БЕЗОПАСНОСТЬ ЧАСТНОГО ОБЛАКА НА ОСНОВЕ ТЕХНОЛОГИЙ MICROSOFT

Бешков Андрей
Руководитель программы информационной безопасности
Microsoft
abeshkov@microsoft.com
http://twitter.com/abeshkov

О чем будем говорить?

- **Основные проблемы безопасности частных облаков**
- **Построение безопасного частного облака**
- **Новинки ИБ в Windows Server 2012**

Что такое облака?

Более 400 облачных сервисов Microsoft

Windows Live

1.4 миллиард Live IDs

Hotmail

350 миллионов активных пользователей

msn

Более 500 миллионов уникальных пользователей ежемесячно

Microsoft Advertising

14 миллиардов рекламных показов ежемесячно

Windows Live Essentials

Microsoft SkyDrive

bing

Более 5.5 миллиардов запросов ежемесячно

Microsoft Forefront

4 миллиарда писем ежедневно

Microsoft Office 365

Windows Live Messenger

5.0 миллиардов сообщений в день

XBOX LIVE

25 миллионов активных пользователей

Как Microsoft видит частное обла

Частное облако предоставляет ОС и набор **виртуализованных разделяемых ресурсов**

В центре внимания приложения. Наборы ресурсов создаваемые автоматически отходят на второй план

Наборы ресурсов создаются на основе бизнес правил с помощью ПО автоматизации

Вы не думаете об инфраструктуре в терминах количества вирт. машин и уровне консолидации, ОЗУ или хранилища. Думаете о размере вычислительной мощности доступной потребителю

Характеристики:

- Самообслуживание арендаторов
- Оплата за потребляемые ресурсы
- Автоматическое развертывание, управление и мониторинг
- Интерфейс мониторинга и отчетности доступный арендаторам

Основные проблемы безопасности

- Безопасность названа главнейшим препятствием на пути к применению облаков

- Основные проблемы:
  - *Изоляция арендаторов друг от друга и инфраструктуры облака на уровне вычислительных ресурсов, хранилища, сети*
  - *Аутентификация / Авторизация / Аудит доступа к облачным ресурсам и физической инфраструктуре*
  - *Влияние на КЦД сервисов или данных с помощью уязвимостей в ПО или зловредного кода*
  - *Неавторизованный доступ или DoS атаки из-за неправильной настройки*

КЦД = Конфиденциальность, Целостность и Доступность

Источник: IDC Enterprise Panel, August 2008

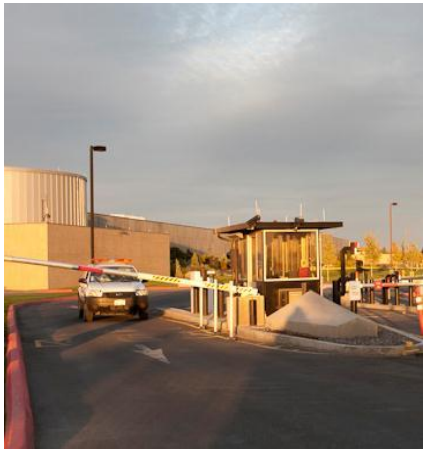
Безопасность ЦОД GFS Microsoft

Физическая безопасность мирового уровня

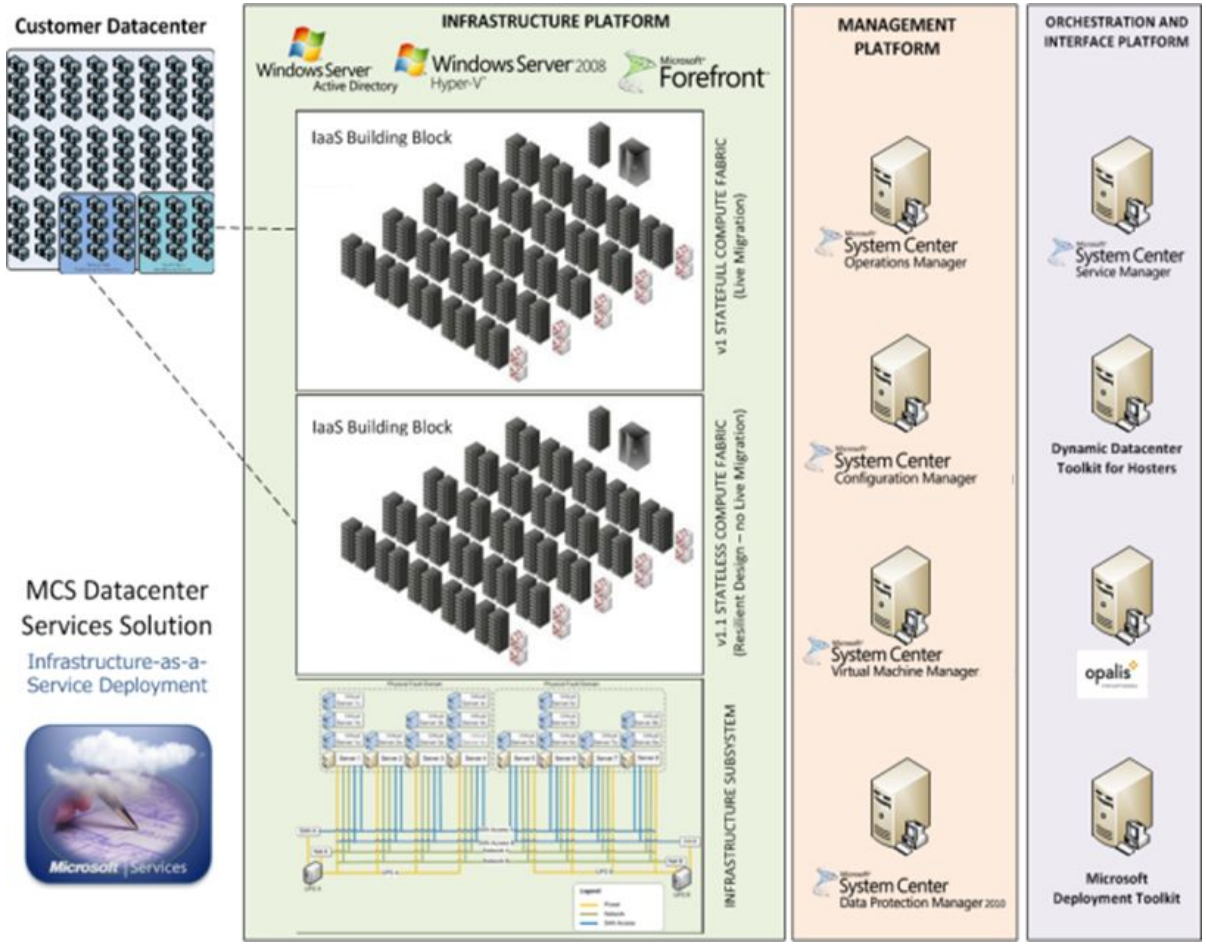
- Ограниченный доступ 24x7
- Системы контроля доступа
- Видео-наблюдение
- Датчики движения
- Сигнализация событий нарушения безопасности

Международная сертификация

- Сертификация системы управления безопасностью ISO/IEC 27001:2005
- Ежегодная аттестация SAS-70 Type II
- Разрешение эксплуатации по FISMA

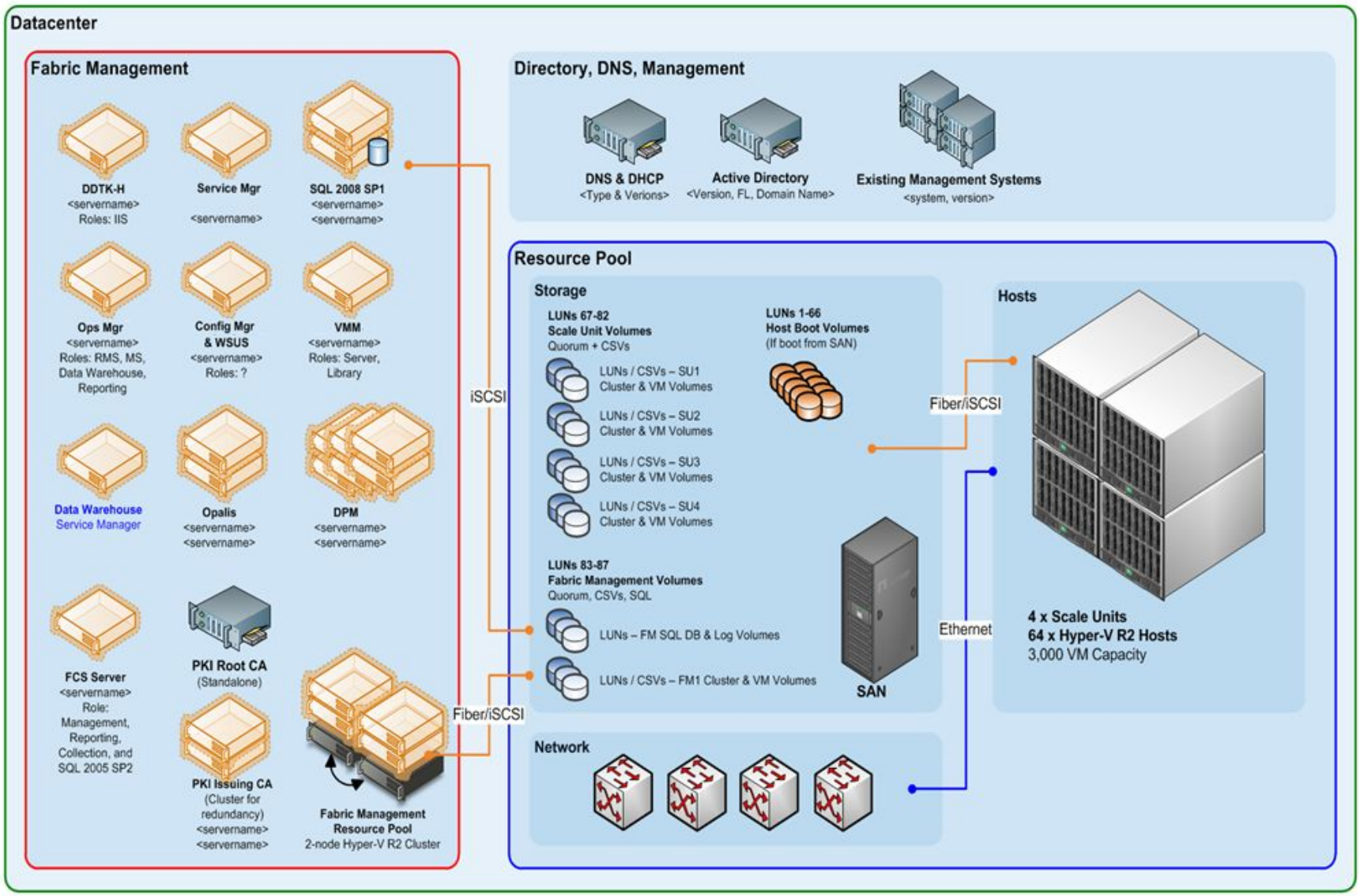


Типовое решение облака IaaS

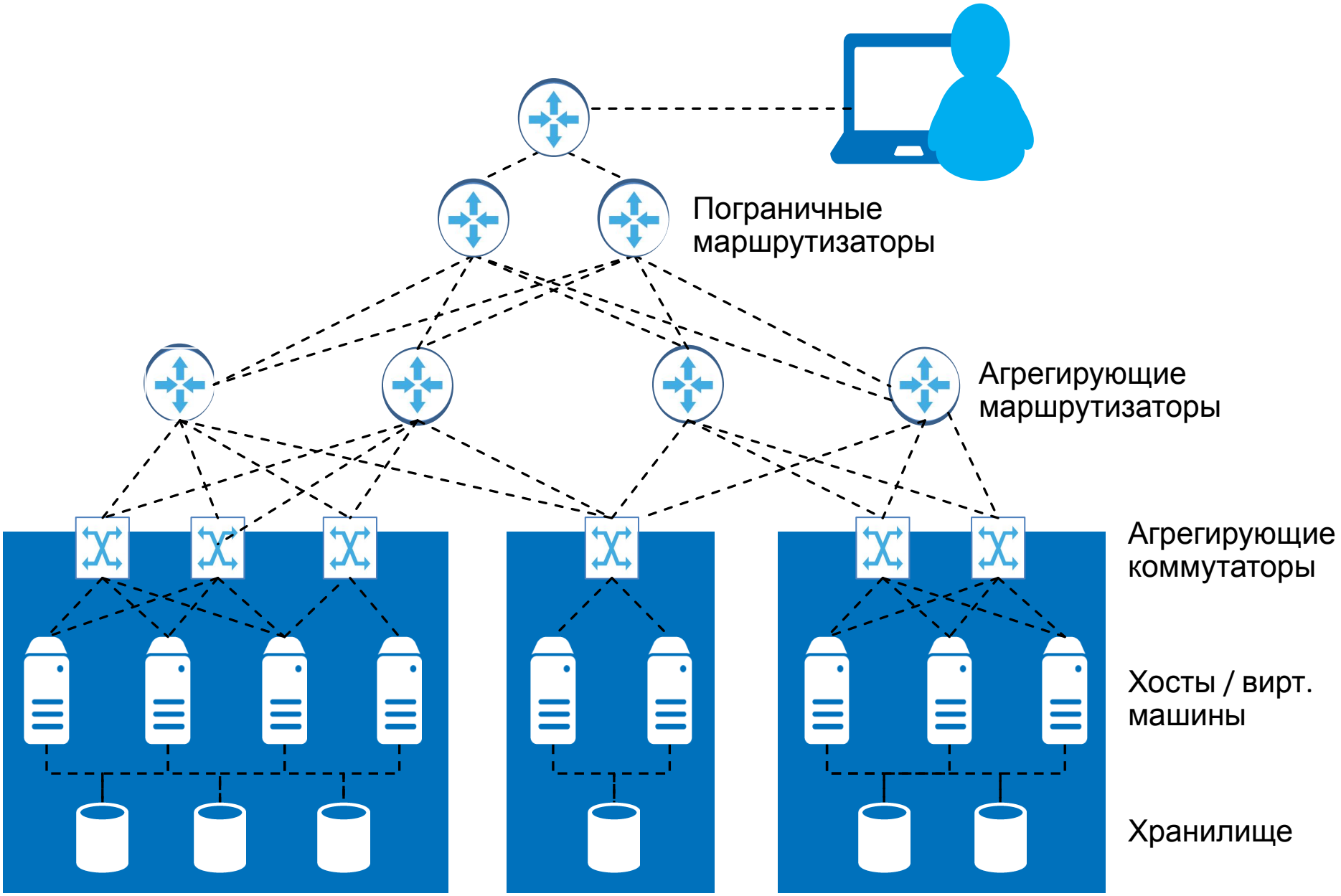


- Автоматическое развертывание вирт. машин
- Раздельное администрирование для арендаторов инфраструктуры
- Автоматическое развертывание юнитов масштабирования (кластерами до 16 узлов)
- Обновление хостов и вирт. машин без прерывания сервиса
- Мониторинг инфраструктуры и автоматические корректирующие действия

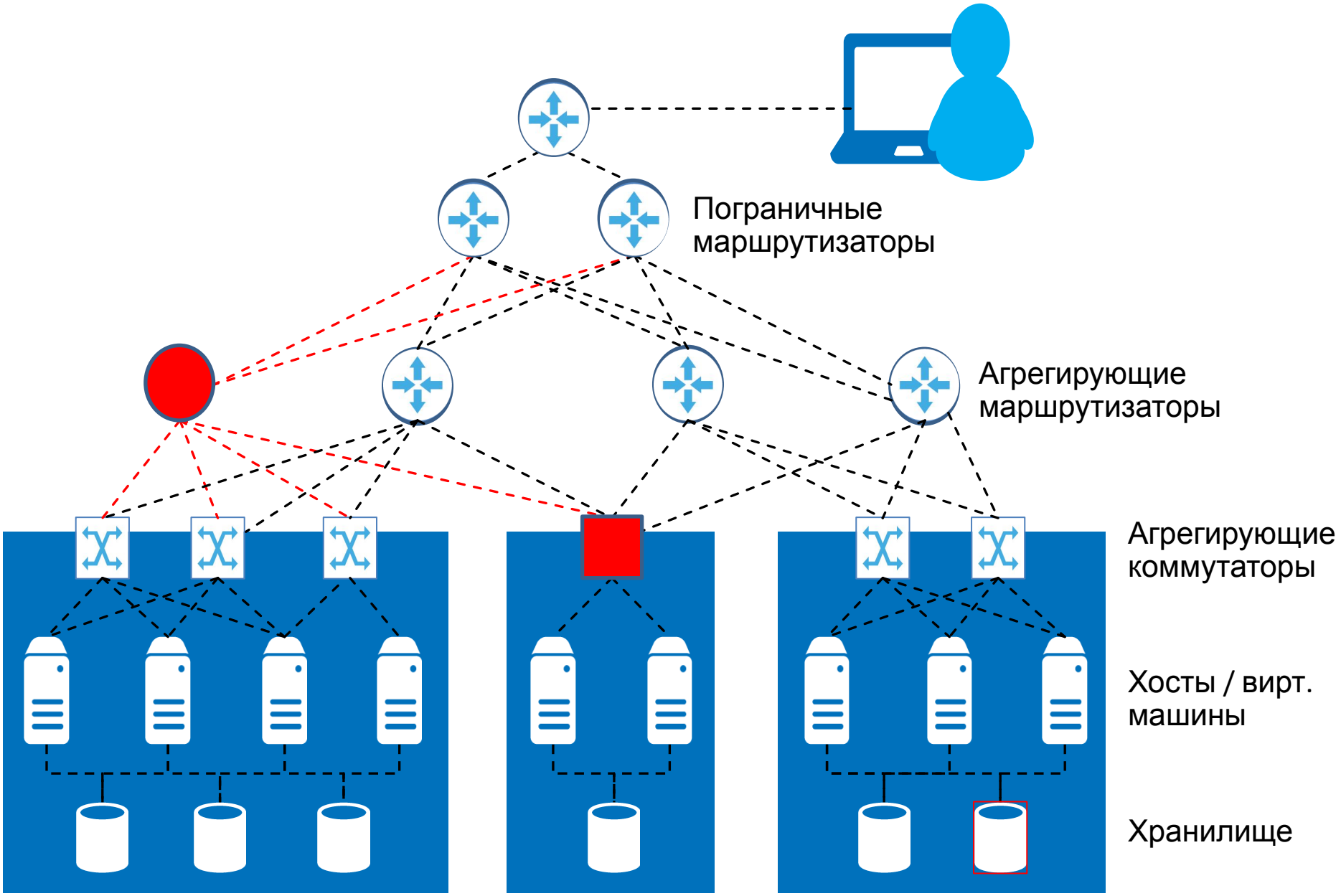
Логическая архитектура облака



Отказоустойчивость и Fault Domain



Отказоустойчивость и Fault Domain



Стек безопасности технологий Microsoft

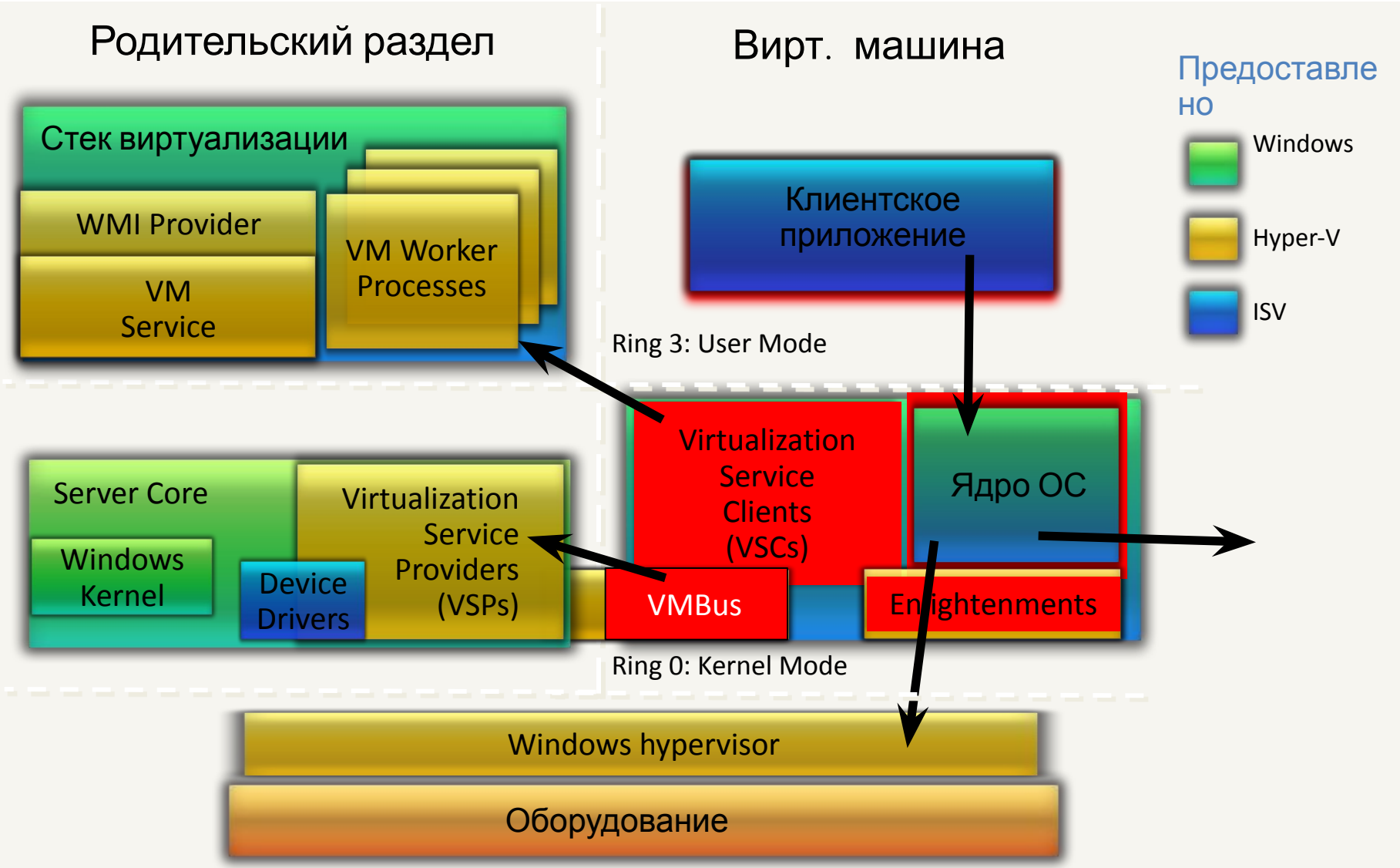
Управляемая инфраструктура ключ к безопасности

Уязвимости ТОП 20 производителей ПО

#	Vendor	History 2006-11	2011 CVEs	Risk	Trend 5yr		1yr	
1	Novell		1,113		+81%	▲	+32%	▲
2	Red Hat		982		+45%	▲	-5%	▼
3	Canonical		625		+48%	▲	+9%	▲
4	Debian		563		+15%	▲	+33%	▲
5	Gentoo		523		+28%	▲	+154%	▲
6	Oracle		497		+27%	▲	+34%	▲
7	Apple		360		+12%	▲	-17%	▼
8	Google		324		+800%	▲	+116%	▲
9	Microsoft		231		+17%	▲	-20%	▼
10	VMware		205		+193%	▲	+63%	▲
11	IBM		192		+21%	▲	-19%	▼
12	Adobe		179		+106%	▲	-16%	▼
13	HP		175		+9%	▲	-34%	▼
14	Cisco		135		+41%	▲	+7%	▲
15	Mozilla		117		+26%	▲	+2%	▲
16	Kernel		81		+8%	▲	-21%	▼
17	Apache		45		+88%	▲	+18%	▲
18	Xerox		43		+330%	▲	+2050%	▲
19	Attachmate		41		+583%	▲	+273%	▲
20	Opera		41		+116%	▲	+28%	▲

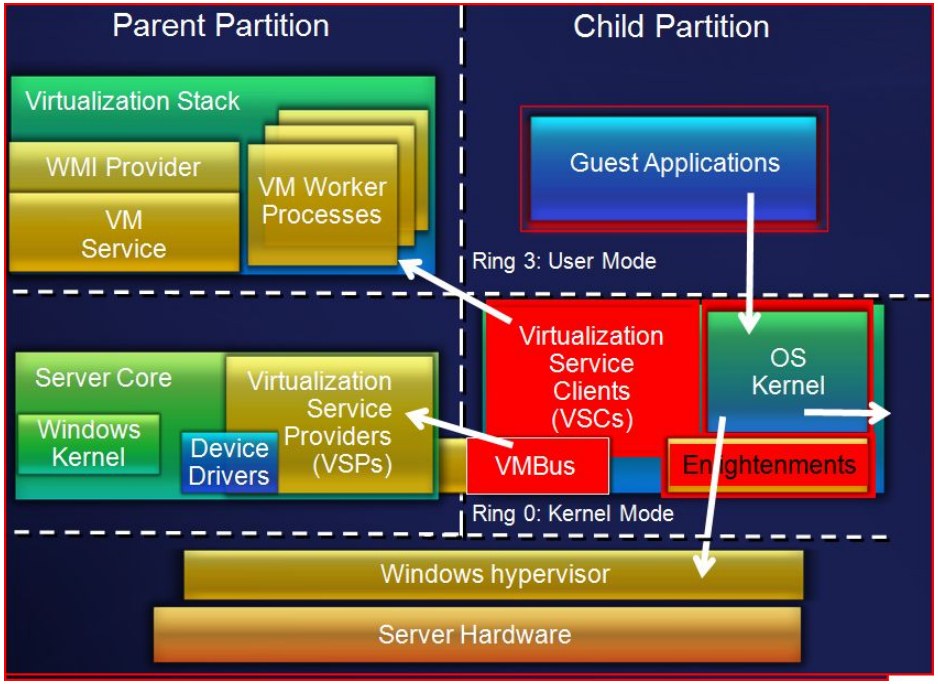
Источник Secunia 2011 yearly

Атаки на стек виртуализации

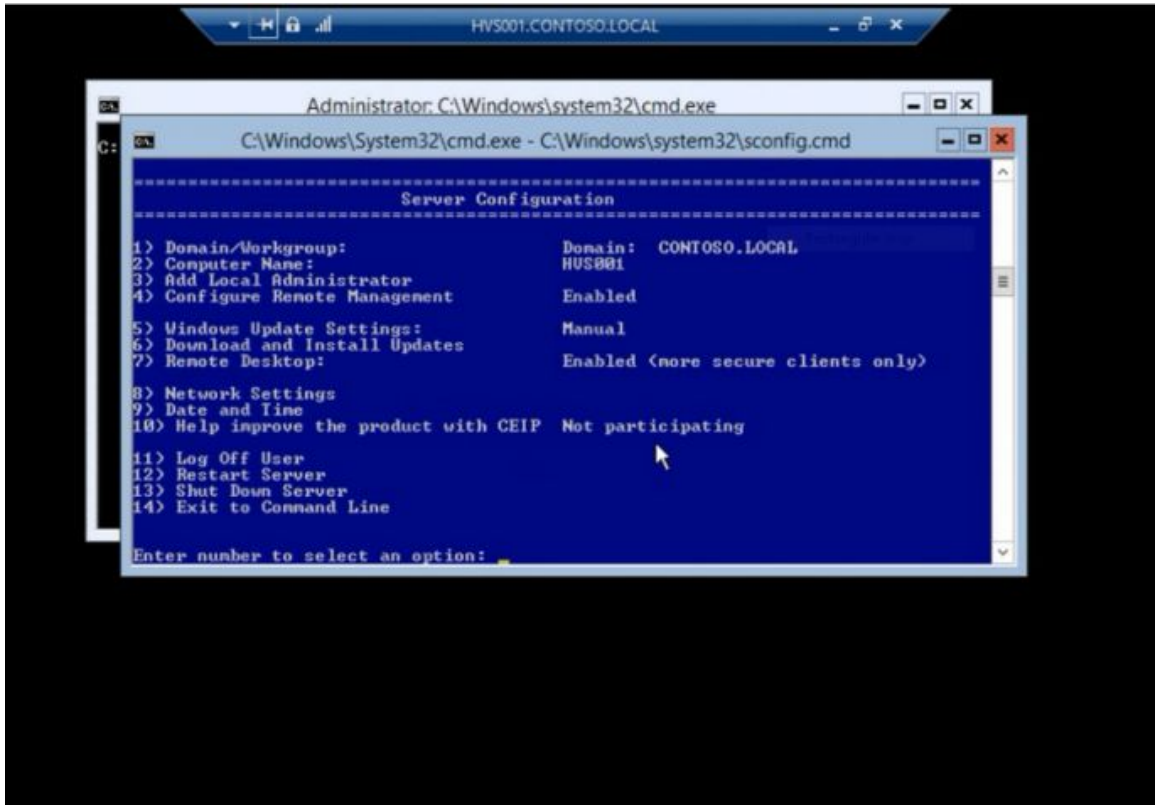


Защита стека виртуализации

- Каждая ВМ получает свой собственный ресурс ОЗУ, дисков, ЦПУ, сетей
- Отдельный процесс обслуживания для каждой ВМ
- Изолированные каналы взаимодействия ВМ и родительского процесса
- ВМ не может влиять на другие ВМ, родительский раздел и гипервизор
- Взаимодействие ВМ только через родительский раздел



Server core лучший выбор

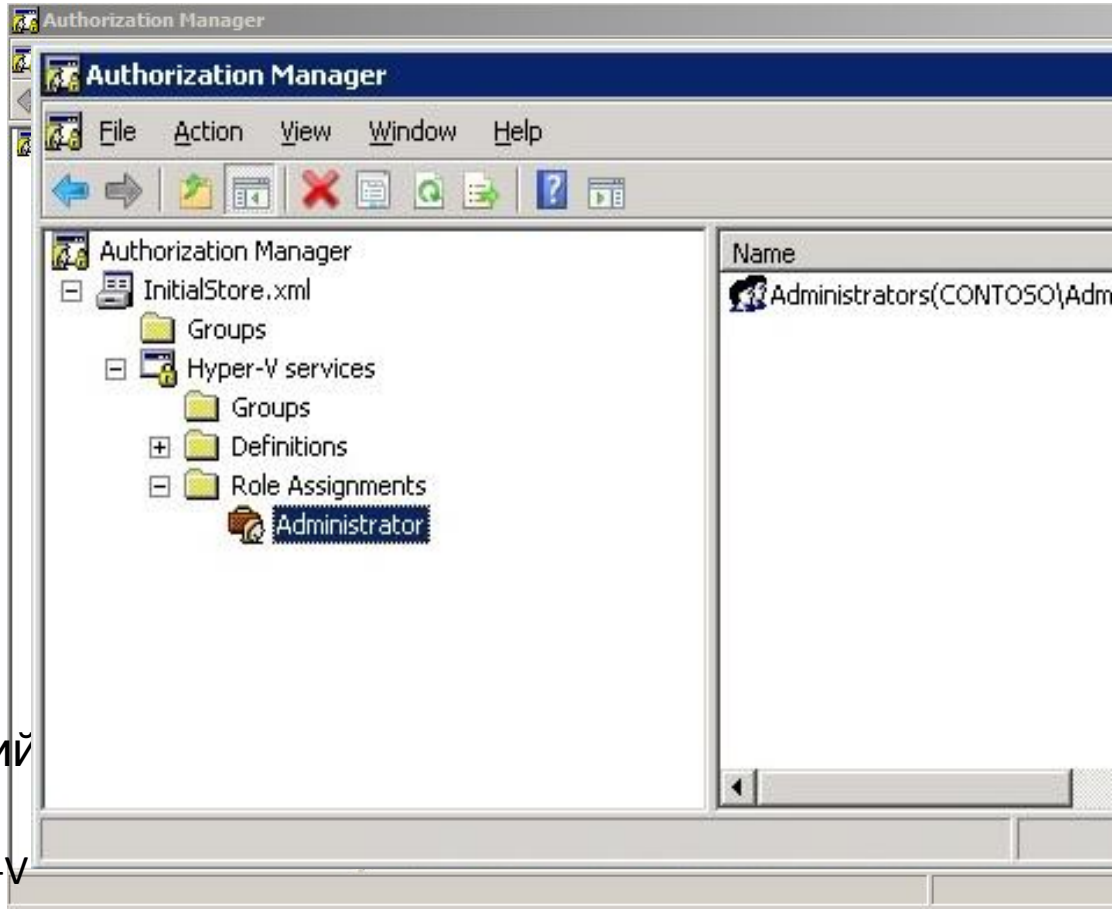


- Server core уменьшает поверхность атаки
- ~50% меньше обновлений и рестартов

Hyper-V Authorization Manager

Единая система авторизации и идентификации

- Ролевое управление группами хостов и ВМ
- Привязка ролей и групп к AD



- Рекомендуется создавать дополнительные роли
  - Комбинация из 33-х операций для каждой роли
    - Обслуживание хоста Hyper-V
    - Обслуживанием сетей Hyper-V
    - Обслуживание ВМ Hyper-V

Virtual Machine Manager

Единая система авторизации и идентификации

Роли:

- Administrator

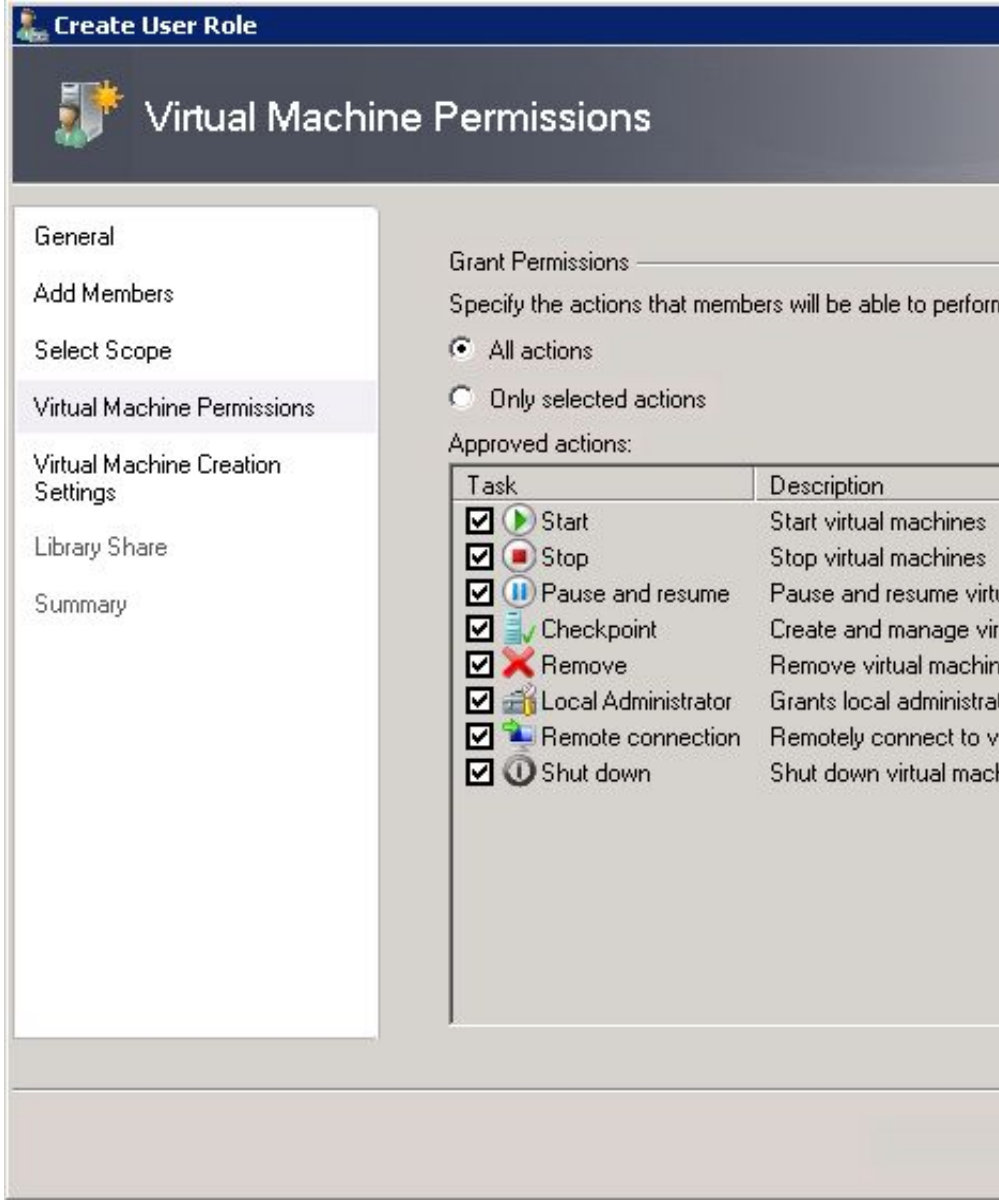
  Полный доступ ко всем хостам, ВМ и серверам библиотек ВМ.

- Delegated Administrator

  Административный доступ к группе хостов и серверов библиотек

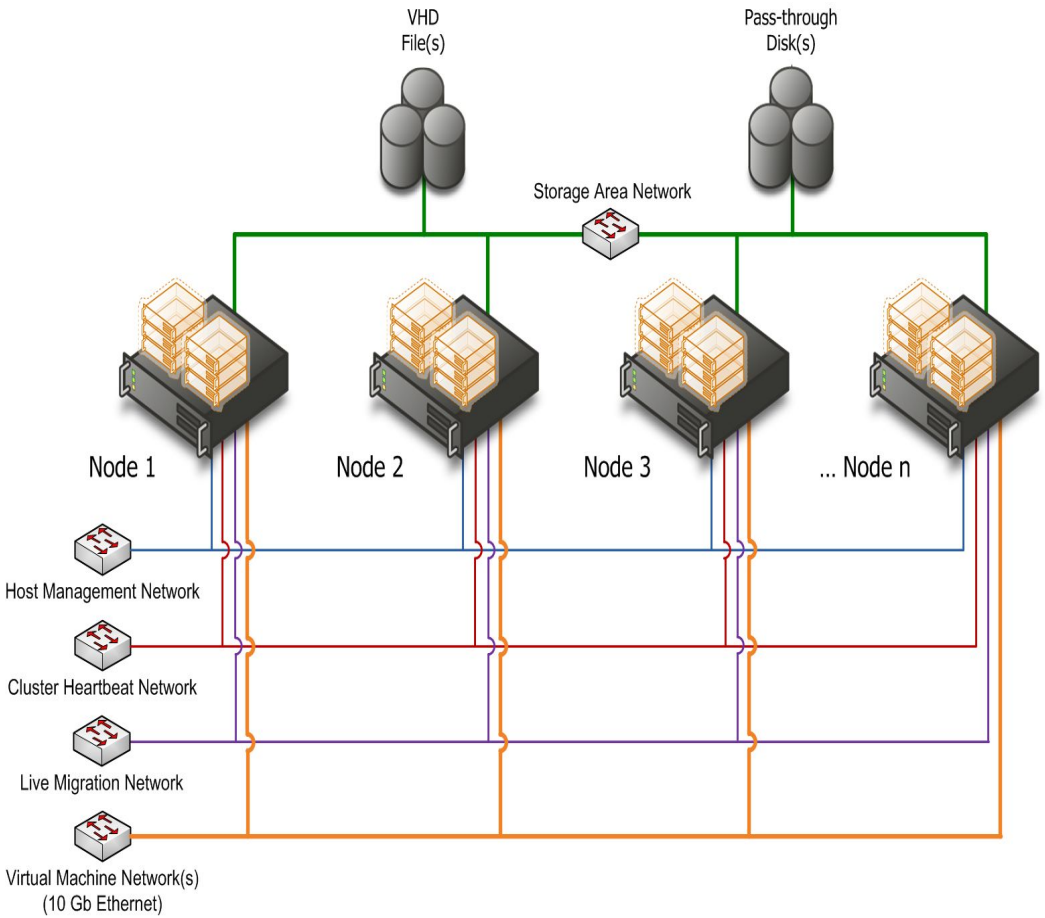
- Self-Service User

  Административный доступ к ограниченному набору ВМ через веб интерфейс портала самообслуживания



Изоляция сетевого траффика

- Только базовые возможности виртуального коммутатора
- Сегментация сети хоста и ВМ с помощью VLAN 802.1Q
- Раздельные физические сетевые адаптеры на хосте Hyper-V
  - Фильтрация трафика между VLAN с помощью межсетевого экрана



Защита сети в Hyper-V

Новые возможности виртуального коммутатора Windows Server 2012

- PVLAN
- Защита от ARP/ND Spoofing
- Защита от подложного DHCP
- Разграничение доступа к портам виртуального коммутатора с помощью Virtual Port ACLs
- Trunk Mode для виртуальных машин
- Мониторинг и проверка траффика портов вирт. Коммутатора

Партнерские расширения

- Cisco: Nexus 1000V & UCS Virtual Machine Fabric Extender (VM-FEX)
- NEC: OpenFlow
- 5nine: Virtual Firewall 3.0
- InMon: sFlow

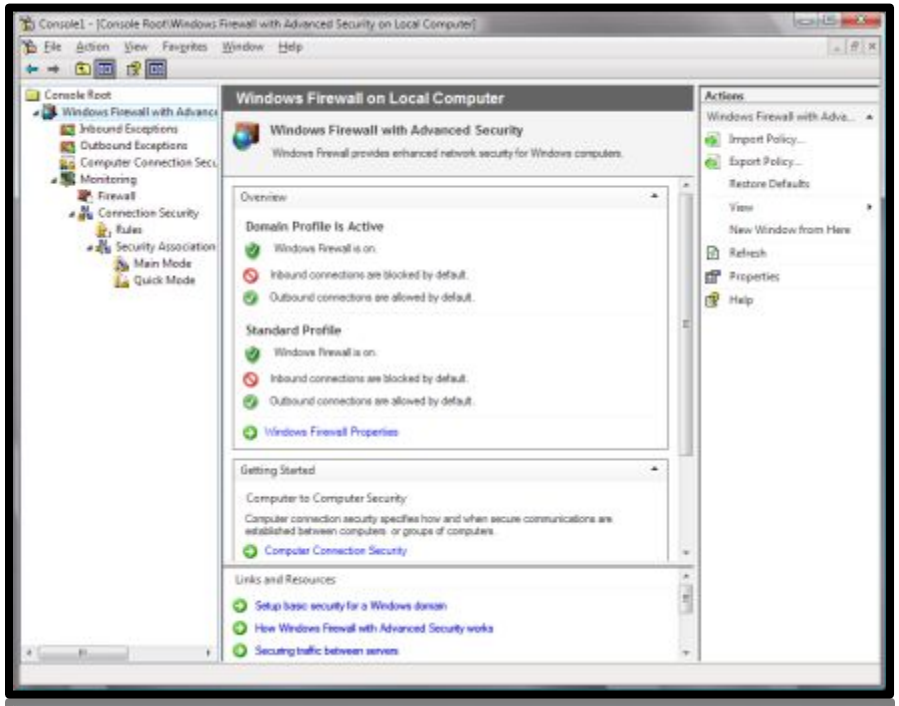
Изоляция сегментов с помощью IPSec

Ограничение доступа к ресурсам в

Управляемый друг с

Определить логические границы

Фильтрация сетевого трафика



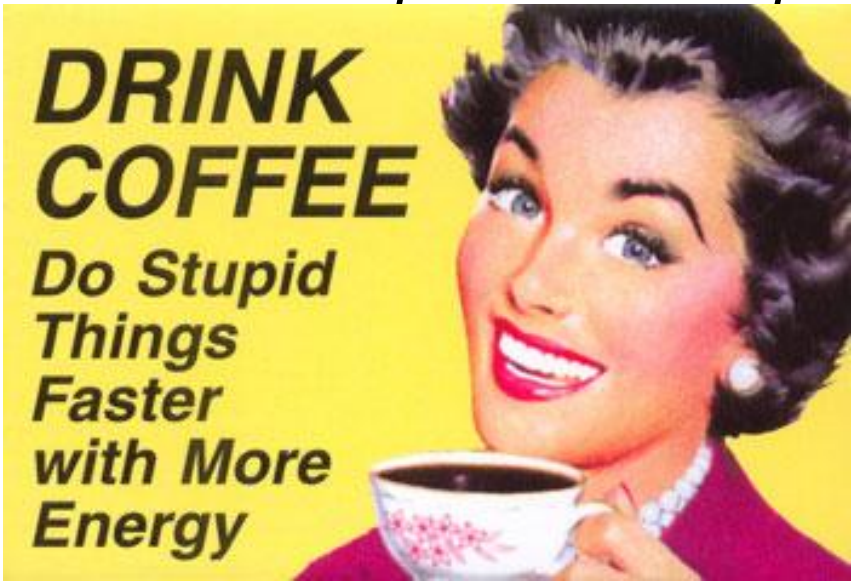
- Использовать Windows Firewall with Advanced Security (WFAS) на хосте и ВМ
- Настройки межсетевого экрана распространять с помощью групповых политик
- Правила межсетевого экрана могут применяться через портал самообслуживания
- Использование IDS/IPS для обнаружения аномалий сетевого трафика и реагирования на них.

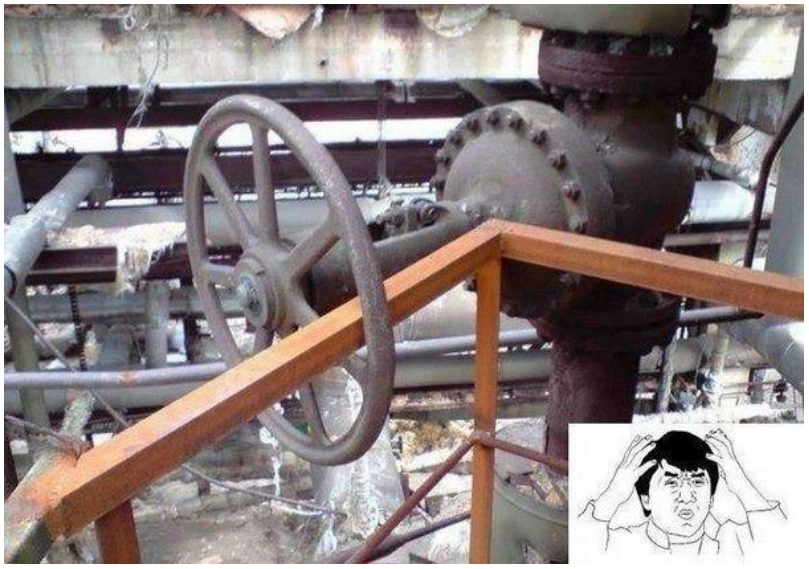
Централизация управления

Развертывание виртуальных машин одной кнопкой прекрасно….

Внедрение виртуализации без управления способно принести больше вреда, чем пользы.

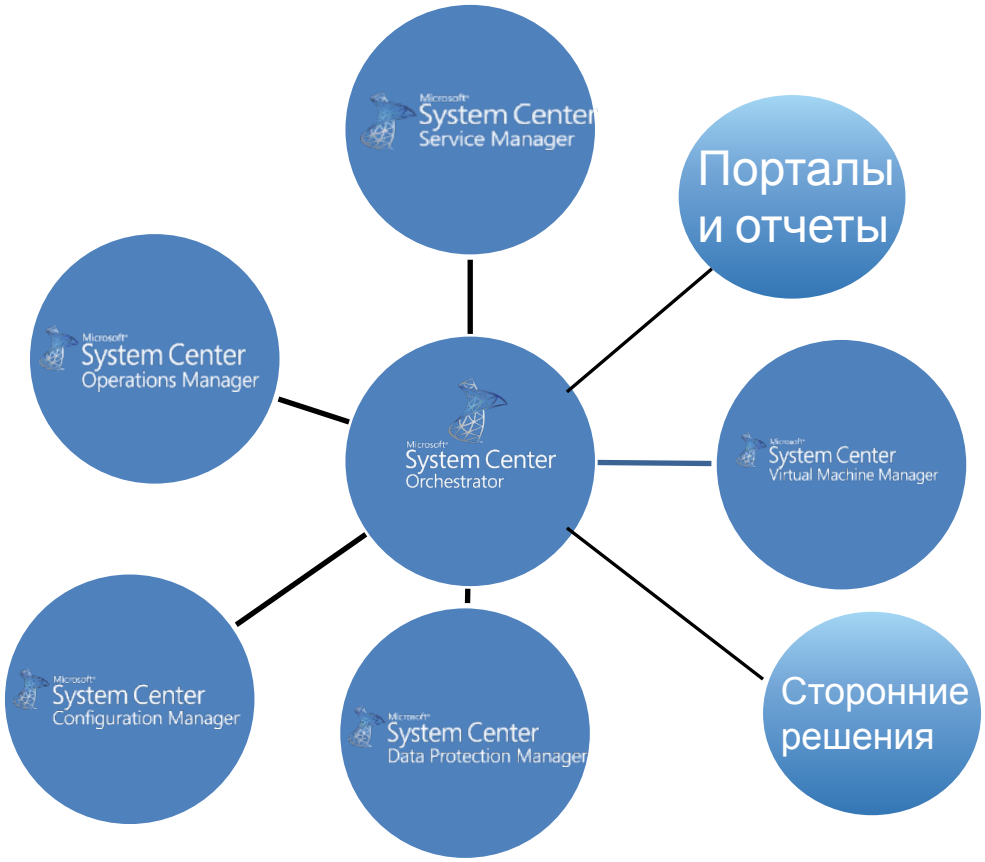
Результатом автоматизации бардака всегда становится *автоматизированный бардак*!





Автоматизация управления, мониторинга и отчетности

- Сложность управления инфраструктурой ухудшает безопасность
  - Ручные операции на множестве систем выполняемые множеством администраторов приводят к ошибкам
  - Если вы не знаете что есть в вашей инфраструктуре вы не можете этим управлять!



Автоматизация управления, мониторинга и отчетности

ИТ задачи

Event Mgmt

Service Desk

Asset/CMDB

Configuration

Virtual

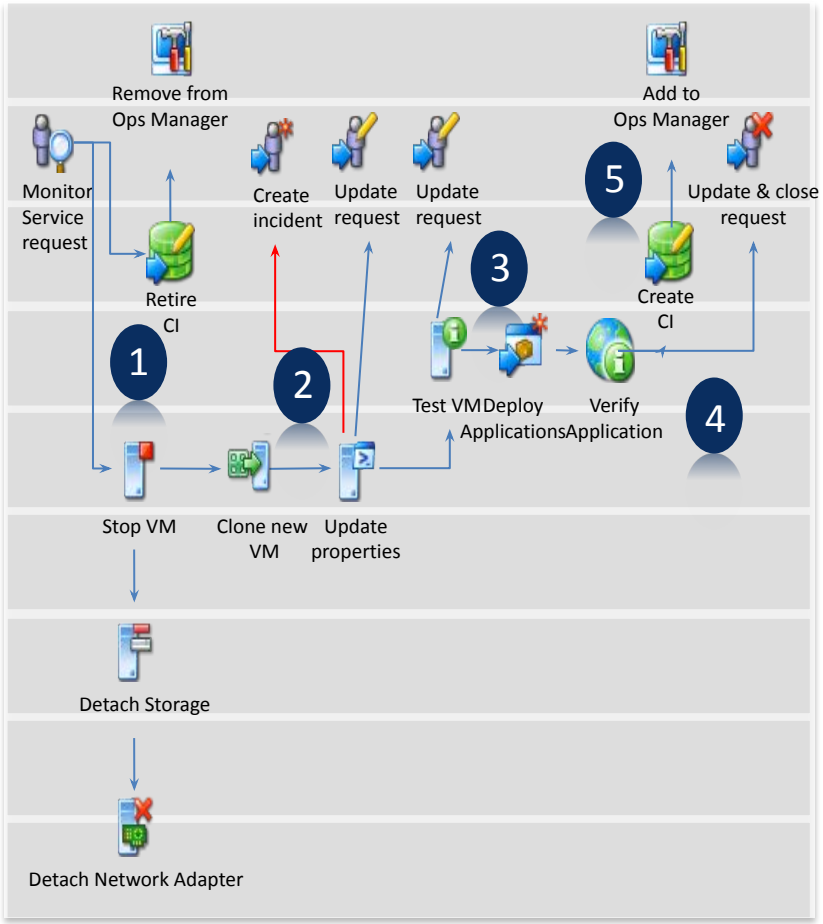
Security

Storage

Server

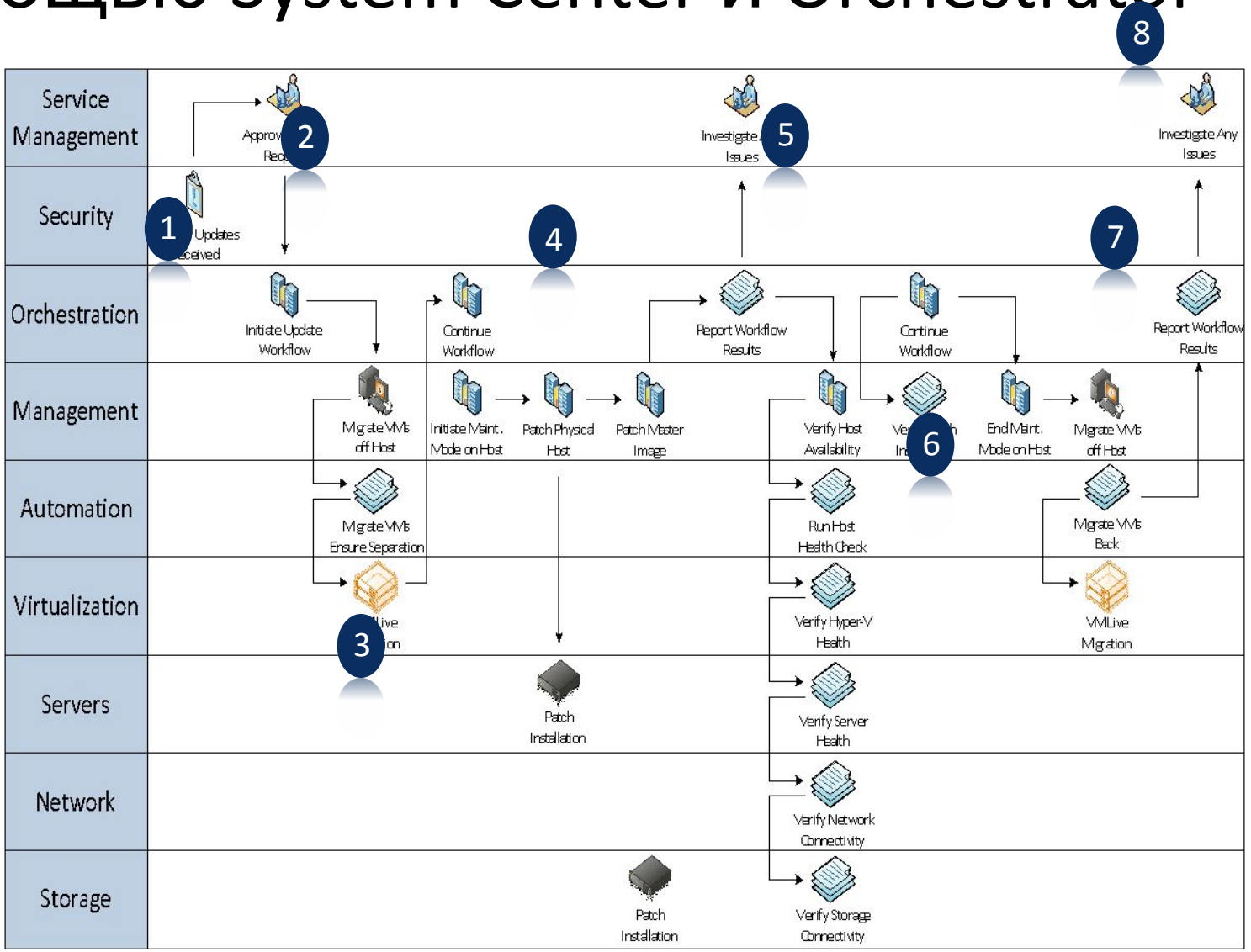
Network

Процесс развертывания ВМ



1. Остановить устаревшую ВМ, освободить ресурсы, удалить из CMDB
2. Клонировать ВМ
3. Обновить ВМ, развернуть приложения
4. Зарегистрировать новый объект в CMDB и подключить мониторинг

Обновление хостов кластера Hyper-V с помощью System Center и Orchestrator

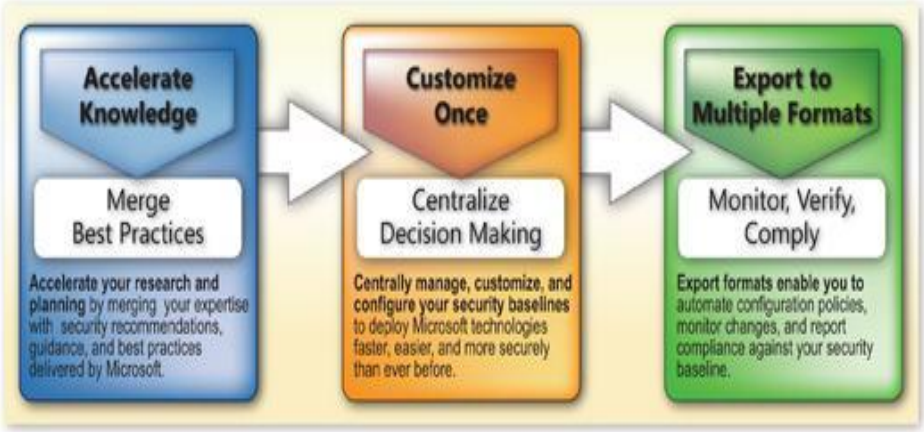


Соответствие Хостов, ВМ, приложений требованиям политики ИБ

- Проверьте базовую конфигурацию рекомендуемую Microsoft для:
  - Членов домена, Хостов Hyper-V, Контроллеров домена и.т.д.

- Применение базовой конфигурации
  - Экспорт из библиотеки Microsoft Security Compliance Manager в групповую политику

- Измерение соответствия базовой конфигурации
  - Экспорт из библиотеки Microsoft Security Compliance Export в DCM пакет Configuration Manager и создание отчетов по собранным данным



Библиотека рекомендаций Microsoft Security Compliance Manager

- Windows Server 2008 R2 AD Certificate Services Server Baseline
- Windows Server 2008 R2 Attack Surface Reference.xlsx
- Windows Server 2008 R2 DHCP Server Baseline
- Windows Server 2008 R2 DNS Server Baseline
- Windows Server 2008 R2 Domain Baseline
- Windows Server 2008 R2 Domain Controller Baseline
- Windows Server 2008 R2 Member Server Baseline
- Windows Server 2008 R2 File Server Baseline
- Windows Server 2008 R2 Hyper-V Baseline
- Windows Server 2008 R2 Network Access Services Server Baseline
- Windows Server 2008 R2 Print Server Baseline
- Windows Server 2008 R2 Remote Desktop Services Baseline
- Windows Server 2008 R2 Web Server Baseline
- Windows Server 2008 R2 Setting Pack
- Windows Server 2008 R2 Security Guide.docx
- Windows 7, Windows Vista, Windows XP,
- Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Internet Explorer 8
- Microsoft Office 2010, and Office 2007

Защита данных от утечек и инсайдеров

- Защита информации в течении всего цикла жизни
- Шифрование данных основных приложений Microsoft

- Шифрование директорий с данными
- Хранение ключей EFS на смарткарте

- Защита данных и ОС
- Безопасная передача данных партнерам и клиентам

Панацея?

Все проблемы безопасности частного облака технически средствами не решить:

- Единая система аутентификации и авторизации доступа к физическим и виртуальным элементам облачного ЦОД
- Единая система мониторинга, управления, развертывания, обновления System Center
- Разделение полномочий развертывания, защиты, аудита
- Включение в проекты сотрудника отдела безопасности
- Строжайшие политики физического доступа в ЦОД

Ресурсы

- Microsoft Virtualization:
  - http://www.microsoft.com/virtualization
- Microsoft Virtualization TechCenter
  - http://technet.microsoft.com/ru-ru/virtualization/default.aspx
- Microsoft Hyper-V Security Guide
  - http://technet.microsoft.com/en-us/library/dd569113.aspx
- Windows Virtualization Blog Site:
  - http://blogs.technet.com/virtualization/default.aspx
- Windows Server 2008 Virtualization & Consolidation:
  - http://www.microsoft.com/windowsserver2008/en/us/virtualization-consolidation.aspx
- System Center Virtual Machine Manager (SCVMM)
  - http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/default.aspx
- Hyper-V FAQ
  - http://www.microsoft.com/windowsserver2008/en/us/hyperv-faq.aspx

Ресурсы

- Virtualization Hypervisors" evaluation criteria: http://www.burtongroup.com/Client/Research/Document.aspx?cid=1569
- Security Best Practices for Hyper-V and Server Virtualization http://bit.ly/hq6chE
- Virtualization Security Overview by Cisco http://bit.ly/eJqi0Z
- Private Cloud Solution Hub
  - www.technet.com/cloud/private-cloud
- Private Cloud IaaS Page
  - www. microsoft.com/privatecloud

Вопросы?

abeshkov@microsoft.com
http://beshkov.ru
http://twitter.com/abeshkov