



WALC 2010

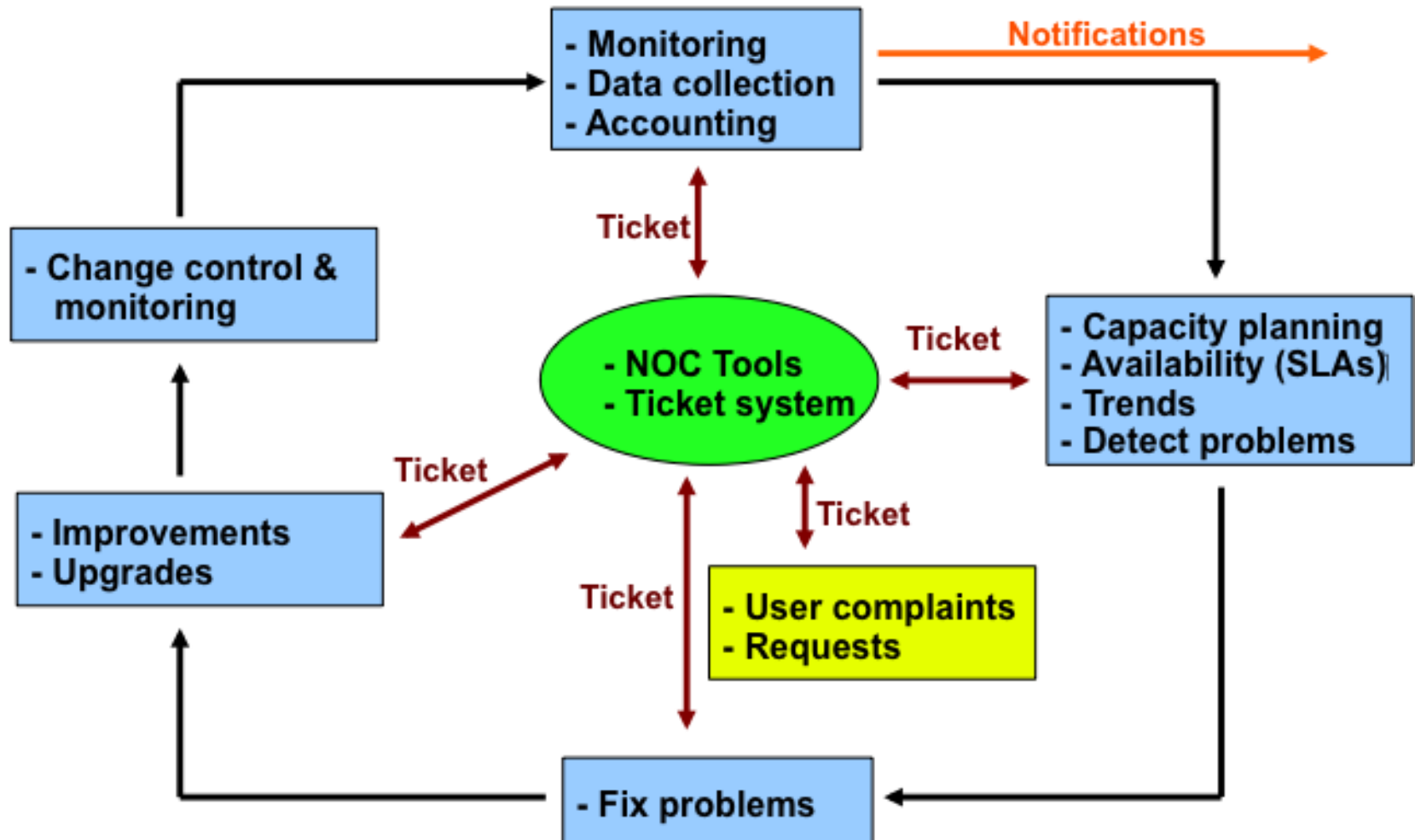
Sistemas de Incidentes con RT



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Porque un Sistema de Incidentes?

Recuerda esto?



Sistemas de Incidentes

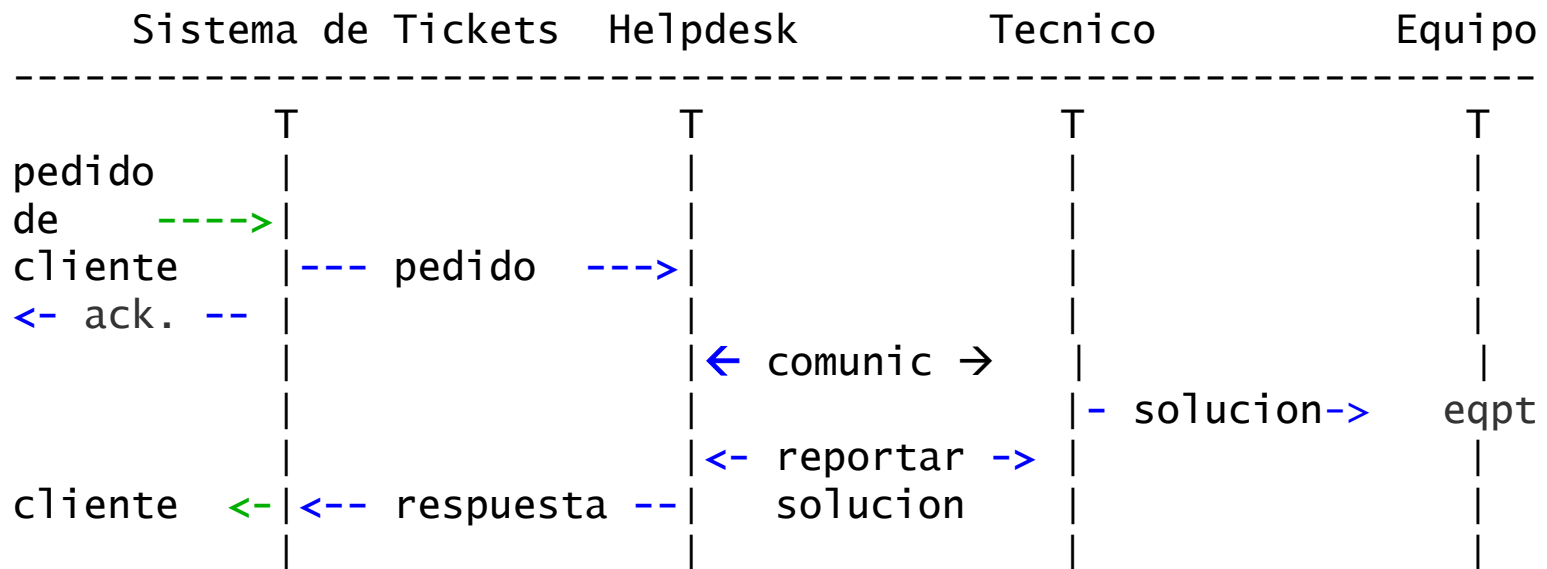
- Porque son importante?
 - Seguir los eventos, fallas y cuestiones
- El/un punto de enfoque para las comunicaciones de Help Desk
- Puede usarlo para seguir todo las comunicaciones
 - Interno y externo
- Eventos con origen de afuera:
 - Quejas de los clientes
- Eventos con origen desde adentro
 - Fallas de sistemas (directo o indirecto)
 - Mantencion planificado, actualizaciones de software y/o hardware, etc.

Sistemas de Incidentes cont.

- Usa un sistema de incidentes para seguir cada caso, incluyendo comunicacion interna entre los tecnicos.
- Cada caso esta asignado un numero de caso
- Cada caso por un ciclo similar
 - *Nuevo*
 - *Abierto*
 - ...
 - *Resuelto*
 - *Cerrado*

Sistema de Incidentes cont.

Un pedido de ayuda con “tickets”



Request Tracker / Trac

RT

- Usado mundialmente
- Puede ser configurado por su organizacion
- Un poco dificil de instalar y configurar
- Funciona bien por instalaciones grandes



trac

- Un sistema hibrido que incluye un wiki y características de gestion de proyectos
- El sistema de tickets no es tan robusto como RT, pero funciona bien por un sistema de tickets a través la web
- Uso comun para seguir ("trac"k) proyectos
- Por esto curso:

<http://noc/trac/>

<http://localhost/trac>





RT: Request Tracker

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

Como se vea?

RT at a glance - Mozilla Firefox (Build 2008061004)

RT for example.com

Logged in as root | Preferences | Logout

RT at a glance [New ticket in](#) [General](#) [Search](#)

Home
Simple Search
Tickets
Tools
Configuration
Preferences
Approval

10 highest priority tickets I own [Edit](#)

#	Subject	Priority	Queue	Status
1	Office has run out of coffee	0	General	(pending 1 other ticket)
2	order more coffee	0	General	(pending 1 other ticket)

10 newest unowned tickets [Edit](#)

#	Subject	Queue	Status	Created	Take
3	Obtain Series-C funding	General	new	16 min ago	Take

Bookmarked Tickets [Edit](#)

#	Subject	Priority	Queue	Status
1	Office has run out of coffee	0	General	(pending 1 other ticket) ★

Quick ticket creation

Subject:

Queue: [General](#) Owner: [root](#)

Content:

[Create](#)

Reminders [Edit](#)

Quick search [Edit](#)

Queue	new	open	stalled
General	3	0	0

Dashboards [Edit](#)

Name	Subscription
SLA Performance	daily at 06:00

Refresh

Don't refresh this page. [Go!](#)

Temas

Que es un sistema de manejo de incidentes?

- Necesidades y ventajas
- Funcionalidad comun

Practica con RT (Request Tracker)

- Configuracion global
- Crear usuarios
- Crear colas
- Asignar acciones a las colas
- Crear filtros de mensajes

Sistemas de Manejo de Incidentes

- Porque usamos el termino “ticket”?
- Para resolver un problema...
 - Quien quiere que?
 - Quien va a trabajar en esto?
 - Cuando se lo pedieron, cuando fue hecho?
 - Cuanto tiempo demaro la solucion (contabilidad, horas)?
 - Que mas hay para hacer?
 - Todo viene con resumen y presentado en una manera simple y intuitivo.

Usos

- Apoyo de usuario
- Manejo de problemas de seguridad
- Seguimiento de asuntos / Manejo de Incidentes

Funcionalidad esencial

- Varias interfaces
 - Web, CLI, correo electronico, etc.
- Multiuser
 - Niveles diferentes: administracion, usuario general, huespede (guest)
- Autenticacion y autorizacion
- Historia de eventos
- Maneja bien las dependencias
- Notificaciones

Componentes

- Registro un evento (creacion de tickets)
- Asignar un dueño
- Asignar grupos interesados
- Mantener una historia de cambios
- Informa cada grupo interesado de cada cambio.
- Iniciar actividades basado en estatus o prioridad

Un escenario tipico de soporte

- Mucho correo pidiendo ayuda, pidiendo servicios, etc.
- Grabado como texto sin clasificacion
- Muy dificil encontrar el estatus corriente o historia de problemas.
- De repente se olvida las problemas o nunca estan resueltas.

RT: Ventajas

- Fuente abierto y gratis
- Muy usado y probado
- En desarrollo muy activo
- Flexible
- Interfaz de Web y/o control por correo

RT: Desventajas

- Un poco difícil de instalar la primera vez...
- Muy poderoso, así tendrá que pasar algo de tiempo aprendiendo como funciona.
 - La mayoría de distribuciones tiene paquetes de instalación que se lo hace todo más fácil:
 - Red Hat, Fedora, SuSE, Debian, Ubuntu, FreeBSD, etc.

Clasificación de Problemas: Colas

RT permite crear colas para clasificar problemas por tipo:

- **Servicios:** DNS, direcciones IP, Radius, LDAP
- **Conectividad:** Comunicaciones y problemas de infraestructura
- **Seguridad:** Ataques, escaneos, abuso, etc.
- **Sistemas:** Cuentas de correo, claves, etc
- Ayuda general

Configuración de Servidor de Web

Dos Opciones

- Virtualhost
<http://rt.host.fqdn>

- Subdirectorio
<http://host.fqdn/rt/>

Usuario administrativo ('*root*')

- Cambia la clave por defecto la primera vez que hace un login ('*password*')
- Asignar el correo completo por la cuenta de *root*
root@host.fqdn
- Asignar todo los derechos a los usuarios:
Global -> User Rights

Creacion de Usuario

- Crear un userid (usuario) por cada miembro de su equipo
- Asignar privilegios a cada usuario.

Creacion de Grupos

Crear grupos de usuarios:

- Aministrando privilegios por grupo es mas eficiente que hacerlo por cada usuario.

Crear Colas

Crear colas por categorías de problemas

- Por ejemplo
 - seguridad
 - cuentas
 - conectividad
- Asignar los usuarios a cada cola
 - Diferente entre AdminCC y CC
- No olvida crear los alias de correo por cada cola

rt-mailgate

Un componente critico de RT. El rt-mailgate nos permite

- Definir usuarios virtuales en su servidor de RT que se correspondan a una cola de tickets en RT.
- Permitir software de terceros (Nagios, Cacti, Smokeping, etc.) automaticamente generar tickets en colas especificas atravez correo
- Ofrece un interfaz simple con que los usuarios pueden comunicar con su empleados de soporte tecnico por RT.

Scripts (acciones)

Por cada cola hacer acciones automaticas

- Hay un grupo de “scripts” que aplica a todo las colas.
 - Es posible personalizar por cada cola o en forma global
 - “scripts” son “pedazitos de codigo de Perl”

Extensiones

Puede extender la funcionalidad de RT. Por ejemplo:

- Mandar correo diariamente para recuedar los usuarios de tickets que no estan tomados
- Manda correos cada dia a cada usuario recordandolos de sus tickets pendientes
- Periodicamente aumenta la prioridad de los tickets
- Puede ejecutar comandos atravez correo

<http://wiki.bestpractical.com/index.cgi?Extensions>

Referenciass

- Sitio de Web de *Best Practical*
<http://bestpractical.com/rt>
- *RT Essentials*. Dave Rolsky et al. O'Reilly Media, Inc.