Защита виртуальной инфраструктуры

Практические рекомендации

Антон Жбанков

Центральный филиал ОАО МегаФон

Сергей Щадных

ЗАО Фирма ЦВ «ПРОТЕК»

Общие понятия

Безопасность информации

- Конфиденциальность
- Доступность
- Целостность

Инфраструктура

1. **В компании работает 1000 человек**
2. **1 Офис**
3. **1 ЦОД**
4. **Практически вся серверная инфраструктура виртуальная**
5. **2 или более недорогих дисковых массивов**

Необходимые сервисы

1. **Active Directory, DNS**
2. **Файловый серверы**
3. **DHCP серверы**
4. **MS Exchange Server 2010**
5. **Сервер печати**
6. **Терминальный доступ Microsoft Terminal Servers**
7. **Базы данных**
8. **MS ISA**
9. **Унаследованные критически важные сервисы**
10. **Специфические серверы приложений имеющие встроенную кластеризацию**
11. **VDI**
12. **Управление виртуальной средой через vCenter**
13. **Резервное копирование**
14. **WDS, WSUS**
15. **Антивирус**

Active Directory и DNS

1. **3+ контроллера домена**
   - 1 контроллер домена для Мастера операций инфраструктуры
   - 2+ контроллера домена для остальных мастеров операций и глобальных каталогов
2. **Контроллеры глобальных каталогов располагаются на различных дисковых массивах**
3. **ВМ в HA кластере**
4. **Anti-affinity DRS**

Файловые серверы

Имеют встроенный механизм горячего резервирования с помощью Microsoft DFS и DFS-R

1. 2 варианта построения:

- С использованием RDM
- С использованием VMDK

2. 2 варианта резервного копирования данных:

- Виртуальную машину целиком
- При помощи агента в гостевой ОС

3. ВМ в HA кластере

4. Anti-affinity DRS

DHCP Сервер

1. 2 варианта горячего резервирования:

- Через MSCS
- Настройка 2-х DHCP серверов с непересекающимися Scope

2. DHCP не рекомендуется устанавливать на Domain Controller

3. ВМ в HA кластере

4. Anti-affinity DRS

MS Exchange Server 2010

Имеет встроенный механизм резервирования:

1. **Хранение почтовых ящиков пользователей (Mailbox Server Role) через механизм DAG (Data Availability Group), включённый в редакции Enterprise**
2. **Доставка сообщений (Hub Transport Server Role) через DNS**
3. **Доступ пользователей к своим почтовым ящикам (Client Access Server Role) через Microsoft NLB**

Подробности настройки Microsoft Exchange Server 2010 под VMware ESX можно прочитать здесь:

http://www.vmware.com/solutions/business-critical-apps/exchange/

Серверы печати

1. **Возможно горячее резервирование на основе MSCS**
2. **Spooling располагается на отдельном диске, исключенном из резервного копирования**
3. **ВМ в HA кластере**

Серверы терминального доступа

1. Имеют встроенный механизм горячего резервирования с помощью Microsoft NLB и Session Broker

2. На серверах приложений необходимо отключить функции Hot Add для невозможности отключения пользователем сетевых адаптеров из терминальной сессии.

3. ВМ в HA кластере

Серверы Баз Данных

1. **Кластеризация серверов БД средствами БД**

2. **Данные БД размещаются на отдельном диске**
   - Осуществлять резервное копирование системного диска в заданиях резервного копирования VM
   - Резервные копии данных создавать средствами БД или специализированным решением

3. **ВМ в HA кластере**

4. **Рекомендации VMware**
   - http://www.vmware.com/solutions/business-critical-apps/sql/
   - http://www.vmware.com/solutions/business-critical-apps/oracle/

Microsoft ISA Server

1. Имеет встроенный механизм горячего резервирования с помощью Microsoft NLB и кластеризацию на уровне приложения

2. Рекомендуется использование внешней кластеризованной БД

3. ВМ в HA кластере

4. Anti-affinity DRS

Унаследованные критически важные сервисы

1. Не имеют встроенных механизмов горячего резервирования

2. Рекомендуется использовать Fault Tolerance для критически важных виртуальных машин

3. ВМ в HA кластере

Специфические серверы приложений, имеющих встроенную кластеризацию

1. Кластеризовать на уровне приложения
2. ВМ в HA кластере
3. Anti-affinity DRS

VDI

1. ВМ в HA кластере

2. Объединять несколько ВМ в одном задании резервного копирования для де-дупликации

3. Использовать Changed Block Tracking

vCenter

1. Обеспечить доступность DNS

2.1 Для не критического уровня доступности

- БД vCenter располагается на внешнем кластеризованном сервере БД
- В HA кластере

2.2 Для критического уровня доступности

- vCenter Server Heartbeat

Резервное копирование

2 подхода к резервному копированию:

1. **Централизованный**
2. **Децентрализованный**

Рекомендации:

1. **Не хранить резервные копии сервиса / данных на том же сервере где располагается сервис**
2. **Не хранить резервные копии на VMFS разделе**

Антивирус

1. Сервису не нужен механизм горячего резервирования
2. Располагать сервис централизованно
3. Разделять БД и сервер приложений

WDS, WSUS

1. Сервисам не нужен механизм горячего резервирования

2. Размещать необходимо в центральном и дополнительных офисах

vmware

Вопросы?