

(19) **DANMARK**

(10) **DK/EP 3353986 T3**



Patent- og
Varemærkestyrelsen

(12) Oversættelse af
europæisk patentskrift

-
- (51) Int.Cl.: **H 04 L 29/06 (2006.01)** **H 04 L 29/08 (2006.01)**
- (45) Oversættelsen bekendtgjort den: **2019-05-06**
- (80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2019-03-13**
- (86) Europæisk ansøgning nr.: **16781511.7**
- (86) Europæisk indleveringsdag: **2016-09-20**
- (87) Den europæiske ansøgnings publiceringsdag: **2018-08-01**
- (86) International ansøgning nr.: **FR2016052372**
- (87) Internationalt publikationsnr.: **WO2017051104**
- (30) Prioritet: **2015-09-21 FR 1558890**
- (84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**
- (73) Patenthaver: **Wallix, 250 Bis Rue du Faubourg Saint-Honoré, 75008 Paris, Frankrig**
- (72) Opfinder: **Adda, Serge, 16 rue des Morteaux, 92160 Antony, Frankrig**
ZHOU, Raphaël, 7, rue Georges Sand, 94600 Choisy Le Roi, Frankrig
- (74) Fuldmægtig i Danmark: **Zacco Denmark A/S, Arne Jacobsens Allé 15, 2300 København S, Danmark**
- (54) Benævnelse: **Fremgangsmåde til sikker forbindelse fra en kundecomputerindretning til en computerkilde**
- (56) Fremdragne publikationer:
EP-A1- 2 894 814
EP-A2- 1 523 152
US-A1- 2013 191 627

Field of the invention

The present invention relates to the field of application servers, more particular methods and systems for access to application resources hosted on one or
5 more servers, by a user.

Prior art

A method for monitoring a session on a target system is known in particular in the prior art, European patent application EP 2894814.

10 A specific temporary agent for monitoring the session is installed on the target system on reception of the opening request coming from the client of the user.

The session is established between the user and
15 the target system through a communication network.

The temporary agent monitors the session, and collects data on events that occur on the target system during the session.

The temporary agent is uninstalled when the
20 session ends.

Drawbacks of the prior art

The solution proposed by the application EP 2894814 provides an installation step, for example by means of a PsExec command, requiring additional network

connections and particular privileges on the target server.

Moreover, it is necessary to carry out a specific step of uninstalling the agent, in order to prevent off-session execution thereof, unnecessarily consuming computing capacities of the server.

Solution afforded by the invention

The aim of the present invention is to remedy these drawbacks by proposing a simpler and safer solution, in particular avoiding an express uninstalling step. The solution that is the subject matter of the present invention also avoids security failings.

The invention, in its most general acceptance, relates to a method for secure connection, from a client computer device, to a target computer resource comprising a server, and where applicable an application executed on said server, using a proxy gateway comprising a memory for recording information relating to said connection as well as at least one agent executable on said server during a session, the method comprising the following steps:

- emission of a request for opening of a session by an application installed on the client station, leading to the creation of a primary session between a client station and the proxy gateway. Said request may contain the identifier of the target server or of the target application,

- opening of a session between said proxy gateway and said server.

Said method is characterised in that

- said step of installation of at least one agent is executed, comprising successively:

• said step of opening a secondary session between said proxy gateway and said server, said step comprising the establishment of the redirection of a disk emulated by the proxy gateway on which said agent is recorded,

• execution of a time-delay script that waits until said emulated disk is available,

• copying the agent to a directory. This directory may advantageously be a temporary directory situated on the server. The automatic destruction of said directory by said server at the end of the session makes a specific step of uninstalling the agent unnecessary,

• execution of the agent on said server,

• establishment of a virtual channel between the server and the gateway for communication between the agent and the gateway,

• next, the opening of an uplink channel between the client station and the server.

The method also comprises the launching by the agent of an application previously selected by the user, where applicable the one that can be the desktop manager if no application has been selected by the user.

5 According to a variant, the method according to the invention comprises a prior step of selection of a target resource, by the transmission by the client terminal of a digital message comprising an identifier of a user, and of verification by said gateway if the
10 information relating to the use rights associated with said identifier in a database (302) relates to said target source.

Advantageously, it comprises a prior step of selection of a target resource, consisting of the
15 transmission by the gateway of digital data comprising the list of the targets corresponding to the data recorded in a database (302) in relation to the identifier transmitted, and the selection by the user of one of the targets proposed.

20 Advantageously, said database (302) comprises a list of the applications and of the servers hosting each of said applications, as well as the accounts for connecting to these servers.

Preferably, said gateway comprises means for
25 calculating a balance of the charges according to the number of connections already opened to each of the

servers, and selection of the least busy server for the new request.

According to an advantageous embodiment, the method comprises a step of executing a computer code
5 for:

- interrogating the gateway with a view to obtaining the authentication information corresponding to the account of the application,

- injecting these data into the application in
10 order to open an application session and to enable the user to use said application.

According to a first variant, said code is installed on the server (500) permanently and in that the access path to this code is defined in the database
15 (302).

According to a second variant, said code is transmitted temporarily, by a dedicated channel provided in the multichannel protocol (400), in order to be executed temporarily on the server (500).

20 Detailed description of a non-limitative example embodiment

The present invention will be understood better from a reading of the following description, referring to non-limitative example embodiments, illustrated by
25 the accompanying drawings, where:

- figure 1 shows a diagram of the functional architecture of the invention

- figure 2 shows a diagram of the functional architecture of a variant embodiment of the invention

5 - figure 3 shows a schematic view of the steps of the process and of the data exchanged between the various computer resources.

Functional architecture

The user is a network or system administrator
10 having limited administration rights, for a set of resources for which he is responsible.

He has a terminal (100) communicating with the proxy gateway (300) (or "administration gateway") by means of a connection (200) according to a protocol for
15 example SSH ("secure shell") or RDP ("remote desktop protocol").

The connection gives rise to the creation of a primary session (301) on the gateway (300).

The user is identified by numerical identifiers
20 that are particular to him, and defining his rights, as well as the charging of the actions that he performs.

The gateway (300) comprises a database (302) in which the identifiers of the authorised users are recorded, as well as the associated rights, defining the

targets (accounts and equipment) on which the user is entitled to act.

At the time of connection, two methods for selecting the resource are possible:

5 - according to the first method, the user, at the time of the connection, specifies the target that he wishes to access. In this case the gateway checks whether the user identified by his identifier has necessary authorisations for accessing this target,
10 according to the information recorded in the database (302).

 - according to the second method, the gateway transmits to the user the list of targets corresponding to the data recorded in the database (302) in relation
15 to the transmitted identifier, to enable the user to select one of the targets proposed.

The following step consists of opening a connection, generally with the same SSH or RDP protocol, or with a second protocol, with the account associated
20 with the selected target. This step comprises successively:

- said step of opening a secondary session between said proxy gateway and said server, said step comprising the establishment of the redirection of an
25 emulated disk emulated by the proxy gateway on which said agent is recorded,

- execution of a time-delay script that waits until said emulated disk is available,

- copying the agent to a temporary directory situated on the server. The automatic destruction of said directory by said server at the end of the session makes a specific step of uninstalling the agent unnecessary,

- execution of the agent on said server,

- the establishment of a virtual channel between the server and the gateway for communication between the agent and the gateway,

- next, the opening of an opening channel between the client station and the server.

When the target is an application, the gateway (300) chooses the appropriate server (500) for executing said application. To this end, the database (302) comprises a list of applications and of the servers hosting each of said applications, as well as the accounts for connecting to these servers.

When a plurality of servers host the same application, the gateway effects a balance of the charge according to the number of connections already opened to each of the servers and, for the new request, selects the busy server.

Likewise, in the absence of a response by a server hosting an application, the gateway successively seeks the other servers hosting the same application, in order to select an available target.

5 The method also comprises the launch by the agent of an application previously selected by the user, where applicable the one that can be the desktop manager if no application has been selected by the user. The launch of an application may be dedicated if necessary
10 to a specialist computer code in order:

- to interrogate the gateway with a view to obtaining the authentication information corresponding to the account of the application, for example a password or a cryptographic certificate, or a Kerberos
15 ticket

- to inject these data into the application in order to open an application session and to enable the user to use said application.

This code may:

20 - be installed on the server (500) permanently. In this case, the access path to this code is defined in the database (302)

- or be transmitted temporarily, by a dedicated channel provided in the multichannel protocol (400), in
25 order to be executed temporarily on the server (500).

The name of this code may be generated uniquely, in order to make it more difficult to alter this code during the execution of the application, by means of a computer attack.

5 This temporarily installed code may also comprise a unique token in order to reduce the risks of unauthorised access to the data recorded in the base (302), by means of the opened session, by an attacker having access to the server (500).

10 Competing access to applications on the same server by a plurality of users

Figure 2 shows a functional diagram of a solution enabling a plurality of users to have access to applications hosted on the same server. The aim is to prevent interference between sessions, and to make them impermeable in terms of security.

To this end, when a second user (150) seeks to execute an application hosted on the same server (500) as an application executed for a first user (100), the gateway (300) will inhibit the data in the base (302) relating to the account used by the first user (100), on the server (500). It will enable the execution of an application on this same server (500) only if an account remains available for a second user (150).

25 Data exchanged between the computer resources

Figure 3 shows a schematic view of the data exchanged between the various computer resources.

At the time of connection by a user, the terminal (100) transmits the primary numerical
5 identifiers to the proxy gateway (300).

These authentication data are checked by the gateway (300), according to the information recorded in its database (302).

In the case of validation, the gateway (302)
10 transmits the list of authorised targets (C1 to C3).

Each target corresponds to a pair:

- application
- account associated with the application.

The account comprises:

- 15
- identification information
 - authentication information, such as a password.

The gateway transmits to the user (100), for each of the authorised targets, only the designation of
20 the application and the designation of the identifier of the account, but not the authentication information, in the form of character strings designating the application/account pairs.

The user (100) selects one of the targets proposed and transmits the identifier thereof to the gateway (300).

5 The gateway (300) chooses a server, and an account for opening a session on said server (500) according to the process of selecting the server and the previously described account.

10 It thus opens a secondary session, on the server. This session presents a disk emulated by the gateway. This disk comprises an agent. Then the gateway copies and starts the agent according to the previously described method. This starts the desktop manager or, in the case where the user has selected a specific application, it proceeds with the execution thereof of
15 either directly or by means of a specialist computer code. This code requests of the gateway the identifier of the account of the application as well as the authentication data associated with this account.

20 The computer code then transmits this information to the application in order to control the execution of the application.

P a t e n t k r a v

1. Fremgangsmåde til sikker forbindelse fra en kundecomputerindretning til en målcomputerkilde, som omfatter en server, og i givet fald, en applikation, der udføres på serveren, som anvender en proxy-gateway, som omfatter et lager til registrering af informationer vedrørende forbindelsen samt mindst én agent, som kan udføres på serveren under en session, hvor fremgangsmåden omfatter følgende trin:

- udsendelse af en anmodning om åbning af en session fra en applikation, der er installeret på kundeindretningen, hvilket fører til dannelsen af en primær session mellem kundeindretningen og proxy-gatewayen. Anmodningen kan indeholde identificeringsmidlet af målserveren eller målapplikationen.

- åbning af en session mellem proxy-gatewayen og serveren

hvor fremgangsmåden er **kendetegnet ved, at**

- trinnet med udsendelse af en anmodning udføres ved forudgående åbning af en primær session [RDP] mellem kundeindretningen og proxy-gatewayen med afsendelse af en besked, som omfatter identificeringsmidlet af målserveren eller målapplikationen

- trinnet med installation af mindst én agent udføres omfattende i rækkefølge:

◦ trinnet med åbning af en sekundær session mellem proxy-gatewayen og serveren, hvor trinnet omfatter etablering af en omdirigering af en emuleret plade gennem proxy-gatewayen, hvorpå agenten er registreret,

◦ udførelse af en tidsstyringsscript, der afventer, at den emulerede plade er disponibel.

◦ kopiering af agenten til et indeks, der befinder sig på serveren.

◦ udførelse af agenten på serveren

◦ etablering af en virtuel kanal mellem serveren og gatewayen til kommunikation mellem agenten og gatewayen

◦ derefter åbning af en uplink-kanal mellem kundeindretningen og serveren.

◦ endelig igangsætter agenten desktop-manageren eller målapplikationen ved at indsætte deri de nødvendige applikationsidentificeringsmidler, som overføres af gatewayen.

2. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** den omfatter et trin med automatisk destruktion af indekset gennem serveren ved slutningen af sessionen.

5

3. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** agenten udføres under sessionen med den identitet, der anvendes til åbning af sessionen.

10

4. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** den omfatter et forudgående trin med udvælgelse af en målressource, ved transmission gennem kundeterminalen af en digital besked, som omfatter et identificeringsmiddel af en bruger, og til kontrol af gatewayen, hvis informationerne vedrørende brugsrettighederne, som er forbundet med identificeringsmidlet i en database (302), angår målressourcen.

15

5. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** den omfatter et forudgående trin med udvælgelse af en målressource, bestående af transmission gennem gatewayen af digitale data, som omfatter listen over mål svarende til de data, der er registreret i en database (302) i forbindelse med det overførte identificeringsmiddel, og til brugerens udvælgelse af et af de foreslåede mål.

20

6. Fremgangsmåde til sikker forbindelse ifølge krav 4 eller 5, **kendetegnet ved, at** databasen (302) omfatter en liste over applikationer og servere, som hver især er vært for applikationerne, samt de konti, der gør det muligt at forbindes med disse servere.

25

7. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** den omfatter et trin med åbning af en forbindelse med den konto, der er forbundet med det udvalgte mål.

30

8. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** gatewayen omfatter midler til beregning af fordelingen af belastning i forhold til antallet af forbindelser, der allerede er åbne til enhver af serverne, og for den nye anmodning til udvælgelse af den mindst søgte server.

5

9. Fremgangsmåde til sikker forbindelse ifølge krav 1, **kendetegnet ved, at** den omfatter et trin med udførelse af en computerkode til:

- at udspørge gatewayen for at opnå autentificeringsoplysninger svarende til kontoen af applikationen,

10

- tilføre disse data i applikationen for at åbne en applikationssession og gøre det muligt for brugeren at anvende applikationen.

10. Fremgangsmåde til sikker forbindelse ifølge det foregående krav, **kendetegnet ved, at** koden er installeret på serveren (500) permanent, og **ved, at** adgangsstien til denne kode defineres i databasen (302).

15

11. Fremgangsmåde til sikker forbindelse ifølge krav 9, **kendetegnet ved, at** koden overføres som en overgang, gennem en dedikeret kanal, som er tilvejebragt i flerkanaalsprotokollen (400), for at udføres som en overgang på serveren (500).

20

Fig. 1

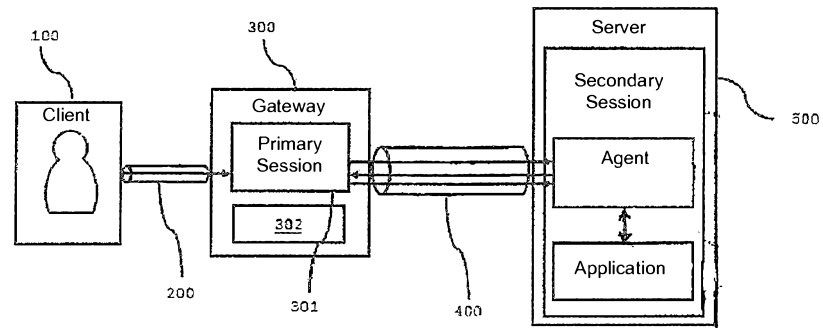


Fig. 2

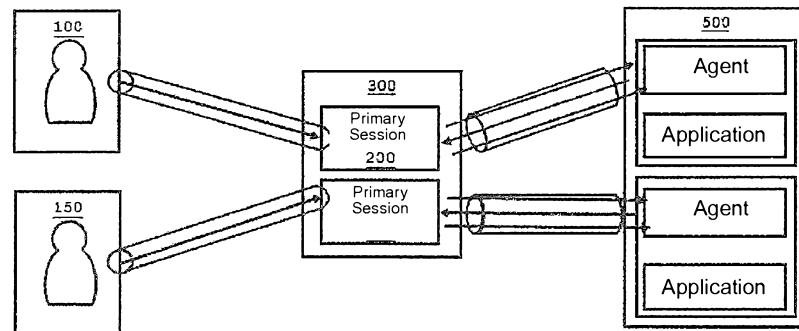


Fig. 3

