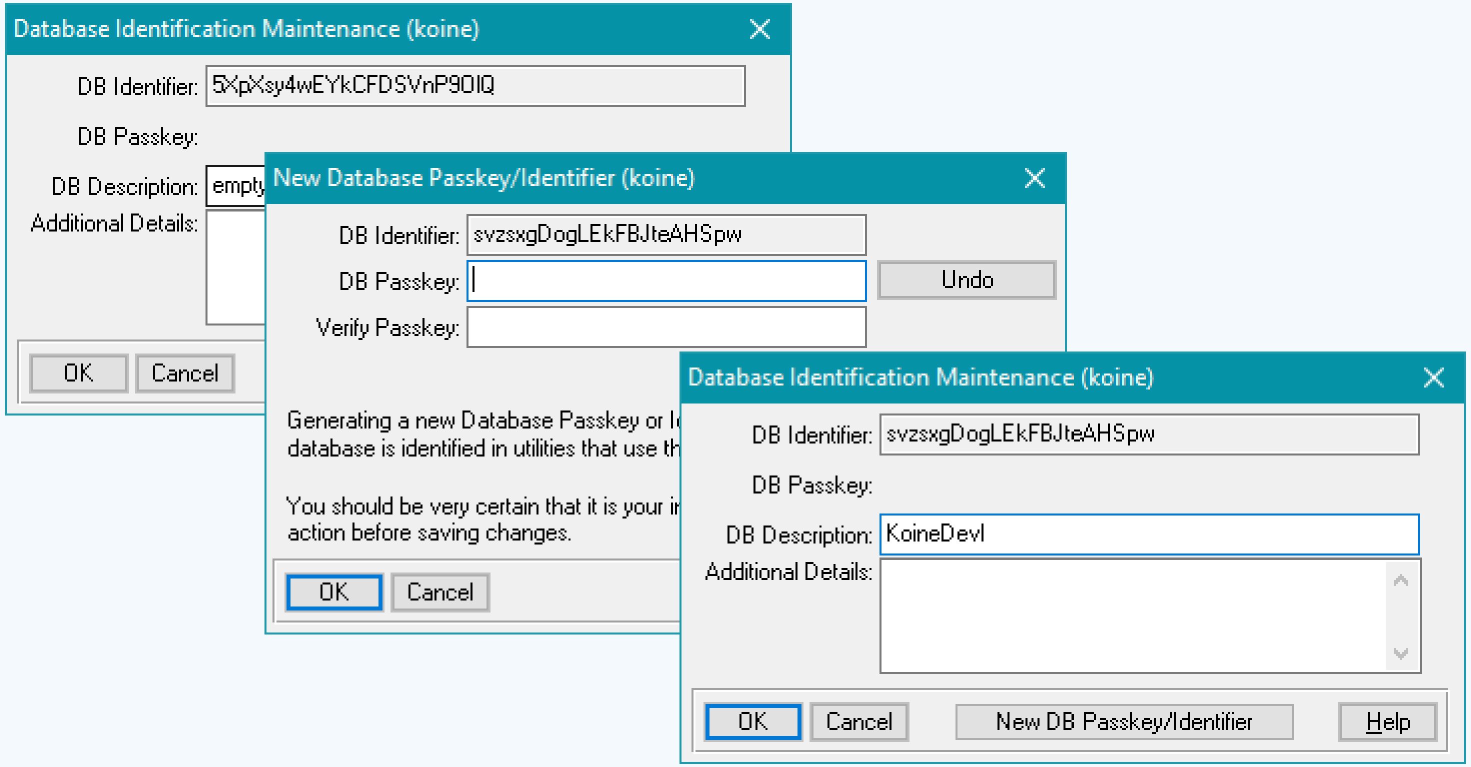


```
proenv>proutil Koine -C enableauditing area "AuditData" indexarea "AuditIndex"
OpenEdge Release 11.7 as of Mon Mar 27 10:21:54 EDT 2017
Auditing has been enabled for database Koine. (12479)

proenv>
```

Examples

3. Setup database identification



Database Identification Maintenance (koine)

DB Identifier: 5XpXsy4wEYkCFDSVnP9OIQ

DB Passkey:

DB Description: empty

Additional Details:

New Database Passkey/Identifier (koine)

DB Identifier: svzsxgDogLEkFBJteAHSpw

DB Passkey:

Verify Passkey:

Generating a new Database Passkey or I
database is identified in utilities that use th

You should be very certain that it is your i
action before saving changes.

Database Identification Maintenance (koine)

DB Identifier: svzsxgDogLEkFBJteAHSpw

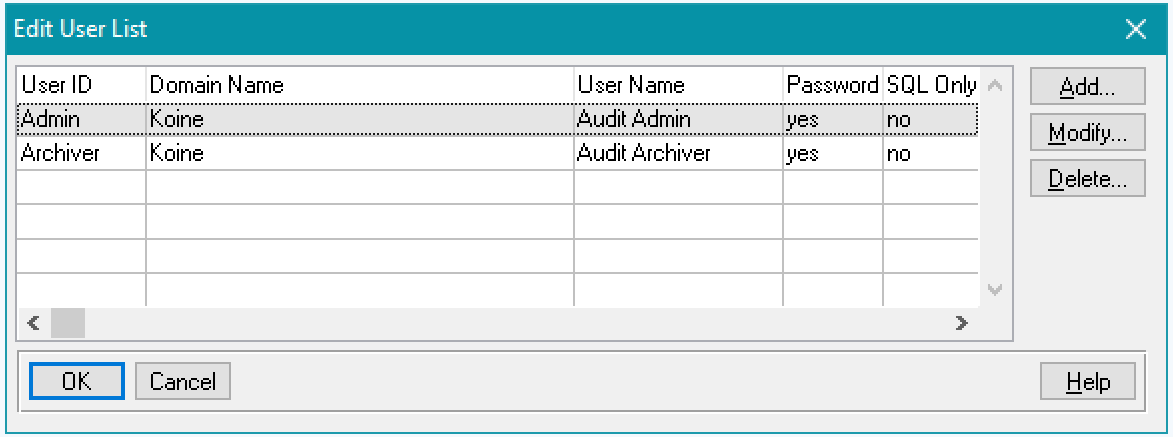
DB Passkey:

DB Description: KoineDevl

Additional Details:

Examples

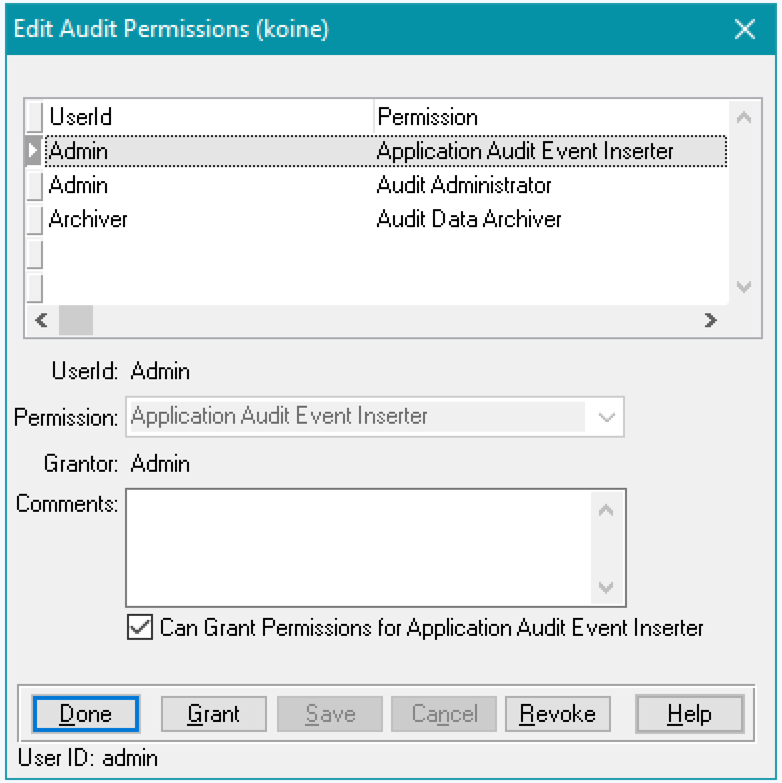
4. Setup audit security



User ID	Domain Name	User Name	Password	SQL Only
Admin	Koine	Audit Admin	yes	no
Archiver	Koine	Audit Archiver	yes	no

Examples

4. Setup audit security



Edit Audit Permissions (koine)

UserId	Permission
Admin	Application Audit Event Inserter
Admin	Audit Administrator
Archiver	Audit Data Archiver

UserId: Admin

Permission: Application Audit Event Inserter

Grantor: Admin

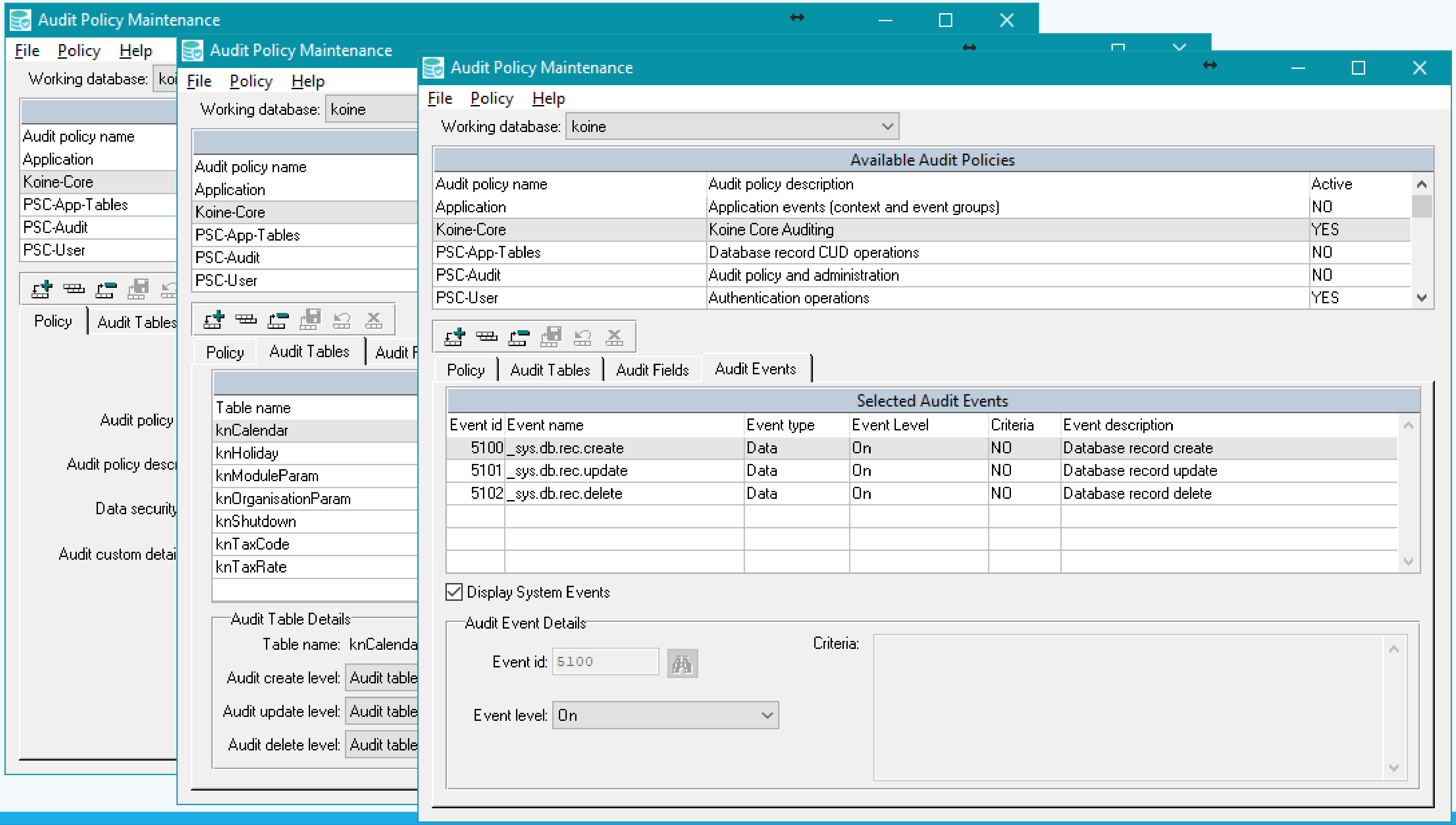
Comments:

☑ Can Grant Permissions for Application Audit Event Inserter

User ID: admin

Examples

5. Setup audit policies



Working database: koine

Table name: knCalenda

Audit create level: Audit table

Audit update level: Audit table

Audit delete level: Audit table

Table name
knCalendar
knHoliday
knModuleParam
knOrganisationParam
knShutdown
knTaxCode
knTaxRate

Available Audit Policies

Audit policy name	Audit policy description	Active
Application	Application events (context and event groups)	NO
Koine-Core	Koine Core Auditing	YES
PSC-App-Tables	Database record CUD operations	NO
PSC-Audit	Audit policy and administration	NO
PSC-User	Authentication operations	YES

Selected Audit Events

Event id	Event name	Event type	Event Level	Criteria	Event description
5100	_sys.db.rec.create	Data	On	NO	Database record create
5101	_sys.db.rec.update	Data	On	NO	Database record update
5102	_sys.db.rec.delete	Data	On	NO	Database record delete

☑ Display System Events

Audit Event Details

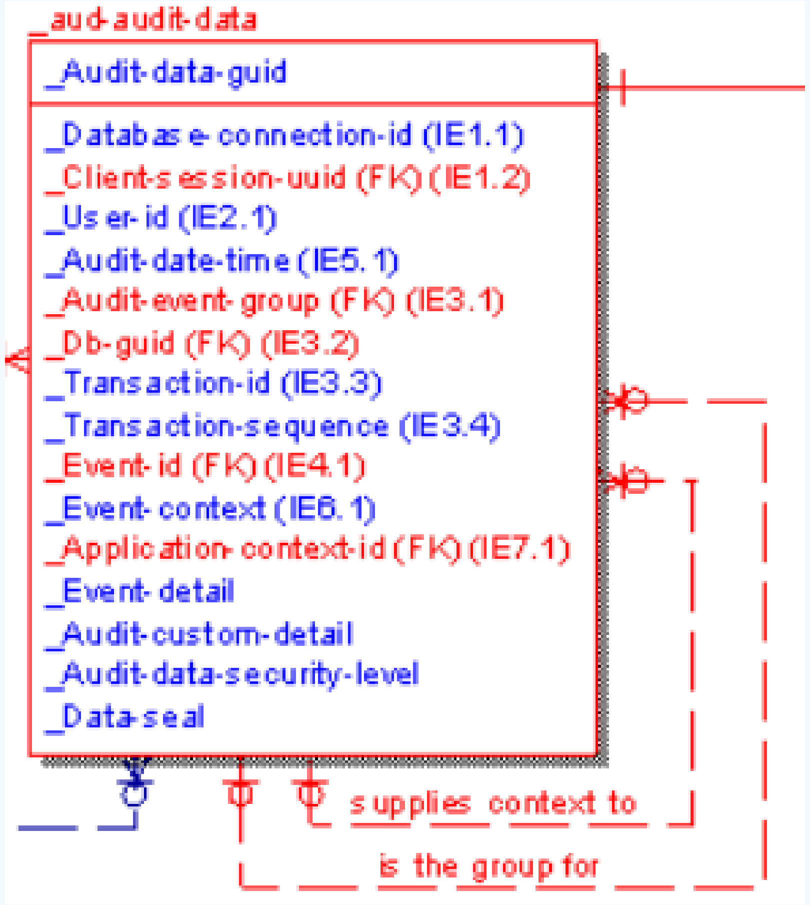
Event id: 5100

Criteria:

Event level: On

PUG CHALLENGE EXCHANGE AMERICAS

Reporting on audit data



_aud-audit-data

_Audit-data-guid

_Database-connection-id (IE1.1)
_Client-session-uuid (FK) (IE1.2)
_User-id (IE2.1)
_Audit-date-time (IE5.1)
_Audit-event-group (FK) (IE3.1)
_Db-guid (FK) (IE3.2)
_Transaction-id (IE3.3)
_Transaction-sequence (IE3.4)
_Event-id (FK) (IE4.1)
_Event-context (IE6.1)
_Application-context-id (FK) (IE7.1)
_Event-detail
_Audit-custom-detail
_Audit-data-security-level
_Data-seal

Separators used in the data

```
DEFINE PUBLIC STATIC PROPERTY Field  AS CHARACTER NO-UNDO INIT "~006" GET.
DEFINE PUBLIC STATIC PROPERTY Record AS CHARACTER NO-UNDO INIT "~007" GET.
DEFINE PUBLIC STATIC PROPERTY Array  AS CHARACTER NO-UNDO INIT "~010" GET.
```

Remember the code works in octal, watch out for CHR(8)!

Some code

Questions?

PUG
CHALLENGE
EXCHANGE
AMERICAS

Feedback welcome

Simon Prinsloo

simon@vidisolve.com