(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 730 125**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2016 PCT/FR2016/052372**

(87) Fecha y número de publicación internacional: **30.03.2017 WO17051104**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2016 E 16781511 (7)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 3353986**

(54) Título: **Procedimiento de conexión de seguridad, desde un dispositivo informático cliente, a un recurso informático**

(30) Prioridad:

21.09.2015 FR 1558890

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.11.2019

(73) Titular/es:

WALLIX (100.0%)
250 Bis Rue du Faubourg Saint-Honoré
75008 Paris, FR

(72) Inventor/es:

ADDA, SERGE y
ZHOU, RAPHAËL

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Procedimiento de conexión de seguridad, desde un dispositivo informático cliente, a un recurso informático

Campo de la invención

La presente invención se refiere al campo de los servidores de aplicación, y más particularmente de los procedimientos y sistemas de acceso a recursos aplicativos alojados en uno o varios servidores, por un usuario.

Estado de la técnica

Se conoce en particular en el estado de la técnica la solicitud de patente europea EP2894814 de un procedimiento de supervisión de una sesión sobre un sistema objetivo.

Se instala un agente transitorio específico para la supervisión de la sesión en el sistema objetivo durante la recepción de la solicitud de apertura que procede del cliente del usuario.

La sesión se establece entre el usuario y el sistema objetivo a través de una red de comunicación.

El agente transitorio supervisa la sesión, recoge los datos de los eventos que se producen en el sistema objetivo en el transcurso de la sesión.

El agente transitorio se desinstala cuanto termina la sesión.

Inconvenientes de la técnica anterior

La solución propuesta por la solicitud EP2894814 prevé una etapa de instalación, por ejemplo mediante un comando PsExec, que necesita conexiones de redes adicionales y privilegios particulares en el servidor objetivo.

Por otra parte, necesita proceder a una etapa específica de desinstalación del agente, para evitar que su ejecución fuera de la sesión consuma inútilmente capacidades de cálculo del servidor.

Solución aportada por la invención

El objeto de la presente invención es solucionar estos inconvenientes proponiendo una solución más simple y más segura, evitando en particular una etapa expresa de desinstalación. La solución objeto de la presente invención evita igualmente fallos de seguridad.

La invención se refiere según su acepción más general a un procedimiento de conexión de seguridad, desde un dispositivo informático cliente, a un recurso informático objetivo que comprende un servidor y si es necesario una aplicación ejecutada en dicho servidor, implementando una pasarela intermediaria que comprende una memoria para el registro de las informaciones relativas a dicha conexión así como al menos un agente ejecutable en dicho servidor durante una sesión, comprendiendo el procedimiento las etapas siguientes:

- la emisión de una solicitud de apertura de sesión por una aplicación instalada en la estación cliente, que implica la creación de una sesión primaria entre la estación cliente y la pasarela intermediaria. Dicha solicitud puede contener el identificador del servidor objetivo o de la aplicación objetivo.
- la apertura de una sesión entre dicha pasarela intermediaria y dicho servidor

Estando dicho procedimiento caracterizado por que

- dicha etapa de instalación de al menos un agente se ejecuta comprendiendo sucesivamente:

    ○ dicha etapa de apertura de una sesión secundaria entre dicha pasarela intermediaria y dicho servidor, comprendiendo dicha etapa la colocación de la redirección de un disco emulado por la pasarela intermediaria en el que se registra dicho agente,
    ○ la ejecución de un guion de temporización que espera que dicho disco emulado esté disponible,
    ○ la copia del agente hacia un directorio. Este directorio puede ser ventajosamente un directorio temporal situado en el servidor. La destrucción automática de dicho directorio por dicho servidor al final de la sesión hace inútil una etapa específica de desinstalación del agente.
    ○ la ejecución del agente en dicho servidor
    ○ el establecimiento de un canal virtual entre el servidor y la pasarela para la comunicación entre el agente y la pasarela
    ○ a continuación, la apertura de un canal ascendente entre la estación cliente y el servidor.

El procedimiento comprende igualmente el lanzamiento por el agente de una aplicación previamente seleccionada

por el usuario, pudiendo ser esta llegado el caso el administrador si no se ha seleccionado ninguna aplicación por el usuario.

Según una variante, el procedimiento según la invención incluye una etapa previa de selección de un recurso objetivo, mediante la transmisión por el terminal cliente de un mensaje numérico que incluye un identificador de usuario y verificación por dicha pasarela de si las informaciones relativas a los derechos de utilización asociados a dicha identificación en una base de datos (302) se refieren a dicho recurso objetivo.

Ventajosamente, incluye una etapa previa de selección de un recurso objetivo, consistente en la transmisión por parte de la pasarela de datos digitales que comprenden la lista de los objetivos correspondientes a los datos registrados en una base de datos (302) en relación con el identificador transmitido y la selección por el usuario de uno de los objetivos propuestos.

Ventajosamente, dicha base de datos (302) comprende una lista de las aplicaciones y de los servidores que alojan cada una de dichas aplicaciones, así como las cuentas que permiten conectarse a estos servidores.

Preferentemente, dicha pasarela incluye unos medios para el cálculo de un balance de las cargas en función del número de conexiones ya abiertas hacia cada uno de los servidores y de selección para la nueva petición del servidor menos solicitado.

Según un modo de realización ventajoso, el procedimiento incluye una etapa de ejecución de un código informático para:

- interrogar a la pasarela para obtener las informaciones de autenticación que corresponden a la cuenta de la aplicación,
- inyectar estos datos en la aplicación con el fin de abrir una sesión aplicativa y permitir al usuario usar dicha aplicación.

Según una primera variante, dicho código se instala en el servidor (500) de manera permanente y por que el camino de acceso a este código se define en la base de datos (302).

Según una segunda variante, dicho código se transmite transitoriamente, por un canal dedicado previsto en el protocolo multicanal (400), para ejecutarse transitoriamente en el servidor (500).

Descripción detallada de un ejemplo no limitativo de realización

La presente invención se comprenderá mejor con la lectura de la descripción que sigue, con referencia a unos ejemplos no limitativos de realización, ilustrados por los dibujos adjuntos en los que:

- la figura 1 representa un esquema de la arquitectura funcional de la invención
- la figura 2 representa un esquema de la arquitectura funcional de una variante de realización de la invención
- la figura 3 representa una vista esquemática de las etapas del proceso y unos datos intercambiados entre los diferentes recursos informáticos.

Arquitectura funcional

El usuario es un administrador de la red o del sistema que dispone de derechos limitados de administración, para un conjunto de recursos de los que se encarga.

Dispone de un terminal (100) que comunica con la pasarela intermediaria (300) (o “pasarela de administración”) por la mediación de una conexión (200) según un protocolo por ejemplo SSH (“secure shell”, en español, intérprete de órdenes seguro) o RDP (“remote desktop protocol”, en español, protocolo de escritorio remoto).

La conexión conlleva la creación de una sesión primaria (301) en la pasarela (300).

El usuario se identifica mediante identificadores digitales que le son propios, y que definen sus derechos, así como la imputación de las acciones que efectúa.

La pasarela (300) incluye una base de datos (302) en la que se registran los identificadores de los usuarios autorizados así como los derechos asociados, que definen los objetivos (cuentas y equipos) en los que el usuario tiene el derecho de actuar.

Durante la conexión, son posibles dos modos de selección del recurso:

- según el primer modo, el usuario precisa, durante la conexión, el objetivo al que quiere acceder. En este caso la pasarela verifica si el usuario identificado por su identificador dispone de las autorizaciones necesarias para

acceder a este objetivo, en función de las informaciones registradas en la base de datos (302).

- Según el segundo modo, la pasarela transmite al usuario la lista de los objetivos que corresponden a los datos registrados en la base de datos (302) en relación con el identificador transmitido, para permitir al usuario la selección de uno de los objetivos propuestos.

La etapa siguiente consiste en abrir una conexión, generalmente con el mismo protocolo SSH o RDP o incluso con un segundo protocolo; con la cuenta asociada al objetivo seleccionado. Esta etapa comprende sucesivamente:

- ○ dicha etapa de apertura de una sesión secundaria entre dicha pasarela intermediaria y dicho servidor, comprendiendo dicha etapa la colocación de la redirección de un disco emulado por la pasarela intermediaria en el que se registra dicho agente,
- ○ la ejecución de un guion de temporización que espera a que dicho disco emulado esté disponible
- ○ la copia del agente hacia un directorio temporal situado en el servidor. La destrucción automática de dicho directorio por dicho servidor al final de la sesión hace inútil una etapa específica de desinstalación del agente.
- ○ la ejecución del agente en dicho servidor
- ○ el establecimiento de un canal virtual entre el servidor y la pasarela para la comunicación entre el agente y la pasarela
- ○ a continuación, la apertura de un canal ascendente entre la estación cliente y el servidor.

Cuando el objetivo es una aplicación, la pasarela (300) elige el servidor (500) adecuado para la ejecución de dicha aplicación. Para tal fin, la base de datos (302) comprende una lista de las aplicaciones y de los servidores que alojan cada una de dichas aplicaciones, así como las cuentas que permiten conectarse a estos servidores.

Cuando varios servidores alojan una misma aplicación, la pasarela realiza un balance de las cargas en función del número de conexiones ya abiertas hacia cada uno de los servidores y selecciona para la nueva petición el servidor menos solicitado.

Asimismo, en ausencia de respuesta por un servidor que aloja una aplicación, la pasarela busca sucesivamente los otros servidores que alojan la misma aplicación, para seleccionar un objetivo disponible.

El procedimiento comprende igualmente el lanzamiento por el agente de una aplicación previamente seleccionada por el usuario, pudiendo ser esta llegado el caso el administrador si no se ha seleccionado ninguna aplicación por el usuario. El lanzamiento de una aplicación puede delegarse si es necesario en un código informático especializado para:

- interrogar a la pasarela para obtener las informaciones de autenticación que corresponden a la cuenta de la aplicación, por ejemplo una contraseña o un certificado criptográfico, o un ticket Kerberos
- inyectar estos datos en la aplicación con el fin de abrir una sesión aplicativa y permitir al usuario usar dicha aplicación.

Este código puede:

- instalarse en el servidor (500) de manera permanente. En este caso, el camino de acceso a este código se define en la base de datos (302)
- o transmitirse transitoriamente, por un canal dedicado previsto en el protocolo multicanal (400), para ejecutarse transitoriamente en el servidor (500).

El nombre de este código puede generarse de manera única, con el fin de dificultar la alteración de este código durante la ejecución de la aplicación, por un ataque informático.

Este código instalado transitoriamente puede incluir igualmente un testigo único con el fin de reducir los riesgos de acceso no autorizado a los datos registrados en la base (302), por medio de la sesión abierta, por un atacante que tenga acceso al servidor (500).

Acceso concurrente a aplicaciones en un mismo servidor por varios usuarios.

La figura 2 representa un esquema funcional de una solución que permite a varios usuarios el acceso a aplicaciones alojadas en un mismo servidor. El objetivo es evitar las interferencias entre las sesiones y hacerlas estancas en términos de seguridad.

Para tal fin, cuando un segundo usuario (150) trata de ejecutar una aplicación alojada en el mismo servidor (500) que una aplicación ejecutada para un primer usuario (100), la pasarela (300) inhibirá los datos de la base (302) relativos a la cuenta usada por el primer usuario (100), en el servidor (500). Solo autorizará la ejecución de una aplicación en este mismo servidor (500) si una cuenta permanece disponible para un segundo usuario (150).

Datos intercambiados entre los recursos informáticos

La figura 3 representa una vista esquemática de los datos intercambiados entre los diferentes recursos informáticos.

Durante la conexión por un usuario, el terminal (100) transmite a la pasarela intermediaria (300) los identificadores digitales primarios.

Estos datos de autenticación se verifican por la pasarela (300), en función de las informaciones registradas en su base de datos (302).

En caso de validación, la pasarela (302) transmite la lista de los objetivos autorizados (C1 a C3).

Cada objetivo corresponde a un par:

- aplicación
- cuenta asociada a la aplicación.

La cuenta comprende:

- una información de identificación

- una información de autenticación, tal como una contraseña.

La pasarela transmite al usuario (100), para cada uno de los objetivos autorizados, solamente la designación de la aplicación y la designación del identificador de la cuenta, pero no la información de autenticación, en la forma de cadenas de caracteres que designan los pares aplicación/cuenta.

El usuario (100) selecciona uno de los objetivos propuestos y transmite de ellos el identificador a la pasarela (300).

La pasarela (300) elige un servidor, y una cuenta para abrir una sesión en dicho servidor (500), según el proceso de selección del servidor y de la cuenta que se ha descrito anteriormente.

Abre de este modo una sesión secundaria, en el servidor. Esta sesión presenta un disco emulado por la pasarela. Este disco incluye un agente. Posteriormente la pasarela vuelve a copiar y arranca el agente según el procedimiento anteriormente descrito. Esto inicia el administrador o en el caso en el que el usuario ha seleccionado una aplicación específica, procede a su ejecución ya sea directamente o ya sea por medio de un código informático especializado. Este código solicita a la pasarela el identificador de la cuenta de la aplicación así como los datos de autenticación asociados a esta cuenta.

El código informático transmite entonces estas informaciones a la aplicación para mandar la ejecución de la aplicación.

REIVINDICACIONES

1. Procedimiento de conexión de seguridad, desde un dispositivo informático cliente, a un recurso informático objetivo que comprende un servidor y si es necesario una aplicación ejecutada en dicho servidor, implementando una pasarela intermediaria que comprende una memoria para el registro de las informaciones relativas a dicha conexión así como al menos un agente ejecutable en dicho servidor durante una sesión, comprendiendo el procedimiento las etapas siguientes:

- la emisión de una solicitud de apertura de sesión por una aplicación instalada en la estación cliente, que implica la creación de una sesión primaria entre la estación cliente y la pasarela intermediaria. Dicha solicitud puede contener el identificador del servidor objetivo o de la aplicación objetivo.
- la apertura de una sesión entre dicha pasarela intermediaria y dicho servidor

estando dicho procedimiento **caracterizado por que**

- dicha etapa de emisión de una solicitud se implementa mediante la apertura previa de una sesión primaria [RDP] entre la estación cliente y la pasarela intermediaria por el envío de un mensaje que comprende el identificador del servidor objetivo o de la aplicación objetivo
- dicha etapa de instalación de al menos un agente se ejecuta comprendiendo sucesivamente:

  - ○ dicha etapa de apertura de una sesión secundaria entre dicha pasarela intermediaria y dicho servidor, comprendiendo dicha etapa la colocación de la redirección de un disco emulado por la pasarela intermediaria en el que se registra dicho agente,
  - ○ la ejecución de un guion de temporización que espera a que dicho disco emulado esté disponible.
  - ○ la copia del agente hacia un directorio situado en el servidor.
  - ○ la ejecución del agente en dicho servidor
  - ○ el establecimiento de un canal virtual entre el servidor y la pasarela para la comunicación entre el agente y la pasarela
  - ○ a continuación, la apertura de un canal ascendente entre la estación cliente y el servidor.
  - ○ finalmente el agente lanza el administrador o la aplicación objetivo inyectándole los identificadores aplicativos necesarios transmitidos por la pasarela.

2. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** incluye una etapa de destrucción automática de dicho directorio por dicho servidor al final de la sesión.

3. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** el agente se ejecuta en el seno de la sesión con la identidad utilizada para la apertura de la sesión.

4. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** incluye una etapa previa de selección de un recurso objetivo, mediante la transmisión por el terminal cliente de un mensaje numérico que incluye un identificador de usuario y verificación por dicha pasarela de si las informaciones relativas a los derechos de utilización asociados a dicha identificación en una base de datos (302) se refieren a dicho recurso objetivo.

5. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** incluye una etapa previa de selección de un recurso objetivo, consistente en la transmisión por parte de la pasarela de datos digitales que comprenden la lista de los objetivos correspondientes a los datos registrados en una base de datos (302) en relación con el identificador transmitido y la selección por el usuario de uno de los objetivos propuestos.

6. Procedimiento de conexión de seguridad según la reivindicación 4 o 5 **caracterizado porque** dicha base de datos (302) comprende una lista de las aplicaciones y de los servidores que alojan cada una de dichas aplicaciones, así como las cuentas que permiten conectarse a estos servidores.

7. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** incluye una etapa de apertura de una conexión con la cuenta asociada al objetivo seleccionado.

8. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** dicha pasarela incluye unos medios para el cálculo de un balance de las cargas en función del número de conexiones ya abiertas hacia cada uno de los servidores y de selección para la nueva petición del servidor menos solicitado.

9. Procedimiento de conexión de seguridad según la reivindicación 1 **caracterizado por que** incluye una etapa de ejecución de un código informático para:

- interrogar a la pasarela para obtener las informaciones de autenticación que corresponden a la cuenta de la aplicación,
- inyectar estos datos en la aplicación con el fin de abrir una sesión aplicativa y permitir al usuario usar dicha aplicación.

10. Procedimiento de conexión de seguridad según la reivindicación anterior **caracterizado por que** dicho código se instala en el servidor (500) de manera permanente y **por que** el camino de acceso a este código se define en la base de datos (302).

11. Procedimiento de conexión de seguridad según la reivindicación 9 **caracterizado por que** dicho código se transmite transitoriamente, por un canal dedicado previsto en el protocolo multicanal (400), para ejecutarse transitoriamente en el servidor (500).

Fig. 1

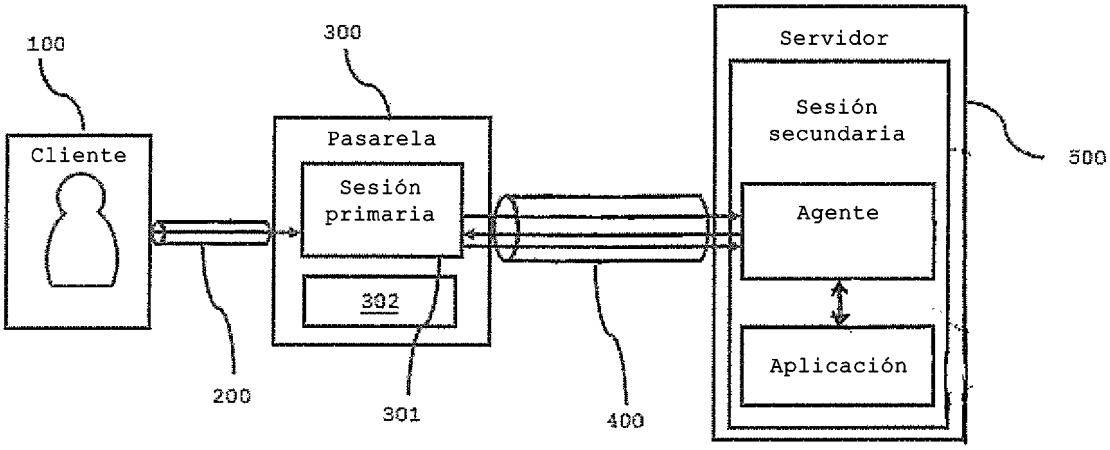

100
Cliente
300
Pasarela
Sesión primaria
302
200
301
400
Servidor
Sesión secundaria
500
Agente
Aplicación

Fig. 2

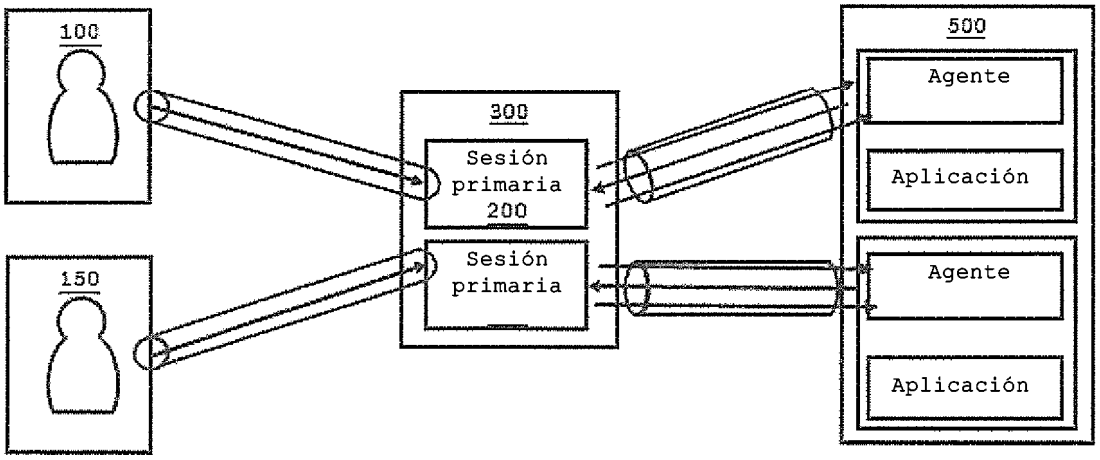
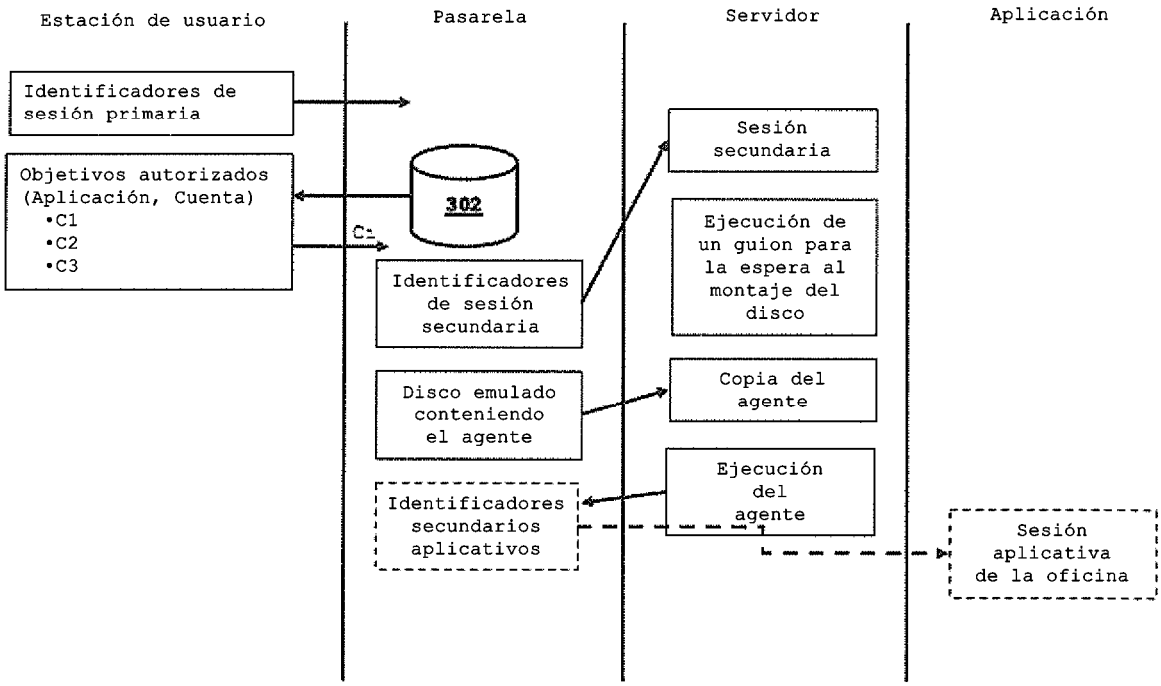

100
150
300
Sesión primaria 200
Sesión primaria
500
Agente
Aplicación
Agente
Aplicación

Fig. 3


Estación de usuario
Pasarela
Servidor
Aplicación
Identificadores de sesión primaria
Objetivos autorizados (Aplicación, Cuenta)
•C1
•C2
•C3
302
Identificadores de sesión secundaria
Disco emulado conteniendo el agente
Identificadores secundarios aplicativos
Sesión secundaria
Ejecución de un guion para la espera al montaje del disco
Copia del agente
Ejecución del agente
Sesión aplicativa de la oficina