ВИРТУАЛИЗАЦИЯ ПРОГРАМНО ОСИГУРЯВАНЕ НА ВИРТУАЛНА ЛАБОРАТОРИЯ

Николай Димов, кореспонденти Димитър Няголов и Христо Узунов
Технически университет - София, Факултет и Колеж – Сливен, България
ndimov78@yahoo.com, d_nyagolov@abv.bg, hvuzunov@gmail.com,

Резюме: *Извършен е анализ и изследване на виртуална лаборатория и програмно осигуряване на учебен процес чрез сървърни hypervisor- и (Microsoft Hyper-V, Proxmox и VMware vSphere).*
В съществуващата ситуация са изградени няколко сървъра с различни счетоводни програми на клиентите, с цел оптимизация на компютърните конфигурации и разходите за текущо използване и поддръжка. На база на реализираната конфигурация е прието да се използва единствен физически сървър и виртуални машини за отделните счетоводни програми.
В тази конкретна реализация са налични три виртуални машини. На първата е инсталиран – Ажур, на втората – Плюс Минус ТРЗ, а на третата – Експерт М. Достъпът до всяка от виртуалните машини се осъществява по технологията за отдалечен достъп (Remote Desktop Connection – RDP) на Microsoft. Така реализирания подход с помощта на посочената технология значително се намалява мрежовия трафик и се подобрява латентността на мрежата. Всеки потребител в зависимост от нуждите за достъп до отделните счетоводни програми има създаден потребителски профил и парола за достъп до съответната виртуална машина. Посредством тях потребителят се свързва(login) със сървъра и получава достъп до предварително конфигурираните му софтуерни приложения.

Ключови думи: *Виртуализация, отдалечен достъп, hypervisor*

1. Въведение

Виртуализацията се отнася до създаването на виртуален ресурс като сървър, десктоп, виртуална машина, файл, хранилище или мрежа. Най-честата форма на виртуализация е виртуализацията на ниво операционна система. При нея е възможно да се стартират множество операционни системи на един и същ хардуер. Технологията на виртуализация включва разделянето на физическия хардуер и софтуер, чрез емулиране на хардуер с помощта на софтуер. Когато някоя операционна система работи върху основната операционна система чрез виртуализация, тя се нарича виртуална машина. В нашият случай ще използваме три виртуални машини VM1, VM2, VM3 Фиг. 1.[1, 2, 3]

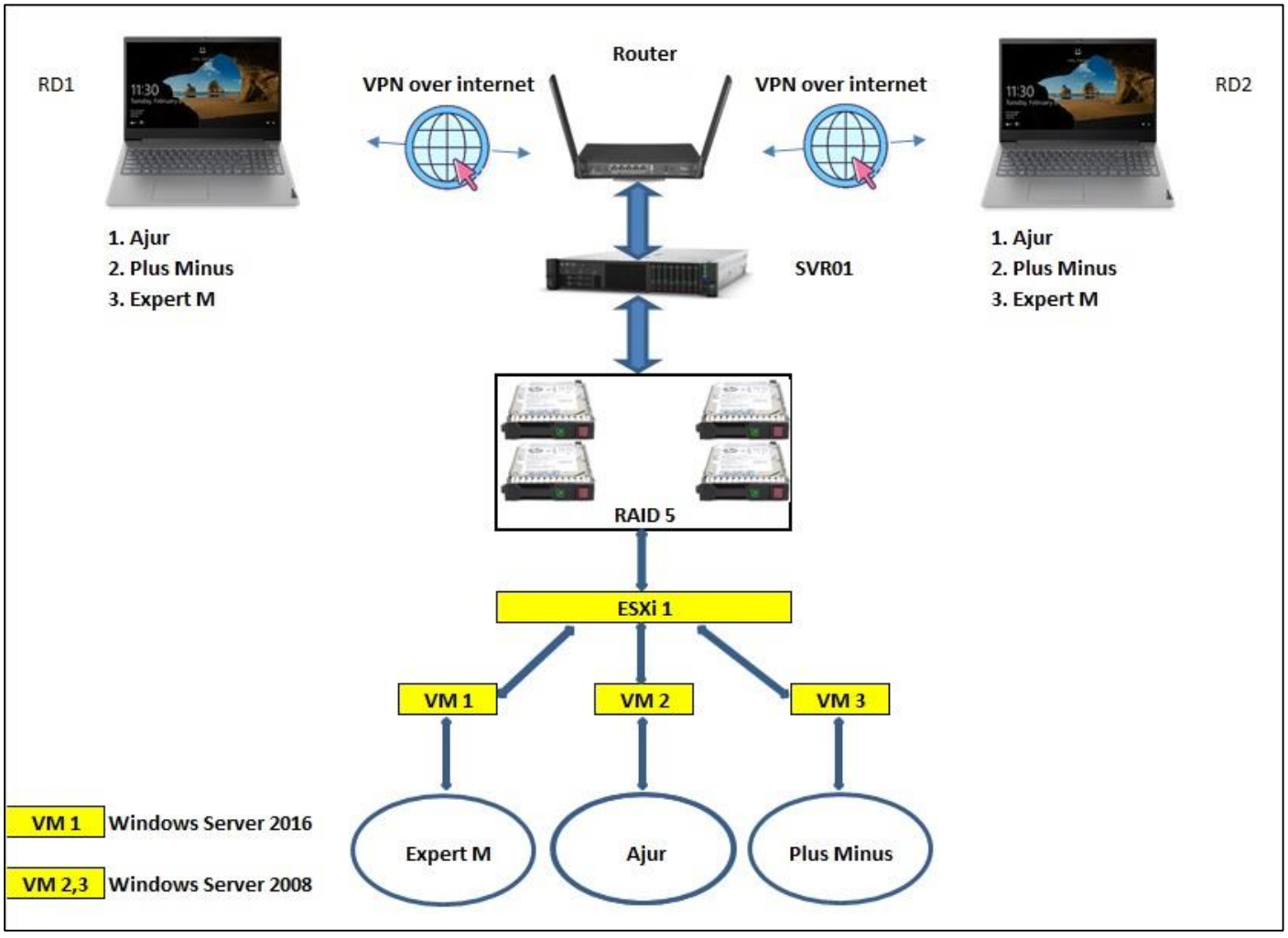
Целта на настоящата статия е да анализира ефективността на виртуализацията в реална среда, като резултатите се използват за нуждите при обучение на студентите.

Преди виртуализацията счетоводната къща е използвала няколко персонални компютъра, на които са инсталирани отделните счетоводни софтуерни продукти. За да могат да се използват от всички потребители тези софтуерни продукти, се е използвало мрежово споделяне (network sharing), което в повечето случаи е забавяло работата на всички, поради прекомерен трафик. При този метод обработката се извършва на всеки компютър поотделно, а данните се прехвърлят на файловия сървър. При реализиране на виртуализацията се премина към нов метод на работа – отдалечен достъп (Remote Desktop Connection), при който трафика значително намалява (между 10 и 100 пъти) и обработката на данните се извършва само на сървъра. На основата на тази структура в бъдеще може да се изгради подобен модел за нуждите на обучителния процес на студентите по различните инженерни дисциплини.

Инженерният анализ на модела ще е промишлен натурален експеримент, при който в реални експлоатационни условия ще се наблюдават всички основни параметри на модела.

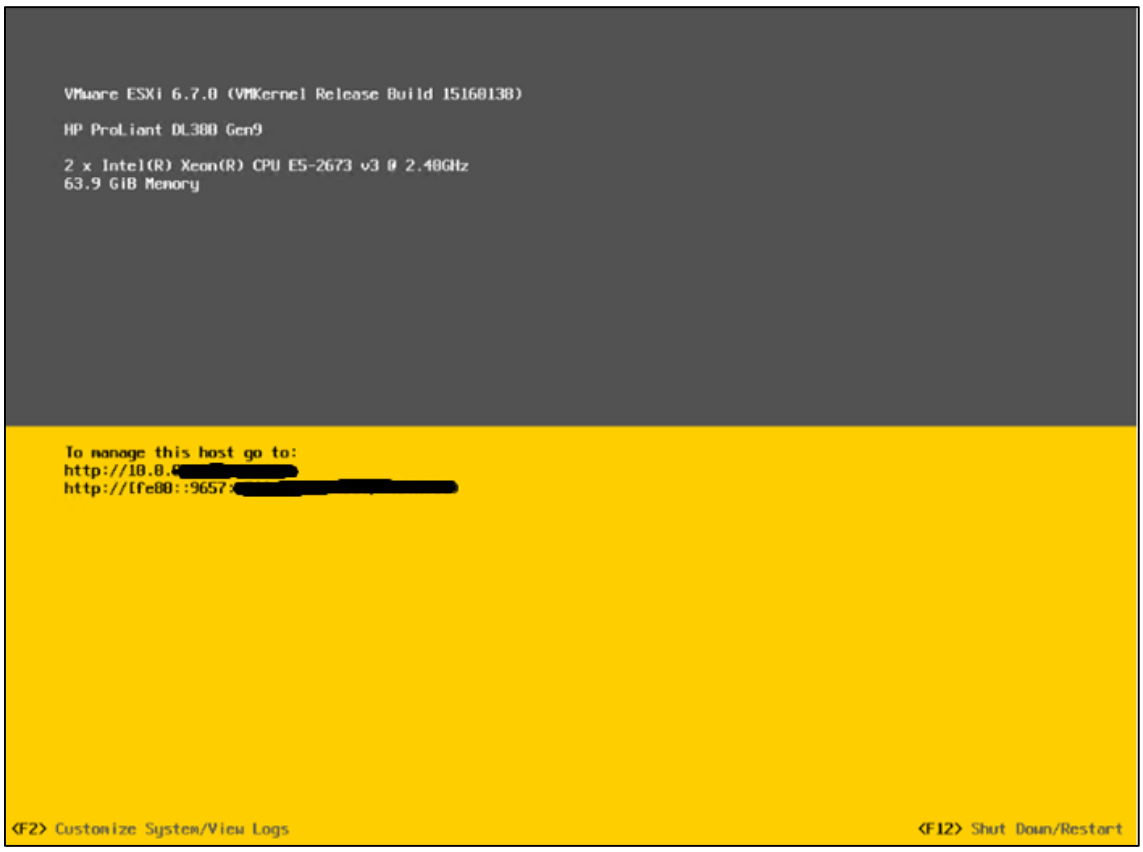
2. Създаване на модела

Системата е изградена с един сървър HP Proliant DL 380 G9, 2x Intel(R) Xeon(R) CPU E5-2673 v3, 64GB ECC DD4 RAM, Smart Array P440ar, 4x 900GB SAS HDD, 4x NetXtreme BCM5719 Gigabit Ethernet. На фигура 1 по-долу е представена архитектурата на системата. Връзката на системата с интернет се осъществява посредством рутера (Router), в този случай това Mikrotik hap AC2. За по-голяма сигурност е изграден VPN сървър(вътре в рутера), през който се осъществява достъпът до ресурсите на системата извън офиса на фирмата. Изграден е RAID 5 масив от четири диска, който се отличава с добра производителност и сигурност на съхранение на данните. Видно от фигурата са използвани две работни станции (лаптопите), това се прави с цел улеснение, броят на едновременните връзки зависи от нуждите фирмата, в случая 16. Мрежовата инфраструктура е изградена с 1GBits комутатори (switch), мрежови карти, кабели и конектори. Когато се осъществява достъп до системата извън офиса на фирмата, първо трябва да се осъществи връзка с VPN сървъра, за да се получи достъп до мрежовата инфраструктура, след което трафика преминава през рутера и достига до сървъра (SVR01), оттам през hypervisor-a (ESXi 1), към съответната виртуална машина (VM1,VM2,VM3) достигайки съответния мрежов протокол на сървъра на съответния счетоводен продукт. След проверка на потребителското име и парола за достъп, сървъра дава достъп до базата си данни и може да се започне работа със счетоводния софтуер.



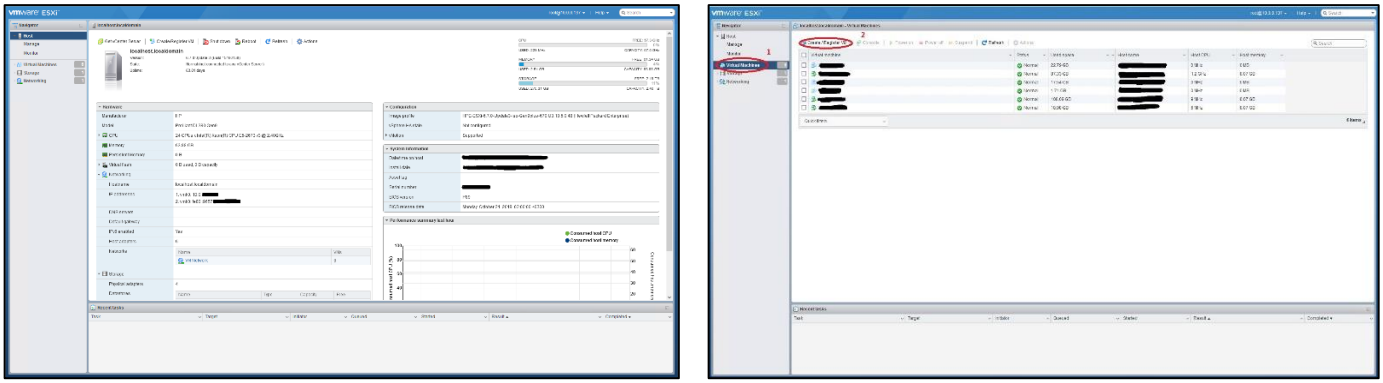
Фиг. 1. Архитектура на системата

След като се инсталира hypervisor-а трябва да се настрой мрежовата конфигурация през конзолата за управление на vSphere, за да получим достъп от уеб базирания клиент фигура 2 [3].



Фиг. 2. Конзола за управление на vSphere

След това се създават трите виртуални машини за всеки от счетоводните софтуери – Expert M, Ajur и Plus-Minus. За всяка от виртуалните машини са заделени по 4vCPU, 8GB RAM и 200GB дисково пространство. Това става през уеб базирания клиент показан на фигура 3[3].

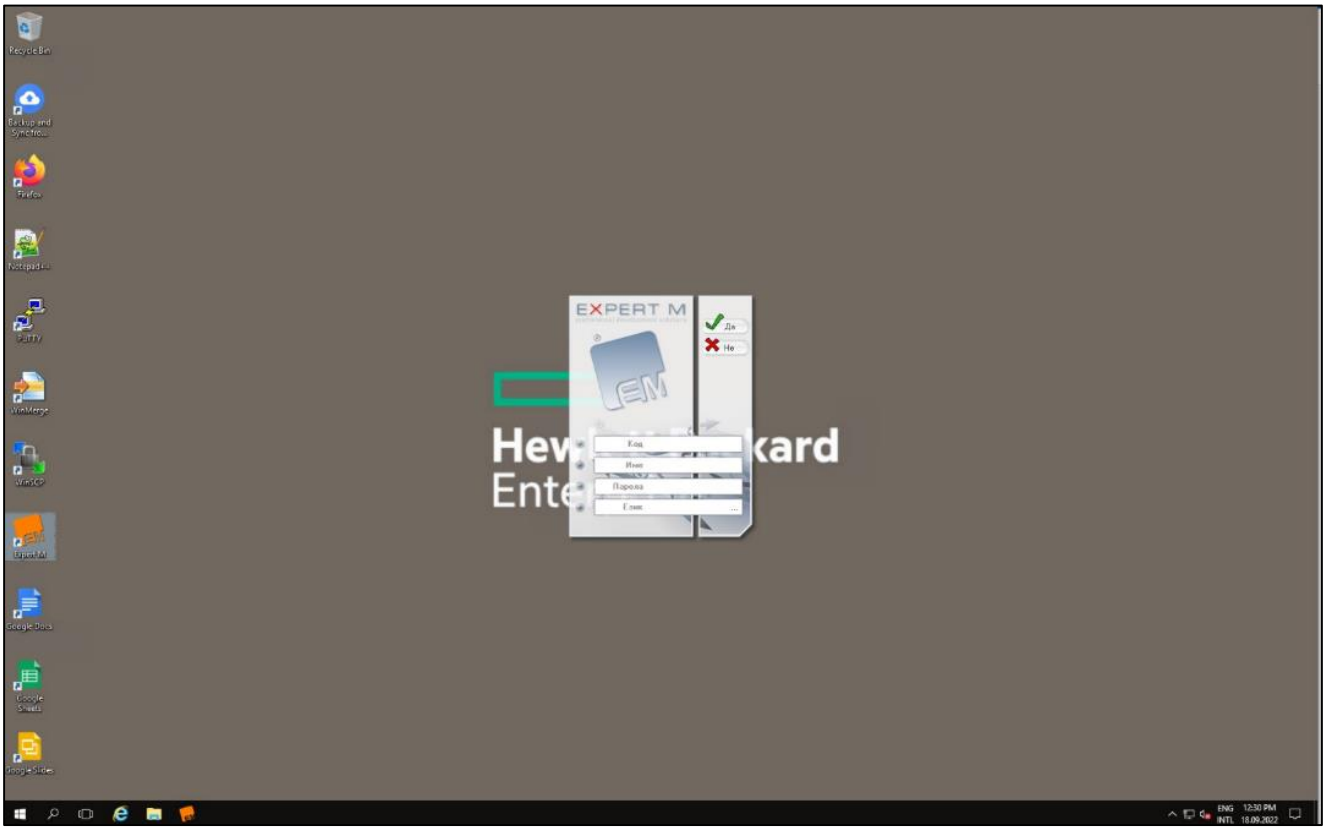


Фиг. 3 Уеб базиран клиент

Това се прави като се натисне бутон Virtual Machines (в лявата част на екрана, означена с цифрата 1), след което се появява бутон Create/Register VM (в централната горна част, означена с

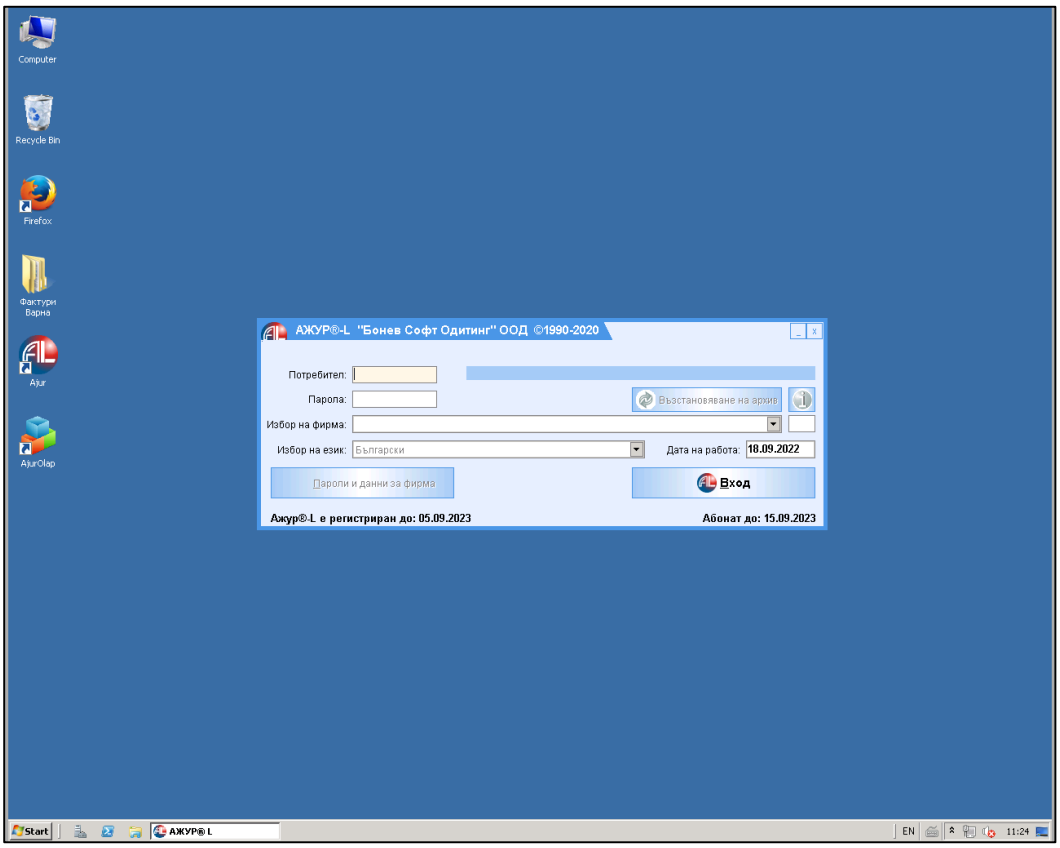
цифрата 2). Появява се помощник (wizard), чрез който се създава нова виртуална машина, изписва се името на новата VM, след което от падащите менюта се избира каква съвместимост на hypervisor –а ще се използва, каква операционна система ще се инсталира, в случая Windows Server 2008 или 2016, след което се преминава към настройване на процесорни ядра; оперативна памет; дисково пространство – обем и тип (200GB, thin provisioning), тип на дисковия контролер (SAS); мрежова карта – тип и скорост; добавя се дисков образ (ISO image), за да може да се стартира инсталацията на операционната система. След правилното конфигуриране трябва да се появи в списъка с виртуални машини, новосъздадената.

След това се инсталират и настройват отделните виртуални машини като резултат от това е показан на фигури 4, 5 и 6.

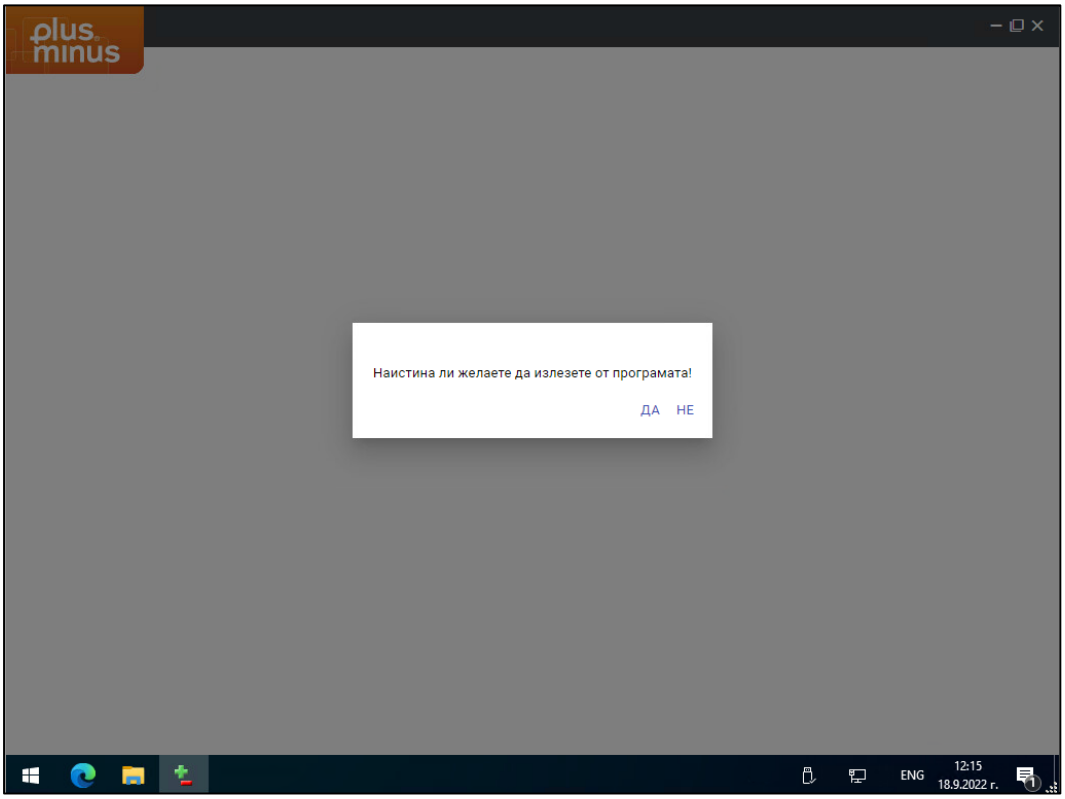


Фиг. 4. Екранна снимка на сървър със счетоводен софтуер Expert M.

Потребителят, за да получи достъп до съответния програмен продукт трябва да стартира „Връзка с отдалечен работен плот“ (Remote Desktop Connection – RDP) като за улеснение са направени отделни преки пътища (Shortcut) на работния плот. Ако се налага достъпът до софтуера да се осъществи извън рамките на офиса е необходимо да се изгради VPN свързаността преди да се премине към самото стартиране на RDP. За да стане това се стартира отново shortcut като този път той е именуван VPN, като след стартиране се извежда прозорец, на който се натиска бутон свързване, след появата на надпис свързан (connected), може да се премине към следващата стъпка. Натиска shortcut за съответния продукт, при което излизат полета за въвеждане на неговите потребителско име и парола, след което се появява екрана от фигури 4, 5 и 6. След това стартира самото приложение и въвежда своите потребителско име и парола за достъп до него [4, 5, 6].



Фиг. 5. Екранна снимка на сървър със счетоводен софтуер Ajur



Фиг. 6. Екранна снимка на сървър със счетоводен софтуер Plus Minus.

3. Резултати и изводи

В резултат на въвеждането на виртуализацията вместо обслужване на три физически машини остава една, като същевременно се използва голяма част от ресурсите ѝ. Намален е мрежовия трафик, могат да се използват т. нар. тънки клиенти вместо персонални компютри, подобрена е сигурността, тъй като мрежовия трафик вече е криптиран. Възможен е достъп до счетоводните софтуери извън офиса от различни устройства посредством направения VPN сървър. Възможно е добавяне на още виртуални машини в бъдеще в зависимост от нуждите на фирмата. Извършва се автоматичен бекъп на виртуалните машини, както на вграденото дисково пространство (storage), така и на външен такъв. Ограничен е достъпа на неоторизирани потребители до ресурсите на сървърите, което повишава конфиденциалността на данните и намалява риска от заразяване с вируси и шпионски софтуер. Постигнати са всички първоначално заложени изисквания по отношение на бързодействие и сигурност.

Литература

[1]. Майкъл Браун, Ник Маршъл, и Райън Джонсън – Mastering VMware VSphere 6.7, 2018
[2]. www.microsoft.com
[3]. www.vmware.com
[4]. www.bsoft.com
[5]. www.plusminus.com
[6]. www.expert-m.net