

Операционные системы

ч. II

Лекция 6

**Дополнительные сервисы
Windows Server 2008-2012-2016**

Терминальные сервисы

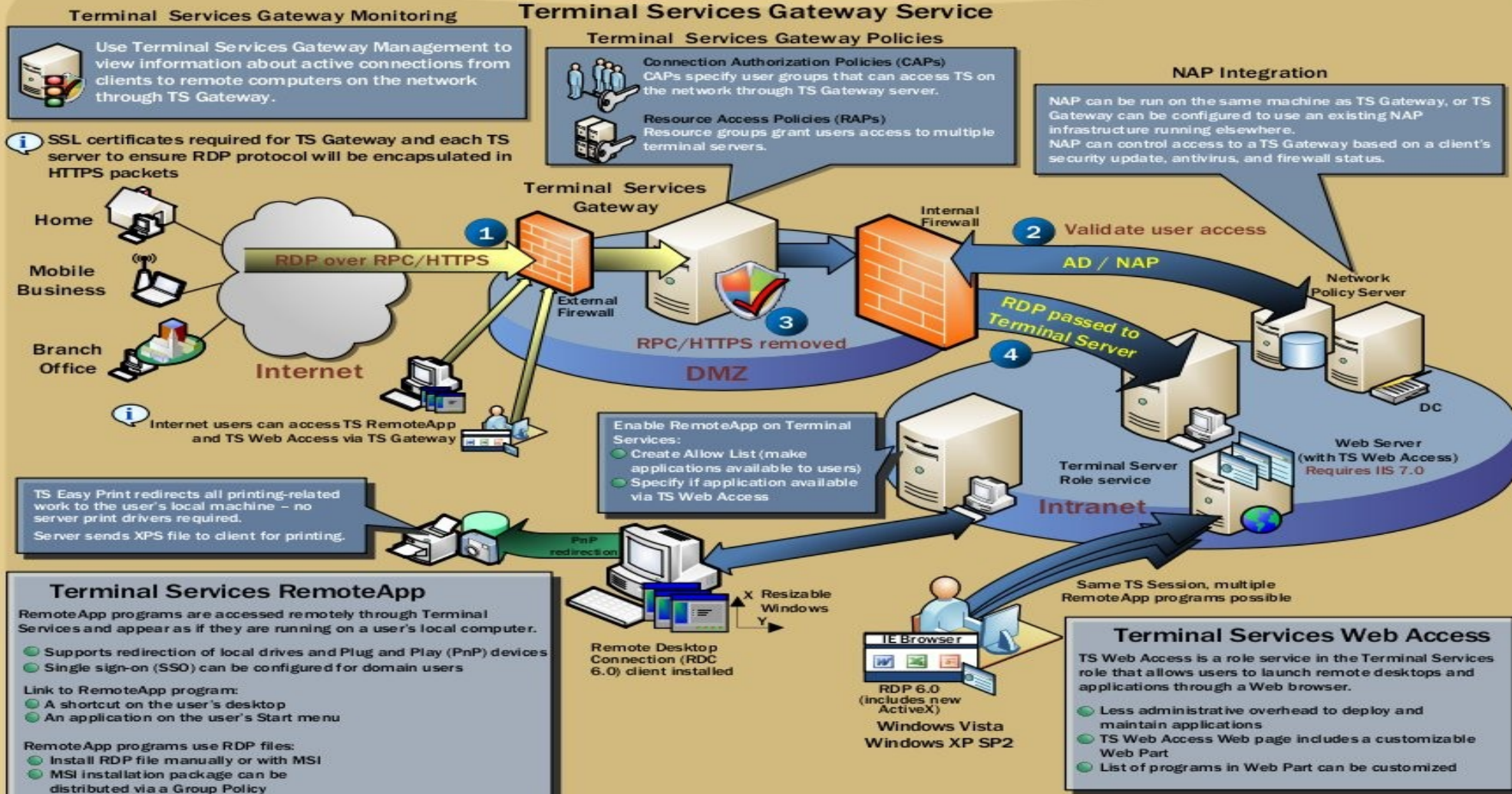
Terminal Services

Product Scenario: Centralized Application Access



Windows Server 2008

Terminal Services provides access to Windows-based programs from a variety of devices. Terminal Services is enhanced with Terminal Services RemoteApp, Terminal Services Web Access, and Terminal Services Gateway.



Терминальные сервисы: RDP over HTTPS - Аутентификация

Веб-доступ к удаленным раб. x

← → ↻ **Ненадежный** | <https://192.168.1.9/RDWeb/Pages/ru-RU/login.aspx>

Веб-доступ к удаленным рабочим столам

Work Resources

Подключение к удаленным рабочим столам и приложениям RemoteApp

[Справка](#)

Домен\имя пользователя:

Пароль:

Безопасность

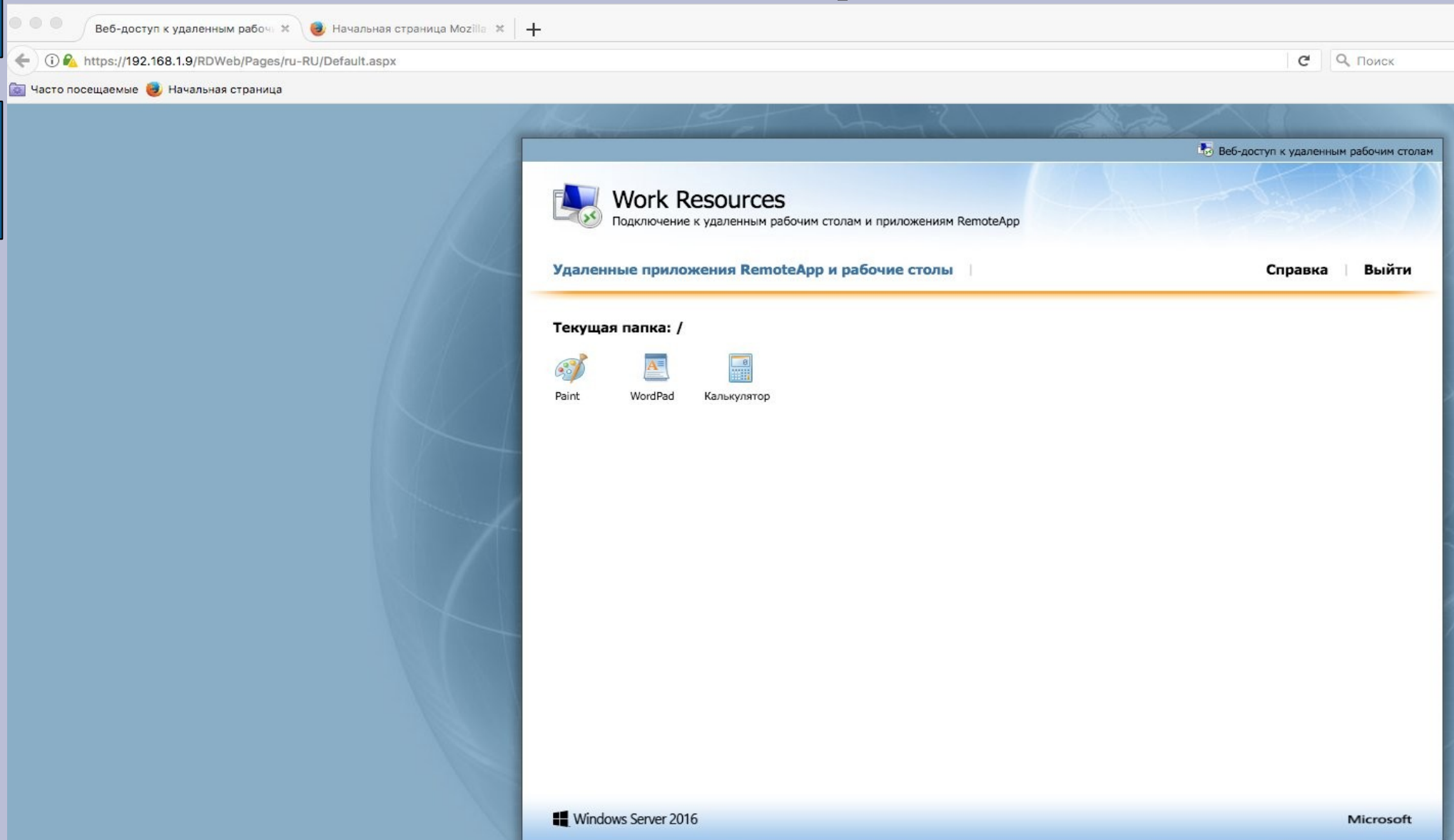
Внимание! Выполнив вход на эту веб-страницу, вы подтверждаете, что этот компьютер соответствует политике безопасности вашей организации.

В целях защиты от несанкционированного доступа сеанс веб-доступа к удаленному рабочему столу будет автоматически завершен после определенного периода бездействия. В случае завершения сеанса обновите страницу в браузере и повторите вход.

Windows Server 2016


Microsoft


Терминальные сервисы: RDP over HTTPS — доступ к коллекции



Терминальные сервисы: RDP over HTTPS — выбор приложения


ps://192.168.1.9/RDWeb/Pages/ru-RU/Default.aspx


 Веб-доступ к удаленным рабочим столам


**Work Resources**
Подключение к удаленным рабочим столам и приложениям RemoteApp


Удаленные приложения RemoteApp и рабочие столы | [Справка](#) | [Выйти](#)

Текущая папка: /

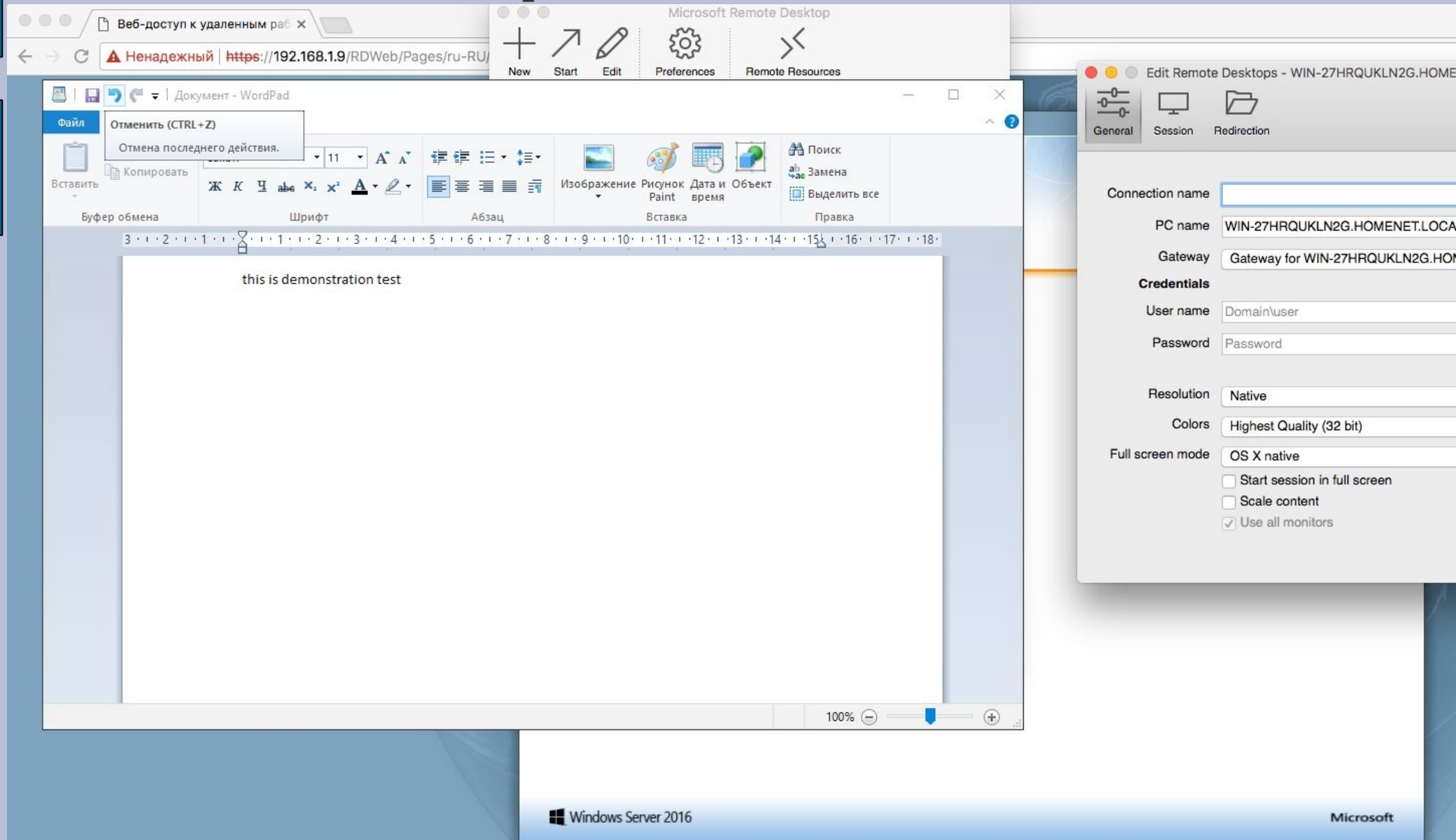

Paint


WordPad


Калькулятор

 Windows Server 2016 Microsoft

Терминальные сервисы: RDP over HTTPS — запуск приложения



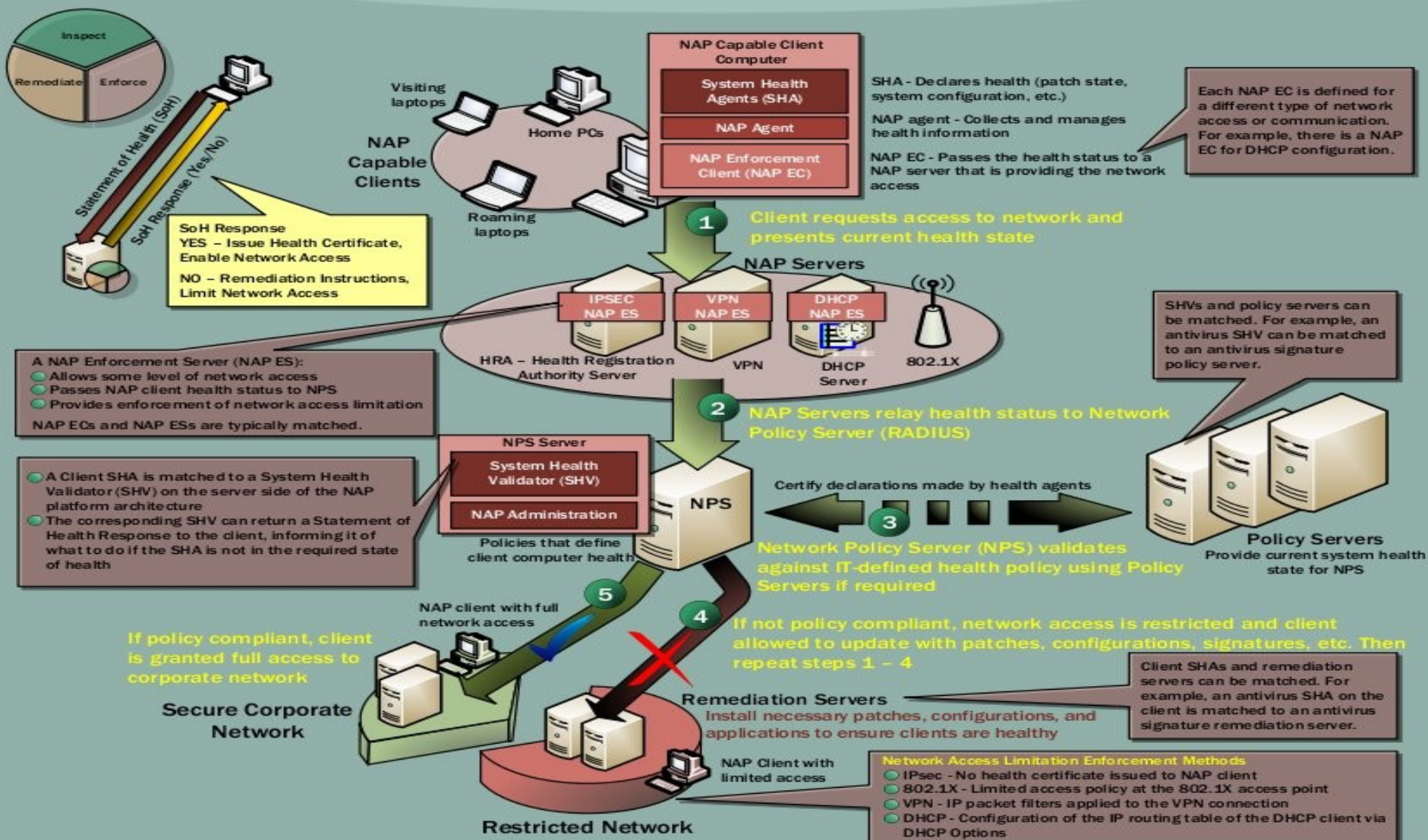
Защита сетевого доступа

Network Access Protection

Product Scenario: Security and Policy Enforcement



Network Access Protection (NAP) is a client health policy creation, enforcement, and remediation technology. NAP defines the required configuration and update conditions for a client computer's operating system and critical software.



IIS 7.0

Internet Information Services 7.0

Product Scenario: Web & Applications Platform



A secure, easy-to-manage server platform for developing and reliably hosting Web applications.

Administration and Diagnostics

Detailed Custom Errors

- What went wrong & why
- How to fix it

Failed Request Tracing

Define rules to capture runtime data only on failures

Specify tracing by:

- Status Code
- Time Taken
- Event Verbosity

IIS Manager and Delegation

- Control feature delegation
- Manage IIS manager users
- Manage site & application administrators

Remote Administration over HTTP

Management Tools

- Graphical - IIS Manager
- Command Line - appcmd
- Script - WMI
- Managed Code - Microsoft.Web.Administration

Runtime State and Control

View real-time server state across:

- Sites & Application Pools
- Application Domains
- Worker Processes
- Executing Requests

Extensible UI

Modular Architecture



Security

- Reduced surface area - Minimum install by default
- Delegated Web site configuration for site owners and developers
- Built-in user and group accounts dedicated to the Web server
- Enhanced Application Pool Isolation

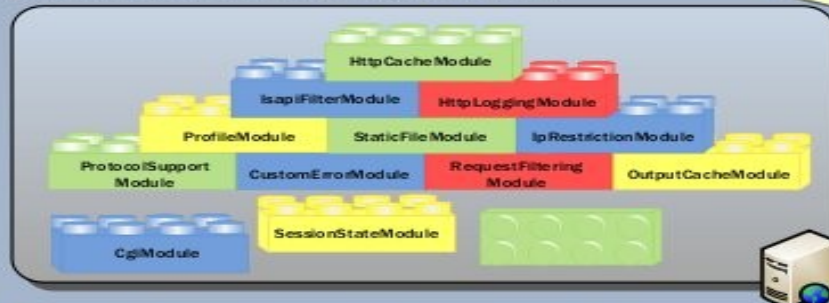


Extensibility

- Powerful User Interface Extensibility
- Extensible, modular architecture - add, remove or replace any built-in module
- Schema-based extensibility for configuration and dynamic data

- Built-in IIS7 request filtering
- Filter requests on the fly based on verb, file extension, size, namespace, sequences, and many more

IIS 7.0 and ASP.NET components work seamlessly together as part of the brand new IIS 7.0 Integrated Pipeline



- Extensible, modular architecture (40+ Components)
- Enhanced ASP.NET integration
- Minimized surface area and patching
- Improved performance and reliability with new FastCGI module

IIS 7.0 Architecture - Modular Web Server

Extensible Schema

IIS7 configuration system based on distributed XML files that hold the configuration settings for the entire Web server platform (e.g. IIS, ASP.NET)



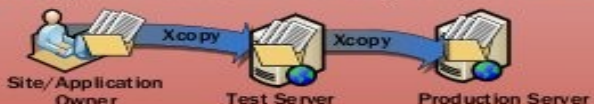
Shared Configuration

Configuration files can be stored on a back-end file server and referenced from multiple front-end Web servers



ApplicationHost.config
Web.config
Application Files

IIS7 enables configuration to be stored in a web.config file in the same directory as the site or application content, which can easily be copied from machine to machine



Configuration and Deployment

Visit www.IIS.net



IIS Team Blogs



Grab Samples from the DownloadCENTER



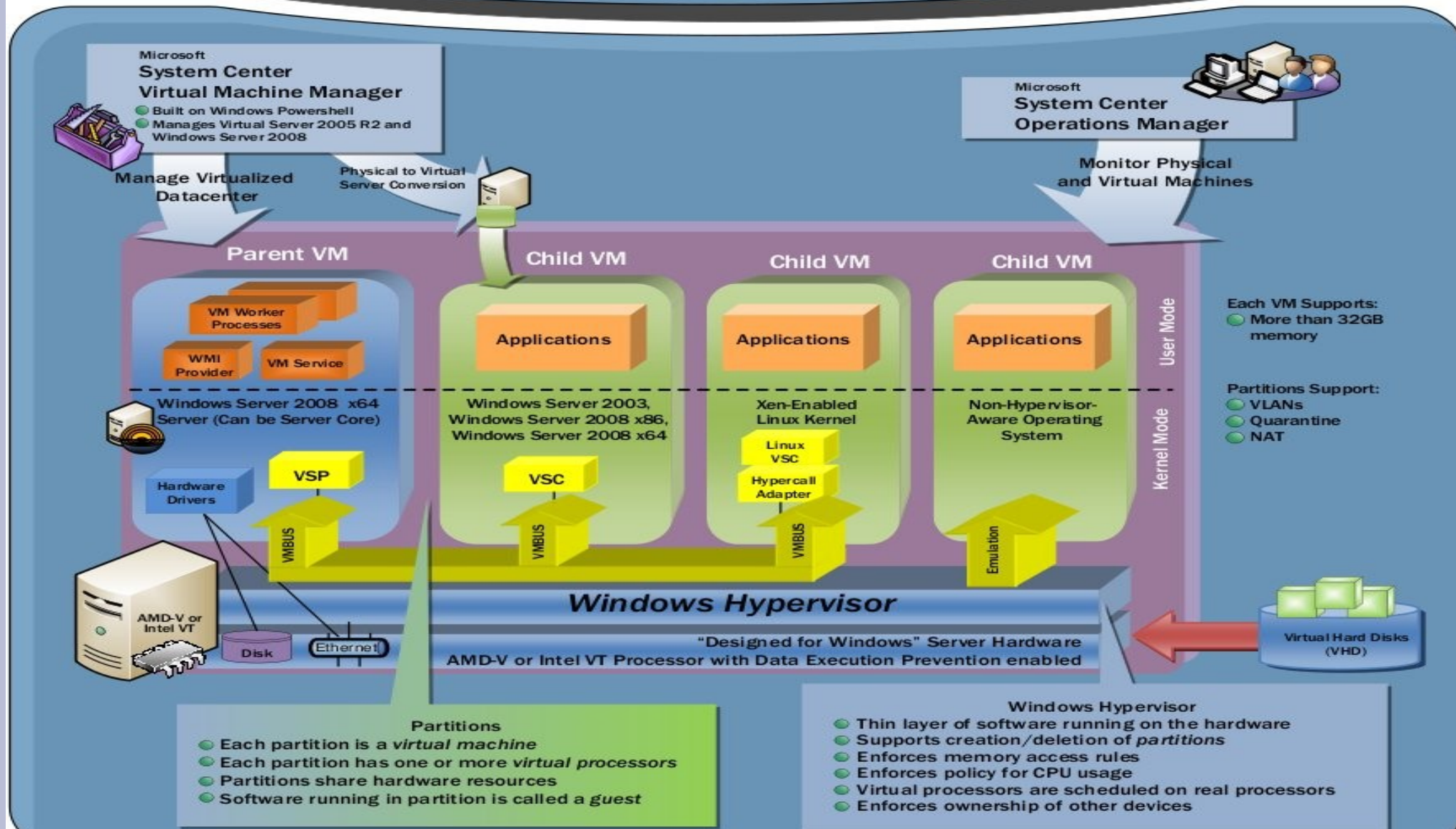
Get Answers in the TechCENTER & Forums

Hyper-V

Virtualization Product Scenario: Server Virtualization



Windows Server 2008 includes Windows Server Virtualization. Windows Server Virtualization is a 64-bit hypervisor-based virtualization technology that facilitates agility and integrated management of both physical and virtual components.



Server Manager

Server Manager and Server Backup

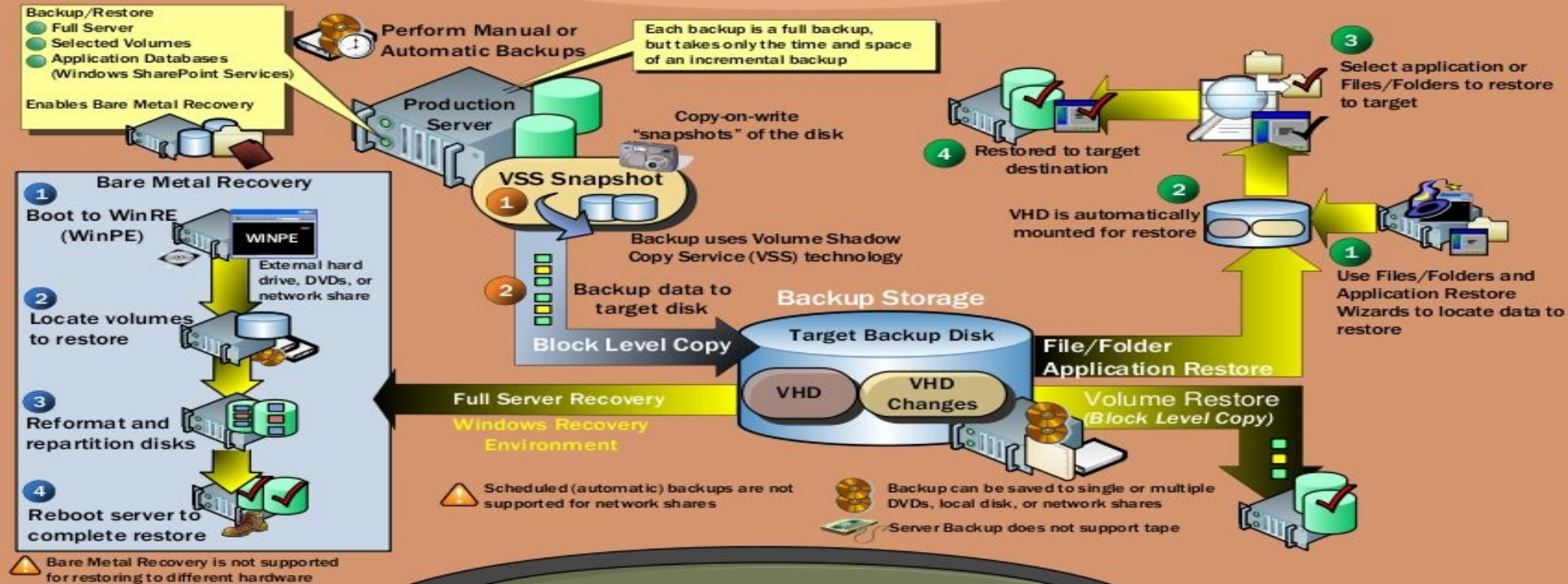
Product Scenario: Server Management



Windows Server 2008

Server Manager provides server configuration and commands for managing roles and features. Server Backup feature provides backup and recovery solutions.

Server Backup



Server Manager

Configuring Roles & Features

Server Roles

Server role describes primary function of server - e.g. File Services

Server Features

Features provide supporting functions to servers - e.g. Failover Clustering

Servers can support single or multiple roles

Add/Remove Roles/Features Wizards



Roles and features installed by using Server Manager are secure by default. No need to run Security Configuration Wizard following role installation or removal.

Server Manager Functionality

- Install and configure roles and features using UI or command line
- View status and events for installed roles
- Identify missing/broken configuration for installed roles
- Manage and configure roles installed on the server

Perform Initial Configuration Tasks

- Computer name, Domain membership
- Administrator password
- Network connections, Windows Firewall



Базовая установка сервера и шифрование

Server Core & BitLocker Product Scenario: Branch Office



Server Core installation option provides a minimal environment for running specific server roles, reducing servicing, management requirements, and the attack surface for those server roles. Windows BitLocker Drive Encryption protects data by encrypting the entire Windows volume.

Server Core

Managing Server Core

- CMD for local command execution
- Terminal Server using CMD
- Windows Remote Shell
- WMI
- SNMP
- Task Scheduler for scheduling jobs/tasks
- Event Logging and Event Forwarding
- RPC and DCOM for remote MMC support
- Group Policy to centralize configuration

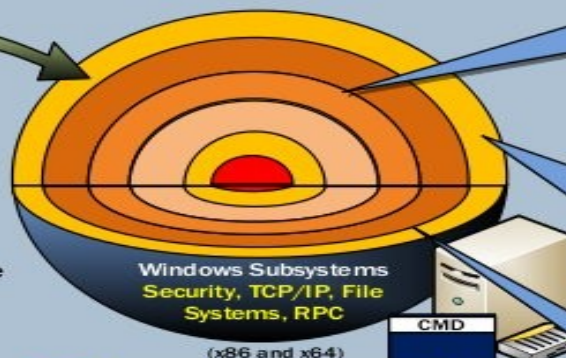


Configuring and Deploying Server Core

- Netdom.exe - join the machine to a domain
- Netsh - configure TCP/IP settings
- SCRegEdit.wsf script - configure Windows Update and enable Remote Desktop
- Slmgr.vbs - Product Activation
- Dcpromo - use unattend installation file
- Ocsetup - add roles/features
- Oclint - list server roles/features



Server Core installation installs only the subset of the binaries required by server roles. Server Core installation requires a clean install.



Command Line interface, no GUI Shell, no Windows Powershell

Server Core Roles:

DHCP, File, Print, AD, AD LDS, Media Services, DNS, and Windows Virtualization Services

Server can run a dedicated role or multiple roles

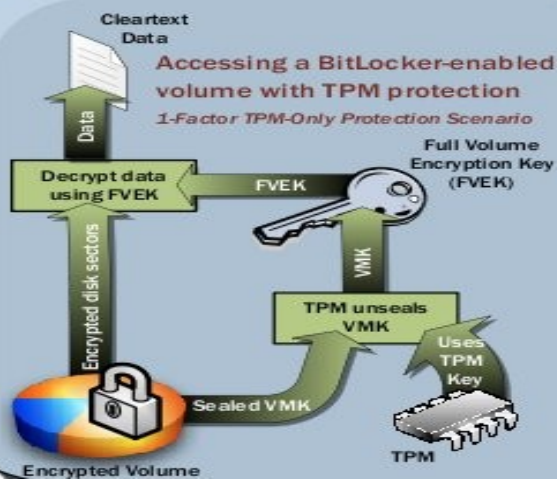
Optional Features:

- WINS & Failover Clustering
- Backup & Removable Storage
- Management & MultiPath IO
- BitLocker Drive Encryption
- SNMP & Telnet Client
- Quality Windows Audio/Video Experience (qWave) Framework

Server Core Functionality Includes:

- IPSec
- Windows File Protection
- Windows Firewall
- Event Log
- Performance Monitor counters

Windows BitLocker Drive Encryption



BitLocker Operational Overview

Windows BitLocker Drive Encryption is a data protection feature that provides enhanced protection against data theft or exposure on computers that are lost or stolen.

Available Authenticators

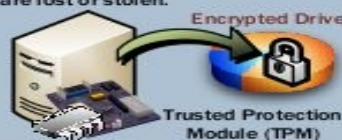
- USB
- TPM
- TPM + Pin
- TPM + USB
- TPM + USB + PIN

USB (without TPM) used for recovery purposes (or non-TPM computers)

BitLocker assists in mitigating unauthorized data access on lost or stolen computers by:

- Encrypting the entire operating system volume on the hard disk
- Checking the integrity of early startup components and startup configuration data

Windows Server 2008 also supports BitLocker encryption of data volumes. BitLocker encrypts data volumes the same way that it encrypts the operating system volume.



BitLocker Disk Configuration

Two partitions are required for BitLocker because pre-startup authentication and system integrity verification must happen outside of the encrypted operating system volume.

- System Partition (green, unencrypted, small, active)
- Windows Operating System Volume (encrypted, blue)

BIOS must support reading USB devices in pre-OS environment

BitLocker Recovery Password Storage

Appropriate recovery password storage is vital since the recovery password is needed if BitLocker locks the drive to prevent tampering.

Domain-Joined Machines

- Use an existing AD DS infrastructure to remotely store BitLocker recovery passwords

Non-Domain-Joined Machines

- Store recovery password on physically secured USB drive
- Store recovery password printout in secured location
- Burn recovery password to CD and store in secured location

Migrating Encrypted Drives

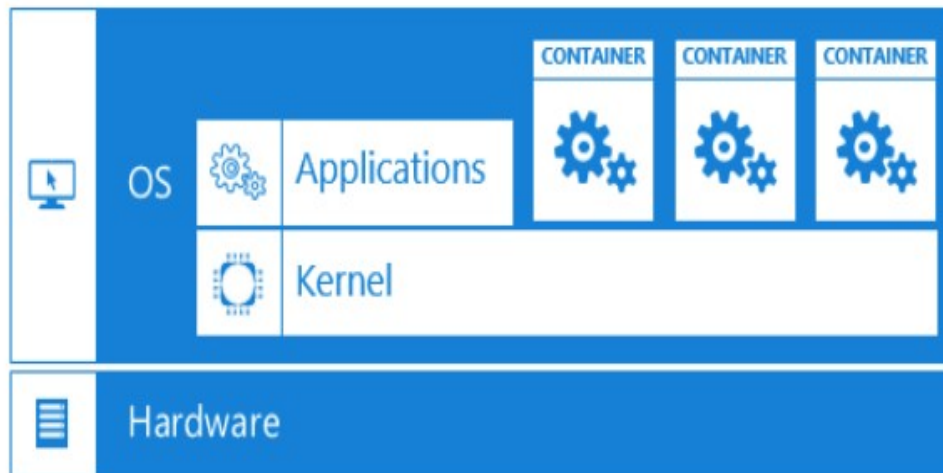
Moving a protected OS volume to another TPM-enabled machine requires using a recovery password from the keyboard or a USB flash drive. VMK must be resealed to the new TPM.

Windows Server 2016 - некоторые ключевые особенности

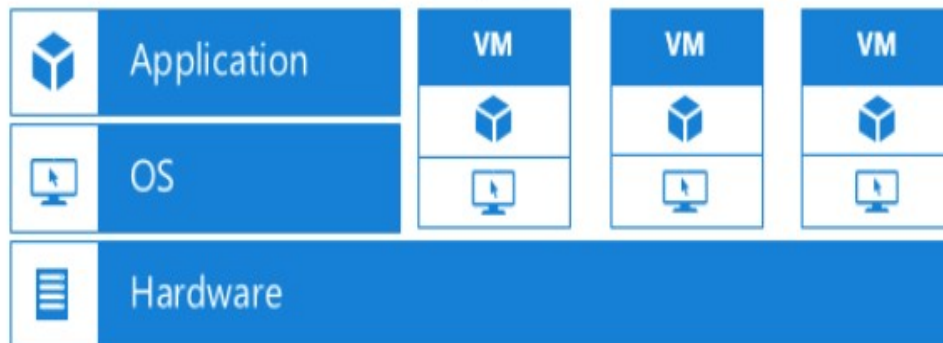
- Механизм обновления ОС хостов кластера без его остановки;
- Синхронная репликация хранилищ на уровне блоков с поддержкой географически распределенных кластеров;
- Виртуальный сетевой контроллер (software-defined networking stack) для одновременного управления физическими и виртуальными сетями;
- Новый формат файлов конфигурации виртуальных машин (.VMCX и .VMRS), с более высокой степенью защиты от сбоев на уровне хранилища. Также предоставляется возможность обновлять версии конфигурационных файлов;
- Создание снапшотов прямо из гостевой ОС;
- Полноценный Storage Quality of Service (QoS) — возможность динамического отслеживания производительности хранилищ и горячая миграция виртуальных машин при превышении этими хранилищами пороговых значений (IOPS).
- Изменения в самом Hyper-V: использование альтернативных аккаунтов, возможность управления предыдущими версиями Hyper-V, обновление и улучшение протокола удалённого управления, возможность безопасной загрузки гостевых ОС Linux;
- Возможность обновления Integration Services через Windows Update.
- «Горячее» добавление сетевых карт, дисков и оперативной памяти.
- Поддержка OpenGL и OpenCL для Remote Desktop.
- Два типа контейнеров: Windows Server Containers и Hyper-V Containers. Контейнеры Windows Server обеспечивают изоляцию через пространство имен и изоляцию процессов. Контейнеры Hyper-V отличаются более надежной изоляцией благодаря их запуску в виртуальной машине
- Вариант установки - nano Server — удалённо управляемая ОС, оптимизированная для частных облаков и ЦОД.

Контейнеры Windows

Контейнеры = виртуализация на уровне операционной системы

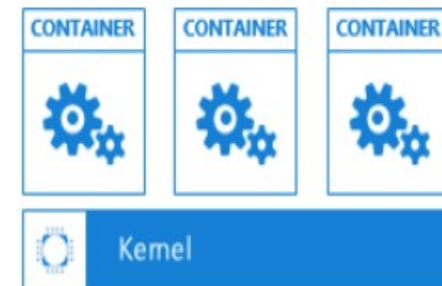


Традиционные виртуальные машины = аппаратная виртуализация



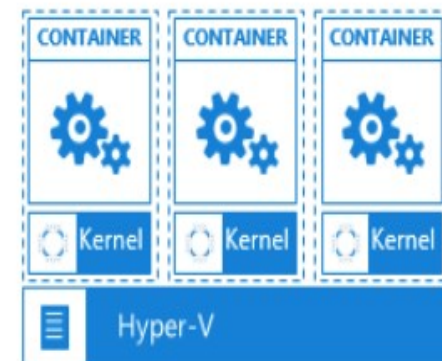
Контейнеры Windows Server

Максимальная скорость и плотность



Контейнеры Hyper-V

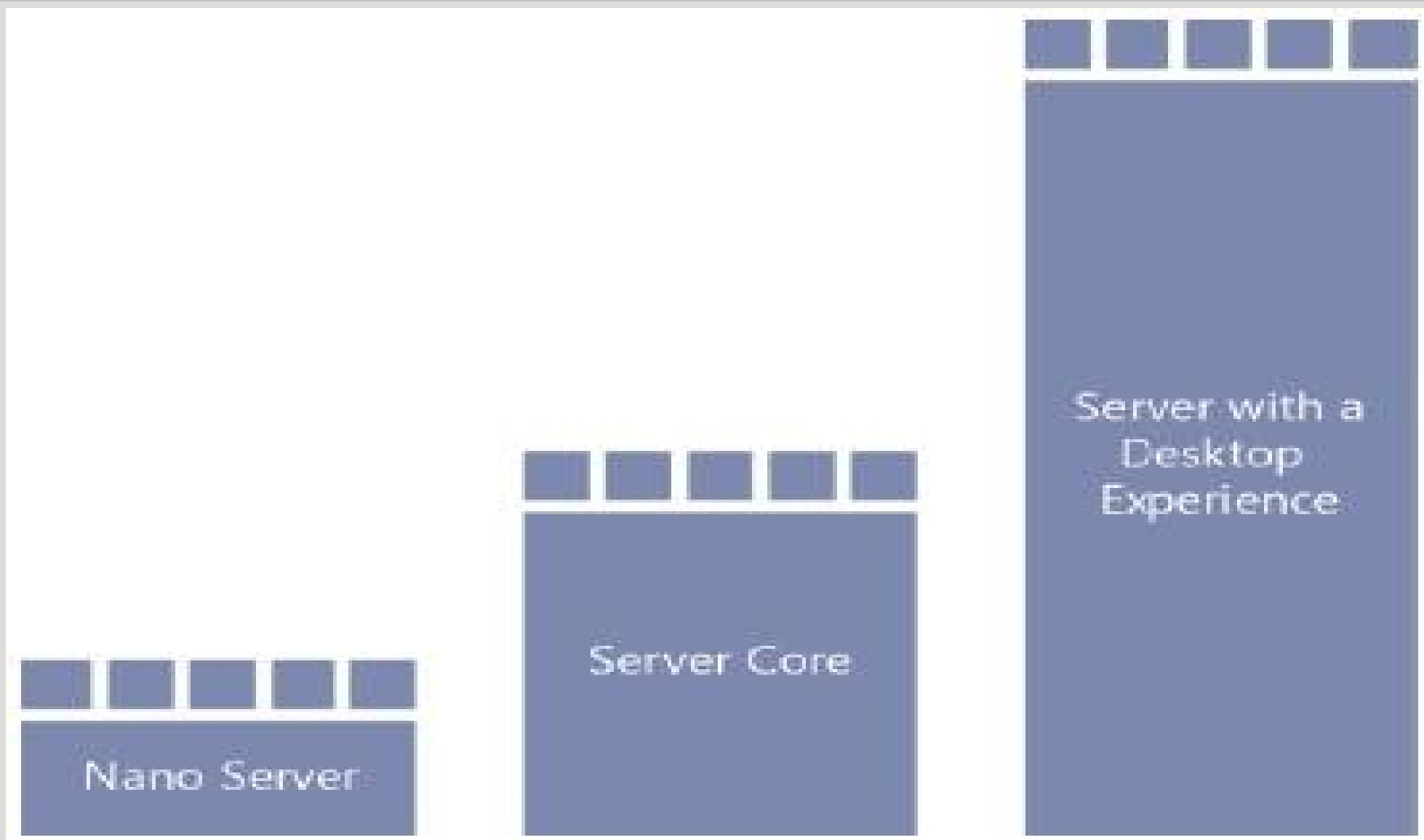
Изоляция и производительность



Windows Server2016 - nano server

- Nano Server — урезанная версия Windows Server, без пользовательского интерфейса
- у Nano Server полностью отсутствует монитор, то есть графический интерфейс
- Nano потребляет значительно меньше ресурсов, чем Windows Server, и Windows Server Core
- У Nano нет графического пользовательского интерфейса и, в отличие от Windows Server Core, также нет ни командной строки, ни консоли PowerShell. Более того, Nano Server не предполагает локальной регистрации. Он предназначен исключительно для поддержки служб и сервисов
- Традиционные приложения Windows с графическим интерфейсом запускать под Nano Server нельзя. Он предназначен для обеспечения работы служб инфраструктуры
- Nano Server предназначен для двух сценариев, а именно для поддержки служб инфраструктуры Server Cloud, таких как Hyper-V, кластер с Hyper-V и масштабируемый файловый сервер (SOFs), а также созданных в «облаке» приложений, запущенных на виртуальных машинах, в контейнерах либо на платформах разработки, для которых не требуется пользовательский интерфейс на сервере. Nano Server поддерживает ряд сред исполнения, включая C#, Java, Node.js и Python. Nano Server по API совместим с Windows Server внутри подмножества компонентов, предусмотренных для Nano
- Помимо отказа от графического пользовательского интерфейса и командных оболочек, исключена поддержка 32-разрядных приложений (компонент WOW64), установщика MSI и многих стандартных компонентов Server Core
- Управление Nano осуществляется дистанционно с помощью WMI и PowerShell

Архитектура установки Windows сервера



Windows Server 2016 - особенности Hyper-V

- Клиент Hyper-V поддерживает Windows 10;
- Назначение дискретного устройства («проброс» устройств в виртуальную машину);
- Мониторинг чрезмерной активности виртуальных машин с целью экономии ресурсов (RCT);
- Использование альтернативных учетных данных при подключении к другой системе Windows Server 2016;
- Обновленный протокол управления - теперь вся коммуникация с удаленными хостами идет по протоколу WS-MAN, который предоставляет функции аутентификации CredSSP, Kerberos или NTLM;
- Управление старыми версиями - в Hyper-V Manager для Windows Server 2016 и Windows 10 можно управлять платформой Hyper-V в ОС Windows Server 2012, Windows 8, Windows Server 2012 R2 и Windows 8.1;
- Linux Secure Boot (безопасная загрузка Linux) - т.е. безопасная загрузка, для гостевых операционных систем Linux (Ubuntu 14.04 и более поздние версии, Red Hat Enterprise Linux 7.0 и выше, и CentOS 7.0 и выше). Данная опция защищает виртуальную машину от атак rootkit и других вредоносных программ, активируемых при загрузке системы. Ранее данная опция была доступна только для Windows 8/8.1 и Windows Server 2012;
- Вложенная виртуализация - функция позволяет использовать виртуальную машину в качестве узла Hyper-V и создании виртуальных машин в рамках этого виртуализированного узла;