Control remoto multiplataforma basado en software libre: automatización de sesión VNC integrando gestión de incidencias e inventario

Multiplatform remote control based on free software: Automating VNC session integrating incident management and inventory

Unai Gangoiti

Resumen

El uso del control remoto se ha convertido en una herramienta imprescindible como complemento al resto de tecnologías necesarias en la gestión y resolución de todas las posibles incidencias relacionadas con las Tecnologías de Información y Comunicaciones. En este sentido, la mayoría de los sistemas operativos implementan soluciones ad hoc para resolver este tipo de acceso. Existe también software comercial de terceros que implementan este tipo de acceso. En este trabajo, se presenta una solución utilizando tecnologías existentes en software libre para resolver gran parte de los problemas que presentan las soluciones convencionales.

Palabras clave: control remoto, VNC, help desk.

Summary

The use of remote control has become an indispensable tool in addition to other technologies needed in the management and resolution of all possible incidents related to Information Technology and Communications. In this sense, most operating systems implement ad hoc solutions to achieve this type of access. There is also commercial software that implements this type of access. This paper presents a solution using existing open source technologies to solve many of the problems that arise in the use of conventional solutions.

Keywords: remote control, VNC, help desk.

El proyecto está siendo desarrollado en el Centro de Atención a Usuarios de la Universidad del País Vasco

1. Introducción

Este documento presenta un sistema de gestión del acceso mediante control remoto para la resolución de incidencias basado en software libre. El proyecto está siendo desarrollado en el Centro de Atención a Usuarios (CAU) de la Universidad del País Vasco, y su objetivo principal es resolver los problemas que presentan las herramientas de control remoto en su uso diario para la resolución de incidencias. Además, se presenta un prototipo en fase de desarrollo que está siendo utilizado en varios centros piloto. La labor fundamental del sistema es facilitar la conexión remota por parte de los técnicos del CAU a los equipos de los usuarios de los servicios informáticos que previamente hayan solicitado su intervención. Los tres perfiles principales de usuarios son: Personal Docente e Investigador (PDI), Personal de Administración y Servicios (PAS) y alumnado en general.

Su objetivo principal es resolver los problemas de las herramientas de control remoto en su uso diario para la resolución de incidencias

2. Particularidades de los equipos y usuarios

El parque actual de equipos a los que se ofrece servicio es el que se detalla a continuación:

A) PAS:
- equipos corporativos con sistema operativo Windows XP, y sin privilegios de administración.

B) PDI:
   - equipos corporativos con privilegios totales o privilegios limitados de administración (Windows XP y GNU/Linux-Ubuntu)
   - equipos compartidos sin privilegios de administración
   - equipos personales autorizados o equipos provenientes de proyectos de investigación (con sistemas operativos diversos y privilegios totales de administración)

C) Investigadores y alumnos:
   - equipos corporativos con privilegios limitados
   - equipos personales autorizados o equipos de laboratorio

El tipo de conexión a la red y direccionamiento utilizado por estos equipos es dirección IP fija en la red cableada, direccionamiento dinámico para equipos conectados a través de VPN, WiFi (eduroam), equipos en roaming inter-centros, VLAN de invitados,... y direccionamiento privado en equipos de aulas docentes o equipos conectados en subredes privadas accediendo al exterior por NAT.

El tipo de conexión a la red y direccionamiento utilizado por estos equipos es dirección IP fija en la red cableada

3. Herramientas de acceso remoto

El software de acceso remoto disponible en los equipos es el que se detalla a continuación:

- Equipos corporativos con Windows XP: software comercial de control remoto preinstalado
- Resto de equipos con Windows XP:
  - Con privilegios de administración: escritorio remoto, invitación de asistencia remota, Virtual Network Computing (VNC)[1]. En este caso es posible indicar al usuario los pasos necesarios para su activación o instalación.
  - Sin privilegios de administración: los mismos que en el caso anterior pero limitados a los servicios existentes y activados en el equipo.
- Otros sistemas operativos: GNU/Linux, OSX... Para cada variante deberemos tener en cuenta las herramientas de acceso remoto apropiadas para poder proceder.

Estas herramientas presentan diversos problemas que en algunos casos dificultan y en otros impiden su correcta utilización:

A) Privilegios de administración: en el caso de los equipos sin privilegios de administración si los servicios no han sido previamente activados por el administrador no será posible utilizarlos (escritorio remoto o invitación de asistencia remota). Tampoco es posible en este caso abrir puertos específicos en el firewall o instalar software adicional.

B) Claves de acceso. Tanto en escritorio remoto como en acceso mediante VNC, en principio es necesario conocer la clave de acceso del equipo remoto.

C) Redes privadas y direccionamiento dinámico. La localización de los equipos conectados con direccionamiento dinámico requiere un trabajo adicional y no siempre es posible acceder a los equipos en redes privadas conectados por NAT al exterior.

D) Diversidad de sistemas operativos. Añade un nivel de dificultad el tener que diferenciar el método de trabajo en función del sistema operativo remoto.

Tanto en escritorio remoto como en acceso mediante VNC es necesario conocer la clave de acceso del equipo remoto

En este sentido la aplicación VNC nos ofrece ventajas que pueden ayudar a solventar en muchos casos gran parte de los problemas anteriores. VNC es una aplicación de escritorio remoto cliente-servidor, con implementaciones para prácticamente todos los sistemas operativos con interfaz gráfica.

VNC utiliza el protocolo Remote Framebuffer (RFB)[2], que en sus implementaciones más actuales incluye autogestión de la compresión/calidad de imagen en función del ancho de banda, encriptación y conexión inversa. El método de conexión inversa[3] permite que el servidor VNC (equipo del usuario) sea el que inicie la comunicación con el cliente (equipo del resolutor: técnico del CAU). Este tipo de conexión resuelve diversos problemas de red, firewall y direccionamiento.

Retomando los cuatro problemas principales que encontrábamos en las herramientas de acceso remoto, mediante el uso de VNC podemos solventar:

A) Privilegios de administración: no es necesario instalar el software, existen implementaciones "single click"[4] de un único binario autónomo ejecutable sin previa instalación.

B) Claves de acceso. Realizando la conexión mediante conexión inversa no es necesario validarse con ninguna clave, es el servidor VNC (en ejecución en el equipo del usuario) el que inicia el acceso remoto buscando el puerto apropiado en el equipo donde reside el cliente VNC (equipo del resolutor: técnico del CAU).

C) Redes privadas y direccionamiento dinámico. El método de conexión inversa resuelve este tipo de problemas.

D) Diversidad de sistemas operativos. Existen implementaciones para prácticamente todos los sistemas operativos basados en interfaz gráfica. El sistema seleccionará el adecuado para cada caso.

El método de conexión inversa permite que el servidor VNC sea el que inicie la comunicación con el cliente

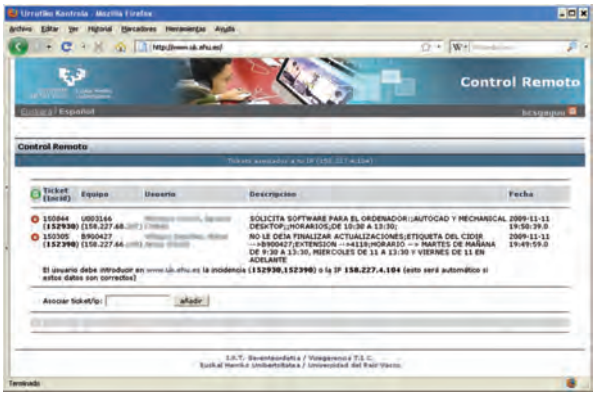
4. Etapas en la resolución de una incidencia

El sistema de gestión de incidencias comprende las siguientes etapas (en el caso de incidencias resolubles mediante control remoto):

1. El usuario informa al CAU de su solicitud/incidencia vía web/email/teléfono.
2. El CAU evalúa la solicitud y en caso de aceptación genera un ticket (vía Remedy[4]) detallando el código de inventario del equipo afectado, usuario... y lo asigna a un resolutor (normalmente al técnico asociado al centro al que pertenece el usuario).
3. El técnico recibe el ticket y a partir de su descripción estudia la viabilidad de resolverlo mediante control remoto.
4. El resolutor se valida en el gestor de sesiones remotas vía web y selecciona una o varias incidencias a resolver de forma remota. En la **figura 1** se muestra el interfaz web.
5. El usuario (guiado telefónicamente por el resolutor) accede a la dirección web del gestor.
6. La web informa al usuario del procedimiento que se va a llevar a cabo en su equipo y solicita su aceptación. La aceptación inicia automáticamente la sesión de control remoto.
7. El resolutor realiza las labores solicitadas con el usuario al teléfono compartiendo su escritorio.
8. En caso favorable, el resolutor finaliza la sesión remota, detalla en el gestor de incidencias su acción y cierra el ticket.

El resolutor se valida en el gestor de sesiones remotas vía web

FIGURA 1. INTERFAZ WEB, SELECCIÓN DE INCIDENCIAS



Se han logrado evitar los problemas relacionados con los cortafuegos de usuario y los de direccionamiento IP privado y dinámico

A continuación se detallan las funciones que internamente realiza el prototipo desarrollado en los pasos anteriores:

FIGURA 2

Paso	Funciones que realiza el gestor
4	- Valida credenciales del resolutor contra el directorio LDAP - Comprueba el estado de la máquina virtual de java y propone su instalación en caso necesario - En el equipo del resolutor, un applet firmado de Java descarga e inicia el visor VNC en modo escucha (vncviewer -listen) - Recibe del gestor de aplicaciones la IP pública del equipo resolutor (IP_resolutor) y la asocia al código de incidencia. Lo registra en tabla_1 (IP_resolutor - incidencia) - Lee de Remedy (interfaz JSON [5]) los detalles de la incidencia indicada y los muestra por pantalla - Lee del inventario (JDBC) los datos asociados al equipo a partir del código de inventario (IP_usuario), y lo registra en la tabla_2 (IP_usuario – incidencia)
5	- En el equipo de usuario, el gestor de aplicaciones muestra al usuario el número de incidencia que se pretende resolver en el equipo en el que se encuentra (lo obtiene a partir de la tabla_2)
6	- En el equipo del usuario, un applet firmado de Java descarga y lanza un servicio vnc parametrizado en modo cliente y con orden de conexión al equipo del resolutor. (winVNC.exe localHost=1 && winVNC.exe –connect IP_Resolutor)
8	- El applet de java envía un comando de cierre al servicio VNC en el equipo del usuario y elimina todos archivos temporales generados

Con el prototipo se ha demostrado la posibilidad de integrar el gestor con herramientas propietarias

5. Conclusiones

La solución propuesta no requiere instalación de ningún tipo de software adicional en los equipos de usuario. Son requisitos la conexión a red y el navegador con soporte Java. Por tanto, evita desplazamientos innecesarios desde el primer momento. Por otra parte, se han logrado evitar los problemas relacionados con los cortafuegos de usuario (Windows) y los de direccionamiento IP privado y dinámico.

Con el prototipo se ha demostrado la posibilidad de integrar el gestor con herramientas propietarias (Remedy en la gestión de incidencias y herramienta de gestión de inventario propia). El sistema es completamente abierto y es fácilmente integrable en cualquier otro escenario. Las tecnologías que se han utilizado son:

A) Applets de java firmados en la interacción navegador a equipo

B) JSON y JDBC en el acceso a bases de datos

C) Un gestor de aplicaciones TOMCAT y base de datos MySQL para las tablas de relaciones así como de caché de la información de los gestores de incidencias e inventario (mejora de rendimiento)

D) Cliente/servidor RealVNC[6] (su versión GPL).

Referencias

[1] Virtual Network Computing (VNC) from Wikipedia: *http://en.wikipedia.org/wiki/VNC* (2009)

[2] Remote Framebuffer protocol (RBF) from Wikipedia: *http://en.wikipedia.org/wiki/RFB_protocol* (2009)

[3] Julius Plenz "Reverse VNC Session" *www.plenz.com/reverse-vnc* (2006)

[4] Single-Click VNC solution from ultraVNC. *www.uvnc.com/addons/singleclick.htm* (2009)

[5] Remedy Action Request System (Remedy, ARS) from Wikipedia. *http://en.wikipedia.org/wiki/Action_Request_System* (2009)

[6] JavasScript Object Notation from Wikipedia. *http://es.wikipedia.org/wiki/JSON* (2009)

[7] RealVNC Free Edition *http://www.realvnc.com/products/free/4.1/* (2009)

El sistema es completamente abierto y fácilmente integrable en cualquier escenario

Unai Gangoiti Gurtubay
(unai.gangoiti@ehu.es)
Bizkaiko IISIG / CIDIR de Bizkaia
IKT Gerenteordetza / Vicegerencia TIC
Euskal Herriko Unibertsitatea / Universidad del País Vasco