

ЗАХОДИ З ЗАХИСТУ КОМП'ЮТЕРНИХ ПРОГРАМ ТА СИСТЕМ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ ВІДДАЛЕННОГО ДОСТУПУ

Староверов Р. М., Фурман І. О.

Харківський національний технічний університет сільського господарства імені Петра Василенка

Запропоновано огляд заходів з захисту комп'ютерних програм та систем за допомогою технологій віддаленого доступу.

Постановка проблеми. Сучасні умови забезпечення безперебійної роботи, а також рівня захищеності даних пред'являють особливо високі вимоги до інформаційно-телекомунікаційної архі-тектури, особливо з урахуванням її можливого розвитку. Зокрема, висувуються серйозні вимоги до централізованого управління і масштабованості IT-сервісів, прискоренню роботи цих комп'ютерних програм та систем за наявності мереж з невисокою пропускнуною спроможністю, забезпеченню роботи в різноманітних обчислювальних середовищах з одночасною роботою в мережі як "тонких" клієнтів, так і персональних комп'ютерів та ін.

Аналіз останніх досліджень та публікацій. Останнім часом технології термінального доступу все активніше стали використовуватися в різних сферах. Найбільший ефект від їх застосування може бути досягнутий в наступних умовах:

- основна частина користувачів працює із завданнями, що вимагають великої обчислювальної потужності, або більшість з них запускають програми одночасно;
- для організації характерна географічна розподіленість її структури і розосередженість баз даних;
- присуття значна кількість успадкованої обчислювальної техніки;
- для зв'язку з віддаленими філіями використовуються повільні або недостатні канали зв'язку;
- у відділеннях і філіях недостатньо кваліфікованого технічного персоналу;
- рівень інформаційної безпеки не відповідає очікуваному.

Мета статті. Описану ситуацію можна вважати характерною як для навчальної сфери, так і для сільськогосподарського сектору. Дійсно, мережі середніх і великих навчальних закладів включають велику кількість персональних комп'ютерів під керуванням різних версій операційних систем та декілька потужних серверів. А сільсько-господарському сектору, в першу чергу, властиві значні відстані між різними об'єктами господарювання. Безперебійна робота цих віддалених філій вимагає і високопродуктивних каналів зв'язку, і забезпечення додаткової надійності.

Основні матеріали дослідження. Технологія термінального доступу має значні переваги в порівнянні із звичним клієнт-серверним підходом.

Централізована обробка інформації. Вона припускає виконання усіх комп'ютерних програм на термінальних серверах і установку на клієнтському місці лише клієнтських термінальних пристроїв. При цьому каналами зв'язку передаються тільки відображення

даних (по суті, оновлення екрану, натиснення клавіш і руху миші), самі дані "не виходять за рамки" серверного приміщення. Такий підхід виключно зручний тим, що не лише мінімізує вимоги до навчання працівників, але і істотно спрощує контроль їх роботи. А спеціальна технологія дозволяє одночасно зробити нову програму доступною багатьом користувачам, підвищує оперативність обслуговування клієнтських місць.

Ефективна робота з філіями. Співробітники можуть знаходитися в місцях, значно віддалених від термінальних серверів, з'єднуючись з ними виділеними каналами або за допомогою модемів. Такий вид зв'язку надає відчутні переваги, оскільки розв'язується традиційна і істотна проблема оперативного збору інформації з місць: виключаються складнощі адміністрування і експлуатації розподіленої бази даних, що вимагає використання дорогих каналів зв'язку з великою пропускнуною спроможністю.

Скорочення сукупної вартості інфраструктури. Термінальні облаштування дешевше комп'ютерів, а найголовніше — вони не вимагають подальшої модернізації і не схильні до морального старіння. Не вимагається купувати ліцензії на клієнтські операційні системи, антивірусні і інші службові програми для обслуговування локальних ресурсів. До того ж зосередження програмного забезпечення в одному місці істотно спрощує процедури оновлення і реконфігурації програмного забезпечення. Забезпечується і можливість використання вже існуючої інфраструктури для впровадження нових сервісів. В якості обладнання доступу до термінальних серверів можна використати будь-які персональні комп'ютери, старі і нові, з будь-якими операційними системами, термінали, ноутбуки, нетбуки і навіть телефони та комунікатори.

Висока захищеність ресурсів. При використанні термінального способу доступу усі інформаційні масиви зосереджені в єдиному місці. Дійсно, централізація зберігання необхідних даних захищає їх як від зовнішніх, так і від внутрішніх порушників. Користувачі не можуть помилково видаляти інформацію. Усі дані зберігаються на серверах, для яких набагато простіше забезпечити надійний захист, чим для клієнтських систем. Унеможливлено установку користувачами несанкціонованих програм.

Термінальний доступ підвищує надійність інформаційної системи в цілому, оскільки переносить виконання клієнтської частини з потенційно ненадійних персональних комп'ютерів на відмово-стійкі термінальні сервери.

Для термінального доступу характерний високий рівень відмовостійкості. Дійсно, у разі виходу з ладу частини устаткування, як серверного, так і каналу зв'язку, користувачі мають можливість працювати із програмами; у разі відмови одного або декількох термінальних серверів користувачі продовжують працювати на серверах, що залишилися. Обробка інформації відбувається на сервері, тому при відключенні "тонкого" клієнта (розриву з'єднання, відключення живлення, поломка і т. д.) усі запущені програми продовжують виконуватися.

Можливість роботи на каналах з низькою пропускнуою спроможністю. Технологія термінального доступу пред'являє мінімальні вимоги до пропускнуої спроможності каналів зв'язку. Можливо працювати з каналами не більше 10-15 Кбіт/с із розрахунку на одну призначену для користувача сесію. Час реакції і швидкість оновлення екрану віддаленими локальними програмами виявляються практично рівними.

Технологій без недоліків і обмежень не буває. У чому ж полягають обмеження при використанні технології термінального доступу?

Апаратно-програмні вимоги до термінального сервера (потужність процесора, об'єм оперативної пам'яті та ін.) при великій кількості споживачів можуть істотно зростати. Конкретні значення навантажень сильно залежать від програм, що запускаються на термінальних серверах, і об'ємів даних, з якими працюють користувачі. При зростанні навантаження можна поставити поруч додатковий сервер і налагодити розподіл навантаження.

У літературі вказується на можливу несумісність окремих програмних продуктів з технологією термінального доступу. Наприклад, деякі старі програмні пакети можуть не працювати в середовищі термінального сервера. Проте моніторинг номен-клатури використовуюваного в сучасних умовах програмного забезпечення показує, що використання таких програм у наш час незначне, а їх кількість постійно зменшується.

Необхідно відмітити, що обмеження застосовності термінального доступу особливо помітні для умов, що вимагають потужних периферійних мереж (понад 100 Мбіт/с), наприклад для завдань, що використовують відеопотоки високої чіткості зображення, стереопотоки звуку з високою якістю та ін. Проте для більшості програм цілком достатньо передачі пакетних даних зі швидкістю не більше 10-15 Кбіт/с. Тому, як представляється, на навчальний процес обмеження застосовності термінального доступу не поширюються. Єдине, на що доцільно звернути увагу, це підвищені вимоги до надійності каналів зв'язку: якщо термінальний сервер недо-ступний, то працювати не зможе ніхто.

Висновки. Таким чином, переваги використання технологій термінального доступу у різних сферах очевидні, а обмеження несуттєві.

На закінчення коротко розглянемо наприклад наш навчальний заклад. Університет працює не перший рік і устаткування вже не відповідає сучасному рівню, хоча для поліпшення якості роботи нерідко закуповуються нові програми та комп'ютери. Є декілька навчальних корпусів, яким необхідно регулярно зв'я-

зуватися з центральним корпусом, обмінюючись необхідними даними. Можливо поставити завдання мінімізувати витрати на оновлення ІТ- інфраструктури.

У разі традиційної клієнт-серверної архітектури необхідно послідовно і напружено оновлювати робочі станції, декілька серверів, клієнтське і серверне програмне забезпечення. На кожній робочій станції встановлювати програми. Кожне робоче місце кожні два три роки модернізувати. На випадок розширення вимагається проводити увесь цей комплекс робіт спочатку. Необхідно приймати на роботу додаткових адміністраторів для забезпечення функціонування мережі і регулярно нести значні витрати на ІТ- підтримку.

У разі реалізації термінального доступу в центральному корпусі будуть встановлені термінальні сервери, що дозволяють організувати віддалений доступ до програм і баз даних. Усі необхідні програми та інформація знаходяться в центральному корпусі — не буде необхідності їх інсталяції і розміщення у філіях. На комп'ютерах співробітників будуть встановлені термінальні клієнти, що не потребують обслуговування, для відображення і керування програмами, що дозволить використовувати дешеві і навіть застарілі комп'ютери. Сукупна вартість усієї ІТ - архітектури значно зменшиться.

Список використаних джерел

1. Тодд Мазерс. Часть III. Реализация служб терминалов и пакета Citrix Metaframe / Тодд Мазерс // Администрирование Windows Server 2003/2000 на терминальном сервере = Windows Server 2003/2000 Thin Client Solutions — 3-е изд. — М.: "Вильямс", 2007. — С. 1072.
2. www.kiev-security.org.ua

Анотація

МЕРОПРИЯТИЯ ПО ЗАЩИТЕ КОМПЬЮТЕРНЫХ ПРОГРАММ И СИСТЕМ С ПОМОЩЬЮ ТЕХНОЛОГИИ УДАЛЕННОГО ДОСТУПА

Староверов Р. Н., Фурман И. А.

Предложен обзор мероприятий по защите компьютерных программ и систем с помощью технологии удаленного доступа.

Abstract

MEASURES ON PROTECTING OF COMPUTER PROGRAMS AND SYSTEMS BY MEANS OF TECHNOLOGY REMOTE ACCESS

R. Staroverov, I. Furman

The review of measures is offered on protecting of the computer programs and systems by means of technology remote access.