



Desenho da Solução

84137 - PROJETO SINERGIA Oi-PT [RA]: Serviços de Instalação da Solução de RA



Histórico

Versão	Referência	Autor	Data Execução	Comentários
1.0	BRA14POI02500	WeDo Technologies	25/02/2014	Versão Inicial
2.0	BRA14POI02500	WeDo Technologies	26/02/2014	Ajuste na Descrição do Portal
3.0	BRA14POI02500	WeDo Technologies	28/02/2014	Ajuste Desenho de Infra do Portal (A solução passará a ter apenas um portal), Incluir a Rastreabilidade dos RQF's e RQNF's
4.0	BRA14POI02500	WeDo Technologies	12/03/2014	Ajuste na descrição do documento conforme o RQF's
5.0	BRA14POI02500	Wedo Technologies	14/03/2014	Inclusão requisitos de segurança
6.0	BRA14POI02500	Wedo Technologies	20/03/2014	Inclusão das informações de volumetria e housekeeping





Aprovação

Departamento	Nome	Função	Date de Aprovação



Índice

1	Introdução	5
1.1	OBJETIVO.....	5
1.2	ÂMBITO	5
1.3	REFERÊNCIAS.....	5
1.4	DEFINIÇÕES.....	5
2	Desenho da Solução.....	7
2.1	VISÃO GERAL DA SOLUÇÃO	7
2.2	REQUISITOS DA APLICAÇÃO	9
2.3	REQUISITOS DO AMBIENTE	10
2.4	REQUISITOS DE BANCO DE DADOS	11
2.5	REQUISITOS DE SISTEMAS OPERACIONAIS	11
2.6	REQUISITOS DE REDE.	12
2.7	REQUISITOS DE VOLUME	12
2.8	REQUISITOS DE SEGURANÇA.....	12
2.9	REQUISITOS DE MANUTENÇÃO E LIMPEZA	12
3	Desenho Detalhado	13
3.1	RAID INTEGRIDADE (PI).....	13
3.1.1	Features – Carregamento	14
3.1.2	Features - Validação	14
3.2	RAID TRÁFEGO (UC).....	15
3.2.1	Features - Carregamento.....	16
3.2.2	Features - Validação.	17
3.3	INTERFACES DE USUÁRIO.	17
3.3.1	PORTAL.....	18
3.3.1.1	Smart Contents.....	19
3.3.1.2	Consultas/Data Lists.....	23
3.3.1.3	Case Management.....	23
3.3.2	RAID Admin.....	24
3.3.2.1	System management	25
3.3.2.2	Loading management	25



3.3.2.3	Validations management	26
3.3.2.4	Alarms management	28
3.3.2.5	Session management, authentication and authorization	28
4	Anexos	30

1 Introdução

1.1 Objetivo

Este documento tem como objetivo especificar o modo que o novo sistema de garantia de receita RAID 7 será instalado nos módulos UC (controle de tráfego) e PI (integridade de plataforma) e as configurações necessárias no ambiente de PORTAL e BANCO DE DADOS.

Este documento inclui:

- Especificações funcionais e desenho dos módulos.
- Requisitos funcionais adicionais da aplicação.
- Desenho detalhado dos módulos envolvidos.

1.2 Âmbito

O âmbito deste documento refere-se à exposição dos conceitos, requisitos e funcionalidades necessários à implantação da solução RAID 7 para o projeto Revenue Assurance para Oi.

1.3 Referências

Lista de documentos utilizados para elaboração deste documento:

- IMN_RAID_001_E - RAID 7.0 - Installation Manual.pdf
- STI 84137 - Visão Macro Solucao_v1 2.pptx
- PRS_RAID_7.0_PLATFORM_INTEGRITY.pptx
- PRS_RAID_7.0_USAGE_CONTROL.pptx
- PRS_RAID_7.0_What is New.pptx

1.4 Definições

A tabela a seguir lista respectivamente os acrônimos e os termos utilizados no corpo do documento.

Acrônimos & Definições

Acrônimo	Definição
AF	WeDo Consulting's Application Framework
API	Application Programming Interface
AB	Application Browser
BPM	Business Process Manager
CM	Case Management Module
GUI	Graphical User Interface
IM	Integration Module
JAF	Java Application Framework
JVM	Java Virtual Machine
OS	Operating System
PI	Platform Integrity Control Module
RAID	Revenue Assurance Integrity Driller
RAS	Revenue Assurance
RFD	Revenue Flow Detailed Design Document
UC	Usage Control Module



CDR	Call Detail Record
CSM	Context Search Manager (data browsing)
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity (an internal subscriber identity used only by the network)
IN	Intelligent Network
KPI	Key Performance Indicator
MSC	Mobile Switch Centre
MSISDN	Mobile Station International ISDN Number
EMM	Ericsson Mediator Mobile
OPSC	Prepayd Platform
IN	Intelligent Network

Tabela 1: Acrônimos & Definições.

2 Desenho da Solução

Neste capítulo, será descrito o desenho geral da solução, bem como os requisitos gerais de aplicação, ambiente, sistema operacional, rede, volume e segurança.

2.1 Visão Geral da Solução

Essa demanda tem como objetivo, instalar no ambiente da Oi a nova ferramenta de garantia de receita RAID 7.

Serão implantados os módulos de integridade de plataforma (RAID 7 PI) e o controle de tráfego (RAID 7 UC) .

Nessa nova solução os módulos UC e PI irão absorver as soluções de garantia de receita existentes Oi.

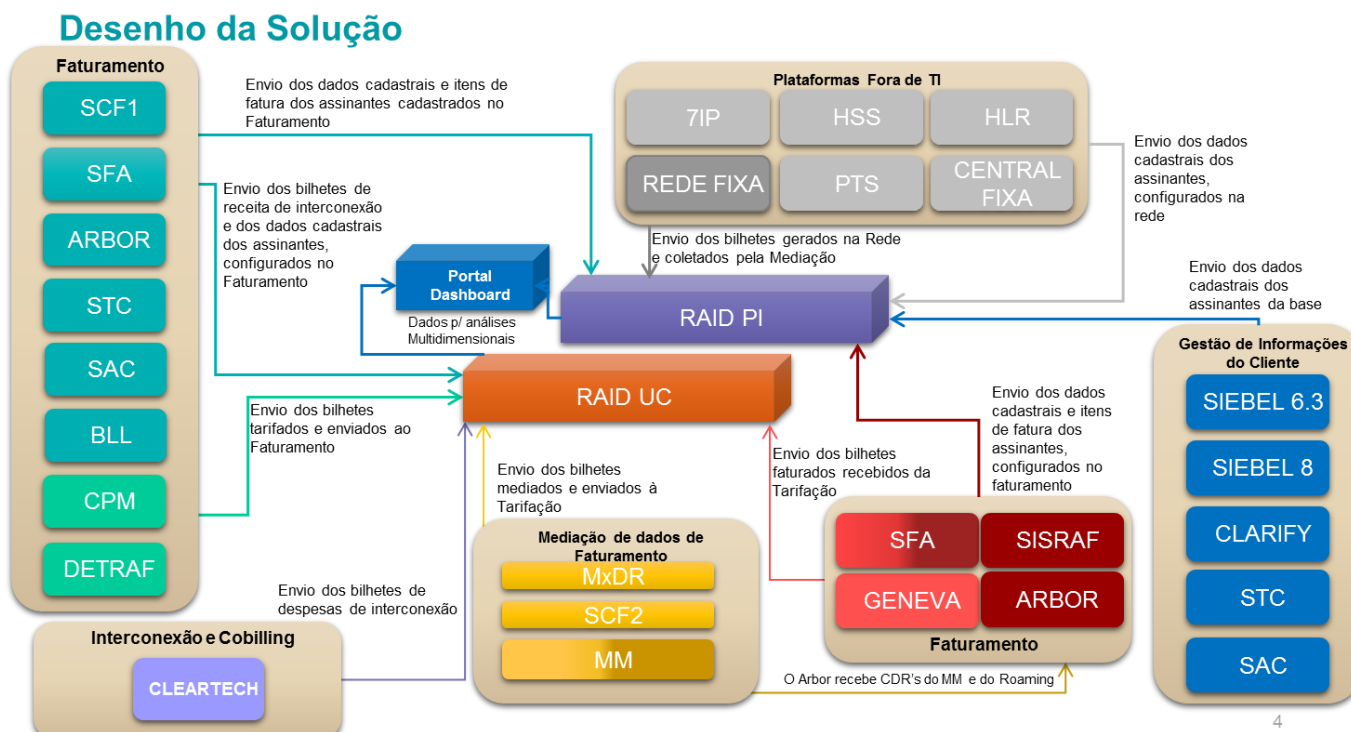
RAID INTEGRIDADE (PI) irá absorver os seguintes sistemas :

- RAID IP MÓVEL – Clientes Oi Móvel da R1 e R3.
- RAID IP FIXA – Clientes Oi Fixa da R1 e R3.
- RAID PI – Clientes Oi Móvel e Fixa da R2 .

RAID TRÁFEGO (UC) irá absorver os seguintes sistemas :

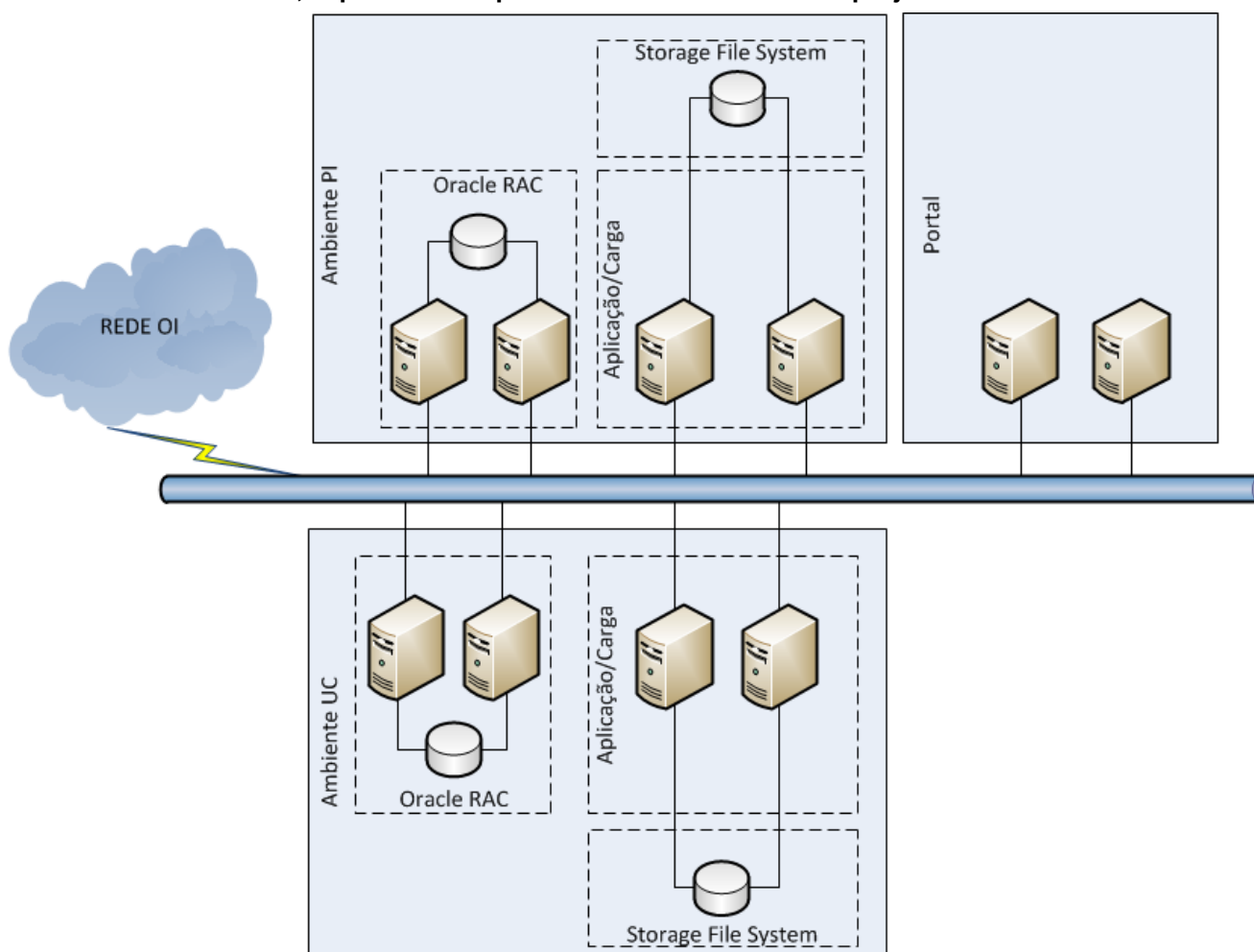
- RAID RC – Tráfego de CDR's da R2
- RAID EC – Tráfego de CDR's da R2
- RAID FR – Tráfego de CDR's da R1 e R3
- RAID MARGEM – Tráfego de CDR's da R1,R2 e R3
- RAID ECDR – Tráfego de CDR's da R1, R2 e R3

O desenho abaixo, especifica o fluxo de informações de entrada e saída do PI e UC na Oi:



Os detalhes das interfaces de integração com o RAID PI e RAID UC estão especificados no documento #9 (anexos).

O desenho abaixo, especifica a arquitetura de infraestrutura do projeto:



PORTAL

Produção Portal – Qtde .02

- Server : RAUPX01A
- Server : RAUPX01B

RAID UC

Produção App – Qtde .02

- Server : RAUPX02A
- Server : RAUPX02B

Produção BD – Qtde .02

- Server : RAUPX03A
- Server : RAUPX03B

Homologação App – Qtde .01

- Server : RAUHX01

**Homologação BD – Qtde .01**

- Server : RAPHX02B

Desenvolvimento App – Qtde .01

- Server : RAPDX01

Desenvolvimento BD – Qtde .01

- Server : RAPDX01

RAID PI**Produção App – Qtde .02**

- Server : RAPPX02A
- Server : RAPPX02B

Produção BD – Qtde .02

- Server : RAPPX03A
- Server : RAPPX03B

Homologação App – Qtde .01

- Server : RAPHX01

Homologação BD – Qtde .01

- Server : RAPHX02A

Desenvolvimento App – Qtde .01

- Server : RAPDX01

Desenvolvimento BD – Qtde .01

- Server : RAPDX01

Hardware de Produção:

As especificações completas de hardware em todos os ambientes estão definidas no documento #01 (anexos).

2.2 Requisitos da Aplicação

- Implantação da solução de integridade de plataforma RAID 7 INTEGRIDADE (PI).
- Implantação da solução de controle de tráfego RAID 7 TRÁFEGO (UC).

Obs: O detalhamento de cada solução está especificado no item 3 (Desenho Detalhado).

2.3 Requisitos do Ambiente

Os requisitos devem ser aplicados nos ambientes de produção, homologação e desenvolvimento do RAID PI e RAID UC.

Para a disponibilização do ambiente necessitamos dos seguintes softwares instalados.

Requisitos do Ambiente

Product	Version/Comments
Oracle Server 11.2 with Partitioning option	Latest version License must be acquired separately SQLLoader tool must be available in the environment when xDR archiving tools are used
Oracle Client 11.2	Latest version SQLLoader tool must be available in the environment when xDR archiving tools are used
JRE 1.7	Latest version. Only SUN™, HP™ and IBM™ VMs are certified to work with the product.
Bash shell	Version 3.2.25
GNU tar utility	Latest version
SFTP utility	Latest version
GCC	GCC/GCC-C++/LIBSTDC++ - According to the table below.

Tabela com as versões de GCC necessárias conforme OS/versão

Product	Version/Comments
Suse Enterprise Linux 11 SP1 – X86-64	4.3.2
Redhat Enterprise Linux 6 – X86-64	4.4.5
Oracle Enterprise Linux 6 – X86-64	4.4.6
Oracle Solaris 10 – SPARC	3.4.3
Oracle Solaris 10 – X86-64	3.4.3 / 3.4.6
Oracle Solaris 11 – SPARC	3.4.3
Oracle Solaris 11 – X86-64	4.5.2
HP-UX 11.31 – IA64	4.2.3 / 4.4.0
IBM AIX 6.1, 7.1 – PPC64	4.2.0

Requisitos Windows Client

Product	Version/Comments
Microsoft Windows XP	(SP3 recommended)
Microsoft Windows 7	(32 & 64 bits)

Requisitos Web Client

Product	Version/Comments
Desktop web browsers:	
Microsoft Internet Explorer	IE 9 (32-bit version) or greater for Windows
Safari	Versão 6 Mac OSX Lion

Chrome	24 or greater for Windows
Tablet web browsers:	
IOS – Safari	Versão 5
Android – Chrome	16+
Android – Navigator	4+

O espaço de swap do servidor deve ser configurado conforme a tabela abaixo:

RAM	Swap Space Required
Entre 1 GB e 2 GB	1.5 vezes o tamanho da RAM
Entre 2 GB e 16 GB	Igual a RAM
Mais de 16 GB	16 GB

Os seguintes usuários e grupos precisarão ser criados e, todos os ambientes do PI e UC:

User	Group	Description	Home dir	Shell	umask
Raid	raid	Usuário do aplicativo para ambiente de Produção/Homologação/Desenvolvimento	/apps/raid	bash	007

File System

User	FS
Raid	/apps/data

2.4 Requisitos de Banco de Dados

Os requisitos devem ser aplicados nos ambientes de produção, homologação e desenvolvimento do RAID PI e RAID UC.

Os requisitos de banco dados referente ao ambiente Oracle, tablespace e parâmetros de SGBD estão definidos nos documentos #03 e #04.

2.5 Requisitos de Sistemas Operacionais

Os requisitos devem ser aplicados nos ambientes de produção, homologação e desenvolvimento do RAID PI e RAID UC.

Os sistemas operacionais homologados para instalação são:

Sistema Operacional para Aplicação

Operating System	Architectures	Version/Comments
Redhat Enterprise Linux	X86-64	6.0 / 6.1 / 6.2 / 6.3 / 6.4

Sistema Operacional para Banco de Dados

Operating System	Architectures	Version/Comments
Oracle Solaris	SPARC / X86-64	10 / 11
Oracle Linux	X86-64	6.0 / 6.1 / 6.2 / 6.3 / 6.4
Redhat Enterprise Linux	X86-64	6.0 / 6.1 / 6.2 / 6.3 / 6.4
Suse Enterprise Linux	X86-64	11 SP1
HP-UX IA64	IA64	11.31

2.6 Requisitos de Rede.

Os requisitos devem ser aplicados nos ambientes de produção, homologação e desenvolvimento do RAID PI e RAID UC.

Todas as portas utilizadas pelo projeto devem estar abertas no firewall, conforme abaixo:

Portas e serviços – Aplicação	
Host	Portas
SFTP	22
SSH	22
WebService (HTTP e HTTPS)	8005, 8080, 8090, 443, 8443
RAID	15000 – 15099
Portas e serviços – Oracle	
Host	Portas
SFTP	22
SSH	22
Oracle	1521 - Pode ser alterada pela Oi, desde que a Wedo seja notificada.

2.7 Requisitos de Volume

A especificação de volumetria para os ambientes de produção, homologação e desenvolvimento estão especificados nos documentos #01.

Estimamos que o ambiente de tráfego vá manipular uma média de 3 bilhões de registros, com picos de 4 bilhões, por dia. Para o ambiente de Integridade vá manipular 1 bilhão de registros por dia.

Os dados brutos utilizados para reconciliação, estarão disponíveis para consulta por 7 dias. Cada dia adicional, representa em um acréscimo de 500Gb no cluster filesystem do servidor de aplicação.

2.8 Requisitos de Segurança

Os detalhes referentes aos requisitos de segurança estão especificados no documento #05 (anexos).

2.9 Requisitos de manutenção e limpeza

O ambiente terá a política de housekeeping, de banco de dados e filesystem, definida em cada etapa do projeto. Cada etapa possui uma característica específica de retenção dos dados históricos e on-line.

3 Desenho Detalhado

Os requisitos funcionais relativos aos sistemas RAID PI e RAID UC estão especificados no anexo #05.

Modelagem lógica de dados referente à arquitetura do RAID PI e RAID UC está definida no anexo #02.

3.1 RAID INTEGRIDADE (PI)

A perda de receitas ocorre quando a ativação ou alteração de procedimentos de serviço do cliente têm algum tipo de problema, seja ela operacional, devido a erros humanos, ou devido a falhas no sistema. Nestes casos, a consistência da informação que está armazenada em diferentes bases de dados de diversos sistemas e plataformas, pode ser seriamente comprometida. Esses problemas poderiam ser, por exemplo:

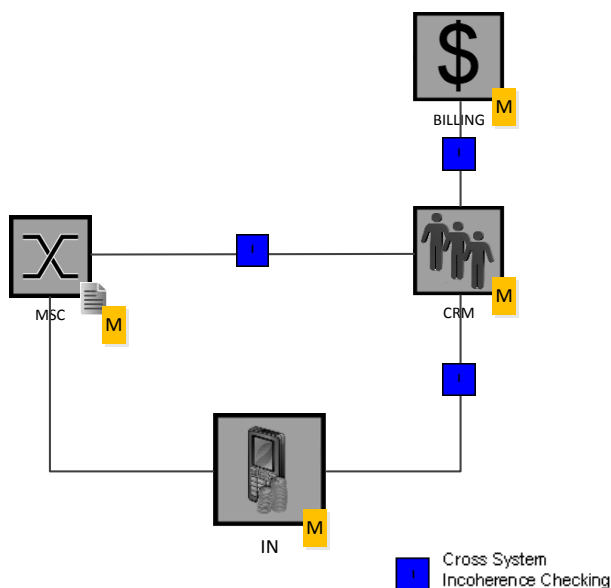
- Clientes ativos sem a emissão de faturas;
- Clientes registrados como Pré-pago e Pós-pago;
- Serviços faturados de forma de forma errada;
- Serviços ativados com clientes ativados.

Para garantir que essas situações não ocorram, a Oi irá atualizar os processos existentes de Revenue Assurance para nova solução RAID7 PI, com foco na validação periódica da consistência das informações dos assinantes nas plataformas CRM, Pré-pago plataforma de rede e Faturamento, permitindo a identificação e posterior à correção de problemas.

Esta atividade é uma medida preventiva importante, que tem um efeito positivo não só sobre a cadeia de receita, assegurando que todos os serviços são cobrados, mas também contribuindo para a excelência no atendimento e satisfação do cliente.

Periodicamente o RAID PI, coletará informações sobre os serviços e o cadastro dos assinantes disponíveis através do seu processo de integração e carregamento de dados. Após o carregamento de todas as interfaces o sistema RAID PI, executará o seu processo de validação que através de regras de negócio irá permitir a detecção de inconsistências de dados nas plataformas.

Exemplo padrão de integridade de plataforma.

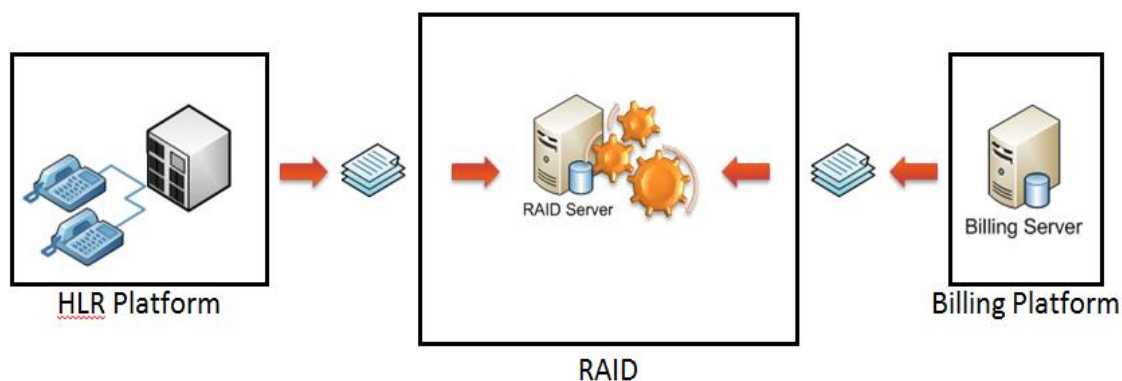


3.1.1 Features – Carregamento

(Requisitos Atendidos: RQF006)

O carregamento é um processo ETL que de forma periódica, coleta e grava no RAID as informações de serviços e cadastros dos clientes das plataformas CRM, pré-pago, rede e faturamento.

Exemplo:



O processo de ETL do RAID é elaborado através de fluxos de carregamentos.

O fluxo de carregamento prover as seguintes funcionalidades:

- Leitura de dados de diversas fontes (ascii, csv, ebcdic, ODBC, XML, hlr);
- Enriquecimento de informações utilizando operadores lógicos;
- Enriquecimento de informações utilizando Lookups Tables;
- Controle de Erro de processamento;
- Agregação de Dados em banco de dados;
- Agregação de Dados em Arquivo físico;
- Gravação simples de Dados em banco de dados;
- Gravação simples de Dados em arquivo físico;

3.1.2 Features - Validação

(Requisitos Atendidos: RQF003, RQF009, RQF011, RQF012, RQF013, RQF014, RQF024, RQF025, RQF033)

A validação é um processo do RAID baseado em regras de batimentos, definidas pelo usuário de R.A. que visam à identificação de forma automática de inconsistências de dados entre as plataformas.

Exemplo :

Billing system

MSISDN	...	Package ID	...
+35387111111	...	Super Save	...
+35387222222	...	Super Save	...
+35387333333	...	Personal	...

Mismatch

Prepaid platform

MSISDN	...	Package ID	...
+35387111111	...	Super Save	...
+35387222222	...	Standard	...
+35387333333	...	My Personal	...

Mismatch

As regras de batimento e geração de alarmes são elaboradas através dos fluxos de validação do RAID.

O fluxo de validação prover as seguintes funcionalidades:

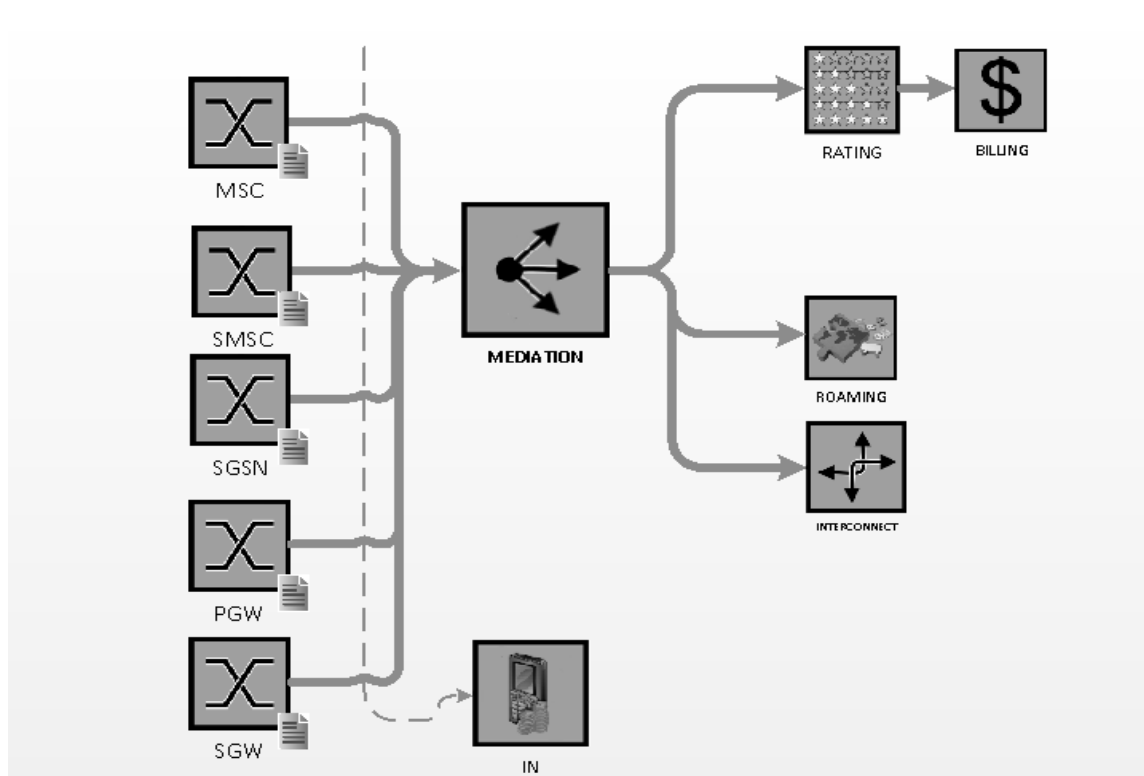
- Conciliar dados de diversas interfaces (ex: plataforma_a VS plataforma_b);
- Realizar qualquer cruzamento de dados desde que o tipo de informações exista entre as plataformas;
- Criar regras de existência de cadastro, serviços de clientes, elemento de rede, volumetria de dados, sequencial de arquivos, histórico de dados e arquivos, idade dos dados e regras que apoiam em tabelas de parâmetros com base em Kpi (utilizando como base da regra os valores de limites superiores, limites inferiores ou timestamp);
- Gerar alarmes de inconsistências de dados em banco de dados ou arquivos físicos com sequencial, por tipo de regra ou identificador de alarmes;
- Reconciliar informações agregadas ou não agregadas;
- Reconciliar dados respeitando a data e recebimento de arquivos no RAID;
- Reconciliar dados de acordo com fuso-horário de diversas regiões;

3.2 RAID TRÁFEGO (UC)

O RAID UC possibilitará a Oi a pontualidade e integridade dos fluxos de receita/despesa gerados desde elementos de rede até o fim da cadeia de faturamento. O sistema oferece uma perspectiva única sobre os fluxos de receita na rede, e se destina a ser utilizado por um departamento de garantia de receita proativo para detectar e resolver problemas relativo a desvio de receita.

RAID UC recolhe CDR's de voz e dados de clientes do fluxo de faturamento da operadora permitindo processar grandes volumes de dados em quase qualquer formato, incluindo telefonia fixa e móvel. Usando agentes de integração. O RAID UC é capaz de ler, processar, enriquecer e carregar os dados necessários para realização das validações de RA.

Exemplo:

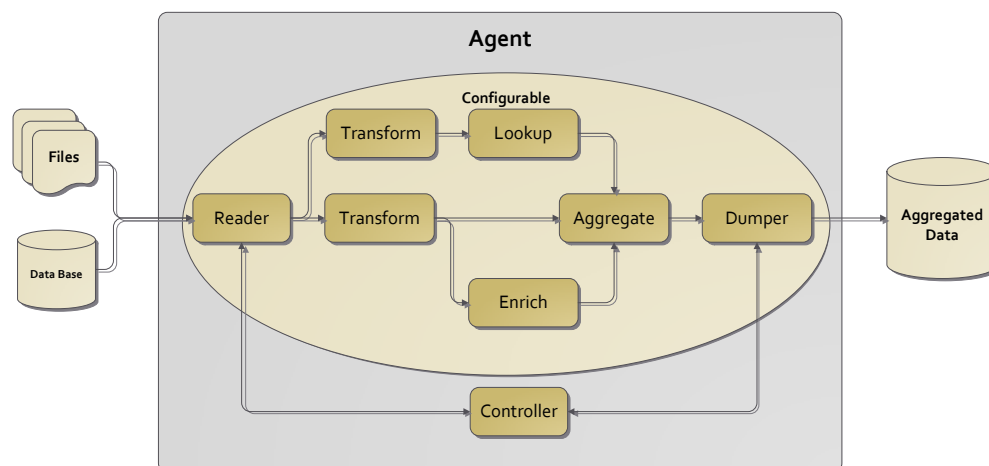


3.2.1 Features - Carregamento

(Requisitos Atendidos: RQF006)

RAID UC recolhe CDR's de voz e dados de clientes a partir das plataformas de OSS e BSS permitindo processar grandes volumes de dados.

Exemplo :



O processo de ETL do RAID é elaborado através de fluxos de carregamentos.

O fluxo de Carregamento prover as seguintes funcionalidades:

- Leitura de dados de diversas fontes (ascii, csv, ebcdic, ODBC, XML, hlr);
- Enriquecimento de informações utilizando operadores lógicos;
- Enriquecimento de informações utilizando Lookups Tables;
- Controle de Erro de processamento;
- Agregação de Dados em banco de dados;

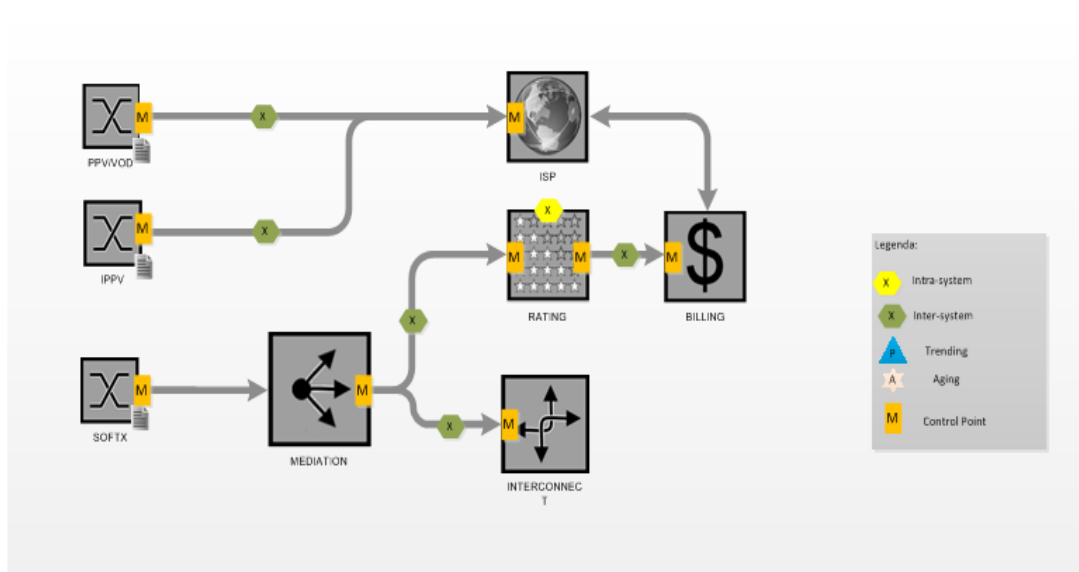
- Agregação de Dados em Arquivo físico;
- Gravação simples de Dados em banco de dados;
- Gravação simples de Dados em arquivo simples;

3.2.2 Features - Validação.

(Requisitos Atendidos: RQF003, RQF009, RQF011, RQF012, RQF013, RQF014, RQF024, RQF025, RQF033)

O processo de validação é um conjunto de regras de negócio, que permitem encontrar vazamentos de receitas de forma automática em toda cadeia de faturamento da Oi e assim gerando alarmes.

Exemplo:



As regras de batimento e geração de alarmes são elaboradas através dos fluxos de validação do RAID.

O fluxo de validação prover as seguintes funcionalidades:

- Conciliar CDR's entre pontos distintos;
- Criar regras de tendência, volumetria de dados, sequencial de arquivos, histórico de dados e arquivos, idade dos dados e regras quase apoiam em tabelas de parâmetros com base em Kpi (utilizando como base da regra os campos de limites superiores, limites inferiores ou timestamp);
- Gerar alarmes de inconsistências de dados em banco de dados ou arquivos físicos com sequencial, por tipo de regra ou identificador de alarmes;
- Reconciliar informações do CDR agregadas ou não agregadas;
- Reconciliar dados respeitando a data e recebimento de arquivos no RAID;
- Reconciliar dados de acordo com fuso-horário de diversas regiões;

3.3 Interfaces de usuário.

O Raid oferece a seguintes interfaces (GUI).

Portal - Projetado para o usuário configurar a lógica de negócio e exibições de dados.

RAID Admin - Possibilita projetar, configurar e executar fluxos de carregamento e validação

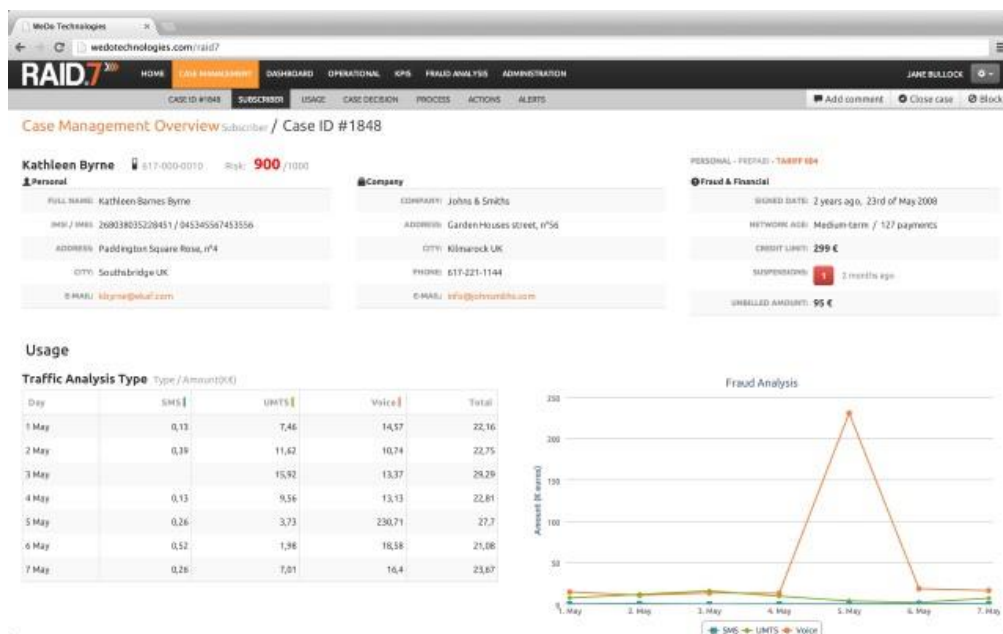
3.3.1 PORTAL

(Requisitos Atendidos: RQF001, RQF002, RQNF001)

O Portal é interface (GUI) de trabalho WEB destinada ao usuário de RA onde poderá acessar o RAID IP e RAID UC.

- Disponibiliza um conjunto completo de componentes de conteúdo inteligente capacitar os usuários acessem facilmente os dados e funcionalidades do produto, proporcionando uma experiência comum interface de usuário em todos os módulos do produto, garantindo uma aparência consistente;
- Permite aos utilizadores acesso a todas as fontes de dados e dados alarmados dos processos de reconciliação do RAID;
- Permite aos utilizadores do sistema personalizar a área de trabalho, assim podendo construir e compartilhar entre os utilizadores suas próprias telas, views e dashboards;
- Gerencia o logon único de usuários, independentemente do número de aplicações / módulos desenvolvidos;
- Oferece uma interface mais configurável.
- Permite ao usuário, que recebeu o treinamento adequado, criar contextos lógicos com isso o usuário poderá juntar em único contexto informações de várias fontes de dados (por exemplo, produtos diferentes ou módulos de um único produto) assim permitindo analisar, criar suas perspectivas e gerar consultas via componente Smart Contents do tipo simples e multidimensionais.
- Permite aos usuários exportar para meios físicos as informações obtidas nos Dashboards, KPI e Consultas e Data Lists. Através do Mashup **Smart Content** do Portal o usuário terá recurso de drag & drop para desenvolver seus charts, data listings e Kpi's, filtros e drill's.
- Permite aos usuários através do componente **Case Management** à gestão de quaisquer problemas, é possível encaminhar um alarme ou um grupo de alarmes para áreas responsáveis.

Exemplo:



3.3.1.1 Smart Contents

(Requisitos Atendidos: RQF016, RQF017, RQF018, RQF019, RQF020, RQF021, RQF022, RQF023, RQF07, RQF031, RQF032, RQF034)

Através área de trabalho Smart Contents que usuário poderá definir suas visões de dashboards e criar KPIs.

Será possível montar painéis dashboard com todos dados processados pelo RAID. Assim visualizando toda cadeia de receita ou pontos de controles distintos.

O portal permite, comparar por volumetria entre saída/ocorrência/entrada ou entre sistemas, volumetria por ponto de controle e comparação por receita entre saída/ocorrência/entrada ou entre sistemas.

O portal permite que o usuário realize drill down até o nível máximo de detalhe carregado.

Raid também tem um mecanismo de cálculo Métricas e KPIs. Os KPIs são usados para controlar o andamento, medir a integridade de um fluxo de receitas, destaque estatística de validação, rastrear um alvo negócio ou controlar um processo.

No Portal o usuário pode configurá-lo com suas próprias métricas, definindo o conceito de negócios que serão analisados e sua periodicidade. No topo, são aplicáveis as medidas, diferentes usuários podem definir KPIs e filtros distintos, definindo metas específicas para essa medida.

Os KPIs podem ser previstos usando várias fórmulas de regressão matemáticas disponíveis pelo motor de KPI.

Edit Kpi
Fields marked with * are mandatory

Name*
KPI Attrition

Description
Attrition

Symbol*
KPI_Attrition

Unit*
Number

Data window size
10

Status*
Ready

Start Date*
2012-01-01

End Date
2012-12-31

Preview
Attrition
2012 Forecast
5/10
Other Targets
undefined

Expression Targets Scheduler Alarms Display

Score*
Score(MSR_Attrition)

Score On Error*
0

Forecast*
RegressionLinear(CurrentWindow(KPI_Attrition);0.2)

Revenue Lost*
0

Min Threshold*
0

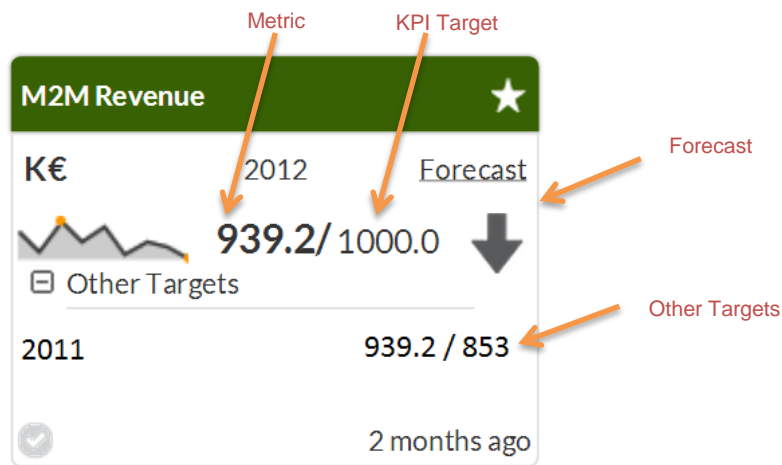
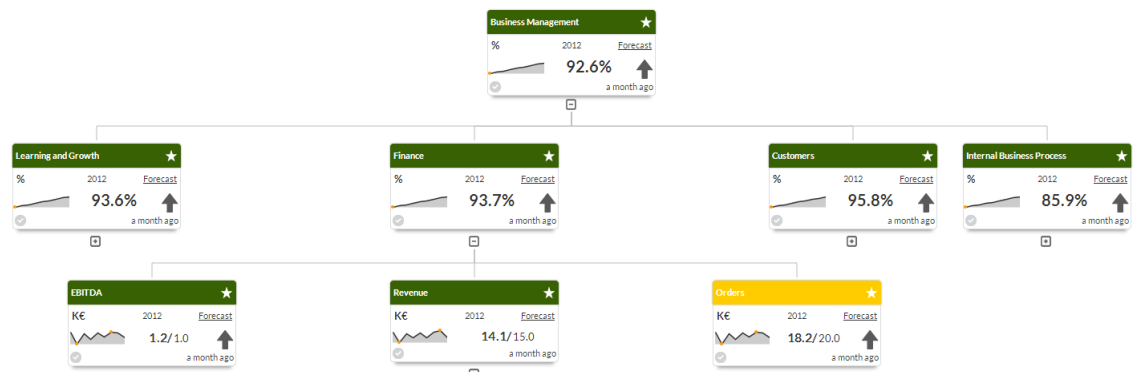
Max Threshold*
0

Save Cancel

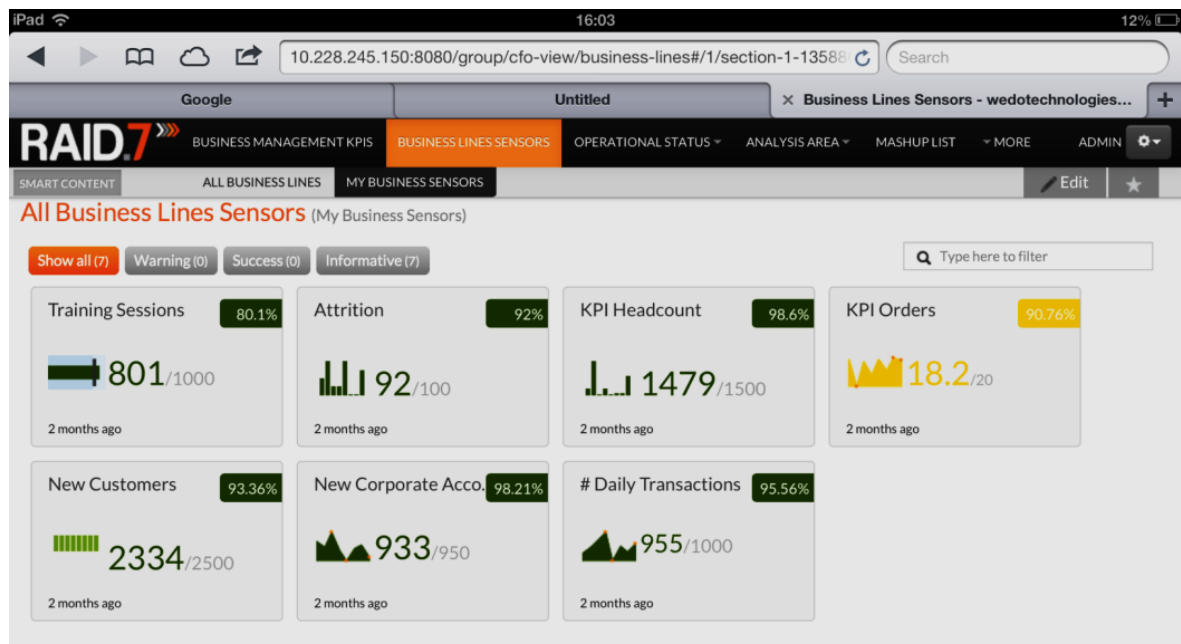
Através do Portal o analista pode:

- Definir, editar, apagar e visualizar as medidas;
- Definir, editar, apagar e visualizar KPIs;
- Definir Kpi com base em volume de dados processados, tempo de processamento, quantidade conciliações de dados e quantidade de receita;
- Mapear um KPI específico sobre o Balanced Scorecard ou Business Sensor;
- Desenhar um gráfico ou uma tabela Datalisting sobre os dados históricos KPI;
- Configurar alarmes e notificações a serem gerados em limites de KPIs específicos.

Exemplo KPI Balanced Scorecards:

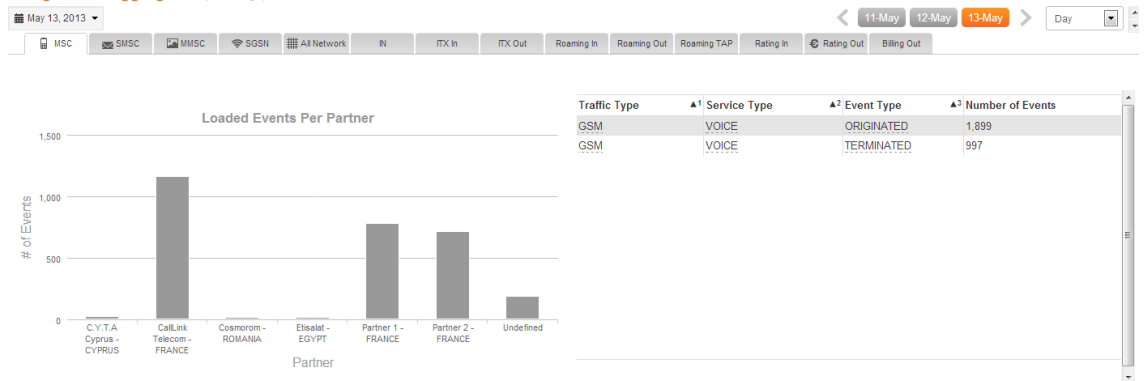


Exemplo KPI Business Sensor:

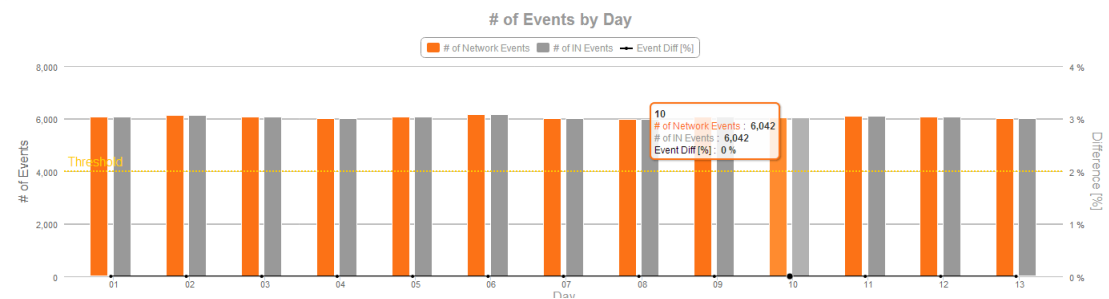


Abaixo, exemplos com screens que podem ser utilizados como visões dashboard's:

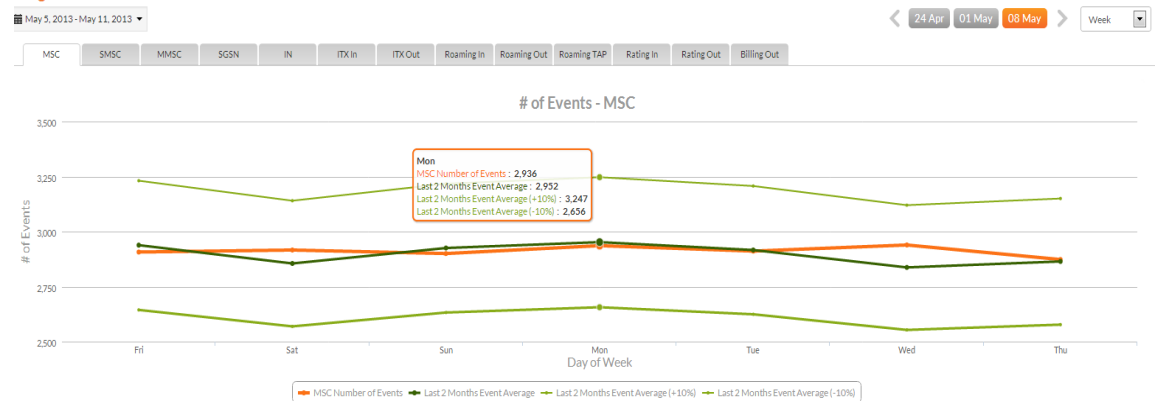
Usage Data Aggregated (Main Page)



Aggregation Reconciliation Trend View (Main Page)



Usage Loaded Data Trend (Network)





Alarms View (Alarms Global View)

May 12, 2013 - May 18, 2013

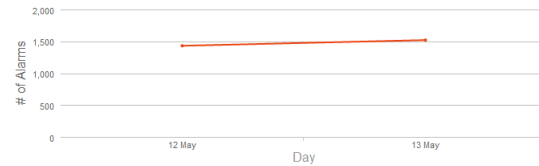
15 Apr 22 Apr 29 Apr 06 May 13 May Week

Alarms View Alarms Network Topology Alarm Detail

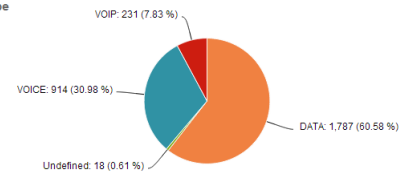
Alarms Trend (Daily)

By Call Type

Alarms Trend (Daily)



By Call Type



Alarm Id	Alarm Description	Reconciliation Id	Alarm Date	Network Element Name	Event Count Diff	Event Duration Diff	Estimated Amount Diff	Traffic Type	Call Type	Service Type
979,596	Intersystem Alarm: MSC vs Interconnect (In) - Duration Count	36	5/13/2013 12:00:00...	MSC02	9	3,210	2 4...	GSM	VOICE	VOICE
979,723	Intersystem Alarm: MSC vs Interconnect (In) - Duration Count		5/13/2013 12:00:00...	MSC05	14	4,186	1 4...	GSM	VOICE	VOICE
979,731	Intersystem Alarm: MSC vs Interconnect (In) - Duration Count		5/13/2013 12:00:00...	MSC05	14	7,403	1 4...	GSM	VOICE	VOICE
1,331,...	Intersystem Alarm: Interconnect (In) vs Interconnect (Out) - Duration ...		5/13/2013 12:00:00...	MSC05	14	4,186	1 4...	GSM	VOICE	VOICE
1,331,...	Intersystem Alarm: Interconnect (In) vs Interconnect (Out) - Duration ...		5/13/2013 12:00:00...	MSC05	14	7,403	1 4...	GSM	VOICE	VOICE
979,629	Intersystem Alarm: MSC vs Interconnect (In) - Duration Count		5/13/2013 12:00:00...	MSC03	7	3,236	1 4...	GSM	VOICE	VOICE
979,628	Intersystem Alarm: MSC vs Interconnect (In) - Duration Count		5/13/2013 12:00:00...	MSC02	7	13,238	1 4...	GSM	VOICE	VOICE
979,565	Intersystem Alarm: MSC vs Interconnect (In) - Duration Count		5/13/2013 12:00:00...	MSC03	7	738	1 4...	GSM	VOICE	VOICE

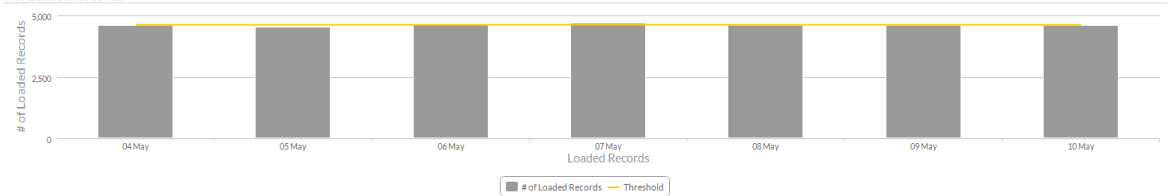
Loading Control Panel (Usage Control) / Loading Control By CP (Loaded Files)

Applied filters Control Point = BIL_IN_CSV

May 5, 2013 - May 11, 2013

24 Apr 01 May 08 May Week

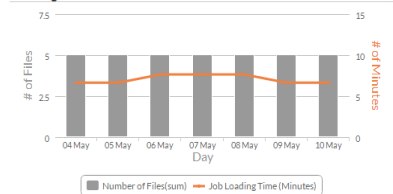
of Loaded Records



Loaded Files

Control Point	Filename	Loaded at	Number of Records
BIL_IN_CSV	BILIN0209.20130512000000.csv	2013-05-11 20:05:19	950
BIL_IN_CSV	BILIN0206.20130512000000.csv	2013-05-11 20:05:19	915
BIL_IN_CSV	BILIN0207.20130512000000.csv	2013-05-11 20:04:19	890
BIL_IN_CSV	BILIN0205.20130512000000.csv	2013-05-11 20:04:19	909
BIL_IN_CSV	BILIN0208.20130512000000.csv	2013-05-11 20:03:19	936
BIL_IN_CSV	BILIN0203.20130511000000.csv	2013-05-10 20:05:19	911
BIL_IN_CSV	BILIN0200.20130511000000.csv	2013-05-10 20:05:19	925
BIL_IN_CSV	BILIN0201.20130511000000.csv	2013-05-10 20:05:19	893
BIL_IN_CSV	BILIN0202.20130511000000.csv	2013-05-10 20:04:19	930

Loading Time



3.3.1.2 Consultas/Data Lists

(Requisitos Atendidos: RQF004, RQF008, RQF010, RQF016, RQF021, RQF022, RQF023, RQF027, RQF031, RQF032)

Através do módulo de consulta do Portal (DataList) é possível recuperar todas as fontes de dados e alarmes do RAID PI e UC

Todas as tabelas de referencia e parâmetros utilizadas pelo RAID estarão disponíveis.

Abaixo um exemplo de uma tabela de parametrização:

Classic

</

As saídas de dados podem ser definidas de acordo com os seguintes tipos de dados :

Tipo de dados	
CHAR	INTERVAL
Date	Long
FLOAT	NUMBER
INT	ROWID
VARCHAR2	

Através de módulo de consulta, o usuário poderá criar seus próprios reports a partir da base dados do RAID e executá-los de forma on-line ou por agendamento de hora/dia/mês/ano e logo disponibilizando para usuários específicos.

O Portal provê ao usuário templates padrão de reports.

Os reports poderão ser exportados para meios físicos (XLS, PDF, JPG e HTML).

3.3.1.3 Case Management

(Requisitos Atendidos: RQNF002, RQF026, RQF027, RQF028, RQF029, RQF030)

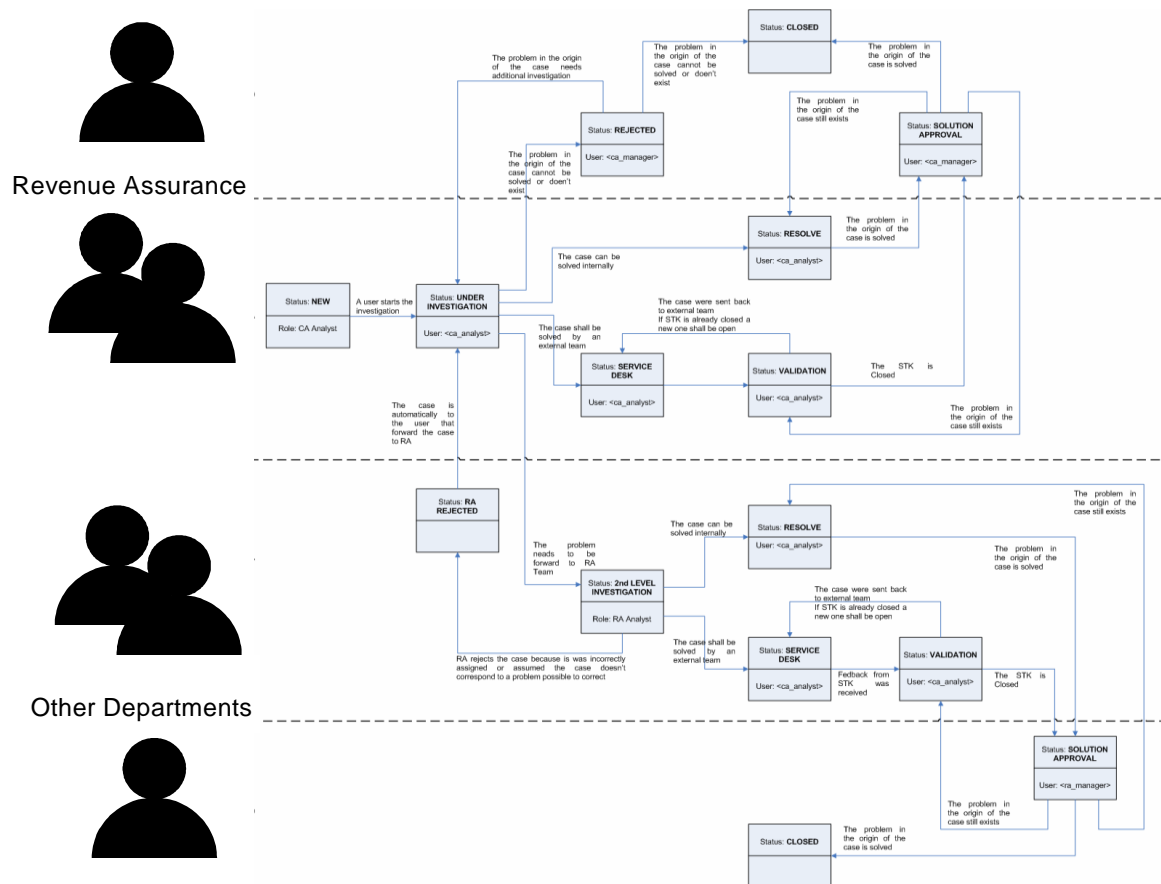
O Case Management permite gerenciar alarmes e logo tramitando os alarmes através fluxos. Alarmes semelhantes podem ser agrupados no mesmo caso. RAID oferece a capacidade de gerenciar esses casos usando um mecanismo de fluxo de trabalho. Isto permite a implementação de um processo de controle que assegura a resolução mais eficaz dos casos identificados.

O usuário através do Case Management, poderá priorizar um alarme ou um grupo de alarmes de forma manual ou automática de acordo com a perda de receita, quantidade de alarmes ou tempo sem resolução, assim entregando os alarmes para área responsável da análise com nível de criticidade determinado pelo Case Management.

No Case Management é possível acessar o registro alarmado no banco de dados do RAID.

No surgimento de caso de alarme é possível notificar e enviar o alarme para as áreas envolvidas, os usuários poderão ser notificados pelo próprio Case Management do Portal, e-mail ou SMS.

Abaixo um exemplo de um fluxo de trabalho do Case Management:



3.3.2 RAID Admin

(Requisitos Atendidos: RQF005, RQF007, RQF008)

O RAID Admin é uma interface Windows Client (Software AppBrowser - instalado no terminal Windows), que permite facilmente desenhar, configurar e executar fluxos de cargas e validações. RAID Admin permite monitorar e gerenciar todos os processos em execução no RAID e Scheduler para execução de fluxos.

Através do RAID Admin o usuário pode realizar as seguintes tarefas:

- Configurar dados dos sistemas de origem;
- Projetar os processos de carregamento e validação;
- Definir a os formatos de dados;
- Configurar regra de validação, geração de alerta e relatório;
- Definir as tarefas de controle, sinais e alertas, e funções de transformação de dados;
- Definir agendamento de execução de qualquer fluxo do sistema (permite definir o horário de execução);

RAID Admin é dividido em cinco áreas:

- i. Systems management
- ii. Loading management
- iii. Validations management
- iv. Alarms management
- v. Session management, authentication and authorization

3.3.2.1 System management

Gerência a definição dos sistemas a serem analisados pelo RAID, e permite a criação das infra-estruturas que armazenam os dados coletados dos sistemas. A configuração dos sistemas a serem analisados pelo RAID implica a definição de alguns valores e que suas definições estão vinculados por um diagrama de árvore.

3.3.2.2 Loading management

(Requisitos Atendidos: RQF007)

Depois de definir os sistemas a partir do qual os dados serão incluídos no RAID, o processo de carregamento dos dados correspondentes a cada uma das instâncias existentes, tem de ser configurado. O carregamento visa garantir a existência de dados para os fluxos de validação.

Quando há uma inconsistência na carga, em outras palavras, os dados de entrada não estão de acordo com as especificações, o mesmo será interrompido manter a consistência dos dados. Ela pode ser retomada após a correção da situação e apenas os restantes dados serão processados.

O processo de carregamento de dados é incremental. A data da última carga bem-sucedida é mantido para cada carregamento. No caso de erro do processo de carga a data da última carga não vai ser alterada, o que vai permitir que a causa do problema a ser corrigida e da recuperação do processo de carregamento .

Com o carregamento de arquivos lá existirá um controle de arquivo para arquivo, para evitar carga de arquivos duplicados ou não carregados.

Todos os registros que não são capazes de ser inserido, na base de dados do sistema RAID, terá uma entrada criada no mecanismo de registro, que vão descrever o problema que ocorreu em detalhe. Esse registro pode ser acessado a qualquer momento, com o objetivo de depurar o problema. Cabe ressaltar que, desde que os registros não poderiam ser carregados, o sistema irá realizar a reversão de carga.

O carregamento é efetuado por agentes, que são responsáveis pelo controle da sequência de integração e, portanto não há necessidade do circuito de carga. Carregamento será feito de forma incremental com controle de integração para cada arquivo, a fim de garantir que nenhum arquivo é integrado duas vezes ou por meio de a data de modificação dos registros se os dados estão sendo integradas a partir do banco de dados.

Todos os dados de entrada poderão ser configurado/editado de forma simples pelo usuário através loading management.

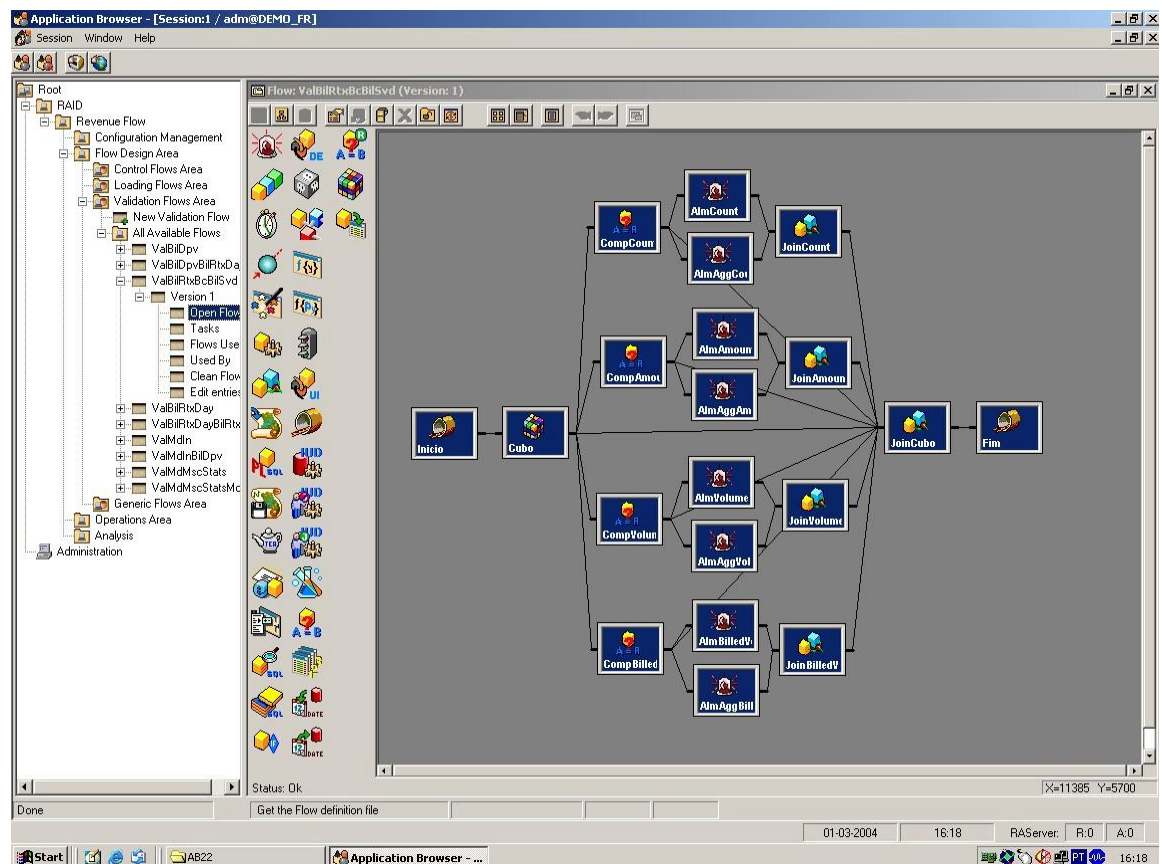
3.3.2.3 Validations management.

(Requisitos Atendidos: RQF001, RQF002, RQF008, RQF009, RQF011, RQF012, RQF025)

Para definir um novo fluxo de validação (dados cubo + comparadores de alarmes) será preciso:

- Definir os sistemas e dados a serem analisados, restrições e transformações;
- Definir regras de comparação entre os dados dos sistemas;
- Definir o tipo de alarmes devem ser deduzido, para cada situação detectada.

A definição de um novo fluxo é feito por meio de uma interface gráfica, com o controle de acesso (e um controle para evitar múltiplas alterações por diferentes usuários), o que permite a criação de diferentes tarefas a serem executadas e para definir a dependência entre tarefas por meio de interconexões.

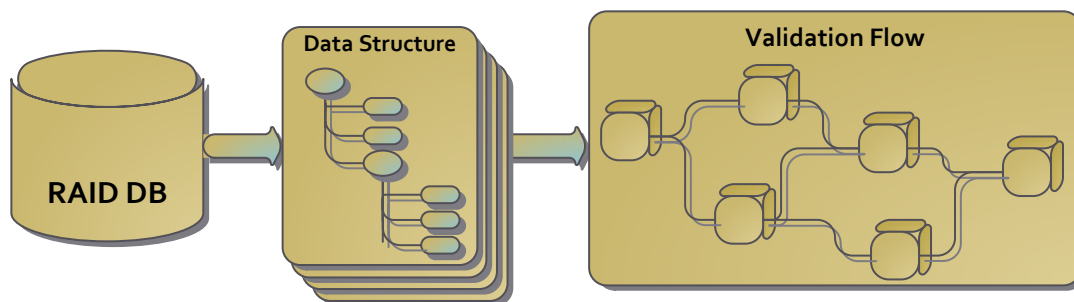


Definição do fluxo de controle de validação.

Fluxo de validação pode ser controlado por semáforos de modo a tornar possível a execução da validação, flui de acordo com os dados carregados e cria as dependências entre os fluxos de validação e carregamento.

O fluxo de controle irá ser desenvolvido de modo que pode ser possível, que o não carregamento de um subsistema específico não impede a execução de fluxos de validação dos outros sistemas. Este mesmo controle também vai assegurar que, quando um sub-sistema específico não é executada, em seguida, os fluxos de validação que estão dependentes dela também não será executado para garantir que não haverá os alarmes inconsistentes.

Os processos de validação podem ser executados diariamente, a cada hora, ou por qualquer outro período de tempo.



Existem várias maneiras de iniciar um processo de validação:

- Via Scheduler usando a interface de usuário Raid Admin (Windows Client – AppBrowser)
- On-demand, usando o recurso Flow Execution do Raid.
- A partir de linha comando no sistema operacional.

As regras de validação são executadas pelos fluxos de validação. Há um fluxo de validação para verificar os dados agregados de cada sistema e flui para verificar dados agregados entre os sistemas .

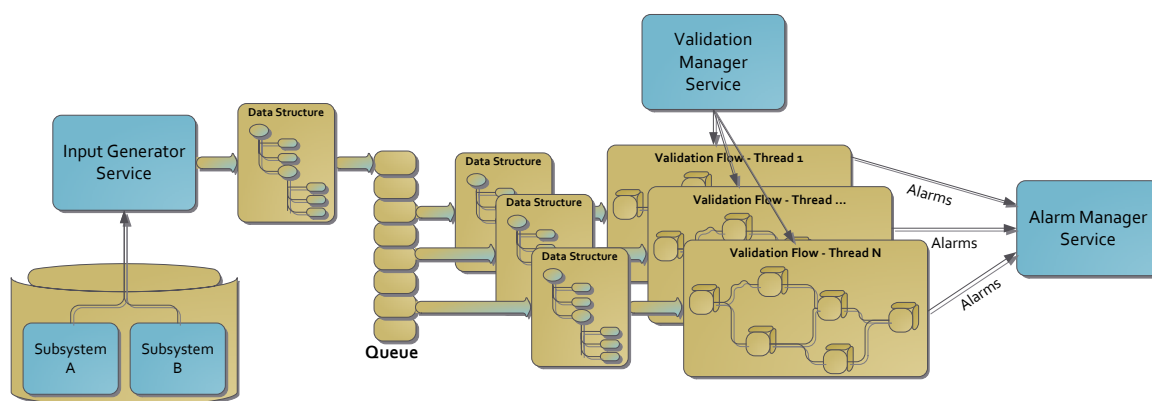
A execução de um processo de validação envolve várias etapas:

- Seleção de dados para validar -Input Serviço Generator;
- Controle da execução de validação dos fluxos - Service Manager Validação;
- Gestão de alarmes gerados - Alarm Service Manager.

O processo de seleção de dados é muito complexo, uma vez que pode incluir vários subsistemas. O Serviço Gerador de entrada é responsável por esta tarefa.

A gestão de quantos segmentos serão executados, o fluxo de validação é da responsabilidade do Serviço de Validação Manager.

A gravação dos alarmes gerados pelos diversos fluxos é de responsabilidade do Service Alarms management.

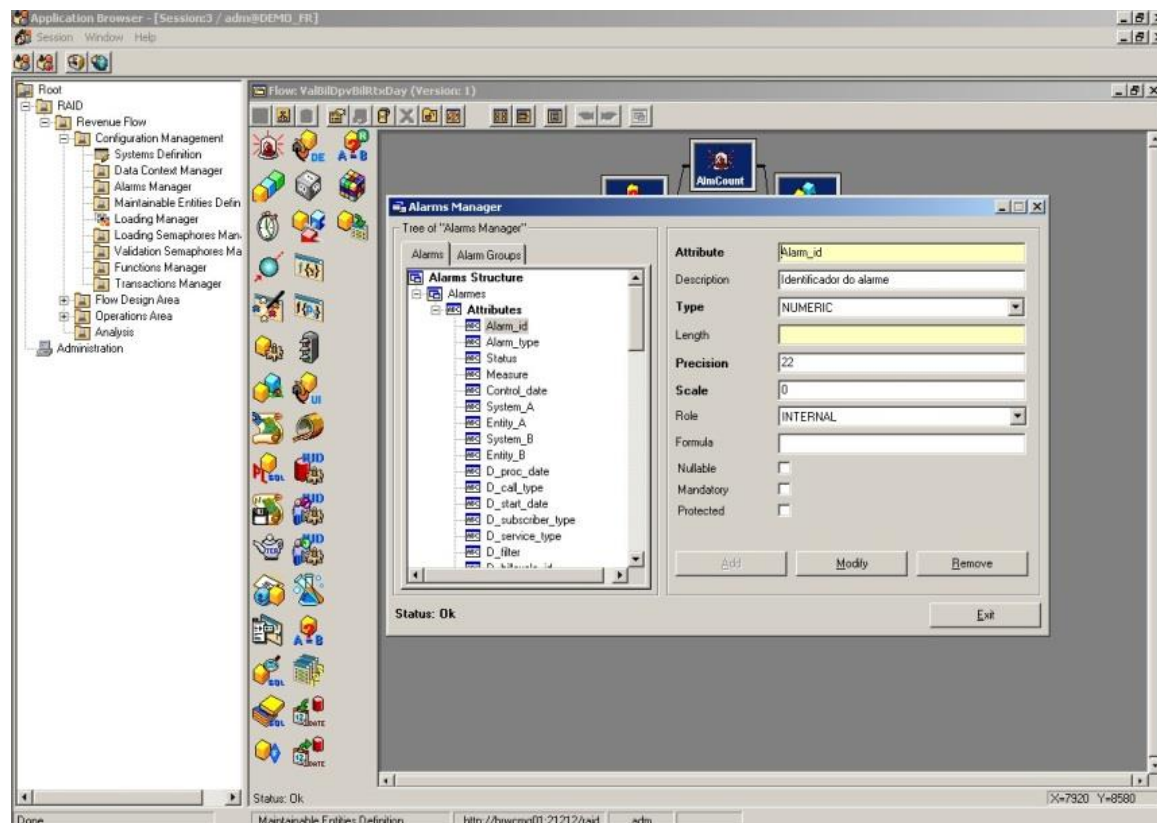


3.3.2.4 Alarms management

(Requisitos Atendidos: RQF001, RQF002, RQF008, RQF009, RQF025)

Através da interface de configuração RAID Admin permite a adição, mudança e desativação de diferentes tipos de alarmes e grupos de alarmes.

A gestão dos alarmes é feita usando a interface gráfica - Gerente de Alarmes, onde é possível criar / alterar / remover alarme e definir seus atributos.



A ação de acionamento do alarme é feito no nível de design de fluxos de validação.

3.3.2.5 Session management, authentication and authorization

Gerenciamento de sessão

RAID gerencia as sessões de usuário e suas próprias sessões de aplicação, permitindo existência de várias sessões simultâneas. Sessões simultâneas pode ser desativada em uma base por usuário.

Permite monitorar através de um painel de semáforo o status de todos processos.

Autenticação e Autorização

A autenticação pode ser fornecida localmente ou externamente usando servidores LDAP padrão (por exemplo, o Microsoft Active Directory). Cada usuário é identificado por um nome de usuário e senha, e atribui um conjunto de funções e grupos de usuários. Cada função concede permissões específicas sobre os recursos específicos (por exemplo, páginas de portlets), assegurando privilégios diferentes para diferentes usuários do sistema. Os dados também podem ser constrangido em uma base por usuário / por papel.

Questões de segurança



Aspectos de segurança são um dos focos desta solução, devido à sua importância e criticidade. Essa preocupação com a segurança é tratada globalmente e inclui elementos ligados à rede, sistemas, aplicações e processos.

Auditoria Acesso

As medidas preventivas tomadas durante e após o desenvolvimento da solução em que se trata de segurança, é também essencial para garantir mecanismos de auditoria uma vez que o sistema é produtivo.

Neste sentido, a solução cria registros de auditoria para todas as ações de negócio relevantes. Nestes registros os dados relevantes sobre a operação realizada ou tentativa será registrada, bem como o usuário, os valores de operações em questão, os dados da sessão. A partir desses registros, será possível detectar situações de uso abusivo e as tentativas de realizar operações proibidas.

A solução proposta permite a definição de regras de acordo com a operação, valores envolvidos, usuários, perfis e níveis de criticidade.

4 Anexos

Arquivo	Nome	Anexo
01	Especificação de Infra	DOC_BRA14POI02500_003_B - Sizing Vanilla RAID 7.xlsx
03	Configuração de Infra Oracle	Config_Infra_SERVER_ORACLE_01.docx
04	Parâmetros Oracle	parametros_oracle.docx
05	Planilha de Macros requisitos(Funcional)	84137 - Planilha de Macro Requisitos_12032014.xlsx
06	Planilha de Requisitos (Negócio)	STI_84137 - _Mapa_de_Requisitos_14032014.xlsx
07	Integrating RAID in High Availability and Disaster Recover environments	DOC_BRA14POI02500_001_E - IntegratingRAIDinHAandDR.pdf
08	Desenho de Infra Estrutura	DOC_BRA14POI02500_001_B - Desenho Infraestrutura.png
09	Planilha de Interfaces dos RAIDs atuais	84137 - Planilha de Interfaces.xlsx