VOMS

Instalación y configuración

Prof. Jesus De Oliveira

Prof. Yudith Cardinale

Agenda

- Introducción al VOMS
- Funcionalidades
- Componentes
- Proceso de registro
- Instalación
- Configuración
- Pruebas

Introducción al VOMS

- **VOMS: Virtual Organization Management Service**
  - Gestiona la **membresía** de usuarios a organizaciones virtuales y roles asociados
  - Provee un mecanismo altamente flexible para **autorizar** el acceso a usuarios *previamente autenticados* a los servicios del grid
  - Actúa como un **repositorio centralizado** de credenciales de usuarios

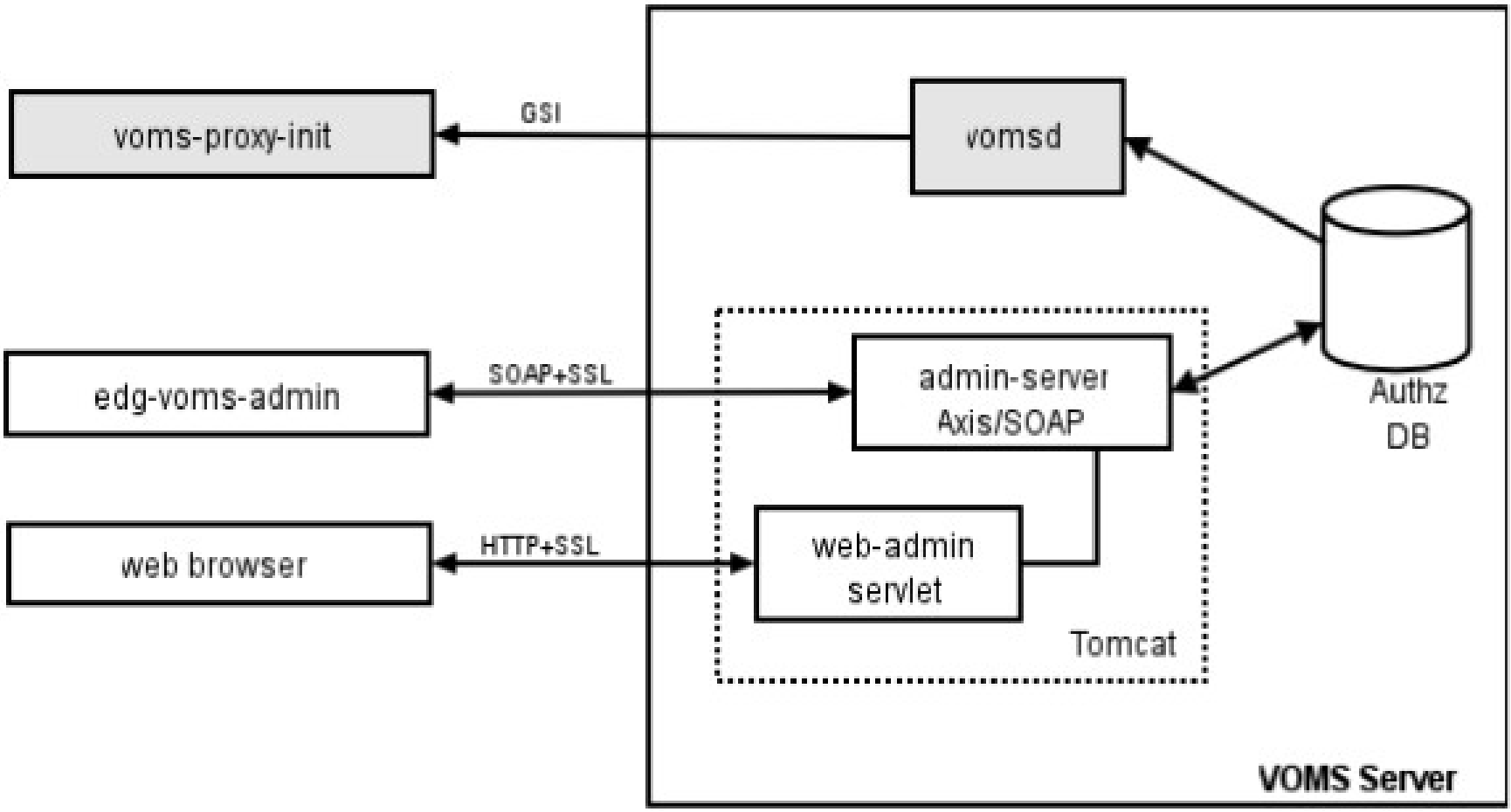
Funcionalidades

- **Usuarios:**
  - se unen a una VO **solicitando membresía** a través de una interfaz web
- **Administradores de la VO:**
  - **Aprueban o rechazan** solicitudes de membresía y asocian roles a usuarios aprobados
- **Recursos del grid:**
  - Consultan periódicamente al VOMS para **mantener tablas de autorización** de usuarios y roles

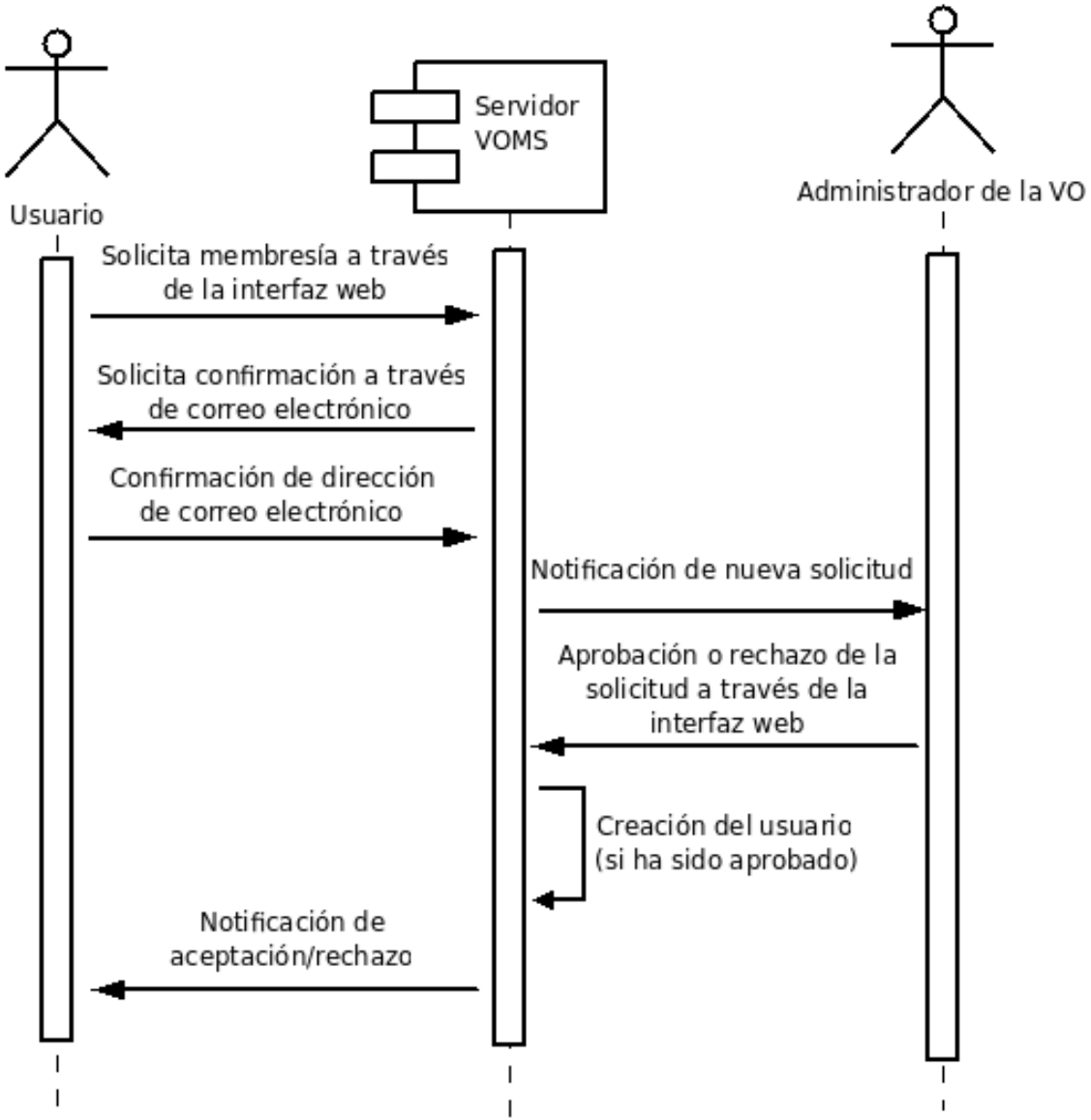
Componentes

- **Del lado del cliente:**
  - Utilidades de línea de comandos para autenticarse en el grid
    - voms-proxy-init –voms <nombre_VO>
    - voms-proxy-info
    - Voms-proxy-destroy
- **Del lado del servidor**
  - Repositorio de credenciales de usuarios (AuthzDB)
  - Interfaz administrativa/de usuarios basada en web y línea de comandos
  - Interfaz basada en web-services (SOAP) para interacción con componentes del grid

Componentes



Proceso de registro



Pre-Instalación

- **Establecer correctamente el nombre completamente calificado de la máquina (FQDN)**
  - # vim /etc/hostname
  - # vim /etc/sysconfig/network
  - # hostname <nombre de la maquina>
  - # vim /etc/hosts
    - Agregar linea "<direccion IP> <nombre>"
    - Ejemplo: "192.168.0.2 mivoms.grid.pe"
- **Desactivar actualizaciones automaticas:**
  - # chkconfig yum off
- **Instalar paquete yum-protectbase**
  - # yum install yum-protectbase
- **Desactivar Firewall (/etc/init.d/iptables stop)**

Pre-Instalación

- **Sincronizar con servidor de tiempo NTP:**
  - # vim /etc/ntp.conf
    - Agregar las siguientes lineas al final:
      - *restrict 159.90.200.7 mask 255.255.255.255 nomodify notrap noquery*
      - *server ntp.usb.ve*
    - Comentar definicion de servidores externos
      - *# --- OUR TIMESERVERS -----*
      - *#server 0.pool.ntp.org*
      - *#server 1.pool.ntp.org*
      - *#server 2.pool.ntp.org*
    - Comentar definicion de servicio de tiempo local
      - *#server 127.127.1.0 # local clock*
      - *#fudge 127.127.1.0 stratum 10*

Pre-Instalación

- **Editar archivo step-tickets:**
  - # vim /etc/ntp/step-tickers
  - Agregar en una linea:
    - ntp.usb.ve
- **Reiniciar el servicio NTP:**
  - # /etc/init.d/ntpd stop
  - # ntpdate ntp.usb.ve
  - # /etc/init.d/ntpd restart
- **Verificar sincronizacion (después de aprox. 5 minutos):**
  - # ntpq -pn
  - # ntpstat

Pre-Instalación

- **Instalar repositorios de autoridades certificadoras y repositorios jpackage y dag:**
  - # wget "http://grid-deployment.web.cern.ch/grid-deployment/glite/repos/lcg-CA.repo" -O /etc/yum.repos.d/lcg-CA.repo
  - # wget "http://grid-deployment.web.cern.ch/grid-deployment/glite/repos/jpackage.repo" -O /etc/yum.repos.d/jpackage.repo
  - # wget "http://grid-deployment.web.cern.ch/grid-deployment/glite/repos/dag.repo" -O /etc/yum.repos.d/dag.repo
  - # apt-get install lcg-CA

- **Instalar certificados de CA GryDs:**
  - # wget "http://doc.gryds.net/grid-deployment/9aa4a84d.0" -O /etc/grid-security/certificates/9aa4a84d.0
  - # wget "http://doc.gryds.net/grid-deployment/9aa4a84d.signing_policy" -O /etc/grid-security/certificates/9aa4a84d.signing_policy

Pre-Instalación

- **Instalar certificado y clave privada del nodo:**
  - # wget "http://doc.gryds.net/grid-deployment/ctic2009/voms.hostcert.pem" -O /etc/grid-security/hostcert.pem
  - # wget "http://doc.gryds.net/grid-deployment/ctic2009/voms.hostkey.pem" -O /etc/grid-security/hostkey.pem

- **Establecer permisología de certifcado y clave privada:**
  - # chmod 644 /etc/grid-security/hostcert.pem
  - # chmod 400 /etc/grid-security/hostkey.pem

- **Verificar certificado:**
  - # openssl verify -CApath /etc/grid-security/certificates /etc/grid-security/hostcert.pem

Pre-Instalación

- **Instalación de JAVA a través del gestor de paquetes:**
  - # cd
  - # wget "http://doc.gryds.net/grid-deployment/ctic2009/instalar_java.sh"
  - # chmod u+x instalar_java.sh
  - # ./instalar_java.sh
    - RESPONDER "YES" A PREGUNTA DE INSTALACIÓN
  - # rpmbuild -ba ~/redhat/SPECS/java-1.5.0-sun.spec
  - # yum localinstall ~/redhat/RPMS/i586/java-1.5.0-sun-1.5.0.15-1jpp.i586.rpm
    - RESPONDER "YES" A PREGUNTA DE INSTALACIÓN
  - # yum localinstall ~/redhat/RPMS/i586/java-1.5.0-sun-devel-1.5.0.15-1jpp.i586.rpm
    - RESPONDER "YES" A PREGUNTA DE INSTALACIÓN

Instalación

- **Instalar servidor de BD MySQL y servidor de correos Postfix**
  - # yum install mysql-server postfix
  - # /etc/init.d/mysqld start
  - #/etc/init.d/postfix star
- **Establecer password de usuario root en MySQL:**
  - # mysqladmin -u root password 'gridctic'
- **Instalar paquete log4j:**
  - # wget http://grid018.ct.infn.it/rep/jpackage17-generic-i386/RPMS.free/log4j-1.2.14-3jpp.noarch.rpm
  - # yum localinstall log4j-1.2.14-3jpp.noarch.rpm

Instalación

- **Instalar repositorios del componente VOMS:**
  - wget "http://grid-deployment.web.cern.ch/grid-deployment/glite/repos/glite-VOMS_mysql.repo" -O /etc/yum.repos.d/glite-VOMS_mysql.repo
- **Instalar paquete glite-VOMS_mysql**
  - # yum install glite-VOMS_mysql
- **Instalar paquete JDK** (ver el ftp de alguno de los repos)
  - # mv /etc/yum.repos.d /etc/yum.repos.d.old
  - # wget http://doc.gryds.net/grid-deployment/ctic2009/repos.tar.gz -O /root/repos.tar.gz
  - # cd /
  - # tar xvfz /root/repos.tar.gz
  - # yum install jdk

Configuración

- **Descargar certificado de usuario:**
  - # wget "http://doc.gryds.net/grid-deployment/ctic2009/ctic.usercert.pem" -O /root/usercert.pem
- **Copiar plantillas de archivos de configuración**
  - cd /opt/glite/etc/config/
  - cp templates/*.xml .

Configuración

- # vim glite-global.cfg.xml

<JAVA_HOME

description="Environment variable pointing to the SUN Java JRE or J2SE package

for example '/usr/java/j2re1.4.2_08/' or '$JAVA_HOME' (if it is defined as

an environment variable)."

value="/usr/java/jdk1.5.0_14"/>

- # vim glite-security-utils.cfg.xml

<cron.mailto

description="E-mail address for sending cron job notifications"

value="jdeoliveira@ldc.usb.ve"/>

Configuración

- **# vim vo-list.cfg.xml**
  - Establecer valores para todas las variables "changeme":
    - vo.name: ctic
    - voms.hostname: voms.grid.ctic.uni.edu.pe
    - voms.port.number: 15000
    - voms.cert.url: /etc/grid-security/hostcert.pem
    - voms.cert.subject: /O=USB/OU=GRyDs/CN=voms.grid.ctic.uni.edu.pe
    - voms.db.name: VOMS_CTIC
    - voms.db.user.name: vo_adm
    - voms.db.user.password: gridctic
    - vo.sgm.vo.role: SoftwareManager
    - pool.account.basename: ctic
    - pool.account.group: ctic
    - pool.account.number: 10

Configuración

- **# vim vo-list.cfg.xml**
  - Establecer valores para todas las variables "changeme" (cont.):
    - pool.lsfgid: <vacio>
    - voms.db.host: localhost
    - voms.admin.smtp.host: localhost
    - voms.admin.notification.email: <direccion de correo>
    - voms.admin.certificate: /root/usercert.pem
- **# vim glite-voms-server.cfg.xml**
  - En el encabezado, reemplazar:
    - <config>
  - Por:
    - <config xmlns:xi="http://www.w3.org/2001/XInclude">
    - <xi:include href="/opt/glite/etc/config/vo-list.cfg.xml" xpointer="" />

- Establecer valores para todas las variables "changeme":
  - voms.db.type: mysql
  - voms.db.host: localhost
  - voms.admin.smtp.host: locahost
  - voms.mysql.admin.password: gridctic

- **Verificar configuración:**
  - # cd /opt/glite/etc/config/scripts/
  - # ./glite-voms-server-config.py -c

- **Aplicar configuración:**
  - # cd /opt/glite/etc/config/scripts/
  - # ./glite-voms-server-config.py --configure
  - # ./glite-voms-server-config.py --configure --vo=CTIC

Configuración

- **Iniciar el servicio:**
  - # cd /opt/glite/etc/config/scripts/
  - # ./glite-voms-server-config.py --start

- **Desactivar comprobación de listas de revocación de certificados:**
  - # vim /etc/tomcat5/server.xml
  - Cambiar propiedad
    - crlRequired="true"
  - por
    - crlRequired="false"
  - /etc/init.d/tomcat5 restart

Configuración

- **Descargar e instalar certificado de usuario, en formato PKCS12, en el browser (máquina real):**
  - Ir al URL:
    - http://doc.gryds.net/grid-deployment/ctic2009/ctic.user.p12
    - (GUARDAR ARCHIVO)
  - En firefox:
    - Menú Herramientas -> Opciones -> ficha Avanzado -> ficha Cifrado
    - Botón "Ver certificados" -> ficha "Sus certificados" -> botón "Importar"
    - Buscar archivo ctic.user.p12
    - CONTRASEÑA: gridctic

- **Usando el browser, entrar en https://<IP DEL VOMS>/voms/ctic**

Preguntas