

Sistemas de Manejo de Incidencias

Práctica con RT (Request Tracker)

Carlos Vicente

Servicios de Redes

Universidad de Oregón

Hervey Allen

Network Startup

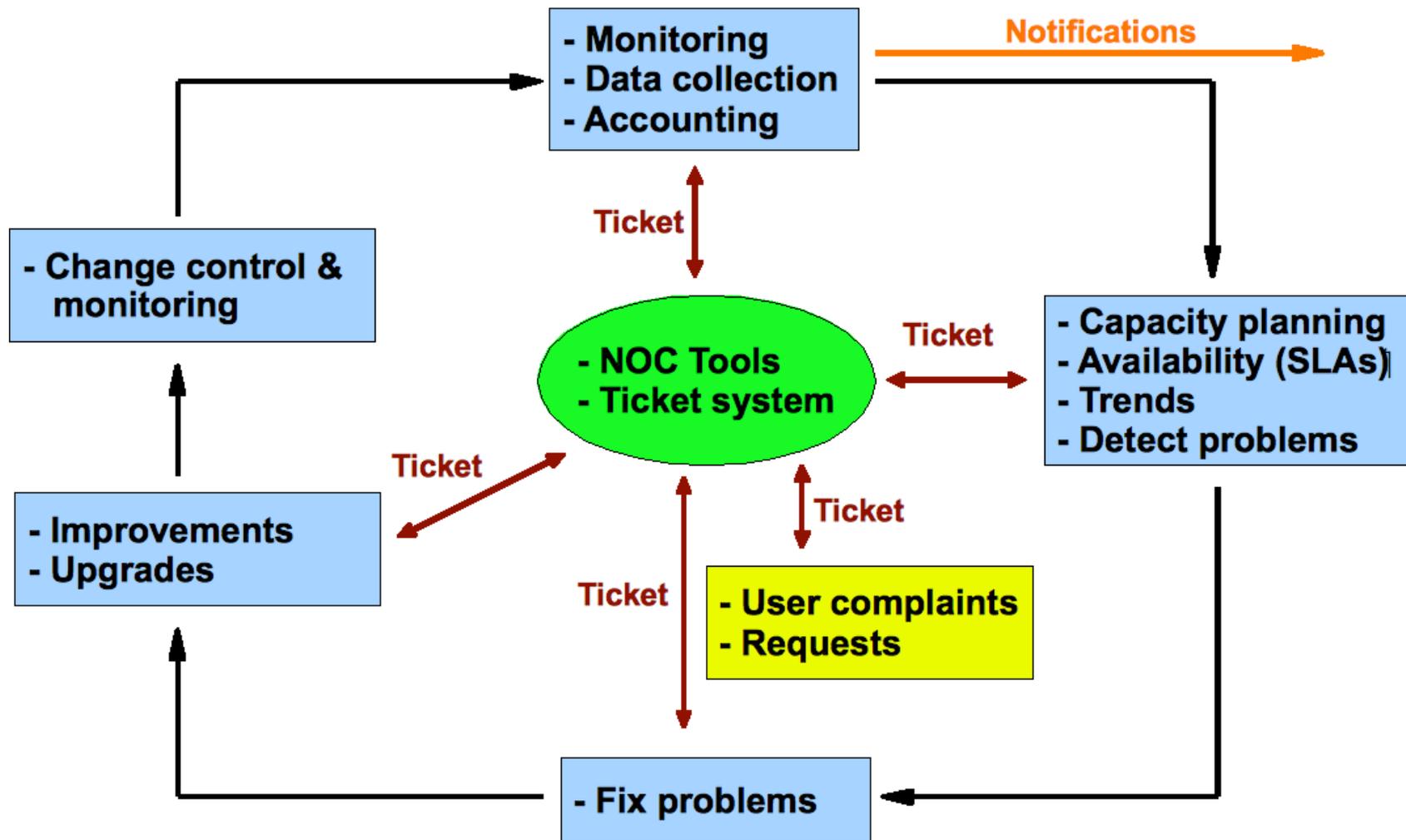
Resource Center



Contenido

- Qué es un sistema de manejo de incidencias
 - Necesidad, ventajas
 - Funcionalidades comunes
- Práctica con RT (Request Tracker)
 - Configuración global
 - Crear usuarios
 - Crear colas
 - Asignar acciones para colas
 - Crear filtros para mensajes

Ticketing con Gestión de Redes



Sistemas de Manejo de Incidencias

- En inglés (ticketing systems)
 - Por qué la palabra “ticket”?
 - Problemas a resolver:
 - Quién quiere qué
 - Quién va a trabajar en eso (o ya trabajó)
 - Cuándo se pidió y cuándo se hizo
 - Cuánto tiempo tomó (facturación en horas)
 - Qué queda por hacer
 - Todo esto resumido y presentado de manera intuitiva y fácil
- 

Aplicaciones

- Soporte a usuarios
- Gestión de proyectos
- Gestión de problemas de seguridad
- Desarrollo de software (gestión de 'bugs')

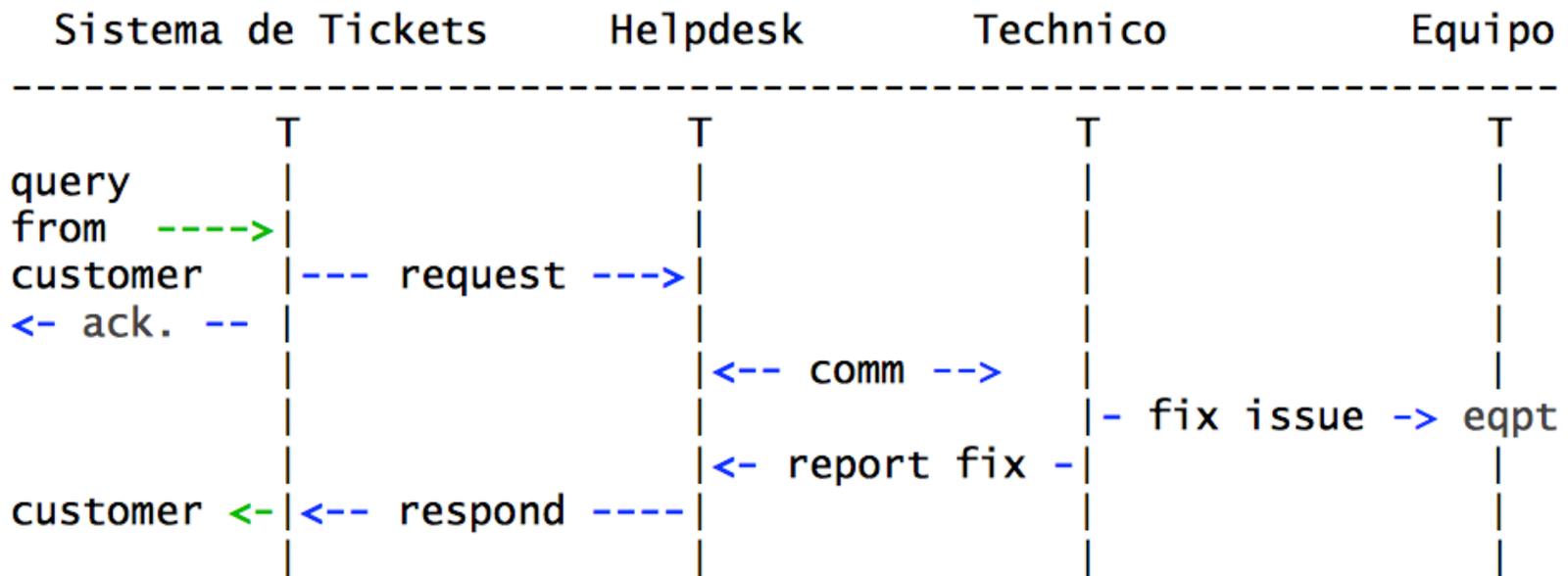


Funcionalidades esenciales

- Múltiples interfaces
 - Web, CLI, e-mail, etc.
 - Multi-usuario
 - A diferentes niveles: administrador, usuarios
 - Autenticación y Autorización
 - Historia de acciones
 - Manejo de dependencias
 - Notificaciones
- 

La “Vida” de un Ticket

Pedido de ayuda con tickets



Componentes

- Registro de una incidencia (crear un ticket)
 - Asignación de un dueño
 - Asignación de partes interesadas
 - Mantener un historial de cambios
 - Informar a las partes interesadas de cada cambio
 - Iniciar una actividad basado en el estatus o prioridad
- 

Necesidad en un Organizacion Grande

- Mucho tráfico de e-mails requiriendo ayuda, servicios, etc
 - Se archivaba en texto, sin clasificación
 - Difícil de encontrar el estatus y toda la historia de un problema
 - A veces los problemas quedaban olvidados y sin resolver
- 



RT: Request Tracker

<http://bestpractical.com/rt/>



RT: Ventajas

- Código abierto y gratis
- MUY utilizado y probado
- Desarrollo muy activo
- Bastante flexible
- Interfaz web y correo electrónico

RT: Desventajas

- Bastante tedioso de instalar
 - Docenas de módulos Perl
 - Algunas distribuciones incluyen paquetes que facilitan el proceso significativamente
 - Gentoo, Debian, FreeBSD, etc.



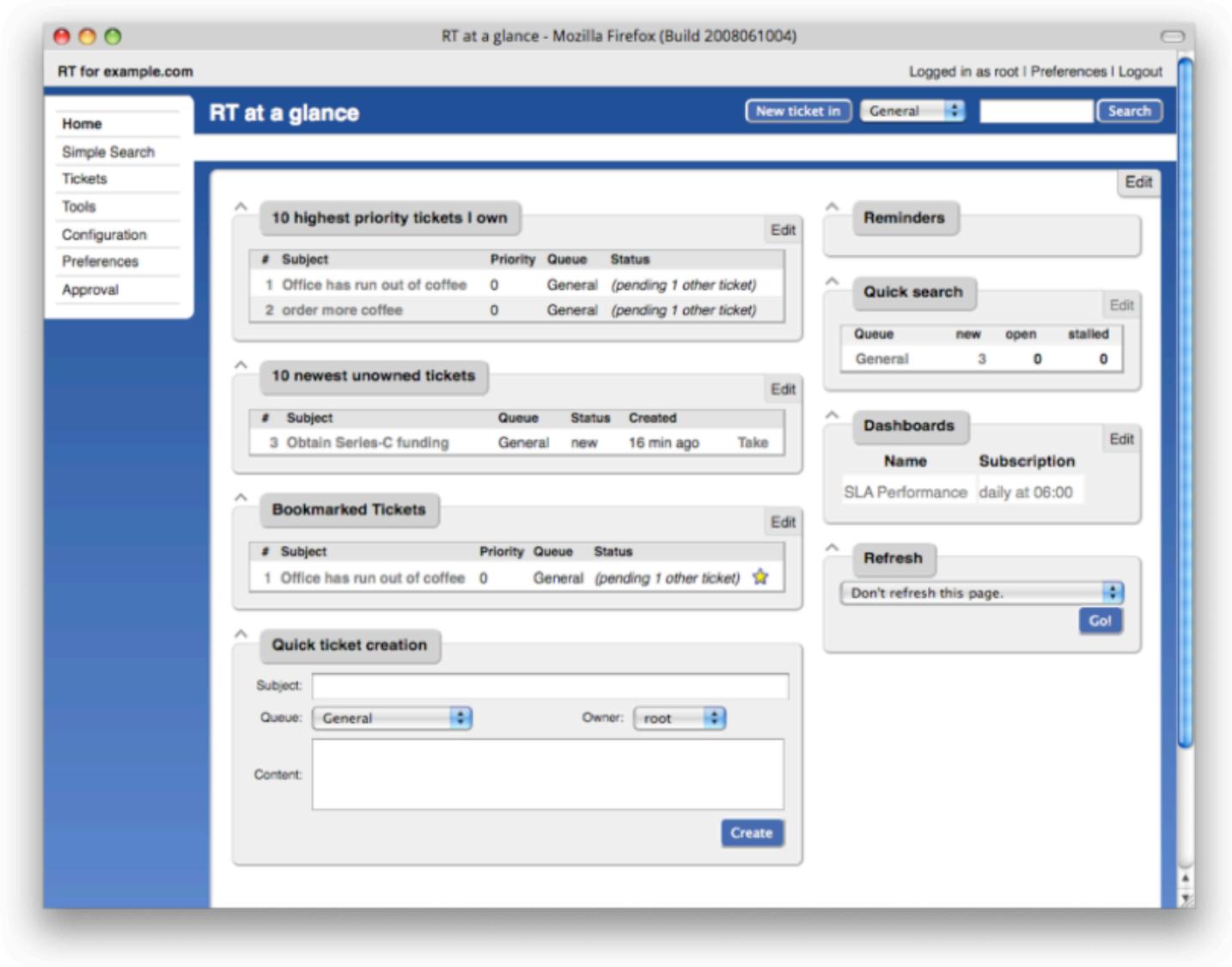
Clasificación de los problemas: Colas

- RT permite crear colas (queues) donde los problemas quedan clasificados según su tipo:
 - **Servicios** (DNS, direcciones IP, Radius, LDAP)
 - **Conectividad** (problemas de infraestructura de comunicación)
 - **Seguridad** (intrusiones, escaneos, abuso, etc)
 - **Sistemas** (cuentas de e-mail, passwords, etc)
 - Ayuda general

Clasificación semi-automática

- Se pueden escribir simples reglas de clasificación utilizando *procmail*
 - Buscar palabras clave en el campo “Asunto” de los e-mails
 - No es perfecto, pero ayuda
 - Es bueno tener un moderador que supervise y asigne tareas

Como se vea RT



Configuración del sitio

- Copiar etc/RT_Config.pm en etc/Site_Config.pm y editar las variables necesarias:
 - \$rtname: Nombre corto para esta instalación
 - \$Organization: Nombre largo para esta instalación
 - \$CorrespondAddress: Dirección por defecto para correspondencias
 - rt@localhost.localdomain
 - \$CommentAddress: Dirección por defecto para comentarios
 - rt-comment@localhost.localdomain
 - \$Timezone: Zona horaria (Ej. 'US/Eastern')
 - \$WebBaseURL: “https://localhost.localdomain”
 - \$WebPath: “/rt3”

Configuración del servidor Web

- Dos opciones
 - Virtualhost
 - `https://soporte.localdomain`
 - Sub-directorio
 - `https://localhost.localdomain/rt3`
- Usuario 'root'
 - Cambiar el password que viene por defecto ('password')
 - Asignar el e-mail completo
 - `(root@localhost.localdomain)`
 - Asignar todos los privilegios
 - Global -> User Rights

Configuración del gateway de E-mail

- Permitir a sendmail que ejecute rt-mailgate

```
ln -s /usr/local/rt3/bin/rt-mailgate rt-mailgate
```

- Añadir los *aliases* necesarios

```
# vi /etc/aliases  
rt: "|rt-mailgate --queue general --action correspond --url http://  
localhost.localdomain/"  
rt-comment: "|rt-mailgate --queue general --action comment --url  
http://localhost.localdomain/"  
# newaliases
```

- Probar lo anterior

```
# echo "probando rt" | mail -s "prueba" rt@localhost
```

Configuración de Procmail

En `/usr/local/rt3/.procmail.rc`:

```
SHELL=/bin/sh
LOGFILE=/var/log/procmail.log
VERBOSE = yes

RT="/usr/local/rt3/bin/rt-mailgate --action correspond --url
http://localhost.localdomain/rt3"

:0
* ^Subject.*(dmca|secur|virus|worm|hack|spam|abuse|firewall|hijack|
ipchains|iptables).*
|$RT --queue seguridad

:0
|$RT --queue general
```

En `/etc/aliases`:

```
soporte: "|procmail /usr/local/rt3/.procmail.rc"
```

Crear Usuarios

- Crear usuarios para cada uno de los miembros de su NOC
- Asignar privilegios a cada usuario



Crear grupos

- Crear grupos que contengan varios usuarios.
 - Administrar privilegios por grupo es más eficiente que hacerlo por cada usuario



Crear Colas

- Crear un grupo de colas para cada categoría de problemas
 - Por ejemplo:
 - seguridad
 - cuentas
 - conectividad
 - Asignar usuarios a cada cola
 - Diferenciar entre AdminCC y CC
 - No olvidar crear *aliases* de e-mail para cada cola

Acciones (scrips)

- Para cada cola, crear acciones automáticas
 - Hay un grupo de *scrips* que aplican a todas las colas
 - Es posible quitar algunos de esta lista y aplicarlos en las colas deseadas solamente



Extensiones

- Es posible extender las funcionalidades de RT
 - Enviar e-mails diarios notificando sobre los tickets que no han sido 'tomados'
 - Enviar e-mails diarios recordando al usuario de sus tickets pendientes
 - Incrementar la prioridad de los tickets periódicamente
 - Ejecutar comandos vía e-mail
 - Ver <http://wiki.bestpractical.com/index.cgi?Extensions>

Referencias

- Sitio web de *Best Practical*

<http://bestpractical.com/rt>

- *RT Essentials*. Dave Rolsky et al. O'Reilly