EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH

INTERSHIP REPORT

Implementation of Corrective Actions for policy violations in Oracle Enterprise Manager

Student :
Alexandre BECHE

Supervisors :
Anton TOPUROV
Pablo MARTINEZ PEDREIRA

31 août 2010

Abstract

"Implementation of Corrective Actions for policy violations in Oracle Enterprise Manager"

Databases are the central point of information systems and having the high availability can be crucial. The mean time to recover for an outage is defined as detection time plus repair time. Monitoring allows maintaining a very short detection time but fixing the problem can prove being time consuming as well. During the internship, I study Enterprise Manager policy violations, analyse which ones can be addressed with automatic fixes and implement these fixes for most common violations.

Contents

1 CERN Overview **3**
- 1.1 Presentation of CERN . . . 3
  - 1.1.1 History . . . 3
  - 1.1.2 Computing facilities . . . 4
- 1.2 Organization . . . 4
  - 1.2.1 Hierarchy . . . 4
  - 1.2.2 Collaboration . . . 5
- 1.3 Major innovations in information technologies . . . 6

2 Theorical concepts and statistics on policy violations **7**
- 2.1 Theorical concepts . . . 7
  - 2.1.1 Definitions . . . 7
  - 2.1.2 Monitoring templates . . . 8
  - 2.1.3 Policy check : Internal mechanism in Oracle Enterprise Manager . . . 8
- 2.2 Analysis on policy violations . . . 9
  - 2.2.1 Evolution of number of alerts . . . 9
  - 2.2.2 Statistics on policy violations . . . 10

3 Implementation and test of corrective actions **13**
- 3.1 Corrective actions : theory and internal mechanism . . . 13
  - 3.1.1 Corrective actions : Why? . . . 13
  - 3.1.2 Policy violation and corrective action process . . . 13
- 3.2 Corrective actions set up . . . 14
  - 3.2.1 Corrective actions constraints . . . 14
  - 3.2.2 Corrective actions set up . . . 15
- 3.3 Simulation : Policy violation + corrective action . . . 17

4 Notification rules and target grouping **21**
- 4.1 How notification rules works? . . . 21
- 4.2 New grouping of targets . . . 22

Annexes **23**

List of figures **28**

Bibliography **30**

Chapter 1

CERN Overview

1.1 Presentation of CERN

1.1.1 History

French physicist Louis de Broglie put the first official proposal for the creation of a European laboratory at the European Cultural Conference in Lausanne in December 1949. Later, 11 countries ratify the convention establishing CERN, the European Organization for Nuclear Research thus marking the birthday of September 29, 1954. The laboratory is located on franco-swiss border on two main sites : Meyrin and Prevessin. Today CERN is the world's largest particle physics laboratory, the organization has 20 member states and 8 observers (Figure 1.1 shows the repartition on the world map). CERN is currently the workplace of approximatively 2,300 staff members, as well as some 15,000 scientists, engineers and students (representing 580 universities and research facilities having 80 nationalities).

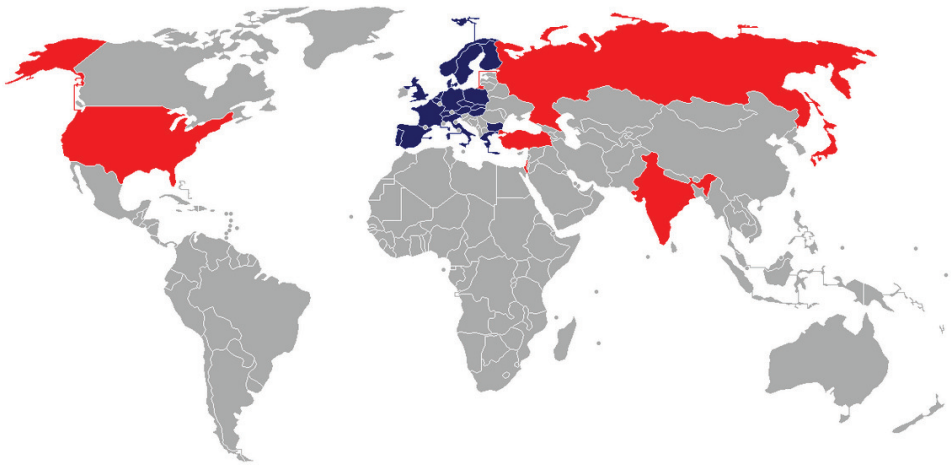


Figure 1.1: CERN members and observers

1.1.2 Computing facilities

In 1972 CERN decided to build the first computer center in Europe. Today there are 7,500 systems distributed on two floors (2650m^2) which total energy consumption of more than 5MW. Following table deals with computer center facts:

Total servers	7,500
Total processing cores	50,000
Storage capacity on disk drive	19,800TB
Storage capacity on tape cartridges	24,400TB
Infrastructure servers	400
Oracle database instances	200
Oracle servers	300
Very high performance routers	150
Switches	2200
Fiber optic cables owned by CERN	5,000km
WAN connectivity	150Gbps

1.2 Organization

1.2.1 Hierarchy

Internal organization of CERN is divided in 3 hierarchical levels: departments, groups and sections. Following schema represents my place in the organization.

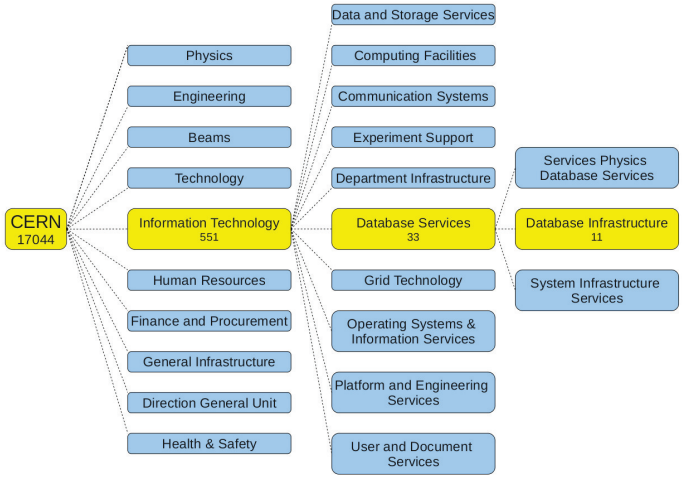


Figure 1.2: hierarchy at CERN

1.2.2 Collaboration

CERN is engaged in many international initiatives. In computing, CERN has three major projects:

- **Enabling Grids for E-sciencE (EGEE)** : European grid for scientific research.
- **Worldwide LHC Computing Grid (WLCG)** : Grid based on EGEE and OSG (Open Science Grid) for analyses of data from the LHC. It's a grid which aggregates computing power from all around the world.
  Following figure shows the service hierarchy in WLCG:

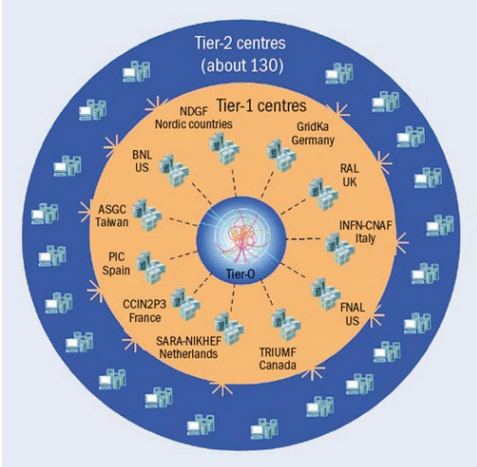


Figure 1.3: WLCG infrastructure

In this collaboration, each tier has predefined tasks:

  - tier-0 : CERN
    - Data recording
    - Initial data reconstruction
    - Data distribution
  - tier-1 : 11 centres
    - Permanent storage
    - Re-processing
    - Analysis
  - tier-2 : 200 centres (2010)
    - Simulation
    - End-user analysis

- **Openlab project** : Collaboration between CERN and leading industry actors (Oracle, HP, Intel and Siemens). Projects are based on the needs of each partner, taking into

account CERN specific needs in the area. For example, Oracle is providing alpha and beta releases of their software for testing. This way Oracle can validate its applications from big real environment while CERN readiness for future Oracle releases.

1.3 Major innovations in information technologies

Although CERN is a physic research laboratory, sometimes major innovations in other domains appear:

- **The World Wide Web:** At the end of 80's, scientists around the world needed to share their work. To facilitate this, in 1989 Tim Berners-Lee invented a global information system known as the **World Wide Web (www)**.
- **The Grid:** Computing grid is similar to electric power grid, with main purpose to share computing resources all over the world in order to increase overall computing performance.

Chapter 2

Theorical concepts and statistics on policy violations

For all activities like physics experiments or human resources management, CERN needs many databases (Schema in annex 1 shows the complex structure of CERN database systems). All RDBMS[1] software is supplied by Oracle, and is monitored by Oracle Enterprise Manager Grid Control. Monitoring is required in big infrastructure in order to react quickly to problems or misconfigurations. This part of the report focuses on theorical concept used in the implementation of corrective actions and the actual state of the policy violations in CERN databases (statistics and their evolution).

2.1 Theorical concepts

2.1.1 Definitions

- **Target:** in Enterprise Manager, a monitored object is called target. The target are of different types: databases, hosts, agents, etc...
- **Policy:** policies define how you want your systems to behave, in order to remain in compliance with organization security, configuration, and storage standards.
- **Policy violation:** abnormal state when system is not compliant with a policy.
- **Corrective action:** Automatic response to a target alerts or policy violations.
- **Monitoring template:** Set of metrics and policies.
- **Management repository:** database which contains all the information relative to Enterprise Manager.

[1] Relational Database Management System

- **Notification rules:** set of conditions that determine when a notification occurs.

2.1.2 Monitoring templates

In order to organize all metrics and policies in Enterprise Manager, **monitoring templates** are used. They allow to group together a set of metrics and policies with common purpose. In Enterprise Manager, the section *Setup->Monitoring templates* displays all monitoring templates. However it is not easy to find targets and groups of targets this templates are applied to. Generally, correlation between monitoring templates and targets is visible in *policy associations* page. But using repository views, it is more straightforward to find all informations about monitoring templates.

The two most interesting views are:

- **MGMT$TEMPLATES**: Displays details of all the management templates stored in the Management Repository.
- **MGMT$TEMPLATE_POLICY_SETTINGS**: Displays policy settings for management templates.

Annex 2 shows monitoring templates used for each policy.

2.1.3 Policy check : Internal mechanism in Oracle Enterprise Manager

In initial state, there are no alerts or policy violations in Enterprise Manager because metrics/policies and targets aren't bind together. To link policies and targets, it is necessary to apply a monitoring template on target or group of targets. Following schema shows the relation between policies, monitoring templates and target groups.

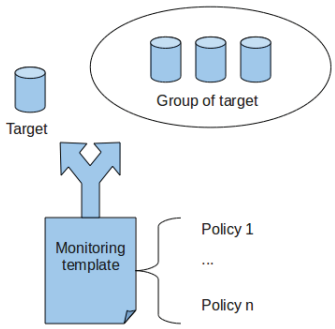


Figure 2.1: Relation between monitoring templates and targets

2.2 Analysis on policy violations

The main page of Enterprise Manager displays a summary of all alerts and policy violations. We can see on next figure a myriad of alerts and policy violations in the existing system (more than 15,000 policy violations and about 800 for the last 24 hours). Policy violations cover all types of targets.

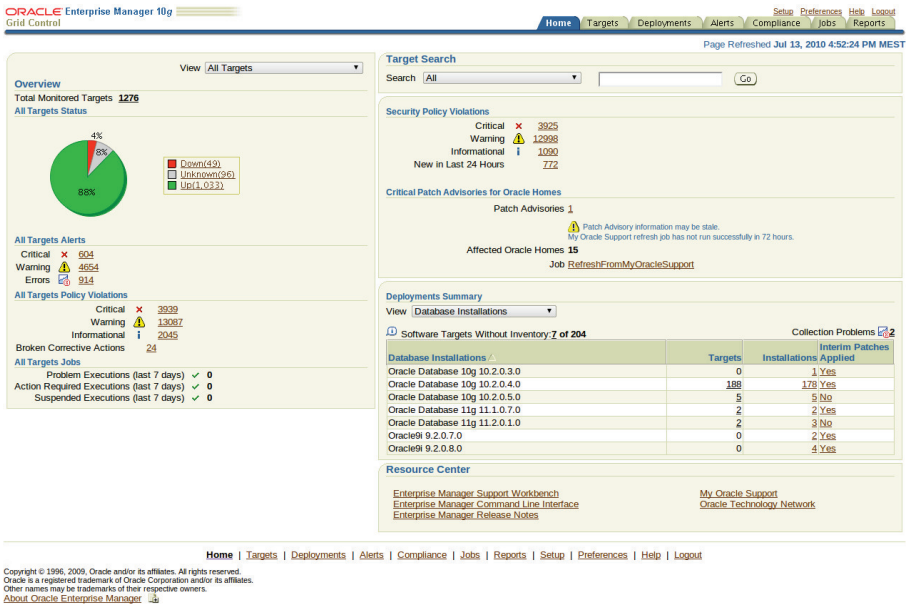


Figure 2.2: Oracle Enterprise Manager Grid Control main page

2.2.1 Evolution of number of alerts

Since policies were implemented at CERN in 2007, quantity of policy violations is continuously increasing and currently approximates at 25 000 violations per year. It is important to analyse this violations and see which of them can be fixed with automated responses thus decreasing their total number.

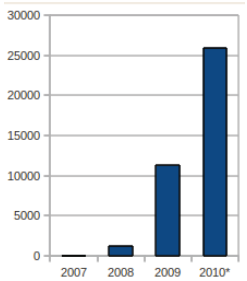
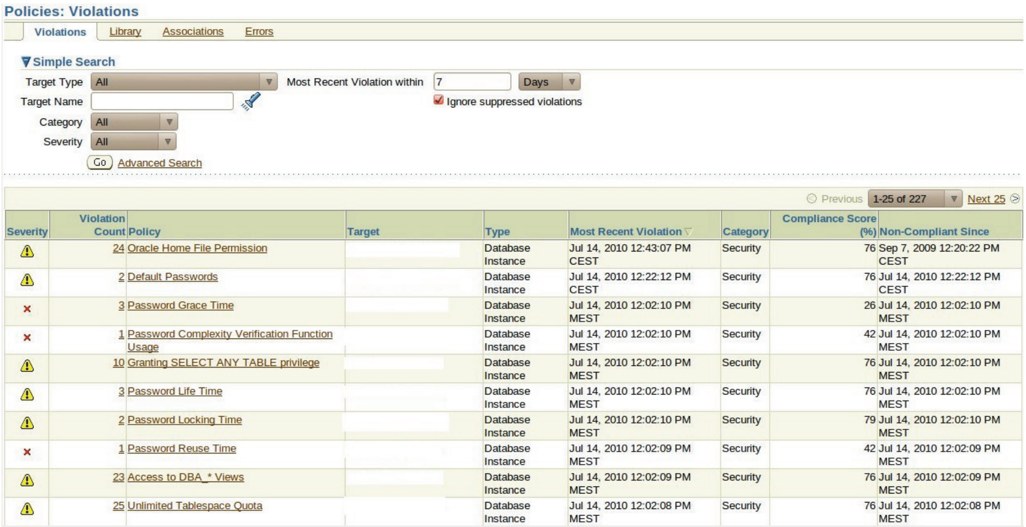


Figure 2.3: Explosion of policy violations

2.2.2 Statistics on policy violations

In Enterprise Manager, we can only see information about current policy violations. We can see on next figure the policy violations page in Enterprise Manager:



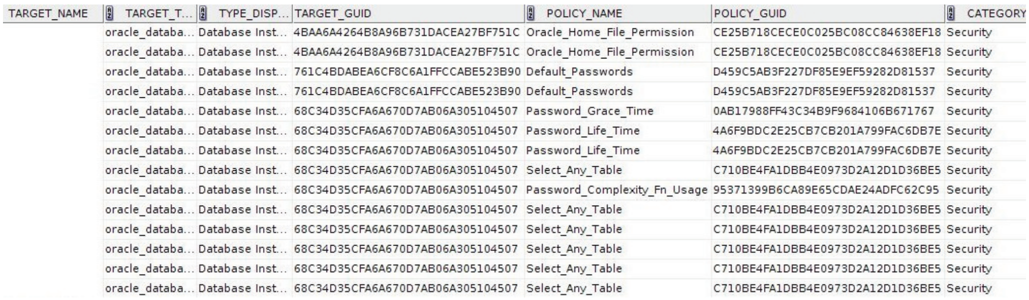
Severity	Violation Count	Policy	Target	Type	Most Recent Violation	Category	Compliance Score (%)	Non-Compliant Since
⚠	24	Oracle Home File Permission		Database Instance	Jul 14, 2010 12:43:07 PM CEST	Security	76	Sep 7, 2009 12:20:22 PM CEST
⚠	2	Default Passwords		Database Instance	Jul 14, 2010 12:22:12 PM CEST	Security	76	Jul 14, 2010 12:22:12 PM CEST
×	3	Password Grace Time		Database Instance	Jul 14, 2010 12:02:10 PM MEST	Security	26	Jul 14, 2010 12:02:10 PM MEST
×	1	Password Complexity Verification Function Usage		Database Instance	Jul 14, 2010 12:02:10 PM MEST	Security	42	Jul 14, 2010 12:02:10 PM MEST
⚠	10	Granting SELECT ANY TABLE privilege		Database Instance	Jul 14, 2010 12:02:10 PM MEST	Security	76	Jul 14, 2010 12:02:10 PM MEST
⚠	3	Password Life Time		Database Instance	Jul 14, 2010 12:02:10 PM MEST	Security	76	Jul 14, 2010 12:02:10 PM MEST
⚠	2	Password Locking Time		Database Instance	Jul 14, 2010 12:02:10 PM MEST	Security	79	Jul 14, 2010 12:02:10 PM MEST
×	1	Password Reuse Time		Database Instance	Jul 14, 2010 12:02:09 PM MEST	Security	42	Jul 14, 2010 12:02:09 PM MEST
⚠	23	Access to DBA_* Views		Database Instance	Jul 14, 2010 12:02:09 PM MEST	Security	76	Jul 14, 2010 12:02:09 PM MEST
⚠	25	Unlimited Tablespace Quota		Database Instance	Jul 14, 2010 12:02:08 PM MEST	Security	76	Jul 14, 2010 12:02:08 PM MEST

Figure 2.4: Policy violations: page in Enterprise Manager

To create statistics on policy violations, we need to query historical views which are stored in Enterprise Manager repository. The two interesting views in the repository for this task are:

- MGMT$POLICY_VIOLATIONS_CURRENT : same informations as Enterprise Manager pages
- MGMT$POLICY_VIOLATIONS_HISTORY : all history of policy violations

Following image displays the content of MGMT$POLICY_VIOLATIONS_CURRENT:



TARGET_NAME	TARGET_T...	TYPE_DISP...	TARGET_GUID	POLICY_NAME	POLICY_GUID	CATEGORY
	oracle_databa...	Database Inst...	4BAA6A4264B8A96B731DACEA27BF751C	Oracle_Home_File_Permission	CE25B718CECE0C025BC08CC84638EF18	Security
	oracle_databa...	Database Inst...	4BAA6A4264B8A96B731DACEA27BF751C	Oracle_Home_File_Permission	CE25B718CECE0C025BC08CC84638EF18	Security
	oracle_databa...	Database Inst...	761C4BDABEA6CF8C6A1FFCCABE523B90	Default_Passwords	D459C5AB3F227DF85E9EF59282D81537	Security
	oracle_databa...	Database Inst...	761C4BDABEA6CF8C6A1FFCCABE523B90	Default_Passwords	D459C5AB3F227DF85E9EF59282D81537	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Password_Grace_Time	0AB17988FF43C34B9F9684106B671767	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Password_Life_Time	4A6F9BDC2E25CB7CB201A799FAC6DB7E	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Password_Life_Time	4A6F9BDC2E25CB7CB201A799FAC6DB7E	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Select_Any_Table	C710BE4FA1DBB4E0973D2A12D1D36BE5	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Password_Complexity_Fn_Usage	95371399B6CA89E65CDAE24ADFC62C95	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Select_Any_Table	C710BE4FA1DBB4E0973D2A12D1D36BE5	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Select_Any_Table	C710BE4FA1DBB4E0973D2A12D1D36BE5	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Select_Any_Table	C710BE4FA1DBB4E0973D2A12D1D36BE5	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Select_Any_Table	C710BE4FA1DBB4E0973D2A12D1D36BE5	Security
	oracle_databa...	Database Inst...	68C34D35CFA6A670D7AB06A305104507	Select_Any_Table	C710BE4FA1DBB4E0973D2A12D1D36BE5	Security

Figure 2.5: Policy violations: contents of MGMT$POLICY_VIOLATIONS_CURRENT

In order to detect the most common violations, we can classify them by target type (database, listener, host etc. . .) or by category (security, configuration, storage).

Violations by target type

Violation target type	total	ratio
Database Instance	10447	55.47%
Cluster Database	5944	31.56%
Listener	1655	8.79%
Host	744	3.95%
other (ASM, OC4J, HTTP, Weblogic)	45	0.24%

Figure 2.6: Policy violations by target type (table)

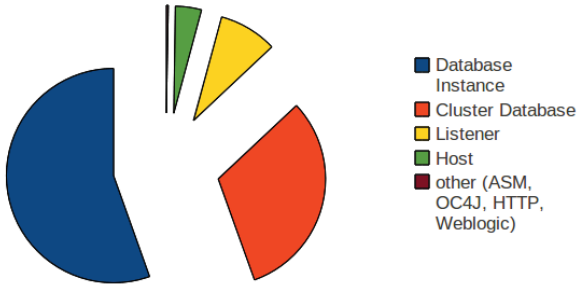


Figure 2.7: Policy violations by target type (chart)

Violations by category

Violation category	total	ratio
Security	17765	94.18%
Configuration	584	3.10%
Storage	513	2.72%

Figure 2.8: Policy violations by category (table)

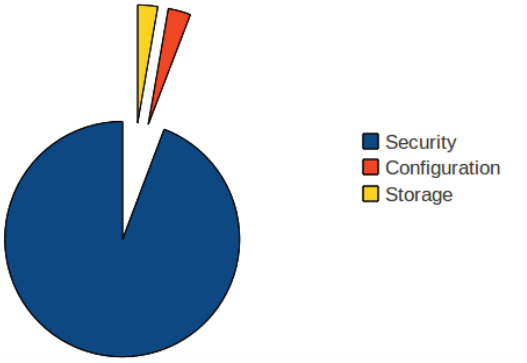


Figure 2.9: Policy violations by category (chart)

By analysing these tables and charts, it is very easy to identify the problem. Most of the violations are on databases (clusters or single instances) and are security related.
Let's see the top 15 policy violations for the last month. Following query results show the number of violations per policy for the last 30 days:

```
1 SELECT policy_name, count(*) AS tot FROM
2     (
3         SELECT * FROM MGMT$POLICY_VIOLATION_CURRENT
4         WHERE collection_timestamp > (sysdate - 30)
5     )
6 GROUP BY policy_name
7 ORDER BY tot desc
```

Policy name	Enterprise manager name	total
Select_Privilege	Access to DBA_* Views	906
Select_Any_Table	Granting SELECT ANY TABLE privilege	351
Oracle_Home_File_Permission	Oracle Home File Permission	253
Unlimited_Table_Space_Quota	Unlimited Tablespace Quota	177
Open_ports	Open Ports	77
Password_Life_Time	Password Life Time	31
Password_Grace_Time	Password Grace Time	26
HIDDEN_PARAMS2	Use of Non-Standard Initialization Parameters	23
SYSTEM_AS_DEFAULT_TBSP	Non-System Users with System Tablespace as Default Tablespace	19
Password_Locking_Time	Password Locking Time	18
EXECUTE_UTL_FILE_Privileges_To_PUBLIC	Execute Privileges on UTL_FILE To PUBLIC	12
Password_Complexity_Fn_Usage	Password Complexity Verification Function Usage	12
Oracle_Home_Executable_Files_Owner	Oracle Home Executable Files Owner	12
Sql92_Security	Use of SQL92 Security Features	12
initora_File_Permission	Initialization Parameter File Permission	10

Figure 2.10: Most common violation

We can see that few policies are responsible for the biggest slice of the violations. These violations we will try to solve by using corrective actions.

Chapter 3

Implementation and test of corrective actions

In this part, we will see what is a corrective action and how to test it by simulating policy violation. There are many types of policy violations corresponding to different target types (example: host related policy violation). This document addresses only databases related policy violations.

3.1 Corrective actions : theory and internal mechanism

3.1.1 Corrective actions : Why?

The MTTR[1] for an outage is defined as the detection time plus the repair time. Grid Control allows us to decrease detection time by monitoring targets with policies and metrics. It is possible to decrease the repair time by implementing automated responses to abnormal behaviour called **corrective actions**. Reducing the overall MTTR can be crucial for meeting service level agreements.

3.1.2 Policy violation and corrective action process

In a production system, an abnormal behaviour can trigger a policy violation if the policy is applied to corresponding target using monitoring template. Enterprise Manager allows the definition of corrective actions in response to this policy violation. If the corrective action succeeds, system returns in a normal state. But if failed, system will stay in an abnormal state

[1] Mean Time To Recovery

until there manual solution is applied, because corrective action is triggered only the first time the policy is violated or severity state changes.

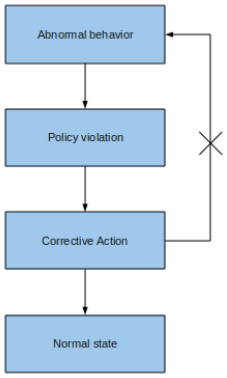


Figure 3.1: policy violation and corrective action process

3.2 Corrective actions set up

3.2.1 Corrective actions constraints

There are three major constraints with corrective actions:

1. Corrective actions will be applied only in response to new policy violations.
2. *"A corrective action is added to a target metric only if it is defined in the monitoring template when that template is **first** applied"*[2]
   The only way to implement corrective actions on existing monitoring templates is the following procedure:
   - ”Create like” new template from existing monitoring template
   - Edit the new template
   - Drop the old one
   - Apply the new one
3. Enterprise Manager needs database credentials (Normal and SYSDBA when we want execute query with system privileges like *REVOKE*) and host credentials of the database server. These credentials are required to execute our query through textitsqlplus. If there are 10 databases, credentials must be set for each of them. Figure 3.2 shows the preferred credentials page.

[2]Oracle Enterprise Manager 10g : Grig Control Implementation Guide

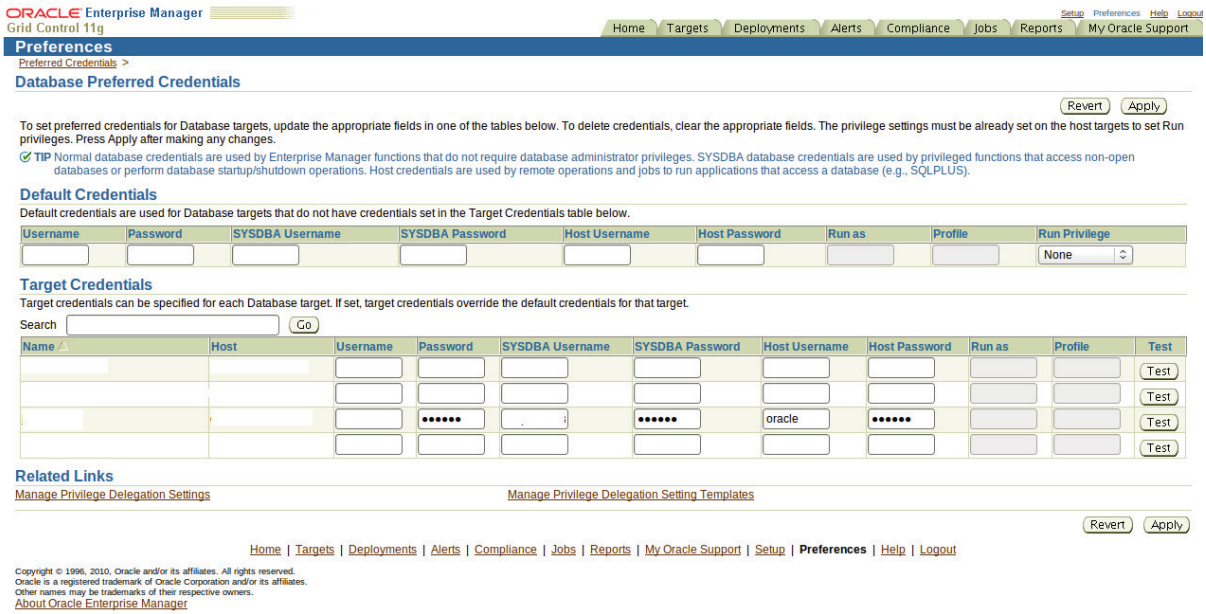


Figure 3.2: Preferred credentials page

3.2.2 Corrective actions set up

In this part, we will explain step by step the set up of a corrective action:

1. Definition of a monitoring template. In Enterprise Manager, the page ***Setup->Monitoring templates*** allows creation of new templates. Figure 3.3 shows the page with all monitoring templates.

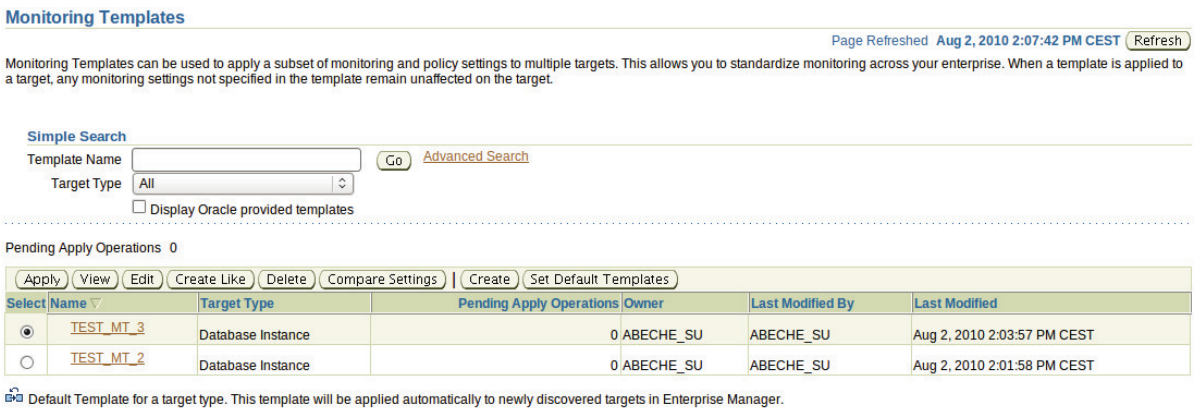


Figure 3.3: Monitoring templates page

2. Common parameters like name and description need to be filled together with dedicated metrics and policies during the creation of monitoring template. Figure 3.4 shows the page where we can assign policies to a monitoring template.

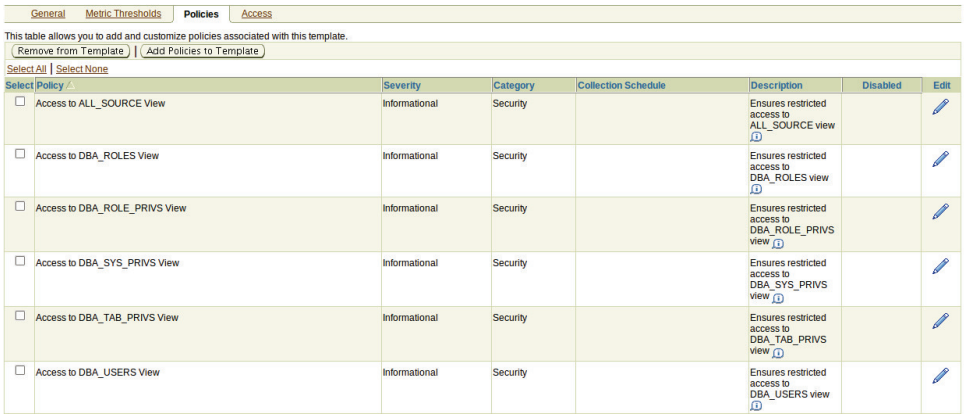


Figure 3.4: Policies assignment to a template

3. For each defined policy, it is possible to attach a corrective action and prevent multiple execution of it as shown in the figure 3.5

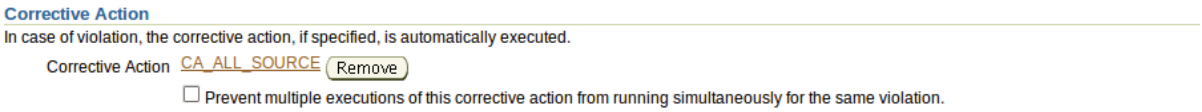


Figure 3.5: definition of new corrective action for a policy

4. During the creation of corrective action, you can choose the type of response (*SQL script*, *host script*, . . .). For example, following figure 3.6 shows the page where a script can be written and displays all parameters available for its use.

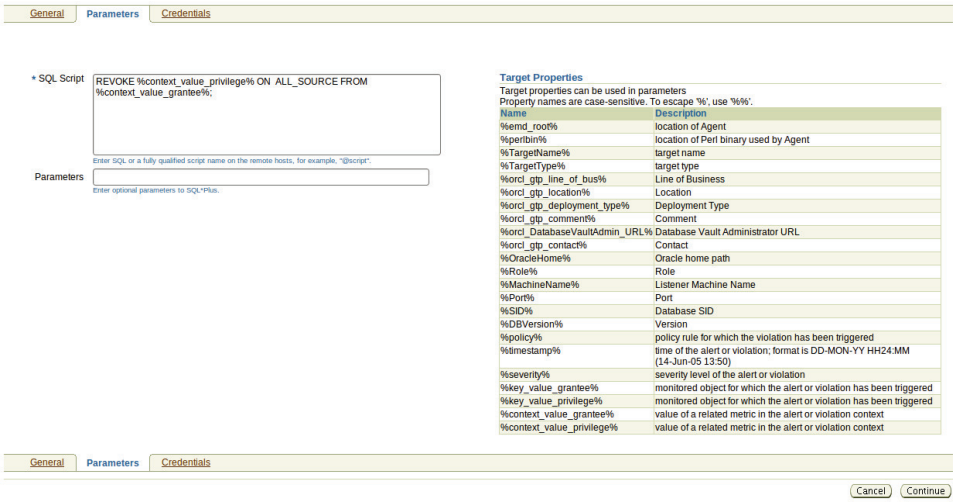


Figure 3.6: corrective action : scripting page

5. In the last step we apply monitoring template to a target or a group of targets

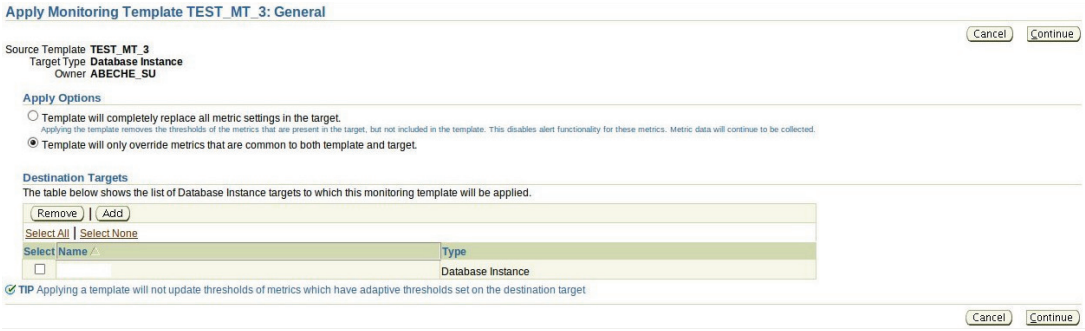


Figure 3.7: Monitoring template : apply page

3.3 Simulation : Policy violation + corrective action

Previously, we have defined a monitoring template with associated corrective actions. In this part, we will generate policy violation in order to test our corrective action.

1. In the initial state, we can see in Enterprise Manager there are no violations in our system, see figure 3.8.

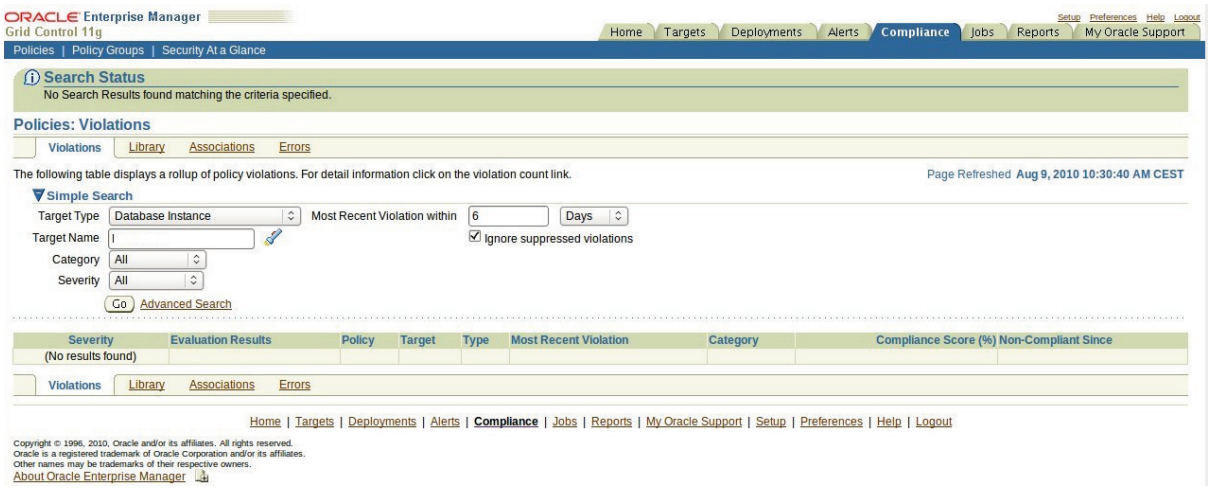


Figure 3.8: Overview of compliance tab without policy violations

2. Corrective action script we created in previous chapter corresponds to the policy *"Granting SELECT ANY TABLE privilege"*. So we will trigger a violation related to this policy with the following query:

```
1 GRANT select any table TO abeche;
```

3. Now, with the same filter as in step 2, we can see in Enterprise Manager there are new violations

Figure 3.9: Overview of compliance tab with policy violations

4. If we click on the number of violation, a new page appears with a summary of the violation and the status of the execution of corrective action.

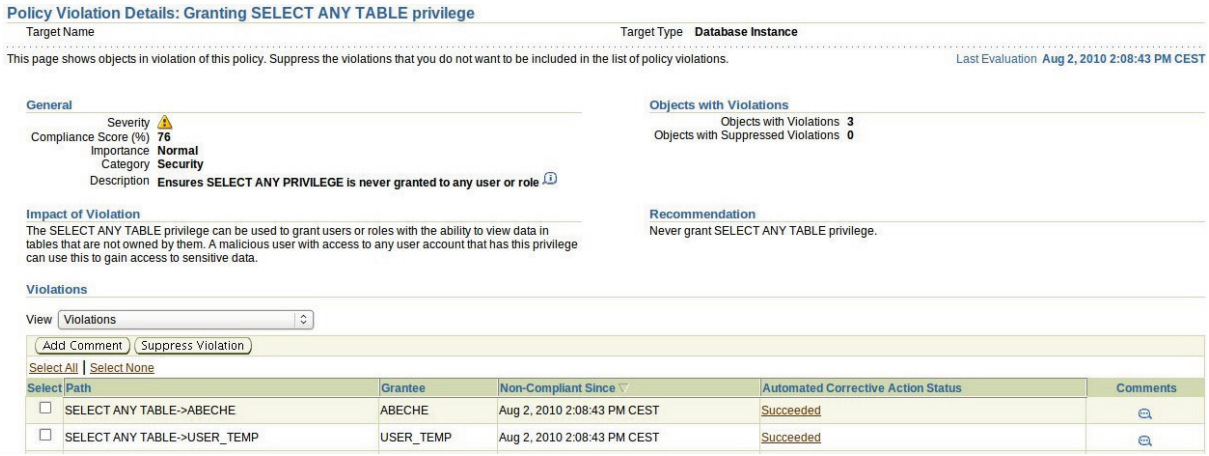


Figure 3.10: Overview of succeeded corrective action

5. We can have a look on the result of our script on the following figure.

```
1 REVOKE select any table FROM %context_value_grantee%
```

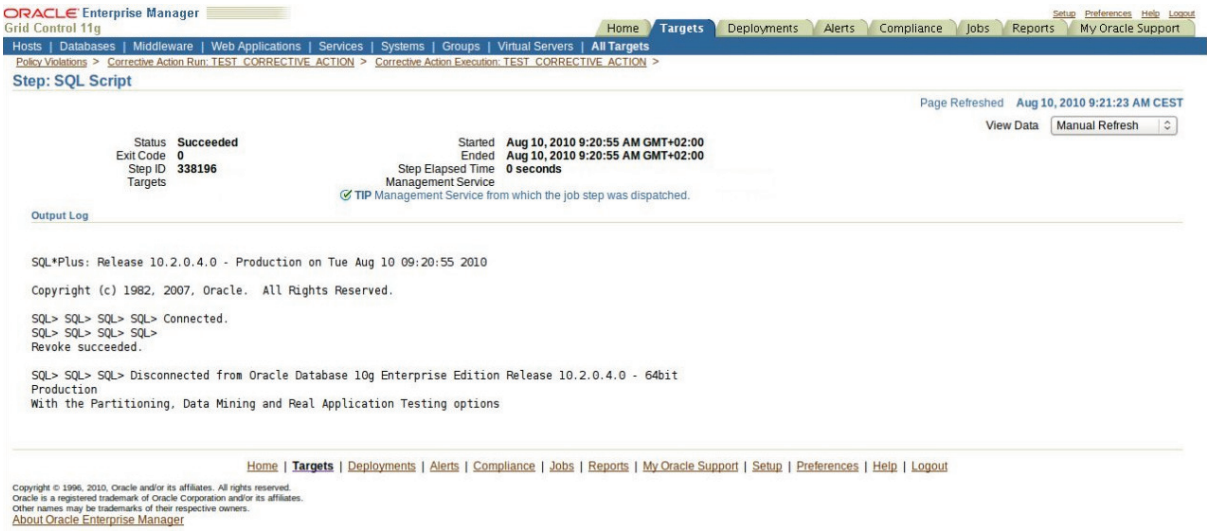


Figure 3.11: sqlplus : result of corrective action

6. After 5 minutes, we can see a return to a normal state due to the success of our automatic script. In our test system, the schedule time is 5 minutes to accelerate the test procedure. In a real production system, the scheduling is set to 24 hours.

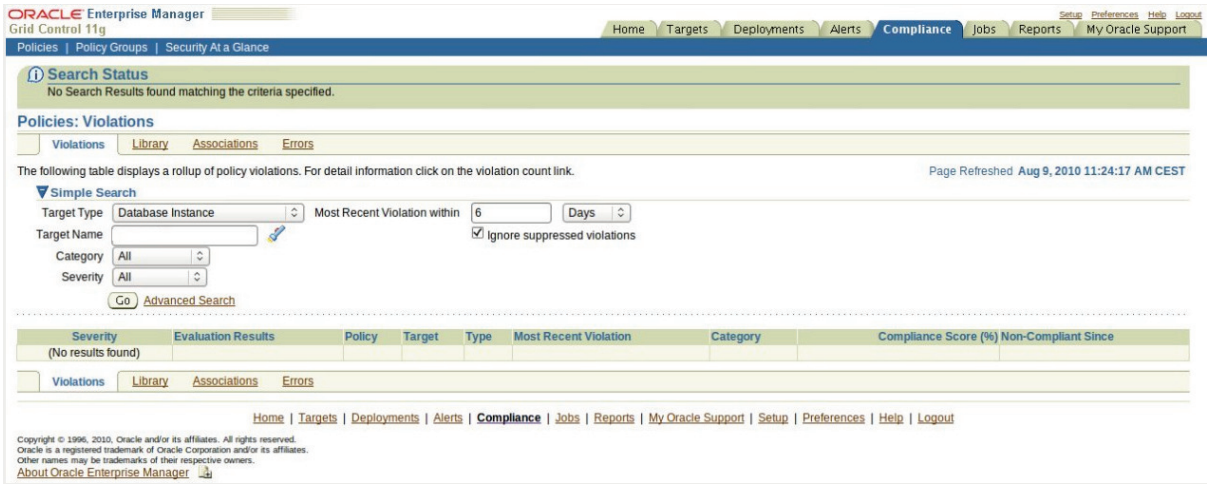


Figure 3.12: Compliance tab : return to normal state

In our production system, we decide to fix automatically some of the policy violations. Annex 3 shows the list of policies we have decided to treat.

Chapter 4

Notification rules and target grouping

Generally, notification rules are used to decrease the reaction time of the administrator. It is more convenient to receive an email when problem occurs than going to Enterprise Manager to see it.

4.1 How notification rules works?

There are two distinct processes, **notification rules** and **notification schedule**. A notification rule is a set of conditions that determine when a problem occurs (for example: target down, critical state for a metric) and a notification schedule which determines when an administrator receives a notification and at which address(es). Following schema shows the internal mechanism of a notification rule:

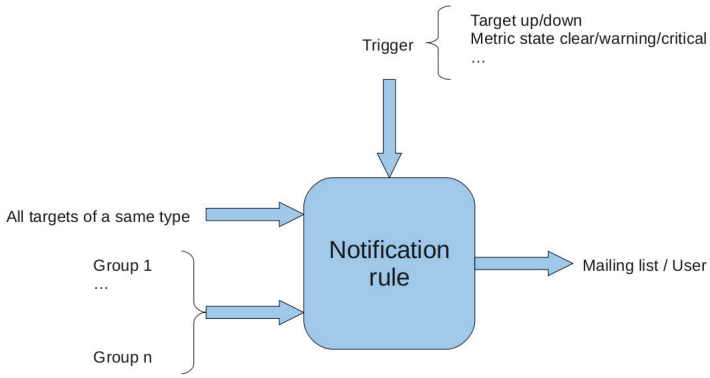


Figure 4.1: Notification rules : internal mechanism

During internal investigation, we have found that some alerts don't trigger any email notification. This was due to some of groups were not bind with notification rules. In order to

clean up the situation, we agreed to regroups the targets an re-apply the notification rules to new groups.

4.2 New grouping of targets

Some groups in Enterprise Manager were not based on logical grouping and had redundant informations in different groups. In order to standardize the grouping, a proposal was made based on the new grouping in the tab.xml (all databases schema) and service catalog. Following schema shows the new grouping approved by our group.

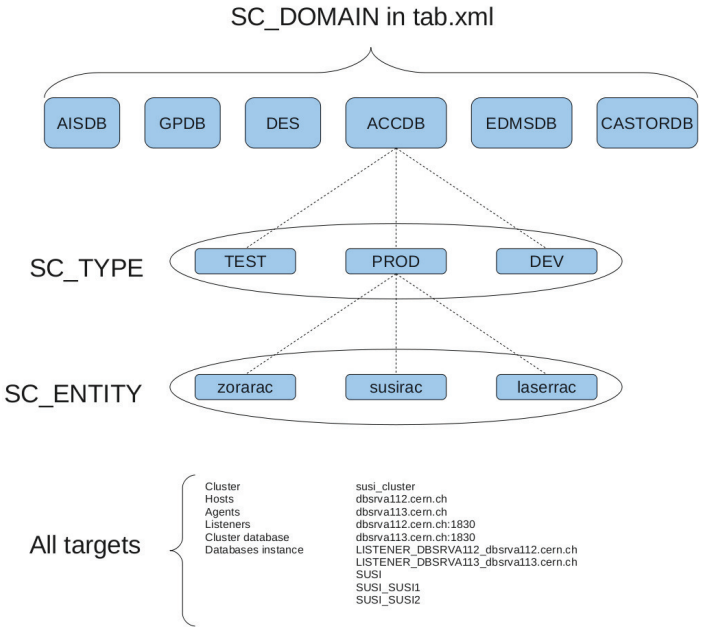
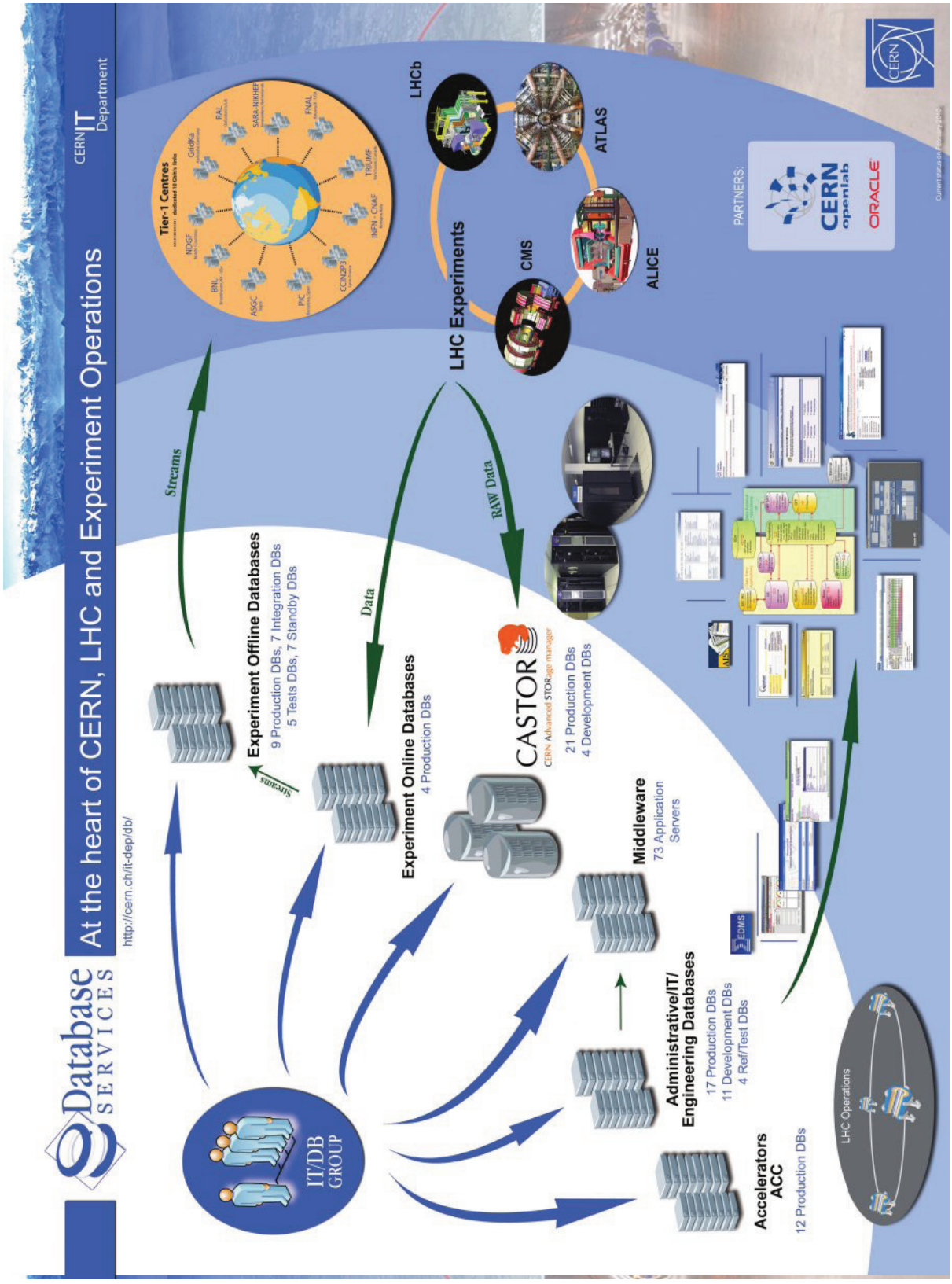


Figure 4.2: New grouping model

Annexes


Database SERVICES
At the heart of CERN, LHC and Experiment Operations
CERN IT Department
http://cern.ch/it-dep/db/
Tier-1 Centres
LHC Experiments
LHCb
ATLAS
CMS
ALICE
Streams
Data
RAW Data
Experiment Offline Databases
9 Production DBs, 7 Integration DBs
5 Tests DBs, 7 Standby DBs
Experiment Online Databases
4 Production DBs
CASTOR
CERN Advanced STORage manager
21 Production DBs
4 Development DBs
Middleware
73 Application Servers
Administrative/IT/
Engineering Databases
17 Production DBs
11 Development DBs
4 Ref/Test DBs
Accelerators
ACC
12 Production DBs
IT/DB GROUP
LHC Operations
PARTNERS:
CERN openlab
ORACLE

List of Figures

1.1 CERN members and observers 3

1.2 hierarchy at CERN 4

1.3 WLCG infrastructure 5

2.1 Relation between monitoring templates and targets 8

2.2 Oracle Enterprise Manager Grid Control main page 9

2.3 Explosion of policy violations 9

2.4 Policy violations: page in Enterprise Manager 10

2.5 Policy violations: contents of MGMT$POLICY_VIOLATIONS_CURRENT 10

2.6 Policy violations by target type (table) 11

2.7 Policy violations by target type (chart) 11

2.8 Policy violations by category (table) 11

2.9 Policy violations by category (chart) 11

2.10 Most common violation 12

3.1 policy violation and corrective action process 14

3.2 Preferred credentials page 15

3.3 Monitoring templates page 15

3.4 Policies assignment to a template 16

3.5 definition of new corrective action for a policy 16

3.6 corrective action : scripting page 16

3.7 Monitoring template : apply page 17

3.8 Overview of compliance tab without policy violations 17

3.9 Overview of compliance tab with policy violations 18

3.10 Overview of succeeded corrective action 18

3.11 sqlplus : result of corrective action 19

3.12 Compliance tab : return to normal state 19

4.1 Notification rules : internal mechanism 21

4.2 New grouping model 22

Bibliography

[1] M.New, “Oracle Enterprise Manager 10g Grid Control Implementation Guide”

[2] H.Meinhard, “Physics Computing at CERN” *openlab summer student lecture*, July 2010

[3] R.Jurga, “Size and complexity of CERN network” *openlab summer student lecture*, July 2010

[4] M.Schulz, “Worldwide LHC Computing Grid overview” *openlab summer student lecture*, August 2010

[5] `http://www.cern.ch`

[6] `http://www.gridcafe.org`