

## 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

#### 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	CER	N 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	Theo	orical 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	Impl	lementation 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	Noti	fication rules and target grouping	21
	4.1	How notification rules works?	21
	4.2	New grouping of targets	22
An	nexes	5	23
Lis	st of fi	gures	28
	bliogr		30
DU	undal	apuy	50

Contents

# **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).

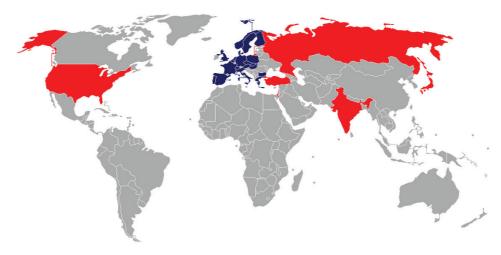


Figure 1.1: CERN members and observers

### **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<sup>2</sup>) 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.

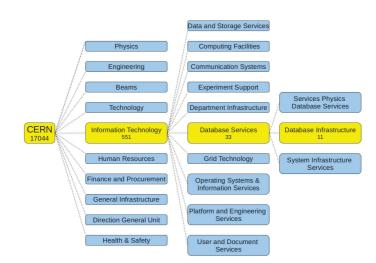


Figure 1.2: hierarchy at CERN

#### **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:

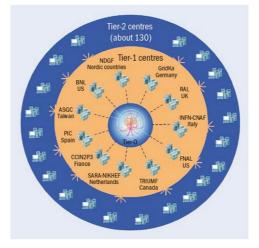


Figure 1.3: WLCG infrastructure

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<sup>1</sup> 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.

<sup>&</sup>lt;sup>1</sup>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.

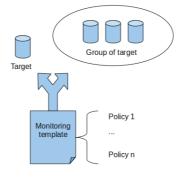


Figure 2.1: Relation between monitoring templates and targets

## 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.

		Page Refre	shed Jul 13, 2010 4:52:24 PM M
View All Targets	Target Search		
erview	Search All	G	5
al Monitored Targets 1276			
Targets Status	Security Policy Violations		
angets Status	Critical × 3925		
4%	Warning 1 12998		
8%	Informational 1090		
Down(49)	New in Last 24 Hours 772		
Unknown(96)			
88% Up(1,033)	Critical Patch Advisories for Oracle Homes		
	Patch Advisories 1		
	Patch Advisory Info My Cracle Support refer	rmation may be stale. esh job has not run successfull	uip 72 bours
Fargets Alerts	Affected Oracle Homes 15	con jou nas not run successiui;	y 11 7 2 1000 6.
ritical × 604	Job RefreshFromMyOra	eleSupport	
iming 🦺 <u>4654</u> Firons 🛃 914	Soo <u>remean ronniyon</u>	Kana Juppon	
Fargets Policy Violations	Deployments Summary		
Critical × <u>3939</u> Warning A 13087	View Database Installations		
Informational i 2045	Software Targets Without Inventory:7 of 204		Collection Problems
ken Corrective Actions 24	- Solution Internet Internet		Interim Patch
Targets Jobs	Database Installations 🛆	Targets	Installations Applied
Problem Executions (last 7 days)  v 0	Oracle Database 10g 10.2.0.3.0	0	<u>1 Yes</u>
ion Required Executions (last 7 days) 🗸 0	Oracle Database 10g 10.2.0.4.0	188	<u>178 Yes</u>
Suspended Executions (last 7 days) </td <td>Oracle Database 10g 10.2.0.5.0</td> <td>5</td> <td><u>5 No</u></td>	Oracle Database 10g 10.2.0.5.0	5	<u>5 No</u>
	Oracle Database 11g 11.1.0.7.0	2	2 Yes
	Oracle Database 11g 11.2.0.1.0	2	3 No
	Oracle9i 9.2.0.7.0 Oracle9i 9.2.0.8.0	0	2 Yes
		0	4 Yes
	0100001012101010		
	Resource Center		
	Resource Center	Mu Ornala S	Tunnert
	Resource Center Enterprise Manager Support Workbench	My Oracle S	
	Resource Center		Support Inology Network

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.

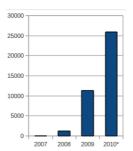


Figure 2.3: Explosion of policy violations

#### 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:

Violati	ons Library Associations Errors					
<b>▼</b> Simple	e Search					
Target Ty		nt Violation within	7 Days	V		
Target Na	me 🖉		Ignore suppressed via	lations		
Categ	ory All V					
Seve	rity All 🔻					
	Go Advanced Search					
						© Previous 1-25 of 227 ▼ <u>Next 2</u>
everity	Violation Count Policy	Target	Туре	Most Recent Violation $ abla$	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
4	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	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	CATEGOR
	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)
0			- 2	

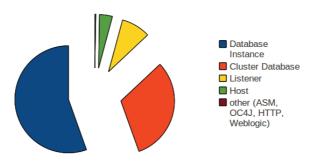


Figure 2.7: Policy violations by target type (chart)

#### Violations by category

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

Figure 2.8:	Policv	violations	by (	category	(table)
		11010010110	~	- megorj	(10010)

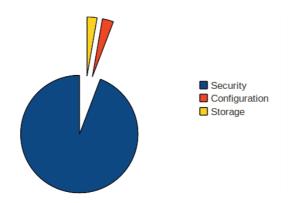


Figure 2.9: Policy violations by category (chart)

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<sup>1</sup> 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

<sup>&</sup>lt;sup>1</sup>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.

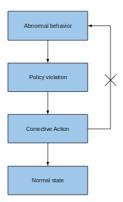


Figure 3.1: policy violation and corrective action process

## 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.
- "A corrective action is added to a target metric only if it is defined in the monitoring template when that template is *first* applied"<sup>2</sup>
   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.

<sup>&</sup>lt;sup>2</sup>Oracle Enterprise Manager 10g : Grig Control Implementation Guide

					lome Targets De	oloyments Ale	rts 丫 Compliar	ce Jobs	Reports My	/ Oracle Sup
references										
eferred Credentials >										
atabase Preferre	ed Credentials									
									Revert	Apply
o set preferred creden rivileges. Press Apply	tials for Database targets after making any change:	, update the appropriate fie s.	elds in one of the	tables below. To delete c	redentials, clear the appro	priate fields. The p	rivilege settings n	nust be already	set on the host ta	rgets to set I
		Enterprise Manager function utdown operations. Host cr							s that access nor	i-open
efault Credentia	als									
efault credentials are	used for Database target	s that do not have credentia	als set in the Tar	get Credentials table belo	Ν.					
Jsername Pa	ssword SYSDE	BA Username	SYSDBA Passw	ord Host User	name Host Pass	word Run	as I	Profile	Run Privileo	e
									None	0
		abase target. If set, target c	redentials overrie	de the default credentials i	for that target.					
arget credentials can b		abase target. If set, target c	redentials overrie	de the default credentials i	for that target.					
arget credentials can b earch			redentials overrie Password	de the default credentials SYSDBA Username	for that target.	Host Username	Host Passwo	ord Run as	Profile	Tes
arget credentials can b earch	be specified for each Data		T			Host Username	Host Passwo	ord Run as	Profile	
Target Credentia arget credentials can b search Name A	be specified for each Data		T			Host Username	Host Passwo	ord Run as	Profile	Tes
arget credentials can be	be specified for each Data		T				Host Passwo	ord Run as	Profile	
arget credentials can b earch	be specified for each Data		T			Host Username	Host Passwo	ord Run as	Profile	Tes
arget credentials can b earch	be specified for each Data		Password		SYSDBA Password			rd Run as	Profile	
arget credentials can t earch [ lame △	be specified for each Data		Password		SYSDBA Password			rd Run as	Profile	
arget credentials can t earch [ lame △	be specified for each Data		Password	SYSDBA Username	SYSDBA Password	oracle		ord Run as	Profile	
arget credentials can b earch	be specified for each Data		Password	SYSDBA Username	SYSDBA Password	oracle		Run as	Profile	Tes
arget credentials can b earch [ lame △ elated Links	be specified for each Data		Password	SYSDBA Username	SYSDBA Password	oracle		rd Run as		

Oracle is a registered trademark of Oracle Corporation Other names may be trademarks of their respective ow <u>About Oracle Enterprise Manager</u>

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:

 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.

Monito	oring Terr	plates				
					Page Re	freshed Aug 2, 2010 2:07:42 PM CEST Refresh
		s can be used to apply a subset of moniton ng settings not specified in the template		This allows you to	standardize monitoring ac	ross your enterprise. When a template is applied to
Sim	ple Search					
Temp	plate Name		Go Advanced Search			
Т	Target Type	All				
		Display Oracle provided templates				
	Apply Opera		are Settings)   (Create ) (Set Default Te	mplates )		
Select N	lame 🗸	Target Type	Pending Apply Operations	Owner	Last Modified By	Last Modified
۲	TEST_MT	_3 Database Instance	0	ABECHE_SU	ABECHE_SU	Aug 2, 2010 2:03:57 PM CEST
0	TEST_MT	2 Database Instance	0	ABECHE SU	ABECHE SU	Aug 2, 2010 2:01:58 PM CEST

🛱 Default Template for a target type. This template will be applied automatically to newly discovered targets in Enterprise Manager.

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.

#### 3.2. Corrective actions set up

	General Metric Thresholds Policies Access						
	ble allows you to add and customize policies associated with this templa	ate.					
-	move from Template)   (Add Policies to Template)						
	t All Select None		-				
	Policy 🛆	Severity	Category	Collection Schedule	Description	Disabled	Ed
	Access to ALL_SOURCE View	Informational	Security		Ensures restricted access to ALL_SOURCE view		6
	Access to DBA_ROLES View	Informational	Security		Ensures restricted access to DBA_ROLES view		1
	Access to DBA_ROLE_PRIVS View	Informational	Security		Ensures restricted access to DBA_ROLE_PRIVS view_		/
	Access to DBA_SYS_PRIVS View	Informational	Security		Ensures restricted access to DBA_SYS_PRIVS view ①		1
	Access to DBA_TAB_PRIVS View	Informational	Security		Ensures restricted access to DBA_TAB_PRIVS view ①		6
	Access to DBA_USERS View	Informational	Security		Ensures restricted access to DBA_USERS view		l

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

Corrective Action	
In case of violation, the corre	ective action, if specified, is automatically executed.
Corrective Action CA	ALL_SOURCE (Remove)
	Prevent multiple executions of this corrective action from running simultaneously for the same violation.

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.

* SQL Script		Target Properties	
	%context_value_grantee%;	Target properties can be used in	
		Property names are case-sensitiv Name	Description
		%emd root%	location of Agent
		96perIbin96	location of Perl binary used by Agent
		%TargetName%	target name
	Enter SQL or a fully qualified script name on the remote hosts, for example, "@script".	%TargetType%	target type
Parameters		% orcl gtp line of bus%	Line of Business
	Enter optional parameters to SQL*Plus.	%orcl gtp location%	Location
		%orcl gtp deployment type%	Deployment Type
		%orcl gtp comment%	Comment
			L% Database Vault Administrator URL
		%orcl gtp contact%	Contact
		%OracleHome%	Oracle home path
		96Bole96	Bole
		%MachineName%	Listener Machine Name
		%Port%	Port
		96SID96	Database SID
		%DBVersion%	Version
		96policy96	policy rule for which the violation has been triggered
		%timestamp%	time of the alert or violation; format is DD-MON-YY HH24:MM (14-Jun-05 13:50)
		%severity%	severity level of the alert or violation
		%key_value_grantee%	monitored object for which the alert or violation has been triggere
		%key value privilege%	monitored object for which the alert or violation has been triggere
		%context_value_grantee%	value of a related metric in the alert or violation context
		%context value privilege%	value of a related metric in the alert or violation context

Figure 3.6: corrective action : scripting page

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

		(Cancel) Continue
urce Template TEST_MT_3 Target Type Database Instance Owner ABECHE_SU		
Apply Options		
O Template will completely replace all metric settin Applying the template removes the thresholds of the metrics to	ngs in the target. This disables alert in the target, but not included in the template. This disables alert functionality for these metrics. Metric data will continue	e to be collected.
<ul> <li>Template will only override metrics that are com</li> </ul>	inon to both template and target.	
Destination Targets	e targets to which this monitoring template will be applied	
The table below shows the list of Database Instance	e targets to which this monitoring template will be applied.	
	e targets to which this monitoring template will be applied.	
The table below shows the list of Database Instance Remove   Add	e targets to which this monitoring template will be applied. Type	_
The table below shows the list of Database Instance           Remove         Add         Add         Select All         Select None         Select None		

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.

ORACLE Ente	erprise Manager				Home	argets Deployments	Alerts Compliance Jobs Report	Setup Preferences Help Logout
	Groups   Security At a Gland	ce			Tione	argets Deproyments	report	s my ordere support
(i) Search S No Search F	Status Results found matching the cri	teria specified.						
Policies: Viol	lations							
Violations	Library Associations	Errors						
The following tabl	e displays a rollup of policy vi earch	olations. For detail informa	tion click on the	violatio	on count link.		Page Refreshed Aug 9,	2010 10:30:40 AM CEST
Target Type Target Name Category Severity		S Most Recent Vi		6 ☑ Ignoi	Days \$			
Severit (No results)		Its Policy	Target T	уре	Most Recent Violation	Category	Compliance Score (%) Non-Comp	pliant Since
Violations	Library Associations	Errors						
Oracle is a registered to Other names may be tr	b, Oracle and/or its affiliates. All rights rademark of Oracle Corporation and/or rademarks of their respective owners.		nents   <u>Alerts</u>	<u>Compl</u>	liance   Jobs   Reports   My C	Dracle Support   Setup   Pre	eferences   Help   Logout	

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

Violations	Library Associations Errors					
he following tabl	e displays a rollup of policy violations. For detail information click on the violation	n count lini	k.			Page Refreshed Aug 2, 2010 2:10:43 PM CES
Simple Se	earch					
Target Type	Database Instance 3 Most Recent Violation within 7		Days 🗘			
Target Name		e suppress	sed violations			
Category						
Severity	All					
Severity						
Severity	All  Co Advanced Search					
	Go Advanced Search	Target	Туре	Most Recent Violation ▽	Category	Compliance Score (%) Non-Compliant Since
	Coo Advanced Search				Category Storage	Compliance Score (%) Non-Compliant Since 97 Jun 15, 2010 12:36:45 PM CES

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.

Target Name		Target Type Da	tabase Instance			
is page shows objects in violation of this policy. Suppres	s the violations that you do not	want to be included in the list of policy violation	ons. L	ast Evaluation Aug 2, 2010 2:08:43 PM CES		
General		Objects w	ith Violations			
Severity A Compliance Score (%) 76 Importance Normal Category Security		Objects wi	Objects with Violations 3 Objects with Suppressed Violations 0			
Description Ensures SELECT ANY PRIVI	EGE is never granted to any	user or role 💷				
Impact of Violation		Recomme	endation			
The SELECT ANY TABLE privilege can be used to gran tables that are not owned by them. A malicious user with can use this to gain access to sensitive data.			t SELECT ANY TABLE privilege.			
Violations						
View Violations						
(Add Comment) (Suppress Violation)						
Select All Select None						
Select Path	Grantee	Non-Compliant Since ▽	Automated Corrective Action Status	Comments		
SELECT ANY TABLE->ABECHE	ABECHE	Aug 2, 2010 2:08:43 PM CEST	Succeeded	Θ.		

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%

				Page Refreshed Aug	10.2010 9:21:23 AM	CES
				View Data	Manual Refresh	0
Exit	Status Succeeded Code 0 tep ID 338196 argets	Ended Step Elapsed Time Management Service	Aug 10, 2010 9:20:55 AM GMT+02:00 Aug 10, 2010 9:20:55 AM GMT+02:00 0 seconds m which the job step was dispatched.	Ten Dau	mandariterean	
Output Log						
SQL> SQL> SQL> S SQL> SQL> SQL> S Revoke succeeded	GQL>					
	isconnected from Oracle	e Database 10g Enterprise Edition	Release 10.2.0.4.0 - 64bit			
Production						

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.

) Search S		d matching the actuals appeals							
		d matching the criteria specifie	ed.						
olicies: Viola	ations								
Violations	Library	Associations Errors							
e following table	e displays a i	rollup of policy violations. For	r detail informatio	on click on th	ne violat	tion count link.		Page Refre	eshed Aug 9, 2010 11:24:17 AM CEST
Simple Sea	arch								
Target Type	Database I	Instance 🔷 N	lost Recent Viol	ation within	6	Days 🗘			
	group and the second s								
Target Name		3			🗹 Ign	ore suppressed violations			
Target Name Category	All	0			✓ Ign	ore suppressed violations			
-	All				✓ Ign	ore suppressed violations			
Category Severity	All	0			🗹 Ign	ore suppressed violations			
Category Severity	All Go Advar	I Cearch			⊠ Ign				
Category Severity Severity	All Go) <u>Advar</u> y	¢   ¢	Policy	Target	✓ Ign	ore suppressed violations Most Recent Violation	Category	Compliance Score (	%) Non-Compliant Since
Category Severity	All Go) <u>Advar</u> y	I Cearch	Policy	Target			Category	Compliance Score (	%) Non-Compliant Since

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:

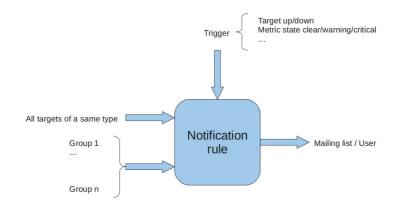


Figure 4.1: Notification rules : internal mechanism

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.

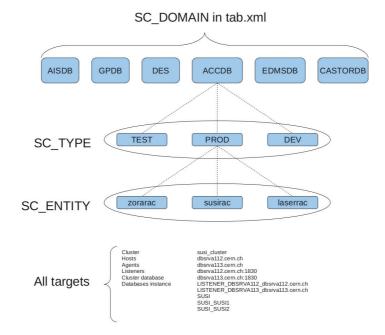
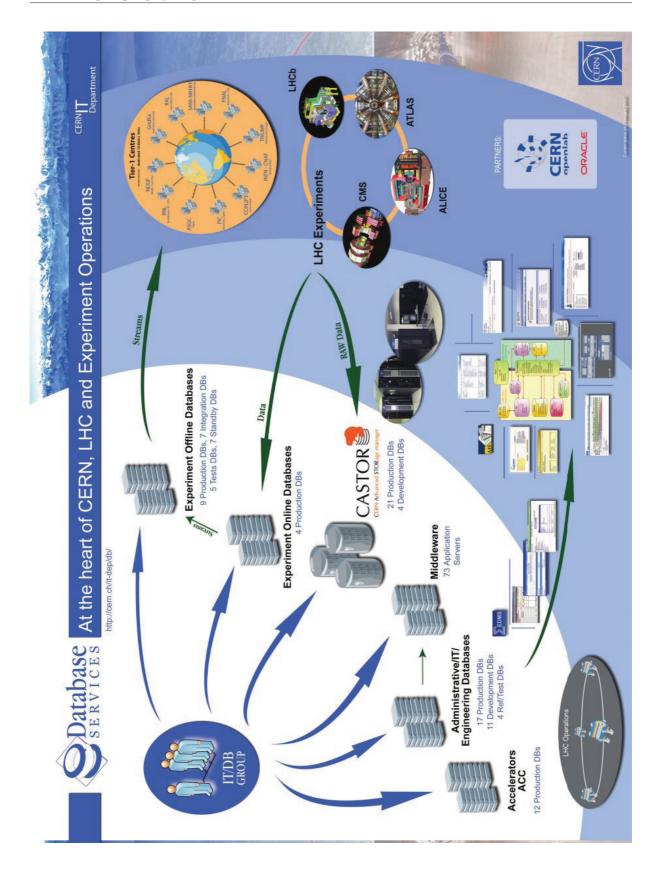


Figure 4.2: New grouping model

# Annexes



# **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
anlah	Like August 2010	20

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