**Une EPM Telecomunicaciones**



**Manual de Administración y Operación del**

**Sistema De Información ROC**

**20-08-2013**

Tabla de Contenido

[CONTROL DE CAMBIOS 4](#_Toc373249002)

[MANUAL DE ADMINISTRACIÓN Y OPERACIÓN 4](#_Toc373249003)

[1. ARQUITECTURA DEL SERVICIO 4](#_Toc373249004)

[*1.1.* *Topología de la solución con todos sus componentes* 4](#_Toc373249005)

[*1.2.* *Funcionamiento del servicio* 7](#_Toc373249006)

[2. FLUJOS TRANSACCIONALES 8](#_Toc373249007)

[3. INSTALACIÓN Y CONFIGURACIONES ESPECIALES 9](#_Toc373249008)

[*3.1.* *Creación de Bases de Datos (SID: SPARKREF y SPARKUSG)* 10](#_Toc373249009)

[Inicialización de parámetros para la instancia SPARKREF 10](#_Toc373249010)

[Inicialización de parámetros para la instancia SPARKUSG 11](#_Toc373249011)

[*3.2.* *Configuraciones de Sistema Operativo* 14](#_Toc373249012)

[4. SERVICIOS 16](#_Toc373249013)

[*4.1.* *Subir y bajar servicios y daemons* 17](#_Toc373249014)

[ROC Fraud Management – Detener Aplicación 17](#_Toc373249015)

[ROC Fraud Management - Iniciar Aplicación 17](#_Toc373249016)

[ROC Fraud Management & ROC Revenue Assurance - Detener Spark 17](#_Toc373249017)

[ROC Fraud Management & ROC Revenue Assurance - Iniciar Spark 17](#_Toc373249018)

[5. PUERTOS 19](#_Toc373249019)

[*5.1.* *Puertos Internos de la Aplicaciones* 19](#_Toc373249020)

[6. COMUNICACIONES 20](#_Toc373249021)

[7. REGLAS CONFIGURADAS EN EL FIREWALL 21](#_Toc373249022)

[8. VPN 22](#_Toc373249023)

[9. FTP Seguro 23](#_Toc373249024)

[10. CONFIGURACIONES EN EL F5 23](#_Toc373249025)

[11. MANEJO DE LOGS 24](#_Toc373249026)

[12. VERIFICACIÓN DE COMPONENTES Y FUNCIONALIDADES 25](#_Toc373249027)

[13. ERRORES COMUNES 27](#_Toc373249028)

[14. SEGURIDAD 28](#_Toc373249029)

[ACCESO A LA APLICACIÓN 28](#_Toc373249030)

[LOG 30](#_Toc373249031)

[PRUEBAS DE INTRUSIÓN 30](#_Toc373249032)

[15. POLITICAS DE RESPALDOS 31](#_Toc373249033)

[16. ANALISTAS DE LA APLICACIÓN 32](#_Toc373249034)

[17. MAPA DE OPERACIONES 32](#_Toc373249035)

[18. ESCALAMIENTOS 32](#_Toc373249036)

[19. FLUJOS EN SERVICE DESK 35](#_Toc373249037)

CONTROL DE CAMBIOS

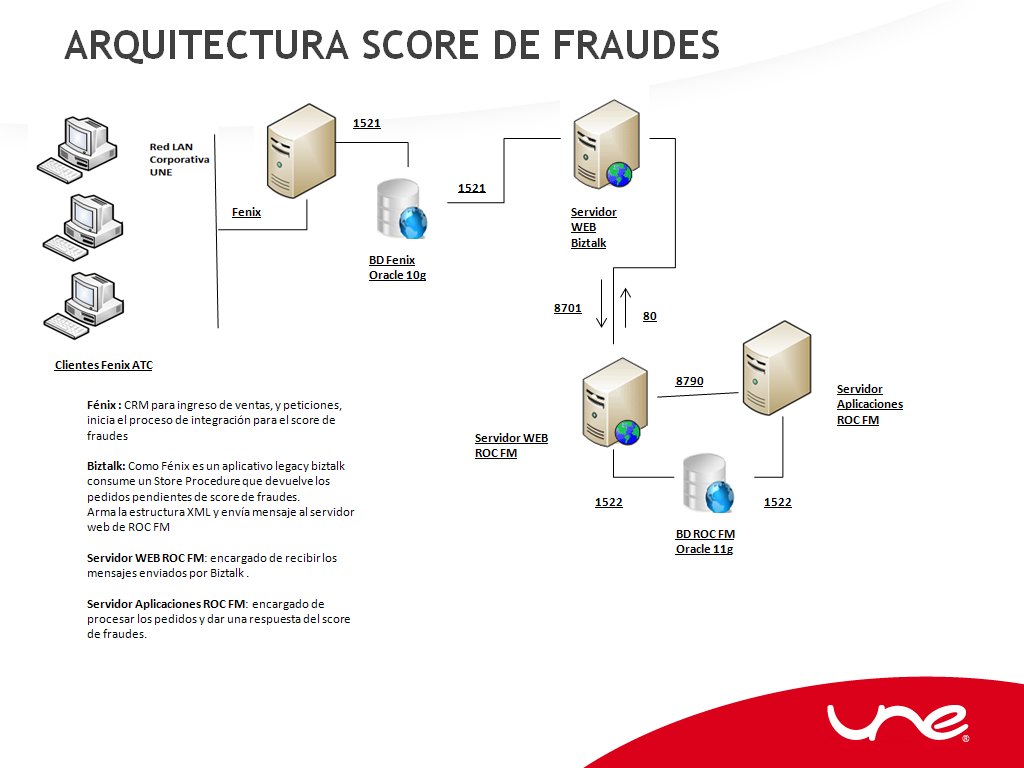
|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Actualizado por** | **Comentarios de la actualización** |
| Versión 1 | 2013-08-13 | Durley Paulina Gómez Builes  Jimmy Romero Alvis | Creación del Documento |
| Version 2 | 2014-01-15 | Luisa Fernanda Zuluaga | Actualización Entregable II |
| Version 3 | 2014-08-27 | Mónica Ofir Aristizaba V | Actualización Entregable II |

MANUAL DE ADMINISTRACIÓN Y OPERACIÓN

El presente documento contiene la información para la administración de la aplicación ROC que adquirió UNE para automatizar los procedimientos de Control de Fraudes y Aseguramiento de Ingresos.

# ARQUITECTURA DEL SERVICIO

## *Topología de la solución con todos sus componentes*



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ROC** | |  | **Fuentes de Información** | | |
| net-pappra01 | 10.100.82.25 |  | OPEN | net-pora20 | 10.100.67.137 |
| net-pwebfmra01 | 10.100.82.24 |  | FENIX | netvm-pmts01 | 10.100.66.170 |
| net-pbdfmra01 | 10.100.67.119 |  | RBM | net-pltebd01-01 | 10.100.67.31 |
| net-pdice01 | 10.100.82.26 |  | net-pltebd01-02 | 10.100.67.153 |
|  |  |  | IAM | net-papp03-01 | 10.100.66.219 |
|  |  |  | net-papp03-02 | 10.100.66.220 |
|  |  |  | LDAP | une-pldapbog01 | 10.158.106.31 |
|  |  |  | une-pldap03 | 10.158.106.14 |
|  |  |  | CROMO | unevm-pmap01 | 10.158.134.5 |
|  |  |  | unevm-pmap02 | 10.158.134.6 |
|  |  |  | unevm-pmap03 | 10.158.134.7 |
|  |  |  | unevm-pmap04 | 10.158.134.4 |
|  |  |  | unevm-pmap05 | 10.158.134.9 |
|  |  |  | unevm-pmap06 | 10.158.134.32 |
|  |  |  | unevm-pmap07 | 10.158.134.33 |
|  |  |  | unevm-pmap08 | 10.158.134.34 |
|  |  |  | unevm-pmapcron | 10.158.134.28 |
|  |  |  | Charging Gateway | MED: ATCAX86\_F0S8 | 10.153.3.4 |
|  |  |  | BOG: ATCAX86\_F0S4 | 10.153.13.4 |
|  |  |  | HSS | unevm-pmvftp01 | 10.158.123.8 |
|  |  |  | SAP | NET-APP09 | 10.100.66.21 |
|  |  |  | **FUENTES ENTREGABLE II** | | |
|  |  |  | DIRECTORIO ACTIVO | Net-pssrs | 10.100.67.60 |
|  |  |  | Portabilidad Numerica | Net-pssrs | 10.100.67.60 |
|  |  |  | Gestor de Recarga | Unevm-pmap01 | 10.158.134.5 |
|  |  |  | Gestor de Recarga | Unevm-pmap02 | 10.158.134.6 |
|  |  |  | Gestor de Recarga | Unevm-pmap03 | 10.158.134.7 |
|  |  |  | Gestor de Recarga | Unevm-pmap04 | 10.158.134.4 |
|  |  |  | Gestor de Recarga | Unevm-pmap05 | 10.158.134.9 |
|  |  |  | Gestor de Recarga | Unevm-pmap06 | 10.158.134.32 |
|  |  |  | Gestor de Recarga | Unevm-pmap07 | 10.158.134.33 |
|  |  |  | Gestor de Recarga | Unevm-pmap08 | 10.158.134.33 |
|  |  |  | ATS | Une-atsdb01 | 10.158.147.21 |
|  |  |  | Canal Online | Unevm-pgweb01 | 10.158.124.91 |
|  |  |  | Canal Online | Unevm-pgweb02 | 10.158.124.92 |
|  |  |  | BDA | Unevm-pmap01 | 10.158.134.5 |
|  |  |  | BDA | Unevm-pmap02 | 10.158.134.6 |
|  |  |  | BDA | Unevm-pmap03 | 10.158.134.7 |
|  |  |  | BDA | Unevm-pmap04 | 10.158.134.4 |
|  |  |  | BDA | Unevm-pmap05 | 10.158.134.9 |
|  |  |  | BDA | Unevm-pmap06 | 10.158.134.32 |
|  |  |  | BDA | Unevm-pmap07 | 10.158.134.33 |
|  |  |  | BDA | Unevm-pmap08 | 10.158.134.33 |

A los servidores de la tabla “Fuentes de información” que están en la Red Corporativa se les hizo montaje de la ruta NAS:

10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/…

Para los que se encuentran en el ISP, en la misma tabla con fondo de color azul “CROMO” se les hizo montaje de la ruta NAS:

10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/…

para que las extracciones queden directamente en el almacenamiento utilizado por el servidor de ROC net-pappra01 que realiza las cargas de información, a excepción del Charging Gateway y HSS que son accedidos vía SFTP.

Configuración NAS

Entregable I

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| FUENTE | NAS | FILE SYSTEM FUENTE | FILE SYSTEM ROC | RUTA DENTRO DE LA NAS O EL SERVIDOR |
| CHARGIN GATEWAY | No Aplica SFTP | No Aplica | No Aplica | /var/igwb/backsave/AP/second/pgwcdr |
| CHARGIN GATEWAY | No Aplica SFTP | No Aplica | No Aplica | /var/igwb/backsave/AP/second/pgwcdr |
| HSS | No Aplica SFTP | No Aplica | No Aplica | /var/lte/dtl/SAE |
| LDAP | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/LDAP | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/LDAP | /spark\_data/ROC\_DataFiles/LDAP |
| LDAP | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/LDAP | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/LDAP | /spark\_data/ROC\_DataFiles/LDAP |
| OPEN | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/OPEN | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/OPEN | /spark\_data/ROC\_DataFiles/OPEN |
| OPEN | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/OPEN | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/OPEN | /spark\_data/ROC\_DataFiles/OPEN |
| OPEN | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/OPEN | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/OPEN | /spark\_data/ROC\_DataFiles/OPEN |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| CROMO | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CROMO | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/CROMO | /spark\_data/ROC\_DataFiles/CROMO/CROMO |
| FENIX | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/FENIX | \\app-files\FENIX\_ROC\ | /spark\_data/ROC\_DataFiles/FENIX | /spark\_data/ROC\_DataFiles/FENIX |
| IAM | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/IAM | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/IAM | /spark\_data/ROC\_DataFiles/IAM |
| IAM | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/IAM | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/IAM | /spark\_data/ROC\_DataFiles/IAM |
| RBM | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/RBM | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/RBM | /spark\_data/ROC\_DataFiles/RBM |

Entregable II

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FUENTE** | **NAS** | **FILE SYSTEM FUENTE** | **FILE SYSTEM ROC** | **RUTA DENTRO DE LA NAS O EL SERVIDOR** |
| ATS | No Aplica | No Aplica | No Aplica | /opt/app/oracle/ARG/rep\_une/ROC |
| CANAL\_ONLINE | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CANAL\_ONLINE | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CANAL\_ONLINE | /spark\_data/ROC\_DataFiles/CANAL\_ONLINE |
| CANAL\_ONLINE | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/CANAL\_ONLINE | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CANAL\_ONLINE | /spark\_data/ROC\_DataFiles/CANAL\_ONLINE |
| SAP | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/SAP | \\app-files\SAP\_ROC\ | /spark\_data/ROC\_DataFiles/SAP | /spark\_data/ROC\_DataFiles/SAP |
| DIRECTORIO\_ACTIVO | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/DIRECTORIO\_ACTIVO | \\app-files\DIRECTORIO\_ACTIVO\_ROC\ | /spark\_data/ROC\_DataFiles/DIRECTORIO\_ACTIVO | /spark\_data/ROC\_DataFiles/DIRECTORIO\_ACTIVO |
| PORTABILIDAD\_NUMERICA | 10.100.68.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/PORTABILIDAD\_NUMERICA | \\app-files\PORTABILIDAD\_NUMERICA\_ROC\ | /spark\_data/ROC\_DataFiles/PORTABILIDAD\_NUMERICA | /spark\_data/ROC\_DataFiles/PORTABILIDAD\_NUMERICA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| GESTOR\_RECARGA | 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/GESTOR\_RECARGA | /ROC\_DataFiles\_GestorRecarga | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA | /spark\_data/ROC\_DataFiles/CROMO/GESTOR\_RECARGA |
| PORTAL\_RESARCIMIENTO | 10.100.65.110:/fs\_app/MediacionUNE/Logs/prod/mediadores/webservices/wsProxyRBM | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/PORTAL\_RESARCIMIENTO | /spark\_data/ROC\_DataFiles/PORTAL\_RESARCIMIENTO |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |
| BDA | 10.158.130.12:/Control\_fraudes/rocfm\_spark\_data\_pdn/ROC\_DataFiles/BDA | /ROC\_DataFiles | /spark\_data/ROC\_DataFiles/CROMO/BDA | /spark\_data/ROC\_DataFiles/CROMO/BDA |

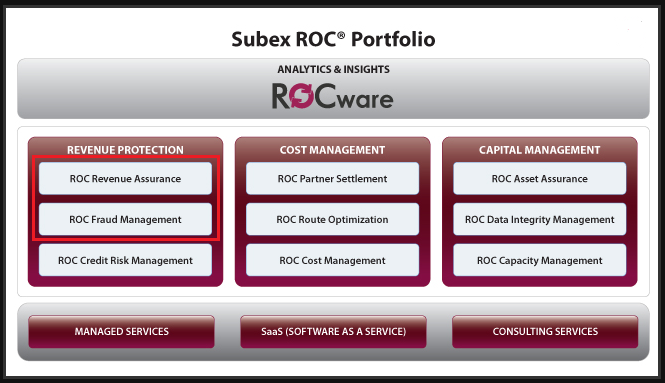
Tabla de la solución con las IP donde se genera la transacción y sus respectivos puertos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TIPO DE COMUNICACIÓN** | **IP ORIGEN** | **IP DESTINO** | **PUERTO** | **TIPO PAQUETE** |
| ROC Fraud Management Client | Cualquier elemento de Red | 10.100.82.24 | 8080,  8700,  9000 | UDP/TCP |
| Oracle Listener | 10.100.82.25  10.100.82.22  10.100.82.23  10.100.82.24  10.100.82.26 | 10.100.67.119 | 1522 |  |
| ROC Fraud Management Core Executables | 10.100.82.25  10.100.82.23  10.100.82.24 | 10.100.82.22 | 20000, 20001, 20003, 20204, 21000, 25001, 25002, 30001, 35001, 50001, 50011, 50012, 50003, 50101, 50201, 50301, 50401, 50502, 90001, 90002, 90012, 90095, 90096, 90097, 90098 |  |
| Spark Client | 10.100.82.25  10.100.82.22  10.100.82.23 | 10.100.82.24 | 8790 |  |
| Stream Controller | 10.100.82.22  10.100.82.23  10.100.82.24 | 10.100.82.25 | 7770, 7777 |  |
| Task Controller | 10.100.82.22  10.100.82.23  10.100.82.24 | 10.100.82.25 | 7779 |  |
| ftp | Cualquier elemento de Red | 10.100.82.25  10.100.82.22  10.100.82.23  10.100.82.24  10.100.82.26  10.100.67.119 | 20,21 |  |
| SSH | Cualquier elemento de Red | 10.100.82.25  10.100.82.22  10.100.82.23  10.100.82.24  10.100.82.26  10.100.67.119 | 22 |  |
| Telnet | Cualquier elemento de Red | 10.100.82.25  10.100.82.22  10.100.82.23  10.100.82.24  10.100.82.26  10.100.67.119 | 23 |  |
| Servicio web Integración Score Fraudes (origina biztalk) | |  | | --- | | Biztalk | | 10.100.66.195 | | 10.100.66.197 | | 10.100.66.83 | | 10.100.66.84 | | 10.100.66.87 | | 10.100.66.86 | | 10.100.66.195 | | 10.100.66.197 | | 10.100.66.83 | | 10.100.66.84 | | 10.100.66.87 | | 10.100.66.86 | | 10.100.82.22, 10.100.82.23 | 8701 |  |
| Servicio web Integración Score Fraudes (origina ROC) | 10.100.82.22, 10.100.82.23 | |  | | --- | | Biztalk | | 10.100.66.195 | | 10.100.66.197 | | 10.100.66.83 | | 10.100.66.84 | | 10.100.66.87 | | 10.100.66.86 | | 10.100.66.195 | | 10.100.66.197 | | 10.100.66.83 | | 10.100.66.84 | | 10.100.66.87 | | 10.100.66.86 | | 8080, 80 |  |

## *Funcionamiento del servicio*

El sistema de información ROC cuenta con 2 aplicaciones que se manejan por interfaz de usuario independiente.

La Suite de ROC comprende varios módulos, no obstante en UNE a la fecha solo se adquirió los módulos de **ROC Revenue Assurance** **RA** y **ROC Fraud Management** **FM**.



**ROC Revenue Assurance**

Es un Sistema de Administración útil para el aseguramiento de la información en términos de Suscripción de Clientes y del Uso de servicios ayudando a detectar potenciales pérdidas de ingresos.

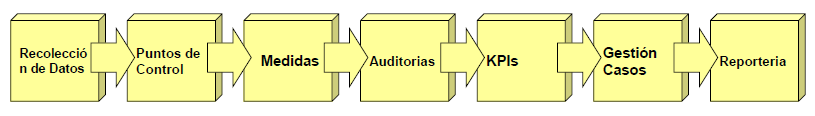
**ROC Fraud Management**

Es un Sistema de Administración para detectar actividades fraudulentas en el dominio de Telecomunicaciones. Opera en modo de tiempo real monitoreando los Registros de los Detalles de Llamadas (CDR), generando alarmas si se detecta algo inusual o sospechoso en los patrones de llamada.

Tiene igualmente la capacidad para detectar tipos de fraude en todos los entornos de telecomunicaciones - líneas (PSTN, ISP, VoIP), inalámbrica (2G, 2.5G, 3G, 4G), Servicios VAS, MMS, y “M-commerce”.

# FLUJOS TRANSACCIONALES

* 1. **ROC Revenue Assurance**



* **Recolección de datos**: Hace referencia a los procesos de File Collections “Captura de archivos de los sistemas fuentes (Fenix, Open, RBM, HSS, Charging Gateway, Cromo)”
* **Puntos de Control**: Hace referencia a los procesos de Parser y Data Load
  + Parseo: transformación de los datos
  + Data Load: Proceso de volcado de información a la base de datos
  + **Medidas**: Son cruces de información para sacar totales de datos para los procesos de Auditorias.
* **Auditorías**: Conjunto de medidas que sirve para generar las conciliaciones del negocio
* **KPI**: Umbrales configurados en las medidas para la generación de alarmas
  1. **ROC Fraud Management**
* **Recolección de datos**: Hace referencia a los procesos de File Collections “Captura de archivos de los sistemas fuentes (Fenix, Open, RBM, HSS, Charging Gateway, Cromo)”
* **Puntos de Control**: Hace referencia a los procesos de Parser y Data Load
  + Parseo: transformación de los datos
  + Data Load: Proceso de volcado de información a la base de datos
  + Stitching: Desnormalización de la información de CRM en una única estructura de Suscriptores y Servicios.
* **Carga de suscriptor**: Sube la información del stitching al modelo relacional de base de datos de FM
* **Generación de alarmas**: Alertas y alarmas que se generan en la aplicación basados en condiciones y reglas configuradas.

PROCESO DE SCORE DE FRAUDES (INTEGRACIÓN FENIX-ROC)

# INSTALACIÓN Y CONFIGURACIONES ESPECIALES

|  |  |  |
| --- | --- | --- |
| **SERVIDOR** | **SISTEMA OPERATIVO** | **SOFTWARE DE TERCEROS** |
| net-pappra01 | Red Hat Enterprise Linux Server release 6.4 | Oracle Client 11g 64 bits |
| net-pappfms01 | Red Hat Enterprise Linux Server release 6.4 | Oracle Client 11g 64 bits |
| net-pappfms02 | Red Hat Enterprise Linux Server release 6.4 | Oracle Client 11g 64 bits |
| net-pwebfmra01 | Red Hat Enterprise Linux Server release 6.4 | Oracle Client 11g 64 bits |
| net-pbdfmra01 | Red Hat Enterprise Linux Server release 6.4 | Oracle Enterprise Edition 11.2.0.3.5 (64 bits)  Partitioning |
| net-pdice01 | Windows Server 2008 Estándar 64 bits | Oracle Client 11g 64 bits |

Paquetes instalados en servidores con sistema operativo Linux Red Hat.

gcc.x86\_64 4.4.7-3.el6  
gawk.x86\_64 3.1.7-10.el6  
perl.x86\_64 4:5.10.1-130.el6\_4  
java-1.6.0-openjdk.x86\_64 1:1.6.0.0-1.61.1.11.11.el6\_4  
java-1.7.0-openjdk.x86\_64 1:1.7.0.19-2.3.9.1.el6\_4  
bash.x86\_64 4.1.2-14.el6  
openssl.x86\_64 1.0.0-27.el6\_4.2  
openssh-clients.x86\_64 5.3p1-84.1.el6  
gzip.x86\_64 1.3.12-18.el6  
gdb.x86\_64 0:7.2-60.el6  
sendmail.x86\_64 8.14.4-8.el6  
perl-DBI.x86\_64 1.609-4.el6

Instalación de fuentes tipográficas, servidor **net-pwebfmra01**:

bitmap-fixed-fonts.noarch  
bitmap-lucida-typewriter-fonts.noarch  
dejavu-lgc-sans-mono-fonts-2.30-2.el6.noarch  
liberation-fonts-common.noarch  
liberation-mono-fonts.noarch  
liberation-sans-fonts.noarch  
liberation-serif-fonts.noarch.  
ghostscript-fonts-5.50-23.1.el6.noarch  
urw-fonts-2.4-10.el6.noarch

Configuración e instalación del motor de base de datos, servidor **net-pbdfmra01**:

Motor Instalado: Oracle Enterprise Edition 11.2.0.3.5 (64 bit) with partitioning option.

## *Creación de Bases de Datos (SID: SPARKREF y SPARKUSG)*

* Select “Custom Database” option.
* Preferred ORACLE\_SID – SPARKREF, SPARKUSG
* Type of instance -Dedicated Server
* Oracle block size - 16 KB
* CHARACTERSET = Default
* Enterprise Manager (optional)

### Inicialización de parámetros para la instancia SPARKREF

|  |  |
| --- | --- |
| **PARÁMETRO** | **VALOR** |
| cursor\_sharing | EXACT |
| db\_block\_size | 16384 |
| db\_cache\_size | 2G |
| Db\_keep\_cache\_size | 3G |
| shared\_pool\_size | 1G |
| db\_file\_multiblock\_read\_count | 16 |
| db\_files | 2000 |
| db\_name | SPARKREF |
| db\_writer\_processes | 2 |
| instance\_name | SPARKREF |
| java\_pool\_size | 52428800 |
| job\_queue\_processes | 0 |
| large\_pool\_size | 209715200 |
| log\_buffer | 52428800 |
| open\_cursors | 3000 |
| pga\_aggregate\_target | 1G |
| Processes | 3000 |
| query\_rewrite\_enabled | FALSE |
| memory\_max\_target | 9G |
| memory\_target | 9G |
| star\_transformation\_enabled | FALSE |
| timed\_statistics | TRUE |
| undo\_management | AUTO |
| undo\_retention | 1800 |
| fast\_start\_mttr\_target | 600 |
| log\_checkpoint\_interval | 0 |
| log\_checkpoint\_timeout | 0 |
| workarea\_size\_policy | Auto |
| statistics\_level | Typical |
| optimizer\_mode | first\_rows |
| Recyclebin | Off |
| db\_cache\_advice | On |
| Parallel\_max\_servers | 20 |
| Deferred\_segment\_creation | FALSE |
| \_optim\_peek\_user\_binds | FALSE |
| \_optimizer\_adaptive\_cursor\_sharing | FALSE |
| \_kgl\_large\_heap\_warning\_threshold | 104857600 |
| \_ash\_size | 201326592 |

**Note:**

Disable the following scheduler jobs-

* EXEC DBMS\_AUTO\_TASK\_ADMIN.DISABLE ('AUTO OPTIMIZER STATS COLLECTION', NULL, NULL);
* EXEC DBMS\_AUTO\_TASK\_ADMIN.DISABLE ('AUTO SPACE ADVISOR', NULL, NULL);

### Inicialización de parámetros para la instancia SPARKUSG

|  |  |
| --- | --- |
| **PARÁMETRO** | **VALOR** |
| cursor\_sharing | EXACT |
| db\_block\_size | 16384 |
| db\_cache\_size | 2G |
| Db\_keep\_cache\_size | 1G |
| shared\_pool\_size | 2G |
| db\_file\_multiblock\_read\_count | 16 |
| db\_files | 2000 |
| db\_name | SPARKUSG |
| db\_writer\_processes | 2 |
| instance\_name | SPARKUSG |
| java\_pool\_size | 52428800 |
| job\_queue\_processes | 0 |
| large\_pool\_size | 209715200 |
| log\_buffer | 52428800 |
| open\_cursors | 3000 |
| pga\_aggregate\_target | 1G |
| Processes | 3000 |
| query\_rewrite\_enabled | FALSE |
| memory\_max\_target | 10G |
| memory\_target | 10G |
| star\_transformation\_enabled | FALSE |
| timed\_statistics | TRUE |
| undo\_management | AUTO |
| undo\_retention | 1800 |
| fast\_start\_mttr\_target | 600 |
| log\_checkpoint\_interval | 0 |
| log\_checkpoint\_timeout | 0 |
| workarea\_size\_policy | Auto |
| statistics\_level | Typical |
| optimizer\_mode | First\_rows |
| Recyclebin | Off |
| db\_cache\_advice | On |
| Parallel\_max\_servers | 20 |
| Deferred\_segment\_creation | FALSE |
| \_optim\_peek\_user\_binds | FALSE |
| \_optimizer\_adaptive\_cursor\_sharing | FALSE |
| \_kgl\_large\_heap\_warning\_threshold | 104857600 |
| \_ash\_size | 201326592 |

|  |  |  |
| --- | --- | --- |
| **NOMBRE DEL ARCHIVO** | **UBICACIÓN** | **INFORMACION A SER MODIFICADA** |
| limits.conf | /etc/ | grid soft nproc 2047  grid hard nproc 16384  grid soft nofile 1024  grid hard nofile 65536  oracle soft nproc 2047  oracle hard nproc 16384  oracle soft nofile 1024  oracle hard nofile 65536 |
| sysctl.conf | /etc/ | #tunning oracle  kernel.shmall = 6291456  kernel.shmmax=      25769803776  kernel.shmmni = 4096  kernel.sem = 250 32000 100 128  fs.file-max = 6815744  net.ipv4.ip\_local\_port\_range = 9000 65500  net.core.rmem\_default = 262144  net.core.rmem\_max = 4194304  net.core.wmem\_default = 262144  net.core.wmem\_max = 1048576  fs.aio-max-nr = 1048576 |

Servidor: **net-pbdfmra01**

Nombre del Archivo: **listener.ora**

# listener.ora Network Configuration File: /oracle/app/grid/11.2.0/network/admin/listener.ora

# Generated by Oracle configuration tools.

LISTENER =

  (DESCRIPTION\_LIST =

    (DESCRIPTION =

      (ADDRESS = (PROTOCOL = IPC)(KEY = extproc))

      (ADDRESS = (PROTOCOL = TCP)(HOST = net-pbdfmra01)(PORT = 1522))

    )

  )

ADR\_BASE\_LISTENER = /oracle/app/grid

ENABLE\_GLOBAL\_DYNAMIC\_ENDPOINT\_LISTENER=ON              # line added by Agent

SID\_LIST\_LISTENER =

(SID\_LIST =

    (SID\_DESC =

        (SDU = 8192)         # Setting SDU to 8192 for this SID

        (TDU = 8192)

     (SID\_NAME = SPARKREF)

        (ORACLE\_HOME = /oracle/app/oracle/product/11.2.0/db\_1))

    (SID\_DESC =

        (SDU = 8192)         # Setting SDU to 8192 for this SID

        (TDU = 8192)

     (SID\_NAME = SPARKUSG)

        (ORACLE\_HOME = /oracle/app/oracle/product/11.2.0/db\_1))

     (SID\_DESC =

        (SID\_NAME = extproc)

        (ORACLE\_HOME = /oracle/app/oracle/product/11.2.0/db\_1)

        (PROGRAM = extproc)

        (ENVS="EXTPROC\_DLLS=ANY, LD\_LIBRARY\_PATH=/rocfm\_software/NIKIRAROOT/lib:/rocfm\_software/NIKIRATOOLS/DAME/lib:/oracle/app/oracle/product/11.2.0/db\_1/lib:"))

)

INBOUND\_CONNECT\_TIMEOUT\_LISTENER =0

Servidores: **net-pappra01; net-pappfms01; net-pappfms02; net-pwebfmra01; net-pbdfmra01**

Nombre del Archivo: **tnsnames.ora**

# tnsnames.ora Network Configuration File: /oracle/app/oracle/product/11.2.0/db\_1/network/admin/tnsnames.ora

# Generated by Oracle configuration tools.

LISTENER\_SPARKREF =

  (ADDRESS = (PROTOCOL = TCP)(HOST = net-pbdfmra01)(PORT = 1522))

LISTENER\_SPARKUSG =

  (ADDRESS = (PROTOCOL = TCP)(HOST = net-pbdfmra01)(PORT = 1522))

SPARKREF =

  (DESCRIPTION =

    (ADDRESS = (PROTOCOL = TCP)(HOST = net-pbdfmra01)(PORT = 1522))

    (CONNECT\_DATA =

      (SERVER = DEDICATED)

      (SERVICE\_NAME = SPARKREF)

    )

  )

SPARKUSG =

  (DESCRIPTION =

    (ADDRESS = (PROTOCOL = TCP)(HOST = net-pbdfmra01)(PORT = 1522))

    (CONNECT\_DATA =

      (SERVER = DEDICATED)

      (SERVICE\_NAME = SPARKUSG)

    )

  )

Se adjunta a esta documentación los manuales de instalación y configuración de la aplicación entregadas por el proveedor al igual que un video con el paso a paso de paso entre ambientes.

/Guía de Instalación

ROC\_Fraud\_Management\_Installation\_Guide\_8.0.1\_04\_A.pdf



ROC\_Revenue\_Assurance\_Installation\_Guide\_5.0\_SP1\_QFE\_595\_04\_A.pdf



/Pasos entre ambientes

Para realizar el paso entre ambientes de entidades de RA.doc

Config\_RocRA\_01.mp4





/\*\*\*\*\*\*\*\*\*\*\*\*\*Documentos levantados por UNE en la instalación inicial\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*



## *Configuraciones de Sistema Operativo*

Archivos del sistema operativo que deben ser modificados, crontabs, archivos con configuración, rutas estáticas, link simbólicos, cuentas técnicas etc.

Parámetros del Kernel configurados:

|  |  |  |
| --- | --- | --- |
| **SERVIDOR** | **INITIALIZATION PARAMETER** | **VALUE REQUIRED** |
| net-pappra01  net-pappfms01  net-pappfms02  net-pwebfmra01 | kernel.shmmax | Total Memory |
| kernel.shmall | SHMMAX/ pagesize |
| kernel.shmmni | 4096 |
| kernel.sem | 250 32000 100 128 |
| fs.file-max | 6815744 |
| net.ipv4.ip\_local\_port\_range | 9000 65500 |
| net.core.rmem\_default | 262144 |
| net.core.rmem\_max | 4194304 |
| net.core.wmem\_default | 262144 |
| net.core.wmem\_max | 1048576 |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 |
| fsize | -1 |
| core | 2097151 |
| cpu | -1 |
| data | -1 |
| rss | -1 |
| stack | 65536 |
| nofiles | 65536 |
| threads | -1 |
| nproc | -1 |

Cambios en archivos del sistema

|  |  |  |  |
| --- | --- | --- | --- |
| **SERVIDOR** | **NOMBRE DEL ARCHIVO** | **UBICACIÓN** | **INFORMACION A SER MODIFICADA** |
| net-pappra01  net-pappfms01  net-pappfms02  net-pwebfmra01  net-pbdfmra01 | hosts.allow | /etc/ | ALL: 10.100.82.0/255.255.255.0  “para que puedan ser alcanzados por servidores en la misma VLAN”  ALL: 10.183.8.0/255.255.255.0  “Para que permita conexiones desde la VPN externa” |
| hosts.deny | /etc/ | ALL: ALL |

**Reglas de Firewall**

**IPTABLE DEL SERVIDOR.**

Table: filter

Chain INPUT (policy ACCEPT)

num  target     prot opt source               destination

1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0

3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0

4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22

5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:28002

6    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0

7    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

num  target     prot opt source               destination

1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

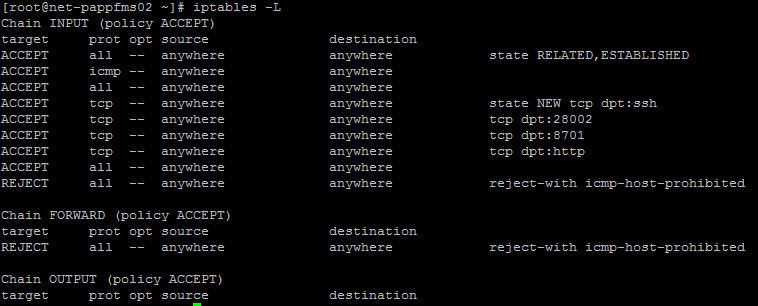
num  target     prot opt source               destination

**SELINUX:**

[root@net-pappra01 ~]# getenforce

Enforcing

IPTABLES SERVIDOR 10.100.82.23 – ONLINE



**Cuentas técnicas**

|  |  |  |
| --- | --- | --- |
| **SERVIDOR** | **GRUPO** | **CUENTA** |
| net-pappra01  net-pappfms01  net-pappfms02  net-pwebfmra01 | ra\_fm  GID: 1000 | Lrocra |
| Lrocfm |
| Oracle |
| subex-support  “Cuenta de soporte creada para el proveedor” |
| net-pbdfmra01 | Oinstall | Oracle |
| N/A | subex-support  “Cuenta de soporte creada para el proveedor” |
| net-pdice01 | N/A | Epmtelco\UNEdiceap |

***Configuraciones de Especiales de TOMCAT***

*No se hicieron configuraciones manuales, el setup de la aplicación deja los archivos con la configuración necesaria para el correcto funcionamiento de la aplicación.*

# SERVICIOS

Servicios necesarios para el correcto funcionamiento de la Aplicación

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Servidor 1**  **net-pappra01**  **10.100.82.25** | **Servidor 2**  **net-pappfms01**  **10.100.82.22** | **Servidor 3**  **net-pappfms02**  **10.100.82.23** | **Servidor 4**  **net-pwebfmra01**  **10.100.82.24** | **Servidor 5**  **net-pbdfmra01**  **10.100.67.119** | **Servidor 6**  **net-pdice01**  **10.100.82.19** |
|  |  |  | TOMCAT (RA)  Apache (FM) | Oracle Enterprise 11g |  |
| SendMail | SendMail | SendMail | SendMail | SendMail |  |
| Oracle Client 11g | Oracle Client 11g | Oracle Client 11g | Oracle Client 11g |  | Oracle Client 11g |
| Task Controller | ROCRA  Core Engine |  | ROCRA Client |  |  |
| Stream Controller | ROCRA  Core Engine |  | ROCRA  Client |  |  |
|  |  | **Inline Apache (Apache WSDL)** |  |  |  |

*Subir y bajar servicios y daemons*

### ROC Fraud Management – Detener Aplicación

| Servicio(s) | Usuario | Comando |
| --- | --- | --- |
| ROC Fraud Management Client (10.100.82.24) | **lrocfm** | $ src $ ./fmsclientctl.sh stop |
| ROCFM Core (10.100.82.22) | **lrocfm** | $ cd Subex\_Working\_Area/EAM  $ . export.sh $ run.pl stop |

### ROC Fraud Management - Iniciar Aplicación

| Servicio(s) | Usuario | Comando |
| --- | --- | --- |
| ROC Fraud Management Client (10.100.82.24) | **lrocfm** | $ src $ ./fmsclientctl.sh start |
| ROCFM Core (10.100.82.22) | **lrocfm** | $ cd Subex\_Working\_Area $ run.pl start |

### ROC Fraud Management & ROC Revenue Assurance - Detener Spark

| Process | User | Command |
| --- | --- | --- |
| Spark Client  (10.100.82.24) | **lrocra** | $ jps $ ./shutdown.sh |
| Spark Process (10.100.82.25) | **lrocra** | $ bin kill -15 <pid of StreamControllerService > kill -15 <pid of TaskControllerService > |

### ROC Fraud Management & ROC Revenue Assurance - Iniciar Spark

| Servicio(s) | Usuario | Comando |
| --- | --- | --- |
| Spark Client  (10.100.82.24) | **lrocra** | $ tomcat $ ./startup.sh |
| Spark Process (10.100.82.25) | **lrocra** | $ bin $ ./nohup\_sc.sh $ ./nohup\_tc.sh |

**Inline Service start up:**

**Cuando hay un problema general con la conexión de la base de datos se reinician los 3 servicios, si solo se necesita reiniciar el proceso Online solo se reinician los servicios del servidor 10.100.82.23**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Name** | **Server** | **User** | **Command** |
| FMS Client | 10.100.82.24 | lrocfm | $ src $ ./fmsclientctl.sh start |
| Apache Web server | 10.100.82.23 | Lrocfm | $ cd /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/bin $ ./apachectl start |
| ROCFM Inline Core | 10.100.82.23 | lrocfm | $ cd Subex\_Working\_Area $ run.pl start |

## Inline Service Stop:

**Cuando hay un problema general con la conexión de la base de datos se paran los 3 servicios, si solo se necesita detener el proceso Online solo se detienen los servicios del servidor 10.100.82.23**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Name** | **Server** | **User** | **Command** |
| FMS Client | 10.100.82.24 | lrocfm | $ src $ ./fmsclientctl.sh stop |
| Apache Web Server | 10.100.82.23 | lrocfm | $ cd /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/bin $ ./apachectl stop |
| ROCFM Core | 10.100.82.23 | lrocfm | $ cd Subex\_Working\_Area/EAM  $ . export.sh $ run.pl stop |

Igualmente Subex construyó las Shells adjuntas para subir automáticamente los servicios de Spark “**S**tream**C**ontroller y **T**ask**C**ontroller” cuando se reinicie el servidor net-pappra01.

**NOTA**: Estas Shells automáticamente renombran los archivos log de dichos servicios por si es requerida una revisión de un algún fallo, se pueda encontrar la historia y no se borre su contenido al iniciarse de nuevo el servicio.



Contenido restart\_sc.sh

----------------------------------------------------------------------------------------------------

#!/bin/sh

SCRIPT\_DIR=/rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/logs

LOG\_DIR=/rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/logs

BIN\_DIR=/rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/bin

cp $LOG\_DIR/stream\_controller.log $SCRIPT\_DIR/`date "+%y%m%d"`\_stream\_controller.log

cd $BIN\_DIR

./nohup\_sc.sh

----------------------------------------------------------------------------------------------------

Contenido restart\_tc.sh

----------------------------------------------------------------------------------------------------

#!/bin/sh

SCRIPT\_DIR=/rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/logs

LOG\_DIR=/rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/logs

BIN\_DIR=/rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/bin

cp $LOG\_DIR/task\_controller.log $SCRIPT\_DIR/`date "+%y%m%d"`\_task\_controller.log

cd $BIN\_DIR

./nohup\_tc.sh

----------------------------------------------------------------------------------------------------

# PUERTOS

A continuación se presenta una tabla con la lista de puertos que debe tener habilitados cada uno de los servidores de la solución

## *Puertos Internos de la Aplicaciones*

| Proceso | Puerto(s) |
| --- | --- |
| ROC Fraud Management Client  (10.100.82.24) | 8080,8700 , 9000 |
| ROC Fraud Management Core Executables (10.100.82.22) | 20000, 20001, 20003, 20204, 21000, 25001, 25002, 30001, 35001, 50001, 50011, 50012, 50003, 50101, 50201, 50301, 50401, 50502, 90001, 90002, 90012, 90095, 90096, 90097, 90098 |
| Spark Client (10.100.82.24) | 8790, |
| Stream Controller (10.100.82.25) | 7770, 7777 |
| Task Controller (10.100.82.25) | 7779 |
| DICE (10.100.82.26) | 8080 Internet traffic 8081 Internet traffic 8090 Network traffic 4437 Dice 4747 QV Server 4774 QVS Server Tunnel 80 Accespoint 443 Accesspoint 4780 QMC/QEMC 4710 Command Center 4720 Distribution Service 4730 Directory Service Connector 4750 Web Server 4799 Remote QMS 14747 QVS.exe 4711 Command Center 4781 Management Service 4748 QlikView Server |

# COMUNICACIONES

De la arquitectura de servidores implantada para ROC, sólo el servidor net-pappra01 se comunica con los servidores del Charging Gatway y de Archivos del HSS para importar archivos planos dejados por dichas plataformas, es conocido dentro del sistema como captura de archivos PULL.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP ORIGEN** | **PUERTO ORIGEN** | **TIPO** | **IP DESTINO** | **PUERTO DESTINO** | **TIPO** | **DESCRIPCION** |
| net-pappfm01  10.100.82.22 | 22 | SFTP | ATCAX86\_F0S8  10.153.3.4 | 22 | SFTP | Comunicación con Charging Gateway **Medellín** para importar los archivos planos que genera la plataforma con información de 4G LTE  **Usuario**: rocra  **Password**: cdrlte2013 |
| net-pappfm01  10.100.82.22 | 22 | SFTP | ATCAX86\_F0S4  10.153.13.4 | 22 | SFTP | Comunicación con Charging Gateway **Bogotá** para importar los archivos planos que genera la plataforma con información de 4G LTE  **Usuario**: rocra  **Password**: cdrlte2013 |
| net-pappra01  10.100.82.25 | 22 | SFTP | unevm-pmvftp01  10.158.123.8 | 22 | SFTP | Comunicación con servidor de archivos del HSS  **Usuario**: cdr\_lte  **Password**: UoGb1234-% |

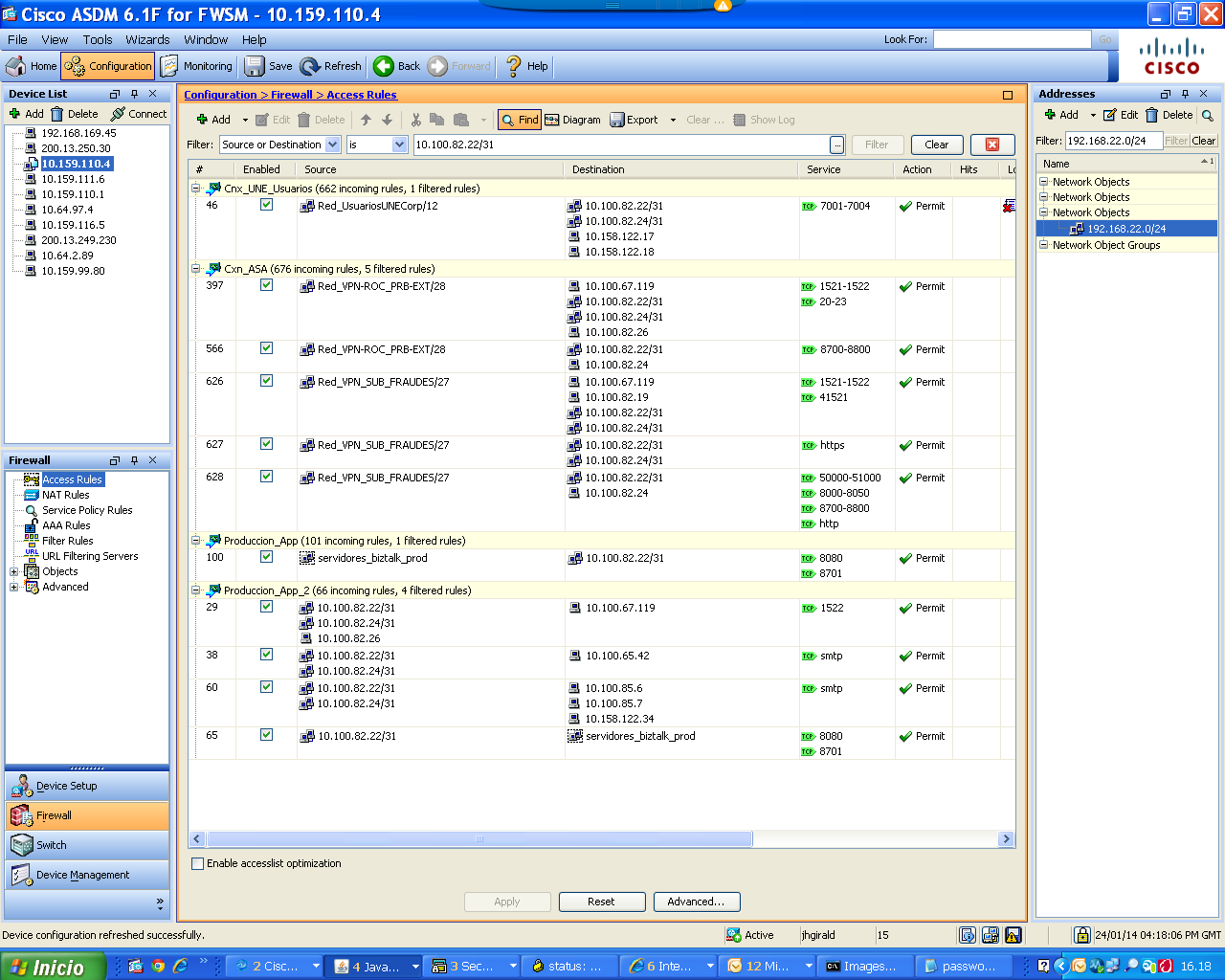
Para el caso del Charging Gateway para que se acepten peticiones desde la IP origen, se deben hacer cambios en SO de los servidores y solicitar una ventana para reiniciarlos.

Adjunto archivos del sistema modificados:



Además de esto se debe realizar un enrutamiento en la red metro para que alcance los servidores de ROC FM, para este caso el 10.100.82.22 (net-pappfm01)

# REGLAS CONFIGURADAS EN EL FIREWALL



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **IP ORIGEN** | **HOST ORIGEN** | **IP DESTINO** | **HOST DESTINO** | **PUERTO** | **TIPO** | **SERVICIO** | **DESCRIPCION** |
| 10.100.82.22 | net-pappfms01 | 10.100.68.12 | app-files | 1234  111  2049  635 | TCP | mount  Information and warning  NFS  NAS | Permisos para que los servidores de ROC, puedan alcanzar la NAS. |
| 10.100.82.23 | net-pappfms02 |
| 10.100.82.25 | net-pappra01 |
| 10.100.82.24 | net-pwebfmra01 |
| 10.100.67.119 | net-pbdfmra01 |
| 10.100.82.26 | net-pdice01 | 10.100.68.11 |
| 10.100.82.22 | net-pappfms01 | 10.100.67.119 | net-pbdfmra01 | 1522 | TCP | Oracle listener | Permisos para que los servidores de aplicación de ROC, puedan alcanzar el servidor de base de datos. |
| 10.100.82.23 | net-pappfms02 |
| 10.100.82.25 | net-pappra01 |
| 10.100.82.24 | net-pwebfmra01 |
| 10.100.82.26 | net-pdice01 | Permisos para que el servidor de reportes de QlikView, pueda alcanzar el servidor de base de datos. |
| 10.100.82.25 | net-pappra01 | 10.153.3.4 | MED: ATCAX86\_F0S8 | 22 | TCP | SFTP | Permisos para que el servidor de ROC donde corre Spark pueda importar los archivos del Charging Gateway y HSS. |
| 10.153.13.4 | BOG: ATCAX86\_F0S4 |
| 10.158.123.8 | unevm-pmvftp01 |
| 10.158.106.31 | une-pldapbog01 | 10.158.100.1 | app-files | 1234  111  2049  635 | TCP | mount  Information and warning  NFS  NAS | Permisos para que en los servidores origen se pueda montar el file system de NAS dónde copiaran los archivos de insumo. |
| 10.158.106.14 | une-pldap03 |
| 10.158.134.5 | unevm-pmap01 |
| 10.158.134.6 | unevm-pmap02 |
| 10.158.134.7 | unevm-pmap03 |
| 10.158.134.4 | unevm-pmap04 |
| 10.158.134.9 | unevm-pmap05 |
| 10.158.134.32 | unevm-pmap06 |
| 10.158.134.33 | unevm-pmap07 |
| 10.158.134.34 | unevm-pmap08 |
| 10.158.134.28 | unevm-pmapcron |
| 10.100.67.31 | net-pltebd01-01 | 10.100.68.12 |
| 10.120.53.129 | net\_po01 |
| 10.100.67.153 | net-pltebd01-02 |
| 10.100.67.137 | net-pora20 |
| NETVM-PBIZ01-01 | 10.100.66.195 | net-papppfms02 | **10.100.82.23** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-02 | 10.100.66.197 | net-papppfms02 | **10.100.82.23** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-03 | 10.100.66.83 | net-papppfms02 | **10.100.82.23** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-04 | 10.100.66.84 | net-papppfms02 | **10.100.82.23** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-05 | 10.100.66.87 | net-papppfms02 | **10.100.82.23** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-06 | 10.100.66.86 | net-papppfms02 | **10.100.82.23** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-01 | 10.100.66.195 | net-papppfms01 | **10.100.82.22** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-02 | 10.100.66.197 | net-papppfms01 | **10.100.82.22** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-03 | 10.100.66.83 | net-papppfms01 | **10.100.82.22** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-04 | 10.100.66.84 | net-papppfms01 | **10.100.82.22** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-05 | 10.100.66.87 | net-papppfms01 | **10.100.82.22** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| NETVM-PBIZ01-06 | 10.100.66.86 | net-papppfms01 | **10.100.82.22** | 8701 | TCP | http | Servicio de integración en línea para Score de Fraudes (Biztalk – ROC) |
| net-papppfms02 | **10.100.82.23** | NETVM-PBIZ01-01 | 10.100.66.195 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms02 | **10.100.82.23** | NETVM-PBIZ01-02 | 10.100.66.197 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms02 | **10.100.82.23** | NETVM-PBIZ01-03 | 10.100.66.83 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms02 | **10.100.82.23** | NETVM-PBIZ01-04 | 10.100.66.84 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms02 | **10.100.82.23** | NETVM-PBIZ01-05 | 10.100.66.87 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms02 | **10.100.82.23** | NETVM-PBIZ01-06 | 10.100.66.86 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms01 | **10.100.82.22** | NETVM-PBIZ01-01 | 10.100.66.195 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms01 | **10.100.82.22** | NETVM-PBIZ01-02 | 10.100.66.197 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms01 | **10.100.82.22** | NETVM-PBIZ01-03 | 10.100.66.83 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms01 | **10.100.82.22** | NETVM-PBIZ01-04 | 10.100.66.84 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms01 | **10.100.82.22** | NETVM-PBIZ01-05 | 10.100.66.87 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |
| net-papppfms01 | **10.100.82.22** | NETVM-PBIZ01-06 | 10.100.66.86 | 80 | TCP | http | Servicio de integración en línea para Score de Fraudes (ROC – Biztalk) |

# VPN

Para el acceso por parte de proveedor “Subex” de forma remota a los servidores del ambiente de producción, se solicito crear la siguiente VPN con los siguientes usuarios y permisos que se detallan a continuación:

Nombre VPN: ROC\_PRB-EXT

|  |  |  |  |
| --- | --- | --- | --- |
| **IP DESTINO** | **HOST DESTINO** | **PUERTO** | **SERVICIO** |
| 10.100.82.25 | net-pappra01 | 8750 | 7777 | 7779 7770 | 7771 | 7772  7773 | 7774 |7775  7776 | ROC**RA** Application  ROC**WEB** Server |
| 10.100.82.24 | net-pwebfmra01 |
| 10.100.82.22 | net-pappfms01 | 8000 to 8050  50000 to 51000  8700 to 8800  80 | ROC**RA** Application  ROC**WEB** Server |
| 10.100.82.23 | net-pappfms02 |
| 10.100.82.24 | net-pwebfmra01 |
| 10.100.82.25 | net-pappra01 | 443 | https |
| 10.100.82.22 | net-pappfms01 |
| 10.100.82.23 | net-pappfms02 |
| 10.100.82.24 | net-pwebfmra01 |
| 10.100.82.25 | net-pappra01 | 1522  20/21  22  23 | Oracle listener  ftp  ssh/sftp  telnet |
| 10.100.82.22 | net-pappfms01 |
| 10.100.82.23 | net-pappfms02 |
| 10.100.82.24 | net-pwebfmra01 |
| 10.100.67.119 | net-pbdfmra01 |
| 10.100.82.26 | net-pdice01 |
| 10.100.82.26 | net-pdice01 | 8080 | 8090 8081 | 4437 3389  4747/tcp 4774/tcp 80/tcp 443/tcp 4780/tcp 4710/tcp 4720/tcp 4730/tcp 4750/tcp 4799/tcp 14747/udp 4711/udp 4781/udp 4748/udp 4721/udp 4731/udp | MAST/Dashboard **Dice “QlikView”** |

Usuarios creados:

|  |  |  |
| --- | --- | --- |
| **NOMBRE DE LA VPN** | **NOMBRE DEL CONSULTOR** | **LOGUIN** |
| ROC\_PRB-EXT | Agustin Smith | sop.asmith |
| Lourdes Barreno | sop.lbarreno |
| Ravi Khurana | sop.rkhurana |
| Kalpana K. | sop.kalpana |
| Matias Bonacossa | sop.mbonacossa |
| Raghu G. | sop.raghug |

Para el acceso a los servidores de producción para temas de soporte la Subdirección de seguridad recomendó utilizar la misma VPN.

# FTP Seguro

Para compartir archivos de gran volumen se solicitó crear el siguiente FTP seguro de 10GB para que el proyecto pueda compartir documentos con el proveedor.

\\net-file\FTPseguro\PROY\_FRAU\_ASE\_INGR

Este FTP debe de eliminarse con la finalización del proyecto.

# CONFIGURACIONES EN EL F5

No fueron realizadas configuraciones en el **F5** para este sistema de información.

|  |  |  |
| --- | --- | --- |
| **NOMBRE DEL POOL** | **NOMBRE DEL SERVIDOR** | **IP DEL SERVIDOR** |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **NOMBRE DEL VIRTUAL SERVER** | **NOMBRE DEL SERVIDOR** | **IP DEL SERVIDOR** |
|  |  |  |

# MANEJO DE LOGS

A continuación se detallan los archivos de logs de la aplicación; mecanismo de rotación y depuración son administrados directamente por el sistema de información.

|  |  |  |  |
| --- | --- | --- | --- |
| **TIPO DE LOG** | **RUTA** | **NOMBRE DEL ARCHIVO** | **DESCRIPCION** |
| Query Manager | 10.100.82.24:/lhome.lrocfm/NIKIRACLIENT/querymanager/LOG | query\_manager.log | Este archivo Log contiene información de las consultas ejecutadas, canceladas, eliminadas sobre la las bases de datos SPARKREF & SPARKUSG, desde la interfaz de usuario. |
| Notification Manager | 10.100.82.24:/home/lrocfm/NIKIRACLIENT/notificationmanager/log/ | notification\_manager.log | Este módulo mantiene la información de registro de errores para ROC Fraud Management Core, Pseudo Rater, and ROC Fraud Management Client.  Los mensajes de error se clasifican en base a los niveles que se pueden configurar en el archivo de configuración.  **$NIKIRACLIENT**/../notificationmanager/config/error\_logger\_config.yml  Los siguientes son los tipos de mensajes de error:  • TRACE  • DEBUG  • WARNING  • ERROR  • CRITICAL  • FATAL |
| Apache | 10.100.82.24:/lhome/lrocfm/NIKIRATOOLS/APACHE/logs/ | error\_log | Contiene información de procesos relacionados con Apache |
| **Spark**  Stream Controller | 10.100.82.25: /rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/logs | stream\_controller.log | Contiene información de las tareas de procesamiento y carga de información tanto para ROC Revenue Assurance como para ROC Fraud Management. |
| **Spark**  Task Controller | task\_controller.log |
| ROCFM Core Engine | 10.100.82.24:/lhome/lrocfm/NIKIRACLIENT/src/../notificationmanager/app\_logs/server/ | **Use Alias** : slog  ó  all\_modules\_all\_users\_all\_ips.log |  |
| Tareas de Cargue a ROCFM Core Engine | 10.100.82.25:/rocfm\_data/FMSData/DS\_LOG/ | **{fuente de datos}/{task}** | Contiene información log de las tareas ejecutadas en ROCFM |
| Inline Process | 10.100.82.23: /lhome/lrocfm/NIKIRACLIENT/InlineWrapperService/log/orderLog | **UneOrder.log** | Contiene el log de los pedidos procesados en el precheck Online, en caso de error deja los errores. |

# VERIFICACIÓN DE COMPONENTES Y FUNCIONALIDADES

Para verificar que tanto la aplicación de ROC Fraud Management y ROC Revenue Assurance se encuentran corriendo y operativos se deben verificar los siguientes servicios:

|  |  |  |  |
| --- | --- | --- | --- |
| **SERVICIO** | **TIPO** | **COMANDO** | **DESCRIPCION** |
| FMS Client | En ejecución | net-pwebfmra01 (10.100.82.24)  $ src $ ./fmsclientctl.sh status | Verificación de los servicios asociados a ROC Fraud Management Cliente.  Con este comando se identifican todos los procesos, cuales están en ejecución y cuáles no.  Ej., de ejecutar el comando **fmsclientctl.sh** status.  Juggernaut: [Running] Memcached: [Already Running] Querymanager: [Running] Notificationmanager: [Running] Apache: [Running] Dashboard: [Running] |
| Apache TOMCAT | En ejecución | 10.100.82.24  [lrocra@net-pwebfmra01 ~]$ jps | Verificación del TOMCAT.  Ej., de ejecutar el comando **jps**.  <PID> Jps <PID> jar  Si no aparece "jar" significa que el Tomcat no está corriendo |
| Stream Controller | En ejecución | 10.100.82.25  [lrocra@net-pappra01 ~]$ jps | Verificación del Stream Controller.  Ej., de ejecutar el comando **jps**.  <PID> StreamControllerService <PID> Jps <PID> TaskControllerService  Si no aparece " StreamControllerService " significa que el servicio no está corriendo.  Para reiniciar el servicio   1. Ir al directorio:  /rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/bin 2. Ejecutar el script: **nohup\_sc.sh** |
| Task Controller | En ejecución | 10.100.82.25  [lrocra@net-pappra01 ~]$ jps | Verificación del Stream Controller.  Ej., de ejecutar el comando **jps**.  <PID> StreamControllerService <PID> Jps <PID> TaskControllerService  Si no aparece " TaskControllerService " significa que el servicio no está corriendo.  Para reiniciar el servicio:   1. Ir al directorio:  /rocra\_software/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Server/bin 2. Ejecutar el script: **nohup\_tc.sh** |
| ROCFM Core Engine | En ejecución | net-pappfms01 (10.100.82.22)  $ cd Subex\_Working\_Area/EAM $ run.pl status | Verificación que los procesos de ROCFM Core están corriendo.  Ej., de ejecutar el comando **run.pl status**.  \* 0 < 1 alarmdenormalizer2  PIDS: \*\*\*SLAVE\*\*\*  1 = 1 alarmgenerator1  PIDS: 17933 \*\*\*SLAVE\*\*\* \* 0 < 1 rtfalertgenerator1  PIDS: \*\*\*SLAVE\*\*\*  1 = 1 smartpatternprocessor  PIDS: 17945 \*\*\*SLAVE\*\*\*  2 = 2 EAM  Si aparecen procesos antepuestos por un asterisco significa que dicho proceso no se está ejecutando.  Para reiniciar **todos** los procesos **“Consultar con equipo Dllo”**:  $ cd Subex\_Working\_Area/EAM $ **run.pl stop** $ **run.pl start** |
| URL App Fraudes | Conectividad | <http://10.100.82.24:8700> | Con la herramienta SiteScope verificación que la URL funciona. |
| URL App Aseguramiento | Conectividad | http://10.100.82.24:8080/UNEColombia\_ROCRevenueAssurance5.0\_SP1-Client/sparkLogin.jsp | Con la herramienta SiteScope verificación que la URL funciona |
| Qlik View | En ejecución | net-pdice01 (10.100.82.26) | Con la herramienta Scom se verifica que los siguientes servicios de windows estén en ejecución:  QlikviewDirectoryServiceConnector  QlikViewDistributionService  QlikviewManagementService  QlikviewServer  QlikviewWebserver |
| ROCFM Core Engine | En ejecución | Check ROCFM Inline Core Engine  $ cd Subex\_Working\_Area/EAM $ run.pl status | Expected Output : It shows all the process running on App server. Showing \* in front of process means particular process is not running.  (For example :  \* 0 < 1 IrmAgent  PIDS: \*\*\*SLAVE\*\*\*  1 = 1 alarmgenerator1  PIDS: 17933 \*\*\*SLAVE\*\*\* \* 0 < 1 Record Processor  PIDS: \*\*\*SLAVE\*\*\*  1 = 1 smartpatternprocessor  PIDS: 17945 \*\*\*SLAVE\*\*\*  2 = 2 EAM  IrmAgent and Record Processor is not running in above case.  Here 0 < 1 means 1 process expected and 0 process running and 1= 1 means 1 process expected and 1 process is running)  Significance : Responsibility of rocfm core engine to process the raw file , check for rule violation and if rule is violated generate the alarm.  Log File : Available on 10.100.82.24 Use Alias : slog or   /rocfm\_software/NIKIRACLIENT/src/../notificationmanager/app\_logs/server/all\_modules\_all\_users\_all\_ips.log   Action to resolve:  on 10.100.82.23 Check the error messages in Log file. Execute : $ cd Subex\_Working\_Area/EAM $ run.pl stop $ run.pl start  If still all process not comes up, contact Subex support team. |
| ROC- ONLINE | En Ejecución | Revisar si el Servicio de APACHE\_WSDL está funcionando de manera correcta  Servidor : 10.100.82.23 net-pappfms02  Ejecutar el comando  ps -eaf|grep $LOGNAME | Revisar que esté corriendo al menos un proceso con  /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/conf/httpd.conf -k start  Y al menos un proceso con  /rocfm\_software/NIKIRAROOT/FMSData/InlineStoreData/  Ejemplo de salida del comando  lrocfm 8797 1 0 Feb28 ? 00:00:10 /rocfm\_software/NIKIRATOOLS/APAC HE\_WSDL/bin/httpd -f /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/conf/httpd.conf -k start  lrocfm 8798 8797 0 Feb28 ? 00:00:05 /rocfm\_software/NIKIRATOOLS/APAC HE\_WSDL/bin/httpd -f /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/conf/httpd.conf -k start  lrocfm 8799 8797 0 Feb28 ? 00:02:00 /rocfm\_software/NIKIRATOOLS/APAC HE\_WSDL/bin/httpd -f /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/conf/httpd.conf -k start  root 9819 2749 0 14:32 ? 00:00:00 sshd: lrocfm [priv]  lrocfm 9823 9819 0 14:32 ? 00:00:00 sshd: lrocfm@notty  lrocfm 9824 9823 0 14:32 ? 00:00:00 /usr/libexec/openssh/sftp-server  root 9876 2749 0 14:41 ? 00:00:00 sshd: lrocfm [priv]  lrocfm 9880 9876 0 14:41 ? 00:00:00 sshd: lrocfm@pts/2  lrocfm 9881 9880 0 14:41 pts/2 00:00:00 -bash  lrocfm 9975 9881 0 14:57 pts/2 00:00:00 ps -eaf  lrocfm 9976 9881 0 14:57 pts/2 00:00:00 grep lrocfm  lrocfm 19354 1 0 Mar04 ? 00:00:04 ./programmanager -f programmanag er.conf.tcp.inline\_orig  lrocfm 19356 19354 0 Mar04 ? 00:00:00 alarmgenerator -r TCP://[127.0.0 .1]:8901 -w TCP://[10.100.82.22]:50017 -N 2 #AG  lrocfm 19364 19354 0 Mar04 ? 00:00:00 smartpatternprocessor -r TCP://[ 127.0.0.1]:8903 -w TCP://[127.0.0.1]:8901 #SP  lrocfm 19365 19354 0 Mar04 ? 00:00:02 recordprocessor -r TCP://[127.0. 0.1]:9023 -w TCP://[127.0.0.1]:8901 -s TCP://[127.0.0.1]:8903 -g INLINE\_RULES -G NOT\_APPLICABLE -l TCP://[127.0.0.1]:8904 -F 1 -C 1 -S -q TCP://[10.100.82.23]:5 678  lrocfm 19366 19354 0 Mar04 ? 00:00:00 irmagent -r IRMAGENT -p TCP://[1 27.0.0.1]:9023 -D 2 -P 1 -w /rocfm\_software/NIKIRAROOT/FMSData/InlineStoreData/ -q TCP://[10.100.82.23]:5678  lrocfm 19367 19354 0 Mar04 ? 00:00:37 recorddispatcher -c INLINE.STORE -r RFF:///rocfm\_software/NIKIRAROOT/FMSData/InlineStoreData/ -p TCP://[127.0.0. 1]:8905 -F 2 -q TCP://[10.100.82.23]:5678  lrocfm 23481 8798 0 Feb28 ? 00:00:30 ruby /rocfm\_software/NIKIRACLIEN T/InlineWrapperService/public/inlinedispatch.fcgi  lrocfm 23957 8798 0 Feb28 ? 00:00:26 ruby /rocfm\_software/NIKIRACLIEN T/InlineWrapperService/public/inlinedispatch.fcgi  lrocfm 23972 8798 0 Feb28 ? 00:00:26 ruby /rocfm\_software/NIKIRACLIEN T/InlineWrapperService/public/inlinedispatch.fcgi  Acciones para Corregir:  Reiniciar el Apache WSDL si no está corriendo  Servidor 10.100.82.23  cd /rocfm\_software/NIKIRATOOLS/APACHE\_WSDL/bin  ./apachectl stop  ./apachectl start  Reiniciar el Servicio Inline con run.pl servidor 10.100.82.23  ROCFM Inline Core  $ cd Subex\_Working\_Area $ run.pl stop  $ run.pl start  Reiniciar el cliente de Fraudes en el servidor 10.100.82.24  $ src $ ./fmsclientctl.sh stop  $ ./fmsclientctl.sh start |

# ERRORES COMUNES

Errores de operación conocidos: el documento adjunto tiene los errores reportados por la herramienta de monitoreo de fraudes ROC FM

Fraudes



Aseguramiento



ERRORES COMUNES ONLINE

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Symptoms** | **Possible Causes** | **Resolution Steps** |
| Alert- Failed to uncompress the file in Spark GUI | File collection has failed | File collection has been specified as compressed, and the input file is  Uncompressed | Input file needs to be uncompressed. |
| User login disabled | Failed user login for ‘User’ | 3 or more failed attempts to login to Moneta Client | Contact the administrator to enable the user |
| Dataload Fail | Dataload Failed In Tables | Check For Tables Definition/Tablespace for the corresponding Table on which Dataload Failed | Correct the Table Definition in DB as Per Moneta/Decoder or increase the table space if issue with table space |
| ROCRA GUI Slow | Search results take more time | Check if large number of Inactive sessions for moneta | Restart tomcat or kill the Inactive sessions |
| **Subscriber data** processing has not happened on a given day | There are no collected files, parse and dataload tasks created. | 1. Subscriber file hasn’t been collected for that given day.  2.SC/TCis not running  3. Stream is paused. | 1. Check the File source of Subscriber data and verify if there is a file available for Moneta to collect.  2. Start the services if they are down.  3. Resume the stream if it was in paused state due to some season. |
| **Tablespace** error on Reference DB when running Audits, Measures | Audit, Measures fail with the log saying that the run has failed due to problem with TEMP tablespace | Audits and Measures create tables to populate results. If TEMP tablespace cannot be extended then an error is thrown. | Speak to DBA and get table space added. |
| Files have not been collected for a given day | No files to be processed in Moneta. | This could happen due to files being unavailable on the collection points, collection points details getting changed without notice. | Reverify the file source path and the file format configured for file sources and make necessary changes according the files received. |
| Services status | It may happen so that the services seem like they have irresponsive for a prolonged period of time. | Problems with DB connection, communication between services/servers. | **1.** GO to the respective directories of the log files of all the services and check the file modified timestamp to find out if the services were logging.  **2.** Also, check last few lines of the log file to determine the current activity that the servers are busy with.  **3.** Run “ps –ef | java” command to find out if the processes are actually running. |
| Triggers not working | Dataload tasks are not being created/triggered. | Stream controller is not running/Trigger has been misconfigured | Start the stream controller if it is not running. Check the trigger configuration and verify if it is as expected. |
| Parse tasks, audit requests fail |  | File system , tablespace full | Remove unnecessary files and delete old audit requests for which case has been closed. |
| Files have been collected but go into waiting state | Moneta GUI displays parse task for this file as waiting | Task controller capabilities may have not been set | Under Streams , click on the task controller tab on the left pane and then on Task controller capabilities. Make sure that the capability for all the tasks is greater than 0 |
| Stream Controller/TaskControllers Out Of Service On GUI But Process running in background | SC/TC process running in background and logs being processed for SC | Upon restart GUI may not be able to update the SC status. | Restart Tomcat Application and check the status of SC on GUI |
| Decoder Changes not effective | Function Changes in decoder may not be reflecting in tables | Reinitialize may not be done for the stream on which the decoder changes are performed. | Reinitialize the stream or restart the TC’s. |

# SEGURIDAD

### ACCESO A LA APLICACIÓN

ROCFM y ROCRA tiene cada uno, un módulo de seguridad que permite configurar Roles y Usuarios sobre la aplicación, estos usuarios son locales y administrados directamente desde el aplicativo, en el entregable II del proyecto el proveedor hará la personalización de los dos aplicativos para que se integren con directorio activo.

Estos dos módulos serán administrados por el grupo de IDC Aplicaciones Corp quienes recibirán los requerimientos de service desk para hacer las respectivas configuraciones; A continuación se describen los perfiles de usuarios implantados en producción:

**ROC Revenue Assurance**

Convención:

T: Acceso Total

C: Acceso de Consulta

N: Sin acceso

A: Acceso sólo a las notificaciones de alarmas

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PERFIL | MODULOS DE ROC | | | | | | | USUARIOS  CREADOS |
| Monitoring | Case management | Revenue assurance | System | Security | Admin | Dashboard |
| Operaciones IDC | T | A | T | T | T | T | N | dgomeb |
| Gestión NOC | T | N | N | C | N | C | C |  |
| Administrador Funcional | T | T | T | T | C | T | T | pcardea wflorezc |
| Soporte Técnico | C | C | C | C | C | C | C | Asoto |
| Consulta | C | C | C | C | N | C | C |  |
| Administrador de Casos | C | T | C | C | N | C | C | chgomez ccanor pmartine pquinteu mvasquej aarroyav cmonsala |
| Configurador de Metricas/Auditorías | C | T | T | C | N | C | T |  |

**ROC Fraud Management**

|  |  |  |
| --- | --- | --- |
| PERFIL | FUNCIONALIDAD EN ROC | USUARIOS |
| Operaciones IDC |  | Dgomeb |
| Gestión NOC |  |  |
| Administrador Funcional | Alarm Management  Alarm Administration  Alarm Archive View  Case Management  Record View  Account View  Subscriber View  Nickname Management  Hotlist Management  ASN Management  Rule Test Facility  Rule Management  Named Filter Management  Advanced Query Management  Auto Threshold Management  Reports  Server Configurations  Audit Log  Workflow Management  I2 Task  Risk Management  Dashboard | ctaborda |
| Soporte Técnico | Alarm Management  Alarm Administration  Alarm Archive View  Case Management  Record View  Account View  Subscriber View  Nickname Management  Hotlist Management  ASN Management  Rule Test Facility  Rule Management  Named Filter Management  Advanced Query Management  Auto Threshold Management  Reports  Server Configurations  Audit Log  Workflow Management  I2 Task  Risk Management  Dashboard | Lfzuluag |
| Coordinador | Alarm Management  Alarm Administration  Alarm Archive View  Case Management  Record View  Account View  Subscriber View  Nickname Management  Hotlist Management  ASN Management Rule  Rule Test Facility  Rule Management  Named Filter Management  Advanced Query Management  Auto Threshold Management  Reports  Workflow Management  I2 Task  Risk Management |  |
| Analista | Alarm Management  Case Management  Record View  Account View  Subscriber View  Named Filter Management  Advanced Query Management  Named Filter Management  I2 Task |  |
| Nadmin | Es el root de la aplicación | Dgomeb |

### LOG

Las aplicaciones ROCFM y ROCRA guardan el LOG de todo lo que hace cada usuario sobre el sistema, como el cierre de alarmas, fecha hora de acción, gestión realizada, etc. dicho log es consultado a través de la interfaz de usuario.

### PRUEBAS DE INTRUSIÓN

Sobre las dos aplicaciones no se realizaron pruebas de intrusión ya que es una aplicación de uso interno, esto fue avalado por la analista de seguridad que nos acompañó en el proyecto.

# POLITICAS DE RESPALDOS

El proyecto se acogió a la política de respaldo estándar tanto para base de datos como para respaldos de los files systems:

\* Respaldos Diarios: Se realizan de lunes a viernes y tienen una retención de una (1) Semana

\* Respaldos Semanales: Se realizan una vez cada fin de semana (sábado o domingo) y tienen una retención de una (4) semanas

\* Respaldos Mensuales: Se realizan una vez al mes; último sábado o domingo del mes y tienen una retención de una (3) meses

Para el respaldo de las bases de datos SparkRef y SparkUsg, primero se hace un respaldo a disco y posterior a Cinta, estas son las rutas donde están quedando dichos backups:

Servidor: net-pbdfmra01 “10.100.67.119”

/Backup\_DB/completo

/Backup\_DB/archive

/Backup\_DB/control

/Backup\_DB/log

La OC para el respaldo a cinta corresponde a la nro. **853857**

A nivel de Files systems de NAS se solicitó respaldar:

|  |  |
| --- | --- |
| **Ruta NAS File** | **System …. Servers** |
| 10.158.100.1:/Control\_fraudes/rocfm\_software\_pdn | /rocfm\_software |
| 10.158.100.1:/Control\_fraudes/rocra\_software\_pdn | /rocra\_software |
| 10.158.100.1:/Control\_fraudes/rocfm\_spark\_data\_pdn | /spark\_data |
| 10.158.100.1:/Control\_fraudes/rocfm\_data\_pdn | /rocfm\_data |

A nivel de carpetas de cada servidor Linux se solicitó respaldar:

/

/usr

/var

/so

Tiquete **30710** – OC **864185**

Los formatos diligenciados se encuentran en la carpeta /Backups de esta entrega.

# ANALISTAS DE LA APLICACIÓN

A continuación se detallan los analistas que apoyan y atienden requerimientos de la aplicación en Service Desk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ROL** | **ÁREA FUNCIONAL** | **NOMBRE** | **LOGIN** | **TEL** |
| Analista Tecnológico y Administrador Cambios  “Operación IDC” | Sub Operación IDC y Ofimática | Durley Paulina Gomez B | dgomeb | 5154378 |
| Analista de seguridad | Sub Gestión Seguridad | Juliana Arango Calderon | jarangc | 5151636 |
| Analistas Funcionales | Sub Aseg de Ingresos  Sub Control de Fraudes | Paola Teresa Cardenas  Carolina Taborda | pcardenas  ctaborda | 5158448  5158020 |
| Analista Desarrollador | Sub Apl de Negocio  Coordinador(a) Equipo BI | Mónica Bibiana Henao Gil  Ana Cecilia Soto | mbhenao  asoto | 3251989  3251899 |
| Usuarios que Gestionan la Aplicación | Sub Aseg de Ingresos  Sub Control de Fraudes | Paola Teresa Cardenas  Carolina Taborda | pcardenas  ctaborda | 5158448  5158020 |
| Súper usuarios para generar Requerimientos | Sub Apl de Negocio  Sub Aseg de Ingresos  Sub Control de Fraudes | Gloria Amparo Castro Diaz  Catalina Ma Herrera Gómez  Fredy A Corrales Sanchez | gcastro  cherrera2  facorrales | 5157948  5158650  5158031 |

Analistas de las fuentes.



# MAPA DE OPERACIONES

Mapa de operaciones



Instructivo para seguir el mapa.



# ESCALAMIENTOS

Para el soporte del sistema ROC, se identificaron los siguientes actores que intervienen en el proceso:

1. **Analista de Gestión** “Primer Nivel”: Responsable de la detección temprana de alarmas que se generen en el NOC; Debe de saber atender:
   * Alarmas relacionadas con la estabilidad del servidor, memoria, Files Systems, Sistema Operativo, Servicios de la aplicación ROC y demás alertas configuradas con la instalación de la línea base.
   * Tareas que se le reporten como fallidas mediante EAM “Early Alert Monitor” y que le llega notificación mediante correo electrónico
   * Tareas del mapa de operaciones incluidas en la plantilla de Excel que estén fallidas y que se deben monitorear con la frecuencia acordada.
2. Analista de **Operación IDC** “Segundo Nivel”: Responsable del soporte técnico de operaciones, y es la persona que conoce en mayor detalle el funcionamiento de la(s) aplicaciones, motor de bases de datos, servicios, acceso “administra los módulos de seguridad” entre otros; esta persona es quién apoya al analista de Gestión ante un eventual fallo que no sea capaz de resolver.

En la numeral 16 de este documento está descrita como “Analista Tecnológico y Administrador Cambios”

1. Analista de **Soporte BI** “Tercer Nivel”: Analista que pertenece a la Subdirección aplicaciones de negocio y conoce el funcionamiento de las 2 aplicaciones, ROC RA y FM.

Cualquier fallo relacionado con procesamiento de archivos planos, llenado de espacio por volumen de archivos procesados, funcionamiento de la aplicación que no sea capaz de resolver el analista de Operación IDC o requiera de alguna aprobación, se apoya en el analista de soporte BI.

1. Analista **Funcional**: Son los coordinadores, responsables de la aplicación, existe uno para cada módulo (FM y RA)

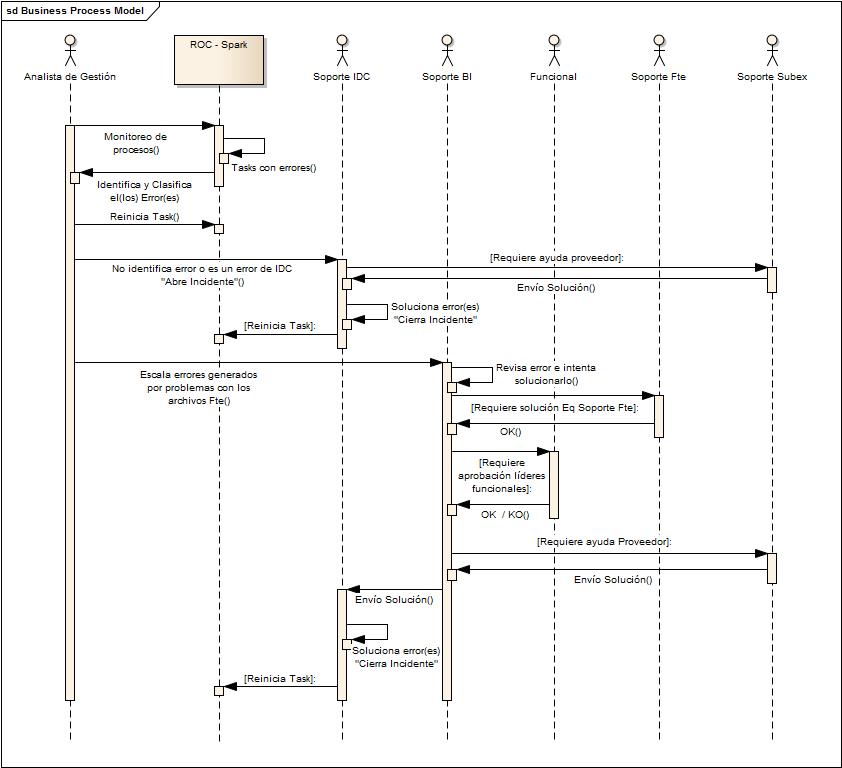
En la numeral 16 de este documento está descrita como “Analistas Funcionales”

1. **Soporte Fuente**: Analistas que soportan los procesos de extracciones de los sistemas fuentes, estas personas son las que apoyan al analista de Soporte BI en caso de alguno fallo relacionado con la información en las extracciones, existe un analista por cada sistema de información.
2. **Soporte Subex**: Es el equipo de soporte por parte del proveedor quienes se encargan de resolver cualquier fallo con el sistema que no esté UNE en capacidad de solucionarlo. Se debe adjuntar a esta entrega el proceso a seguir para abrir un caso con Subex junto con los ANS negociados en el contrato “esto lo entregará el proveedor una vez se haya cerrado los permisos en producción y con el sistema en manos de operación IDC UNE”.

Manual subex support.

A continuación se adjunta el diagrama de interacción para atención de incidentes:



# FLUJOS EN SERVICE DESK

Tipificaciones creadas para atención de Incidentes:

|  |  |
| --- | --- |
| **Tipificación Incidente** | **Descripción** |
| Apl.ROC.Autenticación Falla | Solicitudes relacionadas con fallas en la autenticación de la aplicación ROC. |
| Apl.ROC.Aplicación Falla | Solicitudes relacionadas con fallas en la aplicación ROC. |
| Apl.ROC.Información Inconsistente | Atiende incidentes relacionados con las extracciones de Información de los sistemas fuentes |
| Apl.ROC-**RA**.Configuración | Solicitudes relacionadas con configuraciones y/o parametrizaciones en la aplicación ROC-**RA**. Lider Funcional da el Vobo y transfiere el incidente a Soporte. |
| Apl.ROC-**FM**.Configuración | Solicitudes relacionadas con configuraciones y/o parametrizaciones en la aplicación ROC-**FM**. Lider Funcional da el Vobo y transfiere el incidente a Soporte. |
| Apl.ROC.Administrar Seguridad | Solicitudes relaciones con permisos en la aplicación ROC. Crea orden de cambio y la tipifica MA.Apl.ROC-**RA**.Activar/Modificar/Perfil MA.Apl.ROC-**FM**.Activar/Modificar/Perfil |
| Apl.ROC.Administrar Seguridad Bases de Datos | Solicitudes relaciones con permisos sobre las bases de datos de la aplicación ROC. Crea orden de cambio y la tipifica MA.Apl.ROC-RAFM.Crear/Modificar/Eliminar **Usuario Base de Datos** |

Tipificaciones creadas para atención de OC’s:

|  |  |
| --- | --- |
| **Tipificación Incidente** | **Descripción** |
| MA.Apl.ROC-**RA**.Crear/Modificar/Eliminar Perfil | Creación/Modificación/Eliminación de Cuentas sobre **Revenue Assurance** |
| MA.Apl.ROC-**FM**.Crear/Modificar/Eliminar Perfil | Creación/Modificación/Eliminación de Cuentas sobre **Fraud Management** |
| Catalogo.Apl.ROC-RA.Instalar **DICE** | Instalación Software **DICE** |
| Catalogo.Apl.ROC-RA.Desinstalar **DICE** | Desinstalación Software **DICE** |
| Catalogo.Apl.ROC-FM.Instalar **I2** | Instalación Software **I2** |
| Catalogo.Apl.ROC-FM.Desinstalar **I2** | Desinstalación Software **I2** |
| Catalogo.Apl.ROC-RAFM.Instalar **Diamante** | Instalación Software **Diamante** |
| Catalogo.Apl.ROC-RAFM.Desinstalar **Diamante** | Desinstalación Software **Diamante** |
| MA.Apl.ROC-RAFM.Crear/Modificar/Eliminar **Usuario Base de Datos** | Creación/Modificación/Eliminación de Cuentas sobre bases de datos SparkRef & SparkUsg |

Se adjunta formato de:

1. Solicitud flujos en Service Desk
2. Solicitud de usuarios sistema ROC
3. Solicitud de usuarios de Base de Datos

