1. Основная часть
   1. Windows Server

Это серверная операционная система от Microsoft, являющаяся частью семейства Windows NT. Операционная система была анонсирована 20 марта 2018 года, и в тот же день была выпущена первая сборка по программе Windows Insider. Выход финальной версии состоялся 2 октября 2018 года. Изначально планировалось выпустить Windows Server 2016 R2. Microsoft анонсировала опции для пользователя при инсталляции: Desktop (c GUI) и Server Core (для удаленной поддержки). Среди ключевых новых функций: более глубокая поддержка виртуальных машин, включая виртуальные машины на Linux, интерфейс от Windows 10 (сборка 1809) и улучшенный Windows Defender.

Возможности:

* Подсистема Windows для Linux.
* Поддержка Kubernetes.
* Функции графического интерфейса пользователя из Windows 10 1809 сборки.
* Storage Spaces Direct.
* Storage Migration Service.
* Storage Replica.
* System Insights.
* Обновлённый Защитник Windows.
* Вложенная виртуализация в Hyper-V Windows Admin Center (WAC).
* Гибридное облако

1. Безопасность Microsoft Windows Server 2016

Windows Server 2016 — это оптимизированная под облако операционная система с новыми возможностями защиты доступа и информации и с инновационными технологиями, созданными на основе Azure для приложений и инфраструктуры организаций.

* Дополнительныее уровни безопасности в областях применения серверов: центры обработки данных, виртуальные машины и хостинг-среда.
* Взаимодействие с системами безопасности Windows 10 и Azure для обеспечения защиты различных устройств, рабочих сред, сетевой инфраструктуры и приложений.

Информационная безопасность в наше время считается основным приоритетом для ИТ. Причина такой ситуации в острой публичной критике крупных компаний и государственных учреждений за неспособность защитить от взлома БД, Системный софт, данные клиентов и сотрудников, личную информацию.

Злоумышленникам удается с помощью легко доступных инструментов для проникновения получить доступ в сеть крупных организаций и оставаться незамеченными длительный период времени для планирования атаки на инфраструктуру с целью похищения секретных данных с целью шантажа и вымогательств. Windows Server 2016 (в отличии от предыдущей версии P73-06285 WinSvrStd 2012R2 SNGL OLP NL 2Proc ) обеспечивает новые уровни защиты, которые помогают нейтрализовать подобные угрозы, так как сервер становится активным компонентом защиты безопасности. Такие средства защиты безопасности были разработаны с идеей противодействия общей угрозе продолжающихся атак внутри среды центра обработки данных в зависимости от сопротивления угрозам и усовершенствованные функции обнаружения рисков для управления привилегированной учетной записью и защиты виртуальных машин от потенциально опасных сред.

Если хакеры воспользовались методом фишинга или скомпроментированными учетными данными для получения быстрого доступа к управлению системой администраторам потребуется до 2 суток на устранение последствий инцидента.

С таким подходом, привилегированная идентичность является новой границей зоны безопасности и существует необходимость защиты и мониторинга привилегированного доступа. Использование Just In Time управления позволяет назначать, контролировать и ограничивать отрезок времени, в который пользователи получают права администратора и прочие ограничения возможностей для операций на сервере. Даже если злоумышленник проник на сервер, Credential Guard предотвращает получение учетных данных, которые могут быть использованы для атак на другие системы.

Когда злоумышленник получает доступ к вашей среде, запуск приложений и инфраструктуры на Windows Server 2016 обеспечивают уровни защиты от внутренних атак с использованием технологий сопротивления угрозы, таких как: Control Flow Guard блокировка общего направления атак, целостности кода, чтобы контролировать то, что может запускаться на сервер и встроенный Защитник Windows для обнаружения, защиты и оповещении о вредоносных программах. Кроме того, для более эффективного выявления угроз, Windows Server 2016 включает в себя расширенный аудита безопасности, который может помочь для выявления угроз безопасности и расследования инцидентов в сети.

Виртуализация также является еще одной важной областью, в которой требовалось обновить подход. Хотя есть защита от виртуальной машины атакующего хоста или другие виртуальные машины, нет никакой защиты от взлома хоста и нападения на виртуальные машины, работающие на нем. На самом деле, так как виртуальная машина - это просто файл, он не защищён при хранении, доступе из сети, резервном копировании. Это фундаментальная проблема сегодня присутствует на каждой платформе виртуализации является ли это Hyper-V, VMware или любой другой гипервизор. Получается, что если виртуальная машина скопирована (либо злонамеренно или случайно), то она может быть запущена в любой другой системе.

1.3 ОС серверы

FreeBSD – одна из самых старых ОС с богатой историей. Но с каждым годом количество пользователей этой системой сокращается, хотя она считается одной из числа надежных и безопасных ОС. Есть несколько причин падений популярности данной ОС, главная из них – одна команда разработчиков и совсем небольшое количество коммерческого ПО для FreeBSD. Если у Вас возникнет проблема с FreeBSD, она с большой вероятностью может остаться нерешенной. На данный момент выпущена 10 версия FreeBSD, которая успешно работает на множестве процессорных архитектур и в руках мастера дает возможность для тонкой настройки ядра. В преимущества FreeBSD нужно внести отменную реализацию работы с памятью, сетью и системой ввода-вывода.

Windows Server (на примере Windows Server 2008 R2) – система практична и имеет большой запас производительности. Наилучшее решение для сервера файлов или терминала, имеет инструмент для бэкапов, что значительно повышает надежность. Главным недостатком нужно выделить требовательность к аппаратной части. Windows Server 2008 R2 уже не поддерживает 32-х разрядную архитектуру, да и в целом требует для работы существенно больше ресурсов, чем его аналоги. Важная особенность, ОС требует покупку лицензии. Стоить не забывать о том, что именно на Windows ориентировано огромное количество существующих вирусных программ. В большинстве случаев этот продукт используют для “домашнего” тестирования сайта, для подключения удаленного рабочего стола или при использовании IIS и ASP. HyperHost предлагает VDS с ОС Windows, включая бесплатную лицензию на 180 дней (trial period).

CentOS – бесплатный аналог Red Hat, который пользуется немалой популярностью. Число пользователей этой ОС огромное, что позволяет оперативно решать все возникшие проблемы и баги. Преимущество – наличие множества форумов, где Вам смогут помочь с вопросами о CentOS. К значительным плюсам Centos можно также отнести очень удобный и шустрый менеджер пакетов yum, а минусом считают наличие не самых последних версий сопутствующего программного обеспечения в стандартных хранилищах (репозиториях) пакетов для Centos. Данная ОС поддерживает практически все панели управления хостингом.

Debian – дистрибутив Linux, который имеет множество поклонников и активно развивается. Данная ОС универсальна и применяется на серверах и рядовых рабочих машинах. Debian – отличное решение для сервера, который должен стабильно и бесперебойно работать. Излишняя консервативность ОС – главный недостаток, так как разработчики редко радуют новыми релизами.

Red Hat Enterprise Linux – одна из самых популярных и востребованных ОС. В основном система предназначена для корпоративного использования, и отличается особой надежностью и безопасностью. Доказательство этому то, что данную ОС используют для развертывания важных приложений на мировых биржах, в финансовых учреждениях, ведущих телекоммуникационных компаниях, анимационных студиях и тп. Основной недостаток – ОС платная. Главная особенность – есть коммерческая поддержка дистрибутива. Периодичность выхода новых версий – 3 года.

Дистрибутив Ubuntu был создан с целью стать удобной и понятной ОС (на основе Linux) для рядового пользователя. И вправду, установить и настроить данную ОС просто. Кроме того, в Сети существует большое количество инструкций и советов по пользованию системой для новичков. По официальным данным дистрибутивом Ubuntu пользуются более 20 млн. пользователей.

Главные особенности дистрибутива Ubuntu:

* Стабильность работы – систему часто используют на высоко нагруженных серверах. ОС не требует частых перезагрузок компьютера, даже в случаи обновлений, установки или удаления программ.
* Безопасная система, которая не требует антивирусов. Чтобы подцепить вирус необходимо очень постараться, если Вы используете дистрибутив Ubuntu.
* Бесплатная ОС – установка происходит в несколько кликов, в сети полно версий для бесплатного скачивания, не нужно вводить никаких ключей, можно использовать на множестве компьютеров одновременно.
* Приятный и понятный интерфейс – большое количество бесплатных тем и графических эффектов, на любой вкус и цвет.
* Быстрая установка без усилий – с появлением новых версий установка Ubuntu все упрощается, чем привлекает неопытных пользователей. Основное ПО и драйвера устанавливаются сразу и практически автоматично, в итоге вы получаете готовую к работе ОС. Кроме того, предлагается автоматическое обновление.
* Идеальный вариант для новичков – все настройки и установки выполняются на интуитивно понятном уровне. Через специализированный менеджер пакетов Synaptic выполняется установка необходимых программ. У него есть функции просмотра рейтинга, описания и отзывов о программах.
* Стабильность работы обеспечивается огромной командой поддержки, которая быстро находит и устраняет ошибки.
* Предсказуемость системы – каждый новый релиз выходит с периодичностью в 6 месяцев, пользователи всегда имеют доступ к свежим версиям ОС.
* Отлично уживается на одном ПК с другими ОС, например, Windows.

1.4 Биос

BIOS —Basic Input-Output system. Это программа низкого уровня, хранящаяся на чипе материнской платы компьютера. BIOS загружается при включении компьютера, отвечает за пробуждение его аппаратных компонентов, убеждается в том, что они правильно работают, а потом запускает программу-загрузчик, запускающую операционную систему.

Перед загрузкой ОС, BIOS проходит через POST (Power-On, Self-Test) - самотестирование после включения. Она проверяет корректность настройки аппаратного обеспечения и его работоспособность. Если что-то не так, на экране вы увидите серию сообщений об ошибках или услышите из системного блока загадочный писк. Что именно означают звуковые сигналы описано в инструкции к компьютеру.

При загрузке компьютера по окончанию POST BIOS ищет Master Boot Record, или MBR — главную загрузочную запись. Она хранится на загрузочном устройстве и используется для запуска загрузчика ОС. При запуске компьютера процессор считывает код BIOS из ПЗУ, записывает его в ОЗУ и передаёт управление коду BIOS. В дальнейшем загрузчик ищет и загружает в память код операционной системы и передаёт ему управление.

Следует выделить три основных разновидности БИОСА:

* AWARD
* AMI
* UEFI

AWARD - является лидером в данной области. В далеком 1998 году, фирма Award Software была куплена компанией Phoenix, но до сих пор БИОС маркируют как Award. Традиционно оболочка базовой системы синий (серый) фон с английскими пунктами меню. Интерфейс в разных версиях отличается.

AMI - занимает почетное второе место. Является собственностью компании American Megatrends Incorporated, откуда и вытекает аббревиатура AMI. По всем параметрам заметна схожесть с AWARD BIOS. Совпадают названия и расположение основных разделов, но не всегда. Наличие или отсутствие опций БИОСА в первую очередь зависит от производителя материнской платы и ее функций. Поэтому нельзя однозначно выделить конкретные особенности AMI. Так же в разных версиях различные интерфейсы.

UEFI - третий вид БИОСА является по-настоящему современной технологией. Обладает графическим интерфейсом, чем-то даже напоминает операционную систему. Имеет большое преимущество над старыми типами. Как известно, традиционный БИОС, в силу своих функциональных ограничений способен увидеть не более 2-х ТБ. UEFI ломает пределы, так как ограничений по объему практически нет.