Auditing DB Oracle PARER - RACP

Rev. 2.0 14/05/2018

Redatto	Verificato	Approvato
Data: 14/05/2018	Data: 14/05/2018	Data: 14/05/2018
Firma: Giovanni Pacifico	Firma: Sandra Spadoni	Firma: Alessandro Landi
Classificazione del documento:	Interno	

parer
POLO ARCHIVISTICO REGIONALE DELL'EMILIA ROMAGNA

RegioneEmilia-Romagna

D·HUB
ENGINEERING

Sommario

Scopo del documento

Lo scopo del presente documento è quello di illustrare le politiche di auditing definite per il database RACP del PARER e dettagliare l'implementazione pratica di dette politiche.

Requisiti generali di auditing per il DB del PARER

L'auditing riveste carattere di particolare importanza per il DB di PARER. La missione di conservazione documentale impone infatti, sia per la tipologia di dati contenuti nella base dati, sia per le modalità di gestione dei dati stessi, cautele del tutto particolari.

I requisiti di auditing sono dunque espressi dalle seguenti esigenze:

1) Impostare l'auditing seguendo le ***best practices*** di sicurezza comunemente riconosciute a livello internazionale
2) Ottemperare alle disposizioni del **Garante per la protezione dei dati personali** per quanto concerne le misure e gli accorgimenti relativamente alle attribuzioni delle funzioni di amministratore di sistema
3) Ottemperare alla Determinazione della **Regione Emilia Romagna** che va sotto il nome di "DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA DELLA GIUNTA E DELL'ASSEMBLEA LEGISLATIVA DELLA REGIONE EMILIA-ROMAGNA".
4) Recepire le peculiari esigenze di **PARER** in tema di audit.

Non è il caso di soffermarsi su punti 1) – 3), in considerazione del fatto che sono oramai recepiti per prassi nelle configurazioni dei sistemi della Regione Emilia Romagna effettuate dal SIIR (Sistema Informativo Informatico Regionale) e per approfondimenti si rimanda alla documentazione relativa citata al termine del presente documento. In relazione al punto 4) la peculiare esigenza del PARER può essere espressa in modo semplice nel seguente modo: avere traccia col maggior dettaglio possibile di qualunque operazione effettuata sugli schemi Oracle di pertinenza PARER da parte di qualsivoglia utente che non acceda mediante le applicazioni autorizzate e dotate di funzionalità applicativa di audit.

Implementazione dell'audit DB

Considerazioni generali e configurazione di sistema

Si è ritenuto opportuno optare per la configurazione di Orcale 12c che consenta di beneficiare del cosiddetto ***unified audit trail***. Non è il caso di dilungarsi sui vantaggi che ne derivano: per ulteriori approfondimenti si rimanda ai documenti di riferimento citati. Ci si limita ad evidenziare cha la specifica feature dell'***audit condizionale*** permette di implementare le policy di precipuo interesse PARER in modo efficiente e con relativa semplicità.

L'attivazione dello unified audit trail è stata effettuata seguendo le indicazioni del documento ***Orcale: How To Enable The New Unified Auditing In 12c? (Doc ID 1567006.1)***.

In fase di cancellazione dei record di audit già acquisiti dal SIEM ci si è imbattuti nel ***Bug 18743542 : 12C UNIFIED AUDIT TRAIL, CANNOT DELETE LAST_ARCHIVE_TIME***, ciò ha comportato la necessità di installare: ***Oracle Database 12c Release 12.1.0.2.0 Patch for Bug# 18743542 for Linux-x86-64***.

Policy Oracle predefinite

Tutte le policy predefinite da Oracle e raccomandate dalle best practices sono state attivate. A tal proposito è opportuno precisare che questo non produce un significativo overhead dovuto ad overlap delle policy stesse. Il meccanismo implementato dallo unified audit trail è infatti ottimizzato sotto questo profilo: se più policy attive richiedono che una certa informazione venga registrata non si generano duplicazioni: semplicemente il record di header dell'audit conterrà indicazione di tutte le policy a cui il record fa riferimento. Inoltre i record di dettaglio relativi ad unico evento di audit e facenti capo al medesimo record di header sono poi privi dell'informazione *unified_audit_policies*: la sua presenza avrebbe comportato un'ingiustificata occupazione di spazio.

Di seguito si riporta il dettaglio delle operazioni tracciate dalle policy predefinite.

ORA_ACCOUNT_MGMT

```
CREATE AUDIT POLICY ORA_ACCOUNT_MGMT
 ACTIONS CREATE USER, ALTER USER, DROP USER, CREATE ROLE, DROP ROLE,
  ALTER ROLE, SET ROLE, GRANT, REVOKE;
```

Policy predefinita di unified audit: ORA_ACCOUNT_MGMT

ORA_CIS_RECOMMENDATIONS

```
CREATE AUDIT POLICY ORA_CIS_RECOMMENDATIONS
 PRIVILEGES SELECT ANY DICTIONARY, CREATE ANY LIBRARY,
            DROP ANY LIBRARY, CREATE ANY TRIGGER,
            ALTER ANY TRIGGER, DROP ANY TRIGGER,
            ALTER SYSTEM
 ACTIONS CREATE USER, ALTER USER, DROP USER,
            CREATE ROLE, DROP ROLE, ALTER ROLE,
            GRANT, REVOKE, CREATE DATABASE LINK,
            ALTER DATABASE LINK, DROP DATABASE LINK,
            CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
            CREATE SYNONYM, DROP SYNONYM,
            CREATE PROCEDURE, DROP PROCEDURE, ALTER PROCEDURE;
```

Policy predefinita di unified audit: ORA_CIS_RECOMMENDATIONS

ORA_DATABASE_PARAMETER

```
CREATE AUDIT POLICY ORA_DATABASE_PARAMETER
 ACTIONS ALTER DATABASE, ALTER SYSTEM, CREATE SPFILE;
```

Policy predefinita di unified audit: ORA_DATABASE_PARAMETER

ORA_LOGON_FAILURES

```
CREATE AUDIT POLICY ORA_LOGON_FAILURES ACTIONS LOGON;
```

Policy predefinita di unified audit: ORA_LOGON_FAILURES

ORA_SECURECONFIG

```
CREATE AUDIT POLICY ORA_SECURECONFIG
 PRIVILEGES ALTER ANY TABLE, CREATE ANY TABLE, DROP ANY TABLE,
            CREATE ANY PROCEDURE, DROP ANY PROCEDURE, ALTER ANY PROCEDURE,
            GRANT ANY PRIVILEGE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE,
            AUDIT SYSTEM, CREATE EXTERNAL JOB, CREATE ANY JOB,
            CREATE ANY LIBRARY,
            EXEMPT ACCESS POLICY,
            CREATE USER, DROP USER,
            ALTER DATABASE, ALTER SYSTEM,
            CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
            CREATE SQL TRANSLATION PROFILE, CREATE ANY SQL TRANSLATION PROFILE,
            DROP ANY SQL TRANSLATION PROFILE, ALTER ANY SQL TRANSLATION PROFILE,
            TRANSLATE ANY SQL,
            EXEMPT REDACTION POLICY,
            PURGE DBA_RECYCLEBIN, LOGMINING,
            ADMINISTER KEY MANAGEMENT
 ACTIONS    ALTER USER, CREATE ROLE, ALTER ROLE, DROP ROLE,
            SET ROLE, CREATE PROFILE, ALTER PROFILE,
            DROP PROFILE, CREATE DATABASE LINK,
            ALTER DATABASE LINK, DROP DATABASE LINK,
            CREATE DIRECTORY, DROP DIRECTORY,
            CREATE PLUGGABLE DATABASE,
            DROP PLUGGABLE DATABASE,
            ALTER PLUGGABLE DATABASE,
            EXECUTE ON DBMS_RLS;
```

Policy predefinita di unified audit: ORA_SECURECONFIG

Policy aggiuntive relative ai logon, logoff e datapump

Le numerose azioni coperte dalle policy elencate non comprendono un caso particolarmente rilevante ai fini del rispetto delle indicazioni del Disciplinare RER: le semplici operazioni di ***logon*** e ***logoff***. Le operazioni di ***datapump*** effettuate a qualunque titolo sono inoltre da tracciare in accordo con le esigenze espresse da PARER.

Due policy aggiuntive sono state all'uopo predisposte:

```
CREATE AUDIT POLICY AP_BASIC ACTIONS LOGON, LOGOFF;
```

```
CREATE AUDIT POLICY AP_DATAPUMP_ALL
ACTIONS COMPONENT = DATAPUMP ALL;
```

Auditing di tutte le operazione eseguite sugli oggetti degli schemi SACER*

Policy di auditing relative agli oggetti degli schemi SACER*

Per rispondere alle esigenze relative al punto 4) dell'elenco della sezione "Requisiti generali di auditing per il DB del PARER" si è fatto ricorso ad una nuova feature dell'auditing di Oracle 12c: quella delle ***conditional policy***. La richiesta infatti è quella di avere contezza di qualsivoglia azione (comprese le "semplici" letture) effettuate sugli oggetti degli schemi Oracle di PARER da parte di tutti gli utenti, senza alcuna eccezione per le utenze amministrative. L'unica esclusione riguarda le sessioni aventi per *username* uno degli schemi applicativi di PARER, come *hostname* di origine della sessione uno degli application server censiti e come *os username* l'utente **jboss**, che è l'utenza di sistema nel cui contesto girano le applicazioni Jboss. In sostanza si escludo dall'audit tutte le operazioni effettuate dalle applicazioni.

L'eccezione si motiva sulla base di due considerazioni:

1) Esiste un auditing applicativo che serve a tracciare le operazioni utente ritenute critiche/meritevoli di attenzione
2) Il tracciamento di tutte le operazioni tout court comporterebbe un dispendio di risorse notevolissimo e determinerebbe impatti non banali sulle prestazioni dell'intero sistema.

Esistono oggetti appartenenti ad uno schema applicativo che sono utilizzati da utenti proprietari di altri schemi. A tal proposito è necessario individuare le interazioni cross-schema per poter implementare delle politiche di audit congruenti. Sono di seguito riportate la query utilizzata per determinare le dipendenze e l'elenco di dipendenze risultante con aggregazione per tipologia di privilegio.

Elenco degli schemi di PARER e grant cross-schema Elenco degli schemi di PARER

SACER
SACER_IAM
SACER_KETTLE
SACER_LOG
SACER_PING
SACER_RIC
SACER_TPI
SACER_TPI_TIMERS
SACER_VERSO

```
select OWNER, GRANTEE, PRIVILEGE, COUNT (*) from DBA_TAB_PRIVS
where OWNER IN
(
'SACER',
'SACER_IAM',
'SACER_KETTLE',
'SACER_LOG',
'SACER_PING',
'SACER_RIC',
'SACER_TPI',
'SACER_TPI_TIMERS',
'SACER_VERSO'
)
AND GRANTEE IN
(
'SACER',
'SACER_IAM',
'SACER_KETTLE',
'SACER_LOG',
'SACER_PING',
'SACER_RIC',
'SACER_TPI',
'SACER_TPI_TIMERS',
'SACER_VERSO'
)
GROUP BY OWNER, GRANTEE, PRIVILEGE
ORDER BY OWNER, GRANTEE, PRIVILEGE;
```

OWNER	GRANTEE	PRIVILEGE	COUNT(*)
SACER	SACER_IAM	DELETE	1
SACER	SACER_IAM	REFERENCES	2
SACER	SACER_IAM	SELECT	14
SACER	SACER_PING	SELECT	5
SACER	SACER_RIC	REFERENCES	5
SACER	SACER_RIC	SELECT	25
SACER	SACER_VERSO	SELECT	24
SACER_IAM	SACER	DELETE	1
SACER_IAM	SACER	EXECUTE	3
SACER_IAM	SACER	INSERT	1
SACER_IAM	SACER	REFERENCES	3
SACER_IAM	SACER	SELECT	57
SACER_IAM	SACER	UPDATE	2
SACER_IAM	SACER_LOG	REFERENCES	5
SACER_IAM	SACER_LOG	SELECT	9
SACER_IAM	SACER_PING	EXECUTE	3
SACER_IAM	SACER_PING	REFERENCES	1
SACER_IAM	SACER_PING	SELECT	22
SACER_IAM	SACER_RIC	SELECT	2
SACER_IAM	SACER_VERSO	SELECT	3
SACER_LOG	SACER	ALTER	8
SACER_LOG	SACER	DEBUG	8
SACER_LOG	SACER	DELETE	8
SACER_LOG	SACER	EXECUTE	9
SACER_LOG	SACER	FLASHBACK	8
SACER_LOG	SACER	INDEX	8
SACER_LOG	SACER	INSERT	8
SACER_LOG	SACER	ON COMMIT REFRESH	8
SACER_LOG	SACER	QUERY REWRITE	8
SACER_LOG	SACER	READ	8
SACER_LOG	SACER	REFERENCES	8
SACER_LOG	SACER	SELECT	28
SACER_LOG	SACER	UPDATE	8
SACER_LOG	SACER_IAM	ALTER	10
SACER_LOG	SACER_IAM	DEBUG	10
SACER_LOG	SACER_IAM	DELETE	10
SACER_LOG	SACER_IAM	EXECUTE	9
SACER_LOG	SACER_IAM	FLASHBACK	10
SACER_LOG	SACER_IAM	INDEX	10

SACER_LOG	SACER_IAM	INSERT	10
SACER_LOG	SACER_IAM	ON COMMIT REFRESH	10
SACER_LOG	SACER_IAM	QUERY REWRITE	10
SACER_LOG	SACER_IAM	READ	10
SACER_LOG	SACER_IAM	REFERENCES	10
SACER_LOG	SACER_IAM	SELECT	32
SACER_LOG	SACER_IAM	UPDATE	10
SACER_LOG	SACER_PING	ALTER	8
SACER_LOG	SACER_PING	DEBUG	8
SACER_LOG	SACER_PING	DELETE	8
SACER_LOG	SACER_PING	EXECUTE	8
SACER_LOG	SACER_PING	FLASHBACK	8
SACER_LOG	SACER_PING	INDEX	8
SACER_LOG	SACER_PING	INSERT	8
SACER_LOG	SACER_PING	ON COMMIT REFRESH	8
SACER_LOG	SACER_PING	QUERY REWRITE	8
SACER_LOG	SACER_PING	READ	8
SACER_LOG	SACER_PING	REFERENCES	8
SACER_LOG	SACER_PING	SELECT	28
SACER_LOG	SACER_PING	UPDATE	8
SACER_LOG	SACER_RIC	ALTER	2
SACER_LOG	SACER_RIC	DEBUG	2
SACER_LOG	SACER_RIC	DELETE	2
SACER_LOG	SACER_RIC	FLASHBACK	2
SACER_LOG	SACER_RIC	INDEX	2
SACER_LOG	SACER_RIC	INSERT	2
SACER_LOG	SACER_RIC	ON COMMIT REFRESH	2
SACER_LOG	SACER_RIC	QUERY REWRITE	2
SACER_LOG	SACER_RIC	READ	2
SACER_LOG	SACER_RIC	REFERENCES	2
SACER_LOG	SACER_RIC	SELECT	5
SACER_LOG	SACER_RIC	UPDATE	2
SACER_LOG	SACER_VERSO	ALTER	1
SACER_LOG	SACER_VERSO	DEBUG	1
SACER_LOG	SACER_VERSO	DELETE	1
SACER_LOG	SACER_VERSO	FLASHBACK	1
SACER_LOG	SACER_VERSO	INDEX	1
SACER_LOG	SACER_VERSO	INSERT	1
SACER_LOG	SACER_VERSO	ON COMMIT REFRESH	1
SACER_LOG	SACER_VERSO	QUERY REWRITE	1

SACER_LOG	SACER_VERSO	READ	1
SACER_LOG	SACER_VERSO	REFERENCES	1
SACER_LOG	SACER_VERSO	SELECT	2
SACER_LOG	SACER_VERSO	UPDATE	1
SACER_PING	SACER_IAM	DELETE	1
SACER_PING	SACER_IAM	SELECT	1
SACER_RIC	SACER	SELECT	7

La formulazione delle policy di audit successivamente illustrate tiene conto della necessità di non effettuare l'audit delle operazioni inerenti a queste grant.

Script di creazione delle policy

Si è dunque provveduto, per ciascuno degli schemi applicativi di PARER, che indichiamo con SACER*, a creare una policy che consenta di effettuare l'audit di tutte le possibili azioni sugli oggetti dello schema stesso.

Gli statement di creazione di seguito riportati fanno riferimento alla tabella dummy A0_AUDIT allo scopo di poter creare le policy a prescindere dagli oggetti effettivamente presenti nello schema. Successivamente vengono associati alle policy tutti gli oggetti su cui sia possibile effettuare operazioni di audit. Lo script utilizzato a tale scopo è quello riportato nella sezione relativa al refresh delle policy.

```
CREATE AUDIT POLICY AP_SACER_03
  Actions
    ALL on SACER.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN (''SACER'', ''SACER_IAM'', ''SACER_PING'', ''SACER_RIC'', ''SACER_VERSO'')
OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')     IN (''SACER'', ''SACER_IAM'', ''SACER_PING'', ''SACER_RIC'', ''SACER_VERSO'')
AND (SYS_CONTEXT (''USERENV'', ''OS_USER'') <> ''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;


CREATE AUDIT POLICY AP_SACER_IAM_03
  Actions
    ALL on SACER_IAM.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN (''SACER_IAM'', ''SACER'', ''SACER_LOG'', ''SACER_PING'', ''SACER_RIC'',
''SACER_VERSO'') OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')     IN (''SACER_IAM'', ''SACER'', ''SACER_LOG'', ''SACER_PING'', ''SACER_RIC'',
''SACER_VERSO'') AND (SYS_CONTEXT (''USERENV'', ''OS_USER'') <> ''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;

CREATE AUDIT POLICY AP_SACER_KETTLE_03
  Actions
    ALL on SACER_KETTLE.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN (''SACER_KETTLE'') OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')     IN (''SACER_KETTLE'') AND (SYS_CONTEXT (''USERENV'', ''OS_USER'') <> ''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;

CREATE AUDIT POLICY AP_SACER_LOG_03
  Actions
    ALL on SACER_LOG.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN (''SACER_LOG'', ''SACER'', ''SACER_IAM'', ''SACER_PING'', ''SACER_RIC'',
''SACER_VERSO'') OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')     IN (''SACER_LOG'', ''SACER'', ''SACER_IAM'', ''SACER_PING'', ''SACER_RIC'',
''SACER_VERSO'') AND (SYS_CONTEXT (''USERENV'', ''OS_USER'') <> ''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
```

```
               SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
               SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
               SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
               SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
               SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;


CREATE AUDIT POLICY AP_SACER_PING_03
  Actions
    ALL on SACER_PING.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN (''SACER_PING'', ''SACER_IAM'') OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')     IN (''SACER_PING'', ''SACER_IAM'') AND (SYS_CONTEXT (''USERENV'', ''OS_USER'')
<> ''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;


CREATE AUDIT POLICY AP_SACER_RIC_03
  Actions
    ALL on SACER_RIC.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN (''SACER_RIC'', ''SACER'') OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')     IN (''SACER_RIC'', ''SACER'') AND (SYS_CONTEXT (''USERENV'', ''OS_USER'') <>
''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;


CREATE AUDIT POLICY AP_SACER_TPI_03
  Actions
    ALL on SACER_TPI.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') <> ''SACER_TPI'' OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')  = ''SACER_TPI'' AND (SYS_CONTEXT(''USERENV'', ''OS_USER'') <> ''tomcat''
        OR NOT (SYS_CONTEXT(''USERENV'', ''HOST'') = ''parer-vtc-p01'' OR
                SYS_CONTEXT(''USERENV'', ''HOST'') = ''parer-vtc-p02'')))'
  EVALUATE PER STATEMENT;


CREATE AUDIT POLICY AP_SACER_TPI_TIMERS_03
  Actions
    ALL on SACER_TPI_TIMERS.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') <> ''SACER_TPI_TIMERS'' OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')  = ''SACER_TPI_TIMERS'' AND (SYS_CONTEXT(''USERENV'', ''OS_USER'') <> ''tomcat''
        OR NOT (SYS_CONTEXT(''USERENV'', ''HOST'') = ''parer-vtc-p01'' OR
                SYS_CONTEXT(''USERENV'', ''HOST'') = ''parer-vtc-p02'')))'
  EVALUATE PER STATEMENT;


CREATE AUDIT POLICY AP_SACER_VERSO_03
  Actions
    ALL on SACER_VERSO.A0_AUDIT
  WHEN 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') <> ''SACER_VERSO'' OR
       (SYS_CONTEXT(''USERENV'', ''SESSION_USER'')  = ''SACER_VERSO'' AND (SYS_CONTEXT (''USERENV'', ''OS_USER'') <> ''jboss''
        OR NOT (SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p11.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p12.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p13.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p14.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p15.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p16.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p17.ente.regione.emr.it'' OR
                SYS_CONTEXT (''USERENV'', ''HOST'') = ''parer-vas-p18.ente.regione.emr.it'')))'
  EVALUATE PER STATEMENT;
```

Script di attivazione di tutte le policy

```
AUDIT POLICY ORA_ACCOUNT_MGMT;
AUDIT POLICY ORA_DATABASE_PARAMETER;
AUDIT POLICY ORA_CIS_RECOMMENDATIONS;
AUDIT POLICY ORA_DATABASE_PARAMETER;
AUDIT POLICY ORA_LOGON_FAILURES;
AUDIT POLICY ORA_SECURECONFIG;

AUDIT POLICY AP_BASIC;
AUDIT POLICY AP_DATAPUMP_ALL;

AUDIT POLICY AP_SACER_03;
AUDIT POLICY AP_SACER_IAM_03;
AUDIT POLICY AP_SACER_KETTLE_03;
AUDIT POLICY AP_SACER_LOG_03;
AUDIT POLICY AP_SACER_PING_03;
AUDIT POLICY AP_SACER_RIC_03;
AUDIT POLICY AP_SACER_TPI_03;
AUDIT POLICY AP_SACER_TPI_TIMERS_03;
AUDIT POLICY AP_SACER_VERSO_03;
```

Refresh delle policy di auditing relative agli oggetti degli schemi SACER*

Le policy che operano sugli schemi applicativi hanno la necessità di essere costantemente aggiornate. Se infatti vengono creati nuovi oggetti negli schemi in questione è necessario aggiungere gli oggetti stessi alle policy. E' stato predisposto allo scopo lo script seguente che genera a sua volta uno script di modifica delle policy recuperando le informazioni necessarie dal catalogo del DB.

Script di generazione dello script di refresh

```
SELECT 'ALTER AUDIT POLICY AP_' || OWNER || '_03 ADD ACTIONS ALL ON ' || OWNER
|| '.' || OBJECT_NAME || ';' FROM DBA_OBJECTS
WHERE OWNER IN
(
'SACER',
'SACER_IAM',
'SACER_KETTLE',
'SACER_LOG',
'SACER_PING',
'SACER_RIC',
'SACER_TPI',
'SACER_TPI_TIMERS',
'SACER_VERSO'
)
AND OBJECT_TYPE IN
(
'DIRECTORY',
'FUNCTION',
'JAVA CLASS',
'JAVA RESOURCE',
'JAVA SOURCE',
'LIBRARY',
'MATERIALIZED VIEW',
'MINING MODEL',
'PACKAGE',
'PROCEDURE',
'SEQUENCE',
'TABLE',
'TYPE',
'VIEW'
)
ORDER BY 1;
```

Script di refresh

```
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.A0_AUDIT;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.APL_APPLIC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.APL_PARAM_APPLIC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.APL_SISTEMA_MIGRAZ;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.APL_V_LOG_JOB;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.APL_V_PARAM_APPLIC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_ARCHIV_SEC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_BUSTA_CRITTOG;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_COMP_DOC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO COMP INDICE AIP DA ELAB;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO_COMP_VER_INDICE_AIP_UD;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_CONTENUTO_COMP;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_CONTROFIRMA_FIRMA;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_CONTR_FIRMA_COMP;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_CONTR_MARCA_COMP;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO_CONTR_VERIF_FIRMA_DT_VERS;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_DOC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_ERR_RICH_ANNUL_VERS;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO_FILE_RICH_ANNUL_VERS;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO_FILE_VER_INDICE_AIP_UD;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_FIRMA_COMP;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_INDICE_AIP_UD;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO_INDICE_AIP_UD_DA_ELAB;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON
SACER.ARO_ITEM_RICH_ANNUL_VERS;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_LINK_UNITA_DOC;
ALTER AUDIT POLICY AP_SACER_03 ADD ACTIONS ALL ON SACER.ARO_MARCA_COMP;
.
.
.
```

Il lancio dell'aggiornamento delle policy è schedulato tutte le notti alle ore 1.45 AM.

Collegamento con Arcsight e cancellazione dei record di audit

I dati collezionati mediante i meccanismi di audit di Oracle sono consolidati ed analizzati sul sistema SIEM Arcsight. A tale scopo è stata creata l'utenza Oracle:

```
CREATE USER USRARCSIGHT
  IDENTIFIED BY <password>
  DEFAULT TABLESPACE USERS
  TEMPORARY TABLESPACE TEMP
  PROFILE DEFAULT_UPLT
  ACCOUNT UNLOCK;
  -- 1 Role for USRARCSIGHT
  GRANT CONNECT TO USRARCSIGHT;
  ALTER USER USRARCSIGHT DEFAULT ROLE ALL;
  -- 1 System Privilege for USRARCSIGHT
  GRANT SELECT ANY DICTIONARY TO USRARCSIGHT;
  -- 4 Object Privileges for USRARCSIGHT
    GRANT SELECT ON SYS.AUDIT$ TO USRARCSIGHT;
    GRANT SELECT ON SYS.DBA_AUDIT_TRAIL TO USRARCSIGHT;
    GRANT SELECT ON SYS.DBA_COMMON_AUDIT_TRAIL TO USRARCSIGHT;
    GRANT SELECT ON SYS.V_$INSTANCE TO USRARCSIGHT;
```

che viene utilizzata dal job di Arcsight che ad intervalli regolari estrae dalla vista UNIFIED_AUDIT_TRAIL le informazioni che devono essere conservate sul SIEM. Per poter meglio gestire le sessioni relative all'utenza USRARCSIGHT è stato inoltre creato a livello Oracle RAC uno specifico servizio **SVC_ARCSIGHT**.

La manutenzione dell'audit trail, consistente in una cancellazione giornaliera dei record più vecchi di 8 giorni, è assicurata da un job che giornalmente lancia lo script:

```
BEGIN
  DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP(
   AUDIT_TRAIL_TYPE      =>  DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
   LAST_ARCHIVE_TIME     =>  SYSDATE - 8);
  DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
   AUDIT_TRAIL_TYPE           =>  DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
   USE_LAST_ARCH_TIMESTAMP    =>  TRUE);
END;
```

Considerazioni finali

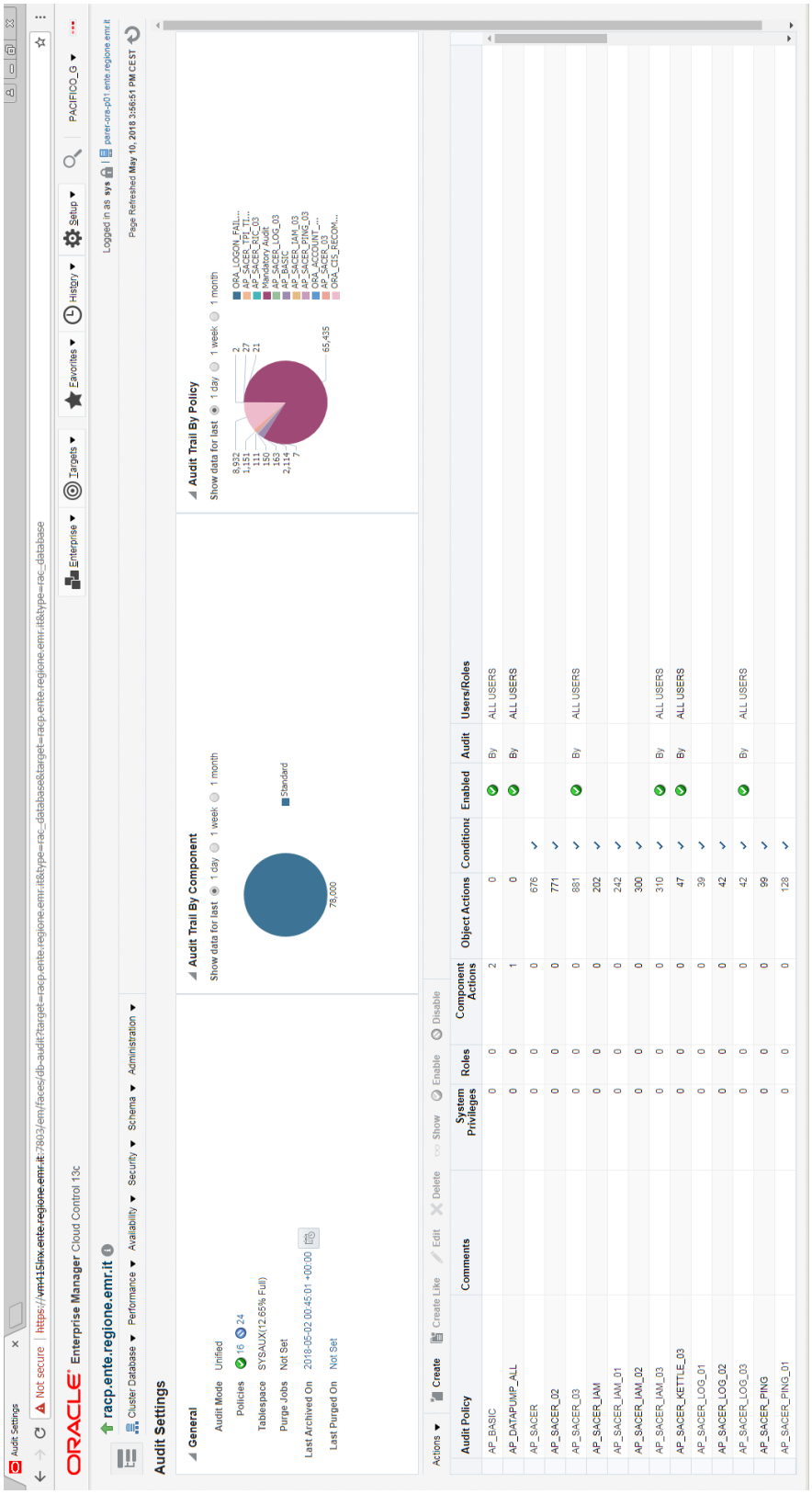
Per dare evidenza della quantità di record accumulati e mostrare la sostenibilità globale della soluzione adottata si riporta una tabella che presenta, per ciascun set di policy di attivazione, il numero di record relativi. L'analisi è relativa agli ultimi sette gioni (interrogazione effettuata in data 10/05/2018).

Valore del campo UNIFIED_AUDIT_POLICIES	Numero di record
AP_BASIC	16349
AP_SACER_IAM_03	488
AP_SACER_LOG_03	125
AP_SACER_PING_03	1925
AP_SACER_RIC_03	93
AP_SACER_TPI_TIMERS_03	305
AP_SACER_TPI_03	7
AP_SACER_03	16472
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS	1345
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, AP_SACER_IAM_03	4424
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, AP_SACER_PING_03	2520
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, AP_SACER_TPI_TIMERS_03	336
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, AP_SACER_TPI_03	224
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, AP_SACER_VERSO_03	357
ORA_ACCOUNT_MGMT, ORA_CIS_RECOMMENDATIONS, ORA_SECURECONFIG, AP_SACER_03	10843
ORA_CIS_RECOMMENDATIONS	114623
ORA_DATABASE_PARAMETER, ORA_SECURECONFIG, ORA_CIS_RECOMMENDATIONS	27
ORA_SECURECONFIG	11067
Righe di dettaglio	846405

Query utilizzata:

```
set linesize 200
set pagesize 2000
select unified_audit_policies, count(*) from unified_audit_trail
where event_timestamp < (sysdate - 7)
group by unified_audit_policies
order by 1;
```

La pagina seguente contiene invece una schermata del sinottico dell'audit presente su Oracle Enterprise Manager Cloud Control.



Schermata riassuntiva dei settaggi di auditing del DB RACP da Oracle Enterprise Manager

Documenti di riferimento

Best practices e white papers

All About Oracle Auditing – Updated for 12C! A White Paper February 2015 - www.dbspecialists.com

CIS Oracle Database 11gR2 Benchmark v2.0.0 27/02/2015 - www.cisecurity.org - benchmarks.cisecurity.org

CIS Oracle Database 12c Benchmark v1.0.0 29/04/2015 - www.cisecurity.org - benchmarks.cisecurity.org

ORACLE 12C UNIFIED AUDITING Version 1.0 – October 2014 - www.integrigy.com

Manualistica Oracle

Oracle® Database Administrator's Guide 12c Release 1 (12.1) E41484-10 August 2014 - www.oracle.com

Oracle® Database Reference 12c Release 1 (12.1) E41527-17 March 2015 - www.oracle.com

Oracle® Database Security Guide 12c Release 1 (12.1) E48135-11 November 2014 - www.oracle.com

Oracle® Database SQL Language Reference 12c Release 1 (12.1) E41329-12 December 2014 - www.oracle.com

Oracle® Database 2 Day + Security Guide 12c Release 1 (12.1) E17609-19 June 2014 - www.oracle.com

Documentazione supporto tecnico Oracle

How To Enable The New Unified Auditing In 12c? (Doc ID 1567006.1) - support.oracle.com

Bug 18743542 : 12C UNIFIED AUDIT TRAIL, CANNOT DELETE LAST_ARCHIVE_TIME - support.oracle.com

Oracle Database 12c Release 12.1.0.2.0 Patch for Bug# 18743542 for Linux-x86-64 Platforms Readme - support.oracle.com

Riferimenti normativi

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 *(G.U. n. 300 del 24 dicembre 2008)* - www.garanteprivacy.it

Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009 *(G.U. n. 149 del 30 giugno 2009)* - www.garanteprivacy.it

REGIONE EMILIA-ROMAGNA - DETERMINAZIONE n° 597 del 23/01/2012 - **DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA DELLA GIUNTA E DELL'ASSEMBLEA LEGISLATIVA DELLA REGIONE EMILIA-ROMAGNA**